Citrix ADC SDX 13.0

Machine translated content

Disclaimer

Contents

Introducción

June 19, 2019

El dispositivo Citrix ADC SDX es una plataforma multiarrendatario en la que puede aprovisionar y administrar varias máquinas virtuales Citrix ADC (instancias). 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 de memoria y CPU dedicados
  - Un espacio separado para entidades
  - La independencia para ejecutar el lanzamiento y construcción de su elección
  - Independencia del ciclo de vida
- Una red completamente aislada. El tráfico destinado a una instancia determinada 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 está preempaquetado para compatibilidad con HTTPS. Citrix recomienda utilizar el modo HTTPS para acceder a la interfaz de usuario de Management Service.

Notas de la versión

June 19, 2019

Las notas de la versión describen las mejoras, los cambios, las correcciones de errores y los problemas conocidos de una versión o compilación concreta del software Citrix ADC. Las notas de la versión de Citrix ADC SDX se tratan como parte de las notas de la versión de Citrix ADC.

Para obtener información detallada sobre las mejoras de SDX 13.0, problemas conocidos y correcciones de errores, consulte Notas de la versión de Citrix ADC.

Introducción a la interfaz de usuario de Management Service

June 19, 2019

Para comenzar a configurar, administrar y supervisar el dispositivo, Management Service y las instancias virtuales, debe conectarse a la interfaz de usuario de Management Service mediante un explorador y, a continuación, aprovisionar las instancias virtuales en el dispositivo.

Puede conectarse a la interfaz de usuario de Management Service mediante uno de los siguientes exploradores compatibles:

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

Iniciar sesión en la interfaz de usuario de Management Service

Para iniciar sesión en la interfaz de usuario de Management Service

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

   ```
   http://Management Service IP Address
   ```

   o

   ```
   https://Management Service IP Address
   ```

2. En la página Inicio de sesión, en Nombre de usuario y contraseña, escriba el nombre de usuario y la contraseña de Management Service. El nombre de usuario y la contraseña predeterminados son nsroot y nsroot. Sin embargo, Citrix recomienda cambiar la contraseña después de la configuración inicial. Para obtener información sobre cómo cambiar la contraseña nsroot, consulteCambiar la contraseña de la cuenta de usuario predeterminada.

3. Haga clic en Mostrar opciones y, a continuación, haga lo siguiente:

   a) En la lista Iniciar 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 período de tiempo (en minutos, horas o días) después del cual quiere que caduque la sesión. El valor mínimo de tiempo de espera es de 15 minutos.

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

4. Haga clic en Iniciar sesión para iniciar sesión en la interfaz de usuario de Management Service.

Asistente de configuración inicial

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

Puede utilizar el asistente para configurar los detalles de la configuración de red y la configuración 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 especificados 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.

En la página Configuración de plataforma, puede configurar los detalles de la configuración de red, la configuración del sistema y cambiar la contraseña administrativa predeterminada.

- Interfaz *: Interfaz a través de la cual los clientes se conectan a Management Service. Valores posibles: 0/1, 0/2. Predeterminado: 0/1.
- Dirección IP de XenServer *: Dirección IP del servidor XenServer.
- Dirección IP de Management Service *: Dirección IP de Management Service.
- Máscara de red *: Máscara de la subred en la que se encuentra el dispositivo SDX.
- Puerta de enlace *: Puerta de enlace predeterminada para la red.
- Servidor DNS: Dirección IP del servidor DNS.

En Configuración del sistema, puede especificar que Management Service y una instancia de Citrix ADC se comuniquen entre sí solo a través de un canal seguro. También puede restringir el acceso a la interfaz de usuario de Management Service. Los clientes pueden iniciar sesión en la interfaz de usuario de Management Service solo mediante https.

Puede modificar la zona horaria de Management Service y del servidor XenServer. La zona horaria predeterminada es UTC. Puede cambiar la contraseña administrativa activando la casilla de verificación Cambiar contraseña y escribiendo la nueva contraseña.

En Administrar licencias, puede administrar y asignar licencias. Puede utilizar su número de serie de hardware (HSN) o su código de activación de licencia (LAC) para asignar sus licencias. Como alternativa, si ya existe una licencia en el equipo local, puede cargarla en el dispositivo.

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

Provisionamiento de instancias en un dispositivo SDX

Puede aprovisionar una o varias instancias de Citrix ADC o de terceros en el dispositivo SDX mediante Management Service. El número 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, 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 instancias de Citrix ADC, Management Service, XenServer y máquinas virtuales de terceros desde la interfaz de Management Service. Esto resulta especialmente útil para depurar y solucionar problemas de las instancias alojadas en el dispositivo SDX.

Para acceder a la consola de máquinas virtuales, desplácese hasta la lista de instancias, seleccione la máquina virtual de la lista y, en el menú desplegable Acción, haga clic en Acceso a la consola.

Para acceder a la consola de Management Service o XenServer, vaya a Configuración > Sistema y, en Acceso a la consola, haga clic en el vínculo Management Service o XenServer.

Nota: El explorador Internet Explorer no admite el acceso a la consola. Citrix recomienda utilizar la función de acceso a la consola únicamente a través de sesiones HTTPS de Management Service.

Estadísticas de Management Service

El panel incluye ahora Estadísticas de Management Service para supervisar el uso de la memoria, la CPU y los recursos de disco por parte de Management Service en el dispositivo SDX.

Single Sign-On en Management Service y las instancias de Citrix ADC

El inicio de sesión en Management Service le proporciona acceso directo a las instancias de Citrix ADC que se aprovisionan en el dispositivo, si las instancias ejecutan la versión 10, compilación 53 y posterior. Si inicia sesión en Management Service con las credenciales de usuario, no es necesario que vuelva 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.

Administración de la página principal

La página inicial de Management Service proporciona una vista de alto nivel del rendimiento del dispositivo SDX y de las instancias aprovisionadas en el dispositivo. La información de instancia y del dispositivo SDX se muestra en gadgets que puede agregar y quitar en función de sus necesidades.

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 del dispositivo.

- CPU del sistema | Uso de memoria (%)

  Muestra el porcentaje de utilización de CPU y 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 Citrix ADC

  Muestra las propiedades de las instancias de Citrix ADC. Las propiedades que se muestran son Nombre, Estado de VM, Estado de instancia, Dirección IP, Rx (Mbps), Tx (Mbps), Req/s HTTP y Uso de CPU (%) y Uso de memoria (%).
  Nota: Al iniciar la primera sesión, la
  página principal no muestra ningún dato relacionado con las instancias de
  Citrix ADC porque no ha aprovisionado ninguna instancia en el dispositivo.

- Eventos
  de monitoreo de 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 Citrix ADC

  Puede ver y ocultar los detalles de una instancia concreta de
  Citrix ADC 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 instancia y Contraer todo para contraer todos los nodos de instancia.

- Agregar y quitar gadgets

  También puede agregar gadgets para ver información adicional 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. Después de mostrar el gadget, haga clic en Agregar al panel.

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

  - Detalles del
    hipervisor

El gadget Detalles del hipervisor muestra detalles sobre el tiempo de actividad de XenServer, la edición, la versión, el nombre calificado iSCSI (IQN), el código del producto, el número de serie, la fecha de compilación y el número de compilación.

- Licencias

  El gadget Licencias muestra detalles sobre 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 principal realizando una búsqueda del gadget, como se describió anteriormente.

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 entrantes (GUI y NITRO). Una de las interfaces principales para acceder a la interfaz de SDX Management Service.
TCP	443	Se utiliza para solicitudes HTTP seguras entrantes (GUI y NITRO). 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 de SDX Management Service escucha las capturas SNMP de las instancias Citrix ADC alojadas en el dispositivo SDX.

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

Actualización de un solo paquete

June 19, 2019

Para versiones 10.5 y anteriores, la configuración del dispositivo SDX incluye la configuración del hipervisor XenServer, sus paquetes y revisiones adicionales, Management Service, las máquinas virtuales Citrix ADC y el firmware LOM. Cada uno de estos componentes tiene un ciclo de liberación diferente. Por lo tanto, la actualización de cada componente de forma independiente, según lo permitido por SDX 10.5 y versiones anteriores, dificulta el mantenimiento. La actualización de cada componente por separado también conduce a combinaciones de componentes no compatibles.

La actualización de un solo paquete, disponible a partir de las versiones 11.0 y posteriores, combina todos los componentes excepto la imagen de instancia de Citrix ADC VPX y el firmware LOM en un solo archivo de imagen, denominado imagen SDX. Con esta imagen, puede actualizar todos los componentes en un solo paso, eliminando las posibilidades de incompatibilidad entre varios componentes. La actualización de un solo paquete también garantiza que el dispositivo esté siempre ejecutando una versión probada y compatible con Citrix. Dado que todos los componentes SDX se combinan en un solo archivo, el archivo de imagen SDX es significativamente mayor que el archivo de imagen de Management Service.

El nombre de archivo de la imagen tiene el formato build-sdx-13.0-<build_number>.tgz.** Después de actualizar Management Service a SDX 13.0, la nueva GUI no muestra las opciones para cargar el archivo de imagen de XenServer, los paquetes complementarios o las revisiones. Esto se debe a que SDX 13.0 no admite la actualización de componentes individuales.

Puntos a 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 Management Service. Vuelva a conectarse a Management Service para supervisar el estado de la actualización.

- A continuación, el nuevo Management Service actualiza XenServer y completa el resto de la actualización del dispositivo. Management Service desde la versión 11.0 y posterior es capaz de realizar una actualización completa de XenServer.
- No reinicie el dispositivo durante la actualización de XenServer.
- Citrix recomienda utilizar una consola serie de XenServer (o una consola LOM) para supervisar la actualización de XenServer.

> Nota: No se admite la actualización directa de la versión 10.5 a 13.0. Primero debe actualizar de 10.5 a 11.0 o 11.1 o 12.0 o 12.1 y, a continuación, actualizar a SDX 13.0.

Actualización de todo el dispositivo a 13.0

Si actualmente está ejecutando la versión 10.5.66.x o posterior de SDX Management Service, puede utilizar el archivo de imagen SDX 13.0 para actualizar el dispositivo. Si Management Service ejecuta una versión anterior, primero debe actualizarla a la versión 10.5.66.x o posterior.

Para actualizar el dispositivo:

1. Cargue el archivo de imagen de paquete único, vaya a **Configuración > Management Service > Imágenes de software** y, a continuación, haga clic en **Cargar**.
2. Vaya a **Configuración > Sistema > Administración del Sistema**. Vaya al **paso 3**. Si va a actualizar desde la versión 10.55 66.x y posterior. Vaya al **paso 4**, si está actualizando desde la versión 11.0
3. En el grupo Administración del sistema, haga clic en **Actualizar Management Service**.
4. En el grupo Administración del sistema, haga clic en **Actualizar dispositivo**.
   El proceso de actualización tarda unos minutos.

Antes de la actualización, Management Service 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 actualizará el dispositivo
- Tiempo aproximado para actualizar el dispositivo
- Información diversa

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

Información relacionada

Desmitificar el proceso de actualización del dispositivo NetScaler SDX

Actualizar una instancia de Citrix ADC

June 19, 2019

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

Es necesario cargar las imágenes del software Citrix ADC en el dispositivo Citrix ADC SDX antes de actualizar las instancias de Citrix ADC. Para instalar una nueva instancia, necesita el archivo XVA de Citrix ADC.

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

- **Nombre**

Nombre del archivo de imagen de software de instancia de Citrix ADC. El nombre del archivo contiene el número de versión y compilación. Por ejemplo, el nombre de archivo build-10-53.5_nc.tgz hace referencia a la versión 10 build 53.5.

- **Última modificación**

Fecha en la que se modificó el archivo por última vez.

- **Tamaño:**

Tamaño, en MB, del archivo.

Para cargar una imagen de software

1. En el panel de navegación, expanda Cirix ADC 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 Citrix ADC**, haga clic en **Examinar** y seleccione el archivo de imagen Citrix ADC que desea cargar.
4. Haz clic en **Subir**. El archivo de imagen aparece en el panel Imágenes de software Citrix ADC.

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

Para cargar un archivo XVA

1. En el panel de navegación, expanda Cirix ADC 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 Citrix ADC**, haga clic en **Examinar** y seleccione el archivo XVA de Citrix ADC que desee cargar.
4. Haz clic en **Subir**. 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 desea 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 del mensaje **Guardar como**, busque la ubicación en la que quiere guardar el archivo y, a continuación, haga clic en **Guardar**.

Actualización de instancias de Citrix ADC VPX

Puede utilizar Management Service para actualizar una o varias instancias de VPX que se ejecutan en el dispositivo. Antes de actualizar una instancia, asegúrese de que ha cargado la compilación correcta en el dispositivo SDX.

Antes de empezar a actualizar cualquier instancia, asegúrese de comprender el marco de licencias y los tipos de licencias. Una actualización de la edición de software puede requerir nuevas licencias, como la actualización de la edición estándar a la edición empresarial, la edición estándar a la edición platino o la edición empresarial a la edición platino. Tenga en cuenta también lo siguiente:

- Para evitar cualquier pérdida de configuración, guarde la configuración en cada instancia antes de actualizar las instancias.
- También puede actualizar una instancia individual desde el nodo Instancias. Para ello, 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.
- Si ha configurado un canal desde la instancia de Citrix ADC y desea actualizar la instancia de Citrix ADC versión 10 a la versión 10.1 o posterior, debe eliminar todos los canales de la instancia de Citrix ADC, actualizarla y, a continuación, crear canales LACP desde Management Service. Si está degradando la instancia de Citrix ADC de la versión 10.1 a la versión 10.0, debe eliminar todos los canales LACP de Management Service, degradar la instancia y, a continuación, crear los canales LACP a partir de la instancia VPX.
- **Importante**

Utilice SDX Management Service únicamente y no la GUI de VPX para actualizar instancias VPX, de modo que durante las copias de seguridad las imágenes de actualización formen parte del archivo de copia de seguridad. Estos archivos de copia de seguridad le ayudan a restaurar la instancia sin problemas

Actualización de instancias VPX

1. En la ficha **Configuración**, en el panel de navegación, haga clic en **Citrix ADC**.
2. En el panel de detalles, en **Configuración de Citrix ADC**, haga clic en **Actualizar**.
3. En el cuadro de diálogo **Actualizar Citrix ADC**, en **Imagen de software**, seleccione el archivo de compilación de actualización de Citrix ADC de la versión a la que desea actualizar.
4. En la lista desplegable **Dirección IP de instancia**, seleccione las direcciones IP de las instancias que desea actualizar.
5. Haga clic en **Aceptar**y, a continuación, haga clic en Cerrar.

Administrar y supervisar el dispositivo SDX

June 19, 2019

Una vez que el dispositivo Citrix ADC SDX esté en funcionamiento, puede realizar varias tareas para administrar y supervisar el dispositivo desde la interfaz de usuario de Management Service.

Si una tarea que necesita realizar no se describe a continuación, consulte la lista de tareas a la izquierda.

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

Modificación de la configuración de red del dispositivo SDX

Puede modificar los detalles de configuración de red proporcionados 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 instalación**, haga clic en **Configuración de red** e introduzca los detalles en el asistente.

Cambiar la contraseña de la cuenta de usuario predeterminada

La cuenta de usuario predeterminada proporciona acceso completo a todas las funciones del dispositivo Citrix SDX. Por lo tanto, para preservar la seguridad, la cuenta nsroot debe usarse solo cuando sea necesario, y solo las personas cuyos deberes requieran acceso completo deben conocer la contraseña de la cuenta nsroot. Citrix recomienda cambiar la contraseña nsroot con frecuencia. Si pierde la contraseña, puede restablecer la contraseña a la predeterminada volviendo la configuración del dispositivo a los valores predeterminados de fábrica y, a continuación, puede cambiar la contraseña.

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.

Modificación de la zona horaria en el dispositivo

Puede modificar la zona horaria de Management Service y del servidor Xen. 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**.

Modificación del nombre de host del dispositivo

Puede cambiar el nombre de host de Management Service.

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 solo alcanza la instancia que pertenece a la VLAN etiquetada correspondiente. Si ninguna de las instancias pertenece a la VLAN etiquetada correspondiente, el paquete se elimina en el nivel de hardware (NIC).

Si el filtrado de VLAN está habilitado en una interfaz, se puede utilizar 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: Elfiltrado de VLAN solo se puede inhabilitar en un dispositivo SDX que ejecute XenServer 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.

Configuración de la sincronización del reloj

Puede configurar el dispositivo SDX para que sincronice su reloj local con un servidor NTP (Network Time Protocol). 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 rebaja. Sin embargo, la configuración no se propaga a la instancia secundaria de Citrix ADC en una configuración de alta disponibilidad.

El reloj se sincroniza inmediatamente si agrega un nuevo 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 oficial de NTP, http://www.ntp.org. Antes de configurar el de Citrix ADC 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 NTP

1. En el panel de navegación, expanda Sistema y, 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 NTP, seleccione Habilitar sincronización NTP.
4. Haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Para modificar las opciones de autenticación

1. En el panel de navegación, expanda Sistema y, 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: Habilite la autenticación NTP. Valores posibles: SÍ, NO. Valor predeterminado: SÍ.

- ID de clave de confianza: ID de clave de confianza. Al agregar un servidor NTP, seleccione un identificador de clave de esta lista. Valor mínimo: 1. Valor máximo: 65534.
- Revocar Intervalo: El intervalo entre la realeatorización de ciertos valores criptográficos utilizados por el esquema de Autoclave, como una potencia de 2, en segundos. Valor predeterminado: 17 (2 ^ 17 = 36 horas).
- Intervalo automático: 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, haga clic en Cerrar.

Visualización de las propiedades del dispositivo SDX

Puede ver las propiedades del sistema, como el número 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 acerca de los recursos del sistema, el hipervisor, la licencia y el sistema:

- **Recursos del sistema**

  Total de núcleos de CPU

  Número de núcleos de CPU en el dispositivo SDX.

- **Total de chips SSL**

  Número total de chips SSL en el dispositivo SDX.

- **Fichas SSL gratuitas**

  Número total de chips SSL que no se han asignado a una instancia.

- **Memoria total (GB)**

  Memoria total del dispositivo en gigabytes.

- **Memoria libre (GB)**

  Memoria libre del dispositivo en gigabytes.

- **Información del hipervisor**

  Tiempo de actividad

  Tiempo transcurrido desde la última vez que se reinició el dispositivo, en número de días, horas y minutos.

- **Edición**

  Edición de XenServer instalada en el dispositivo SDX.

- **Versión**

  Versión de XenServer instalada en el dispositivo SDX.

- **IQN de iSCSI**

  Nombre cualificado de iSCSI.

- **Código de producto**

  Código de producto de XenServer.

- **Número de serie**

  Número de serie de XenServer.

- **Fecha de compilación**

  Fecha de compilación de XenServer.

- **Número de compilación**

  Número de compilación de XenServer.

- **Paquete complementario**

  Versión del paquete complementario instalado en el dispositivo SDX.

- **Información de licencia**

  Plataforma

  Número de modelo de la plataforma de hardware, basado en la licencia instalada.

- **Máximo de instancias**

  Número máximo de instancias que puede configurar en el dispositivo SDX, según la licencia instalada.

- **Instancias disponibles (compartidas)**

  Número de instancias que se pueden configurar en función del número de núcleos de CPU que todavía están disponibles.

- **Rendimiento máximo (Mbps)**

  Rendimiento máximo que se puede lograr en el dispositivo, en función de la licencia instalada.

- **Rendimiento disponible (Mbps)**

  Rendimiento disponible basado en la licencia instalada.

- **Información del sistema**

  Plataforma

  Número de modelo de la plataforma de hardware.

- **Producto**

  Tipo de producto Citrix ADC.

- **Creaciones**

  Citrix ADC lanzan y compilan ejecutándose en el dispositivo SDX.

- **Dirección IP**

  Dirección IP de Management Service.

- **ID de host**

  ID de host XenServer.

- **ID del sistema**

  ID del sistema XenServer.

- **Número de serie**

  Número de serie de XenServer.

- **Hora del sistema**

  La hora del sistema se muestra en el formato Día Mes Fecha Horas:Minutos:Segundos Zona horaria Año.

- **Tiempo de actividad**

  Tiempo desde la última vez que se reinició Management Service, en número de días, horas y minutos.

- **Versión del BIOS**

  Versión del BIOS.

Visualización del rendimiento del dispositivo en tiempo real

El rendimiento total del dispositivo SDX para el tráfico entrante y saliente se traza 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)**.

Visualización del uso de CPU y memoria en tiempo real

Puede ver un gráfico del uso de CPU y 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 de Management Service**.

Visualización del 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 CPU muestra los siguientes detalles:

- Número de núcleo

  El número de núcleo de la CPU del dispositivo.

- CPU física

  El número físico de CPU de ese núcleo.

- Hiperprocesos

  Los hiperprocesos asociados a ese núcleo de CPU.

- Instancias

  Las instancias que están utilizando ese núcleo de CPU.

- Uso medio del núcleo

  El uso medio 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 (%)**.

Instalación de 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 finaliza todas las sesiones de cliente actuales con Management Service, por lo que debe volver a iniciar sesión en Management Service para realizar 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.

Visualización del certificado SSL en Management Service

Management Service utiliza un certificado SSL para conexiones de cliente seguras. Puede ver los detalles de este certificado, como el estado de validez, el emisor, el asunto, los días de caducidad, las fechas válidas de 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 SSL y claves para instancias Citrix ADC

Las vistas separadas de los certificados SSL y las claves para las instancias de Citrix ADC ofrecen una mayor facilidad de uso. Puede utilizar un nuevo nodo de Management Service, Archivos de certificado SSL, para cargar y administrar los certificados SSL y los pares de claves públicas y privadas correspondientes que se pueden instalar en instancias de Citrix ADC.

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

Modificación de la configuración del sistema

Por razones de seguridad, puede especificar que Management Service y una instancia de VPX deben comunicarse entre sí solo a través de un canal seguro. También puede restringir el acceso a la interfaz de usuario de Management Service. Los clientes pueden iniciar sesión en la interfaz de usuario de Management Service 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**.

Reiniciar 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 XenServer. Cuando XenServer 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**.

Apagar el dispositivo

Puede apagar el dispositivo SDX desde Management Service.

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

Crear dominios administrativos de SDX

June 19, 2019

La función de dominios administrativos SDX le ayuda a crear varios dominios administrativos. Puede utilizar los dominios administrativos para segregar 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 envía con recursos fijos, como núcleos de CPU, rendimiento de datos, memoria, espacio en disco, chips SSL y un número específico de instancias que se pueden aprovisionar. El número 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.

Los dominios administrativos que cree son subdominios del dominio propietario. En cada caso, los recursos del subdominio se asignan desde el grupo de recursos del dominio primario. 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 específicamente a su dominio. Sin embargo, los usuarios de un dominio primario pueden tener acceso a los recursos de los subdominios de ese dominio.

Ejemplos de asignación de recursos a subdominios

La Tabla 1 muestra los recursos de un dominio raíz denominado
nsroot (que es el nombre predeterminado del dominio raíz). El administrador de SDX puede asignar estos recursos a subdominios. En este caso, el administrador puede asignar un máximo de, por ejemplo, 10 núcleos de CPU y 840 GB de espacio en disco.

Cuadro 1. Recursos de Propietario
——————–	—–
Núcleo de CPU	10
Rendimiento (Mbps)	18500
Memoria (MB)	87300
Espacio en disco (GB)	840
Fichas SSL	36
Instancias	36

La tabla 2 muestra los recursos asignados a un subdominio denominado
Test. Este subdominio se ha asignado 5 de los 10 núcleos de CPU de su dominio principal, dejando 5 núcleos que se pueden asignar a otros subdominios de Propietario.

Cuadro 2. Probar los recursos del dominio

Núcleo de 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 figura 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 creado un nuevo dominio, inicie sesión en el dominio recién creado mediante la página de inicio de sesión de Management Service y proporcione el nombre de dominio y el nombre de usuario en el campo Nombre de usuario. Por ejemplo, si creó un dominio denominado NewDomain con un usuario NewUser, inicie sesión como NewDomainNewUser.

Asignación de usuarios a dominios

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

Administrar la asignación de discos RAID en dispositivos SDX de la serie 22XXX

June 19, 2019

Los dispositivos Citrix ADC SDX 22040/22060/22080/22100/22120 incluyen ahora una controladora de arreglo redundante de discos independientes (RAID), que puede admitir hasta ocho discos físicos. Var-

ios discos proporcionan no solo mejoras en el rendimiento, sino también confiabilidad mejorada. La confiabilidad es especialmente importante para un dispositivo SDX, ya que el dispositivo aloja un gran número de máquinas virtuales y una falla 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 réplica proporciona inmediatamente todos los datos necesarios.

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

El dispositivo SDX se incluye con una configuración que incluye la unidad lógica 0, que se asigna para Management Service y XenServer, y la unidad lógica 1, que se asigna a instancias de Citrix ADC que se aprovisionarán. Para usar unidades físicas adicionales, debe crear nuevas unidades lógicas.

Visualización de las propiedades y operaciones de la unidad

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

En Management Service, 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, estado, tamaño, de cada unidad lógica e información acerca de sus unidades físicas componentes. En la tabla siguiente se describen los estados de la unidad virtual.

Estado	Descripción
Óptimo	La condición de funcionamiento de la unidad virtual es buena. 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 sin conexión.
Falló	Error en la unidad virtual.

Estado	Descripción
Offline	La unidad virtual no está disponible para el controlador 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 a 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 en marcha y está siendo controlada por RAID.
  - Sin configurar (buena): La unidad física está en buen estado y se puede agregar como parte del par de unidades lógicas.
  - < No configurado (incorrecto): La unidad física no está en buen estado y no se puede agregar como parte de una unidad lógica.
- Estado externo: 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 necesita agregarse como parte del par de unidades lógicas.
- Reconstruir: 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 que se

almacenaron en la unidad antes de que fallara. El controlador RAID vuelve a crear los datos almacenados en las otras unidades del grupo de unidades.
- Localizar: Localice la unidad en el dispositivo, que se indica haciendo que el LED de actividad de unidad asociado a la unidad parpadee.
- Detener localización (Stop Localize): Permite detener la ubicación de la unidad en el dispositivo.
- Prepare to Remove (Prepare to Remove): 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 acerca de una unidad de repositorio de almacenamiento que no está conectada y puede quitar dicha unidad seleccionándola y, a continuación, haciendo clic en **Quitar**. La ficha Repositorio de almacenamiento muestra la siguiente información sobre cada repositorio de almacenamiento:

- Nombre: Nombre de la unidad del repositorio de almacenamiento.
- Está conectado a la unidad: Si el repositorio de almacenamiento está conectado o no. Si la unidad no está conectada, puede hacer clic en **Quitar** para eliminar.
- Tamaño: Tamaño del repositorio de almacenamiento.
- Utilizado: Cantidad de espacio de almacenamiento de información en uso.

Adición de una unidad lógica adicional al dispositivo SDX 22000

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

1. Inicie sesión en Management Service.
2. Vaya a **Configuración > Sistema > RAID**.
3. En la parte posterior del dispositivo SDX 22000, inserte los dos SSD vacíos en los números de ranura 4 y 5. Puede agregar los SSD en un sistema en ejecución.
   Nota: Asegúrese de que los SSD estén certificados por Citrix.
4. En Management Service, vaya a **Configuración > Sistema > RAID** y a la ficha **Unidades físicas**. Vería los 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 en el 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.

Adición de una segunda unidad lógica adicional en el dispositivo SDX 22000

Para agregar otra unidad lógica, inserte las SSD en los números de ranura 6 y 7. En la página **Crear disco lógico** , seleccione 6 en la lista desplegable **Primera ranura** y seleccione 7 en la lista desplegable **Segunda ranura** .

Sustitución de una unidad SSD defectuosa por una unidad SSD vacía

Para reemplazar una unidad SSD defectuosa por una unidad SSD vacía:

1. Vaya a **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 desde la que eliminó 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 las licencias de SDX

June 19, 2019

En Citrix ADC SDX Management Service, puede utilizar su número de serie de hardware (HSN) o su código de acceso a licencias (LAC) para asignar sus licencias. El software Management Service recupera internamente el número de serie del dispositivo y Citrix envía la LAC por correo electrónico cuando compra una licencia.

Como alternativa, si ya existe una licencia en el equipo local, puede cargarla en el dispositivo.

Para todas las demás funciones, como devolver o reasignar su licencia, debe utilizar el portal de licencias. Opcionalmente, puede seguir utilizando el portal de licencias para la asignación de licencias. Para obtener más información, consulte los siguientes recursos:

- Artículo CTX131110.
- Usar Manage Licenses en My Account (Iniciar sesión) en citrix.com

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

- Elegir la plataforma y las opciones de modificación adecuadas.
- Modelos de licencias

Requisitos previos

Para utilizar el número de serie del hardware o el código de activación de la licencia para asignar sus licencias:

1. Debe poder acceder a dominios públicos a través del dispositivo. Por ejemplo, el dispositivo debería 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 de Management Service y configurar un servidor DNS.
2. Su licencia debe estar vinculada a su hardware o debe tener un código de acceso de licencia válido (LAC).

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 de licencia (LAC).

Puede asignar parcialmente licencias 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 de Management Service del dispositivo SDX (por ejemplo, http://10.102.126.251).
2. En **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador (credenciales predeterminadas; **Nombre de usuario**: Nsroot y **Contraseña**: Nsroot).
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, seleccione una de las opciones:

- Cargar archivos de licencia desde un equipo local (esta opción está seleccionada de forma predeterminada)
- Usar código de acceso de licencia
- Usar número de serie de hardware
- **Usar código de acceso de licencia**: Si selecciona esta opción, proporcione el código **LAC** en el campo **Código de acceso de licencia** o active la casilla de verificación para conectarse a través del servidor proxy. A continuación, haga clic en **Obtener licencias**.
  - Seleccione el archivo de licencia que quiere utilizar para asignar sus 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**.

Visualizador de recursos SDX

June 19, 2019

Cuando se aprovisiona una instancia de Citrix ADC en un dispositivo Citrix ADC SDX, se deben asignar a una instancia varios recursos, como CPU, rendimiento y memoria. Con SDX actual, no se muestra la información sobre varios recursos disponibles.

Con el visualizador de recursos, todos los recursos disponibles que se pueden utilizar para aprovisionar una instancia se muestran en un único panel. Todos los recursos disponibles y usados se muestran en formato gráfico. Visualizador de recursos también muestra otros parámetros como el estado de la fuente de alimentación, temperatura, etc. aparte 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 usados en un formato gráfico.

La siguiente ilustración muestra los detalles capturados en el visualizador de recursos:

Administrar interfaces

June 19, 2019

En el panel Interfaces de Management Service, además de configurar la configuración de transmisión para cada interfaz, puede mostrar la asignación de las interfaces virtuales en 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 o recibir tráfico.

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 quiera configurar y, a continuación, haga clic en Modificar.
3. En la ventana Configurar interfaz, especifique valores para los siguientes parámetros:
    - Negociación automática *: Permite la negociación automática. Valores posibles: ON, OFF. Valor predeterminado: OFF.
    - Velocidad *: Velocidad Ethernet para la interfaz, en MB/s. Valores posibles: 10, 100, 1000 y 10000.
    - Duplex *: Tipo de operación dúplex de la interfaz. Valores posibles: Full, Half, NONE. Valor predeterminado: NONE.
    - Negociación automática de control de flujo *: Negocia automáticamente los parámetros de control de flujo. Valores posibles: ON, OFF. Predeterminado: ON
    - Control de flujo Rx *: Habilite el flujo Rx. Valores posibles: ON, OFF. Predeterminado: ON
    - Control de flujo Tx *: El control de flujo EnableTx está habilitado. Valores posibles: ON, OFF. Predeterminado: ON

    * Un parámetro requerido
4. Haga clic en Aceptar y, a continuación, haga clic 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 quiera restablecer y, a continuación, haga clic en Restablecer.

Visualización de la asignación de interfaces virtuales en la instancia VPX a las interfaces físicas en el dispositivo SDX

Si inicia sesión en la instancia de Citrix ADC VPX, la utilidad de configuración y la interfaz de línea de comandos muestran la asignación de las interfaces virtuales de la instancia a las interfaces físicas del dispositivo.

Después de iniciar sesión en la instancia de VPX, en la utilidad de configuración, vaya a **Red**y, 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 figura:

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

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

Asignación de una dirección MAC a una interfaz

Si, mientras está aprovisionando una instancia de Citrix ADC en un dispositivo SDX, XenServer 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 del mismo dispositivo o de otro dispositivo. Para evitar la asignación de direcciones MAC duplicadas, puede imponer direcciones MAC únicas.

Hay dos formas 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 para una interfaz 1G se establece en 8 y el rango para 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

Cuadro 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. Management Service genera direcciones MAC, sobre la base de la dirección MAC base, solo para puertos 1/x y 10/x.

Nota: No se 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, a continuación, 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, por motivos de seguridad, puede inhabilitar la interfaz física mediante Management Service.

Nota: De forma predeterminada, todas las interfaces físicas del dispositivo SDX están habilitadas. Además, si una interfaz es utilizada por un VPX o un canal, no se 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

June 19, 2019

Los dispositivos Citrix ADC SDX admiten la recepción y 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 Citrix ADC SDX puede usar tramas 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 Citrix ADC aprovisionadas en el dispositivo SDX admiten tramas gigantes en una configuración de equilibrio de carga para los siguientes protocolos:

- TCP
- Cualquier otro protocolo sobre TCP
- SIP

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

Caso de uso: Configuración gigante a gigante

Considere un ejemplo de una configuración gigante a gigante en la que el servidor virtual de equilibrio de carga SIP LBVS-1, configurado en la instancia NS1 de Citrix ADC, 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	198.51.100.20
MTU especificadas para las interfaces (mediante la interfaz de Management Service) y las VLAN en NS1 (mediante la CLI).	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
Servicios en NS1 que representan servidores	SVC-S1	Dirección IP: 198.51.100.19; Protocolo: SIP; Puerto: 5060
Servicios en NS1 que representan servidores	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 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 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 IP es igual o menor que la MTU (9000) de la interfaz 10/2, desde la cual 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 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 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 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 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 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 necesaria y haga clic en Modificar. Establezca el valor MTU y haga clic en Aceptar.

Ejemplo:

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

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

En la tabla siguiente se enumeran las tareas, los comandos de NetScaler y los ejemplos para crear la configuración necesaria en las instancias de Citrix ADC.

Tareas	Sintaxis de comandos de NetScaler	Ejemplos
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 9000; 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 SIP.	add service <serviceName> <ip> SIP_UDP <port> ; show service <name>	add service SVC-S1 198.51.100.19 SIP_UDP 5060; dd service SVC-S2 198.51.100.20 SIP_UDP 5060

Tareas	Sintaxis de comandos de NetScaler	Ejemplos
Cree servidores virtuales de equilibrio de carga SIP y enlace los servicios con él.	add lb vserver <name> SIP_UDP <ip> <port>; bind lb vserver <vserverName> <serviceName>; show lb vserver <name>	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
bind lb vserver LBVS-1 SVC-S2	save ns config; show ns config	

Caso de uso: Configuración de no gigante a gigante

Considere un ejemplo de una configuración no gigante a gigante en la que el servidor virtual de equilibrio de carga LBVS1, configurado en una instancia de Citrix ADC NS1, se utiliza para equilibrar el tráfico de carga 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 en 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 en NS1 se establece en un perfil TCP, que luego se enlaza al servicio (SVC-S1) que representa S1 en NS1.

En la tabla siguiente se enumeran los parámetros utilizados 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

Entidad	Nombre	Detalles
	S2	198.51.100.20
MTU para la interfaz 10/1 (mediante la interfaz de Management Service).		1500
MTU configurado para la interfaz 10/2 (mediante la interfaz de Management Service).		9000
MTU para VLAN 10 en NS1 (mediante la interfaz de línea de comandos NetScaler).		1500
MTU configurado para VLAN 20 en NS1 (mediante la interfaz de línea de comandos NetScaler).		9000
Servicios en NS1 que representan servidores	SVC-S1	Dirección IP: 198.51.100.19; Protocolo: HTTP; Puerto: 80; MSS: 8960
	SVC-S2	Dirección IP: 198.51.100.20; Protocolo: HTTP; Puerto: 80; MSS: 8960
Servidor virtual de equilibrio de carga en VLAN 10	LBVS-1	Dirección IP: 203.0.113.15; Protocolo: HTTP; Puerto: 80; Servicios enlazados: 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. Cliente CL1 crea una solicitud HTTP de 200 bytes para enviar al servidor virtual LBVS-1 de NS1.
2. CL1 abre una conexión a LBVS-1 de NS1. CL1 y NS1 intercambian sus respectivos valores TCP MSS mientras establece 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.


```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">

Tamaño del paquete de solicitud = [encabezado IP + encabezado TCP
    + solicitud TCP] = [20 + 20 + 200] = 240

</div>
```

4. NS1 recibe el paquete de solicitud en la interfaz 10/1 y luego 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 respectivos valores TCP MSS mientras establece la conexión.
6. Dado que MSS de S1 es mayor que la solicitud HTTP, NS1 envía los datos de solicitud en un único paquete IP a S1.
    a) Tamaño del paquete de solicitud = [encabezado IP + encabezado TCP + [solicitud TCP] = [20 + 20 + 200] = 240

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 = [IP Header + TCP Header + (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 necesaria y haga clic en Modificar. Establezca el valor MTU y haga clic en Aceptar.

Ejemplo:

Establezca los siguientes valores MTU:

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

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

En la tabla siguiente se enumeran las tareas, los comandos de NetScaler y los ejemplos para crear la configuración necesaria en las instancias de Citrix ADC.

Tareas	Sintaxis de la línea de comandos de NetScaler	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
Save the configuration	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 Citrix ADC. LBVS1 se utiliza para equilibrar la carga del tráfico HTTP entre los servidores S1 y S2, y global se utiliza para equilibrar el tráfico de carga entre los servidores S3 y S4.

CL1 está en VLAN 10, S1 y S2 en VLAN20, CL2 en VLAN 30 y S3 y S4 en 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 clientes. La interfaz 10/2 de NS1 recibe o envía tráfico desde o hacia los servidores.

La interfaz 10/1 está vinculada a VLAN 10 y VLAN 20 como interfaz etiquetada, y la interfaz 10/2 está vinculada a VLAN 30 y VLAN 40 como 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, y 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 NetScaler para paquetes etiquetados VLAN es de la MTU de la interfaz o la MTU de la VLAN, lo que sea menor. Por ejemplo:

- La MTU de la interfaz 10/1 es 9216. La MTU de 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 VLAN 20 es 9000. En la interfaz 10/2, la MTU de VLAN 20 paquetes etiquetados es 9000.
- La MTU de la interfaz 10/1 es 9216. La MTU de 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 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 en 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 en NS1 se establece en un perfil TCP, que luego se enlaza al servicio (SVC-S1) que representa S1 en NS1.

En la tabla siguiente se enumeran los parámetros utilizados 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
|Perfil TCP predeterminado|nstcp_default_profile|MSS: 1460
|Perfil TCP personalizado|ALL-JUMBO|MSS: 8960
|Servicios en NS1 que representan servidores|SVC-S1|Dirección IP: 198.51.100.19; Protocolo: HTTP; Puerto: 80; Perfil TCP: ALL-JUMBO (MSS: 8960)
||SVC-S2|Dirección IP: 198.51.100.20; Protocolo: HTTP; Puerto: 80; Perfil TCP: ALL-JUMBO (MSS: 8960)
||SVC-S3|Dirección IP: 198.51.101.19; Protocolo: HTTP; Puerto: 80; Perfil TCP: Nstcp_default_profile (MSS:1460)
||SVC-S4|Dirección IP: 198.51.101.20; Protocolo: HTTP; Puerto: 80; Perfil TCP: Nstcp_default_profile (MSS:1460)
|Servidores virtuales de equilibrio de carga en NS1|LBVS-1|Dirección IP = 203.0.113.15; Protocolo: HTTP; Puerto: 80; Servicios enlazados: SVC-S1, SVC-S2; Perfil TCP: ALL-JUMBO (MSS: 8960)
||LBVS-2|Dirección IP = 203.0.114.15; Protocolo: HTTP; Puerto: 80; Servicios enlazados: SVC-S3, SVC-S4; Perfil TCP: 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 a LBVS-1 de NS1. CL1 y NS1 intercambian sus valores TCP MSS mientras establece 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 = [IP Header + TCP Header + (segmento TCP = NS1 MSS)] = [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 (9000) efectiva 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 respectivos valores TCP MSS mientras establece la conexión.
7. NS1 segmenta los datos de solicitud en múltiplos de MSS de S1 y envía estos segmentos en paquetes IP etiquetados como VLAN 20 a S1.
    - Tamaño de los dos primeros paquetes = [IP Header + TCP Header + (TCP payload = 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 MTU efectivo (9000) de la interfaz 10/2 para paquetes etiquetados 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 necesaria y haga clic en Modificar. Establezca el valor MTU y haga clic en Aceptar.

Ejemplo:

Establezca los siguientes valores MTU:

- Para interfaz 10/1 como 9216

- Para interfaz 10/2 como 9216

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

En la tabla siguiente se enumeran las tareas, los comandos de NetScaler y los ejemplos para crear la configuración necesaria en las instancias de Citrix ADC.

Tarea	Sintaxis	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 9000; add vlan 20 -mtu 9000; add vlan 30 -mtu 1500; add vlan 40 -mtu 1500
Enlace interfaces con VLAN.	bind vlan <id> -ifnum <interface_name>; show vlan <id>	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
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
Save the configuration	save ns config; show ns config

Configurar SNMP en dispositivos SDX

June 19, 2019

Puede configurar un agente SNMP (Simple Network Management Protocol) en el dispositivo Citrix ADC SDX para generar eventos asincrónicos, que se denominan capturas. 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 el estado anómalo del dispositivo SDX.

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

La siguiente figura ilustra una red con un dispositivo SDX que tiene SNMP habilitado y configurado. En la figura, 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 MIB SDX. 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 captura SNMP.
2. En el panel Destinos de captura SNMP, haga clic en Agregar.
3. En la página Configurar Destino de Captura SNMP, especifique 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 captura, o bien el oyente deja caer 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 (), at (@), igual a (=), dos puntos (:) y guión bajo (_).
      Nota: Debe especificar la misma cadena de comunidad en el dispositivo de escucha de capturas, o el listener deja caer los mensajes. Predeterminado: Public.
4. Haga clic en Agregar y, a continuación, haga clic en Cerrar. El destino de captura SNMP que agregó aparece en el panel Trampas 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 quitar el destino de captura SNMP.

Descargar archivos MIB

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

SDX-MIB-smiv2.mib. Este archivo es utilizado por los administradores SNMPv2 y los detectores de capturas SNMPv2.

El archivo incluye una MIB empresarial Citrix ADC 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 SNMP Manager

Debe configurar el dispositivo SDX para permitir que los administradores SNMP adecuados lo consulten. También debe proporcionar al administrador SNMP la información específica del dispositivo necesaria. 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 a su dirección IP.

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

Para configurar un administrador 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 SNMP Manager, defina los siguientes parámetros:
    - SNMP Manager: Dirección IPv4 del administrador SNMP. Alternativamente, en lugar de una dirección IPv4, puede especificar un nombre de host asignado a un administrador SNMP.

Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP a 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 (.) libra (#), at (@), igual a (=), dos puntos (:) y guión bajo (_).
- Active la casilla de verificación **Habilitar red de administración** para especificar los administradores 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, haga clic en Cerrar.

Configuración del dispositivo SDX para consultas SNMPv3

El protocolo simple de administración de redes versión 3 (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 datos, verificación de la puntualidad de los mensajes y confidencialidad de los datos.

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

- Vistas SNMP
- Usuarios 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 SNMP

Debe configurar el dispositivo CloudBridge para permitir que los administradores SNMP apropiados lo consulten. También debe proporcionar al administrador SNMP la información específica del dispositivo necesaria. 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 a su dirección IP.

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

Para configurar un administrador SNMP:

1. Acceda 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 SNMP Manager, establezca los siguientes parámetros:
    - **SNMP Manager**: Dirección IPv4 del administrador SNMP. Alternativamente, en lugar de una dirección IPv4, puede especificar un nombre de host asignado a un administrador SNMP. Si lo hace, debe agregar un servidor de nombres DNS que resuelva el nombre de host del administrador SNMP a 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 (.) libra (#), at (@), igual a (=), dos puntos (:) y guión bajo (_).
6. Haga clic en Agregar y, a continuación, haga clic 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 (.) libra (#), at (@), igual a (=), dos puntos (:) y guión bajo (_). Debe elegir un nombre que ayude a identificar la vista SNMPv3.
    - Subárbol: Una rama particular (subárbol) del árbol MIB, que quiere asociar a esta vista SNMPv3. Debe especificar el árbol secundario como un OID 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 SNMP tienen acceso a las MIB necesarias para consultar a los administradores 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, establezca 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 (.) libra (#), at (@), igual a (=), dos puntos (:) y guión bajo (_).
    - Nivel de seguridad: Nivel de seguridad necesario para la comunicación entre el dispositivo y los usuarios SNMPv3. Seleccione una de las siguientes 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. Debe especificar el mismo algoritmo de autenticación cuando configure el usuario SNMPv3 en el administrador 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 (.) libra (#), espacio (), at (@), igual a (=), dos puntos (:) y guión bajo (_).
    - Protocolo de privacidad: Algoritmo de cifrado utilizado por el dispositivo y el usuario SNMPv3 para cifrar la comunicación entre ellos. Debe especificar el mismo algoritmo de cifrado cuando configure el usuario SNMPv3 en el administrador SNMP.
    - Nombre de vista: Nombre de la vista SNMPv3 configurada que quiere enlazar a este usuario SNMPv3. Un usuario SNMPv3 puede acceder a los subárboles enlazados a esta vista SNMPv3 como tipo INCLUIDO, pero no puede acceder a los que son de tipo EXCLUIDO.

Configuración de una alarma SNMP

El dispositivo proporciona un conjunto predefinido de entidades de condición denominado 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 captura configurados. Por ejemplo, cuando la alarma DeviceAdded está activada, se genera un mensaje de captura y se envía al detector de cap-

turas siempre que se aprovisione un dispositivo (instancia) en el dispositivo. Puede asignar un nivel de gravedad a una alarma SNMP. Al hacerlo, los mensajes de captura correspondientes se asignan ese nivel de gravedad.

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

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

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

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

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

Configurar notificaciones de Syslog

June 19, 2019

SYSLOG es un protocolo de registro estándar. Tiene dos componentes: El módulo de auditoría SYSLOG, que se ejecuta en el dispositivo Citrix ADC SDX, y el servidor SYSLOG, que puede ejecutarse en un sistema remoto. SYSLOG utiliza el protocolo de datos de usuario (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. Estos mensajes suelen contener 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)
- Información del mensaje

Puede utilizar esta información para analizar el origen de la alerta y tomar medidas correctivas si es necesario. Primero configure un servidor syslog al que el dispositivo envía información de registro y, a continuación, especifique los datos y el formato de hora para grabar los mensajes de registro.

Para 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 de Syslog, especifique 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, haga clic en Cerrar.

Para 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 el cuadro Configurar parámetros de Syslog, especifique el formato de fecha y hora.
4. Haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Configurar notificaciones de correo

June 19, 2019

Debe configurar un servidor SMTP para recibir un mensaje de correo electrónico cada vez que se genera una alerta. Primero configure un servidor SMTP y, a continuación, configure un perfil de correo. En el perfil de correo, utilice comas para separar las direcciones de los destinatarios.

Para configurar un servidor SMTP

1. Vaya a Sistema > Notificaciones > Correo > Correo electrónico.
2. En el panel de detalles, haga clic en Servidor de correo electrónico y, a continuación, haga clic en Agregar.
3. En la página Crear Servidor de Correo Electrónico, especifique valores para los parámetros del servidor. Para obtener una descripción de un parámetro, coloque el cursor sobre el campo correspondiente.

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

Para configurar un perfil de correo

1. Vaya a Sistema > Notificaciones > Correo > Correo electrónico.
2. En el panel de detalles, haga clic en Lista de distribución de correo electrónico y, a continuación, haga clic en Agregar.
3. En la página Crear lista de distribución de correo electrónico, especifique valores para 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, haga clic en Cerrar.

Configurar notificaciones de SMS

June 19, 2019

Debe configurar un servidor de servicio de mensajes cortos (SMS) para recibir un mensaje SMS cada vez que se genera una alerta. Primero configure un servidor SMS y, a continuación, configure un perfil SMS. En el perfil de SMS, utilice comas para separar las direcciones de los destinatarios.

Para configurar un servidor SMS

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

Para 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, haga clic en Agregar.
3. En la página Crear lista de distribución de SMS, especifique valores para 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, haga clic en Cerrar.

Supervisión y administración del estado en tiempo real de las entidades configuradas en un dispositivo SDX

June 19, 2019

El dispositivo Citrix ADC SDX puede supervisar y administrar los estados de servidores virtuales, servicios, grupos de servicios y servidores en todos 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. Esto le da visibilidad del estado en tiempo real de las entidades y facilita la administración de estas entidades cuando tiene un gran número de entidades configuradas en las instancias de Citrix ADC.

Visualización del 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 nombre, dirección IP y 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 Citrix ADC > 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, basado en el estado de los servidores virtuales de seguridad. Por ejemplo, arriba, abajo o fuera de servicio.
     - Estado: Estado actual del servidor virtual. Por ejemplo, arriba, abajo o fuera de 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: (Número de servicios consolidados * 100) / Total de servicios vinculados
     - 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 de 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, la duración del tiempo durante el que 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.

- 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. Esto le permite comprobar el estado de los servicios que pueden hacer que el porcentaje de mantenimiento de un servidor virtual sea bajo, de modo que pueda tomar las medidas adecuadas.

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

  1. En la ficha Configuración, en el panel izquierdo, haga clic en Citrix ADC > 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. Como alternativa, haga clic con el botón secundario en el nombre del servidor virtual y, a continuación, haga clic en Servicios enlazados o Grupos de servicios enlazados.

Visualización del estado de los servicios

Puede supervisar los valores en tiempo real del estado de un servicio y la duración durante la que 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 Citrix ADC > Entidades > Servicio.
2. En el panel de detalles, en Servicios, vea las siguientes estadísticas:
   - Nombre del dispositivo: Nombre del dispositivo en el que está configurado 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, arriba, abajo o fuera de 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 que el servicio ha estado en el estado actual.

- Visualización de los servidores virtuales a los que está enlazado un servicio

  Puede ver los servidores virtuales a los que está enlazado 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 Citrix ADC > 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 en Servidores virtuales enlazados.

Visualización del estado de los grupos de servicios

Puede supervisar el estado en tiempo real de un miembro del 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 Citrix ADC > 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, UP, DOWN o OUT SERVICE
   - Estado: Estado efectivo del grupo de servicios, que se basa en el estado del miembro del grupo de servicios. Por ejemplo, arriba, abajo o fuera de 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 servicios, es decir, la duración del tiempo durante el que el miembro del grupo de servicios 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.

- Visualización de los servidores virtuales a los que está enlazado un servicio

  Puede ver los servidores virtuales a los que está enlazado 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 Citrix ADC > 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. Alternativamente, haga clic con el botón derecho en el servicio y haga clic en Servidores virtuales enlazados.

Visualización del estado de los servidores

Puede supervisar y administrar los estados de los servidores en las instancias de Citrix ADC. Esto le da visibilidad del estado en tiempo real de los servidores y facilita la administración de estos servidores cuando dispone de un gran número de servidores.

Para ver el estado de los servidores

1. En la ficha Configuración, en el panel de navegación, haga clic en Citrix ADC > 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, arriba, abajo y fuera de 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 que el servidor se encuentra en el estado actual.

Configuración del 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 predeterminada, el dispositivo sondea los valores cada 30 minutos.

- Para configurar el intervalo de sondeo para servidores virtuales, servicios, grupos de servicios y servidores.

  1. En la ficha Configuración, haga clic en Citrix ADC > 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.

Supervisar y administrar eventos generados en instancias de Citrix ADC

June 19, 2019

Utilice la función Eventos para supervisar y administrar los eventos generados en las instancias de Citrix ADC. Management Service identifica los eventos en tiempo real, lo que le ayuda a solucionar los problemas de inmediato y a mantener las instancias de Citrix ADC funcionando de manera eficaz. También puede configurar reglas de eventos para filtrar los eventos generados y recibir notificaciones para realizar acciones en la lista filtrada de eventos.

Ver todos los eventos

Puede ver todos los eventos generados en las instancias Citrix ADC aprovisionadas en el dispositivo Citrix ADC SDX. Puede ver los detalles como gravedad, categoría, fecha, origen y mensaje para cada uno de los eventos.

Para ver los eventos, vaya a Configuración > Citrix ADC > Eventos > Todos los eventos

Puede ver el historial del evento y los detalles de la entidad seleccionando el evento y haciendo 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.

- Visualización de informes

  La página Informes muestra el resumen de 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 > Citrix ADC > Eventos > Informes. A continuación se presentan los informes gráficos compatibles con Management Service

  - **Acontecimientos**

    El informe Eventos es un gráfico circular que representa el número de eventos segmentados y codificados por colores en función de su gravedad.

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

    * Fuente: 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 instancias principales de Citrix ADC por todos los eventos**

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

- **Las 10 instancias principales de Citrix ADC por eventos de cambio de estado de entidad**

  Este informe es un gráfico de barras que muestra las 10 instancias principales de Citrix ADC según el número de cambios de estado de entidad para la escala de tiempo seleccionada. Los cambios de estado de entidad reflejan eventos de entidad hacia arriba, entidad hacia abajo o fuera de servicio.

- **Las 10 instancias principales de Citrix ADC por eventos de infracción de umbral**

  Este informe es un gráfico de barras que muestra las 10 instancias principales de Citrix ADC según el número de eventos de infracción de umbral para 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

- **10 instancias principales de Citrix ADC por eventos de falla de hardware**
  Este informe es un gráfico de barras que muestra las 10 instancias de Citrix ADC principales según el número de eventos de falla de hardware para la escala de tiempo seleccionada. Los eventos de error de hardware reflejan los siguientes eventos:
  * hardDiskDriveErrors
  * compactFlashErrors
  * powerSupplyFailed
  * “sslCardFailed”

- **Las 10 instancias principales de Citrix ADC por eventos de cambio de configuración**

  Este informe es un gráfico de barras que refleja las 10 instancias principales de Citrix ADC según el número de eventos de cambio de configuración para la escala de tiempo seleccionada. Puede hacer clic en el gráfico para profundizar y ver los cambios de configuración

basados en el usuario para una instancia concreta. Puede ver los detalles de autorización y estado de ejecución haciendo clic en este gráfico.

- <**10 instancias principales de Citrix ADC por eventos de error de autenticación**

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

- 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 los criterios de filtro de la regla, se ejecuta 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 de envío de correo electrónico: Envía un correo electrónico para los eventos que coinciden con los criterios de filtro.
  - Enviar acción de SMS: Envía un servicio de mensajes cortos (SMS) para los eventos que coinciden con los criterios de filtro.

  Para agregar reglas de evento

  1. Vaya a Configuración > Citrix ADC > Eventos > Reglas de eventos y haga clic en Agregar.
  2. En la página Regla, establezca 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 Citrix ADC para las que quiere definir una regla de evento.
     - Categoría: Categoría o categorías de los eventos generados por las instancias de Citrix ADC.
     - Objetos de error: Instancias o contadores de entidad para los que se ha generado un evento.

     Nota: Esta lista puede contener nombres de contador para todos los eventos relacionados con el umbral, nombres de entidad para todos los eventos relacionados con la entidad y nombres de certificado para eventos relacionados con el certificado.
  3. Haga clic en Guardar.
  4. En Acciones de regla, 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. Un SMS se activa 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 Citrix ADC en el dispositivo SDX. Puede definir los siguientes tipos de niveles de gravedad: Crítico, Principal, Menor, Advertencia, Borrar e Información. También puede suprimir los eventos durante un tiempo específico.
  Para configurar la gravedad:

  1. Vaya a Configuración > Citrix ADC > Eventos > Configuración del evento, seleccione el evento en 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. También puede suprimir los eventos activando la casilla de verificación Suprimir. También puede especificar las instancias de Citrix ADC para las que quiere suprimir este evento mediante la opción Avanzadas.
  4. Haga clic en Aceptar.

Call Home Support para instancias de Citrix ADC en un dispositivo SDX

June 19, 2019

La función Call Home supervisa las instancias de Citrix ADC en busca de condiciones de error comunes. Ahora puede configurar, habilitar o inhabilitar la función Call Home en instancias de Citrix ADC desde la interfaz de usuario de Management Service.

Nota: La instancia de Citrix ADC debe registrarse en el servidor de asistencia técnica de Citrix antes de que Call Home pueda cargar los datos del sistema en el servidor cuando se produzcan condiciones de error predefinidas en el dispositivo. La activación de la función Call Home en la instancia de Citrix ADC inicia el proceso de registro.

- Habilitar e inhabilitar Call Home en una instancia de Citrix ADC

  Puede habilitar la función Call Home en la instancia de Citrix ADC desde Management Service. Cuando habilita la función Call Home, el proceso Call Home registra la instancia de Citrix ADC

con el servidor de asistencia técnica de Citrix. La inscripción tarda algún tiempo en completarse. Durante ese tiempo, Management Service muestra el progreso del registro.

Para habilitar la función Call Home, vaya a Configuración > Citrix ADC > Call Home, seleccione la instancia de Citrix ADC 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 > Citrix ADC > Call Home, seleccione la instancia de Citrix ADC 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 de proxy Call Home. Call Home puede cargar los datos de la instancia de Citrix ADC al servidor Citrix TaaS a través de un servidor proxy. Para utilizar esta función, habilítelo en la instancia de Citrix ADC y especifique la dirección IP y el número de puerto de un servidor proxy HTTP. Todo el tráfico desde el servidor proxy a los servidores TaaS (a través de Internet) está cifrado y SSL, por lo que la seguridad y la privacidad de los datos no se ven comprometidas.

- Para configurar Call home en la instancia de Citrix ADC desde Management Service

  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 Citrix ADC, vaya a Configuración > Citrix ADC > Call Home, seleccione la instancia Citrix ADC 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 Citrix ADC, vaya a Configuración > Citrix ADC, en el panel derecho, haga clic en Call Home, en la página Configurar Inicio de llamada, seleccione las instancias Citrix ADC en la sección Instancias disponibles, especifique otros detalles y haga clic en Aceptar.

  - Sondeo de las instancias de Citrix ADC

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

Supervisión del estado del sistema

June 19, 2019

La supervisión del estado del sistema detecta errores en los componentes supervisados, de modo que puede tomar medidas correctivas para evitar una falla. Los siguientes componentes se supervisan en un dispositivo Citrix ADC 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 detalles de los componentes supervisados, expanda Estado del sistema y, 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 del 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 del 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, memoria o BMC.

- **Estado**

  Estado (condición) del componente. Para el hardware y para la versión de firmware de BMC, ERROR indica una desviación del valor esperado. En el caso de las llamadas a XenServer, ERROR indica que Management Service no puede comunicarse con XenServer mediante una llamada API, HTTP, PING o SSH. Para el complemento Health Monitor, ERROR indica que el complemento no está instalado en XenServer.

- **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 XenServer.

Supervisión de 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. Los detalles se muestran para discos físicos y para discos virtuales o particiones creadas a partir de discos físicos.

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

- **Nombre**

  Nombre del disco físico.

- **Tamaño:**

  Tamaño del disco, en gigabytes (GB).

- **Utilizado**

  Cantidad de datos en el disco, en gigabytes (GB).

- **Transacciones/s**

  Número de bloques que se leen o escriben por segundo. Este número se lee a partir de la salida iostat.

- **Bloques de lectura/s**

  Número de bloques que se leen por segundo. Puede utilizar este valor para medir la velocidad de salida del disco.

- **Bloques de escritura/s**

  Número de bloques que se escriben por segundo. Puede utilizar este valor para medir la velocidad de entrada en el disco.

- **Total de bloques leídos**

  Número de bloques leídos desde la última vez que se inició el dispositivo.

- **Total de bloques escritos**

  Número de bloques escritos desde la última vez que se inició el dispositivo.

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

- **Bahía de**
  Drive

  Número de la unidad en la bahía de la unidad. Puede ordenar los datos de este parámetro.

- **Estado**

  Estado (condición) de la unidad en la bahía de la unidad. Valores posibles:

  - BUENO: La unidad está en buen estado y está lista para su uso.
  - FAIL: La unidad ha fallado y tiene que ser reemplazada.
  - FALTA: No se detecta una unidad en la bahía de la unidad.
  - 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 gigabytes (GB).

- **Utilizado**

  Cantidad de datos en el repositorio de almacenamiento, en gigabytes (GB).

Supervisión de los sensores de hardware en el dispositivo SDX

Puede supervisar los componentes de hardware del 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 monitoreo 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 fan.

- **Estado**

  Estado (condición) 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 sobre la temperatura incluye los siguientes detalles:

- **Nombre**

  Nombre del componente, como CPU o módulo de memoria (por ejemplo, P1-DIMM1A).

- **Estado**

  Estado (condición) del componente. ERROR indica que el valor actual está fuera del intervalo.

- **Valor**
  actual (grado C)

  Temperatura actual, en grados, del componente.

La información sobre voltaje incluye los siguientes detalles:

- **Nombre**

  Nombre del componente, como núcleo de CPU.

- **Estado**

  Estado (condición) del componente. ERROR indica que el valor actual está fuera del intervalo.

- **Valor**
  actual (voltios)

  Tensión de corriente presente 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 funcionando como se esperaba.

Supervisión de las interfaces en el dispositivo SDX

Puede supervisar las interfaces 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 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: Arriba, abajo.

- **VF asignadas/Total**

  Número de funciones virtuales asignadas a la interfaz y número de funciones virtuales disponibles en esa interfaz. Puede asignar hasta siete funciones virtuales en una interfaz 1G y hasta 40 funciones virtuales en una interfaz 10G.

- **Paquetes Tx**

  Número de paquetes transmitidos desde la última vez que se inició el dispositivo.

- **Paquetes Rx**

  Número de paquetes recibidos desde la última vez que se inició el dispositivo.

- **Bytes Tx**

  Número de bytes transmitidos desde la última vez que se inició el dispositivo.

- **Bytes Rx**

  Número de bytes recibidos desde la última vez que se inició el dispositivo.

- **Errores Tx**

  Número de errores en la transmisión de datos desde la última vez que se inició el dispositivo.

- **Errores Rx**

  Número de errores en la recepción de datos desde la última vez que se inició el dispositivo.

Configurar los parámetros de notificación del sistema

June 19, 2019

Puede enviar notificaciones para comunicarse con determinados grupos de usuarios para una serie de funciones relacionadas con el sistema. Puede configurar un servidor de notificaciones en SDX Management Service para configurar servidores de puerta de enlace de correo electrónico y SMS (Short Message Service) 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 está habilitada para todas las categorías de eventos y las notificaciones se envían al perfil de correo electrónico o SMS existente.

Para configurar las opciones de notificación del sistema

1. Vaya a **Sistema > Notificaciones > Configuración y, a continuación,** haga clic en **Cambiar configuración de notificación. **
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 nuevos detalles del 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 nuevos detalles del servidor SMS en los campos correspondientes.
3. Haga clic en **Aceptar**.

Configurar Management Service

June 19, 2019

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 de Management Service. También puede crear archivos TAR de Management Service y XenServer y enviarlos a la asistencia técnica.

Si una tarea que necesita realizar no se describe a continuación, consulte la lista de tareas a la izquierda.

Administración de Sesiones de Cliente

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

En el panel Sesiones, puede ver los siguientes detalles:

- Nombre de usuario

  La cuenta de usuario que se está utilizando para la sesión.

- Dirección IP

  La dirección IP del cliente desde el que se ha creado la sesión.

- Puerto

  El puerto que se utiliza para la sesión.

- Hora de inicio de sesión

  Hora en la que se creó la sesión actual en el dispositivo SDX.

- Hora de la última actividad

  Hora en la que se detectó por última vez la actividad del usuario en la sesión.

- La sesión caduca en

  Tiempo restante para que la sesión caduque.

Para ver las sesiones de cliente, en la ficha Configuración, en el panel de navegación, expanda Sistema y, a continuación, haga clic en Sesiones.

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

No puede finalizar una sesión desde el cliente que ha iniciado esa sesión.

Configuración de directivas

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

La directiva de poda 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 copia de seguridad se ejecuta a las 00:30 a.m. todos los días y crea una copia de seguridad de registros y 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:

- Cifrar los archivos de copia 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 para los que se podan 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 #Previous** 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**, escriba el nombre de host o la dirección IP del servidor de copia 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. Seleccione **Eliminar archivo de Management Service después de la transferencia** 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**.

Reiniciar Management Service

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

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**.

Eliminación de archivos de Management Service

Actualizado: 2013-10-07

Puede eliminar cualquier archivo de documentación y compilación de Management Service que no sea necesario del dispositivo SDX.

Para quitar un archivo de Management Service:

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**.

Generación de 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 archivo TAR se puede generar para Management Service o XenServer, 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 archivo tar. El nombre de archivo indica si el archivo TAR es para Management Service o el servidor XenServer.

- Última modificación

  Fecha en la que se modificó por última vez este archivo.

- 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 adecuada para si quiere archivar datos de XenServer, Management Service, Appliance (incluidos XenServer y Management Service), Instances o Appliance (incluidas las instancias).
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.

Compatibilidad con la interfaz de línea de comandos para Management Service

Ahora puede utilizar la interfaz de línea de comandos para realizar operaciones en Management Service. 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 de Citrix.

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

Puede acceder a información detallada sobre el uso y la sintaxis de los comandos desde las páginas de comando man.

Nota: CLI no es compatible con el acceso a la consola.

Configurar los parámetros de autenticación y autorización

June 19, 2019

La autenticación con Citrix ADC SDX Management Service puede ser local o externa. Con la autenticación externa, Management Service concede acceso al usuario sobre la base de la respuesta de un servidor externo. Management Service admite los siguientes protocolos de autenticación externa:

- Servicio de usuario de marcado de autenticación remota (RADIUS)
- Sistema de control de acceso a controladores de acceso a terminales (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 únicamente 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 de Management Service 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 pueden realizar solo operaciones de lectura. La autorización de los usuarios de SSH se limita únicamente 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 el caso de la autorización TACACS, el administrador del servidor TACACS debe permitir un comando especial, admin para un usuario que tenga privilegios de administrador y denegar este comando para usuarios con privilegios de solo lectura. Cuando un usuario inicia sesión en el dispositivo SDX, Management Service comprueba si el usuario tiene permiso para ejecutar este comando y si el usuario tiene permiso, se le asignan los privilegios de administrador, de lo contrario, se le asignan privilegios de solo lectura.

Adición de un grupo de usuarios

Los grupos son conjuntos lógicos de usuarios que necesitan acceder a información común o realizar tipos similares de tareas. Puede organizar 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 nuevos usuarios.

Si utiliza servidores de autenticación externos para la autenticación, los grupos en SDX se pueden configurar para que coincidan con los grupos configurados en 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 en el dispositivo SDX.

Para agregar un grupo de usuarios

1. En la ficha **Configuración**, en **Sistema**, expanda **Administración** y, a continuación, haga clic en **Grupos**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el cuadro de diálogo Crear grupo de sistemas, defina los siguientes parámetros:
   - Nombre: Nombre del grupo. Longitud máxima: 128
   - Permiso: Acciones que este grupo está autorizado a realizar. Valores posibles: Admin y readonly.
   - Usuarios: Usuarios de bases de datos pertenecientes al grupo. Seleccione los usuarios que quiere agregar al grupo.
4. Haga clic en **Crear** y **cerrar**.

Configuración de 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 XenServer. No cambie la contraseña directamente en XenServer.

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 cuentas de usuario existentes, con sus permisos.
2. En el panel Usuarios, realice una de las acciones siguientes:
   - 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 usuario del 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 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.
     - readonly: 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.
   - 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 u Aceptar y, a continuación, haga clic en Cerrar. El usuario que creó aparece en el panel Usuarios.

Para quitar una cuenta de usuario

1. En la ficha Configuración, en el panel de navegación, expanda Sistema, expanda **Administración**y, 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.

Configuración del tipo de autenticación

Desde la interfaz de Management Service, puede especificar la autenticación local o externa. La autenticación externa está inhabilitada para los usuarios locales de forma predeterminada. Puede activarse marcando la opción
Habilitar autenticación externa al agregar el usuario local o 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 muestra 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 de Management Service 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 de Management Service.

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**.

Configurar el servidor de autenticación externa

June 19, 2019

Citrix ADC SDX Management Service puede autenticar 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.

Adición de 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 respuesta por desafío RADIUS según las especificaciones de RADIUS. Los usuarios de RADIUS se pueden configurar con una contraseña única en el servidor RADIUS. Cuando el usuario inicia sesión en el dispositivo SDX, se le pide al usuario que especifique esta contraseña única.

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 valores para los parámetros:
   - Nombre *: Nombre del servidor.
   - Nombre del servidor / Dirección IP *: FQDN o dirección IP del servidor.
     Nota: DNS debe poder resolver el nombre de dominio completo (FQDN) especificado en una dirección IP, y solo se utiliza el DNS principal para resolver el FQDN. Para establecer 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 predeterminado: 1812.
   - Tiempo de espera *: Número de segundos que el sistema esperará para recibir una respuesta del servidor RADIUS. Valor predeterminado: 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 extracción de direcciones IP del NAS: Si está habilitada, la dirección IP del sistema (Management Service IP) se envía al servidor como “nasip” 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: ID 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: Id. de proveedor del atributo en el RADIUS que denota la IP de la intranet. Un valor de 0 indica que el atributo no está codificado por proveedor.
   - Tipo de atributo de dirección IP: Tipo de atributo del atributo de dirección IP remota en una respuesta RADIUS.
   - Identificador de proveedor de contraseña: ID de proveedor de la contraseña en la respuesta RADIUS. Se utiliza para extraer la contraseña de usuario.
   - Tipo de atributo de contraseña: Tipo de atributo del atributo de contraseña en una respuesta RADIUS.
   - Codificación de contraseñas: Cómo deben codificarse las contraseñas en los paquetes RADIUS que viajan del sistema al servidor RADIUS. Valores posibles: Pap, cap, 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, haga clic en Cerrar.

Adición de 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 valores para los parámetros:
   - Nombre *: Nombre del servidor.
   - Nombre del servidor / Dirección IP *: FQDN o dirección IP del servidor.
     Nota: DNS debe poder resolver el FQDN especificado en una dirección IP, y solo se utiliza el DNS principal para resolver el FQDN. Para establecer 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 predeterminado: 389.
   - Tiempo de espera *: Número de segundos que el sistema esperará para recibir 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 ValidateServerCert está habilitado, este parámetro especifica el nombre de host en el certificado del servidor LDAP. Una falta de coincidencia de nombre de host causa 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 ldaploginname samaccount y el nombre de usuario bob proporcionado por el usuario produciría 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, haga clic en Cerrar.

Compatibilidad con autenticación de clave pública SSH para usuarios 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 funciona con SSH.

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

> **Importante**
>
> Para la autenticación basada en claves, debe especificar una ubicación de las claves públicas estableciendo el valor de *Authorizedkeysfile 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 *Authorizedkeysfile en el archivo/etc/sshd_config*.**

Usuarios LDAP. La clave pública recuperada se almacena en */var/pubkey/<user_name>/tmp_authorized_keys-<pid>*. <pid> es el número único agregado para diferenciar entre las solicitudes SSH simultáneas del mismo usuario. Esta es la ubicación temporal para mantener la clave pública durante el proceso de autenticación. La clave pública se elimina del sistema una vez completada la autenticación.

Para iniciar sesión con el usuario, ejecute el siguiente comando desde el símbolo del sistema de 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**, marque la casilla de verificación **Autenticación** para fines de autenticación.

> **Nota**
>
> Desmarque la casilla de verificación Autenticación para usar “SSHPublicKeys” para la autenticación de 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, debe establecer manualmente el DNS principal para resolver el nombre del servidor, ya sea mediante la GUI o la CLI.

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

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

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

Si vuelve a ejecutar el comando networkconfig, verá el complemento DNS actualizado.

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 valores para los parámetros:
   - Nombre: Nombre del servidor TACA
   - Dirección IP: Dirección IP del servidor TACACS
   - Puerto: Puerto en el que se ejecuta el servidor TACACS. Valor predeterminado: 49
   - Tiempo de espera: Número máximo de segundos que el sistema esperará por una respuesta del servidor TACACS
   - Clave TACACS: Clave compartida entre el cliente y el servidor. Esta información es necesaria para que el sistema se comunique con el servidor TACACS
   - Contabilidad: Permite a Management Service registrar la información de auditoría con el servidor TACACAS.
   - Grupo de autenticación predeterminado: Grupo predeterminado que se elige cuando la autenticación se realiza correctamente, además de los grupos extraídos.
4. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Configurar la agregación de enlaces desde Management Service

June 19, 2019

La agregación de enlaces combina múltiples enlaces Ethernet en un único enlace de alta velocidad. La configuración de la agregación de enlaces aumenta la capacidad y la disponibilidad del canal de comunicación entre el dispositivo Citrix ADC 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, pierde 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 enlazar el canal a la VLAN anterior o a una nueva. Por ejemplo, si enlaza las interfaces de red 1/2 y 1/3 a una VLAN con ID 2 (VLAN 2) y, a continuación, las enlaza al canal LA/1, las interfaces de red se mueven a la VLAN predeterminada, pero puede enlazar el canal a VLAN 2.

Nota:

- Una interfaz debe formar parte de un solo canal.
- Se requieren como mínimo dos interfaces para configurar un canal.
- Las interfaces que forman parte de un canal no aparecen en la vista Configuración de red al agregar o modificar una instancia de Citrix ADC. 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, suponga dos instancias, Instance1 e Instance2. Cuando se aprovisionan estas instancias, las interfaces 10/1, 10/2 y 10/3 se asignan a Instance1 y las interfaces 10/1 y 10/2 se asignan a Instance2. Si se crea un canal LA con las interfaces 10/1, 10/2 y 10/3, instance1 no se reinicia. Sin embargo, Management Service cierra Instance2, asigna la interfaz 10/3 a Instance2 y, a continuación, reinicia Instance2.

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

Configurar un canal desde Management Service

June 19, 2019

Puede configurar un canal manualmente o puede usar el Protocolo de control de agregación de enlaces (LACP). No se puede aplicar LACP a un canal configurado manualmente, ni tampoco se puede configurar manualmente un canal creado por LACP. Configure un canal desde Management Service y seleccione el canal en el momento de aprovisionar una instancia de Citrix ADC o posterior en el momento de modificar una instancia de Citrix ADC.

Para configurar un canal desde Management Service

1. En la ficha Configuración, 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.
  - Active-Pasivo: Configurado solo en las interfaces de administración 0/x.
  - LACP: Configurado en interfaces de datos, así como en 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 alta disponibilidad, la conmutación por error se activa si el canal LA tiene habilitado 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 menor que el umbral normal especificado después de superar el umbral alto, el dispositivo Citrix ADC 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 quiera incluir en este canal.
5. En la ficha Configuración, establezca 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 en el nodo asociado.
   - Supervisión de alta disponibilidad: En una configuración de alta disponibilidad (HA), supervise el canal para detectar eventos de error. La falla de cualquier canal de LA que tiene 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 enlazadas a este canal. OFF aplica la etiqueta para todas las VLAN distintas de 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, haga clic en Cerrar.

Listas de control de acceso

June 19, 2019

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

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

> **Nota**
>
> Las ACL en los dispositivos SDX son compatibles desde la versión 12.0 57.19 en adelante.

Este tema incluye las siguientes secciones:

- Pautas de uso
- Cómo configurar ACL
- Acciones adicionales para reglas de ACL
- Solución de problemas

Pautas de uso

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

- Al actualizar el dispositivo SDX a la versión 12.0 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 Citrix Application Delivery Management para administrar el dispositivo SDX, debe crear reglas ACL adecuadas para permitir la comunicación entre MAS y SDX Management Service.
- Para cualquier otra configuración del dispositivo SDX, como aprovisionamiento o eliminación de VPX, adición o eliminación de servidores externos, administración SNMP, etc., no requiere ningún cambio en la configuración de ACL existente. Management Service se encarga de la comunicación con esas entidades.

Cómo configurar una ACL

La configuración de una ACL implica los siguientes pasos:

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

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

Para 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. Con el botón de alternar, active la función ACL.

![Imagen localizada]

Para crear una regla de ACL

1. En la página ACL, haga clic en **Crear regla**.
2. Se abrirá la ventana Crear regla. Agregue los detalles enumerados en la tabla siguiente.

Propiedad	Descripción
Nombre	Agregue un nombre.
Protocolo	Seleccione un protocolo en el menú. De forma predeterminada, TCP está seleccionado. Puede seleccionar CUALQUIER 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 CUALQUIER si la regla debe aplicarse a todo el tráfico entrante.
IP de destino	La dirección IP de SDX Management Service se rellena automáticamente como IP de destino. Este campo no se puede modificar.
Puerto de destino	Especifique el puerto de destino al que se aplica la regla. Seleccione CUALQUIER si la regla se aplica a todos los puertos de destino.
Acción	Seleccione la acción de regla, que es Permitir o Denegar.

Propiedad	Descripción
Prioridad	Asigne prioridad para especificar el orden en el que se va a evaluar 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 inferior tiene una prioridad más alta. Por ejemplo, la prioridad número 1 tiene una prioridad mayor que la prioridad número 2. Si ninguna de las reglas coincide con el paquete entrante, el paquete se bloquea.

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

Figura: Ejemplo de una regla ACL

Después de crear la regla, se encuentra en estado inhabilitado. Para que la regla sea efectiva, debe habilitarla.

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

Para habilitar una regla ACL

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

Acciones adicionales para 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. Cambiar la numeración de la prioridad de las reglas de ACL

Para 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**
>
> Cuando inhabilita una regla, la regla ya no se aplica al tráfico entrante; sin embargo, la configuración de regla permanece bajo la configuración de ACL.

Para 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 las modificaciones 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 al habilitar la regla.

Para eliminar una regla de ACL

1. Asegúrese de que la regla está 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** de 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 estado habilitado.

Para volver a numerar 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. SDX Management Service 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

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

Solución de problemas

Si las reglas de ACL están configuradas incorrectamente, se puede denegar el acceso a todas las cuentas de usuario. Si pierde inadvertidamente todo el acceso de 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 XenServer mediante SSH y su cuenta "root".

2. Inicie sesión en la consola de la máquina virtual de Management Service mediante los privilegios nsroot.

3. Ejecute el comando "pfctl –d".

4. Inicie sesión en Management Service a través de GUI y vuelva a configurar la ACL en consecuencia.

Configurar un clúster de instancias de Citrix ADC

June 19, 2019

Después de aprovisionar instancias de Citrix ADC en uno o más dispositivos SDX, puede crear un clúster de instancias de Citrix ADC. Los nodos del clúster pueden ser instancias de Citrix ADC en el mismo dispositivo SDX o en otros dispositivos SDX disponibles en la misma subred.

Nota

- Para configurar un clúster, debe comprender la agrupación en clústeres Citrix ADC. Para obtener más información, consulte Agrupar en clústeres.
- Para los clústeres que tienen instancias de Citrix ADC en dispositivos SDX, Citrix recomienda utilizar instancias de Citrix ADC desde tres dispositivos SDX. Esto garantiza que siempre se cumplan los criterios de clúster de un mínimo de nodos (n/2 + 1).

Figura 1. Cluster de instancias de Citrix ADC SDX

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

- Cluster1 incluye dos instancias en SDX1.
- Cluster2 incluye una instancia en SDX1, dos instancias en SDX2 y otras dos instancias en SDX3.

Puntos a recordar

- Todos los nodos de un clúster deben ser del mismo tipo. No puede formar un clúster de hardware y dispositivos virtuales, ni un clúster de instancias de VPX Citrix ADC ni instancias de Citrix ADC SDX.
- Las instancias de Citrix ADC deben ser de la misma versión, que debe ser la versión 10.1 o posterior.
- Todas las instancias de Citrix ADC deben tener la misma licencia de función.
- No se pueden actualizar configuraciones en instancias individuales de Citrix ADC después de agregarlas al clúster. Todos los cambios deben realizarse a través de la dirección IP del clúster.
- Todas las instancias de Citrix ADC deben tener los mismos recursos (memoria, CPU, interfaces, etc.).

Para configurar un clúster en un dispositivo SDX

1. Inicie sesión en el dispositivo SDX.
2. En la ficha Configuración, vaya a Citrix ADC y, a continuación, haga clic en Clusters.
3. Cree el clúster:
   a) Haga clic en Crear clúster.
   b) En el cuadro de diálogo Crear clúster, defina los parámetros necesarios para el 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 configuración.
   d) Haga clic en Finalizar para crear el clúster.
   Nota: Cuando una instancia de Citrix ADC que se aprovisionó en el dispositivo SDX tiene configurada la VLAN L2 y si ese nodo se agrega al clúster, el comando
   add vlan se guarda con el parámetro

sdxvlan 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 configuración.
   d) Haga clic en Finalizar para agregar el nodo al clúster.
   e) Repita los pasos de a a d para agregar otro nodo al clúster.

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

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

Para agregar una instancia Citrix ADC que existe en un dispositivo SDX a un clúster configurado en otro dispositivo SDX

1. Inicie sesión en el dispositivo SDX desde el que quiere agregar la instancia de Citrix ADC.
2. En la ficha Configuración, vaya a Citrix ADC y, a continuación, haga clic en Clusters.
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 configuración.
6. Haga clic en Finalizar para agregar el nodo al clúster.

Configurar agregación de enlaces de clústeres

June 19, 2019

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 vínculos (LA) de Citrix ADC. La única

diferencia es que, mientras que la agregación de enlaces requiere que las interfaces estén en el mismo dispositivo, en la agregación de enlaces de clúster, las interfaces se encuentran en diferentes nodos del clúster. Para obtener más información acerca de la agregación de vínculos, consulteConfiguración de Agregación de Vínculos.

Por ejemplo, considere un clúster de seis nodos, en dos dispositivos SDX, en el que los seis nodos estén conectados a un conmutador ascendente. Un canal LA de clúster (CLA/1) está formado por interfaces de enlace 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 las interfaces de los nodos SDX locales y remotos.
- Un máximo de cuatro canales LA de clúster se admiten en un clúster.
- Se pueden enlazar un máximo de 16 interfaces a cada canal LA del clúster.
- Las interfaces de plano posterior no pueden formar parte de un canal LA de 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 solo puede enlazarse a un canal.
- El acceso de administración a un nodo de clúster no debe configurarse en un canal LA del clúster (por ejemplo, CLA/1) o en sus interfaces miembro. Cuando el nodo está INACTIVE, la interfaz LA del clúster correspondiente se marca como POWER OFF, lo que hace que pierda el acceso a la administración.

Debe implementar configuraciones similares en la dirección IP del clúster y en el dispositivo de conexión externo. Si es posible, configure el conmutador ascendente para distribuir el tráfico sobre la base de la dirección IP o el puerto en lugar de la dirección MAC.

Puntos a recordar:

- Habilite LACP (especificando el modo LACP como ACTIVE o PASSIVE).
  Nota: Asegúrese de que el modo LACP no esté configurado como PASIVO tanto en el clúster Citrix ADC 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 de grupo de agregación de vínculos de clúster (CLAG) no se pueden compartir con otras máquinas virtuales.
- En el switch ascendente, establezca el tiempo de espera LACP en “corto” para evitar agujeros de tráfico de larga duración en los nodos del clúster cuando no se notifique al switch ascendente de apagado de la CLAG y sus interfaces miembro hasta después del tiempo de espera de LACP.

Requisitos previos:

Asegúrese de que ha creado un clúster de instancias de Citrix ADC. Los nodos del clúster pueden ser instancias de Citrix ADC en el mismo dispositivo SDX o en otros dispositivos SDX 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 **Citrix 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 **+**.

Las interfaces seleccionadas se muestran en el cuadro Selección **configurada**.

c. En la sección **Configuración**, haga lo siguiente:

i. En el campo **Alias**, introduzca un nombre alternativo para el canal LA del clúster.

ii. En el campo **Tiempo de espera LACP**, seleccione cualquiera de los siguientes valores para definir el intervalo después del cual no se agrega un enlace, 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 en el nodo asociado:

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

iii. Para la configuración de alta disponibilidad (HA), active la casilla de verificación **Supervisión de alta disponibilidad** para supervisar el canal en busca de eventos de error. La falla de cualquier canal de LA que tiene habilitado HA MON desencadena la conmutación por error de HA.

iv. Seleccione **Etiquetar todo** para agregar una etiqueta 802.1q de cuatro bytes a cada paquete enviado en este canal. La configuración ON aplica etiquetas para todas las VLAN enlazadas a este canal. OFF aplica la etiqueta a todas las VLAN distintas de la VLAN nativa.

d. Haga clic en **Crear** para configurar un CLAG para uno de los dispositivos SDX**.**

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

Nota: Si selecciona **No**, el CLAG no está configurado.

> **Importante**
>
> - Debe actualizar 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 debe cambiarse manualmente en cualquiera de los dispositivos SDX.

6. Para cambiar la configuración de MTU en el cuadro de diálogo **CLAGs**, haga lo siguiente:

i.Seleccione **CLA/1** y haga clic en **Modificar**.

ii.En el cuadro de diálogo **Configurar CLAG**, establezca la MTU manualmente en el campo **MTU** y haga clic en **Aceptar. **

7. En el cuadro de diálogo **Confirmar**, haga clic en **Sí**.

Configurar cifrados SSL para acceder de forma segura a Management Service

June 19, 2019

Puede seleccionar conjuntos de cifrado SSL de una lista de cifrados SSL compatibles con dispositivos Citrix ADC SDX y enlazar 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 enlazados que no forman parte de la lista de cifrados SSL admitidos, o que incluyan estos cifrados en un grupo de cifrado personalizado.

Cifras SSL compatibles

En la tabla siguiente se enumeran los cifrados SSL compatibles.
Nombre de cifrado de Citrix	OpenSSL CipherName	Código hexadecimal	Protocolo	Intercambio de llaves	Auth	MAC
———————————	———————————	———-	———-	———-	——	———–
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)
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-AES-256-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)
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)
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	Ninguna	RC4(128)
SSL3-ADH-DES-CBC3-SHA	ADH-DES-CBC3-SHA	0x001B	SSLv3	DH	Ninguna	3DES(168)
SSL3-ADH-DES-CBC-SHA	ADH-DES-CBC-SHA	0x001A	SSLv3	DH	Ninguna	DES (56)
TLS1-ADH-AES-128-CBC-SHA	ADH-AES128-SHA	0x0034	SSLv3	DH	Ninguna	AES (128)
TLS1-ADH-AES-256-CBC-SHA	ADH-AES256-SHA	0x003A	SSLv3	DH	Ninguna	AES (256)
SSL3-EXP-ADH-RC4-MD5	EXP-ADH-RC4-MD5	0x0017	SSLv3	DH (512)	Ninguna	RC4(40)
SSL3-EXP-ADH-DES-CBC-SHA	EXP-ADH-DES-CBC-SHA	0x0019	SSLv3	DH (512)	Ninguna	DES (40)
SSL3-NULL-MD5	NULL-MD5	0x0001	SSLv3	RSA	RSA	Ninguna
SSL3-NULL-SHA	NULL-SHA	0x0002	SSLv3	RSA	RSA	Ninguna

Grupos de cifrado predefinidos

En la tabla siguiente se enumeran los grupos de cifrado predefinidos proporcionados por el dispositivo SDX.

Nombre de grupo de cifrado	Descripción
TODOS	Todos los cifrados admitidos por el dispositivo SDX, excluidos los cifrados NULL
PREDETERMINADO	Lista de cifrado predeterminada con fuerza de cifrado > = 128 bits
KRSA	Cifradores con Key-ex algo como RSA
KedH	Cifras con Key-ex algo como Ephemeral-DH
DH	Cifras con Key-ex algo como DH
EDH	Cifrados con clave EX/Auth algo como DH
ARSA	Cifradores con Auth algo como RSA
ADS	Cifrados con Auth algo como DSS
Anula	Cifrados con Auth algo como NULL
DSS	Cifrados con Auth algo como DSS
DES	Cifras con Enc algo como DES
3DES	Cifras con Enc algo como 3DES
RC4	Cifras con Enc algo como RC4

Nombre de grupo de cifrado	Descripción
RC2	Cifras con Enc algo como RC2
NULO	Cifradores con Enc algo como NULL
MD5	Cifras con MAC algo como MD5
SHA1	Cifras con MAC algo como SHA-1
SHA	Cifras con MAC algo como SHA
NULO	Cifradores con Enc algo como NULL
RSA	Cifradores con clave EX/Auth algo como RSA
ADH	Cifradores con Key-ex algo como DH y Auth algo como NULL
SSLv2	Cifradores de protocolo SSLv2
SSLv3	Cifradores de protocolo SSLv3
TLSv1	Cifradores de protocolo SSLv3/TLSv1
TLSv1_ONLY	Cifradores de protocolo TLSv1
EXP	Exportar cifrados
EXPORTAR	Exportar cifrados
EXPORT40	Exportar cifrados con cifrado de 40 bits
EXPORT56	Exportar cifrados con cifrado de 56 bits
BAJO	Cifrados de baja resistencia (cifrado de 56 bits)
MEDIANO	Cifrados de fuerza media (cifrado de 128 bits)
ALTO	Cifrados de alta resistencia (cifrado de 168 bits)
ES	Cifrados AES
FIPS	Cifrados aprobados por FIPS
ECDHE	Cifras DH efímeras de curva elíptica
AES-GCM	Cifras con Enc algo como AES-GCM
SHA2	Cifras con MAC algo como SHA-2

Visualización de 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**.

Creación de 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**.

Visualización de enlaces de cifrado SSL existentes

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

> **Nota**
>
> Después de actualizar a la versión más reciente de Management Service, la lista de conjuntos de cifrado existentes muestra los nombres de OpenSSL. Una vez que vincula los cifrados desde Management Service actualizado, la visualización utiliza la convención de nomenclatura de Citrix.

Vinculación de cifrados al servicio HTTPS

Para 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 **Cambiar configuración 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 grupos de cifrado de grupos de cifrado predefinidos proporcionados por el dispositivo SDX, active la casilla de verificación **Grupos de cifrado**, seleccione el grupo de cifrado en la lista desplegable **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**.

Copia de seguridad y restauración de los datos de configuración del dispositivo SDX

June 19, 2019

El proceso de copia de seguridad del dispositivo Citrix ADC SDX es un proceso de un solo paso que crea un archivo de copia de seguridad que contiene lo siguiente:

- Imagen de un solo paquete:
  - Imagen de XenServer
  - Parches rápidos y paquetes complementarios de XenServer
  - Imagen de Management Service
- Imagen XVA
- Actualizar imagen
- Configuración de SDX
- Configuración

Para realizar una copia de seguridad de la configuración actual:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Management Service** y, a continuación, haga clic en **Archivos de copia de seguridad**.
2. En el panel **Archivos de copia** de seguridad, haga clic en **Copia de** seguridad.
3. en el cuadro de diálogo **Nuevo archivo de copia** de seguridad, active la casilla de verificación **Archivo de protección 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 copia de seguridad. El nombre de archivo del archivo de copia de seguridad incluye la dirección IP actual de Management Service y la marca de tiempo cuando se realizó la copia de seguridad.Para comprobar si hay alguna discrepancia que pueda tener el archivo de copia de seguridad, desde la GUI de SDX vaya a Configuración > Sistema > Eventos/Alarmas.

Copia de seguridad programada

De forma predeterminada, SDX crea una copia de seguridad cada 24 horas mediante una directiva de copia de seguridad. Mediante la directiva de copia de seguridad, puede definir el número de archivos de copia de seguridad que quiere conservar en el dispositivo SDX. Además, puede cifrar los archivos de copia de seguridad programados mediante una contraseña para asegurarse de que el archivo de copia de seguridad es seguro.

Para modificar la directiva de copia 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, realice 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, active la casilla de verificación **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.

Transferir manualmente el archivo de copia de seguridad a un servidor de copia de seguridad externo

Puede transferir manualmente el archivo de copia de seguridad a un servidor de copia de seguridad externo. Asegúrese de tener los detalles del servidor de copia de seguridad externo antes de transferir manualmente el archivo de copia de seguridad.

Para transferir manualmente el archivo de copia de seguridad a un servidor de copia de seguridad externo:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Management Service** y, a continuación, haga clic en **Archivos de copia de seguridad**.
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 nombre de host o dirección IP del servidor de copia 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 de Management Service** después de la transferencia 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.
9. Haga clic en **Aceptar**.

Restauración del 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****

- Si restaura el dispositivo SDX mediante el archivo de copia de seguridad de otro dispositivo SDX, asegúrese de agregar la configuración de red configure Management Service en el dispositivo de acuerdo con la configuración disponible en el archivo de copia de seguridad, antes de iniciar el proceso de restauración.
- Asegúrese de que la variante de plataforma en la que se realizó la copia de seguridad es la misma que en la que está intentando restaurar (no se admite la restauración del archivo de copia de seguridad entre dos variantes de plataforma diferentes).

Para restaurar el dispositivo desde el archivo de copia de seguridad:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Management Service** y, a continuación, haga clic en **Archivos de copia de seguridad**.

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 dispositivo** y, a continuación, haga clic en **Continuar** .

Aparece una página que muestra los diferentes componentes de la restauración de la aplicación:

- Licencia
- Imagen SDX
- Archivos XVA
- Configuración de Citrix ADC
- Resumen

Si falta alguno de los componentes necesarios, como una licencia válida y compatible, imágenes XVA, imágenes de Citrix ADC, imagen de paquete único en el archivo de copia de seguridad, se le pedirá que cargue el elemento que falta antes de continuar.

Para saber si se puede restaurar un archivo de copia de seguridad en la versión actual de SDX Single Bundle Image Version, consulte esta tabla.

Versión actual de imagen de paquete único SDX	Versión del archivo de copia de seguridad
11.0	compatible con 11.0, 12.0
11.1	compatible con 11.1, 12.0; no compatible con 11.0

Versión actual de imagen de paquete único SDX	Versión del archivo de copia de seguridad
12.0	compatible con 12.0; no compatible con 11.0 y 11.1

4. En la página **Licencia**, compruebe que existe una licencia válida y haga clic en **Siguiente**.

5. Aparecerá la página **Imagen SDX**. Si no es necesaria 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 falta el archivo XVA de cualquier instancia 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 abrirá la página Configuración de Citrix ADC.Los archivos de configuración de Citrix ADC no son obligatorios. Puede aprovisionar la instancia sin restaurar su configuración. Si falta el archivo de configuración de Citrix ADC en el archivo de copia de seguridad, solo puede proceder con el aprovisionamiento de instancias u omitir la restauración de la instancia. Haga clic en **Siguiente** para ir a la página siguiente.

8. Aparecerá la página de resumen 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 es así, aparece una marca cruzada.
- Mensajes de error: Si el dispositivo o la instancia no están listos para la restauración, aparece un mensaje de error explicando el motivo.

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

Restauración de la instancia de Citrix ADC

Puede restaurar la instancia de Citrix ADC en el dispositivo SDX en las instancias de Citrix ADC que están disponibles en el archivo de copia de seguridad.

Puntos a tener en cuenta:

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

Para restaurar la instancia de Citrix ADC en el archivo de copia de seguridad:

1. En la ficha **Configuración**, en el panel de navegación, expanda **Management Service** y, a continuación, haga clic en **Archivos de copia de seguridad**.
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 Citrix ADC 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 el dispositivo SDX que ejecuta la instancia que se está restaurando esté presente XVA, la imagen de compilación y la configuración de canal adecuados.

Restablecer dispositivos

June 19, 2019

El dispositivo Citrix ADC SDX le permite:

- Restablecer la configuración del dispositivo.
- Restablecer el dispositivo a la versión de fábrica
- Restablecer el dispositivo a una versión determinada de imagen de paquete único

Antes de restablecer un dispositivo, realice una copia de seguridad de todos los datos almacenados en el dispositivo, incluida la configuración de todas las instancias de Citrix ADC aprovisionadas en el dispositivo.

Citrix recomienda almacenar los archivos fuera del dispositivo. Restablecer un dispositivo finaliza todas las sesiones de cliente actuales con Management Service, por lo que debe volver a iniciar sesión en Management Service para realizar 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

Restablecimiento de 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 certificado SSL y clave.
- Elimina los archivos de licencia y archivo técnico.
- Elimina la configuración NTP del dispositivo.
- Restaura la zona horaria a UTC.
- Restaura las directivas de poda y copia de seguridad a su configuración predeterminada.
- Elimina la imagen de Management Service.
- Elimina la imagen de Citrix ADC SDX.
- Elimina todas las imágenes XVA excepto el último archivo de imagen al que se accedió en el dispositivo.
- Restaura la configuración predeterminada de la interfaz.
- Restaura la configuración predeterminada del dispositivo, incluidos los perfiles predeterminados, los usuarios y la configuración del sistema.
- Restaura las direcciones IP predeterminadas para XenServer y Management Service.
- Restaura contraseñas predeterminadas para XenServer y Management Service.
- Reinicia Management Service.

Para restablecer la configuración del dispositivo:

1. En la ficha **Configuración** , haga clic en el nodo **Sistema** y, a continuación, en el grupo **Administración del sistema** , haga clic en **Restablecer equipo** .
2. En el cuadro de diálogo **Restablecer equipo** , seleccione **Restablecer configuración** en la lista desplegable **Restablecer tipo** y haga clic en **Aceptar** .

Restablecimiento del 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 Restablecimiento de fábrica restablece las direcciones IP actuales de Management Service y XenServer a las direcciones IP predeterminadas de Management Service y XenServer.

Antes de realizar un restablecimiento de fábrica, realice una copia de seguridad de todos los datos almacenados en el dispositivo, incluida la configuración de todas las instancias de Citrix ADC aprovisionadas en el dispositivo. Citrix recomienda almacenar los archivos fuera del dispositivo. La realización

de un restablecimiento de fábrica termina todas las sesiones de cliente actuales con Management Service, por lo que debe volver a iniciar sesión en Management Service para realizar cualquier tarea de configuración adicional. Cuando esté 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.

Para restablecer el dispositivo a la versión de fábrica:

1. En la ficha **Configuración**, haga clic en Nodo **Sistema** y, a continuación, en el grupo **Administración del sistema**, haga clic en **Restablecimiento de dispositivo**.
2. En el cuadro de diálogo **Restablecimiento de dispositivo**, seleccione **Restablecimiento de fábrica** en la lista desplegable **Tipo de restablecimiento** y haga clic en **Aceptar**.

Restablecimiento del dispositivo a una versión de imagen de paquete único

Management Service proporciona la opción de instalación limpia que le permite instalar una versión arbitraria de una imagen de paquete único en el dispositivo. Permite realizar una nueva instalación de la imagen de paquete único como la nueva imagen de arranque predeterminada y elimina la configuración existente en el dispositivo SDX.

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 de 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 de 10G
11.1.51.x	Todas las plataformas SDX.

Requisitos previos

Asegúrese de que:

- Se conmutan por error todos los nodos principales de alta disponibilidad a un dispositivo SDX diferente. Si no dispone de capacidades de alta disponibilidad, asegúrese de planificar el tiempo de inactividad en consecuencia.
- Descargue la imagen de un solo paquete en su equipo local.

> **Importante**
>
> Asegúrese de que no reinicia ni enciende el dispositivo mientras utiliza la opción Limpiar instalación.

Para restablecer el dispositivo a una única versión de imagen de paquete:

1. En la ficha **Configuración**, haga clic en Nodo **Sistema** y, a continuación, en el grupo **Administración del sistema**, haga clic en **Restablecimiento de dispositivo**.
2. En el cuadro de diálogo **Restablecimiento de dispositivo**, seleccione **Instalación limpia** en la lista desplegable **Tipo de restablecimiento** y haga clic en **Aceptar**.

Servidores de autenticación externa en cascada

June 19, 2019

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

Para habilitar la autenticación en cascada, debe agregar los servidores de autenticación externos a Management Service. 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, si quiere agregar cuatro servidores de autenticación externos para la autenticación en cascada, puede agregar dos servidores RADIUS, un servidor LDAP y un servidor TACACS, o cuatro servidores del mismo tipo. Puede configurar hasta 32 servidores de autenticación externos en Citrix Application Delivery Management.

Para conectar 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**y, 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 **Servidores de autenticación** como se muestra en la figura siguiente. Puede especificar el orden de autenticación mediante el icono situado junto al nombre de un servidor para mover el servidor hacia arriba o hacia abajo en la lista.

Aprovisionar instancias de Citrix ADC

June 19, 2019

Puede aprovisionar una o más instancias de Citrix ADC en el dispositivo SDX mediante Management Service. El número 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, Management Service no permite aprovisionar más instancias de Citrix ADC.

El aprovisionamiento de una instancia de Citrix ADC VPX en el dispositivo SDX incluye los siguientes pasos.

1. Defina un perfil de administrador para enlazar a la instancia de Citrix ADC. Este perfil especifica las credenciales de usuario que utiliza Management Service para aprovisionar la instancia de Citrix 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 Citrix ADC mediante el asistente Provisioning Citrix ADC en Management Service. Management Service implementa implícitamente la instancia de Citrix ADC en el dispositivo SDX y, a continuación, descarga los detalles de configuración de la instancia.

> **Advertencia**
>
> Asegúrese de modificar las interfaces de red aprovisionadas o VLANS de una instancia mediante Management Service en lugar de realizar las modificaciones directamente en la instancia.

Crear un perfil de administrador

Los perfiles de administración especifican las credenciales de usuario que utiliza Management Service al aprovisionar las instancias de Citrix ADC y posteriormente 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 Citrix ADC a través de la CLI o la utilidad de configuración.

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 un nombre de usuario de nsroot y la contraseña también es nsroot. Este perfil no se puede modificar ni eliminar. Sin embargo, debe anular el perfil predeterminado creando un perfil de administrador definido por el usuario y adjuntándolo a la instancia cuando aprovisione la instancia. El administrador de Management Service puede eliminar un perfil de administrador definido por el usuario si no está asociado a ninguna instancia de Citrix ADC.

Importante:
No cambie la contraseña directamente en la instancia VPX. Si lo hace, la instancia se vuelve inaccesible desde Management Service. Para cambiar una contraseña, primero cree un perfil de administrador y, a continuación, modifique la instancia de Citrix ADC, seleccionando este perfil en la lista Perfil de administración.

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

Para crear un perfil de administrador

1. En la ficha **Configuración**, en el panel de navegación, expanda **Configuración de Citrix ADC** 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**.

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 Citrix ADC. Longitud máxima: 31 caracteres.
- Puerto SSH: Configure el puerto SSH. El puerto predeterminado es 22.
- Active la casilla de verificación **Usar configuración global para la comunicación de Citrix ADC**, si quiere que la configuración se defina en la Configuración del sistema para la comunicación entre Management Service y la instancia de Citrix ADC. Puede desactivar esta casilla y cambiar el protocolo a HTTP o HTTPS.
  - Seleccione la opción **http** para utilizar el protocolo HTTP para la comunicación entre Management Service y la instancia de Citrix ADC.
  - Seleccione la opción **https** para utilizar el canal seguro para la comunicación entre Management Service y la instancia de Citrix ADC

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 **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, haga clic en **Cerrar**. El perfil de administrador que creó aparece en el panel **Perfiles de administración**.

Si el valor de la columna **Default** es true, el perfil predeterminado es el perfil admin. Si el valor es false, 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 de Management Service. 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**.

Cargar una imagen XVA de Citrix ADC

Se necesita un archivo.xva para agregar una instancia de Citrix ADC VPX.

Es necesario cargar los archivos XVA de Citrix ADC SDA en el 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

Nota: De forma predeterminada, un archivo de imagen XVA basado en la versión 9.3 de Citrix ADC está disponible en el dispositivo SDX.

En el panel **Archivos XVA de Citrix ADC**, 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 de archivo NSVPX-XEN-9.3-25_nc.xva hace referencia a la versión 9.3 build 25.

- **Última modificación**

  Fecha en la 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 Citrix ADC

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

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

1. En el panel **Archivos de compilación de Citrix ADC**, seleccione el archivo que desea 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 desea guardar el archivo y, a continuación, haga clic en **Guardar**.

Agregar una instancia de Citrix ADC

Al agregar instancias de Citrix ADC desde Management Service, debe proporcionar valores para algunos parámetros y Management Service configura implícitamente esta configuración en las instancias de Citrix ADC.

- **Nombre ***: Asigne un nombre a la instancia de Citrix ADC.
- Compruebe **Administrar a través de la red interna** para habilitar una conectividad interna independiente siempre activa entre SDX Management Service y la instancia VPX.
- Seleccione una dirección IPv4 o IPv6 o ambas direcciones IPv4 e IPv6 para acceder a la instancia de Citrix VPX con fines de administración. Una instancia de Citrix ADC solo puede tener una IP de administración (también denominada NSIP). No puede quitar una dirección NSIP.
- Asigne una máscara de red, una puerta de enlace predeterminada y un nexthop a Management Service para la dirección IP.

A continuación, agregue el archivo XVA, el perfil de administración 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 Citrix ADC VPX en diferentes dispositivos SDX. Asegúrese de que las instancias de la configuración tienen 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 Citrix ADC. La licencia puede ser Standard, Enterprise y Platinum o Secure Web Gateway.

Nota: ***** indica los campos obligatorios.

> **Nota**
>
> Debe comprar una licencia independiente (SDX 2-Instance Add-On Pack for Secure Web Gateway) para instancias de Citrix Secure Web Gateway (SWG) en dispositivos SDX. Este paquete de instancias es diferente de la licencia de plataforma SDX o del paquete de instancias SDX.

> Para obtener más información acerca de la implementación de una instancia de Citrix SWG en un dispositivo SDX, consulteImplementación de una instancia de Citrix Secure Web Gateway en un dispositivo SDX.

Si necesita capacidad de fragmentación de ancho de banda, seleccione **Flexible** en **Modo de asignación**. Para obtener más información, consulteMedición de ancho de banda en SDX

Asignación de criptografía

A partir de la versión 12.1 48.13, la interfaz para administrar la capacidad de cifrado ha cambiado. Para obtener más información, consulteAdministrar la capacidad de cifrado

Asignación de recursos

En asignación de recursos, asigne memoria total, paquetes por segundo y CPU.

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

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

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

En la siguiente tabla se enumeran las versiones VPX admitidas, Single bungle image y el número de núcleos que puede asignar a una instancia:

Nombre de plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una sola 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 plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una sola 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	10
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S y SDX 14100 40S	12	10	10

Nombre de plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una sola instancia
SDX 25100A, 25160A, 25200A	20	18	9
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	26
15000-50G	16	14	14

> Nota: En la plataforma SDX 26xxx, se puede asignar un máximo de 26 núcleos de CPU a una instancia VPX. Sin embargo, si se asignan unidades criptográficas a la instancia, el número máximo de núcleos depende del número de unidades criptográficas e interfaces de datos. Por ejemplo, si asigna 24000 unidades criptográficas a una instancia, puede asignar 24 núcleos de CPU y un máximo de dos interfaces de datos a la instancia. El dispositivo SDX considera las interfaces de datos y las unidades criptográficas como dispositivos PCI. Con 26000 unidades criptográficas, no se puede aprovisionar una instancia VPX ya que no hay espacio para interfaces de datos.

Administración de instancias

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

Añádase los siguientes detalles:

Nombre de usuario: nombre de usuario del administrador de instancias de Citrix ADC. 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 Shell/Sftp/Spp: acceso permitido al administrador de instancias de Citrix ADC. Esta opción está seleccionada de forma predeterminada.

Configuración de red

- Permitir modo L2 en la configuración de red

Puede permitir el modo L2 en la instancia de Citrix ADC. Seleccione **Permitir 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 Citrix ADC.

Nota: Si inhabilita el modo L2 para una instancia desde Management Service, debe iniciar sesión en la instancia e inhabilitar el modo L2 desde esa instancia. Si no lo hace, es posible que todos los demás modos de Citrix ADC se inhabiliten después de reiniciar la instancia

Por defecto, se seleccionan las interfaces 0/1 y 0/2 para la administración LA.

Etiqueta de VLAN: especifique un ID de VLAN para la interfaz de administración.

A continuación, agregue interfaces de datos.

Nota: Los identificadores de interfaz de las interfaces que se agregan a una instancia no se corresponden necesariamente con la numeración de la interfaz física del dispositivo SDX. Por ejemplo, si la primera interfaz que asocia con la instancia 1 es la interfaz SDX 1/4, aparece como interfaz 1/1 al iniciar sesión en la instancia y ver la configuración de la interfaz, ya que es la primera interfaz que ha asociado a la instancia 1.

- VLAN permitidas: Especifique una lista de identificadores de VLAN que se pueden asociar a una instancia de Citrix ADC.
- Modo de dirección MAC: Asigne una dirección MAC. Seleccione una de las siguientes opciones:
  - Predeterminado: XenServer asigna una dirección MAC.
  - Personalizado: Seleccione este modo para especificar una dirección MAC que invalide la dirección MAC generada.
  - Generado: Generar una dirección MAC mediante la dirección MAC base establecida anteriormente. Para obtener información sobre la configuración de una dirección MAC base, consulte Asignación de una dirección MAC a una interfaz.
- Configuración de VMAC (VRID IPv4 e IPv6 para configurar Virtual MAC)
  - VRID IPv4: El VRID IPv4 que identifica el VMAC. Valores posibles: 1 — 255. Para obtener más información, consulte Configurar las VMC en una interfaz.
  - VRID IPV6: El VRID IPv6 que identifica el VMAC. Valores posibles: 1 — 255. Para obtener más información, consulte Configurar las VMC en una interfaz.

Configuración de la 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 Management Service y la instancia están en subredes diferentes, debe especificar un ID de VLAN en el momento de aprovisionar una instancia VPX, de modo que se pueda acceder a la instancia a través de la red cuando se inicie. Si su implementación requiere que el NSIP no sea accesible a través de ninguna interfaz distinta de la seleccionada en el momento de aprovisionar la instancia VPX, seleccione la opción NSVLAN.

Citrix recomienda no seleccionar **NSVLAN**. No puede cambiar esta configuración después de haber aprovisionado la instancia de Citrix ADC.

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, ejecutar el comando “clear config full” en la instancia VPX elimina la configuración de VLAN.

Haga clic en **Listo** para aprovisionar el dispositivo Citrix ADC VPX.

Modificar una instancia de Citrix ADC

Para modificar los valores de los parámetros de una instancia de Citrix ADC aprovisionada, en el panel de instancias de Citrix ADC, seleccione la instancia que desea modificar y, a continuación, haga clic en **Modificar**. En el Asistente para modificar ADC, modifique los parámetros.

Nota: Si modifica los siguientes parámetros:
número de chips SSL, interfaces, memoria y licencia de función, la instancia de Citrix ADC se detiene y se reinicia implícitamente para que estos parámetros entren en vigor.

No se pueden modificar los parámetros Imagen y Nombre de usuario.

Si quiere quitar una instancia de Citrix ADC aprovisionada en el dispositivo SDX, en el panel **Instancias de Citrix ADC**, seleccione la instancia que quiere quitar y, a continuación, haga clic en **Eliminar**. En el cuadro **Confirmar** mensaje, haga clic en **Sí** para quitar la instancia de Citrix ADC.

Restringir las VLAN a interfaces virtuales específicas

El administrador del dispositivo SDX puede aplicar VLAN 802.1Q específicas en las interfaces virtuales asociadas a instancias de Citrix ADC. Esta capacidad es especialmente útil para restringir el uso de VLAN 802.1Q por parte de los administradores de instancias. Si dos instancias pertenecientes a dos compañías diferentes están alojadas en un dispositivo SDX, puede restringir que las dos compañías utilicen el mismo ID de VLAN, de modo que una compañía no vea el tráfico de la otra compañía. Si un administrador de instancias, al aprovisionar o modificar una instancia VPX, intenta asignar una interfaz a una VLAN 802.1Q, se realiza una validación para verificar que el ID de VLAN especificado forma parte de la lista permitida.

De forma predeterminada, cualquier ID de VLAN se puede usar en una interfaz. Para restringir las VLAN etiquetadas en una interfaz, especifique los ID de VLAN en Configuración de red en el momento de aprovisionar una instancia de Citrix ADC, o posteriormente modificándola. Para especificar un rango, separe los ID con un guión (por ejemplo, 10 — 12). Si inicialmente especifica algunos ID de VLAN pero posteriormente los elimina todos de la lista permitida, 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 de Management Service.

Importante: Si el modo L2 está habilitado, el administrador debe tener cuidado de que los ID de VLAN en distintas instancias de Citrix ADC no se superpongan.

Para especificar los ID de VLAN permitidos

1. En el Asistente para aprovisionar ADC o Asistente para modificar ADC, en la página Configuración de red, en el cuadro de texto **VLAN permitidas**, especifique uno o más Id. de VLAN permitidos en esta interfaz. Utilice un guión para especificar un rango. Por ejemplo, 2 — 4094.
2. Siga las instrucciones del asistente.
3. Haga clic en **Finalizar** y, a continuación, haga clic en **Cerrar**.

Para configurar VLAN para una instancia desde Management Service

1. En la ficha **Configuración**, vaya a Citrix ADC > 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 Citrix ADC**, especifique los siguientes parámetros:
    - ID de VLAN: un entero que identifica de forma exclusiva la VLAN a la que pertenece una trama determinada. Citrix ADC admite un máximo de 4094 VLAN. ID 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, debe iniciar sesión en la instancia y configurar los protocolos de enrutamiento dinámico IPv6 desde la línea de comandos VTYSH.
5. Seleccione las interfaces que deben formar parte de la VLAN.
6. Haga clic en **Crear** y, a continuación, haga clic en **Cerrar**.

Administrar la capacidad de cifrado

June 19, 2019

A partir de la versión 12.1 48.13, la interfaz para administrar la capacidad de cifrado ha cambiado. Con la nueva interfaz, Management Service proporciona unidades criptográficas asimétricas (ACU), unidades criptográficas simétricas (SCU) e interfaces virtuales criptográficas para representar la capacidad SSL en el dispositivo Citrix ADC SDX. La capacidad criptográfica anterior se asignó en unidades de chips SSL, núcleos SSL y funciones virtuales SSL. Consulte laTablas de conversión de chips SSL heredados a ACU y SCUpara obtener más información acerca de cómo los chips SSL heredados se traducen en unidades ACU y SCU.

Mediante la GUI de Management Service, puede asignar capacidad de cifrado a la instancia de Citrix ADC VPX en unidades de ACU y SCU.

La siguiente tabla proporciona descripciones breves sobre las instancias virtuales de cifrado, SCU e unidades virtuales de cifrado.

Cuadro. Unidades criptográficas de unidades

Nuevas unidades criptográficas	Descripción
Unidad criptográfica asimétrica (ACU)	1 ACU = 1 operación por segundo (operaciones) de descifrado (RSA) 2 K (tamaño de clave de 2048 bits). Para obtener más detalles, consulte Tabla de conversión de recursos ACU a PKE.
Unidad criptográfica simétrica (SCU)	1 SCU = 1 Mbps de AES-128-CBC + SHA256-HMAC @ 1024B. Esta definición es aplicable 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 no se puede asignar más a una instancia VPX. Las interfaces virtuales criptográficas son entidades de solo lectura y el dispositivo SDX asigna automáticamente estas entidades.

Ver la capacidad de cifrado del dispositivo SDX

Puede ver la capacidad de cifrado del dispositivo SDX en el panel de control de la GUI de SDX. El panel muestra las interfaces virtuales, SCU y usadas y disponibles en el dispositivo SDX. Para ver la capacidad de cifrado, vaya a **Panel > Capacidad de cifrado**.

Asigne capacidad criptográfica al aprovisionar la instancia VPX

Al aprovisionar una instancia VPX en el dispositivo SDX, en **Asignación de cifrado**, puede asignar el número de unidades de unidad y SCU para la instancia de VPX. Para obtener instrucciones para aprovisionar una instancia VPX, consulteAprovisionar instancias de Citrix ADC.

Para asignar capacidad de cifrado mientras se aprovisionan una instancia VPX, siga estos pasos.

1. Inicie sesión en Management Service.
2. Vaya a **Configuración > Citrix ADC > Instancias**y haga clic en **Agregar**.
3. En **Asignación de cifrado**, puede ver las interfaces virtuales de cifrado, SCU y ACU disponibles. La forma de asignar ACU y SCU difiere según el dispositivo SDX:

   a. Para los dispositivos enumerados enValor mínimo de un contador ACU disponible para diferentes mesas de dispositivos SDX, puede asignar ACs 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 ACU posterior es 8750, 13125, etc.

Ejemplo. Asignación de criptografía donde las SCU se asignan automáticamente y las CAU se asignan en múltiplos de un número especificado.

Valor mínimo de un contador ACU disponible para diferentes mesas de 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 las plataformas SDX, que no figuran en la lista anteriorValor mínimo de un contador ACU disponible para diferentes mesas de dispositivos SDX, puede asignar libremente ACU y SCU. El dispositivo SDX asigna automáticamente interfaces virtuales criptográficas.

Ejemplo. Asignación criptográfica donde tanto ACU como SCU se asignan libremente

4. / Complete todos los pasos para aprovisionar la instancia de VPX y haga clic en **Listo**. Para obtener más información, consulte Aprovisionar instancias de Citrix ADC.

Ver el estado del hardware de cifrado

En Management Service, puede ver el estado del hardware criptográfico proporcionado con el dispositivo SDX. El estado del hardware criptográfico se representa como dispositivos criptográficos y funciones virtuales de cifrado. Para ver el estado del hardware criptográfico, vaya a **Panel > Recursos**.

Puntos a tener en cuenta

Tenga en cuenta los siguientes puntos 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 criptografía sigue siendo el mismo, y solo cambia la representación en SDX GUI.
- 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.
- Al actualizar el 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
14xxx, 14xxx 40G, 25xxx, 25xxx A	4375	25000	4375	625	512	381

Plataforma SDX	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
14xxx FIPS	4375	25000	4375	625	512	381
14xxx 40S	4375	25000	4375	625	512	381
*89xx (8910, 8920, 8930)	1000	4615	1000	136	397	4949
* 26xxx (26100, 26160, 26200 y 26250)	1000	4615	1000	136	397	4949
*15000 50G	1000	4615	1000	136	397	4949

* En estas plataformas los números de PKE son 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:

- Management Service ayuda a asignar Crypto Resources a cada VPX individual. Management Service no puede asignar ni prometer rendimiento.
- El rendimiento real varía según el tamaño del paquete, Cipher/Keyex/HMac (o sus variaciones) utilizados, etc.

El siguiente ejemplo le ayuda a comprender cómo leer y aplicar la ACU a la tabla de conversión de recursos PKE.

Ejemplo. Conversión de recursos ACU a PKE para la plataforma SDX 22040

La asignación de 2187 ACU a una instancia VPX en una plataforma SDX 22040 asigna un recurso criptográfico equivalente a 256 operaciones ECDHE-RSA o 2187 operaciones RSA-2K y así sucesivamente.

Tablas de conversión de chips SSL heredados a ACU y SCU

Para obtener más información acerca de cómo los chips SSL heredados se convierten a ACU y SCU, consulte la tabla siguiente.

Tabla de conversión ACU y SCU

Aprovisionar máquinas virtuales de terceros

June 19, 2019

El dispositivo SDX admite el aprovisionamiento de las siguientes máquinas virtuales (instancias) de terceros:

- SECUREMATRIX GSB
- InterScan Web Security
- Protector de Websense
- BlueCat DNS/DHCP Server
- CA Access Gateway
- VM-Series de Palo Alto

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. VM-Series de Palo Alto en Citrix SDX permite la consolidación de capacidades avanzadas de seguridad y ADC en una única plataforma, para un acceso seguro y confiable a las aplicaciones por parte de empresas, unidades de negocio y clientes de proveedores de servicios. La combinación de VM-Series en Citrix SDX también proporciona una solución completa, validada, de seguridad y ADC para implementaciones de Citrix XenApp y XenDesktop.

Puede aprovisionar, supervisar, administrar y solucionar problemas de una instancia desde Management Service. Todas las instancias anteriores de terceros utilizan el daemon SDXTools para comunicarse con Management Service. El demonio está preinstalado en la instancia aprovisionada. Puede actualizar el daemon cuando estén disponibles nuevas versiones.

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 porque los canales no son compatibles con 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 XenServer a la versión 6.1.0 antes de instalar cualquier instancia de terceros.

SECUREMATRIX GSB

June 19, 2019

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 SECUREMATRIX GSB con servidor de autenticación SECUREMATRIX mejora sustancialmente la seguridad de los puntos finales VPN/SSL-VPN, aplicaciones y recursos basados en la nube, inicio de sesión de escritorio/escritorio virtual y aplicaciones web (proxy inverso con OTP), proporcionando una solución compatible con PCs, escritorios virtuales, tabletas y teléfonos inteligentes.

Mediante el uso de la arquitectura de plataforma multiarrendatario de Citrix ADC SDX en una red definida por software (SDN), la función de autenticación segura de SECUREMATRIX se puede combinar o integrar fácilmente con otros arrendatarios o servicios en la nube proporcionados a través de Citrix ADC, como Web Interface, XenApp, XenDesktop y muchos otros que requieren autenticación.

Nota:
Las interfacesSR-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 SECUREMATRIX GSB.

Para obtener más información, consulte MATRIZ DE SEGURIDAD.

Aprovisionamiento de una instancia de SECUREMATRIX GSB

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 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 porque los canales no son compatibles con una instancia SECUREMATRIX GSB.

Debe descargar una imagen XVA del sitio web de SECUREMATRIX y cargarla 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 Management Service build 118.7 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 desea cargar.

3. Haz clic en Subir. 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 Aprovisionar SECUREMATRX GSB, siga las instrucciones que aparecen en pantalla.
4. Haga clic en Finalizar y, a continuación, haga clic en Cerrar.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice una configuración detallada. Para obtener más información, consulte elMATRIZ DE SEGURIDADsitio web.

Para modificar los valores de los parámetros de una instancia de SECUREMATRIX aprovisionada, en el panel Instancias de SECUREMATRIX, seleccione la instancia que desea modificar y, a continuación, haga clic en Modificar. En el asistente Modificar SECUREMATRIX GSB, modifique los parámetros.

Nota: Si modifica cualquiera de los parámetros de interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para poner en efecto los cambios.

Puede generar un archivo tar para enviarlo al soporte técnico. Para obtener información sobre cómo generar un archivo de soporte técnico, consulteGeneración de un archivo TAR para asistencia técnica.

También puede realizar una copia de seguridad de la configuración de una instancia SECUREMATRIX GSB y, posteriormente, utilizar 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, consulteCopia de seguridad y restauración de los datos de configuración del dispositivo SDX.

Supervisión de una instancia de SECUREMATRIX GSB

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 SECUREMATRIX GSB.

Para ver las estadísticas relacionadas con una instancia de SECUREMATRIX GSB:

1. Vaya a SECUREMATRIX GSB > Instancias.
2. En el panel de detalles, haga clic en la flecha situada junto al nombre de la instancia.

Administración de una instancia de SECUREMATRIX GSB

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de SECUREMATRIX GSB desde Management Service.

En la ficha Configuración, expanda SECUREMATRIX GSB.

Para iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una entrada:

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia en la que desea realizar la operación y, a continuación, seleccione una de las siguientes opciones:
   - Empezad
   - Apagar
   - Reinicie
   - Forzar apagado
   - Forzar reinicio
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Actualización del archivo SDXTools para una instancia SECUREMATRIX GSB

SDXTools, un demonio que se ejecuta en la instancia SECUREMATRIX GSB, 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 al dispositivo SDX.

Para cargar un archivo SDXTools:

1. En el panel de navegación, expanda Management Service y, a continuación, haga clic en Archivos SDXTools.
2. En el panel de detalles, en la lista Acción, seleccione Cargar.
3. En el cuadro de diálogo Cargar archivos SDXTools, haga clic en Examinar, vaya a la carpeta que contiene el archivo y, a continuación, haga doble clic en el archivo.
4. Haz clic en Subir.

Para actualizar SDXTools:

En la ficha Configuración, expanda SECUREMATRIX GSB.

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione una instancia.
3. En la lista Acción, 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.

Actualización y degradación de la instancia de SECUREMATRIX GSB a una versión posterior

El proceso de actualización de la instancia SECUREMATRIX GSB implica cargar la imagen de software de la compilación de destino en el dispositivo SDX y, a continuación, actualizar la instancia. La

degradación 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. Haz clic en Subir.

Para actualizar la instancia:

1. Haga clic 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. Haga clic en Instancias.
2. En el panel de detalles, seleccione una instancia.
3. En la lista Acción, seleccione Rebajar de categoría.
4. En el cuadro Confirmar mensaje, haga clic en Sí.

Solución de problemas de una instancia de SECUREMATRIX GSB

Puede hacer ping a una instancia de SECUREMATRIX GSB desde Management Service para comprobar si el dispositivo es accesible. Puede realizar un seguimiento de la ruta de un paquete desde Management Service a una instancia para determinar el número de saltos implicados en llegar a la instancia.

Puede redescubrir 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 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. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia a la que desea hacer ping y, en la lista Acción, haga clic en Ping. El cuadro Pingmessage muestra si el ping es correcto.

Para rastrear la ruta de una instancia:

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia para la que desea realizar un seguimiento de la ruta y, en la lista Acción, haga clic en TraceRoute. El cuadro de mensaje Traceroute muestra la ruta a la instancia.

Para redescubrir una instancia:

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia que desea redescubrir y, en la lista Acción, haga clic en Redescubrir.
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Trend Micro InterScan Web Security

June 19, 2019

Trend Micro InterScan Web Security es un dispositivo virtual de software que protege dinámicamente contra amenazas web tradicionales y emergentes en la puerta de enlace de Internet. Al integrar el control de aplicaciones, el análisis antimalware, la reputación web en tiempo real, el filtrado flexible de URL y la protección avanzada contra amenazas, ofrece una protección superior y una mayor visibilidad y control sobre el creciente uso de aplicaciones basadas en la nube en la red. La generación de informes en tiempo real y la gestión centralizada proporcionan a sus administradores una herramienta proactiva de toma de decisiones, lo que permite la gestión de riesgos in situ.

InterScan Web Security:

- Permite una mayor visibilidad de la actividad de Internet del usuario final
- Centraliza la gestión para el máximo control
- Supervisa el uso de la web mientras sucede
- Permite la corrección in situ
- Reduce la expansión del dispositivo y los costes de energía
- Proporciona protección opcional contra pérdida de datos y análisis de ejecución del entorno aislado

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 Citrix ADC SDX.

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 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 desea cargar.
4. Haz clic en Subir. El archivo XVA aparece en el panel Archivos XVA.

Para aprovisionar una instancia de TrendMicro IWSVA:

1. En la ficha Configuración, vaya a TrendMicro IWSVA > Instancias.
2. En el panel de detalles, haga clic en Agregar.
3. En el asistente Aprovisionar TrendMicro IWSVA, siga las instrucciones que aparecen en pantalla.
4. Haga clic en Aceptar y, a continuación, haga clic 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 desea modificar y, a continuación, haga clic en Editar. En el asistente Modificar TrendMicro IWSVA, establezca los parámetros en valores adecuados para su entorno.

Protector de Websense

June 19, 2019

El protector de Websense (ahora conocido como Forcepoint) Data Security es una máquina virtual que intercepta el tráfico HTTP saliente (publicaciones) y lo analiza para evitar la pérdida de datos y fugas de información confidencial en la web. El protector se comunica con un servidor Windows dedicado para información de directivas DLP y puede supervisar o bloquear datos para que no se publiquen cuando se detecta una coincidencia. El análisis de contenido se realiza en la caja, por lo que ningún dato sensible deja el protector durante este proceso.

Para utilizar las capacidades de prevención de pérdida de datos (DLP) del protector, debe adquirir e instalar Websense Data Security, configurar directivas de DLP Web en el administrador de seguridad de datos y realizar la configuración inicial a través de Management Service.

Para obtener más información, consulte elProtector de Websensesitio web.

Aprovisionar una instancia del protector de Websense

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 servirá a 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 porque los canales no son compatibles con una instancia del protector de Websense.

Debe descargar una imagen del protector del sitio web de Websense y cargarla en el dispositivo SDX antes de comenzar a aprovisionar la instancia. Para obtener más información acerca de la descarga de una imagen protectora, consulte laSitio web de Websense. Asegúrese de que está utilizando Management Service build 118.7 o posterior en el dispositivo SDX.

En la ficha Configuración, vaya a Protector de Websense > 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 desea cargar.
3. Haz clic en Subir. El archivo XVA aparece en el panel Archivos XVA.

Para aprovisionar una instancia del protector de Websense

1. En la ficha Configuración, vaya a Protector de Websense > Instancias.
2. En el panel de detalles, haga clic en Agregar.
3. En el asistente Aprovisionar protector de Websense, siga las instrucciones que aparecen en pantalla.
4. Haga clic en Finalizar y, a continuación, haga clic en Cerrar.

Después de aprovisionar la instancia, inicie sesión en la instancia y realice una configuración detallada.

Para modificar los valores de los parámetros de una instancia aprovisionada del protector de Websense, en el panel Instancias del protector de Websense, seleccione la instancia que quiera 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 no se puede cambiar a menos que elimine la instancia y aprovisione una nueva.

Puede generar un archivo tar para enviarlo al soporte técnico. Para obtener información sobre cómo generar un archivo de soporte técnico, consulteGeneración de un archivo TAR para asistencia técnica.

Supervisar una instancia del protector de Websense

El dispositivo SDX recopila estadísticas, como la versión de SDXTools, el estado del motor de directivas de Websense© Data Security y el estado del proxy de seguridad de datos, de una instancia del protector de Websense.

Para ver las estadísticas relacionadas con una instancia del protector de Websense:

1. Vaya a Protector de Websense > Instancias.
2. En el panel de detalles, haga clic en la flecha situada junto al nombre de la instancia.

Administrar una instancia del protector de Websense

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia del protector de Websense© desde Management Service.

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. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia en la que desea realizar la operación y, a continuación, seleccione una de las siguientes opciones:
   - Empezad
   - Apagar
   - Reinicie
   - Forzar apagado
   - Forzar reinicio
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Actualizar el archivo SDXTools para una instancia del protector de Websense

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 al dispositivo SDX.

Para cargar un archivo SDXTools

1. En el panel de navegación, expanda Management Service y, a continuación, haga clic en Archivos SDXTools.
2. En el panel de detalles, en la lista Acción, seleccione Cargar.
3. En el cuadro de diálogo Cargar archivos SDXTools, haga clic en Examinar, vaya a la carpeta que contiene el archivo y, a continuación, haga doble clic en el archivo.
4. Haz clic en Subir.

Para actualizar SDXTools

En la ficha
Configuración, expanda
Protector de Websense.

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione una instancia.
3. En la lista Acción, 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 del protector de Websense 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 de 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. Haz clic en Subir.

Para actualizar la instancia

1. Haga clic 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.

Solucionar problemas de una instancia del protector de Websense

Puede hacer ping a una instancia del protector de Websense© desde Management Service para comprobar si el dispositivo es accesible. Puede realizar un seguimiento de la ruta de un paquete desde Management Service a una instancia para determinar el número de saltos implicados en llegar a la instancia.

Puede redescubrir 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. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia a la que desea hacer ping y, en la lista Acción, haga clic en Ping. El cuadro Pingmessage muestra si el ping es correcto.

Para rastrear la ruta de una instancia

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia para la que desea realizar un seguimiento de la ruta y, en la lista Acción, haga clic en TraceRoute. El cuadro de mensaje Traceroute muestra la ruta a la instancia.

Para redescubrir una instancia

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia que desea redescubrir y, en la lista Acción, haga clic en Redescubrir.
3. En el cuadro Confirmar mensaje, haga clic en Sí.

BlueCat DNS/DHCP

June 19, 2019

BlueCat DNS/DHCP Server™ es una solución de software que se puede alojar en la plataforma Citrix SDX para ofrecer servicios de red central DNS y DHCP fiables, escalables y seguros sin necesidad de costes de administración adicionales ni de espacio en el centro de datos. Los servicios DNS críticos se pueden equilibrar la carga en varios nodos DNS dentro de un único sistema o en varios dispositivos SDX sin necesidad de hardware adicional.

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/.

Aprovisionar una instancia de BlueCat DNS/DHCP

Debe descargar una imagen XVA desde el 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 comenzar a aprovisionar la instancia. Asegúrese de que está utilizando Management Service build 118.7 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, consulteConfiguración del canal desde Management Service.

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 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 desea cargar.
3. Haz clic en Subir. 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, escriba 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 desea, 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 se va a administrar la instancia y establezca la dirección IP y la puerta de enlace para esa interfaz. Puede asignar interfaces explícitamente para alta disponibilidad y servicio. Seleccione los parámetros y, a continuación, 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 los tres.
Puede seleccionar una interfaz diferente para los tres.
Puede seleccionar la misma interfaz para administración y servicio, pero seleccionar una interfaz diferente para alta disponibilidad.
Haga clic en Finalizar y, a continuación, haga clic en Cerrar. La instancia se creará, se iniciará y se configurará 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 cómo configurar BlueCat DNS/DHCP Server o colocarlo bajo el control de BlueCat Address Manager, consulte la guía de administración de BlueCat adecuada, disponible en https://care.bluecatnetworks.com.

Para modificar los valores de los parámetros de una instancia de BlueCat DNS/DHCP Server aprovisionada, en el panel Instancias de BlueCat DNS/DHCP, seleccione la instancia que quiera modificar y, a continuación, haga clic en Modificar. En el asistente Modificar BlueCat DNS/DHCP, modifique los parámetros.

Nota: Si modifica cualquiera de los parámetros de interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para poner en efecto los cambios.

Supervisar una instancia de BlueCat DNS/DHCP

El dispositivo SDX recopila estadísticas, como la versión de SDXTools que se ejecuta 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 situada junto al nombre de la instancia.

Administrar una instancia de BlueCat DNS/DHCP

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de BlueCat DNS/DHCP desde Management Service.

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. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia en la que desea realizar la operación y, a continuación, seleccione una de las siguientes opciones:
   - Empezad
   - Apagar
   - Reinicie
   - Forzar apagado
   - Forzar reinicio
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Actualizar el archivo SDXTools para una instancia de BlueCat DNS/DHCP

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 al dispositivo SDX.

Para cargar un archivo SDXTools:

1. En el panel de navegación, expanda Management Service y, a continuación, haga clic en Archivos SDXTools.
2. En el panel de detalles, en la lista Acción, seleccione Cargar.
3. En el cuadro de diálogo Cargar archivos SDXTools, haga clic en Examinar, vaya a la carpeta que contiene el archivo y, a continuación, haga doble clic en el archivo.
4. Haz clic en Subir.

Para actualizar SDXTools:

En la ficha Configuración, expanda BlueCat DNS/DHCP.

1. Haga clic en Instancias.
2. En el panel de detalles, seleccione una instancia.
3. En la lista Acción, 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.

Redescubrir una instancia de BlueCat DNS/DHCP

Puede redescubrir 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. Haga clic en Instancias.
2. En el panel de detalles, seleccione la instancia que desea redescubrir y, en la lista Acción, haga clic en Redescubrir.
3. En el cuadro Confirmar mensaje, haga clic en Sí.

CA Access Gateway

June 19, 2019

CA Access Gateway es un servidor independiente escalable, manejable y extensible 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 dependen de la tecnología tradicional basada en cookies.

El agente web integrado permite el inicio de sesión único (SSO) en toda una empresa. CA Access Gateway proporciona control de acceso para solicitudes HTTP y HTTPS y SSO sin cookies. Además, el producto almacena información de sesión en el almacén de sesiones en memoria. Las reglas de proxy definen la forma en que CA Access Gateway reenvía o redirige las solicitudes a los recursos ubicados en los servidores de destino de la empresa.

Al proporcionar una única puerta de enlace 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 son compatibles con una instancia de CA Access Gateway. Para obtener más información acerca de las funciones de CA Access Gateway, consulte la documentación del producto en su wiki

Aprovisionar una instancia de CA Access Gateway

Antes de poder aprovisionar una instancia de CA Access Gateway, debe descargar una imagen XVA. Una vez descargada la imagen XVA, cárguela en el dispositivo SDX. Asegúrese de que está utilizando

la versión 10.5, compilación 52.3.e de Management Service 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 desea cargar.
4. Haz clic en **Subir**. 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, haga clic 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 desea 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 interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para poner en efecto el cambio.

Supervisar una instancia de CA Access Gateway

El dispositivo SDX recopila estadísticas, como la versión de SDXTools que se ejecuta en la instancia, de una instancia de CA Access Gateway.

Para ver las estadísticas relacionadas con una instancia de CA Access Gateway:

1. Acceda a CA Access Gateway > Instancias.
2. En el panel de detalles, haga clic en la flecha situada 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 Management Service. Para completar estas tareas, siga estos pasos:

1. En la ficha Configuración, expanda CA Access Gateway.
2. Acceda a CA Access Gateway > Instancias.

3. En el panel de detalles, seleccione la instancia en la que desea realizar la operación y, a continuación, seleccione una de las siguientes opciones:
    - Empezad
    - Apagar
    - Reinicie
    - Forzar apagado
    - Forzar reinicio
4. En el cuadro Confirmar mensaje, haga clic en Sí.

VM-Series de Palo Alto Networks

June 19, 2019

Nota:
El aprovisionamiento de instancias de VM-Series de Palo Alto en un dispositivo Citrix ADC SDX solo se admite en la versión 10.1.e de Citrix ADC.

Los firewalls virtuales de VM-Series de Palo Alto Networks utilizan el mismo conjunto de características PAN-OS que está disponible en los dispositivos de seguridad física de la empresa, proporcionando todas las funciones clave de seguridad de red. VM-Series en Citrix SDX permite la consolidación de capacidades avanzadas de seguridad y ADC en una única plataforma, para un acceso seguro y confiable a las aplicaciones por parte de empresas, unidades de negocio y clientes de proveedores de servicios. La combinación de VM-Series en Citrix SDX también proporciona una solución completa, validada, de seguridad y ADC para implementaciones de Citrix XenApp y XenDesktop.

Puede aprovisionar, supervisar, administrar y solucionar problemas de una instancia desde Management Service.

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.
- Debe actualizar la versión de XenServer a la versión 6.1.0 e instalar el paquete complementario xs-netscaler-6.1.0-2.6.32.43 -0.4.1.xs1.6.10.777.170770-100012.
- 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 del protector de Websense. Para obtener más información acerca de VM-Series de Palo Alto Networks, consulte [[Documentación de la red de Palo Alto.

Aprovisionamiento de una instancia de VM-Series de Palo Alto

Antes de poder aprovisionar una instancia de VM-Series de Palo Alto, debe descargar una imagen XVA desde el sitio web de Palo Alto Networks. Una vez descargada la imagen XVA, cárguela en el dispositivo SDX. Asegúrese de que está utilizando Management Service versión 10.1 build 120.130403.e o posterior en el dispositivo SDX.

Para cargar una imagen XVA en el dispositivo SDX:

1. En la ficha **Configuración**, vaya a **Palo Alto 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 desea cargar.
4. Haz clic en **Subir**. El archivo XVA aparece en el panel Archivos **XVA**.

Para aprovisionar una instancia de VM-Series de Palo Alto:

1. En la ficha **Configuración**, vaya a **Palo Alto VM-Series** > **Instancias**.
2. En el panel de detalles, haga clic en **Agregar**.
3. En el asistente Aprovisionar Palo Alto VM-Series, siga las instrucciones que aparecen en pantalla.
4. Haga clic en **Finalizar** y, a continuación, haga clic 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 desea modificar y, a continuación, haga clic en **Modificar**. En el asistente Modificar VM-Series de Palo Alto, defina los parámetros en valores adecuados para su entorno.

Nota:
Si modifica cualquiera de los parámetros de interfaz o el nombre de la instancia, la instancia se detiene y se reinicia para poner en efecto el cambio.

Supervisar una instancia de VM-Series Palo Alto

El dispositivo SDX recopila estadísticas, como la versión de SDXTools que se ejecuta en la instancia, de una instancia de VM-Series de Palo Alto.

Para ver las estadísticas relacionadas con una instancia de VM-Series de Palo Alto:

1. Vaya a Palo Alto VM-Series > Instancias.
2. En el panel de detalles, haga clic en la flecha situada junto al nombre de la instancia.

Administrar una instancia de VM-Series de Palo Alto

Puede iniciar, detener, reiniciar, forzar la detención o forzar el reinicio de una instancia de VM-Series de Palo Alto desde Management Service.

En la ficha Configuración, expanda Palo Alto VM-Series.

1. Vaya a Palo Alto VM-Series > Instancias.
2. En el panel de detalles, seleccione la instancia en la que desea realizar la operación y, a continuación, seleccione una de las siguientes opciones:
   - Empezad
   - Apagar
   - Reinicie
   - Forzar apagado
   - Forzar reinicio
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Solución de problemas de una instancia de VM-Series de Palo Alto

Puede hacer ping a una instancia de VM-Series de Palo Alto desde Management Service para comprobar si el dispositivo es accesible. Puede realizar un seguimiento de la ruta de un paquete desde Management Service a una instancia para determinar el número de saltos implicados en llegar a la instancia.

Puede redescubrir 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 Palo Alto 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 Palo Alto VM-Series.

Para hacer ping a una instancia:

1. Haga clic en **Instancias**.
2. En el panel de detalles, seleccione la instancia a la que desea hacer ping y, en la lista Acción, haga clic en Ping. El cuadro Pingmessage muestra si el ping es correcto.

Para realizar un seguimiento de la ruta de una instancia:

1. Haga clic en **Instancias**.
2. En el panel de detalles, seleccione la instancia a la que desea hacer ping y, en la lista Acción, haga clic en **TraceRoute**. El cuadro de mensaje **Traceroute** muestra la ruta a la instancia.

Para redescubrir una instancia:

1. Haga clic en **Instancias**.
2. En el panel de detalles, seleccione la instancia que desea redescubrir y, en la lista Acción, haga clic en **Redescubrir**.
3. En el cuadro Confirmar mensaje, haga clic en **Sí**.

Implementación de una instancia de Citrix Secure Web Gateway en un dispositivo SDX

June 19, 2019

La solución Secure Web Gateway (SWG) ofrece herramientas que las empresas pueden utilizar para proteger contra amenazas de Internet.

Desde la versión 12.0 56.20, puede implementar una instancia SWG SDX en un dispositivo SDX. Todos los modelos SDX admiten instancias SDX SWG. Para obtener más información, consulte Matriz de compatibilidad de hardware y software SDX.

La implementación de una instancia SWG SDX 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.
- Configuración y configuración de SDX Management Service. Para obtener más información, consulte Introducción a la interfaz de usuario de Management Service y Configurar Management Service.
- Aprovisionamiento de la instancia SWG SDX en el dispositivo SDX. Para obtener más información, consulte Aprovisionar instancias de Citrix ADC.
- Configuración de la instancia SWG SDX. Para obtener más información, consulte lasCitrix Secure Web Gatewaydocumentaciones.

Requisitos previos

- Instale un paquete de instancias exclusivo para SDX SWG. Este paquete de instancias es diferente de la licencia de plataforma SDX o del paquete de instancias SDX.

Puntos a tener en cuenta

Tenga en cuenta lo siguiente al aprovisionar una instancia SDX en un dispositivo SDX:

- La licencia de plataforma determina el rendimiento de la instancia SWG SDX.
- Puede aprovisionar la instancia SWG solo en uno o más núcleos de CPU dedicados.
- Utilice Citrix ADC XVA normal y las imágenes de actualización para aprovisionar y actualizar una instancia SDX SWG. Asegúrese de que la imagen admite la función SWG.
- Puede aprovisionar hasta dos instancias SWG con una licencia SDX 2 Instance Add-On Pack for Secure Web Gateway.

Limitaciones

- No se puede convertir una instancia de Citrix VPX ADC en una instancia SWG, y viceversa.
- No se puede configurar un clúster Citrix ADC de instancias SDX SWG.
- No se admite la conexión de una partición FIPS a una instancia SWG de SDX.
- No se admiten licencias agrupadas.

Medición de ancho de banda en SDX

June 19, 2019

La medición de ancho de banda Citrix ADC SDX le proporciona un esquema de medición preciso, confiable y fácil de usar que le permite asignar eficientemente la capacidad de procesamiento y rentabilizar 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 velocidad fija de rendimiento
- Ancho de banda dedicado con un rendimiento mínimo garantizado y flexibilidad de ancho de banda

Ancho de banda dedicado con una velocidad fija de rendimiento

En el método de asignación de ancho de banda, a cada instancia VPX se le asigna un ancho de banda dedicado. La instancia puede utilizar 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 que el asignado, entonces en el modo dedicado la instancia no puede aumentar su rendimiento. Esto 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 su ancho de banda asignado, entonces en modo dedicado no es posible compartir su ancho de banda no utilizado. Para superar todos estos desafíos, es útil un ancho de banda dedicado con una tasa mínima garantizada 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 un 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.

La ventaja de la capacidad de flexibilidad es que si algunas de las instancias VPX tienen capacidad adicional no utilizada, esa capacidad se puede asignar a otras instancias VPX que hayan utilizado completamente 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.

Selección del modo de asignación de ancho de banda

Antes de elegir el rendimiento flexible, debe habilitar la asignación dinámica de rendimiento de flexibilidad. Para habilitar esta opción, siga estos pasos.

1. Desde SDX Management Console, 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 **SDX Management Service**, haga clic en **Configuración > Citrix ADC > Instancias > Agregar**.
2. Se abrirá la página **Provisioning Citrix ADC**. En **Asignación de licencias**, elija **Flexible** en **Modo de asignación**.

Para obtener más información acerca de cómo aprovisionar una instancia de Citrix ADC, consulteAprovisionar instancias de Citrix ADC.

Si quiere utilizar una tasa de rendimiento fija, seleccione **Fijo**. De forma predeterminada, el modo fijo se establece 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 modo diferente.

Nota: Si va a migrar SDX desde la versión 10.5.e y la versión anterior, de forma predeterminada todas las instancias VPX se encuentran en el modo de asignación fija.

Determinar el ancho de banda flexible máximo para una instancia VPX

La medida en que se permite que cada VPX explote se calcula a través de 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. La siguiente tabla muestra los parámetros:

|Nombre VPX|Parámetro|Valor|
|–|–|–|
|VPX1|Ancho de banda mínimo garantizado|4 Gbps
|-|-|Ancho de banda máximo flexible|2 Gbps
|-|-|Prioridad|P0
|VPX2|Ancho de banda mínimo asegurado|2 Gbps
|-|-|Ancho de banda máximo flexible|1 Gbps
|-|-|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. VPX1 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 superior a 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 escenarios, se asegura de que siempre se respeta el ancho de banda mínimo garantizado.

Comprobación de las estadísticas de rendimiento y consumo de datos

Puede consultar las estadísticas individuales de rendimiento y consumo de datos de VPX en gráficos. Para acceder a los gráficos, siga estos pasos:

1. Desde SDX Management Service, vaya a la página **Configuración > Citrix ADC > 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 proporcionan para comprobar 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 situado 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.

La siguiente ilustración muestra un gráfico de muestra de datos de rendimiento durante 1 semana:

Configurar y administrar instancias de Citrix ADC

June 19, 2019

Una vez que haya aprovisionado instancias Citrix ADC en su dispositivo, estará listo para configurarlas y administrarlas. Comience creando una dirección IP de subred (SNIP) y, a continuación, guardando la configuración. A continuación, puede realizar tareas básicas de administración en las instancias. Compruebe si tiene que aplicar la configuración de administración.

Si una tarea que necesita realizar no se describe a continuación, consulte la lista de tareas a la izquierda.

Advertencia:

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

Creación de una dirección SNIP en una instancia de Citrix ADC

Puede asignar una dirección SNIP a las instancias de Citrix ADC después de que se haya aprovisionado en el dispositivo SDX.

Un SNIP se utiliza en la administración de conexiones y la supervisión del servidor. No es obligatorio especificar un SNIP al configurar inicialmente el dispositivo Citrix ADC SDX. Puede asignar SNIP a la instancia de Citrix ADC desde Management Service.

Para agregar una dirección SNIP en una instancia de Citrix ADC

1. En la ficha Configuración, en el panel de navegación, haga clic en Citrix ADC.
2. En el panel de detalles, en Configuración de Citrix ADC, haga clic en Crear IP.
3. En el cuadro de diálogo Crear IP de Citrix ADC, especifique los valores para 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: Especifique si la configuración debe guardarse en Citrix ADC. El valor predeterminado es false.
- Dirección IP de instancia: Especifique la dirección IP de la instancia de Citrix ADC.

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

Guardar la configuración

Puede guardar la configuración en ejecución de
una instancia de Citrix ADC desde Management Service.

Para guardar la configuración en una instancia de Citrix ADC

1. En la ficha Configuración, en el panel de navegación, haga clic en Citrix ADC.
2. En el panel de detalles, en Configuración de Citrix ADC, 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 Citrix ADC cuya configuración quiere guardar.
4. Haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Administración de una instancia de Citrix ADC

Management Service le permite realizar las siguientes operaciones en las instancias de Citrix ADC, tanto desde el panel de instancias de Citrix ADC de la ficha Configuración como en el gadget de instancias de Citrix ADC de la página de inicio.

Inicie una instancia de Citrix ADC:

Inicie cualquier instancia de Citrix ADC desde la interfaz de usuario de Management Service. Cuando la interfaz de usuario de Management Service reenvía esta solicitud a Management Service, inicia la instancia de Citrix ADC.

Cierre una instancia de Citrix ADC:

Cierre cualquier instancia de Citrix ADC desde la interfaz de usuario de Management Service. Cuando la interfaz de usuario de Management Service reenvía esta solicitud a Management Service, detiene la instancia de Citrix ADC.

Reinicie una instancia de Citrix ADC:

Reinicie la instancia de Citrix ADC.

Eliminar una instancia de Citrix ADC:

Si no quiere utilizar una instancia de Citrix ADC, puede eliminarla mediante Management Service. Al eliminar una instancia, se quita permanentemente la instancia y los detalles relacionados de la base de datos del dispositivo
SDX.

Para iniciar, detener, eliminar o reiniciar una instancia de Citrix ADC

1. En la ficha Configuración, en el panel de navegación, haga clic en Instancias de Citrix ADC.
2. En el panel de instancias de Citrix ADC, seleccione la instancia de Citrix ADC en la que quiere realizar la operación y, a continuación, haga clic en Inicio o Apagar o Eliminar o Reiniciar.
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Eliminación de archivos de instancia de Citrix ADC

Puede quitar del dispositivo cualquier archivo de instancia de Citrix ADC, como XVA, compilaciones, documentación, claves SSL o certificados SSL.

Para quitar archivos de instancia de Citrix ADC

1. En la ficha Configuración, en el panel de navegación, expanda Configuración de Citrix ADC 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.

Aplicación de la configuración de administración

En el momento de aprovisionar una instancia VPX, Management Service crea algunas directivas, el perfil de administración de instancias (admin) y otra configuración en la instancia de VPX. Si Management Service no puede aplicar la configuración de administrador en este momento debido a algún motivo (por ejemplo, Management Service y la instancia de VPX están en diferentes subredes y el enrutador está inactivo o si Management Service y la instancia de VPX están en la misma subred, pero el tráfico tiene que pasar por un conmutador externo y uno de los enlaces requeridos está inactivo), puede enviar explícitamente la configuración de administrador desde Management Service a la instancia de VPX en cualquier momento.

Para aplicar la configuración de administrador en una instancia de Citrix ADC

1. En la ficha Configuración, en el panel de navegación, haga clic en Citrix ADC.
2. En el panel de detalles, en Configuración de Citrix ADC, haga clic en Aplicar configuración de administrador.
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 administrador.
4. Haga clic en Aceptar.

Instalar y administrar certificados SSL

June 19, 2019

El proceso de instalación de certificados SSL implica cargar los archivos de certificado y clave en el dispositivo Citrix ADC SDX y, a continuación, instalar el certificado SSL en las instancias de Citrix ADC.

Carga del 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 correspondiente. El archivo de certificado debe estar presente en el dispositivo SDX cuando instale el certificado SSL en las instancias de Citrix ADC. También puede descargar los archivos de 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**

Fecha en la que se modificó por última vez el archivo de certificado.

- **Tamaño:**

El 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. Haz clic en Subir. El archivo de certificado aparece en el panel Certificados SSL.

Para crear una copia de seguridad descargando 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 correspondiente. El archivo de clave debe estar presente en el dispositivo SDX cuando instale el certificado SSL en las instancias de Citrix ADC. 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**

El nombre del archivo de claves.

- **Última modificación**

Fecha en la que se modificó por última vez el archivo de claves.

- **Tamaño:**

El tamaño del archivo de 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 claves aparece en el panel de claves SSL.

Para crear una copia de seguridad descargando 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 Citrix ADC

Management Service le permite instalar certificados SSL en una o más instancias de Citrix ADC. Antes de comenzar a instalar el certificado SSL, asegúrese de que ha cargado el certificado SSL y los archivos de clave en el dispositivo SDX.

Para instalar certificados SSL en una instancia de Citrix ADC

1. En el panel de navegación, haga clic en Citrix ADC.
2. En el panel de detalles, en Configuración de Citrix ADC, haga clic en Instalar certificados SSL.
3. En el cuadro de diálogo Instalar certificados SSL, especifique valores para los siguientes parámetros. (*) indica 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 Citrix ADC. Longitud máxima: 31
    - Formato de certificado: Especifique el formato del certificado SSL admitido en Citrix ADC. Un dispositivo Citrix ADC SDX admite los formatos PEM y DER para certificados SSL.
    - Contraseña: Especifique la frase de contraseña que se utilizó para cifrar la clave privada. Esta opción se puede utilizar para cargar claves privadas cifradas. Longitud máxima: 32. **Nota**: La clave privada protegida por contraseña solo es compatible con el formato PEM.
    - Guardar configuración: Especifique si la configuración debe guardarse en Citrix ADC. El valor predeterminado es false.
    - Dirección IP de instancia: Especifique las direcciones IP de las instancias de Citrix ADC en las que quiere instalar el certificado SSL.
4. Haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Actualizar un certificado SSL en una instancia de Citrix ADC

Puede actualizar algunos parámetros, como el archivo de certificado, el archivo de clave y el formato de certificado de un certificado SSL instalado en una instancia de Citrix ADC. No puede modificar la dirección IP y el nombre del certificado.

Para actualizar el certificado SSL en una instancia de Citrix ADC

1. En el panel de navegación, expanda Cirix ADC 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, establezca 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 Citrix ADC SDX. El dispositivo admite los formatos PEM y DER para certificados SSL.
- Contraseña: La frase de contraseña que se utilizó para cifrar la clave privada. Esta opción se puede utilizar para cargar claves privadas cifradas. Longitud máxima: 32 caracteres.

  Nota: La clave privada protegida por contraseña solo es compatible con 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, haga clic en Cerrar.

Sondeo de certificados SSL en las instancias de Citrix ADC

Si agrega un nuevo certificado SSL directamente en una instancia de Citrix ADC después de iniciar sesión en esa instancia, Management Service no conoce este nuevo certificado. Para evitar esto, especifique un intervalo de sondeo después del cual Management Service sondeará todas las instancias de Citrix ADC para comprobar si hay nuevos certificados SSL. También puede realizar una encuesta en cualquier momento desde Management Service si, por ejemplo, quiere obtener inmediatamente una lista de todos los certificados SSL de todas las instancias de Citrix ADC.

Para configurar un intervalo de sondeo

1. En el panel de navegación, expanda Cirix ADC 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 Citrix ADC.
   - Unidad de intervalo: La unidad de tiempo. Valores posibles: Horas, Minutos. Valor predeterminado: Horas.
4. Haga clic en Aceptar y, a continuación, haga clic en Cerrar.

Para realizar una encuesta inmediata

1. En el panel de navegación, expanda Cirix ADC 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 nuevos certificados, si los hay, aparecen en la lista.

Permitir el modo L2 en una instancia de Citrix ADC

June 19, 2019

En el modo Capa 2 (L2), una instancia de Citrix ADC actúa como puente de aprendizaje y reenvía todos los paquetes para los que no es el destino. Algunas funciones, como Cloud Bridge, requieren que el modo L2 esté habilitado en la instancia de Citrix ADC. Con el modo L2 habilitado, la instancia puede recibir y reenviar paquetes para direcciones MAC que no sean su propia dirección MAC. Sin embargo, si un usuario quiere habilitar el modo L2 en una instancia de Citrix ADC que se ejecuta en un dispositivo Citrix ADC SDX, el administrador debe permitir primero el modo L2 en esa instancia. Si permite el modo L2, debe tomar precauciones para evitar los bucles de puente.

Precauciones:

1. En una interfaz 1/x determinada, los paquetes sin etiquetar se deben permitir en una sola 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. Tenga en cuenta que si selecciona etiquetado, no puede recibir paquetes sin etiquetar en esa interfaz.

   Si ha seleccionado Etiquetado 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 compartidas por instancias de Citrix ADC en las que se permite el modo L2, asegúrese de que se cumplen las condiciones siguientes:

   - El filtrado de VLAN está habilitado en todas las interfaces.
   - Cada interfaz está en una VLAN 802.1q diferente.
   - Solo una instancia puede recibir paquetes sin etiquetar en la interfaz. Si esa interfaz está asignada a otras instancias, debe seleccionar Etiquetado en esa interfaz para esas instancias.

3. Si permite paquetes no etiquetados para una instancia en una interfaz 1/x, y el modo L2 está permitido para esa instancia, ninguna otra instancia (con el modo L2 permitido o no permitido) puede recibir paquetes sin etiquetar en esa interfaz.

4. Si permite paquetes sin etiquetar para una instancia en una interfaz 1/x, y el modo L2 no está permitido para esa instancia, ninguna instancia con el modo L2 permitido puede recibir paquetes sin etiquetar en esa interfaz.

5. Si ha aprovisionado una instancia (por ejemplo VPX1) en modo L2 en una interfaz 0/x y la misma interfaz también está asignada a otra instancia (por ejemplo, VPX2), seleccione Etiquetado para

todas las demás interfaces (1/x y 10/x) asignadas a la segunda instancia (VPX2).

Nota: Si el modo L2 está habilitado en una instancia de Citrix ADC y ambas interfaces de administración (0/1 y 0/2) están asociadas a esa instancia, solo una de las interfaces de administración se puede asociar a otra instancia de Citrix ADC en la que esté habilitado el modo L2. No puede asociar ambas interfaces de administración con más de una instancia de Citrix ADC en la que esté habilitado el modo L2.

Para permitir el modo L2 en una instancia

1. En el Asistente para aprovisionar ADC o 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 al aprovisionar la instancia o mientras la instancia se está ejecutando.
2. Siga las instrucciones del asistente.
3. Haga clic en Finalizar y, a continuación, haga clic en Cerrar.

Configurar las VMC en una interfaz

June 19, 2019

Una instancia de Citrix ADC utiliza Virtual MACs (VMC) para configuraciones de alta disponibilidad (activo-activo o activo-en espera). Una dirección MAC virtual (VMAC) es una entidad flotante compartida por los nodos primario y secundario en una configuración de alta disponibilidad.

En una configuración de alta disponibilidad, el nodo principal posee todas las direcciones IP flotantes, como las direcciones MIP, SNIP y VIP. El nodo principal responde a las solicitudes de 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 se hace cargo como el nuevo nodo principal. A continuación, utiliza ARP Gratuitous (GARP) para anunciar las direcciones IP flotantes que adquirió del primario. 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 Citrix ADC SDX. Dichos dispositivos conservan la antigua asignación IP a MAC anunciada por el nodo principal anterior, y un sitio puede desaparecer como resultado.

Puede superar este problema configurando un VMAC en ambos nodos de un par de HA. 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 no es necesario actualizar las tablas ARP en los dispositivos externos.

La configuración de un VMAC es un proceso de dos pasos:

1. Configure VMAC en SDX Management Service. Agregar un VRID para una interfaz o un canal LA. Configurar VMAC en SDX Management Service.
2. Configure VMAC en la instancia de Citrix. Para obtener información, consulte el artículoConfigurar VMAC en el canalde asistencia técnica del grupo.

Configurar VMAC en SDX Management Service

Para configurar VMAC, agregue un VRID IPv4 o IPv6 a una interfaz o canal LA desde Management Service. Management Service genera internamente un VMAC. Debe especificar el mismo VRID al configurar el modo activo-activo en la instancia de Citrix ADC.

Tenga en cuenta los siguientes puntos:

1. Agregue un VRID desde Management Service y especifique el mismo VRID en la instancia de Citrix ADC. Si agrega un VRID directamente en la instancia de Citrix ADC, la instancia no puede recibir un paquete que tenga una dirección VMAC como dirección MAC de destino.
2. Puede utilizar los mismos VRID en diferentes instancias en una interfaz 10G si el filtrado de VLAN está habilitado en la interfaz y las instancias asociadas a esa interfaz pertenecen a VLAN 802.1q etiquetadas diferentes.
3. No se pueden utilizar los mismos VRID en instancias diferentes en una interfaz 1G.
4. Puede agregar o eliminar los VRID de una interfaz asignada a una instancia mientras se ejecuta la instancia.
5. En una configuración activa-activa, puede especificar más de un VRID para una interfaz asignada a una instancia.
6. Se permite un máximo de 86 VMC en una interfaz de 10G y un máximo de 16 VMC en una interfaz de 1G. Si no hay más filtros VMAC disponibles, reduzca el número de VRID en otra instancia.

Puede agregar un VRID en el momento de agregar una instancia de Citrix ADC VPX, o bien puede modificar una instancia de Citrix ADC existente para agregar una VRID.

Para agregar un VRID IPv4 o IPv6 a una interfaz o canal LA

1. Mientras agrega una instancia VPX en SDX, en **Configuración de red**, seleccione **Interfaces de datos**. Para obtener más información acerca de cómo agregar una instancia VPX en SDX, consulte Agregar una instancia de Citrix ADC.
2. En el menú desplegable **Interfaces**, seleccione la interfaz o el canal LA.

3. En Configuración de VMAC y establezca uno o ambos de los siguientes valores:
   - VRID IPv4: El VRID IPv4 que identifica el VMAC. Valores posibles: De 1 a 255.
   - VRID IPv6: El VRID IPv6 que identifica el VMAC. Valores posibles: De 1 a 255.
     Nota: Utilice 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, haga clic en **Cerrar**.

Si la instancia ya está aprovisionada, para agregar un VRID IPv4 o IPv6, siga estos pasos.

1. Desde SDX Management Service, vaya a **Configuración > Citrix ADC > 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, establezca los valores de VRID. Haga clic en **Agregar** y, a continuación, haga clic en **Listo**.

Generar direcciones MAC de partición para configurar la partición de administración en una instancia de Citrix ADC en el dispositivo SDX

June 19, 2019

Una instancia de Citrix ADC en un dispositivo Citrix ADC SDX se puede dividir en entidades lógicas denominadas particiones de administrador. Cada partición se puede configurar y utilizar como una instancia de Citrix ADC independiente. Para obtener más información acerca de las particiones de administración, consulte Partición de administración.

Para usar particiones de administración con una configuración VLAN compartida, necesita una dirección MAC virtual para cada partición. Dicha dirección MAC virtual se denomina dirección MAC de partición (PMAC) y se utiliza para clasificar el tráfico recibido en una VLAN compartida. Esta dirección PMAC se utiliza en todas las VLAN compartidas enlazadas a esa partición.

Debe generar y configurar la dirección PMAC mediante la interfaz de usuario de Management Service, antes de utilizar la partición admin. Management Service le permite generar direcciones MAC de partición mediante:

- Uso de una dirección MAC base
- Especificar direcciones MAC personalizadas
- Generación aleatoria de direcciones MAC

Nota
Después de generar las direcciones MAC de partición, debe reiniciar la instancia de Citrix ADC antes de configurar las particiones de administrador.

Para generar las direcciones MAC de partición mediante una dirección MAC base:

1. En la ficha **Configuración**, en el panel izquierdo, expanda **Citrix ADC** y, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias**, seleccione la instancia de Citrix ADC 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 **MacS de partición**, haga clic en **Generar**.
5. En el cuadro de diálogo **Generar Macs 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 **Incrementar por**, introduzca el valor por el que se debe incrementar la dirección MAC base 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. Haga clic en **Generar**.

Para generar las direcciones MAC de partición especificando direcciones MAC personalizadas:

1. En la ficha **Configuración**, en el panel izquierdo, expanda **Citrix ADC** y, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias**, seleccione la instancia de Citrix ADC 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 **MacS de partición**, haga clic en **Generar**.
5. En el cuadro de diálogo **Generar Macs 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, escriba la siguiente dirección MAC. Repita esta operación para especificar direcciones MAC personalizadas adicionales.
8. Haga clic en **Generar**.

Para generar aleatoriamente las direcciones MAC de partición:

1. En la ficha **Configuración**, en el panel izquierdo, expanda **Citrix ADC** y, a continuación, haga clic en **Instancias**.
2. En el panel **Instancias**, seleccione la instancia de Citrix ADC 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 **MacS de partición**, haga clic en **Generar**.
5. En el cuadro de diálogo **Generar Macs 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. Haga clic en **Generar**.

Una vez que haya generado direcciones MAC de partición en el dispositivo SDX, utilice las direcciones MAC de partición generadas para configurar particiones de administración en la instancia de Citrix ADC.

Administración de cambios para instancias VPX

June 19, 2019

Puede realizar un seguimiento de cualquier cambio en la configuración en una instancia de Citrix ADC VPX desde Management Service. En el panel de detalles se muestra el nombre del dispositivo con la dirección IP, la fecha y la hora en que se actualizó por última vez y si existe alguna diferencia entre la configuración guardada y la configuración en ejecución. Seleccione un dispositivo para ver su configuración en ejecución, configuración guardada, 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. Posteriormente, puede utilizar 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 para instancias VPX

1. En la ficha Configuración, vaya a Citrix ADC > Gestión 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 sondear las actualizaciones de la configuración de cualquiera de las instancias de Citrix ADC

1. En la ficha Configuración, vaya a Citrix ADC > Gestión de cambios.
2. En el panel Administración de cambios, en la lista Acción, seleccione una de las siguientes opciones:
   - Encuesta ahora: Management Service realiza una encuesta inmediata 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 Citrix ADC

1. Abra un archivo de configuración existente y copie su lista de comandos.
2. En la ficha Configuración, vaya a Citrix ADC > Gestión 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 copiados del archivo de configuración.
6. Haga clic en Crear y, a continuación, haga clic en Cerrar.

Supervisar instancias de Citrix ADC

June 19, 2019

En la página Supervisión de la interfaz de usuario de Management Service se muestra una vista de alto nivel del rendimiento del dispositivo y de las instancias VPX aprovisionadas en el dispositivo. Después de aprovisionar y configurar la instancia de Citrix ADC, puede realizar varias tareas para supervisar la instancia de Citrix ADC.

Visualización de las propiedades de las instancias VPX

La interfaz de usuario de Management Service muestra la lista y la descripción de todas las instancias VPX aprovisionadas en el dispositivo SDX. Utilice el panel de instancias de Citrix ADC para ver detalles, como el nombre y la dirección IP de la instancia, la utilización de CPU y memoria, el número de paquetes recibidos y transmitidos en la instancia, 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 Citrix ADC 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 Citrix ADC, puede ver los siguientes detalles para la instancia de Citrix ADC:
   - Nombre
     Nombre de host asignado a la instancia de Citrix ADC durante el aprovisionamiento.
   - Estado de VM

     El estado de la máquina virtual.
   - Estado Citrix ADC

     El estado de la instancia de Citrix ADC.
   - Dirección IP

     La dirección IP de la instancia de Citrix ADC. 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 Citrix ADC.
   - Tx (Mbps)

     Los paquetes transmitidos por la instancia de Citrix ADC.
   - Solicitudes HTTP/s

     Número total de solicitudes HTTP recibidas en la instancia de Citrix ADC cada segundo.
   - Uso de CPU (%)

     Porcentaje de utilización de CPU en Citrix ADC.

- Uso de memoria (%)

  Porcentaje de utilización de memoria en Citrix ADC.

3. Haga clic en la flecha situada junto al nombre de una instancia de Citrix ADC para ver las propiedades de esa instancia o haga clic en Expandir todo para ver las propiedades de todas las instancias de Citrix ADC. Puede ver las siguientes propiedades:

   - Máscara de red

     Dirección IP de máscara de red de la instancia de Citrix ADC.

   - 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 cada segundo.

   - NIC

     Los nombres de las tarjetas de interfaz de red utilizadas por la instancia de Citrix ADC, junto con la función virtual asignada a cada interfaz.

   - Versión

     Versión de compilación, fecha de compilación y hora del software de Citrix ADC que se ejecuta actualmente en la instancia.

   - Nombre de host

     Nombre de host de la instancia de Citrix ADC.

   - Memoria total (GB)

     Memoria total asignada a la instancia de Citrix ADC.

   - Rendimiento (Mbps)

     Rendimiento total de la instancia de Citrix ADC.

   - Desde

     La fecha y la hora desde que la instancia ha estado continuamente en estado UP.

   - #SSL Fichas

     Número total de chips SSL
     asignados a la instancia.

   - Dirección IP del mismo nivel

     La dirección IP del par de esta instancia de Citrix ADC si está en una configuración de alta disponibilidad.

- Estado

  Estado de las operaciones que se realizan en una instancia de Citrix ADC, como el estado de si el inventario de la instancia se ha completado o si el reinicio está en curso.

- Estado principal de HA

  El estado del dispositivo. El estado indica si la instancia está configurada en una configuración principal o independiente o independiente 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 alta disponibilidad

  El modo del estado de sincronización de alta disponibilidad, como habilitado o inhabilitado.

- Descripción

  Descripción introducida al aprovisionar la instancia de Citrix ADC.

Visualización de la configuración en ejecución y guardada de una instancia de Citrix ADC

Mediante Management Service puede ver la configuración que se está ejecutando actualmente de una instancia de Citrix ADC. También puede ver la configuración guardada de una instancia de Citrix ADC y la hora en que se guardó la configuración.

Para ver la configuración en ejecución y guardada de una instancia de Citrix ADC

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en la instancia de Citrix ADC 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 de ejecución de Citrix ADC o en la ventana Configuración guardada de Citrix ADC, puede ver la configuración en ejecución o guardada de la instancia de Citrix ADC.

Hacer ping a una instancia de Citrix ADC

Puede hacer ping a una instancia de Citrix ADC desde Management Service para comprobar si el dispositivo es accesible.

Para hacer ping a una instancia de Citrix ADC

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en la instancia de Citrix ADC que quiere hacer ping y, a continuación, haga clic en ping. En el cuadro de mensaje Ping, puede ver si el ping es correcto.

Seguimiento de la ruta de una instancia de Citrix ADC

Puede realizar un seguimiento de la ruta de un paquete desde Management Service a una instancia de Citrix ADC determinando el número de saltos utilizados para llegar a la instancia.

Para rastrear la ruta de una instancia de Citrix ADC

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en la instancia de Citrix ADC que quiere rastrear y, a continuación, haga clic en TraceRoute. En el cuadro de mensaje Traceroute, puede ver la ruta al de Citrix ADC.

Redescubrimiento de una instancia de Citrix ADC

Puede redescubrir una instancia de Citrix ADC cuando necesite ver el estado y la configuración más recientes de una instancia de Citrix ADC.

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 Citrix ADC

1. En la ficha Configuración, en el panel izquierdo, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en la instancia de Citrix ADC que quiera redescubrir y, a continuación, haga clic en Redescubrir.
3. En el cuadro Confirmar mensaje, haga clic en Sí.

Usar registros para supervisar operaciones y eventos

June 19, 2019

Utilice registros de tareas y de auditoría para supervisar las operaciones realizadas en Management Service y en las instancias de Citrix ADC SDX. También puede utilizar el registro de eventos para realizar un seguimiento de todos los eventos de las tareas realizadas en Management Service y XenServer.

Visualización de los registros de auditoría

Todas las operaciones realizadas mediante Management Service se registran en la base de datos del dispositivo. Utilice registros de auditoría para ver las operaciones que ha realizado un usuario de Management Service, la fecha y hora de cada operación y el estado de éxito o error de la operación. También puede ordenar los detalles por usuario, operación, tiempo de auditoría, estado, etc. haciendo clic en el encabezado de columna correspondiente.

La paginación se admite en el panel Registro de auditoría. Seleccione el número de registros que desea mostrar 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, a continuación, haga clic en Auditoría.
2. En el panel Registro de auditoría, puede ver los siguientes detalles.
    - Nombre de usuario: el usuario de Management Service 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 estaba ejecutando el sistema cuando se realizó la operación.
    - Tipo de recurso: tipo de recurso utilizado para realizar la operación, como xen_vpx_image e 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: la hora 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, como Correcto o Error.
    - Mensaje: 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 determinado, haga clic en el encabezado de la columna.

Visualización de registros de tareas

Utilice los registros de tareas para ver y realizar un seguimiento de tareas, como la actualización de instancias e instalación de certificados SSL, que ejecuta Management Service en las instancias de Cit-

rix ADC. El registro de tareas le permite ver si una tarea está en curso o ha fallado o se ha realizado correctamente.

La paginación se admite en el panel Registro de tareas. Seleccione el número de registros que desea mostrar 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 Diagnósticos y, a continuación, haga clic en Registro de tareas.
2. En el panel Registro de tareas, puede ver los siguientes detalles.
    - Nombre: nombre de la tarea que se está ejecutando o que ya se ha ejecutado.
    - Estado: el estado de la tarea, como En curso, Completado o Fallo.
    - Ejecutado por: el usuario de Management Service que ha realizado la operación.
    - Hora de inicio: la hora en la que se inició la tarea.
    - Hora de finalización: la hora en la que terminó la tarea.

Visualización de registros de dispositivos de tareas

Utilice 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 tarea le permite ver si una tarea está en curso o ha fallado o se ha realizado correctamente. También muestra la dirección IP de la instancia en la que se realiza la tarea.

Para ver el registro del dispositivo de tarea, siga estos pasos:

1. En el panel de navegación, expanda Diagnósticos 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 tarea.
3. En el panel Registro del dispositivo de tareas, para ordenar los registros por un campo determinado, haga clic en el encabezado de la columna.

Visualización de 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 Citrix ADC. El registro de comandos de tarea le permite ver si un comando se ha ejecutado correctamente o ha fallado. También muestra el comando que se ejecuta y la razón por la que un comando ha fallado.

Para ver el registro de comandos de tarea, siga estos pasos:

1. En el panel de navegación, expanda Diagnósticos 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 tarea.
3. En el panel Registro de dispositivo de tarea, 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 determinado, haga clic en el encabezado de la columna.

Visualización de eventos

Utilice el panel Eventos de la interfaz de usuario de Management Service para supervisar los eventos generados por Management Service para las tareas realizadas en Management Service.

Para ver los eventos, siga estos pasos:

1. En la ficha Supervisión, en el panel izquierdo, expanda Supervisión y, a continuación, haga clic en Eventos.
2. En el panel Eventos, puede ver los siguientes detalles.
   - Gravedad: gravedad de un evento, que puede ser crítico, mayor, menor, claro e información.
   - Fuente: la dirección IP en la que se genera el evento.
   - Fecha: la fecha en que se genera el evento.
   - Categoría: categoría de evento, como PolicyFailed y DeviceConfigChange.
   - Mensaje: el mensaje que describe el evento.
3. Para ordenar los eventos por un campo determinado, haga clic en el encabezado de la columna.

Casos de uso para dispositivos Citrx ADC SDX

June 19, 2019

Para componentes de red (como firewalls y Application Delivery Controllers), el soporte para multiarrendamiento ha implicado históricamente la capacidad de tallar 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 severamente limitado en cuanto al 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 Citrix ADC 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 administración.

Los casos de uso principales de un dispositivo SDX están relacionados con la consolidación, lo que reduce el número de redes necesarias al tiempo que mantiene el aislamiento de la administración. A continuación se presentan los escenarios básicos de consolidación:

- Consolidación cuando las instancias de Citrix ADC y Management Service están en la misma red.
- Consolidación cuando las instancias de Citrix ADC y Management Service 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 de Citrix ADC y Management Service están en la misma red

June 19, 2019

Un tipo simple de caso de consolidación en el dispositivo SDX es la configuración de las instancias de Management Service y Citrix ADC como parte de la misma red. Este caso de uso es aplicable si el administrador del dispositivo también es el administrador de instancias y el requisito de cumplimiento de normas de la organización no especifica que se requieran redes de administración independientes para Management Service y las direcciones NSIP de las distintas instancias. Las instancias se pueden aprovisionar en la misma red (para tráfico de gestión), pero las direcciones VIP se pueden configurar en diferentes redes (para tráfico de datos) y, por lo tanto, en diferentes zonas de seguridad.

En el ejemplo siguiente, las instancias de Management Service y Citrix ADC forman parte de la red 10.1.1.x.. Las interfaces 0/1 y 0/2 son las interfaces de gestión, 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, el número de instancias se limita al número de interfaces físicas disponibles en el dispositivo. De forma predeterminada, el filtrado de VLAN está habilitado en cada interfaz del dispositivo SDX, lo que restringe el número de VLAN 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 figura ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con Management Service y NSIP para instancias de la misma red

En la tabla siguiente se enumeran los nombres y valores de los parámetros utilizados para aprovisionar la instancia 1 de Citrix ADC en el ejemplo anterior.

Nombre del parámetro	Valores para 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	Platino
Perfil de administrador	ns_nsroot_profile
Nombre de usuario	vpx8
Contraseña	Sdx
Confirmar contraseña	Sdx
Acceso a Shell/Sftp/Spp	Es cierto
Memoria total (MB)	2048
#SSL Fichas	1
Rendimiento (Mbps)	1000
Paquetes por segundo	1000000
CPU	Compartido
Interfaz	0/1 y 1/1

Aprovisionar la instancia 1 de Citrix ADC como se muestra en este ejemplo

1. En la ficha Configuración, en el panel de navegación, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en Agregar.
3. En el Asistente para aprovisionar Citrix, siga las instrucciones del asistente para especificar los valores de parámetros que se muestran en la tabla anterior.
4. Haga clic en Crear y, a continuación, haga clic en Cerrar. La instancia de Citrix ADC que aprovisionó aparece en el panel de instancias de Citrix ADC.

Consolidación cuando las instancias de Citrix ADC y Management Service se encuentran en redes diferentes

June 19, 2019

En algunos casos, el administrador del dispositivo puede permitir a otros administradores realizar tareas de administración en instancias individuales. Esto se puede hacer de forma segura dando a un administrador de instancia individual derechos de inicio de sesión solo a esa instancia. Sin embargo, por razones de seguridad, es posible que el administrador del dispositivo no desee permitir que la instancia esté en la misma red que Management Service. Este es un escenario muy común en entornos de proveedores de servicios, y cada vez es más común en las empresas a medida que adoptan arquitecturas de virtualización y nube.

En el ejemplo siguiente, Management Service se encuentra en la red 10.1.1.x y las instancias de Citrix ADC están en la red 10.1.2.x. Las interfaces 0/1 y 0/2 son las interfaces de gestión, 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, el número de instancias se limita al número de interfaces físicas disponibles en el dispositivo. El filtrado de VLAN no es necesario, ya que 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 es necesario configurar una NSVLAN, ya que las instancias no comparten una interfaz física y no hay VLAN etiquetadas. Para obtener más información acerca de las NSVLAN, consulte Agregar una instancia de Citrix ADC.

La siguiente figura ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con Management Service y NSIP para instancias en redes diferentes

Como administrador del dispositivo, tiene la opción de mantener el tráfico entre Management Service y las direcciones NSIP en el dispositivo SDX, o de forzar el tráfico fuera del dispositivo si, por ejemplo, desea que el tráfico pase a través de un firewall externo o de algún otro intermediario de seguridad y, a continuación, vuelva al dispositivo.

En la tabla siguiente se enumeran los nombres y valores de los parámetros utilizados para aprovisionar la instancia 1 de Citrix ADC en este ejemplo.

Nombre del parámetro	Valores para la instancia 1
Nombre	vpx1
Dirección IP	10.1.2.2
Máscara de red	255.255.255.0
Gateway	10.1.2.1

Nombre del parámetro	Valores para la instancia 1
Archivo XVA	NS-VPX-XEN-10.0-51.308.a_nc.xva
Licencia de funciones	Platino
Perfil de administrador	ns_nsroot_profile
Nombre de usuario	vpx1
Contraseña	Sdx
Confirmar contraseña	Sdx
Acceso a Shell/Sftp/Spp	Es cierto
Memoria total (MB)	2048
#SSL Fichas	1
Rendimiento (Mbps)	1000
Paquetes por segundo	1000000
CPU	Compartido
Interfaz	0/2 y 1/1

Para aprovisionar la instancia 1 de Citrix ADC como se muestra en este ejemplo

1. En la ficha Configuración, en el panel de navegación, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en Agregar.
3. En el Asistente para aprovisionar Citrix ADC, siga las instrucciones del asistente para establecer los parámetros en los valores mostrados en la tabla anterior.
4. Haga clic en Crear y, a continuación, haga clic en Cerrar. La instancia de Citrix ADC que aprovisionó aparece en el panel de instancias de Citrix ADC.

Consolidación en todas las zonas de seguridad

June 19, 2019

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 a la red interna de la organización. En entornos de alto cumplimiento, generalmente no es aceptable una sola instancia de Citrix ADC con direcciones VIP tanto en la DMZ

como en una red interna. Con SDX, puede aprovisionar instancias que hospeden direcciones VIP en la zona desmilitarizada y otras instancias que hospeden direcciones VIP en una red interna.

En algunos casos, es posible que necesite redes de administración independientes para cada zona de seguridad. En tales casos, debe colocar las direcciones NSIP de las instancias en la DMZ en una red y colocar las direcciones NSIP de las instancias con VIP en la red interna en una red de administración diferente. Además, en muchos casos, es posible que la comunicación entre Management Service 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 utilizar los puertos de datos como puertos de administración (por ejemplo, cuando necesite configurar las VLAN etiquetadas, porque el etiquetado no está permitido en las interfaces de administración). Si lo hace, el tráfico de Management Service debe salir del dispositivo y, a continuación, volver al dispositivo. Puede enrutar este tráfico o, opcionalmente, especificar una NSVLAN en una interfaz asignada a la instancia. Si las instancias están configuradas en una interfaz de administración común con Management Service, no es necesario enrutar el tráfico entre las instancias de Management Service y Citrix ADC, a menos que la configuración lo requiera explícitamente.

Nota El etiquetado se admite en XenServer versión 6.0.

Consolidación con interfaces dedicadas para cada instancia

June 19, 2019

En el ejemplo siguiente, 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 de Citrix ADC 2 y 3 forman parte de la red 10.1.200.x (VLAN 100), y las instancias de Citrix ADC 4 y 5 forman parte de la red 10.1.3.x (VLAN 200).

Opcionalmente, puede configurar una NSVLAN en todas las instancias.

La siguiente figura ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con instancias de Citrix ADC en varias redes

El dispositivo SDX está conectado a un conmutador. Asegúrese de que los ID 100 y 200 de VLAN están configurados en el puerto del conmutador al que está conectado el puerto 1/1 del dispositivo.

En la tabla siguiente se enumeran los nombres y valores de los parámetros utilizados para aprovisionar las instancias 5 y 3 de Citrix ADC en este ejemplo.

Nombre del parámetro	Valores para la instancia 5	Valores para la instancia 3
Nombre	vpx5	vpx3
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	Platino	Platino
Perfil de administrador	ns_nsroot_profile	ns_nsroot_profile
Nombre de usuario	vpx5	vpx3
Contraseña	Sdx	raíz
Confirmar contraseña	Sdx	raíz
Acceso a Shell/Sftp/Spp	Es cierto	Es cierto
Memoria total (MB)	2048	2048
#SSL Fichas	1	1
Rendimiento (Mbps)	1000	1000
Paquetes por segundo	1000000	1000000
CPU	Compartido	Compartido
Interfaz	1/1 y 10/4	1/1 y 1/5
NSVLAN	200	100
Agregar (interfaz)	11.	1/1
Interfaz etiquetada	Seleccionar etiquetado	Seleccionar etiquetado

Para aprovisionar instancias 5 y 3 de Citrix ADC como se muestra en este ejemplo

1. En la ficha Configuración, en el panel de navegación, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en Agregar.
3. En el Asistente para aprovisionar Citrix ADC, siga las instrucciones del asistente para establecer los parámetros en los valores mostrados en la tabla anterior.
4. Haga clic en Crear y, a continuación, haga clic en Cerrar. La instancia de Citrix ADC que aprovisionó aparece en el panel de instancias de Citrix ADC.

Consolidación con uso compartido de un puerto físico por más de una instancia

June 19, 2019

Puede habilitar e inhabilitar el filtrado de VLAN en una interfaz según sea necesario. Por ejemplo, si necesita 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 la otra instancia no vea el tráfico de una instancia.

Nota Elfiltrado 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 ejemplo siguiente, 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 Citrix ADC se encuentran en la red 10.1.200.x, y las instancias 4, 5, 6 y 7 están en la red 10.1.3.x. Las instancias 2 y 3 tienen cada una una 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 está etiquetado para VLAN 4 y el tráfico para la instancia 7 está etiquetado para la VLAN 7. Como resultado, el tráfico de la instancia 4 no es visible para la instancia 7, y viceversa. 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 500-599 en la Instancia 5 y las VLAN 600-699 en la Instancia 6. La instancia 5 puede ver el tráfico de difusión y multidifusión desde VLAN 600-699, 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 VLAN 500-599, pero los paquetes se descartan en el nivel de software.

La siguiente figura ilustra el caso de uso anterior.

Figura 1. Topología de red de un dispositivo SDX con instancias de Management Service e Citrix ADC distribuidas en redes

En la tabla siguiente se enumeran los nombres y valores de los parámetros utilizados para aprovisionar instancias 7 y 4 de Citrix ADC en este ejemplo.

Nombre del parámetro	Valores para la instancia 7	Valores para 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	Platino	Platino
Perfil de administrador	ns_nsroot_profile	ns_nsroot_profile
Nombre de usuario	vpx4	vpx4
Contraseña	Sdx	Sdx
Confirmar contraseña	Sdx	Sdx
Acceso a Shell/Sftp/Spp	Es cierto	Es cierto
Memoria total (MB)	2048	2048
#SSL Fichas	1	1
Rendimiento (Mbps)	1000	1000
Paquetes por segundo	1000000	1000000
CPU	Compartido	Compartido
Interfaz	1/1 y 1/7	1/1 y 1/7
NSVLAN	200	200

Para aprovisionar instancias 7 y 4 de Citrix ADC en este ejemplo

1. En la ficha Configuración, en el panel de navegación, expanda Configuración de Citrix ADC y, a continuación, haga clic en Instancias.
2. En el panel de instancias de Citrix ADC, haga clic en Agregar.
3. En el Asistente para aprovisionar Citrix ADC, siga las instrucciones del asistente para establecer los parámetros en los valores mostrados en la tabla anterior.
4. Haga clic en Crear y, a continuación, haga clic en Cerrar. La instancia de Citrix ADC que aprovisionó aparece en el panel de instancias de Citrix ADC.

API de NITRO

June 19, 2019

El protocolo Citrix 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 o .NET o Python, el protocolo NITRO se expone como bibliotecas relevantes que se empaquetan como kits de desarrollo de software (SDK) independientes.

Nota: Debe tener una comprensión básica del dispositivo SDX antes de usar NITRO.

Para utilizar el protocolo NITRO, la aplicación cliente necesita lo siguiente:

- Acceso a un dispositivo SDX.
- Para utilizar interfaces REST, debe disponer de un sistema para generar solicitudes HTTP o HTTPS (carga útil en formato JSON) en el dispositivo SDX. Puede utilizar cualquier lenguaje de programación o herramienta.
- Para clientes Java, debe tener un sistema donde esté disponible la versión Java Development Kit (JDK) 1.5 o superior. El JDK se puede descargar desdehttp://www.oracle.com/technetwork/java/javase/downloads/index.html.
- Para los clientes.NET, debe tener un sistema donde esté disponible la versión de.NET framework 3.5 o superior. El framework de.NET se puede descargar desdehttp://www.microsoft.com/downloads/en/def
- 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

June 19, 2019

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 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 estar instalada en la ruta del cliente. Para obtener instrucciones de instalación, consulte el archivo \/Readme.txt.

SDK de .NET

June 19, 2019

Las API de SDX NITRO se clasifican según el alcance y el propósito de las API en las API del sistema y las API de configuración. También puede solucionar problemas de operaciones de NITRO.

API 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.

Debe crear 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:

“‘ pre codeblock
//Specify the IP address of the appliance and service type
nitro_service nitroservice = new nitro_service (“10.102.31.16”, “https”);

//Specify the login credentials
nitroservice.login(“nsroot”, “verysecret”);

```
Nota: Debe utilizar el objeto
nitro_service en todas las operaciones de NITRO adicionales del
   dispositivo.

Para desconectar del dispositivo, invoque el método logout () de la
   siguiente manera:
```



```
5
6 ``` pre codeblock
7 nitroservice.logout();
```

API de configuración

El protocolo NITRO se puede utilizar 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.<resource_type>. Cada uno de estos paquetes o espacios de nombres contiene una clase llamada <resource_type> que proporciona las API para configurar el recurso.

Por ejemplo, el recurso NetScaler tiene el paquete com.citrix.sdx.nitro.resource.config.ns o espacio de nombres.

Una clase de recurso proporciona API para realizar otras operaciones, como la creación de un recurso, la recuperación de recursos y propiedades de recursos, la actualización de un recurso, la eliminación de recursos y la realización de operaciones masivas en recursos.

Creación de un recurso

Para crear un nuevo recurso (por ejemplo, una instancia de Citrix ADC) 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 necesarios 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 static add ().

El siguiente código de ejemplo crea una instancia Citrix ADC denominada “ns_instance” en el dispositivo SDX:

“‘ pre codeblock
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.name = “ns_instance”;
newns.ip_address = “10.70.136.5”;
newns.netmask = “255.255.255.0”;
newns.gateway = “10.70.136.1”;
newns.image_name = “nsvpx-9.3.45_nc.xva”;
newns.profile_name = “ns_nsroot_profile”;


```
newns.vm_memory_total = 2048;
newns.throughput = 1000;
newns.pps = 1000000;
newns.license = “Standard”;
newns.username = “admin”;
newns.password = “admin”;

int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].port_name = “10/1”;

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].port_name = “10/2”;

newns.network_interfaces = interface_array;

//Upload the Citrix ADC instance
ns result = ns.add(nitroservice, newns);
```

```
### Recuperar 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:

``` pre codeblock
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
Console.WriteLine(returned_ns[i].ip_address);
Console.WriteLine(returned_ns[i].netmask);
```


```

**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 Citrix ADC con ID 123456a:

“‘ pre codeblock
ns obj = new ns();
obj.id = “123456a”;
ns stats = ns.get(nitroservice, obj);
Console.WriteLine(“CPU Usage:” + stats.ns_cpu_usage);
Console.WriteLine(“Memory Usage:” + stats.ns_memory_usage);
Console.WriteLine(“Request rate/sec:” +stats.http_req);

```
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 ID 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 Citrix ADC con ID 123456a a 'ns_instance_new':

``` pre codeblock
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.id = ”123456a”;

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to ”ns_instance_new” locally
```


```

```
update_obj.name = ”ns_instance_new”;

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
```

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.

El siguiente código de ejemplo elimina una instancia de Citrix ADC con ID 1:

“‘ pre codeblock
ns obj = new ns();
obj.id = “123456a”;
ns.delete(nitroservice, obj);

```
### Operaciones en bloque

Puede consultar o cambiar varios recursos simultáneamente y, por lo
    tanto, minimizar el tráfico de red. Por ejemplo, puede agregar
    varios dispositivos Citrix ADC SDX en la misma operación.

Cada clase de recurso tiene métodos que toman una matriz de recursos
    para agregar, actualizar y quitar recursos. Para realizar una
    operación masiva, especifique los detalles de cada operación
    localmente y, a continuación, envíe los detalles a la 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:

- **Salgan.** Cuando se encuentra el primer error, la ejecución se
    detiene. Se han confirmado los comandos que se ejecutaron antes del
    error.
- **Continúe.** Todos los comandos de la lista se ejecutan incluso si
    algunos comandos fallan.

Nota: Debe configurar el comportamiento requerido al establecer una
    conexión con el dispositivo, estableciendo el parámetro
onerror en el método
nitro_service ().
```



```
15
16 El siguiente código de ejemplo agrega dos NetScalers en una operación:
17
18 ``` pre codeblock
19 ns[] newns = new ns[2];
20
21 //Specify details of first NetScaler
22 newns[0] = new ns();
23 newns[0].name = ”ns_instance1”;
24 newns[0].ip_address = ”10.70.136.5”;
25 newns[0].netmask = ”255.255.255.0”;
26 newns[0].gateway = ”10.70.136.1”;
27 ...
28 ...
29
30 //Specify details of second NetScaler
31 newns[1] = new ns();
32 newns[1].name = ”ns_instance2”;
33 newns[1].ip_address = ”10.70.136.8”;
34 newns[1].netmask = ”255.255.255.0”;
35 newns[1].gateway = ”10.70.136.1”;
36 ...
37 ...
38
39 //upload the details of the NetScalers to the NITRO server
40 ns[] result = ns.add(nitroservice, newns);
```

Manejo 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 al procesar la solicitud NITRO.

El campo de mensaje de error proporciona una breve explicación y la naturaleza del error.

Todas las excepciones en la ejecución de las API NITRO son capturadas por la clase com.citrix.sdx.nitro.exception.ni
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 API disponible en la carpeta <NITRO_SDK_HOME>/doc.

Servicios web de REST

June 19, 2019

REST (Representational State Transfer) es un estilo arquitectónico basado en solicitudes HTTP simples y respuestas entre el cliente y el servidor. REST se utiliza 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 donde 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 del contenedor como carpetas, y los recursos secundarios como archivos o subcarpetas. El cliente que realiza la llamada proporciona el estado del recurso que se va a crear. El estado se puede especificar en la solicitud mediante el formato XML o JSON. El cliente también puede especificar la URL única que identificará 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 dirección 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.
- **Suprimir.** Puede destruir un recurso que existe en el lado del servidor mediante el método DELETE HTTP y la dirección URL que identifica el recurso que se va a quitar.

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, con el cuerpo de la solicitud en JSON especificando 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 las API del sistema y las API de configuración.

API 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.

Debe especificar 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
- **Petición**
  - **Encabezado**

```
Content-Type:application/vnd.com.citrix.sdx.login+json
```

Nota: También se pueden usar tipos de contenido como 'application/x -www-form-urlencoded' que se admitían en versiones anteriores de NITRO. Debe asegurarse de que la carga útil es la misma que la utilizada en versiones anteriores. Las cargas útiles proporcionadas en esta documentación solo son aplicables si el tipo de contenido es de la forma 'application/vnd.com.citrix.sdx.login + json'.

  - **Carga útil**

```
{

    "login":
    {

        "username":"nsroot",
        "password":"verysecret"
     }

 }
```

- **Carga útil de respuesta**
  - **Encabezado**

```
HTTP/1.0 201 Created
Set-Cookie:
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
```

Nota: Debe utilizar el ID de sesión en todas las operaciones de NITRO adicionales del 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:

```
{

    ”login”:
    {

        ”username”:”nsroot”,
        ”password”:”verysecret”,
        ”timeout”:3600
     }

 }
```

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 Citrix ADC:

- **URL**
- **Método HTTP**
- **Petición**
  - **Encabezado**

```
X-NITRO-USER:nsroot
X-NITRO-PASS:verysecret
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

  - **Carga útil**

```
{

    ”ns”:
    {

        ...
     }

 }
```

- **Respuesta.**
  - **Encabezado**


```
HTTP/1.0 201 Created
```

Para desconectar del dispositivo, utilice el método DELETE:

- **URL**
- **Método HTTP** DELETE
- **Petición**
  - **Encabezado**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.login+json
```

API de configuración

El protocolo NITRO se puede utilizar para configurar los recursos del dispositivo SDX.

Cada recurso SDX tiene una dirección URL única asociada, dependiendo del tipo de operación que se vaya a realizar. Las URL de las operaciones de configuración tienen el formato:`http://<IP>/nitro/v2/config/<resource_type>`

Creación de un recurso

Para crear un nuevo recurso (por ejemplo, una instancia de Citrix ADC) 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 Citrix ADC denominada vpx1:

- **URL**
- **Método HTTP**
- **Petición**
  - **Encabezado**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

  - **Carga útil**

```
{

    ”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       }
32
33   }
```

Recuperación de detalles y estadísticas de recursos

Los detalles de los recursos SDX se pueden recuperar de la siguiente manera:

- Para recuperar detalles de un recurso específico en el dispositivo SDX, especifique el identificador del recurso en la dirección URL.
- Para recuperar las propiedades de los recursos sobre la base de algún filtro, especifique las condiciones de filtro en la URL.

  La URL tiene la forma:`http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`
- Si es probable que su solicitud produzca un gran número de recursos devueltos desde el dispos-

itivo, puede recuperar estos resultados en fragmentos dividiéndolos en “páginas” y recuperándolos página por página.

Por ejemplo, suponga que quiere recuperar todas las instancias Citrix ADC en un SDX que tenga 53 de ellas. En lugar de recuperar los 53 en una gran respuesta, puede configurar los resultados para que se dividan en páginas de 10 instancias de Citrix ADC cada una (6 páginas en total) y recuperarlos del servidor página por página.

Especifique el recuento de páginas con el parámetro de cadena de consulta de tamaño de página y utilice el parámetro de cadena de consulta “pageno” para especificar el número de página que quiere recuperar.
La URL tiene la forma:`http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

No es necesario recuperar todas las páginas, o recuperar las páginas en orden. Cada solicitud es independiente, e incluso puede cambiar la configuración de tamaño de página entre solicitudes.

Nota: Si quiere tener una idea del número de recursos que es probable que devuelvan una solicitud, puede utilizar el parámetro de cadena de consulta de recuento para solicitar un recuento de los recursos que se devuelvan, en lugar de los propios recursos. Para obtener el número de instancias de Citrix ADC disponibles, la dirección URL sería
`http://<IP>/nitro/v2/config/<resource_type>?count=yes`

Para recuperar la información de configuración de la instancia de Citrix ADC con ID 123456a:

- **URL**
- **Método HTTP GE** T

Actualización de un recurso

Para actualizar un recurso SDX existente, utilice el método PUT HTTP. En la carga útil de solicitud HTTP, especifique el nombre y los demás argumentos que deben cambiarse. Por ejemplo, para cambiar el nombre de la instancia de Citrix ADC con ID 123456a a vpx2:

- **URL**
- **Método HTTP**
- **Solicitar carga útil**
  - **Encabezado**

```
1  Cookie:NITRO_AUTH_TOKEN=tokenvalue
2  Content-Type:application/vnd.com.citrix.sdx.ns+json
```

  - **Carga útil**


```
{

    ”ns”:
    {

        ”name”:”vpx2”,
        ”id”:”123456a”
     }

 }
```

Eliminación de un recurso

Para eliminar un recurso existente, especifique el nombre del recurso que se va a eliminar en la dirección URL. Por ejemplo, para eliminar una instancia de Citrix ADC con ID 123456a:

- **URL**
- **Método HTTP**
- **Petición**
  - **Encabezado**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

Operaciones en bloque

Puede consultar o cambiar varios recursos simultáneamente y, por lo tanto, minimizar el tráfico de red. Por ejemplo, puede agregar varios dispositivos Citrix ADC 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:

- **Salgan.** Cuando se encuentra el primer error, la ejecución se detiene. Se han confirmado los comandos que se ejecutaron antes del error.
- **Continúe.** Todos los comandos de la lista se ejecutan incluso si algunos comandos fallan.

Nota: Debe configurar el comportamiento requerido en el encabezado de solicitud mediante el parámetro X-NITRO-ONERROR.

Para agregar 2 recursos Citrix ADC en una operación y continuar si falla un comando:

- **URL.**
- **Método HTTP.**
- **Solicitar carga útil.**
  - **Encabezado**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
```

  - **Carga útil**

```
{

    ”ns”:
    [
        {

            ”name”:”ns_instance1”,
            ”ip_address”:”10.70.136.5”,
            ”netmask”:”255.255.255.0”,
            ”gateway”:”10.70.136.1”
         }
,
        {

            ”name”:”ns_instance2”,
            ”ip_address”:”10.70.136.8”,
            ”netmask”:”255.255.255.0”,
            ”gateway”:”10.70.136.1”
         }

    ]
 }
```

Para agregar varios recursos (Citrix ADC y dos usuarios MPS) en una operación y continuar si falla un comando:

- **URL.**
- **Método HTTP.** POST
- **Solicitar carga útil.**
  - **Encabezado**


```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
Content-Type:application/vnd.com.citrix.sdx.ns+json
X-NITRO-ONERROR:continue
```

- **Carga útil**

```
{

    ”ns”:
    [
        {

            ”name”:”ns_instance1”,
            ”ip_address”:”10.70.136.5”,
            ”netmask”:”255.255.255.0”,
            ”gateway”:”10.70.136.1”
         }
,
        {

            ”name”:”ns_instance2”,
            ”ip_address”:”10.70.136.8”,
            ”netmask”:”255.255.255.0”,
            ”gateway”:”10.70.136.1”
         }

    ],
     ”mpsuser”:
    [
        {

            ”name”:”admin”,
            ”password”:”admin”,
            ”permission”:”superuser”
         }
,
        {

            ”name”:”admin”,
            ”password”:”admin”,
            ”permission”:”superuser”
         }

```



```
38         ]
39     }
```

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 al procesar la solicitud NITRO.

El campo de mensaje de error proporciona una breve explicación y la naturaleza del error.

Cómo funciona NITRO

June 19, 2019

La infraestructura NITRO consiste en una aplicación cliente y el servicio web NITRO que se ejecuta en un dispositivo Citrix ADC 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 de ejecución NITRO

Como se muestra en la figura anterior, una solicitud NITRO se ejecuta de la siguiente manera:

1. La aplicación cliente envía un mensaje de solicitud REST al servicio web NITRO. Cuando se utilizan 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 todo el estado de un recurso desde el servidor, realice modificaciones en el estado del recurso localmente y, a continuación, vuelva a cargarlo en el servidor en una transacción de red.

Nota: Las operaciones locales en un recurso (cambiando sus propiedades) no afectan a su estado en el servidor hasta que el estado del objeto se cargue explícitamente.

Las API de NITRO son de naturaleza sincrónica. Esto significa que la aplicación cliente espera una respuesta del servicio web NITRO antes de ejecutar otra API de NITRO.

SDK de Java

June 19, 2019

Las API de SDX NITRO se clasifican según el alcance y el propósito de las API en las API del sistema y las API de configuración. También puede solucionar problemas de operaciones de NITRO.

API 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.

Debe crear 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:

“‘ pre codeblock
//Specify the IP address of the appliance and service type
nitro_service nitroservice = new nitro_service (“10.102.31.16”, “https”);

//Specify the login credentials
nitroservice.login(“nsroot”, “verysecret”);

```
Nota: Debe utilizar el objeto
nitro_service en todas las operaciones de NITRO adicionales del
   dispositivo.

Para desconectar del dispositivo, invoque el método logout () de la
   siguiente manera:

``` pre codeblock
nitroservice.logout();
```

API de configuración

El protocolo NITRO se puede utilizar 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.<resource_type>. Cada uno de estos paquetes o espacios de nombres contiene una clase llamada <resource_type> que proporciona las API para configurar el recurso.

Por ejemplo, el recurso NetScaler tiene el paquete com.citrix.sdx.nitro.resource.config.ns o espacio de nombres.

Una clase de recurso proporciona API para realizar otras operaciones, como la creación de un recurso, la recuperación de detalles y estadísticas del recurso, la actualización de un recurso, la eliminación de recursos y la realización de operaciones masivas en recursos.

**Creación de un recurso**

Para crear un nuevo recurso (por ejemplo, una instancia de Citrix ADC) 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 necesarios 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 static add ().

El siguiente código de ejemplo crea una instancia Citrix ADC denominada “ns_instance” en el dispositivo SDX:

“‘ pre codeblock
ns newns = new ns();

//Set the properties of the NetScaler locally
newns.set_name(“ns_instance”);
newns.set_ip_address(“10.70.136.5”);
newns.set_netmask(“255.255.255.0”);
newns.set_gateway(“10.70.136.1”);
newns.set_image_name(“nsvpx-9.3.45_nc.xva”);
newns.set_profile_name(“ns_nsroot_profile”);
newns.set_vm_memory_total(new Double(2048));
newns.set_throughput(new Double(1000));
newns.set_pps(new Double(1000000));
newns.set_license(“Standard”);
newns.set_username(“admin”);
newns.set_password(“admin”);

 

```
int number_of_interfaces = 2;
network_interface[] interface_array = new network_interface[number_of_interfaces];

//Adding 10/1
interface_array[0] = new network_interface();
interface_array[0].set_port_name("10/1");

//Adding 10/2
interface_array[1] = new network_interface();
interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the Citrix ADC instance
ns result = ns.add(nitroservice, newns);
```

```
### 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:

``` pre codeblock
//Retrieve the resource object from the SDX appliance
ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object
System.out.println(returned_ns[i].get_ip_address());
System.out.println(returned_ns[i].get_netmask());
```

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 Citrix ADC con ID 123456a:


```

“‘ pre codeblock
ns obj = new ns();
obj.set_id(“123456a”);
ns stats = ns.get(nitroservice, obj);
System.out.println(“CPU Usage:” + stats.get_ns_cpu_usage());
System.out.println(“Memory Usage:” + stats.get_ns_memory_usage());
System.out.println(“Request rate/sec:” +stats.get_http_req());

```
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 ID 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 Citrix ADC con ID 123456a a 'ns_instance_new':

``` pre codeblock
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated
update_obj.set_id(”123456a”);

//Get existing NetScaler details
update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to ”ns_instance_new” locally
update_obj.set_name(”ns_instance_new”);

//Upload the updated NetScaler details
ns result = ns.update(nitroservice, update_obj);
```


```

**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.

El siguiente código de ejemplo elimina una instancia de Citrix ADC con ID 1:

“‘ pre codeblock
ns obj = new ns();
obj.set_id(“123456a”);
ns.delete(nitroservice, obj);

```
Operaciones en bloque

Puede consultar o cambiar varios recursos simultáneamente y, por lo
    tanto, minimizar el tráfico de red. Por ejemplo, puede agregar
    varios dispositivos Citrix ADC SDX en la misma operación.

Cada clase de recurso tiene métodos que toman una matriz de recursos
    para agregar, actualizar y quitar recursos. Para realizar una
    operación masiva, especifique los detalles de cada operación
    localmente y, a continuación, envíe los detalles a la 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:

- **Salgan.** Cuando se encuentra el primer error, la ejecución se
    detiene. Se han confirmado los comandos que se ejecutaron antes del
    error.
- **Continúe.** Todos los comandos de la lista se ejecutan incluso si
    algunos comandos fallan.

Nota: Debe configurar el comportamiento requerido al establecer una
    conexión con el dispositivo, estableciendo el parámetro
onerror en el método
nitro_service ().

El siguiente código de ejemplo agrega dos dispositivos NetScaler en una
     operación:

``` pre codeblock
ns[] newns = new ns[2];
```


```

```
20
21 //Specify details of first NetScaler
22 newns[0] = new ns();
23 newns[0].set_name("ns_instance1");
24 newns[0].set_ip_address("10.70.136.5");
25 newns[0].set_netmask("255.255.255.0");
26 newns[0].set_gateway("10.70.136.1");
27 ...
28 ...
29 ...
30
31 //Specify details of second NetScaler
32 newns[1] = new ns();
33 newns[1].set_name("ns_instance2");
34 newns[1].set_ip_address("10.70.136.8");
35 newns[1].set_netmask("255.255.255.0");
36 newns[1].set_gateway("10.70.136.1");
37 ...
38 ...
39
40 //upload the details of the NetScalers to the NITRO server
41 ns[] result = ns.add(nitroservice, newns);
```

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 al procesar la solicitud NITRO.

El campo de mensaje de error proporciona una breve explicación y la naturaleza del error.

Todas las excepciones en la ejecución de las API de NITRO son capturadas por la clase com.citrix.sdx.nitro.exception
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 API disponible en la carpeta <NITRO_SDK_HOME>/doc.

Referencia de comandos SDX

June 19, 2019

Para obtener la lista detallada de los comandos que se pueden utilizar para configurar el dispositivo Citrix ADC SDX a través de la CLI, consulte Referencia de comandos SDX.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States