



NetScaler SDX 13.1

Machine translated content

Disclaimer

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

Contents

Introducción	4
Notas de la versión	4
Comience a utilizar la interfaz de usuario del Servicio de administración	5
Gobierno de datos	11
Introducción al servicio NetScaler ADM connect para dispositivos NetScaler SDX	14
Actualización de paquete único	17
Actualización de una instancia de NetScaler	19
Administre y supervise el dispositivo SDX	22
Dominios administrativos de SDX	29
Administración de la asignación de discos RAID en la plataforma SDX 22000	31
Descripción general de licencias de SDX	34
Visualizador de recursos SDX	37
Administrar interfaces	38
Tramas gigantes en dispositivos SDX	42
Configurar SNMP en dispositivos SDX	55
Configurar las notificaciones de syslog	61
Configurar notificaciones de correo	63
Configurar las notificaciones por SMS	64
Supervise y administre el estado en tiempo real de las entidades configuradas en un dispositivo SDX	64
Supervisión y administración de eventos generados en instancias de NetScaler	70
Soporte de Call Home para instancias de NetScaler en un dispositivo SDX	78
Supervisión del estado del sistema	81

Configurar los parámetros de notificación del sistema	84
Habilitar y inhabilitar funciones del Servicio de administración	85
Configurar el Servicio de administración	85
Configurar los ajustes de autenticación y autorización	89
Configuración del servidor de autenticación externo	94
Configurar la agregación de enlaces desde el Servicio de administración	101
Configuración de un canal desde el Servicio de administración	102
Listas de control de acceso	104
Configure un clúster de instancias de NetScaler	110
Configurar la agregación de enlaces de clúster	114
Configurar cifrados SSL para acceder de forma segura al Servicio de administración	119
Realice una copia de seguridad y restaure los datos de configuración del dispositivo SDX	127
Realizar un restablecimiento del dispositivo	132
Servidores de autenticación externos en cascada	136
Desbloquear a un usuario	137
Suministro de instancias de NetScaler	138
Administrar la capacidad de cifrado	154
Aprovisionar máquinas virtuales de terceros	161
SECUREMATRIX GSB	162
Seguridad web de Trend Micro InterScan	166
Protector de Websense	167
DNS y DHCP de BlueCat	172
CA Access Gateway	176
VM-Series de Palo Alto Networks	178

Implemente una instancia Citrix SD-WAN VPX en un dispositivo NetScaler SDX	180
Medición de ancho de banda en SDX	184
Configurar y administrar instancias de NetScaler	189
Instalar y administrar certificados SSL	191
Permitir el modo L2 en una instancia de NetScaler	196
Configuración de un MAC virtual en una interfaz	197
Genere direcciones MAC de partición para configurar una partición de administración en una instancia de NetScaler en el dispositivo SDX	200
Administración de cambios para instancias VPX	202
Supervise las instancias de NetScaler	203
Usar registros para supervisar las operaciones y los eventos	207
Casos de uso de dispositivos NetScaler SDX	210
Consolidación cuando las instancias del Servicio de administración y de NetScaler están en la misma red	211
Consolidación cuando las instancias del Servicio de administración y de NetScaler se encuentran en redes diferentes	213
Consolidación en todas las zonas de seguridad	215
Consolidación con interfaces dedicadas para cada instancia	216
Consolidación con el uso compartido de un puerto físico por más de una instancia	218
API de NITRO	220
Obtener el paquete NITRO	221
SDK de .NET	221
Servicios web REST	226
Cómo funciona NITRO	235
SDK de Java	236

Introducción

November 23, 2023

El dispositivo NetScaler SDX es una plataforma multiusuario en la que puede aprovisionar y administrar varias máquinas virtuales (instancias) de NetScaler. El dispositivo SDX aborda los requisitos de informática en la nube y de multiarrendamiento al permitir a un único administrador configurar y administrar el dispositivo y delegar la administración de cada instancia alojada en los arrendatarios. El dispositivo SDX permite al administrador del dispositivo proporcionar a cada arrendatario las siguientes ventajas:

- Una instancia completa. Cada instancia tiene los siguientes privilegios:
 - Recursos dedicados de CPU y memoria
 - Un espacio separado para las entidades
 - La independencia para ejecutar el lanzamiento y la compilación de su elección
 - Independencia del ciclo vital
- Una red completamente aislada. El tráfico destinado a una instancia en particular se envía solo a esa instancia.

El dispositivo SDX proporciona un servicio Management Service que se ha aprovisionado previamente en el dispositivo. Management Service proporciona una interfaz de usuario (modos HTTP y HTTPS) y una API para configurar, administrar y supervisar el dispositivo, Management Service y las instancias. Un certificado autofirmado de Citrix viene empaquetado previamente para admitir HTTPS. Citrix recomienda utilizar el modo HTTPS para acceder a la interfaz de usuario del Servicio de administración.

Notas de la versión

November 23, 2023

Las notas de la versión describen las mejoras, los cambios, las correcciones de errores y los problemas conocidos de una versión o compilación en particular del software NetScaler. Las notas de la versión de NetScaler SDX se incluyen como parte de las notas de la versión de ADC.

Para obtener información detallada sobre las mejoras, los problemas conocidos y las correcciones de errores del SDX 13.1, consulte las notas de la versión de [ADC](#).

Comience a utilizar la interfaz de usuario del Servicio de administración

November 23, 2023

Para comenzar a configurar, administrar y supervisar el dispositivo, el Servicio de administración y las instancias virtuales, conéctese a la interfaz de usuario del Servicio de administración mediante un explorador. A continuación, aprovisiona las instancias virtuales en el dispositivo.

Puede conectarse a la interfaz de usuario del Servicio de administración mediante uno de los siguientes exploradores compatibles:

- Internet Explorer
- Google Chrome
- Apple Safari
- Mozilla Firefox

Inicie sesión en la interfaz de usuario del Servicio de administración

1. En el campo Dirección del explorador web, escriba una de las siguientes opciones:

`http://Management Service IP Address`

O bien:

`https://Management Service IP Address`

2. En la página de inicio de sesión, en **Nombre de usuario** y **Contraseña**, escriba el nombre de usuario y la contraseña del Servicio de administración. El nombre de usuario predeterminado es `nsroot`. Si la contraseña predeterminada no funciona, intente escribir el número de serie del dispositivo. El código de barras del número de serie está disponible en la parte posterior del dispositivo. Después de iniciar sesión con las credenciales predeterminadas por primera vez, debe cambiar la contraseña `nsroot` predeterminada. Para obtener información sobre cómo cambiar la contraseña de administrador, consulte [Cambio de la contraseña de la cuenta de usuario predeterminada](#).
3. Haga clic en **Mostrar opciones** y, a continuación, haga lo siguiente:
 - a) En la lista **Comenzar en**, seleccione la página que debe mostrarse inmediatamente después de iniciar sesión en la interfaz de usuario. Las opciones disponibles son Inicio, Supervisión, Configuración, Documentación y Descargas. Por ejemplo, si quiere que Management Service muestre la página Configuración al iniciar sesión, seleccione **Configuración** en la lista **Iniciar en**.
 - b) En **Tiempo de espera**, escriba el tiempo (en minutos, horas o días) tras el que quiere que caduque la sesión. El valor de tiempo de espera mínimo es de 15 minutos.

La configuración de **Inicio en** y **Tiempo de espera** persiste en todas las sesiones. Sus valores predeterminados se restauran solo después de borrar la memoria caché.

4. Haga clic en Iniciar **sesión** para iniciar sesión en la interfaz de usuario del Servicio de administración.

Asistente de configuración inicial

Puede usar el Asistente de configuración para completar todas las configuraciones por primera vez en un solo flujo.

Puede usar el asistente para configurar los detalles de configuración de red y los ajustes del sistema, cambiar la contraseña administrativa predeterminada y administrar y actualizar las licencias.

También puede utilizar este asistente para modificar los detalles de configuración de red que especificó para el dispositivo SDX durante la configuración inicial.

Para acceder al asistente, vaya a **Configuración > Sistema** y, en **Configurar dispositivo**, haga clic en **Asistente de configuración**. Introduzca valores para los siguientes parámetros.

- **Interfaz: interfaz** de administración que conecta el dispositivo a una estación de trabajo o red de administración. Valores posibles: 0/1, 0/2. Predeterminado: 0/1.
- **Puerta de enlace:** dirección IP del enrutador que reenvía el tráfico fuera de la subred del dispositivo.
- Active la casilla de verificación IPv4 si quiere utilizar la dirección IPv4 para el Servicio de administración e introduzca los detalles de los siguientes parámetros:
 - **IP de administración del dispositivo:** la dirección IPv4 que se usa para acceder al Servicio de administración mediante un explorador web.
 - **Máscara de red: máscara** de subred en la que se encuentra el dispositivo SDX.
- **DNS:** dirección IPv4 del servidor DNS principal. Las direcciones IPv6 no son compatibles con el servidor DNS principal.
- Seleccione la casilla de verificación IPv6 si desea utilizar la dirección IPv6 para el Servicio de administración e introduzca los detalles de los siguientes parámetros:
 - **Dirección IP del Servicio de administración:** la dirección IPv6 que se utiliza para acceder al Servicio de administración mediante un explorador web.
 - **Dirección IPv6 de puerta de enlace:** la dirección IPv4 del enrutador que reenvía el tráfico fuera de la subred del dispositivo.
- Seleccione **DNS adicional** para agregar las direcciones IP del servidor DNS como un servidor DNS adicional aparte del servidor DNS principal. Las direcciones IP pueden ser IPv4 o IPv6.

Importante.

Citrix recomienda mantener la compatibilidad de dispositivos inhabilitada para mejorar la seguridad. Para inhabilitar la compatibilidad del dispositivo, vaya a **Sistema > Configuración de red** y desactive la casilla de verificación **Configurar compatibilidad del dispositivo**.

En **Configuración del sistema**, puede especificar que el Servicio de administración y una instancia de NetScaler deben comunicarse entre sí únicamente a través de un canal seguro. También puede restringir el acceso a la interfaz de usuario del Servicio de administración. Los clientes pueden iniciar sesión en la interfaz de usuario del Servicio de administración solo mediante https.

Puede modificar la zona horaria del Servicio de administración y Citrix Hypervisor. La zona horaria predeterminada es UTC. Puede cambiar la contraseña administrativa si selecciona la casilla de verificación **Cambiar contraseña** y escribe la nueva contraseña.

En Administrar licencias, puede administrar y asignar licencias. Puede utilizar el número de serie del hardware (HSN) o el código de acceso de licencia para asignar sus licencias. De forma alternativa, si ya hay una licencia en el equipo local, puede cargarla en el dispositivo.

Seleccione las licencias en el dispositivo y haga clic en **Listo** para completar la configuración inicial.

Aprovisionamiento de instancias en un dispositivo SDX

Puede aprovisionar una o más instancias de NetScaler o de terceros en el dispositivo SDX mediante Management Service. La cantidad de instancias que puede instalar depende de la licencia que haya adquirido. Si la cantidad de instancias agregadas es igual a la cantidad especificada en la licencia, Management Service no permite aprovisionar más instancias.

Para obtener información sobre el aprovisionamiento de instancias de [terceros](#), consulte [Máquinas virtuales de terceros](#).

Acceso a la consola

Puede acceder a la consola de las instancias de NetScaler, el Servicio de administración, Citrix Hypervisor y las máquinas virtuales de terceros desde la interfaz del Servicio de administración. Este acceso resulta útil para depurar y solucionar problemas de las instancias alojadas en el dispositivo SDX.

Para acceder a la consola de máquinas virtuales, vaya a la lista de instancias, seleccione la máquina virtual de la lista y, en la lista **Acción**, haga clic en **Acceso a la consola**.

Para acceder a la consola del Servicio de administración o Citrix Hypervisor, vaya a **Configuración > Sistema** y, en **Acceso a la consola**, haga clic en el enlace **Management Service** o **Citrix Hypervisor**.

Nota: El explorador Internet Explorer no admite el acceso a la consola. Citrix recomienda usar la función de acceso a la consola solo a través de sesiones HTTPS del Servicio de administración.

Estadísticas del Servicio de administración

El panel ahora incluye estadísticas del Servicio de administración para supervisar el uso de los recursos de memoria, CPU y disco por parte del Servicio de administración en el dispositivo SDX.



Inicio de sesión único en el Servicio de administración y las instancias de NetScaler

Después de iniciar sesión en Management Service con sus credenciales de usuario, no tiene que volver a proporcionar las credenciales de usuario para iniciar sesión en una instancia. De forma predeterminada, el valor de **Tiempo de espera** se establece en 30 minutos y la ficha de configuración se abre en una nueva ventana del explorador.

Administrar la página de inicio

La página inicial del Servicio de administración proporciona una vista de alto nivel del rendimiento del dispositivo SDX y de las instancias aprovisionadas en el dispositivo. La información sobre el dispositivo y la instancia SDX se muestra en gadgets que puede agregar y eliminar en función de sus requisitos.

Los siguientes gadgets están disponibles en la página de inicio de forma predeterminada.

- **Recursos del sistema:** muestra el número total de núcleos de CPU, el número total de chips SSL, el número de chips SSL libres, la memoria total y la memoria libre en el dispositivo.

**CPU de sistema

Uso de memoria (%):** Muestra el porcentaje de uso de la CPU y la memoria del dispositivo en formato gráfico.

- **Rendimiento WAN/LAN del sistema (Mbps):** muestra el rendimiento total del dispositivo SDX para el tráfico entrante y saliente en un gráfico que se traza en tiempo real y se actualiza a intervalos regulares.
- **Instancias de NetScaler:** muestra las propiedades de las instancias de NetScaler. Las propiedades que se muestran son Nombre, Estado de la VM, Estado de la instancia, Dirección IP, Rx (Mbps), Tx (Mbps), HTTP Req/s y Uso de CPU (%) y Uso de memoria (%).
Nota: En el primer inicio de sesión, la página de inicio no muestra ningún dato relacionado con las instancias de NetScaler porque no ha aprovisionado ninguna instancia en su dispositivo.
- **Sucesos de supervisión del estado:** muestra los últimos 25 eventos, con su gravedad, mensaje y la fecha y hora en que se produjo el evento.

Puede hacer lo siguiente en la página de inicio:

- Ver y ocultar los detalles de la instancia de NetScaler
Puede ver y ocultar los detalles de una instancia de NetScaler concreta haciendo clic en el nombre de la instancia en la columna Nombre.
También puede hacer clic en Expandir todo para expandir todos los nodos de la instancia y en Contraer todo para contraer todos los nodos de la instancia.
- Agregar y eliminar gadgets
También puede agregar gadgets para ver otra información del sistema.
Para agregar estos gadgets, haga clic en el botón de flecha («) situado en la esquina superior derecha de la página de inicio, escriba palabras clave en el cuadro de búsqueda y, a continuación, haga clic en Ir. Los caracteres permitidos son: a-z, A-Z, 0—9, ^, \$, * y _ . Haga clic en Ir sin

escribir ningún carácter en el cuadro de búsqueda para mostrar todos los gadgets disponibles. Cuando se muestre el gadget, haga clic en Agregar al panel de control.

Actualmente, puede agregar los siguientes gadgets a la página de inicio:

- **Detalles del hipervisor:** El gadget Detalles de Hypervisor muestra detalles sobre el tiempo de actividad, la edición, la versión, el nombre calificado de iSCSI (IQN), el código del producto, el número de serie, la fecha de compilación y el número de compilación de Citrix Hypervisor.
- **Licencias:** el gadget Licencias muestra los siguientes detalles: la plataforma de hardware SDX, el número máximo de instancias admitidas en la plataforma, el rendimiento máximo admitido en Mbps y el rendimiento disponible en Mbps.

Si elimina un gadget que está disponible en la página de inicio de forma predeterminada, puede volver a agregarlo a la página de inicio buscando el gadget.

Puertos

Los siguientes puertos deben estar abiertos en el dispositivo SDX para que funcione correctamente.

Tipo	Puerto	Detalles
TCP	80	Se utiliza para solicitudes HTTP (GUI y NITRO) entrantes. Una de las interfaces principales para acceder a la interfaz de SDX Management Service.
TCP	443	Se utiliza para solicitudes HTTP (GUI y NITRO) entrantes seguras. Una de las interfaces principales para acceder a la interfaz de SDX Management Service.
TCP	22	Se utiliza para el acceso SSH y SCP a la interfaz de SDX Management Service.
UDP	162	La interfaz del Servicio de administración del SDX escucha las capturas de SNMP de las instancias de NetScaler alojadas en el dispositivo SDX.

Tipo	Puerto	Detalles
UDP	161	La interfaz de SDX Management Service escucha las solicitudes de paseo/obtención de SNMP.

Gobierno de datos

November 23, 2023

¿Qué es una conexión de servicio ADM de NetScaler?

El servicio NetScaler Application Delivery Management (ADM) Service Connect es una función que permite la incorporación perfecta de los dispositivos NetScaler SDX al servicio NetScaler ADM. Esta función permite que el dispositivo NetScaler SDX se conecte de forma automática y segura con el servicio NetScaler ADM y envíarle datos del sistema, de uso y de telemetría. Con base en estos datos, obtiene información y recomendaciones para su infraestructura NetScaler en el servicio NetScaler ADM.

Al utilizar la función de conexión del servicio NetScaler ADM e incorporar sus dispositivos NetScaler SDX al servicio NetScaler ADM, puede administrar todos sus activos de NetScaler y NetScaler Gateway, ya sea de forma local o en la nube. Además, se beneficia del acceso a un amplio conjunto de funciones de visibilidad que ayudan a identificar rápidamente los problemas de rendimiento, el uso elevado de recursos, los errores críticos, etc. El servicio NetScaler ADM proporciona una amplia gama de capacidades para las instancias y aplicaciones de NetScaler. Para obtener más información sobre el servicio NetScaler ADM, consulte [NetScaler Application Delivery Management Service](#).

Importante

- Este documento se refiere a los dispositivos NetScaler SDX. Para obtener más información sobre el dispositivo NetScaler, consulte [Introducción al servicio NetScaler ADM service connect para dispositivos NetScaler](#).
- NetScaler Gateway también admite la función de conexión al servicio NetScaler ADM. Para mayor facilidad, el dispositivo NetScaler Gateway no se llama explícitamente en las secciones consecutivas.

Nota:

Se ha lanzado la función de conexión al servicio ADM de NetScaler para las instancias de NetScaler y

las instancias de NetScaler Gateway. Sin embargo, la funcionalidad correspondiente del servicio ADM de NetScaler estará disponible en la próxima versión. El valor de esta función se revelará pronto con la versión del servicio NetScaler ADM. Citrix actualizará esta nota cuando ocurra.

Los beneficios de esta nueva capacidad se pueden utilizar una vez que se publique en el servicio ADM de NetScaler.

¿Qué es el servicio NetScaler ADM?

El servicio NetScaler ADM es una solución basada en la nube que le ayuda a administrar, monitorear, orquestar, automatizar y solucionar problemas de sus instancias de NetScaler SDX, al proporcionarle información analítica y recomendaciones seleccionadas basadas en el aprendizaje automático sobre las instancias de NetScaler SDX y sobre el estado, el rendimiento y la seguridad de las aplicaciones. Para obtener más información, consulte Descripción general del [servicio NetScaler ADM](#).

¿Cómo se habilita la conexión al servicio NetScaler ADM?

La conexión del servicio NetScaler ADM está habilitada de forma predeterminada, después de instalar o actualizar NetScaler SDX a la versión 13.1.

¿Qué datos se capturan mediante NetScaler ADM service connect?

Los siguientes detalles se capturan mediante NetScaler ADM service connect:

- **Detalles de NetScaler SDX**
 - Dirección IP de administración
 - Descripción de la plataforma
 - Tipo de plataforma
 - Nombre de host
 - ID del sistema
 - Identificador de serie codificado
 - Versión
 - Identificación de serie
 - ID de host
 - Tipo
 - Tipo de construcción
- **Métricas de uso clave**
 - Porcentaje de CPU de gestión
 - Porcentaje de uso de memoria

- Porcentaje de uso de CPU
- Tiempo de actividad del sistema
- Fecha y hora del sistema

¿Cómo se utilizan los datos?

Al recopilar los datos, NetScaler puede proporcionar información detallada y oportuna sobre sus instalaciones de NetScaler SDX, que incluye lo siguiente:

- **Métricas clave.** Los detalles de las métricas clave relacionadas con la CPU, la memoria, el rendimiento y el rendimiento SSL destacan el comportamiento anómalo en las instancias de NetScaler SDX.
- **Errores críticos.** Cualquier error crítico que pudiera haberse producido en las instancias de NetScaler.
- **Asesoramiento de implementación.** Identifique las instancias de NetScaler que se implementan en modo independiente pero que tienen un alto rendimiento y son vulnerables a un único punto de falla.

¿Durante cuánto tiempo se conservan los datos recopilados?

Todos los datos recopilados se conservan durante no más de 13 meses.

Si decide terminar el uso del servicio inhabilitando la función de conexión del servicio de NetScaler ADM de NetScaler, todos los datos recopilados anteriormente se eliminarán después de un período de 30 días.

¿Dónde se almacenan los datos y qué tan seguros son?

Todos los datos recopilados por NetScaler ADM service connect se almacenan en una de las tres regiones: Estados Unidos, Unión Europea y Australia y Nueva Zelanda (ANZ). Para obtener más información, consulte [Consideraciones geográficas](#).

Los datos se almacenan de forma segura con estricto aislamiento de arrendatarios en la capa de base de datos.

¿Cómo inhabilitar la conexión del servicio NetScaler ADM?

Si quiere inhabilitar la recopilación de datos mediante la conexión del servicio NetScaler ADM, consulte [Cómo habilitar y inhabilitar la conexión del servicio NetScaler ADM](#).

Introducción al servicio NetScaler ADM connect para dispositivos NetScaler SDX

November 23, 2023

El servicio NetScaler ADM es una solución basada en la nube que le ayuda a administrar, supervisar, orquestar, automatizar y solucionar problemas de sus dispositivos NetScaler SDX. También proporciona información analítica y recomendaciones basadas en aprendizaje automático para el estado, el rendimiento y la seguridad de sus aplicaciones. Para obtener más información, consulte el servicio [NetScaler ADM](#).

La conexión del servicio NetScaler Application Delivery Management (ADM) es una función que permite la incorporación sin problemas de dispositivos NetScaler SDX en el servicio NetScaler ADM. Esta función ayuda a que los dispositivos NetScaler SDX y el servicio NetScaler ADM funcionen como una solución integral, que ofrece a los clientes múltiples beneficios.

La función de conexión del servicio NetScaler ADM permite que la instancia de NetScaler SDX se conecte automáticamente con el servicio NetScaler ADM y le envíe datos de sistema, uso y telemetría. Con estos datos, el servicio ADM de NetScaler le ofrece información y recomendaciones sobre su infraestructura NetScaler SDX, como la identificación rápida de los problemas de rendimiento y el alto uso de los recursos.

Para aprovechar la potencia del servicio NetScaler ADM, puede optar por integrar sus dispositivos NetScaler SDX al servicio NetScaler ADM. El proceso de incorporación utiliza la conexión del servicio ADM y hace que la experiencia sea fluida y rápida para usted.

Puntos que tener en cuenta

- NetScaler ADM Service Connect ya está disponible en las instancias de NetScaler MPX, SDX y VPX y en los dispositivos NetScaler Gateway.
- La conexión del servicio NetScaler ADM aún no está disponible en el servicio NetScaler ADM.

Para obtener más información, consulte [Gobernanza de datos](#).

¿Cómo conecta el servicio NetScaler ADM la asistencia con el servicio NetScaler ADM?

A continuación se muestra un flujo de trabajo de alto nivel sobre cómo la función de conexión de servicio de NetScaler ADM en NetScaler interactúa con el servicio NetScaler ADM.

1. La función de conexión del servicio NetScaler ADM en el dispositivo NetScaler SDX se conecta automáticamente con el servicio NetScaler ADM mediante una solicitud de sonda periódica.

2. Esta solicitud contiene datos del sistema, de uso y de telemetría, mediante los cuales el servicio ADM de NetScaler le proporciona información y recomendaciones sobre su infraestructura de NetScaler, como la identificación rápida de los problemas de rendimiento y el uso elevado de los recursos.
3. Puede ver la información y las recomendaciones y decidir integrar sus dispositivos NetScaler SDX en el servicio NetScaler ADM para empezar a administrar sus dispositivos NetScaler SDX.
4. Cuando decide incorporar, la función de conexión del servicio NetScaler ADM ayuda a completar la incorporación sin problemas.

¿En qué versiones de NetScaler es compatible NetScaler ADM service connect?

La conexión del servicio NetScaler ADM se admite en todas las plataformas NetScaler y en todos los modelos de dispositivos (MPX, VPX y SDX). A partir de la versión 13.0 compilación 64.xx de NetScaler, la conexión al servicio NetScaler ADM está habilitada de forma predeterminada para los dispositivos NetScaler SDX.

¿Cómo habilitar la conexión del servicio NetScaler ADM?

Si ya es cliente de NetScaler y actualiza a NetScaler versión 13.0 build 64.xx, la conexión del servicio NetScaler ADM está habilitada de forma predeterminada como parte del proceso de actualización.

Si es un cliente nuevo de NetScaler, al instalar NetScaler versión 13.0 build 64.xx, la conexión del servicio NetScaler ADM está habilitada de forma predeterminada como parte del proceso de instalación.

Nota

A diferencia de los nuevos dispositivos NetScaler, los dispositivos NetScaler SDX existentes encuentran la ruta a través de Citrix Insight Service (CIS) o Call Home.

¿Cómo habilitar y inhabilitar la conexión del servicio NetScaler ADM?

Puede habilitar y inhabilitar la conexión del servicio NetScaler ADM desde los métodos CLI, GUI o API de NITRO.

Uso de la CLI

Para habilitar la conexión del servicio NetScaler ADM mediante la CLI

En la línea de comandos, escriba:

```
1 set autoreg_setting autoreg=true
```


Para inhabilitar la conexión del servicio NetScaler ADM mediante la CLI

En la línea de comandos, escriba:

```
1 set autoreg_setting autoreg=false
```

Para mostrar la configuración de conexión al servicio NetScaler ADM mediante la CLI

```
1 show autoreg_setting
2
3             autoreg: true
4
5     is_banner_displayed: true
6
7 Done
```

Uso de la GUI

Para inhabilitar la conexión del servicio NetScaler ADM mediante la GUI de NetScaler

1. Vaya a **Sistema**. En la página **Sistema**, haga clic en **Configurar la conexión del servicio NetScaler ADM** en la sección **Configuración del sistema**.
2. En la página **Configurar parámetros de ADM**, desactive **Habilitar la conexión del servicio NetScaler ADM** y haga clic en **Aceptar**.



Uso de la API de NITRO

Puede inhabilitar la conexión del servicio NetScaler ADM mediante el comando NITRO.

```
curl -X PUT -H "Content-Type:application/json"http://192.0.2.10/nitro/v1/config/sdx_autoreg -d '{ "sdx_autoreg":{ "autoreg":"false" } } ' -u nsroot:Test@1
```

Comportamiento del agente integrado de NetScaler ADM

A partir de la versión 13.0, compilación 61.xx y versiones posteriores de NetScaler, las instancias SDX de NetScaler cuentan con un agente integrado con la función de conexión al servicio ADM. El agente integrado de NetScaler ADM disponible en las instancias de NetScaler SDX se inicia como un demonio activo y se comunica con el servicio ADM. Una vez establecida la comunicación con el servicio ADM, el agente integrado se actualiza automáticamente a la última versión de software con regularidad.

Referencias

Para obtener más información acerca de NetScaler ADM Service connect, consulte los siguientes temas:

- Gobierno de datos: [gobernanza de datos](#).
- Servicio NetScaler ADM: Servicio de administración de entrega de aplicaciones de [NetScaler](#).

Actualización de paquete único

November 23, 2023

Nota: La conexión del servicio NetScaler ADM está habilitada de forma predeterminada, después de instalar o actualizar el dispositivo NetScaler SDX a la versión 13.1. Para obtener más información, consulte Data Governance y NetScaler ADM Service connect.

La actualización de paquete único, disponible a partir de la versión 11.0 y posteriores, combina todos los componentes, excepto la imagen de instancia de NetScaler VPX y el firmware de LOM, en un solo archivo de imagen. Este archivo se denomina imagen SDX.

Nota

A partir de la versión 12.0 compilación 57.19, el firmware de administración de luces apagadas (LOM) se agrega a la SBI y los clientes de Citrix no tienen que actualizar la LOM por separado. Citrix no escribe el firmware de la LOM.

Con esta imagen, puede actualizar todos los componentes en un solo paso, eliminando las posibilidades de incompatibilidad entre varios componentes. Una actualización de un solo paquete también garantiza que el dispositivo ejecute siempre una versión que Citrix haya probado y compatible. Como todos los componentes SDX se combinan en un solo archivo, el archivo de imagen SDX es más grande que el archivo de imagen del Servicio de administración.

El nombre del archivo de la imagen es del formato `build-sdx-13.1-<build_number>.tgz`. Después de actualizar Management Service a SDX 13.1, la nueva GUI no muestra las opciones para cargar el archivo de imagen de Citrix Hypervisor, los paquetes complementarios o las revisiones. Falta las opciones porque el SDX 13.1 no admite la actualización de componentes individuales.

Puntos que tener en cuenta

- La actualización de un solo paquete es un proceso de varios pasos que puede tardar hasta 90 minutos.
- En primer lugar, Management Service se actualiza a la versión más reciente proporcionada. Durante la actualización, es posible que se pierda la conectividad con el Servicio de administración. Vuelva a conectarse a Management Service para supervisar el estado de la actualización.
- A continuación, el nuevo Servicio de administración actualiza Citrix Hypervisor y completa el resto de la actualización del dispositivo. Management Service de la versión 11.0 y posteriores puede realizar la actualización completa de Citrix Hypervisor.
- No reinicie el dispositivo durante la actualización de Citrix Hypervisor.
- Citrix recomienda utilizar una consola serie de Citrix Hypervisor (o consola LOM) para supervisar la actualización de Citrix Hypervisor.

Actualice todo el dispositivo a la versión 13.1

Nota: El proceso de actualización reinicia todo el dispositivo SDX, incluidas todas las instancias VPX, varias veces. Antes de realizar este procedimiento, si las instancias VPX están en una configuración de alta disponibilidad, conmute por error todos los nodos de alta disponibilidad principales al nodo secundario. Si no tiene una implementación de alta disponibilidad, planifique el tiempo de inactividad en consecuencia.

Para actualizar el dispositivo:

1. Cargue el archivo de imagen de paquete único, vaya a **Configuración > Management Service > Imágenes de software**, a continuación, haga clic en **Cargar**.
2. Vaya a **Configuración > Sistema > Administración del sistema**.
3. En el grupo Administración del sistema, haga clic en **Actualizar dispositivo**.
El proceso de actualización tarda unos minutos.

Antes de la actualización, el Servicio de administración muestra la siguiente información:

- Nombre de archivo de imagen de paquete único.
- La versión actual de SDX que se ejecuta en el dispositivo.
- La versión seleccionada a la que se va a actualizar el dispositivo.
- Tiempo aproximado para actualizar el dispositivo.

- Información miscelánea.

Antes de hacer clic en **Actualizar dispositivo**, asegúrese de haber revisado toda la información que se muestra en pantalla. No puede abortar el proceso de actualización una vez que se inicia.

Rutas de actualización compatibles

	11.1	12.0	12.1	13.0	13.1	14.1
10.5 o 11.0	S	S	S	N*	N*	N*
11.1—65.x y versiones posteriores	NA	No recomendado	12.1-56.x y versiones posteriores	S	S	S
12.1	NA	NA	No recomendado	S	S	S

*A partir de las versiones anteriores de 10.5, 11.0 y 11.1, primero debe actualizar a la versión 11.1 o 12.1 y, a continuación, actualizar a la versión 13.0, 13.1 o 14.1.

Información relacionada

[Matriz de compatibilidad de hardware y software NetScaler SDX](#)

[Desmitificar el proceso de actualización del dispositivo NetScaler SDX](#)

Actualización de una instancia de NetScaler

November 23, 2023

Notas

- La conexión del servicio NetScaler ADM está habilitada de forma predeterminada, después de instalar o actualizar el dispositivo NetScaler SDX a la versión 13.1. Para obtener más información, consulte [Data Governance](#) y [NetScaler ADM Service connect](#).
- El proceso de actualización del dispositivo NetScaler SDX requiere un solo reinicio en lugar de dos reinicios a partir de la versión 13.1, compilación 37.x.

El proceso de actualización de las instancias de NetScaler implica cargar el archivo de compilación y, a continuación, actualizar la instancia de NetScaler.

Importante

No se admite la degradación de una instancia de ADC mediante Management Service. Usa la CLI de la instancia para desactualizar.

Cargue las imágenes del software NetScaler al dispositivo NetScaler SDX antes de actualizar las instancias de NetScaler. Para instalar una instancia nueva, necesita el archivo NetScaler XVA.

En el panel **Imágenes de software**, puede ver los siguientes detalles.

- **Nombre:** nombre del archivo de imagen de software de instancia de NetScaler. El nombre del archivo contiene el número de versión y el número de compilación. Por ejemplo, el nombre de archivo build-10-53.5_nc.tgz se refiere a la versión 10 build 53.5.
- **Última modificación:** fecha en la que se modificó por última vez el archivo.
- **Tamaño:** Tamaño, en MB, del archivo.

Para cargar una imagen de software

1. En el panel de navegación, expanda NetScaler y, a continuación, haga clic en **Imágenes de software**.
2. En el panel **Imágenes de software**, haga clic en **Cargar**.
3. En el cuadro de diálogo **Cargar imagen de software NetScaler**, haga clic en **Examinar** y seleccione el archivo de imagen NetScaler que quiere cargar.
4. Haga clic en **Cargar**. El archivo de imagen aparece en el panel Imágenes del software NetScaler.

Para crear una copia de seguridad mediante la descarga de un archivo de compilación

1. En el panel Imágenes de software, seleccione el archivo que quiere descargar y, a continuación, haga clic en **Descargar**.
2. En el cuadro de mensaje, en la lista **Guardar**, seleccione **Guardar como**.
3. En el cuadro de mensaje Guardar como, busque la ubicación en la que quiera guardar el archivo y, a continuación, haga clic en **Guardar**.

Para cargar un archivo XVA

1. En el panel de navegación, expanda NetScaler y, a continuación, haga clic en **Imágenes de software**.
2. En el panel Imágenes de software, en la ficha **Archivos XVA**, haga clic en **Cargar**.

3. En el cuadro de diálogo **Cargar archivo XVA de NetScaler**, haga clic en **Examinar** y seleccione el archivo XVA de NetScaler que quiera cargar.
4. Haga clic en **Cargar**. El archivo XVA aparece en el panel **Archivos XVA**.

Para crear una copia de seguridad mediante la descarga de un archivo XVA

1. En el panel Archivos XVA, seleccione el archivo que quiere descargar y, a continuación, haga clic en **Descargar**.
2. En el cuadro de mensaje, en la lista Guardar, seleccione **Guardar como**.
3. En el cuadro de mensaje **Guardar como**, busque la ubicación en la que quiere guardar el archivo y, a continuación, haga clic en **Guardar**.

Actualizar instancias de NetScaler VPX

Puede usar Management Service para actualizar una o más de las instancias VPX que se ejecutan en el dispositivo. Antes de actualizar una instancia, asegúrese de haber cargado la compilación correcta en el dispositivo SDX.

Antes de empezar a actualizar cualquier instancia, asegúrese de que comprende el marco de licencias y los tipos de licencias. Una actualización de la edición de software (por ejemplo, de una edición estándar a la edición empresarial o de una edición empresarial a la edición platino) puede requerir nuevas licencias. Tenga en cuenta también lo siguiente:

- Para evitar cualquier pérdida de configuración, guarde la configuración en cada instancia antes de actualizar cualquier instancia.
- También puede actualizar una instancia individual desde el nodo Instancias. Para hacerlo, seleccione la instancia en el nodo Instancias. En el panel de detalles, seleccione la instancia y, a continuación, en el menú desplegable Acciones, haga clic en Actualizar.

Importante Si usa el Servicio de administración de SDX y no la GUI de VPX para actualizar las instancias de VPX, las imágenes de actualización forman parte del archivo de respaldo y le permiten restaurar la instancia sin problemas.

Para actualizar instancias VPX

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **NetScaler**.
2. En el panel de detalles, en **Configuración de NetScaler**, haga clic en **Actualizar**.
3. En el cuadro de diálogo **Actualizar NetScaler**, en **Imagen de software**, seleccione el archivo de compilación de actualización de NetScaler de la versión a la que quiere actualizar.

4. En la lista desplegable **Dirección IP de instancia**, seleccione las direcciones IP de las instancias que quiere actualizar.
5. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Información relacionada

[Matriz de compatibilidad de hardware y software NetScaler SDX](#)

[Desmitificar el proceso de actualización del dispositivo NetScaler SDX](#)

Administre y supervise el dispositivo SDX

February 15, 2024

Una vez que el dispositivo NetScaler SDX esté en funcionamiento, puede realizar diversas tareas para administrar y supervisar el dispositivo desde la interfaz de usuario del Servicio de administración.

Modificar la configuración de red del dispositivo SDX

Puede modificar los detalles de configuración de red que proporcionó para el dispositivo SDX durante la configuración inicial.

Para modificar la configuración de red del dispositivo SDX, haga clic en **Sistema**. En el panel **Sistema**, en el grupo **Dispositivo de configuración**, haga clic en **Configuración de red** e introduzca los detalles en el asistente.

Nota: En la **configuración de red**, al habilitar el acceso al Citrix Hypervisor, aparece el mensaje de advertencia “El acceso se inhabilitará automáticamente después de seis horas”.

Cambiar la contraseña de la cuenta de usuario predeterminada

La cuenta de usuario predeterminada proporciona acceso completo a todas las funciones del dispositivo NetScaler SDX. Para preservar la seguridad, use la cuenta de administrador predeterminada solo cuando sea necesario. Solo las personas cuyas funciones requieren acceso completo deben conocer la contraseña de la cuenta de administrador predeterminada. Citrix recomienda cambiar la contraseña de administrador predeterminada con frecuencia. Si pierde la contraseña, puede restablecer la contraseña al valor predeterminado volviendo la configuración del dispositivo a los valores predeterminados de fábrica y, a continuación, puede cambiarla.

Para cambiar la contraseña de la cuenta de usuario predeterminada, haga clic en **Sistema > Administración de usuario > Usuarios**. Seleccione un usuario y haga clic en **Modificar** para cambiar la contraseña.

Modificar la zona horaria en el dispositivo

Puede modificar la zona horaria del Servicio de administración y Citrix Hypervisor. La zona horaria predeterminada es UTC.

Para modificar la zona horaria, haga clic en **Sistema** y, en el grupo **Configuración del sistema**, haga clic en **Cambiar zona horaria**.

Modificar el nombre de host del dispositivo

Para cambiar el nombre de host del Servicio de administración, vaya a **Sistema > Configuración del sistema > Cambiar nombre de host**.

Se realizará una copia de seguridad del nombre de host de Citrix Hypervisor y se restaurará durante la operación de copia de seguridad o restauración. Durante el restablecimiento de la configuración, el nombre de host de Citrix Hypervisor se restablecerá al valor predeterminado “netscaler-sdx”.

Filtrado de VLAN

El filtrado de VLAN proporciona segregación de datos entre instancias VPX que comparten un puerto físico. Por ejemplo, si ha configurado dos instancias VPX en dos VLAN diferentes y habilita el filtrado de VLAN, una instancia no puede ver el tráfico de la otra instancia. Si el filtrado de VLAN está inhabilitado, todas las instancias pueden ver los paquetes de difusión etiquetados o no etiquetados, pero los paquetes se descartan en el nivel de software. Si el filtrado de VLAN está habilitado, cada paquete de difusión etiquetado llega solo a la instancia que pertenece a la VLAN etiquetada correspondiente. Si ninguna de las instancias pertenece a la VLAN etiquetada correspondiente, el paquete se pierde en el nivel de hardware (NIC).

Si el filtrado de VLAN está habilitado en una interfaz, se puede usar un número limitado de VLAN etiquetadas en esa interfaz. 63 VLAN etiquetadas en una interfaz 10G y 32 VLAN etiquetadas en una interfaz 1G. Una instancia VPX solo recibe los paquetes que tienen los ID de VLAN configurados. Reinicie las instancias VPX asociadas a una interfaz si cambia el estado del filtro VLAN de INHABILITADO a HABILITADO en esa interfaz.

El filtrado de VLAN está habilitado de forma predeterminada en el dispositivo SDX. Si inhabilita el filtrado de VLAN en una interfaz, puede configurar hasta 4096 VLAN en esa interfaz.

Nota: El filtrado de VLAN solo se puede inhabilitar en un dispositivo SDX que ejecute Citrix Hypervisor versión 6.0.

Para habilitar el filtrado de VLAN en una interfaz, haga clic en **Sistema > Interfaces**. Seleccione una interfaz y haga clic en **Filtro de VLAN** e introduzca los detalles para habilitar el filtrado de VLAN.

Configurar la sincronización del reloj

Al habilitar la sincronización del Protocolo de tiempo de red (NTP), se reinicia el Servicio de administración. Puede configurar el dispositivo SDX para que sincronice su reloj local con un servidor NTP. Como resultado, el reloj del dispositivo SDX tiene la misma configuración de fecha y hora que los demás servidores de la red. La configuración de sincronización del reloj no cambia si el dispositivo se reinicia, actualiza o baja de categoría. Sin embargo, la configuración no se propaga a la instancia secundaria de NetScaler en una configuración de alta disponibilidad.

El reloj se sincroniza de inmediato si agrega un servidor NTP o cambia cualquiera de los parámetros de autenticación. También puede habilitar e inhabilitar explícitamente la sincronización NTP.

Nota: Si no tiene un servidor NTP local, puede encontrar una lista de servidores NTP públicos de acceso abierto en el sitio NTP oficial, <http://www.ntp.org>. Antes de configurar el de NetScaler para que use un servidor NTP público, asegúrese de leer la página Reglas de interacción (enlace incluido en todas las páginas Servidores de tiempo público).

Para configurar un servidor NTP, haga clic en **Sistema > Servidores NTP**.

Para habilitar la sincronización de NTP

1. En el panel de navegación, expanda **Sistema**, a continuación, haga clic en **Servidores NTP**.
2. En el panel de detalles, haga clic en **Sincronización NTP**.
3. En el cuadro de diálogo **Sincronización de NTP**, seleccione **Habilitar sincronización de NTP**.
4. Haga clic en **Aceptar**, a continuación, en **Cerrar**.

Para modificar las opciones de autenticación

1. En el panel de navegación, expanda **Sistema**, a continuación, haga clic en **Servidores NTP**.
2. En el panel de detalles, haga clic en **Parámetros de autenticación**.
3. En el cuadro de diálogo **Modificar opciones de autenticación**, defina los siguientes parámetros:
 - **Autenticación:** habilita la autenticación NTP. Valores posibles: Sí, NO. Predeterminado: Sí.
 - **ID de clave de confianza:** Los ID de clave de confianza. Al agregar un servidor NTP, selecciona un identificador de clave de esta lista. Valor mínimo: 1. Valor máximo: 65534.
 - **Intervalo de revocación:** el intervalo entre la reautorización de ciertos valores criptográficos utilizados por el esquema Autokey, como una potencia de 2, en segundos. Valor predeterminado: 17 ($2^{17} = 36$ horas).

- **Intervalo de automax:** el intervalo entre la regeneración de la lista de claves de sesión utilizada con el protocolo Autokey, con una potencia de 2, en segundos. Valor predeterminado: 12 ($2^{12} = 1.1$ horas).

4. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Ver las propiedades del dispositivo SDX

Consulte las propiedades del sistema, como la cantidad de núcleos de CPU y chips SSL, la memoria total disponible y la memoria libre, y varios detalles del producto en la ficha **Configuración**.

Para ver las propiedades del dispositivo SDX, haga clic en la ficha **Configuración**.

Puede ver la siguiente información sobre los recursos del sistema, el hipervisor, la licencia y el sistema:

Recursos del sistema:

- **Núcleos de CPU totales;** la cantidad de núcleos de CPU en el dispositivo SDX.
- **Chips SSL totales:** el número total de chips SSL en el dispositivo SDX.
- **Chips SSL gratuitos:** el número total de chips SSL que no se han asignado a una instancia.
- **Memoria total (GB):** memoria total del equipo en GB.
- **Memoria libre (GB):** memoria del equipo libre en GB.

Información sobre hipervisores:

- **Tiempo de actividad: tiempo** transcurrido desde que se reinició el dispositivo por última vez, en número de días, horas y minutos.
- **Edición:** La edición del Citrix Hypervisor que se instala en el dispositivo SDX.
- **Versión:** la versión de Citrix Hypervisor que está instalada en el dispositivo SDX.
- **IQN iSCSI:** Nombre calificado de iSCSI.
- **Código de producto:** código de producto de Citrix Hypervisor.
- **Número de serie:** número de serie de Citrix Hypervisor.
- **Fecha de compilación:** fecha de compilación de Citrix Hypervisor.
- **Número de compilación:** número de compilación de Citrix Hypervisor.
- **Paquete complementario:** versión del paquete complementario instalado en el dispositivo SDX.

Información de licencia:

- **Plataforma:** número de modelo de la plataforma de hardware, según la licencia instalada.
- **Instancias máximas:** la cantidad máxima de instancias que puede configurar en el dispositivo SDX, en función de la licencia instalada.
- **Instancias disponibles (compartidas):** la cantidad de instancias que se pueden configurar en función de la cantidad de núcleos de CPU que aún están disponibles.
- **Rendimiento máximo (Mbps):** el rendimiento máximo que se puede lograr en el dispositivo, en función de la licencia instalada.
- **Rendimiento disponible (Mbps):** el rendimiento disponible en función de la licencia instalada.

Información del sistema:

- **Plataforma:** número de modelo de la plataforma de hardware.
- **Producto:** Tipo de producto NetScaler.
- **Compilación: lanzamiento y compilación** de NetScaler que se ejecuta en el dispositivo SDX.
- **Dirección IP:** dirección IP del servicio de gestión.
- **ID de host: ID** de host de Citrix Hypervisor.
- **ID del sistema: ID** del sistema Citrix Hypervisor.
- ****Número de serie: número de serie de**** Citrix Hypervisor.
- **Hora del sistema:** La hora del sistema se muestra en formato Día Mes Fecha Horas:Mín:Seg Zona horaria Año.
- **Tiempo de inactividad: tiempo** transcurrido desde que se reinició el Servicio de administración por última vez, en la cantidad de días, horas y minutos.
- **Versión de BIOS:** versión de BIOS.

Ver el rendimiento del dispositivo en tiempo

El rendimiento total del dispositivo SDX para el tráfico entrante y saliente se representa en tiempo real en un gráfico que se actualiza a intervalos regulares. De forma predeterminada, los rendimientos del tráfico entrante y saliente se trazan juntos en el gráfico.

Para ver el rendimiento del dispositivo SDX, en la GUI haga clic en **Panel de control** y compruebe el **rendimiento del sistema (Mbps)**.

Ver el uso de la CPU y la memoria

Puede ver un gráfico del uso de la CPU y la memoria del dispositivo. El gráfico se traza en tiempo real y se actualiza a intervalos regulares.

Para ver el uso de CPU y memoria del dispositivo SDX, en la GUI haga clic en **Panel de control** y compruebe **Estadísticas del Servicio de administración**.

Ver el uso de CPU para todos los núcleos

Puede ver el uso de cada núcleo de CPU en el dispositivo SDX.

El panel **Uso del núcleo de la CPU** muestra los siguientes detalles:

- **Número de núcleo:** el número de núcleo de la CPU en el dispositivo.
- **CPU física:** el número de CPU física de ese núcleo.
- **Hyper Threads:** Los hyper threads asociados a ese núcleo de CPU.
- **Instancias:** las instancias que utilizan ese núcleo de CPU.
- **Uso promedio del núcleo:** El uso promedio del núcleo, expresado como porcentaje.

Para ver el uso de CPU de todos los núcleos del dispositivo SDX, en la GUI haga clic en **Panel** y compruebe **Uso de CPU del sistema (%)**.

Instale un certificado SSL en el dispositivo SDX

El dispositivo SDX se envía con un certificado SSL predeterminado. Por motivos de seguridad, es posible que quiera reemplazar este certificado por su propio certificado SSL. Para ello, primero debe cargar el certificado SSL en Management Service y, a continuación, instalar el certificado. La instalación de un certificado SSL termina todas las sesiones actuales de los clientes con Management Service. Inicie sesión en Management Service para cualquier tarea de configuración adicional.

Para instalar un certificado SSL, haga clic en **Sistema**. En el grupo **Configurar dispositivo**, haga clic en **Instalar certificado SSL** e introduzca los detalles en el asistente.

Ver el certificado SSL en el Servicio de administración

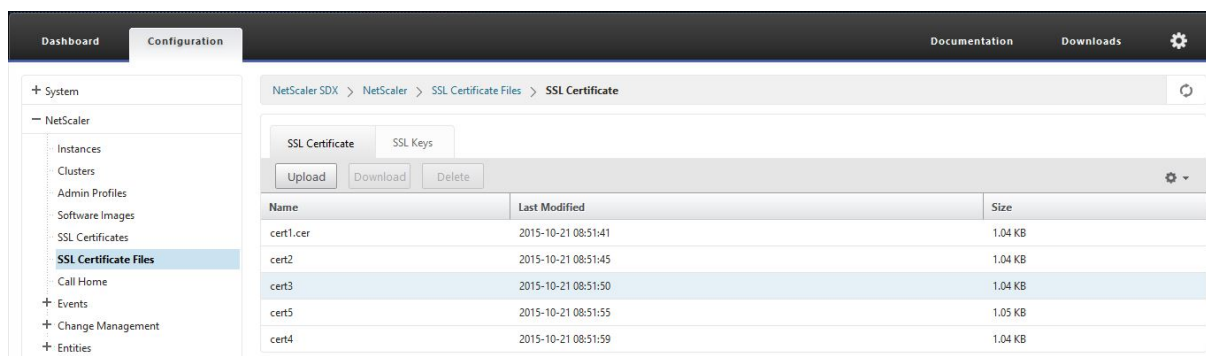
Management Service utiliza un certificado SSL para conexiones de cliente seguras. Vea los detalles de este certificado, como el estado de validez, el emisor, el asunto, los días hasta el vencimiento, las fechas de validez desde y hasta, la versión y el número de serie.

Para ver el certificado SSL, haga clic en **Sistema** y, en el grupo **Configurar dispositivo**, haga clic en **Ver certificado SSL**.

Certificados y claves SSL para instancias de NetScaler

Las vistas separadas de los certificados SSL y las claves para las instancias de NetScaler ofrecen una usabilidad mejorada. Utilice un nuevo nodo del Servicio de administración, los archivos de certificados SSL, para cargar y administrar los certificados SSL y los pares de claves públicas y privadas correspondientes que se pueden instalar en las instancias de NetScaler.

Para acceder a los certificados y claves SSL de las instancias de NetScaler, vaya a **Configuración > NetScaler > Archivos de certificados SSL**.



Modificación de la configuración

Por motivos de seguridad, puede especificar que el Servicio de administración y una instancia VPX deben comunicarse entre sí solo a través de un canal seguro. También puede restringir el acceso a la interfaz de usuario del Servicio de administración. Los clientes pueden iniciar sesión en la interfaz de usuario del Servicio de administración solo mediante https.

Para modificar la configuración del sistema, haga clic en **Configuración > Sistema** y, en el grupo Configuración del sistema, haga clic en **Cambiar configuración del sistema**.

Reinicie el dispositivo

Management Service proporciona una opción para reiniciar el dispositivo SDX. Durante el reinicio, el dispositivo apaga todas las instancias alojadas y, a continuación, reinicia Citrix Hypervisor. Cuando Citrix Hypervisor se reinicia, inicia todas las instancias alojadas junto con Management Service.

Para reiniciar el dispositivo, haga clic en **Configuración > Sistema** y, en el grupo Administración del sistema, haga clic en **Reiniciar dispositivo**.

Apague el dispositivo

Puede apagar el dispositivo SDX desde el Servicio de administración.

Para apagar el dispositivo, haga clic en **Configuración > Sistema**, en el grupo Administración del sistema, haga clic en **Apagar dispositivo**.

Dominios administrativos de SDX

November 23, 2023

La función de dominios administrativos de SDX le ayuda a crear varios dominios administrativos. Puede utilizar los dominios administrativos para segregación de recursos para diferentes departamentos. Por lo tanto, los dominios administrativos pueden mejorar el control sobre los recursos, y los recursos se pueden distribuir entre varios dominios para un uso óptimo.

Un dispositivo SDX se entrega con recursos fijos, como núcleos de CPU, rendimiento de datos, memoria, espacio en disco, chips SSL y una cantidad específica de instancias que se pueden aprovisionar. La cantidad de instancias que puede crear depende de la licencia.

Un dispositivo SDX admite hasta tres niveles de dominios administrativos. Cuando se envía el dispositivo, todos los recursos se asignan al propietario.

Todos los dominios administrativos que cree son subdominios del dominio propietario. En cada caso, los recursos del subdominio se asignan desde el conjunto de recursos del dominio principal. Los usuarios de un dominio administrativo tienen acceso a los recursos de ese dominio. No tienen acceso a los recursos de otros dominios en el mismo nivel jerárquico, ni a los recursos del dominio principal que no se han asignado a su dominio. Sin embargo, los usuarios de un dominio principal pueden acceder a los recursos de los subdominios de ese dominio.

Ejemplos de asignación de recursos a subdominios

En la tabla 1 se enumeran los recursos del dominio raíz predeterminado. El administrador de SDX puede asignar estos recursos a los subdominios. En este caso, el administrador puede asignar un máximo de, por ejemplo, 10 núcleos de CPU y 840 GB de espacio en disco.

Tabla 1. Recursos para propietarios

Núcleo CPU	10
Rendimiento (Mbps)	18500
Memoria (MB)	87300
Espacio en disco (GB)	840

Fichas SSL	36
Instancias	36

En la tabla 2 se enumeran los recursos asignados a un subdominio denominado *Test*. A este subdominio se le asignaron 5 de los 10 núcleos de CPU de su dominio principal, dejando 5 núcleos que se pueden asignar a otros subdominios del propietario.

Tabla 2. Recursos de Test Domain

Núcleo CPU	5
Rendimiento (Mbps)	1024
Memoria (MB)	2048
Espacio en disco (GB)	40
Fichas SSL	8
Instancias	4

Al crear subdominios, el administrador de dominio de *prueba* solo puede asignar los recursos enumerados en la Tabla 2. El dominio de *prueba* solo puede tener un nivel de subdominios, porque solo se pueden crear tres niveles de dominios.

En la ilustración siguiente se muestra otro ejemplo de asignación de recursos entre subdominios, mediante valores diferentes de los enumerados en las tablas 1 y 2.

Para crear un dominio administrativo, vaya a **Configuración > Sistema > Dominio administrativo** y seleccione las opciones que quiera. Siga las instrucciones que aparecen en pantalla. Una vez que se cree un dominio nuevo, inicie sesión en este dominio mediante la página de inicio de sesión del Servicio de administración y proporcione el nombre de dominio y el nombre de usuario. Por ejemplo, si creó un dominio llamado NewDomain con un usuario NewUser, inicie sesión como NewDomain\NewUser.

Asignar usuarios a los dominios

Cuando se crea un subdominio, se crean automáticamente dos grupos de usuarios: un grupo de administradores y un grupo de solo lectura. De forma predeterminada, cada usuario forma parte del grupo de administradores. Se puede agregar un usuario a varios grupos.

Administración de la asignación de discos RAID en la plataforma SDX 22000

November 23, 2023

Los dispositivos NetScaler SDX 22040/22060/22080/22100/22120 ahora incluyen un controlador de matriz redundante de discos independientes (RAID), que puede admitir hasta ocho discos físicos. Los discos múltiples proporcionan no solo mejoras en el rendimiento, sino también una mayor fiabilidad. La fiabilidad es especialmente importante para un dispositivo SDX, ya que el dispositivo aloja muchas máquinas virtuales y un error de disco afecta a varias máquinas virtuales. El controlador RAID en Management Service admite la configuración RAID 1, que implementa el espejado de disco. Es decir, dos discos mantienen los mismos datos. Si falla un disco de la matriz RAID 1, su espejo suministra inmediatamente todos los datos necesarios.

La duplicación de discos RAID 1 combina dos unidades físicas en una unidad lógica. La capacidad utilizable de una unidad lógica equivale a la capacidad de una de sus unidades físicas. La combinación de dos unidades de 1 terabyte, por ejemplo, crea una sola unidad lógica con una capacidad utilizable total de 1 terabyte. Esta combinación de unidades aparece para el dispositivo como una unidad lógica única.

El dispositivo SDX se entrega con una configuración que incluye la unidad lógica 0 y la unidad lógica 1. La unidad lógica 0 se asigna al Servicio de administración y el Citrix Hypervisor y la unidad lógica 1 se asigna a las instancias de NetScaler que aprovisiona. Para usar más unidades físicas, debe crear nuevas unidades lógicas.

Ver las propiedades y operaciones de las unidades

Un dispositivo SDX admite un máximo de ocho ranuras de unidades físicas, es decir, un par de cuatro ranuras en cada lado del dispositivo. Puede insertar unidades físicas en las ranuras. Antes de poder utilizar una unidad física, debe convertirla en parte de una unidad lógica.

En el Servicio de administración, la pantalla **Configuración > Sistema > RAID** incluye fichas para unidades lógicas, unidades físicas y repositorios de almacenamiento.

Unidades lógicas

En la ficha **Configuración > Sistema > RAID > Unidades lógicas**, puede ver el nombre, el estado, el tamaño de cada unidad lógica e información sobre las unidades físicas que lo componen. En la siguiente tabla se describen los estados de la unidad virtual.

State	Descripción
Óptimo	El estado de funcionamiento de la unidad virtual es bueno. Todas las unidades configuradas están en línea.
Degradado	La condición de funcionamiento de la unidad virtual no es óptima. Una de las unidades configuradas ha fallado o está desconectada.
Error	Se produjo un error en la unidad virtual.
Offline (Sin conexión)	La unidad virtual no está disponible para la controladora RAID.

También puede ver los detalles de las unidades físicas asociadas a la unidad lógica seleccionando la unidad lógica y haciendo clic en **Mostrar unidad física**.

Para crear una nueva unidad lógica

1. Vaya a **Configuración > Sistema > RAID** y seleccione la ficha **Unidades lógicas**.
2. Haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear disco lógico**, seleccione dos ranuras que contengan unidades físicas operativas y, a continuación, haga clic en **Crear**.

Unidades físicas

Un dispositivo SDX admite un máximo de ocho ranuras físicas, es decir, un par de cuatro ranuras en cada lado del dispositivo. En la ficha

Configuración > Sistema > RAID > Unidades físicas, puede ver la siguiente información:

- **Ranura:** ranura física asociada a la unidad física.
- **Tamaño:**—Tamaño de la unidad física.
- **Estado del firmware:**—Estado del firmware. Valores posibles:
 - **En línea, girada:**—La unidad física está activa y está siendo controlada por RAID.
 - **Sin configurar (bueno):** la unidad física está en buenas condiciones y se puede agregar como parte del par de unidades lógicas.
 - **Sin configurar (incorrecto):** la unidad física no está en buenas condiciones y no se puede agregar como parte de una unidad lógica.
- **Estado extranjero:**—Indica si el disco está vacío.
- **Unidad lógica:**—Unidad lógica asociada.

En el panel **Unidades físicas**, puede realizar las siguientes acciones en las unidades físicas:

- **Inicializar:**—Inicializar el disco. Puede inicializar la unidad física si no está en buen estado y debe agregarse como parte del par de unidades lógicas.
- **Rebuild:**inicia una reconstrucción de la unidad. Cuando se produce un error en una unidad de un grupo de unidades, puede volver a crear la unidad volviendo a crear los datos almacenados en la unidad antes de que fallara. La controladora RAID vuelve a crear los datos almacenados en las demás unidades del grupo de unidades.
- **Localizar:**ubique la unidad en el dispositivo, lo que se indica haciendo que el LED de actividad de la unidad asociado a la unidad parpadee.
- **Detener ubicación:**deje de localizar la unidad en el dispositivo.
- **Preparar para quitar:**desactive la unidad física seleccionada para que se pueda quitar.

Repositorio de almacenamiento

En la ficha **Configuración > Sistema > RAID > Repositorio de almacenamiento**, puede ver el estado de los repositorios de almacenamiento en el dispositivo SDX. También puede ver información sobre una unidad de repositorio de almacenamiento de información que no esté conectada, y puede quitarla seleccionándola y haciendo clic en **Quitar**. La ficha **Repositorio de almacenamiento** muestra la siguiente información sobre cada repositorio de almacenamiento:

- **Name:**—Nombre de la unidad del repositorio de almacenamiento.
- **Is Drive Attached:**indica si el repositorio de almacenamiento está conectado o no. Si la unidad no está conectada, puede hacer clic en **Quitar** para eliminarla.
- **Tamaño:**—Tamaño del repositorio de almacenamiento.
- **Utilizado:**—Cantidad de espacio en el repositorio de almacenamiento en uso.

Agregue una unidad lógica al dispositivo SDX 22000 Para agregar una unidad lógica adicional a la plataforma SDX 22000:

1. Inicie sesión en Management Service.
2. Navegue hasta **Configuración > Sistema > RAID**.
3. En la parte posterior del dispositivo SDX 22000, inserte las dos SSD en blanco en las ranuras números 4 y 5. Puede agregar las SSD en un sistema en ejecución.
Nota: Asegúrese de que las SSD estén certificadas por NetScaler.
4. En Management Service, vaya a **Configuración > Sistema > RAID** y a la ficha **Unidades físicas**. Verá las SSD que agregó.
5. Vaya a la ficha **Unidad lógica** y haga clic en **Agregar**.
6. En la página **Crear disco lógico**:
 - a) En la lista desplegable **Primera ranura**, seleccione 4.

b) En la lista desplegable **Segunda ranura**, seleccione 5.

c) Haga clic en **Crear**.

Nota: En Management Service, el número de ranura comienza por cero. Por lo tanto, la numeración de ranuras en Management Service difiere de la numeración de ranuras del dispositivo físico.

La unidad lógica se crea y aparece en la

ficha Unidad lógica. Haga clic en el icono de actualización para actualizar el orden de las unidades lógicas.

Agregue una segunda unidad lógica en el dispositivo SDX 22000 Para agregar otra unidad lógica, inserte las SSD en las ranuras números 6 y 7. En la página

Crear disco lógico, seleccione 6 en la lista **Primera ranura** y seleccione 7 en la lista **Segunda ranura**.

Reemplace una unidad SSD defectuosa por una unidad SSD en blanco Para reemplazar una unidad SSD defectuosa por una unidad SSD vacía:

1. Navegue hasta **Configuración > Sistema > RAID**.
2. En la ficha **Unidades físicas**, seleccione la unidad defectuosa que quiere reemplazar.
3. Haga clic en **Preparar para quitar** para quitar la unidad.
4. Haga clic en el icono de actualización para actualizar la lista de unidades físicas.
5. Retire físicamente la unidad defectuosa de la ranura.
6. Inserte la nueva SSD verificada de Citrix en la ranura de la que extrajo la SSD defectuosa.
7. En Management Service, vaya a **Configuración > Sistema > RAID**. El nuevo SSD aparece en la sección **Unidades físicas**. El proceso de reconstrucción de la unidad se inicia automáticamente.

Haga clic en el icono de actualización para comprobar el estado del proceso de reconstrucción. Cuando finalice el proceso de reconstrucción, puede ver el estado En línea, hilado en la columna **Estado del firmware**.

Descripción general de licencias de SDX

February 15, 2024

En el Servicio de administración de NetScaler SDX, puede utilizar el número de serie de hardware (HSN) o el código de acceso a la licencia para asignar las licencias. El software Management Service obtiene internamente el número de serie de su dispositivo y Citrix envía el código de acceso a la licencia por correo electrónico cuando compra una licencia.

De forma alternativa, si ya hay una licencia en el equipo local, puede cargarla en el dispositivo.

Para todas las demás funciones, como devolver o reasignar la licencia, debe utilizar el portal de licencias. Opcionalmente, puede seguir mediante el portal de licencias para la asignación de licencias. Para obtener más información, consulte [Administrar licencias en citrix.com](#).

Para obtener información sobre las opciones de licencia de SDX, consulte:

- [Elegir correctamente las opciones de plataforma y edición](#).
- [Modelos de licencias](#)

Nota: La instalación de una licencia perpetua o agrupada no requiere reiniciar el dispositivo SDX.

Requisitos previos

Para utilizar el número de serie del hardware o el código de acceso de licencia para asignar las licencias:

1. Debe poder acceder a los dominios públicos a través del dispositivo. Por ejemplo, el dispositivo debe poder acceder a www.citrix.com. El software de asignación de licencias accede internamente al portal de licencias de Citrix para su licencia. Para acceder a un dominio público, debe configurar la dirección IP del Servicio de administración y configurar un servidor DNS.
2. La licencia debe estar vinculada al hardware o debe tener un código de acceso de licencia válido.

Asignación de la licencia mediante Management Service

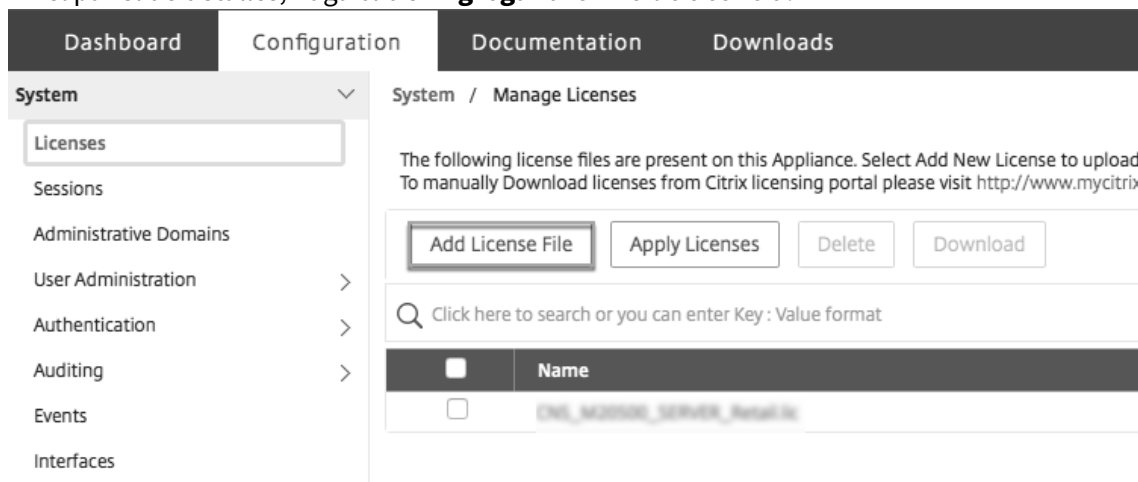
Si la licencia ya está vinculada al hardware, el proceso de asignación de licencias puede utilizar el número de serie del hardware. De lo contrario, debe escribir el código de acceso a la licencia.

Puede asignar licencias parcialmente según sea necesario para su implementación. Por ejemplo, si el archivo de licencia contiene 10 licencias, pero su requisito actual es solo para seis licencias, puede asignar seis licencias ahora y asignar más licencias más tarde. No puede asignar más del número total de licencias presentes en el archivo de licencia.

Para asignar su licencia

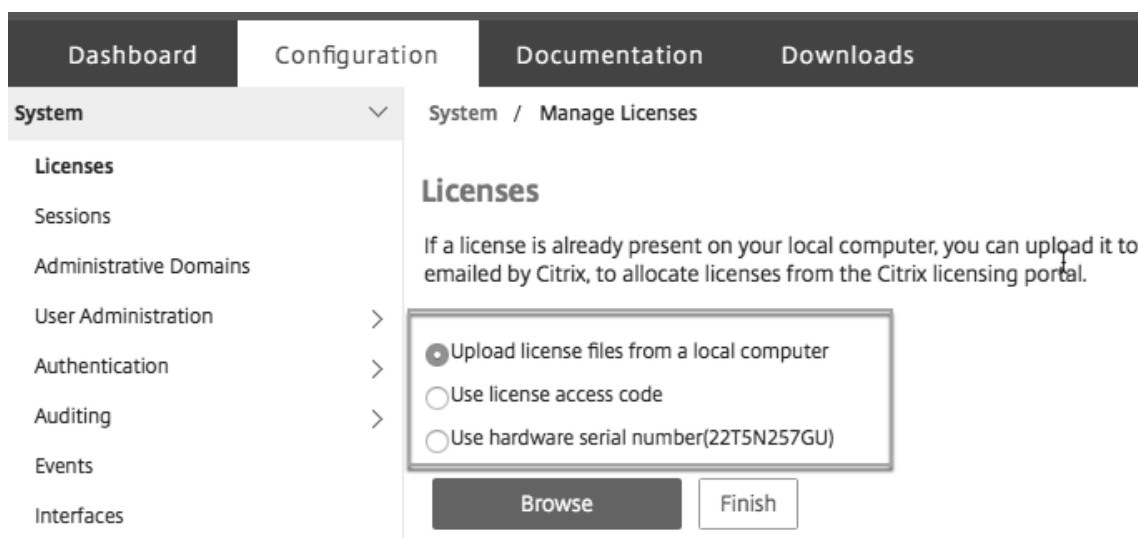
1. En un explorador web, escriba la dirección IP del Servicio de administración del dispositivo SDX (por ejemplo, <http://10.102.126.251>).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema > Licencias**.

4. En el panel de detalles, haga clic en **Agregar archivo de licencia**.



5. A continuación, selecciona una de las opciones:

- Cargar archivos de licencia desde un equipo local (esta opción está seleccionada de forma predeterminada)
- Usar un código de acceso de licencias
- Usar el número de serie del hardware



- **Cargar archivos de licencia desde un equipo local:** Si elige esta opción, haga clic en **Examinar** para seleccionar la licencia de capacidad cero de su máquina local. A continuación, haga clic en **Finalizar**.

1. Una vez que la licencia de capacidad cero se haya aplicado correctamente, la sección **Modo de licencia** aparece en la página **Licencias**.
2. Puede elegir entre **licencias agrupadas** o **licencias de grupo autogestionadas**.
3. En el campo **Nombre del servidor de licencias o Dirección IP**, introduzca los detalles del servidor de licencias.

4. En el campo **Número de puerto**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.
5. Haga clic en **Obtener licencias**.
6. En la ventana **Asignar licencias**, especifique las instancias y el ancho de banda requeridos y haga clic en **Asignar**.
7. En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y las instancias asignadas y el ancho de banda desde el grupo.

Nota:

A partir de la versión 13.1 de NetScaler, compilación 30.x, el dispositivo NetScaler SDX admite la licencia Self Managed Pool. Con esta licencia, puede simplificar y automatizar la carga de archivos de licencia al servidor de licencias. Puede usar NetScaler ADM para crear un marco de licencias que comprenda un ancho de banda común o una vCPU y un grupo de instancias.

- **Usar código de acceso de licencia:** Si selecciona esta opción, proporcione el **LAC** en el campo **Código de acceso de licencia** o seleccione la casilla de verificación para conectarse a través de un servidor proxy. A continuación, haga clic en **Obtener licencias**.
 - Seleccione el archivo de licencias que quiere utilizar para asignar las licencias.
 - En la columna **Asignar**, introduzca el número de licencias que se asignarán. A continuación, haga clic en **Descargar**.

Si se descarga la licencia, aparece en **Archivos de licencias**. Seleccione el archivo de licencia y haga clic en **Aplicar licencias**.

- **Usar número de serie de hardware:** Si elige esta opción, el software obtiene internamente el número de serie del dispositivo y lo utiliza para mostrar las licencias.
 - Haga clic en **Obtener licencias** o active la casilla de verificación **Conectar a través del servidor proxy** y, a continuación, haga clic en **Obtener licencias**.

Después de descargar el archivo de licencias, seleccione el archivo de licencia y haga clic en **Aplicar licencias**.

Para obtener información sobre las licencias agrupadas, consulte [Actualizar una licencia perpetua de un NetScaler SDX a una capacidad agrupada de NetScaler](#).

Visualizador de recursos SDX

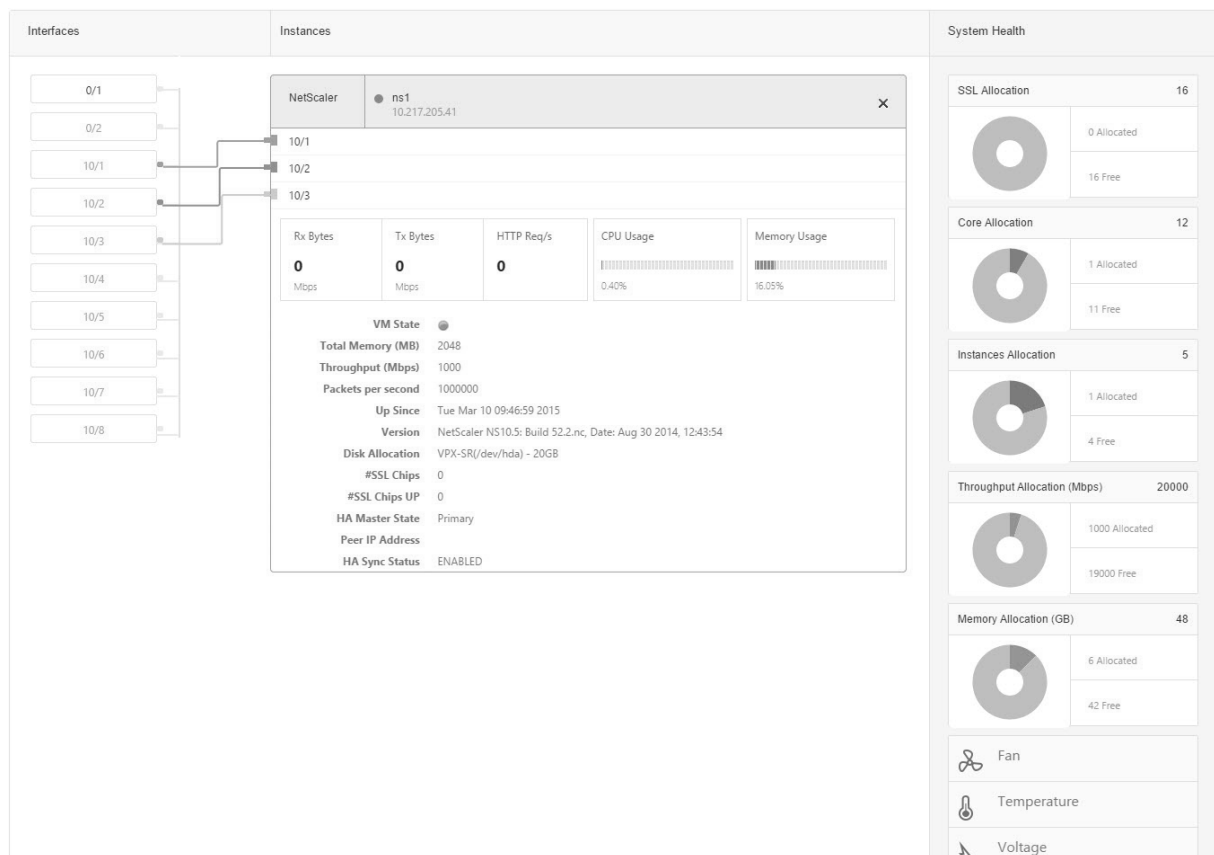
February 15, 2024

Cuando se aprovisiona una instancia de NetScaler en un dispositivo NetScaler SDX, es necesario asignar a una instancia varios recursos, como la CPU, el rendimiento y la memoria. Con el SDX actual, no se muestra la información sobre los diversos recursos disponibles.

Con el visualizador de recursos, todos los recursos disponibles que se pueden usar para aprovisionar una instancia se muestran en un único panel. Todos los recursos disponibles y utilizados se muestran en formato gráfico. El visualizador de recursos también muestra otros parámetros, como el estado de la fuente de alimentación y la temperatura, además de los recursos que se pueden asignar.

El visualizador de recursos también muestra los diversos recursos que utiliza una instancia. Para ver los diversos recursos asociados a una instancia, haga clic en el nombre de la instancia en el visualizador. El lado derecho del visualizador muestra todos los recursos disponibles y utilizados en un formato gráfico.

En la siguiente ilustración se muestran los detalles capturados en el visualizador de recursos:



Administrar interfaces

November 23, 2023

En el panel **Interfaces**, puede mostrar la asignación de las interfaces virtuales de las instancias VPX al dispositivo SDX y asignar direcciones MAC a las interfaces.

Nota: La negociación automática no se admite en una interfaz a la que esté conectado un cable de conexión directa (DAC).

En la lista de **Interfaces del panel Interfaces**, en la columna **Estado**, UP indica que la interfaz recibe tráfico normalmente. DOWN indica un problema de red debido al cual la interfaz no puede enviar ni recibir tráfico.

Importante: No se recomienda el control de flujo en conexiones de más de 1 GB.

Para configurar una interfaz

1. En la ficha **Configuración**, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Interfaces**.
2. En el panel **Interfaces**, haga clic en la interfaz que quiere configurar y, a continuación, haga clic en **Modificar**.
3. En la ventana **Configurar interfaz**, especifique los valores para los siguientes parámetros:
 - **Negociación automática:** habilite la negociación automática. Valores posibles: ON, OFF. Predeterminado: ON.
 - **Velocidad:** velocidad de Ethernet para la interfaz, en MB/s. Valores posibles: 10, 100, 1000 y 10000.
 - **Dúplex:** tipo de operación dúplex de la interfaz. Valores posibles: Full, Half, NONE. Predeterminado: NINGUNO.
 - **Negociación automática de control de flujo:** negocie automáticamente los parámetros de control de flujo. Valores posibles: ON, OFF. Predeterminado: ON
 - **Control de flujo Rx:** active el control de flujo Rx. Valores posibles: ON, OFF. Predeterminado: ON
 - **Control de flujo Tx:** active el control de flujo Tx. Valores posibles: ON, OFF. Predeterminado: ON
4. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Para restablecer los parámetros de una interfaz a sus valores predeterminados

1. En la ficha **Configuración**, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Interfaces**.
2. En el panel **Interfaces**, haga clic en la interfaz que quiere restablecer y, a continuación, haga clic en **Restablecer**.

Mostrar la asignación de interfaces virtuales en la instancia VPX a las interfaces físicas

En la instancia de NetScaler VPX, la GUI y la CLI muestran el mapeo de las interfaces virtuales de la instancia con las interfaces físicas del dispositivo.

Después de iniciar sesión en la instancia de VPX, en la utilidad de configuración, vaya a **Redy**, a continuación, haga clic en **Interfaces**. El número de interfaz virtual de la instancia y el número de interfaz física correspondiente del dispositivo aparecen en el campo **Descripción**, como se muestra en la siguiente ilustración:

En la CLI, escriba el comando `show interface`. Por ejemplo:

```
1 > show interface
2 1) Interface 10/3 (10G VF Interface, PF 10/4) #2
3 flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>
4 MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s
5 Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput
6 10000
7 RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)
8 TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)
9 NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
10 Bandwidth thresholds are not set.
11 ...
12 <!--NeedCopy-->
```

Asignación de una dirección MAC a una interfaz

Mientras aprovisiona una instancia ADC en un dispositivo SDX, Citrix Hypervisor asigna internamente una dirección MAC a una interfaz virtual asociada a esa instancia. Es posible que se asigne la misma dirección MAC a una interfaz virtual asociada a otra instancia en el mismo dispositivo o en otro dispositivo. Para evitar la asignación de direcciones MAC duplicadas, puede aplicar direcciones MAC únicas.

Hay dos maneras de asignar una dirección MAC a una interfaz:

1. Asignar una dirección MAC base y un rango a una interfaz: Management Service asigna una dirección MAC única mediante la dirección y el rango base.
2. Asignar una dirección MAC base global: Una dirección MAC base global se aplica a todas las interfaces. A continuación, Management Service genera las direcciones MAC para todas las interfaces. Si establece la dirección MAC base global, el rango de una interfaz 1G se establece en 8. El rango de una interfaz 10G se establece en 64. Consulte la tabla siguiente para ver las direcciones MAC base de ejemplo si la dirección MAC base global está establecida en 00:00:00:00:00:00.

Interfaz física	Dirección MAC base
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

Tabla 1. Ejemplo de direcciones MAC base generadas a partir de una dirección MAC base global

La dirección MAC base para los puertos de administración es solo para referencia. El Servicio de administración genera direcciones MAC, basadas en la dirección MAC base, solo para los puertos 1/x y 10/x.

Nota: No puede asignar una dirección MAC base a un canal.

Para realizar las distintas operaciones con la dirección MAC, haga clic en **Sistema > Interfaces**. Seleccione una interfaz y luego haga clic en **Modificar**. Realice la operación de dirección MAC, en la ventana **Configurar interfaz**.

Inhabilitar o habilitar las interfaces físicas en el dispositivo SDX

Si no utiliza ninguna de las interfaces físicas del dispositivo SDX, puede inhabilitar la interfaz física mediante el Servicio de administración. Esta acción es útil por motivos de seguridad.

Nota: De forma predeterminada, todas las interfaces físicas del dispositivo SDX están habilitadas. Además, si un VPX o un canal utilizan una interfaz, no puede inhabilitar la interfaz.

Para inhabilitar la interfaz física:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Interfaces**.

2. En el panel **Interfaces**, seleccione la interfaz que quiere inhabilitar.
3. En la lista desplegable **Acción**, haga clic en **Inhabilitar**.

Si quiere utilizar la interfaz física inhabilitada, puede habilitarla mediante Management Service.

Para habilitar la interfaz física inhabilitada:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Sistema** y, a continuación, haga clic en **Interfaces**.
2. En el panel **Interfaces**, seleccione la interfaz de desactivación que quiere habilitar.
3. En la lista desplegable **Acción**, haga clic en **Habilitar**.

Tramas gigantes en dispositivos SDX

November 23, 2023

Los dispositivos NetScaler SDX admiten la recepción y la transmisión de tramas gigantes que contienen hasta 9216 bytes de datos IP. Las tramas gigantes pueden transferir archivos grandes de forma más eficiente de lo que es posible con el tamaño MTU IP estándar de 1500 bytes.

Un dispositivo NetScaler SDX puede utilizar marcos gigantes en los siguientes escenarios de implementación:

- **Gigante a gigante:** El dispositivo recibe datos como tramas gigantes y los envía como tramas gigantes.
- **No gigante a gigante:** El dispositivo recibe datos como tramas no gigantes y los envía como tramas gigantes.
- **Gigante a no gigante:** El dispositivo recibe datos como tramas gigantes y los envía como tramas no gigantes.

Las instancias de NetScaler provisionadas en el dispositivo SDX admiten marcos gigantes en una configuración de equilibrio de carga para los siguientes protocolos:

- TCP
- Cualquier otro protocolo a través de TCP
- SIP

Para obtener más información acerca de las tramas gigantes, vea los casos de uso.

Caso de uso: Configuración gigante a gigante

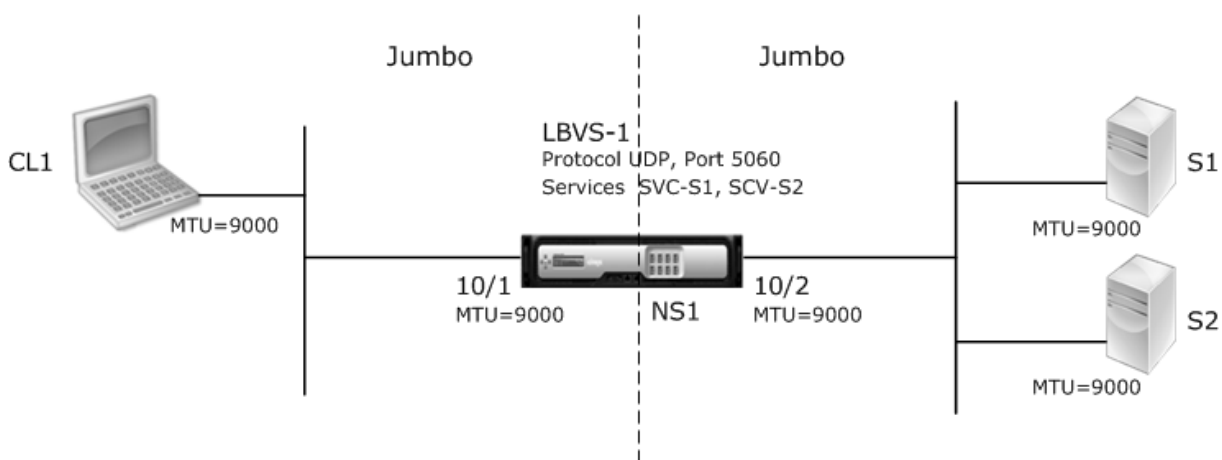
Consideremos un ejemplo de una configuración jumbo a jumbo en la que el servidor virtual de equilibrio de carga SIP LBVS-1, configurado en la instancia NS1 de NetScaler, se utiliza para equilibrar la

carga del tráfico SIP entre los servidores S1 y S2. La conexión entre el cliente CL1 y NS1 y la conexión entre NS1 y los servidores admiten tramas gigantes.

La interfaz 10/1 de NS1 recibe o envía tráfico desde o hacia el cliente CL1. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia el servidor S1 o S2. Las interfaces 10/1 y 10/2 de NS1 forman parte de VLAN 10 y VLAN 20, respectivamente.

Para admitir tramas gigantes, la MTU se establece en 9216 para las interfaces 10/1, 10/2 y VLAN VLAN 10, VLAN 20.

Todos los demás dispositivos de red, incluidos CL1, S1, S2, en este ejemplo de configuración también están configurados para admitir tramas gigantes.



En la tabla siguiente se enumeran los parámetros utilizados en el ejemplo.

Entidad	Nombre	Detalles
Dirección IP del cliente CL1	CL1	192.0.2.10
Dirección IP de los servidores	S1	198.51.100.19
	S2	
MTU especificadas para las interfaces (mediante la interfaz del Servicio de administración) y las VLAN en NS1 (mediante la CLI).	10/1	9000
	10/2	
	VLAN 10	
	VLAN 20	
Servicios en servidores que representan NS1	SVC-S1	Dirección IP: 198.51.100.19; Protocolo: SIP; Puerto: 5060

Entidad	Nombre	Detalles
Servicios en servidores que representan NS1	SVC-S2	Dirección IP: 198.51.100.20; Protocolo: SIP; Puerto: 5060
Servidor virtual de equilibrio de carga en VLAN 10	LBVS-1	Dirección IP: 203.0.113.15; Protocolo: SIP; Puerto: 5060; SVC-S1, SVC-S2

A continuación se presenta el flujo de tráfico de la solicitud de CL1 a NS1:

1. CL1 crea una solicitud SIP de 20000 bytes para LBVS1.
2. CL1 envía los datos de solicitud en fragmentos de IP a LBVS1 de NS1. El tamaño de cada fragmento IP es igual o menor que la MTU (9000) establecida en la interfaz desde la que CL1 envía estos fragmentos a NS1.
 - Tamaño del primer fragmento IP = [encabezado IP+encabezado UDP + segmento de datos SIP] = [20 + 8 + 8972] = 9000
 - Tamaño del segundo fragmento IP = [encabezado IP+segmento de datos SIP] = [20 + 8980] = 9000
 - Tamaño del último fragmento de IP = [encabezado IP+segmento de datos SIP] = [20 + 2048] = 2068
3. NS1 recibe los fragmentos IP de solicitud en la interfaz 10/1. NS1 acepta estos fragmentos porque el tamaño de cada uno de estos fragmentos es igual o menor que la MTU (9000) de la interfaz 10/1.
4. NS1 vuelve a ensamblar estos fragmentos de IP para formar la solicitud SIP de 27000 bytes. NS1 procesa esta solicitud.
5. El algoritmo de equilibrio de carga de LBVS-1 selecciona el servidor S1.
6. NS1 envía los datos de solicitud en fragmentos IP a S1. El tamaño de cada fragmento de IP es igual o menor que la MTU (9000) de la interfaz 10/2, desde la que NS1 envía estos fragmentos a S1. Los paquetes IP se originan con una dirección SNIP de NS1.
 - Tamaño del primer fragmento IP = [encabezado IP+encabezado UDP + segmento de datos SIP] = [20 + 8 + 8972] = 9000
 - Tamaño del segundo fragmento IP = [encabezado IP+segmento de datos SIP] = [20 + 8980] = 9000
 - Tamaño del último fragmento de IP = [encabezado IP+segmento de datos SIP] = [20 + 2048] = 2068

A continuación se presenta el flujo de tráfico de la respuesta de S1 a CL1 en este ejemplo:

1. El servidor S1 crea una respuesta SIP de 30000 bytes para enviarla a la dirección SNIP de NS1.

2. S1 envía los datos de respuesta en fragmentos IP a NS1. El tamaño de cada fragmento IP es igual o menor que la MTU (9000) establecida en la interfaz desde la que S1 envía estos fragmentos a NS1.
 - Tamaño del primer fragmento IP = [encabezado IP+encabezado UDP + segmento de datos SIP] = [20 + 8 + 8972] = 9000
 - Tamaño del segundo y tercer fragmento IP = [encabezado IP+segmento de datos SIP] = [20 + 8980] = 9000
 - Tamaño del último fragmento de IP= [encabezado IP+segmento de datos SIP] = [20 + 3068] = 3088
3. NS1 recibe los fragmentos IP de respuesta en la interfaz 10/2. NS1 acepta estos fragmentos porque el tamaño de cada fragmento es igual o menor que la MTU (9000) de la interfaz 10/2.
4. NS1 vuelve a ensamblar estos fragmentos de IP para formar la respuesta SIP de 27000 bytes. NS1 procesa esta respuesta.
5. NS1 envía los datos de respuesta en fragmentos IP a CL1. El tamaño de cada fragmento de IP es igual o menor que la MTU (9000) de la interfaz 10/1, desde la que NS1 envía estos fragmentos a CL1. Los fragmentos IP se obtienen con la dirección IP de LBVS-1. Estos paquetes IP provienen de la dirección IP de LBVS-1 y están destinados a la dirección IP de CL1.
 - Tamaño del primer fragmento IP = [encabezado IP+encabezado UDP + segmento de datos SIP] = [20 + 8 + 8972] = 9000
 - Tamaño del segundo y tercer fragmento IP = [encabezado IP+segmento de datos SIP] = [20 + 8980] = 9000

Tamaño del último fragmento de IP= [encabezado IP+segmento de datos SIP] = [20 + 3068] = 3088

Tareas de configuración:

En SDX Management Service, vaya a la página **Configuración > Sistema > Interfaces**. Seleccione la interfaz requerida y haga clic en **Modificar**. Defina el valor de MTU y haga clic en **Aceptar**.

Ejemplo:

Establezca el valor de MTU para la interfaz 10/1 como 9000 y para la interfaz 10/2 como 9000.

Inicie sesión en la instancia de NetScaler y utilice la interfaz de línea de comandos de ADC para completar los pasos de configuración restantes.

La siguiente tabla muestra las tareas, los comandos y los ejemplos para crear la configuración requerida en las instancias de NetScaler.

Tareas	Sintaxis de comandos ADC	Ejemplos
Cree VLAN y configure la MTU de las VLAN correspondientes para admitir tramas gigantes.	<code>add vlan <id> -mtu <positive_integer>;show vlan <id></code>	<code>add vlan 10 -mtu 9000;add vlan 20 -mtu 9000</code>
Enlace interfaces con VLAN.	<code>bind vlan <id> -ifnum <interface_name>;show vlan <id></code>	<code>bind vlan 10 -ifnum 10/1;bind vlan 20 -ifnum 10/2</code>
Agregue una dirección SNIP.	<code>add ns ip <IPAddress> <netmask> -type SNIP;show ns ip</code>	<code>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</code>
Cree servicios que representan servidores SIP.	<code>add service <serviceName> <ip> SIP_UDP <port>;show service <name></code>	<code>agregar servicio SVC-S1 198.51.100.19 SIP_UDP 5060;agregar servicio SVC-S2 198.51.100.20 SIP_UDP 5060</code>
Cree servidores virtuales de equilibrio de carga SIP y enlace los servicios con él.	<code>add lb vserver <name> SIP_UDP <ip> <port>;bind lb vserver <vserverName> <serviceName>;show lb vserver <name></code>	<code>add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060;bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS-1 SVC-S2</code>
<code>bind lb vserver LBVS-1 SVC-S2</code>	<code>save ns config;show ns config</code>	

Caso de uso: Configuración de no gigante a gigante

Considere un ejemplo de una configuración que no sea jumbo a jumbo en la que el servidor virtual de equilibrio de carga LBVS1, configurado en una instancia NS1 de NetScaler, se utiliza para equilibrar la carga del tráfico entre los servidores S1 y S2. La conexión entre CL1 cliente y NS1 admite tramas no gigantes, y la conexión entre NS1 y los servidores admite tramas gigantes.

La interfaz 10/1 de NS1 recibe o envía tráfico desde o hacia el cliente CL1. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia el servidor S1 o S2.

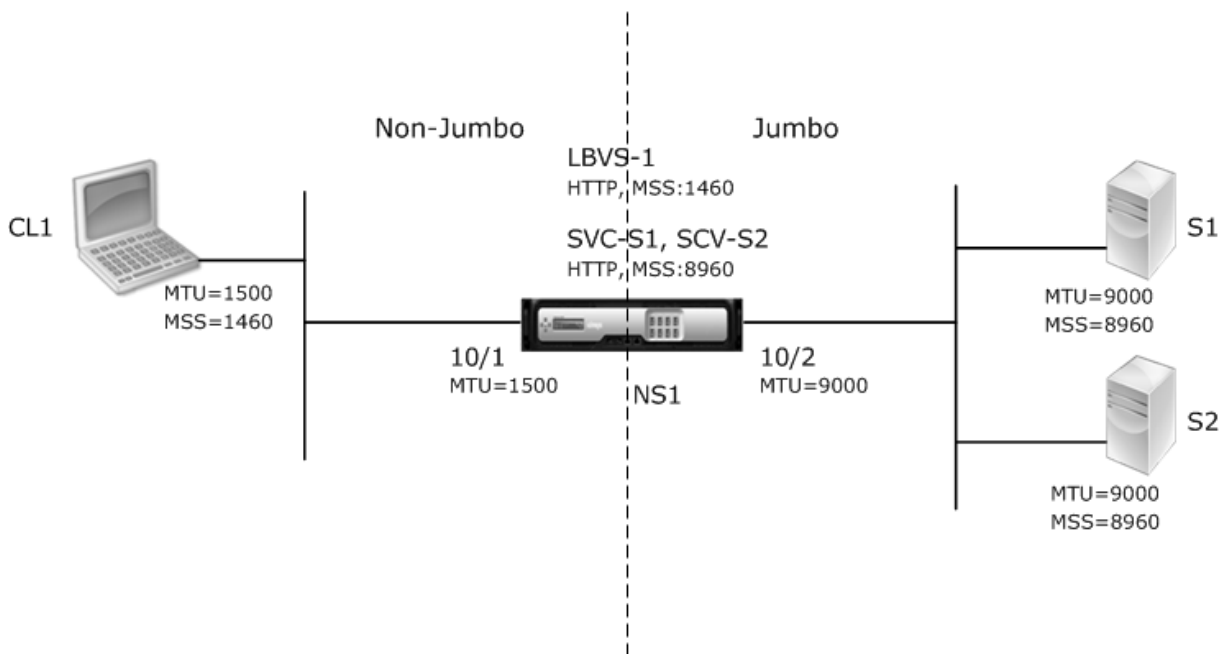
Las interfaces 10/1 y 10/2 de NS1 forman parte de VLAN 10 y VLAN 20, respectivamente. Para admitir

solo tramas no gigantes entre CL1 y NS1, la MTU se establece en el valor predeterminado de 1500 para la interfaz 10/1 y VLAN 10.

Para admitir tramas gigantes entre NS1 y los servidores, la MTU se establece en 9000 para la interfaz 10/2 y VLAN 20.

Los servidores y todos los demás dispositivos de red entre NS1 y los servidores también están configurados para admitir tramas gigantes. Dado que el tráfico HTTP se basa en TCP, MSS se establecen en consecuencia en cada punto final para admitir tramas gigantes:

- Para la conexión entre CL1 y el servidor virtual LBVS1 de NS1, el MSS de NS1 se establece en un perfil TCP, que luego se enlaza a LBVS1.
- Para la conexión entre una dirección SNIP de NS1 y S1, el MSS de NS1 se establece en un perfil TCP, que luego se enlaza al servicio (SVC-S1) que representa S1 en NS1.



En la siguiente tabla se enumeran las configuraciones utilizadas en este ejemplo:

Entidad	Nombre	Detalles
Dirección IP del cliente CL1	CL1	192.0.2.10
Dirección IP de los servidores	S1	198.51.100.19
	S2	
MTU para la interfaz 10/1 (mediante la interfaz del Servicio de administración).		1500
MTU configurada para la interfaz 10/2 (mediante la interfaz del Servicio de administración).		9000

Entidad	Nombre	Detalles
MTU para VLAN 10 en NS1 (mediante la interfaz de línea de comandos ADC).		1500
MTU configurada para VLAN 20 en NS1 (mediante la interfaz de línea de comandos ADC).		9000
Servicios en servidores que representan NS1	SVC-S1	Dirección IP: 198.51.100.19; Protocolo: HTTP; Puerto: 80; MSS: 8960 SVC-S2
Servidor virtual de equilibrio de carga en VLAN 10	LBVS-1	Dirección IP: 203.0.113.15; Protocolo: HTTP; Puerto: 80. Servicios vinculados: SVC-S1, SVC-S2; MSS: 1460

A continuación se presenta el flujo de tráfico de la solicitud de CL1 a S1 en este ejemplo:

1. El cliente CL1 crea una solicitud HTTP de 200 bytes para enviarla al servidor virtual LBVS-1 de NS1.
2. CL1 abre una conexión con el LBVS-1 de NS1. CL1 y NS1 intercambian sus valores MSS TCP respectivos mientras establecen la conexión.
3. Dado que MSS de NS1 es mayor que la solicitud HTTP, CL1 envía los datos de solicitud en un único paquete IP a NS1.

1.

```

1 <div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">
2
3 Size of the request packet = [IP Header + TCP Header + TCP Request
4                               ] = [20 + 20 + 200] = 240
5 </div>
```

4. NS1 recibe el paquete de solicitud en la interfaz 10/1 y, a continuación, procesa los datos de solicitud HTTP en el paquete.
5. El algoritmo de equilibrio de carga de LBVS-1 selecciona el servidor S1 y NS1 abre una conexión entre una de sus direcciones SNIP y S1. NS1 y CL1 intercambian sus valores MSS TCP respectivos mientras establecen la conexión.
6. Dado que el MSS de S1 es mayor que la solicitud HTTP, NS1 envía los datos de solicitud en un único paquete IP a S1.

$$\begin{aligned} \text{a) Tamaño del paquete de solicitud} &= [\text{Encabezado IP} + \text{Encabezado TCP} + [\text{Solicitud TCP}]] \\ &= [20 + 20 + 200] = 240 \end{aligned}$$

A continuación se presenta el flujo de tráfico de la respuesta de S1 a CL1 en este ejemplo:

1. El servidor S1 crea una respuesta HTTP de 18000 bytes para enviarla a la dirección SNIP de NS1.
2. S1 segmenta los datos de respuesta en múltiplos de MSS de NS1 y envía estos segmentos en paquetes IP a NS1. Estos paquetes IP provienen de la dirección IP de S1 y están destinados a la dirección SNIP de NS1.
 - Tamaño de los dos primeros paquetes = [Encabezado IP+encabezado TCP + (segmento TCP = tamaño MSS de NS1)] = [20 + 20 + 8960] = 9000
 - Tamaño del último paquete = [Encabezado IP+encabezado TCP + (segmento TCP restante)] = [20 + 20 + 2080] = 2120
3. NS1 recibe los paquetes de respuesta en la interfaz 10/2.
4. A partir de estos paquetes IP, NS1 ensambla todos los segmentos TCP para formar los datos de respuesta HTTP de 18000 bytes. NS1 procesa esta respuesta.
5. NS1 segmenta los datos de respuesta en múltiplos de MSS de CL1 y envía estos segmentos en paquetes IP, desde la interfaz 10/1 a CL1. Estos paquetes IP provienen de la dirección IP de LBVS-1 y están destinados a la dirección IP de CL1.
 - Tamaño de todo el paquete excepto el último = [Encabezado IP+encabezado TCP + (carga útil TCP = tamaño MSS de CL1)] = [20 + 20 + 1460] = 1500
 - Tamaño del último paquete = [Encabezado IP+encabezado TCP + (segmento TCP restante)] = [20 + 20 + 480] = 520

Tareas de configuración:

En SDX Management Service, vaya a la página **Configuración > Sistema > Interfaces**. Seleccione la interfaz requerida y haga clic en **Modificar**. Defina el valor de MTU y haga clic en **Aceptar**.

Ejemplo:

Defina los siguientes valores de MTU:

- Para interfaz 10/1 como 1500
- Para interfaz 10/2 como 9000

Inicie sesión en la instancia de NetScaler y utilice la interfaz de línea de comandos de ADC para completar los pasos de configuración restantes.

La siguiente tabla muestra las tareas, los comandos y los ejemplos para crear la configuración requerida en las instancias de NetScaler.

Tareas	Sintaxis de línea de comandos ADC	Ejemplo

```
|Cree VLAN y configure la MTU de las VLAN correspondientes para admitir tramas gigantes.|add
vlan <id> -mtu <positive_integer>; show vlan <id>|add vlan 10 -mtu 1500
;add vlan 20 -mtu 9000|
|Enlace interfaces con VLAN.|bind vlan <id> -ifnum <interface_name>; show vlan
<id>|bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2|
|Agregue una dirección SNIP.|add ns ip <IPAddress> <netmask> -type SNIP; show
ns ip|add ns ip 198.51.100.18 255.255.255.0 -type SNIP|
|Cree servicios que representan servidores HTTP.|add service <serviceName> <ip> HTTP
<port>; show service <name>|add service SVC-S1 198.51.100.19 http 80;
add service SVC-S2 198.51.100.20 http 80|
|Cree servidores virtuales de equilibrio de carga HTTP y enlace los servicios con él.|add
lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName>
<serviceName>; show lb vserver <name>|add lb vserver LBVS-1 http
203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1|
|Cree un perfil TCP personalizado y establezca su MSS para admitir tramas gigantes.|add
tcpProfile <name> -mss <positive_integer>; show tcpProfile <name>|add
tcpProfile NS1-SERVERS-JUMBO -mss 8960|
|Enlace el perfil TCP personalizado con los servicios correspondientes.|set service <Name
> -tcpProfileName <string>; show service <name>|set service SVC-S1 -
tcpProfileName NS1-SERVERS-JUMBO; set service SVC-S2 -tcpProfileName
NS1-SERVERS-JUMBO|
|Guarde la configuración|save ns config; show ns config|
```

Caso de uso: Coexistencia de flujos gigantes y no gigantes en el mismo conjunto de interfaces

Considere un ejemplo en el que los servidores virtuales de equilibrio de carga LBVS1 y LBVS2 están configurados en la instancia NS1 de NetScaler. LBVS1 se usa para equilibrar la carga del tráfico HTTP entre los servidores S1 y S2, y el global se usa para equilibrar la carga del tráfico entre los servidores S3 y S4.

CL1 está en la VLAN 10, S1 y S2 están en la VLAN20, CL2 está en la VLAN 30 y S3 y S4 están en la VLAN 40. VLAN 10 y VLAN 20 admiten tramas gigantes, y VLAN 30 y VLAN 40 solo admiten tramas no gigantes.

En otras palabras, la conexión entre CL1 y NS1 y la conexión entre NS1 y el servidor S1 o S2 admiten tramas gigantes. La conexión entre CL2 y NS1 y la conexión entre NS1 y el servidor S3 o S4 solo admiten tramas no gigantes.

La interfaz 10/1 de NS1 recibe o envía tráfico desde o hacia los clientes. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia los servidores.

La interfaz 10/1 está enlazada tanto a la VLAN 10 como a la VLAN 20 como una interfaz etiquetada. La

interfaz 10/2 está enlazada tanto a la VLAN 30 como a la VLAN 40 como una interfaz etiquetada.

Para admitir tramas gigantes, la MTU se establece en 9216 para las interfaces 10/1 y 10/2.

En NS1, la MTU se establece en 9000 para VLAN 10 y VLAN 30 para admitir tramas gigantes. La MTU se establece en el valor predeterminado de 1500 para VLAN 20 y VLAN 40 para admitir solo tramas no gigantes.

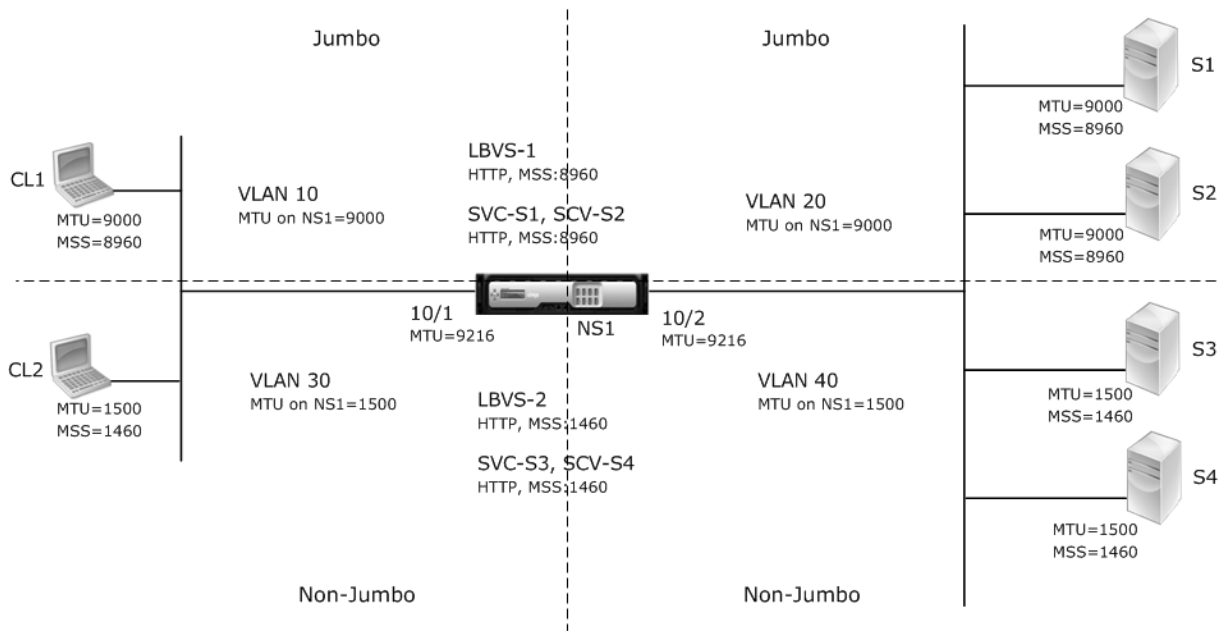
La MTU efectiva en una interfaz ADC para paquetes etiquetados de VLAN es la MTU de la interfaz o la MTU de la VLAN, la que sea inferior. Por ejemplo:

- La MTU de la interfaz 10/1 es 9216. La MTU de la VLAN 10 es 9000. En la interfaz 10/1, la MTU de los paquetes etiquetados VLAN 10 es 9000.
- La MTU de la interfaz 10/2 es 9216. La MTU de la VLAN 20 es 9000. En la interfaz 10/2, la MTU de los paquetes etiquetados VLAN 20 es 9000.
- La MTU de la interfaz 10/1 es 9216. La MTU de la VLAN 30 es 1500. En la interfaz 10/1, la MTU de los paquetes etiquetados VLAN 30 es 1500.
- La MTU de la interfaz 10/2 es 9216. La MTU de la VLAN 40 es 1500. En la interfaz 10/2, la MTU de los paquetes etiquetados VLAN 40 es 9000.

CL1, S1, S2 y todos los dispositivos de red entre CL1 y S1 o S2 están configurados para tramas gigantes.

Dado que el tráfico HTTP se basa en TCP, MSS se establecen en consecuencia en cada punto final para admitir tramas gigantes.

- Para la conexión entre CL1 y el servidor virtual LBVS-1 de NS1, el MSS de NS1 se establece en un perfil TCP, que luego se enlaza a LBVS1.
- Para la conexión entre una dirección SNIP de NS1 y S1, el MSS de NS1 se establece en un perfil TCP, que luego se enlaza al servicio (SVC-S1) que representa S1 en NS1.



En la siguiente tabla se enumeran las configuraciones utilizadas en este ejemplo.

Entidad	Nombre	Detalles
Dirección IP de los clientes	CL1	192.0.2.10
	CL2	192.0.2.20
Dirección IP de los servidores	S1	198.51.100.19
	S2	198.51.100.20
	S3	198.51.101.19
	S4	198.51.101.20
Direcciones SNIP en NS1	198.51.100.18; 198.51.101.18	
MTU especificada para interfaces y VLAN en NS1	10/1	9216
	10/2	9216
VLAN 10	9000	
VLAN 20	9000	
VLAN 30	9000	
VLAN 40	1500	
Default TCP profile	nstcp_default_profile	MSS: 1460
Custom TCP profile	ALL-JUMBO	MSS: 8960
Services on NS1 representing servers	SVC-S1	IP address: 198.51.100.19; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)
	SVC-S2	IP address: 198.51.100.20; Protocol: HTTP; Port: 80; TCP profile: ALL-JUMBO (MSS: 8960)
	SVC-S3	IP address: 198.51.101.19; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS: 1460)
	SVC-S4	IP address: 198.51.101.20; Protocol: HTTP; Port: 80; TCP profile: nstcp_default_profile (MSS: 1460)

1460)

|Load balancing virtual servers on NS1|LBVS-1|IP address = 203.0.113.15; Protocol: HTTP; Port: 80.
Bound services: SVC-S1, SVC-S2; TCP profile: ALL-JUMBO (MSS: 8960)

||LBVS-2|IP address = 203.0.114.15; Protocol: HTTP; Port: 80. Bound services: SVC-S3, SVC-S4; TCP
Profile: nstcp_default_profile (MSS: 1460)

A continuación se presenta el flujo de tráfico de la solicitud de CL1 a S1:

1. Cliente CL1 crea una solicitud HTTP de 20000 bytes para enviar al servidor virtual LBVS-1 de NS1.
2. CL1 abre una conexión con el LBVS-1 de NS1. CL1 y NS1 intercambian sus valores TCP MSS mientras establecen la conexión.
3. Dado que el valor MSS de NS1 es menor que la solicitud HTTP, CL1 segmenta los datos de solicitud en múltiplos de MSS de NS1 y envía estos segmentos en paquetes IP etiquetados como VLAN 10 a NS1.
 - Tamaño de los dos primeros paquetes = [Encabezado IP+encabezado TCP + (segmento TCP = MSS NS1)] = [20 + 20 + 8960] = 9000
 - Tamaño del último paquete = [Encabezado IP+encabezado TCP + (segmento TCP restante)] = [20 + 20 + 2080] = 2120
4. NS1 recibe estos paquetes en la interfaz 10/1. NS1 acepta estos paquetes porque el tamaño de estos paquetes es igual o menor que la MTU efectiva (9000) de la interfaz 10/1 para paquetes etiquetados VLAN 10.
5. Desde los paquetes IP, NS1 ensambla todos los segmentos TCP para formar la solicitud HTTP de 20000 bytes. NS1 procesa esta solicitud.
6. El algoritmo de equilibrio de carga de LBVS-1 selecciona el servidor S1 y NS1 abre una conexión entre una de sus direcciones SNIP y S1. NS1 y CL1 intercambian sus valores MSS TCP respectivos mientras establecen la conexión.
7. NS1 segmenta los datos de solicitud en múltiplos del MSS de S1 y envía estos segmentos en paquetes IP etiquetados como VLAN 20 a S1.
 - Tamaño de los dos primeros paquetes = [Encabezado IP+Encabezado TCP + (Carga útil TCP=S1 MSS)] = [20 + 20 + 8960] = 9000
 - Tamaño del último paquete = [Encabezado IP+encabezado TCP + (segmento TCP restante)] = [20 + 20 + 2080] = 2120

A continuación se presenta el flujo de tráfico de la respuesta de S1 a CL1:

1. El servidor S1 crea una respuesta HTTP de 30000 bytes para enviarla a la dirección SNIP de NS1.
2. S1 segmenta los datos de respuesta en múltiplos de MSS de NS1 y envía estos segmentos en paquetes IP etiquetados como VLAN 20 a NS1. Estos paquetes IP provienen de la dirección IP de S1 y están destinados a la dirección SNIP de NS1.

- Tamaño de los tres primeros paquetes = [Encabezado IP+encabezado TCP + (segmento TCP = tamaño MSS de NS1)] = [20 + 20 + 8960] = 9000
 - Tamaño del último paquete = [Encabezado IP+encabezado TCP + (segmento TCP restante)] = [20 + 20 + 3120] = 3160
3. NS1 recibe los paquetes de respuesta en la interfaz 10/2. NS1 acepta estos paquetes porque su tamaño es igual o menor que el valor de MTU efectivo (9000) de la interfaz 10/2 para paquetes etiquetados de VLAN 20.
 4. A partir de estos paquetes IP, NS1 ensambla todos los segmentos TCP para formar la respuesta HTTP de 30000 bytes. NS1 procesa esta respuesta.
 5. NS1 segmenta los datos de respuesta en múltiplos de MSS de CL1 y envía estos segmentos en paquetes IP etiquetados como VLAN 10, desde la interfaz 10/1 a CL1. Estos paquetes IP provienen de la dirección IP de LBVS y están destinados a la dirección IP de CL1.
 - Tamaño de los tres primeros paquetes = [Encabezado IP+Encabezado TCP + [(Carga útil TCP = tamaño MSS de CL1)] = [20 + 20 + 8960] = 9000
 - Tamaño del último paquete = [Encabezado IP+encabezado TCP + (segmento TCP restante)] = [20 + 20 + 3120] = 3160

Tareas de configuración:

En SDX Management Service, vaya a la página **Configuración > Sistema > Interfaces**. Seleccione la interfaz requerida y haga clic en **Modificar**. Defina el valor de MTU y haga clic en **Aceptar**.

Ejemplo:

Defina los siguientes valores de MTU:

- Para interfaz 10/1 como 9216
- Para interfaz 10/2 como 9216

Inicie sesión en la instancia de NetScaler y utilice la interfaz de línea de comandos de ADC para completar los pasos de configuración restantes.

La siguiente tabla muestra las tareas, los comandos y los ejemplos para crear la configuración requerida en las instancias de NetScaler.

Tarea	Sintaxis	Ejemplo
Cree VLAN y configure la MTU de las VLAN correspondientes para admitir tramas gigantes.	<code>add vlan <id> -mtu <positive_integer>; show vlan <id></code>	<code>add vlan 10 -mtu 9000 add vlan 20 -mtu 9000; add vlan 30 -mtu 1500; add vlan 40 -mtu 1500</code>
Enlace interfaces con VLAN.	<code>bind vlan <id> -ifnum <interface_name>; show vlan <id></code>	<code>bind vlan 10 -ifnum 10/1 -tagged bind vlan 20 -ifnum 10/2 -tagged bind vlan 30 -ifnum 10/1 -tagged; bind vlan 40 -ifnum 10/2 -tagged</code>

```
|Agregue una dirección SNIP.|add ns ip <IPAddress> <netmask> -type SNIP;show
ns ip|add ns ip 198.51.100.18 255.255.255.0 -type SNIP;add ns ip
198.51.101.18 255.255.255.0 -type SNIP|
|Cree servicios que representan servidores HTTP.|add service <serviceName> <ip>
HTTP <port>;show service <name>|add service SVC-S1 198.51.100.19
http 80|add service SVC-S2 198.51.100.20 http 80;add service SVC-S3
198.51.101.19 http 80;add service SVC-S4 198.51.101.20 http 80|
|Cree servidores virtuales de equilibrio de carga HTTP y enlace los servicios con él.|add
lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName>
<serviceName>;show lb vserver <name>|add lb vserver LBVS-1 http
203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1;bind lb vserver LBVS
-1 SVC-S2|
|||add lb vserver LBVS-2 http 203.0.114.15 80; bind lb vserver LBVS-2
SVC-S3;bind lb vserver LBVS-2 SVC-S4|
|Cree un perfil TCP personalizado y establezca su MSS para admitir tramas gigantes.|add
tcpProfile <name> -mss <positive_integer>;show tcpProfile <name>|add
tcpProfile ALL-JUMBO -mss 8960|
|Enlace el perfil TCP personalizado con el servidor virtual y los servicios de equilibrio de carga
correspondientes.|set service <Name> -tcpProfileName <string>;show service
<name>|set lb vserver LBVS-1 - tcpProfileName ALL-JUMBO; set service
SVC-S1 - tcpProfileName ALL-JUMBO;set service SVC-S2 - tcpProfileName
ALL-JUMBO|
|Guardar la configuración|save ns config; show ns config|
```

Configurar SNMP en dispositivos SDX

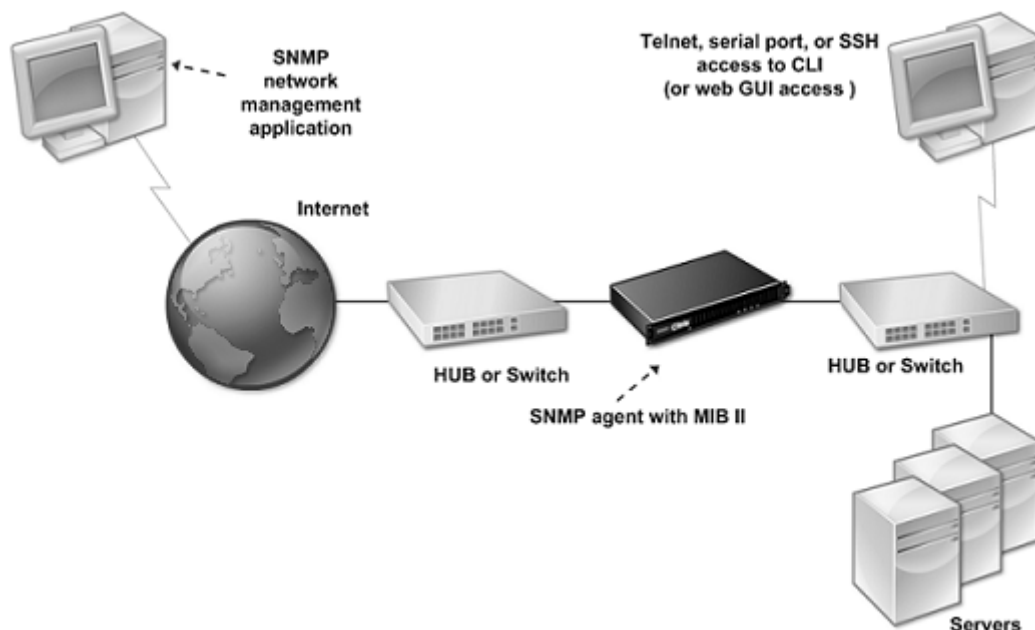
November 23, 2023

Puede configurar un agente SNMP en el dispositivo NetScaler SDX para generar eventos asincrónicos, que se denominan trampas. Las trampas se generan siempre que hay condiciones anormales en el dispositivo SDX. A continuación, las capturas se envían a un dispositivo remoto denominado *detector de capturas*, que indica la condición anormal en el dispositivo SDX.

Además de configurar un destino de captura SNMP, descargar archivos MIB y configurar uno o más administradores de SNMP, puede configurar el dispositivo NetScaler SDX para las consultas SNMPv3.

La siguiente ilustración ilustra una red con un dispositivo SDX que tiene habilitado y configurado SNMP. En la ilustración, cada aplicación de administración de red SNMP utiliza SNMP para comunicarse con el agente SNMP en el dispositivo SDX.

Figura 1. Dispositivo SDX compatible con SNMP



El agente SNMP del dispositivo SDX genera capturas que solo cumplen con SNMPv2. Las capturas admitidas se pueden ver en el archivo SDX MIB. Puede descargar este archivo desde la página Descargas de la interfaz de usuario de SDX.

Para agregar un destino de captura SNMP

1. En la ficha Configuración, en el panel de navegación, expanda **Sistema > SNMP** y, a continuación, haga clic en Destinos de capturas SNMP.
2. En el panel Destinos de capturas SNMP, haga clic en Agregar.
3. En la página Configurar destino de capturas SNMP, especifique los valores para los siguientes parámetros:
 - Servidor de destino: Dirección IPv4 del listener de captura al que se envían los mensajes de captura SNMP.
 - Puerto: Puerto UDP en el que el detector de captura escucha los mensajes de captura. Debe coincidir con la configuración del oyente de capturas, o el oyente descarta los mensajes. Valor mínimo: 1. Predeterminado: 162.
 - Comunidad: Contraseña (cadena) enviada con los mensajes de captura, para que el oyente de captura pueda autenticarlos. Puede incluir letras, números y guiones (-), punto (.), hash (#), espacio (), arroba (@), igual (=), dos puntos (:) y guiones bajos (_).
Nota: Especifique la misma cadena de comunidad en el dispositivo de escucha de capturas, o el agente de escucha descartará los mensajes. Predeterminado: Public.

4. Haga clic en Agregar y, a continuación, en Cerrar. El destino de capturas SNMP que ha agregado aparece en el panel Capturas SNMP.

Para modificar los valores de los parámetros de un destino de captura SNMP, en el panel Destinos de captura SNMP, seleccione el destino de captura que quiere modificar y, a continuación, haga clic en Modificar. En el cuadro de diálogo Modificar destino de captura SNMP, modifique los parámetros.

Para quitar una captura SNMP, en el panel Destinos de captura SNMP, seleccione el destino de captura que quiere quitar y, a continuación, haga clic en Eliminar. En el cuadro Confirmar mensaje, haga clic para eliminar el destino de captura SNMP.

Descarga de archivos MIB

Debe descargar el siguiente archivo antes de empezar a supervisar un dispositivo SDX.

SDX-MIB-smiv2.mib. Este archivo lo utilizan los administradores de SNMPv2 y los agentes de escucha de capturas de SNMPv2.

El archivo incluye una MIB empresarial de NetScaler que proporciona eventos específicos de SDX.

Para descargar archivos MIB

1. Inicie sesión en la página Descargas de la interfaz de usuario del dispositivo SDX.
2. En Archivos SNMP, haga clic en SNMP v2 - Definiciones de objetos MIB. Puede abrir el archivo mediante un explorador MIB.

Adición de una comunidad de administradores SNMP

Configure los administradores de SNMP en el dispositivo SDX para que consulten y supervisen el dispositivo y los dispositivos administrados alojados en el dispositivo. Además, debe proporcionar al administrador de SNMP la información requerida específica del dispositivo. Para un administrador SNMP IPv4, puede especificar un nombre de host en lugar de la dirección IP del administrador. Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP en su dirección IP.

Configure al menos un administrador de SNMP. Si no configura un administrador SNMP, el dispositivo no acepta ni responde a las consultas SNMP desde ninguna dirección IP de la red. Si configura uno o más administradores SNMP, el dispositivo acepta y responde solo a las consultas SNMP de esas direcciones IP específicas.

Para configurar un administrador de SNMP

1. En la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, expanda SNMP.
2. Haga clic en Administradores
3. En el panel de detalles, haga clic en Agregar.
4. En la página Crear comunidad de SNMP Manager, defina los siguientes parámetros:
 - SNMP Manager: Dirección IPv4 del administrador SNMP. Como alternativa, en lugar de una dirección IPv4, puede especificar un nombre de host que se haya asignado a un administrador de SNMP. Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP en su dirección IP.
 - Comunidad: Cadena de comunidad SNMP. Puede constar de 1 a 31 caracteres que incluyen letras mayúsculas y minúsculas, números y guiones (-), punto (.), almohadilla (#), arroba (@), igual (=), dos puntos (:) y guiones bajos (_).
 - Seleccione la casilla de verificación **Habilitar red de administración** para especificar los administradores de SNMP mediante la máscara de red.
 - En el campo **Máscara de red**, introduzca la máscara de red de la comunidad SNMP.
5. Haga clic en Agregar y, a continuación, en Cerrar.

Configuración del dispositivo SDX para consultas SNMPv3

SNMPv3 se basa en la estructura y arquitectura básicas de SNMPv1 y SNMPv2. Sin embargo, SNMPv3 mejora la arquitectura básica para incorporar capacidades de administración y seguridad, como autenticación, control de acceso, verificación de integridad de datos, verificación del origen de los datos, verificación de puntualidad de los mensajes y confidencialidad de los datos.

El dispositivo NetScaler SDX admite las siguientes entidades que permiten implementar las funciones de seguridad de SNMPv3:

- Vistas de SNMP
- Usuarios de SNMP

Estas entidades funcionan juntas para implementar las funciones de seguridad de SNMPv3. Las vistas se crean para permitir el acceso a los subárboles de la MIB.

Adición de un administrador de SNMP

Configure el dispositivo SDX para permitir que los administradores SNMP apropiados lo consulten. Proporcione también al administrador de SNMP la información requerida específica del dispositivo. Para un administrador SNMP IPv4, puede especificar un nombre de host en lugar de la dirección IP

del administrador. Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP en su dirección IP.

Configure al menos un administrador de SNMP. Si no configura un administrador SNMP, el dispositivo no acepta ni responde a las consultas SNMP desde ninguna dirección IP de la red. Si configura uno o más administradores SNMP, el dispositivo acepta y responde solo a las consultas SNMP de esas direcciones IP específicas.

Para configurar un administrador de SNMP:

1. Vaya a la página **Sistema > Configuración**.
2. En la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, expanda SNMP.
3. Haga clic en Administradores
4. En el panel de detalles, haga clic en Agregar.
5. En el cuadro de diálogo Agregar comunidad de SNMP Manager, defina los siguientes parámetros:
 - **SNMP Manager:** Dirección IPv4 del administrador SNMP. Como alternativa, en lugar de una dirección IPv4, puede especificar un nombre de host que se haya asignado a un administrador de SNMP. Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP en su dirección IP.
 - **Comunidad:** Cadena de comunidad SNMP. Puede constar de 1 a 31 caracteres que incluyen letras mayúsculas y minúsculas, números y guiones (-), punto (.), almohadilla (#), arroba (@), igual (=), dos puntos (:) y guiones bajos (_).
6. Haga clic en Agregar y, a continuación, en Cerrar.

Configuración de una vista SNMP

Las vistas SNMP restringen el acceso de los usuarios a partes específicas de la MIB. Las vistas SNMP se utilizan para implementar el control de acceso.

Para configurar una vista

1. En la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, expanda SNMP.
2. Haga clic en Vistas.
3. En el panel de detalles, haga clic en Agregar.
4. En el cuadro de diálogo Agregar vista SNMP, defina los siguientes parámetros:
 - **Nombre:** Nombre para la vista SNMPv3. Puede constar de 1 a 31 caracteres que incluyen letras mayúsculas y minúsculas, números y guiones (-), punto (.), almohadilla (#), arroba

(@), igual (=), dos puntos (:) y guiones bajos (_). Elija un nombre que ayude a identificar la vista de SNMPv3.

- Subárbol: Una rama particular (subárbol) del árbol MIB, que quiere asociar a esta vista SNMPv3. Especifique el subárbol como un OID de SNMP.
- Tipo: Incluye o excluye el árbol secundario, especificado por el parámetro del árbol secundario, en o desde esta vista. Esta configuración puede resultar útil cuando se ha incluido un árbol secundario, como A, en una vista SNMPv3 y se quiere excluir un árbol secundario específico de A, como B, de la vista SNMPv3.

Configuración de un usuario SNMP

Después de crear una vista SNMP, agregue usuarios SNMP. Los usuarios de SNMP tienen acceso a las MIB que se requieren para consultar a los administradores de SNMP.

Para configurar un usuario

1. En la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, expanda SNMP.
2. Haga clic en Usuarios.
3. En el panel de detalles, haga clic en Agregar.
4. En la página Crear usuario SNMP, defina los siguientes parámetros:
 - Nombre: Nombre del usuario SNMPv3. Puede constar de 1 a 31 caracteres que incluyen letras mayúsculas y minúsculas, números y guiones (-), punto (.), almohadilla (#), arroba (@), igual (=), dos puntos (:) y guiones bajos (_).
 - Nivel de seguridad: Nivel de seguridad necesario para la comunicación entre el dispositivo y los usuarios SNMPv3. Seleccione una de estas opciones:
 - noAuthNoPriv: No requiere autenticación ni cifrado.
 - authNoPriv: Requiere autenticación pero no cifrado.
 - authPriv: Requiere autenticación y cifrado.
 - Protocolo de autenticación: Algoritmo de autenticación utilizado por el dispositivo y el usuario SNMPv3 para autenticar la comunicación entre ellos. Especifique el mismo algoritmo de autenticación cuando configure el usuario SNMPv3 en el administrador de SNMP.
 - Contraseña de autenticación: Pase la frase que utilizará el algoritmo de autenticación. Puede constar de 1 a 31 caracteres que incluyen letras mayúsculas y minúsculas, números y guiones (-), punto (.), almohadilla (#), espacio (), arroba (@), igual (=), dos puntos (:) y guiones bajos (_).
 - Protocolo de privacidad: Algoritmo de cifrado utilizado por el dispositivo y el usuario SNMPv3 para cifrar la comunicación entre ellos. Especifique el mismo algoritmo de cifrado al configurar el usuario SNMPv3 en el administrador de SNMP.

- Nombre de vista: Nombre de la vista SNMPv3 configurada que quiere enlazar a este usuario SNMPv3. Un usuario de SNMPv3 puede acceder a los subárboles que están enlazados a esta vista de SNMPv3 como tipo INCLUDED, pero no puede acceder a los que son de tipo EXCLUDED.

Configuración de una alarma SNMP

El dispositivo proporciona un conjunto predefinido de entidades de condición denominadas alarmas SNMP. Cuando se cumple la condición establecida para una alarma SNMP, el dispositivo genera mensajes de captura SNMP que se envían a los detectores de capturas configurados. Por ejemplo, cuando la alarma deviceAdded está habilitada, se genera un mensaje de captura y se envía a la escucha de capturas cada vez que se aprovisiona un dispositivo (instancia) en el dispositivo. Puede asignar un nivel de gravedad a una alarma SNMP. Al hacerlo, a los mensajes de interrupción correspondientes se les asigna ese nivel de gravedad.

A continuación se presentan los niveles de gravedad definidos en el dispositivo, en orden decreciente de gravedad:

- Grave
 - Mayor
- Menor
- Advertencia
- Informativo (predeterminado)

Por ejemplo, si establece un nivel de gravedad de Advertencia para la alarma SNMP denominado deviceAdded, los mensajes de captura generados cuando se agrega un dispositivo se asignan con el nivel de gravedad de Advertencia.

También puede configurar una alarma SNMP para registrar los mensajes de captura correspondientes generados siempre que se cumpla la condición de dicha alarma.

Para modificar una alarma SNMP predefinida, haga clic en **Sistema > SNMP > Alarmas**.

Configurar las notificaciones de syslog

November 23, 2023

SYSLOG es un protocolo de registro estándar. Tiene dos componentes: El módulo de auditoría SYSLOG, que se ejecuta en el dispositivo NetScaler SDX, y el servidor SYSLOG, que puede ejecutarse en un sistema remoto. SYSLOG usa UDP para la transferencia de datos.

Cuando ejecuta un servidor SYSLOG, se conecta al dispositivo SDX. A continuación, el dispositivo comienza a enviar toda la información de registro al servidor SYSLOG y el servidor puede filtrar las entradas de registro antes de almacenarlas en un archivo de registro. Un servidor SYSLOG puede recibir información de registro de más de un dispositivo SDX y un dispositivo SDX puede enviar información de registro a más de un servidor SYSLOG.

La información de registro que un servidor SYSLOG recopila de un dispositivo SDX se almacena en un archivo de registro en forma de mensajes. Por regla general, estos mensajes contienen la siguiente información:

- La dirección IP del dispositivo SDX que generó el mensaje de registro
- Una marca de tiempo
- El tipo de mensaje
- El nivel de registro (Crítico, Error, Aviso, Advertencia, Informativo, Depuración, Alerta o Emergencia)
- La información del mensaje

Puede usar esta información para analizar el origen de la alerta y, si fuera necesario, realizar las correcciones oportunas. En primer lugar, configure un servidor syslog al que el dispositivo envíe información de registro y, a continuación, especifique el formato de datos y hora para grabar los mensajes de registro.

Configurar un servidor syslog

1. Vaya a **Sistema > Notificaciones > Servidores Syslog**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En la página **Crear servidor syslog**, especifique los valores para los parámetros del servidor syslog. Para obtener una descripción de un parámetro, coloque el cursor sobre el campo correspondiente.
4. Haga clic en **Agregar** y, a continuación, en **Cerrar**.

Configurar los parámetros de syslog

1. Vaya a **Sistema > Notificaciones > Servidores Syslog**.
2. En el panel de detalles, haga clic en **Parámetros de Syslog**.
3. En la página **Configurar parámetros de Syslog**, especifique el formato de fecha y hora.
4. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Configurar notificaciones de correo

November 23, 2023

Configure un servidor SMTP para que reciba un mensaje de correo electrónico cada vez que se genere una alerta. Primero configure un servidor SMTP y, a continuación, configure un perfil de correo. En el perfil de correo, use comas para separar las direcciones de los destinatarios.

Para configurar un servidor SMTP

1. Vaya a **Sistema > Notificaciones > Correo electrónico**.
2. En el panel de detalles, haga clic en la ficha **Servidor de correo electrónico** y, a continuación, en **Agregar**.
3. En la página **Crear servidor de correo electrónico**, especifique los valores para los parámetros del servidor.
 - **Nombre del servidor/dirección IP:** Introduzca el nombre del servidor o la dirección IP del servidor de correo SMTP.
 - **Puerto:** Introduzca el número de puerto. El valor predeterminado es 25.
 - **Autenticación:** Seleccione esta opción para autenticar el acceso al servidor de correo electrónico.
 - **Seguro:** Seleccione esta opción para crear una conexión de correo electrónico segura. De forma predeterminada, se usa TLS 1.2 para cifrar la comunicación por correo electrónico.
4. Haga clic en **Crear**.

Para configurar un perfil de correo

1. Vaya a **Sistema > Notificaciones > Correo electrónico**.
2. En el panel de detalles, haga clic en la ficha **Correo electrónico** y, a continuación, en **Agregar**.
3. En la página **Crear lista de distribución de correo electrónico**, especifique los valores de los parámetros. Para obtener una descripción de un parámetro, coloque el cursor sobre el campo correspondiente.
4. Haga clic en **Crear**.

Configurar las notificaciones por SMS

November 23, 2023

Configure un servidor de servicio de mensajes cortos (SMS) para que reciba un mensaje SMS cada vez que se genere una alerta. Primero configure un servidor de SMS y, a continuación, configure un perfil de SMS. En el perfil de SMS, use comas para separar las direcciones de los destinatarios.

Configurar un servidor SMS

1. Vaya a **Sistema > Notificaciones > SMS**.
2. En el panel de detalles, haga clic en **Servidor SMS** y, a continuación, en **Agregar**.
3. En la página **Crear servidor de SMS**, especifique los valores de los parámetros del servidor de SMS. El proveedor proporciona los valores de estos parámetros.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

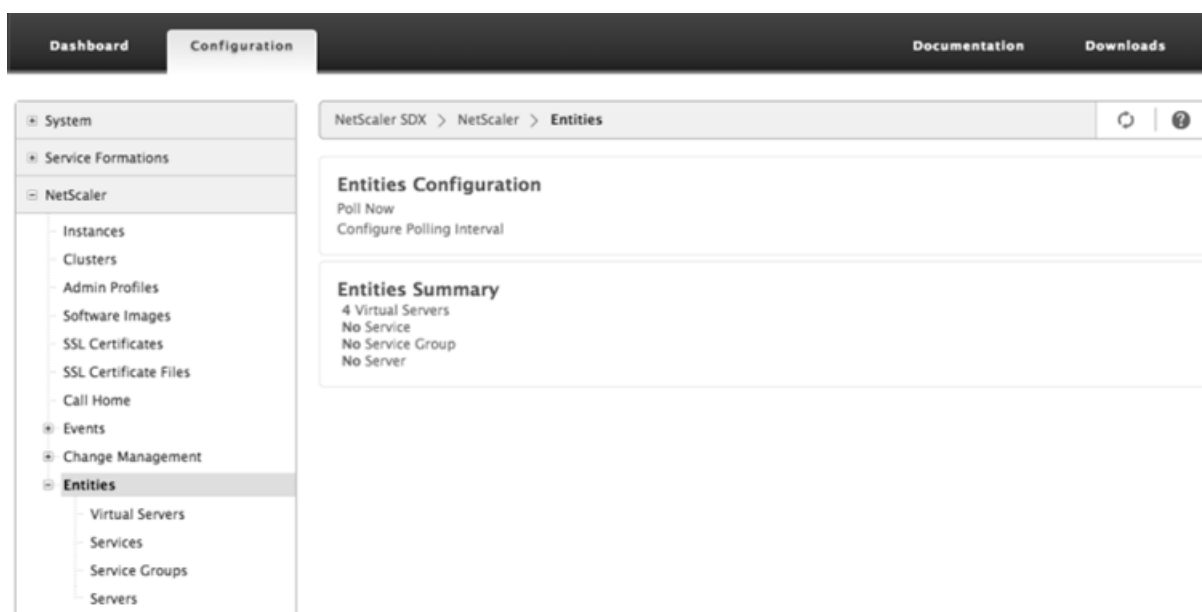
Configurar un perfil de SMS

1. Vaya a **Sistema > Notificaciones > SMS**.
2. En el panel de detalles, haga clic en **Lista de distribución de SMS** y, a continuación, en **Agregar**.
3. En la página **Crear lista de distribución de SMS**, especifique los valores de los parámetros del perfil de correo. Para obtener una descripción de un parámetro, coloque el cursor sobre el campo correspondiente.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Supervise y administre el estado en tiempo real de las entidades configuradas en un dispositivo SDX

February 15, 2024

El dispositivo NetScaler SDX puede monitorear y administrar los estados de los servidores virtuales, los servicios, los grupos de servicios y los servidores en los dispositivos virtuales alojados en el dispositivo SDX. Puede supervisar valores, como el estado de un servidor virtual y el tiempo transcurrido desde el último cambio de estado de un servicio o grupo de servicios. Esta supervisión le brinda visibilidad del estado en tiempo real de las entidades y facilita la administración de estas entidades cuando tiene muchas entidades configuradas en sus instancias de NetScaler.



Ver el estado de los servidores virtuales

Puede supervisar los valores en tiempo real del estado y el estado de un servidor virtual. También puede ver los atributos de un servidor virtual, como el nombre, la dirección IP y el tipo de servidor virtual.

- Para ver el estado de un servidor virtual
 1. En la ficha Configuración, en el panel de navegación, haga clic en **NetScaler > Entidades > Servidores virtuales**.
 2. En el panel derecho, en Servidores virtuales, vea las siguientes estadísticas:
 - Nombre del dispositivo: Nombre del VPX en el que está configurado el servidor virtual.
 - Nombre: Nombre del servidor virtual.
 - Protocolo: Tipo de servicio del servidor virtual. Por ejemplo, HTTP, TCP y SSL.
 - Estado efectivo: estado efectivo del servidor virtual, según el estado de los servidores virtuales de seguridad. Por ejemplo, ACTIVO, INACTIVO o SIN SERVICIO.
 - Estado: Estado actual del servidor virtual. Por ejemplo, ACTIVO, INACTIVO o SIN SERVICIO.
 - Estado: Porcentaje de servicios que están en estado UP y están enlazados al servidor virtual. Para calcular el porcentaje de salud se utiliza la siguiente fórmula: $(\text{Número de servicios vinculados a UP} * 100) / \text{Total de servicios consolidados}$
 - Dirección IP: dirección IP del servidor virtual. Los clientes envían solicitudes de conexión a esta dirección IP.
 - Puerto: puerto en el que el servidor virtual escucha las conexiones del cliente.

- Último cambio de estado: tiempo transcurrido (en días, horas, minutos y segundos) desde el último cambio en el estado del servidor virtual. Es decir, el tiempo durante el cual el servidor virtual ha estado en el estado actual. Esta información solo está disponible para servidores virtuales configurados en NetScaler versión 9.0 y posterior.

The screenshot shows the NetScaler SDX Configuration interface. On the left is a navigation tree with 'Virtual Servers' selected under 'Entities'. The main area displays a table of virtual servers with the following columns: Device Name, Name, Protocol, Effective State, State, Health, IP Address, Port, and Last State Change. All servers listed are in an 'Up' state with a health of 100%.

Device Name	Name	Protocol	Effective State	State	Health	IP Address	Port	Last State Change
ns2(10.102.163.5)	v1	HTTP	Up	Up	100	10.102.161.13	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	v2	HTTP	Up	Up	100	10.102.161.14	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	v3	SSL	Up	Up	100	10.102.161.15	443	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	spotted_vip_1	HTTP	Up	Up	100	10.102.161.16	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	spotted_vip_2	SSL	Up	Up	100	10.102.161.71	443	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	spotted_vip_3	HTTP	Up	Up	100	10.102.161.18	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	v1	HTTP	Up	Up	100	10.102.161.13	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	v2	HTTP	Up	Up	100	10.102.161.14	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	v3	SSL	Up	Up	100	10.102.161.15	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	spotted_vip_1	HTTP	Up	Up	100	10.102.161.16	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	spotted_vip_2	SSL	Up	Up	100	10.102.161.71	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	spotted_vip_3	HTTP	Up	Up	100	10.102.161.18	80	Mon, 10 Mar 2014 17:14:36 GMT

- Visualización de servicios y grupos de servicios enlazados a un servidor virtual

Puede supervisar el estado en tiempo real de los servicios y grupos de servicios enlazados a un servidor virtual. Esta supervisión le permite comprobar el estado de los servicios que pueden provocar que el porcentaje de salud de un servidor virtual sea bajo, para que pueda tomar las medidas adecuadas.

Para ver los servicios y los grupos de servicios enlazados a un servidor virtual

1. En la ficha Configuración, en el panel izquierdo, haga clic en **NetScaler > Entidades > Servidores virtuales**.
2. En el panel de detalles, en Servidores virtuales, haga clic en el nombre del servidor virtual para el que quiere mostrar los servicios y grupos de servicios enlazados y, en Acciones, haga clic en Servicios enlazados o Grupos de servicios enlazados. También puede hacer clic con el botón secundario en el nombre del servidor virtual y, a continuación, hacer clic en Servicios enlazados o Grupos de servicios

Name	Protocol	Effective State	State	Health	IP Address	Port	Last State Change
ns2(10.102.163.5) v2	HTTP	Up	Up	00	10.102.161.13	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) v3	SSL	Up	Up	00	10.102.161.15	443	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) spotted_vip_1	HTTP	Up	Up	00	10.102.161.16	80	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) spotted_vip_2	SSL	Up	Up	00	10.102.161.71	443	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5) spotted_vip_3	HTTP	Up	Up	00	10.102.161.18	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) v1	HTTP	Up	Up	00	10.102.161.13	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) v2	HTTP	Up	Up	00	10.102.161.14	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) v3	SSL	Up	Up	00	10.102.161.15	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_1	HTTP	Up	Up	00	10.102.161.16	80	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_2	SSL	Up	Up	00	10.102.161.71	443	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4) spotted_vip_3	HTTP	Up	Up	00	10.102.161.18	80	Mon, 10 Mar 2014 17:14:36 GMT

Ver el estado de los servicios

Puede supervisar los valores en tiempo real del estado de un servicio y la duración durante la cual el servicio ha estado en el estado actual.

Para ver el estado de los servidores virtuales

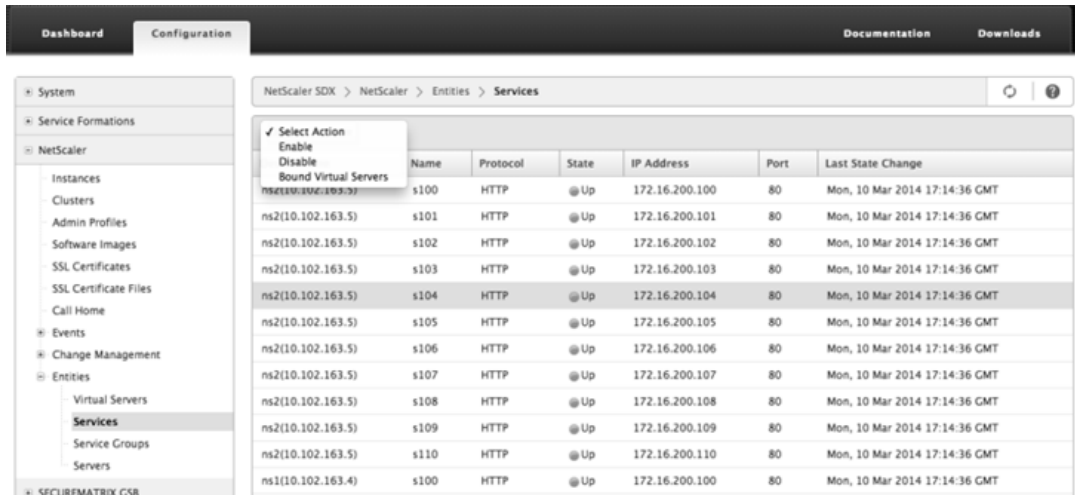
1. En la ficha Configuración, en el panel de navegación, haga clic en **NetScaler > Entidades > Servicio**.
2. En el panel de detalles, en Servicios, vea las siguientes estadísticas:
 - Nombre del dispositivo: nombre del dispositivo en el que se configura el servicio.
 - Nombre: nombre del servicio.
 - Protocolo: tipo de servicio, que determina el comportamiento del servicio. Por ejemplo, HTTP, TCP, UDP o SSL.
 - Estado: estado actual del servicio. Por ejemplo, ACTIVO, INACTIVO o SIN SERVICIO.
 - Dirección IP: dirección IP del servicio.
 - Puerto: puerto en el que escucha el servicio.
 - Último cambio de estado: tiempo transcurrido (en días, horas, minutos y segundos) desde el último cambio en el estado del servicio. Es decir, la duración del tiempo durante el cual el servicio ha estado en el estado actual.

- Ver los servidores virtuales a los que está enlazado un servicio

Puede ver los servidores virtuales a los que está vinculado un servicio y supervisar el estado en tiempo real de los servidores virtuales.

Para ver los servidores virtuales a los que está enlazado un servicio

1. En la ficha Configuración, en el panel de navegación, haga clic en **NetScaler > Entidades > Servicio**.
2. En el panel de detalles, en Servicios, haga clic en el nombre del servicio para el que quiere ver los servidores virtuales enlazados. A continuación, en el menú Acción, seleccione Servidores virtuales enlazados. Como alternativa, haga clic con el botón secundario en el servicio y, a continuación, haga clic



Ver el estado de los grupos de servicios

Puede supervisar el estado en tiempo real de un miembro de un grupo de servicios desde la interfaz SDX.

Para ver el estado de los grupos de servicios

1. En la ficha Configuración, en el panel de navegación, haga clic en **NetScaler > Entidades > Grupos de servicios**.
2. En el panel de detalles, en Grupos de servicios, vea las siguientes estadísticas:
 - Nombre del dispositivo: Nombre del dispositivo en el que está configurado el grupo de servicios.
 - Nombre: Nombre del grupo de servicios.
 - Dirección IP: Dirección IP de cada servicio que es miembro del grupo de servicios.
 - Puerto: puertos en los que escuchan los miembros del grupo de servicios.
 - Protocolo: Tipo de servicio, que determina el comportamiento del grupo de servicios. Por ejemplo, HTTP, TCP, UDP o SSL.
 - Estado efectivo: Estado efectivo del grupo de servidores virtuales, según el estado de los servidores virtuales de copia de seguridad. Por ejemplo, ACTIVO, INACTIVO o SIN SERVICIO
 - Estado: Estado efectivo del grupo de servicios, que se basa en el estado del miembro del grupo de servicios. Por ejemplo, ACTIVO, INACTIVO o SIN SERVICIO.

- Último cambio de estado: tiempo transcurrido (en días, horas, minutos y segundos) desde el último cambio en el estado del miembro del grupo de servicio. Es decir, la duración del tiempo durante el cual el miembro del grupo de servicio ha estado en el estado actual. Esta información solo está disponible para los miembros del grupo de servicios configurados en NetScaler versión 9.0 y posterior.
- Ver los servidores virtuales a los que está enlazado un servicio

Puede ver los servidores virtuales a los que está vinculado un servicio y supervisar el estado en tiempo real de los servidores virtuales.

Para ver los servidores virtuales a los que está enlazado el servicio

1. En la ficha Configuración, en el panel izquierdo, haga clic en **NetScaler > Entidades > Servidores**.
2. En el panel derecho, en Servidores, seleccione el servidor de la lista y, en el menú Acciones, haga clic en Servicios virtuales enlazados. También puede hacer clic con el botón derecho en el servicio y hacer clic en Servidores

Ver el estado de los servidores

Puede supervisar y administrar los estados de los servidores en las instancias de NetScaler. Esta supervisión le brinda visibilidad del estado en tiempo real de los servidores y facilita la administración de estos servidores cuando tiene muchos servidores.

Para ver el estado de los servidores

1. En la ficha Configuración, en el panel de navegación, haga clic en **NetScaler > Entidades > Servidores**.
2. En el panel de detalles, en Servidores, vea las siguientes estadísticas:
 - Nombre del dispositivo: Especifica el nombre del dispositivo en el que está configurado el servidor.
 - Nombre: especifica el nombre del servidor.
 - Dirección IP: Especifica la dirección IP del servidor. Los clientes envían solicitudes de conexión a esta dirección IP.
 - Estado: Especifica el estado actual del servidor. Por ejemplo, ACTIVO, INACTIVO y SIN SERVICIO.
 - Último cambio de estado: especifica el tiempo transcurrido (en días, horas, minutos y segundos) desde el último cambio en el estado del servidor. Es decir, la duración del tiempo durante el cual el servidor se encuentra en el estado actual.

Name	IP Address	State	Last State Change
ns2(10.102.163.5)	172.16.200.100	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.101	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.102	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.103	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.104	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.105	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.106	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.107	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.108	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.109	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns2(10.102.163.5)	172.16.200.110	Enabled	Mon, 10 Mar 2014 17:14:36 GMT
ns1(10.102.163.4)	172.16.200.100	Enabled	Mon, 10 Mar 2014 17:14:36 GMT

Configurar el intervalo de sondeo

Puede establecer el intervalo de tiempo para el que quiere que el dispositivo SDX sondee los valores en tiempo real de los servidores virtuales, servicios, grupos de servicios y servidores. De forma pre-determinada, el dispositivo sondea los valores cada 30 minutos.

- Configurar el intervalo de sondeo para servidores virtuales, servicios, grupos de servicios y servidores.
 1. En la ficha Configuración, haga clic en **NetScaler > Entidades** y, en el panel derecho, haga clic en Configurar intervalo de sondeo.
 2. En el cuadro de diálogo Configurar intervalo de sondeo, escriba el número de minutos que quiere establecer como el intervalo de tiempo para el que SDX debe sondear el valor de entidad. El valor mínimo del intervalo de sondeo es de 30 minutos. Haga clic en Aceptar.

Supervisión y administración de eventos generados en instancias de NetScaler

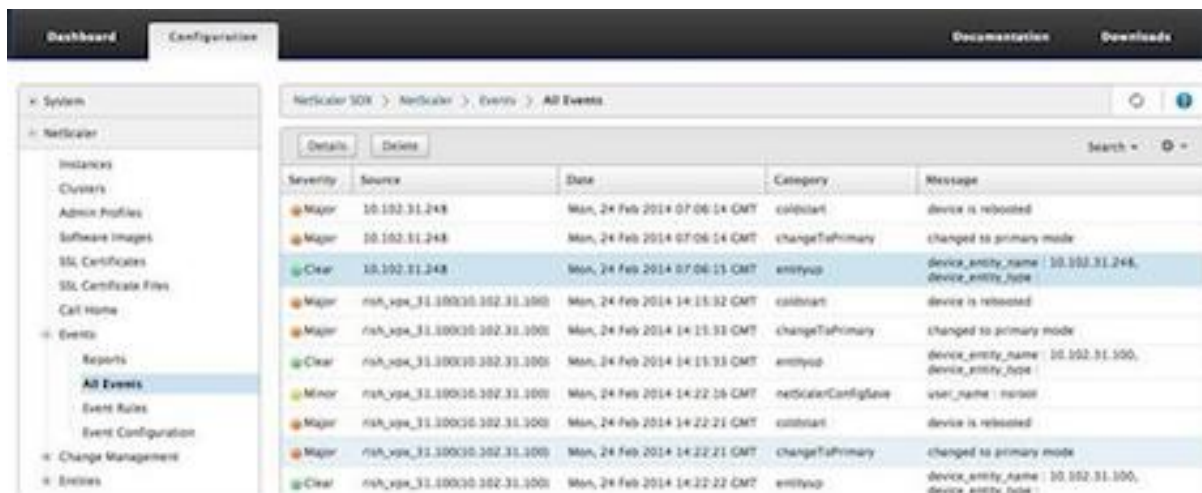
February 15, 2024

Utilice la función Eventos para supervisar y administrar los eventos generados en las instancias de NetScaler. El Servicio de administración identifica los eventos en tiempo real, lo que le ayuda a abordar los problemas de forma inmediata y mantiene las instancias de NetScaler funcionando de manera eficaz. También puede configurar reglas de eventos para filtrar los eventos generados y recibir notificaciones para tomar medidas en la lista de eventos filtrada.

Ver todos los eventos

Puede ver todos los eventos generados en las instancias de NetScaler provisionadas en el dispositivo NetScaler SDX. Puede ver los detalles como la gravedad, la categoría, la fecha, la fuente y el mensaje de cada uno de los eventos.

Para ver los eventos, vaya a **Configuración > NetScaler > Eventos > Todos los eventos**.



Puede ver el historial de eventos y los detalles de la entidad si selecciona el evento y hace clic en el botón **Detalles**. También puede buscar un evento en particular o eliminarlo de esta página.

Nota: Después de eliminar los eventos, no podrá recuperarlos.

- Ver informes

La página Informes muestra el resumen de los eventos en formato gráfico. La vista de los informes se puede basar en varias escalas de tiempo. De forma predeterminada, la escala de tiempo es Día.

Para mostrar los informes, vaya a **Configuración > NetScaler > Eventos** Informes. A continuación se presentan los informes gráficos compatibles con Management Service

- Eventos

El informe de eventos es una representación en gráfico circular del número de eventos, segmentados y codificados por colores en función de su gravedad.

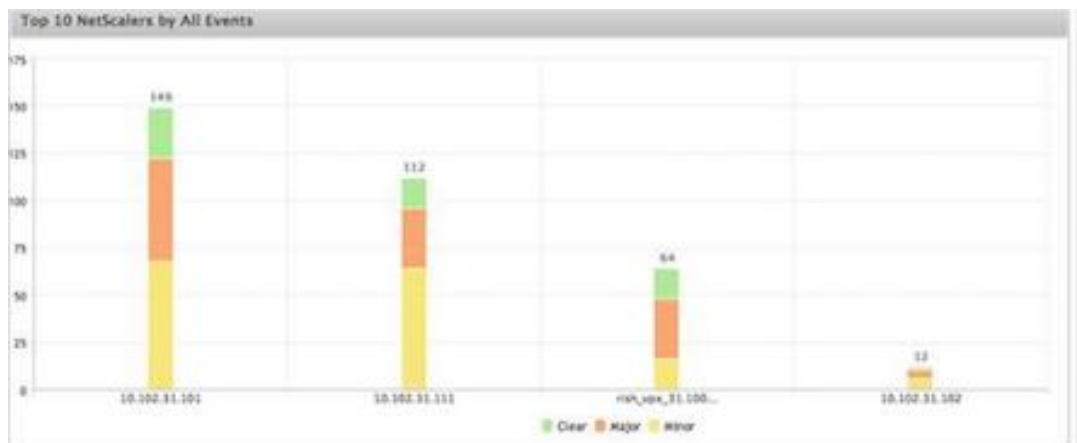


Para ver los detalles de los eventos de una gravedad en particular, haga clic en ese segmento del gráfico circular, puede ver los siguientes detalles:

- * Origen: nombre del sistema, nombre de host o dirección IP en la que se generó el evento.
- * Fecha: fecha y hora en que se generó la alarma.
- * Categoría: categoría de evento (por ejemplo, `entityup`).
- * Mensaje: Descripción del evento.

– Las 10 principales instancias de NetScaler según todos los eventos

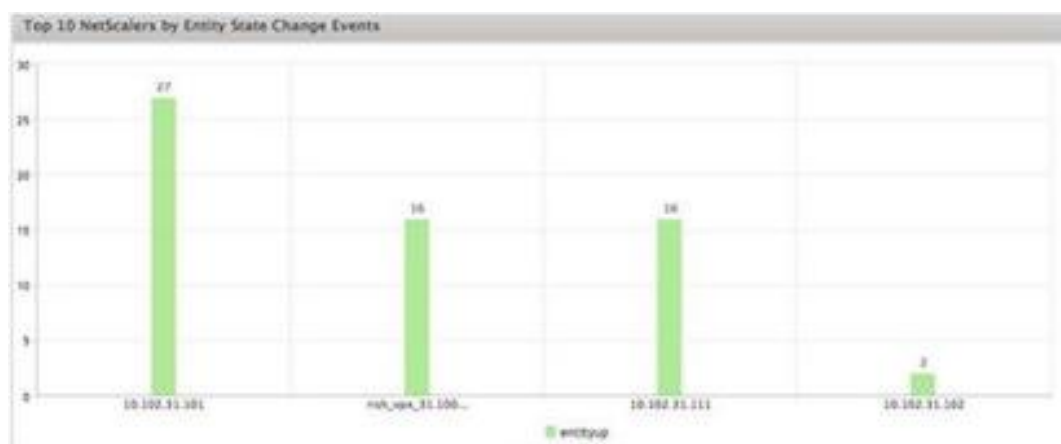
Este informe es un gráfico de barras que muestra las 10 instancias principales de NetScaler según el número de eventos de la escala de tiempo seleccionada.



– Las 10 principales instancias de NetScaler por eventos de cambio de estado de entidad

Este informe es un gráfico de barras que muestra las 10 instancias principales de NetScaler según el número de cambios en el estado de la entidad para la escala de tiempo seleccionada. Los cambios en el estado de la entidad reflejan eventos activos, inactivos o fuera

de servicio de la entidad.



- Las 10 principales instancias de NetScaler por eventos de infracción de umbrales

Este informe es un gráfico de barras que muestra las 10 instancias principales de NetScaler según el número de eventos de violación del umbral de la escala de tiempo seleccionada. Los eventos de infracción de umbral reflejan los siguientes eventos:

- * cpuUtilization
- * memoryUtilization
- * diskUsageHigh
- * temperatureHigh
- * voltageLow
- * voltageHigh
- * fanSpeedLow
- * temperatureCpuHigh
- * interfaceThroughputLow
- * interfaceBWUseHigh
- * aggregateBWUseHigh

- Las 10 principales instancias de NetScaler por eventos de fallas de hardware

Este informe es un gráfico de barras que muestra las 10 instancias principales de NetScaler según la cantidad de eventos de fallas de hardware para la escala de tiempo seleccionada. Los eventos de error de hardware reflejan los siguientes eventos:

- * hardDiskDriveErrors
- * compactFlashErrors
- * powerSupplyFailed
- * “sslCardFailed”

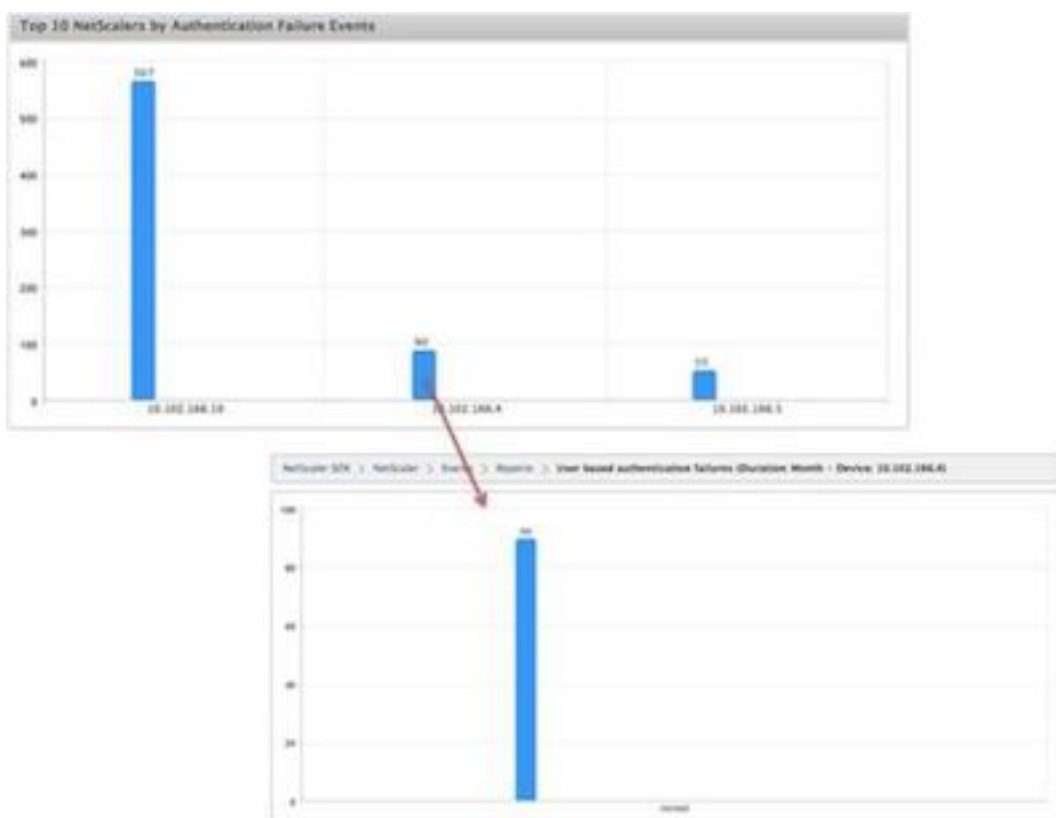
- Las 10 principales instancias de NetScaler por eventos de cambio de configuración

Este informe es un gráfico de barras que refleja las 10 instancias principales de NetScaler

según la cantidad de eventos de cambio de configuración para la escala de tiempo seleccionada. Puede hacer clic en el gráfico para desglosar y ver los cambios de configuración basados en el usuario para una instancia. Puede ver los detalles del estado de autorización y ejecución haciendo clic en este gráfico.

- <**Las 10 principales instancias de NetScaler por eventos de error de autenticación**

Este informe es un gráfico de barras que muestra las 10 instancias principales de NetScaler según el número de eventos de error de autenticación para la escala de tiempo seleccionada. Puede hacer clic en el gráfico para desglosar y ver los errores de autenticación basados en el usuario de una instancia.



- Configuración de reglas de eventos

Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen con los criterios de filtro de la regla, se lleva a cabo la acción asociada a la regla. Las condiciones para las que puede crear filtros son: Gravedad, dispositivos, objetos de error y categoría.

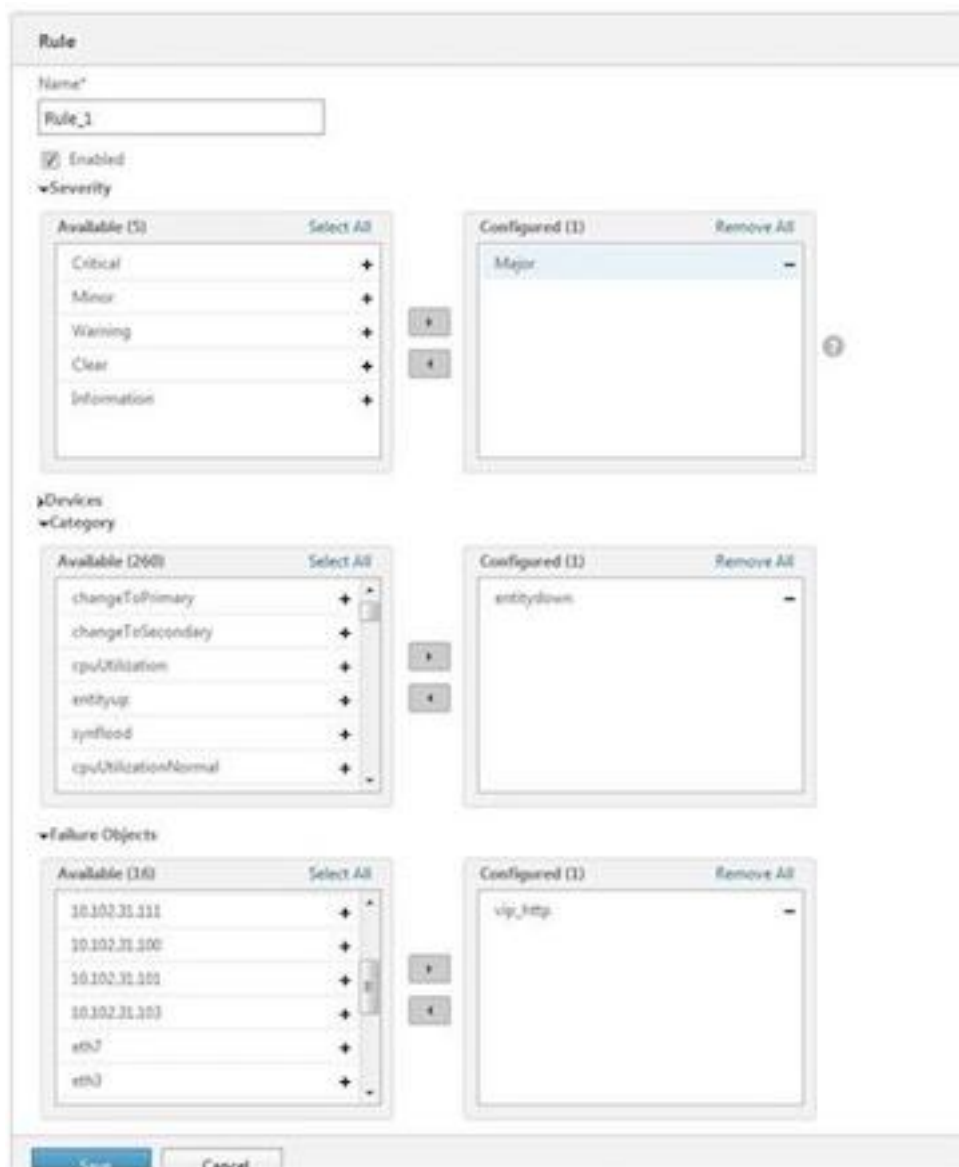
Puede asignar las siguientes acciones a los eventos:

- **Acción Enviar correo electrónico** Envía un correo electrónico para los eventos que coinciden con los criterios del filtro.

- **Acción Enviar SMS** Envía un servicio de mensajes cortos (SMS) para los eventos que coinciden con los criterios del filtro.

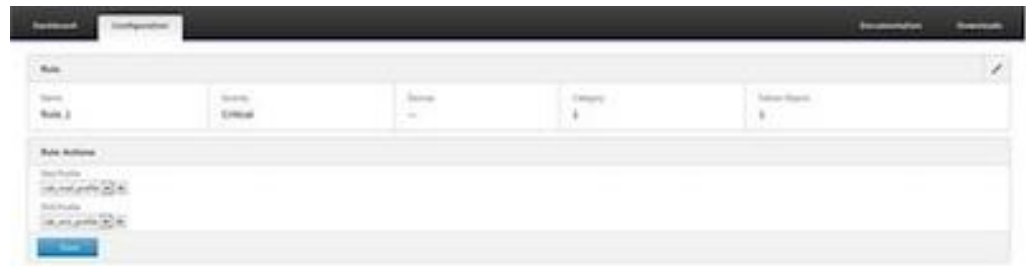
Para agregar reglas de eventos

1. Vaya a **Configuración > NetScaler > Eventos > Reglas de eventos** y haga clic en Agregar.
2. En la página Regla, defina los siguientes parámetros:
 - Nombre: Nombre de la regla de evento.
 - Habilitado: Habilite la regla de evento.
 - Gravedad: Gravedad de los eventos para los que quiere agregar la regla de evento.
 - Dispositivos: direcciones IP de las instancias de NetScaler para las que quiere definir una regla de eventos.
 - Categoría: Categoría o categorías de los eventos generados por las instancias de NetScaler.
 - Objetos de error: Instancias o contadores de entidad para los que se ha generado un evento.



Nota: Esta lista puede contener nombres de contadores para todos los eventos relacionados con umbrales, nombres de entidades para todos los eventos relacionados con entidades y nombres de certificados para eventos relacionados con certificados.

3. Haga clic en Guardar.
4. En Acciones de reglas, puede asignar las acciones de notificación para el evento.
 - a) Perfil de correo: Detalles del servidor de correo y del perfil de correo. Se activa un correo electrónico cuando los eventos cumplen con los criterios de filtro definidos.
 - b) Perfil de SMS: Detalles del servidor SMS y del perfil de SMS. Se activa un SMS cuando los eventos cumplen con los criterios de filtro definidos.



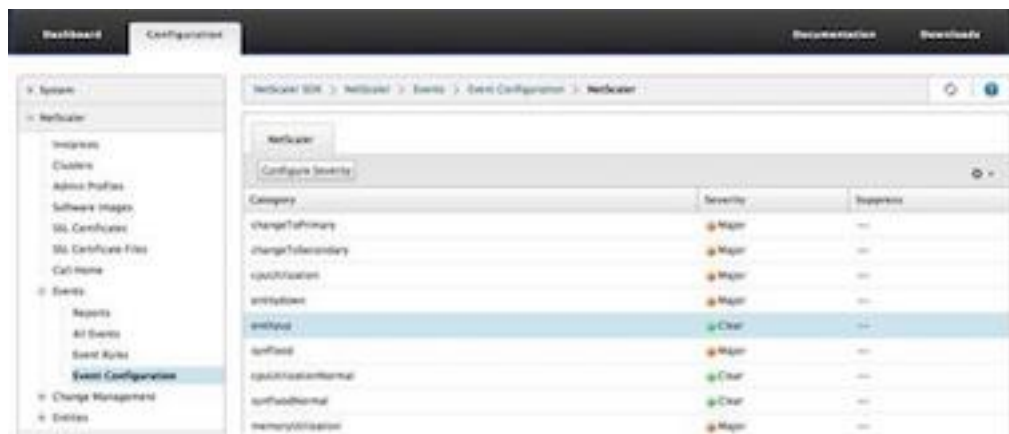
5. Haga clic en Listo.

- Configuración de eventos

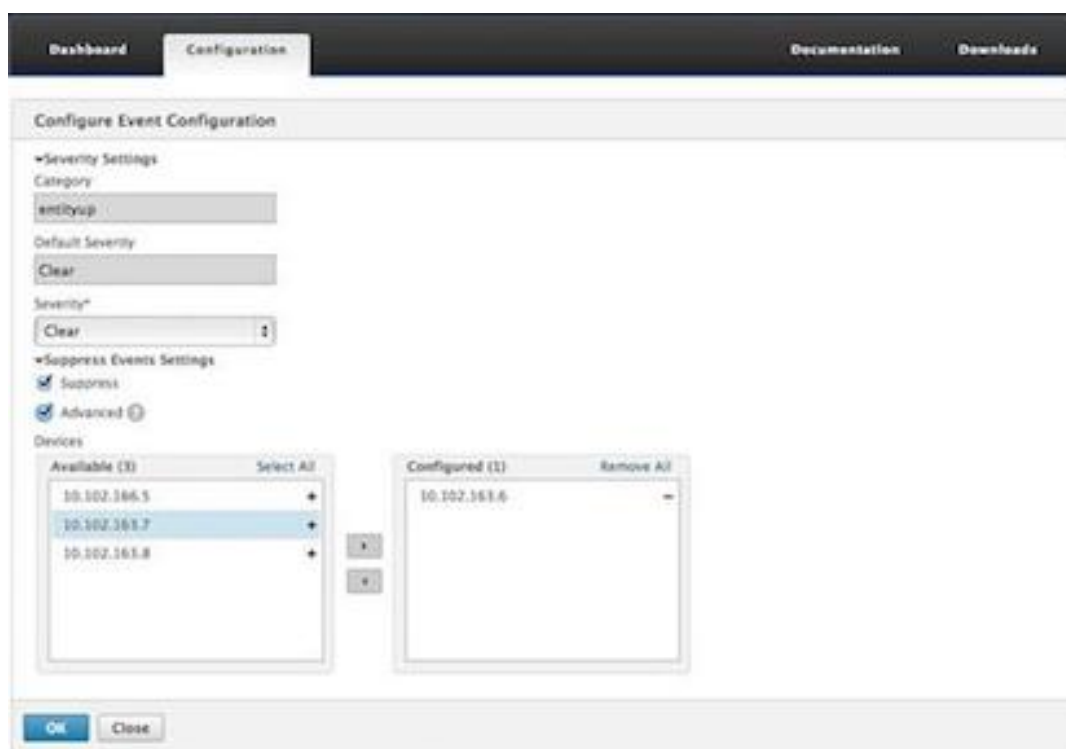
Puede asignar niveles de gravedad a los eventos que se generan para las instancias de NetScaler en el dispositivo SDX. Puede definir los siguientes tipos de niveles de gravedad: Crítico, Mayor, Menor, Advertencia, Borrar e Información. También puede suprimir los eventos durante un tiempo específico.

Para configurar la gravedad:

1. Vaya a **Configuración > NetScaler > Eventos > Configuración** de eventos, seleccione el evento de la lista y, a continuación, haga clic en Configurar gravedad.



2. En la página Configurar configuración de eventos, seleccione el nivel de gravedad requerido en la lista desplegable.
3. Como alternativa, puede suprimir los eventos seleccionando la casilla de verificación Suprimir. También puede especificar las instancias de NetScaler para las que quiere suprimir este evento mediante la opción Avanzadas.



4. Haga clic en Aceptar.

Soporte de Call Home para instancias de NetScaler en un dispositivo SDX

February 15, 2024

La función Call Home monitorea sus instancias de NetScaler para detectar condiciones de error comunes. Ahora puede configurar, habilitar o inhabilitar la función Call Home en las instancias de NetScaler desde la interfaz de usuario del Servicio de administración.

Nota: La instancia de NetScaler debe estar registrada en el servidor de soporte técnico de Citrix para que Call Home pueda cargar los datos del sistema en el servidor cuando se produzcan condiciones de error predefinidas en el dispositivo. Al habilitar la función Call Home en la instancia de NetScaler, se inicia el proceso de registro.

- Habilitar e inhabilitar Call Home en una instancia de NetScaler

Puede habilitar la función Call Home en una instancia de NetScaler desde el Servicio de administración. Al habilitar la función Call Home, el proceso Call Home registra la instancia de NetScaler en el servidor de soporte técnico de Citrix. El registro tarda algún tiempo en completarse. Durante ese tiempo, el Servicio de Gestión muestra el progreso del registro.

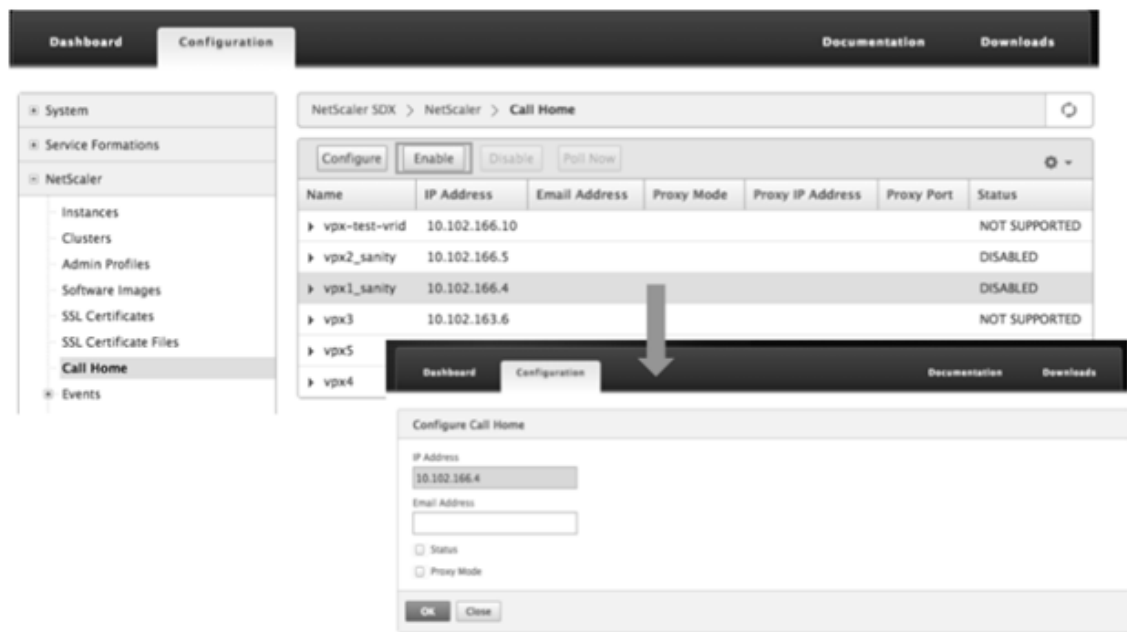
Para habilitar la función Call Home, vaya a **Configuración > NetScaler > Call Home**, seleccione la instancia de NetScaler y haga clic en el botón Habilitar. En la página de confirmación, haga clic en Sí.

Para inhabilitar la función Call Home, vaya a **Configuración > NetScaler > Call Home**, seleccione la instancia de NetScaler y haga clic en el botón Inhabilitar. En la página de confirmación, haga clic en Sí.

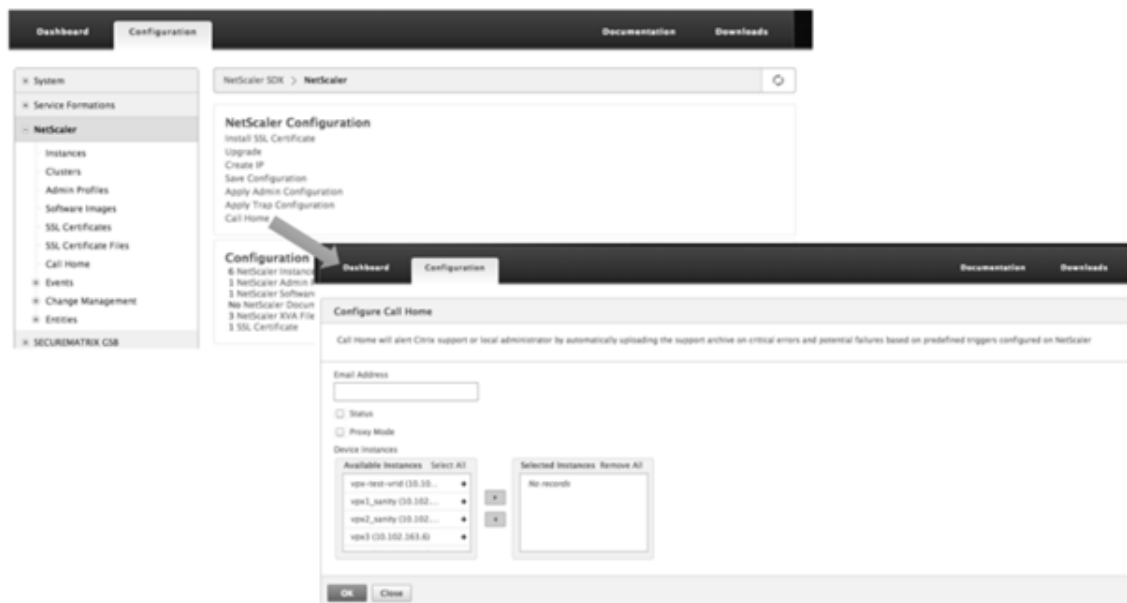
Si habilita Call Home, puede configurar las siguientes opciones:

1. (Opcional) Especifique la dirección de correo electrónico del administrador. El proceso Call Home envía la dirección de correo electrónico al servidor de asistencia técnica, donde se almacena para correspondencia futura con respecto a Call Home.
 2. (Opcional) Habilite el modo proxy de Call Home. Call Home puede cargar los datos de su instancia de NetScaler al servidor TaaS de Citrix a través de un servidor proxy. Para utilizar esta función, habilítela en su instancia de NetScaler y especifique la dirección IP y el número de puerto de un servidor proxy HTTP. Todo el tráfico del servidor proxy a los servidores TaaS (a través de Internet) se realiza a través de SSL y está cifrado, por lo que la seguridad y la privacidad de los datos no se ven comprometidas.
- Para configurar Call Home en la instancia de NetScaler desde el Servicio de administración
Puede configurar la función Call Home en una sola instancia o en varias instancias al mismo tiempo.

Para configurar la función Call Home en una sola instancia de NetScaler, vaya a **Configuración > NetScaler > Call Home**, seleccione la instancia de NetScaler y haga clic en el botón Configurar. En la página Configurar Call Home, haga clic en Aceptar.



Para configurar la función Call Home en varias instancias de NetScaler, vaya a **Configuración** NetScaler. En el panel derecho, haga clic en Call Home. En la página Configurar Call Home, seleccione las instancias de NetScaler en la sección Instancias disponibles, especifique otros detalles y haga clic en Aceptar.



- Sondeo de las instancias de NetScaler

Para sondear la función Call Home de todas las instancias de NetScaler y ver el estado actual, vaya a **Configuración > NetScaler > Call Home** y haga clic en **Sondear ahora**. En la página de confirmación, haga clic en **Sí**.

Supervisión del estado del sistema

November 23, 2023

La supervisión del estado del sistema detecta errores en los componentes supervisados, de modo que pueda tomar medidas correctivas para evitar una falla. Los siguientes componentes se supervisan en un dispositivo NetScaler SDX:

- Recursos de hardware y software
- Discos físicos y virtuales
- <Sensores de hardware, como sensores de ventilador, temperatura, voltaje y fuente de alimentación
- Interfaces

En la ficha **Supervisión**, haga clic en **Estado del sistema**. Se muestra un resumen de todos los componentes. Para ver los detalles de los componentes supervisados, expanda **Estado del sistema**, a continuación, haga clic en el componente que quiere supervisar.

- Supervisión de los recursos en el dispositivo SDX

Puede supervisar los componentes de hardware y software en el dispositivo SDX y tomar medidas correctivas si es necesario. Para ver los componentes supervisados, en la ficha Supervisión, expanda Estado del sistema y, a continuación, haga clic en Recursos. Se muestran los detalles de los recursos de hardware y software. Para todos los componentes de hardware, se muestran los valores actuales y esperados. Para los componentes de software, excepto la versión de firmware de BMC, los valores actuales y esperados se muestran como no aplicables (NA).

- **Nombre:** nombre del componente, como la versión de firmware de la CPU, la memoria o el BMC.
- **Estado:** estado (condición) del componente. Para hardware y para la versión de firmware de BMC, ERROR indica una desviación del valor esperado. Para las llamadas a Citrix Hypervisor, ERROR indica que Management Service no puede comunicarse con Citrix Hypervisor mediante una llamada API, HTTP, PING o SSH. Para el complemento Health Monitor, ERROR indica que el complemento no está instalado en Citrix Hypervisor.
- **Valor actual:** valor actual del componente. En condiciones normales, el valor actual es el mismo que el valor esperado.
- **Valor esperado:** valor esperado para el componente. No se aplica a las llamadas de software a Citrix Hypervisor.

Supervisar los recursos de almacenamiento en el dispositivo SDX

Puede supervisar los discos en el dispositivo SDX y tomar medidas correctivas si es necesario. Para ver los componentes supervisados, en la ficha **Supervisión**, expanda **Estado del sistema** y, a continuación, haga clic en **Almacenamiento**. Se muestran los detalles de los discos físicos y de los discos virtuales o particiones creadas a partir de discos físicos.

Para los discos (disco), se muestran los siguientes detalles:

- **Nombre** Nombre del disco físico.
- **Tamaño:** tamaño del disco, en GB.
- **Utilizados:** cantidad de datos en el disco, en GB.
- **Transacciones/s:** número de bloques que se leen o escriben por segundo. Este número se lee en el resultado de `iostat`.
- **Bloques leídos:** número de bloques que se leen por segundo. Puede usar este valor para medir la velocidad de salida del disco.
- **Bloques escrito/s:** número de bloques que se escriben por segundo. Puede usar este valor para medir la velocidad de entrada en el disco.
- **Total de bloques leídos:** número de bloques leídos desde que se inició el dispositivo por última vez
- **Total de bloques escritos:** número de bloques escritos desde que se inició el dispositivo por última vez.

Para discos virtuales o particiones (repositorio de almacenamiento), se muestran los siguientes detalles:

- **Compartimiento de unidad:** número de la unidad en el compartimiento de unidades. Puede ordenar los datos en este parámetro.
- Estado: **estado** (condición) de la unidad en la bahía de unidades. Valores posibles:
 - BUENO: La unidad está en buen estado y lista para usar.
 - ERROR: la unidad falló y debe reemplazarse.
 - FALTA: No se ha detectado una unidad en la bahía de unidades.
 - UNKNOWN: Existe una nueva unidad sin formato en la bahía de la unidad.
- **Nombre: Nombre** definido por el sistema del depósito de almacenamiento.
- **Tamaño:** tamaño del repositorio de almacenamiento, en GB.
- **Utilizados:** cantidad de datos en el repositorio de almacenamiento, en GB.

Supervisar los sensores de hardware en el dispositivo SDX

Puede supervisar los componentes de hardware en el dispositivo SDX y tomar medidas correctivas si es necesario. En la ficha **Supervisión**, expanda **Estado del sistema** y, a continuación, haga clic en

Sensores de hardware. La función de supervisión muestra detalles sobre la velocidad de los diferentes ventiladores, la temperatura y el voltaje de los diferentes componentes y el estado de la fuente de alimentación.

Para la velocidad del ventilador, se muestran los siguientes detalles:

- **Nombre:** Nombre del ventilador.
- **Estado:** estado (estado) del ventilador. ERROR indica una desviación del valor esperado. NA indica que el ventilador no está presente.
- **Valor actual (RPM):** Rotaciones actuales por minuto.

La información de temperatura incluye los siguientes detalles:

- **Nombre:** nombre del componente, como la CPU o el módulo de memoria (por ejemplo, P1-DIMM1A).
- **Estado:** estado (condición) del componente. ERROR indica que el valor actual está fuera de rango.
- **Valor actual (grado C):** Temperatura actual, en grados, del componente.

La información de voltaje incluye los siguientes detalles:

- **Nombre:** nombre del componente, como el núcleo de la CPU.
- **Estado:** estado (condición) del componente. ERROR indica que el valor actual está fuera de rango.
- **Valor actual (voltios):** voltajes actuales presentes en el componente.

La información sobre la fuente de alimentación incluye los siguientes detalles:

- **Nombre:** Nombre del componente.
- **Estado:** estado (condición) del componente. Valores posibles:
 - **Error:** Solo hay una fuente de alimentación conectada o funcionando.
 - **OK:** Ambas fuentes de alimentación están conectadas y funcionan como se esperaba.

Supervisar las interfaces en el dispositivo SDX

Puede supervisar las interfaces del dispositivo SDX y tomar medidas correctivas si es necesario. En la ficha **Supervisión**, expanda **Estado del sistema** y, a continuación, haga clic en **Interfaces**. La función de supervisión detalla la siguiente información sobre cada interfaz:

- **Interfaz:** número de interfaz en el dispositivo SDX.
- **Estado:** estado de la interfaz. Valores posibles: ACTIVO, INACTIVO.
- **VF asignadas/totales:** Cantidad de funciones virtuales (VF) asignadas a la interfaz y número de funciones virtuales disponibles en esa interfaz. Las diferentes plataformas admiten un número diferente de VF.

- **Paquetes Tx:** número de paquetes transmitidos desde que se inició el dispositivo por última vez.
- **Paquete Rx:** número de paquetes recibidos desde que se inició el dispositivo por última vez.
- **Bytes de transmisión:** número de bytes transmitidos desde que se inició el dispositivo por última vez.
- **Bytes Rx:** número de bytes recibidos desde que se inició el dispositivo por última vez.
- **Errores de transmisión:** número de errores en la transmisión de datos desde que se inició el dispositivo por última vez.
- **Errores de recepción:** número de errores en la recepción de datos desde que se inició el dispositivo por última vez.

Configurar los parámetros de notificación del sistema

November 23, 2023

Puede enviar notificaciones para comunicarse con grupos de usuarios seleccionados para una serie de funciones relacionadas con el sistema. Puede configurar un servidor de notificaciones en SDX Management Service para configurar los servidores de puerta de enlace de correo electrónico y servicio de mensajes cortos (SMS) para enviar notificaciones de correo electrónico y texto (SMS) a los usuarios.

Nota

Después de actualizar a SDX Management Service versión 11.1, la notificación del sistema se habilita para todas las categorías de eventos y las notificaciones se envían al perfil de correo electrónico o SMS existente.

Para configurar los ajustes de notificación del sistema

1. Vaya a **Sistema > Notificaciones > Configuración y**, a continuación, haga clic en **Cambiar configuración de notificaciones**.
2. En la página **Configurar parámetros de notificación del sistema**, introduzca los siguientes detalles:
 - **Categoría:** Categoría o categorías de los eventos generados por SDX Management Service.
 - **Correo electrónico:** Seleccione una lista de distribución de correo electrónico en el menú desplegable. También puede crear una nueva lista de distribución de correo electrónico haciendo clic en el icono **+** e introduciendo los detalles del nuevo servidor de correo electrónico en los campos correspondientes.
 - **SMS (mensaje de texto):** Seleccione una lista de distribución de SMS en el menú desplegable. También puede crear una

nueva lista de distribución de SMS haciendo clic en el icono + e introduciendo los detalles del nuevo servidor de SMS en los campos correspondientes.

3. Haga clic en **Aceptar**.

Habilitar y inhabilitar funciones del Servicio de administración

November 23, 2023

Nota:

Esta función está disponible en la versión 13.1 compilación 12.x y posteriores.

En un dispositivo NetScaler SDX, Management Service sondea las instancias de NetScaler en segundo plano en busca de operaciones, como certificados SSL, funciones de red y auditoría de configuración. Hay una opción disponible para habilitar o inhabilitar este sondeo en función de sus requisitos. La desactivación de este sondeo mejora el rendimiento de las instancias del Servicio de administración y ADC.

Para habilitar o inhabilitar funciones mediante la interfaz gráfica de usuario

1. Vaya a **Sistema > Configuración del sistema**.
2. Haga clic en **Configurar funciones**.
3. Seleccione una función y haga clic en **Habilitar** o **Inhabilitar**.

Configurar el Servicio de administración

November 23, 2023

Management Service le permite administrar sesiones de cliente y realizar tareas de configuración, como la creación y administración de cuentas de usuario y la modificación de las directivas de copia de seguridad y poda de acuerdo con sus requisitos. También puede reiniciar Management Service y actualizar la versión del Servicio de administración. Además, puede crear archivos tar del Servicio de administración y Citrix Hypervisor y enviarlos a la asistencia técnica.

Administrar sesiones de clientes

Se crea una sesión de cliente cuando un usuario inicia sesión en Management Service. Puede ver todas las sesiones de cliente en el dispositivo en el panel **Sesiones**.

En el panel **Sesiones**, puede ver los siguientes detalles:

- **Nombre de usuario:** la cuenta de usuario que se utiliza para la sesión.
- **Dirección IP:** la dirección IP del cliente desde el que se creó la sesión.
- **Puerto:** el puerto que se utiliza para la sesión.
- **Hora de inicio de sesión:** la hora en que se creó la sesión actual en el dispositivo SDX.
- **Hora de la última actividad:** la hora en que se detectó la actividad del usuario por última vez en la sesión.
- **La sesión caduca en:** tiempo restante para que caduque la sesión.

Para ver las sesiones de los clientes, en la ficha **Configuración**, vaya a **Sistema > Sesiones**.

Para finalizar una sesión de cliente, en el panel **Sesiones**, haga clic en la sesión que quiere quitar y, a continuación, haga clic en **Finalizar sesión**.

No puede finalizar una sesión del cliente que inició esa sesión.

Configurar directivas

Para mantener el tamaño de los datos registrados dentro de los límites gestionables, el dispositivo SDX ejecuta directivas de copia de seguridad y poda de datos automáticamente en un momento determinado.

La directiva de recorte se ejecuta a las 00:00 a. m. todos los días y especifica el número de días de datos que se deben conservar en el dispositivo. De forma predeterminada, el dispositivo repasa los datos de más de 3 días, pero puede especificar el número de días de datos que quiere conservar. Solo se podan los registros de eventos, los registros de auditoría y los registros de tareas.

La directiva de seguridad se ejecuta a las 00:30 todos los días y crea una copia de seguridad de los registros y los archivos de configuración. De forma predeterminada, la directiva conserva tres copias de seguridad, pero puede especificar el número de copias de seguridad que quiere conservar. Y, mediante la directiva de copia de seguridad, puede:

- Cifra los archivos de seguridad.
- Configure el dispositivo SDX para transferir los archivos de copia de seguridad a un servidor de copia de seguridad externo mediante FTP, SFTP y SCP.

Para especificar el número de días durante los que se recortan los datos registrados:

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **Sistema**.

2. En el panel **Sistema**, en **Administración de directivas**, haga clic en **Directiva de podar**.
3. En el cuadro de diálogo **Modificar directiva de poda**, en **Datos para conservar (días)**, especifique el número de días de datos que el dispositivo debe conservar en un momento dado.
4. Haga clic en **Aceptar**.

Para configurar la directiva de copia de seguridad:

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **Sistema**.
2. En el panel **Sistema**, en **Administración de directivas**, haga clic en **Directiva de copia de seguridad**.
3. En el cuadro de diálogo **Modificar directiva de copia de seguridad**, en **Copias de seguridad anteriores** para conservar, especifique el número de copias de seguridad que el dispositivo debe conservar en un momento dado.
4. Seleccione **Cifrar archivo de copia de seguridad** para cifrar el archivo de copia de seguridad.
5. Seleccione **Transferencia externa** y haga lo siguiente para transferir el archivo de copia de seguridad a un servidor de copia de seguridad externo:
 - a) En el campo **Servidor**, introduzca el nombre de host o la dirección IP del servidor de seguridad externo.
 - b) En los campos **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña para acceder al servidor de copia de seguridad externo.
 - c) En el campo **Puerto**, introduzca el número de puerto.
 - d) En el campo **Protocolo de transferencia**, seleccione el protocolo que quiere utilizar para transferir el archivo de copia de seguridad al servidor de copia de seguridad externo.
 - e) En el campo **Ruta de directorio**, introduzca la ruta del directorio en el servidor de copia de seguridad externo donde quiere almacenar los archivos de copia de seguridad.
6. **Eliminar archivo del Servicio de administración después de la transferencia:** Seleccione si quiere eliminar el archivo de copia de seguridad del dispositivo SDX después de haber transferido el archivo de copia de seguridad al servidor de copia de seguridad externo.
7. Haga clic en **Aceptar**.

Reinicie el Servicio de administración

Puede reiniciar el Servicio de administración desde el panel **Sistema**. Reiniciar Management Service no afecta al funcionamiento de las instancias. Las instancias continúan funcionando durante el proceso de reinicio del Servicio de administración.

Para reiniciar Management Service:

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **Sistema**.
2. En el panel **Sistema**, en **Administración del sistema**, haga clic en **Reiniciar Management Service**.

Eliminar archivos del Servicio de administración

Puede eliminar cualquier archivo de compilación y documentación del Servicio de administración que no necesite del dispositivo SDX.

Para eliminar un archivo del Servicio de administración:

1. En la ficha **Configuración**, en el panel de exploración, expanda **Management Service** y, a continuación, haga clic en el archivo que quiere quitar.
2. En el panel de **detalles**, seleccione el nombre del archivo y, a continuación, haga clic en **Eliminar**.

Generar un archivo tar para asistencia técnica

Puede utilizar la opción de asistencia técnica para generar un archivo TAR de datos y estadísticas para enviarlos a la asistencia técnica de Citrix. Este tar se puede generar para Management Service o Citrix Hypervisor, o para ambos al mismo tiempo. A continuación, puede descargar el archivo en su sistema local y enviarlo a la asistencia técnica de Citrix.

En el panel **Asistencia técnica**, puede ver los siguientes detalles.

- **Nombre:** el nombre del archivo de almacenamiento tar. El nombre del archivo indica si el tar es para Management Service o para el servidor Citrix Hypervisor.
- **Última modificación:** la fecha en que este archivo se modificó por última vez.
- **Tamaño:** el tamaño del archivo tar.

Para generar el archivo TAR para asistencia técnica:

1. En la ficha **Configuración**, vaya a **Diagnósticos > Asistencia técnica**.
2. En el panel de **detalles**, en la lista **Acción**, seleccione **Generar archivo de asistencia técnica**.
3. En el cuadro de diálogo **Generar archivo de asistencia técnica**, en la lista **Modo**, seleccione la opción apropiada.
4. Haga clic en **Aceptar**.

Para descargar el archivo TAR para asistencia técnica:

1. En el panel **Asistencia técnica**, seleccione el archivo de asistencia técnica que quiere descargar.
2. En la lista **Acción**, seleccione **Descargar**. El archivo se guarda en el equipo local.

Función de CLI para Management Service

Ahora puede usar la CLI para realizar operaciones en el Servicio de administración. Se admiten las siguientes operaciones:

- Agregar, Establecer, Eliminar: Para configurar los recursos.
- Do: Para realizar operaciones a nivel del sistema. Por ejemplo, actualizar o apagar Management Service o reiniciar.
- Guardar: para agregar interfaces, que se utilizan para el aprovisionamiento.

Para acceder a la CLI, inicie el cliente de shell seguro (SSH) desde cualquier estación de trabajo conectada a la dirección IP del Servicio de administración. Inicie sesión con las credenciales de administrador.

Puede acceder a información detallada sobre el uso y la sintaxis de los comandos en las páginas de manual.

Nota: La CLI no se admite en el acceso a la consola.

Configurar los ajustes de autenticación y autorización

November 23, 2023

La autenticación con el Servicio de administración SDX de NetScaler puede ser local o externa. Con la autenticación externa, el Servicio de administración concede acceso a los usuarios en función de la respuesta de un servidor externo. Management Service admite los siguientes protocolos de autenticación externa:

- Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)
- Sistema de control de acceso de controlador de acceso de terminal (TACACS)
- Protocolo ligero de acceso a directorios (LDAP)

Management Service también admite solicitudes de autenticación de SSH. La autenticación SSH solo admite solicitudes de autenticación interactiva de teclado. La autorización de los usuarios de SSH se limita solo a los privilegios de administrador. Los usuarios con privilegios de solo lectura no pueden iniciar sesión a través de SSH.

Para configurar la autenticación, especifique el tipo de autenticación y configure un servidor de autenticación.

La autorización a través del Servicio de administración es local. Management Service admite dos niveles de autorización. Los usuarios con privilegios de administrador pueden realizar cualquier acción en Management Service. Los usuarios con privilegios de solo lectura solo pueden realizar operaciones de lectura. La autorización de los usuarios de SSH se limita solo a los privilegios de administrador. Los usuarios con privilegios de solo lectura no pueden iniciar sesión a través de SSH.

La autorización para RADIUS y LDAP es compatible con la extracción de grupos. Puede establecer los atributos de extracción de grupo durante la configuración de los servidores RADIUS o LDAP en Management Service. El nombre del grupo extraído coincide con los nombres de grupo en Management

Service para determinar los privilegios otorgados al usuario. Un usuario puede pertenecer a varios grupos. En ese caso, si algún grupo al que pertenece el usuario tiene privilegios de administrador, el usuario tiene privilegios de administrador. Se puede establecer un atributo de grupo Autenticación predeterminada durante la configuración. Este grupo se considera junto con los grupos extraídos para su autorización.

En la autorización TACACS, el administrador del servidor TACACS debe permitir un comando especial, admin para un usuario con privilegios de administrador y denegar este comando para los usuarios con privilegios de solo lectura. Cuando un usuario inicia sesión en un dispositivo SDX, el Servicio de administración comprueba si el usuario tiene permiso para ejecutar este comando. Si el usuario tiene permiso, se le asignan los privilegios de administrador; de lo contrario, se le asignan privilegios de solo lectura.

Agregar un grupo de usuarios

Los grupos son conjuntos lógicos de usuarios que necesitan acceder a información común o realizar tareas similares. Puede organizar a los usuarios en grupos definidos por un conjunto de operaciones comunes. Al proporcionar permisos específicos a grupos en lugar de a usuarios individuales, puede ahorrar tiempo al crear usuarios.

Si utiliza servidores de autenticación externos para la autenticación, los grupos de SDX se pueden configurar para que coincidan con los grupos configurados en los servidores de autenticación. Cuando un usuario que pertenece a un grupo cuyo nombre coincide con un grupo en un servidor de autenticación, inicia sesión y se autentica, el usuario hereda la configuración del grupo.

Para agregar un grupo de usuarios

1. En la ficha **Configuración**, en **Sistema**, expanda **Administración de usuarios**, a continuación, haga clic en **Grupos**.
2. En el panel de detalles, haga clic en **Agregar**.

← Create System Group

Group Name*
 ⓘ × Please enter value

Group Description

System Access

Permission*
read-write ▼ ⓘ

Configure User Session Timeout

Users

Available (2)	Select All		Configured (0)	Remove All
nsroot	+	▶	No items	
config-user	+	◀		

All Instances

Create

3. En la página **Crear grupo de sistemas**, defina los siguientes parámetros:

- Nombre del grupo
- Descripción del grupo
- Acceso al sistema: seleccione esta casilla para dar acceso a todo el dispositivo SDX y a las instancias que se ejecutan en él. Como alternativa, para el acceso a nivel de instancia, especifique las instancias en **Instances**.
- Permiso
- Configurar tiempo de espera de sesión de usuario
- Usuarios: usuarios de la base de datos que pertenecen al grupo. Seleccione los usuarios que quiere agregar al grupo.

4. Haga clic en **Crear** y **Cerrar**.

Nota: Para crear un grupo con función de administrador en un dispositivo SDX que se actualice de la versión 10.5 a la versión 11.1, seleccione la casilla de verificación “permiso de lectura y escritura” y “Acceso al sistema”. En SDX 10.5, esta casilla de verificación no está disponible y los valores de Permiso son “administrador” y “solo lectura”.

Configurar cuentas de usuario

Un usuario inicia sesión en el dispositivo SDX para realizar tareas de administración del dispositivo. Para permitir que un usuario acceda al dispositivo, debe crear una cuenta de usuario en el dispositivo SDX para ese usuario. Los usuarios se autentican localmente, en el dispositivo.

Importante: La contraseña se aplica al dispositivo SDX, Management Service y Citrix Hypervisor. No cambie la contraseña directamente en Citrix Hypervisor.

Para configurar una cuenta de usuario

1. En la ficha **Configuración**, en **Sistema**, expanda **Administración** y, a continuación, haga clic en **Usuarios**. El panel Usuarios muestra una lista de las cuentas de usuario existentes, con sus permisos.
2. En el panel **Usuarios**, lleve a cabo una de las siguientes acciones:
 - Para crear una cuenta de usuario, haga clic en **Agregar**.
 - Para modificar una cuenta de usuario, seleccione el usuario y, a continuación, haga clic en **Modificar**.
3. En el cuadro de diálogo **Crear usuariodel sistema o Modificar usuario** del sistema, defina los siguientes parámetros:
 - Nombre *: El nombre de usuario de la cuenta. Se permiten los siguientes caracteres en el nombre: Letras de la a a la z y de la A a la Z, números del 0 al 9, punto (.), espacio y guión bajo (_). Longitud máxima: 128. No se le puede cambiar el nombre.
 - Contraseña *: La contraseña para iniciar sesión en el dispositivo. Longitud máxima: 128
 - Confirmar contraseña *: La contraseña.
 - Permiso *: Privilegios del usuario en el dispositivo. Valores posibles:
 - admin: El usuario puede realizar todas las tareas de administración relacionadas con Management Service.
 - Solo lectura: El usuario solo puede supervisar el sistema y cambiar la contraseña de la cuenta.
Predeterminado: Admin.

- **Habilitar autenticación externa:** Habilita la autenticación externa para este usuario. Management Service intenta la autenticación externa antes de la autenticación del usuario de la base de datos. Si este parámetro está inhabilitado, el usuario no se autentica con el servidor de autenticación externo.

Nota: Si no se puede acceder al servidor de autenticación remota, es posible que el usuario pierda el acceso al dispositivo. En tales casos, la autenticación recurre al usuario administrador predeterminado (`nsroot`).

- **Configurar tiempo de espera de sesión:** Permite configurar el período de tiempo durante el tiempo que un usuario puede permanecer activo. Especifique los siguientes detalles:
 - **Tiempo de espera de sesión:** Período de tiempo durante cuánto tiempo puede permanecer activa una sesión de usuario.
 - **Unidad de tiempo de espera de sesión:** La unidad de tiempo de espera, en minutos u horas.
- **Grupos:** Asigna los grupos al usuario.

*Un parámetro requerido

4. Haga clic en **Crear** o en **Aceptar** y, a continuación, en **Cerrar**. El usuario que creó aparece en el panel **Usuarios**.

Para eliminar una cuenta de usuario

1. En la ficha **Configuración**, en el panel de navegación, expanda **Sistema**, expanda **Administración**, a continuación, haga clic en **Usuarios**.
2. En el panel **Usuarios**, seleccione la cuenta de usuario y, a continuación, haga clic en **Eliminar**.
3. En el cuadro **Confirmar mensaje**, haga clic en **Aceptar**.

Establecer el tipo de autenticación

Desde la interfaz del Servicio de administración, puede especificar la autenticación local o externa. La autenticación externa está inhabilitada para los usuarios locales de forma predeterminada. Se puede habilitar marcando la opción

Habilitar autenticación externa al agregar el usuario local o al modificar la configuración del usuario.

Importante: La autenticación externa solo se admite después de configurar un servidor de autenticación RADIUS, LDAP o TACACS.

Para establecer el tipo de autenticación

1. En la ficha **Configuración**, en **Sistema**, haga clic en **Autenticación**.

2. En el panel de detalles, haga clic en Configuración de autenticación.
3. Defina los siguientes parámetros:
 - Tipo de servidor: Tipo de servidor de autenticación configurado para la autenticación de usuario. Valores posibles: LDAP, RADIUS, TACACS y Local.
 - Nombre del servidor: Nombre del servidor de autenticación configurado en Management Service. El menú enumera todos los servidores configurados para el tipo de autenticación seleccionado.
 - Habilitar autenticación local de reserva: También puede elegir autenticar a un usuario con la autenticación local cuando se produce un error en la autenticación externa. Esta opción está habilitada de forma predeterminada.
4. Haga clic en Aceptar.

Habilitar o inhabilitar la autenticación básica

Puede autenticarse en la interfaz NITRO del Servicio de administración mediante la autenticación básica. De forma predeterminada, la autenticación básica está habilitada en el dispositivo SDX. Realice lo siguiente para inhabilitar la autenticación básica mediante la interfaz del Servicio de administración.

Para inhabilitar la autenticación básica

1. En la ficha **Configuración**, haga clic en **Sistema**.
2. En el grupo **Configuración del sistema**, haga clic en **Cambiar configuración del sistema**.
3. En el cuadro de diálogo Configurar configuración del sistema, desactive la casilla de verificación **Permitir autenticación básica**.
4. Haga clic en **Aceptar**.

Configuración del servidor de autenticación externo

November 23, 2023

El Servicio de administración SDX de NetScaler puede autenticar a los usuarios con cuentas de usuario locales o mediante un servidor de autenticación externo. El dispositivo admite los siguientes tipos de autenticación:

- Local: Se autentica en Management Service mediante una contraseña, sin hacer referencia a un servidor de autenticación externo. Los datos de usuario se almacenan localmente en Management Service.

- RADIUS: Se autentica en un servidor de autenticación RADIUS externo.
- LDAP: Se autentica en un servidor de autenticación LDAP externo.
- TACACS: Se autentica en un servidor de autenticación del Sistema de control de acceso de controlador de acceso de terminal externo (TACACS).

Para configurar una autenticación externa, especifique el tipo de autenticación y configure un servidor de autenticación.

Agregar un servidor RADIUS

Para configurar la autenticación RADIUS, especifique el tipo de autenticación como RADIUS y configure el servidor de autenticación RADIUS.

Management Service admite la autenticación de respuestas a desafíos RADIUS de acuerdo con las especificaciones RADIUS. Los usuarios de RADIUS se pueden configurar con una contraseña de un solo uso en el servidor RADIUS. Cuando el usuario inicia sesión en un dispositivo SDX, se le pide al usuario que especifique esta contraseña de un solo uso.

Para agregar un servidor RADIUS

1. En la ficha **Configuración**, en **Sistema**, expanda **Autenticación** y, a continuación, haga clic en **Radio**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear servidor RADIUS**, escriba o seleccione los valores de los parámetros:
 - **Nombre ***: Nombre del servidor.
 - **Nombre del servidor/Dirección IP***: nombre de dominio completo (FQDN) o dirección IP del servidor.
Nota: El DNS debe poder resolver el FQDN especificado en una dirección IP y solo se utiliza el DNS principal para resolver el FQDN. Para configurar manualmente el DNS principal, consulte la sección “Agregar un DNS principal para la resolución de nombres de FQDN”.
 - **Puerto***: puerto en el que se ejecuta el servidor RADIUS. Valor por defecto: 1812.
 - **Timeout***: número de segundos que el sistema espera una respuesta del servidor RADIUS. Valor por defecto: 3.
 - **Clave secreta ***: Clave compartida entre el cliente y el servidor. Esta información es necesaria para la comunicación entre el sistema y el servidor RADIUS.
 - **Habilitar la extracción de direcciones IP del NAS:** si está habilitada, la dirección IP del Servicio de administración se envía al servidor como `nas_ip` de acuerdo con el protocolo RADIUS.

- **NASID:** Si se configura, esta cadena se envía al servidor RADIUS como `nasid` de acuerdo con el protocolo RADIUS.
- **Prefijo de grupo:** Cadena de prefijo que precede a los nombres de grupo en un atributo RADIUS para la extracción de grupos RADIUS.
- **ID de proveedor de grupo:** identificador de proveedor para utilizar la extracción de grupos RADIUS.
- **Tipo de atributo de grupo:** Tipo de atributo para la extracción de grupos RADIUS.
- **Separador de grupos:** Cadena de separación de grupos que delimita los nombres de grupo dentro de un atributo RADIUS para la extracción de grupos RADIUS.
- **Identificador de proveedor de dirección IP:** identificador de proveedor del atributo en el RADIUS que indica la IP de la intranet. Un valor de 0 indica que el atributo no está codificado por el proveedor.
- **Tipo de atributo de dirección IP:** Tipo de atributo del atributo de dirección IP remota en una respuesta RADIUS.
- **Identificador de proveedor de contraseñas:** identificador de proveedor de la contraseña en la respuesta RADIUS. Se usa para extraer la contraseña del usuario.
- **Tipo de atributo de contraseña:** Tipo de atributo del atributo de contraseña en una respuesta RADIUS.
- **Codificación de contraseñas:** cómo se deben codificar las contraseñas en los paquetes RADIUS que viajan desde el sistema al servidor RADIUS. Valores posibles: `pap`, `chap`, `mschapv1` y `mschapv2`.
- **Grupo de autenticación predeterminado:** Grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.
- **Contabilidad:** Habilite Management Service para registrar la información de auditoría con el servidor RADIUS.

4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Agregar un servidor de autenticación LDAP

Para configurar la autenticación LDAP, especifique el tipo de autenticación como LDAP y configure el servidor de autenticación LDAP.

Para agregar un servidor LDAP

1. En la ficha **Configuración**, en **Sistema**, expanda **Autenticación** y, a continuación, haga clic en **LDAP**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear servidor LDAP**, escriba o seleccione los valores de los parámetros:

- Nombre *: Nombre del servidor.
- Nombre del servidor/Dirección IP*: FQDN o dirección IP del servidor.
Nota: El DNS debe poder resolver el FQDN especificado en una dirección IP y solo se utiliza el DNS principal para resolver el FQDN. Para configurar manualmente el DNS principal, consulte la sección “Agregar un DNS principal para la resolución de nombres de FQDN”.
- **Puerto***: puerto en el que se ejecuta el servidor LDAP. Valor por defecto: 389.
- Timeout*: número de segundos que el sistema espera una respuesta del servidor LDAP.
- DN base: base o nodo en el que debe iniciarse la búsqueda LDAP.
- Tipo: Tipo de servidor LDAP. Valores posibles: Active Directory (AD) y Novell Directory Service (NDS).
- DN de enlace administrativo: Nombre completo que se utiliza para enlazar con el servidor LDAP.
- Contraseña administrativa: Contraseña que se utiliza para enlazar con el servidor LDAP.
- Validar certificado LDAP: marque esta opción para validar el certificado recibido del servidor LDAP.
- Nombre de host LDAP: nombre de host para el servidor LDAP. Si el parámetro validate-ServerCert está habilitado, este parámetro especifica el nombre de host en el certificado del servidor LDAP. Una discrepancia en el nombre de host provoca un error de conexión.
- Atributo de nombre de inicio de sesión de servidor: Atributo de nombre utilizado por el sistema para consultar el servidor LDAP externo o un Active Directory.
- Filtro de búsqueda: Cadena que se va a combinar con la cadena de búsqueda de usuario LDAP predeterminada para formar el valor. Por ejemplo, vpnallowed=true con ldaplogi-name samaccount y el nombre de usuario proporcionado por el usuario bob generaría una cadena de búsqueda LDAP de: (&(vpnallowed=true)(samaccount=bob).
- Atributo de grupo: Nombre de atributo para la extracción de grupo desde el servidor LDAP.
- Nombre de subatributo: Nombre de subatributo para la extracción de grupos desde el servidor LDAP.
- Tipo de seguridad: Tipo de cifrado para la comunicación entre el dispositivo y el servidor de autenticación. Valores posibles:
PLAINTEXT: No se requiere cifrado.
TLS: Se comunica con el protocolo TLS.
SSL: Se comunica con el protocolo SSL
- Grupo de autenticación predeterminado: Grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.
- Referencias: Habilite el siguiente de las referencias LDAP recibidas desde el servidor LDAP.
- Número máximo de referencias LDAP: Número máximo de referencias LDAP a seguir.

- **Habilitar cambio de contraseña:** permite al usuario modificar la contraseña si la contraseña caduca. Puede cambiar la contraseña solo cuando el tipo de seguridad configurado es TLS o SSL.
- **Habilitar extracción de grupos anidados:** Permite habilitar la función de extracción de grupos anidados.
- **Nivel máximo de anidamiento:** Número de niveles en los que se permite la extracción de grupos.
- **Identificador de nombre de grupo:** nombre que identifica de forma exclusiva un grupo en el servidor LDAP.
- **Atributo de búsqueda de grupos:** Atributo de búsqueda de grupos LDAP. Se utiliza para determinar a qué grupos pertenece un grupo.
- **Subatributo de búsqueda de grupos:** Subatributo de búsqueda de grupos LDAP. Se utiliza para determinar a qué grupos pertenece un grupo.
- **Filtro de búsqueda de grupos:** Cadena que se va a combinar con la cadena de búsqueda de grupos LDAP predeterminada para formar el valor de búsqueda.

4. Haga clic en Crear y, a continuación, en Cerrar.

Compatibilidad con autenticación de clave pública SSH para usuarios de LDAP

El dispositivo SDX ahora puede autenticar a los usuarios LDAP a través de la autenticación de clave pública SSH para el inicio de sesión. La lista de claves públicas se almacena en el objeto de usuario en el servidor LDAP. Durante la autenticación, SSH extrae las claves públicas SSH del servidor LDAP. El inicio de sesión se realiza correctamente si alguna de las claves públicas recuperadas admite SSH.

El mismo nombre de atributo de la clave pública extraída debe estar presente tanto en el servidor LDAP como en el dispositivo NetScaler SDX.

Importante

Para la autenticación basada en claves, debe especificar una ubicación de las claves públicas estableciendo el valor de `Authorizedkeyfile` en el archivo `/etc/sshd_config` en el siguiente aspecto:

```
AuthorizedKeysFile .ssh/authorized_keys
```

Usuario del sistema. Puede especificar la ubicación de las claves públicas para cualquier usuario del sistema estableciendo el valor de `Authorizedkeyfile` en el archivo `/etc/sshd_config*`.

Usuarios de LDAP. La clave pública recuperada se almacena en el directorio `/var/pubkey/<user_name>/tmp_authorized_keys-<pid>`. `pid` es el número único agregado para diferenciar entre solicitudes SSH simultáneas del mismo usuario. Esta ubicación es una ubicación

temporal para mantener la clave pública durante el proceso de autenticación. La clave pública se elimina del sistema una vez que se completa la autenticación.

Para iniciar sesión con el usuario, ejecute el siguiente comando desde el símbolo del shell:

```
$ ssh -i <private key> <username>@<IPAddress>
```

Para configurar el servidor LDAP mediante la GUI:

1. Vaya a **Sistema > Autenticación > LDAP**.
2. En la página LDAP, haga clic en la ficha ****Servidores****.
3. Haga clic en cualquiera de los servidores LDAP disponibles.
4. En la página **Configurar servidor LDAP de autenticación**, seleccione **Autenticación**.

Nota:

Desmarque la casilla Autenticación para utilizar “sshPublicKeys” para la autenticación de los usuarios LDAP.

Agregar un DNS principal para la resolución de nombres de FQDN

Si define un servidor RADIUS o LDAP mediante el FQDN del servidor en lugar de su dirección IP, configure manualmente el DNS principal para resolver el nombre del servidor. Puede usar la GUI o la CLI.

Para configurar el DNS principal mediante la GUI, vaya a **Sistema > Configuración de red > DNS**.

Para configurar el DNS principal mediante la CLI, siga estos pasos.

1. Abra una consola Secure Shell (SSH).
2. Inicie sesión en el dispositivo NetScaler SDX mediante las credenciales de administrador.
3. Ejecute el comando `networkconfig`.
4. Seleccione el menú apropiado y actualice la dirección IPv4 de DNS y guarde los cambios.

Si vuelve a ejecutar el comando `networkconfig`, verá la dirección DNS actualizada.

Agregar un servidor TACACS

Para configurar la autenticación TACACS, especifique el tipo de autenticación como TACACS y configure el servidor de autenticación TACACS.

Para agregar un servidor TACACS

1. En la ficha **Configuración**, en **Sistema**, expanda **Autenticación** y, a continuación, haga clic en **TACACS**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo Crear servidor TACACS, escriba o seleccione los valores de los parámetros:
 - Nombre: nombre del servidor TACAS
 - Dirección IP: Dirección IP del servidor TACACS
 - Puerto: Puerto en el que se ejecuta el servidor TACACS. Valor por defecto: 49
 - Tiempo de espera: número máximo de segundos que el sistema espera una respuesta del servidor TACACS
 - Clave TACACS: Clave compartida entre el cliente y el servidor. Esta información es necesaria para que el sistema se comuniquen con el servidor TACACS
 - Contabilidad: Permite que Management Service registre la información de auditoría con el servidor TACACS
 - Nombre de atributo de grupo: Nombre del atributo de grupo configurado en el servidor TACACS+

← Create TACACS Server

Name* ⓘ

IP Address*

Port*

Time-out (seconds)*

TACACS Key*

Confirm TACACS Key* ⓘ

Group Attribute Name

Accounting

4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Configurar la agregación de enlaces desde el Servicio de administración

November 23, 2023

La agregación de enlaces combina varios enlaces Ethernet en un solo enlace de alta velocidad. La configuración de la agregación de enlaces aumenta la capacidad y la disponibilidad del canal de comunicación entre el dispositivo NetScaler SDX y otros dispositivos conectados. Un enlace agregado también se conoce como un “canal”.

Cuando una interfaz de red está enlazada a un canal, los parámetros del canal tienen prioridad sobre los parámetros de la interfaz de red (es decir, los parámetros de la interfaz de red se ignoran). Una interfaz de red solo puede enlazarse a un canal.

Cuando una interfaz de red está enlazada a un canal, descarta su configuración de VLAN. La interfaz se elimina de la VLAN a la que pertenecía originalmente y se agrega a la VLAN predeterminada. Sin

embargo, puede volver a vincular el canal a la VLAN anterior o a una nueva. Por ejemplo, si vincula las interfaces de red 1/2 y 1/3 a una VLAN con ID 2 (VLAN 2) y, a continuación, las vincula al canal LA/1, las interfaces de red se mueven a la VLAN predeterminada, pero puede vincular el canal a la VLAN 2.

Nota:

- Una interfaz debe formar parte de un solo canal.
- Se requieren un mínimo de dos interfaces para configurar un canal.
- Las interfaces que forman parte de un canal no se enumeran en la vista Configuración de red cuando se agrega o modifica una instancia de NetScaler. En lugar de las interfaces, se enumeran los canales.

Si configura un canal mediante tres interfaces asignadas a una instancia y una segunda instancia utiliza algunas de estas interfaces, Management Service cierra la segunda instancia, modifica la configuración de red y reinicia la instancia. Por ejemplo, supongamos que hay dos instancias, Instance1 e Instance2. Cuando se aprovisionan estas instancias, las interfaces 10/1, 10/2 y 10/3 se asignan a la Instancia1, y las interfaces 10/1 y 10/2 se asignan a la Instancia2. Si se crea un canal LA con las interfaces 10/1, 10/2 y 10/3, instance1 no se reinicia. Sin embargo, el Servicio de administración cierra Instance2, asigna la interfaz 10/3 a Instance2 y, a continuación, reinicia Instance2.

Si elimina una interfaz de un canal LA, los cambios se almacenan en la base de datos y la interfaz aparece en la vista Configuración de red cuando agrega o modifica una instancia. Antes de eliminar la interfaz, solo se muestra el canal del que forma parte la interfaz.

Configuración de un canal desde el Servicio de administración

November 23, 2023

Puede configurar un canal manualmente o puede usar el Protocolo de control de agregación de enlaces (LACP). No puede aplicar LACP a un canal configurado manualmente, ni puede configurar manualmente un canal creado por LACP. Configure un canal desde el Servicio de administración. A continuación, seleccione el canal en el momento de aprovisionar o modificar una instancia de NetScaler.

Un canal LA es una entidad lógica para proporcionar redundancia de enlaces y agregación de ancho de banda. A las interfaces que forman parte de un canal no se les pueden asignar direcciones IP separadas.

Nota: Un dispositivo NetScaler SDX admite la agregación de enlaces, pero no admite la redundancia de enlaces. A partir de la versión 13.1, compilación 27.x y posteriores de NetScaler, la configuración de redundancia de enlaces no se admite explícitamente en una instancia de NetScaler VPX alojada en un dispositivo NetScaler SDX.

Para configurar un canal desde el Servicio de administración

1. Vaya a **Sistema > Canales**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar canal**, defina los siguientes parámetros:
 - ID de canal: ID del canal LA que se va a crear. Especifique un canal LA en notación LA/x, donde x puede oscilar entre 1 y un número igual a la mitad del número de interfaces. No se puede cambiar después de crear el canal LA.
 - Tipo: Tipo de canal. Valores posibles:
 - Estático: Configurado solo en las interfaces de datos.
 - Activo-Activo: Configurado solo en las interfaces de administración 0/x.
 - Activo-Pasivo: Configurado solo en las interfaces de administración 0/x.
 - LACP: configurado en las interfaces de datos y las interfaces de administración 0/x.
 - Rendimiento (solo se aplica a un canal estático y LACP): Valor de umbral bajo para el rendimiento del canal LA, en Mbps. En una configuración de HA, la conmutación por error se desencadena si el canal LA tiene activado HA MON y el rendimiento está por debajo del umbral especificado.
 - Ancho de banda alto (solo se aplica a un canal estático y LACP): Valor de umbral alto para el uso del ancho de banda del canal LA, en Mbps. El dispositivo genera un mensaje de captura SNMP cuando el uso del ancho de banda del canal LA es igual o mayor que el valor de umbral alto especificado.
 - Ancho de banda normal (solo se aplica a un canal estático y LACP): Valor de umbral normal para el uso del ancho de banda del canal LA, en Mbps. Cuando el uso del ancho de banda del canal LA pasa a ser igual o inferior al umbral normal especificado tras superar el umbral alto, el dispositivo NetScaler SDX genera un mensaje de captura SNMP para indicar que el uso del ancho de banda ha vuelto a la normalidad.
4. En la ficha **Interfaces**, agregue las interfaces que quiere incluir en este canal.
5. En la ficha **Configuración**, defina los siguientes parámetros:
 - Estado del canal (solo se aplica a un canal estático): Habilite o inhabilite el canal LA.
 - Tiempo LACP (solo se aplica a LACP): Tiempo después del cual un enlace no se agrega si el enlace no recibe una LACPDU. El valor debe coincidir en todos los puertos que participan en la agregación de enlaces en el dispositivo SDX y el nodo asociado.
 - Supervisión de alta disponibilidad: En una configuración de alta disponibilidad (HA), supervise el canal para detectar eventos de error. El fallo de cualquier canal LA que tenga habilitado HA MON desencadena la conmutación por error de HA.
 - Etiquetar todo: Agregue una etiqueta 802.1q de cuatro bytes a cada paquete enviado en este canal. La configuración ON aplica etiquetas para todas las VLAN que están enlazadas a este canal. OFF aplica la etiqueta para todas las VLAN que no sean la VLAN nativa.

- Nombre de alias: Nombre de alias para el canal LA. Se utiliza solo para mejorar la legibilidad. Para realizar cualquier operación, debe especificar el ID del canal LA.

6. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Notas

- No puede crear una LA de administración si las interfaces 0/1 y 0/2 forman parte de una instancia VPX y esa instancia forma parte de un clúster.
- No puede eliminar una LA de administración si forma parte de una instancia VPX y esa instancia forma parte de un clúster.

Listas de control de acceso

February 15, 2024

Una lista de control de acceso (ACL) es un conjunto de condiciones que puede aplicar a un dispositivo de red para filtrar el tráfico IP y proteger su dispositivo del acceso no autorizado.

Puede configurar una ACL en la GUI de NetScaler SDX Management Service para limitar y controlar el acceso al dispositivo.

Nota:

Las ACL de los dispositivos SDX se admiten desde la versión 12.0 57.19 en adelante.

Este tema incluye las siguientes secciones:

- Directrices de uso
- Cómo configurar las ACL
- Otras acciones para las reglas de ACL
- Solución de problemas

Directrices de uso

Tenga en cuenta los siguientes puntos al crear ACL en su dispositivo:

- Al actualizar el dispositivo SDX a la versión 11.0 57.19, la función ACL se inhabilita de forma predeterminada.
- Los administradores de SDX solo pueden controlar los paquetes entrantes a través de ACL en el dispositivo SDX.

- Si utiliza NetScaler Application Delivery Management para administrar su dispositivo SDX, debe crear las reglas de ACL adecuadas para permitir la comunicación entre MAS y el Servicio de administración de SDX.
- Cualquier otra configuración en el dispositivo SDX, como aprovisionar o eliminar VPX, agregar/eliminar servidores externos, administración SNMP, no requiere ningún cambio en la configuración de ACL existente. El Servicio de Gestión se encarga de la comunicación con estas entidades.

Cómo configurar una ACL

La configuración de una ACL implica los siguientes pasos:

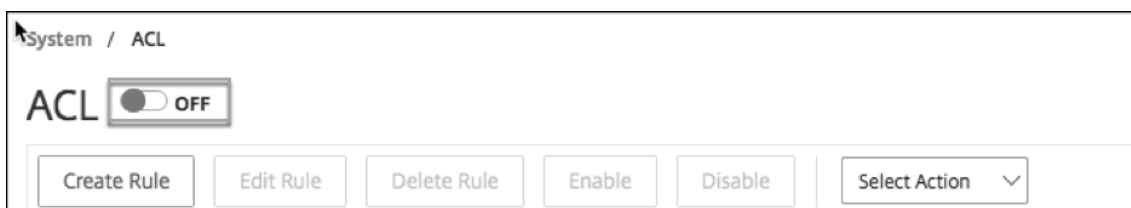
- Habilitar la función ACL
- Crear una regla de ACL
- Habilitar la regla de ACL

Nota:

Puede crear reglas de ACL sin habilitar la función de ACL. Sin embargo, si la función no está habilitada, no podrá habilitar una regla de ACL después de haberla creado.

Habilitar la función ACL

1. Para habilitar la función ACL, inicie sesión en la GUI de SDX Management Service y vaya a **Configuración > Sistema > ACL**.
2. Mediante el botón de alternancia, active la función ACL.



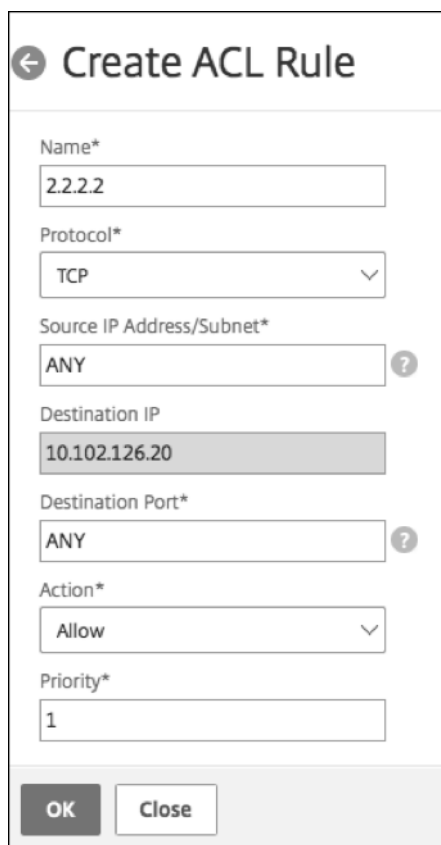
Crear una regla de ACL

1. En la página ACL, haga clic en **Crear regla**.
2. Se abre la ventana **Crear regla**. Agregue los detalles que se indican en la siguiente tabla.

Propiedad	Descripción
Nombre	Agregue un nombre.
Protocolo	Selecciona un protocolo en el menú. De forma predeterminada, se selecciona TCP. Puede seleccionar CUALQUIERA para permitir todos los protocolos.
Dirección IP de origen/subred	Especifique la dirección IP de origen o la subred de origen a la que se aplica la regla. Seleccione CUALQUIERA si la regla debe aplicarse a todo el tráfico entrante.
IP de destino	La dirección IP de SDX Management Service se rellena automáticamente como la IP de destino. Este campo no se puede modificar.
Puerto de destino	Especifique el puerto de destino al que se aplica la regla. Seleccione CUALQUIERA si la regla se aplica a todos los puertos de destino.
Acción	Seleccione la acción de la regla, que es Permitir o Denegar.
Prioridad	Asigne prioridad para especificar el orden en que se evaluará la regla. Los números de prioridad determinan el orden en que las reglas de ACL se comparan con un paquete entrante. Un número de prioridad más baja tiene una prioridad más alta. Por ejemplo, el número de prioridad 1 tiene una prioridad más alta que el número de prioridad 1. Si ninguna de las reglas coincide con el paquete entrante, el paquete se bloquea.

3. Haga clic en **Aceptar** para crear la regla.

Ilustración: Ejemplo de regla de ACL



Create ACL Rule

Name*
2.2.2.2

Protocol*
TCP

Source IP Address/Subnet*
ANY

Destination IP
10.102.126.20

Destination Port*
ANY

Action*
Allow

Priority*
1

OK Close

Una vez creada la regla, se encuentra en estado inhabilitado. Para que la regla sea efectiva, debe habilitarla.

Nota:

Para habilitar una regla, la función de ACL debe estar habilitada. Si la función está inhabilitada e intenta habilitar una regla de ACL, aparece el mensaje “ACL no se está ejecutando”.

Habilitar una regla de ACL

1. Pase el cursor sobre la regla que quiera habilitar y haga clic en el círculo con tres puntos.
2. En el menú, selecciona **Habilitar**.
3. Como alternativa, seleccione el botón de opción para esa regla y haga clic en la ficha **Habilitar**.
4. Cuando se le solicite, haga clic en **Sí** para confirmar.

Otras acciones para las reglas de ACL

Puede aplicar las siguientes acciones a las reglas de ACL:

1. Inhabilitar una regla ACL
2. Modificar una regla de ACL
3. Eliminar una regla de ACL
4. Renumerar la prioridad de las reglas de ACL

Inhabilitar una regla ACL

1. Pase el cursor sobre la regla que quiere inhabilitar y seleccione el círculo con tres puntos.
2. Haga clic en **Inhabilitar** en la lista.
3. Como alternativa, seleccione el botón de opción para esa regla y haga clic en la ficha **Inhabilitar**.
4. Haga clic en **Sí** para confirmar.

Nota:

Al inhabilitar una regla, la regla ya no se aplica al tráfico entrante. Sin embargo, la configuración de reglas permanece en la configuración de ACL.

Modificar una regla de ACL

1. Pase el cursor sobre la regla que quiera modificar y seleccione el círculo con tres puntos.
2. Haga clic en **Modificar regla** en la lista. Se abrirá la ventana **Modificar regla**.
3. Como alternativa, seleccione el botón de opción para esa regla y haga clic en la ficha **Modificar regla**. Se abre la ventana **Modificar regla**.
4. Realice los cambios y haga clic en **Aceptar**.

Nota:

Puede modificar una regla en estado habilitado e inhabilitado. Si modifica una regla que ya está habilitada, las modificaciones se aplicarán inmediatamente. Para una regla en estado inhabilitado, las modificaciones se aplican cuando se habilita la regla.

Eliminar una regla de ACL

1. Asegúrese de que la regla esté en estado inhabilitado.
2. Pase el cursor sobre la regla que quiera eliminar y seleccione el círculo con tres puntos. Haga clic en **Eliminar regla** en la lista.

3. Como alternativa, seleccione el botón de opción para esa regla y haga clic en la ficha **Eliminar regla**.
4. Haga clic en **Sí** para confirmar.

Nota:

No se puede eliminar una regla en el estado habilitado.

Renumerar las prioridades de las reglas de ACL

1. Pase el cursor sobre la regla para la que quiere volver a numerar las prioridades y seleccione el círculo con tres puntos. Haga clic en **Renumerar prioridades** en la lista.
2. Como alternativa, seleccione el botón de opción para esa regla y haga clic en la ficha **Seleccionar acción**.
3. Seleccione **Renumerar prioridades**.
4. El Servicio de administración de SDX asigna automáticamente nuevos números de prioridad, que son múltiplos de 10, a todas las reglas existentes.
5. Modifique las reglas para asignar números de prioridad según su requisito. Consulte la sección “Para modificar una regla ACL” para obtener más información sobre cómo modificar una regla.

Figura. Un ejemplo de números de prioridad existentes

<input type="checkbox"/>	Priority ↑	Name	Source IP Address/Subnet
<input type="checkbox"/>	1	2.2.2.2	ANY
<input type="checkbox"/>	2	test1	1.1.1.1
<input type="checkbox"/>	3	test2	ANY

Figura. Un ejemplo de números de prioridad en múltiplos de 10, después de que se renumeran las prioridades

<input type="checkbox"/>	Priority ↑	Name	Source IP Address/Subnet
<input type="checkbox"/>	10	2.2.2.2	ANY
<input type="checkbox"/>	20	test1	1.1.1.1
<input type="checkbox"/>	30	test2	ANY

Solución de problemas

Si las reglas de ACL no se configuran correctamente, se puede denegar el acceso a todas las cuentas de usuario. Si pierde sin darse cuenta todo el acceso a la red a SDX Management Service debido a una configuración de ACL incorrecta, siga estos pasos para obtener acceso.

1. Inicie sesión en la dirección IP de administración de Citrix Hypervisor mediante SSH y su cuenta “root”.
2. Inicie sesión en la consola de la máquina virtual del Servicio de administración con los privilegios de administrador.
3. Ejecute el comando `pfctl -d`.
4. Inicie sesión en Management Service a través de la GUI y vuelva a configurar la ACL en consecuencia.

Configure un clúster de instancias de NetScaler

November 23, 2023

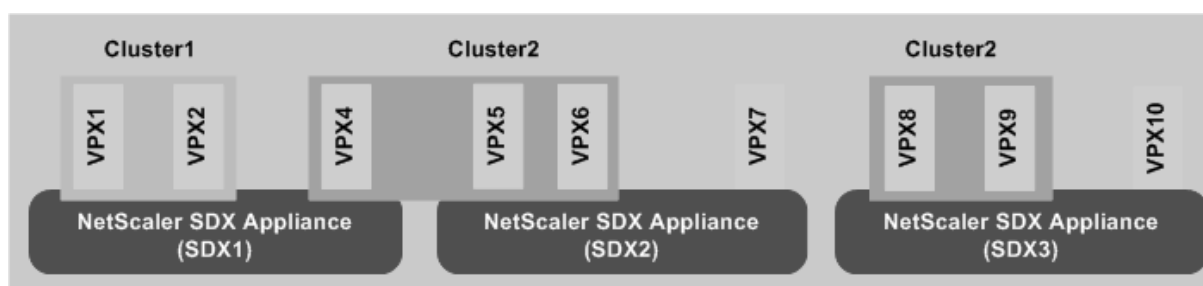
Tras aprovisionar instancias de NetScaler en uno o más dispositivos SDX, puede crear un clúster de instancias de NetScaler.

Citrix recomienda realizar la configuración del clúster desde el Servicio de administración. Cuando realiza la configuración del clúster desde una instancia VPX, el Servicio de administración aprende sobre la configuración durante el descubrimiento automático cada 30 minutos. En el peor de los casos, la información de agrupación en clústeres no se descubre durante 30 minutos. Si bien el clúster puede funcionar correctamente, se omiten algunas comprobaciones de validación esenciales para las dependencias del clúster. El Servicio de administración realiza estas comprobaciones antes de configurar el clúster en las instancias de ADC. Por lo tanto, debe realizar cualquier configuración de clúster desde el Servicio de administración.

Nota:

- Para configurar un clúster, debe entender los clústeres de NetScaler. Para obtener más información, consulte [Agrupamiento](#).
- Para los clústeres que tienen instancias de NetScaler en todos los dispositivos SDX, Citrix recomienda utilizar instancias de NetScaler de tres dispositivos SDX. Este proceso garantiza que siempre se cumplan los criterios de clúster de un mínimo de nodos ($n/2 + 1$).

Figura 1. Clúster de instancias de NetScaler de SDX



La ilustración anterior muestra tres dispositivos SDX, SDX1, SDX2 y SDX3, en la misma subred. Las instancias de NetScaler de estos dispositivos se utilizan para formar dos clústeres: Cluster1 y Cluster2.

- El clúster 1 incluye dos instancias en SDX1.
- El clúster 2 incluye una instancia en SDX1, dos instancias en SDX2 y otras dos instancias en SDX3.

Puntos que tener en cuenta

- La formación de CLAG con interfaces Mellanox (50G y 100G) no se admite en una plataforma SDX.
- Todos los nodos de un clúster deben ser del mismo tipo. No se puede formar un clúster con las siguientes combinaciones:
 - Hardware y dispositivos virtuales.
 - Instancias de NetScaler VPX e instancias de NetScaler SDX.
 - Instancias ADC en diferentes plataformas de hardware SDX.
- Las instancias de NetScaler deben ser de la misma versión, que debe ser la versión 10.1 o posterior.
- Todas las instancias de NetScaler deben tener la misma licencia de funciones.
- No se puede actualizar ninguna configuración en instancias individuales de NetScaler después de agregarlas al clúster. Todos los cambios se deben realizar a través de la dirección IP del clúster.
- Todas las instancias de NetScaler deben tener los mismos recursos (memoria, CPU, interfaces, etc.).
- La MTU del plano posterior debe tener 78 bytes más que la MTU de la interfaz de datos.
- Asegúrese de que cualquier MTU de interfaz de datos esté dentro de los 9138 bytes.
- A partir de la versión 13.0 compilación 82.x, se le solicitará que agregue una dirección SNIP mientras agrega un nodo a un clúster. También puede crear direcciones SNIP de forma dinámica mientras agrega un nodo. Esta función ayuda a abordar los problemas de seguridad en la verificación estricta de la dirección IP de origen.
- **Importante.** Use la opción **Eliminar clúster** con precaución. Al hacer clic en **Eliminar clúster**, el clúster se elimina sin ningún aviso.

Configurar un clúster en un dispositivo SDX

1. Inicie sesión en el dispositivo SDX.
2. En la ficha **Configuración**, vaya a **NetScaler > Clústeres > Instancias de clúster**.
3. Cree el clúster:
 - a) Haga clic en **Crear clúster**.
 - b) En el cuadro de diálogo **Crear clúster**, defina los parámetros requeridos para el clúster. Para ver la descripción de un parámetro, coloque el cursor del ratón sobre el campo correspondiente.
 - c) Haga clic en **Siguiente** para ver el resumen de la configuración.
 - d) Haga clic en **Finalizar** para crear el clúster.

Nota: Cuando se agrega al clúster una instancia de NetScaler con una VLAN de nivel 2 configurada, el comando `add VLAN` se guarda con el `sdxvlan` parámetro establecido en Sí. Este parámetro es un argumento interno y se utiliza para evitar la pérdida de conectividad durante la formación de clústeres SDX.
4. Agregue nodos al clúster:
 - a) Haga clic en **Agregar nodo**.
 - b) En el cuadro de diálogo **Agregar nodo**, configure los parámetros necesarios para agregar un nodo de clúster. Para obtener una descripción de un parámetro, coloque el cursor del cursor sobre el campo correspondiente.
 - c) Haga clic en **Siguiente** para ver el resumen de la configuración.
 - d) Haga clic en **Finalizar** para agregar el nodo al clúster.
 - e) Repita los pasos 1 a 4 para agregar otro nodo al clúster.

Después de crear el clúster, debe configurarlo accediendo a él a través de la dirección IP del clúster.

Si los nodos de una instancia de clúster pertenecen al mismo dispositivo Citrix NetScaler SDX, es posible que perdamos el quórum si se produce un error en un dispositivo NetScaler SDX.

Puede implementar un nodo de clúster mediante los siguientes métodos:

1. Cree varias instancias de clúster con una instancia VPX de cada dispositivo NetScaler SDX.

Ejemplo:

SDX1	SDX2	InstanceID
VPX1	VPX1	1

SDX1	SDX2	InstanceID
VPX2	VPX2	2

1. Si hay más de dos dispositivos NetScaler SDX, cree una única instancia de clúster con instancias VPX de todos los dispositivos con. `quorumType Majority` En este caso, asegúrese de que las instancias VPX estén distribuidas equitativamente en todos los dispositivos NetScaler SDX.

Ejemplo 1:

SDX1	SDX2	SDX3	InstanceID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	NA
VPX3	VPX3	VPX3	NA

Ejemplo 2:

SDX1	SDX2	SDX3	InstanceID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	NA
VPX3	VPX3	VPX3	NA
VPX4	NA	NA	NA

1. Cree una única instancia de clúster con todas las instancias VPX de todos los dispositivos NetScaler SDX. Pero usa `quorum type NONE`. Esto tiene algunas limitaciones.

Ejemplo:

SDX1	SDX2	InstanceID
VPX1	VPX1	1
VPX2	VPX2	2
VPX3	NA	NA

Limitaciones cuando el parámetro `-quorumType` se establece en `NONE`:

- Las topologías deben tener enlaces redundantes entre los nodos del clúster para evitar la partición de la red debido a un único punto de error.
- El clúster puede volverse inestable durante cualquier operación de clúster, como la adición o eliminación de nodos.

Nota:

Para obtener una lista actualizada de los clústeres de NetScaler, cada uno de los cuales tiene al menos una instancia de NetScaler del dispositivo SDX, utilice la opción **Redescubrir**.

Agregue una instancia de NetScaler que exista en un dispositivo SDX a un clúster configurado en otro dispositivo SDX

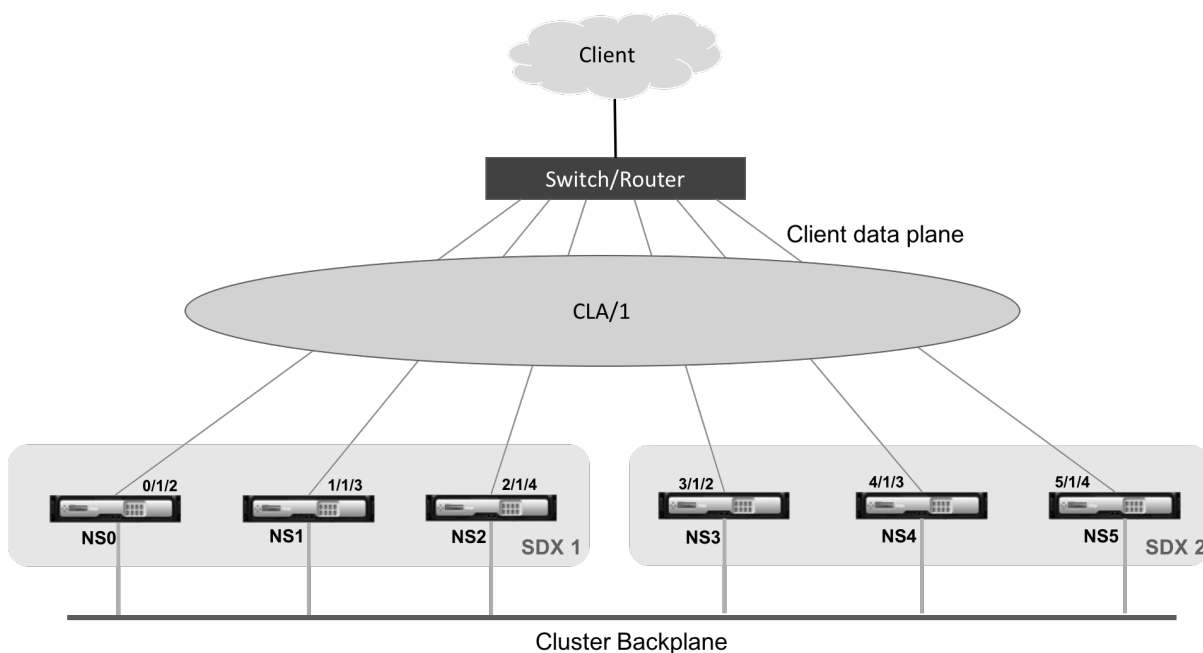
1. Inicie sesión en el dispositivo SDX desde el que desea agregar la instancia de NetScaler.
2. En la ficha **Configuración**, vaya a **NetScaler** y, a continuación, haga clic en **Clústeres**.
3. Haga clic en **Agregar nodo**.
4. En el cuadro de diálogo **Agregar nodo**, configure los parámetros necesarios para agregar un nodo de clúster. Para obtener una descripción de un parámetro, coloque el cursor del cursor sobre el campo correspondiente.
Nota: Asegúrese de que los valores de los parámetros Dirección IP del clúster y Contraseña IP del clúster corresponden al clúster al que quiere agregar el nodo.
5. Haga clic en **Siguiente** para ver el resumen de la configuración.
6. Haga clic en **Finalizar** para agregar el nodo al clúster.

Configurar la agregación de enlaces de clúster

February 15, 2024

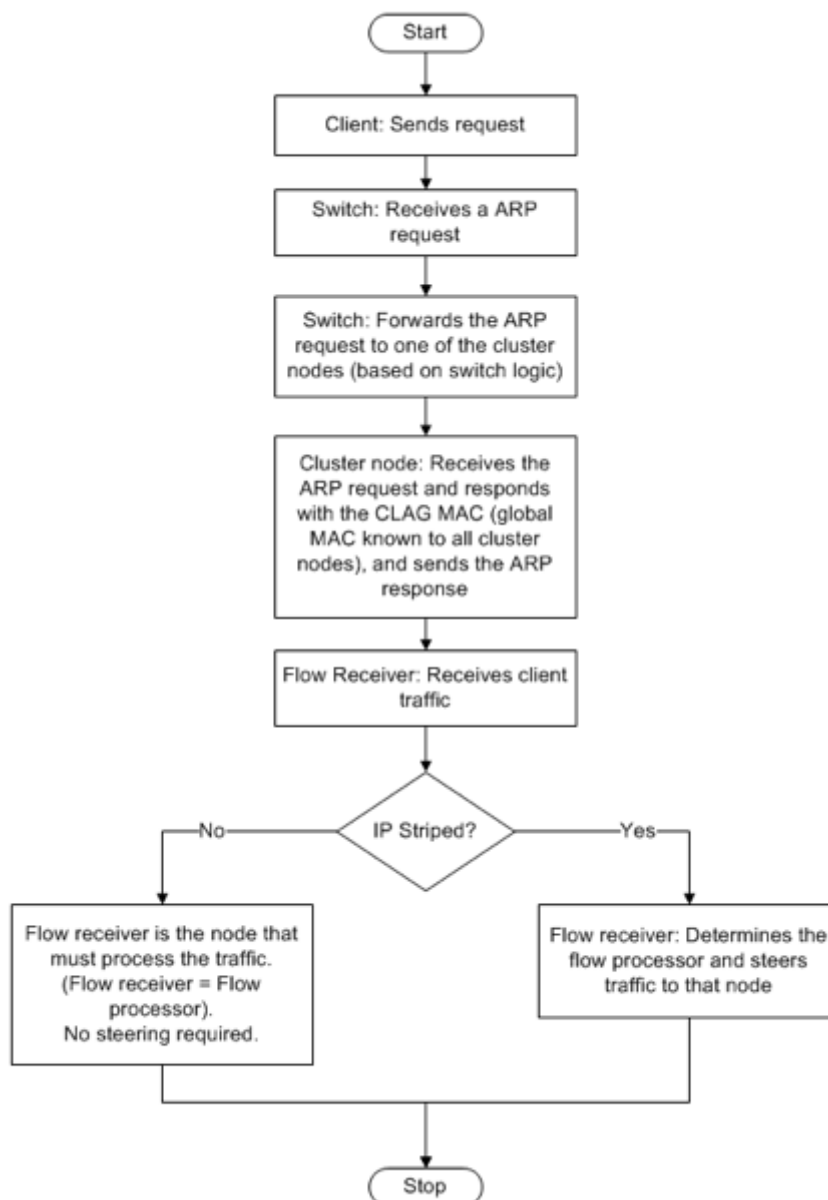
La agregación de enlaces de clúster, como su nombre indica, combina un grupo de interfaces de nodo de clúster en un canal. Es una extensión de la agregación de enlaces (LA) de NetScaler. La única diferencia es que, si bien la agregación de enlaces requiere que las interfaces estén en el mismo dispositivo, en la agregación de enlaces de clúster, las interfaces están en nodos diferentes del clúster. Para obtener más información sobre la agregación de enlaces, consulte [Configuración de la agregación de enlaces](#).

Por ejemplo, imagine un clúster de seis nodos, en dos dispositivos SDX, en el que los seis nodos están conectados a un conmutador ascendente. Un canal LA de grupo (CLA/1) se forma mediante interfaces de unión 0/1/2, 1/1/3, 2/1/4, 3/1/2, 4/1/3 y 5/1/4.



Un canal LA de clúster tiene los siguientes atributos:

- Cada canal tiene una dirección MAC única acordada por los nodos del clúster.
- El canal puede enlazar interfaces de nodos SDX locales y remotos.
- Se admite un máximo de cuatro canales LA de clúster en un clúster.
- Se puede enlazar un máximo de 16 interfaces a cada canal LA del clúster.
- Las interfaces de placa posterior no pueden formar parte de un canal LA del clúster.
- Cuando una interfaz está enlazada a un canal LA del clúster, los parámetros del canal tienen prioridad sobre los parámetros de la interfaz de red.
- Una interfaz de red puede estar vinculada a un solo canal.
- No configure el acceso de administración a un nodo de clúster en un canal LA de clúster (por ejemplo, CLA/1) o sus interfaces miembro. Cuando el nodo está INACTIVO, la interfaz LA del clúster correspondiente se marca como APAGADO, lo que hace que pierda el acceso de administración.



Implemente configuraciones similares en la dirección IP del clúster y en el dispositivo de conexión externo. Si es posible, configure el conmutador ascendente para que distribuya el tráfico en función de la dirección IP o el puerto en lugar de en la dirección MAC.

Puntos que tener en cuenta:

- Habilite LACP (especificando el modo LACP como ACTIVO o PASIVO).
Nota: Asegúrese de que el modo LACP no esté configurado como PASIVO tanto en el clúster de NetScaler como en el dispositivo de conexión externo.
- Para crear un canal LA de clúster, la clave LACP puede tener un valor de 5 a 8. Estas claves LACP se asignan a CLA/1, CLA/2, CLA/3 y CLA/4.

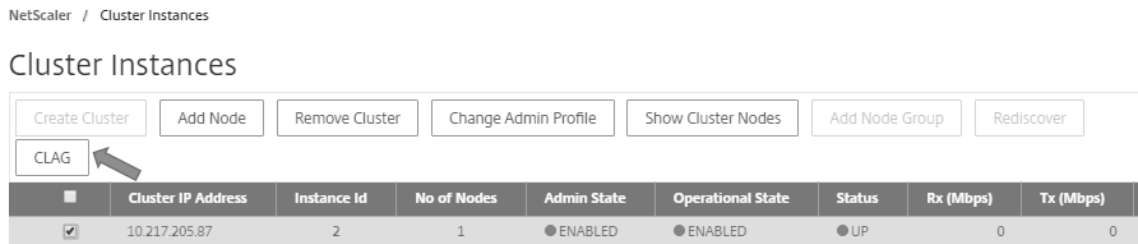
- En el dispositivo SDX, las interfaces miembro del grupo de agregación de enlaces de clúster (CLAG) no se pueden compartir con otras máquinas virtuales.
- En el conmutador ascendente, establezca el tiempo de espera de LACP en “corto” para evitar agujeros negros de tráfico de larga duración en los nodos del clúster. Esta configuración es útil cuando el switch ascendente no recibe notificación del apagado del CLAG y sus interfaces miembro hasta después del tiempo de espera de LACP.

Requisitos previos:

Cree un clúster de instancias de NetScaler. Los nodos del clúster pueden ser instancias de NetScaler en el mismo dispositivo SDX o en otros dispositivos SDX que estén disponibles en la misma subred.

Para configurar un canal de LA de clúster mediante Management Service:

1. Inicie sesión en el dispositivo SDX.
2. En la ficha **Configuración**, vaya a **NetScaler ADC** y, a continuación, haga clic en **Clusters**.
3. En la página **Instancias de Cluster**, seleccione el clúster y haga clic en **CLAG**.



4. En el cuadro de diálogo **Crear CLAG**, haga lo siguiente:
 - a) En la lista desplegable **ID de canal**, seleccione el ID del canal LA del clúster.
 - b) En la sección **Interfaces**, en el cuadro de selección **Disponible**, seleccione las interfaces y haga clic en **+**.
 - c) Las interfaces seleccionadas se muestran en el cuadro de selección **Configurado**.
5. En la sección **Configuración**, haga lo siguiente:
 - a) En el campo **Alias**, introduzca un nombre alternativo para el canal LA del clúster.
 - b) En el campo Tiempo de **espera de LACP**, seleccione uno de los siguientes valores para definir el intervalo después del cual un enlace no se agrega, si el enlace no recibe una LACPDU.

El valor debe coincidir en todos los puertos que participan en la agregación de enlaces en el dispositivo SDX y el nodo asociado:

- **Largo:** 30 segundos.
- **Corto:** 1 segundo

- c) Para la configuración de alta disponibilidad (HA), seleccione la casilla de verificación **Supervisión de HA** para supervisar el canal en busca de eventos de error. El fallo de cualquier canal LA que tenga habilitado HA MON desencadena la conmutación por error de HA.
 - d) Seleccione **Etiquetar todo** para agregar una etiqueta 802.1q de cuatro bytes a cada paquete enviado por este canal. La configuración **ON** aplica etiquetas para todas las VLAN que están enlazadas a este canal. OFF aplica la etiqueta a todas las VLAN que no sean la VLAN nativa.
6. Haga clic en **Crear** para configurar un CLAG para uno de los dispositivos SDX.

The screenshot displays the 'Create CLAG' configuration page in the Citrix NetScaler SDX (8400) web interface. At the top, there is a navigation bar with 'Dashboard', 'Configuration', 'Documentation', and 'Downloads'. The main heading is 'Create CLAG'. Below this, the 'Channel ID*' is set to 'CLA/2'. The 'Interfaces' section is divided into two panes: 'Available (3)' and 'Configured (0)'. The 'Available' pane lists three interfaces: '1/2', '1/3', and '1/6', each with a '+' icon. The 'Configured' pane is empty, showing 'No items'. Below the interface panes are 'Settings' options: an empty 'Alias' field, 'LACP Timeout' with 'Long' selected (radio buttons), 'HA Monitoring' checked (checkbox), and 'Tag All' unchecked (checkbox). At the bottom of the form are 'Create' and 'Close' buttons.

7. En el cuadro de diálogo **Confirmar**, haga clic en **Sí** para actualizar la configuración de CLAG en los demás dispositivos SDX.

Notas:

- Si selecciona **No**, el CLAG no está configurado.
- Actualice manualmente la configuración de CLAG en los demás dispositivos SDX.

- La configuración de MTU debe ser la misma en ambos dispositivos SDX. La configuración de MTU se debe cambiar manualmente en cualquiera de los dispositivos SDX.

8. Para cambiar la configuración de MTU en el cuadro de diálogo **CLAGs**, haga lo siguiente:
 - a) Seleccione **CLA/1** y haga clic en **Editar**.
 - b) En el cuadro de diálogo **Configurar CLAG**, defina la MTU manualmente en el campo **MTU** y haga clic en **Aceptar**.
9. En el cuadro de diálogo **Confirmar**, haga clic en **Sí**.

Configurar cifrados SSL para acceder de forma segura al Servicio de administración

February 15, 2024

Puede seleccionar conjuntos de cifrado SSL de una lista de cifrados SSL compatibles con los dispositivos NetScaler SDX. Enlaza cualquier combinación de cifrados SSL para acceder a SDX Management Service de forma segura a través de HTTPS. Un dispositivo SDX proporciona 37 grupos de cifrado predefinidos, que son combinaciones de cifrados similares, y puede crear grupos de cifrado personalizados a partir de la lista de cifrados SSL compatibles.

Limitaciones

- No se admiten cifrados de enlace con intercambio de claves = “DH”o “ECC-DHE”.
- No se admite la vinculación de los cifrados con Authentication = “DSS”.
- No se admiten los cifrados vinculantes que no forman parte de la lista de cifrados SSL admitidos o que incluyen estos cifrados en un grupo de cifrado personalizado.

Cifrados SSL compatibles

En la siguiente tabla se enumeran los cifrados SSL admitidos. El valor de la columna **Protocolo** es el protocolo más bajo admitido. Por ejemplo, si aparece SSLv3, todos son compatibles con SSLv3/TLSv1/TLSv1.1/TLSv1.2.

Nombre de cifrado de Citrix	Nombre de cifrado de OpenSSL	Código hexadecimal	Protocolo	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de código de autenticación de mensajes
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	SSLv3	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	SSLv3	RSA	RSA	AES(128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES(256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES(128)
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	SSLv3	ECC-DHE	RSA	AES(256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLv3	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES(256)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES(128)

Nombre de cifrado de Citrix	Nombre de cifrado de OpenSSL	Código hexadecimal	Protocolo	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de código de autenticación de mensajes
TLS1.2-ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA-AES256-GCM-SHA384	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES(256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES(128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)
TLS1-DHE-RSA-AES-256-CBC-SHA	DHE-RSA-AES256-SHA	0x0039	SSLv3	DH	RSA	AES(256)

Nombre de cifrado de Citrix	Nombre de cifrado de OpenSSL	Código hexadecimal	Protocolo	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de código de autenticación de mensajes
TLS1-DHE-RSA-AES-128-CBC-SHA	DHE-RSA-AES128-SHA	0x0033	SSLv3	DH	RSA	AES(128)
TLS1-DHE-DSS-AES-256-CBC-SHA	DHE-DSS-AES256-SHA	0x0038	SSLv3	DH	DSS	AES(256)
TLS1-DHE-DSS-AES-128-CBC-SHA	DHE-DSS-AES128-SHA	0x0032	SSLv3	DH	DSS	AES(128)
TLS1-ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA-DES-CBC3-SHA	0xC012	SSLv3	ECC-DHE	RSA	3DES(168)
SSL3-EDH-RSA-DES-CBC3-SHA	EDH-RSA-DES-CBC3-SHA	0x0016	SSLv3	DH	RSA	3DES(168)
SSL3-EDH-DSS-DES-CBC3-SHA	EDH-DSS-DES-CBC3-SHA	0x0013	SSLv3	DH	DSS	3DES(168)
TLS1-ECDHE-RSA-RC4-SHA	ECDHE-RSA-RC4-SHA	0xC011	SSLv3	ECC-DHE	RSA	RC4(128)
SSL3-DES-CBC3-SHA	DES-CBC3-SHA	0x000A	SSLv3	RSA	RSA	3DES(168)
SSL3-RC4-SHA	RC4-SHA	0x0005	SSLv3	RSA	RSA	RC4(128)
SSL3-RC4-MD5	RC4-MD5	0x0004	SSLv3	RSA	RSA	RC4(128)
SSL3-DES-CBC-SHA	DES-CBC-SHA	0x0009	SSLv3	RSA	RSA	DES(56)
SSL3-EXP-RC4-MD5	EXP-RC4-MD5	0x0003	SSLv3	RSA(512)	RSA	RC4(40)

Nombre de cifrado de Citrix	Nombre de cifrado de OpenSSL	Código hexadecimal	Protocolo	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de código de autenticación de mensajes
SSL3-EXP-DES-CBC-SHA	EXP-DES-CBC-SHA	0x0008	SSLv3	RSA(512)	RSA	DES(40)
SSL3-EXP-RC2-CBC-MD5	EXP-RC2-CBC-MD5	0x0006	SSLv3	RSA(512)	RSA	RC2(40)
SSL2-DES-CBC-MD5	DHE-DSS-AES128-SHA256	0x0040	SSLv2	RSA	RSA	DES(56)
SSL3-EDH-DSS-DES-CBC-SHA	EDH-DSS-DES-CBC-SHA	0x0012	SSLv3	DH	DSS	DES(56)
SSL3-EXP-EDH-DSS-DES-CBC-SHA	EXP-EDH-DSS-DES-CBC-SHA	0x0011	SSLv3	DH(512)	DSS	DES(40)
SSL3-EDH-RSA-DES-CBC-SHA	EDH-RSA-DES-CBC-SHA	0x0015	SSLv3	DH	RSA	DES(56)
SSL3-EXP-EDH-RSA-DES-CBC-SHA	EXP-EDH-RSA-DES-CBC-SHA	0x0014	SSLv3	DH(512)	RSA	DES(40)
SSL3-ADH-RC4-MD5	ADH-RC4-MD5	0x0018	SSLv3	DH	Ninguno	RC4(128)
SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	Ninguno	3DES(168)
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	SSLv3	DH	Ninguno	DES(56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	Ninguno	AES(128)

Nombre de cifrado de Citrix	Nombre de cifrado de OpenSSL	Código hexadecimal	Protocolo	Algoritmo de intercambio de claves	Algoritmo de autenticación	Algoritmo de código de autenticación de mensajes
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	Ninguno	AES(256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH(512)	Ninguno	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH(512)	Ninguno	DES(40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	Ninguno
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	Ninguno

Grupos de cifrado predefinidos

En la siguiente tabla se enumeran los grupos de cifrado predefinidos que proporciona el dispositivo SDX.

Nombre del grupo de cifrado	Descripción
ALL	Todos los cifrados compatibles con el dispositivo SDX, excepto los cifrados NULL
PREDETERMINADO	Lista de cifrado predeterminada con fuerza de cifrado ≥ 128 bits
kRSA	Cifrados con el algoritmo Key-ex como RSA
kEDH	Cifrados con el algoritmo Key-Ex como Ephemeral-DH
DH	Cifrados con el algoritmo Key-ex como DH
EDH	Cifrados con el algoritmo Key-EX/Auth como DH
aRSA	Cifrados con el algoritmo de autenticación como RSA

Nombre del grupo de cifrado	Descripción
aDSS	Cifrados con el algoritmo de autenticación como DSS
aNULL	Cifrados con el algoritmo de autenticación como NULL
DSS	Cifrados con el algoritmo de autenticación como DSS
DES	Cifrados con Enc algo como DES
3DES	Cifrados con Enc algo como 3DES
RC4	Cifrados con Enc algo como RC4
RC2	Cifrados con Enc algo como RC2
NULO	Cifrados con Enc algo como NULL
MD5	Cifrados con el algoritmo MAC como MD5
SHA1	Cifrados con el algoritmo MAC como SHA-1
SHA	Cifrados con el algoritmo MAC como SHA
NULO	Cifrados con Enc algo como NULL
RSA	Cifrados con el algoritmo Key-ex/Auth como RSA
ADH	Cifra con el algoritmo Key-ex como DH y el algoritmo de autenticación como NULL
SSLv2	Cifrados de protocolo SSLv2
SSLv3	Cifrados de protocolo SSLv3
TLSv1	Cifradore de protocolo SSLv3/TLSv1
TLSv1_ONLY	Cifrados de protocolo TLSv1
EXP	Cifrados de exportación
EXPORTAR	Cifrados de exportación
EXPORT40	Exportación de cifrados con cifrado de 40 bits
EXPORT56	Exportación de cifrados con cifrado de 56 bits
BAJO	Cifrados de baja potencia (cifrado de 56 bits)
MEDIANO	Cifrados de potencia media (cifrado de 128 bits)
ALTO	Cifrados de alta potencia (cifrado de 168 bits)
AES	Cifrados AES
FIPS	Cifrados aprobados por FIPS

Nombre del grupo de cifrado	Descripción
ECDHE	Cifrados DH efímeros de curva elíptica
AES-GCM	Cifrados con Enc algo como AES-GCM
SHA2	Cifrados con el algoritmo MAC como SHA-2

Ver los grupos de cifrado predefinidos

Para ver los grupos de cifrado predefinidos, en la ficha **Configuración**, en el panel de navegación, expanda **Management Service** y, a continuación, haga clic en **Grupos de cifrado**.

Crear grupos de cifrado personalizados

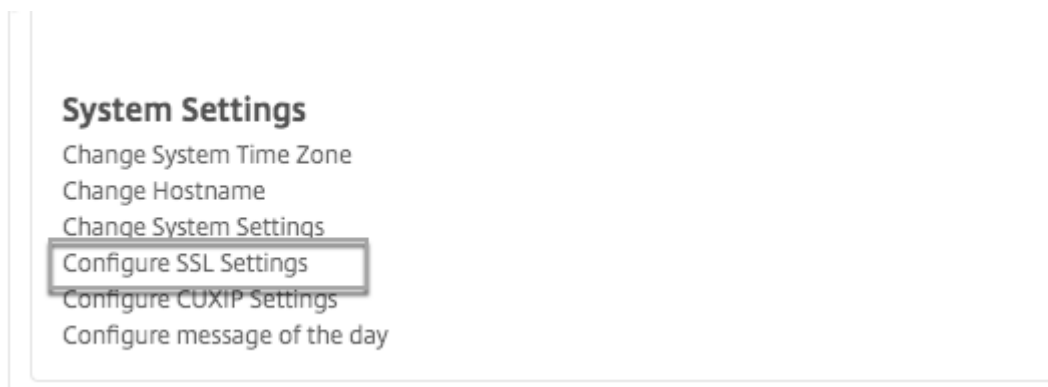
Puede crear grupos de cifrado personalizados a partir de la lista de cifrados SSL compatibles.

Para crear grupos de cifrado personalizados:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Management Service** y, a continuación, haga clic en **Grupos de cifrado**.
2. En el panel **Grupos de cifrado**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Crear grupo de cifrado**, realice lo siguiente:
 - a) En el campo **Nombre de grupo**, escriba un nombre para el grupo de cifrado personalizado.
 - b) En el campo **Descripción del grupo de cifrado**, introduzca una breve descripción del grupo de cifrado personalizado.
 - c) En la sección **Cipher Suites**, haga clic en **Agregar** y seleccione los cifrados que quiere incluir en la lista de cifrados SSL compatibles.
 - d) Haga clic en **Crear**.

Ver enlaces de cifrado SSL existentes

Para ver los enlaces de cifrado existentes, en la ficha **Configuración**, en el panel de navegación, expanda **Sistema**, a continuación, haga clic en **Configurar configuración de SSL en Configuración del sistema**.

**Nota:**

Tras la actualización a la versión más reciente del servicio de administración, la lista de conjuntos de cifrado existentes muestra los nombres de OpenSSL. Una vez que vincula los cifrados del Management Service actualizado, la pantalla utiliza la convención de nomenclatura de Citrix.

Enlazar cifrados al servicio HTTPS

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **Sistema**.
2. En el panel **Sistema**, en Configuración del sistema, haga clic en **Configurar configuración de SSL**.
3. En el panel **Modificar configuración**, haga clic en **Suites de cifrado**.
4. En el panel **Suites de cifrado**, realice una de las acciones siguientes:
 - Para elegir un grupo de cifrado de los grupos de cifrado predefinidos, seleccione Grupos de **cifrado**, seleccione un grupo de cifrado en la lista **Grupos de cifrado** y, a continuación, haga clic en **Aceptar**.
 - Para elegir de la lista de cifrados admitidos, active la casilla de verificación **Suites de cifrado**, haga clic en **Agregar** para seleccionar los cifrados y, a continuación, haga clic en **Aceptar**.

Realice una copia de seguridad y restaure los datos de configuración del dispositivo SDX

February 15, 2024

El proceso de respaldo del dispositivo NetScaler SDX es un proceso de un solo paso que crea un archivo de respaldo que contiene lo siguiente:

- Imagen de paquete individual:

- Imagen de Citrix Hypervisor
 - Revisiones y paquetes complementarios de Citrix Hypervisor
 - Imagen del Servicio de administración
-
- Imagen XVA
 - Imagen de actualización
 - Configuración SDX
 - Configuración

La carpeta de reserva es `/var/mps/backup`.

Realizar copias de seguridad de la configuración actual

1. En la ficha **Configuración**, en el panel de navegación, expanda **Servicio de administración** y, a continuación, haga clic en **Archivos de copia de reserva**.
2. En el panel **Copias de seguridad**, haga clic en **Copia de seguridad**.
3. en el cuadro de diálogo **Nuevo archivo de copia** de seguridad, seleccione la casilla de verificación **Proteger con contraseña** para cifrar el archivo de copia de seguridad.
4. En los campos **Contraseña** y **Confirmar contraseña**, escriba y confirme la contraseña del archivo de copia de seguridad.
5. Haga clic en **Continuar**.

El proceso de copia de seguridad crea un archivo de seguridad. El nombre de archivo del archivo de copia de seguridad incluye la dirección IP actual del Servicio de administración y la marca de tiempo cuando se realizó la copia de seguridad. Para comprobar cualquier discrepancia que pueda tener el archivo de copia de seguridad, desde la GUI de SDX, vaya a **Configuración > Sistema > Eventos/alar-mas**.

Backup programado

De forma predeterminada, SDX crea una copia de seguridad cada 24 horas mediante una directiva de copia de seguridad. Con la directiva de copia de seguridad, puede definir la cantidad de archivos de copia de seguridad que quiere conservar en el dispositivo SDX. Además, puede cifrar los archivos de copia de seguridad programados con una contraseña para garantizar que el archivo de copia de seguridad sea seguro.

Modificar la directiva de copias de seguridad

1. En la ficha **Configuración**, haga clic en **Sistema**.
2. En el panel **Administración de directivas**, haga clic en **Directiva de copia de seguridad**.

3. En el panel **Configurar directiva de copia de seguridad**, lleve a cabo lo siguiente:
 - a) En el campo **Copias de seguridad anteriores para conservar**, escriba el número de archivos de copia de seguridad que quiere conservar.
 - b) Para cifrar los archivos de copia de seguridad, seleccione la casilla **Cifrar archivo de copia de seguridad**.
 - c) En los campos **Contraseña** y **Confirmar contraseña**, escriba y confirme la contraseña para cifrar el archivo de copia de seguridad.

Transfiera manualmente el archivo de seguridad a un servidor de seguridad externo

Asegúrese de tener los detalles del servidor de seguridad externo antes de transferir manualmente el archivo de seguridad.

Transfiera el archivo de seguridad a un servidor de seguridad externo

1. En la ficha **Configuración**, en el panel de navegación, expanda **Servicio de administración** y, a continuación, haga clic en **Archivos de copia de reserva**.
2. En el panel **Archivos de copia de seguridad**, seleccione el archivo de copia de seguridad y, a continuación, haga clic en **Transferir**.
3. En el campo **Servidor**, escriba el nombre de host o la dirección IP del servidor de seguridad externo.
4. En los campos **Nombre de usuario** y **Contraseña**, escriba el nombre de usuario y la contraseña para acceder al servidor de copia de seguridad externo.
5. En el campo **Puerto**, escriba el número de puerto.
6. En el campo **Protocolo de transferencia**, seleccione el protocolo que quiere utilizar para transferir el archivo de copia de seguridad al servidor de copia de seguridad externo.
7. En el campo **Ruta de acceso del directorio**, escriba la ruta del directorio en el servidor de copia de seguridad externo donde quiere almacenar los archivos de copia de seguridad.
8. Seleccione **Eliminar archivo del Servicio de administración** para eliminar el archivo de copia de seguridad del dispositivo SDX después de haber transferido el archivo de copia de seguridad al servidor de copia de seguridad externo.
9. Haga clic en **Aceptar**.

Restaurar el dispositivo

Puede restaurar el dispositivo SDX a la configuración disponible en el archivo de copia de seguridad. Durante la restauración del dispositivo, se elimina toda la configuración actual.

Puntos a tener en cuenta:

- Antes de restaurar el dispositivo SDX mediante el archivo de copia de seguridad de un dispositivo SDX diferente, agregue la configuración de red del Servicio de administración de acuerdo con la configuración disponible en el archivo de copia de seguridad.
- Asegúrese de que la variante de plataforma en la que se realizó la copia de seguridad sea la misma que en la que intenta restaurar. No se admite la restauración del archivo de copia de seguridad entre dos variantes de plataforma diferentes.
- Citrix recomienda restaurar la copia de seguridad de SDX solo después de establecer la configuración de red. Puede especificar la siguiente configuración de red para la SVM:
 - Dirección IP de SVM
 - Dirección IP del hipervisor
 - Máscara de subred
 - Gateway
 - Servidor DNS

Restaurar el dispositivo desde el archivo de copia de seguridad

1. En la ficha **Configuración**, en el panel de navegación, expanda **Servicio de administración**, a continuación, haga clic en **Copiar archivos**.
2. En el panel **Archivos de copia de seguridad**, haga clic en el archivo de copia de seguridad y, a continuación, haga clic en **Aceptar**.
3. En el cuadro de diálogo **Restaurar**, seleccione **Restaurar equipo**, a continuación, haga clic en **Continuar**.

Se muestran los diferentes componentes de la restauración de la aplicación:

- Licencia
- Imagen SDX
- Archivos XVA
- Configuración de NetScaler
- Resumen

Si falta alguno de los componentes requeridos en el archivo de copia de seguridad, se le pedirá que cargue el elemento que falta antes de continuar.

Para saber si un archivo de copia de seguridad se puede restaurar en la versión actual de imagen de paquete único de SDX, consulte la siguiente tabla. Como regla general para la imagen de paquete único, ninguna copia de seguridad de una versión inferior no se puede restaurar en una versión posterior.

Versión actual de imagen de paquete único de SDX	Versión del archivo de seguridad
11.1	Se admiten 11.1, 12.0, 12.1, 13.0; 11.0 no se admite
12.0	Se admiten 12.0, 12.1, 13.0; no se admiten 11.0 y 11.1
12.1	12.1, 13.0 compatibles, 11.0, 11.1, 12.0 no compatibles
13.0	Se admite 13.0; 11.0, 11.1, 12.0, 12.1 no se admite
13.1	Compatible con 13.1; 11.0, 11.1, 12.0, 12.1, 13.0 no compatible

4. En la página **Licencia**, compruebe que existe una licencia válida y haga clic en **Siguiente**.
5. Aparecerá la página **Imagen SDX**. Si no se requiere una imagen SDX para realizar la restauración, haga clic en **Siguiente**. De lo contrario, cuando se le solicite cargue una imagen SDX válida y haga clic en **Siguiente**.
6. Se abrirá la página **Archivo XVA**. Haga clic en **Siguiente** si hay imágenes XVA para todas las instancias. Si el archivo XVA de cualquier instancia falta en el archivo de copia de seguridad, puede cargarlo u omitir la restauración de esta instancia. Haga clic en **Siguiente** para ir a la página siguiente.
7. Se abre la página de configuración de NetScaler. Los archivos de configuración de NetScaler no son obligatorios. Puede aprovisionar la instancia sin restaurar su configuración. Si falta el archivo de configuración de NetScaler en el archivo de copia de seguridad, puede continuar solo con el aprovisionamiento de instancias u omitir la restauración de la instancia. Haga clic en **Siguiente** para ir a la página siguiente.
8. La página de resumen aparece con los siguientes detalles sobre todas las instancias presentes en el archivo de copia de seguridad:
 - Dirección IP
 - Nombre de host
 - Versión SDX
 - Versión XVA
 - Bit de versión
 - Restaurar: Si el dispositivo o la instancia están listos para la restauración, aparece una marca de verificación. Si no lo está, aparecerá una cruz.
 - Mensajes de error: si el dispositivo o la instancia no están listos para la restauración, aparece un mensaje de error para explicar el motivo.

9. Haga clic en **Restaurar** para completar el proceso de restauración de aplicaciones.

Restaurar la instancia de NetScaler

Puede restaurar la instancia de NetScaler del dispositivo SDX a las instancias de NetScaler que están disponibles en el archivo de respaldo.

Nota: Una instancia VPX no se restaura si:

- La instancia no tiene asignada una NIC de administración y
- La instancia se administra desde SDX Management Service solo a través de LACP.
La restauración falla porque SDX Management Service no puede restaurar las configuraciones de canal automáticamente. Para evitar este problema, restaure manualmente la configuración del canal para completar la restauración de la instancia VPX.

Para restaurar la instancia de NetScaler en el archivo de respaldo:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Servicio de administración**, a continuación, haga clic en **Copiar archivos**.
2. En el panel **Archivos de copia de seguridad**, seleccione el archivo de copia de seguridad y, a continuación, haga clic en **Restaurar**.
3. En el cuadro de diálogo **Restaurar**, seleccione **Restaurar instancia**.
4. Seleccione las instancias NetScaler que quiere restaurar y, a continuación, haga clic en **Continuar**.
5. (opcional) Si el archivo de copia de seguridad está cifrado, cuando se le solicite, escriba la contraseña y, a continuación, haga clic en **Aceptar**.

Nota:

Asegúrese de que haya una configuración adecuada de XVA, imagen de compilación y canal en el dispositivo SDX que ejecuta la instancia que se está restaurando.

Realizar un restablecimiento del dispositivo

November 23, 2023

El dispositivo NetScaler SDX le permite:

- Restablezca la configuración del dispositivo.

Nota:

Al restablecer la configuración, debe iniciar sesión con el número de serie del dispositivo como contraseña.

- Restablezca el dispositivo a la versión de fábrica.
- Restablezca el dispositivo a una versión de imagen de paquete único en particular.

Antes de restablecer el dispositivo, haga una copia de seguridad de todos los datos almacenados en el dispositivo, incluida la configuración de todas las instancias de NetScaler aprovisionadas en el dispositivo.

Citrix recomienda almacenar los archivos fuera del dispositivo. Al realizar un restablecimiento del dispositivo, se finalizan todas las sesiones actuales del cliente con el Servicio de administración. Vuelva a iniciar sesión en Management Service para cualquier tarea de configuración adicional. Cuando tenga todo listo para restaurar los datos, importe los archivos de copia de seguridad mediante Management Service.

Management Service proporciona las siguientes opciones para restablecer el dispositivo:

- Restablecimiento de configuración
- Restablecimiento de fábrica
- Instalación limpia

Restablecer la configuración del dispositivo

Management Service proporciona la opción de restablecimiento de configuración para restablecer la configuración del dispositivo. La opción Restablecer configuración hace lo siguiente:

- Elimina instancias VPX.
- Elimina los archivos de claves y certificados SSL.
- Elimina los archivos de licencias y archivos técnicos.
- Elimina la configuración de NTP del dispositivo.
- Restaura la zona horaria a UTC.
- Restaura las directivas de recorte y copia de seguridad a su configuración predeterminada.
- Elimina la imagen del Servicio de administración.
- Elimina la imagen de NetScaler SDX.
- Elimina todas las imágenes XVA excepto el último archivo de imagen al que se accedió en el dispositivo.
- Restaura la configuración de interfaz predeterminada.
- Restaura la configuración predeterminada del dispositivo, incluidos los perfiles, los usuarios y la configuración del sistema predeterminados.

- Restaura las contraseñas predeterminadas para Citrix Hypervisor y el Servicio de administración.
- Reinicia Management Service.

Restablecer la configuración del dispositivo

1. Vaya al **grupo Configuración > Sistema > Administración del sistema**.
2. Haga clic en **Restablecer equipo**.
3. En el cuadro de diálogo **Restablecer dispositivo**, seleccione **Reinicio de configuración** en la lista **Tipo de restablecimiento**.
4. Haga clic en **Aceptar**.

Restablecer el dispositivo a la versión de fábrica

Management Service proporciona la opción de restablecimiento de fábrica para restablecer el dispositivo a la versión de fábrica. La opción de restablecimiento de valores de fábrica restablece las direcciones IP actuales del Servicio de administración y Citrix Hypervisor a las direcciones IP predeterminadas del Servicio de administración y Citrix Hypervisor.

Asegúrese de hacer una copia de seguridad de todos los datos almacenados en el dispositivo, incluida la configuración de todas las instancias de NetScaler aprovisionadas en el dispositivo. Citrix recomienda almacenar los archivos fuera del dispositivo. Al realizar un restablecimiento de fábrica, se finalizan todas las sesiones actuales de los clientes con Management Service. Vuelva a iniciar sesión en Management Service para cualquier tarea de configuración adicional. Cuando tenga todo listo para restaurar los datos, importe los archivos de copia de seguridad mediante Management Service.

Importante

Asegúrese de conectar un cable de consola serie al dispositivo antes de realizar un restablecimiento de fábrica.

Restablecer el dispositivo a la versión de fábrica

1. Vaya a **Configuración > Sistema > Administración del sistema**.
2. Haga clic en **Restablecer equipo**.
3. En el cuadro de diálogo **Restablecer dispositivo**, seleccione **Restablecimiento a valores de fábrica** en la lista **Tipo de restablecimiento**.
4. Haga clic en **Aceptar**.

Restablecer el dispositivo a una sola versión de imagen de paquete

El Servicio de administración proporciona la opción Instalación limpia que le permite instalar una versión arbitraria de una sola imagen de paquete en el dispositivo. Le permite realizar una instalación nueva de la imagen de paquete único como la nueva imagen de arranque predeterminada. La instalación limpia elimina la configuración existente, excepto la configuración de red, en el dispositivo SDX.

Nota:

Si el dispositivo SDX se envió con la versión de software 11.0 o anterior, se produce un error en la instalación limpia en la versión 13.1 o posterior.

La opción Instalación limpia se admite en lo siguiente:

Versión de imagen de paquete único	Plataformas SDX
11.0.xx	SDX 14xxx, SDX 25xxx. Nota: La opción de instalación limpia se admite en otras plataformas SDX si tienen una partición de fábrica 10G.
11.1.xx	SDX 14xxx, SDX 25xxx. Nota: La opción de instalación limpia se admite en otras plataformas SDX si tienen una partición de fábrica 10G
11.1.51.x	Todas las plataformas SDX.
12.1.xx	Todas las plataformas SDX.
13.0.xx	Todas las plataformas SDX.
13.1.xx	Todas las plataformas SDX.

Requisitos previos

Asegúrese de que:

- Puede conmutar por error todos los nodos principales de alta disponibilidad a un dispositivo SDX diferente. Si no tiene capacidades de alta disponibilidad, asegúrese de planificar el tiempo de inactividad en consecuencia.
- Descargue la imagen del paquete único en su máquina local.

Importante:

Asegúrese de que no reinicie ni apague y apague el dispositivo mientras utiliza la opción **Instalación limpia**.

El dispositivo se reinicia varias veces.

Restablecer el dispositivo a una sola versión de imagen de paquete

1. Navegue hasta el grupo **Configuración > Sistema > Administración del sistema**.
2. Haga clic en **Restablecer equipo**.
3. En el cuadro de diálogo **Restablecer dispositivo**, seleccione **Instalación limpia** en la lista **Tipo de restablecimiento**.
4. Haga clic en **Aceptar**.

Servidores de autenticación externos en cascada

February 15, 2024

La conexión en cascada de varios servidores de autenticación externos proporciona un proceso continuo y fiable para autenticar y autorizar a los usuarios externos. Si la autenticación falla en el primer servidor de autenticación, Management Service intenta autenticar al usuario mediante el segundo servidor de autenticación externo.

Para habilitar la autenticación en cascada, agregue los servidores de autenticación externos al Servicio de administración. Para obtener más información, consulte [Configuración de la autenticación externa](#). Puede agregar cualquier tipo de servidores de autenticación externos compatibles (RADIUS, LDAP y TACACS). Por ejemplo, para agregar cuatro servidores de autenticación externos para la autenticación en cascada, puede agregar cualquier combinación de servidores RADIUS, LDAP y TACACS. También puede agregar los cuatro servidores del mismo tipo. Puede configurar hasta 32 servidores de autenticación externos en NetScaler Application Delivery Management.

Servidores de autenticación externos en cascada

1. En la ficha **Configuración**, en **Sistema**, expanda **Autenticación**.
2. En la página **Autenticación**, haga clic en **Configuración de autenticación**.
3. En la página **Configuración de autenticación**, seleccione **EXTERNAL** en la lista desplegable **Tipo de servidor** (solo se pueden conectar en cascada los servidores externos).
4. Haga clic en **Insertar**, en la página **Servidores externos** que se abre, seleccione uno o varios servidores de autenticación que quiera en cascada.

5. Haga clic en **Aceptar**.

Los servidores seleccionados se muestran en la página **Authentication Servers**, como se muestra en la siguiente ilustración. Para cambiar el orden de autenticación, use el icono junto al nombre de un servidor para mover el servidor hacia arriba o hacia abajo en la lista.

← Authentication Configuration

The appliance can authenticate users with local user accounts or by using an external authentication server.

Server Type*

EXTERNAL

External Servers

Insert Delete

<input checked="" type="checkbox"/>	Server Type	Server Name
<input checked="" type="checkbox"/>	RADIUS	10.102.166.80
<input checked="" type="checkbox"/>	LDAP	_LDAP2
<input checked="" type="checkbox"/>	LDAP	_LDAP1

Enable fallback local authentication

OK Close

Desbloquear a un usuario

November 23, 2023

Un administrador de NetScaler SDX puede desbloquear a un usuario antes de que caduque el intervalo de bloqueo. El bloqueo no se aplica si un usuario inicia sesión en Management Service a través de la consola. El intervalo de bloqueo también cambia de segundos a minutos. Valor mínimo = 1 minuto. Valor máximo = 30 minutos.

Desbloqueo de un usuario mediante la GUI

1. Vaya a **Configuración > Sistema > Administración de usuarios > Usuarios**.
2. Seleccione el usuario que quiere desbloquear.
3. Haga clic en **Desbloquear**.

Desbloqueo de un usuario mediante la CLI

En la línea de comandos, escriba:

```
set systemuser id=<ID> unlock=true
```

Suministro de instancias de NetScaler

November 23, 2023

Nota

La conexión del servicio NetScaler ADM está habilitada de forma predeterminada, después de instalar o actualizar el dispositivo NetScaler SDX a la versión 13.1. Para obtener más información, consulte Data Governance y NetScaler ADM Service connect.

Puede aprovisionar una o más instancias de NetScaler en el dispositivo SDX mediante el Servicio de administración. La cantidad de instancias que puede instalar depende de la licencia que haya adquirido. Si el número de instancias agregadas es igual al número especificado en la licencia, el Servicio de administración no permite aprovisionar más instancias de NetScaler.

Nota:

Puede configurar hasta 20 instancias VPX en una interfaz de red independiente de la plataforma de hardware subyacente.

El Aprovisionamiento de una instancia de NetScaler VPX en el dispositivo SDX comprende los siguientes pasos.

1. Defina un perfil de administrador para adjuntarlo a la instancia de NetScaler. Este perfil especifica las credenciales de usuario que Management Service utiliza para aprovisionar la instancia de ADC y, posteriormente, para comunicarse con la instancia para recuperar los datos de configuración. También puede usar el perfil de administrador predeterminado.
2. Cargue el archivo de imagen XVA en Management Service.
3. Agregue una instancia de NetScaler mediante el asistente Provision NetScaler del Servicio de administración. El Servicio de administración implementa implícitamente la instancia de NetScaler en el dispositivo SDX y, a continuación, descarga los detalles de configuración de la instancia.

Advertencia

Asegúrese de modificar las interfaces de red provisionadas o VLANs de una instancia mediante Management Service en lugar de realizar las modificaciones directamente en la instancia.

Crea un perfil de administrador

Los perfiles de administrador especifican las credenciales de usuario que utiliza el Servicio de administración al provisionar las instancias de NetScaler. Estas credenciales se usan más adelante al comunicarse con las instancias para recuperar los datos de configuración. El cliente también utiliza las credenciales de usuario especificadas en un perfil de administrador al iniciar sesión en las instancias de NetScaler a través de la CLI o la GUI.

Los perfiles de administración también permiten especificar que Management Service y una instancia de VPX se comuniquen entre sí solo a través de un canal seguro o mediante HTTP.

El perfil de administrador predeterminado de una instancia especifica el nombre de usuario administrador predeterminado. Este perfil no se puede modificar ni eliminar. Sin embargo, debes anular el perfil predeterminado creando un perfil de administrador definido por el usuario y adjuntándolo a la instancia cuando provisiona la instancia. El administrador del Servicio de administración puede eliminar un perfil de administrador definido por el usuario si no está adjunto a ninguna instancia de NetScaler.

Importante

No cambie la contraseña directamente en la instancia VPX. Si lo hace, la instancia se vuelve inaccesible desde el Servicio de administración. Para cambiar una contraseña, cree primero un perfil de administrador y, a continuación, modifique la instancia de NetScaler, seleccionando este perfil en la lista de perfiles de administrador.

Para cambiar la contraseña de las instancias de NetScaler en una configuración de alta disponibilidad, primero cambie la contraseña de la instancia designada como nodo secundario. A continuación, cambie la contraseña de la instancia designada como nodo principal. Recuerde cambiar las contraseñas solo mediante Management Service.

Crea un perfil de administrador

1. En la ficha **Configuración**, en el panel de navegación, expanda **Configuración de NetScaler** y, a continuación, haga clic en **Perfiles de administración**.
2. En el panel **Perfiles de administración**, haga clic en **Agregar**.
3. Aparecerá el cuadro **de diálogo Crear perfil de administrador**.

← Create Citrix ADC Profile

Profile Name*
 X Please enter value

User Name

Password*

Use global settings for Citrix ADC communication

▼ SNMP

Version
 v2 v3

Security Name*

Security Level*
 ▼

▼ Timeout Settings

commandcenter.timeout_settings

Timeout (in Seconds)

Defina los siguientes parámetros:

- Nombre del perfil: Nombre del perfil de administrador. El nombre de perfil predeterminado es `nsroot`. Puede crear nombres de perfil definidos por el usuario.
- Contraseña: La contraseña utilizada para iniciar sesión en la instancia de NetScaler. Longitud máxima: 31 caracteres.
- Puerto SSH: Configure el puerto SSH. El puerto predeterminado es 22.

- **Usar la configuración global para la comunicación de NetScaler:** Seleccione esta opción si quiere que la configuración se defina en la Configuración del sistema para la comunicación entre Management Service y la instancia de NetScaler. Puede desactivar esta casilla y cambiar el protocolo a HTTP o HTTPS.
 - Seleccione la opción **http** para usar el protocolo HTTP para la comunicación entre el Servicio de administración y la instancia de NetScaler.
 - Seleccione la opción **https** para usar el canal seguro para la comunicación entre el Servicio de administración y la instancia de NetScaler.
4. En **SNMP**, seleccione la versión. Si selecciona v2, vaya al paso 5. Si selecciona v3, vaya al paso 6.
 5. En SNMP v2, agregue el nombre de la **comunidad** SNMP.
 6. En SNMP v3, agregue **Nombre de seguridad** y **Nivel de seguridad**.
 7. En **Configuración de tiempo de espera**, especifique el valor.
 8. Haga clic en **Crear** y, a continuación, en **Cerrar**. El perfil de administrador que creó aparece en el panel **Perfiles de administrador**.

Si el valor de la columna **Predeterminado** es verdadero, el perfil predeterminado es el perfil de administrador. Si el valor es falso, un perfil definido por el usuario es el perfil de administrador.

Si no quiere utilizar un perfil de administrador definido por el usuario, puede quitarlo del Servicio de administración. Para quitar un perfil de administrador definido por el usuario, en el panel **Perfiles de administración**, seleccione el perfil que quiere quitar y, a continuación, haga clic en **Eliminar**.

Cargue una imagen de NetScaler.xva

Se requiere un archivo.xva para agregar una instancia de NetScaler VPX.

Cargue los archivos.xva de NetScaler SDX al dispositivo SDX antes de aprovisionar las instancias VPX. También puede descargar un archivo de imagen.xva en un equipo local como copia de seguridad. El formato de archivo de imagen .xva es: `NSVPX-XEN-ReleaseNumber-BuildNumber_nc.xva`.

En el panel **Archivos XVA de NetScaler**, puede ver los siguientes detalles.

- **Nombre:** Nombre del archivo de imagen.xva. El nombre del archivo contiene la versión y el número de compilación. Por ejemplo, el nombre del archivo `NSVPX-XEN-12.1-56.22.xva.gz` hace referencia a la versión 12.1, compilación 56.22.
- **Última modificación:** fecha en que se modificó por última vez el archivo de imagen.xva.
- **Tamaño:** Tamaño, en MB, del archivo de imagen.xva.

Para cargar un archivo.xva de NetScaler

1. En la ficha **Configuración**, en el panel de navegación, expanda **Configuración de NetScaler** y, a continuación, haga clic en **Archivos XVA**.
2. En el panel **Archivos XVA de NetScaler**, haga clic en **Cargar**.
3. En el cuadro de diálogo **Cargar instancia de NetScaler XVA**, haga clic en **Examinar** y seleccione el archivo de imagen XVA que quiere cargar.
4. Haga clic en **Cargar**. El archivo de imagen XVA aparece en el panel **Archivos XVA de NetScaler** después de cargarlo.

Para crear una copia de seguridad mediante la descarga de un archivo XVA de NetScaler

1. En el panel **Archivos de compilación de NetScaler**, seleccione el archivo que quiere descargar y, a continuación, haga clic en **Descargar**.
2. En el cuadro de mensaje **Descarga de archivos**, haga clic en **Guardar**.
3. En el cuadro de mensaje **Guardar como**, busque la ubicación en la que quiere guardar el archivo y, a continuación, haga clic en **Guardar**.

Agregar una instancia de NetScaler

Al agregar instancias de NetScaler desde el Servicio de administración, debe proporcionar valores para algunos parámetros. El Servicio de administración configura implícitamente estos parámetros en las instancias de NetScaler.

← Provision Citrix ADC

Name*

 ⓘ × Please enter value

Manage through internal network

IPv4

IPv6

XVA File*

Choose File

Admin Profile*

ns_nsroot_profile

Description

- **Nombre:** asigne un nombre a la instancia de NetScaler.
- Seleccione **Administrar a través de una red interna** para habilitar una conectividad interna permanente e independiente entre el Servicio de administración de SDX y la instancia VPX. Esta función está disponible en las versiones 13.0-36.27 y versiones posteriores de las instancias de VPX que se ejecutan en el dispositivo SDX.
- Seleccione una dirección IPv4 o IPv6 o ambas direcciones IPv4 e IPv6 para acceder a la instancia de NetScaler VPX con fines de administración. Una instancia de NetScaler solo puede tener una IP de administración (NSIP). No puede eliminar una dirección NSIP.
- Asigne una máscara de red, una puerta de enlace predeterminada y el siguiente salto a Management Service para la dirección IP.
- Los campos **Gateway** y **Nexthop to Management Service** son opcionales en cualquiera de las siguientes condiciones, cuando VPX se aprovisiona con las versiones 13.0—88.9 o 13.1—37.8 y sus versiones posteriores:
 - Cuando la opción **Administrar a través de la red interna** está habilitada.
 - Cuando la dirección IPv4 configurada se encuentra en la misma subred que la dirección IP del Servicio de administración.

IPv4

IPv4 Address*

Netmask*

Gateway

Nexthop to Management Service

A continuación, agrega el archivo XVA, el perfil de administrador y una descripción de la instancia.

Nota: Para una configuración de alta disponibilidad (active-active o active-standby), Citrix recomienda configurar las dos instancias de NetScaler VPX en diferentes dispositivos SDX. Asegúrese de que las instancias de la configuración tengan recursos idénticos, como CPU, memoria, interfaces, paquetes por segundo (PPS) y rendimiento.

Asignación de licencias

En esta sección, especifique la licencia que ha adquirido para NetScaler. La licencia puede ser Standard, Enterprise y Platinum.

Nota: Un asterisco indica que los campos son obligatorios.

License Allocation			
Feature License*		For more information about Citrix ADC editions, see Citrix ADC Editions	
Standard			
Pool	Total	Available	Allocate
Instance	0	0	1
Bandwidth			Allocation Mode* Fixed
	0 Gbps	0 Gbps	Throughput (Mbps)* 1000

Si necesita la capacidad de reventar el ancho de banda, seleccione **Flexible** en **Modo de asignación**. Para obtener más información, consulte [Medición del ancho de banda en SDX](#).

Asignación criptográfica

A partir de la versión 12.1 48.13, la interfaz para gestionar la capacidad de cifrado ha cambiado. Para obtener más información, consulte [Administrar la capacidad de cifrado](#).

Asignación de recursos

En Asignación de recursos, asigne la memoria total, los paquetes por segundo y la CPU.

Resource Allocation

Total Memory (MB)*

Packets per second*

CPU*

CPU

Asigne un núcleo o núcleos dedicados a la instancia, o la instancia compartirá un núcleo con otras instancias. Si seleccionas compartido, se asigna un núcleo a la instancia, pero el núcleo se puede compartir con otras instancias si hay escasez de recursos. Reinicie las instancias afectadas si se reasignan los núcleos de la CPU. Reinicie las instancias en las que se reasignen los núcleos de la CPU para evitar cualquier degradación del rendimiento.

A partir de la versión SDX 11.1.x.x (MR4), si utiliza la plataforma SDX 25000xx, puede asignar un máximo de 16 núcleos a una instancia. Además, si utiliza la plataforma SDX 2500xxx, puede asignar un máximo de 11 núcleos a una instancia.

Nota: Para una instancia, el rendimiento máximo que se configura es de 180 Gbps.

En la siguiente tabla se enumeran las VPX compatibles, la versión de imagen de paquete único y la cantidad de núcleos que puede asignar a una instancia:

Nombre de la plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una única instancia
SDX 8015, SDX 8400 y SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 y SDX 20500	12	10	5

Nombre de la plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una única instancia
SDX 11515, SDX 11520, SDX 11530, SDX 11540 y SDX 11542	12	10	5
SDX 17500, SDX 19500 y SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 y SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 y SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 y SDX 22120	16	14	7
SDX 24100 y SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G y SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS, y SDX 14100 FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S y SDX 14100 40S	12	10	10
SDX 25100A, 25160A, 25200A	20	18	9

Nombre de la plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una única instancia
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (si la versión es 11.1-51.x o superior); 9 (si la versión es 11.1-50.x o inferior; todas las versiones de 11.0 y 10.5)
SDX 26100, 26160, 26200, 26250	28	26	16
SDX 26100-50S, 26160-50S, 26200-50S, 26250-50S	28	26	16
SDX 26100-100 G, 26160-100 G, 26200-100 G, 26250-100 G	28	26	25
SDX 15000	16	14	14
SDX 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

Nota:

Los núcleos dedicados se asignan a la cantidad de motores de paquetes que se ejecutan en la instancia. Para una instancia VPX creada con núcleos dedicados, se asigna una CPU adicional para la administración.

Administración de instancias

Para crear un usuario administrador para la instancia VPX, seleccione **Agregar administración de instancias** en **Administración de instancias**.

Instance Administration

Add Instance Administration

User Name*

Password*

Confirm Password*

Shell/SFTP/SCP Access

Agregue los siguientes detalles:

Nombre de usuario: El nombre de usuario del administrador de instancias de NetScaler. Este usuario tiene acceso de superusuario, pero no tiene acceso a comandos de red para configurar VLAN e interfaces.

Contraseña: la contraseña del nombre de usuario.

Acceso a Shell/Sftp/Scp: El acceso permitido al administrador de instancias de NetScaler. Esta opción está seleccionada de forma predeterminada.

Configuración de la red

- **Permitir el modo L2:** puede permitir el modo L2 en la instancia de NetScaler. Seleccione **Permitir el modo L2** en **Configuración de red**. Antes de iniciar sesión en la instancia y habilitar el modo L2. Para obtener más información, consulte [Permitir el modo L2 en una instancia de NetScaler](#).

Network Settings

Allow L2 Mode ?

0/1 VLAN Tag

0/2 ? VLAN Tag

Data Interfaces

Add Edit Delete

Interface	Allow Untagged Traffic	Allowed VLANs
No items		

Nota:

- Si inhabilitas el modo L2 para una instancia desde el Servicio de administración, debes iniciar sesión en la instancia e inhabilitar el modo L2 de esa instancia. De lo contrario, es posible que se inhabiliten todos los demás modos de NetScaler después de reiniciar la instancia.
- Después de aprovisionar una instancia de ADC en SDX, no puede eliminar una interfaz o un canal de la instancia de ADC. Sin embargo, puede agregar una interfaz o un canal a la instancia de ADC.

- **Interfaz 0/1 y 0/2:** De forma predeterminada, se seleccionan las interfaces 0/1 y 0/2 para LA de administración.
- **Etiqueta de VLAN:** Especifique un ID de VLAN para la interfaz de administración. A continuación, agregue interfaces de datos.

Nota:

Los ID de interfaz de las interfaces que agrega a una instancia no se corresponden necesariamente con la numeración de la interfaz física del dispositivo SDX. Si la primera interfaz que asocia con la instancia 1 es la interfaz 1/4, aparece como interfaz 1/1 cuando ve la configuración de la interfaz en la instancia. La numeración cambia porque es la primera interfaz que asoció con la instancia 1.

Add Data Interface

Interfaces*

1/4

 Allow Untagged Traffic

Allowed VLANs

100-110,142,151-155

MAC Address Mode*

Default

▼ VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)

VRID IPv4

100-110,142,151-155

VRID IPv6

100-110,142,151-155

Add

Close

- **Permitir tráfico sin etiquetas:** Marque la casilla **Permitir tráfico sin etiquetas** para permitir que la instancia de NetScaler procese el tráfico sin etiquetas.

Nota:

Cuando la versión del dispositivo SDX es 13.1-24.x o posterior y la versión de la instancia de NetScaler es anterior a 13.1-24.x, la instancia de ADC procesa el tráfico sin etiquetar en las interfaces de Mellanox incluso si la casilla **Permitir tráfico sin etiquetar** está desactivada.

- **VLAN permitidas:** Especifique una lista de identificadores de VLAN que se pueden asociar a una instancia de NetScaler.
- **Modo de dirección MAC:** Asigne una dirección MAC. Seleccione una de estas opciones:
 - **Predeterminado:** Citrix Hypervisor asigna una dirección MAC.
 - **Personalizado:** Elija este modo para especificar una dirección MAC que anule la dirección MAC generada.
 - **Generado:** Genere una dirección MAC mediante la dirección MAC base establecida anteriormente. Para obtener información sobre cómo configurar una dirección MAC base, con-

sulte Asignación de una dirección MAC a una interfaz.

- Configuración de VMAC (VRID IPv4 e IPv6 para configurar Virtual MAC)
 - **VRID IPV4:** El VRID de IPv4 que identifica la VMAC. Valores posibles: 1-255. Para obtener más información, consulte Configuración de VMAC en una interfaz.
 - **VRID IPV6:** El VRID de IPv6 que identifica la VMAC. Valores posibles: 1-255. Para obtener más información, consulte Configuración de VMAC en una interfaz.

Configuración de VLAN de administración

Normalmente, Management Service y la dirección de administración (NSIP) de la instancia VPX se encuentran en la misma subred y la comunicación se realiza a través de una interfaz de administración. Sin embargo, si el Servicio de administración y la instancia están en subredes diferentes, debe especificar un identificador de VLAN en el momento de aprovisionar una instancia VPX. Este identificador es necesario para que se pueda acceder a la instancia a través de la red cuando se inicie. Si su implementación requiere que solo se pueda acceder al NSIP mediante la interfaz seleccionada en el momento de aprovisionar la instancia VPX, seleccione la opción NSVLAN.

Si se selecciona la opción **NSVLAN**, no puede cambiar esta configuración después de haber aprovisionado la instancia de NetScaler.

Management VLAN Settings

VLAN for Management Traffic

L2VLAN

When this option is selected, the configured VLAN is created as a data VLAN on NetScaler instance, and is used by the Management Service to access the NSIP for all communication with the instance. This option is suitable for performing in-band management of the instance over the data VLAN, without creating a separate management network.

NSVLAN

When this option is selected, the configured VLAN is created as the NSVLAN on NetScaler instance, and is used by the Management Service to access the NSIP for all communication with the instance. This option is suitable for performing out-of-band management of the instance over a separate management network. i.e., the NSVLAN.

Tagall

Interfaces

Configured (0) Remove All

No items

+ Add

Done
Close

Nota:

- Los latidos de HA se envían solo en las interfaces que forman parte de la NSVLAN.
- Puede configurar una NSVLAN solo desde VPX XVA build 9.3 53.4 y versiones posteriores.

Importante: Si no se selecciona NSVLAN, al ejecutar el comando “clear config full” en la instancia VPX se elimina la configuración de VLAN.

Haga clic en **Listo** para aprovisionar el dispositivo NetScaler VPX.

Modificar una instancia de NetScaler

Para modificar los valores de los parámetros de una instancia de ADC provisionada, en el panel **Instancias de NetScaler**, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar ADC, modifique los parámetros.

Puntos a tener en cuenta:

- Si modifica los siguientes parámetros: número de chips SSL, interfaces, memoria y licencia de funciones, la instancia de NetScaler se detiene y se reinicia implícitamente para que estos parámetros entren en vigor.
- No puede modificar los parámetros Imagen y Nombre de usuario.
- Las interfaces o los canales no se pueden eliminar de la instancia ADC. Sin embargo, se pueden agregar nuevas interfaces o canales a la instancia de ADC.
- Para eliminar una instancia de ADC provisionada en el dispositivo SDX, en el panel **Instancias de NetScaler**, seleccione la instancia que quiere eliminar y, a continuación, haga clic en **Eliminar**. En el cuadro **Confirmar** mensaje, haga clic en **Sí** para eliminar la instancia de NetScaler.

Restringir las VLAN a interfaces virtuales específicas

El administrador del dispositivo SDX puede aplicar VLAN 802.1Q específicas en las interfaces virtuales asociadas a las instancias de NetScaler. Esta capacidad resulta especialmente útil para restringir el uso de las VLAN 802.1Q por parte de los administradores de instancias. Si dos instancias que pertenecen a dos empresas diferentes se alojan en un dispositivo SDX, puede restringir que las dos empresas utilicen el mismo identificador de VLAN. Al hacerlo, una empresa no ve el tráfico de la otra empresa. Si un administrador de instancias intenta asignar una interfaz a una VLAN 802.1Q, se realiza una validación para verificar que el identificador de VLAN especificado forme parte de la lista de permitidos.

De forma predeterminada, cualquier identificador de VLAN se puede utilizar en una interfaz. Para restringir las VLAN etiquetadas en una interfaz, especifique los ID de VLAN en la configuración de red al provisionar una instancia de NetScaler. También puede especificarlo más adelante modificando la instancia. Para especificar un rango, separe los ID con un guion (por ejemplo, 10—12). Si inicialmente especifica algunos ID de VLAN pero luego los elimina todos de la lista de permitidos, puede usar cualquier ID de VLAN en esa interfaz. En efecto, ha restaurado la configuración predeterminada.

Después de crear una lista de VLAN permitidas, el administrador de SDX no tiene que iniciar sesión en una instancia para crear las VLAN. El administrador puede agregar y eliminar VLAN para instancias específicas del Servicio de administración.

Importante: Si el modo L2 está habilitado, el administrador debe asegurarse de que los ID de VLAN en diferentes instancias de NetScaler no se superpongan.

Para especificar los identificadores de VLAN permitidos

1. En el Asistente para aprovisionar ADC o en el Asistente para modificar ADC, en la página Configuración de red, en **VLAN permitidas**, especifique uno o más ID de VLAN permitidos en esta interfaz. Use un guión para especificar un rango. Por ejemplo, 2—4094.
2. Siga las instrucciones indicadas en el asistente.
3. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Para configurar VLAN para una instancia desde el Servicio de administración

1. En la ficha **Configuración**, vaya a NetScaler > Instancias.
2. Seleccione una instancia y, a continuación, haga clic en **VLAN**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo **Crear VLAN NetScaler**, especifique los siguientes parámetros:
 - ID de VLAN: un entero que identifica de manera única la VLAN a la que pertenece una trama en particular. NetScaler admite un máximo de 4094 VLAN. El identificador 1 está reservado para la VLAN predeterminada.
 - Enrutamiento dinámico IPV6: habilite todos los protocolos de enrutamiento dinámico IPV6 en esta VLAN. Nota: Para que la **configuración** ENABLED funcione, debes iniciar sesión en la instancia y configurar los protocolos de enrutamiento dinámico IPV6 desde la línea de comandos de VTYSH.
5. Seleccione las interfaces que deben formar parte de la VLAN.
6. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Administrar la capacidad de cifrado

November 23, 2023

A partir de la versión 12.1 48.13, la interfaz para gestionar la capacidad de cifrado ha cambiado. El Servicio de administración proporciona unidades criptográficas (ACU) asimétricas, unidades criptográficas simétricas (SCU) e interfaces criptovirtuales para indicar la capacidad SSL en el dispositivo NetScaler SDX. La capacidad criptográfica anterior se asignaba en unidades de chips SSL, núcleos SSL y funciones virtuales SSL. Consulte la tabla de conversión de chips SSL heredados a ACU y SCU para obtener más información sobre cómo los chips SSL heredados se traducen en unidades ACU y SCU.

Mediante la GUI del Servicio de administración, puede asignar capacidad de cifrado a la instancia de NetScaler VPX en unidades de ACU y SCU.

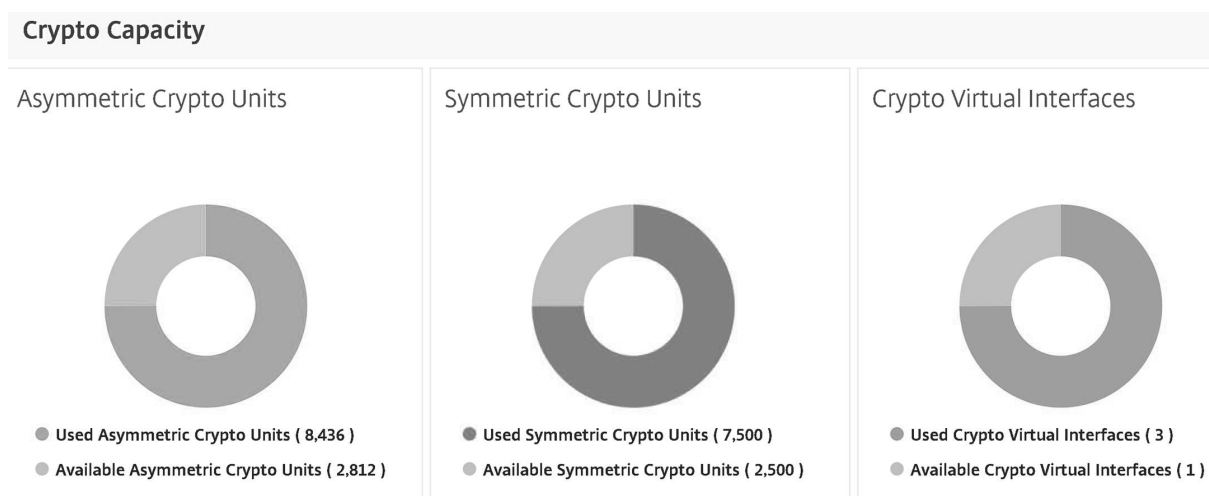
En la siguiente tabla se proporcionan descripciones breves sobre las ACU, las SCU y las instancias virtuales criptográficas.

Tabla. Unidades criptográficas unitarias

Nuevas unidades criptográficas	Descripción
Unidad criptográfica asimétrica (ACU)	1 ACU = 1 operación por segundo (operaciones) de descifrado (RSA) 2K (tamaño de clave de 2048 bits). Para obtener más información, consulte la tabla de conversión de recursos de ACU a PKE.
Unidad criptográfica simétrica (SCU)	1 SCU = 1 Mbps de AES-128-CBC+SHA256-HMAC a 1024B. Esta definición se aplica a todas las plataformas SDX.
Interfaces virtuales criptográficas	También conocidas como funciones virtuales, las interfaces virtuales criptográficas representan la unidad básica del hardware SSL. Una vez agotadas estas interfaces, el hardware SSL ya no se puede asignar a una instancia VPX. Las interfaces virtuales criptográficas son entidades de solo lectura y el dispositivo SDX asigna automáticamente estas entidades.

Ver la capacidad criptográfica del dispositivo SDX

Puede ver la capacidad de cifrado del dispositivo SDX en el panel de la GUI de SDX. El panel muestra las ACU, las SCU y las interfaces virtuales usadas y disponibles en el dispositivo SDX. Para ver la capacidad criptográfica, vaya a **Panel de control > Capacidad criptográfica**.



Asigna la capacidad de cifrado mientras se aprovisiona la instancia

Al aprovisionar una instancia VPX en el dispositivo SDX, en **Asignación criptográfica**, puede asignar el número de ACU y SCU para la instancia VPX. Para obtener instrucciones sobre cómo aprovisionar una instancia VPX, consulte [Aprovisionamiento de instancias de NetScaler](#).

Para asignar capacidad de cifrado mientras se aprovisiona una instancia VPX, siga estos pasos.

1. Inicie sesión en Management Service.
2. Vaya a **Configuración > NetScaler > Instancias** y haga clic en **Agregar**.
3. En **Asignación criptográfica**, puede ver las ACU, SCU e interfaces virtuales criptográficas disponibles. La forma de asignar las ACU y las SCU varía según el dispositivo SDX:
 - a. Para los dispositivos enumerados en el Valor mínimo de un contador de ACU disponible para diferentes dispositivos SDX, puede asignar ACU en múltiplos de un número especificado. Las SCU se asignan automáticamente y el campo de asignación de SCU no se puede modificar. Puede aumentar la asignación de ACU en los múltiplos de la ACU mínima disponible para ese modelo. Por ejemplo, si la ACU mínima es 4375, el incremento de la ACU es 8750, 13125, etc.

Un ejemplo. Asignación criptográfica en la que las SCU se asignan automáticamente y las ACU se asignan en múltiplos de un número específico.

Crypto Allocation			
	Asymmetric Crypto Units	Symmetric Crypto Units	Crypto Virtual Interfaces
Available	70000	56000	16
Total	70000	56000	16

Asymmetric Crypto Units	4375
Symmetric Crypto Units	3500

Valor mínimo de un contador ACU disponible para diferentes dispositivos SDX

Plataforma SDX	Valor mínimo del contador ACU
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 puertos)	2187
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375

Plataforma SDX	Valor mínimo del contador ACU
14xxx	4375
14xxx 40S	4375
14xxx 40G	4375
14xxx FIPS	4375
25xxx	4375
25xxx A	4575

b. Para el resto de plataformas SDX, que no se enumeran en la tabla anterior, puede asignar ACU y SCU libremente. El dispositivo SDX asigna automáticamente interfaces virtuales criptográficas.

Un ejemplo. Asignación criptográfica en la que tanto la ACU como las SCU se asignan libremente

Crypto Allocation			
	Asymmetric Crypto Units	Symmetric Crypto Units	Crypto Virtual Interfaces
Available	39000	41000	32
Total	39000	41000	32
Asymmetric Crypto Units			
	<input type="text" value="2000"/>		
Symmetric Crypto Units			
	<input type="text" value="2000"/>		

4./ Complete todos los pasos para aprovisionar la instancia VPX y haga clic en **Listo**. Para obtener más información, consulte [Aprovisionamiento de instancias de NetScaler](#).

Ver el estado del hardware criptográfico

En Management Service, puede ver el estado del hardware criptográfico que se proporciona con el dispositivo SDX. La salud del hardware criptográfico se representa como dispositivos criptográficos y funciones virtuales criptográficas. Para ver el estado del hardware criptográfico, vaya a **Panel de control > Recursos**.

The screenshot shows the 'Resources' page in the NetScaler SDX GUI. It features a 'Hardware' tab and a table with the following data:

Name	Status	Current Value	Expected Value
CPUs	● Ok	1	1
Hyper-threads	● Ok	16	16
Memory	● Ok	32 GB	32 GB
Crypto Virtual Functions	● Ok	32	32
Crypto Devices	● Ok	1	1
Management Interfaces	● Ok	1	1
10G Interfaces	● Ok	4	4
1G Interfaces	● Ok	6	6
40G Interfaces	● Ok	0	0
Disks	● Ok	1	1

Puntos que tener en cuenta

Tenga en cuenta lo siguiente cuando actualice el dispositivo SDX a la versión más reciente.

- Solo se actualiza la interfaz de usuario SDX, pero la capacidad del hardware del dispositivo sigue siendo la misma.
- El mecanismo de asignación de criptomonedas sigue siendo el mismo y solo cambia la representación en la GUI de SDX.
- La interfaz criptográfica es compatible con versiones anteriores y no afecta a ningún mecanismo de automatización existente que utilice la interfaz NITRO para administrar el dispositivo SDX.
- Tras la actualización del dispositivo SDX, la criptografía asignada a las instancias VPX existentes no cambia; solo cambia su representación en Management Service.

Tabla de conversión de recursos ACU a PKE

Plataforma SDX	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE- ECDSA
22040, 22060, 22080, 22100, 22120, 24100, 24150 (36 puertos)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	N/D
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060, 22080, 22100, 22120 (24 puertos)	4375	25000	4375	625	512	381
17500, 19500, 21500	2812	17000	2812	424	330	N/D
17550, 19550, 20550, 21550	2812	17000	2812	424	330	N/D
11500, 13500, 14500, 16500, 18500, 20500	2812	17000	2812	424	330	N/D

Plataforma SDX	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE- ECDSA
14000, 14000-40G, 25000, 25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40S	4375	25000	4375	625	512	381
*8900 (8910, 8920, 8930)	1000	4615	1000	136	397	494
*9100 (9110, 9120, 9130)	1000	4615	1000	136	397	494
*26000- 100G (26100, 26160, 26200 y 26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494

*En estas plataformas, los números de PKE son los valores mínimos garantizados.

Cómo leer la tabla de conversión de recursos ACU a PKE

La tabla de conversión de recursos ACU a PKE se basa en los siguientes puntos:

- El Servicio de administración ayuda a asignar recursos criptográficos a cada VPX individual. El Servicio de administración no puede asignar ni prometer rendimiento.
- El rendimiento real varía según el tamaño del paquete, el cifrado/Keyex/HMAC (o sus variaciones) utilizado, etc.

El siguiente ejemplo le ayuda a entender cómo leer y aplicar la ACU a la tabla de conversión de recursos de PKE.

Un ejemplo. Conversión de recursos de ACU a PKE para la plataforma SDX 22040

La asignación de 2187 ACU a una instancia VPX en una plataforma SDX 22040 asigna recursos criptográficos equivalentes a 256 operaciones ECDHE-RSA u 2187 operaciones RSA-2K, etc.

Tabla de conversión de chips SSL heredados a ACU y SCU

Para obtener más información sobre cómo los chips SSL heredados se convierten en ACU y SCU, consulte la siguiente tabla.

[Tabla de conversión de ACU y SCU](#)

Aprovisionar máquinas virtuales de terceros

November 23, 2023

Advertencia:

La compatibilidad **con instancias de terceros** está obsoleta en la GUI de NetScaler SDX a partir de la versión 13.1, compilación 37.x. Si aún quiere utilizar las instancias de terceros, Citrix recomienda realizar las siguientes operaciones:

- Inicie sesión en la consola del Servicio de administración.
- Cree un archivo `.thirdPartyVM` en el directorio `/mpsconfig`.
- Reinicie el Servicio de administración con el comando `svmd restart`.

El dispositivo SDX admite el aprovisionamiento de las siguientes máquinas virtuales de terceros (instancias):

- SECUREMATRIX GSB
- InterScan Web Security
- Protector de Websense
- Servidor DNS/DHCP de BlueCat
- CA Access Gateway
- VM-Series de PaloAlto

SECUREMATRIX GSB proporciona un sistema de contraseñas altamente seguro que elimina la necesidad de llevar cualquier dispositivo token. El protector de Websense proporciona funciones de supervisión y bloqueo para evitar la pérdida de datos y fugas de información confidencial. BlueCat DNS/DHCP Server ofrece DNS y DHCP para su red. La serie VM de PaloAlto en NetScaler SDX permite la consolidación de las capacidades avanzadas de seguridad y ADC en una sola plataforma, para que las empresas y los clientes proveedores de servicios accedan de forma segura y confiable a las aplicaciones. La combinación de la serie VM en NetScaler SDX también proporciona una solución ADC completa, validada y segura para las implementaciones de Citrix Virtual Apps and Desktops.

Puede aprovisionar, supervisar, administrar y solucionar problemas de una instancia desde el Servicio de administración. Todas las instancias de terceros anteriores usan el demonio `SDXTools` para comunicarse con el Servicio de administración. El daemon está preinstalado en la instancia aprovisionada. Puede actualizar el daemon cuando haya nuevas versiones disponibles.

Al configurar máquinas virtuales de terceros, las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces. Faltan las interfaces porque los canales no se admiten en máquinas virtuales de terceros.

Nota:

El número total de instancias que puede aprovisionar en un dispositivo SDX depende de la licencia instalada en el dispositivo.

Importante: Debe actualizar la versión de Citrix Hypervisor a la versión 6.1.0 antes de instalar cualquier instancia de terceros.

SECUREMATRIX GSB

November 23, 2023

SECUREMATRIX es una solución de autenticación de contraseña única (OTP) altamente segura y sin tokens que resulta fácil de usar y rentable. Utiliza una combinación de ubicación, secuencia y patrón de imagen de una tabla matricial para generar una contraseña de un solo uso. El servidor GSB SECUREMATRIX con el servidor de autenticación SECUREMATRIX mejora sustancialmente la seguridad de los puntos finales VPN/SSL-VPN, las aplicaciones y los recursos basados en la nube, el inicio de sesión de escritorio/escritorio virtual y las aplicaciones web (proxy inverso con OTP). Proporciona una solución que es compatible con PC, escritorios virtuales, tabletas y smartphones.

Al utilizar la arquitectura de plataforma multiarrendatario NetScaler SDX en una red definida por software, la función de autenticación segura de SECUREMATRIX se puede integrar con otros arrendatarios o servicios en la nube entregados a través de NetScaler, como Web Interface, Citrix Virtual Apps and Desktops y muchas otras aplicaciones servicios que requieren autenticación.

Para obtener más información, consulte [SECUREMATRIX](#).

Aprovisionar una instancia GSB SECUREMATRIX

SECUREMATRIX GSB requiere un servidor de autenticación SECUREMATRIX que debe configurarse fuera del dispositivo SDX. Seleccione exactamente una interfaz y especifique la configuración de red solo para esa interfaz.

Nota: Las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces. Los canales no se admiten en una instancia GSB de SECUREMATRIX.

Descargue una imagen XVA del sitio web de SECUREMATRIX y cárguela en el dispositivo SDX antes de comenzar a aprovisionar la instancia. Para obtener más información sobre la descarga de una imagen XVA, consulte el sitio web de SECUREMATRIX. Asegúrese de que está utilizando la compilación 118.7 del Servicio de administración o posterior en el dispositivo SDX.

En la ficha **Configuración**, vaya a **SECUREMATRIX GSB > Imágenes de software**.

Para cargar una imagen XVA en el dispositivo SDX:

1. En el panel de detalles, en **Archivos XVA > Acción**, haga clic en **Cargar**.
2. En el cuadro de diálogo que aparece, haga clic en **Examinar** y, a continuación, seleccione el archivo XVA que quiere cargar.
3. Haga clic en **Cargar**. El archivo XVA aparece en el panel Archivos XVA.

Para aprovisionar una instancia de SECUREMATRIX

1. En la ficha **Configuración**, vaya a **SECUREMATRIX GSB > Instancias**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el **asistente Provision SECUREMATRIX GSB**, siga las instrucciones que aparecen en pantalla.
4. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice una configuración detallada. Para obtener más información, consulte el sitio web de [SECUREMATRIX](#).

Para modificar la configuración de una instancia de SECUREMATRIX aprovisionada, en el panel **Instancias de SECUREMATRIX**, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar GSB de SECUREMATRIX, modifique los parámetros.

Nota: Si modificas alguno de los parámetros de la interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para que los cambios surtan efecto.

Genere un archivo tar para enviarlo a la asistencia técnica. Para obtener información sobre cómo generar un archivo de asistencia técnica, consulte [Generación de un archivo TAR para asistencia técnica](#).

Realice una copia de seguridad de la configuración de una instancia GSB de SECUREMATRIX y, posteriormente, utilice los datos de copia de seguridad para restaurar la configuración de la instancia en el dispositivo SDX. Para obtener información sobre cómo realizar copias de seguridad y restaurar una instancia, consulte [Copia de seguridad y restauración de los datos de configuración del dispositivo SDX](#).

Supervisar una instancia GSB SECUREMATRIX

El dispositivo SDX recopila estadísticas, como la versión de [SDXTools](#), los estados de los demonios SSH y CRON, y el estado del servidor web, de una instancia GSB de SECUREMATRIX.

Para ver las estadísticas relacionadas con una instancia GSB de SECUREMATRIX:

1. Vaya a **SECUREMATRIX GSB > Instancias**.
2. En el panel de detalles, haga clic en la flecha junto al nombre de la instancia.

Administrar una instancia GSB de SECUREMATRIX

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia GSB de SECUREMATRIX desde el Servicio de administración.

En la ficha **Configuración**, expanda **SECUREMATRIX GSB**.

Para iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia en la que quiere realizar la operación y, a continuación, seleccione una de las siguientes opciones:
 - Iniciar
 - Apagar
 - Reiniciar
 - Forzar apagado
 - Reinicio forzado
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Actualizar el archivo de herramientas SDX para una instancia GSB de SECUREMATRIX

[SDXTools](#), un demonio que se ejecuta en la instancia GSB de SECUREMATRIX, se utiliza para la comunicación entre Management Service y la instancia.

La actualización de [SDXTools](#) implica cargar el archivo en el dispositivo SDX y, a continuación, actualizar [SDXTools](#) después de seleccionar una instancia. Puede cargar un archivo [SDXTools](#) desde un equipo cliente en el dispositivo SDX.

Para cargar un archivo de SDXTools:

1. En el panel de navegación, expanda **Servicio de administración** y, a continuación, haga clic en **Archivos de SDXTools**.
2. En el panel de detalles, en la lista **Acción**, seleccione **Cargar**.

3. En el cuadro de diálogo **Cargar archivos de SDXTools**, haga clic en **Examinar**, desplácese hasta la carpeta que contiene el archivo y, a continuación, haga doble clic en el archivo.
4. Haga clic en **Cargar**.

Para actualizar SDXTools:

En la ficha **Configuración**, expanda **SECUREMATRIX GSB**.

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione una instancia.
3. En la lista **Acciones**, seleccione **Actualizar SDXTools**.
4. En el cuadro de diálogo **Actualizar SDXTools**, seleccione un archivo, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Actualizar y degradar una instancia GSB de SECUREMATRIX

El proceso de actualización de la instancia GSB de SECUREMATRIX implica cargar la imagen de software de la compilación de destino en el dispositivo SDX y, a continuación, actualizar la instancia. Al cambiar a una versión anterior, se carga una versión anterior de la instancia.

En la ficha **Configuración**, expanda **SECUREMATRIX GSB**.

Para cargar la imagen del software:

1. Haga clic en **Imágenes de software**.
2. En el panel de detalles, en la lista **Acción**, seleccione **Cargar**.
3. En el cuadro de diálogo, haga clic en **Examinar**, vaya a la carpeta que contiene el archivo de compilación y, a continuación, haga doble clic en el archivo de compilación.
4. Haga clic en **Cargar**.

Para actualizar la instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione una instancia.
3. En la lista **Acción**, seleccione **Actualizar**.
4. En el cuadro de diálogo que aparece, seleccione un archivo, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Para degradar una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione una instancia.
3. En la lista **Acción**, seleccione **Reducir**.
4. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Solución de problemas de una instancia GSB de SECUREMATRIX

Haga ping a una instancia GSB de SECUREMATRIX desde el Servicio de administración para comprobar si se puede acceder al dispositivo. Puede realizar un seguimiento de la ruta de un paquete desde el Servicio de administración a una instancia para determinar el número de saltos implicados en llegar a la instancia.

Redescubra una instancia para ver el estado y la configuración más recientes de una instancia. Durante la redetección, el Servicio de administración obtiene la configuración y la versión de SECUREMATRIX GSB que se ejecuta en el dispositivo SDX. De forma predeterminada, Management Service programa las instancias para redescubrimiento una vez cada 30 minutos.

En la ficha **Configuración**, expanda **SECUREMATRIX GSB**.

Para hacer ping a una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia a la que quiere hacer ping y, en la lista **Acción**, haga clic en **Ping**. El mensaje Ping muestra si el ping se ha realizado correctamente.

Para rastrear la ruta de una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia para la que quiere rastrear la ruta y, en la lista **Acción**, haga clic en **TraceRoute**. El cuadro de mensajes de Traceroute muestra la ruta a la instancia.

Para detectar de nuevo una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia que quiere redescubrir y, en la lista **Acción**, haga clic en **Redescubrir**.
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Seguridad web de Trend Micro InterScan

November 23, 2023

Trend Micro InterScan Web Security es un dispositivo virtual de software que protege dinámicamente contra las amenazas web tradicionales y emergentes en la puerta de enlace de Internet. Integra el control de aplicaciones, el análisis antimalware, la reputación web en tiempo real, el filtrado flexible de URL y la protección avanzada contra amenazas. Como resultado, ofrece una protección superior y una mayor visibilidad y control sobre el uso creciente de aplicaciones basadas en la nube en la red.

Los informes en tiempo real y la gestión centralizada brindan a sus administradores una herramienta de toma de decisiones proactiva, lo que permite la gestión de riesgos en

InterScan Web Security:

- Permite una mayor visibilidad de la actividad de Internet del usuario final
- Centraliza la administración para un control máximo
- Supervisa el uso web a medida que ocurre
- Permite la corrección in situ
- Reduce la expansión del dispositivo y los costes de energía
- Proporciona protección opcional contra la pérdida de datos y análisis de ejecución de sandbox

Antes de poder aprovisionar una instancia de InterScan Web Security, debe descargar una imagen XVA del sitio web de Trend Micro. Después de descargar la imagen XVA, cárguela en el dispositivo NetScaler SDX.

Nota: Las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces. Los canales no se admiten en una instancia de InterScan Web Security.

Para cargar una imagen XVA en el dispositivo SDX:

1. En la ficha **Configuración**, vaya a **TrendMicro IWSVA > Imágenes de software**.
2. En el panel de detalles, en la ficha **Archivos XVA**, haga clic en **Cargar**.
3. En el cuadro de diálogo que aparece, haga clic en **Examinar** y, a continuación, seleccione el archivo XVA que quiere cargar.
4. Haga clic en **Cargar**. El archivo XVA aparece en el panel Archivos XVA.

Para aprovisionar una instancia IWSVA de TrendMicro:

1. En la ficha **Configuración**, vaya a **TrendMicro IWSVA > Instancias**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el asistente **Provision TrendMicro IWSVA**, siga las instrucciones que aparecen en pantalla.
4. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice la configuración detallada.

Para modificar los valores de los parámetros de una instancia aprovisionada, en el panel de detalles, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente **Modificar IWSVA de TrendMicro**, defina los parámetros en valores adecuados para su entorno.

Protector de Websense

November 23, 2023

El protector de seguridad de datos de Websense (ahora conocido como Forcepoint) es una máquina virtual que intercepta el tráfico HTTP saliente (publicaciones). Luego, analiza el tráfico para evitar la pérdida de datos y la filtración de datos confidenciales en la web. El protector se comunica con un servidor Windows dedicado para obtener información de directivas de DLP y puede supervisar o bloquear la publicación de datos cuando se detecta una coincidencia. El análisis de contenido se realiza en la caja, por lo que ningún dato confidencial sale del protector durante este proceso.

Para utilizar las capacidades de prevención de pérdida de datos (DLP) del protector, haga lo siguiente:

- Adquiera e instale Websense Data Security
- Configurar directivas de Web DLP en el administrador de seguridad de datos
- Realice la configuración inicial a través del Servicio de administración.

Para obtener más información, consulte el sitio web de [Websense Protector](#).

Aprovisionar una instancia de Websense Protector

El protector de Websense® requiere un servidor de administración de seguridad de datos que debe configurarse fuera del dispositivo SDX. Seleccione exactamente una interfaz de administración y dos interfaces de datos. Para las interfaces de datos, debe seleccionar Permitir modo L2. Compruebe que se puede acceder a Data Security Management Server a través de la red de administración del protector de Websense. Para el servidor de nombres, escriba la dirección IP del servidor de nombres de dominio (DNS) que sirve este protector.

Nota: Las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces. Los canales no se admiten en una instancia de protector de Websense.

Descargue una imagen de protector del sitio web de Websense y cárguela en el dispositivo SDX antes de comenzar a aprovisionar la instancia. Para obtener más información sobre la descarga de una imagen de protector, consulte el sitio web de [Websense. Asegúrese de que está utilizando la compilación 118.7 del Servicio de administración o posterior en el dispositivo SDX.

En la ficha **Configuración**, vaya a **Websense Protector > Imágenes de software**.

Para cargar una imagen XVA en el dispositivo SDX

1. En el panel de detalles, en **Archivos XVA > Acción**, haga clic en **Cargar**.
2. En el cuadro de diálogo que aparece, haga clic en Examinar y, a continuación, seleccione el archivo XVA que quiere cargar.
3. Haga clic en **Cargar**. El archivo XVA aparece en el panel Archivos XVA.

Para aprovisionar una instancia del protector de Websense

1. En la ficha **Configuración**, vaya a **Websense Protector > Instancias**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el asistente **Provision Websense Protector**, siga las instrucciones que aparecen en pantalla.
4. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice la configuración detallada.

Para modificar la configuración de una instancia de protector de Websense aprovisionada, en el panel Instancias de protector de Websense, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar protector de Websense, defina los parámetros. No modifique las interfaces que se seleccionaron en el momento de aprovisionar una instancia de Websense. El archivo XVA solo se puede cambiar después de eliminar la instancia y aprovisionar una nueva.

Puede generar un archivo tar para enviarlo a la asistencia técnica. Para obtener información sobre cómo generar un archivo de asistencia técnica, consulte [Generación de un archivo TAR para asistencia técnica](#).

Supervisar una instancia de Websense Protector

El dispositivo SDX recopila estadísticas, como la versión de [SDXTools](#), el estado del motor de directivas de seguridad de datos Websense© y el estado del proxy de seguridad de datos.

Para ver las estadísticas relacionadas con una instancia del protector de Websense:

1. Vaya a **Websense Protector > Instancias**.
2. En el panel de detalles, haga clic en la flecha junto al nombre de la instancia.

Administrar una instancia de Websense Protector

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia del protector de Websense© desde el Servicio de administración.

En la ficha **Configuración**, expanda **Protector de Websense**.

Para iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia del protector de Websense

1. Pulse en **Instancias**.

2. En el panel de detalles, seleccione la instancia en la que quiere realizar la operación y, a continuación, seleccione una de las siguientes opciones:
 - Iniciar
 - Apagar
 - Reiniciar
 - Forzar apagado
 - Reinicio forzado
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Actualizar el archivo de herramientas SDX para una instancia de Websense Protector

SDXTools, un demonio que se ejecuta en la instancia de terceros, se utiliza para la comunicación entre Management Service y la instancia de terceros.

La actualización de **SDXTools** implica cargar el archivo en el dispositivo SDX y, a continuación, actualizar **SDXTools** después de seleccionar una instancia. Puede cargar un archivo **SDXTools** desde un equipo cliente en el dispositivo SDX.

Para cargar un archivo de herramientas SDX

1. En el panel de navegación, expanda **Servicio de administración** y, a continuación, haga clic en **Archivos de SDXTools**.
2. En el panel de detalles, en la lista **Acción**, seleccione **Cargar**.
3. En el cuadro de diálogo **Cargar archivos de SDXTools**, haga clic en **Examinar**, desplácese hasta la carpeta que contiene el archivo y, a continuación, haga doble clic en el archivo.
4. Haga clic en **Cargar**.

Para actualizar las herramientas SDX

En la ficha **Configuración**, expanda **Protector de Websense**.

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione una instancia.
3. En la lista **Acciones**, seleccione **Actualizar SDXTools**.
4. En el cuadro de diálogo **Actualizar SDXTools**, seleccione un archivo, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Actualizar la instancia de Websense Protector a una versión posterior

El proceso de actualización de la instancia del protector de Websense© implica cargar la imagen de software de la compilación de destino en el dispositivo SDX y, a continuación, actualizar la instancia.

En la ficha **Configuración**, expanda **Protector de Websense**.

Para cargar la imagen del software

1. Haga clic en **Imágenes de software**.
2. En el panel de detalles, en la lista **Acción**, seleccione **Cargar**.
3. En el cuadro de diálogo, haga clic en **Examinar**, vaya a la carpeta que contiene el archivo de compilación y, a continuación, haga doble clic en el archivo de compilación.
4. Haga clic en **Cargar**.

Para actualizar la instancia

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione una instancia.
3. En la lista **Acción**, selecciona **Actualizar**.
4. En el cuadro de diálogo que aparece, seleccione un archivo, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Solucionar problemas de una instancia de Websense Protector

Haga ping a una instancia de protector de Websense desde el Servicio de administración para comprobar si se puede acceder al dispositivo. Puede realizar un seguimiento de la ruta de un paquete desde el Servicio de administración a una instancia para determinar el número de saltos implicados en llegar a la instancia.

Redescubra una instancia para ver el estado y la configuración más recientes de una instancia. Durante el redescubrimiento, Management Service recupera la configuración y la versión del protector de Websense que se ejecuta en el dispositivo SDX. De forma predeterminada, Management Service programa las instancias para redescubrimiento una vez cada 30 minutos.

En la ficha **Configuración**, expanda **Protector de Websense**.

Para hacer ping a una instancia

1. Pulse en **Instancias**.

2. En el panel de detalles, seleccione la instancia a la que quiere hacer ping y, en la lista **Acción**, haga clic en **Ping**. El mensaje Ping muestra si el ping se ha realizado correctamente.

Para rastrear la ruta de una instancia

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia para la que quiere rastrear la ruta y, en la lista **Acción**, haga clic en **TraceRoute**. El cuadro de mensajes de Traceroute muestra la ruta a la instancia.

Para redescubrir una instancia

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia que quiere redescubrir y, en la lista **Acción**, haga clic en **Redescubrir**.
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

DNS y DHCP de BlueCat

November 23, 2023

BlueCat DNS/DHCP Server™ es una solución de software compatible con el dispositivo NetScaler SDX. Se aloja en la plataforma NetScaler SDX para ofrecer servicios de red principales de DNS y DHCP fiables, escalables y seguros sin incurrir en costes de administración adicionales ni en espacio en el centro de datos. Los servicios DNS críticos se pueden equilibrar en carga en varios nodos DNS dentro de un solo sistema o en varios dispositivos SDX sin necesidad de más hardware.

Las instancias virtuales de BlueCat DNS/DHCP Server™ se pueden alojar en SDX para proporcionar una forma más inteligente de conectar dispositivos móviles, aplicaciones, entornos virtuales y nubes.

Para obtener más información sobre BlueCat y Citrix, visite el sitio web de BlueCat en <https://citrixready.citrix.com/bluecat-networks.html>.

Si ya es cliente de BlueCat, puede descargar software y documentación a través del portal de asistencia de BlueCat en <https://care.bluecatnetworks.com/>.

Aprovisionamiento de una instancia de BlueCat DNS/DHCP

Descargue una imagen XVA del Servicio de atención al cliente de BlueCat, en <https://care.bluecatnetworks.com>. Después de descargar la imagen XVA, cárguela en el dispositivo SDX antes de empezar

a aprovisionar la instancia. Asegúrese de que está utilizando la compilación 118.7 del Servicio de administración o posterior en el dispositivo SDX.

El canal de administración a través de interfaces 0/1 y 0/2 se admite en las VM de BlueCat DNS/DHCP. Para obtener más información, consulte [Configuración del canal desde el Servicio de administración](#).

Nota: Las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces porque los canales no son compatibles con una instancia de BlueCat DNS/DHCP.

En la ficha **Configuración**, vaya a **BlueCat DNS/DHCP > Imágenes de software**.

Para cargar una imagen XVA al dispositivo SDX:

1. En el panel de detalles, en **Archivos XVA > Acción**, haga clic en **Cargar**.
2. En el cuadro de diálogo que aparece, haga clic en **Examinar** y, a continuación, seleccione el archivo XVA que quiere cargar.
3. Haga clic en **Cargar**. El archivo XVA aparece en el panel Archivos XVA.

Para aprovisionar una instancia de BlueCat DNS/DHCP:

1. En la ficha Configuración, vaya a BlueCat DNS/DHCP > Instancias.
2. En el panel de detalles, haga clic en Agregar. Se abrirá la página Aprovisionar BlueCat DNS/DHCP Server.
3. En el asistente Aprovisionar BlueCat DNS/DHCP, siga las instrucciones que aparecen en pantalla.
 - En Creación de instancias, en el campo Nombre, introduzca un nombre para la instancia y seleccione la imagen cargada en el menú desplegable Archivo XVA y, a continuación, haga clic en Siguiente. Si lo quiere, en el campo Nombre de dominio, introduzca un nombre de dominio para la instancia.

Nota: El nombre no debe contener espacios.
 - En Configuración de red, en el menú desplegable Interfaz de administración, seleccione la interfaz a través de la cual administrar la instancia, establezca la dirección IP y la puerta de enlace para esa interfaz. Puede asignar interfaces de forma explícita para obtener alta disponibilidad y servicio. Seleccione los parámetros y haga clic en **Siguiente**.

Nota: Al asignar interfaces para administración, alta disponibilidad y servicio, asegúrese de asignar las interfaces en función de la combinación de interfaces admitida:

Puede seleccionar la misma interfaz para las tres.

Puede seleccionar una interfaz diferente para las tres.

Puede seleccionar la misma interfaz para la administración y el servicio, pero seleccionar una interfaz diferente para la alta disponibilidad.

Haga clic en **Finalizar** y, a continuación, en **Cerrar**. La instancia se crea, arranca y configura con la dirección IP seleccionada.

Después de aprovisionar la instancia, inicie sesión en la instancia a través de SSH para completar la configuración. Para obtener más información sobre la configuración del servidor DNS/DHCP de

BlueCat o ponerlo bajo el control de BlueCat Address Manager, consulte la documentación de BlueCat, disponible en <https://care.bluecatnetworks.com>.

Para modificar la configuración de una instancia del servidor DNS/DHCP de BlueCat, **en el panel Instancias de BlueCat DNS/DHCP**, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar BlueCat DNS/DHCP, modifique los parámetros.

Nota: Si modificas alguno de los parámetros de la interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para que los cambios surtan efecto.

Supervisar una instancia de BlueCat DNS/DHCP

El dispositivo SDX recopila estadísticas, como la versión de **SDXTools** activa en la instancia, de una instancia de BlueCat DNS/DHCP.

Para ver las estadísticas relacionadas con una instancia de BlueCat DNS/DHCP:

1. Vaya a BlueCat DNS/DHCP > Instancias.
2. En el panel de detalles, haga clic en la flecha junto al nombre de la instancia.

Administrar una instancia de DNS/DHCP de BlueCat

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de BlueCat DNS/DHCP desde el Servicio de administración.

En la ficha **Configuración**, expanda **BlueCat DNS/DHCP**.

Para iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de BlueCat DNS/DHCP:

1. Pulse en Instancias.
2. En el panel de detalles, seleccione la instancia en la que quiere realizar la operación y, a continuación, seleccione una de las siguientes opciones:
 - Iniciar
 - Apagar
 - Reiniciar
 - Forzar apagado
 - Reinicio forzado
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Actualizar el archivo SDXTools para una instancia de DNS/DHCP de BlueCat

SDXTools, un demonio que se ejecuta en la instancia de terceros, se utiliza para la comunicación entre Management Service y la instancia de terceros.

La actualización de **SDXTools** implica cargar el archivo en el dispositivo SDX y, a continuación, actualizar **SDXTools** después de seleccionar una instancia. Puede cargar un archivo **SDXTools** desde un equipo cliente en el dispositivo SDX.

Para cargar un archivo de SDXTools:

1. En el panel de navegación, expanda **Servicio de administración** y, a continuación, haga clic en **Archivos de SDXTools**.
2. En el panel de detalles, en la lista **Acción**, seleccione **Cargar**.
3. En el cuadro de diálogo **Cargar archivos de SDXTools**, haga clic en **Examinar**, desplácese hasta la carpeta que contiene el archivo y, a continuación, haga doble clic en el archivo.
4. Haga clic en **Cargar**.

Para actualizar SDXTools:

En la ficha **Configuración**, expanda **BlueCat DNS/DHCP**.

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione una instancia.
3. En la lista de acciones, seleccione **Actualizar SDXTools**.
4. En el cuadro de diálogo **Actualizar SDXTools**, seleccione un archivo, haga clic en **Aceptar** y, a continuación, haga clic en **Cerrar**.

Redescubra una instancia de BlueCat DNS/DHCP

Puede volver a descubrir una instancia para ver el estado y la configuración más recientes de una instancia. Durante el redescubrimiento, Management Service recupera la configuración. De forma predeterminada, Management Service programa las instancias para el redescubrimiento de todas las instancias una vez cada 30 minutos.

En la ficha **Configuración**, expanda **BlueCat DNS/DHCP**.

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia que quiere redescubrir y, en la lista **Acción**, haga clic en **Redescubrir**.
3. En el cuadro de mensaje **Confirmar**, haga clic en **Sí**.

CA Access Gateway

November 23, 2023

CA Access Gateway es un servidor independiente escalable, administrable y ampliable que proporciona una solución basada en proxy para el control de acceso. CA Access Gateway emplea un motor proxy que proporciona una puerta de enlace de red para la empresa y admite varios esquemas de sesión que no se basan en la tecnología tradicional basada en cookies.

El agente web integrado permite el inicio de sesión único (SSO) en toda la empresa. CA Access Gateway proporciona control de acceso para solicitudes HTTP y HTTPS y SSO sin cookies. Además, el producto almacena la información de la sesión en el almacén de sesiones en memoria. Las reglas de proxy definen cómo CA Access Gateway reenvía o redirige las solicitudes a los recursos ubicados en los servidores de destino dentro de la empresa.

Al proporcionar una puerta de enlace única para los recursos de red, CA Access Gateway separa la red corporativa y centraliza el control de acceso.

Nota: Las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces porque los canales no se admiten en una instancia de CA Access Gateway. Para obtener más información sobre las funciones de CA Access Gateway, consulte la documentación de ese producto.

Proporcionar una instancia de CA Access Gateway

Antes de poder aprovisionar una instancia de CA Access Gateway, debe descargar una imagen XVA. Después de descargar la imagen XVA, cárguela en el dispositivo SDX. Asegúrese de que está utilizando la versión 10.5, compilación 52.3.e del Servicio de administración o posterior en el dispositivo SDX. Para aprovisionar una instancia de CA Access Gateway, primero debe cargar la imagen XVA en el dispositivo SDX y, a continuación, aprovisionar una instancia.

Para cargar una imagen XVA en el dispositivo SDX:

1. En la ficha **Configuración**, vaya a **CA Access Gateway > Imágenes de software**.
2. En el panel de detalles, en **Archivos XVA**, en la lista desplegable **Acción**, haga clic en **Cargar**.
3. En el cuadro de diálogo que aparece, haga clic en **Examinar** y, a continuación, seleccione el archivo XVA que quiere cargar.
4. Haga clic en **Cargar**. El archivo XVA aparece en el panel Archivos **XVA**.

Para aprovisionar una instancia de CA Access Gateway:

1. En la ficha **Configuración**, vaya a **CA Access Gateway > Instancias**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el asistente Aprovisionar CA Access Gateway, siga las instrucciones que aparecen en pantalla.

4. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice la configuración detallada.

Para modificar los valores de los parámetros de una instancia aprovisionada, en el panel de detalles, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar CA Access Gateway, establezca los parámetros en valores adecuados para su entorno.

Nota:

Si modifica cualquiera de los parámetros de la interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para que el cambio entre en vigor.

Supervisión de una instancia de CA Access Gateway

El dispositivo SDX recopila estadísticas, como la versión de [SDXTools](#) activa en la instancia, de una instancia de CA Access Gateway.

Para ver las estadísticas relacionadas con una instancia de CA Access Gateway:

1. Desplácese hasta **CA Access Gateway > Instancias**.
2. En el panel de detalles, haga clic en la flecha junto al nombre de la instancia.

Administrar una instancia de CA Access Gateway

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de CA Access Gateway desde el Servicio de administración. Para completar estas tareas, siga estos pasos:

1. En la ficha **Configuración**, expanda **CA Access Gateway**.
2. Desplácese hasta **CA Access Gateway > Instancias**.
3. En el panel de detalles, seleccione la instancia en la que quiere realizar la operación y, a continuación, seleccione una de las siguientes opciones:
 - Iniciar
 - Apagar
 - Reiniciar
 - Forzar apagado
 - Reinicio forzado
4. En el cuadro Confirmar mensaje, haga clic en **Sí**.

VM-Series de Palo Alto Networks

November 23, 2023

Los firewalls virtuales de VM-Series de Palo Alto Networks utilizan el mismo conjunto de funciones PAN-OS que está disponible en los dispositivos de seguridad física de la empresa, proporcionando todas las funciones clave de seguridad de red. La serie VM de NetScaler SDX permite la consolidación de las capacidades avanzadas de seguridad y ADC en una única plataforma, para que las empresas, las unidades de negocio y los clientes proveedores de servicios accedan de forma segura y confiable a las aplicaciones. La combinación de la serie VM en NetScaler SDX también proporciona una solución ADC y de seguridad completa y validada para las implementaciones de Citrix Virtual Apps and Desktops.

Puede aprovisionar, supervisar, administrar y solucionar problemas de una instancia desde el Servicio de administración.

Puntos a tener en cuenta:

- El número total de instancias que puede aprovisionar en un dispositivo SDX depende de los recursos de hardware SDX disponibles.
- Las interfaces SR-IOV (1/x y 10/x) que forman parte de un canal no aparecen en la lista de interfaces porque los canales no se admiten en una instancia de la serie VM de Palo Alto. Para obtener más información sobre la serie VM de Palo Alto Network, consulte la [documentación de Palo Alto Network](#).

Aprovisionar una instancia de la serie VM de Palo Alto

Antes de poder aprovisionar una instancia de la serie VM de Palo Alto, debe descargar una imagen XVA del [sitio web de Palo Alto Networks](#). Después de descargar la imagen XVA, cárguela en el dispositivo SDX.

Para cargar una imagen XVA en el dispositivo SDX:

1. En la ficha **Configuración**, vaya a **PaloAlto VM-Series > Imágenes de software**.
2. En el panel de detalles, en **Archivos XVA**, en la lista desplegable **Acción**, haga clic en **Cargar**.
3. En el cuadro de diálogo que aparece, haga clic en **Examinar** y, a continuación, seleccione el archivo XVA que quiere cargar.
4. Haga clic en **Cargar**. El archivo XVA aparece en el panel Archivos **XVA**.

Para aprovisionar una instancia de la serie VM de Palo Alto:

1. En la ficha **Configuración**, vaya a **PaloAlto VM-Series > Instancias**.
2. En el panel de detalles, haga clic en **Agregar**.

3. En el asistente Aprovisionar PaloAlto VM-Series, siga las instrucciones que aparecen en pantalla.
4. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice la configuración detallada.

Para modificar los valores de los parámetros de una instancia aprovisionada, en el panel de detalles, seleccione la instancia que quiere modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar VM-Series de PaloAlto, defina los parámetros en valores adecuados para su entorno.

Nota: Si modificas cualquiera de los parámetros de la interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para que el cambio entre en vigor.

Supervisar una instancia de la serie VM de Palo Alto

El dispositivo SDX recopila estadísticas, como la versión de [SDXTools](#) activa en la instancia, de una instancia de la serie VM de Palo Alto.

Para ver las estadísticas relacionadas con una instancia de la serie VM de Palo Alto:

1. Diríjase a **PaloAlto VM-Series**> Instancias.
2. En el panel de detalles, haga clic en la flecha junto al nombre de la instancia.

Administrar una instancia de la serie VM de PaloAlto

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de VM-Series de PaloAlto desde el Servicio de administración.

En la ficha **Configuración**, expanda la **Serie VM de PaloAlto**.

1. Diríjase a **PaloAlto VM-Series**> Instancias.
2. En el panel de detalles, seleccione la instancia en la que quiere realizar la operación y, a continuación, seleccione una de las siguientes opciones:
 - Iniciar
 - Apagar
 - Reiniciar
 - Forzar apagado
 - Reinicio forzado
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Solucionar problemas de una instancia de la serie VM de PaloAlto

Haga ping a una instancia de la serie VM de PaloAlto desde el Servicio de administración para comprobar si se puede acceder al dispositivo. Puede realizar un seguimiento de la ruta de un paquete desde el Servicio de administración a una instancia para determinar el número de saltos implicados en llegar a la instancia.

Redescubra una instancia para ver el estado y la configuración más recientes de una instancia. Durante el redescubrimiento, Management Service recupera la configuración y la versión de VM-Series PaloAlto que se ejecuta en el dispositivo SDX. De forma predeterminada, Management Service programa las instancias para redescubrimiento una vez cada 30 minutos.

En la ficha **Configuración**, expanda la **Serie VM de PaloAlto**.

Para hacer ping a una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia a la que quiere hacer ping y, en la lista **Acción**, haga clic en **Ping**. El mensaje Ping** muestra si el ping se ha realizado correctamente.

Para rastrear la ruta de una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia a la que quiere hacer ping y, en la lista **Acción**, haga clic en **TraceRoute**. El cuadro de mensajes de **Traceroute** muestra la ruta a la instancia.

Para detectar de nuevo una instancia:

1. Pulse en **Instancias**.
2. En el panel de detalles, seleccione la instancia que quiere redescubrir y, en la lista **Acción**, haga clic en **Redescubrir**.
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Implemente una instancia Citrix SD-WAN VPX en un dispositivo NetScaler SDX

November 23, 2023

La tecnología Citrix SD-WAN aplica conceptos de redes definidas por software (SDN) a las conexiones WAN. La tecnología abstrae la administración y la supervisión del tráfico del hardware de red y las aplica a aplicaciones individuales. El resultado es un rendimiento mejorado, experiencias de usuario de alta calidad en ubicaciones geográficamente dispersas y una implementación simplificada de redes de área amplia y acceso a la nube. Para obtener más información, consulte [Citrix SD-WAN](#).

Nota: Solo se admite la edición SD-WAN VPX Standard. Para obtener más información, consulte [Ediciones VPX de SD-WAN](#).

La implementación de una instancia VPX de Citrix SD-WAN en un dispositivo SDX incluye las siguientes tareas:

- Instalación del hardware: Asegúrese de que el hardware SDX esté correctamente instalado. Para obtener más información, consulte [Instalación del hardware](#).
- Instalación y configuración de SDX Management Service. Para obtener más información, consulte [Introducción a la interfaz de usuario del Servicio de administración](#) y [Configuración del Servicio de administración](#).
- Aprovisionamiento de la instancia VPX de SD-WAN en el dispositivo SDX. Para obtener más información, consulte [Aprovisionar la instancia de Citrix SD-WAN VPX en un NetScaler SDX](#).
- Configuración de la instancia VPX de SD-WAN. Para obtener más información, consulte la documentación de [Configuración](#) y [Configuración del servicio de ruta virtual entre el MCN y los sitios del cliente](#).

Requisitos previos

Asegúrese de tener las siguientes licencias:

- Licencia VPX de Citrix SD-WAN
- Licencia de plataforma NetScaler SDX

Requisitos de Citrix SD-WAN VPX

Citrix SD-WAN VPX en la plataforma SDX puede actuar como un sitio y como MCN. El MCN puede gestionar un rendimiento bidireccional de 1 Gb/s y 64 sitios.

Rendimiento admitido para MCN y sitio

- Rendimiento bidireccional de 250 MB/s a 1 Gb/s
- MCN admite 64 sitios

Requisito de hardware para rendimiento admitido Sitio

- 4 CPUs a 16 CPUs
- RAM de 4 GB a 16 GB
- Almacenamiento en disco de 60 GB a 250 GB
- Mínimo 4 NICs: Una para administración y un mínimo restante 3 para ruta de datos

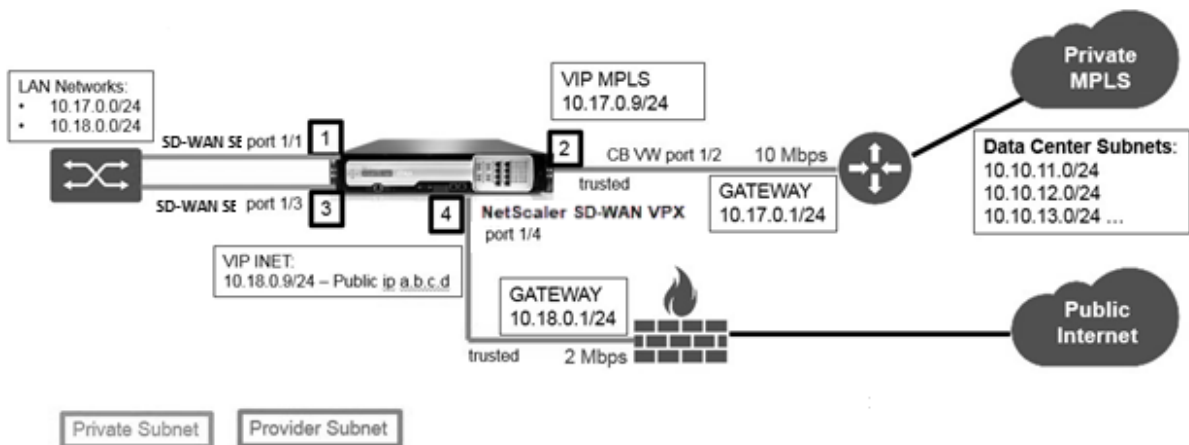
Nodo de control maestro (MCN)

- 4, 8 y 16 CPU
- 16 GB de RAM
- Almacenamiento en disco de 250 GB
- Mínimo 4 NIC: Una para administración y 3 restantes para ruta de datos, con NICs dedicadas para ruta de datos

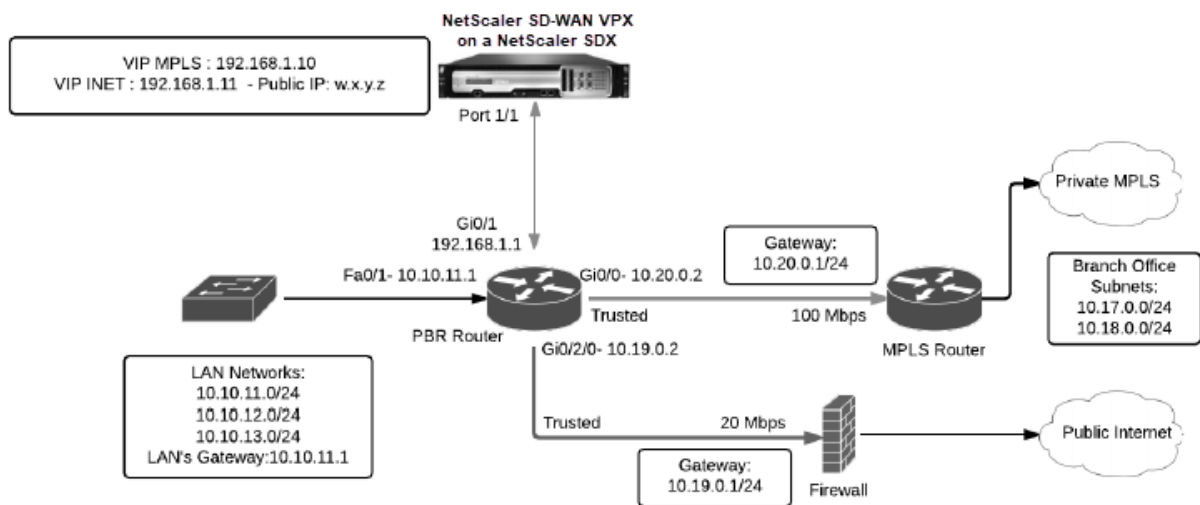
Topología del centro de datos

Puede implementar un dispositivo Citrix SD-WAN VPX en un NetScaler SDX en modo de ruta basada en políticas (PBR) o en modo en línea. Consulte los casos 1 y 2 para conocer la topología del centro de datos para estos dos modos compatibles. Para obtener más información, consulte [Implementación de SD-WAN en modo virtual en línea](#).

Caso 1: modo en línea



Caso 2: modo PBR o modo virtual en línea



Aprovisione la instancia de Citrix SD-WAN VPX en un NetScaler SDX

Antes de aprovisionar el dispositivo Citrix SD-WAN VPX, descargue la imagen SD-WAN VPX del sitio de descargas de productos de NetScaler.:

<https://www.citrix.com/downloads/netscaler-sd-wan/>

Siga estos pasos para aprovisionar el dispositivo Citrix SD-WAN VPX.

1. Inicie sesión en el dispositivo NetScaler SDX.
2. Vaya a **Configuración > SD-WAN > Instancias**.
3. Seleccione **Imágenes de software > Cargar** y cargar el archivo XVA de SD-WAN.



4. Seleccione **Instancias > Agregar**. Aparecerá la página **Aprovisionar instancia de SD-WAN**.
5. En la página **Aprovisionar instancias de SD-WAN**, introduzca lo siguiente:
 - a. Nombre
 - b. Dirección IP
 - c. Máscara de red
 - d. Dirección de la puerta de enlace
 - e. Cargar el archivo XVA
 - f. En **Asignación de recursos**, asigne recursos.

Resource Allocation
Total Memory (MB)*
<input type="text" value="4096"/>
CPU Cores*
<input type="text" value="Dedicated (4 CPU)"/>

- g. En **Configuración de red**, provisione interfaces de administración y seleccione **Aceptar** para crear para aprovisionar la instancia VPX de SD-WAN en el dispositivo SDX.

Nota: El Servicio de administración SDX vincula las interfaces a la instancia VPX en la secuencia ascendente de nombres de interfaz. Por ejemplo, si agrega 1/4 y 1/1, Management Service los organiza como 1/1, 1/4.

Al agregar nuevas interfaces, se conserva la secuencia existente y se crea una nueva secuencia. Por ejemplo, se agregan interfaces 1/2, 10/1, 1/3. La nueva secuencia sería 1/1, 1/4; 1/2, 1/3, 10/1.

6. La instancia VPX de SD-WAN aparece en la **página Instancia**. He aquí un ejemplo.

1 ! [Image] (/en-us/sdx/media/sd-wan-vpx-example.png)

Para modificar la instancia, vaya a **Configuración > SD-WAN > Instancias**. Seleccione y haga clic en la instancia. Una vez que haya completado la modificación, haga clic en **Aceptar** para guardar los cambios.

Configuración de la instancia VPX de Citrix SD-WAN

Después de crear una instancia de SD-WAN en el dispositivo SDX, configure la instancia de SD-WAN completando estas dos tareas:

1. Aplique la configuración tanto para MCN como para los dispositivos de sitio.
2. Configure la ruta virtual y transmita el tráfico.

Para obtener más información, consulte estos temas:

- [Configuración](#)
- [Configuración del servicio de rutas virtuales entre los sitios de MCN y cliente](#)

Información relacionada

Para obtener más información sobre cómo empezar a utilizar un dispositivo Citrix SD-WAN, consulte [Citrix SD-WAN](#).

Para obtener más información sobre el dispositivo NetScaler SDX, consulte [NetScaler SDX](#).

Medición de ancho de banda en SDX

February 15, 2024

La medición del ancho de banda de NetScaler SDX le proporciona un esquema de medición preciso, confiable y fácil de usar que le permite asignar de manera eficiente la capacidad de procesamiento y monetizar el uso del ancho de banda. Se requiere un esquema de medición para asignar de manera óptima el ancho de banda entre varios recursos, teniendo en cuenta que todos los usuarios en todo momento obtienen el ancho de banda asignado.

La asignación de ancho de banda se puede realizar en los dos modos siguientes:

- Ancho de banda dedicado con una tasa de rendimiento fija
- Ancho de banda dedicado con un rendimiento mínimo garantizado y flexibilidad de ancho de banda

Ancho de banda dedicado con una tasa de rendimiento fija

En el método de asignación de ancho de banda, a cada instancia VPX se le asigna un ancho de banda dedicado. La instancia puede usar el ancho de banda hasta el límite establecido. En el modo dedicado, el ancho de banda mínimo y máximo asignado es el mismo. Si durante un período, la instancia VPX requiere más ancho de banda del asignado, en el modo dedicado la instancia no puede aumentar su rendimiento. Este problema puede ser un inconveniente si una instancia VPX atiende solicitudes críticas.

Además, si un dispositivo SDX tiene algunas instancias VPX y algunas de ellas no utilizan el ancho de banda asignado, no puede compartir el ancho de banda no utilizado en modo dedicado. Para superar todos estos desafíos, es útil un ancho de banda dedicado con una velocidad mínima asegurada con la capacidad de aumentar dinámicamente el ancho de banda.

Ancho de banda dedicado con un rendimiento mínimo garantizado y flexibilidad de ancho de banda

En este método de asignación de ancho de banda, a una VPX se le asigna un ancho de banda mínimo garantizado con la flexibilidad de aumentar su ancho de banda hasta un límite preestablecido. El ancho de banda adicional que un VPX puede usar se denomina capacidad de flexibilidad.

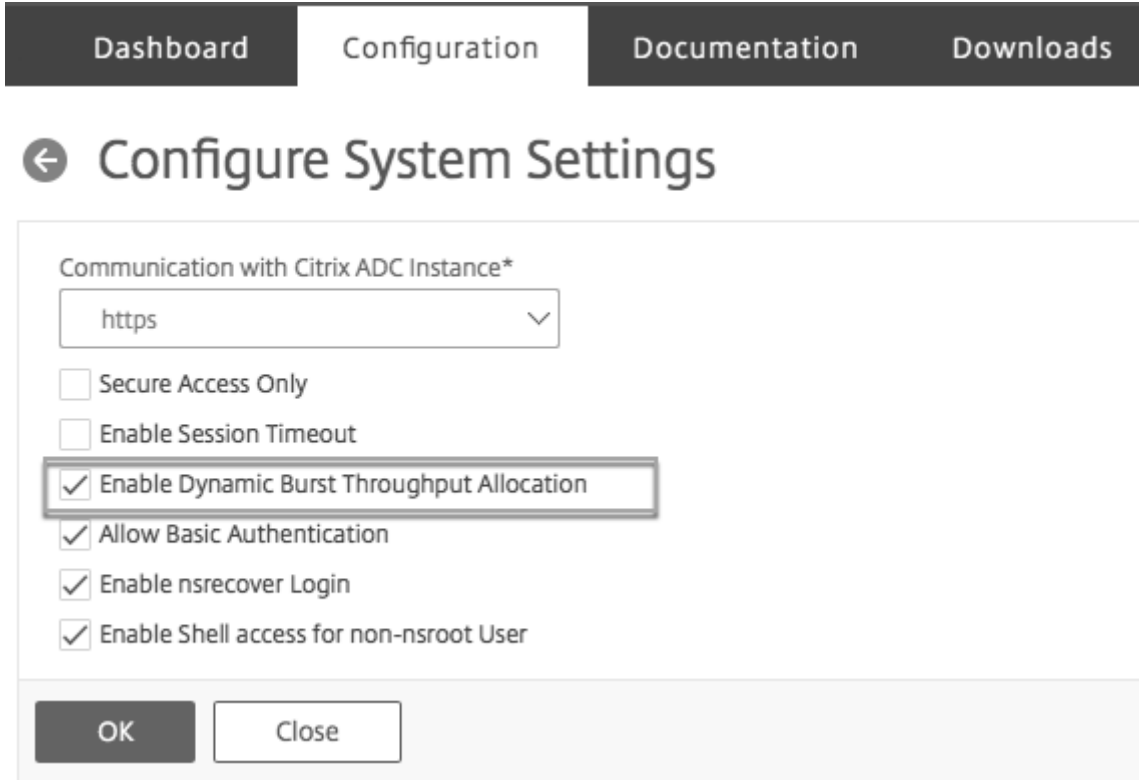
El beneficio de la capacidad de ráfaga se ve cuando tiene algunas instancias que tienen capacidad adicional y algunas VPX con capacidad no utilizada. La capacidad adicional de estas instancias VPX se puede asignar a otras instancias VPX que hayan utilizado por completo su ancho de banda asignado y requieran más durante algún tiempo. Varios proveedores de servicios también están interesados en proporcionar varios servicios adicionales a sus clientes que requieren una capacidad dedicada. Al mismo tiempo, no quieren sobreaprovisionar el ancho de banda. El ancho de banda flexible ayuda en situaciones en las que los clientes tienen la seguridad de un ancho de banda específico con la opción de aumentar el ancho de banda durante períodos de alta demanda.

Cómo seleccionar el modo de asignación de ancho

Antes de elegir el rendimiento flexible, debe habilitar la asignación dinámica de rendimiento de flexibilidad. Para habilitar esta opción, siga estos pasos.

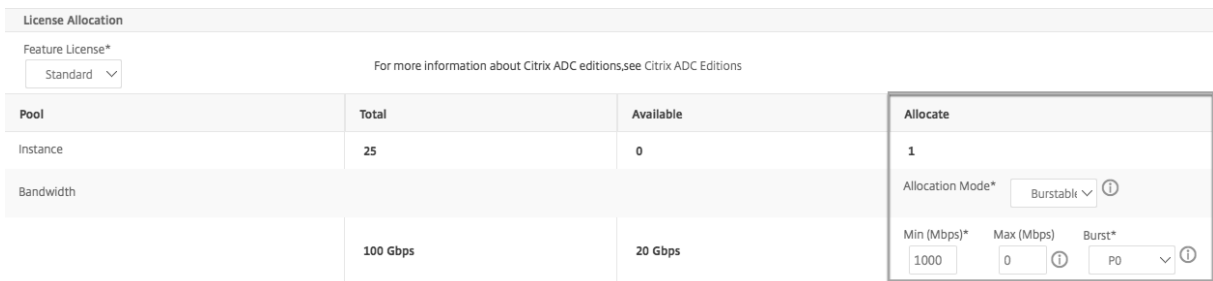
1. En la consola de administración de SDX, vaya a **Configuración > Sistema**.

2. En el grupo **Configuración del sistema**, seleccione **Cambiar configuración del sistema**.
3. Haga clic en la casilla de verificación **Habilitar asignación dinámica de rendimiento de flexibilidad** para habilitar el rendimiento dinámico.



Al aprovisionar una instancia VPX, puede seleccionar la flexibilidad de ancho de banda o un rendimiento dinámico.

1. En el **Servicio de administración de SDX**, haga clic en **Configuración > NetScaler > Instancias > Agregar**.
2. Se abrirá la página **Provisioning NetScaler**. En **Asignación de licencias**, elija **Flexible** en **Modo de asignación**.



Para obtener más información sobre cómo aprovisionar una instancia de NetScaler, consulte [Provisionar instancias de NetScaler](#).

Si quiere utilizar una tasa de rendimiento fija, seleccione **Fijo**. De forma predeterminada, el modo fijo

está configurado para la asignación de ancho de banda. No es necesario que todas las instancias VPX funcionen en el mismo modo. Cada instancia VPX se puede configurar en un modo diferente.

Nota: Si va a migrar SDX desde 10.5.e y versiones anteriores, de forma predeterminada, todas las instancias VPX están en el modo de asignación fija.

Determinar el ancho de banda flexible máximo para una instancia VPX

La extensión en la que se permite que cada VPX se rompa se calcula mediante un algoritmo. Al aprovisionar una instancia VPX con ancho de banda explotable, cada VPX debe recibir una prioridad. La asignación de ancho de banda flexible depende de esta prioridad de flexibilidad. La prioridad varía de P0 a P4, siendo P0 la prioridad más alta y P4 la más baja.

Tomemos un caso en el que hay 2 VPX, a saber, VPX1 y VPX2. El ancho de banda mínimo asignado a VPX1 y VPX2 es de 4 Gbps y 2 Gbps respectivamente con un ancho de banda flexible de 2 Gbps y 1 Gbps cada uno. En la siguiente tabla se muestran los parámetros:

Nombre VPX	Parámetro	Valor
VPX1	Ancho de banda mínimo garantizado	4 Gbps
VPX1	Ancho de banda máximo flexible	2 Gbps
VPX1	Prioridad	P0
VPX2	Ancho de banda mínimo asegurado	2 Gbps
VPX2	Ancho de banda máximo flexible	1 Gbps
VPX2	Prioridad	P1

En este caso, supongamos que el ancho de banda total con licencia es de 8 Gbps. Si ambas instancias VPX llegan a sus límites máximos flexibles, es decir:

1. VPX1 está utilizando su ancho de banda máximo flexible, es decir, 2 Gbps; por lo tanto, está usando un total de $4 + 2 = 6$ Gbps
2. VPX2 está utilizando su ancho de banda máximo flexible, es decir, 1 Gbps; por lo tanto, está usando un total de $2 + 1 = 3$ Gbps

En este caso, el ancho de banda máximo que se utiliza es mayor que la capacidad con licencia de 8 Gbps. Por lo tanto, para reducir el uso a un ancho de banda dentro de la capacidad licenciada, uno de los VPX tendría que renunciar a su ancho de banda flexible. En este caso, ya que VPX2 tiene menor prioridad que VPX1, por lo que renuncia a su ancho de banda flexible de 1 Gbps. VPX1 seguiría siendo flexible ya que tiene mayor prioridad que VPX2. En todos estos casos, se asegura de que siempre se respete el ancho de banda mínimo garantizado.

Comprobación de las estadísticas de rendimiento y consumo de datos

Para cada VPX, puede comprobar las estadísticas de rendimiento y consumo de datos en los gráficos. Para acceder a los gráficos, siga estos pasos:

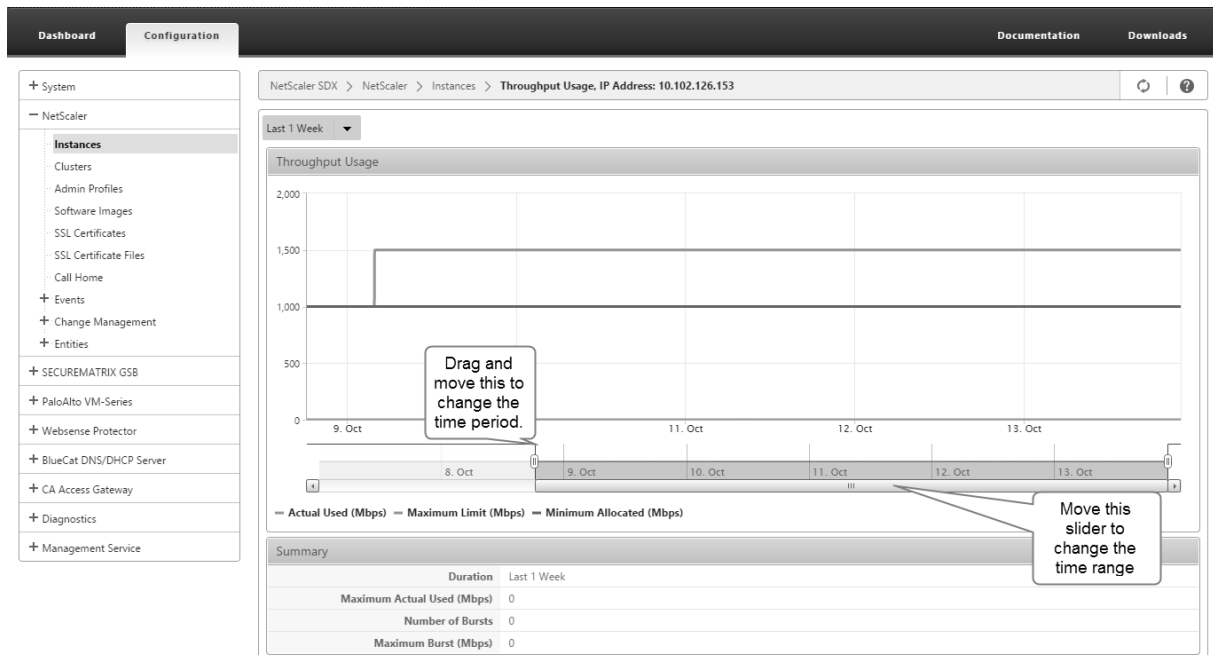
1. Desde el Servicio de administración de SDX, vaya a la página **Configuración > NetScaler > Instancias**.
2. Seleccione una instancia VPX y, a continuación, haga clic en la lista desplegable **Acción**.
3. En la lista, seleccione **Estadísticas de rendimiento** o **Estadísticas de uso de datos**.

Los gráficos le permiten verificar las estadísticas de consumo y rendimiento de datos durante varios períodos de tiempo, como:

- Hace 1 hora
- Hace 1 día
- Hace 1 semana
- Hace 1 mes
- Mes anterior

También puede seleccionar un período de tiempo específico en el gráfico ajustando el control deslizante en la parte inferior del gráfico. Mueva el cursor sobre las líneas del gráfico para comprobar el consumo de datos o el rendimiento de datos durante un tiempo específico.

En la siguiente ilustración se muestra un gráfico de muestra de datos de rendimiento durante 1 semana:



Configurar y administrar instancias de NetScaler

November 23, 2023

Después de aprovisionar las instancias de NetScaler en su dispositivo, estará listo para configurar y administrar las instancias. Comience por crear una dirección IP de subred (SNIP) y, a continuación, guarde la configuración. A continuación, puede realizar tareas de administración básicas en las instancias. Compruebe si tiene que aplicar la configuración de administración.

Advertencia: Asegúrese de modificar las interfaces de red aprovisionadas o las VLAN de una instancia mediante Management Service en lugar de realizar las modificaciones directamente en la instancia.

Crear una dirección SNIP en una instancia de NetScaler

Puede asignar una dirección SNIP a las instancias de NetScaler después de aprovisionarla en el dispositivo SDX.

Se utiliza un SNIP en la administración de conexiones y en la supervisión del servidor. No es obligatorio especificar un SNIP al configurar inicialmente el dispositivo NetScaler SDX. Puede asignar el SNIP a la instancia de NetScaler desde el Servicio de administración.

Para agregar una dirección SNIP a una instancia de NetScaler

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **NetScaler**.
2. En el panel de detalles, en **Configuración de NetScaler**, haga clic en **CrearIP**.
3. En el cuadro de diálogo **Crear IP de NetScaler**, especifique los valores de los siguientes parámetros.
 - **Dirección IP:** especifique la dirección IP asignada como dirección SNIP.
 - **Máscara de red:** especifique la máscara de subred asociada a la dirección SNIP.
 - **Tipo:** de forma predeterminada, el valor es SNIP.
 - **Guardar configuración:** Seleccione esta opción para guardar la configuración en NetScaler. El valor predeterminado es false.
 - **Dirección IP de la instancia:** especifique la dirección IP de la instancia de NetScaler.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Guarda la configuración

Puede guardar la configuración en ejecución de una instancia de NetScaler desde el Servicio de administración.

Para guardar la configuración en una instancia de NetScaler

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **NetScaler**.
2. En el panel de detalles, en **Configuración de NetScaler**, haga clic en **Guardar configuración**.
3. En el cuadro de diálogo **Guardar configuración**, en **Dirección IP de instancia**, seleccione las direcciones IP de las instancias de NetScaler cuya configuración quiere guardar.
4. Haga clic en **Aceptar** y, a continuación, en **Cerrar**.

Administrar una instancia de NetScaler

El Servicio de administración le permite realizar las siguientes operaciones en las instancias de NetScaler. Puede realizar estas operaciones desde el panel **Instancias de NetScaler** en la ficha **Configuración** o desde el gadget de instancias de NetScaler en la página principal.

Iniciar una instancia de NetScaler: inicie cualquier instancia de NetScaler desde la interfaz de usuario del Servicio de administración. Cuando la interfaz de usuario del Servicio de administración reenvía esta solicitud al Servicio de administración, inicia la instancia de NetScaler.

Apagar una instancia de NetScaler: cierre cualquier instancia de NetScaler desde la interfaz de usuario del Servicio de administración. Cuando la interfaz de usuario del Servicio de administración reenvía esta solicitud al Servicio de administración, detiene la instancia de NetScaler.

Reiniciar una instancia de NetScaler: reinicie la instancia de NetScaler.

Eliminar una instancia de NetScaler: Si no quiere usar una instancia de NetScaler, puede eliminar esa instancia mediante Management Service. Al eliminar una instancia, se eliminan permanentemente la instancia y sus detalles relacionados de la base de datos del dispositivo SDX.

Para iniciar, detener, eliminar o reiniciar una instancia de NetScaler

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **Instancias de NetScaler**.
2. Seleccione la instancia de NetScaler en la que quiere realizar la operación y, a continuación, haga clic en **Iniciar** **Apagar** **Eliminar** **Reiniciar**.
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Eliminar archivos de instancia de NetScaler

Puede eliminar del dispositivo cualquier archivo de instancia de NetScaler, como archivos XVA, compilaciones, documentación, claves SSL o certificados SSL.

Para eliminar los archivos de instancia de NetScaler

1. En la ficha **Configuración**, en el panel de navegación, expanda **Configuración de NetScaler** y, a continuación, haga clic en el archivo que quiere quitar.
2. En el panel de detalles, seleccione el nombre del archivo y, a continuación, haga clic en **Eliminar**.

Aplicar la configuración de administración

En el momento de aprovisionar una instancia VPX, el Servicio de administración crea algunas directivas, un perfil de administración (admin) de la instancia y otra configuración en la instancia VPX. Si Management Service no aplica la configuración de administrador, puede enviar explícitamente la configuración desde el Servicio de administración a la instancia VPX. Una de las razones del error puede ser que el Servicio de administración y la instancia VPX estén en subredes diferentes y el enrutador esté inactivo. Otra razón puede ser que ambos están en la misma subred, pero el tráfico tiene que pasar a través de un conmutador externo y uno de los enlaces está inactivo.

Para aplicar la configuración de administración en una instancia de NetScaler

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **NetScaler**.
2. En el panel de detalles, en Configuración de **NetScaler**, haga clic en **Aplicar configuración de administración**.
3. En el cuadro de diálogo **Aplicar configuración de administrador**, en **Dirección IP de instancia**, seleccione la dirección IP de la instancia VPX en la que quiere aplicar la configuración de administración.
4. Haga clic en **Aceptar**.

Instalar y administrar certificados SSL

November 23, 2023

El proceso de instalación de los certificados SSL implica cargar primero los archivos de certificados y claves en el dispositivo NetScaler SDX. A continuación, instale el certificado SSL en las instancias de NetScaler. Al instalar o actualizar un certificado SSL en el dispositivo SDX, el Servicio de administración se reinicia.

Cargue el archivo de certificado en el dispositivo SDX

Para cualquier transacción SSL, el servidor necesita un certificado válido y el par de claves privadas y públicas correspondientes. El archivo de certificado debe estar presente en el dispositivo SDX al instalar el certificado SSL en las instancias de NetScaler. También puede descargar los archivos del certificado SSL en un equipo local como copia de seguridad.

En el panel **Certificados SSL**, puede ver los siguientes detalles.

- **Nombre**

Nombre del archivo de certificado.

- **Última modificación**

La fecha en que se modificó por última vez el archivo del certificado.

- **Tamaño**

Tamaño del archivo de certificado en bytes.

Para cargar archivos de certificado SSL en el dispositivo SDX

1. En el panel de navegación, expanda Management Service y, a continuación, haga clic en Archivos de certificado SSL.
2. En el panel Certificados SSL, haga clic en Cargar.
3. En el cuadro de diálogo Cargar certificado SSL, haga clic en Examinar y seleccione el archivo de certificado que quiere cargar.
4. Haga clic en Cargar. El archivo de certificado aparece en el panel Certificados SSL.

Para crear una copia de seguridad mediante la descarga de un archivo de certificado SSL

1. En el panel Certificados SSL, seleccione el archivo que quiere descargar y, a continuación, haga clic en Descargar.
2. En el cuadro de mensaje, en la lista Guardar, seleccione Guardar como.
3. En el cuadro de mensaje Guardar como, busque la ubicación en la que quiere guardar el archivo y, a continuación, haga clic en Guardar.

Carga de archivos de clave SSL en el dispositivo SDX

Para cualquier transacción SSL, el servidor necesita un certificado válido y el par de claves privadas y públicas correspondientes. El archivo clave debe estar presente en el dispositivo SDX al instalar el

certificado SSL en las instancias de NetScaler. También puede descargar los archivos de clave SSL en un equipo local como copia de seguridad.

En el panel Claves SSL, puede ver los siguientes detalles.

- **Nombre**

Nombre del archivo clave.

- **Última modificación**

La fecha en que se modificó por última vez el archivo de claves.

- **Tamaño**

Tamaño del archivo clave en bytes.

Para cargar archivos de clave SSL en el dispositivo SDX

1. En el panel de navegación, expanda Management Service y, a continuación, haga clic en Archivos de certificado SSL.
2. En el panel Certificado SSL, en la ficha Claves SSL, haga clic en Cargar.
3. En el cuadro de diálogo Cargar archivo de clave SSL, haga clic en Examinar y seleccione el archivo de clave que quiere cargar.
4. Haga clic en Cargar para cargar el archivo de clave en el dispositivo SDX. El archivo de clave aparece en el panel Claves SSL.

Para crear una copia de seguridad mediante la descarga de un archivo de clave SSL

1. En el panel Certificado SSL, en la ficha Claves SSL, seleccione el archivo que quiere descargar y, a continuación, haga clic en Descargar.
2. En el cuadro de mensaje, en la lista Guardar, seleccione Guardar como.
3. En el cuadro de mensaje Guardar como, busque la ubicación en la que quiere guardar el archivo y, a continuación, haga clic en Guardar.

Instalación de un certificado SSL en una instancia de NetScaler

El Servicio de administración le permite instalar certificados SSL en una o más instancias de NetScaler. Antes de comenzar a instalar el certificado SSL, asegúrese de haber cargado el certificado SSL y los archivos de clave en el dispositivo SDX.

Para instalar certificados SSL en una instancia de NetScaler

1. En el panel de navegación, haga clic en NetScaler.
2. En el panel de detalles, en Configuración de NetScaler, haga clic en Instalar certificados SSL.
3. En el cuadro de diálogo Instalar certificados SSL, especifique los valores para los siguientes parámetros. (*) indica los campos obligatorios.
 - Archivo de certificado: Especifique el nombre de archivo del certificado válido. El archivo de certificado debe estar presente en el dispositivo SDX.
 - Archivo de clave: Especifique el nombre de archivo de la clave privada utilizada para crear el certificado. El archivo de clave debe estar presente en el dispositivo SDX.
 - Nombre del certificado: Especifique el nombre del par de claves de certificado que se va a agregar al de NetScaler. Longitud máxima: 31
 - Formato de certificado: Especifique el formato del certificado SSL admitido en NetScaler. Un dispositivo NetScaler SDX admite los formatos PEM y DER para los certificados SSL.
 - Contraseña: Especifique la frase de contraseña que se utilizó para cifrar la clave privada. Esta opción se puede usar para cargar claves privadas cifradas. Longitud máxima: 32.
Nota: La clave privada protegida con contraseña solo se admite para el formato PEM.
 - Guardar configuración: especifique si la configuración debe guardarse en NetScaler. El valor predeterminado es false.
 - Dirección IP de instancia: Especifique las direcciones IP de las instancias de NetScaler en las que quiere instalar el certificado SSL.
4. Haga clic en Aceptar y, a continuación, en Cerrar.

Actualización de un certificado SSL en una instancia de NetScaler

Puede actualizar algunos parámetros, como el archivo de certificado, el archivo de clave y el formato de certificado de un certificado SSL que esté instalado en una instancia de NetScaler. No puede modificar la dirección IP y el nombre del certificado.

Para actualizar el certificado SSL en una instancia de NetScaler

1. En el panel de navegación, expanda NetScaler y, a continuación, haga clic en Certificados SSL.
2. En el panel Certificados SSL, haga clic en Actualizar.
3. En el cuadro de diálogo Modificar certificado SSL, defina los siguientes parámetros:
 - Archivo de certificado: El nombre de archivo del certificado válido. El archivo de certificado debe estar presente en el dispositivo SDX.

- Archivo de clave: El nombre de archivo de la clave privada utilizada para crear el certificado. El archivo de clave debe estar presente en el dispositivo SDX.
- Formato de certificado: Formato del certificado SSL admitido en el dispositivo NetScaler SDX. El dispositivo admite los formatos PEM y DER para los certificados SSL.
- Contraseña: La frase de contraseña que se utilizó para cifrar la clave privada. Esta opción se puede usar para cargar claves privadas cifradas. Longitud máxima: 32 caracteres.
Nota: La clave privada protegida con contraseña solo se admite para el formato PEM.
- Guardar configuración: especifique si la configuración debe guardarse en el dispositivo SDX. El valor predeterminado es false.
- Sin comprobación de dominio: No compruebe el nombre de dominio mientras actualiza el certificado.

4. Haga clic en Aceptar y, a continuación, en Cerrar.

Encuesta de certificados SSL en las instancias de NetScaler

Si agrega un certificado SSL directamente a una instancia de NetScaler después de iniciar sesión en esa instancia, el Servicio de administración no tendrá conocimiento de este nuevo certificado. Para evitar este escenario, especifique un intervalo de sondeo tras el cual el Servicio de administración sondee todas las instancias de NetScaler para comprobar si hay nuevos certificados SSL. También puede realizar una encuesta en cualquier momento desde el Servicio de administración. Por ejemplo, si quiere obtener inmediatamente una lista de los certificados SSL de todas las instancias de NetScaler.

Para configurar un intervalo de sondeo

1. En el panel de navegación, expanda NetScaler y, a continuación, haga clic en Certificados SSL.
2. En el panel Certificados SSL, haga clic en Configurar intervalo de sondeo.
3. En el cuadro de diálogo Configurar intervalo de sondeo, defina los siguientes parámetros:
 - Intervalo de sondeo: El tiempo después del cual Management Service sondea las instancias de NetScaler.
 - Unidad de intervalo: La unidad de tiempo. Valores posibles: Horas, minutos. Predeterminado: Horas.
4. Haga clic en Aceptar y, a continuación, en Cerrar.

Para realizar un sondeo inmediato

1. En el panel de navegación, expanda NetScaler y, a continuación, haga clic en Certificados SSL.
2. En el panel Certificados SSL, haga clic en Sondear ahora.
3. En el cuadro de diálogo Confirmar, haga clic en Sí. El panel Certificados SSL se actualiza y los certificados nuevos, si los hay, aparecen en la lista.

Permitir el modo L2 en una instancia de NetScaler

November 23, 2023

En el modo de capa 2 (L2), una instancia de NetScaler actúa como puente de aprendizaje y reenvía todos los paquetes de los que no es el destino. Algunas funciones, como Citrix CloudBridge, requieren que el modo L2 esté habilitado en la instancia de NetScaler. Con el modo L2 habilitado, la instancia puede recibir y reenviar paquetes para direcciones MAC que no sean su propia dirección MAC. Sin embargo, para habilitar el modo L2 en una instancia de NetScaler que se ejecuta en un dispositivo NetScaler SDX, el administrador primero debe permitir el modo L2 en esa instancia. Si permite el modo L2, debe tomar precauciones para evitar bucles de conexión en puente.

Precauciones:

1. En una interfaz 1/x determinada, los paquetes sin etiqueta deben permitirse solo en una instancia. Para todas las demás instancias habilitadas en la misma interfaz, debe seleccionar Etiquetado.

Nota:

Citrix recomienda seleccionar Etiquetado para todas las interfaces asignadas a instancias en modo L2. Si selecciona etiquetado, no podrá recibir paquetes sin etiquetar en esa interfaz.

Si seleccionó Tagged para una interfaz asignada a una instancia, inicie sesión en esa instancia y configure una VLAN 802.1q para recibir paquetes en esa interfaz.

2. Para las interfaces 1/x y 10/x que comparten las instancias de NetScaler en las que se permite el modo L2, asegúrese de que se cumplan las siguientes condiciones:
 - El filtrado de VLAN está habilitado en todas las interfaces.
 - Cada interfaz se encuentra en una VLAN 802.1q diferente.
 - Solo una instancia puede recibir paquetes sin etiquetar en la interfaz. Si esa interfaz se asigna a otras instancias, debe seleccionar Etiquetado en esa interfaz para esas instancias.
3. Si permite paquetes sin etiqueta en una interfaz 1/x para una instancia en la que se permite el modo L2, ninguna otra instancia puede recibir paquetes sin etiqueta en esa interfaz. Esta condición se aplica independientemente de si el modo L2 se permite o no en la otra instancia.

4. Si permite paquetes sin etiqueta en una interfaz 1/x para una instancia con el modo L2 inhabilitado, una instancia con el modo L2 permitido no puede recibir paquetes sin etiqueta en esa interfaz.
5. Si se asigna una interfaz 0/x a instance1 provisionada en modo L2 y esa interfaz también se asigna a instance2, seleccione Tagged para todas las demás interfaces asignadas a instance2.

Nota: Si ambas interfaces de administración se asignan a una instancia con el modo L2, solo una de estas interfaces se puede asignar a otra instancia de ADC con el modo L2 habilitado. Es decir, no puede asociar ambas interfaces de administración a más de una instancia de NetScaler en la que esté habilitado el modo L2.

Para permitir el modo L2 en una instancia

1. En el Asistente para provisionar ADC o en el Asistente para modificar ADC, en la página **Configuración de red**, seleccione **Permitir modo L2**.
Nota: Puede activar el ajuste Permitir modo L2 en una instancia cuando provisione la instancia o mientras la instancia se está ejecutando.
2. Siga las instrucciones indicadas en el asistente.
3. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Configuración de un MAC virtual en una interfaz

November 23, 2023

Una instancia de NetScaler utiliza un MAC virtual (VMAC) para configuraciones de alta disponibilidad (activo-activo o activo-espera). Una dirección MAC virtual (VMAC) es una entidad flotante compartida por los nodos principal y secundario en una configuración de alta disponibilidad.

En una configuración de alta disponibilidad, el nodo principal es propietario de todas las direcciones IP flotantes, como las direcciones MIP, SNIP y VIP. El nodo principal responde a las solicitudes del Protocolo de resolución de direcciones (ARP) para estas direcciones IP con su propia dirección MAC. Como resultado, la tabla ARP de un dispositivo externo (por ejemplo, un enrutador ascendente) se actualiza con la dirección IP flotante y la dirección MAC del nodo principal.

Cuando se produce una conmutación por error, el nodo secundario pasa a ser el nuevo nodo principal. A continuación, utiliza ARP gratuito (GARP) para anunciar las direcciones IP flotantes que adquirió del principal. Sin embargo, la dirección MAC que anuncia el nuevo principal es la dirección MAC de su propia interfaz.

Algunos dispositivos (especialmente algunos enrutadores) no aceptan los mensajes GARP generados por el dispositivo NetScaler SDX. Dichos dispositivos conservan la antigua asignación de IP a MAC anunciada por el nodo principal anterior y, como resultado, un sitio puede caer.

Puede solucionar este problema configurando una VMAC en ambos nodos de un par de alta disponibilidad. Ambos nodos poseen direcciones MAC idénticas. Por lo tanto, cuando se produce una conmutación por error, la dirección MAC del nodo secundario permanece sin cambios y las tablas ARP de los dispositivos externos no necesitan actualizarse.

La configuración de una VMAC es un proceso de dos pasos:

1. Configure VMAC en el Servicio de administración de SDX. Agrega un VRID para una interfaz o un canal LA. Configure VMAC en el Servicio de administración de SDX.
2. Configure VMAC en la instancia de Citrix. Para obtener información, consulte el artículo de asistencia [Configurar VMAC en el grupo de canales](#).

Configurar VMAC en el Servicio de administración SDX

Para configurar VMAC, agregue un VRID IPv4 o IPv6 a una interfaz o canal LA del Servicio de administración. Management Service genera internamente un VMAC. Especifique el mismo VRID al configurar el modo activo-activo en la instancia de NetScaler. Esta configuración activo-activa no es compatible con las interfaces de Mellanox.

Tenga en cuenta los siguientes puntos:

1. Agregue un VRID del Servicio de administración y especifique el mismo VRID en la instancia de NetScaler. Si agrega un VRID directamente a la instancia de NetScaler, la instancia no puede recibir un paquete que tenga una dirección VMAC como dirección MAC de destino.
2. No puede usar el mismo VRID en instancias diferentes que se ejecuten en el mismo dispositivo SDX.
3. Puede agregar o eliminar los VRID de una interfaz asignada a una instancia mientras la instancia está en ejecución.
4. En una configuración activa-activa, puede especificar más de un VRID para una interfaz asignada a una instancia. La implementación activa-activa no es compatible con las interfaces de Mellanox.
5. Se permite un máximo de 86 VMAC en una interfaz 10G y un máximo de 16 VMAC en una interfaz 1G. Si no hay más filtros VMAC disponibles, reduzca la cantidad de VRID en otra instancia.

Puede agregar un VRID en el momento de agregar una instancia de NetScaler VPX o puede modificar una instancia de NetScaler existente para agregar un VRID.

Para agregar un VRID IPv4 o IPv6 a una interfaz o canal LA

1. Al agregar una instancia VPX en SDX, en **Configuración de red**, seleccione **Interfaces de datos**. Para obtener más información sobre cómo agregar una instancia VPX en SDX, consulte [Agregar una instancia de NetScaler](#).
2. En el menú desplegable **Interfaces**, seleccione la interfaz o el canal LA.
3. En Configuración de VMAC, y defina uno o ambos de los siguientes valores:
 - VRID IPv4: El VRID IPv4 que identifica el VMAC. Valores posibles: 1-255.
 - VRID IPv6: El VRID IPv6 que identifica el VMAC. Valores posibles: 1-255.Nota: Use una coma para separar varios VRID. Por ejemplo, 12,24.
4. Haga clic en **Agregar** para agregar la configuración de **VMAC** a la interfaz.
5. Haga clic en **Finalizar** y, a continuación, en **Cerrar**.

Add Data Interface

Interfaces*

LA/1 (LACP) ▾

The option "Allow Untagged Traffic" needs to be always enabled on a

Allow Untagged Traffic

VLANs

100-110,142,151-155

MAC Address Mode*

Default ▾

▼ VMAC Settings (IPv4 and IPv6 VRIDs to configure Virtual MAC)

VRID IPv4

2,10,111

VRID IPv6

2,10,111

Add

Si la instancia ya está aprovisionada, para agregar un VRID IPv4 o IPv6, siga estos pasos.

1. Desde el Servicio de administración de SDX, vaya a **Configuración > NetScaler**Instancias.
2. Seleccione la instancia y haga clic en **Modificar**.
3. En **Interfaces de datos**, seleccione la interfaz y haga clic en **Modificar**.
4. En Configuración de VMAC, defina los valores de VRID. Haga clic en **Agregar** y, a continuación, haga clic en **Listo**.

Genere direcciones MAC de partición para configurar una partición de administración en una instancia de NetScaler en el dispositivo SDX

November 23, 2023

Una instancia de NetScaler en un dispositivo NetScaler SDX se puede particionar en entidades lógicas denominadas particiones de administración. Cada partición se puede configurar y utilizar como una instancia de NetScaler independiente. Para obtener más información sobre las particiones de [administración](#), consulte [Particionado](#) de administración.

Para usar particiones de administración con una configuración de VLAN compartida, necesita una dirección MAC virtual para cada partición. Dicha dirección MAC virtual se denomina dirección MAC de partición (PMAC) y se usa para clasificar el tráfico recibido en una VLAN compartida. Esta dirección PMAC se usa en todas las VLAN compartidas enlazadas a esa partición.

Genere y configure la dirección PMAC mediante la interfaz de usuario del Servicio de administración, antes de usar la partición admin. Management Service le permite generar direcciones MAC de partición mediante:

- Uso de una dirección MAC base
- Especificación de direcciones MAC personalizadas
- Generación aleatoria de direcciones MAC

Nota:

Tras generar las direcciones MAC de las particiones, debe reiniciar la instancia de NetScaler antes de configurar las particiones de administración.

Para generar las direcciones MAC de partición mediante una dirección MAC base:

1. En la ficha **Configuración**, en el panel izquierdo, expanda **NetScaler**y, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias**, seleccione la instancia de NetScaler para la que quiere generar las direcciones MAC de partición.
3. En la lista desplegable **Acción**, haga clic en **Partición de Mac**.
4. En el panel **MAC de partición**, haga clic en **Generar**.

5. En el cuadro de diálogo **Generar MAC de partición**, en la sección **Método de generación**, seleccione **Using Base Address**.
6. En el campo **Dirección MAC base**, introduzca la dirección MAC base.
7. En el campo **Incremento por**, introduzca el valor por el que la dirección MAC base debe incrementarse para cada dirección MAC posterior.
Por ejemplo, si ha especificado la dirección MAC base como 00:A1:C9:11:C8:11 y el valor de incremento como 2, la siguiente dirección MAC se genera como 00:A1:C9:11:C8:13.
8. En el campo **Recuento**, introduzca el número de direcciones MAC de partición que quiere generar.
9. Pulse en **Generar**.

Para generar las direcciones MAC de partición especificando direcciones MAC personalizadas:

1. En la ficha **Configuración**, en el panel izquierdo, expanda **NetScaler**, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias**, seleccione la instancia de NetScaler para la que quiere generar las direcciones MAC de partición.
3. En la lista desplegable **Acción**, haga clic en **Partición de Mac**.
4. En el panel **MAC de partición**, haga clic en **Generar**.
5. En el cuadro de diálogo **Generar MAC de partición**, en la sección **Método de generación**, seleccione **Especificado por el usuario**.
6. En el campo **Direcciones MAC**, introduzca una dirección MAC.
7. Haga clic en el icono **+** y, a continuación, introduzca la siguiente dirección MAC. Repita para especificar más direcciones MAC personalizadas.
8. Pulse en **Generar**.

Para generar aleatoriamente las direcciones MAC de partición:

1. En la ficha **Configuración**, en el panel izquierdo, expanda **NetScaler**, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias**, seleccione la instancia de NetScaler para la que quiere generar las direcciones MAC de partición.
3. En la lista desplegable **Acción**, haga clic en **Partición de Mac**.
4. En el panel **MAC de partición**, haga clic en **Generar**.
5. En el cuadro de diálogo **Generar MAC de partición**, en la sección **Método de generación**, seleccione **Aleatorio**.
6. En el campo **Recuento**, introduzca el número de direcciones MAC de partición que quiere generar.
7. Pulse en **Generar**.

Después de generar las direcciones MAC de partición en un dispositivo SDX, utilice las direcciones MAC de partición generadas para configurar las particiones de administración en la instancia de

NetScaler.

Administración de cambios para instancias VPX

November 23, 2023

Puede realizar un seguimiento de cualquier cambio en la configuración de una instancia de NetScaler VPX desde el Servicio de administración. El panel de detalles muestra el nombre del dispositivo con la dirección IP, la fecha y la hora en que se actualizó por última vez. También indica si hay alguna diferencia entre la configuración guardada y la configuración en ejecución. Seleccione un dispositivo para ver su configuración en ejecución, la configuración guardada, el historial de cambios de configuración y cualquier diferencia entre las configuraciones antes y después de una actualización. Puede descargar la configuración de una instancia VPX en su equipo local. De forma predeterminada, Management Service sondea todas las instancias cada 24 horas, pero puede cambiar este intervalo. Puede crear una plantilla de auditoría copiando los comandos de un archivo de configuración existente. Más adelante, puede usar esta plantilla para buscar cualquier cambio en la configuración de una instancia y tomar medidas correctivas si es necesario.

Para ver la administración de cambios de las instancias VPX

1. En la ficha **Configuración**, vaya a **NetScaler > Administración de cambios**.
2. En el panel **Administración de cambios**, seleccione una instancia VPX y, a continuación, en la lista **Acción**, seleccione una de las siguientes opciones:
 - Configuración en ejecución: Muestra la configuración en ejecución de la instancia VPX seleccionada en una nueva ventana.
 - Configuración guardada: Muestra la configuración guardada de la instancia VPX seleccionada en una nueva ventana.
 - Guardado vs. Ejecución de diferencias: Muestra la configuración guardada, la configuración en ejecución y el comando correctivo (la diferencia).
 - Diff del historial de revisiones: Muestra la diferencia entre el archivo de configuración base y el segundo archivo de configuración.
 - Pre vs. Diff posterior a la actualización: Muestra la diferencia en la configuración antes y después de una actualización, y el comando correctivo (la diferencia).
 - Diferencia de plantilla: Muestra la diferencia entre la configuración guardada o en ejecución y la plantilla. Puede guardar esta diferencia como un archivo por lotes. Para aplicar la configuración de la plantilla a la instancia, aplique este archivo por lotes a la instancia.
 - Descargar: Descarga la configuración de la instancia VPX seleccionada y la guarda en un dispositivo local.

Para buscar actualizaciones en la configuración de cualquiera de las instancias de NetScaler

1. En la ficha **Configuración**, vaya a **NetScaler > Administración de cambios**.
2. En el panel **Administración de cambios**, en la lista **Acción**, seleccione una de las siguientes opciones:
 - **Sondear ahora:** Management Service realiza un sondeo inmediato para obtener actualizaciones de la configuración (ns.conf) de cualquiera de las instancias VPX instaladas en el dispositivo.
 - **Configurar intervalo de sondeo:** Tiempo tras el cual Management Service busca actualizaciones de la configuración (ns.conf) de cualquiera de las instancias VPX instaladas en el dispositivo. El intervalo de sondeo predeterminado es de 24 horas.

Para configurar una plantilla de auditoría para una instancia de NetScaler

1. Abra un archivo de configuración existente y copie su lista de comandos.
2. En la ficha **Configuración**, vaya a **NetScaler > Administración de cambios > Plantillas de auditoría**.
3. En el panel de detalles, haga clic en **Agregar**.
4. En el cuadro de diálogo **Agregar plantilla**, agregue un nombre y una descripción para la plantilla.
5. En el cuadro de texto **Comando**, pegue la lista de comandos que ha copiado del archivo de configuración.
6. Haga clic en **Crear** y, a continuación, en **Cerrar**.

Supervise las instancias de NetScaler

November 23, 2023

En la página Supervisión de la interfaz de usuario del Servicio de administración se muestra una vista de alto nivel del rendimiento del dispositivo y de las instancias VPX aprovisionadas en el dispositivo. Tras aprovisionar y configurar la instancia de NetScaler, puede realizar varias tareas para supervisar la instancia de NetScaler.

Ver las propiedades de las instancias VPX

La interfaz de usuario del Servicio de administración muestra la lista y la descripción de todas las instancias VPX aprovisionadas en el dispositivo SDX. Utilice el panel de **instancias de NetScaler** para ver

detalles, como el nombre y la dirección IP de la instancia, el uso de la CPU y la memoria, el rendimiento y la memoria total asignada a la instancia.

Al hacer clic en la dirección IP de la instancia VPX se abre la utilidad de configuración (GUI) de esa instancia en una nueva ficha o explorador.

Para ver las propiedades de las instancias VPX

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de NetScaler y, a continuación, haga clic en Instancias.

Nota: También puede ver las propiedades de una instancia VPX desde la ficha Inicio.

2. En el panel de instancias de NetScaler, puede ver los siguientes detalles de la instancia de NetScaler:

- **Nombre:** el nombre de host asignado a la instancia de NetScaler durante el aprovisionamiento.
- **Estado de VM:** el estado de la máquina virtual.
- **Estado de NetScaler:** el estado de la instancia de NetScaler.
- **Dirección IP:** la dirección IP de la instancia de NetScaler. Al hacer clic en la dirección IP, se abre la GUI de esta instancia en una nueva ficha o explorador.
- **Rx (Mbps):** los paquetes recibidos en la instancia de NetScaler.
- **Tx (Mbps):** los paquetes transmitidos por la instancia de NetScaler.
- **Req/s HTTP:** el número total de solicitudes HTTP recibidas en la instancia de NetScaler cada segundo.
- **Uso de CPU (%):** el porcentaje de utilización de la CPU en NetScaler.
- **Uso de memoria (%):** el porcentaje de utilización de memoria en NetScaler.

3. Haga clic en la flecha situada junto al nombre de una instancia de NetScaler para ver las propiedades de esa instancia. También puede hacer clic en **Expandir todo** para ver las propiedades de todas las instancias de NetScaler. Puede ver las siguientes propiedades:

- **Máscara de red:** la dirección IP de la máscara de red de la instancia de NetScaler.
- **Puerta de enlace:** la dirección IP de la puerta de enlace predeterminada, el enrutador que reenvía el tráfico fuera de la subred en la que está instalada la instancia.
- **Paquetes por segundo:** el número total de paquetes que pasan por segundo.
- **NIC:** los nombres de las NIC utilizadas por la instancia de NetScaler, junto con la función virtual asignada a cada interfaz.
- **Versión:** la versión de compilación, la fecha de compilación y la hora del software NetScaler que se ejecuta actualmente en la instancia.
- **Nombre de host:** el nombre de host de la instancia de NetScaler.

- **Memoria total (GB):** la memoria total que se asigna a la instancia de NetScaler.
- **Rendimiento (Mbps):** el rendimiento total de la instancia de NetScaler.
- **Activo desde:** la fecha y la hora desde que la instancia ha estado activo de forma continua.
- **Chips SSL:** el número total de chips SSL asignados a la instancia.
- **Dirección IP de par:** la dirección IP del par de esta instancia de NetScaler si se encuentra en una configuración de HA.
- **Estado:** el estado de las operaciones que se están realizando en una instancia de NetScaler, como el estado de si el inventario de la instancia se ha completado.
- **Estado maestro de HA:** el estado del dispositivo. El estado indica si la instancia está configurada en una configuración independiente o principal o si forma parte de una configuración de alta disponibilidad. En una configuración de alta disponibilidad, el estado también muestra si está en modo primario o secundario.
- **Estado de sincronización de HA:** el modo del estado de sincronización de HA, como habilitado o inhabilitado.
- **Descripción:** la descripción introducida al aprovisionar la instancia de NetScaler.

Notas:

Cuando una instancia de ADC deja de funcionar debido a un error de autenticación, el color del estado de la instancia cambia a gris si se cumplen las siguientes condiciones:

- La contraseña de la instancia de ADC se cambia directamente mediante la CLI de la instancia.
- La contraseña no coincide con la contraseña del perfil de administrador de la instancia almacenada en Management Service.
- La sesión anterior se pierde después de reiniciar la instancia por primera vez.

Por lo general, cuando una instancia deja de funcionar, el color del estado de la instancia es amarillo.

Para recuperar la instancia, siga uno de estos procedimientos:

- En la CLI de la instancia, modifica la contraseña de la instancia para que coincida con la contraseña en el perfil de administrador de la instancia. A continuación, vuelva a descubrir la instancia desde el Servicio de administración.
- Cree un perfil de administrador con la misma contraseña que la contraseña actual de la instancia de ADC. A continuación, actualice la instancia de ADC con el nuevo perfil de administrador.

Ver la configuración en ejecución y guardada de una instancia de NetScaler

Al utilizar el Servicio de administración, puede ver la configuración que se está ejecutando actualmente de una instancia de NetScaler. También puede ver la configuración guardada de una instancia de NetScaler y la hora en que se guardó la configuración.

Para ver la configuración en ejecución y guardada de una instancia de NetScaler

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de NetScaler y, a continuación, haga clic en Instancias.
2. En el panel de instancias de NetScaler, haga clic en la instancia de NetScaler para la que quiere ver la configuración en ejecución o guardada.
3. Para ver la configuración en ejecución, haga clic en Configuración en ejecución y, para ver la configuración guardada, haga clic en Configuración guardada.
4. En la ventana Configuración en ejecución de NetScaler o en la ventana Configuración guardada de NetScaler, puede ver la configuración en ejecución o guardada de la instancia de NetScaler.

Haga ping a una instancia de NetScaler

Puede hacer ping a una instancia de NetScaler desde el Servicio de administración para comprobar si se puede acceder al dispositivo.

Para hacer ping a una instancia de NetScaler

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de NetScaler y, a continuación, haga clic en Instancias.
2. En el panel de instancias de NetScaler, haga clic en la instancia de NetScaler a la que desee hacer ping y, a continuación, haga clic en Ping. En el cuadro de mensaje Ping, puede ver si el ping se ha realizado correctamente.

Rastrea la ruta de una instancia de NetScaler

Puede rastrear la ruta de un paquete desde el Servicio de administración hasta una instancia de NetScaler determinando el número de saltos utilizados para llegar a la instancia.

Para rastrear la ruta de una instancia de NetScaler

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de NetScaler y, a continuación, haga clic en Instancias.
2. En el panel de instancias de NetScaler, haga clic en la instancia de NetScaler que quiere rastrear y, a continuación, haga clic en TraceRoute. En el cuadro de mensajes de Traceroute, puede ver la ruta al NetScaler.

Redescubra una instancia de NetScaler

Puede volver a descubrir una instancia de NetScaler cuando necesite ver el estado y la configuración más recientes de una instancia de NetScaler.

Durante el redescubrimiento, Management Service recupera la configuración. De forma predeterminada, Management Service programa los dispositivos para redescubrimiento una vez cada 30 minutos.

Para redescubrir una instancia de NetScaler

1. En la ficha **Configuración**, en el panel izquierdo, expanda **Configuración de NetScaler** y, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias de NetScaler**, haga clic en la instancia de NetScaler que quiere volver a detectar y, a continuación, haga clic en **Redescubrir**.
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Usar registros para supervisar las operaciones y los eventos

November 23, 2023

Utilice los registros de auditoría y tareas para supervisar las operaciones realizadas en el Servicio de administración y en las instancias de NetScaler SDX. También puede usar el registro de eventos para realizar un seguimiento de todos los eventos de las tareas realizadas en Management Service y Citrix Hypervisor.

Ver los registros de auditoría

Todas las operaciones realizadas mediante Management Service se registran en la base de datos del dispositivo. Use los registros de auditoría para ver las operaciones que ha realizado un usuario del

Servicio de administración, la fecha y la hora, y el estado de éxito o fracaso de cada operación. También puede ordenar los detalles por usuario, operación, tiempo de auditoría, estado, etc., haciendo clic en el encabezado de columna apropiado.

La paginación se admite en el panel Registro de auditoría. Seleccione el número de registros que se mostrarán en una página. De forma predeterminada, se muestran 25 registros en una página.

Para ver los registros de auditoría, siga estos pasos:

1. En el panel de navegación, expanda Sistema y luego haga clic en Auditoría.
2. En el panel Registro de auditoría, puede ver los siguientes detalles.
 - **Nombre de usuario:** el usuario del Servicio de administración que ha realizado la operación.
 - **Dirección IP:** la dirección IP del sistema en el que se realizó la operación.
 - **Puerto:** el puerto en el que se ejecutaba el sistema cuando se realizó la operación.
 - **Tipo de recurso:** el tipo de recurso utilizado para realizar la operación, como xen_vpx_image y login.
 - **Nombre del recurso:** el nombre del recurso utilizado para realizar la operación, como vpx_image_name y el nombre de usuario utilizado para iniciar sesión.
 - **Tiempo de auditoría:** el momento en que se generó el registro de auditoría.
 - **Operación:** la tarea que se realizó, como agregar, eliminar y cerrar sesión.
 - **Estado:** el estado de la auditoría, por ejemplo, correcta o fallida.
 - **Mensaje:** un mensaje que describe la causa del error si la operación ha fallado y el estado de la tarea, como Hecho, si la operación se ha realizado correctamente.
3. Para ordenar los registros por un campo en particular, haga clic en el encabezado de la columna.

Ver registros de tareas

Utilice los registros de tareas para ver y realizar un seguimiento de las tareas, como actualizar las instancias e instalar certificados SSL, que ejecuta el Servicio de administración en las instancias de NetScaler. El registro de tareas le permite ver si una tarea está en curso, si ha fallado o si ha tenido éxito.

La paginación se admite en el panel **Registro de tareas**. Seleccione el número de registros que se mostrarán en una página. De forma predeterminada, se muestran 25 registros en una página.

Para ver el registro de tareas, siga estos pasos:

1. En el panel de navegación, expanda Diagnóstico y, a continuación, haga clic en Registro de tareas.
2. En el panel Registro de tareas, puede ver los siguientes detalles.

- **Nombre:** el nombre de la tarea que se está ejecutando o que ya se ha ejecutado.
- **Estado:** el estado de la tarea, como En curso, Completada o Fallida.
- **Ejecutado por:** el usuario del Servicio de administración que ha realizado la operación.
- **Hora de inicio:** la hora en que comenzó la tarea.
- **Hora de finalización:** la hora en que finalizó la tarea.

Ver registros de dispositivos de tareas

Utilice los registros de dispositivos de tareas para ver y realizar un seguimiento de las tareas que se realizan en cada instancia SDX. El registro del dispositivo de tareas le permite ver si una tarea está en curso, si ha fallado o si ha tenido éxito. También muestra la dirección IP de la instancia en la que se realiza la tarea.

Para ver el registro del dispositivo de tareas, siga estos pasos:

1. En el panel de navegación, expanda **Diagnóstico** y, a continuación, haga clic en **Registro de tareas**.
2. En el panel **Registro de tareas**, haga doble clic en la tarea para ver los detalles del dispositivo de tareas.
3. En el panel **Registro del dispositivo de tareas**, para ordenar los registros por un campo en particular, haga clic en el encabezado de la columna.

Ver registros de comandos de tareas

Utilice los registros de comandos de tareas para ver el estado de cada comando de una tarea ejecutada en una instancia de NetScaler. El registro de comandos task le permite ver si un comando se ha ejecutado correctamente o si ha fallado. También muestra el comando que se ejecuta y el motivo por el que se ha producido un error en un comando.

Para ver el registro de comandos de tareas, siga estos pasos:

1. En el panel de navegación, expanda **Diagnóstico** y, a continuación, haga clic en **Registro de tareas**.
2. En el panel **Registro de tareas**, haga doble clic en la tarea para ver los detalles del dispositivo de tareas.
3. En el panel **Registro de dispositivos de tareas**, haga doble clic en la tarea para ver los detalles del comando de tarea.
4. En el panel **Registro de comandos de tareas**, para ordenar los registros por un campo en particular, haga clic en el encabezado de la columna.

Ver eventos

Utilice el panel **Eventos** de la interfaz de usuario del Servicio de administración para supervisar los eventos generados por Management Service para las tareas realizadas en Management Service.

Para ver los eventos, sigue estos pasos:

1. Vaya a **Sistema > Eventos**.
2. En el panel **Eventos**, puede ver los siguientes detalles.
 - **Gravedad:** la gravedad de un evento, que puede ser crítica, grave, leve, clara e informativa.
 - **Fuente:** la dirección IP en la que se genera el evento.
 - **Fecha:** la fecha en que se genera el evento.
 - **Categoría:** la categoría del evento, como PolicyFailed y DeviceConfigChange.
 - **Mensaje:** el mensaje que describe el evento.
3. Para ordenar los eventos por un campo en particular, haga clic en el encabezado de la columna.

Casos de uso de dispositivos NetScaler SDX

November 23, 2023

Para los componentes de red (como firewalls y controladores de entrega de aplicaciones), la compatibilidad con multitenencia ha implicado históricamente la capacidad de dividir un solo dispositivo en varias particiones lógicas. Este enfoque permite implementar diferentes conjuntos de directivas para cada arrendatario sin la necesidad de numerosos dispositivos separados. Tradicionalmente, sin embargo, está muy limitado en términos del grado de aislamiento que se logra.

Por diseño, el dispositivo SDX no está sujeto a las mismas limitaciones. En la arquitectura SDX, cada instancia se ejecuta como una máquina virtual (VM) independiente con su propio núcleo de NetScaler dedicado, recursos de CPU, recursos de memoria, espacio de direcciones y asignación de ancho de banda. La E/S de red en el dispositivo SDX no solo mantiene el rendimiento agregado del sistema, sino que también permite la segregación completa del tráfico del plano de datos y del plano de administración de cada arrendatario. El plano de administración incluye las interfaces 0/x. El plano de datos incluye las interfaces 1/x y 10/x. Un plano de datos también se puede utilizar como plano de gestión.

Los casos de uso principales de un dispositivo SDX están relacionados con la consolidación, lo que reduce la cantidad de redes necesarias y, al mismo tiempo, mantiene el aislamiento de la administración. A continuación se presentan los casos básicos de consolidación:

- Consolidación cuando el Servicio de administración y las instancias de NetScaler están en la misma red.
- Consolidación cuando las instancias del Servicio de administración y de NetScaler se encuentran en redes diferentes, pero todas las instancias están en la misma red.
- Consolidación en toda la seguridad.
- Consolidación con interfaces dedicadas para cada instancia.
- Consolidación con uso compartido de un puerto físico por más de una instancia.

Consolidación cuando las instancias del Servicio de administración y de NetScaler están en la misma red

November 23, 2023

Un tipo sencillo de consolidación en el dispositivo SDX es la configuración del Servicio de administración y las instancias de NetScaler como parte de la misma red. Este caso de uso se aplica si:

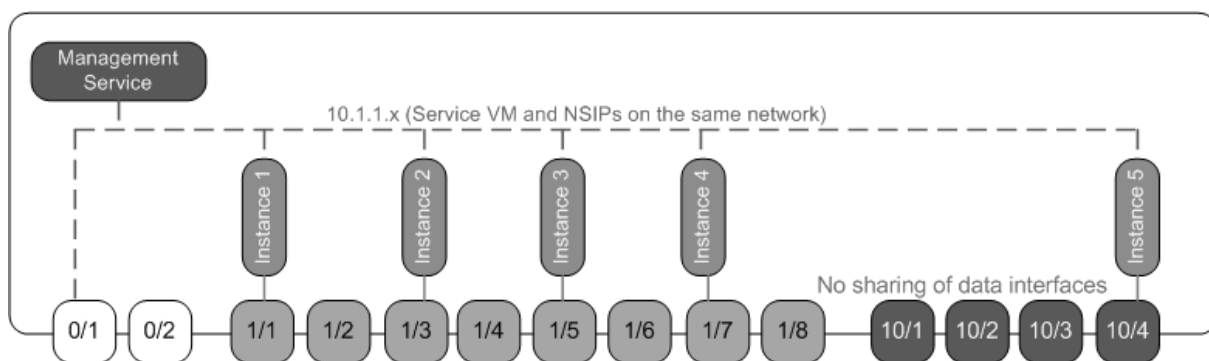
- El administrador del dispositivo también es el administrador de instancias.
- El requisito de cumplimiento de su organización no especifica que se requieran redes de administración separadas para el Servicio de administración y las direcciones NSIP de las diferentes instancias.

Las instancias se pueden aprovisionar en la misma red (para el tráfico de administración). Las direcciones VIP se pueden configurar en diferentes redes (para el tráfico de datos) y, por lo tanto, en diferentes zonas de seguridad.

En el siguiente ejemplo, el Servicio de administración y las instancias de NetScaler forman parte de la red 10.1.1.x. Las interfaces 0/1 y 0/2 son las interfaces de administración, 1/1 a 1/8 son interfaces de datos 1G y 10/1 a 10/4 son interfaces de datos 10G. Cada instancia tiene su propia interfaz física dedicada. Por lo tanto, la cantidad de instancias se limita a la cantidad de interfaces físicas disponibles en el dispositivo. De forma predeterminada, el filtrado de VLAN está habilitado en cada interfaz del dispositivo SDX. La cantidad de VLAN está restringida a 32 en una interfaz 1G y 63 en una interfaz 10G. El filtrado de VLAN se puede habilitar e inhabilitar para cada interfaz. Inhabilite el filtrado de VLAN para configurar hasta 4096 VLAN por interfaz en cada instancia. En este ejemplo, el filtrado de VLAN no es necesario porque cada instancia tiene su propia interfaz dedicada. Para obtener más información sobre el filtrado de VLAN, consulte la sección **Filtrado de VLAN** en [Administrar y supervisar el dispositivo SDX](#).

La siguiente ilustración ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con Management Service y NSIP para instancias en la misma red



En la siguiente tabla se enumeran los nombres y valores de los parámetros utilizados para aprovisionar la instancia 1 de NetScaler en el ejemplo anterior.

Nombre del parámetro	Valores de la instancia 1
Nombre	vpx8
Dirección IP	10.1.1.2
Máscara de red	255.255.255.0
Gateway	10.1.1.1
Archivo XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licencia de funciones	Platinum
Perfil de administrador	ns_nsroot_profile
Nombre de usuario	vpx8
Contraseña	Sdx1
Confirm Password	Sdx1
Acceso a Shell/Sftp/Scp	True
Memoria total (MB)	2048
Fichas #SSL	1
Rendimiento (Mbps)	1000
Paquetes por segundo	1000000
CPU	Compartida
Interfaz	0/1 y 1/1

Aprovisione la instancia 1 de NetScaler como se muestra en este ejemplo

1. En la ficha Configuración, en el panel de navegación, expanda Configuración de NetScaler y, a continuación, haga clic en Instancias.
2. En el panel de instancias de NetScaler, haga clic en Agregar.
3. En el Asistente para aprovisionar Citrix, siga las instrucciones del asistente para especificar los valores de los parámetros que se muestran en la tabla anterior.
4. Haga clic en Crear y, a continuación, en Cerrar. La instancia de NetScaler que aprovisionó aparece en el panel de instancias de NetScaler.

Consolidación cuando las instancias del Servicio de administración y de NetScaler se encuentran en redes diferentes

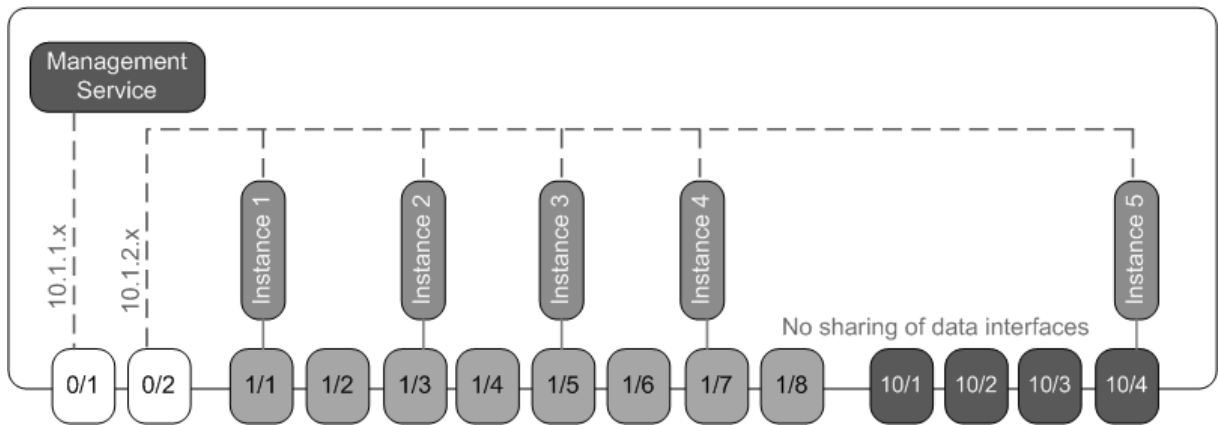
November 23, 2023

En ciertos casos, el administrador del dispositivo puede permitir que otros administradores realicen tareas de administración en instancias individuales. Esto se puede hacer de forma segura otorgando a un administrador de instancias individual derechos de inicio de sesión solo para esa instancia. Sin embargo, por razones de seguridad, es posible que el administrador del dispositivo no quiera permitir que la instancia esté en la misma red que Management Service. Este es un caso común en los entornos de proveedores de servicios, y se está volviendo cada vez más común en las empresas a medida que adoptan arquitecturas de virtualización y de nube.

En el siguiente ejemplo, el Servicio de administración está en la red 10.1.1.x y las instancias de NetScaler están en la red 10.1.2.x. Las interfaces 0/1 y 0/2 son las interfaces de administración, 1/1 a 1/8 son interfaces de datos 1G y 10/1 a 10/4 son interfaces de datos 10G. Cada instancia tiene su propio administrador dedicado y su propia interfaz física dedicada. Por lo tanto, la cantidad de instancias se limita a la cantidad de interfaces físicas disponibles en el dispositivo. El filtrado de VLAN no es necesario porque cada instancia tiene su propia interfaz dedicada. Si quiere, también puede desactivar el filtrado de VLAN para configurar hasta 4096 VLAN por instancia e interfaz. En este ejemplo, no necesita configurar una NSVLAN, porque las instancias no comparten una interfaz física y no hay VLAN etiquetadas. Para obtener más información sobre NSVLAN, consulte [Agregar una instancia de NetScaler](#)

La siguiente ilustración ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con Management Service y NSIP para instancias en diferentes redes



Como administrador del dispositivo, puede mantener el tráfico entre el Servicio de administración y las direcciones NSIP en el dispositivo SDX. O puede forzar el tráfico fuera del dispositivo si, por ejemplo, quiere que el tráfico pase a través de un firewall externo o algún otro intermediario de seguridad y, a continuación, vuelva al dispositivo.

En la siguiente tabla se enumeran los nombres y valores de los parámetros utilizados para aprovisionar la instancia 1 de NetScaler en este ejemplo.

Nombre del parámetro	Valores de la instancia 1
Nombre	vpx1
Dirección IP	10.1.2.2
Máscara de red	255.255.255.0
Gateway	10.1.2.1
Archivo XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licencia de funciones	Platinum
Perfil de administrador	ns_nsroot_profile
Nombre de usuario	vpx1
Contraseña	Sdx1
Confirm Password	Sdx1
Acceso a Shell/Sftp/Scp	True
Memoria total (MB)	2048
Fichas #SSL	1
Rendimiento (Mbps)	1000
Paquetes por segundo	1000000

Nombre del parámetro	Valores de la instancia 1
CPU	Compartida
Interfaz	0/2 y 1/1

Para aprovisionar la instancia 1 de NetScaler, como se muestra en este ejemplo

1. En la ficha **Configuración**, en el panel de navegación, expanda **Configuración de NetScaler** y, a continuación, haga clic en **Instancias**.
2. En el panel de instancias de NetScaler, haga clic en **Agregar**.
3. En el **asistente de aprovisionamiento de NetScaler**, siga las instrucciones del asistente para establecer los parámetros en los valores que se muestran en la tabla anterior.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**. La instancia de NetScaler que aprovisionó aparece en el panel de instancias de NetScaler.

Consolidación en todas las zonas de seguridad

November 23, 2023

Un dispositivo SDX se utiliza a menudo para la consolidación en todas las zonas de seguridad. La DMZ agrega una capa adicional de seguridad a la red interna de una organización, ya que un atacante solo tiene acceso a la DMZ. No tiene acceso a la red interna de la organización. En entornos de alto cumplimiento, no se acepta una sola instancia de NetScaler con direcciones VIP tanto en la DMZ como en una red interna. Con SDX, puede aprovisionar instancias que alojen direcciones VIP en la DMZ y otras instancias que alojen direcciones VIP en una red interna.

En ocasiones, es posible que necesite redes de administración separadas para cada zona de seguridad. Las direcciones NSIP de las instancias en la DMZ pueden estar en una red. Las direcciones NSIP de las instancias con VIP en la red interna pueden estar en una red de administración diferente. Además, a menudo, es posible que la comunicación entre el Servicio de administración y las instancias deba enrutarse a través de un dispositivo externo, como un enrutador. Puede configurar directivas de firewall para controlar el tráfico que se envía al firewall y para registrar el tráfico.

El dispositivo SDX tiene dos interfaces de administración (0/1 y 0/2) y, según el modelo, hasta ocho puertos de datos 1G y ocho puertos de datos 10G. También puede usar los puertos de datos como puertos de administración (por ejemplo, cuando necesite configurar VLAN etiquetadas, porque el etiquetado no está permitido en las interfaces de administración). Si lo hace, el tráfico del Servicio de administración debe salir del dispositivo y, a continuación, volver al dispositivo. Puede enrutar este

tráfico u, de manera opcional, especificar una NSVLAN en una interfaz asignada a la instancia. Si una interfaz de administración es común entre una instancia y el Servicio de administración, el tráfico entre los dos no tiene que enrutarse. Sin embargo, si su configuración lo requiere explícitamente, el tráfico se puede enrutar.

Nota El etiquetado se admite en la versión 6.0 de Citrix Hypervisor.

Consolidación con interfaces dedicadas para cada instancia

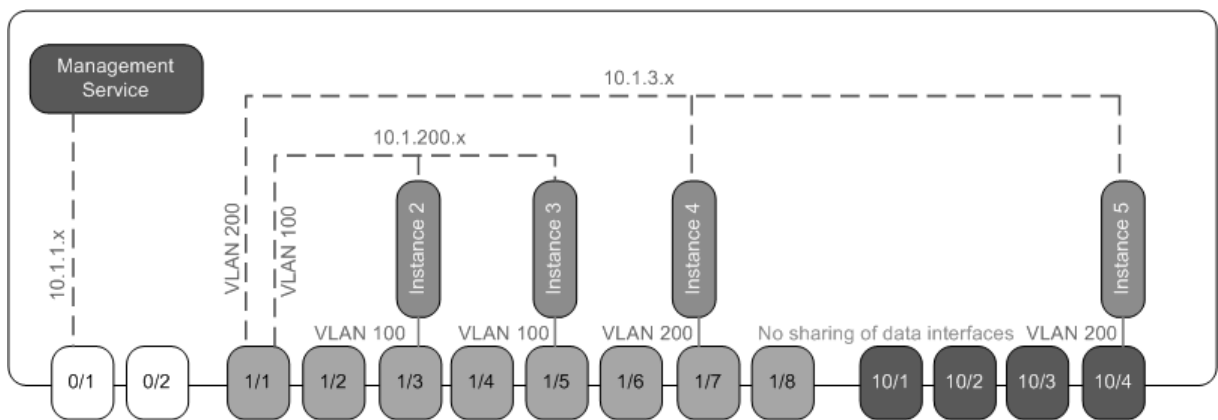
November 23, 2023

En el siguiente ejemplo, las instancias forman parte de varias redes. La interfaz 0/1 se asigna a Management Service, que forma parte de la red interna 10.1.1.x. Las instancias 2 y 3 de NetScaler forman parte de la red 10.1.200.x (VLAN 100). Las instancias 4 y 5 de NetScaler forman parte de la red 10.1.3.x (VLAN 200).

De manera opcional, puede configurar una NSVLAN en todas las instancias.

La siguiente ilustración ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con instancias de NetScaler en varias redes



El dispositivo SDX está conectado a un conmutador. Asegúrese de que los identificadores de VLAN 100 y 200 estén configurados en el puerto del conmutador al que está conectado el puerto 1/1 del dispositivo.

En la siguiente tabla se enumeran los nombres y valores de los parámetros utilizados para aprovisionar las instancias de NetScaler 5 y 3 en este ejemplo.

Nombre del parámetro	Valores de la instancia 5	Valores de la instancia 3
Nombre	vpx5	vpx3

Nombre del parámetro	Valores de la instancia 5	Valores de la instancia 3
Dirección IP	10.1.3.2	10.1.200.2
Máscara de red	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.200.1
Archivo XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licencia de funciones	Platinum	Platinum
Perfil de administrador	ns_nsroot_profile	ns_nsroot_profile
Nombre de usuario	vpx5	vpx3
Contraseña	Sdx1	root
Confirm Password	Sdx1	root
Acceso a Shell/Sftp/Scp	True	True
Memoria total (MB)	2048	2048
Fichas #SSL	1	1
Rendimiento (Mbps)	1000	1000
Paquetes por segundo	1000000	1000000
CPU	Compartida	Compartida
Interfaz	1/1 y 10/4	1/1 y 1/5
NSVLAN	200	100
Agregar (interfaz)	1/1	1/1
Interfaz etiquetada	Seleccione etiquetado	Seleccione etiquetado

Para aprovisionar las instancias 5 y 3 de NetScaler, como se muestra en este ejemplo

1. En la ficha **Configuración**, en el panel de navegación, expanda **Configuración de NetScaler** y, a continuación, haga clic en **Instancias**.
2. En el panel de instancias de NetScaler, haga clic en **Agregar**.
3. En el **asistente de aprovisionamiento de NetScaler**, siga las instrucciones del asistente para establecer los parámetros en los valores que se muestran en la tabla anterior.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**. La instancia de NetScaler que aprovisionó aparece en el panel de instancias de NetScaler.

Consolidación con el uso compartido de un puerto físico por más de una instancia

November 23, 2023

Puede habilitar e inhabilitar el filtrado de VLAN en una interfaz según sea necesario. Por ejemplo, para configurar más de 100 VLAN en una instancia, asigne una interfaz física dedicada a esa instancia e inhabilite el filtrado de VLAN en esa interfaz. Habilite el filtrado de VLAN en instancias que comparten una interfaz física, de modo que una instancia no pueda ver el tráfico de otra instancia.

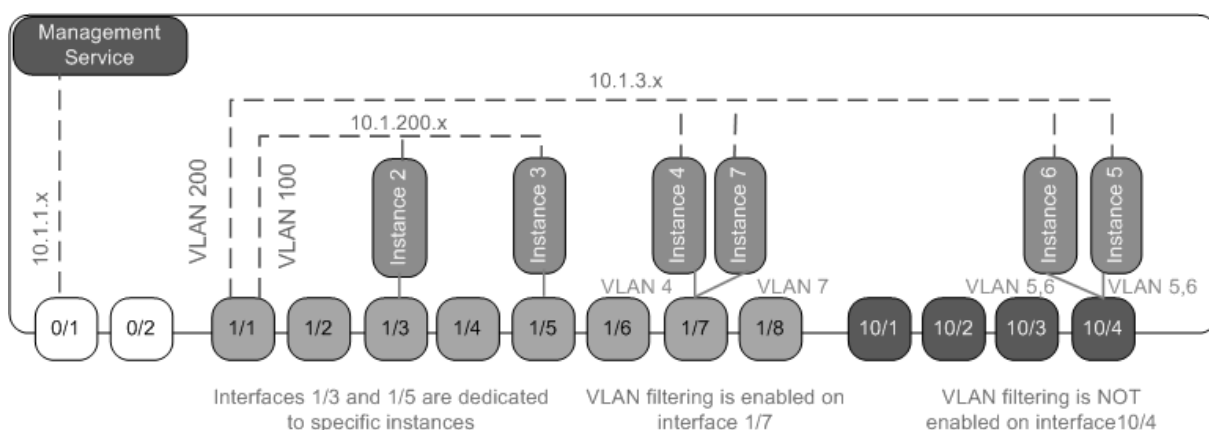
Nota: El filtrado de VLAN no es una configuración global en el dispositivo. Se habilita o inhabilita el filtrado de VLAN en una interfaz, y la configuración se aplica a todas las instancias asociadas a esa interfaz. Si el filtrado de VLAN está inhabilitado, puede configurar hasta 4096 VLAN. Si el filtrado de VLAN está habilitado, puede configurar hasta 63 VLAN etiquetadas en una interfaz 10G y hasta 32 VLAN etiquetadas en una interfaz 1G.

En el siguiente ejemplo, las instancias forman parte de varias redes.

- La interfaz 1/1 se asigna como interfaz de administración a todas las instancias. La interfaz 0/1 se asigna a Management Service, que forma parte de la red interna 10.1.1.x.
- Las instancias 2 y 3 de NetScaler están en la red 10.1.200.x y las instancias 4, 5, 6 y 7 están en la red 10.1.3.x. Cada una de las instancias 2 y 3 tiene una interfaz física dedicada. Las instancias 4 y 7 comparten la interfaz física 1/7, y las instancias 5 y 6 comparten la interfaz física 10/4.
- El filtrado de VLAN está habilitado en la interfaz 1/7. El tráfico de la instancia 4 se etiqueta para la VLAN 4 y el tráfico de la instancia 7 se etiqueta para la VLAN 7. Como resultado, el tráfico de la instancia 4 no es visible para la instancia 7. Por el contrario, el tráfico de la instancia 7 no es visible para la instancia 4. Se puede configurar un máximo de 32 VLAN en la interfaz 1/7.
- El filtrado de VLAN está inhabilitado en la interfaz 10/4, por lo que puede configurar hasta 4096 VLAN en esa interfaz. Configure las VLAN 500 a 599 en la instancia 5 y las VLAN 600 a 699 en la instancia 6. La instancia 5 puede ver el tráfico de difusión y multidifusión de VLAN 600 a 699, pero los paquetes se descartan en el nivel de software. Del mismo modo, la instancia 6 puede ver el tráfico de difusión y multidifusión desde las VLAN 500 a 599, pero los paquetes se descartan en el nivel de software.

La siguiente ilustración ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con instancias del Servicio de administración y NetScaler distribuidas en redes



En la siguiente tabla se enumeran los nombres y valores de los parámetros utilizados para aprovisionar las instancias de NetScaler 7 y 4 en este ejemplo.

Nombre del parámetro	Valores de la instancia 7	Valores de la instancia 4
Nombre	vpx7	vpx4
Dirección IP	10.1.3.7	10.1.3.4
Máscara de red	255.255.255.0	255.255.255.240
Gateway	10.1.3.1	10.1.3.1
Archivo XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licencia de funciones	Platinum	Platinum
Perfil de administrador	ns_nsroot_profile	ns_nsroot_profile
Nombre de usuario	vpx4	vpx4
Contraseña	Sdx1	Sdx1
Confirm Password	Sdx1	Sdx1
Acceso a Shell/Sftp/Scp	True	True
Memoria total (MB)	2048	2048
Fichas #SSL	1	1
Rendimiento (Mbps)	1000	1000
Paquetes por segundo	1000000	1000000
CPU	Compartida	Compartida
Interfaz	1/1 y 1/7	1/1 y 1/7
NSVLAN	200	200

Para aprovisionar instancias 7 y 4 de NetScaler en este ejemplo

1. En la ficha **Configuración**, en el panel de navegación, expanda Configuración de NetScaler y, a continuación, haga clic en **Instancias**.
2. En el panel de instancias de NetScaler, haga clic en **Agregar**.
3. En el asistente de aprovisionamiento de NetScaler, siga las instrucciones del asistente para establecer los parámetros en los valores que se muestran en la tabla anterior.
4. Haga clic en **Crear** y, a continuación, en **Cerrar**. La instancia de NetScaler que aprovisionó aparece en el panel de instancias de NetScaler.

API de NITRO

November 23, 2023

El protocolo NetScaler SDX NITRO permite configurar y supervisar el dispositivo SDX mediante programación.

NITRO expone su funcionalidad a través de interfaces de transferencia de estado representacional (REST). Por lo tanto, las aplicaciones NITRO se pueden desarrollar en cualquier lenguaje de programación. Además, para las aplicaciones que deben desarrollarse en Java, .NET o Python, el protocolo NITRO se expone como bibliotecas relevantes que se empaquetan como kits de desarrollo de software separados.

Nota: Debe tener un conocimiento básico del dispositivo SDX antes de usar NITRO.

Para usar el protocolo NITRO, la aplicación cliente necesita lo siguiente:

- Acceso a un dispositivo SDX.
- Para usar interfaces REST, debe tener un sistema para generar solicitudes HTTP o HTTPS (carga útil en formato JSON) para el dispositivo SDX. Puede usar cualquier lenguaje o herramienta de programación.
- Para los clientes de Java, debe tener un sistema en el que esté disponible la versión 1.5 o superior de Java Development Kit (JDK). El JDK se puede descargar desde <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.
- Para los clientes .NET, debe tener un sistema en el que esté disponible la versión .NET framework 3.5 o superior. .NET framework se puede descargar desde <http://www.microsoft.com/downloads/en/default.aspx>.
- Para los clientes de Python, debe tener un sistema donde esté instalada la versión de Python 2.7 o una posterior y la biblioteca de solicitudes (disponible en <NITRO_SDK_HOME>/lib).

Obtener el paquete NITRO

November 23, 2023

El paquete NITRO está disponible como un archivo TAR en la página Descargas de la utilidad de configuración del dispositivo SDX. Debe descargar y extraer el archivo TAR en una carpeta del sistema local. Esta carpeta se conoce como <NITRO_SDK_HOME> en esta documentación.

La carpeta contiene las bibliotecas NITRO en la subcarpeta lib. Las bibliotecas deben agregarse a la ruta de clase de la aplicación cliente para acceder a la funcionalidad de NITRO. La carpeta <NITRO_SDK_HOME> también proporciona ejemplos y documentación que pueden ayudarle a comprender el SDK de NITRO.

Nota:

- El paquete REST contiene solo documentación para el uso de las interfaces REST.
 - Para el SDK de Python, la biblioteca debe instalarse en la ruta del cliente. Para obtener instrucciones de instalación, consulte el archivo \Readme.txt.
- </div>

SDK de .NET

November 23, 2023

Las API de SDX NITRO se clasifican según el alcance y el propósito de las API en API del sistema y API de configuración. También puede solucionar los problemas de las operaciones de NITRO.

APIs del sistema

El primer paso para utilizar NITRO es establecer una sesión con el dispositivo SDX y, a continuación, autenticar la sesión mediante las credenciales del administrador.

Cree un objeto de la clase nitro_service especificando la dirección IP del dispositivo y el protocolo para conectarse al dispositivo (HTTP o HTTPS). A continuación, utilice este objeto e inicie sesión en el dispositivo especificando el nombre de usuario y la contraseña del administrador.

Nota: Debe tener una cuenta de usuario en ese dispositivo. Las operaciones de configuración que puede realizar están limitadas por la función administrativa asignada a su cuenta.

El siguiente código de ejemplo se conecta a un dispositivo SDX con la dirección IP 10.102.31.16 mediante el protocolo HTTPS:

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
3 );
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

Nota: Utilice el objeto

`nitro_service` en todas las operaciones NITRO posteriores en el dispositivo.

Para desconectarse del dispositivo, invoque el método `logout()` de la siguiente manera:

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

API de configuración

El protocolo NITRO se puede usar para configurar los recursos del dispositivo SDX.

Las API para configurar un recurso se agrupan en paquetes o espacios de nombres que tienen el formato `com.citrix.sdx.nitro.resource.config..` Cada uno de estos paquetes o espacios de nombres contiene una clase llamada que proporciona las API para configurar el recurso.

Por ejemplo, el recurso de NetScaler tiene el paquete o espacio de nombres `com.citrix.sdx.nitro.resource.config.ns`.

Una clase de recursos proporciona API para realizar otras operaciones. Estas operaciones pueden consistir en crear un recurso, recuperar recursos y propiedades de recursos, actualizar un recurso, eliminar recursos y realizar operaciones masivas en los recursos.

Crear un recurso

Para crear un recurso (por ejemplo, una instancia de NetScaler) en el dispositivo SDX:

1. Establezca el valor de las propiedades requeridas del recurso mediante el nombre de propiedad correspondiente. El resultado es un objeto de recurso que contiene los detalles requeridos para el recurso.

Nota: Estos valores se establecen localmente en el cliente. Los valores no se reflejan en el dispositivo hasta que se carga el objeto.

2. Cargue el objeto de recurso en el dispositivo mediante el método `add()` estático.

El siguiente código de ejemplo crea una instancia NetScaler denominada “`ns_instance`” en el dispositivo SDX:

```
1 ns newns = new ns();
2
3 //Set the properties of the NetScaler locally
4 newns.name = "ns_instance";
5 newns.ip_address = "10.70.136.5";
6 newns.netmask = "255.255.255.0";
7 newns.gateway = "10.70.136.1";
8 newns.image_name = "nsvpx-9.3.45_nc.xva";
9 newns.profile_name = "ns_nsroot_profile";
10 newns.vm_memory_total = 2048;
11 newns.throughput = 1000;
12 newns.pps = 1000000;
13 newns.license = "Standard";
14 newns.username = "admin";
15 newns.password = "admin";
16
17 int number_of_interfaces = 2;
18 network_interface[] interface_array = new network_interface[
    number_of_interfaces];
19
20 //Adding 10/1
21 interface_array[0] = new network_interface();
22 interface_array[0].port_name = "10/1";
23
24 //Adding 10/2
25 interface_array[1] = new network_interface();
26 interface_array[1].port_name = "10/2";
27
28 newns.network_interfaces = interface_array;
29
30 //Upload the NetScaler instance
31 ns result = ns.add(nitroservice, newns);
32 <!--NeedCopy-->
```

Recuperar detalles del recurso

Para recuperar las propiedades de un recurso en el dispositivo SDX, haga lo siguiente:

1. Recupere las configuraciones del dispositivo mediante el método `get()`. El resultado es un objeto de recurso.
2. Extraiga la propiedad requerida del objeto mediante el nombre de propiedad correspondiente.

El siguiente código de ejemplo recupera los detalles de todos los recursos de NetScaler:

```
1 //Retrieve the resource object from the SDX appliance
2 ns[] returned_ns = ns.get(nitroservice);
3
4 //Extract the properties of the resource from the object
5 Console.WriteLine(returned_ns[i].ip_address);
6 Console.WriteLine(returned_ns[i].netmask);
```



```
7 <!--NeedCopy-->
```

Recuperar estadísticas de recursos

Un dispositivo SDX recopila estadísticas sobre el uso de sus funciones. Puede recuperar estas estadísticas mediante NITRO.

El siguiente código de ejemplo recupera las estadísticas de una instancia de NetScaler con el ID 123456a:

```
1 ns obj = new ns();
2 obj.id = "123456a";
3 ns stats = ns.get(nitroservice, obj);
4 Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);
5 Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);
6 Console.WriteLine("Request rate/sec:" + stats.http_req);
7 <!--NeedCopy-->
```

Actualizar un recurso

Para actualizar las propiedades de un recurso existente en el dispositivo, haga lo siguiente:

1. Establezca la propiedad id en el identificador del recurso que se va a actualizar.
2. Establezca el valor de las propiedades requeridas del recurso mediante el nombre de propiedad correspondiente. El resultado es un objeto de recurso.
Nota: Estos valores se establecen localmente en el cliente. Los valores no se reflejan en el dispositivo hasta que se carga el objeto.
3. Cargue el objeto de recurso en el dispositivo mediante el método update().

El siguiente código de ejemplo actualiza el nombre de la instancia de NetScaler con el ID 123456a a "ns_instance_new":

```
1 ns update_obj = new ns();
2
3 //Set the ID of the NetScaler to be updated
4 update_obj.id = "123456a";
5
6 //Get existing NetScaler details
7 update_obj = ns.get(nitroservice, update_obj);
8
9 //Update the name of the NetScaler to "ns_instance_new" locally
10 update_obj.name = "ns_instance_new";
11
12 //Upload the updated NetScaler details
13 ns result = ns.update(nitroservice, update_obj);
14 <!--NeedCopy-->
```

Eliminar un recurso

Para eliminar un recurso existente, invoque el método estático `delete()` en la clase de recurso, pasando el ID del recurso que se va a quitar, como argumento.

En el siguiente código de ejemplo, se elimina una instancia de NetScaler con ID 1:

```
1 ns obj = new ns();
2 obj.id = "123456a";
3 ns.delete(nitroservice, obj);
4 <!--NeedCopy-->
```

Operaciones a granel

Puede consultar o cambiar varios recursos simultáneamente y, por lo tanto, minimizar el tráfico de red. Por ejemplo, puede agregar varios dispositivos NetScaler SDX en la misma operación.

Cada clase de recurso tiene métodos que toman una serie de recursos para agregar, actualizar y eliminar recursos. Para realizar una operación masiva, especifique los detalles de cada operación localmente y, a continuación, envíe los detalles de una vez al servidor.

Para tener en cuenta el error de algunas operaciones dentro de la operación masiva, NITRO le permite configurar uno de los siguientes comportamientos:

- **Salir.** Cuando se encuentra el primer error, la ejecución se detiene. Se confirman los comandos que se ejecutaron antes del error.
- **Continúe.** Todos los comandos de la lista se ejecutan incluso si algunos comandos fallan.

Nota: Configure el comportamiento requerido mientras establece una conexión con el dispositivo, estableciendo el parámetro `onerror` en el método `nitro_service()`.

El siguiente código de ejemplo agrega dos dispositivos ADC en una operación:

```
1 ns[] newns = new ns[2];
2
3 //Specify details of first NetScaler
4 newns[0] = new ns();
5 newns[0].name = "ns_instance1";
6 newns[0].ip_address = "10.70.136.5";
7 newns[0].netmask = "255.255.255.0";
8 newns[0].gateway = "10.70.136.1";
9 ...
10 ...
11
12 //Specify details of second NetScaler
13 newns[1] = new ns();
```

```
14 newns[1].name = "ns_instance2";
15 newns[1].ip_address = "10.70.136.8";
16 newns[1].netmask = "255.255.255.0";
17 newns[1].gateway = "10.70.136.1";
18 ...
19 ...
20
21 //upload the details of the ADC appliances to the NITRO server
22 ns[] result = ns.add(nitroservice, newns);
23 <!--NeedCopy-->
```

Gestión de excepciones

El campo `errorcode` indica el estado de la operación.

- Un código de error de 0 indica que la operación se ha realizado correctamente.
- Un código de error distinto de cero indica un error en el procesamiento de la solicitud NITRO.

El campo de mensaje de error proporciona una breve explicación y la naturaleza del error.

La clase `com.citrix.sdx.nitro.exception.nitro_exception` captura todas las excepciones en la ejecución de las API de NITRO. Para obtener información sobre la excepción, puede utilizar el método `getErrorCode()`.

Para obtener una descripción más detallada de los códigos de error, consulte la referencia de la API disponible en la carpeta `<NITRO_SDK_HOME>/doc`.

Servicios web REST

November 23, 2023

REST (Transferencia de estado representacional) es un estilo arquitectónico basado en solicitudes y respuestas HTTP simples entre el cliente y el servidor. REST se usa para consultar o cambiar el estado de los objetos en el lado del servidor. En REST, el lado del servidor se modela como un conjunto de entidades en el que cada entidad se identifica mediante una URL única.

Cada recurso también tiene un estado en el que se pueden realizar las siguientes operaciones:

- **Crear.** Los clientes pueden crear nuevos recursos del lado del servidor en un recurso “contenedor”. Puede pensar en los recursos contenedores como carpetas y en los recursos secundarios como archivos o subcarpetas. El cliente que llama proporciona el estado para que se cree el recurso. El estado se puede especificar en la solicitud mediante el formato XML o JSON. El cliente también puede especificar la URL única que identifica el nuevo objeto. Alternativamente, el

servidor puede elegir y devolver una URL única que identifique el objeto creado. El método HTTP utilizado para crear solicitudes es POST.

- **Lee.** Los clientes pueden recuperar el estado de un recurso especificando su URL con el método HTTP GET. El mensaje de respuesta contiene el estado del recurso, expresado en formato JSON.
- **Actualización.** Puede actualizar el estado de un recurso existente; para ello, especifique la dirección URL que identifica ese objeto y su nuevo estado en JSON o XML, o bien utilice el método PUT HTTP.
- **Eliminar.** Puede destruir un recurso que exista en el lado del servidor mediante el método HTTP DELETE y la URL que identifica el recurso que se va a eliminar.

Además de estas cuatro operaciones CLAE (Crear, Leer, Actualizar y Eliminar), los recursos pueden admitir otras operaciones o acciones. Estas operaciones utilizan el método HTTP POST, en el que el cuerpo de la solicitud en JSON especifica la operación que se va a realizar y los parámetros para esa operación.

Las API de SDX NITRO se clasifican según el alcance y el propósito de las API en API del sistema y API de configuración.

APIs del sistema

El primer paso para utilizar NITRO es establecer una sesión con el dispositivo SDX y, a continuación, autenticar la sesión mediante las credenciales del administrador.

Especifique el nombre de usuario y la contraseña en el objeto de inicio de sesión. El identificador de sesión que se crea debe especificarse en el encabezado de solicitud de todas las operaciones posteriores de la sesión.

Nota: Debe tener una cuenta de usuario en ese dispositivo. Las configuraciones que puede realizar están limitadas por la función administrativa asignada a su cuenta.

Para conectarse a un dispositivo SDX con la dirección IP 10.102.31.16 mediante el protocolo HTTPS:

- **URL** `https://10.102.31.16/nitro/v2/config/login/`
- **Método HTTP** POST
- **Solicitar**

- **Header**

```
1 Content-Type:application/vnd.com.citrix.sdx.login+json
2 <!--NeedCopy-->
```

Nota: También se pueden utilizar tipos de contenido como “application/x-www-form-urlencoded” que se admitían en versiones anteriores de NITRO. Asegúrese de que la carga útil sea la misma que la utilizada en versiones anteriores. Las cargas útiles propor-

cionadas en esta documentación solo son aplicables si el tipo de contenido es de la forma 'application/vnd.com.citrix.sdx.login + json'.

- Payload

```
1  {
2
3      "login":
4      {
5
6          "username": "nsroot",
7          "password": "verysecret"
8      }
9
10 }
11
12 <!--NeedCopy-->
```

• Carga útil de respuesta

- Header

```
1  HTTP/1.0 201 Created
2  Set-Cookie:
3  NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
4  <!--NeedCopy-->
```

Nota: Utilice el ID de sesión en todas las operaciones de NITRO posteriores en el dispositivo.

Nota: De forma predeterminada, la conexión con el dispositivo caduca después de 30 minutos de inactividad. Puede modificar el período de tiempo de espera especificando un nuevo período de tiempo de espera (en segundos) en el objeto de inicio de sesión. Por ejemplo, para modificar el período de tiempo de espera a 60 minutos, la carga útil de la solicitud es:

```
1  {
2
3      "login":
4      {
5
6          "username": "nsroot",
7          "password": "verysecret",
8          "timeout": 3600
9      }
10 }
11
12
13 <!--NeedCopy-->
```

También puede conectarse al dispositivo para realizar una sola operación, especificando el nombre de usuario y la contraseña en el encabezado de solicitud de la operación. Por ejemplo, para conectarse

a un dispositivo mientras se crea una instancia de NetScaler:

- **URL**
- **HTTP (método)**
- **Solicitar**

- **Header**

```
1 X-NITRO-USER:nsroot
2 X-NITRO-PASS:verysecret
3 Content-Type:application/vnd.com.citrix.sdx.ns+json
4 <!--NeedCopy-->
```

- **Payload**

```
1 {
2
3     "ns":
4     {
5
6         ...
7     }
8
9 }
10
11 <!--NeedCopy-->
```

- **Respuesta.**

- **Header**

```
1 HTTP/1.0 201 Created
2 <!--NeedCopy-->
```

Para desconectarse del dispositivo, utilice el método DELETE:

- **URL**
- **Método HTTP DELETE**
- **Solicitar**

- **Header**

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.login+json
3 <!--NeedCopy-->
```

API de configuración

El protocolo NITRO se puede usar para configurar los recursos del dispositivo SDX.

Cada recurso SDX tiene una URL única asociada, según el tipo de operación que se vaya a realizar. Las URL de las operaciones de configuración tienen el siguiente formato: `http://<IP>/nitro/v2/config/<resource_type>`

Crear un recurso

Para crear un recurso (por ejemplo, una instancia de NetScaler) en el dispositivo SDX, especifique el nombre del recurso y otros argumentos relacionados en el objeto de recurso específico. Por ejemplo, para crear una instancia de NetScaler llamada vpx1:

- **URL**
- **HTTP (método)**
- **Solicitar**

- Header

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.ns+json
3 <!--NeedCopy-->
```

- Payload

```
1 {
2
3   "ns":
4   {
5
6     "name":"vpx1",
7     "ip_address":"192.168.100.2",
8     "netmask":"255.255.255.0",
9     "gateway":"192.168.100.1",
10    "image_name":"nsvpx-9.3-45_nc.xva",
11    "vm_memory_total":2048,
12    "throughput":1000,
13    "pps":1000000,
14    "license":"Standard",
15    "profile_name":"ns_nsroot_profile",
16    "username":"admin",
17    "password":"admin",
18    "network_interfaces":
19    [
20      {
21
22        "port_name":"10/1"
23      }
24    ,
25      {
26
27        "port_name":"10/2"
28      }
29    ]
30  }
31 }
```

```
29
30     ]
31   }
32
33 }
34
35 <!--NeedCopy-->
```

Recuperar datos y estadísticas de los recursos

Los detalles de los recursos SDX se pueden recuperar de la siguiente manera:

- Para recuperar los detalles de un recurso específico en el dispositivo SDX, especifique el identificador del recurso en la URL.
- Para recuperar las propiedades de los recursos en función de algún filtro, especifique las condiciones del filtro en la URL.

La URL tiene el siguiente formato: `http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`

- Si es probable que su solicitud devuelva muchos recursos del dispositivo, puede recuperar estos resultados en fragmentos dividiéndolos en “páginas” y recuperándolos página por página.

Por ejemplo, suponga que quiere recuperar todas las instancias de NetScaler en un SDX que tenga 53 de ellas. En lugar de recuperar las 53 en una respuesta grande, configure los resultados para que se dividan en páginas de 10 instancias de NetScaler cada una (6 páginas en total). A continuación, recuperarlos del servidor página por página.

Especifique el recuento de páginas con el parámetro de cadena de consulta de tamaño de página y use el parámetro de cadena de consulta de número de página para especificar el número de página que quiere recuperar.

La URL tiene el siguiente formato: `http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

No tiene que recuperar todas las páginas ni recuperar las páginas en orden. Cada solicitud es independiente e incluso puede cambiar la configuración del tamaño de página entre solicitudes.

Nota: Para tener una idea de la cantidad de recursos que es probable que devuelva una solicitud, puede usar el parámetro de cadena de consulta `count` para solicitar que se devuelva un recuento de los recursos, en lugar de los recursos en sí. Para obtener el número de instancias de NetScaler disponibles, la URL sería

`http://<IP>/nitro/v2/config/<resource_type>?count=yes`

Para recuperar la información de configuración de la instancia de NetScaler con ID 123456a:

- **URL**

- **Método HTTP GET**

Actualizar un recurso

Para actualizar un recurso SDX existente, use el método PUT HTTP. En la carga útil de la solicitud HTTP, especifique el nombre y los demás argumentos que se deben cambiar. Por ejemplo, para cambiar el nombre de la instancia de NetScaler con el ID 123456a a vpx2:

- **URL**
- **HTTP (método)**
- **Solicitar carga útil**

- Header

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.ns+json
3 <!--NeedCopy-->
```

- Payload

```
1 {
2
3     "ns":
4     {
5
6         "name":"vpx2",
7         "id":"123456a"
8     }
9
10 }
11
12 <!--NeedCopy-->
```

Eliminar un recurso

Para eliminar un recurso existente, especifique el nombre del recurso que se eliminará en la URL. Por ejemplo, para eliminar una instancia de NetScaler con ID 123456a:

- **URL**
- **HTTP (método)**
- **Solicitar**

- Header

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.ns+json
3 <!--NeedCopy-->
```

Operaciones a granel

Puede consultar o cambiar varios recursos simultáneamente y, por lo tanto, minimizar el tráfico de red. Por ejemplo, puede agregar varios dispositivos NetScaler SDX en la misma operación. También puede agregar recursos de diferentes tipos en una solicitud.

Para tener en cuenta el error de algunas operaciones dentro de la operación masiva, NITRO le permite configurar uno de los siguientes comportamientos:

- **Salir.** Cuando se encuentra el primer error, la ejecución se detiene. Se confirman los comandos que se ejecutaron antes del error.
- **Continúe.** Todos los comandos de la lista se ejecutan incluso si algunos comandos fallan.

Nota: Configure el comportamiento requerido en el encabezado de la solicitud mediante el parámetro `X-NITRO-ONERROR`.

Para agregar 2 recursos de NetScaler en una operación y continuar si falla un comando:

- **URL.**
- **Método HTTP.**
- **Solicitar carga útil.**

- Header

```
1 Cookie:NITRO_AUTH_TOKEN=tokenvalue
2 Content-Type:application/vnd.com.citrix.sdx.ns+json
3 X-NITRO-ONERROR:continue
4 <!--NeedCopy-->
```

- Payload

```
1 {
2
3   "ns":
4   [
5     {
6
7       "name":"ns_instance1",
8       "ip_address":"10.70.136.5",
9       "netmask":"255.255.255.0",
10      "gateway":"10.70.136.1"
11    }
12   ,
13   {
14
15     "name":"ns_instance2",
16     "ip_address":"10.70.136.8",
17     "netmask":"255.255.255.0",
18     "gateway":"10.70.136.1"
19   }
20 }
```

```
21     ]
22   }
23
24   <!--NeedCopy-->
```

Para agregar varios recursos (NetScaler y dos usuarios de MPS) en una operación y continuar si falla un comando:

- **URL.**
- **Método HTTP.** POST
- **Solicitar carga útil.**

- **Header**

```
1  Cookie:NITRO_AUTH_TOKEN=tokenvalue
2  Content-Type:application/vnd.com.citrix.sdx.ns+json
3  X-NITRO-ONERROR:continue
4  <!--NeedCopy-->
```

- **Payload**

```
1  {
2
3    "ns":
4    [
5      {
6
7        "name":"ns_instance1",
8        "ip_address":"10.70.136.5",
9        "netmask":"255.255.255.0",
10       "gateway":"10.70.136.1"
11      }
12     ,
13     {
14
15       "name":"ns_instance2",
16       "ip_address":"10.70.136.8",
17       "netmask":"255.255.255.0",
18       "gateway":"10.70.136.1"
19     }
20   ],
21   "mpsuser":
22   [
23     {
24
25       "name":"admin",
26       "password":"admin",
27       "permission":"superuser"
28     }
29   ],
30   {
31
```

```
32
33     "name": "admin",
34     "password": "admin",
35     "permission": "superuser"
36   }
37
38 ]
39 }
40
41 <!--NeedCopy-->
```

Gestión de excepciones

El campo errorcode indica el estado de la operación.

- Un código de error de 0 indica que la operación se ha realizado correctamente.
- Un código de error distinto de cero indica un error en el procesamiento de la solicitud NITRO.

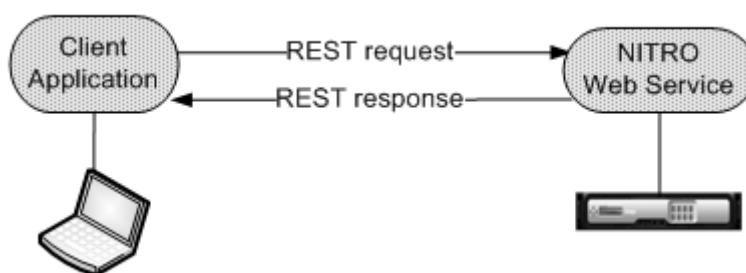
El campo de mensaje de error proporciona una breve explicación y la naturaleza del error.

Cómo funciona NITRO

November 23, 2023

La infraestructura de NITRO consiste en una aplicación cliente y el servicio web NITRO que se ejecuta en un dispositivo NetScaler SDX. La comunicación entre la aplicación cliente y el servicio web NITRO se basa en la arquitectura REST mediante HTTP o HTTPS.

Figura 1. Flujo NITRO trabajo de



Pasos que describen el flujo de trabajo:

1. La aplicación cliente envía un mensaje de solicitud REST al servicio web NITRO. Cuando se usan los SDK, una llamada a la API se traduce en el mensaje de solicitud REST apropiado.
2. El servicio web procesa el mensaje de solicitud REST.

3. El servicio web NITRO devuelve el mensaje de respuesta REST correspondiente a la aplicación cliente. Cuando se utilizan los SDK, el mensaje de respuesta REST se traduce en la respuesta adecuada para la llamada a la API.

Para minimizar el tráfico en la red, recupere el estado completo de un recurso del servidor. Realice modificaciones en el estado del recurso de forma local. A continuación, vuelva a cargarlo en el servidor en una transacción de red.

Nota: Las operaciones locales de un recurso (cambios en sus propiedades) no afectan a su estado en el servidor hasta que el estado del objeto se cargue de forma explícita.

Las API de NITRO son sincrónicas. Es decir, la aplicación cliente espera una respuesta del servicio web de NITRO antes de ejecutar otra API de NITRO.

SDK de Java

November 23, 2023

Las API de SDX NITRO se clasifican según el alcance y el propósito de las API en API del sistema y API de configuración. También puede solucionar los problemas de las operaciones de NITRO.

APIs del sistema

El primer paso para utilizar NITRO es establecer una sesión con el dispositivo SDX y, a continuación, autenticar la sesión mediante las credenciales del administrador.

Cree un objeto de la clase `nitro_service` especificando la dirección IP del dispositivo y el protocolo para conectarse al dispositivo (HTTP o HTTPS). A continuación, utilice este objeto e inicie sesión en el dispositivo especificando el nombre de usuario y la contraseña del administrador.

Nota: Debe tener una cuenta de usuario en ese dispositivo. Las operaciones de configuración que puede realizar están limitadas por la función administrativa asignada a su cuenta.

El siguiente código de ejemplo se conecta a un dispositivo SDX con la dirección IP 10.102.31.16 mediante el protocolo HTTPS:

```
1 //Specify the IP address of the appliance and service type
2 nitro_service nitroservice = new nitro_service ("10.102.31.16", "https"
3 );
4 //Specify the login credentials
5 nitroservice.login("nsroot", "verysecret");
6 <!--NeedCopy-->
```

Nota: Utilice el objeto

`nitro_service` en todas las operaciones NITRO posteriores en el dispositivo.

Para desconectarse del dispositivo, invoque el método `logout()` de la siguiente manera:

```
1 nitroservice.logout();
2 <!--NeedCopy-->
```

API de configuración

El protocolo NITRO se puede usar para configurar los recursos del dispositivo SDX.

Las API para configurar un recurso se agrupan en paquetes o espacios de nombres que tienen el formato `com.citrix.sdx.nitro.resource.config..` Cada uno de estos paquetes o espacios de nombres contiene una clase llamada que proporciona las API para configurar el recurso.

Por ejemplo, el recurso de NetScaler tiene el paquete o espacio de nombres `com.citrix.sdx.nitro.resource.config.ns`.

Una clase de recursos proporciona API para realizar muchas otras operaciones. Estas operaciones pueden consistir en crear un recurso, recuperar los detalles y las estadísticas de los recursos, actualizar un recurso, eliminar recursos y realizar operaciones masivas en los recursos.

Creación de un recurso

Para crear un recurso (por ejemplo, una instancia de NetScaler) en el dispositivo SDX, haga lo siguiente:

1. Establezca el valor de las propiedades requeridas del recurso mediante el nombre de propiedad correspondiente. El resultado es un objeto de recurso que contiene los detalles requeridos para el recurso.
Nota: Estos valores se establecen localmente en el cliente. Los valores no se reflejan en el dispositivo hasta que se carga el objeto.
2. Cargue el objeto de recurso en el dispositivo mediante el método `add()` estático.

El siguiente código de ejemplo crea una instancia NetScaler denominada “`ns_instance`” en el dispositivo SDX:

```
1 ns newns = new ns();
2
3 //Set the properties of the NetScaler locally
4 newns.set_name("ns_instance");
5 newns.set_ip_address("10.70.136.5");
6 newns.set_netmask("255.255.255.0");
7 newns.set_gateway("10.70.136.1");
8 newns.set_image_name("nsvpx-9.3.45_nc.xva");
9 newns.set_profile_name("ns_nsroot_profile");
```

```
10 newns.set_vm_memory_total(new Double(2048));
11 newns.set_throughput(new Double(1000));
12 newns.set_pps(new Double(1000000));
13 newns.set_license("Standard");
14 newns.set_username("admin");
15 newns.set_password("admin");
16
17 int number_of_interfaces = 2;
18 network_interface[] interface_array = new network_interface[
    number_of_interfaces];
19
20 //Adding 10/1
21 interface_array[0] = new network_interface();
22 interface_array[0].set_port_name("10/1");
23
24 //Adding 10/2
25 interface_array[1] = new network_interface();
26 interface_array[1].set_port_name("10/2");
27
28 newns.set_network_interfaces(interface_array);
29
30 //Upload the NetScaler instance
31 ns result = ns.add(nitroservice, newns);
32 <!--NeedCopy-->
```

Recuperación de detalles de recursos

Para recuperar las propiedades de un recurso en el dispositivo SDX, haga lo siguiente:

1. Recupere las configuraciones del dispositivo mediante el método `get()`. El resultado es un objeto de recurso.
2. Extraiga la propiedad requerida del objeto mediante el nombre de propiedad correspondiente.

El siguiente código de ejemplo recupera los detalles de todos los recursos de NetScaler:

```
1 //Retrieve the resource object from the SDX appliance
2 ns[] returned_ns = ns.get(nitroservice);
3
4 //Extract the properties of the resource from the object
5 System.out.println(returned_ns[i].get_ip_address());
6 System.out.println(returned_ns[i].get_netmask());
7 <!--NeedCopy-->
```

Recuperación de estadísticas de recursos

Un dispositivo SDX recopila estadísticas sobre el uso de sus funciones. Puede recuperar estas estadísticas mediante NITRO.

El siguiente código de ejemplo recupera las estadísticas de una instancia de NetScaler con el ID 123456a:

```
1 ns obj = new ns();
2 obj.set_id("123456a");
3 ns stats = ns.get(nitroservice, obj);
4 System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());
5 System.out.println("Memory Usage:" + stats.get_ns_memory_usage());
6 System.out.println("Request rate/sec:" + stats.get_http_req());
7 <!--NeedCopy-->
```

Actualización de un recurso

Para actualizar las propiedades de un recurso existente en el dispositivo, haga lo siguiente:

1. Establezca la propiedad id en el identificador del recurso que se va a actualizar.
2. Establezca el valor de las propiedades requeridas del recurso mediante el nombre de propiedad correspondiente. El resultado es un objeto de recurso.
Nota: Estos valores se establecen localmente en el cliente. Los valores no se reflejan en el dispositivo hasta que se carga el objeto.
3. Cargue el objeto de recurso en el dispositivo mediante el método update().

El siguiente código de ejemplo actualiza el nombre de la instancia de NetScaler con el ID 123456a a “ns_instance_new”:

```
1 ns update_obj = new ns();
2
3 //Set the ID of the NetScaler to be updated
4 update_obj.set_id("123456a");
5
6 //Get existing NetScaler details
7 update_obj = ns.get(nitroservice, update_obj);
8
9 //Update the name of the NetScaler to "ns_instance_new" locally
10 update_obj.set_name("ns_instance_new");
11
12 //Upload the updated NetScaler details
13 ns result = ns.update(nitroservice, update_obj);
14 <!--NeedCopy-->
```

Eliminación de un recurso

Para eliminar un recurso existente, invoque el método estático delete() en la clase de recurso, pasando el ID del recurso que se va a quitar, como argumento.

En el siguiente código de ejemplo, se elimina una instancia de NetScaler con ID 1:


```
1 ns obj = new ns();
2 obj.set_id("123456a");
3 ns.delete(nitro_service, obj);
4 <!--NeedCopy-->
```

Operaciones a granel

Puede consultar o cambiar varios recursos simultáneamente y, por lo tanto, minimizar el tráfico de red. Por ejemplo, puede agregar varios dispositivos NetScaler SDX en la misma operación.

Cada clase de recurso tiene métodos que toman una serie de recursos para agregar, actualizar y eliminar recursos. Para realizar una operación masiva, especifique los detalles de cada operación localmente y, a continuación, envíe los detalles de una vez al servidor.

Para tener en cuenta el error de algunas operaciones dentro de la operación masiva, NITRO le permite configurar uno de los siguientes comportamientos:

- **Salir.** Cuando se encuentra el primer error, la ejecución se detiene. Se confirman los comandos que se ejecutaron antes del error.
- **Continúe.** Todos los comandos de la lista se ejecutan incluso si algunos comandos fallan.

Nota: Configure el comportamiento requerido mientras establece una conexión con el dispositivo, estableciendo el parámetro

`onerror` en el método `nitro_service()`.

El siguiente código de ejemplo agrega dos dispositivos ADC en una operación:

```
1 ns[] newns = new ns[2];
2
3 //Specify details of first NetScaler
4 newns[0] = new ns();
5 newns[0].set_name("ns_instance1");
6 newns[0].set_ip_address("10.70.136.5");
7 newns[0].set_netmask("255.255.255.0");
8 newns[0].set_gateway("10.70.136.1");
9 ...
10 ...
11 ...
12
13 //Specify details of second NetScaler
14 newns[1] = new ns();
15 newns[1].set_name("ns_instance2");
16 newns[1].set_ip_address("10.70.136.8");
17 newns[1].set_netmask("255.255.255.0");
18 newns[1].set_gateway("10.70.136.1");
19 ...
20 ...
```

```
21
22 //upload the details of the NetScalers to the NITRO server
23 ns[] result = ns.add(nitroservice, newns);
24 <!--NeedCopy-->
```

Gestión de excepciones

El campo `errorcode` indica el estado de la operación.

- Un código de error de 0 indica que la operación se ha realizado correctamente.
- Un código de error distinto de cero indica un error en el procesamiento de la solicitud NITRO.

El campo de mensaje de error proporciona una breve explicación y la naturaleza del error.

La clase `com.citrix.sdx.nitro.exception.nitro_exception` captura todas las excepciones en la ejecución de las API de NITRO. Para obtener información sobre la excepción, puede utilizar el método `getErrorCode()`.

Para obtener una descripción más detallada de los códigos de error, consulte la referencia de la API disponible en la carpeta `<NITRO_SDK_HOME>/doc`.



© 2023 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).
