NetScaler Application Delivery Management 12.1

Machine translated content

Disclaimer

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

Contents

Notas de la versión

January 30, 2024

Las notas de la versión de NetScaler Application Delivery Management (ADM) 12.1 describen las nuevas funciones, las mejoras de las funciones existentes y los problemas conocidos de una compilación. La sección de notas de la versión 12.1 incluye las siguientes secciones:

- **Novedades**: Las nuevas funciones y mejoras de las funciones existentes publicadas en una compilación.
- **Problemas conocidos**: Los problemas que existen en una compilación y sus soluciones, siempre que corresponda.
- **Problemas resueltos**: Los problemas abordados en una compilación.

Para ver el documento completo de notas de la versión, haga clic en el siguiente enlace.

Notas de la versión	Fecha de publicación	Versión
Rutas de publicación para la compilación 62.21 de la versión 12.1 de NetScaler ADM	Publicado: 13 de mayo de 2021	Versión de las notas de versión: 1.0
Rutas de publicación para la compilación 61.18 de la versión 12.1 de NetScaler ADM	Publicado: 04 de febrero de 2021	Versión de las notas de versión: 1.0
Notas de la versión de la compilación 60.16 de la versión 12.1 de NetScaler ADM	Publicado: 06 de Noviembre de 2020	Versión de las notas de versión: 1.0
Notas de la versión de la compilación 59.16 de la versión 12.1 de NetScaler ADM	Publicado: 28 de septiembre de 2020	Versión de las notas de versión: 1.0
Notas de la versión de la compilación 58.14 de la versión 12.1 de NetScaler ADM	Publicado: 20 de agosto de 2020	Versión de las notas de versión: 1.0
Notas de la versión de la compilación 57.18 de la versión 12.1 de NetScaler ADM	Publicado: 11 de junio de 2020	Versión de las notas de versión: 1.0

Notas de la versión	Fecha de publicación	Versión
Notas de la versión de la compilación 56.22 de la versión 12.1 de NetScaler ADM	Publicado: 30 de Marzo de 2020	Versión de las notas de versión: 1.0
Notas de la versión de la compilación 55.13 de la versión 12.1 de NetScaler ADM	Publicado: 07 de Noviembre de 2019	Versión de las notas de versión: 1.0
Notas de la versión de la compilación 54.13 de la versión 12.1 de NetScaler ADM	Publicado: 20 de septiembre de 2019; actualizado el 26 de septiembre	Versión de las notas de versión: 2.0
Notas de la versión de la compilación 53.12 de la versión 12.1 de NetScaler ADM	Publicado: 28 de agosto de 2019	Versión de las notas de versión: 3.0
Notas de la versión de la compilación 52.15 de la versión 12.1 de NetScaler ADM	Publicado: 10 de Junio de 2019	Versión de las notas de versión: 1.0
Notas de la versión de compilación 50.43 de la versión 12.1 de NetScaler ADM	Publicado: 17 de Mayo de 2019	Versión de las notas de versión: 2.0
Notas de la versión de compilación 50.39 de la versión 12.1 de NetScaler ADM	Publicado: 17 de Mayo de 2019	Versión de las notas de versión: 2.0
Notas de la versión de compilación 50.33 de la versión 12.1 de NetScaler ADM	Publicado: 16 de abril de 2019	Versión de las notas de versión: 1.0
Notas de la versión de compilación 50.30 de la versión 12.1 de NetScaler ADM	Publicado: 14 de enero de 2019	Versión de las notas de versión: 1.0
Notas de la versión de compilación 50.28 de la versión 12.1 de NetScaler ADM	Publicado: 1 de diciembre de 2018	Versión de las notas de versión: 1.0
Notas de la versión de compilación 49.23 de la versión 12.1 de NetScaler ADM	Publicado: 29 de agosto de 2018	Versión de las notas de versión: 1.0

Notas de la versión	Fecha de publicación	Versión
Notas de la versión de compilación 48.18 de la versión 12.1 de NetScaler ADM	Publicado: 18 de Junio de 2018	Versión de las notas de versión: 2.0

> **Nota**
>
> Estas notas de la versión no documentan las correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

Introducción

January 30, 2024

En este documento se explica cómo empezar a implementar y configurar NetScaler Application Delivery Management (ADM) por primera vez. Este documento está dirigido a administradores de redes y aplicaciones que administran dispositivos de red Citrix (Citrix SD-WAN WO, NetScaler Gateway, etc.) y también dispositivos de terceros, como HAProxy. Siga los pasos de este documento independientemente del tipo de dispositivo que tenga previsto administrar con NetScaler ADM.

Si ya es usuario de NetScaler ADM, se recomienda revisar las notas de la versión,los requisitos del sistemay los detalles de las licencias antes de actualizar el servidor a la última versión de NetScaler ADM.

Paso 1: Revisar los requisitos del sistema

Antes de empezar a implementar Citrix ADM en su centro de datos, revise los requisitos de software, los requisitos del explorador, la información de puertos, la información de licencias y las limitaciones.

- **Información sobre la licencia**. Puede administrar y supervisar cualquier número de instancias y entidades sin licencia. Sin embargo, solo puede administrar 30 aplicaciones descubiertas y ver la información de análisis de solo 30 servidores virtuales sin aplicar una licencia. Para administrar más de 30 aplicaciones o ver análisis de más de 30 servidores virtuales, debe comprar las licencias apropiadas. Obtenga más información.
- **Requisitos del sistema operativo y del receptor**. Revise esta información para asegurarse de que tiene la versión correcta del receptor para los sistemas operativos compatibles. Obtenga más información.

- **Requisitos del explorador**. Para acceder a la GUI de NetScaler ADM, debe asegurarse de que dispone del explorador necesario y de la versión correcta. Obtenga más información.
- **Puertos**. Asegúrese de que los puertos requeridos estén abiertos para que NetScaler ADM se comunique con las instancias de NetScaler ADC o SD-WAN o con las instancias de NetScaler ADC y SD-WAN. Obtenga más información.
- **Requisitos de instancia de NetScaler ADC**. Las diferentes versiones del software NetScaler ADC admiten diferentes funciones de NetScaler ADM. Revise esta información para asegurarse de que ha actualizado las instancias de NetScaler ADC a la versión correcta. Obtenga más información.
- **Requisitos de instancia Citrix SD-WAN**.Revise esta información para asegurarse de que ha actualizado las instancias de Citrix SD-WAN a la versión correcta y de que dispone de las ediciones de plataforma correctas. Obtenga más información.

Paso 2: Implementar NetScaler ADM

Para administrar y supervisar las aplicaciones y la infraestructura de red, primero debe instalar NetScaler ADM en uno de los hipervisores. Puede implementar NetScaler ADM como un único servidor o en un modo de alta disponibilidad. Si utiliza NetScaler ADC Insight Center, puede migrar a NetScaler ADM y aprovechar las funciones de administración, monitoreo, orquestación y administración de aplicaciones, además de las funciones de análisis.

- **Despliegue**de un solo servidor .En una implementación de un solo servidor de NetScaler ADM, la base de datos se integra con el servidor y un solo servidor procesa todo el tráfico. Puede implementar NetScaler ADM con Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM. Consulte:
  - Citrix ADM con Citrix Hypervisor
  - NetScaler ADM con Microsoft Hyper-V
  - NetScaler ADM con VMware ESXi
  - NetScaler ADM con servidor KVM Linux
- **Implementación de alta disponibilidad.** Una implementación de alta disponibilidad (HA) de dos servidores NetScaler ADM proporciona operaciones ininterrumpidas. En una configuración de alta disponibilidad, ambos nodos de NetScaler ADM deben implementarse en modo activo-pasivo, en la misma subred con la misma versión y compilación de software, y deben tener las mismas configuraciones. Con la implementación de HA, la capacidad de configurar la dirección IP flotante en el nodo principal de NetScaler ADM elimina la necesidad de un equilibrador de carga de NetScaler ADC independiente. Para obtener más información, consulteConfigurar en

una implementación de alta disponibilidad.

Paso 3: Agregar instancias a NetScaler ADM

Las instancias son dispositivos Citrix o dispositivos virtuales o dispositivos de terceros que desea descubrir, administrar y supervisar desde Citrix ADM. Debe agregar instancias al servidor Citrix ADM si quiere administrar y supervisar estas instancias. Puede agregar las siguientes instancias a NetScaler ADM:

- Citrix ADC
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX
  - Citrix Gateway
  - Citrix SD-WAN
- HAProxy

Cuando agrega una instancia al servidor NetScaler ADM, el servidor se comunica implícitamente con las instancias y recopila un inventario de estas instancias.

Más información

Paso 4: Habilitar el análisis en servidores virtuales

Para ver los datos de análisis del flujo de tráfico de su aplicación, debe habilitar la función de análisis en los servidores virtuales que reciben tráfico para las aplicaciones específicas.

Más información

Paso 5: Configurar el servidor NTP en NetScaler ADM

Configure un servidor de Protocolo de tiempo de red (NTP) en NetScaler ADM para sincronizar su reloj con el servidor NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

Más información

Paso 6: Configurar la configuración del sistema para un rendimiento óptimo de NetScaler ADM

Antes de empezar a usar NetScaler ADM para administrar y supervisar sus instancias y aplicaciones, se recomienda configurar algunos parámetros del sistema que garanticen un rendimiento óptimo del servidor NetScaler ADM.

- **Configure las alarmas del sistema**. Debe configurar las alarmas del sistema para asegurarse de que conoce cualquier problema crítico o importante del sistema. Por ejemplo, es posible que quiera recibir una notificación si el uso de CPU es alto o si hay varios errores de inicio de sesión en el servidor.
- **Configure las notificaciones del sistema**. Puede enviar notificaciones a grupos de usuarios seleccionados para diversas funciones relacionadas con el sistema. Puede configurar un servidor de notificaciones en NetScaler ADM y configurar servidores de Gateway de correo electrónico y servicio de mensajes cortos (SMS) para enviar notificaciones de correo electrónico y texto a los usuarios. Esto garantiza que se le notifique cualquier actividad a nivel del sistema, como el inicio de sesión del usuario o el reinicio del sistema.
- **Configure las opciones de poda del sistema**.Para limitar la cantidad de datos de informes que se almacenan en la base de datos del servidor NetScaler ADM, puede especificar el intervalo durante el que quiere que NetScaler ADM conserve los datos de informes de red, los eventos, los registros de auditoría y los registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).
- **Configure las opciones de copia de seguridad del sistema**. NetScaler ADM realiza automáticamente una copia de seguridad del sistema todos los días a las 00:30 horas. De forma predeterminada, guarda tres archivos de copia de seguridad. Es posible que desee conservar un mayor número de copias de seguridad del sistema.
- **Configure las opciones de copia de seguridad de instancia**. Si realiza una copia de seguridad del estado actual de una instancia de NetScaler ADC, puede usar los archivos de copia de seguridad para restaurar la estabilidad en caso de que la instancia se vuelva inestable. Hacerlo es especialmente importante antes de realizar una actualización. De forma predeterminada, se realiza una copia de seguridad cada 12 horas y se conservan tres archivos de respaldo en el sistema.
- **Configure los parámetros de poda del evento de instancia**.Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos del servidor NetScaler ADM, puede especificar el intervalo durante el que quiere que NetScaler ADM conserve los datos de informes de red, los eventos, los registros de auditoría y los registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00:00 horas).
- **Configure la configuración de purga del syslog de la instancia**. Para limitar la cantidad de

datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog. Puede especificar el número de días tras los que se eliminarán los siguientes datos de syslog de NetScaler ADM:

- Datos genéricos de Syslog
- Datos de AppFirewall
- Datos de NetScaler Gateway.

  Más información

A continuación

Una vez que haya implementado y configurado NetScaler ADM, puede empezar a administrar y monitorear sus instancias y aplicaciones.

Administración de instancias y aplicaciones de Citrix ADC. Todas las funciones de NetScaler ADM son compatibles con las instancias de NetScaler ADC. Puede empezar a utilizar cualquiera de las funciones.

Administración de instanciasde SD-WAN de Citrix ADC . No todas las funciones de NetScaler ADM son compatibles con las instancias WO de SD-WAN; por ejemplo, no se admite la administración de certificados o la auditoría de configuración. Para obtener información sobre qué funciones se admiten y cómo usarlas, consulte Administración de WO de Citrix SD-WAN con NetScaler ADM.

Gestión de instancias y aplicaciones de HAProxy. Puede supervisar los front-ends, los back-ends y los servidores configurados en una implementación de HAProxy. También puede utilizar la función Administración de aplicaciones para supervisar las estadísticas en tiempo real de los front-end supervisados por NetScaler ADM. Para obtener más información sobre las funciones compatibles con HAProxy y cómo usarlas, consulte Administración y supervisión de instancias de HAProxy mediante NetScaler ADM.

Todos los artículos

January 30, 2024

Los «artículos prácticos» de Citrix Application Delivery Management (Citrix ADM) son artículos sencillos, relevantes y fáciles de implementar sobre las funciones de Citrix ADM. Estos artículos contienen información sobre algunas de las funciones más populares de NetScaler ADM, como la administración de instancias, la administración de aplicaciones, los StyleBooks, la administración de certificados y Analytics.

Haga clic en el nombre de una función en la tabla siguiente para ver la lista de artículos prácticos sobre esa función.

		Temas	
Administración de instancias	Gestión de eventos	StyleBooks	Administración de certifi
Administración de aplicaciones	Administración de la configuración	Autenticación	Análisis

Administración de instancias

Cómo supervisar sitios distribuidos globalmente

Cómo administrar las particiones de administración de las instancias de NetScaler ADC

Cómo agregar instancias a NetScaler ADM

Cómo crear grupos de instancias en NetScaler ADM

Cómo configurar sitios para Geomaps en NetScaler ADM

Cómo forzar una conmutación por error a la instancia secundaria de NetScaler ADC mediante NetScaler ADM

Cómo forzar que una instancia secundaria de NetScaler ADC permanezca secundaria mediante NetScaler ADM

Cómo hacer copias de seguridad y restaurar una instancia mediante NetScaler ADM

Cómo utilizar el panel de control de NetScaler ADM para supervisar una instancia de HAProxy

Cómo mostrar los detalles de las interfaces configuradas en las instancias de HAProxy

Cómo mostrar los detalles de los backends configurados en las instancias de HAProxy

Cómo mostrar los detalles de los servidores configurados en las instancias de HAProxy

Cómo reiniciar una instancia de HAProxy desde NetScaler ADM

Cómo hacer una copia de seguridad y restaurar una instancia de HAProxy mediante NetScaler ADM

Cómo editar el archivo de configuración de HAProxy mediante Citrix ADM

Cómo redescubrir varias instancias de NetScaler ADC VPX

Cómo sondear instancias y entidades de NetScaler ADC en NetScaler ADM

Cómo desadministrar una instancia en NetScaler ADM

Cómo rastrear la ruta a una instancia desde NetScaler ADM

Administración de la configuración

Cómo crear un trabajo de configuración en NetScaler ADM

Cómo usar el comando SCP (put) en trabajos de configuración

Cómo actualizar instancias de NetScaler ADC SDX mediante NetScaler ADM

Cómo programar los trabajos creados mediante plantillas integradas en NetScaler ADM

Cómo reprogramar trabajos configurados mediante plantillas integradas en NetScaler ADM

Cómo reutilizar los trabajos de configuración ejecutados

Cómo actualizar instancias de NetScaler ADC con NetScaler ADM

Cómo usar variables en trabajos de configuración en NetScaler ADM

Cómo usar plantillas de configuración para crear plantillas de auditoría en NetScaler ADM

Cómo crear trabajos de configuración a partir de comandos correctivos en NetScaler ADM

Cómo replicar los comandos de configuración en ejecución y guardados de una instancia de NetScaler ADC a otra en NetScaler ADM

Cómo crear trabajos de configuración para instancias WO de Citrix SD-WAN de Citrix en NetScaler ADM

Cómo utilizar Record-and-Play para crear trabajos de configuración

Cómo utilizar trabajos de configuración para replicar la configuración de una instancia a varias instancias

Cómo utilizar la plantilla de configuración maestra en NetScaler ADM

Cómo sondear la auditoría de configuración de las instancias de NetScaler ADC

Cómo reutilizar las plantillas de auditoría de configuración en los trabajos de configuración

Cómo importar y exportar plantillas de configuración

Cómo generar una diferencia de auditoría de configuración para las trampas SNMP de ConfigChange

Administración de certificados

Cómo configurar una directiva empresarial en NetScaler ADM

Cómo instalar certificados SSL en una instancia de NetScaler ADC desde NetScaler ADM

Cómo actualizar un certificado instalado desde NetScaler ADM

Cómo vincular y desvincular certificados SSL mediante NetScaler ADM

Cómo crear una solicitud de firma de certificados (CSR) mediante NetScaler ADM

Cómo configurar notificaciones para la caducidad de certificados SSL desde NetScaler ADM

Cómo utilizar el panel SSL en NetScaler ADM

Cómo sondear certificados SSL desde instancias NetScaler ADC

Administración de aplicaciones

Cómo crear una definición de aplicación en Citrix ADM

StyleBooks

Cómo ver diferentes grupos de StyleBooks

Cómo utilizar los StyleBooks suministrados con Citrix ADM

Cómo crear sus propios StyleBooks

Cómo usar StyleBooks definidos por el usuario en NetScaler ADM

Cómo usar la API para crear configuraciones a partir de StyleBooks

Cómo habilitar análisis y configurar alarmas en un servidor virtual definido en un StyleBook

Cómo crear un StyleBook para subir archivos a NetScaler ADM

Cómo usar la API para crear configuraciones para cargar cualquier tipo de archivo

Cómo crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM

Cómo usar la API para crear configuraciones para cargar archivos de certificados y claves

Cómo usar Microsoft Skype Empresarial StyleBook en empresas empresariales

Cómo utilizar Microsoft Exchange StyleBook en empresas comerciales

Cómo usar Microsoft SharePoint StyleBook en empresas empresariales

Análisis

Cómo habilitar el análisis en las instancias

Cómo configurar umbrales adaptativos

Cómo configurar la administración de SLA

Cómo configurar el resumen de bases de datos para análisis

Cómo crear umbrales y alertas con NetScaler ADM

Cómo inhabilitar la recopilación de datos de URL para el análisis desde Citrix ADM

Cómo ver el tipo de vídeos transmitidos y el volumen de datos consumido de la red

Cómo ver la velocidad máxima de datos para un período de tiempo determinado

Cómo comparar la cantidad optimizada y no optimizada de reproducciones de vídeos ABR

Cómo comparar el tiempo de reproducción optimizado y no optimizado de los vídeos ABR

Cómo comparar el consumo de ancho de banda de vídeos ABR optimizados y no optimizados

Cómo comparar el volumen de datos utilizado por los vídeos ABR optimizados y no optimizados

Cómo ver la eficiencia de la red

Gestión de eventos

Cómo configurar la edad de los eventos en NetScaler ADM

Cómo programar un filtro de eventos mediante NetScaler ADM

Cómo configurar notificaciones de correo electrónico repetidas para eventos de NetScaler ADM

Cómo suprimir eventos mediante NetScaler ADM

Cómo utilizar el panel de eventos para supervisar eventos

Cómo crear reglas de eventos en Citrix ADM

Cómo modificar la gravedad reportada de los eventos que ocurren en instancias de NetScaler ADC

Cómo ver el resumen de eventos en NetScaler ADM

Cómo mostrar la gravedad de los eventos y los sesgos de las trampas de SNMP en NetScaler ADM

Cómo exportar mensajes syslog mediante NetScaler ADM

Cómo suprimir los mensajes de syslog en NetScaler ADM

Cómo configurar los ajustes de poda para eventos de ejemplo

Autenticación

Cómo conectar en cascada servidores de autenticación externos

Cómo agregar servidores de autenticación RADIUS

Cómo agregar servidores de autenticación LDAP

Cómo agregar servidores de autenticación TACACS

Cómo extraer el grupo de servidores de autenticación en NetScaler ADM

Cómo habilitar la autenticación local de reserva

Sistema NetScaler ADM

Cómo actualizar NetScaler ADM

Cómo restablecer la contraseña para Citrix ADM

Cómo generar un archivo de soporte técnico para NetScaler ADM

Cómo hacer copias de seguridad y restaurar su servidor NetScaler ADM en una implementación de un solo servidor

Cómo hacer una copia de seguridad y restaurar una configuración de NetScaler ADM en un par HA

Cómo habilitar el acceso a la consola para usuarios no predeterminados en NetScaler ADM

Cómo configurar el servidor NTP en NetScaler ADM

Cómo configurar la configuración de SSL para NetScaler ADM

Cómo configurar el intervalo de purga de syslog para NetScaler ADM

Cómo ver la información de auditoría de NetScaler ADM

Cómo configurar los ajustes de notificación del sistema de NetScaler ADM

Cómo supervisar el uso de la CPU, la memoria y el disco de NetScaler ADM

Cómo configurar un grupo de cifrado para NetScaler ADM

Cómo crear trampas, administradores y usuarios de SNMP en NetScaler ADM

Cómo asignar un nombre de host a un servidor NetScaler ADM

Cómo configurar los ajustes de poda del sistema para NetScaler ADM

Cómo configurar los ajustes de copia de seguridad del sistema mediante NetScaler ADM

Cómo configurar y ver alarmas del sistema en NetScaler ADM

Cómo diagnosticar y solucionar problemas de instancias de Citrix ADC

Funciones de red

Cómo generar informes para entidades de equilibrio de carga

Cómo exportar o programar la exportación de informes de funciones de red

Overview

January 30, 2024

Citrix Application Delivery Management (ADM) es una solución de administración centralizada que simplifica las operaciones al proporcionar a los administradores visibilidad en toda la empresa y automatizar los trabajos de administración que deben ejecutarse en varias instancias. Puede administrar y supervisar los productos de red de aplicaciones Citrix que incluyen NetScaler ADC MPX, NetScaler ADC VPX, NetScaler ADC SDX, NetScaler ADC CPX, NetScaler Gateway y Citrix SD-WAN. Puede usar ADM para administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada.

ADM es un dispositivo virtual que se ejecuta en Citrix Hypervisor, VMware ESXi y Linux KVM. ADM aborda el desafío de la visibilidad de las aplicaciones mediante la recopilación de la siguiente información detallada sobre el tráfico de aplicaciones web y escritorios virtuales:

- información de nivel de sesión de usuario
- datos de rendimiento de la página web
- información de base de datos que fluye a través de las instancias ADC en su sitio y proporciona informes prácticos.

ADM permite a los administradores de TI solucionar problemas y supervisar de forma proactiva los problemas de los clientes en cuestión de minutos.

Funciones y soluciones

January 30, 2024

NetScaler Application Delivery Management (ADM) ofrece las siguientes funciones:

Gestión y análisis de aplicaciones

Análisis del rendimiento de las aplicaciones

App Score es el producto de un sistema de puntuación que define el rendimiento de una aplicación. Muestra si la aplicación está funcionando bien en términos de capacidad de respuesta, no es vulnerable a las amenazas y tiene todos los sistemas en funcionamiento.

Análisis de seguridad de aplicaciones

El Panel de seguridad de aplicaciones proporciona una vista holística del estado de seguridad de sus aplicaciones. Por ejemplo, muestra métricas de seguridad clave, como infracciones de seguridad, infracciones de firmas, índices de amenazas. El panel de seguridad de la aplicación también muestra información relacionada con los ataques, como los ataques de sincronización, los ataques de ventanas pequeñas y los ataques de inundación de DNS para las instancias de ADC descubiertas.

Redes

Instances

Le permite administrar las instancias de Citrix ADC, Citrix Gateway, Citrix SD-WAN y HAProxy.

Grupos de instancias

Le permite agrupar sus instancias de la siguiente manera:

- Grupo estático: le permite definir un grupo de dispositivos que puede utilizar en diferentes tareas, como trabajos de configuración, etc.
- Bloqueo de IP privado: permite agrupar las instancias en función de las ubicaciones geográficas.

Gestión de eventos

Cuando la dirección IP de una instancia ADC se agrega a ADM, ADM envía una llamada NITRO y se agrega implícitamente como destino de captura para que la instancia reciba sus capturas o eventos.

Los eventos representan ocurrencias de eventos o errores en una instancia de ADC administrada.

Administración de certificados

Citrix ADM ahora optimiza todos los aspectos de la administración de certificados por usted. A través de una sola consola, puede establecer directivas automatizadas para garantizar el emisor correcto, la fortaleza de la clave y los algoritmos correctos, al tiempo que mantiene una estrecha ficha sobre los certificados que no se utilizan o que caducan pronto. Para empezar a utilizar el panel de control SSL de ADM y sus funcionalidades, debe comprender qué es un certificado SSL y cómo puede utilizar ADM para realizar un seguimiento de sus certificados SSL.

Administración de la configuración

NetScaler ADM le permite crear trabajos de configuración que lo ayuden a realizar tareas de configuración, como la creación de entidades, la configuración de funciones, la replicación de cambios de configuración, las actualizaciones del sistema y otras actividades de mantenimiento con facilidad en varias instancias. Los trabajos de configuración y las plantillas simplifican las tareas administrativas más repetitivas en una sola tarea en ADM.

Auditoría de configuración

Permite supervisar e identificar anomalías en las configuraciones de las instancias.

- Consejos de configuración: le permite identificar una anomalía en la configuración.
- Plantilla de auditoría: permite supervisar los cambios en una configuración específica.

Informes de red

Puede optimizar el uso de los recursos supervisando los informes de su red en ADM.

Análisis

Información web

Proporciona visibilidad de las aplicaciones web empresariales y permite a los administradores de TI supervisar todas las aplicaciones web que ofrece NetScaler ADC al proporcionar una supervisión integrada y en tiempo real de las aplicaciones. Web Insight proporciona información crítica, como el tiempo de respuesta del usuario y del servidor, lo que permite a las organizaciones de TI supervisar y mejorar el rendimiento de las aplicaciones.

HDX Insight

Proporciona visibilidad de extremo a extremo del tráfico ICA que pasa por NetScaler ADC. HDX Insight permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento.

Gateway Insight

Proporciona visibilidad sobre los errores que encuentran los usuarios al iniciar sesión, independientemente del modo de acceso. Puede ver una lista de usuarios que han iniciado sesión en un momento determinado, junto con el número de usuarios activos, el número de sesiones activas y los bytes y licencias utilizados por todos los usuarios en un momento determinado.

Security Insight

Proporciona una solución de panel único que le ayuda a evaluar el estado de seguridad de sus aplicaciones y a tomar medidas correctivas para protegerlas.

Insight SSL

SSL Insight proporciona visibilidad de las transacciones web seguras (HTTPS) y permite a los administradores de TI monitorear todas las aplicaciones web seguras que ofrece NetScaler ADC al proporcionar una supervisión histórica e integrada en tiempo real de las transacciones web seguras.

Información TCP

TCP Insight proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias (o algoritmos) de control de la congestión utilizadas en las instancias de ADC a fin de evitar la congestión de la red en la transmisión de datos.

Video Insight

La función Video Insight proporciona una solución sencilla y escalable para monitorear las métricas de las técnicas de optimización de vídeo utilizadas por las instancias de NetScaler ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa.

WAN Insight

El análisis de WAN Insight permite a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre los dispositivos de optimización WAN del centro de datos y las sucursales. WAN Insight también proporciona visibilidad de los clientes, las aplicaciones y las sucursales de la red, para ayudar a solucionar los problemas de la red de manera eficaz.

Orchestration

Orquestación en la nube

Permite la integración de los productos NetScaler ADC con la orquestación en la nube de OpenStack. NetScaler ADM y OpenStack implementan las API de cada uno, lo que permite la integración de la función de equilibrio de carga (LBaaS) de la instancia de NetScaler ADC con la orquestación en la nube de OpenStack.

Orchestration

Citrix ADM admite SDN en redes empresariales al integrarse con los controladores SDN de diferentes proveedores. ADM admite VMware NSX Manager y Cisco Application Policy Infrastructure Controller (APIC).

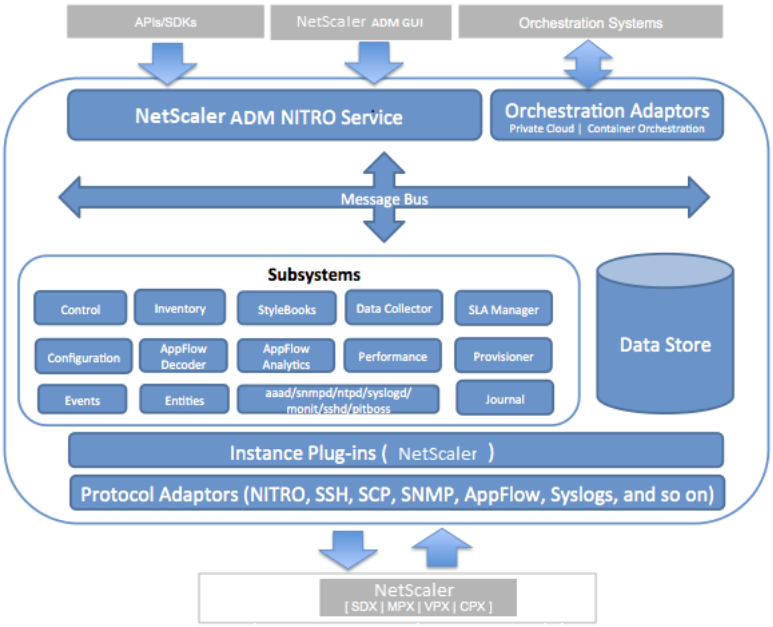
Arquitectura

January 30, 2024

La base de datos Citrix Application Delivery Management (ADM) está integrada con el servidor y el servidor administra todos los procesos clave, como la recopilación de datos y las llamadas NITRO. En su almacén de datos, el servidor almacena un inventario de los detalles de la instancia, como el nombre del host, la versión del software, la configuración guardada y en ejecución, los detalles del certificado y las entidades configuradas en la instancia. La implementación de un solo servidor es adecuada si desea procesar pequeñas cantidades de tráfico o almacenar datos durante un tiempo limitado.

Actualmente, ADM admite dos tipos de implementaciones de software: servidor único y alta disponibilidad.

La siguiente imagen muestra los diferentes subsistemas dentro de ADM y cómo ocurre la comunicación entre el servidor ADM y las instancias administradas.



El subsistema de servicio de ADM actúa como un servidor web que gestiona las solicitudes y respuestas HTTP que se envían a los subsistemas de ADM desde la GUI o la API, mediante los puertos 80 y 443. Estas solicitudes se envían a los subsistemas a través del bus de mensajes (sistema de procesamiento de mensajes) mediante el mecanismo IPC (comunicación entre procesos). Se envía una solicitud al subsistema Control, que procesa la información o la envía al subsistema correspondiente. Cada uno de los demás subsistemas (Inventory, Stylebooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Performance, Events, Entities, SLA Manager, Provisioner y Journal) tiene una función específica.

Los complementos de instancia son bibliotecas compartidas que son exclusivas de cada tipo de instancia admitido por ADM. La información se transfiere entre ADM y las instancias administradas mediante llamadas NITRO o mediante el protocolo SNMP, Secure Shell (SSH) o Secure Copy (SCP). Esta información se procesa y almacena en la base de datos interna (data store).

Cómo descubre NetScaler ADM instancias

January 30, 2024

Las instancias son dispositivos Citrix o dispositivos virtuales que desea detectar, administrar y supervisar desde Citrix Application Delivery Management (ADM). Para administrar y monitorear estas instancias, debe agregarlas al servidor NetScaler ADM. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a ADM:

- Instancias de Citrix ADC

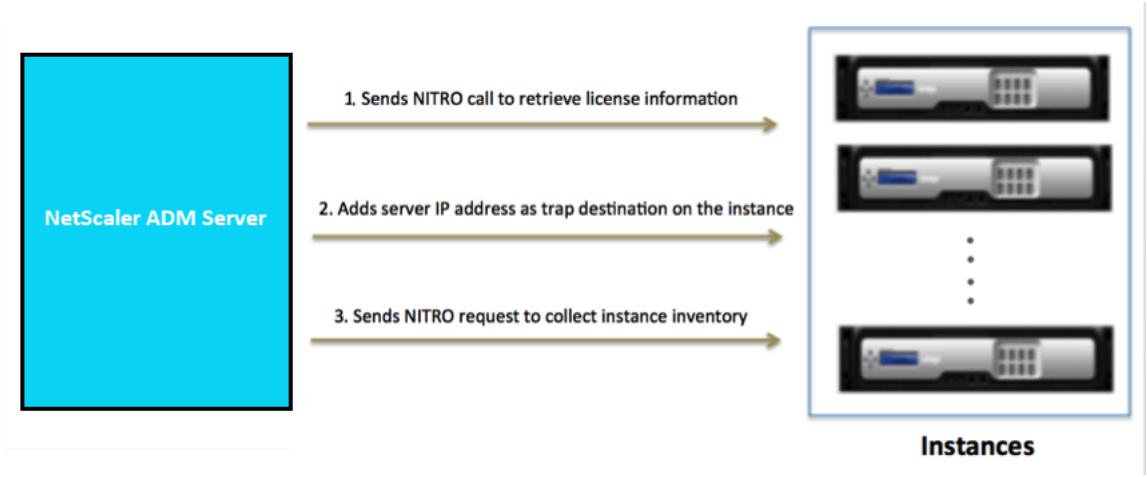
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
- Instancias de NetScaler Gateway
- Instancias de Citrix SD-WAN

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde.

> **Nota**
>
> Citrix ADM utiliza la dirección IP de NetScaler (NSIP) de las instancias Citrix ADC para la comunicación. ADM también puede detectar instancias ADC con dirección IP de subred (SNIP) que tiene habilitado el acceso de administración. Para obtener información sobre los puertos que deben estar abiertos entre las instancias de ADC y ADM, consulte Puertos.
>
> Para Citrix SD-WAN WO, ADM utiliza la dirección IP de administración de las instancias para la comunicación.
>
> No puede agregar instancias de Citrix SD-WAN SE/PE en ADM. Puede configurar ADM como un recopilador AppFlow en los dispositivos Citrix SD-WAN SE/PE.

Cuando agrega una instancia al servidor ADM, el servidor se agrega implícitamente como destino de captura para la instancia y recopila el inventario de la instancia.

El siguiente diagrama describe cómo ADM descubre y agrega instancias implícitamente.



Como se muestra en el diagrama, Citrix ADM realiza los siguientes pasos de forma implícita.

1. NetScaler ADM utiliza los detalles del perfil de instancia para iniciar sesión en la instancia. Mediante una llamada de ADC NITRO, ADM recupera la información de licencia de la instancia. En

función de la información de licencias, determina si la instancia es una instancia de ADC y el tipo de plataforma ADC (por ejemplo, Citrix ADC MPX, ADC VPX, ADC SDX o Citrix Gateway). Al detectar correctamente la instancia, se agrega a la base de datos de ADM.

Para las instancias de Citrix SD-WAN WO, ADM no detecta la instancia mediante la información de licencias. Envía una solicitud NITRO a la instancia para comprobar el tipo y la versión de la instancia.

Este paso puede fallar si el perfil de instancia no incluye las credenciales correctas. En el caso de las instancias ADC MPX, ADC VPX, ADC SDX y Citrix Gateway, este paso también puede fallar si las licencias no se aplican a la instancia.

> **Nota**
>
> Con HTTP, puede agregar todas las instancias a ADM incluso si las licencias no están configuradas en las instancias.

2. ADM agrega su dirección IP a la lista de destinos de captura de la instancia. Esto permite que ADM reciba las trampas generadas en la instancia de ADC.

   Este paso puede fallar si el número de destinos de captura de la instancia supera el límite máximo de destinos de captura. El límite máximo de instancias es de 20.

   Para las instancias de Citrix SD-WAN WO, ADM agrega su dirección IP como administrador SNMP en la instancia.

3. ADM recopila el inventario de la instancia mediante el envío de una solicitud NITRO. Recopila detalles de la instancia, como el nombre de host, la versión de software, la configuración en ejecución y guardada, los detalles del certificado, las entidades configuradas en la instancia, etc.

   Este paso puede fallar debido a problemas de red o firewall.

   Para aprender a agregar instancias a ADM, consulte Agregar instancias.

Visión general de sondeo

January 30, 2024

El sondeo es un proceso en el que Citrix Application Delivery Management (ADM) recopila determinada información de las instancias de Citrix ADC. Es posible que haya configurado varias instancias de Citrix ADC para su organización en todo el mundo. Para supervisar sus instancias a través de Citrix ADM, Citrix ADM debe recopilar determinada información, como el uso de la CPU, el uso de la memoria, los certificados SSL, las funciones con licencia, los tipos de licencia, etc., de todas las instancias

de ADC administradas. Los siguientes son los diferentes tipos de sondeo que se producen entre ADM y las instancias administradas:

- Sondeo de instancias
- Encuesta de inventario
- Colección de datos de rendimiento
- Encuesta de respaldo de instancias
- Encuesta de auditoría de configuración
- Sondeo de certificados SSL
- Sondeo de entidades

Citrix ADM utiliza protocolos como NITRO call, Secure Shell (SSH) y Secure Copy (SCP) para sondear la información de las instancias de Citrix ADC.

Cómo Citrix ADM sondea las instancias y entidades administradas

De forma predeterminada, Citrix ADM sondea automáticamente a intervalos regulares. Citrix ADM también le permite configurar los intervalos de sondeo para algunos tipos de sondeo y permite realizar sondeos manualmente cuando sea necesario.

La siguiente tabla describe los detalles de los tipos de sondeo, el intervalo de sondeo, el protocolo utilizado, etc.:

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Sondeo de instancias	Cada 5 minutos (de forma predeterminada)	Información estadística, como el estado, las solicitudes HTTP por segundo, el uso de la CPU, el uso de la memoria y el rendimiento.	Llamada NITRO.	No

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Encuesta de inventario	Cada 30 minutos (de forma predeterminada)	Detalles del inventario, como la versión de compilación, la información del sistema, las funciones con licencia y los modos.	Llamadas NITRO y SSH	No
Colección de datos de rendimiento	Cada 5 minutos (de forma predeterminada)	Información de informes de red	Llamada NITRO	No
Encuesta de respaldo de instancias	Cada 12 horas (por defecto)	Archivo de respaldo del estado actual de las instancias de ADC administradas	Llamadas NITRO, SSH y SCP.	Sí. Desplácese a **Redes** > **Instancias** > **NetScaler ADC**. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Copia de seguridad/restauración**.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Encuesta de auditoría de configuración	Cada 10 horas (por defecto)	Cambios de configuración que se producen en las instancias de ADC (por ejemplo, configuración en ejecución o configuración guardada)	Llamada SSH, SCP y NITRO	Sí. Vaya a **Redes** > **Auditoría de configuración**. En la página Auditoría de configuración, haga clic en **Configuración** y configure el intervalo de sondeo para el sondeo de auditoría de configuración. Puede sondear las auditorías de configuración manualmente y agregar todas las auditorías de configuración de las instancias inmediatamente a Citrix ADM. Para ello, vaya a **Redes** > **Auditoría de configuración** y haga clic en **Sondear ahora**. La página **Sondear ahora** le permite sondear todas las instancias o seleccionadas de la red.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
sondeo de certificados SSL	Cada 24 horas (de forma predeterminada)	Certificados SSL que se instalan en las instancias de Citrix ADC.	Llamadas NITRO y SCP	Sí. Vaya a **Redes** > **Panel de SSL**. En la página Tablero SSL, haga clic en **Configuración** para configurar el intervalo de sondeo Puede sondear los certificados SSL manualmente y agregar todos los certificados de las instancias inmediatamente a Citrix ADM. Para ello, vaya a **Redes** > **Tablero SSL** y haga clic en **Sondear ahora**. La página **Sondear ahora** le permite sondear todas las instancias o seleccionadas de la red.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Sondeo de entidades	Cada 30 minutos (de forma predeterminada)	Todas las entidades configuradas en las instancias. Una entidad es una directiva, un servidor virtual, un servicio o una acción asociada a una instancia de ADC.	NITRO llama.	Sí, pero no se puede establecer en menos de 10 minutos. Para configurar, vaya a **Redes** > **Funciones de red**. En la página Función de redes, haga clic en **Configuración** para configurar el intervalo de sondeo. Puede sondear entidades manualmente y agregar todas las entidades de las instancias inmediatamente a Citrix ADM. Para ello, vaya a **Redes** > **Funciones de red** y haga clic en **Sondear ahora**. La página **Sondear ahora** le permite sondear todas las instancias o seleccionadas de la red

> **Nota**
>
> Además del sondeo, Citrix ADM recibe eventos generados por instancias de ADC administradas a través de capturas SNMP enviadas a las instancias. Por ejemplo, se genera un evento cuando hay un error del sistema o un cambio en la configuración.
>
> Durante la copia de seguridad de la instancia, se descargan en Citrix ADM los archivos SSL, los archivos de certificados de CA, las plantillas de ADC, la información de la base de datos, Durante una auditoría de configuración, los archivos ns.conf se descargan y almacenan en el sistema de archivos. Toda la información recopilada de las instancias administradas de Citrix ADC se almacena internamente en la base de datos.

Diferentes formas de sondear instancias

A continuación se muestran las diferentes formas de sondeo que Citrix ADM realiza en las instancias administradas:

- Sondeo global de instancias
- Sondeo manual de instancias
- Encuesta manual de entidades

Sondeo global de instancias

Citrix ADM sondea automáticamente todas las instancias administradas en la red, dependiendo del intervalo configurado por usted. Aunque el intervalo de sondeo predeterminado es de 30 minutos, puede configurarlo en función de sus requisitos navegando a **Redes** > **Funciones de red** > **Configuración**.

Sondeo manual de instancias

Cuando Citrix ADM administra muchas entidades, el ciclo de sondeo tarda más tiempo en generar el informe, lo que podría dar como resultado una pantalla en blanco o que el sistema siguiera mostrando datos anteriores.

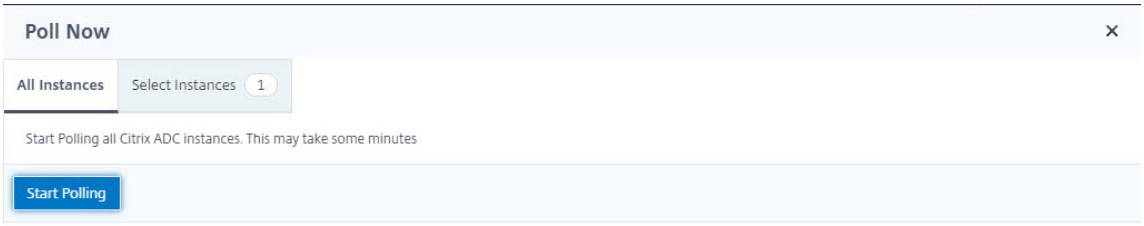
En Citrix ADM, hay un período mínimo de intervalo de sondeo en el que no se realiza el sondeo automático. Si agrega una nueva instancia de Citrix ADC o si se actualiza una entidad, Citrix ADM no reconoce la nueva instancia ni las actualizaciones realizadas en una entidad hasta que se realice el siguiente sondeo. Además, no hay forma de obtener inmediatamente una lista de direcciones IP virtuales para futuras operaciones. Debe esperar a que transcurra el intervalo mínimo de sondeo. Si bien puede realizar una encuesta manual para descubrir las instancias recién agregadas, esto lleva a que

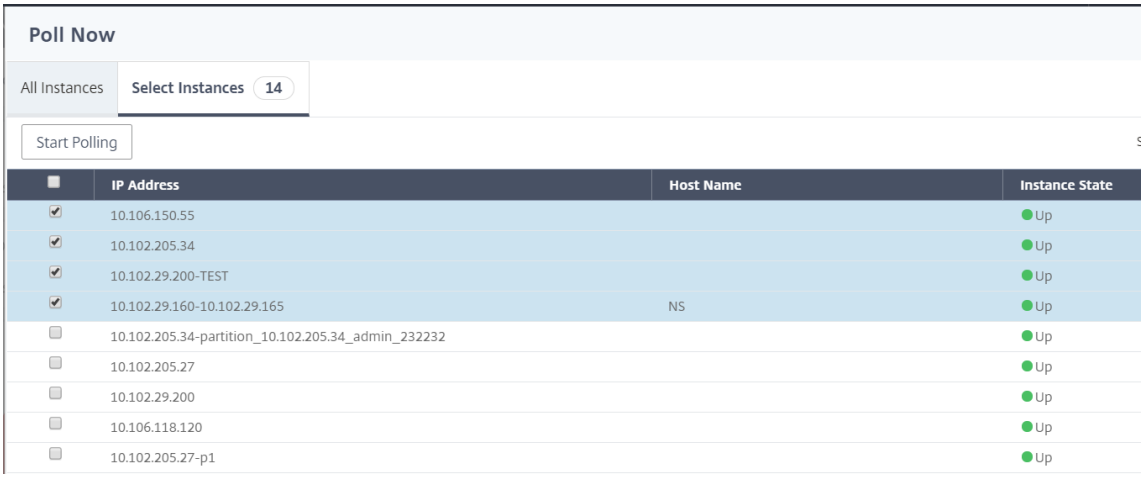
se sondee toda la red NetScaler, lo que genera una carga pesada en la red. En lugar de sondear toda la red, Citrix ADM ahora le permite sondear solo instancias y entidades seleccionadas en un momento dado.

Citrix ADM sondea automáticamente las instancias administradas para recopilar información a determinadas horas del día. El sondeo seleccionado reduce el tiempo de actualización que requiere Citrix ADM para mostrar el estado más reciente de las entidades enlazadas a estas instancias seleccionadas.

Para sondear instancias específicas en Citrix ADM:

1. En Citrix ADM, vaya a **Redes** > **Funciones de red**.
2. En la página **Funciones de red**, en la esquina superior derecha, haga clic en **Sondear ahora**.
3. La página emergente **Poll Now** ofrece la opción de sondear todas las instancias de Citrix ADC de la red o sondear las instancias seleccionadas.
    a) Ficha**Todas las instancias**: haga clic en **Iniciar sondeo** para sondear todas las instancias.
    b) **Seleccione la ficha Instancias**: seleccione las instancias de la lista
4. Haga clic en **Iniciar sondeo**.





Citrix ADM inicia el sondeo manual y agrega todas las entidades.

Encuesta manual de entidades

Citrix ADM también le permite sondear solo unas pocas entidades seleccionadas que están enlazadas a una instancia determinada. Por ejemplo, puede utilizar esta opción para conocer el estado más reciente de una entidad concreta en una instancia. En tal caso, no necesita sondear la instancia como un todo para conocer el estado de una entidad actualizada. Al seleccionar y sondear una entidad, nCitrix ADM sondea solo esa entidad y actualiza el estado en la GUI de Citrix ADM.

Considere un ejemplo de un servidor virtual que está INACTIVO . Es posible que el estado de ese servidor virtual haya cambiado a ACTIVO antes de que se realice el siguiente sondeo automático. Para ver el estado modificado del servidor virtual, es posible que desee sondear solo ese servidor virtual para que se muestre inmediatamente el estado correcto en la GUI.

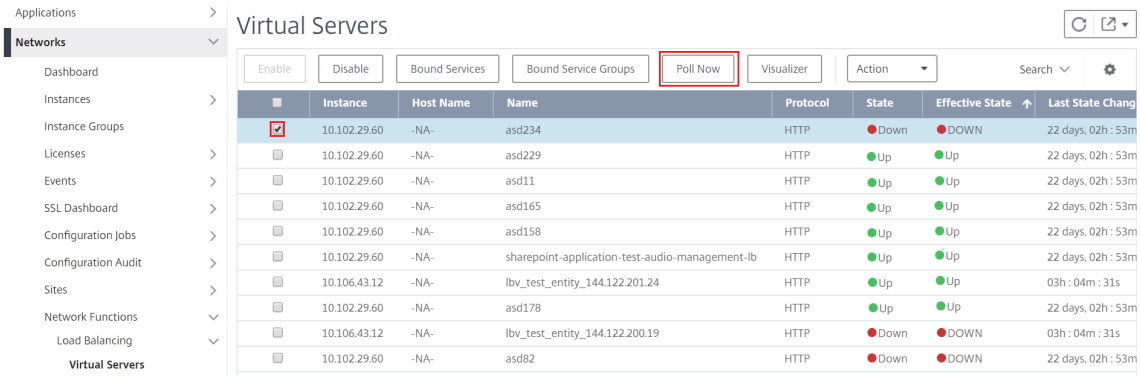
Ahora puede sondear las siguientes entidades para detectar cualquier actualización en su estado: servicios, grupos de servicios, servidores virtuales de equilibrio de carga, servidores virtuales de reducción de caché, servidores virtuales de conmutación de contenido, servidores virtuales de autenticación, servidores virtuales VPN, servidores virtuales GSLB y servidores de aplicaciones.

> **Nota**
>
> Si sondea un servidor virtual, solo se sondea ese servidor virtual. Las entidades asociadas, como servicios, grupos de servicios y servidores, no se sondean. Si necesita sondear todas las entidades asociadas, debe sondear manualmente las entidades o debe sondear la instancia.

Para sondear entidades específicas en Citrix ADM:

Por ejemplo, esta tarea le ayuda a sondear los servidores virtuales de equilibrio de carga. Del mismo modo, también puede sondear otras entidades de función de red.

1. En Citrix ADM, vaya a**Redes** > **Funciones de red** > **Equilibrio de carga** > **Servidores virtuales**.
2. Seleccione el servidor virtual que muestra el estado como DOWN y haga clic en **Sondear ahora**. El estado del servidor virtual ahora cambia a ACTIVO .



Gobierno de datos

January 30, 2024

La autenticación de clientes es de vital importancia para una organización porque permite a la organización proteger sus recursos de red al permitir que solo los clientes o usuarios autenticados accedan a su red. Como administrador, es importante que identifique a los usuarios antes de permitir que se conecten a los recursos de la red Citrix.

A partir de la versión 50.x de la versión 12.1, Citrix Application Delivery Management (ADM) requiere que se autentique en la GUI de ADM antes de empezar a acceder a la información. Es un requisito registrarse en los servicios en la nube de Citrix antes de autenticarse en ADM. Debe proporcionar las credenciales de usuario de Citrix Cloud en la GUI de ADM. Para obtener más información, consulte Inscríbase en Citrix Cloud.

Existen diferentes formas de autenticarse en Citrix ADM. En las secciones siguientes se describen los flujos de trabajo si es un usuario nuevo o un usuario existente en ADM.

Flujo de trabajo si es un usuario nuevo

1. Complete la instalación de Citrix ADM en el Hypervisor seleccionado.
2. Configure las distintas direcciones IP necesarias.
3. En un explorador web, escriba la dirección IP de Citrix ADM.
4. En los campos Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
5. Se abre la página Configurar la identidad del cliente, donde debe identificarse con sus credenciales de Citrix Cloud.

   Si no ha creado una cuenta en Citrix Cloud, haga clic en Citrix Cloud para registrarse.
6. Haga clic en Autenticar e introduzca la dirección de correo electrónico que utilizó para registrarse en Citrix Cloud.
7. Active la casilla de verificación situada junto a “Acepto compartir datos para telemetría”y haga clic en Enviar.

Flujo de trabajo si es un usuario existente que actualiza a la versión más reciente de la versión 12.1

1. Tras actualizar Citrix ADM a la versión más reciente de la versión 12.1, escriba la dirección IP del Citrix ADM en un explorador web.

2. En los campos Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. Se abre la página Configurar la identidad del cliente, donde debe identificarse con sus credenciales de Citrix Cloud.

   Si no ha creado una cuenta en Citrix Cloud, haga clic en Citrix Cloud para registrarse.
4. Haga clic en Autenticar e introduzca la dirección de correo electrónico que utilizó para registrarse en Citrix Cloud.
5. Active la casilla de verificación situada junto a "Acepto compartir datos para telemetría"y haga clic en Enviar.

Como usuario existente, también puede configurar su identidad en ADM más adelante de una de las dos maneras siguientes:

- navegando a **Sistema** > Administración del sistema y haciendo clic en Autenticación.
- haciendo clic en el símbolo de nube situado en la parte superior derecha de la GUI de ADM. Tras una autenticación exitosa, la «X» se convierte en una marca de verificación de color verde.

> **Nota**
>
> Asegúrese de que los siguientes dominios estén en la lista de permitidos:
>
> - *.citrixnetworkapi.net
> - *.blob.core.windows.net

Al cargar sus datos en Citrix ADM y utilizar las funciones de Citrix ADM, usted acepta y consiente que Citrix pueda recopilar, almacenar, transmitir, mantener, procesar y utilizar información técnica, de usuario o relacionada sobre sus productos y servicios de Citrix.

En todo momento, la información que reciba Citrix se tratará de acuerdo con la Política de privacidad de Citrix.com.

Sistema de licencias

January 30, 2024

Citrix Application Delivery Management (ADM) requiere una licencia Citrix ADC verificada para administrar y supervisar las instancias de Citrix ADC, cuando las instancias se detectan mediante el protocolo https.

Puede administrar y supervisar cualquier número de instancias y entidades sin licencia. Sin embargo, solo puede administrar 30 aplicaciones descubiertas en el panel de aplicaciones y ver los datos de

análisis de solo 30 servidores virtuales sin solicitar una licencia. Para administrar más de 30 aplicaciones descubiertas o ver los análisis de más de 30 servidores virtuales, debe comprar y aplicar licencias.

	Función Citrix ADM	[**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales	Se requiere una licencia Citrix ADM para > 30 servidores virtuales	Requisitos de licencia de Citrix ADC
Análisis	Información web	No	Sí	No aplicable
	HDX Insight*	No	Sí	Enterprise (informes de menos de 1 hora) Premium (informes = ilimitados)
	Security Insight	No	Sí	Licencia Premium (o) Enterprise con App Firewall
	Insight SSL	No	Sí	No aplicable
	Gateway Insight	No	Sí	Enterprise (informes de menos de 1 hora) Premium (informes = ilimitados)
	Información TCP	No	Sí	No aplicable
	Video Insight	No	Sí	Premium (serie Citrix-T 1000, VPX-T)

	Función Citrix ADM	[**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales	Se requiere una licencia Citrix ADM para > 30 servidores virtuales	Requisitos de licencia de Citrix ADC
	WAN Insight	No	No aplicable	La instancia de Citrix SD-WAN debe ser Optimization Edition (WANOP)
Aplicaciones				
	Estadísticas de aplicaciones (Panel de aplicaciones, Panel de seguridad de aplicaciones)	No	Sí	La información relacionada con Citrix ADC Web App Firewall en el panel de aplicaciones y el panel de seguridad de aplicaciones necesita una licencia Premium (o) Enterprise con App Firewall.
	StyleBooks	Sí	No	No aplicable
Redes				
	Servidor de licencias	Sí	No	No aplicable

	Función Citrix ADM	[**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales	Se requiere una licencia Citrix ADM para > 30 servidores virtuales	Requisitos de licencia de Citrix ADC
	Gestión de inventario: panel de infraestructura, grupos de instancias, panel de instancias y sitios	Sí	No	No aplicable
	Gestión de eventos y Syslog	Sí	No	No aplicable
	Trabajos de configuración, auditoría de configuración y consejos de configuración	Sí	No	No aplicable
	Informes de red (nivel de instancia)	Sí	No	No aplicable
	Informes de red (nivel de servidor virtual)	Sí	No	No aplicable
	Funciones de red (visibilidad y administración de servidores virtuales, servicios, grupos de servicios, servidores)	Sí	No	No aplicable

	Función Citrix ADM	[**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales	Se requiere una licencia Citrix ADM para > 30 servidores virtuales	Requisitos de licencia de Citrix ADC
	Gestión, supervisión y panel de control de certificados SSL (nivel de instancia)	Sí	No	No aplicable
	Panel de certificados SSL (nivel de servidor virtual)	Sí	No	No aplicable
Sistema				
	RBAC y autenticación externa (nivel de instancia)	Sí	No	No aplicable
	RBAC y autenticación externa	Sí	No	No aplicable
Orchestration				
	Integración con OpenStack	Sí	No	No aplicable
	Integración con VMware NSX	Sí	No	No aplicable
	Integración de Cisco APIC	Sí	No	No aplicable
	Integración de contenedores	Sí	No	No aplicable
Equilibradores de carga de terceros				

	Función Citrix ADM	[**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales	Se requiere una licencia Citrix ADM para > 30 servidores virtuales	Requisitos de licencia de Citrix ADC
	HAProxy: visibilidad en el host/instancia/backend/servidores/frontend, configuración de descarga o carga y reinicio del dispositivo.	Sí	No	No aplicable
	Panel de aplicaciones	No	Sí (requiere una licencia independiente)	No aplicable

*Para la integración de Citrix Director con la compatibilidad con Citrix ADM, Citrix Director debe tener una licencia Premium.

Las licencias para más servidores virtuales están disponibles en paquetes de servidores virtuales de 10. Puede obtener una licencia válida y agregar las licencias en los servidores Citrix ADM a través de la GUI de Citrix ADM.

Alta disponibilidad

El servidor Citrix ADM puede contener licencias VIP, CICO y capacidad agrupada. Cuando las licencias se emiten a un servidor ADM, las licencias están enlazadas al identificador de host del servidor. Además, la asignación de licencias a un servidor ADM diferente está restringida.

Si configura un par de alta disponibilidad de ADM como servidor de licencias, los servidores principal y secundario deben tener los mismos archivos de licencia. Por lo tanto, en la implementación de alta disponibilidad de ADM, Citrix ADM admite la asignación de los mismos archivos de licencia a ambos servidores.

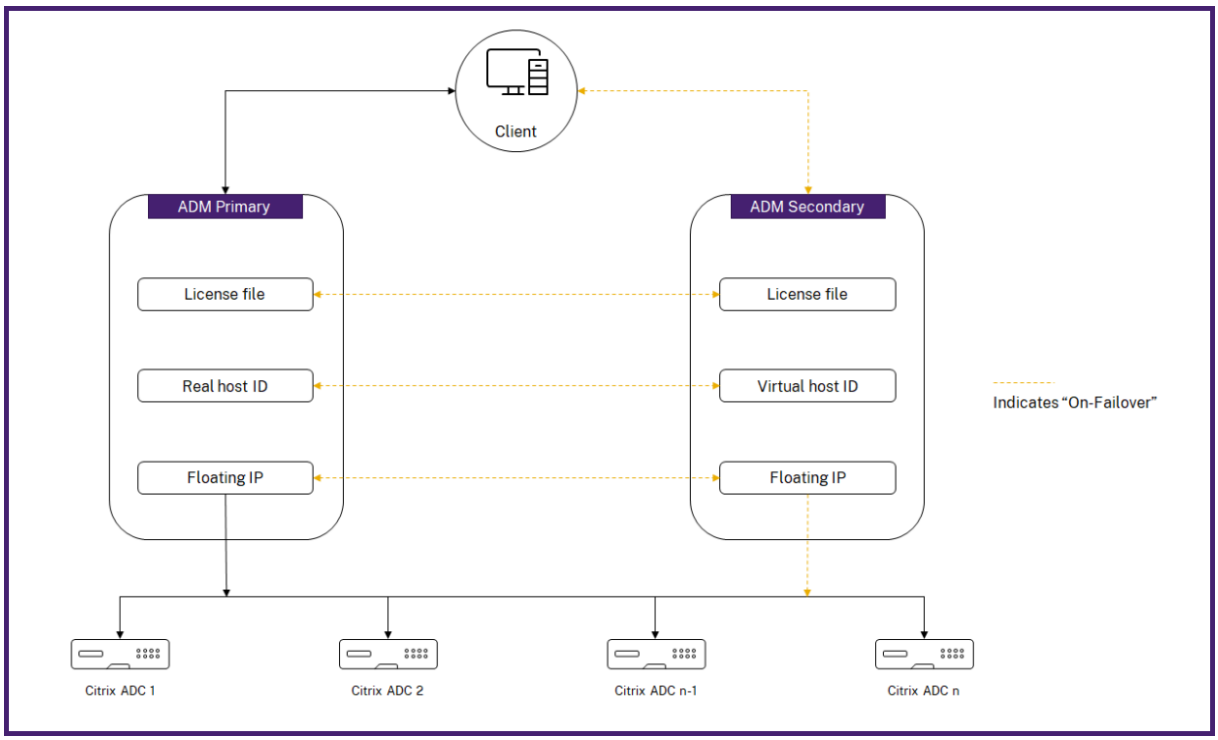
Nota

- Si ha instalado Citrix ADM 12.1.49.x o versiones anteriores, dispondrá de un período de gracia de 30 días para mantener las licencias en el nodo secundario. Tras el período de gracia, debe ponerse en contacto con Citrix para volver a alojar la licencia original.
- Para 12.1.50.x o versiones posteriores, la licencia de Citrix ADM se sincroniza automáticamente con el nodo secundario.
- Las licencias agrupadas se sincronizan automáticamente con el nodo secundario desde la versión 12.1.50.x o posterior.

¿Cómo se sincronizan las licencias entre nodos de alta disponibilidad de ADM?

Cada vez que se produce una conmutación por error, el servidor secundario asume la función del servidor principal. El ID de host real del servidor principal se configura como el ID de host virtual del nuevo servidor principal. Los archivos de licencia reconocen el nuevo servidor principal mediante el identificador de host virtual.

- **ID de host real** - Este ID se genera a partir de una dirección MAC del servidor ADM. Cada implementación independiente de ADM tiene un identificador de host único.
- **Identificador de host virtual**: Este identificador se genera automáticamente durante la implementación de HA. El ID de host real de un servidor primario de ADM se utiliza como ID de host virtual de un servidor secundario. Este ID se almacena en la base de datos ADM en un formato cifrado y las modificaciones de este ID están restringidas. El identificador de host virtual es preferible sobre el ID de host real.



Supongamos que el nodo-1 es el servidor principal y el Nodo-2 es el servidor secundario. El identificador de host virtual del Node-1 está sincronizado con el Node-2.

1. Los archivos de licencia disponibles en Node-1 se sincronizan con Node-2.
2. Cualquier nuevo archivo de licencia del Node-1 se sincroniza periódicamente con el Node-2.
3. ADM garantiza que el servidor de licencias se ejecuta solo en el Nodo-1 para evitar duplicar la capacidad de licencia.
4. Las instancias de Citrix ADC retiran las licencias del Node-1 mediante la dirección IP flotante.

Las licencias están bloqueadas para instancias de ADC. Para obtener licencias de un Citrix ADM HA, las instancias requieren la dirección IP del dispositivo específico. Cuando aplique licencias en un servidor principal, se encargará de las licencias y aplicará todas las licencias futuras en esa instancia. Solo puede eliminar licencias del servidor en el que haya instalado las licencias.

Orchestration

El módulo de orquestación es independiente de la licencia y siempre está disponible.

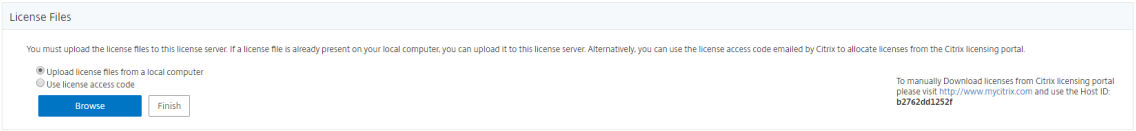
Actualización de las licencias de servidor virtual

Puede actualizar las licencias en Citrix ADM para supervisar y administrar más servidores virtuales alojados en los dispositivos Citrix ADC.

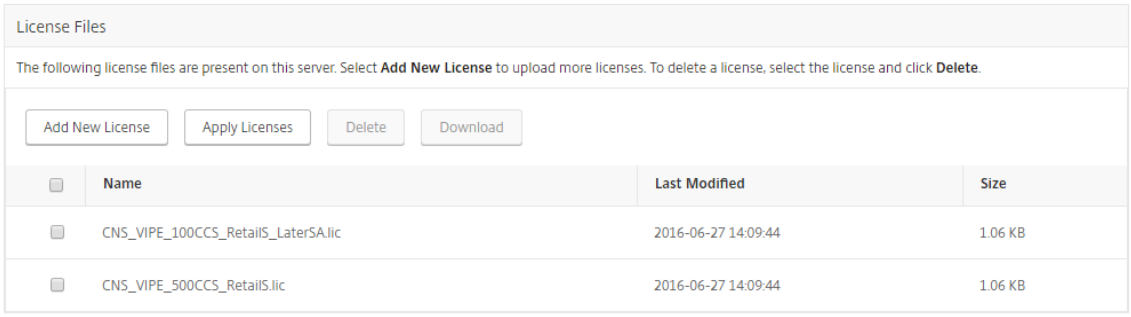
Para actualizar las licencias del dispositivo:

1. Inicie sesión en Citrix ADM con las credenciales de administrador.
2. Vaya a **Redes** > **Licencias** > **Configuración**.
3. En el panel de detalles, vaya a Archivos de licencias y seleccione una de las siguientes opciones:
   - **Cargue los archivos de licencia desde un equipo local**. Si ya hay una licencia en su equipo local, haga clic en**Examinar** y seleccione el archivo de licencia (.lic) que desee utilizar para asignar las licencias. Haz clic en **Finalizar** .
   - **Utilice el código de activación de licencia**. Citrix envía por correo electrónico el código de acceso de licencia de la licencia que adquirió. Introduzca el código de acceso de la licencia en el cuadro de texto y haga clic en **Obtener licencias**.

> **Nota**
>
> Si selecciona esta opción, Citrix ADM debe estar conectado a Internet o un servidor proxy debe estar disponible.

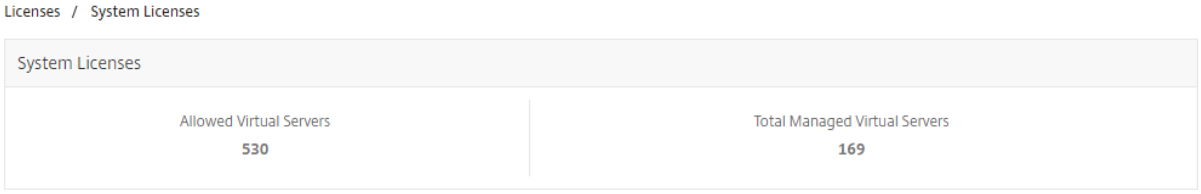


4. Puede agregar más licencias desde la página Configuración de licencias en cualquier momento.



Verificación

Puede comprobar las licencias instaladas en su Citrix ADM accediendo a**Redes** > **Licencias > Licencias del sistema**.



Licenciar los servidores virtuales

Puede seleccionar los servidores virtuales que quiere administrar y supervisar a través de Citrix ADM. Si la cantidad total de servidores virtuales alojados en las instancias de Citrix ADC detectadas es inferior a la cantidad de licencias de servidores virtuales instaladas, Citrix ADM otorga licencias a todos los servidores virtuales.

Puede seleccionar los servidores virtuales que quiere administrar y supervisar a través de Citrix ADM.

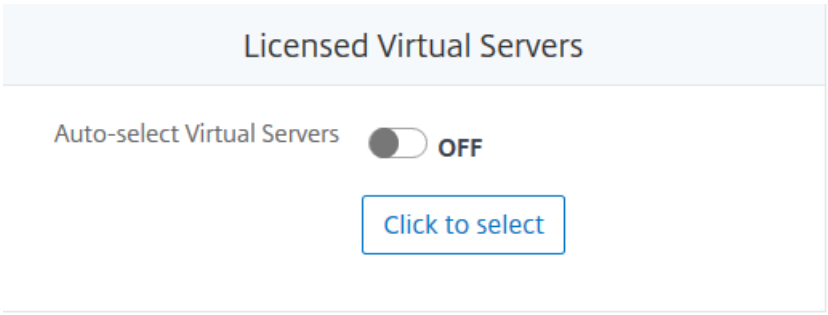
Puntos a tener en cuenta:

- De forma predeterminada, Citrix ADM licencia automáticamente los servidores virtuales aleatoriamente después de cada ciclo de sondeo de servidores virtuales.
- Si el número total de servidores virtuales descubiertos en su Citrix ADM es inferior al número de licencias de servidor virtual instaladas, Citrix ADM, de forma predeterminada, otorga licencias a todos los servidores virtuales.
- Para seleccionar manualmente los servidores virtuales o para restringir las licencias a los servidores virtuales limitados, primero debe inhabilitar la concesión automática de licencias de los servidores virtuales y, a continuación, seleccionar los servidores virtuales que quiere administrar.
- Citrix ADM no otorga licencias a los servidores virtuales no direccionables. Para administrarlos, debe licenciarlos manualmente.

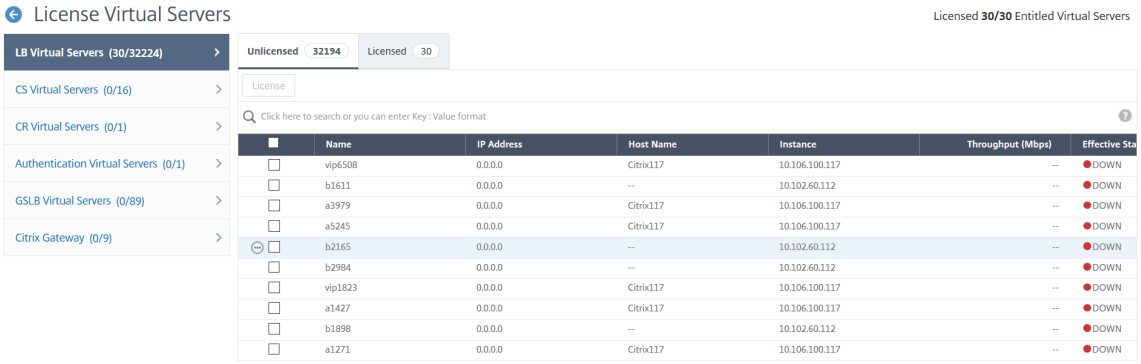
Para administrar los servidores virtuales con licencia:

1. Inicie sesión en Citrix ADM con las credenciales de administrador.
2. Vaya a **Redes > Licencias > Licencias de sistema**.

   Aparece el panel de licencias del sistema.
3. En **Servidores virtuales con licencia**, desactive la **selección automática de servidores virtuales** y haga clic en la opción **Haga clic para seleccionar**.



4. En la pantalla**License Virtual Server**, seleccione el tipo de servidores virtuales haciendo clic en la ficha correspondiente.



5. En la ficha **Sin licencia**, seleccione los servidores virtuales a los que quiere licenciar y haga clic en **Licencia**. En la ficha **Licencias**, seleccione los servidores virtuales de los que desee anular la licencia y haga clic en **Quitar licencia**.
6. Haga clic en**Siguiente**para ir a la ficha de los demás servidores virtuales o haga clic en**Guardar y salir** para licenciar los servidores virtuales seleccionados.

Configurar la compatibilidad con licencias automáticas para servidores virtuales no direccionables

Citrix ADM, de forma predeterminada, no aplica licencias automáticamente a servidores virtuales no direccionables. Para obtener licencias de servidores virtuales no direccionables, debe inhabilitar la opción de licencia automática y seleccionar manualmente los servidores virtuales no direccionables. Esto aumenta su esfuerzo por seleccionar manualmente los servidores no direccionables inicialmente cuando aplica las licencias. También debe seleccionar manualmente los nuevos servidores virtuales no direccionables cada vez que se agregan a la red.

Citrix ADM ofrece una nueva opción en **Redes** > **Licencias > Licenciasdel sistema**. Es decir, la nueva opción**Selección automática de servidores virtuales no direccionables**. Habilitar esta opción ahora permite especificar explícitamente que la licencia debe incluir también servidores virtuales no direccionables.

> **Nota**
>
> - Citrix ADM, de forma predeterminada, aún no selecciona automáticamente los servidores virtuales no direccionables para la concesión de licencias.
> - Application Analytics (App Dashboard) es la única analítica admitida actualmente en servidores virtuales con licencia no direccionables.

Comprobaciones de caducidad de las licencias de servidores virtuales

Ahora puede ver el estado de Citrix ADM y establecer alertas para la caducidad de la licencia del servidor virtual.

Para ver el estado de las licencias:

1. Vaya a **Redes**> **Licencias** > **Licencias de sistema.**
2. En la sección **Información de caducidad de licencia**, puede encontrar los detalles de las licencias que van a caducar:
    - **Función:**tipo de licencia que va a caducar.
    - **Recuento:** número de instancias o servidores virtuales que se ven afectados.
    - **Días hasta la fecha de caducidad:**número de días que quedan antes de la fecha de caducidad.

Para configurar los valores de notificación de las licencias:

1. Vaya a **Redes** > **Licencias** > **Configuración**.
2. En la sección **Configuración de notificaciones**, haga clic en el icono del lápiz y modifique los parámetros.
    - **Perfil de correo electrónico:** Perfil de correo electrónico o lista de distribución para enviar notificaciones cuando las licencias alcancen el umbral o vayan a caducar.
    - **Perfil SMS: perfil** de SMS o lista de distribución para enviar notificaciones cuando las licencias alcancen el límite o estén a punto de caducar.
    - **Umbral de alerta:** establece el porcentaje de licencias agrupadas para notificar a los administradores por correo electrónico o SMS.
    - **Umbral de caducidad de licencia:** Número de días antes de que expire el número de licencias determinadas por Alert Threshold.
    - **Días hasta la fecha de caducidad:**número de días que quedan antes de la fecha de caducidad.

Requisitos del sistema

January 30, 2024

Antes de instalar Citrix Application Delivery Management (ADM), debe comprender los requisitos de software, los requisitos del explorador, la información de puertos, la información de licencia y las limitaciones.

Requisitos de Citrix ADM

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs **Nota**: Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM.
Espacio de almacenamiento	El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Utilice la calculadora de tamaño que se menciona en la sección **Límites máximos** (página número 7) de la Guía de implementación de Citrix ADM HA. Esta guía está disponible en nuestro sitio de descargas, en **NetScaler MAS Release 12.1 > Versiones anteriores**. **Nota**: necesita una cuenta Citrix para acceder a la guía de implementación y a la calculadora de tamaño. Si el requisito de almacenamiento Citrix ADM supera los 120 GB, debe adjuntar un disco adicional. Solo se puede agregar un disco adicional. Citrix recomienda estimar el almacenamiento y adjuntar disco adicional en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps

> Nota
>
> Citrix ADM no es compatible con el chipset AMD.

Requisitos para el agente de Citrix ADM on-prem

Componente	Requisito
RAM	8 GB **Nota**: El valor predeterminado es de 8 GB. Citrix recomienda aumentar el valor predeterminado a 32 GB para un mejor rendimiento.
CPU virtual	2 CPU **Nota**: El valor predeterminado es de 2 CPU. Citrix recomienda aumentar el valor predeterminado a 8 CPU para obtener un mejor rendimiento.
Espacio de almacenamiento	30 GB
Interfaces de red virtual	1
Rendimiento	1 Gbps

> Nota
>
> El agente Citrix ADM no se admite en el chipset AMD.

Se requiere una versión mínima de Citrix ADC para las funciones de Citrix ADM

> **Importante**
>
> La versión y compilación de Citrix ADM deben ser **iguales o superiores a** la versión y compilación de Citrix ADC. Por ejemplo, si ha instalado Citrix ADM 12.1 compilación 50.39, asegúrese de haber instalado Citrix ADC 12.1 compilación 50.28/50.31 o anterior.

Función Citrix ADM	Versión del software Citrix ADC
StyleBooks	10.5 y versiones posteriores
Compatibilidad con OpenStack/CloudStack	11.0 y posteriores, si se requiere una partición 11.1 y posteriores, si se requiere una partición en una LAN virtual compartida
Soporte de NSX	11.1 Compilación 47.14 y posteriores (VPX)
Soporte Mesos/Marathon	10.5 y versiones posteriores
Copia de seguridad/Restauración	Para Citrix ADC, 10.1 y posteriores Para Citrix SDX, 11.0 y posteriores

Función Citrix ADM	Versión del software Citrix ADC
Monitorización/generación de informes y configuración mediante trabajos	10.1 y versiones posteriores
Funciones de análisis	
Información web	10.5 y versiones posteriores
HDX Insight	10.1 y versiones posteriores
Security Insight	11.0.65.31 y posteriores
Gateway Insight	11.0.65.31 y posteriores
Insight de caché	10.5 y posteriores*
Insight SSL	12.0 y versiones posteriores

* Las métricas de caché integradas no se admiten en Citrix ADM con instancias de Citrix ADC que ejecutan la versión 11.0 build 66.x.

Requisitos para la administración de instancias de Citrix SD-WAN

Matriz de interoperabilidad de las ediciones/versiones de la plataforma Citrix SD-WAN y las funciones de Citrix ADM

Modificación de plataforma	Citrix SD-WAN WANOP	Citrix SD-WAN SE	Citrix SD-WAN PE
Detección	Sí	Sí	Sí
Configuración	Sí	No	No
Supervisión	Sí	No	No
Informes (informes de red)	Sí	No	No
Gestión de eventos	Sí	No	No
HDX Insight	Sí	No	No
WAN Insight	Sí	No	No
HDX Insight (implementación de varios saltos)	Sí	Sí	No

Clientes ligeros admitidos para instancias Citrix SD-WAN

Citrix ADM admite los siguientes clientes ligeros para supervisar las implementaciones de Citrix SD-WAN:

- Cliente ligero Dell Wyse WTOS modelo R10L Rx0L
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced SUSE Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

Requisitos para el análisis de Citrix ADM

Versiones mínimas de Citrix Virtual Apps and Desktops requeridas para las funciones de Citrix ADM

Función Citrix ADM	Versión de Citrix Virtual Apps and Desktops
HDX Insight	Citrix Virtual Apps and Desktops 7.0 y posteriores

> **Nota**
>
> La función Citrix Gateway (con la marca Access Gateway Enterprise para las versiones 9.3 y 10.x) debe estar disponible en la instancia de Citrix ADC. Citrix ADM no admite dispositivos Access Gateway Standard independientes.

Citrix ADM puede generar informes para aplicaciones que se publican en Citrix Virtual Apps o Citrix Virtual Desktops y a las que se accede a través de Citrix Receiver. Sin embargo, esta capacidad depende del sistema operativo en el que esté instalado Receiver. Actualmente, un Citrix ADC no analiza el tráfico ICA para aplicaciones o escritorios a los que se accede a través de Citrix Receiver que se ejecutan en sistemas operativos iOS o Android.

Clientes ligeros compatibles con conocimientos de HDX

- Clientes ligeros basados en Dell Wyse Windows
- Clientes ligeros basados en Dell Wyse Linux
- Clientes ligeros basados en Dell Wyse ThinOS
- Clientes ligeros basados en Ubuntu 10ZiG
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

Se requiere una licencia de instancia de Citrix ADC para HDX Insight

Los datos recopilados por Citrix ADM para HDX Insight dependen de la versión y las licencias de las instancias de Citrix ADC que se están supervisando. Los informes de HDX Insight solo se muestran para los dispositivos NetScaler ADC Platinum y Enterprise que ejecutan la versión 10.5 y posteriores.

Licencia y duración de Citrix ADC	5 minutos	1 hora	1 día	1 semana	1 mes
Estándar	No	No	No	No	No
Empresarial	Sí	Sí	No	No	No
Platinum	Sí	Sí	Sí	Sí	Sí

Hipervisores compatibles

En la siguiente tabla se enumeran los hipervisores admitidos por Citrix ADM.

Hipervisor	Versiones
Citrix Hypervisor	7.1 y 7.4
VMware ESX	6.0, 6.5 y 6.7
Microsoft Hyper-V	2012 R2 y 2016
KVM genérico	RHEL 7.4 y Ubuntu 16.04

Sistemas operativos y versiones de receptor compatibles

En la siguiente tabla se enumeran los sistemas operativos compatibles con Citrix ADM y las versiones de Citrix Receiver que se admiten actualmente con cada sistema:

Sistema operativo	Versión de Receiver
Windows	Edición estándar 4.0
Linux	13.0.265571 y posteriores
Mac	11.8, compilación 238301 y posteriores
HTML5	1.5*
Aplicación Chrome	1.5*

* Aplicable con la versión 7.4 y posteriores de Citrix CloudBridge (Citrix SD-WAN WANOP).

Exploradores web compatibles

En la siguiente tabla se enumeran los exploradores web compatibles con Citrix ADM:

Explorador web	Versión
Internet Explorer	11.0 y versiones posteriores
Google Chrome	Chrome 19 y versiones posteriores
Safari	Safari 5.1.1 y versiones posteriores
Mozilla Firefox	Firefox 3.6.25 y posterior

Puertos compatibles

Citrix ADM utiliza la dirección IP de Citrix ADC (conocida como NSIP) para comunicarse con Citrix ADC. Para las comunicaciones entre las instancias de NetScaler ADC y NetScaler ADM, o las instancias de Citrix SD-WAN y NetScaler ADM, los siguientes puertos deben estar abiertos en NetScaler ADM:

> **Nota**
>
> Si ha configurado Citrix ADC en modo Alta disponibilidad, Citrix ADM utiliza la dirección IP de subred (Management SNIP) de Citrix ADC para comunicarse con Citrix ADC. Para la comunicación mediante SNIP con Citrix ADM, los siguientes puertos siguen siendo los mismos.

Tipo	Puerto	Detalles	Dirección de comunicación
———	———-	———	———
TCP	80/443	Para la comunicación NITRO desde Citrix ADM a Citrix ADC o Citrix SD-WAN instance.443. Para la comunicación NITRO entre servidores Citrix ADM en modo de alta disponibilidad.	Citrix ADM a Citrix ADC y Citrix ADC a Citrix ADM
TCP	22	Para la comunicación SSH desde Citrix ADM a Citrix ADC o instancia de Citrix SD-WAN. Para la sincronización entre los servidores Citrix ADM implementados en modo de alta disponibilidad. Además, este puerto es necesario para la comunicación SSH entre el agente ADM y Citrix ADC.	Citrix ADM a Citrix ADC y agente de Citrix ADM a Citrix ADC
UDP	4739	Para la comunicación de AppFlow desde Citrix ADC o Citrix SD-WAN instancia a Citrix ADM.	Citrix ADC o Citrix SD-WAN a Citrix ADM
ICMP	Sin puerto reservado	Detectar la accesibilidad de la red entre las instancias Citrix ADM y Citrix ADC, las instancias SD WAN o el servidor Citrix ADM secundario implementado en modo de alta disponibilidad.
UDP	161, 162	Para recibir eventos SNMP desde la instancia de Citrix ADC a Citrix ADM.	**Puerto 161**: Citrix ADM a Citrix ADC
			Puerto 162 - NetScaler ADC a NetScaler ADM
UDP	514	Para recibir mensajes de syslog desde Citrix ADC o una instancia de Citrix SD-WAN a Citrix ADM.	Citrix ADC o Citrix SD-WAN a Citrix ADM
TCP	25	Para enviar notificaciones SMTP desde Citrix ADM a los usuarios.
TCP	389/636	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre Citrix ADM y el servidor de autenticación externo LDAP.	Servidor de autenticación externa de Citrix ADM a LDAP
UDP	123	Puerto de servidor NTP predeterminado para, sincronización con varias fuentes de tiempo.
RADIUS	1812	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre Citrix ADM y el servidor de autenticación externo RADIUS.	Citrix ADM a servidor de autenticación externa RADIUS
TACACS	49	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre Citrix ADM y el servidor de autenticación externo TACACS.	Citrix ADM a servidor de autenticación externa TACACS
TCP	5563	Para recibir métricas ADC (contadores), eventos del sistema y mensajes de registro de auditoría desde la instancia NetScaler ADC a NetScaler ADM.	Citrix ADC a Citrix ADM
TCP	5557/5558	Para **la**comunicación de flujo de registros (para Security Insight, Web Insight y HDX Insight) desde Citrix ADC a Citrix ADM.	Citrix ADC a Citrix ADM
TCP	5454	Puerto predeterminado para la comunicación y sincronización de bases de datos entre nodos Citrix ADM en modo de alta disponibilidad.	Nodo principal de Citrix ADM a nodo secundario de Citrix ADM
TCP	27000	Puerto de licencia para la comunicación entre el servidor de licencias NetScaler ADM y

la instancia CPX.|Citrix ADC a Citrix ADM |
| TCP | 7279 | Puerto del demonio de proveedor Citrix.|Citrix ADC a Citrix ADM |
|TCP| 443/8443/7443|Puerto para la comunicación entre el agente NetScaler ADM y NetScaler ADM. El agente ADM inicia la comunicación con NetScaler ADM. | Agente NetScaler ADM con NetScaler ADM|
|

Limitaciones

En 12.1 NetScaler ADM, las siguientes funciones admiten el formato IPv6 de las direcciones IP:

1. Acceso de administración para la GUI de Citrix ADM
2. Acceso de administración para Citrix ADC
3. Registro e inventario
4. Panel de mandos de las redes
5. Tablero SSL
6. Trabajos de configuración
7. Auditoría de configuración
8. Funciones de red
9. Informes de red
10. Copia de seguridad y restauración de instancias de ADC
11. Eventos SNMP de Citrix ADC

Las siguientes funciones no admiten IPv6:

1. IP flotante de alta disponibilidad
2. Syslogs recibidos de ADC que admiten IPv6
3. StyleBooks en ADC que admiten IPv6
4. Análisis
5. Licencias agrupadas

Implementar

January 30, 2024

Para administrar y supervisar las aplicaciones y la infraestructura de red, primero debe instalar NetScaler ADM en uno de los hipervisores. Puede implementar NetScaler ADM como un único servidor o en un modo de alta disponibilidad. Si utiliza NetScaler Insight Center, puede migrar a NetScaler ADM y aprovechar las funciones de administración, monitoreo, orquestación y administración de aplicaciones, además de las funciones de análisis.

- **Despliegue**de un solo servidor .En una implementación de un solo servidor de NetScaler ADM, la base de datos se integra con el servidor y un solo servidor procesa todo el tráfico. Puede implementar Citrix ADM con Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM. Consulte:
  - Citrix ADM con Citrix Hypervisor
  - NetScaler ADM con Microsoft Hyper-V
  - NetScaler ADM con VMware ESXi
  - NetScaler ADM con servidor KVM Linux
- **Despliegue de alta disponibilidad (HA).** Una implementación de alta disponibilidad de dos servidores Citrix ADM de Citrix proporciona operaciones ininterrumpidas. En una configuración de alta disponibilidad, ambos nodos NetScaler ADM deben implementarse en modo activo-pasivo, en la misma subred mediante la misma versión de software y compilación, y deben tener las mismas configuraciones. Con la implementación de alta disponibilidad, la capacidad de configurar la dirección IP flotante en el nodo principal de Citrix ADM elimina la necesidad de un balanceador de carga de NetScaler independiente. Consulte:Configurar en una implementación de alta disponibilidad.
- **Migre de NetScaler Insight Center a Citrix ADM**. Puede migrar la implementación de NetScaler Insight Center a Citrix ADM sin perder la configuración, los parámetros o los datos existentes. Con Citrix ADM, no solo puede ver los distintos análisis generados por las instancias SD-WAN de NetScaler y NetScaler, sino que también puede administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada. Consulte:Migración de NetScaler Insight Center a NetScaler ADM
- **Integre Citrix ADM con Director**. Director se integra con Citrix ADM para el análisis de redes y la administración del rendimiento. Consulte: Integración de NetScaler ADM con Director

Requisitos previos para instalar NetScaler ADM

January 30, 2024

Puede descargar e instalar Citrix ADM para las plataformas Microsoft HyperV, VMware ESXi, Linux KVM y Citrix Hypervisor como un dispositivo virtual. Antes de instalar
NetScaler ADM, debe comprender los requisitos de software, los requisitos del explorador, la información de puertos, la información de licencias y las limitaciones de todas estas plataformas.

Para conocer los requisitos de plataforma específicos y los pasos detallados para instalar Citrix ADM, consulte los siguientes temas:

- Citrix ADM con Citrix Hypervisor
- Citrix ADM con Microsoft Hyper-V
- NetScaler ADM con VMware ESXi
- NetScaler ADM con servidor KVM Linux

Requisitos generales para la versión 12.1 de Citrix ADM

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs
Espacio de almacenamiento	Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. El espacio de almacenamiento predeterminado requerido es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Utilice la calculadora de tamaño que se menciona en la sección **Límites máximos** (página número 7) de la Guía de implementación de Citrix ADM HA. Esta guía está disponible en nuestro sitio de descargas, en **NetScaler MAS Release 12.1 > Versiones anteriores**. **Nota**: necesita una cuenta Citrix para acceder a la guía de implementación y a la calculadora de tamaño Si el requisito de almacenamiento Citrix ADM supera los 120 GB, debe adjuntar un disco adicional.

Componente	Requisito
	Citrix recomienda estimar el almacenamiento y adjuntar disco adicional en el momento de la implementación inicial. Solo se puede agregar un disco adicional. Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps

> Nota:
>
> Citrix recomienda hospedar NetScaler ADM VHD en un almacenamiento local. Cuando se aloja en dispositivos de almacenamiento en una SAN, es posible que NetScaler ADM no funcione como se esperaba.

Citrix ADM con Citrix Hypervisor

January 30, 2024

Para instalar Citrix ADM en Citrix Hypervisor (anteriormente conocido como XenServer), primero debe descargar el archivo de imagen de Citrix ADM .xva en su equipo local. Debe utilizar Citrix XenCenter para realizar la instalación de Citrix ADM.

> **Nota:**
>
> Citrix ADM no admite XenMotion.

Requisitos previos

Antes de instalar Citrix ADM, compruebe que se cumplen los siguientes requisitos:

- Citrix Hypervisor versión 7.1 o posterior está instalado en el hardware que cumple los requisitos mínimos.
- XenCenter se instala en una estación de trabajo de administración que cumple con los requisitos mínimos. Debe utilizar XenCenter para instalar Citrix ADM en Citrix Hypervisor.
- Ha descargado el archivo de imagen XVA de Citrix ADM.

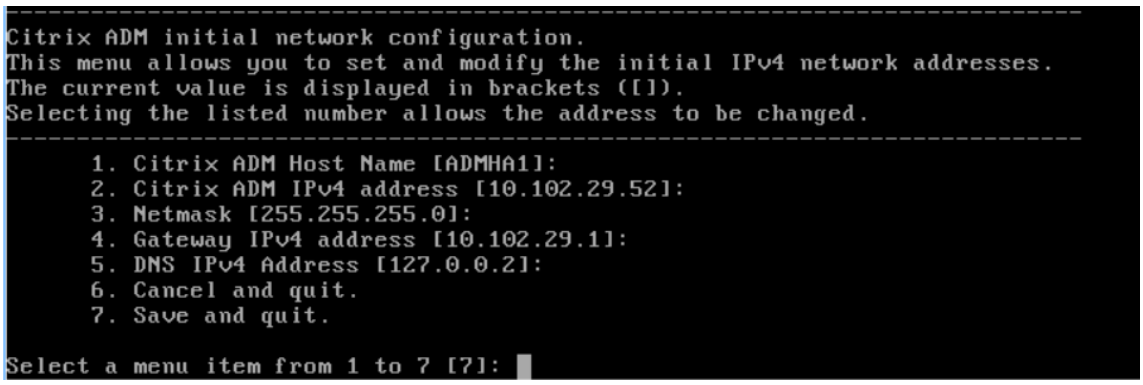
requisitos del sistema de XenCenter

XenCenter es una aplicación cliente de Windows. No puede ejecutarse en la misma máquina que el host de Citrix Hypervisor. En la siguiente tabla se describen los requisitos mínimos del sistema.

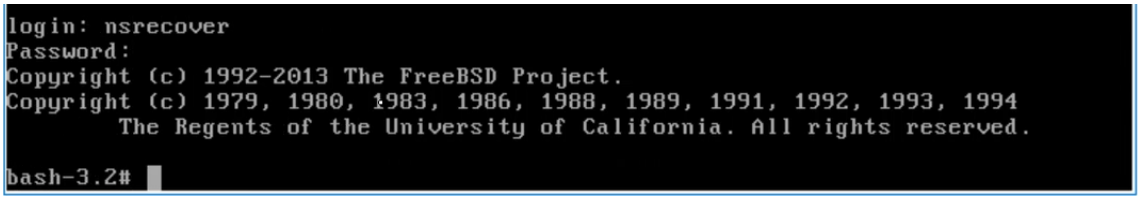
Componente	Requisito
Sistema operativo	Windows 7, Windows Server 2003 o Windows 10
.NET framework	Versión 2.0 o posterior
CPU	750 megahercios (MHz), recomendado: 1 gigahercio (GHz) o más rápido
RAM	1 GB, Recomendado: 2 GB
Tarjeta de interfaz de red	NIC de 100 megabits por segundo (Mbps) o más rápido

Instalación de Citrix Application Delivery Management

1. Importe el archivo de imagen XVA a su Citrix Hypervisor y, desde la ficha **Consola**, configure las opciones de configuración de red iniciales.



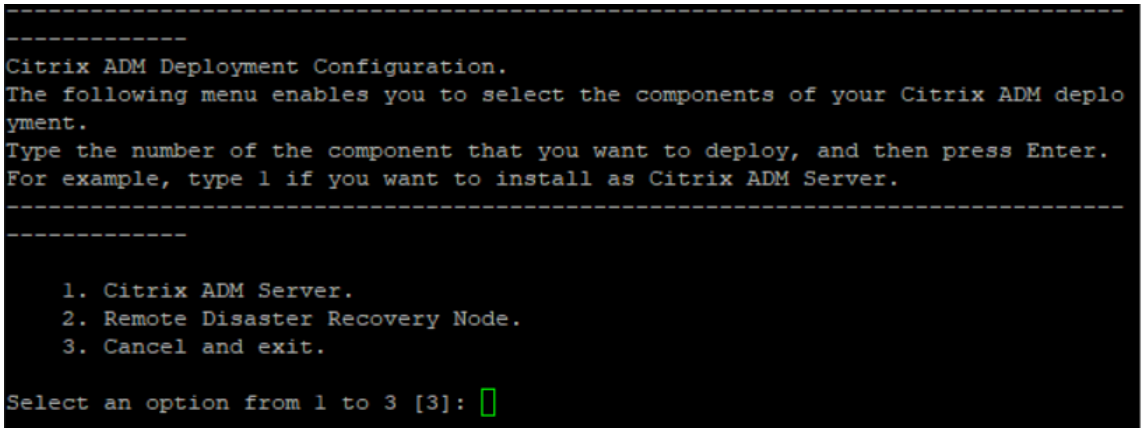
2. Después de especificar las direcciones IP necesarias, guarde los ajustes de configuración.
3. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.



> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

4. Ejecute el script de implementación escribiendo el comando en la línea de comandos del shell: `/mps/deployment_type.py`

5. Seleccione el tipo de implementación como **Citrix ADM Server**. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.



6. Escriba **Sí** para implementar Citrix ADM como una implementación independiente.
7. Escriba **Sí** para reiniciar el servidor de Citrix ADM.

> **Nota**
>
> Después de instalar Citrix ADM, puede actualizar los valores de configuración inicial más adelante.

Verificación

Una vez instalado el servidor, puede acceder a la interfaz gráfica de usuario (GUI) escribiendo la dirección IP del servidor Citrix ADM en el explorador web. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son nsroot/nsroot.

El explorador muestra la utilidad de configuración Citrix ADM.

NetScaler ADM con Microsoft Hyper-V

January 30, 2024

Para instalar NetScaler ADM en Microsoft Hyper-V, primero debe descargar el archivo de imagen NetScaler ADM en el equipo local. Además, asegúrese de que el sistema tenga las extensiones de virtualización de hardware y compruebe que las extensiones de virtualización de la CPU estén disponibles.

Requisitos previos

Antes de instalar el dispositivo virtual Citrix ADM, compruebe que se cumplen los siguientes requisitos:

- La versión 6.2 o posterior de Microsoft Hyper-V se instala en un hardware que cumple los requisitos mínimos.
- Instale Microsoft Hyper-V Manager en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.
- Ha descargado el archivo de imagen Citrix ADM.

Requisitos del sistema Microsoft Hyper-V

Microsoft Hyper-V es una aplicación cliente de Windows. En la siguiente tabla se describen los requisitos mínimos del sistema.

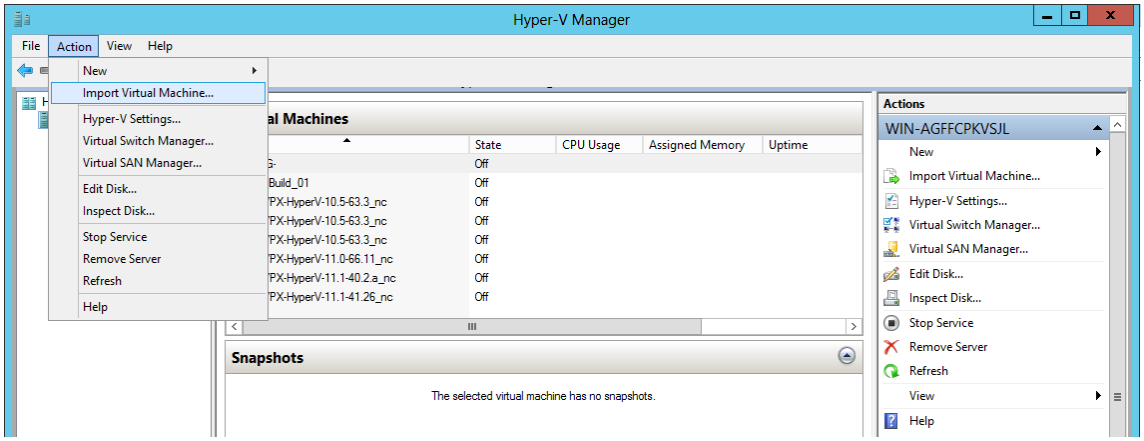
Componente	Requisito
Sistema operativo	Windows Server 2012 R2
.NET framework	Versión 2.0 o posterior
CPU	750 megahercios (MHz), recomendado: 1 gigahercio (GHz) o más rápido
RAM	1 GB, Recomendado: 2 GB
Tarjeta de interfaz de red	NIC de 100 megabits por segundo (Mbps) o más rápido

Instalación de NetScaler Application Delivery Management

La cantidad de servidores Citrix ADM que puede instalar depende de la memoria disponible en el servidor Hyper-V.

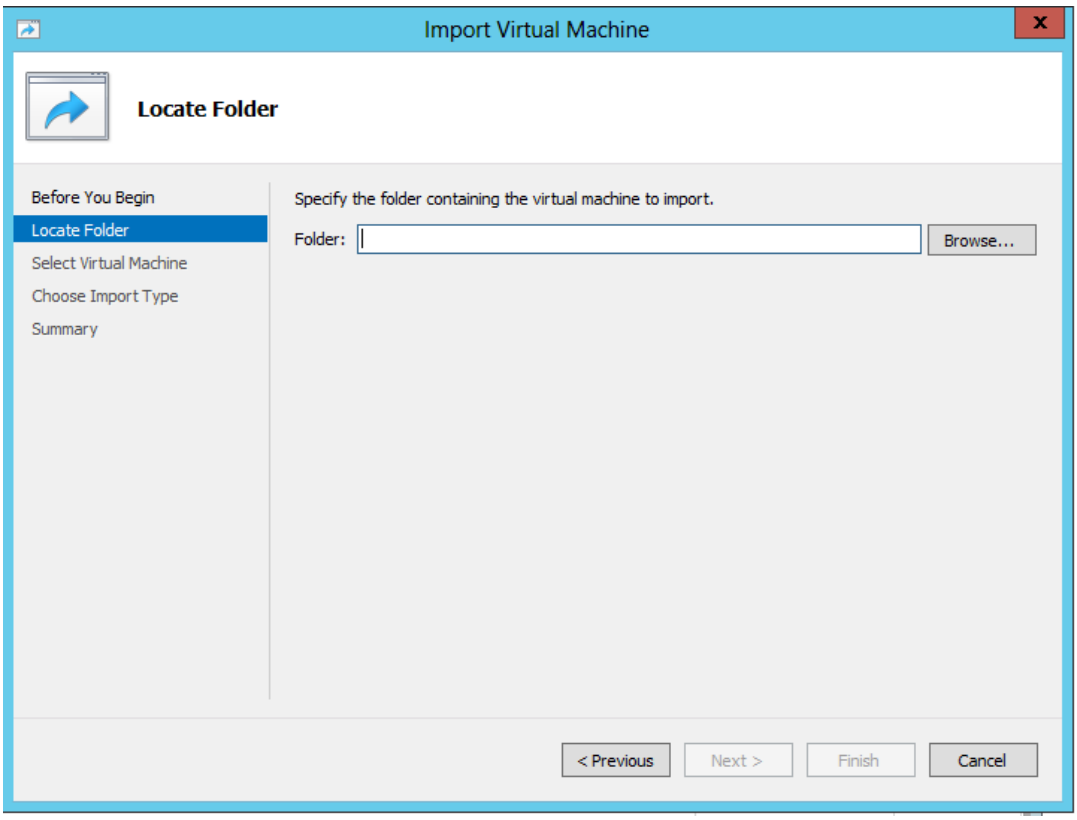
Para instalar NetScaler ADM:

1. Inicie el cliente Hyper-V Manager en su estación de trabajo.
2. En el menú **Acción**, haga clic en **Importar máquina virtual**.



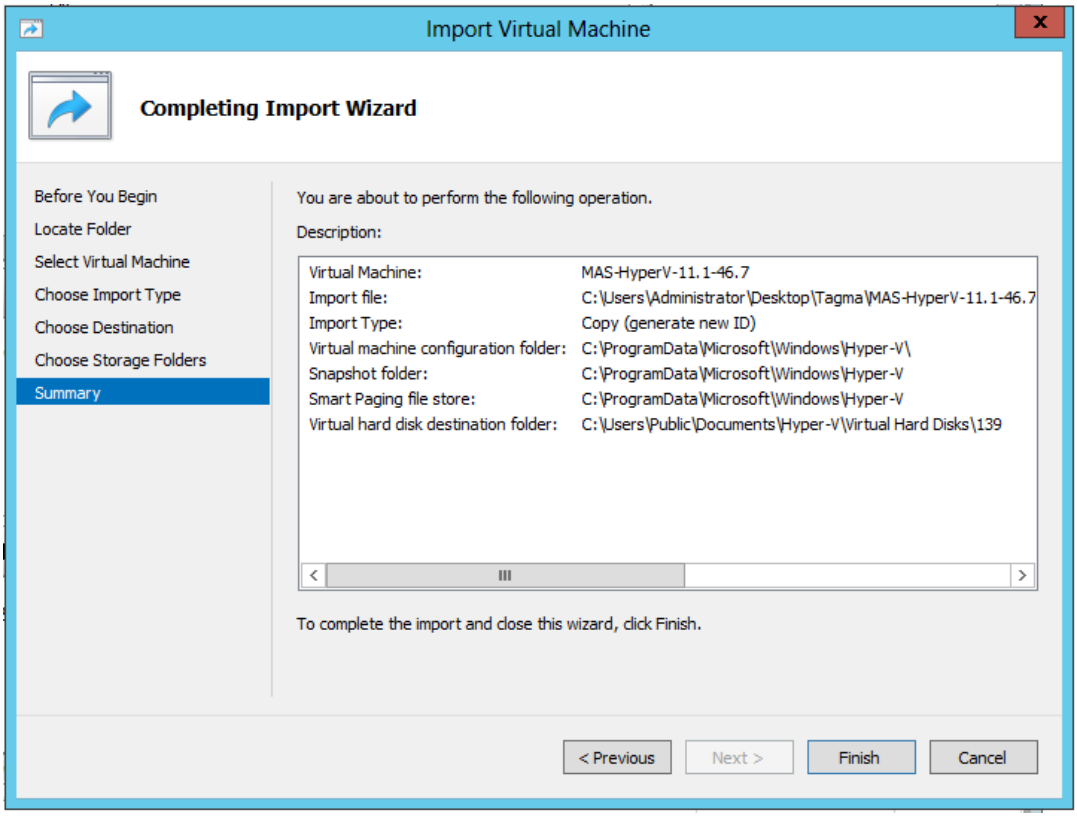
3. Importe la imagen de Hyper-V y haga lo siguiente:
   a) En el cuadro de diálogo Importar máquina virtual, en la sección **Localizar carpeta** , vaya a la carpeta en la que guardó la imagen de Citrix ADM Hyper-V, seleccione la carpeta y haga clic en **Siguiente**.
   b) En la sección Seleccionar máquina virtual, seleccione el nombre de máquina virtual correspondiente.
   c) En la sección **Elija el tipo de importación**, seleccione la opción Copiar la máquina virtual (crear un nuevo identificador único) y haga clic en Siguiente.
   d) En la sección **Elegir destino**, puede especificar las carpetas para almacenar los archivos de la máquina virtual.

> **Nota**
>
> De forma predeterminada, el asistente importa los archivos de la máquina virtual a las carpetas predeterminadas de Hyper-V del host local.



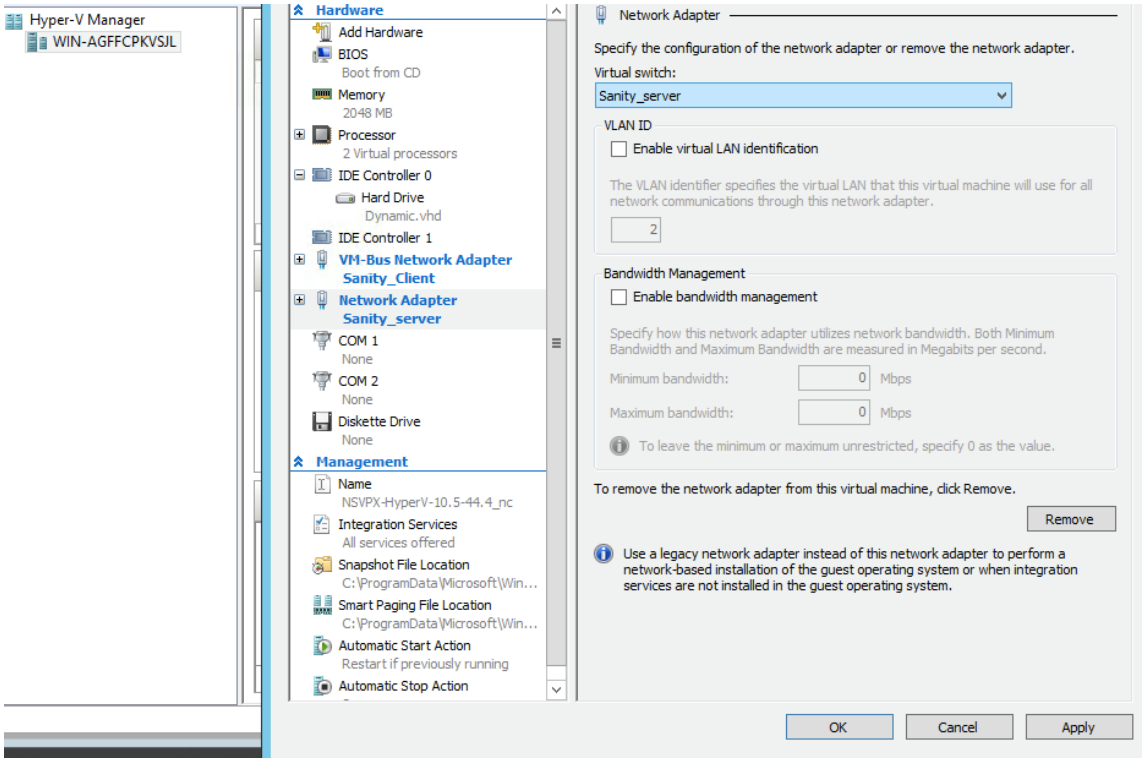
e) En la sección **Elegir carpetas de almacenamiento**, puede seleccionar la ubicación en la que desea almacenar los discos duros virtuales y, a continuación, hacer clic en **Siguiente**.

f) Puede comprobar los detalles de la máquina virtual en el panel de resumen y hacer clic en **Finalizar**.



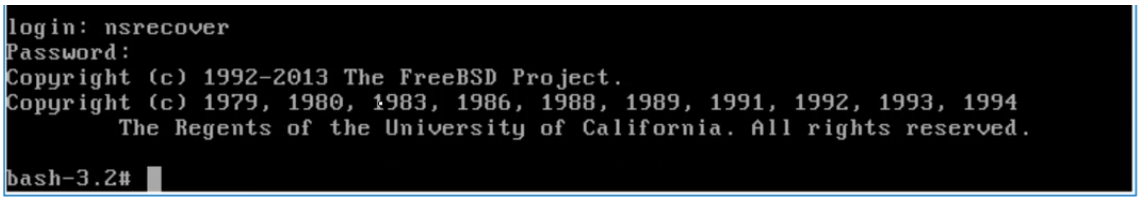
La imagen de Citrix ADM Hyper-V aparece en el panel derecho.

4. Haga clic con el botón secundario en la imagen de NetScaler ADM Hyper-V y, a continuación, haga clic en **Configuración**.
5. En el panel izquierdo del cuadro de diálogo que aparece, vaya a **Hardware** > **Adaptador de red VM_Bus** y, en el panel derecho, en la lista desplegable Red, seleccione la red adecuada.



6. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7. Haga clic con el botón derecho en la imagen de Citrix ADM Hyper-V y haga clic en **Conectar**.
8. En la ventana de la consola, haga clic en el botón **Inicio**.
9. Configure las opciones de configuración de red iniciales.

10. Después de especificar las direcciones IP necesarias, guarde los ajustes de configuración.
11. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.



> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

12. Ejecute el script de despliegue escribiendo el comando en la línea de comandos del shell:

```
deployment_type.py
<!--NeedCopy-->
```

```
bash-3.2# deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

13. Seleccione el tipo de implementación como **Citrix ADM Server**. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.

```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

14. Escriba **Yes** para implementar Citrix ADM como implementación independiente.
15. Escriba **Sí** para reiniciar el servidor de Citrix ADM.

> **Nota**
>
> Tras instalar Citrix ADM, puede actualizar los valores de configuración iniciales más adelante.

Verificación

Una vez instalado el servidor, puede acceder a la interfaz gráfica de usuario (GUI) escribiendo la dirección IP del servidor Citrix ADM en la barra de direcciones del explorador. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son nsroot/nsroot.

El explorador muestra la utilidad de configuración Citrix ADM.

NetScaler ADM con VMware ESXi

January 30, 2024

Para instalar dispositivos virtuales NetScaler ADM en VMware ESXi, utilice el cliente VMware vSphere.

Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, compruebe que los siguientes requisitos:

- Instale una versión compatible de VMware ESXi (6.0, 6.5 y 6.7).
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Descargue los archivos de configuración de NetScaler ADM.

> **Nota**
>
> Citrix ADM no admite vMotion.

Para instalar NetScaler ADM

1. Inicie el cliente de VMware vSphere en su estación de trabajo.
2. En el cuadro de texto **Dirección IP/Nombre**, escriba la dirección IP del servidor de VMware ESXi al que desea conectarse.
3. En los cuadros de texto **Nombre de usuario** y **Contraseña** , escriba las credenciales de administrador y, a continuación, haga clic **en**Iniciar sesión .
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla de OVF**, en **Implementar desde un archivo o URL**, seleccione el archivo OVF y haga clic en **Siguiente**.

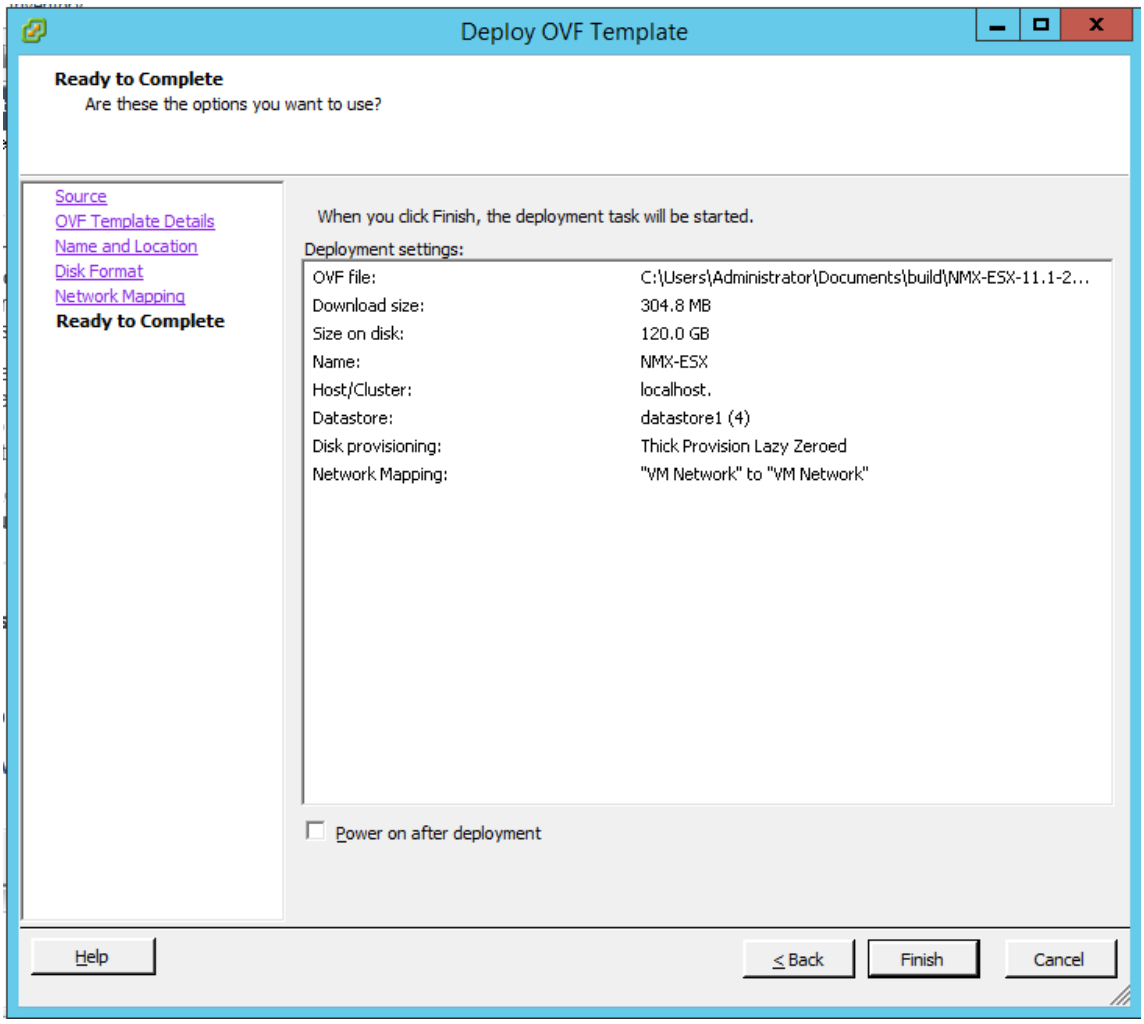
   > **Nota**
   >
   > Si aparece un mensaje de advertencia con el siguiente texto: El identificador del sistema operativo no es compatible con el host seleccionado, compruebe si el servidor VMware admite el sistema operativo FreeBSD. Haga clic en **Sí**.

6. En la página **Detalles de plantilla de OVF**, haga clic en **Siguiente**.

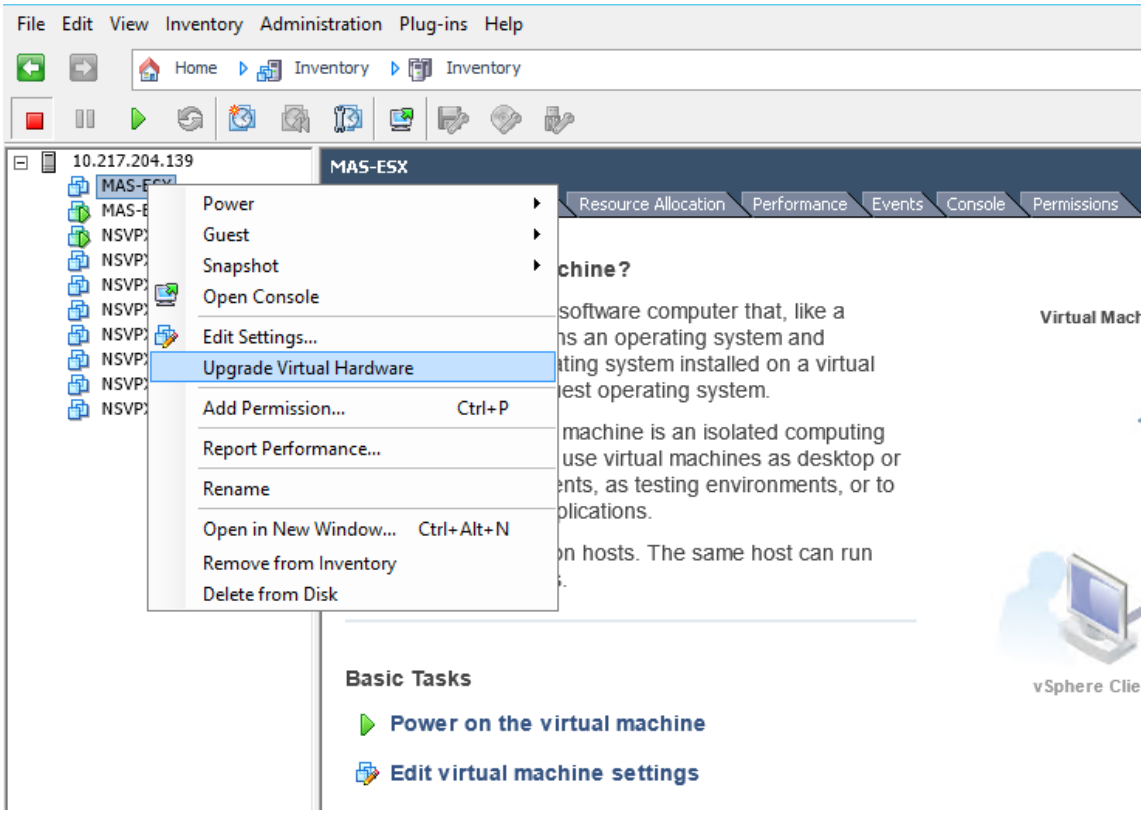
7. Escriba un nombre para el dispositivo virtual NetScaler ADM y, a continuación, haga clic en **Siguiente**.
8. Especifique el formato de disco seleccionando Formato de aprovisionamiento fino o Formato de aprovisionamiento grueso.

   > **Nota**
   >
   > Citrix recomienda seleccionar el **formato de aprovisionamiento grueso**.

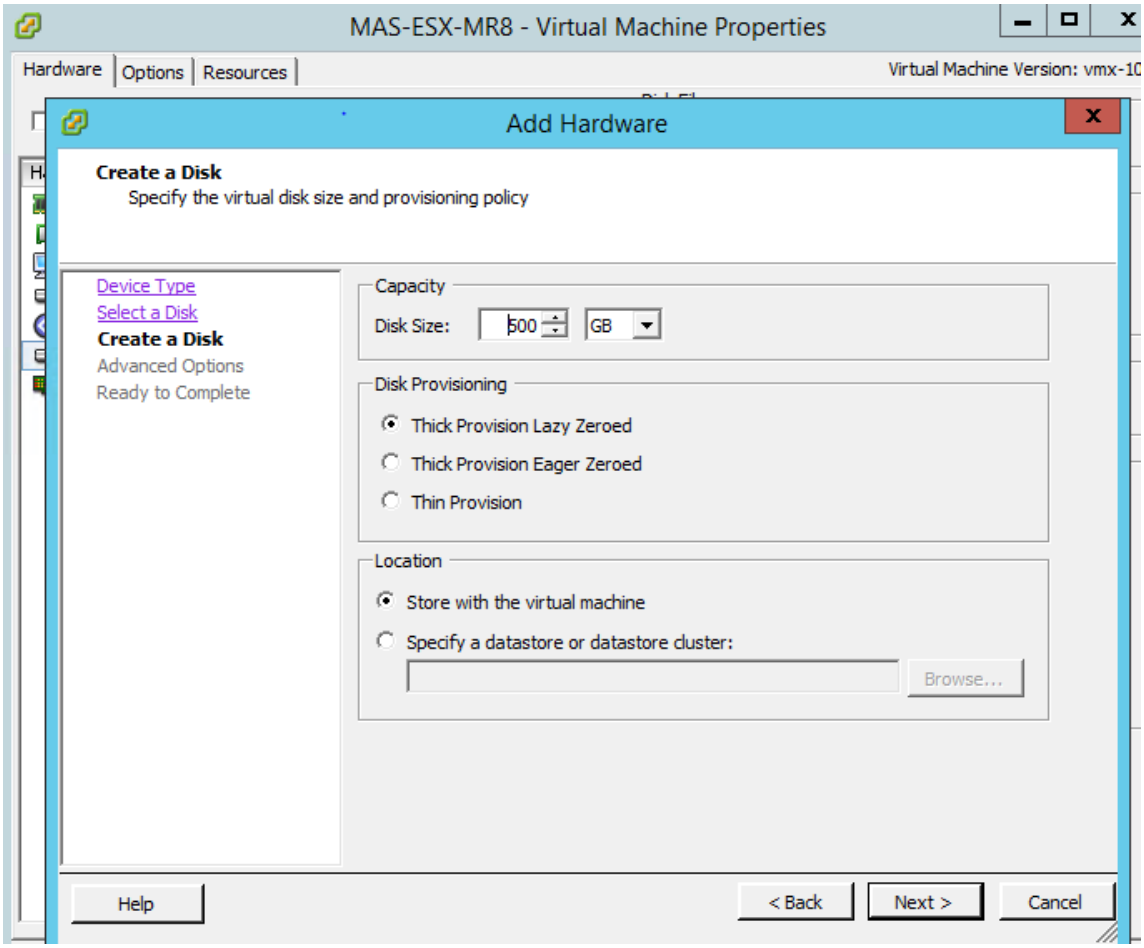
9. Haga clic en **Finalizar** para iniciar el proceso de instalación.



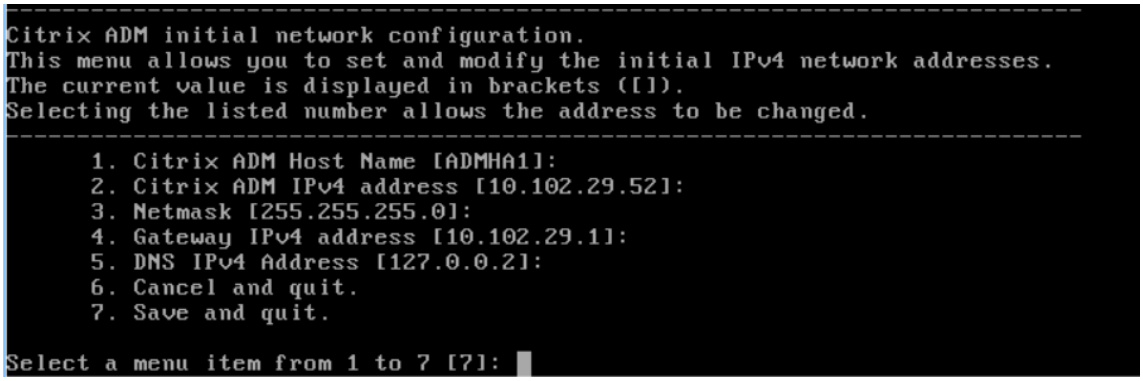
10. Ya tiene todo listo para iniciar el dispositivo virtual NetScaler ADM.
11. En el panel de navegación, seleccione el dispositivo virtual que instaló. En el menú **Inventario**, haga clic con el botón derecho en la **máquina virtual** y, a continuación, haga clic en **Actualizar hardware virtual**. En el cuadro de diálogo **Confirmar máquina virtual**, haga clic en **Sí**.



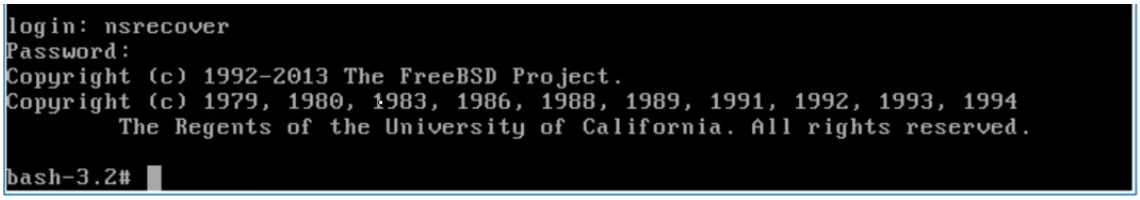
12. En el menú **Inventario**, haga clic en **Máquina virtual** y, a continuación, en **Modificar configuración**.
13. En el cuadro de diálogo **Propiedades de la máquina virtual**, en la ficha **Hardware**, haga clic en **Memoria** y, a continuación, en el panel derecho, especifique el **Tamaño de memoria** como 32 GB.
14. Haga clic en **CPU** y, a continuación, en el panel derecho, especifique las CPU como 8. Haga clic en **Aceptar**.
15. Agregue un disco adicional según sus necesidades.



16. En el panel de navegación, seleccione el dispositivo virtual que instaló. En el menú **Inventario**, haga clic en **Máquina virtual**, en **Encender** y, a continuación, en **Encender**.
17. Haga clic en la ficha **Consola** para ver las opciones de Configuración de red inicial de NetScaler ADM.



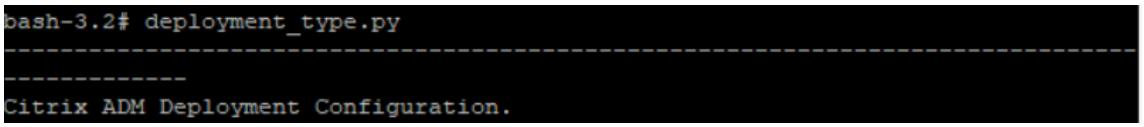
18. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.
19. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.



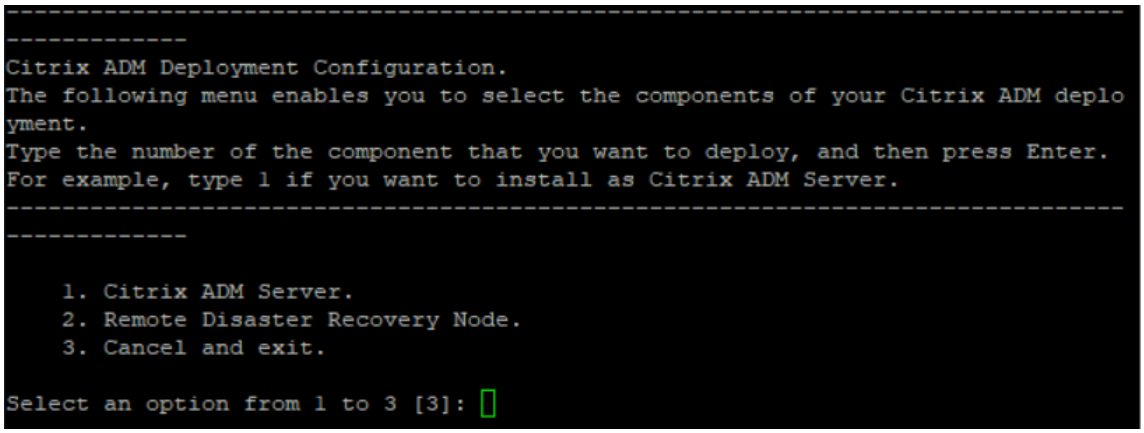
> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

20. Ejecute el script de despliegue escribiendo el comando en la línea de comandos del shell:

```
deployment_type.py
<!--NeedCopy-->
```



21. Seleccione el tipo de implementación como **Citrix ADM Server**. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.



22. Escriba **Sí** para implementar Citrix ADM como una implementación independiente.
23. Escriba **Sí** para reiniciar el servidor de Citrix ADM.

> **Nota**
>
> Después de instalar Citrix ADM, puede actualizar los valores de configuración inicial más adelante.

Verificación

Una vez instalado el servidor, puede acceder a la GUI escribiendo la dirección IP del servidor de NetScaler ADM en el explorador. Las credenciales de administrador predeterminadas para iniciar

sesión en el servidor son nsroot/nsroot.

El explorador muestra la utilidad de configuración Citrix ADM.

> **Nota**
>
> Cuando se implementa en VMware ESXi, Citrix ADM puede tardar hasta 30 minutos o más en activarse.

NetScaler ADM con servidor KVM Linux

January 30, 2024

Las plataformas de virtualización en las que se puede aprovisionar NetScaler Application Delivery Management (ADM) incluyen Linux-KVM.

Antes de instalar NetScaler ADM en Linux-KVM, asegúrese de que el sistema tiene las extensiones de virtualización de hardware y compruebe que las extensiones de virtualización de CPU están disponibles. Compruebe que *virsh* (una herramienta de línea de comandos para administrar máquinas virtuales) esté disponible en el hipervisor.

Utilice sus credenciales de administrador para iniciar sesión en el sitio web de Citrix.com, acceder a los archivos de configuración de NetScaler ADM más recientes y descargarlos en su equipo. A continuación, instale Citrix ADM en la plataforma Linux-KVM y configúrelo para la red.

Requisitos previos

Antes de instalar el dispositivo virtual Citrix ADM, compruebe que la versión 3.6.11-4 y posteriores de Linux-KVM esté instalada en un hardware que cumpla con los requisitos mínimos.

Requisitos de hardware

Componente	Requisito
CPU	Un procesador x86 de 64 bits con las funciones de virtualización de hardware incluidas en el procesador Intel VT-X. Proporcione al menos 2 núcleos de CPU para alojar Linux-KVM. **Nota** Para comprobar si la CPU es compatible con el host Linux, introduzca el siguiente comando en el símbolo del shell de host Linux: `*. egrep'^flags.\* ( vmx | svm )' /proc/cpuinfo*` Si la configuración del BIOS para la extensión está inhabilitada, debe habilitarlos en el BIOS. No hay ninguna recomendación específica para la velocidad del procesador, pero más alta la velocidad, mejor es el rendimiento de NetScaler ADM.
Memoria (RAM)	Mínimo 4 GB para el kernel Linux host. Agregue memoria adicional según lo requieran las máquinas virtuales.
Disco duro	Calcule el espacio para los requisitos del núcleo y la máquina virtual de Host Linux. Una sola máquina virtual Citrix ADM requiere 120 GB de espacio en disco.

> **Nota**
>
> Los requisitos de memoria y disco duro especificados son para implementar Citrix ADM en la plataforma OpenStack, teniendo en cuenta que no hay otras máquinas virtuales ejecutándose en el host. Los requisitos de hardware para OpenStack dependen del número de máquinas virtuales que se ejecutan en él.

Requisitos de software

Citrix recomienda núcleos más nuevos, como la versión de 64 bits del núcleo 3.6.11-4 o posterior.

Requisitos de la red Citrix ADM solo admite una interfaz de red paravirtualizada de VirtIO. Esta interfaz debe estar conectada a la red de administración del host Linux-KVM para que Citrix ADM y Linux-KVM puedan comunicarse.

Descargar archivos de configuración de NetScaler ADM

Para descargar los archivos de configuración de NetScaler ADM desde www.citrix.com:

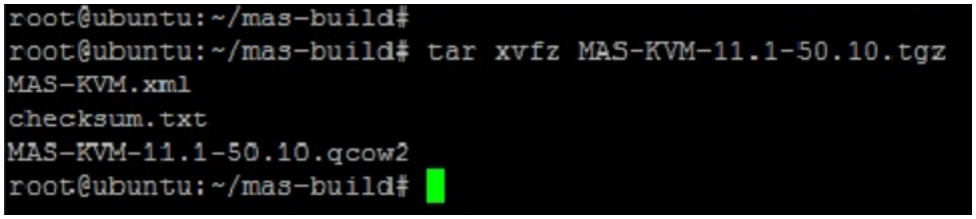
1. Abra un explorador web y escriba www.citrix.com en la barra de direcciones.
2. Pase el cursor sobre la opción **Iniciar sesión y haga clic enMy Account**, escriba sus credenciales de Citrix y, a continuación, vuelva a hacer clic**en Iniciar sesión**.
3. Vaya a la sección **Descargas**.
4. En la lista desplegable **Descargas** , seleccione **Citrix Application Delivery Management** .
5. En la página **NetScaler Application Delivery Management**, seleccione la versión. Por ejemplo, selecciona la **versión 12.1** .
6. Haga clic en **Software de producto** para expandirlo y haga clic en la versión más reciente. Por ejemplo, seleccione **Citrix ADM Release (Feature Phase) 12.1 Build 49.23/49.37**.

   Se muestra la página de creación seleccionada.
7. En la lista desplegable Ir **a la descarga** , seleccione **Imagen Citrix ADM para KVM, 12.1 Build xx.xx**
8. Haga clic en **Descargar archivo**, acepte el contrato de licencia de usuario final y descargue el archivo de imagen comprimido en cualquier carpeta del equipo local.

Instalación de NetScaler Application Delivery Management en Linux-KVM

1. Con SSH, inicie sesión en el host KVM.
2. En la línea de comandos de la CLI, copie la imagen en una carpeta del servidor mediante cualquiera de los programas de transferencia de archivos.
3. Navegue hasta el directorio donde ha guardado la imagen descargada.
4. Realice lo siguiente en la línea de comandos:
   a) Haga una lista de los archivos del directorio y verifique la presencia del archivo de imagen.
   b) Utilice el comando tar para descomprimir el archivo de imagen de Citrix Application Delivery Management. El paquete descomprimido contiene los siguientes componentes:
      i. Un archivo XML de dominio que especifica los atributos de Citrix ADM
      ii. Archivo de texto que especifica la suma de comprobaciones de la imagen de disco del dominio
      iii. Una imagen de disco de dominio


```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--NeedCopy-->
```



iv. Cree una copia de MAS-KVM.xml como MAS1-KVM.xml, como opción de copia de seguridad. Abra el archivo MAS1-KVM.xml mediante el editor vi.

v. Modifique MAS1-KVM.xml para los siguientes atributos de red:

   A. nombre: especifique el nombre.

   B. mac: especifique la dirección MAC.

   C. archivo fuente: especifique la ruta de origen absoluta de la imagen de disco. La ruta del archivo tiene que ser absoluta.

   > **Nota**
   >
   > El nombre de dominio y la dirección MAC deben ser únicos.

   D. modo: especifique el modo.

   E. tipo de modelo: establecido en VirtIO.

   F. source dev: especifique la interfaz.

```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
<!--NeedCopy-->
```

vi. *<FileName\ >Defina los atributos de la máquina virtual en el archivo MAS1-KVM.xml mediante el siguiente comando: virsh define \.xml*

```
virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
<!--NeedCopy-->
```



```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

Inicie Citrix ADM introduciendo el siguiente comando: *virsh start\ [\ <DomainName\ > \ <DomainUUID\ >]*

vii.

```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

root@ubuntu:/home/mas-build#
```

viii. Puede conectarse a la máquina virtual Citrix ADM mediante el siguiente comando: *virsh console\ <DomainName\ >*

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
<!--NeedCopy-->
```

```
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]
```

Configurar NetScaler Application Delivery Management

> **Nota**
>
> En algunos servidores KVM de Linux, los huéspedes de FreeBSD no se reinician correctamente si tienen más de una CPU. Cuando se reinicia el dispositivo virtual Citrix ADM, la CLI y la GUI de Citrix ADM dejan de responder. Para obtener más información, consulte https://bugs.launchpad.net/qemu/+bug/1329956
>
> Para evitar que la CLI y la GUI de NetScaler ADM no respondan cuando se reinicia el dispositivo virtual NetScaler ADM, apague todas las máquinas virtuales del host KVM y realice lo siguiente en el host KVM:
>
> 1. Elimine el módulo kvm_intel con el siguiente comando:

> *rmmod kvm_intel*
>
> 2. Inhabilite APICV y vuelva a cargar el módulo kvm_intel con el siguiente comando: *modprobe kvm_intel enable_apicv=N*
> 3. Inicie las máquinas virtuales en el host KVM.

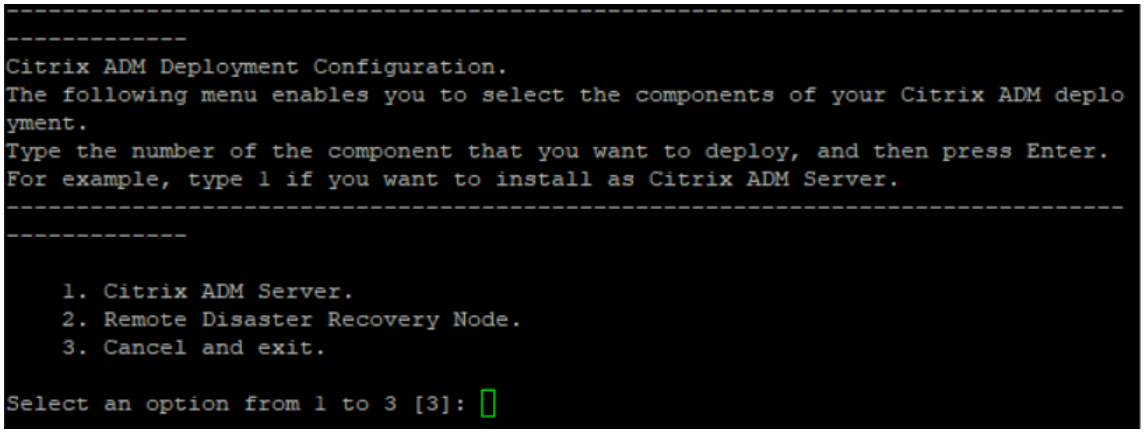
Después de instalar NetScaler ADM, espere unos 10 minutos para que los servicios estén disponibles y, a continuación, inicie sesión en NetScaler ADM.

1. En la línea de comandos, utilice las credenciales de administrador del sistema predeterminadas para iniciar sesión en el sistema:
   - Nombre de usuario: nsroot
   - Contraseña: nsroot

   > **Nota**
   >
   > Tras iniciar sesión por primera vez, debe cambiar la contraseña administrativa. A continuación, configure el MAS para que funcione en su red. Puede cambiar la contraseña desde la interfaz de usuario de NetScaler ADM. En la página principal de Citrix ADM, vaya a **Sistema** > **Administración** de usuarios > **Usuarios** . Seleccione el usuario y haga clic en **Modificar** y, a continuación, actualice la contraseña en el campo Contraseña.

2. Cuando se le solicite, escriba: *shell*
3. Escriba **networkconfig** para acceder al menú de configuración de red inicial de Citrix ADM. Configure la dirección IP de administración.
4. Para completar la configuración de red inicial de Citrix ADM, siga las instrucciones. La consola muestra las opciones de configuración de red iniciales de Citrix ADM para establecer los siguientes parámetros para Citrix ADM. El nombre del host se rellena de forma predeterminada.
   a) Introduzca **2** para actualizar la dirección IPv4 de Citrix ADM: la dirección IP de administración en la que accede a un Citrix ADM
   b) Introduzca **3** para actualizar Máscara de red: Máscara de subred asociada a la dirección IP de administración.
   c) Introduzca **4** para actualizar la dirección IPv4 de la puerta de enlace: la dirección IP de la puerta de enlace predeterminada para la subred de la dirección IP de administración de Citrix ADM
   d) Escriba **7** para guardar y salir: Guarda los cambios de configuración y sale del sistema.

5. Ejecute el script de despliegue escribiendo el comando en la línea de comandos: *deployment_type.py*
6. En la pantalla de implementación que aparece, seleccione el tipo de implementación como **servidor NetScaler ADM**.



7. Escriba **Sí** para implementar NetScaler ADM como implementación independiente.
8. Escriba **Sí** para reiniciar el servidor Citrix ADM.
9. Una vez reiniciado el servidor Citrix ADM, inicie sesión en Citrix ADM con las credenciales de administrador predeterminadas, nsroot/nsroot, a través de la línea de comandos o la GUI.

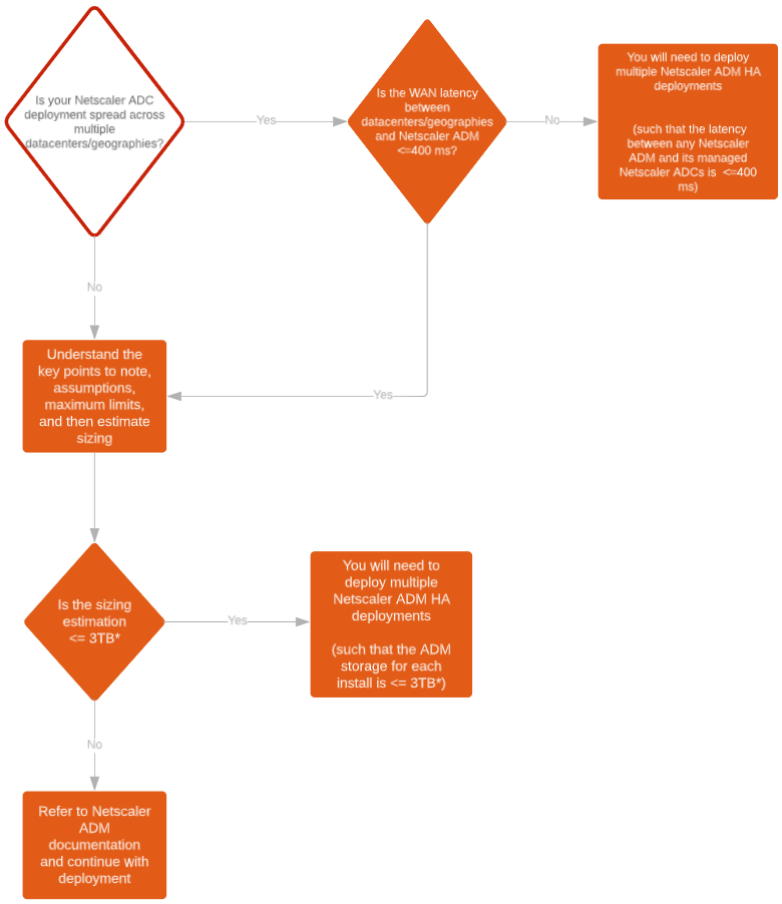
   Más adelante, puede acceder al Citrix ADM escribiendo la dirección IP del servidor Citrix ADM en la barra de direcciones del explorador. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son *nsroot/nsroot* .

Configurar la implementación de alta disponibilidad

January 30, 2024

La alta disponibilidad (HA) se refiere a un sistema que siempre está disponible para el usuario sin interrumpir los servicios. La configuración de alta disponibilidad es crucial durante el tiempo de inactividad del sistema, los errores de la red o las aplicaciones, y es un requisito clave para cualquier empresa. Una implementación de alta disponibilidad de dos nodos Citrix ADM en modo activo-pasivo con las mismas configuraciones proporciona operaciones ininterrumpidas.

Caso de implementación



> **Nota**
>
> El límite máximo de almacenamiento validado para una implementación única de Citrix ADM HA es de 3 TB. Para obtener más información, consulte la guía de implementación.
>
> **Importante**
>
> **Para acceder a Citrix ADM 12.1, compilación 48.18 o versiones posteriores, mediante HTTPS:**
>
> Si ha configurado una instancia de Citrix ADC para equilibrar la carga de Citrix ADM en modo de alta disponibilidad, primero elimine la instancia de Citrix ADC. A continuación, configure una

> dirección IP flotante para acceder a Citrix ADM en modo de alta disponibilidad.

Las siguientes son las ventajas de la implementación de alta disponibilidad en Citrix ADM:

- Un mecanismo mejorado para monitorizar los latidos del corazón entre el nódulo primario y el secundario.
- Proporciona una replicación en streaming física de la base de datos en lugar de una replicación bidireccional lógica.
- Capacidad de configurar la dirección IP flotante en el nodo principal para eliminar la necesidad de un balanceador de cargas Citrix ADC independiente.
- Proporciona un acceso sencillo a la interfaz de usuario de Citrix ADM mediante la dirección IP flotante.
- La interfaz de usuario Citrix ADM solo se proporciona en el nodo principal. Mediante el nodo principal, puede eliminar el riesgo de acceder al nodo secundario y realizar cambios en él.
- La configuración de la dirección IP flotante permite gestionar la situación de conmutación por error y no es necesario volver a configurar las instancias.
- Proporciona la capacidad incorporada para detectar y manejar situaciones de cerebro dividido.

En la siguiente tabla se describen los términos utilizados en la implementación de alta disponibilidad.

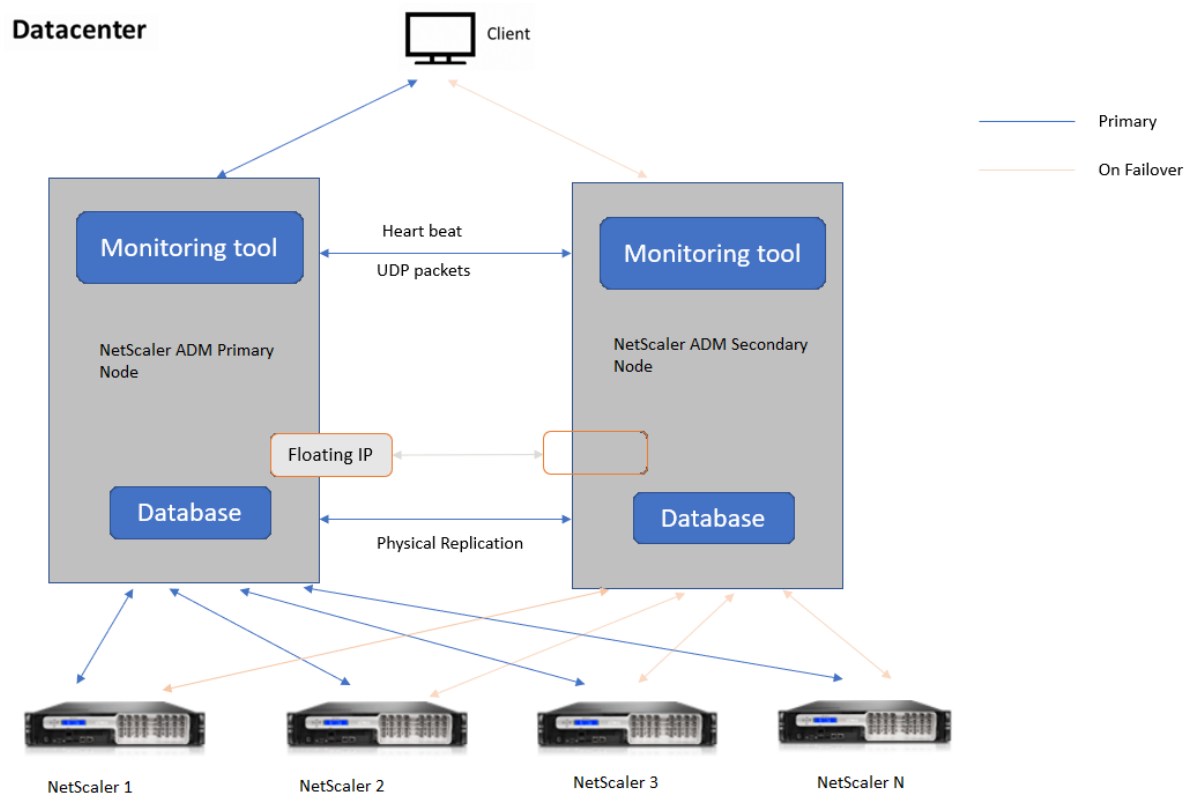
Términos y condiciones	Descripción
Nodo principal	Primer nodo registrado en la implementación de alta disponibilidad.
Nodo secundario	Segundo nodo registrado en la implementación de alta disponibilidad.
Latido	Mecanismo utilizado para intercambiar mensajes entre el nodo principal y el secundario en la configuración de alta disponibilidad. Los mensajes determinan el estado y el estado de la aplicación en cada nodo individual.

Términos y condiciones	Descripción
Dirección IP flotante	Una IP flotante es una dirección IP que se puede mover instantáneamente de un nodo a otro de la misma subred. Internamente, se configura como un alias en la interfaz de red del nodo principal. Si se produce una conmutación por error, la dirección IP flotante se mueve sin problemas de la antigua principal a la nueva. Es útil en la configuración de alta disponibilidad porque permite a los clientes comunicarse con los nodos de alta disponibilidad mediante una sola dirección IP.

> **Nota**
>
> Para obtener más información sobre los detalles de puertos y protocolos, consulte Puertos.

Componentes de la arquitectura de alta disponibilidad

En la siguiente ilustración se muestra la arquitectura de dos nodos Citrix ADM implementados en modo de alta disponibilidad.



En la implementación de alta disponibilidad, un nodo Citrix ADM se configura como nodo principal (MAS 1) y el otro como nodo secundario (MAS 2). Si el nodo principal cae por algún motivo, el nodo secundario se hace cargo como el nuevo nodo principal.

Herramienta de monitorización

La herramienta de supervisión es un proceso interno que se utiliza para supervisar, alertar y gestionar situaciones de conmutación por error. La herramienta está activa y se ejecuta en cada nodo en alta disponibilidad. Es responsable de iniciar los subsistemas, iniciar la base de datos en ambos nodos, decidir cuál es el nodo principal o el secundario en caso de que se produzca una conmutación por error, etc.

Nodo principal

El nodo principal acepta las conexiones y administra las instancias. El nodo principal administra todos los procesos, como AppFlow, SNMP, LogStream, syslog, etc. El acceso a la interfaz de usuario de Citrix ADM está disponible en el nodo principal. La dirección IP flotante se configura en el nodo principal.

Nodo secundario

El nodo secundario escucha los mensajes de latidos del corazón enviados desde el nodo principal. La base de datos del nodo secundario solo está en modo de lectura-réplica. Ninguno de los procesos está activo en el nodo secundario y no se puede acceder a la interfaz de usuario de Citrix ADM en el nodo secundario.

Replicación de transmisión física

Los nodos primario y secundario se sincronizan mediante el mecanismo de los latidos del corazón. Con la replicación física en streaming de la base de datos, el nodo secundario se inicia en modo de lectura-réplica. El nodo secundario escucha los mensajes de latidos del corazón recibidos del nodo principal. Si el nodo secundario no recibe ningún latido cardíaco durante un período de tiempo de 180 segundos, se considera que el nodo principal está inactivo. A continuación, el nodo secundario pasa a ser el nodo principal.

Mensajes de latidos

Los mensajes Heartbeat son paquetes de datagramas de usuario (UDP) que se envían y reciben entre el nodo principal y el secundario. Supervisa todos los subsistemas de Citrix ADM y la base de datos para intercambiar información sobre el estado, el estado, los procesos, etc. del nodo. La información se comparte entre los nodos de alta disponibilidad cada segundo. Las notificaciones se envían como alertas al administrador si se produce una conmutación por error o una interrupción de los estados de alta disponibilidad.

Dirección IP flotante

La dirección IP flotante está asociada al nodo principal en la configuración de alta disponibilidad. Es un alias asignado a la dirección IP del nodo principal que el cliente puede utilizar para conectarse a Citrix ADM en el nodo principal. Como la dirección IP flotante está configurada en el nodo principal, no es necesaria la reconfiguración de la instancia en caso de conmutación por error. Las instancias se vuelven a conectar a la misma dirección IP para llegar a la nueva primaria.

Puntos clave a tener en cuenta

- En una configuración de alta disponibilidad, los dos nodos Citrix ADM se implementan en modo activo-pasivo. Deben estar en las mismas subredes con la misma versión y compilación de software, y tener las mismas configuraciones.

- Dirección IP flotante:
  - La dirección IP flotante se configura en el nodo principal.
  - No es necesario volver a configurar las instancias si se produce una conmutación por error.
  - Puede acceder a un nodo de alta disponibilidad desde la interfaz de usuario, ya sea mediante la IP del nodo principal o la dirección IP flotante.

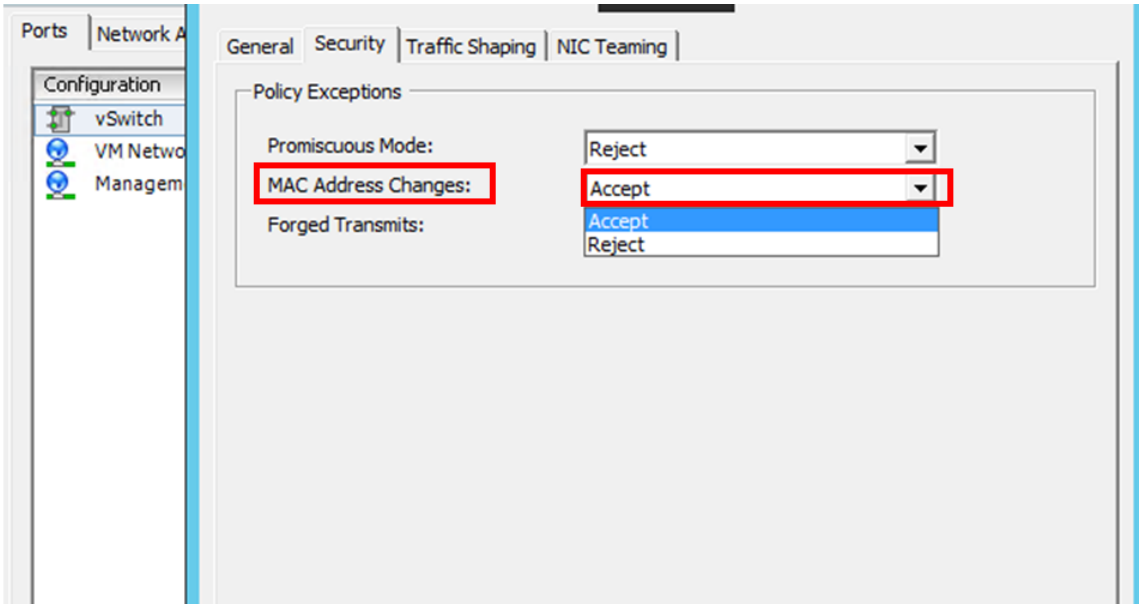
    > **Nota**
    >
    > Citrix recomienda utilizar la dirección IP flotante para acceder a la interfaz de usuario.

- Base de datos:
  - En una configuración de alta disponibilidad, todos los archivos de configuración se sincronizan automáticamente del nodo principal al nodo secundario en un intervalo de un minuto.
  - La sincronización de bases de datos se realiza al instante mediante la replicación física de la base de datos.
  - La base de datos del nodo secundario está en modo de lectura-réplica.

- Actualización de Citrix ADM:
  - Los procesos internos actualizan implícitamente Citrix ADM desde las versiones anteriores.

    > **Nota**
    >
    > Una vez que la actualización se haya realizado correctamente, debe configurar la dirección IP flotante.

- El puerto UDP predeterminado 5005 está disponible tanto en los nodos para enviar latidos como para recibir mensajes.
- Dirección MAC
  La configuración de la opción "Cambios de dirección MAC"de un hipervisor afecta al tráfico que recibe una máquina virtual. Permitir que los cambios de dirección MAC se habiliten en el conmutador virtual para que la dirección IP flotante se mueva sin problemas al nuevo nodo principal después de la conmutación por error.
  Por ejemplo, al implementar Citrix ADM con alta disponibilidad en Vmware ESXi, asegúrese de aceptar los cambios en la dirección MAC. ESXi ahora permite que las solicitudes cambien la dirección MAC activa a otra que la dirección MAC inicial.



Requisitos previos

Antes de configurar la alta disponibilidad para los nodos Citrix ADM, tenga en cuenta los siguientes requisitos previos:

- La implementación de alta disponibilidad de Citrix ADM es compatible con la versión 12.0, compilación 51.24 de Citrix ADM.
- Descargue el archivo de imagen de Citrix Application Delivery Management (.xva) del sitio de descargas de Citrix: https://www.citrix.com/downloads/

Citrix recomienda establecer la prioridad de la CPU (en las propiedades de la máquina virtual) en el nivel más alto para mejorar el comportamiento de la programación y la latencia de la red.

En la siguiente tabla se enumeran los requisitos mínimos para los recursos informáticos virtuales:

Componente	Requisito
RAM	**32 GB**
CPU virtual	**8 CPUs**

Componente	Requisito
Espacio de almacenamiento	Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Si sus requisitos de almacenamiento de Citrix ADM superan los 120 GB, debe conectar un disco adicional. **Nota** Solo puede agregar un disco adicional. Citrix recomienda estimar el almacenamiento y adjuntar disco adicional en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps
Hypervisor	**Versiones**
Citrix Hypervisor	6.2 y 6.5
VMware ESXi	5.5 y 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu y Fedora

Para configurar Citrix ADM en modo de alta disponibilidad

1. Registre e implemente el primer servidor (nodo principal).
2. Registre e implemente el segundo servidor (nodo secundario).
3. Implementar el nodo principal y secundario para la configuración de alta disponibilidad.

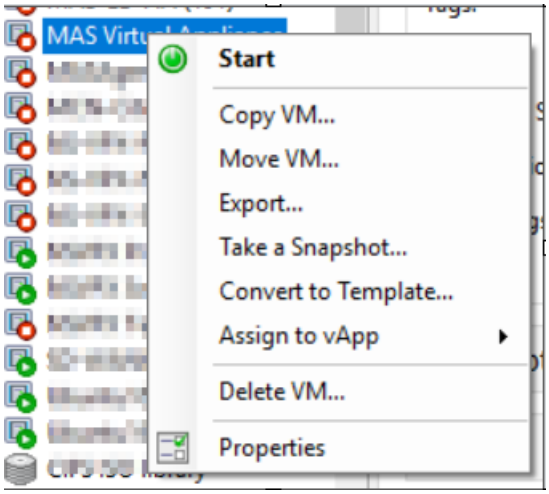
Registrar e implementar el primer servidor (nodo principal)

Para registrar el primer nodo:

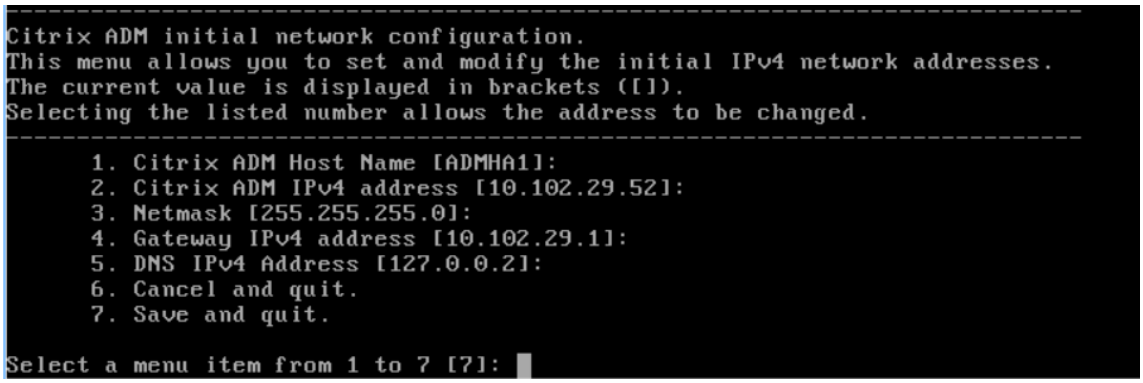
1. Utilice el archivo de imagen.xva descargado del sitio de descargas de Citrix e impórtelo al hipervisor.

> **Nota:**
>
> Es posible que el archivo de imagen.xva tarde unos minutos en importarse y comenzar. Puede ver el estado en la parte inferior de la pantalla.
>
>
>

2. Una vez que la importación se haya realizado correctamente, haga clic con el botón derecho y haga clic en **Inicio**.



3. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales.

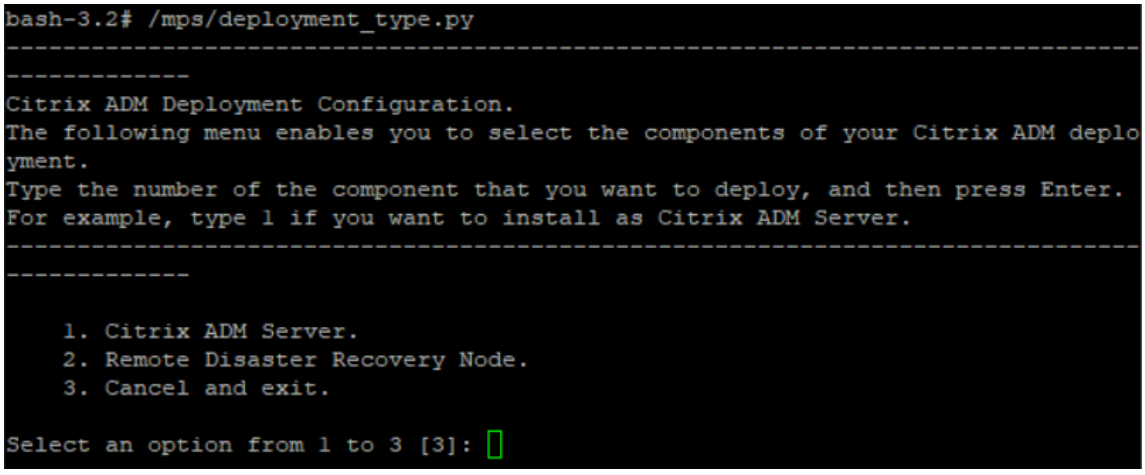


4. Una vez completada la configuración de red inicial, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: *nsrecover/nsroot*.

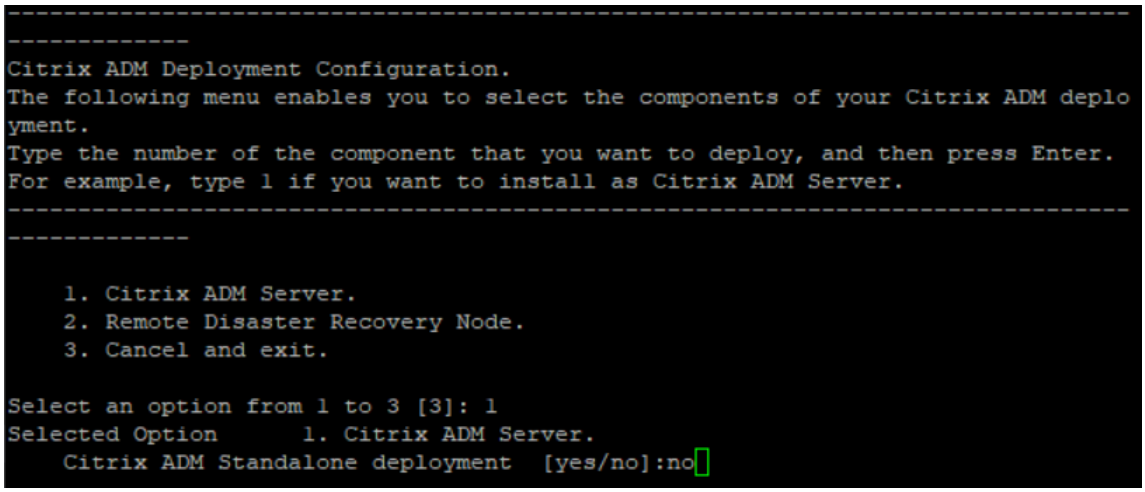
> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

5. Para implementar el nodo principal, escriba **/mps/deployment_type.py**. Aparece el menú de configuración de implementación de Citrix ADM .

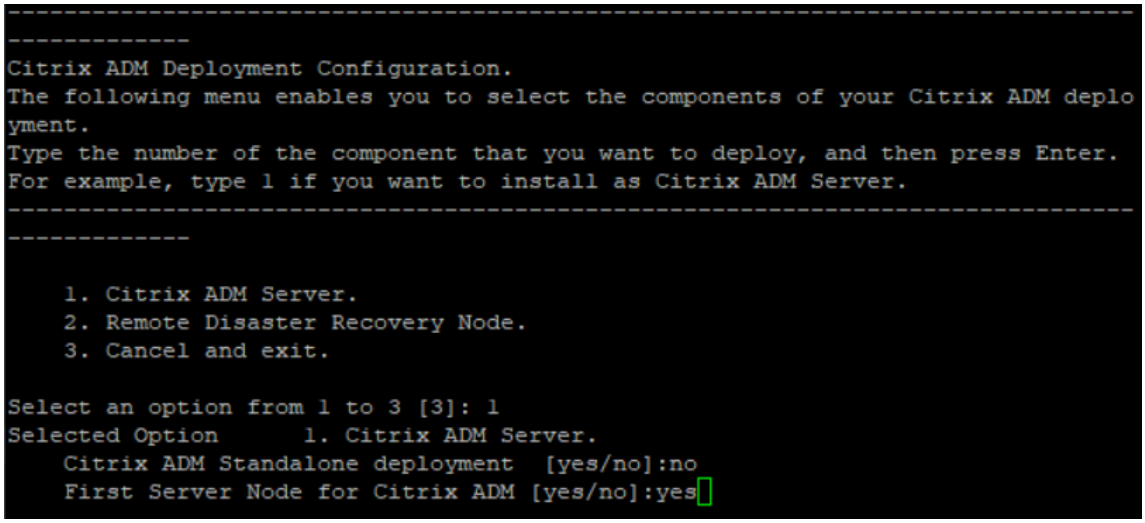
6. Seleccione **1** para registrar el servidor Citrix ADM como nodo principal.



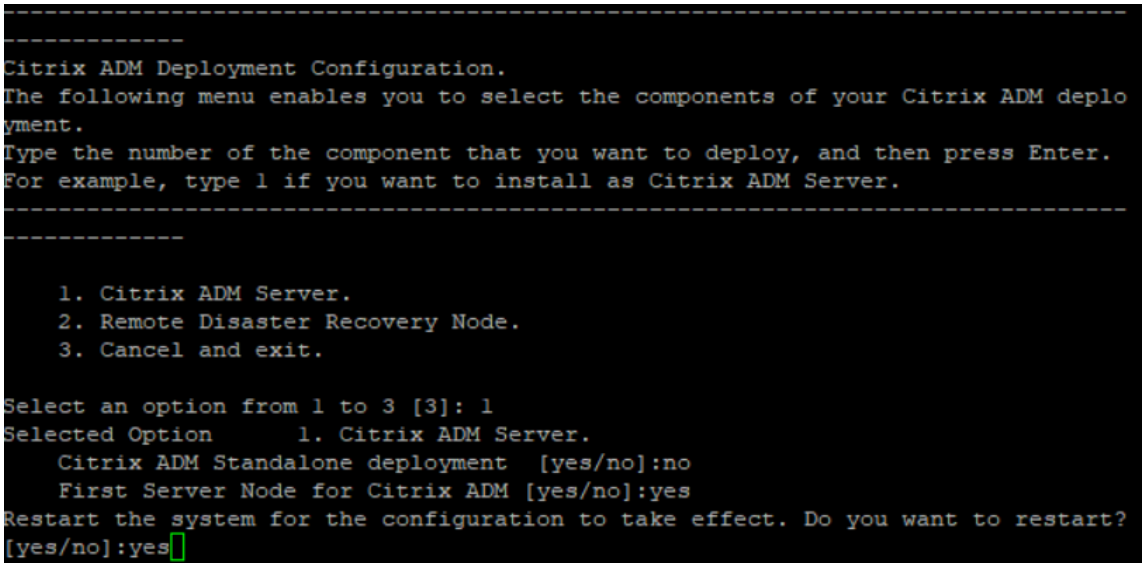
7. La consola le pide que seleccione la implementación independiente de Citrix ADM. Introduzca**No** para confirmar la implementación como alta disponibilidad.



8. La consola le pide que seleccione el primer nodo del servidor. Escriba**Sí** para confirmar el nodo como el primer nodo.



9. La consola le pide que reinicie el sistema. Escriba**Sí** para reiniciar.



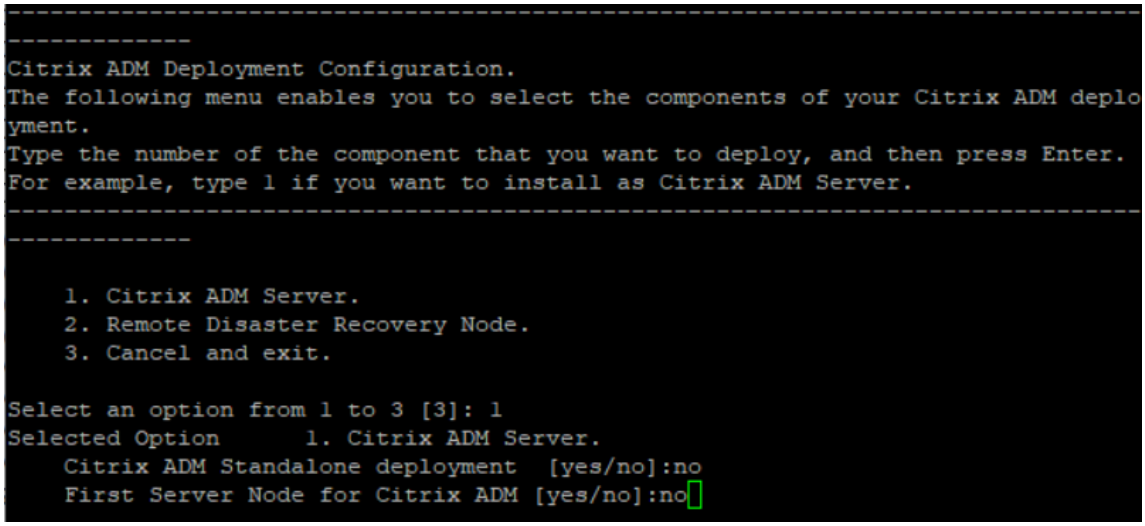
El sistema se reinicia y se muestra como nodo principal en la interfaz de usuario de Citrix ADM.

Registrar e implementar el segundo servidor (nodo secundario)

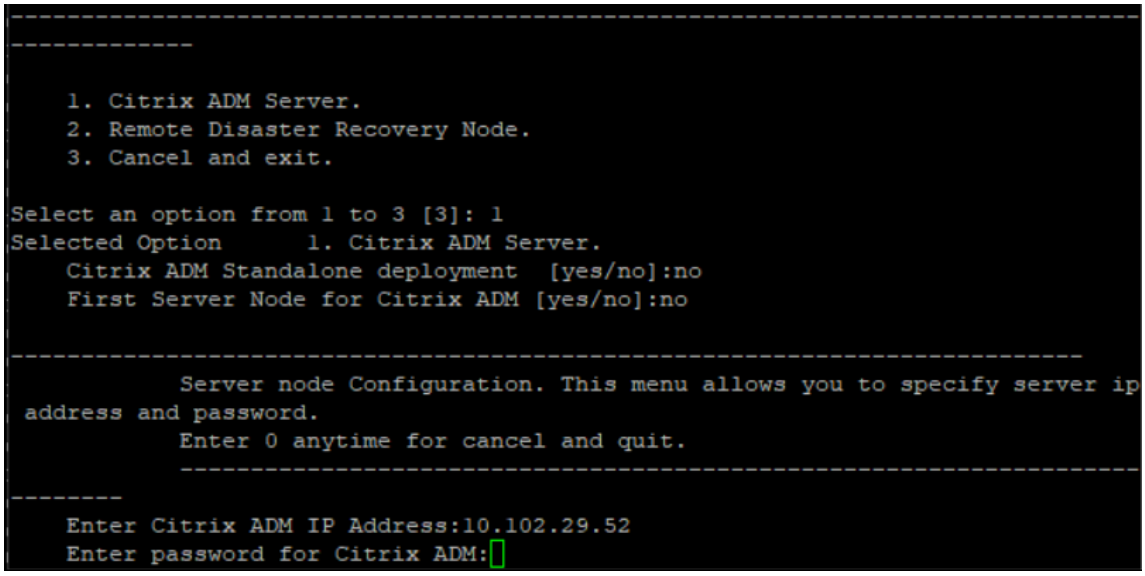
1. Utilice el archivo de **imagen.xva** descargado del sitio de descargas de Citrix e impórtelo al hipervisor.
2. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales, como se muestra en la siguiente imagen.
3. Una vez completada la configuración inicial de la red, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: *nsrecover/nsroot*.

> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

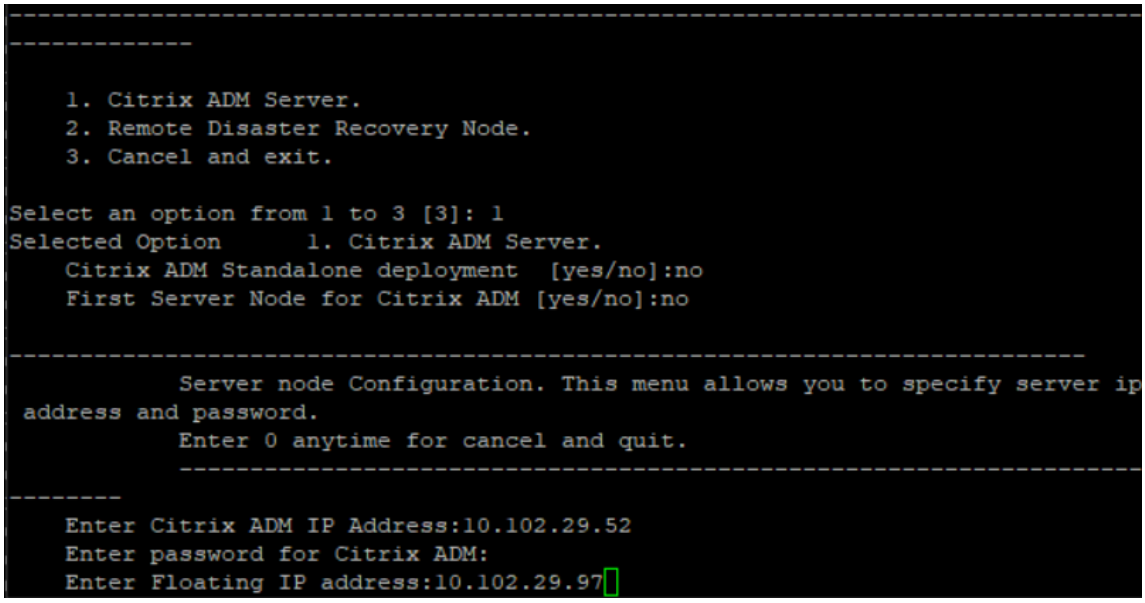
4. Para implementar el nodo secundario, escriba **/mps/deployment_type.py**. Aparece el menú de configuración de implementación de Citrix ADM.
5. Seleccione **1** para registrar el servidor Citrix ADM como nodo secundario.
6. La consola le pide que seleccione Citrix ADM como implementación independiente. Introduzca**No** para confirmar la implementación como alta disponibilidad.
7. La consola le pide que seleccione el primer nodo del servidor. Escriba**No** para confirmar el nodo como segundo servidor.



8. La consola le pide que introduzca la dirección IP y la contraseña del nodo principal.



9. La consola le pide que introduzca la dirección IP flotante.



10. La consola le pide que reinicie el sistema. Escriba**Sí** para reiniciar.

> **Nota**
>
> - La dirección IP flotante es obligatoria para la implementación de nodos de alta disponibilidad.
> - El sistema mostrará mensajes de error si hay algún problema en la configuración.
> - El sistema se reinicia y las configuraciones tardan unos minutos en surtir efecto.

Implemente el nodo principal y el secundario como un par de alta disponibilidad

Tras el registro, los nodos principales y secundarios se muestran en la interfaz de usuario de Citrix ADM. Implemente estos nodos en un par de alta disponibilidad.

> **Nota**
>
> - Antes de implementar los nodos en un par de alta disponibilidad, asegúrese de que el nodo secundario se haya completado con un reinicio, después de la configuración inicial de la red.
> - Una vez finalizada la implementación de alta disponibilidad, utilice la dirección IP flotante para acceder a la interfaz de usuario de Citrix ADM.

Para implementar nodos como un par de alta disponibilidad:

1. Abra un explorador web e introduzca la dirección IP del primer nodo del servidor Citrix ADM.

2. En los campos**Nombre de usuario**y**contraseña**, introduzca las credenciales de administrador.
3. Haga clic en **Comenzar** en la página de inicio.
4. Seleccione el tipo de implementación como**Dos servidores implementados en modo de alta disponibilidad**y haga clic en**Siguiente**.
5. En la página Implementación, haga clic en**Implementar**.
6. Aparece un mensaje de confirmación. Haga clic en **Sí**.

   Citrix ADM se reinicia y tarda aproximadamente 10 minutos en que la configuración surta efecto.

   > Nota:
   >
   > Ahora puede comenzar a usar la dirección IP flotante.

7. Inicie sesión en Citrix ADM con credenciales de administrador, haga clic en **Comenzar** en la página de inicio y, si lo quiere, complete lo siguiente:

   a) Agregar instancias de Citrix ADC

   b) Configurar la identidad del cliente

   > Nota:
   >
   > También puede hacer clic en **Omitir** para completarlo más tarde y hacer clic en **Finalizar**.

8. Navegue hasta **Sistema** > **Implementación** para validar la implementación.

   Para obtener más información, consulte las Preguntas frecuentes.

Inhabilitar alta disponibilidad

Puede inhabilitar la alta disponibilidad en un par de alta disponibilidad de Citrix ADM y convertir los nodos en servidores Citrix ADM independientes.

> **Nota**
>
> Desactive la alta disponibilidad desde el nodo principal.

Para inhabilitar la alta disponibilidad:

1. En un explorador web, introduzca la dirección IP del nodo principal del servidor Citrix ADM.
2. En los campos **Nombre de usuario**y**Contraseña**, introduzca las credenciales del administrador.

3. En la ficha**Sistema**, vaya a**Deployment** y haga clic en**Break HA**.

   Se muestra un cuadro de diálogo. Haga clic en **Sí** para interrumpir la implementación de alta disponibilidad.

Reimplemente la alta disponibilidad

Después de inhabilitar la alta disponibilidad en una implementación independiente, puede volver a implementarla en el modo de alta disponibilidad. Redistribuir alta disponibilidad es similar a la primera implementación de alta disponibilidad. Para obtener más información, consulte Implementar el nodo principal y el secundario como un par de alta disponibilidad.

Casos de conmutación por error de alta disponibilidad

Se produce una conmutación por error si se da una de las siguientes condiciones:

- **Fallo de nodo**: el nodo principal deja de funcionar y no se detecta ningún latido del nodo principal durante 180 segundos.
- **Error de mantenimiento de la aplicación**: El nodo principal está activo y en ejecución, pero uno de los procesos Citrix ADM está inactivo.

Caso de cerebro dividido

Cuando no hay comunicación entre ambos nodos debido a un tiempo de inactividad en el enlace de red, entonces:

- El nodo principal sigue funcionando como principal
- El nódulo secundario pasa a ser el primario debido a la incapacidad de recibir los latidos del corazón
- Ambos nodos ejecutarían sus instancias de bases de datos individuales

Por ejemplo, en una empresa se han implementado dos nodos Citrix ADM como principales y secundarios. Debido a un posible tiempo de inactividad del enlace de red, la comunicación entre los dos nodos de Citrix ADM se interrumpe por completo. Como no hay intercambio de latidos durante más de 180 segundos, ambos nodos se consideran el nodo principal. Ambos nodos actúan como nodos activos y ejecutan sus propias instancias de base de datos.

Con Citrix ADM 12.1, esta situación de cerebro dividido se gestiona sin problemas una vez restaurados el enlace de red y el latido del corazón. La sincronización de alta disponibilidad se restaura automáticamente. El tiempo de recuperación depende de los datos y de la velocidad del enlace entre los nodos.

> **Nota**
>
> Durante la afección de cerebro dividido, los cambios que se produjeron en el nodo principal antiguo se restablecen con el nuevo primario cuando se vuelve a unir a él en alta disponibilidad. Los cambios que ocurrieron en el nuevo nodo primario durante el split-brain permanecen intactos.

Configurar la recuperación ante desastres para alta disponibilidad

January 30, 2024

El desastre es una interrupción repentina de las funciones empresariales causada por desastres naturales o eventos causados por seres humanos. Los desastres afectan a las operaciones del centro de datos, después de lo cual los recursos y los datos perdidos en el sitio del desastre deben reconstruirse y restaurarse por completo. La pérdida de datos o el tiempo de inactividad en el centro de datos es fundamental y colapsa la continuidad del negocio.

La función de recuperación ante desastres (DR) de Citrix ADM 12.1 proporciona capacidades completas de copia de seguridad y recuperación del sistema para Citrix ADM implementado en modo de alta disponibilidad. En el momento de la recuperación, los certificados, los archivos de configuración y una copia de seguridad completa de la base de datos están disponibles en el sitio de recuperación.

En la tabla siguiente se describen los términos que se utilizan al configurar la recuperación ante desastres en Citrix ADM.

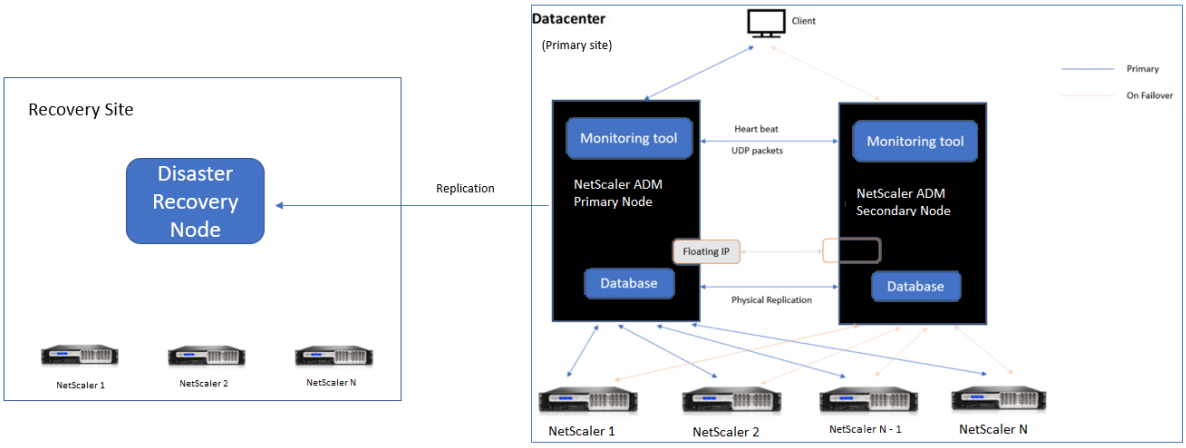
Términos y condiciones	Descripción
Sitio principal (centro de datos A)	El sitio principal tiene nodos Citrix ADM implementados en modo de alta disponibilidad.
Sitio de recuperación (centro de datos B)	El sitio de recuperación tiene un nodo de recuperación ante desastres implementado en modo independiente. Este nodo está en modo de solo lectura y no estará operativo hasta que el sitio principal esté inactivo.
Nodo de recuperación ante desastres	El nodo de recuperación es un nodo independiente implementado en el sitio de recuperación. Este nodo se pone en funcionamiento (para el nuevo servidor principal) en caso de que se produzca un desastre en el sitio principal y no funcione.

> Nota: El sitio principal y el sitio DR se comunican entre sí a través de los puertos 5454 y 22, y estos puertos están habilitados de forma predeterminada.
> Para obtener más información sobre los detalles de puertos y protocolos, consulte Puertos.

Flujo de trabajo de recuperación ante desastres

La siguiente imagen muestra el flujo de trabajo de recuperación ante desastres, la configuración inicial antes del desastre y el flujo de trabajo posterior al desastre.

Configuración inicial antes del desastre



La imagen muestra la configuración de recuperación ante desastres antes del desastre.

El sitio principal tiene nodos Citrix ADM implementados en el modo de alta disponibilidad. Para obtener más información, consulte Implementación de alta disponibilidad

El sitio de recuperación tiene un nodo de recuperación ante desastres de Citrix ADM independiente implementado de forma remota. El nodo de recuperación ante desastres está en modo de solo lectura y recibe datos del nodo principal para crear copias de seguridad de datos. También se detectan instancias de Citrix ADC en el sitio de recuperación, pero no hay tráfico que fluya a través de ellas. Durante el proceso de copia de seguridad, todos los datos, archivos y configuraciones se replican en el nodo de recuperación ante desastres desde el nodo principal.

Requisitos previos

Antes de configurar el nodo de recuperación ante desastres, tenga en cuenta los siguientes requisitos previos:

- Para habilitar la configuración de recuperación ante desastres, el sitio principal debe tener los nodos Citrix ADM configurados en modo de alta disponibilidad.
- La implementación independiente de Citrix ADM en el sitio principal no admite la función de recuperación ante desastres.
- El par Citrix ADM HA (en el sitio principal) y el nodo independiente (en el sitio de recuperación ante desastres) deben tener la misma versión de software, compilación y configuraciones.

Citrix recomienda establecer la prioridad de la CPU (en las propiedades de la máquina virtual) en el nivel más alto para mejorar el comportamiento de la programación y la latencia de la red.

En la siguiente tabla se enumeran los requisitos mínimos para configurar el nodo de recuperación ante desastres:

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs
Espacio de almacenamiento	Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Si sus requisitos de almacenamiento de Citrix ADM superan los 120 GB, debe conectar un disco adicional. **Nota** Solo puede agregar un disco adicional. Citrix recomienda estimar el almacenamiento y adjuntar disco adicional en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps
Hypervisor	**Versiones**
Citrix Hypervisor	6.2 y 6.5
VMware ESXi	5.5 y 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu y Fedora

Configuración de recuperación ante desastres por primera vez

- Implementar Citrix ADM en modo de alta disponibilidad
- Implementar y registrar el nodo de recuperación ante desastres de Citrix ADM
- Habilitar y inhabilitar la configuración de recuperación ante desastres desde la interfaz de usuario

Implementar Citrix ADM en modo de alta disponibilidad

Para configurar la configuración de recuperación ante desastres, asegúrese de que Citrix ADM esté implementado en modo de alta disponibilidad. Para obtener información sobre la implementación de Citrix ADM en alta disponibilidad, consulteImplementación de alta disponibilidad

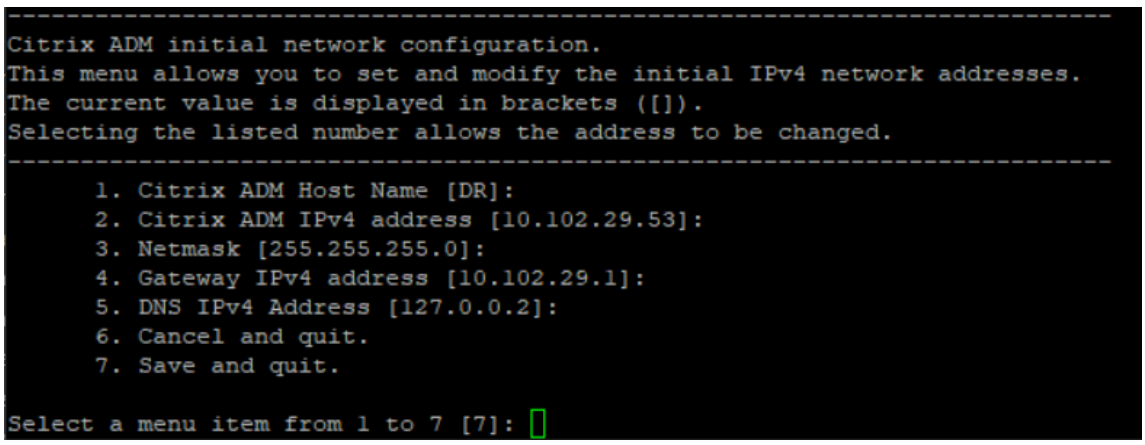
> **Nota**
>
> - Citrix ADM implementado en modo de alta disponibilidad debe actualizarse a la versión 12.1 de Citrix ADM.
> - **La dirección IP flotante es obligatoria** para registrar el nodo de recuperación ante desastres con el nodo principal.

Implementar y registrar el nodo de recuperación ante desastres de Citrix ADM

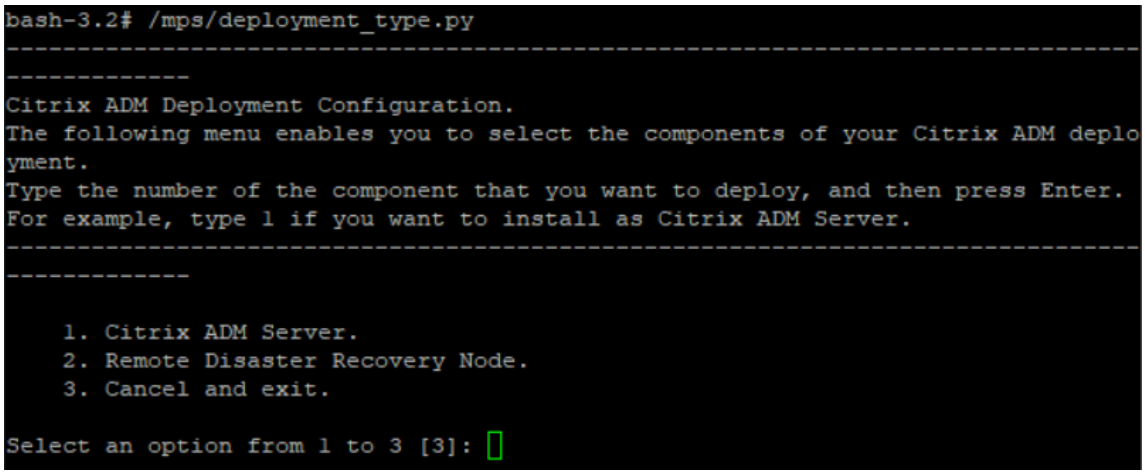
Para registrar el nodo de recuperación ante desastres de Citrix ADM:

1. Descargue el archivo de imagen.xva del sitio de descargas de Citrix e impórtelo a su hipervisor.
2. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales.

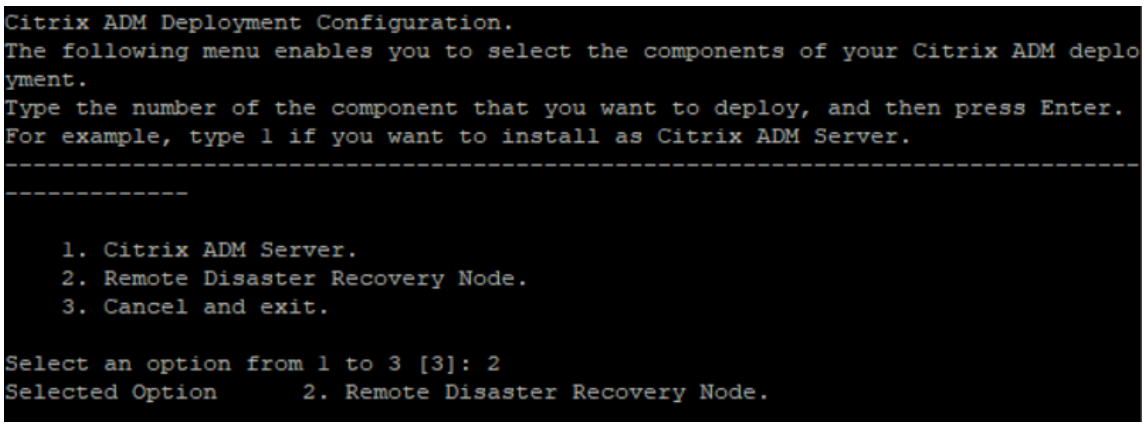
> **Nota**
>
> El nodo de recuperación ante desastres puede estar en una subred diferente.



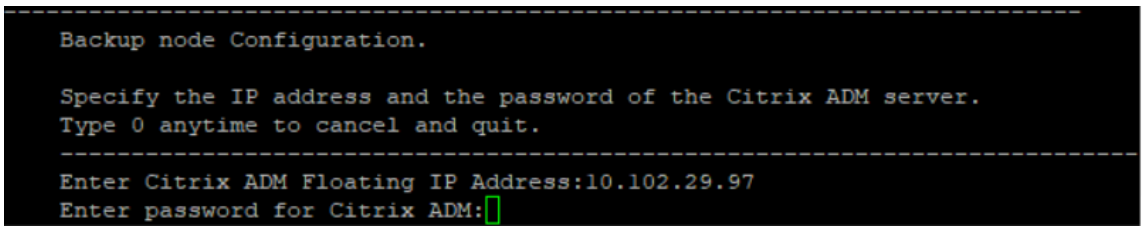
3. Una vez completada la configuración de red inicial, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: *nsrecover/nsroot* .
4. Para implementar el nodo de recuperación ante desastres, escriba **/mps/deployment_type.py** y presione Entrar. Aparece el menú de configuración de implementación de Citrix ADM.



5. Seleccione **2** para registrar el nodo de recuperación ante desastres.



6. La consola solicita la dirección IP flotante del nodo de alta disponibilidad y la contraseña.
7. Introduzca la dirección IP flotante y la contraseña para registrar el nodo de recuperación ante desastres en el nodo principal.



El nodo de recuperación ante desastres se ha registrado correctamente.

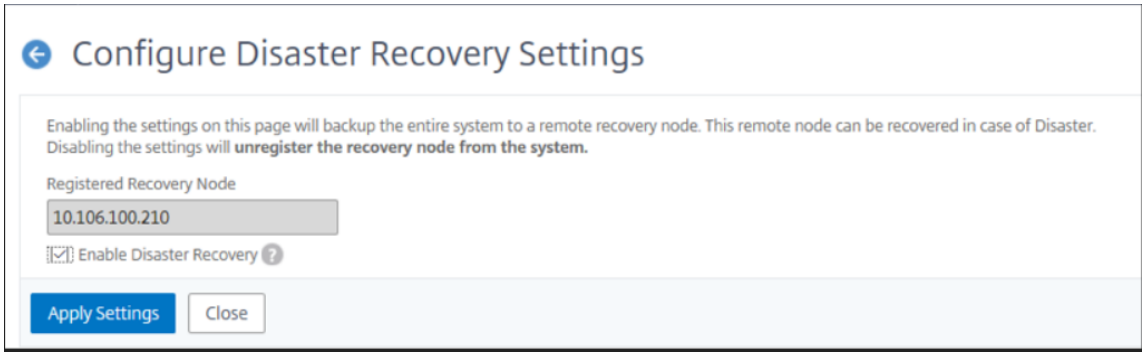

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
    ------------------------------------------------------------------------
```

> **Nota**
>
> El nodo de recuperación ante desastres no tiene una GUI.

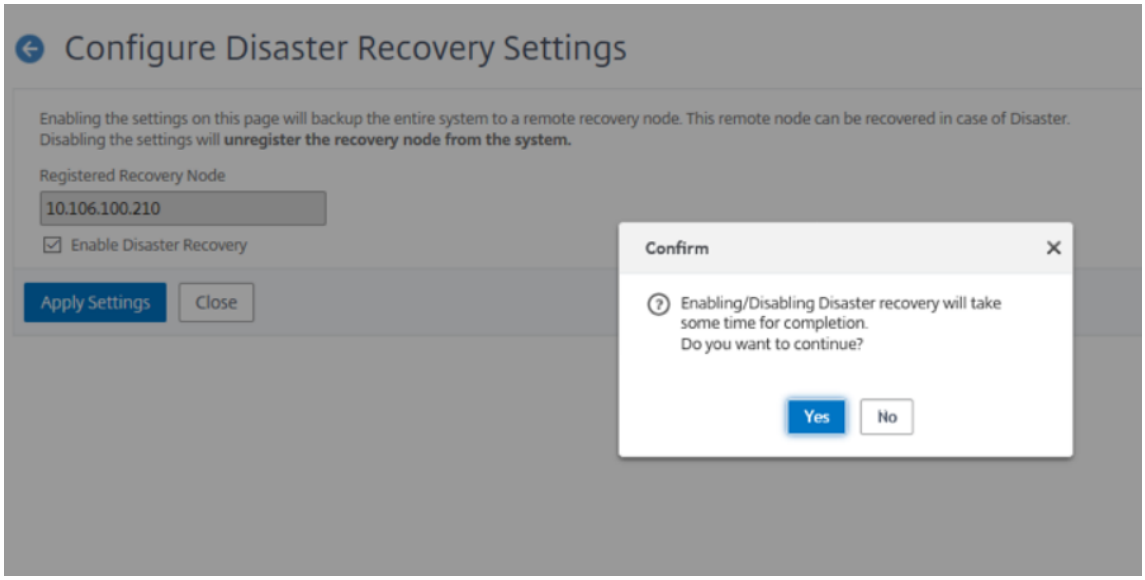
Habilite la configuración de recuperación ante desastres desde la GUI de Citrix ADM

Una vez que el nodo de recuperación ante desastres se haya registrado correctamente, puede habilitar la configuración de recuperación ante desastres desde la interfaz de usuario del sitio principal de Citrix ADM.

1. Vaya a **Sistema > Administración del sistema > Configuración de recuperación ante desastres.**
2. En la página **Configurar las opciones de recuperación** ante desastres , seleccione la casilla Habilitar la recuperación ante desastres y haga clic en **Aplicar configuración** .



3. Se muestra un cuadro de diálogo de confirmación. Haga clic en **Sí** para continuar.



> **Nota**
>
> El tiempo necesario para realizar la copia de seguridad del sistema depende del tamaño de los datos y de la velocidad del enlace WAN (red de área amplia).

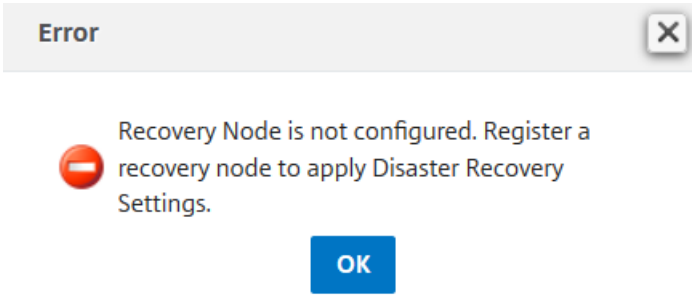
Para deshabilitar la configuración de recuperación ante desastres, desactive la casilla **Habilitar recuperación ante desastres** y haga clic en **Aplicar configuración.**

Se muestra un cuadro de diálogo de confirmación. Haga clic en**Sí** para continuar.

> **Importante**
>
> - Es responsabilidad del administrador detectar que se ha producido un desastre en el sitio principal.
> - El flujo de trabajo de recuperación ante desastres no está automatizado y el administrador debe iniciarlo manualmente después de que el sitio principal deje de funcionar.
> - Un administrador debe iniciar manualmente el proceso ejecutando una script de recuperación en el nodo de recuperación ante desastres en el sitio de recuperación.
> - Si actualiza el par HA en el sitio principal, debe actualizar manualmente el nodo independiente en el sitio de DR.

Si inhabilita la opción **Habilitar recuperación ante desastres** y hace clic en **Aplicar configuración** , Citrix ADM no le permite volver a seleccionar la opción **Habilitar recuperación ante desastres** .

Al hacer clic en **Configuración de recuperación ante desastres** , aparece el siguiente mensaje de error:



Para volver a habilitar el nodo DR, vuelva a configurar el nodo DR para el par de alta disponibilidad:

a) Inicie sesión en el nodo DR mediante un Hypervisor o una consola SSH.

b) Configure el nodo de recuperación ante desastres siguiendo el procedimiento disponible en Implementar y registrar el nodo de recuperación ante desastres de Citrix ADM.

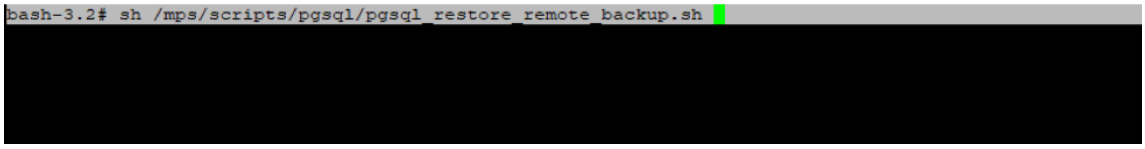
c) Habilite la opciónde recuperación ante desastres.

Para obtener más información, consulte las Preguntas frecuentes.

Flujo de trabajo después del desastre

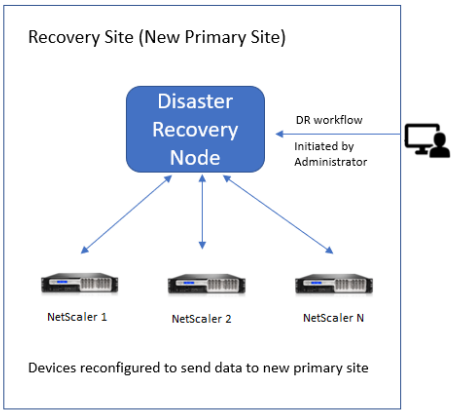
Cuando el sitio principal deja de funcionar después de un desastre, el flujo de trabajo de recuperación ante desastres se debe iniciar de la siguiente manera:

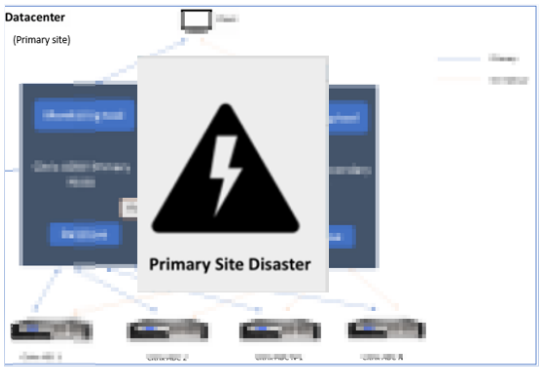
1. El administrador identifica que un desastre ha afectado al sitio principal y que no está operativo.
2. El administrador inicia el proceso de recuperación.
3. El administrador debe ejecutar manualmente el siguiente script de recuperación en el nodo de recuperación ante desastres (en el sitio de recuperación): **/mps/scripts/pgsql/pgsql_restore_remote_backup.sh**



4. Internamente, las instancias Citrix ADC se reconfiguran automáticamente para enviar los datos al nodo de recuperación ante desastres que ahora se ha convertido en el nuevo sitio principal.

   La imagen siguiente muestra que el flujo de trabajo de recuperación ante desastres después de que el sitio principal se golpea con un desastre.





> Nota:
>
> Después de iniciar el script en el sitio de DR, el sitio de DR ahora se convierte en el nuevo sitio principal. También puede acceder a la interfaz de usuario DR.

Recuperación posterior a desastres

Una vez que se haya producido el desastre y el administrador inicie el script de recuperación, el sitio de recuperación ante desastres pasará a ser el nuevo sitio principal.

> **Importante**
>
> - Si ha instalado Citrix ADM 12.1.49.x o versiones anteriores, dispone de un período de gracia de 30 días para ponerse en contacto con Citrix para volver a alojar la licencia original en Citrix ADM (en el sitio de recuperación ante desastres).
> - Para la versión 12.1.50.x o versiones posteriores, la licencia Citrix ADM se sincroniza automáticamente con el sitio de recuperación ante desastres (no es necesario ponerse en contacto con Citrix para obtener la licencia).
> - La licencia agrupada para el sitio de DR se admite desde la versión 12.1.50.x o versiones posteriores. Si ha aplicado licencias agrupadas para las instancias, vuelva a configurar manualmente las instancias en el sitio de recuperación ante desastres.

Configurar agentes en prem para la implementación en varios sitios

January 30, 2024

En las versiones anteriores de Citrix ADM, las instancias de Citrix ADC implementadas en centros de datos remotos podían administrarse y supervisarse desde Citrix ADM que se ejecutaba en un centro de

datos principal. Las instancias Citrix ADC enviaron datos directamente a la instancia principal de Citrix ADM que dieron como resultado el consumo de ancho de banda WAN (Wide Area Network). Además, el procesamiento de los datos de análisis utiliza los recursos de CPU y memoria del Citrix ADM principal.

Los clientes tienen sus centros de datos ubicados en todo el mundo. Los agentes juegan un papel vital en los siguientes escenarios en los que los clientes pueden elegir:

- instalar agentes en centros de datos remotos para reducir el consumo de ancho de banda de la WAN.
- para limitar el número de instancias que envían tráfico directamente al Citrix ADM principal para el procesamiento de datos.

> **Nota**
>
> - Se recomienda instalar agentes para instancias en el centro de datos remoto, pero no es obligatorio. Si es necesario, los usuarios pueden agregar directamente instancias de Citrix ADC al Citrix ADM principal.
> - Si ha instalado agentes para los centros de datos remotos, la comunicación entre los agentes y el sitio principal se realiza a través de una dirección IP flotante. Para obtener más información, consulte port.
> - Puede instalar agentes y aplicar licencias agrupadas a las instancias de los centros de datos remotos. En este escenario, la comunicación entre el sitio principal y los centros de datos remotos se realiza a través de la dirección IP flotante.

En Citrix ADM 12.1, las instancias se pueden configurar con agentes para que se comuniquen con el Citrix ADM principal ubicado en un centro de datos diferente.

> **Nota**
>
> Los agentes locales para la implementación en varios sitios solo se admiten con la implementación de alta disponibilidad de Citrix ADM.

Los agentes funcionan como intermediarios entre la instancia principal de Citrix ADM y las instancias descubiertas en diferentes centros de datos. Los siguientes son los beneficios de instalar agentes:

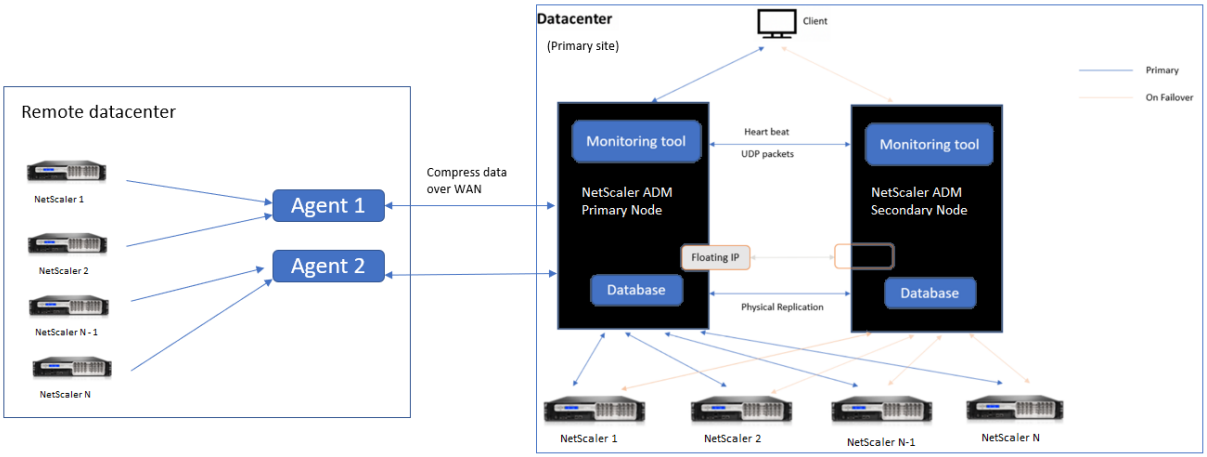
- Las instancias se configuran para agentes de modo que los datos no procesados se envíen directamente a los agentes en lugar de la instancia principal de Citrix ADM. Los agentes realizan el primer nivel de procesamiento de datos y envían los datos procesados en formato comprimido al Citrix ADM principal para su almacenamiento.
- Los agentes y las instancias se encuentran en el mismo centro de datos para que el procesamiento de datos sea más rápido.

- La agrupación en clústeres de los agentes proporciona una redistribución de instancias de Citrix ADC en caso de conmutación por error del agente. Cuando un agente de un sitio falla, el tráfico de las instancias de Citrix ADC se cambia a otro agente disponible en el mismo sitio.

> **Nota**
>
> El número de agentes que se instalarán por sitio depende del tráfico que se esté procesando. Actualmente, Citrix ha validado dos agentes por sitio para el escenario de conmutación por error de agentes. Citrix recomienda instalar al menos dos agentes por sitio, de modo que el tráfico fluya a otro agente en caso de que se produzca una conmutación por error del agente.

Arquitectura

En la siguiente ilustración se muestran las instancias de Citrix ADC en dos centros de datos y la implementación de alta disponibilidad de Citrix ADM mediante una arquitectura basada en agentes multisitio.



El sitio principal tiene los nodos Citrix ADM implementados en una configuración de alta disponibilidad. Las instancias de Citrix ADC del sitio principal se registran directamente en Citrix ADM.

En el sitio secundario, los agentes se implementan y registran con el servidor Citrix ADM en el sitio principal. Estos agentes trabajan en un clúster para gestionar el flujo continuo de tráfico en caso de que se produzca una conmutación por error del agente. Las instancias de Citrix ADC del sitio secundario se registran en el servidor Citrix ADM principal a través de agentes ubicados en ese sitio. Las instancias envían datos directamente a los agentes en lugar de la instancia principal de Citrix ADM. Los agentes procesan los datos recibidos de las instancias y los envían a la instancia principal de Citrix ADM en un formato comprimido. Los agentes se comunican con el servidor de Citrix ADM a través de un canal seguro y los datos enviados por el canal se comprimen para aumentar la eficiencia del ancho de banda.

Introducción

- Instalar el agente en un centro de datos
  - Registrar el agente
  - Agregar el agente
- Agregar instancias de Citrix ADC
  - Agregar una nueva instancia
  - Actualizar una instancia existente

Instalar el agente en un centro de datos

Puede instalar y configurar el agente para habilitar la comunicación entre la instancia principal de Citrix ADM y las instancias administradas de Citrix ADC en otro centro de datos.

Puede instalar un agente en los siguientes hipervisores del centro de datos de su empresa:

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Servidor KVM Linux

> **Nota**
>
> Los agentes locales para la implementación en varios sitios solo se admiten con la implementación de alta disponibilidad de Citrix ADM.

Antes de comenzar a instalar el agente, asegúrese de que dispone de los recursos informáticos virtuales necesarios que el Hypervisor debe proporcionar para cada agente.

Componente	Requisito
RAM	8 GB **Nota**: Citrix recomienda aumentar el valor predeterminado a 32 GB para mejorar el rendimiento.
CPU virtual	2 CPU

Componente	Requisito
	Nota: Citrix recomienda aumentar el valor predeterminado a 8 CPU para mejorar el rendimiento.
Espacio de almacenamiento	30 GB
Interfaces de red virtual	1
Rendimiento	1 Gbps

Puertos

A efectos de comunicación, los siguientes puertos deben estar abiertos entre el agente y el servidor de Citrix ADM on-prem.

Tipo	Puerto	Detalles
TCP	8443, 7443, 443	Para la comunicación entrante y saliente entre el agente y el servidor de Citrix ADM on-prem.

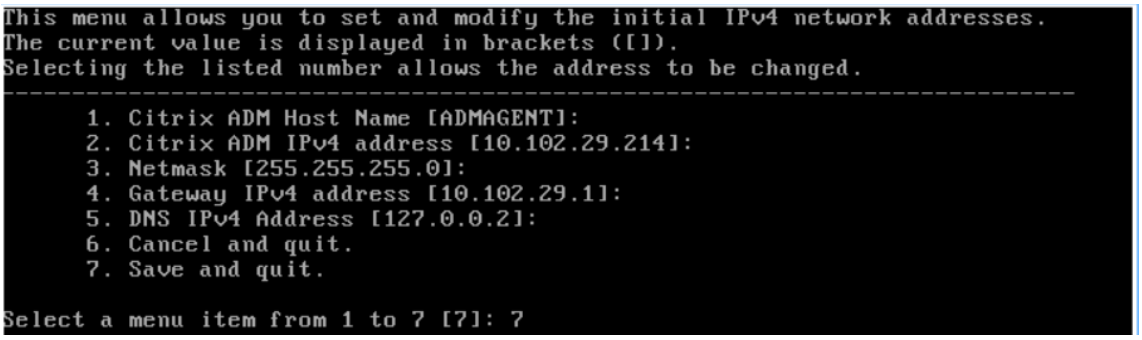
Los siguientes puertos deben estar abiertos entre el agente y las instancias de Citrix ADC.

Tipo	Puerto	Detalles
TCP	80	Para la comunicación NITRO entre el agente y la instancia Citrix ADC o Citrix SD-WAN.
TCP	22	Para la comunicación SSH entre el agente y la instancia de Citrix ADC o Citrix SD-WAN. Para la sincronización entre los servidores Citrix ADM implementados en modo de alta disponibilidad.

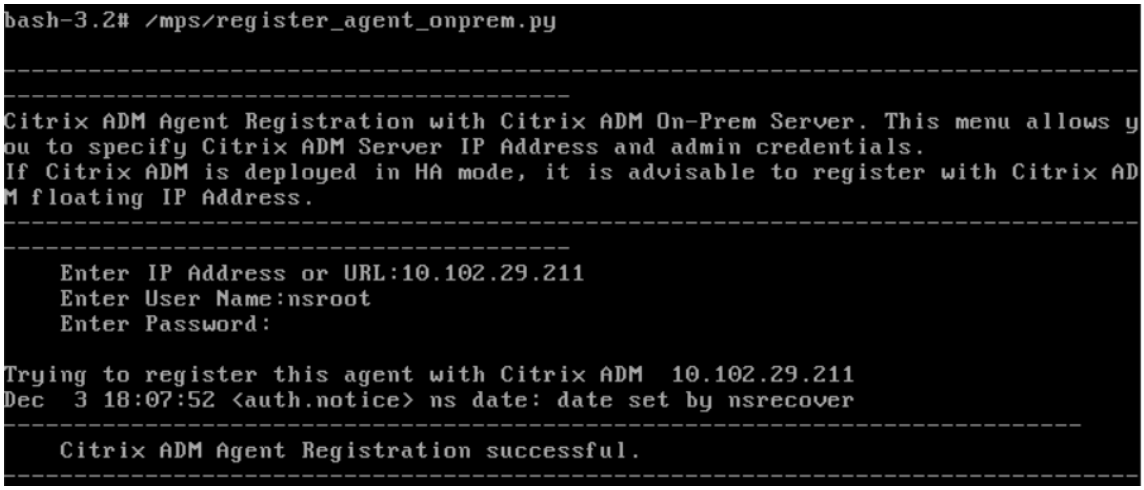
Tipo	Puerto	Detalles
UDP	4739	Para la comunicación de AppFlow entre el agente y la instancia Citrix ADC o Citrix SD-WAN.
ICMP	Sin puerto reservado	Detectar la accesibilidad de la red entre las instancias Citrix ADM y Citrix ADC, las instancias SD WAN o el servidor Citrix ADM secundario implementado en modo de alta disponibilidad.
SNMP	161, 162	Para recibir eventos SNMP desde la instancia de Citrix ADC al agente.
Syslog	514	Para recibir mensajes de syslog de la instancia de Citrix ADC o Citrix SD-WAN al agente.
TCP	5557	Para la comunicación de flujo de registros entre el agente y las instancias de Citrix ADC.

Registrar el agente

1. Utilice el archivo de imagen del agente descargado desde el sitio de descarga de Citrix e impórtelo en el Hypervisor. <Version.no\ >El patrón de nombres del archivo de imagen del agente es el siguiente:**MASAGENT- \-**<HYPERVISOR\ >. Por ejemplo: **MASAGENT-XEN-12.1-xy.xva**
2. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales.
3. Introduzca el nombre de host de Citrix ADM, la dirección IPv4 y la dirección IPv4 de la puerta de enlace. Seleccione la opción 7 para guardar y salir de la configuración.



4. Una vez que el registro se realiza correctamente, la consola le pedirá que inicie sesión. Utilice *nsrecover/nsroot* como credenciales.
5. Para registrar el agente, escriba**/mps/register_agent_onprem.py**. Las credenciales de registro del agente Citrix ADM se muestran como se muestra en la siguiente imagen.
6. Introduzca la dirección IP flotante Citrix ADM y las credenciales de usuario.



Una vez que el registro se realiza correctamente, el agente se reinicia para completar el proceso de instalación.

Una vez reiniciado el agente, acceda a la GUI de Citrix ADM y, en el menú principal, vaya **a la página Redes > Agentes** para comprobar el estado del agente.El agente recién agregado se muestra en estado **Activo**.

> **Nota**
>
> Citrix ADM muestra la versión del agente y también comprueba si el agente está en la versión más reciente. El icono de descarga indica que el agente no está en la versión más reciente y debe actualizarse. Citrix recomienda actualizar la versión del agente a la versión de Citrix ADM.

Agregar agente al sitio

1. Seleccione el agente y haga clic en **Adjuntar sitio.**
2. En la página**Adjuntar sitio**, seleccione un sitio de la lista o cree uno nuevo con el botón más (+).
3. Haz clic en **Guardar.**

> **Nota**
>
> - De forma predeterminada, todos los agentes recién registrados se agregan al centro de datos predeterminado.

> - Es importante asociar el agente con el sitio correcto. En caso de que se produzca un error en el agente, las instancias de Citrix ADC asignadas se conmutan automáticamente a otros agentes en funcionamiento en el mismo sitio.

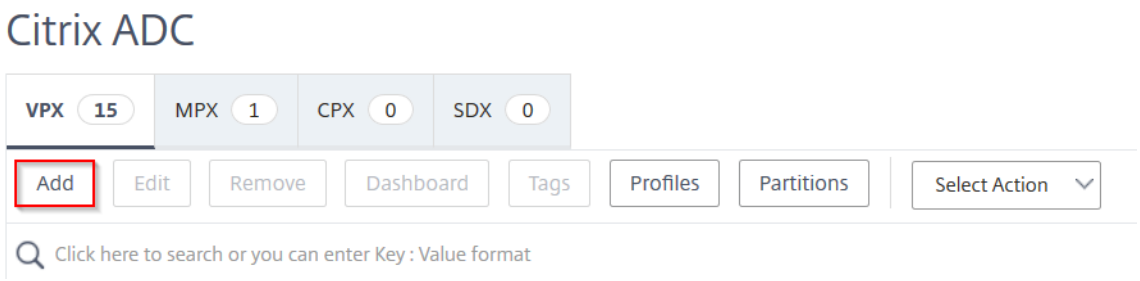
Agregar instancias de Citrix ADC

Las instancias son dispositivos Citrix o dispositivos virtuales que quiere descubrir, administrar y supervisar desde Citrix ADM a través de agentes. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a Citrix ADM o agentes:

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WO

Agregar una nueva instancia

1. Vaya a **Redes > Instancias** y seleccione el tipo de instancia. Por ejemplo, Citrix ADC.
2. Haga clic en **Agregar**para agregar una nueva instancia.

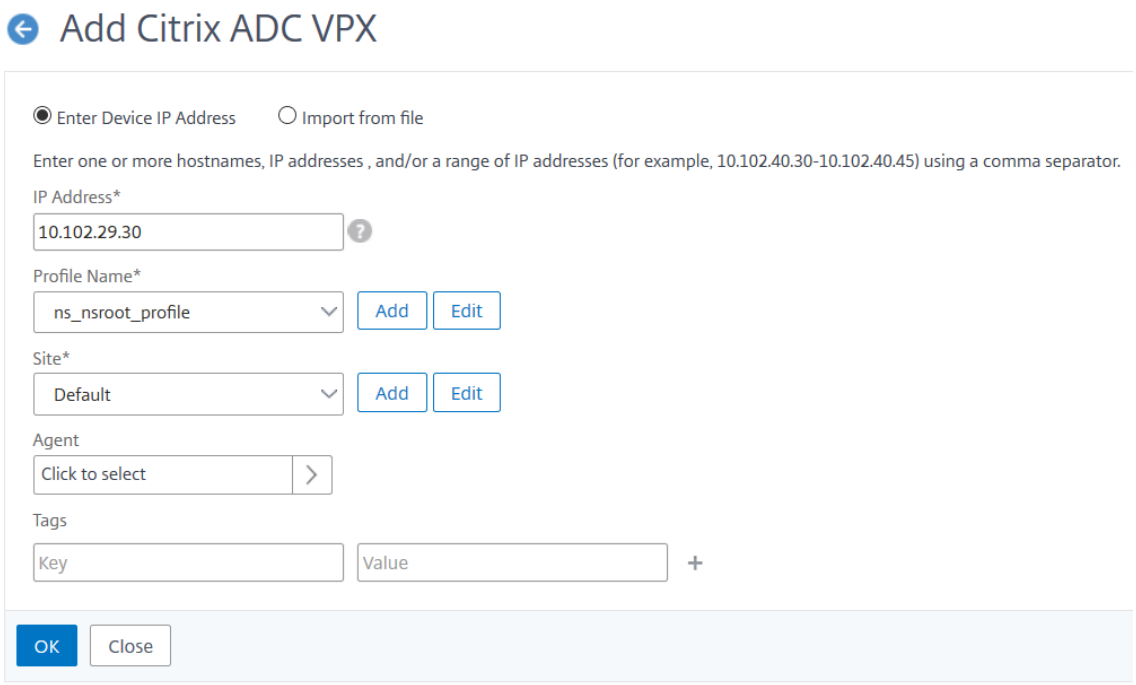


3. Marque **Introducir la dirección IP del dispositivo** e introduzca la dirección IP.
4. En Nombre del**perfil** , seleccione el perfil de instancia apropiado o cree uno nuevo haciendo clic en el icono**+** .

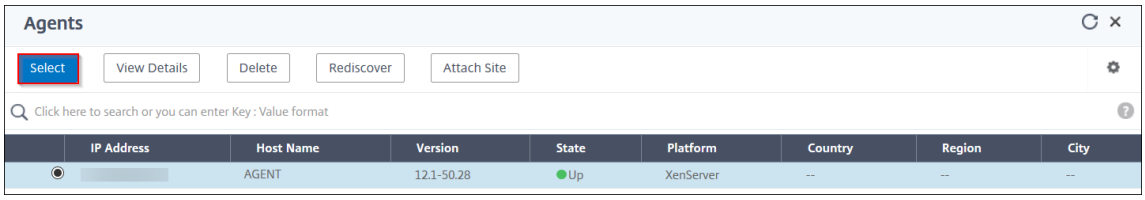
> **Nota**
>
> Para cada tipo de instancia, hay un perfil predeterminado disponible. Por ejemplo, ns-root-profile es el perfil predeterminado para las instancias de Citrix ADC.

5. Selecciona el **sitio** al que quieres asociar la instancia.

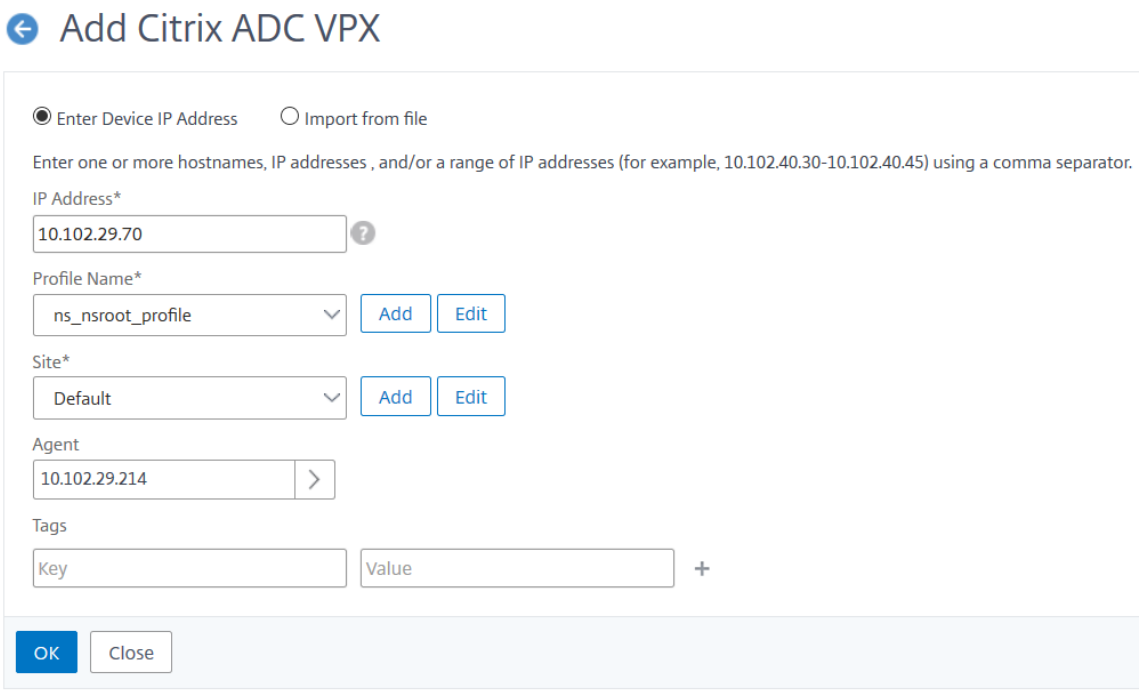
> **Nota**
>
> Según el sitio seleccionado, se muestra la lista de agentes asociados a ese sitio. Asegúrese de seleccionar el **sitio** al que quiere asociar la instancia.



6. Haga clic para seleccionar el agente. En la página**Agente**, seleccione el agente al que quiere asociar la instancia y, a continuación, haga clic en**Seleccionar**.



7. En la página Agregar Citrix VPX, haga clic en **Aceptar**.



Actualizar una instancia existente para adjuntarla a un agente

Si ya se ha agregado una instancia al Citrix ADM principal, puede adjuntarla a un agente editando el flujo de trabajo de adición de instancias y seleccionando un agente.

1. Vaya a **Redes > Instancias** y seleccione el tipo de instancia. Por ejemplo, Citrix ADC.
2. Haga clic en el botón **Modificar** para editar una instancia existente.
3. Haga clic para seleccionar el agente.
4. En la página**Agente**, seleccione el agente al que quiere asociar la instancia y, a continuación, haga clic en**Aceptar**.

> **Nota**
>
> Asegúrese de seleccionar el **sitio** al que quiere asociar la instancia.

Acceder a la GUI de una instancia para validar eventos

Una vez agregadas las instancias y configurado el agente, acceda a la GUI de una instancia para comprobar si el destino de la captura está configurado.

En Citrix ADM, vaya a**Redes > Instancias**. En**Instancias**, seleccione el tipo de instancia a la que quiere acceder (por ejemplo, Citrix ADC VPX) y, a continuación, haga clic en la dirección IP de una instancia específica.

La GUI de la instancia seleccionada se muestra en una ventana emergente.

De forma predeterminada, el agente está configurado como destino de captura en la instancia. Para confirmarlo, inicie sesión en la GUI de la instancia y compruebe los destinos de las trampas.

> **Importante**
>
> Se recomienda agregar un agente para las instancias de Citrix ADC en centros de datos remotos, pero no es obligatorio.
>
> En caso de que quiera agregar la instancia directamente al MAS principal, no seleccione**un agente** al agregar instancias.

Agrupa el agente

El término **clúster de agentes** se refiere a un mecanismo en el que los agentes adjuntos a un sitio se agrupan de forma lógica, de modo que, si uno de los agentes falla, las instancias de Citrix ADC que le envían tráfico se reconfiguran automáticamente para empezar a enviar tráfico a los otros agentes en buen estado de ese grupo o sitio.

La ventaja de tener agentes agrupados en un sitio remoto es que, si un agente falla, Citrix ADM lo detecta e implícitamente todas las instancias se redistribuyen a otros agentes disponibles en ese clúster.

Por ejemplo, tenemos dos agentes 10.106.1xx.2x y 10.106.1xx.7x que están conectados y operativos en el sitio de Bangalore, como se muestra a continuación.

Si un agente deja de funcionar, Citrix ADM lo detectará y mostrará el estado como inactivo.

Las instancias adjuntas a ese agente se reconfiguran automáticamente para usar el otro agente del mismo clúster como destino de captura, servidor syslog, etc.

> **Nota:**
>
> Habrá algún retraso al reconfigurar las instancias.

Migrar la implementación de un solo servidor de Citrix ADM a una implementación de alta disponibilidad

January 30, 2024

Puede actualizar su servidor único Citrix ADM a una implementación de alta disponibilidad de dos servidores Citrix ADM. Un par de servidores Citrix ADM de alta disponibilidad están en modo activo-

pasivo y ambos servidores tienen la misma configuración. En este tipo de implementación activa-pasiva, un servidor Citrix ADM se configura como nodo principal y el otro como nodo secundario. Si por alguna razón, el nodo principal deja de funcionar, el nodo secundario toma el relevo.

Para migrar un servidor único de Citrix ADM a un par de alta disponibilidad, debe aprovisionar un nuevo nodo de servidor Citrix ADM, configurarlo como el segundo servidor único de Citrix ADM e implementar ambos servidores Citrix ADM como un par de alta disponibilidad.

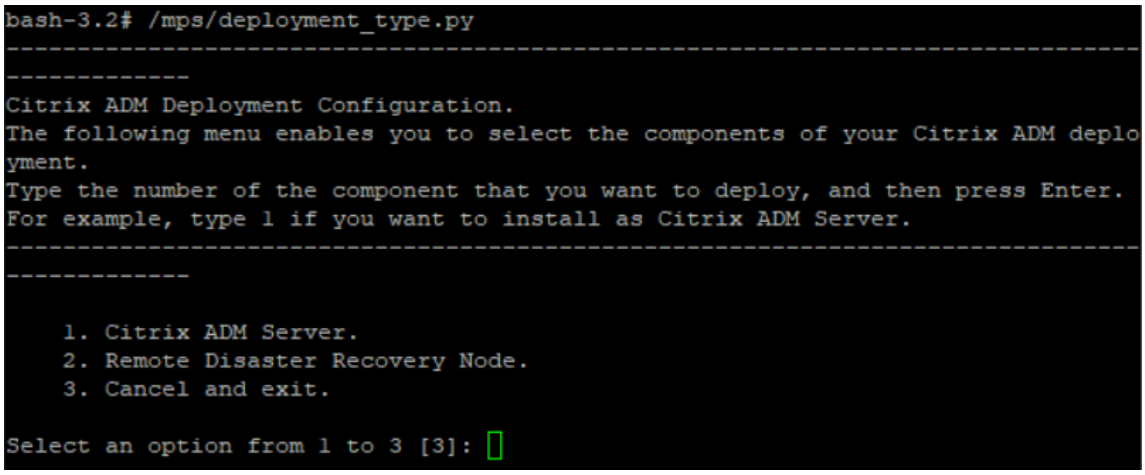
La migración de un servidor único Citrix ADM a un modo de alta disponibilidad implica los siguientes pasos:

1. Modificación del nodo de servidor existente
2. Provisioning del segundo nodo del servidor
3. Implementación de los dos nodos en modo HA
4. Configuración del par de alta disponibilidad

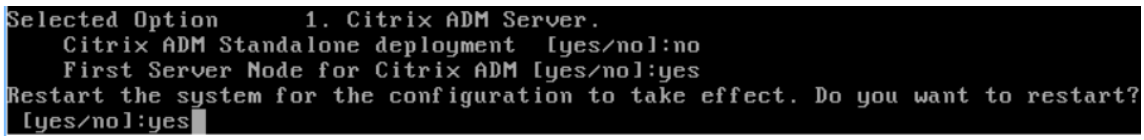
Modificar el nodo del servidor Citrix ADM existente

Para migrar Citrix ADM del modo de servidor único al modo de alta disponibilidad, debe cambiar el tipo de implementación inicial del nodo del servidor al modo de alta disponibilidad.

1. En una estación de trabajo o portátil, abra la consola del nodo del servidor Citrix ADM existente. Por ejemplo, considere que ha implementado un Citrix ADM con la dirección IP 10.106.171.17 como servidor independiente.
2. Inicie sesión en Citrix ADM. Las credenciales predeterminadas son nsroot y nsroot.
3. En la línea de comandos del shell, escriba **/mps/deployment_type.py**y presione **Entrar**.
4. Seleccione el tipo de implementación como servidor Citrix ADM. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.



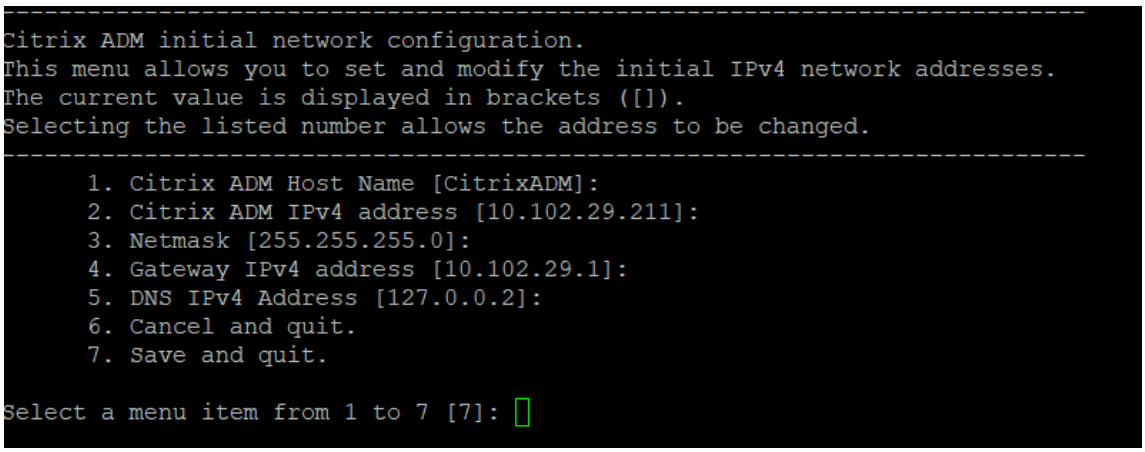
5. La consola de implementación le pide que seleccione la implementación del servidor (como independiente). Escriba **No** para confirmar la implementación como par de alta disponibilidad.
6. La consola le pide que seleccione el (primer nodo del servidor). Introduzca **Sí** para confirmar que el nodo es el primer nodo del servidor.
7. La consola le pide que reinicie el servidor.
8. Escriba **Sí** para reiniciar.



Aprovisione el segundo nodo del servidor

Debe aprovisionar el segundo servidor del hipervisor. Utilice el mismo archivo de imagen que utilizó para instalar el primer servidor u obtenga un archivo de imagen de la misma versión en el sitio de descargas de Citrix.

1. Importe el archivo de imagen al Hypervisor y, a continuación, desde la ficha Consola, configure las opciones de configuración de red iniciales como se explica en la siguiente pantalla:



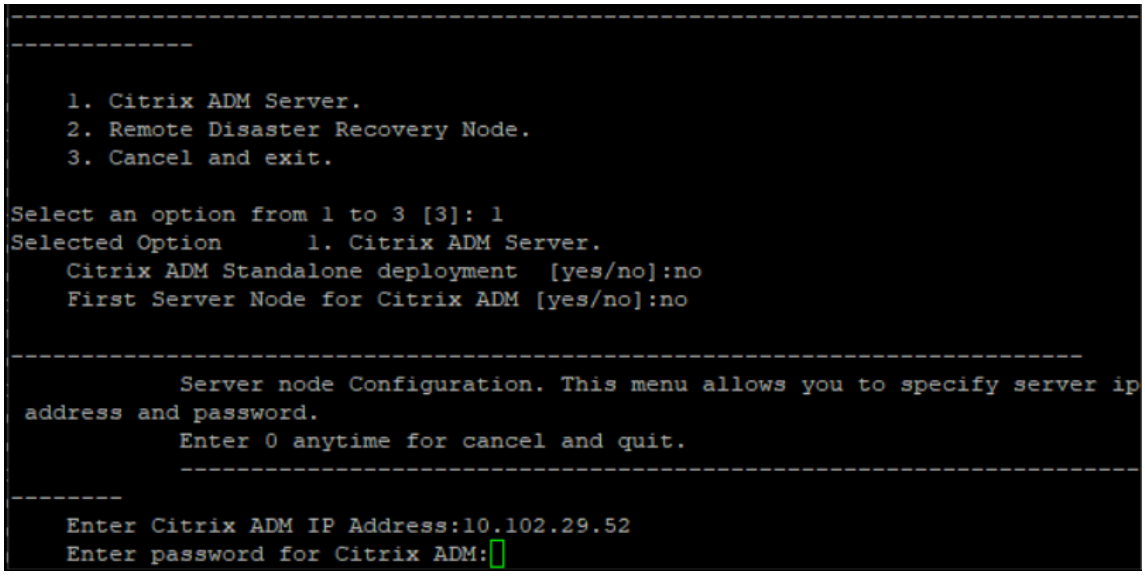
2. Tras especificar las direcciones IP necesarias, en la línea de comandos, escriba /mps/deployment_type.py y pulse enter.
3. Seleccione el tipo de implementación como **servidor Citrix ADM**.
4. La consola de implementación le pide que seleccione la implementación del servidor (como independiente). Escriba **No** para confirmar la implementación como par de alta disponibilidad.


```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

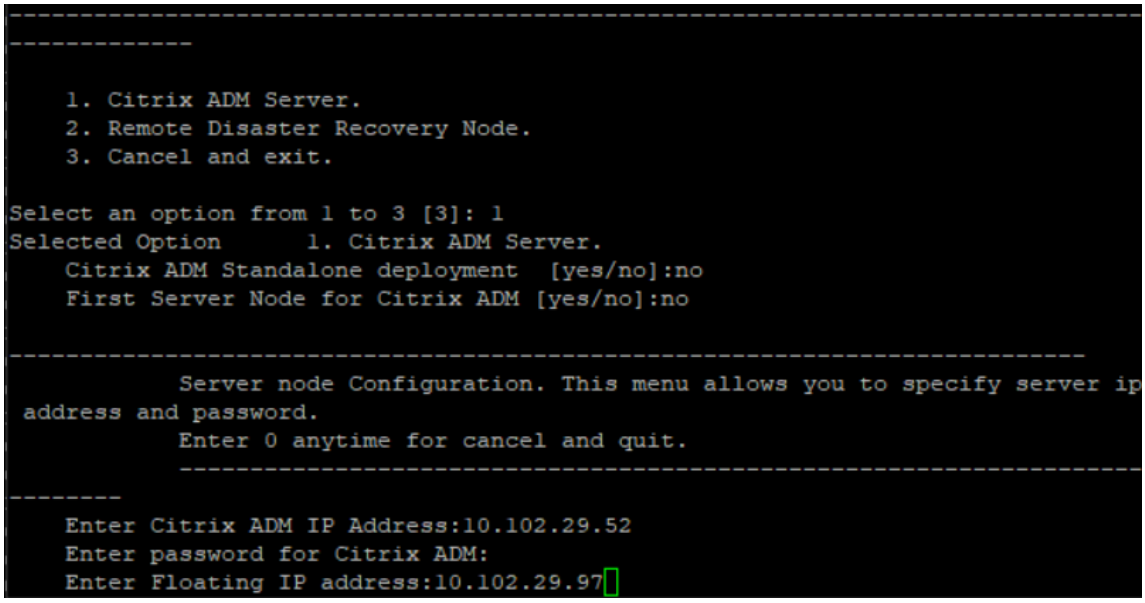
5. A continuación, la consola le pide que seleccione el (primer nodo del servidor). Escriba **No** para confirmar el nodo como el segundo nodo del servidor.

```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no
```

6. Introduzca la dirección IP y la contraseña del primer servidor.



7. Introduzca la dirección IP flotante del primer nodo.



8. La consola le pide que reinicie el sistema. Escriba**Sí** para reiniciar.

Implemente los dos servidores en un modo de alta disponibilidad

Para completar el proceso de instalación de los dos nodos de servidor como un par de alta disponibilidad, debe implementar estos nodos desde la GUI del nodo de servidor Citrix ADM existente anteriormente. La comunicación interna entre los dos servidores se inicia al implementar los dos nodos de servidor.

1. En un explorador web, escriba la dirección IP del nodo del servidor Citrix ADM existente anteriormente.

2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Sistema**, vaya a **Implementación** y haga clic en **Implementar**.
4. Aparece un mensaje de confirmación. Haga clic en **Sí**.

   > **Nota:**
   >
   > Después de implementar Citrix ADM en alta disponibilidad, puede acceder al nodo principal mediante la IP flotante. No se puede acceder al nodo secundario desde la versión 12.1 en adelante.

5. Si bien ha introducido la IP flotante al configurar el segundo nodo del servidor, tiene la opción de actualizar el FIP en la página **Sistemas**. Haga clic en **Configuración de HA** > **Configurar una dirección IP flotante para el modo de alta disponibilidad**. Puede ver la dirección IP flotante que configuró anteriormente. Puede introducir una nueva dirección IP y hacer clic en **Aceptar**.

Migrate from NetScaler Insight Center to NetScaler ADM

January 30, 2024

Ahora puede migrar la implementación de NetScaler Insight Center a NetScaler ADM sin perder la configuración, la configuración o los datos existentes. Con Citrix ADM, no solo puede ver los distintos análisis generados por las instancias de NetScaler asociadas a una aplicación, sino que también puede administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada.

> **Nota**
>
> Actualmente, la migración solo se admite en las instancias independientes de NetScaler Insight Center.

Requisitos previos

Antes de migrar el dispositivo virtual NetScaler Insight Center a Citrix ADM, compruebe que se cumplen los siguientes requisitos:

- Está instalado NetScaler Insight Center 11.1 Build 47.14 o posterior.
- Ha descargado el archivo de imagen de NetScaler ADM 12.0, compilación 57.24 .tgz.

> **Nota**
>
> Debe instalar Citrix ADM 12.0 build 57.24 y, a continuación, actualizar a la última versión de Citrix ADM 12.1. Para obtener más información, consulte Actualizar.

- Ha descargado el archivo de imagen.tgz de compilación más reciente de NetScaler ADM 12.1.

Requisito de hardware

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs
Espacio de almacenamiento	120 GB **Nota:** Citrix recomienda utilizar**500 GB**para obtener un mejor rendimiento. Además, Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps
Requisitos de hipervisor	
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu, Fedora

Procedimiento de instalación

Para migrar NetScaler Insight Center a NetScaler ADM:

1. Inicie sesión en el intérprete de comandos de NetScaler Insight Center.
2. Descargue NetScaler ADM 12.0 compilación 57.24 en la carpeta */var/mps/mps_images*.
3. Descomprima el archivo TGZ mediante el comando **tar -zxvf build-mas-12.0-57.24.tgz**.


```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. Instale NetScaler ADM mediante **./installmas**.

```
bash-3.2# ./installmas
```

5. Tras instalar Citrix ADM 12.0 build 57.24, debe actualizar a la última versión de Citrix ADM 12.1 realizando los pasos anteriores.

Tras la migración, todas las instancias de NetScaler que se descubrieron en el inventario de NetScaler Insight Center aparecen en la sección **Redes Instancias** de Citrix ADM. Sin embargo, por primera vez debe sondear manualmente los servidores virtuales alojados en los dispositivos detectados.

> **Nota**
>
> En Citrix ADM, de forma predeterminada, no hay ningún coste de licencia para administrar y supervisar 30 servidores virtuales creados en las instancias de NetScaler descubiertas. Para monitorear y administrar más de 30 servidores virtuales, instale las licencias MAS necesarias. Para obtener más información, consulteLicencias de NetScaler ADM.

Migrar configuraciones del Command Center a NetScaler ADM

January 30, 2024

Ahora puede migrar sus configuraciones de Command Center a NetScaler Application Delivery Management (ADM) sin perder la configuración, los ajustes ni los datos existentes de su implementación de Command Center y NetScaler ADM. Puede ver las configuraciones de Command Center migradas en NetScaler ADM una vez finalizado el proceso de migración.

Puntos que tener en cuenta

- La migración de configuraciones de Command Center a NetScaler ADM se admite en las siguientes implementaciones:
  - Desde Command Center de forma independiente hasta la implementación independiente de NetScaler ADM o la implementación de alta disponibilidad de NetScaler ADM.

  - Alta disponibilidad de Command Center para la implementación independiente de NetScaler ADM o la implementación de alta disponibilidad de NetScaler ADM.

> **Nota:**
>
> Debe utilizar únicamente la dirección IP del nodo principal de la implementación de alta disponibilidad de Command Center y NetScaler ADM al migrar la implementación independiente o de alta disponibilidad de Command Center a la implementación independiente o de alta disponibilidad de NetScaler ADM.

- Puede ejecutar la herramienta Command Center varias veces en las mismas implementaciones de NetScaler ADM o diferentes:
  - Siempre que ejecute la herramienta Command Center más allá de la primera vez para el mismo Citrix ADM, los registros se mostrarán como fallidos para las configuraciones que ya se han migrado y existen en Citrix ADM.
  - Si se ha agregado alguna nueva configuración en Command Center desde el momento en que se ejecutó la herramienta antes hasta ahora para el mismo NetScaler ADM, todas estas configuraciones, excepto las nuevas tareas personalizadas, se migrarán a NetScaler ADM.
- La migración de las configuraciones de Command Center a Citrix ADM es compatible con los dispositivos Citrix ADC, Citrix ADC SDX y Citrix SD-WAN WO.
- Toda la comunicación entre Command Center y NetScaler ADM se realiza mediante una conexión HTTPS.
- Se recomienda encarecidamente hacer copias de seguridad de los datos existentes de NetScaler ADM antes de migrar las configuraciones de Command Center.
- Una vez completada la migración de Command Center, las particiones de administración de NetScaler ADC se descubren automáticamente en NetScaler ADM.

Limitaciones

Las siguientes configuraciones de Command Center no se migran del dispositivo Command Center a NetScaler ADM:

- Archivos de configuración de copia de seguridad del dispositivo
- Detalles del tiempo de espera en los perfiles de dispositivos WO de SD-WAN
- Los siguientes detalles en desencadenadores de eventos y alarmas no se migran:
  - Detalles de cancelación para ejecutar la acción del comando
  - Detalles de la tarea de ejecución

  - Los desencadenadores con todos los parámetros vacíos (severidad/categoría/instancias/objetos de error) no se migran
  - Los desencadenadores que tienen instancias con el estado de clúster de alta disponibilidad, primario y secundario no se migran si se seleccionan los tres estados de las instancias

- Las tareas personalizadas sin descripción no se migran
- Configuración de severidad de eventos
- Detalles del cronograma de reglas de eventos
- Filtros de supresión de Syslog
- Detalles de la tarea de configuración
- Plantillas de auditoría
- Directivas de auditoría sin dispositivos
- Detalles del cronograma de directivas de auditoría
- Agrupa la configuración del alcance autorizado por RBAC
- Configuración de monitorización y administración de bases de datos
- Informes personalizados de rendimiento
- Umbrales de rendimiento
- Vistas personalizadas de Fault/Syslog/Reports/Entity Monitoring
- Informes de AppFirewall y NS Gateway y detalles de su programación
- Detalles de configuración automática de SD-WAN WO
- Ajustes de alta disponibilidad
- Configuración de copia de seguridad programada del sistema
- Configuración de reintentos de base de datos
- Hora programada de purga de Syslog
- Todos los datos estadísticos, como el registro del sistema, los eventos y los registros de auditoría de todos los módulos.

Requisitos previos

Antes de migrar las configuraciones de Command Center a NetScaler ADM, asegúrese de que se cumplan los siguientes requisitos previos:

- Está ejecutando la versión 5.2 de Command Center, compilación 48.2 o posterior.

- Ha instalado y configurado NetScaler ADM versión 12.0, compilación 51.24 o posterior.
- Solo el usuario administrador ejecutará la migración de la configuración de Command Center.
- Para migrar correctamente las tareas personalizadas, el campo de descripción es obligatorio en Command Center.
- La comunicación entre el Command Center y NetScaler ADM se basa en NITRO. Debe configurar y abrir los parámetros de protocolo SSL (Secure Socket Layer) y TLS (Transport Layer Security) necesarios en Command Center y NetScaler ADM para la comunicación con NITRO.

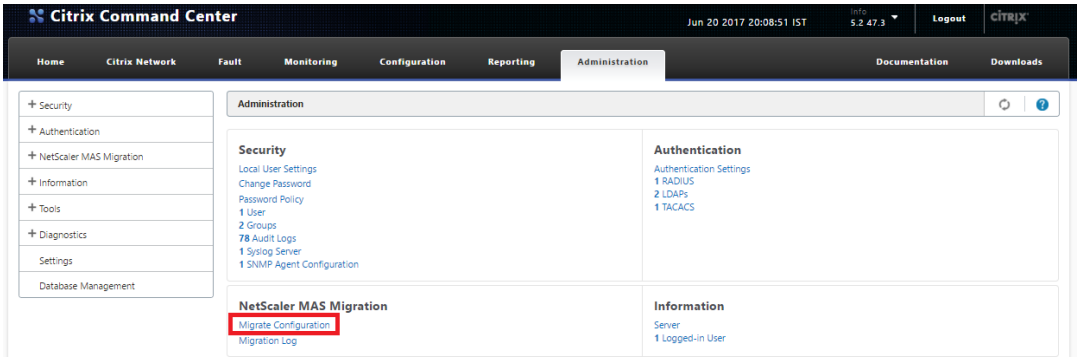
> **Nota**
>
> Si está utilizando una versión de Command Center anterior a 5.2 build 48.2, debe actualizar la versión de Command Center a 5.2 build 48.2 y, a continuación, migrar las configuraciones de Command Center a NetScaler ADM. Para obtener información detallada sobre la actualización del dispositivo Command Center, consulte Actualización de Command Center.

Migrar las configuraciones

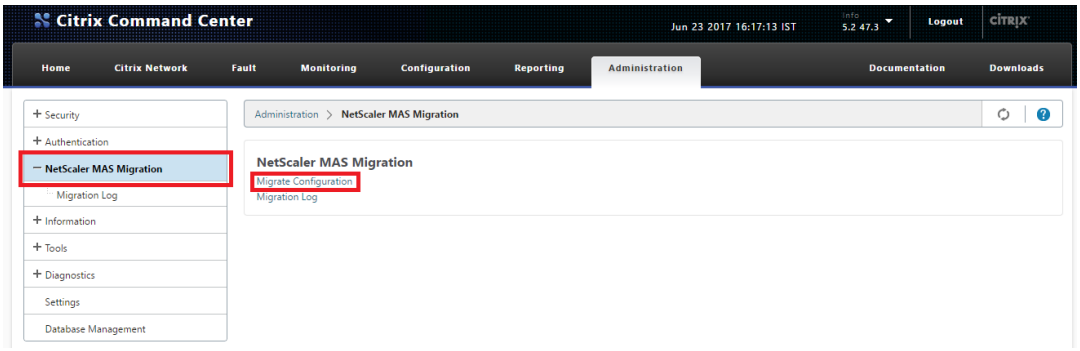
Para migrar una configuración de Command Center a NetScaler ADM, necesita la dirección IP del dispositivo Command Center y las credenciales de administrador.

Para migrar las configuraciones de Command Center a NetScaler ADM:

1. En un navegador web, escriba la dirección IP del dispositivo Command Center.
2. En los campos**Nombre de usuario**y**Contraseña**, escriba las credenciales de administrador e inicie sesión.
3. Después de iniciar sesión correctamente, en la pantalla que aparece, seleccione la ficha **Administración** y realice una de las acciones siguientes:
   - En el panel derecho, en **Citrix ADM Migration**, seleccione **Migrar configuración** , como se muestra en la siguiente figura.

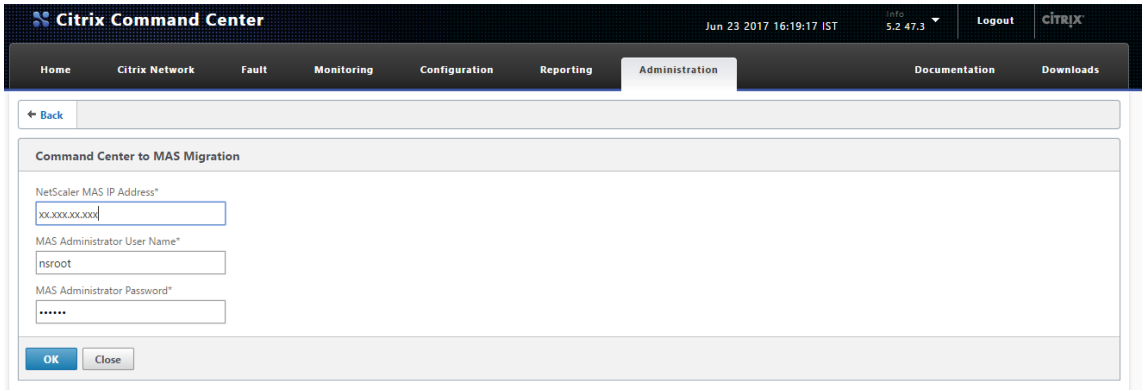


- En el panel izquierdo, seleccione **Citrix ADM Migration** y, a continuación, haga clic en **Migrar configuración** , como se muestra en la siguiente figura.

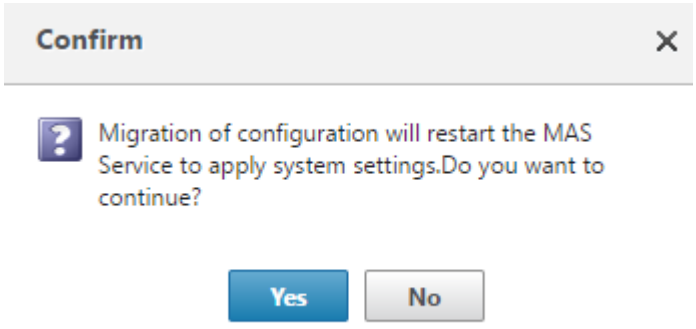


4. En el cuadro de diálogo **Migración de Command Center a MAS** , introduzca la dirección IP del servidor Citrix ADM y las credenciales de administrador y, a continuación, haga clic **en**Aceptar.

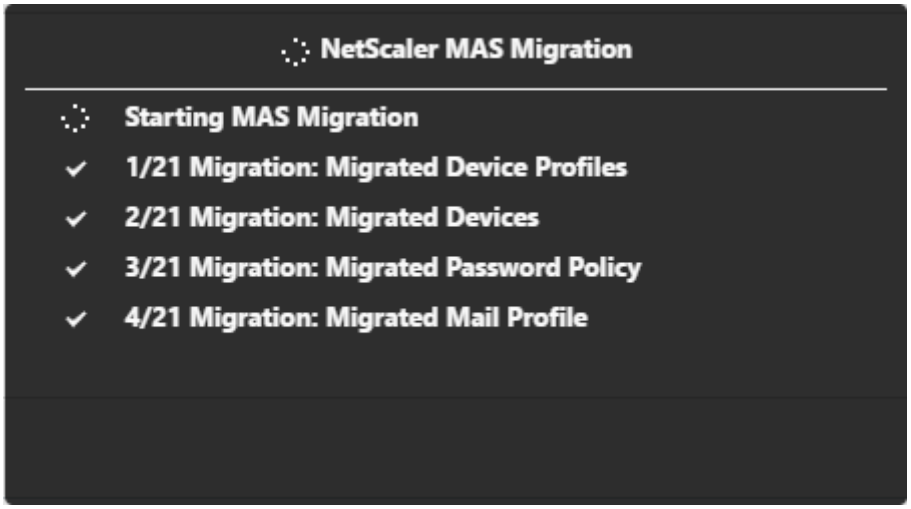
> **Nota**
>
> En caso de implementación de alta disponibilidad de NetScaler ADM, introduzca la dirección IP del nodo principal.



5. En el mensaje de confirmación, haga clic en **Sí**.



La pantalla informa del progreso de las tareas de migración.



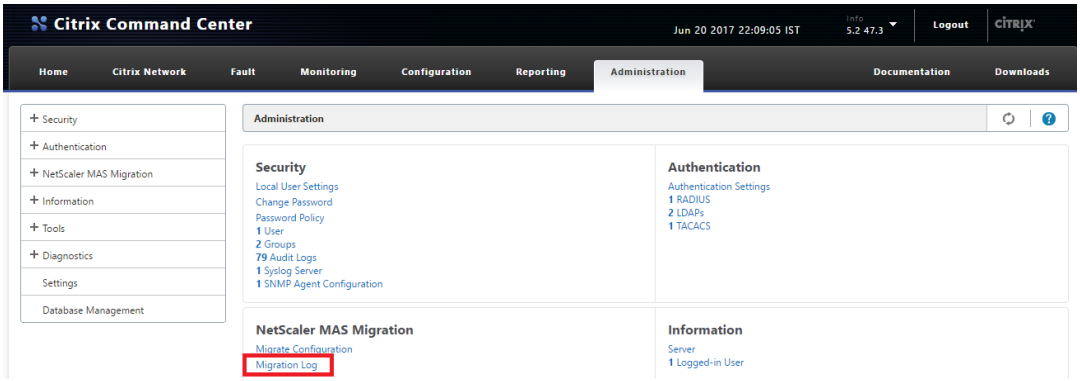
La operación **Migrar configuración** toma como entrada los detalles de la implementación de NetScaler ADM y sus credenciales de administrador. A continuación, la operación **Migrate Configuration** migra la configuración de la implementación de Command Center a la implementación de NetScaler ADM.

Cuando finalicen las tareas, puede comprobar la configuración de Command Center migrada a partir de los registros de migración de Command Center y los datos de NetScaler ADM.

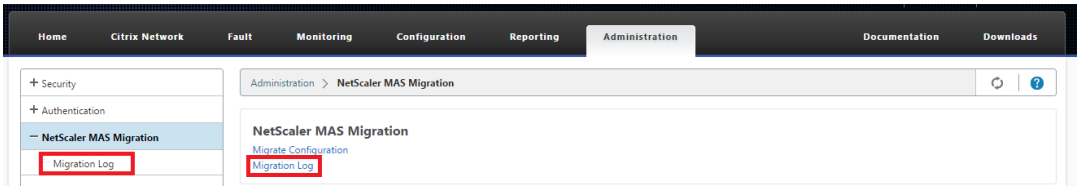
Para usar los registros de migración de Command Center para verificar la migración

1. En la GUI del Command Center, en la ficha **Administración**, realice una de las siguientes acciones:

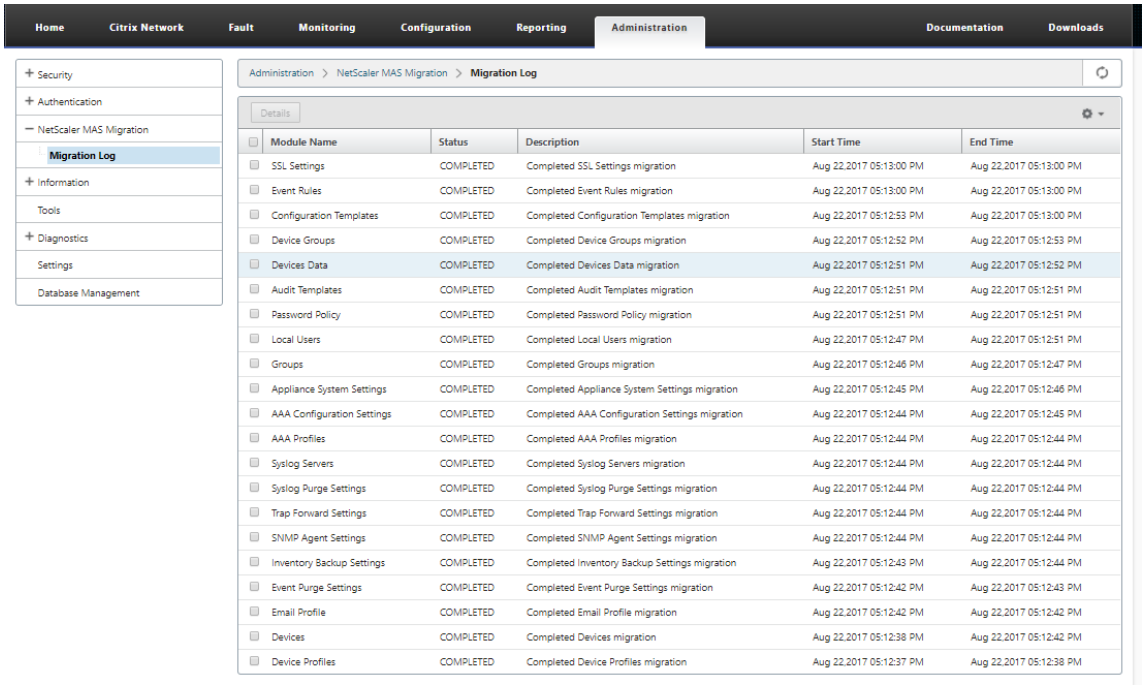
   - En el panel derecho, en **Citrix ADM Migration** , haga clic en **Registro** de migración .



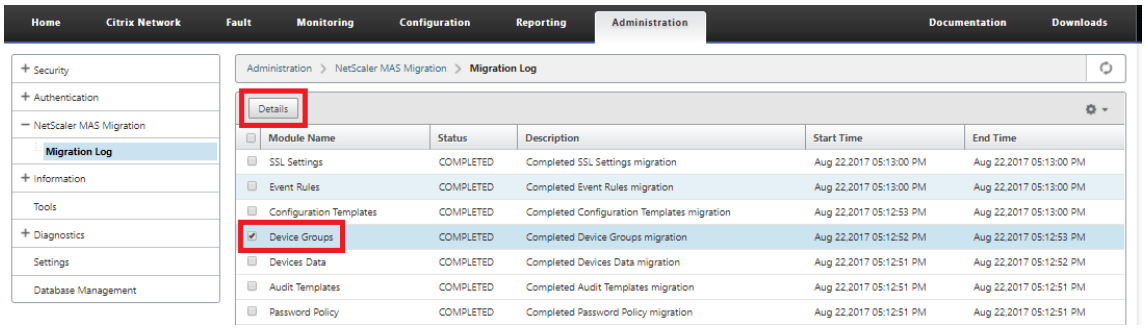
   - En el panel izquierdo, seleccione **Citrix ADM Migration** y, a continuación, haga clic en **Registro** de migración .



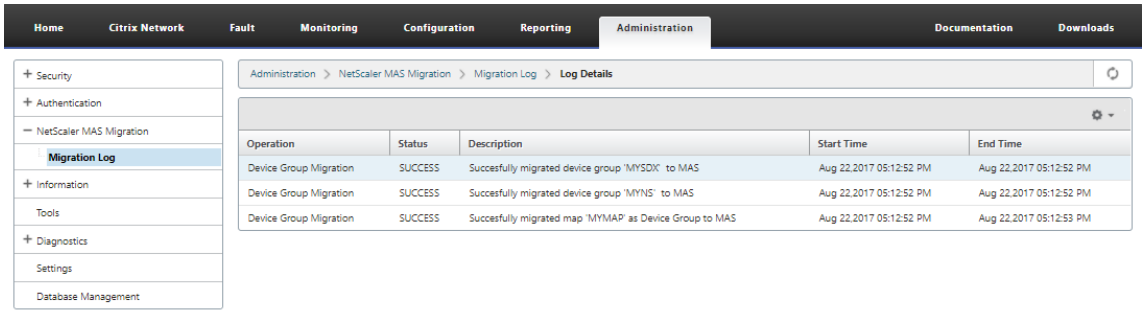
2. Revise la lista de registros de migración.



3. Para mostrar más detalles, seleccione **Nombre del módulo** para mostrar detalles de un módulo concreto, seleccione ese módulo y, a continuación, haga clic en **Detalles**.



4. En el ejemplo siguiente se muestran los detalles del registro de un módulo seleccionado.



Para usar NetScaler ADM para verificar la migración

Durante el proceso de migración, las configuraciones de Command Center se migran a NetScaler ADM y se muestran como configuraciones de NetScaler ADM en la GUI de NetScaler ADM.

Una vez finalizado el proceso de migración, el servidor NetScaler ADM se reinicia y es posible que se produzca un tiempo de inactividad momentáneo. Cuando el servidor Citrix ADM esté en funcionamiento, acceda a la GUI de Citrix ADM escribiendo la dirección IP del servidor Citrix ADM en la barra de direcciones del explorador.

La siguiente tabla muestra cómo la terminología de NetScaler ADM para las configuraciones migradas se corresponde con la terminología utilizada en Command Center.

Terminología del Command Center	Terminología de NetScaler ADM
Perfiles de dispositivos	Perfiles de instancia
Los dispositivos y su estado (como administrados o no administrados)	Instancias y su estado (como administradas o no administradas)
Anotaciones del dispositivo	Anotaciones de instancia
Grupos de dispositivos	Grupos de instancias
Mapas	Grupos de instancias
Activadores de eventos y alarmas	Reglas del evento
Comandos de tareas integrados y personalizados	Plantillas de configuración en el editor de tareas de creación
Directivas de auditoría programadas	Plantillas de auditoría
Directiva de contraseñas	Directiva de contraseñas
Usuarios (solo usuarios locales)	Usuarios del sistema
Grupos*	Grupos de sistemas
Perfiles de autenticación y ajustes de autenticación	Perfiles de autenticación y configuración de autenticación

Terminología del Command Center	Terminología de NetScaler ADM
Parámetros del correo electrónico	Servidor de correo electrónico/lista de distribución de correo
Servidor syslog	Servidor syslog
Configuración de SSL	Configuración de SSL
Configuración del agente SNMP	Gestor SNMP
Configuración de captura directa	Ajustes de trampa
Configuración de purga de eventos	Configuración de borrado de eventos
Configuración de inventario	Configuración de backup de instancias
Configuración de purga de Syslog	Configuración de Syslog Prune
Configuración de red del dispositivo, como DNS, NTP y zona horaria	Configuración de red NetScaler ADM, como DNS, NTP y zona horaria

*Los grupos con todos los permisos en Command Center se migran como grupos con una función de «administrador» en Citrix ADM. Todos los demás grupos de Command Center se migran como grupos con una función de «solo lectura» en Citrix ADM.

Integración de NetScaler ADM con Citrix Director

January 30, 2024

Director se integra con NetScaler ADM para el análisis de redes y la gestión del rendimiento.

- El análisis de red obtiene los informes de HDX Insight de NetScaler ADM y proporciona una vista de la red desde las aplicaciones y el escritorio. Con esta función, Director proporciona una vista analítica avanzada del tráfico ICA en su implementación.
- La función de administración del rendimiento (Performance Management) proporciona la retención del historial y los informes de tendencias. Con la retención del historial de datos frente a la evaluación en tiempo real, puede crear informes de tendencias que incluyen las tendencias de capacidad y estado.

Tras integrar NetScaler ADM con Director, los informes de HDX Insight le proporcionan la siguiente información en Director:

- La ficha Red de la página Tendencias muestra los efectos de latencia y ancho de banda para las aplicaciones, los escritorios y los usuarios de toda la implementación.

- La página Detalles del usuario muestra la información de latencia y ancho de banda específica de la sesión de un usuario en particular.

Requisitos previos

Requisitos de hardware para la migración de HDX Insight a Citrix ADM

Componente	Requisito
RAM	32 GB
CPU virtual	8
Espacio de almacenamiento	500 GB. Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps

Requerimientos de software

Antes de migrar al dispositivo virtual NetScaler ADM, compruebe que se cumplen los siguientes requisitos:

- Está instalada la versión 1811 de Director
- NetScaler HDX Insight versión 10.1 o posterior está instalado
- HDX Insight y Citrix ADM admiten Citrix VDA 7.0 y versiones posteriores
- Citrix Workspace es compatible con Citrix Virtual Apps and Desktops versión 7.0 y posterior
- Asegúrese de que MAC Citrix Receiver para Mac versión 11.8 y posteriores y Windows Citrix Receiver para Windows 14.0 y posteriores estén disponibles para mostrar métricas ICA RTT precisas
- NetScaler ADM versión 11.0 y posterior está instalado. Para obtener más información sobre cómo instalar NetScaler ADM, consulte Implementar NetScaler ADM.

Limitaciones

- La disponibilidad de esta función depende de la licencia de la organización y los permisos de administrador.

- El tiempo de ida y vuelta (RTT) de la sesión ICA muestra los datos correctamente para Citrix Receiver para Windows 3.4 o posterior y para Citrix Receiver para Mac 11.8 o posterior. Para las versiones anteriores de estos paquetes de Receiver, los datos no se muestran correctamente.
- En la vista Tendencias, los datos de inicio de sesión de la conexión HDX no se recopilan para los VDA anteriores a la versión 7. Para los VDA anteriores, los datos gráficos se muestran como 0.
- Para las implementaciones que ya tienen un disco duro externo con un espacio de almacenamiento inferior a 500 GB, no puede agregar otro disco duro.

> **Nota**
>
> - Para obtener más información sobre Director y los pasos para integrar NetScaler ADM con Director, consultehttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.html.
> - Para obtener más información sobre HDX Insight, consultehttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Adjuntar un disco adicional a NetScaler ADM

January 30, 2024

Los requisitos de almacenamiento de NetScaler Application Delivery Management (ADM) se determinan en función de la estimación del tamaño de NetScaler ADM. De forma predeterminada, NetScaler ADM proporciona una capacidad de almacenamiento de 120 GB. Si necesita más de 120 GB para almacenar los datos, puede adjuntar un disco adicional.

> **Nota**
>
> - Calcule los requisitos de almacenamiento y conecte un disco adicional al servidor en el momento de la implementación inicial de Citrix ADM.
> - Para una implementación de un solo servidor de NetScaler ADM, solo puede conectar un disco al servidor además del disco predeterminado.
> - Para una implementación de alta disponibilidad de Citrix ADM, debe conectar un disco adicional a cada nodo. El tamaño de ambos discos debe ser idéntico.
> - Si anteriormente había conectado un disco externo de menor capacidad, debe quitar el disco antes de conectar un disco nuevo.
> - Puede conectar un disco adicional con una capacidad superior a 2 terabytes. Si es necesario, el tamaño del disco también puede ser inferior a 2 terabytes.

> - Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM.

En este documento se explican los siguientes escenarios sobre la conexión de un nuevo disco adicional, la creación de particiones y el cambio de tamaño de los discos adicionales:

1. Adjuntar un disco adicional nuevo
2. Inicie la herramienta de partición de disco
3. Crear particiones en el nuevo disco adicional
4. Cambiar el tamaño del disco adicional existente
5. Eliminar particiones en el disco adicional

Adjunte un disco adicional en un Citrix ADM independiente

Realice los siguientes pasos para conectar un disco a la máquina virtual:

1. Apague la máquina virtual NetScaler ADM.
2. En el hipervisor, conecte un disco adicional del tamaño de disco requerido a la máquina virtual Citrix ADM.

   El disco más grande recién conectado almacena los datos de la base de datos y los archivos de registro NetScaler ADM. El disco predeterminado existente de 120 gigabytes ahora se usa para almacenar los archivos principales, los archivos de registro del sistema operativo, etc.
3. Inicie la máquina virtual NetScaler ADM.

Herramienta de partición de disco NetScaler ADM

NetScaler ADM ahora proporciona la **herramienta de partición de disco NetScaler ADM**, una nueva herramienta de línea de comandos. Las funcionalidades de esta herramienta se describen en detalle de la siguiente manera:

1. Con la herramienta, puede crear particiones en el disco adicional recién agregado.
2. También puede cambiar el tamaño del disco adicional existente con esta herramienta. Sin embargo, el disco externo existente no debe superar los 2 terabytes.

   > **Nota**
   >
   > - No es posible cambiar el tamaño de los discos existentes más allá de 2 terabytes sin perder datos. Esto se debe a una limitación conocida de la plataforma.
   > - Para crear una capacidad de almacenamiento superior a 2 terabytes, debe eliminar

> las particiones existentes y crear particiones con esta nueva herramienta.

3. Con esta nueva herramienta, puede realizar cualquier acción de partición en el disco de forma explícita. La herramienta le proporciona una visibilidad y un control claros sobre el disco y los datos asociados.

> **Nota:**
>
> Solo puede usar esta herramienta en el disco adicional que haya conectado al servidor NetScaler ADM. No puede crear particiones en el disco principal (predeterminado) de 120 gigabytes con esta herramienta.

Inicie la herramienta de partición de disco

1. Abra una conexión SSH a NetScaler ADM mediante un cliente SSH, como PuTTY.
2. Inicie sesión en Citrix ADM con las credenciales de administrador.
3. Cambie al símbolo del shell y escriba:

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

```
bash-3.2# /mps/DiskPartitionTool.py

-------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
-------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

> **Nota**
>
> Para NetScaler ADM en la implementación de alta disponibilidad, debe iniciar la herramienta en ambos nodos y crear o cambiar el tamaño de las particiones después de conectar los discos a las máquinas virtuales respectivas.

Crear particiones en el nuevo disco adicional

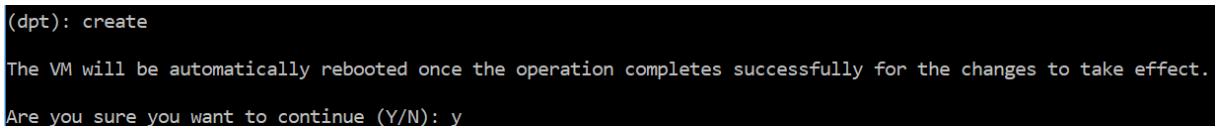
El comando **create** se usa para crear particiones siempre que se agrega un disco secundario nuevo. También puede usar este comando para crear particiones en un disco secundario existente después de eliminar las particiones existentes mediante el comando "remove".

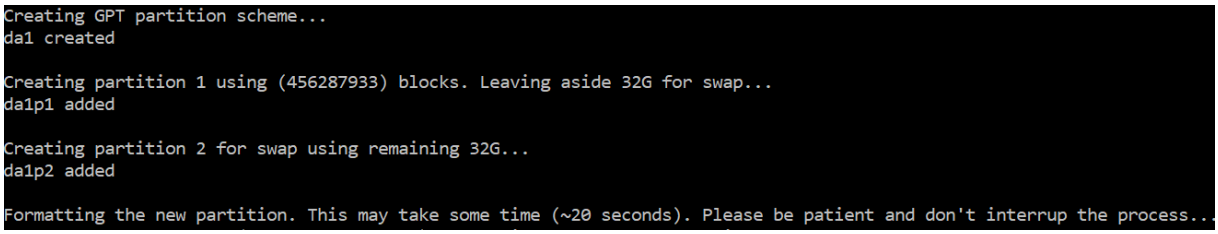
```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```


> **Nota**No
>
> hay limitación de tamaño de 2 terabytes al crear particiones con la herramienta de partición de disco. La herramienta puede crear particiones de más de 2 terabytes. Al particionar el disco, se agrega automáticamente una partición de intercambio de 32 GB de tamaño. A continuación, la partición principal utiliza todo el espacio restante en el disco.

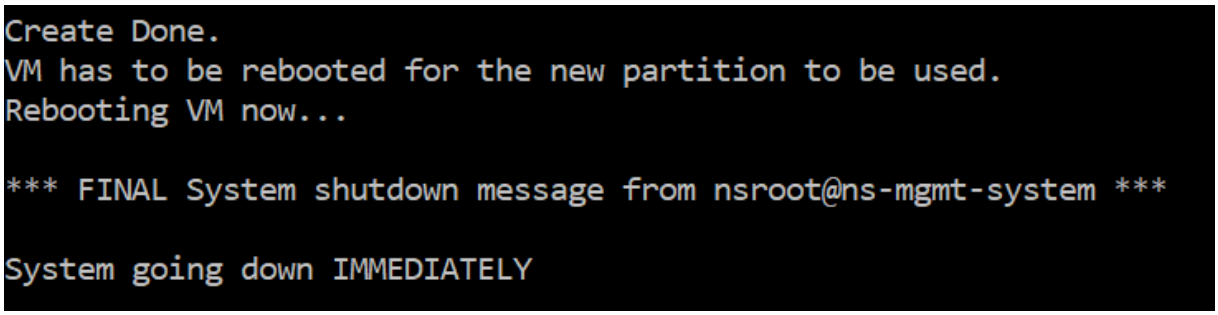
Una vez ejecutado el comando, se crea un esquema de particiones de tabla de particiones GUID (GPT). También se crean una partición de intercambio de 32 GB y una partición de datos para utilizar el resto del espacio. A continuación, se crea un nuevo sistema de archivos en la partición principal.

> **Nota**
>
> Este proceso puede tardar unos segundos y no debe interrumpir el proceso.





Una vez que se completa el comando create, la máquina virtual se reinicia automáticamente para que la nueva partición se monte.



Después del reinicio, la nueva partición se monta en /var/mps.


```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

La partición swap agregada se muestra como espacio swap en la salida del comando "create".

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Nota**
>
> La herramienta reinicia la máquina virtual después de crear la partición.

Cambiar el tamaño de las particiones en el disco adicional existente

Puede utilizar el comando **resize** para cambiar el tamaño del disco adjunto (secundario). Puede cambiar el tamaño de un disco que tenga un registro de arranque maestro (MBR) o un esquema GPT. El tamaño del disco debe ser inferior a 2 terabytes y un máximo de 2 terabytes.

> **Nota**
>
> - El comando "cambiar tamaño"está diseñado para funcionar sin perder ningún dato existente. Sin embargo, Citrix recomienda hacer una copia de seguridad de los datos críticos de este disco en un almacenamiento externo antes de intentar cambiar el tamaño. La copia de seguridad de datos es útil en los casos en que los datos del disco pueden dañarse durante la operación de cambio de tamaño.
> - Asegúrese de aumentar el espacio en disco en incrementos de 100 GB de espacio mientras cambia el tamaño de las particiones. Este incremento incremental garantiza que no tendrá que cambiar el tamaño con más frecuencia.


```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

El comando "cambiar tamaño"comprueba todas las condiciones previas y continúa si se cumplen todas las condiciones previas y después de que haya dado su consentimiento para cambiar el tamaño. Detiene los procesos que acceden al disco, lo que incluye los subsistemas NetScaler ADM, los procesos de base de datos de PostgreSQL y el proceso de supervisión de NetScaler ADM. Una vez que se detienen los procesos, se desmonta el disco para prepararlo para el cambio de tamaño. El cambio de tamaño se realiza extendiendo la partición para que ocupe todo el espacio disponible y luego aumentando el sistema de archivos. Si existe una partición de intercambio en el disco, se elimina y se vuelve a crear al final del disco después de cambiar el tamaño. La partición swap se describe en la sección **Crear** comando del documento.

> **Nota**
>
> El proceso de "sistema de archivos en crecimiento"puede tardar algunos en completarse y tener cuidado de no interrumpir el proceso mientras está en curso. La herramienta reinicia la máquina virtual después de cambiar el tamaño de la partición.

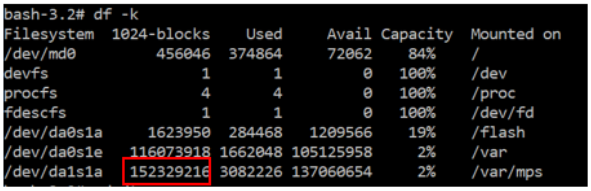
```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

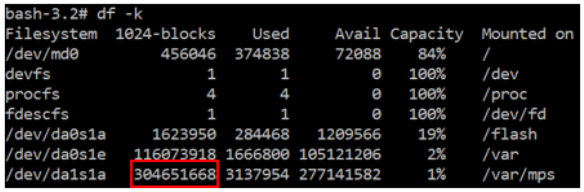
Todos los pasos intermedios en el proceso de cambio de tamaño (detener aplicaciones, cambiar el tamaño del disco, el crecimiento del sistema de archivos) se muestran en la consola. Una vez completado el proceso, se ve el siguiente mensaje.


```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Después de reiniciar, el aumento de tamaño se puede observar con el comando "df". Aquí está el antes y después de aumentar el tamaño:



```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```



```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

Elimine las particiones en el disco adicional

Se puede cambiar el tamaño de una partición existente en el disco secundario hasta 2 terabytes. Esto se debe a una limitación conocida de la partición. Si quiere un disco de más de 2 terabytes, conecte un disco nuevo y particione con la herramienta de partición de disco. También puede eliminar la partición existente mediante el comando **remove** y, a continuación, crear una partición.

> **Nota**
>
> Al eliminar la partición existente, se eliminan todos los datos existentes. Por lo tanto, se debe realizar una copia de seguridad de los datos críticos en almacenamiento externo antes de utilizar este comando.

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

La ejecución del comando "remove"le pide confirmación y, una vez confirmado, detiene todos los procesos (como los subsistemas ADM, los procesos PostgreSQL y el monitor ADM) que utilizan el disco secundario. Si existe una partición de intercambio y el intercambio está habilitado en la partición, el intercambio está inhabilitado.


```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

Cuando escribe "y", el comando desmonta el disco y elimina todas las particiones del disco.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

> **Nota**
>
> La herramienta reinicia la máquina virtual después de eliminar la partición.

Reinicie la máquina virtual

Cuando se crea o cambia el tamaño de una partición, o cuando se crea un archivo de intercambio, reinicie la máquina virtual. Los cambios solo surtirán efecto después de reiniciarse. Para este propósito, se proporciona un comando de **reinicio** en la herramienta.

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

Se le pide confirmación y, una vez confirmado, detiene todos los procesos (como subsistemas ADM, procesos PostgreSQL y monitor ADM). A continuación, se reinicia la máquina virtual.

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

```
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```


Crear un archivo de copia de seguridad de los datos del disco

Estos son los pasos a seguir para hacer una copia de seguridad de los datos de NetScaler ADM antes de cambiar el tamaño de las particiones

> **Nota La**
>
> creación de un archivo de copia de seguridad requiere espacio en disco. Citrix recomienda asegurarse de que hay suficiente espacio libre en disco disponible (50% o más) antes de ejecutar los comandos de copia de seguridad.

1. Detenga ADM.

```
/mps/masd stop
<!--NeedCopy-->
```

2. Detenga PostgreSQL.

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. Detenga ADM Monitor.

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. Crea un tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> **Nota**
>
> La operación lleva tiempo dependiendo del tamaño de los datos a los que se debe realizar una copia de seguridad.

5. Generar suma de comprobación.

```
md5 mps_backup.tgz > mps_backup_checksum
<!--NeedCopy-->
```

6. Copia remotamente el archivo tar y la suma de verificación.

```
scp
<!--NeedCopy-->
```

7. Validar la exactitud del tarball copiado. Genere una suma de comprobación del archivo transferido y compárela con la suma de comprobación de origen.
8. Elimine el tarball de la máquina virtual ADM.


```
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

Comandos adicionales

Además de los comandos enumerados anteriormente, también puede usar los siguientes comandos en la herramienta:

Comando de ayuda:

Para enumerar los comandos admitidos, escriba **help** o **?** y presione Entrar. Para obtener más ayuda en cada uno de los comandos, presione **ayuda** o **?** seguido del nombre del comando y pulse la tecla **Intro**.

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

Comando Info:

El comando **info** proporciona información sobre el disco secundario conectado, si el disco existe. El comando proporciona el nombre del dispositivo, el esquema de particiones, el tamaño en formato legible por humanos y la cantidad de bloques de disco. El esquema puede ser MBR o GPT. Un esquema MBR significa que el disco se particionó con una versión anterior de la versión de NetScaler ADM. La partición basada en MBR/GPT se puede cambiar de tamaño, pero no más de 2 terabytes. El esquema de partición GPT significa que el disco se particionó con NetScaler ADM 12.1 o posterior.

> **Nota**
>
> Una partición GPT puede tener más de 2 terabytes pero cuando se crea. Sin embargo, no puede cambiar el tamaño del disco a un tamaño superior a 2 terabytes después de crear un disco con un tamaño más pequeño. Esta es una limitación conocida de la plataforma.


```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
-------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
-------------
(dpt):
```

Create_swapfile (comando):

La partición de intercambio predeterminada en el disco principal de NetScaler ADM es de 4 GB y, por lo tanto, el espacio de intercambio predeterminado es de 4 GB. Para la configuración de memoria predeterminada de NetScaler ADM, que es de 2 GB, este espacio de intercambio es suficiente. Sin embargo, cuando ejecuta NetScaler ADM con una configuración de memoria más alta, debe tener más espacio de intercambio asignado en el disco.

> **Nota**
>
> La partición de intercambio suele ser una partición dedicada que se crea en una unidad de disco duro (HDD) durante la instalación del sistema operativo. Dicha partición también se denomina espacio de intercambio. La partición swap se usa para la memoria virtual que simula la memoria principal adicional.

Los discos secundarios que se agregaron en las versiones anteriores de NetScaler ADM no tienen una partición de intercambio creada de forma predeterminada. El comando «create_swapfile» está destinado a discos secundarios creados con versiones anteriores de Citrix ADM que no tienen una partición de intercambio. El comando comprueba lo siguiente:

- Presencia de un disco secundario
- Disco que se monta
- Tamaño del disco (al menos 500 GB)
- La existencia del archivo swap

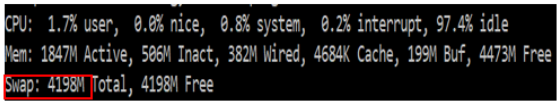
El comando "create_swapfile"solo es útil cuando la memoria es mayor o igual a 16 GB y no cuando la memoria es baja. Por lo tanto, este comando también comprueba si hay memoria antes de continuar con la creación de archivos de intercambio.

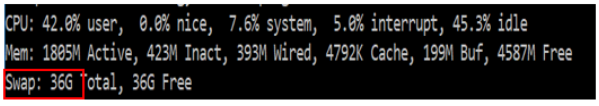

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Si se cumplen todas las condiciones y el usuario consiente en continuar, se crea un archivo de intercambio de 32 GB en el disco secundario. El proceso de creación del archivo de intercambio tarda unos minutos en completarse y tiene cuidado de no interrumpir el proceso mientras está en curso. Después de completarse correctamente, se realiza un reinicio para que el archivo de intercambio surta efecto.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

Después del reinicio, el aumento en el intercambio se puede observar con el comando top.





Comando Salir:

Para salir de la herramienta, escriba exit y presione la tecla **Intro**.

```
(dpt): exit
bash-3.2#
```

Adjuntar discos adicionales a NetScaler ADM implementados en alta disponibilidad

Consideremos un caso en el que haya configurado un par de servidores NetScaler ADM en una configuración de alta disponibilidad sin discos secundarios. Además, consideremos que ha agregado dos o más instancias de Citrix ADC y que ha comprobado y se ha asegurado de que todos los procesos se están ejecutando. Es posible que quiera agregar discos secundarios a las máquinas virtuales en esta instalación. En una configuración de alta disponibilidad, debe agregar discos adicionales a ambos nodos como se detalla en esta tarea:

1. Supongamos que los nombres de los nodos de NetScaler ADM son ‘‘ADM_primary’’y ‘‘ADM_secondary. ‘‘
2. Primero, ejecute la herramienta de partición en ADM_secondary y, a continuación, agregue un disco secundario. La máquina virtual se reinicia después de agregar el disco.
3. Apague el ADM_secondary después de que se reinicie.
4. Ahora ejecute la herramienta de partición en ADM_primary y agregue un disco secundario. La máquina virtual se reinicia después de agregar el disco.

   Asegúrese de agregar discos de capacidad similar a ambos nodos. Por ejemplo, si agrega un disco con una capacidad de 500 GB al nodo principal, agregue también un disco de 500 GB de capacidad al nodo secundario.
5. Después de que se reinicie ADM_primary, compruebe que es el nodo principal.
6. Ahora inicie el nodo ADM_secondary. Asegúrese de que aparezca como nodo secundario y de que las bases de datos se hayan sincronizado.
7. Confirme que todos los datos aún existen.

Realice los siguientes pasos para aumentar la capacidad de la RAM en ambos nodos:

1. Cierre ADM_Secondary y aumente el tamaño de RAM según sea necesario. No reinicie el nodo.
2. Cierre ADM_Primary y aumente el tamaño de RAM según sea necesario.

   Asegúrese de aumentar el tamaño de la RAM por igual en ambos nodos. Por ejemplo, si aumenta el tamaño de la RAM en el nodo principal a 16 GB, haga lo mismo en el nodo secundario también.
3. Reinicie ADM_primary.
4. Después de que se reinicie ADM_primary, compruebe que es el nodo principal.
5. Ahora inicie el nodo ADM_secondary. Después de que se reinicie, asegúrese de que aparezca como secundario y que la sincronización de la base de datos esté funcionando.
6. Ahora confirma que todos los datos siguen existiendo.

> **Nota:**
>
> Después de agregar el disco secundario, el nodo principal tarda un tiempo en aparecer. Además, todo el proceso de agregar discos secundarios a ambos nodos y aumentar la capacidad de RAM requiere que ambos nodos estén inactivos durante algún tiempo. Tenga en cuenta este tiempo de inactividad al planificar esta actividad de mantenimiento.

Configuración

January 30, 2024

Solo puede acceder a un servidor NetScaler ADM mediante la interfaz gráfica de usuario (GUI). Debe acceder a la GUI para agregar instancias, administrar y supervisar las instancias y aplicaciones, ver los análisis y configurar el servidor Citrix ADM.

Su estación de trabajo debe tener un explorador web compatible para acceder a la utilidad de configuración y al Panel de control.

Se admiten los siguientes exploradores.

Navegador web	Versión
Internet Explorer	11.0 y versiones posteriores
Google Chrome	Chrome 19 y versiones posteriores
Safari	Safari 5.1.1 y versiones posteriores
Mozilla Firefox	Firefox 3.6.25 y posterior

Para acceder a la GUI de NetScaler ADM:

1. En un explorador web, escriba la dirección IP de NetScaler ADM (por ejemplo,http://192.168.100.1). Es la misma dirección IP que especificó al instalar el servidor.
2. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de administrador. Las credenciales de administrador predeterminadas son nsroot/nsroot.

   Después de iniciar sesión en NetScaler ADM, debe hacer lo siguiente para comenzar:

   - Agregue instancias a NetScaler ADM. Debe agregar instancias al servidor Citrix ADM si quiere administrar y supervisar estas instancias.
   - Habilite el análisis en servidores virtuales. Para ver los datos de análisis del flujo de tráfico de su aplicación, debe habilitar la función de análisis en los servidores virtuales que reciben el tráfico de las aplicaciones específicas.
   - Configure el servidor NTP en NetScaler ADM. Debe configurar un servidor de protocolo de hora de red (NTP) en Citrix ADM para sincronizar su reloj con el servidor NTP.
   - Configure los parámetros del sistema para un rendimiento óptimo de NetScaler ADM. Antes de empezar a utilizar Citrix ADM para administrar y supervisar las instancias y aplicaciones, se recomienda configurar algunos ajustes del sistema que garantizarán un rendimiento óptimo del servidor Citrix ADM.

Agregar instancias a Citrix ADM

January 30, 2024

Las instancias son dispositivos Citrix o dispositivos virtuales que quiere descubrir, administrar y supervisar desde Citrix ADM. Debe agregar instancias al servidor Citrix ADM si quiere administrar y supervisar estas instancias. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a Citrix ADM:

- Citrix ADC
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX
- Citrix Gateway
- Citrix SD-WAN

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde. A continuación, debe especificar un perfil de instancia que Citrix ADM pueda usar para acceder a la instancia.

> **Nota**
>
> - Citrix ADM utiliza la dirección IP de NetScaler (NSIP) de las instancias Citrix ADC para la comunicación. Para obtener información sobre los puertos que deben estar abiertos entre las instancias de Citrix ADC y Citrix ADM, consulte Puertos.
> - Para las instancias de Citrix SD-WAN WO y Citrix SD-WAN EE, Citrix ADM utiliza la dirección IP de administración de las instancias para la comunicación.
> - Para obtener información sobre cómo Citrix ADM descubre instancias, consulte Descubrir instancias.

Cómo crear un perfil de Citrix ADC

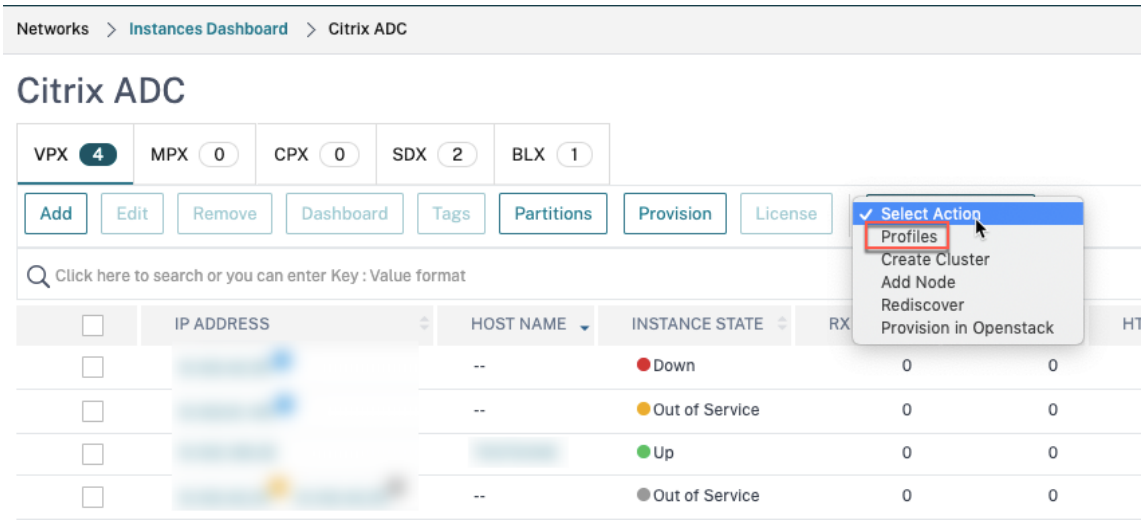
El perfil Citrix ADC contiene el nombre de usuario, la contraseña, los puertos de comunicación y los tipos de autenticación de las instancias que quiere agregar a Citrix ADM. Para cada tipo de instancia, está disponible un perfil predeterminado. Por ejemplo, nsroot es el perfil predeterminado para las instancias de Citrix ADC. El perfil predeterminado se define mediante las credenciales de administrador predeterminadas de Citrix ADC. Si ha cambiado las credenciales de administrador predeterminadas

de las instancias, puede definir perfiles de instancia personalizados para esas instancias. Si cambia las credenciales de una instancia después de detectarse la instancia, debe modificar el perfil de instancia o crear un perfil y, a continuación, volver a descubrir la instancia.

Puede crear un perfil de Citrix ADC desde la página **Instancia** o al agregar o cambiar una instancia.

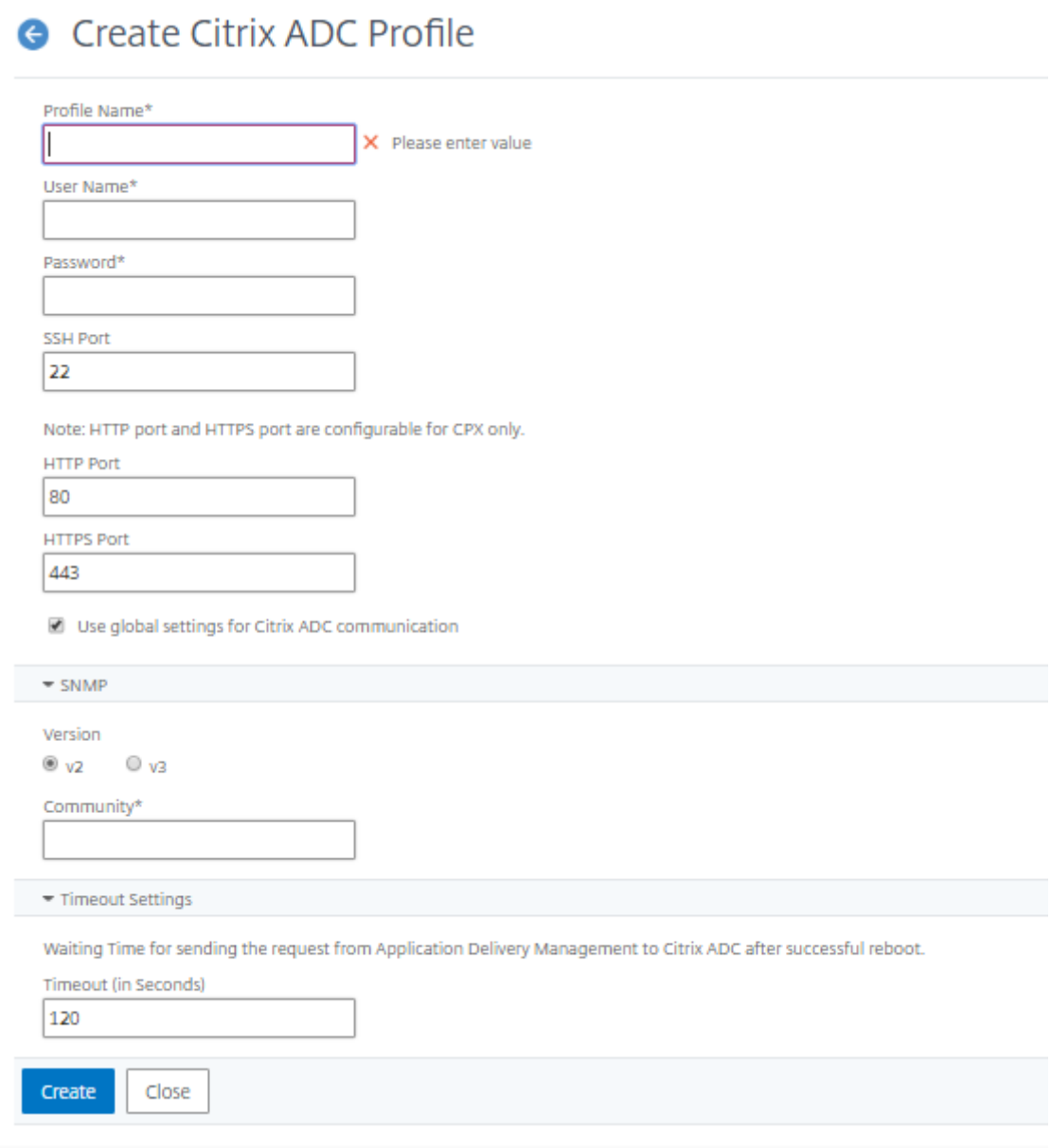
Para crear un perfil de Citrix ADC desde la página Instancia:

1. Vaya a **Redes > Instancias**.
2. Seleccione una instancia. Por ejemplo, Citrix ADC.
3. En la página Citrix ADC, seleccione **Perfiles**.



4. En la página **Perfiles de administrador**, seleccione **Agregar**.

5. En la página **Crear perfil de Citrix ADC**, haga lo siguiente:



a) **Nombre de perfil**: especifique un nombre de perfil para la instancia de Citrix ADC.

b) **Nombre de usuario**: especifique un nombre de usuario para iniciar sesión en la instancia de Citrix ADC.

c) **Contraseña**: especifique una contraseña para iniciar sesión en la instancia de Citrix ADC.

d) **Puerto SSH**: especifique el puerto para la comunicación SSH entre Citrix ADM y la instancia de Citrix ADC.

e) **Puerto HTTP**: especifique el puerto para la comunicación HTTP entre Citrix ADM y la instancia de Citrix ADC.

> **Nota**
>
> El puerto HTTP predeterminado es 80. También puede especificar el puerto HTTP personalizado o no predeterminado que podría haber configurado en su instancia de Citrix ADC CPX. El puerto HTTP personalizado solo se puede utilizar para la comunicación entre Citrix ADM y Citrix ADC CPX.

f) **Puerto HTTPS**: especifique el puerto para la comunicación HTTPS entre Citrix ADM y la instancia de Citrix ADC.

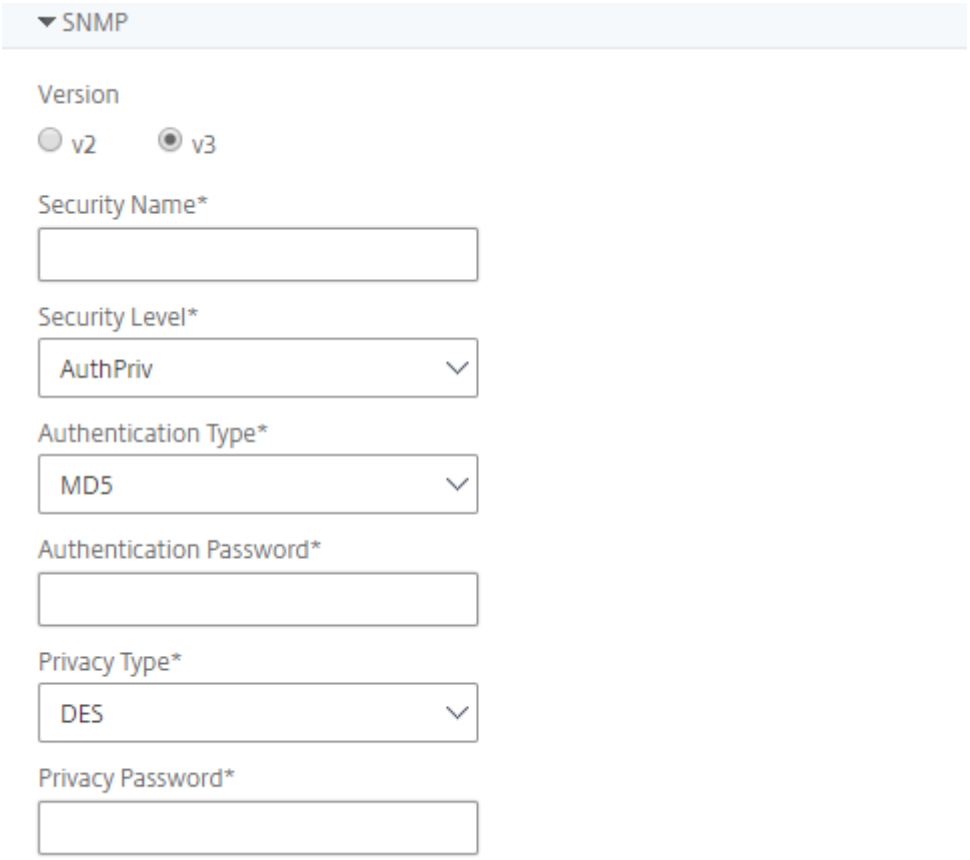
> **Nota**
>
> El puerto HTTPS predeterminado es 443. También puede especificar el puerto HTTPS personalizado o no predeterminado que podría haber configurado en su instancia de Citrix ADC CPX. El puerto HTTPS personalizado solo se puede utilizar para la comunicación entre Citrix ADM y Citrix ADC CPX.

g) **Utilizar la configuración global para la comunicación de Citrix ADC**: seleccione esta opción si quiere utilizar la configuración del sistema para la comunicación entre Citrix ADM y la instancia de Citrix ADC; de lo contrario, seleccione http o https.

h) **Versión SNMP**: seleccione **SNMPv2 o**SNMPv3** y haga lo siguiente:

   i. Si selecciona SNMPv2, especifique el nombre de la **comunidad** para la autenticación.

   ii. Si selecciona SNMPv3, especifique el **nombre de seguridad** y el **nivel de seguridad**. Según el nivel de seguridad, seleccione **Tipo de autenticación** y **Tipo de privacidad**.



> **Nota**
>
> Para Citrix ADC SDX, solo se admite **SNMPv2**.

i) **Configuración de tiempo de espera**: especifique el tiempo que debe esperar Citrix ADM antes de enviar una solicitud de conexión a la instancia de Citrix ADC tras un reinicio.

j) Seleccione **Create**.

Agregar instancias de ADC a Citrix ADM

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde.

Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de Citrix ADC, o un intervalo de direcciones IP.

Para las instancias SD-WAN, especifique la dirección IP de cada instancia o un intervalo de direcciones IP. Tenga en cuenta que Citrix ADM solo admite las ediciones Citrix SD-WAN WO y Citrix SD-WAN PE.

> **Nota**
>
> - Para agregar instancias de Citrix ADC configuradas en un clúster, debe especificar la direc-

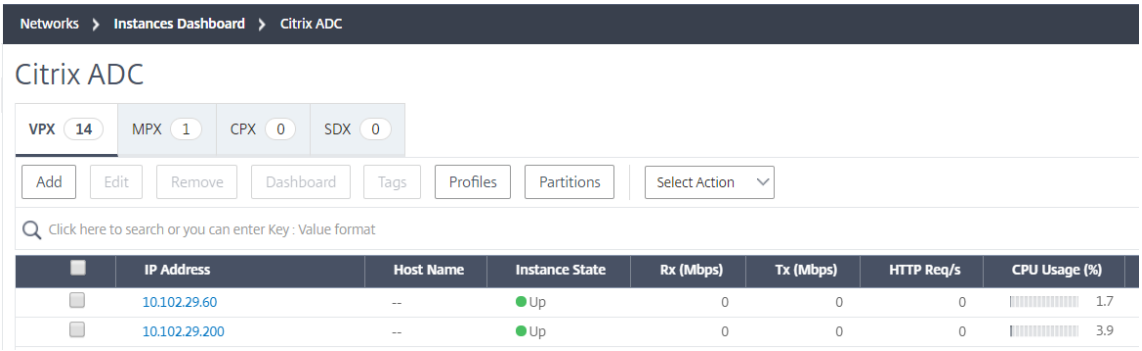
> ción IP del clúster o cualquiera de los nodos individuales de la configuración del clúster. Sin embargo, en Citrix ADM, el clúster se representa únicamente mediante la dirección IP del clúster.
>
> - Para las instancias de Citrix ADC configuradas como un par de HA, cuando agrega una instancia, la otra instancia del par se agrega automáticamente.

Si dos servidores Citrix ADM están configurados en modo de alta disponibilidad, cuando se agrega una instancia, la fuente de tráfico es a través de la dirección IP flotante de ADM.

Cuando se agrega una instancia de datos remotos configurados con un agente local, el origen de tráfico se realiza a través del agente ADM.

Para agregar una instancia a Citrix ADM:

1. Inicie sesión en Citrix ADM con las credenciales de administrador.
2. Vaya a**Redes**>**Instancias** > **Citrix ADC**. Seleccione el tipo de instancia que quiere agregar (por ejemplo, Citrix ADC VPX) y haga clic en**Agregar**.



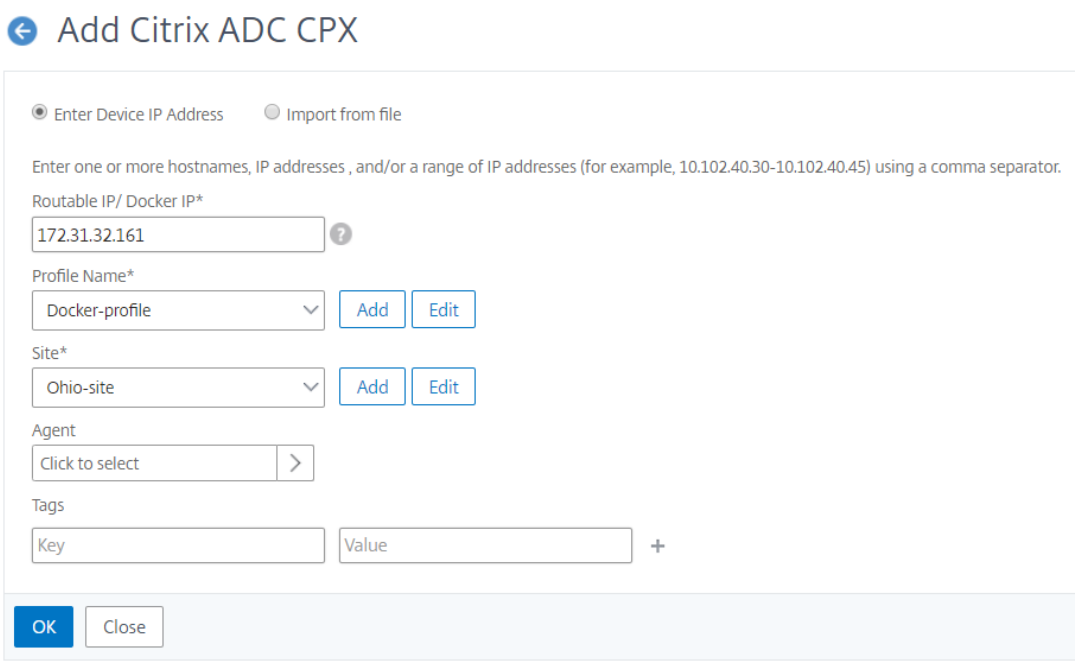
3. Seleccione una de estas opciones:
   - **Escriba la dirección IP del dispositivo**: Para las instancias Citrix ADC, especifique el nombre de host o la dirección IP de cada instancia, o un rango de direcciones IP. Para las instancias SD-WAN, especifique la dirección IP de cada instancia o un intervalo de direcciones IP.
   - **Importar desde un archivo**: desde tu sistema local, sube un archivo de texto que contenga las direcciones IP de todas las instancias que quieras agregar.
4. En **Nombre de perfil**, selecciona el perfil de instancia correspondiente o crea un perfil nuevo haciendo clic en el icono +.
5. En **Sitio**, selecciona la ubicación en la que quieres agregar la instancia o crea una nueva ubicación haciendo clic en el icono **+**.
6. Haga clic en**Aceptar**para iniciar el proceso de agregar instancias a Citrix ADM.

> **Nota**
>
> Si quiere volver a descubrir una instancia, vaya a **Redes** > **Instancias** > **Citrix ADC**. Seleccione la instancia que desee volver a descubrir y, a continuación, en la lista **Seleccionar acción**, haga clic en **Redescubrir**.

Agregar instancias CPX de ADC a Citrix ADM

Se ha mejorado Citrix ADM para brindar soporte a las mejoras que se han realizado en las funcionalidades de CPX. La instancia CPX de Citrix ADC ahora se agrega a Citrix ADM al proporcionar una dirección IP para el CPX junto con un perfil de dispositivo. El proceso de adición de una instancia CPX ahora es similar a cómo se agregan otros tipos de ADC como VPX o MPX en ADM. Además, se ha mejorado el registro de CPX en ADM. Cuando se inicia un CPX, Citrix ADM descubre y registra automáticamente la instancia CPX. Una instancia CPX ya no se descubre a través del host Docker.

1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y haga clic en la ficha **CPX**.
2. Haga clic en **Agregar**.
3. Se abrirá la página **Add Citrix ADC CPX**. Introduzca los valores de los siguientes parámetros:
    a) Puede agregar instancias de CPX proporcionando la dirección IP accesible de la instancia CPX o la dirección IP del contenedor Docker donde está alojada la instancia de CPX.
    b) Seleccione el perfil de la instancia CPX.
    c) Seleccione el sitio en el que se van a implementar las instancias.
    d) Seleccione el agente.
    e) Como opción, puede introducir el par clave-valor en la instancia. Agregar par clave-valor hace que sea fácil para usted buscar la instancia más adelante.



> **Nota**
>
> Para las instancias CPX de Citrix ADC, debe especificar los detalles de los puertos **HTTP, HTTPS, SSH**y **SNMP** del host al crear el perfil de instancia CPX. También puede especificar el rango de puertos que publicó el host en el campo **Puerto de inicio** y **número de puertos**.

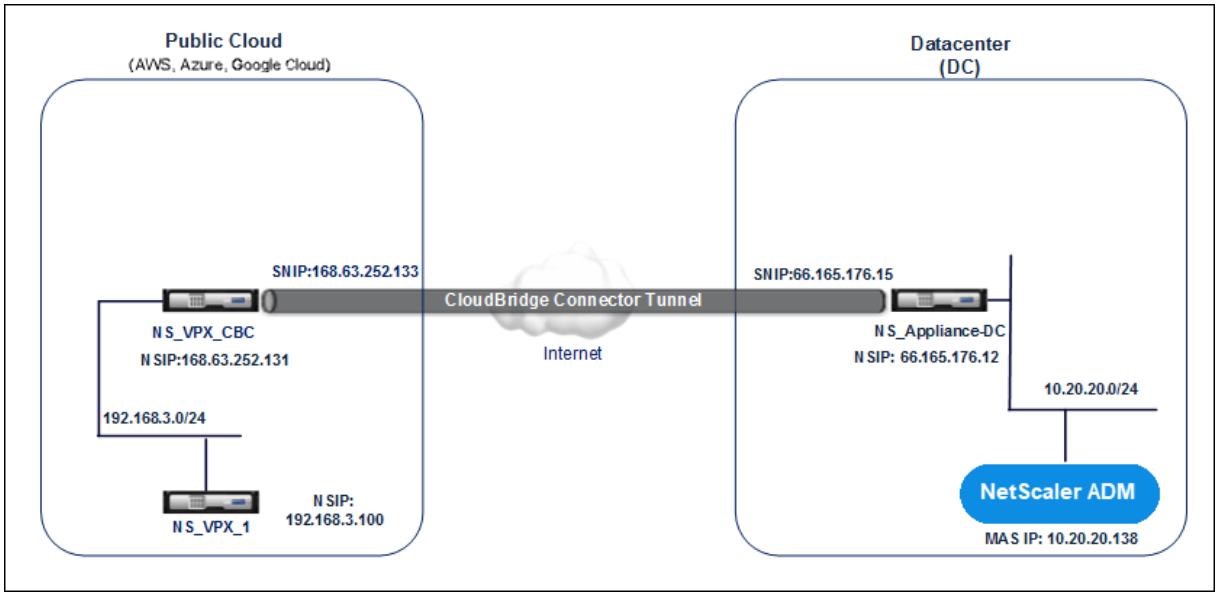
4. Haga clic en **Aceptar**.

Agregar instancias de NetScaler ADC VPX implementadas en la nube a NetScaler ADM

January 30, 2024

Puede usar Citrix ADM para administrar y supervisar las instancias de Citrix ADC VPX implementadas en una nube pública, como Amazon Web Services (AWS) o Microsoft Azure. Debe establecer conectividad de Capa 3 entre NetScaler ADM y las instancias de NetScaler ADC VPX implementadas en la nube pública. Para establecer la conectividad de capa 3, puede usar soluciones como NetScaler CloudBridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN en Azure o conectores de terceros como Equinix, etc.

La siguiente topología de ejemplo utiliza NetScaler CloudBridge Connector para la conectividad de capa 3 entre Citrix ADM y las instancias de Citrix ADC VPX implementadas en la nube.



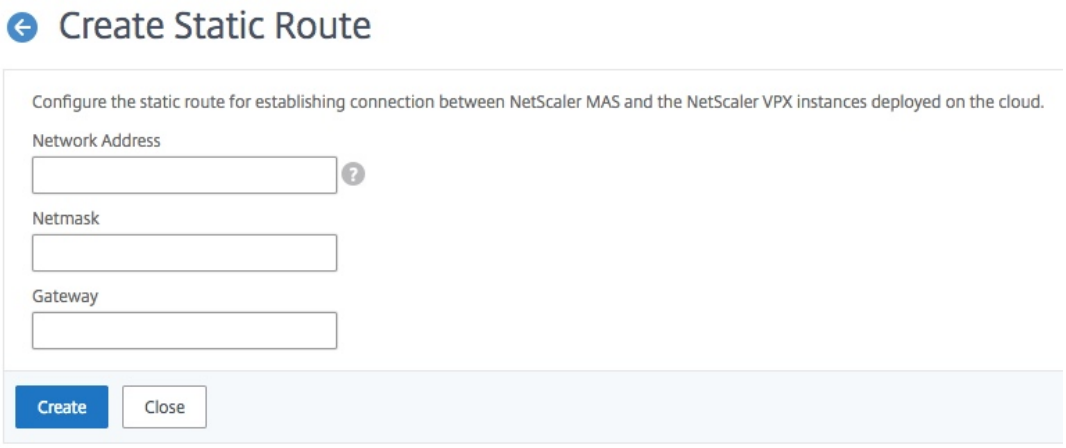
Se configura un túnel CloudBridge Connector entre el dispositivo Citrix ADC NS_Appliance-DC, en el centro de datos DC, y el dispositivo virtual Citrix ADC (VPX) NS_VPX_CBC, en la nube pública. NS_Appliance-DC y NS_VPX_CBC permiten la comunicación entre NetScaler ADM y la instancia de NetScaler ADC VPX, NS_VPX_1, implementada en la nube pública. Una vez establecida la comunicación, puede descubrir NS_VPX_1 en NetScaler ADM.

Para configurar esta topología:

1. Instale, configure e inicie una instancia de NetScaler ADC VPX en la nube pública.
   - Para obtener instrucciones, consulte Instalación de Citrix ADC VPX en AWS.
   - Para obtener instrucciones, consulte Instalación de Citrix ADC VPX en Microsoft Azure.
2. Implementar y configurar un dispositivo físico NetScaler ADC, o aprovisionar y configurar un dispositivo virtual NetScaler ADC (VPX) en una plataforma de virtualización en el centro de datos.
   - Para obtener instrucciones, consulte Instalación de dispositivos virtuales Citrix ADC en Citrix Hypervisor.
   - Para obtener instrucciones, consulte Instalación de dispositivos virtuales Citrix en VMware ESXi.
   - Para obtener instrucciones, consulte Instalación de dispositivos virtuales Citrix ADC en Microsoft Hyper-V.
3. Configure CloudBridge Connector entre el centro de datos y la nube pública. Para obtener instrucciones, consulte Configuración de CloudBridge Connector.
4. Configure la ruta estática para establecer la conexión entre Citrix ADM y las instancias de Citrix ADC VPX implementadas en la nube, de la siguiente manera:

a) Inicie sesión en Citrix ADM.

b) Desplácese hasta **Sistema > Rutas estáticas** y haga clic en **Agregar**.



c) En el campo **Dirección de red** , introduzca la dirección de la red en la que desea establecer una ruta estática desde Citrix ADM a través del conector.

d) En el campo **Máscara** de red, introduzca la máscara de red de la red.

e) En el campo **Puerta** de enlace, introduzca la dirección de la puerta de enlace.

5. Agregue las instancias de nube de NetScaler ADC VPX al NetScaler ADM especificando el rango de direcciones IP de las instancias de NetScaler ADC VPX en la nube pública. Para obtener instrucciones detalladas, consulte Agregar instancias a NetScaler ADM.

Habilitar análisis en servidores virtuales

January 30, 2024

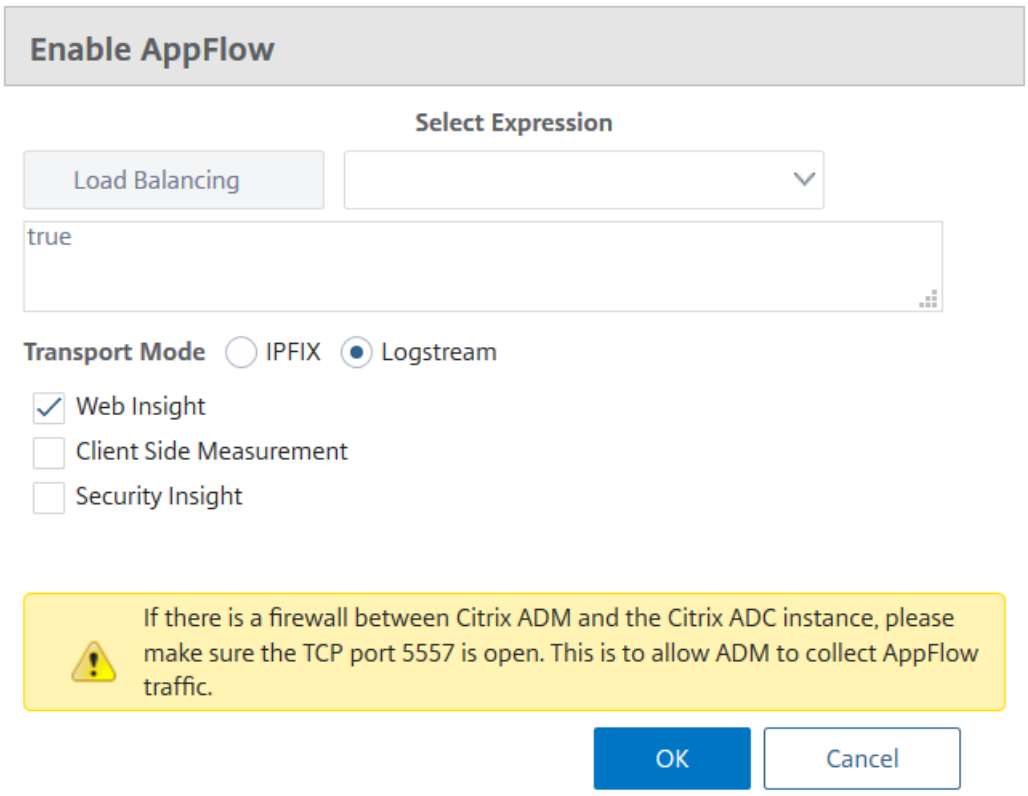
Puede habilitar el análisis para un servidor virtual específico en la instancia seleccionada, que representa un servidor de aplicaciones, y supervisar el tráfico de ese servidor de aplicaciones. Los análisis proporcionan estadísticas para el servidor virtual.

> **Nota**
>
> Para las instancias NetScaler ADC de la versión 11.0, versión 65.30 y versiones posteriores, no hay ninguna opción en NetScaler ADM para habilitar Security Insight explícitamente. Asegúrese de configurar los parámetros de AppFlow en las instancias de Citrix ADC. Una vez finalizada la configuración de los parámetros de AppFlow, Citrix ADM comienza a recibir el tráfico de Security Insight junto con el tráfico de Web Insight. Para obtener más información sobre cómo estable-

> cer los parámetros de AppFlow en las instancias de NetScaler ADC, consulte Para establecer los parámetros de AppFlow mediante la utilidad de configuración.

Para habilitar Analytics en cada instancia de Citrix ADM:

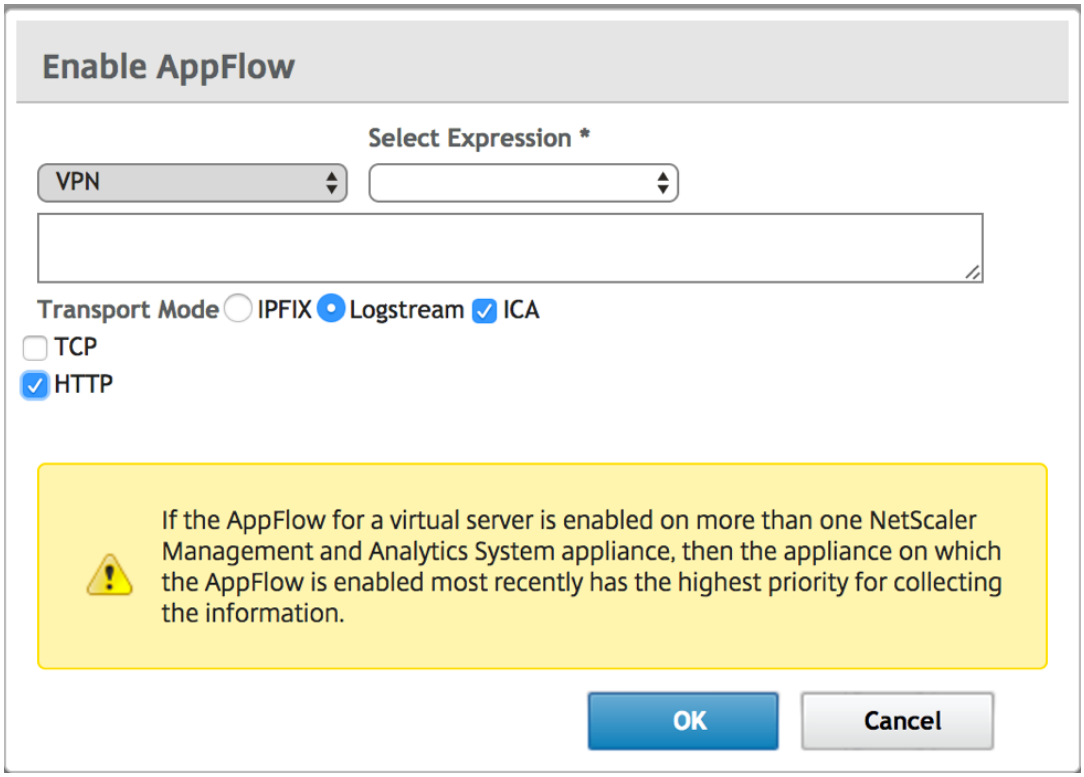
1. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC en la que quiere habilitar el análisis. Por ejemplo, Citrix ADC.
2. En la lista de instancias, seleccione una instancia.
3. En la lista **Seleccionar acción** , seleccione **Configurar análisis** .
4. En la lista de aplicaciones, seleccione los servidores virtuales y haga clic en **Habilitar AppFlow** .
5. En el campo **Habilitar AppFlow**, escriba **true** y, según los análisis que desee habilitar, seleccione **Security Insight** o **Web Insight**, o ambos.



> **Nota**
>
> Citrix ADM utiliza Citrix ADC SNIP para Logstream y NSIP para IPFIX. Si hay un firewall habilitado entre Citrix ADM y la instancia de Citrix ADC, asegúrese de abrir el siguiente puerto para permitir que Citrix ADM recopile el tráfico de AppFlow:

Modo de transporte	IP de origen	Tipo	Puerto
IPFIX	NSIP	UDP	4739
Flujo de registro	SNIP	TCP	5557

- Para **HDX Insight** y **Gateway Insight** , al hacer clic en **Habilitar AppFlow**, debe seleccionar el **servidor virtual VPN** configurado en su instancia de Citrix ADC y seleccionar las casillas **ICA** o **HTTP** correspondientes.



- Para **TCP Insight** , vaya a **Sistema** > **Configuración de análisis** > **Configurar** funciones y seleccione **Habilitar TCP Insight** .
- Para **Video Insight** , debe realizar los cambios de configuración en el dispositivo Citrix ADC. Para obtener más información sobre cómo habilitar el análisis para Video Insight, consulte Video Insight.
- Para **WAN Insight** ,
  a) Vaya a **Infraestructura** > **Instancias** > **NetScaler SD-WAN WO** y seleccione el dispositivo de optimización de WAN del centro de datos.
  b) En el menú desplegable **Acción**, seleccione **Habilitar información**.
  c) Seleccione los siguientes parámetros según sea necesario:

- Recopilación de datos geográficos para HDX Insight: comparte la dirección IP del cliente con la API Google Geo.
- AppFlow: comienza a recopilar datos de las instancias de optimización de WAN
  - TCP y WANOpt: proporciona informes de TCP y WANOpt Insight.
  - HDX: Proporciona informes HDX Insight.
  - TCP solo para HDX: Proporciona TCP solo para los informes HDX Insight.

Puede seleccionar el **modo de transporte de AppFlow** a IPFIX o Logstream mientras habilita AppFlow en las instancias de Citrix ADC descubiertas en Citrix ADM. Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

En la siguiente tabla se describen las funciones de Citrix ADM que admite IPFIX y Logstream como modo de transporte:

Función	IPFIX	Flujo de registro
Información web	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
Insight SSL	No compatible	•
CR Insight	•	•
Reputación IP	•	•
AppFirewall	•	•
Medición del lado del	•	•
Syslog/Auditlog	•	•

También puede habilitar o inhabilitar el procesamiento del tráfico de Web Insight mediante la opción **Habilitar Web Insight** de Citrix ADM. Si no quiere supervisar el tráfico de Web Insight, puede inhabilitar la opción. Para obtener más información, consulte Procesamiento del tráfico de Web Insight mediante Citrix ADM.

Configurar servidor NTP

January 30, 2024

Puede configurar un servidor de protocolo de hora de red (NTP) en Citrix ADM para sincronizar su reloj con el servidor NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

Para configurar un servidor NTP en Citrix ADM:

1. Vaya a **Sistema** > **Servidores NTP** y, a continuación, haga clic en **Agregar** .
2. En la página **Crear servidor NTP**, introduzca los siguientes detalles:
    - **Nombre del servidor/dirección IP**: Introduzca el nombre de dominio o la dirección IP del servidor NTP. El nombre o la dirección IP no se pueden cambiar después de agregar el servidor NTP.
    - **Intervalo mínimo de sondeo**: Especifique el valor mínimo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que el intervalo mínimo de sondeo sea de 64 segundos, que se puede expresar como 2^6, introduzca 6
    - **Intervalo máximo de sondeo**: Especifique el valor máximo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que el intervalo máximo de sondeo sea de 256 segundos, que se puede expresar como 2^8, introduzca 8.
    - **Identificador de clave**: introduzca el identificador de clave que se puede utilizar para la autenticación de clave simétrica con el servidor NTP. No añada un identificador de clave si decide seleccionar Autokey.
    - **Clave automática**: Seleccione **Autokey** si desea utilizar la autenticación de clave pública con el servidor NTP. No seleccione si desea agregar un identificador de clave.
    - **Preferido**: Seleccione esta opción si desea especificar este servidor NTP como servidor preferido para la sincronización de relojes. Esto solo se aplica si hay más de un servidor configurado.
3. Haga clic en **Crear**.

Para habilitar la sincronización NTP en NetScaler ADM:

1. Vaya a **Sistema** > **Servidores NTP**.
2. Haga clic en **Sincronización de NTP** y seleccione la casilla de verificación **Habilitar sincronización de NTP** .
3. Haga clic en **Aceptar**.

Configurar la configuración del sistema

January 30, 2024

Antes de empezar a utilizar NetScaler ADM para administrar y supervisar sus instancias y aplicaciones, se recomienda configurar algunas opciones del sistema que garanticen un rendimiento óptimo de su servidor NetScaler ADM.

Configurar alarmas del sistema

Debe configurar las alarmas del sistema para asegurarse de estar al tanto de cualquier problema crítico o importante del sistema. Por ejemplo, es posible que quiera recibir una notificación si el uso de CPU es alto o si hay varios errores de inicio de sesión en el servidor. Para algunas categorías de alarmas, como cpuUsageHigh o memoryUsageHigh, puede establecer umbrales y definir la gravedad (como Crítica o Mayor) de cada una. Para algunas categorías, como InventoryFailed o LoginFailure, solo puede definir la gravedad. Cuando se supera el umbral de una categoría de alarma (por ejemplo, MemoryUsageHigh) o cuando se produce un evento correspondiente a la categoría de alarma (por ejemplo, LoginFailure), se graba un mensaje en el sistema y puede verlo como mensaje de syslog.

Para configurar alarmas del sistema:

1. Vaya a **Sistema > Alarmas** , seleccione la alarma que desea configurar y haga clic en **Editar** .
2. En la página **Configurar alarma**, seleccione la gravedad de la alarma y establezca el umbral.
3. Para ver las alarmas que han superado el umbral o en las que se ha producido un evento, vaya a **Sistema > Auditoría** y haga clic en **Mensajes de Syslog** .

Configurar notificaciones del sistema

Puede enviar notificaciones a grupos de usuarios seleccionados para una serie de funciones relacionadas con el sistema. Puede configurar un servidor de notificaciones en NetScaler ADM y configurar servidores de Gateway de correo electrónico y servicio de mensajes cortos (SMS) para enviar notificaciones de correo electrónico y texto a los usuarios. Esto garantiza que se le notifique cualquier actividad a nivel del sistema, como el inicio de sesión del usuario o el reinicio del sistema.

Para configurar las notificaciones del sistema:

1. Vaya a **Sistema > Notificaciones** . En **Configuración** , haz clic en **Cambiar configuración de notificaciones** .
2. En la página **Configurar configuración de notificación del sistema**, seleccione la categoría o categoría de eventos generados por NetScaler ADM.

3. A continuación, configure el servidor de correo electrónico o el servidor de SMS para recibir notificaciones por correo electrónico o SMS o ambos.

Configurar las opciones de poda del sistema

Para limitar la cantidad de datos de informes que se almacenan en la base de datos del servidor Citrix ADM, puede especificar el intervalo durante el que quiere que Citrix ADM conserve los datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

Para configurar la configuración de poda delsistema :

1. Vaya a **Sistema > Administración del sistema**. En **Configuración de poda**, haga clic en Configuración de **poda del sistema** .
2. En la página **Configurar las opciones de poda del sistema** , especifique el número de días durante los que desea conservar los datos **y** haga clic en Aceptar .

Configurar las opciones de copia de seguridad del sistema

Citrix ADM realiza copias de seguridad automáticas del sistema todos los días a las 00:30 horas. De forma predeterminada, guarda tres archivos de copia de seguridad. Es posible que desee conservar un mayor número de copias de seguridad del sistema. También puede cifrar el archivo de respaldo. También puede optar por guardar la copia de seguridad en un servidor externo.

Para configurar las opciones de copia de seguridad del sistema:

1. Vaya a **Sistema > Administración del sistema**.
2. En **Configuración de copia de seguridad**, haga clic en **Configuración de copia de seguridad del sistema**.
3. En la página Configurar los **ajustes de copia de seguridad del sistema** , especifique los valores necesarios.

Configurar las opciones de copia de seguridad de instancia

Si hace una copia de seguridad del estado actual de una instancia de Citrix ADC, puede utilizar los archivos de copia de seguridad para restaurar la estabilidad en caso de que la instancia se vuelva inestable. Hacerlo es especialmente importante antes de realizar una actualización. De forma predeterminada, se realiza una copia de seguridad cada 12 horas y se conservan tres archivos de respaldo en el sistema.

Para configurar las opciones de copia de seguridad de instancias:

1. Vaya a **Sistema > Administración del sistema**.
2. En **Configuración de copia** de seguridad, seleccione **Configuración de copia de seguridad de instancia** y especifique los valores necesarios.

Configurar las opciones de poda del evento de instancia

Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos del servidor Citrix ADM, puede especificar el intervalo durante el que quiere que Citrix ADM conserve los datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00:00 horas).

Para configurar los ajustes de poda deeventos de instancia :

1. Vaya a **Sistema > Administración del sistema**.
2. En **Configuración de podar**, haga clic en **Configuración de podar eventos de instancia**.
3. Introduzca el intervalo de tiempo, en días, para el que desea conservar los datos en el servidor Citrix ADM **y** haga clic en Aceptar.

Configurar los ajustes de purga de syslog de instancias

Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog. Puede especificar el número de días después de los cuales se eliminarán los datos genéricos de Syslog de Citrix ADM.

Para configurar los ajustes de purga delsyslog de la instancia :

1. Vaya a **Sistema** > **Administración del sistema**. En Configuración de poda, haga clic en Configuración de **purga de Syslog de instancias** .
2. En la página Configurar los ajustes de depuración de Syslog de la instancia, especifique el número de días entre 1 y 180 en el campo **Conservar datos genéricos de Syslog** .
3. Haga clic en **Aceptar**.

Actualizaciones

January 30, 2024

Cada versión de Citrix ADM ofrece funciones nuevas y actualizadas con mayor funcionalidad. Citrix recomienda actualizar Citrix ADM a la versión más reciente para aprovechar las nuevas funciones y

correcciones de errores. En las notas de la versión que acompañan a cada anuncio de lanzamiento se incluye una lista completa de las mejoras, los problemas conocidos y las correcciones de errores. También es importante comprender el marco de licencias y los tipos de licencias que se pueden utilizar antes de empezar a actualizar. Para obtener información sobre licencias de Citrix ADM, consulteLicencias.

La información de la ruta de actualización también está disponible en la Guía de actualización de Citrix.

Antes de actualizar la versión

Descargue el paquete de actualización de la página de descargas de Citrix ADM y siga las instrucciones de este artículo para actualizar el sistema a la versión 12.1 más reciente. Una vez iniciada la operación de actualización, Citrix ADM se reinicia y las conexiones existentes se finalizan y se vuelven a conectar cuando la actualización se completa correctamente. La configuración existente se conserva, pero Citrix ADM no procesa ningún dato hasta que la actualización se complete correctamente.

> **Importante**
>
> La versión y compilación de Citrix ADM deben ser **iguales o superiores a** la versión y compilación de Citrix ADC. Por ejemplo, si ha instalado Citrix ADM 12.1 compilación 50.39, asegúrese de haber instalado Citrix ADC 12.1 compilación 50.28/50.31 o anterior.

Puntos a tener en cuenta antes de actualizar a 12.1:

- Si va a actualizar a la versión 12.1 de la compilación 48.18 de Citrix ADM desde la versión 11.1 o desde la versión 12.0 de compilación anterior a la 56.x, lleve a cabo los siguientes pasos.
  - Actualice desde la versión existente a la versión 12.0 build 57.24.
  - A continuación, actualice a la versión más reciente de la versión 12.1.

    Debe seguir este proceso de dos pasos porque se requieren ciertos procedimientos de limpieza para actualizar correctamente a la versión 12.1. Estos procedimientos solo están disponibles a partir de 12.0 build 56.x.
- Con la versión 12.1, la implementación de alta disponibilidad tiene la capacidad de configurar una dirección IP flotante en el nodo principal y eliminar la necesidad de un balanceador de cargas Citrix ADC independiente. Debido a esta mejora, la implementación de alta disponibilidad debe estar en la misma subred. Si su implementación actual se encuentra en diferentes subredes, debe revisar este artículo para obtener información sobre el proceso de actualización.
- Con 12.1, se ha eliminado el soporte avanzado de copia de seguridad. La función de copia de seguridad avanzada ya no está disponible después de actualizar a Citrix ADM 12.1. Revisa este artículo para obtener más información.

> **Nota**
>
> No puede cambiar Citrix ADM de una compilación 12.1 a ninguna compilación de una versión anterior.

Precauciones recomendadas:

- Realice una copia de seguridad del servidor Citrix ADM antes de actualizar.
- Después de la actualización, es posible que deba restablecer las conexiones entre el servidor Citrix ADM y las instancias administradas. Un mensaje de confirmación le avisa de que las conexiones pueden fallar si continúa.
- Para los servidores de Citrix ADM en configuración de alta disponibilidad, al actualizar la versión, no realice ningún cambio de configuración en ninguno de los nodos.

  > **Advertencia**
  >
  > No actualice el explorador hasta que el proceso de actualización se haya completado correctamente. El proceso de actualización puede tardar unos minutos en finalizar.

- Después de la actualización, el nodo activo puede cambiar en un par de alta disponibilidad.

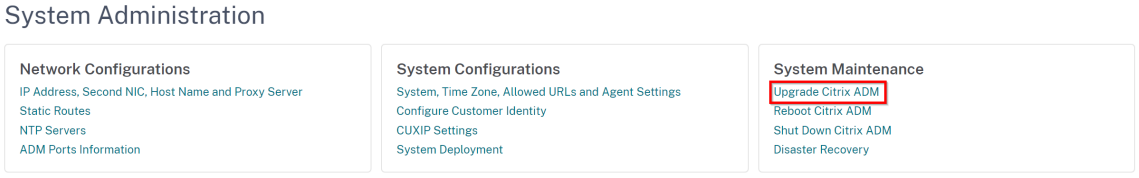
Actualizar un único servidor Citrix ADM

Para actualizar un único servidor Citrix ADM:

1. En un navegador web, escriba la dirección IP del servidor Citrix ADM.

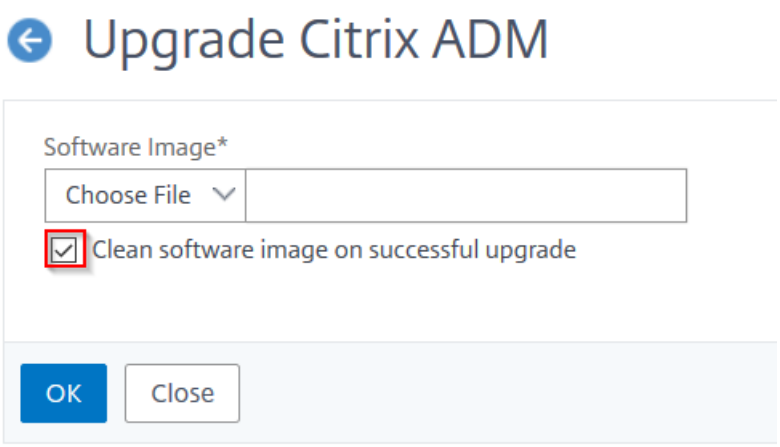
   > **Nota:**
   >
   > Para los servidores Citrix ADM en modo de alta disponibilidad, escriba la dirección IP de cualquiera de los servidores Citrix ADM del par HA o del servidor virtual de equilibrio de carga.

2. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de administrador.
3. Vaya a**Sistema** > **Administraciones del sistema**. En el subtítulo **Administración del sistema**, haga clic en **Actualizar Citrix ADM**.

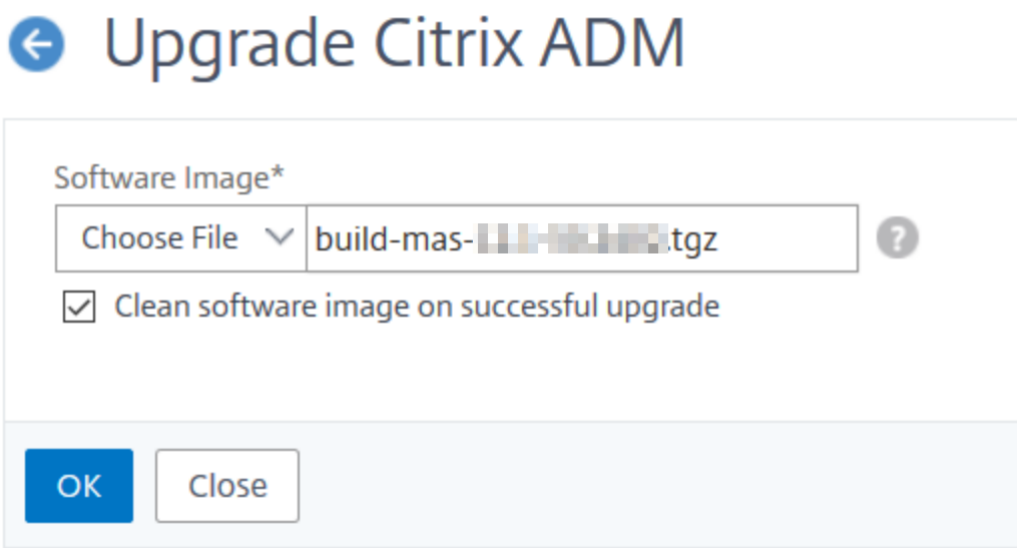


4. En la página **Actualizar Citrix ADM**, marque la casilla **Limpiar imagen de software en una actualización correcta** para eliminar archivos de imagen después de la actualización. Al seleccionar esta opción, se quitan automáticamente los archivos de imagen Citrix ADM tras la actualización.

   > **Nota**
   >
   > Esta opción está seleccionada de forma predeterminada. Si no activa esta casilla de verificación antes de iniciar el proceso de actualización, debe eliminar manualmente las imágenes.



5. A continuación, puede cargar un nuevo archivo de imagen seleccionando **Local** (su equipo local) o **Dispositivo**. El archivo de compilación debe estar presente en el dispositivo virtual Citrix ADM.



   Aparece el cuadro de diálogo Confirmar. Haga clic en **Aceptar**.

6. Haga clic en **Aceptar**.

Se inicia el proceso de actualización.

Actualice un par de alta disponibilidad de versiones anteriores a la 12.1

Para los servidores Citrix ADM en modo de alta disponibilidad, puede actualizarlos accediendo al nodo activo o a la dirección IP del servidor virtual de equilibrio de carga. Ambos servidores Citrix ADM se actualizan automáticamente a la versión más reciente una vez que se inicia el proceso de actualización en cualquiera de los servidores.

> **Importante**
>
> **Puntos a tener en cuenta al actualizar Citrix ADM en modo de alta disponibilidad**
>
> Al actualizar Citrix ADM en modo de alta disponibilidad a 12.1 desde una versión anterior, la conexión de alta disponibilidad se establece internamente mediante el script "join HA"que se ejecuta en el nodo secundario. El tiempo necesario para el proceso de actualización depende de la infraestructura de red, los datos presentes en la base de datos y la velocidad del enlace. El restablecimiento de la conexión entre los dos nodos puede tardar algunas horas. Durante este período, el nodo primario no recibe ningún latido del nodo secundario. Aparece una notificación de falta de latidos en la interfaz de usuario principal hasta que se complete el proceso de actualización. Una vez finalizado el proceso de actualización, el nodo secundario se reinicia y se completa la implementación de alta disponibilidad.
>
> **Nota**
>
> Para conocer el estado de la actualización, inicie sesión en cada nodo mediante SSH, ejecute los siguientes comandos y compruebe el resultado:
>
> pgrep -lf installmas
>
> pgrep -lf maintenance
>
> pgrep -lf join_streaming_replication
>
> pgrep -lf pg_basebackup
>
> Si alguno de estos comandos muestra un proceso en ejecución en alguno de los nodos, significa que la actualización está en curso y no debe interrumpirse. No reinicie Citrix ADM durante este tiempo ni intente forzar la conmutación por error en el nodo secundario.
>
> Una vez finalizado el proceso de actualización, es posible que no pueda iniciar sesión con nsroot/nsroot ni con sus credenciales de usuario. Esto se debe a que el subsistema Citrix ADM no se ha reiniciado por completo o es posible que la migración aún esté en curso. No reinicie Citrix ADM ni intente recuperar la contraseña. Esto podría tener un efecto no deseado y el sistema podría comportarse de manera incoherente. Si es necesario, puede intentar iniciar sesión con las <your_password_for_the_nsroot_user>credenciales nsrecover/.

> Tras la actualización y antes de iniciar las operaciones, asegúrese de que tanto el nodo principal como el secundario estén actualizados y que se haya completado el reinicio.
>
> **Nota:**
>
> No puede actualizar Citrix ADM en modo de alta disponibilidad mediante la CLI.

Licencias agrupadas en servidores Citrix ADM en alta disponibilidad:

Cuando los servidores Citrix ADM se implementan en modo de alta disponibilidad, el archivo de licencia se adjunta al nodo principal y se configura (se bloquea el nodo) con el HostID o la dirección MAC del servidor principal. Citrix ADM ahora admite la función de licencias agrupadas en alta disponibilidad a partir de la versión 12.1. Para configurar la función de licencias agrupadas en ambos nodos, debe tener archivos de licencia idénticos en ambos nodos. Para instalar una licencia idéntica en el nodo secundario, debe volver a alojar la licencia en el HostID (dirección MAC) del nodo secundario.

Considere un escenario en el que Citrix ADM tiene dos nodos de servidor S1 y S2 en modo de alta disponibilidad. El archivo de licencia original, L1, está instalado en el servidor S1. El archivo de licencia L2 realojado ahora debe asignarse a S2.

Siga los pasos para actualizar Citrix ADM en modo de alta disponibilidad de la versión 12.0 a la 12.1 y configurar la función de licencia agrupada:

1. Inicie sesión en el nodo principal de los servidores Citrix ADM en modo de alta disponibilidad y realice el proceso de actualización.
2. Instale el archivo de licencia L2 realojado en el nodo S2 del servidor secundario.

   En este momento:

   - Si S2 es el nodo principal, puede instalar la licencia L2 accediendo a la GUI de esa instancia.
   - Si S2 es el nodo secundario, debe realizar una conmutación por error de forma manual para que S2 pase a ser el nodo principal. Instale la licencia L2 en el nuevo nodo principal mediante la interfaz gráfica de usuario.
     Esto se debe a que solo puede acceder al servidor principal en alta disponibilidad a través de la GUI.
3. Configure la dirección IP flotante en el nuevo nodo principal.
4. Elimine las direcciones IP del servidor de licencias en las instancias de Citrix ADC y vuelva a configurarlas para usar la dirección IP flotante. Realice esto en todas las instancias de Citrix ADC.

Citrix recomienda realizar la actualización de las licencias agrupadas de alta disponibilidad de Citrix ADM mediante la creación de una ventana de mantenimiento en las instancias de Citrix ADC. Esto se debe a que al eliminar el servidor de licencias y agregar una dirección IP flotante, las instancias de Citrix ADC vuelven temporalmente al soporte mínimo de ancho de banda.

Escenarios de actualización de alta disponibilidad

Puede haber dos escenarios en los que los servidores Citrix ADM se implementen en modo de alta disponibilidad.

- Los servidores principal y secundario se implementan en la misma subred.
- Los servidores principal y secundario se implementan en diferentes subredes.

Este documento de actualización le ayuda a actualizar Citrix ADM en estos dos escenarios.

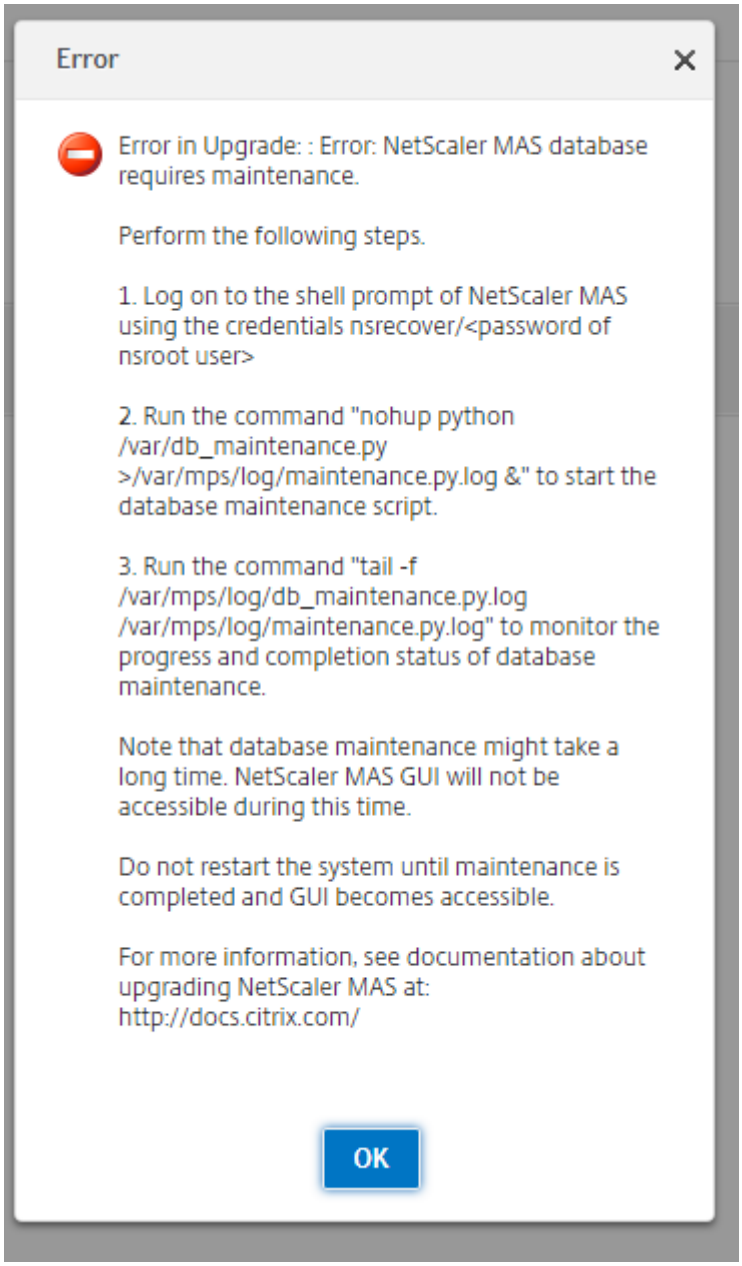
- Actualización de una configuración de alta disponibilidad en la misma subred
- Actualización de una configuración de alta disponibilidad en diferentes subredes

Actualizar una configuración de alta disponibilidad en la misma subred

Citrix ADM 12.1 gestiona automáticamente la actualización de los servidores Citrix ADM implementados en modo de alta disponibilidad en la misma subred.

Para actualizar Citrix ADM implementado en modo de alta disponibilidad en la misma subred:

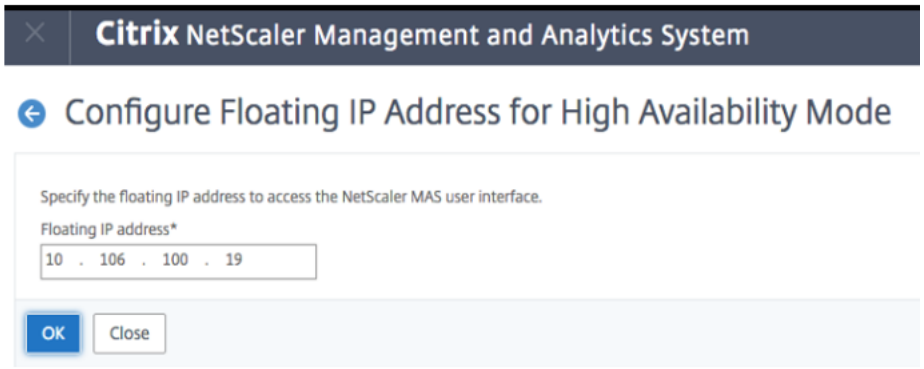
1. Inicie sesión en el nodo principal y vaya a **Sistema** > **Administraciones del sistema**.
2. En**Administración del sistema**, haga clic en **Actualizar Citrix ADM**.
3. Si se produce un error durante la actualización, aparece el siguiente mensaje de error. Siga las instrucciones que se indican en el mensaje del servidor principal.



4. Como parte del proceso de actualización, debe realizar un procedimiento de limpieza a través de la CLI. Durante el proceso de limpieza, el nodo secundario pasa a ser el nodo principal. No se puede acceder al nodo principal antiguo a través de su GUI. No reinicie el nodo principal antiguo ni el nuevo mientras el proceso de limpieza esté en curso. Una vez finalizado el proceso de limpieza, continúe con el procedimiento de actualización a través del nuevo nodo principal.
5. Una vez finalizado el proceso de actualización, los dos nodos deben sincronizar sus bases de datos. El tiempo necesario para completar la sincronización y para que aparezca el nuevo nodo secundario depende de los datos presentes en las bases de datos.

> **Nota**
>
> Una vez que la actualización se haya realizado correctamente, debe configurar la dirección IP flotante mediante la interfaz de usuario de Citrix ADM.

6. Para configurar la dirección IP flotante, vaya a**Sistema > Implementación > Configurar la dirección IP flotante para el modo de alta disponibilidad**.
7. Especifique la dirección IP flotante como se muestra en la siguiente imagen y haga clic en**Aceptar**.



Actualizar una configuración de alta disponibilidad en diferentes subredes

Un administrador debe gestionar la actualización de los servidores Citrix ADM implementados en modo de alta disponibilidad en diferentes subredes.

En este escenario, el nodo 1 de Citrix ADM HA (principal) está en la subred 1 y el nodo 2 de Citrix ADM HA (secundario) está en la subred 2.

Para actualizar Citrix ADM implementado en modo de alta disponibilidad en diferentes subredes:

1. Rompa manualmente la configuración de alta disponibilidad. Para obtener más información, consulte Desactivar la alta disponibilidad.
2. Actualice el nodo independiente 1 de Citrix ADM. Para obtener más información sobre cómo actualizar Citrix ADM, consulte Actualizar un único servidor Citrix ADM.
3. Configure y registre un nuevo nodo 3 independiente de Citrix ADM en la subred 1.
4. Después de registrar el nodo 1 y el nodo 3, implemente ambos nodos en modo de alta disponibilidad. Para obtener más información, consulte Implementación del nodo principal y secundario como un par de alta disponibilidad.

> **Nota**
>
> La configuración de la dirección IP flotante es obligatoria.

5. Elimine el nodo Citrix ADM 2.

Actualice un par de alta disponibilidad de las versiones 12.1 anteriores a la versión más reciente

Puede actualizar los servidores Citrix ADM implementados en alta disponibilidad desde una versión 12.1 anterior a una versión 12.1 posterior.

Para actualizar Citrix ADM implementado en modo de alta disponibilidad:

1. Descargue el archivo de imagen Citrix ADM 12.1 build 49.37 de la página de descargas de Citrix.com.
2. Inicie sesión en el nodo principal y vaya a **Sistema** > **Administraciones del sistema**.
3. En Administración del sistema, haga clic en **Actualizar Citrix ADM**.
4. Navega hasta la carpeta en la que se encuentra la imagen.

   Durante la actualización, no realice ningún cambio de configuración en ninguno de los nodos.

   > **Advertencia**
   >
   > - No actualice el explorador hasta que el proceso de actualización se haya completado correctamente. El proceso de actualización puede tardar unos minutos en finalizar.

   Después de la actualización, el nodo activo puede cambiar en un par de alta disponibilidad.

Actualice la implementación de recuperación ante desastres de Citrix ADM

Actualizar la implementación de recuperación ante desastres de Citrix ADM es un proceso de dos pasos:

Primero debe actualizar los nodos Citrix ADM configurados en modo de alta disponibilidad en el sitio principal. Más adelante, debe actualizar el nodo de recuperación ante desastres.

Asegúrese de que ha actualizado los servidores Citrix ADM implementados en alta disponibilidad antes de actualizar el nodo de recuperación ante desastres.

- Si está actualizando los servidores Citrix ADM en modo de alta disponibilidad de las versiones anteriores a la 12.1, consulte Actualizar un par de alta disponibilidad de versiones anteriores a la 12.1 en este documento.

- Si va a actualizar de una versión 12.1 anterior a una versión 12.1 posterior en el par de alta disponibilidad, consulte Actualizar un par de alta disponibilidad de las versiones 12.1 anteriores a la versión más reciente de este documento.

Actualizar el nodo de recuperación ante desastres de Citrix ADM

1. Descargue el archivo de imagen de actualización de Citrix ADM desde el sitio de descarga de Citrix.
2. Cargue este archivo en el nodo de recuperación ante desastres con las credenciales "nsrecover" .
3. Inicie sesión en el nodo de recuperación ante desastres con las credenciales "nsrecover".

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 31 05:41:16 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-mas-12.1-500.113.tgz
```

4. Desplácese hasta la carpeta donde colocó el archivo de imagen y descomprima el archivo.
5. Ejecute el siguiente script:

   ./installmas

```
bash-3.2# ./installmas
```

Actualizar agentes en prem para la implementación en varios sitios

La actualización de la implementación del agente Citrix ADM es un proceso de tres pasos.
Asegúrese de haber realizado las siguientes tareas antes de actualizar los agentes locales:

1. Actualice los servidores Citrix ADM implementados en alta disponibilidad.
   - Si está actualizando los servidores Citrix ADM en modo de alta disponibilidad de las versiones anteriores a la 12.1, consulte Actualizar un par de alta disponibilidad de versiones anteriores a la 12.1 en este documento.
   - Si va a actualizar de una versión 12.1 anterior a una versión 12.1 posterior en el par de alta disponibilidad, consulte Actualizar un par de alta disponibilidad de las versiones 12.1 anteriores a la versión más reciente
2. Actualice el nodo de recuperación ante desastres de Citrix ADM.

Para obtener más información, consulte Actualizar la implementación de recuperación ante desastres de Citrix ADM.

Actualizar el agente on-prem

1. Descargue el archivo de imagen de actualización del agente Citrix ADM desde el sitio de descargas de Citrix.
2. Cargue este archivo en el nodo del agente con las credenciales "nsrecover".
3. Asegúrese de descargar la imagen de actualización del agente correcta. El nombre del archivo de imagen tiene el siguiente formato:

   build-masagent-12.1-48.18.tgz
4. Inicie sesión en el agente local con las credenciales "nsrecover".
5. Desplácese hasta la carpeta donde colocó el archivo de imagen y descomprima el archivo.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Ejecute el siguiente script:

   . /instalar como agente

```
bash-3.2# ./installmasagent
```

Eliminar la compatibilidad con la función de copia de seguridad y restauración avanzadas de Citrix ADM

En lugar de utilizar la función de respaldo avanzada para realizar una copia de seguridad completa de su servidor Citrix ADM, ahora puede utilizar la nueva función de **recuperación ante desastres** disponible en la versión 12.1 de Citrix ADM para realizar una copia de seguridad completa de su configuración de alta disponibilidad de Citrix ADM y ayudar en los casos prácticos de continuidad empresarial.

> **Importante**
>
> 1. La función de copia de seguridad avanzada ya no está disponible después de actualizar a Citrix ADM 12.1. Para eliminar la función de copia de seguridad avanzada y seguir realizando copias de seguridad mediante la función de recuperación ante desastres, consulte

> Hacer una copia de seguridad de Citrix ADM después de actualizar a Citrix ADM 12.1. La recuperación ante desastres solo se admite con Citrix ADM HA.
>
> 2. Para seguir realizando una copia de seguridad parcial del servidor Citrix ADM que incluya los archivos de configuración, los detalles de la instancia, los datos del sistema, etc. y, a continuación, restaurar el servidor Citrix ADM en una implementación independiente (copia de seguridad parcial), consulte Cómo hacer una copia de seguridad y restaurar el servidor Citrix ADM en una implementación de un solo servidor.

En caso de desastre en el servidor principal, utilice la función de recuperación ante desastres para iniciar y configurar Citrix ADM en el mismo servidor principal sin perder datos. La función solo está disponible en los servidores Citrix ADM implementados en una configuración de alta disponibilidad a partir de la versión 12.1 de Citrix ADM.

Haga una copia de seguridad de su servidor Citrix ADM después de actualizar a Citrix ADM 12.1

Para continuar realizando copias de seguridad del servidor Citrix ADM, Citrix recomienda lo siguiente:

1. Elimine la configuración de copia de seguridad remota en Citrix ADM de la siguiente manera:
    a) Vaya a **Sistema** > **Administración del sistema** > **Configuración avanzada de copia de seguridad del sistema**.
    b) En la página Configurar opciones de copia de seguridad avanzadas, seleccione **No** para inhabilitar las copias de seguridad remotas.
    c) Haga clic en **Aplicar configuración**. Espere a que el servidor Citrix ADM se reinicie y aplique la configuración modificada.
    d) Elimine el nodo de respaldo remoto.
2. Implemente y configure un nuevo servidor Citrix ADM, cree una configuración de alta disponibilidad con el servidor Citrix ADM existente que se reinició en el paso anterior.
    - Para obtener más información sobre la implementación independiente de Citrix ADM, consulteImplementar Citrix ADM.
    - Para obtener más información sobre la implementación de Citrix ADM HA, consulteImplementación de alta disponibilidad.
3. Configure Disaster Recovery para continuar con la copia de seguridad y la restauración de los datos. Para obtener más información sobre la recuperación ante desastres, consulte Configurar la recuperación ante desastres para una alta disponibilidad.

Agregar un disco adicional al servidor Citrix ADM

Si sus requisitos de almacenamiento de Citrix ADM superan el espacio en disco predeterminado (120 gigabytes), puede conectar un disco adicional. Puede conectar un disco adicional tanto en las implementaciones de un solo servidor como en las de alta disponibilidad.

Al actualizar Citrix ADM de la versión 12.0 a la 12.1, las particiones que había creado en el disco adicional en la versión anterior siguen siendo las mismas. Las particiones no se eliminan ni se cambian de tamaño.

El procedimiento para conectar un disco adicional sigue siendo el mismo en la versión actualizada. Ahora puede utilizar la nueva herramienta de partición de discos en Citrix ADM para crear particiones en el disco recién agregado. También puede utilizar la herramienta para cambiar el tamaño de las particiones en el disco adicional existente. Para obtener más información sobre cómo conectar discos adicionales y utilizar la nueva herramienta de particionamiento de discos, consulte Cómo conectar un disco adicional a Citrix ADM.

Aprovisione instancias de Citrix ADC en OpenStack mediante StyleBooks

A partir de la compilación 49.23 de Citrix ADM 12.1, se actualizó la arquitectura del flujo de trabajo de orquestación de OpenStack. El flujo de trabajo utiliza ahora los StyleBooks de Citrix ADM para configurar instancias de Citrix ADC. Si va a actualizar a Citrix ADM 12.1 compilación 49.23 desde la versión 12.0 o desde la versión 12.1 compilación 48.18, debe ejecutar la siguiente script de migración:

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

Para obtener más información sobre el StyleBook “os-cs-lb-mon”y el script de migración, consulte Provisioningof Citrix ADC VPX en OpenStack mediante StyleBook

Autenticación

January 30, 2024

24 de mayo de 2018

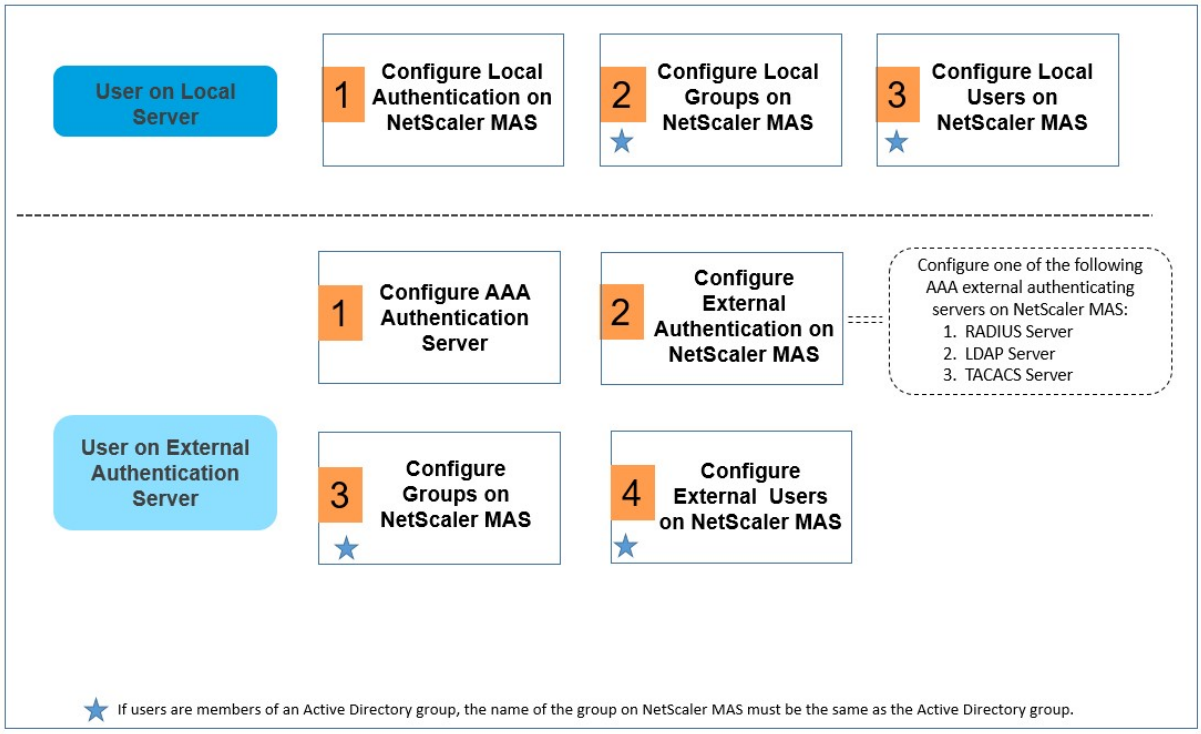
Los usuarios pueden autenticarse internamente mediante Citrix Application Delivery Management (ADM), externamente mediante un servidor de autenticación o ambos. Si se utiliza la autenticación local, el usuario debe estar en la base de datos de seguridad Citrix ADM. Si el usuario se autentica externamente, el «nombre externo» del usuario debe coincidir con la identidad del usuario externo registrada en el servidor de autenticación, según el protocolo de autenticación seleccionado.

Citrix ADM admite la autenticación externa mediante los protocolos RADIUS, LDAP y TACACS. Este soporte unificado proporciona una interfaz común para autenticar y autorizar a todos los usuarios del servidor de autenticación, autorización y contabilidad (AAA) locales y externos que acceden al sistema. Citrix ADM puede autenticar a los usuarios independientemente de los protocolos reales que utilicen para comunicarse con el sistema. Cuando un usuario intenta acceder a una implementación de Citrix ADM configurada para la autenticación externa, el servidor de aplicaciones solicitado envía el nombre de usuario y la contraseña al servidor RADIUS, LDAP o TACACS para su autenticación. Si la autenticación se realiza correctamente, se utiliza el protocolo correspondiente para identificar al usuario en Citrix ADM.

Puede autenticar a sus usuarios en Citrix ADM de dos maneras:

- Mediante servidores locales Citrix ADM
- Mediante el uso de servidores de autenticación externos

El siguiente diagrama de flujo muestra el flujo de trabajo a seguir al autenticar usuarios locales o externos:



Configurar servidores de autenticación externos

Citrix ADM admite varios protocolos para proporcionar servicios externos de autenticación, autorización y contabilidad (AAA).

Citrix ADM envía todas las solicitudes de servicio de autenticación, autorización y contabilidad (AAA)

al servidor RADIUS, LDAP o TACACS+ remoto. El servidor AAA remoto recibe la solicitud, la valida y envía una respuesta a Citrix ADM. Cuando se configura para utilizar un servidor RADIUS, TACACS+ o LDAP remoto para la autenticación, Citrix ADM se convierte en un cliente RADIUS, TACACS+ o LDAP. En cualquiera de estas configuraciones, los registros de autenticación se almacenan en la base de datos del servidor host remoto. El nombre de la cuenta de inicio y cierre de sesión, los permisos asignados y los registros de contabilidad del tiempo también se almacenan en el servidor AAA para cada usuario.

Además, puede utilizar la base de datos interna de NetScaler ADM para autenticar usuarios localmente. Crear entradas en la base de datos para los usuarios y sus contraseñas y roles predeterminados. También puede crear grupos de servidores para tipos específicos de autenticación. La lista de servidores de un grupo de servidores es una lista ordenada. El primer servidor de la lista siempre se utiliza a menos que no esté disponible, en cuyo caso se utiliza el siguiente servidor de la lista. Puede configurar servidores de diferentes tipos en un grupo y también puede incluir la base de datos interna como respaldo de autenticación alternativo en la lista configurada de servidores AAA.

Configurar un servidor de autenticación RADIUS

Puede configurar Citrix ADM para autenticar el acceso de los usuarios con uno o más servidores RADIUS. Es posible que su configuración requiera el uso de una dirección IP del servidor de acceso a la red (IP del NAS) o un identificador del servidor de acceso a la red (ID del NAS). Al configurar Citrix ADM para usar un servidor de autenticación RADIUS, siga las siguientes pautas: Si habilita el uso de la dirección IP del NAS, el dispositivo envía su dirección IP configurada al servidor RADIUS, en lugar de enviar la dirección IP de origen utilizada para establecer la conexión RADIUS.

- Si configura el ID del NAS, el dispositivo envía el identificador al servidor RADIUS. Si no configura el ID del NAS, el dispositivo envía su nombre de host al servidor RADIUS.
- Si habilita la dirección IP del NAS, el dispositivo ignora cualquier ID de NAS que esté configurado y utiliza la IP del NAS para comunicarse con el servidor RADIUS.

Para configurar un servidor de autenticación RADIUS:

1. En NetScaler ADM, vaya a **Sistema** > **Autenticación** > **RADIUS**.
2. En la página **RADIUS**, haga clic en **Agregar**.
3. En la página **Crear servidor RADIUS** , defina los parámetros y haga clic en **Crear** para agregar el servidor a la lista de servidores de autenticación RADIUS. Los siguientes parámetros son obligatorios:

    a) **Nombre**. Nombre del servidor RADIUS.

    b) **Nombre del servidor/ Dirección**IP . Nombre del servidor o dirección IP del servidor RADIUS.

c) **Puerto**. De forma predeterminada, el puerto 1812 se usa para la autenticación RADIUS. Si es necesario, puede especificar un número de puerto diferente.

d) **Tiempo de espera (segundos)**. Tiempo, en segundos, durante el que el sistema Citrix ADM espera una respuesta del servidor RADIUS.

e) **Clave**secreta . Cualquier expresión alfanumérica. Esta es la clave que comparten Citrix ADM y el servidor RADIUS para permitir la comunicación.

4. Haga clic en **Detalles** para expandir la sección y establecer los parámetros adicionales y, a continuación, haga clic en **Crear.**

Para obtener más información sobre cómo agregar servidores RADIUS, consulte [Cómo agregar servidores de autenticación RADIUS.] (/en-us/netscaler-application-delivery-management-software/12-1/authentication/authentication-how-to-articles/add-radius-authentication-server.html)

Configurar un servidor de autenticación LDAP

Puede configurar Citrix ADM para autenticar el acceso de los usuarios con uno o más servidores LDAP. La autorización LDAP requiere nombres de grupo idénticos en Active Directory, en el servidor LDAP y en Citrix ADM. Los caracteres y la caja también deben coincidir.

Para configurar un servidor de autenticación LDAP:

1. En NetScaler ADM, vaya a **Sistema** > **Autenticación** > **LDAP**.
2. En la página **LDAP**, haga clic en **Agregar**.
3. En la página **Crear servidor LDAP** , defina los parámetros y haga clic en **Crear** para agregar el servidor a la lista de servidores de autenticación LDAP. Los siguientes parámetros son obligatorios:

   a) **Nombre**. Nombre del servidor LDAP.

   b) **Nombre del servidor/ Dirección**IP . Nombre del servidor o dirección IP del servidor LDAP.

   c) **Tipo**de seguridad . Tipo de comunicación requerida entre el sistema y el servidor LDAP. Seleccione una opción de la lista desplegable. Si la comunicación de texto sin formato es inadecuada, puede elegir la comunicación cifrada seleccionando Transport Layer Security (TLS) o SSL.

   d) **Puerto**. De forma predeterminada, el puerto 389 se usa para la autenticación LDAP. Si es necesario, puede especificar un número de puerto diferente.

   e) **Tipo**de servidor . Seleccione **Active Directory (AD)** o **Novell Directory Service (NDS)** como tipo de servidor LDAP.

f) **Tiempo de espera (segundos).** Tiempo, en segundos, durante el cual el sistema Citrix ADM espera una respuesta del servidor LDAP.

Puede proporcionar detalles adicionales. También puede validar el certificado LDAP seleccionando la casilla **Validar certificado LDAP** y especificando el nombre de host que se va a introducir en el certificado . Algunos de los parámetros adicionales que puede agregar son los detalles del servidor de nombres de dominio (DN) para las consultas a un servicio de directorio, el grupo de autenticación predeterminado, los atributos de grupo y otros atributos.

El DN base normalmente se deriva del DN de Bind eliminando el nombre de usuario y especificando el grupo al que pertenecen los usuarios. En el cuadro de texto Administrator Bind DN, escriba el administrador Bind DN para las consultas al directorio LDAP.

Algunos ejemplos de sintaxis para el DN base son:

- ou=usuarios, dc=ace, dc=com
- CN=usuarios, dc=ace, dc=com

Algunos ejemplos de sintaxis para bind DN son:

- nombre de dominio/usuario
- ou=administrador, dc=ace, dc=com
- user@domain.name (para Active Directory)
- CN=administrador, CN=usuarios, dc=ace, dc=com

El nombre del grupo y el nombre de los usuarios que defina en Citrix ADM deben ser similares a los configurados en el servidor LDAP.

> **Nota**
>
> Al configurar un servidor RADIUS o LDAP, en la sección **Detalles** , puede introducir el nombre de un **grupo de autenticación predeterminado** . Este grupo predeterminado se elige para autorizar al usuario cuando la autenticación se realiza correctamente, independientemente de que el usuario esté vinculado a un grupo o no. A continuación, el usuario recibe una combinación de permisos configurados en este grupo predeterminado y en los demás grupos, independientemente de que el usuario esté asignado al grupo o no.

Para obtener más información sobre cómo agregar servidores LDAP, consulte Cómo agregar servidores de autenticación LDAP .

Para obtener más información sobre cómo conectar en cascada servidores de autenticación externos, consulte Cómo conectar en cascada servidores de autenticación externos .

Configurar un servidor de autenticación TACACS

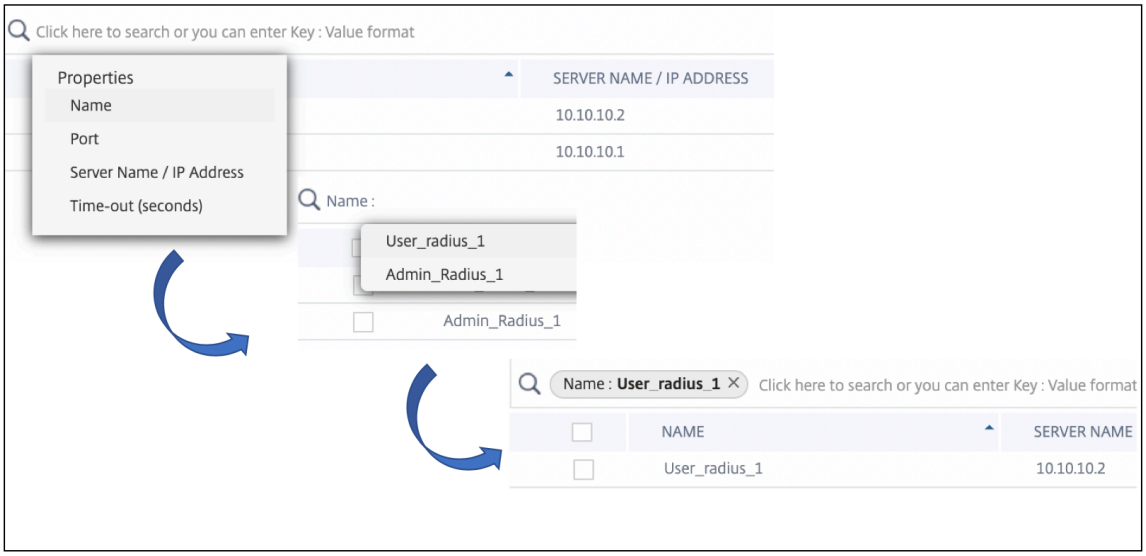
Los TACACS, al igual que RADIUS y LDAP, gestionan los servicios de autenticación remota para el acceso a la red.

Configure un servidor de autenticación TACACS:

1. En **Citrix ADM** , vaya a **Sistema** > **Autenticación** > **TACACS** .
2. En la página **TACACS** , haga clic en **Agregar** .
3. En la página **Crear servidor TACACS** , introduzca los siguientes detalles:
    a) Nombre del servidor TACACS
    b) Dirección IP del servidor TACACS
    c) Puerto y tiempo de espera (en segundos)
    d) La clave que comparten el sistema y el servidor TACACS para la comunicación.
    e) Seleccione Contabilidad si quiere que el dispositivo registre la información de auditoría con el servidor TACACS.
4. Haga clic en **Crear**.

Para obtener más información sobre cómo agregar servidores TACACS, consulte Cómo agregar servidores de autenticación TACACS .

> **Nota**
>
> Para buscar servidores de autenticación agregados a Citrix ADM, haga clic en la barra de búsqueda y seleccione los criterios de búsqueda necesarios.



Configurar una autenticación local de usuarios en Citrix ADM

Si utiliza la autenticación local, cree usuarios y, a continuación, agréguelos a los grupos que cree en Citrix ADM. Tras configurar usuarios y grupos, puede aplicar directivas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar la dirección IP de los recursos compartidos de archivos y los servidores a los que los usuarios tienen acceso.

Para configurar una autenticación local en Citrix ADM:

1. En Citrix ADM, vaya a **Sistema** > **Autenticación** y haga clic en **Configuración de autenticación** .
2. En la página **Configuración de autenticación** , seleccione **LOCAL** en el cuadro desplegable **Tipo de servidory** haga clic en Aceptar .

Configurar una autenticación externa en Citrix ADM

Al configurar servidores de autenticación externos en Citrix ADM, los grupos de usuarios que se autentican en esos servidores externos se importan a Citrix ADM. No es necesario crear usuarios en Citrix ADM. Los usuarios se administran en los servidores externos desde Citrix ADM. Sin embargo, debe asegurarse de que los niveles de permisos que tienen los grupos de usuarios en los servidores de autenticación externos se mantengan en Citrix ADM. Citrix ADM autoriza a los usuarios asignando permisos de grupo para acceder a servidores virtuales de equilibrio de carga específicos y a aplicaciones específicas del sistema. Si más adelante se quita un servidor de autenticación del sistema, los grupos y los usuarios se eliminarán automáticamente del sistema.

Para configurar una autenticación externa en Citrix ADM:

1. En Citrix ADM, vaya a **Sistema** > **Autenticación** y haga clic en **Configuración de autenticación** .
2. En la página **Configuración de autenticación** , seleccione **EXTERNO** en la lista desplegable **Tipo de servidor** .
3. Haga clic en **Insertar**.
4. En la página **Servidores externos** , seleccione un servidor de autenticación. Si lo desea, puede seleccionar varios servidores de autenticación para que se conecten en cascada.

   > **Nota**
   >
   > Solo los servidores externos se pueden conectar en cascada.

5. Seleccione **Habilitar la autenticación local** alternativa si desea que la autenticación local asuma el control si la autenticación externa falla.

6. Haga clic en **Aceptar** para cerrar la página.

   Los servidores seleccionados se muestran en la página **Servidores de autenticación** .

   También puede especificar el orden de autenticación mediante el icono situado junto a los nombres de servidor para mover los servidores hacia activo o hacia abajo en la lista.

Configurar grupos en Citrix ADM

NetScaler ADM le permite autenticar y autorizar a sus usuarios mediante la creación de grupos y la adición de usuarios a los grupos. Un grupo puede tener permisos de «administrador» o de «solo lectura» y todos los usuarios de ese grupo recibirán los mismos permisos.

En Citrix ADM, un grupo se define como un conjunto de usuarios que tienen permisos similares. Un grupo puede tener uno o varios roles. Un usuario se define como una entidad que puede tener acceso en función de los permisos asignados. Un usuario puede pertenecer a uno o más grupos.

Puede crear grupos locales en NetScaler ADM y utilizar la autenticación local para los usuarios de los grupos. Si utiliza servidores externos para la autenticación, configure los grupos en Citrix ADM para que coincidan con los grupos configurados en los servidores de autenticación de la red interna. Cuando un usuario inicia sesión y se autentica, si un nombre de grupo coincide con un grupo de un servidor de autenticación, el usuario hereda la configuración del grupo en NetScaler ADM.

Después de configurar los grupos, puede aplicar políticas de autorización y sesión, crear marcadores, especificar aplicaciones y especificar las direcciones IP de los servidores y recursos compartidos de archivos a los que el usuario tiene acceso.

Si utiliza la autenticación local, cree usuarios y agréguelos a los grupos configurados en Citrix ADM. A continuación, los usuarios heredan la configuración de esos grupos.

> **Nota**
>
> Si los usuarios son miembros de un grupo de Active Directory, el nombre del grupo y los nombres de los usuarios de Citrix ADM deben ser los mismos que en el grupo Active Directory.

Para configurar grupos de usuarios en Citrix ADM:

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > **Grupos**.
2. En la página **Grupos** , haga clic en **Agregar** para crear un grupo. De forma predeterminada, se crean dos grupos en Citrix ADM, con los permisos establecidos en administrador y de solo lectura. Puede agregar sus usuarios a estos grupos o puede crear otros grupos para sus usuarios.
3. En la pestaña **Configuración del grupo** de la página **Crear grupo del sistema** , escriba el nombre del grupo y defina los **roles** como de administrador o de solo lectura. Puede seleccionar **Configurar el tiempo de espera de la sesión de usuario** para establecer un límite de tiempo de espera para las sesiones de usuario que hayan iniciado sesión en ese grupo.

> **Nota**
>
> Asegúrese de que el nombre del grupo de usuarios creado en Citrix ADM sea el mismo que en los servidores de autenticación externos. De lo contrario, el sistema no reconocerá el grupo y los miembros del grupo no se incorporarán al sistema.

4. En la pestaña **Configuración de autorización** , seleccione los grupos necesarios. Haga clic en **Crear grupo**.
5. En la pestaña **Asignar usuarios** , seleccione los usuarios que desea agregar al grupo. Los usuarios se agregan a esta tabla cuando se configuran los usuarios en Configurar usuarios en Citrix ADM.
6. Haga clic en **Finalizar**.

Cuando termine de crear un grupo en el sistema, todos los usuarios del servidor de autenticación externo se extraerán al sistema. Si el nombre del grupo coincide con el nombre del grupo del servidor de autenticación externo, el usuario hereda todas las definiciones de autorización cuando inicia sesión en el sistema.

Configurar usuarios en Citrix ADM

Puede crear cuentas de usuario localmente en NetScaler ADM para complementar los usuarios de los servidores de autenticación. Por ejemplo, puede que quiera crear cuentas de usuario locales para usuarios temporales, como consultores o visitantes, sin crear una entrada para esos usuarios en el servidor de autenticación. Si está autenticando localmente a los usuarios que están presentes en servidores de autenticación externos, asegúrese de que los mismos usuarios estén presentes tanto en los servidores de autenticación como en Citrix ADM.

Para configurar usuarios en Citrix ADM:

1. En Citrix ADM, vaya a **Sistema** > **Administración** de **usuarios > Usuarios**.
2. En la página **Usuarios** , haga clic en **Agregar** para agregar usuarios a Citrix ADM.
3. En la página **Crear usuario del sistema** , defina los siguientes parámetros:
    a) **Nombre de usuario**. Nombre del usuario
    b) **Contraseña**. Contraseña que utilizará el usuario para iniciar sesión en Citrix ADM
    c) **Habilite la autenticación**externa . Si no está habilitada, el usuario se autenticará como usuario local.
    d) **Configure el tiempo de espera de la sesión de**usuario . Tiempo durante el cual un usuario puede permanecer activo. Este período de tiempo se puede configurar en minutos u horas.

4. En la tabla **Grupos** , seleccione el grupo al que desea añadir el usuario. Los miembros del grupo se agregan a esta tabla al configurar los grupos en Configuración de grupos de usuarios en Citrix ADM.
5. Haga clic en **Crear**.

> **Nota**
>
> Si los usuarios están en Active Directory, asegúrese de que el nombre del grupo en Citrix ADM sea el mismo que el del grupo Active Directory en el servidor externo.

Cómo extraer un grupo de servidores de autenticación

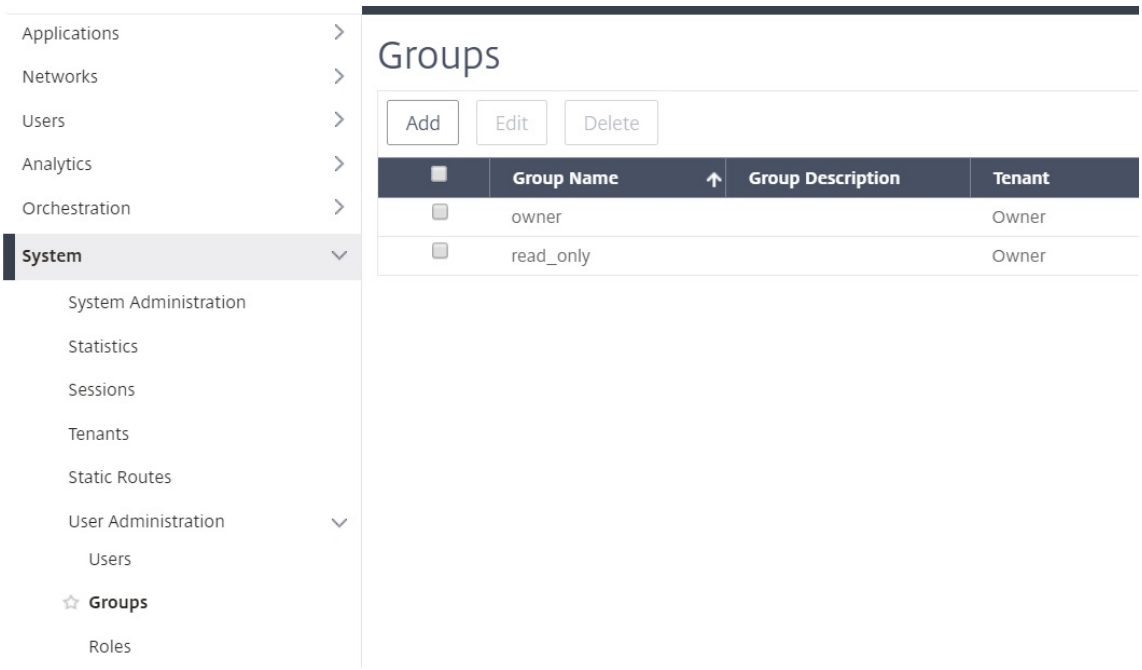
January 30, 2024

Citrix Application Delivery Management (ADM) le permite extraer el grupo de usuarios existente en el servidor de autenticación externo y asignarles permisos según lo exija su función y según las definiciones de Citrix ADC. Esto tiene dos ventajas:

1. No es necesario crear usuarios en Citrix ADM. Aunque los grupos se extraen al servidor Citrix ADM, se administran en los servidores externos desde Citrix ADM en lugar de agregarlos al sistema.
2. Citrix ADM realiza la autorización de los usuarios asignando permisos de grupo para acceder a servidores virtuales del equilibrador de carga específicos y para aplicaciones específicas del sistema. En el futuro, cuando el servidor de autenticación en particular se elimine del sistema, los grupos y usuarios se eliminarán automáticamente del sistema.

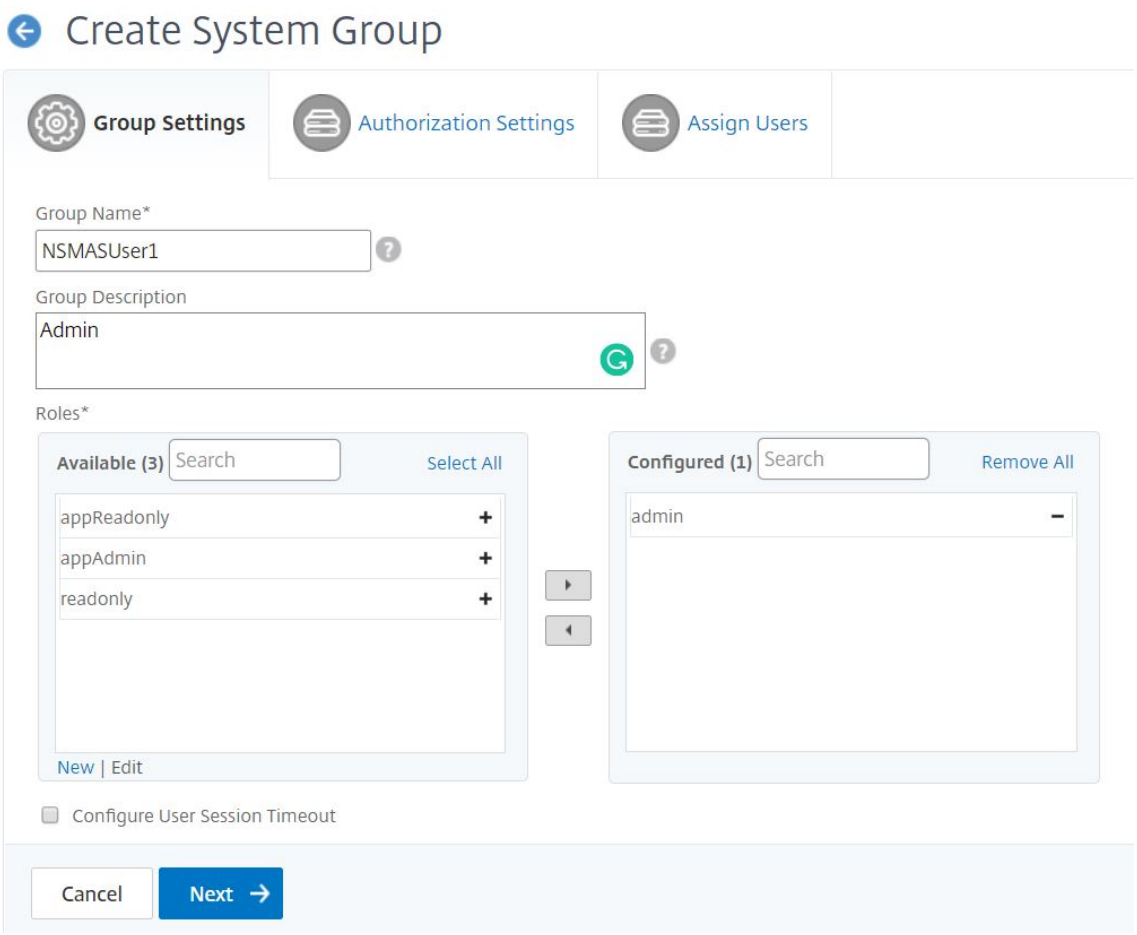
Configuración de grupos y asignación de permisos a grupos

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > **Grupos**.
2. Haga clic en **Agregar** para crear un grupo.



3. En la ficha **Configuración del grupo**, escriba el nombre del grupo y defina los permisos como admin, readonly, appReadOnly o AppAdmin. Las otras opciones que puede configurar son el tiempo de espera de la sesión, donde puede establecer un límite de tiempo de espera para las sesiones registradas en los usuarios de ese grupo, y también puede configurar las instancias de VM a las que pueden acceder los miembros del grupo.

> **Nota**
>
> Asegúrese de que el nombre del grupo de usuarios creado en Citrix ADM sea exactamente el mismo que el creado en los servidores de autenticación externos. De lo contrario, el sistema no reconocerá el grupo y los miembros del grupo no se extraerán al sistema.



4. En la ficha **Configuración de autorización**, puede proporcionar la configuración de autorización para los cuatro grupos siguientes:

   - Instancias
   - Aplicaciones
   - Plantillas de configuración
   - StyleBooks

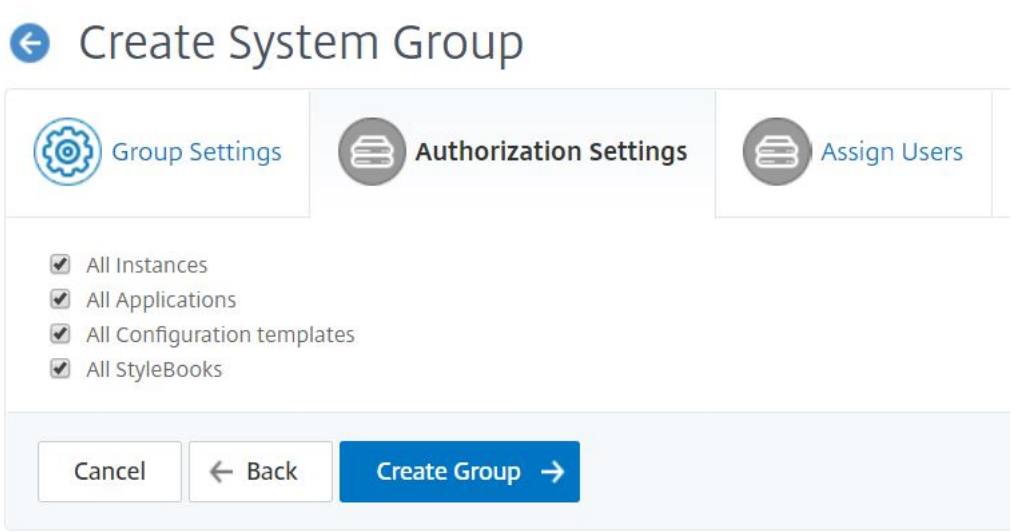
De forma predeterminada, el usuario puede acceder a todos los grupos anteriores. Puede desactivar las casillas de verificación y proporcionar acceso selectivo a cada uno de estos grupos.

Por ejemplo:

- Puede desactivar la casilla de verificación**Instancias** y seleccionar solo las instancias necesarias a las que desee proporcionar acceso a sus usuarios.
- Desactive la casilla**Todas las aplicaciones** y seleccione solo las aplicaciones y plantillas necesarias. Al agregar aplicaciones a un grupo en Citrix ADM, puede utilizar expresiones regulares para buscar y agregar las aplicaciones que cumplen los criterios de expresiones regulares de

los grupos. Los usuarios que están vinculados a estos grupos solo pueden acceder a esas aplicaciones específicas. La expresión regular especificada se conserva en Citrix ADM. Es decir, Citrix ADM permite almacenar en el sistema la expresión regular proporcionada en el cuadro de texto**Agregar expresión regular**y actualiza dinámicamente el alcance de la autorización siempre que las nuevas aplicaciones cumplan con esta expresión regular. Cuando se agregan nuevas aplicaciones al sistema, Citrix ADM aplica los criterios de búsqueda a las nuevas aplicaciones y la aplicación que cumple los criterios se agrega dinámicamente al grupo. No es necesario que agregue manualmente las nuevas aplicaciones al grupo. Las aplicaciones se actualizan dinámicamente en el sistema y los usuarios del grupo respectivo pueden ver las aplicaciones en los módulos correspondientes de Citrix ADM.

- Desactive la casilla de verificación**Todas las plantillas de configuración**para permitir el acceso únicamente a las plantillas necesarias.
- Desactive la casilla**Todos losStyleBooks** y seleccione los StyleBooks necesarios a los que pueda acceder el usuario.
- Puede seleccionar los StyleBooks necesarios cuando cree grupos y agregue usuarios a ese grupo. Cuando el usuario selecciona el StyleBook permitido, también se seleccionan todos los StyleBooks dependientes. Los paquetes de configuración de ese StyleBook también se incluyen en lo que el usuario tiene acceso.



Al terminar de crear un grupo en el sistema, todos los usuarios del servidor de autenticación externo se extraen al sistema. Puede comprobarlo seleccionando el grupo y haciendo clic en **Modificar**. La tabla Usuarios de Crear grupo de sistemas muestra la lista de usuarios conectados al grupo. También puede asignar usuarios al grupo en la ficha**Asignar usuarios**.

Si el nombre del grupo coincide con el nombre del grupo en el servidor de autenticación externo, el

usuario hereda todas las definiciones de autorización al iniciar sesión en el sistema.

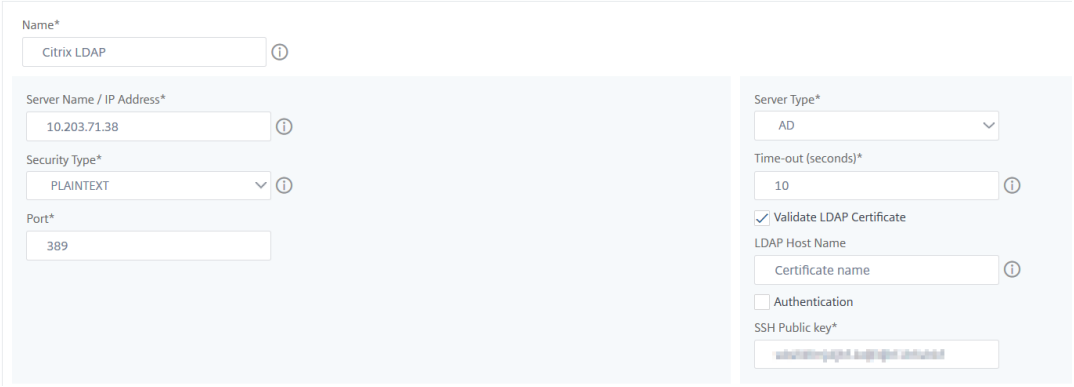
Agregar servidor de autenticación LDAP

January 30, 2024

Al integrar el protocolo LDAP con los servidores de autenticación RADIUS y TACAS, puede utilizar Citrix ADM para buscar y autenticar las credenciales de usuario en los directorios distribuidos.

1. Vaya a **Sistema** > **Autenticación**.
2. Seleccione la ficha **LDAP** y, a continuación, haga clic en **Agregar**.
3. En la página **Crear servidor LDAP**, especifique los siguientes parámetros:
    a) **Nombre**: Especifique el nombre del servidor LDAP
    b) **Nombre del servidor/dirección IP**: Especifique la dirección IP LDAP o el nombre del servidor
    c) **Tipo de seguridad**: Tipo de comunicación requerida entre el sistema y el servidor LDAP. Seleccione una opción de la lista. Si la comunicación en texto plano no es adecuada, puede elegir la comunicación cifrada seleccionando Transport Layer Security (TLS) o SSL
    d) **Puerto**: De forma predeterminada, el puerto 389 se utiliza para PLAINTEXT. También puede especificar el puerto 636 para SSL/TSL
    e) **Tipo de servidor**: Seleccione Active Directory (AD) o Novell Directory Service (NDS) como el tipo de servidor LDAP
    f) Tiempo de**espera (segundos)**: tiempo en segundos durante el que el sistema Citrix ADM espera una respuesta del servidor LDAP
    g) **Nombre de host LDAP: active** la casilla Validar certificado LDAP y especifique el nombre de host que se introducirá en el certificado.

    Desactive la opción **Autenticación** y especifique la clave pública SSH. Con la autenticación basada en claves, puede obtener la lista de claves públicas almacenadas en el objeto de usuario. Estas claves públicas se almacenan en el servidor LDAP a través de SSH.



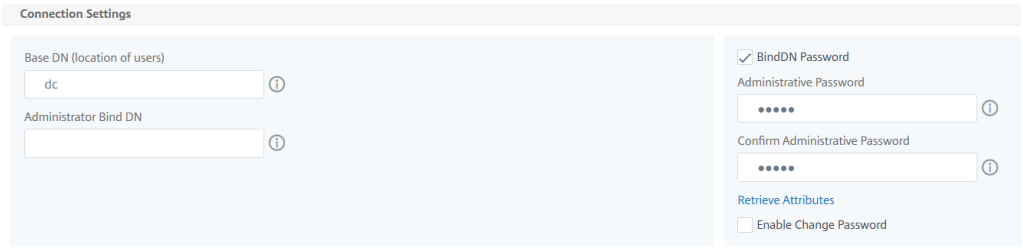
En Configuración de conexión, especifique los siguientes parámetros:

i. **Base DN**: El nodo base para que el servidor LDAP inicie la búsqueda

ii. **Administrator Bind DN**: Nombre de usuario al que se vincula al servidor LDAP. Por ejemplo, admin@aaa.local.

iii. **Contraseña de enlace de DN**: seleccione esta opción para proporcionar una contraseña de autenticación.

iv. **Habilitar cambio de contraseña**: Seleccione esta opción para habilitar el cambio de contraseña



En **Otros ajustes**, especifique los siguientes parámetros

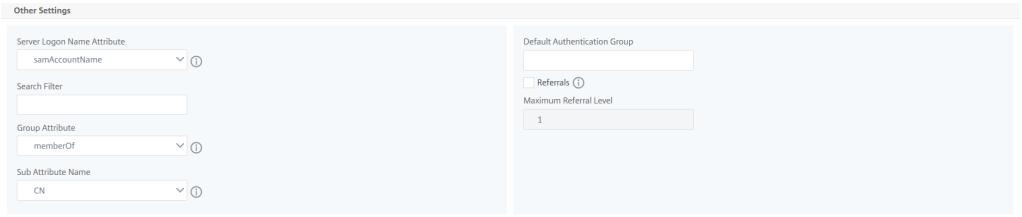
i. **Atributo de nombre de inicio de sesión del servidor**: Atributo de nombre que utiliza el sistema para consultar el servidor LDAP externo o un Active Directory. Seleccione **samAccountname** de la lista.

ii. **Filtro de búsqueda**: Configure usuarios externos para la autenticación de dos factores según el filtro de búsqueda configurado en el servidor LDAP. Por ejemplo, vpnallowed=true con ldaploginame samaccount y el nombre de usuario bob proporcionado por el usuario generaría una cadena de búsqueda LDAP de:. `&(vpnallowed=true)(samaccount=bob)`

iii. **Atributo de grupo**: Seleccione memberOf de la lista.

iv. **Nombre de subatributo**: El nombre del subatributo para la extracción de grupos del servidor LDAP.

v. **Grupo de autenticación predeterminado**: Grupo predeterminado para elegir cuando la autenticación se realiza correctamente, además de los grupos extraídos.



4. Haga clic en **Crear**.

   El servidor LDAP ya está configurado.

   > Nota
   >
   > Si los usuarios son miembros del grupo de Active Directory, el grupo y los nombres de los usuarios de Citrix ADM deben tener los mismos nombres de los miembros del grupo de Active Directory.

Cómo habilitar la autenticación local de reserva

January 30, 2024

La función de autenticación local alternativa permite que la autenticación local asuma el control si la autenticación externa falla. Un usuario configurado tanto en Citrix Application Delivery Management (ADM) como en un servidor de autenticación externo puede iniciar sesión en Citrix ADM, aunque el servidor de autenticación externo configurado esté inactivo o inaccesible. Para que la autenticación local alternativa funcione, asegúrese de tener en cuenta estos tres factores:

- Debería poder acceder a Citrix ADM incluso después de que el servidor de autenticación externo deje de funcionar.
- Debe estar configurado tanto en Citrix ADM como en el servidor de autenticación externo.
- Debe agregar al menos un servidor externo.

Para habilitar la autenticación local alternativa, haga lo siguiente:

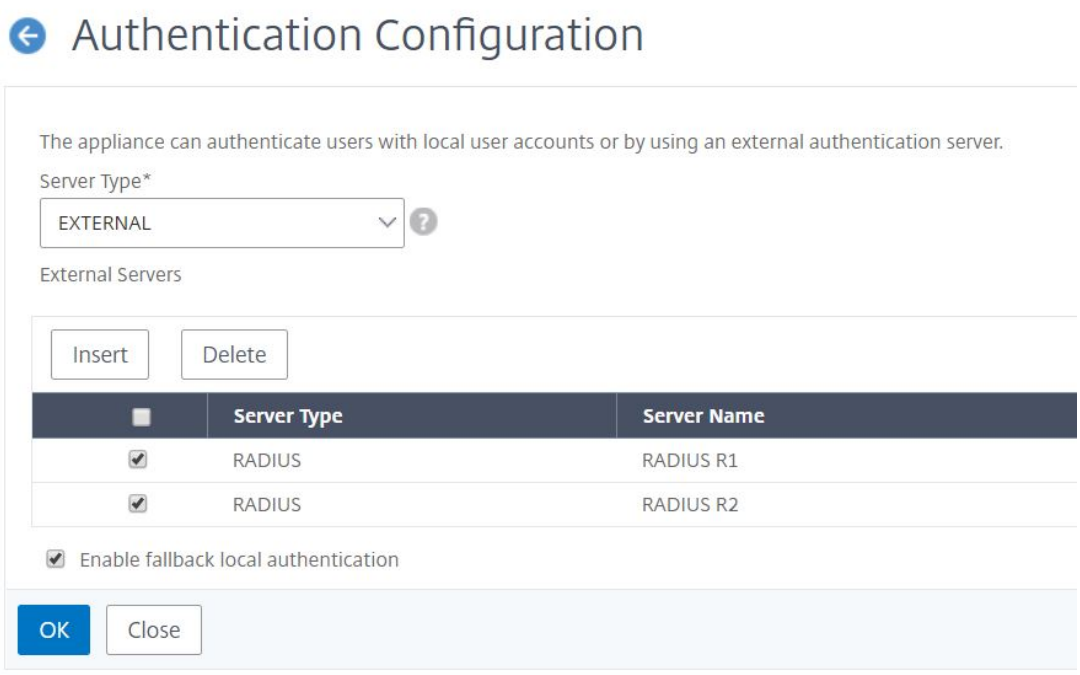
1. En Citrix ADM, vaya a **Sistema** > **Autenticación** y haga clic en **Configuración de autenticación** .
2. Seleccione **EXTERNO** en la lista de tipos de servidor.

> **Nota**: Si selecciona **LOCAL** en la lista, la autenticación de los usuarios se realiza en el servidor de autenticación local predeterminado.

3. Haga clic en **Insertar,** seleccione un servidor externo de la lista de servidores externos que se muestra **y** haga clic en Aceptar para agregar el servidor externo.

> **Nota**: Ya debería haber agregado los servidores externos antes de este paso para que aparezcan en la lista. Para obtener más información sobre cómo agregar servidores externos, consulte los siguientes artículos:
>
> - Cómo agregar servidores Radius
> - Cómo agregar servidores LDAP
> - Cómo agregar servidores TACACS

4. Seleccione la opción **Habilitar la autenticación local** alternativa.



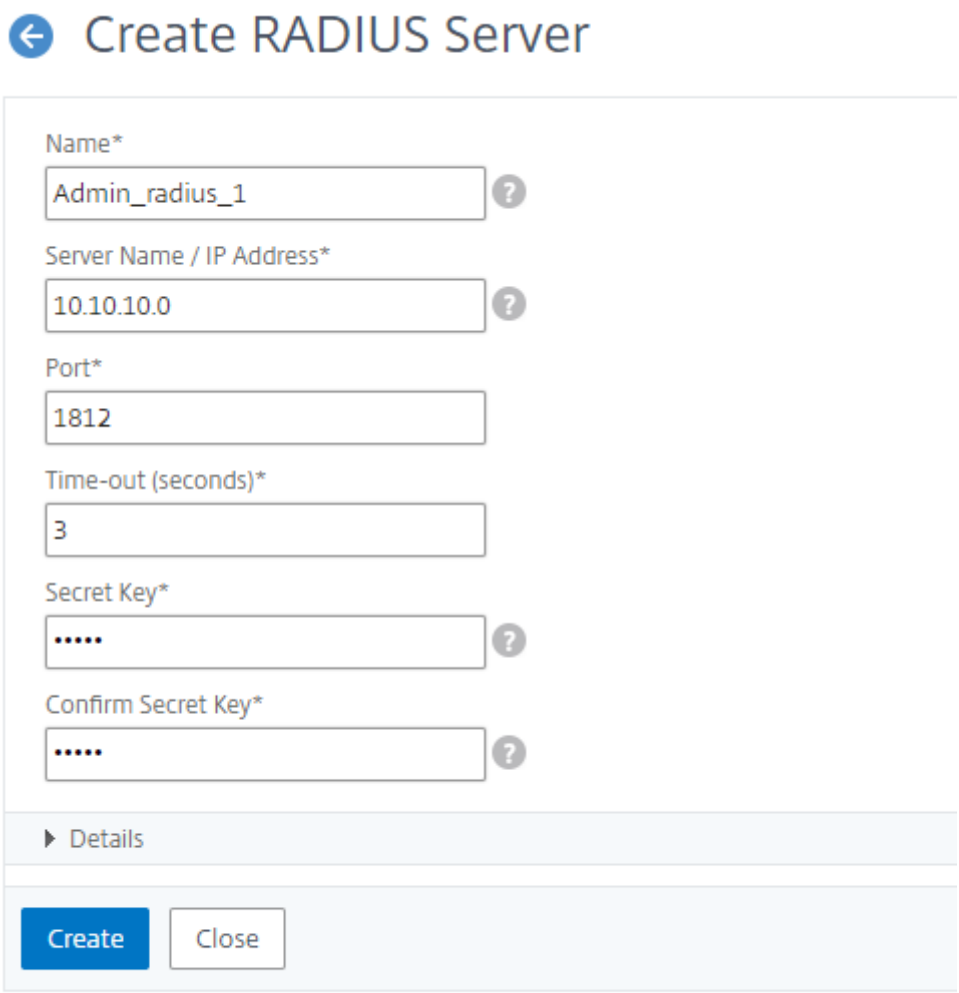
Cómo agregar servidores de autenticación RADIUS

January 30, 2024

Un servidor de autenticación RADIUS funciona mediante el Protocolo de datagramas de usuario (UDP). El servidor RADIUS recibe la solicitud de conexión de un usuario y autentica al usuario. A continuación, el servidor devuelve la información de configuración al sistema que presta los servicios al usuario. El servidor RADIUS está conectado a un servidor de acceso a la red (NAS). Cuando el NAS envía una solicitud de acceso, el servidor RADIUS busca en su base de datos el nombre de usuario y otros detalles. Si el nombre de usuario no existe en la base de datos, el servidor RADIUS envía inmediatamente un mensaje de rechazo de acceso o puede cargar un perfil predeterminado en Citrix ADM. En RADIUS, la autenticación y la autorización se combinan. Si se autentican los detalles del usuario, el servidor RADIUS devuelve una respuesta de aceptación de acceso. También envía una lista de pares atributo-valor que describen los parámetros que se utilizarán para esa sesión en particular.

Configuración de un servidor de autenticación RADIUS

1. En NetScaler ADM, vaya a **Sistema** > **Autenticación** > **RADIUS**.
2. En la página **RADIUS**, haga clic en **Agregar**.
3. En la página **Crear servidor RADIUS** , defina los parámetros y haga clic en **Crear** para agregar el servidor a la lista de servidores de autenticación RADIUS.
4. Los siguientes parámetros son obligatorios para crear el servidor RADIUS:
    - **Nombre**: escriba el nombre del servidor RADIUS
    - **Nombre del servidor/dirección**IP : escriba el nombre del servidor o la dirección IP del servidor RADIUS
    - **Puerto**: de forma predeterminada, el puerto 1812 se usa para los mensajes de autenticación RADIUS. Si es necesario, puede especificar un número de puerto diferente.
    - **Tiempo de espera (segundos)**: escriba el número de segundos. El tiempo que el sistema Citrix ADM espera una respuesta del servidor RADIUS.
    - **Clave**secreta : escriba cualquier expresión alfanumérica. La clave que se comparte entre Citrix ADM y el servidor RADIUS para la comunicación.
5. Haga clic en **Detalles** para expandir la sección y establecer los parámetros adicionales.

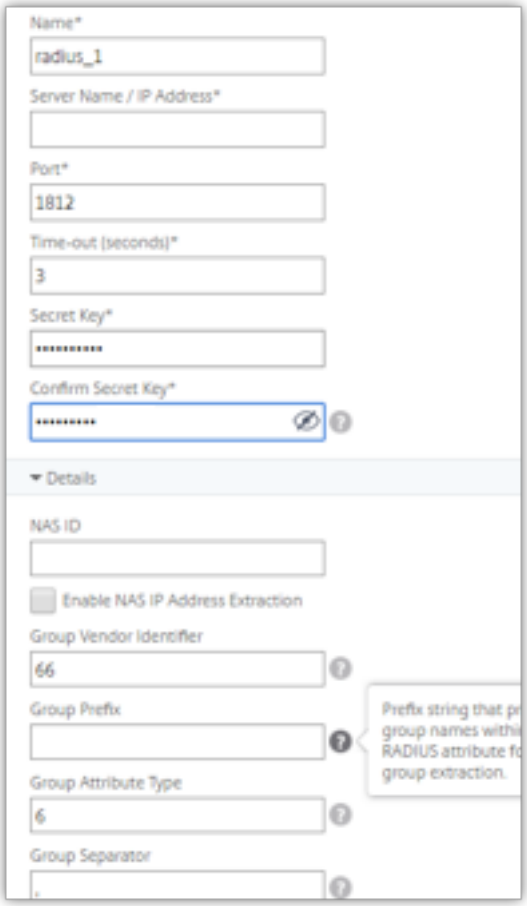


Puede proporcionar más detalles opcionales al agregar un servidor RADIUS. Algunos de los parámetros adicionales que puede introducir son los detalles del NAS, la información del proveedor, la información de los atributos y el tipo de autenticación con contraseña.

> **Nota**
>
> Para que la autenticación RADIUS funcione, asegúrese de que el grupo configurado en Citrix ADM y el grupo extraído mediante el usuario RADIUS sean el mismo. El usuario está autorizado en función de los permisos asignados al grupo.
>
> Por ejemplo, consideremos un escenario en el servidor FreeRADIUS, donde,
>
> - Cleartext-Password = «1.citrix»
> - Nombres de grupo = «radiusgroup1, group1”

En este caso, el usuario pertenece a dos grupos: radiusgroup1 y group1. El separador de grupos en este caso es «,»

. Si inicia sesión en Citrix ADM como un usuario RADIUS «RadiusUser1"que pertenece al grupo «radiusgroup1», asegúrese de que el mismo nombre de grupo «radiusgroup1» esté configurado también en Citrix ADM.



Proporcione los detalles relacionados con el ID del proveedor, el tipo de atributo y el separador de grupos (si corresponde) para que la extracción del grupo se lleve a cabo, como se muestra en la siguiente imagen.

```
#
# Created for Citrix Use

# currently only using attribute 6 in this setup.

VENDOR Citrix 66


BEGIN-VENDOR Citrix
ATTRIBUTE Group-Names 6 string
END-VENDOR Citrix
```

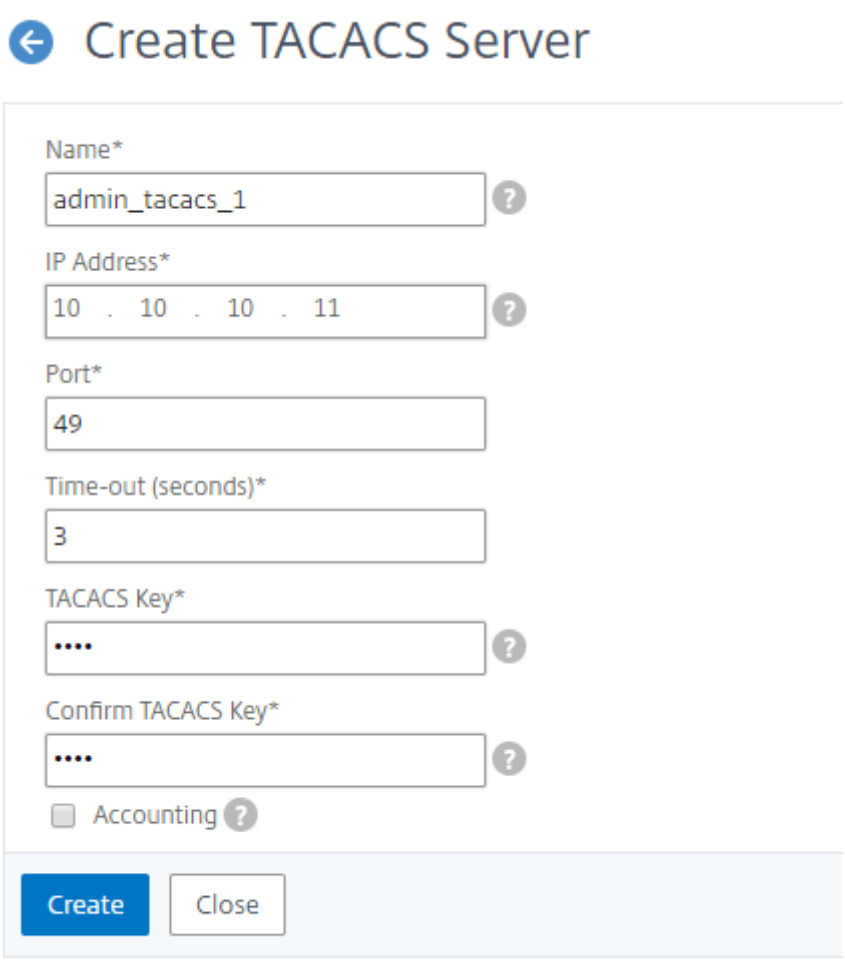

Cómo agregar servidores de autenticación TACACS

January 30, 2024

TACACS, junto con RADIUS y LDAP, gestiona los servicios de autenticación remota para el acceso a la red.

Configuración de un servidor de autenticación TACACS

1. En **Citrix ADM**, vaya a **Sistema** > **Autenticación** > **TACACS**.
2. En la página **TACACS** , haga clic en **Agregar** .
3. En la página **Crear servidor TACACS** , introduzca los siguientes detalles:
    a) Nombre del servidor TACACS
    b) Dirección IP del servidor TACACS
    c) Puerto y tiempo de espera en segundos
    d) Escriba la clave que comparten el sistema y el servidor TACACS para la comunicación.
4. Seleccione **Contabilidad** si desea que el dispositivo registre la información de auditoría en el servidor TACACS.
5. Haga clic en **Crear**.



Cómo conectar en cascada servidores de autenticación externos

January 30, 2024

Un Citrix Application Delivery Management (ADM) admite un sistema unificado de protocolos de autenticación, autorización y contabilidad (AAA), que incluye RADIUS, LDAP y TACACS, además de admitir servidores locales para autenticar usuarios y grupos locales. El soporte unificado proporciona una interfaz común para autenticar y autorizar a todos los clientes AAA locales y externos que acceden al sistema. Citrix ADM puede autenticar a los usuarios independientemente de los protocolos reales que se comuniquen con el sistema.

Los servidores de autenticación externa en cascada proporcionan un proceso continuo y sin fallos para autenticar y autorizar a los usuarios externos. Si la autenticación falla en el primer servidor de

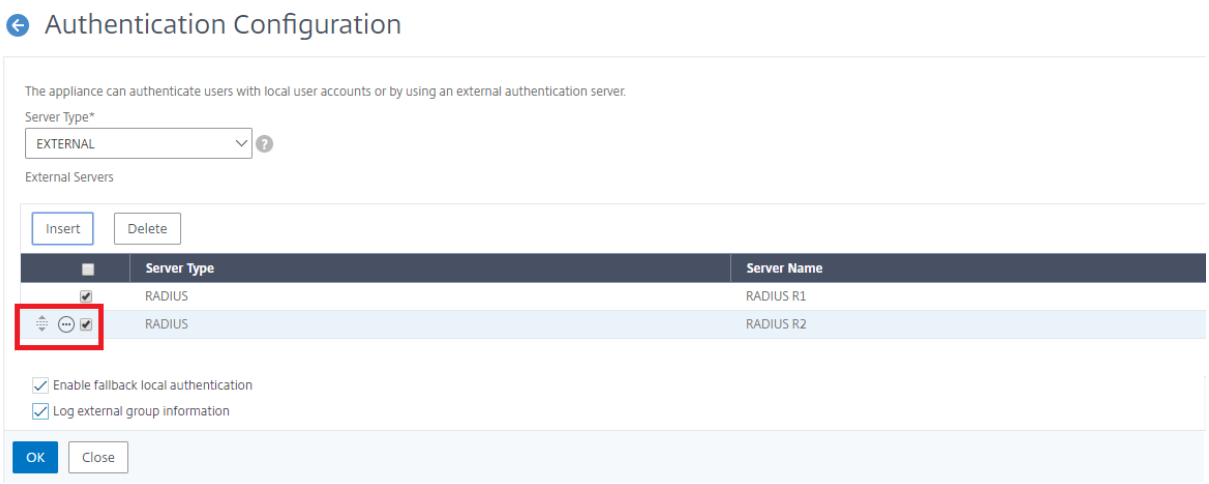
autenticación, Citrix ADM intenta autenticar al usuario mediante el segundo servidor de autenticación externo, etc. Para habilitar la autenticación en cascada, debe agregar los servidores de autenticación externos a Citrix ADM. Puede agregar cualquier tipo de servidores de autenticación externos compatibles (RADIUS, LDAP y TACACS). Por ejemplo, si desea agregar cuatro servidores de autenticación externos para la autenticación en cascada, puede agregar dos servidores RADIUS, un servidor LDAP y un servidor TACACS, o todos los servidores pueden ser de tipo RADIUS. Puede configurar hasta 32 servidores de autenticación externos en Citrix ADM.

Configuración de servidores de autenticación externos en cascada

1. En Citrix ADM, vaya a **Sistema** > **Autenticación**.
2. En la página de **autenticación** , haga clic en **Configuración de autenticación** .
3. En la página **Configuración de autenticación** , seleccione **EXTERNO** en la lista desplegable **Tipo de servidor** (solo los servidores externos se pueden conectar en cascada).
4. Haga clic en **Insertar** y, en la página **Servidores externos** , seleccione uno o varios servidores de autenticación que desee conectar en cascada.
5. Seleccione **Habilitar la autenticación local** alternativa si desea que la autenticación local asuma el control si la autenticación externa falla.
6. Haga clic en **Aceptar** para cerrar la página.

Los servidores seleccionados se muestran en Servidores externos, como se muestra en la siguiente figura.

También puede especificar el orden de autenticación mediante el icono situado junto a los nombres de los servidores para moverlos hacia arriba o hacia abajo en la lista.



Control de acceso

January 30, 2024

La autenticación es un proceso mediante el cual se verifica que alguien es quien afirma ser. Para realizar la autenticación, el usuario ya debe tener una cuenta creada en un sistema que pueda ser interrogada por el mecanismo de autenticación, o se debe crear una cuenta como parte del proceso de la primera autenticación. NetScaler Application Delivery Management (ADM) proporciona un método para autenticar usuarios locales y externos. Si bien los usuarios locales se autentican internamente, Citrix ADM admite la autenticación externa mediante los protocolos RADIUS, LDAP y TACACS. Cuando un usuario intenta acceder a NetScaler ADM configurado para autenticación externa, el servidor de aplicaciones solicitado envía el nombre de usuario y la contraseña al servidor RADIUS, LDAP o TACACS para la autenticación. Una vez autenticado, se utiliza el protocolo necesario para identificar al usuario en Citrix ADM.

El control de acceso es el proceso de aplicar la seguridad requerida para un recurso en particular. Es una técnica de seguridad que se puede utilizar para regular quién puede ver o utilizar los recursos en un entorno informático. El objetivo del control de acceso es limitar las acciones u operaciones que un usuario legítimo de un sistema informático puede realizar. El control de acceso restringe lo que un usuario puede hacer directamente, así como lo que pueden hacer los programas que se ejecutan en nombre de los usuarios. De esta manera, el control de acceso busca evitar actividades que puedan conducir a una violación de la seguridad. El control de acceso supone que la autenticación del usuario se ha verificado correctamente antes de la aplicación del control de acceso a través de un monitor de referencia. Citrix ADM permite un control de acceso detallado y basado en roles (RBAC) mediante el cual los administradores pueden proporcionar permisos de acceso a los usuarios en función de las funciones de los usuarios individuales dentro de una empresa. El RBAC en Citrix ADM se logra mediante la creación de políticas de acceso, funciones, grupos y usuarios.

Control de acceso por roles

January 30, 2024

Citrix Application Delivery Management (ADM) proporciona un control de acceso detallado basado en funciones (RBAC) con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales de la empresa. En este contexto, el acceso es la capacidad de realizar una tarea específica, como ver, crear, modificar o eliminar un archivo. Los roles se definen de acuerdo con la autoridad y responsabilidad de los usuarios dentro de la empresa. Por ejemplo, es posible que un usuario pueda realizar todas las operaciones de red, mientras que otro usuario puede observar el flujo de tráfico en las aplicaciones y ayudar a crear plantillas de configuración.

Los roles están determinados por las directivas. Después de crear las directivas, se crean las funciones, se vinculan las funciones a una o más directivas y se asignan las funciones a los usuarios. También puede asignar roles a grupos de usuarios.

Un grupo es un conjunto de usuarios que tienen permisos en común. Por ejemplo, los usuarios que administran un centro de datos concreto se pueden asignar a un grupo. Un rol es una identidad que se otorga a usuarios o grupos en función de condiciones específicas. En Citrix ADM, la creación de funciones y políticas es específica de la función RBAC de Citrix ADC. Los roles y las directivas se pueden crear, cambiar o interrumpir fácilmente a medida que evolucionan las necesidades de la empresa, sin tener que actualizar individualmente los privilegios de cada usuario.

Los roles pueden estar basados en funciones o en recursos. Por ejemplo, considere un administrador SSL/Security y un administrador de aplicaciones. Un administrador de SSL/Security debe tener acceso completo a las funciones de supervisión y administración de certificados SSL, pero debe tener acceso de solo lectura para las operaciones de administración del sistema. El administrador de la aplicación debe poder acceder solo a los recursos que estén dentro de su ámbito.

Ejemplo:

Chris, el jefe del grupo ADC, es el superadministrador de NetScaler ADM en su organización. Crea tres funciones de administrador: Administrador de seguridad, administrador de aplicaciones y administrador de red.

David, el administrador de seguridad, debe tener acceso completo para la administración y supervisión de certificados SSL, pero debe tener acceso de solo lectura para las operaciones de administración del sistema.

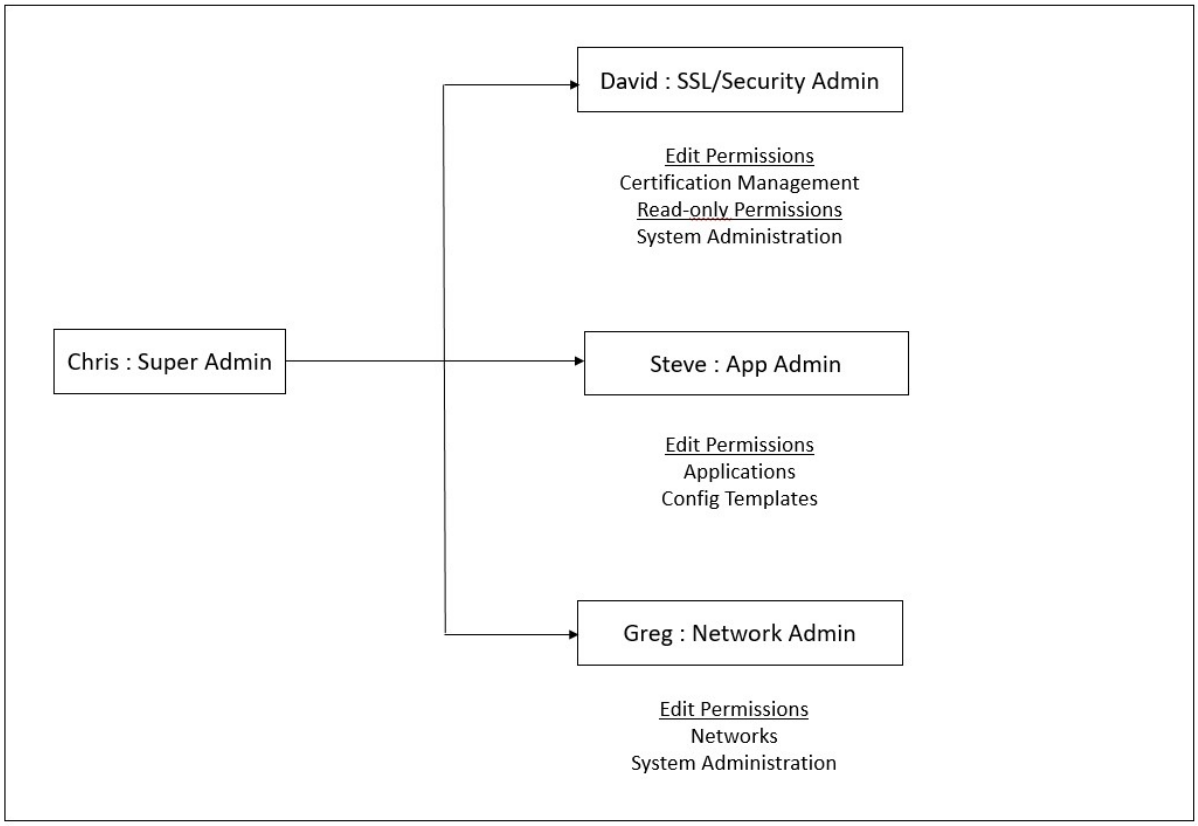
Steve, un administrador de aplicaciones, necesita acceso solo a aplicaciones específicas y a plantillas de configuración específicas.

Greg, un administrador de red, necesita acceso a la administración de sistemas y redes.

Chris también debe proporcionar RBAC a todos los usuarios, independientemente de que sean locales, externos o multiusuario.

Los usuarios de NetScaler ADM pueden estar autenticados localmente o autenticados a través de un servidor externo (RADIUS/LDAP/TACACS). La configuración de RBAC debe ser aplicable a todos los usuarios independientemente del método de autenticación adoptado.

La imagen siguiente muestra los permisos que tienen los administradores y otros usuarios y sus roles en la organización.



Limitaciones

El RBAC no es totalmente compatible con las siguientes funciones de Citrix ADM:

- **Analytics**: RBAC no es totalmente compatible con los módulos de análisis. La compatibilidad con RBAC se limita al nivel de instancia y no es aplicable a nivel de aplicación en los módulos de análisis Web Insight, SSL Insight, Gateway Insight, HDX Insight y Security Insight. Por ejemplo:

Ejemplo 1: RBAC basado en instancias (compatible)

Un administrador al que se le hayan asignado algunas instancias solo puede ver esas instancias en **Web Insight** > **Instancias**y solo los servidores virtuales correspondientes en **Web Insight** > **Aplicaciones**, ya que el RBAC es compatible a nivel de instancia.

Ejemplo 2: RBAC basado en aplicaciones (no compatible)

Un administrador al que se le hayan asignado algunas aplicaciones puede ver todos los servidores virtuales en **Web Insight** > **Aplicaciones**, pero no puede acceder a ellos porque el RBAC no se admite a nivel de aplicaciones.

- **StyleBooks**: RBAC no es totalmente compatible con StyleBooks.

  - En Citrix ADM, los Stylebooks y los paquetes de configuración se consideran recursos independientes. Los permisos de acceso, ya sea para ver, editar o ambos, para Stylebook y los paquetes de configuración se pueden proporcionar por separado o simultáneamente. Un permiso de visualización o edición en los paquetes de configuración permite implícitamente al usuario ver los StyleBooks, lo cual es esencial para obtener los detalles del paquete de configuración y crear nuevos paquetes de configuración.
  - No se admite el permiso de acceso para paquetes de configuración o Stylebook específicos. Ejemplo: Si ya hay un paquete de configuración en la instancia, los usuarios pueden modificar la configuración en una instancia de Citrix ADC de destino incluso si no tienen acceso a esa instancia.

- **Orquestación**: RBAC no es compatible con Orchestration.

Configurar directivas de acceso

January 30, 2024

Las directivas de acceso definen los permisos. Se puede aplicar una directiva a un solo usuario o grupo, o a varios usuarios y grupos. Citrix Application Delivery Management (ADM) proporciona cuatro directivas de acceso predefinidas:

1. **adminpolicy**. Concede acceso a todas las funciones de Citrix ADM. El usuario tiene permisos de visualización y edición, puede ver todo el contenido de Citrix ADM y puede realizar todas las operaciones de edición. Es decir, el usuario puede realizar operaciones de adición, modificación y eliminación en los recursos.
2. **readonlypolicy**. Otorga permisos de solo lectura. El usuario puede ver todo el contenido de Citrix ADM, pero no está autorizado a realizar ninguna operación.
3. **appAdminPolicy**. Otorga permisos administrativos para acceder a las funciones de la aplicación en Citrix ADM. Un usuario sujeto a esta directiva puede agregar, modificar y eliminar aplicaciones personalizadas y puede habilitar o inhabilitar los servicios, los grupos de servicios y los distintos servidores virtuales, como la conmutación de contenido, la redirección de caché y los servidores virtuales HAProxy.
4. **appReadOnlyPolicy**. Otorga permisos de solo lectura para las funciones de la aplicación. Un usuario vinculado a esta directiva puede ver las aplicaciones, pero no puede realizar ninguna operación de adición, modificación, eliminación, activación o desactivación.

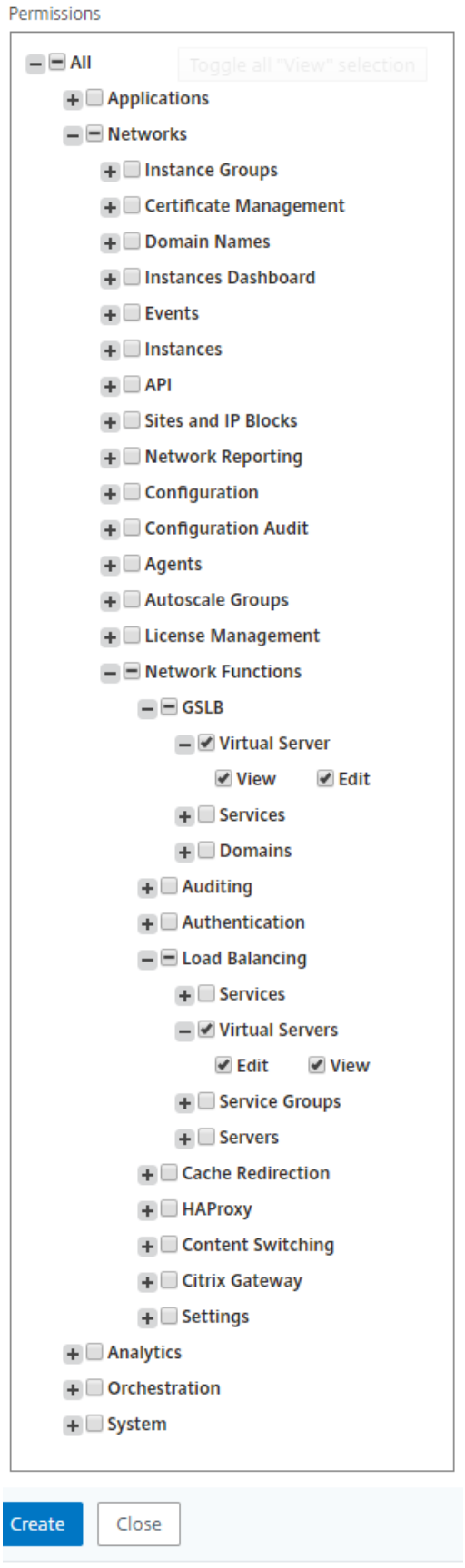
> **Nota:** Las directivas predefinidas no se pueden modificar.

También puede crear sus propias directivas (definidas por el usuario).

Para crear directivas de acceso definidas por el usuario:

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > Directivas de **acceso**.
2. Haga clic en **Agregar**.
3. En el campo **Nombre de la directiva**, introduzca el nombre de la directiva e introduzca la descripción en el campo **Descripción de la directiva**.
4. La sección **Permisos** muestra todas las funciones de Citrix ADM, con opciones para especificar el acceso de solo lectura o edición. Haga clic en el icono (+) para expandir cada grupo de entidades en varias entidades. Debe seleccionar la casilla de verificación situada junto al nombre de la función para conceder a los usuarios los permisos de visualización o edición. La opción Editar incluye el permiso para ver. Selecciona **Ver** para solo lectura o **Editar** para tener acceso completo.

   > **Nota**: Amplíe el equilibrio de carga y GSLB para ver más opciones de configuración.

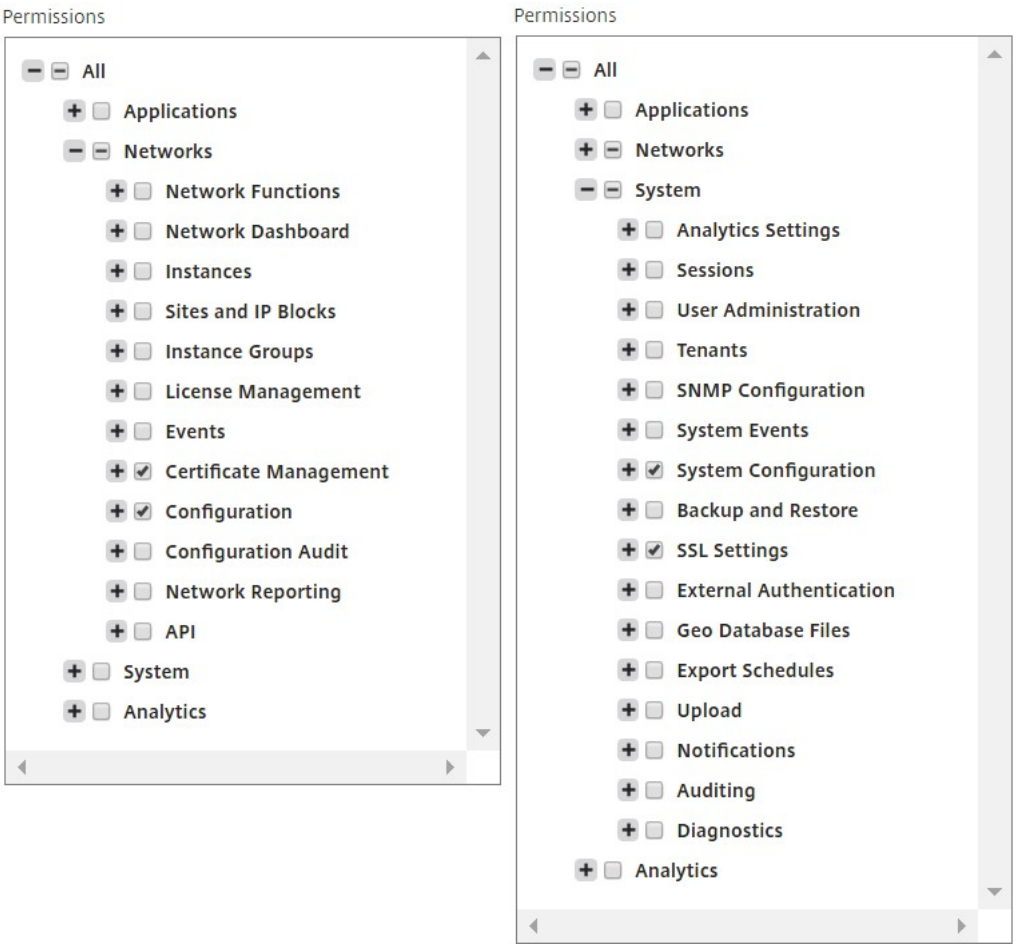


> **Nota**Al seleccionar **Editar** , es posible que se asignen internamente permisos dependientes que no se muestran como habilitados en la sección **Permisos** . Por ejemplo, cuando habilita permisos de edición para la administración de errores, NetScaler ADM proporciona internamente permisos para configurar un perfil de correo o para crear configuraciones de servidor SMTP, de modo que el usuario pueda enviar el informe como correo.

Ejemplo:

David es el administrador de seguridad y administración de certificados SSL en Citrix ADM. En la política asignada a David, el administrador selecciona las siguientes casillas de verificación en la sección **Permisos** :

- **Redes**> **Configuración** > **Editar**
- **Redes**> **Administración de certificados** > **Editar**
- **Sistema**> **Configuración de SSL** > **Editar**
- **Sistema**> **Configuración del sistema** > **Editar**



5. Haga clic en **Crear**.

Configurar grupos

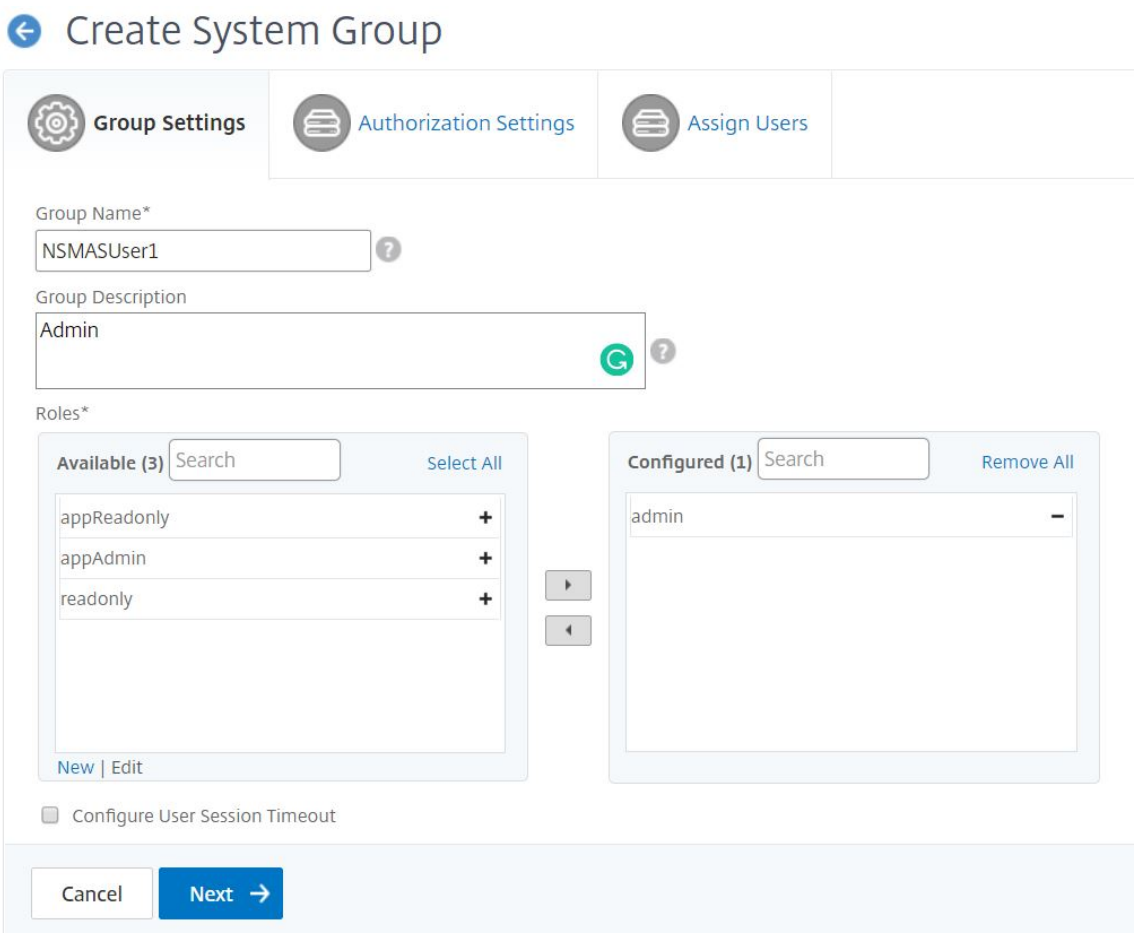
January 30, 2024

En Citrix Application Delivery Management (ADM), un grupo puede tener acceso tanto a nivel de función como a nivel de recursos. Por ejemplo, un grupo de usuarios puede tener acceso solo a instancias seleccionadas de Citrix ADC; otro grupo solo a unas pocas aplicaciones seleccionadas, etc. Al crear un grupo, puede asignar roles al grupo, proporcionar acceso de nivel de aplicación al grupo y asignar usuarios al grupo. A todos los usuarios de ese grupo se les asignan los mismos derechos de acceso en Citrix ADM.

Para crear grupos de usuarios y asignar funciones a los grupos de usuarios:

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > **Grupos**.
2. Haga clic en **Agregar**.
3. En el campo **Nombre de grupo**, escriba el nombre del grupo.
4. En el campo**Descripción del grupo**, escriba una descripción del grupo. Proporcionar una buena descripción del grupo le ayuda a comprender mejor el papel y la función del grupo en un momento posterior.
5. En la sección **Roles**, agregue o mueva uno o más roles a la lista **Configurado**.

> **Nota** En la lista **Disponible**, puede hacer clic en **Nuevo** o **Modificar** y crear o modificar roles. También puede navegar a **Sistema** > **Administración** de **usuarios > Usuarios** y crear o modificar usuarios.



Nota

Puede crear un nuevo rol haciendo clic en **Nuevo**, o puede ir a **Sistema** > **Administración de usuarios** > **Usuarios** y crear nuevos usuarios desde esta pantalla.

6. Haga clic en **Siguiente**. En la ficha **Configuración de autorización**, puede proporcionar la configuración de autorización para los cuatro grupos siguientes:

   - Instancias
   - Aplicaciones
   - Plantillas de configuración
   - StyleBooks

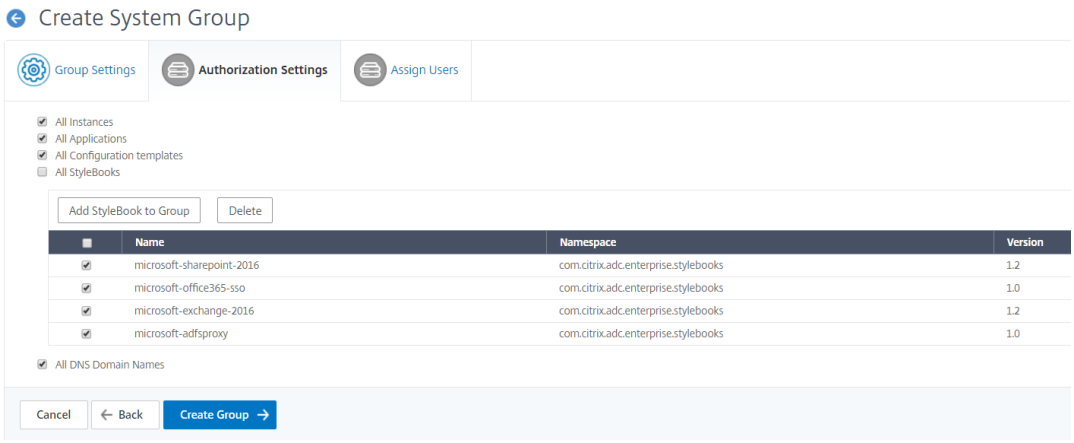
   De forma predeterminada, el usuario puede acceder a todos los grupos anteriores. Puede desactivar las casillas de verificación y proporcionar acceso selectivo a cada uno de estos grupos.

   Por ejemplo:

   - Puede desactivar la casilla de verificación**Instancias** y seleccionar solo las instancias necesarias a las que desee proporcionar acceso a sus usuarios.

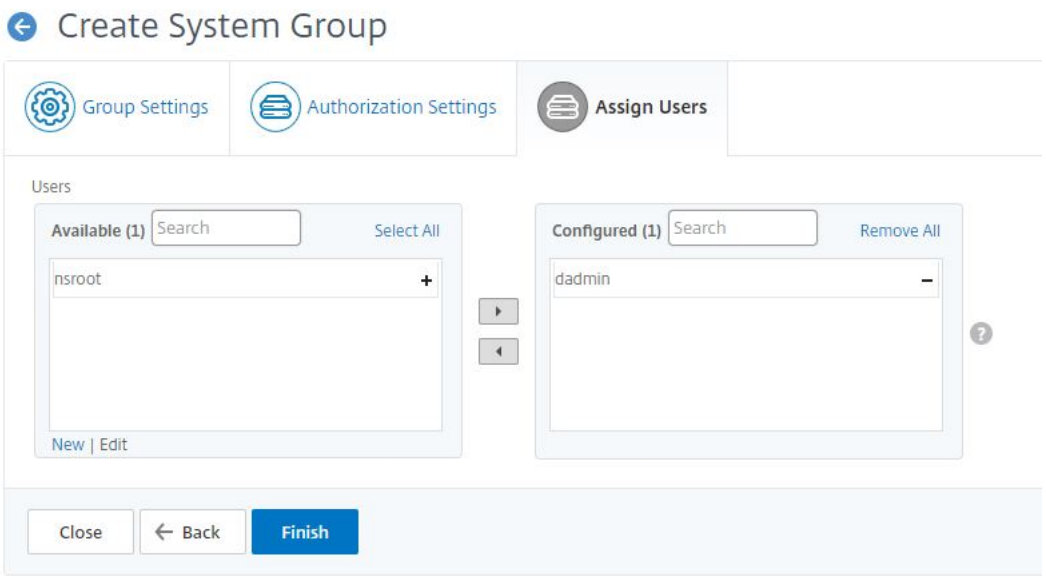
- Desactive la casilla**Todas las aplicaciones** y seleccione solo las aplicaciones y plantillas necesarias. Al agregar aplicaciones a un grupo en Citrix ADM, puede utilizar expresiones regulares para buscar y agregar las aplicaciones que cumplen los criterios de expresiones regulares de los grupos. Los usuarios que están vinculados a estos grupos solo pueden acceder a esas aplicaciones específicas. La expresión regular especificada se conserva en Citrix ADM. Es decir, Citrix ADM permite almacenar en el sistema la expresión regular proporcionada en el cuadro de texto**Agregar expresión regular**y actualiza dinámicamente el alcance de la autorización siempre que las nuevas aplicaciones cumplan con esta expresión regular. Cuando se agregan nuevas aplicaciones al sistema, Citrix ADM aplica los criterios de búsqueda a las nuevas aplicaciones y la aplicación que cumple los criterios se agrega dinámicamente al grupo. No es necesario que agregue manualmente las nuevas aplicaciones al grupo. Las aplicaciones se actualizan dinámicamente en el sistema y los usuarios del grupo respectivo pueden ver las aplicaciones en los módulos correspondientes de Citrix ADM.
- Desactive la casilla de verificación**Todas las plantillas de configuración**para permitir el acceso únicamente a las plantillas necesarias.
- Desactive la casilla**Todos los StyleBooks** y seleccione los StyleBooks necesarios a los que pueda acceder el usuario.

  Puede seleccionar los StyleBooks necesarios cuando cree grupos y agregue usuarios a ese grupo. Cuando el usuario selecciona el StyleBook permitido, también se seleccionan todos los StyleBooks dependientes. Los paquetes de configuración de ese StyleBook también se incluyen en lo que el usuario tiene acceso.



- Desactive la casilla **Todos los nombres de dominio DNS** y agregue los nombres de dominio de la lista a los que quiere que accedan sus usuarios.

7. Haga clic en **Crear grupo**.
8. En la ficha **Asignar usuarios**, seleccione el usuario de la lista **Disponible** y agregue el usuario a la lista **Configurada**. Por ejemplo, “dadmin”.



> **Nota** También puede añadir nuevos usuarios haciendo clic en **Nuevo**.

9. Haga clic en **Finalizar**.

> **Nota:**
>
> Como administrador de Citrix ADM, puede conceder permisos de "solo lectura"o permisos de "visualización y edición"a sus usuarios para las interfaces de usuario individuales de los módulos ADM en función de la configuración de la directiva de acceso de RBAC. Si el usuario está asignado a dos o más grupos, es decir, si el usuario está asignado internamente a más de un ámbito de autorización y a más de una directiva de acceso, ADM combina todos los permisos de esos grupos y autoriza al usuario en consecuencia.
>
> Por ejemplo, considere que el usuario 1 está asignado a un grupo que tiene dos directivas de acceso, P1 y P2. Cada directiva tiene un tipo de permiso diferente. P1 tiene permiso de "solo lectura", mientras que P2 tiene permiso de "ver y editar". Desea que el usuario vea un conjunto de aplicaciones como parte de la directiva P1 y edite un conjunto diferente de aplicaciones como parte de la directiva P2. Sin embargo, como comportamiento predeterminado, Citrix ADM combina los dos tipos de permisos y asigna el permiso de "ver y editar"al usuario. De este modo, su usuario ahora podrá ver y editar todas las aplicaciones.
>
> ADM no admite estos casos de uso en los que se pueden asignar diferentes tipos de permisos al mismo usuario. Solo puede asignar un tipo de permiso a sus usuarios. ADM puede permitir que el Usuario1 vea todas las aplicaciones o un conjunto seleccionado de aplicaciones, o permitir que el Usuario1 vea y edite todas las aplicaciones o el conjunto de aplicaciones seleccionado.

Mapeo de RBAC al actualizar Citrix ADM de 12.0 a 12.1

Al actualizar Citrix ADM de 12.0 a 12.1, no ve las opciones para proporcionar permisos de "lectura-escritura"o "lectura"al crear grupos. Estos permisos se han reemplazado por "roles y directivas de acceso", que le dan más flexibilidad para proporcionar permisos basados en roles a los usuarios. En la siguiente tabla se muestra cómo se asignan los permisos de la versión 12.0 a la versión 12.1:

12.0	Permitir solo aplicaciones	12.1
admin read-write	False	admin
admin read-write	True	appAdmin
admin read-only	False	readonly
admin read-only	True	appReadonly

Configurar roles

January 30, 2024

En Citrix Application Delivery Management (ADM), cada función está vinculada a una o más directivas de acceso. Puede definir relaciones uno a uno, uno a varios y muchos a muchos entre directivas y roles. Puede vincular un rol a varias directivas y puede vincular varios roles a una directiva.

Por ejemplo, un rol puede estar enlazado a dos directivas, con una directiva que defina los permisos de acceso para una función y la otra que defina los permisos de acceso para otra función. Una directiva puede conceder permiso para agregar instancias de Citrix ADC en Citrix ADM y la otra directiva puede conceder permiso para crear e implementar StyleBooks y configurar instancias de Citrix ADC.

Cuando varias directivas definen permisos de edición y solo lectura para una sola función, los permisos de edición tienen prioridad.

Citrix ADM proporciona cuatro funciones predefinidas:

- **administrador**. Tiene acceso a todas las funciones de Citrix ADM. (Este rol está vinculado a adminpolicy).
- **solo lectura**. Tiene acceso de solo lectura. (Este rol está vinculado a readonlypolicy).
- **appAdmin**. Tiene acceso administrativo solo a las funciones de la aplicación en Citrix ADM. (Este rol está vinculado a appAdminPolicy).

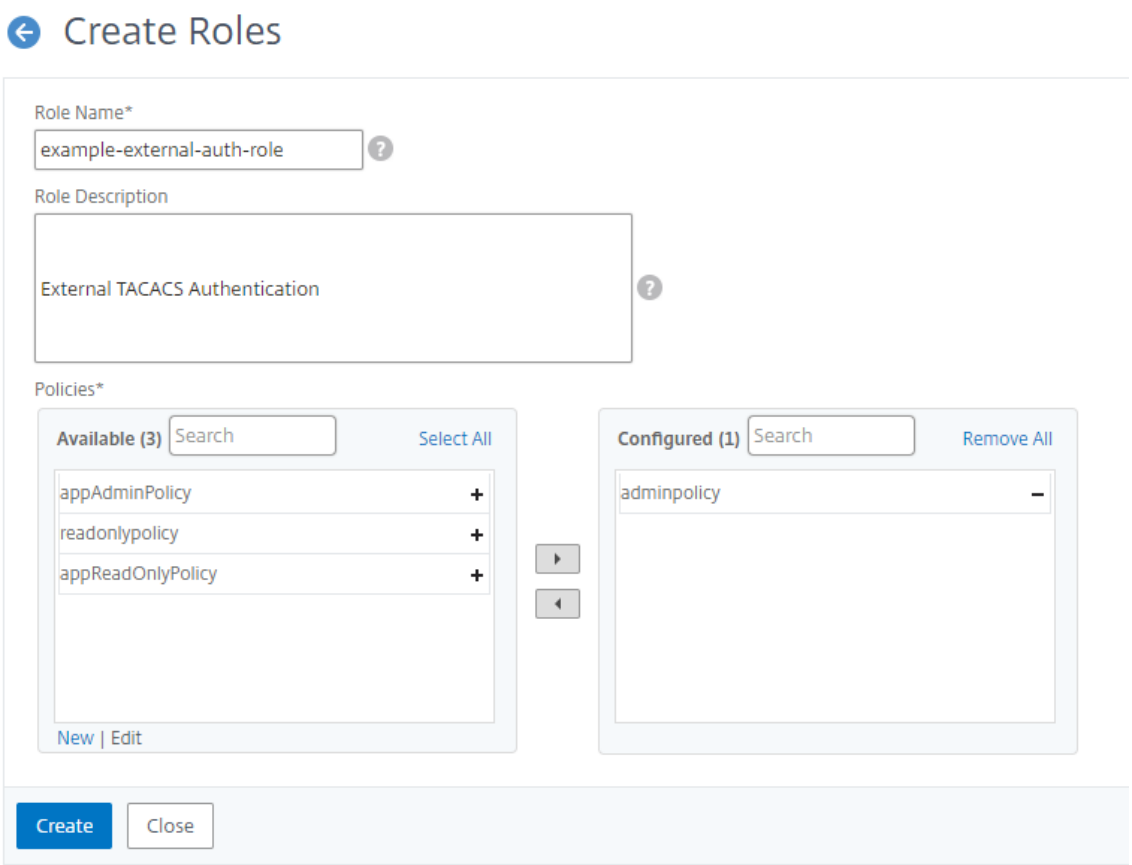
- **appReadonly**. Tiene acceso de solo lectura a las funciones de la aplicación. (Este rol está vinculado a appReadOnlyPolicy).

> **Nota:** Los roles predefinidos no se pueden modificar.

También puede crear sus propios roles (definidos por el usuario).

Para crear roles y asignarles directivas:

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > **Funciones**.
2. Haga clic en **Agregar**.
3. En el campo **Nombre del rol**, introduzca el nombre del rol y proporcione la descripción en el campo **Descripción del rol** (opcional).
4. En la sección **Directivas**, agregue o mueva una o más directivas a la lista **Configurados**.



5. Haga clic en **Crear**.

Configurar usuarios

January 30, 2024

De forma predeterminada, Citrix Application Delivery Management (ADM) tiene un usuario:

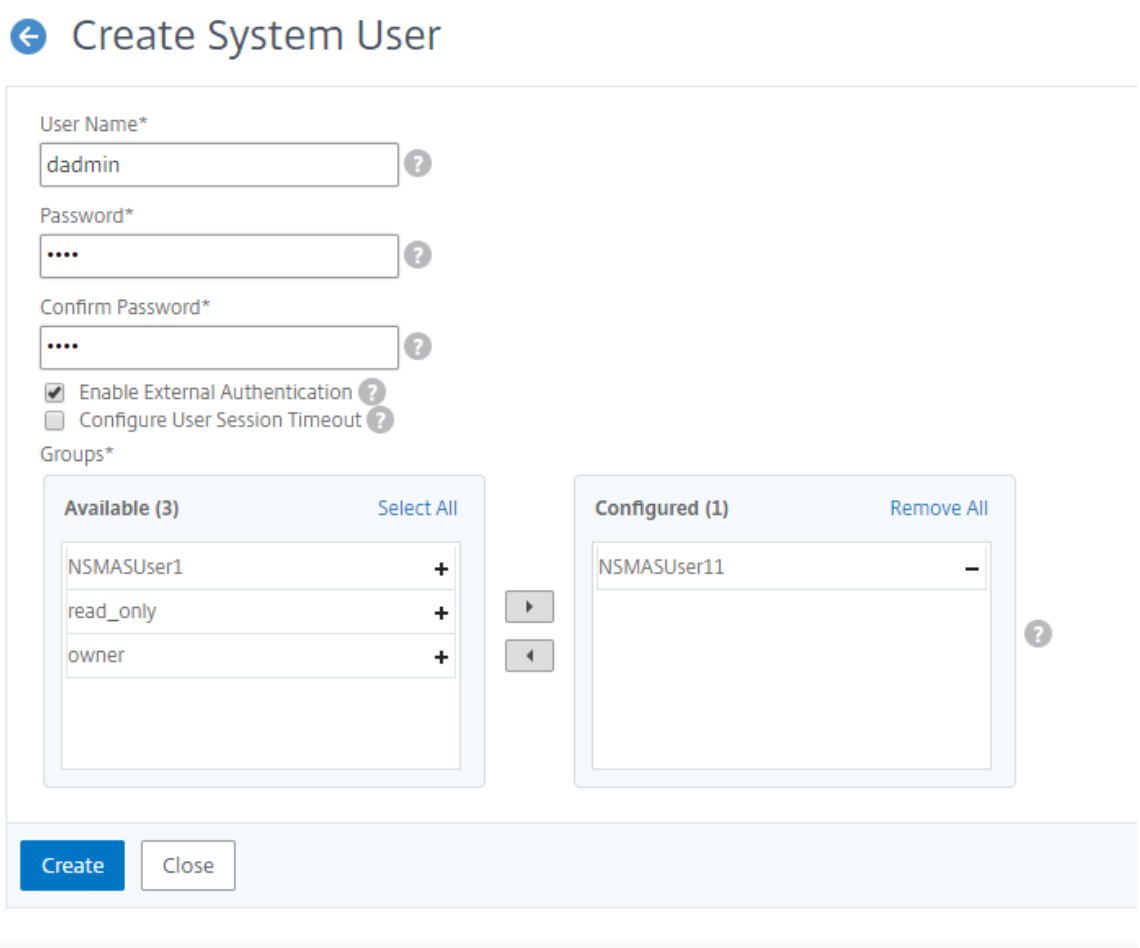
nsroot: el usuario root (nsroot) tiene todos los privilegios administrativos en el dispositivo. El usuario nsroot es el superadministrador de Citrix ADM.

Puede crear usuarios adicionales configurando cuentas para ellos. Cuando agrega nuevos usuarios a Citrix ADM, puede definir sus permisos asignando los grupos, funciones y directivas adecuados.

Puede asignar un usuario a un grupo y vincular el grupo a roles. Puede definir una relación de uno a uno, de uno a muchos o de muchos a muchos entre los usuarios, los grupos, las funciones y las directivas de acceso. Se puede asignar un usuario a varios grupos. Un grupo puede tener varias funciones y varios grupos pueden tener funciones idénticas.

Para configurar usuarios en Citrix ADM:

1. En Citrix ADM, vaya a **Sistema** > **Administración** de **usuarios > Usuarios**.
2. Haga clic en **Agregar**.
3. Introduzca los siguientes detalles:
    a) **Nombre de usuario**. Nombre del usuario
    b) **Contraseña**. Contraseña con la que el usuario inicia sesión en Citrix ADM
4. Si lo quiere, seleccione **Habilitar la autenticación externa**para que el usuario pueda autenticarse a través de un servidor de autenticación externo.
5. Si ha creado grupos y quiere asignar al usuario a un grupo, en la sección **Grupos**, mueva uno o más grupos de la lista **Disponible** a la lista **Configurada**.



6. Haga clic en **Crear**.

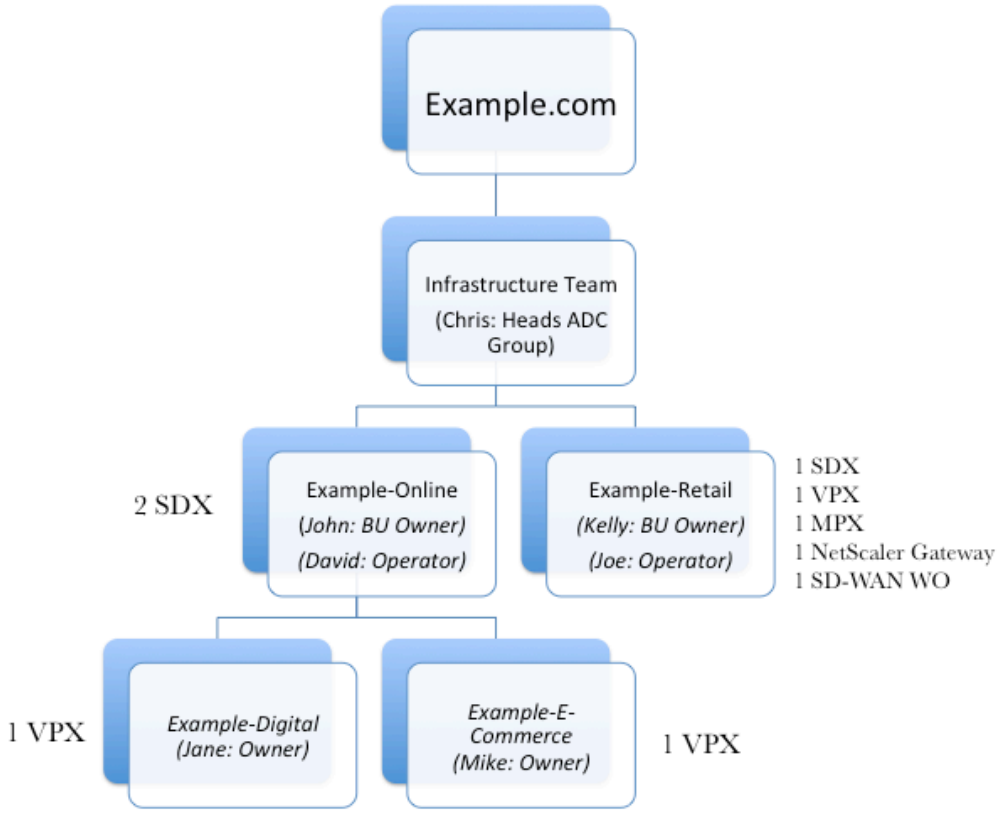
Tenencia múltiple: brinde un entorno de administración exclusivo a sus inquilinos

January 30, 2024

Citrix Application Delivery Management (ADM) proporciona una funcionalidad de tenencia múltiple en la que puede configurar el sistema para varios inquilinos. Cada arrendatario puede agregar sus instancias de red, administrar y supervisar estas instancias y aplicaciones, y crear sus propios usuarios y grupos. Ningún arrendatario tiene visibilidad de las instancias y aplicaciones de los demás arrendatarios. Solo el administrador del sistema tiene visibilidad de todas las instancias, aplicaciones e informes de todos los arrendatarios. Sin embargo, el administrador del sistema no puede crear usuarios para los arrendatarios. Todas las tareas a nivel del sistema solo las puede realizar el administrador del sistema.

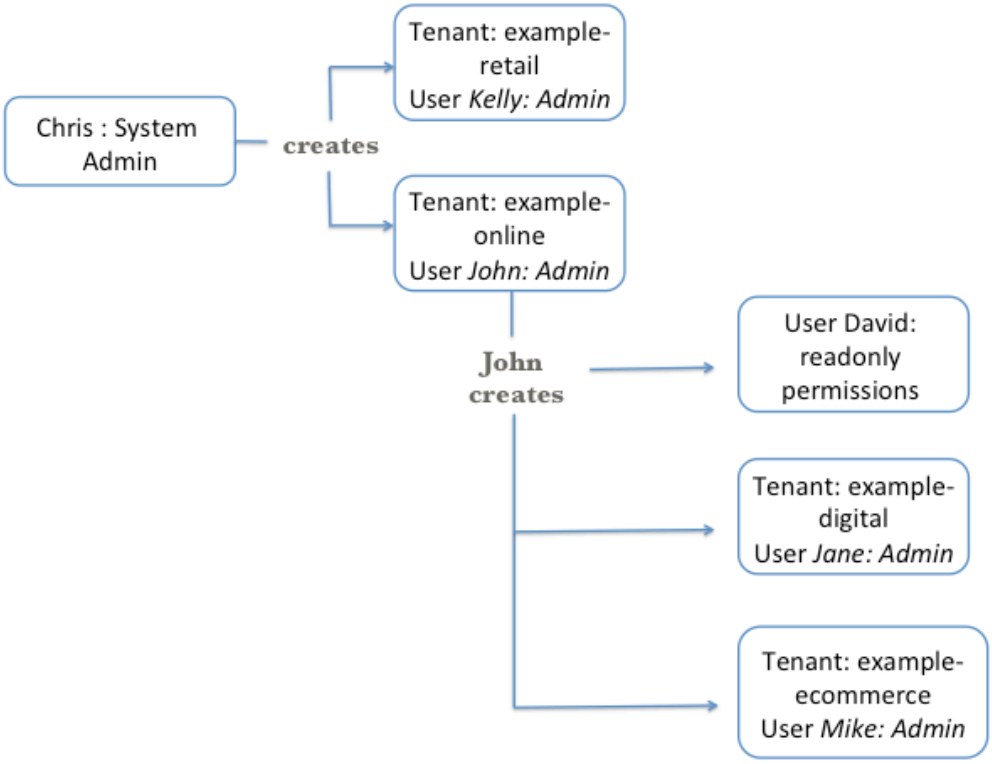
Imaginemos un caso en el que una organización como example.com tenga un grupo de infraestructura y varias unidades de negocio dentro de ella. Quieren gestionar de forma centralizada todas las instancias de su red. Sin embargo, quieren proporcionar un entorno exclusivo a cada unidad de negocio.

La siguiente imagen muestra cómo está estructurado el grupo de infraestructura organizacional de example.com. Quieren que cada una de las cuatro unidades de negocio tenga entornos de gestión exclusivos. Esta imagen también muestra la cantidad de instancias que cada unidad de negocio desea gestionar.



Chris, el jefe del grupo ADC, es el administrador del sistema de NetScaler ADM. Chris crea dos arrendatarios para las dos unidades de negocio, Example-Online y Example-Retail, y asigna dos usuarios como administradores de estos arrendatarios. Cada administrador de inquilinos ahora puede agregar más usuarios, agregar las instancias que quiera administrar y crear subarrendatarios dentro de su entorno de inquilinos.

La siguiente imagen muestra los arrendatarios y usuarios que se crean en NetScaler ADM para este ejemplo.

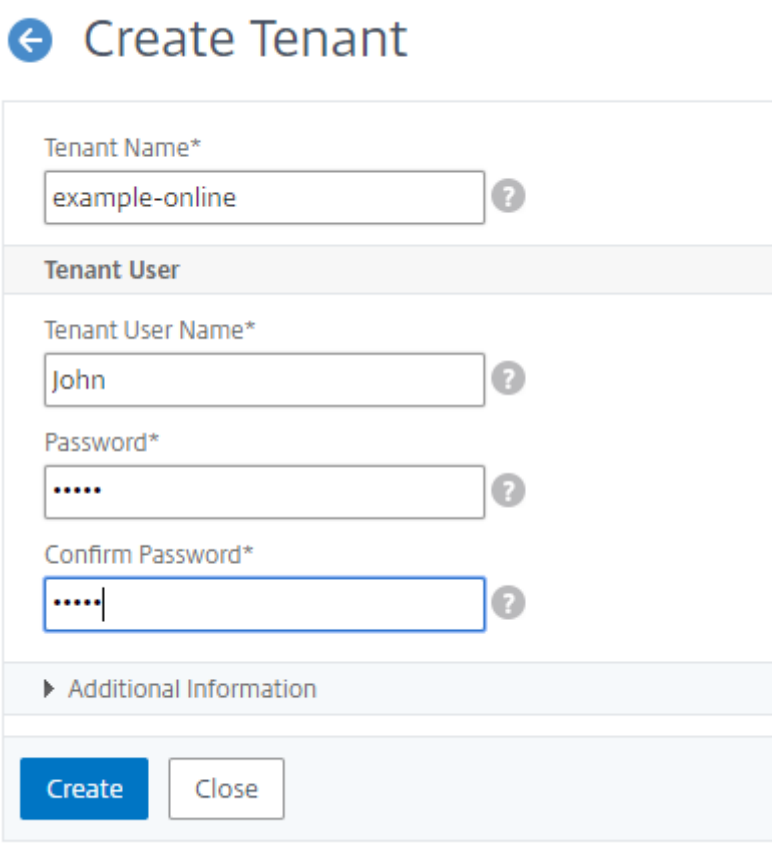


Añadir arrendatarios

En este ejemplo, Chris, el administrador del sistema, crea dos inquilinos: example-online y example-retail. Al crear los arrendatarios, Chris también crea un usuario administrador predeterminado para cada arrendatario.

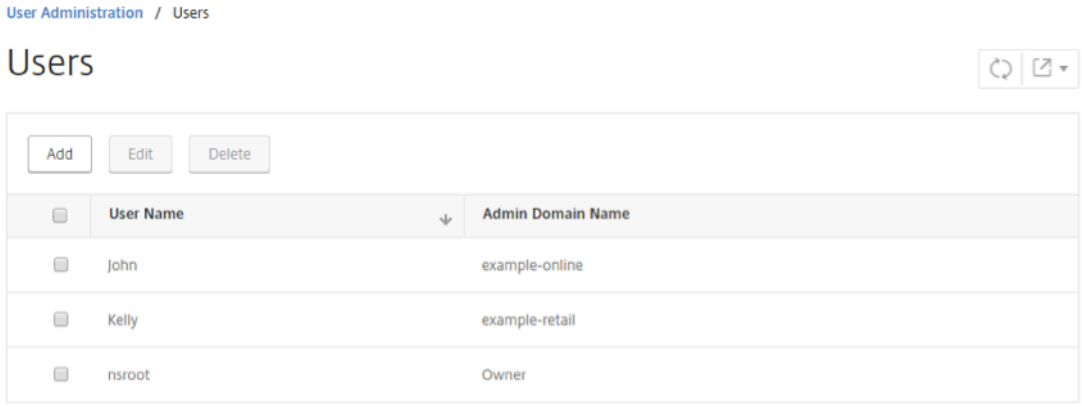
Para agregar arrendatarios

1. Vaya a **Sistema** > **Arrendatarios**y haga clic en **Agregar**.
2. En la página **Crear arrendatario**, especifique el nombre del arrendatario y el nombre de usuario del arrendatario que desea asignar como administrador de este arrendatario. Además, proporcione la contraseña.
3. Haga clic en **Crear**.



En la página **Arrendatarios**, puede ver la lista de arrendatarios que se han creado.

También puede ver la lista de usuarios administradores de cada inquilino en la página **Sistema** > **Administración** de usuarios > **Usuarios** .

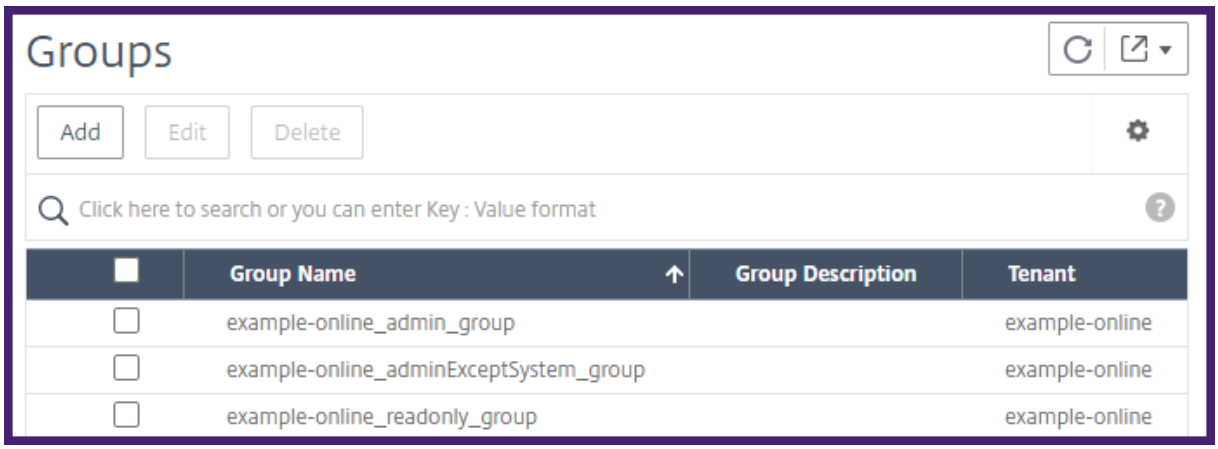


Al crear un arrendatario, se crean tres grupos predeterminados del sistema: admin group, AdminExceptSystem_Group y grupo de solo lectura.

Ejemplo :

El inquilino de ejemplo en línea tiene los siguientes grupos predeterminados:

- `example-online_admin_group`
- `example-online_adminExceptSystem_group`
- `example-online_readonly_group`

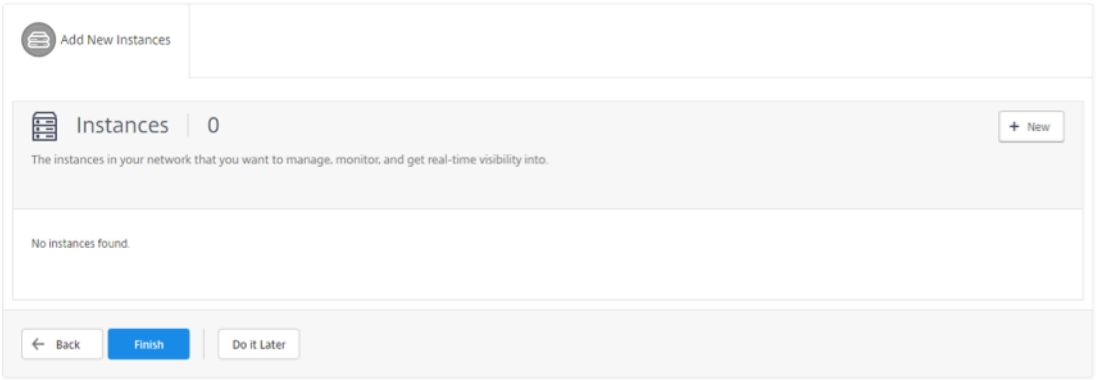


Inicie sesión en Citrix ADM como usuario inquilino

Una vez creados los arrendatarios, un usuario arrendatario puede iniciar sesión en Citrix ADM con las credenciales de usuario arrendatario. Para ello, un arrendatario tiene que proporcionar tanto el nombre de dominio como el nombre de usuario, por ejemplo, ejemplo-online\ John.

Añadir instancias como usuario arrendatario

Cuando un inquilino inicia sesión, Citrix ADM le pide que agregue instancias. Haga clic en **+ Nuevo** para agregar las instancias que quiere administrar. Como alternativa, puede hacer clic en Hacerlo más tarde y agregar las instancias más adelante desde la pestaña Infraestructura. Para obtener más información, consulte *Adición de una instancia a NetScaler ADM*.



En este ejemplo, John agrega dos instancias de NetScaler ADC SDX.

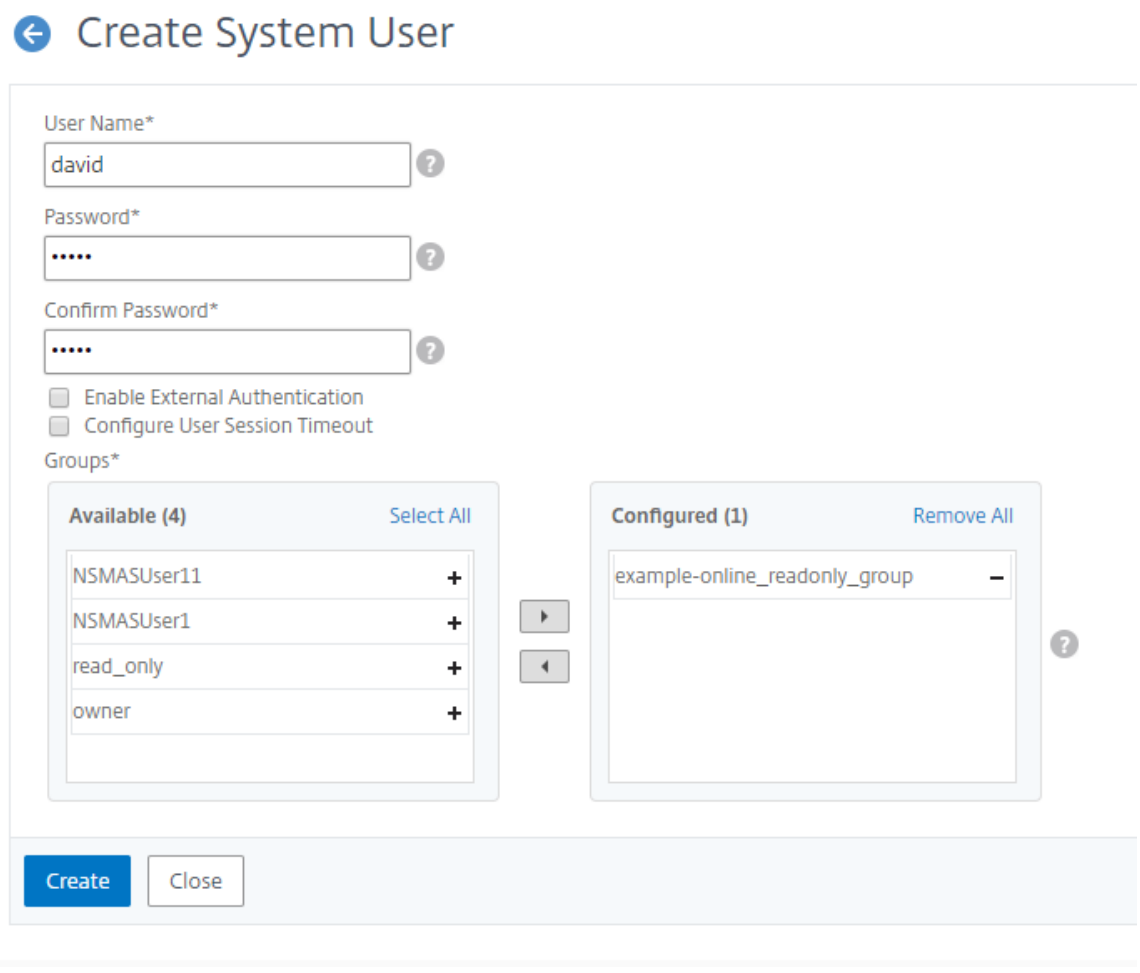
Especifique el tipo de instancia, las direcciones IP (separadas por comas) y el nombre de perfil que Citrix ADM puede usar para acceder a las instancias y, a continuación, haga clic **en**Aceptar.

Crear un usuario

John, el administrador del inquilino, ahora quiere crear un usuario para David para que David pueda supervisar todas las instancias y aplicaciones de este inquilino. Sin embargo, Chris no quiere que David realice ninguna tarea de configuración en las instancias ni cambie ninguna configuración del sistema para el arrendatario. Por lo tanto, Chris crea un usuario david con permisos de solo lectura.

Para crear un usuario:

1. Vaya a **Sistema** > **Administración de usuarios** > **Usuarios** y haga clic en **Agregar** .
2. En la página **Crear usuario del sistema**, especifique el nombre de usuario y la contraseña del usuario que quiere crear.
3. En **Grupos**, selecciona el grupo que quieres asignar a este usuario. En este ejemplo, el example-online_readonly_group se asigna al usuario david.

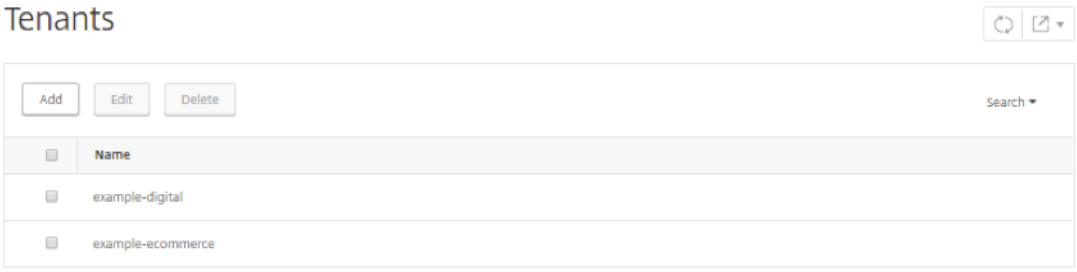


Crear arrendatarios dentro de arrendatarios

Un administrador de inquilinos puede crear subarrendatarios si quiere dividir aún más a su inquilino. Sin embargo, solo puede crear un nivel de subarrendatarios. En este ejemplo, John crea dos subarrendatarios, example-digital y example-ecommerce. Al crear estos dos subarrendatarios, Chris asigna a Jane y Mike como usuarios administradores, respectivamente.

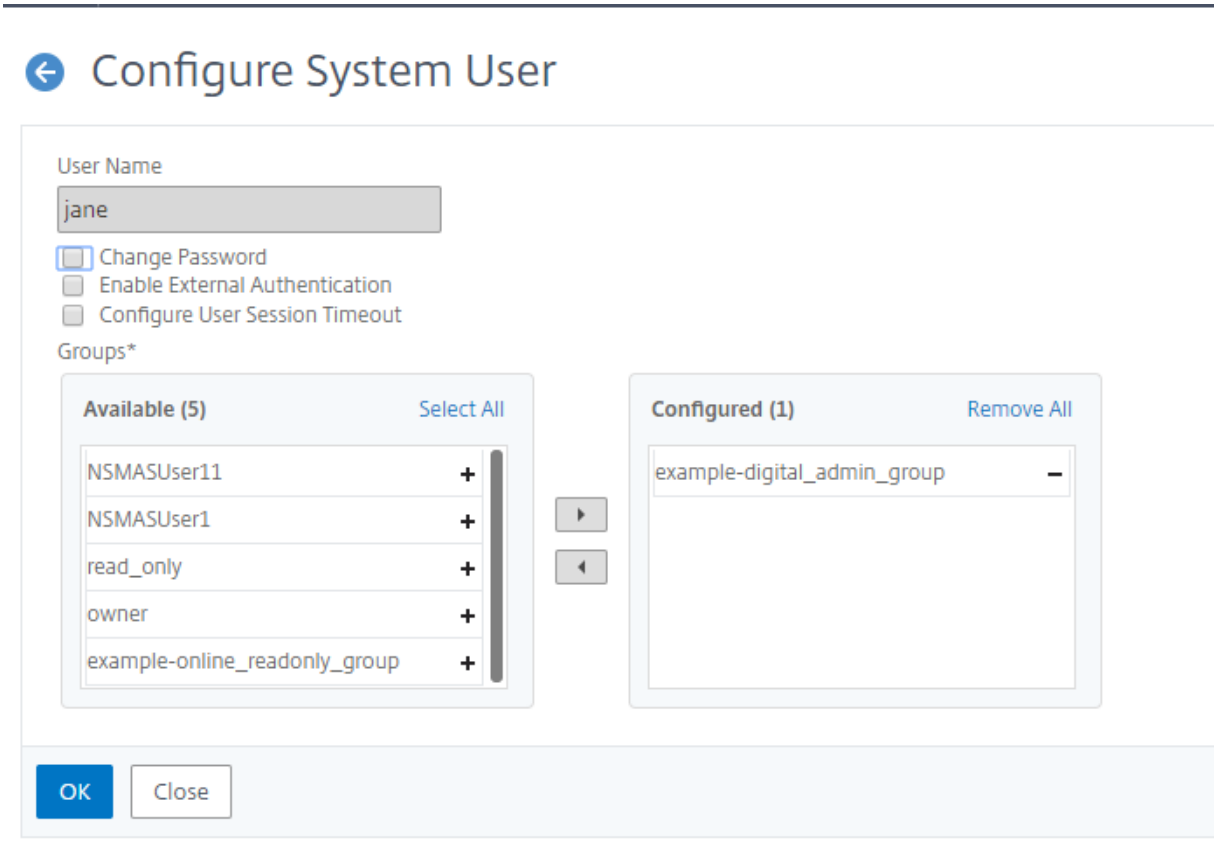
Para crear un arrendatario dentro de un arrendatario, siga los pasos descritos en Agregar arrendatarios.

Puede ver los arrendatarios creados en la página **Arrendatarios**.



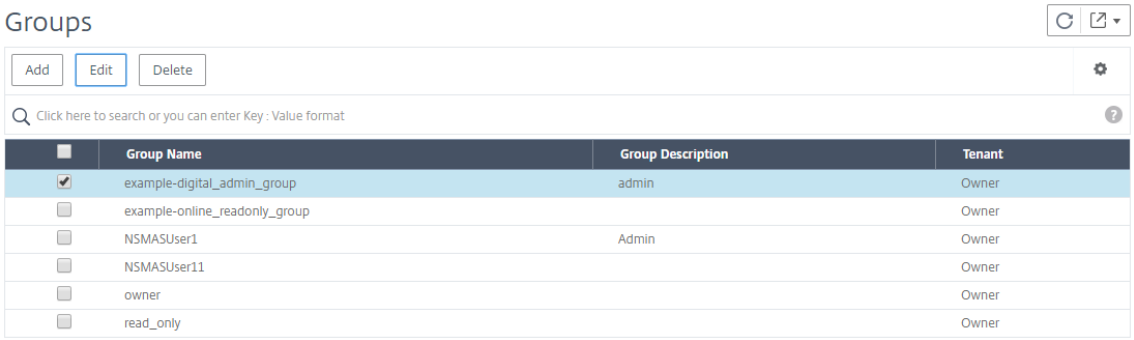
También puede ver los permisos asignados a los usuarios. Vaya a **Sistema** > **Administración** de usuarios > **Usuarios** , seleccione un usuario y haga clic en **Editar** .

En la página **Configurar usuario del sistema** , en Grupos, puede ver los grupos asignados a ese usuario. En este ejemplo, puede ver que example-digital_admin_group está asignado a Jane.

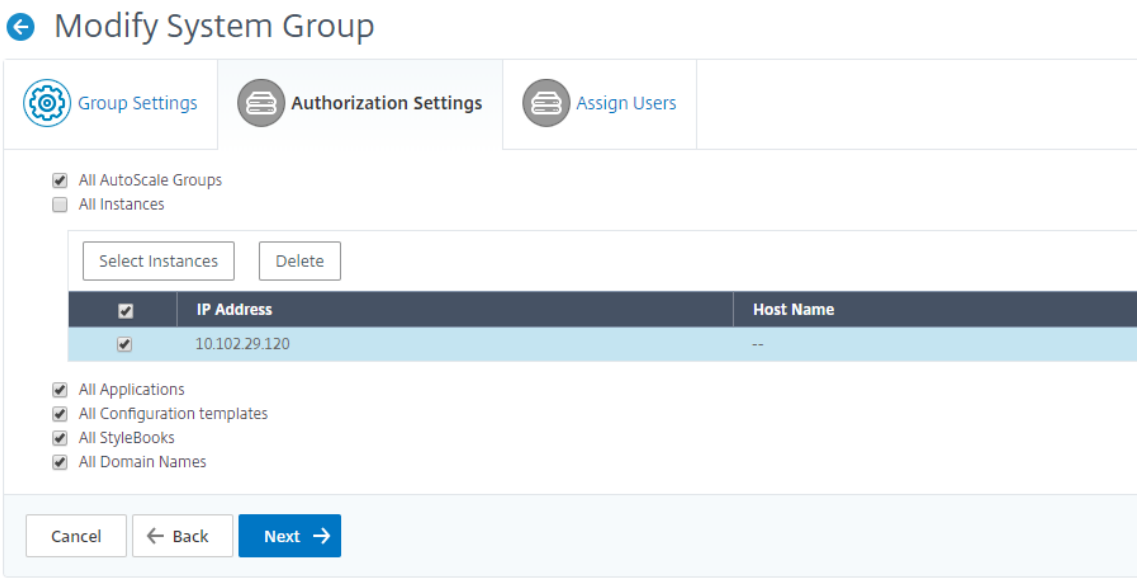


Como administrador de inquilinos, si ya ha agregado instancias a Citrix ADM, puede asignar las instancias a los usuarios de su inquilino o subarrendatarios para su administración y supervisión. Por ejemplo, John puede asignar una instancia VPX a Jane para fines de administración.

1. Vaya a **Sistema** > **Administración de usuarios** > **Grupo** .
2. Seleccione el grupo al que está asignado el usuario y haga clic en **Modificar**.



3. En la página **Modificar grupo de sistemas**, en la ficha **Configuración de autorización**, desactive la casilla de verificación **Todas las instancias**.



4. Seleccione las instancias que desee que el usuario administre y, a continuación, haga clic en **Seleccionar instancias**.
5. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Aplicaciones

January 30, 2024

La función de análisis y administración de aplicaciones de NetScaler ADM refuerza el enfoque centrado en las aplicaciones para ayudarlo a abordar diversos desafíos de entrega de aplicaciones. Este enfoque le brinda visibilidad de la puntuación de estado de las aplicaciones, lo ayuda a determinar los riesgos de seguridad y lo ayuda a detectar anomalías en los flujos de tráfico de las aplicaciones y a tomar medidas correctivas.

La siguiente ilustración proporciona una descripción general de las diversas tareas que puede realizar para la administración y el análisis de aplicaciones:

Las aplicaciones pueden ser aplicaciones descubiertas, aplicaciones HAProxy o aplicaciones personalizadas.

Aplicaciones descubiertas

Aplicaciones que se crean automáticamente para cada servidor virtual administrado. Las aplicaciones descubiertas siempre tendrán un servidor virtual y estas aplicaciones no se pueden editar ni eliminar directamente.

Aplicaciones personalizadas

Aplicaciones creadas por los usuarios a partir de aplicaciones descubiertas. Citrix ADM permite agregar, editar y eliminar estas aplicaciones. Las aplicaciones personalizadas se crean mediante:

- Uno o más servidores virtuales
- Una o más interfaces de HAProxy.

Al crear una aplicación personalizada, todas las aplicaciones descubiertas agregadas a la aplicación personalizada se eliminan del panel de control de la aplicación.

Puntos que tener en cuenta

- No puede agregar una aplicación descubierta en varias aplicaciones personalizadas.
- No puede crear una aplicación personalizada si todas las aplicaciones descubiertas ya están asignadas a otra aplicación personalizada. Debe eliminar una aplicación personalizada existente para liberar las aplicaciones descubiertas y poder seguir componiendo aplicaciones personalizadas nuevas.
- No puede crear una aplicación personalizada que contenga servidores virtuales y interfaces HAProxy.

Aplicaciones HAProxy

Las aplicaciones discretas de HAProxy se crean automáticamente para cada interfaz de HAProxy gestionada. También puede agrupar estas aplicaciones para formar aplicaciones personalizadas similares a las aplicaciones NetScaler ADC. Para obtener más información, consulte Administración y supervisión de instancias de HAProxy con Citrix ADM.

Puntos que tener en cuenta

Las siguientes funciones o métricas del panel de aplicaciones no son compatibles con las aplicaciones HAProxy:

- Investigador de actividad de aplicaciones
- Puntuación de la aplicación
- Índice de amenazas
- Tendencia de uso máximo
- Rendimiento

- Conexiones de servidor
- Transacciones

Creación de una aplicación personalizada

Puede crear aplicaciones personalizadas añadiendo una o más aplicaciones descubiertas mientras define una aplicación.

Para crear una aplicación personalizada:

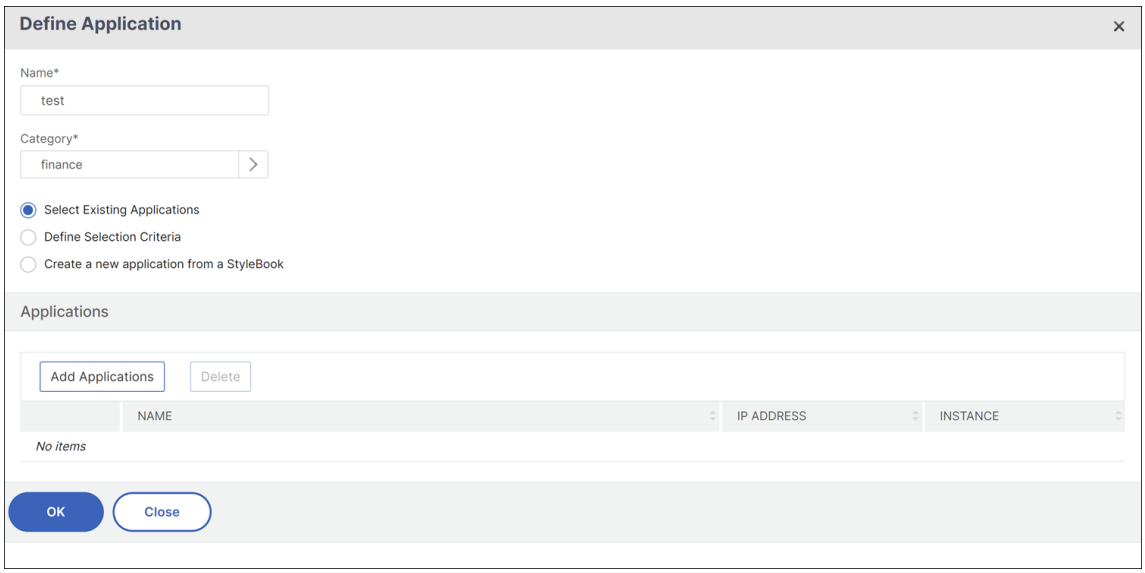
1. Vaya a **Aplicaciones** > **Panel** y haga clic en **Definir aplicación personalizada**.
2. En la pantalla Definir aplicación, defina los siguientes parámetros:

Campo	Descripción
Nombre	Nombre de la aplicación personalizada
Categoría	Nombre de la categoría en la que se agruparán todas las aplicaciones relacionadas con esa categoría en el panel de control de la aplicación.
Seleccionar aplicaciones existentes	Opción para agregar servidores virtuales si los criterios de definición se basan en los servidores virtuales con licencia supervisados por Citrix ADM.
Definir criterios de selección	Opción para definir la aplicación por rango de servidores virtuales o por rango de direcciones IP de servidor/servicio de origen. • **Servidor.** Debe especificar la dirección IP del servidor o servicio, el nombre del servidor o el puerto del servidor back-end en el que se ejecutan las aplicaciones. Puede introducir una dirección IP, un intervalo de direcciones IP o una combinación de ambas separadas por comas. Por ejemplo, puede escribir 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

Campo	Descripción
	• **Servidores virtuales.** Puede especificar una de las siguientes opciones: la dirección IP del servidor virtual, el nombre del servidor virtual o el puerto del servidor backend en el que se ejecutan las aplicaciones. Puede introducir una dirección IP o un intervalo de direcciones IP o una combinación de ambas separadas por comas. Por ejemplo, puede escribir 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

3. Haga clic en Aceptar.

> **Nota**
>
> Actualmente, Application Dashboard solo admite servidores virtuales de equilibrio de carga y conmutación de contenido.

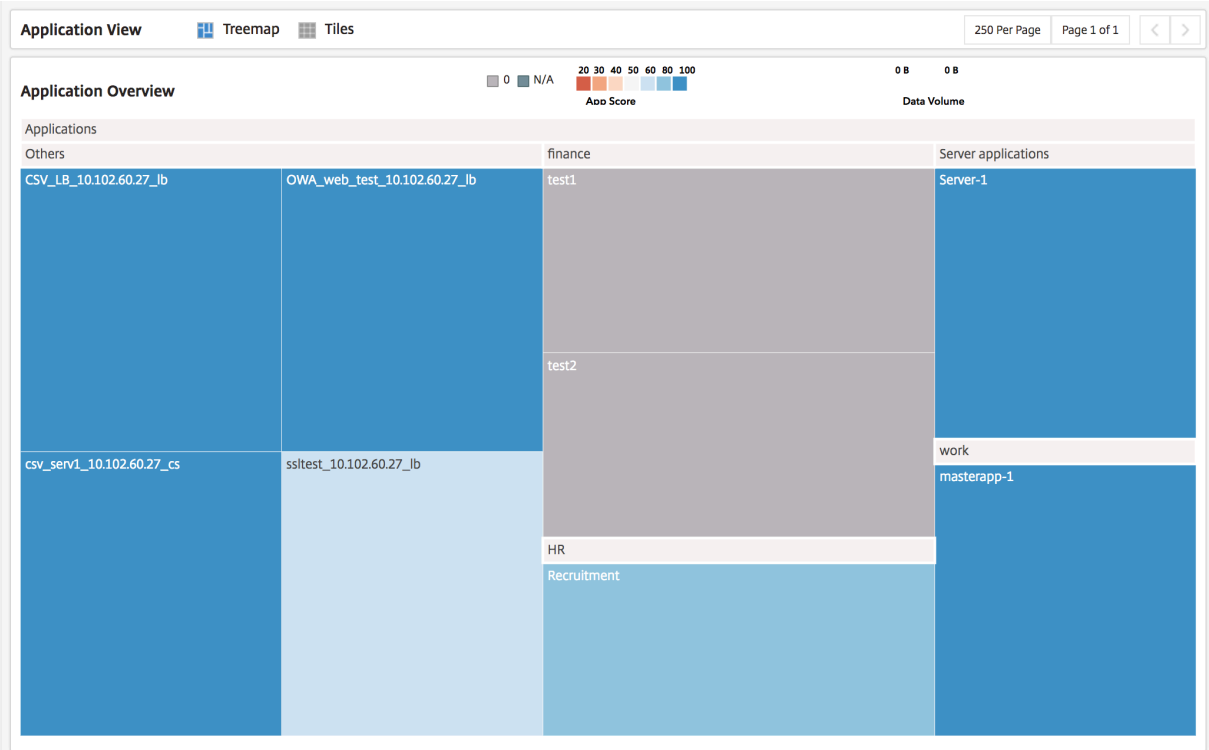


Agrupe sus aplicaciones

La agrupación de sus aplicaciones le permite administrarlas y supervisarlas con facilidad. Puede agrupar sus aplicaciones seleccionando o creando una categoría al definir una aplicación. Para crear o

seleccionar la categoría, al definir la aplicación, haga clic en el botón **situado junto al campo Categoría.

Las aplicaciones que no se agregan a ninguna categoría se muestran en la categoría **Otros** .



Panel de aplicaciones

El panel de aplicaciones proporciona una vista holística de todas las aplicaciones supervisadas por Citrix ADM y proporciona información clave relacionada con todas las aplicaciones. Por ejemplo, el panel muestra las métricas de rendimiento y seguridad, los contadores y el estado de las aplicaciones. Para mostrar información sobre una aplicación concreta, selecciónela. Además, en el panel Resumen, los gráficos de barras muestran métricas como la puntuación de las aplicaciones y los índices de amenazas de todas las aplicaciones supervisadas.

Vea sus aplicaciones

El panel de aplicaciones muestra las aplicaciones como nodos en un mapa de árbol, cuyo tamaño depende del volumen de datos de la aplicación. El color de un icono indica la puntuación de la aplicación en la aplicación: el rojo indica un estado de salud mínimo y el azul indica un buen estado de salud.

Puede cambiar la vista del panel de la aplicación a un mapa de árbol o a mosaicos seleccionando una de las opciones de la pantalla del panel de la aplicación, donde puede ver los detalles de las aplica-

ciones en forma de tarjetas. De forma predeterminada, se muestran 250 aplicaciones en el panel de aplicaciones. Para ver más aplicaciones, haga clic en la opción de la página siguiente.

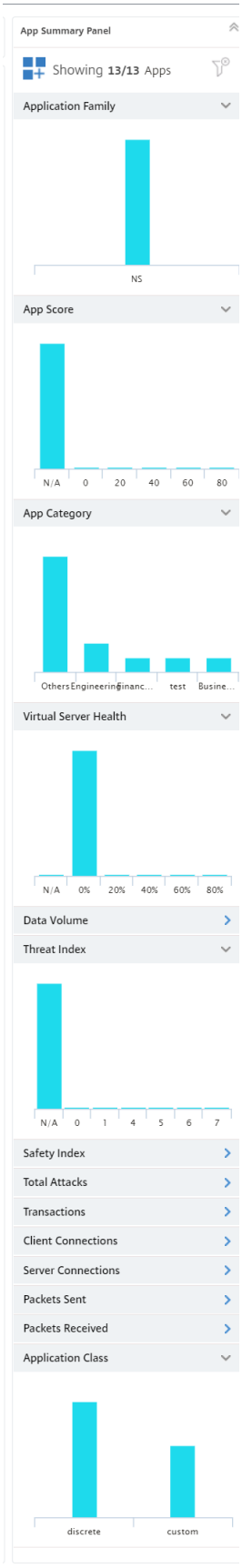
Las aplicaciones se agrupan según las categorías que se seleccionaron al definirlas. Las aplicaciones se pueden ordenar o hacer visibles seleccionando las métricas de la aplicación en el panel de resumen de la aplicación. Por ejemplo, si quieres mostrar las aplicaciones que tienen una puntuación de aplicación entre 20 y 40, selecciona el gráfico de barras correspondiente en la sección Puntuación de la aplicación del panel de resumen de la aplicación. Del mismo modo, puede seleccionar otras métricas en el panel de resumen de la aplicación.

Panel de resumen de la aplicación

El panel de resumen de la aplicación muestra todas las métricas de las aplicaciones que están visibles en el panel de control de la aplicación. Este panel le permite ordenar y ver las aplicaciones en el panel seleccionando o deseleccionando las métricas de las aplicaciones. El panel de resumen de la aplicación muestra las siguientes métricas:

Métricas	Descripciones
Familia de aplicaciones	Gráfico de barras que agrupa el número de aplicaciones según el tipo de instancias de Citrix ADC en las que están configuradas.
Puntuación de la aplicación	Un sistema de puntuación que define el rendimiento de una aplicación
Categoría de la aplicación	Gráfico de barras que muestra un histograma para todas las categorías definidas en Citrix ADM. Todas las aplicaciones discretas aparecen ahora en la categoría «Otras» y las aplicaciones personalizadas aparecen en sus respectivos nombres de categoría.
Estado del servidor virtual	Un gráfico de barras que muestra el número de solicitudes de cada categoría. Las solicitudes se clasifican para tener un valor de puntuación de salud del 0%, 20%, 40%, 60%, 80% y 100%.
Volumen de datos	Un sistema de puntuación que agrupa el número de solicitudes según el volumen de datos de la aplicación. El volumen de datos se calcula según el número total de bytes solicitados por las aplicaciones y el número de bytes recibidos como respuestas de las aplicaciones.

Métricas	Descripciones
Índice de amenazas	Un sistema de clasificación de un solo dígito que indica la gravedad de los ataques a la aplicación, independientemente de si la aplicación está protegida o no por un dispositivo Citrix ADC.
Índice de seguridad	Sistema de clasificación de un solo dígito que indica con qué seguridad ha configurado las instancias NetScaler ADC para proteger las aplicaciones de amenazas y vulnerabilidades externas.
Ataques totales	El número total de ataques contra las aplicaciones
Transacciones	El rango de transacciones realizadas por las aplicaciones.
Conexiones de clientes	El número de conexiones de cliente establecidas por las aplicaciones.
Conexiones de servidor	El número de conexiones de servidor establecidas por las aplicaciones.
Paquetes enviados	El número de paquetes enviados por las aplicaciones.
Paquetes recibidos	La cantidad de paquetes que reciben las aplicaciones.
Clase de aplicación	Gráfico de barras que agrupa el número de aplicaciones en función de si son aplicaciones discretas o personalizadas.

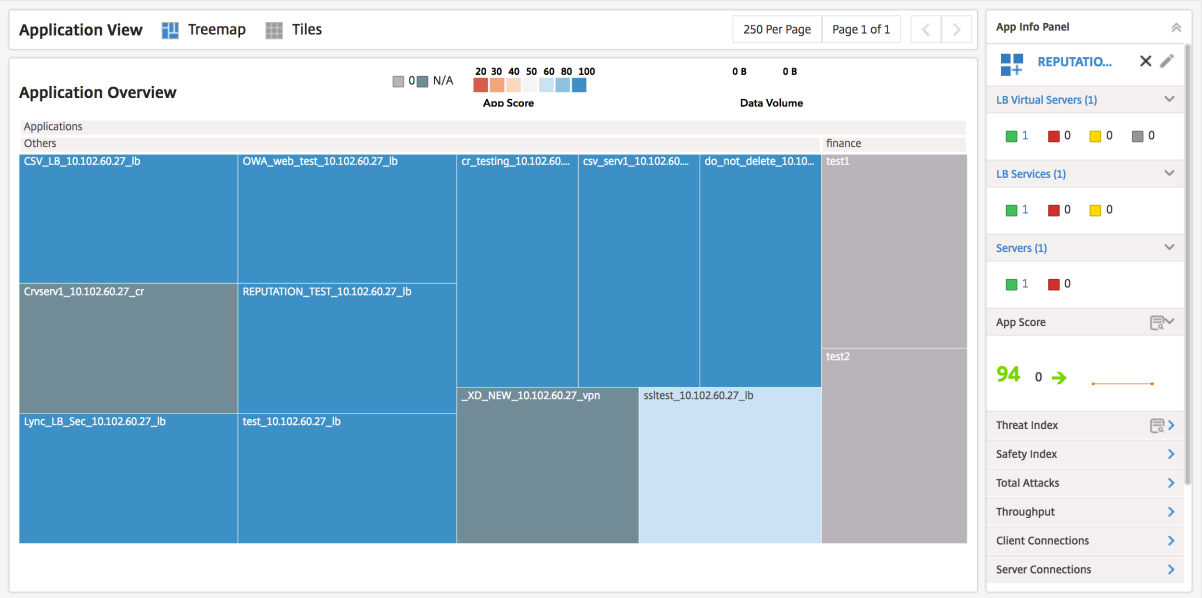


Por ejemplo, en el panel de resumen de la aplicación, desplázate hacia abajo para encontrar el gráfico de barras «Estado del servidor virtual». En el gráfico de barras del estado del servidor virtual, Citrix ADM clasifica las aplicaciones en función del porcentaje del estado del servidor virtual. El gráfico de barras muestra la cantidad de aplicaciones que tienen un valor de estado de los servidores virtuales entre el 0% y el 100%.

El estado del servidor virtual representa el estado de los servidores virtuales que se agrupan en aplicaciones discretas. Sin embargo, si hay aplicaciones personalizadas que comprenden dos o más servidores virtuales, se considera el menor estado del servidor virtual del grupo.

Ahora puede aplicar un filtro y ver solo las aplicaciones en el panel de aplicaciones que coincidan con los criterios de selección. Haz clic en la barra que dice 0%. Esta barra muestra la cantidad de aplicaciones que tienen un estado de servidor virtual entre el 0% y el 20%. Ahora puede segregar las aplicaciones que tienen un estado de servidor virtual bajo y tomar medidas correctivas.

Panel de información de la aplicación El panel de información de la aplicación se encuentra en el primer nivel cuando se profundiza en una aplicación. Muestra las métricas y componentes clave de la aplicación, junto con su estado. Por ejemplo, para cualquier aplicación seleccionada, el panel Información de la aplicación muestra la cantidad total de servidores virtuales, la cantidad total de servicios, la puntuación de la aplicación y otra información. Para mostrar el panel de información de la aplicación, haga clic en cualquier icono de la aplicación en el panel de control de la aplicación. El panel Información de la aplicación reemplaza al panel Resumen de la aplicación.

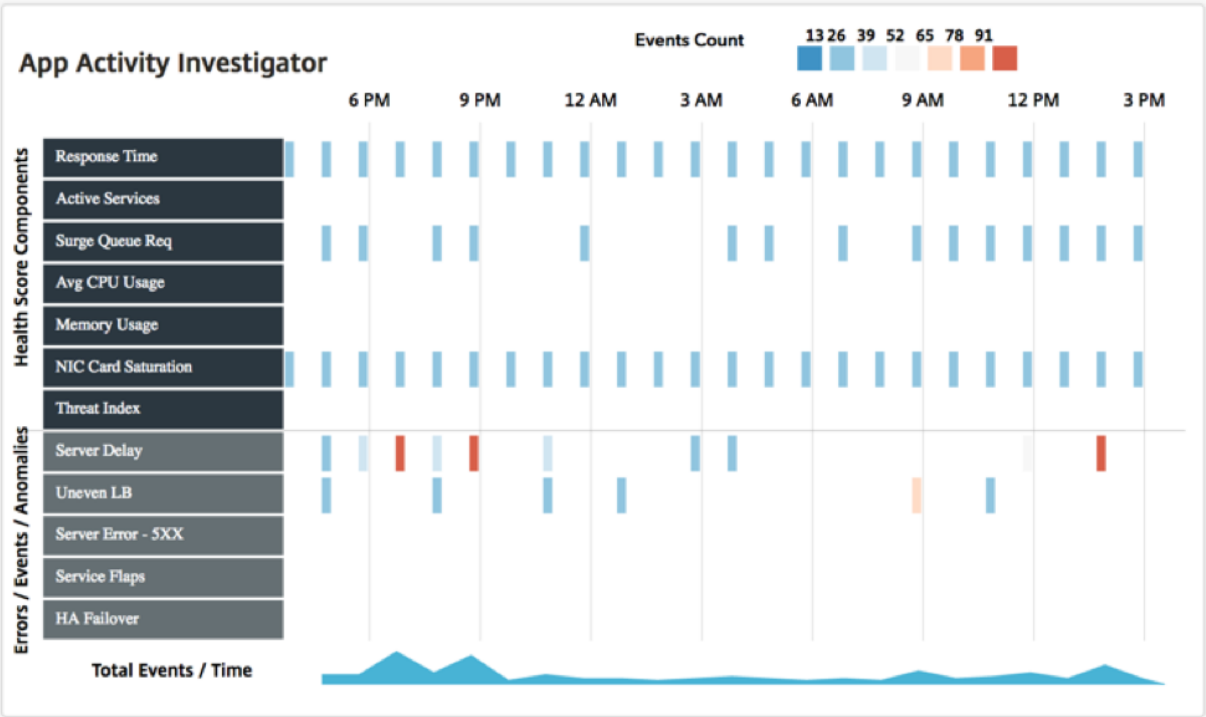


Investigador de actividad de aplicaciones El investigador de actividad de la aplicación es uno de los del segundo nivel cuando se profundiza desde una aplicación. Para llegar al investigador de

actividad de la aplicación, seleccione el icono de búsqueda en el panel de información de la aplicación o haga doble clic en el icono de la aplicación en el panel de control de la aplicación.

El investigador de actividad de la aplicación muestra información clave, como los componentes de la puntuación de la aplicación, los errores, los eventos y las anomalías.

Cada una de las leyendas se agrega en un intervalo de un minuto si la duración seleccionada es de una hora, y en un intervalo de una hora si la duración seleccionada es de un día.



Estas desviaciones se muestran como leyendas rectangulares en el gráfico. Estas leyendas se agregan y se codifican por colores según el número de eventos que se han producido. El azul indica el número más bajo de eventos y el rojo el máximo. Puede colocar el puntero del ratón sobre una leyenda para mostrar detalles como el tipo de error, la hora y el número de eventos agregados para la leyenda seleccionada. Puede personalizar el período de tiempo del gráfico seleccionando el menú desplegable de tiempo desde el período de tiempo.

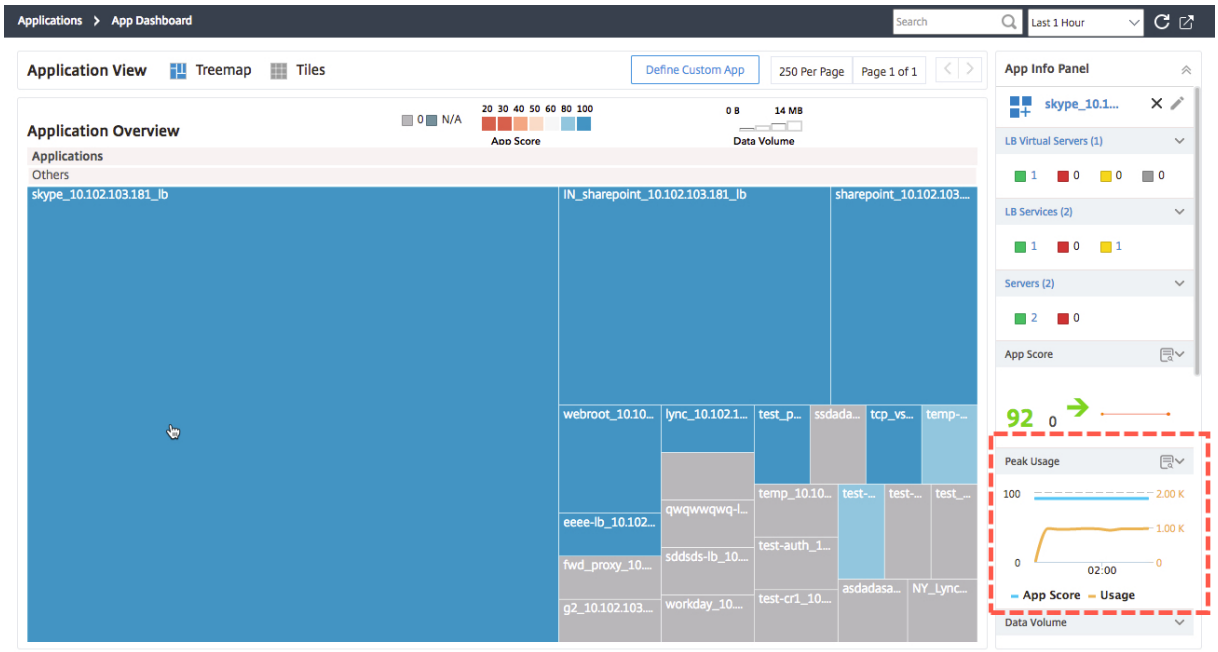
Tendencia de uso de aplicaciones En la mayoría de los casos, usted, como propietario de una empresa, toma decisiones sobre la eficacia de su aplicación y las tendencias de uso basándose en estadísticas y datos. Para comprender la tendencia de uso de las aplicaciones, debe recopilar información de varias entidades de su implementación, como la infraestructura de backend, los proxies, las redes CDN, etc. Luego, correlacione la información recopilada para obtener un análisis adecuado, esto consume mucho tiempo.

En cambio, el dispositivo Citrix ADC implementado como ADC en su implementación contiene toda la información sobre la aplicación y las estadísticas de uso de la aplicación. Puede reenviar esta infor-

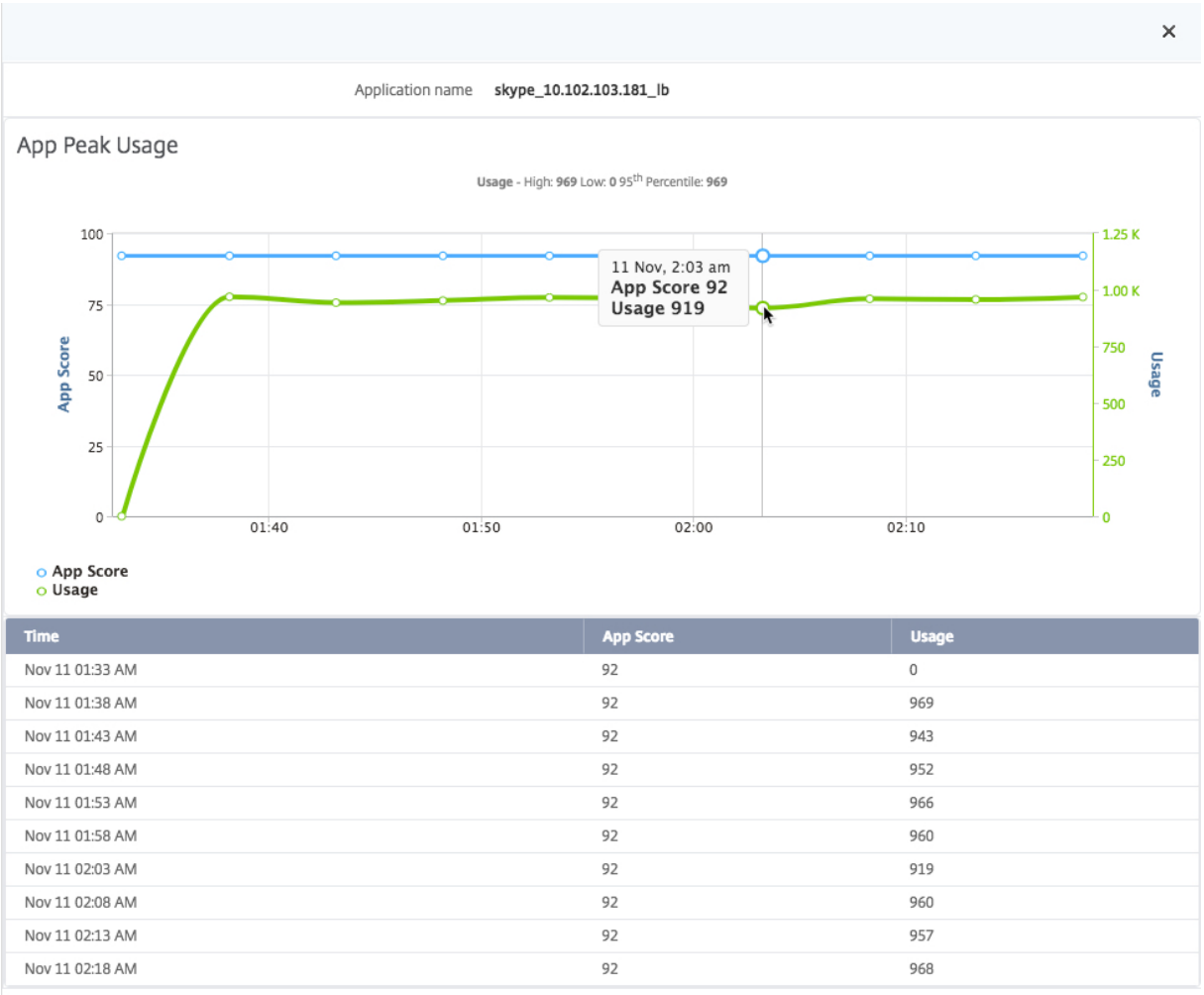
mación a Citrix ADM. Citrix ADM recopila esta información y proporciona información detallada sobre el uso y el rendimiento de las aplicaciones. Puede utilizar esta información para tomar decisiones eficaces en función del uso y el rendimiento de las aplicaciones.

El panel de información de la aplicación del panel de control de aplicaciones muestra la tendencia de uso máximo de una aplicación. Puede utilizar la tendencia de uso máximo para evaluar el rendimiento de la aplicación y tomar las medidas adecuadas para mejorar el rendimiento de la aplicación.

Para ver la tendencia de uso máximo de una aplicación, vaya a **Aplicaciones > Panel** de control de aplicaciones . Seleccione la aplicación y la tendencia de uso máximo de la aplicación se mostrará en la sección **Uso máximo** del panel de información de la aplicación.



También puedes hacer clic en la sección **Uso máximo** para ver la puntuación de la aplicación y el uso de la aplicación. Con esta información, puede identificar el uso máximo de la aplicación y asociarlo con la puntuación de la aplicación correspondiente para evaluar el impacto en el rendimiento de la aplicación durante el período de uso máximo.



Time	App Score	Usage
Nov 11 01:33 AM	92	0
Nov 11 01:38 AM	92	969
Nov 11 01:43 AM	92	943
Nov 11 01:48 AM	92	952
Nov 11 01:53 AM	92	966
Nov 11 01:58 AM	92	960
Nov 11 02:03 AM	92	919
Nov 11 02:08 AM	92	960
Nov 11 02:13 AM	92	957
Nov 11 02:18 AM	92	968

Exportar informes del panel de aplicaciones y del panel de seguridad

Citrix ADM le permite tomar una instantánea de las páginas actuales de App Dashboard y App Security Dashboard y exportarlas como informes. En un intervalo de tiempo frecuente, es posible que los administradores de la aplicación necesiten usar estos informes para actualizar el uso de la aplicación y las sanciones de rendimiento.

Con esta función, los administradores pueden extraer estos datos como informes.png o.pdf.

> **Nota** A diferencia de otras opciones de exportación de informes de Citrix ADM, puede exportar los informes de App Dashboard y Security Dashboard solo como archivos.pdf o.png. Otras opciones como,.jpg y.csv no son compatibles actualmente.

1. En la página **Panel de control de aplicaciones** o **Panel de seguridad** de aplicaciones, haga clic en el icono de exportación en la parte superior derecha de la página.
2. Elija la opción de exportación como archivo PDF o PNG.

3. Haga clic en **Aceptar**.

El informe se descarga en su sistema. Desde las páginas del panel de control de aplicaciones y del panel de seguridad de la aplicación, también puede navegar a páginas de segundo nivel y exportarlas como informes. Actualmente, puede descargar informes de una sola aplicación a la vez.

Análisis del rendimiento de las aplicaciones

January 30, 2024

App Score es el producto de un sistema de puntuación que define el rendimiento de una aplicación. Muestra si la aplicación funciona bien en términos de capacidad de respuesta y si tiene todos los sistemas en funcionamiento. La puntuación de la aplicación se muestra en el nivel de la aplicación. El cálculo de la puntuación se basa en los siguientes tres componentes clave:

- **Puntuación de rendimiento de la aplicación (puntuación APDEX de la aplicación)**. Derivado de la variación del tiempo de respuesta del servidor de la aplicación.
- **Recurso**del sistema Citrix ADC . Derivado en base a tres componentes más:
  - Uso de CPU
  - Uso de memoria
  - Saturación de tarjeta NIC
- **Recurso**de servidor de aplicaciones . Derivado de dos componentes más:
  - Porcentaje de servicios activos
  - Solicitudes de Cola de Sobretensión

La puntuación de aplicación se calcula a partir de estas puntuaciones, donde la puntuación de recursos del sistema NetScaler ADC y la puntuación de recursos del servidor de aplicaciones se resta de la puntuación de rendimiento de aplicaciones. App Score está disponible para todas las aplicaciones que se definen con los servidores virtuales de equilibrio de carga y conmutación de contenido que se descubren, así como para las aplicaciones personalizadas que defina en el panel de aplicaciones.

Para configurar la puntuación de la aplicación en NetScaler ADM:

1. En Citrix ADM, vaya a **Análisis** > **Configuración** .
2. En la página de **ajustes** , haga clic en **Configurar puntuación de la aplicación** .
3. En la página **Configurar puntuación de aplicación**, introduzca los valores para los siguientes parámetros:

a) **Umbral de cola de sobretensión inferior**. El valor de umbral inferior de la relación entre el número total de conexiones pendientes de envío para el servidor virtual y las conexiones establecidas.

b) **Umbral**de cola de sobretensión más alto . Valor de umbral más alto de la relación entre el número total de conexiones pendientes de envío para el servidor virtual y las conexiones establecidas.

c) **Umbral de CPU bajo (%)**. El valor de umbral inferior del uso total de la CPU en la instancia de Citrix ADC.

d) **Umbral de CPU alto (%)**. El valor de umbral más alto del uso total de la CPU en la instancia de Citrix ADC.

e) **Umbral de memoria bajo (%)**. El valor de umbral inferior del uso total de memoria en la instancia de Citrix ADC.

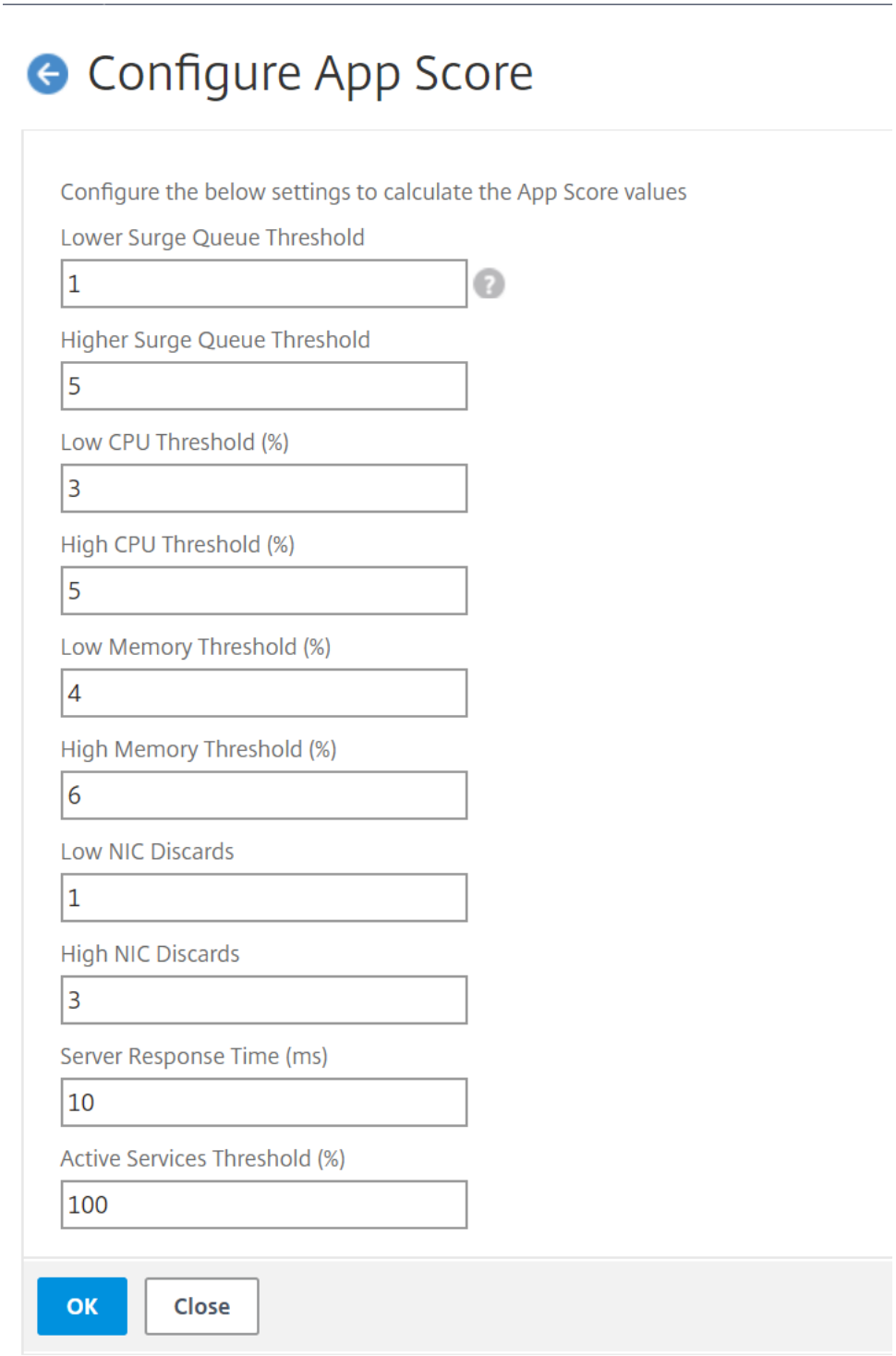
f) **Umbral de memoria alto (%)**. El valor de umbral más alto del uso total de memoria en la instancia de Citrix ADC.

g) **Descartes**de NIC bajos. El valor umbral inferior de los paquetes descartados por las interfaces.

h) **Descartes**de NIC altos. El valor umbral más alto de los paquetes descartados por las interfaces.

i) **Tiempo de respuesta**. Intervalo de tiempo entre el envío de un paquete de solicitud y la recepción del primer paquete de respuesta del servicio configurado en el servidor virtual. El valor predeterminado configurado en Citrix ADM es de 500 ms.

j) **Umbral de servicios activos**. Valor de umbral del porcentaje de servicios que deben estar activos que están enlazados al servidor virtual.



4. Haga clic en **Aceptar**.

Análisis de seguridad de aplicaciones

January 30, 2024

El Panel de seguridad de aplicaciones proporciona una vista holística del estado de seguridad de sus aplicaciones. Por ejemplo, muestra métricas de seguridad clave, como infracciones de seguridad, infracciones de firmas, índices de amenazas. El panel de seguridad de aplicaciones también muestra información relacionada con los ataques, como los ataques de sincronización, los ataques de ventanas pequeñas y los ataques de inundación de DNS para las instancias de Citrix ADC descubiertas.

> **Nota**
>
> Para ver las métricas del panel de seguridad de aplicaciones, AppFlow for Security Insight debe estar habilitado en las instancias de Citrix ADC que quiera supervisar.

Para ver las métricas de seguridad de las instancias de Citrix ADC en el panel de seguridad de la aplicación:

1. En un explorador web, escriba la dirección IP de Citrix Application Delivery Management (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **contraseña** , introduzca las credenciales de administrador.
3. Vaya a **Aplicaciones** > **Panel de seguridad** de aplicaciones y seleccione la dirección IP de la instancia en la lista desplegable **Dispositivos** .

Puede profundizar más en las discrepancias reportadas en App Security Investigator haciendo clic en las burbujas trazadas en el gráfico.

Crear una definición de aplicación

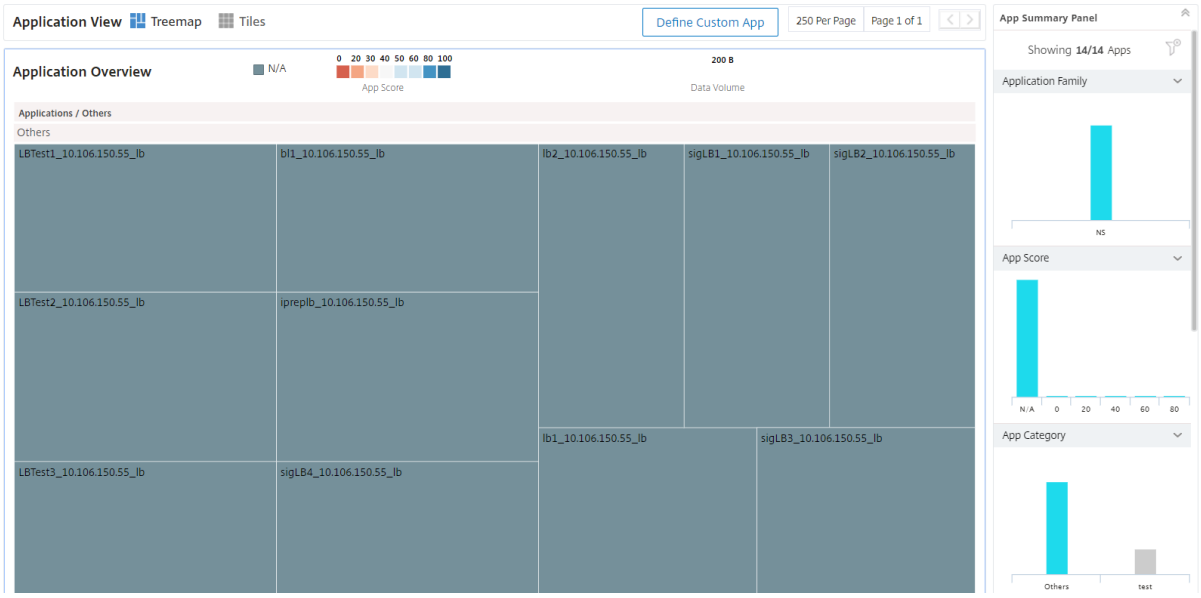
January 30, 2024

Puede definir una aplicación personalizada en función de una colección de aplicaciones descubiertas en Citrix ADM.

En Citrix ADM, al ir a **Application Dashboard** , la página **Descripción** general de la aplicación muestra las aplicaciones predeterminadas. Estas aplicaciones predeterminadas o «aplicaciones discretas» son las 30 aplicaciones para las que tiene las licencias predeterminadas. Estas aplicaciones se descubren al instalar Citrix ADM en su entorno empresarial.

Al crear «aplicaciones personalizadas», las aplicaciones personalizadas sustituyen a las aplicaciones discretas. Las aplicaciones personalizadas se organizan en el panel de control según la categoría que haya elegido al crearlas.

Puede ver estas aplicaciones, tanto descubiertas como personalizadas, de dos maneras: mapa de árbol y mosaicos.



Puede crear una aplicación personalizada a través de una configuración estática o dinámica.

1. **Definición estática de aplicaciones**: en una definición estática, puede definir una aplicación. Esta definición no se actualiza cuando se configuran nuevos servidores virtuales en la instancia de Citrix ADC. Debe actualizar manualmente esta lista para incluir más servidores virtuales.
2. **Definición dinámica de aplicaciones**: en una definición dinámica, puede utilizar uno de los tres criterios que se enumeran a continuación para definir una aplicación:

    a) **Servidores**. Especifique la dirección IP del servidor o servicio, el nombre del servidor o el puerto del servidor backend en el que se ejecutan las aplicaciones. Puede introducir una dirección IP, un intervalo de direcciones IP o una combinación de ambas separadas por comas. Por ejemplo, puede escribir 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

    b) **Servidores**virtuales . Puede especificar una de las siguientes opciones:

        i. Dirección IP del servidor virtual

        ii. Nombre del servidor virtual, o

        iii. Puerto del servidor backend en el que se ejecutan las aplicaciones.

    Puede introducir una dirección IP o un intervalo de direcciones IP o una combinación de ambas separadas por comas. Por ejemplo, puede escribir 10.102.29.20, 10.102.43.10-60, 10.216.43.45.

3. **StyleBooks**. Puede crear aplicaciones personalizadas mediante un StyleBook predeterminado o personalizado que ya esté presente en Citrix ADM. Los StyleBooks simplifican la tarea de administrar configuraciones complejas de NetScaler ADC para sus aplicaciones. Seleccione un StyleBook que esté presente en Citrix ADM y escriba los valores de los parámetros del StyleBook. Citrix ADM crea la configuración (configpack) en las instancias de Citrix ADC de destino en función del StyleBook seleccionado. Citrix ADM también crea una aplicación personalizada que incluye todos los servidores virtuales definidos en el paquete de configuración.

> **Nota**
>
> Se crean una aplicación y un paquete de configuración personalizados si hay suficientes licencias de Citrix ADC disponibles.

Cuando crea una aplicación que cumpla estas condiciones definidas anteriormente en uno de los tres criterios, la aplicación se actualiza automáticamente en el Panel de aplicaciones cuando NetScaler ADM sondea las entidades. Para iniciar una encuesta manualmente, haga clic en Sondear **ahora** en la pestaña **Aplicaciones** .

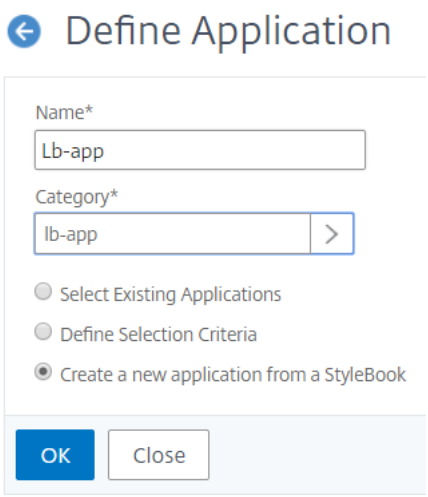
Para crear una aplicación

1. En NetScaler ADM, vaya a **Aplicaciones** > **panel** y haga clic en **Definir aplicación personalizada** para crear una aplicación personalizada.
2. En la ventana **Definir aplicación** , escriba el nombre de la aplicación en el campo **Nombre** .
3. Seleccione la categoría de la aplicación en la sección **Categoría** . NetScaler ADM permite definir categorías para agrupar las aplicaciones definidas por el usuario. También puede agregar más categorías si es necesario.
4. Puede crear una aplicación personalizada en uno de los tres métodos siguientes:
    a) **Seleccione Aplicaciones existentes**. Para seleccionar las aplicaciones existentes, asegúrese de que la opción **Seleccionar aplicaciones existentes** esté habilitada. Elija la aplicación de la lista de la sección **Aplicaciones** . Haga clic en **Agregar aplicaciones** para agregar nuevas aplicaciones a la lista.
    b) **Defina los criterios**de selección . También puede definir un criterio de selección para agregar aplicaciones en Citrix ADM. Puede agregar aplicaciones mediante uno de los tres métodos siguientes:
        i. Especificar la dirección IP del servidor virtual. Puede introducir una dirección IP o un intervalo de direcciones IP o una combinación de ambas separadas por comas.
        ii. Especificar el nombre del servidor en el que se ejecutan las aplicaciones o los servicios.

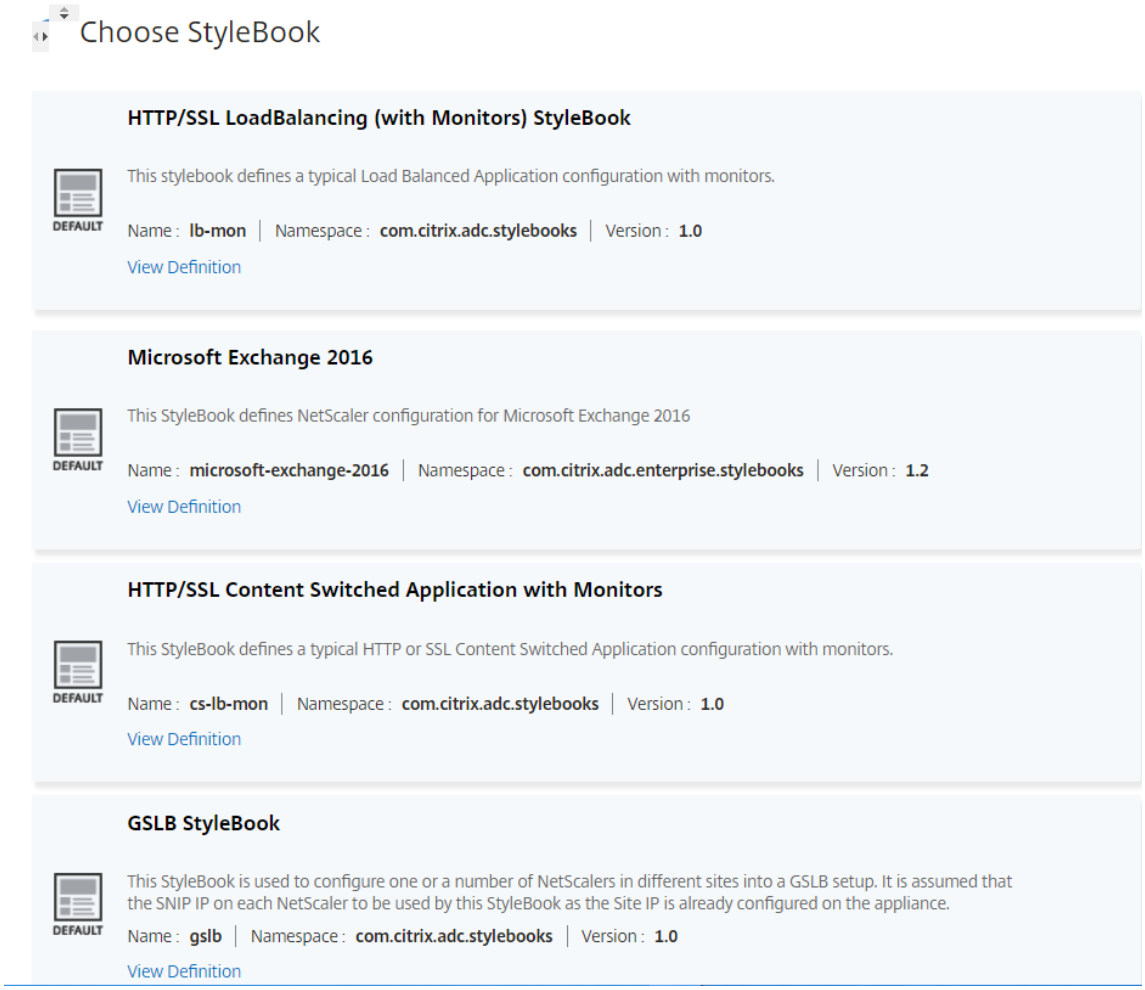
> **Nota**También
>
> puede buscar nombres de servidor mediante extensiones comodín. Por ejemplo, ssl* agregará todos los servidores virtuales ssl a la aplicación.

iii. Especificar el número de puerto en el que la aplicación está escuchando en el servidor seleccionado.

c) **Crea una nueva aplicación desde StyleBook**. Seleccione el StyleBook necesario en Citrix ADM para crear paquetes de configuración en las instancias de Citrix ADC y asociar los servidores virtuales a una aplicación personalizada.



5. Haga clic en **Aceptar**. Si ha optado por crear aplicaciones a partir de StyleBooks, se abre la página **Elegir StyleBook** . Esta página contiene una lista de todos los StyleBooks presentes en NetScaler ADM.



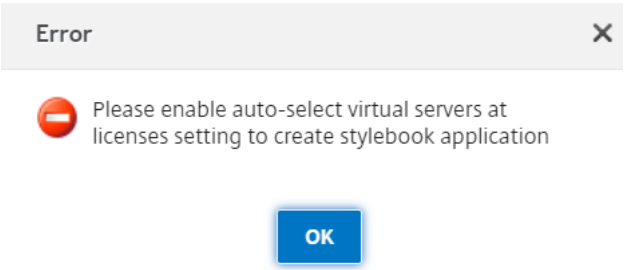
6. Seleccione el StyleBook. El StyleBook se abre como un formulario de interfaz de usuario. Introduzca los valores de todos los parámetros del StyleBook. También puede hacer clic en **View Definition** para ver la construcción del StyleBook antes de usarlo. Para obtener más información sobre cómo usar StyleBooks personalizados o predeterminados, consulte Usar StyleBooks predeterminados.
7. Ahora se crean una aplicación personalizada y el paquete de configuración en las instancias de Citrix ADC que ha seleccionado en la sección de destino del StyleBook.

> **Nota**
>
> Se crean una aplicación y un paquete de configuración personalizados si hay suficientes licencias de Citrix ADM disponibles.

Para seleccionar automáticamente servidores virtuales para licencias

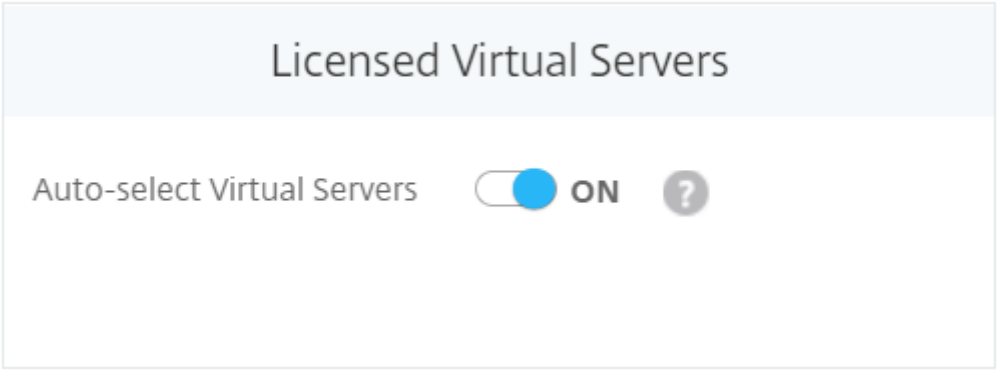
Debe permitir que NetScaler ADM seleccione automáticamente los servidores virtuales para la concesión de licencias cuando utilice la opción StyleBook para crear configuraciones. Si no has activado

la selección automática, es posible que recibas un mensaje de error como el que se muestra en la imagen siguiente:



Para habilitar la selección automática de servidores virtuales:

1. En Citrix ADM, vaya a **Redes** > **Licencias** > **Licencias del sistema**.
2. Haga clic en **Seleccionar automáticamente servidores virtuales** para habilitar la opción en la sección **Servidores virtuales con licencia** .



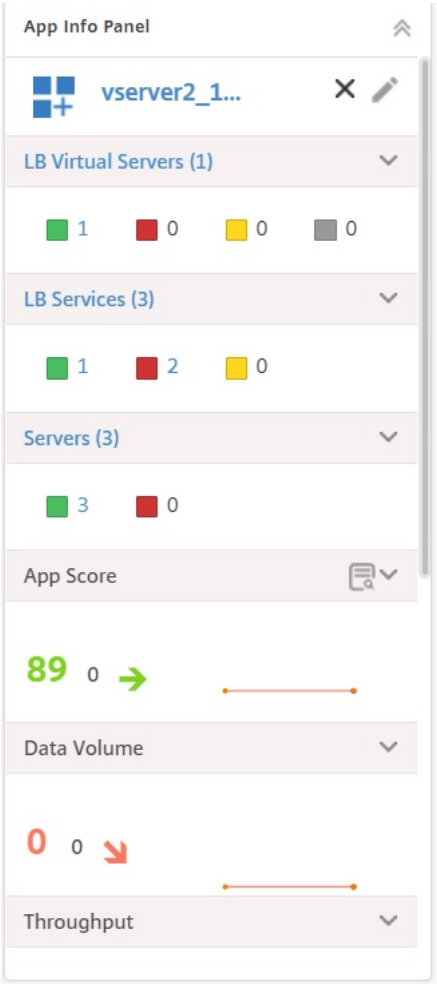
Cuando está habilitado, NetScaler ADM selecciona automáticamente los servidores virtuales a los que se van a conceder licencias. Y cuando no está habilitada, debe seleccionar explícitamente los servidores virtuales.

Para ver los detalles de la aplicación en Citrix ADM

Citrix ADM muestra todos los detalles de una aplicación en un panel independiente en el extremo derecho, conocido como **Panel de información** de la aplicación .

Para ver el panel de información de la aplicación:

1. En Citrix ADM, vaya a **Aplicación** > **Panel** .
2. En la sección **Descripción** general de la aplicación, haga clic en la aplicación de la que desea ver los detalles.



Las entidades enlazadas a la aplicación que ha seleccionado se organizan verticalmente en el panel del **panel de información** de la aplicación . Los cuadros dispuestos verticalmente en el panel muestran lo siguiente:

- nombre de cada entidad
- el número de entidades que están activas
- entidades que están inactivas
- entidades que están fuera de servicio

Las entidades que se muestran aquí son los servidores virtuales, los servicios, los grupos de servicios y los servidores de aplicaciones. El panel también muestra otros datos, como la puntuación de la aplicación, el volumen de datos, el rendimiento, las conexiones de servidor y cliente y las transacciones que se producen en cada aplicación.

Puede ver el recuento de servidores virtuales, servicios y grupos de servicios que se encuentran en diferentes estados para cada aplicación. Puede hacer clic en el nombre de la entidad o en el recuento

mostrado para habilitar o deshabilitar directamente las entidades. También puede habilitar o deshabilitar otras entidades enlazadas, como servidores virtuales, servicios y grupos de servicios.

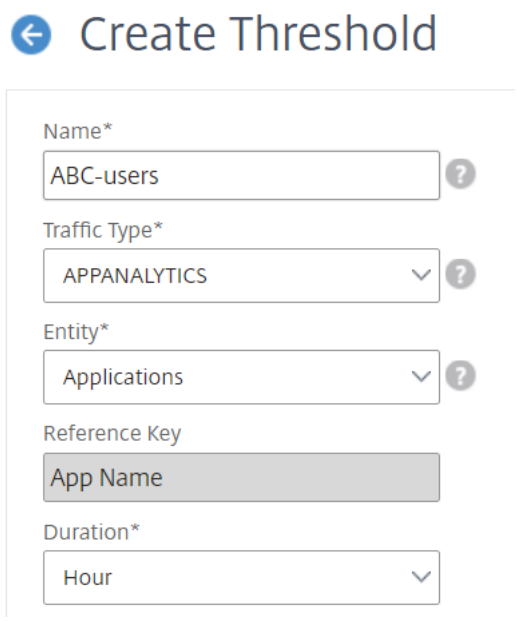
Para obtener más información sobre cómo configurar los servidores de equilibrio de carga, consulte Crear soporte de equilibrio de carga a través de Application Dashboard.

Crear un umbral y una alerta para el análisis de aplicaciones

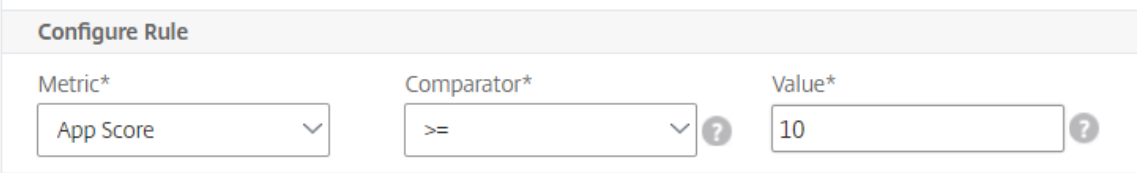
January 30, 2024

El análisis de aplicaciones en Citrix ADM le permite supervisar los distintos tipos de tráfico que pasan por las instancias de Citrix. NetScaler ADM le permite establecer umbrales en varios contadores utilizados para supervisar el tráfico de información. También puede configurar reglas y crear alertas en Citrix ADM.

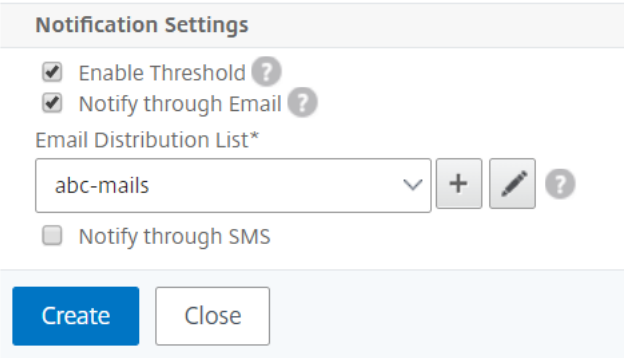
1. En NetScaler ADM, vaya a **Analytics** > **Configuración** > **Umbrales**. En la página **Umbrales** , haga clic en **Agregar** .
2. En la página **Crear umbral** , especifique los siguientes detalles:
    a) **Nombre**. Escriba un nombre para crear un evento para el que Citrix ADM genere una alerta.
    b) ****Tipo** de tráfico **. En el cuadro de lista, seleccione APPANALYTICS.
    c) **Entidad**. En el cuadro de lista, seleccione la categoría o el tipo de recurso. De forma predeterminada, “aplicaciones”se selecciona como entidad.
    d) ****Clave** de referencia **. Se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.
    e) **Duración**. En el cuadro de lista, seleccione el intervalo de tiempo durante el que quiere supervisar la entidad. Puede supervisar las entidades durante una hora, un día o una semana de duración.



3. En la sección **Configurar regla** , cree una regla seleccionando la métrica **App Score** , un comparador obligatorio, y proporcione un valor de umbral.



4. Haga clic en **Habilitar Threshold** para permitir que Citrix ADM comience a supervisar las entidades.
5. Opcionalmente, configure acciones como notificaciones por correo electrónico y notificaciones por SMS. Haga clic en **Crear**.



StyleBooks

January 30, 2024

Los StyleBooks simplifican la tarea de administrar configuraciones complejas de NetScaler ADC para sus aplicaciones. Un StyleBook es una plantilla que puede utilizar para crear y administrar configuraciones de NetScaler ADC. Puede crear un StyleBook para configurar una función específica de NetScaler ADC, o puede diseñar un StyleBook para crear configuraciones para la implementación de una aplicación empresarial, como Microsoft Exchange o Lync.

Los StyleBooks se ajustan perfectamente a los principios de la infraestructura como código que practican los equipos de DevOps, donde las configuraciones son declarativas y se controlan por versiones. Las configuraciones también se repiten y se implementan como un todo. Los StyleBooks ofrecen las siguientes ventajas:

- **Declarativo**: Los StyleBooks se escriben en una sintaxis declarativa en lugar de imperativa. Los StyleBooks le permiten centrarse en describir el resultado o el "estado deseado"de la configuración en lugar de las instrucciones paso a paso sobre cómo lograrlo en una instancia específica de NetScaler ADC. Citrix Application Delivery Management (ADM) calcula la diferencia entre el estado existente en un Citrix ADC y el estado deseado que especificó, y realiza las modificaciones necesarias en la infraestructura. Dado que los StyleBooks utilizan una sintaxis declarativa, escrita en YAML, los componentes de un StyleBook se pueden especificar en cualquier orden, y NetScaler ADM determina el orden correcto en función de sus dependencias calculadas.
- **Atomic**: Cuando usa StyleBooks para implementar configuraciones, se implementa la configuración completa o no se implementa ninguna de ellas, lo que garantiza que la infraestructura se mantenga siempre en un estado coherente.
- **Versionado**: un StyleBook tiene un nombre, un espacio de nombres y un número de versión que lo distingue de forma única de cualquier otro StyleBook del sistema. Cualquier modificación de un StyleBook requiere una actualización de su número de versión (o de su nombre o espacio de nombres) para mantener este carácter único. La actualización de la versión también permite mantener varias versiones del mismo StyleBook.
- **Composable**: una vez definido un StyleBook, el StyleBook se puede usar como unidad para crear otros StyleBooks. Puede evitar repetir los patrones de configuración comunes. También le permite establecer componentes básicos estándar en su organización. Dado que los StyleBooks están versionados, los cambios en los StyleBooks existentes dan como resultado nuevos StyleBooks, lo que garantiza que los StyleBooks dependientes nunca se rompan
- **Centrado en aplicaciones**: los StyleBooks se pueden utilizar para definir la configuración de NetScaler ADC de una aplicación completa. La configuración de la aplicación se puede abstraer mediante el uso de parámetros. Por lo tanto, los usuarios que crean configuraciones a partir

de un StyleBook pueden interactuar con una interfaz sencilla que consiste en rellenar algunos parámetros para crear lo que puede ser una configuración compleja de Citrix ADC. Las configuraciones creadas a partir de StyleBooks no están vinculadas a la infraestructura. De este modo, se puede implementar una única configuración en uno o varios ADC de Citrix y también se puede mover de una instancia a otra.

- **Interfaz de usuario generada automáticamente**: NetScaler ADM genera automáticamente formularios de interfaz de usuario utilizados para rellenar los parámetros del StyleBook cuando se realiza la configuración mediante la interfaz gráfica de usuario de NetScaler ADM. Los autores de StyleBook no necesitan aprender un nuevo lenguaje de interfaz gráfica de usuario ni crear páginas y formularios de interfaz de usuario por separado.
- Basado en**API:**todas las operaciones de configuración se admiten mediante la GUI de NetScaler ADM o mediante las API REST. Las API se pueden usar en modo sincrónico o asíncrono. Además de las tareas de configuración, las API de StyleBooks también permiten descubrir el esquema (descripción de los parámetros) de cualquier StyleBook en tiempo de ejecución.

Puede utilizar un StyleBook para crear varias configuraciones. Cada configuración se guarda como un paquete de configuración. Por ejemplo, considere que tiene un StyleBook que define una configuración típica de la aplicación de equilibrio de carga HTTP. Puede crear una configuración con valores para las entidades de equilibrio de carga y ejecutarla en una instancia de Citrix ADC. Esta configuración se guarda como un paquete de configuración. Puede usar el mismo StyleBook para crear otra configuración con valores diferentes y ejecutarla en la misma instancia de Citrix ADC o en una instancia diferente. Se crea un nuevo paquete de configuración para esta configuración. Un paquete de configuración se guarda tanto en Citrix ADM como en la instancia de Citrix ADC en la que se ejecuta la configuración.

Puede utilizar StyleBooks predeterminados, incluidos con NetScaler ADM, para crear configuraciones para su implementación, o diseñar sus propios StyleBooks e importarlos a NetScaler ADM. Puede usar los StyleBooks para crear configuraciones mediante la GUI de NetScaler ADM o mediante las API.

Este documento incluye la siguiente información:

- Cómo ver StyleBooks
- StyleBooks predeterminados
- Libros de estilo desarrollados para aplicaciones empresariales
- StyleBooks personalizados
- APIs en StyleBooks
- Gramática de StyleBooks

Grupos de StyleBook

January 30, 2024

Los StyleBooks de Citrix Application Delivery Management (ADM) se pueden agrupar de dos maneras. Se pueden agrupar como StyleBooks predeterminados o StyleBooks personalizados. O también se pueden agrupar como StyleBooks públicos o privados. En Citrix ADM, puede ver todos los StyleBooks que están presentes en el sistema. Citrix ADM también le permite ordenar y ver los StyleBooks. También puede ver una visualización gráfica de cómo los StyleBooks están conectados entre sí.

Este documento también le indica cómo descargar y eliminar StyleBooks personalizados. Puede descargar un StyleBook personalizado para realizar modificaciones o crear un nuevo StyleBook basado en el anterior. También puede eliminar un StyleBook personalizado.

StyleBooks predeterminados y personalizados

- Los StyleBooks predeterminados son los StyleBooks que están presentes en el sistema de archivos Citrix ADM y permiten crear configuraciones que puede implementar en las instancias de Citrix ADC.
- Los StyleBooks personalizados son sus propios StyleBooks que puede escribir e importar a Citrix ADM y crear objetos de configuración.

Los StyleBooks predeterminados y personalizados pueden ser públicos o privados.

StyleBooks públicos y privados

Los StyleBooks a partir de los que puede crear paquetes de configuración para implementarlos en las instancias de Citrix ADC se pueden clasificar como StyleBooks «públicos». Es decir, todos están disponibles para su uso directo para crear configuraciones.

Sin embargo, algunos StyleBooks se utilizan como bloques de construcción para otros StyleBooks. Estos bloques de creación son los StyleBooks integrados que componen los StyleBooks predeterminados. Estos StyleBooks se denominan StyleBooks «privados». Aunque no se utilizan directamente para crear paquetes de configuración en las instancias, es posible que desee mostrar estos StyleBooks en Citrix ADM. Para marcar un StyleBook como privado, puede usar el atributo private para evitar que un StyleBook aparezca en Citrix ADM.

```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration and is a building block to build other load balancing
   configurations.
display-name: Load Balancing Configuration
```



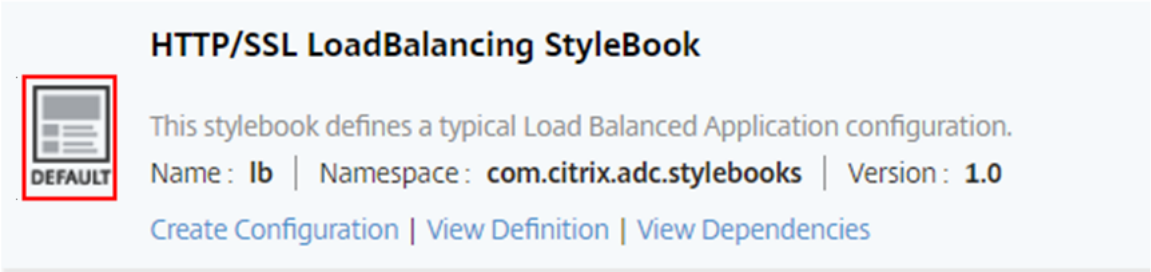
```
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Visualización de StyleBooks

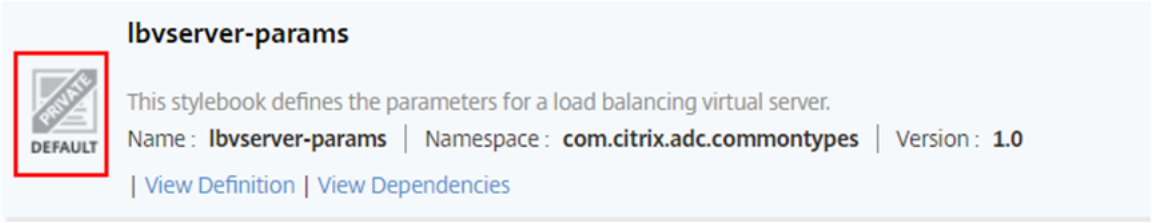
La cantidad de StyleBooks, tanto predeterminados como privados, está aumentando en Citrix ADM. Es posible que desee buscar el StyleBook en particular al que desea acceder. Es posible que también desee ver ambos tipos de StyleBooks por separado.

En Citrix ADM, cuando vaya a **Aplicaciones** > **StyleBooks** , puede ver una lista de los StyleBooks que están presentes en el sistema.

Un StyleBook público predeterminado tiene el siguiente icono en su panel:

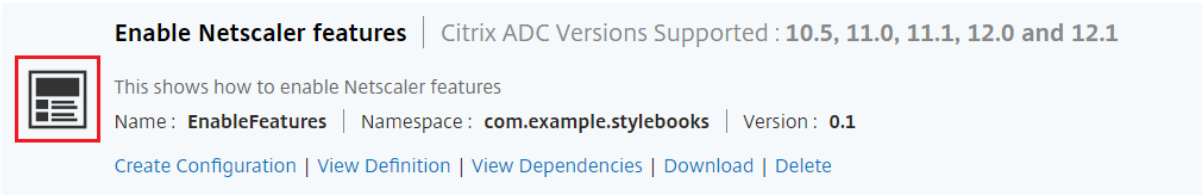


Mientras que un StyleBook privado predeterminado tiene un icono que lo declara como un StyleBook privado:

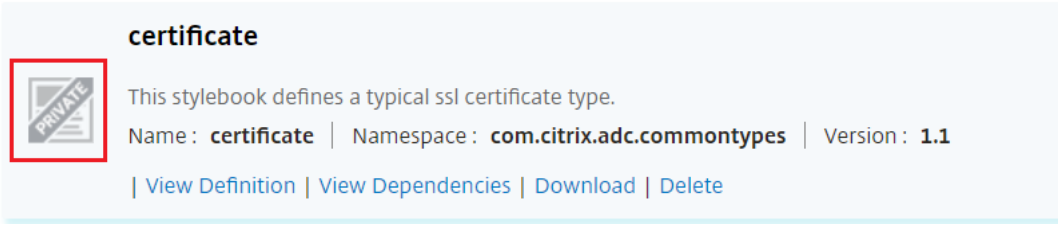


Aunque puede ver la definición y las dependencias de un StyleBook privado, no puede crear un paquete de configuración a partir de un StyleBook privado. Aún puede usar un StyleBook privado en su propio StyleBook.

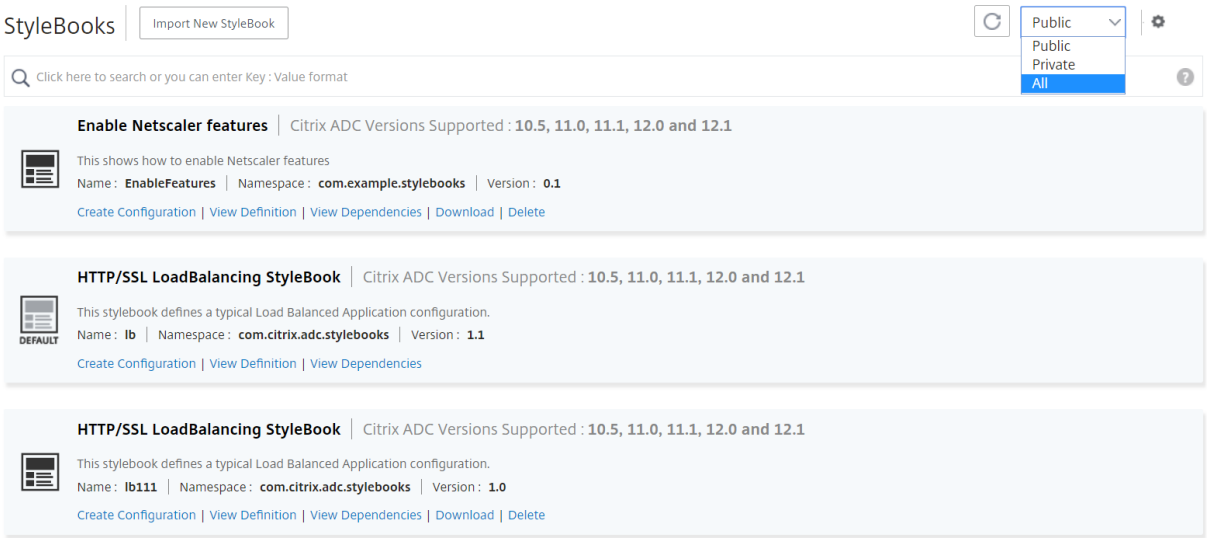
Un StyleBook público personalizado tiene un icono diferente como se muestra en la siguiente imagen:



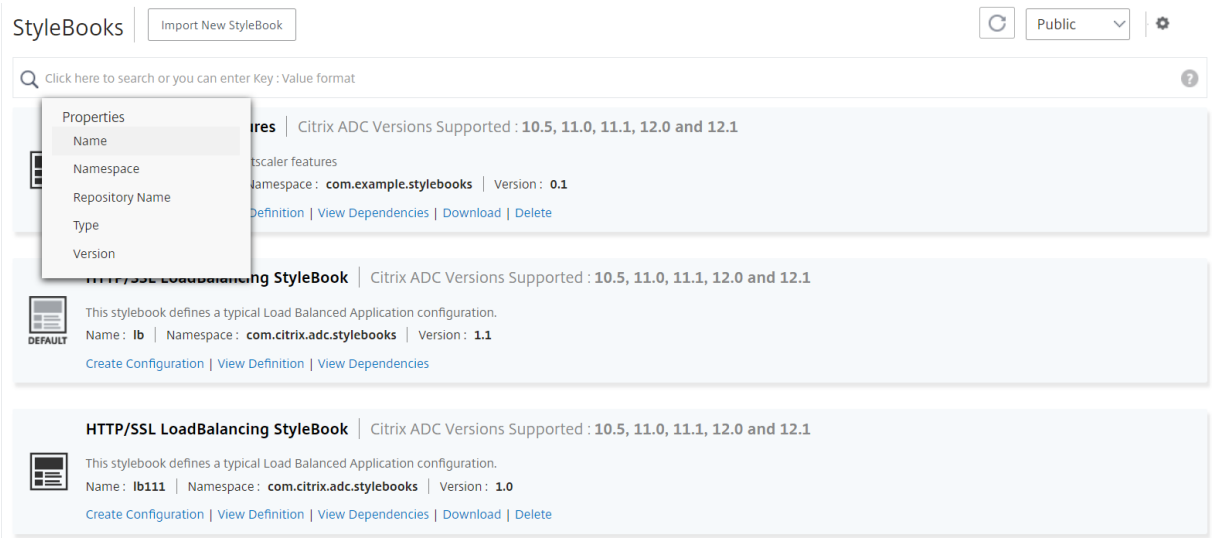
Mientras, aparece un StyleBook privado personalizado con este icono:



En la parte superior derecha de la página, puede ver una opción para ordenar los StyleBooks. Hay tres opciones: todos los StyleBooks, públicos o privados. Haga clic en una de las opciones.



También puede buscar un StyleBook en particular haciendo clic en el icono de búsqueda. Las tres opciones de búsqueda disponibles son nombre, espacio de nombres y versión. La operación de búsqueda no distingue entre mayúsculas y minúsculas.



Visualización de dependencias de StyleBook

Citrix ADM le permite ver una visualización gráfica de cómo los StyleBooks están conectados entre sí.

En Citrix ADM, puede utilizar los StyleBooks predeterminados para crear configuraciones para la implementación. También puede diseñar sus propios StyleBooks e importarlos a Citrix ADM.

Una función importante y poderosa de StyleBooks es que se pueden usar como bloques de construcción para otros StyleBooks. Puede importar un StyleBook a otro StyleBook. Un Stylebook importado se declara como un tipo y los componentes o parámetros del segundo StyleBook lo utilizan.

Un StyleBook utilizado por otros StyleBooks no se puede eliminar del sistema. Sin embargo, una visualización gráfica de los StyleBooks le permite saber qué StyleBooks impiden la eliminación de un StyleBook. Al observar el gráfico, es posible ver las relaciones entre varios StyleBooks.

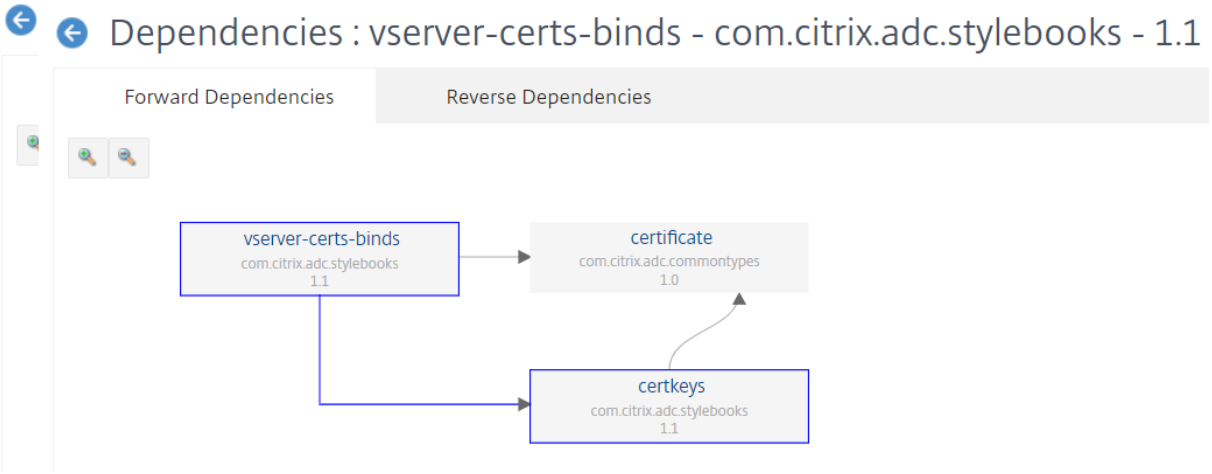
Para ver las dependencias de StyleBook

En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks**. La página StyleBooks muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplázate hacia abajo y encuentra tu StyleBook. El panel StyleBook muestra enlaces para crear una configuración, ver la definición de StyleBook y ver las dependencias de StyleBook. Haga clic en **Ver dependencias**.

Reenviar dependencias

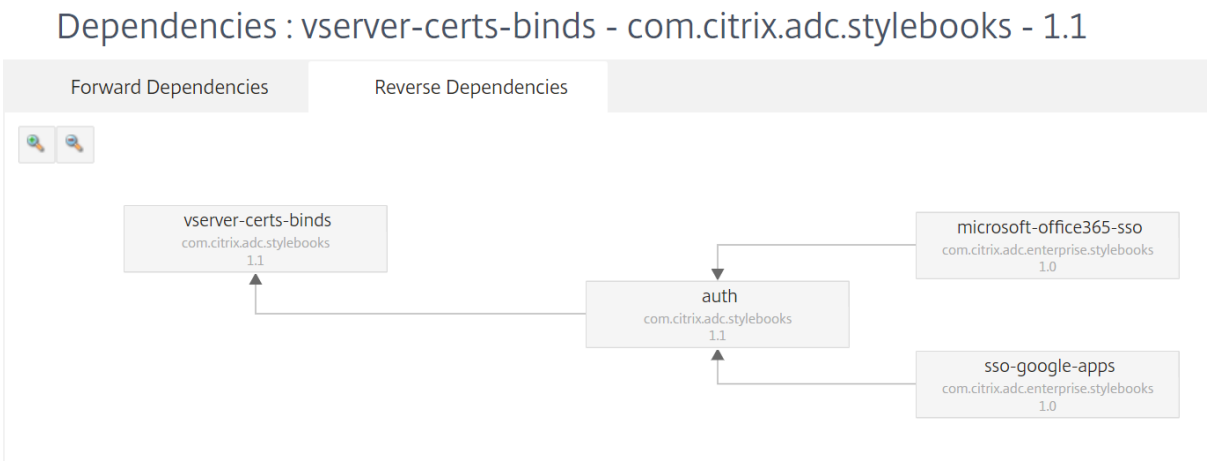
La ficha Forward Dependencies le permite ver los diferentes StyleBooks predeterminados que utiliza su StyleBook. Siga las flechas para encontrar el StyleBook que utiliza un StyleBook. Al apuntar con

el mouse a una de las flechas, se resaltan la flecha y los StyleBooks que están conectados entre sí. También puede hacer clic en los nombres de StyleBook para ver la definición de ese StyleBook.



Dependencias inversas

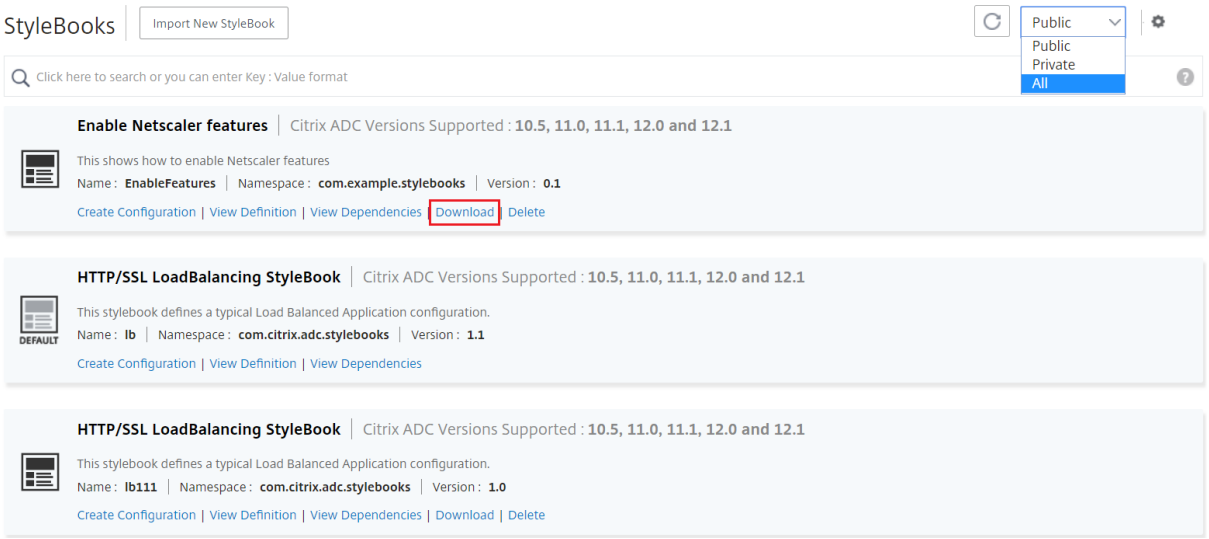
La pestaña Dependencias inversas le permite ver gráficamente los StyleBooks que utilizan su StyleBook. Si sigue las flechas, puede ver que todos los StyleBooks de la pantalla apuntan hacia su StyleBook. Algunos StyleBooks pueden estar mediante el StyleBook directamente y algunos StyleBooks pueden estar mediante el StyleBook a través de otro StyleBook.



Descargar StyleBooks personalizados

Para descargar Stylebooks personalizados de Citrix ADM, vaya a **Aplicaciones** > **StyleBooks** > **Configuraciones** . En la lista de StyleBooks que se muestran en el panel derecho, los StyleBooks definidos a medida tienen la opción de descargarlos. Haga clic en **Download**. Si el StyleBook tiene StyleBooks personalizados dependientes, incluso esos StyleBooks se descargan a su sistema.

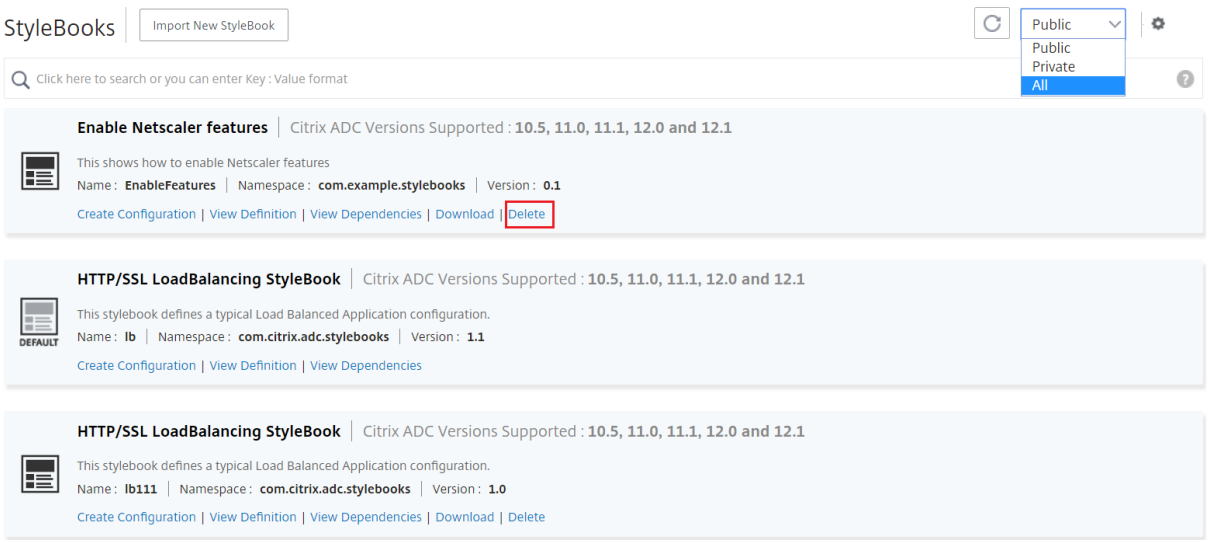
> **Nota**No
>
> puede descargar StyleBooks predeterminados o personalizados que estén marcados como públicos o privados.



> **Nota**
>
> No puede descargar los StyleBooks predeterminados de Citrix ADM. Sin embargo, puede ver sus definiciones y dependencias haciendo clic en los enlaces **Ver**definición**y Ver dependencias** del panel StyleBook.

Eliminar StyleBooks personalizados

También puede eliminar los StyleBooks personalizados haciendo clic en el icono «X» en el lado derecho del panel StyleBook. Una ventana emergente le pide que confirme si quiere quitar StyleBook de Citrix ADM. Si el StyleBook usa otros StyleBooks personalizados (que no utilizan otros StyleBooks), también puede optar por eliminarlos seleccionando la casilla de verificación.



> **Nota**
>
> No puede eliminar un StyleBook personalizado que tenga otros StyleBooks en NetScaler ADM que dependan de él.

Importar y sincronizar StyleBooks desde el repositorio de GitHub

January 30, 2024

Ten en cuenta que estás usando procesos de CI/CD para tu desarrollo o que estás administrando todos los objetos de implementación en GitHub. Es posible que haya creado varios StyleBooks para implementar sus configuraciones de Citrix ADC y que esté administrando los StyleBooks en los repositorios de GitHub. Ahora puede importar directamente estos StyleBooks a Citrix Applications and Delivery Management (ADM). No es necesario copiarlos manualmente de GitHub y cargarlos en Citrix ADM.

Ahora puede definir un repositorio en Citrix ADM que represente un repositorio de GitHub proporcionando la URL del repositorio de GitHub. Debes proporcionar tu nombre de usuario y contraseña (o token de API) creados en GitHub. Esto significa que solo los usuarios autorizados que tengan una cuenta válida en GitHub pueden importar y sincronizar StyleBooks.

Después de crear el repositorio, puede sincronizar NetScaler ADM con su repositorio de GitHub. Citrix ADM importa los StyleBooks que se encuentran en ese repositorio, los valida y los agrega a la lista de StyleBooks de Citrix ADM. Los StyleBooks no se agregan a NetScaler ADM si no se validan. Debes corregir los errores y confirmar las versiones actualizadas en tu repositorio de GitHub. Más adelante, puede intentar importarlos o sincronizarlos de nuevo en NetScaler ADM.

> **Nota**
>
> - Actualmente, solo puede importar y sincronizar StyleBooks que no tengan StyleBooks dependientes asociados a ellos. Es decir, el StyleBook debe tener todas las configuraciones que necesita para definirse en un solo archivo.
> - La sincronización desde un repositorio de GitHub debe iniciarse manualmente desde la GUI o la API de Citrix ADM. Es decir, actualmente, la importación de StyleBooks no se realiza automáticamente en función de la actividad de confirmación de GitHub.
>
> Actualmente, solo puede importar archivos de StyleBooks desde la rama maestra.

Requisitos previos

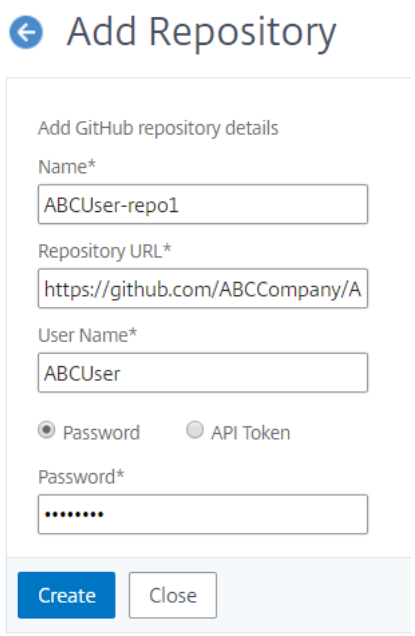
- Debes tener una cuenta válida en GitHub.
- Los archivos StyleBook deben existir en la carpeta raíz de la rama maestra del repositorio de GitHub.

Agregar un repositorio e importar StyleBooks desde GitHub

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuraciones** > **Repositorios** .
2. Haga clic en **Agregar**. En la ventana **Agregar Repositorio**, introduzca los siguientes parámetros:
   - **Nombre**. Escriba el nombre del repositorio. Este nombre puede ser el mismo que el nombre del repositorio en GitHub o uno diferente.
   - **URL del repositorio**. Escribe la URL del repositorio de GitHub.
   - **Nombre de usuario y contraseña**. Escriba el nombre de usuario y la contraseña con la que acceda a la cuenta de GitHub.

   > **Nota**También puedes proporcionar el token de API en lugar de una contraseña. Los tokens de API se pueden usar en lugar de una contraseña para GitHub a través de HTTPS. También puede utilizarlos para autenticarse en la API mediante la autenticación básica.

3. Haga clic en **Crear**.



El repositorio se crea en NetScaler ADM.

4. **Para importar o sincronizar StyleBooks, seleccione el repositorio en la página**Repositorios**y haga clic en Sincronizar.**

Las otras acciones que puede utilizar aquí son:

- **Modificar**. Puede modificar la URL del repositorio, el nombre de usuario y la contraseña (o el token de API).
- **Eliminar**. Puede eliminar el repositorio junto con todos los StyleBooks presentes en Citrix ADM que se importaron anteriormente desde ese repositorio de GitHub.

  > **Nota**No
  >
  > puede eliminar un repositorio de NetScaler ADM si tiene StyleBooks que tengan Config-Packs asociados a ellos.

- **Restablecer**. Puede eliminar todos los StyleBooks de Citrix ADM sincronizados de ese repositorio sin eliminar realmente la entrada del repositorio de Citrix ADM.
- **Lista de archivos**. Puede ver una lista de todos los StyleBooks presentes en Citrix ADM que se originan en el repositorio de GitHub.

Usar StyleBooks predeterminados

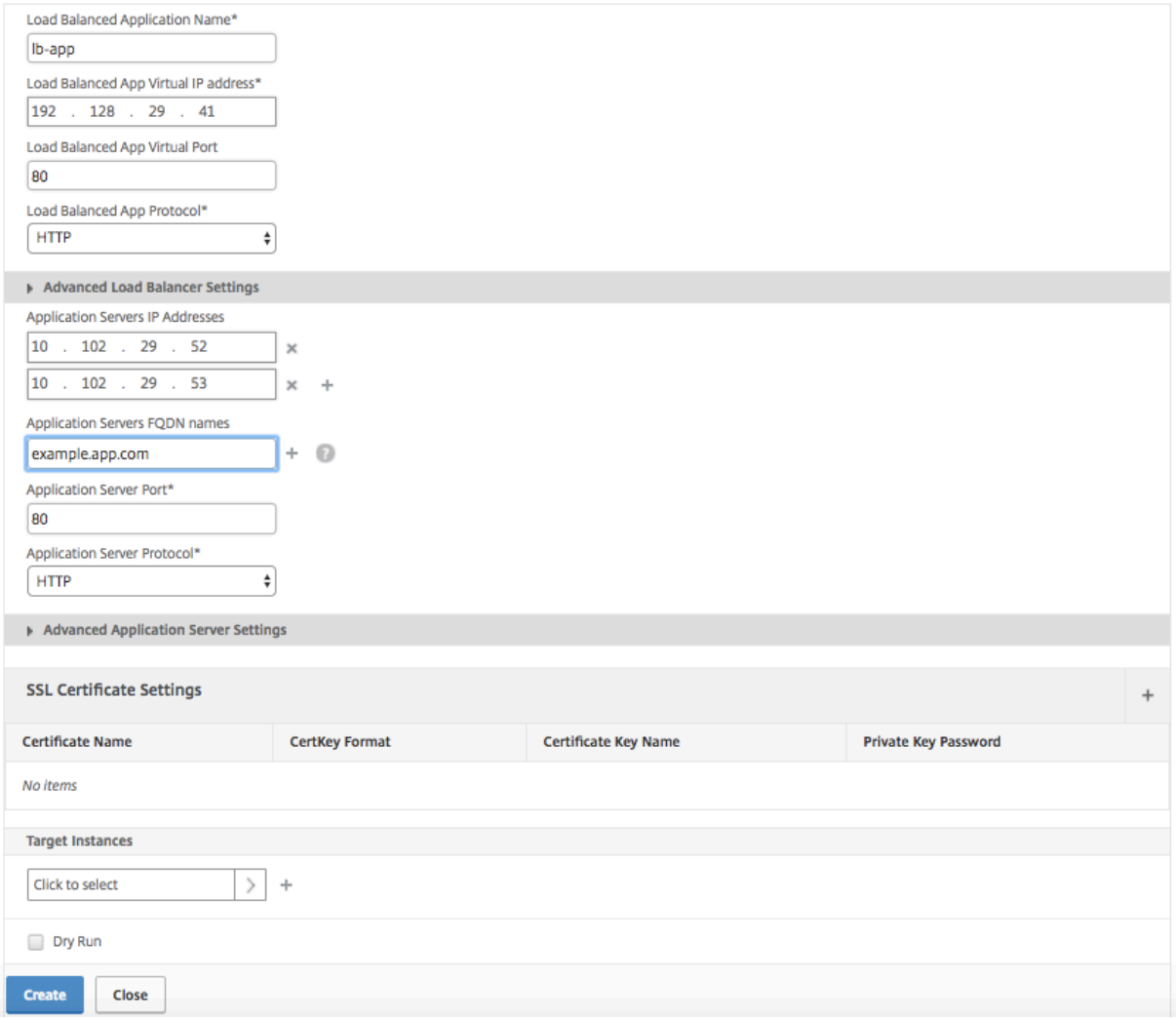
January 30, 2024

Se proporciona un conjunto de StyleBooks predeterminados con NetScaler Application Delivery Management (ADM). Cuando utiliza un StyleBook predeterminado, debe especificar valores para los parámetros en el StyleBook y seleccionar las direcciones IP de las instancias de NetScaler ADC en las que quiere ejecutar la configuración. Después de enviar la configuración, NetScaler ADM valida los valores de los parámetros que ha especificado, crea un gráfico de la configuración, se conecta a las instancias de NetScaler ADC y ejecuta la configuración en las instancias.

Para crear una configuración a partir de un StyleBook predeterminado

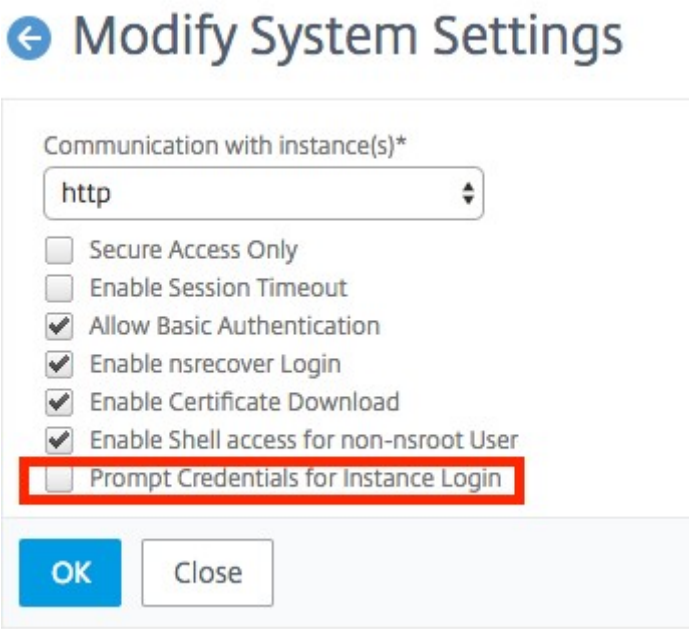
1.Vaya a **Aplicaciones** > **Configuraciones > StyleBooks**. La página StyleBooks muestra todos los StyleBooks de NetScaler ADM. Esta lista incluye los StyleBooks predeterminados y personalizados. Puede escribir el nombre del StyleBook en el campo de búsqueda y presionar la tecla **Intro**. De lo contrario, puede desplazarse hacia abajo en la lista para encontrar el Stylebook.

2. Haga clic en **Crear configuración**. Especifique los valores necesarios para los parámetros.

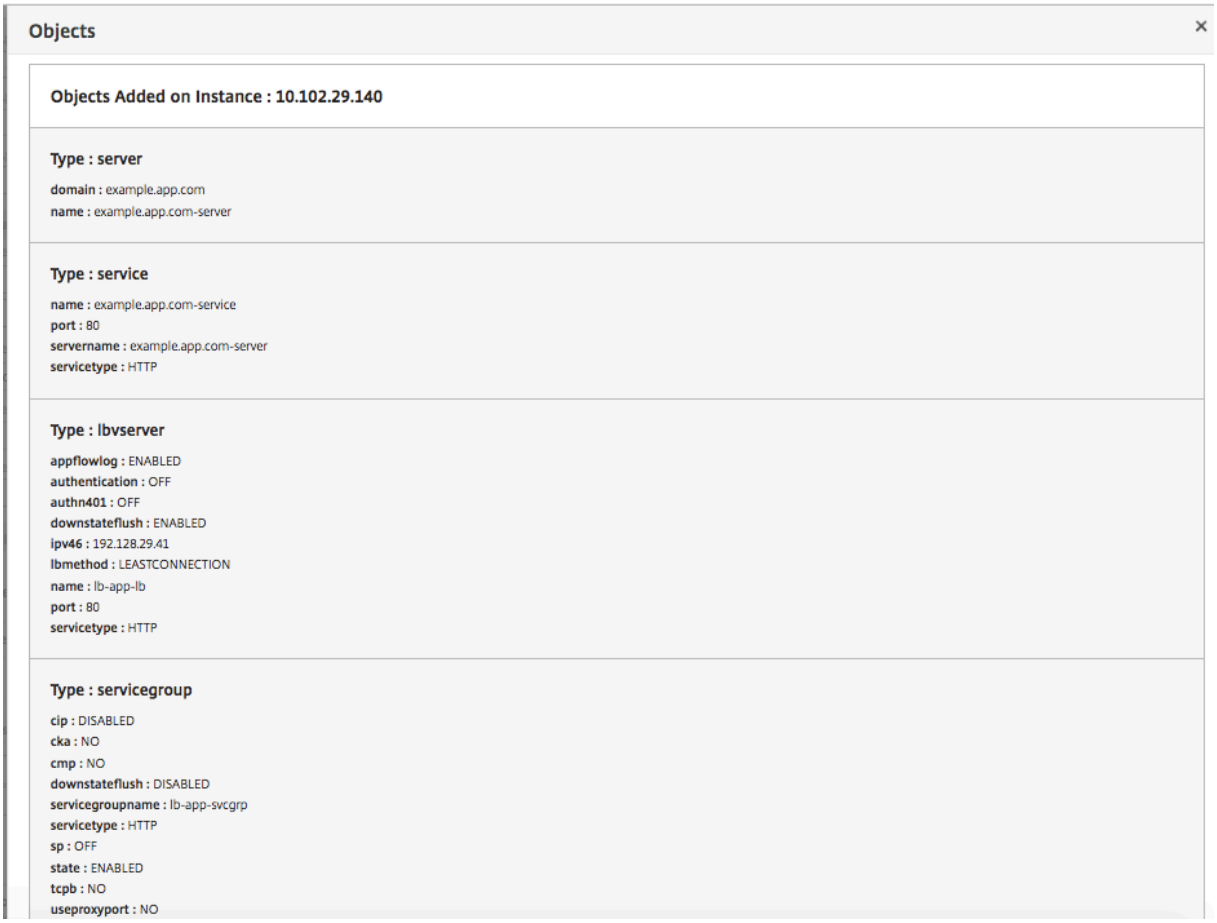


3. En **Instancias de destino**, haga clic en y seleccione la dirección IP de la instancia de NetScaler ADC en la que quiere ejecutar la configuración. Si quiere ejecutar esta configuración en varias instancias, haga clic en "+"para agregar más instancias.

Si la opción Solicitar **credenciales para iniciar sesión en la instancia** está habilitada en **Citrix ADM** > **Sistema** > **Cambiar la configuración del**sistema**>** **Modificar** la configuración del sistema , se le solicitarán las credenciales de la instancia de Citrix ADC al ejecutar las configuraciones en las instancias de Citrix ADC seleccionadas. De lo contrario, NetScaler ADM utiliza las credenciales de instancia almacenadas en el perfil de instancia para iniciar sesión en la instancia.



Si quiere probar o validar la configuración antes de ejecutarla en la instancia de NetScaler ADC, seleccione **Simulacro** y, a continuación, haga clic en **Crear**. Si la configuración es válida, se muestran los objetos creados sobre la base de los valores proporcionados.



4. Desmarque la casilla **Simulacro**y haga clic en **Crear** para crear la configuración y ejecutar la configuración en la instancia de NetScaler ADC. La configuración de StyleBook que ha creado aparece en la lista de configuraciones, como se muestra a continuación.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

Ahora puede examinar, actualizar o eliminar este paquete de configuración mediante NetScaler ADM.

Ocultar todos los StyleBooks predeterminados

January 30, 2024

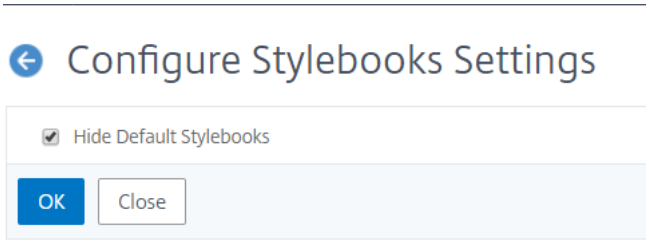
Citrix ADM muestra todos los StyleBooks presentes en el sistema de carpetas Citrix ADM. La lista de StyleBooks incluye StyleBooks predeterminados y personalizados que pueden ser tanto privados

como públicos. Como administrador, es posible que quiera ocultar todos los StyleBooks predeterminados. Puede permitir que sus usuarios vean y accedan solo a los StyleBooks personalizados creados por usted o por los usuarios.

NetScaler ADM le permite mostrar sus StyleBooks personalizados y ocultar todos los StyleBooks predeterminados que se envían con NetScaler ADM. Se proporciona una nueva opción de interfaz gráfica de usuario donde puede ocultar todos los StyleBooks predeterminados.

Para ocultar todos los StyleBooks predeterminados:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones > Configuración**.
2. La página de **configuración** muestra información sobre si los StyleBooks predeterminados están visibles para los usuarios o no.
3. Para ocultar los StyleBooks predeterminados, haga clic en el icono de edición situado en la parte superior derecha.
4. En la página **Configurar los ajustes de StyleBook**, seleccione la opción **Ocultar libros de estilos predeterminados**.
5. Haga clic en **Aceptar**.



Los usuarios seguirán viendo la página **Configurar los ajustes de StyleBook** si no ha optado por ocultarla mediante la función RBAC. Es posible que los usuarios sigan teniendo la opción de mostrar los StyleBooks predeterminados.

Para ocultar la página **Configurar ajustes de StyleBook**, debe crear una directiva y asignarla a los usuarios que no deberían ver los StyleBooks predeterminados.

Para crear una directiva RBAC:

1. En NetScaler ADM, vaya a **Cuenta** > **Administración de usuarios** > **Directivas de acceso**.
2. Haga clic en **Add** para crear una directiva.
3. Introduzca el nombre de la directiva.
4. En la sección **Permisos**, asegúrese de que no esté seleccionada la opción **Todas** > **Aplicaciones** > **Configuración> Configuración**y haga clic en**Aceptar**.

Después de crear directivas, debe crear roles, enlazar cada rol a una o varias directivas y asignar roles a grupos de usuarios. Para obtener más información sobre cómo asociar directivas a los usuarios, consulte Configuración del control de acceso basado en funciones.

StyleBook del SSO de Google Apps

January 30, 2024

Google Apps es un conjunto de herramientas, software y productos de computación en la nube, productividad y colaboración desarrollados por Google. El inicio de sesión único (SSO) permite a los usuarios acceder a todas sus aplicaciones empresariales en la nube, incluidos los administradores que inician sesión en la consola de administración, iniciando sesión una vez para todos los servicios mediante sus credenciales de empresa.

El SSO Google Apps StyleBook de NetScaler ADM le permite habilitar el SSO para Google Apps a través de instancias de NetScaler ADC. StyleBook configura la instancia de NetScaler ADC como un proveedor de identidad SAML para autenticar a los usuarios para que accedan a Google Apps.

Al habilitar el SSO para las aplicaciones de Google en una instancia de NetScaler ADC mediante este StyleBook, se obtienen los siguientes pasos:

1. Configuración del servidor virtual de autenticación
2. Configuración de una directiva y un perfil de IDP de SAML
3. Vinculación de la directiva y el perfil al servidor virtual de autenticación
4. Configuración de un servidor y una directiva de autenticación LDAP en la instancia
5. Enlazar el servidor y la directiva de autenticación LDAP a su servidor virtual de autenticación configurado en la instancia

Detalles de configuración:

En la siguiente tabla se enumeran las versiones de software mínimas necesarias para que esta integración funcione correctamente. El proceso de integración también debería funcionar con versiones superiores del mismo.

Producto	Versión mínima requerida
Citrix ADC	Versión 11.0, licencia Enterprise/Platinum

En las instrucciones siguientes se supone que ya ha creado las entradas DNS externas y/o internas adecuadas para redirigir las solicitudes de autenticación a una dirección IP supervisada por NetScaler ADC.

Implementación de configuraciones de StyleBook de aplicaciones de Google SSO:

La siguiente tarea le ayudará a implementar el SSO de Google Apps StyleBook de Microsoft en su red empresarial.

Para implementar aplicaciones de SSO Google StyleBook

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** >**StyleBooks**. La página StyleBooks muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplázate hacia abajo y busca **SSO Google Apps StyleBook**. Haga clic en **Crear configuración**.
2. El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.
3. Introduzca valores para los siguientes parámetros:

    a) **Nombre de la aplicación**. Nombre de la configuración de SSO de Google Apps que se implementará en la red.

    b) **Autenticación Dirección IP virtual**. Dirección IP virtual utilizada por el servidor virtual AAA al que está vinculada la política de IdP de SAML de Google Apps.

    c) **Expresión de regla SAML**. De forma predeterminada, se utiliza la siguiente expresión de directiva (PI) de Citrix ADC: HTTP.REQ.HEADER («Referer») .CONTAINS («google»). Actualice este campo con otra expresión si su requisito es diferente. Esta expresión de política coincide con el tráfico al que se aplican estas configuraciones de SSO de SAML y garantiza que el encabezado de referencia proviene de un dominio de Google.

4. La sección Configuración de IDP de SAML le permite configurar su instancia de Citrix ADC como proveedor de identidades SAML mediante la creación del perfil y la directiva de IDP de SAML que utiliza el servidor virtual AAA creado en el paso 3.

    a) **Nombre del emisor SAML**. En este campo, introduzca el FQDN público de su servidor virtual de autenticación. Ejemplo:`https://<Citrix ADC Auth VIP>/saml/login`

    b) **ID de proveedor de servicios (SP) SAML**. (opcional) El proveedor de identidades NetScaler ADC acepta solicitudes de autenticación SAML de un nombre de emisor que coincida con este ID.

    c) **URL de Assertion Consumer Service** Introduzca la URL del proveedor de servicios a la que el proveedor de identidades de NetScaler ADC debe enviar las afirmaciones SAML después de una autenticación de usuario exitosa. La URL del servicio al consumidor de afirmación se puede iniciar en el sitio del servidor del proveedor de identidad o en el sitio del proveedor de servicios.

d) Hay otros campos opcionales que puede introducir en esta sección. Por ejemplo, puede configurar las siguientes opciones:

i. Perfil de enlace SAML (el perfil predeterminado es "POST").

ii. Algoritmo de firma para verificar/firmar las solicitudes/respuestas de SAML (el predeterminado es "RSA-SHA1").

iii. Método para digerir el hash de las solicitudes/respuestas de SAML (el predeterminado es "SHA-1").

iv. Algoritmo de cifrado (el predeterminado es AES256) y otros ajustes.

> **Nota**
>
> Citrix recomienda conservar la configuración predeterminada, ya que se ha comprobado que funcionan con Google Apps.

e) También puede activar la casilla de verificación Atributos de usuario para introducir los detalles del usuario, como:

i. Nombre del atributo de usuario

ii. Expresión de API de NetScaler ADC que se evalúa para extraer el valor del atributo

iii. Nombre fácil de usar del atributo

iv. Seleccione el formato del atributo de usuario.

Estos valores se incluyen en la afirmación SAML emitida. Puede incluir hasta cinco conjuntos de atributos de usuario en una afirmación emitida por NetScaler ADC con este StyleBook.

5. En la sección Configuración de LDAP, introduce los siguientes detalles para autenticar a los usuarios de Google Apps. Para que los usuarios del dominio puedan iniciar sesión en la instancia de NetScaler ADC mediante sus direcciones de correo electrónico corporativas, debe configurar lo siguiente:

a) **Base LDAP (Active Directory)**. Escriba el nombre de dominio base para el dominio en el que residen las cuentas de usuario en Active Directory (AD) para el que quiere permitir la autenticación. Por ejemplo, dc=netscaler, dc=com

b) **DN de enlace de LDAP (Active Directory)**. Agregue una cuenta de dominio (mediante una dirección de correo electrónico para facilitar la configuración) que tenga derechos para examinar el árbol de AD. Por ejemplo, cn=Manager, dc=netscaler, dc=com

c) **Contraseña de DN de enlace LDAP (Active Directory)**. Introduzca la contraseña de la cuenta de dominio para la autenticación.

d) Algunos otros campos que debe introducir en esta sección son los siguientes:

i. Dirección IP del servidor LDAP a la que se conecta NetScaler ADC para autenticar usuarios

ii. Nombre FQDN del servidor LDAP

> **Nota**
>
> Debe especificar al menos una de las dos opciones anteriores: la dirección IP del servidor LDAP o el nombre de FQDN.

iii. Puerto de servidor LDAP al que NetScaler ADC se conecta para autenticar usuarios (el valor predeterminado es 389).

iv. Nombre de host LDAP. Esto se utiliza para validar el certificado LDAP si la validación está activada (de forma predeterminada, está desactivada).

v. Atributo de nombre de inicio de sesión LDAP. El atributo predeterminado que se utiliza para extraer los nombres de inicio de sesión es "samAccountName".

vi. Otros parámetros opcionales de LDAP diversos

6. En la sección Certificado SSL SAML IdP, puede especificar los detalles del certificado SSL:

a) **Nombre del certificado**. Introduzca el nombre del certificado SSL.

b) **Archivo**de certificado . Elija el archivo de certificado SSL en el directorio de su sistema local o en NetScaler ADM.

c) **Formato CertKey**. Seleccione el formato del certificado y los archivos de clave privada en el cuadro de lista desplegable. Los formatos admitidos son las extensiones de archivo.pem y .der.

d) **Nombre de clave de certificado**. Introduzca el nombre de la clave privada del certificado.

e) **Archivo de clave de certificado**. Seleccione el archivo que contiene la clave privada del certificado de su sistema local o de NetScaler ADM.

f) **Contraseña de clave privada**. Si el archivo de clave privada está protegido por una contraseña, introdúzcala en este campo.

g) También puede activar la casilla Configuración avanzada de certificados para introducir detalles como el período de notificación de caducidad del certificado o habilitar o inhabilitar el monitor de caducidad del certificado.

7. Si lo quiere, puede seleccionar el certificado de CA SSL de IdP si el certificado de IdP de SAML introducido anteriormente requiere la instalación de un certificado público de CA en NetScaler ADC. Asegúrese de seleccionar "Es un certificado de CA"en la configuración avanzada.

8. Si lo quiere, puede seleccionar el certificado SSL SP de SAML para especificar el certificado SSL de Google (clave pública) que se utiliza para validar las solicitudes de autenticación de Google Apps (SAML SP).
9. Haga clic en Instancias de **destino y seleccione las instancias** de NetScaler ADC en las que quiere implementar esta configuración de SSO de Google Apps. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

También

> **Consejo**
>
> > >
>
> Citrix recomienda que, antes de ejecutar la configuración real, seleccione **Dry Run** para confirmar visualmente los objetos de configuración que el StyleBook crea en las instancias de Citrix ADC de destino.

StyleBook del SSO de Office 365

January 30, 2024

Microsoft™ Office 365 es un conjunto de aplicaciones de colaboración y productividad basadas en la nube proporcionadas por Microsoft sobre una base de suscripción. Incluye las populares aplicaciones basadas en servidor de Microsoft, como Exchange, SharePoint, Office y Skype Empresarial. El inicio de sesión único (SSO) permite a los usuarios acceder a todas sus aplicaciones empresariales en la nube:

- Incluye los administradores que inician sesión en la consola de administración
- Inicio de sesión único para todos los servicios de Microsoft Office 365 con sus credenciales empresariales.

El SSO Office 365 StyleBook le permite habilitar el SSO para Microsoft Office 365 a través de instancias de NetScaler ADC. Ahora puede configurar la autenticación SAML con NetScaler ADC como proveedor de identidades (IdP) de SAML y Microsoft Office 365 como proveedor de servicios de SAML.

Para habilitar el SSO para Microsoft Office 365 en una instancia de NetScaler ADC mediante este StyleBook, se deben seguir los siguientes pasos:

1. Configuración del servidor virtual de autenticación
2. Configuración de una directiva y un perfil de IDP de SAML
3. Vinculación de la directiva y el perfil al servidor virtual de autenticación
4. Configuración de un servidor y una directiva de autenticación LDAP en la instancia
5. Enlazar el servidor y la directiva de autenticación LDAP a su servidor virtual de autenticación configurado en la instancia.

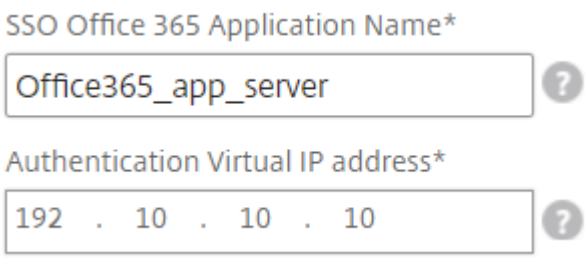
La tabla muestra las versiones de software mínimas necesarias para que esta integración funcione correctamente. El proceso de integración también debería funcionar con versiones superiores del mismo.
Producto	Versión mínima requerida
———	———————————
Citrix ADC	11.0, licencia Enterprise/Platinum

En las instrucciones siguientes se supone que ya ha creado las entradas DNS externas e internas adecuadas. Estas entradas son esenciales para enrutar las solicitudes de autenticación a una dirección IP supervisada por NetScaler ADC.

Las siguientes instrucciones le ayudarán a implementar el SSO Office 365 StyleBook en su red empresarial.

Para implementar el SSO Microsoft Office 365 StyleBook

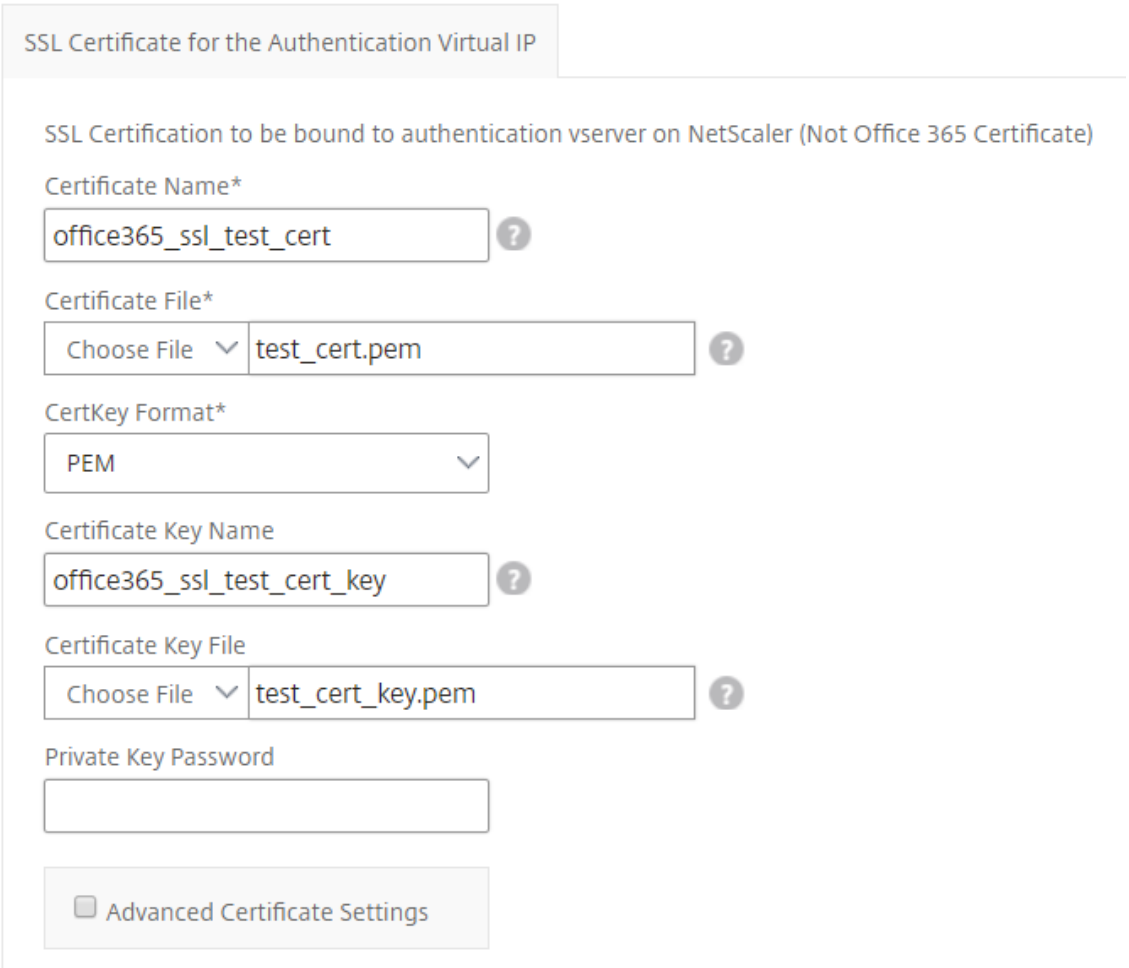
1. En Citrix Application Delivery Management (ADM), vaya a **Aplicaciones**> **StyleBooks** . La página **StyleBooks** muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplázate hacia abajo y busca **SSO Office 365 StyleBook**. Haga clic en **Crear configuración**.
2. El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.
3. Introduzca valores para los siguientes parámetros:
    a) **Nombre de la aplicación**. Nombre de la configuración de SSO de Microsoft Office 365 que se va a implementar en la red.
    b) **Autenticación Dirección IP virtual**. Dirección IP virtual que utilizará el servidor virtual AAA al que está vinculada la directiva de IdP SAML de Microsoft Office 365.



4. En la sección **Configuración de certificados SSL**, introduzca los nombres del certificado SSL y la clave de certificado.

   > **Nota**
   >
   > Este no es el certificado de proveedor de servicios de Office 365. Este certificado SSL está enlazado al servidor de autenticación virtual de la instancia NetScaler ADC.

5. Selecciona los archivos correspondientes de tu carpeta de almacenamiento local. También puede escribir la contraseña de clave privada para cargar claves privadas cifradas en formato PEM.



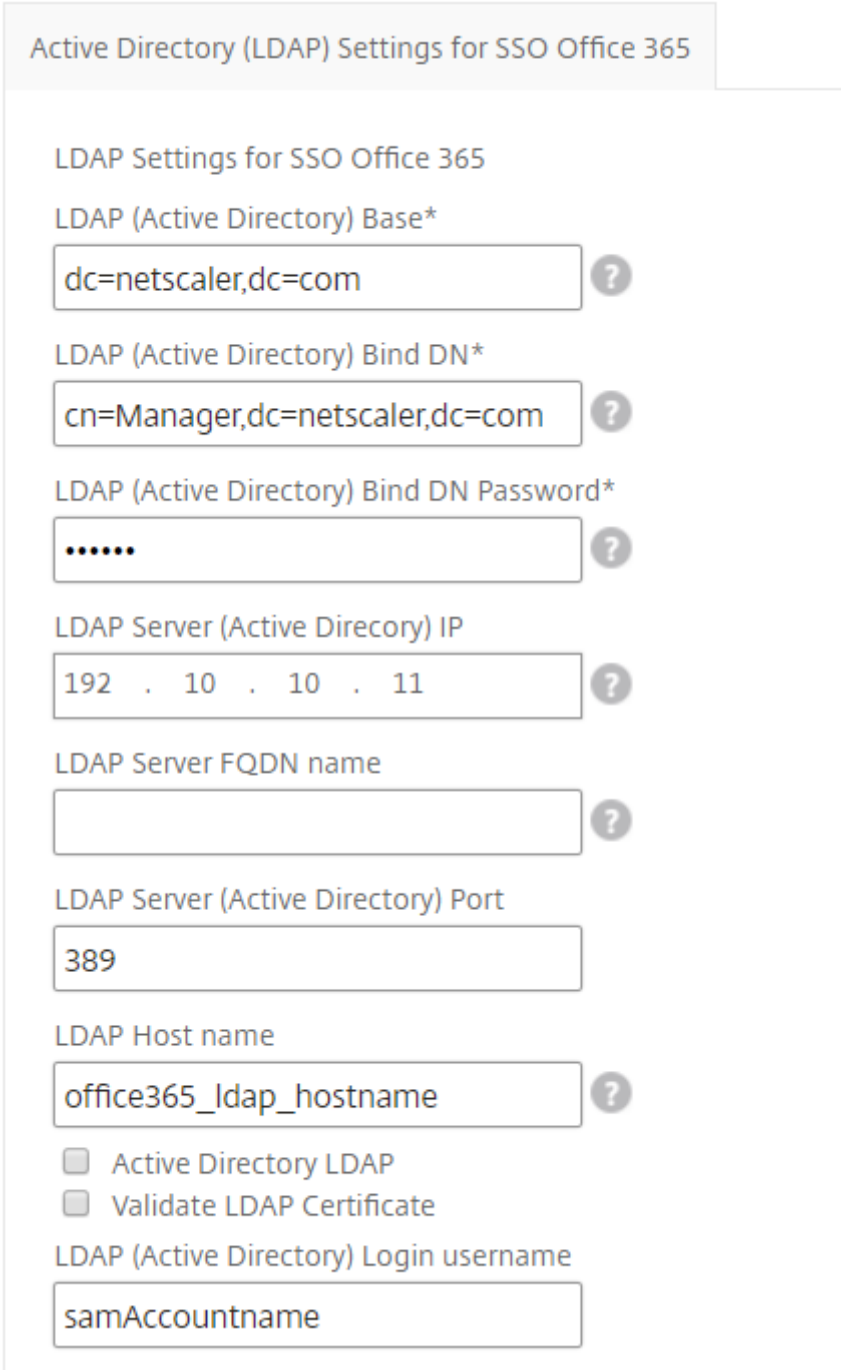
6. También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.
7. Si lo quiere, puede seleccionar el **certificado SSL CA para la casilla de verificación IP virtual de autenticación** si el certificado SSL requiere la instalación de un certificado público de CA en NetScaler ADC. Asegúrese de elegir "Es un certificado de CA"en la sección **Configuración avanzada de certificados** anterior.

8. En la sección **Configuración de LDAP para SSO Office 365**, introduzca los siguientes detalles para autenticar a los usuarios de Office 365. Para permitir que los usuarios del dominio inicien sesión en la instancia de NetScaler ADC mediante sus direcciones de correo electrónico corporativas, configure lo siguiente:

   - **Base LDAP (Active Directory)**. Escriba el nombre de dominio base del dominio en el que residen las cuentas de usuario en Active Directory (AD) para permitir la autenticación. Por ejemplo, dc=netscaler, dc=com
   - **DN de enlace de LDAP (Active Directory)**. Agregue una cuenta de dominio (mediante una dirección de correo electrónico para facilitar la configuración) que tenga derechos para examinar el árbol de AD. Por ejemplo, cn=Manager, dc=netscaler, dc=com
   - **Contraseña de DN de enlace LDAP (Active Directory)**. Introduzca la contraseña de la cuenta de dominio para la autenticación.
   - Algunos otros campos que debe introducir en esta sección son los siguientes:
     - Dirección IP del servidor LDAP a la que se conecta NetScaler ADC para autenticar a los usuarios.
     - Nombre de FQDN del servidor LDAP.

       > **Nota**
       >
       > Debe especificar al menos una de las dos opciones anteriores: la dirección IP del servidor LDAP o el nombre de FQDN.

     - Puerto de servidor LDAP al que NetScaler ADC se conecta para autenticar usuarios (el valor predeterminado es 389). LDAPS usa 636.
     - Nombre de host LDAP. El nombre de host se usa para validar el certificado LDAP si la validación está activada (de forma predeterminada, está desactivada).
     - Atributo de nombre de inicio de sesión LDAP. El atributo predeterminado que se utiliza para extraer los nombres de inicio de sesión es “samAccountName”.
     - Otras opciones opcionales de varios LDAP.



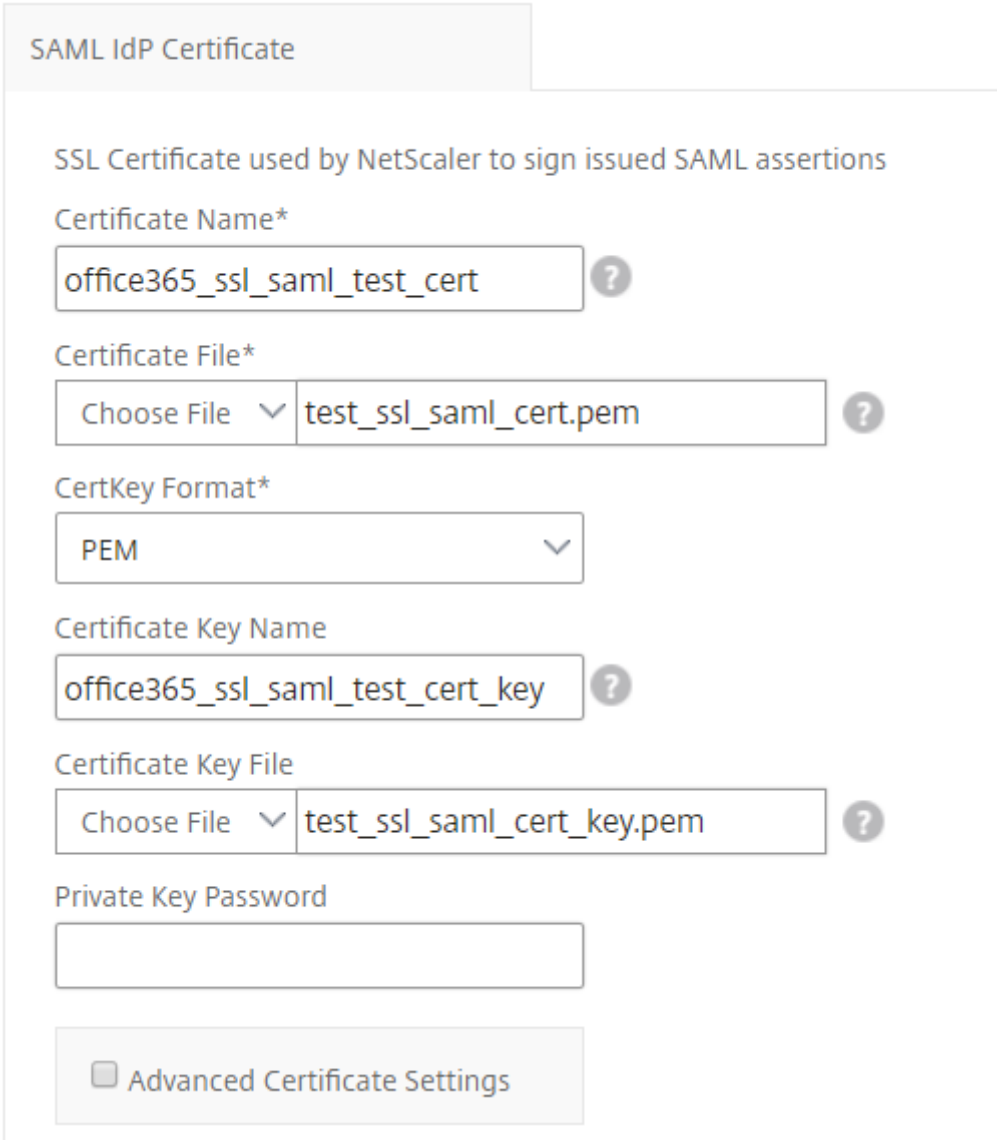
9. En la sección **Certificado de IdP de SAML**, puede especificar los detalles de los certificados SSL utilizados para la aserción de SAML.

   - **Nombre del certificado**. Introduzca el nombre del certificado SSL.
   - **Archivo**de certificado . Elija el archivo de certificado SSL del directorio de su sistema local.
   - **Formato CertKey**. Seleccione el formato del certificado y los archivos de clave privada en el cuadro de lista desplegable. Los formatos admitidos son las extensiones de archivo.pem

y .der.

- **Nombre de clave de certificado**. Introduzca el nombre de la clave privada del certificado.
- **Archivo de clave de certificado**. Seleccione el archivo que contiene la clave privada del certificado del sistema local.
- **Contraseña de clave privada**. Escribe la contraseña que protege tu archivo de clave privada.

También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.

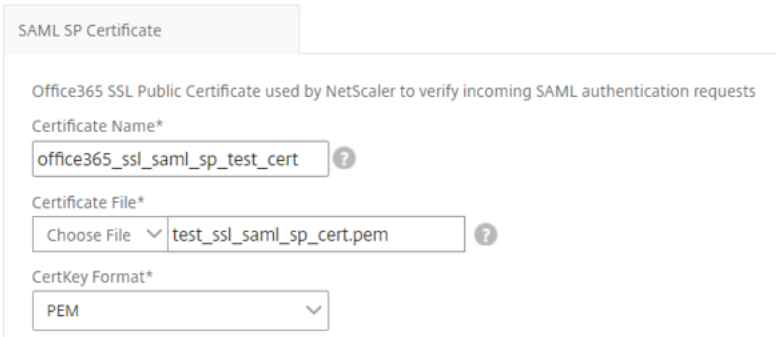


10. Opcionalmente, puede seleccionar el **Certificado de CA de IdP** de SAML si el certificado de IdP de SAML especificado anteriormente requiere que se instale un certificado público de CA en

NetScaler ADC. Asegúrese de seleccionar **Es un certificado de CA** en la sección **Configuración avanzada del certificado** anterior.

11. En la sección **Certificado SP de SAML**, introduzca los siguientes detalles para el certificado público SSL de Office 365. La instancia de NetScaler ADC utiliza este certificado para verificar las solicitudes de autenticación SAML entrantes.

    - **Nombre del certificado**. Escriba el nombre del certificado SSL.
    - **Archivo**de certificado . Elija el archivo de certificado SSL del directorio de su sistema local.
    - **Formato CertKey**. Seleccione el formato del certificado y los archivos de clave privada en el cuadro de lista desplegable. Los formatos admitidos son las extensiones de archivo.pem y .der.
    - También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.



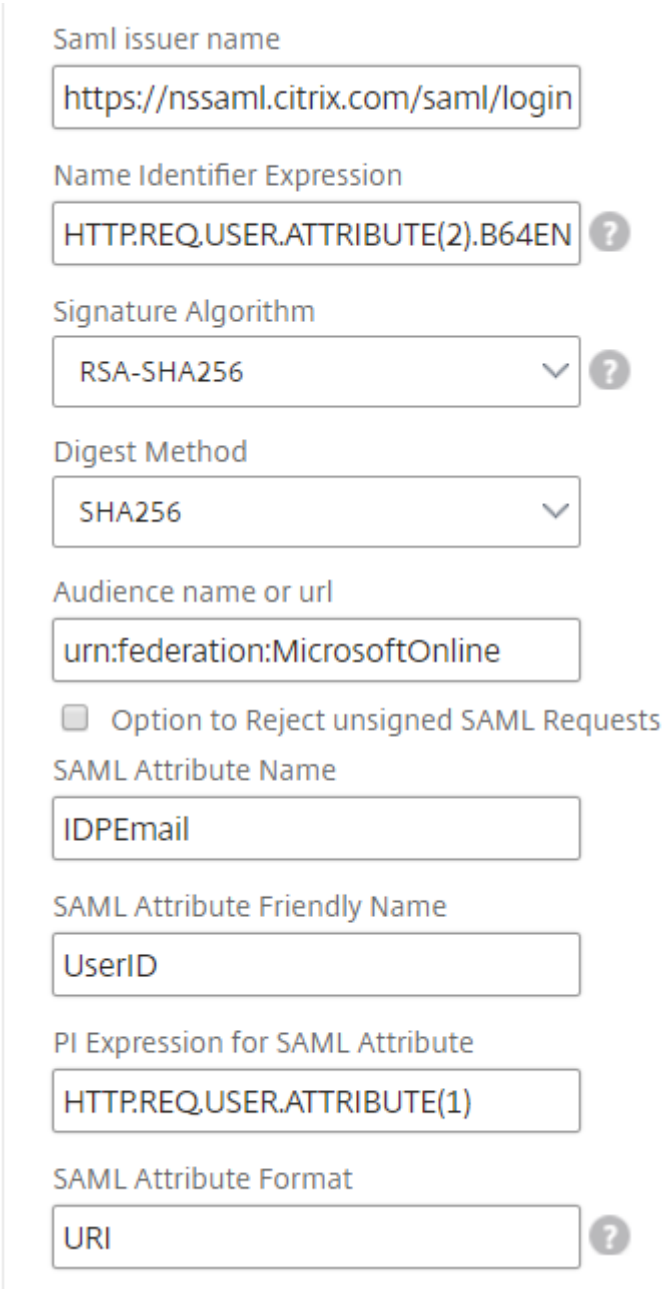
12. La sección **Configuración de IDP de SAML** le permite configurar su instancia de Citrix ADC como proveedor de identidades SAML mediante la creación del perfil y la directiva de IDP de SAML que utiliza el servidor virtual AAA creado en el paso 3.

    - **Nombre del emisor SAML**. En este campo, escriba el FQDN público de su servidor virtual de autenticación. Ejemplo:`https://<Citrix ADC Auth VIP>/saml/login`
    - **Expresión de identificador de nombre**. Escriba la expresión de NetScaler ADC que se evalúa para extraer el SAML NameIdentifier enviado en la aserción SAML. Ejemplo:`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - **Algoritmo de firma**: seleccione el algoritmo para verificar/firmar las solicitudes/respuestas de SAML (el valor predeterminado es “RSA-SHA256”).
    - **Método Digest**. Seleccione el método para digerir el hash de las solicitudes/respuestas de SAML (el valor predeterminado es “SHA256”).
    - **Nombre del público**. Escriba el nombre de la entidad o la URL que representa al proveedor de servicios (Microsoft Office 365).

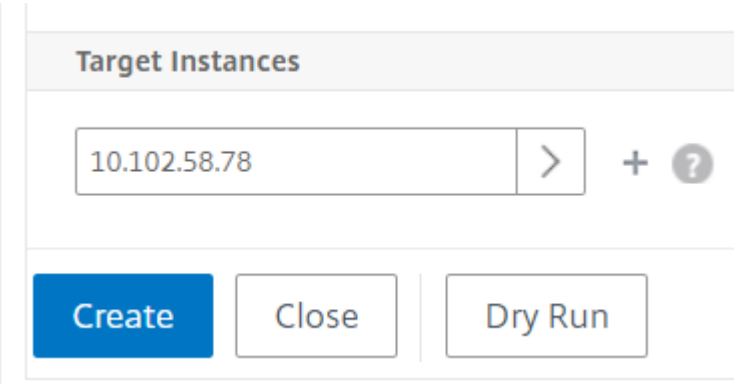
- **ID de proveedor de servicios (SP) SAML**. (opcional) El proveedor de identidades NetScaler ADC acepta solicitudes de autenticación SAML de un nombre de emisor que coincida con este ID.
- **URL de Assertion Consumer Service** Introduzca la URL del proveedor de servicios a la que el proveedor de identidades de NetScaler ADC debe enviar las afirmaciones SAML después de una autenticación de usuario exitosa. La URL del servicio al consumidor de afirmación se puede iniciar en el sitio del servidor del proveedor de identidad o en el sitio del proveedor de servicios.
- Hay otros campos opcionales que puede introducir en esta sección. Por ejemplo, puede configurar las siguientes opciones:
  - **Nombre del atributo SAML**. Nombre del atributo de usuario enviado en la aserción SAML.
  - **Nombre descriptivo del atributo SAML**. Nombre descriptivo del atributo de usuario enviado en la aserción SAML.
  - **Expresión PI para el atributo SAML**. De forma predeterminada, se utiliza la siguiente expresión de directiva de NetScaler ADC (PI): HTTP.REQ.USER.ATTRIBUTE(1). Este campo especifica el primer atributo de usuario enviado desde el servidor LDAP (correo) como atributo de autenticación SAML.
  - Seleccione el formato del atributo de usuario.

  Estos valores se incluyen en la afirmación SAML emitida.

  > **Sugerencia**
  >
  > Citrix recomienda conservar la configuración predeterminada, ya que se ha probado que funciona con las aplicaciones de Microsoft Office 365.



13. Haga clic en Instancias de **destino y seleccione las instancias** NetScaler ADC en las que quiere implementar esta configuración de SSO de Microsoft Office 365. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.



Sugerencia

Citrix recomienda que, antes de ejecutar la configuración real, seleccione**Ejecutar en seco**para ver los objetos de configuración creados en las instancias de NetScaler ADC de destino por el StyleBook.

StyleBook de Microsoft Skype Empresarial

January 30, 2024

La aplicación Skype Empresarial 2015 se basa en varios componentes externos para funcionar. La red Skype Empresarial consta de varios sistemas, como servidores y sus sistemas operativos, bases de datos, sistemas de autenticación y autorización, sistemas e infraestructura de redes y sistemas de PBX telefónicos. Skype Empresarial Server 2015 está disponible en dos versiones, Standard Edition y Enterprise Edition. La principal diferencia radica en la compatibilidad con las funciones de alta disponibilidad que solo se incluyen en la edición empresarial. Para implementar la alta disponibilidad, se deben implementar varios servidores front-end en un grupo y los servidores SQL deben reflejarse.

Una implementación de Enterprise Edition permite la creación de varios servidores con diferentes funciones.

Componentes principales

Los componentes principales de la aplicación Skype Empresarial 2015 son:

- Servidores frontales
- Servidores Edge
- Servidores de Director
- Servidores de base de datos (SQL)

Servidores frontales

En la aplicación Skype Empresarial, el servidor front-end es el servidor principal de la red. Proporciona los enlaces y los servicios para la autenticación de usuarios, el registro, la presencia, la libreta de direcciones, las conferencias audiovisuales, el intercambio de aplicaciones, la mensajería instantánea y las conferencias web. Si va a implementar Skype Empresarial 2015 Enterprise Edition, la topología suele consistir en al menos dos servidores Front-End equilibrados de carga en un grupo Front-End con un servidor de base de datos que aloja la instancia de SQL Server que contiene la base de datos de Skype Empresarial.

Servidores Edge

La implementación de servidores perimetrales para Skype Empresarial es necesaria si los usuarios externos que no han iniciado sesión en la red interna de su organización necesitan poder interactuar con usuarios internos. Estos usuarios externos pueden ser usuarios remotos anónimos y autenticados, socios federados u otros clientes móviles.

Hay cuatro tipos de funciones en el servidor Edge de Skype For Business:

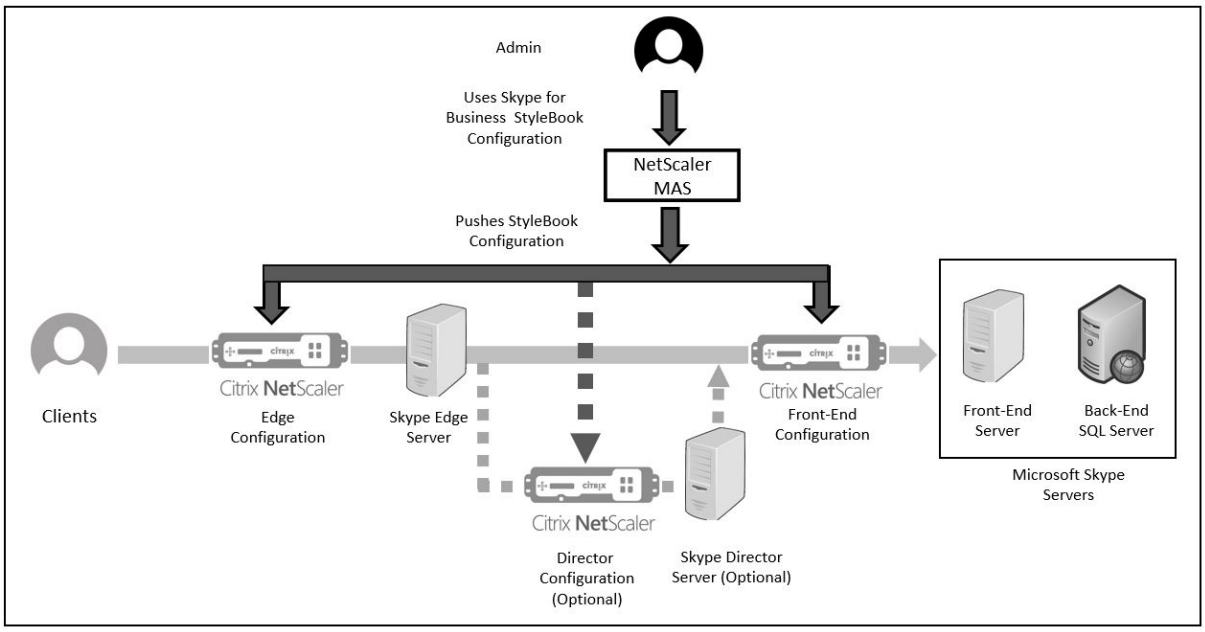
- Access Edge, que gestiona el tráfico SIP y autentica las conexiones externas, permite la conexión remota y permite la conexión de federación
- Conferencing Web, que gestiona los paquetes de conferencia de datos y permite a los usuarios externos acceder a Skype Empresarial
- Conferencias A/V, que gestiona paquetes de conferencias A/V y extiende el audio y el vídeo, el uso compartido de aplicaciones y la transferencia de archivos a usuarios externos
- Proxy XMPP, que maneja paquetes XMPP y permite que servidores o clientes basados en XMPP se conecten a Skype Empresarial.

Servidores de Director

La función principal del servidor de Director en Skype Empresarial 2015 es autenticar los dispositivos de punto final y "dirigir"a los usuarios al grupo que contiene su cuenta. En Skype Empresarial 2015, aunque el Director es un rol completamente dedicado y específico en un servidor independiente, es un servidor opcional. Esto facilita la seguridad al facilitar la implementación o la eliminación de las configuraciones.

Los directores son más útiles cuando existen varios grupos porque proporcionan un único punto de contacto para autenticar los puntos de conexión. Además, para los usuarios remotos, un Director sirve como salto adicional entre el grupo Edge y el grupo Front-End, lo que agrega una capa adicional de protección contra ataques.

La siguiente ilustración representa de forma diagramática la implementación de servidores de Skype en la red:



Configuración de instancias de Citrix ADC en una empresa

En la tabla siguiente se enumeran las direcciones IP utilizadas en la configuración de ejemplo que se incluye en las instrucciones siguientes:

Servidores de Skype Empresarial	Dirección IP virtual	Direcciones IP del servidor	Instancia Citrix ADC
Servidores Edge	VIP externo - 192.20.20.20 VIP interno - 10.10.10.20	192.20.20.21; 192.20.20.22 10.10.10.21; 10.10.10.22	10.102.29.141
Servidores frontales	10.10.10.10	10.10.10.11; 10.10.10.12	10.102.29.60
Servidor de Director	10.10.10.30	10.10.10.31; 10.10.10.32	10.102.29.93

Para configurar servidores frontales

1. En Citrix Application Delivery Management (ADM), vaya a **Aplicaciones** > **Configuración**y haga clic en **Crear nuevo**. La página **Choose StyleBook** muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplácese hacia abajo y seleccione **Microsoft Skype Empresarial**

2015 StyleBook. El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.

2. En la sección **Servidor Edge**, introduzca las siguientes direcciones IP virtuales (VIP) y las direcciones IP de todos los servidores Edge de la red.

    a) Dirección VIP externa y direcciones IP de los servidores Edge que se utilizarán para Access Edge, las conferencias web Edge y A/V Edge.
    b) Dirección VIP interna y direcciones IP de los servidores Edge que se conectarán a la red interna.
    c) Dos servidores Edge externos y dos internos en su red.

3. En la sección **Servidor front-end**, escriba la dirección IP del servidor front-end virtual (VIP) que se va a crear para los servidores front-end de Skype Empresarial. Además, introduzca las direcciones IP de todos los servidores front-end de Skype Empresarial de la red.
4. En la sección de **Director Server**, escriba la dirección IP virtual (VIP) para los servidores de Director que se va a crear para la aplicación Skype Empresarial. Además, introduzca las direcciones IP de todos los servidores de Skype Empresarial Director de la red. Cree al menos dos servidores Director para una alta disponibilidad.
5. La sección **Configuración avanzada** enumera todos los puertos predeterminados configurados en las instancias de Citrix ADC para los tres servidores de Skype.

La siguiente tabla proporciona una lista de todos los puertos y protocolos predeterminados:

Etiqueta	Puerto	Protocolo	Descripción
Puerto HTTP	80	HTTP	Se utiliza para la comunicación de los servidores front-end a los FQDN de la comunidad web cuando no se utiliza HTTPS.
Puerto HTTPS	443	HTTPS	Se utiliza para la comunicación de los servidores front-end a los FQDN de la comunidad de servidores web.

Etiqueta	Puerto	Protocolo	Descripción
Puerto interno de AutoDiscover	4443	HTTPS	Comunicaciones entre grupos mediante HTTPS (de Reverse Proxy) y HTTPS Front-End para el inicio de sesión de AutoDiscover.
Puerto RPC	135	DCOM y llamada de procedimiento remoto (RPC)	Se utiliza para operaciones basadas en DCOM, como el traslado de usuarios, la sincronización de replicadores de usuarios y la sincronización de libretas de direcciones.
Puerto SIP	5061	TCP (TLS)	Los servidores Front-End lo utilizan para todas las comunicaciones SIP internas.
Puerto de enfoque SIP	444	HTTPS, TCP	Se utiliza para la comunicación HTTPS entre el Focus (el componente que administra el estado de la conferencia de Skype) y los servidores individuales.
Puerto de grupo SIP	5071	TCP	Se usa para las solicitudes SIP entrantes para la aplicación del grupo de respuestas.

Etiqueta	Puerto	Protocolo	Descripción
Puerto SIP para compartir aplicaciones	5065	TCP	Se utiliza para las solicitudes de escucha SIP entrantes para compartir aplicaciones.
Puerto de asistente SIP	5072	TCP	Se utiliza para las solicitudes SIP entrantes para el operador (es decir, para las conferencias de acceso telefónico).
Puerto de anuncio SIP Conf	5073	TCP	Se utiliza para las solicitudes SIP entrantes para el servicio de anuncio de conferencia de Skype Empresarial Server (es decir, para las conferencias de acceso telefónico).
Puerto SIP CallPark	5075	TCP	Se utiliza para las solicitudes SIP entrantes para la aplicación CallPark.
Puerto de admisión de llamadas SIP	448	TCP	Se utiliza para el control de admisión de llamadas por el servicio de directivas de ancho de banda del servidor de Skype Empresarial.

Etiqueta	Puerto	Protocolo	Descripción
Puerto TURN de admisión de llamadas SI	5080	TCP	El servicio de directivas de ancho de banda lo utiliza para controlar la admisión de llamadas para el tráfico TURN de Audio/Video Edge
Puerto de prueba de audio SIP	5076	TCP	Se usa para las solicitudes SIP entrantes para el servicio de prueba de audio.
Puerto externo HTTPS	443	HTTPS	Se utiliza para puertos externos para la comunicación SIP/TLS para el acceso remoto de usuarios, el acceso a conferencias web internas y las comunicaciones multimedia entrantes y salientes de STUN/TCP para acceder a los medios internos y a las sesiones de A/V.

Etiqueta	Puerto	Protocolo	Descripción
Puerto interno HTTPS	443	HTTPS	Se utiliza como puertos internos para la comunicación SIP/TLS para el acceso remoto de usuarios, el acceso a conferencias web internas y las comunicaciones multimedia entrantes y salientes de STUN/TCP para acceder a los medios internos y a las sesiones de A/V.
Puerto de acceso remoto externo SIP	5061	TCP	Se utiliza para puertos externos para la comunicación SIP/MTLS para el acceso remoto de usuarios o la federación.
Puerto de acceso remoto interno SIP	5061	TCP	Se utiliza como puertos internos para la comunicación SIP/MTLS para el acceso remoto de usuarios o la federación.
Puerto SIP STUN UDP externo	3478	UDP	Se utiliza para puertos externos para comunicaciones multimedia entrantes y salientes de STUN/ UDP.

Etiqueta	Puerto	Protocolo	Descripción
Puerto SIP STUN UDP interno	3478	UDP	Se utiliza para los puertos internos para las comunicaciones multimedia entrantes y salientes de STUN/UDP.
Puerto IM interno SIP	5062		Se utiliza para los puertos internos para la autenticación SIP/MTLS de las comunicaciones de mensajería instantánea que salen a través del firewall interno.
Puerto HTTP	80	TCP	Se utiliza para la comunicación inicial de Directores a los FQDN de la comunidad de servidores web.
Puerto HTTPS	443	HTTPS	Se utiliza para la comunicación de Directores a los FQDN de la comunidad de servidores web.
Puerto interno de AutoDiscover	4443	HTTPS	Se utiliza para las comunicaciones entre grupos de HTTPS (de Reverse Proxy) y HTTPS Director para el inicio de sesión de AutoDiscover.
Puerto interno SIP	5061	TCP	Se utiliza para las comunicaciones internas entre servidores y para las conexiones de cliente.

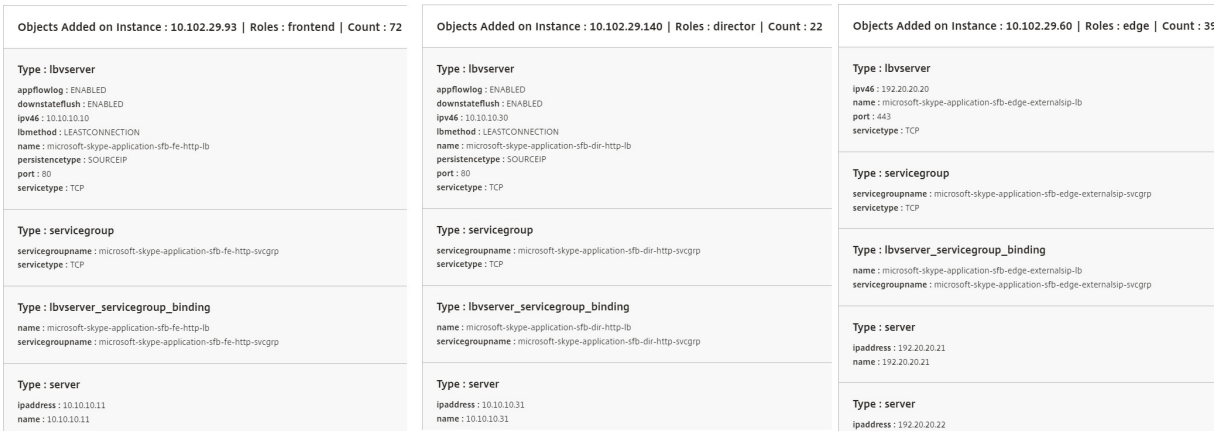
6. En la sección **Instancias de destino, seleccione las tres instancias** de Citrix ADC diferentes en las que quiere implementar los tres servidores de Skype Empresarial.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

7. Haga clic en**Crear** para crear la configuración en las instancias de Citrix ADC seleccionadas.

> **Sugerencia**
>
> Citrix recomienda seleccionar**Ejecución en seco**para comprobar los objetos de configuración que se deben crear en la instancia de destino antes de ejecutar la configuración real en la instancia.
>
> Cuando la configuración se crea correctamente, StyleBook crea 25 servidores virtuales de equilibrio de carga. Es decir, para cada puerto, se define un servidor virtual de equilibrio de carga junto con un grupo de servicios, y el grupo de servicios está enlazado al servidor virtual de equilibrio de carga. La configuración también agrega los servidores Front-End como miembros del grupo de servicios y los vincula al grupo de servicios. La cantidad de miembros del grupo de servicios creados es igual a la cantidad de servidores Front-End creados.

La siguiente ilustración muestra los objetos creados en cada servidor:



StyleBook de Microsoft Exchange

January 30, 2024

Puede usar el StyleBook de Microsoft Exchange 2016 para implementar una configuración de Citrix ADC que optimice y proteja una aplicación empresarial de Microsoft Exchange 2016 en su red. Mi-

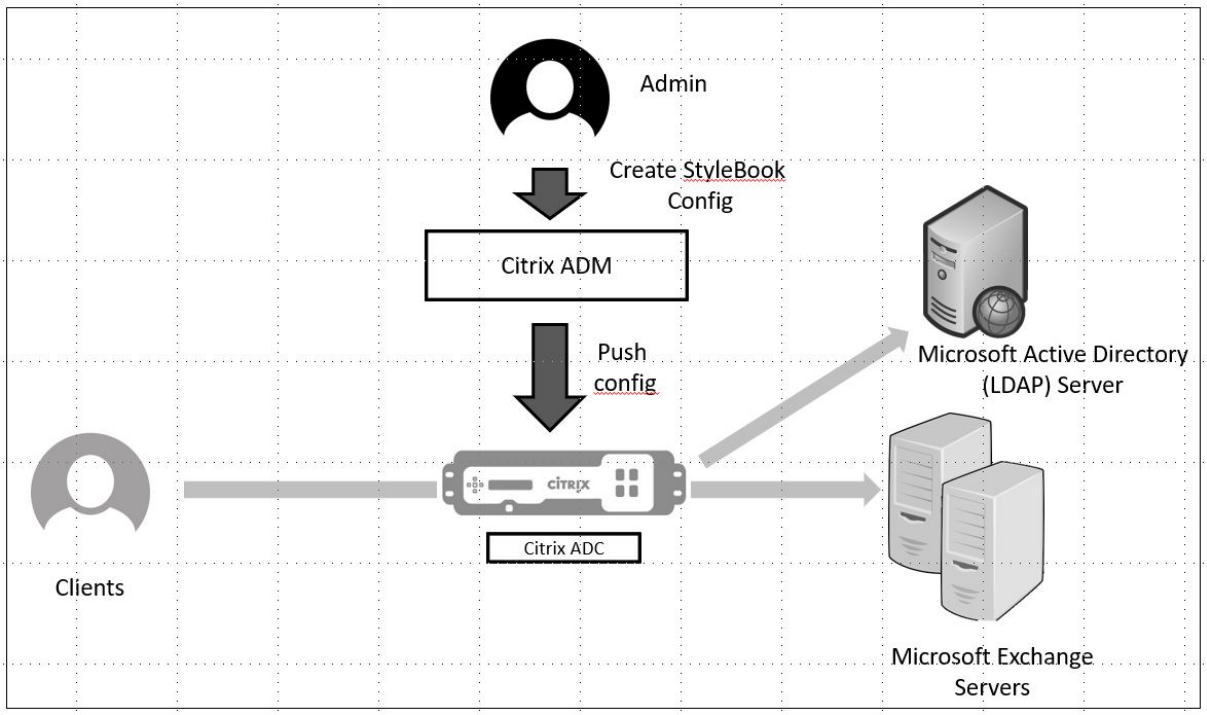
crosoft Exchange 2016 es una aplicación empresarial clave para proporcionar servicios de correo electrónico, administración de información personal y mensajería a sus empleados y otras partes interesadas.

Funciones de Citrix ADC configuradas mediante Microsoft Exchange StyleBook

El StyleBook de Microsoft Exchange 2016 habilita y configura las siguientes funciones de Citrix ADC para los servidores de Microsoft Exchange 2016:

- Equilibrio de carga: equilibrio de carga básico que permite equilibrar la carga de varios servidores de Exchange
- Conmutación de contenido: cambio de contenido que permite el acceso con una sola IP y la redirección de las consultas a los servidores virtuales de equilibrio de carga correctos
- Reescribir: redirige a los usuarios a páginas seguras
- Descarga de SSL: descarga el procesamiento de SSL al Citrix ADC y, por lo tanto, reduce la carga en el servidor Exchange

La siguiente ilustración representa de forma diagramática la implementación de servidores Exchange en la red:



Requisitos previos

- Para la autenticación basada en certificados, todos los hosts direccionables que forman parte de la configuración de la red deben tener nombres de dominio resolubles y no solo direcciones IP.
- Asegúrese de que se pueda acceder a los puertos SIP en el servidor Microsoft Exchange 2016.

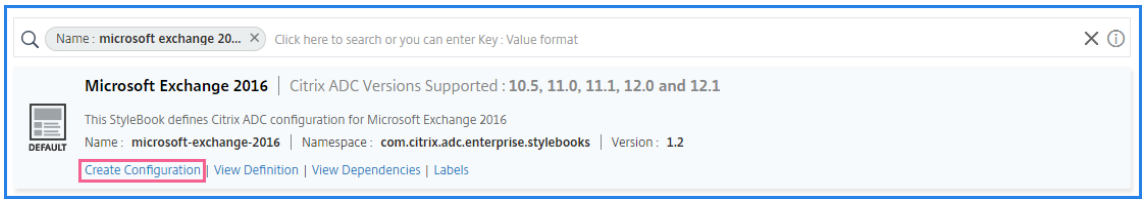
Configuración de Microsoft Exchange StyleBook

Configure el StyleBook de Microsoft Exchange en su empresa empresarial para implementar la configuración de Citrix ADC.

Para configurar la aplicación Microsoft Exchange

1. En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks**.
2. Busque **Microsoft Exchange 2016 StyleBook** y haga clic en **Crear configuración**.

   El StyleBook aparece como un formulario de interfaz de usuario en el que puede introducir los valores de todos los parámetros definidos en este StyleBook.

3. Introduzca los detalles de los siguientes parámetros:

   - **Nombre de la aplicación de Exchange**: Nombre de la aplicación Microsoft Exchange de la red
   - **Exchange VIP**: dirección IP virtual en Citrix ADC que recibe las solicitudes de los clientes para la aplicación Microsoft Exchange
   - **IPs de Exchange Server**: Direcciones IP de todos los servidores de Exchange de la red.

     Si quiere agregar más direcciones IP, haga clic en el icono con el signo más (**+**). Normalmente, dos servidores Exchange están configurados en la red.

4. En la sección **Certificados de Exchange**, cargue los certificados de intercambio en Citrix ADM. Introduzca los nombres del certificado y de los archivos de clave y cárguelos desde el almacenamiento local. También puede proporcionar una contraseña de clave privada para cifrar el archivo de claves.

> **Nota**
>
> Asegúrese de que los archivos de certificado tengan el formato ‘‘.pem’’o ‘‘.der’’. Citrix ADM rechaza los archivos de otros formatos.

Si quiere especificar los detalles de caducidad del certificado o cualquier configuración avanzada, seleccione **Configuración avanzada del certificado**.

5. En la sección **Configuración de autenticación de Active Directory de Exchange**, configure los ajustes de AD introduciendo los datos.
   - **Active Directory Authentication VIP** : la dirección IP virtual utilizada para crear y configurar el servidor virtual AD (LDAP) en un dispositivo Citrix ADC.
   - **IP del servidor Active Directory**: la dirección IP del controlador de dominio de Active Directory.
   - **Cadena base de Active Directory: la cadena**base LDAP de Active Directory. Por ejemplo, CN=Users, DC=CTXNSSFB, DC=COM.
   - Nombre**distintivo de enlace LDAP (DN) de Active Directory: el nombre** distintivo (DN) de enlace de LDAP se utiliza para vincular este objeto al servidor LDAP (AD). Por ejemplo, ‘‘cn=Administrator,cn=Users,dc=acme,dc=com’’
   - Contraseña de**nombre distintivo (DN) de enlace LDAP de Active Directory: el nombre distintivo (DN) de enlace de LDAP es la contraseña** para la autenticación de AD
   - Atributo de**nombre de usuario de Active Directory: atributo** AD para el nombre de usuario. El Citrix ADC utiliza el atributo LDAP para consultar servidores Active Directory externos. Por ejemplo, ‘‘sAMAccountName’’
   - **Nombre de atributo del grupo de Active Directory**: los nombres de los atributos del grupo LDAP configurados en el servidor LDAP. Por ejemplo, ‘‘memberOf’’para el atributo de grupo en LDAP.
   - **Nombre de subatributo de Active Directory**: Los nombres de los subatributos de LDAP configurados en el servidor LDAP. Por ejemplo, ‘‘cn’’para el subatributo de LDAP.
   - **Dominio de autenticación de Active Directory**: El nombre de dominio AD/LDAP utilizado para la autenticación. Por ejemplo, ctxnssfb.com.
6. En la sección**Instancias de destino**, seleccione la instancia de Citrix ADC en la que implementar esta configuración de Exchange.

> **Nota**

> Si quiere ver las instancias de Citrix ADC detectadas recientemente, haga clic en el icono de actualización.

7. Haga clic en **Crear** para crear el archivo de configuración y ejecutar la configuración en la instancia de Citrix ADC seleccionada.

   Citrix recomienda seleccionar primero**Ejecución en seco**para comprobar los objetos de configuración que se crean en la instancia de destino antes de ejecutar la configuración real en la instancia.

Cuando la configuración se ha creado correctamente, StyleBook ha creado un servidor virtual de conmutación de contenido, cinco servidores virtuales de equilibrio de carga y una directiva LDAP vinculada a un servidor virtual de autenticación LDAP. Además, los grupos de servicios correspondientes creados y enlazados a los servidores virtuales de equilibrio de carga.

StyleBook de Microsoft SharePoint

January 30, 2024

Microsoft SharePoint 2016 es una aplicación empresarial clave que proporciona principalmente un sistema de almacenamiento y administración de documentos, altamente configurable y compatible con todos los principales navegadores.

Puede usar el StyleBook de Microsoft SharePoint 2016 para implementar una configuración de Citrix ADC que optimice y proteja la aplicación empresarial de Microsoft SharePoint 2016 en su red.

Requisitos previos

- Microsoft SharePoint 2016
- Citrix ADM, versión 12.0 y posteriores
- Citrix ADC, versión 10.5 y posterior

Funciones de Citrix ADC configuradas por el StyleBook de Microsoft SharePoint 2016

Puede usar el StyleBook de Microsoft SharePoint 2016 para habilitar y configurar las siguientes funciones de Citrix ADC para Microsoft SharePoint 2016:

- Equilibrio de carga
- Conmutación de contenido
- Responder

- Reescritura
- Compresión
- Almacenamiento en caché integrado

Equilibrio de carga

El equilibrio de carga de Citrix ADC distribuye uniformemente las solicitudes a los servidores de backend de SharePoint. La supervisión inteligente de los servidores de fondo evita que las solicitudes se envíen a servidores que no funcionan correctamente.

SharePoint StyleBook configura 12 servidores virtuales de equilibrio de carga, cada uno dedicado a solicitudes de equilibrio de carga para un determinado tipo de contenido, como documentos, imágenes, audio, vídeo y otros tipos de archivo.

El StyleBook de SharePoint ahora admite el modo SSL de la aplicación SharePoint mediante la configuración de servidores virtuales LB basados en SSL. Asegúrese de que SSL esté seleccionado como protocolo de interfaz. Tenga en cuenta que el puerto virtual está establecido en 443 de forma predeterminada. También puede seleccionar SSL para vincular grupos de servicios (servidores de aplicaciones de SharePoint) a los servidores virtuales de equilibrio de carga de destino. Tenga en cuenta que el protocolo de backend está configurado de forma predeterminada en HTTP.

Cambio de contenido

La función de cambio de contenido se utiliza para distribuir las solicitudes de los clientes en varios servidores virtuales de equilibrio de carga en función de tipos específicos de contenido de SharePoint solicitado (por ejemplo, documentos, imágenes y archivos de audio o vídeo). El módulo de conmutación de contenido dirige el tráfico entrante a un servidor virtual de equilibrio de carga óptimo que puede procesar ese tipo de contenido. Por lo tanto, puede aplicar diferentes directivas de optimización a diferentes tipos de tráfico. Por ejemplo, es posible que quiera utilizar directivas de compresión o almacenamiento en caché diferentes para los vídeos que para los documentos de texto.

Responder

La funcionalidad de respuesta de una instancia de Citrix ADC se puede utilizar para redirigir sin problemas a los usuarios de HTTP a HTTPS. El respondedor también se puede configurar para proporcionar páginas de error personalizadas. La directiva de respuesta determina las solicitudes (tráfico) en las que se debe realizar una acción y vincula cada directiva a un servidor virtual de equilibrio de carga. El StyleBook de SharePoint incluye una configuración que redirige a los usuarios de las URL HTTP a HTTPS.

Reescritura

El módulo de reescritura se utiliza para modificar los encabezados, las URL o el contenido de las solicitudes o respuestas sobre la marcha. Este módulo funciona en línea con el procesamiento del tráfico y, por lo tanto, puede cambiar el flujo de tráfico según corresponda para casos de uso particulares. Por ejemplo, la reescritura puede proporcionar acceso al contenido solicitado sin exponer detalles innecesarios sobre el servidor del sitio web.

En el StyleBook de SharePoint, la función de reescritura se utiliza para eliminar los encabezados innecesarios de las solicitudes de los usuarios.

Compresión

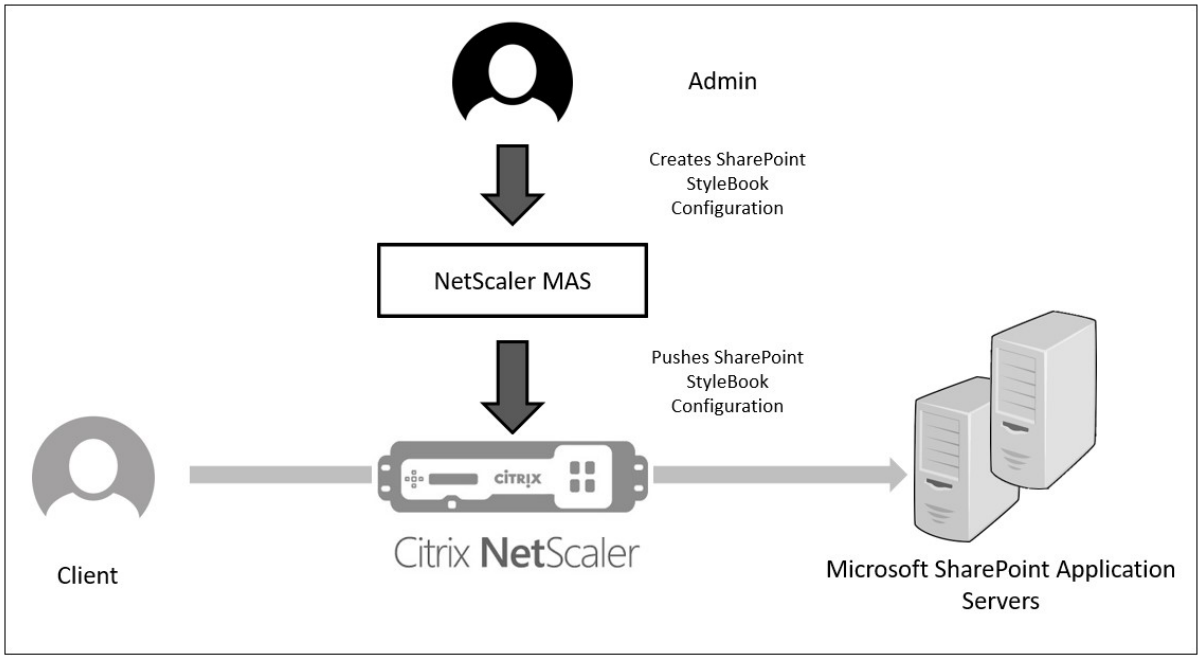
El motor de compresión Citrix ADC identifica y comprime el contenido que se puede comprimir. Este proceso mejora el tiempo de transmisión de datos y reduce los requisitos de ancho de banda de la red para los clientes, al tiempo que ahorra los ciclos de CPU en los servidores Una instancia de Citrix ADC puede comprimir datos generados tanto estáticos como dinámicamente. Aplica el algoritmo de compresión GZIP o DEFLATE para eliminar información extraña y repetitiva de las respuestas del servidor y representar la información original en un formato más compacto y eficiente. La capacidad del explorador cliente para descomprimir los datos depende del algoritmo o algoritmos que admita: GZIP, DEFLATE o ambos.

Una instancia de Citrix ADC está configurada para comprimir el texto en HTML, XML, texto sin formato, hojas de estilos en cascada (CSS) y documentos de Microsoft Office, pero no comprime las imágenes en formato GIF o JPG. Los principales beneficios del tráfico comprimido incluyen la reducción de los costes de ancho de banda, la reducción de la latencia de la WAN y un mejor rendimiento

Almacenamiento en caché integrado

La caché en memoria de Citrix ADC puede almacenar objetos de SharePoint para entregar rápidamente el contenido solicitado con frecuencia a los usuarios. El contenido en caché incluye documentos descargados y archivos de audio, vídeo e imagen.

La siguiente ilustración representa de forma diagramática la implementación de servidores SharePoint en una instancia de Citrix ADC en la que se utiliza Citrix ADM para implementar una configuración de SharePoint StyleBook.



Implementación de configuraciones de SharePoint StyleBook

La siguiente tarea le ayudará a implementar el StyleBook de Microsoft SharePoint 2016 en su red empresarial.

Para implementar Microsoft SharePoint 2016 StyleBook:

1. En Citrix ADM, vaya a **Aplicaciones** > **Administración** > **Configuración**y haga clic en **Crear nuevo**.

   La página **Choose StyleBook** muestra todos los StyleBooks disponibles para su uso en Citrix ADM.

2. Desplázate hacia abajo y selecciona **Microsoft SharePoint 2016 StyleBook**.

   > **Nota:**
   >
   > En Citrix ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**. Desplácese hacia abajo para buscar el **StyleBook de Microsoft SharePoint 2016** y haga clic en **Crear configuración**.

   El StyleBook se abre como un formulario de interfaz de usuario en el que puede introducir los valores de todos los parámetros definidos en este StyleBook.

   Introduzca valores para los siguientes parámetros:

   a) **Nombre de la aplicación SharePoint**. Nombre de la configuración de SharePoint que se va a implementar en la red.

b) **IP virtual de SharePoint**. Dirección IP virtual en la que la instancia de Citrix ADC recibe las solicitudes de los clientes para la aplicación Microsoft SharePoint.

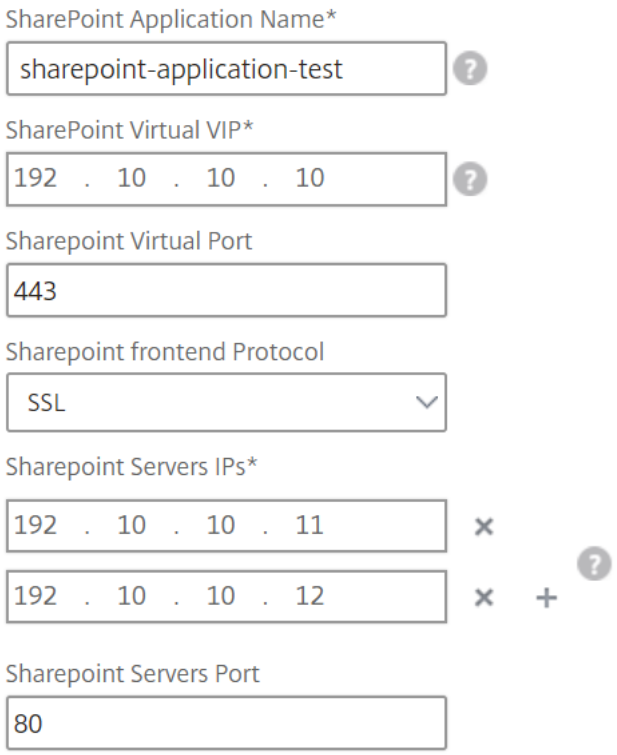
c) **Puerto virtual de SharePoint**. El puerto TCP que utilizarán los usuarios para acceder a la aplicación SharePoint

d) **Protocolo de interfaz de SharePoint**. Seleccione el protocolo de interfaz de SharePoint en la lista desplegable. Las opciones disponibles son HTTP o SSL.

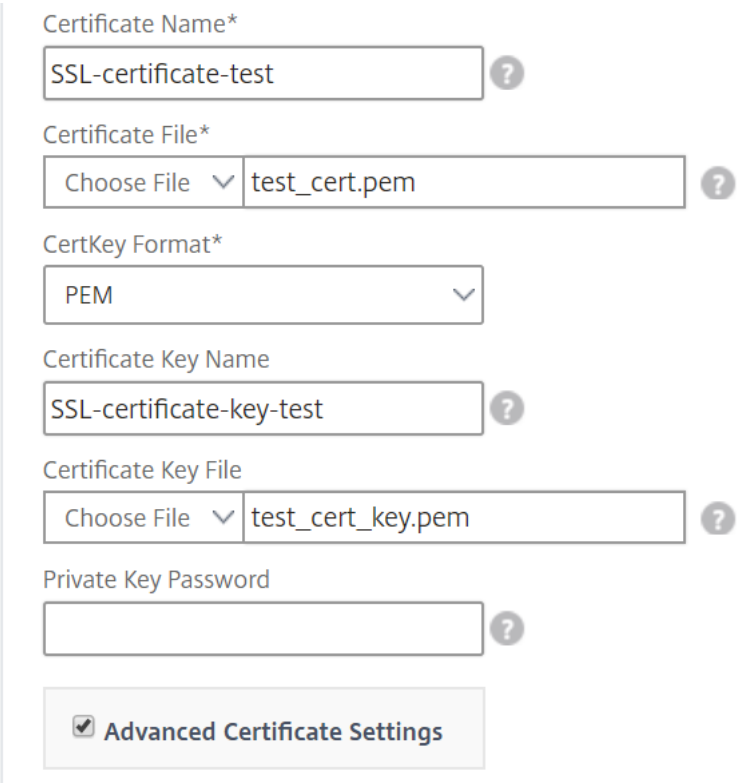
> **Nota:**
>
> Si selecciona SSL, asegúrese de que el parámetro Reescritura de configuración esté habilitado en la sección Configuración avanzada de SharePoint de este StyleBook.

e) **IPs de SharePoint Server**. Direcciones IP de todos los servidores SharePoint de la red.

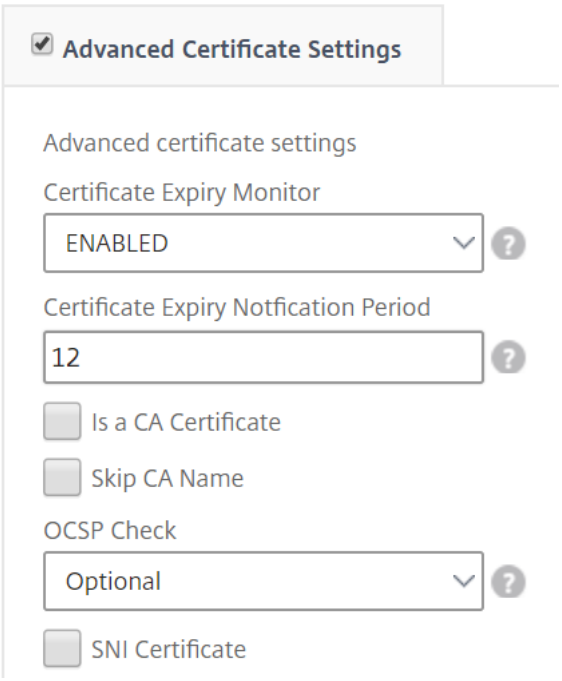
f) **Puerto de servidores SharePoint**. Número de puerto TCP utilizado por los servidores de SharePoint. De forma predeterminada, es 80. Puede modificar este valor si es necesario, pero asegúrese de que este puerto es accesible en servidores de Microsoft SharePoint 2016.



3. En la sección **Configuración de certificados SSL**, haga clic en + para introducir el nombre del certificado SSL, la clave de certificado y seleccionar los archivos respectivos de la carpeta de almacenamiento local.

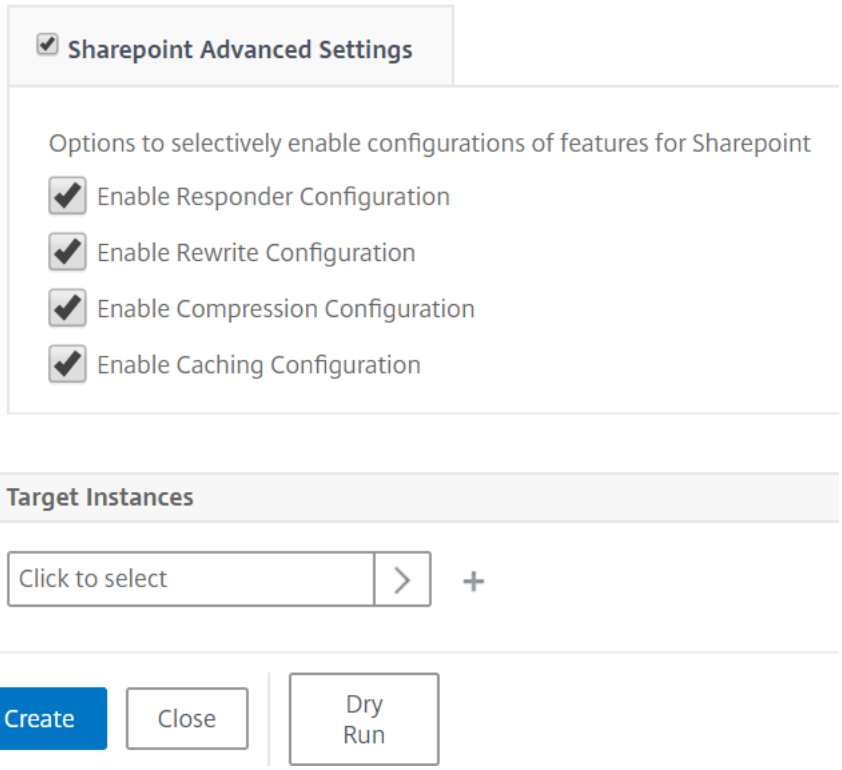


4. Si lo quiere, haga clic en **Configuración avanzada de certificados** para habilitar o inhabilitar la supervisión de caducidad de certificados SSL. Si habilita la supervisión de la caducidad de los certificados, defina el número de días para que Citrix ADM emita una alarma después de esos días cuando el certificado esté a punto de caducar. También tiene la opción de realizar la comprobación OCSP como una función opcional o una función obligatoria.



5. La sección **Configuración avanzada** de SharePoint le permite habilitar las funciones de Citrix ADC que se configurarán en las instancias de Citrix ADC. Si bien las funciones de equilibrio de carga y cambio de contenido están configuradas en las instancias de forma predeterminada, puede elegir las demás funciones, es decir, la configuración del respondedor, la configuración de reescritura, la configuración de compresión y la configuración de almacenamiento en caché integrado, que deseas configurar en la instancia.
6. Haga clic en **Instancias de destino** y seleccione la instancia de Citrix ADC en la que quiere implementar esta configuración de SharePoint. Haga clic en **Crear** para crear la configuración e implementarla en la instancia de Citrix ADC seleccionada.

   > **Nota**
   >
   > También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.



> **Nota:**
>
> Citrix recomienda que, antes de ejecutar la configuración real, seleccione **Ejecución en seco** para comprobar los objetos de configuración que se crearán en la instancia de destino.

Cuando se crea la configuración y se implementa correctamente, SharePoint StyleBook crea un servidor virtual de conmutación de contenido y 12 servidores virtuales de equilibrio de carga. También

crea directivas y grupos de servicios y los vincula a los servidores virtuales de equilibrio de carga. Las directivas que se creen dependen de las funciones seleccionadas en el StyleBook durante la creación del paquete de configuración.

Visualización de los objetos definidos en la instancia de Citrix ADC

Una vez creado el paquete de configuración en Citrix ADM, puede ver todos los objetos creados en la instancia de Citrix ADC para el StyleBook de SharePoint. Vaya a **Aplicaciones** > **Administración** > **Configuración** y haga clic en **Ver objetos creados**. La siguiente ilustración muestra algunos de los objetos creados, con las direcciones IP especificadas en el ejemplo que se muestra en "Implementación de configuraciones de SharePoint StyleBook desde Citrix ADM. "

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

StyleBook proxy de Microsoft ADFS

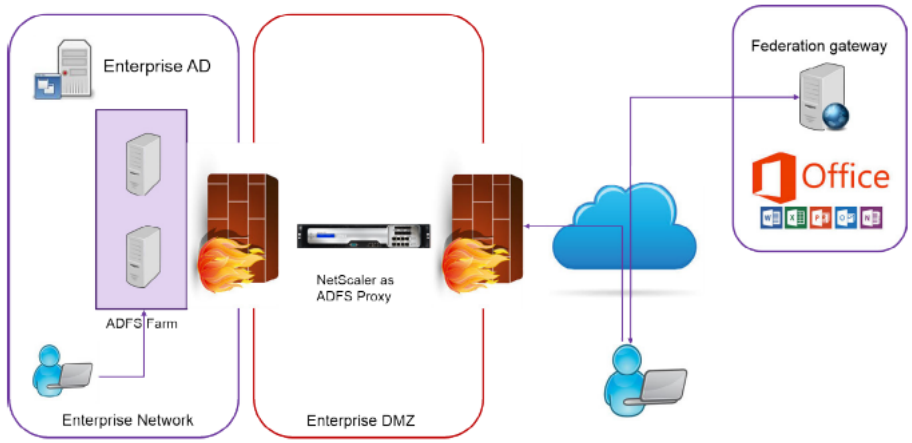
January 30, 2024

El proxy ADFS de Microsoft™ desempeña un papel importante al ofrecer acceso con inicio de sesión único tanto a los recursos internos habilitados por la federación como a los recursos en la nube. Un ejemplo de recursos en la nube es Office 365. El propósito del servidor proxy ADFS es recibir y reenviar solicitudes a servidores ADFS que no son accesibles desde Internet. El proxy ADFS es un proxy inverso y, por lo general, reside en la red perimetral (DMZ) de la organización. El proxy ADFS desempeña un papel fundamental en la conectividad de usuarios remotos y el acceso a aplicaciones.

NetScaler ADC cuenta con la tecnología precisa para permitir la conectividad, la autenticación y el manejo seguros de la identidad federada. El uso de NetScaler ADC como proxy ADFS evita la necesidad de implementar un componente adicional en la DMZ.

Microsoft ADFS Proxy StyleBook en NetScaler Application Delivery Management (ADM) permite configurar un servidor proxy ADFS en una instancia de NetScaler ADC.

La siguiente imagen muestra la implementación de una instancia de Citrix ADC como servidor proxy ADFS en la DMZ empresarial.



Ventajas de usar NetScaler ADC como proxy ADFS

1. Satisface tanto las necesidades de equilibrio de carga como las de proxy ADFS
2. Admite casos de acceso de usuario internos y externos
3. Admite métodos enriquecidos para la autenticación previa
4. Proporciona una experiencia de inicio de sesión único para los usuarios
5. Soporta protocolos activos y pasivos

a) Ejemplos de aplicaciones de protocolo activo son: Microsoft Outlook, Microsoft Skype Empresarial
b) Ejemplos de aplicaciones de protocolo pasivo son: Aplicación web de Microsoft Outlook, exploradores web

6. Dispositivo reforzado para implementación basada en DMZ
7. Añade valor mediante el uso de funciones principales adicionales de Citrix ADC ADC

a) Conmutación de contenido
b) Descarga SSL
c) Reescritura
d) Seguridad (NetScaler ADC AAA)

Para casos basados en protocolos activos, puede conectarse a Office 365 y proporcionar sus credenciales. Microsoft Federation Gateway se pone en contacto con el servicio ADFS (a través del proxy ADFS) en nombre del cliente de protocolo activo. A continuación, la puerta de enlace envía las credenciales mediante la autenticación básica (401). NetScaler ADC gestiona la autenticación del cliente antes de acceder al servicio ADFS. Tras la autenticación, el servicio ADFS proporciona un token SAML a Federation Gateway. Federation Gateway, a su vez, envía el token a Office 365 para proporcionar acceso al cliente.

Para los clientes pasivos, el ADFS Proxy StyleBook crea una cuenta de usuario de delegación restringida de Kerberos (KCD). La cuenta KCD es necesaria para que la autenticación SSO de Kerberos se conecte a los servidores ADFS. El StyleBook también genera una directiva de LDAP y una directiva de sesión. Estas directivas se vinculan posteriormente al servidor virtual AAA de NetScaler ADC que gestiona la autenticación de los clientes pasivos.

El StyleBook también puede garantizar que los servidores DNS del NetScaler ADC estén configurados para ADFS.

La sección de configuración que aparece a continuación describe cómo configurar NetScaler ADC para gestionar la autenticación de clientes basada en protocolos activa y pasiva.

Detalles de configuración

La siguiente tabla muestra las versiones de software mínimas necesarias para que esta integración se implemente correctamente.

Producto	Versión mínima requerida
Citrix ADC	11.0, licencia Enterprise/Platinum

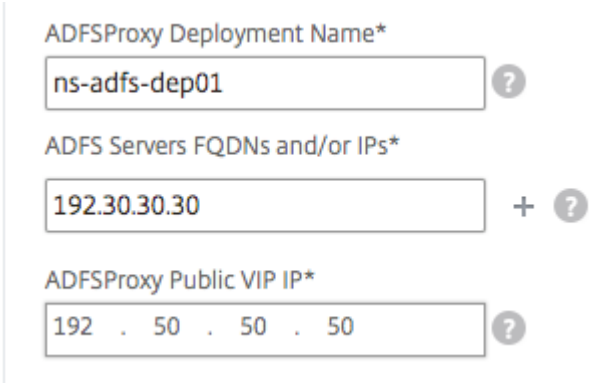
En las instrucciones siguientes se supone que ya ha creado las entradas DNS externas e internas adecuadas.

Implementación de configuraciones de StyleBook de proxy ADFS de Microsoft desde NetScaler ADM

Las siguientes instrucciones le ayudarán a implementar el proxy StyleBook de Microsoft ADFS en su red empresarial.

Para implementar el proxy StyleBook de Microsoft ADFS

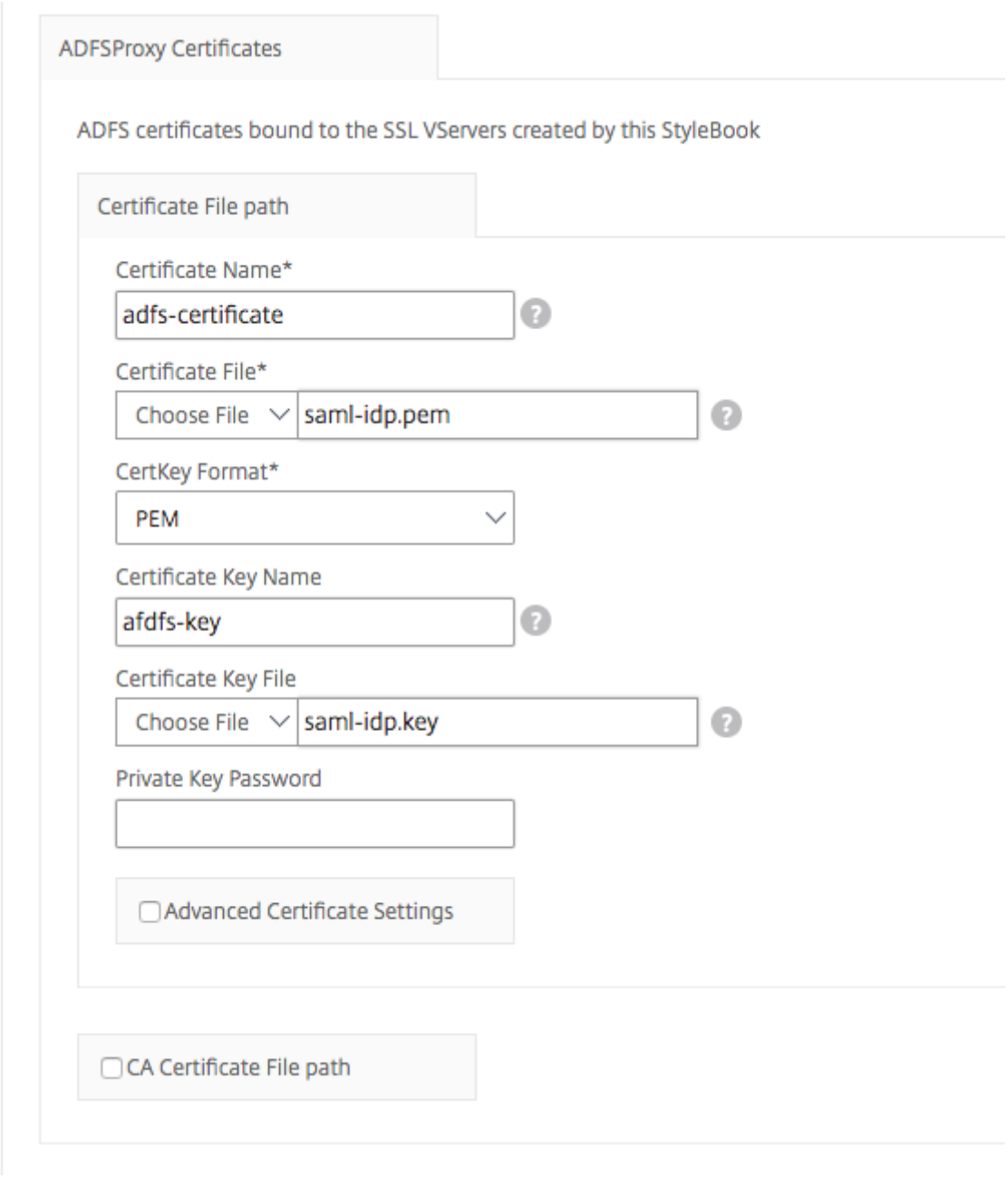
1. En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks**. La página **StyleBooks** muestra todos los StyleBooks disponibles para su uso en Citrix ADM.
2. Desplázate hacia abajo y busca el **proxy de Microsoft ADFS StyleBook**. Haga clic en **Crear configuración**.
   El StyleBook se abre como una página de interfaz de usuario en la que puede escribir los valores de todos los parámetros definidos en este StyleBook.
3. Escriba los valores de los siguientes parámetros:
   a) **Nombre de implementación del proxy ADFS**. Seleccione un nombre para la configuración de proxy ADFS implementada en su red.
   b) **FQDN o IP de los servidores ADFS**. Escriba las direcciones IP o los FQDN (nombres de dominio) de todos los servidores ADFS de la red.
   c) **IP VIP pública de ADFS Proxy**. Escriba la dirección IP virtual pública en el NetScaler ADC que funciona como un servidor proxy ADFS.



4. En la sección **Certificados de proxy ADFS**, escriba los detalles del certificado SSL y la clave de certificado.

   Este certificado SSL está enlazado a todos los servidores virtuales creados en la instancia de NetScaler ADC.

Selecciona los archivos correspondientes de tu carpeta de almacenamiento local. También puede escribir la contraseña de clave privada para cargar claves privadas cifradas en formato.pem.



También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede escribir detalles como el período de notificación de caducidad del certificado, habilitar o inhabilitar el monitor de caducidad del certificado.

5. Opcionalmente, puede activar la casilla de verificación **Certificado de CA SSL** si el certificado SSL requiere que se instale un certificado público de CA en NetScaler ADC. Asegúrese de seleccionar **Es un certificado de CA** en la sección **Configuración avanzada del certificado**.

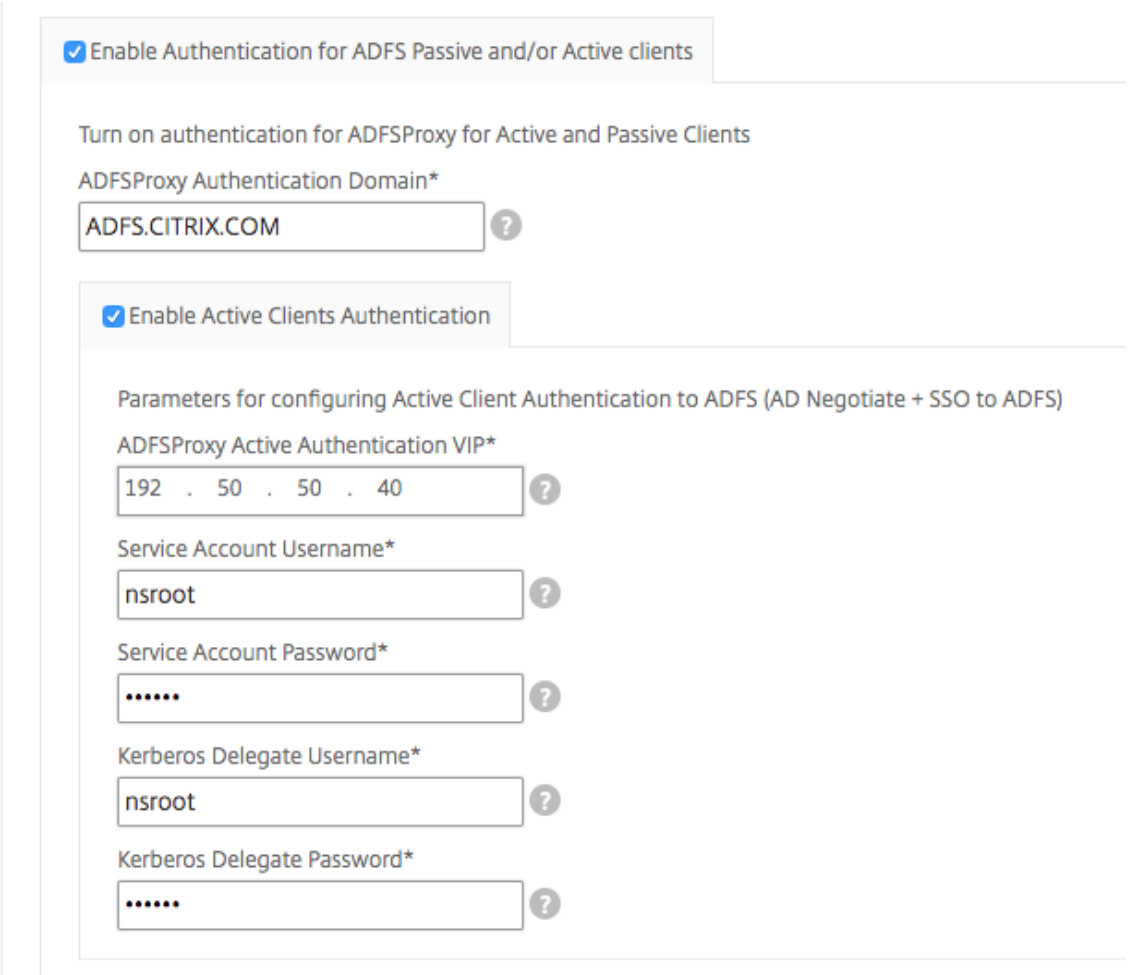
6. Habilitar la autenticación para clientes activos y pasivos. Escriba el nombre de dominio DNS utilizado en Active Directory para la autenticación de usuarios. A continuación, puede configurar la autenticación para los clientes activos o pasivos, o para ambos.
7. Escriba los siguientes detalles para habilitar la autenticación para los clientes activos:

   > **Nota**
   >
   > Es opcional configurar el soporte para los clientes activos.

   a) **Autenticación activa del proxy ADFS VIP**. Escriba la dirección IP virtual del servidor de autenticación virtual en la instancia de NetScaler ADC a la que se redirige a los clientes activos para la autenticación.

   b) Nombre de**usuario de cuenta de servicio** Escriba el nombre de usuario de la cuenta de servicio que utiliza NetScaler ADC para autenticar a los usuarios en el directorio activo.

   c) **Contraseña de cuenta de servicio** Escriba la contraseña utilizada por NetScaler ADC para autenticar a los usuarios en el directorio activo.



8. Configure la autenticación para clientes pasivos habilitando la opción correspondiente y configurando la configuración de LDAP.

   > **Nota**
   >
   > Es opcional configurar el soporte para clientes pasivos.

   Escriba los siguientes detalles para habilitar la autenticación para los clientes pasivos:

   a) **Base LDAP (Active Directory)**. Escriba el nombre de dominio base del dominio en el que residen las cuentas de usuario en Active Directory (AD) para permitir la autenticación. Por ejemplo, dc=netscaler, dc=com

   b) **DN de enlace de LDAP (Active Directory)**. Agregue una cuenta de dominio (mediante una dirección de correo electrónico para facilitar la configuración) que tenga privilegios para examinar el árbol de AD. Por ejemplo, cn=Manager, dc=netscaler, dc=com

   c) **Contraseña de DN de enlace LDAP (Active Directory)**. Escriba la contraseña de la cuenta de dominio para la autenticación.

   Algunos otros campos que debe escribir en los valores de esta sección son los siguientes:

   d) **IP del servidor LDAP (Active Directory)**. Escriba la dirección IP del servidor de Active Directory para que la autenticación de AD funcione correctamente.

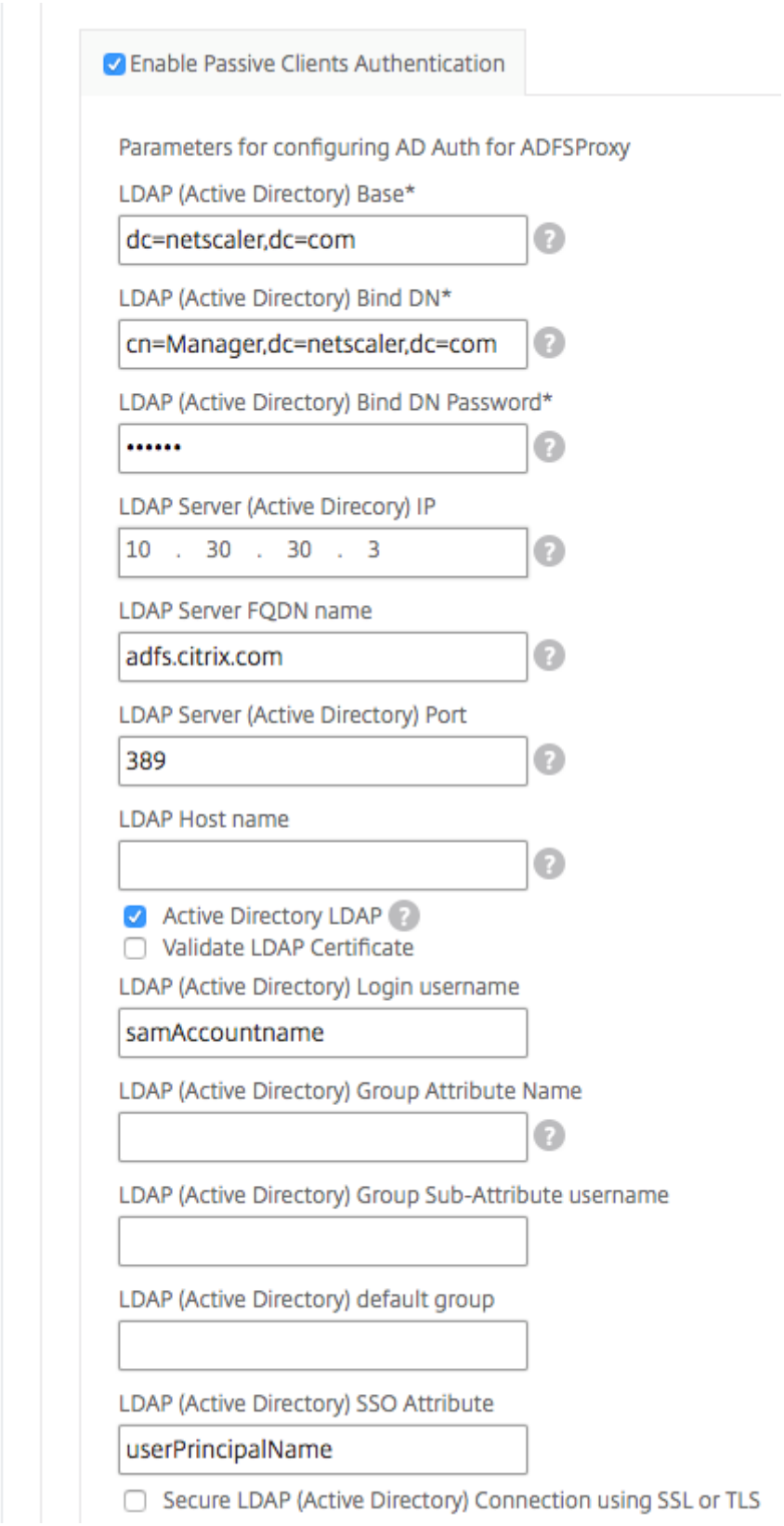
   e) **Nombre de FQDN del servidor LDAP**. Escriba el nombre de FQDN del servidor de Active Directory. El nombre FQDN es opcional. Proporcione la dirección IP tal como se indica en el paso 1 o el nombre del FQDN.

   f) **Puerto de Active Directory del servidor LDAP**. De forma predeterminada, los puertos TCP y UDP del protocolo LDAP son 389, mientras que el puerto TCP del LDAP seguro es 636.

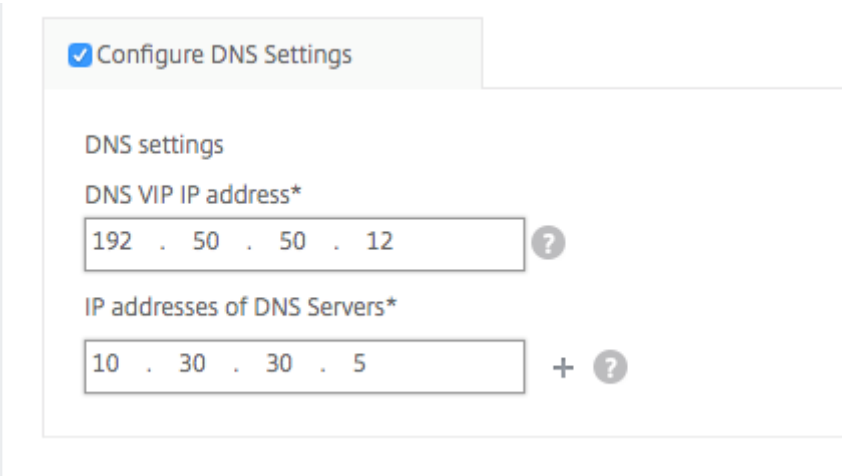
   g) Nombre de**usuario de inicio de sesión LDAP (Active Directory)**. Escriba el nombre de usuario como “samAccountName”.

   h) **Autenticación pasiva de proxy ADFS VIP**. Escriba la dirección IP del servidor virtual proxy ADFS para clientes pasivos.

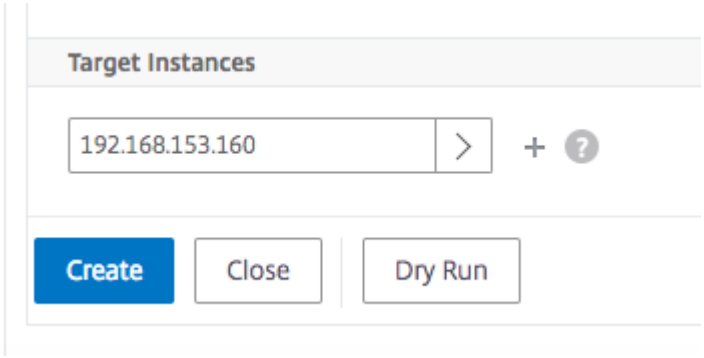
      > **Nota**
      >
      > Los campos marcados con “*”son obligatorios.



9. Opcionalmente, también puede configurar un VIP DNS para sus servidores DNS.



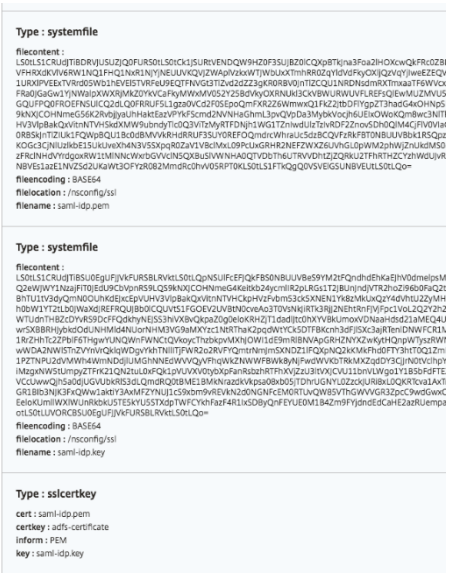
10. Haga clic en **Instancias de destino** y seleccione las instancias de NetScaler ADC para implementar esta configuración de proxy ADFS de Microsoft. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.



> **Nota:**
>
> Citrix recomienda que, antes de ejecutar la configuración real, seleccione **Ejecución en seco**. En primer lugar, puede ver los objetos de configuración que el StyleBook crea en las instancias NetScaler ADC de destino. A continuación, puede hacer clic en **Crear** para implementar la configuración en las instancias seleccionadas.

Objetos creados

Se crean varios objetos de configuración cuando la configuración del proxy ADFS se implementa en la instancia de NetScaler ADC. La siguiente imagen muestra la lista de objetos creados.



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

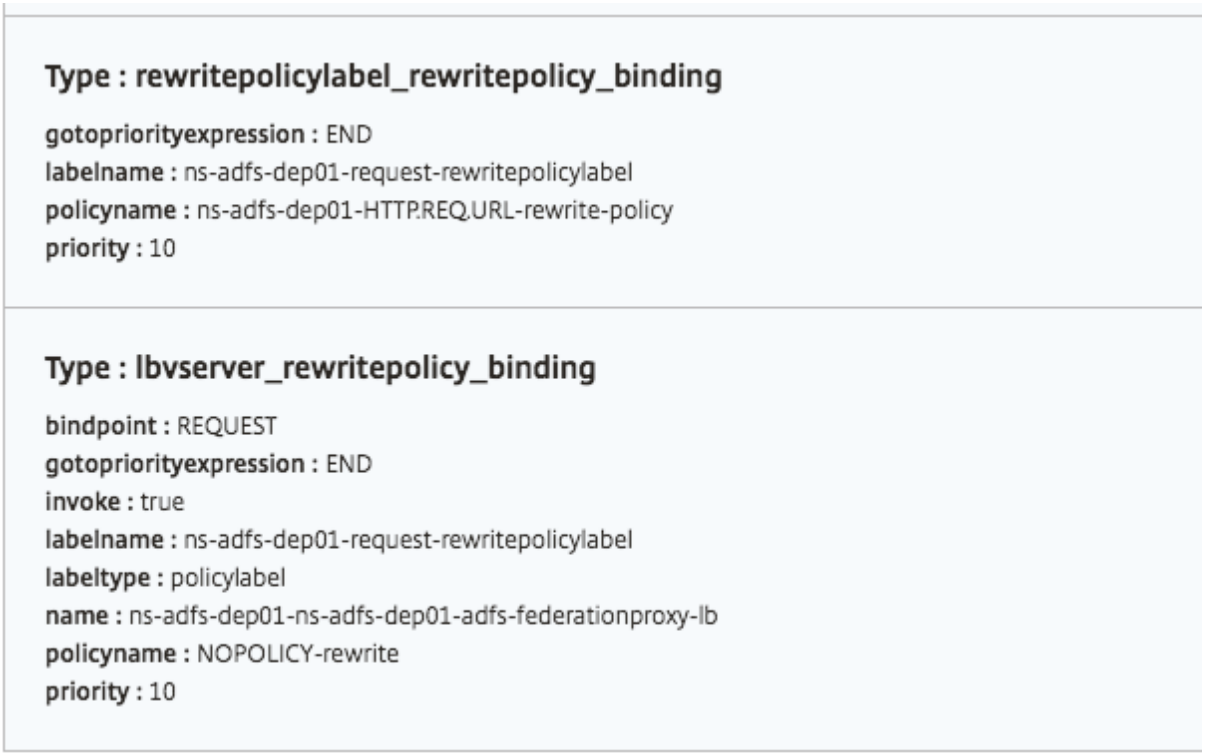
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



StyleBook de Oracle e-business

January 30, 2024

Oracle E-Business Suite es el conjunto más completo de aplicaciones empresariales globales e integradas. Esta suite permite a las organizaciones tomar mejores decisiones, reducir los costes y aumentar el rendimiento, y consta de las siguientes aplicaciones.

- Planificación de recursos empresariales (ERP)
- Gestión de relaciones con los clientes (CRM)
- Gestión de la cadena de suministro (SCM)

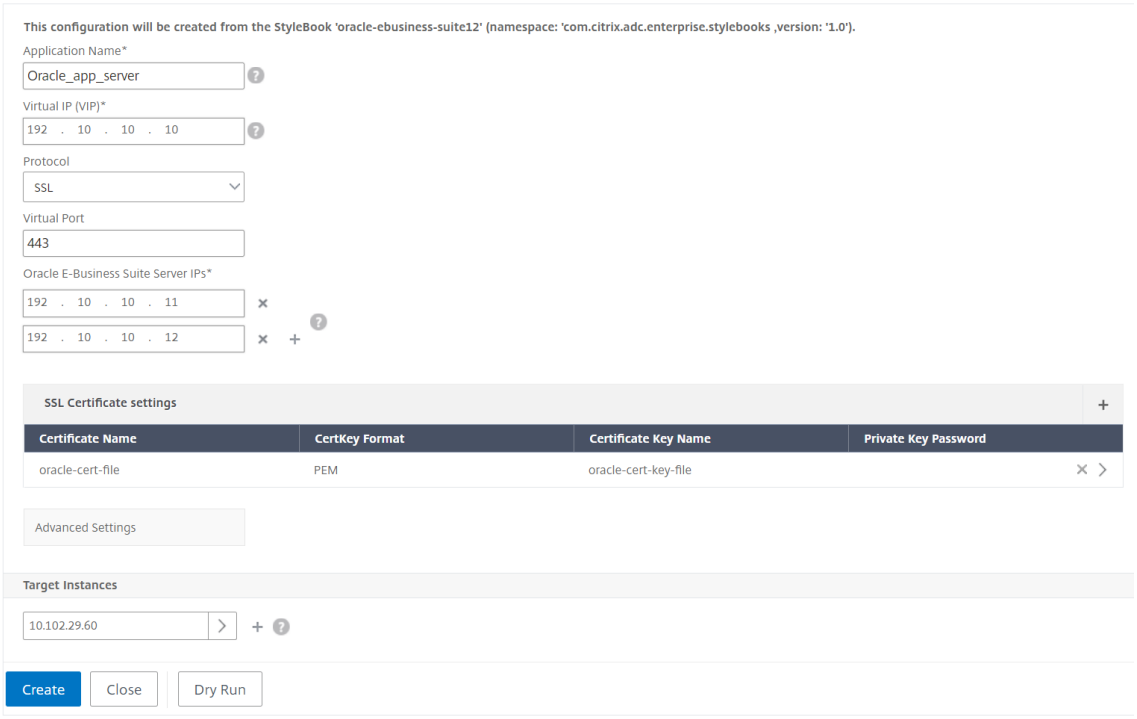
Estas aplicaciones informáticas son desarrolladas o adquiridas por Oracle. El StyleBook de Oracle E-Business Suite 12.2 le permite implementar la configuración en las instancias de NetScaler ADC seleccionadas.

Este StyleBook crea una configuración de equilibrio de carga que incluye un servidor virtual de equilibrio de carga, un grupo de servicios y una lista de servicios. También vincula los servicios al grupo de servicios y enlaza el grupo de servicios al servidor virtual. Puede elegir la comunicación cifrada seleccionando SSL y proporcionando los archivos SSL y los archivos clave de su sistema local.

Para crear una configuración para Oracle E-Business Suite 12.2

1. En NetScaler Application Delivery Management (ADM), vaya a **Aplicaciones** > **Configuración > StyleBooks**. La página **StyleBooks** muestra todos los StyleBooks que están disponibles en su NetScaler ADM. Desplácese hacia abajo y seleccione **Oracle E-Business Suite 12.2**. También puede utilizar la opción de búsqueda para buscar en el StyleBook.
2. Haga clic en **Crear configuración** en el panel StyleBook.
3. Escriba el nombre de la aplicación del balanceador de carga y la dirección IP virtual en la sección de configuración del balanceador de carga.
4. Seleccione el protocolo requerido. Aquí tiene dos opciones: HTTP y HTTPS/SSL. También puede escribir el número de puerto.
5. Escriba las direcciones IP de todos los servidores de aplicaciones de Oracle E-Business Suite de la red que van a equilibrar la carga. Haga clic en **+** para agregar más direcciones IP de servidor.
6. En la sección **Configuración de certificados SSL**, selecciona los archivos correspondientes de tu almacenamiento local. También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede configurar más detalles, como el período de notificación de caducidad del certificado. También puede habilitar o inhabilitar el monitor de caducidad de los certificados.

   Seleccione la instancia de NetScaler ADC de destino en la que debe crearse la configuración y haga clic en **Crear**.



> **Sugerencia**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana. El icono de actualización solo está disponible actualmente en Citrix ADM.

Crear y utilizar StyleBooks personalizados

January 30, 2024

Puede escribir su propio StyleBook para su implementación, importarlo a Citrix Application Delivery Management (ADM) y crear objetos de configuración. También puede usar la API para crear configuraciones desde sus StyleBooks.

Este documento incluye la siguiente información:

Antes de comenzar

Antes de empezar a crear StyleBooks, asegúrese de tener conocimiento de lo siguiente:

- API de NITRO. Para obtener más información, consulte la documentación de la APIde
- YAML

Los archivos StyleBook utilizan el formato YAML. Para obtener información sobre el formato YAML, consulte Sintaxis YAML.

La siguiente es una lista de pautas de YAML que debe tener en cuenta al crear StyleBooks:

- YAML distingue mayúsculas de minúsculas
- YAML requiere una indentación adecuada
- Utilice la tecla <spacebar> para crear una indentación adecuada. No utilice la tecla <tab>. El uso de la tecla <tab> crea un error de compilación al importar su StyleBook a MA Service.
- No utilice cadenas entre comillas. Incluya la cadena entre comillas únicamente si la cadena contiene signos de puntuación (guiones, dos puntos, etc.). Si quiere interpretar un número como una cadena, inclúyalo entre comillas o utilice la función integrada str () de StyleBooks.
- Los literales como sí/sí/sí/y/no/no/no/n/n, encendido/encendido/apagado/apagado/apagado y verdadero/verdadero/falso/falso/falso/falso se consideran booleanos y equivalen a verdadero y falso, respectivamente. Para interpretarlas como cadenas, inclúyalas entre comillas. Por ejemplo:

- "SÍ"
- "No"
- "Cierto"
- "Falso"y así sucesivamente.

> **Nota**
>
> Antes de importar el archivo de StyleBook a NetScaler ADM, se recomienda que valide si el archivo es compatible con el formato YAML. Citrix recomienda utilizar el validador YAML integrado en StyleBooks para validar e importar el contenido YAML.
>
> Al configurar StyleBooks, solo puede usar recursos de configuración de Nitro que admitan las operaciones **Create** y **Delete** (métodos POST y DELETE HTTP). Para obtener más información, consulte la documentación de API de Nitro.

Anatomía de un StyleBook

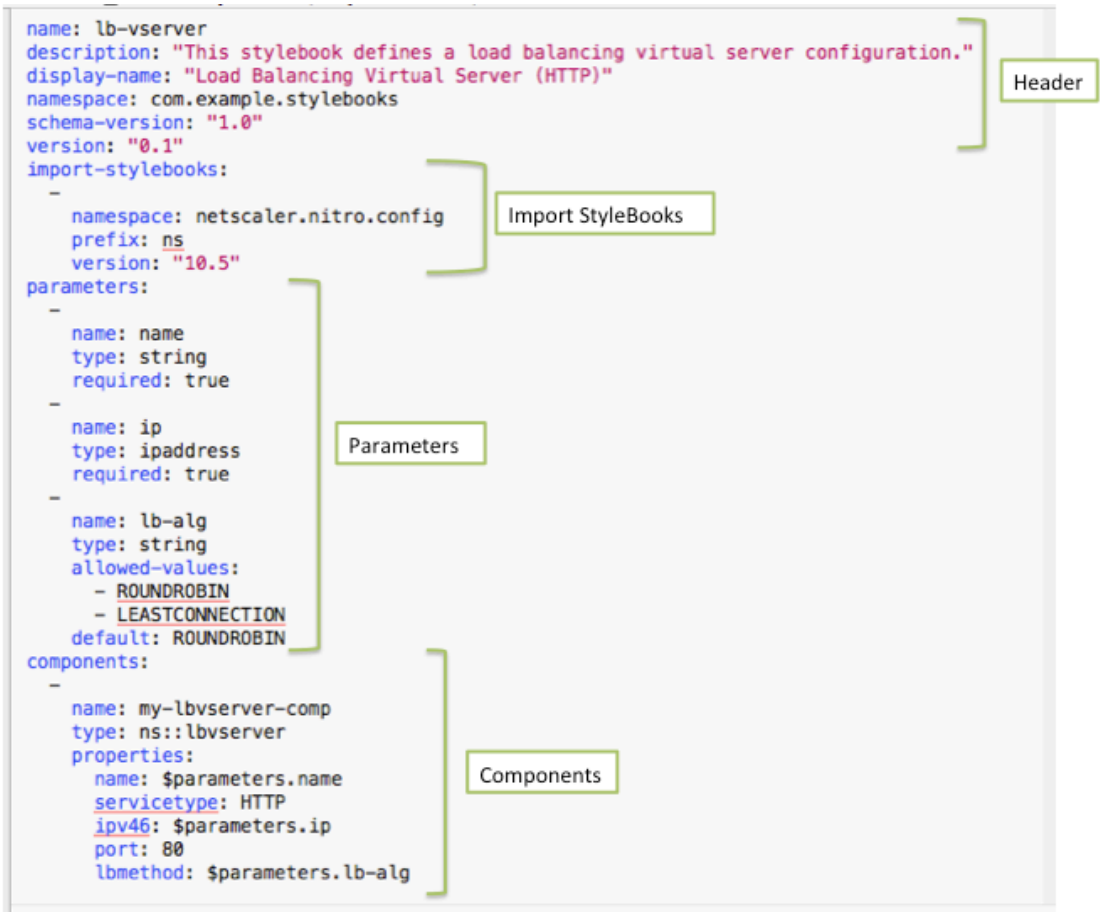
Escribir StyleBooks requiere que comprenda la gramática, la sintaxis y la estructura de los StyleBooks. Un StyleBook típico tiene las siguientes secciones:

- **Encabezado**: esta sección permite definir la identidad de un StyleBook y describir su función. Se trata de una sección obligatoria.
- **Importar StyleBooks**: esta sección le permite declarar a qué otros StyleBook quiere hacer referencia desde su StyleBook actual. Es necesario importar la configuración de NetScaler ADC NITRO, StyleBooks u otros StyleBooks para escribir un StyleBook. Se trata de una sección obligatoria.
- **Parámetros**: esta sección le permite definir los parámetros que necesita en su StyleBook para crear una configuración. Describe la entrada que toma su StyleBook. Se trata de una sección opcional.
- **Componentes**: esta sección le permite definir las entidades (objetos de configuración) que crea el StyleBook para una configuración específica. Esta sección se considera el núcleo de un StyleBook. Los componentes suelen utilizar la entrada proporcionada en la sección de parámetros para adaptar la configuración generada por el StyleBook. Se trata de una sección opcional.

  Un StyleBook puede tener una sección de parámetros, una sección de componentes o ambas. Un StyleBook con solo la sección de parámetros es útil para definir una lista de parámetros que pueden usar otros StyleBooks. Esto promueve la reutilización de los grupos de parámetros en un conjunto de StyleBooks. Se puede usar un StyleBook con solo una sección de componentes cuando quiera especificar los valores de los atributos en el StyleBook en lugar de definir parámetros para tomar las entradas del usuario.

- **Salidas**: mientras que la sección de parámetros define las entradas del StyleBook, esta sección opcional define sus salidas. En esta sección de salidas opcionales, puede especificar los componentes que quiere exponer a los usuarios que creen una configuración a partir de este StyleBook y a otros StyleBooks que lo importen. Los usuarios que importen StyleBooks podrán entonces hacer referencia a las propiedades de los componentes expuestos.
- **Operaciones**: un StyleBook puede contener una sección opcional para habilitar los análisis en NetScaler ADM en cualquier servidor virtual que forme parte del StyleBook.

La siguiente ilustración muestra un esquema simple de un StyleBook.



Los siguientes ejemplos le ayudan a aprender sobre la gramática y la estructura de un StyleBook y cómo escribir StyleBooks con niveles cada vez mayores de complejidad.

- StyleBook para crear un servidor virtual de equilibrio de carga
- StyleBook para crear una configuración básica de equilibrio de carga
- Crear un StyleBook compuesto
- Personaliza su StyleBook usando atributos GUI

StyleBook para crear un servidor virtual de equilibrio de carga

January 30, 2024

En este ejemplo, diseña un StyleBook básico que crea un servidor virtual de equilibrio de carga del tipo de protocolo HTTP y escucha en el puerto 80. Los parámetros del nombre del servidor virtual, la dirección IP y el método de equilibrio de carga aceptan valores definidos por el usuario, es decir, son los parámetros del StyleBook.

Header

Las seis primeras líneas de un StyleBook forman la sección de cabecera. En este ejemplo, la sección de encabezado se escribe de la siguiente manera:

```
name: lb-vserver
description: This StyleBook defines a load balancing virtual server
   configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

La sección del encabezado incluye los siguientes detalles:

- **nombre**: un nombre para este StyleBook.
- **description**: Una descripción que define lo que hace este StyleBook. Esta descripción aparece en NetScaler ADM.
- **display-name**: nombre descriptivo del StyleBook que aparece en NetScaler ADM.
- espacio de**nombres**: un espacio de nombres forma parte de un identificador único de un StyleBook para evitar colisiones de nombres.
- **schema-version**: siempre toma el valor "1.0"en esta versión.
- **version**: El número de versión del StyleBook. Puede cambiar el número de versión al actualizar el StyleBook.

La combinación de **nombre** , **espacio**de nombres y **versión** identifica de forma única un StyleBook en el sistema. No puede tener dos StyleBooks con la misma combinación de nombre, espacio de nombres y versión en NetScaler ADM. Sin embargo, puede tener dos StyleBooks con el mismo nombre y versión pero espacios de nombres diferentes, o con el mismo espacio de nombres y versión pero nombres diferentes.

> **Nota**
>
> Tenga en cuenta que ha actualizado su StyleBook y que tiene un número de versión actualizado. Ahora, si se refiere a (es decir, si va a importar) este StyleBook en otros StyleBooks, asegúrese de actualizar también el número de versión en otros StyleBooks, para que utilicen la versión correcta del StyleBook importado.

Importar StyleBooks

La sección que sigue al encabezado se denomina "import-stylebooks". En esta sección, debe declarar el espacio de nombres y el número de versión de cualquier otro StyleBook al que quiera hacer referencia en su StyleBook actual. Esto le permite importar y reutilizar otros StyleBooks en lugar de volver a crear la misma configuración en su propio StyleBook.

En este ejemplo, la sección de importación de libros de estilo se escribe de la siguiente manera:

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

Cada StyleBook debe hacer referencia al espacio de nombres netscaler.nitro.config si utiliza directamente cualquiera de los objetos de configuración NITRO. Este espacio de nombres contiene todos los tipos de NetScaler ADC NITRO, como lbvserver. Como se admiten las versiones de software 10.5 y posteriores, puede utilizar StyleBook para crear y ejecutar configuraciones en cualquier instancia de NetScaler ADC que ejecute la versión 10.5 y posterior.

El prefijo utilizado en la sección de libros de estilos de importación es una forma abreviada para hacer referencia a la combinación de espacio de nombres y versión. En este caso, ns hace referencia a netscaler.nitro.config de la versión 10.5. En las secciones posteriores del StyleBook, en lugar de utilizar el espacio de nombres y la versión para hacer referencia al StyleBook importado, puede utilizar la cadena de prefijo elegida, por ejemplo, ns, en el ejemplo anterior.

La versión utilizada en los StyleBooks es la versión NetScaler ADC NITRO. Se puede usar un StyleBook basado en la versión X de Nitro para configurar cualquier Citrix ADC de la versión X o superior.

> **Nota**
>
> Para garantizar que los StyleBooks se puedan usar para configurar cualquier instancia de Citrix ADC de la versión 10.5 o posterior, Citrix recomienda que, para obtener la máxima compatibilidad, importe el espacio de nombres Nitro 10.5 en los StyleBooks que usen directamente los StyleBooks integrados de Nitro (espacio de nombres: netscaler.nitro.config, versión: 10.5).

Es importante que un StyleBook que importe otros StyleBooks esté basado en una versión de Nitro igual o superior a la de los StyleBooks que importa. Por ejemplo, un StyleBook basado en la versión 10.5 de Nitro no puede depender de, usar o importar un StyleBook basado en la 11.1. Pero un StyleBook basado en la versión 11.1 puede importar un StyleBook basado en cualquier versión inferior a 11.1.

También es posible que un StyleBook no importe en absoluto el espacio de nombres de Nitro. Esto significa que un StyleBook no necesita definir directamente los componentes de Nitro, sino que puede importar (depender de) los StyleBooks que definen los componentes de Nitro. El StyleBook que importa otros StyleBooks siempre adquiere la versión de Nitro más alta en la jerarquía de sus dependencias y, por lo tanto, podría usarse para configurar los ADC de Citrix que sean de esa versión o superior.

Parámetros

La sección de parámetros le permite declarar todos los parámetros que necesita en su StyleBook. Usted, como desarrollador de StyleBook, tiene que decidir cuál es la entrada que quiere que especifiquen los usuarios de su StyleBook. En este ejemplo, ha creado su StyleBook de forma que requiere que sus usuarios proporcionen el nombre del servidor virtual, su dirección IP y el método de equilibrio de carga.

La sección de parámetros tendría el siguiente aspecto:

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Name of the application configuration.
  required: true

 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access.
  required: true

-
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm (method) used for
     load balancing client request between the application servers.
  allowed-values:
   - ROUNDROBIN
   - LEASTCONNECTION
   default: ROUNDROBIN
```



```
<!--NeedCopy-->
```

> **Nota**
>
> Si no proporciona la etiqueta de un parámetro, NetScaler ADM utilizará el atributo name al mostrar este parámetro. Siempre debe definir una etiqueta para los parámetros de modo que pueda controlar cómo se muestran en NetScaler ADM.
>
> Sin embargo, al utilizar las API, el parámetro se designa por su nombre.

En esta sección, ha declarado tres parámetros indicados por sus valores de atributos de **nombre**: **nombre** para el nombre del servidor virtual, **ip** para la dirección IP del servidor virtual y **lb-alg** para el método de equilibrio de carga.

- **type**. Tipo de valor que pueden tomar estos parámetros. Por ejemplo, name y lb-alg pueden tomar un valor de cadena y el valor ip debe ser del tipo ip address. Los parámetros de un StyleBook pueden ser de cualquiera de los siguientes tipos incorporados:
- **cadena**. Una variedad de personajes. Si no se especifica una longitud, el valor de cadena puede tener cualquier número de caracteres. Sin embargo, puede limitar la longitud de un tipo de cadena utilizando los atributos longitud mínima y longitud máxima.
- **número**. Un número entero. Puede especificar el número mínimo y máximo que puede tomar este tipo mediante los atributos valor mínimo y valor máximo.
- **booleano**. Puede ser verdadera o falsa. Además, ten en cuenta que YAML considera todos los literales como booleanos (por ejemplo, Sí o No).
- **ipaddress**. Cadena que representa una dirección IPv4 o IPv6 válida.
- **puerto TCP.** Número comprendido entre 0 y 65535 que representa un puerto TCP o UDP.
- **contraseña**. Un valor de cadena opaco/secreto. Cuando NetScaler ADM muestra un valor para este parámetro, se muestra como asteriscos (*****).
- **archivo de certificados.** Archivo de certificado.
- **archivo de claves**. Archivo de clave privada del certificado.
- **archivo**. Un parámetro de este tipo requiere que el usuario cargue un archivo, por ejemplo, un archivo de certificado o clave.
- **objeto**. Consta de varios elementos y cada uno de ellos es un parámetro. Este tipo se puede utilizar para agrupar varios parámetros relacionados bajo un parámetro principal.
- **requerida**. Indica si un parámetro es obligatorio u opcional. Si se establece en true, el parámetro es obligatorio y el usuario tiene que proporcionar un valor para este parámetro al crear configuraciones con este StyleBook. De forma predeterminada, todos los parámetros

son opcionales. En este ejemplo, **name** e **ip** son parámetros obligatorios, mientras que **lb-alg** es un parámetro opcional, cuyo valor predeterminado es "ROUNDROBIN".

Utilice el atributo **predeterminado** para asignar un valor por defecto a un parámetro opcional. Al crear una configuración, si un usuario no especifica un valor, se utiliza el valor predeterminado. Por ejemplo, para el parámetro **lb-alg**, el valor predeterminado es ROUNDROBIN.

Utilice el atributo **de valores permitidos** para definir valores específicos entre los que el usuario puede elegir al crear una configuración. En este ejemplo, especificó dos valores para el parámetro **lb-alg**: ROUNDROBIN y LEASTCONNECTION.

Al importar su StyleBook y usarlo, NetScaler ADM muestra un formulario con estos tres parámetros. Los campos que se muestran para nombre e IP permiten introducir el tipo de valor de cadena y dirección IP, y el campo lb-alg se muestra como una lista desplegable con ROUNDROBIN seleccionado como valor predeterminado.

> **Nota**
>
> Además de los tipos integrados, un parámetro puede tener otro StyleBook como tipo. Se trata de una forma de reutilizar los parámetros definidos en otros StyleBooks.

Componentes

La última sección de este StyleBook se llama la sección de componentes y se considera como la sección más importante del StyleBook. En esta sección, se definen los objetos de configuración que debe crear el SyleBook.

Para este ejemplo, debe escribir la sección de componentes de la siguiente manera:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Este ejemplo contiene solo un componente. Los atributos principales de un componente son el nombre, el tipo y las propiedades. El tipo de componente determina las propiedades que proporciona este componente. Los componentes son de dos tipos:

- **Tipo incorporado**. El sistema proporciona este tipo y no es necesario que lo defina; por ejemplo, los tipos de entidades NITRO son "lbvserver"o "servicegroup". En este ejemplo, utiliza un

tipo de componente integrado.

- **Tipo compuesto**. Este tipo es el StyleBook que creó e importó en NetScaler ADM, o el StyleBook predeterminado que se incluye con NetScaler ADM. Puede obtener más información sobre los StyleBooks compuestos en Crear un StyleBook compuesto.

En este ejemplo, ha definido un componente denominado **lbvserver-comp**. Este componente es de tipo **ns::lbvserver** (un tipo Nitro incorporado), donde "ns"es el prefijo que hace referencia al espacio de nombres netscaler.nitro.config y la versión 10.5 que había especificado en la sección import-stylebooks, y "lbvserver"es un recurso Nitro en este espacio de nombres.

Las **propiedades** definidas aquí son los atributos del recurso "lbvserver". Para obtener más información sobre todos los recursos disponibles de NetScaler ADC Nitro y sus atributos, consulte la documentación de la API REST de NetScaler ADC NITRO.

Las propiedades de esta sección incluyen los atributos obligatorios del recurso "lbvserver"y le permiten especificar valores para estos atributos. En este ejemplo, está especificando valores estáticos para servicetype y port, mientras que las propiedades name, ipv46 y lbmethod obtienen sus valores de los parámetros de entrada. En el resto del StyleBook, puede hacer referencia a los nombres de parámetros definidos en la sección de parámetros mediante la expresión **$parameters.<parameter-name>**, por ejemplo, **$parameters.ip**.

> **Nota**
>
> Por convención, el prefijo «ns» siempre se usa para designar un espacio de nombres Citrix ADC Nitro en la sección «libros de estilo de importación». Aunque no es obligatorio, Citrix recomienda utilizar la misma convención en sus propios StyleBooks para mayor coherencia.

Crea su StyleBook

Ahora que ha definido todas las secciones requeridas de este StyleBook, reúna todas para crear su primer StyleBook. Copie y pegue el contenido de StyleBook en un editor de texto y, a continuación, guarde el archivo como **lb-vserver.yaml**. Citrix recomienda utilizar el validador de YAML integrado en StyleBooks para validar e importar el contenido de YAML.

El contenido completo del archivo lb-vserver.yaml se reproduce a continuación:

```
1 name: lb-vserver
2 namespace: com.example.stylebook
3 version: "1.0"
4 display-name: Load Balancing Virtual Server (HTTP)
5 description: "This stylebook defines a very simple load balancing HTTP
     virtual server configuration"
6 schema-version: "1.0"
7
8 import-stylebooks:
```



```
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION

components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC load balancing virtual server configuration
     object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
   lbmethod: $parameters.lb-alg
   servicetype: HTTP
   port: 80
<!--NeedCopy-->
```

Para comenzar a usar su StyleBook para crear configuraciones, debe importarlo a NetScaler ADM y luego usarlo. Para obtener más información, consulte Cómo utilizar StyleBooks definidos por el usuario.

También puede importar este StyleBook a otros StyleBooks (usando la construcción import-

stylebooks). O bien, puede modificar este StyleBook para incluir más parámetros y componentes como se describe en la siguiente sección.

StyleBook para crear una configuración básica de equilibrio de carga

January 30, 2024

En el ejemplo anterior, creó un StyleBook básico para crear un servidor virtual de equilibrio de carga. Puede guardar este StyleBook con un nombre diferente y, a continuación, actualizarlo para incluir parámetros y componentes adicionales para una configuración básica de equilibrio de carga. Guarde este archivo de StyleBook como **basic-lb-config.yaml**.

En esta sección, diseñará un nuevo StyleBook que cree una configuración de equilibrio de carga compuesta por un servidor virtual de equilibrio de carga, un grupo de servicios y una lista de servicios. También vincula los servicios al grupo de servicios y enlaza el grupo de servicios al servidor virtual.

Header

Para crear este StyleBook, tiene que empezar por actualizar la sección del encabezado. Esta sección es similar a la que creó para el servidor virtual de equilibrio de carga StyleBook. En la sección del encabezado, cambie el valor del **nombre** a basic-lb-config. Además, actualice la **descripción** y el **nombre de visualización** para describir este StyleBook de forma adecuada. No es necesario cambiar los valores del espacio de **nombres** ni de la **versión**. Como ha cambiado el nombre, la combinación de nombre, espacio de nombres y versión crea un identificador único para este StyleBook en el sistema.

```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Importar StyleBooks

La sección Import-StyleBooks sigue siendo la misma. Hace referencia al espacio de nombres netscaler.nitro.config para usar los objetos de configuración de Nitro.

```
import-stylebooks:
```



```
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

Parámetros

Tiene que actualizar la sección de parámetros para agregar dos parámetros adicionales para definir la lista de servicios o servidores y el puerto en el que los servicios escuchan. Los tres primeros parámetros, name, ip y lb-alg, siguen siendo los mismos.

```
parameters:
 -
 name: name
 type: string
 label: Application Name
 description: Name of the application configuration
 required: true
  -
   name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
   description: Application VIP that the clients access
   required: true
  -
   name: lb-alg
   type: string
   label: LoadBalancing Algorithm
   description: Choose the load balancing algorithm used for load
      balancing client requests between the application servers.
     allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
      default: ROUNDROBIN
  -
   name: svc-servers
   type: ipaddress[]
   label: Application Server IPs
   description: The IP addresses of all the servers of this application
   required: true
  -
   name: svc-port
   type: tcp-port
   label: Server Port
   description: The TCP port open on the application servers to receive
       requests.
   default: 80
<!--NeedCopy-->
```

En este ejemplo, se agrega el parámetro **svc-servers** para aceptar una lista de direcciones IP de los

servicios que representan los servidores de fondo de la aplicación. Este es un parámetro obligatorio como se indica por **requerido: True**. El segundo parámetro, **svc-port**, indica el número de puerto en el que escuchan los servidores. El número de puerto predeterminado es 80 para el parámetro svc-port, si el usuario no lo ha especificado.

Componentes

También debe actualizar la sección de componentes para definir componentes adicionales de modo que utilicen los dos nuevos parámetros y creen la configuración completa de equilibrio de carga.

Para este ejemplo, debe escribir la sección de componentes de la siguiente manera:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

En este ejemplo, el componente original **lbvserver-comp** (del ejemplo anterior) ahora tiene un com-

ponente secundario llamado **svcg-comp**. Además, el componente **svcg-comp** contiene dos componentes secundarios. Al anidar un componente dentro de otro componente, el componente anidado puede crear objetos de configuración haciendo referencia a los atributos del componente principal. El componente anidado puede crear uno o más objetos para cada objeto creado en el componente principal.

El componente **svcg-comp** se usa para crear un grupo de servicios en la instancia de NetScaler ADC mediante los valores proporcionados para los atributos del recurso "servicegroup". En este ejemplo, especificará un valor estático para el tipo de servicio, mientras que el nombre obtiene su valor del parámetro de entrada. Para hacer referencia al **nombre** del parámetro definido en la sección de parámetros, utilice la notación **$parameters.name + "-svcgrp", donde**-svcgrp** se agrega (concatena) al nombre definido por el usuario.

El componente **svcg-comp** tiene dos componentes secundarios, **lbvserver-svg-binding-comp** y **members-svcg-comp**.

El primer componente secundario, **lbvserver-svg-binding-comp**, se usa para vincular un objeto de configuración entre el grupo de servicios creado por su componente principal y el servidor virtual de equilibrio de carga (lbvserver) creado por el componente principal del componente principal. La notación $principal, también llamada referencia principal, se utiliza para hacer referencia a entidades en los componentes principal. Por ejemplo, **servicegroupname: $parent.properties.name** hace referencia al grupo de servicios creado por el componente principal **svcg-comp**, y **name: $parent.parent.properties.name** hace referencia al servidor virtual creado por el componente principal **lbvserver-comp**.

El componente **members-svcg** se utiliza para vincular los objetos de configuración de la lista de servicios al grupo de servicios creado por el componente principal. La creación de múltiples objetos de configuración de enlace se logra mediante el uso de la construcción de **repetición** de StyleBook para iterar sobre la lista de servidores especificados en el parámetro **svc-servers**. Durante la iteración, este componente StyleBook crea un objeto de configuración Nitro de tipo **servicegroup_servicegroupmember_binding** para cada servicio (denominado srv en la construcción **repeat-item**) en el grupo de servicios, y establece el atributo **ip** en cada Nitro objeto de configuración a la dirección IP del servidor correspondiente.

Por lo general, puede utilizar las construcciones **repeat y**repeat-item**** de un componente para hacer que ese componente genere varios objetos de configuración del mismo tipo. Puede asignar un nombre de variable a la construcción **repeat-item**, por ejemplo, srv, para designar el valor actual en la iteración. En las propiedades del mismo componente o en los componentes secundarios se hace referencia a este nombre de variable como **$<varname>**, por ejemplo, $srv.

En el ejemplo anterior, ha utilizado anidamiento de componentes dentro de otros para construir fácilmente esta configuración. En este caso concreto, el anidamiento de los componentes no era la única forma de crear la configuración. Podrías haber obtenido el mismo resultado sin anidar, como se muestra a continuación:


```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
  name: $parameters.name + "-svcgrp"
  servicetype: HTTP
<!--NeedCopy-->
```

Aquí, todos los componentes están en el mismo nivel (es decir, no están anidados) pero el resultado obtenido (la configuración de Citrix ADC generada) es el mismo que el de los componentes anidados utilizados anteriormente. Además, el orden en el que se declaran los componentes en el StyleBook no afecta al orden de creación de los objetos de configuración. En este ejemplo, los componentes **svcg-comp y**lbvserver-comp****, aunque se declaren en último lugar, se deben crear antes de compilar el segundo componente **lbvserver-svg-binding-comp**porque hay referencias directas a estos componentes en el segundo componente.

> **Nota**
>
> Por convención, los nombres de los StyleBooks, los parámetros, las sustituciones, los componentes y las salidas aparecen en minúsculas. Cuando contienen varias palabras, están separadas por un carácter "-". Por ejemplo, "lb-bindings", "app-name", "rewrite-config", etc. Otra convención consiste en agregar el sufijo "-comp"a los nombres de los componentes.

Resultados

La última sección que puede agregar al nuevo StyleBook es la sección de salidas donde se especifica lo que este StyleBook expone a sus usuarios (o en otros StyleBooks) después de que se use para crear una configuración. Por ejemplo, puede especificar en la sección de salidas que se muestren los objetos de configuración lbvserver y servicegroup que crearía este StyleBook.

```
outputs:
 -
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
 -
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

La sección de salidas de un StyleBook es opcional. No es necesario que un StyleBook devuelva las salidas. Sin embargo, al devolver algunos componentes internos como salidas, permite a los StyleBooks que importen este StyleBook una mayor flexibilidad, como se puede ver al crear un StyleBook compuesto.

> **Nota**
>
> Se recomienda exponer un componente completo del StyleBook en la sección de resultados, en lugar de una sola propiedad de un componente (por ejemplo, exponer el $components.lbvserver-comp completo en lugar de solo el nombre $components.lbvserver-comp.properties.name). Agregue también una descripción a la salida que explique lo que representa la salida específica.

Crea su StyleBook

Ahora que ha definido todas las secciones requeridas de este StyleBook, reúna todas para crear su segundo StyleBook. Ya ha guardado este archivo StyleBook como **basic-lb-config.yaml**. Citrix recomienda utilizar el validador de YAML integrado en la página StyleBooks para validar e importar el contenido de YAML.

El contenido completo del archivo **basic-lb-config.yaml** se reproduce a continuación:

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
```



```
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
  type: ipaddress[]
  label: Application Server IPs
  description: The IP addresses of all the servers of this application
  required: true

components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
```



```
56      servicegroupname: $parameters.name + "-svcgrp"
57      servicetype: HTTP
58
59   -
60    name: lbvserver-svg-binding-comp
61    type: ns::lbvserver_servicegroup_binding
62    properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65   -
66    name: members-svcg-comp
67    type: ns::servicegroup_servicegroupmember_binding
68    repeat: $parameters.svc-servers
69    repeat-item: srv
70    properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74 outputs:
75 -
76    name: lbvserver-comp
77    value: $components.lbvserver-comp
78    description: The component that builds the Nitro lbvserver
         configuration object
79 -
80    name: servicegroup-comp
81    value: $components.svcg-comp
82    description: The component that builds the Nitro servicegroup
         configuration object
83 <!--NeedCopy-->
```

Para comenzar a usar su StyleBook para crear configuraciones, debe importarlo a NetScaler ADM y luego usarlo. Para obtener más información, consulte Cómo utilizar StyleBooks definidos por el usuario.

También puede importar este StyleBook a otros StyleBooks y utilizar sus propiedades como se describe en la siguiente sección.

Crear un StyleBook compuesto

January 30, 2024

Una función importante y poderosa de StyleBooks es que se pueden usar como bloques de construcción para otros StyleBooks. Se puede importar un StyleBook a otro StyleBook y se le puede denominar como el **tipo** que utilizan los componentes del segundo StyleBook, de forma similar a un StyleBook integrado en Nitro.

Por ejemplo, puede usar el StyleBookbasic-lb-config**que creaste en la sección anterior para crear**

otro StyleBook llamado composite-example. Para usar el StyleBook "basic-lb-config", debe importarlo al nuevo StyleBook en la sección de importación de libros de estilo.

Crea su StyleBook

El nuevo StyleBook se vería de la siguiente manera:

```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
   namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    description: Give a name to the application configuration.
    required: true
  -
    name: ip
    type: ipaddress
    label: Application Virtual IP (VIP)
    description: The Application VIP that clients access
    required: true
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this
       application
    required: true

  -
    name: response-code
    type: string[]
    label: List of Response Codes
    description: List of Response Codes - Provide a list of response
       codes in integer.

components:
```



```
43    -
44      name: basic-lb-comp
45      type: stlb::basic-lb-config
46      description: This component's type is another StyleBook that builds
            the NetScaler lbvserver, servicegroups and services
           configuration objects.
47      properties:
48       name: $parameters.name
49       ip: $parameters.ip
50       svc-servers: $parameters.svc-servers
51    -
52       name: monit-comp
53       type: ns::lbmonitor
54       description: This component is a basic Nitro type (a Builtin
            StyleBook) that builds the NetScaler monitor configuration
            object.
55       properties:
56         monitorname: $parameters.name + "-mon"
57         type: HTTP
58         respcode: $parameters.response-code
59         httprequest: "'GET /'"
60         lrtm: ENABLED
61         secure: "YES"
62
63       components:
64          -
65            name: monit-svcgrp-bind-comp
66            type: ns::servicegroup_lbmonitor_binding
67            properties:
68              servicegroupname: $components.basic-lb-comp.outputs.
                    servicegroup-comp.properties.servicegroupname
69              monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

En la sección Import-stylebooks, se importa el StyleBook basic-lb-config utilizando su espacio de nombres y su versión, denominados con el prefijo “stlb”.

En la sección de componentes, se definen dos componentes. El primer componente es de tipo **stlb::basic-lb-config**, donde “basic-lb-config”es el nombre del StyleBook que creó en StyleBook para crear una configuración básica de equilibrio de carga. Las propiedades definidas para este componente corresponden a los parámetros obligatorios declarados en el StyleBook basic-lb-config. Sin embargo, puede utilizar cualquier parámetro del StyleBook (obligatorio y opcional). En lugar de volver a crear un lbvserver, un grupo de servicios y los enlaces de servicios y grupos de servicios, importa el StyleBook que hace todo esto como un componente y lo usa para crear estos objetos de configuración en el nuevo StyleBook.

StyleBook agrega un segundo componente, “monit-comp”, que utiliza los atributos del recurso “lbmonitor”de Nitro (un StyleBook integrado) para crear un objeto de configuración de monitor. También tiene un subcomponente “monit-svcgrp-bind-comp”para crear el objeto de configuración de enlace que vincula el monitor al grupo de servicios creado en el primer componente.

Como el componente servicegroup creado en el StyleBook "basic-lb-config"se expone como salida, este StyleBook puede acceder a él mediante la expresión $components.basic-lb-comp.outputs.servicegroup-comp. Este es un ejemplo de cómo la sección de salidas puede ser utilizada por los StyleBooks importadores para tener acceso a los componentes de los StyleBooks importados a los que no habrían podido acceder de otro modo.

A continuación, copie y pegue el contenido de StyleBook en un editor de texto y, a continuación, guarde el archivo como **composite-example.yaml**. Asegúrese de validar el contenido de YAML antes de importar el archivo en NetScaler ADM. A continuación, impórtelo a NetScaler ADM y cree una o varias configuraciones con este StyleBook.

Citrix recomienda utilizar el validador YAML integrado en StyleBooks para validar e importar el contenido YAML.

Usar atributos de GUI en un StyleBook personalizado

January 30, 2024

Puede agregar atributos de GUI en la sección de parámetros de su StyleBook para que los campos sean intuitivos cuando se muestren en NetScaler Application Delivery Management (ADM).

Un ejemplo. Puede agregar un nombre descriptivo al parámetro mediante el atributo label y agregar una descripción emergente para este parámetro mediante el atributo description.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
   balanced application.
type: ipaddress
required: true
<!--NeedCopy-->
```

Un ejemplo. Si tiene un parámetro de tipo objeto, puede definir el diseño mediante el atributo **gui**. En este ejemplo, el diseño es un objeto contraíble donde los campos se muestran en dos columnas.

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

Un ejemplo. También puede mostrar una vista resumida de un parámetro de tipo object [] (lista de objetos) como una tabla con los parámetros internos que representan las columnas. Para incluir o

excluir un parámetro interno de la vista de resumen, puedes usar el atributo summary_display en la sección de la interfaz gráfica de usuario de la siguiente manera:

```
name: settings
label: Settings
type: object[]
parameters:
  -
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

Un ejemplo. Algunos StyleBooks de Citrix ADM solo se utilizan como componentes básicos para otros StyleBooks. Además, es posible que no quiera que los usuarios creen configuraciones directamente desde estos StyleBooks. Porque estos StyleBooks deben usarse como parte de otros StyleBooks. Marque el StyleBook como privado para asegurarse de que el StyleBook no se utiliza directamente para crear configuraciones en la GUI de NetScaler ADM.

```
name: basic-lb-config
description: This stylebook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

Usar StyleBooks personalizados

January 30, 2024

Una vez creado el StyleBook, debe importarlo a NetScaler ADM para usarlo. NetScaler ADM le permite importar un único StyleBook en formato YAML o varios archivos YAML de StyleBook como un paquete en un formulario.zip,.tgz o.gz. El sistema NetScaler ADM valida sus StyleBooks al importar. El Stylebook ya está listo para usarse para crear configuraciones.

NetScaler ADM también tiene un editor YAML integrado que puede utilizar para componer el contenido YAML de StyleBook. El editor YAML permite validar las construcciones YAML desde la propia GUI de Citrix ADM. No es necesario utilizar una herramienta independiente para estas comprobaciones de validación. El contenido se valida según los estándares YAML y cualquier desviación se resalta. A

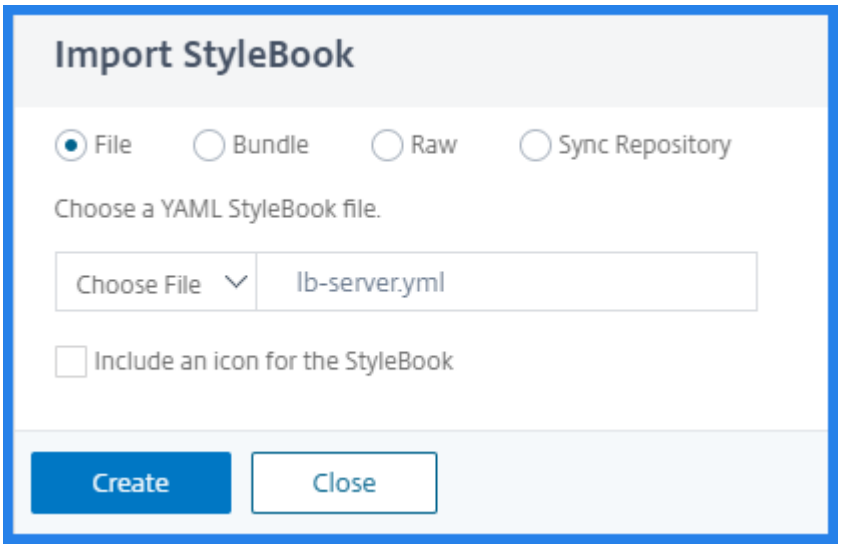
continuación, puede corregir el contenido e intentar importar el StyleBook a NetScaler ADM. El editor YAML integrado proporciona dos ventajas mientras escribe su propio StyleBook.

- **Codificado por colores**. El editor muestra el contenido del StyleBook analizado según las pautas de YAML, y el código de colores le ayuda a diferenciar fácilmente entre las claves y los valores definidos en el contenido de YAML.
- **Validación de YAML**. El contenido se valida para cualquier error de YAML a medida que escribe y cualquier desviación se resalta inmediatamente. Esto le permite escribir texto que se ajuste a las directrices de YAML incluso antes de importar StyleBook en NetScaler ADM. Actualmente, el editor valida el contenido de acuerdo con las directrices de YAML. No valida la corrección del código y los errores tipográficos.

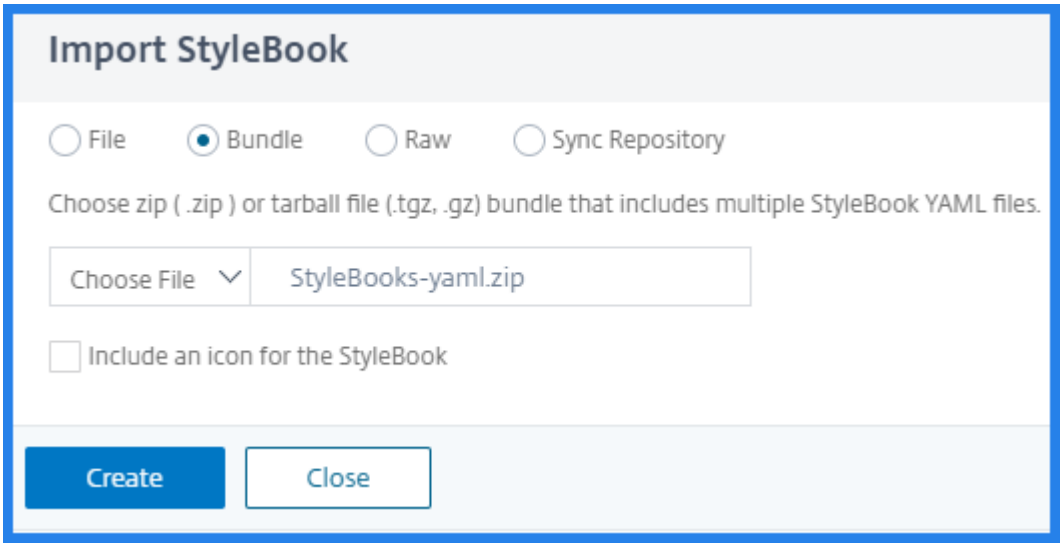
Importación de su StyleBook

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración** > **StyleBooks** y, a continuación, haga clic en **Importar nuevo StyleBook** .
2. Haga clic en una de las tres opciones disponibles para importar el StyleBook.
   a) **Expediente**. Seleccione el archivo requerido o el paquete de archivos de su almacenamiento local.

   > **Nota**
   >
   > En este ejemplo, importe el StyleBook «lb-vserver.yaml» que había creado en StyleBook para crear un servidor virtual de equilibrio de carga.

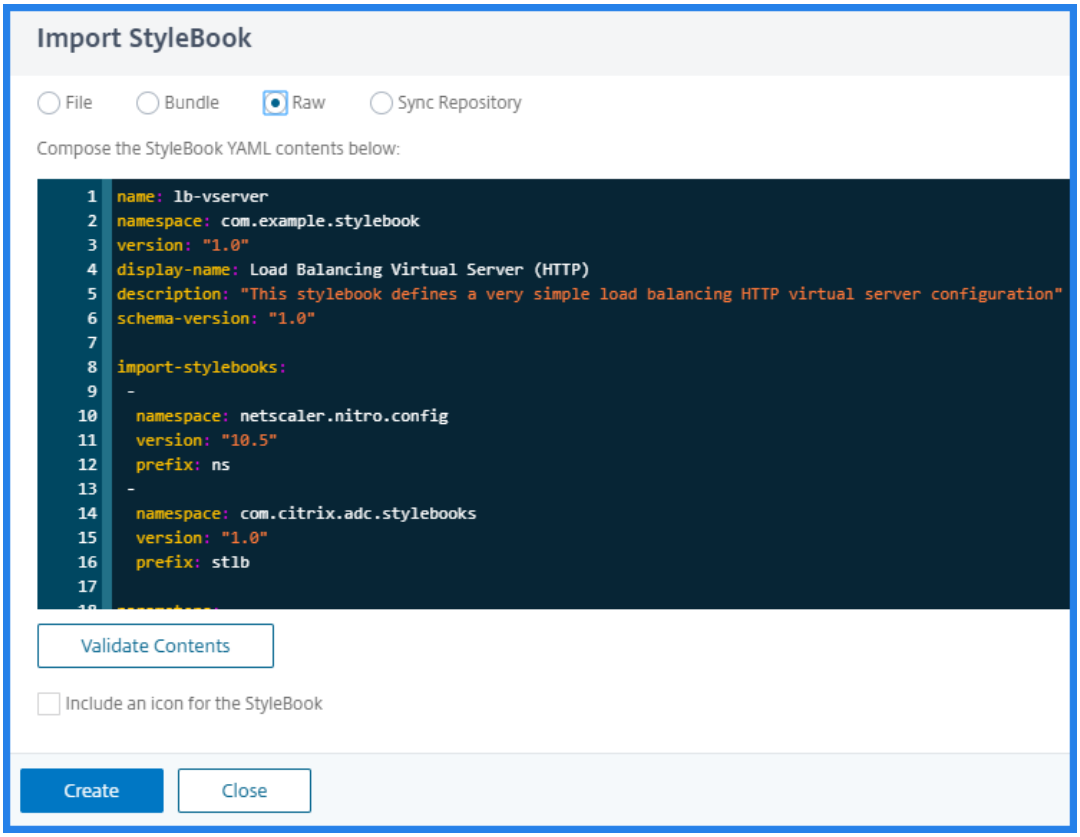
   b) **Paquete**. Citrix ADM permite importar varios StyleBooks en formato YAML. Puede importar más de un archivo YAML StyleBook comprimido en formato zip (.zip) o tarball (.tgz,.gz).



c) **Crudo**. Redacta el contenido de tu StyleBook en el editor YAML.

> **Nota**
>
> Al redactar StyleBook, asegúrese de tener conocimiento de lo siguiente:
>
> - API de NITRO
> - YAML

Para obtener más información sobre cómo escribir sus propios StyleBooks, consulta Cómo crear sus propios StyleBooks.



> **Nota**
>
> También puede copiar y pegar el contenido de un archivo YAML de StyleBook para validar el contenido.

3. Haga clic en **Create**.

   NetScaler ADM ahora valida su StyleBook para todos los errores sintácticos y semánticos de acuerdo con la gramática de StyleBook. Su StyleBook no se importa a NetScaler ADM si hay algún error. Si no hay errores, el StyleBook se importa correctamente y ahora aparece en la página StyleBooks. Puede identificar el StyleBook por el nombre para mostrar que haya definido en la sección de encabezado del StyleBook.

   > **Nota**
   >
   > Si va a importar un paquete de archivos, NetScaler ADM descomprime la carpeta comprimida y valida todos los StyleBooks.
   > El paquete no se importa incluso si un archivo StyleBook falla la prueba de validación.

   Para obtener más información sobre la gramática de StyleBook y la sintaxis de las diferentes construcciones y atributos, consulte Gramática de StyleBook.

4. Para crear configuraciones a partir de este StyleBook, haga clic en el enlace **Crear configuración** . El StyleBook se abre como una página de interfaz de usuario en la que puede introducir

los valores de todos los parámetros definidos en este StyleBook.

5. Especifique los valores necesarios para los parámetros. En el siguiente ejemplo, puedes ver que los campos del **nombre de la aplicación** y de la **dirección IP del balanceador de cargas** se muestran como campos obligatorios y pueden aceptar valores de usuario. El **algoritmo LB** solo tiene dos valores entre los que puede elegir y, de forma predeterminada, está seleccionado ROUNDROBIN.
6. En **Instancias** de destino , haga clic en y seleccione la dirección IP de la instancia de Citrix ADC en la que quiere ejecutar la configuración. También puede implementar la configuración en más de un NetScaler ADC, especificando tantas instancias de destino como sea necesario.

Si quiere ver los objetos de configuración de Citrix ADC (Nitro) que se crearían en su Citrix ADC antes de crear la configuración, haga clic en **Ejecutar en seco**. Si la configuración es válida, se muestran los objetos de configuración que se crearían en función de los valores que ha proporcionado. En este ejemplo, solo se crea un objeto de tipo lbvserver con este ejemplo StyleBook. Este lbvserver fue el único componente que se definió en este ejemplo básico de StyleBook. Más adelante, puede hacer clic en **Crear** para crear realmente la configuración en las instancias de Citrix ADC seleccionadas.

Una vez completada la creación, el nuevo ConfigPack aparece en la página Configuraciones.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

Buscar StyleBooks personalizados

Citrix ADM ahora permite buscar StyleBooks según su tipo. Es decir, ahora puede buscar StyleBooks predeterminados o StyleBooks personalizados. Esta opción es especialmente útil cuando tiene que buscar los StyleBooks definidos por el usuario entre una gran cantidad de StyleBooks predeterminados.

Para buscar StyleBooks personalizados

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**.
2. Haga clic en el icono de búsqueda situado en la parte superior derecha.
3. En la barra de búsqueda que aparece, selecciona **Tipo** en la primera lista y selecciona **Personalizado** en la siguiente lista de opciones.
4. Citrix ADM muestra solo los StyleBooks definidos por el usuario.

Crear un StyleBook para cargar archivos a NetScaler ADM

January 30, 2024

Los StyleBooks de Citrix Application Delivery Management (Citrix ADM) permiten crear configuraciones de Citrix ADC que pueden incluir, entre otras cosas, la carga de archivos de cualquier tipo desde el sistema de archivos local a la instancia de Citrix ADC, mediante la GUI de Citrix ADM o las API. Estos archivos pueden ser los archivos de certificado o los archivos de geolocalización de ejemplo. También puede especificar el directorio para cargar estos archivos.

Configuración de StyleBook

El siguiente es un ejemplo de StyleBook que describe cómo cargar un archivo de geolocalización en la instancia de NetScaler ADC. Los archivos geográficos se utilizan normalmente en configuraciones GSLB para definir la proximidad estática en función de la ubicación geográfica:

Crea tu StyleBook -1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
```



```
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```

> **Nota**
>
> El parámetro utilizado en este ejemplo es de un archivo de tipo. Puede importar este StyleBook en NetScaler ADM y utilizarlo para cargar archivos de geolocalización.

Este StyleBook requiere que el archivo ya esté presente en Citrix ADM (por ejemplo, ya lo habría copiado en Citrix ADM mediante una utilidad como scp).

Si quiere cargar un archivo en NetScaler ADC a través de NetScaler ADM sin copiarlo primero en el sistema de archivos NetScaler ADM, puede crear un StyleBook que tenga dos parámetros de "cadena" , uno es para especificar el nombre de archivo que se va a utilizar en NetScaler ADC y el otro para especificar el contenido de la y utilice estos dos parámetros en los componentes upload-file-comp. El siguiente es un StyleBook alternativo para cargar un archivo de geolocalización:

Construye su StyleBook: 2

```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

```



```
components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
<!--NeedCopy-->
```

Crear configuraciones para subir archivos

El siguiente procedimiento crea una configuración en una instancia de NetScaler ADC seleccionada que cargaría un archivo de geolocalización mediante el primer StyleBook descrito anteriormente.

Para crear una configuración para cargar archivos:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración**y haga clic en **Crear nuevo**. La página Choose StyleBook muestra todos los StyleBooks que están disponibles en su NetScaler ADM. Desplázate hacia abajo y selecciona el StyleBook que has importado.

   Los parámetros de StyleBook aparecen como una página de interfaz de usuario que permite introducir los valores de todos los parámetros definidos en este StyleBook.

2. Introduzca el nombre del equilibrador de carga y la dirección IP virtual en la sección de configuración básica del equilibrador de cargas.

3. En la sección **Archivo de ubicación**, introduzca el nombre o la ubicación del archivo.

   > **Nota**
   >
   > Asegúrese de que en Citrix ADM el archivo esté ubicado únicamente en la carpeta del inquilino actual. Utilice cualquier protocolo de transferencia de archivos para copiar el archivo al sistema de archivos Citrix ADM.

4. Es posible que se le pida que proporcione sus credenciales de usuario antes de acceder a las instancias de destino.

5. Seleccione la instancia de NetScaler ADC de destino en la que se debe crear la configuración y haga clic en **Crear**.

> **Nota**
>
> Citrix recomienda que seleccione**Ejecutar en seco**para comprobar los objetos de configuración que se crean en la instancia de destino antes de ejecutar la configuración real en la instancia.

Cuando la creación del paquete de configuración se realiza correctamente, el archivo se guarda en el sistema de archivos de instancias Citrix ADC en la ubicación: /var/netscaler/inbuilt_db/

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

Uso de la API Citrix ADM para crear un paquete de configuración

También puede utilizar la API Citrix ADM para crear un paquete de configuración que cargue archivos en la instancia de Citrix ADC seleccionada. Para obtener más información sobre cómo usar las API, consulteCómo usar la API para crear configuraciones para cargar cualquier tipo de archivo.

Crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM

January 30, 2024

Al crear una configuración de StyleBook que utilice el protocolo SSL, debe cargar los archivos de certificado SSL y los archivos de clave de certificado según lo requiera los parámetros de StyleBook. StyleBook le permite cargar directamente los archivos SSL y los archivos clave desde su sistema local mediante la GUI de NetScaler ADM. También puede utilizar las API NetScaler ADM para cargar archivos de certificado y archivos clave que ya están administrados por NetScaler ADM.

Configuración de StyleBook

Este documento le ayuda a crear su propio servidor virtual StyleBook: **Load Balancing Virtual Server (SSL)**
con componentes para cargar certificados SSL y archivos clave. El StyleBook que se proporciona aquí como ejemplo crea una configuración básica de servidor virtual de equilibrio de carga en la instancia de NetScaler ADC seleccionada. La configuración utiliza el protocolo SSL. Para crear una configuración con este StyleBook, debe proporcionar el nombre y la dirección IP del servidor virtual, seleccionar los parámetros del método de equilibrio de carga y cargar el archivo de certificado y el archivo de clave de certificado para el servidor virtual, o utilizar un archivo de certificado y un archivo de clave de certificado que ya estén presente en NetScaler ADM. Estos se especifican en la sección “parámetros”, tal y como se muestra a continuación:

```
parameters:
 -
  name: name
  type: string
```



```
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
  -
    name: certificate
    label: "SSL Certificate File"
    description: "The file name of the SSL certificate file"
    type: certfile
  -
    name: key
    label: "SSL Certificate Key File"
    description: "The file name of the server certificate's private key
       file"
    type: keyfile
<!--NeedCopy-->
```

A continuación, se crean dos componentes en la sección de componentes del StyleBook, como se muestra a continuación. El componente "my-lbvserver-comp"es de tipo ns::lbvserver, donde:

- "ns"es el prefijo que hace referencia al espacio de nombres integrado netscaler.nitro.config y a la versión 10.5 que especificaste en la sección Import-stylebooks.
- "lbvserver"es un StyleBook integrado en este espacio de nombres. Corresponde al recurso del servidor virtual de equilibrio de carga Citrix ADC NITRO del mismo nombre.

El segundo componente "lbvserver-certificate-comp"es de tipo stlb::vserver-certs-binds. El prefijo "stlb"hace referencia al espacio de nombres "com.citrix.adc.stylebooks"y a la versión 1.0 que se especifica en la sección Import-stylebooks del StyleBook. Si el espacio de nombres "com.citrix.adc.stylebooks"puede considerarse una carpeta, "vserver-certs-binds"es otro StyleBook (o un archivo) de esa carpeta. Los StyleBooks que están en el espacio de nombres "com.citrix.adc.stylebooks"se envían como parte de NetScaler ADM.

El StyleBook «vserver-certs-binds» que utilizan los StyleBooks definidos por el usuario le permite configurar fácilmente los certificados cargando los archivos de certificado y clave en la instancia de Citrix ADC de destino y configurando el enlace de los archivos de certificado y clave a los servidores virtuales correspondientes. Las propiedades de este componente son: el nombre del servidor virtual lb y los nombres de los certificados SSL que proporciona al crear el paquete de configuración.

```
components:
  -
    name: my-lbvserver-comp
```



```
4    type: ns::lbvserver
5    properties:
6     name: $parameters.name
7     servicetype: SSL
8     ipv46: $parameters.ip
9     port: 443
10    lbmethod: $parameters.lb-alg
11   -
12    name: lbvserver-certificate-comp
13    type: stlb::vserver-certs-binds
14    description: Binds lbvserver with server certificate
15    properties:
16     vserver-name: $components.my-lbvserver-comp.properties.name
17     certificates:
18      -
19       cert-name: $parameters.name + "-lb-cert"
20       cert-file: $parameters.certificate
21       ssl-inform: PEM
22       key-name: $parameters.name + "-key"
23       key-file: $parameters.key
24  <!--NeedCopy-->
```

Cuando use la API para crear una configuración a partir de tal StyleBook, use solo los nombres de archivo (no la ruta completa del archivo). Se espera que estos archivos ya estén disponibles en las carpetas de archivos de certificados y claves de NetScaler ADM. El archivo de certificado SSL cargado se almacena en NetScaler ADM en /var/mps/tenants/…El directorio /ns_ssl_certs y el archivo de clave del certificado SSL se almacenan en /var/mps/tenants/…directorio /ns_ssl_keys en NetScaler ADM.

Crear configuraciones para cargar archivos SSL

El siguiente procedimiento crea una configuración básica de servidor virtual de equilibrio de carga en una instancia de NetScaler ADC seleccionada mediante el protocolo SSL del StyleBook especificado anteriormente. Puede utilizar este procedimiento para cargar los archivos de certificado SSL y los archivos de claves de certificado en NetScaler ADM.

Para crear una configuración para cargar archivos

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración > StyleBooks**. La página **StyleBooks** muestra todos los StyleBooks que están disponibles en su Citrix ADM.
2. Desplázate hacia abajo y selecciona **Servidor virtual de equilibrio de carga (SSL)** o escribe **Servidor virtual de equilibrio de carga (SSL)** en el campo de búsqueda y presiona la tecla **Entrar** .
3. Haga clic en el enlace **Crear configuración** en el panel StyleBook.

Los parámetros de StyleBook aparecen como una página de interfaz de usuario que permite introducir los valores de todos los parámetros definidos en este StyleBook.

4. Introduzca el nombre del equilibrador de carga y la dirección IP virtual en la sección de configuración básica del equilibrador de cargas.
5. En la sección **Configuración de certificados SSL**, seleccione los archivos correspondientes de su carpeta de almacenamiento local. Como alternativa, puede seleccionar los archivos presentes en el propio NetScaler ADM.
6. Seleccione la instancia de NetScaler ADC de destino en la que se debe crear la configuración y haga clic en **Crear**.

> **Notas:**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.
>
> En Citrix ADM, los siguientes StyleBooks predeterminados, que se envían como parte de Citrix ADM, permiten crear compatibilidad con SSL cargando los certificados y claves SSL.
>
> - HTTP/SSL LoadBalancing StyleBook (lb)
> - Equilibrio de carga HTTP/SSL (con monitores) StyleBook (lb-mon)
> - Aplicación de conmutación de contenido HTTP/SSL con monitores (cs-lb-mon)
> - Ejemplo de StyleBook de aplicaciones con funciones de CS, LB y SSL (sample-cs-app)
>
> También puede crear sus propios StyleBooks que hacen uso de certificados SSL de la misma manera que se describe en el StyleBook anterior

Crea su StyleBook

El contenido completo del archivo lb-vserver-ssl.yaml se muestra a continuación:

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
    configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
```



```
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
  name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key
     file"
  type: keyfile

components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 443
    lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $ components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
```



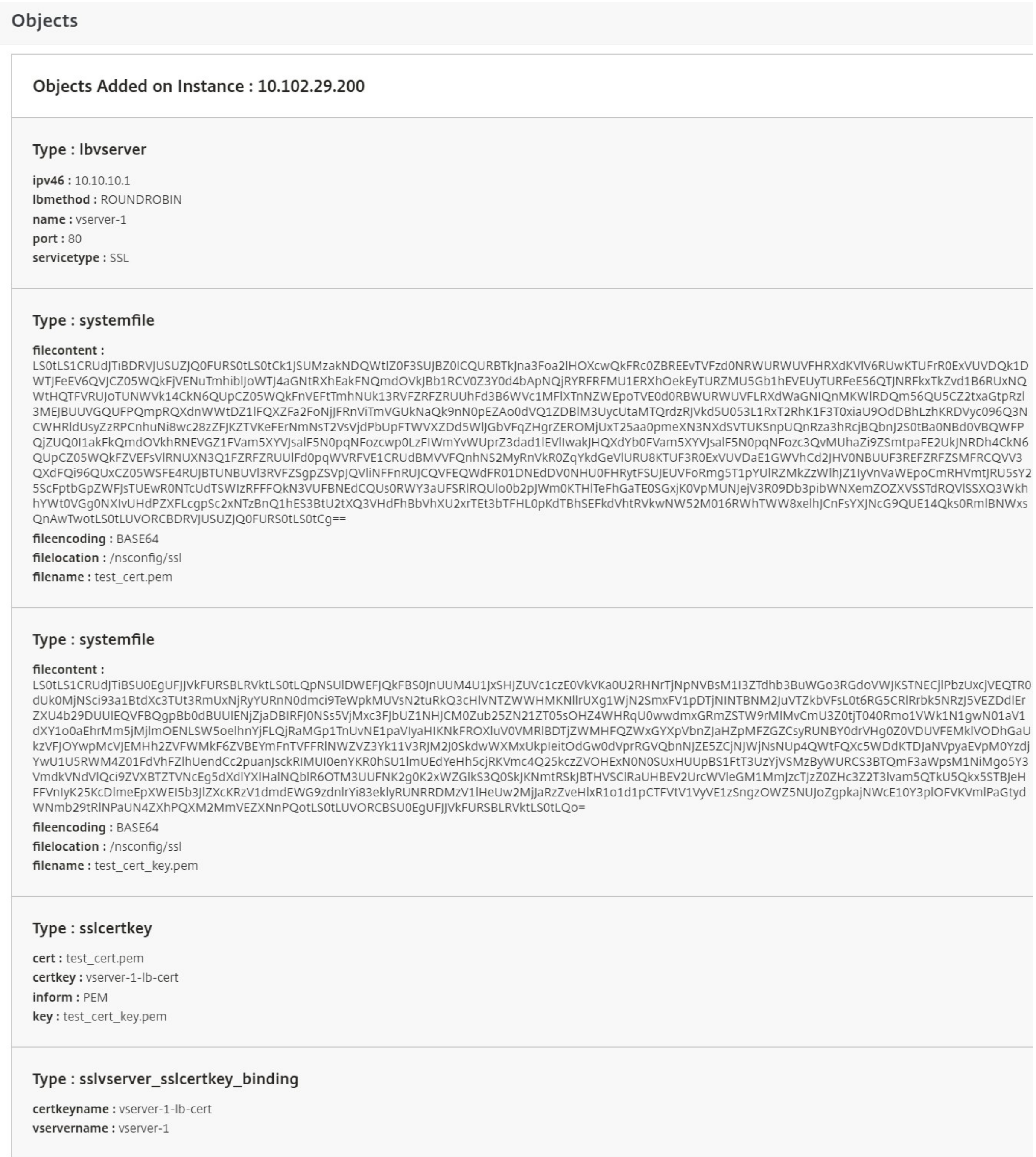
```
67       key-file: $parameters.key
68  <!--NeedCopy-->
```

Uso de la API NetScaler ADM para crear un paquete de configuración

También puede utilizar la API Citrix ADM para crear un paquete de configuración que cargue los archivos de certificado y clave en la instancia de Citrix ADC seleccionada. Para obtener más información sobre cómo usar las API, consulte Cómo usar la API para crear configuraciones para cargar archivos de certificados y claves .

Visualización de los objetos definidos en la instancia de Citrix ADC

Una vez creado el paquete de configuración de StyleBook (configpack) en Citrix ADM, haga clic en **Ver objetos creados** para mostrar todos los objetos Citrix ADC creados en la instancia de Citrix ADC de destino



Habilitar análisis y configurar alarmas en un servidor virtual definido en un StyleBook

January 30, 2024

Puede utilizar la construcción de operaciones para configurar los análisis de Citrix ADM a fin de recopilar registros de flujo de aplicaciones en todas o algunas de las transacciones de tráfico gestionadas por cualquier componente de servidor virtual que forme parte de un StyleBook. También puede utilizar esta construcción para configurar alarmas para obtener información sobre el tráfico administrado por el servidor virtual.

El siguiente ejemplo muestra una sección de operaciones de un StyleBook:

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
    target: $components.basic-lb-comp.outputs.lbvserver
    filter: HTTP.REQ.URL.CONTAINS("catalog")
   -
    alarms:
     -
      name: lbvserver-alarm
      properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"

    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
<!--NeedCopy-->
```

Los atributos de la sección de análisis se utilizan para indicar a la función de análisis Citrix ADM que recopile registros de flujo de aplicaciones en un componente de servidor virtual identificado por la propiedad de destino. También puede especificar opcionalmente una propiedad de filtro que acepte una expresión de directiva NetScaler ADC para filtrar las solicitudes para las que se recopilan registros de flujo de aplicaciones en el servidor virtual.

Cuando se crea un paquete de configuración a partir de este StyleBook, la función de análisis Citrix ADM se configura para recopilar registros de flujo de aplicaciones en los servidores virtuales que se especificaron cuando se crearon durante el proceso de creación de un paquete de configuración.

Los atributos de la sección alarmas se utilizan para establecer umbrales para generar alarmas y enviar notificaciones en el servidor virtual identificado por la propiedad de destino. En el ejemplo anterior, las propiedades perfil de correo electrónico y perfil de SMS se utilizan para especificar dónde se deben

enviar las notificaciones. La sección de reglas define los umbrales. Por ejemplo, si el total de solicitudes manejadas por el servidor virtual es superior a 25 y durante un período definido por el usuario, se establece una alarma y se envía una notificación. La "unidad de período"especifica la frecuencia con la que se activa una alarma. Puede tomar el valor del día, la hora o la semana.

Puede utilizar los siguientes operadores al comparar el valor de métrica con el valor de umbral:

- "mayor que"para ">"
- "menor que"para "<"
- "mayor que igual"para ">="
- "menor que igual"para "<="

Tenga en cuenta que los StyleBooks utilizan nombres de API para las métricas y no los nombres que se muestran en la GUI de análisis de NetScaler ADM.

Para obtener información sobre cómo ver y analizar los datos recopilados en servidores virtuales que se crearon como parte de un paquete de configuración, consulte la documentación de análisis de NetScaler ADM.

Roles de instancia

January 24, 2024

En NetScaler Application Delivery Management (ADM), puede haber un caso en el que tenga que configurar varias instancias de NetScaler ADC para una sola aplicación, pero también en el que cada instancia de ADC requiera una configuración diferente para implementarlas. Un ejemplo de este caso es el predeterminado de Microsoft Skype Empresarial StyleBook.

Actualmente, StyleBooks admite la posibilidad de crear un paquete de configuración y aplicar la misma configuración en varias instancias de Citrix ADC. Tal caso en el que la configuración es idéntica en todas las instancias ADC, puede denominarse configuración simétrica.

Ahora, con la función «roles de instancia» de StyleBooks, puede crear una configuración asimétrica, es decir, un paquete de configuración que se puede aplicar en varias instancias de ADC, pero con diferentes configuraciones en diferentes instancias de ADC.

Cuando se utiliza un StyleBook con funciones de instancia para crear un paquete de configuración, a cada instancia de ADC de un paquete de configuración se le puede asignar una función diferente. Esta función determina los objetos de configuración del paquete de configuración que recibirá la instancia de ADC.

Puntos a tener en cuenta:

- El conjunto de roles de instancia en un StyleBook se define al crear el StyleBook.

- Los roles se asignan a una instancia de ADC específica al crear o actualizar el paquete de configuración.

Sección de roles de destino

Se introduce una nueva sección en un StyleBook llamada "roles de destino", donde se declaran todos los roles admitidos por el StyleBook.

Esta sección suele colocarse después de la sección "Importar libros de estilos"de un StyleBook y antes de la sección de parámetros.

En el siguiente ejemplo de StyleBook, se definen dos funciones en la sección "funciones de destino": A y B.

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

Puede ver que el rol B también define dos sub-propiedades opcionales, min-targets y max-targets.

Aunque estas dos subpropiedades son opcionales, los objetivos mínimos especifican el número mínimo obligatorio de instancias de ADC a las que se les debe asignar esta función al crear un paquete de configuración a partir de este StyleBook, y los objetivos máximos especifican el número máximo de instancias de ADC a las que se les puede asignar esta función al crear un paquete de configuración a partir de este StyleBook.

Si no se especifican estas subpropiedades, no hay límite en el número de instancias ADC que se pueden configurar para ese rol. Si min-targets = 0, la configuración asociada a ese rol es opcional y si min-targets = 1, esa configuración es obligatoria y al menos se debe configurar una instancia ADC para ese rol.

Función "predeterminada"

Además de los roles explícitamente definidos, hay un rol implícito que tienen todos los StyleBooks, y ese rol se llama como un rol predeterminado. Este rol se puede usar como cualquier otro rol en un StyleBook. Al crear un paquete de configuración, si a una instancia de ADC no se le asigna un rol específico, la instancia se asigna implícitamente al rol «predeterminado». La instancia recibirá ahora todos los objetos de configuración generados por los componentes que tengan la función "predeterminada".

Componentes con roles

Una vez definidas las funciones que admite un StyleBook (incluida la función "predeterminada"), las funciones se pueden utilizar en la sección de componentes de un StyleBook. Si quiere que un componente se implementación solo en instancias ADC que desempeñan un determinado rol, puede especificar el atributo roles como parte del componente, como se ilustra en el siguiente ejemplo de componente:

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

En el ejemplo anterior, el componente genera un "lbvserver"que se implementará en las instancias que desempeñen la función A. Tenga en cuenta que el atributo roles de un componente es una lista y que a un componente se le pueden asignar varias funciones. Estas funciones se habrían declarado en la sección "funciones de destino"del StyleBook.

Nota: Si un componente de un StyleBook no especifica un atributo de rol, los objetos de configuración generados por el componente se crean en todas las instancias de NetScaler ADC, independientemente de su rol. Puede utilizar esta función de forma eficaz para crear objetos de configuración que se puedan aplicar a todas las instancias de un paquete de configuración.

Supongamos que hay un StyleBook con dos roles definidos: A y B, y que contiene cuatro componentes.

- El componente C1 tiene los roles A y B
- El componente C2 tiene el rol B
- El componente C3 no tiene ningún rol definido
- El componente C4 tiene la función "predeterminada"

La sección de componentes de este StyleBook se reproduce a continuación:

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
```



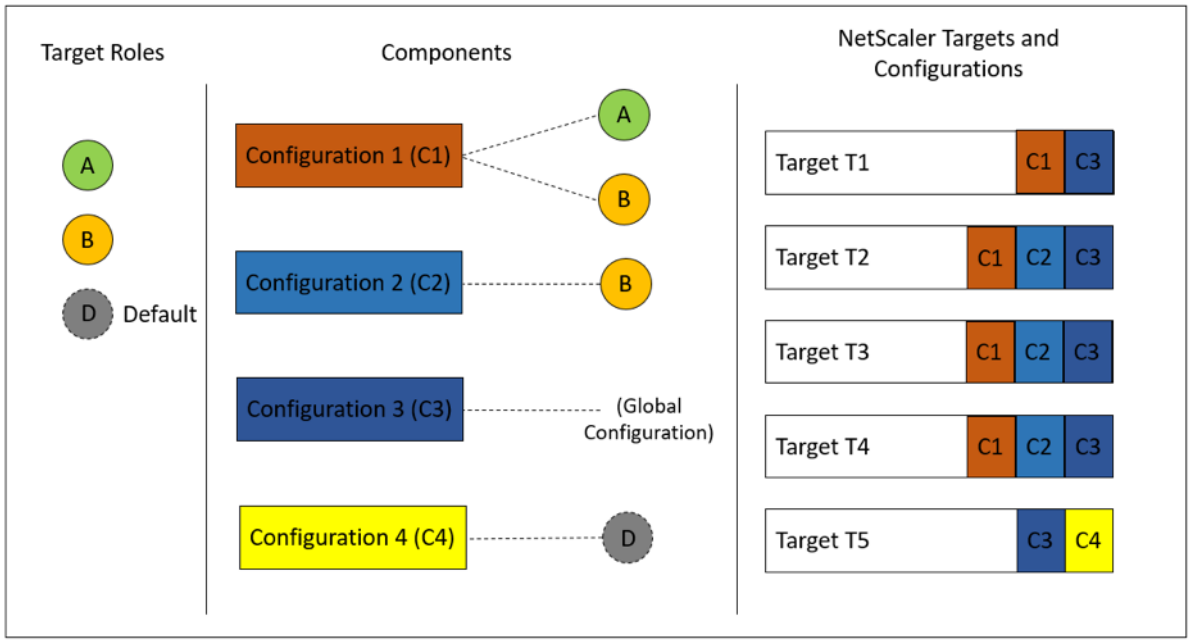
```
9         name: lb1
10        servicetype: HTTP
11        ipv46: 1.1.1.1
12        port: 80
13    -
14      name: C2
15      type: ns::lbvserver
16      roles:
17        - B
18      properties:
19        name: lb2
20        servicetype: HTTP
21        ipv46: 12.12.12.12
22        port: 80
23    -
24      name: C3
25      type: ns::lbvserver
26      properties:
27        name: lb3
28        servicetype: HTTP
29        ipv46: 13.13.13.13
30        port: 80
31    -
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
41  <!--NeedCopy-->
```

Tenga en cuenta que el componente C3 no tiene un rol definido, lo que significa que el componente se implementa en todas las instancias, independientemente de su rol. Por otro lado, el componente C4 tiene la función "predeterminada", lo que significa que se aplica a cualquier instancia que no tenga asignada una función explícita.

Ahora, considere que desea crear un paquete de configuración con este StyleBook e implementarlo en cinco instancias de ADC. En esta etapa, puede asignar los roles a las instancias de la siguiente manera:

- La función A se asigna a las instancias T1, T2, T3 y T4
- La función B está asignada a las instancias T2, T3 y T4
- A la instancia T5 no se le asigna ningún rol

La siguiente imagen resume las asignaciones de roles y muestra la configuración resultante que recibirá cada instancia de ADC:



Tenga en cuenta que el componente C3 se implementa en todas las instancias independientemente del rol, ya que este componente no tenía atributo roles.

También puedes usar la función «Ejecutar en seco» al crear un paquete de configuración para ver y verificar la asignación correcta de las funciones y los objetos de configuración que se crearán en cada instancia de ADC.

Crea su StyleBook

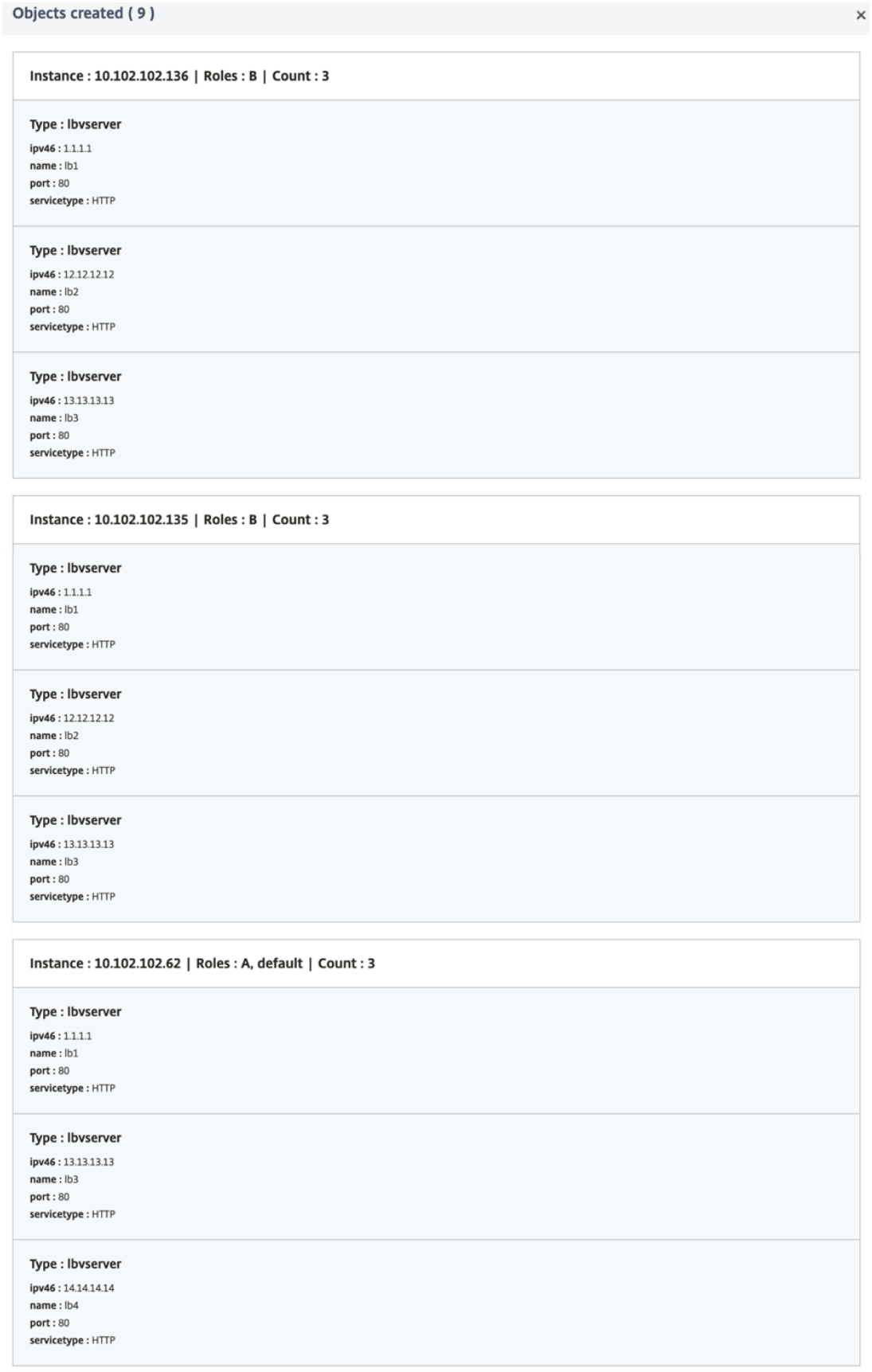
El contenido completo del StyleBook “demo-target-roles”se muestra a continuación:

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
    name: A
```



```
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

La siguiente imagen muestra los objetos creados para un paquete de configuración de ejemplo:



Uso de API

Al usar la API REST, puedes especificar roles para cada instancia de ADC al crear o actualizar el paquete de configuración de la siguiente manera. En el bloque «destinos», especifique el UUID de la instancia específica de Citrix ADC en la que quiere implementar los componentes individuales.

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

Se proporciona una API REST de muestra completa para su referencia.

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
```



```
            "roles": ["A", "B"]
          }
 ,
        {

          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
          }

       ]
      }

 }

<!--NeedCopy-->
```

Crear un StyleBook para realizar operaciones que no sean CRUD

January 30, 2024

Los StyleBooks administran las configuraciones de NetScaler ADC calculando los objetos de configuración necesarios en las instancias de NetScaler ADC. Estos objetos se agregan, actualizan o eliminan de la instancia cada vez que creas o actualizas un ConfigPack. Es entonces cuando se especifica el "estado deseado. "

Sin embargo, algunos objetos de configuración de Citrix ADC admiten algunas operaciones además de crear, actualizar o eliminar (operaciones CRUD). Por ejemplo, un objeto de equilibrio de carga (lbvserver) o un objeto de función de Citrix ADC (nsfeature) pueden admitir la operación de «habilitar» o «deshabilitar». Del mismo modo, las claves de certificación Citrix ADC admiten las operaciones de «vincular» y «desvincular» para vincular o desvincular un certificado a otro certificado. Estas operaciones en objetos NetScaler ADC se denominan operaciones que no son CRUD. En esta sección se describe cómo realizar operaciones que no sean CRUD en objetos de configuración que los admitan mediante StyleBooks.

> **Nota**
>
> La vinculación entre objetos de configuración (por ejemplo, vincular una clave de certificado a un lbvserver) no se considera una operación que no sea CRUD. Esto se debe a que los enlaces de Nitro se representan como objetos de configuración por derecho propio. Estos objetos se crean y eliminan como cualquier otro objeto de configuración de NetScaler ADC.

Apoyo a las operaciones no relacionadas con CRUD

Un nuevo componente fijo llamado “meta-properties”se agrega en el componente en el mismo nivel que el componente “propiedades”. El único atributo admitido en esta construcción actualmente se llama “action”Este atributo puede tomar valores como “enable”o “disable”que son compatibles con ese objeto de configuración.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
   properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

En el ejemplo anterior, el componente “my-lbvserver-comp”es de tipo “ns::lbvserver”. El “ns”es el prefijo que hace referencia al espacio de nombres netscaler.nitro.config y a la versión 10.5 que especificaste en la sección import-stylebooks. El “lbvserver”es un recurso de NITRO en este espacio de nombres. Como acción implícita, el styleBook crea primero el lbvserver y, a continuación, se realiza la operación de “habilitar”en él.

La acción especificada en las meta-propiedades se realiza en el objeto de configuración solo durante la creación del ConfigPack. Las actualizaciones del ConfigPack no realizan acciones que no sean de CRUD.

> **Nota**
>
> El valor del atributo action no puede ser una expresión StyleBook que se evalúe dinámicamente.

Usar API para crear configuraciones a partir de StyleBooks

January 30, 2024

Una vez creado el StyleBook, tiene que importarlo a Citrix Application Delivery Management (ADM) para usarlo mediante Citrix ADM o mediante las API de Citrix ADM. NetScaler ADM valida el StyleBook al importarlo y, si la validación se realiza correctamente, el StyleBook aparece en el catálogo de StyleBooks de NetScaler ADM, listo para usarse en la creación de configuraciones.

Ahora puede usar las API de StyleBook para crear configuraciones basadas en este StyleBook. Puede utilizar cualquier herramienta como la herramienta de línea de comandos curl o la extensión del explorador Chrome Postman para enviar solicitudes HTTP a NetScaler ADM.

Ejemplo 1

Considere el StyleBook "lb-vserver"que ha creado en StyleBook para crear un servidor virtual de equilibrio de carga. Use la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks

<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "target_devices":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
 }

 }

<!--NeedCopy-->
```

En esta solicitud HTTP, el identificador (por ejemplo, "deecee30-f478-4446-9741-a85041903410") es el ID de instancia de NetScaler ADC en la que se crea el servidor virtual de equilibrio de carga lb1 con la dirección IP 10.102.117.31. El ID de instancia de la instancia de NetScaler ADC se recupera de NetScaler ADM.

Para obtener el ID de una instancia administrada por NetScaler ADM, puede utilizar las API de NetScaler ADM. Por ejemplo, para recuperar el ID de instancia de una instancia de Citrix ADC cuya dirección IP es 192.168.153.160, puede utilizar la siguiente API:

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
   :192.168.153.160
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

La respuesta contiene el ID en la carga útil:

```
200
OK
Content-Type: application/json
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    ..."id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }

<!--NeedCopy-->
```

Si la configuración (configpack) se crea correctamente, recibirá la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json
{

  "configpack":
  {

    "config_id": "1460806080"
```



```
    }

  }

<!--NeedCopy-->
```

Ha creado su primera configuración (paquete de configuración) que se identifica de forma única mediante el identificador 1460806080. Puede utilizar este ID para consultar, actualizar o eliminar la configuración.

Ejemplo 2

Puede usar el mismo StyleBook para crear otra configuración o paquete de configuración y ejecutarlo en la misma instancia de Citrix ADC o en diferentes instancias. En este ejemplo, cree otra configuración y proporcione un nombre y una dirección IP diferentes para el servidor virtual y también especifique LEASTCONNECTION como método de equilibrio de carga. Implemente esta configuración en dos instancias de NetScaler ADC.

La solicitud HTTP es la siguiente:

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
     }
 ,
    "target_devices"
    [
     {
 "id": "deecee30-f478-4446-9741-a85041903410" }
 ,
     {
 "id": "debecc60-d589-4557-8632-a74032802412" }

```



```
    ]
   }

 }

<!--NeedCopy-->
```

En esta solicitud HTTP, el servidor virtual de equilibrio de carga lb2 con la dirección IP 10.102.117.32 se crea en las dos instancias NetScaler ADC representadas por los identificadores “deecee30-f478-4446-9741-a85041903410”y “debecc60-d589-4557-8632-a74032802412”.

Al crear correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json
{

   "configpack":
  {

     "config_id": "1657696292"
   }

 }

<!--NeedCopy-->
```

Este nuevo paquete de configuración tiene un identificador diferente 165769629. Puede actualizar o eliminar esta configuración mediante este id.

Ejemplo 3

Considere el StyleBook “basic-lb-config”que ha creado en StyleBook para crear una configuración básica de equilibrio de carga. Use la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
    .stylebooks/0.1/basic-lb-config/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
```



```
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers":
      ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
,
   "target_devices":
   [
    {

     "id": "deecee30-f478-4446-9741-a85041903410"
     }
,
    {

     "id": "debecc60-d589-4557-8632-a74032802412"
     }

   ]
  }

}

<!--NeedCopy-->
```

En esta solicitud HTTP, la configuración de equilibrio de carga se ejecuta en dos instancias de NetScaler ADC. Puede iniciar sesión en estas instancias de NetScaler ADC para comprobar si se crean un servidor virtual y un grupo de servicios con dos servicios enlazados.

Ejemplo 4

Considere el **ejemplo** compuesto de StyleBook que creó en Crear un StyleBook compuesto. Use la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

```



```
      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
     }
 ,
    "target_devices":
    [
    {

      "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
    {

      "id": "debecc60-d589-4557-8632-a74032802412"
     }

    ]
  }

 }

<!--NeedCopy-->
```

En esta solicitud HTTP, la configuración se crea en dos instancias de NetScaler ADC representadas por sus ID. Si inicia sesión en las instancias NetScaler ADC, puede ver los objetos de configuración creados por el StyleBook "basic-lb-config"que se importó en el StyleBook "composite-example". También puede ver un nuevo monitor HTTP llamado "myapp-mon"que formaba parte del StyleBook de "ejemplos compuestos".

Al crear correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Actualización de una configuración

Para actualizar esta configuración, por ejemplo, agregando un nuevo servidor backend con la dirección IP 10.102.29.54 al servidor virtual de equilibrio de carga myapp, use la API para actualizar un paquete de configuración de la siguiente manera:


```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
   }
 ,
  "target_devices":
  [
    {

    "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
  {

    "id": "debecc60-d589-4557-8632-a74032802412"
   }

]
 }

 }

<!--NeedCopy-->
```

Al actualizar correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```


Eliminación de una configuración

Para eliminar esta configuración (de todas las instancias de Citrix ADC), puede usar la API para eliminar un paquete de configuración de la siguiente manera:

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

Al eliminar correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

Puede iniciar sesión en la instancia de Citrix ADC y comprobar que se han eliminado todos los objetos de configuración que forman parte de este paquete de configuración.

Si quiere eliminar la configuración de instancias específicas de Citrix ADC en lugar de todas, utilice la operación de actualización del paquete de configuración descrita anteriormente y cambie el atributo «target_devices» en la carga útil JSON para eliminar los ID de instancia de Citrix ADC específicos.

Usar API para crear configuraciones para cargar archivos de certificados y claves

January 30, 2024

Utilice las API de StyleBook para crear configuraciones basadas en este StyleBook. Puede utilizar cualquier herramienta como la herramienta de línea de comandos curl o la extensión del explorador Chrome Postman para enviar solicitudes HTTP a NetScaler Application Delivery Management (ADM).

Considere el ejemplo de StyleBook que creó para cargar los archivos de certificado y clave en Cómo crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM.

Use la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
<!--NeedCopy-->
```

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {

           "lb-appname": "lbmon",
           "lb-virtual-ip": "13.1.11.10",
           "lb-virtual-port": "80",
           "lb-service-type": "HTTP",
           "svc-service-type": "HTTP",
           "svc-servers": [
               {

                   "ip": "14.1.1.15",
                   "port": "80"         }

      ],
           "certificates": [
               {

                   "cert-name": "server_cert",
                   "cert-file": "server_cert.pem",
                   "ssl-inform": "PEM",
                   "key-name": "server_key",
                   "key-file": "server_key.pem",
                   "cert-password": "secret",
                   "cert-advanced": {

                       "is-ca-cert": false,
                       "skip-ca-name": false
           }

         }

      ],
           "lb-advanced": {

               "flush-on-state-down": "ENABLED",
               "auth-params": {

                   "authentication": "OFF",
                   "authentication-http-401": "OFF"
         }
```



```
45  ,
46                  "appflow-log": "ENABLED",
47                  "algorithm": "LEASTCONNECTION"
48          }
49  ,
50              "svcg-advanced": {
51
52                  "svc-client-ip": "DISABLED",
53                  "svc-use-source-ip": "NO",
54                  "svc-use-proxy-port": "NO",
55                  "svc-surge-protection": "OFF",
56                  "svc-client-keepalive": "NO",
57                  "svc-tcp-buffering": "NO",
58                  "svc-compression": "NO",
59                  "svc-state": "ENABLED",
60                  "svc-downstate-flush": "DISABLED",
61                  "svc-enable-health-monitor": "NO"
62          }
63
64       }
65  ,
66          "targets": [
67              {
68
69                  "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
70          }
71
72       ]
73     }
74
75  }
76
77  <!--NeedCopy-->
```

Este paquete de configuración se identifica de forma única mediante el id 8c158e7a-0087-423f-91b0-0ccf16de552a. Puede utilizar este ID para consultar, actualizar o eliminar la configuración. Cuando se actualiza correctamente el paquete de configuración, los archivos de certificado y clave se cargan en el sistema de archivos NetScaler ADM.

Use API para crear configuraciones para cargar cualquier tipo de archivo

January 30, 2024

También puede usar la API Citrix Application Delivery Management (ADM) para crear un paquete de configuración que cargue archivos en la instancia de Citrix ADC seleccionada.

Considere el ejemplo de StyleBook que creó para cargar archivos de cualquier tipo enCómo crear un StyleBook para cargar archivos en NetScaler ADC MA Service. Como en el ejemplo del tema anterior,

cree un paquete de configuración y especifique el valor del parámetro «locationfile» como ruta de archivo del archivo de ubicación en Citrix ADM.
Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
   stylebooks.samples/1.0/upload-geolocations/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ /
          custom_geolocations.csv"
      }
 ,
      "targets": [
         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
       }

    ]
   }

 }

<!--NeedCopy-->
```

Usar API para importar StyleBooks personalizados

January 30, 2024

Ahora puede utilizar las API de StyleBook para importar StyleBooks personalizados en NetScaler Application Delivery Management (ADM). Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera en cualquier herramienta, como la herramienta de línea de comandos curl o la extensión del navegador Chrome Postman. Por ejemplo, puede importar un StyleBook denominado example-lb que se puede utilizar para crear una configuración de equili-

brador de carga en una instancia de NetScaler ADC.

```
HTTP Method: POST
URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
Headers:
Content-Type: application/json
Accept: application/json
RequestBody:
{

       "stylebook":
  {

     "file_name": "example-lb.yaml",
     "source": "<base64-contents>",
     "encoding": "base64"
   }

 }

<!--NeedCopy-->
```

donde, el valor del atributo “source”, es la codificación en base64 del contenido del archivo StyleBook. Puede pegar el contenido YAML del archivo StyleBook en una herramienta en línea, por ejemplo,https://www.browserling.com/tools/file-to-base64 para obtener la cadena base64 que luego puede usar como valor para el atributo “fuente”anterior.

Mediante esta llamada a la API, también puede cargar un archivo comprimido (archivo TGZ) que contenga varios archivos StyleBook en una operación de API. Para ello, basta con cambiar el atributo file_name por el nombre de archivo .tgz y el valor del atributo source por la codificación base64 del contenido del archivo.tgz.

Después de ejecutar correctamente la API en la herramienta, obtendrá la siguiente respuesta que indica que el StyleBook se ha importado a NetScaler ADM.

```
200 OK
<!--NeedCopy-->
```

Cuerpo de respuesta:

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

```



```
    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

Usar API para descargar StyleBooks personalizados

January 30, 2024

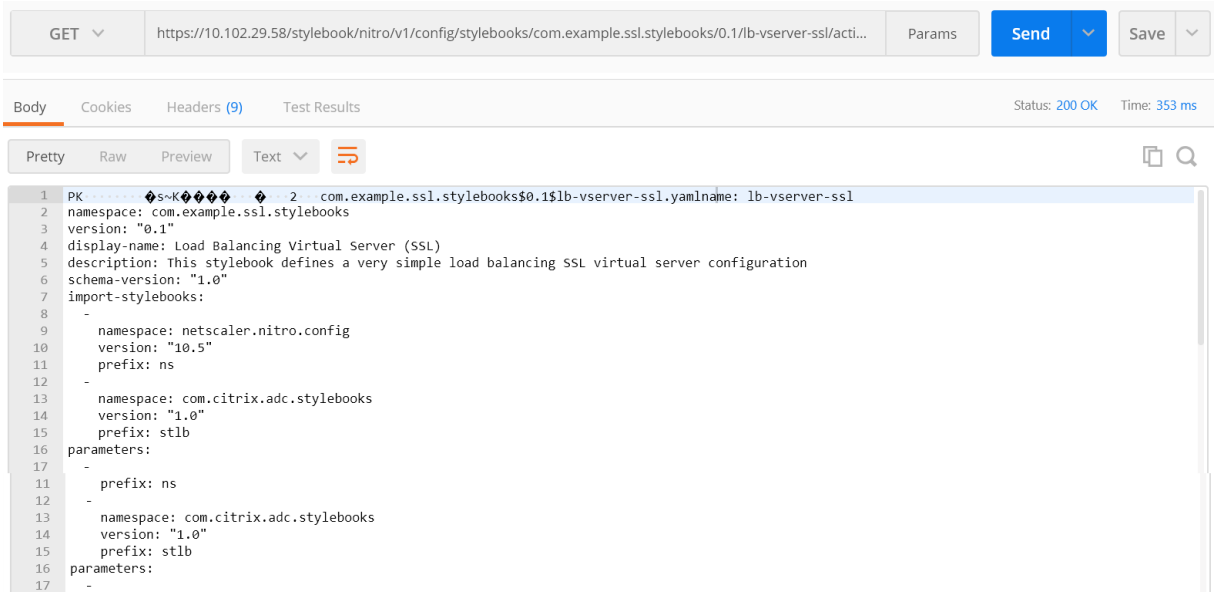
Puede descargar un StyleBook personalizado si proporciona la siguiente API REST de StyleBooks:

```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
   VERSION>/<NAME>/actions/download
<!--NeedCopy-->
```

Puede ejecutar la API en cualquier herramienta, como la herramienta de línea de comandos curl o la extensión del navegador Postman para Chrome, después de realizar modificaciones en los campos de dirección IP, nombre, versión y espacio de nombres.

```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
   ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
<!--NeedCopy-->
```

Se descarga el StyleBook en formato.yaml.



Usar API para eliminar StyleBooks personalizados

January 30, 2024

Puede eliminar el StyleBook personalizado proporcionando la siguiente API REST de StyleBooks:

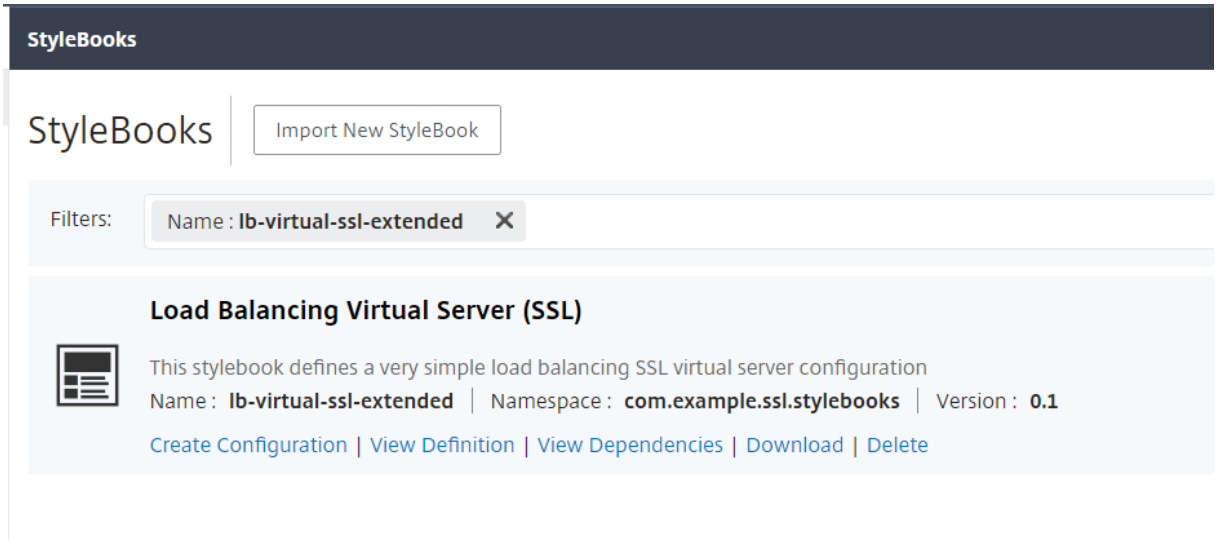
```
DELETE

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
<!--NeedCopy-->
```

Si no se proporciona el parámetro de consulta de dependencias en la URL o su valor se establece en false, las dependencias de StyleBook no se eliminan (solo se elimina el propio StyleBook).

Cuando recibe un código de estado de respuesta HTTP de 200, significa que el StyleBook personalizado (y sus dependencias) se ha eliminado correctamente de Citrix ADM.

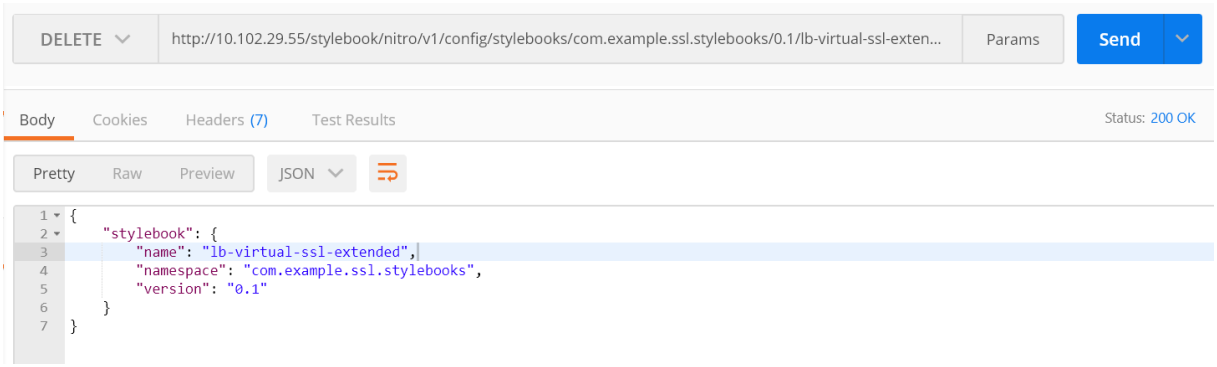
> **Nota**No
>
> puede eliminar un StyleBook personalizado que tenga otros StyleBooks en MA Service que dependan de él.

Por ejemplo, supongamos que ha creado un StyleBook denominado «lb-virtual-ssl-extended» en Citrix ADM. Más tarde decidió eliminar ese StyleBook.

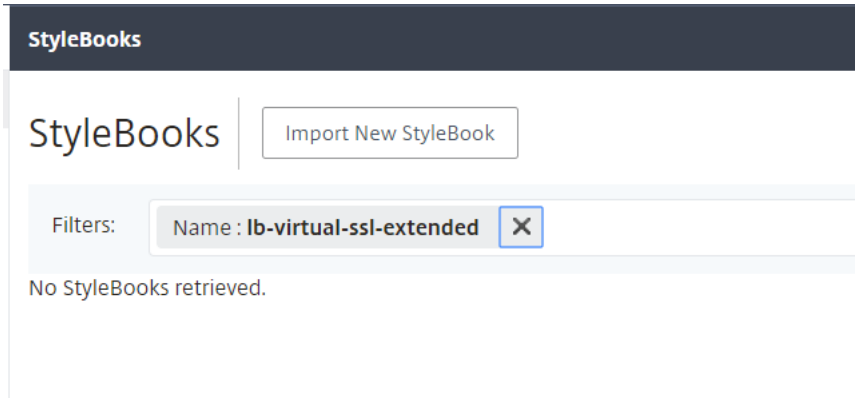


Puede ejecutar la API en cualquier herramienta, como la herramienta de línea de comandos curl o la extensión del navegador Postman para Chrome, después de realizar modificaciones en los campos de dirección IP, nombre, versión y espacio de nombres.

BORRARhttps://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



El StyleBook se elimina de NetScaler ADM.



Gramática de StyleBooks

January 30, 2024

Puede diseñar sus propios StyleBooks, importarlos a Citrix Application Delivery Management (ADM) y, a continuación, usarlos para crear configuraciones mediante la GUI de Citrix ADM o mediante las API. Para poder crear sus propios StyleBooks, primero debes entender la gramática y la sintaxis de los diferentes constructos y atributos que puede usar.

Este documento describe las diferentes construcciones y referencias que puede utilizar al crear StyleBooks.

Haga clic en el nombre de una sección, componente fijo o referencia de la tabla siguiente para ver los detalles.

[Header](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/header-section.html)	[Importar StyleBooks](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/import-stylebooks-section.html)
[Parameters](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-section.html)	[Construcción Parameters-Default-sources](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html)
[Substitutions](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions.html)	[Components](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components.html)
[Propiedades opcionales](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/optional-properties.html)	[Componentes auxiliares](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/helper-components.html)
[Fuentes predeterminadas de propiedades](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/properties-default-sources.html)	[Componentes anidados](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-components.html)
[Construcción de condición](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/condition-construct.html)	[Repetir componente fijo](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-construct.html)
[Construcción de condición de repetición](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	[Outputs](/es-

es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/outputs.html) |
[Repeticiones anidadas](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/styleboo grammar/nested-repeats.html)	[Referencia de principal](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parent-reference.html)
[Referencia de parámetros](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameter-reference.html)	[Referencia de sustituciones](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions-reference.html)
[Referencia de componentes](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components-reference.html)	[Operations](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/operations.html)
[Referencia de variable](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebook grammar/variable-reference.html)	[Alarms](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/alarms.html)
[Analytics](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/analytics.html)	[Funciones integradas](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/built-in-functions.html)
[Expressions](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/expressions.html)	[Detección de dependencias](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/dependency-detection.html)
Interpolaciones in situ

> **Nota**
>
> Al definir el elemento de repetición, el índice de repetición o los argumentos de las funciones de sustitución, no utilice las siguientes palabras reservadas para nombrar una variable definida por el usuario, `$<var-name>`
>
> - libro de estilos, parámetros, sustituciones, componentes, propiedades, salidas, elemento principal, propio, operaciones, análisis, alarmas
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - índice de repeticiones, índice de repeticiones 0, índice de repeticiones 1, índice de repeticiones 2
> - default
> - funciones, función, objetivos, objetivo
> - context, parent-context, parent_context

Para obtener información y ejemplos sobre cómo diseñar sus propios StyleBooks, consulta Cómo crear sus propios StyleBooks.

Header

January 30, 2024

Las seis primeras líneas de un StyleBook forman la sección de cabecera. Esta sección permite definir la identidad de un StyleBook y describir su función. Se trata de una sección obligatoria.

En la tabla siguiente se describen los atributos de la sección de encabezado:

|Atributo| Descripción|
—	—
name	Un nombre para identificar el StyleBook. Este atributo es obligatorio.
description	Descripción que define lo que hace un StyleBook. Esta descripción aparece en la GUI de NetScaler ADM. Este es un atributo opcional.
display-name	Nombre descriptivo del StyleBook. Este nombre aparece en la GUI de NetScaler ADM. Este es un atributo opcional.
author	Autor, persona u organización que crea el StyleBook. Este es un atributo opcional.
namespace	Un espacio de nombres forma parte de un identificador único de un StyleBook para evitar colisiones de nombres. Un espacio de nombres puede ser cualquier cadena, pero se recomienda utilizarla para asignar un nombre a la empresa, el departamento o la unidad que creó o posee un conjunto de StyleBooks. Por ejemplo, puede utilizar el siguiente formato: <company>.<department>.<unit>.stylebooks. Se trata de un atributo obligatorio.
version	El número de versión del StyleBook. Puede cambiar el número de versión al actualizar un StyleBook. Los StyleBooks de diferentes versiones pueden coexistir juntos. Se trata de un atributo obligatorio.
schema-version	La versión del esquema de StyleBooks. Toma el valor «1.0” de la versión actual de NetScaler ADM. Se trata de un atributo obligatorio.
private	Si este atributo se establece en true, el StyleBook no se muestra en la GUI de NetScaler ADM. Esta es una configuración útil para los StyleBooks, que son componentes básicos de otros StyleBooks y no están pensados para que los usuarios los utilicen directamente. Este es un atributo opcional. Su valor predeterminado es false.

Ejemplo:

```
      name: lb
    description: "This stylebook defines a sample load balancing
    configuration."
    display-name: "Load Balancing StyleBook (HTTP)"
    author: Mike Smith (ACME Infra team)
    namespace: com.example.stylebooks
    schema-version: "1.0"
    version: "0.1"
<!--NeedCopy-->
```


La combinación de nombre , espacio de nombres y versión identifica de forma única un StyleBook en el sistema. No puede tener dos StyleBooks con la misma combinación de nombre, espacio de nombres y versión en NetScaler ADM. Sin embargo, puede tener dos StyleBooks con el mismo nombre y versión pero espacios de nombres diferentes, o con el mismo espacio de nombres y versión pero nombres diferentes.

Importar StyleBooks

January 30, 2024

Esta es la segunda sección de tu StyleBook y te permite declarar a qué otro StyleBook quieres hacer referencia desde tu StyleBook actual. Esto le permite importar y reutilizar otros StyleBooks en lugar de volver a crear la misma configuración en su propio StyleBook. Se trata de una sección obligatoria.

Debe declarar el espacio de **nombres** y el número de **versión** de los StyleBook a los que desea hacer referencia en su StyleBook actual. Cada StyleBook debe hacer referencia al espacio de nombres netscaler.nitro.config si utiliza directamente cualquiera de los objetos de configuración NITRO. Este espacio de nombres contiene todos los tipos de Citrix ADC NITRO, como lbvserver service o monitor. Se admiten los StyleBooks para NetScaler ADC versiones 10.5 y posteriores, lo que significa que puede utilizar su StyleBook para crear y ejecutar configuraciones en cualquier instancia de NetScaler ADC que ejecute la versión 10.5 o posterior.

El atributo **prefix** utilizado en la sección import-stylebooks es una abreviatura para referirse a la combinación de espacio de nombres y versión. Por ejemplo, el prefijo "ns"se puede utilizar para hacer referencia al espacio de nombres netscaler.nitro.config con la versión 10.5. En las secciones posteriores de su StyleBook, en lugar de utilizar el espacio de nombres y la versión cada vez que quiera hacer referencia a un StyleBook con este espacio de nombres y versión, puede utilizar simplemente la cadena de prefijos elegida junto con el nombre del StyleBook para identificarlo de forma única.

Ejemplo:

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
      -
       namespace: com.acme.stylebooks
        version: "0.1"
        prefix: stlb
<!--NeedCopy-->
```

En el ejemplo anterior, el primer prefijo definido se denomina ns y hace referencia al espacio de nombres netscaler.nitro.config y a la versión 10.5. El segundo prefijo que se define se denomina stlb y hace

referencia al espacio de nombres com.acme.stylebooks y a la versión 0.1.

Después de definir un prefijo, cada vez que quiera hacer referencia a un tipo o a un StyleBook que pertenece a un espacio de nombres y versión determinados, puede usar la notación**<namespace-shorthand>:: <type-name>. Por ejemplo, **ns::lbvserver** hace referencia al tipo lbvserver definido en el espacio de nombres netscaler.nitro.config, versión 10.5.

Del mismo modo, si quiere hacer referencia a un StyleBook con la versión "0.1"en el espacio de nombres com.acme.stylebooks, puede usar la notación**stlb:: <stylebook-name>**.

> **Nota**
>
> Por convención, el prefijo «ns» se utiliza para hacer referencia al espacio de nombres NITRO de Citrix ADC.

Parámetros

January 30, 2024

Esta sección le permite definir todos los parámetros que necesita en su StyleBook para crear una configuración. Describe la entrada que toma su StyleBook. Aunque esta es una sección opcional, es posible que la mayoría de los StyleBooks la necesiten. Puede consultar la sección de parámetros para definir las preguntas a las que desea que respondan los usuarios cuando usen el StyleBook para crear una configuración en una instancia de Citrix ADC.

Al importar el StyleBook a Citrix ADM y usarlo para crear una configuración, la GUI utiliza esta sección del StyleBook para mostrar un formulario que introduce los valores de los parámetros que ha definido.

En la siguiente sección se describen los atributos que debe especificar para cada parámetro de esta sección:

name

El nombre del parámetro que quiere definir. Puede especificar un nombre alfanumérico.

El nombre debe empezar por un alfabeto y puede incluir alfabetos, números, guiones (-) o caracteres de subrayado (_) adicionales.

Tenga en cuenta que al escribir un StyleBook, puede usar este atributo «name» para hacer referencia al parámetro en otras secciones utilizando la notación $parameters. <name>.

¿**Obligatorio**? Sí

etiqueta

Cadena que se muestra en la GUI de ADM como nombre de este parámetro.

¿**Obligatorio**? No

description

Cadena de ayuda que describe para qué se utiliza el parámetro. La GUI de ADM muestra este texto cuando el usuario hace clic en el icono de ayuda de este parámetro.

¿**Obligatorio**? No

type

El tipo de valor que pueden tomar estos parámetros. Los parámetros pueden ser de cualquiera de los siguientes tipos incorporados:

- cadena: matriz de caracteres. Si no se especifica una longitud, el valor de cadena puede tener cualquier número de caracteres. Sin embargo, puede limitar la longitud de un tipo de cadena utilizando los atributos longitud mínima y longitud máxima.
- number: un número entero. Puede especificar el número mínimo y máximo que puede tomar este tipo mediante los atributos valor mínimo y valor máximo.
- booleano: puede ser verdadero o falso. Además, ten en cuenta que YAML considera todos los literales como booleanos (por ejemplo, Sí o No).
- ipaddress: cadena que representa una dirección IPv4 o IPv6 válida.
- tcp-port: número entre 0 y 65535 que representa un puerto TCP o UDP.
- contraseña: representa un valor de cadena opaco o secreto. Cuando la GUI de Citrix ADM muestra un valor para este parámetro, aparece con asteriscos (*****).
- certfile: representa un archivo de certificado. Esto le permite cargar los archivos directamente desde su sistema local al crear una configuración de StyleBook mediante la GUI de ADM. El archivo de certificado cargado se almacena en el directorio /var/mps/tenants//ns_ssl_certs en ADM.

  El archivo de certificado se agregará a la lista de certificados administrados por ADM.
- keyfile: representa un archivo de claves de certificado. Esto le permite cargar el archivo directamente desde el sistema local al crear una configuración de StyleBook mediante la GUI de Citrix ADM. El archivo de certificado cargado se almacena en el directorio /var/mps/-tenants//ns_ssl_keys en Citrix ADM.

El archivo de claves de certificado se agregará a la lista de claves de certificado administradas por Citrix ADM.

- archivo: representa un archivo.
- objeto: este tipo se usa cuando desea agrupar varios parámetros relacionados en un elemento principal. Debe especificar el parámetro principal del tipo como «objeto». Un parámetro de tipo ‘‘objeto’’puede tener una sección de ‘‘parámetros’’anidada para describir los parámetros que contiene.
- otro StyleBook: Cuando se utiliza este tipo de parámetro, este parámetro espera que su valor sea en forma de los parámetros definidos en el StyleBook que denota su tipo.

Un parámetro también puede tener un tipo que sea una lista de cualquiera de los tipos enumerados anteriormente, añadiendo
«[]» al final del tipo. Por ejemplo, si el atributo de tipo es string [], este
parámetro toma una lista de cadenas como entrada. Puede proporcionar una, dos o varias cadenas para
este parámetro al crear una configuración a partir de este StyleBook.

¿**Obligatorio**? Sí

clave

Especifique true o false para indicar si este parámetro es un parámetro clave para StyleBook.

Un StyleBook solo puede tener un parámetro definido como parámetro ‘‘clave’’.

Al crear diferentes configuraciones desde el mismo StyleBook (en la misma instancia de Citrix ADC o en diferentes instancias), cada configuración tiene un valor diferente o único para este parámetro.

El valor predeterminado es false.

¿**Obligatorio**? No

requerido

Especifique true o false para indicar si un parámetro es obligatorio u opcional. Si se establece en true, el parámetro es obligatorio y el usuario debe proporcionar un valor para este parámetro al crear configuraciones.

La GUI de NetScaler ADM obliga al usuario a proporcionar un valor válido para este parámetro.

El valor predeterminado es false.

¿**Obligatorio**? No

> **Nota**
>
> Si un parámetro tiene `type: object` y `required: false`, los subparámetros de este parámetro no se evalúan.

Si desea que el valor predeterminado de los subparámetros surta efecto, defina `required: true` para main-parameter de la siguiente manera:

```
    type: object
    required: true
    gui:
      collapse_pane: true
<!--NeedCopy-->
```

El atributo collapse_pane muestra el objeto y sus subparámetros contraídos en la interfaz de usuario, a menos que el usuario amplíe el panel.

valores permitidos

Utilice este atributo para definir una lista de valores válidos para un parámetro, cuando el tipo se establece en "cadena".

Al crear una configuración desde la GUI de NetScaler ADM, se pide al usuario que seleccione un valor de parámetro de esta lista.

Ejemplo 1:

nombre: dirección IP

tipo: Cadena

valores permitidos:

- SOURCEIP
- CONSEJO DE REPOSO
- NONE

Ejemplo 2:

nombre: TCP Port

type: Tcp-port

valores permitidos:

- 80
- 81
- 8080

Ejemplo 3:

(lista de tcp-ports, donde cada elemento de la lista solo puede tener valores
especificados en valores permitidos)

nombre: Tcpports

tipo: puerto tcp []

valores permitidos:

- 80
- 81
- 8080
- 8081

¿**Obligatorio**? No

default

Utilice este atributo para asignar un valor predeterminado a un parámetro opcional. Al crear una configuración, si un usuario no especifica un valor, se utiliza el valor predeterminado.

Al crear la configuración desde la GUI de Citrix ADM, si un usuario no proporciona
un valor para un parámetro que no tiene un valor predeterminado, no se establece ningún valor para ese
parámetro.

Ejemplo 1:

nombre: timeout

tipo: número

adulto sordo: 200

Ejemplo 2:

(donde, el valor predeterminado del parámetro es una lista de valores):

nombre: Protocolos

tipo: cadena []

predeterminado:

- TCP
- UDP
- IP

Ejemplo 3:

nombre: timeout

tipo: número

adulto sordo: 200

Ejemplo 4:

nombre: tcpport

type: Tcp-port

adulto sordo: 200

¿**Obligatorio**? No

patrón

Utilice este atributo para definir un patrón (expresión regular) para los valores válidos de este parámetro, cuando el tipo del parámetro sea ‘‘cadena’’.

Ejemplo:

nombre: appname

tipo: Cadena

patrón: «[a-z] +»

¿**Obligatorio**? No

valor mínimo

Utilice este atributo para definir el valor mínimo de los parámetros de tipo «number» o «tcp-port». «

Ejemplo:

nombre: audio-port

type: Tcp-port

valor mínimo: 5000

El valor min-valor de los números puede ser negativo, pero el valor min-valor para tcp-port no debe ser
negativo.

¿**Obligatorio**? No

valor máximo

Utilice este atributo para definir el valor máximo de los parámetros de tipo «number» o «tcp-port». «

El valor máximo debe ser mayor que el valor mínimo, si está definido.

Ejemplo:

nombre: audio-port

type: Tcp-port

valor mínimo: 5000

valor máximo: 15000

¿**Obligatorio**? No

longitud mínima

Utilice este atributo para definir la longitud mínima de los valores aceptados para un parámetro de tipo "cadena".

La longitud mínima de los caracteres definidos como valores debe ser mayor o igual a cero.

Ejemplo:

nombre: appname

tipo: Cadena

longitud mínima: 3

¿**Obligatorio**? No

longitud máxima

Utilice este atributo para definir la longitud máxima de los valores aceptados para un parámetro de tipo "cadena".

La longitud máxima de los valores debe ser mayor o igual a la longitud de los caracteres definidos en la longitud mínima.

Ejemplo:

nombre: appname

tipo: Cadena

longitud máxima: 64

¿**Obligatorio**? No

artículos mínimos

Utilice este atributo para definir el número mínimo de elementos de un parámetro que es una lista.

El número mínimo de elementos debe ser mayor o igual a cero.

Ejemplo:

nombre: Server-ips

tipo: dirección IP []

artículos mínimos: 2

¿**Obligatorio**? No

artículos máximos

Utilice este atributo para definir el número máximo de elementos en un parámetro que es una lista.

La cantidad máxima de artículos debe ser mayor que la cantidad mínima de artículos si está definida.

Ejemplo:

nombre: Server-ips

tipo: dirección IP []

artículos mínimos: 2

número máximo de artículos: 250

¿**Obligatorio**? No

interfaz gráfica

Utilice este atributo para personalizar el diseño del parámetro de tipo «objeto» en la GUI de Citrix ADM.

¿**Obligatorio**? No

columnas

Este es un subatributo del atributo gui. Úselo para definir el número de columnas que se mostrarán en la GUI de Citrix ADM.

¿**Obligatorio**? No

actualizable

Este es un subatributo del atributo gui. Use esto para especificar si el parámetro se puede actualizar después de crear la configuración.

Si el valor se establece en falso, el campo del parámetro aparece en gris al actualizar la configuración.

¿**Obligatorio**? No

colapsar panel

Este es un subatributo del atributo gui. Utilice esta opción para especificar si el panel que define el diseño de este parámetro de objeto es plegable.

Si el valor se establece en true, el usuario puede expandir o contraer los parámetros secundarios bajo este parámetro principal.

Ejemplo:

```
    gui:

     collapse_pane: true

     columns: 2

     updatable: false
<!--NeedCopy-->
```

Ejemplo de una sección completa de parámetros:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

```



```
        type: string

        required: true

         -

           name: ip

           label: IP Address

           description: The virtual IP address used for this application

           type: ipaddress

           required: true

        -

           name: svc-servers

           label: Servers

           type: object[]

           required: true

           parameters:

              -

                 name: svc-ip

                 label: Server IP

                 description: The IP address of the server

                 type: ipaddress

                 required: true

                  -

                    name: svc-port

                    label: Server Port

                    description: The TCP port of the server

                    type: tcp-port

                    default: 80

        -
```



```
64
65            name: lb-alg
66
67            label: LoadBalancing Algorithm
68
69            type: string
70
71            allowed-values:
72
73              - ROUNDROBIN
74
75              - LEASTCONNECTION
76
77            default: ROUNDROBIN
78
79        -
80
81            name: enable-healthcheck
82
83            label: Enable HealthCheck?
84
85            type: boolean
86
87            default: true
88  <!--NeedCopy-->
```

A continuación se muestra un ejemplo que define todos los atributos de una lista y los valores explicados en secciones anteriores:

"'Nombre YAML
: features-list

tipo: cadena []**

longitud mínima: 1

longitud máxima: 3

artículos mínimos: 1

número máximo de artículos: 3

patrón: «[A-Z] +»

valores permitidos:

- 1 CUCHARADITA

- LIBRA

- 4 PIEZAS

predeterminado:

- LIBRA

Construcción Parameters-Default-sources

January 30, 2024

Puede utilizar esta construcción para reutilizar las definiciones de parámetros de otros StyleBooks.

Considere un caso en el que un parámetro o un grupo de parámetros se utiliza repetidamente en varios StyleBooks. Para evitar redefinir estos parámetros, cada vez que quiera crear un nuevo StyleBook, puede definirlos una vez y, a continuación, importar sus definiciones a los StyleBooks que los necesiten mediante la construcción **parameters-default-sources**.

Por ejemplo, si muchos de sus StyleBooks necesitan configurar una IP virtual, es posible que tenga que definir los mismos parámetros relacionados con las IP virtuales en cada nuevo StyleBook que cree. En su lugar, puede crear un StyleBook independiente llamado, por ejemplo, "vip-params", donde defina todos los parámetros relacionados con él, como se muestra en el siguiente ejemplo:

```
1       -
2       name: vip-params
3       namespace: com.acme.commontypes
4       version: "1.0"
5       description: This StyleBook defines a typical virtual IP config.
6       private: true
7       schema-version: "1.0"
8       parameters:
9         -
10            name: lb-appname
11            label: Load Balanced Application Name
12           description: Name of the Load Balanced application
13            type: string
14            required: true
15        -
16            name: lb-virtual-ip
17            label: Load Balanced App Virtual IP address
18            description: Virtual IP address representing the Load
      Balanced application
19            type: ipaddress
20            required: true
21        -
22            name: lb-virtual-port
23            label: Load Balanced App Virtual Port
24            description: TCP port representing the Load Balanced
      application
25            type: tcp-port
26            default: 80
27        -
28            name: lb-service-type
29            label: Load Balanced App Protocol
30            description: Protocol used for the Load Balanced application
      .
31            type: string
```



```
            default: HTTP
            required: true
            allowed-values:
                 - HTTP
                 - SSL
                 - TCP
<!--NeedCopy-->
```

A continuación, puede crear otros StyleBooks que utilicen estos parámetros. Lo que sigue es un ejemplo de tal StyleBook.

```
      -
      name: acme-biz-app
      namespace: com.acme.stylebooks
      version: "1.0"
      description: This stylebook defines the Citrix ADC configuration
     for Biz App
      schema-version: "1.0"
      import-stylebooks:
        -
          namespace: com.acme.commontypes
          prefix: cmtypes
          version: "1.0"
      parameters-default-sources:
           - cmtypes::vip-params
      parameters:
          -
            name: monitorname
            label: Monitor Name
            description: Name of the monitor
            type: string
            required: true
          -
            name: type
            label: Monitor Type
            description: Type of the monitor
            type: string
            required: true
            allowed-values:
              - PING
              - TCP
              - HTTP
              - HTTP-ECV
              - TCP-ECV
              - HTTP-INLINE
<!--NeedCopy-->
```

En StyleBook, acme-biz-app, primero se importan el espacio de nombres y la versión del StyleBook de vip-params mediante la sección "importar libros de estilos". A continuación, se agrega la construcción **parameters-default-sources** y se especifica el nombre de StyleBook, es decir, vip-params. Esto tiene el mismo efecto que definir los parámetros del StyleBook de parámetros vip-params directamente en

este StyleBook.

Puede incluir parámetros de varios StyleBooks porque los parameters-default-sources es una lista y se espera que cada elemento de la lista sea un StyleBook.

Además de incluir parámetros de otros StyleBooks, también puede definir sus propios parámetros mediante la sección de parámetros. La lista completa de parámetros del StyleBook es la combinación de los parámetros incluidos en otros StyleBook y los parámetros definidos en este StyleBook. Por lo tanto, la expresión **$parameters** hace referencia a esta combinación de parámetros.

Tenga en cuenta que si un parámetro se define tanto en un StyleBook importado como en el StyleBook actual, la definición del StyleBook actual anula la definición importada de otro StyleBook. Puede utilizar esto de manera eficaz personalizando algunos de los parámetros importados si es necesario, mientras usa el resto de los parámetros importados tal como están.

La construcción parameters-default-sources también se puede utilizar en parámetros anidados como se muestra:

```
parameters:
    -
      name: vip-details
      label: Virtual IP details
      description: Details of the Virtual IP
      type: object
      required: true
      parameters-default-sources:
              - cmtypes::vip-params
<!--NeedCopy-->
```

Esto es similar a agregar los parámetros de los parámetros vip de StyleBook directamente como parámetros secundarios del parámetro vip-details en este StyleBook.

Sustituciones

January 30, 2024

La sección de sustituciones se usa para definir nombres abreviados para expresiones complejas que se pueden usar en el resto del StyleBook para facilitar la lectura del StyleBook. También son útiles cuando la misma expresión o valor se repite más de una vez en el StyleBook, por ejemplo, un valor constante. El uso de un nombre de sustitución para este valor le permite actualizar solo el valor de sustitución cuando sea necesario cambiarlo, en lugar de actualizarlo en cada ubicación en la que aparezca en el StyleBook, lo que podría provocar errores.

Las sustituciones también se utilizan para definir asignaciones entre valores como se describe en ejemplos más adelante en este documento.

Cada sustitución de la lista se compone de una clave y un valor. El valor puede ser un valor simple, una expresión, una función o un mapa.

En el siguiente ejemplo, se definen dos sustituciones. El primero es «http-port», que se puede usar como abreviatura de 8181. Al usar una sustitución, puede referirse a esto en el resto del StyleBook como **$substitutions.http-port** en lugar de 8181.

sustituciones:

puerto http: 8181

Esto le permite especificar un nombre mnemotécnico para un número de puerto, así como definir este número de puerto en un solo lugar del StyleBook, independientemente del número de veces que se utilice. Si desea modificar el número de puerto a 8080, puede modificarlo en la sección de sustitución y el cambio tendrá efecto siempre que se utilice el nombre mnemotécnico http-port. En el ejemplo siguiente se muestra cómo se utiliza una sustitución en un componente.

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: \*\*$substitutions.http-port\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Una sustitución también puede ser una expresión compleja. El siguiente ejemplo muestra cómo dos sustituciones utilizan expresiones.

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```

Una expresión de sustitución también puede utilizar expresiones de sustitución existentes, como se muestra en el siguiente ejemplo.

```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-
    port) + str("-app")
<!--NeedCopy-->
```

Otra función útil de las sustituciones son los mapas, donde puede asignar claves a valores. El siguiente es un ejemplo de sustitución de mapas.

```
substitutions:
```



```
    secure-port:
        true: int("443")
        false: int("80")
    secure-protocol:
        true: SSL
        false: HTTP
<!--NeedCopy-->
```

En el ejemplo siguiente se muestra cómo utilizar los mapas de puerto seguro y protocolo seguro.

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: \*\*$substitutions.secure-protocol[$parameters.
    is-secure]\*\*
          ipv46: $parameters.ip
          port: \*\*$substitutions.secure-port[$parameters.is-secure
    ]\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

Esto implica que si el usuario del StyleBook especifica el valor booleano «true» para el parámetro is-secure o selecciona la casilla correspondiente a este parámetro en la GUI de Citrix ADM, a la propiedad servicetype de este componente se le asigna el valor **SSL** y a la propiedad port el valor **443**. Sin embargo, si el usuario especifica «false» para este parámetro o desmarca la casilla correspondiente en la GUI de Citrix ADM, a la propiedad servicetype se le asigna el valor **HTTP** y al puerto se le asigna el valor **80**.

En el ejemplo siguiente se muestra cómo utilizar sustituciones como función. Una función de sustitución puede tomar uno o más argumentos. Los argumentos deben ser de tipo simple, por ejemplo, cadena, número, dirección IP, booleano y otros tipos.

sustituciones:

form-lb-name (nombre): $nombre + “-lb”

En este ejemplo, definimos una función de sustitución «form-lb-name» que toma un argumento de cadena denominado «name» **y lo usa para crear una nueva cadena con el sufijo «-lb» de la cadena del argumento name. Una expresión mediante esta función de sustitución se puede escribir como:

$substitutions.form-lb-name («mi»)

que devuelve «my-lb»

Considere otro ejemplo:

sustituciones:

cspol-priority(priority): 10100 - 100 * $priority

La sustitución cspol-priority es una función que toma un argumento llamado priority y lo usa para calcular un valor. En el resto del StyleBook, esta sustitución se puede utilizar como se muestra en el siguiente ejemplo:

```
components:
  -
    name: cspolicy-binding-comp
    type: ns::csvserver_cspolicy_binding
    condition: not $parameters.is-default
    properties:
         name: $parameters.csvserver-name
         policyname: $components.cspolicy-comp.properties.policyname
         priority: $substitutions.cspol-priority($parameters.pool.
   priority)
<!--NeedCopy-->
```

La sustitución también puede estar compuesta por una clave y un valor. El valor puede ser un valor simple, una expresión, una función, un mapa, una lista o un diccionario.

El siguiente es un ejemplo de una sustitución llamada «slist» cuyo valor es una lista:

```
substitutions:
  slist:
    - a
    - b
    - c
<!--NeedCopy-->
```

El valor de una sustitución también puede ser un diccionario de pares clave-valor, como se ve en el siguiente ejemplo de una sustitución llamada «sdict»:

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
<!--NeedCopy-->
```

Puede crear atributos más complejos combinando listas y diccionarios. Por ejemplo, una sustitución denominada «slistofdict» devuelve una lista de pares clave-valor.

```
  slistofdict:
    -
      a: $parameters.cs1.lb1.port
      b: $parameters.cs1.lb2.port
    -
      a: $parameters.cs2.lb1.port
      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

Sin embargo, en el siguiente ejemplo, una sustitución «sdictoflist» devuelve un par clave-valor, donde

el valor en sí mismo es otra lista.

```
  sdictoflist:
    a:
      - 1
      - 2
    b:
      - 3
      - 4
<!--NeedCopy-->
```

En los componentes, estas sustituciones se pueden utilizar en construcciones de condición, propiedades, repetición, repetición de condición.

El siguiente ejemplo de un componente muestra cómo se puede utilizar una sustitución para especificar las propiedades:

```
    properties:
      a: $substitutions.slist
      b: $substitutions.sdict
      c: $substitutions.slistofdict
      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

Un caso de uso para definir una sustitución cuyo valor es una lista o un diccionario es cuando está configurando un servidor virtual de conmutación de contenido y varios servidores virtuales de equilibrio de carga. Dado que todos los servidores virtuales lb vinculados al mismo servidor virtual cs pueden tener una configuración idéntica, puede usar la lista de sustituciones y el diccionario para crear esta configuración y evitar repetirla para cada servidor virtual lb.

El siguiente ejemplo muestra la sustitución y el componente en los StyleBooks cs-lb-mon para crear una configuración de servidor virtual de conmutación de contenido. Al construir las propiedades de los StyleBooks cs-lb-mon, la compleja sustitución «lb-properties» especifica las propiedades de los servidores virtuales lb asociados al servidor virtual cs. La sustitución de "lb-properties"es una función que toma el nombre, el tipo de servicio, la dirección IP virtual, el puerto y los servidores como parámetros y genera un par clave-valor como valor. En el componente «cs-pools», asignamos el valor de esta sustitución al parámetro lb-pool para cada grupo.

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
```



```
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
    description: | Updates the cs-lb-mon configuration with the
    different pools provided. Each pool with rule result in a dummy LB
    vserver, cs action, cs policy, and csvserver_cspolicy_binding
    configuration.
    condition: $parameters.server-pools
    repeat: $parameters.server-pools
    repeat-item: pool
    repeat-condition: $pool.rule
    repeat-index: ndx
    properties:
      appname: $parameters.appname + "-cs"
      cs-virtual-ip: $parameters.vip
      cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
    HTTP")
      cs-service-type: $parameters.protocol
      pools:
        -
          lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
    , "0.0.0.0", 0, $pool.servers)
          rule: $pool.rule
          priority: $ndx + 1
<!--NeedCopy-->
```

Mapa de sustitución:

Puede crear sustituciones que asignen las claves a los valores. Por ejemplo, considere un caso en el que quiera definir el puerto predeterminado (valor) que se utilizará para cada protocolo (clave). Para esta tarea, escriba un mapa de sustitución de la siguiente manera.

```
substitutions:
     port:
          HTTP: 80
          DNS: 53
          SSL: 443
<!--NeedCopy-->
```

En este ejemplo, HTTP se asigna a 80, DNS a 53 y SSL se asigna a 443. Para recuperar el puerto de un protocolo determinado que se da como parámetro, utilice la expresión

$substitutions.port[$parameters.protocol]

La expresión devuelve un valor basado en el protocolo especificado por el usuario.

- Si la clave es HTTP, la expresión devuelve 80
- Si la clave es DNS, la expresión devuelve 53
- Si la clave es SSL, la expresión devuelve 443
- Si la clave no está presente en el mapa, la expresión no devuelve ningún valor

Componentes

January 30, 2024

La construcción Componentes de un StyleBook se considera la sección más importante del StyleBook. En esta sección, definirá los objetos de configuración que deben crearse. Con esta construcción, puede crear uno o varios objetos de configuración del mismo tipo.

La construcción de componentes puede utilizar la entrada proporcionada en la sección de parámetros para adaptar la configuración generada por el StyleBook. Se trata de una sección opcional, aunque la mayoría de los StyleBooks tienen una sección de componentes.

En la tabla siguiente se describen los principales atributos de un componente.

|Atributo| Descripción|
—	—
name	El nombre del componente. Puede especificar un nombre alfanumérico. El nombre debe empezar por un alfabeto y puede incluir alfabetos, números, guiones (-) o caracteres de subrayado (_) adicionales.
description	Descripción de la función de este componente en el StyleBook.
type	El tipo determina las propiedades que proporciona este componente. Los componentes tienen dos tipos: **tipo integrado: este tipo**lo proporciona el sistema y no es necesario definirlo, por ejemplo, los tipos de entidades NITRO ”lbvserver” o ”servicegroup”. Cuando un componente tiene un atributo de tipo integrado, crea un objeto de configuración de ese tipo en NetScaler ADC. Por ejemplo, si un componente hace referencia al tipo integrado «lbvserver», este componente crea un servidor virtual de equilibrio de carga en la instancia de Citrix ADC que es el destino de la configuración. **Tipo compuesto**: este tipo hace referencia a un StyleBook existente que creó e importó a NetScaler ADM. Cuando un componente tiene un atributo de tipo compuesto, crea todos los objetos de configuración, que se especifican en el StyleBook al que se hace referencia, en la instancia NetScaler ADC que es el destino de la configuración. Esto le permite combinar varios StyleBooks donde cada StyleBook crea una parte de la configuración final. Para obtener más información sobre StyleBooks compuestos, consulte [Crear un StyleBook compuesto](/es-es/netscaler-application-delivery-management-software/12-1/stylebooks/how-to-create-custom-stylebooks).
properties	Los subatributos que se pueden usar para un atributo de tipo de componente. Las propiedades que son válidas para un componente están dictadas por su tipo. Para un tipo integrado,

estas son las propiedades o atributos del objeto Nitro correspondiente. Para un componente cuyo tipo es otro StyleBook, es decir, un tipo compuesto, las propiedades corresponden a los parámetros definidos en ese StyleBook.|
|

Ejemplo:

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

En este ejemplo, ha definido un componente denominado my-lbvserver-comp. Este componente es de tipo ns::lbvserver (un tipo integrado), donde "ns"es el prefijo que hace referencia al espacio de nombres netscaler.nitro.config y la versión 10.5 que había especificado en la sección import-stylebooks, y "lbvserver"es un recurso NITRO en este espacio de nombres.

Las propiedades de esta sección incluyen cuatro atributos obligatorios y uno opcional (lbmethod) del recurso "lbvserver"y permiten especificar valores para estos atributos. En este ejemplo, está especificando valores estáticos para servicetype y port, mientras que las propiedades name, ipv46 y lbmethod obtienen sus valores de los parámetros de entrada. Se hace referencia a los nombres de los parámetros definidos en la sección de parámetros mediante la notación $parameters.<name>, por ejemplo, $parameters.ip.

> **Nota**
>
> Debe utilizar minúsculas para los nombres de los atributos de los tipos de recursos NITRO (sus propiedades de componentes). De lo contrario, la importación de un StyleBook fallará.

Componentes auxiliares

January 30, 2024

El uso principal de la sección de componentes de un StyleBook es generar objetos de configuración a través de los tipos integrados de Nitro u otro StyleBook que cree los objetos de configuración reales. Los componentes auxiliares no crean objetos de configuración por sí mismos. Los componentes auxiliares toman las entradas de otras secciones, como los objetos de parámetros, las propiedades de

otros componentes o las salidas de otros componentes, y las transforman en otras formas. Otros componentes pueden usarlo posteriormente para generar los objetos de configuración reales. Un componente auxiliar puede ser de dos tipos: Tipo de objeto u otro StyleBook que no contenga una sección de componente.

El siguiente ejemplo muestra un fragmento de un StyleBook que se utiliza para crear un servidor de equilibrio de carga con monitor (lb-mon-comp) en una instancia de Citrix ADC.

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress

components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
<!--NeedCopy-->
```

La sección de parámetros le permite introducir el nombre de la aplicación y las direcciones IP de los servidores de equilibrio de carga. En la sección de componentes lb-mon-comp, el parámetro svc-servers de lb-mon StyleBook espera una lista de objetos en la que cada elemento tiene dos sub-parámetros: ip y port.

Sin embargo, la sección de parámetros de este StyleBook solo acepta las direcciones IP del servidor a través de $parameters.ips. El StyleBook asume que todos los servidores se ejecutan en el puerto 80. Para crear la configuración de equilibrio de carga con lb-mon StyleBook, debe transformar $parameters.ips en una lista de objetos. Esto se logra utilizando el componente auxiliar, help-comp, en

el ejemplo anterior. El componente help-comp es del tipo server-ip-port-params StyleBook. Este StyleBook no tiene ningún componente. Como resultado, no crea ningún objeto de configuración. El help-comp crea una lista de repetición sobre $parameters.ips y construye un objeto que consiste en ip y port (que se establece en un 80 estático) para cada elemento de $parameters.ips. Por lo tanto, help-comp transforma una lista de direcciones IP en una lista de objetos que se pueden usar posteriormente en lb-mon-comp para asignar la propiedad svc-servers. El resultado de help-comp se asigna a la propiedad svc-servers de lb-mon-comp.

Propiedades opcionales

January 30, 2024

En algunos casos, una propiedad de un componente toma su valor de una expresión, que puede ser una expresión simple, como una referencia a un parámetro, o una expresión más compleja. Establecer este valor de propiedad es opcional en el componente. Puede elegir establecer el valor de la propiedad solo si la expresión devuelve un valor real; de lo contrario, puede optar por no establecer esta propiedad.

Por ejemplo, considere que una de las propiedades que quiere establecer es el lbmethod (algoritmo de equilibrio de carga) de un componente cuyo tipo es ns::lbvserver. El valor de la propiedad lbmethod se toma de un valor de parámetro proporcionado por el usuario, como se muestra a continuación:

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

Ahora, considere que el parámetro **lb-advanced.algorithm** es un parámetro opcional. Y, si el usuario no proporciona un valor para este parámetro porque es opcional, la expresión **$parameters.lb-advanced.algorithm** se evalúa como valor en blanco. Por lo tanto, se pasa un valor no válido para la propiedad lbmethod. Para evitar tal situación, puede anotar la propiedad como opcional sufijo su nombre con "?"según se indica a continuación:

```
components
   -
     name: lbvserver_comp
```



```
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod?: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

¿El uso de "?"omite la propiedad si la expresión del derecho no se evalúa como nada, lo que sería equivalente, en este caso, a un componente definido de la siguiente manera:

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
<!--NeedCopy-->
```

Como **lbmethod** es opcional, su omisión hace que sea un componente válido. Tenga en cuenta que lbmethod podría tomar su valor predeterminado si uno está definido en su tipo "ns::lbvserver".

Properties-default-sources construct

January 30, 2024

La construcción properties-default-sources es análoga a la construcción parameters-default-sources. Mientras que la construcción parameters-default-sources permite reutilizar los parámetros existentes (de otros StyleBooks) en un StyleBook, la construcción properties-default-sources permite al usuario especificar las propiedades de un componente en función de las fuentes existentes.

Las propiedades de un componente pueden distribuirse en varias secciones del StyleBook. Por ejemplo, las propiedades pueden provenir de parámetros de objetos, sustituciones que devuelven un objeto, propiedades de otros componentes o salidas de otros componentes. En tales casos, debe redefinir las propiedades que aparecen en otras secciones del StyleBook en la definición del componente. Evidentemente, esto es redundante y puede provocar errores. Para solucionar este problema, se puede utilizar la construcción properties-default-sources. El componente fijo properties-default-sources es una lista en la que cada elemento identifica un origen para algunas propiedades del componente.

Por ejemplo, considere un componente que crea una configuración de lbvserver. Este componente

debe definir las propiedades del lbvserver de la siguiente manera.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```

En el ejemplo anterior, observe que los valores de todas las propiedades definidas en la sección de componentes se toman de $parameters.lb objeto. Aunque se toman de una sola fuente, las propiedades se definen de nuevo en el StyleBook. Además, si se agrega un nuevo subparámetro al objeto $parameters.lb que sea relevante para la configuración del servidor lbvserver, debe actualizar el componente lb-comp para agregar la nueva propiedad que corresponde al nuevo subparámetro.

Para evitar redefinir las propiedades y obtener todas las propiedades relevantes de un componente sin enumerarlas explícitamente en la sección de propiedades, se puede utilizar la construcción properties-default-sources. El ejemplo anterior se puede escribir de la siguiente manera.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
<!--NeedCopy-->
```

En el ejemplo anterior, el uso de la construcción properties-default-sources reduce el tamaño de la definición del componente, lo que permite definir un componente de forma concisa. Además, cada vez que cambia el origen de las propiedades del componente, los cambios se reflejan automáticamente. Por ejemplo, cuando se agrega una nueva propiedad, por ejemplo «persistencetype», al objeto $parameters.lb, esta propiedad se agrega a la configuración de lb-comp de forma predeterminada, ya que persistencetype es una propiedad de lbvserver. Por lo tanto, la construcción properties-default-sources proporciona una interfaz dinámica para definir los componentes sin preocuparse por los cambios que ocurren en las fuentes de las propiedades del componente.

Cálculo de las propiedades del componente

En esta sección se explica cómo se obtienen las propiedades si se utiliza la construcción properties-default-sources en un componente. En primer lugar, el compilador de StyleBooks identifica la lista de propiedades de un componente en función de su tipo (en el ejemplo anterior, lbvserver). A continuación, el compilador obtiene estas propiedades de las múltiples fuentes en el orden en que están definidas (en la sección properties-default-sources del componente). Si una propiedad existe en varios orígenes, la propiedad que aparece en el último origen tiene prioridad sobre otras. Por último, una propiedad obtenida mediante la construcción properties-default-sources se puede reemplazar en la sección de propiedades del componente. Es importante tener en cuenta que la definición de una sección de componentes debe tener al menos una sección de properties-default-sources o una sección de propiedades. Puede que tenga ambas cosas.

Componentes anidados

January 30, 2024

Al anidar un componente dentro de otro componente, el componente anidado puede crear sus objetos de configuración haciendo referencia a los objetos de configuración o al contexto creado por el componente principal. El componente anidado puede crear uno o más objetos para cada objeto creado en el componente principal. Anidar un componente dentro de otro componente no indica ninguna relación entre los objetos de configuración creados. El anidamiento es una forma de facilitar la tarea de los componentes para construir objetos de configuración dentro de un contexto existente de los componentes principales.

Ejemplo:

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
```



```
18          components:
19             -
20               name: lbvserver-svg-binding-comp
21               type: ns::lbvserver_servicegroup_binding
22               properties:
23                 name: $parent.parent.properties.name
24                 servicegroupname: $parent.properties.name
25                   -
26                     name: members-svcg-comp
27                     type: ns::servicegroup_servicegroupmember_binding
28                     repeat:
29                       repeat-list: $parameters.svc-servers
30                       repeat-item: srv
31                     properties:
32                       ip: $srv
33                       port: str($parameters.svc-port)
34                       servicegroupname: $parent.properties.name
35 <!--NeedCopy-->
```

En este ejemplo, se utiliza el anidamiento de varios niveles. El componente my-lbvserver-comp tiene un componente secundario denominado my-svcg-comp. Además, el componente my-svcg-comp tiene dos componentes secundarios. El componente my-svcg-comp se utiliza para crear un objeto de configuración de grupos de servicios en la instancia de Citrix ADC proporcionando valores a los atributos del tipo de recurso NITRO integrado «servicegroup». « El primer componente secundario del componente my-svcg, lbvserver-svg-binding-comp, se usa para vincular el grupo de servicios creado por su componente principal al servidor virtual de equilibrio de carga (lbvserver) creado por el componente principal del componente principal. La notación $principal, también llamada referencia principal, se utiliza para hacer referencia a entidades en los componentes principal. El segundo componente secundario, members-svcg-comp, se usa para vincular la lista de servicios al grupo de servicios creado por el componente principal. El enlace se logra mediante el uso de la construcción de repetición de StyleBook para iterar sobre la lista de servicios especificados para el parámetro svc-servers. Para obtener información sobre las construcciones repetidas, consulte Repetir construcción.

También puede crear los mismos objetos de configuración sin utilizar el anidamiento de componentes. Para obtener más información y ejemplos, consulte StyleBook to Create a Basic Load Balancing Configuration.

Construcción de condición

January 30, 2024

Puede hacer que un componente sea condicional mediante una construcción de condiciones. El valor de una construcción condicional es una expresión booleana que se evalúa como verdadera o falsa.

Si la condición es verdadera, el componente se usa para crear sus objetos de configuración. Si la condición es falsa, se omite el componente y no se crea ningún objeto de configuración a través de él. La expresión booleana se basa a menudo en valores de parámetros.

Ejemplo:

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
             name: $parameters.name + "-svcgrp"
             servicetype: HTTP
<!--NeedCopy-->
```

En este ejemplo, si el usuario especifica un valor para el parámetro opcional svc-server-ips, el motor StyleBook procesa el componente servicegroup-comp. Si la condición es falsa, es decir, si el usuario no proporciona un valor a este parámetro, se asigna un valor nulo a este parámetro y se evalúa como falso, el motor StyleBook ignora la presencia de este componente y no se crea ningún grupo de servicios.

Tenga en cuenta que la expresión booleana puede basarse en cualquier expresión válida admitida en StyleBooks (por ejemplo, si hay otro componente o si un parámetro tiene un valor determinado).

En el ejemplo siguiente se crea el objeto de configuración de NITRO tipo ns::systemfile si la condición se evalúa como true.

Ejemplo:

```
    components
         -
           name: pem_key_files
           type: ns::systemfile
           condition: "$components.der-certificate-files-comp or
  $components.pem-certificate-files-comp"
           properties:
                  filecontent: $certificate.keyfile.contents
                  fileencoding: "BASE64"
                  filelocation: "/nsconfig/ssl"
                  filename: $certificate.keyfile.filename
<!--NeedCopy-->
```

En este ejemplo, la condición es una expresión «OR» compleja, en la que desea que el StyleBook cree este objeto de configuración solo si otros dos componentes del StyleBook se han procesado (no se han omitido) y, por lo tanto, se crea una dependencia entre los componentes.

Repetir componente fijo

January 30, 2024

Puede utilizar la construcción **repetida** de un componente para crear varios objetos de configuración del mismo tipo.

En el ejemplo siguiente, el componente **members-svcg-comp** se utiliza para enlazar la lista de servicios al grupo de servicios creado por el componente principal. Para crear un objeto de configuración que vincule cada servidor al grupo de servicios, utilice la construcción **repeat** para recorrer la lista de servicios especificada para el parámetro **svc-servers** . Durante la iteración, el componente crea un objeto NITRO de tipo **servicegroup_servicegroupmember_binding** para cada servicio (denominado **srv** en la construcción **repeat-item**) en el grupo de servicios, y establece el atributo **ip** en cada NITRO a la dirección IP del servicio correspondiente.

Ejemplo:

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
          components:
                -
                   name: my-svcg-comp
                   type: ns::servicegroup
                   properties:
                        name: $parameters.name + "-svcgrp"
                        servicetype: HTTP
                  components:
                         -
                         name: lbvserver-svg-binding-comp
                         type: ns::lbvserver\servicegroup\binding
                         properties:
                               name: $parent.parent.properties.name
                               servicegroupname: $parent.properties.
    name
                         -
                         name: members-svcg-comp
                         type: ns::servicegroup\servicegroupmember\
    binding
                         repeat:
                           repeat-list: $parameters.svc-servers
                           repeat-item: srv
                         properties:
```



```
32                                  ip: $srv
33                                  port: $parameters.svc-port
34                                  servicegroupname: $parent.properties.
    name
35 <!--NeedCopy-->
```

La **repetición** es un objeto en sí misma, y **repeat-list** y **repeat-item** son atributos del objeto repetido.

- repeat-list es un atributo obligatorio que identifica la lista en la que itera el componente.
- repeat-item es opcional, y se utiliza para dar un nombre descriptivo al elemento actual en la iteración.

Si no se especifica, se puede acceder al elemento actual mediante la expresión**$repeat-item**. El último componente en el ejemplo anterior también se puede escribir de la siguiente manera:

```
1            -
2            name: members-svcg-comp
3            type: ns::servicegroup_servicegroupmember_binding
4            repeat:
5              repeat-list: $parameters.svc-servers
6            properties:
7                   ip: $repeat-item
8                   port: $parameters.svc-port
9                   servicegroupname: $parent.properties.name
10 <!--NeedCopy-->
```

Además de poder hacer referencia al elemento actual en blanco iterando sobre una lista, también es posible hacer referencia al índice actual del elemento de la lista mediante el índice **repetido**. En el ejemplo siguiente, **repeat-index** se utiliza para calcular un número de puerto basado en el índice actual:

```
1              name: services
2              type: ns::service
3              repeat:
4                 repeat-list: $parameters.app-services
5                 repeat-item: srv
6              properties:
7                  ip: $parameters.app-ip
8                  port: $parameters.base-port + repeat-index
9                  servicegroupname: $parent.properties.name
10 <!--NeedCopy-->
```

Al igual que en la construcción **repeat-item** , puedes asignar un nombre de variable diferente para hacer referencia al índice actual de la iteración. El ejemplo anterior es equivalente al siguiente ejemplo:

```
1      -
2              name: services
3              type: ns::service
```



```
            repeat:
               repeat-list: $parameters.app-services
               repeat-item: srv
               repeat-index: idx
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + $idx
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

Construcción de condición de repetición

January 30, 2024

La construcción de condición de repetición se evalúa en cada iteración de una construcción de repetición y el resultado determina si se debe generar el objeto de configuración en esa iteración o pasar a la siguiente iteración. El siguiente ejemplo muestra el uso de la construcción de condición de repetición:

Ejemplo:

```
components
   -
      name: der-key-files-comp
      type: ns::systemfile
      repeat:
      repeat-list: $parameters.certificates
      repeat-item: certificate
        repeat-condition: $certificate.ssl-inform == DER
        properties:
         filecontent: base64($certificate.keyfile.contents)
         fileencoding: BASE64
         filelocation: /nsconfig/ssl
         filename: $certificate.keyfile.file
<!--NeedCopy-->
```

En este ejemplo, el componente der-key-files-comp itera sobre todos los certificados proporcionados por el usuario, pero solo crea objetos de configuración que corresponden a los certificados con codificación DER. En cada iteración, la expresión de condición de repetición se evalúa para probar si la codificación del certificado es del tipo DER. Si no es de tipo DER, no se genera ningún objeto de configuración en la iteración actual y la iteración se mueve al siguiente certificado de la lista.

Repeticiones anidadas

January 30, 2024

Con la construcción de repetición anidada, puede tener más de una construcción de repetición en cada componente, según la definición del componente. Considere una repetición anidada de dos niveles. Para cada elemento de la lista externa (primera lista repetida), puede crear una lista repetida para todos los elementos de la lista interna (segunda lista repetida). El compilador StyleBook admite hasta tres repeticiones anidadas. Cada nivel de repetición tiene asociados los atributos repeat-item y repeat-index. Tanto los atributos repeat-item como repeat-index son opcionales. Además, cada repetición también puede especificar una condición de repetición.

Ejemplo:

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
  -
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
         repeat-list: $parameters.vips
         repeat-item: ip
         repeat:
              repeat-list: $parameters.vip-ports
              repeat-item: port
      properties:
         name: str("lb-") + str($ip) + '-' + str($port)
         servicetype: HTTP
         ipv46: $ip
         port: $port
<!--NeedCopy-->
```

En el ejemplo anterior, para cada elemento de $parameters.vips, iteramos sobre todos los elementos de $parameters.vip-ports. Por lo tanto, para cada dirección IP especificada en $parameters.vips, creamos objetos de configuración lbvserver para todos los puertos especificados en $parameters.vip-ports. La sección de propiedades define el nombre del objeto con «lb» como prefijo para la combinación de la dirección IP y el puerto. Por lo tanto, para cada iteración, $ip + $port define una combinación única de la dirección IP y el número de puerto.

Si no se proporciona el atributo repeat-item, el compilador genera un valor predeterminado para él. Los valores predeterminados para repeat-item son: $repeat-item, $repeat-item-1, $repeat-item-

2 respectivamente para cada nivel de repetición. Del mismo modo, si no se proporciona el atributo repeat-index, el compilador genera un valor predeterminado para él. Los valores predeterminados para repeat-index son: $repeat-index, $repeat-index-1 y $repeat-index-2 respectivamente para cada nivel de repetición.

El siguiente ejemplo describe la convención de nomenclatura en ausencia de los atributos repeat-item y repeat-index en un objeto repetido anidado.

Ejemplo:

```
components:
-
     name: lbvservers-comp
     type: ns::lbvserver
     repeat:
         repeat-list: $parameters.vips
         repeat:
            repeat-list: $parameters.vip-ports
     properties:
        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
    -1)
         servicetype: HTTP
         ipv46: $repeat-item
         port: $repeat-item-1
<!--NeedCopy-->
```

Resultados

January 30, 2024

En la sección de resultados, especifique lo que un StyleBook expone a sus usuarios una vez que haya terminado de crear correctamente todos los objetos de configuración. La sección de salidas de un StyleBook es opcional. No es necesario que un StyleBook devuelva las salidas. Sin embargo, al devolver algunos componentes internos como salidas, permite que los StyleBooks que los importen tengan más flexibilidad, como puede ver al crear un StyleBook compuesto.

En la siguiente tabla se describen los atributos que se utilizan en la sección de salidas.

Atributo	Descripción	Obligatorio
name	El nombre de la salida correspondiente al objeto de configuración que desea exponer.	Sí

Atributo	Descripción	Obligatorio
description	Cadena de texto que describe la salida.	No
value	Este atributo especifica cómo extraer el valor devuelto por un StyleBook.	Sí

Ejemplo:

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

En este ejemplo, expondrá el componente **lbvserver** y el **nombre** del grupo de servicios que crearía StyleBook. El valor de la salida llamada **lbvserver** es el componente **my-lbvserver-comp**. Del mismo modo, el valor de la salida denominada **svc-grp** es el nombre del grupo de servicios creado por el componente **my-svcg**.

Referencia de parámetros

January 30, 2024

En la construcción de componentes, se hace referencia a los parámetros definidos en la sección de parámetros mediante la `$parameters.<parametername>` notación. Si `<parametername>` en sí mismo contiene parámetros (cuando el tipo es objeto), entonces debe usar la notación `$parameters.<parametername>.<sub-parametername>`, etc.

Ejemplo:

```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
```



```
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
<!--NeedCopy-->
```

Referencia de principal

January 30, 2024

Si utiliza componentes anidados, puede hacer referencia al componente principal mediante la notación $parent. Si el componente principal crea varios objetos de configuración utilizando el componente fijo de repetición, y dentro de cada iteración, los componentes secundarios crean otros objetos de configuración, la notación $parent siempre hace referencia a la iteración actual del componente principal. Por ejemplo, $parent.properties.name hace referencia a la propiedad name del objeto de configuración creado en la iteración actual por el padre.

Ejemplo:

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
```



```
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
          name: my-svcg-comp
          type: ns::servicegroup
          properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
            components:
             -
               name: lbvserver-svg-binding-comp
               type: ns::lbvserver_servicegroup_binding
               properties:
                  name: $parent.parent.properties.name
                  servicegroupname: $parent.properties.name
                    -
                      name: members-svcg-comp
                      type: ns::servicegroup_servicegroupmember_binding
                      repeat: $parameters.svc-servers
                      repeat-item: srv
                      properties:
                        ip: $srv
                        port: str($parameters.svc-port)
                        servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

También puede desplazarse hacia activo a través de la jerarquía de componentes accediendo a las propiedades de los principales de los principales hasta los componentes de nivel superior. Por ejemplo, el nombre de propiedad del componente **lbvserver-svg-binding-comp** toma su valor del nombre de la propiedad principal de su componente principal, el componente **my-lbvserver-comp** , mediante la notación **$parent.parent**.

Referencia de componentes

January 30, 2024

En la construcción de componentes, se hace referencia al componente de nivel superior en el StyleBook mediante el uso de la notación **$components.<componentname>**. Si hay componentes anidados dentro de un componente de nivel superior, la notación utilizada es **$components.<componentname>.components.<component-name>** para hacer referencia a ellos, y así sucesivamente.

Ejemplo:

```
components:
```



```
2   -
3      name: my-lbvserver-comp
4       type: ns::lbvserver
5       properties:
6             name: $parameters.name + "-lb"
7             servicetype: HTTP
8             ipv46: $parameters.ip
9             port: 80
10            lbmethod: $parameters.lb-alg
11   -
12      name: my-svcg-comp
13      type: ns::servicegroup
14      properties:
15           name: $parameters.name + "-svcgrp"
16           servicetype: HTTP
17  -
18      name: members-svcg-comp
19      type: ns::servicegroup_servicegroupmember_binding
20      repeat: $parameters.svc-servers
21      repeat-item: srv
22      properties:
23         ip: $srv
24           port: str($parameters.svc-port)
25           servicegroupname: $components.my-svcg-comp.properties.name
26  -
27      name: lbvserver-svg-binding-comp
28      type: ns::lbvserver_servicegroup_binding
29      properties:
30             name: $components.my-lbvserver-comp.properties.name
31             servicegroupname: $components.my-svcg-comp.properties.name
32  <!--NeedCopy-->
```

En este ejemplo, los componentes **my-svcg-comp** y **my-lbvserver-comp** tienen que construirse antes de construir el último componente **lbvserver-svg-binding-comp** porque hay referencias a estos componentes en este último componente. Estas referencias se proporcionan mediante el uso de referencias de componentes denotadas por **$components.<componentname>**.

Referencia de sustituciones

January 30, 2024

En la sección de componentes o en la sección de operaciones, se hace referencia a las sustituciones definidas en la sección de sustituciones mediante la notación **$substitutions.<substitution-name>**. Por ejemplo, **$substitutions.http-port**.

Si una sustitución es un mapa, puede hacer referencia a un elemento en el mapa como **$substitutions.<substitutions-name>[<map-key>]**. Por ejemplo: **$substitutions**

.protocol-map[$parameters.port].

Referencia de variable

January 30, 2024

Al utilizar las construcciones repeat y repeat-item en los componentes para crear varios objetos de configuración, puede asignar un nombre de variable a la construcción repeat-item. A continuación, se puede hacer referencia a esta variable en las propiedades de ese componente o en los componentes secundarios mediante la notación **$\<varname\>**. Tenga en cuenta que cuando la construcción repeat se usa sin la construcción repeat-item en un componente, se puede usar una variable predeterminada llamada $repeat-item para acceder a los elementos de iteración.

Ejemplo:

```
components:
  -
    name: server-members-comp
    type: ns::server
    condition: $parameters.svc-server-domain-names
    repeat: $parameters.svc-server-domain-names
    repeat-item: server-name
    properties:
      name: $server-name + "-server"
      domain: $server-name
    components:
      -
         name: service-members-comp
         type: ns::service
         properties:
           name: $server-name + "-service"
           servername: $parent.properties.name
           servicetype: $parameters.svc-service-type
           port: $parameters.svc-server-port
<!--NeedCopy-->
```

En el ejemplo anterior, se asigna un nombre de variable, server-name, a la construcción repeat-item. Este nombre de variable se hace referencia en las propiedades del mismo componente, así como en los componentes secundarios**$\<varname\>**.

Operaciones

January 30, 2024

Las operaciones son una sección opcional de un StyleBook. En esta sección, puede configurar los análisis de Citrix Application Delivery Management (ADM) para recopilar registros de AppFlow en todas o algunas de las transacciones de tráfico. El servidor virtual creado en una instancia de NetScaler ADC mediante el StyleBook maneja estas transacciones de tráfico. En esta sección, también puede configurar NetScaler ADM para que active alarmas cuando se cumplan determinadas condiciones de tráfico en un servidor virtual.

Puede configurar NetScaler ADM a través de StyleBooks para recopilar estadísticas de tráfico de varios NetScaler ADM Insights que se enumeran a continuación:

- Información web
- Security Insight
- HDX Insight
- Citrix Gateway Insight.

Los servidores virtuales admitidos son el equilibrio de carga, la conmutación de contenido y los servidores virtuales VPN.

Habilite Web Insight y Security Insight o uno de ellos para análisis en un servidor virtual de equilibrio de carga o cambio de contenido. Sin embargo, para los servidores virtuales VPN, debe habilitar HDX Insight y NetScaler Gateway Insight o uno de ellos.

Cualquier Citrix ADM Insight habilitado en instancias de Citrix ADC a través de StyleBooks utiliza el protocolo IPFIX (AppFlow) para enviar los datos de las instancias a Citrix ADC.

Además, cuando habilita Web Insight, "Mediciones del lado del cliente"se habilita en el equilibrio de carga y en los servidores virtuales de conmutación de contenido.

Ejemplo 1:

El siguiente ejemplo muestra cómo escribir la sección de operaciones en un StyleBook para habilitar tanto HDX Insight como Citrix Gateway Insight en un servidor virtual VPN:

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
   a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
```



```
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                 type: hdxinsight**
                  -
                    type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

Ejemplo 2:

El siguiente ejemplo muestra cómo escribir la sección de operaciones en un StyleBook para habilitar Web Insight y Security Insight en un servidor virtual de equilibrio de carga:

```
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on
    LB vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: lbvserver-comp
        type: ns::lbvserver
        properties:
            name: str("lb-") + str($current-target.ip)
            servicetype: HTTP
            ipv46: 1.1.21.37
            port: 80
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.lbvserver-comp
```



```
                  filter: "true"
                   insights:
                   -
                    type: webinsight
                     -
                    type: securityinsight
outputs:
  -
    name: mylbs
    value: $components.lbvserver-comp
<!--NeedCopy-->
```

Análisis

January 30, 2024

La subsección de análisis de la sección de operaciones tiene una estructura similar a la sección de componentes. Cada elemento de la sección de análisis se utiliza para configurar la función NetScaler ADM Analytics para uno o más servidores virtuales creados por el StyleBook.

Un elemento de la sección de análisis tiene los siguientes atributos:

Atributo	Descripción	Obligatorio
name	Nombre del elemento de análisis.	Sí
description	Una cadena de texto que describe qué es este elemento.	No
condition	Expresión booleana. Cuando esta condición se evalúa como falsa, se omite todo el elemento de análisis.	No
repeat	Itera sobre una lista.	No
repeat-condition	Expresión booleana. Si la expresión se evalúa como falsa, se omite la iteración actual.	No
repetir artículo	Nombre del elemento de la iteración actual.	No
repeat-index	Nombre del valor de índice de la iteración actual.	No
properties	La lista de propiedades de la analítica.	Sí

Atributo	Descripción	Obligatorio
target	Una de las propiedades de la lista. La expresión de destino es el nombre de un servidor virtual, configurado en el NetScaler ADC, para el que se recopilarán los análisis.	Sí
filter	Una de las propiedades de la lista. El valor de este atributo es una expresión de directiva avanzada de NetScaler ADC que se utiliza para filtrar las solicitudes en el servidor virtual para las que se recopilarán los análisis. De forma predeterminada, los datos de análisis se recopilan de todo el tráfico que pasa por el servidor virtual.	No

Ejemplo:

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
<!--NeedCopy-->
```

Cada atributo de la sección de análisis se utiliza para indicar a la función de NetScaler ADM Analytics que configure las instancias de NetScaler ADC para recopilar registros de flujo de aplicaciones en el servidor virtual identificado por la propiedad de destino.

Alarmas

January 30, 2024

La subsección de alarmas de la sección de operaciones tiene una estructura similar y los mismos atributos que en la subsección de análisis. La única diferencia está en el atributo properties. Para obtener una lista de todos los atributos (excepto el atributo properties), consulte Analytics.

Las siguientes propiedades están disponibles en una subsección de alarmas:

Atributo	Descripción	Obligatorio
target	Expresión que se evalúa como el nombre de un servidor virtual, configurado en NetScaler ADC, para el que se configuran las alarmas.	Sí
email-profile	Nombre de un perfil de correo electrónico que se define en la función NetScaler ADM Analytics y que contiene una lista de direcciones de correo electrónico a las que quiere notificar cuando se active la alarma.	No (se debe definir un perfil de correo electrónico o un perfil de SMS)
sms-profile	Nombre de un perfil SMS definido en la función de NetScaler ADM Analytics y contiene una lista de números de teléfono que quiere notificar cuando se activa la alarma.	No (se debe definir un perfil de correo electrónico o un perfil de SMS)
rules	Lista de reglas que definen las condiciones que desencadenarían una alarma para el servidor virtual definido por la propiedad de destino.	Sí
metric	Un atributo de regla. El nombre de una métrica que quiere rastrear relacionada con el servidor virtual NetScaler ADC.	Sí

Atributo	Descripción	Obligatorio
operator	Un atributo de regla. El operador que se va a utilizar para comparar la métrica con el valor. Los operadores válidos son ‘‘mayor que’’y ‘‘menor que’’ .	Sí
value	Un atributo de regla. El valor de umbral con el que se compara la métrica mediante el operador. Si el valor de la métrica supera este umbral, se activan las alarmas asociadas.	Sí
period-unit	Atributo de una regla. Frecuencia a la que se debe alertar a los usuarios si se cumple la regla de alarma. Puede contener el valor día, hora o semana. Esto significa que si se cumple la regla, se enviará una alarma una vez por unidad de período (por ejemplo, una vez al día).	Sí

La siguiente tabla proporciona una lista de las métricas de las que se hace un seguimiento en relación con el servidor virtual NetScaler ADC.

Contadores|Descripción|Descripción detallada|Cálculo de NetScaler ADM
|—|—|—|—|
|Para un servidor virtual VPN:|
total_requests|Recuento total de lanzamientos de sesiones VPN|Número total de sesiones activas en este servidor virtual VPN que se iniciaron durante un intervalo de tiempo especificado por el usuario.|Contador que aumenta monótonamente, se incrementa con cada inicio de sesión nueva|
|app_count|Recuento de lanzamientos de aplicaciones VPN|Número total de aplicaciones VPN únicas en este servidor virtual VPN lanzadas durante un intervalo de tiempo especificado por el usuario.|El contador aumenta monótonamente cada vez que se lanza una nueva aplicación|
|app_launch_duration|Duración del lanzamiento de la aplicación VPN|Tiempo promedio necesario para lanzar una aplicación (en milisegundos)|Valor promedio calculado a través de las duraciones de tiempo de lanzamiento de todas las aplicaciones VPN iniciadas en este servidor virtual VPN|

|Otros servidores virtuales (CS, LB, Auth, GSLB) | | |
total_requests|Número de solicitudes|Número de solicitudes de clientes en este servidor virtual desde el último reinicio del dispositivo o desde la creación del servidor virtual, lo que sea más reciente. |Contador que aumenta monótonamente, se incrementa en cada nueva solicitud a este servidor virtual. |
|total_bytes|bytes|Total de bytes transferidos desde el servidor virtual a Citrix ADM durante el intervalo de tiempo especificado. |El contador aumenta monótonamente para tener en cuenta la cantidad total de bytes servidos por este servidor virtual. |
|APPLICATION_RESPONSE_TIME|Tiempo de respuesta|Tiempo de respuesta promedio del servidor virtual. |El valor promedio de los tiempos de respuesta de todas las solicitudes recibidas por este servidor virtual desde el último reinicio del dispositivo (o desde la creación del servidor virtual), lo que sea último. |

Ejemplo de una sección de alarmas en un StyleBook:

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day

<!--NeedCopy-->
```

Expresiones

January 30, 2024

Una de las características más poderosas de StyleBook es el uso de expresiones. Puede utilizar expresiones StyleBooks en varios casos para calcular valores dinámicos. El ejemplo siguiente muestra una expresión para concatenar el valor de un parámetro con una cadena literal.

Ejemplo:

$parameters.appname + «-mon»

Esta expresión recupera el parámetro denominado appname y lo concatena con la cadena «-mon».

Se admiten los siguientes tipos de expresiones:

Expresiones aritméticas

- Adición (+)
- Sustracción (-)
- Multiplicación (*)
- División (/)
- Módulo (%)

Ejemplos:

- Sumar dos números: $parameters.a + $parameters.b
- Multiplicar dos números: $parameters.a * 10
- Encontrar el resto después de la división de un número por otro:

15% 10 resultados en 5

Expresiones de cadena

- Concatenar dos cadenas (+)

Ejemplo:

Encadenar dos cadenas: str(‘‘app-‘‘) + $parameters.appname

Expresiones de lista

Fusiona dos listas (+)

Ejemplo:

- Encadenar dos listas: $parameters.external-servers + $parameters.internal-servers
- Si $parameters.ports-1 es [80, 81] y $parameters.port-2 es [81, 82], $parameters.ports-1 + $parameters.ports-2 da como resultado una lista [80, 81, 81, 82]

Expresiones relacionales

- ==: Comprueba si dos operandos son iguales y devuelve verdadero si son iguales, de lo contrario devuelve false.
- !=: Comprueba si dos operandos son diferentes y devuelve verdadero si son diferentes, de lo contrario devuelve false.
  - : Devuelve true si el primer operando es mayor que el segundo operando, de lo contrario devuelve false.
  - =: Devuelve true si el primer operando es mayor o igual que el segundo operando, de lo contrario devuelve false.
- <: Devuelve true si el primer operando es menor que el segundo operando, de lo contrario devuelve false.
- <=: Devuelve true si el primer operando es menor o igual que el segundo operando, de lo contrario devuelve false.

Ejemplo:

- Uso del operador de igualdad: $parameters.name = = «abcd»
- Uso del operador de desigualdad: $parameters.name! = «predeterminado»
- Ejemplos para otros operadores relacionales
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

Expresiones lógicas (booleanas)

- y: El operador lógico 'y'. Si ambos operandos son verdaderos, el resultado es verdadero; de lo contrario, es falso.
- o: El operador lógico 'o'. Si uno de los operandos es verdadero, el resultado es verdadero; de lo contrario, es falso.
- no: El operador unario. Si el operando es verdadero, el resultado es falso y viceversa.
- in: Comprueba si el primer argumento es una subcadena del segundo argumento
- en: Comprueba si un elemento forma parte de una lista

> **Nota**
>
> Puede escribir expresiones de conversión en las que las cadenas se puedan convertir en números y los números en cadenas. Del mismo modo, un puerto TCP se puede convertir a un número y una dirección IP se puede convertir a una cadena.

Debe usar un delimitador antes y después de cualquier operador. Puede utilizar los siguientes delimitadores:

- Antes de un operador: espacio, tabulación, coma, (,), [,]
- Después de un operador: space, tab, (, [
- Por ejemplo:
- abc + def
- 100 % 10
- 10 > 9

Validación de tipo de expresión

El motor StyleBook ahora permite una verificación de tipos más sólida durante el tiempo de compilación, es decir, las expresiones utilizadas al escribir el StyleBook se validan durante la importación del propio StyleBook en lugar de al crear el paquete de configuración.

Todas las referencias a parámetros, sustituciones, componentes, propiedades de componentes, salidas de componentes, variables definidas por el usuario (repeat-item, repeat-index, argumentos a funciones de sustitución), etc., se validan en cuanto a su existencia y tipo.

Ejemplo de comprobaciones de tipo:

En el siguiente ejemplo, el tipo esperado de propiedad de puerto de lbvserver StyleBook es tcp-port. En las versiones anteriores de Citrix Application Delivery Management (ADM), el compilador StyleBook calculaba el valor como una cadena y el StyleBook se importaba y ejecutaba. Ahora, las validaciones de tipos se realizan en tiempo de compilación (tiempo de importación). El compilador encuentra que string y tcp-port no son tipos compatibles y, por lo tanto, el compilador StyleBook arroja un error y no puede importar o migrar el StyleBook.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
```



```
9         servicetype: HTTP
10
11  You should now declare this as a number for the compiler to
       successfully compile this StyleBook.
12
13    port: 80
14  <!--NeedCopy-->
```

Ejemplo de marcado de expresiones no válidas:

En versiones anteriores, cuando se asignó una expresión no válida a un nombre de propiedad, el compilador no detectó expresiones no válidas y permitió que los StyleBooks se importaran en NetScaler ADM. Ahora, si este StyleBook se importa a Citrix ADM, el compilador identificará esas expresiones no válidas y las marcará. Como resultado, el StyleBook no se importará a Citrix ADM.

En este ejemplo, la expresión asignada a la propiedad de nombre en el componente lb-sg-binding-comp es: $components.lbvserver-comp.properties.lbvservername. Sin embargo, no hay ninguna propiedad denominada lbvservername en el componente lbvserver-comp. En versiones anteriores de NetScaler ADM, el compilador habría permitido esta expresión y la habría importado correctamente. El error real se produciría cuando un usuario quisiera crear un paquete de configuración con este StyleBook. Sin embargo, ahora, este tipo de error se identifica durante la importación y el StyleBook no se importa a NetScaler ADM. Debe corregir manualmente dichos errores e importar los StyleBooks.

```
1  components:
2    -
3      name: lbvserver-comp
4      type: ns::lbvserver
5      properties:
6        name: mylb
7        ipv46: 10.102.190.15
8        port: 80
9        servicetype: HTTP
10   -
11     name: sg-comp
12     type: ns::servicegroup
13     properties:
14       servicegroupname: mysg
15       servicetype: HTTP
16   -
17     name: lb-sg-binding-comp
18     type: ns::lbvserver_servicegroup_binding
19     condition: $parameters.create-binding
20     properties:
21       name: $components.lbvserver-comp.properties.lbvservername
22       servicegroupname: $components.sg-comp.properties.servicegroupname
23 <!--NeedCopy-->
```


Listas de indización

Ahora se puede acceder a los elementos de una lista indexándolos directamente:

Expresión	**Descripción**
$components.test-lbs [0]	Hace referencia al primer elemento del componente test-lbs
$components.test-lbs [0] .properties.p1	Hace referencia a la propiedad p1 del primer elemento en el componente test-lbs
$components.lbcomps [0] .outputs.servicegroups [1] .properties.servicegroupname	Hace referencia a la propiedad servicegroupname del segundo elemento del componente servicegroup, que es una salida del primer elemento del componente lbcomps

Interpolaciones in situ

February 2, 2024

Ahora es posible reemplazar partes de una cadena mediante expresiones de StyleBook. Cuando el compilador de StyleBook evalúe estas expresiones de cadena, la parte de la cadena que usa una expresión de StyleBook se reemplazará por el valor de la expresión. Para incluir expresiones StyleBook en una cadena, usamos la siguiente notación:

"…%{…}%…"

donde los caracteres incluidos entre»% {"y «}%» forman una expresión de StyleBook. Estas expresiones se conocen como "interpolaciones in situ. "

Por ejemplo, la cadena "lb-%{$parameters.appname}%-svc"es una expresión de cadena con interpolación in situ de una expresión StyleBook. El valor de la expresión de cadena depende del valor de la expresión de interpolación. Considere que **$parameters.appname** está asignado con "app1". A continuación, la expresión de cadena se evalúa como **lb-app1-svc**. Esto permite que los valores no se codifiquen en expresiones de cadena, sino que se evalúen en función de los valores definidos por el usuario.

Un caso práctico de interpolaciones in situ es parametrizar las expresiones de política en StyleBooks. Considere un caso en el que quiera escribir una expresión de directiva que compruebe si la dirección URL HTTP contiene una palabra específica, por ejemplo, "jpeg".

Para ello, escriba una expresión de directiva de la siguiente manera: "HTTP.REQ.URL.CONTAINS(\ "jpeg\")".

Ahora, si desea parametrizar el objeto en la URL HTTP, puede agregar un parámetro de cadena en el StyleBook, por ejemplo, $parameters.url-object. La expresión de política debe escribirse en función de este parámetro. Para hacer eso, usa la concatenación de cadenas para lograr el resultado. La expresión se vería así:

str("HTTP.REQ.URL.CONTAINS(\""+ $parameters.url-object + "\")")

Si a $parameter.url-object se le asigna "csv", la expresión anterior se evaluará como "HTTP.REQ.URL.CONTAINS(\ "csv\")". Sin embargo, esta expresión no es fácil de leer. Para que esta parametrización sea fácil de leer y entender, puede utilizar interpolaciones in situ.

La expresión con interpolación in situ es ahora:

str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")

En la expresión anterior, utilizó una expresión de interpolación que agrega las comillas internas alrededor del valor de $parameters.url-object. El resultado de esta expresión es el mismo que el anterior, pero parece más intuitivo y se acerca más al resultado real.

Tipos permitidos dentro de interpolaciones

Puede usar expresiones que generen valores de los siguientes tipos dentro de las interpolaciones: boolean, number, tcp-port, ipaddress y string. El valor generado se transforma automáticamente en una cadena cuando las interpolaciones se reemplazan con el resultado.

Las expresiones de cadena pueden tener 0, 1 o más interpolaciones. En una interpolación secuencial, diferentes partes de la expresión de cadena se pueden reemplazar por diferentes expresiones de StyleBook. Por ejemplo, la cadena lb-% {$parameters.appname} %-% {$parameters.vip}% devuelve "lb-app1-1.1.1.1", si $parameters.appname es "app1"y $parameters.vip es "1.1.1.1"

Las expresiones de cadena también admiten interpolaciones anidadas. Es decir, una expresión de interpolación se puede anidar dentro de otra expresión de interpolación para que el valor de una expresión pueda convertirse en una entrada a la segunda expresión.

Por ejemplo, considere una cadena «% {lb-% {$parameters.port + 1}%}%»

La cadena interna "**% {$parameters.port + 1}%** "devuelve «lb-81"si $parameters.port es 80. Aquí, esta expresión está anidada dentro de otra expresión de interpolación.

En la siguiente tabla se describen los diferentes tipos de interpolaciones con ejemplos y resultados correspondientes. El valor de los parámetros utilizados en los ejemplos es:

- $parameters.appname: "lb1"
- $parámetros.vip: «1.1.1.1»
- $parameters.n1: 1
- $parameters.n2: 3

Interpolaciones simples

Expresión	Resultado
lb-% {$parameters.appname} %-def	lb-lb1-def

Conversiones automáticas de tipos

Expresión	Resultado
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-% {verdadero}%	LB-verdadero

Interpolaciones secuenciales

Expresión	Resultado
% {$parameters.appname} %-% {str ($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

Interpolaciones anidadas

Expresión	Resultado
% {abc-% {$parámetros.n1 + 1}%}%	abc-2
str («% {abc-% {$parámetros.n1}%} %-% {$parámetros.n2}%»)	bc-1-3

Interpolaciones con quotewrap

Expresión	Resultado
str («% {quotewrap (abcd)}%»)	«abcd
str («% {quotewrap (https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	“«code class=”language-plaintext highlighter-rouge”>https://”+HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code>

Escapar caracteres en interpolaciones

Si los caracteres «% {» o «}%» forman parte de la cadena, debe proporcionar “\» como carácter de escape para que el compilador de StyleBook no los evalúe como etiquetas de interpolación.

Ejemplo:

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%”if $parameters.vip is 1.1.1.1

En la siguiente tabla se describen algunas expresiones más y sus resultados:

Categoría	Expresión	Resultado
Escaping interpolations	str(“%{str($parameters.n1) + }\%}%”)	1}%
	lb-%{str($parameters.n1) + }\%}%	lb-1}%
	”%{str($parameters.n1) + \” }\%\”}%”	1}%

Funciones integradas

January 30, 2024

Las expresiones en StyleBooks pueden hacer uso de funciones integradas.

Por ejemplo, puedes usar la función integrada str () para transformar un número en una cadena.

str ($parameters.order)

O bien, puede usar la función integrada int () para transformar una cadena en un entero.

int ($parameters.priority)

La siguiente es la lista de funciones integradas admitidas en expresiones StyleBook con ejemplos de cómo se pueden usar:

str()

La función str () transforma el argumento de entrada en un valor de cadena.

Tipos de argumentos permitidos:

- string
- number
- Puerto TCP
- booleano
- Dirección IP

Ejemplos:

- «set-» + str (10) devuelve «set-10”
- str (10) devuelve «10”
- str (1.1.1.1) devuelve «1.1.1.1»
- str (T verdadero) devuelve «T verdadero»
- str (mas) devuelve «mas»

int()

La función int () toma una cadena, un número o un tcpport como argumento y devuelve un entero.

Ejemplos:

- int («10”) devuelve 10
- int (10) devuelve 10

bool()

La función bool () toma cualquier tipo como argumento. Si el valor del argumento es falso, está vacío o no existe, esta función devuelve false.

De lo contrario, devuelve el valor verdadero.

Ejemplos:

- bool (true) devuelve «verdadero»
- bool (false) devuelve «falso»
- bool ($parameters.a) devuelve false si
- $parameters.a es falso, está vacío o no está presente.

len()

La función len () toma una cadena o una lista como argumento y devuelve el número de caracteres de una cadena o el número de elementos de una lista.

Ejemplo 1:

Si define una sustitución de la siguiente manera:

elementos: [“123”, «abc», «xyz”]

len ($substitutions.items) devuelve 3

Ejemplo 2:

len («netscaler mas») devuelve 13

Ejemplo 3:

len ($parameters.vips) devuelve 3 si a $parameters.vip se
le asigna un valor [‘1.1.1.1’, ‘1.1.1.2’, ‘1.1.1.3’]

min()

La función min () toma una lista o una serie de números o puertos TCP como argumentos y devuelve el elemento más pequeño.

Ejemplos con una serie de números/tcp-ports:

- min (80, 100, 1000) devuelve 80
- min (-20, 100, 400) devuelve -20
- min (-80, -20, -10) devuelve -80
- min (0, 100, -400) devuelve -400

Ejemplos con una lista de números/tcp-ports:

- Support $parameters.ports es una lista de puertos tcp y tiene el valor: [80, 81, 8080].

  min ($parameters.ports) devuelve 80.

max()

La función max () toma una lista o una serie de números o puertos TCP como argumentos y devuelve el elemento más grande.

Ejemplos con una serie de números/tcp-ports:

- max (80, 100, 1000) devuelve 1000
- max (-20, 100, 400) devuelve 400
- max (-80, -20, -10) devuelve -10
- max (0, 100, -400) devuelve 100

Ejemplos con una lista de números/tcp-ports:

- Support $parameters.ports es una lista de puertos tcp y tiene el valor: [80, 81, 8080].

  max ($parameters.ports) devuelve 8080.

bin()

La función bin () toma un número como argumento y devuelve una cadena que representa el número en formato binario.

Ejemplos de expresiones:

bin (100) devuelve «0b1100100”

oct()

La función oct () toma un número como argumento y devuelve una cadena que representa el número en formato octal.

Ejemplos de expresiones:

oct (100) devuelve «0144”

hex()

La función hex () toma un número como argumento y devuelve una cadena en minúscula que representa el número en formato hexadecimal.

Ejemplos de expresiones:

hex (100) devuelve «0x64”

lower()

La función lower () toma una cadena como argumento y devuelve la misma cadena en minúsculas.

Ejemplo:

lower («MAS») devuelve «mas»

upper()

La función upper () toma una cadena como argumento y devuelve la misma cadena en mayúsculas.

Ejemplo:

upper («netscaler_mas») devuelve «NET SCALER_MAS»

sum()

La función sum () toma una lista de números o tcpports como argumentos y devuelve la suma de los números de la lista.

Ejemplo 1:

Si define una sustitución de la siguiente manera:
sustituciones:

- lista de números:
  - 11
  - 22
  - 55

  sum ($substitutions.list-of-numbers) devuelve 88

Ejemplo 2:

Si $parameters.ports es [80, 81, 82], sum ($parameters.ports) devuelve 243

pow()

La función pow () toma dos números como argumentos y devuelve un número que representa el primer argumento elevado a la
potencia del segundo.

Ejemplo:

pow (3,2) devuelve 9

ip()

La función ip toma una cadena o una dirección IP como argumento y devuelve la dirección IP en función del valor de entrada.

Ejemplos:

- ip («2.1.1.1”) devuelve «2.1.1.1»
- ip (3.1.1.1) devuelve «3.1.1.1»

base64.encode()

La función base64.encode () toma un argumento de cadena y devuelve la cadena codificada en base64.

Ejemplo:

base64.encode («abcd») devuelve «ywJjza==»

base64.decode()

La función base64.decode toma la cadena codificada en base64 como argumento y devuelve la cadena decodificada.

Ejemplo:

base64.decode («ywJjza==») devuelve «abcd»

exists()

La función exists toma un argumento de cualquier tipo y devuelve un valor booleano. El valor devuelto es True si la entrada tiene algún valor. El valor devuelto es False si el argumento de entrada no tiene un valor (es decir, ningún valor).

Tenga en cuenta que $parameters.monitor es un parámetro opcional. Si proporcionas un valor a este parámetro al crear un paquete de configuración, exists ($parameters.monitor) devuelve True.

De lo contrario, devuelve False.

filter()

La función filter () toma dos argumentos.

Argumento 1: una función de sustitución que toma un argumento y devuelve un valor booleano.

Argumento 2: una lista.

La función devuelve un subconjunto de la lista original donde cada elemento se evalúa como «Verdadero» cuando se pasa a la función de sustitución en el primer
argumento.

Ejemplo:

Supongamos que hemos definido una función de sustitución de la siguiente manera.

sustituciones:

```
1 x(a): $a != 81
```

Esta función devuelve True si el valor de entrada no es igual a 81. De lo contrario, devuelve False.

Supongamos que

$parameters.ports es [81, 80, 81, 89]

filter ($substitutions.x, $parameters.ports) devuelve [80, 89] eliminando todas las apariciones de 81 de la lista.

if-then-else()

La función if-then-else () toma tres argumentos.

Argumento 1: Expresión booleana

Argumento 2: Cualquier expresión

Argumento 3: Cualquier expresión (opcional)

Si la expresión del argumento 1 se evalúa como verdadera, la función devuelve el valor de la expresión proporcionada como argumento 2.

De lo contrario, si se proporciona el argumento 3, la función devuelve el valor de la expresión en el argumento 3.

Si no se proporciona el argumento 3, la función no devuelve ningún valor.

Ejemplo 1:

if-then-else ($parameters.servicetype == HTTP, 80, 443) devuelve «80”si $parameters.servicetype tiene el valor «HTTP». « De lo contrario, la función devuelve
«443”.

Ejemplo 2:

if-then-else ($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport) devuelve el valor de «$parameters.hport» si $parameters.servicetype tiene el valor «HTTP». «

De lo contrario, la función devuelve el valor de «$parameters.sport». «

Ejemplo 3:

if-then-else ($parameters.servicetype == HTTP, 80) devuelve «80”si $parameters.servicetype tiene el valor «HTTP». «

De lo contrario, la función no devuelve ningún valor.

join()

La función join () toma dos argumentos:

Argumento 1: lista de números, puertos TCP, cadenas o direcciones IP

Argumento 2: cadena delimitadora (opcional)

La función une los elementos de la lista proporcionada como argumento uno en una cadena, donde cada elemento está separado por la cadena delimitadora proporcionada como argumento dos. Si no se proporciona el argumento dos, los elementos de la lista se unen en una sola cadena.

Ejemplo:

- $parameters.ports es [81, 82, 83].
  - Con argumento delimitador:

    join ($parameters.ports, ‘-‘) devuelve «81-82-83”
  - Sin argumento delimitador:

    join ($parameters.ports) devuelve «818283”

map()

La función de mapa toma dos argumentos;

Argumento 1: Cualquier función

Argumento 2: Una lista de elementos.

La función devuelve una lista en la que cada elemento de la lista es el resultado de aplicar la función de mapa (argumento uno) al elemento correspondiente del argumento dos.

Funciones permitidas en el argumento 1:

- Funciones integradas que toman un argumento:

  base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode

- Funciones de sustitución que toman al menos un argumento.

Ejemplo:

Supongamos que $parameters.nums es [81, 82, 83].

- Mapa mediante una función integrada, str

  map (str, $parameters.nums) devuelve [“81”, «82”, «83”]

  El resultado de la función de mapa es la lista de cadenas donde cada elemento es cadena se calcula aplicando la función str en el elemento correspondiente en la lista de entrada ($parameters.nums).

- Mapear mediante una función de sustitución

  - Sustituciones:

    add-10 (puerto): $puerto + 10

  - Expresión :

    mapa ($substitutions.add-10,

    $parameters.nums) devuelve una lista de números:
    [91, 92, 93]

El resultado de esta función de mapa es una lista de números. Cada elemento se calcula aplicando la función de sustitución $substitutions.add-10 en el elemento correspondiente de la lista de entrada ($parameters.nums).

quotewrap()

La función quotewrap toma una cadena como argumento y devuelve una cadena después de agregar comillas dobles antes y después del valor de entrada.

Ejemplo:

quotewrap («mas») devuelve «» mas»

replace()

La función de reemplazo utiliza tres argumentos:

Argumento 1: cadena

Argumento 2: cadena

Argumento 3: cadena (opcional)

La función reemplaza todas las apariciones del argumento dos por el argumento tres en el argumento uno.

Si no se proporciona el argumento tres, todas las apariciones del argumento dos se eliminan del argumento uno (en otras palabras, se reemplazan por una cadena vacía).

Reemplazar una subcadena por otra subcadena:

- replace (‘abcdef’, ‘def’, ‘xyz’) devuelve «abcxyz».
  - Todas las apariciones de «def» se sustituyen por «xyz».
- replace (‘abcdefabc’, ‘def’) devuelve «abcabc».
  - Como no hay un tercer argumento, se elimina «def» de la cadena resultante.

trim()

La función trim devuelve una cadena en la que los espacios en blanco iniciales y finales se eliminan de la cadena de entrada.

Ejemplo:

trim (‘abc’) devuelve «abc»

truncate()

La función truncar utiliza dos argumentos:

Argumento 1: cadena

Argumento 2: número

La función devuelve una cadena en la que la cadena de entrada del argumento uno se trunca a la longitud especificada por el argumento dos.

Ejemplo:

truncate (‘netscaler mas’, 9) devuelve «netscaler»

url.encode

La función url.encode devuelve una cadena en la que los caracteres se transforman utilizando el conjunto de caracteres ASCII de acuerdo con el RFC 3986.

Ejemplo:

url.encode («a/b/c») devuelve «a%2Fb%2Fc»

url.decode

La función url.decode devuelve una cadena en la que el argumento codificado en la URL se decodifica en una cadena normal de acuerdo con el RFC 3986.

Ejemplo:

url.decode(“a%2Fb%2Fc”) devuelve “a/b/c”

is-ipv4()

La función is-ipv4 () toma una dirección IP como argumento y devuelve «true» si la dirección IP tiene el formato IPv4.

is-ipv4 (10.10.10.10) devuelve «Verdadero»

is-ipv6()

La función is-ipv6 () toma una dirección IP como argumento y devuelve «true» si la dirección IP tiene el formato IPv6.

is-ipv6 (2001:DB8::) devuelve «Verdadero»

Detección de dependencias

January 30, 2024

Los componentes de un StyleBook pueden hacer referencia a propiedades o secciones de otros componentes del mismo StyleBook. Los componentes son bloques completos por sí mismos y es posible que no se escriban en el mismo orden en que deben ejecutarse. El compilador StyleBook comprueba el orden en que se escriben los componentes y, a continuación, los ejecuta en un orden lógico.

Ejemplo:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
```



```
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
<!--NeedCopy-->
```

En el ejemplo anterior, hay tres componentes definidos: **lbvserver-comp**, **lb-sg-binding-comp** y **sg-comp**. Cuando se ejecuta este StyleBook, primero se crea el lbvserver-comp. El lb-sg-binding-comp hace referencia a las propiedades de lbvserver-comp, pero no se puede crear a continuación, aunque es el segundo componente definido en el StyleBook. Esto se debe a que el lb-sg-binding-comp también depende del sg-comp que aún no se ha creado. Como resultado, el compilador reordena los componentes para que las dependencias de un componente se resuelvan cuando se crea un componente y ejecuta esta lista reordenada de componentes. El orden de ejecución del StyleBook anterior es: lbvserver-comp, sg-comp y lb-sg-binding-comp.

Por lo tanto, el autor de un StyleBook no necesita preocuparse por el orden correcto de los componentes. Los componentes pueden aparecer en cualquier orden. El compilador calcula el orden correcto de ejecución de los componentes en función de cómo los componentes se refieren entre sí. Tenga en cuenta que esta detección y reordenamiento de dependencias también funcionan para las secciones de sustituciones y salidas.

Dependencias cíclicas

Dado que un componente puede hacer referencia a otro componente, es posible que se introduzca el ciclo de dependencias en la definición del StyleBook. Por ejemplo, si el componente A hace referencia a una propiedad definida en el componente B, que de nuevo hace referencia a una propiedad definida en el componente A. Este tipo de dependencia se denomina dependencias cíclicas. Las dependencias cíclicas no se pueden resolver automáticamente. El autor del StyleBook debe corregir manualmente la definición del StyleBook para eliminar esas dependencias cíclicas. El compilador podrá identificar dependencias cíclicas, si existen, e informarlo.

El siguiente ejemplo muestra una dependencia cíclica de componentes:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
```



```
6         name: $components.lb-sg-binding-comp.properties.name
7         ipv46: 10.102.190.15
8         port: 80
9         servicetype: HTTP
10    -
11      name: lb-sg-binding-comp
12      type: ns::lbvserver_servicegroup_binding
13      condition: $parameters.create-binding
14      properties:
15       name: mylb
16        servicegroupname: $components.sg-comp.properties.servicegroupname
17    -
18      name: sg-comp
19      type: ns::servicegroup
20      properties:
21        servicegroupname: mysg
22        servicetype: $components.lbvserver-comp.properties.servicetype
23  <!--NeedCopy-->
```

En el ejemplo anterior, hay tres componentes: **lbvserver-comp**, **lb-sg-binding-comp** y **sg-comp**. lbvserver-comp depende de lb-sg-binding-comp, lb-sg-binding comp depende de sg-comp y sg-comp depende de lbvserver-comp. Aquí, se forma un ciclo de dependencias entre estos componentes y esto no se puede resolver automáticamente. Como resultado, este StyleBook no se puede ejecutar. El compilador de StyleBook detecta esto e impide que StyleBook se importe a NetScaler ADM.

Administración de instancias

January 30, 2024

Las instancias son dispositivos Citrix Application Delivery Controller (ADC) que puede administrar, supervisar y solucionar problemas mediante NetScaler Application Delivery Management (ADM). Debe agregar instancias a NetScaler ADM para supervisarlas. Las instancias se pueden agregar al configurar Citrix ADM o también más adelante. Después de agregar instancias a NetScaler ADM, se sondean continuamente para recopilar información que posteriormente se puede utilizar para resolver problemas o como datos de informes.

Las instancias se pueden agrupar como un grupo estático o como un bloque IP privado. Un grupo estático de instancias puede resultar útil cuando desee ejecutar tareas específicas, como trabajos de configuración, etc. Un bloque IP privado agrupa sus instancias en función de sus ubicaciones geográficas.

Agregar una instancia

Puede agregar instancias al configurar el servidor Citrix ADM por primera vez o más adelante. Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de Citrix ADC, o un intervalo de direcciones IP.

Para obtener información sobre cómo agregar una instancia a NetScaler ADM, consulte Agregar instancias a NetScaler ADM.

Cuando agrega una instancia al servidor NetScaler ADM, el servidor se agrega implícitamente como destino de captura para la instancia y recopila el inventario de la instancia. Para obtener más información, consulte Cómo NetScaler ADM descubre instancias.

Después de agregar una instancia, puede eliminarla navegando a **Redes**> **Panel** y haciendo clic en **Todas las instancias**. En la página Instancias, seleccione la instancia que quiere eliminar y haga clic en **Quitar**.

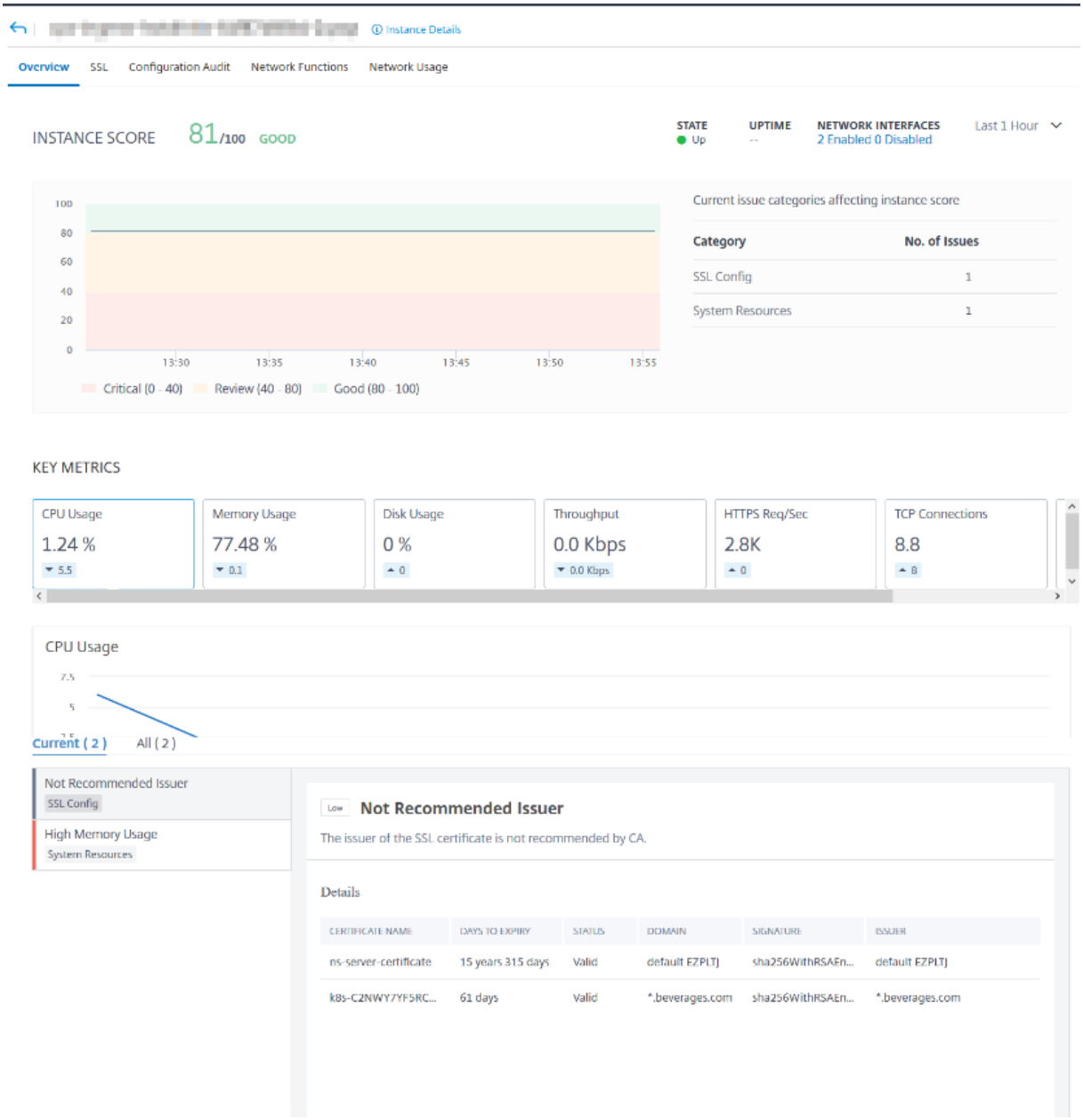
Cómo usar el panel de instancias

El panel de control por instancia de NetScaler ADM muestra los datos en formato tabular y gráfico de la instancia seleccionada. Los datos recopilados de su instancia durante el proceso de sondeo se muestran en el panel de control.

De forma predeterminada, cada minuto, las instancias administradas se sondean para la recopilación de datos. Información estadística como el estado, las solicitudes HTTP por segundo, el uso de CPU, el uso de memoria y el rendimiento se recopilan continuamente mediante llamadas NITRO. Como administrador, puede ver todos estos datos recopilados en una sola página, identificar problemas en la instancia y tomar medidas inmediatas para rectificarlos.

Para ver el panel de control de una instancia específica, vaya a **Redes** > **Instancias** . En el resumen, elija el tipo de instancia y, a continuación, seleccione la instancia que quiere ver y haga clic en **Panel**.

La siguiente ilustración proporciona una visión general de los diversos datos que se muestran en el panel de control por instancia:



- **Visión general**. La ficha de información general muestra el uso de la CPU y la memoria de la instancia elegida. También puede ver los eventos generados por la instancia y los datos de rendimiento. Aquí también se muestra información específica de la instancia, como la dirección IP, sus versiones de hardware y LOM, los detalles del perfil, el número de serie, la persona de contacto, etc. Desplácese hacia abajo más, las funciones con licencia que están disponibles en la instancia elegida junto con los modos configurados en ella.
- **Tablero SSL**. Puede usar la ficha SSL del panel de control por instancia para ver o supervisar los detalles de los certificados SSL, los servidores virtuales SSL y los protocolos SSL de la instancia elegida. Puede hacer clic en los "números"de los gráficos para ver más detalles.

- **Auditoría de configuración**. Puede utilizar la ficha Auditoría de configuración para ver todos los cambios de configuración que se han producido en la instancia elegida. Los gráficos de**estado guardado de la configuración de NetScaler** y de **deriva de la configuración de NetScaler**del panel muestran detalles de alto nivel sobre los cambios de configuración en las configuraciones guardadas frente a las no guardadas.
- **Funciones de red**. Mediante el panel de funciones de red, puede supervisar el estado de las entidades configuradas en la instancia de NetScaler ADC seleccionada. Puede ver gráficos de sus servidores virtuales que muestran datos como las conexiones de los clientes, el rendimiento y las conexiones de los servidores.
- **Uso de red**. Puede ver los datos de rendimiento de la red de la instancia seleccionada en la ficha Uso de la red. Puede mostrar informes de una hora, un día, una semana o un mes. La función deslizante de línea de tiempo se puede utilizar para personalizar la duración de los informes de red que se generan. De forma predeterminada, solo se muestran ocho informes, pero puedes hacer clic en el icono «más» en la esquina inferior derecha de la pantalla para añadir un informe de rendimiento adicional.

Supervisar sitios distribuidos globalmente

January 30, 2024

Como administrador de red, es posible que tenga que supervisar y administrar las instancias de red implementadas en ubicaciones geográficas. Sin embargo, no es fácil medir los requisitos de la red cuando se administran instancias de red en centros de datos distribuidos geográficamente.

Geomaps de NetScaler Application Delivery Management (ADM) le proporciona una representación gráfica de sus sitios y desglosa su experiencia de supervisión de red por geografía. Con las geometrías, puede visualizar la distribución de instancias de red por ubicación y supervisar los problemas de red.

En la siguiente sección se explica cómo puede supervisar los centros de datos en NetScaler ADM.

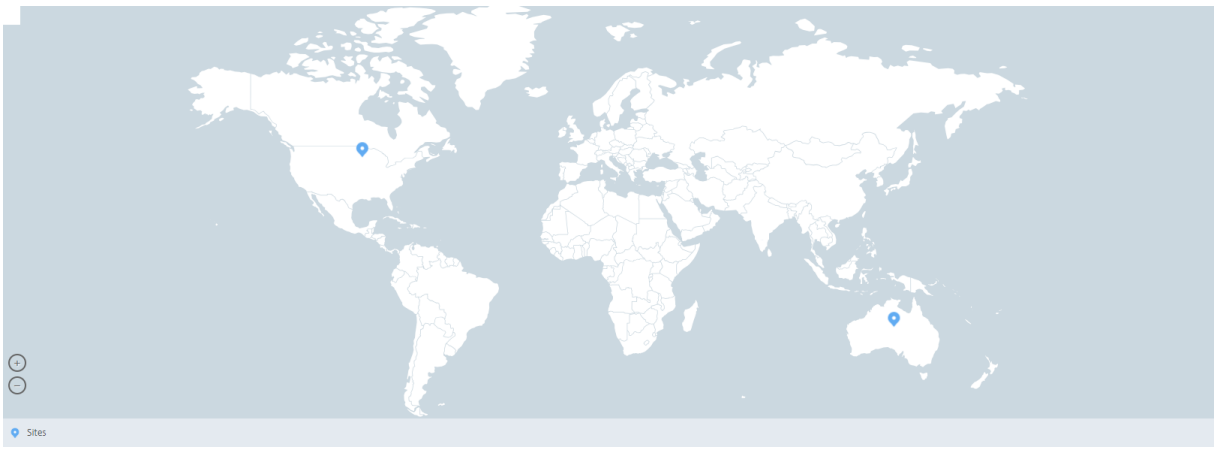
El sitio de NetScaler ADM es una agrupación lógica de instancias de Citrix Application Delivery Controller (ADC) en una ubicación geográfica específica. Por ejemplo, mientras que un sitio está asignado a Amazon Web Services (AWS) y otro sitio puede estar asignado a Azure™. Otro sitio más está alojado en las instalaciones del arrendatario. NetScaler ADM administra y supervisa todas las instancias de NetScaler ADC conectadas a todos los sitios. Puede usar NetScaler ADM para supervisar y recopilar syslog, AppFlow, SNMP y cualquier dato de este tipo que se origine en las instancias administradas.

Geomaps en NetScaler ADM le proporciona una representación gráfica de sus sitios. Geomaps también desglosa su experiencia de supervisión de red por área geográfica. Con las geometrías, puede

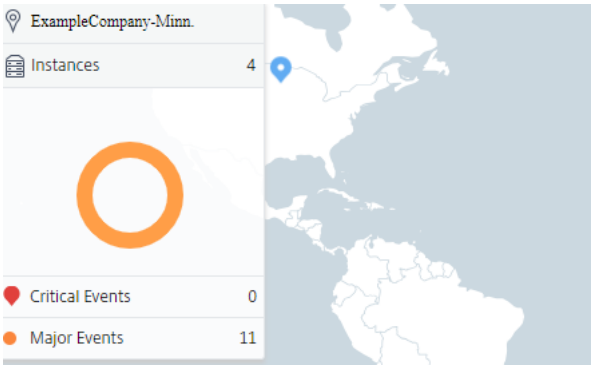
visualizar la distribución de instancias de red por ubicación y supervisar todos los problemas de red. Puede ir a la página **Redes** > **Panel** de control para obtener una representación visual de los sitios creados en el mapa mundial.

Caso de uso

Una empresa líder de telefonía móvil, ExampleCompany, dependía de proveedores de servicios privados para alojar sus recursos y aplicaciones. La empresa ya tenía dos sedes: una en Minneapolis (Estados Unidos) y otra en Alice Springs (Australia). En esta imagen, puede ver que dos marcadores representan los dos sitios existentes.



Los marcadores también muestran un número, que muestra el número de aplicaciones en cada sitio. Puede hacer clic en estos marcadores para obtener más información sobre cada sitio.

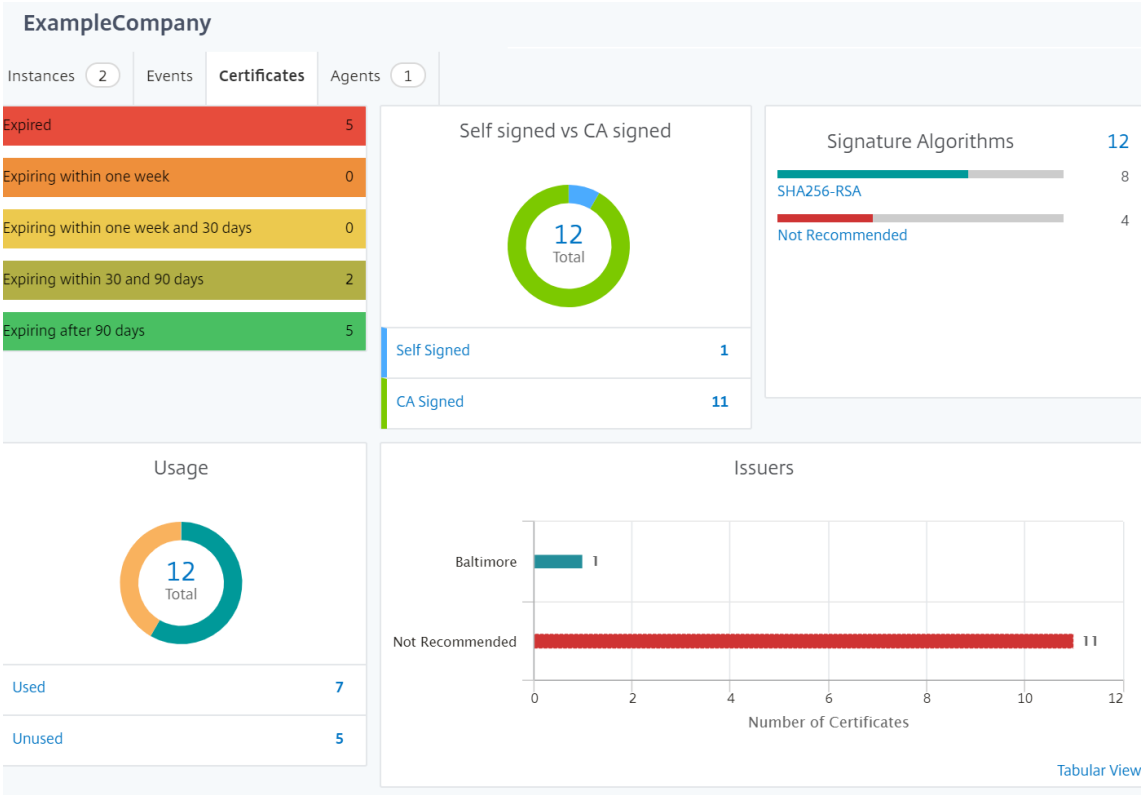


Haga clic en las fichas para ver más información:

- Ficha**Instancias**: consulte lo siguiente en esta ficha:
  - Dirección IP de cada instancia de red
  - Tipo de instancia
  - Número de eventos críticos en ellos

  - Eventos significativos y todos los eventos generados en una instancia de NetScaler ADC.

- Ficha**Eventos**: consulta una lista de los eventos importantes y críticos que se producen en las instancias.
- Ficha**Certificados**: vea lo siguiente en esta ficha:
  - Lista de certificados de todas las instancias
  - Estado de caducidad
  - Información vital y las 10 instancias principales según muchos certificados en uso.
- Ficha**Agentes**: Permite ver una lista de agentes a los que están enlazadas las instancias.



Configuración de Geomaps

ExampleCompany decidió crear un tercer sitio en Bangalore, India. La empresa quería probar la nube descargando algunas de sus aplicaciones de TI internas menos críticas a la oficina de Bangalore. La empresa decidió utilizar los servicios de computación en la nube de AWS.

Como administrador, primero debe crear un sitio y, a continuación, agregar las instancias de NetScaler ADC en NetScaler ADM. También debe agregar la instancia al sitio, agregar un agente y vincular el agente al sitio. A continuación, NetScaler ADM reconoce el sitio al que pertenecen la instancia de NetScaler ADC y el agente.

Para obtener más información sobre cómo agregar instancias de Citrix ADC, consulte Agregar instancias.

Para crear sitios:

Cree sitios antes de agregar instancias en NetScaler ADM. Proporcionar información de ubicación le permite localizar el sitio con precisión.

Vaya a **Redes** > **Sitios** y, a continuación, haga clic en **Agregar** .

1. En la página**Crear Sitio**, especifique la siguiente información:
   a) **Tipo de sitio**: seleccione **Centro de datos**.

   > **Nota**
   >
   > El sitio puede funcionar como centro de datos principal o como sucursal. Elija según corresponda.

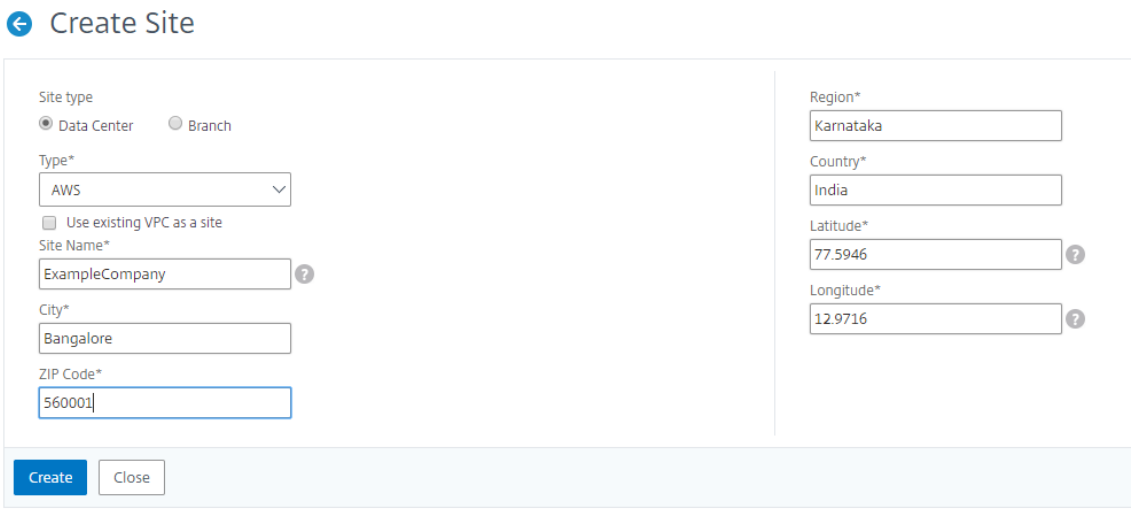
   b) **Tipo**: seleccione AWS como proveedor de nube de la lista.

   > **Nota**
   >
   > Active la casilla **Usar VPC existente como sitio** en consecuencia.

   c) **Nombre del sitio**: escriba el nombre del sitio.
   d) **Ciudad**: escriba la ciudad.
   e) **Código postal**: escriba el código postal.
   f) **Región**: escriba la región.
   g) **País**: Escriba el país
   h) **Latitud**: Escriba la latitud de la ubicación.

      Para la latitud sur, especifique valores negativos. Ejemplo: `-77.5946`.
   i) **Longitud**: Escriba la longitud de la ubicación.

      Para la longitud oeste, especifique valores negativos. Ejemplo: `-12.9716`.
2. Haga clic en **Create**.

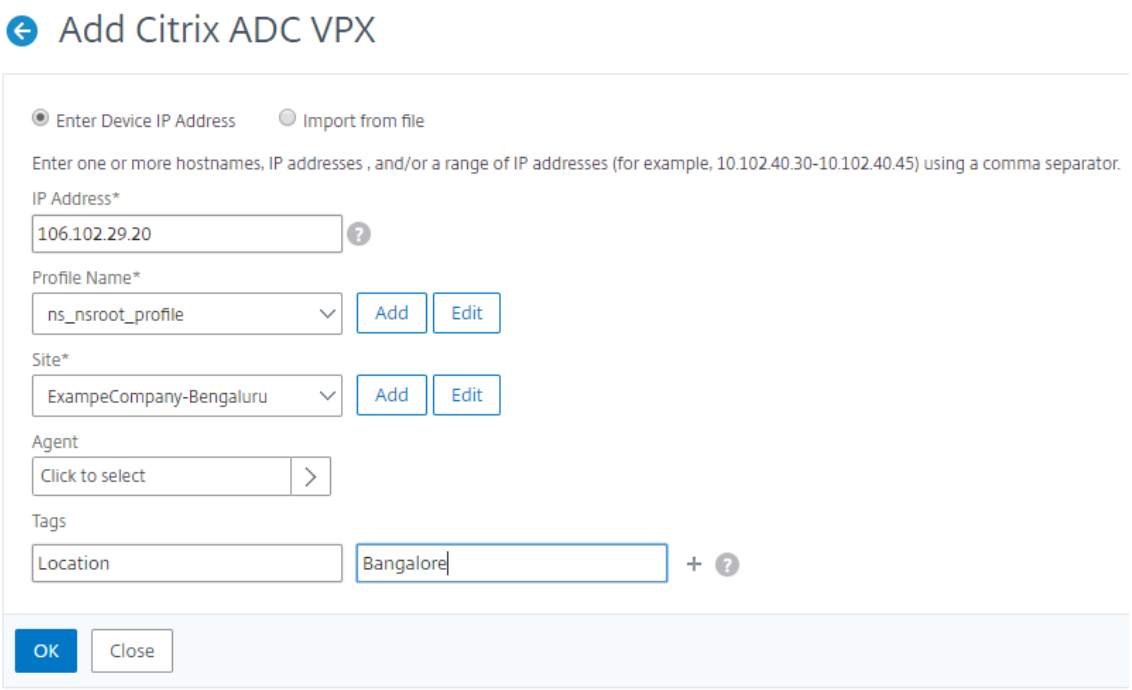


Para agregar instancias y seleccionar sitios:

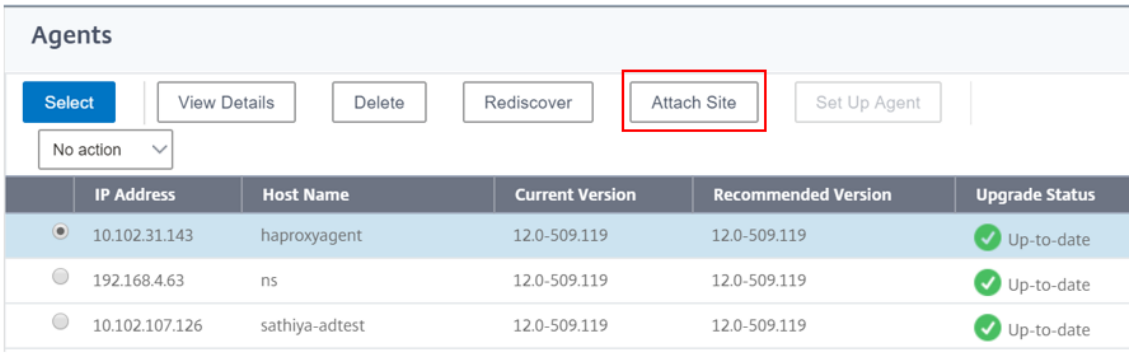
Tras crear los sitios, debe agregar instancias en NetScaler ADM. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

Tras crear los sitios, debe agregar instancias en NetScaler ADM. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

1. En Citrix ADM, vaya a **Redes** > **Instancias**.
2. Seleccione el tipo de instancia que quiere crear y haga clic en **Agregar**.
3. En la página **Agregar NetScaler ADC VPX**, escriba la dirección IP y seleccione el perfil de la lista.
4. Seleccione el sitio de la lista. Puede hacer clic en el signo + situado junto al campo **Sitio** para crear un sitio o hacer clic en el icono de edición para cambiar los detalles del sitio predeterminado.
5. Haga clic en la flecha derecha y seleccione el agente de la lista que aparece.



6. Después de elegir el agente, debe asociar el agente con el sitio. Este paso permite que el agente esté vinculado al sitio. Seleccione el agente y haga clic en **Adjuntar sitio**.



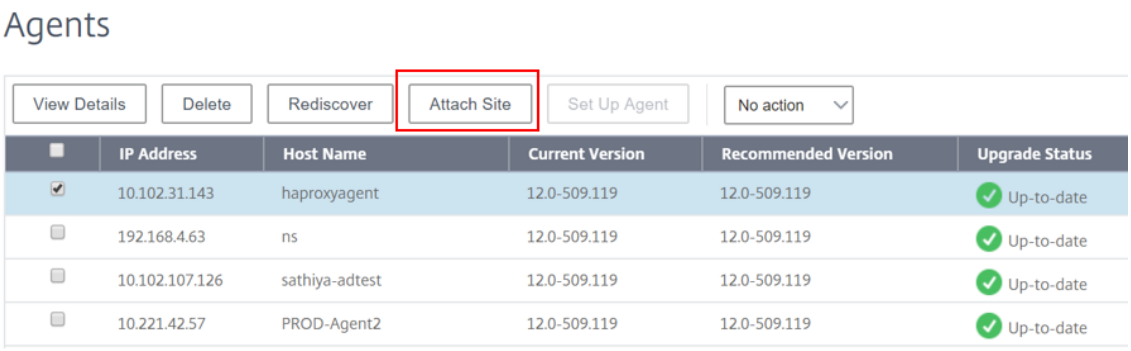
1. Seleccione el sitio de la lista y haga clic en **Guardar**.

1. Haga clic en **Aceptar**.

También puede adjuntar un agente a un sitio accediendo a **Redes** > **Agentes** .

Para asociar un agente NetScaler ADM al sitio:

1. En Citrix ADM, vaya a **Redes** > **Agentes** .
2. Seleccione el agente y haga clic en **Adjuntar sitio**.



1. Puede asociar el sitio y hacer clic en **Guardar**.

NetScaler ADM comienza a supervisar las instancias de NetScaler ADC agregadas en el sitio de Bangalore junto con las instancias en los otros dos sitios.

Cómo crear etiquetas y asignar a instancias

January 30, 2024

Citrix Application Delivery Management (ADM) ahora le permite asociar las instancias de Citrix Application Delivery Controller (ADC) con etiquetas. Una etiqueta es una palabra clave o un término de una palabra que puede asignar a una instancia. Las etiquetas agregan información adicional sobre la instancia. Las etiquetas pueden considerarse metadatos que ayudan a describir una instancia. Las etiquetas le permiten clasificar y buscar instancias basadas en estas palabras clave específicas. También puede asignar varias etiquetas a una sola instancia.

Los siguientes casos de uso le ayudan a entender cómo el etiquetado de las instancias le ayudará a supervisarlas mejor.

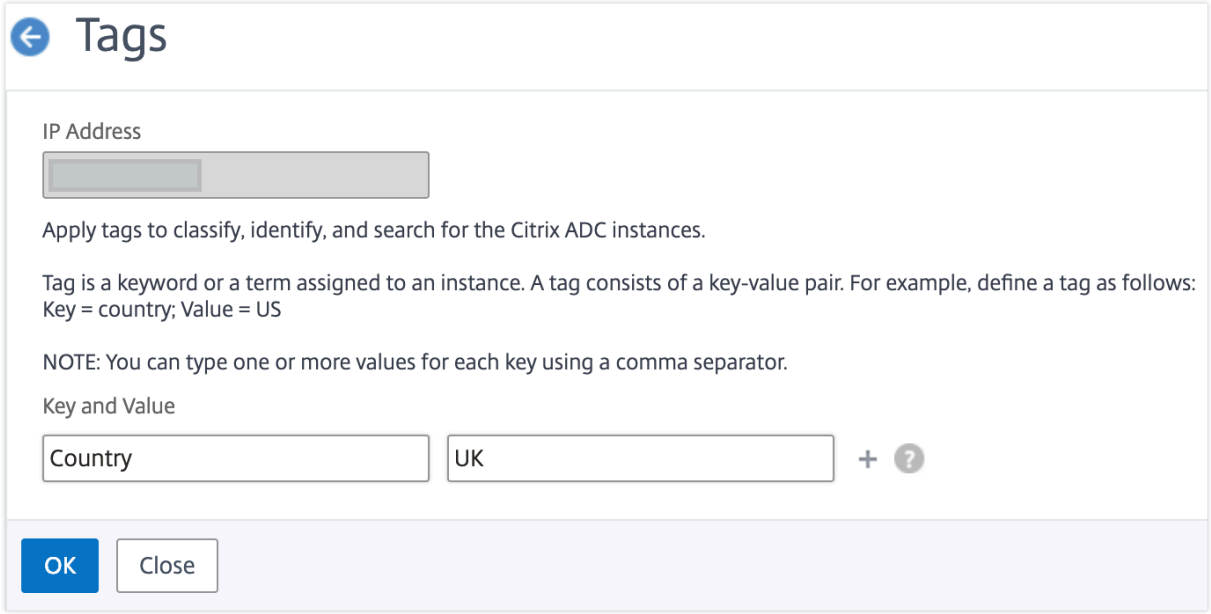
- **Caso de uso 1**: Puede crear una etiqueta para identificar todas las instancias que se encuentran en el Reino Unido. Aquí puedes crear una etiqueta con la clave «País» y el valor como «Reino Unido». « Esta etiqueta le ayuda a buscar y supervisar todas las instancias que se encuentran en el Reino Unido.
- **Caso de uso 2**: Quiere buscar instancias que se encuentran en el entorno provisional. Aquí puedes crear una etiqueta con la clave «Propósito» y el valor como «Staging_ns». « Esta etiqueta le ayuda a separar todas las instancias que se están utilizando en el entorno de ensayo de las instancias que tienen solicitudes de cliente ejecutándose a través de ellas.
- **Caso práctico 3**: plantéese una situación en la que quiera averiguar la lista de instancias de Citrix ADC que se encuentran en el área de Swindon (Reino Unido) y que son de su propiedad, David T. Puede crear etiquetas para todos estos requisitos y asignarlas a todas las instancias que cumplan estas condiciones.

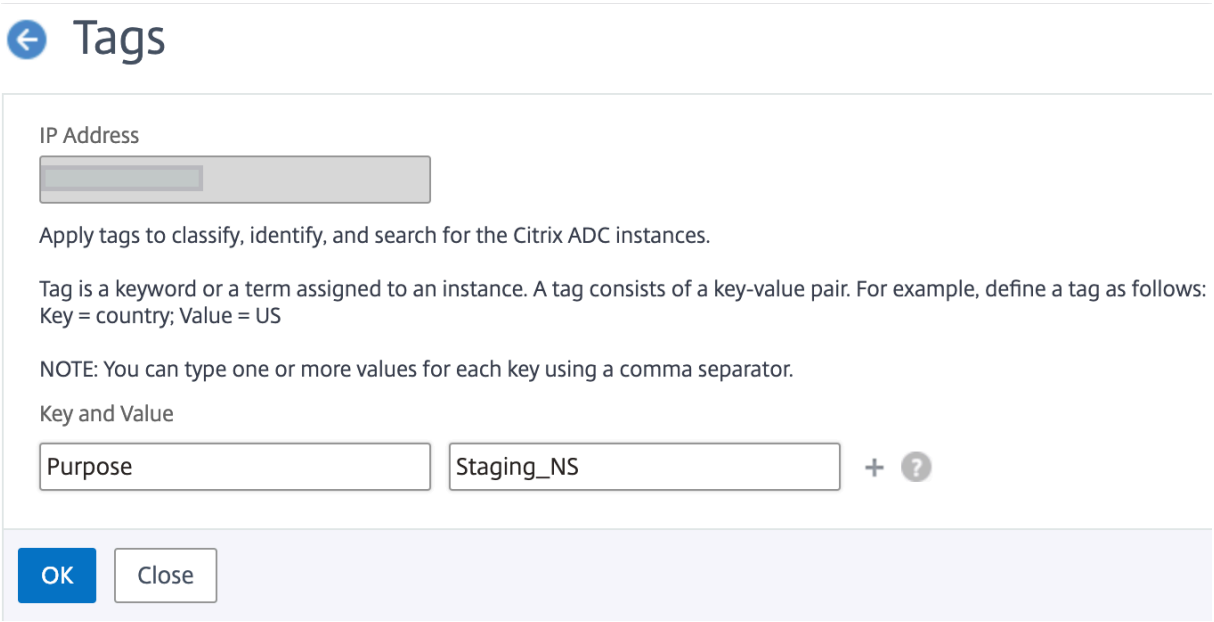
Para asignar etiquetas a la instancia de NetScaler ADC VPX:

1. En Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix ADC** .
2. Seleccione la ficha **NetScaler ADC VPX**.
3. Seleccione el Citrix VPX requerido.
4. Haga clic en **Etiquetas**.
5. Cree etiquetas y haga clic en **Aceptar**.

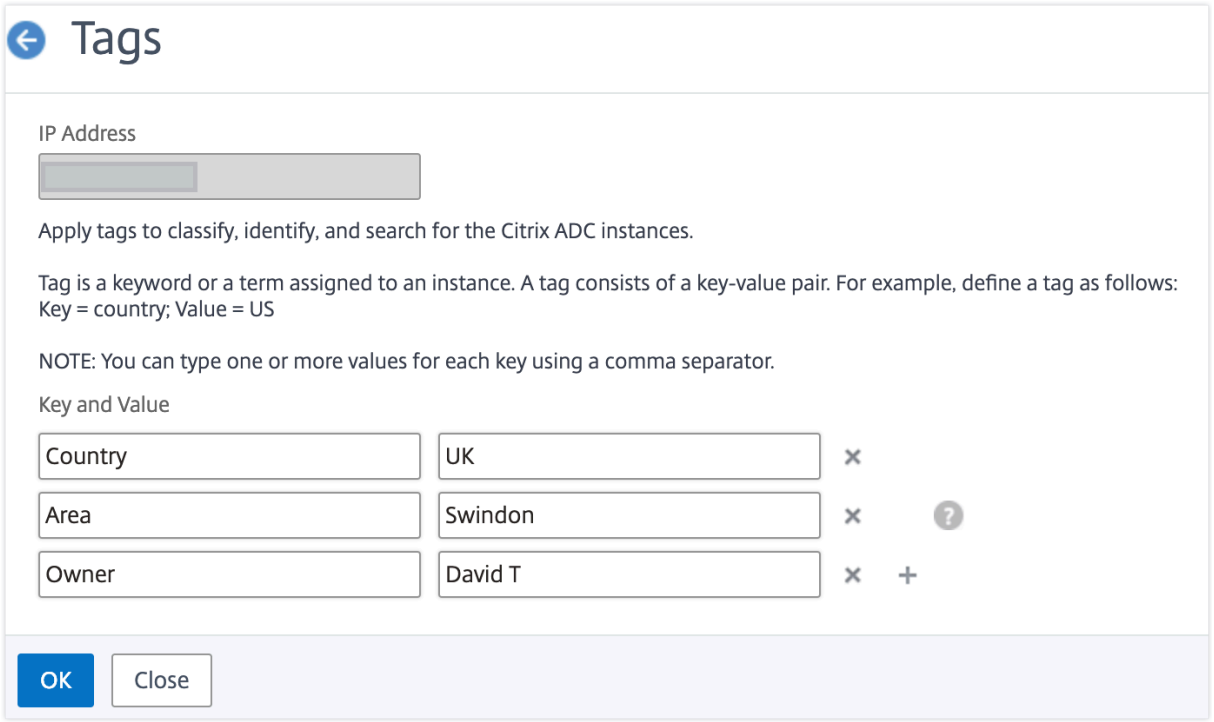
La ventana de **etiquetas** que aparece le permite crear sus propios pares de "clave-valor"asignando valores a cada palabra clave que cree.

Por ejemplo, las siguientes imágenes muestran algunas palabras clave creadas y sus valores. Puede agregar sus propias palabras clave y escribir un valor para cada palabra clave.



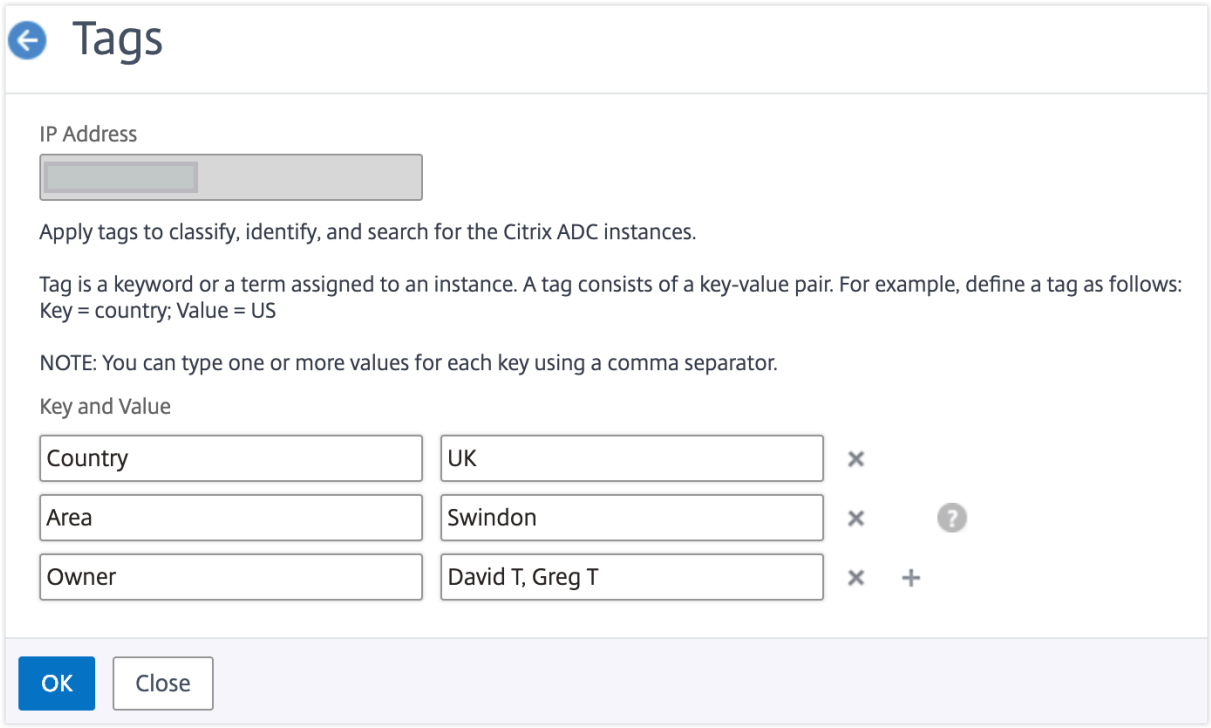


También puede agregar varias etiquetas haciendo clic en "+. "La adición de etiquetas múltiples y significativas le permite buscar las instancias de manera muy eficiente.



Puede agregar varios valores a una palabra clave separándolos con comas.

Por ejemplo, está asignando el rol de administrador a otro compañero de trabajo, Greg T. Puede agregar su nombre separado por una coma. Agregar varios nombres le ayuda a buscar por cualquiera de los nombres o por ambos nombres. NetScaler ADM reconoce los valores separados por comas en dos valores diferentes.



Para obtener más información sobre cómo buscar instancias basadas en etiquetas, consulta Cómo buscar instancias con valores de etiquetas y propiedades.

> **Nota**Posteriormente,
>
> puede agregar nuevas etiquetas o eliminar etiquetas existentes. No hay restricción en el número de etiquetas que se crean.

Cómo buscar instancias mediante valores de etiquetas y propiedades

January 30, 2024

Puede darse una situación en la que Citrix Application Delivery Management (ADM) administre una gran cantidad de instancias de Citrix ADC. Como administrador, es posible que desees tener la flexibilidad de buscar en el inventario de instancias en función de ciertos parámetros. NetScaler ADM ahora ofrece una capacidad de búsqueda mejorada para buscar en un subconjunto de instancias de NetScaler ADC en función de los parámetros que defina en el campo de búsqueda. Puede buscar las instancias en función de dos criterios: etiquetas y propiedades.

- **Etiquetas**. Las etiquetas son términos o palabras clave que puede asignar a una instancia de NetScaler ADC para agregar una descripción adicional sobre la instancia de NetScaler ADC. Ahora puede asociar sus instancias de NetScaler ADC con etiquetas. Estas etiquetas se pueden usar para identificar y buscar mejor las instancias de NetScaler ADC.

- **Propiedades**. Cada instancia de NetScaler ADC agregada en NetScaler ADM tiene algunos parámetros o propiedades predeterminados asociados a esa instancia. Por ejemplo, cada instancia tiene su propio nombre de host, dirección IP, versión, ID de host, ID de modelo de hardware, etc. Puede buscar instancias especificando valores para cualquiera de estas propiedades.

Por ejemplo, considere una situación en la que quiere obtener la lista de instancias de NetScaler ADC que están en la versión 12.0 y están en estado ACTIVO. Aquí, la versión y el estado de la instancia se definen mediante las propiedades predeterminadas.

Además de la versión 12.0 y el estado de funcionamiento de las instancias, también puede buscar aquellas instancias que le pertenezcan. Puede crear una etiqueta de "Propietario"y asignarle un valor "David T". Para obtener más información sobre cómo crear y asignar etiquetas, consulta Cómo crear etiquetas y asignar a instancias.

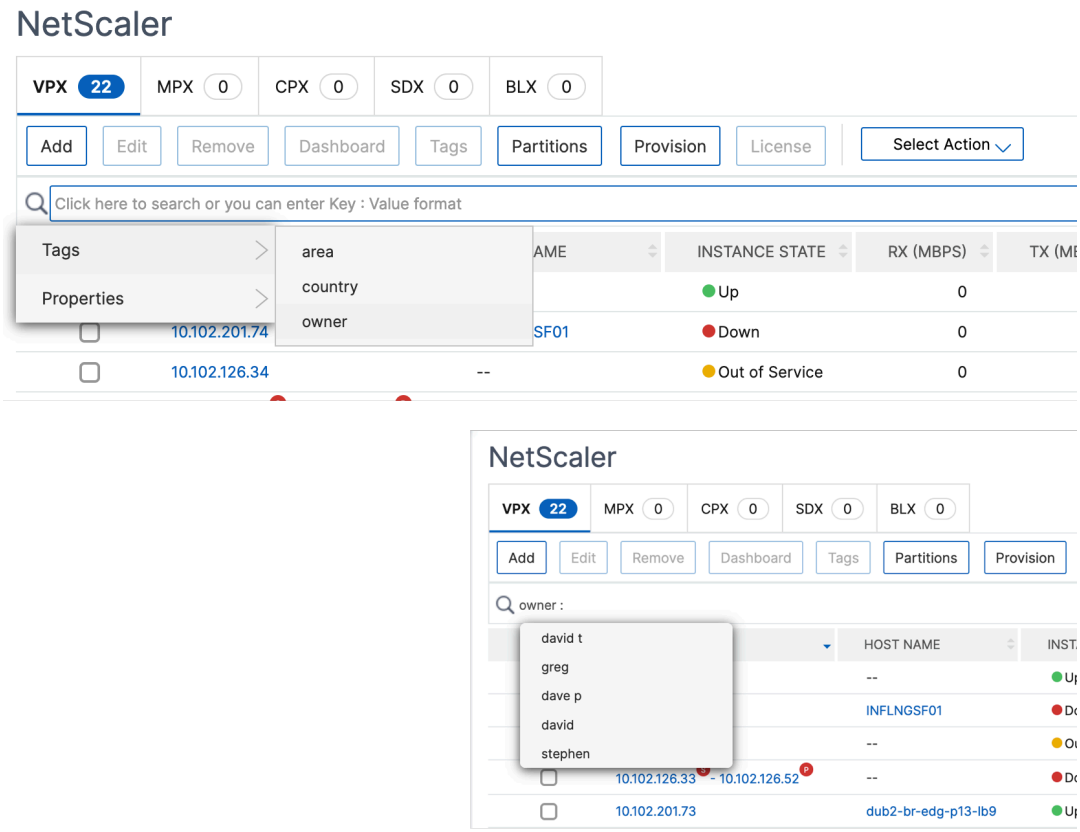
Puede utilizar una combinación de etiquetas y propiedades para crear sus propios criterios de búsqueda.

Para buscar instancias de NetScaler ADC VPX

1. En Citrix ADM, vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX**.
2. Haga clic en el campo de búsqueda. Puede crear una expresión de búsqueda mediante etiquetas o propiedades o combinando ambas.

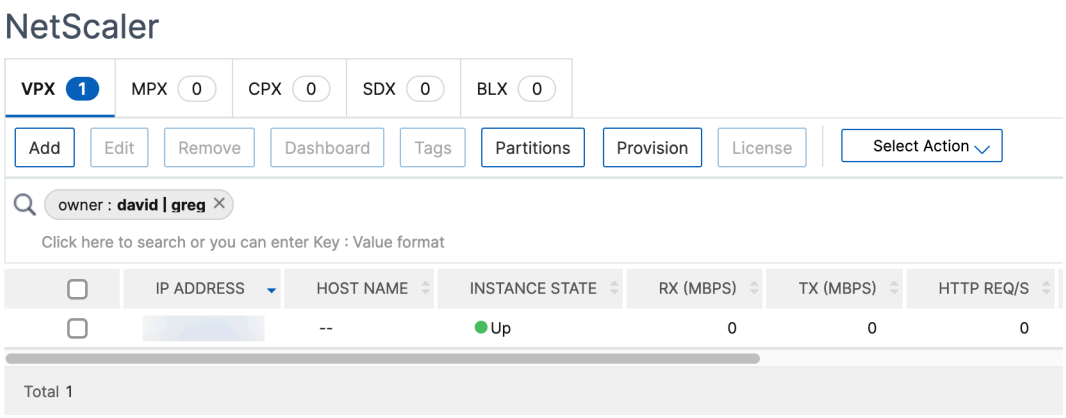
   Los siguientes ejemplos muestran cómo puede utilizar la expresión de búsqueda de manera eficiente para buscar la instancia.

   a) Seleccione la opción **Etiquetas** y seleccione **Propietario**. Selecciona "David T."

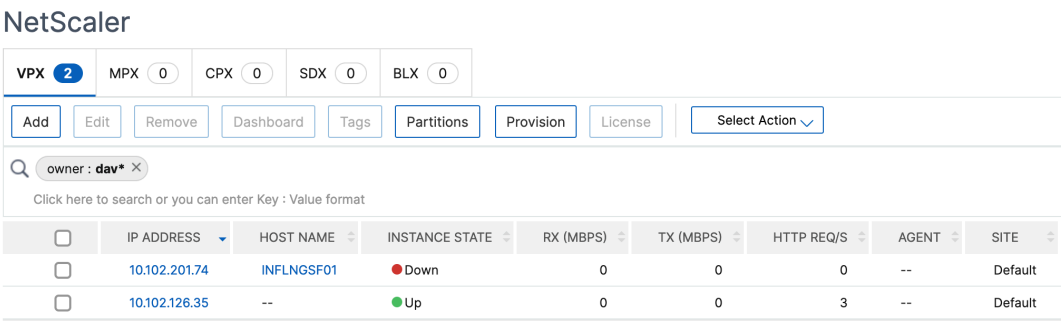


NetScaler ADM admite expresiones regulares y caracteres comodín en las expresiones de búsqueda.

b) Puede utilizar expresiones regulares para ampliar aún más los criterios de búsqueda. Por ejemplo, quiere buscar instancias que sean propiedad de David o Stephen. En tal caso, puede escribir los valores separando los valores con una expresión "|".



c) También puede utilizar caracteres comodín para reemplazar o representar uno o más caracteres. Por ejemplo, puede escribir «Dav*» para buscar todas las instancias que pertenecen a David T y Dave P.



Nota

Para obtener más información sobre expresiones regulares y caracteres comodín y cómo usarlos, haga clic en el icono "información"de la barra de búsqueda.

Administrar particiones de administración de instancias NetScaler ADC

January 30, 2024

Puede configurar particiones de administración en sus instancias de Citrix Application Delivery Controller (ADC) para que a los diferentes grupos de su organización se les asignen diferentes particiones en la misma instancia de Citrix ADC. Se puede asignar un administrador de red para administrar varias particiones en varias instancias de Citrix ADC.

Citrix Application Delivery Management (ADM) proporciona una forma sencilla de administrar todas las particiones que pertenecen a un administrador desde una única consola. Puede administrar estas particiones sin interrumpir otras configuraciones de particiones.

Para permitir que varios usuarios administren diferentes particiones de administración, debe crear grupos y, a continuación, asignar usuarios y particiones a esos grupos. Cada usuario puede ver y administrar solo las particiones del grupo al que pertenece el usuario. Cada partición de administración se considera como una instancia en NetScaler ADM. Cuando detecta una instancia de NetScaler ADC, las particiones de administración configuradas en esa instancia de NetScaler ADC se agregan al sistema automáticamente.

Tenga en cuenta que tiene dos instancias de Citrix VPX con dos particiones configuradas en cada instancia. Por ejemplo, la instancia de ADC 10.102.216.49 de Citrix tiene Partition_1, Partition_2 y Partition_3, y la instancia de NetScaler ADC 10.102.29.120 tiene p1 y p2 como se muestra en la imagen siguiente.

Para ver las particiones, vaya a**Redes > Instancias > NetScaler ADC > VPX**y, a continuación, haga clic en **Particiones**.

Puede asignar al usuario p1 las siguientes particiones: 10.102.29.120-p1 y 10.102.216.49-Partition_1. Además, puede asignar user-p2 para administrar las particiones 10.102.29.80-p2, 10.102.216.49-Partition_2 y 10.102.216.49-Partition_3.

A continuación, debe crear los dos usuarios, user-p1 y user-p2, y debe asignar los usuarios a los grupos que creó para ellos.

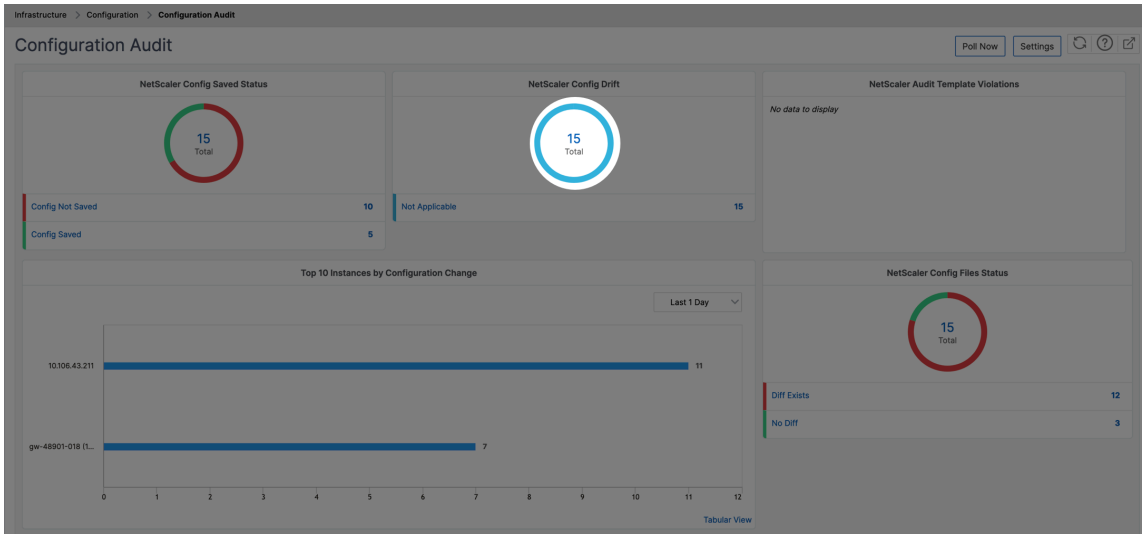
En primer lugar, debe crear dos grupos con los permisos adecuados (por ejemplo, permisos de administrador) e incluir las instancias de partición de administración necesarias en cada grupo. Por ejemplo, cree el grupo del sistema Partition1-admin y agregue las particiones 10.102.29.120-p1 y 10.102.216.49-Partition_1 de Citrix ADC a este grupo. Cree también el grupo de sistemas Partition2-admin y agregue las particiones de administración 10.102.29.120-p2, 10.102.216.49-Partition_2 y 10.102.216.49-Partition_3 de Citrix ADC y a este grupo.

Una vez creada la partición de administración, también puede utilizar la función de diferencia en el historial de revisiones y la función plantilla de auditoría para la partición de administración con fines de auditoría para fines de auditoría.

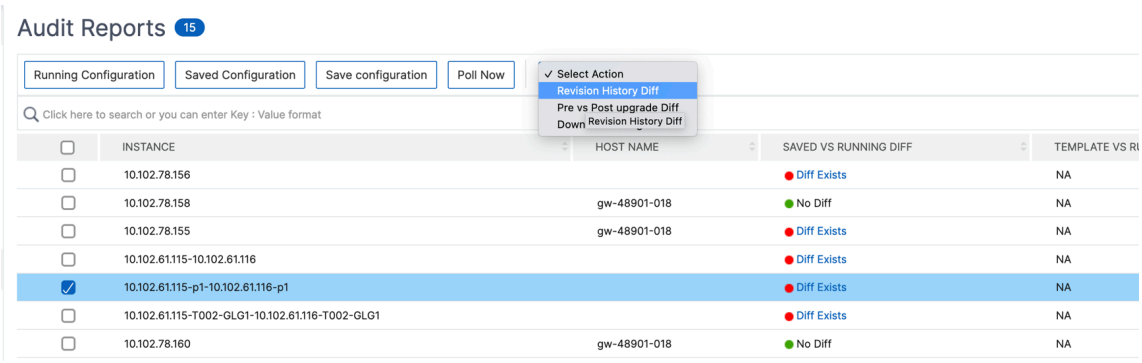
La diferenciadel historial de revisiones para la partición de administración le permite ver la diferencia entre los cinco archivos de configuración más recientes de una instancia de Citrix ADC particionada. Puede comparar los archivos de configuración entre sí (por ejemplo, la revisión de configuración 1 con la revisión de configuración -2) o con la configuración actual en ejecución o guardada con la revisión de configuración. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. Puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.

Para ver la diferencia en el historial de revisiones:

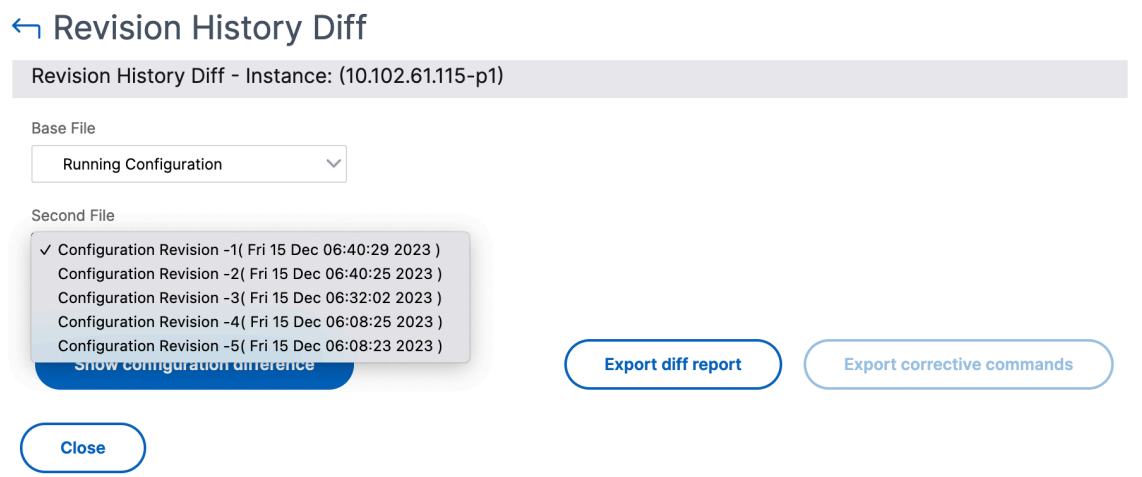
1. Vaya a **Redes > Auditoría de configuración.** Haga clic dentro del gráfico de donut que representa el estado de configuración de instancia. En la página **Informes de auditoría** que se abre, haga clic en la instancia de NetScaler ADC particionada.



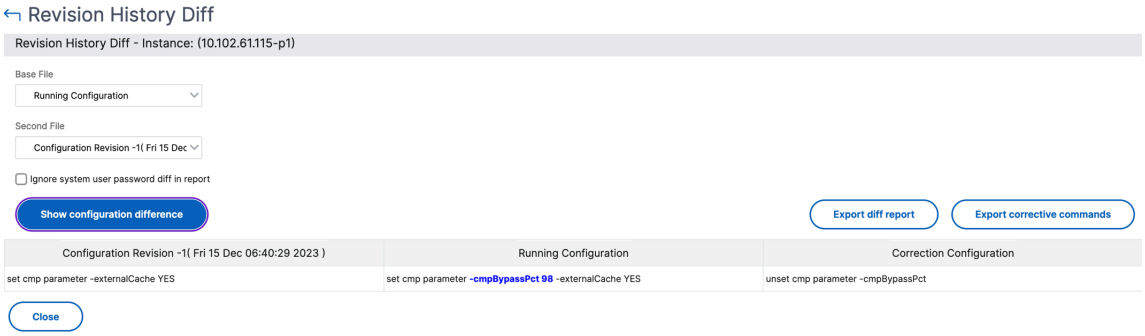
2. En el menú **Acción**, haga clic en Diferencia del **historial de revisiones.**



3. En la página **Diferencia del historial de revisiones**, seleccione los archivos que quiere comparar. Por ejemplo, compare la configuración guardada con la revisión de configuración -1 y, a continuación, haga clic en **Mostrar diferencia de configuración**.



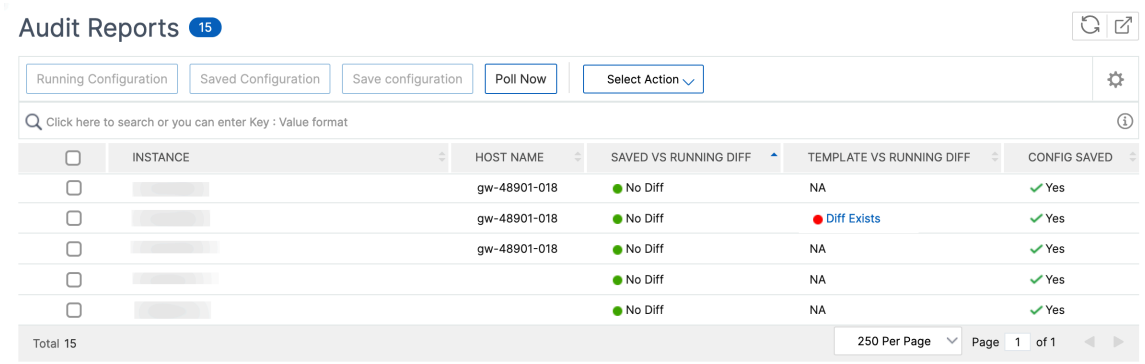
4. A continuación, puede ver la diferencia entre los cinco archivos de configuración más recientes para la instancia de NetScaler ADC con particiones seleccionada, como se muestra a continuación. También puede ver los comandos de configuración correctiva y exportar estos comandos correctivos a la carpeta local. Estos comandos correctivos son los comandos que deben ejecutarse en el archivo base para que la configuración alcance el estado deseado (archivo de configuración que se utiliza para la comparación).



Las plantillas de auditoría para partición le permiten crear una plantilla de configuración personalizada y asociarla a una instancia de partición. Cualquier variación en la configuración en ejecución de la instancia con la plantilla de auditoría se muestra en la columna **Diferencia entre plantilla y ejecución** de la página **Informes de auditoría**. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. También puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.

Para ver la plantilla frente a la diferencia de ejecución:

1. En la página **Informes de auditoría**, haga clic en la instancia de NetScaler ADC con particiones.



2. Si hay alguna diferencia entre la plantilla de auditoría y la configuración en ejecución, la diferencia se muestra como un hipervínculo. Haga clic en el hipervínculo para ver las diferencias si las hay. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. También puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.

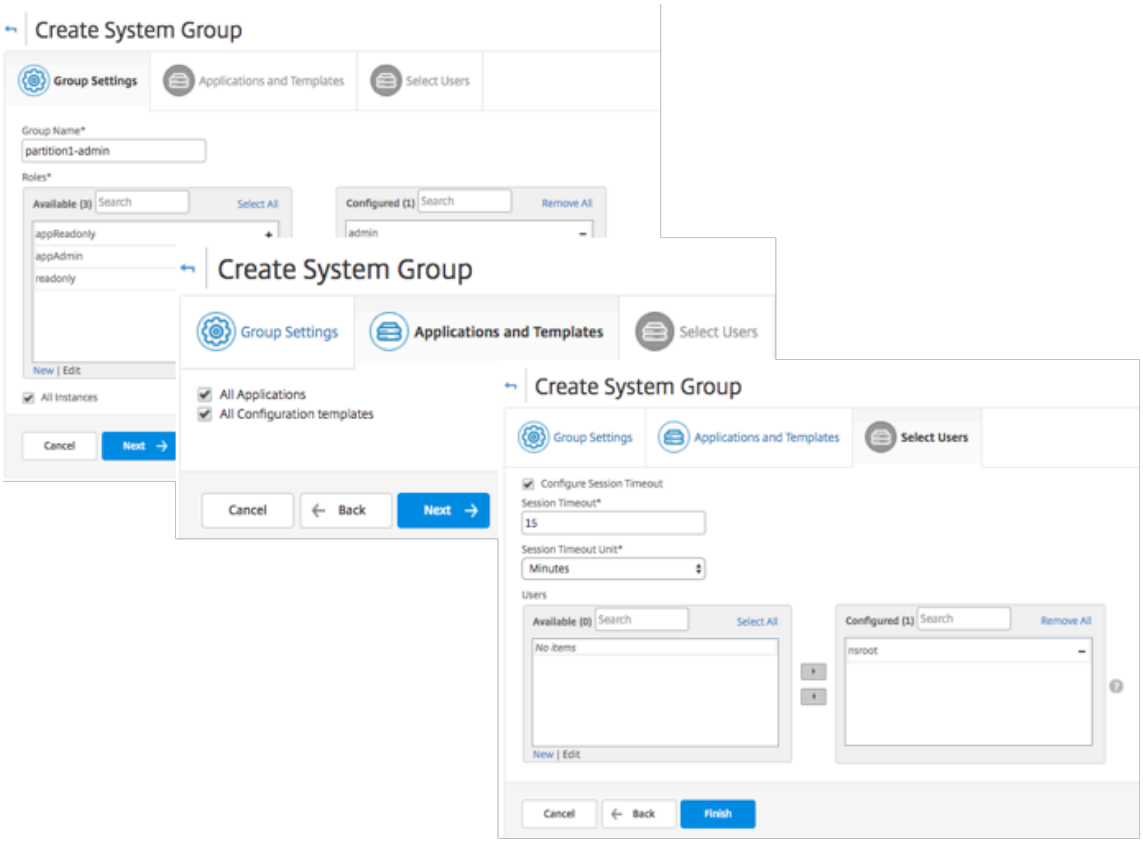
Para crear grupos:

1. Vaya a **Sistema** > **Administración de usuarios** > **Grupos** y, a continuación, haga clic en **Agregar** .
2. En la página **Crear Usuario del Sistema**, especifique lo siguiente:
   - Ficha **Configuración de grupo**: Introduzca el nombre del grupo y los permisos de rol. Para

permitir el acceso a instancias específicas, desactive la casilla**Todas las instancias**y, a continuación, seleccione sus instancias en la página **Seleccionar instancias**.

- Pestaña**Aplicaciones y plantillas**: Puede optar por utilizar este grupo en todas las aplicaciones y plantillas de configuración.
- **Seleccione la ficha Usuarios**: Seleccione los usuarios que desee agregar a este grupo. Puede hacer clic en el enlace **Nuevo** de la tabla **Disponible** para crear nuevos usuarios. Opcionalmente, configure el tiempo de espera de la sesión, donde puede configurar el período de tiempo durante el tiempo que un usuario puede permanecer activo.

3. Haga clic en **Finalizar**.



Para crear usuarios:

1. Vaya a **Sistema** > **Administración de usuarios** > **Usuarios** y, a continuación, haga clic en **Agregar** .
2. En la página**Crear usuario del sistema**, especifique el nombre de usuario y la contraseña. Si lo desea, puede habilitar la autenticación externa y configurar el tiempo de espera de la sesión.
3. Asigne el usuario a un grupo añadiendo el nombre del grupo de la lista**Disponible**a la lista**Configurada**.
4. Haga clic en **Create**.

Ahora cierre sesión e inicie sesión con las credenciales user-p1. Puede ver y administrar solo las particiones de administración que se le asignaron para administrarlas y supervisarlas.

Realizar copias de seguridad y restaurar instancias de NetScaler ADC

January 30, 2024

Puede realizar una copia de seguridad del estado actual de una instancia de NetScaler ADC y posteriormente utilizar los archivos de copia de seguridad para restaurarla al mismo estado. Siempre debe realizar una copia de seguridad de una instancia antes de actualizarla o por motivos de precaución. Una copia de seguridad de un sistema estable le permite restaurarlo a un punto estable si se vuelve inestable.

Existen varias formas de realizar copias de seguridad y restauraciones en una instancia de NetScaler ADC. Puede realizar copias de seguridad y restaurar manualmente las configuraciones de Citrix ADC mediante la GUI y la CLI. También puede utilizar Citrix ADM para realizar copias de seguridad automáticas y restauraciones manuales.

NetScaler ADM realiza una copia de seguridad del estado actual de las instancias de NetScaler ADC administradas mediante llamadas NITRO y los protocolos Secure Shell (SSH) y Secure Copy (SCP).

NetScaler ADM crea una copia de seguridad completa y restaura los siguientes tipos de instancias de NetScaler ADC:

- Citrix SDX
- Citrix VPX
- Citrix MPX

Para obtener más información, consulte Realizar [copias de seguridad y restaurar una instancia de ADC].(https://docs.citrix.com/en-us/citrix-adc/12-1/system/basic-operations/backup-restore-citrix-adc-appliance.html)

> **Nota**
>
> - Desde NetScaler ADM, no puede realizar la operación de copia de seguridad y restauración en un clúster de NetScaler ADC.
> - No puede usar el archivo de copia de seguridad tomado de una instancia para restaurar una instancia diferente.

Los archivos de copia de seguridad se almacenan como un archivo TAR comprimido en el siguiente directorio:


```
/var/mps/tenants/root/device_backup/
<!--NeedCopy-->
```

Para evitar problemas debido a la falta de disponibilidad de espacio en disco, puede guardar un máximo de 50 archivos de copia de seguridad en este directorio.

Para realizar copias de seguridad y restaurar instancias de NetScaler ADC, primero debe configurar las opciones de copia de seguridad en NetScaler ADM. Tras configurar los parámetros, puede seleccionar una sola instancia de Citrix ADC o varias instancias y crear una copia de seguridad de los archivos de configuración en estas instancias. Si es necesario, también puede restaurar las instancias de Citrix ADC mediante estos archivos de copia de seguridad.

Configurar las opciones de copia de seguridad de instancia

La página **Configuración de Copia de Seguridad de Instancia** permite configurar opciones en NetScaler ADM para realizar copias de seguridad de una instancia de NetScaler ADC seleccionada o varias instancias:

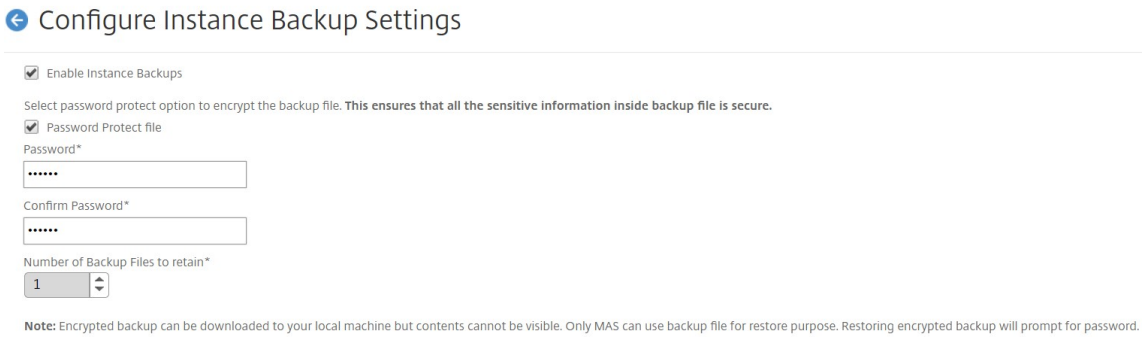
En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**. En el panel derecho, en Configuración de la **instancia, seleccione Configuración** de copia de **seguridad de la instancia** y especifique lo siguiente:

1. **Habilitar copias de seguridad de instancias**: De forma predeterminada, NetScaler ADM está habilitado para realizar copias de seguridad de instancias de NetScaler ADC. Desactive esta opción si no quiere crear archivos de respaldo para las instancias.
2. **Archivo**protegido con contraseña : (opcional) Seleccione la opción de protección con contraseña para cifrar el archivo de respaldo. El cifrado del archivo de respaldo garantiza que toda la información confidencial del archivo de respaldo esté segura.

   > **Nota**
   >
   > Puede descargar el archivo de copia de seguridad cifrado en su equipo local, pero no puede abrirlo con NetScaler ADM GUI ni con ningún editor de texto. Solo Citrix ADM puede recuperar y utilizar el archivo. Se le pedirá que proporcione la contraseña al restaurar el archivo de copia de seguridad cifrado. Sin embargo, puede abrir un archivo de respaldo sin cifrar en su sistema.

3. **Número de archivos de copia de seguridad que se deben conservar**: Especifique el número de archivos de copia de seguridad que se deben conservar en NetScaler ADM. Puede conservar hasta 50 archivos de respaldo del estado actual de una instancia de Citrix ADC. El valor predeterminado es tres archivos de copia de seguridad.

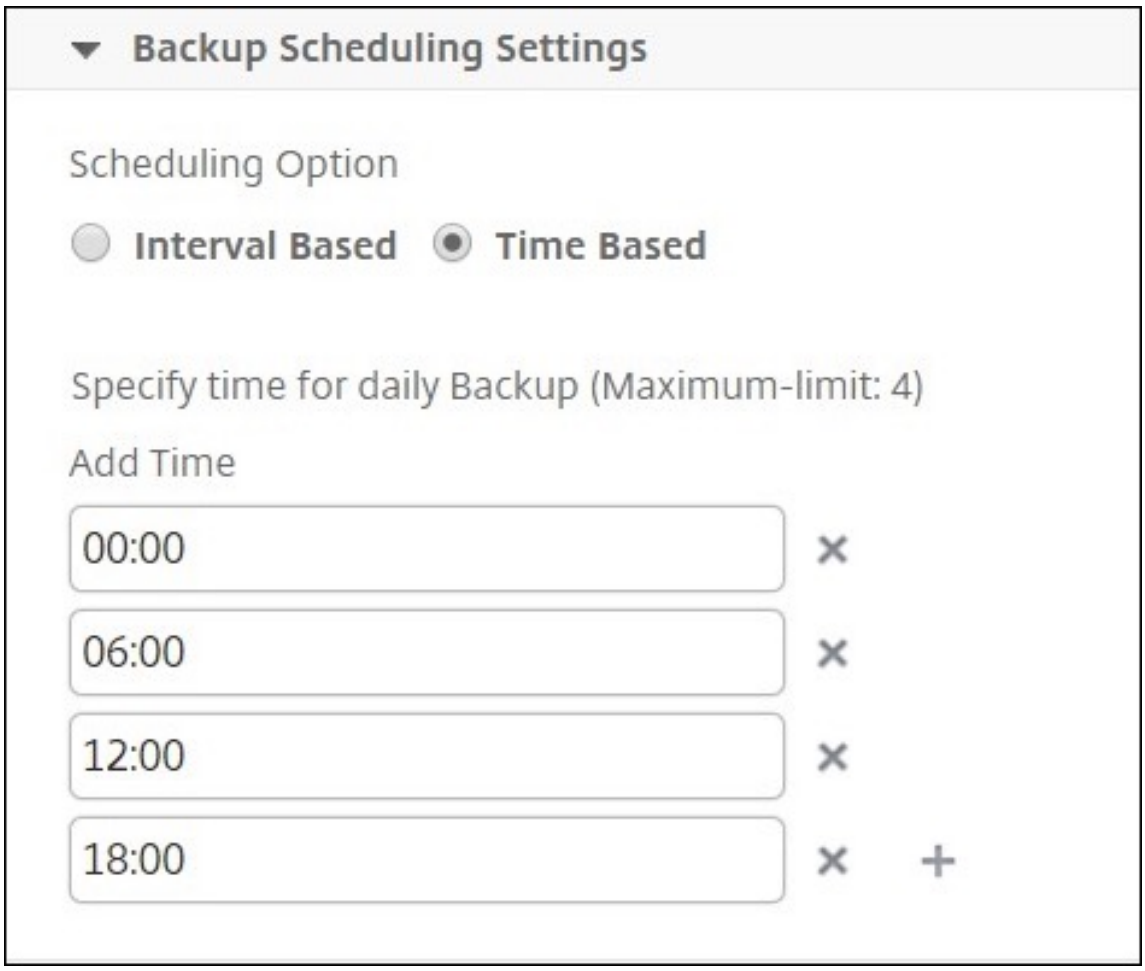
> **Nota**
>
> Cada archivo de respaldo tiene en cuenta algunos requisitos de almacenamiento. Citrix recomienda almacenar un número óptimo de archivos de copia de seguridad de NetScaler ADC en NetScaler ADM según sus necesidades.



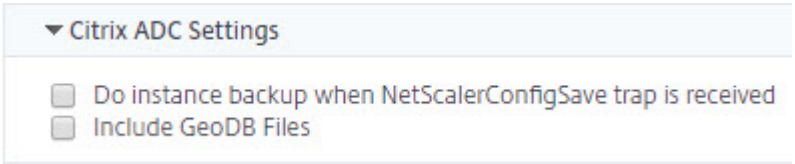
4. **Configuración de programación de copias**de seguridad: (opcional) Hay dos opciones disponibles para crear archivos de copia de seguridad, aunque solo se puede utilizar una opción a la vez:

   a) La opción de programación de copias de seguridad predeterminada es "basada en intervalos". Se crea un archivo de respaldo en Citrix ADM una vez transcurrido el intervalo especificado. El intervalo de copia de seguridad predeterminado es de 12 horas.

   b) También puede cambiar el tipo de copias de seguridad programadas a "basadas en el tiempo. "En esta opción, especifica la hora en formato «horas:minutos» a la que debe realizarse la copia de seguridad. NetScaler ADM permite realizar un máximo de cuatro copias de seguridad diarias en las instancias.



5. **Configuración de NetScaler ADC**: (opcional) De forma predeterminada, NetScaler ADM no crea un archivo de copia de seguridad cuando recibe la trampa "NetScalerConfigSave". Sin embargo, puede habilitar la opción de crear un archivo de respaldo siempre que una instancia de Citrix ADC envíe una captura «NetScalerConfigSave» a Citrix ADM. Una instancia de Citrix ADC envía «NetScalerConfigSave» cada vez que se guarda la configuración de la instancia.
6. **Archivos**de geodatabase : (opcional) De forma predeterminada, Citrix ADM no hace copias de seguridad de los archivos de geodatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.



7. **Transferencia externa:**(opcional) NetScaler ADM le permite transferir los archivos de copia de seguridad de instancias de NetScaler ADC a una ubicación externa:

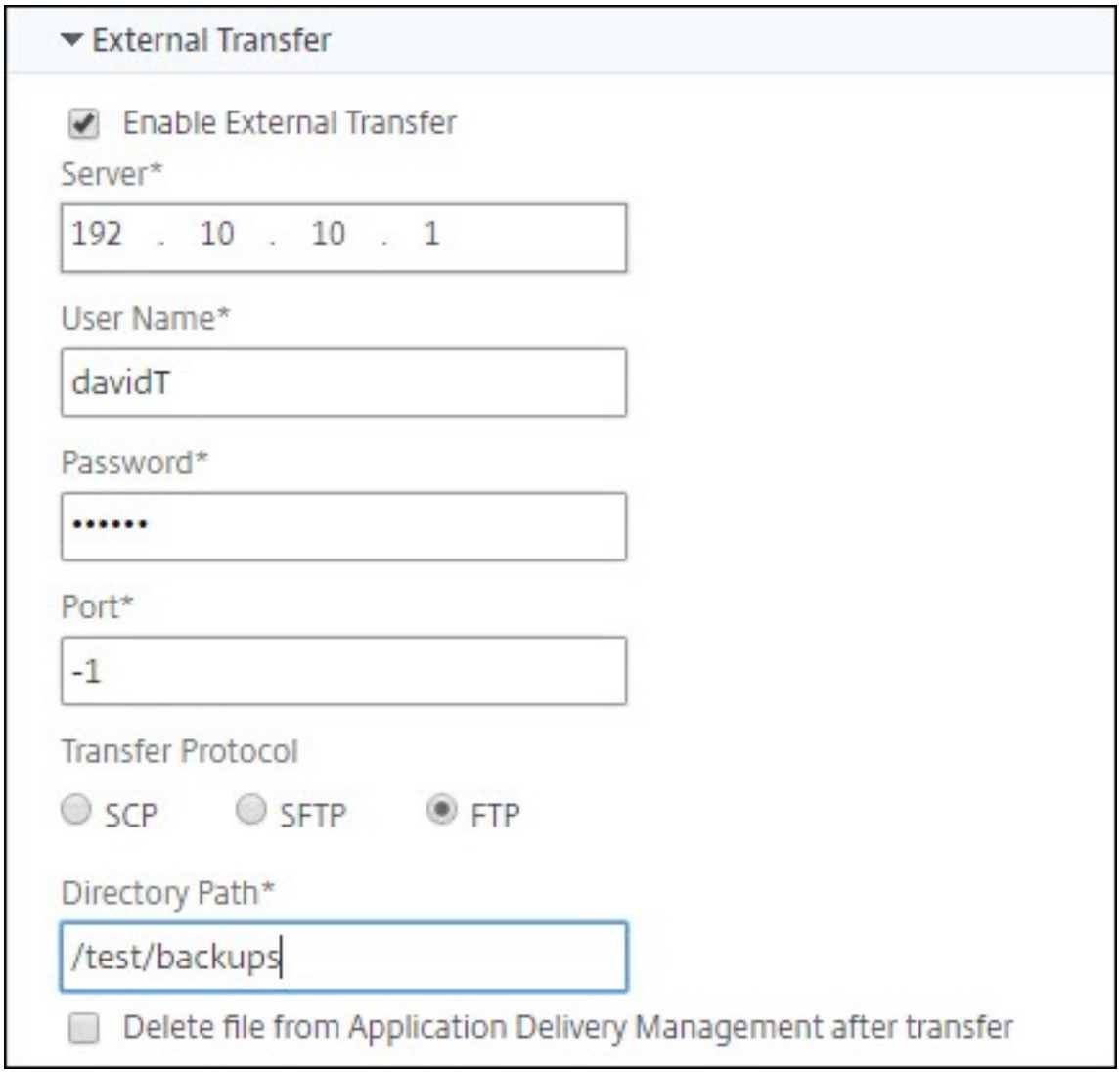
   a) Especifique la dirección IP de la ubicación.

b) Especifique el nombre de usuario y la contraseña del servidor externo al que quiere transferir los archivos de copia de seguridad.

c) Especifique el protocolo de transferencia y el número de puerto.

d) Puede especificar la ruta del directorio en el que se debe almacenar el archivo.

e) También tiene la opción de eliminar el archivo de copia de seguridad de Citrix ADM después de transferirlo al servidor externo.



Nota

Citrix ADM se envía una captura de SNMP o una notificación de Syslog cuando se produce un error de copia de seguridad en alguna de las instancias de Citrix ADC seleccionadas.

Crear una copia de seguridad para una instancia de NetScaler ADC seleccionada mediante NetScaler ADM

Realice esta tarea si quiere realizar una copia de seguridad de una instancia de NetScaler ADC seleccionada o de varias instancias:

1. En Citrix ADM, vaya a **Redes** > **Instancias**. En**Instancias**, seleccione el tipo de instancias (por ejemplo, Citrix VPX) que quiere mostrar en la pantalla.
2. Seleccione la instancia de la que quiere realizar una copia de seguridad.
    - Para las instancias MPX y VPX, seleccione **Copia de seguridad o restauración** en la lista **Seleccionar acción**.
    - Para una instancia SDX, haga clic en **Copia de seguridad/restauración**.
3. En la página**Archivos de copia**de seguridad, haga clic en**Copia de**seguridad.
4. Puede especificar si desea cifrar el archivo de copia de seguridad para mayor seguridad. Puede introducir su contraseña o utilizar la contraseña global que especificó anteriormente en la página Configuración de copia de seguridad de instancias.
5. Haga clic en **Continuar**.

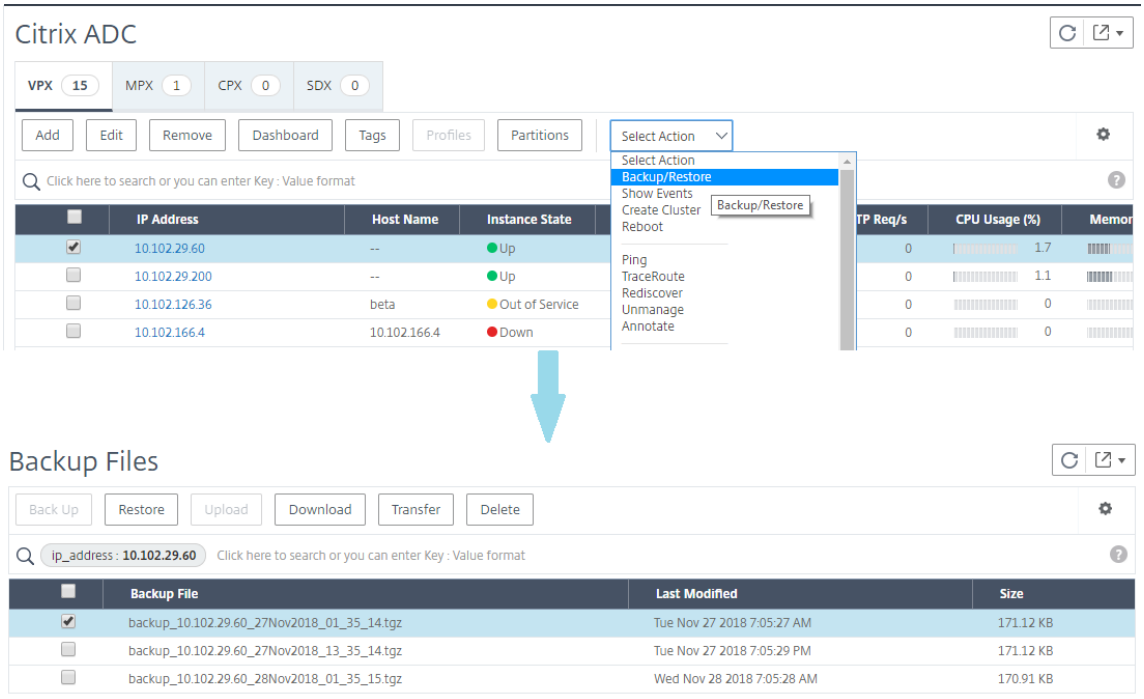
Restaurar una instancia de NetScaler ADC con NetScaler ADM

> Nota:
>
> Si tiene instancias de NetScaler ADC en un par HA, debe tener en cuenta lo siguiente:
>
> - Restaure la misma instancia desde la que se creó el archivo de copia de seguridad. Por ejemplo, consideremos un caso en el que se tomó una copia de seguridad de la instancia principal del par HA. Durante el proceso de restauración, asegúrese de restaurar la misma instancia, aunque ya no sea la instancia principal.
> - Al iniciar el proceso de restauración en la instancia de ADC principal, no puede acceder a la instancia principal y la instancia secundaria se cambia a **STAYSECONDARY**. Una vez que se completa el proceso de restauración en la instancia principal, la instancia de ADC secundaria pasa del modo **STAYSECONDARYal** modo ENABLED y vuelve a formar parte del par HA. Puede esperar un posible tiempo de inactividad en la instancia principal hasta que se complete el proceso de restauración.

Realice esta tarea para restaurar una instancia de NetScaler ADC mediante el archivo de copia de seguridad que había creado anteriormente:

1. Vaya a **Redes** > **Instancias** , seleccione la instancia que desea restaurar y, a continuación, haga clic en Ver copia de **seguridad** .

2. En la página**Archivos de copia**de seguridad, seleccione el archivo de copia de seguridad que contiene la configuración que quiere restaurar y, a continuación, haga clic en**Restaurar**.



Restaurar un dispositivo NetScaler ADC SDX con NetScaler ADM

En Citrix ADM, la copia de seguridad del dispositivo Citrix ADC SDX incluye lo siguiente:

- Instancias de NetScaler ADC alojadas en el dispositivo
- Certificados y claves SSL SVM
- Configuración de poda de instancias (en formato XML)
- Configuración de copia de seguridad de instancias (en formato XML)
- Configuración del sondeo de certificados SSL (en formato XML)
- Archivo SVM db
- Archivos de configuración NetScaler ADC de los dispositivos presentes en SDX
- Imágenes de creación de NetScaler ADC
- Imágenes de NetScaler ADC XVA, estas imágenes se almacenan en la siguiente ubicación: `/var/mps/sdx_images/`
- Imagen de paquete único de SDX (SVM+XS)
- Imágenes de instancias de terceros (si se aprovisionan)

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

Si está restaurando el dispositivo NetScaler ADC SDX mediante una copia de seguridad de otro dispositivo NetScaler ADC SDX, asegúrese de agregar las licencias y configurar la configuración de red

del servicio de administración del dispositivo para que coincida con la del archivo de copia de seguridad antes de iniciar el proceso de restauración.

Asegúrese de que la variante de la plataforma Citrix ADC SDX de la que se hizo la copia de seguridad sea la misma en la que está intentando restaurar. No se puede restaurar desde una variante de plataforma diferente.

> **Nota**
>
> Antes de restaurar un dispositivo SDX RMA, asegúrese de que la versión de la copia de seguridad sea igual o superior a la versión de RMA.

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

1. En la GUI de Citrix ADM, vaya a **Redes > Instancias > Citrix ADC** .
2. Haga clic en **Copia de seguridad/restauración**.
3. Selecciona el archivo de copia de seguridad de la misma instancia que deseas restaurar.
4. Haga clic en **Reempaquetar respaldo**.

   Cuando se realiza una copia de seguridad del dispositivo SDX, los archivos e imágenes XVA se almacenan por separado para ahorrar el ancho de banda de la red y el espacio en disco. Por lo tanto, debe volver a empaquetar el archivo de la copia de seguridad antes de restaurar el dispositivo SDX.

   Al volver a empaquetar el archivo de copia de seguridad, incluye todos los archivos de la copia de seguridad juntos para restaurar el dispositivo SDX. El archivo de copia de seguridad reempaquetado garantiza la restauración correcta del dispositivo SDX.
5. Seleccione el archivo de copia de seguridad que se ha reempaquetado y haga clic en **Restaurar**.

Forzar una conmutación por error a la instancia secundaria de NetScaler ADC

January 30, 2024

Es posible que desee forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar la instancia principal de Citrix Application Delivery Controller (ADC). Puede forzar la conmutación por error desde la instancia principal o la instancia secundaria. Cuando se fuerza una conmutación por error en la instancia principal, la instancia principal se convierte en la secundaria y la secundaria en la principal. La conmutación por error forzada solo es posible cuando la instancia principal puede determinar que la instancia secundaria está activa.

Una conmutación por error forzada no se propaga ni sincroniza. Para ver el estado de la sincronización tras una conmutación por error forzada, puede ver el estado de la instancia.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

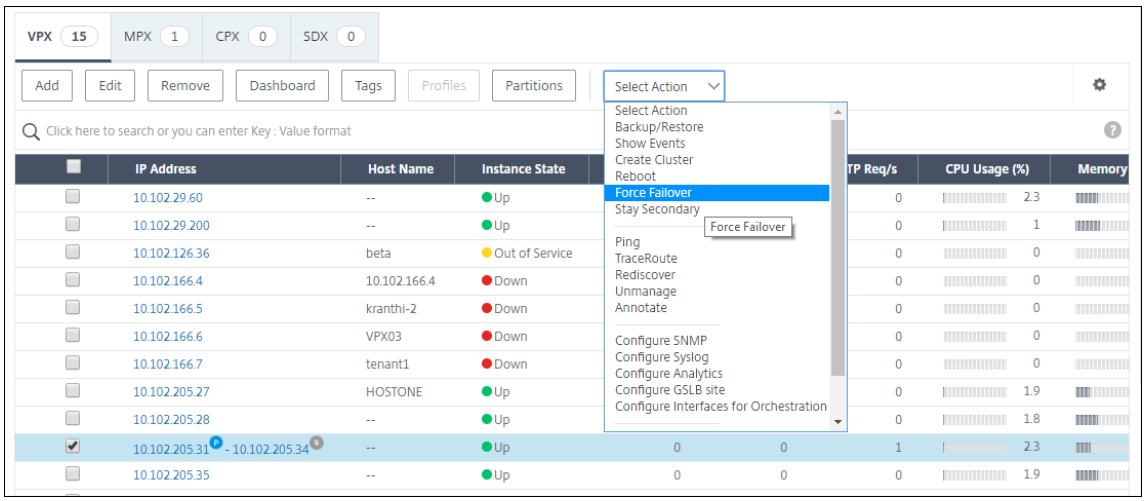
- Se fuerza la conmutación por error en un sistema independiente.
- La instancia secundaria está inhabilitada o inactiva. Si la instancia secundaria se encuentra en un estado inactivo, debe esperar a que su estado sea ACTIVO para forzar una conmutación por error.
- La instancia secundaria está configurada para permanecer secundaria.

La instancia de NetScaler ADC muestra un mensaje de advertencia si detecta un posible problema al ejecutar el comando force failover. El mensaje incluye la información que activó la advertencia y solicita confirmación antes de continuar.

Puede forzar una conmutación por error en una instancia principal o secundaria.

Para forzar una conmutación por error a la instancia secundaria de NetScaler ADC mediante NetScaler ADM:

1. En Citrix Application Delivery Management (ADM), vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** y, a continuación, seleccione una instancia.
2. Seleccione instancias en una configuración de alta disponibilidad de las instancias enumeradas en el tipo de instancia seleccionado.
3. En el menú **Acción**, selecciona Forzar **la conmutación por error.**
4. Haga clic en **Sí** para confirmar la acción de conmutación por error forzada.



Forzar una instancia secundaria de NetScaler ADC para que permanezca secundaria

January 30, 2024

En una configuración de HA, se puede obligar al nodo secundario a permanecer secundario independientemente del estado del nodo principal.

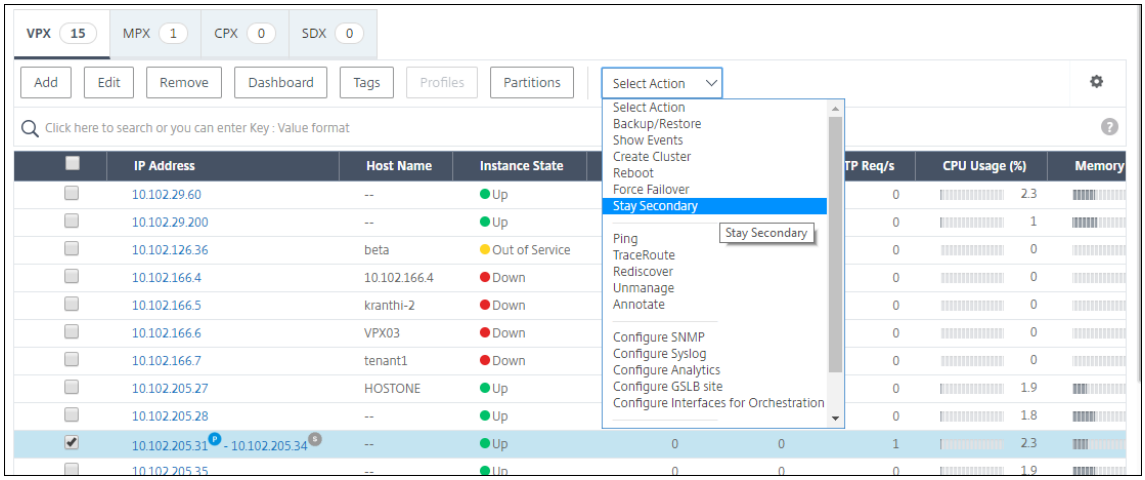
Por ejemplo, supongamos que el nodo principal necesita ser actualizado y el proceso tarda unos segundos. Durante la actualización, es posible que el nodo principal deje de funcionar durante unos segundos, pero no desea que el nodo secundario tome el control; desea que siga siendo el nodo secundario aunque detecte un error en el nodo principal.

Cuando obligas al nodo secundario a permanecer secundario, seguirá siendo secundario aunque el nodo principal deje de funcionar. Además, cuando se fuerza el estado de un nodo de un par de HA a permanecer secundario, no participa en las transiciones de la máquina de estado HA. El estado del nodo se muestra como STAYSECONDARY.

> **Nota**
>
> Cuando se fuerza a un sistema a permanecer secundario, el proceso de forzamiento no se propaga ni se sincroniza. Solo afecta al nodo en el que se ejecuta el comando.

Para configurar una instancia secundaria de NetScaler ADC para que permanezca secundaria mediante NetScaler ADM:

1. En Citrix Application Delivery Management (ADM), vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** y, a continuación, seleccione una instancia.
2. Seleccione instancias en una configuración de alta disponibilidad de las instancias enumeradas en el tipo de instancia seleccionado.
3. En el menú **Acción**, seleccione **Permanecer secundario**.
4. Haga clic en **Sí** para confirmar la ejecución de la acción "Permanecer secundario".



Crear grupos de instancias

January 30, 2024

Para crear un grupo de instancias, primero debes agregar todas las instancias de Citrix Application Delivery Controller (ADC) a Citrix Application Delivery Management (ADM). Una vez que hayas agregado las instancias correctamente, crea grupos de instancias en función de su familia de dispositivos. Al crear un grupo de instancias, puedes realizar simultáneamente acciones como la actualización, la copia de seguridad y la restauración en todas las instancias que se han agrupado, en lugar de realizarlas en cada instancia por separado.

Para crear un grupo de instancias con Citrix ADM:

1. En NetScaler ADM, vaya a **Redes** > **Grupos de instancias** y, a continuación, haga clic en **Agregar**.
2. Da un nombre a tu grupo de instancias y selecciona la familia de instancias de la lista.
3. Seleccione el tipo de instancia en el menú **Familia** de instancias .
4. Haga clic en **Seleccionar instancias** y seleccione las instancias en la ventana que se abre.
5. Haga clic en **Crear**.

Redescubrir varias instancias de Citrix VPX

January 30, 2024

Ahora puede volver a detectar varias instancias de Citrix VPX en la configuración de Citrix Application Delivery Management (ADM). Anteriormente, solo podía redescubrir instancias individuales de Citrix

VPX. Puede volver a descubrir varias instancias de Citrix VPX cuando quiera ver los estados y configuraciones más recientes de esas instancias. El servidor NetScaler ADM vuelve a descubrir todas las instancias de Citrix VPX y comprueba si se puede acceder a las instancias de Citrix Application Delivery Controller (ADC).

Para redescubrir varias instancias de Citrix VPX:

1. En un explorador web, escriba la dirección IP del servidor Citrix ADM (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador. Las credenciales de administrador predeterminadas son nsroot y nsroot.
3. Vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** y seleccione las instancias que quiere volver a detectar.
4. En el menú **Seleccionar acción**, haga clic en **Redescubrir**.
5. Cuando aparezca el mensaje de confirmación para ejecutar la utilidad Redetección, haga clic en **Sí**.

   La pantalla informa del progreso de la redetección de cada una de las instancias de Citrix VPX.

Desadministrar una instancia

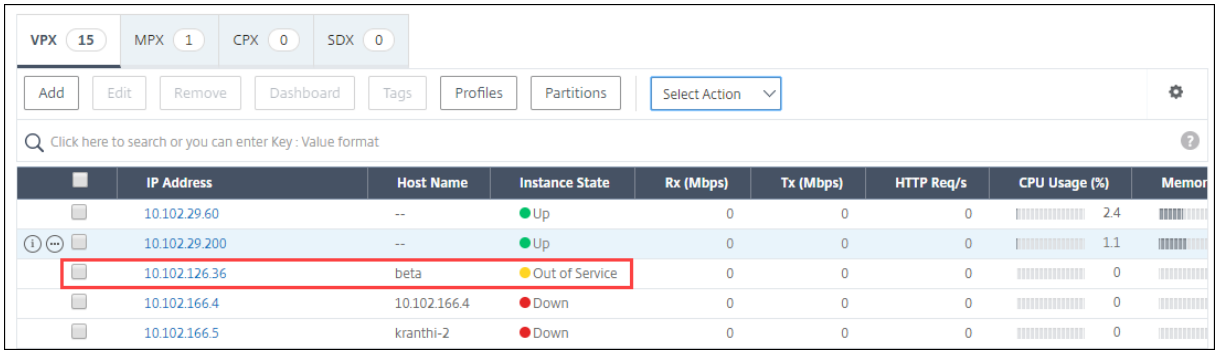
January 30, 2024

Si quiere detener el intercambio de información entre Citrix Application Delivery Management (ADM) y las instancias de la red, puede desadministrar las instancias.

Para anular la gestión de una instancia:

Vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** . En la lista de instancias, haga clic con el botón derecho en una instancia y, a continuación, seleccione **Desadministrar**, o seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Desadministrar**.

El estado de la instancia seleccionada cambia a **Fuera de servicio** como se muestra en la siguiente ilustración.



NetScaler ADM ya no administra la instancia y ya no intercambia datos con NetScaler ADM.

Rastrear la ruta a una instancia

January 30, 2024

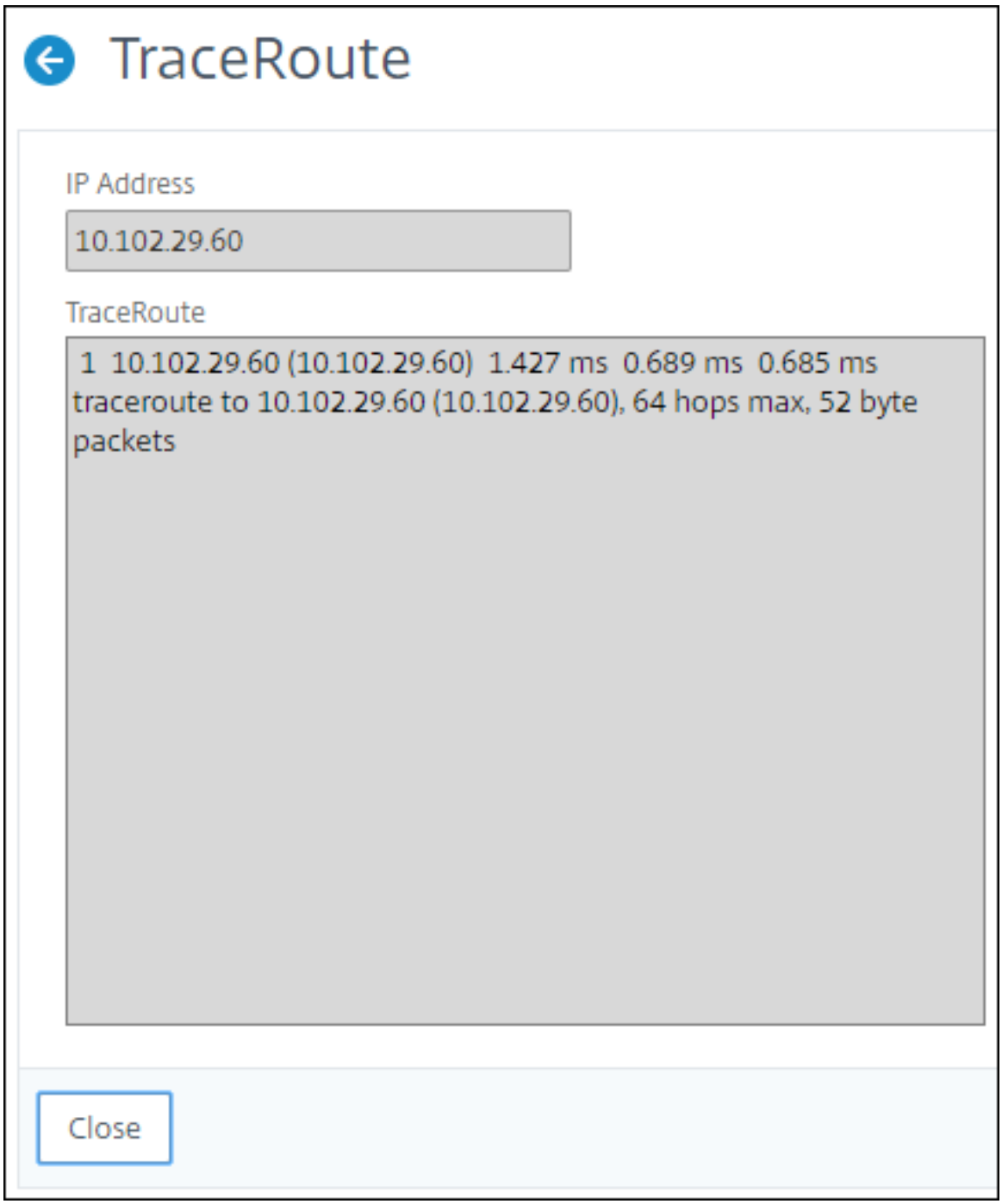
Al rastrear la ruta de un paquete desde Citrix Application Delivery Management (ADM) hasta una instancia, puede encontrar información como la cantidad de saltos necesarios para llegar a la instancia. Traceroute traza la ruta del paquete desde el origen hasta el destino. Muestra la lista de saltos de red junto con el nombre de host y la dirección IP de cada entidad en la ruta.

Traceroute también registra el tiempo que tarda un paquete en viajar de un salto a otro. Si hay alguna interrupción en la transferencia de paquetes, traceroute muestra dónde existe el problema.

Para rastrear la ruta de una instancia:

1. En Citrix ADM, vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX**.
2. En la lista de instancias, haga clic con el botón derecho en una instancia y, a continuación, seleccione **TraceRoute** o seleccione la instancia y, en el menú **Seleccionar acción**, haga clic en **TraceRoute**.

El cuadro de mensaje TraceRoute muestra la ruta a la instancia y la cantidad de tiempo, en milisegundos, consumida por cada salto.



Eventos

January 30, 2024

Cuando la dirección IP de una instancia de Citrix Application Delivery Controller (ADC) se agrega a

NetScaler Application Delivery Management (ADM), NetScaler ADM envía una llamada NITRO y se agrega implícitamente como destino de captura para que la instancia reciba sus capturas o eventos.

Los eventos representan ocurrencias de eventos o errores en una instancia de Citrix ADC administrada. Por ejemplo, cuando hay un error en el sistema o un cambio en la configuración, se genera un evento y se registra en el servidor NetScaler ADM. Los eventos recibidos en NetScaler ADM se muestran en la página Resumen de eventos (**Redes** > **Eventos**) y todos los eventos activos se muestran en la página Mensajes de eventos (**Redes** > **Eventos** > **Mensajes de eventos**).

Citrix ADM también comprueba los eventos generados en las instancias para formar alarmas de diferentes niveles de gravedad y las muestra como mensajes, algunos de los cuales pueden requerir atención inmediata. Por ejemplo, una falla del sistema podría clasificarse como una gravedad de evento «crítica» y tendría que abordarse de inmediato.

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de una gran cantidad de eventos generados en la infraestructura de Citrix ADC.

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

También puede asegurarse de que se activan varias notificaciones para un intervalo de tiempo específico para un evento hasta que se borre el evento. Como medida adicional, puede personalizar su correo electrónico con una línea de asunto específica, un mensaje de usuario y cargar un archivo adjunto.

Usar panel de eventos

January 30, 2024

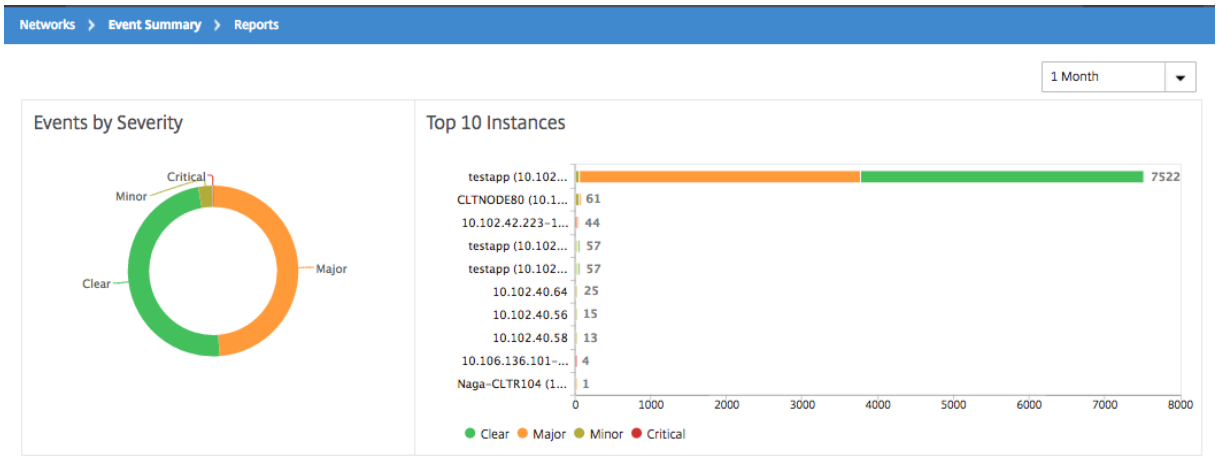
Como administrador de red, puede ver detalles como los cambios de configuración, las condiciones de inicio de sesión, los errores de hardware, las infracciones de los umbrales y los cambios en el estado de la entidad en sus instancias de Citrix Application Delivery Controller (ADC), junto con los eventos y su gravedad en instancias específicas. Puede utilizar el panel de eventos de NetScaler Application Delivery Management (ADM) para ver los informes generados con detalles sobre la gravedad de los eventos críticos en todas sus instancias de NetScaler ADC.

Para ver los detalles en el panel de eventos:

Vaya a **Redes** > **Eventos** > **Informes** .

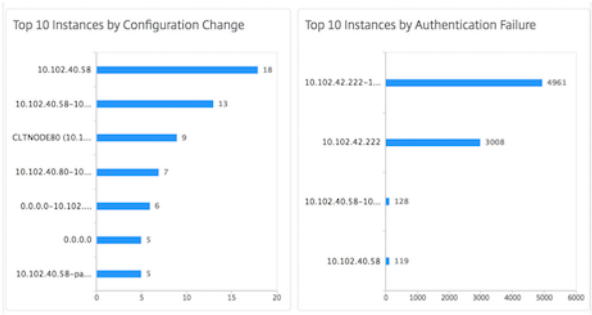
El gráfico 10 dispositivos principales del panel muestra un informe de las 10 instancias principales

según el número de eventos generados en ellas. Puede hacer clic en una instancia del gráfico para ver más detalles sobre la gravedad del evento.

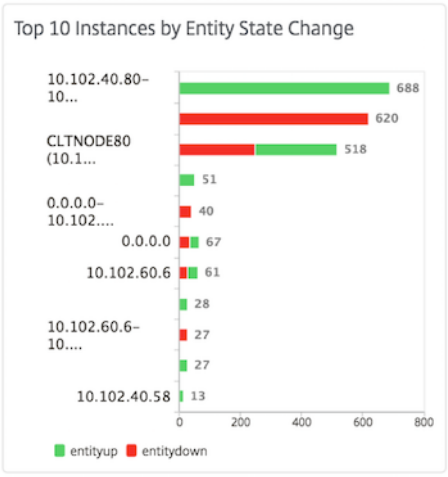


Para ver más detalles, vaya al tipo de instancia de Citrix ADC (**Redes** > **Eventos** > **Informes** > **NetScaler/ NetScaler SDX/ NetScaler SD-WAN WO**) para ver lo siguiente:

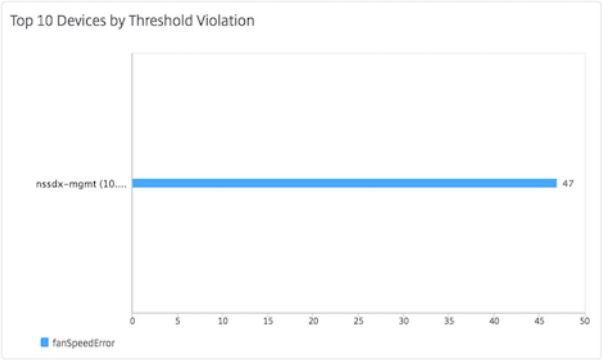
- Los 10 dispositivos principales por fallo de hardware
- Los 10 dispositivos principales por cambio de configuración
- Los 10 dispositivos principales por error de autenticación



- Los 10 principales dispositivos por cambios de estado de entidad



- Los 10 dispositivos principales por infracción de umbral



Establecer la edad del evento para los eventos

January 30, 2024

Puede configurar la opción de antigüedad del evento para especificar el intervalo de tiempo (en segundos). NetScaler ADM supervisa los dispositivos hasta la duración establecida y genera un evento solo si la antigüedad del evento supera la duración establecida.

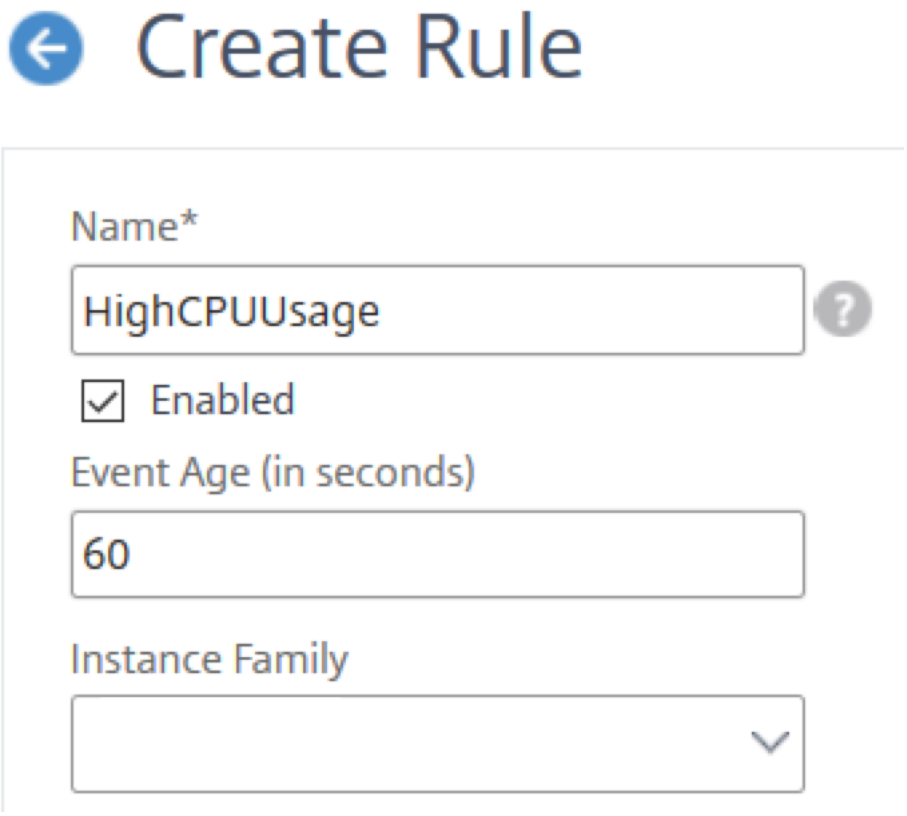
> Nota:
>
> El valor mínimo para la antigüedad del evento es de 60 segundos. Si mantiene el campo **Edad del evento** en blanco, la regla de evento se aplica inmediatamente después de que se produzca el evento.

Por ejemplo, considere que quiere administrar varios dispositivos ADC y recibir una notificación por correo electrónico cuando alguno de sus servidores virtuales deje de funcionar durante 60 segundos o más. Puede crear una regla de evento con los filtros necesarios y establecer la edad del evento

de la regla en 60 segundos. Luego, cada vez que un servidor virtual permanezca inactivo durante 60 segundos o más, recibirá una notificación por correo electrónico con detalles como el nombre de la entidad, el cambio de estado y la hora.

Para establecer la edad del evento en NetScaler ADM:

1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar**.
2. En la página **Crear regla**, establezca los parámetros de regla.
3. Especifique la edad del evento en segundos.



Asegúrate de configurar todas las trampas relacionadas entre sí en la sección **Categoría** y también establece la gravedad correspondiente en la sección **Gravedad** cuando establezcas la antigüedad del evento. En el ejemplo anterior, seleccione las trampas entityup, entitydown y entityofs.

Programar un filtro de eventos

January 30, 2024

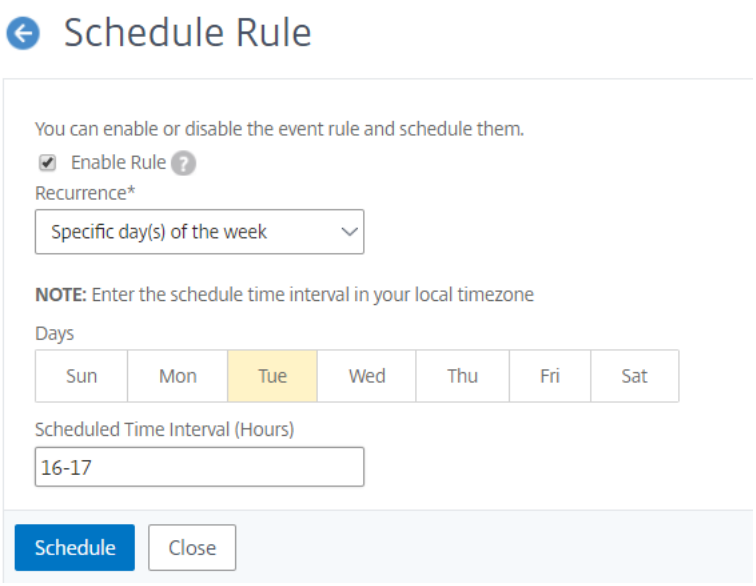
Después de crear un filtro para la regla, si no desea que el servidor Citrix Application Delivery Management (ADM) envíe una notificación cada vez que el evento generado cumpla los criterios de filtro, puede programar el filtro para que se active solo en intervalos de tiempo específicos, por ejemplo, de forma diaria, semanal o mensual.

Por ejemplo, si ha programado una actividad de mantenimiento del sistema para diferentes aplicaciones en las instancias en diferentes momentos, las instancias pueden generar varias alarmas.

Si ha configurado un filtro para estas alarmas y ha habilitado las notificaciones por correo electrónico para estos filtros, el servidor envía un gran número de notificaciones por correo electrónico cuando Citrix ADM recibe estas trampas. Si quiere que el servidor envíe estas notificaciones por correo electrónico únicamente durante un período de tiempo específico, puede hacerlo programando un filtro.

Para programar un filtro con NetScaler ADM:

1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Reglas** .
2. Seleccione la regla para la que quiere programar un filtro y haga clic en **Ver planificación**.
3. En la página **Regla programada**, haga clic en **Programar** y especifique los siguientes parámetros:
    - **Habilitar regla**: seleccione esta casilla para habilitar la regla de eventos programados.
    - **Periodicidad**: Intervalo en el que se planifica la regla. Seleccione un día específico de la semana o una fecha específica de un mes.
    - **Días**: seleccione el día de la semana para ejecutar la regla. Puede seleccionar varios días.
    - **Fechas**: Escriba las fechas. Puede escribir varias fechas como valores separados por comas.
    - **Intervalo de tiempo programado (horas)**: hora (s) en la que programar la regla (utilice el formato de 24 horas).
4. Haga clic en **Programar**.



Establecer notificaciones de correo electrónico repetidas para eventos

January 30, 2024

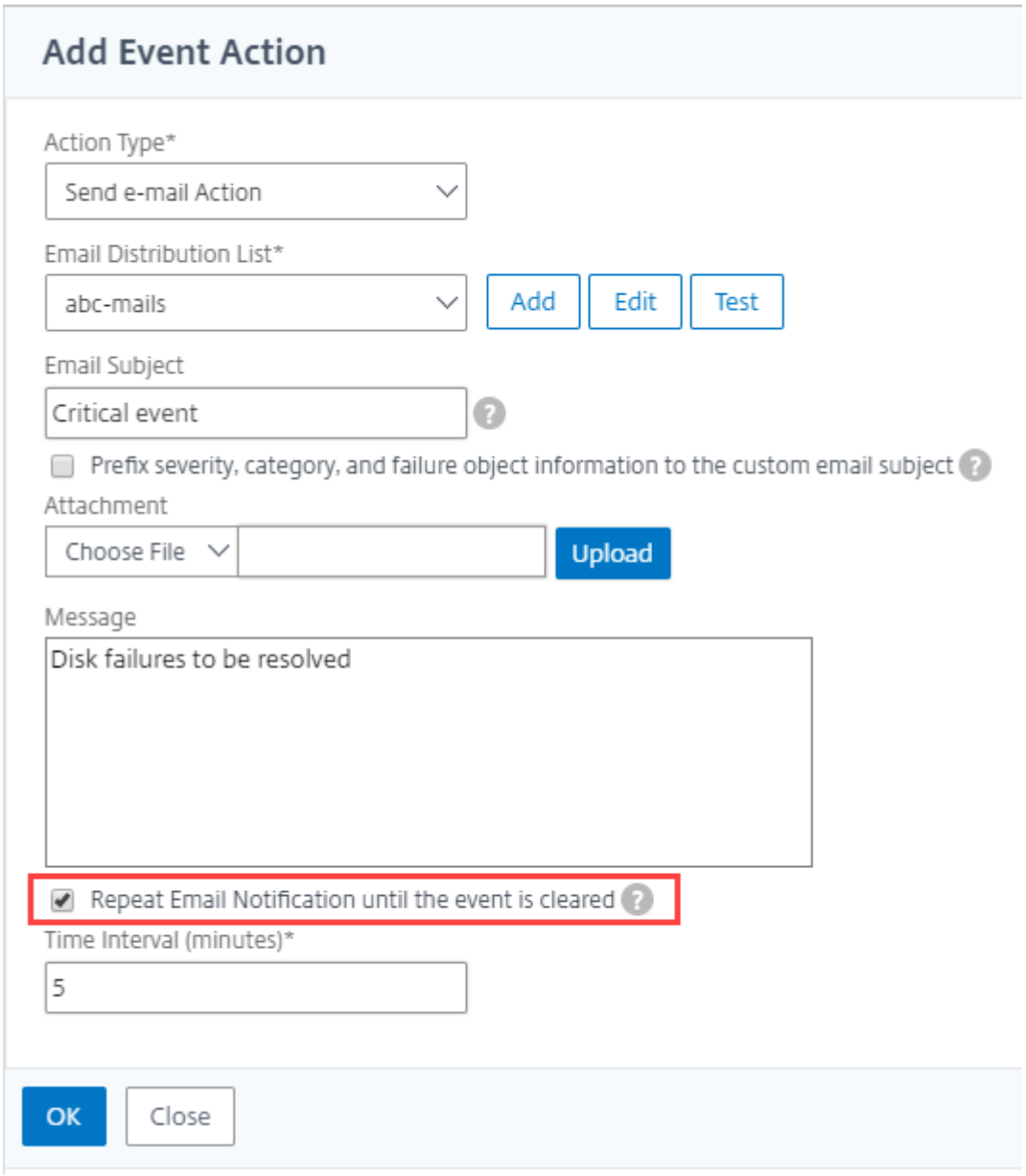
Para garantizar que se aborden todos los eventos críticos y no se omita ninguna notificación importante por correo electrónico, puede optar por enviar notificaciones por correo electrónico repetidas para las reglas de eventos que cumplan con los criterios que has seleccionado. Por ejemplo, si ha creado una regla de evento para las instancias que implican errores de disco y quiere recibir una notificación hasta que se resuelva el problema, puede optar por recibir notificaciones por correo electrónico repetidas sobre esos eventos.

Estas notificaciones por correo electrónico se envían repetidamente, a intervalos predefinidos, hasta que el destinatario reconoce haber visto la notificación o se borra la regla de evento.

> **Nota**
>
> Los eventos solo se pueden borrar automáticamente si hay una trampa "clara"equivalente establecida y enviada desde su instancia de Citrix Application Delivery Controller (ADC).
>
> Para borrar un evento manualmente, puede hacer lo siguiente:
>
> - Vaya a **Redes > Eventos > Resumen del evento** , elija una **categoría** , seleccione un evento de la categoría y haga clic **en**Borrar .
> - O bien, vaya a **Redes > Eventos > Mensajes de eventos**. Elija un tipo de instancia y, a continuación, seleccione un evento de la siguiente cuadrícula y haga clic en **Borrar**.

Para configurar notificaciones de correo electrónico repetidas desde NetScaler ADM:

1. En Citrix Application Delivery Management (ADM), vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar** para crear una regla.
2. En la página **Crear regla**, establezca los parámetros de regla.
3. En Acciones de **reglas de eventos** , haga clic en **Agregar acción** . A continuación, seleccione **Enviar acción de correo electrónico** en la lista desplegable **Tipo de acción** y seleccione una lista de **distribución de correo electrónico**.
4. También puede agregar una línea de asunto personalizada y un mensaje de usuario, y cargar un archivo adjunto al correo electrónico cuando un evento entrante coincida con la regla configurada.
5. Active la casilla de verificación **Repetir notificación por correo electrónico hasta que se desactive el evento**.



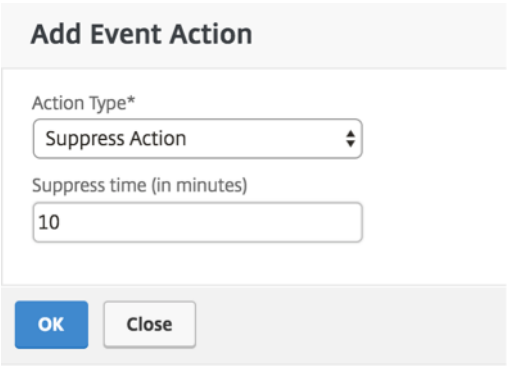
Suprimir eventos

January 30, 2024

Al elegir la acción **Suprimir** evento de acción, puede configurar un período de tiempo, en minutos, durante el cual se suprime o descarta un evento. Puede suprimir el evento durante un mínimo de 1 minuto.

Para suprimir eventos mediante NetScaler ADM:

1. En Citrix Application Delivery Management (ADM), vaya a **Redes** > **Eventos** > **Reglas** . Haga clic en **Agregar**.
2. Especifique todos los parámetros necesarios para crear una regla.
3. En **Acciones de regla de evento**, haga clic en **Agregar acción** para asignar acciones de notificación al evento.
4. En la página **Agregar acción de evento** , seleccione **Suprimir acción** en el menú desplegable **Tipo** de acción y especifique el período de tiempo, en minutos, durante el que se debe suprimir un evento.
5. Haga clic en **Aceptar**.



Crear reglas de eventos

January 30, 2024

24 de mayo de 2018

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de una gran cantidad de eventos generados en la infraestructura de Citrix Application Delivery Controller (ADC).

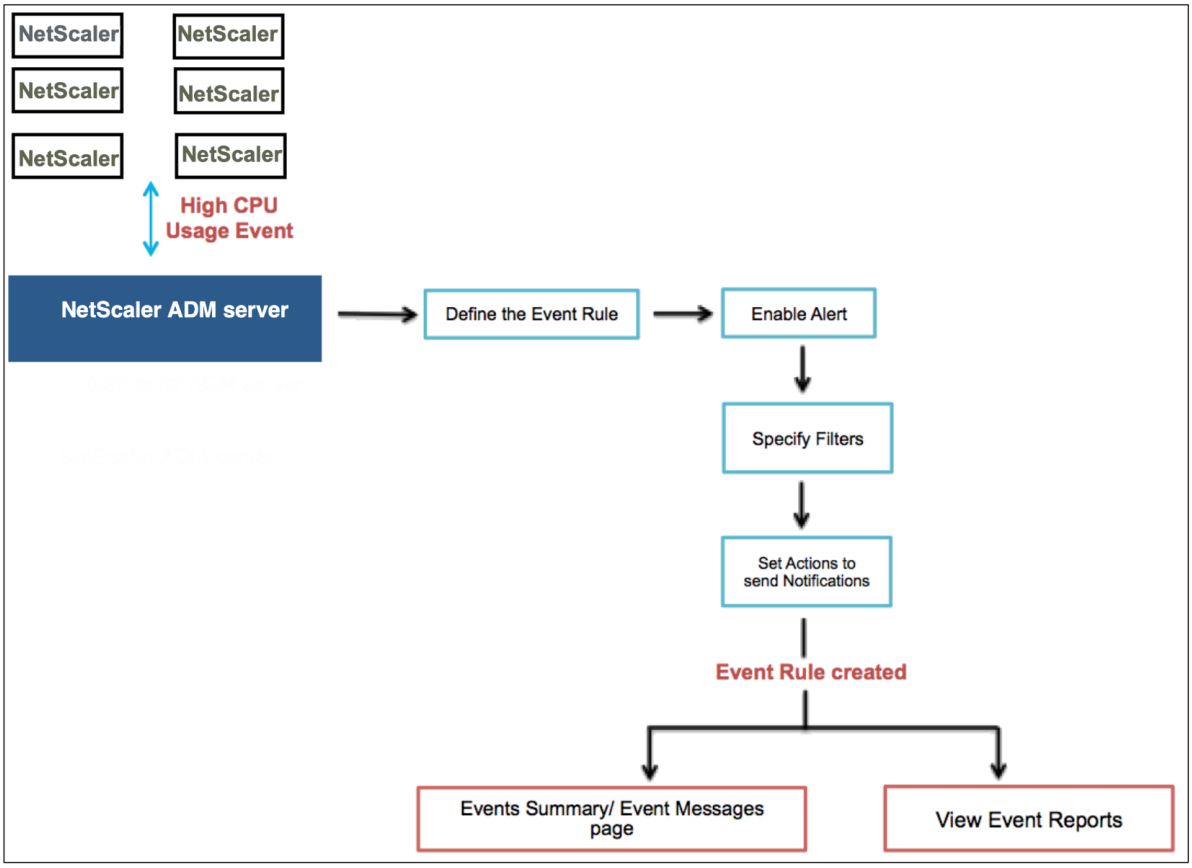
Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen con los criterios de filtro de la regla, se ejecuta la acción asociada a la regla. Las condiciones para las que puede crear filtros son: Gravedad,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

Puede asignar las siguientes acciones a los eventos:

- **Acción de envío de correo electrónico**: Enviar un correo electrónico para los eventos que coinciden con los criterios de filtrado.
- **Enviar acción de captura**: Enviar o reenviar capturas SNMP a un destino de captura externo

- **Acción**de envío de SMS : envía un mensaje de servicio de mensajes cortos (SMS) para cada evento que coincida con los criterios del filtro.
- **Ejecutar acción de comando**: Ejecute un comando cuando un evento entrante cumpla con la regla configurada.
- **Ejecutar acción**de trabajo : ejecutar un trabajo es para eventos que coinciden con los criterios de filtro que ha especificado.
- **Suprimir acción**: Suprime la eliminación de un evento durante un período de tiempo específico.

También puede hacer que las notificaciones se reenvíen en un intervalo especificado hasta que se borre un evento. Además, puede personalizar el correo electrónico con un asunto, un mensaje de usuario o un archivo adjunto específicos.



Por ejemplo, como administrador, es posible que quiera supervisar los eventos de "alto uso de CPU" para instancias específicas de NetScaler ADC si esos eventos pudieran provocar una interrupción de las instancias de NetScaler ADC. Puedes crear una regla para supervisar las instancias y especificar una acción que te envíe una notificación por correo electrónico cuando se produzca un evento de la categoría «uso elevado de la CPU». Puede programar la regla para que se ejecute a una hora específica, por ejemplo, entre las 11 de la mañana y las 11 de la noche, de modo que no se le notifique cada vez

que se genere un evento.

La configuración de una regla de evento implica las siguientes tareas:

1. Defina la regla
2. Elija la gravedad del evento que detecta la regla
3. Especifica la categoría del evento
4. Especificar instancias NetScaler ADC a las que se aplica la regla
5. Especificar objetos de error
6. Especifique cualquier filtro adicional
7. Especificar las acciones que se deben realizar cuando la regla detecta un evento

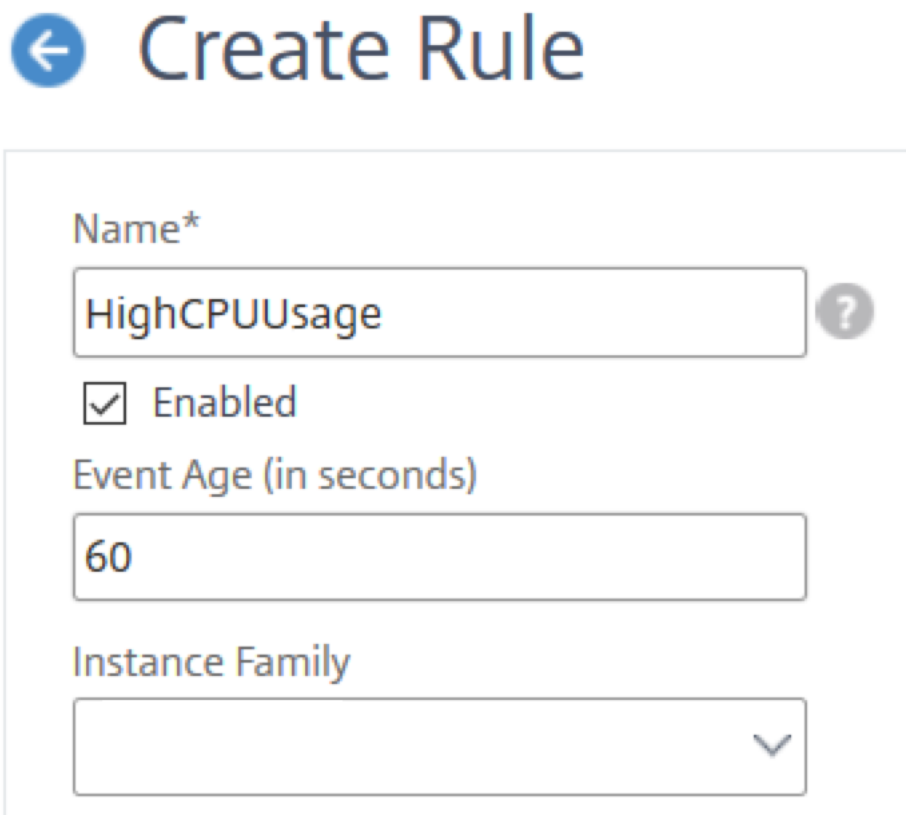
Paso 1: Definir una regla de evento

Vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar** . Si quiere habilitar la regla, active la casilla de verificación **Habilitar regla**.

Puede configurar la opción **Event Age** para especificar el intervalo de tiempo (en segundos) tras el cual Citrix Application Delivery Management (ADM) actualiza una regla de evento.

> Nota:
>
> El valor mínimo para la antigüedad del evento es de 60 segundos. Si mantiene el campo **Edad del evento** en blanco, la regla de evento se aplica inmediatamente después de que se produzca el evento.

Según el ejemplo anterior, es posible que desee recibir una notificación por correo electrónico cada vez que su instancia de Citrix ADC tenga un evento de «uso elevado de CPU» durante un período de 60 segundos o más. Puede establecer la antigüedad del evento en 60 segundos, de modo que cada vez que su instancia de Citrix ADC tenga un evento de «uso elevado de CPU» durante 60 segundos o más, recibirá una notificación por correo electrónico con los detalles del evento.

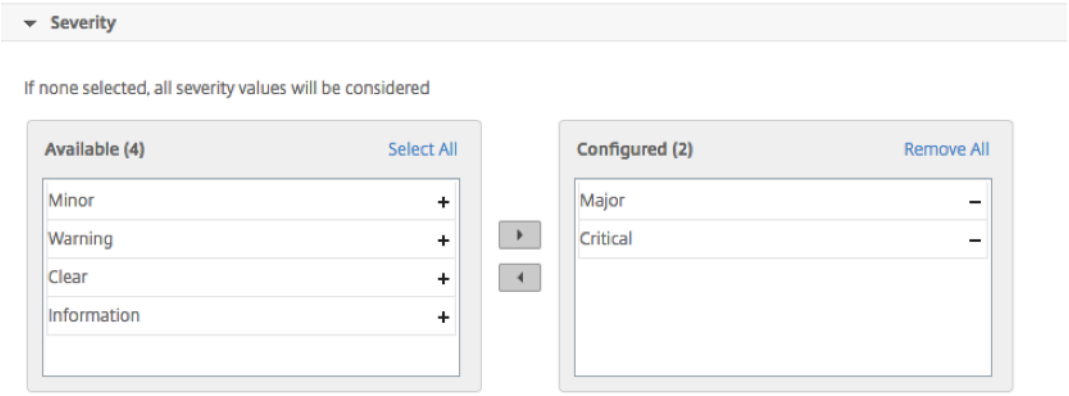


También puede filtrar las reglas de eventos por **familia de dispositivos** para rastrear la instancia de Citrix ADC desde la que Citrix ADM recibe un evento.

Paso 2: Elige la gravedad del evento

Puede crear reglas de evento que utilicen la configuración de gravedad predeterminada. La gravedad especifica la gravedad actual de los eventos a los que quiere agregar la regla de eventos.

Puede definir los siguientes niveles de gravedad: Crítico, Mayor, Menor, Advertencia, Borrar e Información.

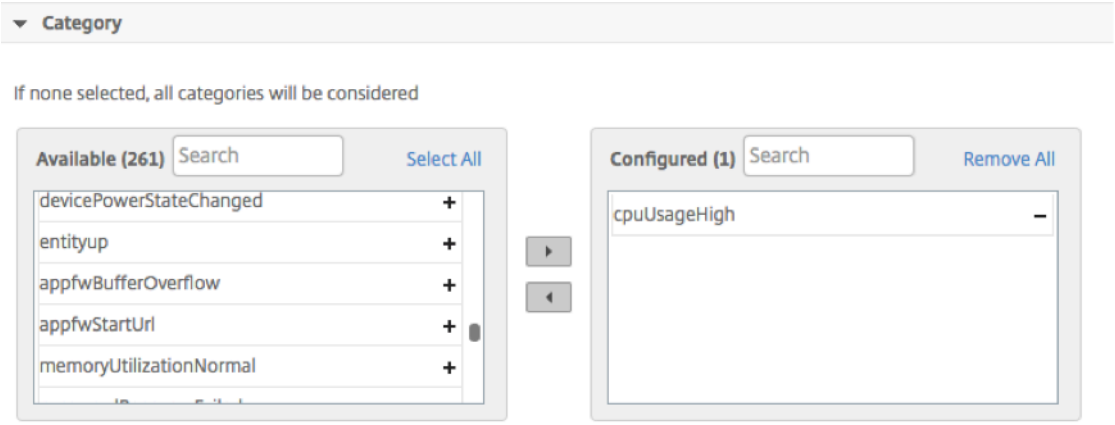


> **Nota**
>
> Puede configurar la gravedad para eventos genéricos y específicos de la empresa. Para modificar la gravedad de los eventos de las instancias NetScaler ADC administradas en NetScaler ADM, vaya a **Redes** > **Eventos** > **Configuración de eventos**. Elija la **categoría** para la que quiere configurar la gravedad del evento y haga clic en **Configurar gravedad**. Asigne un nuevo nivel de gravedad y haga clic en **Aceptar**.

Paso 3: Especificar la categoría del evento

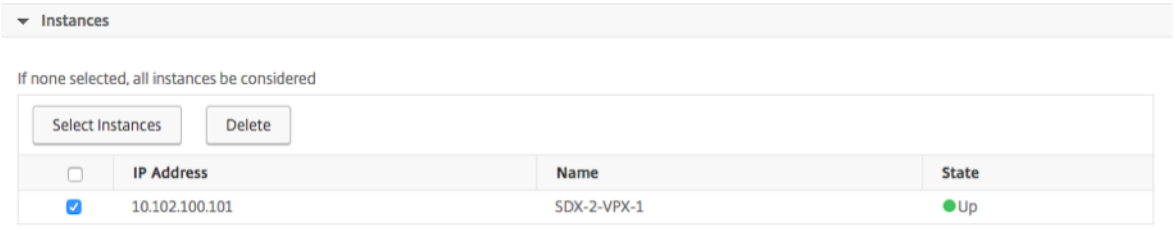
Puede especificar la categoría o las categorías de los eventos generados por las instancias NetScaler ADC. Todas las categorías se crean en instancias de NetScaler ADC. A continuación, estas categorías se mapean con NetScaler ADM, que se puede utilizar para definir reglas de eventos. Seleccione la categoría que quiera considerar y muévalo de la tabla **Disponible** a la tabla **Configurada**.

En el ejemplo anterior, tendrás que elegir "CpuUsageHigh"como categoría de eventos de la tabla que se muestra.



Paso 4: Especificar instancias de NetScaler ADC

Seleccione las direcciones IP de las instancias de NetScaler ADC para las que quiere definir la regla de eventos. En la sección **Instancias**, haga clic en **Seleccionar instancias**. En la página **Seleccionar Instancias**, elija las instancias y haga clic en **Seleccionar**.

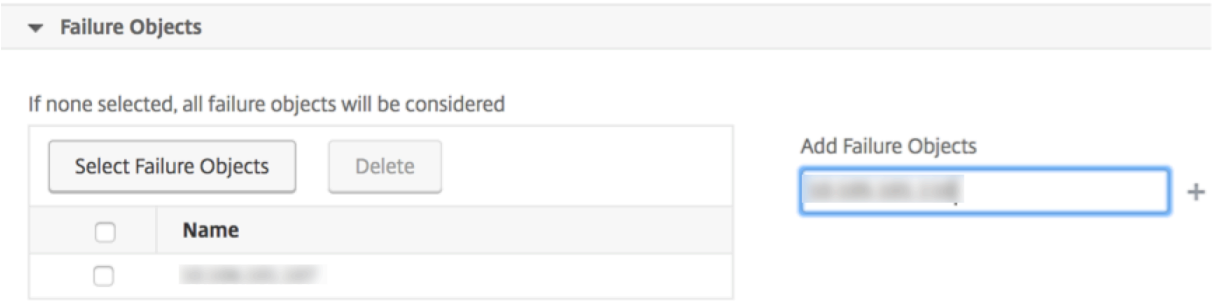


Paso 5: Seleccione objetos de error

Puede seleccionar un objeto de error de la lista desplegable proporcionada o agregar un objeto de error para el que se haya generado un evento. Los objetos de error son instancias de entidad o contadores para los que se ha generado un evento.

El objeto de error afecta a la forma en que se procesa un evento y garantiza que el objeto de error refleja el problema exacto tal como se ha notificado. Esto se puede usar para rastrear problemas rápidamente e identificar el motivo de la falla, en lugar de simplemente informar eventos sin procesar. Por ejemplo, si un usuario tiene problemas para iniciar sesión, el objeto de error aquí es el nombre de usuario o la contraseña, como «nsroot».

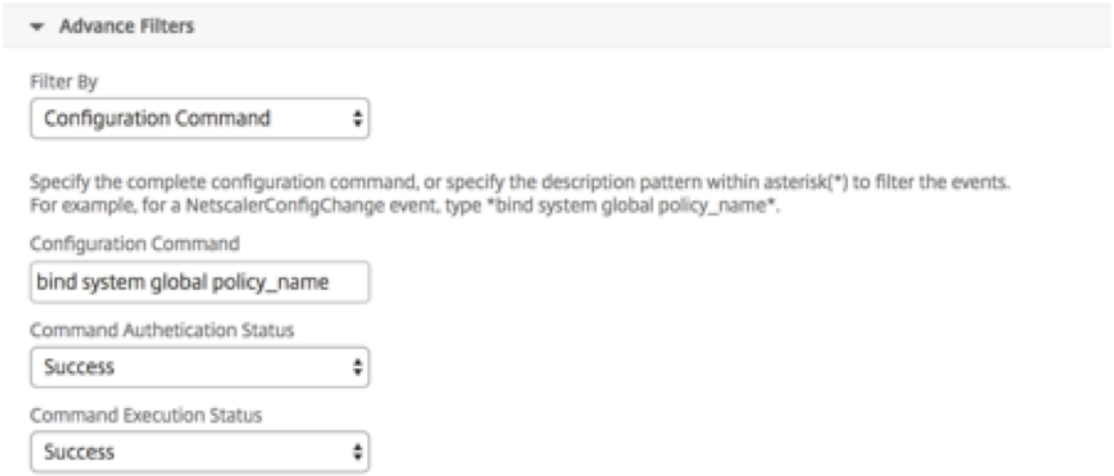
Esta lista puede contener nombres de contador para todos los eventos relacionados con umbrales, nombres de entidades para todos los eventos relacionados con entidades, nombres de certificados para eventos relacionados con certificados, etc.



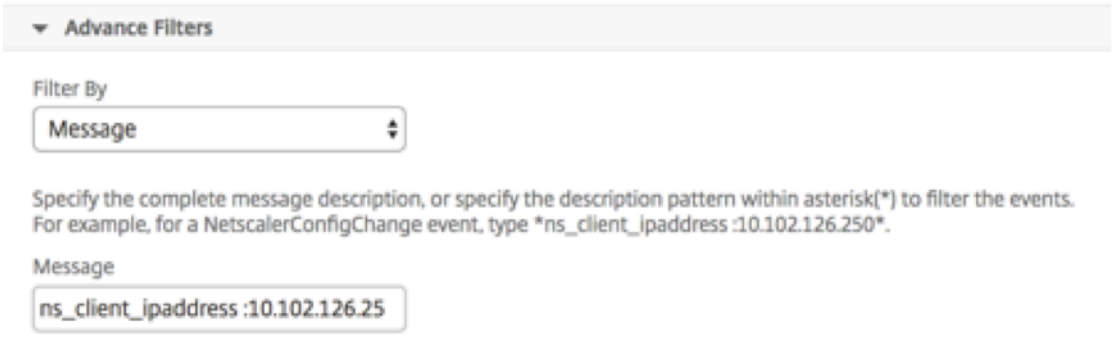
Paso 6: Especificar filtros adicionales

Puede filtrar aún más una regla de evento por:

- **Comandos de configuración**: Puede especificar el comando de configuración completo o especificar el patrón de descripción dentro del asterisco (*) para filtrar los eventos. Además del comando, puede optar por filtrar aún más la regla de eventos según el estado de autenticación del comando y/ o su estado de ejecución. Por ejemplo, para un evento NetScalerConfigChange, escriba *bind system global policy_name*.



- **Mensajes**: puede especificar la descripción completa del mensaje o especificar el patrón de descripción dentro de un asterisco (*) para filtrar los eventos.
  Por ejemplo, para un evento NetScalerConfigChange, escriba *ns_client_ipaddress:10.102.126.250*.



Paso 7: Agregar acciones de reglas de eventos

Puede agregar acciones de regla de evento para asignar acciones de notificación a un evento. Estas notificaciones se envían o realizan cuando un evento cumple con los criterios de filtro definidos anteriormente. Puede agregar las siguientes acciones de evento:

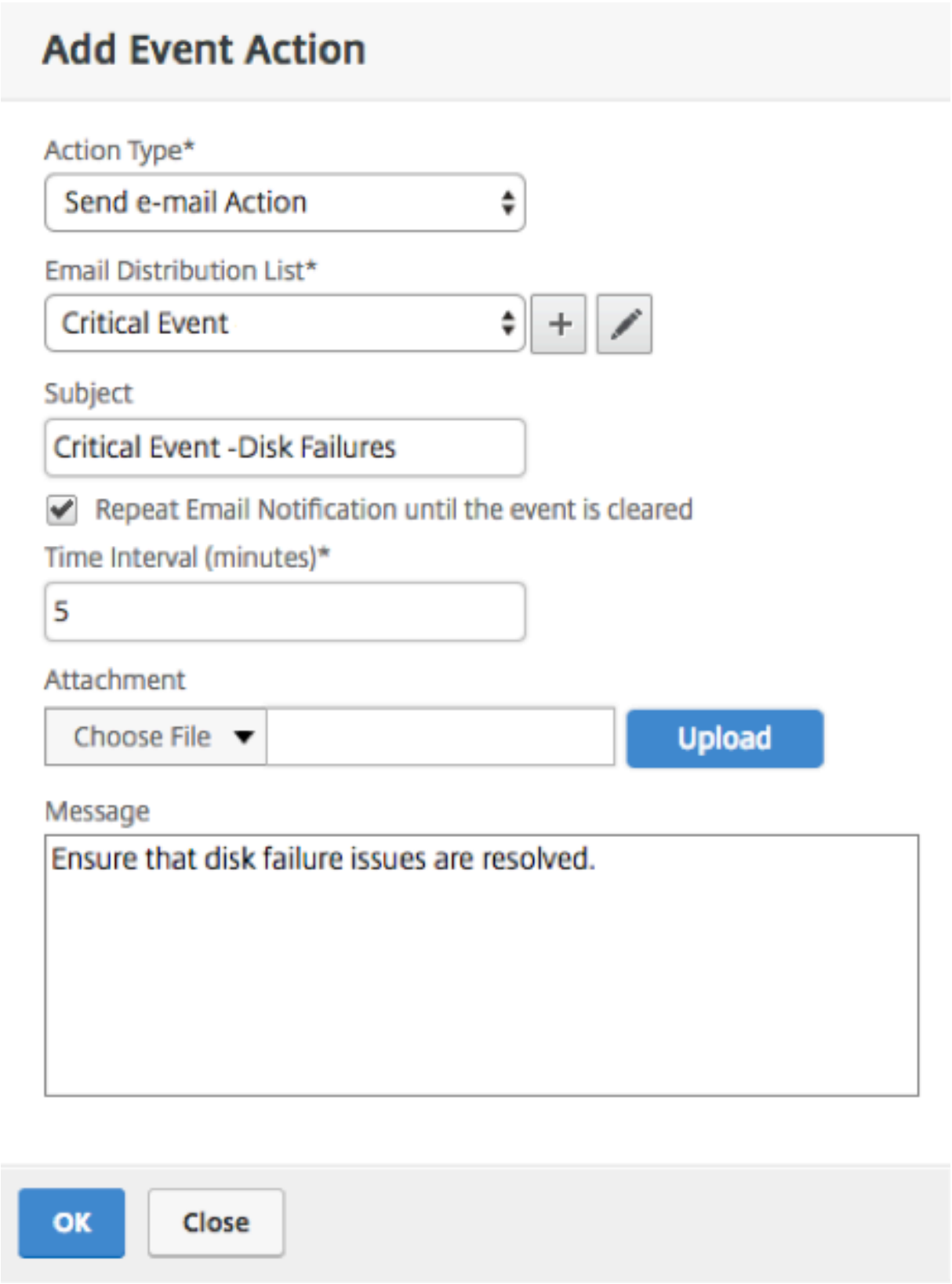
- Acción de envío de correo electrónico
- Acción de captura de envío
- Acción de envío de SMS
- Ejecutar acción de comando
- Ejecutar acción de trabajo
- Acción de supresión

Para configurar la acción de la regla de eventos de correo electrónico:

Al elegir el tipo de acción de evento Enviar correo electrónico, se activa un correo electrónico cuando los eventos cumplen los criterios de filtro definidos. Tendrá que crear una lista de distribución de correo electrónico proporcionando los detalles del servidor de correo o del perfil de correo o puede seleccionar una lista de distribución de correo electrónico que haya creado previamente.

También puede agregar una línea de asunto personalizada y un mensaje de usuario, y cargar un archivo adjunto al correo electrónico cuando un evento entrante coincida con la regla configurada.

Con esta opción, también puede asegurarse de que se abordan todos los eventos críticos y de que no se pierde ninguna notificación importante por correo electrónico, seleccionando la casilla **Repetir notificación por correo electrónico hasta que se desactive el evento** para enviar notificaciones por correo electrónico repetidas para las reglas de eventos que cumplan los criterios que ha seleccionado. Por ejemplo, si ha creado una regla de evento para las instancias que implican errores de disco y quiere recibir una notificación hasta que se resuelva el problema, puede optar por recibir notificaciones por correo electrónico repetidas sobre esos eventos.



Para configurar la acción Trap Event Rule:

Al elegir el tipo de **acción de evento Enviar acción de captura**, las capturas SNMP se envían o reenvían a un destino de captura externo. Al definir una lista de distribución de trampas (o un destino de captura y detalles del perfil de captura), los mensajes de captura se envían a un receptor de captura específico cuando los eventos cumplen con los criterios de filtro definidos.

Para configurar la acción de la regla de eventos de SMS:

Al elegir el tipo de acción de evento **Enviar acción SMS** , aparece un **mensaje del servicio de mensajes cortos** (SMS) para cada evento que coincida con los criterios del filtro. Tendrá que crear una lista de distribución de SMS proporcionando los detalles del servidor de SMS o del perfil de SMS o puede seleccionar una lista de distribución de SMS que haya creado anteriormente.

Para configurar la acción Ejecutar comando:

Al elegir la acción de evento **Ejecutar acción de comando**, puede crear un comando o una script que se pueda ejecutar en NetScaler ADM para eventos que coincidan con un criterio de filtro determinado. Por ejemplo, si se produce un evento de gravedad «crítica» cuando hay un cambio de configuración en una instancia gestionada, puedes ejecutar un script de comandos.

También puede establecer los siguientes parámetros para el script **Run Command Action** :

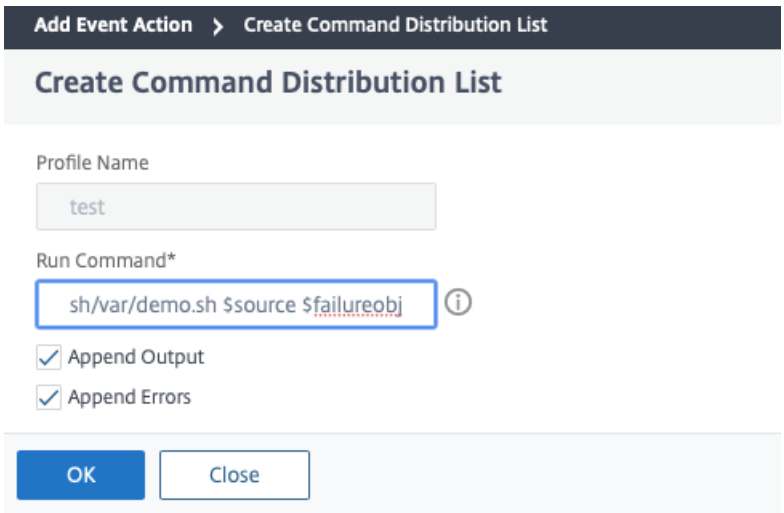
Parámetro	Descripción
$fuente	Este parámetro corresponde a la dirección IP de origen del evento recibido.
$categoría	Este parámetro corresponde al tipo de trampas definido en la categoría del filtro
$entidad	Este parámetro corresponde a las instancias o contadores de entidades para los que se ha generado un evento. Puede incluir los nombres de los contadores de todos los eventos relacionados con el umbral, los nombres de las entidades de todos los eventos relacionados con la entidad y los nombres de los certificados de todos los eventos relacionados con los certificados.
$gravedad	Este parámetro corresponde a la gravedad del evento.

$failure.obj	El objeto de error afecta a la forma en que se procesa un evento y garantiza que el objeto de error refleja el problema exacto tal como se ha notificado. Esto se puede usar para rastrear problemas rápidamente e identificar el motivo de la falla, en lugar de simplemente informar eventos sin procesar.

> **Nota**
>
> Durante la ejecución del comando, estos parámetros se reemplazarán por valores reales.

Para configurar la acción del evento «Run Command Action» en Citrix ADM:

1. En **Acciones de reglas de eventos** , haga clic en **Agregar acción** y seleccione Ejecutar **acción de comando** en el menú desplegable **Tipo** de acción .
2. En la página **Crear lista de distribución** de comandos , especifique un nombre de perfil y el comando que se va a ejecutar. Este comando se ejecutará cuando los eventos cumplan con los criterios de filtro definidos.

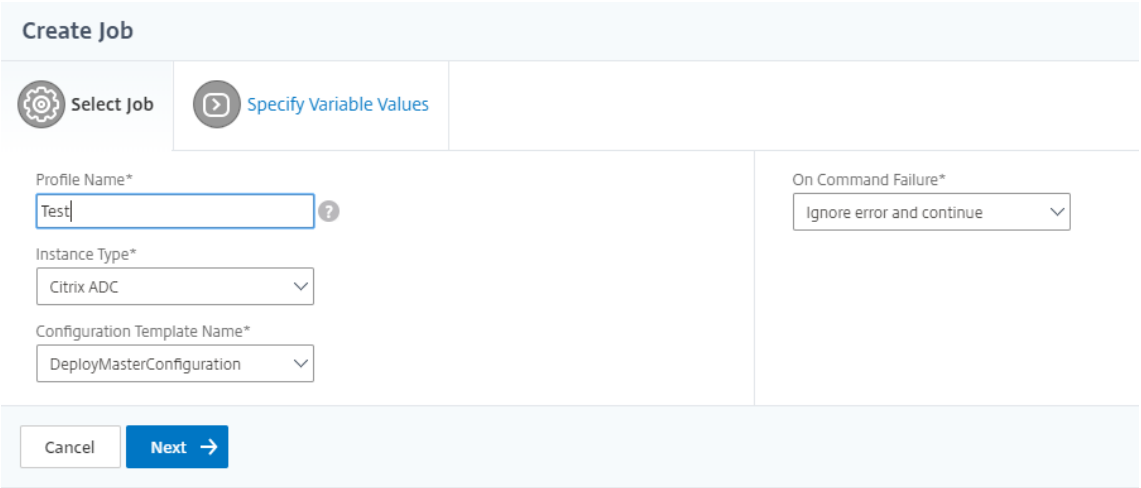


> **Nota**
>
> Puede habilitar las opciones **Anexar salida** y **Anexar errores** si quiere almacenar la salida y los errores generados (si los hay) al ejecutar un script en los archivos de registros del servidor NetScaler ADM. Si no habilita estas opciones, NetScaler ADM descartará todas las salidas y errores generados al ejecutar la script.

Para configurar la acción Ejecutar trabajo:

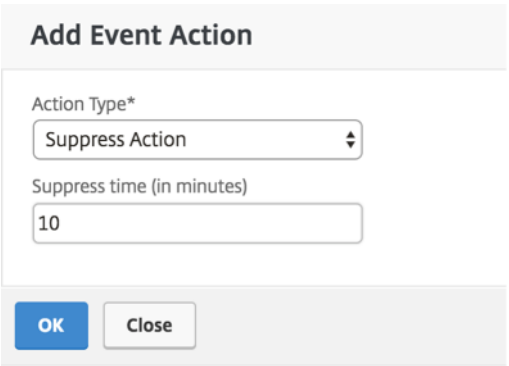
Al crear un perfil con trabajos de configuración, un trabajo se ejecuta como un trabajo integrado o un trabajo personalizado para las instancias WO de Citrix ADC, Citrix SDX y Citrix SD-WAN, para eventos y alarmas que coinciden con los criterios de filtro que ha especificado.

1. En **Acciones de reglas de eventos** , haga clic en **Agregar acción** y seleccione **Ejecutar acción de trabajo** en el menú **Tipo de acción** .
2. Cree un perfil con un trabajo que desee ejecutar cuando los eventos cumplan con los criterios de filtro definidos.
3. Al crear un trabajo, especifique un nombre de perfil, el tipo de instancia, la plantilla de configuración y la acción que quiere realizar si los comandos del trabajo fallan.
4. En función del tipo de instancia seleccionado y de la plantilla de configuración elegida, especifique los valores de las variables y haga clic en **Finalizar** para crear el trabajo.



Para configurar la acción de supresión:

Al elegir la **acción Suprimir** el evento Acción, puede configurar un período de tiempo, en minutos, durante el cual se suprime o se elimina un evento. Puede suprimir el evento durante un mínimo de 1 minuto.



La regla de evento se crea ahora con filtros apropiados y acciones de regla de evento bien definidas.

Modificar la gravedad reportada de los eventos que se producen en instancias de NetScaler ADC

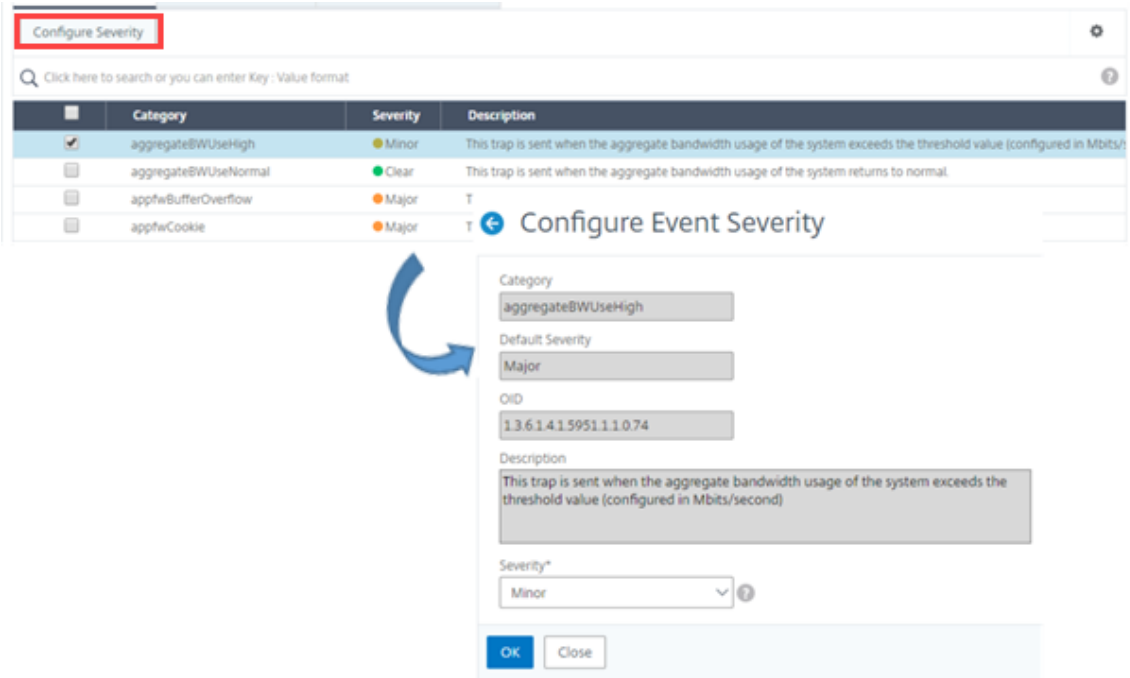
January 30, 2024

Puede gestionar los informes de eventos generados en todos sus dispositivos, de modo que pueda ver los detalles de los eventos relacionados con un evento en particular en una instancia determinada y ver los informes en función de la gravedad del evento. Puede crear reglas de eventos que usen la configuración de gravedad predeterminada y puede cambiar la configuración de gravedad. Puede configurar la gravedad para eventos genéricos y específicos de la empresa.

Puede definir los siguientes niveles de gravedad: Crítico, Mayor, Menor, Advertencia y Borrar.

Para modificar la gravedad del evento:

1. Vaya a **Redes** > **Eventos** > **Configuración** de eventos .
2. Haga clic en la ficha del tipo de instancia de Citrix Application Delivery Controller (ADC) que quiere modificar. A continuación, seleccione la categoría de la lista y haga clic en **Configurar gravedad**.
3. En **Configurar la gravedad del evento**, seleccione el nivel de gravedad en la lista desplegable.
4. Haga clic en **Aceptar**.

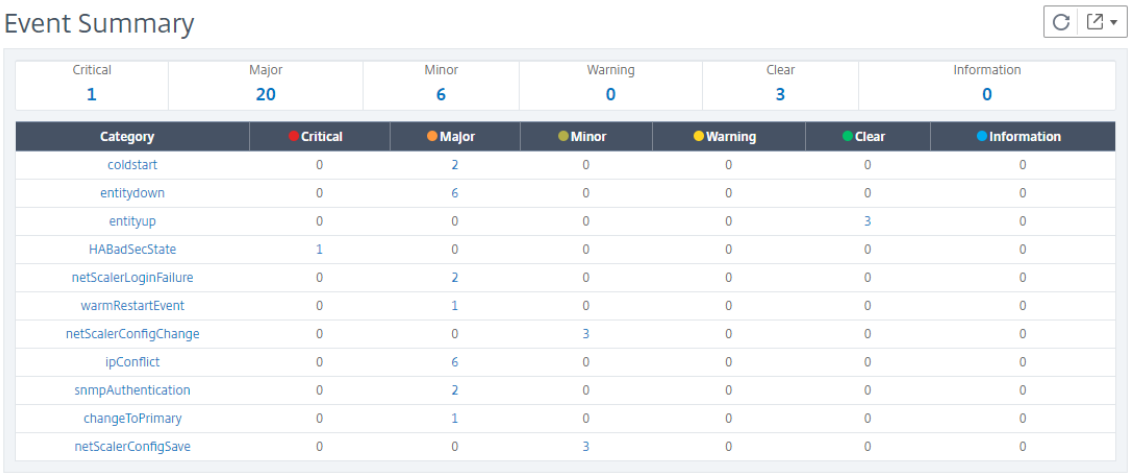


Ver resumen de eventos

January 30, 2024

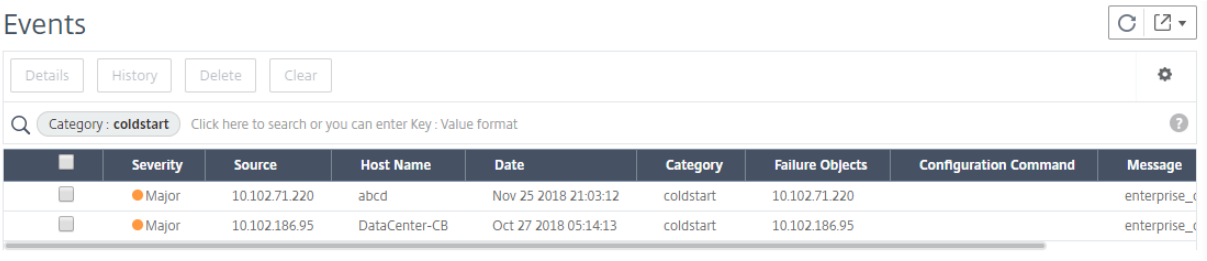
Ahora puede ver una página Resumen de eventos para supervisar los eventos y las capturas recibidas en el servidor NetScaler Application Delivery Management (ADM). Vaya a **Redes** > **Eventos** . La página Resumen de Eventos muestra la siguiente información en formato de tabla:

- **Resumen de todos los eventos recibidos por NetScaler ADM**. Los eventos se enumeran por categoría y sus diferentes niveles de gravedad se muestran en diferentes columnas: Crítico, Principal, Menor, Advertencia, Borrar e Información. Por ejemplo, se producirá un evento crítico cuando una instancia de Citrix Application Delivery Controller (ADC) se desactiva y deja de enviar información al servidor NetScaler ADM. Durante el evento, se envía una notificación a un administrador en la que se explica el motivo por el que la instancia está inactiva, el tiempo durante el cual estuvo inactiva, etc. A continuación, el evento se registra en la página Resumen de eventos, en la que puede ver un resumen y acceder a los detalles del evento.



- **Número de trampas recibidas para cada categoría**. El número de trampas recibidas, clasificadas por gravedad. De forma predeterminada, cada captura enviada desde instancias de NetScaler ADC a NetScaler ADM tiene asignada una gravedad, pero como administrador de red, puede especificar su gravedad en la GUI de NetScaler ADM.

Si hace clic en un tipo de categoría o en una trampa, accederás a la página
Eventos , en la que se preseleccionan filtros como la Categoría y la Gravedad. Esta página muestra más información sobre el evento, como la dirección IP y el nombre del host de la instancia de NetScaler ADC, la fecha en la que se recibió la captura, la categoría, los objetos de error, la ejecución del comando de configuración y la notificación del mensaje.



Mostrar severidades de eventos y detalles de capturas SNMP

January 30, 2024

Al crear un evento y su configuración en Citrix Application Delivery Management (ADM), puede ver el evento inmediatamente en la página Resumen del evento. Del mismo modo, puede ver y supervisar el estado, el tiempo de actividad, los modelos y las versiones de todas las instancias de Citrix Application Delivery Controller (ADC) agregadas a su servidor Citrix ADM con todo detalle en Infrastructure Dashboard.

En el panel Infraestructura, ahora puede enmascarar valores irrelevantes para que pueda ver y supervisar con más facilidad información como eventos por severidades, estado, tiempo de actividad, modelos y versión de instancias de NetScaler ADC en detalle.

Por ejemplo, los eventos con un nivel de gravedad **crítico** pueden ocurrir con poca frecuencia. Sin embargo, cuando se produzcan estos eventos críticos en la red, es posible que quiera investigar más a fondo, solucionar problemas y supervisar dónde y cuándo ocurrió el evento. Si selecciona todos los niveles de gravedad excepto Crítico, el gráfico muestra solo las ocurrencias de eventos críticos. Además, al hacer clic en el gráfico, accederás a la página de **eventos basados en la gravedad** , donde podrás ver todos los detalles sobre cuándo se produjo un evento crítico durante el tiempo que hayas seleccionado: el origen de la instancia, la fecha, la categoría y la notificación de mensaje enviada cuando ocurrió el evento crítico.

Del mismo modo, puede ver el estado de una instancia de Citrix VPX en el Panel de control. Puede enmascarar el tiempo durante el cual la instancia estaba en funcionamiento y en ejecución, y mostrar solo las veces que la instancia estuvo fuera de servicio. Al hacer clic en el gráfico, se le lleva a la página de esa instancia, donde el filtro *fuera de servicio* ya está aplicado, y ver detalles como el nombre de host, el número de solicitudes HTTP recibidas por segundo, el uso de CPU, etc. También puede seleccionar la instancia y consultar el panel de control de esa instancia de Citrix en particular para obtener más información.

Para seleccionar eventos específicos por gravedad en NetScaler ADM:

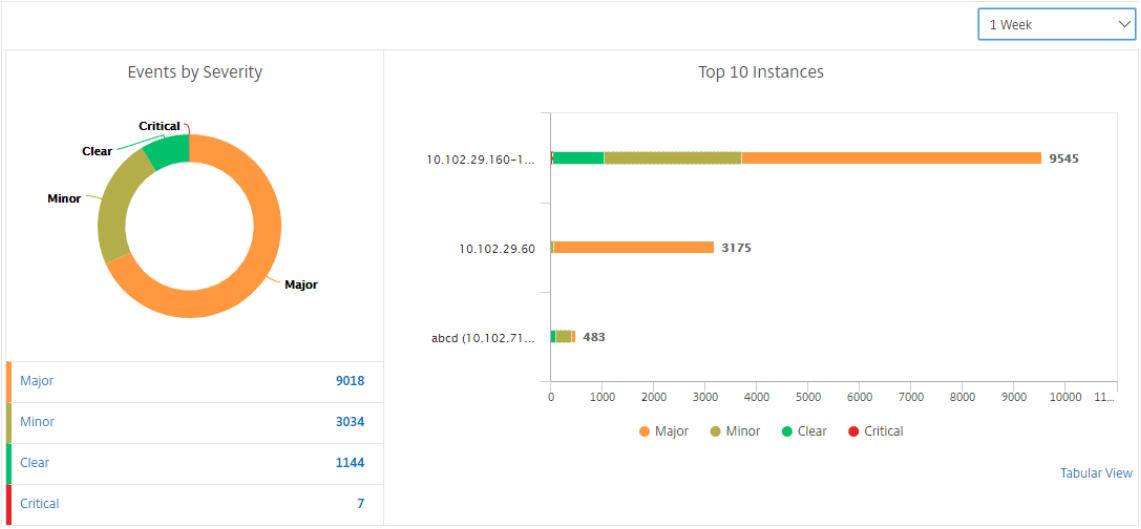
1. Inicie sesión en NetScaler ADM con sus credenciales de administrador.

2. Vaya a **Redes > Panel de control**.

   O bien:

   Vaya a **Redes > Eventos > Informes**.

3. En el menú de la esquina superior derecha de la página, seleccione la duración para la que quiere ver los eventos por gravedad.

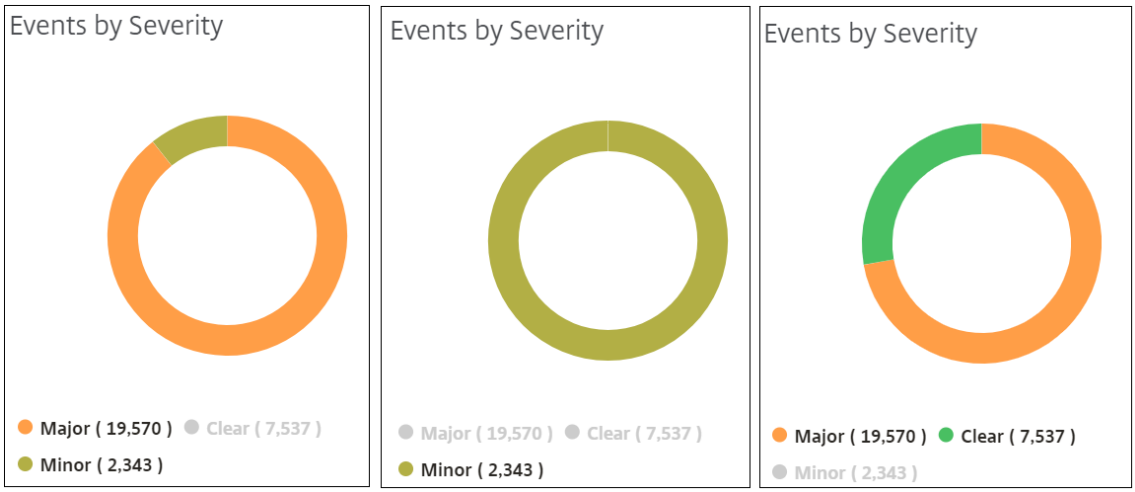


4. El gráfico de donut **Eventos por gravedad**muestra una representación visual de todos los eventos según su gravedad. Los diferentes tipos de eventos se representan como secciones de colores diferentes, y la longitud de cada sección corresponde al número total de eventos de ese tipo de gravedad.

5. Puede hacer clic en cada sección del gráfico de anillos para ver la página de **eventos basada en la gravedad** correspondiente, que muestra los siguientes detalles de la gravedad seleccionada durante la duración seleccionada:

   - Origen de instancia
   - Datos del evento
   - Categoría de eventos generados por la instancia de NetScaler ADC
   - Notificación de mensaje enviada

> **Nota**
>
> Debajo del gráfico de rosquillas se puede ver una lista de las severidades que se representan en el gráfico. De forma predeterminada, un gráfico de donut muestra todos los eventos de todos los tipos de gravedad y, por lo tanto, se resaltan todos los tipos de gravedad de la lista. Puede alternar los tipos de gravedad para ver y supervisar más fácilmente la gravedad elegida.



Para ver los detalles de la captura SNMP de NetScaler ADC en NetScaler ADM:

Ahora puede ver los detalles de cada captura SNMP recibida de sus instancias de NetScaler ADC administradas en el servidor NetScaler ADM en la página **Configuración de eventos**. Vaya a **Redes** > **Eventos** > **Configuración** de eventos . Para una captura específica recibida de su instancia, puede ver los siguientes detalles en formato tabular:

- **Categoría**: especifica la categoría de la instancia a la que pertenece el evento.
- **Gravedad**: la gravedad del evento se indica mediante los colores y el tipo de gravedad.
- **Descripción**: especifica los mensajes asociados al evento.

Por ejemplo, en un evento con la categoría de captura **monRespTimeoutBelowThresh**, la descripción de la trampa aparece como "Esta captura se envía cuando el tiempo de espera de respuesta de una sonda de monitor vuelve a la normalidad, inferior al umbral establecido".

Exportar mensajes syslog

January 30, 2024

Ahora puede ver los mensajes syslog sin iniciar sesión en NetScaler Application Delivery Management (ADM), programando una exportación de todos los mensajes syslog recibidos en el servidor. Puede exportar los mensajes de syslog que se generan en las instancias de Citrix Application Delivery Controller (ADC) en formatos PDF, CSV, PNG y JPEG. Puede programar la exportación de estos informes a direcciones de correo electrónico especificadas en distintos intervalos.

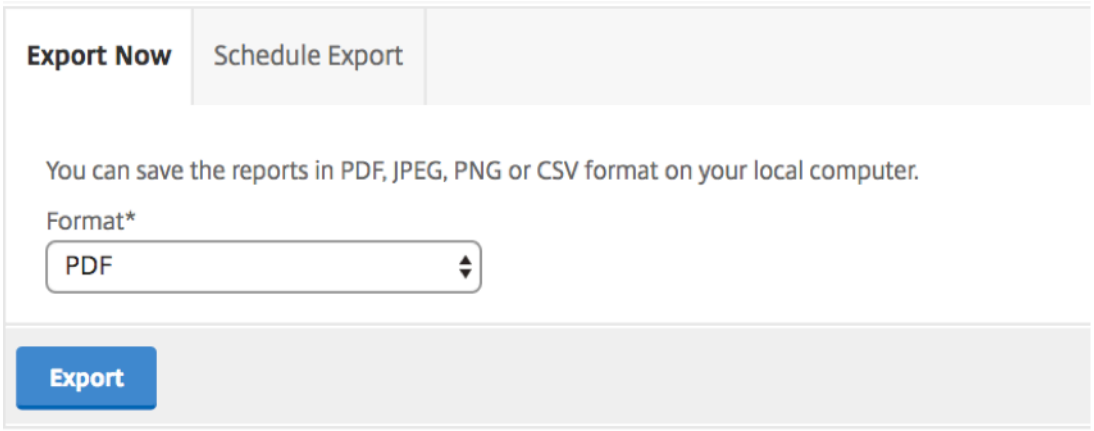
> **Nota**
>
> Para obtener más información sobre la configuración de un servidor syslog, el formato de datos

> y hora de syslog y cómo ver los mensajes de syslog en Citrix ADM, consulte Ver información de auditoría.

Para ver los mensajes de syslog, vaya a **Redes** > **Eventos** > **Mensajes de syslog** . En el panel derecho, en Syslog **Viewer** , puede filtrar los mensajes de syslog que desea ver por módulo, tipo de evento, gravedad y dirección IP de origen. Haga clic en **Aplicar** para generar los mensajes de syslog.

Para exportar un informe de mensajes de syslog mediante NetScaler ADM:

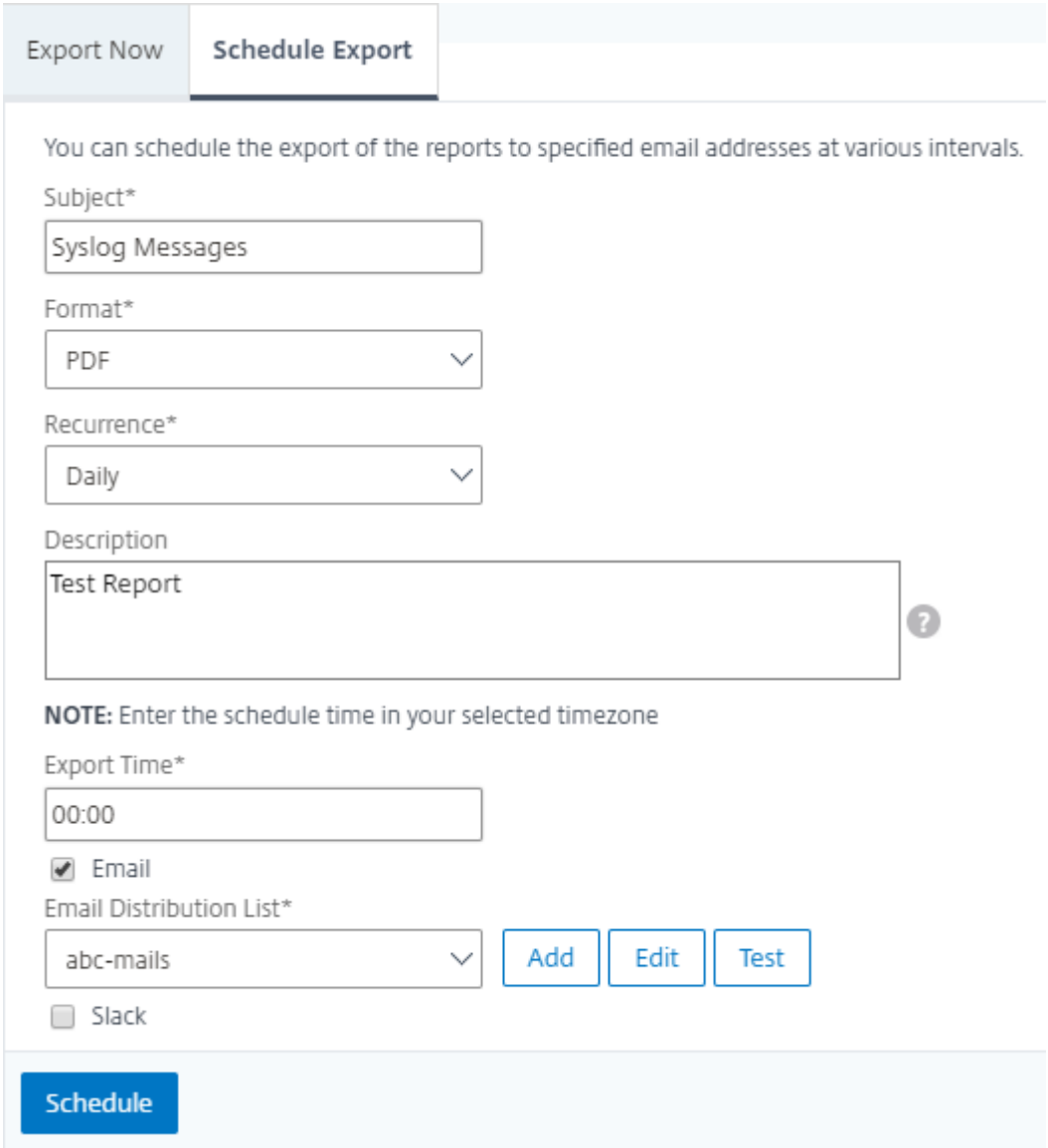
1. Vaya a**Redes**> **Eventos** > **Mensajes de Syslog**.
2. En el panel derecho, haga clic en el botón de exportación en la esquina superior derecha de la página de mensajes de Syslog.
3. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.



Para programar la exportación del informe de mensajes de syslog mediante NetScaler ADM:

1. Vaya a **Redes** > **Eventos** > **Mensajes de Syslog**.
2. En la página **Mensajes de Syslog** , en el panel derecho, haga clic en **Exportar**.
3. En la ficha **Informe de planificación**, defina los siguientes parámetros:
   - **Descripción**: Mensaje que describe el motivo para exportar el informe.
   - **Formato**: formato en el que se va a exportar el informe.
   - **Periodicidad**: intervalo en el que se exporta el informe.
   - **Hora de exportación**: Hora a la que se exporta el informe. Introduzca la hora en un formato de 24 horas para su zona horaria local.
   - **Lista de distribución de correo electrónico**: Lista de destinatarios para recibir el informe por correo electrónico. Elija una lista de distribución de correo electrónico de la lista desplegable proporcionada. Un correo electrónico se activa cuando se genera el informe y

cumple los criterios de tiempo programados. Si desea crear una nueva lista de distribución de correo electrónico, haga clic en **+** y proporcione los detalles del servidor de correo y del perfil de correo.



Cómo configurar la configuración de la poda de eventos mediante NetScaler ADM

Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos del servidor Citrix ADM, puede especificar el intervalo durante el que quiere que Citrix ADM conserve los datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

Vaya a **Sistema**>**Administración del sistema**. En **Configuración de instancia** , haga clic en **Configuración de poda de eventos**. Introduzca el intervalo de tiempo, en días, para el que desea conservar

los datos en el servidor Citrix ADM **y** haga clic en Aceptar.

Suprimir mensajes de syslog

January 30, 2024

Cuando se configura como un servidor syslog, Citrix Application Delivery Management (ADM) recibe todos los mensajes syslog que le envían las instancias configuradas de Citrix Application Delivery Controller (ADC). Es posible que haya una gran cantidad de mensajes que quizás no desee ver. Por ejemplo, puede que no le interese ver todos los mensajes de nivel informativo. Ahora puede descartar algunos de los mensajes syslog que no le interesan. Puede suprimir algunos de los mensajes de syslog que llegan a NetScaler ADM configurando algunos filtros. Citrix ADM elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de NetScaler ADM y estos mensajes tampoco se almacenan en la base de datos de NetScaler ADM del cliente.

Puede suprimir algunos de los mensajes de syslog registrados que llegan a NetScaler ADM configurando algunos filtros. Los dos filtros que se pueden utilizar para suprimir mensajes syslog son gravedad y facilidad. También puede suprimir los mensajes procedentes de una instancia concreta de NetScaler ADC o de varias instancias. También puede proporcionar un patrón de texto para que NetScaler ADM busque y suprima mensajes. Citrix ADM elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de NetScaler ADM y estos mensajes tampoco se almacenan en la base de datos del cliente. Por lo tanto, se ahorra una buena cantidad de espacio en el servidor de almacenamiento.

Algunos casos de uso para suprimir los mensajes de syslog son los siguientes:

- Si quiere ignorar todos los mensajes de nivel de información, suprima el nivel 6 (informativo)
- Si solo quiere registrar las condiciones de error del firewall, suprima todos los niveles que no sean el nivel 3 (errores)

Supresión de mensajes de syslog mediante la creación de filtros

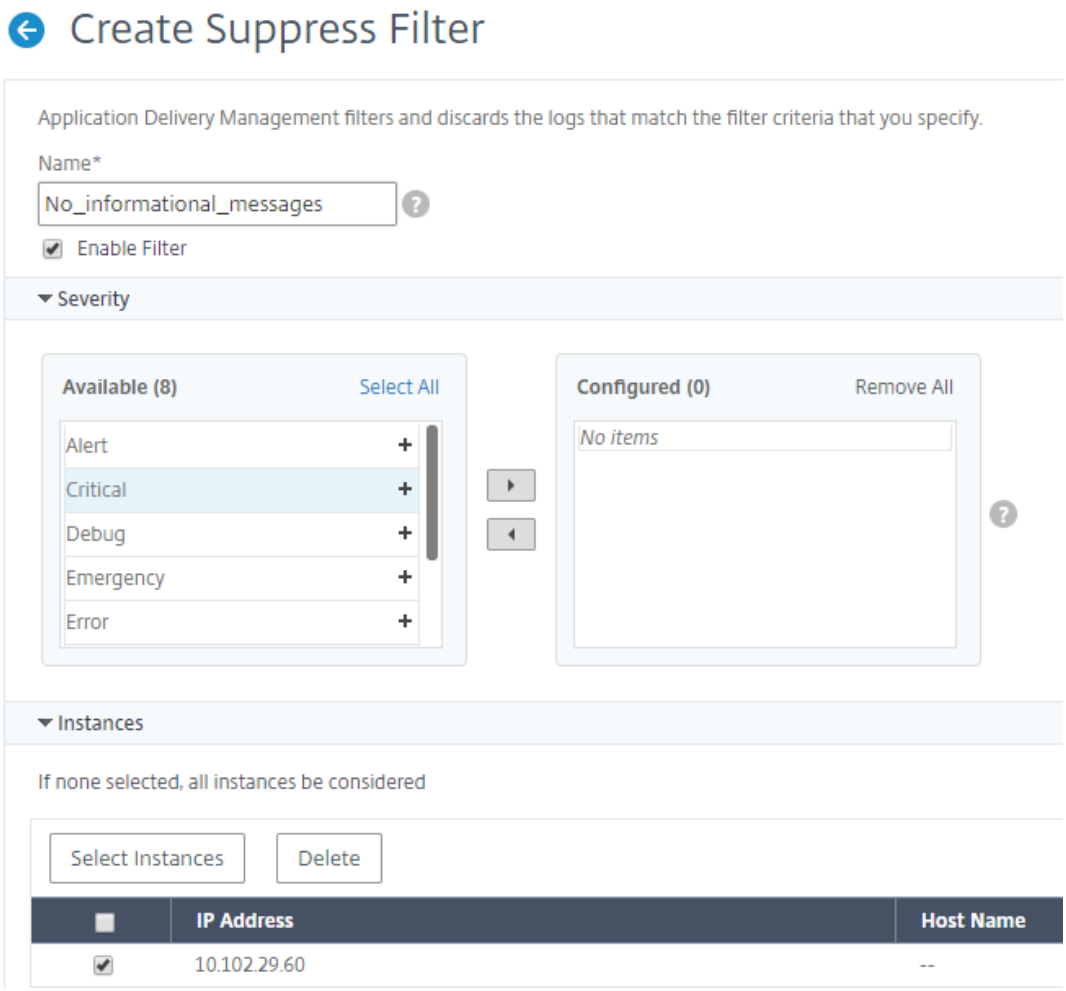
1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Mensajes de Syslog** > **Filtro de supresión**.
2. En la página **Crear filtro de supresión**, actualice la siguiente información:
    a) **Nombre**: Escriba un nombre para el filtro.

    > **Nota:**
    >
    > Si los diferentes usuarios tienen diferentes accesos a varias instancias de NetScaler ADC, se deben crear diferentes filtros para diferentes instancias, ya que los usuarios

> solo pueden ver los filtros en los que tienen acceso a todas las instancias.

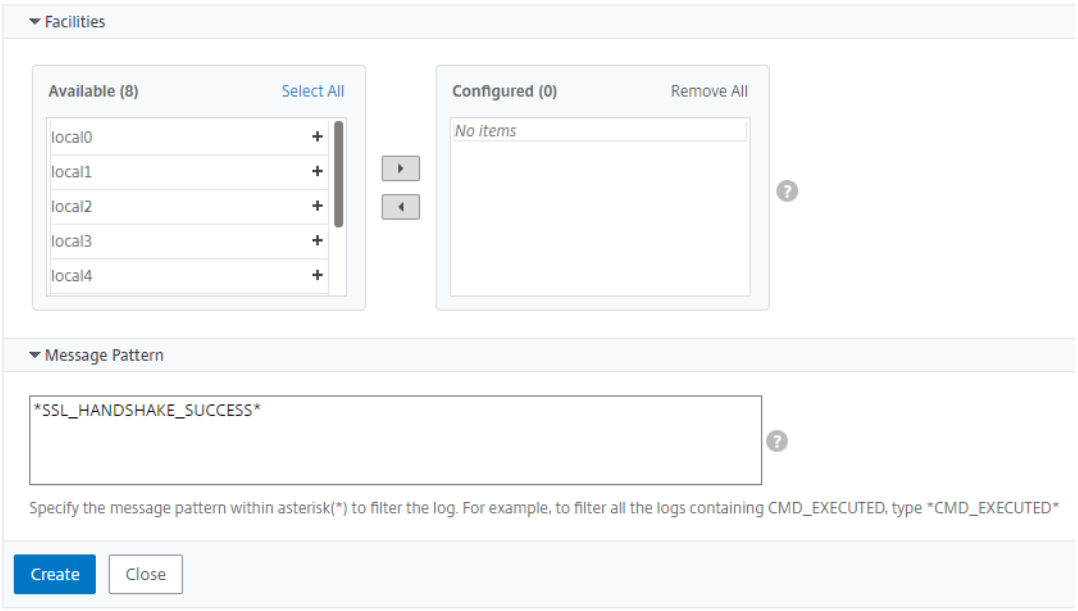
b) **Gravedad**: Seleccione y agregue los niveles de registro para los que debe suprimir los mensajes. Por ejemplo, si no quiere ver ningún mensaje informativo que llegue, puede seleccionar Informativo para suprimirlos.

c) **Instancias**: Seleccione las instancias NetScaler ADC en las que se han configurado los mensajes syslog.



d) **Instalaciones**: Seleccione la función para suprimir los mensajes en función de la fuente que los genera.

e) **Patrón de mensajes**: También puede escribir un patrón de texto rodeado de un asterisco (*) para suprimir los mensajes. En los mensajes se busca la cadena de patrón de texto y se suprimen los mensajes que contienen este patrón.



Inhabilitar el filtro

Para permitir que los mensajes se vean en NetScaler ADM, debe inhabilitar el filtro.

1. Vaya a **Redes** > **Eventos** > **Mensajes de Syslog** > **Suprimir filtro** y, en la página **Suprimir filtro** , seleccione el filtro y haga clic en **Editar**.
2. En la página **Configurar suprimir filtro**, desactive la casilla de verificación **Habilitar filtro** para inhabilitar el filtro.

Configurar los parámetros de poda para eventos de instancia

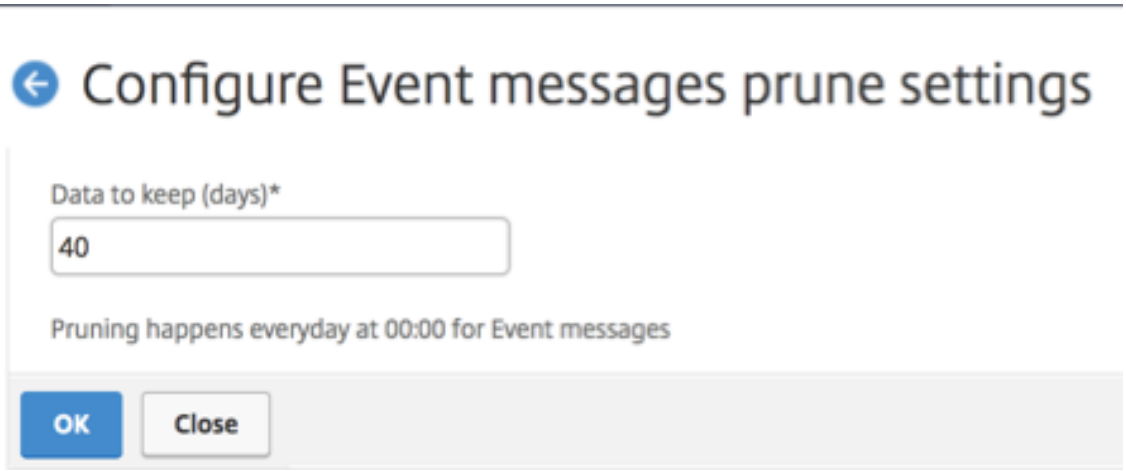
January 30, 2024

Las instancias de Citrix Application Delivery Controller (ADC) administradas por el servidor Citrix Application Delivery Management (ADM) envían datos de mensajes de eventos de forma continua para almacenarlos en Citrix ADM. Puede especificar el intervalo para el que quiere que NetScaler ADM conserve datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

> **Nota**
>
> El valor que puede especificar no puede superar los 40 días ni ser inferior a 1 día.

Para configurar los parámetros de poda para eventos de instancia:

1. Vaya a **Sistema**>**Administración del sistema**.
2. En **Configuración de poda**, haga clic en Configuración de **poda de eventos** de **instancia** .
3. Introduzca el intervalo de tiempo, en días, para el que desea conservar los datos en el servidor Citrix ADM **y** haga clic en Aceptar.



Tablero SSL

January 30, 2024

NetScaler Application Delivery Management (ADM) ahora optimiza todos los aspectos de la administración de certificados por usted. A través de una sola consola, puede establecer directivas automatizadas para garantizar el emisor correcto, la fortaleza de la clave y los algoritmos correctos, al tiempo que mantiene una estrecha ficha sobre los certificados que no se utilizan o que caducan pronto. Para empezar a utilizar el panel SSL de Citrix ADM y sus funcionalidades, debe entender qué es un certificado SSL y cómo puede utilizar Citrix ADM para realizar un seguimiento de sus certificados SSL.

Un certificado Secure Socket Layer (SSL), que forma parte de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. El certificado tiene un componente de clave pública visible para cualquier cliente que quiera iniciar una transacción segura con el servidor. La clave privada correspondiente, que reside de forma segura en el dispositivo Citrix Application Delivery Controller (ADC), se utiliza para completar el cifrado y descifrado de clave asimétrica (o clave pública).

Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

- De una autoridad de certificación autorizada (CA)
- Al generar un nuevo certificado SSL y una clave en el dispositivo Citrix ADC

NetScaler ADM proporciona una vista centralizada de los certificados SSL instalados en todas las instancias administradas de NetScaler ADC. En el panel de control de SSL, puede ver gráficos que le ayudan a rastrear los emisores de certificados, los puntos fuertes clave, los algoritmos de firma, los certificados caducados o no utilizados, etc. También puede ver la distribución de los protocolos SSL que se ejecutan en sus servidores virtuales y las claves que están habilitadas en ellos.

También puede configurar notificaciones para informarle cuando los certificados están a punto de caducar e incluir información sobre las instancias NetScaler ADC que utilizan dichos certificados.

Puede vincular los certificados de una instancia de NetScaler ADC a un certificado de CA. Sin embargo, asegúrese de que los certificados que enlace al mismo certificado de CA tengan el mismo origen y el mismo emisor. Después de vincular los certificados a un certificado de CA, puede desvincularlos.

Usar el panel SSL

January 30, 2024

Puede usar el panel de certificados SSL de Citrix Application Delivery Management (ADM) para ver gráficos que le ayudan a realizar un seguimiento de los emisores de certificados, los puntos fuertes clave y los algoritmos de firma. El panel de control de certificados SSL también muestra gráficos que indican lo siguiente:

- Número de días después de los cuales caducan los certificados
- Número de certificados usados y no utilizados
- Número de certificados autofirmados y firmados por una CA
- Número de emisores
- algoritmos de firma
- Protocolos SSL
- Las 10 instancias principales por número de certificados en uso

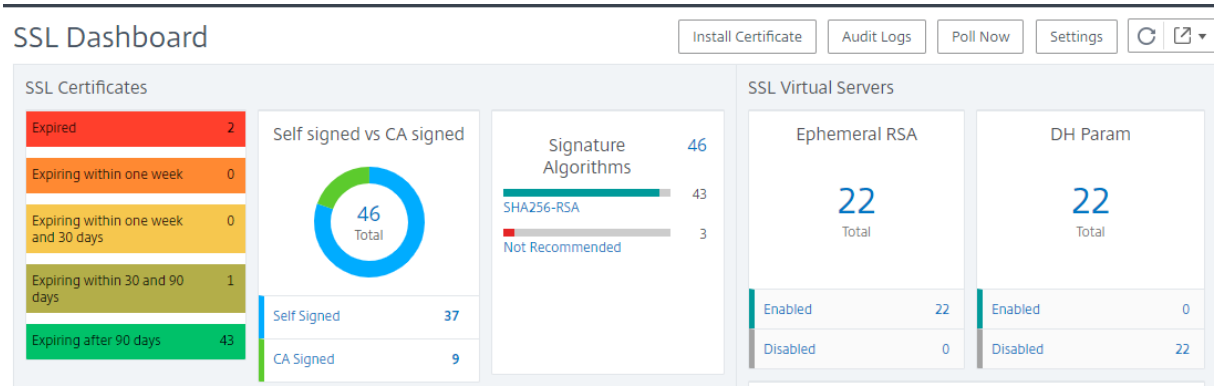
Para supervisar certificados SSL

Puede utilizar el panel de control SSL de Citrix ADM para supervisar sus certificados si su empresa tiene una política SSL en la que ha definido ciertos requisitos de certificado SSL, como que todos los certificados deben tener un nivel mínimo de claves de 2048 bits y una autoridad de CA de confianza debe autorizarlos.

En otro ejemplo, es posible que haya subido un certificado nuevo pero haya olvidado vincularlo a un servidor virtual. El panel de control SSL resalta los certificados SSL que se están utilizando o no. En

la sección Uso, puede ver el número de certificados que se han instalado y el número de certificados que se están utilizando. Puede seguir haciendo clic en el gráfico para ver el nombre del certificado, la instancia en la que se está utilizando, su validez, su algoritmo de firma, etc.

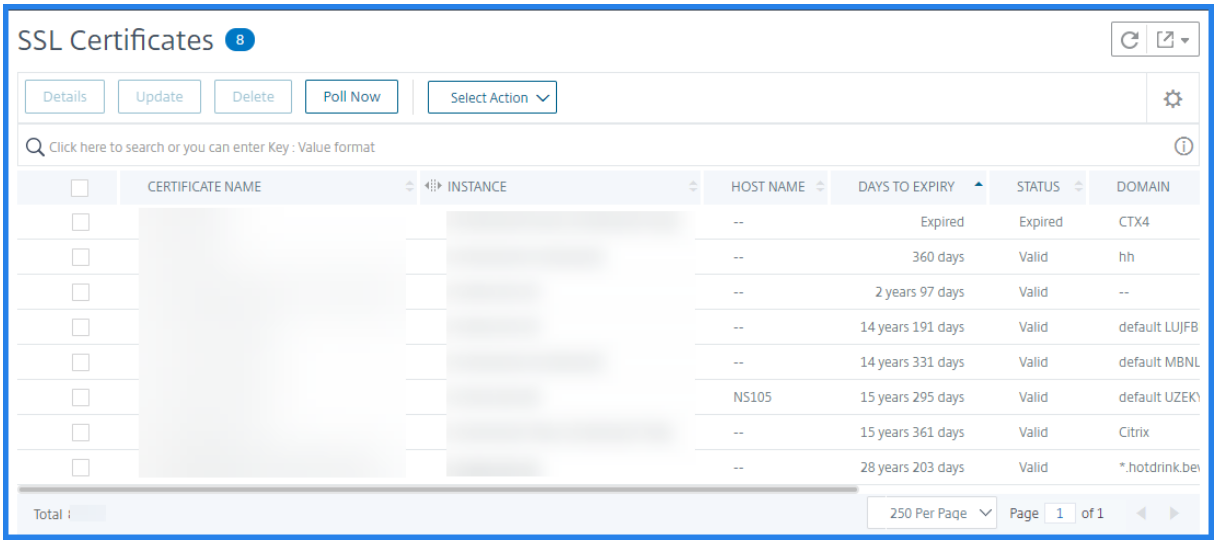
Para supervisar los certificados SSL en Citrix ADM, vaya a**Redes**> **Tablero SSL**.



Citrix ADM le permite sondear certificados SSL y agregar todos los certificados SSL de las instancias inmediatamente a Citrix ADM. Para hacerlo, vaya a **Redes** > **Panel de control SSL** y haga clic en **Sondear ahora** . Aparece la página Sondear **ahora** , que presenta la opción de sondear todas las instancias de Citrix Application Delivery Controller (ADC) de la red o sondear las instancias seleccionadas.

Puede utilizar el panel SSL de Citrix ADM para ver o supervisar los detalles de los certificados SSL, los servidores virtuales SSL y los protocolos SSL de Citrix ADC. Los números "totales"son hipervínculos, en los que puede hacer clic para mostrar detalles relacionados con certificados SSL, servidores virtuales SSL o protocolos SSL.

Por ejemplo, cuando un usuario hace clic en el número 52 de «Autofirmado vs. CA firmada"en la figura anterior, aparece una nueva ventana que muestra los detalles de los 52 certificados SSL en las instancias NetScaler ADC.



El panel de control SSL de Citrix ADM también muestra la distribución de los protocolos SSL que se

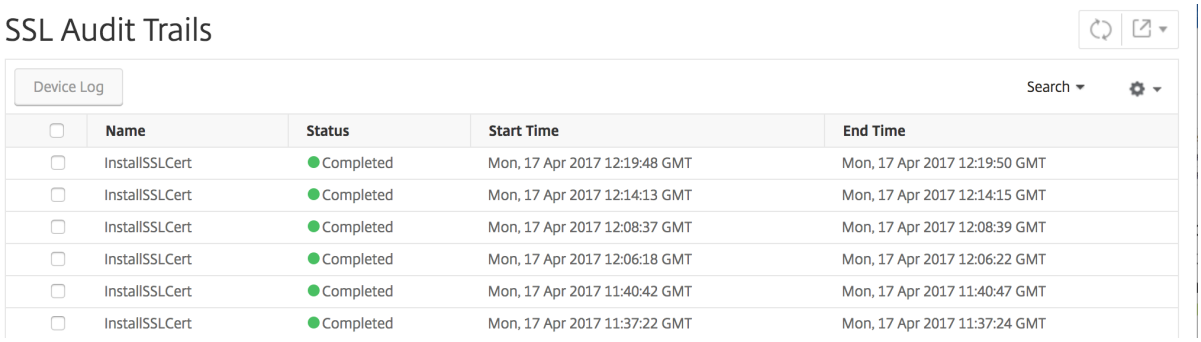
ejecutan en los servidores virtuales. Como administrador, puede especificar los protocolos que desea supervisar mediante la política SSL. Los protocolos compatibles son SSLv2, SSLv3, TLS1.0, TLS1.1 y TLS1.2. Los protocolos SSL utilizados en servidores virtuales aparecen en formato de gráfico de barras. Al hacer clic en un protocolo específico, se muestra una lista de servidores virtuales que utilizan ese protocolo.

Aparece un gráfico de anillos después de habilitar o deshabilitar las claves RSA Diffie-Hellman (DH) o Ephermeral en el panel de control SSL. Estas claves permiten la comunicación segura con clientes de exportación incluso si el certificado del servidor no admite clientes de exportación, como en el caso de un certificado de 1024 bits. Al hacer clic en el gráfico correspondiente, se muestra una lista de los servidores virtuales en los que están habilitadas las claves DH o RSA efímeras.

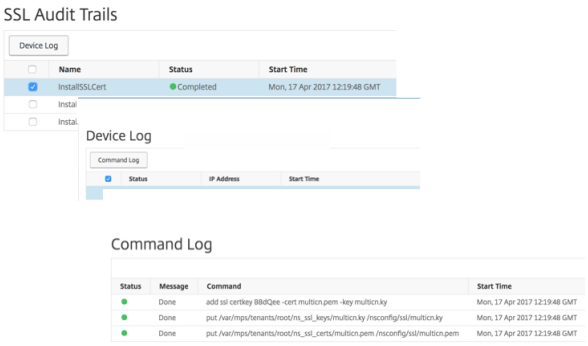
Para ver pistas de auditoría de certificados SSL

Ahora puede ver los detalles de registro de certificados SSL en Citrix ADM. Los detalles del registro muestran las operaciones realizadas con certificados SSL en Citrix ADM, como la instalación de certificados SSL, la vinculación y desvinculación de certificados SSL, la actualización de los certificados SSL y la eliminación de certificados SSL. La información de seguimiento de auditoría es útil mientras se supervisan los cambios en los certificados SSL realizados en una aplicación con varios propietarios.

Para ver un registro de auditoría de una operación concreta realizada en Citrix ADM mediante certificados SSL, vaya a **Redes** > **Panel de control SSL** > Registros de **auditoría SSL** .



Para una operación concreta realizada con certificado SSL, puede ver su estado, hora de inicio y hora de finalización. Además, puede ver la instancia en la que se realizó la operación y los comandos ejecutados en esa instancia.

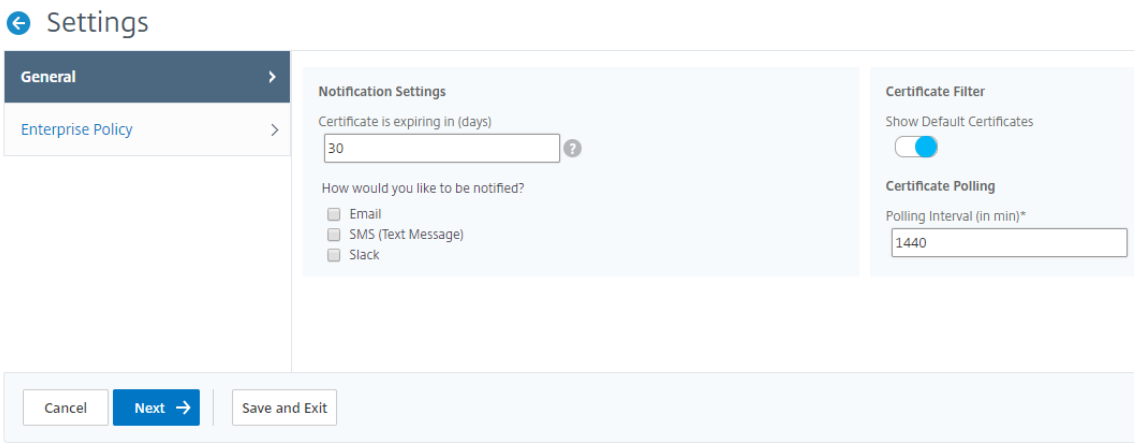


Para excluir certificados Citrix ADC predeterminados en el panel SSL

Citrix ADM le permite mostrar u ocultar los certificados predeterminados de Citrix ADC que aparecen en los gráficos de SSL Dashboard según sus preferencias. De forma predeterminada, todos los certificados se muestran en el panel SSL, incluidos los certificados predeterminados.

Para mostrar u ocultar certificados predeterminados en el panel SSL:

1. Vaya a **Networks** > **SSL Dashboard** en la GUI de Citrix ADM.
2. En la página **Tablero de SSL**, haga clic en **Configuración**.
3. En la página **Configuración**, seleccione **General**.
4. Escriba el número de días en que caduca el certificado para recibir una notificación sobre la caducidad del certificado.
5. Seleccione el método de notificación y cree los perfiles respectivos.
6. En la sección **Filtro de certificados**, desactive la casilla de verificación **Mostrar certificados predeterminados** y haga clic en **Guardar y salir**.



Configurar notificaciones para la caducidad del certificado SSL

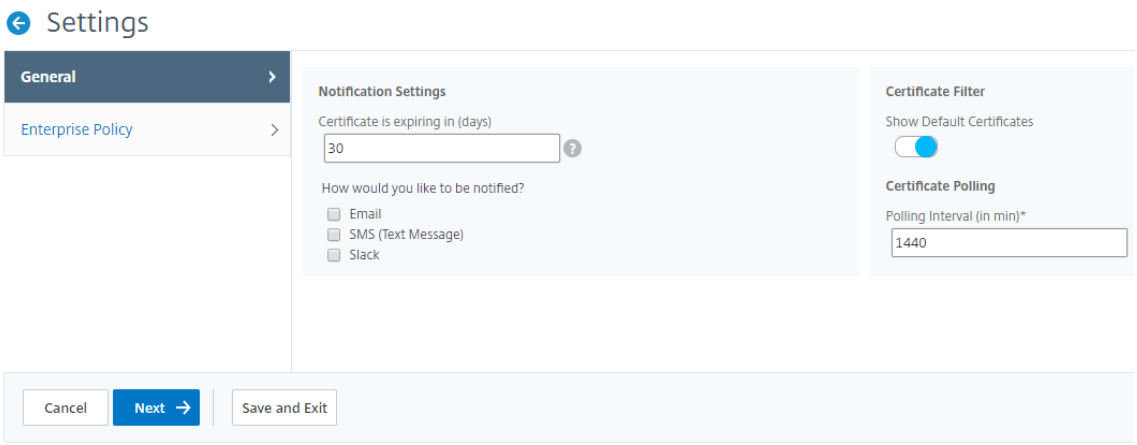
January 30, 2024

Como administrador de seguridad, puede configurar notificaciones para que le informen cuando los certificados estén a punto de caducar e incluir información sobre las instancias de Citrix Application Delivery Controller (ADC) que utilizan esos certificados. Al habilitar las notificaciones, puede renovar sus certificados SSL a tiempo.

Por ejemplo, puede configurar una notificación por correo electrónico para que se envíe una lista de distribución por correo electrónico 30 días antes de la fecha de caducidad del certificado.

Para configurar notificaciones desde NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a **Redes** > **SSL Dashboard**.
2. En la página **Tablero de SSL**, haga clic en **Configuración**.
3. En la página de **configuración de SSL**, haga clic en el icono **Editar**.
4. En la sección **Configuración de notificaciones**, especifique cuándo desea enviar la notificación en términos de número de días antes de la fecha de caducidad.
5. Elige el tipo de notificación que deseas enviar. Seleccione el tipo de notificación y la lista de distribución en el menú desplegable. Los tipos de notificación son los siguientes:
   - **Correo electrónico**: especifique un servidor de correo y los detalles del perfil. Un correo electrónico se activa cuando sus certificados están a punto de caducar.
   - **SMS**: Especifique un servidor del servicio de mensajes cortos (SMS) y los detalles del perfil. Se activa un mensaje SMS cuando sus certificados están a punto de caducar.
   - **Slack**: Especifique los detalles del perfil Slack.
6. Haz clic en **Guardar y salir.**



NetScaler ADM envía ahora la captura de caducidad de certificados SSL al servidor de destino de capturas externo cuando los certificados SSL están vencidos. Citrix ADM envía una trampa cuando se cumplen las dos condiciones siguientes:

- Ha configurado el número de días para que caduque el certificado en la página de configuración del panel SSL.
- Ha agregado el destino de captura.

Para establecer los destinos de captura, vaya a **Sistema** > **SNMP** > **Destinos** de captura . Escriba la dirección IP del servidor SNMP de destino al que se envían las capturas. Introduzca el número de puerto y escriba "public"(sin comillas) como cadena comunitaria.

Actualizar un certificado instalado

January 30, 2024

Tras recibir un certificado renovado de la autoridad de certificación (CA), puede actualizar los certificados existentes desde Citrix Application Delivery Management (ADM) sin necesidad de iniciar sesión en instancias individuales de Citrix Application Delivery Controller (ADC).

Para actualizar un certificado SSL, una clave o ambos desde NetScaler ADM:

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. En la página **Certificados SSL**, seleccione un certificado y haga clic en **Actualizar**. También puede hacer clic en el certificado SSL para ver sus detalles y, a continuación, haga clic en **Actualizar** en la esquina superior derecha de la página **Certificado SSL**.
4. En la página **Actualizar el certificado SSL**, realice las modificaciones necesarias en el certificado, la clave o ambos y haga clic en **Aceptar**.

Instalar certificados SSL en una instancia de NetScaler ADC

January 30, 2024

Antes de instalar los certificados SSL en las instancias de Citrix Application Delivery Controller (ADC), asegúrese de que los certificados estén emitidos por CA de confianza. Además, asegúrese de que la intensidad de clave de las claves de certificado sea 2048 bits o superior y que las claves estén firmadas con algoritmos de firma seguros.

Para instalar un certificado SSL desde otra instancia de NetScaler ADC:

También puede importar un certificado desde una instancia de NetScaler ADC seleccionada y aplicarlo a otras instancias de NetScaler ADC de destino desde la GUI de NetScaler Application Delivery Management (ADM).

1. Vaya a **Redes** > **Panel de SSL**.
2. En la esquina superior derecha del panel SSL, haga clic en **Instalar**.
3. En la página **Instalar el certificado SSL en las instancias de NetScaler**, especifique los siguientes parámetros:

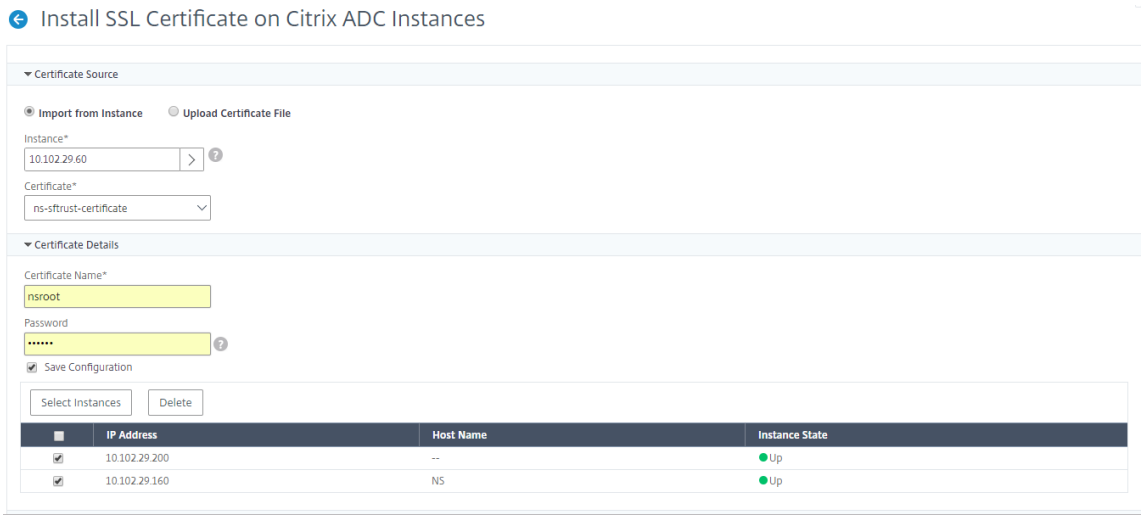
   a) Origen de certificado
   Seleccione la opción **Importar desde instancia**.

   - Elija la **instancia** desde la que quiere importar el certificado.
   - Elija el **Certificado** de la lista de todos los archivos de certificado SSL de la instancia.

   b) Detalles del certificado

   - **Nombre del certificado**. Especifique un nombre para la clave del certificado.
   - **Contraseña**. Contraseña para cifrar la clave privada. Puede utilizar esta opción para cargar claves privadas cifradas.

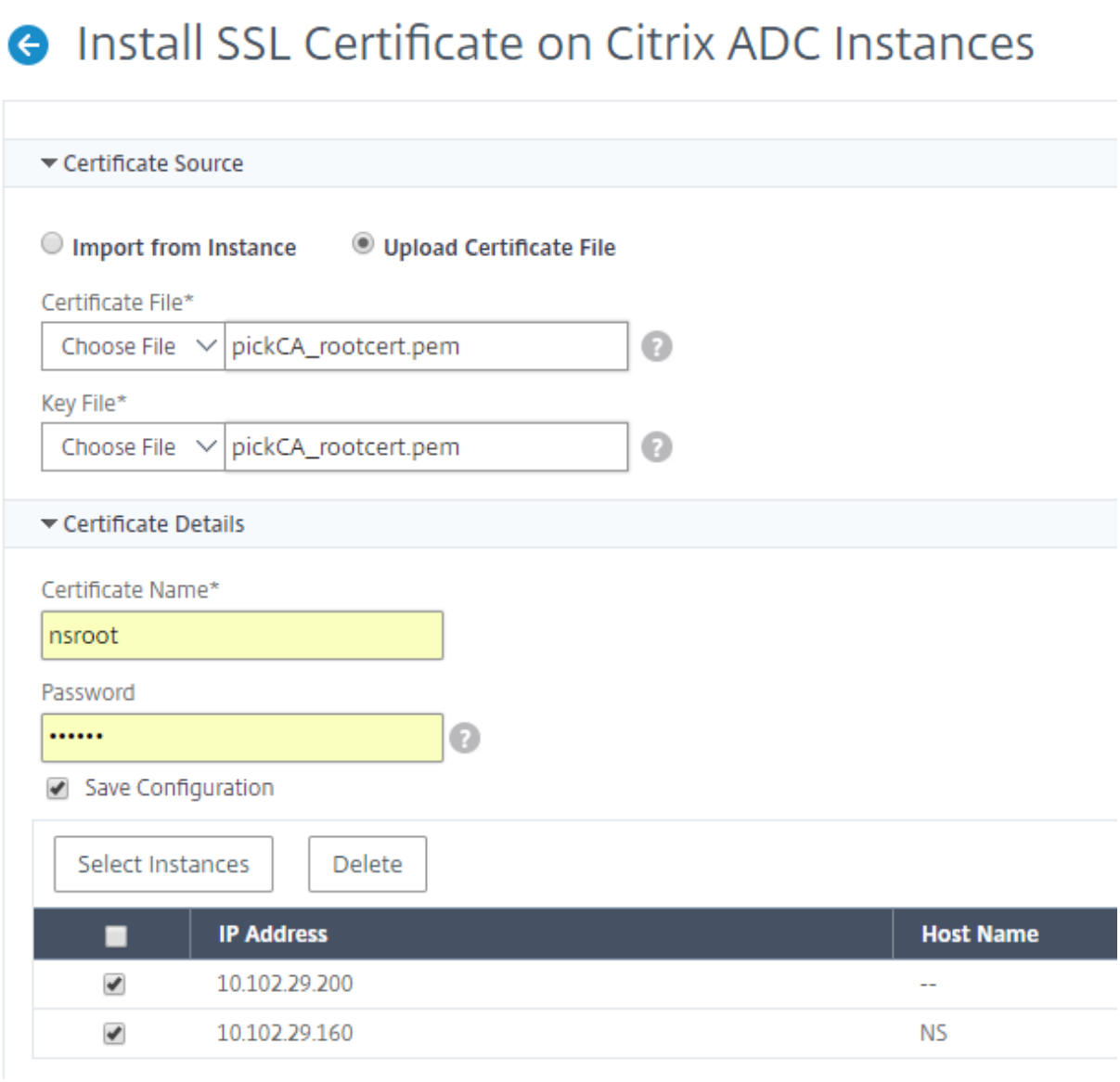
4. Haga clic en **Seleccionar instancias** para seleccionar las instancias de NetScaler ADC en las que quiere instalar sus certificados.
5. Haga clic en **Aceptar**.



Para instalar un certificado SSL desde NetScaler ADM:

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.

2. En la esquina superior derecha del panel, haga clic en **Instalar**.
3. En la página **Instalar certificado SSL en NetScaler Instance**, seleccione **Cargar archivo de certificados** y especifique los parámetros siguientes:
    - **Archivo de certificado**: Cargue un archivo de certificado SSL seleccionando **Local** (su máquina local) o **Dispositivo** (el archivo de certificado debe estar presente en la instancia virtual de NetScaler ADM).
    - **Archivo clave**: Cargue el archivo clave.
    - **Nombre del certificado**: Especifique un nombre para la clave del certificado.
    - **Contraseña**: Contraseña para cifrar la clave privada. Puede utilizar esta opción para cargar claves privadas cifradas.
    - **Seleccione instancias**: seleccione las instancias de Citrix ADM en las que quiere instalar los certificados.
4. Para guardar la configuración para usarla en el futuro, active la casilla **Guardar configuración**.
5. Haga clic en **Aceptar**.



Crear una solicitud de firma de certificados (CSR)

January 30, 2024

Una solicitud de firma de certificado (CSR) es un bloque de texto cifrado que se genera en el servidor en el que se utilizará el certificado. Contiene información que se incluirá en el certificado, como el nombre de su organización, el nombre común (nombre de dominio), la localidad y el país.

Para crear una CSR con NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a **Redes** > **SSL Dashboard**.

2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL instalados y, a continuación, seleccione el certificado para el que quiere crear una CSR y seleccione **Crear CSR** en la lista **Seleccionar acción**.
3. En la página **Crear solicitud de firma de certificado (CSR)**, especifique un nombre para la CSR.
4. Lleve a cabo una de las siguientes acciones:
   - **Cargar una clave**: Selecciona la opción **Tengo una clave**. Para cargar el archivo de claves, seleccione **Local** (su máquina local) o **Appliance** (el archivo de claves debe estar presente en la instancia virtual NetScaler ADM).
   - **Crear una clave**: seleccione la opción No tengo una clave y, a continuación, especifique los siguientes parámetros:

Algoritmo de cifrado	Tipo de llave. Por ejemplo, RSA.
Nombre de archivo de clave	Nombre del archivo en el que está almacenada la clave RSA.
Tamaño de clave	Tamaño de la clave en bits.
Valor del exponente público	Elija **3** o **F4** de la lista desplegable proporcionada. Este valor es parte del algoritmo de cifrado que se requiere para crear la clave RSA.
Formato de clave	Por defecto, se selecciona PEM. PEM es el formato de clave recomendado para su certificado SSL.
Algoritmo de codificación PEM	En la lista desplegable, seleccione el algoritmo (**DES** o **DES3**) que quiere utilizar para cifrar la clave RSA generada. Si seleccionas este algoritmo, tendrás que proporcionar una contraseña PEM.
Contraseña PEM	Si ha elegido el algoritmo de codificación PEM, introduzca una contraseña.
Confirmar contraseña PEM	Confirma tu contraseña de PEM.

5. Haga clic en **Continuar**.
6. En la página siguiente, proporciona detalles adicionales. Si desea crear la CSR sin cambiar los valores predeterminados, haga clic en **Continuar**.

> **Nota**
>
> La mayoría de los campos tienen valores predeterminados extraídos del asunto del certificado seleccionado. El asunto contiene detalles como el nombre común, el nombre de la organización, el estado y el país.
>
> La mayoría de los CA aceptan envíos de certificados por correo electrónico. La CA devolverá un certificado válido a la dirección de correo electrónico desde la que envíe el CSR.

Vincular y desvincular certificados SSL

January 30, 2024

Para crear un paquete de certificados, debe vincular varios certificados entre sí. Para vincular un certificado a otro certificado, el emisor del primer certificado debe coincidir con el dominio del segundo certificado. Por ejemplo, si desea vincular el certificado A con el certificado B, el "emisor"del certificado A debe coincidir con el "dominio"del certificado B.

Para vincular un certificado SSL a otro certificado mediante NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a **Redes** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Seleccione el certificado que desee vincular y, a continuación, seleccione **Vincular** en la lista desplegable **Acción**.
4. En la lista de certificados coincidentes, seleccione el certificado al que quiere vincular y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Si no se encuentra ningún certificado coincidente, aparece el siguiente mensaje: No se ha encontrado ningún certificado que vincular.

Para desvincular un certificado SSL mediante NetScaler ADM:

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Elija uno de los certificados vinculados que estén vinculados y, a continuación, seleccione **Desvincular** en la lista desplegable **Acción**.
4. Haga clic en **Aceptar**.

> **Nota**
>
> Si el certificado seleccionado no está vinculado a otro certificado, se muestra el mensaje siguiente: El certificado no tiene ningún vínculo de CA.

Configurar una directiva de empresa

January 30, 2024

Puede configurar una directiva empresarial y agregar todas las CA de confianza, algoritmos de firma segura y seleccionar la seguridad de clave recomendada para las claves de certificado en NetScaler Application Delivery Management (ADM). Si alguno de los certificados instalados en la instancia de Citrix Application Delivery Controller (ADC) no se ha agregado a la directiva de empresa, el panel de certificados SSL muestra el emisor de esos certificados como No recomendado.

Además, si la seguridad de la clave del certificado no coincide con la seguridad clave recomendada en la directiva empresarial, el panel de certificados SSL muestra la fortaleza de esas claves como No recomendada.

Para configurar una directiva de empresa en NetScaler ADM:

1. En Citrix ADM, vaya a **Infraestructura** > **Panel de control SSL** y, a continuación, haga clic en **Configuración**.
2. En la página Configuración de SSL, haga clic en el icono **Modificar** para agregar todas las CA de confianza, algoritmos de firma segura y seleccionar la seguridad de clave recomendada para sus certificados y claves.
3. Haga clic en **Guardar** para guardar la directiva de empresa.

Encuesta de certificados SSL de instancias Citrix ADC

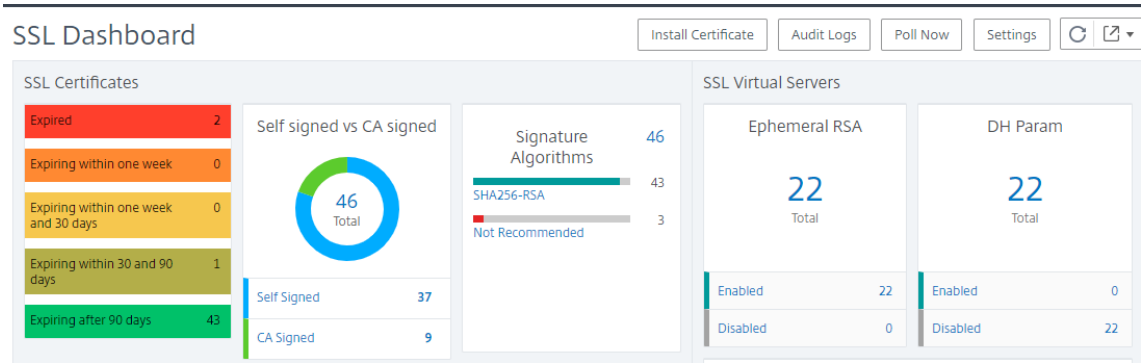
January 30, 2024

Citrix Application Delivery Management (ADM) sondea automáticamente los certificados SSL una vez cada 24 horas mediante llamadas NITRO y el protocolo Secure Copy (SCP). También puede sondear manualmente los certificados SSL para descubrir los certificados SSL recién agregados en las instancias de Citrix Application Delivery Controller (ADC). El sondeo de todos los certificados SSL de instancias Citrix ADC coloca una carga pesada en la red.

En lugar de sondear todos los certificados SSL de las instancias de Citrix ADC, puede sondear manualmente solo los certificados SSL de una o varias instancias seleccionadas.

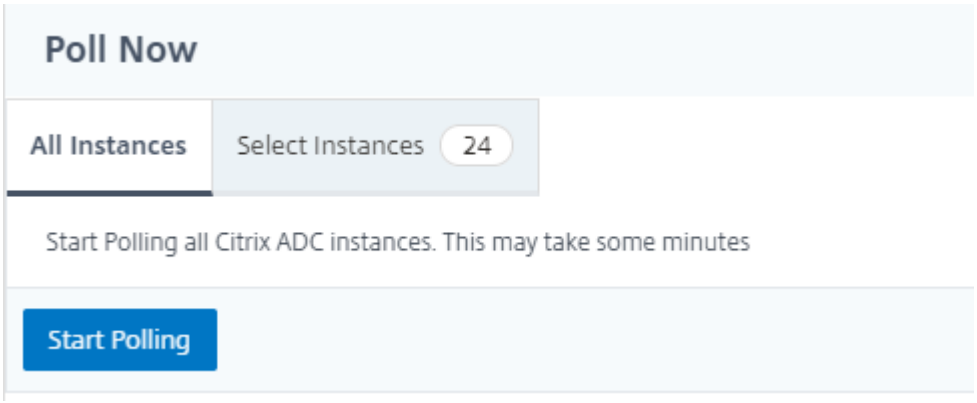
Para sondear certificados SSL en instancias Citrix ADC:

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. En la página **SSL Dashboard**, en la esquina superior derecha, haga clic en **Sondear ahora**.

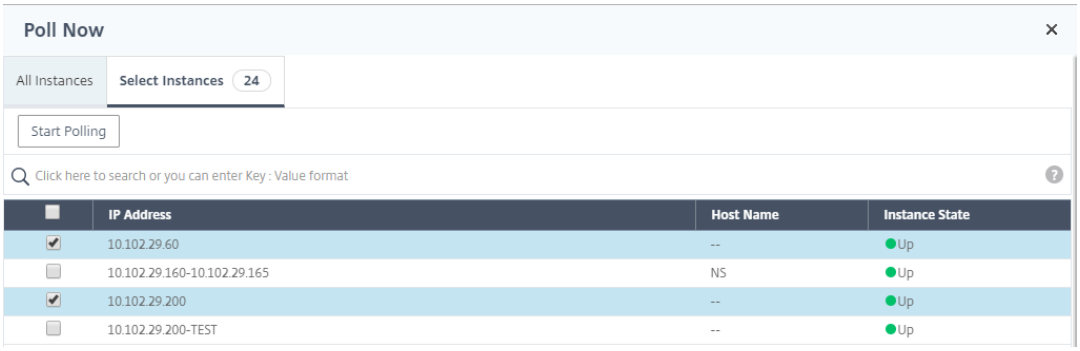


3. Aparece la página **Sondear ahora**, que le ofrece la opción de sondear todas las instancias de Citrix ADC de la red o sondear las instancias seleccionadas.

   a) Para sondear los certificados SSL de todas las instancias de Citrix ADC, seleccione la ficha **Todas las instancias** y haga clic en **Iniciar sondeo**.



   b) Para sondear instancias específicas, seleccione la ficha **Seleccionarinstancias**, seleccione las instancias de la lista y haga clic en**Sondear ahora**.



Trabajos de configuración

January 30, 2024

El proceso de administración de configuración de NetScaler Application Delivery Management (NetScaler ADM) garantiza la replicación adecuada de los cambios de configuración, las actualizaciones del sistema y otras actividades de mantenimiento en varias instancias de Citrix Application Delivery Controller (ADC) en la red.

Citrix ADM le permite crear trabajos de configuración que le ayudarán a realizar todas estas actividades con facilidad en varios dispositivos como una sola tarea. Las plantillas y los trabajos de configuración simplifican las tareas administrativas más repetitivas en una sola tarea en NetScaler ADM. Un trabajo de configuración contiene un conjunto de comandos de configuración que se pueden ejecutar en uno o varios dispositivos gestionados.

Los trabajos de configuración pueden usar comandos SSH para ejecutar los comandos de configuración o usar SCP para copiar archivos de forma local o a otro dispositivo; por ejemplo, podemos programar una conmutación por error de HA o una actualización de HA.

Puede crear un trabajo de configuración mediante una de las cuatro opciones siguientes en NetScaler ADM. Utilice una de estas opciones para crear una fuente reutilizable de comandos e instrucciones para que el sistema ejecute un trabajo de configuración.

1. Plantilla de configuración
2. Instancia
3. Archivo
4. Grabar y reproducir

Plantilla de configuración

Puede crear plantillas de configuración mientras crea un nuevo trabajo y guarda un conjunto de comandos de configuración como plantilla. Al guardar estas plantillas en la página Crear trabajos , se muestran automáticamente en la página Crear plantilla . Puede utilizar una de las siguientes plantillas:

Editor de configuración: puede usar el editor de configuración para escribir los comandos de la CLI, guardar la configuración como una plantilla y usarla para configurar los trabajos.

Plantilla incorporada: puede elegir de una lista de plantillas de configuración. Estas plantillas proporcionan las sintaxis de los comandos CLI y permiten especificar valores para las variables. Las plantillas integradas aparecen en la lista, con sus descripciones en la tabla siguiente. Puede programar un trabajo mediante la opción de plantilla integrada. Un trabajo es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Por ejemplo, puede utilizar la opción de plantilla integrada para programar un trabajo para configurar servidores syslog. También puede optar por ejecutar el trabajo inmediatamente o programar la ejecución del trabajo en una etapa posterior.

Instancia

Puede realizar una actualización de un solo paquete de las instancias de Citrix SDX que ejecuten Citrix ADC versión 11.0 y versiones posteriores. Para realizar una actualización de un solo paquete, utilice una tarea integrada en NetScaler ADM. También puede actualizar una instancia de Citrix ADC extrayendo la configuración en ejecución o una configuración guardada y ejecutando los comandos en otra instancia de Citrix ADC del mismo tipo. Esto le permite replicar la configuración de una instancia en la otra.

Archivo

Puede cargar un archivo de configuración desde su máquina local y crear trabajos.

Ventajas de usar un archivo

- Puede utilizar cualquier archivo de texto para crear una fuente reutilizable de comandos de configuración.
- No se requiere ningún tipo de formato.
- El archivo se puede guardar en el equipo local.

Puede crear y guardar un archivo nuevo o importar un archivo existente y ejecutar los comandos.

Grabar y reproducir

Con Create job, puede introducir sus propios comandos de la CLI o puede utilizar el botón de grabación y reproducción para obtener los comandos de una sesión de Citrix ADC. Cuando ejecuta el trabajo, los cambios en ns.conf en la instancia seleccionada se registran y copian en NetScaler ADM.

Artículos relacionados

- Cómo utilizar el comando SCP (put) en los trabajos de configuración
- Cómo utilizar variables en los trabajos de configuración
- Cómo crear trabajos de configuración a partir de comandos correctivos
- Cómo utilizar plantillas de configuración para crear plantillas de auditoría
- Cómo utilizar Record-and-Play para crear trabajos de configuración
- Cómo utilizar la plantilla de configuración maestra en NetScaler ADM

Crear un trabajo de configuración

January 30, 2024

Un trabajo es un conjunto de comandos de configuración que puede crear y ejecutar en una o varias instancias administradas. Puede crear trabajos para realizar cambios de configuración en las instancias, replicar configuraciones en varias instancias de la red y grabar y reproducir tareas de configuración mediante la GUI de NetScaler Application Delivery Management (ADM) y convertirlas en comandos de la CLI.

Puede utilizar la función Trabajos de configuración de NetScaler ADM para crear un trabajo de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados.

Para crear un trabajo de configuración en NetScaler ADM:

1. Vaya a **Redes > Trabajos de configuración**.
2. Haga clic en **Crear trabajo**.
3. En la página **Crear trabajo** , en la pestaña **Seleccionar configuración** , especifique el nombre del trabajo y seleccione el tipo de instancia en la lista desplegable.
4. En la lista desplegable **Origen de configuración**, seleccione la plantilla de trabajo de configuración que desea crear. Agregue los comandos para la plantilla seleccionada. Puede introducir los comandos o importar los comandos existentes desde las plantillas de configuración

guardadas. También puede agregar varias plantillas de diferentes tipos en el editor de configuración mientras crea un trabajo en los trabajos de configuración. En la lista desplegable Origen de configuración, seleccione las diferentes plantillas y, a continuación, arrastre y suelte las plantillas en el editor de configuración. Los tipos de plantilla pueden ser plantilla de configuración, plantilla incorporada, configuración maestra, grabación y reproducción, instancia y archivo.

> **Nota**
>
> Si agrega la plantilla Implementar trabajo de configuración maestra por primera vez y, a continuación, agrega una plantilla de otro tipo, toda la plantilla de trabajo será del tipo Configuración maestra.

5. También puede reorganizar y reordenar los comandos en el editor de configuración. Puede mover el comando de una línea a otra arrastrando y soltando la línea de comandos. También puede mover o reorganizar la línea de comandos de una línea a cualquier línea de destino simplemente cambiando el número de línea de comandos en el cuadro de texto. También puede reorganizar y reordenar la línea de comandos más adelante mientras edita el trabajo de configuración.
6. Puede definir variables que le permitan asignar valores diferentes para estos parámetros o ejecutar un trabajo en varias instancias. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada. Haga clic en la pestaña Vista **previa de variables** para obtener una vista previa de las variables en una única vista consolidada que ha definido al crear o editar un trabajo de configuración.
7. En la pestaña **Seleccionar instancias** , seleccione las instancias en las que desea ejecutar la auditoría de configuración y haga clic en **Siguiente.**
8. En la ficha **Especificar valores de variable**, tiene dos opciones:
    a) Descargue el archivo de entrada para especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor NetScaler ADM.
    b) Introduzca valores comunes para las variables que ha definido para todas las instancias.
9. Haga clic en **Siguiente**.
10. Puede evaluar y verificar los comandos que se van a ejecutar en cada instancia en la pestaña Vista **previa del trabajo** . Para evaluar los comandos de reversión, seleccione la casilla de verificación Vista **previa de los comandos de reversión**
11. En la pestaña **Ejecutar** , elija ejecutar el trabajo ahora o programar la ejecución del trabajo más adelante. Además, también debe seleccionar qué acción debe realizar Citrix ADM si se produce un error en el comando.

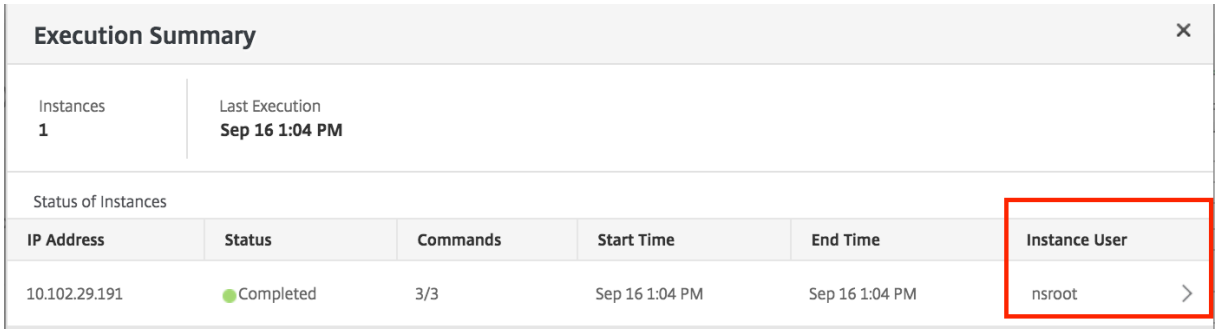
Para enviar una notificación por correo electrónico para un trabajo:

Ahora se envía una notificación por correo electrónico cada vez que se ejecuta o programa un trabajo. La notificación incluirá detalles como el éxito o el fracaso del trabajo, junto con los detalles pertinentes.

Tras crear un trabajo, en la pestaña Ejecutar, seleccione la casilla **Correo** electrónico en la sección Recibir un informe de ejecución mediante. Elija una lista de distribución de correo electrónico de la lista desplegable. También puede crear una lista de distribución de correo electrónico haciendo clic en el icono **+** y especificando los detalles del servidor de correo electrónico.

Para ver los detalles del resumen de ejecución:

Vaya a **Redes** > **Trabajos de configuración**. Selecciona un trabajo y haz clic en **Detalles** . Haga clic en **Resumen de ejecución** para ver el estado de la instancia en la que se ejecutó el trabajo, los comandos ejecutados en el trabajo, la hora de inicio y finalización del trabajo y el nombre del usuario de la instancia.



Usar grabación y reproducción para crear trabajos de configuración

January 30, 2024

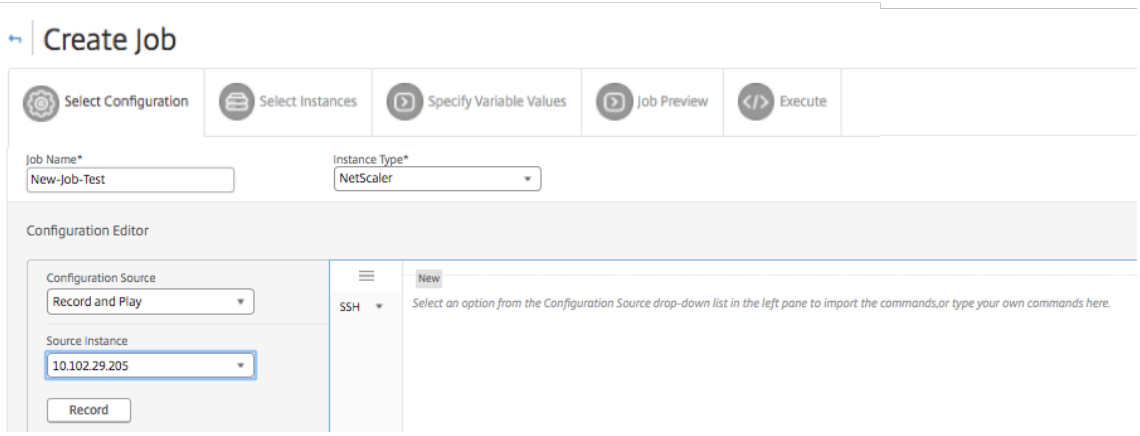
Si está acostumbrado a utilizar la GUI de NetScaler para configurar una instancia de NetScaler, a veces le resultará difícil recuperar los comandos de CLI exactos para crear una tarea de configuración y ejecutarla en varias instancias de NetScaler.

Citrix ADM le permite registrar las tareas de configuración realizadas mediante la GUI de una instancia de NetScaler y convertirlas en comandos de CLI. A continuación, puede crear una tarea de configuración a partir de estos comandos de CLI y ejecutar esta tarea en varias instancias.

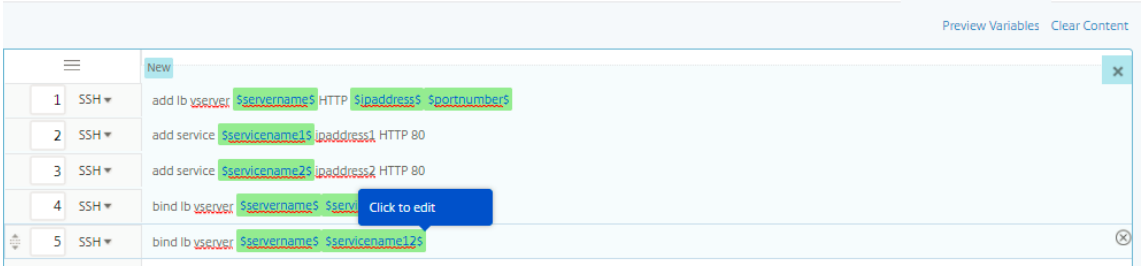
Para registrar la configuración de la interfaz gráfica de usuario y convertirla en una tarea de configuración

1. Vaya a **Redes > Trabajos de configuración** y, a continuación, haga clic en **Crear trabajo** .

2. Especifique el nombre del trabajo y el tipo de instancia.
3. En la lista de **fuentes de configuración**, seleccione **Grabar y reproducir**y, a continuación, seleccione la instancia de origen desde la que quiere grabar la configuración. Haga clic en **Grabar**.



4. Se abre la **GUI de NetScaler**. Configure las funciones y los valores que quiere que contenga la tarea de configuración. A continuación, cierre la ventana GUI de NetScaler y haga clic en **Detener** en el **Editor de configuración**. Los comandos aparecen como un vínculo en el panel izquierdo. Arrastre y suelte los comandos en el panel derecho y, a continuación, haga clic en **Siguiente**.



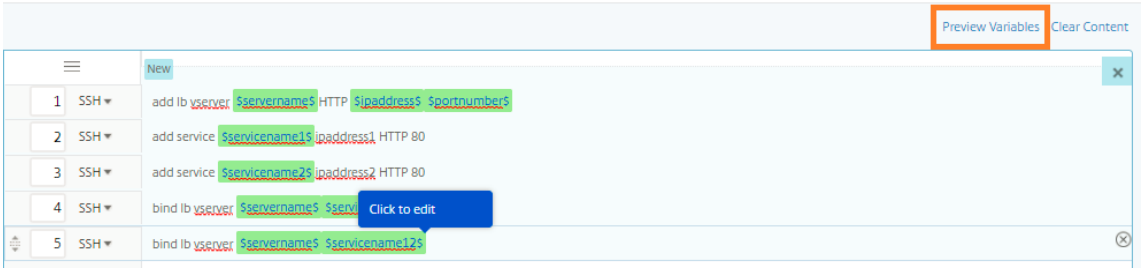
A continuación, puede reorganizar y reordenar los comandos en el editor de configuración según corresponda. Puede mover el comando de una línea a otra arrastrando y soltando la línea de comandos. También puede mover o reorganizar la línea de comandos de una línea a cualquier línea de destino simplemente cambiando el número de línea de comandos en el cuadro de texto.

5. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
6. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:

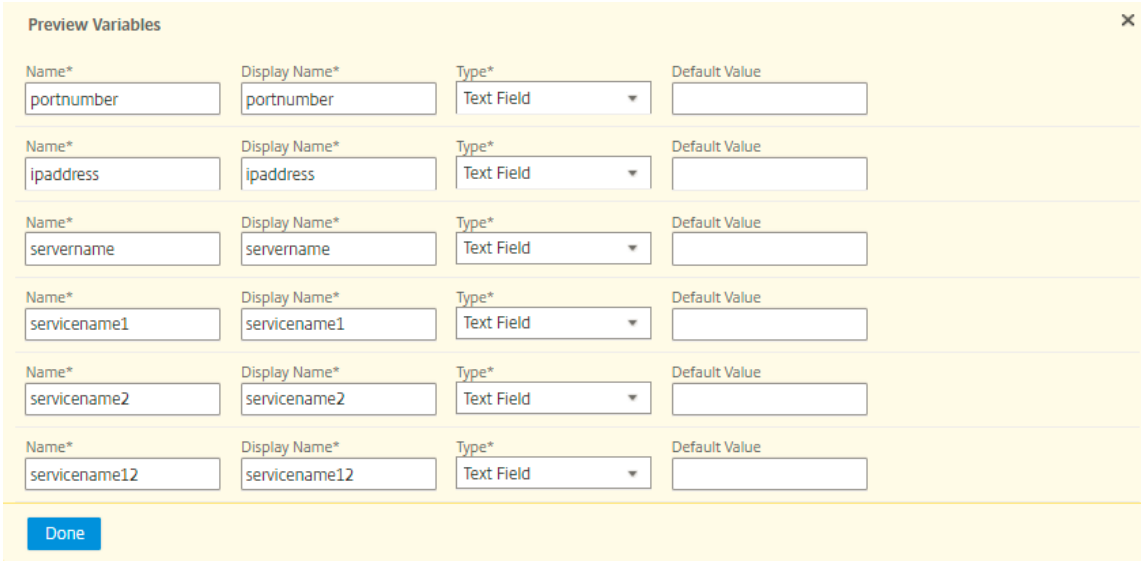
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.

- Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.

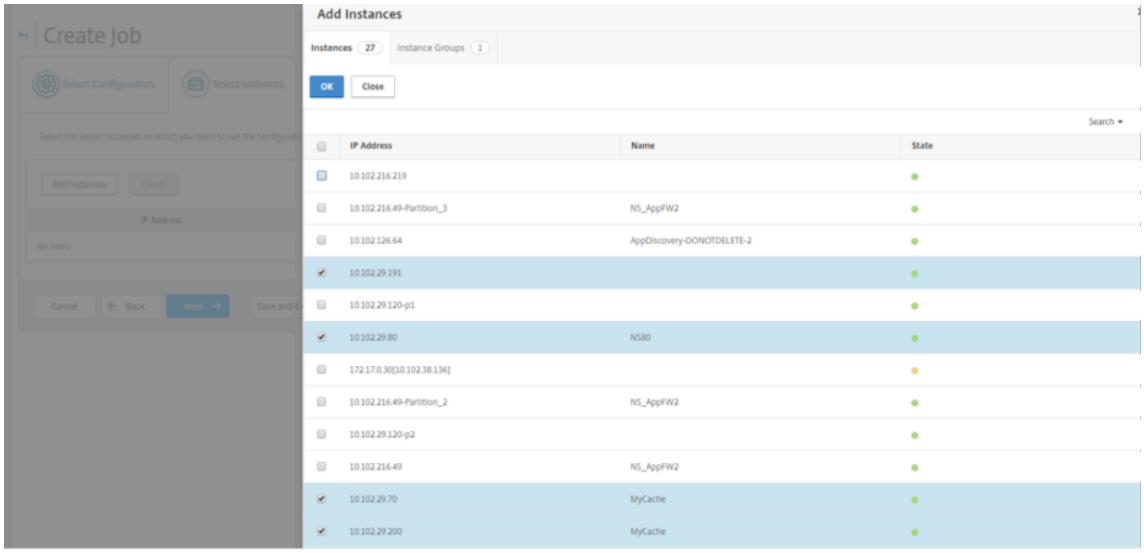
7. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que definió al crear o editar un trabajo de configuración.



8. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.



9. Haga clic en**Agregar instancias**y seleccione las instancias en las que desee ejecutar el trabajo de configuración. Haga clic en**Aceptar**y, a continuación, en**Siguiente**.



10. Si ha especificado variables en los comandos, en la ficha **Especificar valores de variable**, seleccione una de las siguientes opciones para especificar variables para las instancias:

    - **Cargar archivo de entrada para valores de variables:** haga clic en **Descargar archivo de claves** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca valores para las variables definidas en los comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
    - **Valores de variables comunes para todas las instancias**: introduzca valores para las variables. Las variables varían en función de la plantilla seleccionada.

    Los archivos de entrada que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

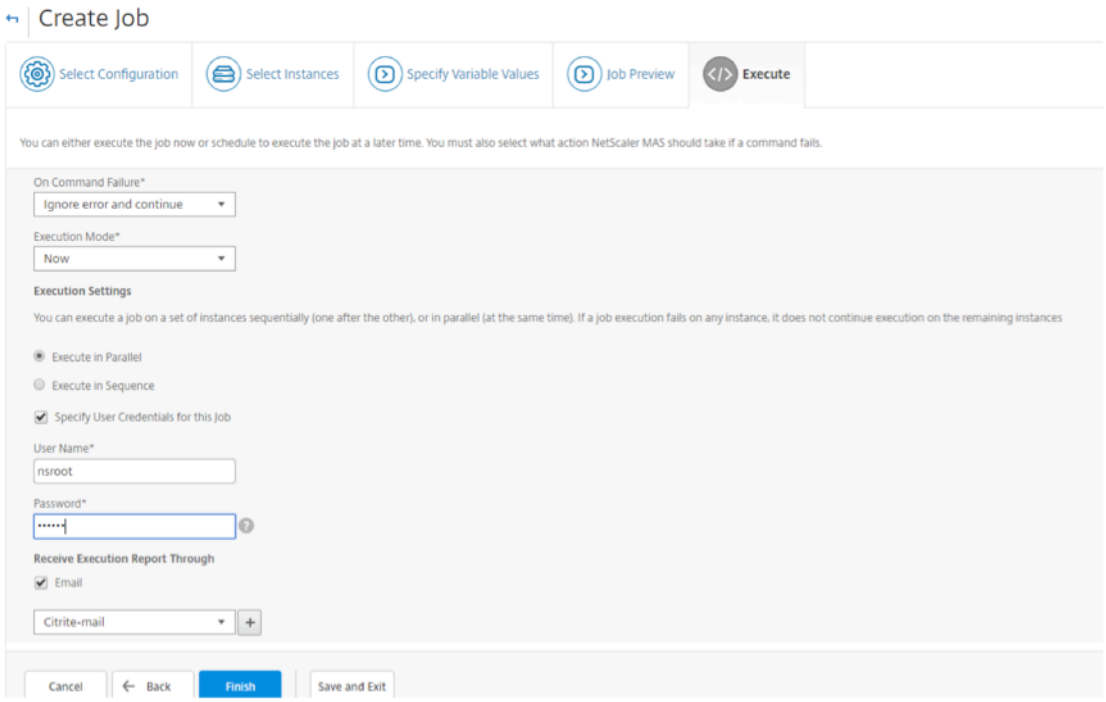
    Para ver los trabajos de configuración ejecutados al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear trabajo**. En la página **Crear trabajo**. En la ficha **Especificar valores de variables**, seleccione la opción **Valores de variables comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

    Para ver los trabajos de configuración ya ejecutados mientras se modifica un trabajo de configuración, vaya a **Red > Trabajos de configuración**, seleccione el nombre del trabajo y haga clic en **Modificar**. En la página **Configurar Trabajo**, en la ficha **Especificar Valores de Variable**, seleccione la opción **Valores de Variable Comunes para todas las Instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).10.En la

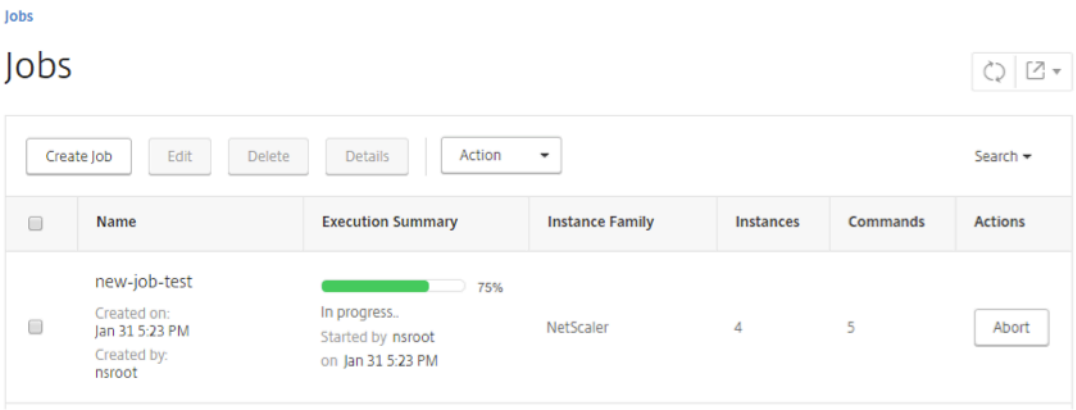
ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

11. En la ficha**Vista previa del trabajo**, puede evaluar y verificar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
12. En la ficha**Ejecutar**, puede elegir ejecutar su trabajo ahora o programarlo para que se ejecute más adelante. También puede elegir qué acción debe realizar Citrix ADM si se produce un error en el comando.

    También puede optar por permitir que los usuarios autorizados ejecuten trabajos en sus instancias administradas y elegir si deseas enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo, junto con otros detalles.



13. En la página **Trabajos**, puede ver el progreso de la ejecución de la tarea de configuración en todas las instancias.



Utilizar trabajos de configuración para replicar la configuración de una instancia a varias instancias

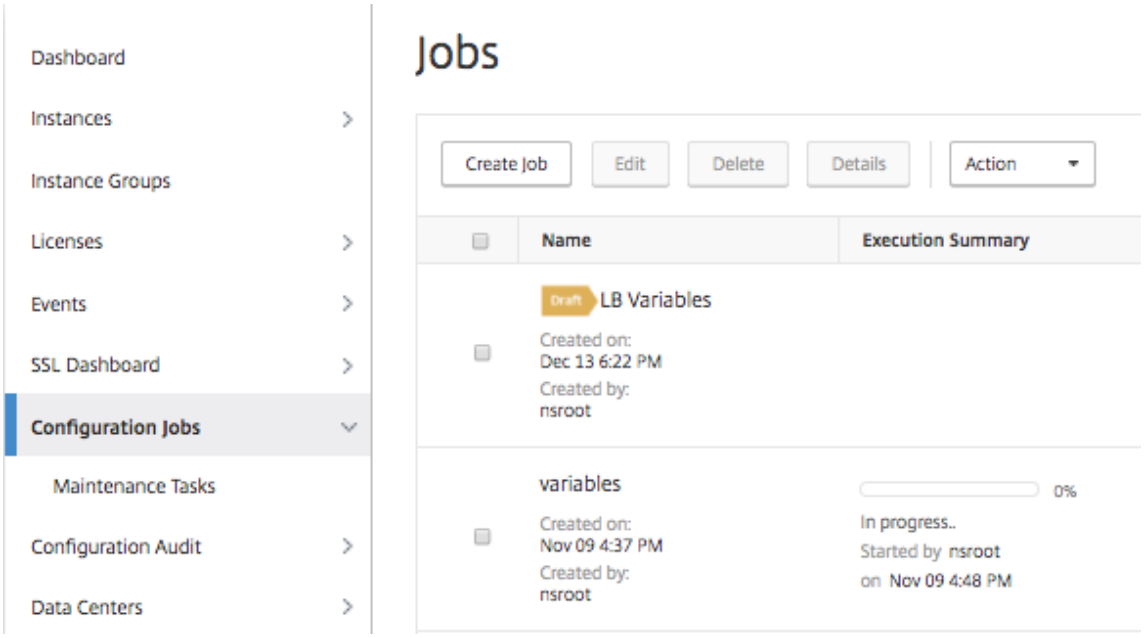
January 30, 2024

Puede utilizar la función Configuration Jobs de Citrix ADM para extraer una configuración concreta de una instancia de NetScaler y replicarla en varias instancias.

Por ejemplo, es posible que haya configurado el equilibrio de carga y la optimización de interfaz (FEO) en una instancia de NetScaler para su implementación. Sin embargo, ahora solo quiere replicar la configuración de FEO en otras instancias de NetScaler.

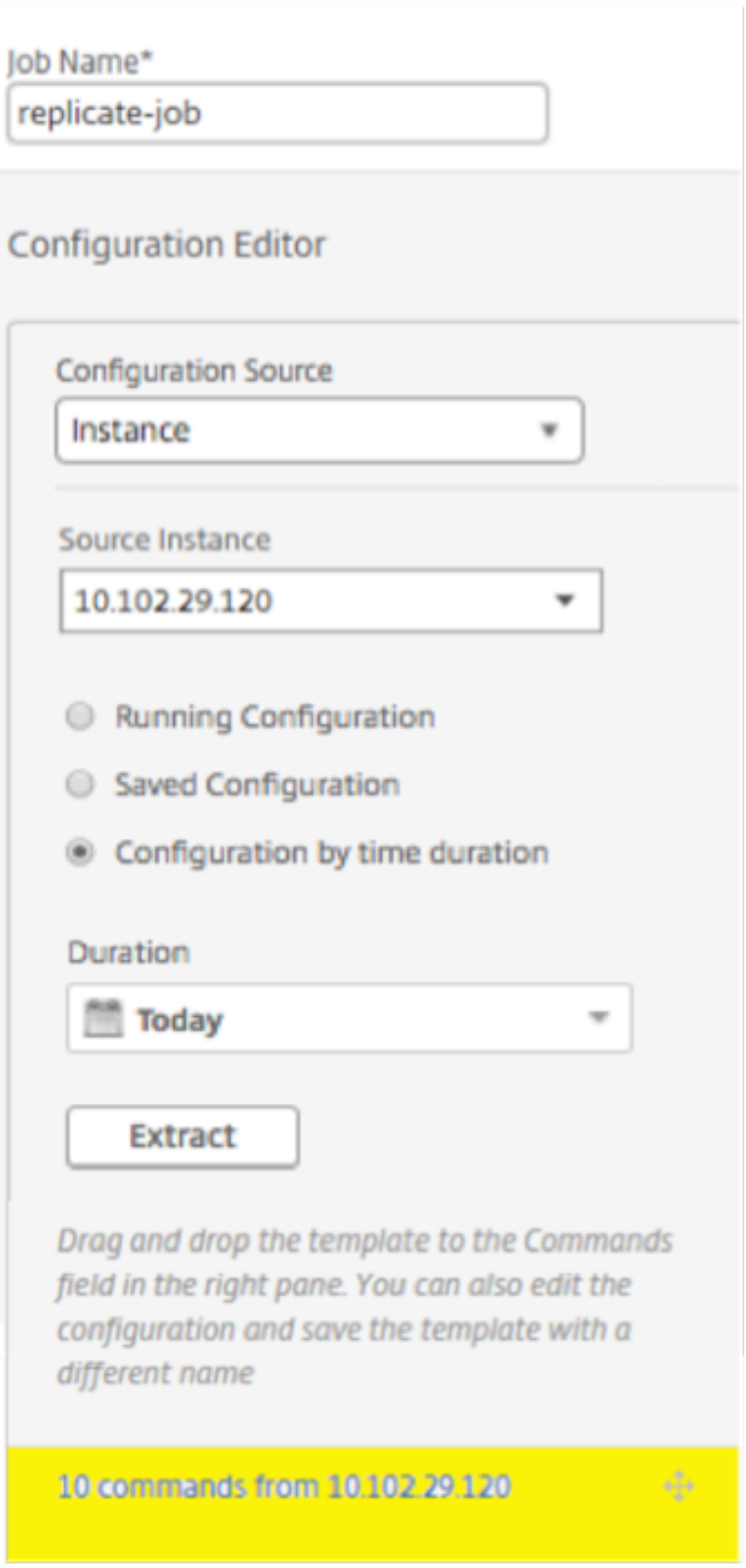
Para recuperar y replicar la configuración de una instancia a otras instancias de NetScaler:

1. Vaya a **Redes** > **Trabajos de configuración** y, a continuación, haga clic en **Crear trabajo**.



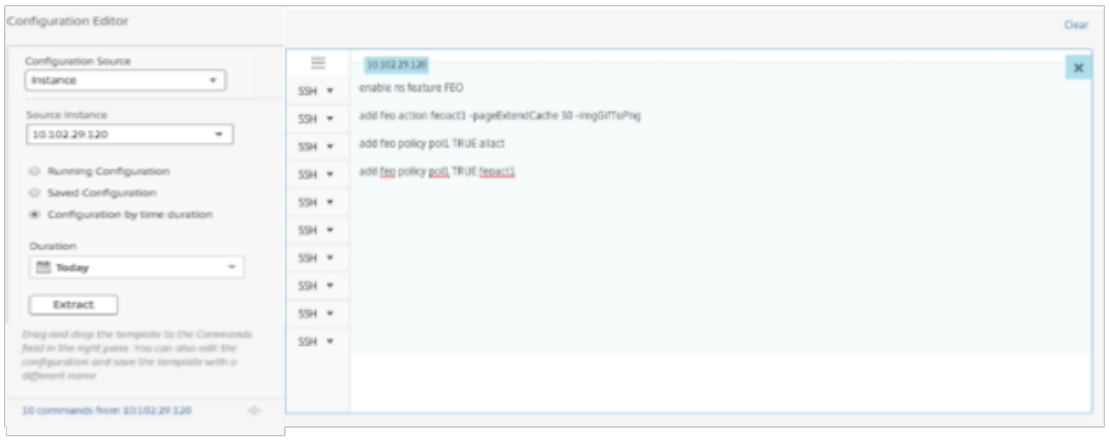
2. Especifique el nombre del trabajo y el tipo de instancia.
3. Seleccione **Instancia** como **fuente de configuración** y seleccione la instancia de origen cuya configuración quiere replicar. Seleccione el tipo de configuración que quiere extraer. Si selecciona la opción "Configuración por duración de tiempo", establezca el período de tiempo en el que ejecutó esta configuración y, a continuación, haga clic en **Extraer**.

   El número de comandos ejecutados en esa instancia durante el tiempo que ha seleccionado se muestra en la pantalla, tal como se resalta en la imagen siguiente.



4. Arrastre y suelte los **comandos en el campo Comandos** del panel derecho.

Mantenga solo los comandos relacionados con FEO y elimine manualmente los comandos relacionados con el equilibrio de carga o los comandos relacionados con cualquier otra configuración y, a continuación, haga clic en **Siguiente**.



5. Haga clic en **Agregar instancias** y agregue las instancias en las que quiere aplicar la configuración FEO. Haga clic en **Aceptar**y, a continuación, en **Siguiente**.
6. Si ha especificado variables en los comandos, en la pestaña Especificar valores de variables, haga clic en **Descargar archivo de claves** de entrada . En el archivo descargado, especifique los valores de las variables y, a continuación, cargue el archivo a Citrix ADM.
7. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
8. En la ficha **Ejecutar**, haga clic en **Finalizar** para ejecutar el trabajo en las instancias de NetScaler seleccionadas.

Usar variables en trabajos de configuración

January 30, 2024

Un trabajo de configuración es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Al ejecutar la misma configuración en varias instancias, es posible que desee utilizar valores diferentes para los parámetros utilizados en la configuración. Puede definir variables que le permitan asignar valores diferentes para estos parámetros o ejecutar un trabajo en varias instancias.

Por ejemplo, considere una configuración básica de equilibrio de carga en la que agregue un servidor virtual de equilibrio de carga, agregue dos servicios y vincule los servicios al servidor virtual. Ahora, es posible que quiera tener la misma configuración en dos instancias, pero con valores diferentes para los nombres y direcciones IP del servidor y los servicios virtuales. Puede utilizar la función de trabajos de configuración para lograrlo mediante variables para definir los nombres y las direcciones IP del servidor y los servicios virtuales.

En este ejemplo, se utilizan los siguientes comandos y variables:

add lb vserver **servername** HTTP **ipaddress portnumber**

add service **servicename1 ipaddress1** HTTP 80

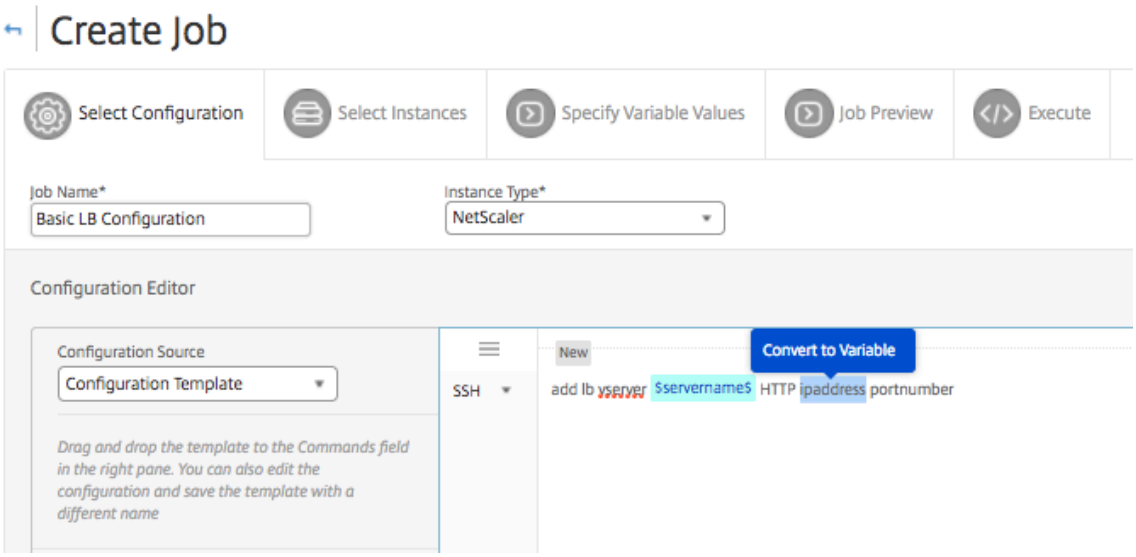
agregar servicio **servicename2 ipaddress2** HTTP 80

bind lb vserver **servername servicename1**

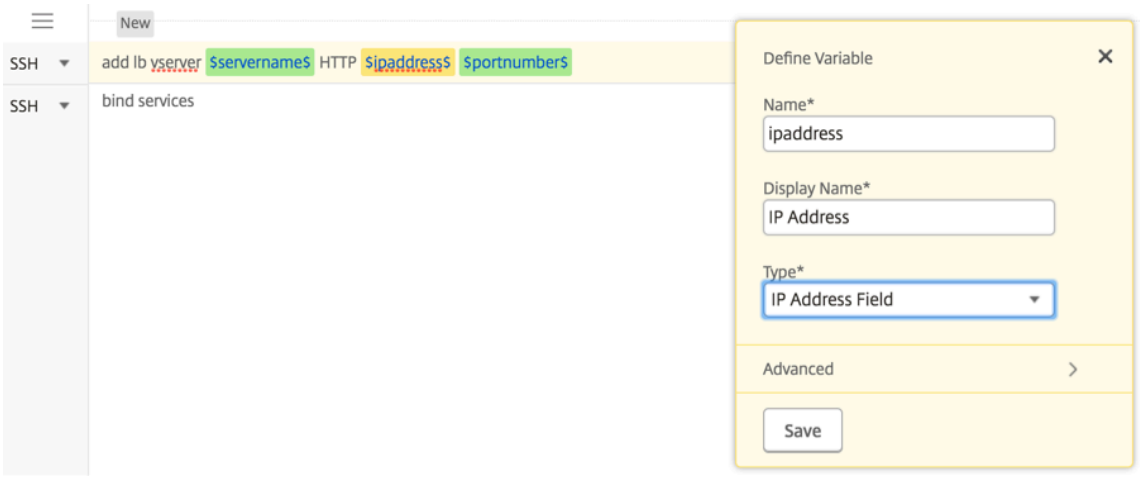
bind lb vserver **servername servicename2**

Para crear un trabajo de configuración definiendo variables en Citrix ADM:

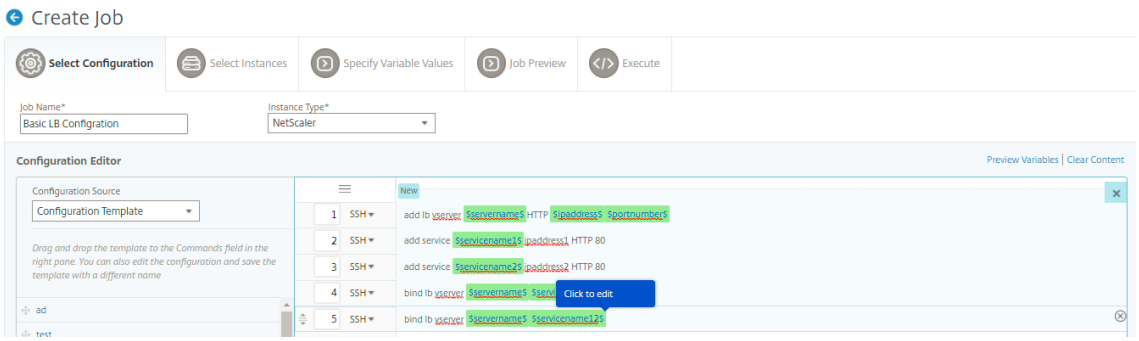
1. Vaya a **Redes** > **Trabajos de configuración**.
2. Haga clic en **Crear trabajo**.
3. En la página **Crear trabajo**, seleccione los parámetros personalizados del trabajo, como el nombre del trabajo, el tipo de instancia y el tipo de configuración.
4. En el Editor de configuración, escriba los comandos para agregar un servidor virtual de equilibrio de carga, dos servicios y enlazar los servicios al servidor virtual. Haga doble clic para seleccionar los valores que desee convertir en una variable y, a continuación, haga clic en **Convertir en variable**. Por ejemplo, seleccione la dirección IP de la *dirección IP*del servidor de equilibrio de carga y haga clic en **Convertir en variable** como se muestra en la imagen siguiente.



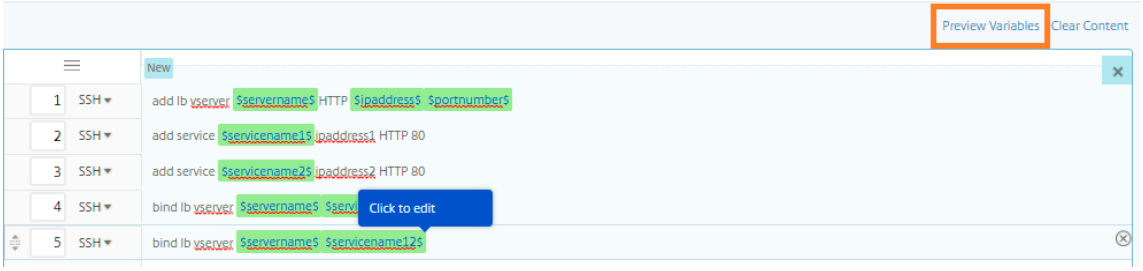
5. Cuando vea los signos del dólar que encierran el valor de la variable, haga clic en la variable para especificar con más detalle los detalles de la variable, como el nombre, el nombre para mostrar y el tipo. También puede hacer clic en la opción **Avanzado** si quiere especificar un valor predeterminado para la variable. Haga clic en **Guardar** y, a continuación, haga clic en **Siguiente**.



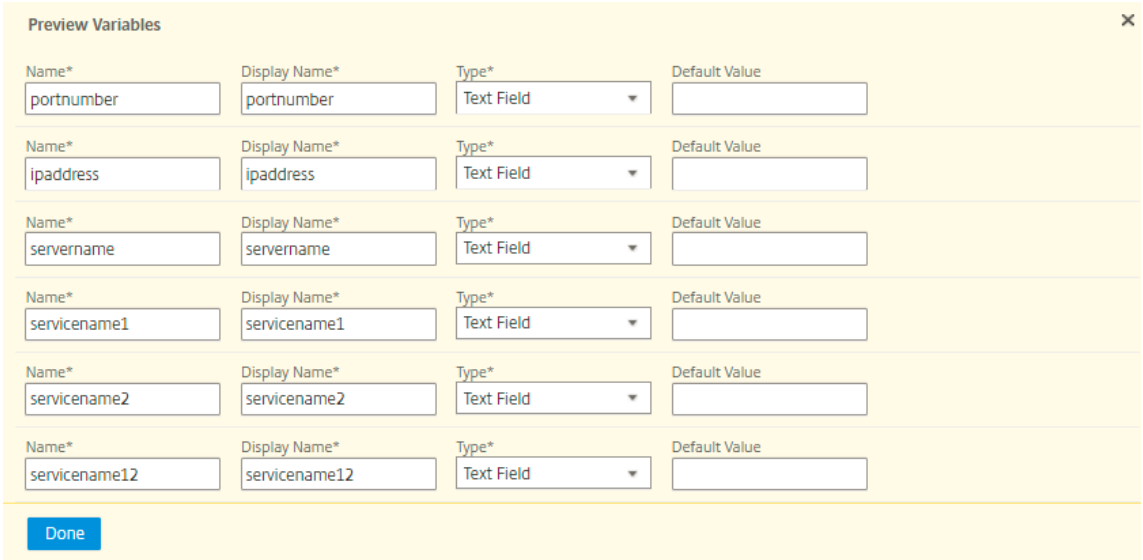
Escriba el resto de sus comandos y defina todas las variables.



6. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
7. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.
8. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que definió al crear o editar un trabajo de configuración.



9. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.



10. A continuación, puede reorganizar y reordenar los comandos en el editor de configuración

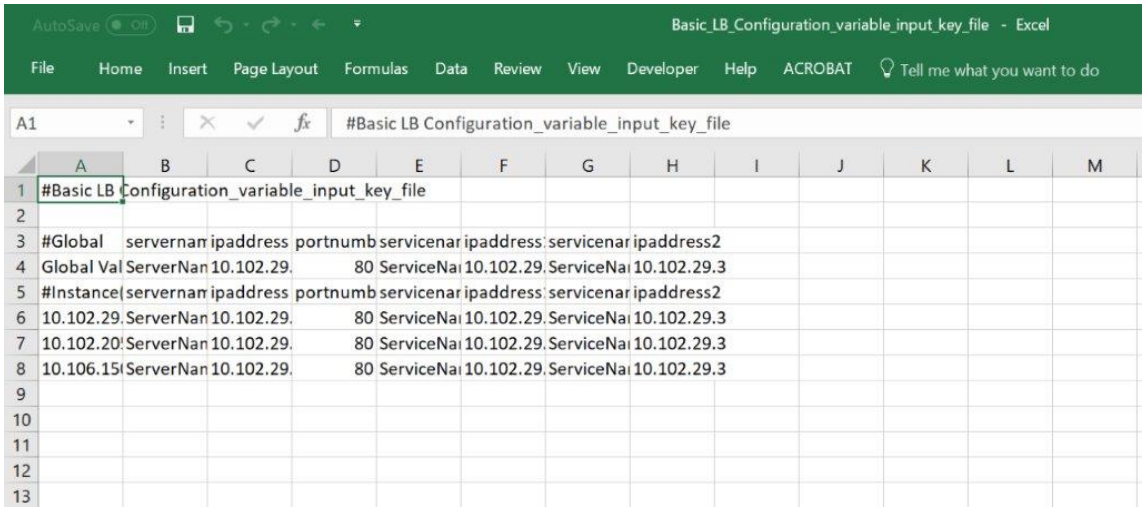
según corresponda. Puede mover el comando de una línea a otra arrastrando y soltando la línea de comandos. También puede mover o reorganizar la línea de comandos de una línea a cualquier línea de destino simplemente cambiando el número de línea de comandos en el cuadro de texto.

11. Seleccione las instancias en las que quiere ejecutar el trabajo de configuración.
12. En la ficha **Especificar valores variables**, seleccione la opción **Cargar archivo de entrada para valores variables**y, a continuación, haga clic en **Descargar archivo clave de entrada**. En nuestro ejemplo, deberá especificar el nombre del servidor en cada instancia, las direcciones IP del servidor y los servicios, los números de puerto y los nombres de servicio. Guarde el archivo y cárguelo. Si sus valores no están definidos con precisión, el sistema podría generar un error.
13. El archivo de claves de entrada se descarga en el sistema local y puede editarlo especificando los valores de las variables de cada instancia de NetScaler que haya seleccionado anteriormente y haciendo **clic en** Cargar para cargar el archivo de claves de entrada en Citrix ADM. Haga clic en **Siguiente**. El archivo de clave de entrada se descarga en su sistema local y puede modificarlo especificando los valores de las variables para cada instancia de NetScaler que haya seleccionado anteriormente.

    > **Nota** En el archivo de clave de entrada, las variables se definen en tres niveles:
    >
    > - Nivel mundial
    > - Nivel de grupo de instancias
    > - Nivel de instancia

    Las variables globales son valores variables que se aplican a todas las instancias. Los valores de las variables de nivel de grupo de instancias se aplican a todas las instancias que se definen en un grupo. Los valores de las variables de nivel de instancia solo se aplican a una instancia específica.

    Citrix ADM da la primera prioridad a los valores a nivel de instancia. Si no se proporcionan valores a las variables de las instancias individuales, Citrix ADM utiliza el valor proporcionado a nivel de grupo. Si no se proporcionan valores a nivel de grupo, Citrix ADM utiliza el valor de la variable proporcionado a nivel global. Si proporciona una entrada para una variable en los tres niveles, Citrix ADM utiliza el valor de nivel de instancia como valor predeterminado.
14. Haga clic en **Cargar** para cargar el archivo de claves de entrada en Citrix ADM. Haga clic en **Siguiente**.



> **Importante**
>
> Cuando carga un archivo CSV desde un Mac, Mac almacena el archivo CSV con punto y coma en lugar de comas. Esto hará que la configuración falle al cargar el archivo de entrada y ejecutar el trabajo. Si está utilizando un Mac, utilice un editor de texto para realizar los cambios necesarios y, a continuación, cargue el archivo.

15. También puede proporcionar valores de variable comunes en todas las instancias y hacer clic en **Cargar**para cargar el archivo de clave de entrada en Citrix ADM.

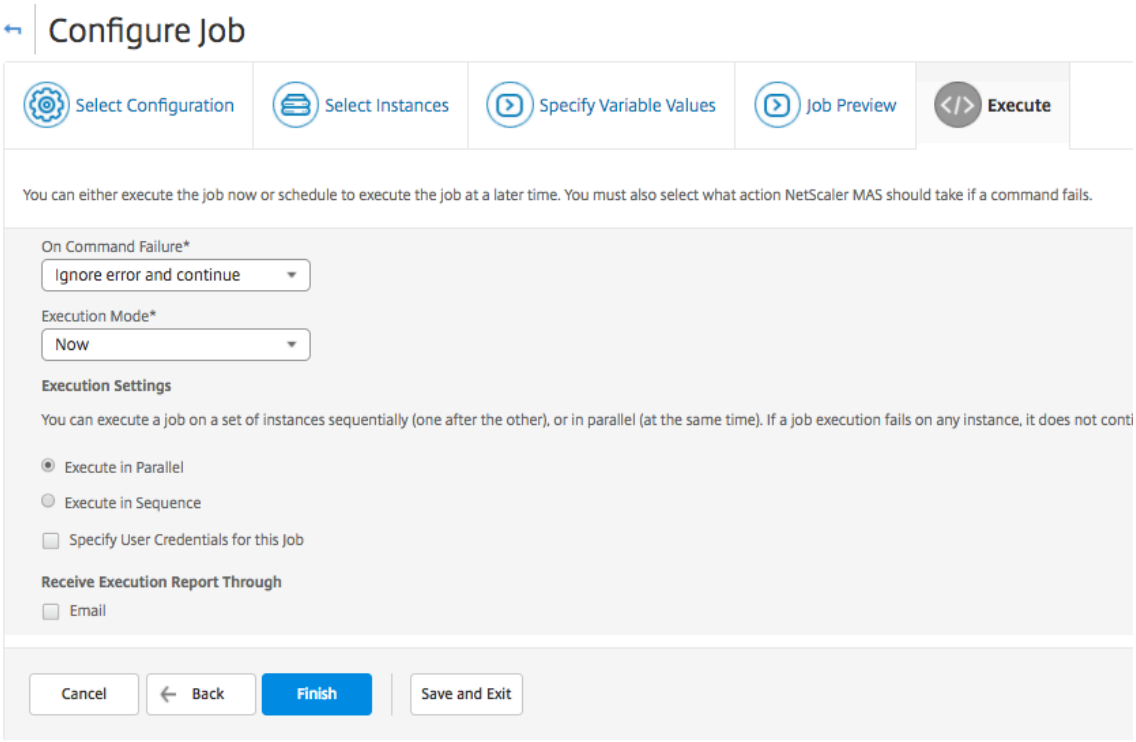
    Los archivos de entrada clave que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

    Para ver los trabajos de configuración ejecutados al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear trabajo**. En la página **Crear trabajo**. En la ficha **Especificar valores de variables**, seleccione la opción **Valores de variables comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

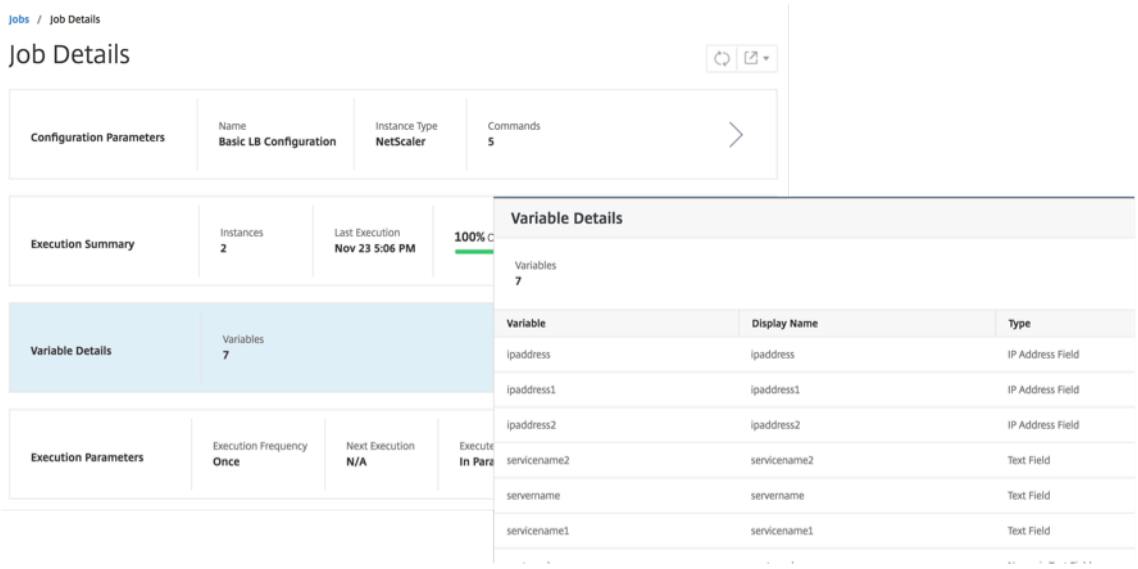
    Para ver los trabajos de configuración ya ejecutados mientras se modifica un trabajo de configuración, vaya a **Red > Trabajos de configuración**, seleccione el nombre del trabajo y haga clic en **Modificar**. En la página **Configurar Trabajo**, en la ficha **Especificar Valores de Variable**, seleccione la opción **Valores de Variable Comunes para todas las Instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

16. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

17. En la ficha **Ejecutar**, puede elegir ejecutar su trabajo ahora o programarlo para que se ejecute más adelante. También puede elegir qué acción debe realizar Citrix ADM si el comando falla y si quiere enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo junto con otros detalles.



Tras configurar los trabajos y ejecutarlos, puede ver los detalles del trabajo navegando hasta **Redes** > **Trabajos de configuración y seleccionando** el trabajo que acaba de configurar. Haga clic en **Detalles** y, a continuación, haga clic en **Detalles de variables** para ver la lista de variables añadidas a su trabajo.



> **Nota**
>
> Citrix ADM conserva los valores que ha proporcionado para las variables en **PASO 5** al guardar el trabajo y salir, o al programar la ejecución de un trabajo en un momento posterior.

Crear trabajos de configuración a partir de comandos correctivos

January 30, 2024

Puede utilizar la función de plantilla de auditoría de Citrix Application Delivery Management (ADM) para supervisar los cambios de configuración en las instancias administradas de Citrix ADC y solucionar errores de configuración.

El flujo de trabajo típico para auditar los cambios de configuración mediante plantillas de auditoría consiste en los siguientes pasos:

1. Cree una plantilla de auditoría con un conjunto de comandos Citrix ADC válidos o esperados para auditar las configuraciones de instancias.
2. Seleccione las instancias de Citrix ADC en las que quiere ejecutar la plantilla de auditoría para comprobar si existen diferencias entre la configuración en ejecución y las configuraciones esperadas.
3. Comprenda los comandos diferenciales y correctivos y utilice la función "Crear tarea"para llevar las configuraciones de la instancia al estado deseado

Considere un caso en el que varios administradores administran cinco instancias de Citrix ADC. Todos estos administradores actualizan la configuración de la instancia existente a medida que se necesitan cambios. El superadministrador quiere asegurarse de que un determinado conjunto de configuraciones importantes permanece intacto independientemente de los cambios realizados por otros administradores. Para este caso de uso, el superadministrador crea una plantilla de la configuración que se espera que esté presente en las instancias de Citrix ADC y la ejecuta en las instancias. Citrix ADM compara la configuración de la plantilla de auditoría con la configuración en ejecución e informa de cualquier discrepancia en el panel **de auditoría de configuración**.

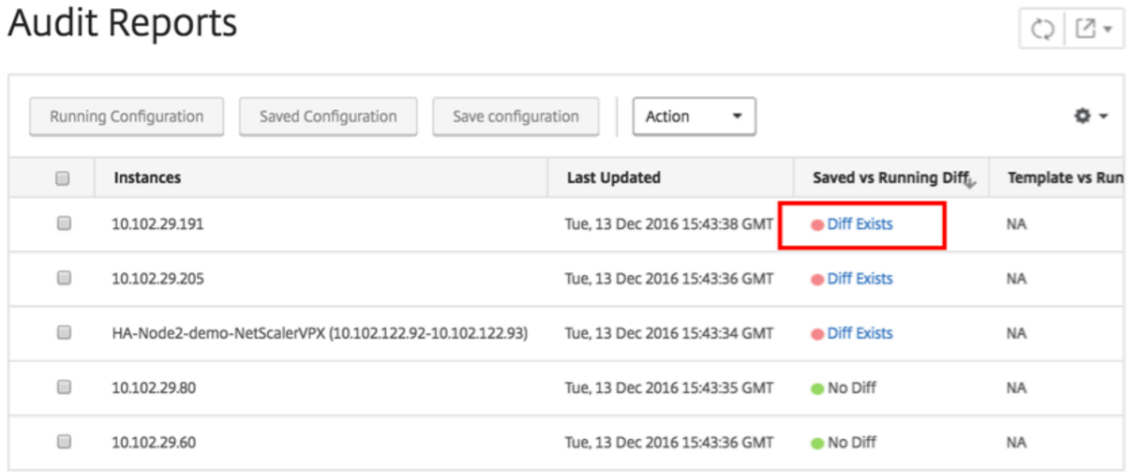
Si observa que hay un cambio en la configuración de algunas instancias, puede usar la función de comandos correctivos de Citrix ADM para crear un trabajo de configuración con los comandos de configuración modificados y corregidos para instancias específicas de Citrix ADC.

Si existe alguna diferencia entre la configuración de la plantilla de auditoría y la configuración en ejecución, aparecerá un mensaje de estado **Diff Exists** en la página **Informe de auditoría**. Al hacer clic

en el enlace **Diff Exits** , accederá a la página **Configuration Diff** , donde podrá ver el comando correctivo. También puede utilizar estos comandos correctivos para crear un trabajo de configuración y ejecutarlo en las instancias específicas de Citrix ADC para que vuelvan a la configuración deseada.

Para crear un trabajo de configuración a partir de comandos correctivos en Citrix ADM

1. Vaya a **Redes** > **Auditoría de configuración**.
2. En la página **Auditoría de configuración**, haga clic dentro de cualquiera de los dos gráficos de donut para acceder a la página **Informes de auditoría**.
3. Haga clic en el enlace **Diff Exists(en la columna Diferencia entre guardados y en ejecución**de la tabla) de la instancia para la que quiera corregir los comandos de configuración. Aparecerá la página**Configuración Diff**, en la que se enumeran las diferencias entre la configuración guardada, la configuración en ejecución y la configuración de corrección para esa instancia.



4. Haga clic en **Crear Trabajo** para ir a la página **Crear Trabajo**, en la que se rellenan los comandos correctivos. Para obtener instrucciones sobre cómo crear un trabajo de configuración, consulte Cómo crear un trabajo de configuración en Citrix ADM.

Replicar la configuración en ejecución y guardada de una instancia de NetScaler a otra

January 30, 2024

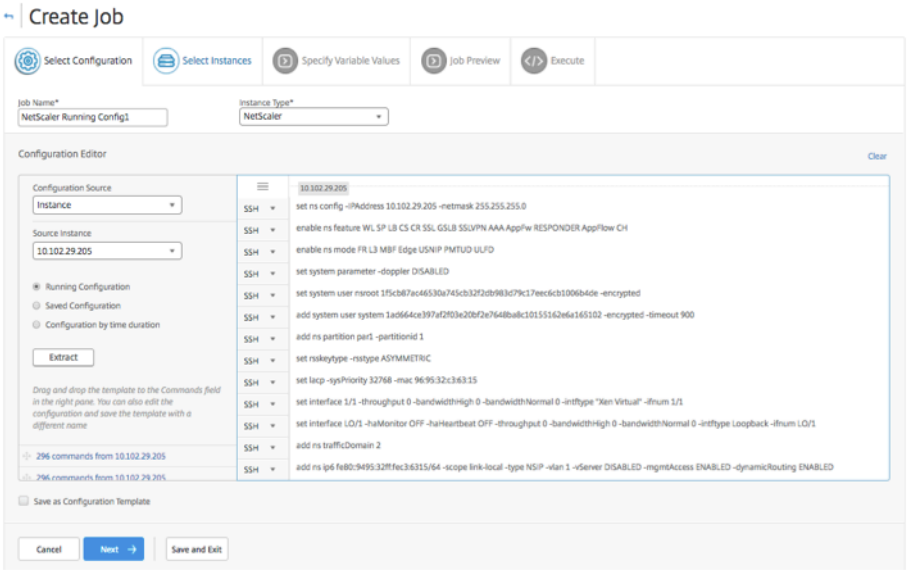
24 de mayo de 2018

Ahora puede replicar la configuración de una instancia de NetScaler en otras instancias. Cuando configure un trabajo en Citrix ADM, seleccione una instancia como origen de configuración y elija la configuración en ejecución o guardada de la instancia seleccionada.

Por ejemplo, cuando selecciona **Ejecutar configuración** y hace clic en **Extraer**, Citrix ADM envía una solicitud a la instancia de NetScaler seleccionada para localizar la configuración en ejecución y la muestra como una plantilla. Puede arrastrar y soltar la plantilla en el campo **Comandos** del panel derecho. Puede modificar los comandos, los parámetros y las instancias.

Para replicar comandos de configuración en ejecución y guardados de una instancia en otra instancia en Citrix ADM:

1. Vaya a **Redes** > **Trabajos de configuración**y haga clic en **Crear trabajo**.
2. Especifique el nombre del trabajo y el tipo de instancia. Por ejemplo, especifique *NetScaler Running Config1* como nombre de su trabajo y el tipo de instancia como *NetScaler*.
3. Seleccione **Instancia** como **Origen de configuración**, seleccione la instancia de origen cuya configuración quiere replicar en otras instancias.
4. Verás las tres opciones siguientes:
    - Ejecución de la configuración
    - Configuración guardada
    - Configuración por duración de tiempo
5. Seleccione **Configuración en ejecución**y haga clic en **Extraer**. Se muestra el número de comandos de configuración en ejecución ejecutados en esa instancia.



6. Arrastre y suelte los **comandos en el campo Comandos** del panel derecho.
7. Puede modificar los comandos en el campo Comandos. Por ejemplo, si los comandos extraídos van a configurar una instancia de NetScaler. Esto puede incluir agregar particiones, configurar el equilibrio de carga, vincular el servidor de equilibrio de carga a los servicios, etc. Es posible que quiera modificar los comandos para configurar las nuevas instancias de NetScaler sin particiones. Por lo tanto, para eliminar particiones, elimine manualmente los comandos relacionados con la creación de particiones y haga clic en **Siguiente**.
8. Haga clic en **Agregar instancias** y agregue las instancias en las que quiera aplicar los comandos de configuración en ejecución. Haga clic en **Aceptar** y, a continuación, en **Siguiente**.
9. Si ha especificado variables en los comandos, en la pestaña **Especificar valores** de variables , haga clic en **Descargar archivo de claves** de entrada . En el archivo descargado, especifique los valores de las variables y, a continuación, cargue el archivo a Citrix ADM.
10. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

11. En la ficha **Ejecutar**, puede elegir ejecutar su trabajo ahora o programarlo para que se ejecute más adelante. También puede elegir qué acción debe realizar Citrix ADM en caso de que el comando falle y si quiere enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo junto con otros detalles.

Reutilizar trabajos de configuración ejecutados

January 30, 2024

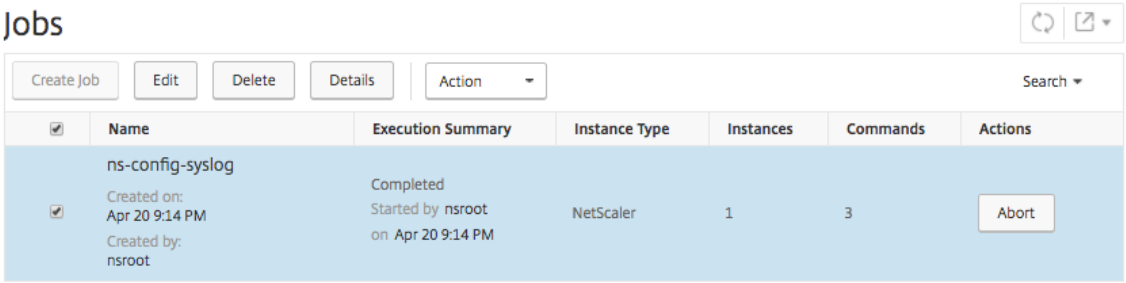
Los trabajos de configuración le permiten crear un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. También puede ejecutar el mismo conjunto de trabajos de configuración guardados después de modificar los comandos, los parámetros, el origen de configuración y las instancias del trabajo. Esto resulta útil cuando se deben ejecutar los mismos conjuntos de comandos en una instancia diferente o cuando el trabajo detecta un error y detiene la ejecución posterior.

Citrix Application Delivery Management (ADM) proporciona una función para volver a ejecutar los trabajos completados. Con esta función, los trabajos que se ejecutan por completo pueden volver a ejecutarse sin cambiar el nombre del trabajo.

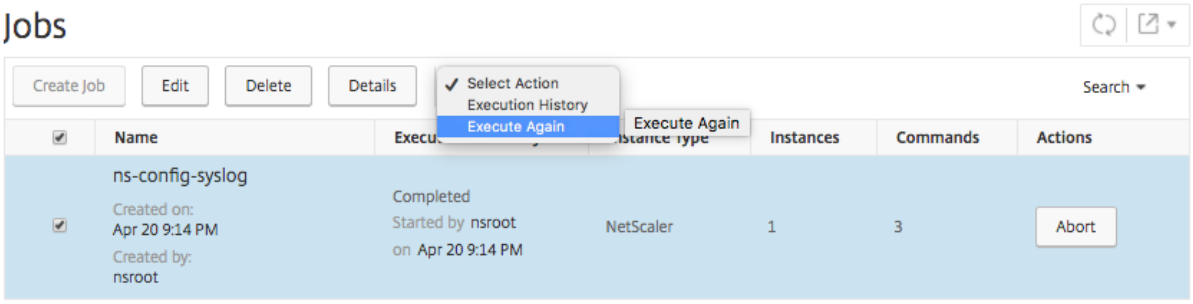
> **Nota** Solo puede volver a ejecutar los trabajos que se ejecutan cuando el modo de ejecución es «Ahora».

Para modificar trabajos completados:

1. Desde la página principal de Citrix ADM, vaya a **Redes > Trabajos de configuración**.
2. En la página **Trabajos**, seleccione un trabajo que muestre el resumen de ejecución como completado y haga clic en **Modificar**. También puede modificar un trabajo de configuración programado.
3. En la página **Configurar trabajo**, puede ver que el nombre del trabajo y el tipo de instancia no son modificables. Puede modificar otros campos, como la fuente de configuración, agregar instancias, modificar los valores de las variables y establecer los ajustes de ejecución.
4. Haga clic en **Finalizar** para ejecutar de nuevo el trabajo de configuración.



> **Nota**
>
> También puede seleccionar el trabajo y volver a hacer clic en **Ejecutar** para ejecutar el trabajo sin modificar ningún origen, instancia ni comando. Esto es útil cuando tiene que ejecutar el mismo conjunto de comandos en las mismas instancias. A veces, el trabajo puede encontrar un error transitorio desde el lado del servidor y es posible que tenga que volver a ejecutar el trabajo.



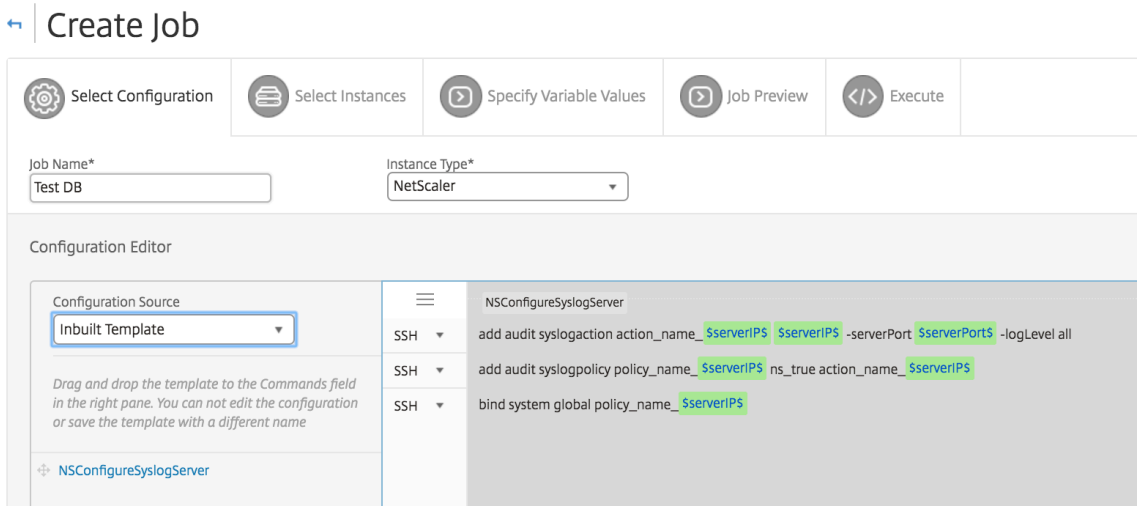
Programar trabajos creados mediante plantillas integradas

January 30, 2024

Puede programar un trabajo mediante la opción de plantilla integrada. Un trabajo es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Por ejemplo, utilice la opción de plantilla integrada para programar un trabajo para configurar servidores syslog. También puede optar por ejecutar el trabajo inmediatamente o programar el trabajo para que se ejecute en una etapa posterior.

Para programar un trabajo mediante plantillas integradas en Citrix Application Delivery Management (ADM)

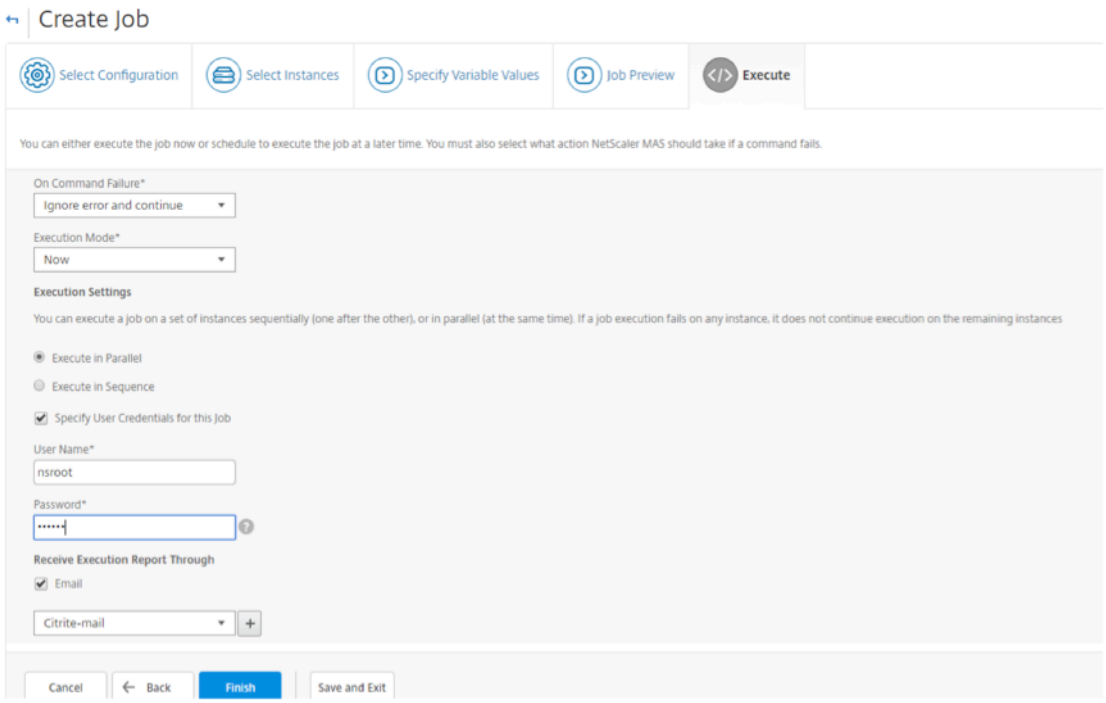
1. En Citrix ADM, vaya a **Redes** > **Trabajos de configuración**y, a continuación, haga clic en **Crear**trabajo.
2. En la página **Crear Trabajo**, en la ficha **Seleccionar Configuración**, especifique el **Nombre del Trabajo** y seleccione el **Tipo de Instancia** en la lista desplegable.
3. Seleccione **Plantilla incorporada** en la lista desplegable **Origen de configuración**. Arrastre y suelte el comando ***NSConfigureSyslogServer** en el panel derecho y, a continuación, haga clic en **Siguiente**.



4. En la ficha **Seleccionar instancias**, haga clic en **Agregar instancias**, seleccione las instancias en las que quiere ejecutar el trabajo y, a continuación, haga clic en **Aceptar**.
5. Haga clic en **Siguiente**. En la ficha **Especificar valores variables**, seleccione una de las siguientes opciones para especificar las variables de sus instancias:
   - **Valores de variables de un archivo de entrada**: Descargue un archivo de entrada para introducir valores para las variables que ha definido en los comandos. A continuación, cargue el archivo en el servidor Citrix ADM.
   - **Valores de variables comunes para todas las instancias**: Especifique la dirección IP y el puerto del servidor syslog.
6. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
7. Haga clic en **Siguiente**.
8. En la ficha **Ejecutar**, defina las siguientes condiciones:
   - **En caso de error** de comando: si se produce un error en un comando, puede optar por ignorar los errores y continuar con la ejecución del trabajo o detener la ejecución posterior del mismo. Elija la acción que quiere ejecutar en la lista desplegable.
   - **Modo de ejecución** : puede ejecutar el trabajo ahora o programar la ejecución del trabajo más adelante. Si quiere programar el trabajo más adelante, debe especificar la configuración de frecuencia de ejecución para ese trabajo. Elija el cronograma que quiere que siga el trabajo en la lista desplegable.
9. También puede ejecutar un trabajo en un conjunto de instancias de forma secuencial o en paralelo seleccionando el método necesario en **Configuración de ejecución**. Si se produce un error en la ejecución de un trabajo en cualquier instancia, no continúa en las instancias restantes.

Puede elegir permitir que los usuarios autorizados ejecuten trabajos en sus instancias administradas. También se puede enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo, junto con otros detalles.

10. Haga clic en **Finalizar**.



Utilizar trabajos de mantenimiento para actualizar instancias de NetScaler SDX

January 30, 2024

Puede realizar una actualización de un solo paquete de las instancias de NetScaler SDX que ejecuten NetScaler versión 11.0 y posterior. Para realizar una actualización de un solo paquete, utilice una tarea integrada en NetScaler ADM. Con esta tarea integrada, puede actualizar el servicio de administración NetScaler SDX, Citrix Hypervisor y los paquetes y parches complementarios para Citrix Hypervisor.

Para actualizar instancias de NetScaler SDX con NetScaler ADM:

1. Vaya a **Redes** > **Trabajos de configuración** > **Trabajos de mantenimiento.**
2. Haga clic en **Crear trabajo**. En la página Crear trabajo, seleccione la tarea integrada **Actualizar NetScaler SDX** para actualizar las instancias de NetScaler SDX. Haga clic en **Continuar**.
3. En una o más páginas de actualización de dispositivos NetScaler, en la pestaña **Selección** de instancias, especifique el **nombre del trabajo** y haga clic en **Agregar instancias.**

4. Seleccione las instancias de destino o los grupos de instancias que quiere actualizar.
5. Después de agregar las instancias o grupos de instancias de NetScaler, haga clic en**Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas. La pantalla informa del progreso de la validación previa de cada una de las instancias NetScaler.
6. En la página**Modificar actualización de NetScaler Appliance (s)**, seleccione la ficha**Actualización**. En el menú **Imagen del software** , seleccione **Local** (su máquina local) o **Dispositivo** (el archivo de compilación debe estar presente en Citrix ADM).
7. También puede ver si alguna instancia tiene errores de actualización previa a la validación. Estos errores se muestran en forma de mensaje. Los mensajes muestran los errores relacionados con el espacio en disco, la unidad de disco duro y la personalización del usuario. Si no quieres continuar con las instancias que no superaron la comprobación de actualización previa a la validación, puedes eliminar las instancias. Para eliminar las instancias, selecciónelas y haga clic en **Eliminar.**
8. En la ficha**Planificar tarea**, también puede establecer detalles de ejecución en los que puede realizar el proceso de actualización ahora o programarlo para una fecha posterior. También puede optar por hacer una copia de seguridad de su instancia de NetScaler SDX, recibir un informe de ejecución por correo electrónico o realizar una actualización en dos etapas para los nodos de HA.

La actualización de dos etapas para nodos en HA le da la opción de realizar la actualización inmediatamente o programar una hora para que los nodos se actualicen uno tras otro.La sincronización y propagación de los nodos se desactivan hasta que ambos nodos se actualizan correctamente.

Crear trabajos de configuración para instancias Citrix SD-WAN WANOP

January 30, 2024

Un trabajo es un conjunto de comandos de configuración que se pueden crear y programar en una o más instancias administradas. Para las instancias WANOP de Citrix SD-WAN, puede usar las siguientes opciones para crear trabajos:

- **Plantilla de configuración**: puede usar el editor de configuración para escribir los comandos de la CLI, guardar la configuración como una plantilla y usarla para configurar los trabajos.
- **Plantilla incorporada**: puede elegir de una lista de plantillas de configuración. Estas plantillas proporcionan las sintaxis de los comandos CLI y permiten especificar valores para las variables. Las plantillas integradas aparecen en la lista, con sus descripciones en la tabla siguiente.
- **Archivo**: Puede cargar un archivo de configuración desde su máquina local y crear trabajos.

Una vez creado un trabajo, puede elegir entre ejecutarlo inmediatamente o programarlo para que se ejecute más adelante. También puede establecer la frecuencia de ejecución

Plantilla incorporada	Descripción
Activar Cloudbridge WAN Opt	Permite el tráfico a través del dispositivo Citrix SD-WAN WANOP.
DisableCloudBridgeWANOpt	Deshabilita el tráfico a través del dispositivo Citrix SD-WAN WANOP.
RestartCloudBridgeWANOpt	Reinicia el dispositivo Citrix SD-WAN WANOP.
RestoreConfig	Restaura la configuración del dispositivo Citrix SD-WAN WANOP.
AddLink	La creación o definición de enlaces permite que el dispositivo SD-WAN WANOP evite la congestión y la pérdida de los enlaces y modele el tráfico. Puede definir el ancho de banda máximo enviado o recibido a través del enlace y también especificar si es tráfico del lado LAN o del lado WAN.
Configurar ancho de banda	Establece los límites del ancho de banda y otros ajustes de administración del ancho de
Agregar usuario	Agrega un usuario nuevo, al que puede asignar privilegios.
AddUserAdvancedPlatform	Agrega un nuevo usuario y permite asignar privilegios que no están disponibles en la plantilla AddUser.
AddService-class	Crea una clase de servicio para el dispositivo Citrix SD-WAN WANOP con uno o más filtros de clase de servicio y la habilita.
SetApplication	Establece la definición del clasificador de aplicaciones.
Agregar o eliminar puertos de almacenamiento en caché de vídeo	Añade o elimina el número de puerto en el que la fuente de vídeo puede enviar o recibir datos. El puerto predeterminado es 80.
RemoveVideoCachingSource	Elimina una o más fuentes de almacenamiento en caché de vídeo. Especifique la dirección IP o el nombre de dominio de la fuente de vídeo.
Eliminar todo el almacenamiento en caché de vídeo	Elimina todas las fuentes de almacenamiento en caché de vídeo disponibles.

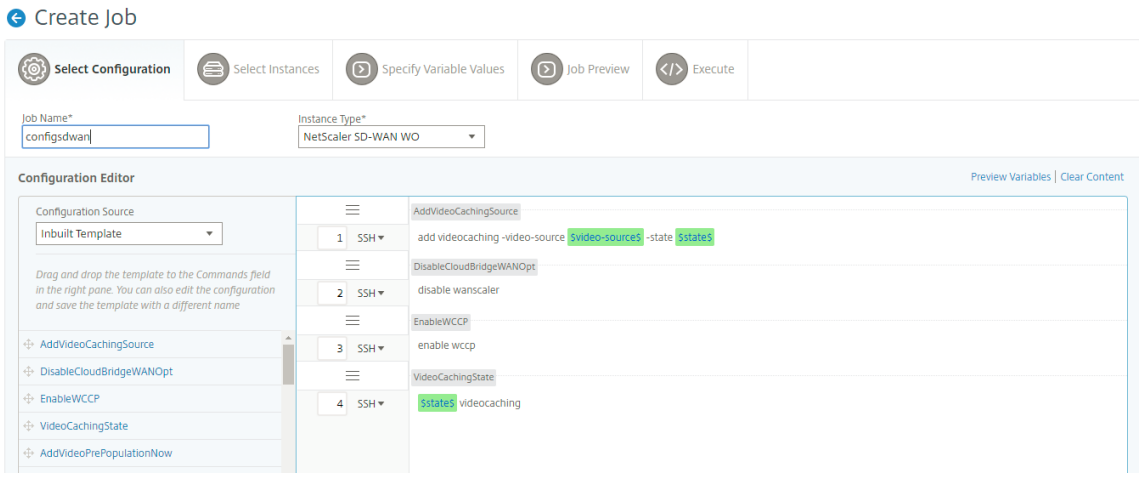
Plantilla incorporada	Descripción
Estado de caché de vídeo	Habilita o deshabilita la función de almacenamiento en caché de vídeo en los dispositivos Citrix SD-WAN WANOP.
Borrar almacenamiento en caché	Borra la caché de vídeo o las estadísticas de almacenamiento en caché de vídeo.
Configurar almacenamiento de vídeo	Establece el tamaño máximo de los objetos en caché. Un objeto que supere este límite no se almacena en caché. De forma predeterminada, el tamaño máximo del objeto de almacenamiento en caché es de 100 MB.
Agregar fuente de caché de vídeo	Añade la dirección IP o el nombre de dominio de la fuente de vídeo. Incluye opciones para habilitar o deshabilitar el almacenamiento en caché de vídeo para esa fuente.
Configurar servidor de licencias remoto	Configura el servidor de licencias centralizado. Especifique el modelo del servidor de licencias, la dirección IP y el número de puerto.
Configurar el servidor de licencias local	Establece la ubicación del servidor de licencias como local.
InstallCACert	Instala los certificados de CA en el dispositivo Citrix SD-WAN WANOP. Especifique el nombre del certificado, el nombre del archivo y la contraseña del almacén de claves.
Instale Combined Cer Key	Instala un par de archivos combinados de claves de certificado SSL.
Instala una clave de cert independiente	Instala el certificado SSL y la clave como archivos separados.
Activar WCCP	Activa el modo de despliegue del WCCP.
AddWCCPServiceGroup	Agrega una nueva definición de grupo de servicios WCCP para el dispositivo Citrix SD-WAN WANOP.
DisableWCCP	Desactiva el modo de despliegue del WCCP.
Agregar directiva de modelado de tráfico	Crea una directiva de modelado de tráfico para el dispositivo Citrix SD-WAN. La directiva controla el ancho de banda de la red.

Plantilla incorporada	Descripción
SetTrafficShapingPolicy	Modifica la política de modelado del tráfico del dispositivo Citrix SD-WAN WANOP. La directiva controla el ancho de banda de la red.
Agregar prepoblación de vídeo	Crea una entrada de prepoblación de vídeos, que permite descargar y almacenar en caché un vídeo con antelación. También puede especificar cuándo almacenar en caché un vídeo.
Actualizar la prepoblación de vídeos	Modifica una entrada de prepoblación de vídeo, que especifica cuándo almacenar en caché un vídeo.
Agregue la prepoblación de vídeos ahora	Configura la prepoblación de vídeos, lo que le permite descargar y almacenar en caché un vídeo de forma inmediata. Puedes controlar cómo quieres descargar y almacenar en caché los vídeos desde las URL.
VideoPrePopulationState	Cambia, inicia, actualiza o elimina la prepoblación de vídeos.
Configurar Syslog Server	Establece la dirección IP y el número de puerto del servidor syslog.
Configurar alerta	Configura el nivel de alerta.

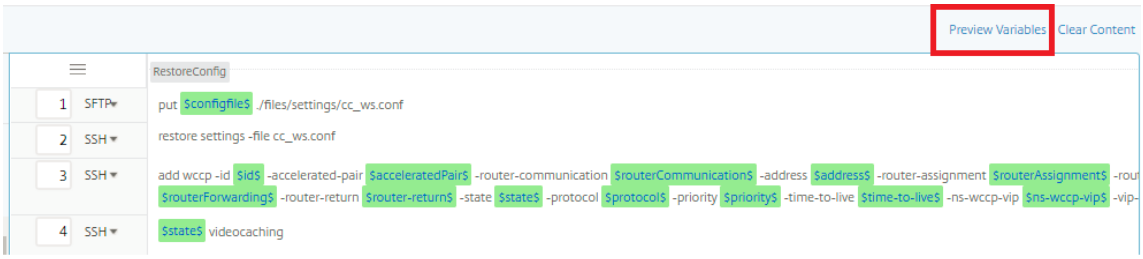
Para crear un trabajo de configuración para instancias de Citrix SD-WAN WANOP:

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración** y, a continuación, haga clic en **Crear trabajo**.
2. En la página **Crear Trabajo**, en la ficha **Seleccionar Configuración**, especifique el **Nombre del Trabajo**.
3. En el campo **Tipo de instancia**, seleccione **Citrix SD-WAN WO**.
4. En la lista desplegable **Fuente de configuración**, seleccione una opción para crear un trabajo.

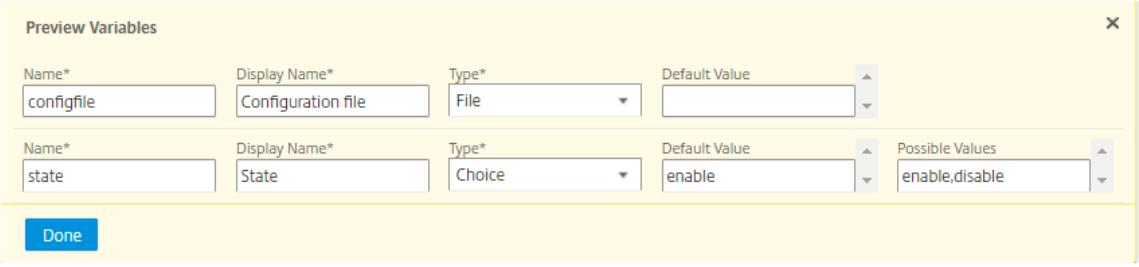
   > **Nota**
   >
   > Seleccione **Guardar como plantilla de configuración** y especifique un nombre para guardar la configuración como plantilla y volver a utilizarla.



5. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
6. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.
7. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que definió al crear o editar un trabajo de configuración.

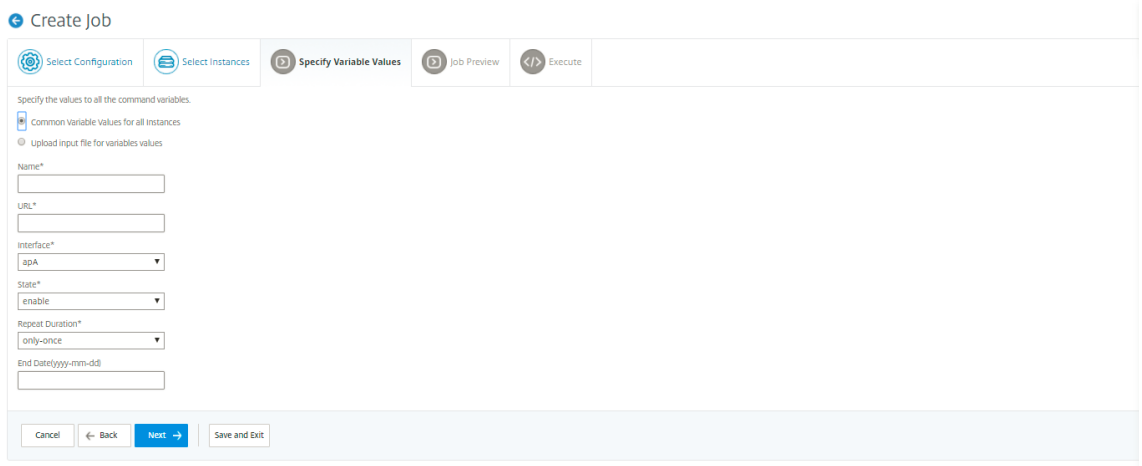


8. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.



9. Haga clic en **Siguiente** y, a continuación, en la pestaña **Seleccionar instancias** , haga clic en **Agregar instancias.** Seleccione las instancias en las que desea ejecutar el trabajo y, a continuación, haga clic **en**Aceptar .
10. Haga clic en **Siguiente** y, a continuación, en la ficha **Especificar valores de variable**, seleccione una de las siguientes opciones para especificar variables para las instancias:

    - **Cargar archivo de entrada para valores de variables:** haga clic en **Descargar archivo de claves** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca valores para las variables definidas en los comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
    - **Valores de variables comunes para todas las instancias**: introduzca valores para las variables. Las variables varían en función de la plantilla seleccionada.



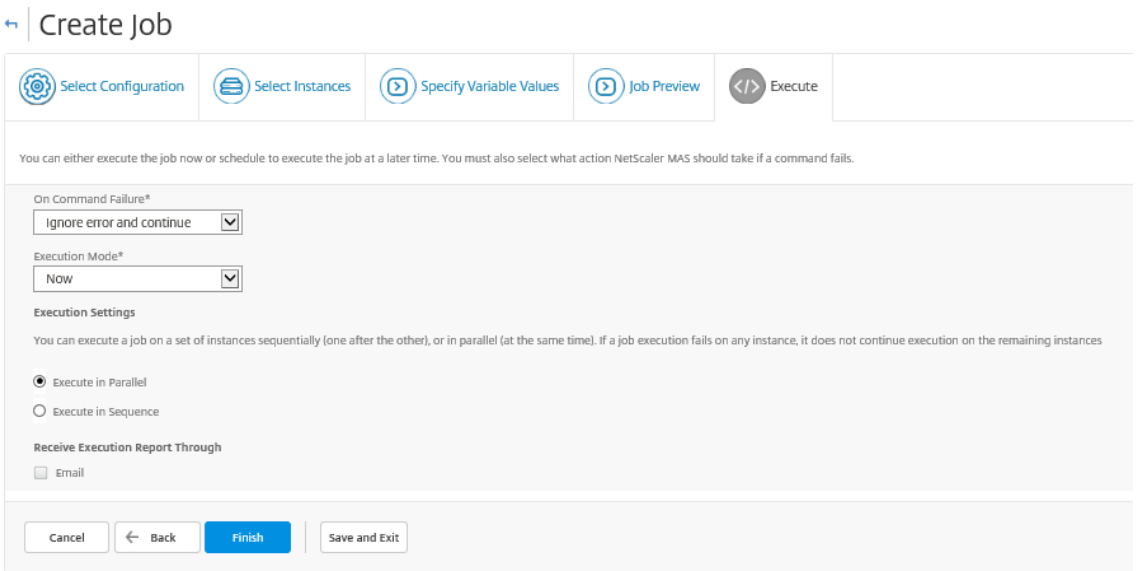
Los archivos de entrada que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

Para ver los trabajos de configuración ejecutados al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración** y haga clic en **Crear trabajo** . En la página**Crear Trabajo**. En la ficha **Especificar valores de variable**, seleccione la opción **Valores de variable comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de en-

trada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

Para ver los trabajos de configuración ya ejecutados mientras modifica un trabajo de configuración, vaya a**Red > Trabajos de configuración**, seleccione el nombre del trabajo y haga clic en**Modificar**. En la página **Configurar trabajo**, en la ficha **Especificar valores de variable**, seleccione la opción **Valores de variable comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y luego modifique y cargue los archivos (manteniendo el mismo nombre de archivo)

11. Haga clic en **Siguiente** , en la pestaña Vista **previa del trabajo** , para evaluar y verificar los comandos que se ejecutarán como un trabajo.
12. Haga clic en **Siguiente**, en la ficha **Ejecutar**, establezca las condiciones siguientes:
    - **En caso de error de comando**: qué hacer si un comando falla: ignorar los errores y continuar con el trabajo o detener la ejecución posterior del trabajo. Elija una acción de la lista desplegable.
    - **Modo**de ejecución : ejecuta el trabajo inmediatamente o programa la ejecución para más adelante. Si planifica la ejecución para un momento posterior, debe especificar la configuración de frecuencia de ejecución para el trabajo. Elija la programación que quiere que siga el trabajo en la lista desplegable **Frecuencia de ejecución**.



13. En **Configuración de ejecución** , seleccione ejecutar el trabajo de forma secuencial (uno tras otro) o en paralelo (al mismo tiempo).
14. Para enviar un informe de ejecución de un trabajo por correo electrónico a una lista de destinatarios, seleccione la casilla **Correo** electrónico en la sección **Recibir el informe de ejecución mediante** . En la lista desplegable que aparece, elija una lista de distribución de correo

electrónico. Para crear una lista de distribución de correo electrónico, haga clic en el icono **+** e introduzca las direcciones de correo electrónico de los destinatarios y los detalles del servidor de correo electrónico.

15. Haga clic en **Finalizar**.

Utilizar la plantilla de configuración maestra

January 30, 2024

El uso de una plantilla de configuración maestra es una opción flexible para crear e implementar una configuración maestra en varias instancias de Citrix ADC.

Como administrador, es posible que desee realizar cambios en la configuración y guardar las licencias, los certificados y otros archivos en la instancia de ADC. Puede guardar la nueva configuración como una plantilla de configuración maestra (archivo.conf).

Para guardar la plantilla de configuración maestra de una instancia de ADC, puede realizar una de las siguientes acciones:

- En la solicitud de comando, escriba **save ns config**. La configuración se guarda en la memoria FLASH de la instancia, en el archivo /nsconfig/ns.conf.
- Desde la interfaz gráfica de usuario de la instancia, vaya a **Diagnóstico** > **Ver configuración**. Elige el tipo de configuración que quieres guardar. Por ejemplo, si quieres guardar la configuración guardada de su instancia, selecciona **Configuración guardada en**.Haga clic en el enlace **Guardar texto en un archivo** para guardar el archivo 'ns.conf'en su equipo local.

Al implementar la plantilla de configuración maestra mediante la plantilla de configuración «DeployMasterConfiguration» al crear un nuevo trabajo, puede personalizarla aún más para cada instancia de ADC específica añadiendo comandos adicionales, modificando los comandos existentes y proporcionando diferentes valores de variables en el archivo de entrada.

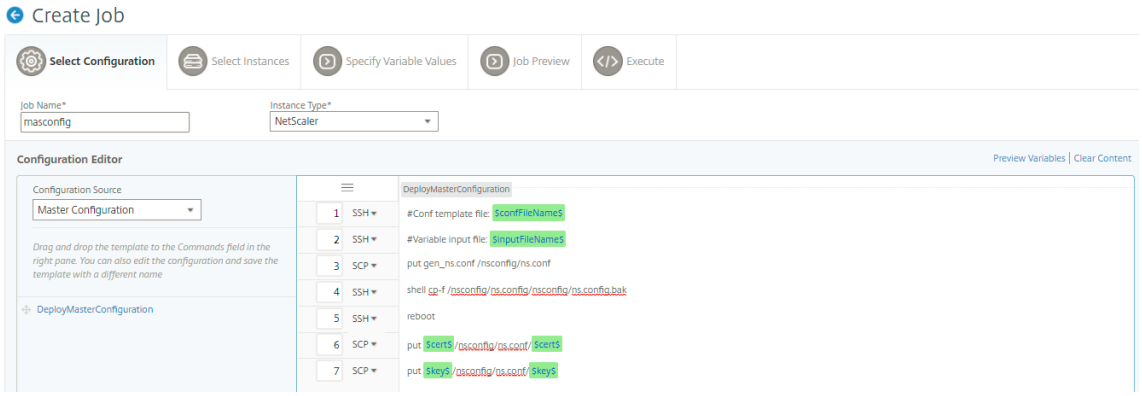
Por ejemplo, como administrador, puede que desee cargar claves de certificado en sus instancias de ADC, además del archivo ns.conf, e implementar también la configuración maestra en ellas.

> **Importante**
>
> No puede ejecutar un trabajo de configuración mediante la plantilla DeployMasterConfiguration en instancias CPX de Citrix ADC, instancias configuradas en un clúster o instancias de ADC particionadas.

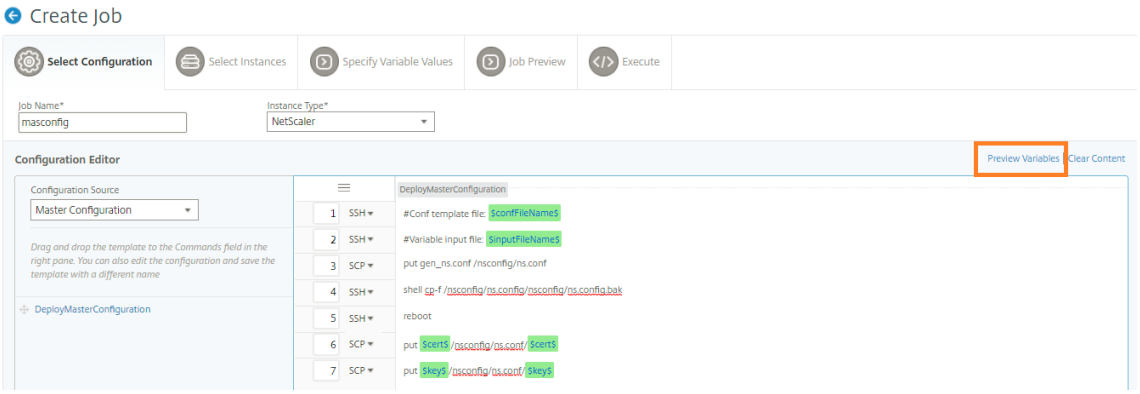
Para crear un trabajo de configuración con la plantilla de configuración Master Config en Citrix ADM:

1. En Citrix ADM, vaya a **Redes** > **Trabajos de configuración**y, a continuación, haga clic en **Crear**trabajo.
2. En la página **Crear Trabajo**, en la ficha **Seleccionar Configuración**, especifique el **Nombre del Trabajo** y seleccione el **Tipo de Instancia** en la lista desplegable.
3. Seleccione **Configuración maestra** en la lista desplegable **Fuente de configuración**. Arrastre y suelte los comandos de la plantilla DeployMasterConfiguration en el panel derecho. También puede agregar, modificar o eliminar comandos en el panel derecho. Haga clic en **Siguiente**.

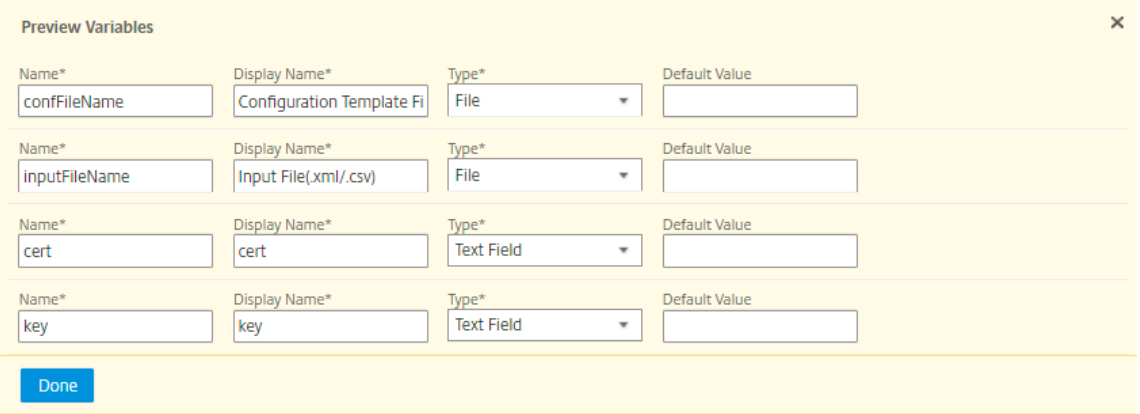
   > **Nota**
   >
   > Puede agregar comandos ***put*** para agregar archivos de entrada a su plantilla. En nuestro ejemplo, tendremos que cargar los archivos de certificado y clave además del archivo de plantilla de configuración y los archivos de entrada de variables.



4. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
5. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.
6. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que definió al crear o editar un trabajo de configuración.



7. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.



8. Seleccione las instancias en las que quiere ejecutar el trabajo de configuración y, a continuación, haga clic en **Siguiente**.
9. En la ficha **Especificar valores variables**, cargue lo siguiente:

   - **Archivo de plantilla de configuración (.conf)**: Cargue el archivo.conf que ha extraído de una instancia de ADC.
   - **Cargar el archivo de entrada (XML/CSV)**: Cargar el archivo de entrada con valores para las variables que ha definido en sus comandos.

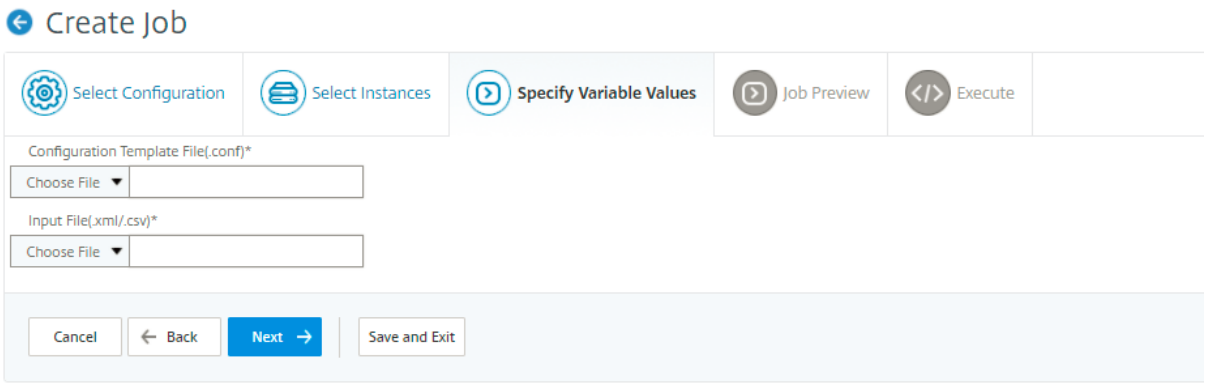
   Aquí se proporciona un archivo xml de muestra para su uso. Asegúrese de que los archivos xml contienen los detalles correspondientes a las instancias ADC que está utilizando.

```
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

```



```
Provide inputs for all the parameters defined in the master config file.

- global. This tag contains all the common parameters and value.

- devicegroup. This tag contains all the instance group specific parameters and values.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence over the instance group. The instance group specific parameters value will take precedence over global parameters in the execution.

- name. This attribute represents the name of the instance group.

- device. This tag contains all the instance specific parameters and value.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence in the execution.

- name. This attribute represents the IP Address of the instance. Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>. Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters names are case sensitive.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>

<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```


10. Haga clic en **Siguiente**.

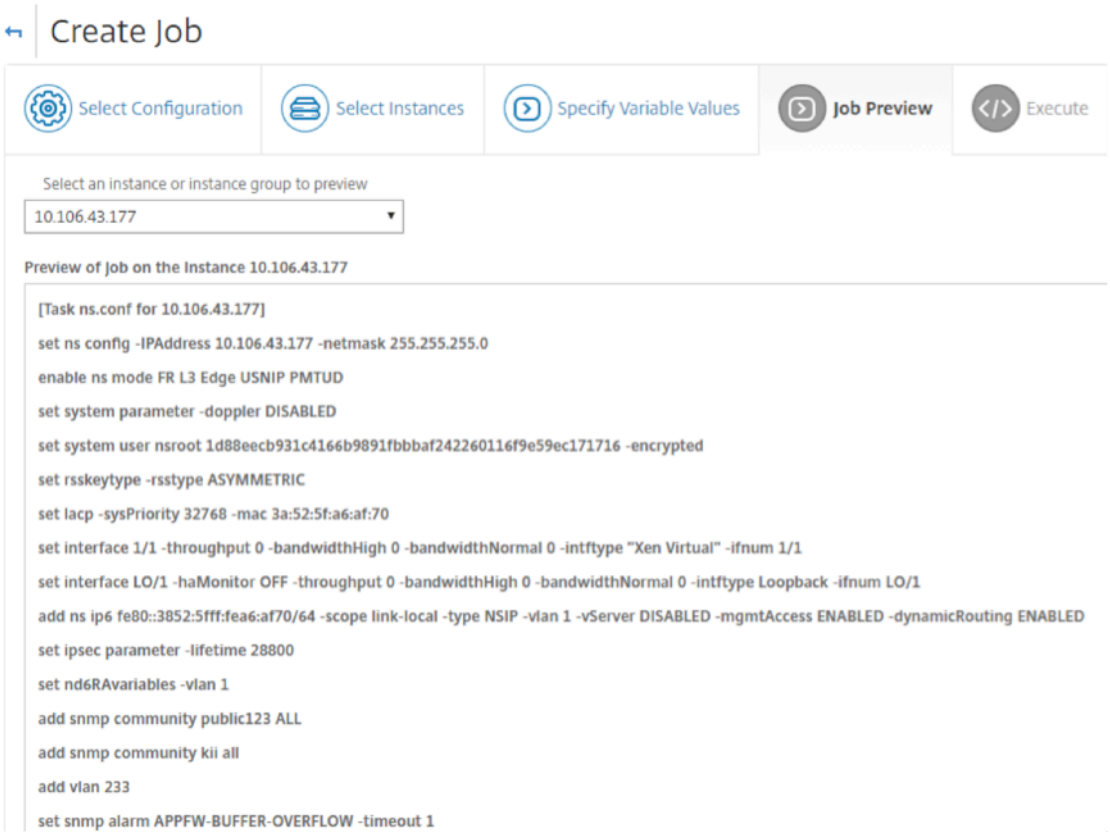


Los archivos de entrada que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

Para ver los trabajos de configuración ejecutados al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear trabajo**. En la página **Crear trabajo**. En la ficha **Especificar valores de variables**, seleccione la opción **Valores de variables comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

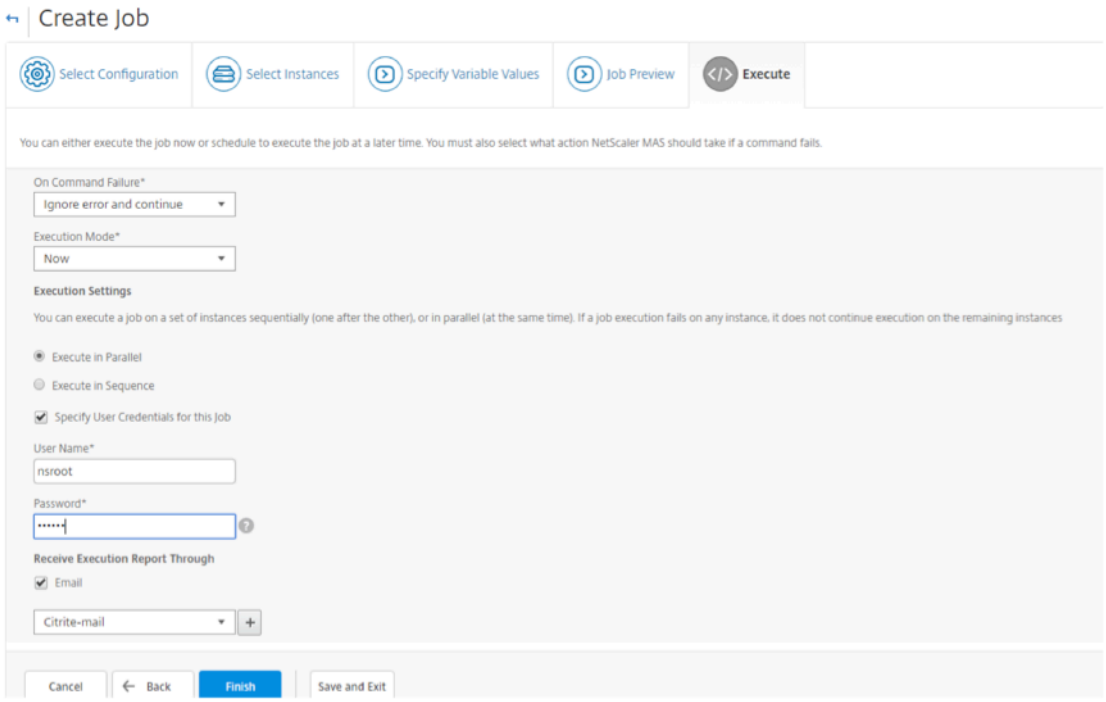
Para ver los trabajos de configuración ya ejecutados mientras se modifica un trabajo de configuración, vaya a **Red > Trabajos de configuración**, seleccione el nombre del trabajo y haga clic en **Modificar**. En la página **Configurar Trabajo**, en la ficha **Especificar Valores de Variable**, seleccione la opción **Valores de Variable Comunes para todas las Instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

1. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias y, a continuación, hacer clic en **Siguiente**.



2. En la ficha **Ejecutar**, puede elegir ejecutar su trabajo ahora o programarlo para que se ejecute más adelante. También puede elegir qué acción debe realizar Citrixx ADM si se produce un error en el comando.

   También puede optar por permitir que los usuarios autorizados ejecuten trabajos en sus instancias administradas y elegir si deseas enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo, junto con otros detalles.



Después de ejecutar el trabajo, puede ver los detalles del trabajo navegando hasta**Redes** >**Trabajos de configuración**y seleccionar el trabajo que acaba de configurar. Haga clic en**Detalles** y, a continuación, haga clic en**Resumen de ejecución** para ver los detalles de su trabajo. Haga clic en la instancia para ver los **registros de comandos** y ver los comandos ejecutados en el trabajo.

Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

Usar trabajos para actualizar instancias de Citrix ADC

January 30, 2024

Puede utilizar Citrix Application Delivery Management (ADM) para actualizar una o más instancias de Citrix ADC. Antes de actualizar una instancia, asegúrese de haber cargado los archivos de compilación y documentación correctos en las instancias de Citrix ADC. Debe conocer el marco de licencias y los

tipos de licencias antes de actualizar una instancia.

Al actualizar la instancia de Citrix ADC mediante la creación de una tarea de mantenimiento, puede hacer lo siguiente:

- Realice una comprobación previa a la validación de las instancias que se están actualizando. La comprobación previa a la validación consiste en las siguientes comprobaciones:
    1. Compruebe si hay personalizaciones existentes en las instancias de Citrix ADC y elimínelas. Puede volver a aplicar todas las personalizaciones una vez finalizado el proceso de actualización.
    2. Compruebe el uso del disco de las instancias de Citrix ADC. Si el uso del disco es superior al 80%, limpie el espacio en disco.
    3. Compruebe si hay problemas de hardware de disco de instancias de NetScaler ADC.
- Realice la actualización del par NetScaler ADC HA en dos etapas.
    1. Realice la tarea de actualización en un nodo inmediatamente o incluso puede programarla para más adelante.
    2. Programe la actualización para el otro nodo más adelante. Debe programarse después de actualizar el nodo inicial.

Cuando actualice un par Citrix ADC HA, tenga en cuenta lo siguiente:

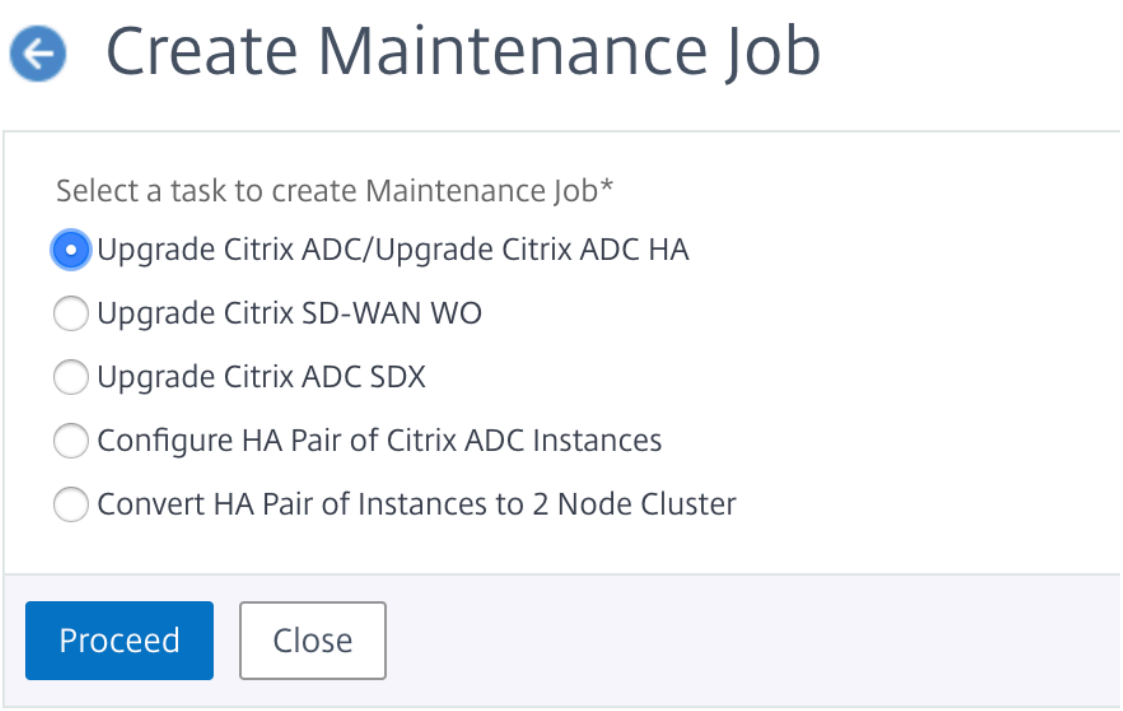
- Actualmente, el segundo nodo del par HA se actualiza primero y, a continuación, la actualización del primer nodo está programada para realizarse más adelante.
- La sincronización y propagación de los nodos se desactivan hasta que ambos nodos se actualizan correctamente.
- Después de la actualización de ambos nodos, verá un mensaje de error en el historial de ejecución (que indica que la sincronización de HA no está habilitada) si sus nodos en el par de HA están en versiones o versiones diferentes.

Para crear una tarea de mantenimiento para actualizar la instancia de NetScaler ADC:

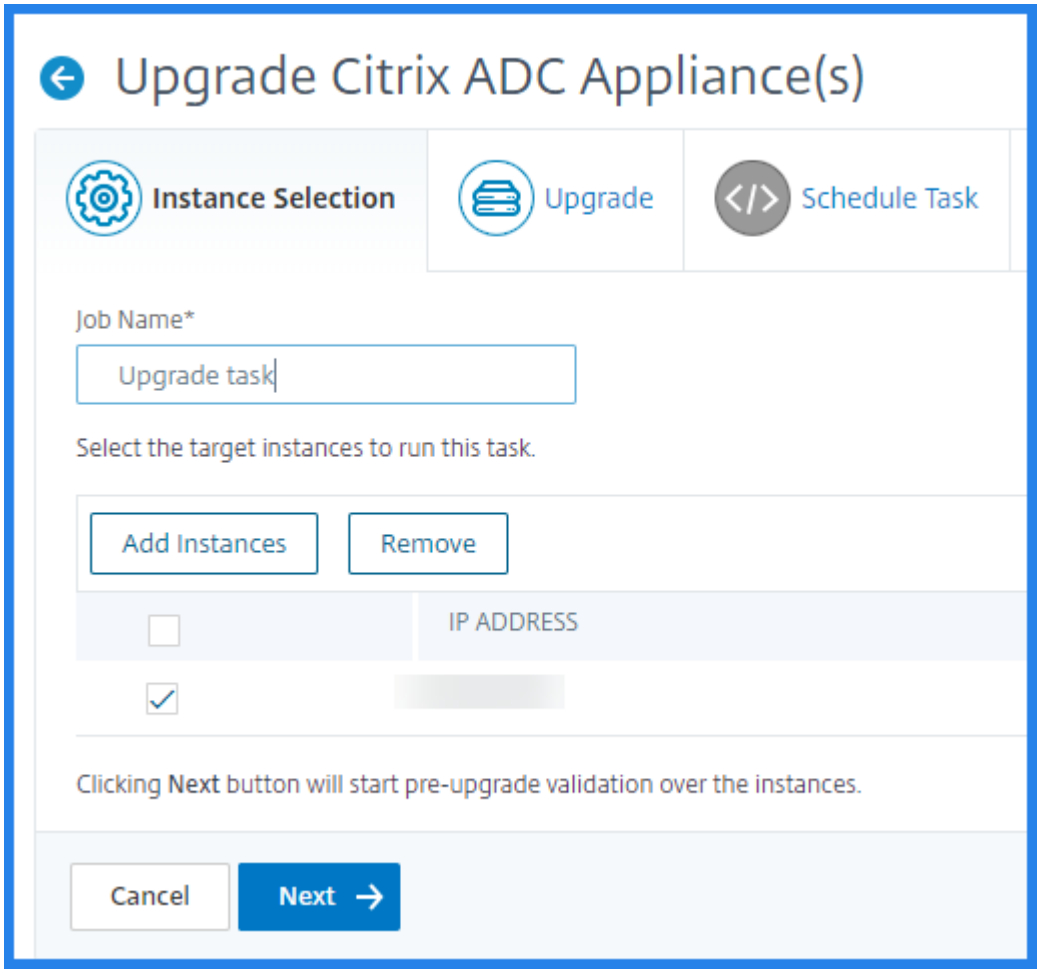
> **Nota**
>
> No se admite la actualización de ADC de una versión superior a una versión inferior. Por ejemplo, si su instancia de Citrix ADC es 13.0 82.x, no puede cambiar la instancia de ADC a 13.0 79.x ni a ninguna otra versión anterior.

1. Vaya a **Redes** > Trabajos de **configuración > Trabajos** de **mantenimiento** .
2. En la página Trabajos de Mantenimiento, haga clic en **Crear Trabajo**.

3. En la página Crear trabajo de mantenimiento, seleccione **Actualizar NetScaler ADC/Actualizar NetScaler ADC HA** y haga clic en **Continuar**.



4. En una o más páginas Actualizar dispositivos NetScaler ADC, en la ficha **Selección de instancias**, especifique el **Nombre del trabajo** y haga clic en **Agregar instancias.**



5. Seleccione las instancias de destino o los grupos de instancias que quiere actualizar.

> **Nota**
>
> - Para actualizar las instancias de Citrix ADC en modo de alta disponibilidad, debe seleccionar las direcciones IP de las instancias principales o secundarias. Sin embargo, se recomienda utilizar siempre el nodo principal para la actualización.
> - Para actualizar instancias de NetScaler ADC en modo clúster, seleccione la dirección IP del clúster.

6. Una vez que haya agregado las instancias o los grupos de instancias de NetScaler ADC, haga clic en **Siguiente**para iniciar la validación previa a la actualización en las instancias seleccionadas. La pantalla informa del progreso de la validación previa de cada una de las instancias NetScaler ADC.

7. En la página **Actualizar dispositivo (s) NetScaler ADC**, seleccione la ficha **Actualizar**. En el menú **Imagen de software**, seleccione **Local** (su máquina local) o **Dispositivo** (el archivo de compilación debe estar presente en NetScaler ADM).

8. También puede ver si alguna instancia tiene errores de actualización previa a la validación. Estos errores se muestran en forma de mensaje. Los mensajes muestran los errores relacionados con el espacio en disco, la unidad de disco duro y la personalización del usuario.

Si no quieres continuar con las instancias que no superaron la comprobación de actualización previa a la validación, puedes eliminar las instancias. Para eliminar las instancias, selecciónelas y haga clic en **Eliminar** .

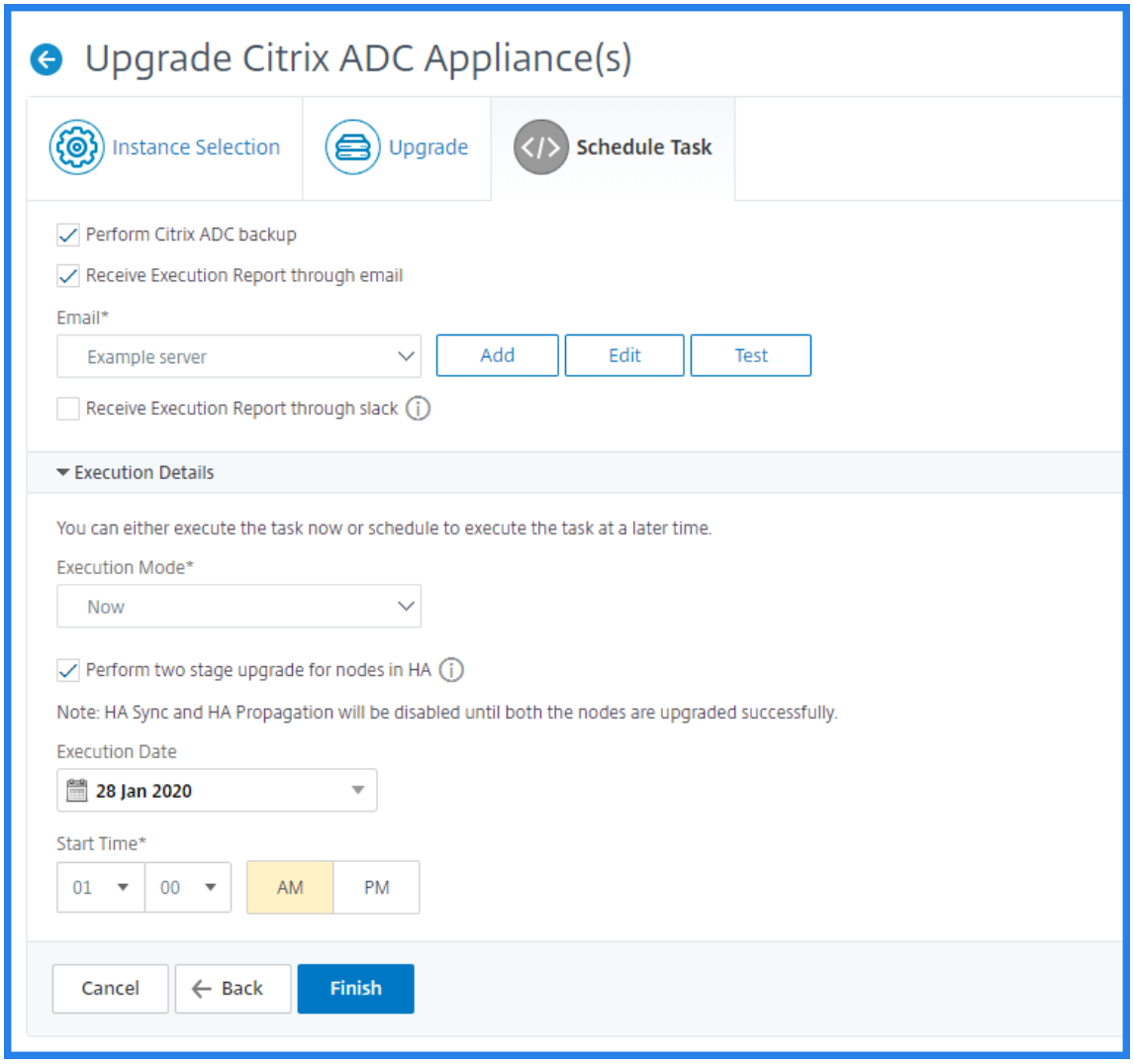
1. Haga clic en **Siguiente**.

   > **Nota**
   >
   > Se recomienda encarecidamente continuar con el proceso de actualización, solo si la comprobación de validación previa a la actualización pasa para las instancias de NetScaler ADC.

2. En la ficha **Planificar tarea**, también puede establecer detalles de ejecución en los que puede realizar el proceso de actualización ahora o programarlo para una fecha posterior.
3. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución de la actualización de instancias de NetScaler ADC. Haga clic en la casilla **Recibir informe de ejecución por correo electrónico** para habilitar la notificación por correo electrónico. Para crear una lista de distribución de correo electrónico:

   - Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
   - En la página **Crear lista de distribución de correo electrónico**, especifique un **nombre** para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el cuadro **De**, agregue la dirección de correo electrónico desde la que quiere enviar mensajes. En el cuadro **Para**, agregue la dirección o las direcciones de correo electrónico a las que quiere enviar los mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en Crear. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

4. En la ficha **Programar tarea**, también puede realizar la actualización en dos etapas para los nodos de HA. Puede realizar la actualización inmediatamente o programar una hora para que los nodos se actualicen uno tras otro. La sincronización y propagación de los nodos se desactivan hasta que ambos nodos se actualizan correctamente.



Usar plantillas de configuración para crear plantillas de auditoría

January 30, 2024

Ahora puede utilizar comandos de configuración que se guardaron anteriormente como plantillas de configuración para crear plantillas de auditoría que se pueden aplicar a instancias específicas de NetScaler. Al crear una plantilla de auditoría, puede arrastrar y soltar las plantillas de configuración guardadas anteriormente en el campo Comandos y modificar la plantilla según sus necesidades. A continuación, puede aplicar la plantilla de auditoría a instancias específicas de NetScaler. Citrix ADM compara estas instancias con la plantilla de auditoría e informa de cualquier discrepancia. Este proceso le ayuda a identificar errores y rectificarlos de manera oportuna.

Puede crear plantillas de configuración mientras crea un nuevo trabajo y guarda un conjunto de co-

mandos de configuración como plantilla. Al guardar estas plantillas en la página **Crear trabajos** , se muestran automáticamente en la página **Crear plantilla** .

Por ejemplo, considere una configuración básica de equilibrio de carga para la que agregue un servidor virtual de equilibrio de carga, agregue dos servicios y vincule los servicios al servidor virtual.

En este ejemplo se utilizan los siguientes comandos:

add lb vserver **servername** HTTP **ipaddress portnumber**

agregar servicio **servicename1** ipaddress1 HTTP 80

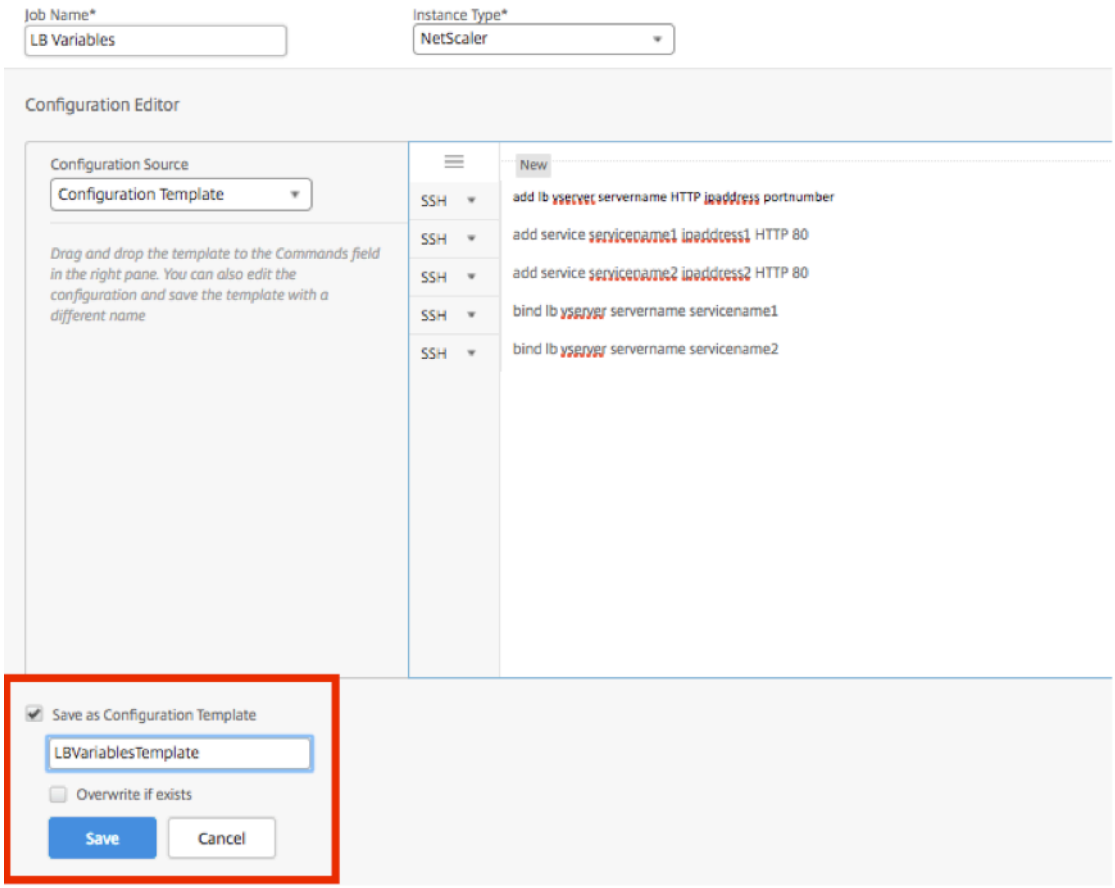
agregar servicio **servicename2** ipaddress2 HTTP 80

bind lb vserver **servername**servicename1

bind lb vserver **servername**servicename2

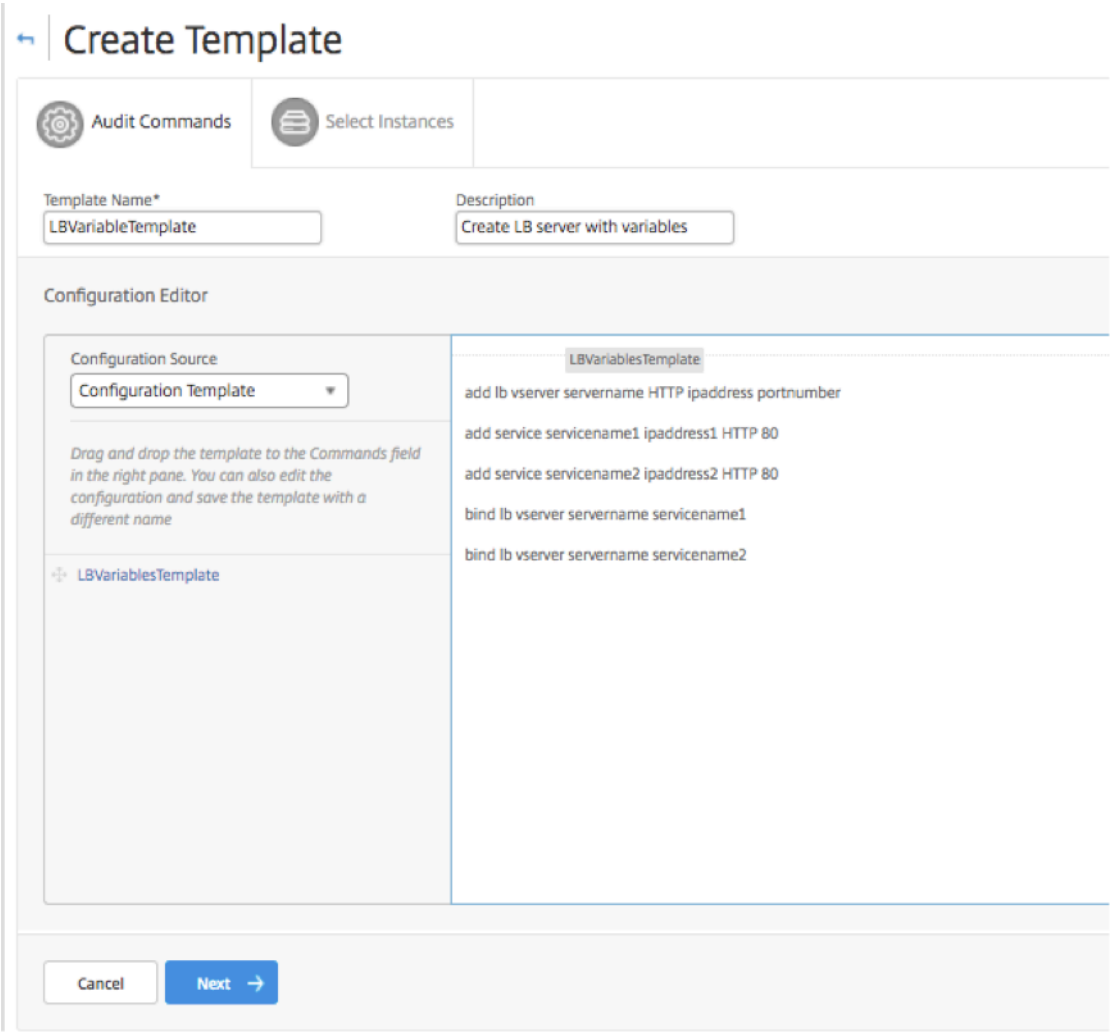
Para guardar una plantilla de configuración en Citrix ADM:

1. Vaya a **Redes** > **Trabajos de configuración**y haga clic en **Crear trabajo**.
2. En la página **Crear Trabajo**, especifique el nombre del trabajo y el tipo de instancia.
3. Elija la **plantilla de configuración** como fuente de configuración y, en el campo **Comandos**, introduzca comandos como los del ejemplo anterior.
4. Seleccione la casilla **Guardar como plantilla de configuración** y especifique un nombre para la plantilla. Puede optar por sobrescribir otras plantillas que existen con el mismo nombre.
5. Haga clic en **Guardar**.



Para utilizar una plantilla de configuración para crear una plantilla de auditoría en Citrix ADM:

1. Vaya a **Redes** > **Auditoría de configuración** > **Plantillas de auditoría**y haga clic en **Agregar**.
2. En la página **Crear plantilla**, especifique un nombre para el nombre de plantilla e introduzca una descripción.
3. En la lista **Fuente de configuración**, seleccione **Plantilla de configuración**y, a continuación, arrastre y suelte la plantilla en el campo Comandos del panel derecho. También puede modificar la configuración y guardar la plantilla con un nombre diferente. Haga clic en **Siguiente**.
4. En la ficha **Seleccionar instancias**, haga clic en **Agregar instancias** y agregue las instancias en las que quiera ejecutar la configuración. Haga clic en **Aceptar**.
5. Haga clic en **Finalizar**.



La plantilla de auditoría aparece en la lista Plantillas de auditoría y se ejecuta cada 12 horas en las configuraciones de las instancias especificadas.

Usar el comando SCP (put) en trabajos de configuración

January 30, 2024

Puede utilizar la función Trabajos de configuración de Citrix ADM para crear trabajos de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados. Un trabajo es un conjunto de comandos de configuración que puede crear y ejecutar en una única instancia administrada o en varias instancias administradas. Por ejemplo, puede utilizar los trabajos de configuración para actualizar los dispositivos.

Los trabajos de configuración de Citrix ADM utilizan comandos Secure Shell (SSH) para configurar instancias, y puede configurar un trabajo de configuración para usar copia segura (SCP) para transferir

archivos de forma segura. SCP se basa en el protocolo SSH. Uno de los comandos SCP que puede incluir en un trabajo de configuración es el comando "put". Puede usar el comando «poner» en los trabajos de configuración para cargar o transferir uno o más archivos almacenados en un directorio local del sistema a Citrix ADM y, luego, a un directorio de la instancia o instancias de NetScaler.

> **Nota** El archivo se carga en Citrix ADM y, posteriormente, se copia (coloca) en las instancias de NetScaler seleccionadas. El archivo cargado se almacena en Citrix ADM y solo se elimina cuando se elimina el trabajo. Esto es necesario para los trabajos programados para ejecutarse más adelante.

El comando tiene la siguiente sintaxis:

```
put <local_filename> <remote_path/remote_filename>
```

donde,

<local_filename> es el nombre del archivo local que se va a cargar.

<remote_path / remote_filename> es la ruta a un directorio remoto y el nombre que se asignará al archivo cuando se copie en ese directorio.

Al crear el trabajo de configuración, puede convertir los parámetros de nombre de archivo local y remoto en variables. Esto le permite asignar diferentes archivos a estos parámetros para el mismo conjunto de instancias de NetScaler cada vez que ejecute el trabajo. Además, cuando se utiliza un archivo en varios lugares de un trabajo y se quiere cambiar el nombre del archivo, se puede redefinir la variable en lugar de cambiar el nombre del archivo en todos los lugares.

Para utilizar el comando put para cargar archivos en un trabajo de configuración:

1. Vaya a **Redes** > **Trabajos de configuración**.
2. En la página **Trabajos**, haga clic en **Crear Trabajo**.
3. En la página **Crear trabajo**, escriba el nombre del trabajo en el campo Nombre del trabajo y, en el panel **Editor de configuración**, escriba el comando "poner".

   Por ejemplo, si quiere crear un trabajo de configuración que copie un archivo de certificado SSL guardado en el sistema local en varias instancias de NetScaler, puede agregar un comando «put» que utilice una variable en lugar del nombre de un archivo determinado y definir el tipo de variable como «archivo».

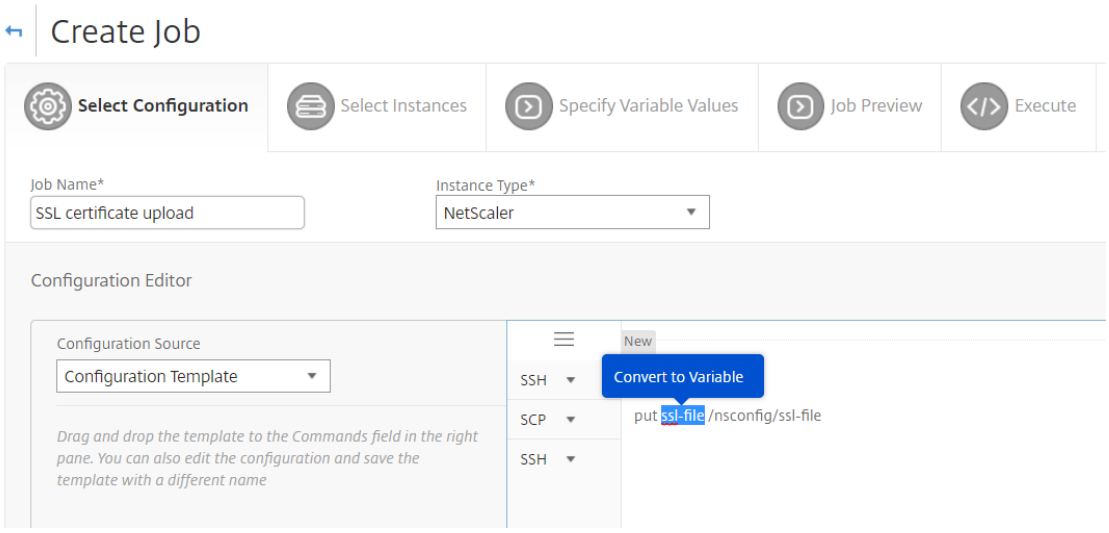
   ```
   1 put ssl-file /nsconfig/ssl-file
   2 <!--NeedCopy-->
   ```

   En este ejemplo,

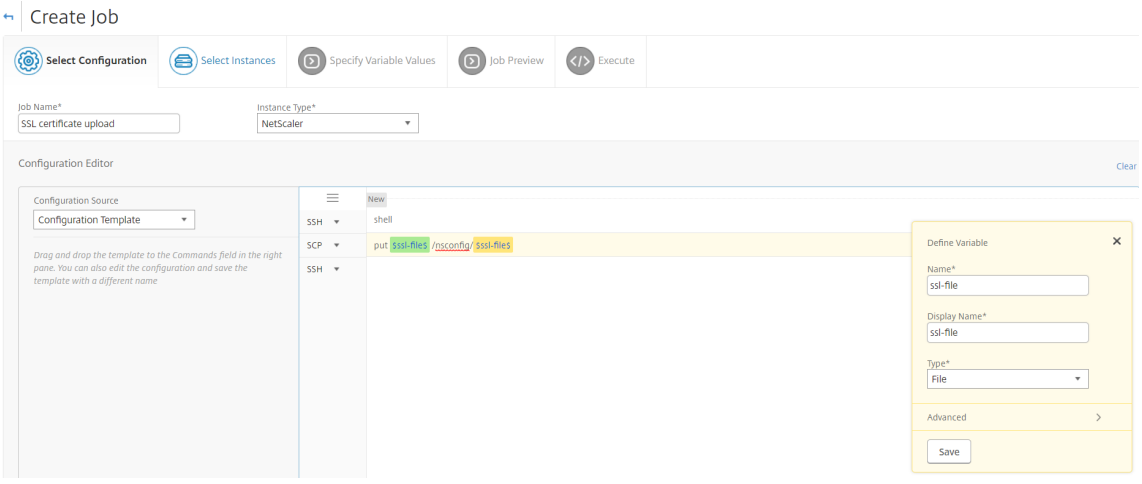
   - ssl-file: este es el nombre del archivo que se debe cargar en la instancia de NetScaler.

- /nsconfig/ssl-file: Esta es la carpeta de destino en la instancia donde se colocará el archivo ssl-después de la ejecución de la tarea.

4. En el comando que acaba de escribir, seleccione el nombre de archivo que desee convertir en una variable y, a continuación, haga clic en**Convertir en variable**, como se muestra en la siguiente figura.

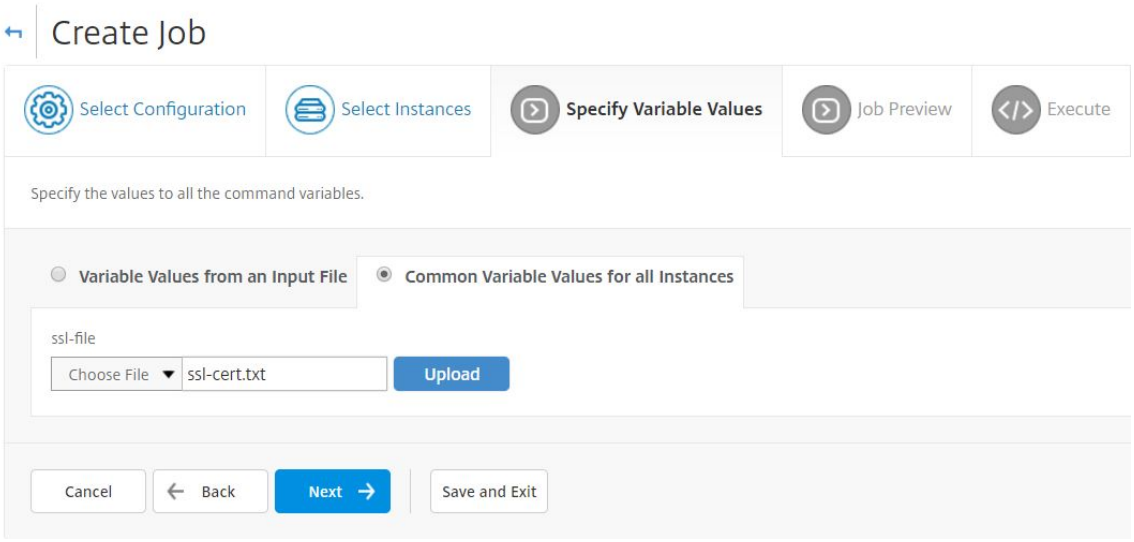


5. Compruebe que el nombre del archivo ha sido incluido con signos de dólar (lo que indica que ahora es una variable) y, a continuación, haga clic en la variable.
6. Especifique los detalles de la variable, como nombre, nombre para mostrar y tipo.
7. En la lista desplegable **Tipo**, seleccione **Archivo**. Haga clic en **Guardar**. Declarar la variable como un tipo de "Archivo"le permite cargar archivos en Citrix ADM.

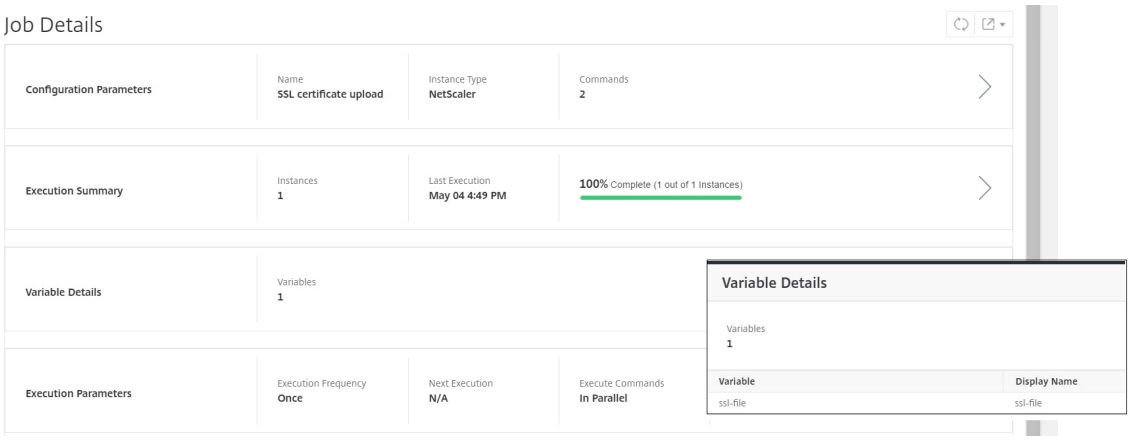


8. Haga clic en **Siguiente** y seleccione las instancias de NetScaler en las que desea copiar los archivos.

9. En la ficha **Especificar valores de variables**, seleccione la sección **Valores de variables comunes para todas las instancias**, seleccione el archivo del almacenamiento local del sistema, haga clic en **Cargar** para cargar el archivo en Citrix ADM y haga clic en **Siguiente**.



10. En la ficha**Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
11. En la ficha**Ejecutar**, puede ejecutar el trabajo ahora o programarlo para que se ejecute más adelante. También puede elegir qué acción debe realizar Citrix ADM si se produce un error en el comando. También puede crear una notificación por correo electrónico para recibir una notificación sobre el éxito o el fracaso del trabajo, y otros detalles. Haga clic en **Finalizar**.
12. Para ver los detalles del trabajo, vaya a**Redes** >**Trabajos de configuración** y seleccione el trabajo que acaba de configurar. Haga clic en **Detalles** y, a continuación, en **Detalles de variables** para mostrar las variables agregadas a su trabajo.



Reprogramar trabajos configurados mediante plantillas integradas

January 30, 2024

Puede reprogramar un trabajo que haya programado mediante plantillas integradas en Citrix Application Delivery Management (ADM). Por ejemplo, puede cambiar la acción que debe realizar NetScaler ADM si se produce un error en un comando. Si previamente optó por ignorar un error y continuar, puede cambiarlo para revertir todos los comandos correctos si falla un comando.

Para reprogramar un trabajo configurado mediante plantillas integradas en NetScaler ADM

1. En Citrix ADM, vaya a **Redes** > **Trabajos de configuración** .
2. Seleccione el trabajo que quiere modificar, agregar o quitar instancias, especifique valores de variables y, a continuación, cambie las acciones de ejecución y la configuración.
3. Haga clic en **Finalizar** para reprogramar el trabajo.

> **Nota**
>
> También puede seleccionar el trabajo y hacer clic en **Ejecutar de nuevo** para ejecutar el trabajo sin modificar ningún origen, instancia ni comando. Esto es útil cuando tiene que ejecutar el mismo conjunto de comandos en las mismas instancias. A veces, el trabajo puede encontrar un error transitorio desde el lado del servidor, y es posible que tenga que ejecutar el trabajo de nuevo.

Reutilizar plantillas de auditoría de configuración en trabajos de configuración

January 30, 2024

Como administrador, ahora puede guardar los comandos de configuración como un conjunto de plantillas de configuración reutilizables al crear un trabajo y ejecutar una auditoría de configuración. La plantilla de configuración creada y guardada en Configuration Jobs está disponible en Configuration Audit para crear una plantilla de auditoría que se pueda aplicar a instancias específicas de Citrix ADC. Del mismo modo, la plantilla de auditoría creada en el módulo Auditoría de configuración está disponible en Configuration Jobs para que pueda ejecutar la plantilla como un trabajo de configuración. Cualquier cambio realizado en la plantilla es ahora visible tanto en los módulos Configuration Jobs como en Configuration Audit.

Anteriormente, el trabajo de configuración y las plantillas de auditoría de configuración tenían que crearse por separado para la misma configuración y guardarse como archivos diferentes. Esto provocó una duplicación de esfuerzos en la creación y el mantenimiento de las plantillas.

Citrix Application Delivery Management (ADM) le permite guardar esta plantilla en el sistema para que la plantilla de auditoría también esté disponible en los trabajos de configuración. Ahora las plantillas de auditoría se pueden utilizar para crear trabajos de configuración. De esta forma, las plantillas se pueden usar indistintamente entre los trabajos de configuración y las auditorías de configuración.

Por ejemplo, considere una configuración básica de equilibrio de carga para la que agregue un servidor virtual de equilibrio de carga, agregue dos servicios y vincule los servicios al servidor virtual.

En este ejemplo se utilizan los siguientes comandos:

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
<!--NeedCopy-->
```

Creación de una plantilla en auditorías de configuración y reutilización en trabajos de configuración

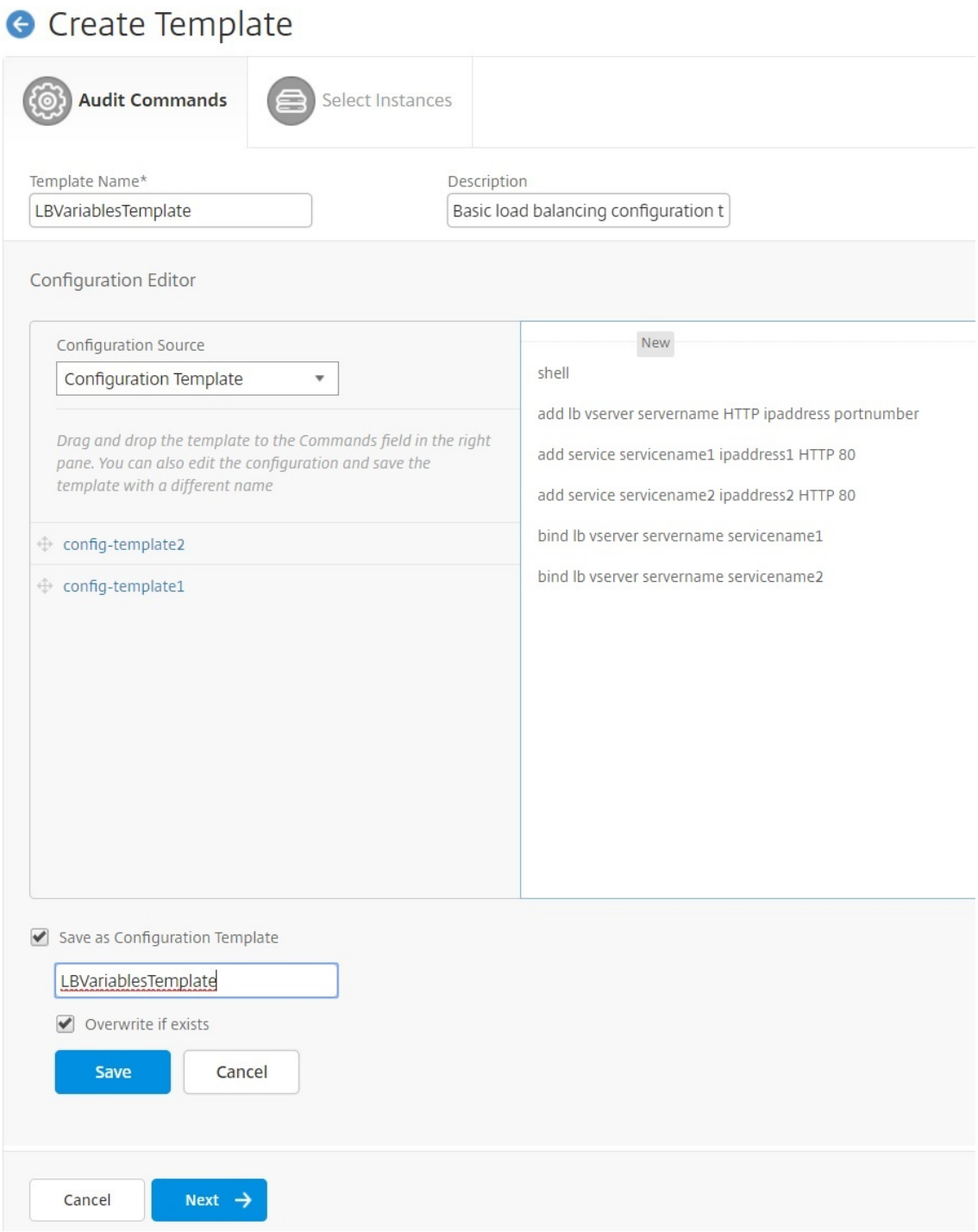
Realice la siguiente tarea para crear una plantilla en el módulo de auditoría de configuración y reutilizarla en el módulo de trabajos de configuración.

Para crear una plantilla de auditoría:

1. **En Citrix ADM, vaya a** Redes > Auditoría de configuración > Plantilla de auditoría**y haga clic en Agregar.**
2. En la página**Crear plantilla**, especifique el nombre de la plantilla. También puede agregar más información sobre la plantilla en el campo **Descripción**.
3. En el panel **Comandos**, escriba comandos en el ejemplo.
4. Active la casilla de verificación**Guardar como plantilla de configuración** y especifique un nombre para la plantilla; por ejemplo, puede asignar el nombre a esta plantilla como "LB-VariablesTemplate". Puede optar por sobrescribir otras plantillas que existen con el mismo nombre.

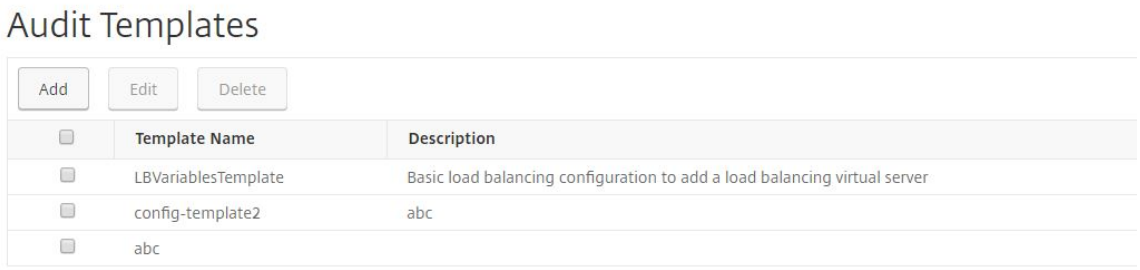
> **Nota:** El nombre de la plantilla de auditoría puede ser el mismo que el nombre de la plantilla de configuración.

5. Haga clic en**Guardar** y haga clic en **Siguiente**.



6. Haga clic en **Siguiente**.

7. En la ficha **Seleccionar instancias**, seleccione las **instancias de Citrix ADC en las** que quiere ejecutar estos comandos de configuración y haga clic en **Finalizar.** La nueva plantilla está ahora visible en la lista de plantillas de auditoría.



8. Cuando quiera ejecutar estos comandos de configuración, vaya a **Redes** > **Trabajos de configuración y haga** clic en **Crear trabajo**. La plantilla de auditoría que creó anteriormente aparece como plantilla de configuración.

Para reutilizar la plantilla de auditoría en trabajos de configuración:

1. Introduzca un nombre para el trabajo, seleccione el tipo de instancia y arrastre y suelte la plantilla en el panel de comandos.

   Al crear el trabajo de configuración, puede convertir los parámetros de nombre de archivo local y remoto en variables. Esto le permite asignar diferentes archivos a estos parámetros para el mismo conjunto de instancias de Citrix ADC cada vez que ejecute el trabajo.

2. En el comando que ha introducido, seleccione el nombre del archivo que desee convertir en variable y, a continuación, haga clic en**Convertir en variable.**

3. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar estos comandos.

4. Si ha especificado alguna variable en los comandos, en la ficha **Especificar valores variables**, seleccione una de las siguientes opciones para especificar las variables de sus instancias:

   - Valores de variables de un archivo de entrada: descargue un archivo de entrada para introducir valores para las variables que ha definido en los comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
   - Valores de variables comunes para todas las instancias: especifique la dirección IP y el puerto del servidor syslog.

5. En la ficha**Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias y hacer clic en**Siguiente**.

6. En la ficha**Ejecutar**, haga clic en**Finalizar** para ejecutar el trabajo de configuración. Ahora, si quiere agregar otro servicio a este servidor de equilibrio de carga y enlazar el servicio con el servidor, puede modificar los comandos en la página de comandos y guardarlos.
7. Desplácese hasta **Plantillas de auditoría** y haga clic en **Agregar**.
8. Arrastra y suelta la plantilla «LBVariablesTemplate» en el panel de comandos. Puede ver que la plantilla se ha actualizado con los nuevos comandos.

La plantilla de auditoría aparece en la lista Plantillas de auditoría y se ejecuta cada 12 horas en las configuraciones de las instancias especificadas. Ahora puede crear plantillas y reutilizarlas entre trabajos de configuración y módulos de auditoría de configuración.

Importar y exportar plantillas de configuración

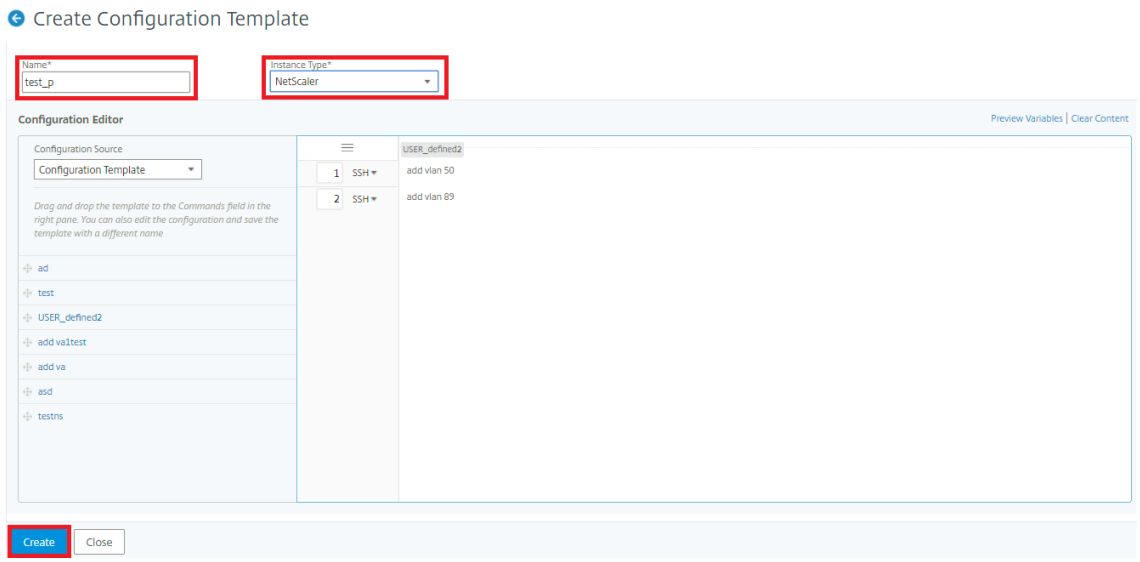
January 30, 2024

Puede exportar las plantillas de configuración desde cualquier Citrix Application Delivery Management (ADM). También puede importar el archivo al mismo Citrix ADM o a otro en cualquier momento en el futuro. Los datos de las plantillas de configuración (como los comandos de configuración, las definiciones de variables y los parámetros) no se pierden.

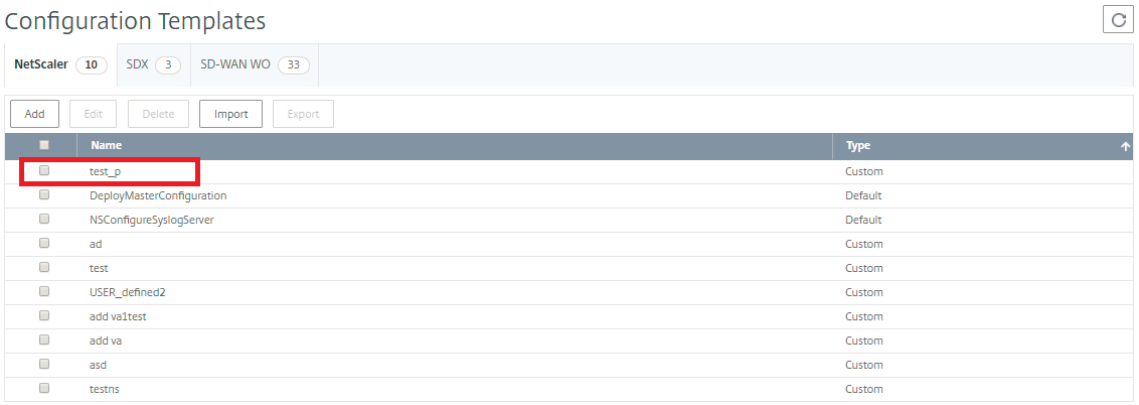
Puede exportar las plantillas de configuración a un formato de **archivo JSON** y guardarlas en la carpeta local. Puede importar la plantilla de configuración. archivos**json** en Citrix ADM. Este archivo puede ser nuevo o el que haya exportado desde el mismo Citrix ADM u otro.

Para exportar las plantillas de configuración:

1. Vaya a **Redes > Trabajos de Configuración > Plantillas de Configuración**.
2. Haga clic en el botón **Agregar** para crear la plantilla de configuración.
3. En la página **Crear Plantilla de Configuración**, especifique el nombre de la plantilla de configuración y elija el tipo de instancia. En el **Editor de configuración**, seleccione el origen de configuración como Plantilla de configuración en el menú desplegable. Puede arrastrar y soltar las plantillas de configuración existentes en el editor de configuración. Haga clic en **Crear**.



4. Vaya a **Redes > Trabajos de configuración > Plantillas de configuración** para ver las plantillas creadas en la lista de plantillas de configuración.

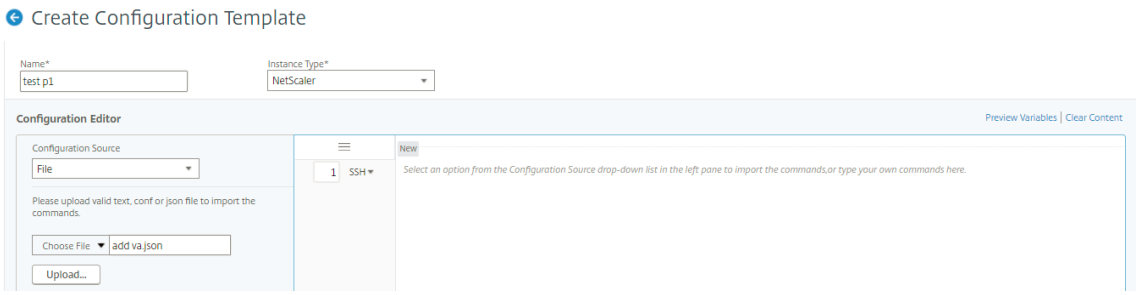


5. Seleccione la plantilla de configuración recién creada y haga clic en el botón **Exportar**.

La plantilla de configuración correspondiente se descarga en su sistema local en **formato.json**.

Para importar las plantillas de configuración:

1. Vaya a **Redes > Trabajos de configuración > Plantillas de configuración** y haga clic en el botón **Importar**. Seleccione la ruta en la que tiene. **json** de la plantilla de configuración y cargar los archivos **JSON**. Se recomienda encarecidamente cargar los archivos **JSON** que ya ha exportado.
2. También puede importar la plantilla de configuración mediante la opción **Archivo** del Editor de configuración.
3. Seleccione **Archivo** en el menú desplegable del **Editor de configuración**.
4. Selecciona **Elegir archivo** (. archivos **json**) desde su sistema local y cargue la plantilla de configuración. archivos **json** .



Nota

- Cada nueva plantilla importada se almacena con una nueva cadena de identificación.
- Puede importar las plantillas de configuración solo si el archivo está guardado en. formato **json** . Si importa las plantillas de configuración que no sean archivos **.json**, desde su sistema local, se mostrará un error y no se importarán los archivos.

Trabajos de mantenimiento

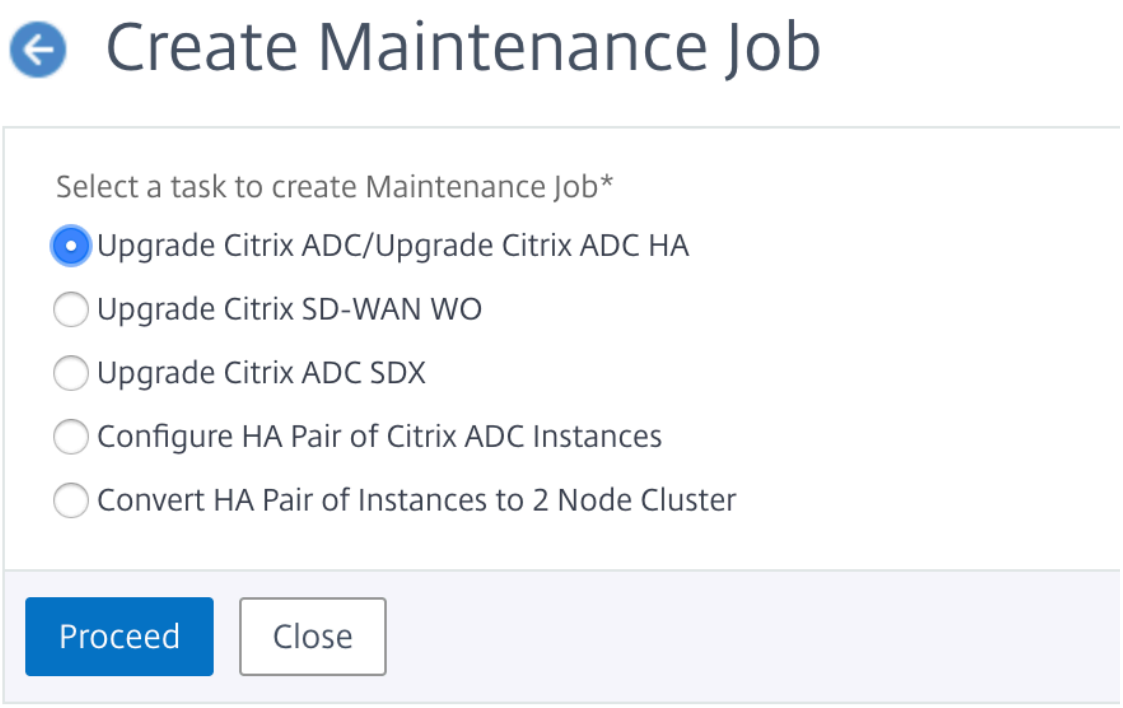
January 24, 2024

Puede crear los siguientes trabajos de mantenimiento mediante Citrix ADM. A continuación, puede programar los trabajos de mantenimiento en una fecha y hora específicas.

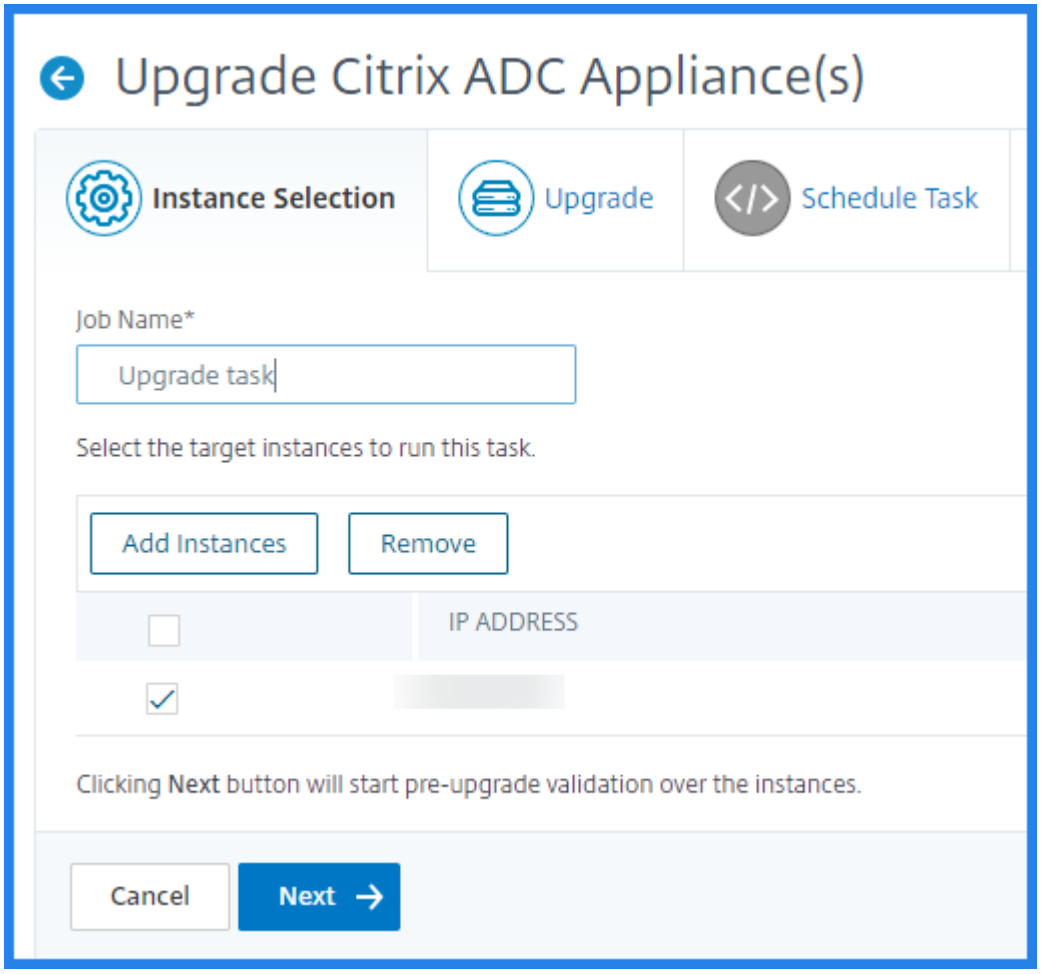
- Actualizar instancias de NetScaler ADC
- Actualice las instancias WAN-WO de Citrix SD
- Actualizar instancias SDX de NetScaler ADC
- Configurar el par HA de instancias NetScaler ADC
- Convierta un par de instancias de alta disponibilidad en un clúster de 2 nodos

Programar la actualización de instancias NetScaler ADC

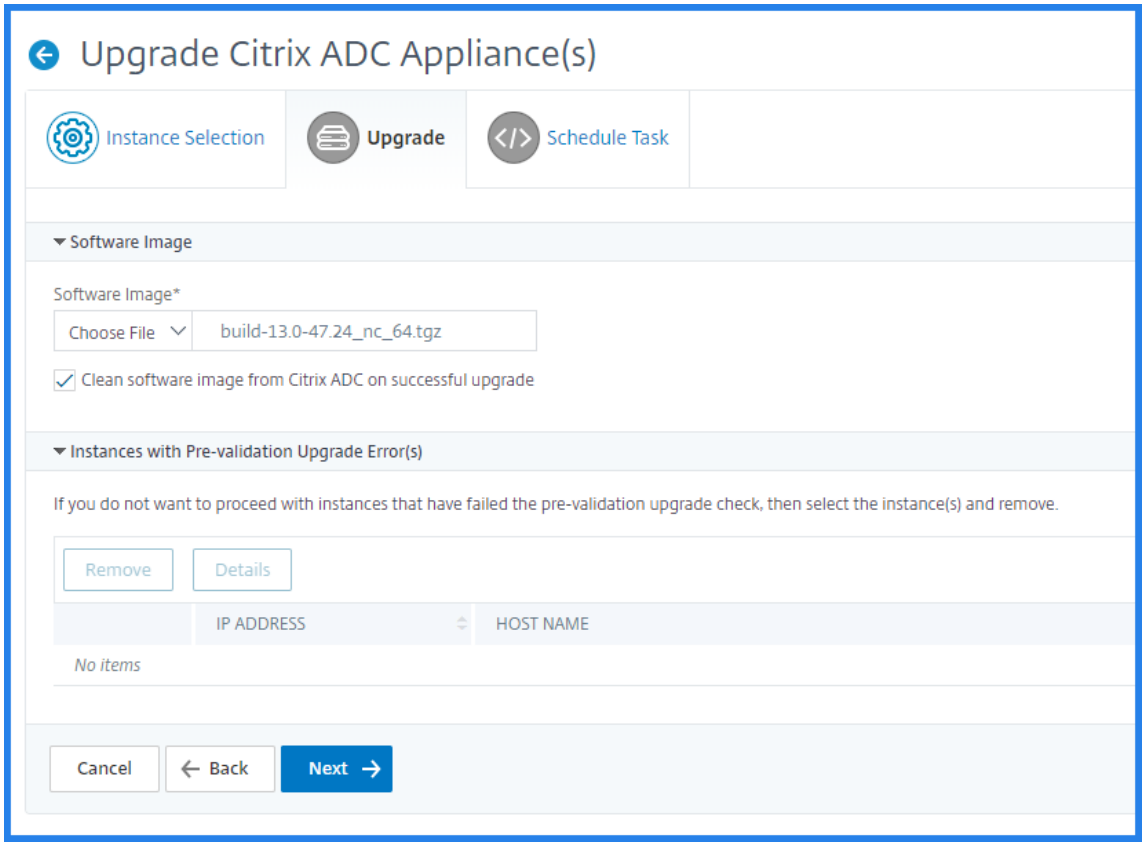
1. Vaya a **Redes** > Trabajos de **configuración > Trabajos** de **mantenimiento** . Haga clic en el botón **Crear trabajo**.
2. En la página Crear tarea de mantenimiento, seleccione **Actualizar Citrix ADC o Actualizar Citrix ADC HA** y haga clic en **Continuar**.



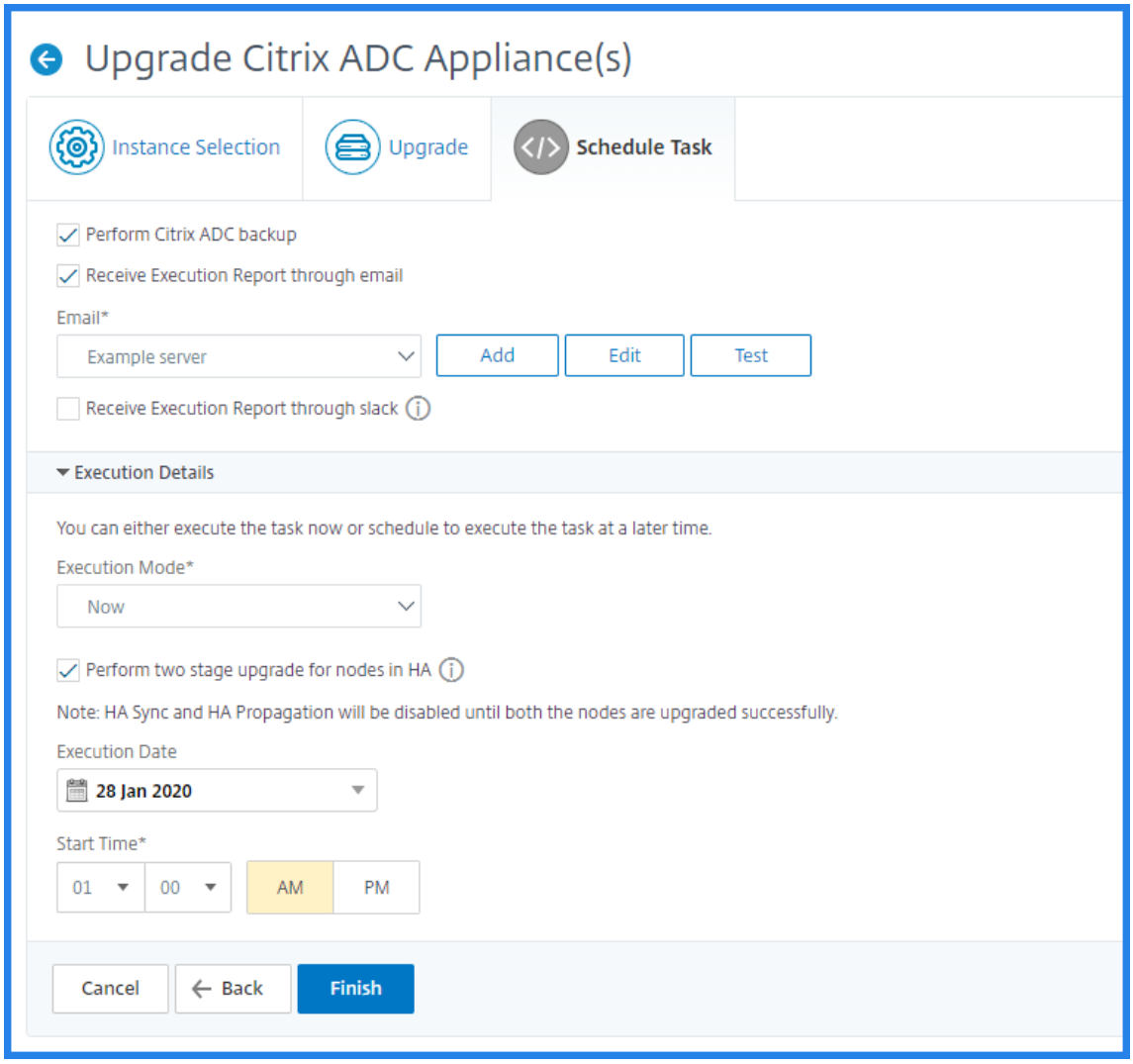
3. En la página Actualizar dispositivos Citrix ADC, en la pestaña **Selección** de instancias , agregue las instancias Citrix ADC en las que quiere ejecutar el proceso de actualización. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.



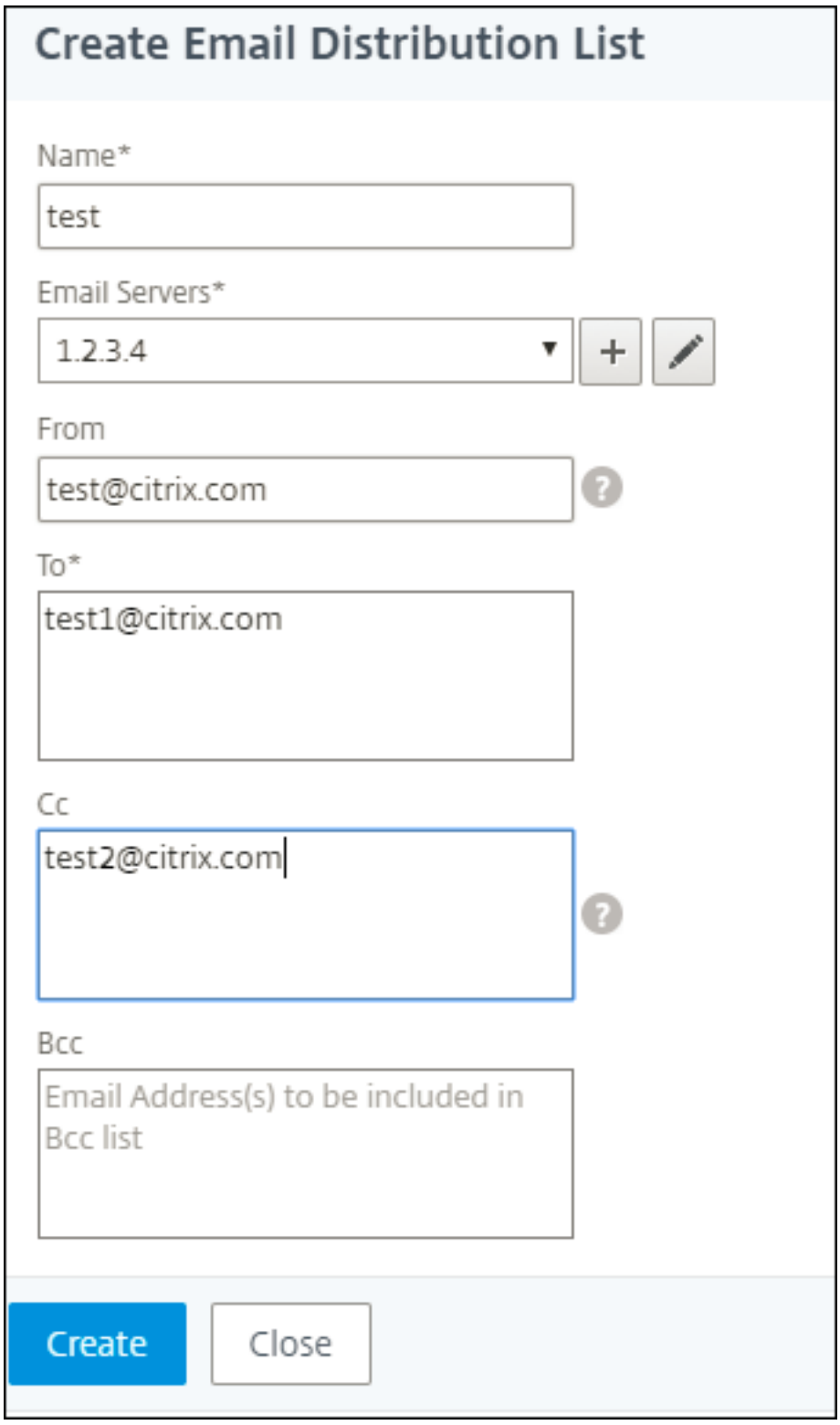
4. En la pestaña **Actualización** , en la lista de imágenes de software, seleccione Local (su máquina local) o Dispositivo (el archivo de compilación debe estar presente en el dispositivo virtual Citrix ADM).



5. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución de la actualización de instancias de NetScaler ADC. Haga clic en la casilla **Recibir informe de ejecución por correo electrónico** para habilitar la notificación por correo electrónico.
6. Seleccione el icono + para crear la lista de distribución de correo electrónico.
7. Para actualizar la instancia de Citrix ADC ahora, seleccione **Ahora** en la lista Modo de ejecución.
8. Para actualizar la instancia de Citrix ADC más adelante, seleccione Más **tarde** en la lista Modo de ejecución. A continuación, puede elegir la fecha de ejecución y la hora de inicio para actualizar las instancias de Citrix ADC.

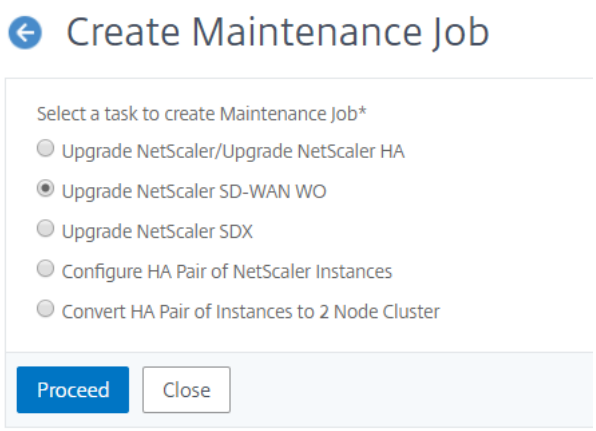


9. En la página **Crear lista de distribución de correo** electrónico , especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el cuadro **De**, agregue la dirección de correo electrónico desde la que quiere enviar mensajes. En el cuadro **Para**, agregue la dirección o las direcciones de correo electrónico a las que quiere enviar los mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en Crear. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

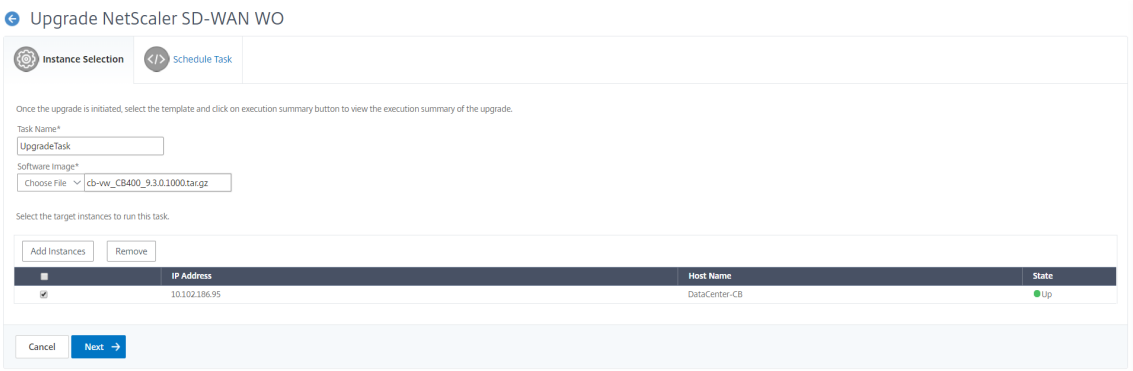


Programar la actualización de instancias WO de Citrix SD-WAN

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.
2. En la página **Crear trabajo de mantenimiento**, seleccione **Actualizar Citrix SD-WAN WO** y haga clic en **Continuar**.



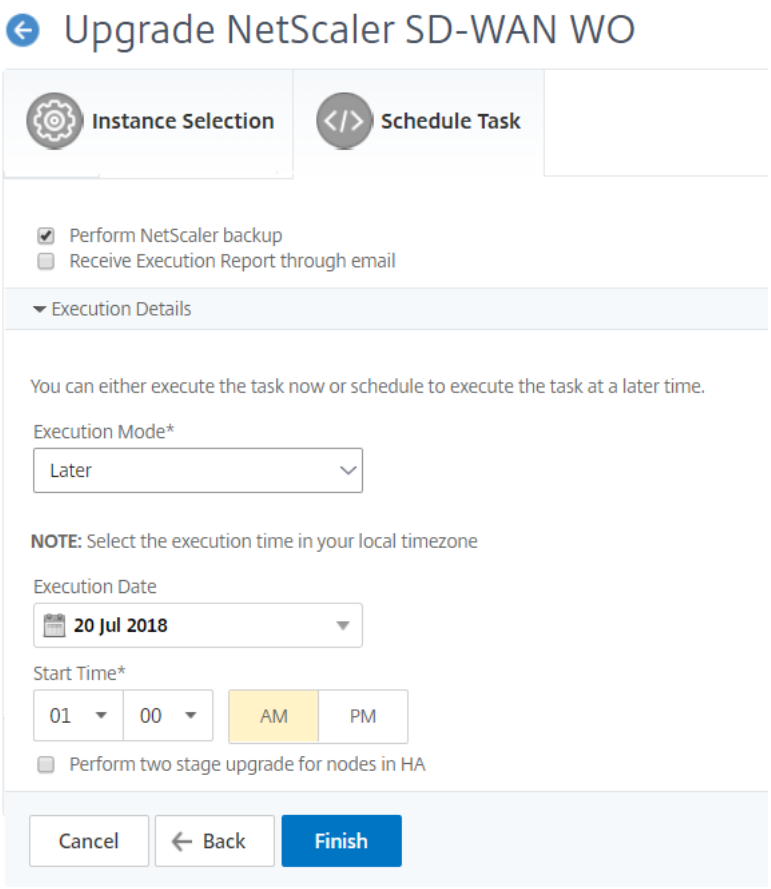
3. En la página **Actualizar Citrix SD-WAN WO** , en la pestaña **Selección de instancias** , agregue un **nombre de tarea** . En la lista de imágenes de software, seleccione Local (su máquina local) o Dispositivo (el archivo de compilación debe estar presente en el dispositivo virtual Citrix MAS). Agregue las instancias WO de Citrix SD-WAN en las que desea ejecutar el proceso de actualización. Haga clic en **Siguiente**.



4. Para actualizar ahora la instancia WO de Citrix SD-WAN, seleccione **Ahora** en la lista **Modo de ejecución**. Haga clic en **Finalizar**.
5. Para actualizar la instancia WO de Citrix SD-WAN más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de ejecución y la hora de inicio para actualizar la instancia WO de Citrix SD-WAN.
6. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución de la actualización de la instancia WO de Citrix SD-WAN. Haga clic en la casilla **Recibir informe de**

ejecución por correo electrónico para habilitar la notificación por correo electrónico.

7. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.

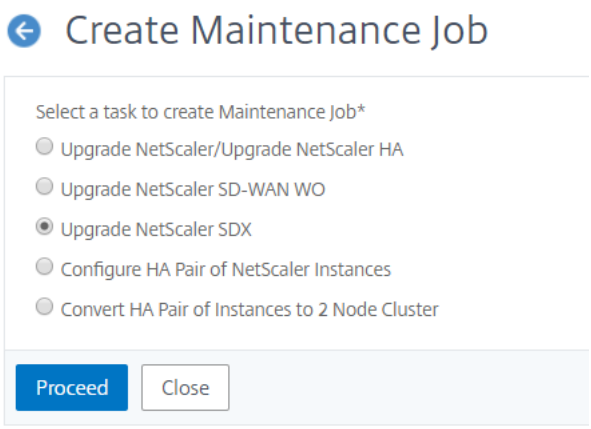


8. En la página **Crear lista de distribución de correo electrónico**, especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el cuadro **De**, agregue la dirección de correo electrónico desde la que quiere enviar mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

Programar la actualización de instancias de NetScaler ADC SDX

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.

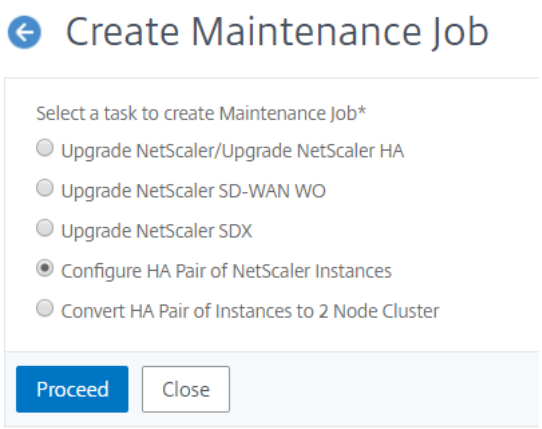
2. En la página **Crear trabajo de mantenimiento** , seleccione **Actualizar Citrix ADC SDX** y haga clic en **Continuar**.



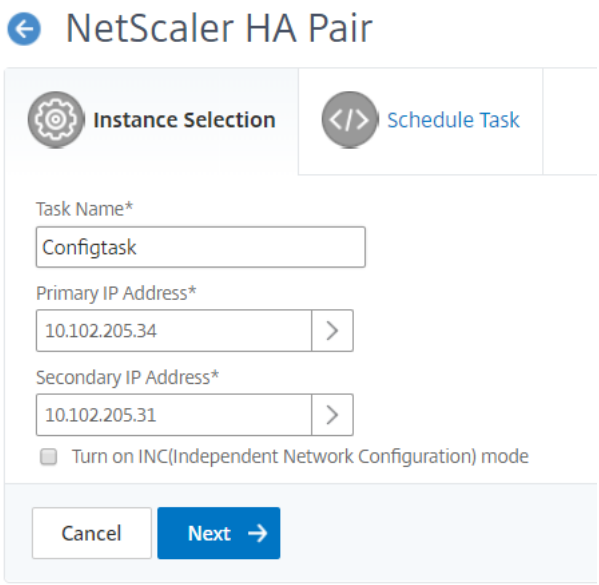
3. En la página **Actualizar dispositivos NetScaler ADC SDX**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. En la lista de imágenes de software, seleccione Local (su máquina local) o Dispositivo (el archivo de compilación debe estar presente en el dispositivo virtual NetScaler ADM). Agregue las instancias de NetScaler ADC SDX en las que quiere ejecutar el proceso de actualización. Haga clic en **Siguiente**.
4. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución de la actualización de la instancia SDX de NetScaler ADC. Haga clic en la casilla **Recibir informe de ejecución por correo electrónico** para habilitar la notificación por correo electrónico.
5. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
6. Para actualizar la instancia Citrix ADC SDX ahora, seleccione **Ahora** en la lista **Modo de ejecución**. Haga clic en **Finalizar**.
7. Para actualizar la instancia Citrix ADC SDX más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de ejecución y la hora de inicio para actualizar la instancia de NetScaler ADC SDX.
8. En la página **Crear lista de distribución de correo electrónico**, especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el cuadro **De**, agregue la dirección de correo electrónico desde la que quiere enviar mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

Programar la configuración del par HA de instancias NetScaler ADC

1. Vaya a **Redes** > Trabajos de **configuración > Trabajos** de **mantenimiento** . Haga clic en el botón **Crear trabajo**.
2. En la página **Crear trabajo de mantenimiento**, seleccione **Configurar par de instancias de NetScaler ADC** y haga clic en **Continuar**.



3. En la página **NetScaler ADC HA Pair**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. Introduzca la dirección IP principal y la dirección secundaria y haga clic en **Siguiente**.

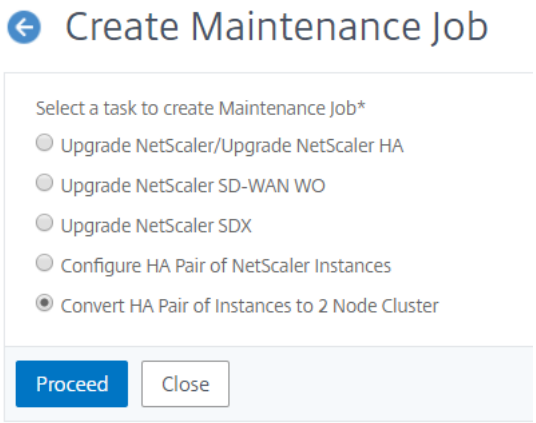


4. En la ficha **Programar tarea**, puede elegir configurar el par NetScaler ADC HA ahora o posterior.
5. Para configurar ahora el par Citrix ADC HA, seleccione **Ahora** en la lista **Modo de ejecución** . Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución del par de NetScaler ADC HA. Haga clic en la casilla **Recibir informe de ejecución por correo electrónico** para habilitar la notificación por correo electrónico.

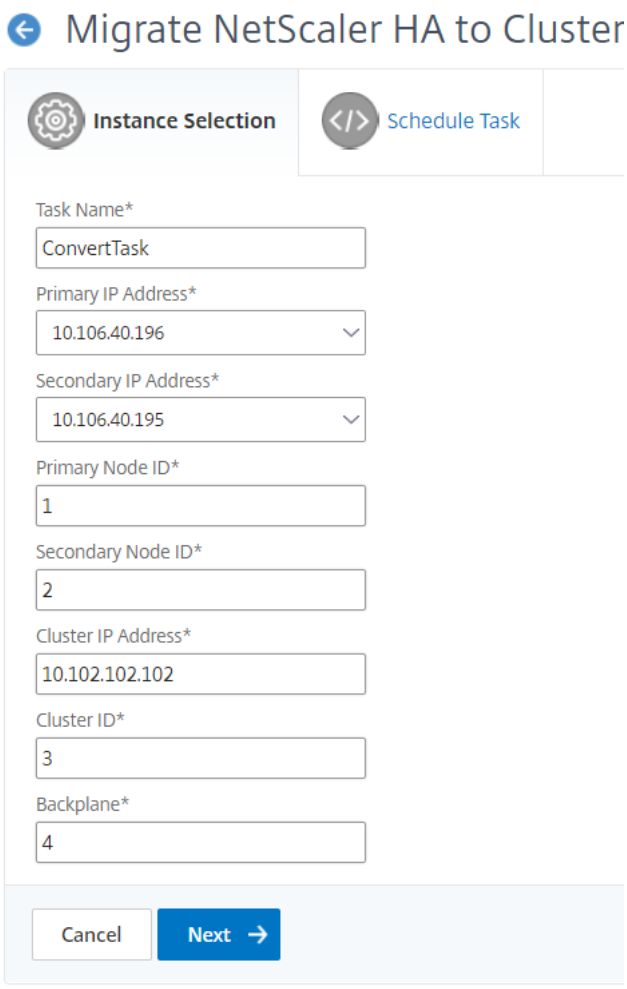
6. Para configurar el par Citrix ADC HA más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de eExecution y la hora de inicio. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución del par de NetScaler ADC HA. Haga clic en la casilla **Recibir informe de ejecución por correo electrónico** para habilitar la notificación por correo electrónico.
7. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
8. En la página **Crear lista de distribución de correo** electrónico , especifique un **nombre** para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el **cuadro**De , agrega la dirección de correo electrónico desde la que deseas enviar los mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

Programar la conversión de par de instancias de alta disponibilidad en clúster

1. Vaya a **Redes** > Trabajos de **configuración > Trabajos** de **mantenimiento** . Haga clic en el botón **Crear trabajo**.
2. En la página **Crear Trabajo de Mantenimiento**, seleccione **Convertir par de instancias de HA a clúster de 2 nodos** y haga clic en **Continuar**.



3. En la página **Migrar NetScaler ADC HA al clúster**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. Especifique la dirección IP principal, la dirección secundaria, el ID del nodo principal, el ID del nodo secundario, la dirección IP del clúster, el ID del clúster y el plano posterior. Haga clic en **Siguiente**.



4. En la ficha **Programar tarea**, puede optar por migrar NetScaler ADC HA al clúster ahora o posterior.
5. Para configurar el par Citrix ADC HA más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de ejecución y la hora de inicio. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución del par de NetScaler ADC HA. Haga clic en la casilla **Recibir informe de ejecución por correo electrónico** para habilitar la notificación por correo electrónico.
6. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
7. En la página **Crear lista de distribución de correo electrónico**, especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el **cuadro**De , agrega la dirección de correo electrónico desde la que deseas enviar los mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que en-

viar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

Auditoría de configuración

January 30, 2024

Este documento incluye:

- Creación de plantillas de auditoría
- Visualización de Informes de Auditoría
- Modificaciones de configuración de auditoría en todas las instancias
- Obtener consejos de configuración sobre la configuración de red
- Cómo sondear la auditoría de configuración de instancias de NetScaler

Crear plantillas de auditoría

January 30, 2024

Debe asegurarse de que ciertas configuraciones se ejecuten en instancias específicas para lograr un rendimiento óptimo de la red. También querrá supervisar los cambios de configuración en las instancias administradas de Citrix Application Delivery Controller (ADC), solucionar errores de configuración y recuperar las configuraciones no guardadas tras un cierre repentino del sistema. Puede crear plantillas de auditoría con configuraciones específicas que quiera auditar en determinadas instancias. Citrix Application Delivery Management (Citrix ADM) compara estas instancias con la plantilla de auditoría e informa si hay alguna discrepancia en la configuración. Cuando hay una discrepancia en la configuración, Citrix ADM genera un informe de diferencias de configuración que permite solucionar problemas y rectificar los cambios de configuración no deseados.

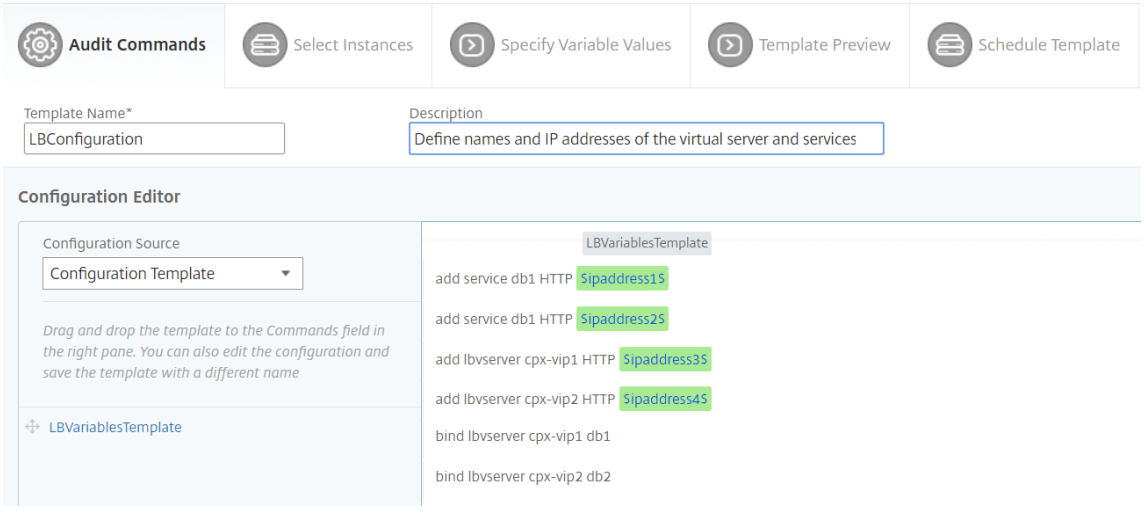
Puede automatizar la ejecución de la plantilla de auditoría mediante

- Programar la hora a la que se debe ejecutar la plantilla
- Establecer la frecuencia con la que Citrix ADM debe ejecutar la plantilla. Puede ejecutar la plantilla diariamente, en un día específico de una semana o en una fecha específica de un mes.

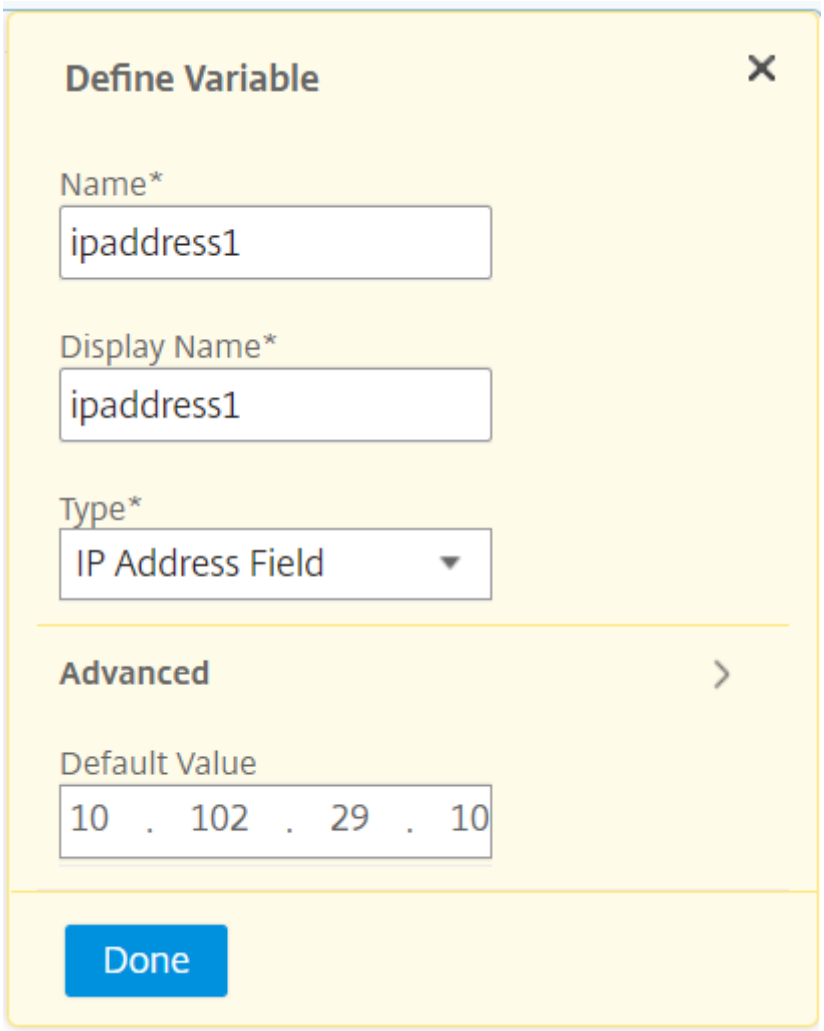
Además, tiene la opción de enviar el informe de diferencias generado por NetScaler ADM a las direcciones de correo electrónico especificadas que puede configurar. Con esta opción, el usuario puede recibir el informe como datos adjuntos de correo y no es necesario que el usuario inicie sesión en NetScaler ADM para exportar los informes manualmente.

Para crear plantillas de auditoría:

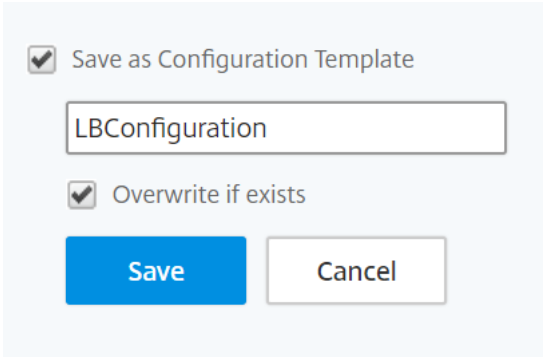
1. Vaya a **Redes** > **Auditoría de configuración** > **Plantillas de auditoría** y haga clic en **Agregar** .
2. En la página**Crear plantilla** y en la ficha**Comandos de auditoría**, especifique el nombre de la plantilla y su descripción.
3. En la página **Editor de configuración**, escriba los comandos y guárdelos como una plantilla de configuración. También puede arrastrar una plantilla existente desde el panel izquierdo hasta el editor.
4. Seleccione los valores que desee convertir en una variable y, a continuación, haga clic en**Convertir en variable**. Por ejemplo, seleccione la dirección IP del servidor de equilibrio de carga “ipaddress1”y haga clic en**Convertir**en variable. La variable ahora se incluye con “$”, como se muestra en la imagen siguiente.



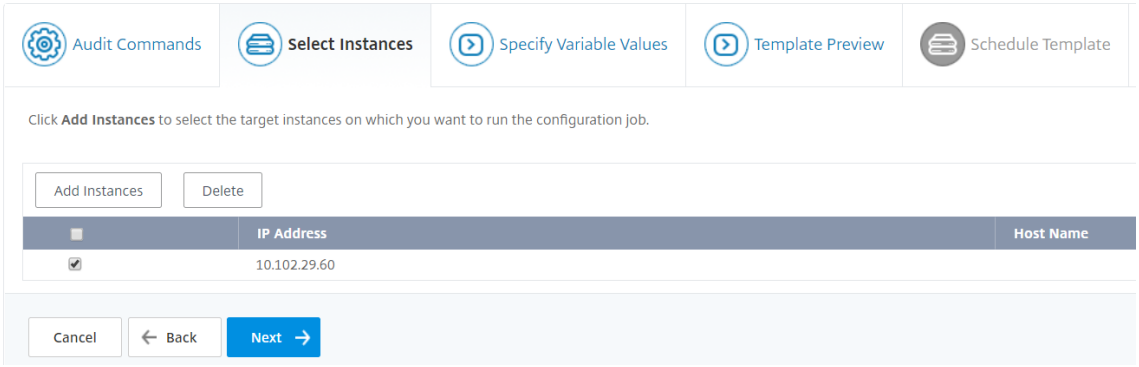
En la ventana **Definir variable**, defina las propiedades de esta variable: Nombre, nombre para mostrar y tipo de variable. Haga clic en la opción **Avanzado** si quiere especificar un valor predeterminado para la variable.



También puede guardar los comandos como una plantilla de configuración.



5. Haga clic en **Guardar** y, a continuación, en **Siguiente** .
6. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración y haga clic en **Siguiente**.

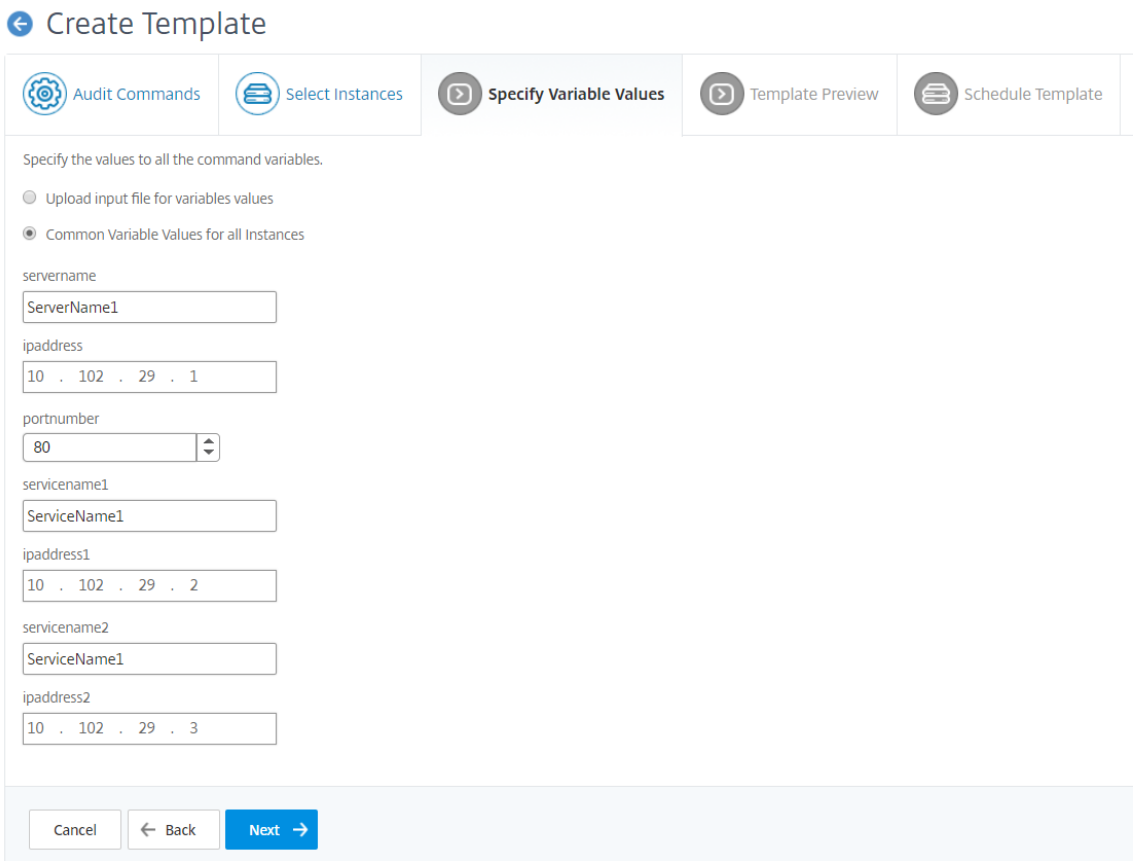


7. En la ficha **Especificar valores de variable**, tiene dos opciones:

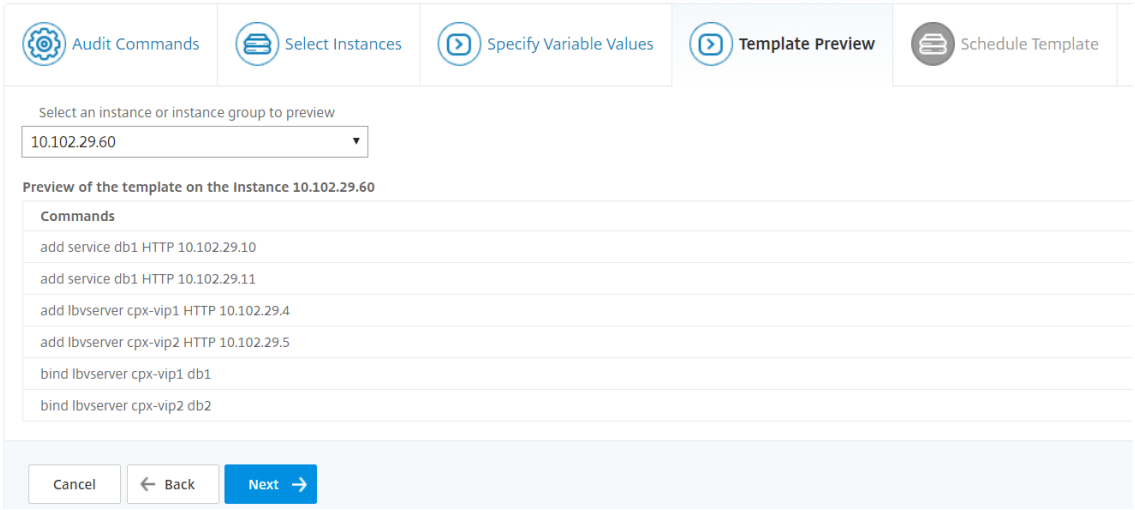
   a) Descargue el archivo de entrada para especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor NetScaler ADM

   b) Introduzca valores comunes para las variables que ha definido para todas las instancias.

8. Haga clic en **Siguiente**.



9. En la ficha **Vista previa de plantilla**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias. Haga clic en **Siguiente**.



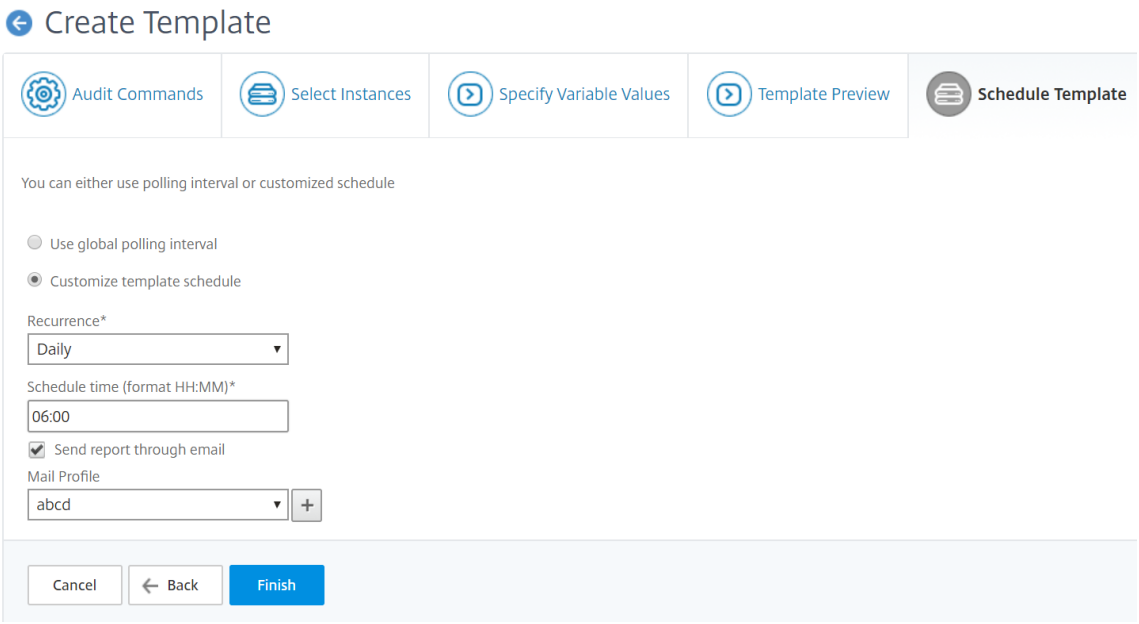
10. En la ficha **Plantilla de programación**, tiene las siguientes opciones para programar la ejecución de la plantilla y configurar la dirección de correo para enviar el informe de diferencias.

    - **Utilice el intervalo de sondeo global**. Seleccione esta opción para ejecutar la plantilla en las instancias a la vez configuradas globalmente en NetScaler ADM.

      > **Nota**
      >
      > Para configurar el intervalo de sondeo global en NetScaler ADM, vaya a **Redes** > **Auditoría de configuración** > **Plantillas de auditoría y haga** clic en **Intervalo de sondeo global**. En el campo **Intervalo de sondeo** , introduzca los minutos en los que Citrix ADM debe sondear las instancias de forma global.

    - **Personalizar la planificación de plantillas**. Utilice esta opción para configurar la hora y la frecuencia a la que se deben ejecutar las plantillas
    - **Enviar el informe por correo**electrónico . Utilice esta opción para configurar el perfil de correo al que se debe enviar el informe de diferencias como archivo adjunto de correo.

11. Haga clic en **Finalizar**.



La plantilla de auditoría aparece en la lista **Plantillas de auditoría** y se ejecuta a la hora programada en las configuraciones de las instancias especificadas.

Ver informes de auditoría

January 30, 2024

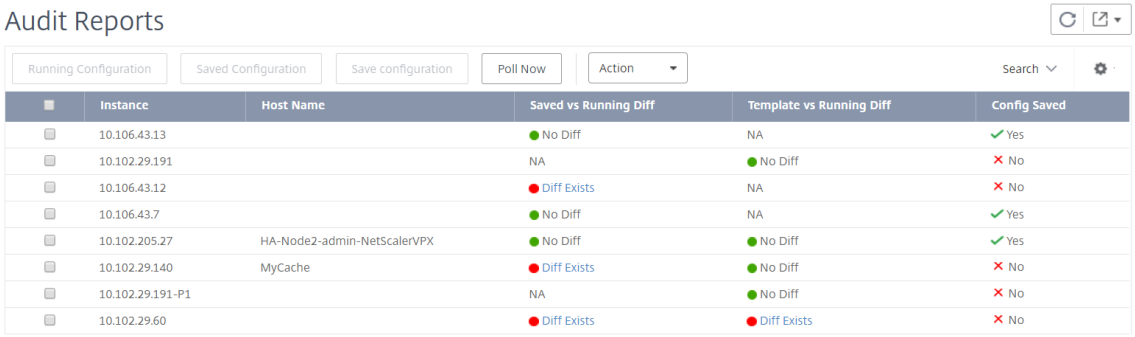
Citrix Application Delivery Management (Citrix ADM) le permite ver y descargar el informe de diferencias de auditoría de configuración en la sección de auditoría de configuración. La sección de auditoría de configuración le permite exportar el informe resumido en todas las instancias y por instancia, y también le permite exportar un informe detallado de diferencias para cada par instancia-plantilla.

Las plantillas de auditoría que aparecen en la lista Plantillas de auditoría se ejecutan a la hora programada en las configuraciones de las instancias especificadas. El gráfico de **desviaciones de configuración de NetScaler** del panel de **auditoría de configuración** muestra detalles de alto nivel sobre los cambios de configuración entre las configuraciones guardadas y no guardadas. Al hacer clic en el gráfico de **derivas de NetScaler Config** , la siguiente página de **informes de auditoría** muestra una lista de instancias que muestra tanto «La diferencia existe» como «No hay diferencia». « Puede descargar los informes de diferencias que muestra Citrix ADM.

NetScaler ADM también ofrece una opción para programar la exportación automática de informes diff como datos adjuntos de correo. Para obtener más información sobre cómo programar la exportación de informes, consulte Creación de plantillas de auditoría.

Para exportar informes de auditoría de configuración:

1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .
2. En la página **Auditoría de configuración**, haga clic dentro del gráfico de **desviaciones de configuración de NetScaler**.
3. La página **Informes de Auditoría** muestra las instancias que tienen una diferencia. La página también muestra una lista de instancias que no tienen ninguna diferencia en sus configuraciones en ejecución.

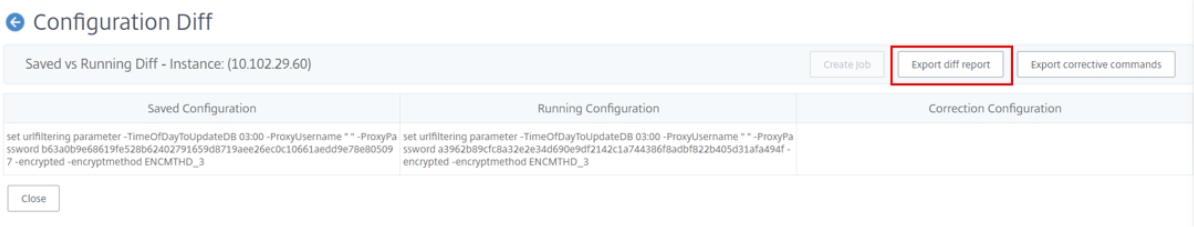


En la imagen puede ver que para algunos casos un diff está presente solo en **Saved Vs Running Diff** y para algunos casos, un diff está presente solo en **Template vs Running Diff**. En algunos casos, existen diferencias entre **Saved Vs Running Diff** y **Template vs Running Diff.**

Diferencia guardada frente a ejecución

Puede ver un informe de la diferencia entre la configuración guardada en la instancia y la configuración que se ejecuta actualmente en esa instancia. Por ejemplo, haga clic en **Diff Exists**para ver una instancia en **Saved Vs Running Diff.**

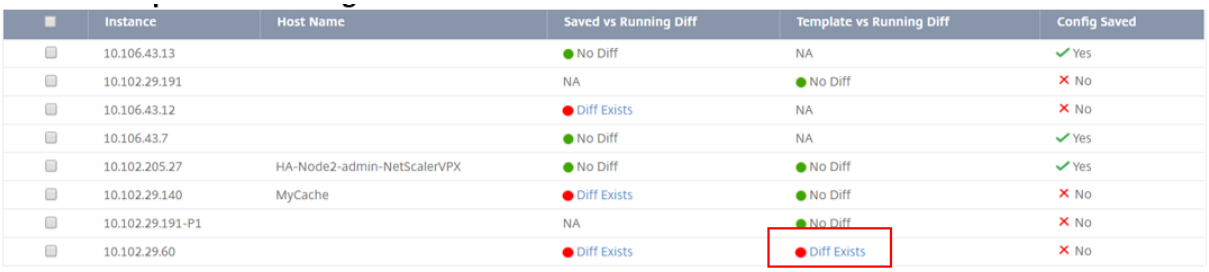
Aquí, puede ver un informe para la configuración guardada contra la ejecución de diff de configuración para esa instancia.



Haga clic en **Exportar informe de diferencias** para descargar un archivo CSV del informe de diferencias. También puede hacer clic en Exportar comandos correctivos para exportar los comandos a un archivo.txt. A continuación, puede ejecutar los comandos en la instancia de Citrix ADM asociada desde los trabajos de configuración para corregir la configuración en esa instancia.

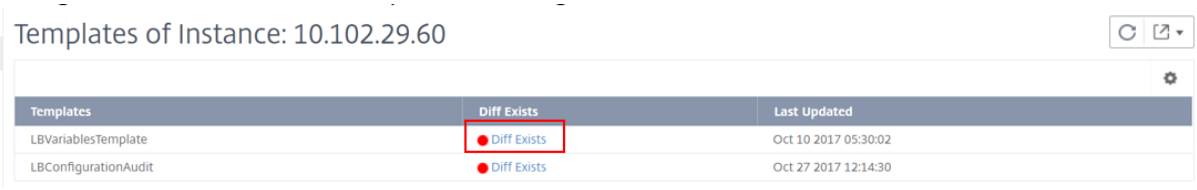
Plantilla vs Diff Running

La **diferencia entre plantilla y ejecución** incluye todas las plantillas excepto **Saved Vs Running Diff**, que es la plantilla predeterminada. Puede ver la diferencia que existe entre la plantilla y la configuración en ejecución. Por ejemplo, haga clic en **Diff Exists** para una de las instancias en **Template vs Running Diff.**

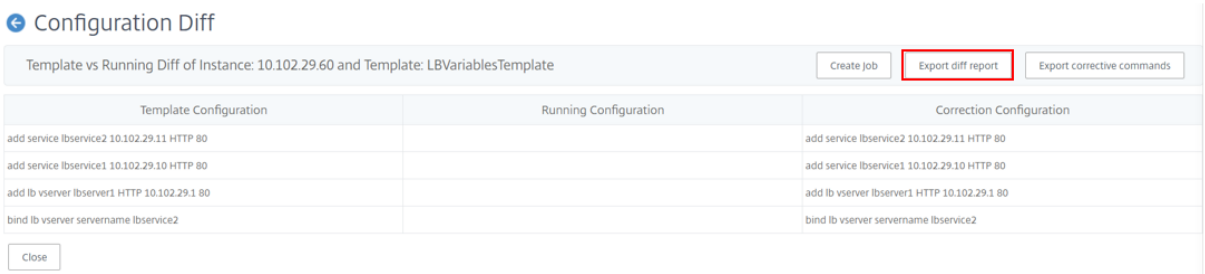


Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

Ahora puede ver que dos plantillas muestran diff y que la instancia NetScaler ADM tiene una configuración diferente de la que está buscando la plantilla.



Haga clic de nuevo en**Diff Exists**. La siguiente imagen muestra la configuración que está buscando la plantilla y la configuración en ejecución que está en blanco, ya que no se ha configurado ni se ha eliminado ningún comando de este tipo. También puede ver las configuraciones de corrección o los comandos que se van a ejecutar para corregir la configuración.



Haga clic en **Exportar informe de diferencias** para descargar un archivo CSV del informe de diferencias. También puede hacer clic en **Exportar comandos correctivos** para exportar los comandos a un

archivo.txt. A continuación, puede ejecutar los comandos de la CLI para corregir la configuración en esa instancia.

La siguiente imagen muestra un ejemplo de archivo diff CSV que se descarga en su sistema:

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

Auditar los cambios de configuración en todas las instancias

January 30, 2024

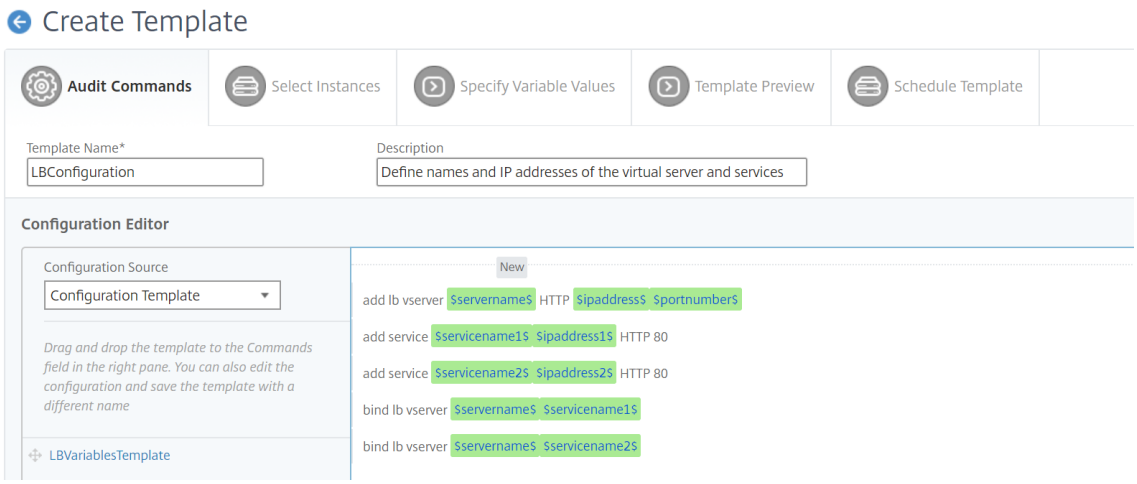
Debe asegurarse de que ciertas configuraciones se ejecuten en instancias específicas para lograr un rendimiento óptimo de la red. También querrá supervisar los cambios de configuración en las instancias administradas de Citrix Application Delivery Controller (ADC), solucionar errores de configuración y recuperar las configuraciones no guardadas tras un cierre repentino del sistema. Puede crear plantillas de auditoría con configuraciones específicas que desee que se ejecuten en determinadas instancias. NetScaler Application Delivery Management (NetScaler ADM) compara estas instancias con la plantilla de auditoría y los informes si la configuración no coincide. Esto le permite solucionar problemas y rectificar los errores.

Puede automatizar la ejecución de la plantilla de auditoría programando la hora a la que se debe ejecutar la plantilla. También puede establecer la frecuencia con la que Citrix ADM debe ejecutar la plantilla. Puede ejecutar la plantilla diariamente, en un día específico de una semana o en una fecha específica de un mes. También tiene la opción de enviar el informe de diferencias generado por Citrix ADM a las direcciones de correo electrónico especificadas que puede configurar. Con esta opción, el usuario recibe el informe como datos adjuntos de correo y no es necesario que el usuario inicie sesión en NetScaler ADM para comprobar los informes manualmente.

Para crear plantillas de auditoría:

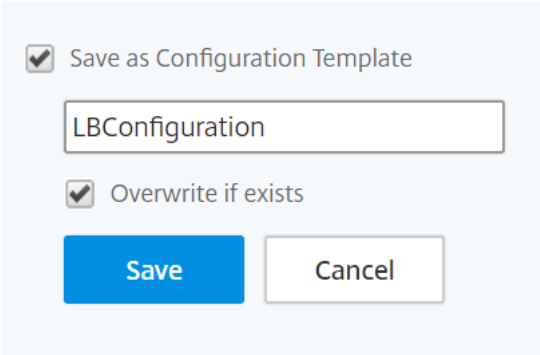
1. Vaya a **Redes > Auditoría de configuración > Plantillas de auditoría** y haga clic en **Agregar** .
2. En la página**Crear plantilla** y en la ficha**Comandos de auditoría**, especifique el nombre de la plantilla y su descripción.
3. En el **Editor de configuración**, escriba los comandos y guárdelos como una plantilla de configuración. También puedes arrastrar y soltar una plantilla existente desde el panel izquierdo del editor.

4. Seleccione los valores que desee convertir en una variable y, a continuación, haga clic en**Convertir en variable**. Por ejemplo, seleccione la dirección IP del servidor de equilibrio de carga «ipaddress» y haga clic en **Convertir en variable** , como se muestra en la imagen siguiente.



Haga clic en la opción **Avanzado** si quiere especificar un valor predeterminado para la variable.

También puede guardar los comandos como una plantilla de configuración.

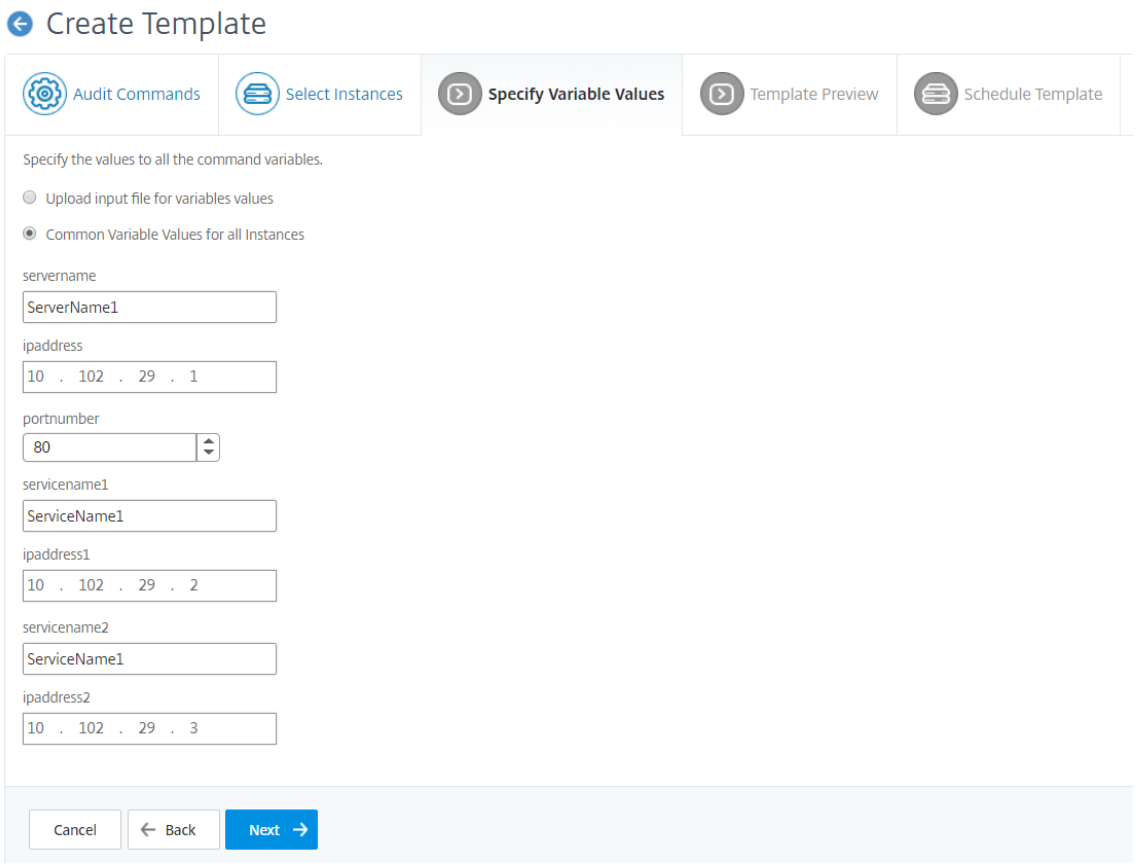


5. Haga clic en **Guardar** y, a continuación, en **Siguiente** .
6. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración.
7. En la ficha **Especificar valores de variable**, tiene dos opciones:

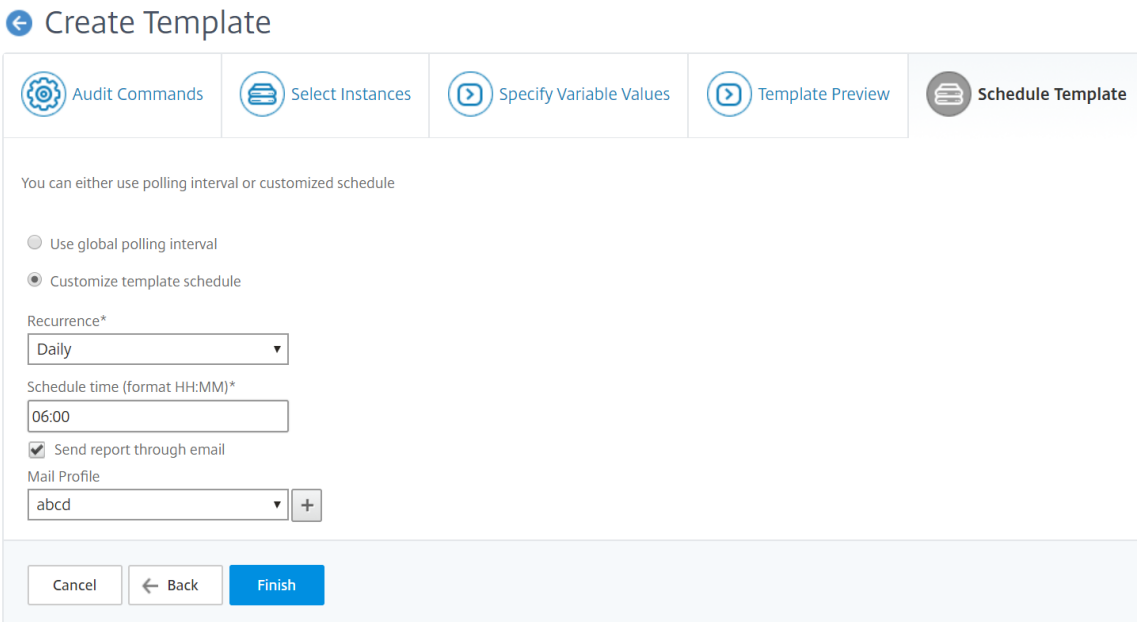
   a) Descargue el archivo de entrada para especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor NetScaler ADM

   b) Introduzca valores comunes para las variables que ha definido para todas las instancias.

8. Haga clic en **Siguiente**.



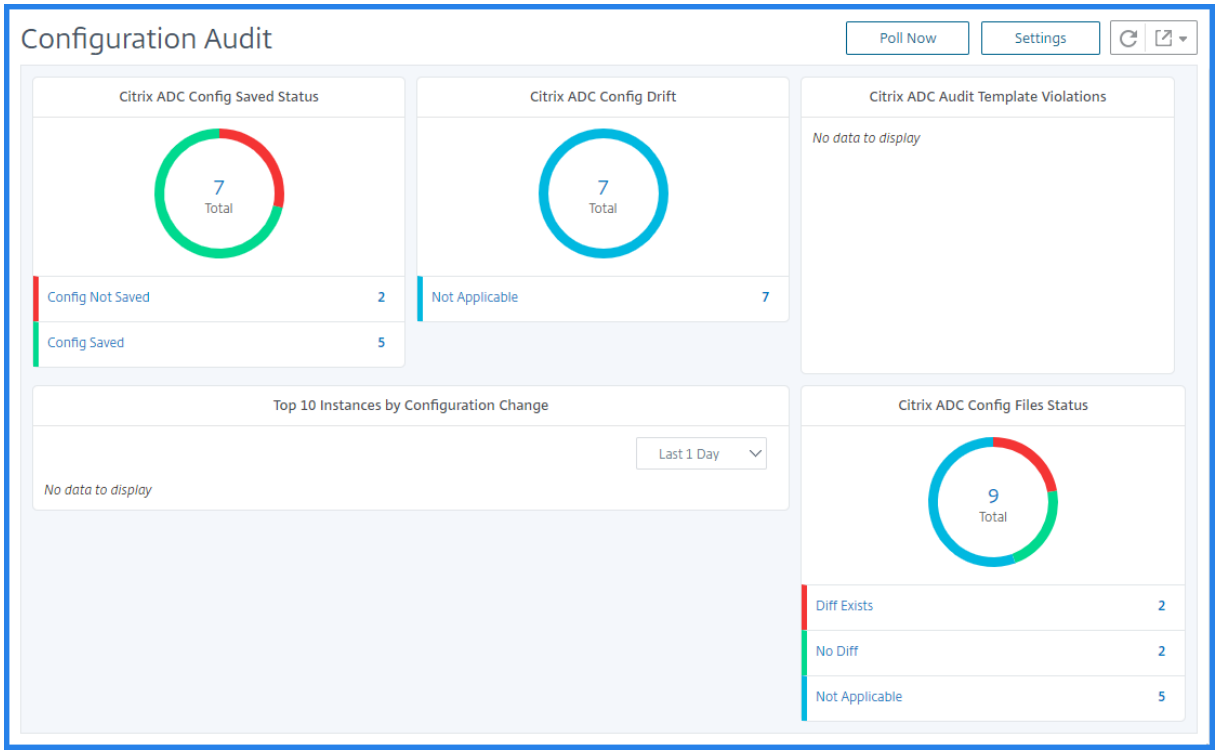
9. En la ficha **Vista previa de plantilla**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias. Haga clic en **Siguiente**.
10. En la ficha **Plantilla de programación**, tiene tres opciones para automatizar la ejecución de la plantilla y la dirección de correo para enviar el informe de diferencias.
    - **Utilice el intervalo de sondeo global**. Seleccione esta opción para ejecutar la plantilla en las instancias a la hora configurada globalmente en NetScaler ADM.
    - **Personalizar la planificación de plantillas**. Utilice esta opción para configurar la hora y la frecuencia a la que se deben ejecutar las plantillas
    - **Enviar el informe por correo**electrónico . Utilice esta opción para configurar el perfil de correo al que se debe enviar el informe de diferencias como archivo adjunto de correo.
11. Haga clic en **Finalizar**.



La plantilla de auditoría aparece en la lista Plantillas de auditoría y se ejecuta a la hora programada en las configuraciones de las instancias especificadas.

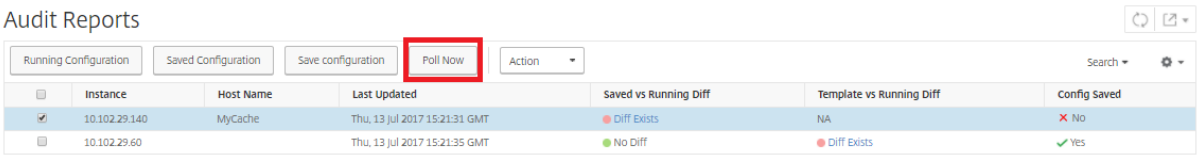
Visualización de detalles de cambios de configuración

También puede usar el panel de auditoría de configuración para ver detalles de alto nivel sobre los cambios de configuración, como las diez instancias principales por cambio de configuración o el número de configuraciones guardadas y no guardadas.



NetScaler ADM también le permite sondear auditorías de configuración manualmente y agrega todas las auditorías de configuración de las instancias inmediatamente al NetScaler ADM. Para ello, vaya a Redes **>** **Auditoría de configuración,** haga clic en Sondear **ahora** . La página emergente Sondear **ahora** le ofrece la opción de sondear todas las instancias de Citrix ADC de la red o sondear las instancias seleccionadas.

También puede forzar una auditoría en una instancia. Para ello, haga clic en el gráfico **NetScaler Config Saved Status** o en el gráfico **NetScaler Config Drift**. En la página **Informes de auditoría** , seleccione la instancia y, en la lista **Acción** , seleccione P Poll **No** w.



Para configurar las notificaciones de auditoría de configuración:

1. Vaya a **Redes** > **Auditoría de configuración**.
2. En la página **Auditoría de configuración**, haga clic en **Configuración**.
3. En la página **Configuración de notificaciones**, haga clic en el icono **Editar** para habilitar la configuración de notificaciones.
4. Seleccione la casilla **Habilitado** y, a continuación, seleccione una lista de distribución de correo electrónico en la lista desplegable. También puede crear una lista de distribución de correo

electrónico haciendo clic en el icono **+** y especificando los detalles del servidor de correo electrónico.

Obtener consejos de configuración sobre la configuración de la red

January 30, 2024

Configure las instancias de Citrix Application Delivery Controller (ADC) con configuraciones óptimas para que pueda lograr un rendimiento óptimo en sus aplicaciones. Sin embargo, puede ocurrir que algunas configuraciones no sean configuraciones estándar y esto pueda afectar al rendimiento de las aplicaciones.

Para ayudarle a optimizar el rendimiento de las aplicaciones, NetScaler Application Delivery Management (NetScaler ADM) analiza la configuración de instancias de NetScaler ADC y le proporciona recomendaciones. Puede aplicar las configuraciones recomendadas desde NetScaler ADM.

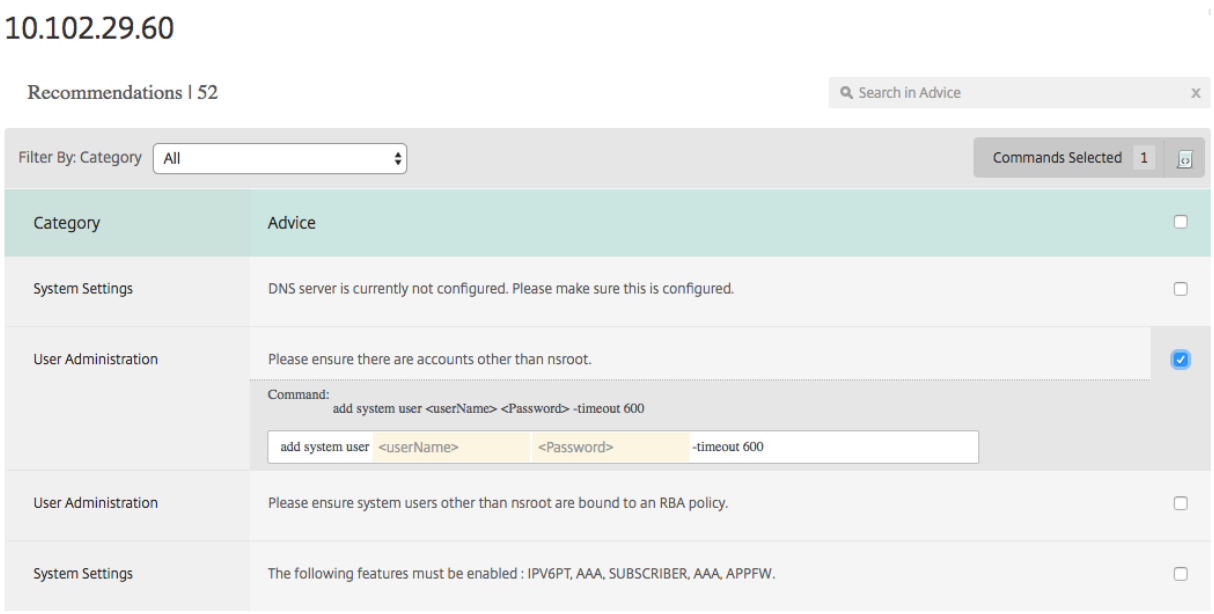
Para analizar la instancia de NetScaler ADC:

1. Vaya a **Redes** > **Auditoría de configuración** > **Asesoramiento de configuración** .
2. Lleve a cabo una de las siguientes acciones:

   - Haga clic en **Cargar archivo de configuración** y cargue el archivo de configuración de su instancia de red.

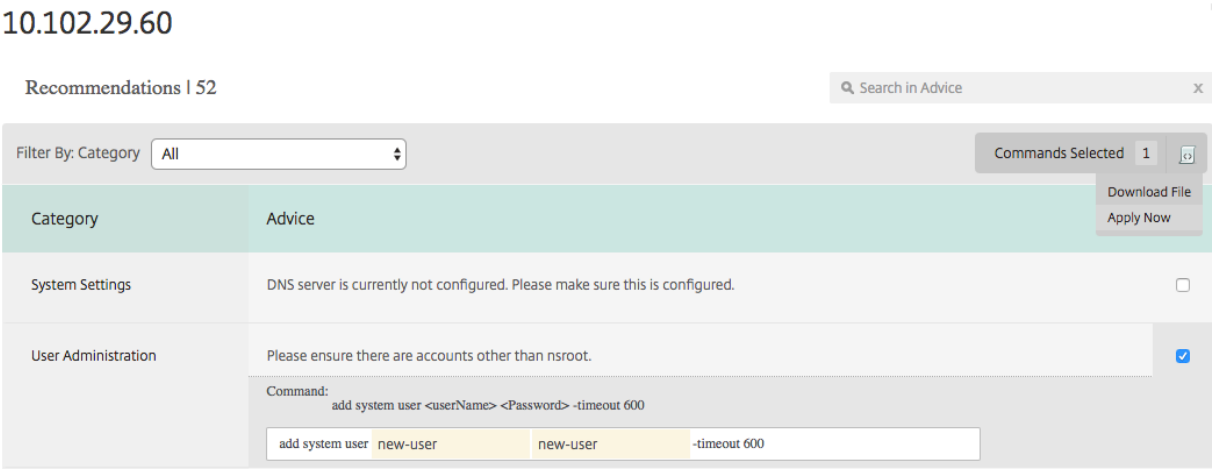
   - Haga clic en Seleccionar **dispositivo** y seleccione la instancia de Citrix ADC que quiere analizar.

Citrix ADM analiza la configuración de la instancia y proporciona una lista de recomendaciones de configuración, como se muestra en la imagen siguiente. Haga clic en la casilla de verificación situada junto a un consejo de configuración para ver los comandos correctivos.

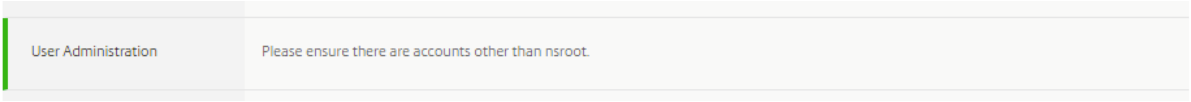


Si desea actualizar la configuración, especifique los valores de las variables en los comandos correctivos y haga clic en **Aplicar ahora** , como se muestra en la imagen siguiente.

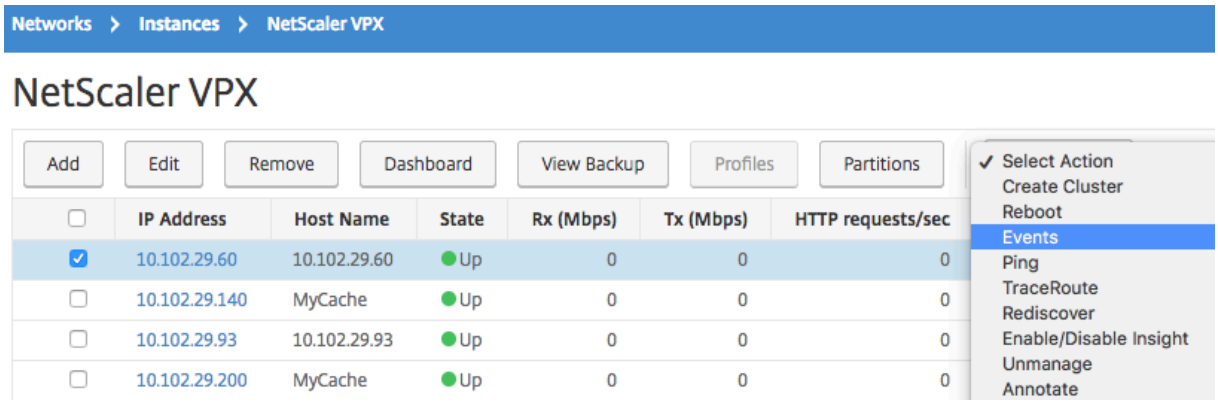
> **Nota**
>
> Los comandos que se enumeran aquí son solo recomendaciones. Un usuario con acceso de lectura y escritura podría modificar cualquier comando mediante esta función. Asegúrese de conceder un acceso privilegiado limitado a los usuarios que crea que no deberían editar los comandos.



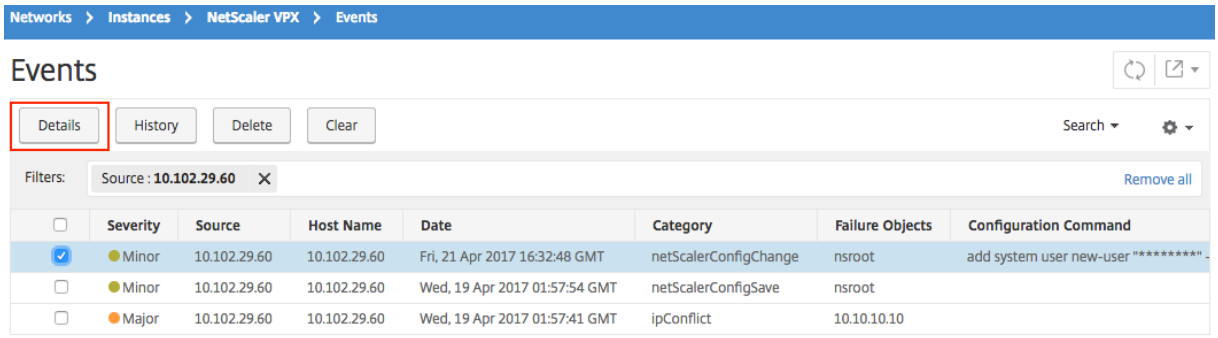
Cuando el comando se ejecuta correctamente en la instancia de red, la casilla de verificación situada junto al consejo desaparece.



Si desea ver los detalles de los comandos que se ejecutan en la instancia de red, vaya a **Redes** > **Instancias**> **, <Instance_Type>**seleccione la dirección IP de la instancia y, a continuación, haga clic en **Eventos** en la lista desplegable **Acciones** .



En la página **Eventos**, puede ver los detalles del cambio de configuración.



Auditoría de configuración de sondeo de instancias NetScaler ADC

January 30, 2024

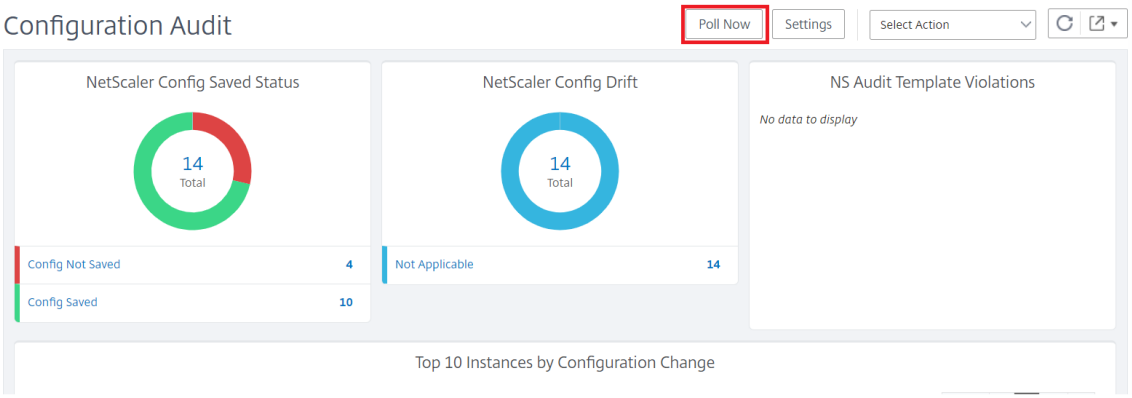
Citrix Application Delivery Management (Citrix ADM) sondea automáticamente las auditorías de configuración cada 10 horas para buscar los cambios de configuración que se producen en las instancias de Citrix Application Delivery Controller (ADC). También puede sondear manualmente las auditorías de configuración para detectar cambios recientes, pero sondear todas las instancias de configuración de NetScaler ADC coloca una carga pesada en la red.

En lugar de sondear toda la auditoría de configuración de las instancias de NetScaler ADC, puede sondear manualmente solo las auditorías de configuración de una instancia o instancias seleccionadas.

Para sondear auditorías de configuración de instancias NetScaler ADC:

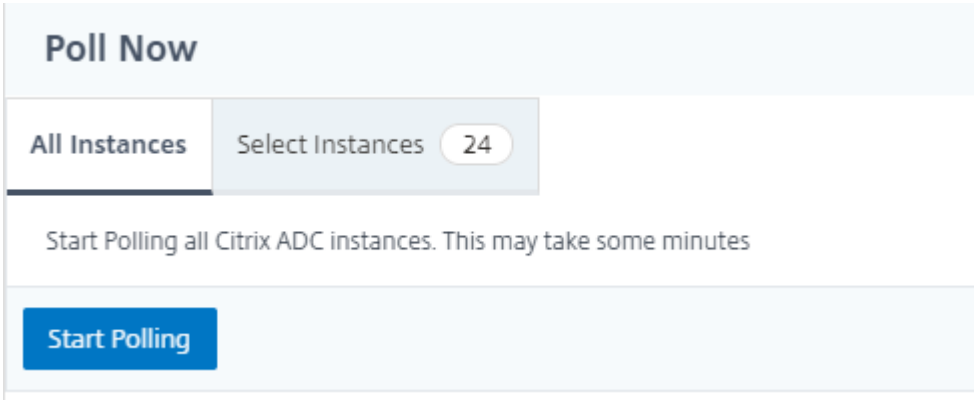
1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .

2. En la página **Auditoría de configuración**, en la esquina superior derecha, haga clic en **Sondear ahora**.

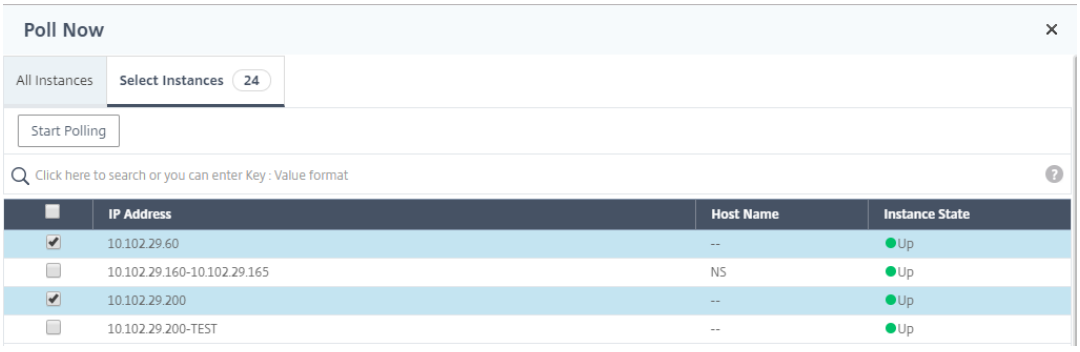


3. Aparece la página **Encuesta ahora**, que le da la opción de sondear todas las instancias de NetScaler ADC en la red o sondear las instancias seleccionadas.

   a) Para sondear todas las instancias de NetScaler ADC, seleccione la ficha **Todas las instancias** y haga clic en **Iniciar sondeo**.



   b) Para sondear instancias específicas, seleccione la ficha **Seleccionarinstancias**, seleccione las instancias de la lista y haga clic en**Sondear ahora**.



Generar diferencias de auditoría de configuración para capturas SNMP de ConfigChange

January 30, 2024

Siempre que se produzca un cambio de configuración en una instancia de Citrix Application Delivery Controller (ADC) de la red, se actualiza el archivo de configuración. La instancia envía una captura SNMP de ConfigChange a Citrix Application Delivery Management (Citrix ADM). Puede habilitar NetScaler ADM para realizar una auditoría de configuración en esa instancia cuando ésta envía una captura SNMP de ConfigChange.

Si existe alguna diferencia entre la configuración de la plantilla de auditoría y la configuración en ejecución, aparecerá un mensaje de estado Diff Exists en la página Informe de auditoría. Al hacer clic en el enlace Diff Exits , accederá a la página Configuration Diff , donde podrá ver el comando correctivo. Puede utilizar estos comandos correctivos para crear un trabajo de configuración y ejecutarlo en las instancias específicas de Citrix ADC. Cuando ejecuta el trabajo de configuración, las instancias vuelven a la configuración deseada. Para obtener más información sobre cómo crear un trabajo de configuración a partir de comandos correctivos, consulte Cómo crear trabajos de configuración a partir de comandos correctivos en NetScaler ADM.

Para ejecutar plantillas de auditoría de configuración al recibir la captura SNMP de ConfigChange:

NetScaler ADM le permite habilitar la opción de ejecutar la plantilla de auditoría de configuración en NetScaler ADM.

1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .
2. Haga clic **en ****Configuración en la página Auditoría** de configuración .
3. Haga clic en el icono de edición en la sección **Ajustes de auditoría de cambios de configuración**.
4. Seleccione la casilla **Realizar una auditoría de configuración cuando se reciba el evento netScalerConfigChange**.

> **Nota:**
>
> Se trata de una configuración global para todas las instancias. NetScaler ADM realiza una auditoría de configuración para cada instancia en la que reciba las capturas SNMP de NetScalerConfigChange en el futuro.

1. En el campo **Tiempo de espera para ejecutar la plantilla de auditoría** (en minutos), escriba los minutos. NetScaler ADM ejecuta la plantilla de auditoría de configuración en la instancia de

NetScaler ADC después de este retraso de tiempo cuando recibe la captura de ConfigChange SNMP por esa instancia.

Funciones de red

January 30, 2024

Con la función Funciones de red, puede supervisar el estado de las entidades configuradas en sus instancias administradas de Citrix Application Delivery Controller (ADC). Puede ver estadísticas como detalles de transacciones, detalles de conexión y rendimiento de un servidor virtual de equilibrio de carga. También puede habilitar o inhabilitar las entidades cuando planifique un mantenimiento.

El panel de funciones de red le proporciona los siguientes gráficos:

- Los 5 mejores servidores virtuales con mayor cantidad de conexiones de clientes
- Los 5 mejores servidores virtuales con el mayor número de conexiones
- Los 5 mejores servidores virtuales con un rendimiento máximo (MB/seg)
- Los 5 servidores virtuales más bajos con el rendimiento más bajo (MB/seg)
- Las 5 mejores instancias con la mayoría de los servidores virtuales
- Estado de los servidores virtuales
- Estado de los servidores virtuales de equilibrio de carga
- Protocolos

Generar informes para entidades de equilibrio de carga

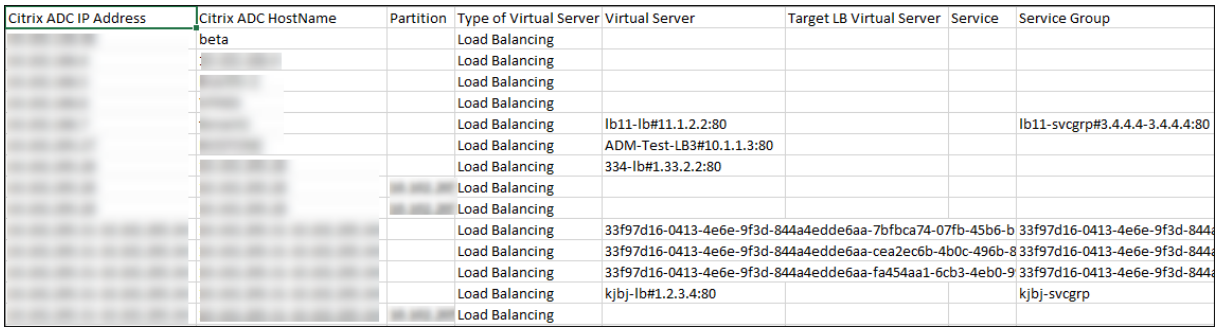
January 30, 2024

Citrix Application Delivery Management (ADM) le permite ver los informes de las entidades de instancia de Citrix Application Delivery Controller (ADC) en todos los niveles. Hay dos tipos de informes que puede descargar en Citrix ADM > Network Functions : informes consolidados e informes individuales.

Informes consolidados: puede descargar y ver un informe consolidado o resumido de todas las entidades que se administran en instancias de Citrix ADC.

Este informe le permite tener una vista de alto nivel de la asignación entre las instancias, particiones y las entidades de equilibrio de carga correspondientes (servidores virtuales, grupos de servicios y servicios) de Citrix ADC que están presentes en la red.

La siguiente imagen muestra un ejemplo de un informe resumido.



Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

El informe consolidado está en formato CSV. Las entradas de cada columna se describen de la siguiente manera:

- Dirección IP de**NetScaler: la dirección IP**de la instancia de Citrix ADC se muestra en el informe
- **Nombre de host de NetScaler**: el nombre del host se muestra en el informe.
- **Partición**: se muestra la dirección IP de la partición administrativa
- **Servidor virtual**: <name_of_the_virtual_server>#virtual_IP_address :port_number
- **Servicios**: <name_of_the_service>#service -IP_Address:port_number
- **Grupos de servicio**: <name_of_service_group>#server_member1_IP_address:port,server_member2_IP_a
  ……..,server_membern_IP_address:port

> **Nota**
>
> - Si no hay ningún nombre de host disponible, se muestra la dirección IP correspondiente.
> - Las columnas en blanco indican que las entidades respectivas no están configuradas para esa instancia de Citrix ADC.

Informes individuales: también puede descargar y ver informes independientes de todas las instancias y entidades. Por ejemplo, puede descargar un informe solo para servidores virtuales o servicios de equilibrio de carga o grupos de servicios de equilibrio de carga.

Citrix ADM le permite descargar el informe al instante. También puede programar el informe para que se genere a una hora fija una vez al día, una vez a la semana o una vez al mes.

Generar un informe de equilibrio de carga combinado

1. En Citrix ADM, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga**.

2. En la página **Equilibrio de carga**, haga clic en  .
3. En la página **Exportar** que se abre, tiene dos opciones para ver el informe:
   a) Seleccione la ficha **Exportar ahora** y haga clic en **Aceptar**.

      El informe consolidado se descarga en su sistema.

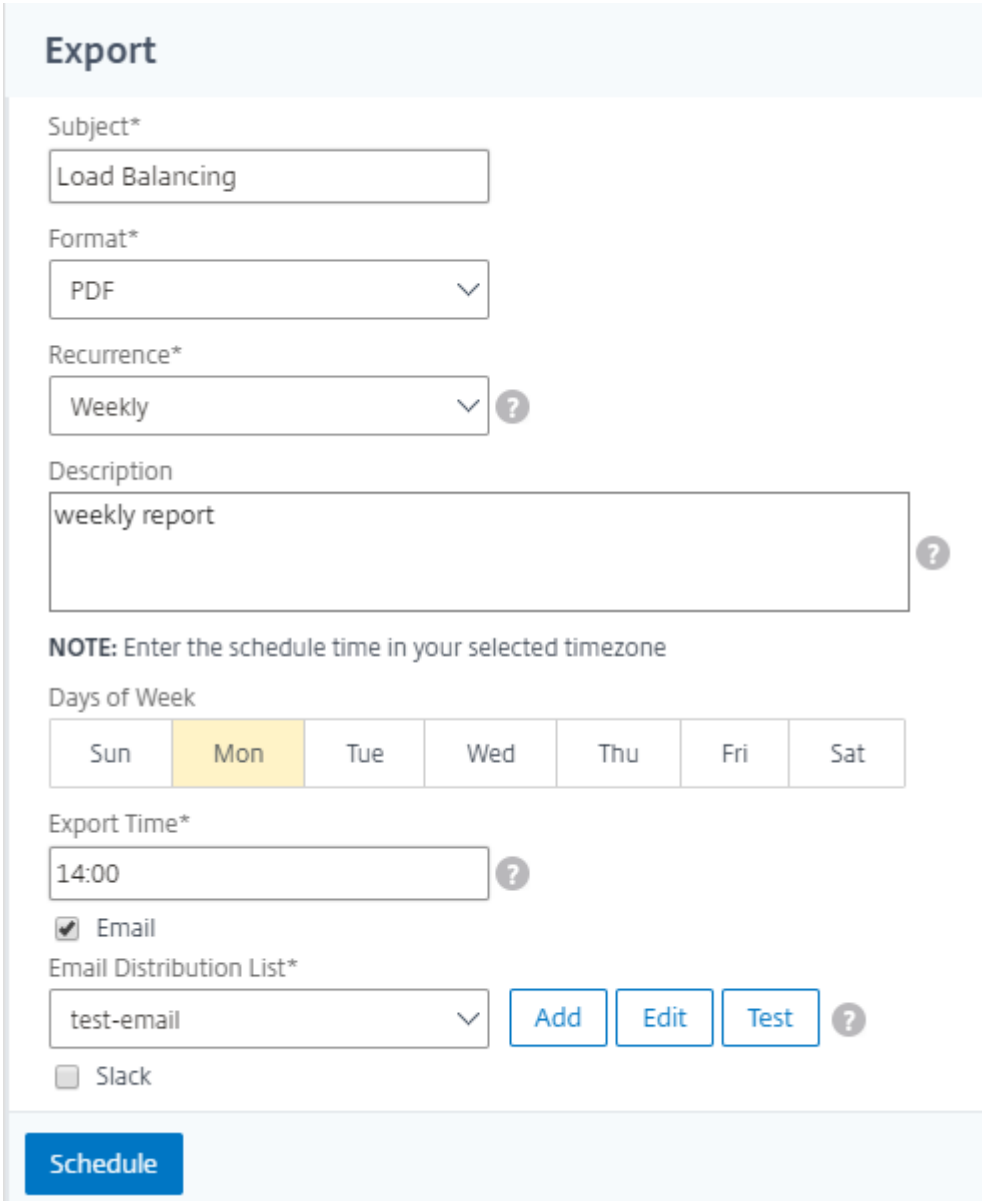
   b) Seleccione la pestaña **Programar informe** para programar la generación y exportación del informe a intervalos regulares. Especifique la configuración de recurrencia de generación de informes y cree un perfil de correo electrónico al que se exporta el informe.

      i. **Periodicidad**: seleccione**Diariamente**,**Semanalmente**o**Mensualmente**en el cuadro de lista desplegable.

      ii. **Tiempo de recurrencia**: Introduzca la hora como Hora:Minuto en formato de 24 horas.

      iii. **Perfil de correo electrónico**: selecciona un perfil del cuadro de lista desplegable o haga clic en**+**para crear un perfil de correo electrónico.

> **Nota**
>
> Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.



Nota

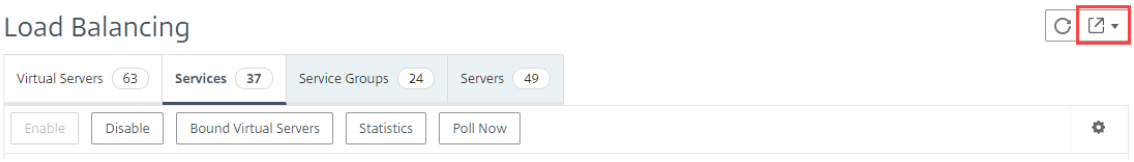
Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

Generar un informe de entidad de equilibrio de carga individual

Puede generar y exportar un informe individual para un tipo concreto de entidad asociada a las instancias. Por ejemplo, considere un caso en el que quiera ver una lista de todos los servicios de equilibrio de carga de la red.

1. En Citrix ADM, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga > Servicios.**

2. En la página **Servicios**, haga clic en el botón **Exportar** en la esquina superior derecha.



   a) Seleccione la ficha **Exportar ahora** si quiere generar y ver el informe en este instante.

   b) Seleccione **Programar exportación** para programar la generación y exportación del informe a intervalos regulares.

> **Nota**
>
> Solo puede descargar los informes o exportarlos como archivos adjuntos de correo. No puede ver los informes en la GUI de Citrix ADM.

Exportar o programar la exportación de informes de funciones de red

January 30, 2024

Puede generar un informe completo para determinadas funciones de red, como Equilibrio de carga, Content Switching, Redirection de caché, Global Server Load Balancing (GSLB), Autenticación y Citrix Gateway en Citrix Application Delivery Management (ADM). Este informe le permite tener una vista de alto nivel de la asignación entre las instancias, particiones de Citrix ADC y las entidades enlazadas correspondientes (servidores virtuales, grupos de servicios y servicios) que están presentes en la red. Puede exportar estos informes en formato de archivo CSV.

El informe muestra los siguientes datos del servidor virtual:

- Dirección IP de NetScaler
- Nombre de host
- Datos de partición
- Nombre del servidor virtual
- Tipo de servidor virtual
- Servidor virtual
- Servidor virtual LB de destino

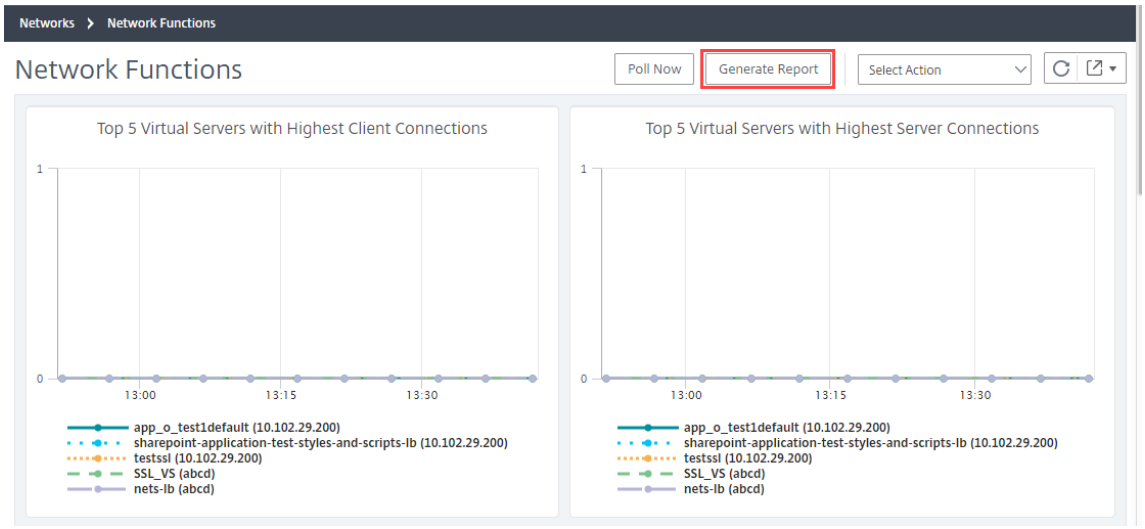
> **Nota**
>
> Para los servidores virtuales de conmutación de contenido y redirección de caché, la columna Servidor virtual de Target LB muestra todos los servidores LB, es decir, los servidores predeterminados y los servidores basados en directivas.
>
> - Nombre del servicio
> - Nombre del grupo de servicios

Puede programar la exportación de estos informes a direcciones de correo electrónico especificadas en diferentes intervalos.

> **Nota**
>
> - Para los servidores virtuales GSLB, el informe de funciones de red muestra solo los servidores virtuales GSLB y los servicios asociados.
> - Para los servidores virtuales de conmutación de contenido y redirección de caché, el informe muestra solo los enlaces a los servidores LB asociados.
> - Los servidores virtuales SSL no aparecen en este informe porque Citrix ADM no mantiene una lista independiente de servidores virtuales SSL.
> - Cuando se genera un nuevo informe, los informes antiguos se depuran automáticamente de su cuenta.
> - No puede generar un informe de funciones de red para HAProxy.

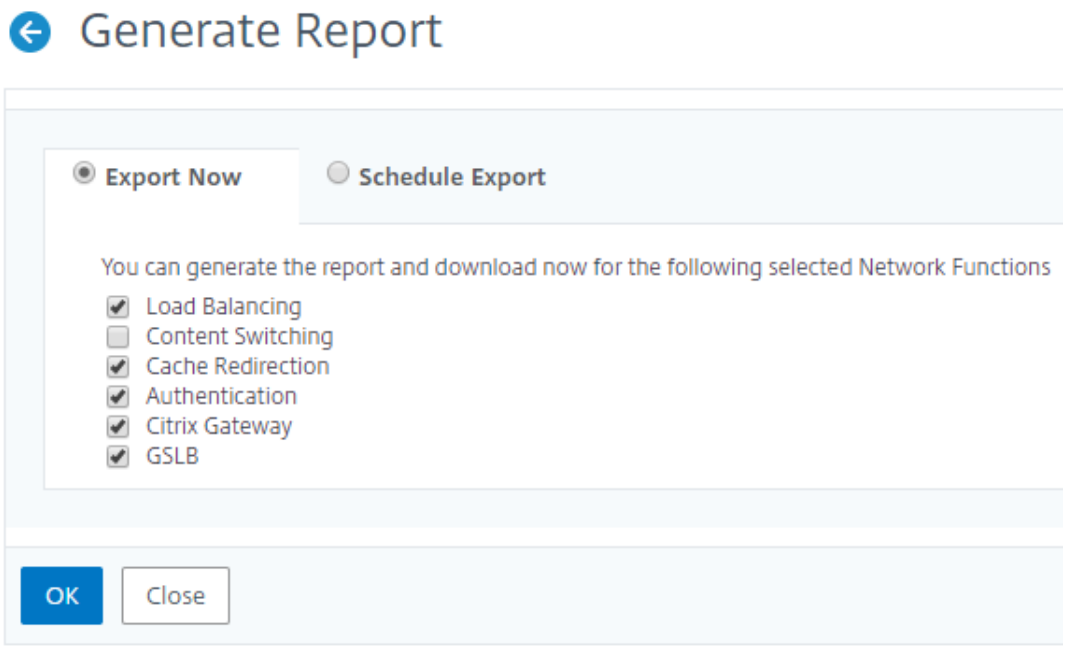
Para exportar y programar informes de funciones de red:

1. Vaya a**Redes > Funciones de red**.
2. En la página**Funciones de red**, en el panel derecho, haga clic en**Generar informe**en la esquina superior derecha de la página.



3. En la página **Generar informe**, tiene las dos opciones siguientes:

   a) Seleccione la ficha **Exportar ahora** y haga clic en **Aceptar**. El informe se descarga en su sistema.



   La imagen siguiente muestra un ejemplo de un informe de funciones de red.

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.10	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

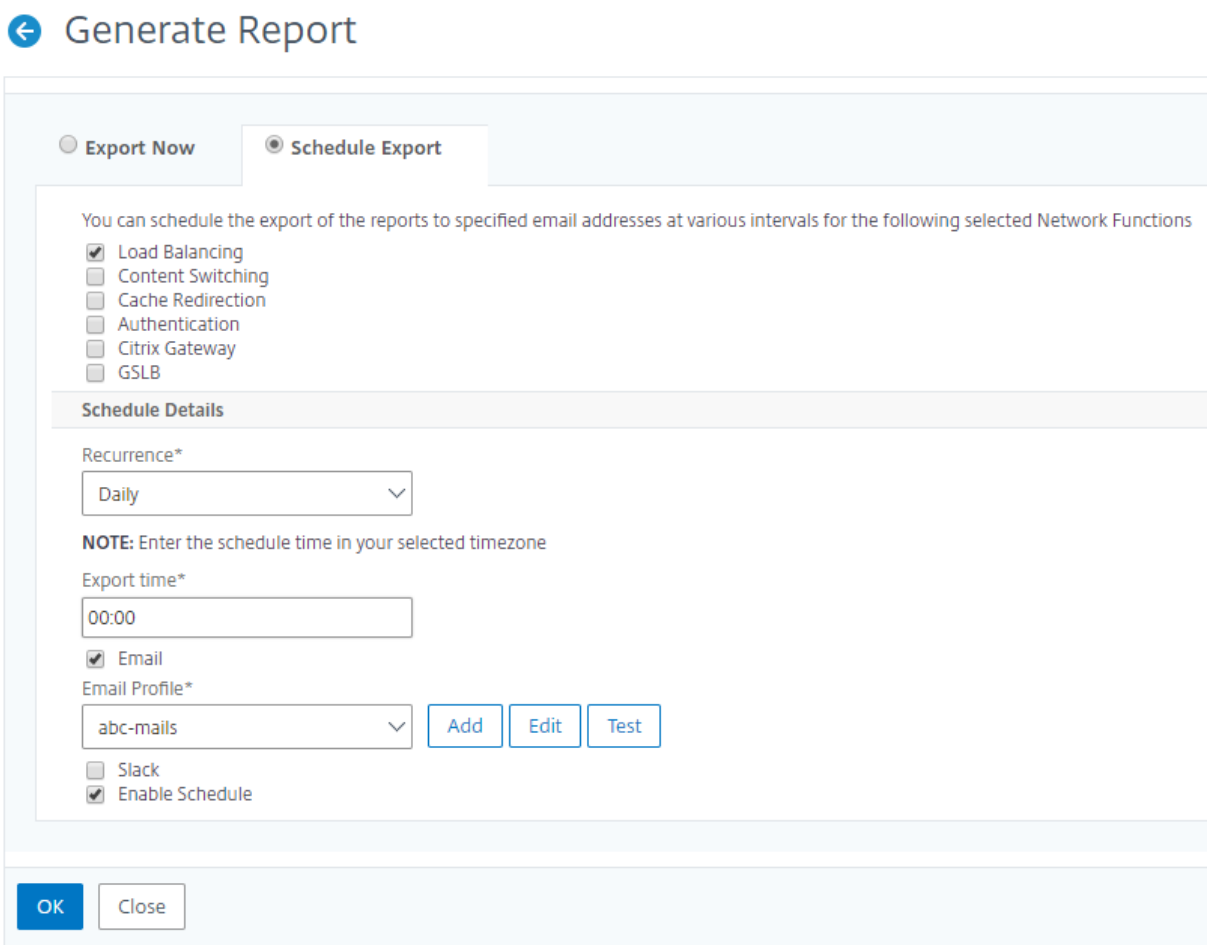
   b) Seleccione la ficha**Informe**de programación para programar la generación y exportación del informe a intervalos regulares. Especifique la configuración de recurrencia de generación de informes y cree un perfil de correo electrónico al que se exporta el informe.

      i. **Periodicidad**: seleccione**Diariamente**,**Semanalmente**o**Mensualmente**en el cuadro de lista desplegable.

      ii. **Tiempo de recurrencia**: introduzca la hora como Hora: Minuto en formato de 24 horas.

      iii. **Perfil de correo electrónico**: selecciona un perfil del cuadro de lista desplegable o haga clic en**+**para crear un perfil de correo electrónico.

Haga clic en **Habilitar programación** para programar el informe y, a continuación, haga clic en **Aceptar**. Al hacer clic en la casilla de verificación **Habilitar programación**, puede generar los informes seleccionados.



Informes de red

January 30, 2024

Puede optimizar el uso de los recursos supervisando los informes de red en Citrix Application Delivery Management (ADM). Es posible que tenga una implementación distribuida con muchas aplicaciones implementadas en varias ubicaciones. Para garantizar un rendimiento óptimo de las aplicaciones, también ha implementado varias instancias de Citrix Application Delivery Controller (ADC) para equilibrar la carga, cambiar el contenido o comprimir el tráfico. El rendimiento de la red puede afectar al rendimiento de la aplicación. Para seguir manteniendo el rendimiento de sus aplicaciones, debe supervisar periódicamente el rendimiento de la red y asegurarse de que todos los recursos se utilizan de forma óptima.

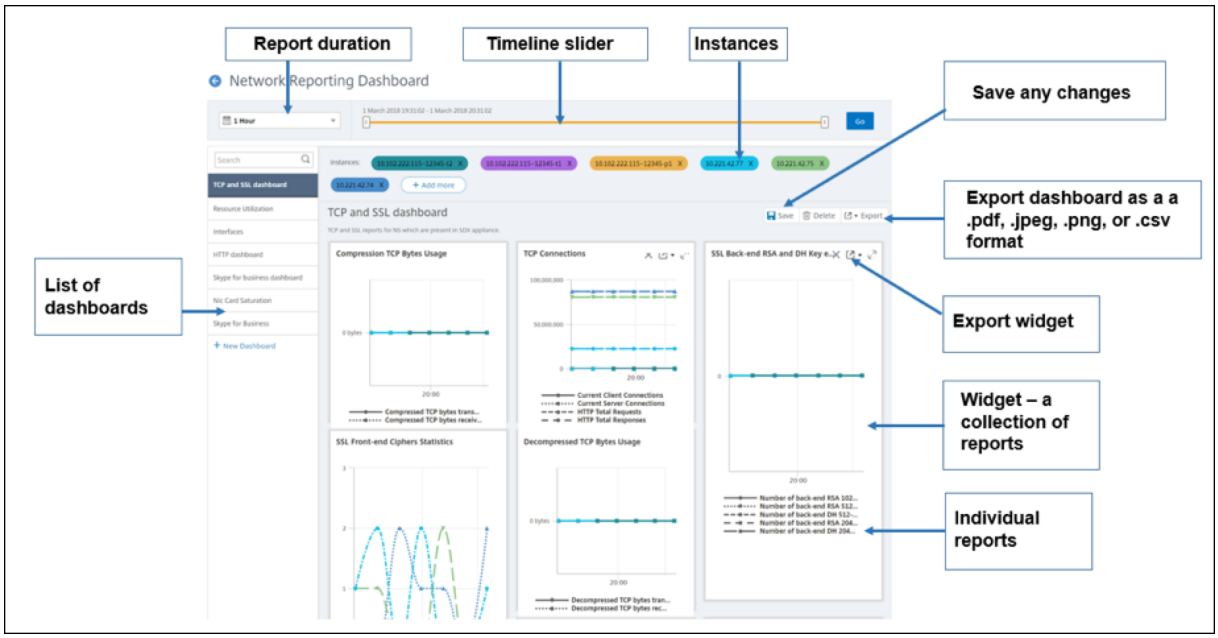
NetScaler ADM ahora le permite generar informes no solo para instancias a nivel global, sino también para entidades como los servidores virtuales y las interfaces de red. La familia de instancias comprende instancias de NetScaler ADC y SD-WAN. Los servidores virtuales para los que puede generar informes son los siguientes:

- Servidores de equilibrio de carga
- Servidores de conmutación de contenido
- Redirección de memoria caché
- Equilibrio de carga de servicio global (GSLB)
- Autenticación
- Citrix Gateway

El panel de informes de red de NetScaler ADM es altamente personalizable. Ahora puede crear varios paneles para varias instancias, servidores virtuales y otras entidades.

Panel de informes de red

La siguiente imagen muestra las distintas funciones del panel de control:



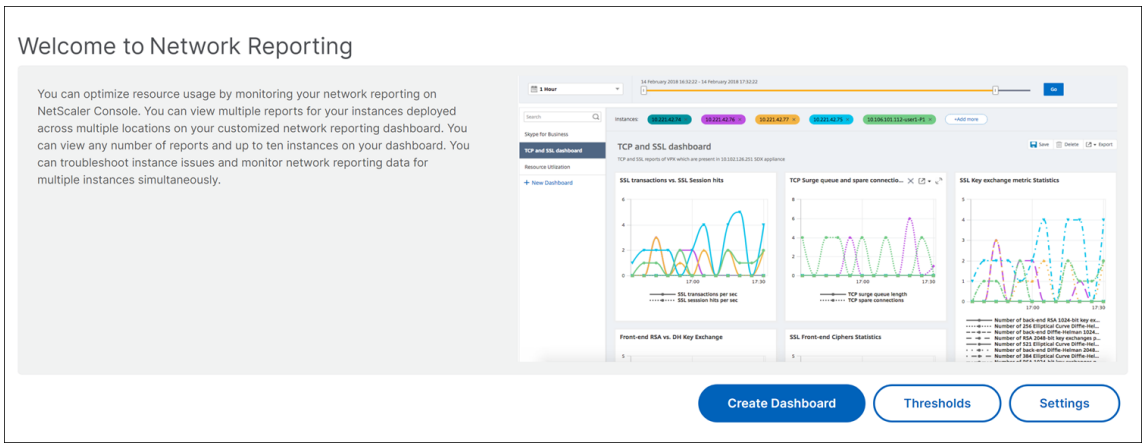
- El panel del lado izquierdo muestra todos los paneles personalizados creados en NetScaler ADM. Puede hacer clic en uno de ellos para ver los distintos informes que componen el panel de control. Por ejemplo, un panel TCP y SSL contiene varios informes relacionados con protocolos TCP y SSL.

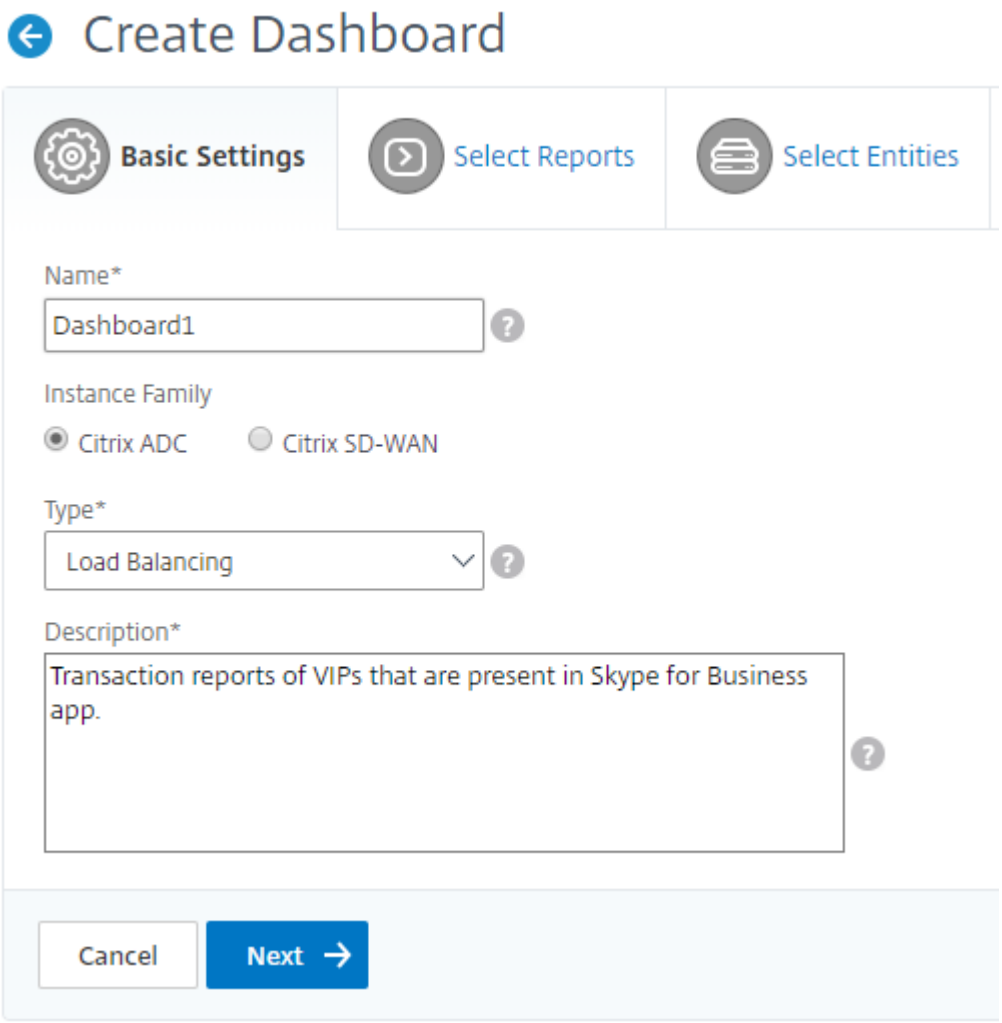
- Puede personalizar cada panel con varios widgets para mostrar una variedad de informes. Un widget representa un informe en el panel, es decir, una colección de informes más relacionados. Por ejemplo, un informe de uso de bytes TCP de compresión contiene informes de bytes TCP comprimidos transferidos y recibidos por segundo.
- Puede mostrar informes de una hora, un día, una semana o un mes. Además, ahora puede usar la opción de control deslizante de la línea de tiempo para personalizar la duración de los informes que se generan en NetScaler ADM.
- Para eliminar un informe, haga clic en la "X". También puede exportar el informe como formato.pdf,.jpeg,.png o.csv al sistema. También puede programar una hora y repetición de cuándo se debe generar el informe. También puede configurar una lista de distribución de correo electrónico a la que se deben enviar los informes.
- La sección Instancias en la parte superior del panel muestra las direcciones IP de todas las instancias para las que se genera el informe.
- Puede eliminar instancias haciendo clic en la "X"o agregar más instancias a los informes. Sin embargo, actualmente Citrix ADM permite ver los informes de diez instancias.
- También puede exportar todo el panel de control en formato.pdf,.jpeg, png o.csv a su sistema. Se deben guardar todos los cambios realizados en el panel de control. Haga clic en Guardar para guardar los cambios.

En la siguiente sección se explican en detalle las tareas para crear un panel, generar informes y exportar informes.

Para ver o crear un panel

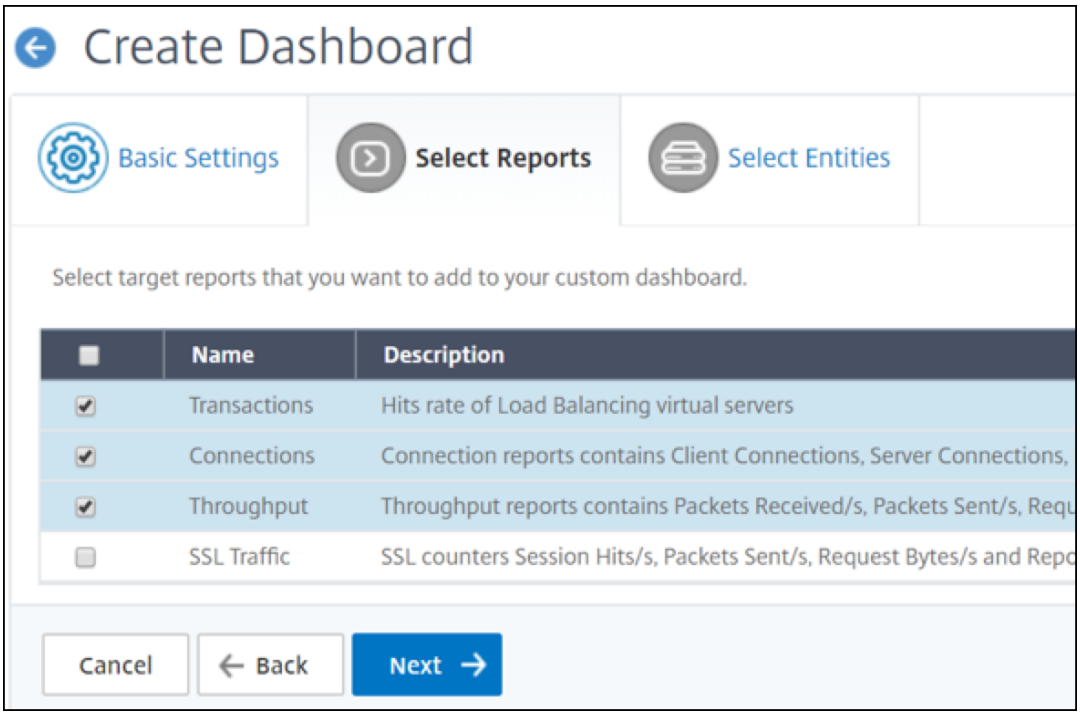
1. En NetScaler ADM, vaya a **Redes** > **Informes de red**.





2. En la ficha **Seleccionar informes**, seleccione los informes necesarios. En este ejemplo, puede seleccionar las transacciones, las conexiones y el rendimiento. Haga clic en **Siguiente**.
3. Para ver los paneles existentes, haga clic en **Ver panel**. Se abre la página **Panel** de informes de red, donde puede ver todos los paneles y widgets de informes.
4. Para crear un panel, haga clic en **Crear panel**.
5. Se abre la página **Crear panel**.
6. En la ficha **Configuración básica**, introduzca los siguientes detalles:
    a) **Nombre**. Escriba el nombre del panel de control.
    b) **Familia**de instancias . Seleccione el tipo de instancia: Citrix ADC o Citrix SD-WAN
    c) **Escriba**. Seleccione el tipo de entidad para el que quiere generar informes. En este ejemplo, seleccione servidores virtuales de equilibrio de carga.
    d) **Descripción**. Escriba una descripción significativa para el panel de control.

e) Haga clic en **Siguiente**.



7. En la ficha **Seleccionar entidades**, haga clic en **Agregar**.
8. En la ventana **Elegir servidores virtuales LB** que aparece, seleccione cualquier número de servidores virtuales que desee supervisar.

> **Nota**
>
> Según el tipo de entidad que haya seleccionado en la pestaña Configuración básica, la pestaña Entidades se rellena con las entidades correspondientes. Por ejemplo, si seleccionas global, puedes agregar instancias.

9. Haz clic en **Crear.**

Se crea el panel de **TCP y SSL** y muestra todos los informes que ha seleccionado.

> **Nota**
>
> Actualmente, los cambios que realice en leyendas o filtros no se pueden guardar.

Exportación de informes de red

Si bien puede exportar informes de widgets en los formatos.pdf, png,.jpeg o.csv, puede exportar todos los paneles solo en los formatos.pdf,.jpeg o png.

> **Nota**
>
> No puede exportar informes en NetScaler ADM si tiene permisos de solo lectura. Necesita un permiso de edición para poder crear un archivo en NetScaler ADM y poder exportarlo.

Para exportar informes de paneles:

1. Vaya a **Redes** > **Informes de red**
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, haga clic en **Panel 1**.
4. Haga clic en el botón de exportación situado en la esquina superior derecha de la página.
5. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.

Al programar informes de red, puede personalizar el encabezado del informe escribiendo una cadena de texto en el campo Asunto. El informe creado a la hora programada tendrá esta cadena como nombre.

Por ejemplo, para los informes de red que se originan en un servidor virtual concreto, puede escribir el asunto "authentication-reports-10.106.118.120", donde 10.106.118.120 es la dirección IP del servidor virtual supervisado.

> **Nota:**
>
> Actualmente, esta opción solo está disponible cuando se programa la exportación de informes. No puede agregar un encabezado al informe cuando los exporta al instante.

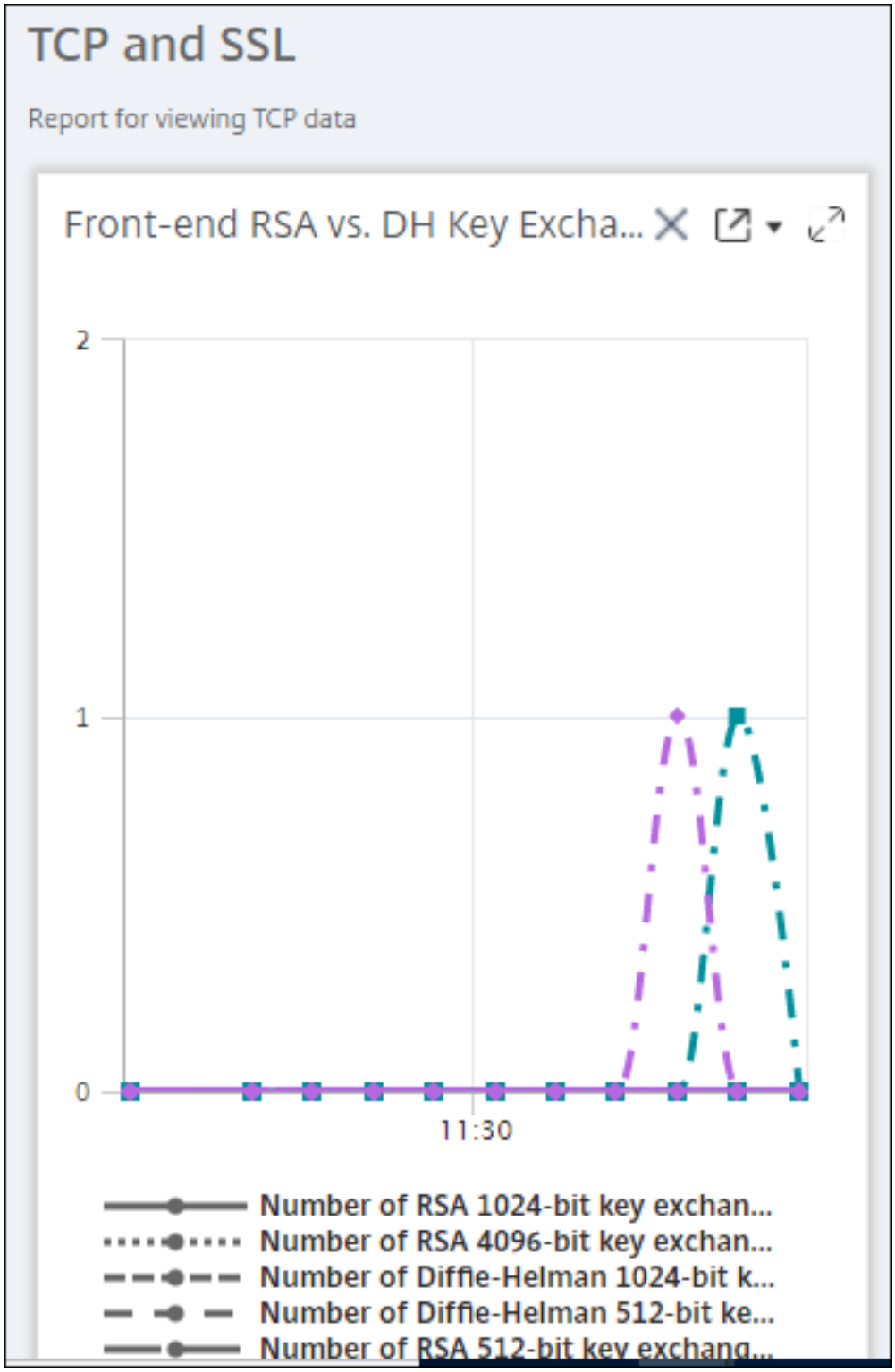
Para exportar informes de paneles:

1. Vaya a **Redes** > **Informes de red**
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, haga clic en **Panel 1**.

4. Haga clic en el botón de exportación situado en la esquina superior derecha de la página.
5. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.**

Para exportar informes de widgets:

1. Vaya a **Redes** > **Informes de red.**
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, haga clic también en **TCP y SSL** .
4. Seleccione un widget. Por ejemplo, seleccione **Front-end RSA vs. Intercambio**de claves DH .
5. Haga clic en el botón de exportación en la esquina superior derecha de la página
6. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.



Cómo administrar Umbrales para Informes de Red en NetScaler ADM

Para supervisar el estado de una instancia de NetScaler ADC, puede establecer umbrales en los contadores y recibir notificaciones cuando se supera un umbral. En NetScaler ADM, puede configurar los umbrales y verlos, modificarlos y eliminarlos.

Por ejemplo, puede recibir una notificación por correo electrónico cuando el contador de conexiones de un servidor virtual de conmutación de contenido alcance un valor especificado. Puede definir un umbral para un tipo de instancia específico. También puede elegir los informes que quiere generar para métricas específicas de contador de la instancia elegida.

Cuando el valor de un contador supera o cae por debajo (según lo especificado por la regla) del valor umbral, se genera un evento de la gravedad especificada para indicar un problema relacionado con el rendimiento. Cuando el valor del contador vuelve a un valor que considera normal, el evento se borra. Estos eventos se pueden ver navegando a **Redes** > **Eventos** > **Informes** . En la página Informes, puede hacer clic en el anillo **Eventos por gravedad** para ver los eventos según su gravedad.

También puede asociar una acción a un umbral, como enviar un mensaje de correo electrónico o SMS cuando se incumple el umbral.

Para crear un umbral

1. En Citrix ADM, vaya a **Redes** > **Informes de red** > **Umbrales** . En **Umbrales**, haga clic en **Agregar**.
    1. En la página **Crear umbral** , especifique los siguientes detalles:
        - **Nombre**del umbral . Nombre del umbral.
        - **Tipo de instancia**. Elija Citrix ADC o Citrix SD-WAN WO.
        - **Nombre del informe**. Nombre del informe de rendimiento que proporciona información sobre este umbral.
    2. También puede establecer reglas para especificar cuándo se va a generar o borrar un evento. Puede especificar los siguientes detalles en la sección **Configurar regla** :
        - **Métrico**. Seleccione la métrica para la que quiere establecer un umbral.
        - **Comparador**. Seleccione un comparador para comprobar si el valor monitorizado es mayor o igual o menor que el valor umbral.
        - **Valor de umbral**. Escriba el valor para el que se calcula la gravedad del evento. Por ejemplo, puede que quiera generar un evento con una gravedad de evento crítica si el valor supervisado para las conexiones de clientes actuales alcanza el 80 por ciento. En este caso, escriba 80 como valor de umbral. Para ver los eventos de «gravedad crítica», vaya a **Redes**

> **Eventos** > **Informes** . En la página Informes, puede hacer clic en el anillo **Eventos por gravedad** para ver los eventos según su gravedad.

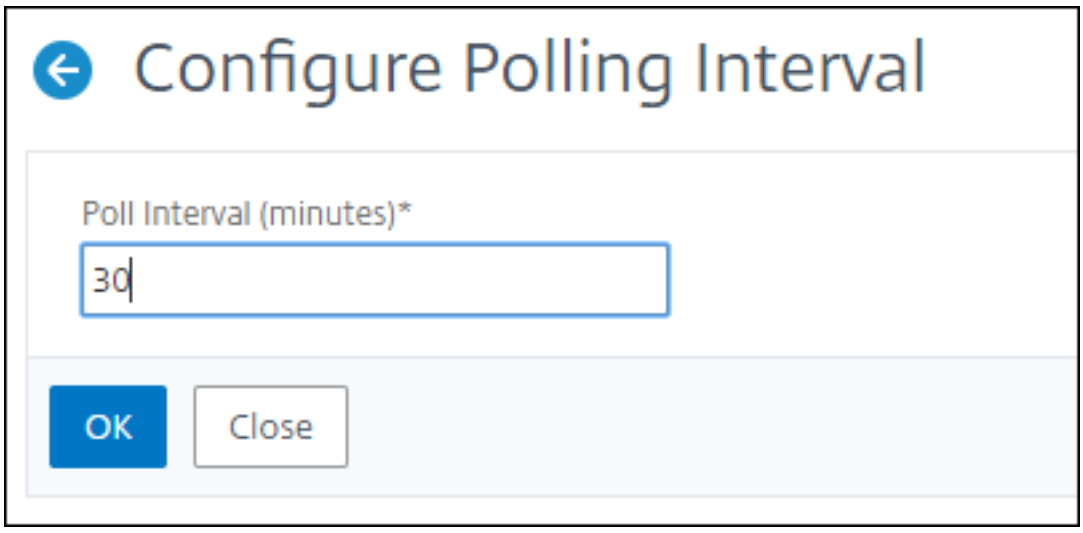
- **Valor claro**. Escriba el valor que indica cuándo borrar el valor. Por ejemplo, puede que quiera borrar el umbral de conexiones de clientes actuales cuando el valor supervisado alcance el 50 por ciento. En este caso, escriba 50 como valor de borrado.
- **Gravedad del evento** Seleccione el nivel de seguridad que quiera establecer para el valor del umbral.

3. Elija la dirección IP de la instancia o instancias para las que quiere establecer el umbral.
4. También puedes añadir un **mensaje de evento** . Escriba el mensaje que quiera que aparezca cuando se alcance el umbral. NetScaler ADM agrega el valor supervisado y el valor umbral a este mensaje.
5. Seleccione**Activar**para habilitar el umbral para generar alarmas.
6. Si lo desea, puede configurar **acciones** como las notificaciones por correo electrónico o SMS.
7. Haga clic en **Crear**.

Establecer el intervalo de sondeo de rendimiento para los informes

De forma predeterminada, cada 5 minutos, las llamadas NITRO recopilan datos de rendimiento para la generación de informes de red. Esto recupera las estadísticas de la instancia, como la información de los contadores, y las agrega por minuto, por hora, por día o por semana. Puede ver estos datos agregados en informes predefinidos.

Para establecer el intervalo de sondeo de rendimiento, vaya a **Redes** > **Informes de red** y haga clic en **Configurar intervalo de sondeo** . El intervalo de sondeo no puede ser inferior a 5 minutos ni superior a 60 minutos.



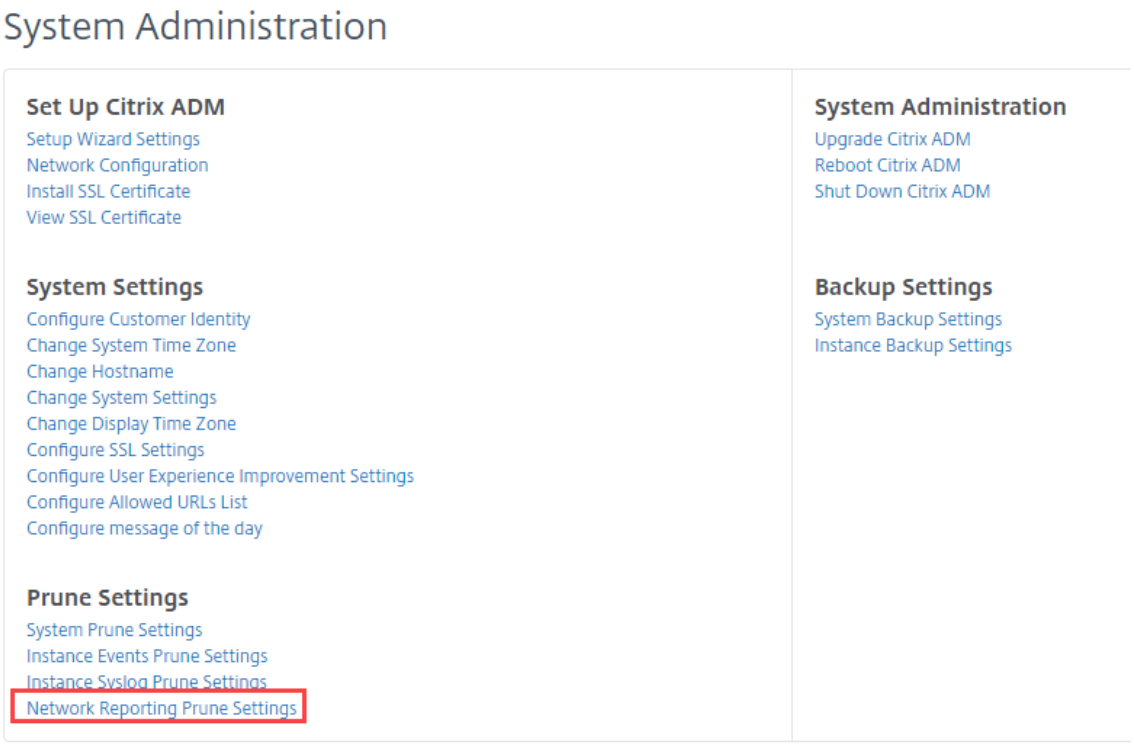
Configuración de la Prune de Network Reporting

Puede configurar el intervalo de depuración de los datos de informes de red en NetScaler ADM. Esto limita la cantidad de datos de informes de red que se almacenan en la base de datos del servidor Citrix ADM. De forma predeterminada, la poda ocurre cada 24 horas (a las 01.00 horas) para la red que informa de datos históricos.

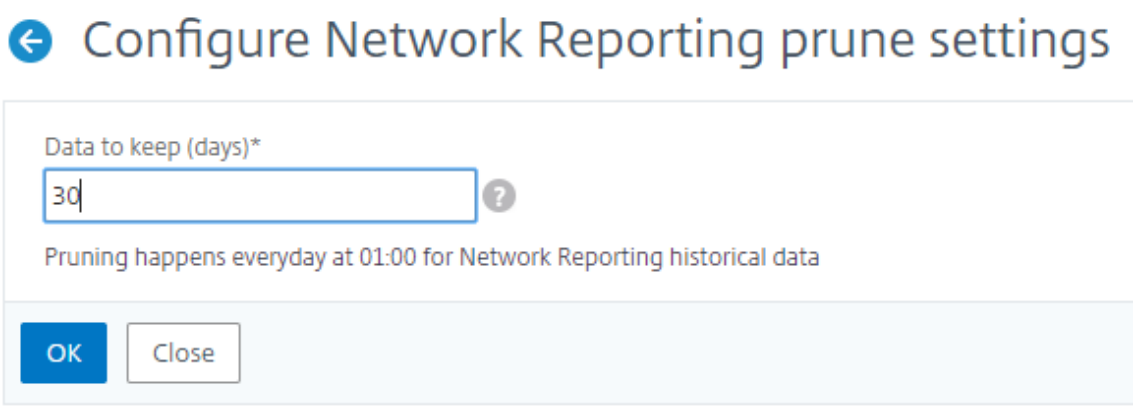
> **Nota** El valor que puede especificar no puede superar los 90 días ni ser inferior a 1 día.

Para configurar los ajustes de poda de informes de red:

1. Vaya a **Sistema > Administración del sistema**. En **Configuración de poda**, haga clic en **Configuración de poda de Network Reporting** .



2. En la página **Configurar los ajustes de recorte de informes de red** , especifique el número de días durante los que desea conservar los datos **y** haga clic en Aceptar .



Todos los datos de rendimiento de los informes de red se conservan en la base de datos Citrix ADM durante el número de días seleccionado.

Análisis

January 30, 2024

La función Citrix ADM Analytics proporciona una forma fácil y escalable de analizar varios datos de Citrix ADC para analizar y mejorar el rendimiento de las aplicaciones. Puede utilizar una o varias funciones de análisis simultáneamente en NetScaler ADM.

En la siguiente tabla se describen varias funciones de análisis compatibles con Citrix ADM:

Función de análisis	Descripción
Información web	Web Insight permite la visibilidad de las aplicaciones web empresariales y permite supervisar todas las aplicaciones web en Citrix ADC. Como administrador, puede ver la supervisión integrada y en tiempo real de las aplicaciones.
HDX Insight	HDX Insight proporciona visibilidad de extremo a extremo para el tráfico ICA que pasa a través de NetScaler ADC. HDX Insight le permite ver las métricas de latencia de los clientes y de la red en tiempo real, los informes históricos y los datos de rendimiento de principio a fin y solucionar problemas de rendimiento.

Función de análisis	Descripción
Gateway Insight	Gateway Insight proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, en el momento de iniciar sesión en Citrix Gateway.
Security Insight	Security Insight proporciona una solución de panel único para ayudarle a evaluar el estado de seguridad de su aplicación y a tomar medidas correctivas para proteger sus aplicaciones.
Insight SSL	SSL Insight proporciona visibilidad de las transacciones web seguras (HTTPS) y le permite supervisar todas las aplicaciones web seguras de Citrix ADC. Como administrador, puede ver la supervisión integrada, en tiempo real e histórica, de las transacciones web seguras.
Información TCP	TCP Insight proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias (o algoritmos) de control de la congestión que se utilizan en las instancias de Citrix ADC para evitar la congestión de la red en la transmisión de datos.
Video Insight	La función Video Insight proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización de vídeo utilizadas por los dispositivos Citrix ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa.
WAN Insight	El análisis de WAN Insight permite a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre los dispositivos de optimización WAN del centro de datos y las sucursales. WAN Insight también proporciona visibilidad en clientes, aplicaciones y sucursales de la red, para ayudar a solucionar problemas de red de manera eficaz.

Requisitos de licencia

January 30, 2024

La siguiente tabla describe los requisitos de licencia de las instancias de NetScaler ADC para ver los distintos informes de análisis en NetScaler ADM:

Funciones de NetScaler ADM Analytics	Requisito de licencia de NetScaler ADC
Información web	El informe Web Insight sobre Citrix ADM es compatible con todas las ediciones de licencias de Citrix ADC (Standard/Enterprise/Platinum).
HDX Insight	El informe HDX Insight sobre Citrix ADM es compatible con cualquiera de las siguientes licencias de Citrix ADC: Enterprise Edition (para informes de menos de 1 hora) o Platinum Edition (para informes ilimitados). **Nota**: La edición de licencia estándar no es compatible.
Security Insight	El informe Security Insight sobre Citrix ADM es compatible con las licencias Platinum Edition o Enterprise Edition con App Firewall. **Nota**: La edición de licencia estándar y la licencia de Firewall de aplicaciones independientes no son compatibles.
Insight SSL	El informe SSL Insight sobre Citrix ADM es compatible con todas las ediciones de licencias de Citrix ADC (Standard/Enterprise/Platinum).
Gateway Insight	El informe Gateway Insight sobre Citrix ADM es compatible con cualquiera de las siguientes licencias de Citrix ADC: Enterprise Edition (para informes de menos de 1 hora) o Platinum Edition (para informes ilimitados). **Nota**: La edición de licencia estándar no es compatible.
Información TCP	El informe TCP Insight es compatible con todas las ediciones de licencias de Citrix ADC (Standard/Enterprise/Platinum).
Video Insight	El informe Video Insight sobre NetScaler ADM es compatible con NetScaler ADC Premium (VPX-T 1000 series, VPX-T) edición.

Funciones de NetScaler ADM Analytics	Requisito de licencia de NetScaler ADC
WAN Insight	El informe WAN Insight sobre NetScaler ADM es compatible con Citrix SD-WAN WO Edition (WAN Optimization Edition).

Visión general de Logstream

January 30, 2024

Las instancias Citrix ADC generan registros de AppFlow y son un punto central de control para todo el tráfico de aplicaciones en el centro de datos. IPFIX y Logstream son los protocolos que transportan estos registros de AppFlow desde las instancias de Citrix ADC a Citrix ADM. Para obtener más información, consulte AppFlow.

- IPFIX es un estándar abierto del Grupo de Trabajo de Ingeniería de Internet (IETF) definido en el RFC 5101. IPFIX utiliza el protocolo UDP que es un protocolo de transporte poco confiable utilizado para el flujo de datos en una dirección. Dado que IPFIX utiliza el protocolo UDP, la adhesión al estándar IPFIX permite procesar más recursos en Citrix ADM.
- Logstream es un protocolo propiedad de Citrix que se utiliza como uno de los modos de transporte para transferir eficientemente los datos de registro de análisis de las instancias de Citrix ADC a Citrix ADM. Logstream utiliza un protocolo TCP confiable y requiere menos recursos para procesar los datos.

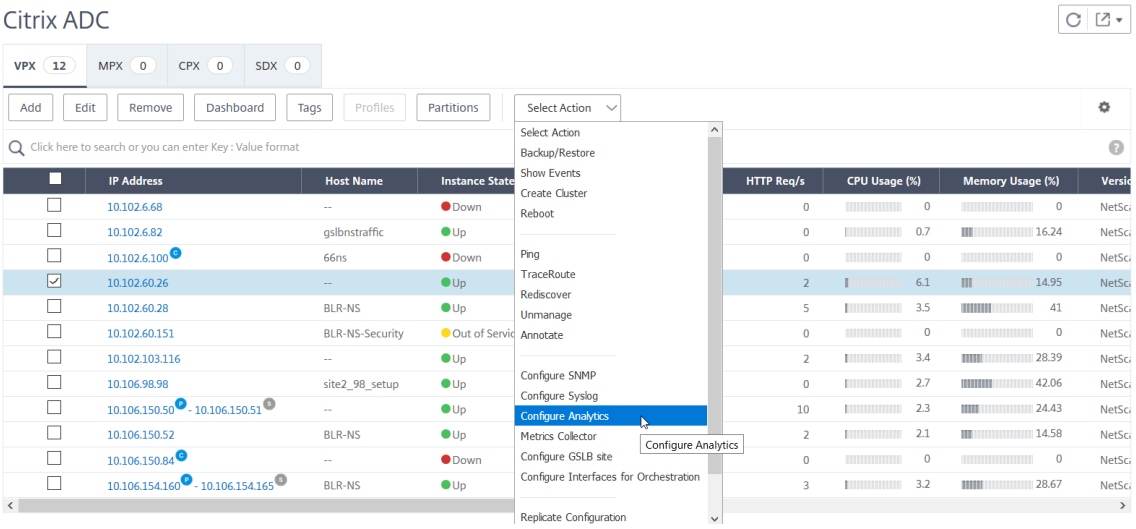
Para Citrix ADC entre **11.1 Build 47.14 y 11.1 Build 62.8** , Logstream es el modo de transporte predeterminado para habilitar Web Insight (HTTP) e IPFIX es el único modo de transporte para habilitar otros insights. Para la versión de Citrix ADC desde la **12.0 hasta la versión más reciente** , puede seleccionar Logstream o IPFIX como modo de transporte.

> **Nota**
>
> La versión y compilación de Citrix ADM deben ser iguales o superiores a las de la versión y compilación de Citrix ADC. Por ejemplo, si ha instalado Citrix ADC 12.1 Build 50.28/50.31 o una versión anterior, asegúrese de haber instalado Citrix ADM 12.1 Build 50.39.

Para utilizar Logstream como modo de comunicación y, al mismo tiempo, habilitar el análisis en Citrix ADM:

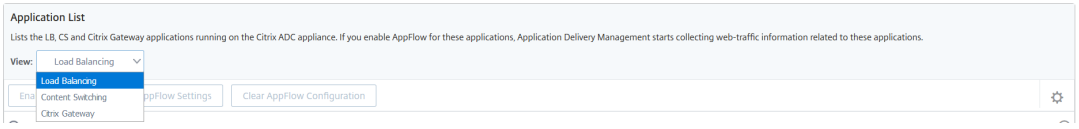
1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione la instancia de NetScaler ADC en la que quiere habilitar el análisis.

2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.

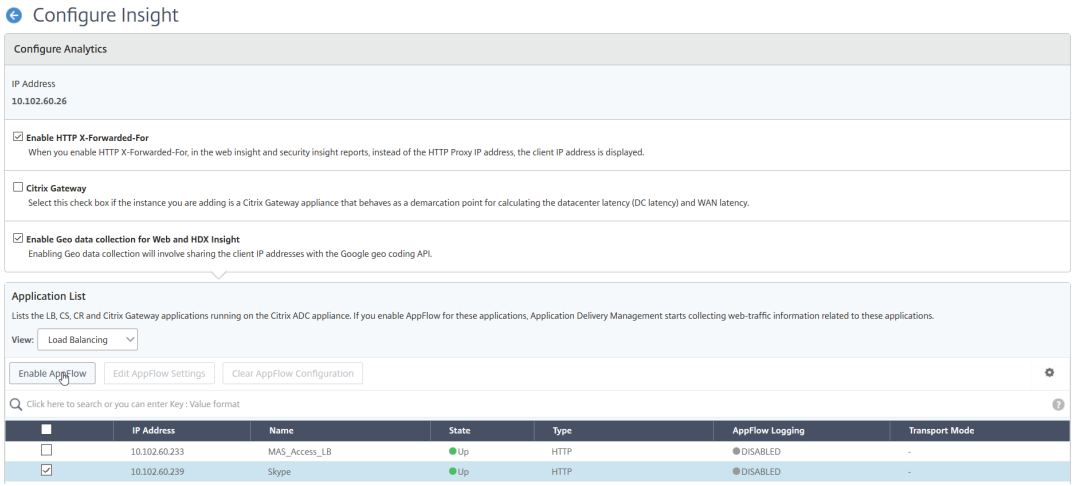


3. En la página **Configurar información** :

   a) Seleccione la **Lista de aplicaciones** para Equilibrio de carga o Content Switching.



   b) Seleccione el servidor virtual y haga clic en **Habilitar AppFlow**.

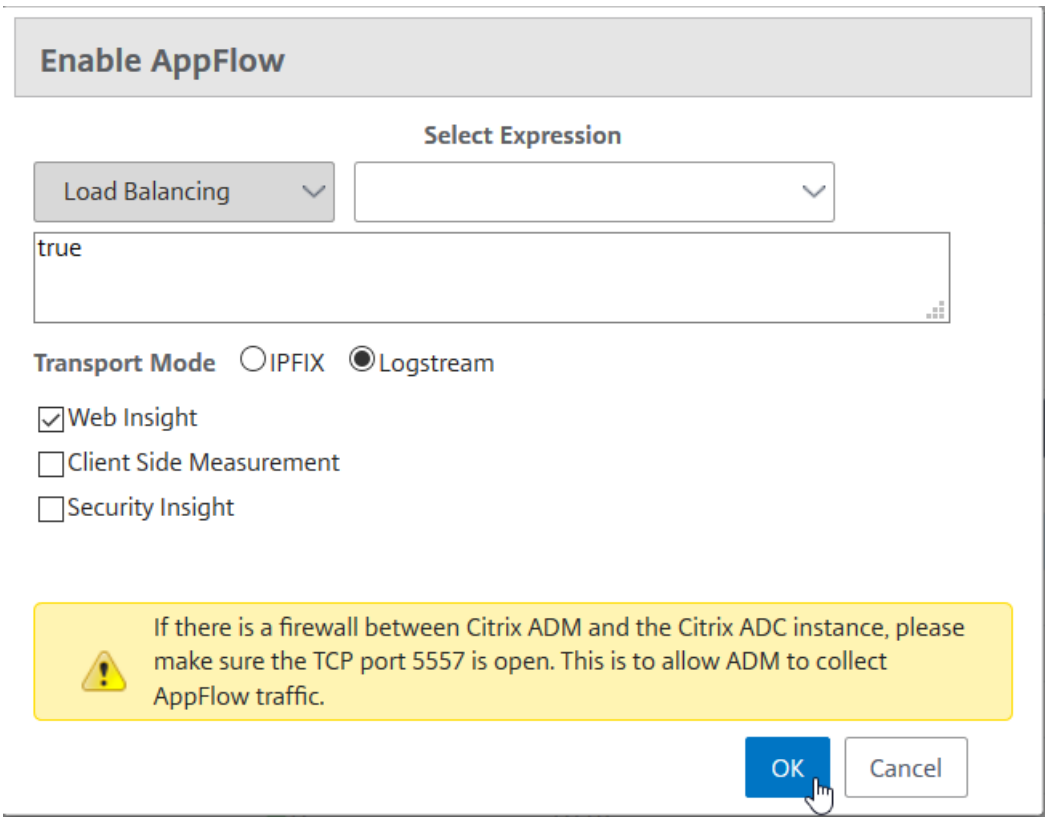


4. En el cuadro de diálogo Habilitar AppFlow:

   - Introduzca **true** en el cuadro de texto
   - Seleccione **Logstream** como modo de transporte

> **Nota**
>
> Citrix recomienda seleccionar Logstream como modo de transporte.

- Seleccione el tipo de conocimiento y haga clic **en**Aceptar .



En la siguiente tabla se describen las funciones de Citrix ADM que admiten Logstream como modo de transporte:

Función	IPFIX	Flujo de registro
Información web	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
Insight SSL	No compatible	•
CR Insight	•	•
Reputación IP	•	•
AppFirewall	•	•

Función	IPFIX	Flujo de registro
Medición del lado del	•	•
Syslog/Auditlog	•	•

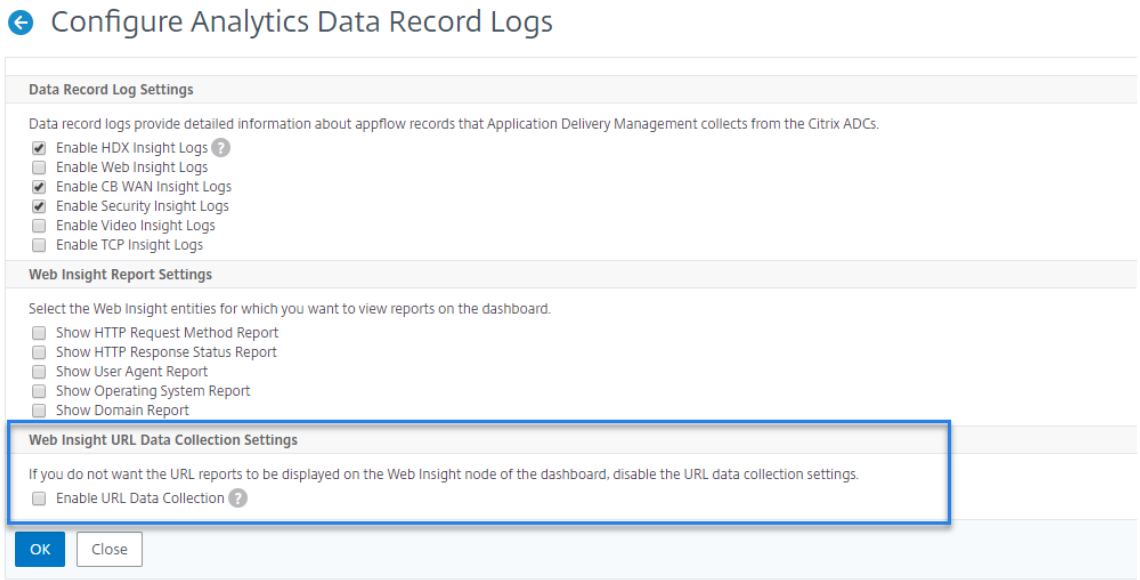
Inhabilitar la recopilación de datos de URL

January 30, 2024

Puede inhabilitar la recopilación de datos de URL si no quiere que los informes de URL se muestren en el nodo Web Insight del panel de control de Citrix Application Delivery Management (ADM).

Para inhabilitar la recopilación de datos de URL desde NetScaler ADM

1. En Citrix ADM, vaya a **Analytics** > **Parámetros** y, a continuación, haga clic en **Configurar registros de registros de datos** de análisis .
2. En la sección **Configuración de recopilación de datos de URL de Web Insight**, si la opción **Habilitar recopilación de datos de URL** está activada, desactive la casilla de verificación.
3. Haga clic en **Aceptar**.



Crear umbrales y alertas

January 30, 2024

Puede establecer umbrales y alertas para supervisar el estado de una instancia de Citrix ADC. Puede establecer umbrales en contadores y supervisar instancias y entidades en instancias administradas.

Cuando el valor de un contador supera el umbral, Citrix Application Delivery Management (ADM) genera un evento para indicar un problema relacionado con el rendimiento. Cuando el valor del contador coincide con el valor de borrado especificado en el umbral, el evento se borra, lo que significa que el umbral en particular ha vuelto a su estado normal.

También puede asociar una acción al umbral. Las acciones incluyen enviar una alerta, un correo electrónico o una notificación por SMS. Cuando se supera el umbral, Citrix ADM realiza automáticamente la acción que usted defina, como habilitar una alerta y enviar una notificación por correo electrónico o SMS.

Para crear un umbral y una alerta mediante NetScaler ADM

1. En NetScaler ADM, vaya a **Analytics** > **Configuración** > **Umbrales**. En **Umbrales**, haga clic en **Agregar**.
2. En la página **Crear umbrales**, especifique los siguientes detalles:
    - **Nombre**: Nombre para configurar el umbral.
    - **Tipo de tráfico**: Tipo de tráfico para el que desea configurar el umbral.
    - **Entidad**: Categoría o tipo de recurso para el que quiere configurar el umbral.
    - **Clave de referencia**: Valor generado automáticamente según el tipo de tráfico y la entidad seleccionados.
    - **Duración**: Intervalo para el que quiere configurar el umbral.
    - **Configurar regla**: Regla para la métrica para la que desea configurar el umbral.
    - **Configuración**de notificaciones : habilite el umbral y reciba notificaciones a través de varios canales, como correo electrónico, Slack o SMS, cuando se supere el umbral.
3. Haga clic en **Crear**.

Para HDX Insight, también puede establecer varios umbrales para los que se genere una alerta solo si se infringen todas las entidades del umbral configurado.

Configurar umbrales adaptativos

January 31, 2024

La funcionalidad de umbral adaptativo establece el valor umbral para el número máximo de visitas en cada URL. Si el número máximo de visitas a una URL es mayor que el valor umbral establecido para la URL, se envía un mensaje syslog a un servidor syslog externo. El intervalo del valor umbral puede ser de días o semanas.

El valor umbral se calcula de la siguiente manera:

Valor umbral = número máximo de aciertos * Multiplicador de umbral

Donde:

- El número máximo de visitas es el número máximo de visitas en una URL.
- El multiplicador de umbral es un valor entero que se define (predeterminado: 2).

Para crear un umbral adaptativo mediante Citrix ADM

1. En Citrix ADM, vaya a **Analytics** > **Configuración** > **Umbrales adaptativos** y, a continuación, haga clic en **Agregar**.
2. En la página **Umbrales adaptativos** , especifique los siguientes parámetros:
    - **Nombre: nombre** del umbral
    - **Entidad**: URL
    - **Duración**: Duración del umbral (día o semana)
    - **Multiplicador de umbrales**: Número entero definido por el usuario que se multiplica por el número máximo de visitas de la URL especificada para obtener el umbral adaptativo de la URL.

Configurar la persistencia de la base de datos

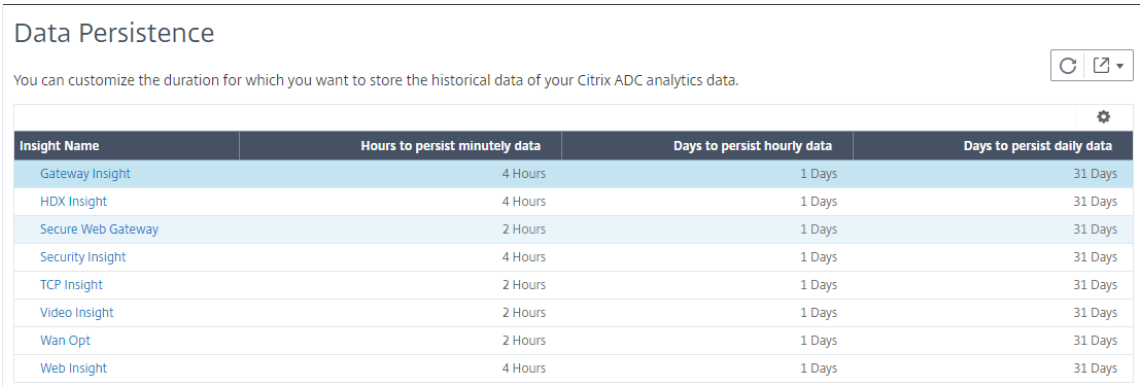
January 30, 2024

Configurar la persistencia de la base de datos en Citrix Application Delivery Management (ADM) le permite personalizar la duración durante la que desea almacenar los datos históricos de sus datos de análisis de Citrix ADC. Puede elegir los siguientes tipos de persistencia de bases de datos para los datos históricos de sus análisis:

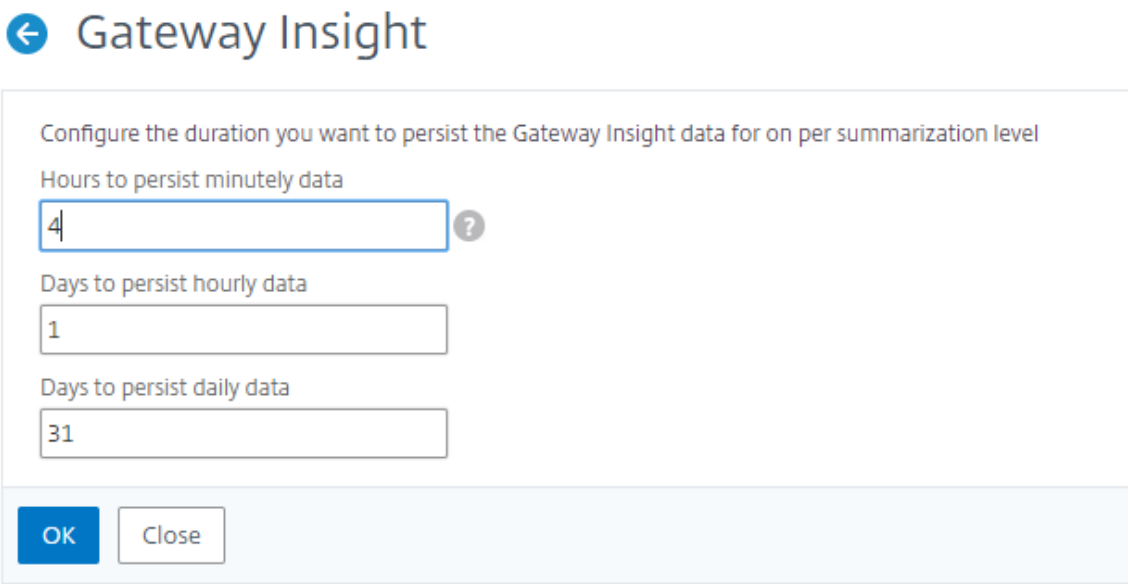
- Horas para conservar los datos minuciosamente
- Días para conservar los datos horarios
- Días para conservar los datos por día

Para configurar la persistencia de la base de datos

1. Vaya a > **Analytics** > **Configuración** > **Persistencia de base de datos**.
2. Haga clic en el tipo de Insight en el que desea configurar la persistencia de la base de datos.



3. Especifique el tiempo durante el que desea conservar los datos de Insight en Citrix ADM. Por ejemplo, para Gateway Insight, puede almacenar los datos históricos minuciosamente de los analíticos durante 2 horas, o los datos por hora durante 1 día.



Diagnósticos de autoservicio para Analytics

January 30, 2024

Citrix Application Delivery Management (ADM) realiza diagnósticos de autoservicio para identificar los problemas de licencia y configuración en las instancias administradas para las siguientes funciones de análisis:

- Información web
- HDX Insight
- Gateway Insight
- Security Insight
- Análisis de Secure Web Gateway

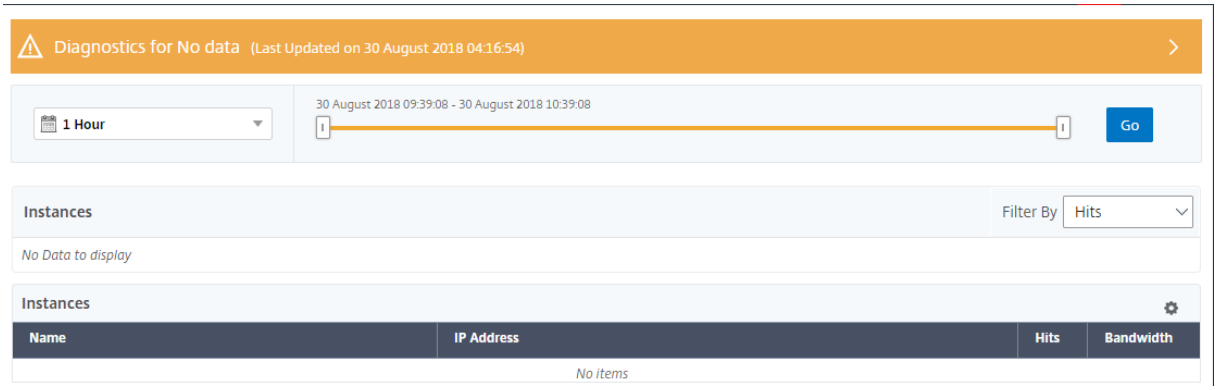
El diagnóstico de autoservicio se ejecuta cada 12 horas y genera un informe de diagnóstico si se encuentran problemas para cada una de las funciones de análisis especificadas. El informe de diagnóstico proporciona las fuentes de los problemas, los tipos de problemas y las acciones correctivas para resolverlos. El diagnóstico de autoservicio le ayuda a identificar y solucionar los problemas con mayor rapidez.

Por ejemplo, si la directiva de AppFlow no está vinculada a un servidor virtual o un servidor virtual no tiene licencia, NetScaler ADM no obtiene los datos deseados para la supervisión de Web Insight. El diagnóstico de autoservicio identifica los problemas y genera un informe de diagnóstico. Puede ver el informe de diagnóstico para comprobar los problemas y realizar las acciones correctivas.

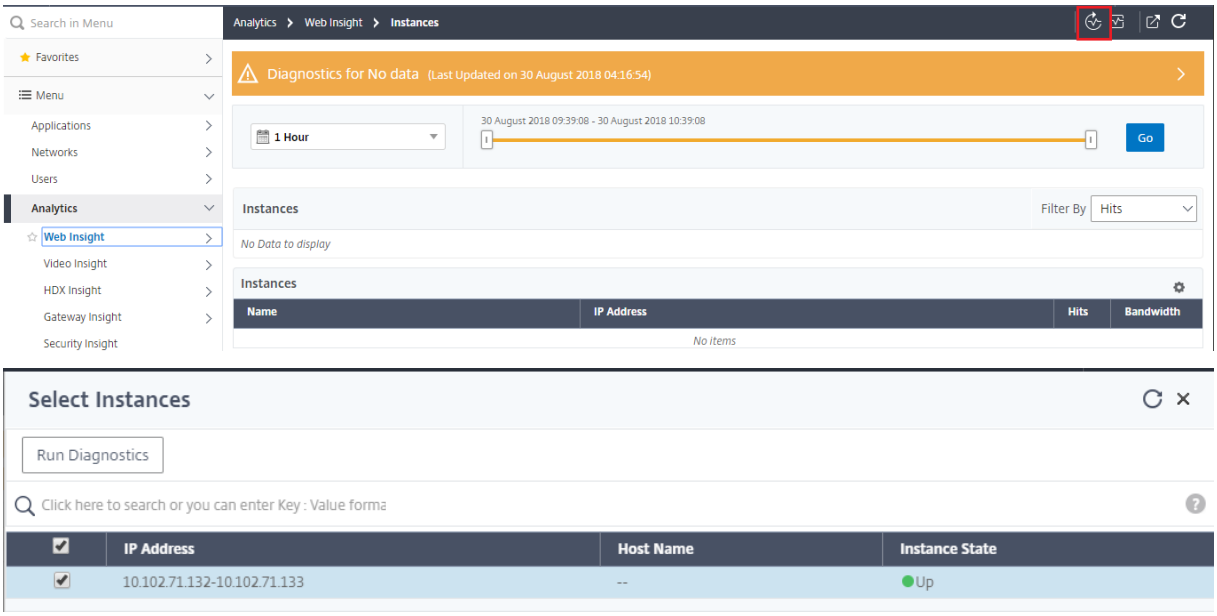
Ver el informe de diagnóstico

Para ver los informes de diagnóstico de las funciones de análisis especificadas, debe ir al nodo de análisis correspondiente en el panel de control de NetScaler ADM.

Por ejemplo, para ver el informe de diagnóstico de Web Insight, vaya a **Analytics > Web Insight**. En la página web Insight, seleccione el icono **Mostrar diagnósticos**.



También puede ejecutar un diagnóstico instantáneo si quiere comprobar si hay problemas. Haga clic en **Ejecutar diagnósticos**. Seleccione las instancias y seleccione **Ejecutar diagnósticos**.



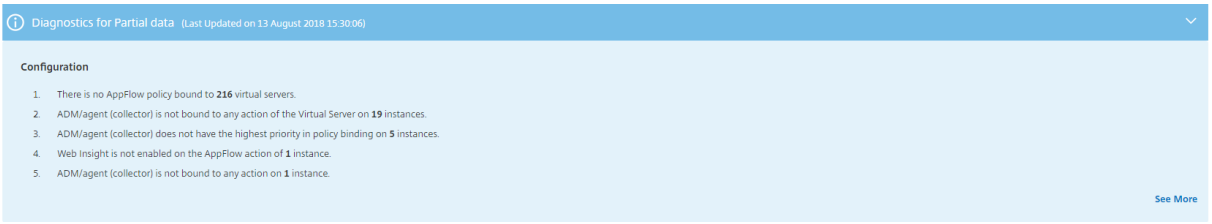
Analizar el informe de diagnóstico

El diagnóstico de autoservicio muestra el informe de diagnóstico en un fondo naranja o azul según la gravedad de los problemas.

El informe de diagnóstico en el fondo naranja indica una criticidad mayor que el fondo azul.

Por ejemplo, hay cinco servidores virtuales configurados en su instancia de NetScaler ADC. Si no ha habilitado los parámetros de AppFlow en ningún servidor virtual, NetScaler ADM no recibirá el tráfico de Web Insight y Security Insight para su análisis. Los diagnósticos de autoservicio identifican los problemas de configuración como críticos. Verá los informes de diagnóstico en fondo naranja en Web Insight y en la función Security Insight.

Si ha habilitado AppFlow en uno de los servidores virtuales, NetScaler ADM recibe datos para análisis. Verá el informe de diagnóstico en fondo azul porque al menos un servidor virtual envía tráfico para su análisis.

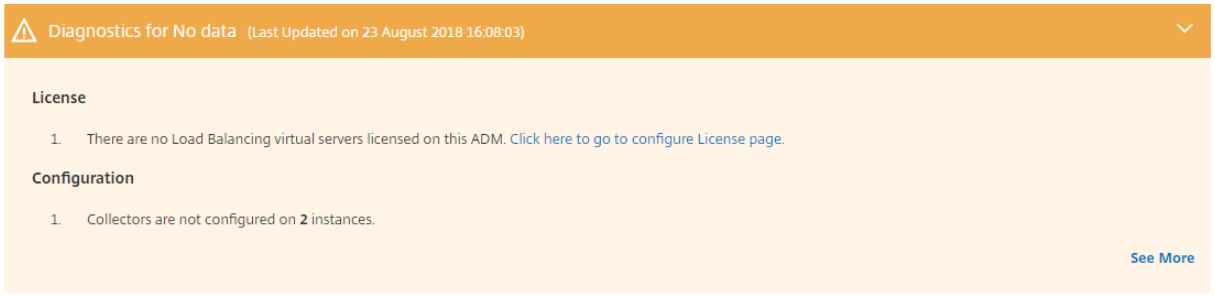


> **IMPORTANTE**: El diagnóstico de autoservicio no verifica el flujo de tráfico. Solo comprueba si existen problemas de licencia o configuración asociados con las funciones de análisis especificadas en las instancias administradas. A veces, no ve ningún dato de análisis porque no hay tráfico activo que fluya a través de los servidores virtuales.

El informe de diagnóstico tiene una página de resumen y una página de información detallada.

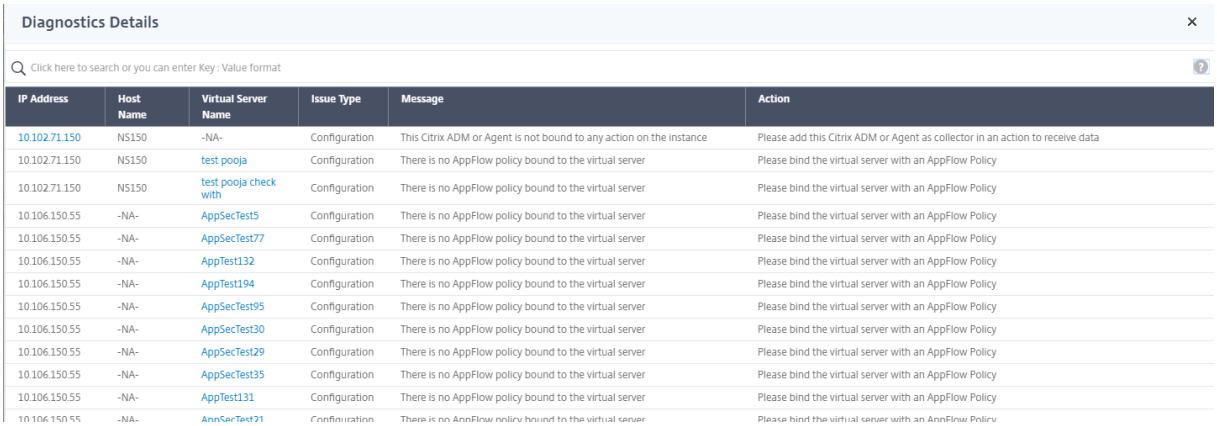
La página de resumen proporciona una descripción general de los tipos de problemas: licencia o configuración. La página puede contener hipervínculos que le dirijan a las páginas de configuración relevantes.

Por ejemplo, si no hay servidores virtuales de equilibrio de carga con licencia en NetScaler ADM, la página de resumen proporciona un hipervínculo que le dirige a la página **Licencias del sistema**.

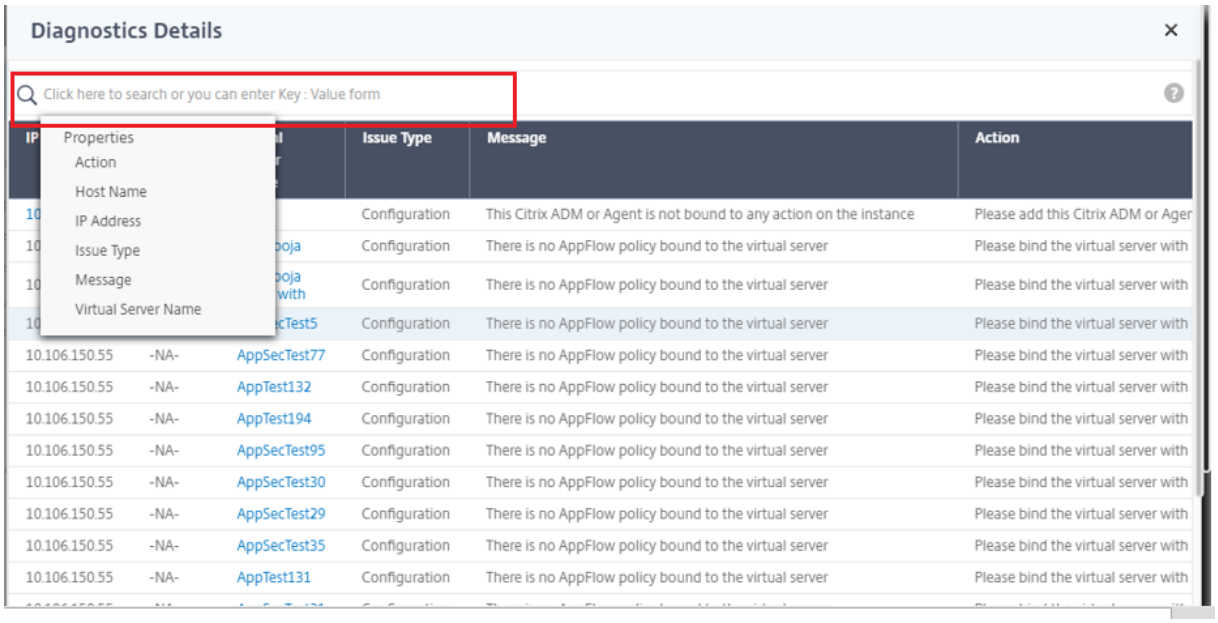


Para ver la información detallada sobre los problemas, haga clic en **Ver más** en la página de resumen.

La página de información detallada proporciona la información completa sobre los problemas y recomienda las acciones que debe realizar. Puede hacer clic en el hipervínculo en cada problema para configurar la instancia administrada o el servidor virtual.



También puede buscar los problemas en función de la acción, el nombre del host, la dirección IP y el tipo de problema, etc.



Después de resolver los problemas, debe ejecutar un diagnóstico instantáneo para generar el informe de diagnóstico más reciente.

Información web

January 30, 2024

Web Insight permite a los administradores supervisar todas las aplicaciones web servidas por las instancias de Citrix ADC. Como administrador, puede obtener una supervisión integrada y en tiempo real de las aplicaciones de las instancias de Citrix ADC. Web Insight proporciona información crítica, como la latencia de la red del cliente y el tiempo de respuesta del servidor, lo que garantiza la super-

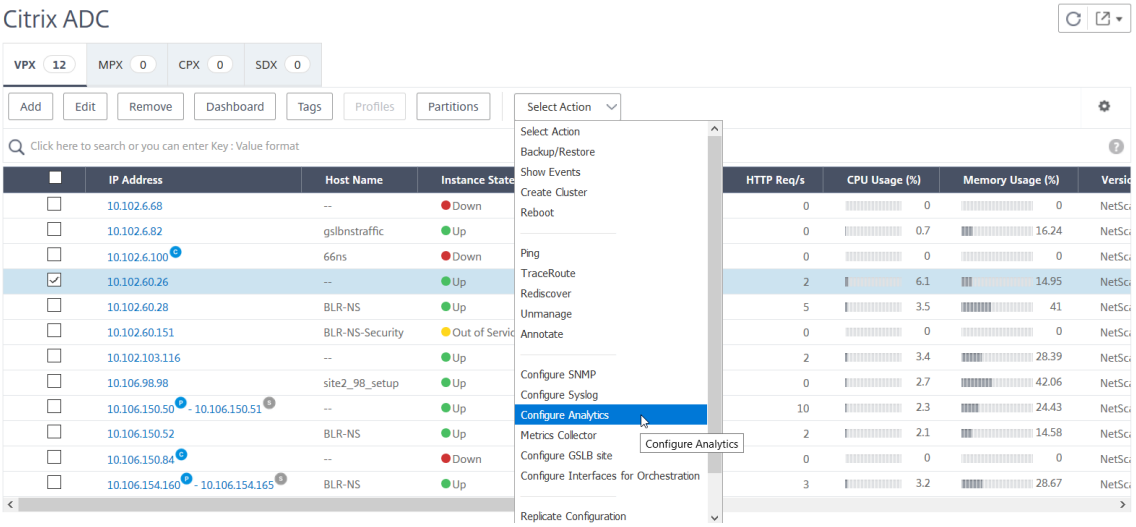
visión y la mejora del rendimiento de las aplicaciones. Los datos utilizados para el análisis se capturan de cada transacción HTTP y HTTPS que procesa la instancia de Citrix ADC. Los datos de análisis le permiten analizar el rendimiento de las instancias, la aplicación, la URL, el cliente y el servidor de Citrix ADC en su entorno.

Los siguientes son algunos de los casos de uso en los que puede ver los datos con Web Insight:

- La lista de clientes que experimentan una latencia alta al acceder a una aplicación como SharePoint
- La aplicación principal que tuvo más visitas en una hora
- La lista de aplicaciones y URL a las que se accede desde los clientes
- El sistema operativo y el explorador utilizados por un cliente en particular
- Las aplicaciones o los servidores que envían la mayor cantidad de respuestas relacionadas con errores
- Problemas de accesibilidad con un cliente en particular
- Problemas de accesibilidad en pocas o todas las aplicaciones de un cliente en particular
- Pocas páginas de una aplicación son lentas desde un cliente en particular y desde un servidor back-end
- La aplicación es lenta cuando se accede desde un cliente en particular y desde un servidor back-end

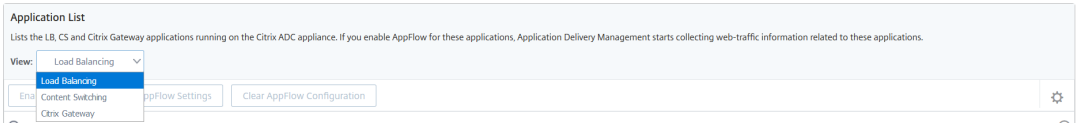
Puede habilitar Web Insight para un servidor virtual específico en una instancia seleccionada para supervisar el tráfico en la aplicación web. A continuación, la función Web Insight proporciona estadísticas para el servidor virtual en Citrix ADM. Para habilitar Web Insight:

1. Inicie sesión en Citrix ADM con credenciales de administrador.
2. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione la instancia de NetScaler ADC en la que quiere habilitar el análisis.
3. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.

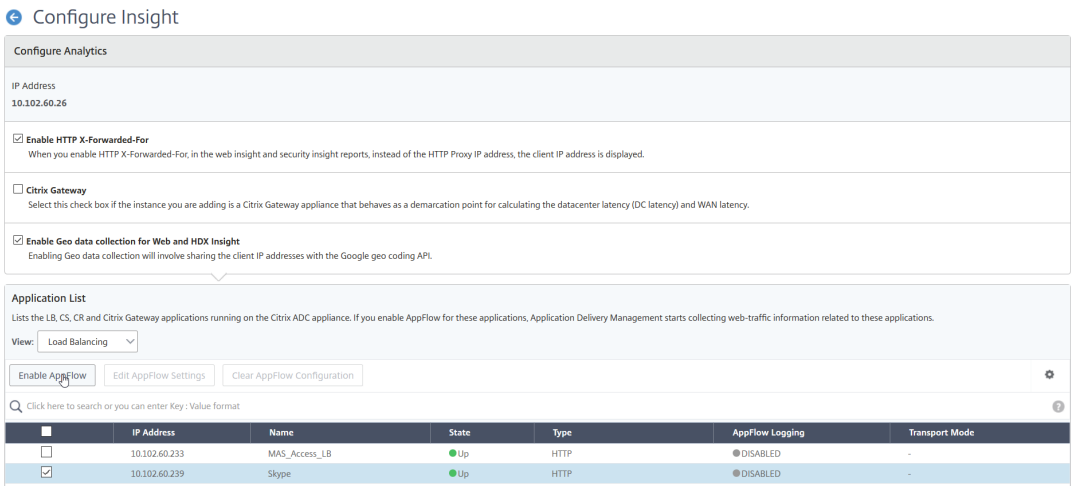


4. En la página **Configurar información** :

   a) Seleccione la **Lista de aplicaciones** para Equilibrio de carga o Content Switching.



   b) Seleccione el servidor virtual y haga clic en **Habilitar AppFlow**.

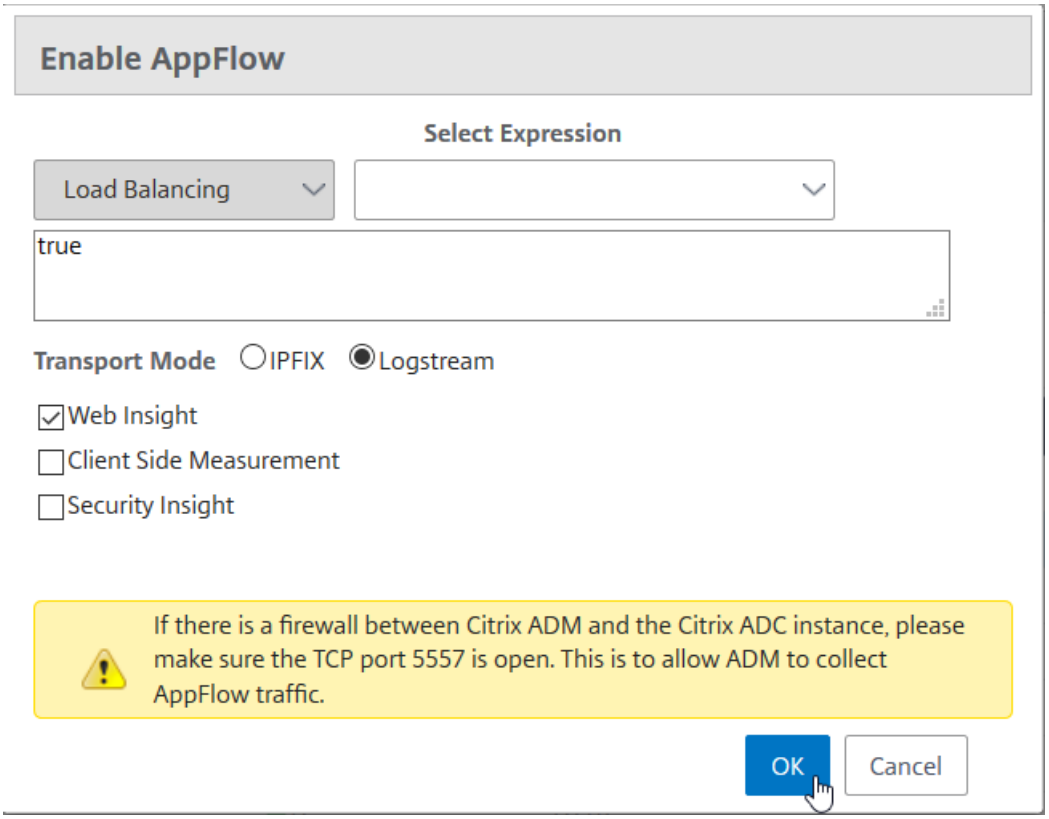


5. En el cuadro de diálogo Habilitar AppFlow:

   - Introduzca **true** en el cuadro de texto
   - Seleccione **Logstream** como modo de transporte

     > Nota: Citrix recomienda seleccionar Logstream como modo de transporte.

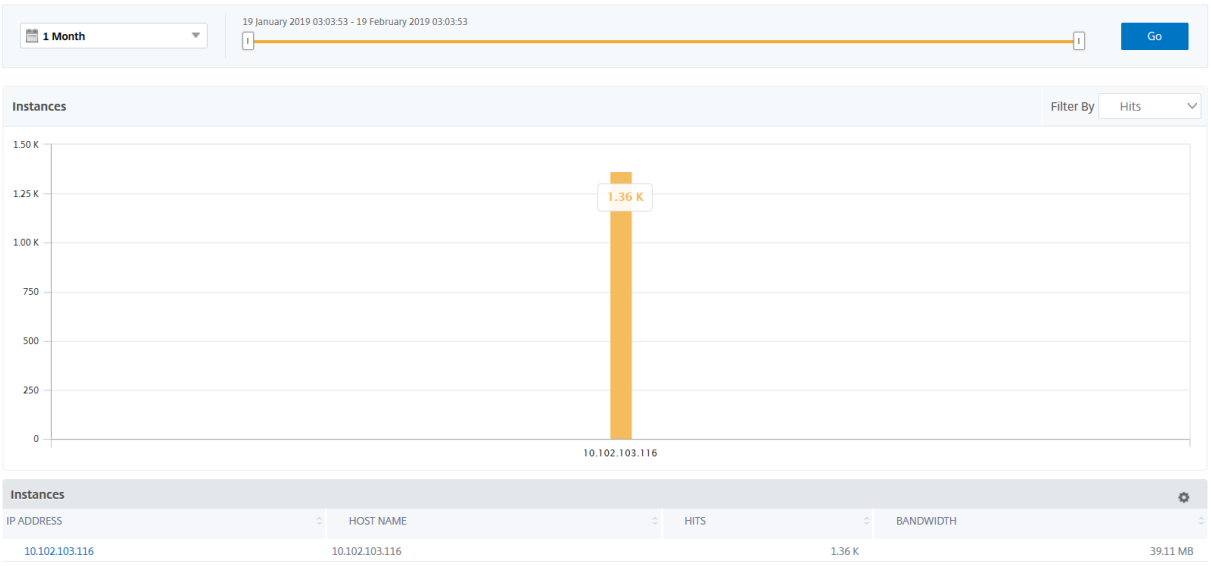
   - Seleccione **Web Insight** y haga clic en **Aceptar**.



Analizar problemas de aplicaciones web

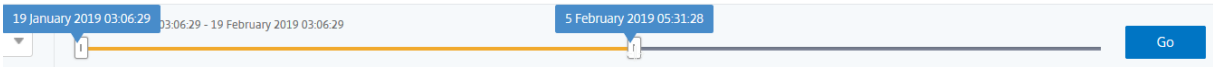
Uno de los problemas comunes que un administrador debe identificar son los problemas de latencia. Como administrador, debe averiguar si el problema de latencia proviene de la red del servidor, la red del cliente o el tiempo de respuesta del servidor. Con Citrix ADM, puede identificar esta información yendo a **Analytics** > **Web Insight** .

Cuando navega a **Analytics** > **Web Insight** , se muestran las instancias de Citrix ADC que están habilitadas con Web Insight. Puede ver la información detallada de las instancias, como la dirección IP, el nombre de host, el número total de visitas y el ancho de banda.



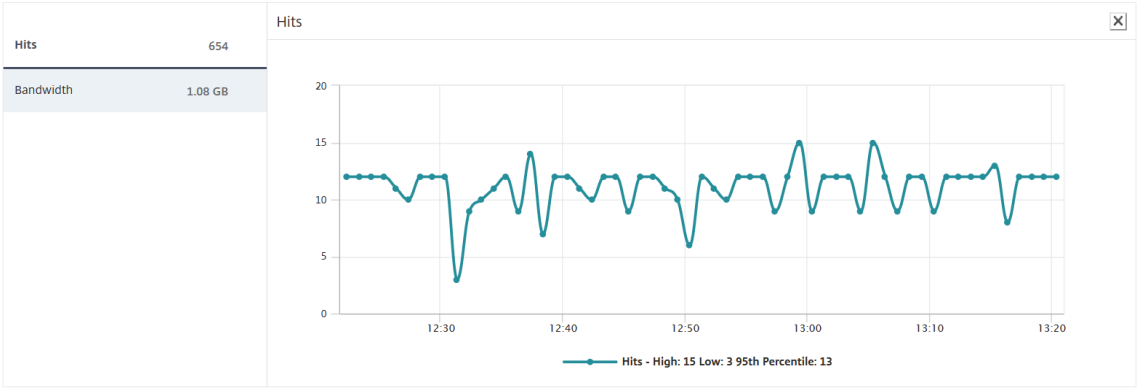
Mediante la lista, puede seleccionar la duración del tiempo para ver las perspectivas de las instancias.

También puede utilizar el control deslizante para personalizar la duración del tiempo y hacer clic en **Ir** para mostrar los resultados.

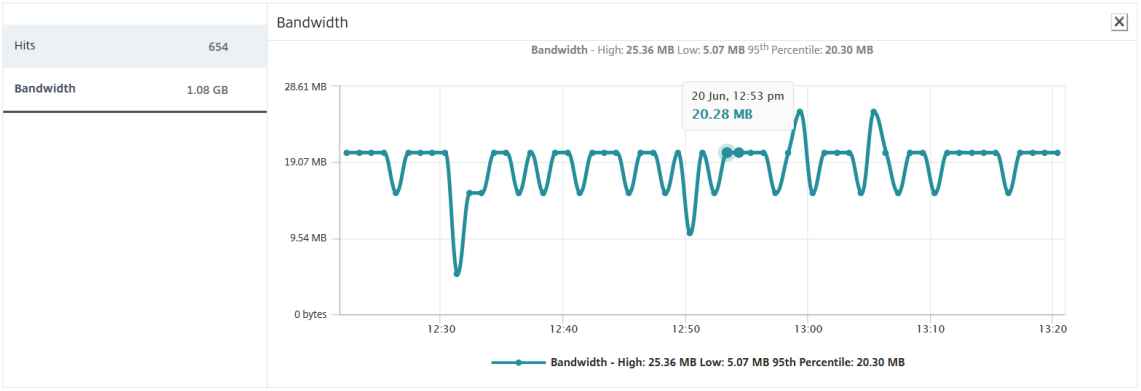


Al hacer clic en el gráfico o en la dirección IP de la instancia, se muestra la información detallada sobre la instancia. Puede ver información sobre lo siguiente:

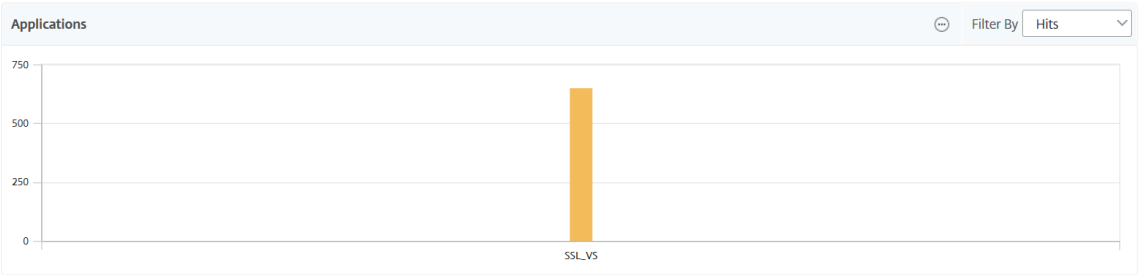
- **Número total de visitas**



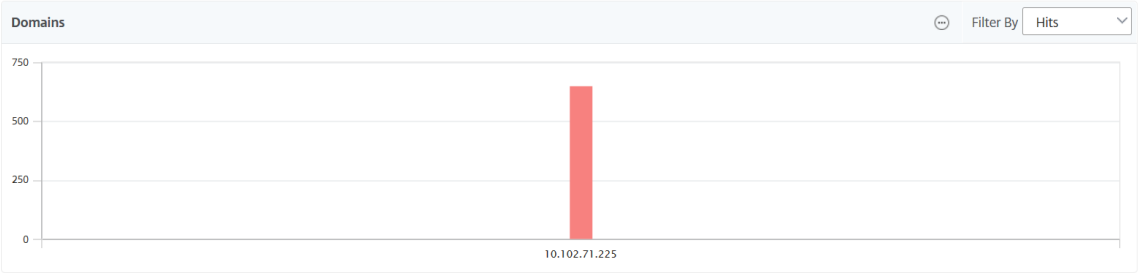
- **Ancho de banda**



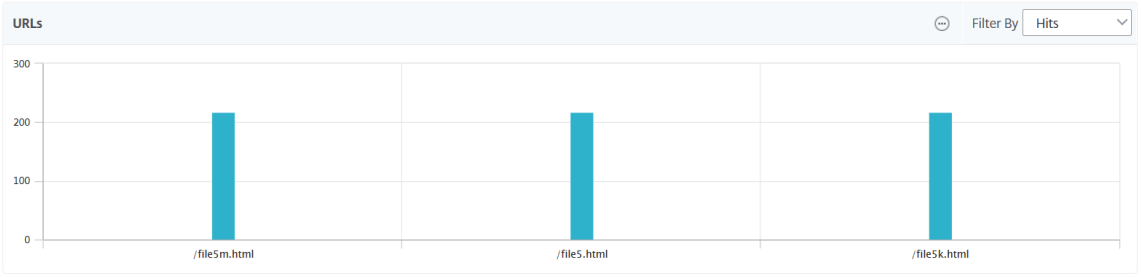
- **Aplicaciones**



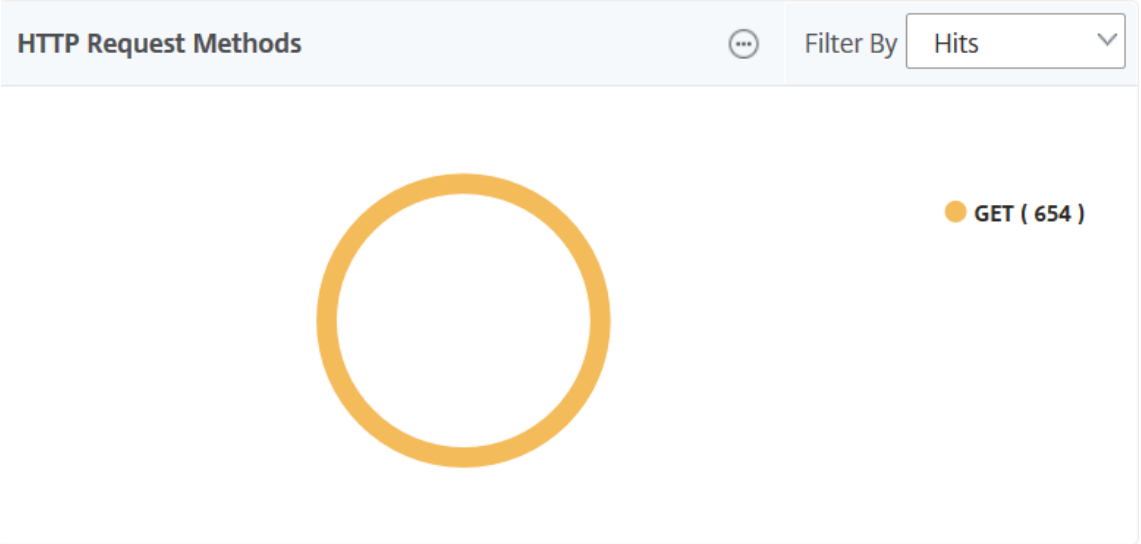
- **Dominios**



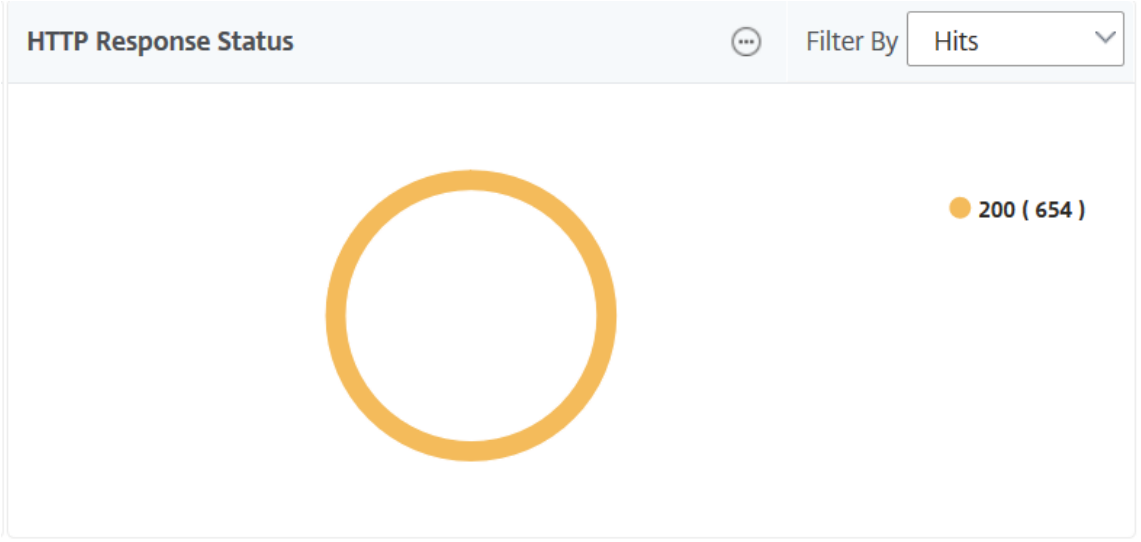
- **URLs**



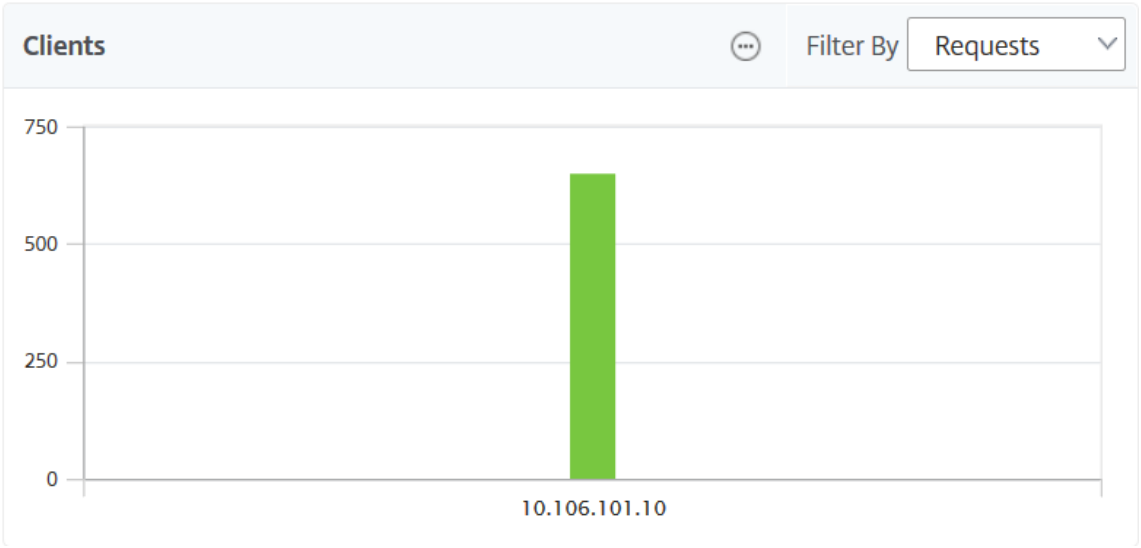
- **Métodos de solicitud HTTP**



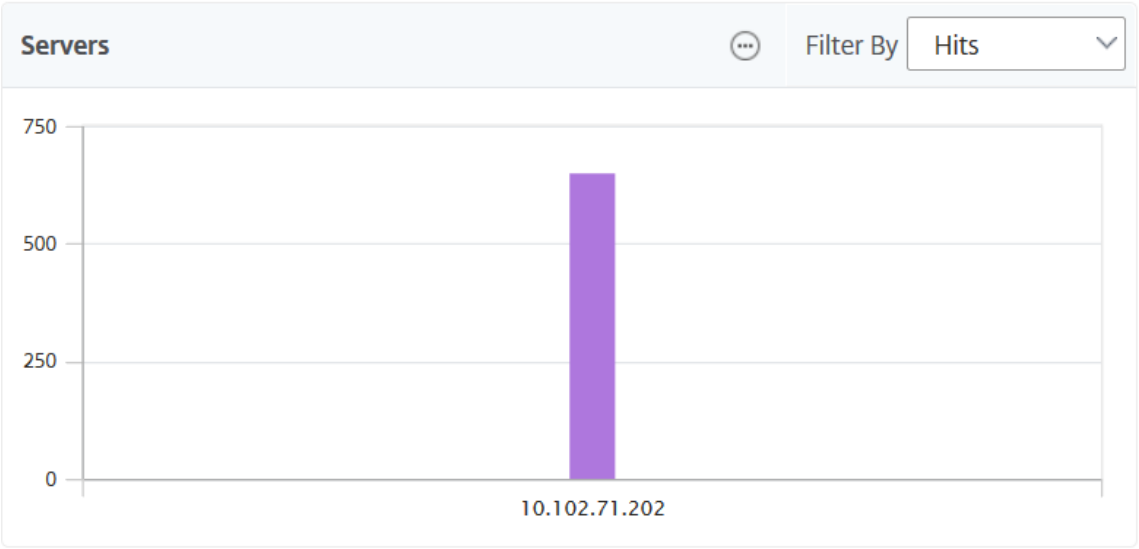
- **Estado de respuesta HTTP**



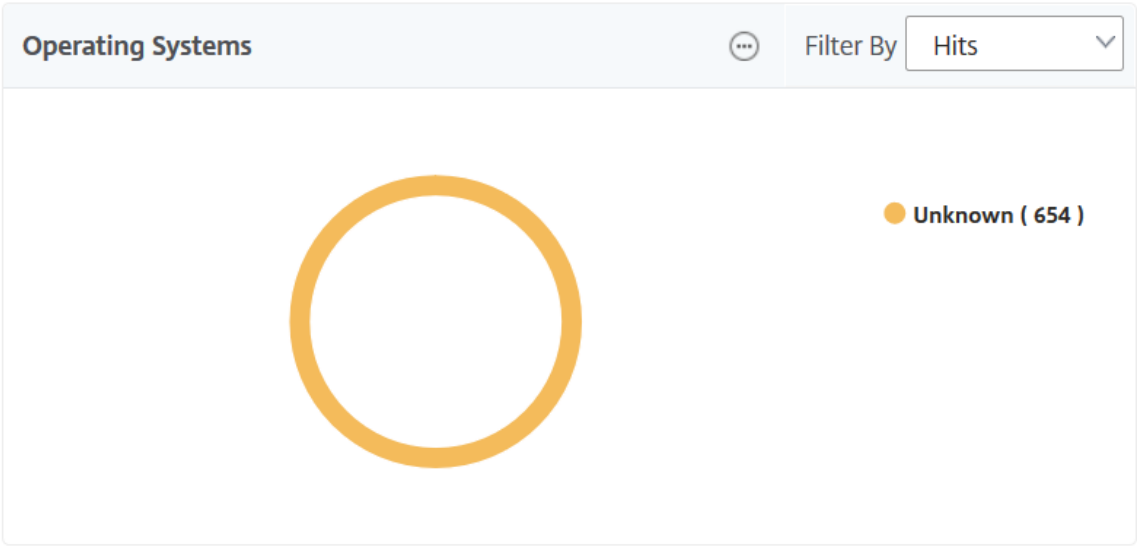
- **Clientes**



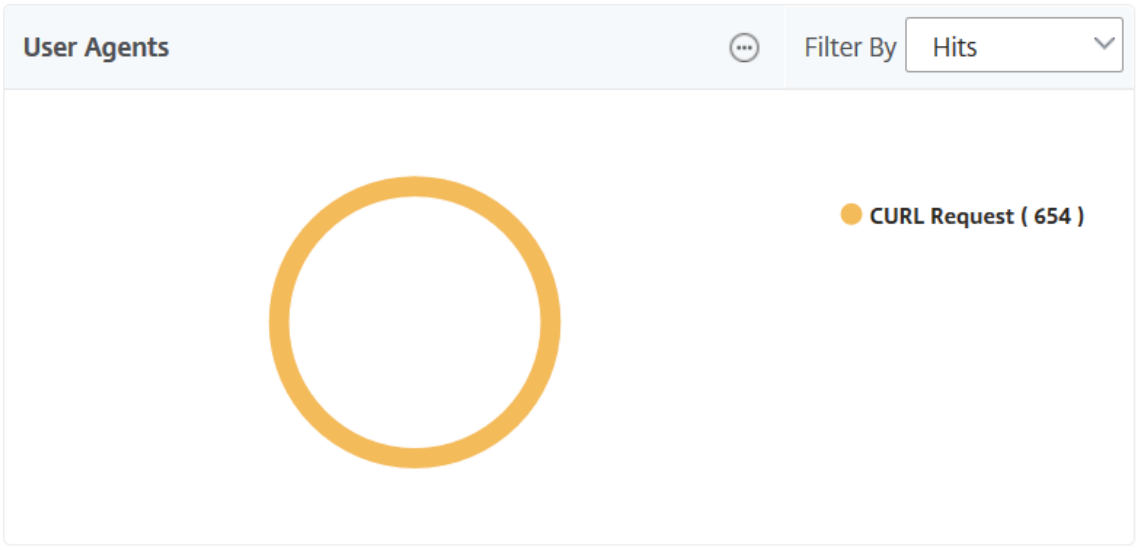
- **Servidores**



- **Sistemas operativos**

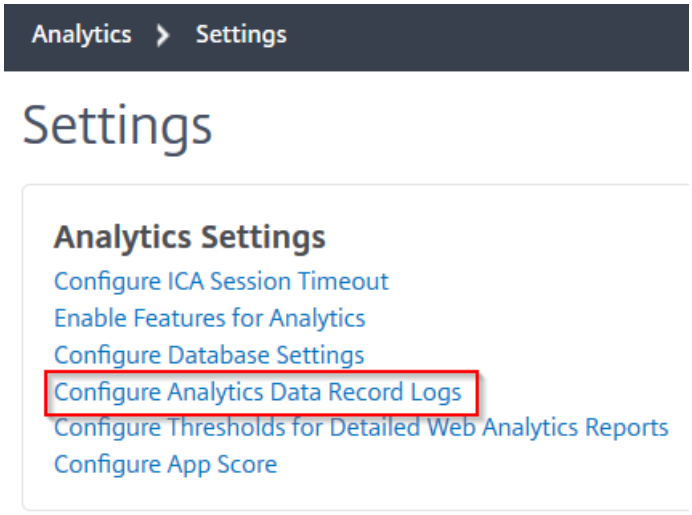


- **Agentes de usuario**

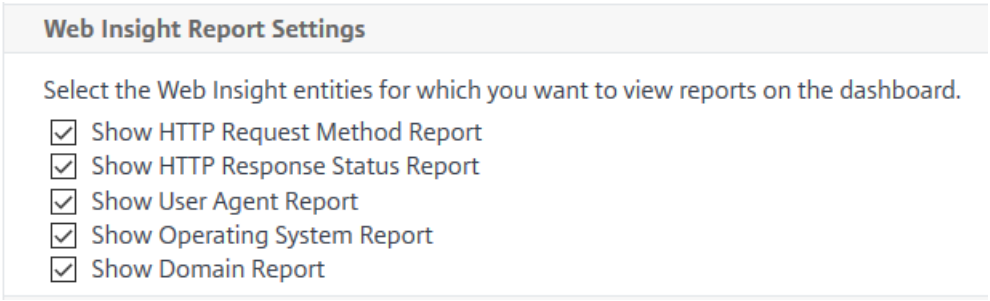


También puede seleccionar las **entidades de Web Insight** para las que desea ver los informes en la GUI.

1. Vaya a **Analytics** > **Web Insight** > **Configuración** .
2. Haga clic en **Configurar registros de datos de Analytics**.



3. En **Configuración del informe de Web Insight**, seleccione las entidades que quiere ver los informes en la GUI.



4. Haga clic en **Aceptar**.

Para profundizar en el análisis, puede hacer clic en cada categoría de información en Web Insight en la GUI. Por ejemplo, si desea comprobar los problemas de los servidores configurados:

1. Vaya a **Analytics** > **Web Insight** > **Servidores** .
2. Se muestra la página Servidores con todos los servidores configurados.
3. Haga clic en la dirección IP del gráfico. También puede hacer clic en la dirección IP de la tabla.

Se muestra la vista detallada del servidor seleccionado. Desde esta vista, puede comprobar si hay varios datos, como:

- Número total de visitas recibidas por el servidor
- Ancho de banda
- Tiempo de procesamiento del servidor
- Latencia de red del servidor
- Servidores virtuales configurados para el servidor
- Número total de clientes que acceden al servidor
- Número total de códigos de respuesta proporcionados por el servidor

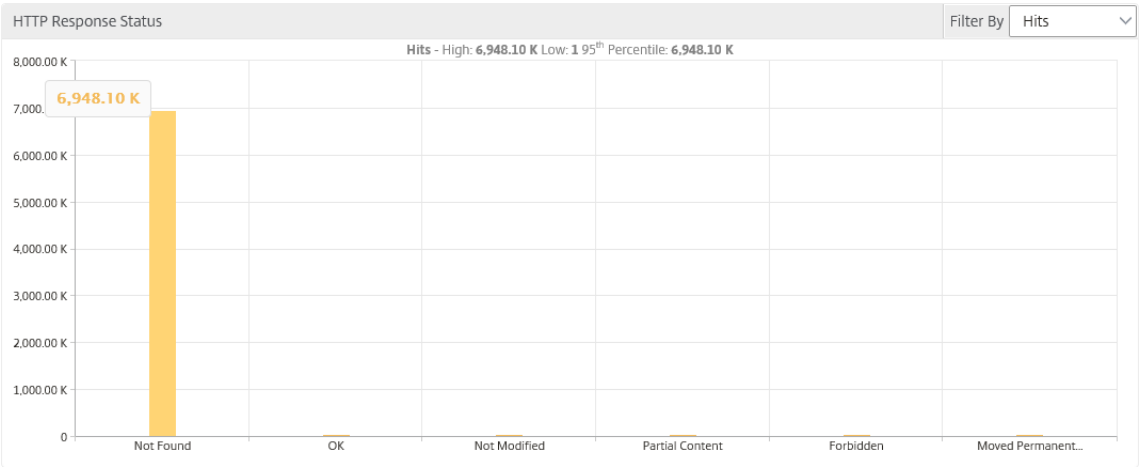
Caso de uso 1: error interno del servidor

Considere un caso en el que los usuarios están experimentando el error 500 de inaccesibilidad para su aplicación web. El error 500 (no encontrado) es un error de estado de respuesta HTTP que indica un problema en el servidor web, pero el servidor no indica el problema explícitamente. Para identificar y profundizar en el problema real:

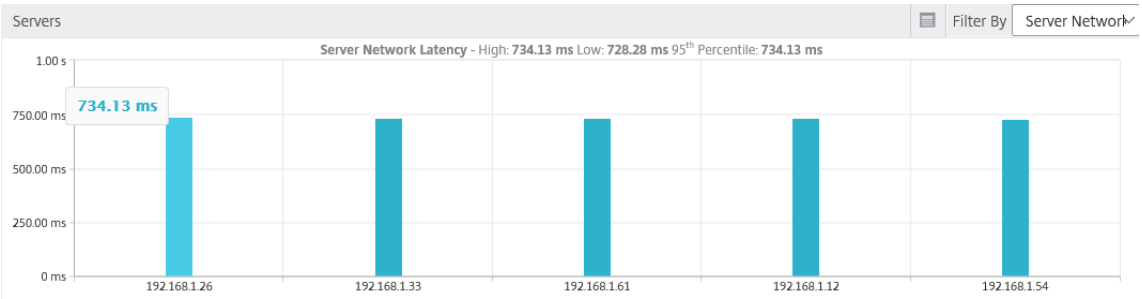
1. Vaya a **Analytics** > **Web Insight** > Estado de **respuesta** .

   Se muestra la página del panel de control. El panel le proporciona las métricas que puede usar para analizar el éxito y el fracaso de las transacciones HTTP que se procesan.

2. Haga clic en **No encontrado** en el gráfico.



3. Desplázate hacia abajo para ver el **gráfico de servidores** y, en la lista **Filtrar por** , selecciona **Latencia de red de servidores** .



El gráfico indica que cada servidor de aplicaciones tuvo un problema al recuperar la aplicación web y, por lo tanto, aumenta el tiempo de respuesta para el servidor web. El problema puede deberse a que el servidor web no responde a ninguna solicitud de ningún servidor.

Caso de uso 2: el usuario experimenta lentitud para acceder a la aplicación web

Considere un caso en el que su aplicación web está alojada a través de 10 servidores web diferentes. Cuando varios usuarios acceden a la aplicación al mismo tiempo, es posible que uno o más usuarios experimenten lentitud en la aplicación. Como administrador, debe analizar los siguientes casos para comprender la causa raíz del problema:

Caso 1: Tiempo de procesamiento del servidor:

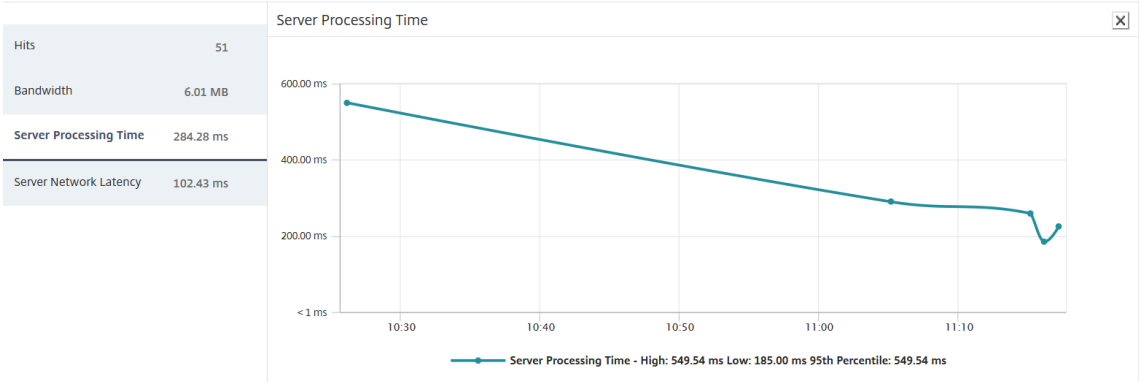
Cuando varias solicitudes llegan a los 10 servidores web al mismo tiempo, el tiempo necesario para cargar la solicitud varía en función de:

- Número de solicitudes en la cola.
- El ancho de banda consumido por cada solicitud para procesar la transacción HTTP.

  El gráfico del servidor puede ayudarlo a comprender el tiempo de procesamiento de cada servidor para la solicitud procesada por los servidores. Del mismo modo, el gráfico de la aplicación

muestra las visitas, el tiempo de respuesta y el ancho de banda consumido por cada transacción HTTP.

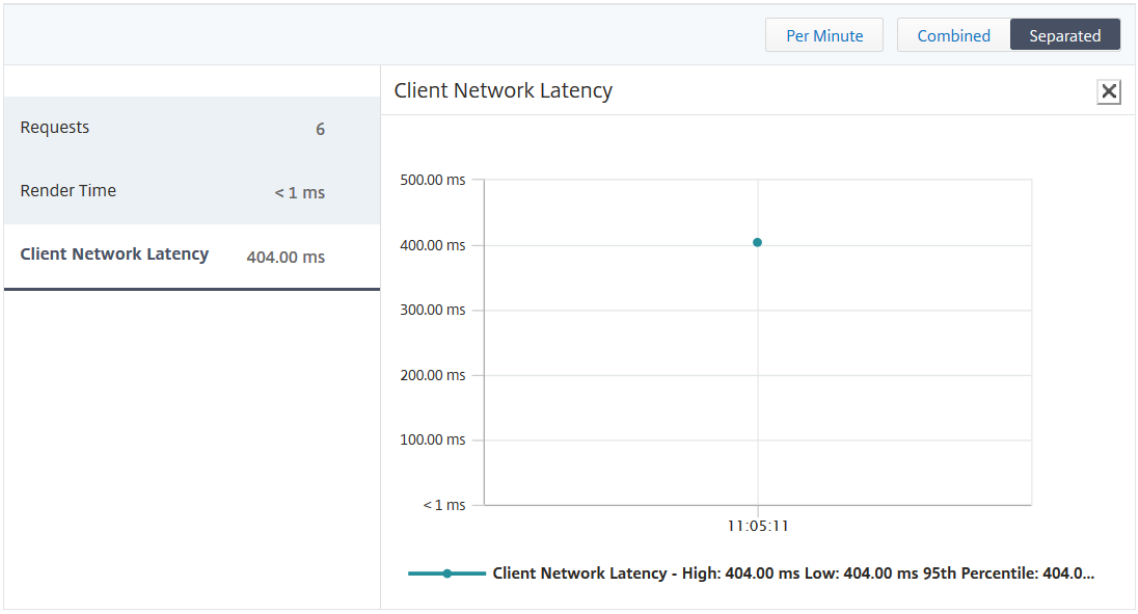
1. Vaya a **Analytics** > **Web Insight** > **Servidores** .
2. Seleccione el servidor en el gráfico.
3. Haga clic en **Tiempo de procesamiento del servidor** para analizar el tiempo de procesamiento del servidor.



Caso 2: Latencia del cliente:

El tiempo de respuesta y el número total de visitas a la aplicación pueden ser la razón de la lentitud del acceso a la aplicación. Puede comprobar la latencia de la red del cliente y analizar las métricas de la latencia de la red del cliente. Para analizar la causa principal:

1. Vaya a **Analytics** > **Web Insight** > **Clientes** .
2. Seleccione el cliente del gráfico.
3. Haga clic en **Latencia de red cliente** para analizar la latencia alta.



En este ejemplo, como administrador, puede ver que la causa raíz del problema proviene de la red del cliente porque la latencia de la red del cliente indica alta.

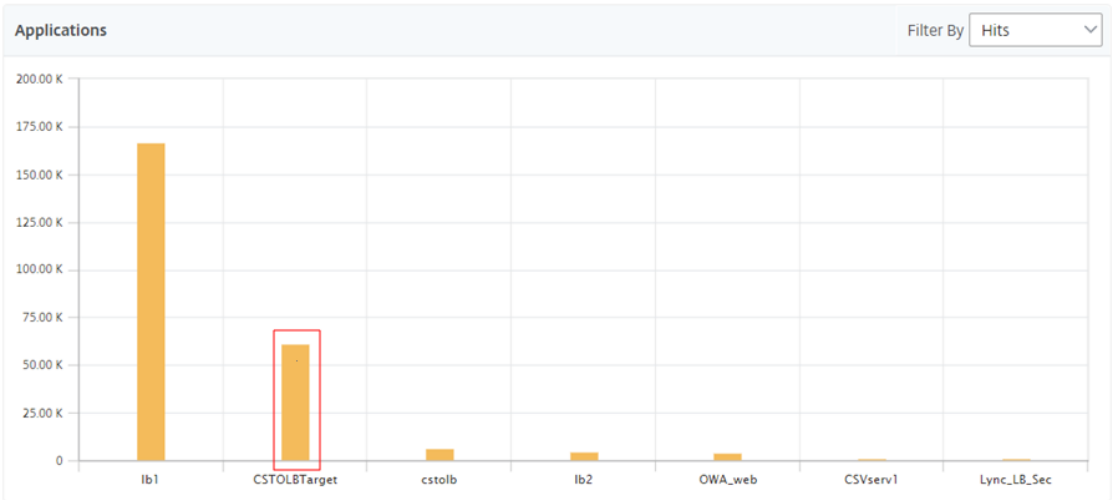
Caso de uso 3: Lentitud en el acceso a la aplicación web

Considere un caso en el que tiene servidores web para usuarios de Windows y servidores web para usuarios de Mac, y los usuarios están informando de lentitud en el acceso a la aplicación web. Como administrador, sabe que tiene:

- Configuró un servidor virtual de conmutación de contenido para usuarios de Windows.
- Configuró un servidor virtual de conmutación de contenido para usuarios de Mac.
- Se configuraron los servicios asociados enlazados a los servidores virtuales para redirigir las solicitudes en función de los usuarios de Windows y Mac.

Para analizar la causa principal del problema de lentitud de las aplicaciones web:

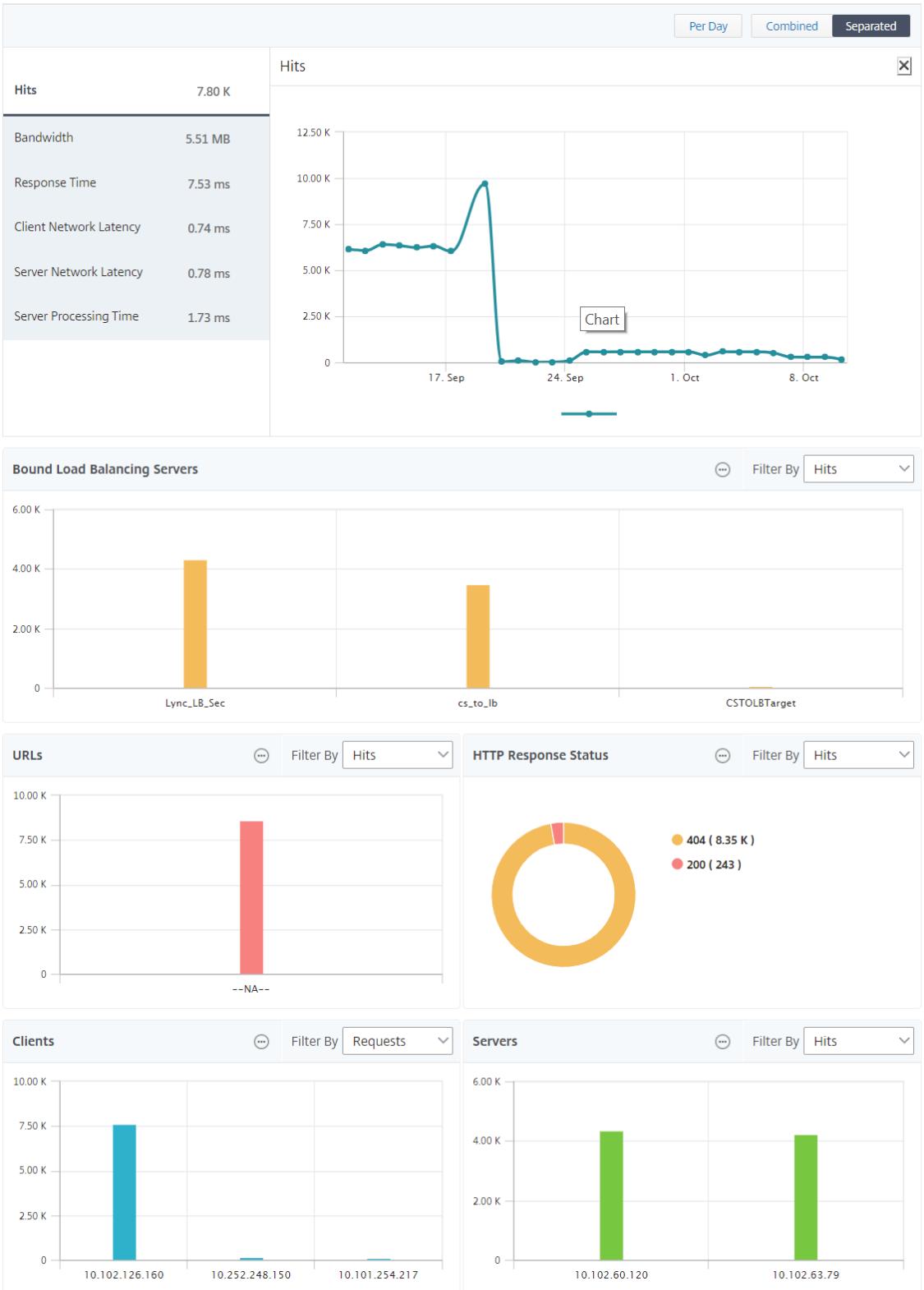
1. Vaya a **Analytics** > **Web Insight** > **Aplicaciones**
2. Seleccione el servidor virtual de conmutación de contenido.
   Por ejemplo, la aplicación «csTolbTarget» de la imagen es un servidor virtual de conmutación de contenido que está enlazado a otros servidores virtuales de equilibrio de carga.



Applications

Name	Hits ↓	Bandwidth	Response Time
lb1	167.05 K	136.74 MB	0.74 ms
CSTOLBTarget	61.06 K	60.14 MB	8.66 ms
cstolb	6.61 K	4.80 MB	374.97 ms
lb2	4.83 K	3.61 MB	0.67 ms
OWA_web	4.31 K	3.27 MB	3.21 ms
CSVserv1	291	184.82 KB	157.12 ms
Lync_LB_Sec	10	12.63 KB	86.43 ms

3. Haga clic en el servidor virtual de conmutación de contenido para ver el otro servidor virtual de equilibrio de carga. También puede hacer clic en el nombre de la aplicación en la tabla.



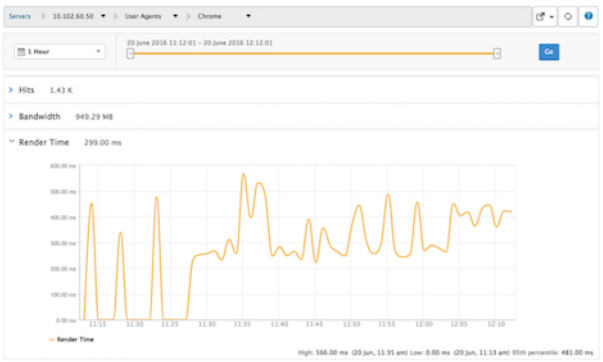
También puede hacer clic en los servidores de equilibrio de carga enlazados para ver los detalles de Web Insight de esas aplicaciones.

Analizar información para exploradores y sistemas operativos

Puedes usar Web Insight para ayudarte a separar los problemas de latencia L7 y entender el uso de los dispositivos móviles. Como administrador, la información puede ayudarlo a comprender las diferentes adopciones de los sistemas operativos en su base de usuarios.

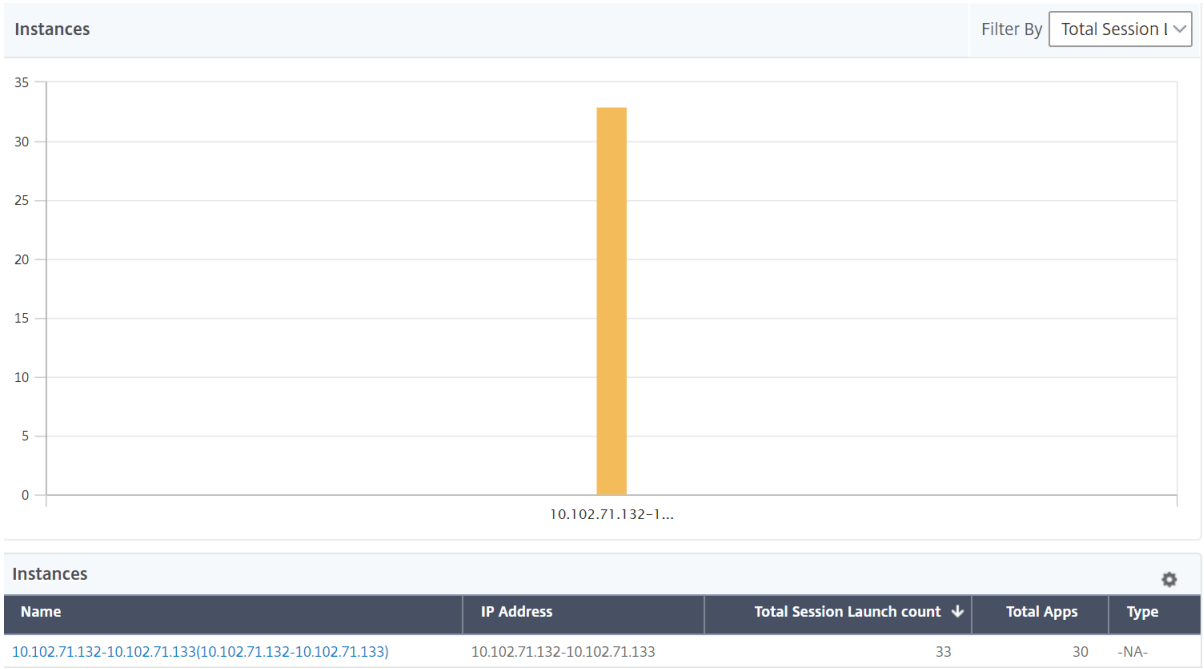
Vaya a **Analytics** > **Web Insight** > **Sistema operativo** para ver por qué hay lentitud en el acceso de los usuarios y si se debe a la incompatibilidad entre determinados exploradores. También puede ver qué sistemas operativos se están utilizando en determinados clientes y los exploradores a los que se accede. Puede comparar el tiempo de procesamiento en los diferentes navegadores y profundizar en un navegador en particular para identificar qué páginas de la aplicación están asociadas con el tiempo de procesamiento más alto para ese navegador.

Por ejemplo, puede seleccionar Google Chrome y ver los tiempos de representación correspondientes para las diferentes páginas URL de una aplicación concreta.

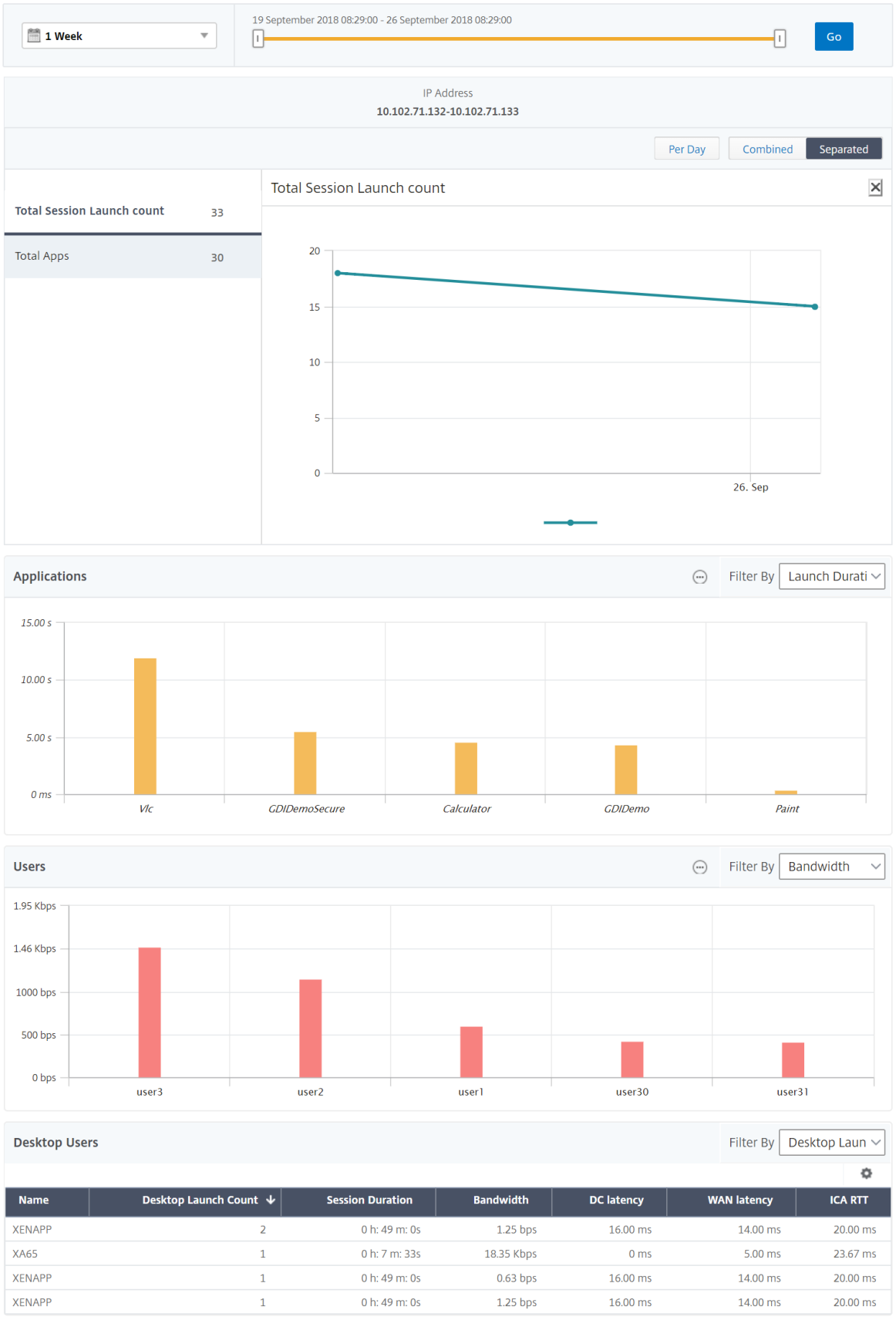


Instancias NetScaler ADC implementadas en modo de alta disponibilidad

Citrix ADM proporciona informes para las instancias de ADC que se implementan en modo de alta disponibilidad. Todos los análisis admiten informes agregados para instancias en modo de alta disponibilidad.



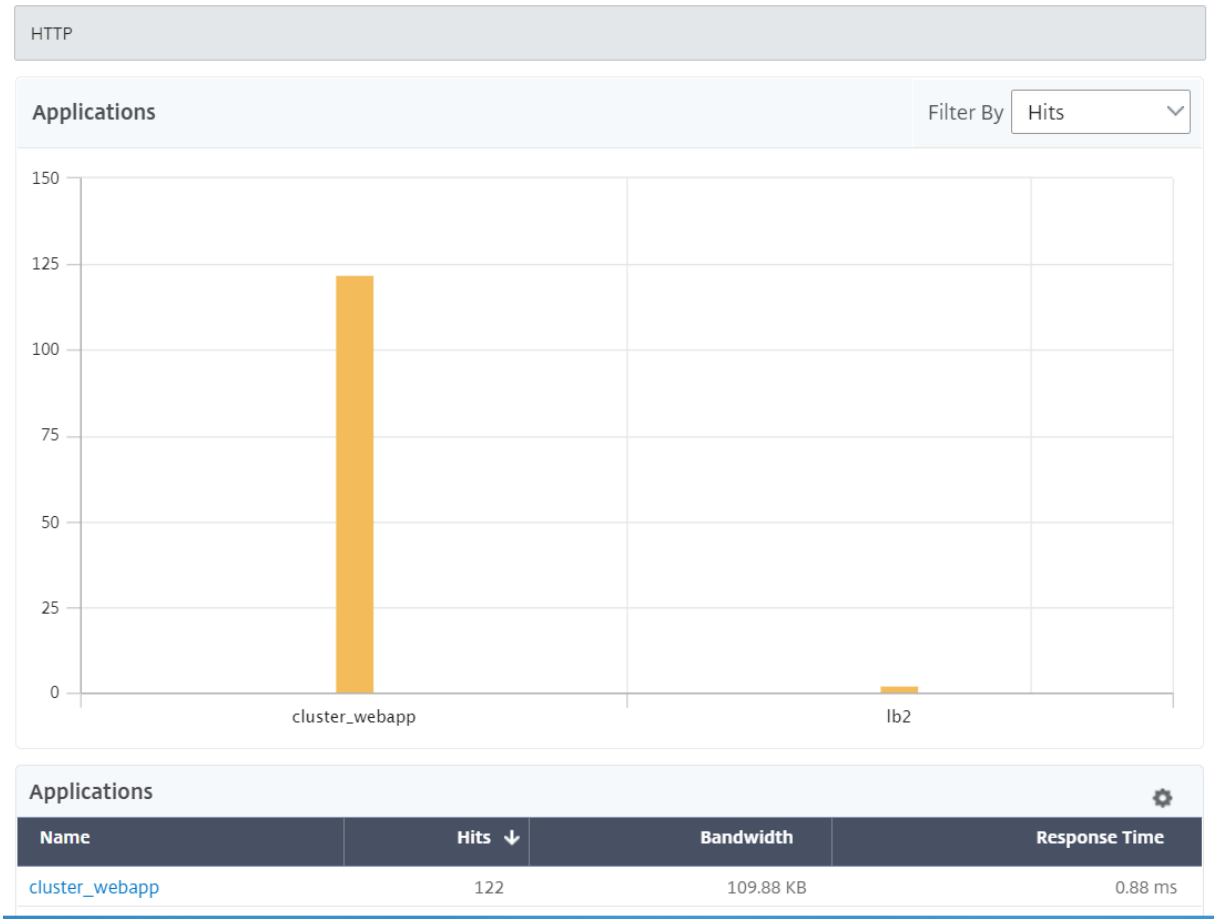
Puede hacer clic en el nombre de las instancias que están en alta disponibilidad para ver más detalles.



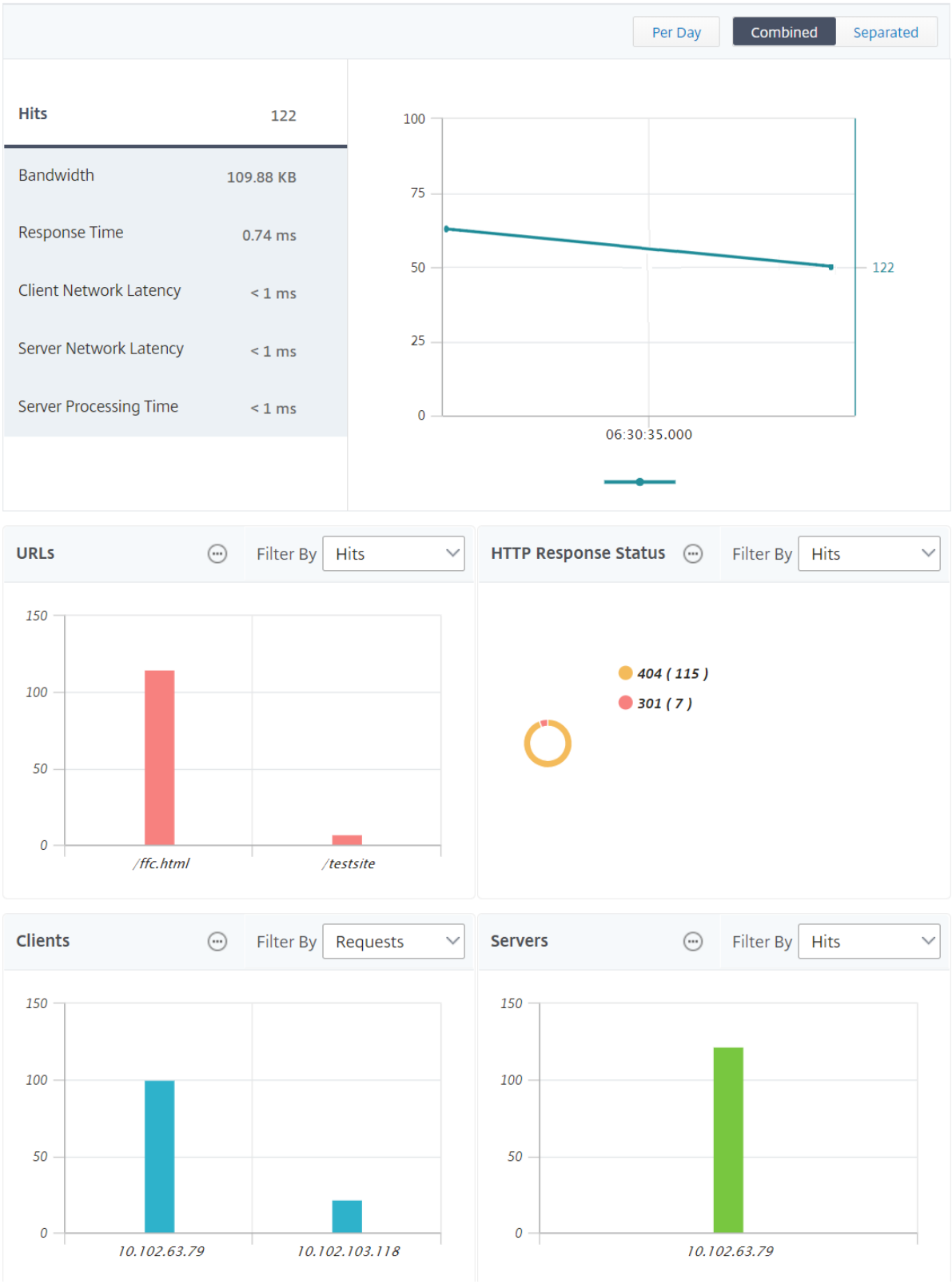
Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

Instancias NetScaler ADC implementadas en modo de clúster

Citrix ADM proporciona informes para las instancias de ADC que se implementan en modo clúster. Todos los análisis admiten informes agregados de instancias en modo de clúster.



También puede hacer clic en el nombre de host CLIP para ver todos los detalles sobre las instancias de ADC que se implementan en modo de clúster.



Nota

- Todos los datos recopilados anteriormente antes de actualizar a Citrix ADM 12.1 build 503.x siguen mostrándose como informes independientes durante el período hasta que los datos persistan.
- Para las instancias de ADC implementadas en modo clúster, el ID del dominio de observación o los nombres de dominio de observación se sustituyen por el nombre de host CLIP y CLIP. Todos los datos recopilados anteriormente continúan reportando el ID del dominio de observación/el nombre del dominio de observación.

Configuración del mapa geográfico de Web Insight

La función Geomaps de NetScaler ADM muestra el uso de aplicaciones web en diferentes ubicaciones geográficas en un mapa. Los administradores pueden utilizar esta información para comprender las tendencias en el uso de aplicaciones y para la planificación de la capacidad.

Geomap proporciona información sobre las siguientes métricas específicas de un país, estado y ciudad:

- Número total de visitas: Número total de veces que se accede a una aplicación.
- Ancho de banda: ancho de banda total consumido al atender las solicitudes
- Tiempo de respuesta: Tiempo medio necesario para enviar respuestas a las solicitudes de los clientes.

Los geomapas proporcionan información que se puede utilizar para abordar varios casos de uso, como los siguientes:

- Región que tiene el número máximo de clientes que acceden a una aplicación
- Región que tiene el tiempo de respuesta más alto
- Región que consume más ancho de banda

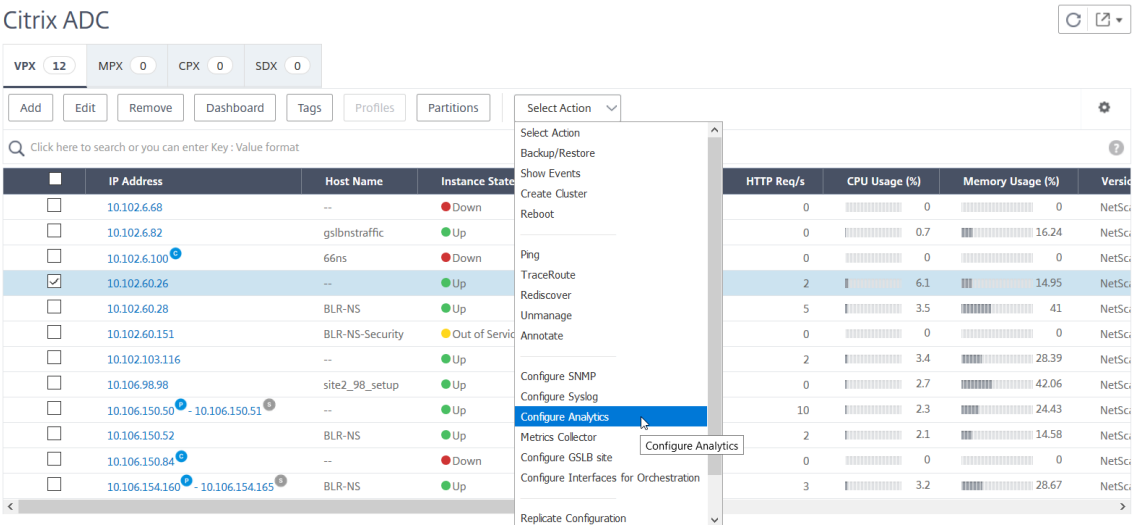
Citrix ADM le ofrece la opción de configurar mapas geográficos para direcciones IP privadas o direcciones IP públicas.

Configurar geometrías para direcciones IP privadas

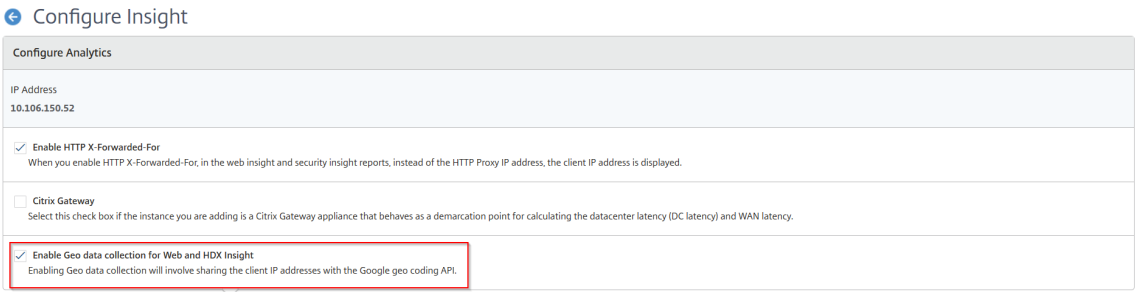
Para ver el tráfico de aplicaciones web que se origina desde direcciones IP privadas en la geomapa, primero debe crear bloques de direcciones IP privadas y, a continuación, habilitar la recopilación de datos geográficos.

Para habilitar la recopilación de datos geográficos:

1. Vaya a **Redes** > **Instancias** > **Citrix ADC** y seleccione la instancia de Citrix ADC.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.



3. En la página **Configurar Insight** , seleccione **Habilitar la recopilación de datos geográficos para Web y HDX Insight**.



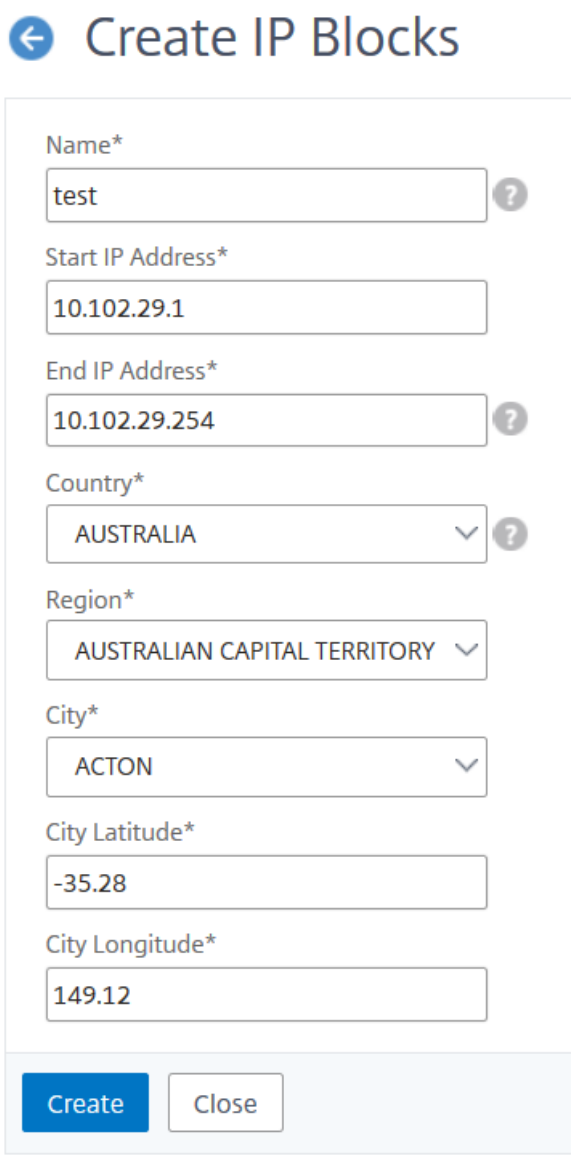
Crear un bloque de IP privado NetScaler ADM puede reconocer la ubicación de un cliente cuando la dirección IP privada del cliente se agrega al servidor NetScaler ADM. Por ejemplo, si la dirección IP de un cliente se encuentra dentro del intervalo de un bloque de direcciones IP privado asociado con Ciudad A, NetScaler ADM reconoce que el tráfico se origina desde Ciudad A para este cliente.

Para crear un bloque IP:

1. En Citrix ADM, vaya a **Analytics** > **Configuración** > **Bloques de IP** y, a continuación, haga clic en **Agregar**.
2. En la página **Crear Bloques de IP**, especifique los siguientes parámetros:
   - **Nombre**. Especifique un nombre para el bloque de IP privado
   - **Dirección IP inicial**. Especifique el rango de direcciones IP más bajo para el bloque de IP.
   - **Dirección IP final**. Especifique el rango de direcciones IP más alto para el bloque de IP.

- **País**. Selecciona el país de la lista.
- **Región**. Según el país, la región se rellena automáticamente, pero puede seleccionarla.
- **Ciudad**. Según la región, la ciudad se rellena automáticamente, pero puede seleccionar la ciudad.
- **Latitud** y **longitud de la ciudad**. Según la ciudad que selecciones, la latitud y la longitud se rellenan automáticamente.

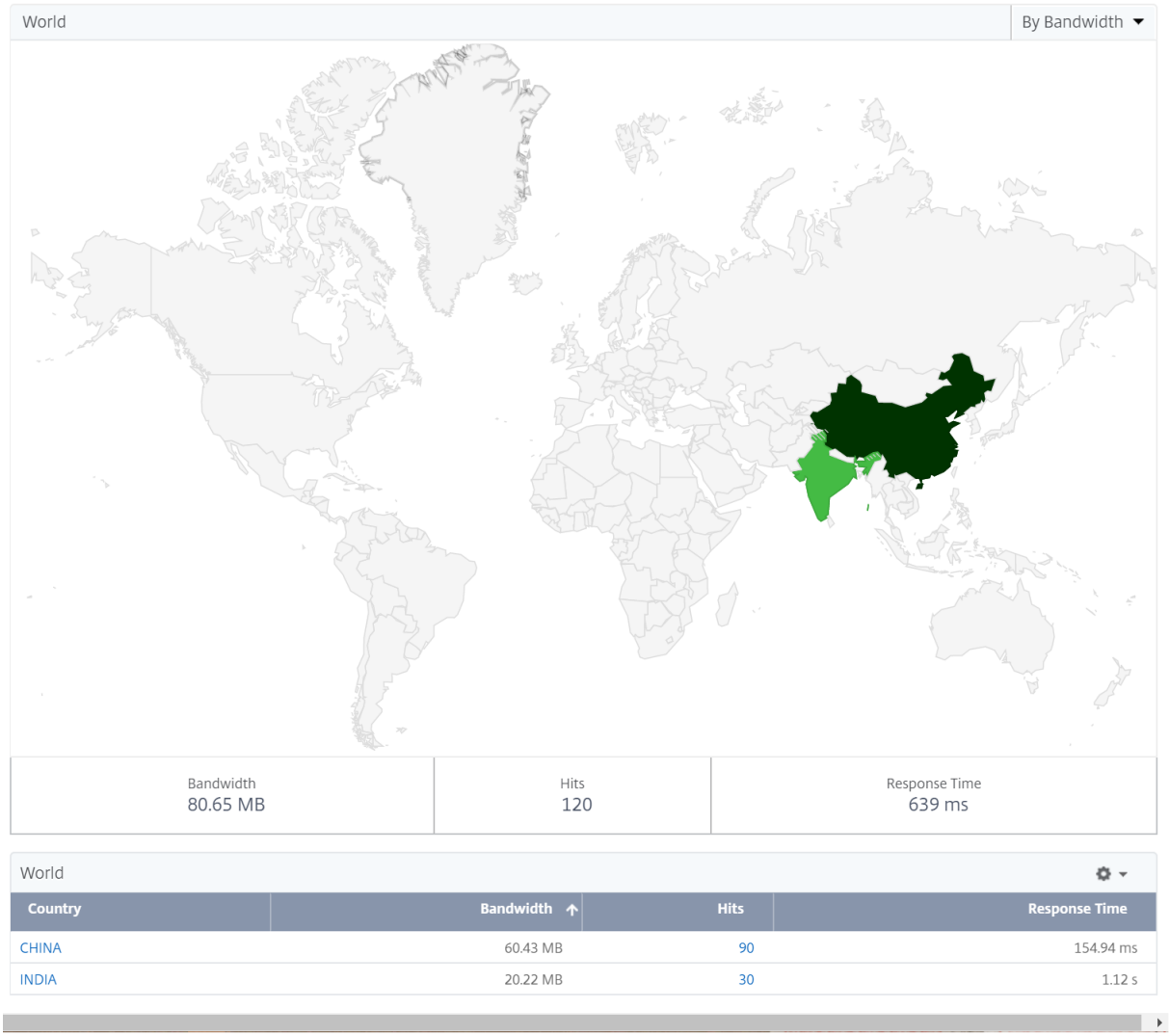
3. Haga clic en **Crear** para finalizar.



Bloques IP públicos Citrix ADM también puede reconocer la ubicación de un cliente si el cliente utiliza una dirección IP pública. NetScaler ADM tiene su archivo CSV de ubicación integrado que coincide

con la ubicación según el intervalo de direcciones IP del cliente. Para usar un bloque de IP público, el único requisito es habilitar la recopilación de datos geográficos desde la página Configure Insight.

> Nota
>
> NetScaler ADM requiere una conexión a Internet para mostrar los mapas geográficos de una ubicación geográfica determinada. También se requiere conexión a Internet para exportar el GeoMap en formatos.pdf,.png o.jpg.



Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.

2. Seleccione la ficha **Planificar exportación**. Programar el informe a diario, semanal o mensual y enviarlo por correo electrónico o mensaje de Slack.

> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

Configurar umbrales

Puede crear umbrales y recibir una notificación cada vez que se supere el valor del umbral. En una implementación típica, puede establecer umbrales para:

- Realice un seguimiento de las diferentes métricas
- Facilitar la planificación
- Reciba notificaciones cuando el valor de la métrica de la aplicación supere el umbral establecido

Para configurar el umbral:

1. Vaya a **Analytics** > **Configuración** > **Umbrales**.
2. En la página **Umbrales**, haga clic en **Agregar**.

   Aparece la página **Crear umbral** .
3. Especifique los siguientes detalles:

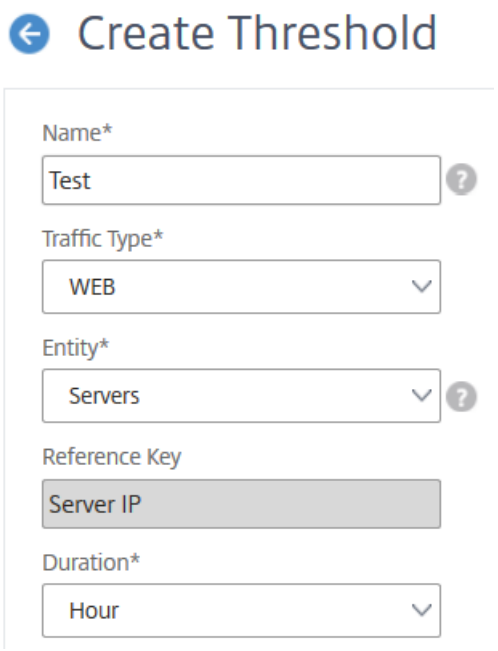
   a) **Nombre**: especifique un nombre para crear un evento.

   b) **Tipo**de tráfico : en la lista, selecciona WEB.

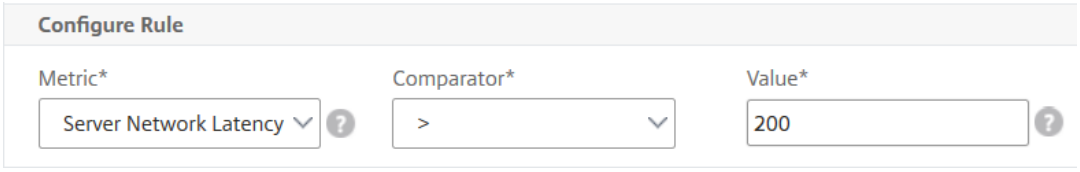
   c) **Entidad**: en la lista, seleccione la categoría o el tipo de recurso. De forma predeterminada, se selecciona «aplicaciones» como entidad.

   d) **Clave**de referencia: se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.

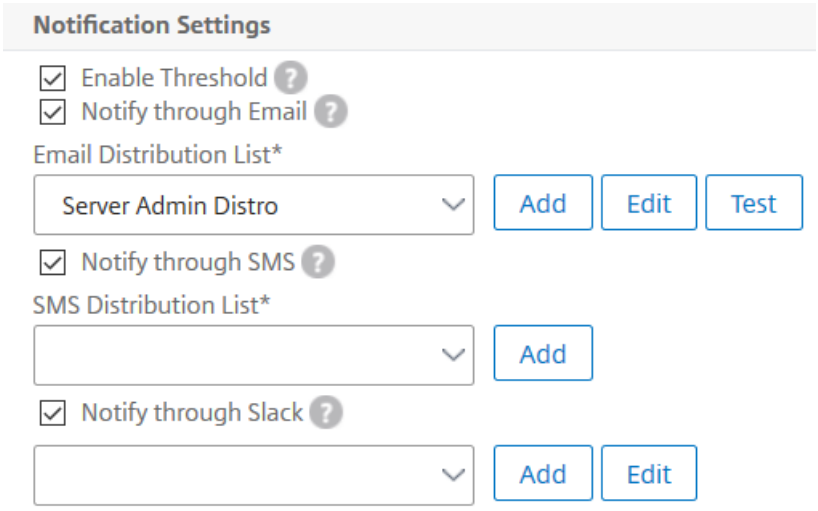
   e) **Duración**: en la lista, seleccione el intervalo de tiempo durante el que desea supervisar la entidad. Puede supervisar las entidades durante una hora, un día o una semana de duración.



f) En la sección **Configurar regla**, cree una regla eligiendo la métrica, un comparador necesario y proporcione un valor de umbral.



g) En la sección **Configuración de notificaciones**, seleccione **Habilitar umbral** y el modo de alerta para el que quiere obtener las alertas.



4. Haga clic en **Crear**.

HDX Insight

January 30, 2024

HDX Insight proporciona una visibilidad integral del tráfico de HDX a Citrix Virtual Apps and Desktops que pasa por Citrix ADC. También permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento. La disponibilidad de datos de visibilidad en tiempo real e históricos permite que Citrix Application Delivery Management (ADM) admita una amplia variedad de casos de uso.

Para que aparezcan los datos, debe habilitar AppFlow en sus servidores virtuales de Citrix Gateway. AppFlow se puede entregar mediante el protocolo IPFIX o el método LogStream.

> **Nota** Para permitir que se registren los cálculos del tiempo de ida y vuelta de ICA, habilite la siguiente configuración de directiva:

- Cálculo de ida y vuelta de ICA
- Intervalo de cálculo de ida y vuelta
- Cálculo ICA de ida y vuelta para conexiones inactivas

Si hace clic en un usuario individual, podrá ver cada sesión de HDX, activa o finalizada, que el usuario haya realizado en el período de tiempo seleccionado. Otra información incluye varias estadísticas de latencia y ancho de banda consumido durante la sesión. También puede obtener información de ancho de banda de canales virtuales individuales, como el audio, la asignación de impresoras y la asignación de unidades de cliente.

También puede navegar a **HDX Insight** > **Aplicaciones** y hacer clic en **Duración del lanzamiento**para ver el tiempo que tarda la aplicación en iniciarse. También puede ver el agente de usuario de todos los usuarios conectados navegando hasta**HDX Insight**-> Usuarios.

> **Nota**HDX Insight admite Particiones de administración configuradas en instancias de Citrix ADC que se ejecutan en la versión 12.0 de software.

Los siguientes clientes ligeros admiten HDX Insight:

- Thin Clients WYSE basados en Windows
- Clientes ligeros basados en Linux de WYSE
- Thin Clients de WYSE basados en ThinOS
- Clientes ligeros basados en Ubuntu de 10Zig

Identificación de la causa raíz de los problemas de rendimiento lento

Caso 1

El usuario experimenta retrasos al acceder a Citrix Virtual Apps and Desktops.

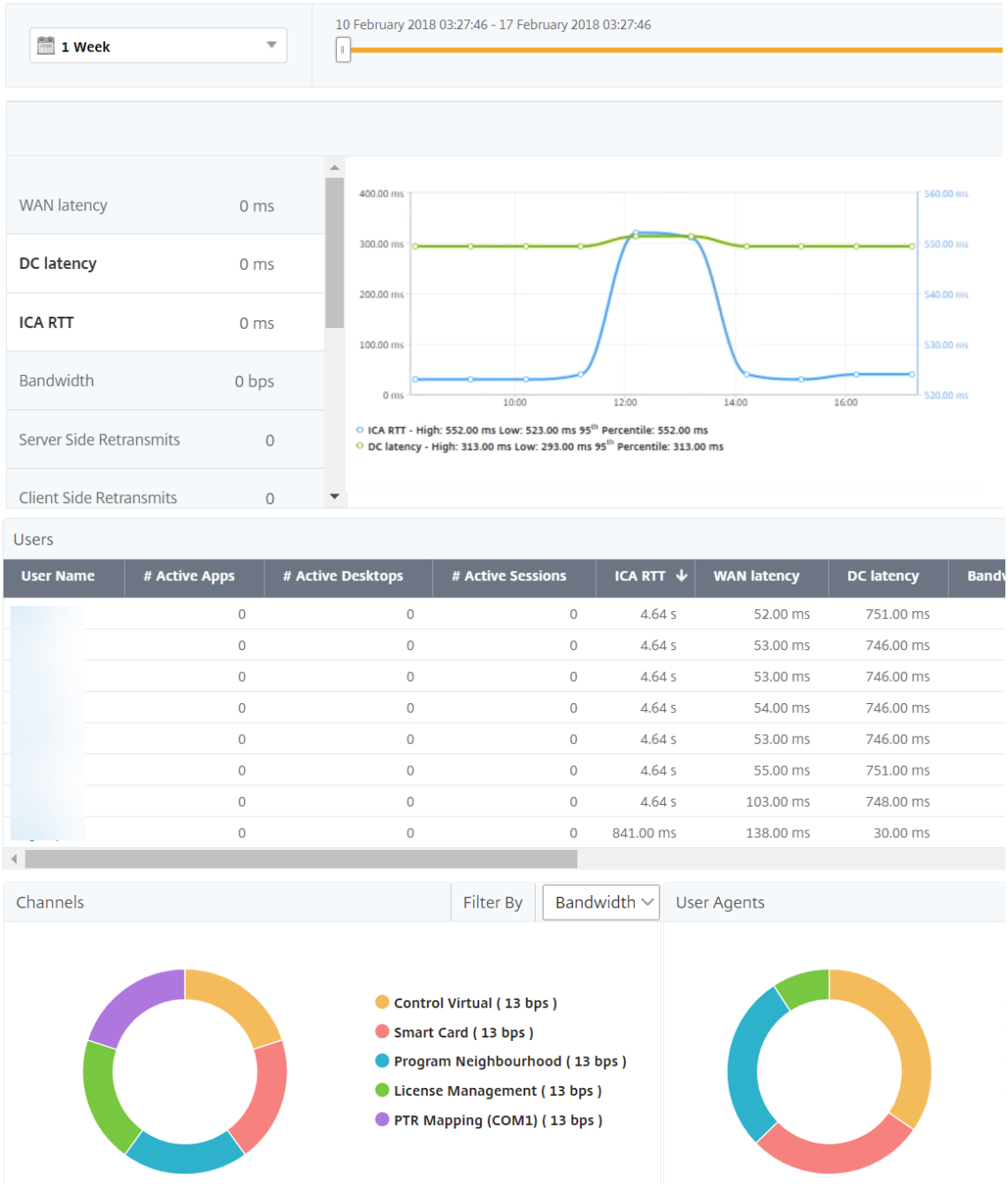
Los retrasos pueden deberse a la latencia en la red del servidor, retrasos en el tráfico ICA causados por la red del servidor o latencia en la red del cliente.

Para identificar la causa principal del problema, analice las siguientes métricas:

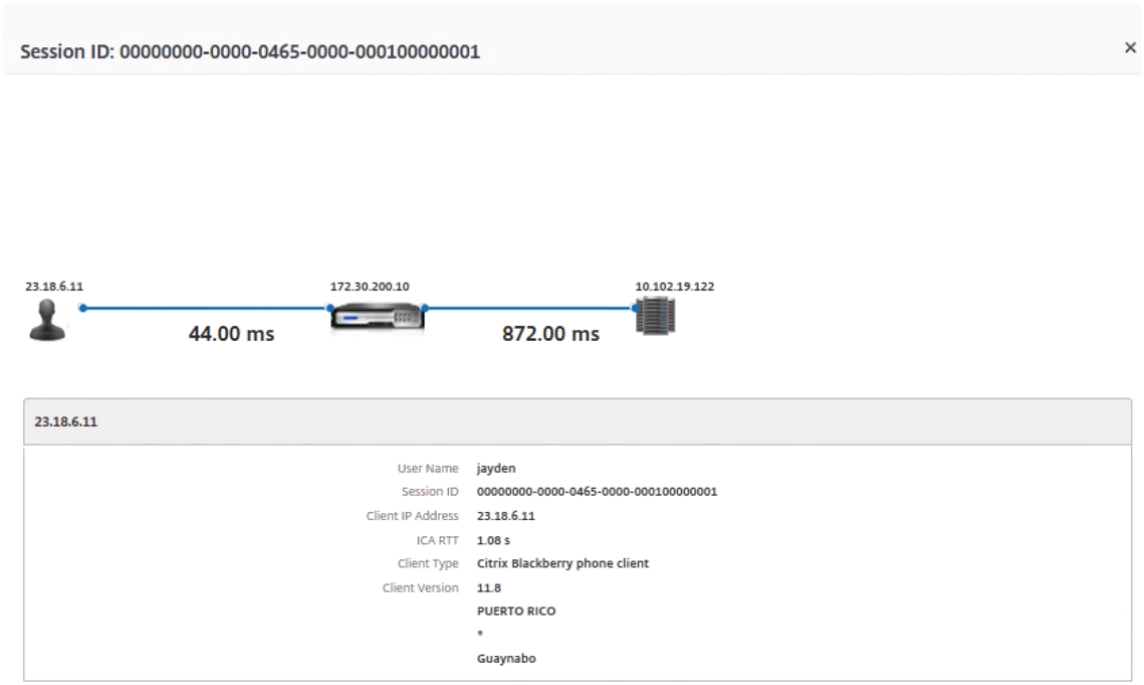
- Latencia de WAN
- Latencia de DC
- Demora de host

Para ver las métricas del cliente:

1. En la ficha**Analytics**, vaya a**HDX Insight** >**Usuarios**.
2. Desplázate hacia abajo y selecciona el nombre de usuario y selecciona el período de la lista. El período puede ser de un día, una semana, un mes o incluso puede personalizar el período del que quiere ver los datos.
3. El gráfico muestra los valores de latencia ICA RTT y DC del usuario para el período especificado como un gráfico.



4. En la tabla**Sesiones actuales**, coloque el mouse sobre el valor de**RTT**y observe los valores de retraso del host, latencia de DC y latencia de WAN.
5. En la tabla**Sesiones actuales**, haga clic en el símbolo del diagrama de saltos para mostrar información sobre la conexión entre el cliente y el servidor, incluidos los valores de latencia.



Resumen En este ejemplo, la **latencia de DC** es de 751 milisegundos, la **latencia de la WAN** es de 52 milisegundos y **los retrasos de host** son de 6 segundos. Esto indica que el usuario está experimentando un retraso debido a la latencia promedio causada por la red del servidor.

Caso 2

El usuario experimenta un retraso al iniciar una aplicación en Citrix Virtual Apps or Desktops

El retraso puede deberse a la latencia en la red del servidor, retrasos de tráfico ICA causados por la red del servidor, latencia en la red del cliente o tiempo tardado en iniciar una aplicación.

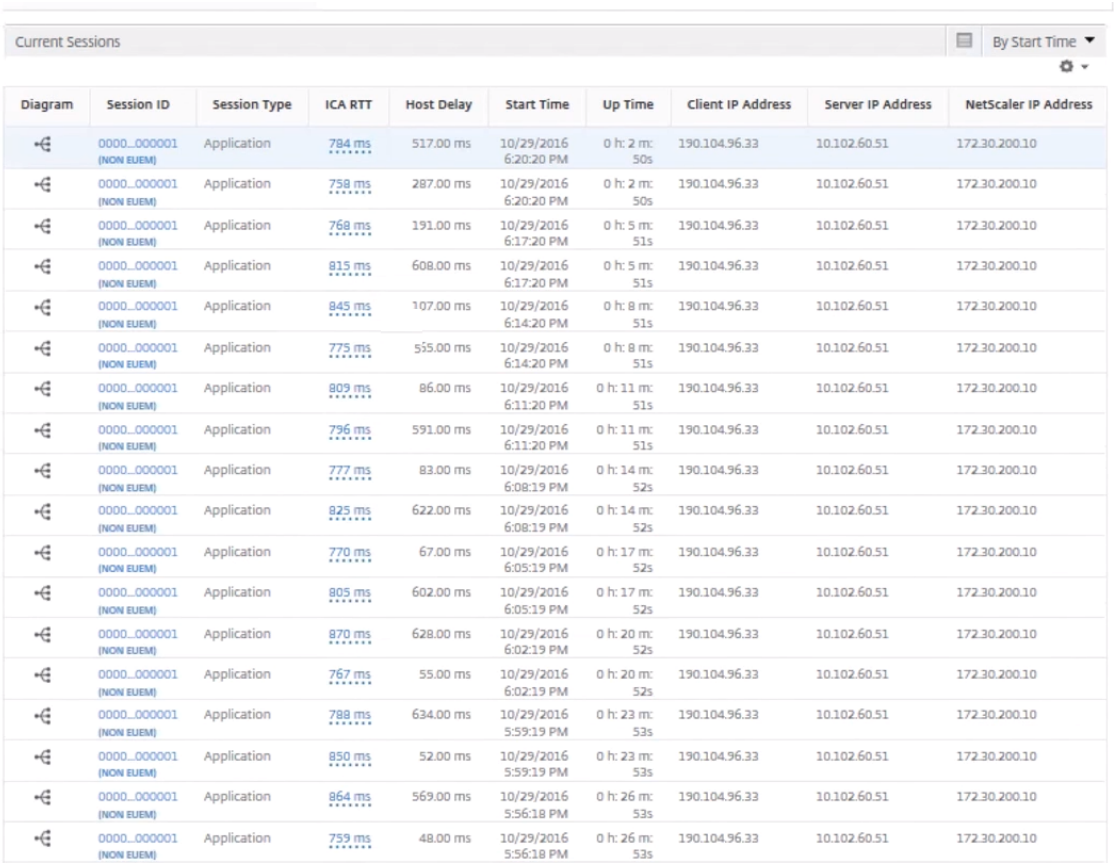
Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia de WAN
- Latencia de DC
- Demora del host

Para ver las métricas de usuario:

1. En la ficha **Análisis**, vaya a **HDX** Insight **Usuarios.
2. Desplácese hacia abajo y haga clic en el nombre de usuario.
3. En la representación gráfica, observe los valores de Latencia de WAN, Latencia de DC y RTT para la sesión en particular.

4. En la tabla **Sesiones actuales**, tenga en cuenta que el retraso del host es alto.



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

Resumen En este ejemplo, la**latencia de DC**es de 1 milisegundo, la**latencia de la WAN** es de 12 milisegundos, pero el**retraso del host** es de 517 milisegundos. RTT alto con latencias de DC y WAN bajas indica un error de aplicación en el servidor host.

> **Nota :**HDX Insight también muestra métricas de usuario adicionales, como la fluctuación de la WAN y las retransmisiones del lado del servidor, si utiliza Citrix ADM que ejecuta el software 11.1, compilación 51.21 o posterior. Para ver estas métricas, vaya a **Analytics** > **HDX Insight** > **Usuarios** y seleccione un nombre de usuario. Las métricas de usuario aparecen en la tabla junto al gráfico.

Geomapas para HDX Insight

La funcionalidad de geomapas de Citrix ADM muestra el uso de aplicaciones en diferentes ubicaciones geográficas en un mapa. Los administradores pueden usar esta información para comprender las tendencias en el uso de las aplicaciones en diversas ubicaciones geográficas.

Puede configurar Citrix ADM para que muestre los geomapas de una ubicación geográfica o LAN determinada especificando el rango de IP privadas (direcciones IP de inicio y final) de la ubicación.

También puede ver los detalles históricos y activos de los usuarios desde los mapas de ubicación geográfica en HDX Insight. Vaya a **Analytics** > **HDX**Insight y, en la sección Mundo del mapa, haga clic en el país o la región de los que quiere ver los detalles. Puede profundizar más para ver la información por ciudad y estado.

Para configurar una geomapa para centros de datos:

En la ficha **Analytics**, vaya a **Configuración** > **Bloques de IP** para configurar geometrías para una ubicación concreta.

Caso de uso

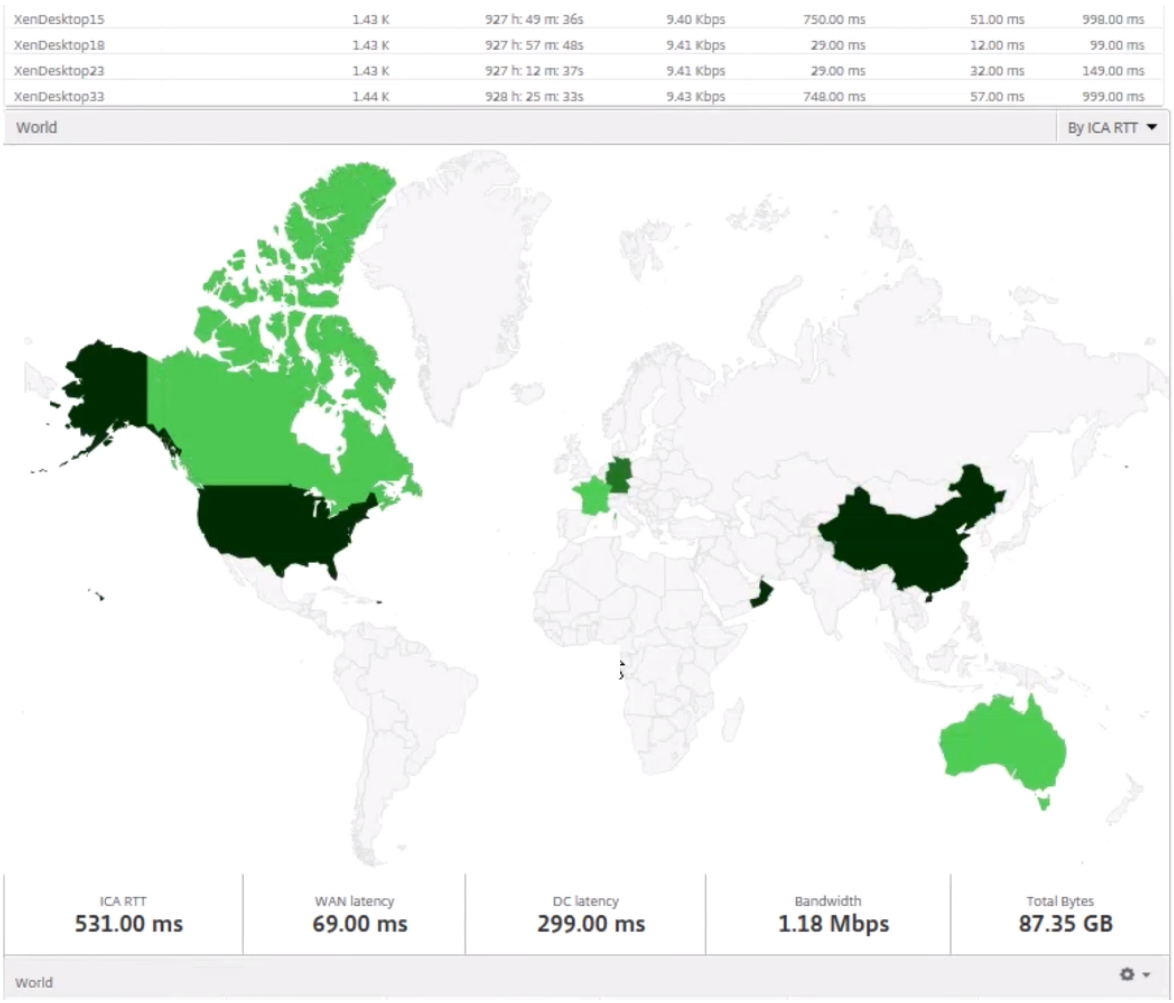
Considere un caso en el que la organización ABC tiene 2 sucursales, una en Santa Clara y la otra en India.

Los usuarios de Santa Clara utilizan el dispositivo Citrix Gateway en SClara.x.com para acceder al tráfico VPN. Los usuarios indios utilizan el dispositivo Citrix Gateway en India.x.com para acceder al tráfico de VPN.

Durante un intervalo de tiempo determinado, por ejemplo, de 10 a. m. a 5 p. m., los usuarios de Santa Clara se conectan a SClara.x.com para acceder al tráfico de VPN. La mayoría de los usuarios acceden

a la misma puerta de Citrix Gateway, lo que provoca un retraso en la conexión a la VPN, por lo que algunos usuarios se conectan a India.x.com en lugar de a SClara.x.com.

Un administrador de Citrix ADC que analice el tráfico puede usar la funcionalidad geomapa para mostrar el tráfico en la oficina de Santa Clara. El mapa muestra que el tiempo de respuesta en la oficina de Santa Clara es muy alto, porque la oficina de Santa Clara solo tiene un dispositivo Citrix Gateway a través del cual los usuarios pueden acceder al tráfico de VPN. Por lo tanto, es posible que el administrador decida instalar otro Citrix Gateway, de modo que los usuarios dispongan de dos dispositivos Citrix Gateway locales a través de los cuales acceder a la VPN.



Limitaciones

Si las instancias de Citrix ADC tienen una licencia empresarial, los umbrales establecidos en Citrix ADM para HDX Insight no se activarán, ya que los datos analíticos se recopilan durante solo 1 hora.

Habilitar la recopilación de datos de HDX Insight

January 30, 2024

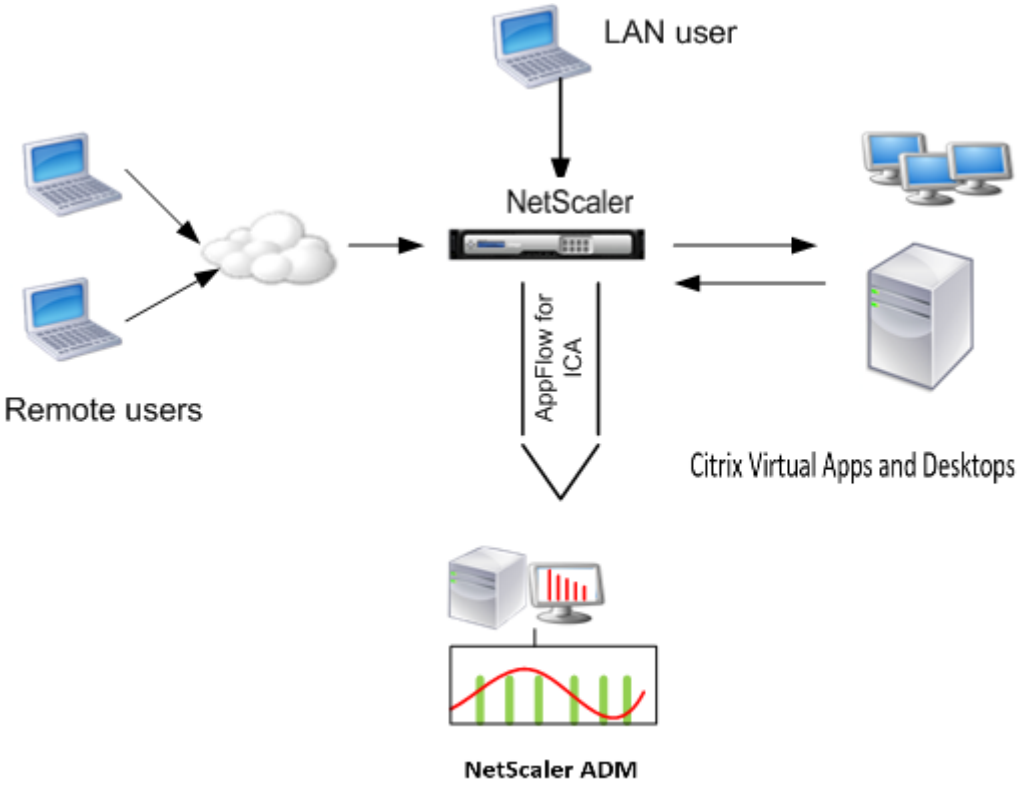
HDX Insight permite a TI ofrecer una experiencia de usuario excepcional al proporcionar una visibilidad end-to-end sin precedentes del tráfico ICA que pasa a través de las instancias Citrix ADC o los dispositivos Citrix SD-WAN, y forma parte de Citrix Application Delivery Management (ADM) Analytics. HDX Insight ofrece capacidades potentes y convincentes de inteligencia empresarial y análisis de fallos para la red, los escritorios virtuales, las aplicaciones y la estructura de aplicaciones. HDX Insight puede analizar al instante los problemas de los usuarios, recopilar datos sobre las conexiones de escritorio virtual y generar registros de AppFlow y presentarlos como informes visuales.

La configuración para habilitar la recopilación de datos en Citrix ADC difiere según la posición del dispositivo en la topología de implementación.

Habilitar la recopilación de datos para monitorear los dispositivos de Citrix ADC implementados en modo de usuario LAN

Los usuarios externos que acceden a las aplicaciones de Citrix Virtual Apps and Desktops deben autenticarse en Citrix Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a Citrix Gateway. Además, en una implementación de modo transparente, el administrador debe aplicar manualmente las directivas de redirección para que las solicitudes se redirijan al dispositivo Citrix ADC.

Para superar estos desafíos y para que los usuarios de LAN se conecten directamente a aplicaciones de Citrix Virtual Apps and Desktops, puede implementar el dispositivo Citrix ADC en modo de usuario de LAN configurando un servidor virtual de redirección de caché, que actúa como proxy SOCKS en el dispositivo Citrix Gateway.



> **Nota** Citrix ADM y el dispositivo Citrix Gateway residen en la misma subred.

Para supervisar los dispositivos Citrix ADC implementados en este modo, primero agregue el dispositivo Citrix ADC al inventario de NetScaler Insight, habilite AppFlow y, a continuación, consulte los informes en el panel.

Después de agregar el dispositivo Citrix ADC al inventario de Citrix ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - En una instancia de ADC, puede ir a **Sistema** > **AppFlow****Collectors para comprobar si el recopilador (es decir, Citrix ADM) está activo o no. La instancia Citrix ADC envía registros AppFlow a Citrix ADM mediante NSIP. Sin embargo, la instancia usa su SNIP para verificar la conectividad con Citrix ADM. Por lo tanto, asegúrese de que el SNIP esté configurado en la instancia.
> - No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo de usuario de LAN mediante la utilidad de configuración de Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte lareferencia de comandos.
> - Para obtener información sobre las expresiones de directiva, consulteDirectivas y expre-

siones.

Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Agregue un servidor virtual de redirección de caché de proxy de reenvío con la IP y el puerto proxy, y especifique el tipo de servicio como HDX.

   add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType <cachetype>] [- cltTimeout <secs>]

   Ejemplo

   ```
   add cr vserver cr1 HDX 10.12.2.2 443 –cacheType FORWARD –
      cltTimeout 180
   <!--NeedCopy-->
   ```

   Nota Si accede a la red LAN mediante un dispositivo Citrix Gateway, agregue una acción que aplique una directiva que coincida con el tráfico VPN.

   add vpn trafficAction <name> <qual> [-HDX (ON u OFF)]

   add vpn trafficPolicy <name> <rule> <action>

   Ejemplo

   ```
   add vpn trafficAction act1 tcp -HDX ON

   add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
   <!--NeedCopy-->
   ```

3. Agregue Citrix ADM como recopilador de flujo de aplicaciones en el dispositivo Citrix ADC.

   add appflow collector <name> **-IPAddress** <ip_addr>

   Ejemplo :

   ```
   add appflow collector MyInsight -IPAddress 192.168.1.101
   <!--NeedCopy-->
   ```

4. Cree una acción de flujo de aplicaciones y asocie el recopilador con la acción.

   add appflow action <name> **-collectors** <string> …

   Ejemplo :

   ```
   add appflow action act -collectors MyInsight
   <!--NeedCopy-->
   ```


5. Cree una directiva de flujo de aplicaciones para especificar la regla para generar el tráfico.

   add appflow policy <policyname> <rule> <action>

   Ejemplo :

   ```
   add appflow policy pol true act
   <!--NeedCopy-->
   ```

6. Enlazar la directiva de flujo de aplicaciones a un punto de enlace global.

   bind appflow global <policyname> <priority> **-type** <type>

   Ejemplo :

   ```
   bind appflow global pol 1 -type ICA_REQ_DEFAULT
   <!--NeedCopy-->
   ```

   > **Nota:** El valor del tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para poder aplicarse al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para Appflow en 60 segundos.

   set appflow param -flowRecordInterval 60

   Ejemplo :

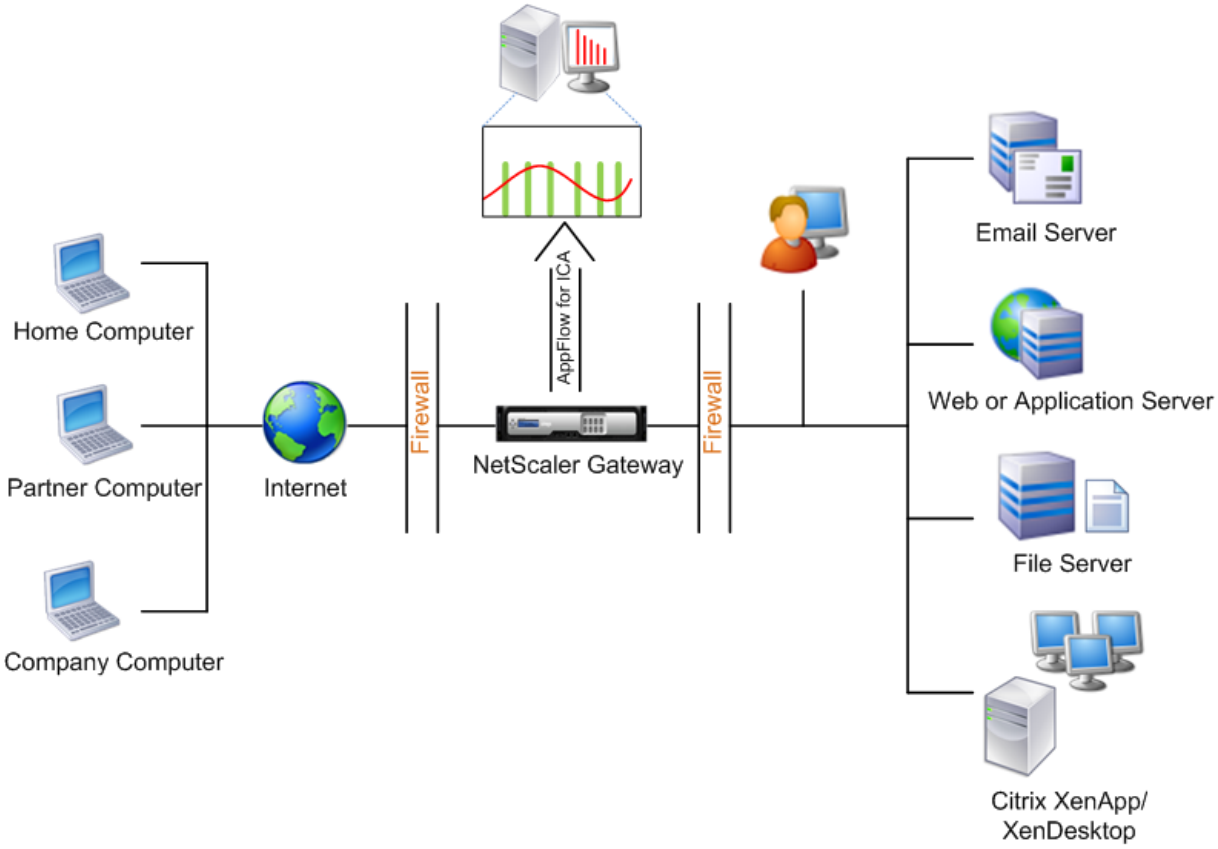
   ```
   set appflow param -flowRecordInterval 60
   <!--NeedCopy-->
   ```

8. Guarde la configuración. Tipo: `save ns config`

Habilitar la recopilación de datos para los dispositivos Citrix Gateway implementados en modo de salto único

Cuando implementa Citrix Gateway en modo de salto único, se encuentra en el borde de la red. La instancia de Gateway proporciona conexiones ICA de proxy a la infraestructura de entrega de escritorio. El salto único es la implementación más simple y común. El modo de salto único proporciona seguridad si un usuario externo intenta acceder a la red interna de una organización.
En el modo de salto único, los usuarios acceden a los dispositivos Citrix ADC a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo Citrix Gateway al inventario de Citrix Application Delivery Management (ADM) y habilitar AppFlow en ADM.



Para habilitar la función AppFlow desde Citrix ADM:

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC que quiere habilitar el análisis.
4. En el menú desplegable **Seleccionar acción**, seleccione **Configurar Analytics**.
5. Seleccione los servidores virtuales VPN y haga clic en **Habilitar AppFlow**.
6. En el campo **Habilitar AppFlow**, escriba **true** y seleccione **ICA**.
7. Haga clic en **Aceptar**.

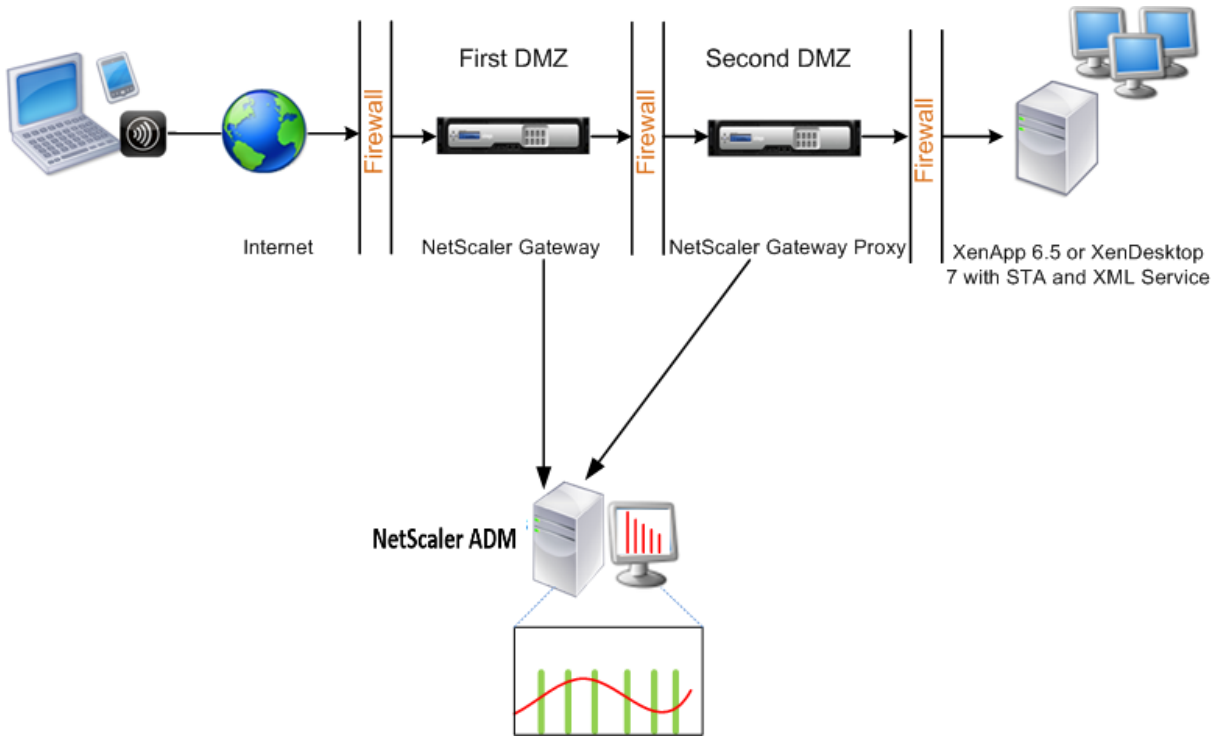
> Nota: Los siguientes comandos se ejecutan en segundo plano cuando se habilita AppFlow en modo de salto único. Estos comandos se especifican explícitamente aquí para solucionar problemas.
>
> - add appflow collector <name> -IPAddress <ip_addr>
> - add appflow action <name> -collectors <string>
> - set appflow param -flowRecordInterval <secs>
> - disable ns feature AppFlow

- enable ns feature AppFlow
- add appflow policy <name> <rule> <expression>
- set appflow policy <name> -rule <expression>
- bind vpn vserver <vsname> -policy <string> -type <type> -priority <positive_integer>
- set vpn vserver <name> -appflowLog ENABLED
- save ns config

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el Citrix ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual de EUEM no está habilitado, los datos restantes de HDX Insight se mostrarán en Citrix ADM.

Habilitación de la recopilación de datos para los dispositivos Citrix Gateway implementados en modo de doble salto

El modo de salto doble de Citrix Gateway proporciona protección adicional a la red interna de una organización porque un atacante necesitaría penetrar varias zonas de seguridad o zonas desmilitarizadas (DMZ) para llegar a los servidores de la red segura. Si quiere analizar el número de saltos (dispositivos Citrix Gateway) a través de los cuales pasan las conexiones ICA, así como los detalles sobre la latencia en cada conexión TCP y cómo se compara con la latencia total de ICA percibida por el cliente, debe instalar Citrix ADM para que los dispositivos Citrix Gateway reportar estas estadísticas vitales.



Citrix Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguri-

dad de una VPN SSL. Citrix Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

Citrix Gateway en la segunda DMZ sirve como dispositivo proxy de Citrix Gateway. Este Citrix Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores.

El Citrix ADM se puede implementar en la subred que pertenece al dispositivo Citrix Gateway en la primera DMZ o en la subred que pertenece a la segunda DMZ del dispositivo Citrix Gateway. En la imagen de arriba, Citrix ADM y Citrix Gateway de la primera DMZ se implementan en la misma subred.

En modo de salto doble, Citrix ADM recopila los registros TCP de un dispositivo y los registros ICA del otro dispositivo. Tras agregar los dispositivos Citrix Gateway al inventario de Citrix ADM y habilitar la recopilación de datos, cada uno de los dispositivos exporta los informes realizando un seguimiento del recuento de saltos y del identificador de la cadena de conexiones.

Para que Citrix ADM identifique qué dispositivo está exportando registros, cada dispositivo se especifica con un recuento de saltos y cada conexión se especifica con un ID de cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos Citrix Gateway a través de los cuales fluye el tráfico desde un cliente a los servidores. El ID de cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos Citrix Gateway y generar los informes.

Para supervisar los dispositivos Citrix Gateway implementados en este modo, primero debe agregar Citrix Gateway al inventario de Citrix ADM, habilitar AppFlow en Citrix ADM y, a continuación, ver los informes en el panel de Citrix ADM.

Habilitar la recopilación de datos en Citrix ADM

Si habilita Citrix ADM para comenzar a recopilar los detalles de ICA de ambos dispositivos, los detalles recopilados serán redundantes. Es decir, tanto los dispositivos informan de las mismas métricas. Para superar esta situación, debe habilitar AppFlow para ICA en uno de los primeros dispositivos Citrix Gateway y, a continuación, habilitar AppFlow para TCP en el segundo dispositivo. Al hacerlo, uno de los dispositivos exporta registros ICA AppFlow y el otro dispositivo exporta registros TCP AppFlow. Esto también ahorra tiempo de procesamiento al analizar el tráfico ICA.

Para habilitar la función AppFlow desde Citrix ADM:

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC que quiere habilitar el análisis.

4. En el menú desplegable **Seleccionar acción**, seleccione **Configurar Analytics**.
5. Seleccione los servidores virtuales VPN y haga clic en **Habilitar AppFlow**.
6. En el campo **Habilitar AppFlow**, escriba **true** y seleccione **ICA/TCP** para tráfico ICA y tráfico TCP respectivamente.

   > **Nota** Si el registro de AppFlow no está habilitado para los servicios o grupos de servicios respectivos del dispositivo Citrix ADC, el panel de control de Citrix ADM no muestra los registros, incluso si la columna Insight muestra Habilitado.

7. Haga clic en **Aceptar**.

Configuración de dispositivos Citrix Gateway para exportar datos

Después de instalar los dispositivos Citrix Gateway, debe configurar las siguientes opciones en los dispositivos Citrix Gateway para exportar los informes a Citrix ADM:

- Configure los servidores virtuales de los dispositivos Citrix Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ.
- Habilite el salto doble en Citrix Gateway en la segunda DMZ.
- Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.
- Habilite uno de los dispositivos Citrix Gateway para exportar registros ICA
- Habilite el otro dispositivo Citrix Gateway para exportar registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

Configuración de Citrix Gateway mediante la interfaz de línea de comandos:

1. Configure el servidor virtual de Citrix Gateway en la primera DMZ para comunicarse con el servidor virtual de Citrix Gateway en la segunda DMZ.

   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [**-secure**(ON u OFF)] [**-imgGifToPng**] …

   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON

2. Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ. Ejecute el siguiente comando en Citrix Gateway en la primera DMZ:

   bind vpn vserver <name> **-nextHopServer** <name>

   bind vpn vserver vs1 -nextHopServer nh1

3. Habilite el salto doble y AppFlow en Citrix Gateway en la segunda DMZ.

   set vpn vserver <name> [**- doubleHop** (ENABLED or DISABLED)] [**- appflowLog** (ENABLED or DISABLED)]

   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED

4. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

   set vpn vserver<name> [**-authentication** (ON or OFF)]

   set vpn vserver vs -authentication OFF

5. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

   vincular vpn vserver<type\>\<name\>\[**-policy\ -priority**<string**] [**-type**<positive_integer>\\]

   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type OTHERTCP_REQUEST

6. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

   bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA_REQUEST

7. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway:

   set appFlow param [**-connectionChaining** (ENABLED or DISABLED)]

   set appflow param -connectionChaining ENABLED

Configuración de Citrix Gateway mediante la Utilidad de configuración:

1. Configure Citrix Gateway en la primera DMZ para comunicarse con Citrix Gateway en la segunda DMZ y enlazar Citrix Gateway en la segunda DMZ a Citrix Gateway en la primera DMZ.

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzadas, expanda**Aplicaciones publicadas**.

   c) Haga clic en**Servidor de salto siguiente** y vincule un servidor de salto siguiente al segundo dispositivo Citrix Gateway.

2. Habilite el salto doble en Citrix Gateway en la segunda DMZ.

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.

   c) Expanda **Más**, seleccione **Doble salto** y haga clic en **Aceptar**.

3. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

a) En la ficha **Configuración**, expanda **NetScaler Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.

c) Expanda **Más** y desmarque **Habilitar autenticación**.

4. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzadas, expanda Directivas.

c) Haga clic en el icono + y, en la lista desplegable**Elegir directiva**, seleccione**AppFlow** y, en la lista desplegable **Elegir tipo**, seleccione**Otra solicitud de TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

5. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

a) En la ficha **Configuración**, expanda **NetScaler Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Avanzado**, expanda**Directivas**.

c) **Haga clic en el icono + y, en la lista desplegable**Elegir directiva**, seleccione** AppFlow**y, en la lista desplegable Elegir tipo , seleccione Otra solicitud de TCP.**

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

6. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

a) En la ficha **Configuración**, vaya a **Sistema** > **Appflow**.

b) En el panel derecho, en el grupo**Configuración**, haga clic en**Cambiar la configuración de Appflow**.

c) Seleccione **Conexión encadenamiento** y haga clic en **Aceptar**.

7. Configure Citrix Gateway en la primera DMZ para comunicarse con Citrix Gateway en la segunda DMZ y enlazar Citrix Gateway en la segunda DMZ a Citrix Gateway en la primera DMZ.

a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

b) En el panel derecho, haga doble clic en el servidor virtual y, en el**grupo Avanzado** , expanda**Aplicaciones publicadas**.

c) Haga clic en**Servidor de siguiente salto**y vincule un servidor de siguiente salto al segundo dispositivo Citrix Gateway.

8. Habilite el salto doble en Citrix Gateway en la segunda DMZ.

a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo **Configuración básica**, haga clic en el icono de edición.

c) Amplíe Más , seleccione **Double Hop y** haga clic en Aceptar .

9. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

a) En la pestaña Configuración , expanda Citrix Gateway y haga clic en **Servidores virtuales** .

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.

c) Expanda **Más** y desmarque **Habilitar autenticación**.

10. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado , expanda**Directivas**.

c) Haga clic en el icono**+** y, en la lista desplegable Elegir directiva , seleccione**AppFlow** y, en la lista desplegable **Elegir tipo**, seleccione**Otra solicitud de TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

11. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA.

a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda **Políticas** .

c) Haga clic en el icono**+** y, en la lista desplegable**Elegir directiva** , seleccione**AppFlow** y, en la lista desplegable **Elegir tipo** , seleccione**Otra solicitud de TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

12. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

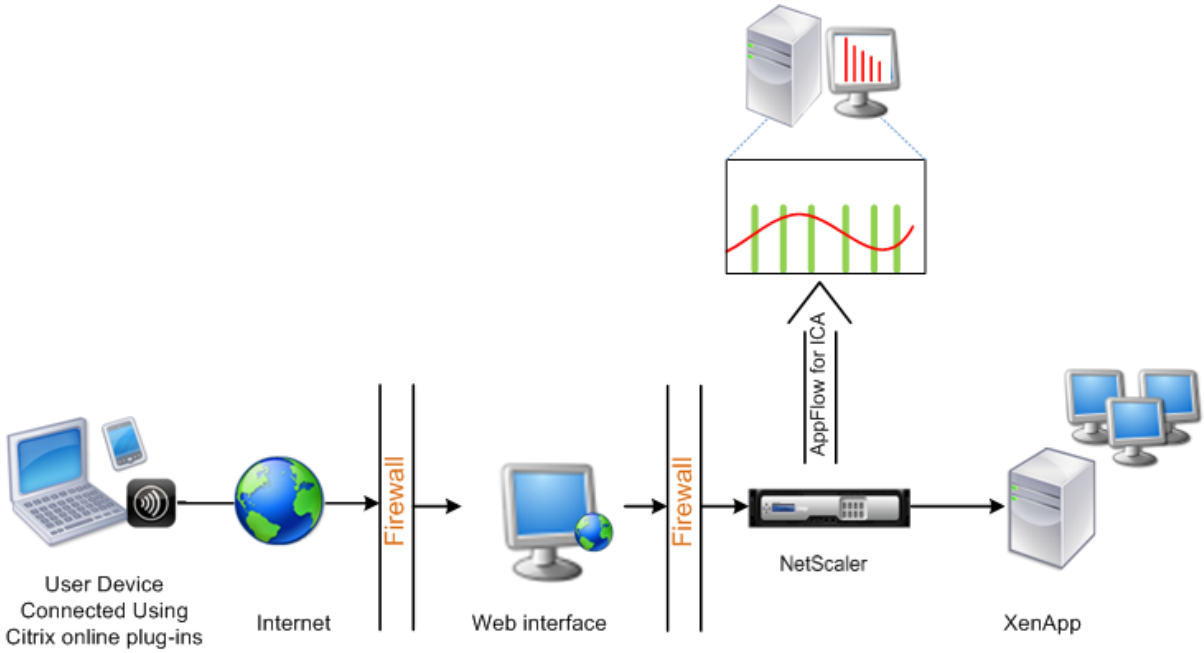
Habilitar la recopilación de datos para supervisar los dispositivos de Citrix ADC implementados en modo transparente

Cuando un Citrix ADC se implementa en modo transparente, los clientes pueden acceder a los servidores directamente, sin que intervenga ningún servidor virtual. Si un dispositivo Citrix ADC se implementa en modo transparente en un entorno de Citrix Virtual Apps and Desktop, el tráfico ICA no se transmite a través de una VPN.

Después de agregar Citrix ADC al inventario Citrix ADM, debe habilitar AppFlow para la recopilación de datos. Habilitar la recopilación de datos depende del dispositivo y del modo. En ese caso, debe agregar Citrix ADM como recopilador de AppFlow en cada dispositivo Citrix ADC y debe configurar una directiva de Appflow para recopilar todo el tráfico ICA que fluye a través del dispositivo o uno específico.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo transparente mediante la utilidad de configuración de Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte lareferencia de comandos.
> - Para obtener información sobre las expresiones de directiva, consulteDirectivas y expresiones.

La siguiente ilustración muestra la implementación en red de un Citrix ADM cuando un Citrix ADC se implementa en modo transparente:



Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Especifique los puertos ICA en los que el dispositivo Citrix ADC escucha el tráfico.

```
set ns param --icaPorts <port>...
<!--NeedCopy-->
```

Ejemplo:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Nota**
>
> - Puede especificar hasta 10 puertos con este comando.
> - El número de puerto predeterminado es 2598. Puede modificar el número de puerto según sea necesario.

3. Agregue NetScaler Insight Center como recopilador de flujo de aplicaciones en el dispositivo Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```


Ejemplo:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Nota** Para ver los recopiladores de flujo de aplicaciones configurados en el dispositivo Citrix ADC, utilice el comando**show appflow collector**.

4. Cree una acción de flujo de aplicaciones y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Ejemplo:

add appflow action act -collectors MyInsight

5. Cree una directiva de flujo de aplicaciones para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlazar la directiva de flujo de aplicaciones a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Ejemplo:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Nota :**El valor del**tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para poder aplicarse al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para Appflow en 60 segundos.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Ejemplo:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

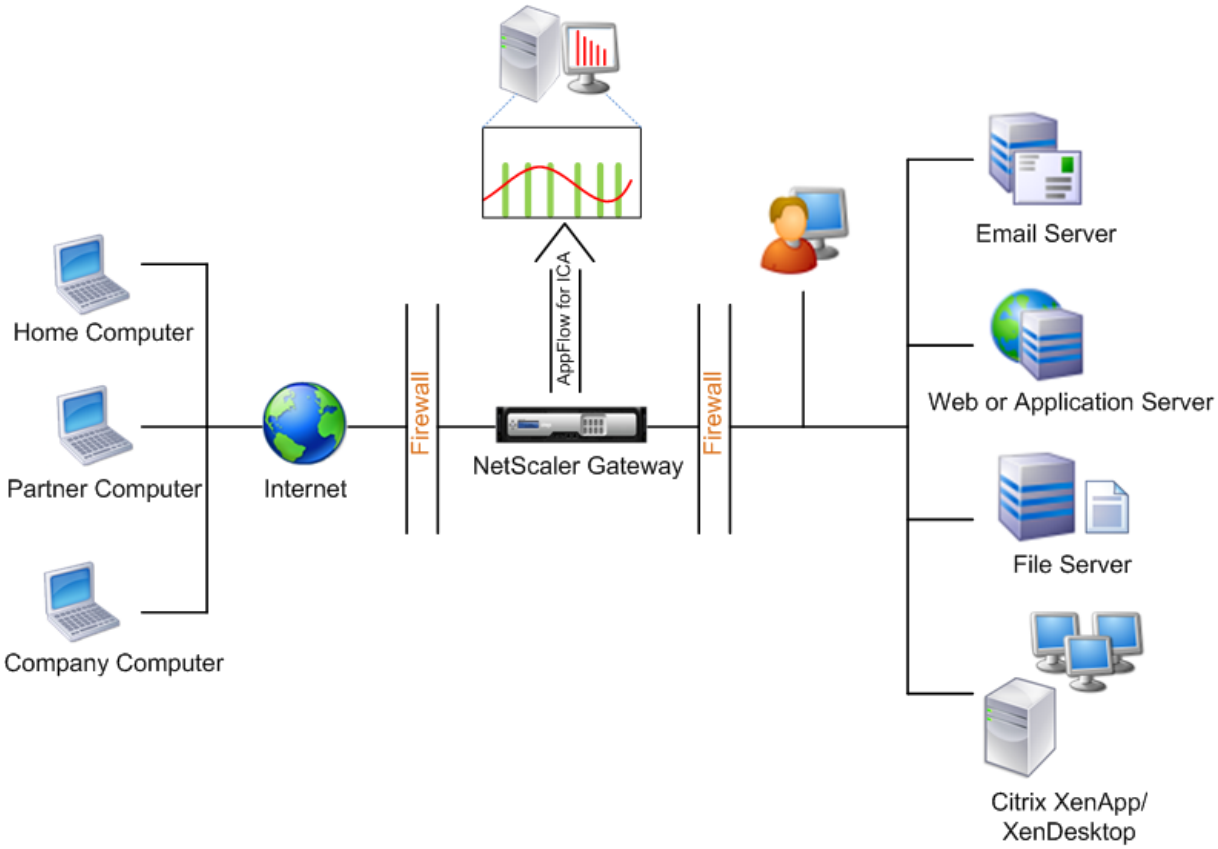
8. Guarde la configuración. Tipo: `save ns config`

Habilitar la recopilación de datos para dispositivos Citrix Gateway implementados en modo de salto único

January 30, 2024

Cuando implementa Citrix Gateway en modo de salto único, se encuentra en el borde de la red. La instancia de Gateway proporciona conexiones ICA de proxy a la infraestructura de entrega de escritorio. El salto único es la implementación más simple y común. El modo de salto único proporciona seguridad si un usuario externo intenta acceder a la red interna de una organización.
En el modo de salto único, los usuarios acceden a los dispositivos Citrix ADC a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo Citrix Gateway al inventario de Citrix Application Delivery Management (ADM) y habilitar AppFlow en ADM.



Para habilitar la función AppFlow desde ADM:

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.

3. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia de NetScaler en la que desea habilitar el análisis.
4. En el menú desplegable **Acción**, seleccione **Activar/Desactivar información**.
5. Seleccione los **servidores virtuales VPN** y haga clic en **Habilitar AppFlow** .
6. En el campo **Habilitar AppFlow**, escriba **true** y seleccione **ICA**.
7. Haga clic en **Aceptar**.

> **Nota:** Los siguientes comandos se ejecutan en segundo plano cuando se habilita AppFlow en el modo de salto único. Estos comandos se especifican explícitamente aquí para solucionar problemas.
>
> - add appflow collector <name> -IPAddress <ip_addr>
> - add appflow action <name> -collectors <string>
> - set appflow param -flowRecordInterval <secs>
> - disable ns feature AppFlow
> - enable ns feature AppFlow
> - add appflow policy <name> <rule> <expression>
> - set appflow policy <name> -rule <expression>
> - bind vpn vserver <vsname> -policy <string> -type <type> >-priority <positive_integer>
> - set vpn vserver <name> -appflowLog ENABLED
> - save ns config

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el Citrix ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual de EUEM no está habilitado, los datos restantes de HDX Insight se mostrarán en Citrix ADM.

Habilitar la recopilación de datos para supervisar los dispositivos de NetScaler ADC implementados en modo transparente

January 30, 2024

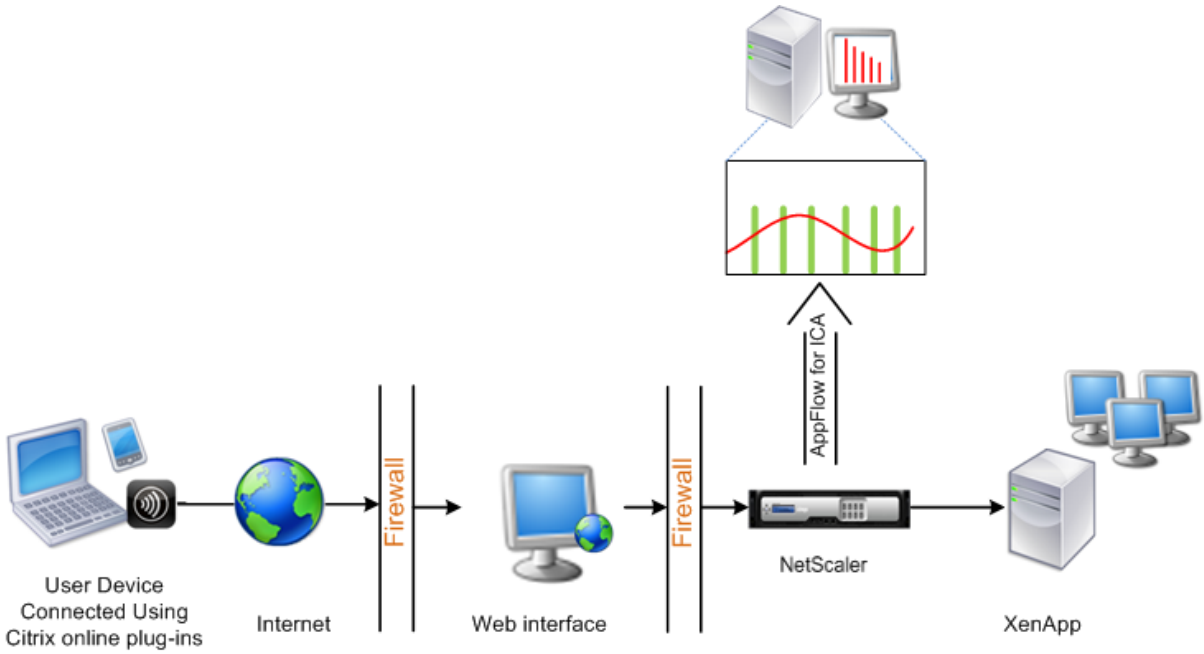
Cuando se implementa un NetScaler ADM en modo transparente, los clientes pueden acceder a los servidores directamente, sin la intervención de un servidor virtual. Si un dispositivo NetScaler se implementa en modo transparente en un entorno de Citrix Virtual Apps and Desktops, el tráfico ICA no se transmite a través de una VPN.

Después de agregar Citrix ADC al inventario Citrix ADM, debe habilitar AppFlow para la recopilación de datos. Habilitar la recopilación de datos depende del dispositivo y del modo. En ese caso, debe

agregar Citrix ADM como recopilador de AppFlow en cada dispositivo NetScaler y debe configurar una directiva de Appflow para recopilar todo el tráfico ICA que fluye a través del dispositivo o uno específico.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un NetScaler ADM implementado en modo transparente mediante la utilidad de configuración Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte lareferencia de comandos.
> - Para obtener información sobre las expresiones de directiva, consulteDirectivas y expresiones.

En la siguiente figura se muestra la implementación en red de un Citrix ADM cuando se implementa un en modo transparente:



Para configurar la recopilación de datos en un dispositivo NetScaler mediante la interfaz de línea de comandos:

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Especifique los puertos ICA en los que el dispositivo NetScaler escucha el tráfico.

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```


Ejemplo:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Nota**
>
> - Puede especificar hasta 10 puertos con este comando.
> - El número de puerto predeterminado es 2598. Puede modificar el número de puerto según sea necesario.

3. Agregue NetScaler Insight Center como recopilador de flujo de aplicaciones en el dispositivo NetScaler.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Nota** Para ver los recopiladores de flujo de aplicaciones configurados en el dispositivo NetScaler, utilice**el** comando show appflow collector.

4. Cree una acción de flujo de aplicaciones y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Ejemplo:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Cree una directiva de flujo de aplicaciones para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlazar la directiva de flujo de aplicaciones a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```


Ejemplo:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

Nota : El valor del**tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para poder aplicarse al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para Appflow en 60 segundos.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Guarde la configuración.

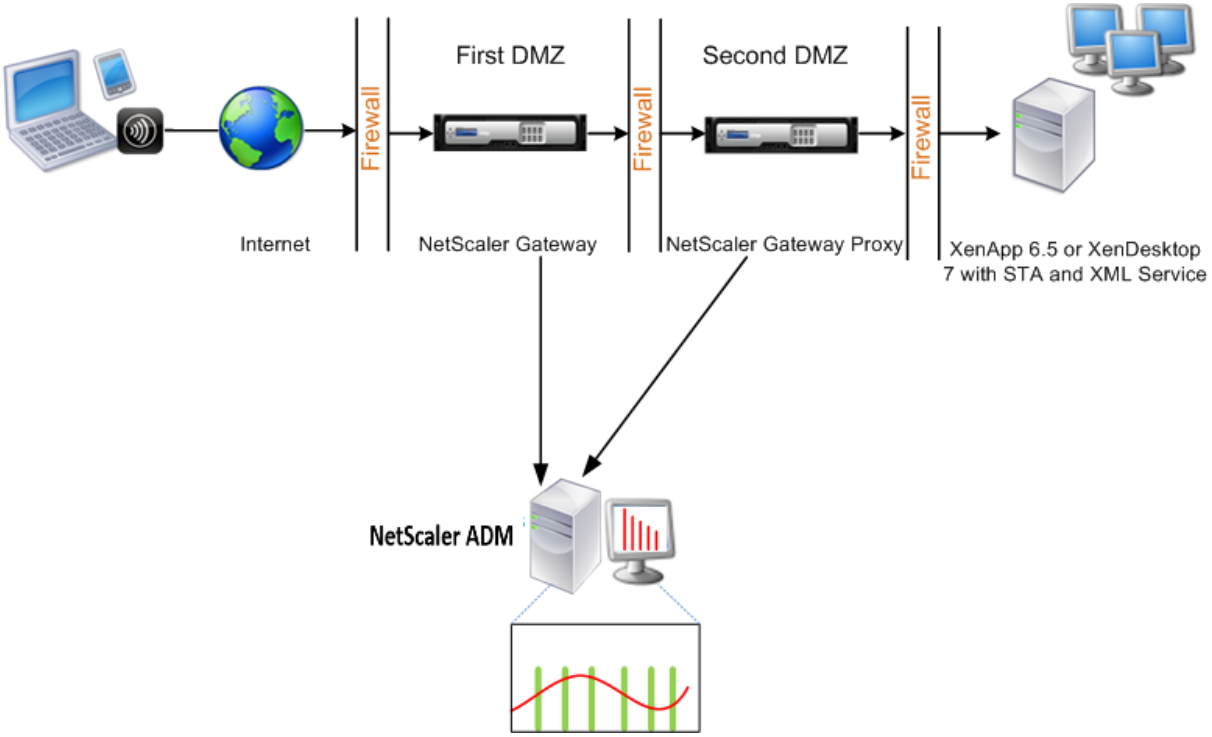
```
save ns config
<!--NeedCopy-->
```

Habilitar la recopilación de datos para dispositivos Citrix Gateway implementados en modo de salto doble

January 30, 2024

El modo de salto doble de NetScaler Gateway proporciona protección adicional a la red interna de una organización porque un atacante necesitaría penetrar varias zonas de seguridad o zonas desmilitarizadas (DMZ) para llegar a los servidores de la red segura. Si quiere analizar el número de saltos (dispositivos Citrix Gateway) a través de los cuales pasan las conexiones ICA, así como los detalles sobre la latencia en cada conexión TCP y cómo se compara con la latencia total de ICA percibida por el cliente, debe instalar Citrix ADM para que los dispositivos Citrix Gateway reportar estas estadísticas vitales.

Figura 3 . Citrix ADM implementado en modo de salto doble



Citrix Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Citrix Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

Citrix Gateway en la segunda DMZ sirve como dispositivo proxy de Citrix Gateway. Este Citrix Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores.

El Citrix ADM se puede implementar en la subred que pertenece al dispositivo Citrix Gateway en la primera DMZ o en la subred que pertenece a la segunda DMZ del dispositivo Citrix Gateway. En la imagen de arriba, Citrix ADM y Citrix Gateway de la primera DMZ se implementan en la misma subred.

En modo de salto doble, Citrix ADM recopila los registros TCP de un dispositivo y los registros ICA del otro dispositivo. Tras agregar los dispositivos Citrix Gateway al inventario de Citrix ADM y habilitar la recopilación de datos, cada uno de los dispositivos exporta los informes realizando un seguimiento del recuento de saltos y del identificador de la cadena de conexiones.

Para que Citrix ADM identifique qué dispositivo está exportando registros, cada dispositivo se especifica con un recuento de saltos y cada conexión se especifica con un ID de cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos Citrix Gateway a través de los cuales fluye el tráfico desde un cliente a los servidores. El ID de cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos Citrix Gateway y generar los informes.

Para supervisar los dispositivos Citrix Gateway implementados en este modo, primero debe agregar Citrix Gateway al inventario de Citrix ADM, habilitar AppFlow en Citrix ADM y, a continuación, ver los informes en el panel de Citrix ADM.

Habilitar la recopilación de datos en Citrix ADM

Si habilita Citrix ADM para comenzar a recopilar los detalles de ICA de ambos dispositivos, los detalles recopilados serán redundantes. Es decir, tanto los dispositivos informan de las mismas métricas. Para superar esta situación, debe habilitar AppFlow para TCP en uno de los primeros dispositivos Citrix Gateway y, a continuación, habilitar AppFlow para ICA en el segundo dispositivo. Al hacerlo, uno de los dispositivos exporta registros ICA AppFlow y el otro dispositivo exporta registros TCP AppFlow. Esto también ahorra tiempo de procesamiento al analizar el tráfico ICA.

Para habilitar la función AppFlow desde Citrix ADM:

1. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia de NetScaler en la que desea habilitar el análisis.
2. En el menú desplegable **Acción**, seleccione **Activar/Desactivar información**.
3. Seleccione los servidores virtuales VPN y haga clic en **Habilitar AppFlow**.
4. En el campo **Habilitar AppFlow**, escriba **true** y seleccione **ICA/TCP** para tráfico ICA y tráfico TCP respectivamente.

   > **Nota** Si el registro de AppFlow no está habilitado para los servicios o grupos de servicios respectivos en el dispositivo NetScaler, el panel de Citrix ADM no muestra los registros, incluso si la columna Insight muestra Habilitado.

5. Haga clic en **Aceptar**.

Configuración de dispositivos Citrix Gateway para exportar datos

Después de instalar los dispositivos Citrix Gateway, debe configurar las siguientes opciones en los dispositivos Citrix Gateway para exportar los informes a Citrix ADM:

- Configure los servidores virtuales de los dispositivos Citrix Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ.
- Habilite el salto doble en Citrix Gateway en la segunda DMZ.
- Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.
- Habilite uno de los dispositivos Citrix Gateway para exportar registros ICA

- Habilite el otro dispositivo Citrix Gateway para exportar registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

Configuración de Citrix Gateway mediante la interfaz de línea de comandos:

1. Configure el servidor virtual de Citrix Gateway en la primera DMZ para comunicarse con el servidor virtual de Citrix Gateway en la segunda DMZ.

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] ...

```
add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
<!--NeedCopy-->
```

2. Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ. Ejecute el siguiente comando en Citrix Gateway en la primera DMZ:

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. Habilite el salto doble y AppFlow en Citrix Gateway en la segunda DMZ.

---

set vpn vserver [**- doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED
<!--NeedCopy-->
```

4. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

---

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```


6. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
1 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
     ICA_REQUEST
2 <!--NeedCopy-->
```

7. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway:

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
1 set appflow param -connectionChaining ENABLED
2 <!--NeedCopy-->
```

Configuración de Citrix Gateway mediante la utilidad de configuración:

1. Configure Citrix Gateway en la primera DMZ para comunicarse con Citrix Gateway en la segunda DMZ y enlazar Citrix Gateway en la segunda DMZ a Citrix Gateway en la primera DMZ.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.
   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzadas, expanda**Aplicaciones publicadas**.
   c) Haga clic en **Servidor de salto siguiente**y enlace un servidor de salto siguiente al segundo dispositivo Citrix Gateway.
2. Habilite el salto doble en Citrix Gateway en la segunda DMZ.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.
   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.
   c) Expanda **Más**, seleccione **Doble salto** y haga clic en **Aceptar**.
3. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.
   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.
   c) Expanda **Más** y desmarque **Habilitar autenticación**.
4. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzadas, expanda Directivas.

c) Haga clic en el icono + y, en la lista**Elegir directiva**, seleccione**AppFlow**y, en la lista**Elegir tipo**, seleccione**Otra solicitud TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

5. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

a) En la ficha **Configuración**, expanda **NetScaler Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Avanzadas**, expanda**Directivas**.

c) Haga clic en el icono + y, en la lista desplegable **Elegir directiva**, seleccione **AppFlow** y, en la lista **Elegir tipo**, seleccione **Otra solicitud TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

6. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

a) En la ficha **Configuración**, vaya a **Sistema** > **Appflow**.

b) En el panel derecho, en el grupo**Configuración**, haga clic en**Cambiar configuración del flujo de aplicaciones**.

c) Seleccione **Conexión encadenamiento** y haga clic en **Aceptar**.

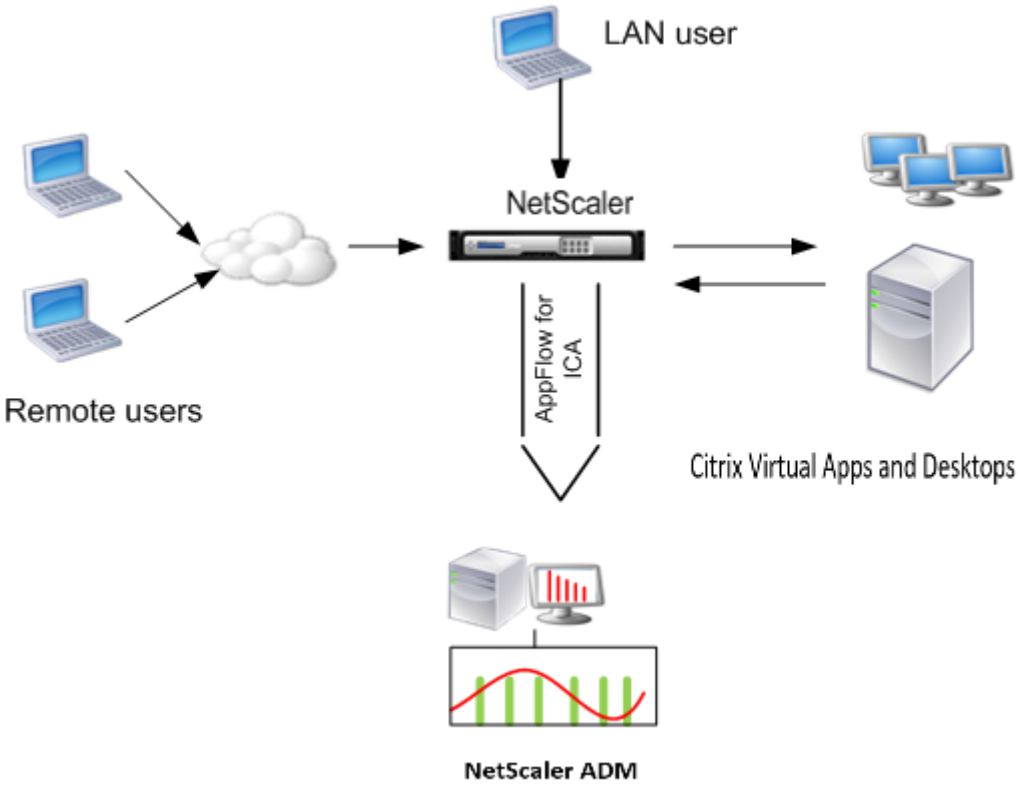
Habilitar la recopilación de datos para supervisar los dispositivos de NetScaler ADC implementados en modo de usuario de LAN

January 30, 2024

Los usuarios externos que acceden a las aplicaciones de Citrix Virtual Apps and Desktops deben autenticarse en Citrix Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a Citrix Gateway. Además, en una implementación de modo transparente, el administrador debe aplicar manualmente las directivas de redirección para que las solicitudes se redirijan al dispositivo NetScaler.

Para superar estos desafíos y para que los usuarios de LAN se conecten directamente a las aplicaciones Citrix Virtual Apps and Desktops, puede implementar el dispositivo NetScaler en modo de usuario de LAN configurando un servidor virtual de redirección de caché, que actúa como proxy SOCKS en el dispositivo Citrix Gateway.

Figura 4 . Citrix ADM implementado en modo de usuario de LAN



> **Nota**
>
> Los dispositivos Citrix ADM y Citrix Gateway residen en la misma subred.

Para supervisar los dispositivos Citrix implementados en este modo, primero agregue el dispositivo Citrix al inventario de NetScaler Insight, habilite AppFlow y, a continuación, consulte los informes en el panel de control.

Tras añadir el dispositivo Citrix al inventario de Citrix ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un NetScaler ADM implementado en modo de usuario de LAN mediante la utilidad de configuración Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte Referencia de comandos .

> • Para obtener información sobre las expresiones de políticas, consulte Políticas y expresiones .

Para configurar la recopilación de datos en un dispositivo NetScaler mediante la interfaz de línea de comandos:

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Agregue un servidor virtual de redirección de caché de proxy de reenvío con la IP y el puerto proxy, y especifique el tipo de servicio como HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Ejemplo:

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
   cltTimeout 180
<!--NeedCopy-->
```

> **Nota** Si accede a la red LAN mediante un dispositivo Citrix Gateway, agregue una acción que aplique una directiva que coincida con el tráfico VPN.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

Ejemplo:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Agregue Citrix ADM como recopilador de flujo de aplicaciones en el dispositivo Citrix ADC.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
   \\>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Cree una acción de flujo de aplicaciones y asocie el recopilador con la acción.


```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

Ejemplo:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Cree una directiva de flujo de aplicaciones para especificar la regla para generar el tráfico.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlazar la directiva de flujo de aplicaciones a un punto de enlace global.

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
   type\>
<!--NeedCopy-->
```

Ejemplo:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Nota:** El valor del tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para poder aplicarse al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para Appflow en 60 segundos.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

Ejemplo:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Guarde la configuración.

```
save ns config
<!--NeedCopy-->
```


Crear umbrales y configurar alertas para HDX Insight

January 30, 2024

HDX Insight en Citrix Application Delivery Management (ADM) le permite supervisar el tráfico HDX que pasa por las instancias de Citrix ADC. Citrix ADM le permite establecer umbrales en varios contadores utilizados para supervisar el tráfico de Insight. También puede configurar reglas y crear alertas en Citrix ADM.

El tipo de tráfico HDX está asociado con varias entidades, como aplicaciones, escritorios, puertas de enlace, licencias y usuarios. Cada entidad puede contener diferentes métricas asociadas a ellas. Por ejemplo, la entidad de la aplicación está asociada a un número de resultados, al ancho de banda consumido por la aplicación y al tiempo de respuesta del servidor. Una entidad de usuario puede asociarse con latencia de WAN, latencia DC, RTT ICA y ancho de banda consumido por un usuario.

La administración de umbrales de HDX Insight en Citrix ADM le permitió crear reglas y configurar alertas de forma proactiva cada vez que se superaban los umbrales establecidos. Ahora, esta administración de umbrales se amplía para configurar un grupo de reglas de umbrales. Ahora puede supervisar el grupo en lugar de las reglas individuales. Un grupo de reglas de umbral comprende una o más reglas de umbral definidas por el usuario para las métricas elegidas de entidades como usuarios, aplicaciones y escritorios. Cada regla se controla con un valor esperado que se introduce al crear la regla. En el caso de una entidad de usuario, el grupo umbral también se puede asociar a una geolocalización.

Una alerta se genera en Citrix ADM solo si se incumplen todas las reglas del grupo de umbrales configurado. Por ejemplo, puede supervisar una aplicación según el recuento total de inicios de sesión y también el recuento de lanzamientos de aplicaciones como un grupo umbral. Solo se genera una alerta si se infringen ambas reglas. Esto le permite establecer umbrales más realistas en una entidad.

A continuación se enumeran algunos ejemplos:

- Regla de umbral 1: El RTT de ICA (métrica) para los usuarios (entidad) debe ser <= 100 ms
- Regla de umbral 2: La latencia de la WAN (métrica) para los usuarios (entidad) debe ser <= 100 ms

Un ejemplo de grupo de umbral puede ser: {Regla de umbral 1 + Regla de umbral 2}

Para crear una regla, primero debe seleccionar la entidad que quiere supervisar. A continuación, elija una métrica mientras crea una regla. Por ejemplo, puede seleccionar la entidad de aplicaciones y, a continuación, seleccionar Recuento total de inicio de sesión o Recuento de inicio de aplicaciones. Puede crear una regla para cada combinación de una entidad y una métrica. Utilice los comparadores proporcionados (>, <, >= y <=) y escriba un valor de umbral para cada métrica.

> **Nota**
>
> Si no quiere supervisar varias entidades en un solo grupo, debe crear un grupo de reglas de umbral independiente para cada entidad.

Cuando el valor de un contador supera el valor de un umbral, Citrix ADM genera un evento que indica una violación del umbral y se crea una alerta para cada evento.

Debe configurar cómo recibe la alerta. Puede habilitar la alerta para que se muestre en Citrix ADM o recibirla como correo electrónico o SMS en su dispositivo móvil. Para las dos últimas acciones, debe configurar el servidor de correo electrónico o el servidor de SMS en Citrix ADM.

Los grupos de umbral también se pueden vincular a las geolocalizaciones para el supervisión geoespecífico de la entidad de usuario.

Ejemplos de casos de uso

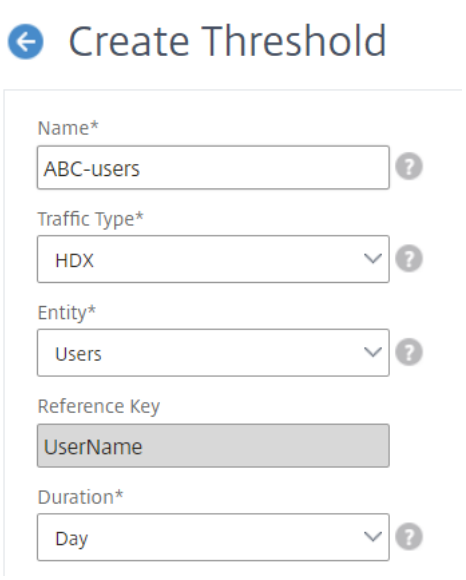
ABC Inc. es una empresa global y tiene oficinas en más de 50 países. La firma cuenta con dos centros de datos, uno en Singapur y otro en California que albergan las Citrix Virtual Apps and Desktops. Los empleados de la empresa acceden a las Citrix Virtual Apps and Desktops de Citrix en todo el mundo mediante la redirección basada en Citrix Gateway y Citrix GSLB. Eric, el administrador de Citrix Virtual Apps and Desktops para ABC Inc. quiere realizar un seguimiento de la experiencia del usuario en todas sus oficinas con el fin de optimizar la entrega de aplicaciones y escritorios para el acceso en cualquier lugar y en cualquier momento. Eric también quiere verificar las métricas de experiencia del usuario como RTT de ICA, latencias y plantear cualquier desviación de forma proactiva.

Los usuarios de ABC Inc. tienen una presencia distribuida. Algunos usuarios se encuentran cerca del centro de datos, mientras que otros se encuentran más lejos del centro de datos. Como la base de usuarios se distribuye ampliamente, las métricas y los umbrales correspondientes también varían entre estas ubicaciones. Por ejemplo, el RTT ICA para una ubicación cercana al centro de datos puede ser de 5 a 10 ms, mientras que lo mismo para una ubicación remota puede ser de alrededor de 100 ms.

Con la gestión de grupos de reglas de umbral para HDX Insight, Eric puede establecer grupos de reglas de umbral geoespecíficos para cada ubicación y recibir alertas por correo electrónico o SMS en caso de infracciones por área. Eric también puede combinar el seguimiento de más de una métrica dentro de un grupo de reglas de umbral y reducir la causa raíz a los problemas de capacidad, en su caso. Eric ahora puede realizar un seguimiento proactivo de cualquier desviación sin tener que preocuparse por la complejidad de buscar manualmente todas las métricas de la cartera de Citrix Virtual Apps and Desktops.

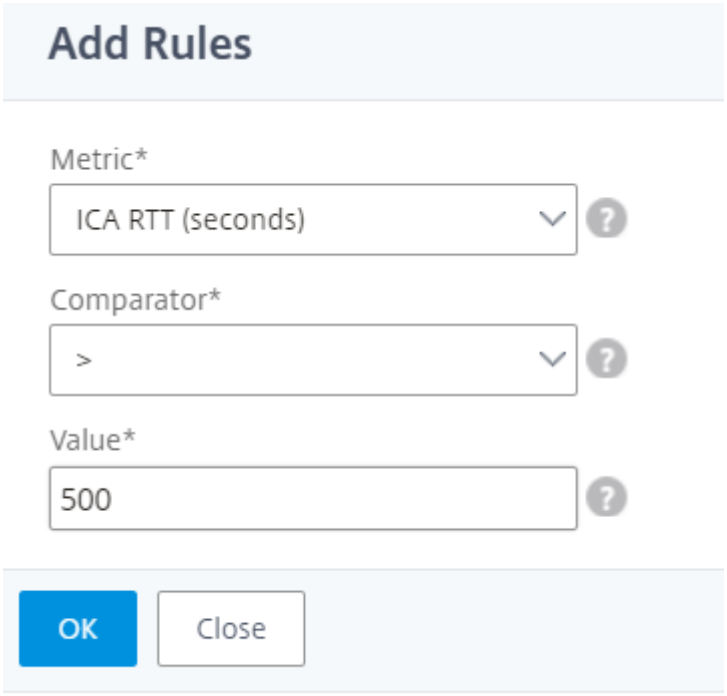
Para crear un grupo de reglas de umbral y configurar alertas para HDX Insight mediante Citrix ADM:

1. En Citrix ADM, vaya a **Analytics** > **Configuración** > **Umbrales**. En la página **Umbrales** que se abre, haga clic en **Agregar**.
2. En la página **Crear umbrales y alertas**, especifique los siguientes detalles:
   a) **Nombre**. Escriba un nombre para crear un evento para el que Citrix ADM genere una alerta.
   b) **Tipo de tráfico**. En el cuadro de lista desplegable, seleccione HDX.
   c) **Entidad**. En el cuadro de lista desplegable, seleccione la categoría o el tipo de recurso. Las entidades difieren para cada tipo de tráfico seleccionado anteriormente.
   d) **Clave de referencia**. Se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.
   e) **Duración**. En el cuadro de lista desplegable, seleccione el intervalo de tiempo durante el que quiere supervisar la entidad. Puede supervisar las entidades durante una hora, un día o una semana de duración.

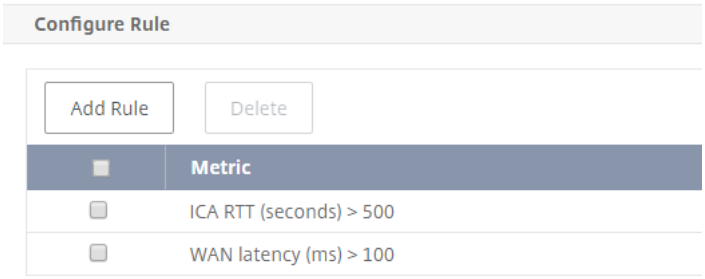


3. Creación de grupo de reglas de umbral para todas las entidades:

   Para el tráfico HDX, debe crear una regla haciendo clic en **Agregar regla.**Introduzca los valores en la ventana emergente **Agregar reglas** que se abre.

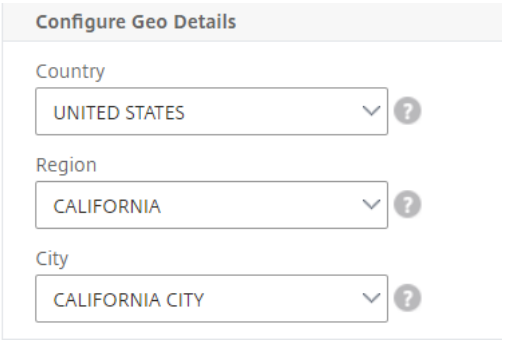


Puede crear varias reglas para supervisar cada entidad. La creación de varias reglas en un solo grupo le permite supervisar las entidades como un grupo de reglas de umbral en lugar de reglas individuales. Haga clic en **Aceptar** para cerrar la ventana.



4. Configuración del etiquetado de geolocalización para la entidad Usuarios

   Si lo quiere, puede crear una alerta basada en la ubicación para la entidad de usuario en la sección **Configurar detalles geográficos**. La siguiente imagen muestra un ejemplo de creación de un etiquetado basado en geolocalización para supervisar el rendimiento de latencia de WAN para los usuarios de la costa oeste de los Estados Unidos.



5. Haga clic en **Habilitar umbrales** para permitir que Citrix ADM comience a supervisar las entidades.
6. Opcionalmente, configure acciones como notificaciones por correo electrónico y notificaciones por SMS.
7. Haga clic en **Crear** para crear un grupo de reglas de umbral.

Visualización de informes y métricas de HDX Insight

January 30, 2024

HDX insight proporciona una visibilidad completa de los informes y las métricas relacionados con el tráfico HDX en sus instancias de NetScaler ADC.

Puede ver las métricas de HDX de cualquier entidad seleccionada. Las vistas incluyen las siguientes categorías de entidades:

- **Usuarios**: Muestra los informes de todos los usuarios que acceden a Citrix Virtual Apps and Desktops dentro del intervalo de tiempo seleccionado.
- **Aplicaciones:**muestra los informes del número total de aplicaciones y toda la información relevante relacionada, como el número total de veces que las aplicaciones se iniciaron dentro del intervalo de tiempo especificado.
- **Instancias**: Muestra los informes de las instancias NetScaler ADC que actúan como puertas de enlace para el tráfico entrante.
- **Escritorios**: muestra los informes de los escritorios utilizados en el período de tiempo seleccionado.
- **Licencias**: muestra los informes del total de licencias de VPN con SSL utilizadas dentro del intervalo de tiempo especificado.

> **Nota**
>
> El valor Licencias no se aplica a los dispositivos Citrix SD-WAN.

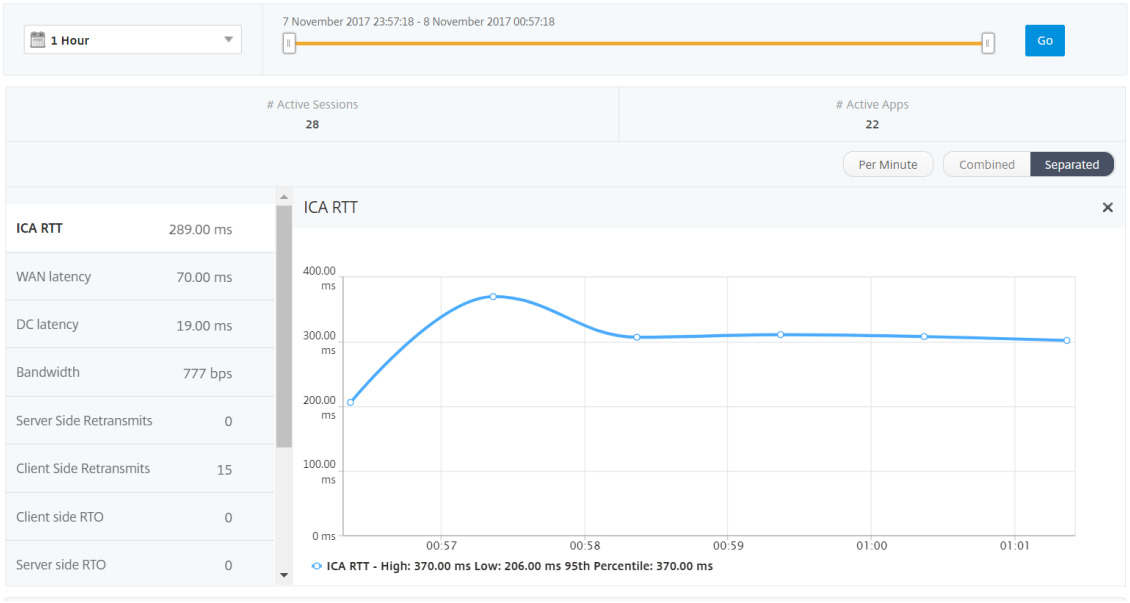
Informes y métricas de vista de usuario

6 de noviembre de 2017

Los informes y las métricas de esta vista se muestran por usuario de Citrix Virtual Apps and Desktops.

Para navegar a la vista Usuarios:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**



Los informes y las métricas de vistas de usuario constan de las siguientes secciones:

- Vista resumida
- Por vista de usuario
- Vista de sesión por usuario

Vista de resumen

La vista de resumen muestra los informes de todos los usuarios que han iniciado sesión durante la línea de tiempo seleccionada. Todas las métricas o informes de esta vista muestran los valores correspondientes para el período de tiempo seleccionado, a menos que se especifique lo contrario.

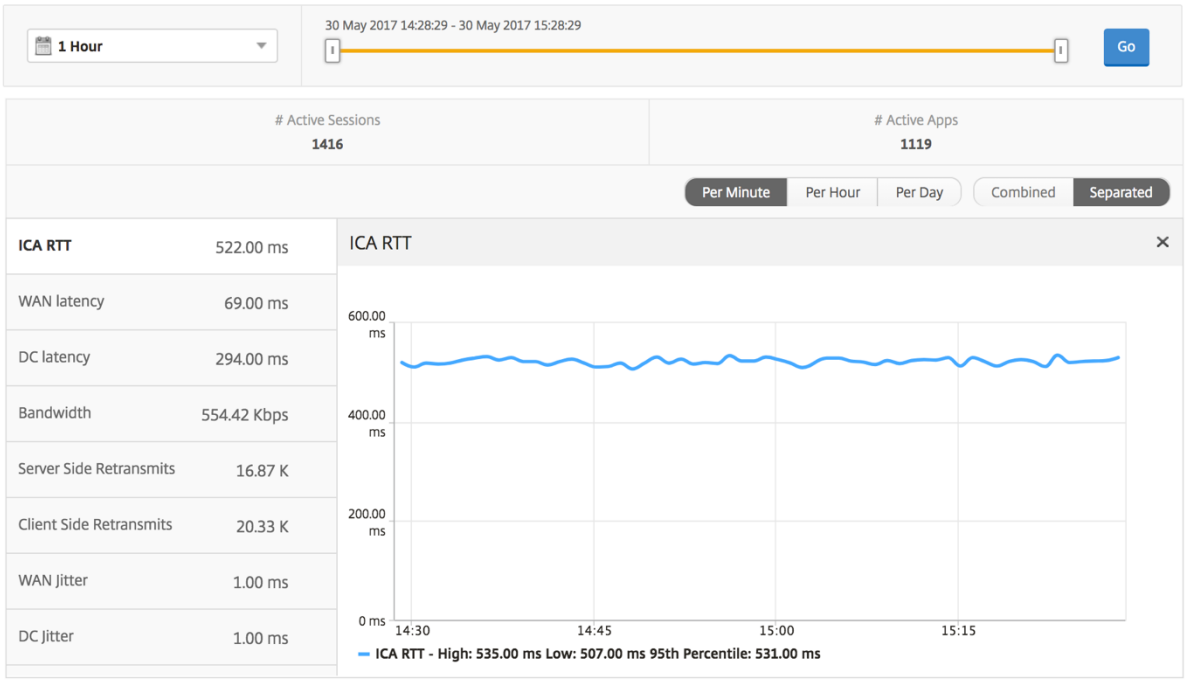
Para cambiar el período de tiempo seleccionado:

1. Utilice la lista de períodos de tiempo o el control deslizante de tiempo para establecer el intervalo de tiempo deseado.
2. Haga clic en **Ir**.

Gráfico de líneas

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual App.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.

Métricas	Descripción
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe de resumen de usuario A continuación se presentan las métricas específicas de este informe.

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual App.

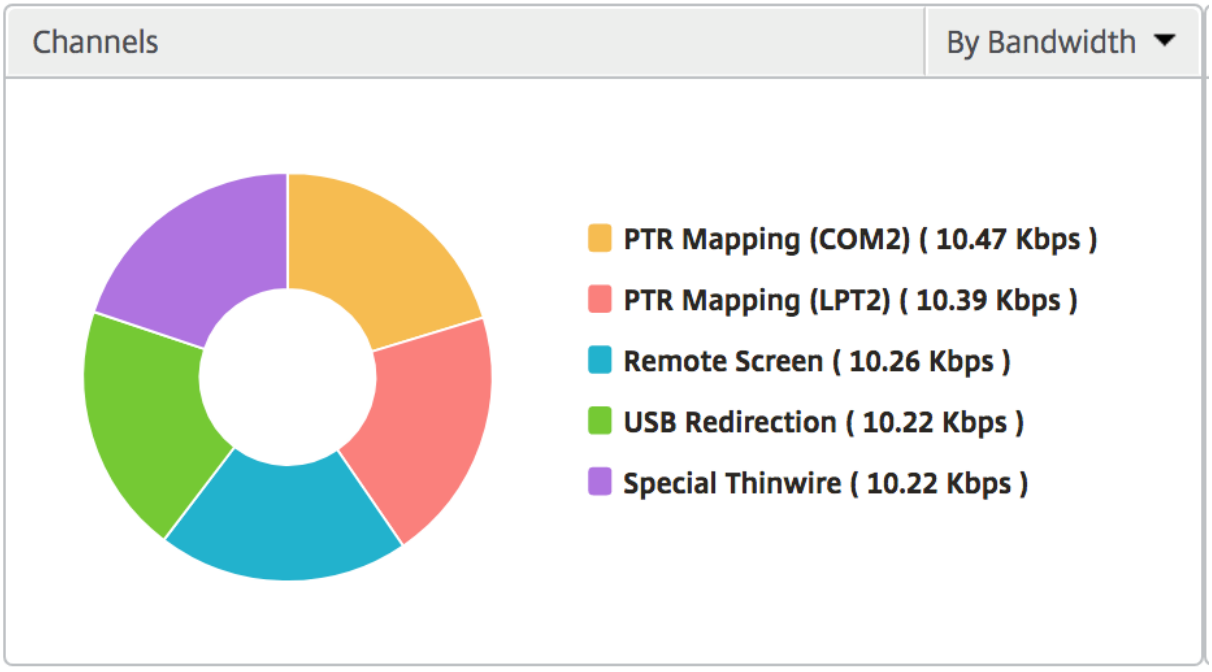
Métricas	Descripción
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
Recuento total de aplicaciones iniciadas	Total de aplicaciones lanzadas por el usuario durante el período de tiempo seleccionado.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Escritorios activos	Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado.

Users

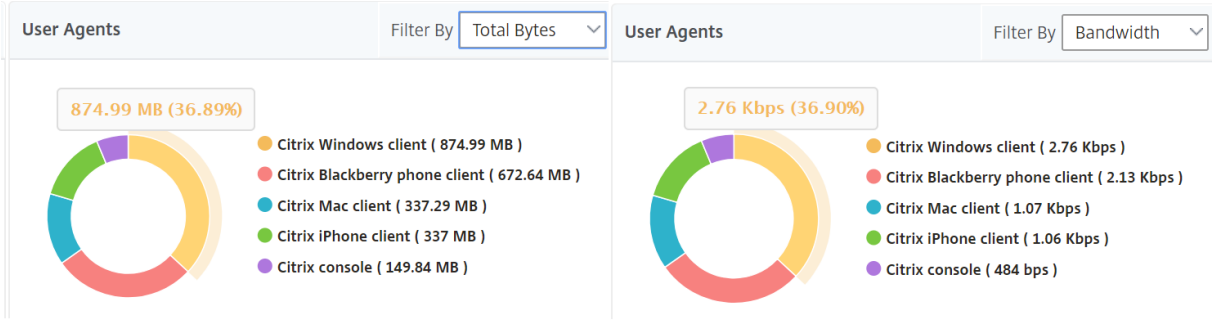
Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

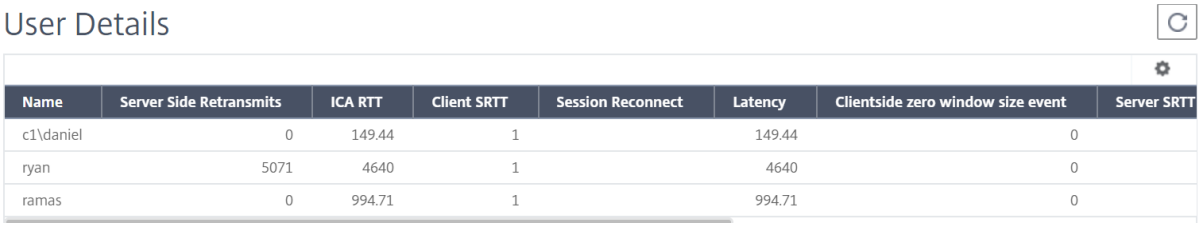
Canales Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Agentes de usuario Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada cliente receptor en forma de gráfico de anillos. Cada segmento coloreado del gráfico representa un cliente receptor. La longitud del segmento depende de la cantidad de usuarios que inician sus aplicaciones en ese cliente receptor. También puede ordenar las métricas por ancho de banda o bytes totales.



Haga clic en cada segmento para ver los detalles de los usuarios que utilizan ese cliente receptor.



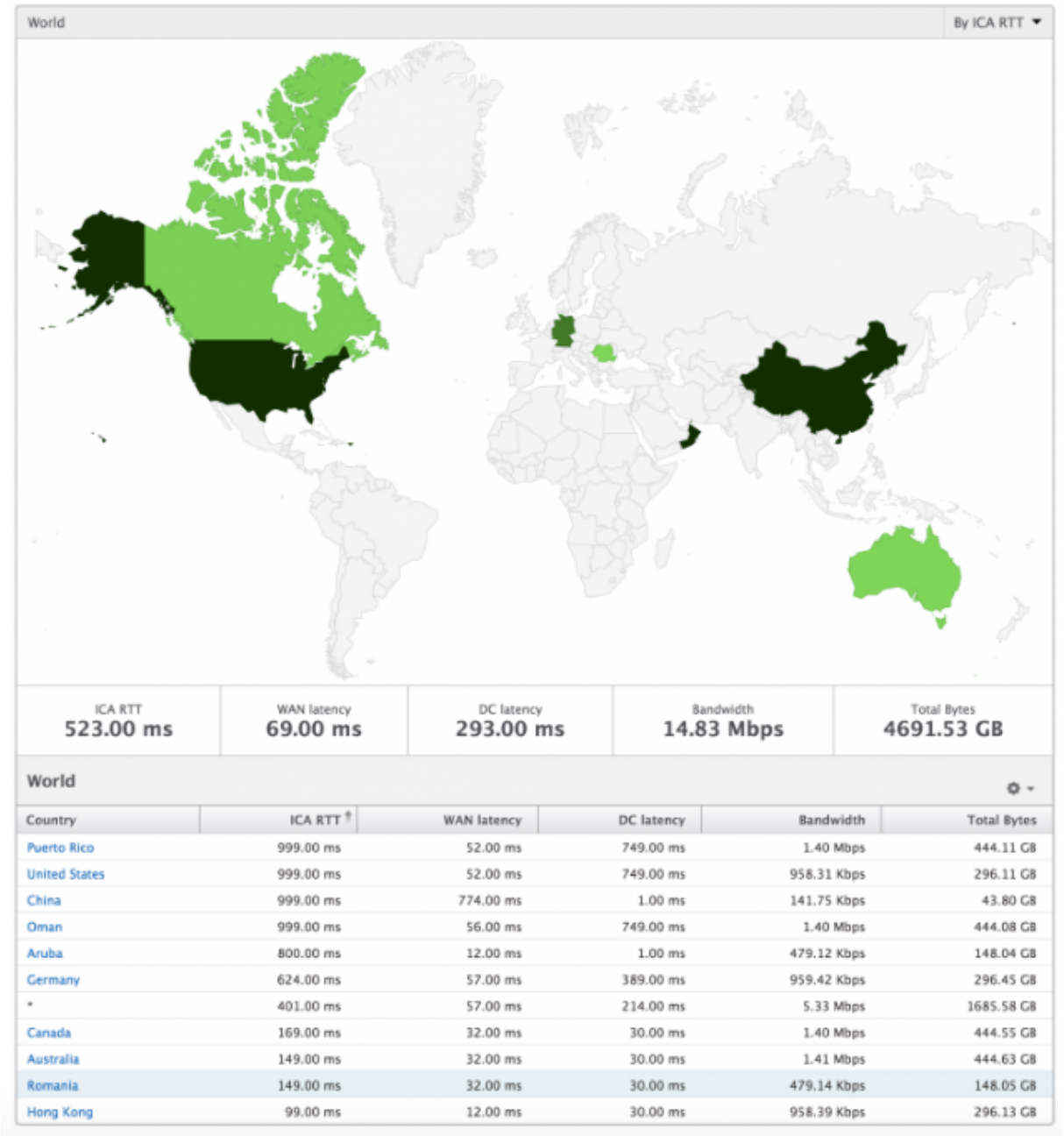
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

Recuento de incumplimiento de umbrales Las métricas de recuento de infracciones de Umbrales representan el recuento de umbrales incumplidos en el período de tiempo seleccionado.

Mapa del mundo La vista de mapa mundial en HDX Insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión mundial del sistema, profundizar en un país en particular y más en las ciudades, así como hacer clic en la región. Los administradores pueden profundizar más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Por vista de usuario

La vista por usuario proporciona informes detallados de la experiencia del usuario final para cualquier usuario seleccionado en particular.

Para navegar a métricas específicas de usuario:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.

3. Seleccione un usuario concreto en el informe Resumen de usuarios.

Gráfico de líneas El gráfico de líneas muestra el resumen de todas las métricas del usuario seleccionado en particular durante el período de tiempo seleccionado.

Informe de sesiones actuales/terminadas Este informe es pertinente para todas las sesiones de usuario actuales/terminadas del usuario seleccionado. Estas métricas se pueden ordenar por hora de inicio, reconexiones de sesión y recuento de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor Backend/Citrix Virtual App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de Receiver: Citrix Windows Client
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.

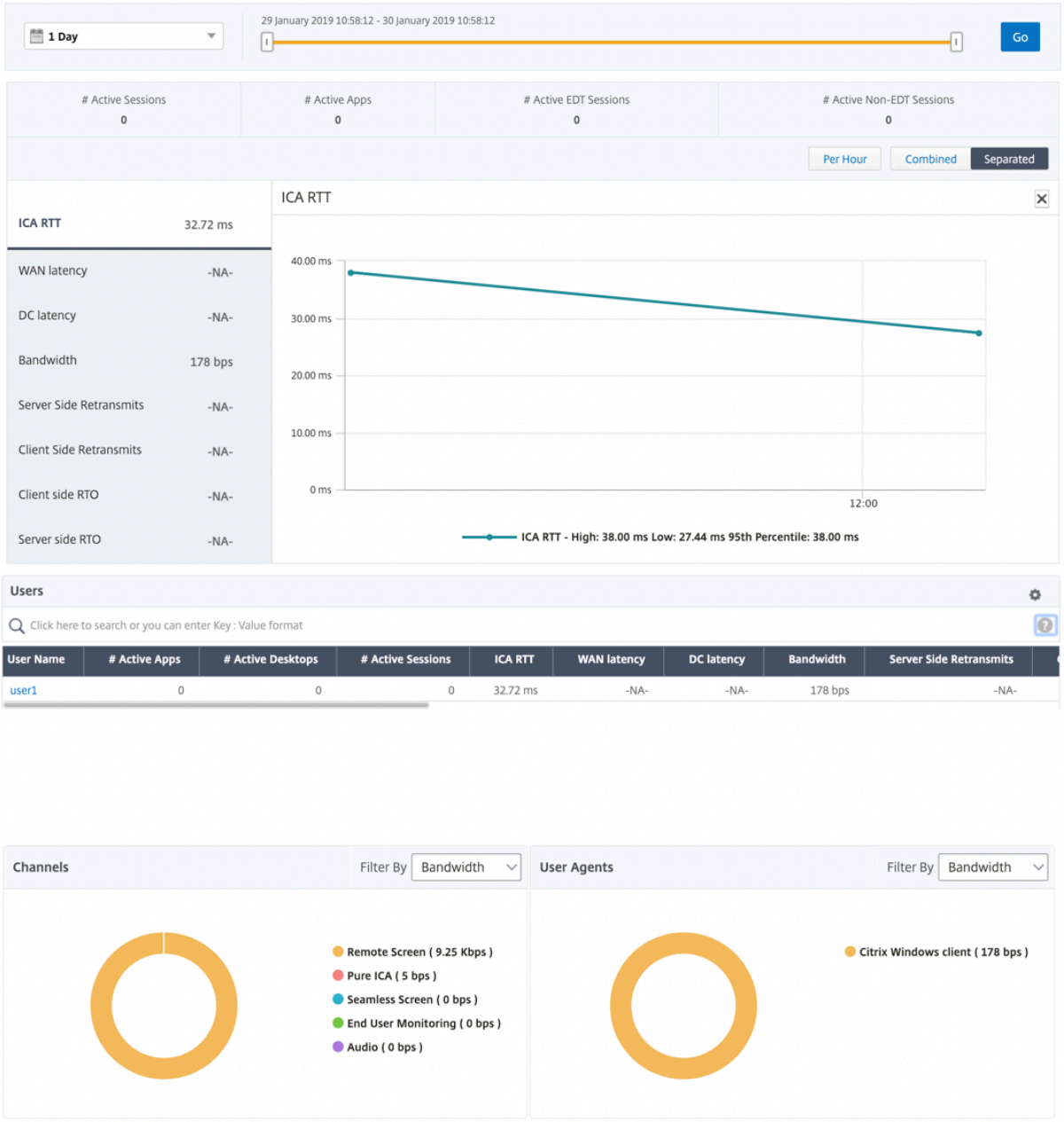
Métricas	Descripción
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.

Métricas	Descripción
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.

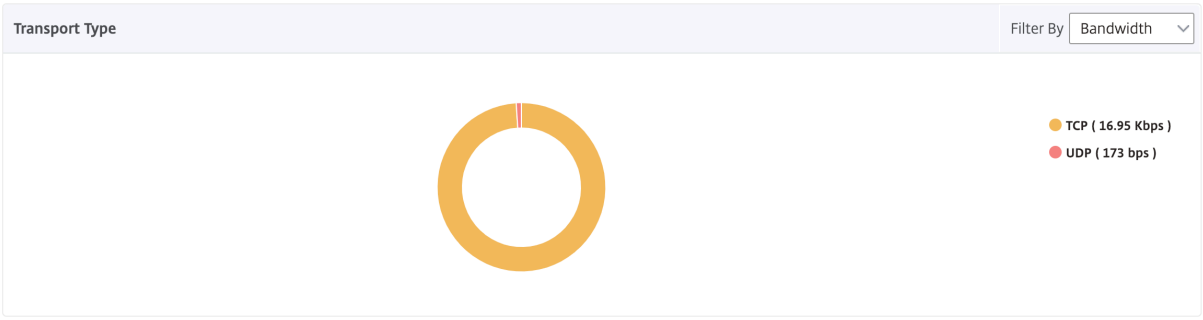
Soporte para EDT en HDX Insight

NetScaler Application Delivery Management (ADM) ahora admite el transporte de datos ilustrados (EDT) para mostrar análisis para HDX Insight. Es decir, ADM ahora admite los protocolos UDP y TCP. La compatibilidad de EDT con NetScaler Gateway garantiza una experiencia de usuario de alta definición durante la sesión de los escritorios virtuales para los usuarios que ejecutan Citrix Receiver

HDX Insight ahora muestra el número de sesiones de EDT y de sesiones que no son de EDT como parte del informe de sesiones activas. La tabla Usuarios muestra un informe detallado de todos los usuarios del sistema. La tabla muestra métricas como la latencia de WAN, la latencia de DC, las retransmisiones, los RTO y algunas de estas métricas no están disponibles para los usuarios que tienen sesiones de EDT, ya que se calculan a partir de la pila TCP actualmente. Por lo tanto, aparecerán como «NA».



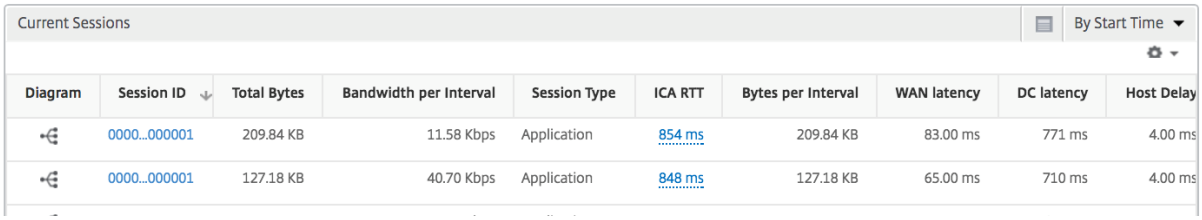
Se ha introducido un nuevo gráfico de donut para permitirle ver el ancho de banda consumido por el usuario y también el número total de bytes según el tipo de protocolo utilizado por los usuarios.

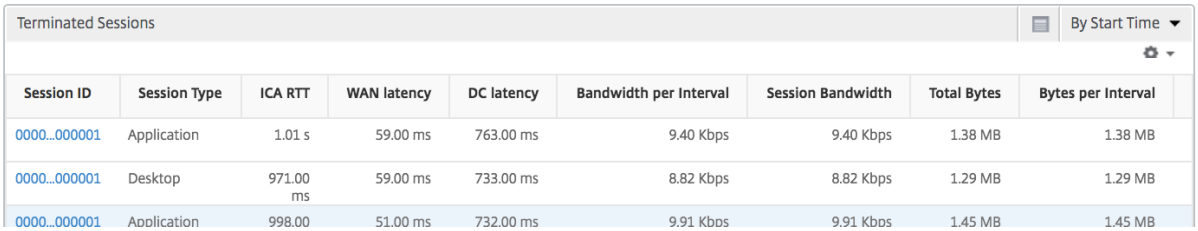


> **Nota**
>
> EDT en HDX Insight es compatible con NetScaler ADM desde la versión 12.1 compilación 50.28 y está disponible en instancias ADC desde la versión 12.1 compilación 49.23.

Métricas de HDX Insight disponibles en NetScaler ADM 12.0 y versiones posteriores:

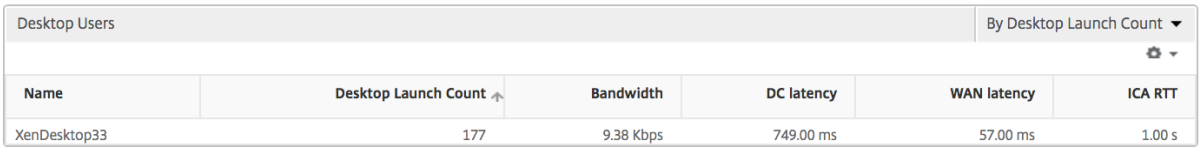
Latencia del lado del cliente L7	Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler ADC. Esta métrica es útil en dispositivos que no son Citrix que están presentes en la ruta de entrega.
Latencia L7 del lado del servidor	La latencia media de L7 observada entre el dispositivo NetScaler ADC y Citrix Virtual App. Esta métrica es útil en dispositivos que no son Citrix que están presentes en la ruta de entrega.
Latencia de vulneración máxima	El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido.
Latencia de violación promedio	El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de “latencia L7 infringida”.
Recuento de incumplimiento de umbral L7	Número de veces que se ha producido una infracción del umbral L7.



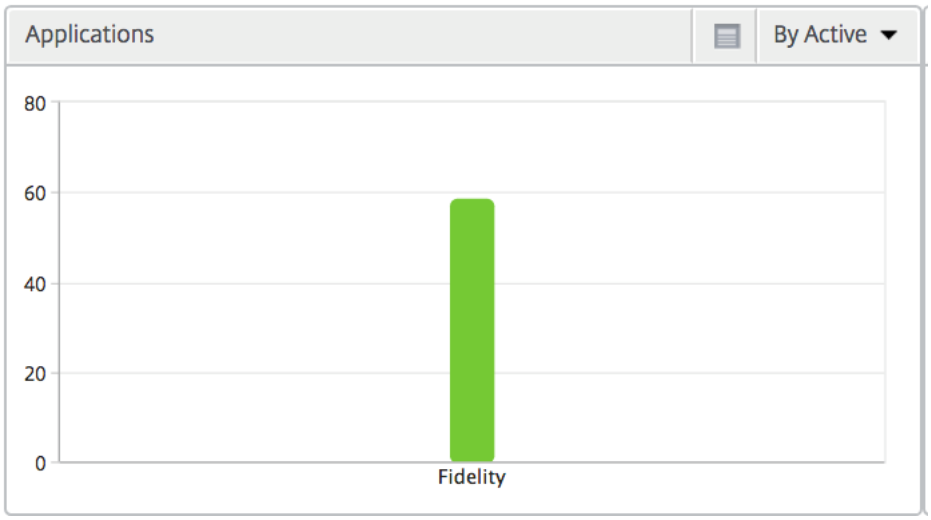


Usuarios de escritorio Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

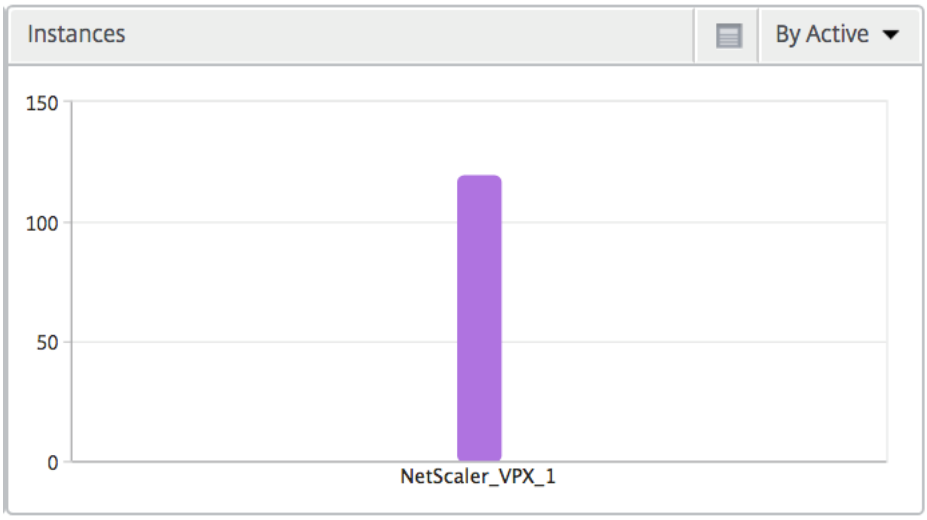
Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.



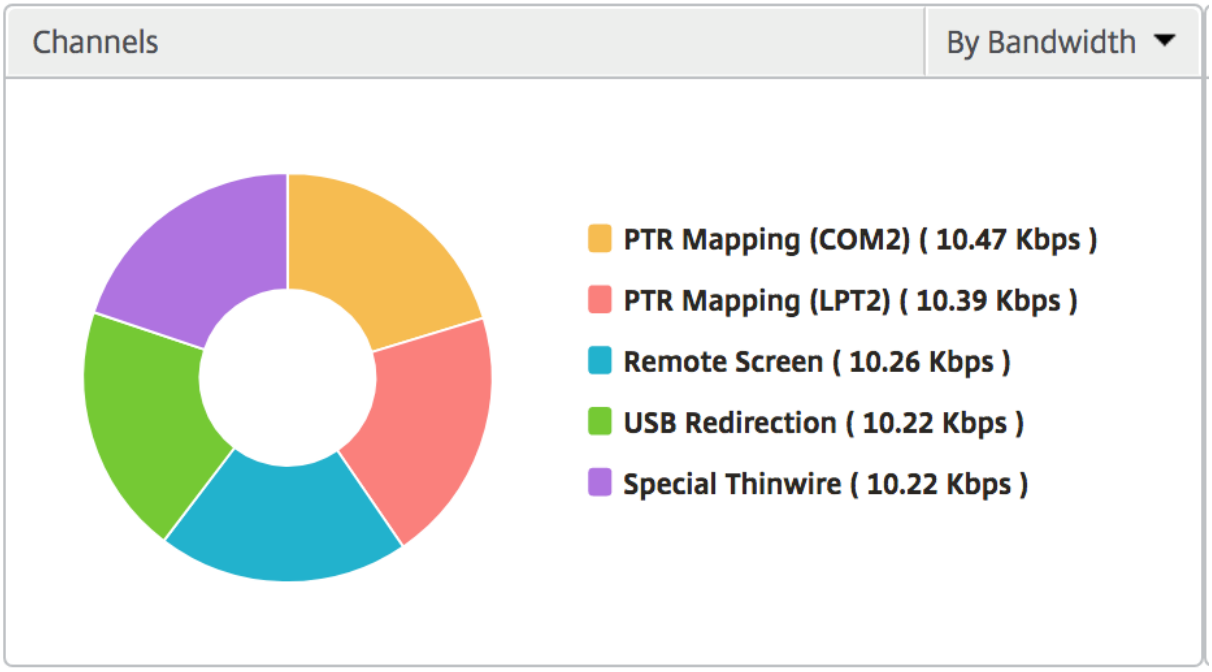
Aplicaciones Un gráfico de barras que representa las aplicaciones ordenadas por Activas, recuento total de inicios de sesiones, recuento total de inicios de aplicaciones y duración del lanzamiento.



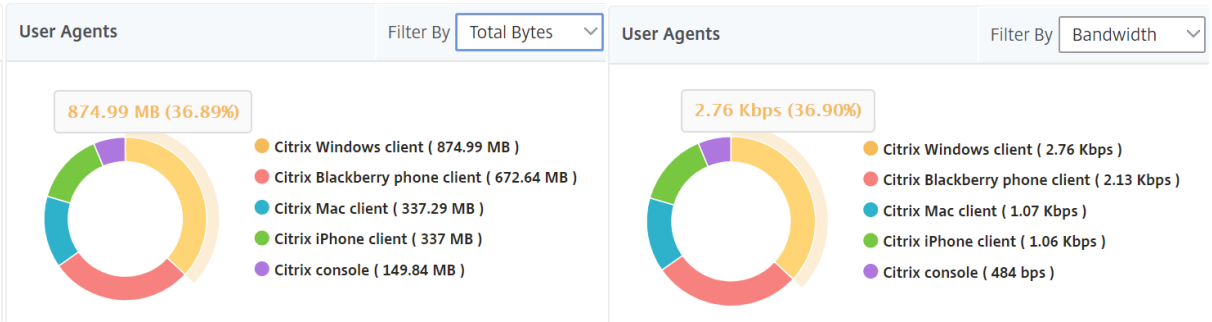
Instancias Un gráfico de barras que representa las instancias de NetScaler ADC ordenadas por aplicaciones activas y totales



Canales Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Agentes de usuario Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada punto final en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



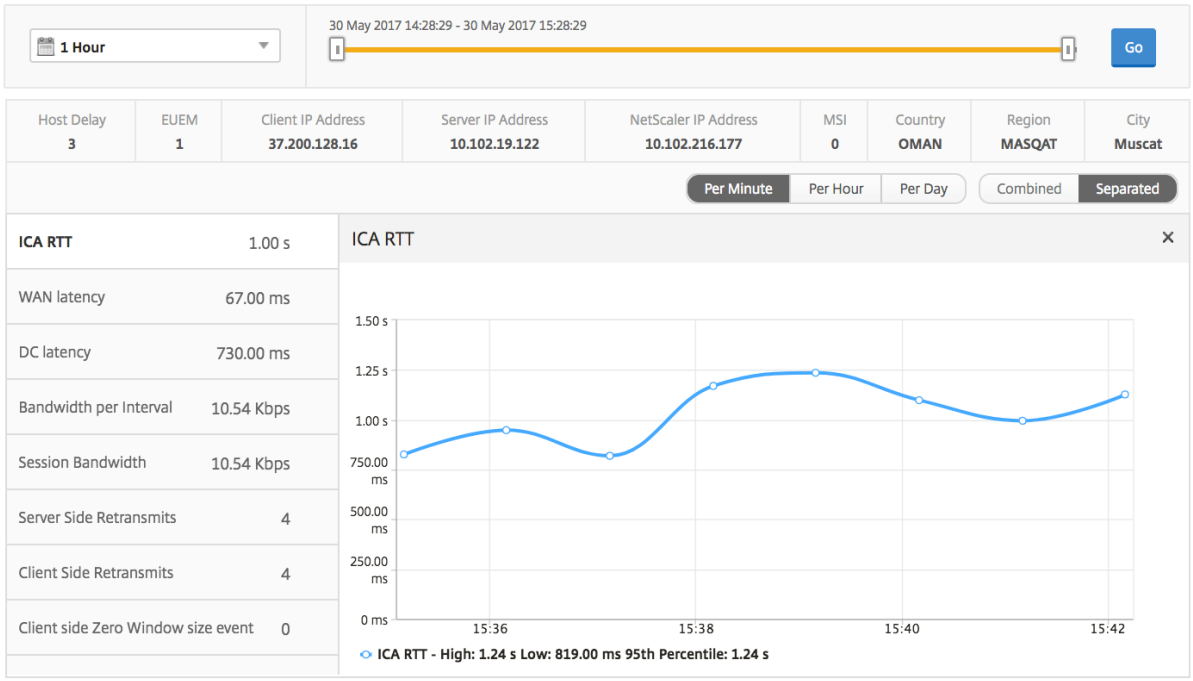
Vista por sesión de usuario La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

Para ver las métricas de la sesión de un usuario seleccionado:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
3. Select un usuario concreto en la sección **Informe de resumen de usuario**.
4. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

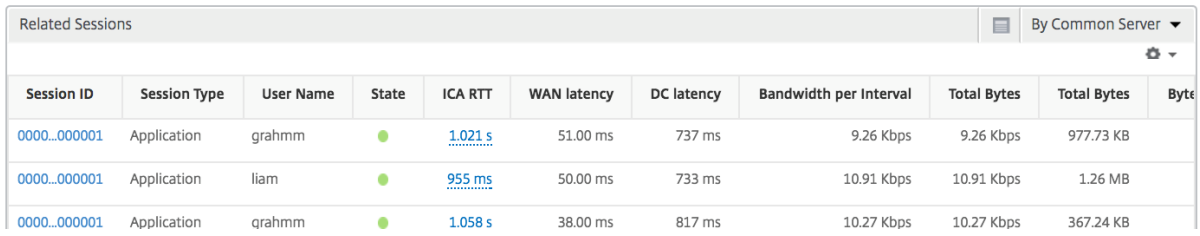
Gráfico cronológico

Métricas	Descripción
Reconexiones de sesión	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
Recuento de ACR	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.



Aplicación activa La sección **Aplicaciones activas** muestra las aplicaciones activas del usuario seleccionado. Estas aplicaciones también se pueden ordenar por número de sesiones activas y duración de inicio.

Sesiones relacionadas La sección Sesiones relacionadas muestra las sesiones relacionadas de las sesiones del usuario seleccionado. La relación se puede seleccionar como servidores comunes o común de NetScaler ADC.



Informes y métricas de Application View

Los informes y métricas de esta vista se centran en Citrix Virtual Apps.

Para desplazarse a la vista Aplicación:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.

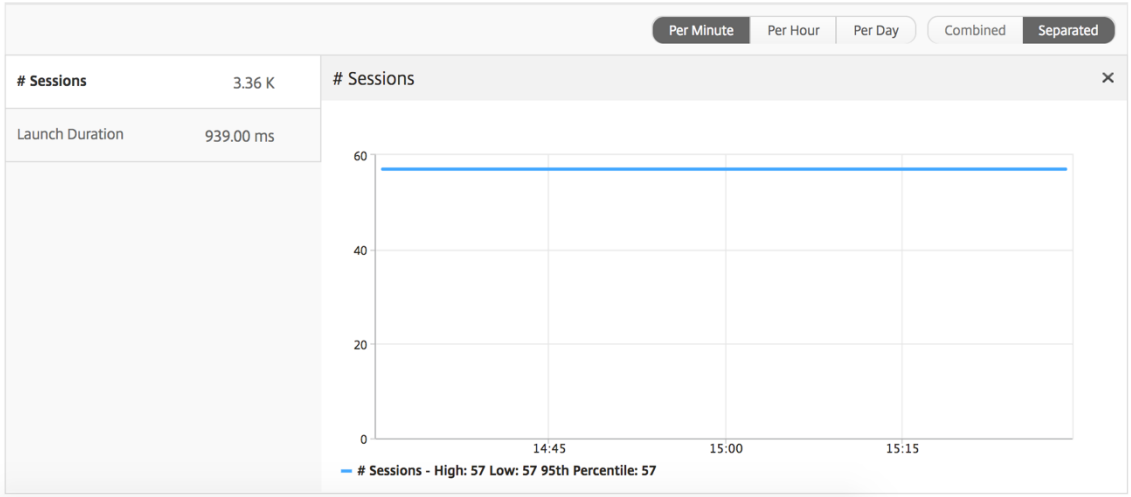
Vista de resumen

La vista de resumen muestra los informes de todas las aplicaciones que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas e informes siguientes, a menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

Gráfico de líneas

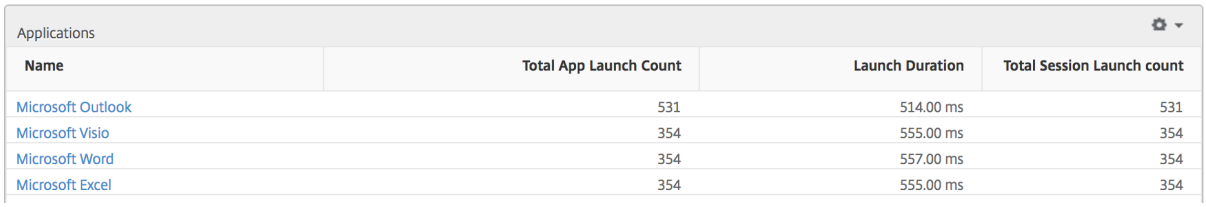
Métricas	Descripción
N.º de sesiones	Número total de sesiones durante un intervalo de tiempo determinado.
Duración de inicios	Promedio de tiempo necesario para iniciar una aplicación.



Informe resumido de aplicaciones

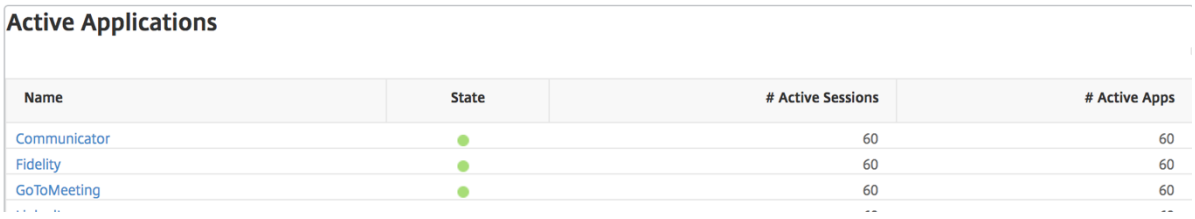
Métricas	Descripción
Nombre	Nombre de Citrix Virtual Apps.

Métricas	Descripción
Recuento total de sesiones iniciadas	Número total de sesiones activas de Citrix Virtual Apps durante el intervalo de tiempo dado.
Recuento total de aplicaciones iniciadas	Número total de Citrix Virtual Apps lanzadas durante el intervalo de tiempo especificado.
Duración de inicios	Tiempo promedio que se tarda en iniciar la aplicación virtual de Citrix.



Informe de aplicaciones activas

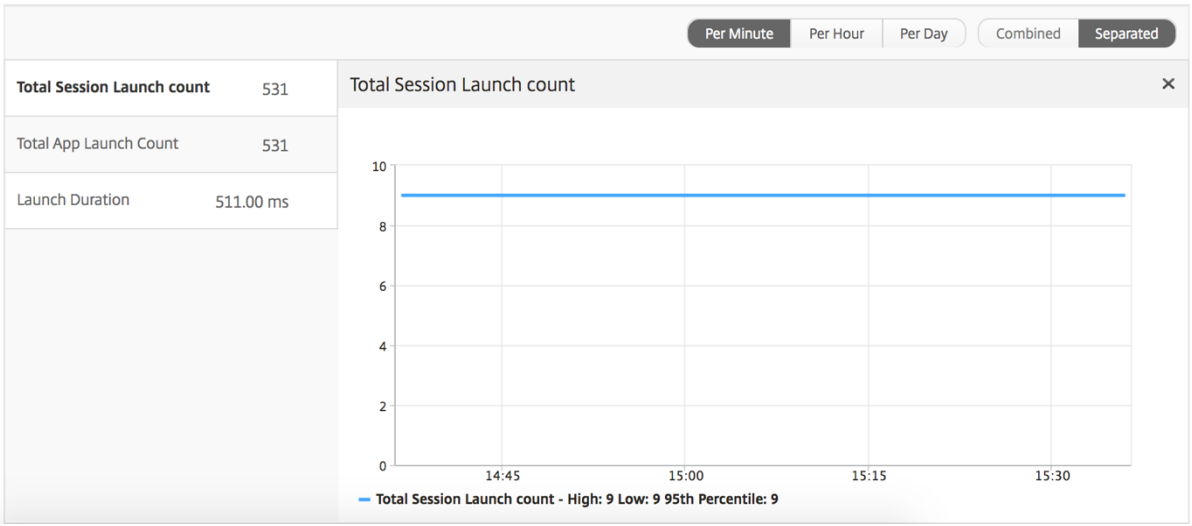
Métricas	Descripción
Nombre	Nombre de la aplicación virtual Citrix.
State	Muestra el estado de la aplicación: Verde-Activa, Rojo-Inactiva
N.º de sesiones activas	Número de sesiones de usuario activas que utilizan esta aplicación durante un intervalo de tiempo determinado.
Aplicaciones #Active	Número de sesiones activas para esta aplicación.



Informe Umbral El informe de umbrales representa el recuento de umbrales incumplidos cuando la *entidad* es seleccionada como *Solicitud* en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

Gráfico de líneas

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
Duración de inicios	Promedio de tiempo necesario para iniciar una aplicación.



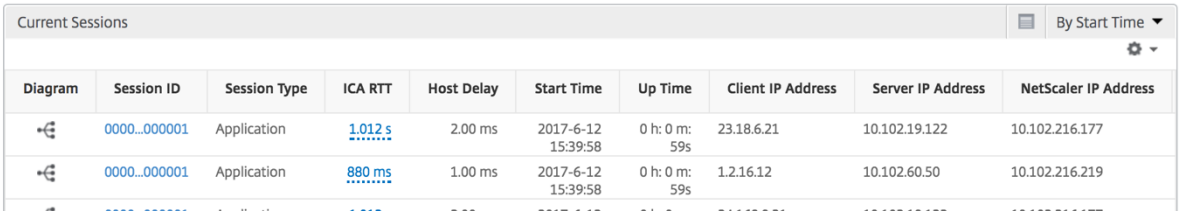
Informe de sesiones actuales

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.

Métricas	Descripción
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor backend/Citrix Virtual Apps.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de Receiver: Citrix Windows Client
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.

Métricas	Descripción
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Nombre de usuario	El nombre de usuario del usuario que accede a esta aplicación virtual de Citrix en particular.
ID de sesión	Identificador único para la sesión de Citrix Virtual Apps.
Tipo de sesión	Será “Solicitud”.
State	Estado de la sesión: verde para activa, rojo para inactiva.

Métricas	Descripción
Latencia de vulneración máxima	El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido.
Latencia de violación promedio	El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de "latencia L7 infringida".
Recuento de incumplimiento de umbral L7	Número de veces que se ha producido una infracción del umbral L7.
Latencia del lado del cliente L7	Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler ADC. Esta métrica es útil en dispositivos que no son Citrix que están presentes en la ruta de entrega.
Latencia L7 del lado del servidor	La latencia L7 promedio observada entre el dispositivo NetScaler ADC y Citrix Virtual Apps. Esta métrica es útil en dispositivos que no son Citrix que están presentes en la ruta de entrega.



Vista Por sesión de aplicación

La vista por sesión de aplicación muestra los informes de una sesión de aplicación seleccionada concreta.

Para ver los informes de sesión:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.
3. Seleccione un usuario concreto del informe resumido de la aplicación.
4. Se seleccionó una sesión del informe de sesiones actuales.

Gráfico de líneas

Métricas	Descripción
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir,. de NetScaler ADC al usuario final.
Evento de ventana cero en el lado del servidor	Latencia causada por el lado del servidor de la red. Es decir,. de NetScaler ADC a servidores backend.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.

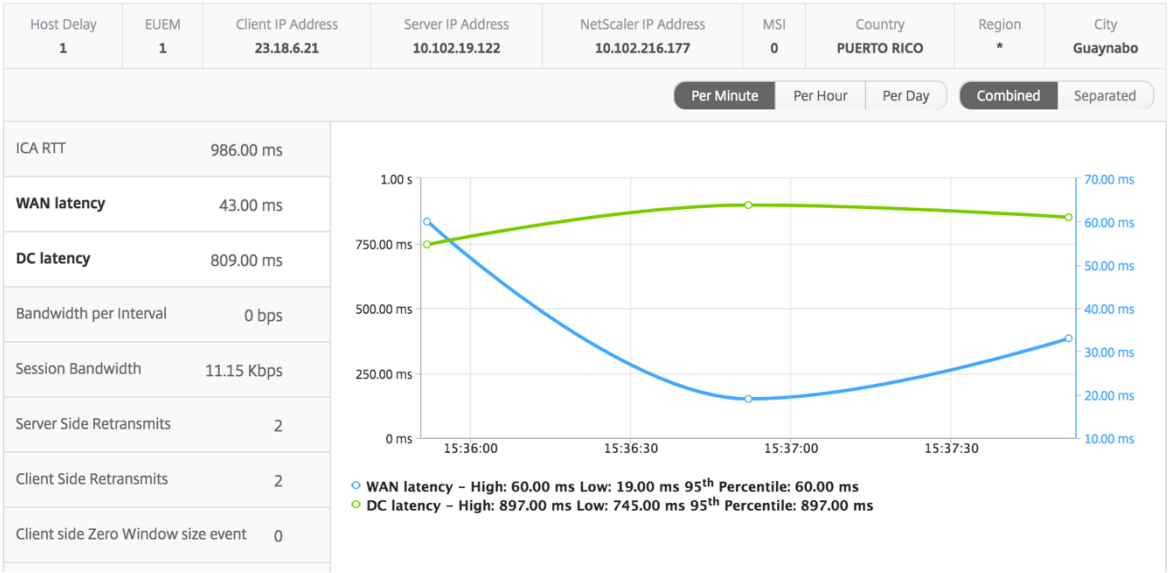
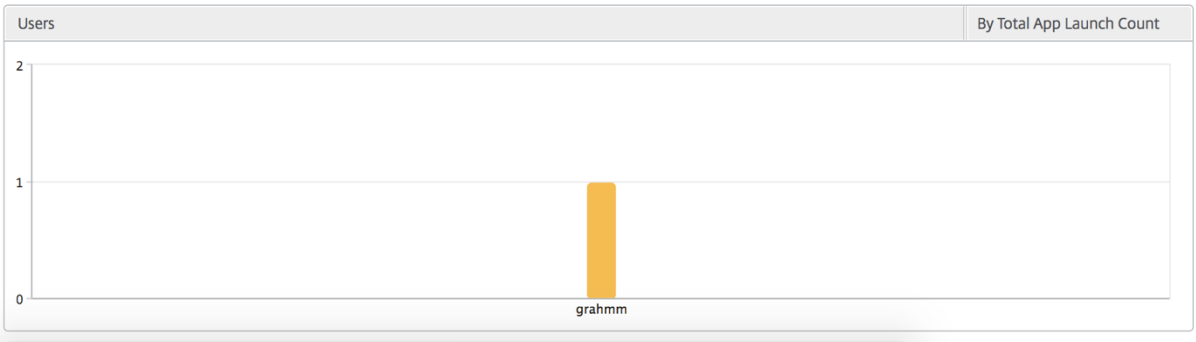


Gráfico de barras de usuario El gráfico de barras del usuario representa a los usuarios que han iniciado sesión en esta aplicación en particular.



Informes y métricas de Desktop View

Los informes y las métricas de esta vista se centran en los Citrix Virtual Desktops.

Para desplazarse a la vista Escritorio:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX InsightEscritorio**.

Vista de resumen

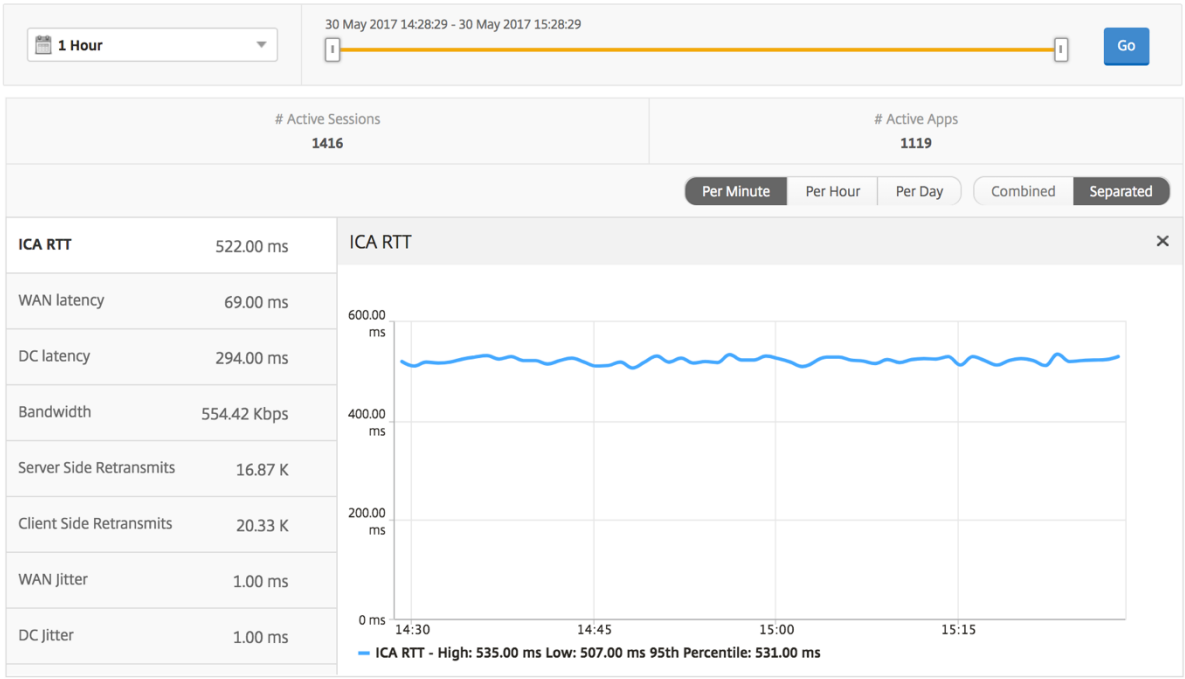
La vista de resumen muestra los informes de todos los Citrix Virtual Desktops que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas e informes siguientes, a menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

Gráfico de líneas

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.

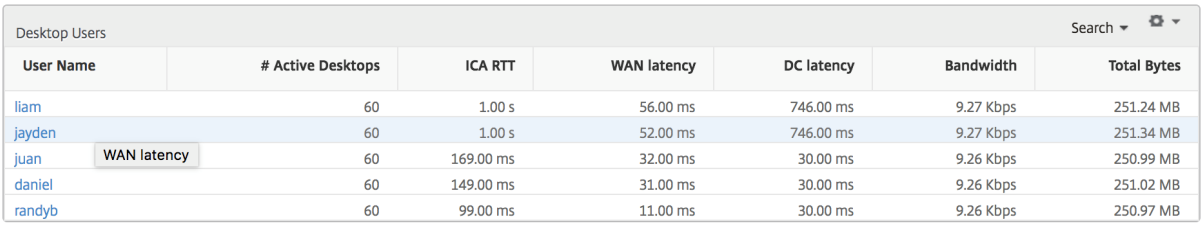
Métricas	Descripción
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe de resumen de escritorio

Métricas	Descripción
Sesiones activas	Número total de sesiones activas de Citrix Virtual Desktops durante un intervalo de tiempo determinado.
Escritorios activos	Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.

Métricas	Descripción
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.



Informe Umbral El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Escritorio en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

Por vista de escritorio

Por vista de escritorio proporciona informes detallados de la experiencia del usuario final para un escritorio virtual de Citrix seleccionado.

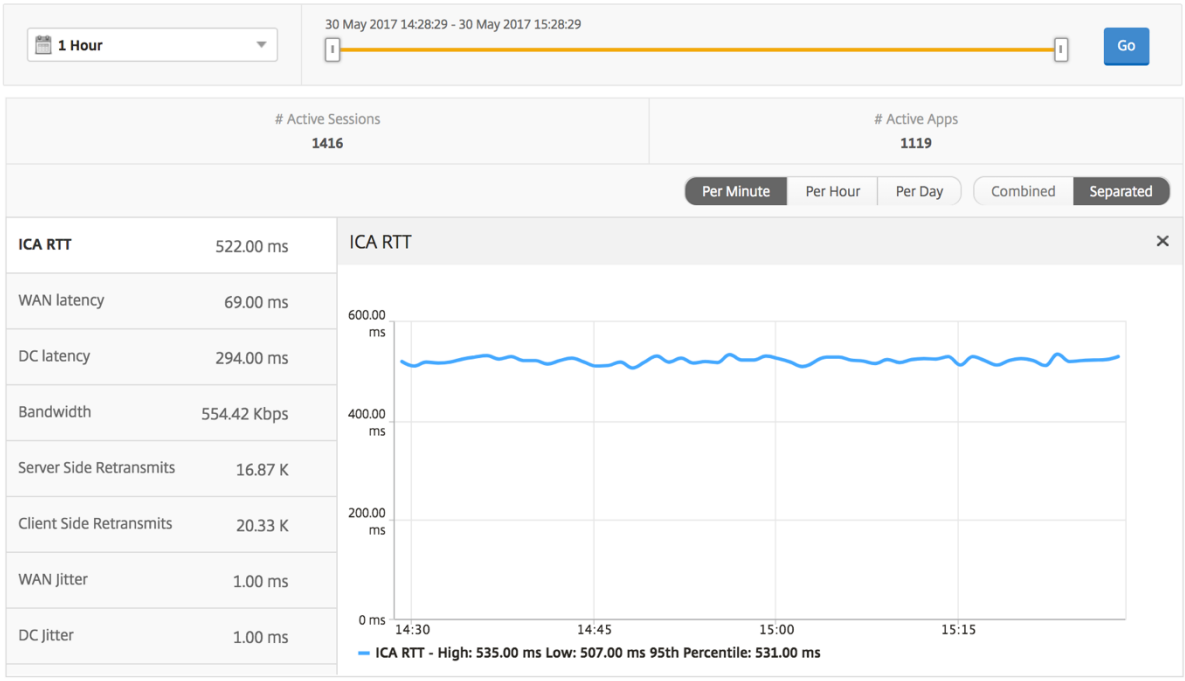
Para navegar a la vista Escritorio en particular:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Escritorio**.
3. Seleccione un **escritorio** concreto en el **informe de resumen de escritorios**.

Gráfico de líneas

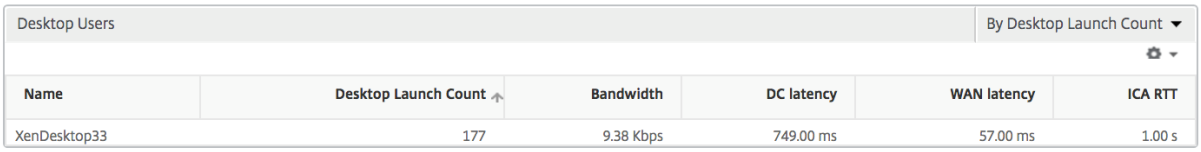
Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.

Métricas	Descripción
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe Usuarios de escritorio Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.

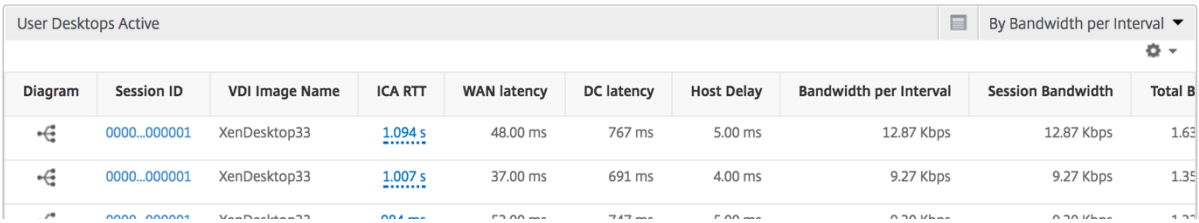


Informe de escritorios de usuario activos e inactivos Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor backend/Citrix Virtual Apps.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de Receiver: Citrix Windows Client
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.

Métricas	Descripción
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.

Métricas	Descripción
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Nombre de la imagen VDI	Nombre del Citrix Virtual Desktops al que está conectado el usuario
Diagrama	



Vista Por sesión de escritorio

Por vista de sesión de escritorio proporciona informes para una determinada sesión de Citrix Virtual Desktops seleccionada.

Para desplazarse a la vista de sesión de Escritorio:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Escritorio**.
3. Seleccione un escritorio concreto en el **informe de resumen de escritorios**.
4. Seleccione una sesión del informe de sesiones actuales.

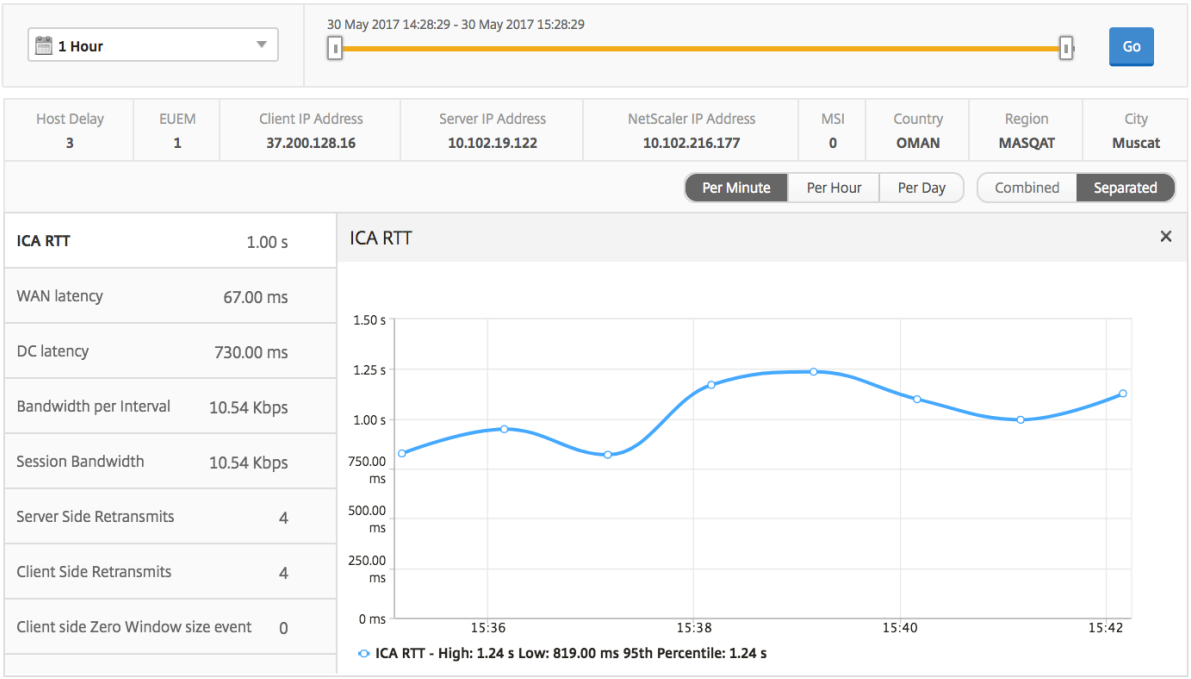
Gráfico cronológico La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

Para ver las métricas de la sesión de un usuario seleccionado:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
3. Select un usuario concreto en la sección **Informe de resumen de usuario**.
4. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

Métricas	Descripción
Reconexiones de sesión	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
Recuento de ACR	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.

Métricas	Descripción
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.

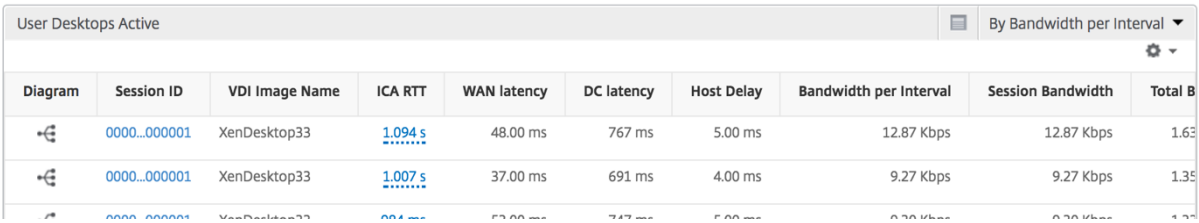


Informe Sesiones de escritorio relacionadas Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.

Métricas	Descripción
Demora de host	Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor backend/Citrix Virtual Apps.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de Receiver: Citrix Windows Client
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.

Métricas	Descripción
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end.



Informes y métricas de la vista de instancias

Los informes y las métricas de la vista de instancias se centran en las instancias de NetScaler ADC.

Para desplazarse a la vista Instancia:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Instancias**.

Los informes y las métricas de vistas de instancias constan de las siguientes secciones:

- Vista resumida de la instancia
- Vista por instancia

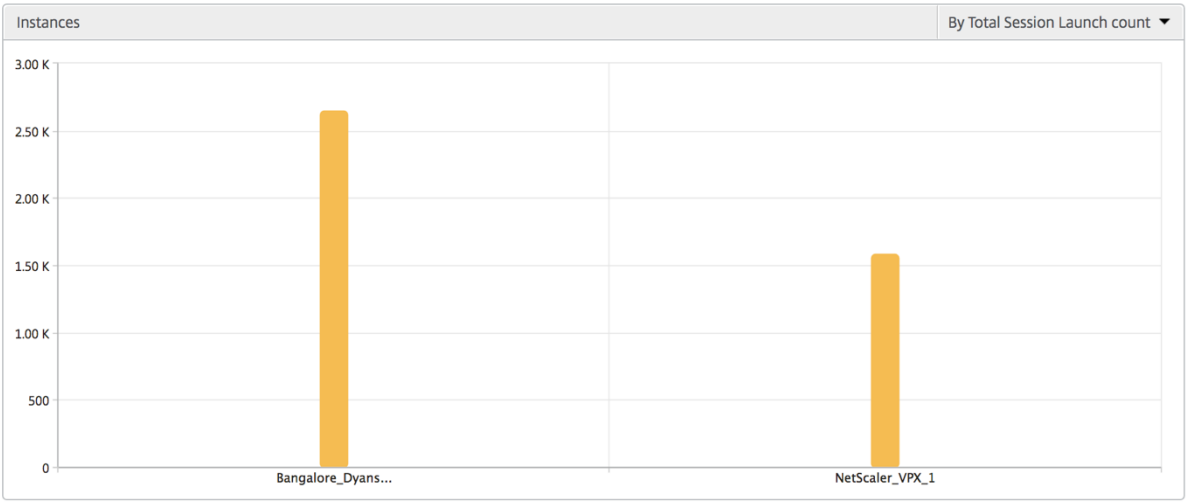
Vista Resumen de instancias

Esta vista se denomina vista de resumen, ya que muestra los informes de todas las instancias de NetScaler ADC que se agregan a NetScaler ADM.

Todas las métricas/informes a continuación, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

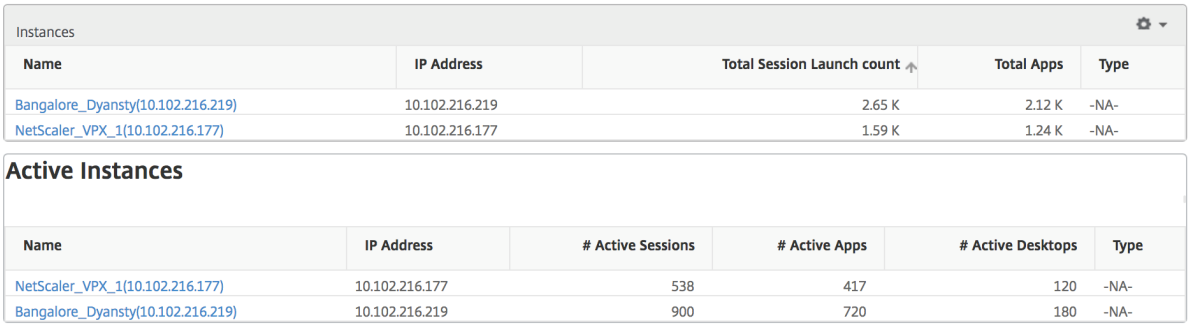
Gráfico de barras de instancias

Este gráfico muestra la instancia frente al recuento de inicio total de sesión	Aplicaciones totales que se pueden seleccionar en el menú desplegable de la parte superior derecha del lienzo del gráfico.



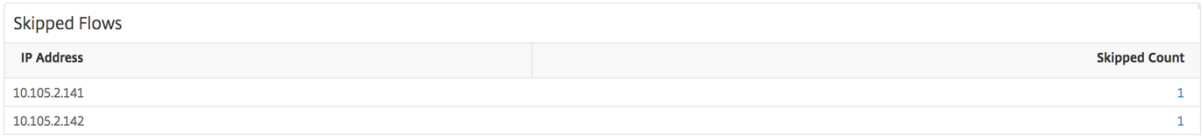
Informe resumido de instancias/instancias activas

Métricas	Descripción
Nombre	Nombre de host de la instancia de NetScaler ADC.
Dirección IP	Dirección IP de NetScaler.
Recuento total de sesiones iniciadas	Número total de sesiones de usuario únicas creadas durante un intervalo de tiempo determinado.
Total de aplicaciones	Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado.
Tipo	N/D



Informe Umbral El informe Umbral representa el recuento de umbrales incumplidos cuando se selecciona la *entidad* como Instancia en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

Flujos omitidos Un flujo omitido es un registro que omitió el análisis de la conexión ICA. Esto puede deberse a varios motivos, como el uso de versiones no compatibles de Citrix Virtual Apps and Desktops, una versión no compatible del receptor o el tipo de receptor, etc. Esta tabla muestra la dirección IP y el recuento de flujo omitido. Estos receptores pueden no ser parte de receptores en la lista blanca; por lo tanto, estas sesiones se omiten de la supervisión.

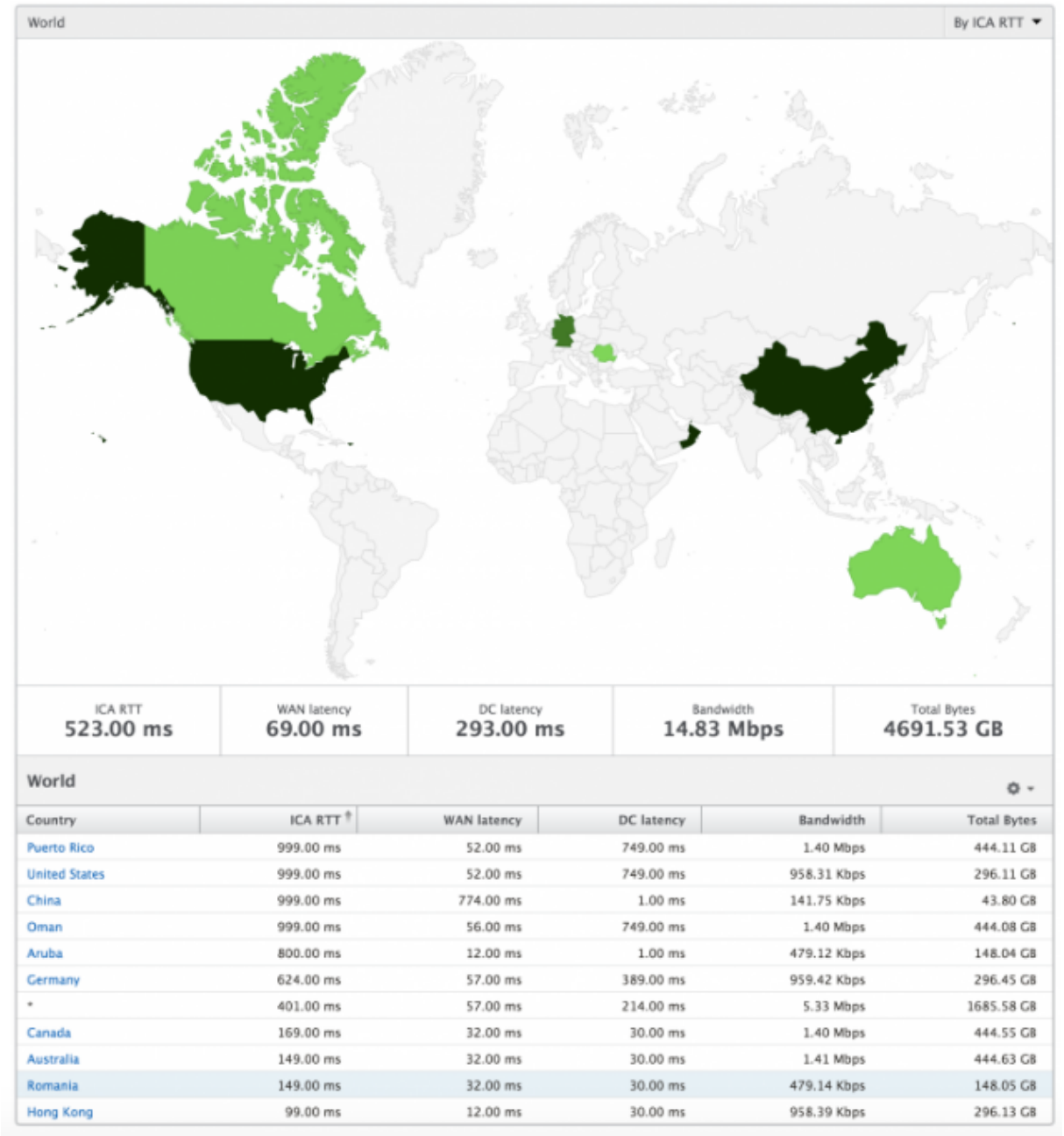

Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Visión del mundo La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión del mundo del sistema, profundizar en un país en particular y más en las ciudades, así como simplemente haciendo clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el mapa mundial de HDX insight, y la densidad de cada métrica se muestra en forma de mapa de calor:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Vista Por instancia

Por vista de instancia proporciona informes detallados sobre la experiencia del usuario final para una instancia específica de NetScaler ADC seleccionada.

Para desplazarse a la vista Instancia:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Instancias**.

3. Seleccione una instancia en particular del **Informe resumido de instancias**.

Gráfico de líneas

Métricas	Descripción
Dirección IP	Representa la dirección IP de NetScaler de la instancia seleccionada.
Recuento total de sesiones iniciadas	Número total de sesiones activas de Citrix Virtual Apps durante el intervalo de tiempo dado.
Total de aplicaciones	Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado.

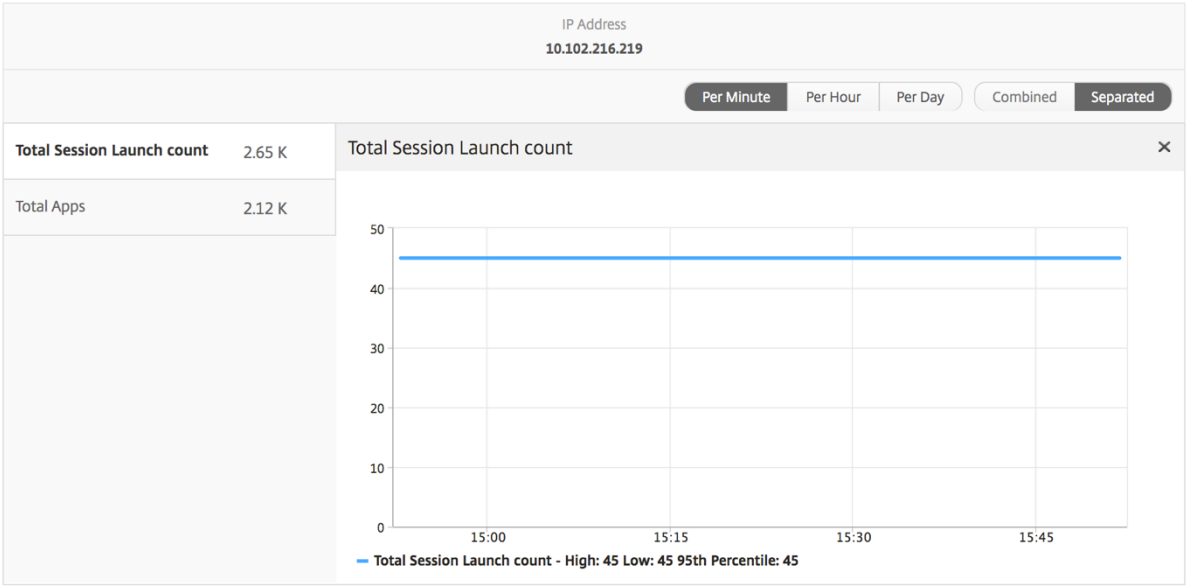


Gráfico de barras de aplicaciones Muestra las 5 aplicaciones principales basadas en los siguientes criterios: Por aplicaciones activas, recuento total de inicios de sesión, recuento total de inicios de aplicación o duración de los inicios.

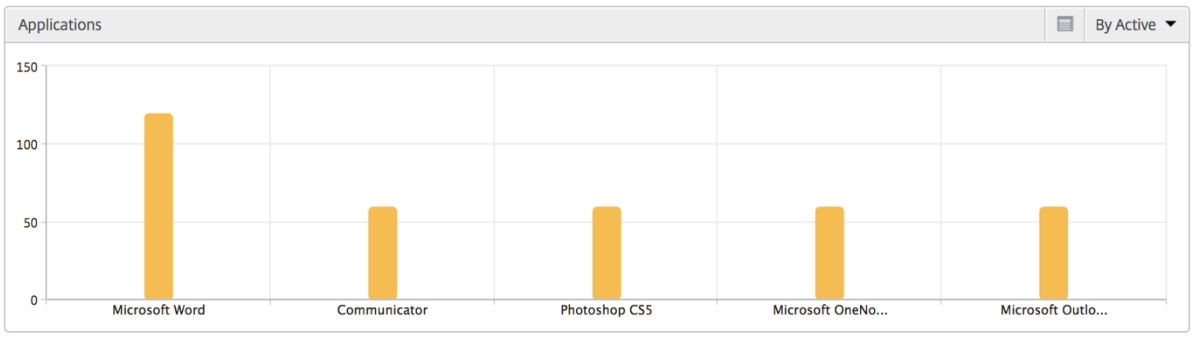
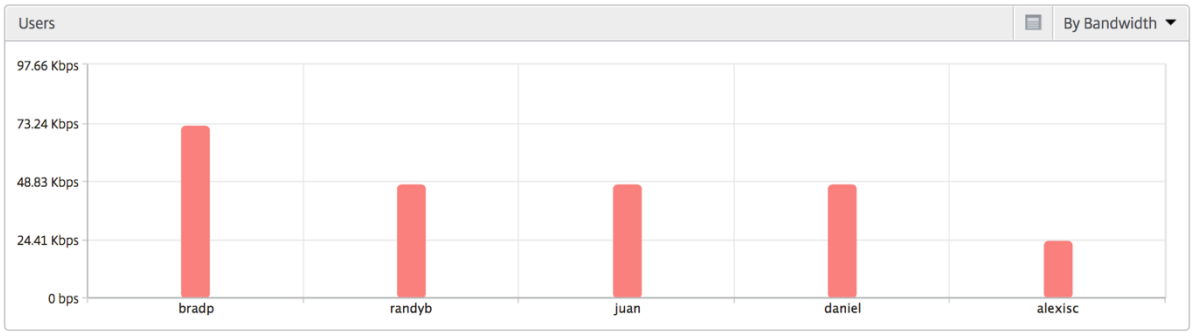


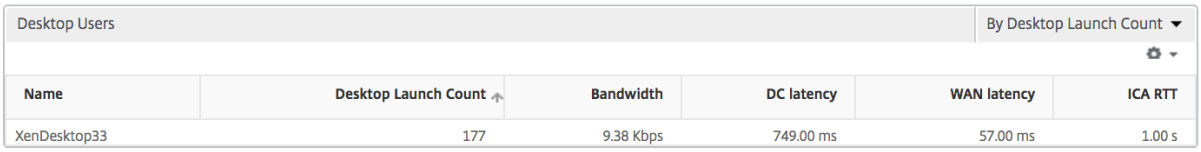
Gráfico de barras de usuarios El gráfico de barras Usuarios muestra los 5 usuarios principales en función de los siguientes criterios

- Ancho de banda
- Latencia de WAN
- Latencia de DC
- RTT de ICA



Informe Usuarios de escritorio Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

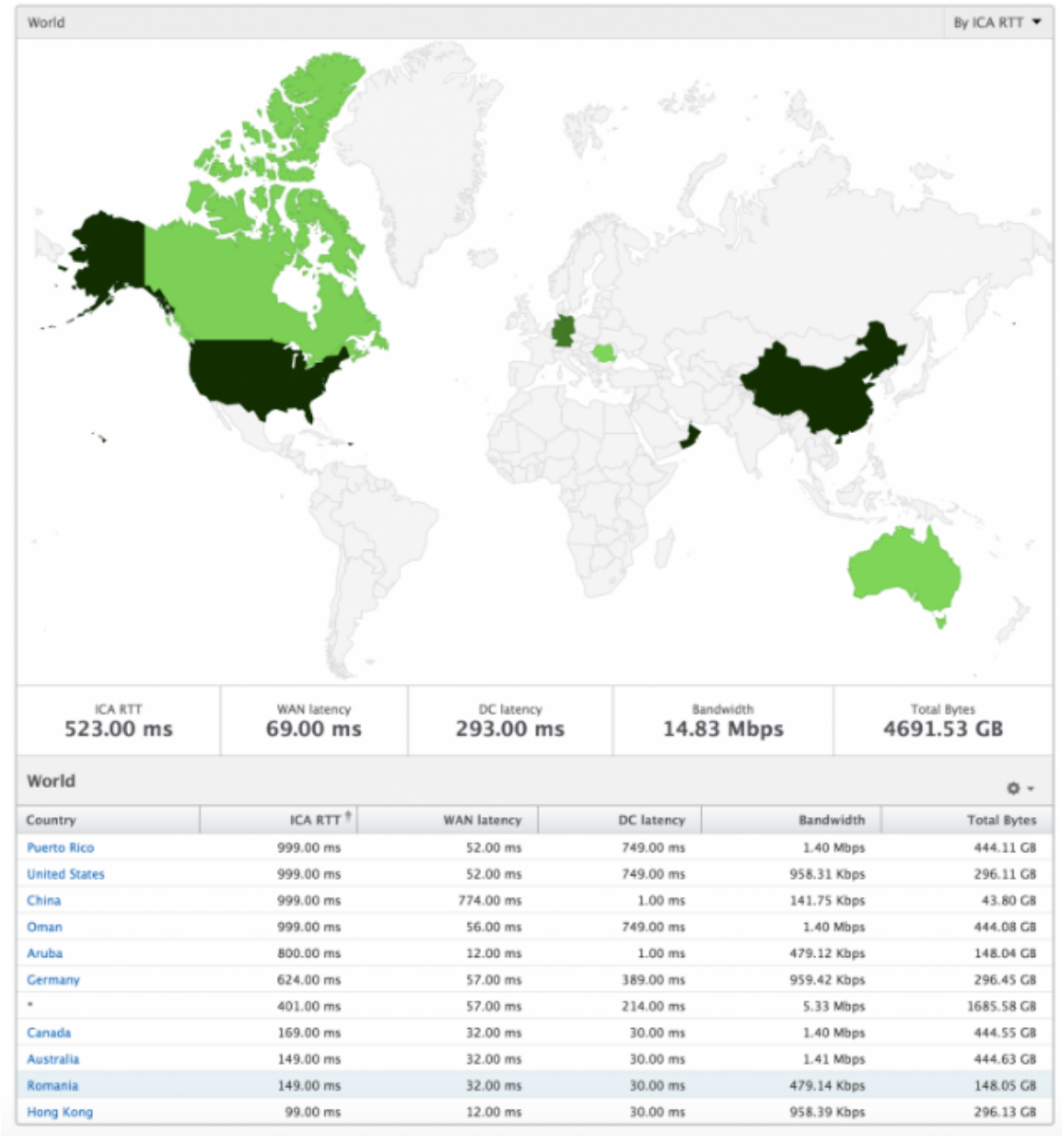
Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.



Visión del mundo La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión del mundo del sistema, profundizar en un país en particular y más en las ciudades, así como simplemente haciendo clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el mapa mundial de HDX insight, y la densidad de cada métrica se muestra en forma de mapa de calor:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Informes y métricas de vista de licencias

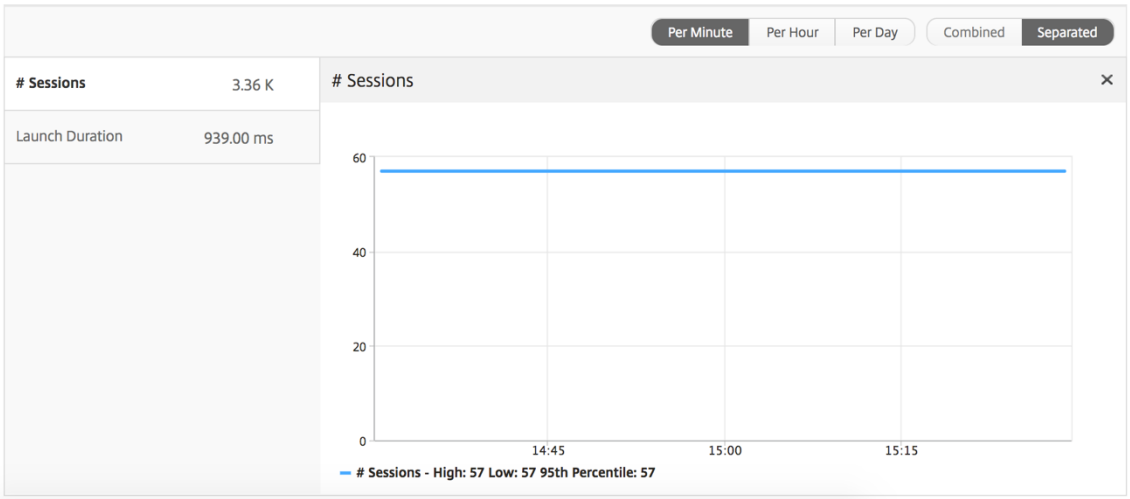
La vista de licencia proporciona detalles sobre la información de licencia de NetScaler Gateway.

Para navegar a la vista Licencia:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Licencias**.

Gráfico de líneas

Métricas	Descripción
Licencias en uso	Las licencias de CCU de NetScaler Gateway que se utilizan durante el plazo seleccionado. Cada recuento representa el número de sesiones de usuario. Esto es independiente de las sesiones de aplicaciones y escritorios iniciadas por ese usuario.
Total de licencias	Número total de licencias CCU de NetScaler Gateway disponibles para que el cliente las utilice.



Informe Umbral El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Licencia en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

Informes y métricas de vista de aplicaciones

January 30, 2024

Los informes y métricas de esta vista se centran en Citrix Virtual Apps.

Para desplazarse a la vista Aplicación:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.

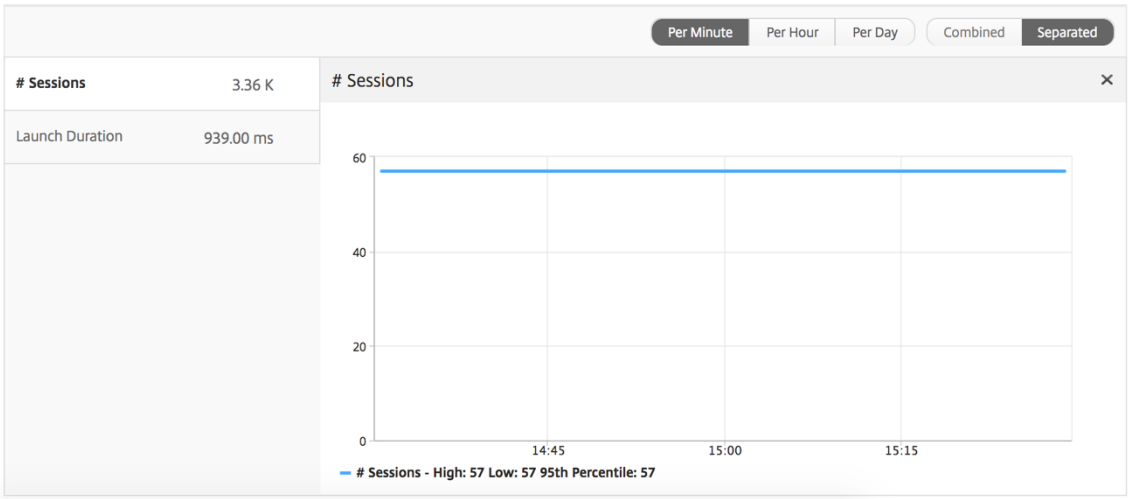
Vista resumida

La vista de resumen muestra los informes de todas las aplicaciones que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas e informes siguientes, a menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

Gráfico de líneas

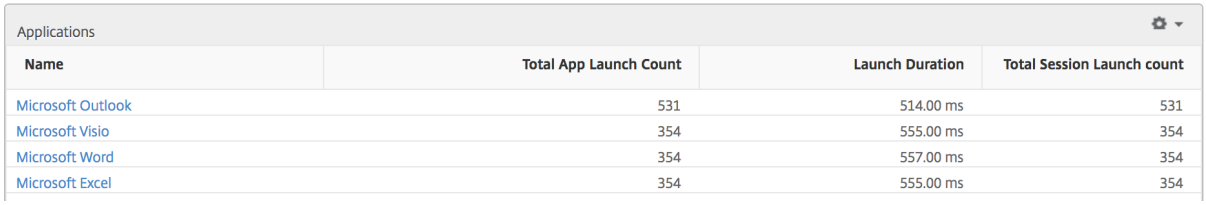
Métricas	Descripción
N.º de sesiones	Número total de sesiones durante un intervalo de tiempo determinado.
Duración de inicios	Promedio de tiempo necesario para iniciar una aplicación.



Informe de resumen de aplicaciones

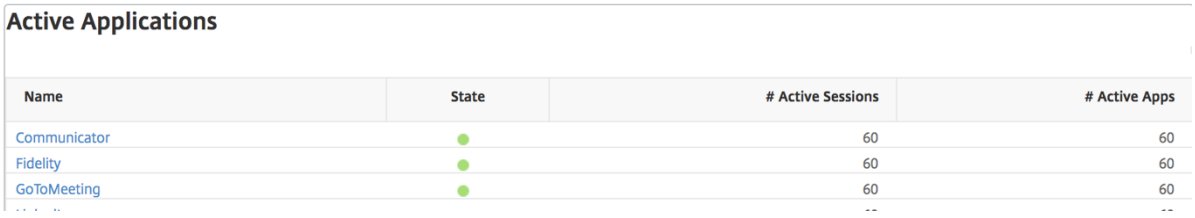
Métricas	Descripción
Nombre	Nombre de la aplicación virtual Citrix.

Métricas	Descripción
Recuento total de sesiones iniciadas	Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado.
Recuento total de aplicaciones iniciadas	Número total de Citrix Virtual Apps lanzadas durante el intervalo de tiempo especificado.
Duración de inicios	Tiempo medio necesario para iniciar Citrix Virtual Apps.



Informe de aplicaciones activas

Métricas	Descripción
Nombre	Nombre de la aplicación virtual Citrix.
State	Muestra el estado de la aplicación: Verde-Activa, Rojo-Inactiva
N.º de sesiones activas	Número de sesiones de usuario activas que utilizan esta aplicación durante un intervalo de tiempo determinado.
Aplicaciones #Active	Número de sesiones activas para esta aplicación.

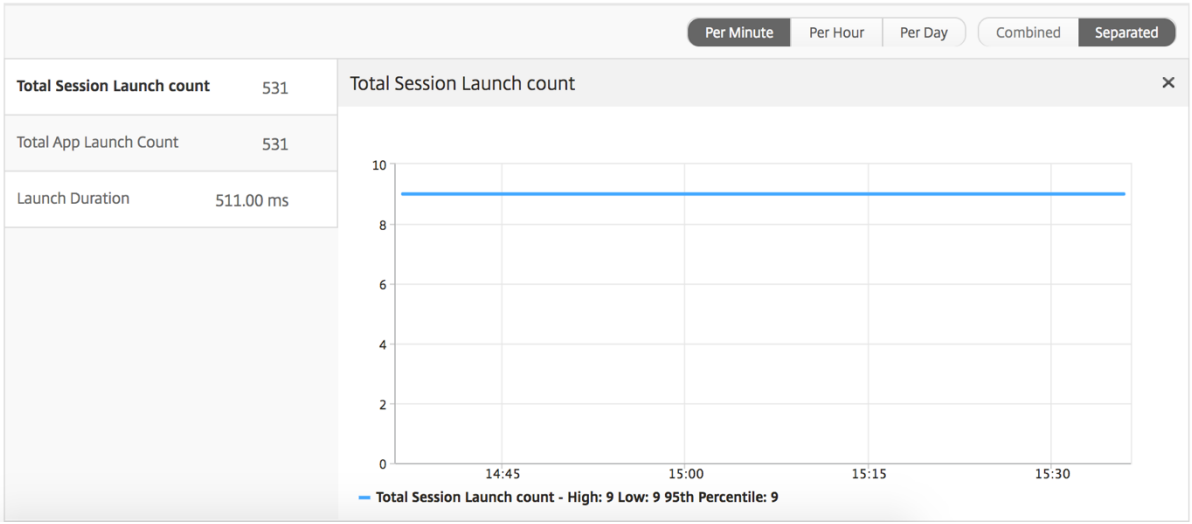


Informe Umbral

El informe de umbrales representa el recuento de umbrales incumplidos cuando la *entidad* es seleccionada como Solicitud en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

Gráfico de líneas

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
Duración de inicios	Promedio de tiempo necesario para iniciar una aplicación.



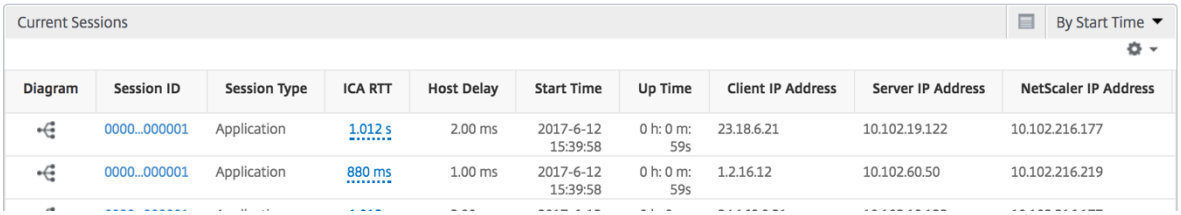
Informe sobre sesiones actuales

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa por los ADC de NetScaler causado por la red de servidores.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.

Métricas	Descripción
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor Backend/Citrix Virtual App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de receptor: Citrix Windows Client, etc.
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.

Métricas	Descripción
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Nombre de usuario	El nombre de usuario del usuario que accede a esta Citrix Virtual Apps en particular.
ID de sesión	Identificador único para la sesión de Citrix Virtual App.
Tipo de sesión	Será ‘‘Solicitud’’.
State	Estado de la sesión: verde para activa, rojo para inactiva.

Métricas	Descripción
Latencia de vulneración máxima	El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido.
Latencia de violación promedio	El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de "latencia L7 infringida".
Recuento de incumplimiento de umbral L7	Número de veces que se ha producido una infracción del umbral L7.
Latencia del lado del cliente L7	Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler. Esta métrica es útil en caso de que haya dispositivos que no sean de Citrix en la ruta de entrega.
Latencia L7 del lado del servidor	La latencia L7 promedio observada entre el dispositivo NetScaler y Citrix Virtual Apps. Esta métrica es útil en caso de que haya dispositivos que no sean de Citrix en la ruta de entrega.



Vista de sesión por aplicación

La vista por sesión de aplicación muestra los informes de una sesión de aplicación seleccionada concreta.

Para ver los informes de sesión:

1. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.
2. Seleccione un usuario concreto del informe resumido de la aplicación.
3. Se seleccionó una sesión del informe de sesiones actuales.

Gráfico de líneas

Métricas	Descripción
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Evento de ventana cero en el lado del servidor	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.

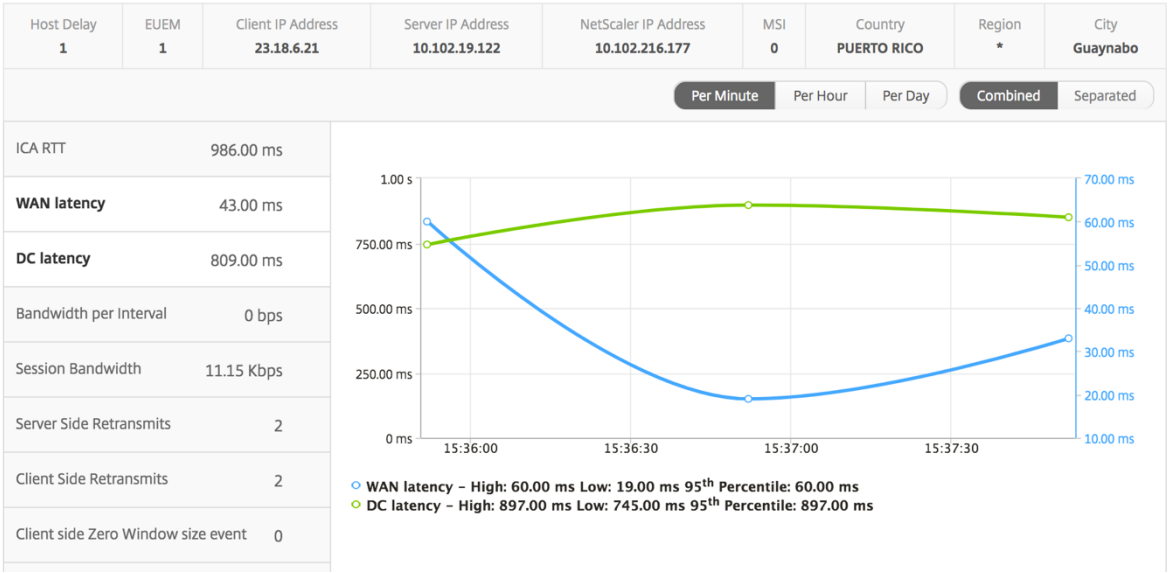
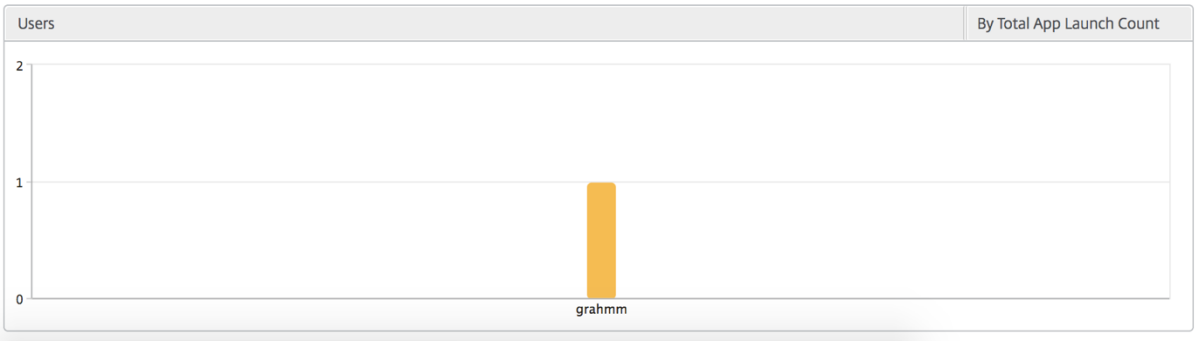


Gráfico de barras de usuario

El gráfico de barras del usuario representa a los usuarios que han iniciado sesión en esta aplicación en particular.



Informes y métricas de Desktop View

January 30, 2024

Los informes y las métricas de esta vista se centran en los escritorios virtuales de Citrix.

Para desplazarse a la vista Escritorio:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX InsightEscritorio**.

Vista resumida

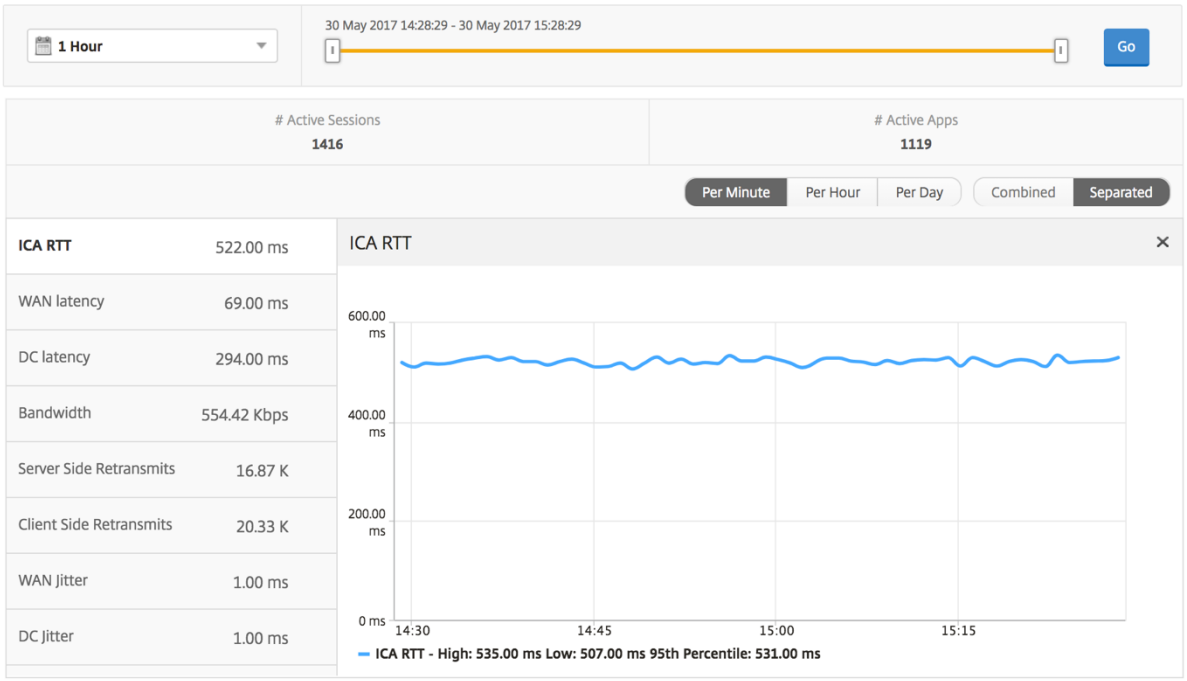
La vista de resumen muestra los informes de todos los Citrix Virtual Desktops que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas e informes siguientes, a menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

Gráfico de líneas

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual App.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.

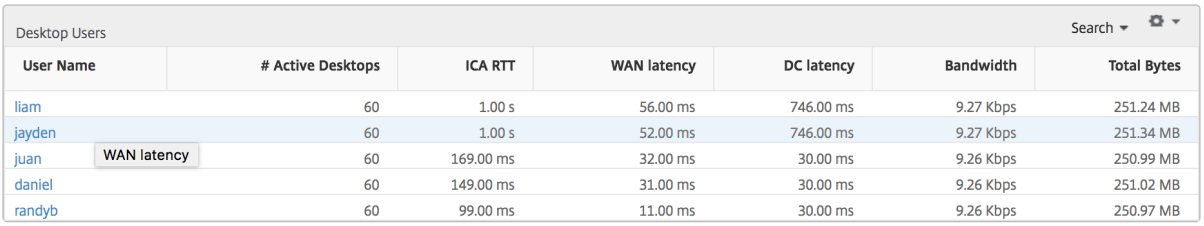
Métricas	Descripción
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe de resumen de escritorio

Métricas	Descripción
Sesiones activas	Número total de sesiones activas de Citrix Virtual Desktop durante un intervalo de tiempo determinado.
Escritorios activos	Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado.

Métricas	Descripción
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.



Informe Umbral

El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Escritorio en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

Vista por escritorio

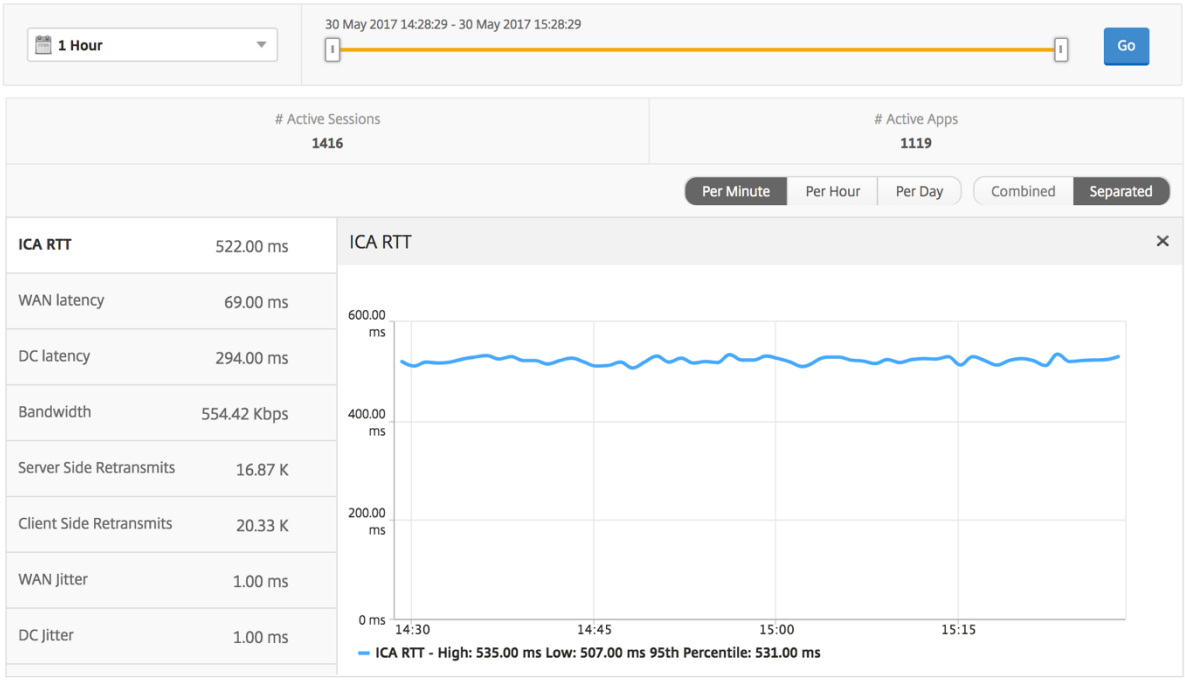
Por vista de escritorio proporciona informes detallados de la experiencia del usuario final para un escritorio virtual de Citrix seleccionado.

Para navegar a la vista Escritorio en particular:

1. Vaya a **Analytics > HDX Insight > Escritorio**.
2. Seleccione un **escritorio** concreto en el **informe de resumen de escritorios**.

Gráfico de líneas

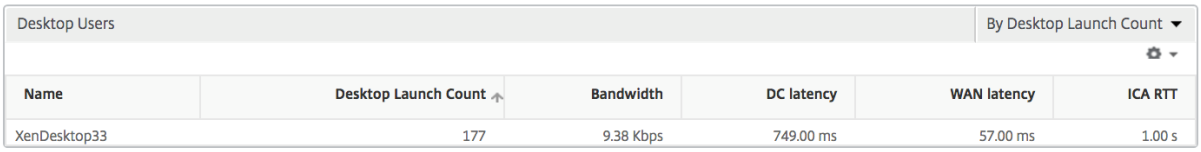
Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe de usuarios de equipos de escritorio

Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.



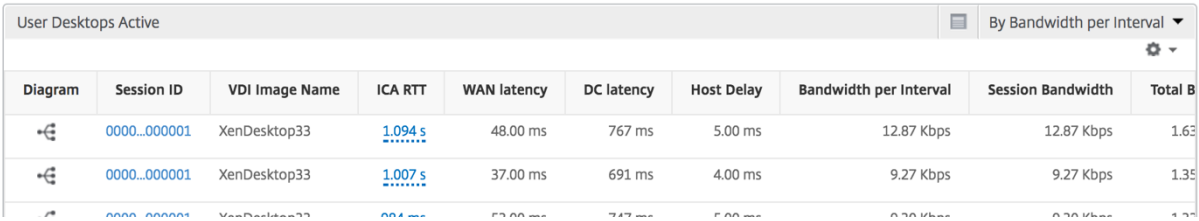
Informe activo/inactivo de escritorios de usuario

Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa por los ADC de NetScaler causado por la red de servidores.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor Backend/Citrix Virtual App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de receptor: Citrix Windows Client, etc.
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.

Métricas	Descripción
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.

Métricas	Descripción
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Nombre de la imagen VDI	Nombre del Citrix Virtual Desktops al que está conectado el usuario
Diagrama	



Vista por sesión de escritorio

Por vista de sesión de escritorio proporciona informes para una determinada sesión de Citrix Virtual Desktops seleccionada.

Para desplazarse a la vista de sesión de Escritorio:

1. Vaya a **Analytics** > **HDX InsightEscritorio**.
2. Seleccione un escritorio concreto en el **informe de resumen de escritorios**.
3. Seleccione una sesión del informe de sesiones actuales.

Gráfico cronológico

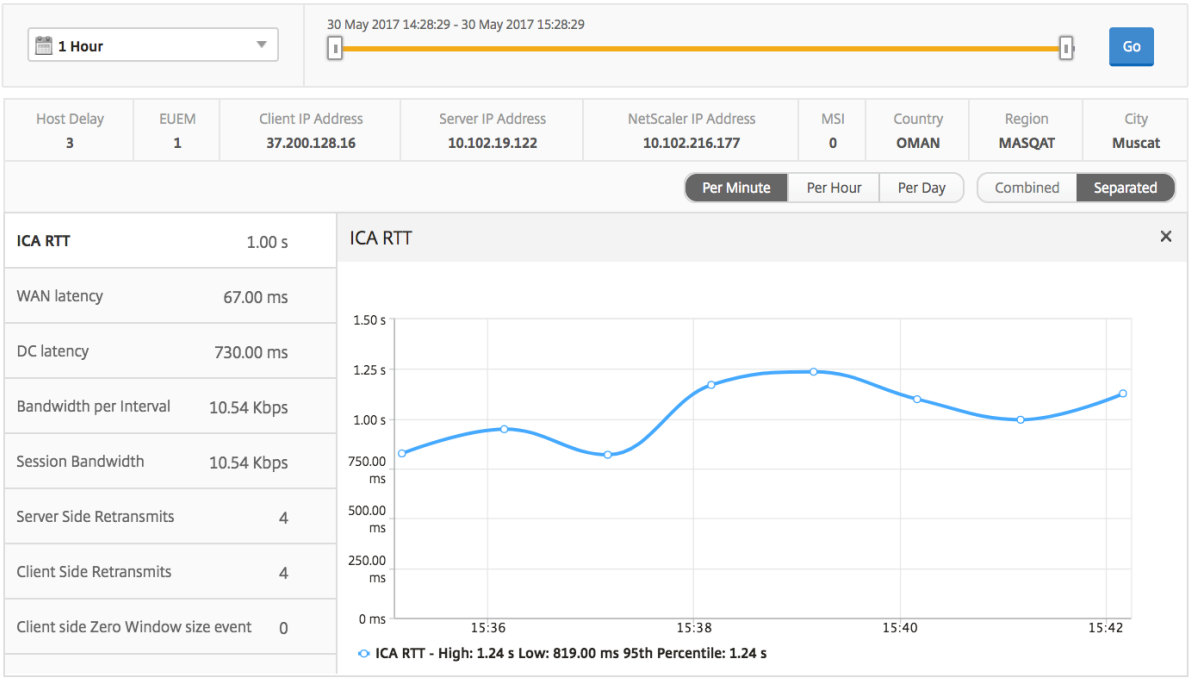
La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

Para ver las métricas de la sesión de un usuario seleccionado:

1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Select un usuario concreto en la sección **Informe de resumen de usuario**.
3. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

Métricas	Descripción
Reconexiones de sesión	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
Recuento de ACR	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.

Métricas	Descripción
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.



Informe de sesiones de escritorio relacionadas

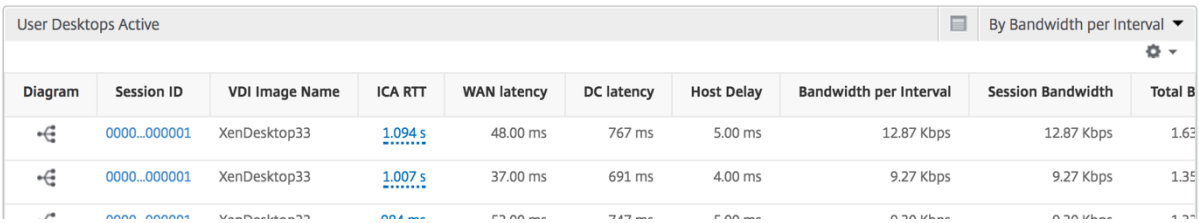
Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.

Métricas	Descripción
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa por los ADC de NetScaler causado por la red de servidores.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor Backend/Citrix Virtual App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de receptor: Citrix Windows Client, etc.
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.

Métricas	Descripción
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.

Métricas	Descripción
Nombre de la imagen VDI	Nombre del Citrix Virtual Desktops al que está conectado el usuario



Informes y métricas de visualización de usuarios

January 30, 2024

Los informes y las métricas de esta vista se muestran por usuario de Citrix Virtual Apps and Desktops.

Para navegar a la vista Usuarios:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**

Vista de resumen

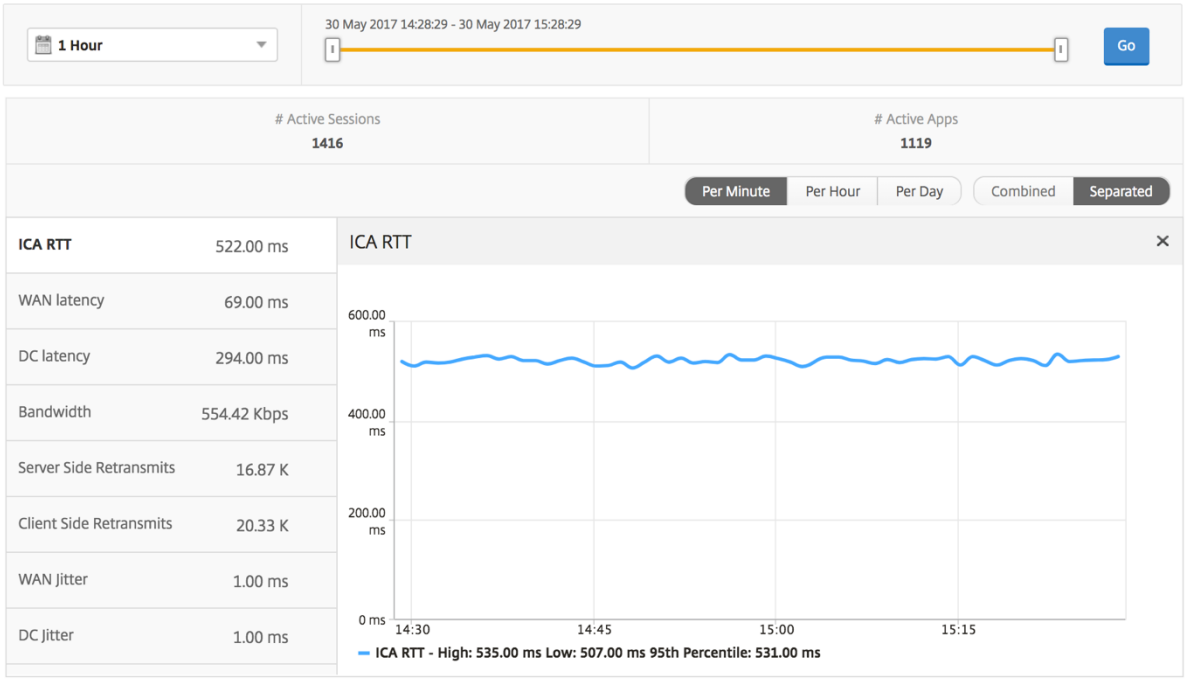
La vista de resumen muestra los informes de todos los usuarios que han iniciado sesión durante la línea de tiempo seleccionada. Todas las métricas o informes de esta vista muestran los valores correspondientes para el período de tiempo seleccionado, a menos que se especifique lo contrario.

Para cambiar el período de tiempo seleccionado:

1. Usa el menú desplegable del período de tiempo o el control deslizante de tiempo para establecer el intervalo de tiempo deseado.
2. Haga clic en **Ir**.

Gráfico de líneas

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe de resumen de usuarios

A continuación se presentan las métricas específicas de este informe.

Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual App.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.

Métricas	Descripción
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
Recuento total de aplicaciones iniciadas	Total de aplicaciones lanzadas por el usuario durante el período de tiempo seleccionado.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Escritorios activos	Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado.

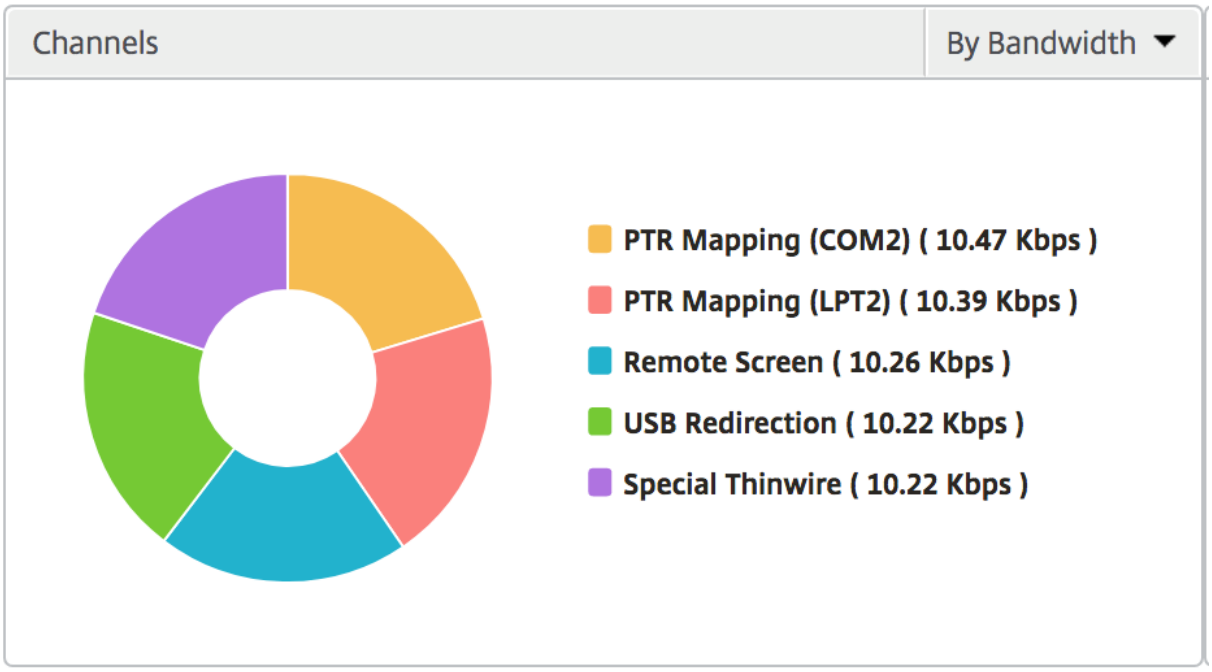
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

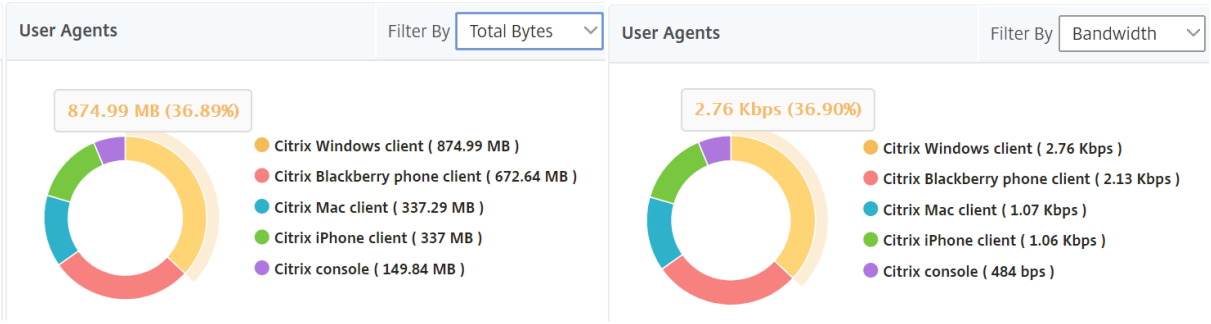
Canales

Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Agentes de usuario

Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada punto final en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Recuento de Infracción de Umbrales

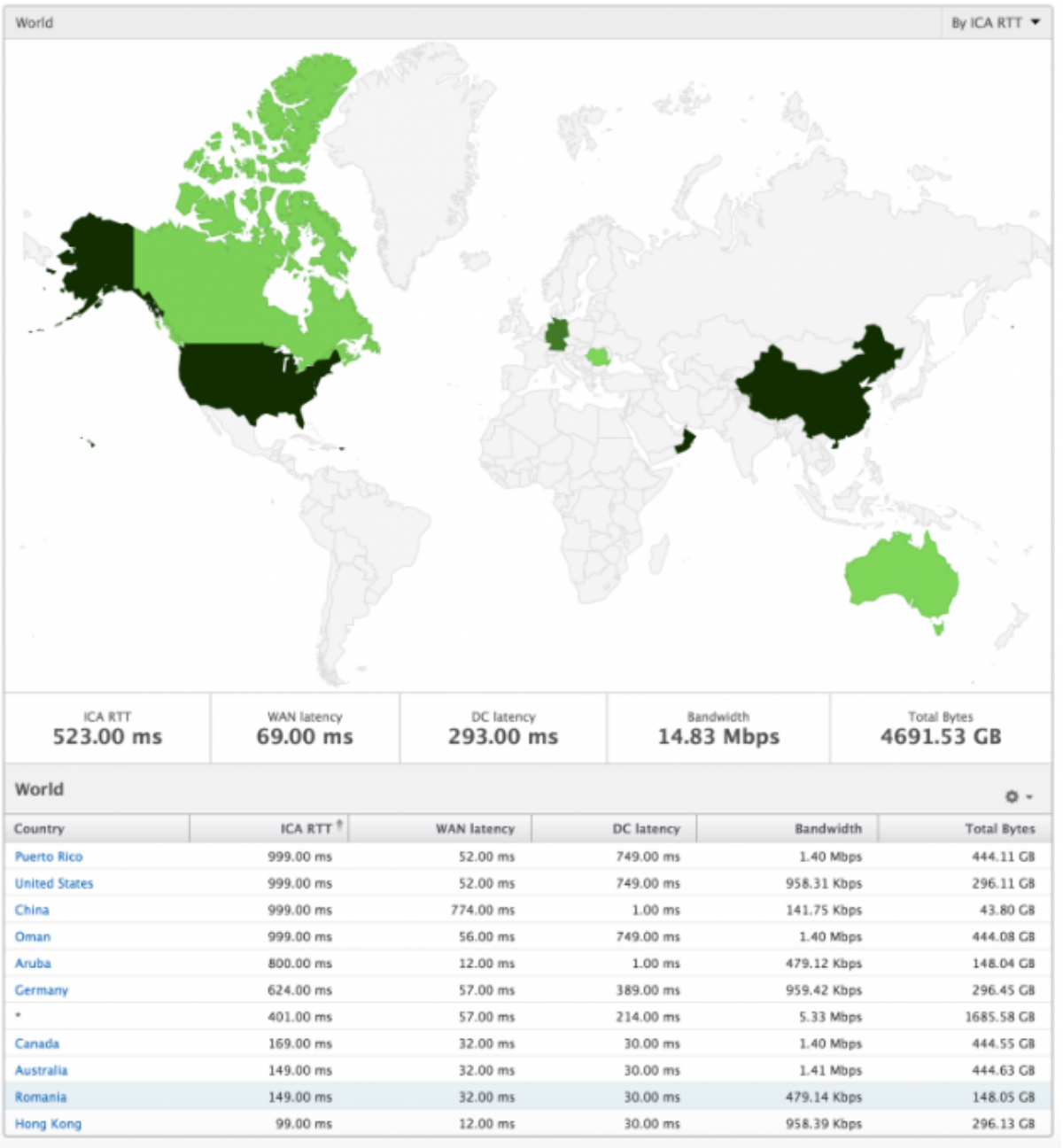
Las métricas de recuento de infracciones de Umbrales representan el recuento de umbrales incumplidos en el período de tiempo seleccionado. Para obtener más información, consulta cómo crear umbrales y alertas.

Mapa del mundo

La vista de mapa mundial en HDX Insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión del mundo del sistema, profundizar en un país en particular y más en las ciudades, así como simplemente haciendo clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el mapa mundial de HDX insight, y la densidad de cada métrica se muestra en forma de mapa de calor:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Por vista de usuario

La vista por usuario proporciona informes detallados de la experiencia del usuario final para cualquier usuario seleccionado en particular.

Para navegar a métricas específicas de usuario:

1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Seleccione un usuario concreto en el informe Resumen de usuarios.

Gráfico de líneas

El gráfico de líneas muestra el resumen de todas las métricas del usuario seleccionado en particular durante el período de tiempo seleccionado.

Informe de sesiones actuales/terminadas

Este informe es pertinente para todas las sesiones de usuario actuales/terminadas del usuario seleccionado. Estas métricas se pueden ordenar por hora de inicio, reconexiones de sesión y recuento de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa por los ADC de NetScaler causado por la red de servidores.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Bytes por intervalo	Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular.
Hora de inicio	Hora de inicio de sesión.
Tiempo de actividad	Duración de la sesión.
Dirección IP del cliente	IP del usuario final.
Dirección IP del servidor	IP del servidor Backend/Citrix Virtual App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de receptor: Citrix Windows Client, etc.
Versión del cliente	Versión receptor.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.

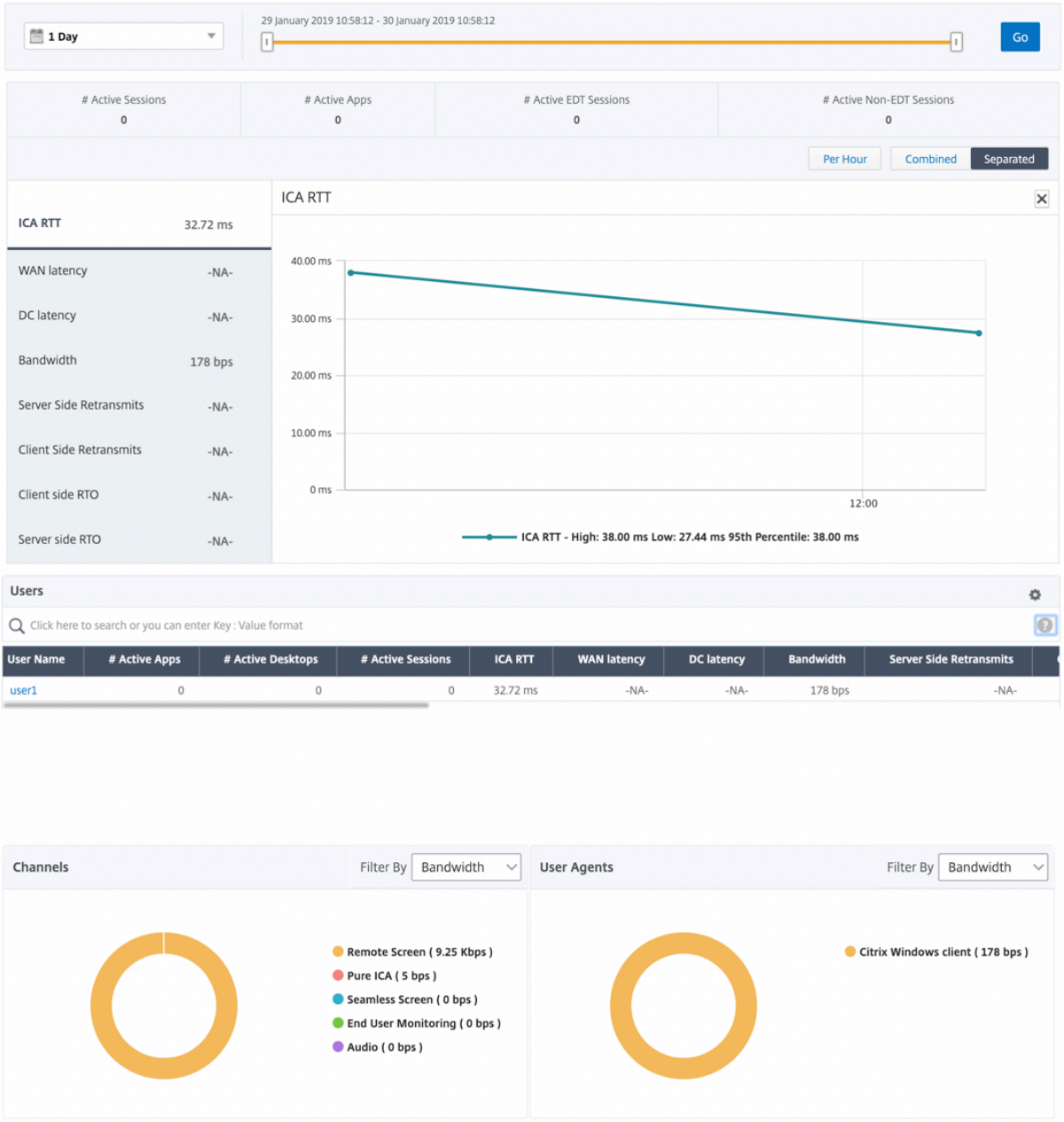
Métricas	Descripción
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que se estableció la sesión.
Region	Región desde la que se estableció la sesión.
City	Ciudad desde la que se estableció la sesión.
Estado USB	Activo/Inactivo -Verde/Rojo.
Número de instancias USB aceptadas	El recuento de instancias USB aceptadas.
Número de instancias USB rechazadas	El recuento de instancias USB rechazadas.
Número de instancias USB detenidas	Se detuvo el recuento de instancias USB.
Nombre de host del cliente	El nombre de host del cliente.
Recuento de failover de HA	Número de veces que se produjo la conmutación por error de HA
Motivo de rescisión	Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Total de bytes	Total de bytes consumidos por el usuario durante el período de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.

Métricas	Descripción
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.

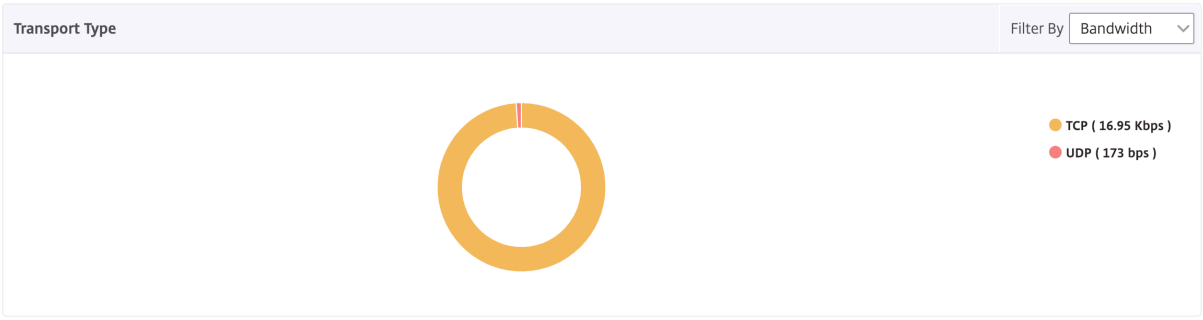
Soporte para EDT en HDX Insight

NetScaler Application Delivery Management (ADM) ahora admite el transporte de datos ilustrados (EDT) para mostrar análisis para HDX Insight. Es decir, ADM ahora admite los protocolos UDP y TCP. La compatibilidad de EDT con NetScaler Gateway garantiza una experiencia de usuario de alta definición durante la sesión de los escritorios virtuales para los usuarios que ejecutan Citrix Receiver

HDX Insight ahora muestra el número de sesiones de EDT y de sesiones que no son de EDT como parte del informe de sesiones activas. La tabla Usuarios muestra un informe detallado de todos los usuarios del sistema. La tabla muestra métricas como la latencia de WAN, la latencia de DC, las retransmisiones, los RTO y algunas de estas métricas no están disponibles para los usuarios que tienen sesiones de EDT, ya que se calculan a partir de la pila TCP actualmente. Por lo tanto, aparecerán como «NA».

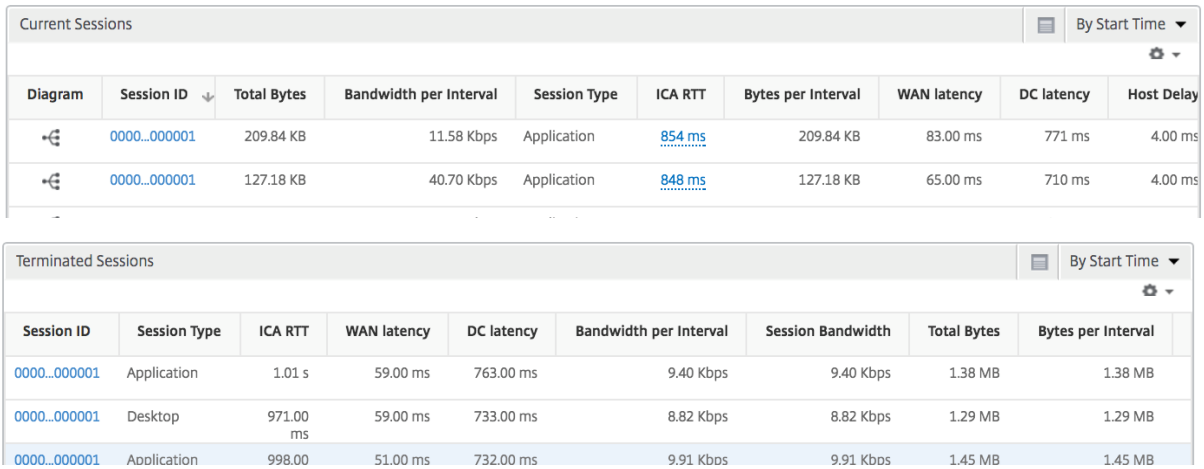


Se ha introducido un nuevo gráfico de anillos que permite ver el ancho de banda consumido por el usuario y también el número total de bytes según el tipo de protocolo utilizado por los usuarios.



Métricas de HDX Insight disponibles en NetScaler ADM 12.0 y versiones posteriores:

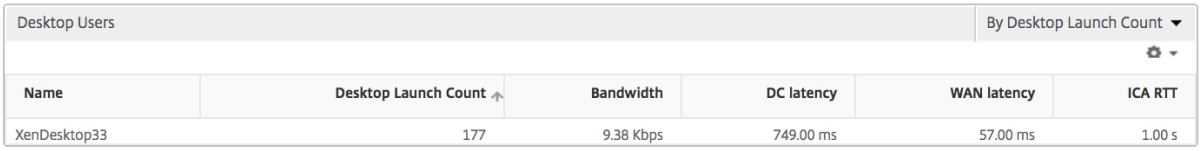
Latencia del lado del cliente L7	Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler. Esta métrica es útil en caso de que haya dispositivos que no sean de Citrix en la ruta de entrega.
Latencia L7 del lado del servidor	La latencia media de L7 observada entre el dispositivo NetScaler y Citrix Virtual App. Esta métrica es útil en caso de que haya dispositivos que no sean de Citrix en la ruta de entrega.
Latencia de vulneración máxima	El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido.
Latencia de violación promedio	El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de "latencia L7 infringida".
Recuento de incumplimiento de umbral L7	Número de veces que se ha producido una infracción del umbral L7.



Usuarios de escritorio

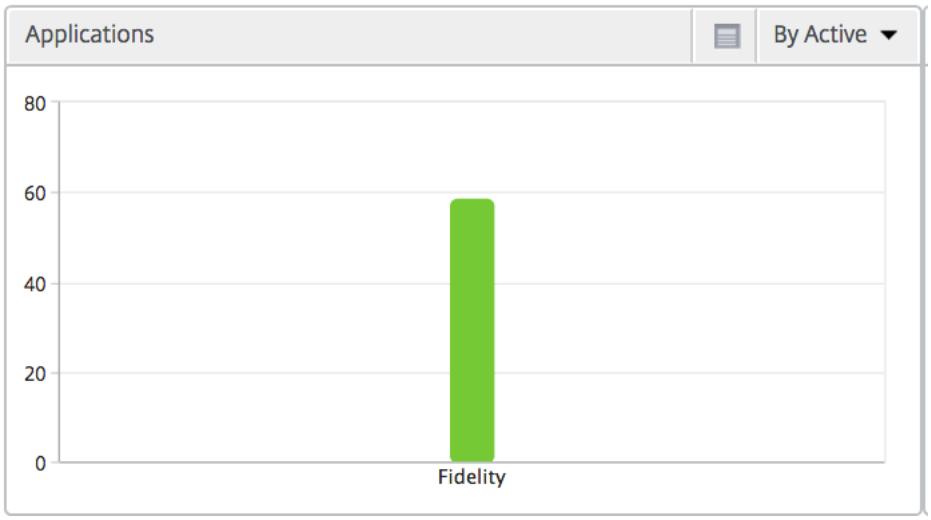
Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.



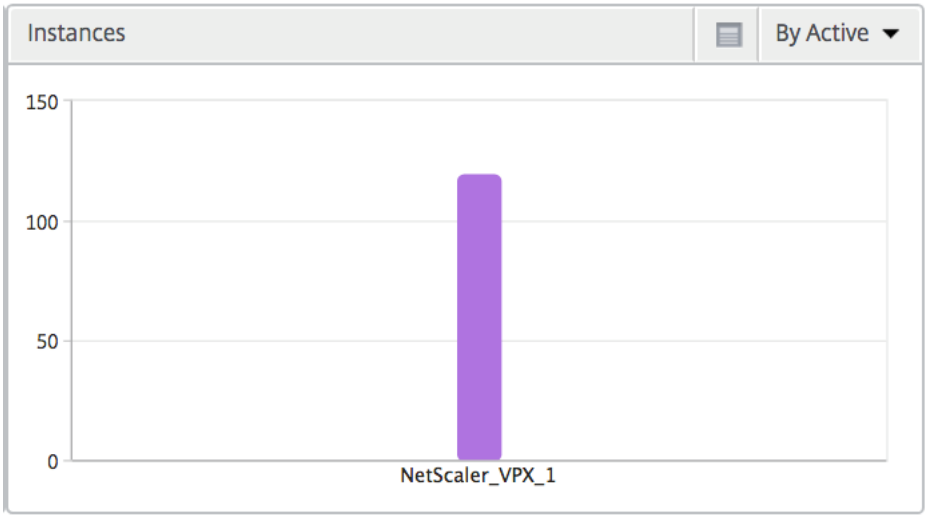
Aplicaciones

Un gráfico de barras que representa las aplicaciones ordenadas por Activas, recuento total de inicios de sesiones, recuento total de inicios de aplicaciones y duración del lanzamiento.



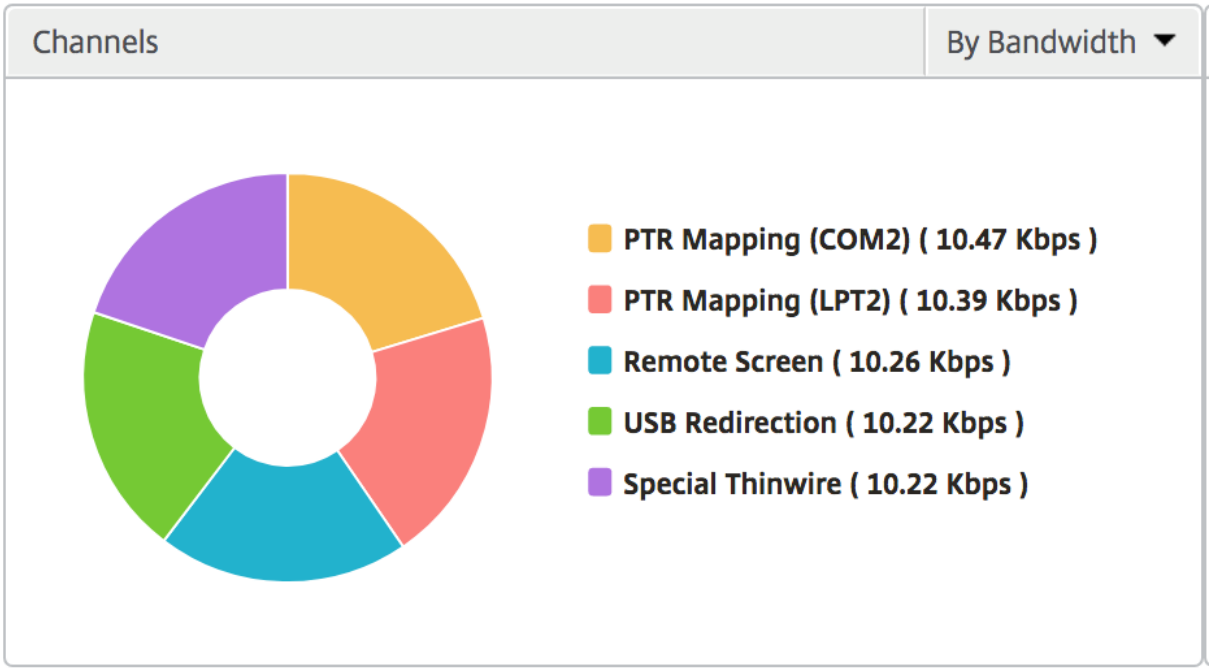
Instancias

Un gráfico de barras que representa las instancias de NetScaler ordenadas por aplicaciones activas y totales



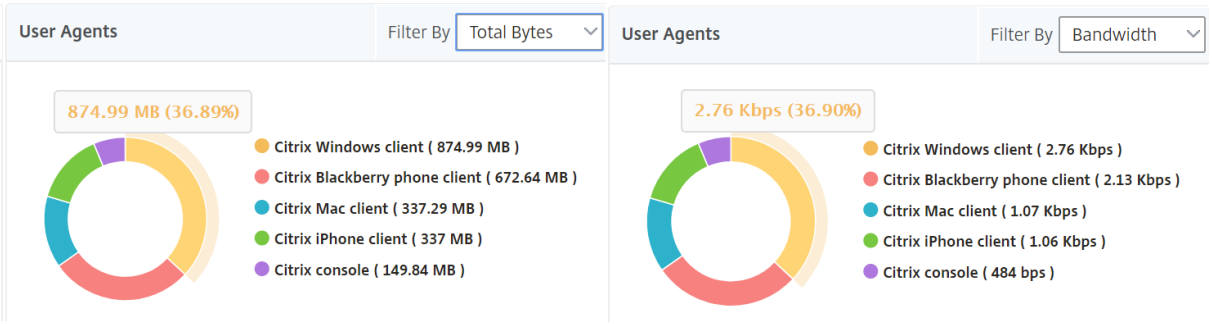
Canales

Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Agentes de usuario

Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada punto final en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Vista de sesión por usuario

La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

Para ver las métricas de la sesión de un usuario seleccionado:

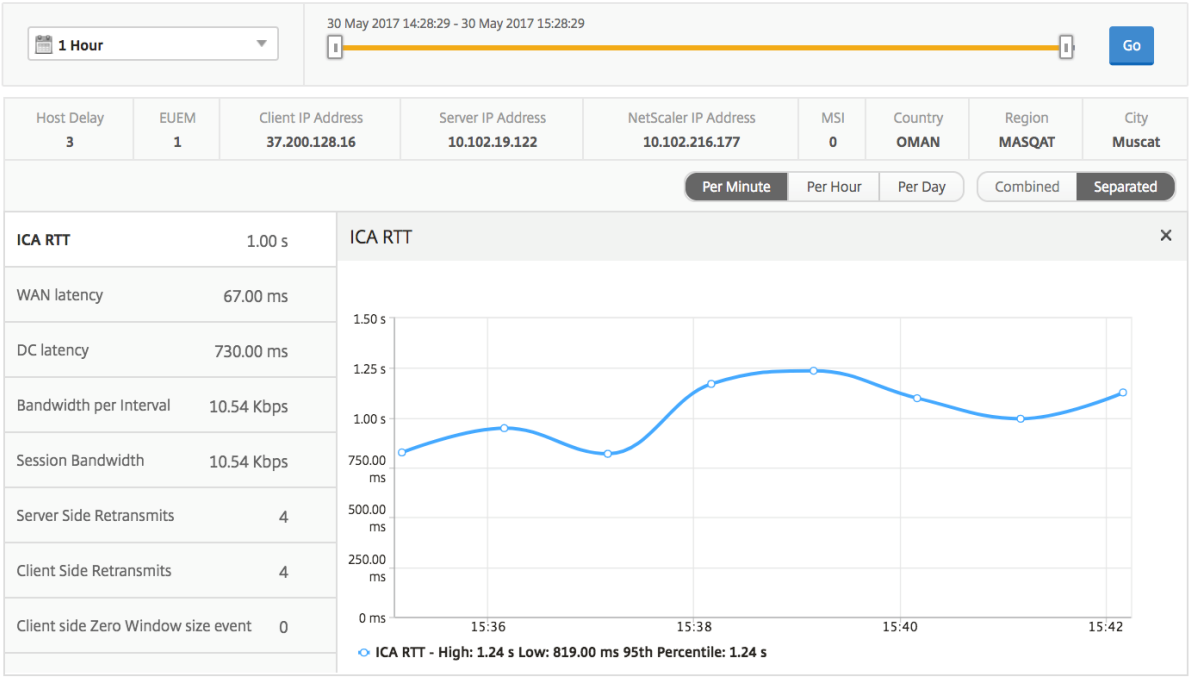
1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Select un usuario concreto en la sección **Informe de resumen de usuario**.

3. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

Gráfico cronológico

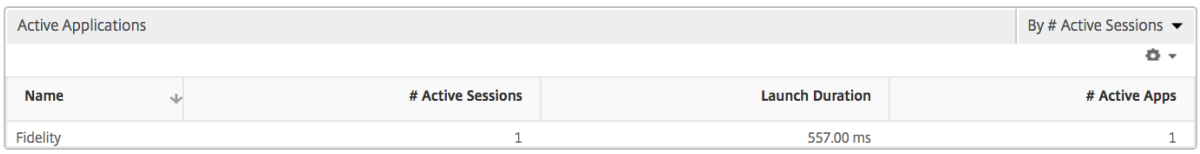
Métricas	Descripción
Reconexiones de sesión	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
Recuento de ACR	Este número indica el recuento de sesiones activas de Citrix Virtual App.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Ancho de banda de la sesión	El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor backend.
Retransmisiones del lado del cliente	El número de paquetes retransmitidos en la conexión entre NetScaler y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones.
RTO rápido del lado del cliente	Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler y el usuario final.
RTO rápido del lado del servidor	Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Ancho de banda por intervalo	El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular.
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.

Métricas	Descripción
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana TCP cero.



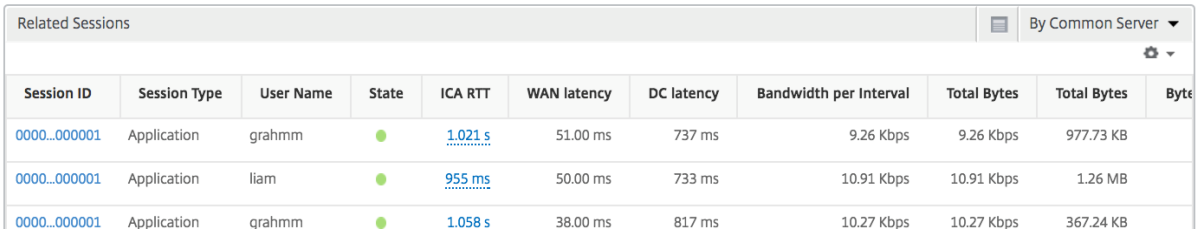
Aplicación activa

La sección Aplicaciones activas muestra las aplicaciones activas del usuario seleccionado. Estas aplicaciones también se pueden ordenar por número de sesiones activas y duración de inicio.



Sesiones relacionadas

La sección Sesiones relacionadas muestra las sesiones relacionadas de las sesiones del usuario seleccionado. La relación se puede seleccionar como servidores comunes o común de NetScaler.



Informes y métricas de vista de instancias

January 30, 2024

Los informes y las métricas de la vista de instancias se centran en las instancias de NetScaler.

Para desplazarse a la vista Instancia:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX InsightInstancias**.

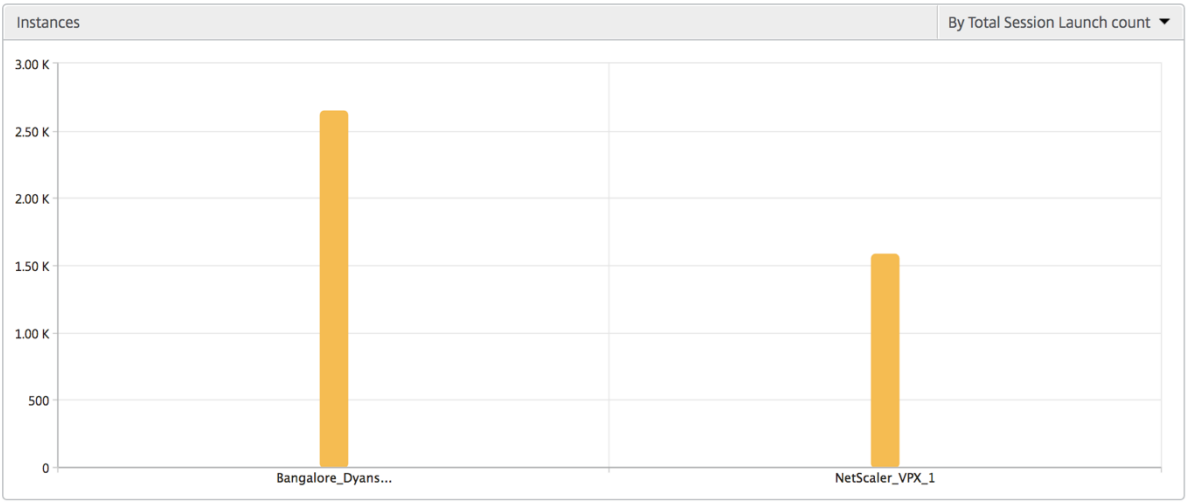
Vista resumida de la instancia

Esta vista se denomina vista de resumen, ya que muestra los informes de todas las instancias de NetScaler que se agregan a NetScaler ADM.

Todas las métricas/informes a continuación, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

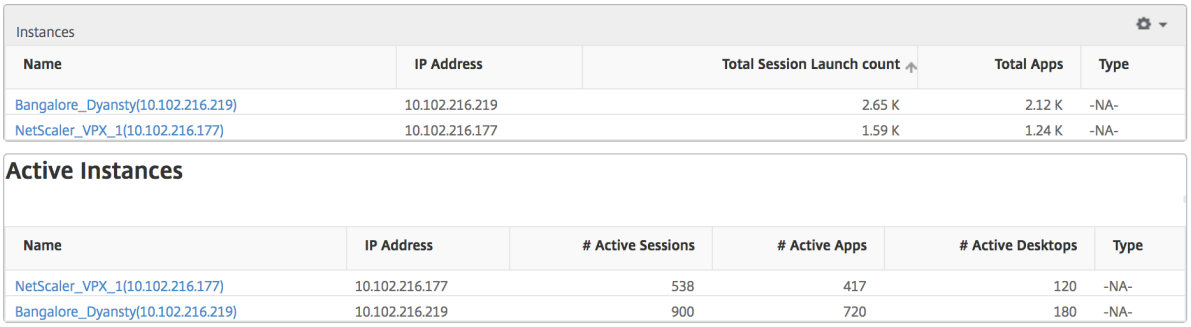
Gráfico de barras de instancias

Este gráfico muestra la instancia en comparación con el recuento total de inicios de sesión y el total de aplicaciones, que se pueden seleccionar en el menú desplegable de la parte superior derecha del lienzo gráfico.



Informe resumido de instancias/instancias activas

Métricas	Descripción
Nombre	Nombre de host de la instancia de NetScaler.
Dirección IP	Dirección IP de NetScaler.
Recuento total de sesiones iniciadas	Número total de sesiones de usuario únicas creadas durante un intervalo de tiempo determinado.
Total de aplicaciones	Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado.
Tipo	N/D



Informe Umbral

El informe Umbral representa el recuento de umbrales incumplidos cuando se selecciona la *entidad* como Instancia en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

Flujos omitidos

Un flujo omitido es un registro que omitió el análisis de la conexión ICA. Esto puede deberse a varios motivos, como el uso de versiones no compatibles de Citrix Virtual Apps and Desktops, una versión no compatible del receptor o del tipo de receptor, etc. Esta tabla muestra la dirección IP y el recuento de flujo omitido. Estos receptores pueden no ser parte de receptores en la lista blanca; por lo tanto, estas sesiones se omiten de la supervisión.

Visite **¡Error! La referencia de hipervínculo no es válida.** para obtener más información sobre cuestiones relacionadas con el análisis de ICA.


Skipped Flows

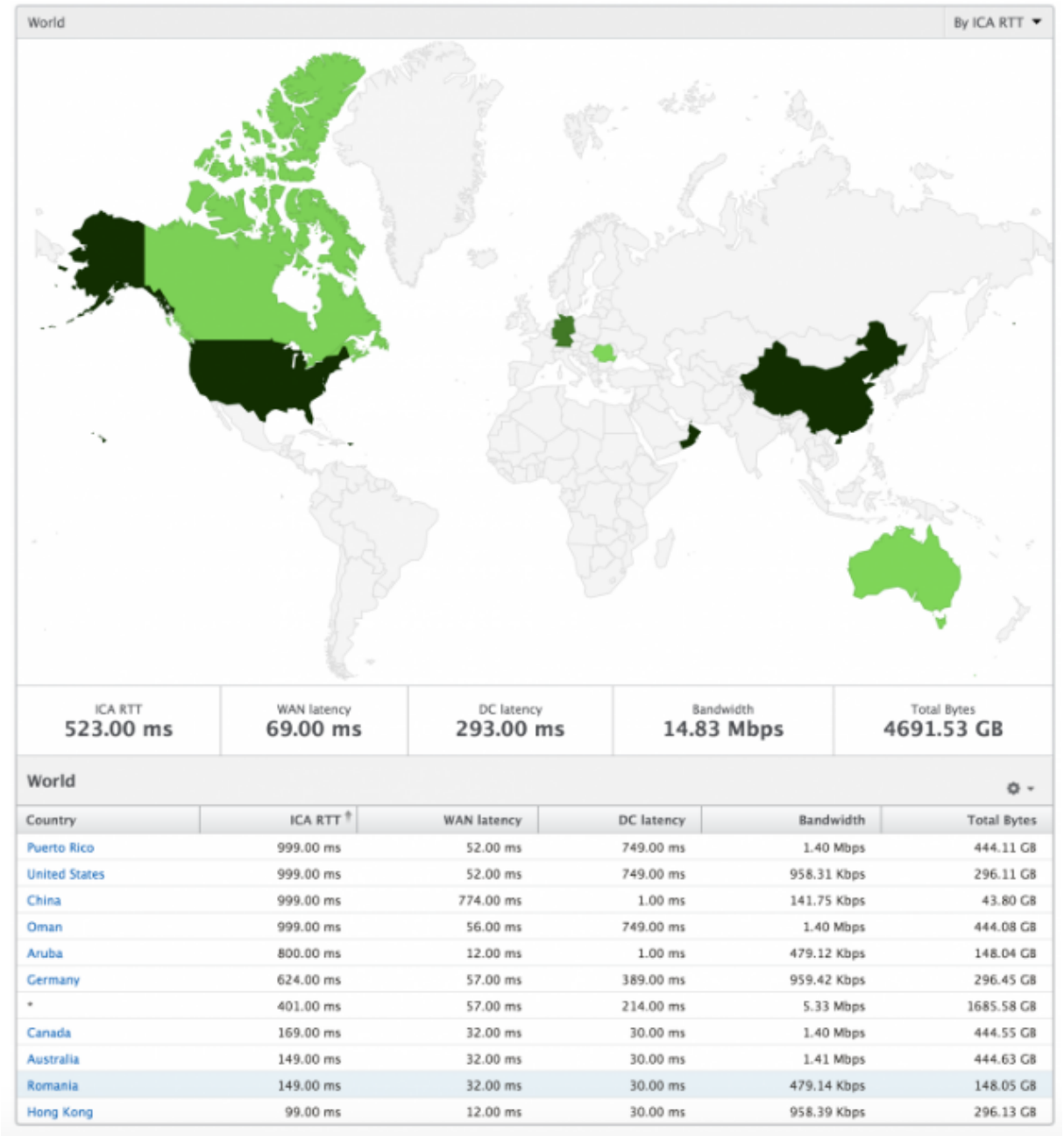
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

Visión del mundo

La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión del mundo del sistema, profundizar en un país en particular y más en las ciudades, así como simplemente haciendo clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el mapa mundial de HDX insight, y la densidad de cada métrica se muestra en forma de mapa de calor:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Vista por instancia

Por vista de instancia proporciona informes detallados sobre la experiencia del usuario final para una instancia específica de NetScaler seleccionada.

Para desplazarse a la vista Instancia:

1. Vaya a **Analytics** > **HDX InsightInstancias**.
2. Seleccione una instancia en particular del **Informe resumido de instancias**.

Gráfico de líneas

Métricas	Descripción
Dirección IP	Representa la dirección IP de NetScaler de la instancia seleccionada.
Recuento total de sesiones iniciadas	Número total de sesiones activas de Citrix Virtual Apps durante el intervalo de tiempo dado.
Total de aplicaciones	Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado.

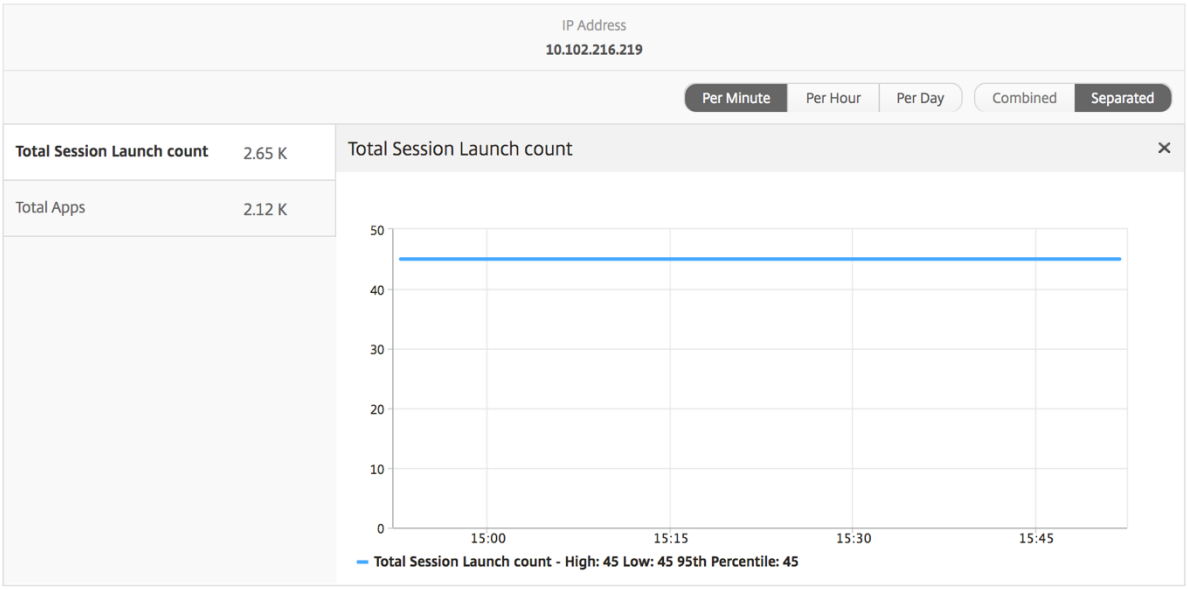


Gráfico de barras de aplicaciones

Muestra las 5 aplicaciones principales basadas en los siguientes criterios: Por aplicaciones activas, recuento total de inicios de sesión, recuento total de inicios de aplicación o duración de los inicios.

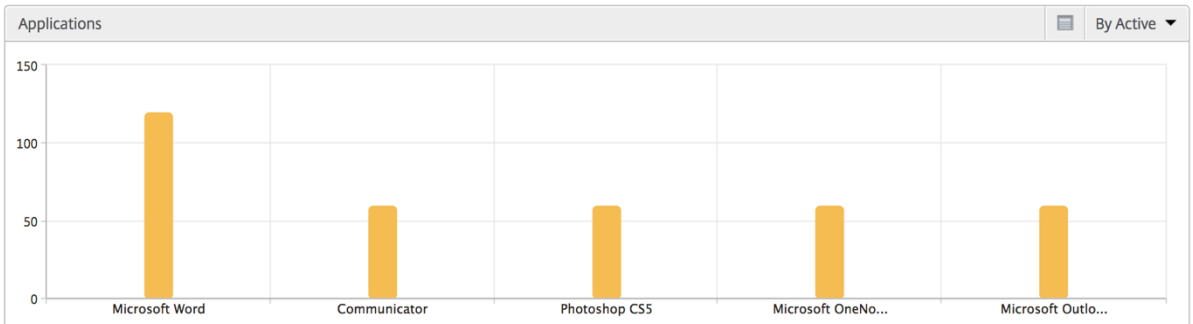
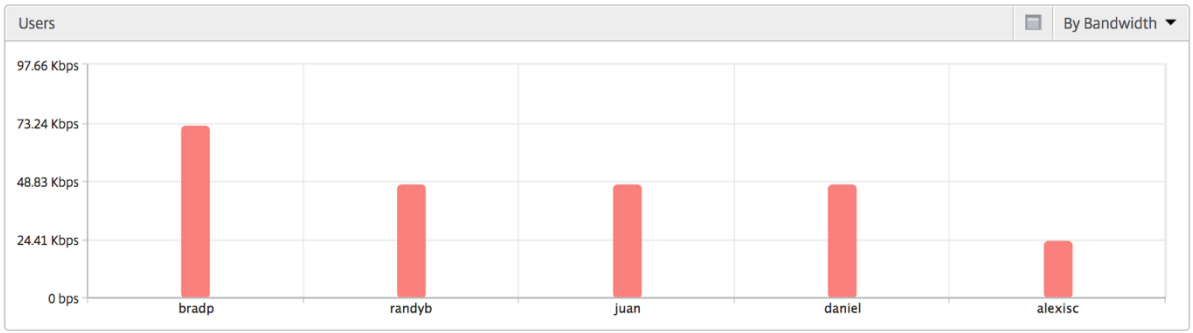


Gráfico de barras de usuarios

El gráfico de barras Usuarios muestra los 5 usuarios principales en función de los siguientes criterios

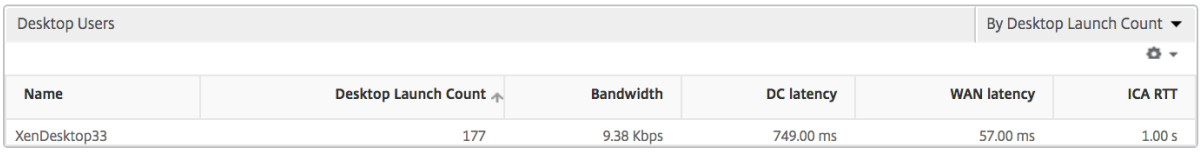
- Ancho de banda
- Latencia de WAN
- Latencia de DC
- RTT de ICA



Informe de usuarios de equipos de escritorio

Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta los servidores back-end.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, de NetScaler al usuario final.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente.

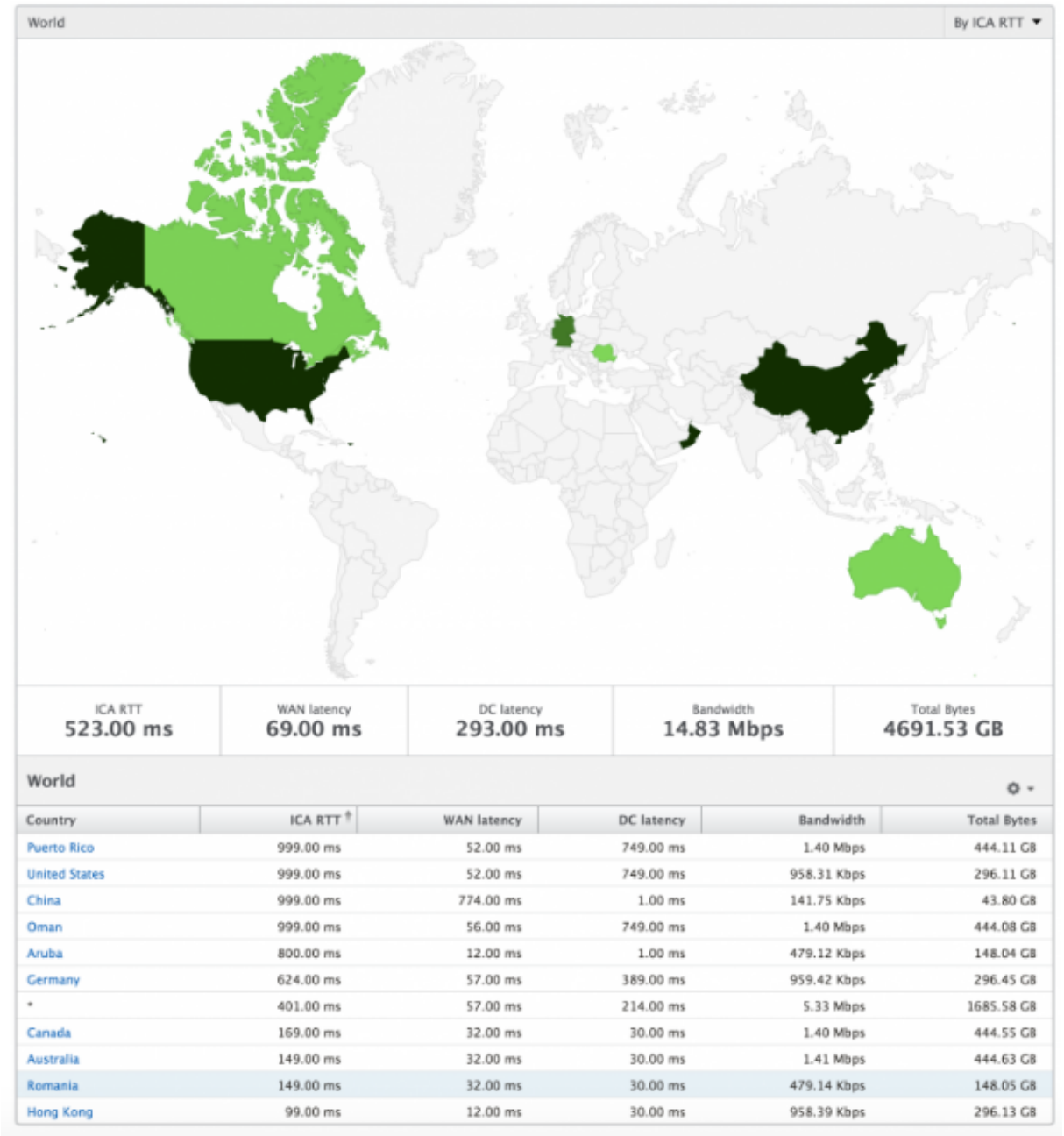


Visión del mundo

La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión del mundo del sistema, profundizar en un país en particular y más en las ciudades, así como simplemente haciendo clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el mapa mundial de HDX insight, y la densidad de cada métrica se muestra en forma de mapa de calor:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

Informes y métricas de vista de licencias

January 30, 2024

La vista de licencia proporciona detalles sobre la información de licencia de NetScaler Gateway.

Para navegar a la vista Licencia:

1. Inicie sesión en su NetScaler MA Service con un navegador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Licencias**.

Gráfico de líneas

Métricas	Descripción
Licencias en uso	Las licencias de CCU de NetScaler Gateway que se utilizan durante el plazo seleccionado. Cada recuento representa el número de sesiones de usuario. Esto es independiente de las sesiones de aplicaciones y escritorios iniciadas por ese usuario.
Total de licencias	Número total de licencias CCU de NetScaler Gateway disponibles para que el cliente las utilice.

! [imagen localizada] (/en-us/netscaler-application-delivery-management-software/media hdx-line-chart.png)

Informe Umbral

El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Licencia en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

Solucionar problemas de HDX Insight

January 30, 2024

Si la solución HDX Insight no funciona según lo esperado, es posible que el problema se deba a uno de los siguientes motivos. Consulte las listas de comprobación de las secciones correspondientes para la solución de problemas.

- Configuración de HDX Insight.
- Conectividad entre NetScaler ADC y NetScaler ADM.
- Generación de registros para el tráfico HDX/ICA en NetScaler ADC.
- Población de registros en NetScaler ADM.

Lista de comprobación de configuración de HDX Insight

- Asegúrese de que la función AppFlow esté habilitada en NetScaler ADC. Para obtener más información, consulte Habilitar AppFlow.
- Compruebe la configuración de HDX Insight en la configuración de NetScaler ADC en ejecución.

  Ejecute el comando `show running | grep -i <appflow_policy>` para comprobar la configuración de HDX Insight. Asegúrese de que el tipo de enlace es ICA REQUEST. Por ejemplo:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Para el modo transparente, el tipo de enlace debe ser ICA_REQ_DEFAULT. Por ejemplo:

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Para la implementación de Access Gateway o de un solo salto, asegúrese de que la directiva de HDX Insight AppFlow esté enlazada al servidor virtual VPN, por donde fluye el tráfico HDX/ICA.
- Para el modo transparente o el modo de usuario LAN, asegúrese de que los puertos ICA 1494 y 2598 están configurados.
- Compruebe que el parámetro «appflowlog» en Citrix Gateway o el servidor virtual VPN esté habilitado para la implementación de Access Gateway o de doble salto. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.
- Compruebe que "Conexión encadenamiento"está activado en NetScaler ADC de doble salto. Para obtener más información, consulte Configuración de dispositivos NetScaler Gateway para exportar datos.
- Después de la conmutación por error de HA si se analizan los detalles de HDX Insight, compruebe que el parámetro ICA "enableSRonHAFailover"está habilitado. Para obtener más información, consulte Fiabilidad de sesión en el par de alta disponibilidad de NetScaler ADC.

Lista de comprobación de conectividad entre NetScaler ADC y NetScaler ADM

- Compruebe el estado del recopilador AppFlow en NetScaler ADC. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler ADC y AppFlow Collector.
- Compruebe los resultados de las directivas de HDX Insight AppFlow.

  Ejecute el comando `show appflow policy <policy_name>` para comprobar los aciertos de la directiva de AppFlow.

  También puede ir a **Sistema > AppFlow > Directivas** en la GUI para comprobar los aciertos de las directivas de AppFlow.

- Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

Generación de registros para el tráfico HDX/ICA en la lista de comprobación de NetScaler ADC

Ejecute el comando `tail -f /var/log/ns.log | grep -i "default ICA Message"` para la validación del registro. En función de los registros que se generan, puede utilizar esta información para solucionar problemas.

- Registro: Se **ha omitido el análisis de la conexión ICA; HDX Insight no es compatible con este host**

  Causa: versiones de Citrix Virtual Apps and Desktops no compatibles

  Solución alternativa: actualice los servidores Citrix Virtual Apps and Desktops a una versión compatible.

- Registro: **Tipo de cliente recibido 0x53, NO compatible**

  Causa: versión no compatible de la aplicación Citrix Workspace

  Solución: actualice la aplicación Citrix Workspace a una versión compatible. Para obtener más información, consulte la aplicación Citrix Workspace.

- Log: **Error de Expand Packet: Omitir todo el procesamiento hdx para este flujo**

  Causa: problema al descomprimir el tráfico ICA

  Solución: no hay informes disponibles para esta sesión de ICA hasta que se establezca una nueva sesión.

- Registro: **Transición no válida: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT”**

  Causa: problema al analizar el protocolo de enlace ICA

  Solución: No hay informes disponibles para esta sesión de ICA en particular hasta que se establezca una nueva sesión.

- Registro: **Falta EUEM ICA RTT**

  Causa: No se pueden analizar los datos del canal de End-User Experience Monitoring

  Solución: asegúrese de que el servicio de supervisión de la experiencia del usuario final esté iniciado en los servidores Citrix Virtual Apps and Desktops. Asegúrese de usar las versiones compatibles de la aplicación Citrix Workspace.

- Registro: **encabezado de canal no válido**

  Causa: no se puede identificar el encabezado del canal

Solución: No hay informes disponibles para esta sesión de ICA en particular hasta que se establezca una nueva sesión.

- Registro: **omitir código**

  Si ves alguno de los siguientes valores para el código de omisión, se omiten los detalles de Insight.

  > El código de omisión 0 indica que el registro se ha exportado correctamente desde NetScaler ADC.

Omitir código	Mensaje de error	Causa del error
100	NS_ICA_ERR_NULL_FRAG	Error en el manejo de fragmentos ICA, probablemente debido a condiciones de memoria
101	NS_ICA_ERR_INVALID_HS_CMD	Se recibió un comando de enlace no válido
102	NS_ICA_ERR_REDUC_PARAM_CNT	Parámetro no válido especificado para la inicialización del expansor V3
103	NS_ICA_ERR_REDUC_INIT	No se puede inicializar correctamente el expansor V3
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Bytes insuficientes para asignar un codificador a un canal
105	NS_ICA_ERR_INVALID_CHANNEL	Número de canal ICA no válido
106	NS_ICA_ERR_INVALID_DECODER	Decodificador no válido especificado para un canal
107	NS_ICA_ERR_INVALID_TW_PARAM	Recuento de parámetros no válido especificado en el canal Thinwire
108	NS_ICA_ERR_INVALID_TW_DECODER	Decodificador no válido para el canal Thinwire
109	NS_ICA_ERR_REDUC_NO_DECODER	No hay decodificador definido para el canal
110	NS_ICA_ERR_REDUC_V3_EXPANDER	No se pudieron expandir los datos del canal
111	NS_ICA_ERR_REDUC_BYTES_V3_COR	Error de expansión: los bytes consumieron más de los bytes disponibles

Omitir código	Mensaje de error	Causa del error
112	NS_ICA_ERR_REDUC_BYTES_OOR	Error: desbordamiento de datos sin comprimir
113	NS_ICA_ERR_REDUC_INVALID_CMD	Comando Expander no definido
114	NS_ICA_ERR_CGP_FILL_HOLE	Error al gestionar tramas CGP divididas
115	NS_ICA_ERR_MEM_NSB_ALLOC	Error de asignación de NSB debido a condiciones de memoria baja
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	Error de asignación de memoria para el contexto del expansor
117	NS_ICA_ERR_ICA_OLD_SERVER	Servidor antiguo, bloques de capacidad no admitidos
118	NS_ICA_ERR_PIR_MANY_FRAG	La solicitud Packet Init está fragmentada, no se puede procesar
119	NS_ICA_ERR_INIT_ICA_CAPS	Error de inicialización de la capacidad ICA
120	NS_ICA_ERR_NO_MSI_SUPPORT	El host no admite la función MSI. Indica para la versión de XenApp inferior a 6.5 o para las versiones de XenDesktop inferiores a 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Se encontró un comando CGP no válido
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Bytes insuficientes en el canal
123	NS_ICA_ERR_CHANNEL_DATA	Datos incorrectos en el canal EUEM, CONTROL o SEAMLESS
124	NS_ICA_ERR_INVALID_PURE_CMD	Se recibió un comando no válido al procesar datos de canal ICA puros
125	NS_ICA_ERR_INVALID_PURE_LEN	Se encontró una longitud no válida al procesar datos de canal ICA puros
126	NS_ICA_ERR_INVALID_PURE_LEN	Se encontró una longitud no válida al procesar los datos del canal ICA PURO

Omitir código	Mensaje de error	Causa del error
127	NS_ICA_ERR_INVALID_CLNT_DATA	Longitud de datos no válida recibida del cliente
128	NS_ICA_ERR_MSI_GUID_SZ	Error en el tamaño del GUID MSI
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	Encabezado de canal no válido
130	NS_ICA_ERR_CGP_PARSE_RECONNECT_ID	Error en la recuperación de la sesión reconectada
131	NS_ICA_ERR_DISABLE_SR_NON_RECONNECT	Error al inhabilitar SR
132	NS_ICA_ERR_REDUC_NOT_V3	Versión ICA Reducer no compatible
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compresión desactivada, no respetada por el host
134	NS_ICA_ERR_IDENT_PROTO	No se puede identificar el protocolo ICA o CGP, visto con receptores incorrectos
135	NS_ICA_ERR_INVALID_SIGNATURE	Firma ICA o cadena mágica incorrectas
136	NS_ICA_ERR_PARSE_RAW	Error al analizar el paquete de enlace ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquete incompleto recibido en el protocolo de enlace
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	La trama ICA es demasiado grande, supera los 1460 bytes
139	NS_ICA_ERR_FORWARD	Error al reenviar los datos ICA
140	NS_ICA_ERR_MAX_HOLES	No se puede procesar el comando CGP porque se divide más allá del límite admitido
141	NS_ICA_ERR_ASSEMBLE_FRAME	No se puede volver a montar el marco ICA correctamente
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Se omite el análisis ICA para este receptor (cliente) porque no está en la lista blanca
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	No se puede detectar el estado de análisis de la cookie de reconexión del cliente

Omitir código	Mensaje de error	Causa del error
144	NS_ICA_ERR_SYNCUP_RECONNECT_LEN	Se detectó una longitud de cookie de reconexión no válida después de la
145	NS_ICA_ERR_INVALID_RECONNECT_ID	La cookie de reconexión del cliente no alcanzó la restricción necesaria
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Cadena de versión de receptor no válida recibida del cliente
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	Producto no válido recibido del cliente
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	Longitud de canal no válida tras la expansión
149	NS_ICA_ERR_SPECIAL_THINWIRE	Error de descompresión
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Se encontraron bytes insuficientes para un comando transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Se encontraron bytes insuficientes para el comando EUEM
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Evento no válido para el análisis continuo de canales
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Evento no válido para el análisis del canal CTRL
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Evento no válido para el análisis del canal de EUEM
155	NS_ICA_ERR_USB_INVALID_EVENT	Evento no válido para el análisis de canales USB
156	NS_ICA_ERR_PURE_INVALID_EVENT	Evento no válido para el análisis de canal puro
157	NS_ICA_ERR_VCP_INVALID_EVENT	Evento no válido para el análisis de canales virtuales
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Evento no válido para el análisis de datos ICA
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Evento no válido para el análisis de datos CGP
160	NS_ICA_ERR_BASICCRYPT_INVALID_STATE	Estado no válido para un comando crypt en el cifrado básico

Omitir código	Mensaje de error	Causa del error
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	Comando crypt no válido en el cifrado básico
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	Estado no válido para un comando crypt en el cifrado RC5
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	Comando crypt no válido en el cifrado RC5
164	NS_ICA_ERR_ADVCRYPT_ENC	Error en el cifrado/descifrado RC5
165	NS_ICA_ERR_ADVCRYPT_DEC	Error en el cifrado/descifrado RC5
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	El VDA no admite la versión 3 de Reducer
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	El receptor no es compatible con Reducer Version 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Número inesperado de bytes en el protocolo de enlace ICA
169	NS_ICA_ERR_HIGHER_RECONSEQ	Número de secuencia de reanudación de CGP más alto desde la reconexión posterior al par
170	NS_ICA_ERR_DESCSRINFO_ABSENT	No se puede restaurar el estado de análisis de ICA después de la reconexión
171	NS_ICA_ERR_NSAP_PARSING	Error al analizar los datos del canal Insight
172	NS_ICA_ERR_NSAP_APP	Error al analizar los detalles de la aplicación de los datos del canal Insight
173	NS_ICA_ERR_NSAP_ACR	Error al analizar los detalles de ACR de los datos del canal Insight
174	NS_ICA_ERR_NSAP_SESSION_END	Error al analizar los detalles de finalización de la sesión de los datos del canal Insight

Omitir código	Mensaje de error	Causa del error
175	NS_ICA_ERR_NON_NSAP_SN	Se ha omitido el análisis de ICA en el nodo de servicio debido a la ausencia de soporte del canal Insight
176	NS_ICA_ERR_NON_NSAP_CLIENT	El cliente no admite NSAP
177	NS_ICA_ERR_NON_NSAP_SERVER	El VDA no admite NSAP
178	NS_ICA_ERR_NSAP_NEG_FAIL	Error durante la negociación de datos de NSAP
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	Error al obtener el ticket de reconexión del servicio en el nodo de servicio
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	Error al recibir un número de secuencia de reconexión más alto en el nodo de servicio
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONNSAP	Error al deshabilitar HDXInsight para conexiones que no son de NSAP

Registros de ejemplo:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
 ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
 send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
 Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
 [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```


Contadores de errores

Se capturan varios contadores analizando ICA. En la siguiente tabla se enumeran los distintos contadores para el análisis ICA.
Ejecute el comando `nsconmsg –g hdx –d statswt0` para ver los detalles del contador.

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_tot_ica_conn	Indica el número total de conexiones ICA puras detectadas por NS. Se incrementa cada vez que se detecta una conexión ICA basada en la firma ICA en una PCB cliente.	Estadísticas
hdx_tot_cgp_conn	Indica el número total de conexiones CGP detectadas por NS (Session Reliability ON). Se incrementa cada vez que se detecta una conexión CGP basada en la firma CGP en una PCB cliente.	Estadísticas
hdx_dbg_tot_udt_conn	Indica el número total de conexiones UDP ICA detectadas por NS	Estadísticas
hdx_dbg_tot_nsap_conn	Indica el número total de conexiones compatibles con NSAP detectadas por NS	Estadísticas
hdx_tot_skip_conn	Indica cuántas conexiones ICA omitió el analizador debido a una firma ICA o CGP no válida.	Estadísticas
hdx_dbg_active_conn	Total de conexiones EDT/CGP/ICA activas en ese instante.	Estadísticas
hdx_dbg_active_nsap_conn	Número total de conexiones EDT/CGP/ICA NSAP activas en ese instante.	Estadísticas

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_dbg_skip_appflow_disabled	Número total de instancias en las que AppFlow se desconectó de una sesión debido a la desactivación de AppFlow	Estados/Diagnósticos
hdx_dbg_transparent_user	Número total de accesos de usuarios transparentes	Estados/Diagnósticos
hdx_dbg_ag_user	Número total de accesos de usuarios de Access Gateway	Estados/Diagnósticos
hdx_dbg_lan_user	Número total de accesos en modo de usuario de LAN	Estados/Diagnósticos
hdx_basic_enc	Indica el número de conexiones ICA que utilizan cifrado básico	Estados/Diagnósticos
hdx_advanced_enc	Indica el número de conexiones ICA que utilizan un cifrado avanzado basado en RC5	Estados/Diagnósticos
dx_dbg_wanscaler_on_clientside	Número total de conexiones CGP/ICA que tienen Citrix SD-WAN en el lado del cliente	Estados/Diagnósticos
hdx_dbg_wanscaler_on_serverside	Número total de conexiones CGP/ICA que tienen el lado del servidor de Citrix SD-WAN	Estados/Diagnósticos
hdx_dbg_reconnected_session	Número total de solicitudes de reconexión del cliente sin ningún error de NetScaler ADC	Estados/Diagnósticos
hdx_dbg_host_rejected_ns_reconnect	Número total de solicitudes de reconexión de hosts rechazadas por cliente	Estados/Diagnósticos
hdx_euem_available	Indica el número de conexiones que tienen disponible el canal de supervisión de la experiencia del usuario final. El canal de supervisión de la experiencia del usuario final es necesario para recopilar estadísticas como ICA RTT.	Estados/Diagnósticos

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_err_disabled_sr	La confiabilidad de la sesión se deshabilita mediante el mando nsapimgr.La sesión no funciona para esta sesión.	Error
hdx_err_skip_no_msi	Al servidor XA/XD le falta la capacidad MSI. Esto indica una versión de servidor anterior, HDX Insight omite esta conexión.	Error
hdx_err_skip_old_server	Versión de servidor antigua no compatible	Error
hdx_err_clnt_not_whitelist	El receptor del cliente no está en la lista blanca, HDX Insight omite esta conexión	Error
hdx_sm_ica_cam_channel_disabled	Número total de NS_ICA_CAM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_usb_channel_disabled	Número total de NS_ICA_USB_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_clip_channel_disabled	Número total de NS_ICA_CLIP_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_ccm_channel_disabled	Número total de NS_ICA_CCM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_cdm_channel_disabled	Número total de NS_ICA_CDM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_sm_ica_com1_channel_disabled	Número total de NS_ICA_COM1_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_com2_channel_disabled	Número total de NS_ICA_COM2_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_cpm_channel_disabled	Número total de NS_ICA_CPM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_lpt1_channel_disabled	Número total de NS_ICA_LPT1_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_lpt2_channel_disabled	Número total de NS_ICA_LPT2_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
dx_dbg_sm_ica_msi_disabled	Número total de casos en los que MSI está inhabilitado mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_file_channel_disabled	El número total de NS_ICA_FILE_CHANNEL está inhabilitado mediante la directiva SmartAccess	Diagnóstico
hdx_dbg_usb_accept_device	Número total de dispositivos USB aceptados	Diagnóstico
hdx_dbg_usb_reject_device	Número total de dispositivos USB rechazados	Diagnóstico
hdx_dbg_usb_reset_endpoint	Número total de puntos finales USB restablecidos	Diagnóstico
hdx_dbg_usb_reset_device	Número total de dispositivos USB restablecidos	Diagnóstico
hdx_dbg_usb_stop_device	Número total de dispositivos USB detenidos	Diagnóstico

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_dbg_usb_stop_device_response	Número total de respuestas de dispositivos USB detenidos	Diagnóstico
hdx_dbg_usb_device_gone	Número total de dispositivos USB desaparecidos	Diagnóstico
hdx_dbg_usb_device_stopped	Número total de dispositivos USB detenidos	Diagnóstico

Validación de nstrace

Compruebe el protocolo CFLOW para ver todos los registros de AppFlow que salen de NetScaler ADC.

Población de registros en la lista de comprobación de NetScaler ADM

- Ejecute el comando `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` y compruebe los registros para confirmar que Citrix ADM recibe registros de AppFlow.
- Confirme que la instancia de NetScaler ADC se haya agregado a NetScaler ADM.
- Validar que el servidor virtual de NetScaler Gateway/VPN tiene licencia en NetScaler ADM.
- Asegúrese de que la configuración de parámetros de salto múltiple esté habilitada para el doble salto.
- Asegúrese de que NetScaler Gateway esté autorizado para el segundo salto en la implementación de doble salto.

Antes de contactar al soporte técnico de Citrix

Para una resolución rápida, asegúrese de contar con la siguiente información antes de ponerse en contacto con el soporte técnico de Citrix:

- Detalles de la implementación y la topología de la red.
- Versiones de NetScaler ADC y NetScaler ADM.
- Versiones del servidor Citrix Virtual Apps and Desktops.
- Versiones de Receiver cliente

- Número de sesiones ICA activas cuando se produjo el problema.
- Paquete de soporte técnico capturado al ejecutar el comando `show techsupport` en la línea de comandos de Citrix ADC.
- Paquete de soporte técnico capturado para NetScaler ADM.
- Rastreos de paquetes capturados en todos los NetScaler ADC.
  Para iniciar un seguimiento de paquete, escriba,`start nstrace -size 0'`
  Para detener un seguimiento de paquete, escriba,`stop nstrace`
- Recopile entradas en la tabla ARP del sistema ejecutando el comando.`show arp`

Problemas conocidos

Consulte las notas de la versión de NetScaler ADC para conocer los problemas conocidos en HDX Insight.

Gateway Insight

January 30, 2024

En una implementación de Citrix Gateway, la visibilidad de los detalles de acceso de un usuario es esencial para solucionar problemas de error de acceso. Como administrador de red, quiere saber cuándo un usuario no puede iniciar sesión en Citrix Gateway y quiere conocer la actividad del usuario y los motivos del error de inicio de sesión, pero esa información normalmente no está disponible a menos que el usuario envíe una solicitud de resolución.

Gateway Insight proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, en el momento de iniciar sesión en Citrix Gateway. Puede ver una lista de todos los usuarios disponibles, el número de usuarios activos, el número de sesiones activas y los bytes y licencias utilizados por todos los usuarios en un momento dado. Puede ver los errores del análisis de puntos finales (EPA), la autenticación, el inicio de sesión único (SSO) y el inicio de aplicaciones de un usuario. También puede ver los detalles de las sesiones activas y finalizadas de un usuario.

Gateway Insight también proporciona visibilidad de los motivos del error de inicio de aplicaciones para aplicaciones virtuales. Esto mejora su capacidad para solucionar cualquier tipo de problemas de inicio de sesión o inicio de aplicaciones. Puede ver el número de aplicaciones lanzadas, el número de sesiones totales y activas, el número total de bytes y el ancho de banda consumidos por las aplicaciones. Puede ver los detalles de los usuarios, las sesiones, el ancho de banda y los errores de inicio de una aplicación.

Puede ver la cantidad de puertas de enlace, la cantidad de sesiones activas, el total de bytes y el ancho de banda que utilizan todas las puertas de enlace asociadas a un dispositivo Citrix Gateway en un momento dado. Puede ver los errores de EPA, autenticación, inicio de sesión único y lanzamiento de aplicaciones para una Gateway. También puede ver los detalles de todos los usuarios asociados a una Gateway y su actividad de inicio de sesión.

Todos los mensajes de registro se almacenan en la base de datos Citrix ADM, por lo que puede ver los detalles de los errores de cualquier período de tiempo. También puede ver un resumen de los errores de inicio de sesión y determinar en qué etapa del proceso de inicio de sesión se ha producido un error.

Puntos que tener en cuenta

- Gateway Insight se admite en las siguientes implementaciones:
  - Access Gateway
  - Unified Gateway
- La versión y la compilación de Citrix ADM deben ser iguales o posteriores a las del dispositivo Citrix Gateway.
- Se puede ver una hora de informes de Gateway Insight para instancias de Citrix ADC con licencia Enterprise. Se requiere una licencia Platinum para ver los informes de Gateway Insight más allá de una hora.

Limitaciones

- Citrix Gateway no admite Gateway Insight cuando el método de autenticación está configurado como autenticación basada en certificados.
- Para los informes de Gateway Insight, la información de ubicación geográfica no se proporciona desde el dispositivo Citrix ADC.
- Los inicios de sesión de usuario correctos, la latencia y los detalles de nivel de aplicación para aplicaciones y escritorios ICA virtuales solo están visibles en el panel Usuarios de HDX Insight.
- En el modo de doble salto, no está disponible la visibilidad de los errores en el dispositivo Citrix Gateway en la segunda DMZ.
- No se notifican problemas de acceso al escritorio de Protocolo de escritorio remoto (RDP).
- Gateway Insight es compatible con los siguientes tipos de autenticación. Si se utiliza otro tipo de autenticación distinto de estos, es posible que veas algunas discrepancias en Gateway Insight.

- Locales
- LDAP
- RADIUS
- TACACS
- SAML
- OTP nativo

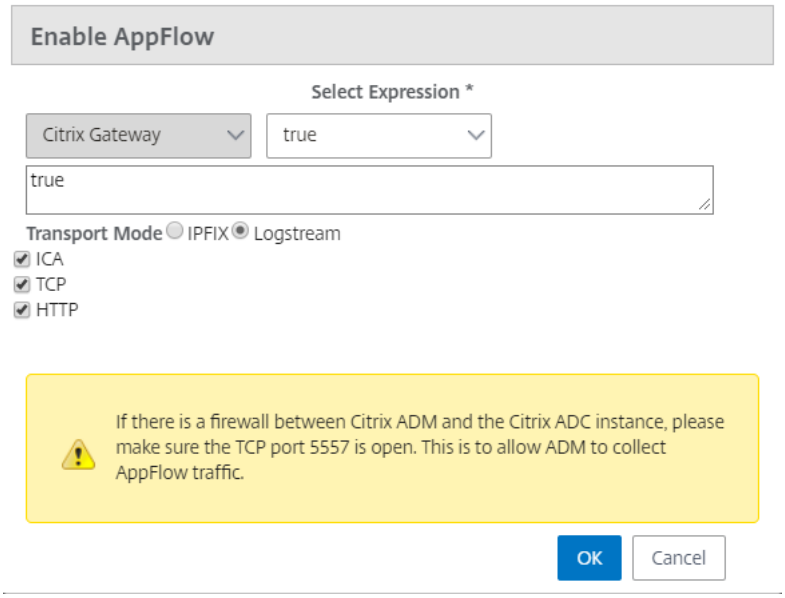
Habilitación de Gateway Insight

Para habilitar Gateway Insight para su dispositivo Citrix Gateway, primero debe agregar el dispositivo Citrix Gateway a Citrix ADM. A continuación, debe habilitar AppFlow para el servidor virtual que representa la aplicación VPN. Para obtener información sobre cómo agregar dispositivos a Citrix ADM, consulte Agregar dispositivos.

> **Nota**
>
> Para ver los errores del análisis de punto final (EPA) en Citrix ADM, debe habilitar la autenticación, la autorización y el registro de nombres de usuario de auditoría de AppFlow en el dispositivo Citrix Gateway.

Para habilitar AppFlow para un servidor virtual en Citrix ADM

1. Inicie sesión en Citrix ADM.
2. Vaya a **Redes** >**Instancias** y seleccione la instancia para la que quiere habilitar AppFlow.
3. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
4. En la página **Configurar Insight**, en **Configurar Analytics**, seleccione **Citrix Gateway**.
5. Seleccione el servidor virtual para el que quiere habilitar AppFlow y haga clic en **Habilitar AppFlow**.
6. En la pantalla **Habilitar AppFlow**, en la lista **Seleccionar expresión**, haga clic en true.
7. Junto a **Modo de transporte**, active la casilla de verificación **Logstream**.



> **Nota**
>
> Puede elegir entre IPFIX o `Logstream` como modo de transporte.

8. Haga clic en **Aceptar**.

Para habilitar la autenticación, la autorización y el registro de nombres de usuario de auditoría de AppFlow en un dispositivo Citrix Gateway mediante la GUI

1. Vaya a **Configuración > Sistema > AppFlow > Configuración** y, a continuación, haga clic en **Cambiar configuración de AppFlow**.
2. En la pantalla **Configurar ajustes de AppFlow**, seleccione Nombre de **usuario AAA**y, a continuación, haga clic en **Aceptar**

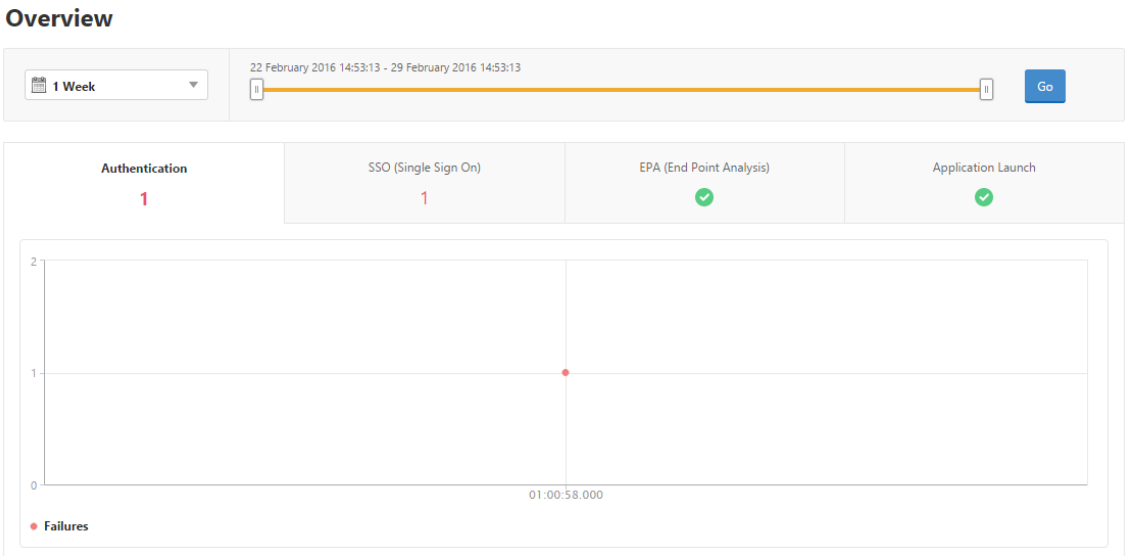
Ver los informes de Gateway Insight

En Citrix ADM, puede ver los informes de todos los usuarios, aplicaciones y puertas de enlace asociados a los dispositivos Citrix Gateway, y puede ver los detalles de un usuario, aplicación o puerta de enlace en particular. En la sección **Descripción general**, puede ver los errores de EPA, SSO, Autenticación y Lanzamiento de aplicaciones. También puede ver un resumen de los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora.

Para ver los errores de EPA, SSO, autenticación, autorización y lanzamiento de aplicaciones

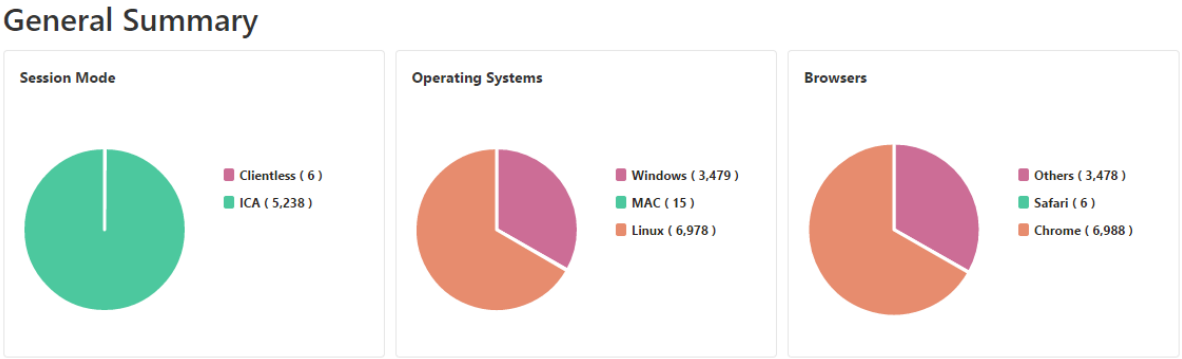
1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.

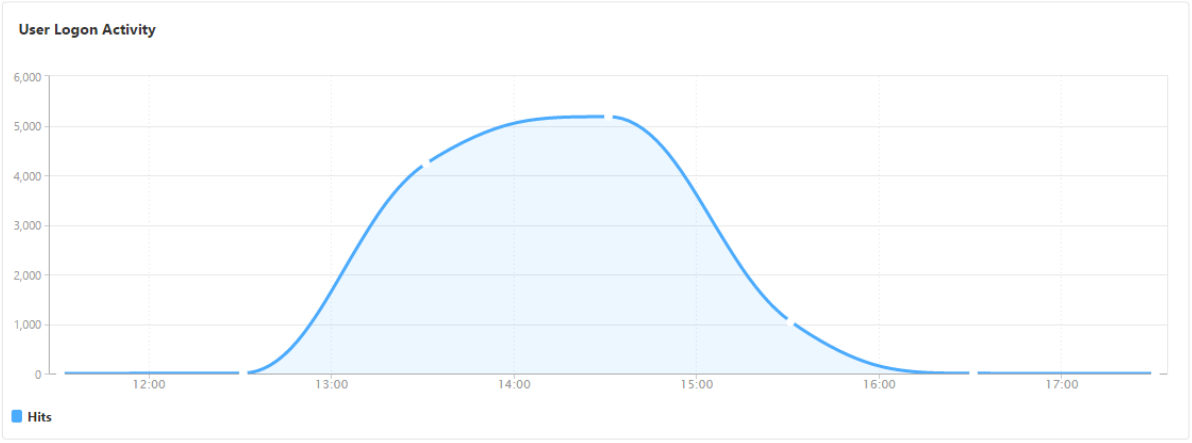
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Haga clic en las fichas EPA (Análisis de punto final), Autenticación, Autorización, SSO (Inicio de sesión único) o Inicio de aplicación para mostrar los detalles del error.



Para ver un resumen de los modos de sesión, los clientes y el número de usuarios

En Citrix ADM, vaya a **Analytics > Gateway Insight**, desplácese hacia abajo para ver los informes.



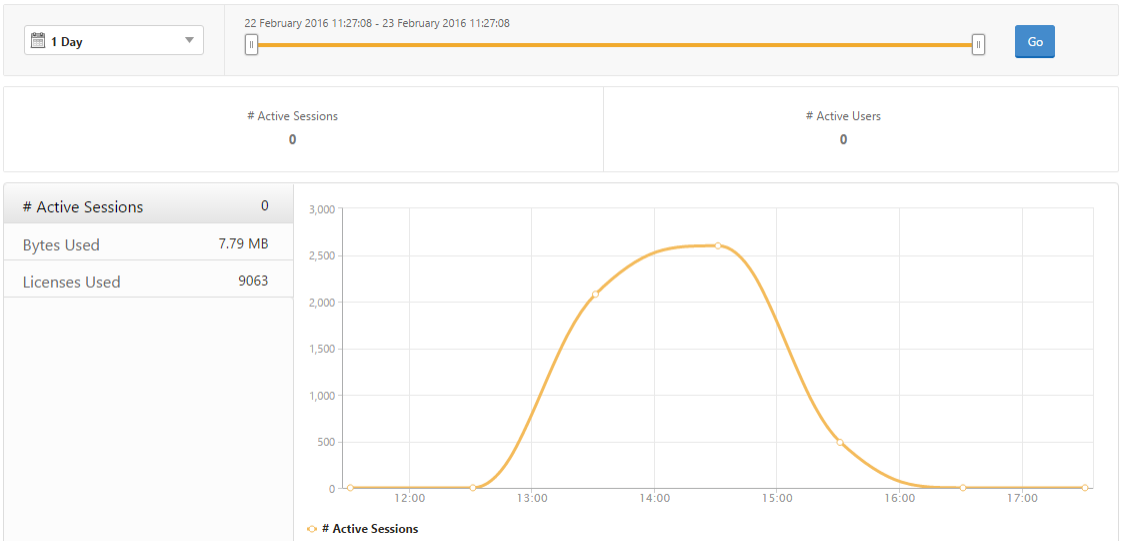


Visualización de informes de Gateway Insight para usuarios

Puede ver los informes de todos los usuarios asociados a los dispositivos Citrix Gateway. Puede ver los errores de EPA, autenticación, SSO e inicio de aplicaciones de un usuario. También puede ver los detalles de las sesiones activas y finalizadas de un usuario.

Para ver los detalles del usuario

1. En Citrix ADM, vaya a **Analytics > Gateway Insight > Usuarios**.
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Ahora puede ver el número de usuarios activos, el número de sesiones activas, bytes y licencias utilizadas por todos los usuarios durante el período de tiempo.



Desplácese hacia abajo para ver una lista de usuarios disponibles y usuarios activos.

User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

En la ficha **Usuarios** o **Usuarios activos**, puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de EPA, autenticación, SSO e inicio de aplicaciones y otros detalles para ese usuario.

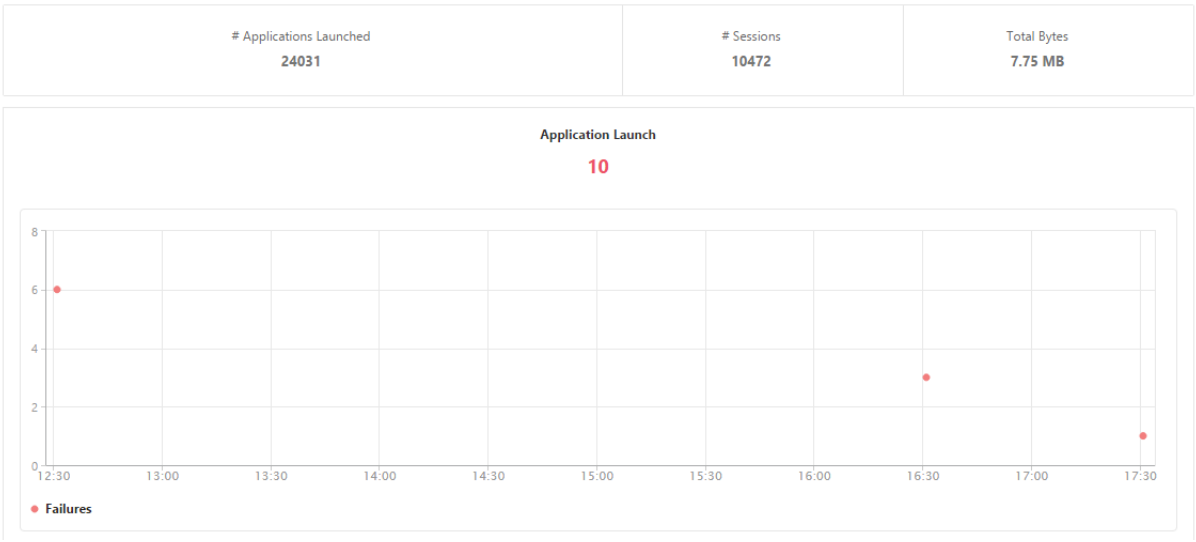
Visualización de informes de Gateway Insight para aplicaciones

Puede ver el número de aplicaciones lanzadas, el número de sesiones totales y activas, el número total de bytes y el ancho de banda consumidos por las aplicaciones. Puede ver los detalles de los usuarios, las sesiones, el ancho de banda y los errores de inicio de una aplicación.

Para ver los detalles de la aplicación

1. En NetScaler ADM, vaya a **Analytics > Gateway Insight > Aplicaciones**.
2. Seleccione el período de tiempo para el que quiere ver los detalles de la aplicación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

Ahora puede ver el número de aplicaciones lanzadas, el número de sesiones totales y activas, el número total de bytes y el ancho de banda consumidos por las aplicaciones.



Desplácese hacia abajo para ver el número de sesiones, ancho de banda y bytes totales consumidos por ICA y otras aplicaciones.

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

En la ficha **Otras aplicaciones**, puede hacer clic en una aplicación de la columna **Nombre** para mostrar los detalles de esa aplicación.

Visualización de informes de Gateway Insight para puertas de enlace

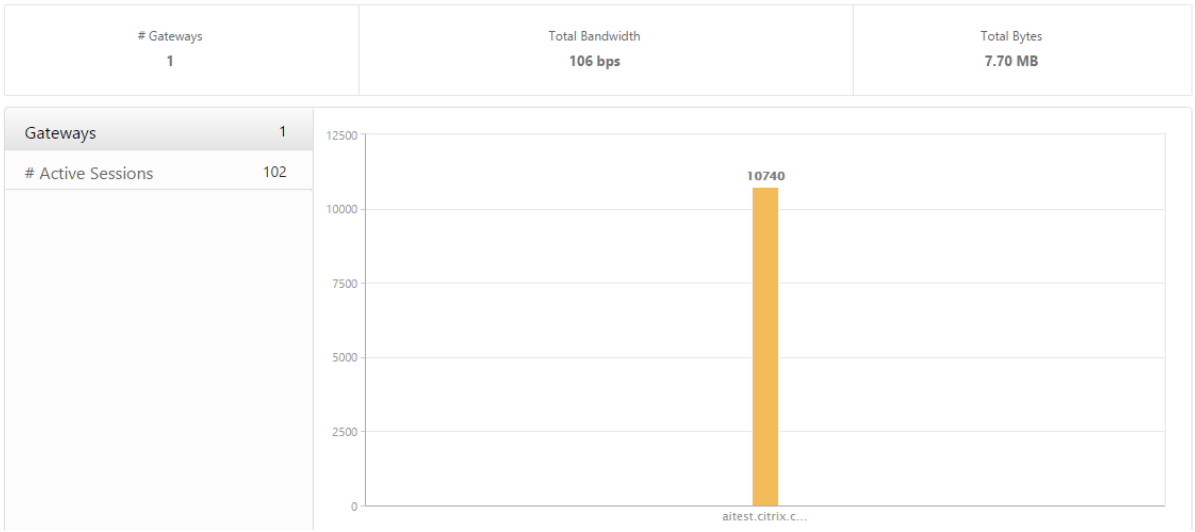
Puede ver la cantidad de puertas de enlace, la cantidad de sesiones activas, el total de bytes y el ancho de banda utilizados por todas las puertas de enlace asociadas a un dispositivo Citrix Gateway en un momento dado. Puede ver los errores de EPA, autenticación, inicio de sesión único y lanzamiento de aplicaciones para una Gateway. También puede ver los detalles de todos los usuarios asociados a una Gateway y su actividad de inicio de sesión.

Para ver los detalles de la Gateway

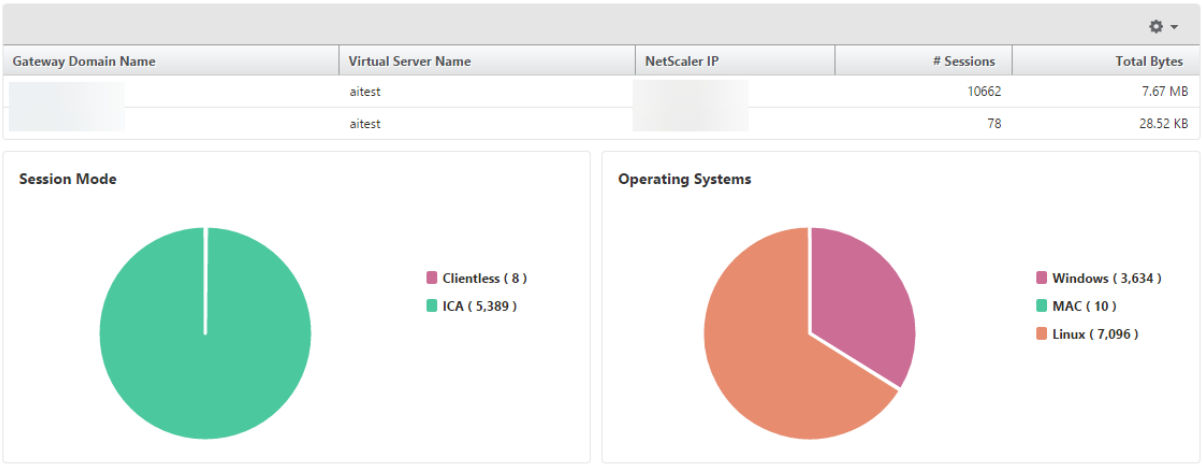
1. En **Citrix ADM**, vaya a **Analytics > Gateway Insight > Gateway**.

2. Seleccione el período de tiempo para el que quiere ver los detalles de la Gateway. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

Ahora puede ver el número de puertas de enlace, el número de sesiones activas, el total de bytes y el ancho de banda que utilizan todas las puertas de enlace asociadas con un dispositivo Citrix Gateway en un momento dado.



Desplácese hacia abajo para ver los detalles de la Gateway, como el nombre de dominio de la puerta de enlace, el nombre del servidor virtual, la dirección IP de NetScaler, los modos de sesión y los bytes totales.



Puede hacer clic en una Gateway de la columna **Nombre de dominio de Gateway** para mostrar los errores de EPA, autenticación, inicio de sesión único e inicio de aplicaciones y otros detalles de una puerta de enlace.

Exportación de informes

Puede guardar los informes de Gateway Insight con todos los detalles que se muestran en la GUI en formato PDF, JPEG, PNG o CSV en su computadora local. También puede programar la exportación de los informes a direcciones de correo electrónico especificadas en varios intervalos.

> **Nota**
>
> - Los usuarios con acceso de solo lectura no pueden exportar informes.
> - Los informes de mapas geográficos se exportan solo si el Citrix ADM tiene conectividad a Internet.

Para exportar un informe

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.

Para programar la exportación:

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Planificar exportación**, especifique los detalles y haga clic en **Planificar**.

Para agregar un servidor de correo electrónico o una lista de distribución de correo electrónico:

1. En la ficha **Configuración**, vaya a **Sistema** > **Notificaciones** > **Correo electrónico**.
2. En el panel derecho, seleccione **Servidor de correo electrónico**para agregar un servidor de correo electrónico o seleccione Lista de **distribución de correo electrónico para crear una lista** de distribución de correo electrónico.
3. Especifique los detalles y haga clic en **Crear**.

Para exportar todo el panel de Gateway Insight:

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Exportar ahora**, seleccione Formato **PDF** y, a continuación, haga clic en **Exportar**.

Casos de uso de Gateway Insight

Los siguientes casos de uso muestran cómo puede usar Gateway Insight para obtener visibilidad de los detalles de acceso, las aplicaciones y las puertas de enlace de los usuarios en los dispositivos Citrix Gateway.

Un usuario no puede iniciar sesión en el dispositivo Citrix Gateway ni en los servidores web internos

Es un administrador de Citrix Gateway que supervisa los dispositivos Citrix Gateway a través de Citrix ADM y quiere ver por qué un usuario no puede iniciar sesión o en qué etapa del proceso de inicio de sesión se produjo el error.

Citrix ADM le permite ver los detalles del error de inicio de sesión del usuario en las siguientes etapas del proceso de inicio de sesión:

- Autenticación
- Análisis de puntos finales (EPA)
- Single Sign-On

En Citrix ADM, puede buscar un usuario en particular y, a continuación, ver todos los detalles de ese usuario.

Para buscar un usuario:

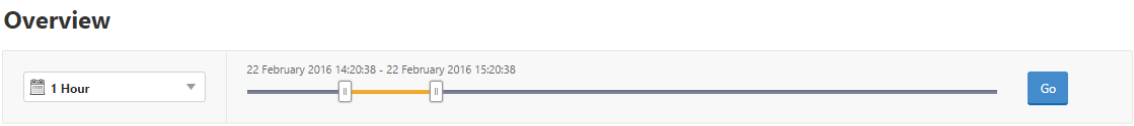
En Citrix ADM, vaya a **Analytics > Gateway Insight** y, en el cuadro de texto **Buscar usuarios**, especifique el usuario en el que quiere buscar.

Fallos de autenticación

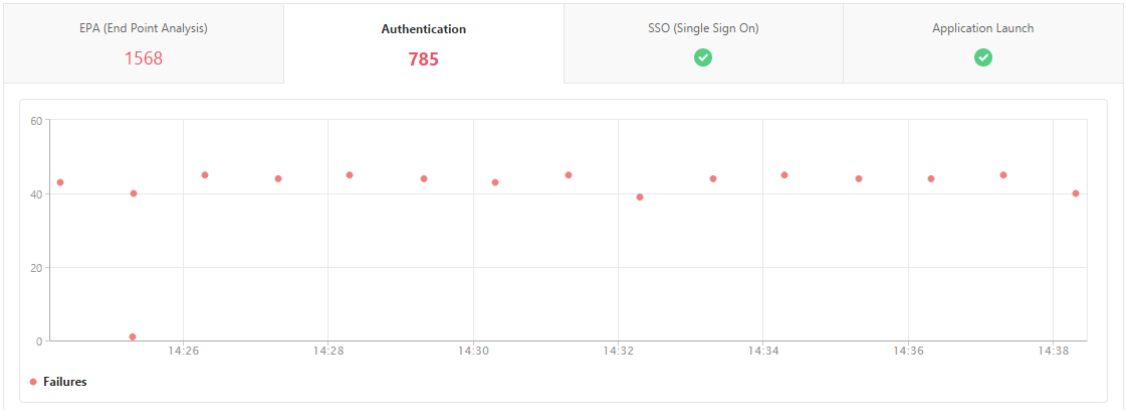
Puede ver errores de autenticación, como credenciales incorrectas o ninguna respuesta del servidor de autenticación. Si ha configurado la autenticación en dos etapas, puede ver si han fallado las etapas principal, secundaria o ambas de la autenticación.

Para ver los detalles del error de autenticación:

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de autenticación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **Autenticación**. Puede ver el número de errores de autenticación en un momento dado en el gráfico de **errores**.



Desplácese hacia abajo para ver los detalles de cada error de autenticación, como **Nombre de usuario, Dirección IP del cliente, Tiempo de error, Tipo de autenticación, Dirección IP del servidor de autenticación**, etc. en la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra el motivo del error de inicio de sesión y la columna **Estado** muestra en qué etapa de una autenticación en dos etapas se produjo el error.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de autenticación y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo como se indica en la siguiente captura de pantalla.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

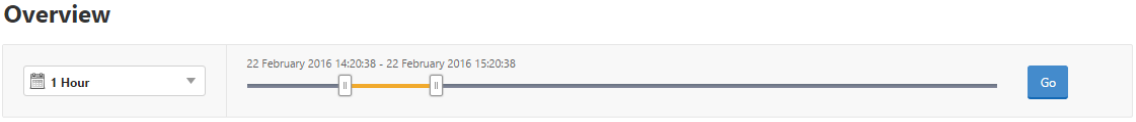
Errores de EPA

Puede ver los errores de EPA en la etapa previa o posterior a la autenticación.

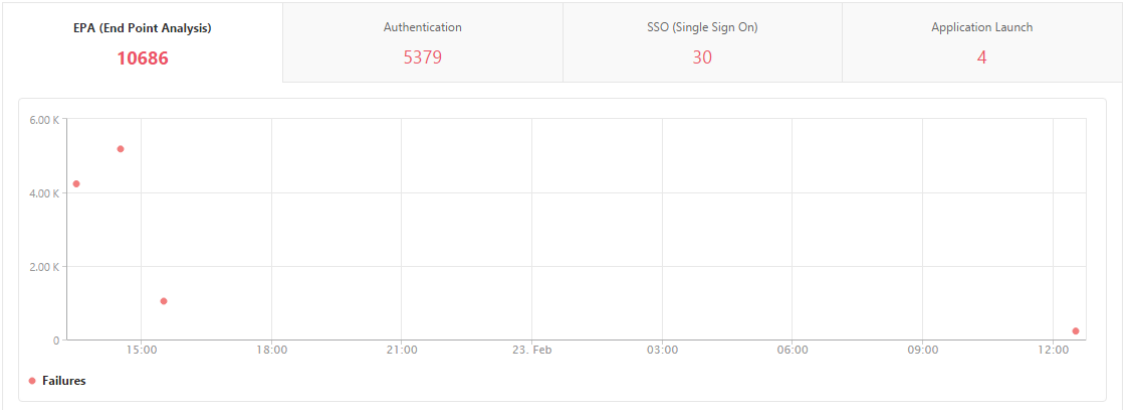
> **Importante:**
>
> - Los errores de EPA solo se registran cuando se configuran expresiones clásicas.
> - Los errores de la EPA no se notifican si la expresión avanzada se configura en la directiva de autenticación previa o posterior a la autenticación.
> - Los errores de EPA no se registran si EPA se configura como uno de los factores en un flujo de autenticación de nFactor.

Para ver los detalles de fallo de EPA:

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de EPA. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **EPA (Análisis de punto final)**. Puede ver el número de errores de EPA en un momento dado en el gráfico de **errores**.



Desplázate hacia abajo para ver los detalles de cada error de la EPA, como el nombre de **usuario, la dirección IP de NetScaler, la dirección IP de Gateway, la VPN, el tiempo de error, el nombre de la directiva, el nombre de dominio de Gateway** y más, de la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra el motivo del error EPA y la columna **Nombre de la directiva** muestra la directiva que dio lugar al error.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de EPA y otros detalles de ese usuario.
Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

> **Nota**
>
> Citrix Gateway no informa de los errores de la EPA cuando la expresión “clientSecurity”se configura como una regla de directiva de sesión de VPN.

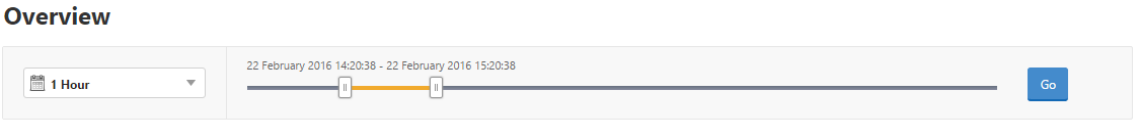
Errores de SSO

Puede ver todos los errores de SSO en cualquier etapa de un usuario que accede a cualquier aplicación a través del dispositivo Citrix Gateway.

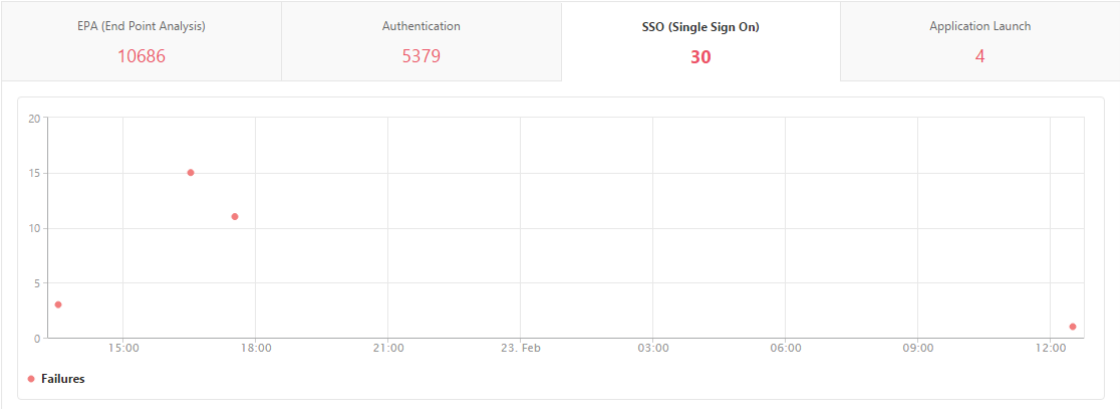
Para ver los detalles del error de inicio de SSO:

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.

2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **SSO (Inicio de sesión único)**. Puede ver el número de errores de SSO en cualquier momento dado en el gráfico de errores.



Desplácese hacia abajo para ver los detalles de cada error de SSO **, como Nombre de usuario, Dirección IP de NetScaler, Tiempo de error, Descripción del error, Nombre del recurso** y más desde la tabla de la misma ficha.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de SSO y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

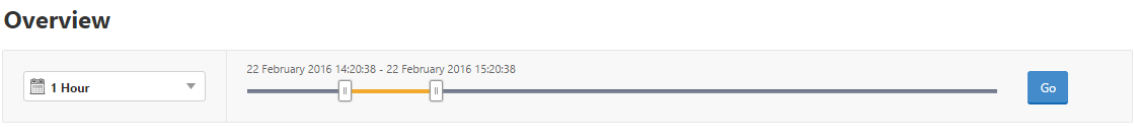
Después de iniciar sesión correctamente en Citrix Gateway, un usuario no puede iniciar ninguna aplicación virtual

En el caso de un error al iniciar una aplicación, puede obtener visibilidad de los motivos, como el servidor de Secure Ticket Authority (STA) o Citrix Virtual Apps inaccesibles, o el vale STA no válido.

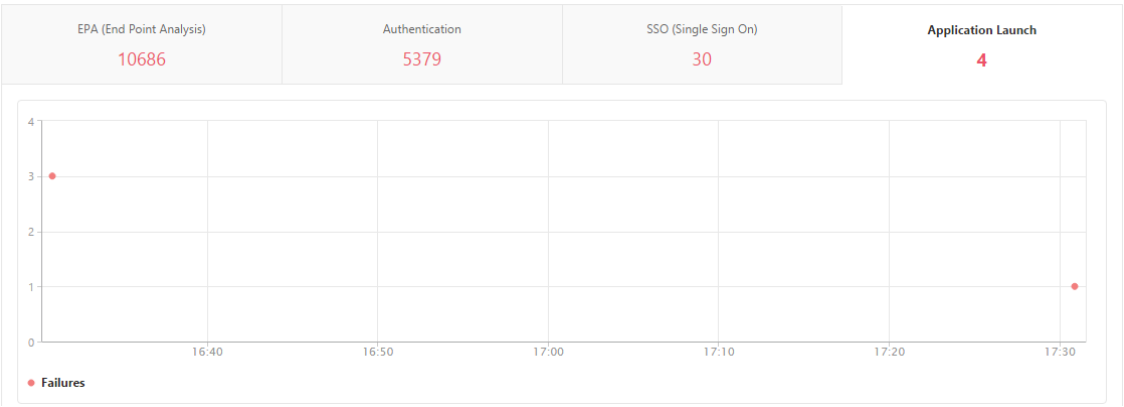
Puede ver la hora en que se produjo el error, los detalles del error y el recurso para el que falló la validación STA.

Para ver los detalles del error de inicio de la aplicación:

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **Inicio de la aplicación**. Puede ver el número de errores de inicio de la aplicación en un momento dado en el gráfico **Fallos**.



Desplácese hacia abajo para ver los detalles de cada error de inicio de la aplicación, como **NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name**, etc., desde la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra la dirección IP del servidor STA y la columna **Nombre del recurso** muestra los detalles del recurso para el que ha fallado la validación STA.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de inicio de la aplicación y otros detalles de ese usuario.

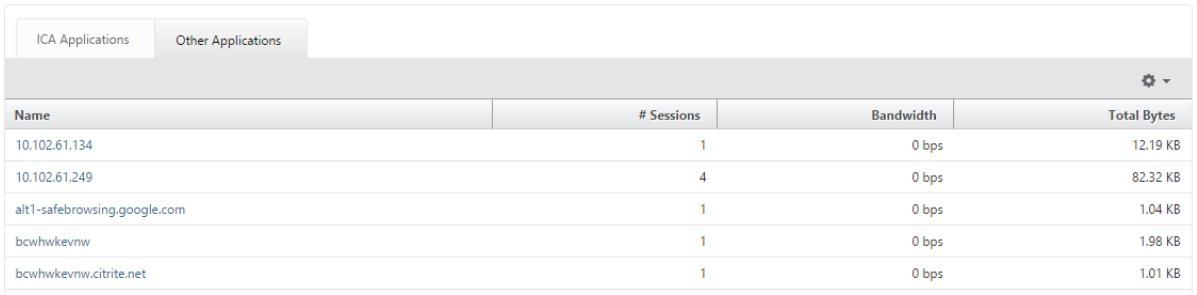
Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

Después de iniciar correctamente una nueva aplicación, un usuario quiere ver el total de bytes y ancho de banda consumidos por esa aplicación

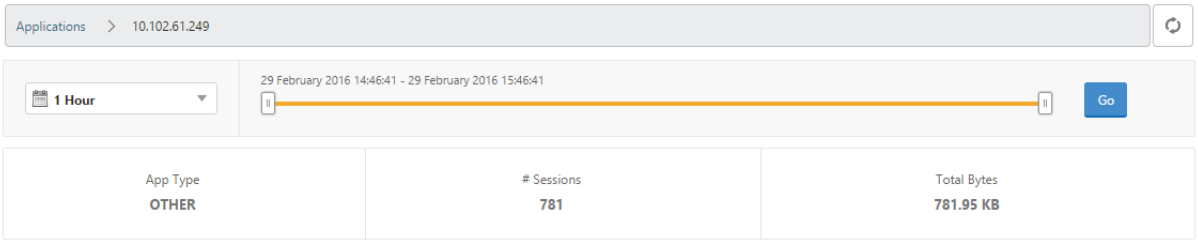
Después de haber iniciado correctamente una nueva aplicación, en Citrix ADM, puede ver el total de bytes y ancho de banda consumidos por esa aplicación.

Para ver el total de bytes y ancho de banda consumidos por una aplicación:

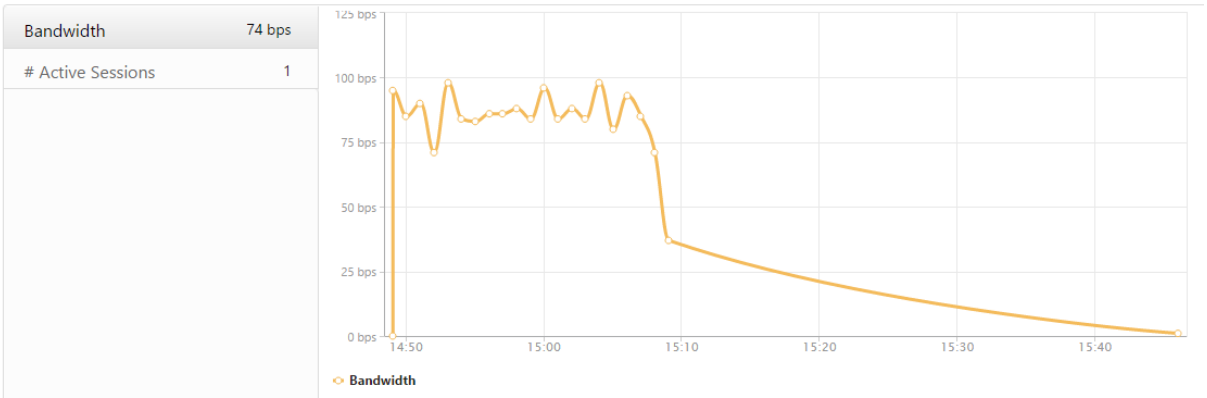
En Citrix ADM, vaya a **Analytics > Gateway Insight > Aplicaciones**, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, haga clic en la aplicación para la que quiere ver los detalles.



Puede ver el número de sesiones y el número total de bytes consumidos por esa aplicación.



También puede ver el ancho de banda consumido por esa aplicación.

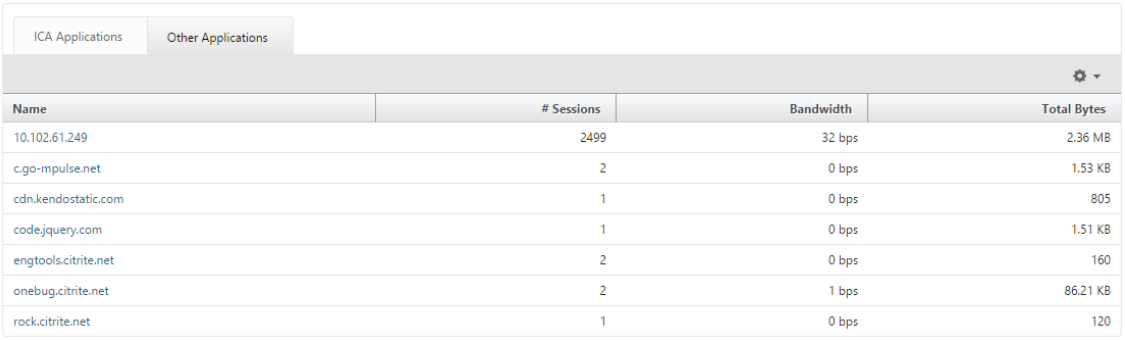


Un usuario ha iniciado sesión correctamente en Citrix Gateway, pero no puede acceder a determinados recursos de red de la red interna

Con Gateway Insight, puede determinar si el usuario tiene acceso a los recursos de red o no. También puede ver el nombre de la directiva que dio lugar al error.

Para ver el acceso de los usuarios para los recursos:

1. En Citrix ADM, **vaya a Analytics > Gateway Insight > Aplicaciones**.
2. En la pantalla que aparece, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, seleccione la aplicación en la que el usuario no pudo iniciar sesión.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

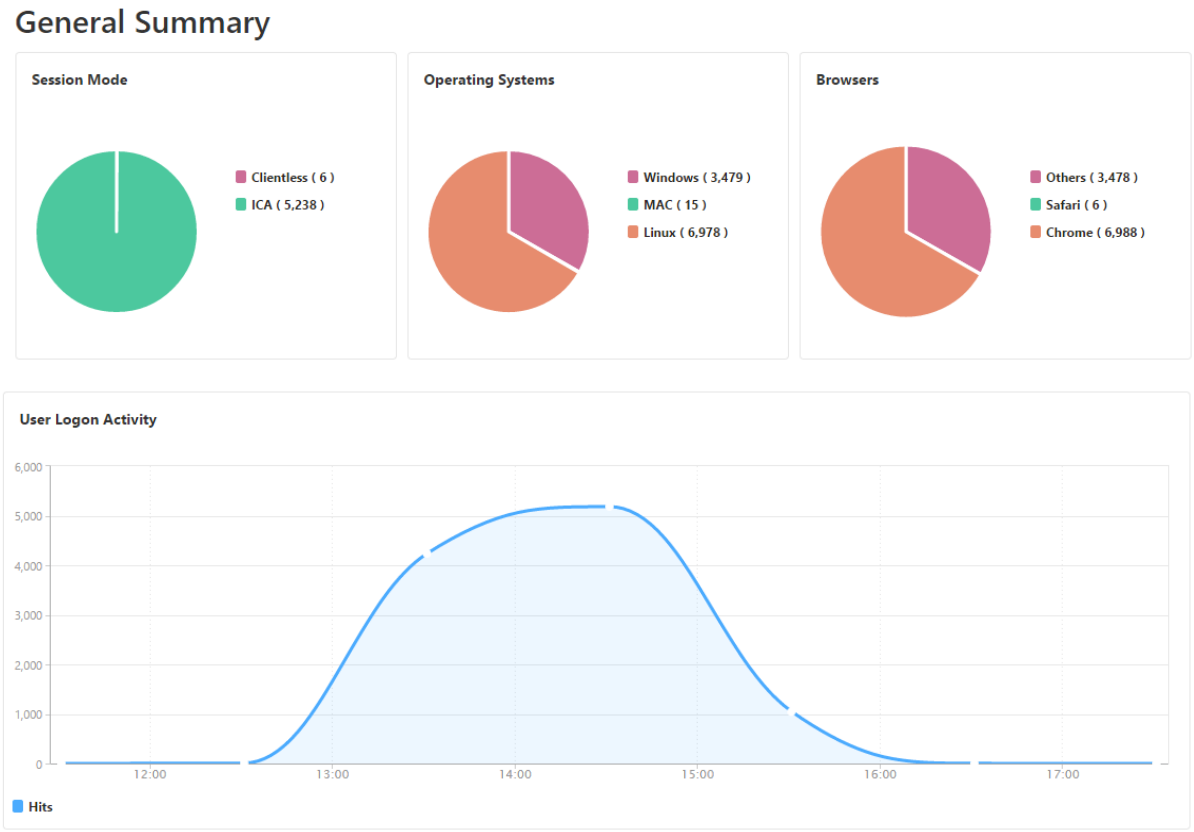
3. Desplácese hacia abajo y, en la tabla **Usuarios**, se muestran todos los usuarios que tienen acceso a esa aplicación.

Es posible que diferentes usuarios usen distintas implementaciones de Citrix Gateway o que inicien sesión en Citrix Gateway a través de diferentes modos de acceso. El administrador debe poder ver detalles sobre los tipos de implementación y los modos de acceso

Con Gateway Insight, puede ver un resumen de los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora. También puede determinar si la implementación de un usuario es una puerta de enlace unificada o una implementación clásica de Citrix Gateway. Para implementaciones de Gateway unificada, puede ver el nombre y la dirección IP del servidor virtual de conmutación de contenido y el nombre del servidor virtual VPN.

Para ver el resumen de los modos de sesión, el tipo de clientes y la cantidad de usuarios que han iniciado sesión:

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección **Descripción general**, desplácese hacia abajo para ver los gráficos **Modo de sesión, Sistemas operativos, Exploradores** y **Actividad de inicio de sesión del usuario** que muestran los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora.



Solucionar problemas de Gateway Insight

January 30, 2024

Si la solución Gateway Insight no funciona como se esperaba, el problema podría estar relacionado con una de las siguientes opciones. Consulte las listas de comprobación de las secciones correspondientes para la solución de problemas.

- Configuración de Gateway Insight.
- Problema de conectividad entre NetScaler ADC y NetScaler ADM.
- Generación de registros en NetScaler ADC.
- Validaciones en NetScaler ADM.

Lista de comprobación de configuración de Gateway Insight

- Asegúrese de que la función AppFlow esté habilitada en NetScaler ADC. Para obtener más información, consulte Habilitar AppFlow.

- Compruebe la configuración de Gateway Insight en la configuración de NetScaler ADC en ejecución.

  Ejecute el comando `show running | grep -i <appflow_policy>` para comprobar la configuración de Gateway Insight. Asegúrese de que el tipo de enlace sea REQUEST. Por ejemplo:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- Para la implementación de un solo salto, Access Gateway o Unified Gateway, asegúrese de que la directiva Gateway Insight AppFlow esté enlazada al servidor virtual VPN, donde fluye el tráfico VPN. Para obtener más información, consulte Habilitar la recopilación de datos de HDX Insight
- Compruebe el parámetro «appflowlog» en el servidor virtual Citrix Gateway/VPN. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.

Lista de comprobación de conectividad entre NetScaler ADC y NetScaler ADM

- Compruebe el estado del recopilador AppFlow en NetScaler ADC. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler ADC y AppFlow Collector.
- Compruebe los aciertos de la directiva de Gateway Insight AppFlow.

  Ejecute el comando `show appflow policy <policy_name>` para comprobar los aciertos de la directiva de AppFlow.

  También puede ir a **Sistema > AppFlow > Directivas** en la GUI para comprobar los aciertos de las directivas de AppFlow.

- Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

Generación de registros en la lista de comprobación de NetScaler ADC

- Ejecute el comando `nsconmsg -d stats -g ai_tot` y compruebe los incrementos de las estadísticas en Citrix ADC.
- Capture los registros de Nstrace y compruebe si hay paquetes CFLOW para confirmar que Citrix ADC exporta los registros de AppFlow.

Validaciones en NetScaler ADM

- Ejecute el comando `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` para comprobar los registros y confirmar que Citrix ADM recibe registros de AppFlow.

- Asegúrese de que la instancia de NetScaler ADC se haya agregado a NetScaler ADM.
- Asegúrese de que el servidor virtual NetScaler Gateway/VPN tiene licencia en NetScaler ADM.

Estadísticas de Gateway In

Están disponibles las siguientes estadísticas de Gateway Insight.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_archivoinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_discordancia
- ai_tot_appflow_disabled

Póngase en contacto con el soporte técnico de Citrix

Para una resolución rápida, asegúrese de contar con la siguiente información antes de ponerse en contacto con el soporte técnico de Citrix:

- Detalles de la implementación y la topología de la red.
- Versiones de NetScaler ADC y NetScaler ADM.
- Paquete de soporte técnico para NetScaler ADC y NetScaler ADM.
- Instrace la captura durante la emisión.

Problemas conocidos

Consulte las notas de la versión de NetScaler ADC para obtener Insight sobre los problemas conocidos en Gate

Security Insight

January 30, 2024

Las aplicaciones web y de servicios web que están expuestas a Internet se han vuelto cada vez más vulnerables a los ataques. Para proteger las aplicaciones de los ataques, debe tener visibilidad de las amenazas, datos procesables en tiempo real sobre los ataques y recomendaciones sobre contramedidas. Security Insight proporciona una solución de panel único para ayudarle a evaluar el estado de seguridad de su aplicación y a tomar medidas correctivas para proteger sus aplicaciones.

> **Nota**
>
> Security Insight es compatible con Citrix Application Delivery Management (ADM) con dispositivos Citrix ADC que se ejecutan en la versión 11.0 Build 65.31 y versiones posteriores.

Cómo funciona Security Insight

Security Insight es una solución intuitiva de análisis de seguridad basada en paneles que le proporciona una visibilidad completa del entorno de amenazas asociado con sus aplicaciones. La información sobre seguridad se incluye en Citrix ADM y genera informes periódicamente basados en las configuraciones de seguridad del sistema Application Firewall y Citrix ADC. Los informes incluyen la siguiente información para cada aplicación:

- **Índice de amenazas.** Un sistema de clasificación de un solo dígito que indica la gravedad de los ataques a la aplicación, independientemente de si la aplicación está protegida o no por un dispositivo Citrix ADC. Cuanto más críticos sean los ataques a una aplicación, mayor será el índice de amenazas para esa aplicación. Los valores oscilan entre 1 y 7.

  El índice de amenazas se basa en la información de ataque. La información relacionada con el ataque, como el tipo de infracción, la categoría del ataque, la ubicación y los detalles del cliente, le brinda información sobre los ataques a la aplicación. La información de infracción se envía a NetScaler ADM solo cuando se produce una infracción o un ataque. Una gran cantidad de brechas y vulnerabilidades conducen a un valor elevado del índice de amenazas.

- **Índice de seguridad.** Sistema de clasificación de un solo dígito que indica con qué seguridad ha configurado las instancias NetScaler ADC para proteger las aplicaciones de amenazas y vulnerabilidades externas. Cuanto menores sean los riesgos de seguridad de una aplicación, mayor será el índice de seguridad. Los valores oscilan entre 1 y 7.

  El índice de seguridad considera tanto la configuración del firewall de aplicaciones como la configuración de seguridad del sistema NetScaler ADC. Para un valor de índice de seguridad elevado, ambas configuraciones deben ser fuertes. Por ejemplo, si se realizan comprobaciones

rigurosas del firewall de las aplicaciones pero no se han adoptado medidas de seguridad del sistema Citrix ADC, como una contraseña segura para el usuario nsroot, a las aplicaciones se les asigna un valor de índice de seguridad bajo.

- **Información procesable.** La información que necesita para reducir el índice de amenazas y aumentar el índice de seguridad, lo que mejora significativamente la seguridad de las aplicaciones. Por ejemplo, puede revisar la información sobre las infracciones, las configuraciones de seguridad existentes y faltantes para el firewall de aplicaciones y otras funciones de seguridad, la velocidad a la que se atacan las aplicaciones, etc.

Configurar Security Insight

Citrix ADM admite Security Insight desde todas las instancias de Citrix ADC que tengan configurado un firewall de aplicaciones.

Para configurar la información de seguridad en una instancia de ADC, primero configure un perfil de firewall de aplicaciones y una política de firewall de aplicaciones. Si bien, a continuación, puede vincular la directiva de firewall de aplicaciones de forma global, Citrix recomienda que la directiva esté enlazada al servidor virtual.

Para ver los análisis en Citrix ADM, habilite la función AppFlow en la instancia, configure un recopilador, una acción y una política de AppFlow y vincule la directiva de forma global. También en este caso, aunque puede vincular la directiva de firewall de aplicaciones de forma global, Citrix recomienda que la directiva esté enlazada al servidor virtual. Citrix también recomienda utilizar Citrix ADM para implementar las configuraciones de AppFlow en las instancias de ADC. Al configurar el recopilador, debe especificar la dirección IP del servidor NetScaler ADM en el que quiere supervisar los informes.

Para configurar la información de seguridad en una instancia de Citrix ADC:

1. Ejecute los siguientes comandos para configurar un perfil y una directiva de firewall de aplicaciones y enlazar la directiva de firewall de aplicaciones globalmente o al servidor virtual de equilibrio de carga.

---

add appfw profile [**-defaults** (basic advanced)]

---

set appfw profile <name> [**-startURLAction** <startURLAction> …]

add appfw policy <name> <rule> <profileName>

bind appfw global <policyName> <priority>

o,

bind lb vserver <lb vserver> **-policyName** <policy> **-priority** <priority>


```
add appfw profile pr_appfw -defaults advanced
set  appfw profile pr_appfw -startURLaction log stats learn
add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
   pr_appfw
bind appfw global pr_appfw_pol 1
or,
bind lb vserver outlook  – policyName pr_appfw_pol  – priority  “ 20
    ”
<!--NeedCopy-->
```

2. Ejecute los siguientes comandos para habilitar la función AppFlow, configurar un recopilador, una acción y una directiva de AppFlow y enlazar la directiva globalmente o al servidor virtual de equilibrio de carga:

   add appflow collector <name> **-IPAddress** <ipaddress>

---

set appflow param DISABLED)]
[**-SecurityInsightRecordInterval**]
[**-SecurityInsightTraffic** (ENABLED

---

agregar appflow action\ <name\ > **-collectors** \ <string\ >

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

O bien:

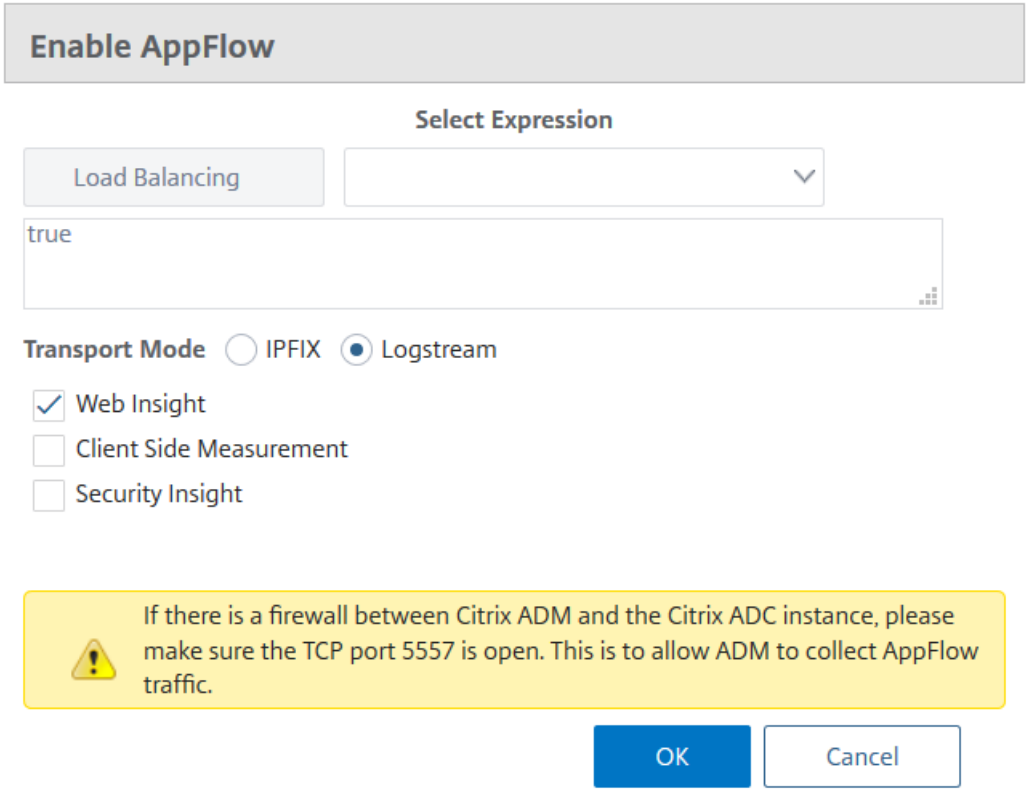
bind lb vserver <vserver> **-policyName** <policy> **-priority** <priority>

```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
   SecurityInsightTraffic ENABLED
add appflow action act1 -collectors col
add appflow action af_action_Sap_10.102.63.85 -collectors col
add appflow policy pol1 true act1
add appflow policy af_policy_Sap_10.102.63.85 true
   af_action_Sap_10.102.63.85
bind appflow global pol1 1 END -type REQ_DEFAULT
or,
bind lb vserver Sap  – policyName af_action_Sap_10.102.63.85  –
   priority  “ 20 ”
<!--NeedCopy-->
```

Para habilitar AppFlow desde Citrix ADM:

1. En un explorador web, escriba la dirección IP del **Citrix ADM** (por ejemplo, http://192.168.100.1).

2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Instancias** y seleccione la instancia de NetScaler ADC que quiere habilitar AppFlow.
4. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
5. Seleccione los servidores virtuales y haga clic en **Habilitar AppFlow** .
6. En el campo **Enable AppFlow** , escriba **true** y seleccione **Security Insight** .
7. Haga clic en **OK**.



Ver ubicaciones geográficas para los informes de Security Insight

Los informes de Security Insight incluyen las ubicaciones geográficas exactas desde las que se originan las solicitudes de los clientes. Puede ver las ubicaciones geográficas en Citrix ADM. El archivo de base de datos geográfica incorporado en Citrix ADC contiene la mayoría de las direcciones IP públicas. El archivo está disponible en la ubicación **/var/netscaler/inbuilt_db** en Citrix ADC.

Para habilitar las ubicaciones geográficas:

Ejecute los siguientes comandos para habilitar el registro de ubicación geográfica y el registro en formato CEF:

- **add locationFile** <Completar ruta con el nombre de archivo de la BD>
- **establecer la configuración de appfw -GeolocationLogging ON**
- **establecer la configuración de appfw -CEFLOGGING ON**

Si no hay ninguna dirección IP disponible en el archivo de base de datos geográfica, puede agregar la dirección IP para la ubicación geográfica. Junto con la dirección IP, también puedes añadir el nombre de una ciudad/estado/país y las coordenadas de latitud y longitud de cada ubicación.

Abra el archivo de base de datos geográfica con un editor de texto, como vi editor, y agregue una entrada para cada ubicación.

La entrada debe tener el siguiente formato:

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,
latitude
```

Por ejemplo,

```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
<!--NeedCopy-->
```

Reputación IP

Puede utilizar NetScaler Insight Center para supervisar y administrar la reputación IP de su tráfico entrante. Puede configurar directivas para agregar más IP como maliciosas y crear una lista de bloques personalizada.

Para obtener información sobre cómo configurar y usar la reputación de IP, consulte Reputación de IP.

Supervise la reputación de IP

La función Reputación de IP proporciona información relacionada con ataques sobre direcciones IP malintencionadas. Por ejemplo, informa de la puntuación de la reputación IP, la categoría de la reputación IP, el tiempo de ataque de la reputación IP, la IP del dispositivo y los detalles sobre la dirección IP del cliente.

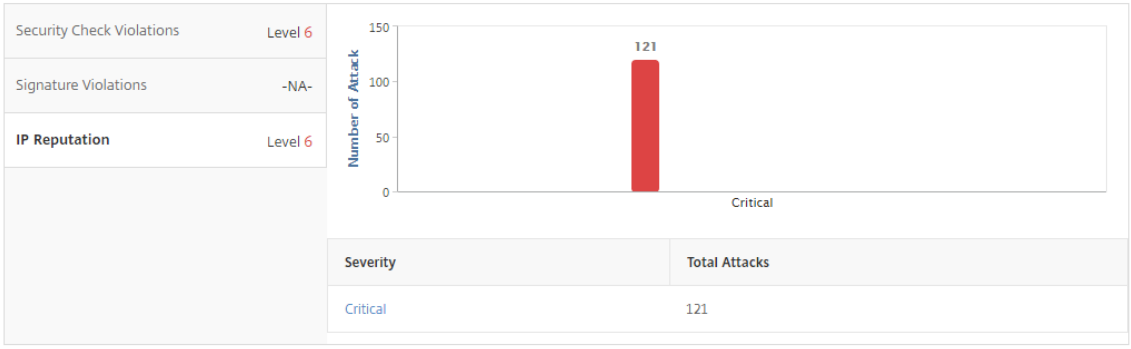
La puntuación de reputación IP indica el riesgo asociado a una dirección IP. La puntuación tiene los siguientes rangos:

Puntuación de reputación IP	Nivel de riesgo
1–20	Alto riesgo

Puntuación de reputación IP	Nivel de riesgo
21–40	Sospechoso
41–60	Riesgo moderado
61–80	Riesgo bajo
81–100	Confiable

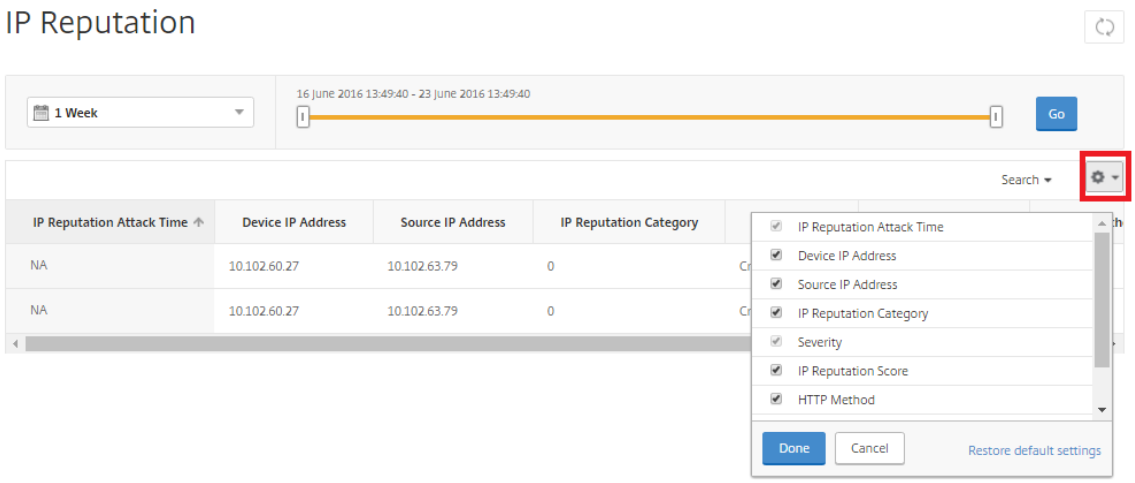
Para supervisar la reputación IP:

1. Vaya a **Analytics** > **Security Insight** y seleccione la aplicación que desea supervisar.
2. En la ficha **Índice de amenazas**, seleccione **Reputación de IP.**



3. Seleccione una gravedad para mostrar más detalles de los ataques que estaban en ese nivel. Puede hacer clic en el gráfico de barras o en la tabla situada debajo del gráfico.
4. Seleccione el período de tiempo para el que desea ver los detalles. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. A continuación, haga clic en **Ir**.

5. Para personalizar la pantalla, haga clic en el botón de configuración.



Umbrales

Puede establecer y ver los umbrales del índice de seguridad y el índice de amenazas de las aplicaciones en Security Insight.

Para establecer un umbral:

1. Vaya a **Analytics** > **Configuración** > **Umbrales** y seleccione **Agregar** .
2. Seleccione el tipo de tráfico como **Seguridad** en el campo **Tipo de tráfico** e introduzca la información requerida en los demás campos correspondientes, como Nombre, Duración y entidad.
3. En la sección **Configurar regla** , utilice los campos Métrica, Comparador y Valor para establecer un umbral.

   Por ejemplo, “Índice de amenazas”“>”“5”

4. En la **configuración** de notificaciones , selecciona el tipo de notificación.
5. Haga clic en **Crear**.

Para ver los incumplimientos de los umbrales:

1. Vaya a **Analytics** > **Security Insight** > **Dispositivos** y seleccione la instancia de Citrix ADC.
2. En la sección **Aplicación**, puede ver el número de infracciones de umbral ocurridas para cada servidor virtual en la columna **Infracción de umbral**.

Casos de uso de Security Insight

En los siguientes casos de uso se describe cómo puede utilizar Security Insight para evaluar la exposición a las amenazas de las aplicaciones y mejorar las medidas de seguridad.

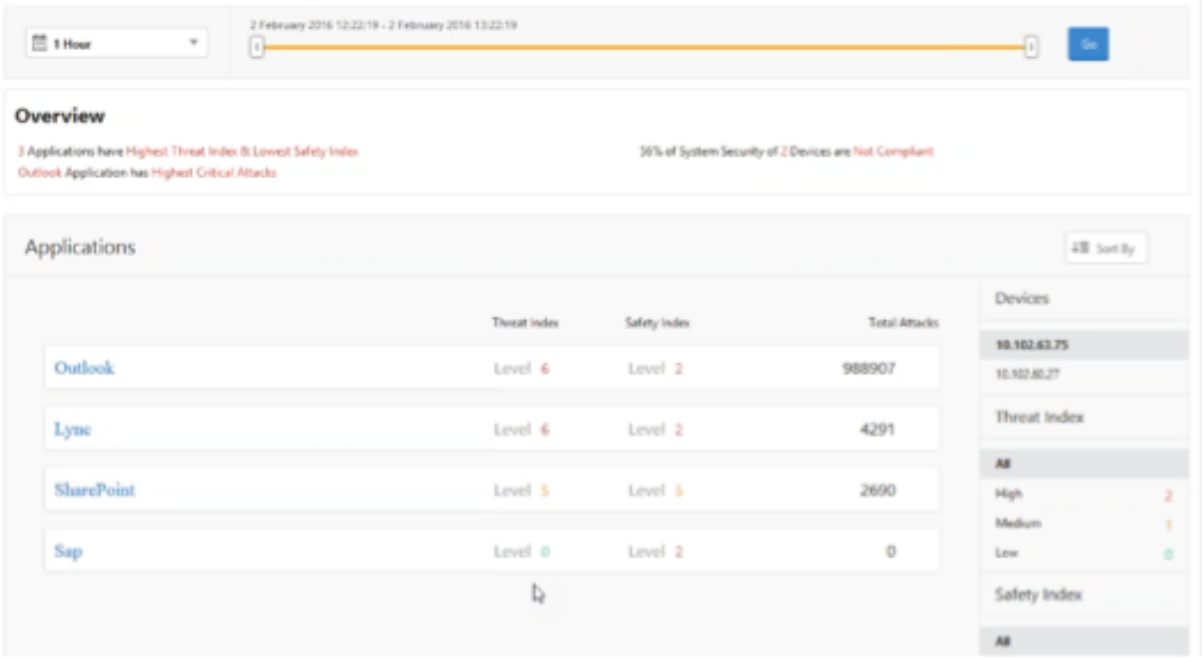
Obtenga una visión general del entorno de amenazas

En este caso de uso, tiene un conjunto de aplicaciones expuestas a ataques y ha configurado NetScaler ADM para supervisar el entorno de amenazas. Debe revisar con frecuencia el índice de amenazas, el índice de seguridad y el tipo y la gravedad de los ataques que podrían haber sufrido las aplicaciones. Esta revisión le permite centrarse primero en las aplicaciones que necesitan más atención. El panel de información de seguridad proporciona un resumen de las amenazas experimentadas por las aplicaciones durante un período de tiempo que elija y para un dispositivo NetScaler ADC seleccionado. Muestra la lista de aplicaciones, sus índices de amenazas y seguridad y el número total de ataques durante el período de tiempo elegido.

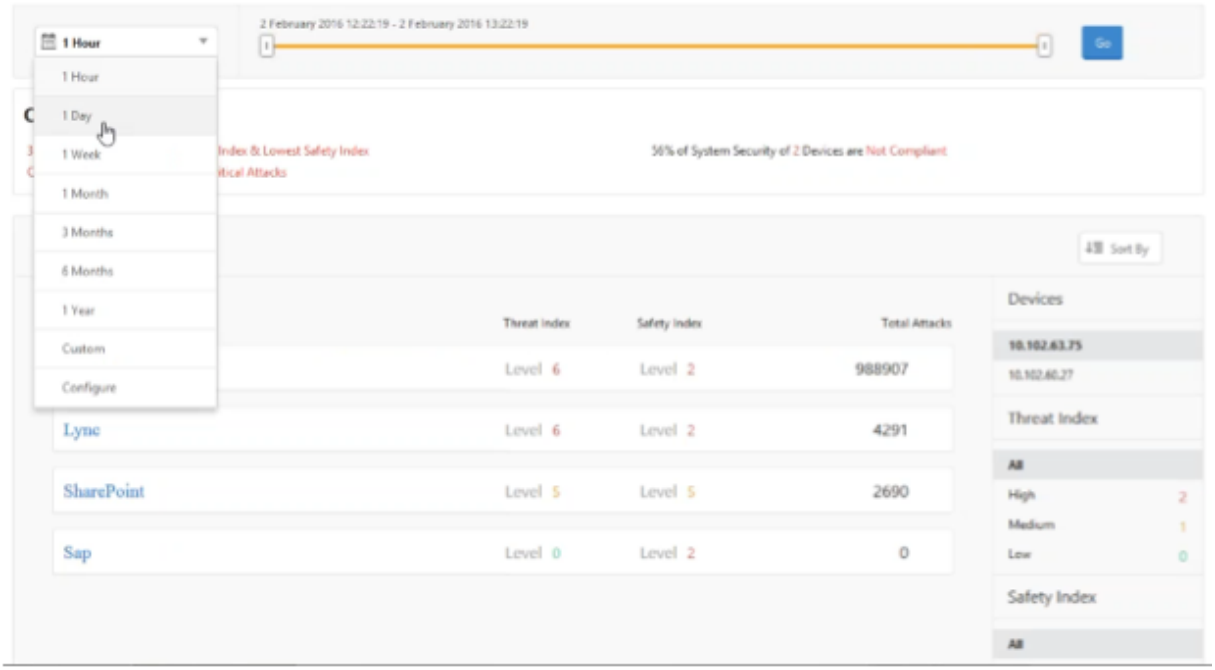
Por ejemplo, es posible que esté supervisando Microsoft Outlook, Microsoft Lync, SharePoint y una aplicación SAP, y es posible que desee revisar un resumen del entorno de amenazas para estas aplicaciones.

Para obtener un resumen del entorno de amenazas, inicie sesión en **NetScaler ADM**y, a continuación, vaya a **Analytics > Security Insight**.

Se muestra información clave para cada aplicación. El período de tiempo predeterminado es 1 hora.



Para ver información de un período de tiempo diferente, seleccione un período de tiempo en la lista situada en la parte superior izquierda.



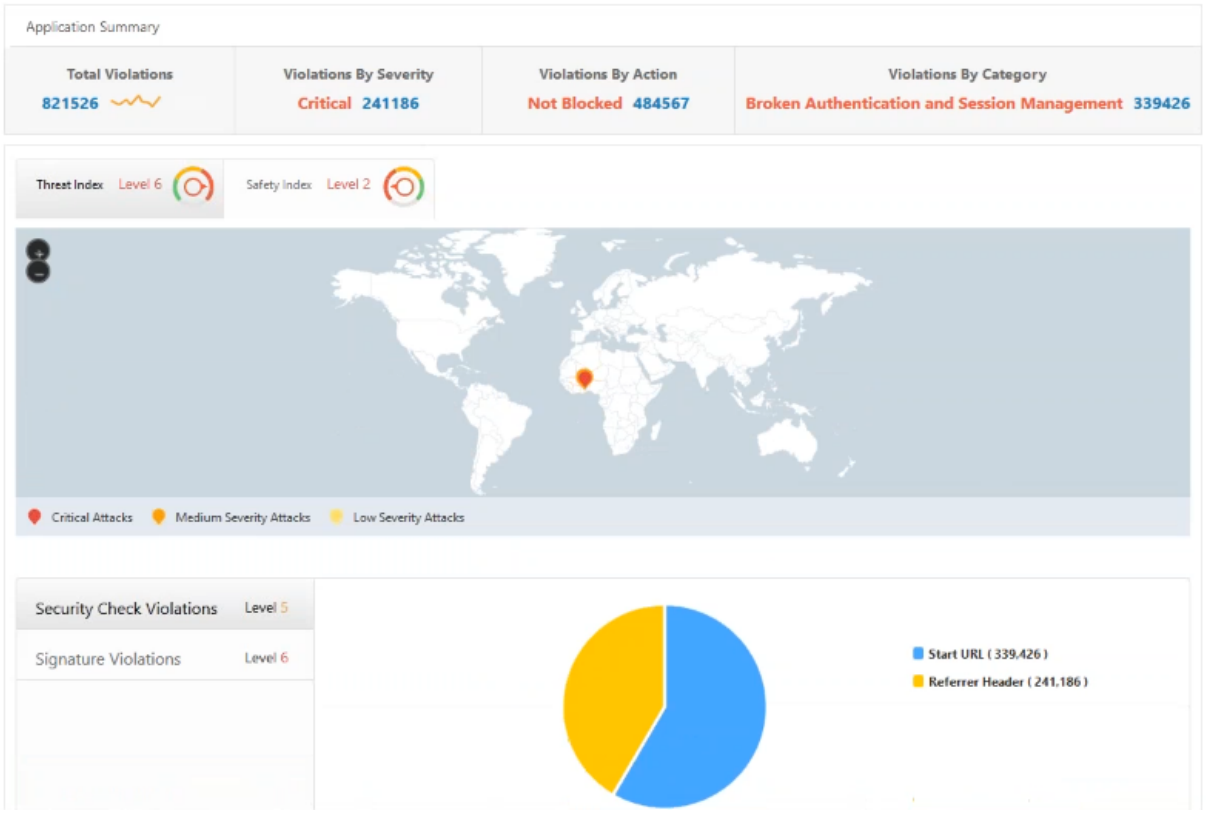
Para ver un resumen de otra instancia de NetScaler ADC, en **Dispositivos**, haga clic en la dirección IP de la instancia de NetScaler ADC. Para ordenar la lista de aplicaciones por una columna determinada, haga clic en el encabezado de la columna.

Determinar la exposición a amenazas de una aplicación

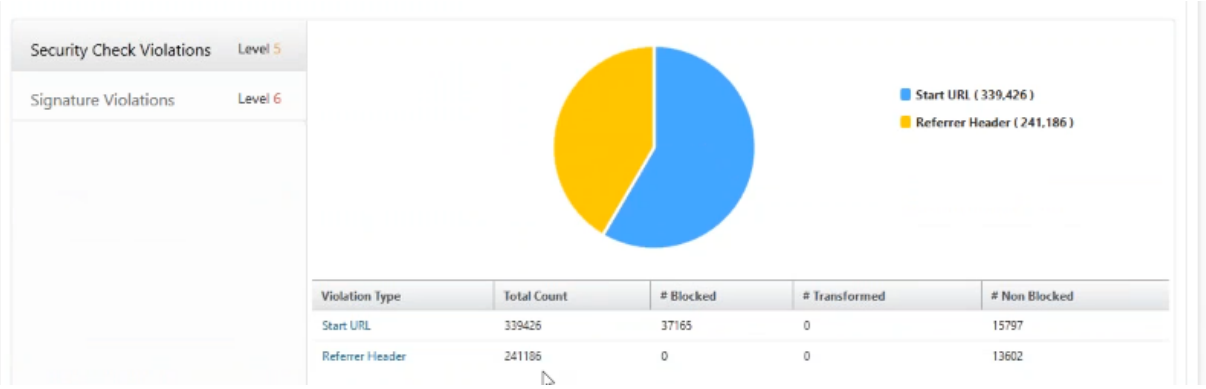
Para identificar las aplicaciones que tienen un índice de amenazas alto y un índice de seguridad bajo en el panel de control de Security Insight, debe determinar la exposición a las amenazas antes de decidir protegerlas. Es decir, desea determinar el tipo y la gravedad de los ataques que han degradado sus valores de índice. Puede determinar la exposición a amenazas de una aplicación consultando el resumen de la solicitud.

En este ejemplo, Microsoft Outlook tiene un valor de índice de amenazas de 6 y desea saber qué factores contribuyen a este índice de amenazas alto.

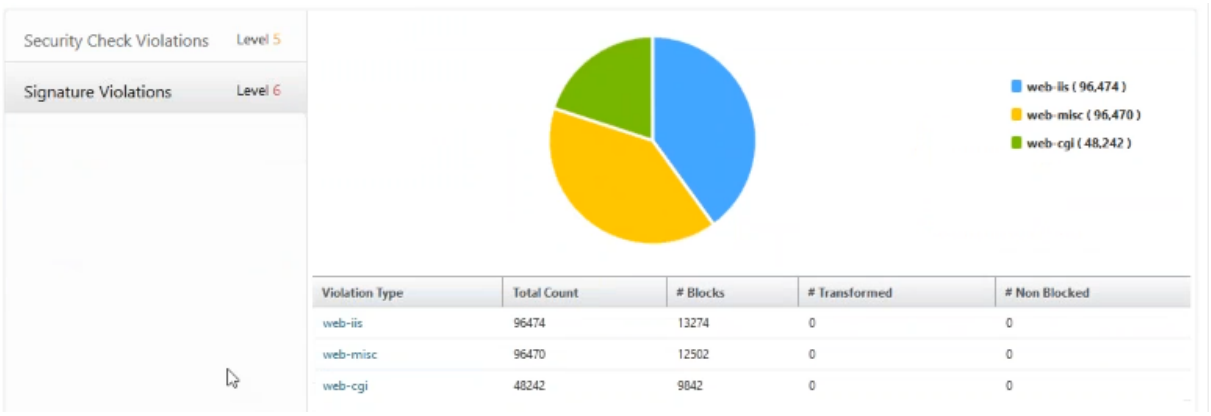
Para determinar la exposición a amenazas de Microsoft Outlook, en el panel **Security Insight** , haga clic en **Outlook** . El resumen de la aplicación incluye un mapa que identifica la ubicación geográfica del servidor.



Haga clic en **Índice de amenazas > Infracciones de comprobación de seguridad** y revise la información de infracción que aparece.



Haga clic en **Infracciones de firma** y revise la información de infracción que aparece.

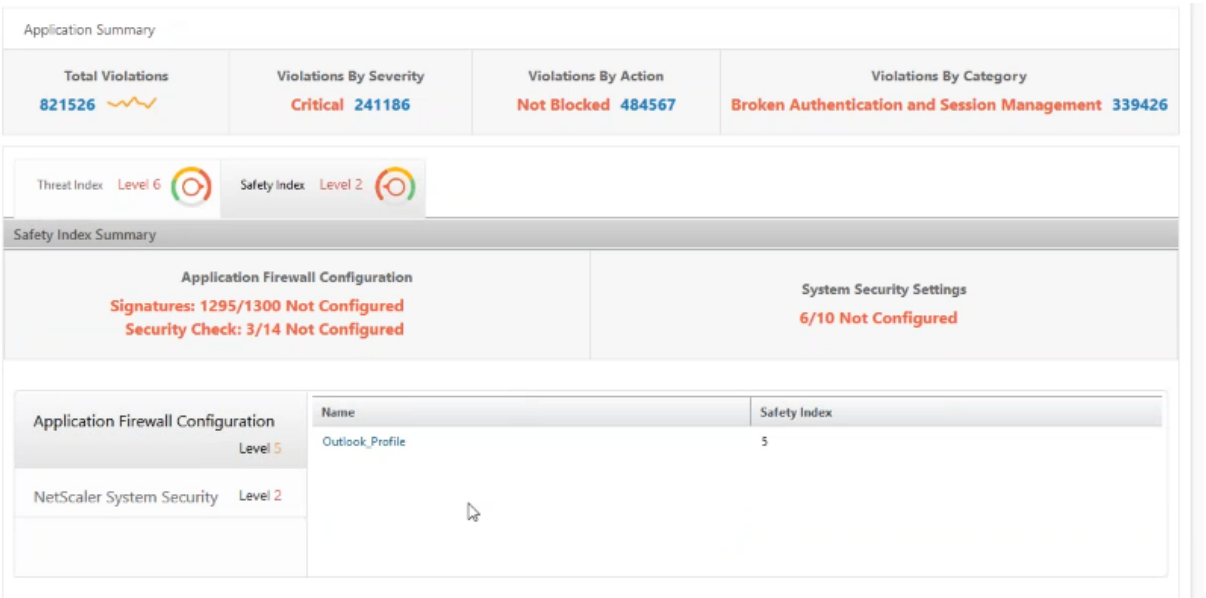


Determinar la configuración de seguridad existente y faltante para una aplicación

Después de revisar la exposición a amenazas de una aplicación, quiere determinar qué configuraciones de seguridad de la aplicación están implementadas y qué configuraciones faltan para esa aplicación. Puede obtener esta información profundizando en el resumen del índice de seguridad de la aplicación.

El resumen del índice de seguridad proporciona información sobre la eficacia de las siguientes configuraciones de seguridad:

- **Configuración del firewall de aplicaciones.** Muestra cuántas entidades de firma y seguridad no están configuradas.
- **Seguridad del sistema NetScaler.** Muestra cuántas opciones de seguridad del sistema no están configuradas.

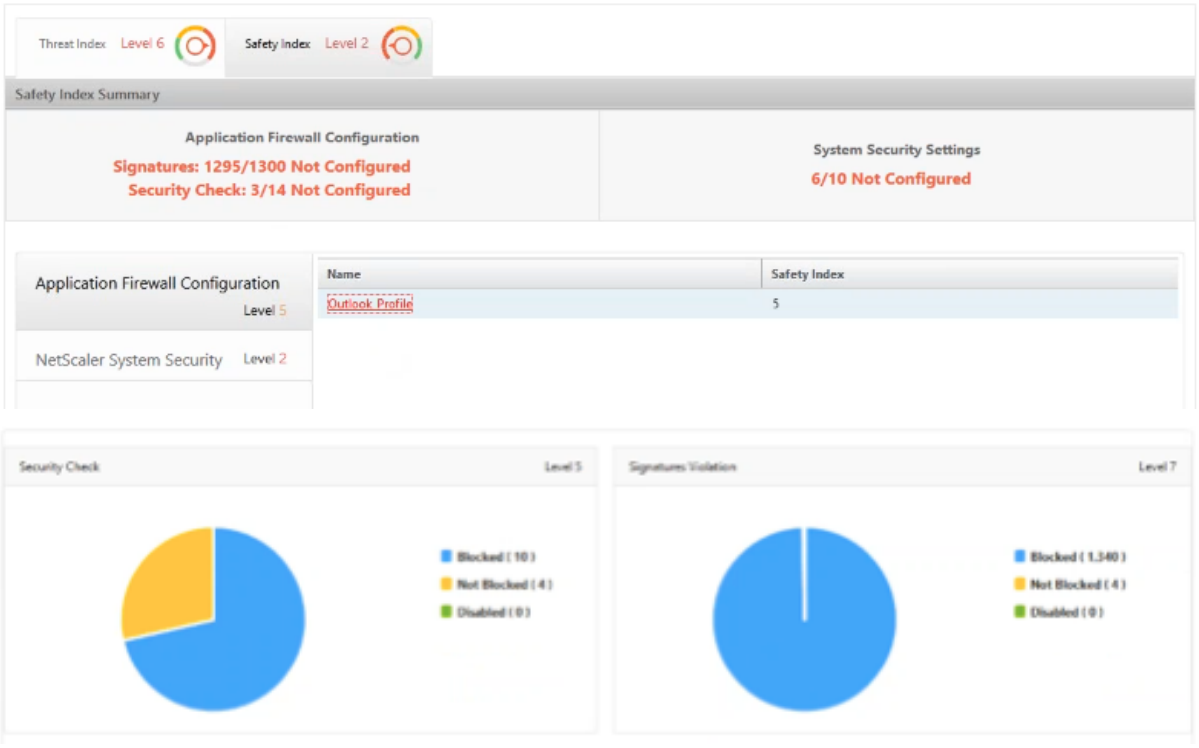


En el caso de uso anterior, revisó la exposición a amenazas de Microsoft Outlook, que tiene un valor de

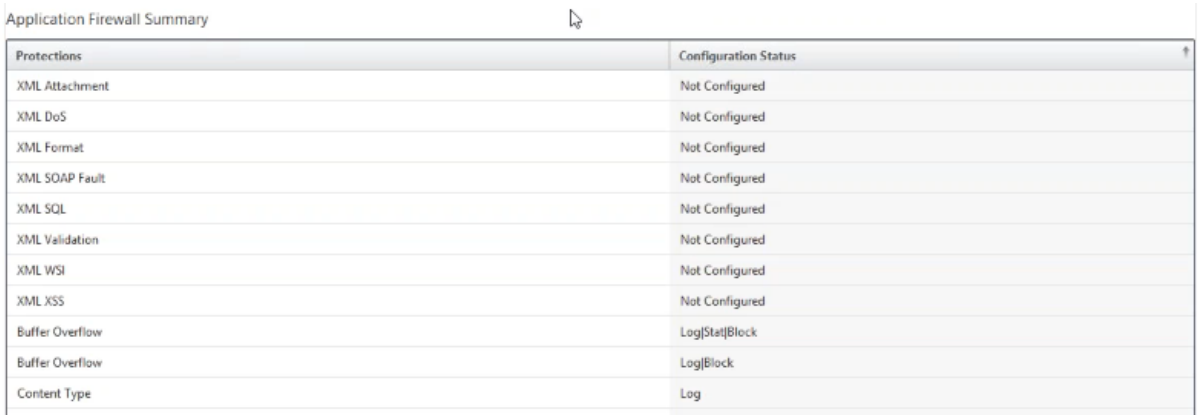
índice de amenazas de 6. Ahora, desea saber qué configuraciones de seguridad existen para Outlook y qué configuraciones se pueden agregar para mejorar su índice de amenazas.

En el panel **Security Insight** , haga clic en **Outlook** y, a continuación, en la pestaña **Índice de seguridad** . Revise la información proporcionada en el área **Resumen del índice de seguridad**.

En el nodo **Configuración del firewall de aplicaciones**, haga clic en **Outlook_Profile** y revise la información de comprobación de seguridad e infracción de firmas en los gráficos circulares.



Revise el estado de configuración de cada tipo de protección en la tabla de resumen del firewall de aplicaciones. Para ordenar la tabla en una columna, haga clic en el encabezado de la columna.

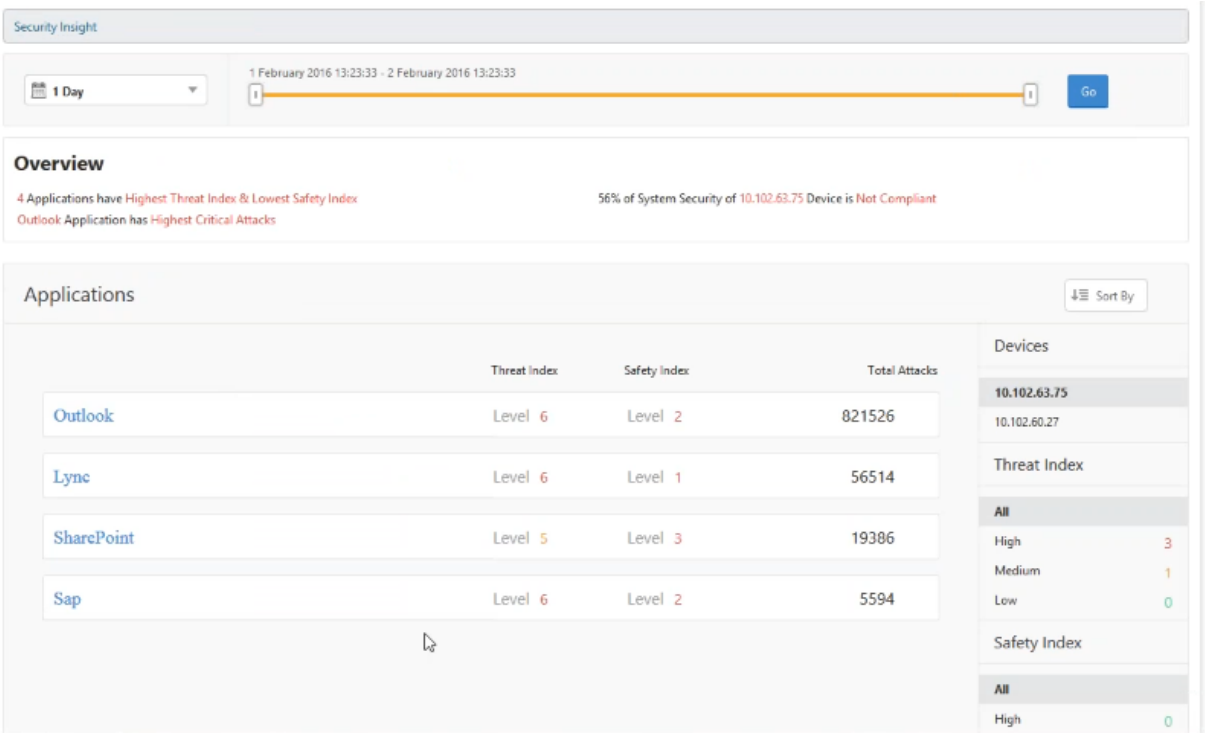


Haga clic en el nodo **NetScaler System Security** y revise la configuración de seguridad del sistema y las recomendaciones de Citrix para mejorar el índice de seguridad de las aplicaciones.

Identificar aplicaciones que requieren atención inmediata

Las aplicaciones que requieren atención inmediata son aquellas que tienen un índice de amenaza alto y un índice de seguridad bajo.

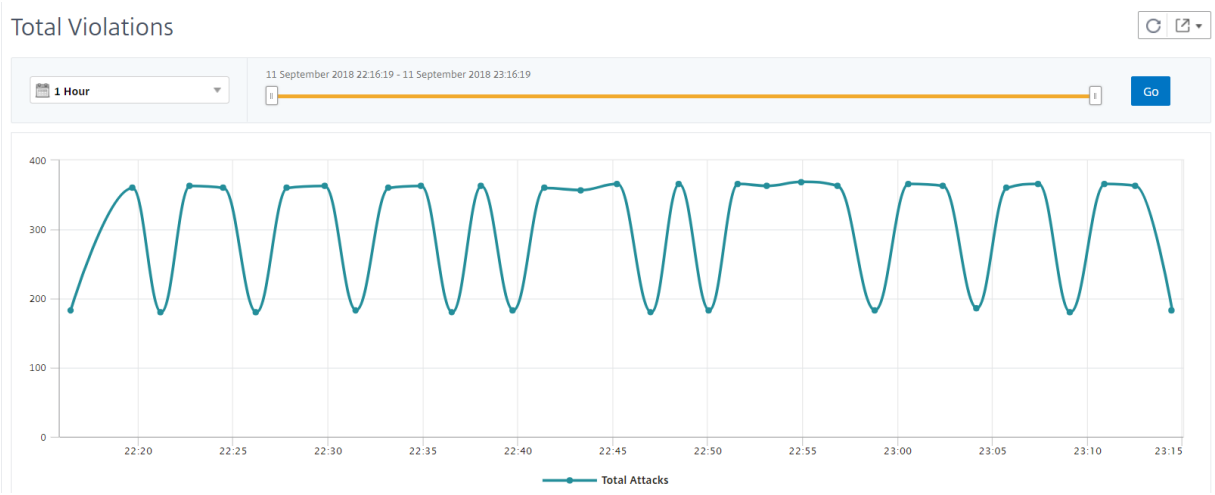
En este ejemplo, tanto Microsoft Outlook como Microsoft Lync tienen un valor de índice de amenazas alto de 6, pero Lync tiene el menor de los dos índices de seguridad. Por lo tanto, es posible que tenga que centrar su atención en Lync antes de mejorar el entorno de amenazas para Outlook.



Determine la cantidad de ataques en un período de tiempo determinado

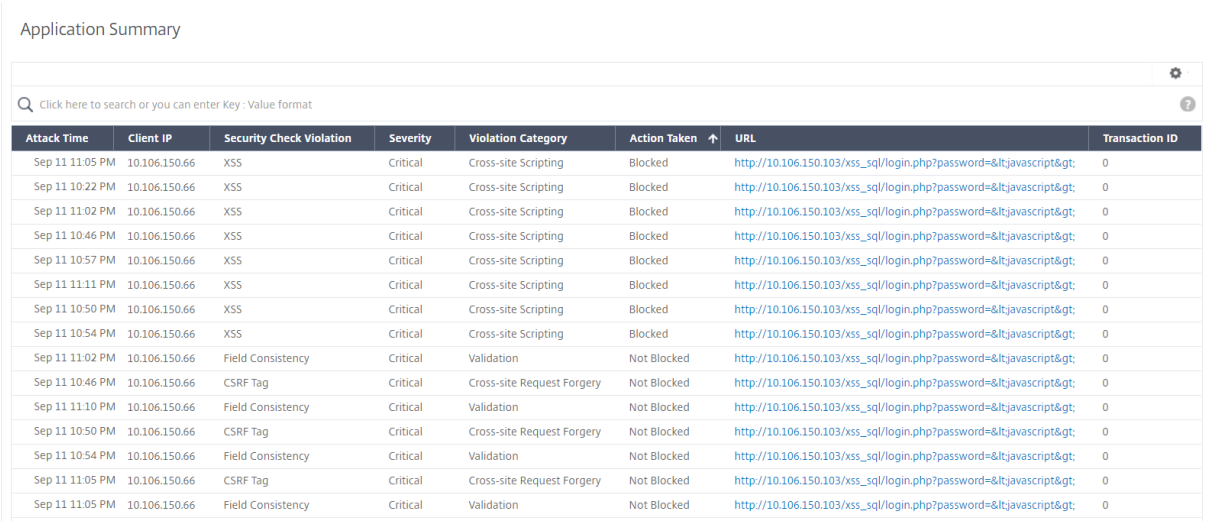
Es posible que quiera determinar cuántos ataques se produjeron en una aplicación determinada en un momento determinado o que quiera estudiar la tasa de ataques durante un período de tiempo específico.

En la página Security Insight, haga clic en cualquier aplicación y, en el **Resumen** de la solicitud , haga clic en el número de infracciones. La página Total de Infracciones muestra los ataques de forma gráfica durante una hora, un día, una semana y un mes.

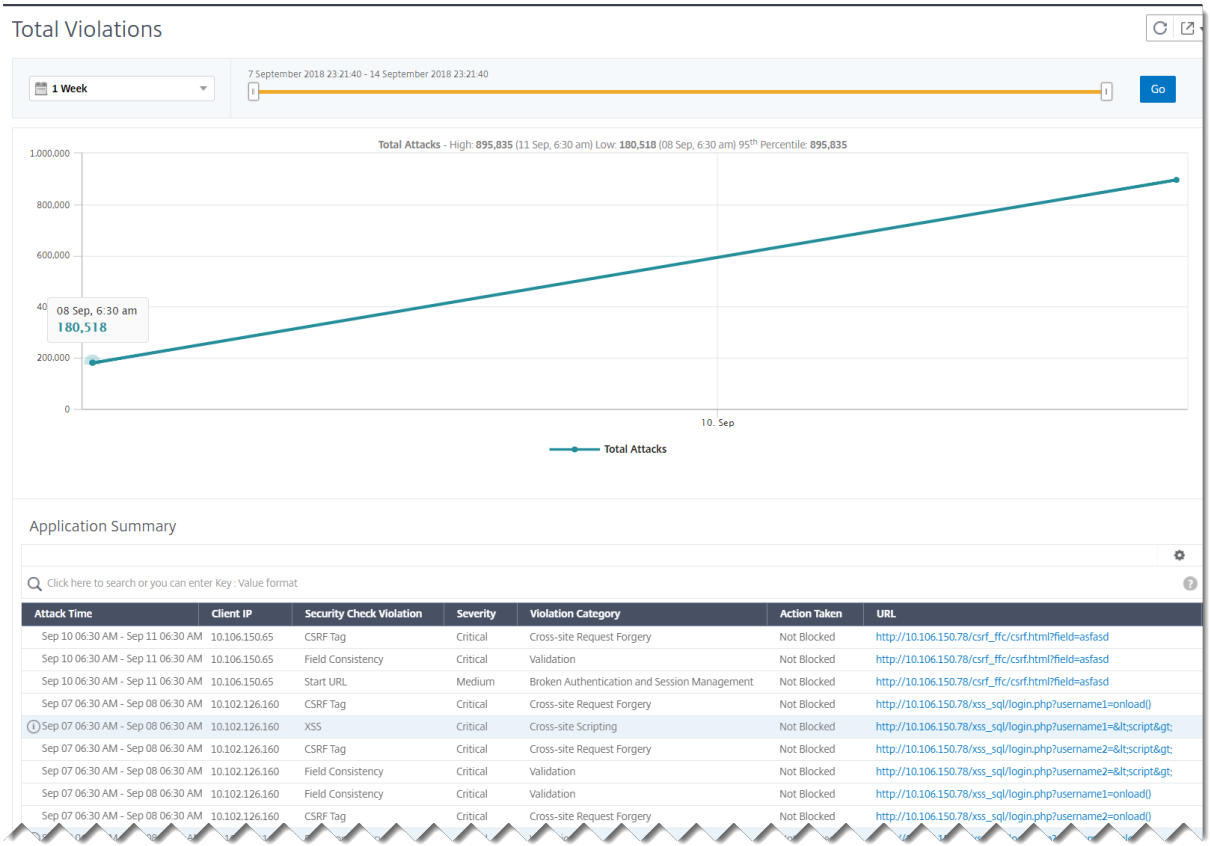


La tabla Resumen de la aplicación proporciona los detalles sobre los ataques. Algunos de ellos son los siguientes:

- Tiempo de ataque
- Dirección IP del cliente desde el que se produjo el ataque
- Gravedad
- Categoría de infracción
- URL desde la que se originó el ataque y otros detalles.



Aunque siempre puede ver la hora del ataque en un informe por hora como se ve en la imagen, ahora puede ver el intervalo de tiempo de ataque para los informes agregados, incluso para los informes diarios o semanales. Si selecciona «1 día» en la lista de períodos de tiempo, el informe Security Insight muestra todos los ataques agregados y el tiempo de ataque se muestra en un rango de una hora. Si elige "1 semana"o "1 mes", todos los ataques se agregan y el tiempo de ataque se muestra en un intervalo de un día.

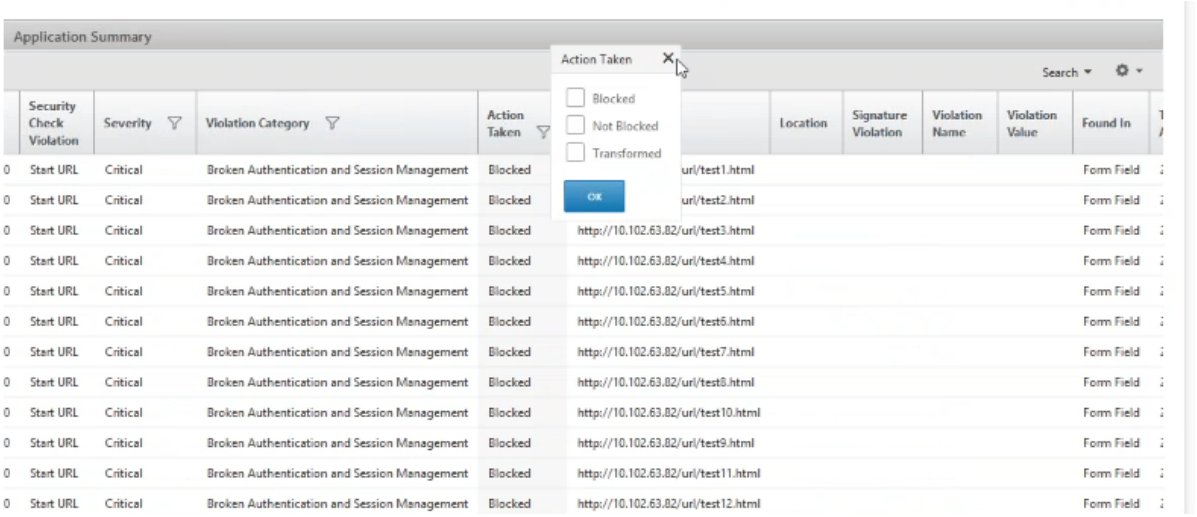


Obtener información detallada sobre infracciones de seguridad

Es posible que desee ver una lista de los ataques a una aplicación y obtener información sobre el tipo y la gravedad de los ataques, las acciones realizadas por la instancia de Citrix ADC, los recursos solicitados y el origen de los ataques.

Por ejemplo, es posible que desee determinar cuántos ataques a Microsoft Lync se bloquearon, qué recursos se solicitaron y las direcciones IP de las fuentes.

En el **panel Security Insight**, haga clic en **Lync > Total de infracciones**. En la tabla, haga clic en el icono de filtro en el encabezado de columna **Acción tomada** y, a continuación, seleccione **Bloqueado**.



Para obtener información acerca de los recursos solicitados, revise la columna **URL**. Para obtener información sobre las fuentes de los ataques, consulte la columna **IP del cliente** .

Ver detalles de expresiones de registro

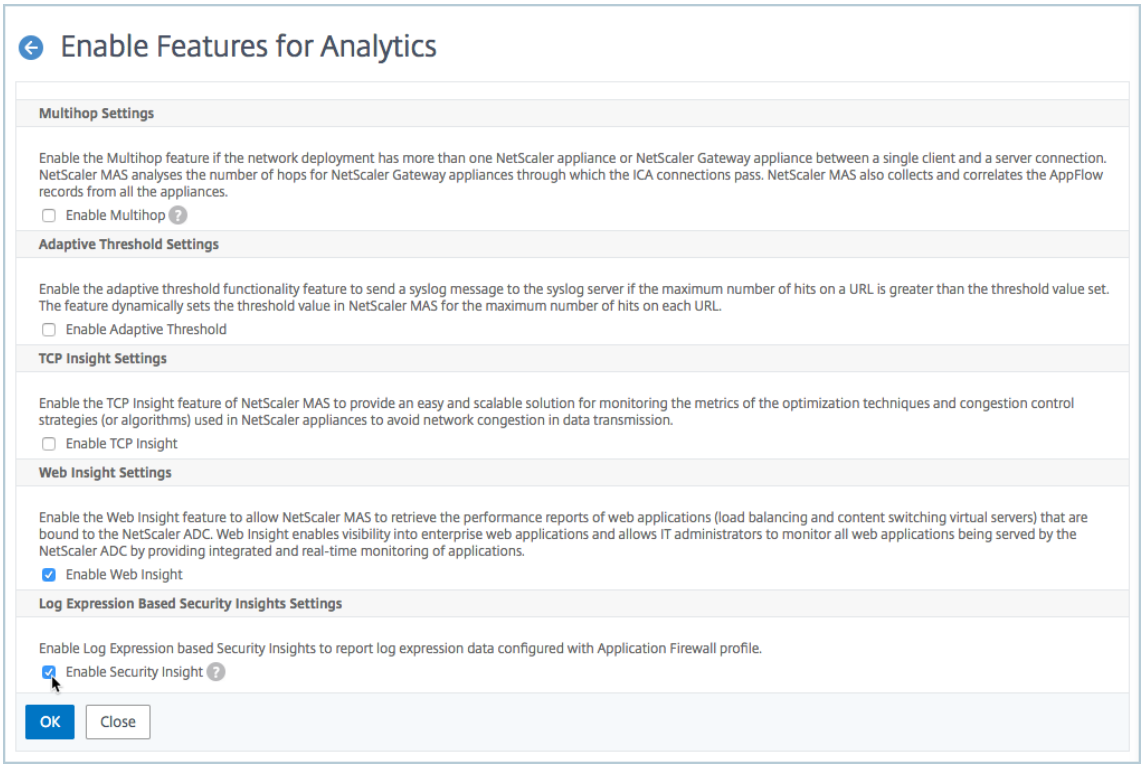
Las instancias de Citrix ADC utilizan expresiones de registro configuradas con el perfil de Application Firewall para tomar medidas en caso de ataques a una aplicación de la empresa. En Security Insight, puede ver los valores devueltos para las expresiones de registro utilizadas por la instancia de Citrix ADC. Estos valores incluyen el encabezado de la solicitud, el cuerpo de la solicitud, etc. Además de los valores de las expresiones de registro, también puede ver el nombre de la expresión de registro y el comentario de la expresión de registro definida en el perfil de Application Firewall que la instancia de Citrix ADC utilizó para tomar medidas contra el ataque.

Requisitos previos Asegúrese de que:

- Configure expresiones de registro en el perfil de Firewall de aplicaciones. Para obtener más información, consulte Application Firewall.

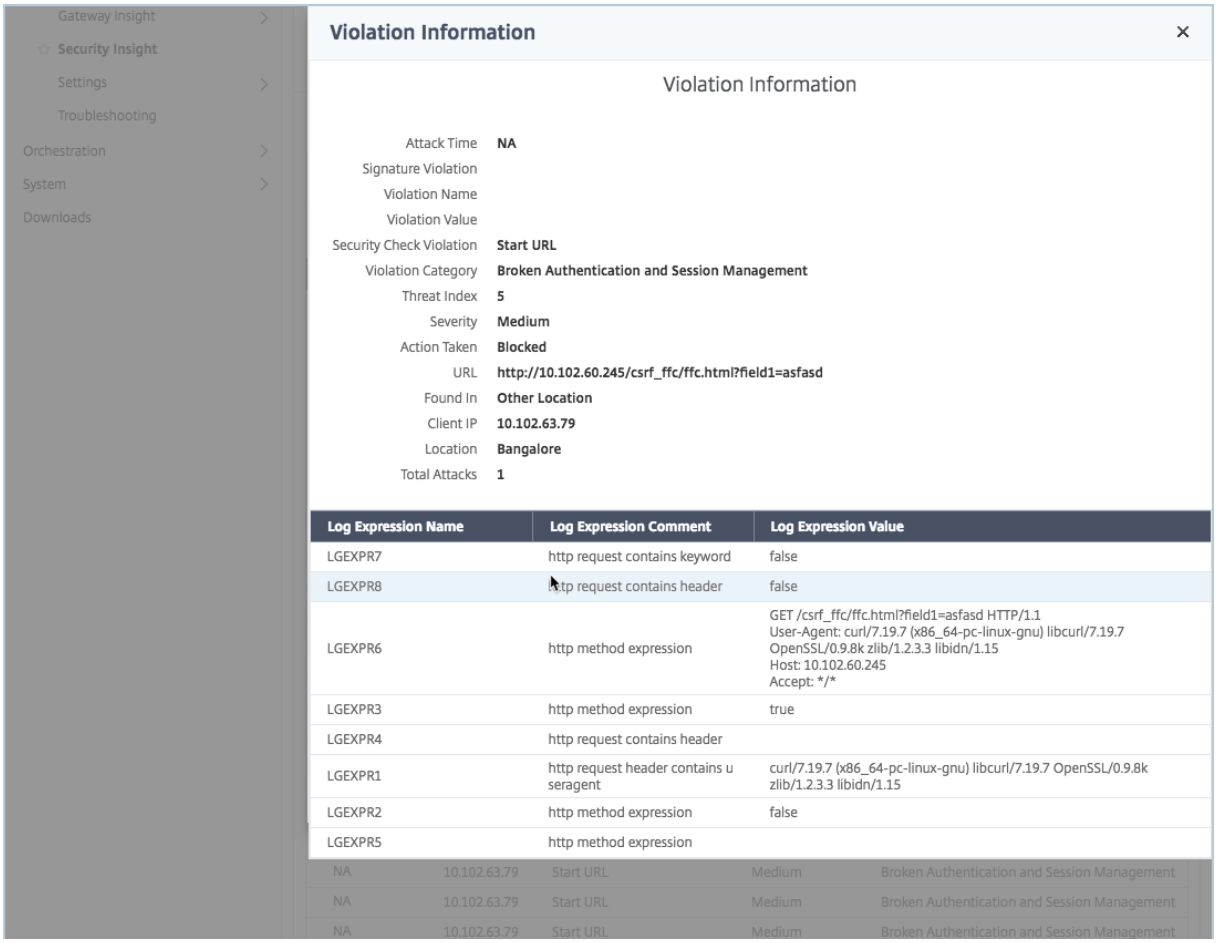
- Habilite la configuración Security Insights basada en expresiones de registro en Citrix ADM. Haga lo siguiente:

  1. Vaya a **Analytics > Configuración** y haga clic en **Habilitar funciones para Analytics** .
  2. En la página Habilitar función para análisis, seleccione **Habilitar Security Insight** en la sección **Configuración de Security Insight basada en expresiones de registro** y haga clic en **Aceptar**.



Por ejemplo, es posible que desee ver los valores de la expresión de registro devuelta por la instancia de Citrix ADC para la acción que llevó a cabo para atacar Microsoft Lync en su empresa.

En el panel de control de Security Insight, vaya a **Lync > Total de infracciones**. En la **tabla Resumen de la aplicación**, haga clic en la dirección URL para ver los detalles completos de la infracción en la página **Información de infracción**, incluidos el nombre de la expresión de registro, el comentario y los valores devueltos por la instancia de NetScaler ADC para la acción.

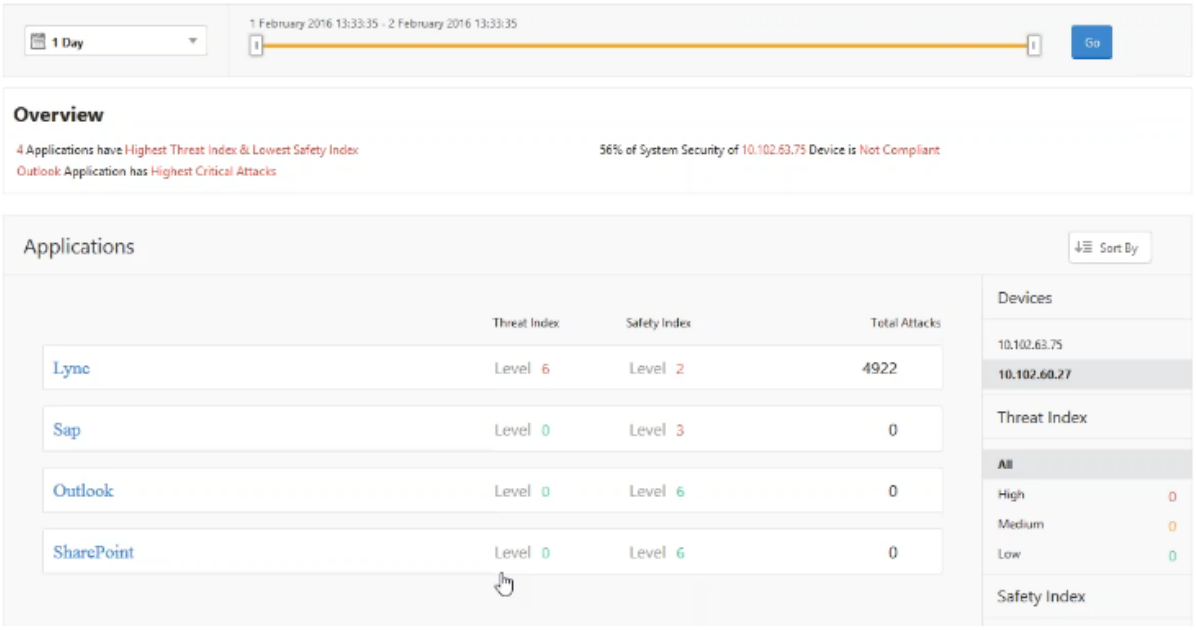


Determine el índice de seguridad antes de implementar la configuración

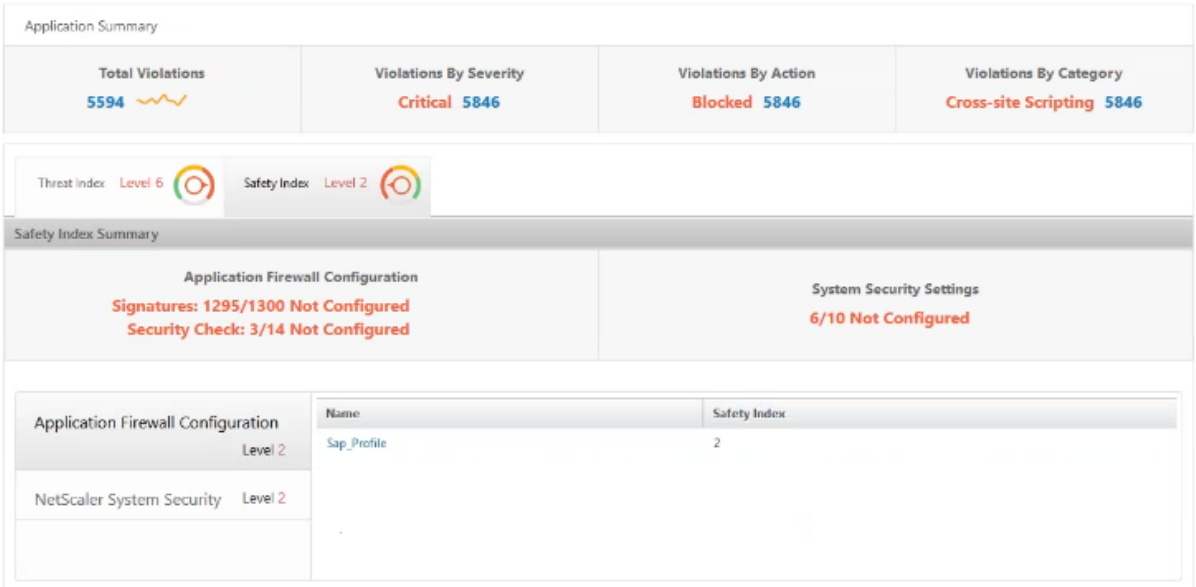
Las infracciones de seguridad se producen después de implementar la configuración de seguridad en una instancia de NetScaler ADC, pero es posible que quiera evaluar la eficacia de la configuración de seguridad antes de implementarla.

Por ejemplo, es posible que desee evaluar el índice de seguridad de la configuración de la aplicación SAP en la instancia de Citrix ADC con la dirección IP 10.102.60.27.

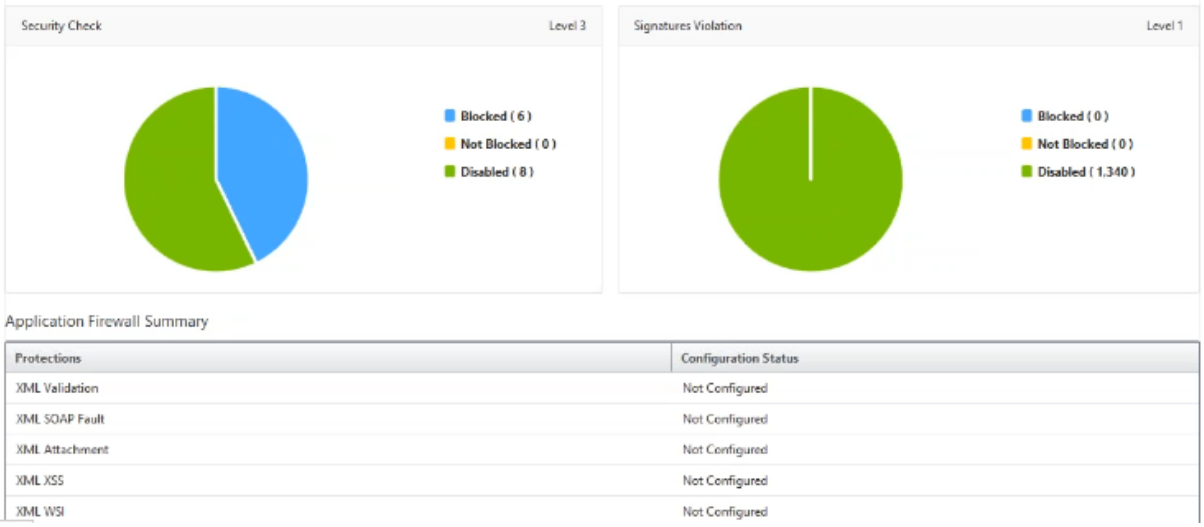
En el panel **Security Insight** , en **Dispositivos** , haga clic en la dirección IP de la instancia de Citrix ADC que configuró. Puede ver que tanto el índice de amenazas como el número total de ataques son 0. El índice de amenazas es un reflejo directo del número y el tipo de ataques a la aplicación. Cero ataques indican que la aplicación no está bajo ninguna amenaza.



Haga clic en **Sap > Índice de seguridad > SAP_profile** y evalúe la información del índice de seguridad que aparece.



En el resumen del firewall de la aplicación, puede ver el estado de configuración de diferentes configuraciones de protección. Si se establece una configuración para registrar o si no se ha configurado una configuración, se asigna a la aplicación un índice de seguridad inferior.



Insight SSL

January 30, 2024

SSL Insight proporciona visibilidad de las transacciones web seguras (HTTPS) y permite a los administradores de TI monitorear todas las aplicaciones web seguras que ofrece NetScaler ADC al proporcionar una supervisión histórica e integrada en tiempo real de las transacciones web seguras. Con esta visibilidad, el administrador puede evaluar lo siguiente:

- **Determine el impacto del cambio de configuración en el uso**de los clientes: el administrador puede comprender el impacto en los clientes de realizar un cambio de configuración, como desactivar SSLv3 o eliminar un cifrado como el RC4-MD5. Esto se puede hacer evaluando los datos históricos de transacciones en este protocolo y cifrado.
- **Cuantificar el rendimiento del cliente**: El administrador puede comprender el impacto en el tiempo de respuesta de la aplicación según los cifrados/protocolo SSL utilizados o los certificados negociados.
- **Seguridad**de las aplicaciones : evalúe si alguna de las aplicaciones tiene transacciones que se ejecutan con protocolos de baja seguridad, cifrados o claves con un nivel de seguridad débil.

Cuando SSL Analytics está habilitado en una instancia de NetScaler ADC, las estadísticas SSL se registran y registran para cada transacción SSL. Las estadísticas muestran los detalles del flujo SSL. Además, Citrix Application Delivery Management (ADM)
registra y muestra cada conexión correcta .

SSL Insight proporciona la siguiente información crítica, que muestra NetScaler ADM Analytics:

- Versión del protocolo SSL negociada
- El cifrado negociado y la fuerza del cifrado
- Algoritmo de hash de firma del certificado utilizado
- Tipo y tamaño de certificado
- Errores de frontend y backend de SSL

> **Nota**
>
> Para conexiones SSL correctas, el registro SSL AppFlow ocurre al final de cada transacción.

Requisitos previos

- La instancia de NetScaler ADC en la que pretende configurar SSL Insight debe ejecutar la versión 11.1 51.21 y superior del software NetScaler ADC. Ejecute los siguientes comandos en la instancia ADC que ejecuta 11.1 51.21 para habilitar Logstream como tipo de transporte para SSL Insight.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   Para las instancias ADC que ejecutan la versión 12.0 y superior, seleccione Logstream como tipo de transporte mientras habilita AppFlow desde ADM.

- La versión y la compilación de NetScaler ADM deben ser iguales o superiores a la versión y la compilación de NetScaler ADC. Por ejemplo, si ha instalado NetScaler ADM 11.1 build 61.7, asegúrese de haber instalado NetScaler ADC 11.1 build 60.14 o anterior.

Configuración de SSL Insight

Las Métricas de Insight SSL se incluyen en los informes de Web Insight si habilita los siguientes elementos:

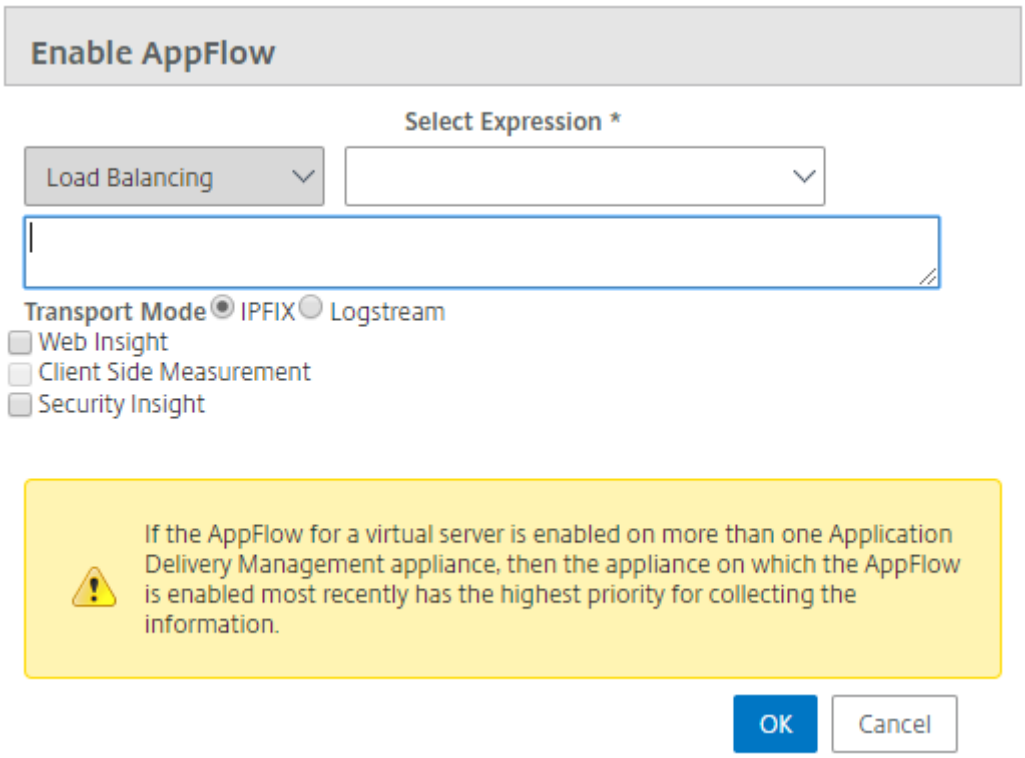
- Habilite AppFlow for Web Insight en cada instancia de Citrix ADC.
- Habilite el modo ULFD en cada instancia de Citrix ADC.
- Habilite los parámetros necesarios de AppFlow en cada instancia de NetScaler ADC.

Activación de la función AppFlow

> **Nota**
>
> Puede habilitar la función AppFlow desde Citrix ADM o desde cada instancia de Citrix ADC.

Para habilitar la función AppFlow desde Citrix ADM:

1. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC en la que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione los servidores virtuales y haga clic en **Habilitar AppFlow** .
4. En el campo Enable AppFlow, escriba **true** y seleccione **Web Insight** .
5. Repita los pasos del 3 al 6 en cada instancia de Citrix ADC.
6. Haga clic en **Aceptar**.



> **Nota**
>
> No puede habilitar la recopilación de datos en un servidor virtual si el estado operativo del servidor virtual es distinto de UP.

Para habilitar la función AppFlow mediante la GUI de NetScaler ADC:

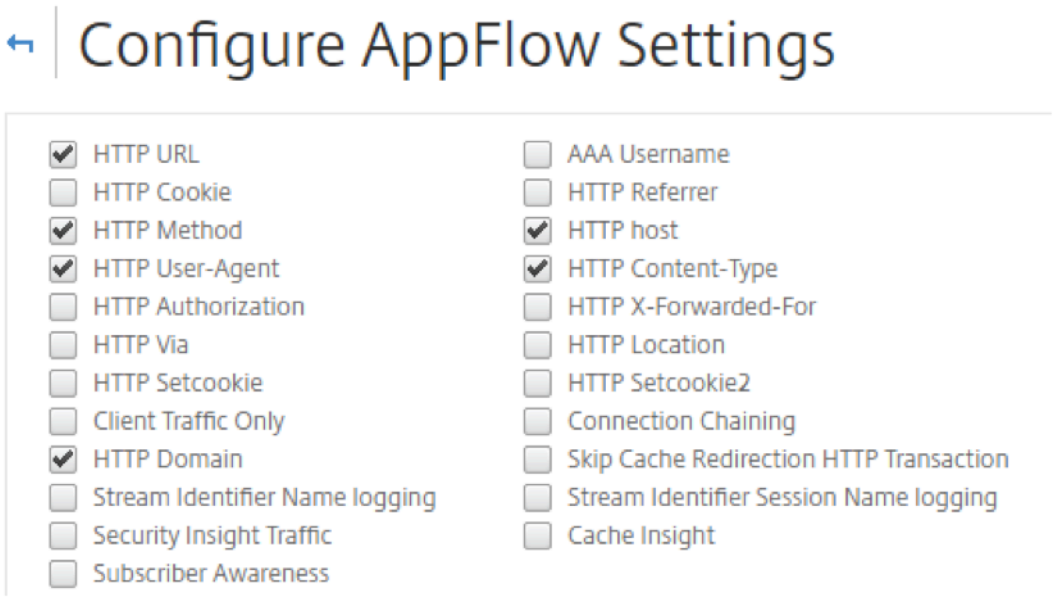
En la GUI de una instancia de NetScaler ADC, vaya a **Configuración** > **Sistema** > **Configuración**, haga clic en **Configurar funciones avanzadas** y seleccione **AppFlow**.

Activación de los parámetros de SSL Insight

En cada instancia de NetScaler ADC, debe habilitar algunos parámetros HTTP para mostrar registros SSL Insight en NetScaler ADM.

Para habilitar los parámetros de SSL Insight desde la utilidad de configuración Citrix ADC:

1. Vaya a **Configuración** > **Sistema** > **AppFlow**y haga clic en **Cambiar configuración de AppFlowSettings**.
2. Seleccione las siguientes casillas de verificación: **dominio HTTP, hostHTTP, método HTTP**, **URL HTTP, agente de usuarioHTTP, tipo de contenido HTTP**.
3. Haga clic en **Aceptar**.



Visualización de las métricas de SSL Insight

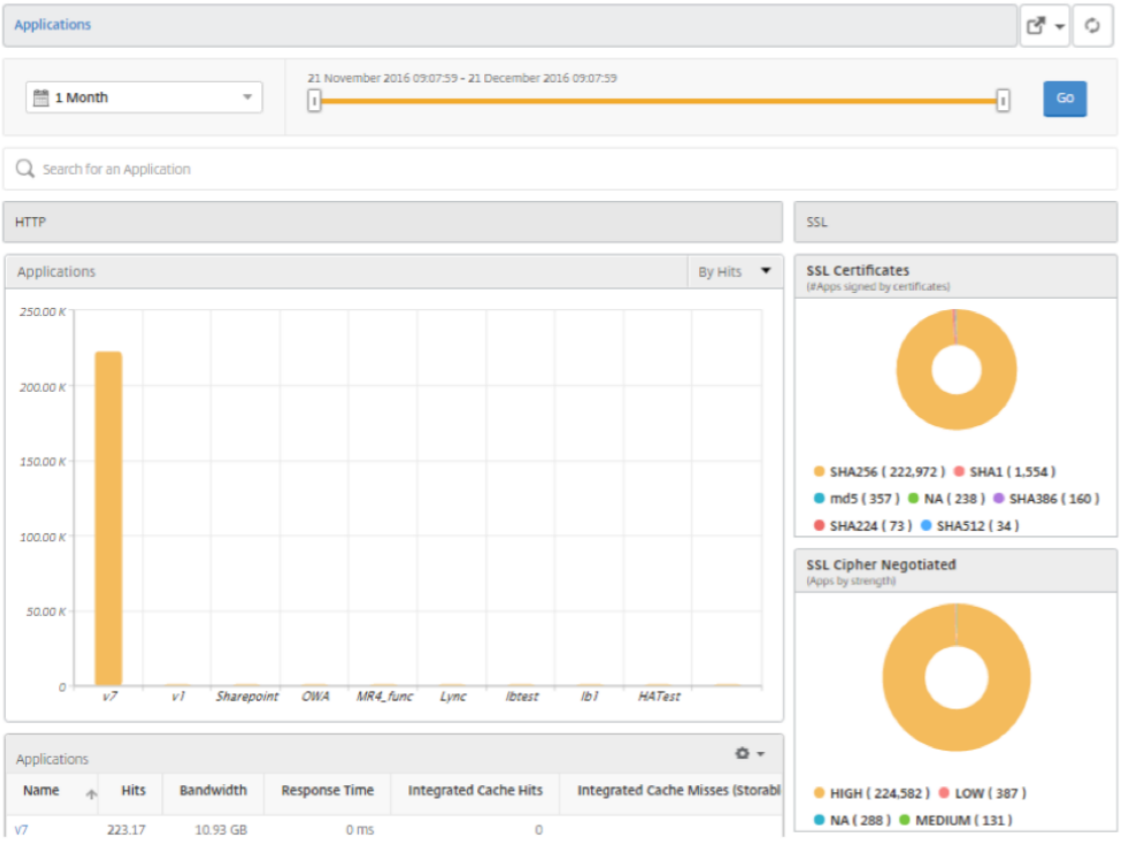
Las métricas SSL Insight de NetScaler ADM proporcionan una vista detallada del rendimiento de las transacciones SSL servidas por las instancias NetScaler ADC. Puede ver las métricas de SSL Insight a nivel de cliente, servidor o aplicación, y las métricas de las transacciones de éxito y error de SSL. Con la ayuda de estas métricas, puede analizar y optimizar la configuración de HTTPS y la configuración del certificado SSL de NetScaler ADC, y realizar un seguimiento de los problemas de rendimiento.

Para supervisar las métricas de SSL Insight en NetScaler ADM:

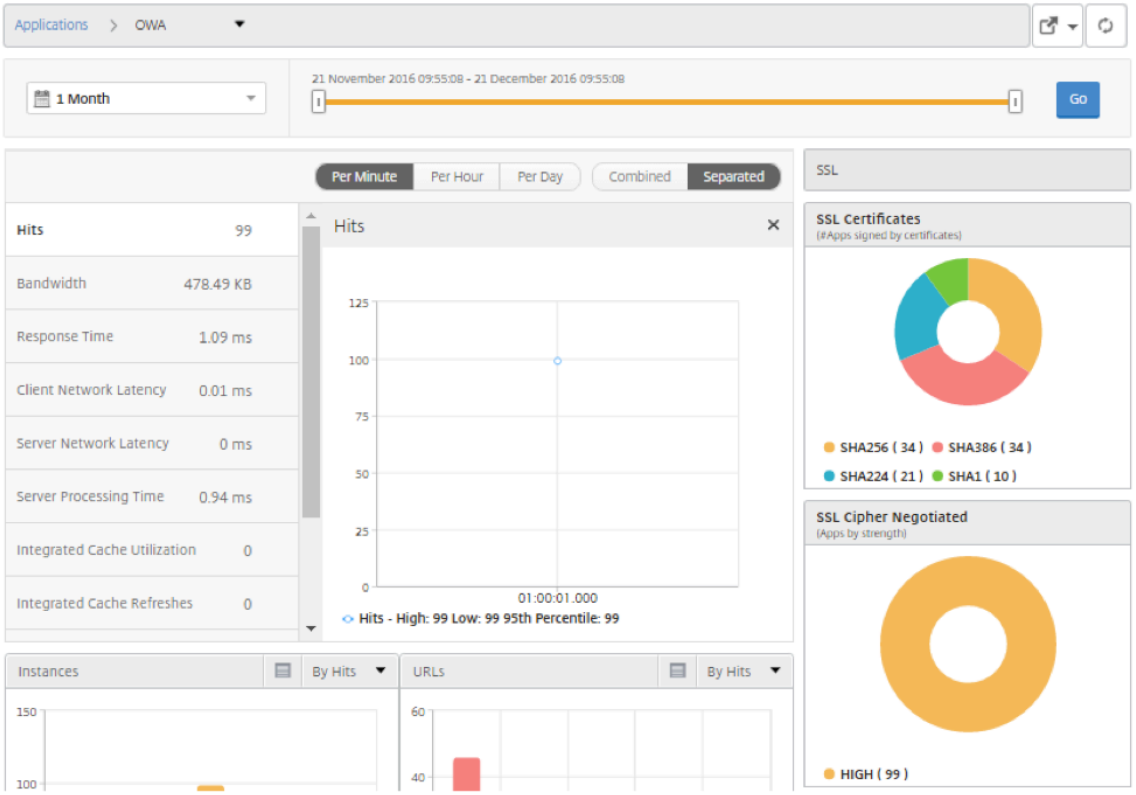
1. En la pestaña **Analytics**, vaya a Web Insight y haga clic en el nodo **Cliente**, **Servidor** o **Aplicación** para mostrar las métricas sobre los clientes, el servidor o las aplicaciones, respectivamente.

2. En el panel superior izquierdo, en la lista de períodos, selecciona el período de tiempo cuyas métricas quieres mostrar. Puede personalizar el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir**.
3. Las métricas de SSL Insight aparecen como gráficos circulares, en los que puede hacer clic para obtener más información.

> **Nota**
>
> Los gráficos circulares muestran las métricas de todas las aplicaciones, clientes o servidores.



4. Para mostrar los detalles de una aplicación, cliente o servidor específicos, haga clic en el valor correspondiente en el gráfico de barras.



5. Para ver las transacciones SSL fallidas, en la sección SSL, seleccione el botón de opción en la sección SSL.

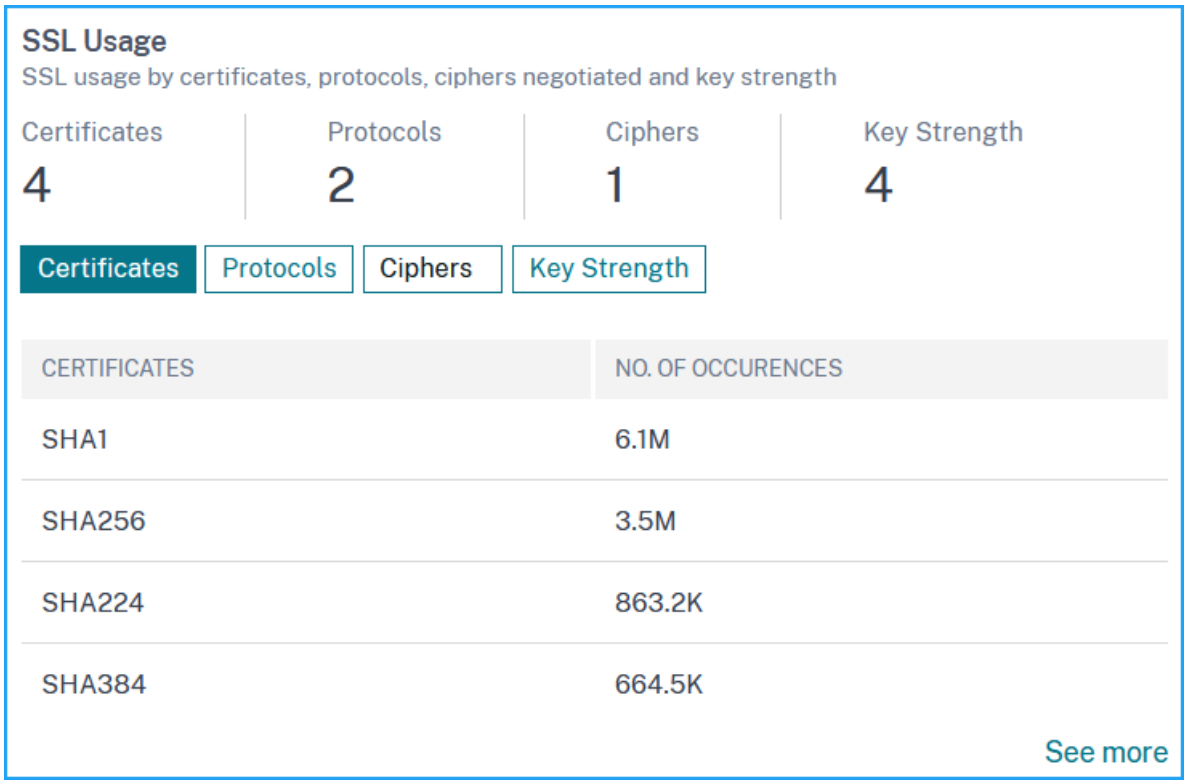
Caso de uso: obtenga una descripción general de las transacciones SSL de aplicaciones, clientes o servidores

El siguiente caso de uso describe cómo puede usar SSL Insight para evaluar el uso de varios parámetros de SSL en aplicaciones, clientes y servidores, y mejorar las medidas de seguridad.

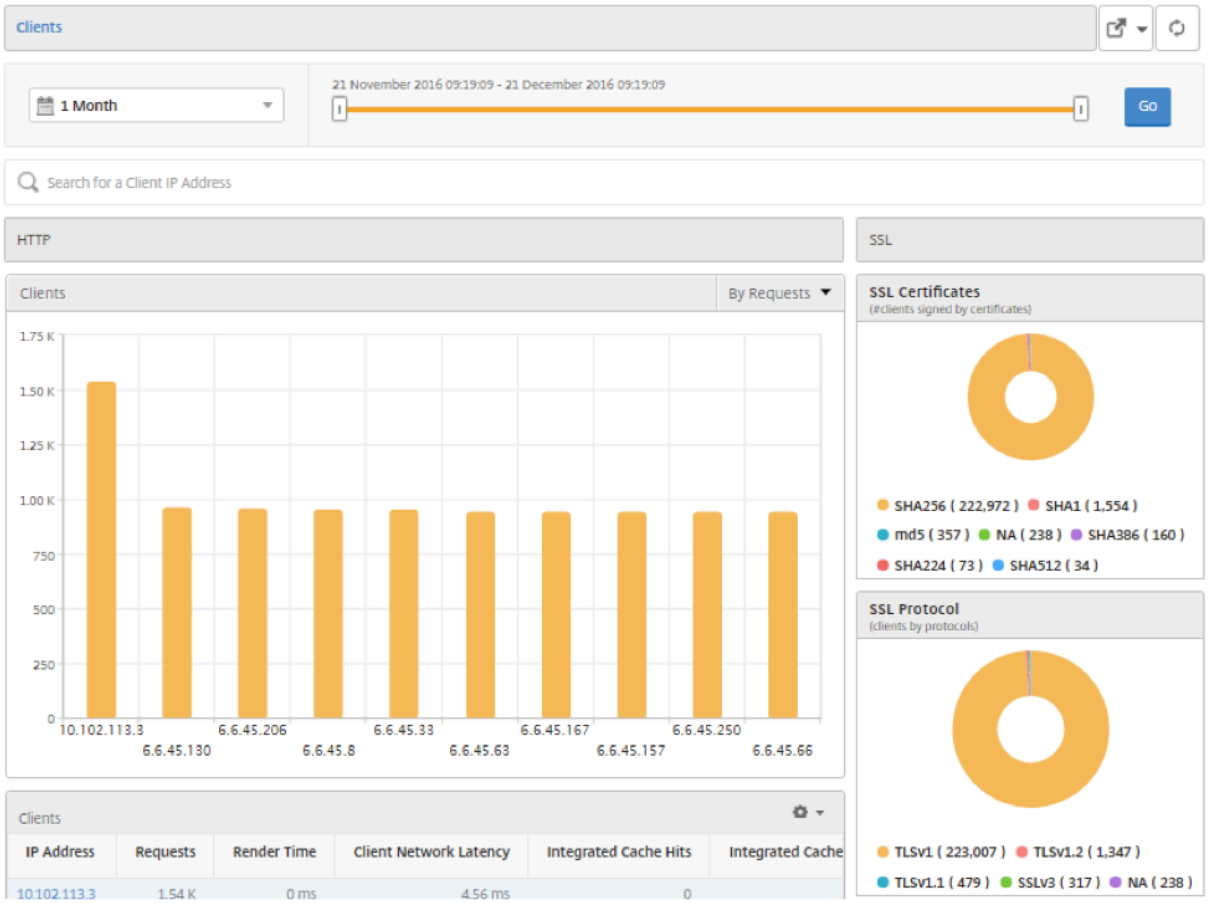
Tenga en cuenta que tiene un conjunto de aplicaciones que utilizan transacciones SSL (HTTPS) para la comunicación y que ha configurado NetScaler ADM para supervisar los componentes SSL. Es posible que tenga que revisar con frecuencia las aplicaciones para poder centrarse primero en las aplicaciones que necesitan más atención. El panel de información sobre SSL proporciona un resumen de los diversos parámetros SSL utilizados por las aplicaciones durante el período de tiempo que elija y para un dispositivo Citrix ADC seleccionado. Se trata de:

- Certificados SSL
- Protocolos SSL
- Cifrado SSL negociado
- Seguridad de la clave SSL

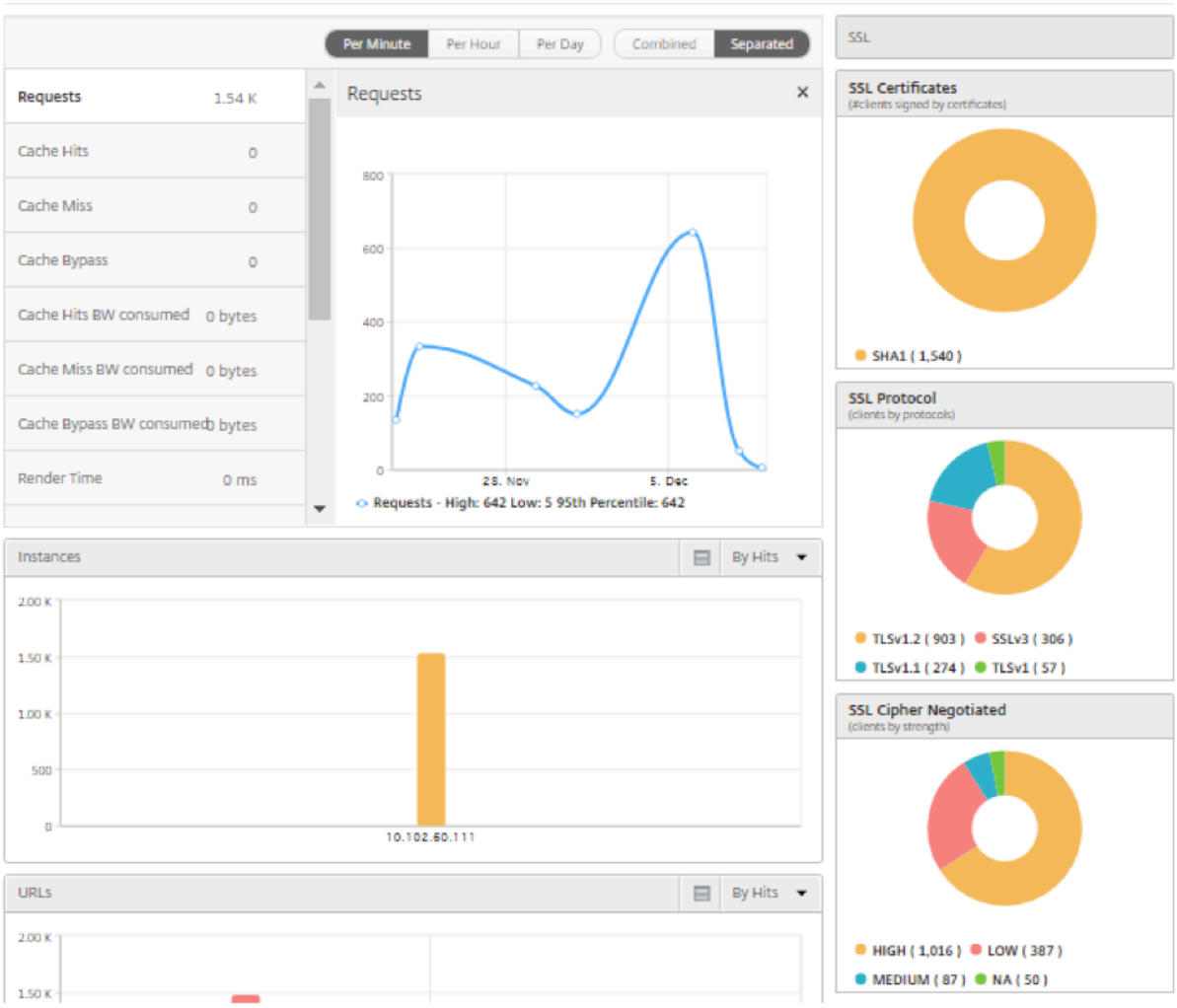
- Fallo de SSL —Frontend
- Fallo de SSL: backend



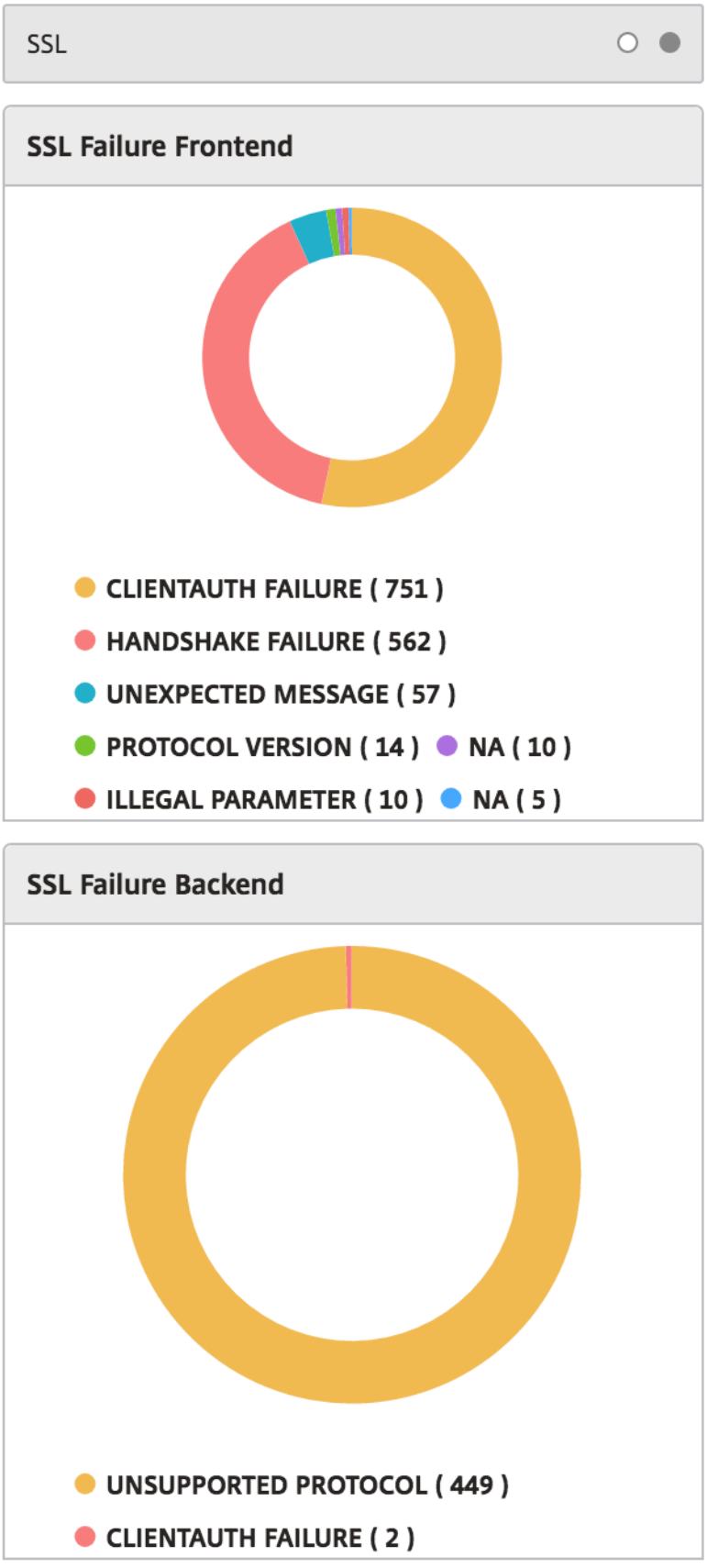
En el siguiente ejemplo, puede ver la lista de clientes (identificados por sus direcciones IP) y los hits SSL por cliente. Además, a la derecha, puede ver los parámetros SSL para todos los clientes.



Para mostrar los detalles SSL de un cliente, seleccione el cliente en el gráfico de barras o en la tabla debajo del gráfico. En el siguiente ejemplo, las transacciones del cliente seleccionado utilizan un certificado SSL SHA1 y cuatro protocolos principales: TSLv1.2, TSLv1.1, TSLv1 y SSLv3. También puede ver que se negociaron cifrados de varias fortalezas. El código de color indica la fuerza del protocolo SSL, que le proporciona información sobre los cifrados débiles y los cifrados fuertes.



Del mismo modo, para ver la información sobre las transacciones SSL fallidas, seleccione el botón de opción en la sección **SSL**. Los errores de front-end y back-end de SSL se muestran por separado en dos gráficos circulares. En el ejemplo siguiente, puede ver que los principales errores SSL de back-end son errores de protocolo de enlace y los principales errores SSL de front-end son parámetros ilegales.



Información TCP

January 30, 2024

La función TCP Insight de Citrix Application Delivery Management (ADM) proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias (o algoritmos) de control de la congestión que se utilizan en los dispositivos Citrix ADC para evitar la congestión de la red en la transmisión de datos. Esta función utiliza la función "Informe de velocidad de TCP", que mide el rendimiento de carga o descarga de archivos TCP con y sin optimización de TCP.

Puede ver las métricas clave de la capa de transporte, como el volumen de datos, el rendimiento y la velocidad, y utilizar esa información para medir el volumen de tráfico servido por las instancias de NetScaler ADC y validar los beneficios de la optimización de TCP. Para las métricas se proporcionan desgloses por dirección de transmisión (del cliente al Citrix ADC y del Citrix ADC al servidor de origen), el puerto TCP y la LAN virtual.

Requisitos previos

Antes de empezar a configurar la función TCP Insight, asegúrese de que se cumplen los siguientes requisitos previos:

- Las instancias de NetScaler ADC se ejecutan en la versión 11.1 del software, compilación 51.21 o posterior.
- Ha instalado NetScaler ADM en la versión 11.1 del software, compilación 51.21 o posterior.
- Todos los servidores virtuales configurados para una aplicación tienen licencia para administración y supervisión en NetScaler ADM.
  Para obtener información sobre las licencias de Citrix ADM, consulte Licencias.

Requisitos de hardware para Citrix ADM:

Componente	Requisito
RAM	8 GB
CPU virtual	4 **Nota**: Citrix recomienda usar 8 CPU para un mejor rendimiento.
Espacio de almacenamiento	120 GB

Componente	Requisito
	Nota: Citrix recomienda usar 500 GB para un mejor rendimiento.

Habilitación de TCP Insight

Antes de poder ver las métricas de TCP Insight, debe habilitar la función en NetScaler ADM.

Para habilitar TCP Insight:

1. Inicie sesión en Citrix ADM con las credenciales de administrador.
2. Vaya a **Analytics** > **Configuración** y haga clic en **Habilitar funciones para Analytics**.
3. En la página **Habilitar funciones para Analytics**, seleccione **Habilitar TCP Insight**.
4. En la ventana de confirmación, haga clic en **Aceptar**.

Visualización de las métricas de TCP Insight en Citrix ADM

Después de habilitar TCP Insight en NetScaler ADM, puede ver información clave de la capa de transporte, como el modo de tráfico (datos de Internet o móviles), el volumen de datos, el rendimiento, las interfaces, los puertos, la velocidad media de carga y la velocidad media de descarga.

Para mostrar métricas de TCP Insight en NetScaler ADM:

Vaya a **Analytics** > **TCP Insight** .

Puede colocar el puntero del mouse sobre los gráficos de barras para ver el volumen de datos de las técnicas de transporte correspondientes. También puede ver el volumen de datos y otras métricas en la tabla debajo del gráfico.

> **Nota**
>
> Puede personalizar las métricas que se muestran en el gráfico mediante el icono de configuración de la tabla. También puede seleccionar el período de tiempo al que pertenecen las métricas y utilizar el control deslizante de tiempo para ajustar el período de tiempo.

También puede ver las métricas de elementos como las interfaces, los puertos y las velocidades de bits seleccionándolos de la lista TCP Insight.

Casos de uso

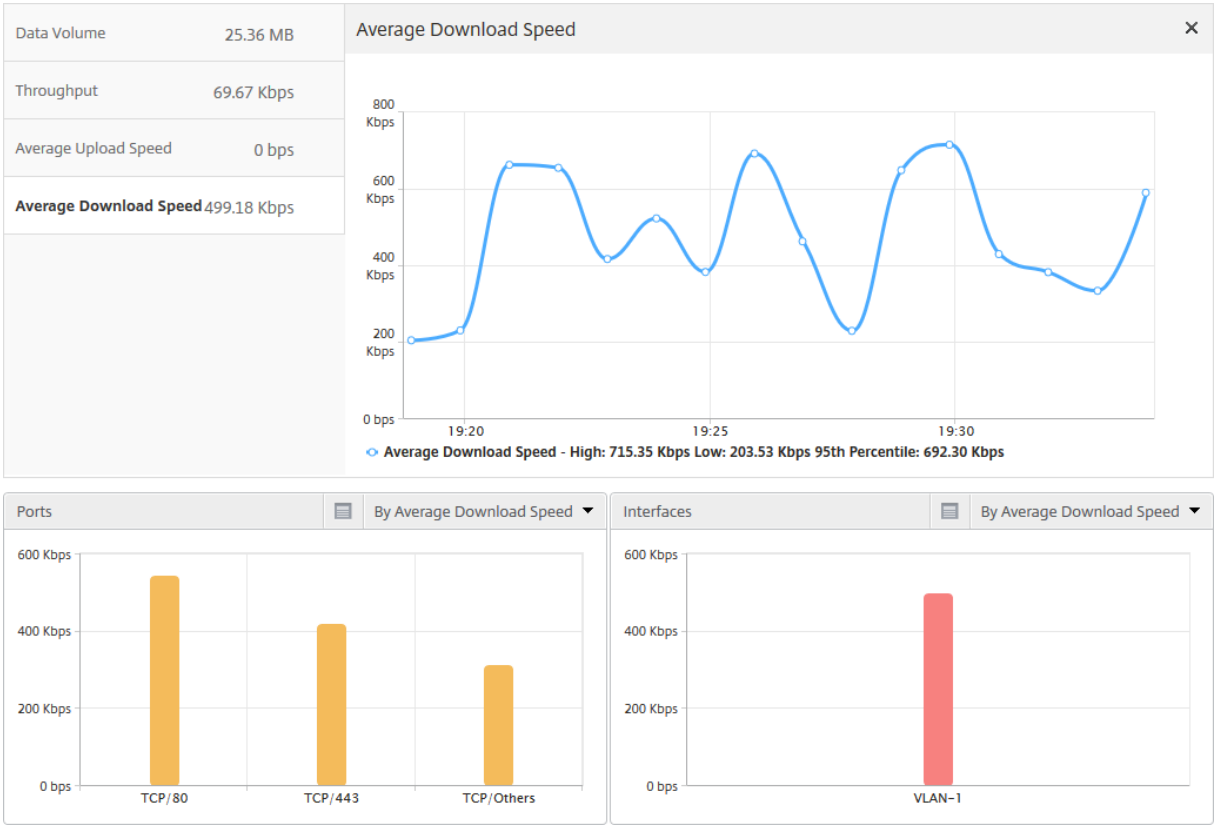
Los siguientes casos de uso ilustran algunas de las formas de usar TCP Insight en los dispositivos NetScaler ADC:

- Evalúe los beneficios de la optimización
- Ajustar parámetros TCP
- Medir el impacto de la optimización TCP en el volumen de tráfico

Evalúe los beneficios de la optimización

¿En qué medida beneficia realmente la optimización TCP de NetScaler ADC a una red móvil (radio) o empresarial (Internet)? Puede ver la velocidad de las transferencias de datos que se realizan a través de TCP y comparar el rendimiento optimizado y no optimizado. Estas mediciones se muestran por separado para las instrucciones de descarga y carga (siempre en el lado de la radio/cliente), y para diferentes puertos de destino, HTTP (80) y HTTPS (443).
Al examinar las métricas de TCP Insight, puede cuantificar la mejora de velocidad obtenida al optimizar los flujos de TCP.

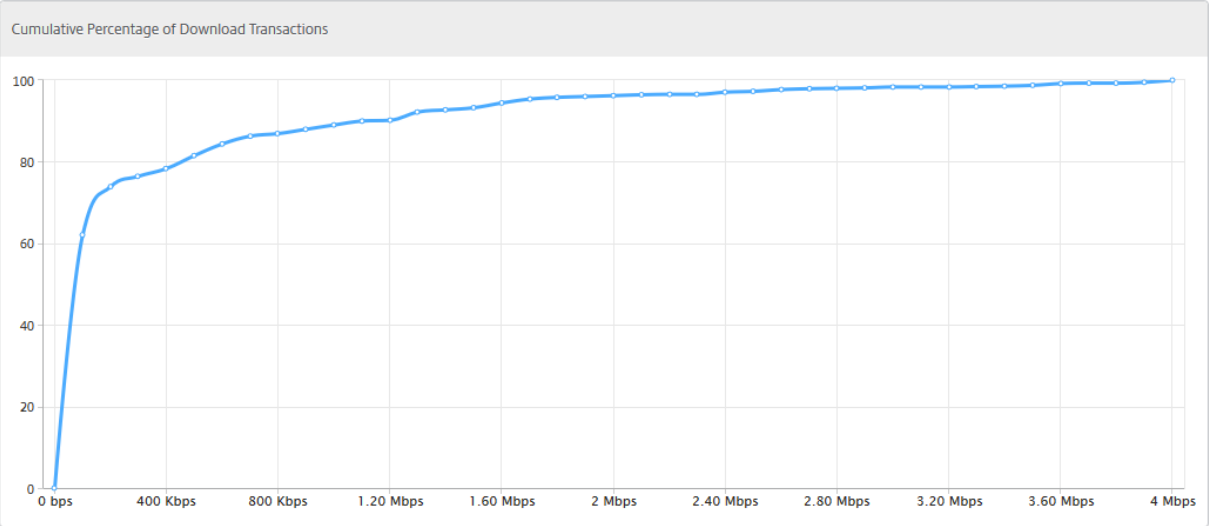
Para ver un resumen de estos parámetros, inicie sesión en NetScaler ADM y haga clic en la ficha **TCP Insight**. A continuación, haga clic en **Lados** y seleccione **Internet** o **Radio** en el gráfico de barras o en la tabla debajo del gráfico.



Ajustar parámetros TCP

El uso de diferentes perfiles TCP puede generar diferentes salidas para el mismo tráfico. En tales situaciones, es posible que quiera ver y comparar las mediciones de velocidad de los períodos en los que NetScaler ADC ejecuta diferentes perfiles de optimización de TCP. Puede utilizar los resultados para ajustar los parámetros de TCP para una transmisión más rápida y desarrollar un perfil TCP que maximice la experiencia percibida por el usuario en una red de cliente específica.

Para ver los informes, inicie sesión en NetScaler ADM. A continuación, en la ficha **TCP Insight**, haga clic en **Bitrates**y seleccione la velocidad de bits deseada en el gráfico de barras o en la tabla situada debajo del gráfico.

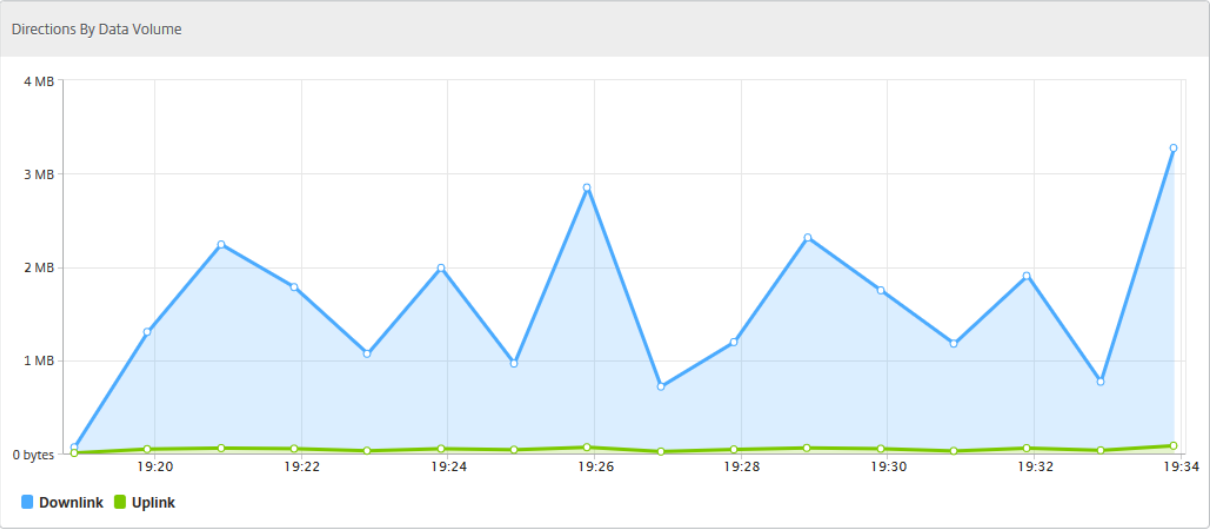


Medir el impacto de la optimización TCP en el volumen de tráfico

Las mediciones del volumen/rendimiento de datos de la capa IP gestionadas por una instancia de NetScaler ADC se pueden comparar entre diferentes períodos de tiempo para evaluar el efecto de la optimización de TCP en el consumo de datos de los suscriptores. Las mediciones se pueden aplicar por separado para cada lado de la red (lado de la radio frente al lado de Internet), para diferentes segmentos de tráfico (delineados por diferentes interfaces o VLAN), para cada dirección (enlace descendente o enlace ascendente) y para diferentes puertos de destino (HTTP y HTTPS). La comparación se puede utilizar para confirmar que la optimización de TCP alienta a los suscriptores a consumir más datos.

Para obtener un resumen de las mediciones, inicie sesión en NetScaler ADM y, en la ficha **TCP Insight**, haga clic en **Lados**y, a continuación, seleccione **Internet** o **Radio** en el gráfico de barras o en la tabla situada debajo del gráfico.

También puede seleccionar un período de tiempo diferente de la lista de tiempos. Puede personalizar el marco de tiempo mediante el control deslizante de marco de tiempo.

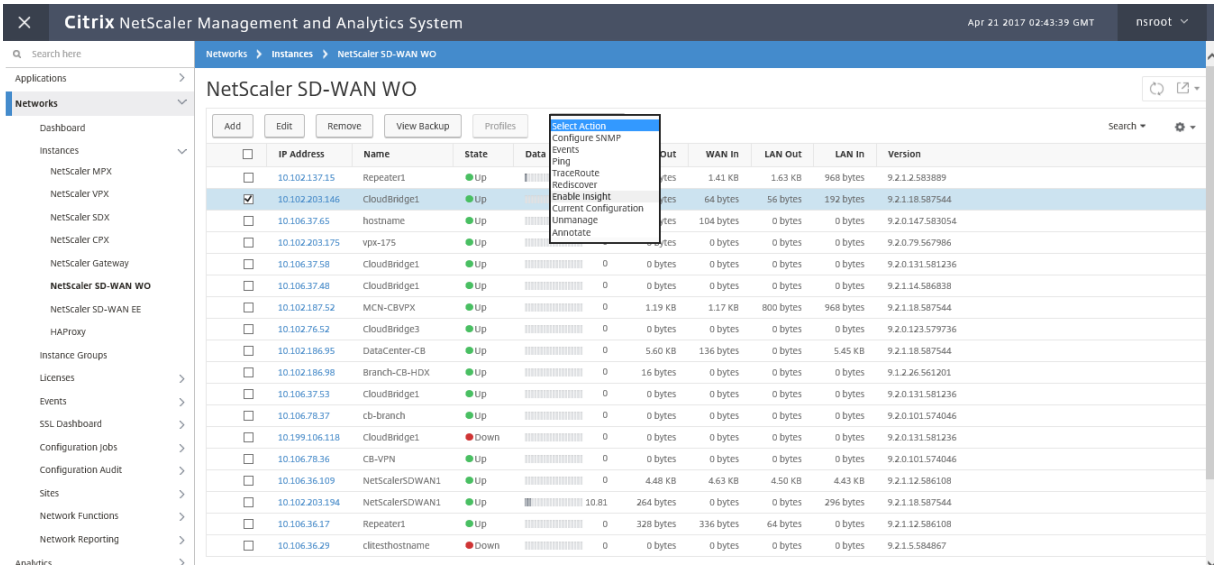


WAN Insight

January 30, 2024

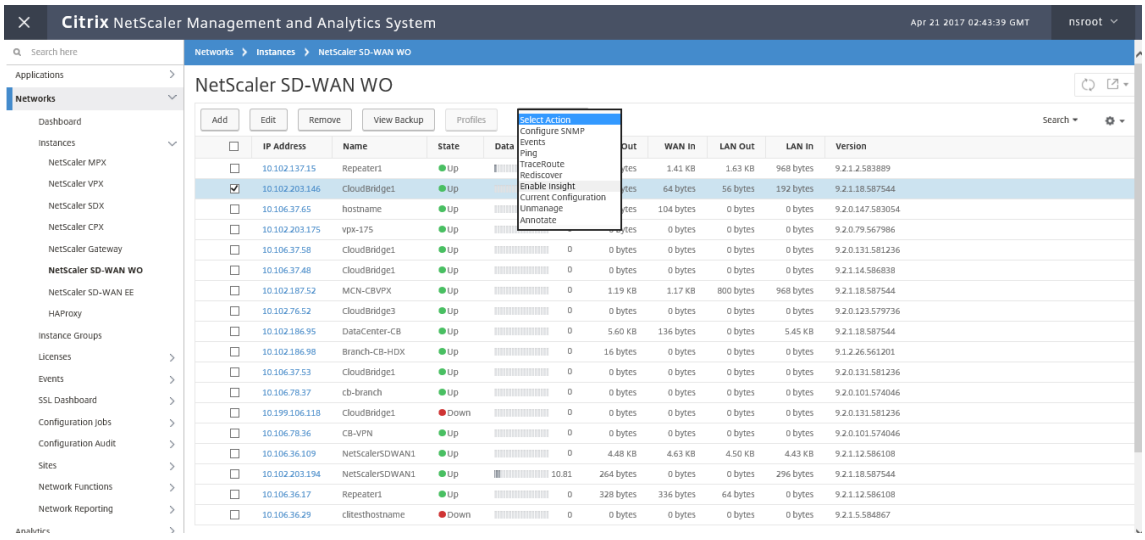
Los dispositivos de optimización WAN (WO) de Citrix SD-WAN optimizan la entrega de una gran cantidad de aplicaciones a través de la WAN, al mejorar la eficiencia del flujo de datos a través de la red entre el centro de datos y las sucursales. El análisis de WAN Insight permite a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre los dispositivos de optimización WAN del centro de datos y las sucursales. WAN Insight proporciona visibilidad a los clientes, aplicaciones y sucursales de la red, para ayudar a solucionar problemas de red de manera eficaz. Los informes en vivo e históricos le permiten abordar de forma proactiva los problemas, si los hay.

Al habilitar el análisis en el dispositivo de optimización WAN del centro de datos, NetScaler Application Delivery Management (ADM) puede recopilar datos y proporcionar informes y estadísticas para el centro de datos y los dispositivos de optimización WAN de sucursal.



Para habilitar el análisis en el dispositivo de optimización WAN:

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de administrador.
3. Vaya a **Redes**> **Instancias** > **Citrix SD-WAN** y seleccione la instancia de SD-WAN WO.

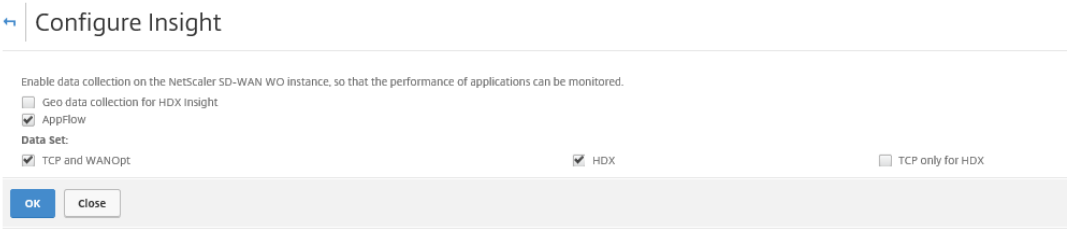


4. En el menú desplegable **Seleccionar acción** , seleccione **Configurar análisis** .
5. Seleccione los siguientes parámetros según sea necesario:

   - **Recopilación de datos geográficos para HDX Insight**: comparte la dirección IP del cliente con la API de Google Geo.

   - **AppFlow** : comienza a recopilar datos de las instancias de optimización de WAN.

- **TCP y WanOpt**: proporciona informes TCP y WanOpt Insight.
- **HDX**: Proporciona informes HDX Insight.
- **TCP solo para HDX**: Proporciona TCP solo para los informes HDX Insight.



6. Haga clic en **Aceptar**.

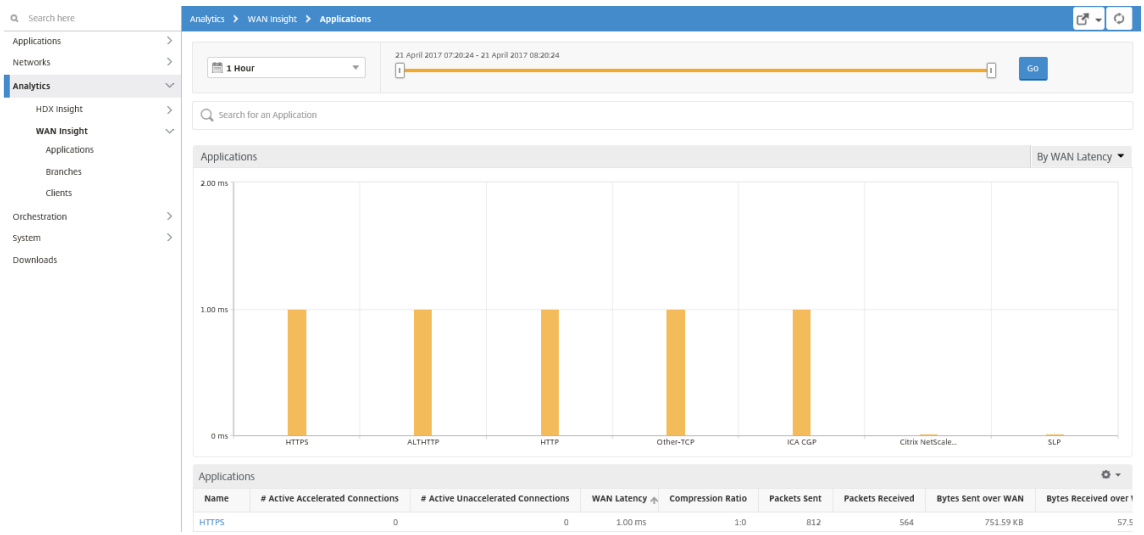
Para ver informes de WAN Insight:

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de administrador.
3. Vaya a **Analytics** > **WAN Insight**.

> **Nota**
>
> La opción WAN Insight solo está visible después de agregar una instancia WO de SD-WAN a NetScaler ADM.

Puede ver los siguientes informes:

- **Aplicaciones** : muestra las estadísticas de uso y rendimiento de todas las aplicaciones durante la duración seleccionada.
- **Sucursales**: Muestra las estadísticas de uso y rendimiento de todos los dispositivos de sucursal de optimización WAN.
- **Clientes**: Muestra las estadísticas de uso y rendimiento de todos los clientes que acceden a los dispositivos de optimización WAN, en cada rama.



Se muestran las siguientes métricas:

Métrica	Descripción
Conexiones rápidas activas	Número de conexiones WAN activas que se aceleran.
Conexiones no aceleradas activas	Número de conexiones WAN activas que no están aceleradas.
Latencia de WAN	Retraso, en milisegundos, que experimenta el usuario al interactuar con una aplicación.
Índice de compresión	Proporción de compresión de datos entre la sucursal y los dispositivos del centro de datos durante la duración seleccionada.
Paquetes enviados	Número de paquetes que el dispositivo de optimización de WAN ha enviado a través de la red durante el tiempo seleccionado.
Paquetes recibidos	Número de paquetes que el dispositivo de optimización de WAN ha recibido de la red durante el tiempo seleccionado.
Bytes enviados a través de WAN	Número de bytes que el dispositivo de optimización de WAN de Citrix ha enviado a través de la WAN durante el tiempo seleccionado.
Bytes recibidos a través de WAN	Número de bytes que el dispositivo de optimización de WAN recibió de la WAN durante el tiempo seleccionado.

Métrica	Descripción
RTO LAN	Número de veces que el dispositivo de optimización de WAN ha agotado el tiempo de espera de la retransmisión a la LAN durante el tiempo seleccionado.
RTO WAN	Número de veces que el dispositivo de optimización de WAN ha agotado el tiempo de espera de la retransmisión a la WAN durante el tiempo seleccionado.
Paquetes de retransmisión (LAN)	Número de paquetes que el dispositivo de optimización de WAN ha retransmitido a la red LAN durante el tiempo seleccionado.
Paquetes de retransmisión (WAN)	Número de paquetes que el dispositivo de optimización de WAN ha retransmitido a la red WAN durante el tiempo seleccionado.

Video Insight

January 30, 2024

La función Video Insight proporciona una solución fácil y escalable para monitorear las métricas de las técnicas de optimización de vídeo utilizadas por los dispositivos NetScaler ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa, y ofrece beneficios como:

- Administre la red durante la congestión en las horas pico.
- Mejore la coherencia de la reproducción de vídeo y reduzca el bloqueo de vídeo
- Habilite nuevas ofertas de servicios de video (por ejemplo, los servicios de video Binge-on).
- Permita que los clientes seleccionen la mejor calidad de vídeo sostenible.
- Ofrezca una experiencia de usuario coherente para el suscriptor.

Mientras optimiza el tráfico de vídeo, el dispositivo NetScaler ADC utiliza un mecanismo especial para acelerar dinámicamente la velocidad de bits de vídeo y una técnica de muestreo aleatorio para estimar los ahorros derivados de la técnica de optimización. Para obtener más información sobre la función de optimización de vídeo de NetScaler ADC, consulte Optimización de vídeo.Cuando integra NetScaler ADC appliance con NetScaler Application Delivery Management (ADM), recopila información clave de los datos de vídeo que fluyen a través del dispositivo NetScaler ADC. Puede utilizar esta

información para comparar el rendimiento optimizado y no optimizado del tráfico de vídeo ABR, determinar el ahorro debido a la optimización, etc.

> **Nota**
>
> Las estadísticas de las sesiones no optimizadas proporcionadas en NetScaler ADM corresponden a las sesiones seleccionadas de muestreo aleatorio en NetScaler ADC Appliance. Para obtener más información sobre el muestreo aleatorio, consulteOptimización de vídeo.

Video Insight en NetScaler ADM proporciona métricas para los siguientes tipos de tráfico de vídeo:

- Descarga progresiva (PD) de vídeos a través de HTTP
- Vídeos de ABR a través de HTTP
- Vídeos de ABR a través de HTTPS
- Vídeos ABR de YouTube a través de QUIC

Configuración de Video Insight

> **Nota**
>
> Video Insight es compatible con las instancias de NetScaler ADC con licencia NetScaler ADC Premium. La licencia NetScaler ADC Premium es compatible con las plataformas NetScaler ADC Telco (VPX T1000 y VPX-T).

Para configurar Video Insight en una instancia de Citrix ADC, primero habilite la función AppFlow, configure un recopilador, una acción y una directiva de AppFlow y vincule la directiva de forma global. Al configurar el recopilador, debe especificar la dirección IP del servidor Citrix ADM en el que desea supervisar los informes.

Para configurar la información de vídeo en una instancia de NetScaler ADC, ejecute los siguientes comandos para configurar un perfil y una directiva de AppFlow y enlazar la directiva de AppFlow globalmente.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -**videoInsight** ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode ulfd

habilitar el flujo de aplicacionesde funciones

Sample

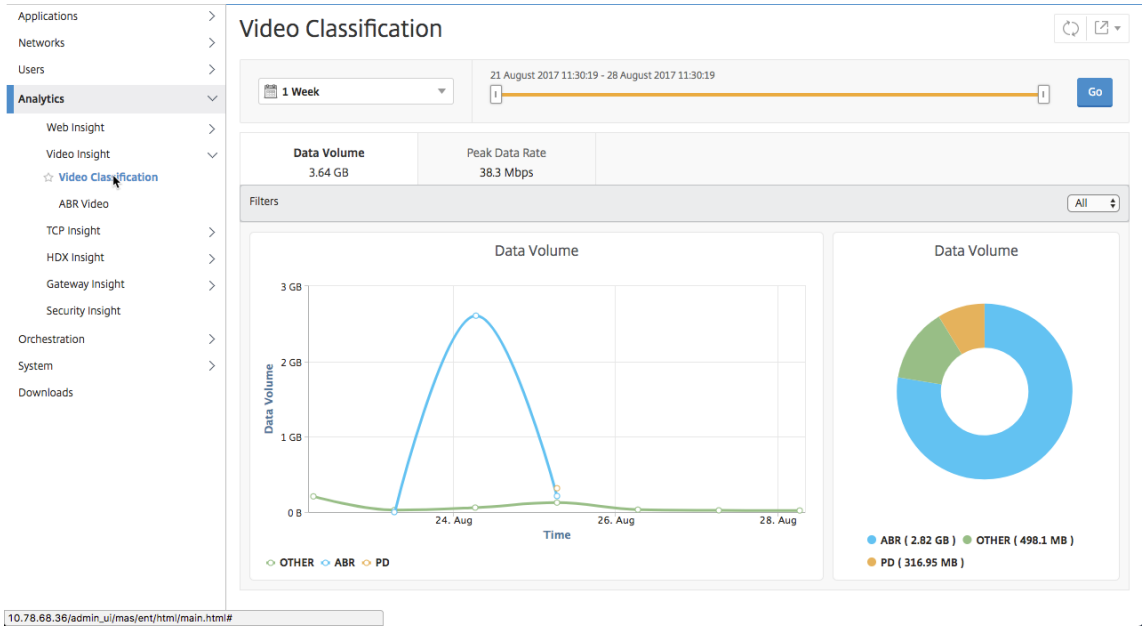
```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Ver las métricas de Video Insight en NetScaler ADM

Después de habilitar Video Insight en NetScaler ADM, puede ver métricas de optimización de vídeo, como clasificación de vídeo, volumen de datos, velocidad máxima de datos y reproducciones de vídeo ABR. Estas métricas le ayudan a analizar su red y optimizar los vídeos para mejorar la experiencia del suscriptor, la eficiencia operativa y otros criterios de rendimiento.

Para ver las métricas de Video Insight en Citrix ADM:

1. En un explorador web, escriba la dirección IP del dispositivo virtual NetScaler ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Analytics > Video Insight**.



> **Nota**
>
> Los valores proporcionados por la leyenda **OTHER** en los gráficos representan los datos no ABR y no PD en el tráfico de vídeo en función del filtro que haya seleccionado:
>
> - **All**: Suma de datos no ABR (HTTP, HTTPS y QUIC) y no PD (HTTP) en el tráfico de vídeo.
> - **HTTP**: Suma de los datos que no son ABR y que no son PD en el tráfico de vídeo.
> - **HTTPS**: Suma de los datos de vídeo que no son ABR en el tráfico de vídeo.
> - **QUIC**: Suma de los datos de vídeo que no son ABR en el tráfico de vídeo.

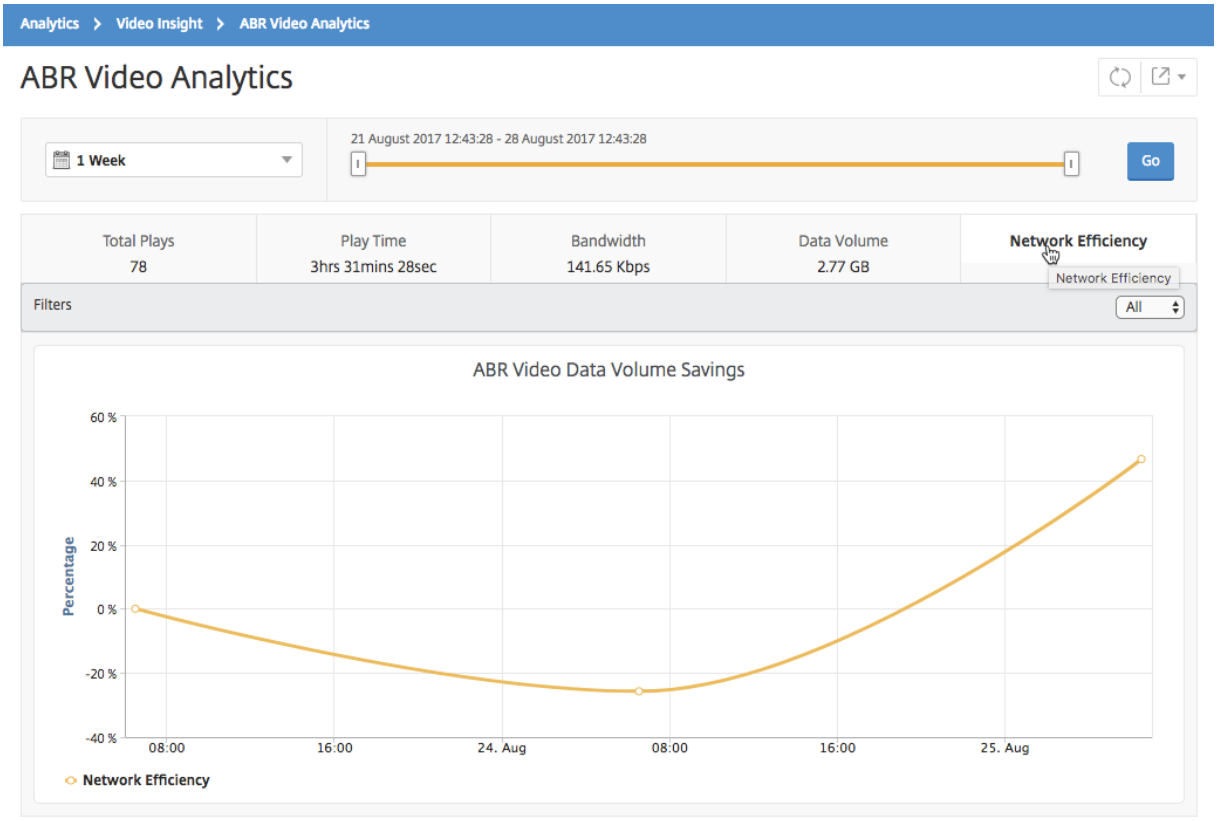
Ver la eficiencia de la red

January 30, 2024

Para un período determinado, Citrix Application Delivery Management (ADM) proporciona un gráfico que muestra la proporción de sesiones de vídeo optimizadas y no optimizadas en ese período. También muestra el porcentaje de ancho de banda ahorrado por la optimización. El porcentaje de ancho de banda ahorrado se calcula con la siguiente fórmula:

Porcentaje de ancho de banda ahorrado = Volumen de **datos de vídeo ABR optimizado promedio/Volumen de datos de vídeo ABR no optimizado**.

Para ver el porcentaje de ancho de banda que se ahorra mediante la optimización, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **ABR Video**. Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir** y seleccione la ficha **Eficiencia de la red**.



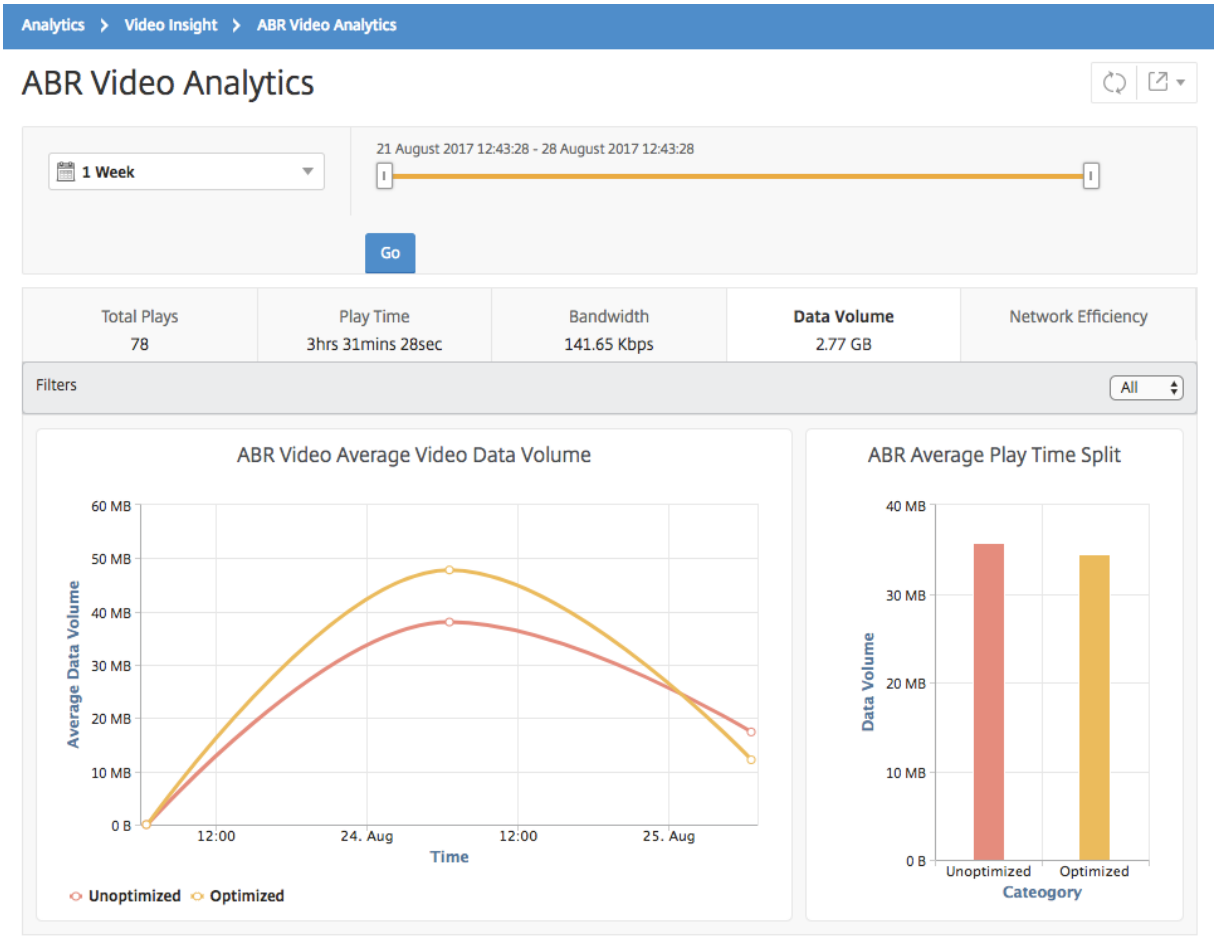
Compare el volumen de datos utilizado por los videos ABR optimizados y no optimizados

January 30, 2024

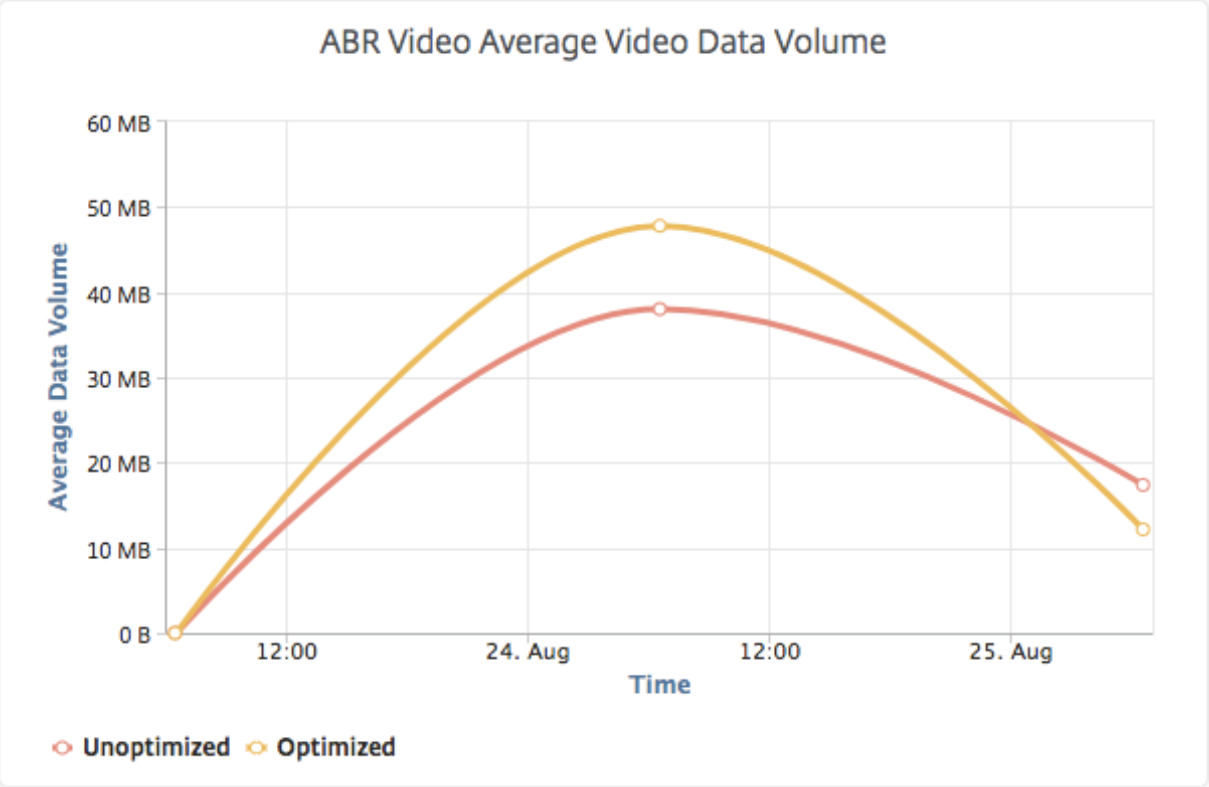
Durante un período determinado, Citrix Application Delivery Management (ADM) muestra el volumen de datos utilizado por los vídeos de ABR optimizados y no optimizados, para que pueda comparar los dos volúmenes.

Para ver el volumen de datos que utilizan los vídeos de ABR, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **ABR Video** . Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir** y seleccione la ficha **Volumen de datos**.

Puedes usar la lista desplegable **Filtros** para seleccionar los vídeos ABR de HTTP, HTTPS o QUIC.



La ficha **Volumen de datos** proporciona un gráfico de líneas y un gráfico circular que describe el volumen de datos promedio utilizado por los vídeos ABR y el volumen de datos consumido por los vídeos ABR optimizados y no optimizados de la red para el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver el volumen de datos promedio utilizado durante un período de tiempo determinado:



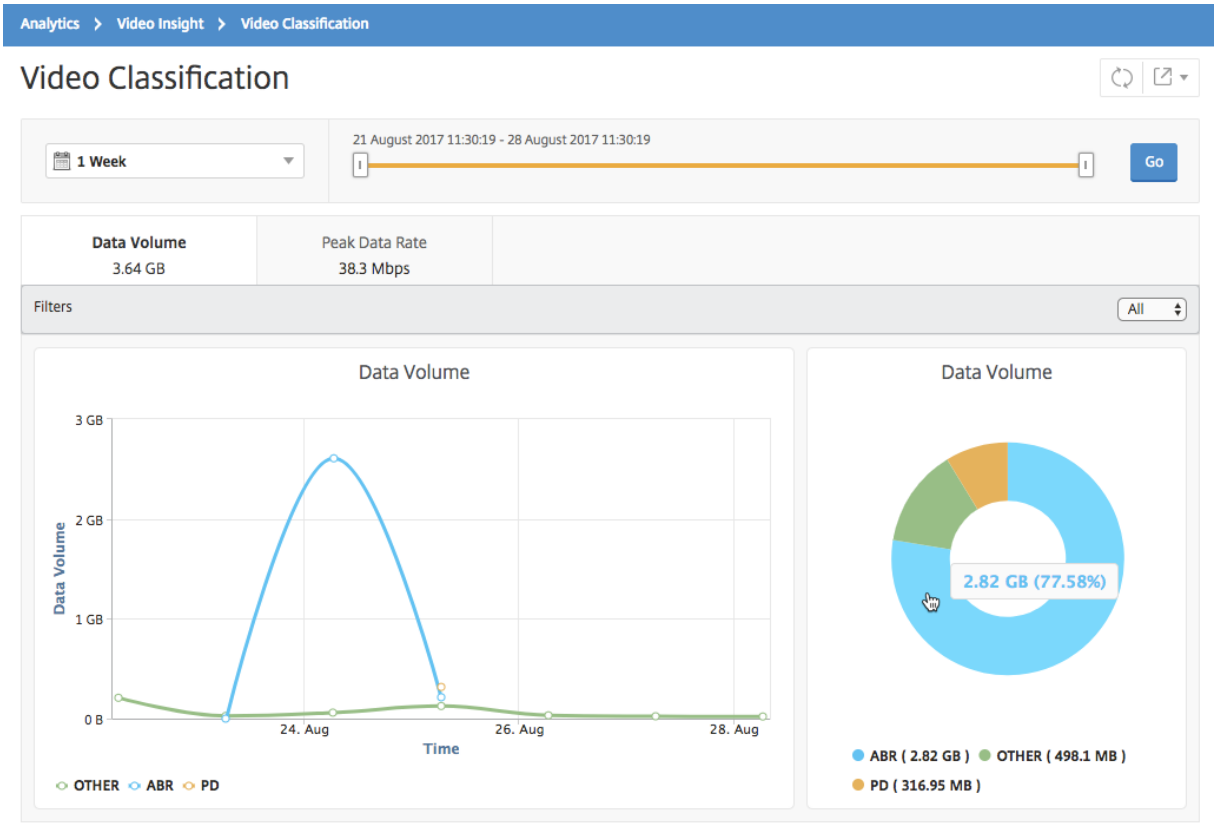
Ver el tipo de vídeos transmitidos y el volumen de datos consumido de la red

January 30, 2024

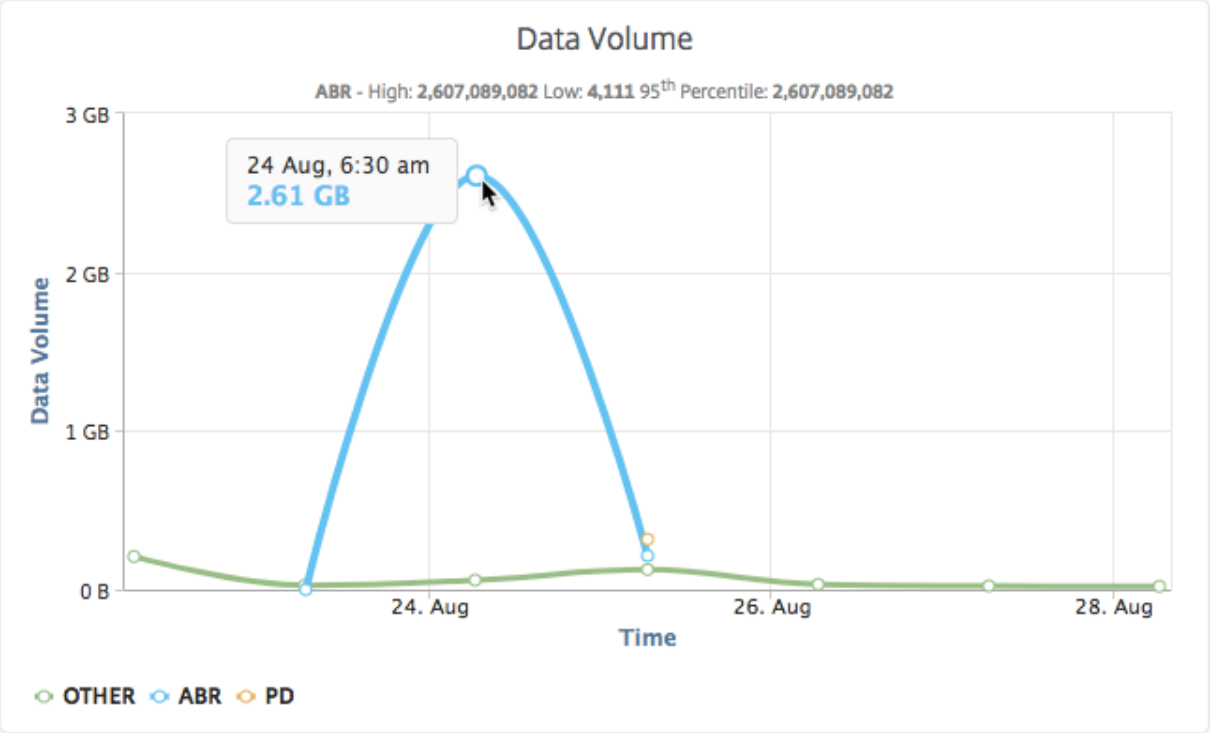
El dispositivo NetScaler ADC detecta el tráfico de vídeo cifrado o no cifrado de la red y el tipo de transmisión de vídeo (PD o ABR). NetScaler Application Delivery Management (ADM) muestra estas métricas y el volumen de datos consumido por el tráfico de vídeo durante un período de tiempo definido.

Para ver los tipos de vídeos y el volumen de datos consumido, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **Clasificación** de vídeos . Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir**.

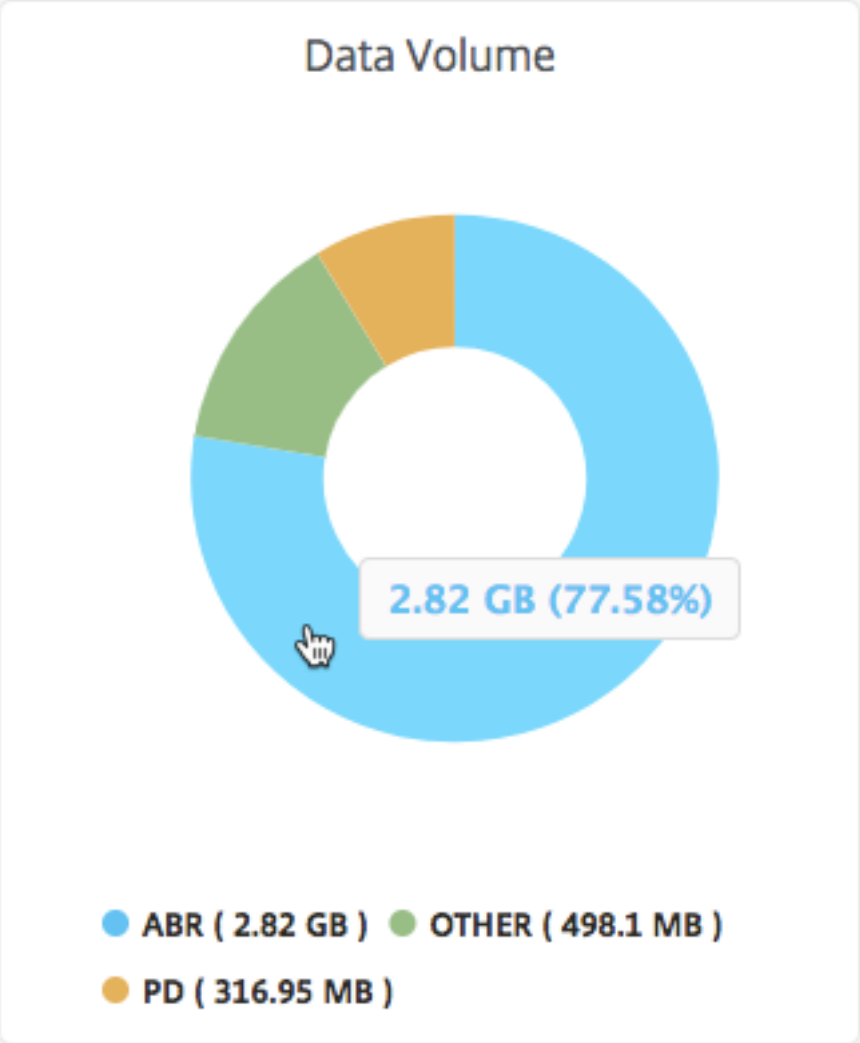
Puede usar la lista desplegable **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.



La ficha **Volumen de datos** proporciona un gráfico de líneas y un gráfico circular que muestra los tipos de transmisión de tráfico de vídeo desde la red y el volumen de datos consumido por la red. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver los datos consumidos durante un período de tiempo determinado:



Además, puede colocar el puntero del mouse sobre el gráfico circular para ver el porcentaje de volumen de datos consumido por un tipo determinado de tráfico de vídeo.



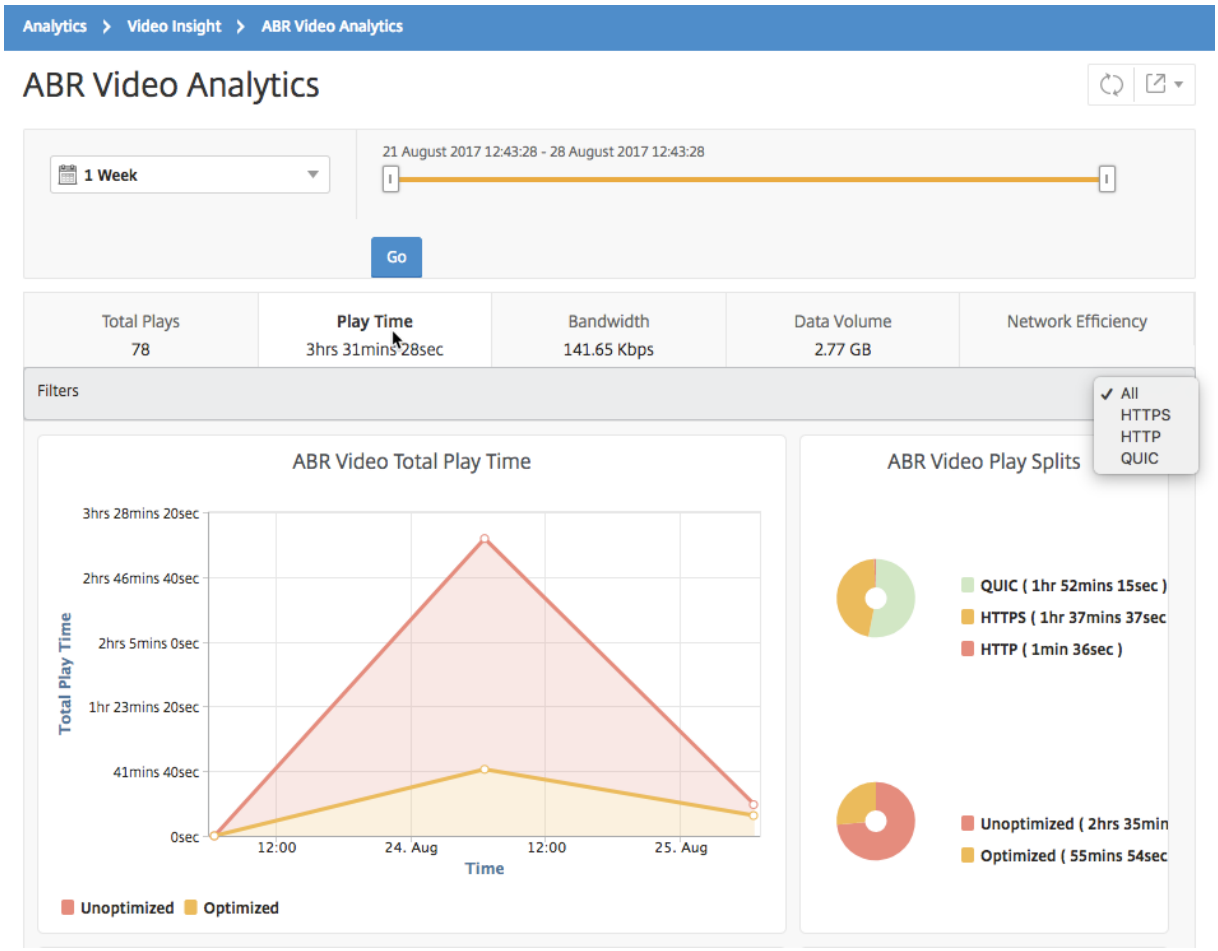
Compare el tiempo de reproducción optimizado y no optimizado de los vídeos ABR

January 30, 2024

Durante un período determinado, Citrix Application Delivery Management (ADM) proporciona el tiempo de reproducción de los vídeos ABR y también le permite comparar el tiempo de reproducción de los vídeos ABR optimizados y no optimizados de la red.

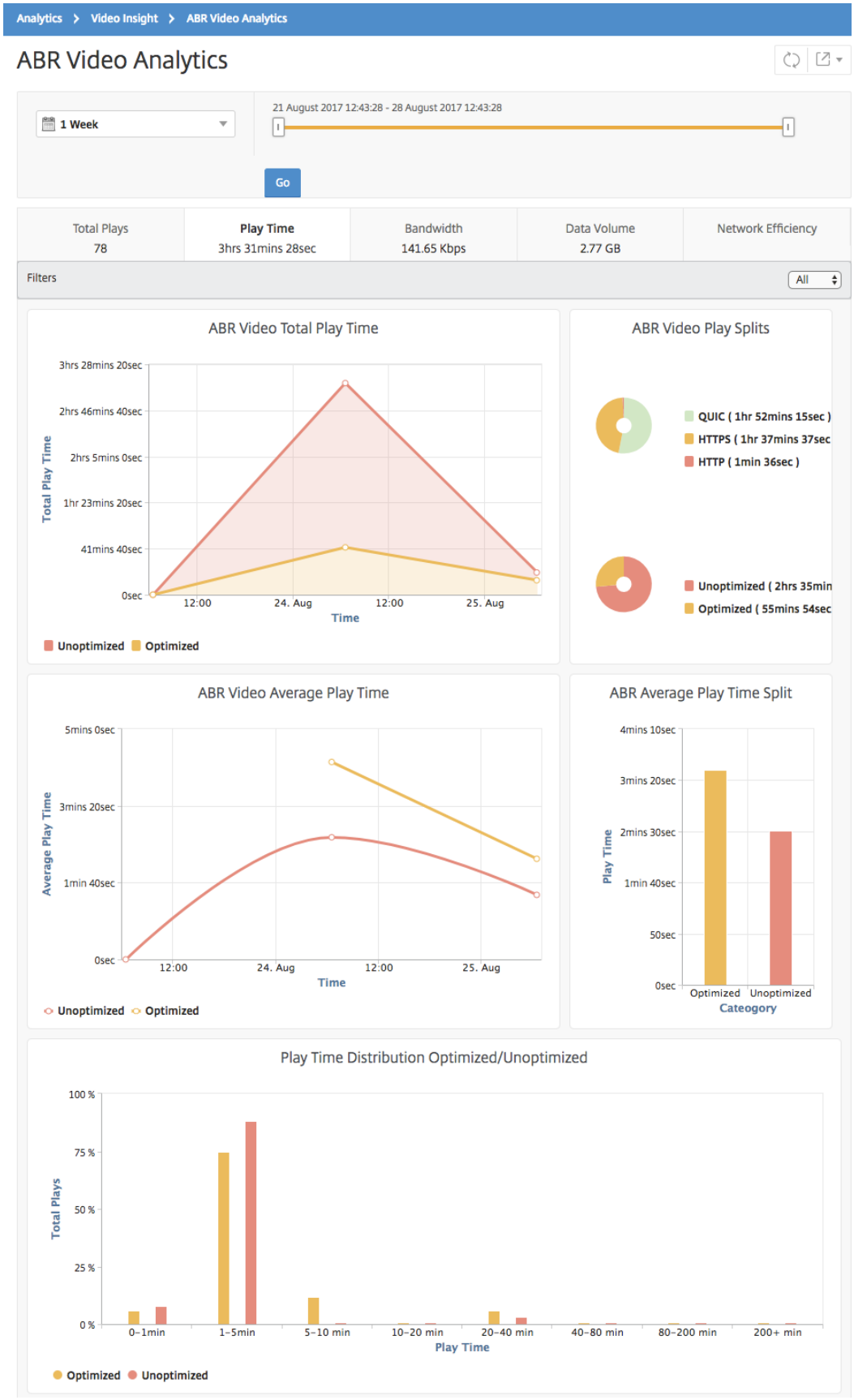
Para ver el tiempo de reproducción, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **ABR Video**. Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir** y seleccione la ficha **Tiempo de reproducción**.

Puedes usar la lista desplegable **Filtros** para seleccionar los vídeos ABR de HTTP, HTTPS o QUIC.



Para el marco de tiempo seleccionado, la ficha **Tiempo de reproducción** proporciona un gráfico de líneas y un gráfico circular que describe:

- Tiempo total de reproducción de los vídeos ABR de su red
- Tiempo total de reproducción de las reproducciones optimizadas y no optimizadas de vídeos ABR de su red durante el período de tiempo seleccionado.
- Tiempo total de reproducción de vídeos ABR cifrados y no cifrados.
- Tiempo medio de reproducción de los vídeos ABR
- Tiempo de reproducción promedio de reproducciones optimizadas y no optimizadas de vídeos ABR
- Tiempo medio de reproducción de vídeos ABR cifrados y no cifrados
- Distribución del tiempo de reproducción entre vídeos ABR optimizados y no optimizados



Compare el consumo de ancho de banda de vídeos ABR optimizados y no optimizados

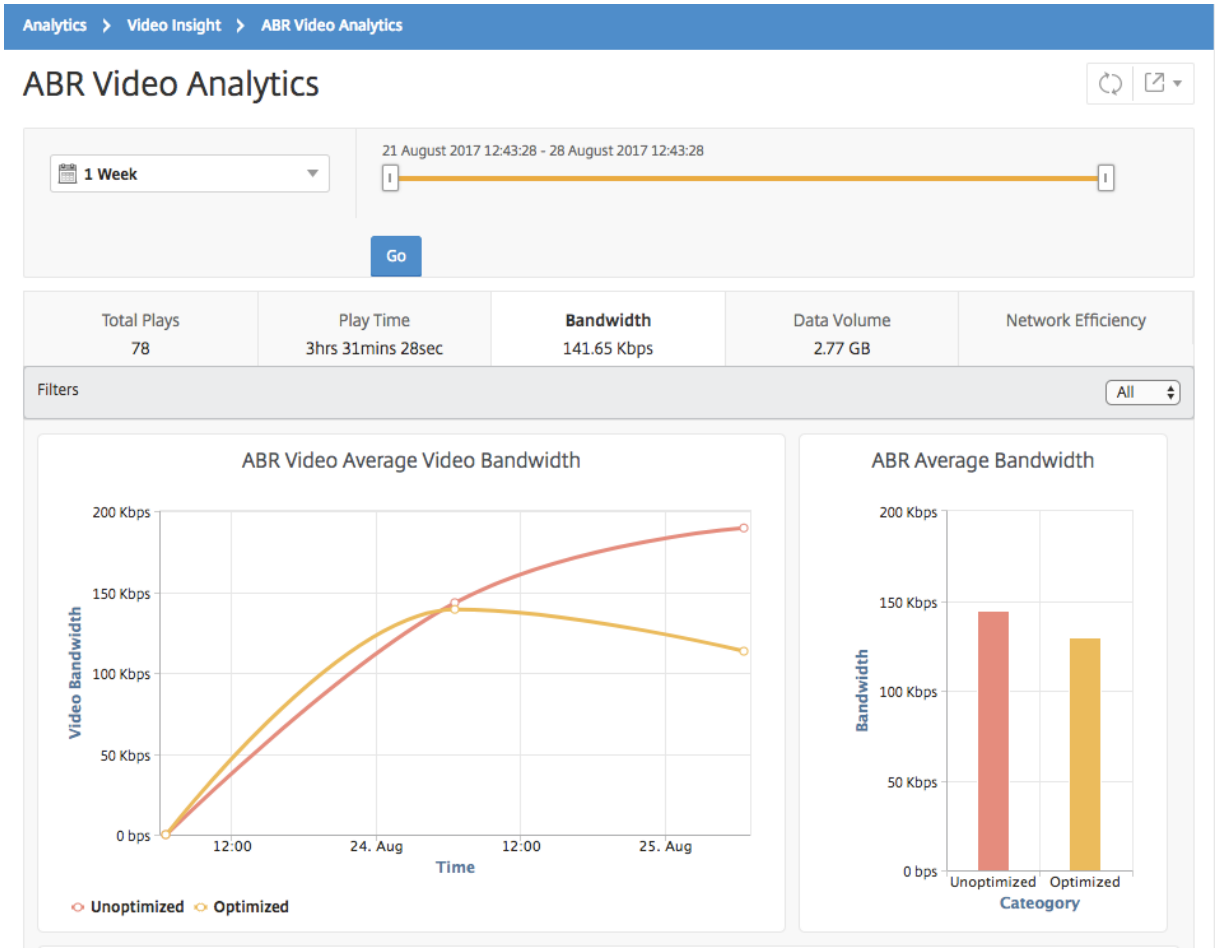
January 30, 2024

Durante un período determinado, Citrix Application Delivery Management (ADM) proporciona el ancho de banda que consumen los vídeos ABR optimizados y no optimizados y también le permite comparar el ancho de banda que consumen los vídeos ABR optimizados y no optimizados de la red en función de:

- Tiempo de reproducción
- Volumen de datos

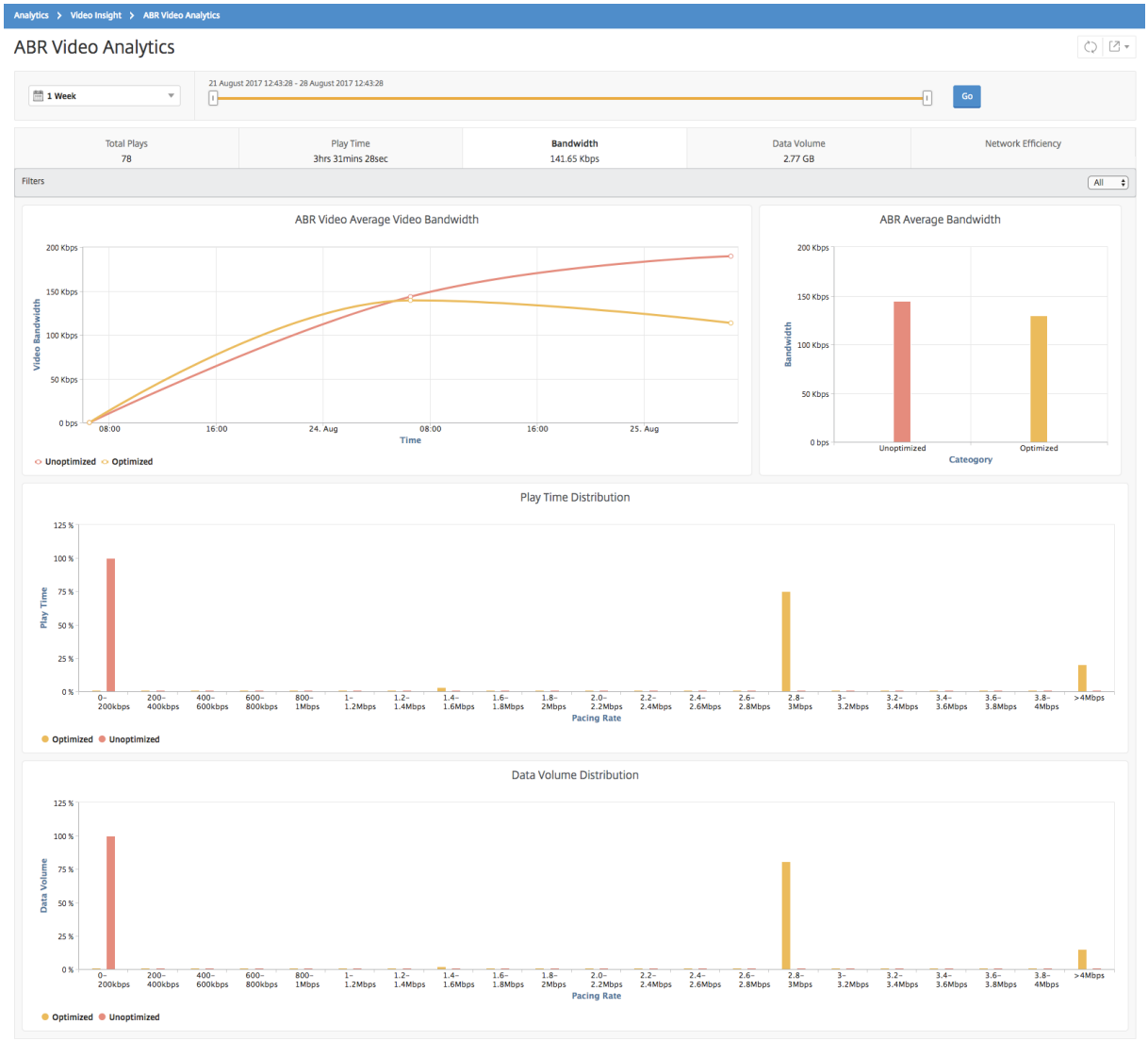
Para ver el consumo de ancho de banda, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **ABR Video Analytics**. Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir** y seleccione la ficha **Ancho de banda**.

Puedes usar la lista desplegable **Filtros** para seleccionar los vídeos ABR de HTTP, HTTPS o QUIC .



Para el período de tiempo seleccionado, la ficha Ancho de banda proporciona un gráfico de líneas y un gráfico circular que describe:

- Ancho de banda promedio consumido por los vídeos ABR optimizados y no optimizados.
- El ancho de banda consumido depende de la distribución del tiempo de reproducción entre vídeos ABR optimizados y no optimizados.
- Ancho de banda consumido en función del volumen de datos distribuido entre los vídeos ABR optimizados y no optimizados.



Compare el número optimizado y no optimizado de reproducciones de videos ABR

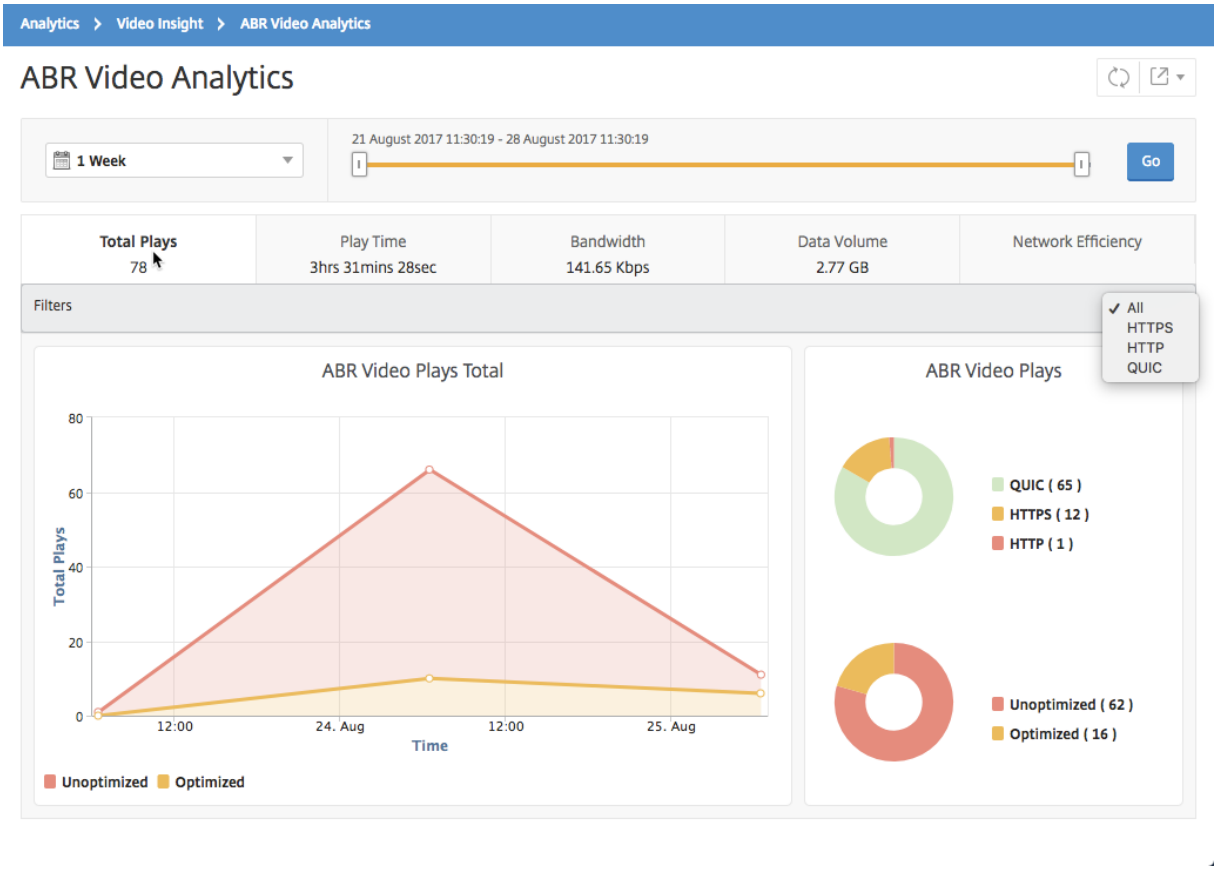
January 30, 2024

Para un período de tiempo determinado, NetScaler Application Delivery Management (ADM) muestra el número de reproducciones de vídeos ABR y permite comparar el número de reproducciones optimizadas y no optimizadas de la red.

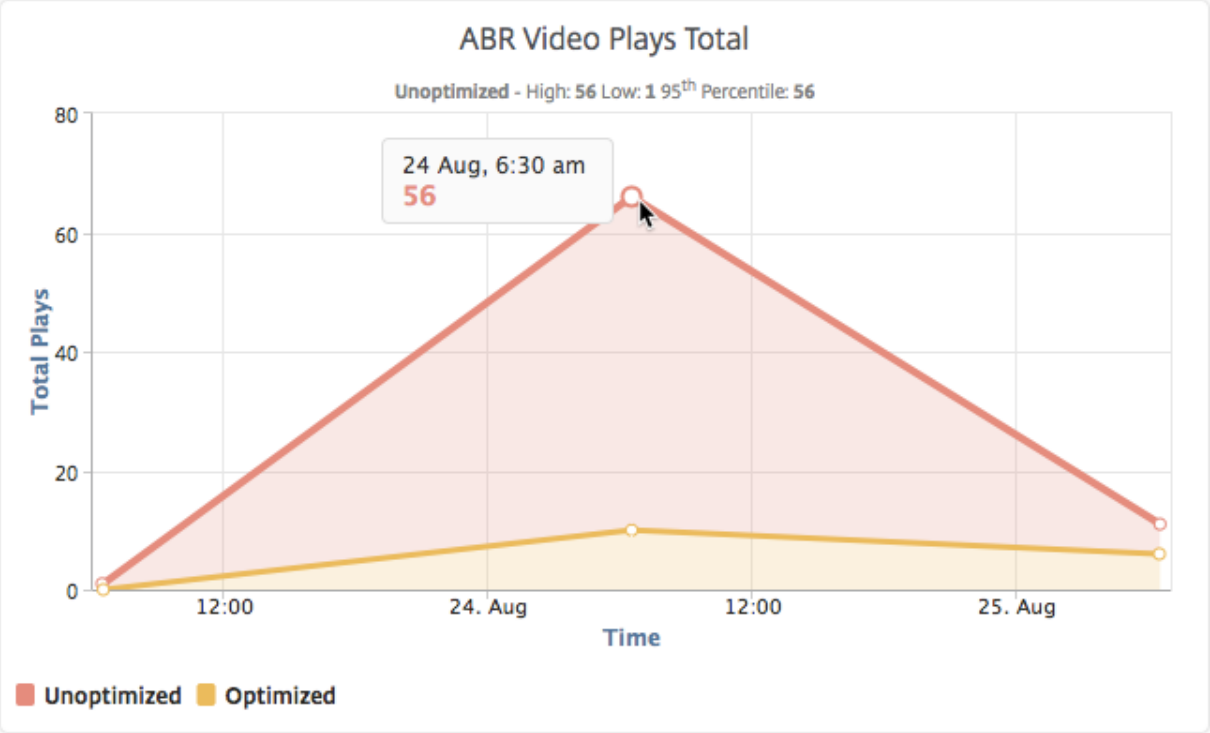
Para ver el número de reproducciones, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **ABR Video Analytics**. Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de

marco de tiempo. Haga clic en **Ir** y seleccione la ficha **N.º de reproducciones**.

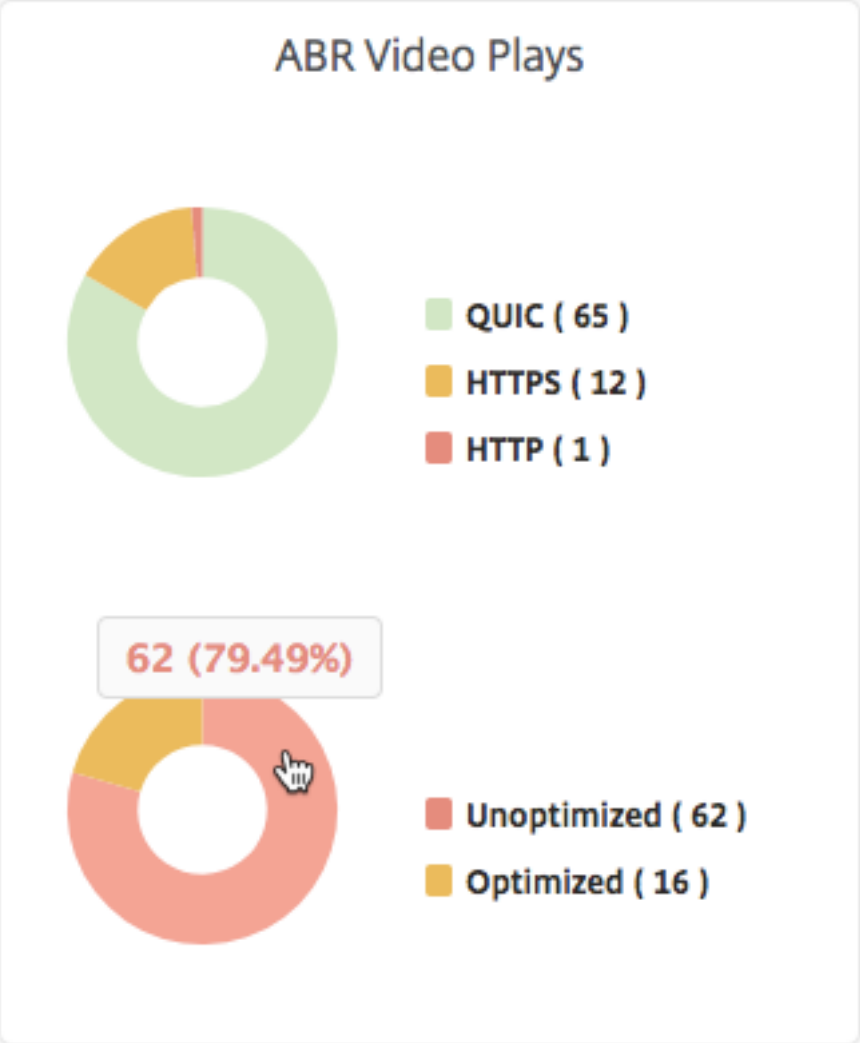
Puedes usar la lista desplegable **Filtros** para seleccionar los vídeos ABR de HTTP, HTTPS o QUIC.



La ficha **N.º de reproducciones** proporciona un gráfico de líneas y un gráfico circular que describe el número de reproducciones de vídeos ABR de la red y el número de reproducciones optimizadas y no optimizadas de vídeos ABR de la red para el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver el número de reproducciones durante un período de tiempo determinado:



Además, puede colocar el puntero del mouse sobre el gráfico circular para mostrar el porcentaje de reproducciones optimizadas y no optimizadas y el porcentaje de vídeos ABR cifrados y no cifrados para el período de tiempo seleccionado.



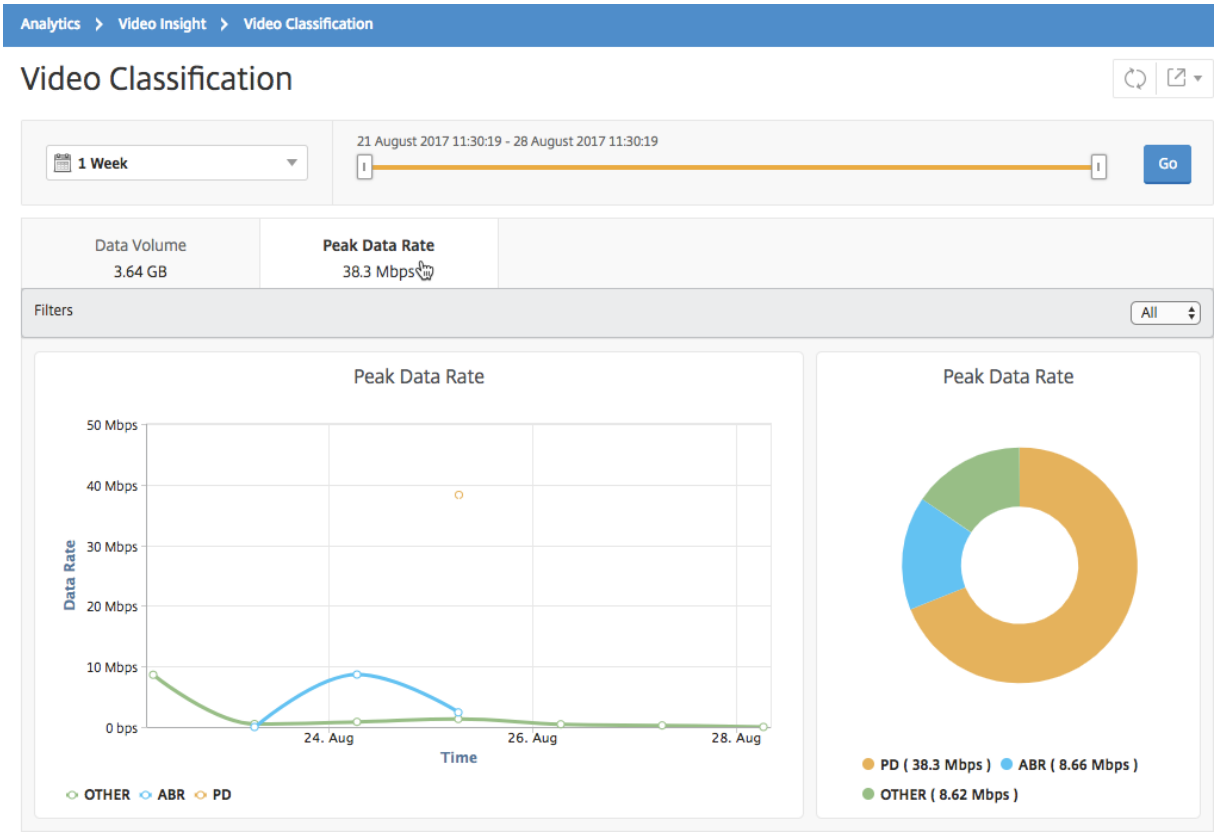
Ver la velocidad máxima de datos para un período de tiempo específico

January 30, 2024

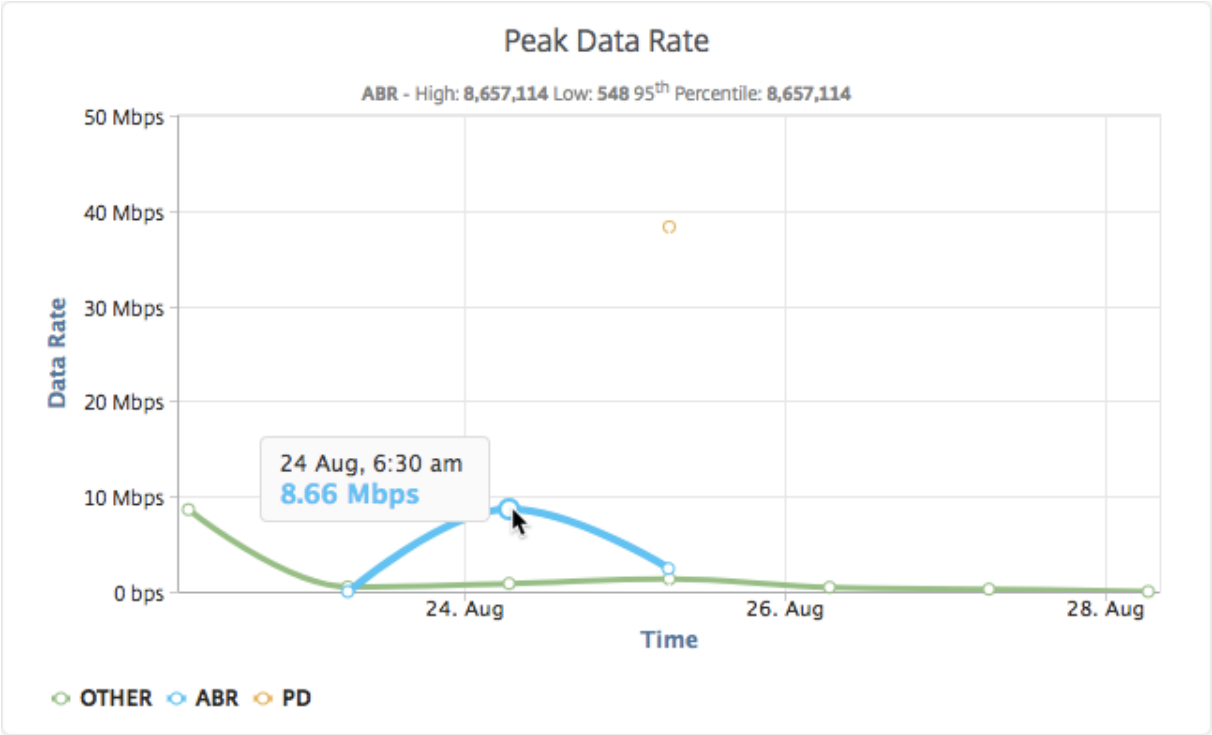
NetScaler Application Delivery Management (ADM) muestra el rendimiento máximo o la velocidad de datos del tráfico de vídeo de la red.

Para ver la velocidad máxima de datos del tráfico de vídeo, inicie sesión en Citrix ADM, vaya a **Analytics > Video Insight** y haga clic en **Clasificación** de vídeos . Luego, en el panel derecho, selecciona un período de tiempo de la lista desplegable. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo. Haga clic en **Ir** y seleccione la ficha **Tasa de datos máxima**.

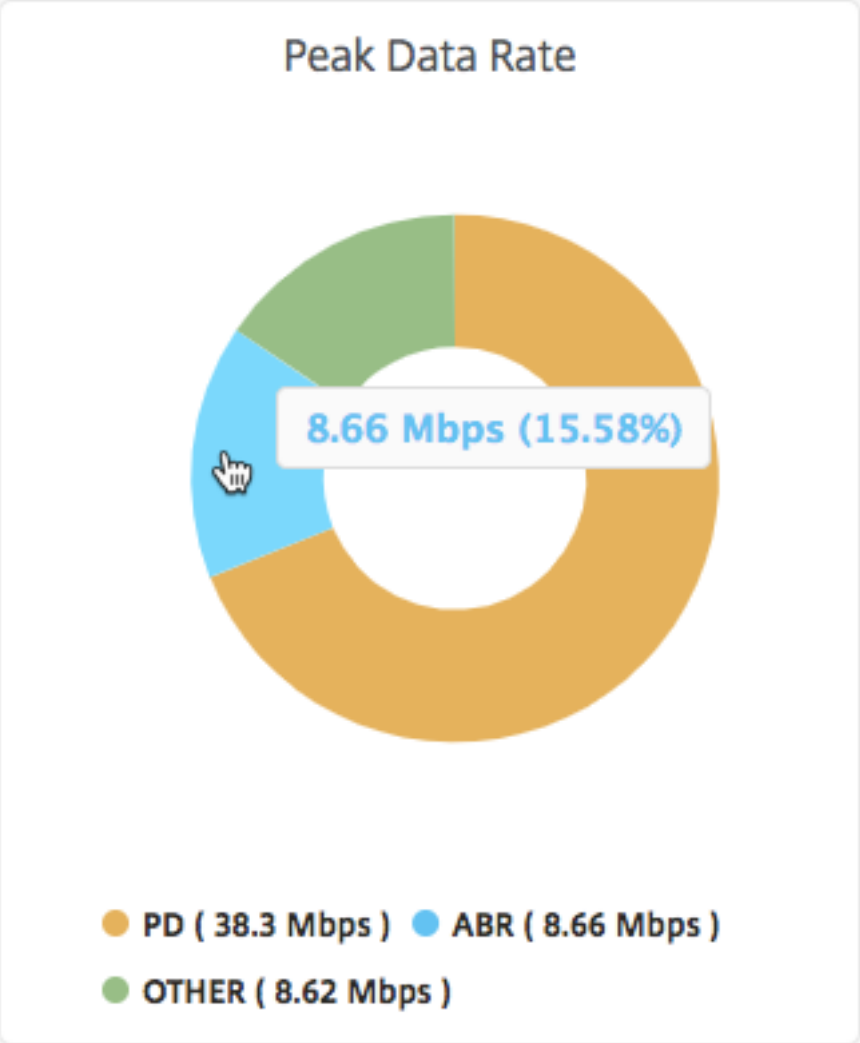
Puede usar la lista desplegable **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.



La ficha **Velocidad máxima de datos** proporciona un gráfico de líneas y un gráfico circular que describe la velocidad máxima de datos del tipo de transmisión de tráfico de vídeo desde la red y la velocidad máxima de datos del tráfico de vídeo en la red durante el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para mostrar la velocidad máxima de datos durante un período de tiempo determinado.



Además, puede colocar el puntero del mouse sobre el gráfico circular para mostrar el porcentaje de la velocidad máxima de datos consumida por el tipo de tráfico de vídeo transmitido durante el período de tiempo seleccionado.



Análisis de Secure Web Gateway

January 30, 2024

Un dispositivo Citrix Secure Web Gateway (SWG) en el extremo de la red empresarial actúa como un proxy de Internet. El dispositivo puede funcionar en modo proxy transparente o modo proxy explícito y ofrece controles para interceptar el tráfico de Internet, incluido HTTPS. La decisión de interceptar, omitir o bloquear cualquier solicitud se toma en función de las directivas configuradas en el dispositivo. Un usuario se autentica antes de iniciar sesión en la red empresarial. Todas las solicitudes y respuestas se etiquetan al usuario y las actividades del usuario se registran en el dispositivo. Para obtener más información, consulte Citrix Secure Web Gateway.

Al integrar Citrix Application Delivery Management (ADM) con un dispositivo Citrix SWG, la actividad del usuario registrada y los registros posteriores del dispositivo se exportan a Citrix ADM mediante

logstream. NetScaler ADM recopila y presenta información sobre las actividades de los usuarios, como los sitios web visitados y el ancho de banda gastado. También informa sobre el uso del ancho de banda y las amenazas detectadas, como malware y sitios de phishing. Puede utilizar estas métricas clave para supervisar la red y realizar acciones correctivas con el dispositivo Citrix SWG.

Para integrar un dispositivo Citrix SWG con Citrix ADM:

1. En el dispositivo Citrix SWG, al configurar Secure Web Gateway, habilite **Analytics** y proporcione los detalles de la instancia de Citrix ADM que quiere usar para el análisis.
2. En Citrix ADM, agregue el dispositivo Citrix SWG como instancia a Citrix ADM. Para obtener más información, consulte Agregar instancias a NetScaler ADM.

Paneles

January 30, 2024

24 de mayo de 2018

NetScaler Application Delivery Management (ADM) proporciona dos paneles, el Panel de **tráfico saliente y el Panel** de **usuario**. Estos paneles muestran varios gráficos que resumen los sitios web o las aplicaciones a las que se accede desde la red empresarial, así como las actividades realizadas por los usuarios de la red.

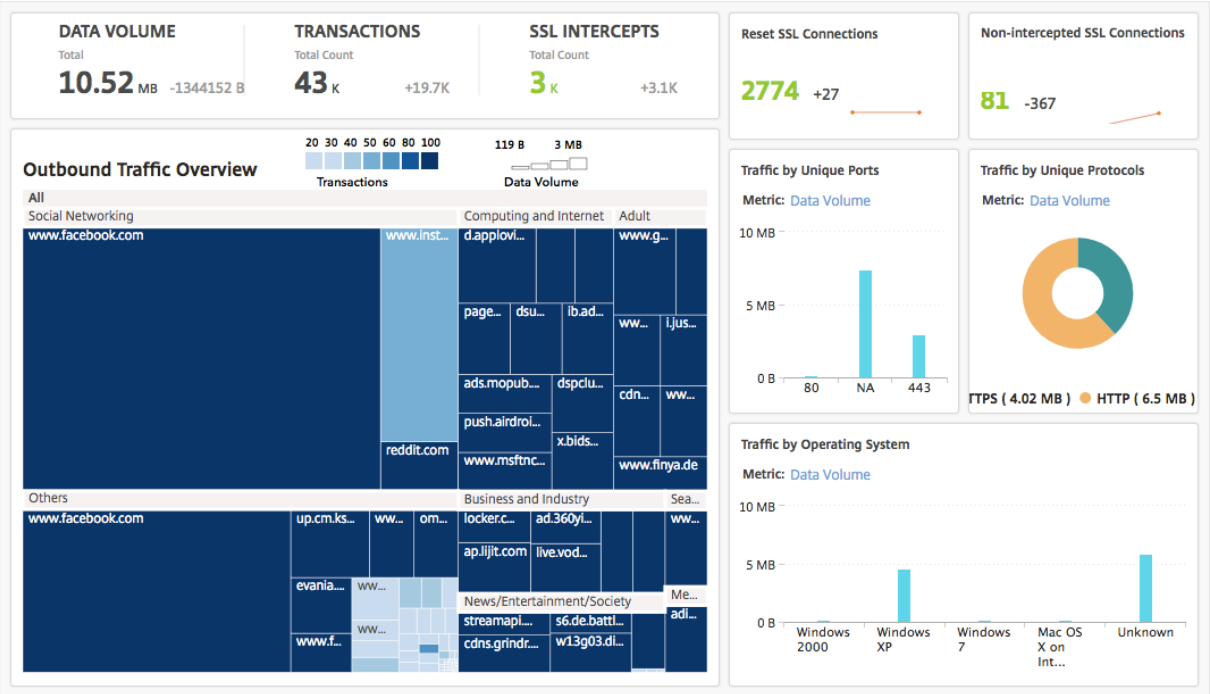
Panel de tráfico saliente

El **Panel de control de tráfico saliente** proporciona un resumen de las direcciones URL o dominios a los que se accede desde la red. Proporciona una visión holística de todas las URL o dominios por número de transacciones o volumen de datos consumido por las URL o dominios.
También proporciona detalles como los siguientes:

1. Cantidad de ancho de banda que consumen las URL o los dominios a los que se accede desde la red.
2. Número de transacciones que se produjeron al acceder a las direcciones URL y dominios de la red.
3. Número de conexiones SSL interceptadas por el dispositivo Citrix SWG durante las transacciones.
4. Número de conexiones SSL no interceptadas por el dispositivo Citrix SWG durante las transacciones.

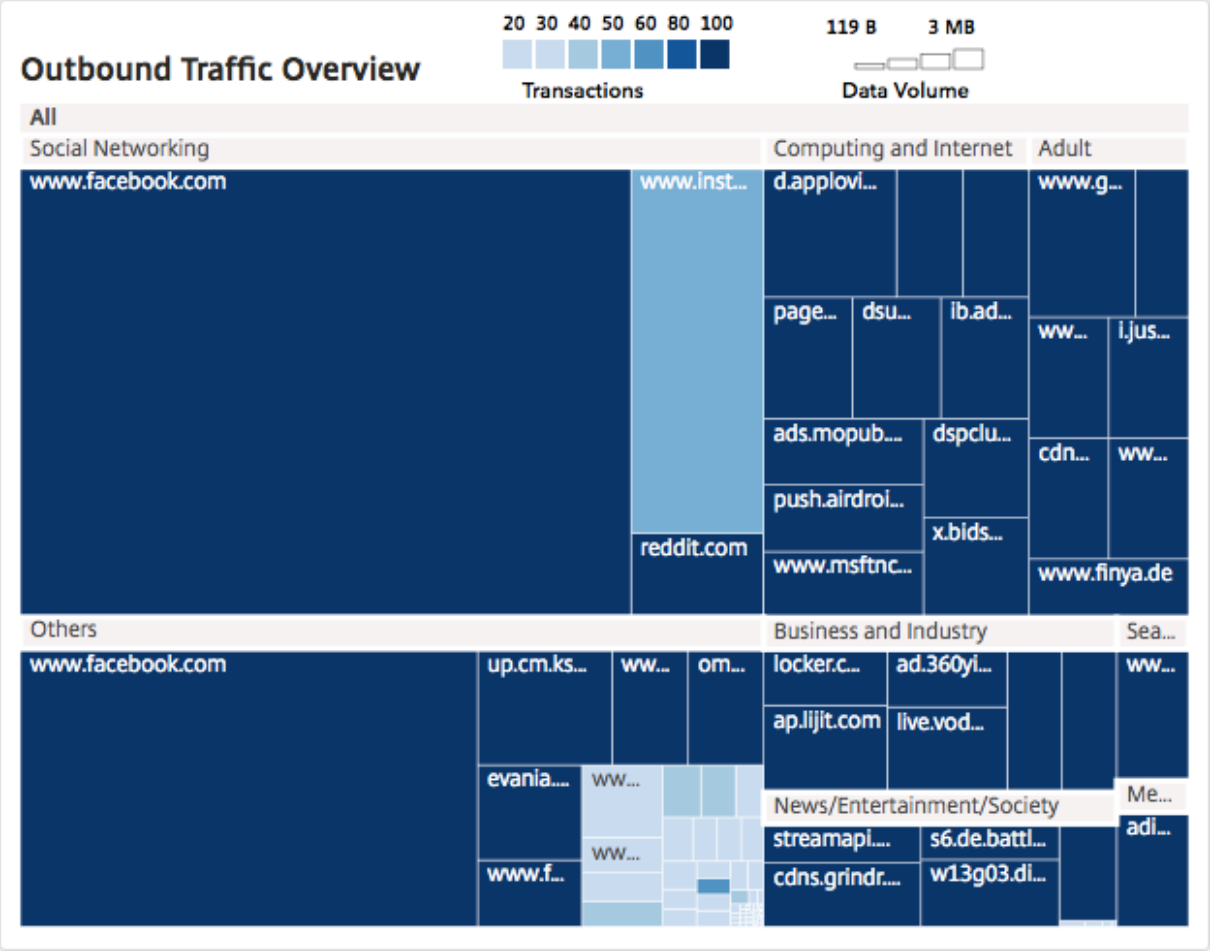
5. Número de conexiones SSL restablecidas por el dispositivo Citrix SWG durante las transacciones.
6. Cantidad de tráfico web transmitido, basado en el puerto utilizado para transmitir el tráfico, el protocolo utilizado por el tráfico web y los sistemas operativos cliente utilizados para transmitir el tráfico.

Para acceder al Panel de control de tráfico saliente, vaya a **Aplicaciones > Panel de control de tráfico saliente**.



Ver el tráfico saliente de la red

El **Panel de control de tráfico salienteincluye un panel Información general del tráfico saliente**. En el panel**Descripción general del tráfico saliente**, NetScaler ADM agrupa las URL o dominios a los que se accede en categorías, como Compras, Noticias, Redes sociales, etc. El panel**Descripción general del tráfico saliente** muestra las URL o los dominios a los que se accede desde la red como nodos en las categorías de URL. El tamaño de los nodos se ajusta al volumen de datos consumido al acceder a la URL o al dominio. El color del nodo indica el número de transacciones que se produjeron al acceder a la dirección URL o dominio.



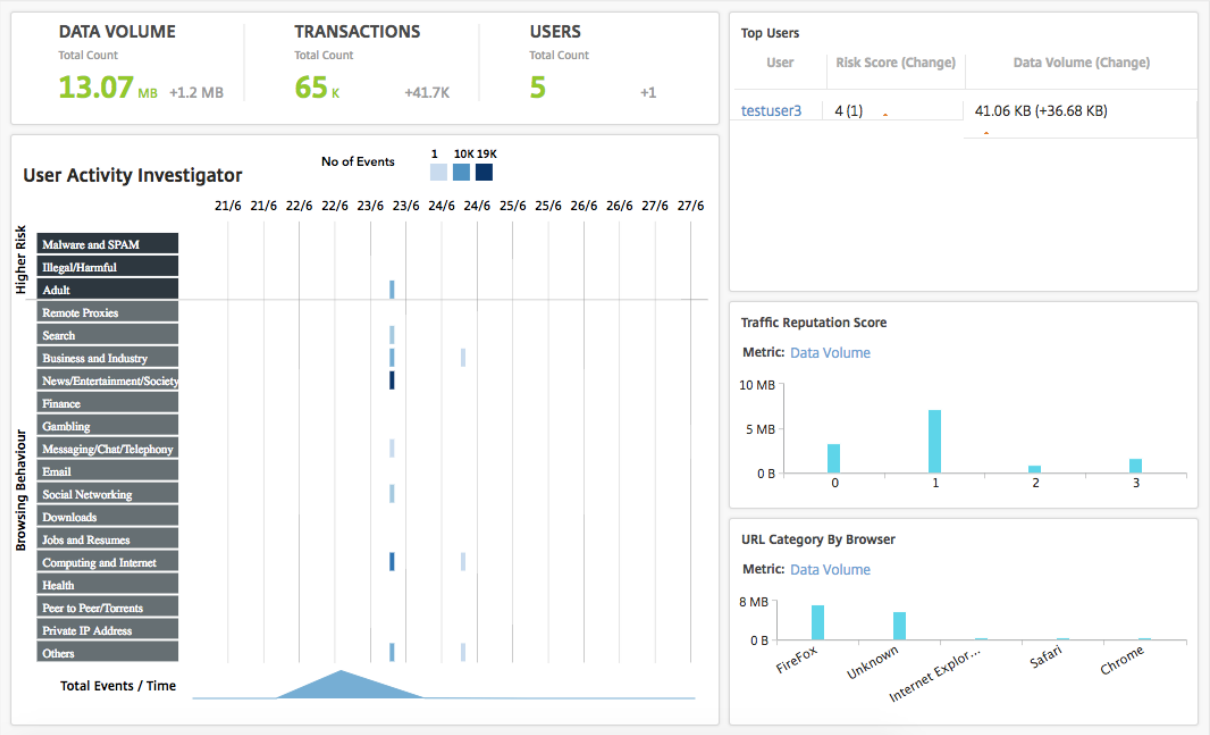
Puede hacer clic en una categoría para filtrar los gráficos y mostrar los detalles relacionados con la categoría durante el período de tiempo especificado.

Panel de usuario

El **Panel de control de usuario** muestra un resumen de las actividades realizadas por los usuarios de la empresa. Proporciona métricas clave que puede utilizar para determinar lo siguiente:

1. Comportamiento de navegación de los usuarios de su empresa.
2. Categorías de URL a las que acceden los usuarios de su empresa.
3. Los cinco usuarios principales, en función de sus puntuaciones de riesgo y del ancho de banda que consumen. Para obtener más información sobre la puntuación de riesgo, consulte Puntuación de riesgo.
4. Exploradores utilizados para acceder a las URL o dominios.
5. Cantidad del tráfico web generado por los usuarios, en función de la puntuación de la reputación del tráfico.

Para acceder al **Panel de control de usuarios**, vaya a **Usuarios > Panel de control**.

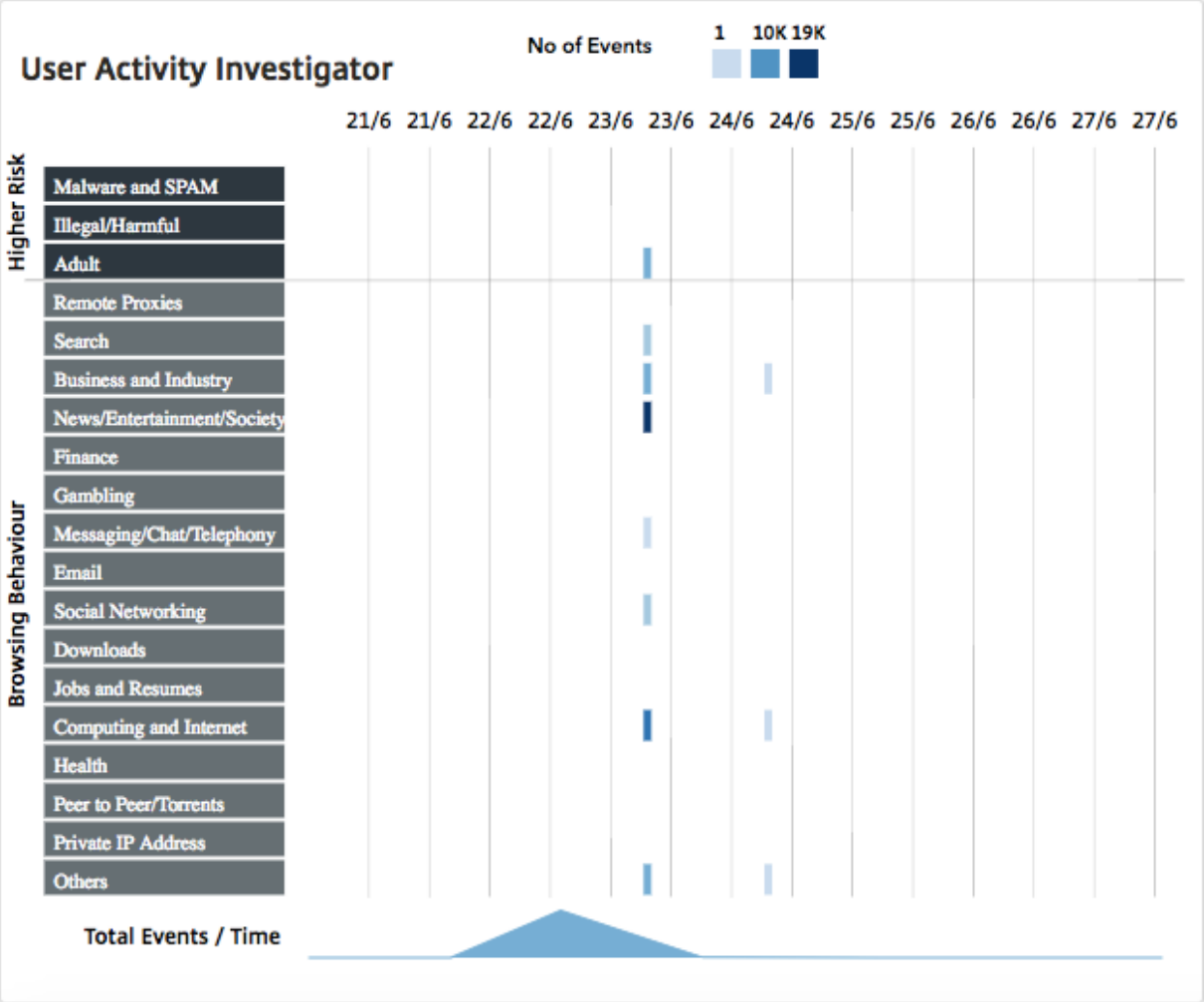


Puede hacer clic en un usuario en el panel **Usuarios** principales para filtrar los gráficos y mostrar los detalles de la actividad web realizada por el usuario en el período de tiempo especificado.

Investigador de actividad de usuario

El **Panel** de control de **usuario incluye un panel Investigador de actividad** de usuario que muestra diversas actividades web realizadas por los usuarios. Muestra las categorías de URL a las que acceden los usuarios durante el período de tiempo seleccionado, y varios eventos desencadenados por categoría de URL. Puede hacer clic en los eventos para obtener los detalles del nivel de transacción.

El **Investigador de actividad de usuario** muestra información clave, como el comportamiento de exploración del usuario, la actividad de alto riesgo del usuario y los eventos desencadenados, por categoría de URL. Los eventos se muestran como leyendas rectangulares en el gráfico. Cada una de las leyendas se agrega a intervalos de un minuto si la duración seleccionada es de una hora, y a intervalos de una hora si la duración seleccionada es de un día.



Estas leyendas se agregan y se codifican por colores según el número de eventos que se han producido. Puede colocar el puntero del mouse sobre una leyenda para mostrar detalles como la hora y el número de eventos agregados para la leyenda seleccionada. Puede personalizar el período de tiempo del gráfico seleccionando un tiempo en el menú desplegable de períodos de tiempo.

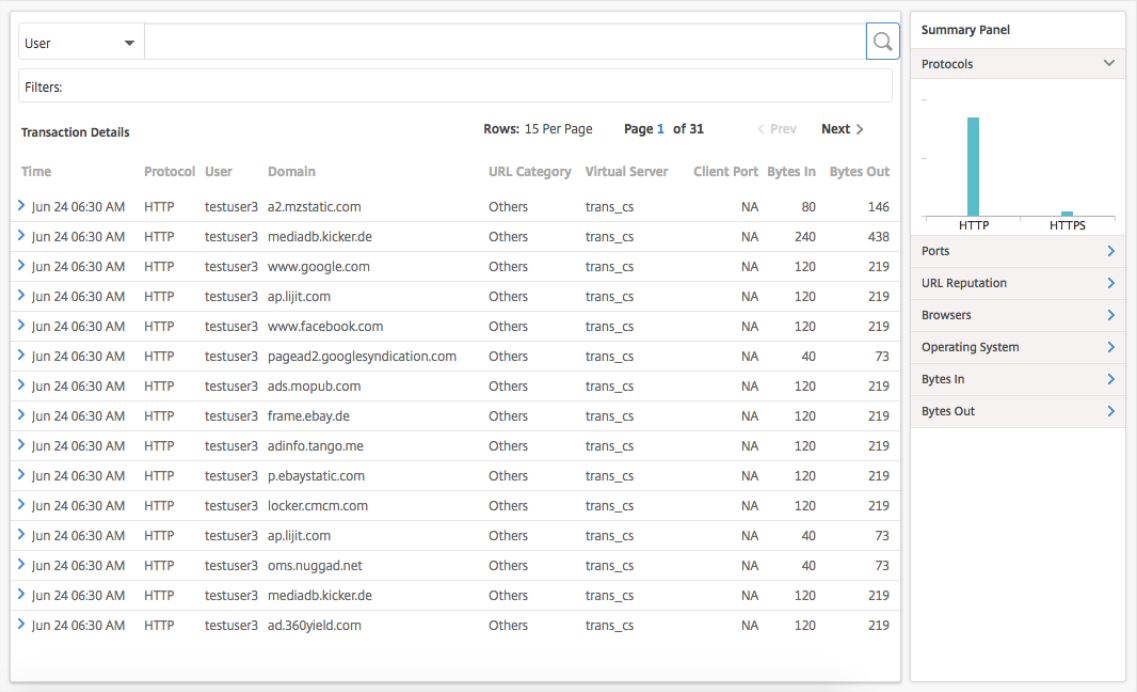
Puede hacer clic en los eventos para profundizar en los detalles de las transacciones.

Transacciones de usuario

La página Transacciones de Usuario muestra los detalles de las transacciones de usuario de la red. Proporciona detalles a nivel de transacción, como:

1. Hora en la que se produjo la transacción
2. Protocolo utilizado para la transacción
3. Nombre de usuario
4. Dominio al que accedió el usuario

5. Categoría de URL
6. Servidor proxy utilizado para interceptar la transacción
7. Detalles del puerto del cliente
8. Bytes en
9. Bytes de salida



Panel Resumen El **panel de resumen** muestra todas las métricas de las transacciones que están visibles en el panel **Detalles de la transacción**. Este panel le permite ordenar y ver las transacciones en el panel **Detalles de la transacción** seleccionando o deseleccionando las métricas. El **panel de resumen** muestra las siguientes métricas:

Métricas	Descripción
Protocolos	Protocolos utilizados en las transacciones
Puertos	Puertos utilizados para las transacciones
Reputación URL	Puntuación de reputación de URL
Exploradores web	Exploradores utilizados para las transacciones
Sistema de operación	Sistema operativo utilizado para las transacciones

Métricas	Descripción
Bytes en	Cantidad de datos recibidos a través del dispositivo Citrix SWG.
Bytes de salida	Cantidad de datos enviados a través del dispositivo Citrix SWG.

Puntuación de riesgo

Risk Score es un sistema de puntuación utilizado en NetScaler ADM para determinar los riesgos asociados con los usuarios de su empresa. Citrix ADM asigna una puntuación de riesgo basada en la puntuación de reputación de URL asignada por el dispositivo Citrix SWG a las URL a las que acceden los usuarios de la red. Para obtener información sobre la puntuación de reputación de URL, consulte Puntuación de reputaciónde URL. En la siguiente tabla se describen las puntuaciones de riesgo asignadas por NetScaler ADM.

Puntuación de riesgo	Descripción
1	La actividad web del usuario no se percibe como una amenaza o no es anormal.
2	La actividad web del usuario no se percibe como una amenaza o no es anormal, pero el usuario accede a “sitios desconocidos”, que no tienen puntuaciones de reputación en las URL.
3	No se detecta ninguna amenaza en la actividad web del usuario, pero este ha intentado acceder a sitios que son potencialmente vulnerables o están afiliados a sitios que son potencialmente vulnerables.
4	Usuario potencialmente comprometido.
5	La actividad web del usuario es anormal y el usuario ha accedido a sitios maliciosos conocidos.

Casos de uso

January 30, 2024

Supervisión de las interceptaciones de SSL

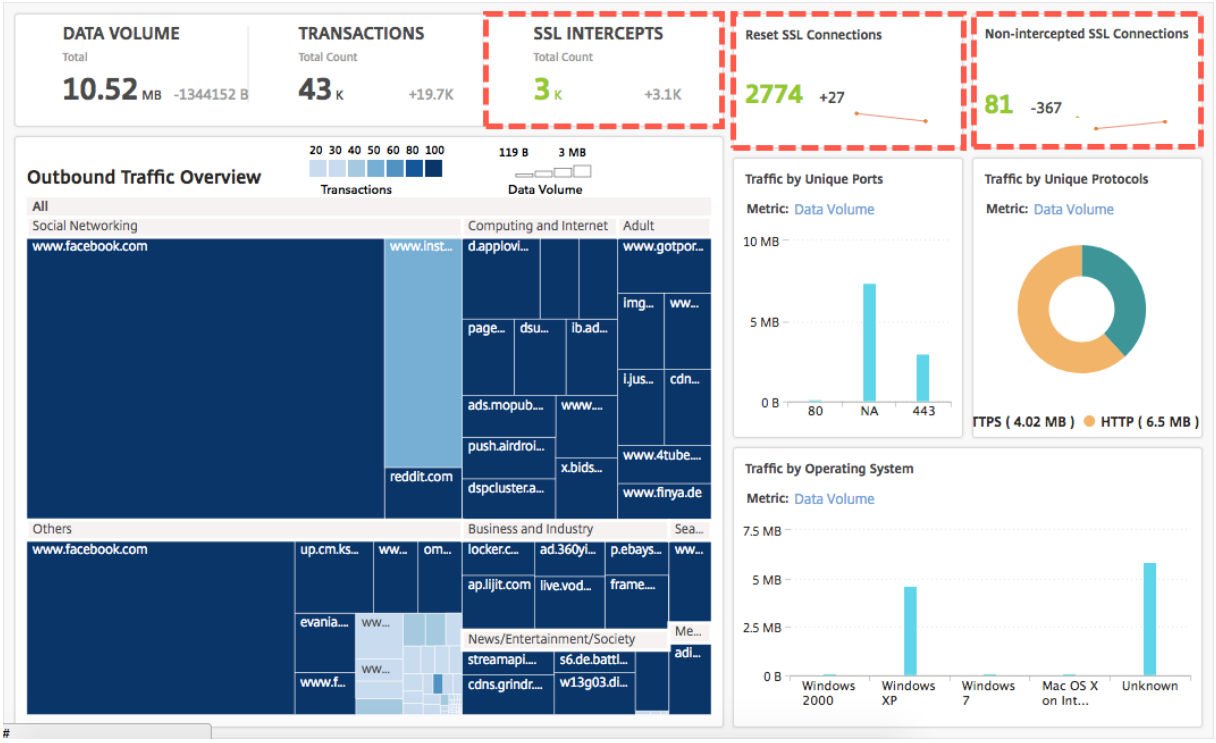
Un dispositivo Citrix SWG le permite inspeccionar el tráfico saliente cifrado. Puede interceptar, omitir o bloquear cualquier solicitud HTTPS en función de las políticas configuradas en el dispositivo. NetScaler Application Delivery Management (ADM) proporciona los siguientes detalles acerca de las conexiones SSL en el **Panel de control de tráfico saliente** para un período de tiempo seleccionado:

- Número de conexiones SSL interceptadas, no interceptadas y restablecidas por el dispositivo Citrix SWG
- Detalles de transacción de las conexiones SSL

Con estos detalles, puede ajustar aún más las políticas de su dispositivo Citrix SWG para inspeccionar de manera eficiente el tráfico saliente cifrado. Para obtener más información, consulte Citrix Secure Web Gateway.

Para mostrar el número de conexiones SSL que se han interceptado, no interceptado y restablecer:

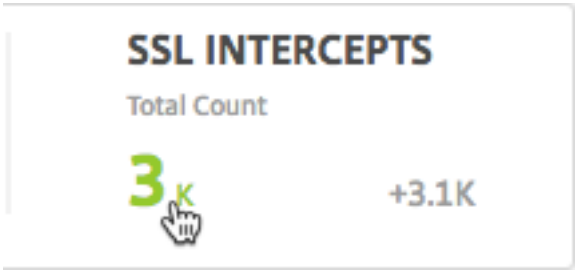
Vaya a **Aplicaciones > Panel de control de tráfico saliente**.El Panel de control de tráfico fuera de borda muestra el número de conexiones SSL interceptadas, no interceptadas y restablecidas.



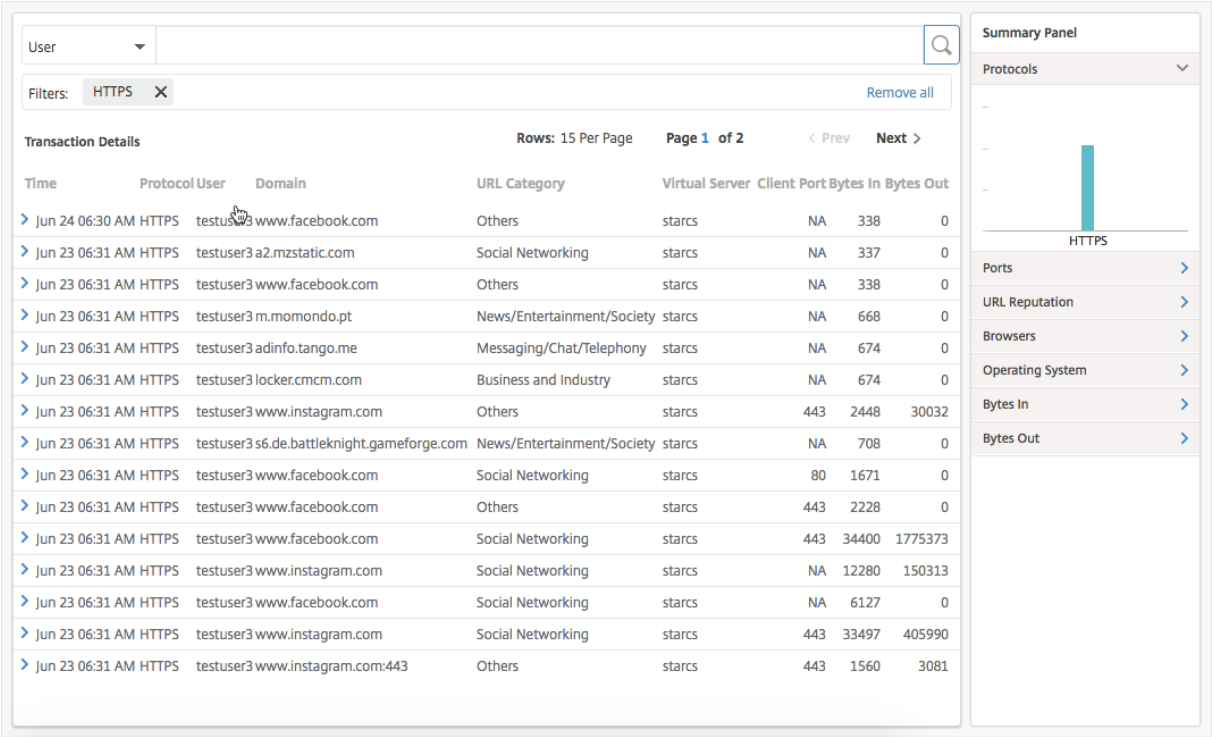
Para mostrar los detalles de transacción de las conexiones SSL que se han interceptado:

1. Vaya a **Aplicaciones > Panel de control de tráfico saliente**.

2. En el **panel de control de tráfico fuera**de borda, haga clic en el recuento total en la sección **SSL INTERCEPTS**.



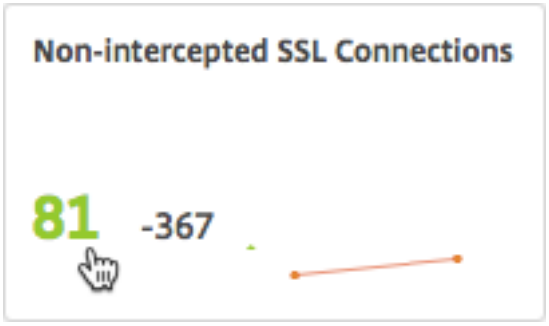
Los detalles de transacción de las conexiones SSL interceptadas durante el período de tiempo seleccionado se muestran en la página **Detalles de Transacción**.



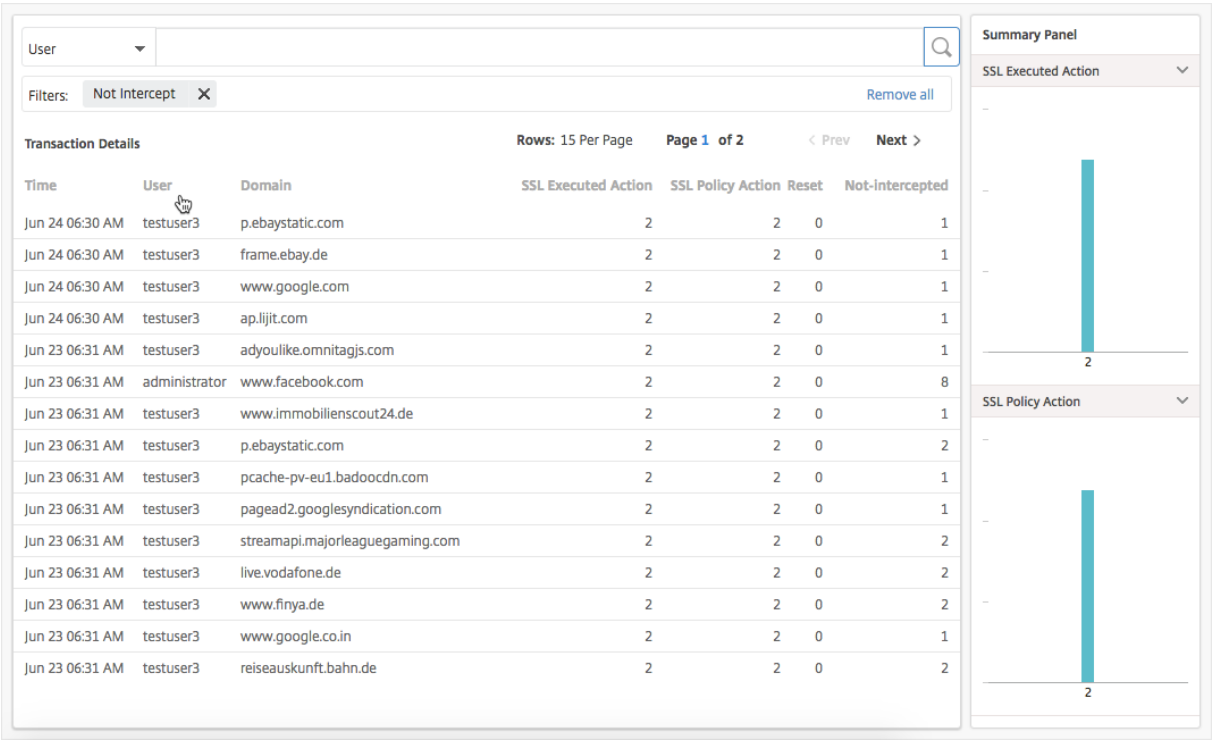
Puede filtrar aún más los detalles de las transacciones por usuario y categoría de URL.

Para ver los detalles de las transacciones de las conexiones SSL en las que no se interceptó el tráfico:

1. Vaya a **Aplicaciones > Panel de control de tráfico saliente**.
2. En el **Panel de control de tráfico fuera**de borda, haga clic en el recuento total de la sección **Conexiones SSL no interceptadas**.



Los detalles de transacción de las conexiones SSL en las que no se interceptó tráfico durante el período de tiempo seleccionado aparecen en la página **Detalles de Transacción**.

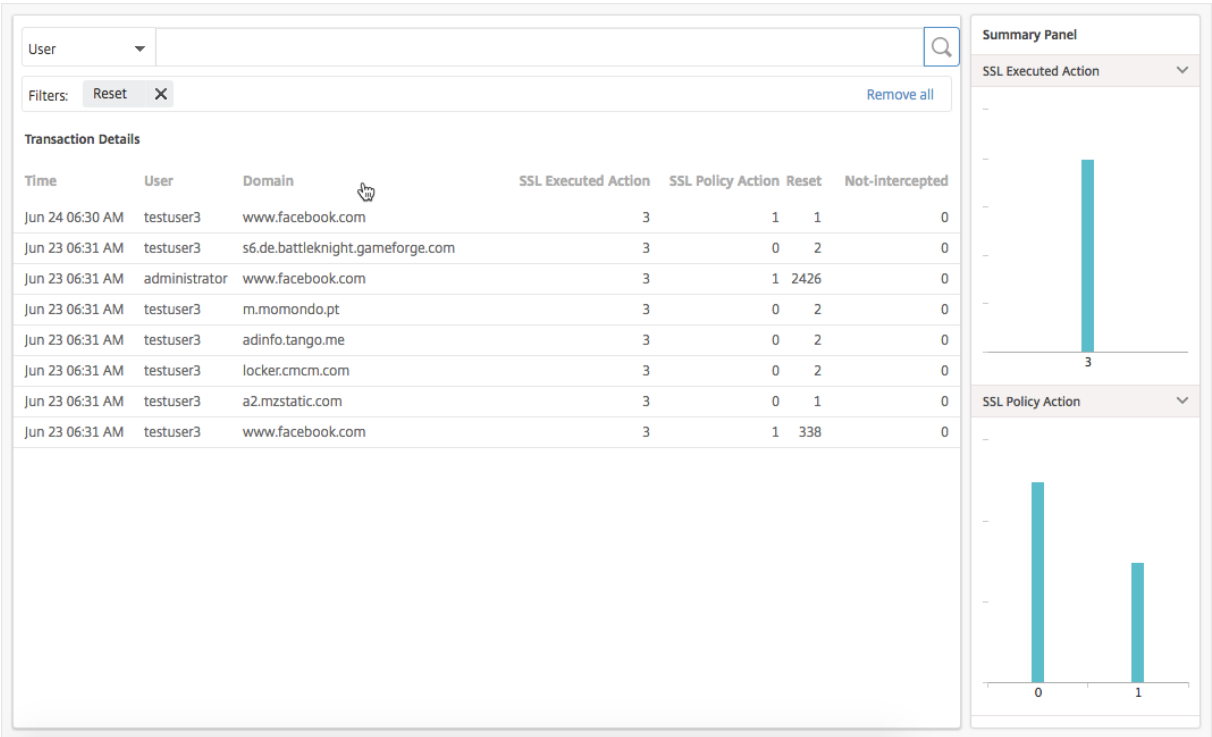


Puede filtrar aún más los detalles de las transacciones por usuario y categoría de URL.

Para mostrar los detalles de las transacciones de las conexiones SSL que se han restablecido:

1. Vaya a **Aplicaciones > Panel de control de tráfico saliente**.
2. En el **Panel de control de tráfico fuera**de borda, haga clic en el recuento total en la sección **Restablecer conexiones SSL**.

Los detalles de la transacción de las conexiones SSL en las que no se interceptó tráfico durante el período de tiempo seleccionado aparecen en la página **Detalles de la transacción**.



Puede filtrar aún más los detalles de las transacciones por la categoría de usuario y URL.

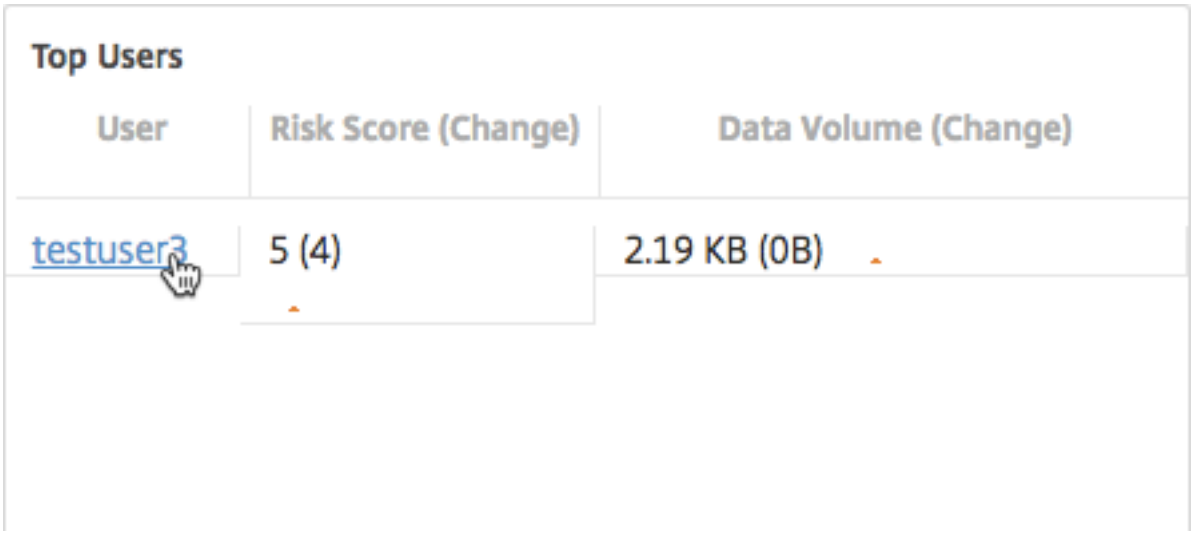
Inspección de puntos finales

Las políticas que ha configurado en un dispositivo Citrix SWG especifican cómo el dispositivo registra todas las actividades de los usuarios realizadas en su empresa. NetScaler ADM proporciona métricas clave que puede utilizar para determinar:

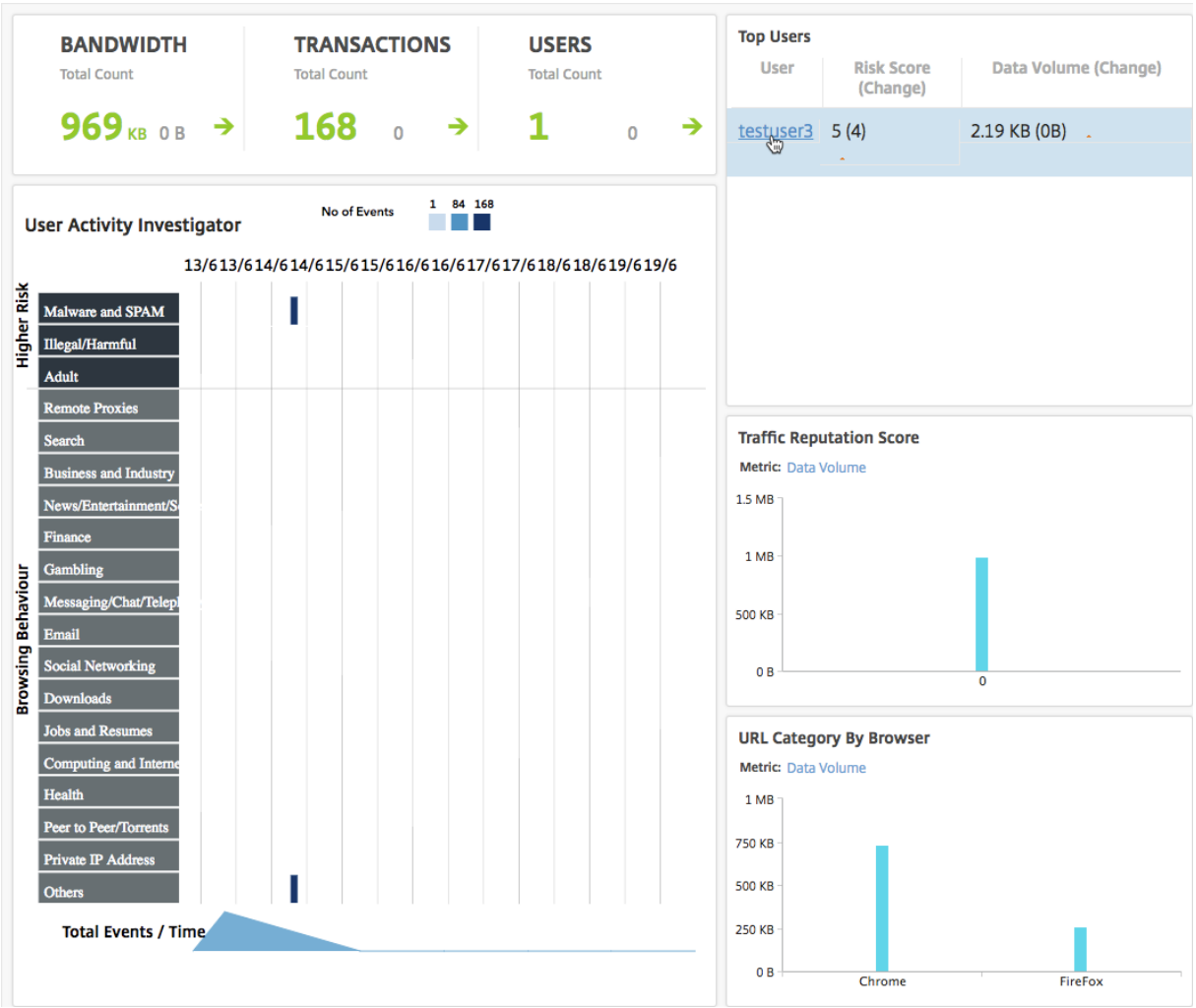
1. Comportamiento de navegación de los usuarios de su empresa.
2. Categorías de URL a las que acceden los usuarios de su empresa.

3. Los cinco usuarios principales, en función de sus puntuaciones de riesgo y del ancho de banda que consumen. Para obtener más información sobre las puntuaciones de riesgo, consulte Puntuación de riesgo.
4. Exploradores utilizados para acceder a las URL o dominios.
5. Cantidad del tráfico web generado por los usuarios, en función de la puntuación de la reputación del tráfico.

Por ejemplo, si un usuario con el identificador de usuario testuser3 accede constantemente a sitios relacionados con malware en su empresa, NetScaler ADM identifica al usuario como usuario con actividad de alto riesgo y le asigna una puntuación de riesgo más alta. La información de testuser3 se muestra en la sección **Usuarios principales** del **Panel de usuarios**.

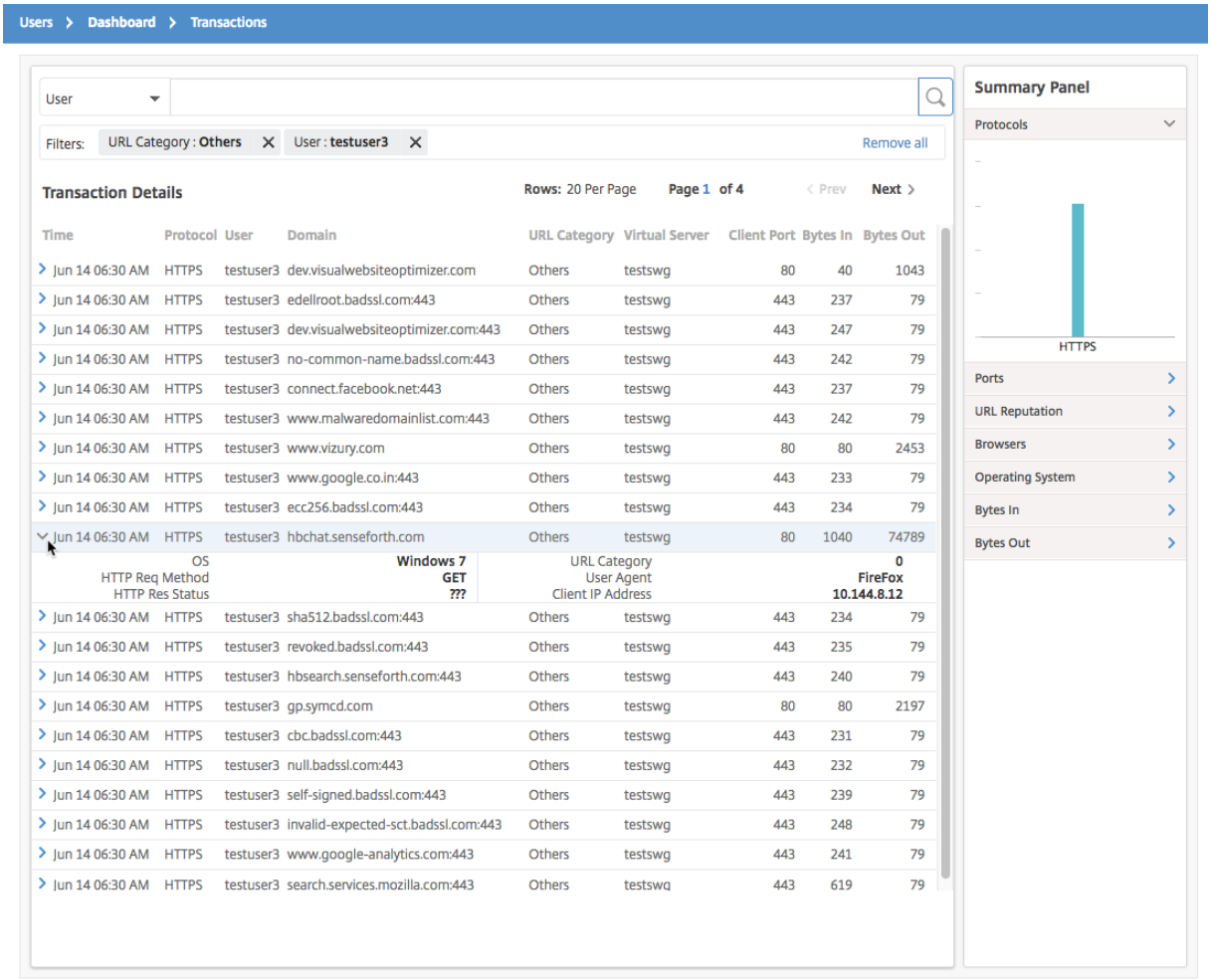


Puedes hacer clic en testuser3 para filtrar el **panel de usuario** y mostrar todas las métricas clave relacionadas con testuser3.



En el panel **Investigación de actividad del usuario**, la actividad de alto riesgo de testuser3 se muestra como eventos en las respectivas categorías de URL.

Puede colocar el cursor sobre los eventos para ver el número de eventos y hacer clic en los eventos para investigar las transacciones que se produjeron durante los eventos.

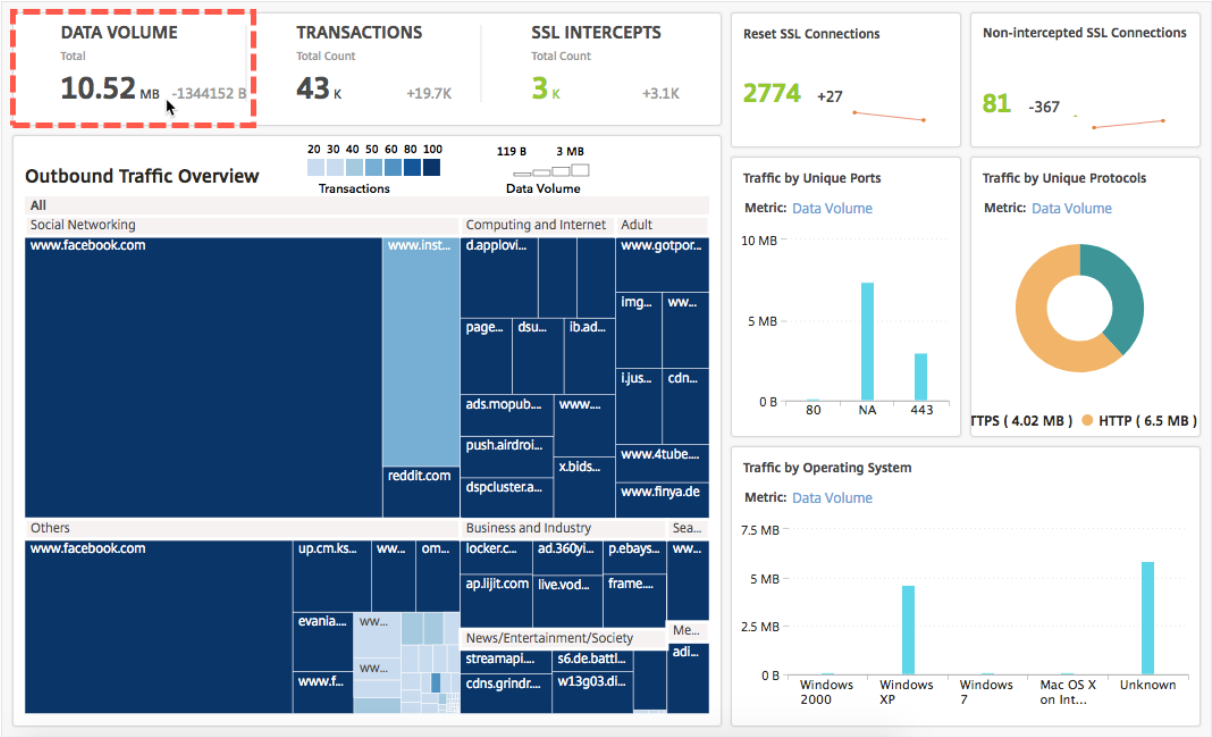


Con esta información, puede determinar si el sistema del usuario está infectado por malware o puede comprender el patrón de consumo de ancho de banda del usuario y ajustar las políticas SWG de Citrix. Para obtener más información, consulte la documentación de Citrix Secure Web Gateway.

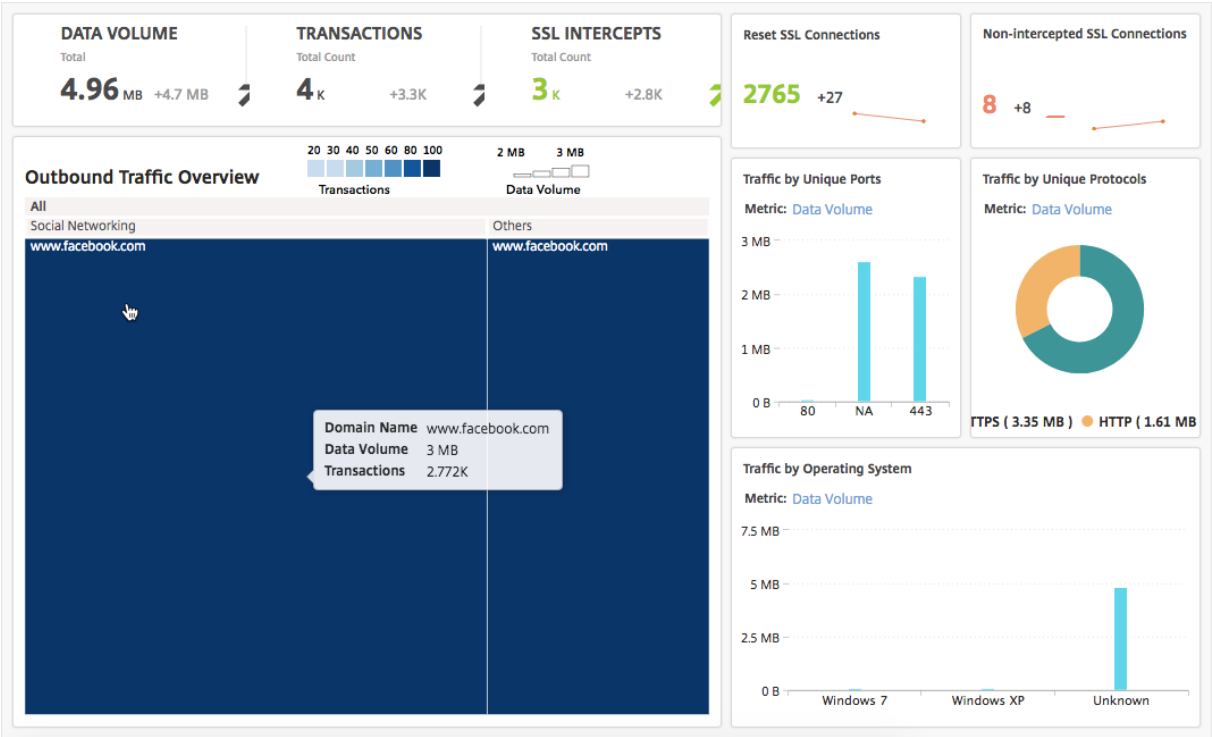
Informes del consumo de ancho de banda

El **Panel de control de tráfico saliente** y el **Panel de usuario** proporcionan varios gráficos que resumen los sitios web o las aplicaciones a las que se accede desde la red empresarial, así como las actividades realizadas por los usuarios de la red.

El **panel de tráfico saliente** proporciona los detalles del consumo del volumen de datos por parte de las URL o los dominios a los que se accedió desde la red. Vaya a **Aplicaciones > Panel de control de tráfico saliente**, donde los detalles del volumen de datos se muestran en la sección **Volumen de datos**.

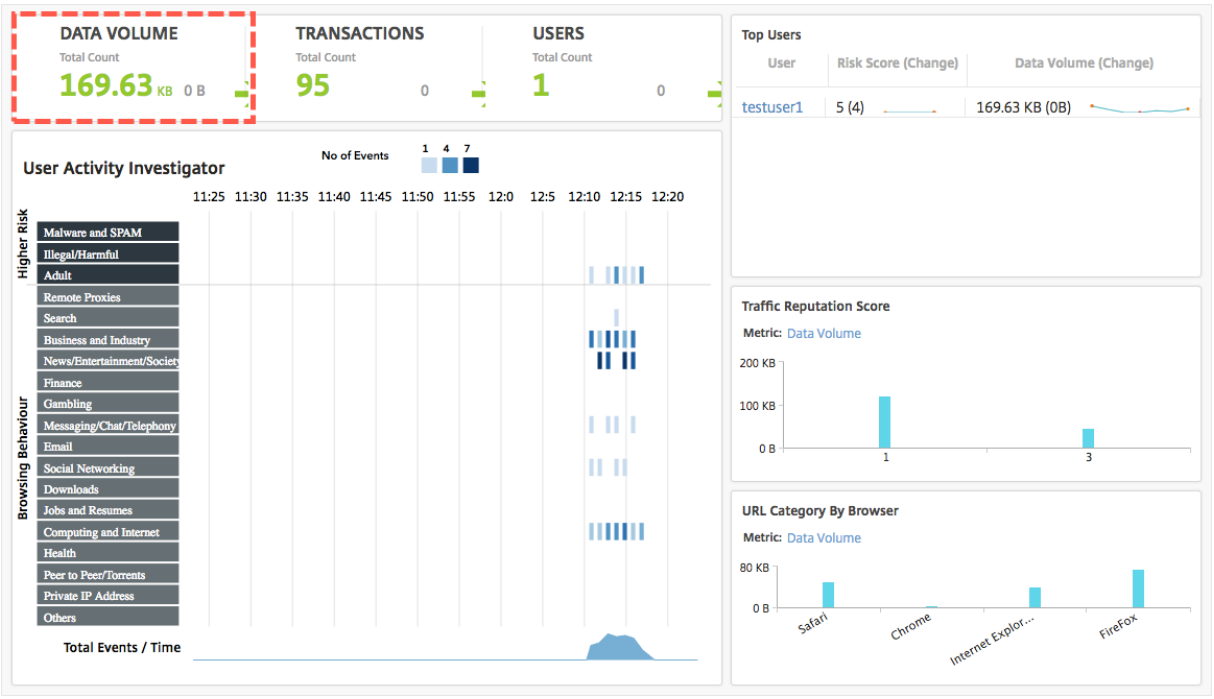


En el panel **Descripción general del tráfico** saliente , puede hacer clic en un dominio o URL para ver los detalles del volumen de datos consumido por el dominio o la URL.

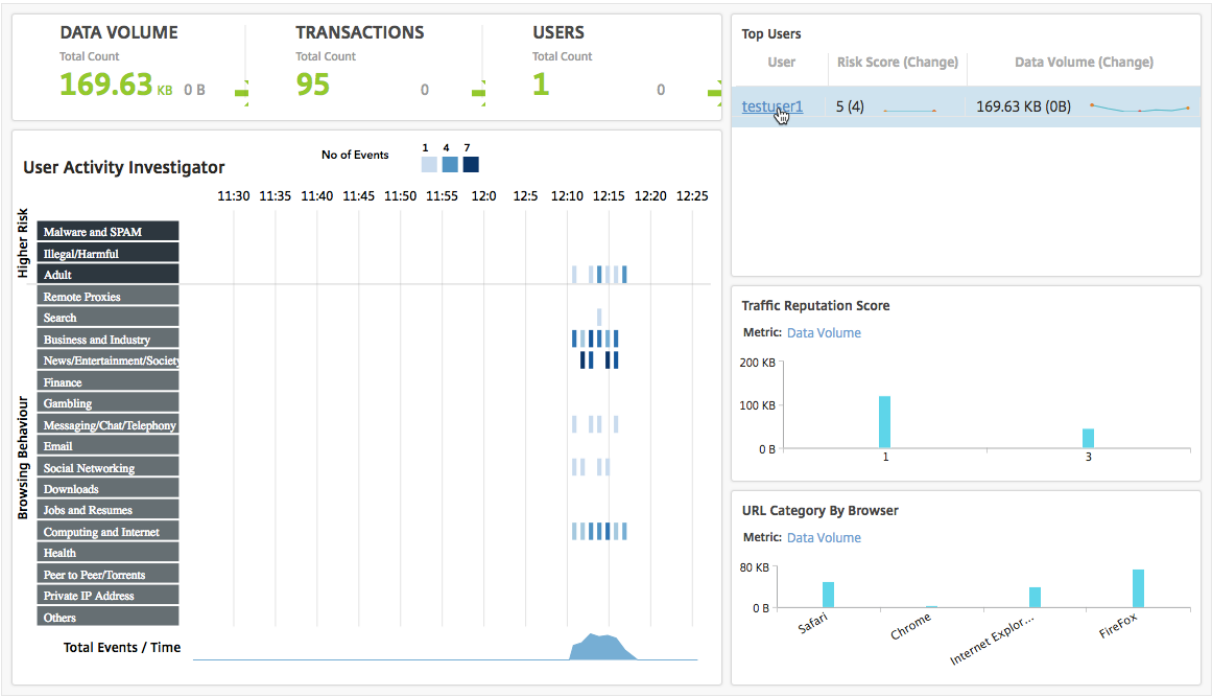


El **Panel de control de usuario** proporciona detalles sobre el ancho de banda consumido por los usuarios de la red. Vaya a **Usuarios > Panel de control** para mostrar los detalles del ancho de banda

consumido por los usuarios en la sección **VOLUMEN DE DATOS** del **Panel de usuario**.



Puede ver los detalles del ancho de banda consumido por un usuario seleccionándolo en la sección **Usuarios principales**. La sección **VOLUMEN DE DATOS** y otras métricas clave del gráfico se filtran para el usuario seleccionado.



Mediante estos detalles, puede comprender el consumo de ancho de banda y el motivo del consumo. Por ejemplo, si un usuario accede a sitios web de redes sociales y esto ha provocado un gran consumo

de ancho de banda, el administrador puede acceder al dispositivo Citrix SWG y configurar una función de lista de URL para controlar el acceso a los sitios web. Para obtener más información, consulte el tema Caso de uso: filtrado de URL mediante conjunto de URL personalizado.

Visualización de la distribución del tráfico saliente

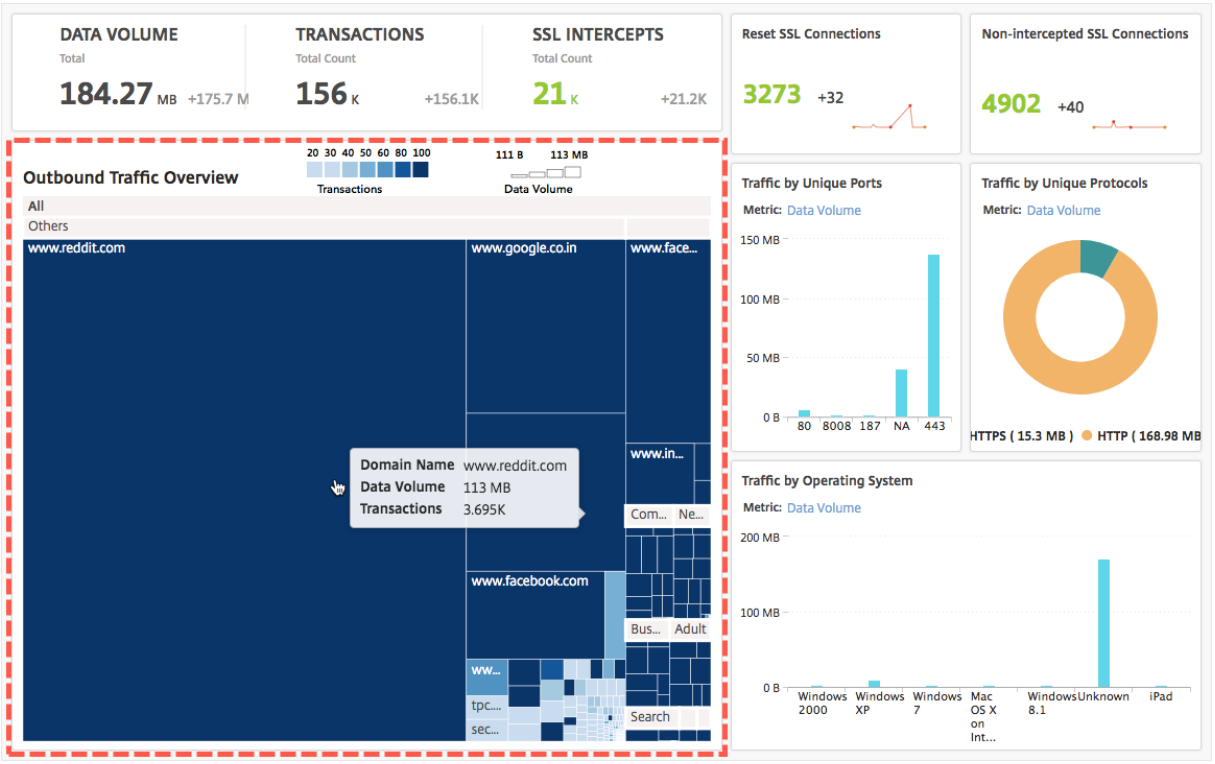
El dispositivo Citrix SWG proporciona funciones de categorización y filtrado de URL que puede utilizar para clasificar las URL a las que se accede desde la red. En NetScaler ADM, el **Panel de control de tráfico saliente** incluye un panel **Descripción general del tráfico saliente**. En el panel **Descripción general del tráfico saliente**, NetScaler ADM agrupa las direcciones URL o dominios a los que se accede en categorías, como Compras, Noticias, Móviles, etc. para mostrar la distribución del tráfico saliente en la red. Para un período de tiempo seleccionado, puede hacer clic en la URL para comprender:

1. Ancho de banda consumido accediendo a la URL
2. Transacciones que se produjeron al acceder a la URL
3. Número de conexiones SSL que se interceptaron, no se interceptaron y se restablecieron al acceder a la URL

Con esta información, puede comprender el patrón del tráfico saliente y tomar decisiones correctivas, como bloquear determinadas URL.

Para ver la distribución del tráfico saliente:

Vaya a **Aplicaciones > Panel de control de tráfico saliente**.El **Panel de control de tráfico externo** muestra las direcciones URL en el panel **Información general del tráfico saliente** :



Si quiere ver los detalles de una URL concreta, seleccione la URL.

Con esta información, puede comprender el patrón de tráfico saliente y controlar el tráfico de red mediante un filtro de URL configurado en su dispositivo SWG. Para obtener más información, consulte Filtrado de URL.

Orchestration

January 30, 2024

En las redes definidas por software (SDN), un controlador de aplicaciones de software administra una red y sus actividades en lugar del hardware que la soporta. Es decir, SDN permite a los administradores de red virtualizar una conectividad de red física en una conectividad de red lógica y administrar los servicios de red mediante una herramienta de administración centralizada basada en software. La SDN permite a los ingenieros y administradores de redes responder a los requisitos empresariales que cambian rápidamente.

Si bien las ventajas más conocidas de la SDN son la programabilidad del tráfico, la mayor agilidad, la capacidad de crear una supervisión de red basada en directivas y la implementación de la automatización de la red, algunas de las ventajas específicas de la SDN se enumeran a continuación:

- Aprovisionamiento de red centralizado

- Mayor seguridad de red a nivel granular
- Costes operativos reducidos
- Mayores niveles de abstracción en la nube
- Entrega de contenido garantizada
- Menor tiempo de inactividad de la red

Citrix Application Delivery Management (ADM) admite la SDN en la red empresarial al integrarse con los controladores SDN de diferentes proveedores. Citrix ADM admite tanto VMware NSX Manager como Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

Citrix ADM se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios Citrix ADC. Esta integración elimina las complejidades tradicionales asociadas con la topología de la red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios Citrix ADC de forma programática con mayor rapidez.

VMware NSX Manager expone firewalls lógicos, conmutadores, enrutadores, puertos y otros elementos de red para permitir la creación de redes virtuales entre diversos hipervisores, sistemas de administración de la nube y el hardware de red asociado. También es compatible con redes externas y servicios de seguridad.

La función Cloud Orchestration de Citrix ADM permite la integración de los productos Citrix ADC con VMware NSX y proporciona las siguientes funciones:

- Capacidad de asignar una VPX preaprovisionada bajo demanda a una determinada puerta de enlace Edge como parte de la inserción del servicio.
- Capacidad para configurar funciones avanzadas de NetScaler ADC, como SSL y CS, junto con el equilibrio de carga básico a través de plantillas de aplicación en las instancias que se ejecutan dentro del entorno NSX.
- Posibilidad de desasignar una VPX de una puerta de enlace Edge determinada como parte de la eliminación del servicio y reasignar la misma VPX a otra puerta de enlace Edge.
- Capacidad para implementar rápidamente funciones de NetScaler ADC desde la consola de vCenter como parte del flujo de trabajo de implementación de toda la infraestructura necesaria para una aplicación.

Ventajas:

- Asignación automatizada y a demanda de nuevos servicios de ADC como parte del flujo de trabajo de implementación de aplicaciones
- Configuración simplificada de la funcionalidad ADC avanzada y específica de la aplicación mediante plantillas de aplicación
- Separación de funciones entre múltiples inquilinos y modelo de consumo de autoservicio, a la vez que proporcionan a los administradores de la nube un único punto de control
- Integración más sencilla con las API NetScaler ADM, que ayudan a admitir usos futuros imprevistos.

Para obtener más información sobre cómo configurar VMware NSX Manager en NetScaler ADM, consulte Integración de dispositivos NetScaler ADC con VMware NSX Manager.

Modo híbrido ACI de Cisco

Cisco ACI introdujo la compatibilidad con el modo híbrido en la versión 1.3 (2f). En el modo híbrido, puede realizar la automatización de la red a través del controlador de infraestructura de políticas de aplicaciones (APIC) y delegar la configuración L4-L7 a Citrix ADM, que actúa como administrador de dispositivos en la APIC.

La solución Citrix ADC Hybrid Mode es compatible con un paquete de dispositivos de modo híbrido y Citrix ADM. Debe cargar el paquete de dispositivos de modo híbrido en la APIC. Para obtener más información, consulteNetScaler ADC Automation Using NetScaler ADM in Cisco ACI Hybrid Mode.

OpenStack: integre instancias de Citrix ADC

January 30, 2024

La función Cloud Orchestration de NetScaler Application Delivery Management (ADM) permite la integración de los productos Citrix NetScaler ADC con la plataforma OpenStack. Al utilizar esta función con la plataforma OpenStack, los usuarios de OpenStack pueden aprovechar la función de equilibrio de carga (LBaaS) del NetScaler ADC. Después de esto, los usuarios de OpenStack pueden implementar sus configuraciones de balanceador de carga desde OpenStack en la instancia de Citrix ADC.

En las siguientes secciones se proporciona una breve descripción de las funciones del flujo de trabajo de integración de Citrix ADM y OpenStack.

Controlador NetScaler ADC para OpenStack Neutron LBaaS

El complemento OpenStack Neutron LBaaS incluye un controlador Citrix ADC que permite a OpenStack comunicarse con el Citrix ADM. OpenStack utiliza este controlador para reenviar cualquier con-

figuración de equilibrio de carga realizada a través de las API de LBaaS, al NetScaler ADM, que crea la configuración del equilibrador de carga en las instancias de NetScaler ADC deseadas. OpenStack también utiliza el controlador para llamar a Citrix ADM a intervalos regulares y recuperar el estado de las diferentes entidades (como los VIP y los grupos) de todas las configuraciones de equilibrio de carga de los ADC de Citrix. El software de controlador Citrix ADC para la plataforma OpenStack se incluye junto con el Citrix ADM. Para descargar e instalar los controladores, primero debe instalar NetScaler ADM e iniciar la aplicación.

Registrar Citrix ADM y OpenStack entre sí

Primero debe registrar la información de OpenStack en NetScaler ADM. Especifique la dirección IP del controlador OpenStack y las credenciales de usuario administrativo de la nube, así como las credenciales de usuario del controlador Citrix ADC de OpenStack. Más adelante, puede especificar las mismas credenciales de inicio de sesión en la sección Citrix ADC_Driver del archivo de configuración de Neutron (neutron.conf) para que el controlador Citrix ADC de OpenStack pueda conectarse a Citrix ADM durante las configuraciones de LB.

Una vez registrados OpenStack y Citrix ADM, ambos pueden comunicarse entre sí. Además, los usuarios de OpenStack pueden usar sus credenciales existentes en OpenStack para iniciar sesión en la interfaz de usuario de Citrix ADM y comprobar el rendimiento de sus configuraciones de LB en los ADC de Citrix.

Arrendatarios en OpenStack

En OpenStack, un arrendatario también se denomina proyecto. Un arrendatario es un grupo de usuarios; un arrendatario o un proyecto también se pueden definir como un conjunto de recursos (procesamiento, red, almacenamiento, etc.) asignados a un grupo aislado de usuarios.

Directivas de colocación

Las políticas de ubicación brindan la flexibilidad de decidir qué instancia de Citrix ADC se usa en cada configuración de balanceador de carga creada por los usuarios. Como alternativa, Citrix ADM también ofrece la opción de asignar una instancia de Citrix ADC en función de los inquilinos de OpenStack.

Paquetes de servicios

Los paquetes de servicios son paquetes que combinan directivas y SLA, especificaciones de configuración de dispositivos o aprovisionamiento automático y directivas de arrendatarios y ubicación. Un

paquete de servicios generalmente se define en términos de las directivas de aislamiento que se proporcionan al arrendatario.

Los siguientes son algunos puntos relacionados con los paquetes de servicios:

- Un arrendatario no puede formar parte de más de un paquete de servicios.
- Se pueden asociar varios arrendatarios al mismo paquete de servicios.
- En un paquete de servicios configurado para el aprovisionamiento automático, las instancias de NetScaler ADC virtuales se pueden crear desde un solo tipo de plataforma (en la plataforma SDX o en la plataforma OpenStack Compute).

Funciones compatibles con LBaaS V1 y LBaaS V2

Mientras que el controlador LBaaS V1 en OpenStack admite operaciones desde la interfaz de usuario de OpenStack Horizon, el controlador LBaaS V2 solo admite operaciones de línea de comandos.

La siguiente lista muestra las funciones compatibles con LBaaS V1 y LBaaS V2 en OpenStack:

- LBaaS V1
  - Equilibrio de carga
- LBaaS V2
  - Equilibrio de carga
  - Descarga SSL con certificados gestionados por Barbican, el administrador de claves en OpenStack
  - Paquetes de certificados (incluye a las autoridades de certificación intermediarias)
  - Soporte SNI

Este documento proporciona información sobre:

- Escenario de caso de uso
- Integración de Citrix ADM con OpenStack Workflow
- Prerequisites
- Tareas previas a la configuración en Citrix ADM y OpenStack
- Pasos de configuración de LBaaS V1 con Horizon
- Pasos de configuración para LBaaS V2 mediante línea de comandos
- Aprovisionamiento manual de la instancia de Citrix ADC VPX en OpenStack
- Integración de Citrix ADM con OpenStack Heat Services
- Supervisión de aplicaciones OpenStack en NetScaler ADM

Escenario de caso de uso

El siguiente caso de caso de uso explica el flujo de trabajo de interconexión de NetScaler ADM con la plataforma OpenStack:

Una empresa, Example-Cloud-Provider, ha utilizado componentes de OpenStack para configurar una nube a fin de proporcionar infraestructura a sus arrendatarios. Steve es el administrador de este proveedor de nube, mientras que Tom es arrendatario de la infraestructura en la nube del proveedor de nube de Example-Cloud-Provider. La organización de Tom, Example-Sportsonline.com, requiere dos servidores S1 y S1, y Tom también requiere un dispositivo NetScaler ADC dedicado para equilibrar la carga entre los servidores S1 y S2 en la plataforma OpenStack.

Para cumplir este requisito, Steve tiene que instalar y configurar OpenStack y Citrix ADM, y prepararlos para que funcionen entre sí. Steve tiene que crear una cuenta de arrendatario llamada Example-SportsOnline en OpenStack y, a continuación, asignar recursos a la cuenta de arrendatario. Steve también tiene que crear diferentes credenciales de inicio de sesión (usuarios) para, por ejemplo, SportsOnline, a fin de gestionar sus recursos y su configuración. Tom ahora puede crear los dos servidores S1 y S2 en OpenStack para gestionar el tráfico de su organización.

Steve tiene que registrar los detalles de OpenStack en Citrix ADM y configurar el controlador Citrix ADC LBaaS en el componente de red de OpenStack, Neutron. Una vez completado el registro, Citrix ADM muestra los detalles de todos los inquilinos de OpenStack. Steve puede seleccionar Example-SportsOnline de la lista si quiere las funciones LBaaS de Citrix ADC y configurar a Tom para que le asignen un Citrix ADC dedicado para sus configuraciones de balanceador de carga en Citrix ADM.

Para ello, Steve puede aprovisionar una instancia de Citrix ADC VPX en la capa informática (Nova) de OpenStack mediante la interfaz de usuario de Citrix ADM o permitir que MAS aprovisione automáticamente una instancia de Citrix ADC VPX a petición, cuando Tom realiza su configuración de LB en OpenStack. En cualquier caso, Citrix ADM administra la instancia VPX. Para lograrlo, Steve crea un paquete de servicios en Citrix ADM y define las condiciones del paquete de servicios que se acordaron en el SLA con Tom. Por ejemplo, Steve selecciona la directiva de aislamiento "dedicada"para proporcionar una instancia dedicada a proporcionar a Tom las configuraciones del balanceador de carga. Es decir, Steve selecciona una instancia no compartida para Tom en el paquete de servicios. A continuación, asigna muchas instancias de Citrix ADC VPX al paquete de servicios y asocia Example-SportsOnline, junto con otros inquilinos, que necesitan un Citrix ADC dedicado al paquete de servicios. Como resultado, cuando Tom realiza su primera configuración de balanceador de carga, Citrix ADM asigna una de las instancias de Citrix ADC VPX del paquete de servicios a Example-SportsOnline y también implementa su configuración en ese Citrix ADC.

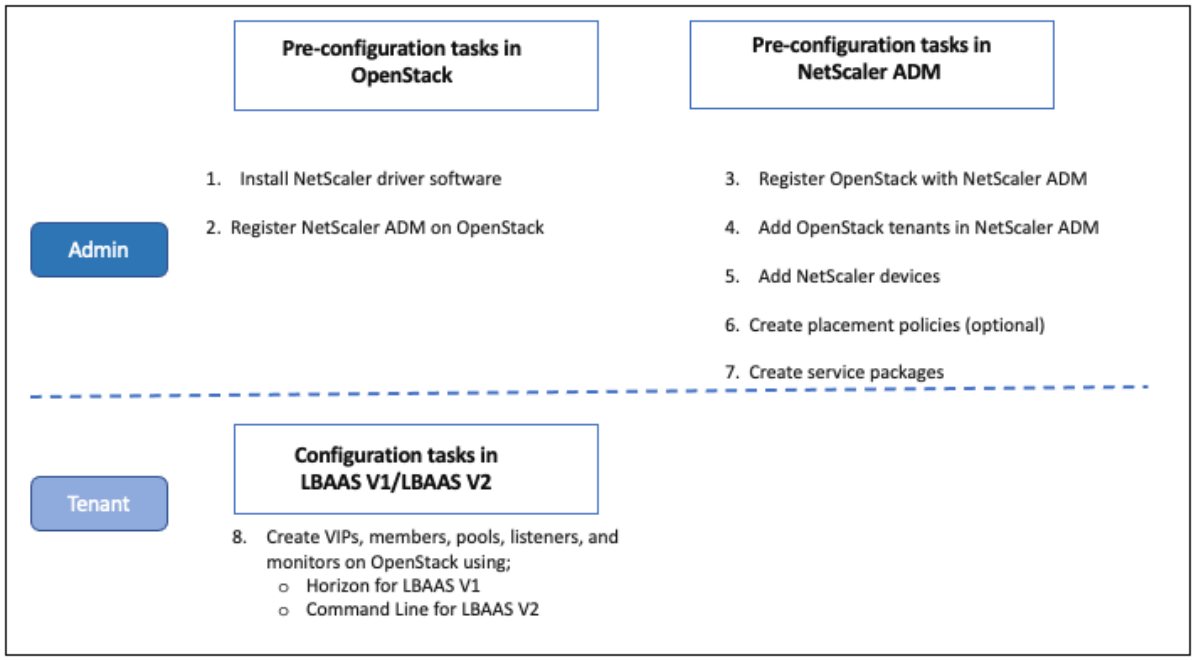
Tom ahora puede crear configuraciones de equilibrio de carga mediante la creación de grupos, IP virtuales (VIP) y monitores de salud mediante OpenStack LBaaS/UI. Los grupos y los VIP de OpenStack se implementan como grupos de servicios y servidores virtuales en la instancia de Citrix ADC. Tom también puede crear monitores de estado para supervisar los servidores y enviar el tráfico de apli-

caciones solo a aquellos servidores que estén activos en cualquier momento y a los que se pueda acceder desde Citrix ADC.

La configuración de equilibrio de carga creada en OpenStack ahora está implementada en la instancia de Citrix ADC. Una vez configurada completamente, la instancia de NetScaler ADC VPX se hace cargo de la funcionalidad de equilibrio de carga y comienza a aceptar tráfico de aplicaciones y equilibra la carga el tráfico entre los servidores S1 y S2 creados por Tom.

Integración de Citrix ADM con el flujo de trabajo de OpenStack

El siguiente diagrama de flujo muestra el flujo de trabajo que debe seguir al configurar LBaaS V1 y LBaaS V2.



Requisitos previos

January 30, 2024

Antes de integrar la instancia virtual de Citrix ADC con la plataforma OpenStack, asegúrese de que se cumplen los siguientes requisitos:

Requisitos de software de NetScaler ADM y OpenStack

- Citrix ADM 12.1 está instalado en una estación de trabajo de hipervisor compatible que cumple con los requisitos mínimos del sistema de hardware.
- Los componentes de OpenStack están instalados y en ejecución.
- Citrix ADM 12.1 admite las siguientes versiones de OpenStack: Newton, Ocata y Pike.

Requisitos de hardware de NetScaler ADM

En la siguiente tabla se enumeran los recursos informáticos virtuales que debe tener en el servidor OpenStack para instalar instancias virtuales de Citrix ADC.

Componente	Requisito
RAM	8 GB
CPU virtual	8
Espacio de almacenamiento	500 GB
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps

> **Nota**
>
> Los requisitos de memoria y disco duro especificados anteriormente son para implementar Citrix ADM en la plataforma OpenStack, teniendo en cuenta que no hay otras máquinas virtuales ejecutándose en el host. Los requisitos de hardware para OpenStack dependen del número de máquinas virtuales que se ejecutan en él.

Tareas previas a la configuración en NetScaler ADM y OpenStack

January 30, 2024

Esta sección le ayuda a realizar las tareas previas a la configuración antes de configurar Citrix Application Delivery Management (ADM) y OpenStack.

Instalación de Citrix ADM

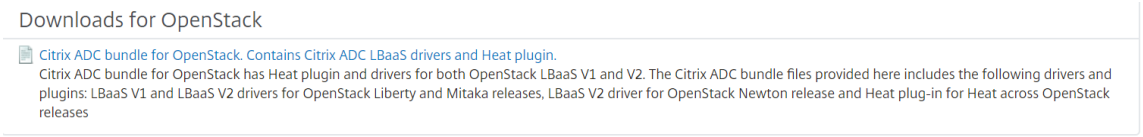
Instale NetScaler ADM en un Hypervisor compatible. Para obtener más información sobre cómo descargar e instalar NetScaler ADM, consulte Implementación de NetScaler ADM.

Instalación del software del controlador NetScaler ADC y registro de NetScaler ADM en OpenStack

Descargue el paquete Citrix ADC para OpenStack desde la página de descargas de Citrix ADM.

Para instalar el controlador Citrix ADC en la plataforma OpenStack mediante la GUI de Citrix ADM:

1. En Citrix ADM, haga clic en **Descargas**. La página de **descargas** de Citrix ADM proporciona enlaces para descargar el **paquete Citrix ADC para el software OpenStack** necesario para las versiones de OpenStack de Newton, Ocata y Pike.
2. Descargue el archivo tar del paquete Citrix ADC más reciente en un directorio temporal (por ejemplo, /tmp) de OpenStack Controller. Este paquete incluye el controlador LBaaS V2 y el plug-in Heat para todas las versiones de OpenStack.



3. Ejecute el siguiente comando para extraer los archivos del archivo tar del controlador NetScaler ADC:
   `tar -xvzf <name_of_tar_file>`
4. Si tiene un OpenStack <Release Name> setup, en el indicador, escriba el siguiente comando:

   `cd <Release Name>`

   Ejemplo:

   `cd Newton`
5. Ejecute el siguiente comando para instalar el controlador y especificar la dirección IP de Citrix ADM, la contraseña del controlador Citrix ADC que configuró al registrar OpenStack en Citrix ADM y el protocolo:

   `./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>`

   Ejemplo de configuración de OpenStack de nodo único:


```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --
neutron-lbaas-path=/opt/stack/neutron-lbaas
```

Ejemplo de configuración multinodo de OpenStack:

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --
neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

> **Nota**
>
> Proporcionar la ruta del directorio neutron-lbaas del sistema es opcional. Proporcionar la ruta puede ayudar al script a encontrar los controladores.
>
> Una vez que Citrix ADM se haya registrado correctamente en OpenStack, también puede iniciar sesión en Citrix ADM con sus credenciales de usuario de OpenStack.
>
> Una vez que Citrix ADM se haya registrado correctamente en OpenStack, reinicie los servicios Neutron de OpenStack.

Registro de OpenStack con Citrix ADM

Para registrar OpenStack en Citrix ADM mediante la GUI de Citrix ADM:

1. En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** .
2. Haga clic en **Configurar los ajustes de OpenStack.**
3. En la página **Configurar opciones de OpenStack** , puede establecer los parámetros para configurar OpenStack en Citrix ADM. Aquí tiene dos opciones: Predeterminado y Personalizado.

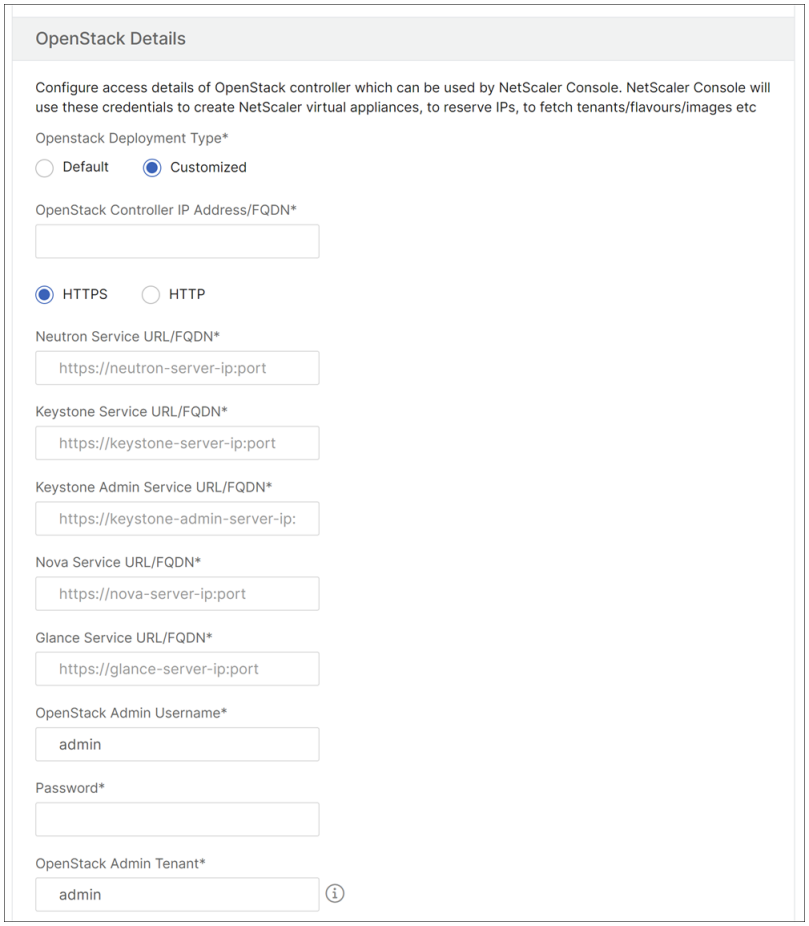
   Para las versiones de OpenStack de Newton y Ocata, puede usar el tipo de implementación predeterminado o personalizado. Sin embargo, para la versión de Pike, debe usar un tipo de implementación personalizado para registrar OpenStack en Citrix ADM.

- **Tipo de implementación predeterminado**

  Seleccione**Predeterminado**si los servicios de OpenStack se ejecutan en los puertos predeterminados. Por ejemplo, el portal predeterminado para los servicios de Neutron es 9696 y el portal predeterminado para los servicios de Keystone es 5000.

1. Dirección IP de OpenStack Controller: dirección IP del controlador OpenStack (tanto el servicio KeyStone como el servicio Neutron deben estar disponibles en esta dirección IP). Por ejemplo, introduzca la dirección IP 10.102.205.23.
2. Nombre de usuario de administrador de OpenStack: nombre de usuario administrativo del controlador OpenStack. Por ejemplo, escriba admin1.
3. Contraseña: contraseña del usuario administrativo del controlador OpenStack.

4. OpenStack Admin Tenant: el nombre del arrendatario administrativo de OpenStack. Por ejemplo, introduzca admin.

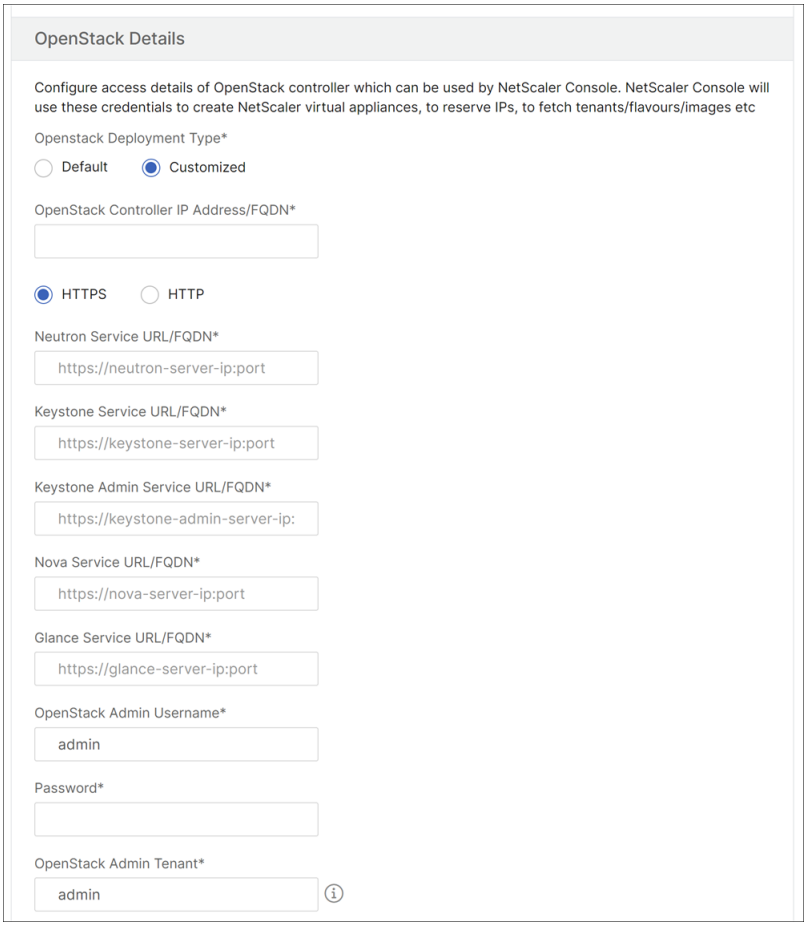


- **Tipo de implementación personalizado**

  Seleccione el tipo de implementación como**Personalizado** si los servicios de OpenStack se ejecutan en puertos distintos de los puertos predeterminados. Si estos servicios se ejecutan en puertos diferentes, especifíquelos aquí. El registro de las versiones de OpenStack Newton y Ocata en NetScaler ADM es diferente del registro de la versión de OpenStack Pike.

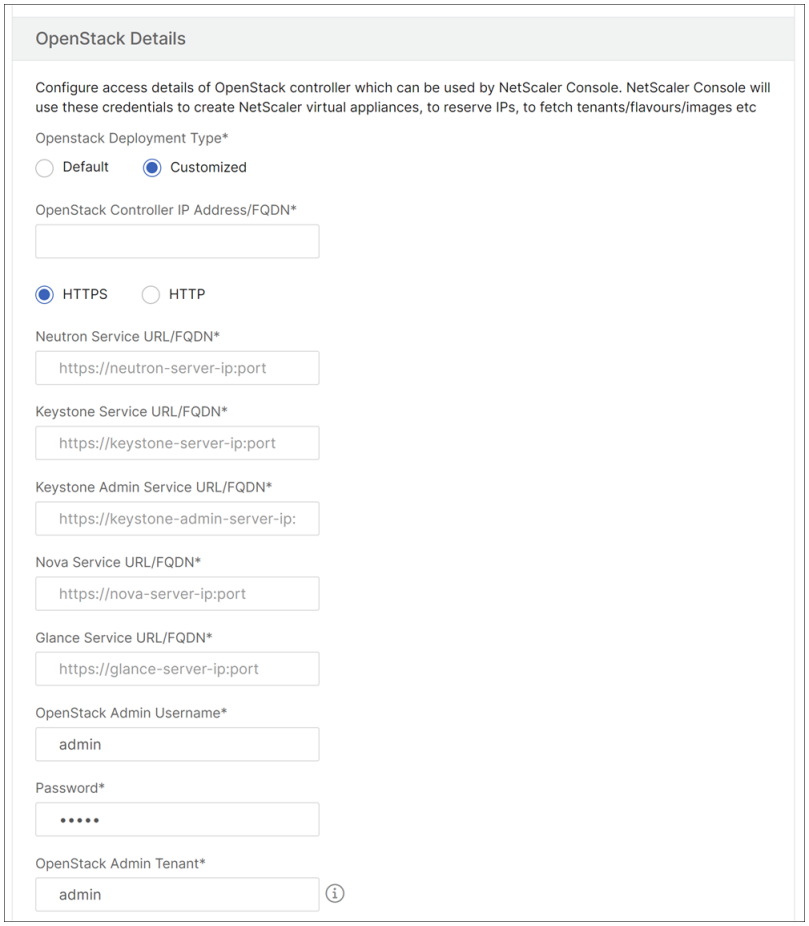
  Lanzamiento de OpenStack por Newton y Ocata:

  1. Especifique los números de puerto para los diversos servicios de OpenStack si está registrando la versión Newton de OpenStack.
  2. Especifique el nombre de usuario, la contraseña y el nombre de usuario del administrador de OpenStack como especificó anteriormente en la **configuración**predeterminada .

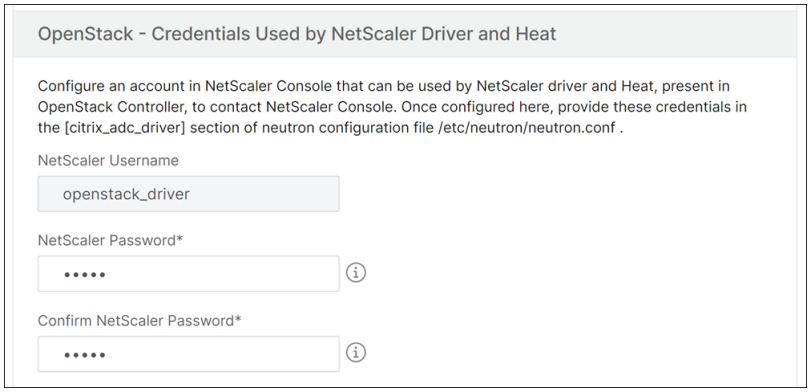


Lanzamiento de Pike de OpenStack:

Si está registrando la versión Pike de OpenStack introduzca los detalles de los servicios de OpenStack como se muestra en la siguiente imagen. También debe especificar el nombre de usuario, la contraseña y el nombre de usuario del administrador de OpenStack como en la configuración predeterminada.



1. En la sección**OpenStack Neutron LBaaS: Credentials Used by NetScaler ADC Driver**, establezca la contraseña del controlador NetScaler ADC para la cuenta de usuario del controlador ADC de OpenStack Citrix. NetScaler ADM autentica las llamadas desde el controlador OpenStack NetScaler ADC mediante estas credenciales. Debe especificar la misma contraseña al ejecutar el script de instalación del controlador Citrix ADC en el controlador OpenStack.



2. Haga clic en **Aceptar**.

Crear un arrendatario en OpenStack

Cree un proyecto o un arrendatario en OpenStack, añada usuarios al proyecto o arrendatario y asigne funciones a todos los usuarios. KeyStone, el servicio de identidad de OpenStack, proporciona servicios de autenticación para cada servicio OpenStack. El servicio de autenticación utiliza una combinación de dominios, proyectos (arrendatarios), usuarios y roles.

Para obtener más información sobre cómo crear un proyecto y realizar otras tareas en OpenStack, consulte la documentación de OpenStack en.http://docs.openstack.org/

Agregar arrendatarios de OpenStack

1. En Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > OpenStack > **OpenStackTenants**y, a continuación, haga clic en**Agregar**.
2. En la página **Agregar arrendatarios de OpenStack**, haga clic en **+Agregar y, a**continuación, seleccione el arrendatario de OpenStack.
3. Haga clic en **Aceptar**.

En función de si está utilizando una instancia preaprovisionada o aprovisionando automáticamente la instancia al integrar OpenStack, siga una de estas dos tareas:

- Preaprovisione los dispositivos NetScaler ADC
- Aprovisione automáticamente los dispositivos Net Scaler VP X en OpenStack

Aprovisionamiento de dispositivos NetScaler ADC

En función de si está utilizando una instancia preaprovisionada o aprovisionando automáticamente la instancia al integrar OpenStack, siga una de estas dos tareas:

- Preaprovisione los dispositivos NetScaler ADC
- Aprovisione automáticamente los dispositivos Net Scaler VP X en OpenStack

Aprovisionamiento previo de dispositivos NetScaler ADC

Instale el dispositivo Citrix ADC en cualquiera de las plataformas de hipervisores, como Citrix Hypervisor, KVM o ESX, y agregue la instancia a Citrix ADM. A continuación, NetScaler ADM administra este dispositivo que equilibra la carga el tráfico en los servidores.

Para agregar una instancia de Citrix ADC VPX existente en Citrix ADM:

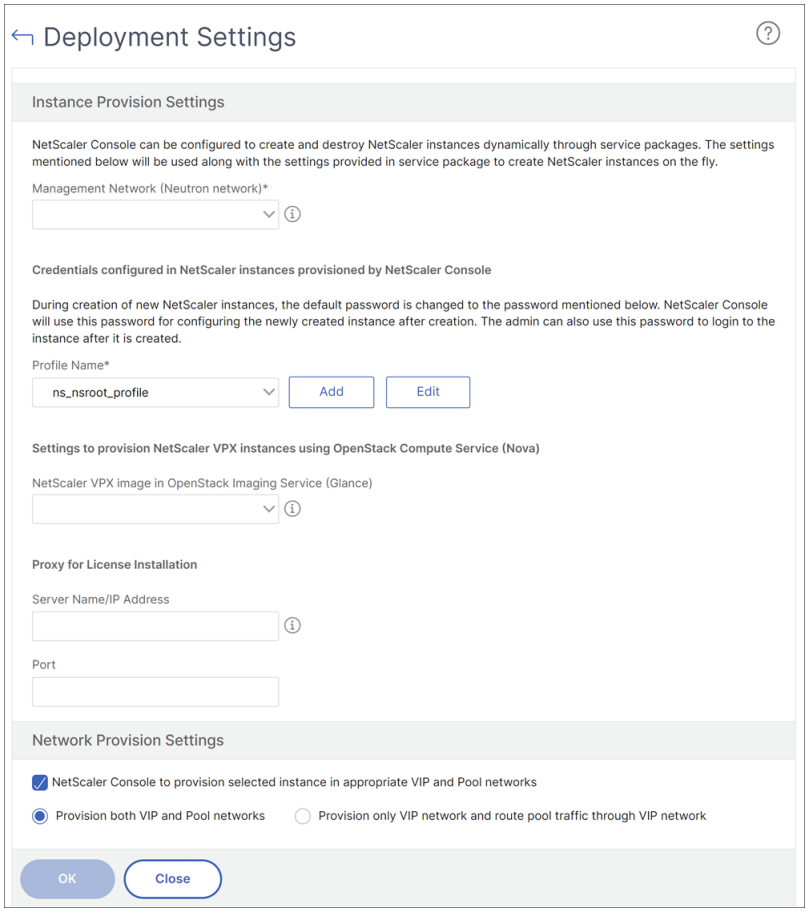
1. En Citrix ADM, vaya a **Infraestructura** > **Instancias** > **Citrix ADC VPX** y, a continuación, haga clic en **Agregar**.
2. En la página **Agregar Citrix ADC VPX** , especifique la dirección IP de la instancia de Citrix ADC VPX y seleccione un perfil de instancia en la lista de **nombres de perfil**. El perfil de instancia contiene las credenciales utilizadas para iniciar sesión en Citrix ADC VPX. También puede crear un nuevo perfil de instancia haciendo clic en el icono +. Haga clic en **Aceptar**.

Aprovisionamiento automático de dispositivos Citrix ADC

Descargue la imagen de instancia de Citrix ADC requerida de la página de descargas de Citrix y cárguela en Glance, el servicio de imágenes de OpenStack. Tener una imagen disponible en Glance le permite configurar una instancia de Citrix ADC bajo demanda al asignar la instancia al inquilino.

Para aprovisionar automáticamente los dispositivos Citrix ADC VPX en OpenStack:

1. En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack**.
2. Haga clic en**Configuración de implementación**.
3. Defina los siguientes parámetros:
    a) Red de administración: seleccione la red de administración en OpenStack a la que está conectado el Citrix ADC VPX de aprovisionamiento automático.
    b) Nombre del perfil: seleccione el perfil en la lista desplegable. NetScaler ADM utiliza la contraseña contenida en este perfil para configurar nuevas instancias de NetScaler ADC VPX aprovisionadas automáticamente.
    c) Licencias: proporcionan los códigos de activación de licencias (LAC) de Citrix ADM que se utilizan para licenciar nuevas instancias de Citrix ADC aprovisionadas automáticamente. NetScaler ADM aprovisiona instancias NetScaler ADC en el proceso OpenStack en la red de administración y, a continuación, desencadena la instalación de licencias en ellas mediante el código de licencia especificado. A continuación, la instancia de Citrix ADC descarga los archivos de licencia del sitio web de Citrix mediante el LAC especificado aquí.
    d) Imagen de NetScaler ADC VPX en un vistazo: Seleccione la imagen de NetScaler ADC VPX disponible en OpenStack Glance que se utiliza para crear una instancia de NetScaler ADC VPX.
    e) Configuración de proxy: proporcione detalles del servidor proxy Citrix ADC para instalar licencias. Esto puede ser necesario cuando Citrix ADC no tiene acceso directo a Internet a través de la red de administración.
4. Haga clic en **Aceptar**.



Creación de un paquete de servicios en NetScaler ADM

Para crear paquetes de servicios para un inquilino en Citrix ADM:

1. En Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > **OpenStack** > **Service Packages** y, a continuación, haga clic en **Agregar**.
2. En la página **del paquete de servicios**, especifique los siguientes parámetros:
   a) Nombre: Nombre para el paquete de servicios. Por ejemplo, escriba SVC-PKG-GOLD.
   b) Asignación de instancias de Citrix ADC: el tipo de asignación de instancias definido en el paquete de servicios en función del cual los recursos de instancias de Citrix ADC se asignan a un inquilino. Seleccione **Dedicado**. Para obtener más información sobre las directivas, consulte Directivas de aislamiento de paquetes de servicios.
   c) Aprovisionamiento de instancias de NetScaler ADC: Seleccione **Instancia existente**para asignar una instancia de NetScaler ADC existente a un arrendatario. Si quiere crear instancias de Citrix ADC durante la propia configuración, seleccione **Crear instancia bajo demanda**.

d) Tipo de instancia de Citrix ADC: seleccione **Citrix ADC VPX** .

> **Nota**
>
> Seleccione Citrix ADC VPX para asignar instancias Citrix ADC previamente aprovisionadas alojadas en la plataforma SDX.

3. Haga clic en **Continuar** para asociar a un arrendatario a un paquete de servicios.

> **Nota**
>
> Habilite el **aprovisionamiento de un par de instancias de Citrix ADC para una alta disponibilidad** , si está implementando las instancias de Citrix ADC en modo de alta disponibilidad.

4. En la sección **Asignar instancias** , haga clic en **Agregar** y, a continuación, seleccione la instancia de Citrix ADC que quiere asignar al inquilino y haga clic en **Continuar** .
5. En la sección **Asignar arrendatarios y directivas de ubicación de OpenStack**, en **OpenStack Arrendatarios, haga clic en**Agregar**y seleccione el arrendatario**.
6. Haga clic en **Continue** y, a continuación, en **Done**.

> **Nota**
>
> Si no se encuentra la directiva, se reviva el mecanismo de reserva y NetScaler ADM asigna instancias de NetScaler ADC basadas en arrendatarios. Si el arrendatario no forma parte de ningún paquete de servicios, NetScaler ADM muestra un mensaje de error que dice: “Tenant\ <admin\ > no forma parte de ningún paquete de servicios y no hay un paquete de servicios predeterminado. “

Creación de directivas de ubicación (opcional)

Las directivas de aislamiento no se basan únicamente en los arrendatarios. Puede crear directivas de ubicación flexibles, en las que las directivas no solo se basen en el nombre o la identificación del arrendatario, sino también en otros atributos personalizados.

Para crear políticas de colocación para un inquilino en Citrix ADM:

1. En Citrix ADM, vaya a Orchestration > **CloudOrchestration**>**OpenStack**>**Política de ubicación**y, a continuación, haga clic en**Agregar**.
2. En la página **Agregar directiva de ubicación**, defina los siguientes parámetros:

   a) Nombre: escriba un nombre para la directiva de colocación

b) Expresiones de ejemplo: seleccione una expresión de ejemplo de la lista. Estos ejemplos son útiles para construir la directiva de colocación.

c) Expresión: en este campo se rellena una expresión booleana en función de la expresión de muestra que ha seleccionado en el campo anterior. Modifique los nombres de los campos según sea necesario.

3. Haga clic en **Aceptar**.

Habilitar el tráfico desde las instancias de Citrix ADC a los servidores back-end a través de la red de clientes

De forma predeterminada, en el flujo de trabajo de orquestación de OpenStack, las instancias NetScaler ADC se vinculan dinámicamente a las redes del equilibrador de carga o cliente y a las redes de miembros o servidores.

En ciertas implementaciones, también se puede acceder a los servidores a través de las redes de clientes y se pueden enrutar a través de la puerta de enlace del cliente. En estos casos, las instancias de Citrix ADC no necesitan estar enlazadas a redes de servidores, sino que solo deben estar enlazadas a redes de clientes.

Realice la siguiente configuración para configurar el tráfico a través de la puerta de enlace del cliente.

Vaya a **Orquestación > Orquestación** en la **nube** > **OpenStack** > **Configuración de implementación**y, a continuación, seleccione la opción **Aprovisionar solo redes VIP y enrutar el tráfico del grupo a través de la red VIP**.

A continuación, Citrix ADM configura la instancia de Citrix ADC para las redes de los clientes añadiendo un SNIP en esa red y, además, añadirá una ruta predeterminada a la puerta de enlace de la red del cliente. Esto permite que la instancia llegue a los servidores a través de la puerta de enlace del cliente.

Aprovisionamiento automático de dispositivos Citrix ADC VPX implementados en la plataforma Citrix ADC SDX

Agregue la plataforma Citrix ADC SDX a Citrix ADM para que Citrix ADM aprovisione las instancias de esta plataforma bajo demanda.

Para proporcionar automáticamente instancias de NetScaler ADC implementadas en la plataforma NetScaler ADC SDX:

1. En la GUI de Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix ADC SDX** y haga clic en **Agregar** para agregar una plataforma Citrix ADC SDX.

2. Vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Configuración de implementación.**
3. En la sección **Red** de administración , seleccione la red de administración de OpenStack a la que está conectado el Citrix ADC SDX de aprovisionamiento automático.
    a) En**Nombre de perfil**, seleccione el perfil en la lista desplegable. NetScaler ADM utiliza la contraseña contenida en este perfil para configurar nuevas instancias de NetScaler ADC VPX aprovisionadas automáticamente.
    b) Haga clic en **Aceptar**.
4. Para aprovisionar la plataforma Citrix ADC SDX en OpenStack, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Package** .
    a) Haga clic en**Agregar** para crear un nuevo paquete de servicios.
    b) Introduzca el nombre del paquete de servicios.
    c) En el campo **Asignación de instancias de Citrix ADC** , seleccione **Dedicado** .
    d) En el campo **Citrix ADC Instance Provisioning** , seleccione **Create Instance OnDemand** y, en el campo **Auto Provision Platform** , seleccione **Citrix ADC SDX**.
    e) De forma predeterminada, solo las instancias de Citrix ADC VPX se aprovisionan en la plataforma Citrix ADC SDX.
    f) Haga clic en **Continuar**.
    g) En la sección**Configuración de aprovisionamiento automático**, defina las propiedades de**los recursos**.
        i. Campo**de rendimiento**. Introduzca 1000 Mbps.
        ii. Campo**Versión de NetScaler ADC**. En la lista, seleccione la versión correcta de la imagen de NetScaler ADC VPX presente en la plataforma NetScaler ADC SDX.Configurar LBaaS V2 mediante la línea de comandos
    h) En la sección**NetScaler ADC SDX Platforms**, haga clic en**Agregar** para agregar la plataforma SDX al paquete de servicios.
    i) Haga clic en **Continuar**.
    j) En la sección**Configurar arrendatarios de OpenStack**, haga clic en**Agregar** para agregar los arrendatarios. También puede agregar nuevos arrendatarios haciendo clic en**Nuevo**.
    k) Haga clic en **Done**.
5. Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron. Conéctese a cualquier cliente de Neutron y ejecute las tareas de configuración. Para obtener

más información sobre cómo ejecutar los comandos de configuración, consulte Configuración de LBaaS V2 mediante la línea de comandos.

Configurar LBaaS V1 mediante Horizon

January 30, 2024

Tom ahora puede iniciar sesión en el portal OpenStack Horizon, crear un grupo de LBaaS y seleccionar una subred en la que se encuentren todos los miembros de este grupo. Tom tiene que agregar una dirección IP virtual (VIP) y asignar esta VIP al grupo que ha creado. Tom también puede realizar esto en la línea de comandos o mediante APIs. Los clientes externos de los servidores de Tom pueden conectarse a esta dirección VIP, que está alojada en el Citrix ADC asignado, y Citrix ADC distribuye todas las solicitudes a los miembros del grupo en los puertos configurados.

Los miembros del grupo LBaaS son los servidores con equilibrio de carga que se agregan al grupo seleccionado. Tom puede asignar un peso y un puerto a cada uno de estos miembros.

Los monitores de salud se utilizan para vigilar la salud y el buen funcionamiento de todos los miembros de la agrupación. Tom puede crear una plantilla de supervisión del estado en OpenStack especificando los límites de retraso, tiempo de espera y reintentos, y también especificar el método, la ruta de URL y los códigos HTTP esperados en caso de éxito. Después de crear un monitor, Tom tiene que asociar el monitor con el grupo que se creó previamente.

Para obtener más información sobre cómo crear grupos y otras tareas de configuración de LBaaS en OpenStack, consulte la documentación de OpenStack.

> **Importante**
>
> LBaaS V1 no es compatible con la versión Liberty de OpenStack. Para obtener más información, consulte Notas de la versión de OpenStack.

Configurar LBaaS V2 mediante la línea de comandos

January 30, 2024

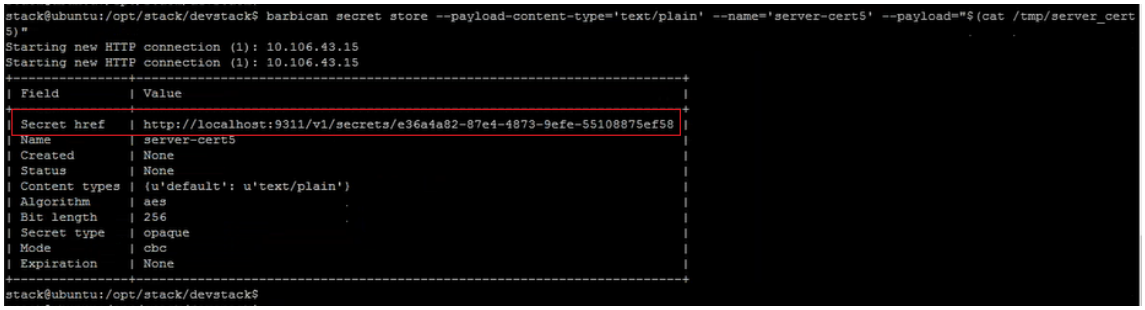
LBaaS V2 admite la descarga SSL con certificados administrados por Barbican, paquetes de certificados (incluye Autoridades de certificación intermediarias), compatibilidad con SNI junto con las funciones regulares de equilibrio de carga. LBaaS V2 solo admite la interfaz de línea de comandos para ejecutar las tareas de configuración. Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron.

> **Nota**
>
> Cargue el certificado y la clave al servicio Barbican cuando necesite la función de descarga SSL. Realice los pasos 1, 2 y 3 si se admite la descarga SSL; de lo contrario, continúe desde el paso 4 para crear un equilibrador de carga, un agente de escucha, un grupo y un miembro.

1. Cargue el certificado al servicio Barbican mediante el siguiente comando:

   <content_type><certificate_name>barbican secret store –payload-content-type –name –payload <certificate_location>

   Ejemplo: barbican secret store –payload-content-type=’text/plain’–name=’hp_server_certificate’–payload=» hp_server/tmp/server_certificate»



2. Cargue la clave en el servicio Barbican mediante el siguiente comando:

   <content_type><key_name>barbican secret store –payload-content-type –name –payload <key_location>

   Ejemplo: barbican secret store –payload-content-type=’text/plain’–name=’shp_server_key’–payload=”hp-server/tmp/server_key»

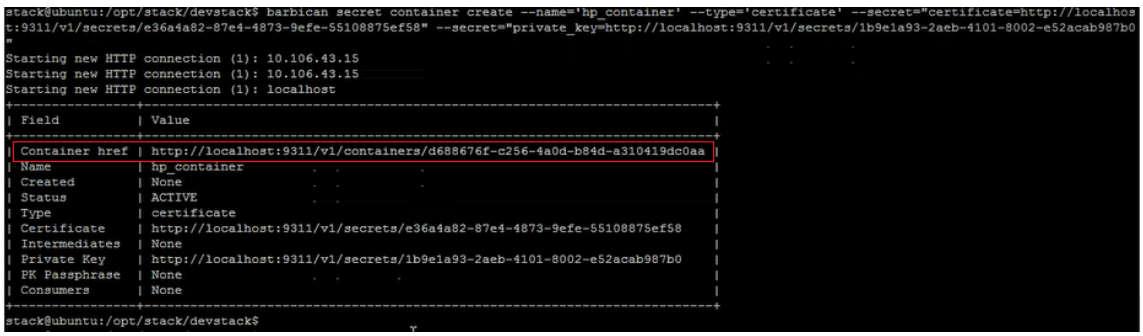
> **Nota**
>
> Al ejecutar estos dos comandos de Barbican para cargar el certificado y la clave, los campos href secretos proporcionan una ubicación o URL. Aquí es donde el certificado y la clave se almacenan en el sistema donde está instalado OpenStack. Copie estos vínculos y proporcione estos enlaces como parámetros cuando cree el contenedor en el servicio Barbican en el paso 3.

3. Cree un contenedor en el servicio Barbican para almacenar el certificado y la clave mediante el siguiente comando:

   En el comando, <certificate_url>sustitúyalo por la URL que obtuvo del campo Href secreto cuando cargó el certificado. Del mismo modo, <key_url>sustitúyala por la URL que obtuviste en el campo Href secreto cuando subiste la clave.

   <container_type><certificate_url>contenedor secreto barbican create –name –type –secret <container_name>–secret <key_url>

   Ejemplo: barbican secret container create –name='hp_container' –type='certificate' –secret=" "certificate=http://localhost:9311/v1/secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb-4101-8002-e52acab987b0



   Copie el valor href del contenedor. Debe proporcionar el enlace al contenedor al crear el oyente en el paso 6.

4. Configure las variables de entorno en OpenStack. Las variables permiten que los comandos del cliente de OpenStack se comuniquen con los servicios de OpenStack.

   Ejemplo:

   export OS_PASSWORD-hp

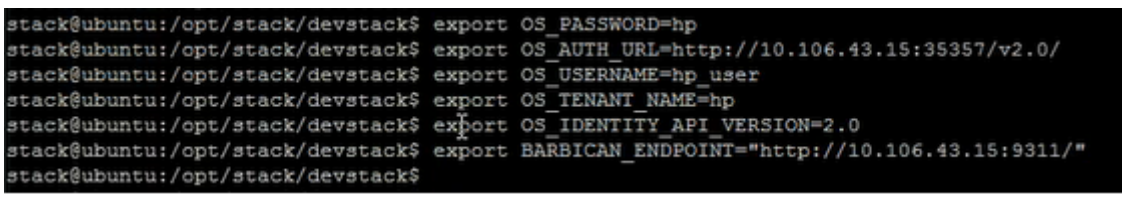
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

   export OS_IDENTITY_API_VERSION=2.0

   export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"



> **Nota**
>
> Establezca estas variables para cada sesión SSH antes de ejecutar otros comandos. Para obtener más información sobre las variables de entorno OpenStack, consulte Variables de entorno OpenStack.

5. Cree un equilibrador de carga con el siguiente comando:

   <loadbalancer-name\ > <subnet-name\ >neutron labas-loadbalancer-create –name\\ –provider\ <netscaler\ >

   Ejemplo: neutron lbaas-loadbalancer-create –name hp-lb-test hp-sub1 –provider netscaler

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| admin_state_up      | True                                 |
| description         |                                      |
| id                  | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners           |                                      |
| name                | hp-lb-test                           |
| operating_status    | OFFLINE                              |
| provider            | netscaler                            |
| provisioning_status | PENDING_CREATE                       |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f     |
| vip_address         | 15.0.0.27                            |
| vip_port_id         | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id       | 0bb433c4-4b90-4de0-803f-9df92aa16ac4 |
+---------------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

   El estado cambia de PENDING_CREATE a ACTIVE después de crear correctamente el equilibrador de carga.

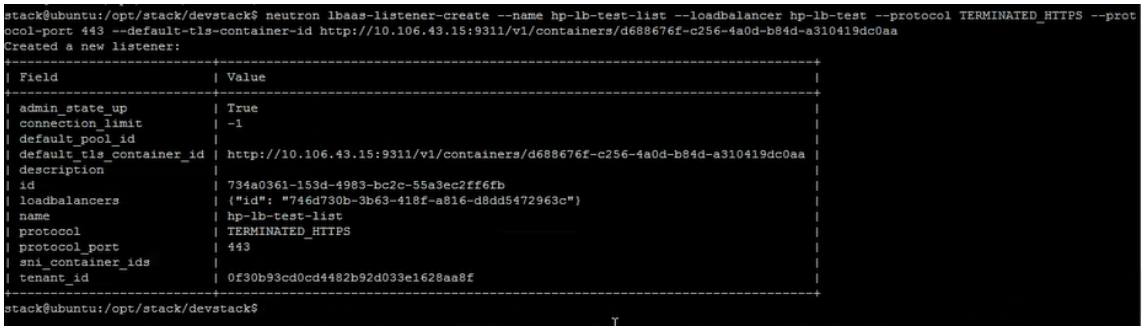
```
+--------------------------------------+------------+-------------+---------------------+-----------+
| id                                   | name       | vip_address | provisioning_status | provider  |
+--------------------------------------+------------+-------------+---------------------+-----------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25   | ACTIVE              | netscaler |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19   | ACTIVE              | netscaler |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24   | ACTIVE              | netscaler |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27   | ACTIVE              | netscaler |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18   | ACTIVE              | netscaler |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23   | ACTIVE              | netscaler |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20   | ERROR               | netscaler |
+--------------------------------------+------------+-------------+---------------------+-----------+
```

6. Cree un oyente con el siguiente comando:

   <loadbalancer-name><listener-name><protocol_type><port_number>neutron labas-listener-create –loadbalancer –name –protocol –protocol-port –default-tls-container-id <container_url>

   Ejemplo: neutron lbaas-listener-create –name hp-lb-test-list –loadbalancer hp-lb-test –protocol TERMINATED_HTTPS –protocol-port 443 –default-tls-container-id `http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`

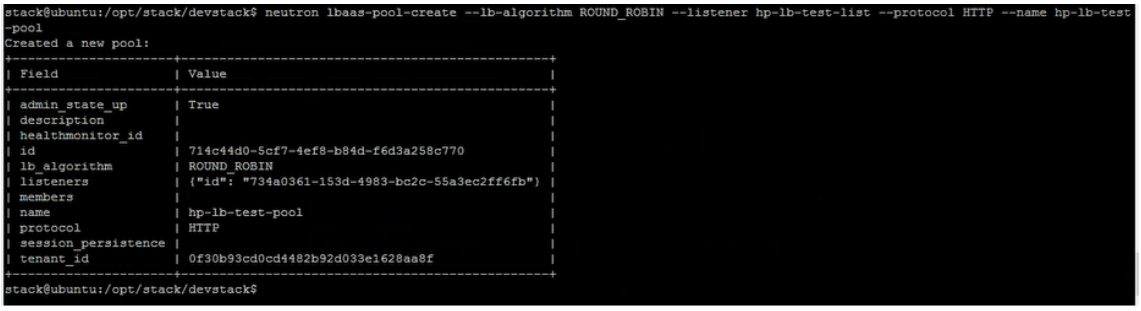
> **Nota**
>
> Si va a crear un agente de escucha sin soporte de descarga SSL, ejecute el siguiente comando sin proporcionar ubicaciones al contenedor:
>
> <loadbalancer-name><listener-name><protocol_type>neutron labas-listener-create –loadbalancer –name –protocol –protocol-port <port_number>



7. Cree un grupo con el siguiente comando:

   <algorithm_type><listener-name><protocol_type>neutron lbaas-pool-create –lb-algorithm –listener –protocol –name <pool-name>

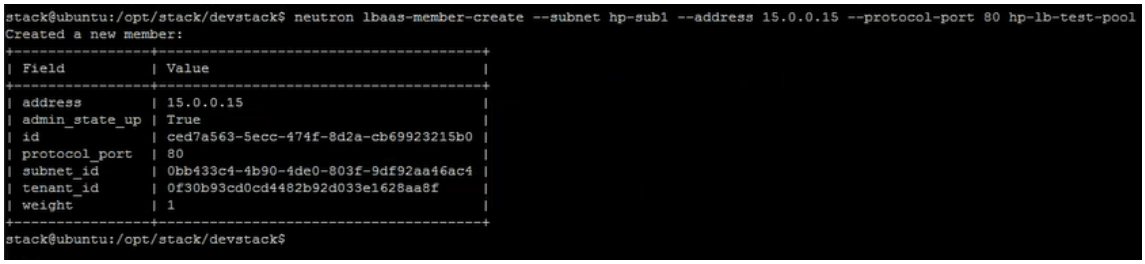
   Ejemplo: neutron lbaas-pool-create –lb-algorithm LEAST_CONNECTIONS –listener demolistener –protocol http –name demopool



8. Cree un miembro con el siguiente comando:

   <subnet-name><ip-address of the web server>neutron labas-member-create –subnet –address –protocol-port <port_number><pool-name>

   Ejemplo: neutron lbaas-member-create –subnet hp-sub1 –address 15.0.0.15 –protocol-port 80 hp-lb-test-pool



Supervisión de aplicaciones OpenStack en NetScaler ADM

Los inquilinos pueden iniciar sesión en Citrix Application Delivery Management (ADM) con sus credenciales de OpenStack para supervisar los VIP y los grupos creados a partir de OpenStack desde cualquier explorador. La URL debe tener el siguiente formato:

http://\<mas_ip\>/\<admin_ui\>/mas/ent/html/cc_tenant_main.html

Dónde <mas-ip-address>está la dirección IP de Citrix ADM que está registrada en OpenStack.

> **Nota**
>
> - Los VIP de OpenStack corresponden a los servidores virtuales de Citrix ADM.
> - Los grupos de OpenStack corresponden a los grupos de servicios de Citrix ADM.
> - Los miembros del grupo de OpenStack corresponden a los miembros del grupo de servicios en NetScaler ADM.

Configurar la conmutación de contenido de capa 7

January 30, 2024

Citrix Application Delivery Management (ADM) se organiza con OpenStack para configurar las funcionalidades de conmutación de capa 7 (L7) o de conmutación basada en contenido en las instancias de Citrix ADC. El cambio de contenido difiere del simple equilibrio de carga en que se pueden dirigir tipos específicos de solicitudes a servidores específicos. Cuando las configuraciones L7 se crean en OpenStack con una instancia de Citrix ADC como proveedor, Citrix ADM asigna una instancia de Citrix ADC e implementa las configuraciones de respuesta y conmutación de contenido correspondientes a las configuraciones L7. A continuación, las instancias de Citrix ADC pueden distribuir y equilibrar la carga de las solicitudes de los usuarios en función de las características de nivel de aplicación de las solicitudes.

La función de equilibrio de carga de capa 7 (L7) de OpenStack combina equilibrio de carga y conmutación de contenido para proporcionar una entrega optimizada de tipos específicos de contenido. Esto mejora el rendimiento del balanceador de cargas al ejecutar solo las políticas que son aplicables al contenido. El equilibrio de carga de la capa 7 también facilita una mayor eficiencia de la infraestructura de la aplicación. La capacidad de separar el contenido según el tipo, URI o datos permite una mejor asignación de recursos físicos en la infraestructura de la aplicación. Por ejemplo, un usuario final que `http://example-sports.com/about-us`navegue debe ser atendido por un grupo de servidores que alojen contenido sobre la empresa y los servicios, mientras que un usuario que navegue `http://example-sports.com/shopping-cart-football`debe ser atendido por un grupo diferente de servidores que permita a los usuarios realizar compras en línea.

En la conmutación de L7, un equilibrador de carga se implementa como un servidor virtual de conmutación de contenido que acepta solicitudes HTTP de los usuarios y las distribuye a los servidores de aplicaciones. La conmutación L7 o el cambio de contenido permiten tener una entrada de un solo punto para acceder a una variedad de servicios de fondo (por ejemplo, no solo las aplicaciones web, los portales de servicios web, los correos web, sino también la administración de dispositivos móviles, el contenido en diferentes idiomas, etc.). Es decir, puede proporcionar una dirección IP pública para todos los servicios que ofrece a sus usuarios.

A diferencia del equilibrio de carga de nivel inferior, la conmutación de capa 7 no requiere que todos los servidores del grupo tengan el mismo contenido. Una configuración de balanceador de carga que utiliza la conmutación L7 espera que los servidores de aplicaciones o back-end de diferentes grupos tengan un contenido diferente. Los conmutadores L7 pueden dirigir solicitudes sobre la base de URI, host, encabezados HTTP o cualquier otra cosa en el mensaje de la aplicación. Los servidores de aplicaciones deben servir esencialmente tipos de contenido específicos. Por ejemplo, un servidor podría servir solo imágenes, otro podría ejecutar lenguajes de secuencias de comandos del lado del servidor, como PHP y ASP, y otro podría servir contenido estático, como HTML, CSS y JavaScript.

Reglas L7

Los siguientes atributos se definen en una regla para evaluar el tráfico y se comparan con los valores definidos en la regla:

- nombre de host: el nombre de host de la solicitud HTTP se compara con el parámetro de valor de la regla. Por ejemplo, “www.example-sports.com”.
- ruta: la parte de ruta del URI HTTP se compara con el parámetro de valor de la regla. Por ejemplo, “www.example-sports.com/shopping-cart/football_pump.html”
- file_type: La última parte del URI se compara con el parámetro value de la regla. Por ejemplo, txt, html, jpg, png, xls y otros.

- header: El encabezado definido en el parámetro clave se compara con el parámetro value en la regla.
- cookie: La cookie nombrada por el parámetro clave se compara con el parámetro de valor de la regla. El valor del campo del encabezado de la solicitud de la cookie contiene un par de información de nombre y valor almacenados para esa URL; la sintaxis general es la siguiente: Cookie: name=value. Por ejemplo, una regla que busca una cookie llamada "almacenes"con el valor que empieza por "football-"se verá así: Type = Cookie, compare_type=StartsWith, key = stores value = football-.

Tipos de comparación

Al evaluar el tráfico, la directiva L7 compara las siguientes expresiones con los atributos definidos en la regla.

- regex: coincidencia de expresiones regulares de tipo Perl
- starts_with: Cadena que comienza con
- ends_with: La cadena termina en
- contiene: La cadena contiene
- equal_to: Cadena es igual a

> **Nota**
>
> Los atributos hostname, path, header y cookie admiten todos los tipos de comparación, pero el atributo file_type solo admite expresiones regulares y equal_to.

Directivas L7

Una directiva L7 procesa el tráfico HTTP entrante y devuelve un valor "verdadero"cuando coinciden todas las reglas definidas en la directiva.

En cualquier directiva L7, todas las reglas se unen de forma lógica con un operador AND. Una solicitud debe cumplir con todas las reglas para que la directiva devuelva un valor "verdadero". La acción que realiza el balanceador de cargas se basa en el valor devuelto por la directiva. Puede crear una segunda directiva con la misma acción para lograr una operación OR lógica entre las reglas.

Por ejemplo, puede crear una directiva en la que la solicitud HTTP entrante pueda contener las palabras "EXAMPLE-SPORTS", "SPORTS-FOOTBALL"o "EXAMPLE-FOOTBALL", de modo que el balanceador de cargas tome las medidas adecuadas de reenviar estas solicitudes al grupo de servidores de la empresa de comercio electrónico de Example-Sports para ofrecer el contenido solicitado. Puede crear otra directiva que realice la misma acción pero que coincida con "ejemplo-deportes"

, "ejemplo-deportes-fútbol"o "ejemplo-fútbol". Cuando un usuario envía una solicitud HTTP con alguna de estas seis palabras clave, el balanceador de carga reenvía la solicitud al servidor Example-Sports.

Según las reglas definidas en la directiva, una directiva L7 puede realizar cualquiera de las siguientes acciones:

- Redirigir al grupo: reenvía la solicitud al grupo de servidores de aplicaciones identificado por las reglas asociadas a la directiva L7. Es decir, puede crear una regla de aplicación para dirigir las solicitudes a un grupo de balanceadores de carga específico según el nombre de dominio. Por ejemplo, puede crear una regla que dirija algunas solicitudes a example-football.com a pool_1 y otras solicitudes a example-sports-online_purchase.com a pool_2.
- Redirigir a URL: envía al cliente una respuesta HTTP de redireccionamiento en la que el encabezado de la respuesta de ubicación contenga la nueva ubicación. El navegador actualizará la barra de direcciones con la nueva ubicación y emitirá una nueva solicitud. Los casos de uso son muchos. Por ejemplo, si la dirección de un sitio web ha cambiado, puede redirigir las solicitudes a la nueva dirección en lugar de eliminarlas. O bien, durante el mantenimiento del sitio web, puede redirigir a los usuarios a un sitio de solo lectura.
- Rechazar: rechaza la solicitud y no realiza ninguna otra acción. Por ejemplo, puede devolver una respuesta 401 no autorizada para denegar el acceso a los usuarios de páginas web restringidas.

Una configuración de conmutación de contenido consiste en un servidor virtual de conmutación de contenido, una configuración de equilibrio de carga que consiste en servidores y servicios virtuales de equilibrio de carga y directivas de conmutación de contenido. Después de crear el servidor virtual y las directivas de conmutación de contenido, enlaza cada directiva al servidor virtual de conmutación de contenido. Al vincular la directiva al servidor virtual de conmutación de contenido, se especifica el servidor virtual de equilibrio de carga de destino. Cuando una solicitud llega al servidor virtual de conmutación de contenido, el servidor virtual aplica las directivas de conmutación de contenido asociadas a esa solicitud. La prioridad de la directiva define el orden en que se evalúan las directivas vinculadas al servidor virtual de conmutación de contenido.

Cualquier grupo que tenga el identificador de escucha se puede asignar como grupo predeterminado de servidores virtuales a los que se desvía el tráfico. El grupo está vinculado vagamente a un oyente y solo se asocia a un oyente mediante la implementación de una directiva L7. También se puede crear un grupo directamente debajo de un balanceador de carga sin estar necesariamente vinculado a un oyente. En tal caso, el grupo se crea en el estado "pending_create". Como las directivas de L7 están estrechamente vinculadas a los oyentes, se debe crear e implementar una directiva de L7 que contenga el ID del grupo para que el grupo se vuelva "activo"y comience a recibir solicitudes de tráfico.

Varias directivas de L7 pueden prestar servicio a un grupo, pero permanece en estado "activo"si tiene

al menos una directiva asociada. Cuando se elimina la última directiva, el grupo vuelve al estado ‘‘pending_create’’hasta que se cree otra directiva y se asocie a ella. Si se elimina el grupo en sí, todas las solicitudes HTTP que de otro modo habría recibido se redirigen al grupo predeterminado.

Asignación entre las políticas L7 de OpenStack y las entidades Citrix ADC

OpenStack	Entidad Citrix ADC	Descripción
Directiva L7 con acción REDIRECT_TO_POOL	Directiva de cambio de contenido > Acción de cambio de contenido	Citrix ADM crea una directiva de conmutación de contenido que está enlazada al servidor virtual de conmutación de contenido y asociada a una acción de conmutación de contenido que especifica el grupo de servidores de aplicaciones de destino para la recuperación y presentación de contenido al usuario.
Directiva L7 con acción REDIRECT_TO_URL	Directiva de respuesta > Acción de respuesta	Citrix ADM crea una directiva de respuesta que está enlazada al servidor virtual de conmutación de contenido y asociada a una acción de respuesta que especifica la URL de destino que se presentará a los usuarios.
Directiva L7 con acción RECHAZAR	Directiva de respuesta > Eliminar la solicitud	Citrix ADM crea una directiva de respuesta que está enlazada al servidor virtual de conmutación de contenido y asociada a una acción de respuesta que descarta la solicitud.

Si la acción de una directiva L7 que se evalúa como «verdadera» redirige el tráfico a un grupo que está en estado «create_pending», Citrix ADM implementa el grupo especificado junto con un servidor virtual de equilibrio de carga. Citrix ADM crea una directiva de conmutación de contenido a partir

de la directiva L7 y utiliza la acción de conmutación de contenido correspondiente para redirigir las solicitudes al servidor virtual de equilibrio de carga asociado a ese grupo. Si una segunda directiva L7 redirige al mismo grupo, Citrix ADM crea una directiva de conmutación de contenido y una acción de conmutación de contenido para redirigir el tráfico al servidor virtual de equilibrio de carga existente asociado al grupo.

Posicionamiento político

La evaluación de las directivas de nivel 7 en OpenStack está determinada por sus prioridades. En OpenStack, de forma predeterminada, a las directivas se les asignan prioridades en el orden en que se crean. La directiva que se creó primero lleva el número "1"y las directivas que se crean posteriormente se numeran consecutivamente. Sin embargo, puede cambiar las prioridades de las directivas y asignarles prioridades diferentes. Las directivas siempre se evalúan en el orden de sus prioridades. La primera política que coincide con una solicitud específica siempre se ejecuta primero.

Al crear directivas, tenga en cuenta los siguientes puntos:

- Si asigna a una nueva directiva la misma prioridad que a una directiva existente, la nueva directiva tendrá esa prioridad. Se reduce la prioridad de la directiva actual. Si es necesario, las prioridades de otras directivas también se reducen para mantener el orden en que se evalúan las directivas.
- Si crea una nueva directiva sin especificar una posición, la nueva directiva simplemente se agregará a la lista.
- Si crea una nueva directiva y le asigna una posición superior a la cantidad de directivas que ya figuran en la lista, la nueva directiva se anexará a la lista, es decir, la nueva directiva siempre tendrá la siguiente prioridad disponible. Por ejemplo, si hay tres directivas A, B y C con prioridades 1, 2 y 3, y si crea una directiva y asigna una prioridad de 8, la prioridad de la nueva directiva pasa a ser 4.
- Si agrega una directiva a la lista o elimina una directiva de la lista, los valores de posición de la directiva se reordenan desde el 1 sin omitir los números. Por ejemplo, si la directiva A, B, C y D tienen valores de posición de 1, 2, 3 y 4, y si elimina la directiva B de la lista, la directiva C ahora toma la segunda posición y la directiva D toma la tercera posición.

En Citrix ADM, siempre hay una directiva predeterminada asociada a un servidor csv con una prioridad de 1. Esta política predeterminada especifica la cantidad de conexiones TCP que un lbvserver debe procesar en un momento dado. Por lo tanto, cuando se crean las directivas de respuesta correspondientes y las directivas de conmutación de contenido en NetScaler ADC, siempre se les asigna una prioridad 1 mayor que la prioridad de la directiva L7 correspondiente. Por ejemplo, cuando se evalúa una directiva L7 con una prioridad de 1 y se crea una directiva de cambio de contenido con una

prioridad de 2. Del mismo modo, cuando se evalúa una directiva L7 con una prioridad de 2 y se crea una directiva de respuesta con una prioridad de 3.

En OpenStack, primero se evalúan las políticas «rechazar» y/o «redirect_to_url» y, a continuación, se evalúa la política «redirect_to_pool». En una instancia de NetScaler ADC, las directivas de respuesta siempre se evalúan primero para descartar la solicitud o presentar al usuario una dirección web redirigida, y las directivas de cambio de contenido se evalúan en último lugar. Este orden de evaluación no suele causar ningún conflicto si las directivas de cambio de contenido y de respuesta se excluyen mutuamente. Es decir, dos políticas L7 no deben tener expresiones idénticas. Las expresiones derivadas deben agregarse a las políticas de respuesta y de conmutación de contenido para evitar este tipo de conflictos. Por ejemplo, escribe una expresión para rechazar todas las solicitudes a ‘‘sports-football.com’’y otra expresión para permitir las solicitudes a ‘‘example-sports-football.com’’. Cree las directivas de L7 para que todas las directivas de respondedor para rechazar la solicitud se organicen en la parte superior de la lista de evaluación, seguidas de las directivas de respondedor para Web Direct, seguidas de las directivas de conmutación de contenido.

En Citrix ADM, siempre hay una directiva predeterminada asociada a un servidor csv con una prioridad de 1. Esta política predeterminada especifica la cantidad de conexiones TCP que un lbvserver debe procesar en un momento dado. Por lo tanto, cuando se crean las directivas de respuesta correspondientes y las directivas de conmutación de contenido en NetScaler ADC, siempre se les asigna una prioridad 1 mayor que la prioridad de la directiva L7 correspondiente. Por ejemplo, cuando se evalúa una directiva L7 con una prioridad de 1 y se crea una directiva de cambio de contenido con una prioridad de 2. Del mismo modo, cuando se evalúa una directiva L7 con una prioridad de 2 y se crea una directiva de respuesta con una prioridad de 3.

En OpenStack, primero se evalúan las políticas «rechazar» y/o «redirect_to_url» y, a continuación, se evalúa la política «redirect_to_pool». En NetScaler ADC, las directivas de respuesta siempre se evalúan primero para descartar la solicitud o presentar al usuario una dirección web redirigida, y las directivas de cambio de contenido se evalúan en último lugar. Este orden de evaluación no suele causar ningún conflicto si las directivas de cambio de contenido y de respuesta se excluyen mutuamente. Es decir, no hay dos políticas de L7 que deban tener expresiones similares. Se deben agregar expresiones derivadas similares en las políticas de respuesta y de conmutación de contenido para evitar este tipo de conflictos. Por ejemplo, escribe una expresión para rechazar todas las solicitudes a ‘‘sports-football.com’’y otra expresión para permitir las solicitudes a ‘‘example-sports-football.com’’. Cree las directivas de L7 para que todas las directivas de respondedor para rechazar la solicitud se organicen en la parte superior de la lista de evaluación, seguidas de las directivas de respondedor para Web Direct, seguidas de las directivas de conmutación de contenido.

Tareas de configuración

Las implementaciones de directivas y acciones del L7 se realizan mediante los comandos LBaaS de Neutron.

Configure las variables de entorno en OpenStack y cree el balanceador de carga (por ejemplo, LB1). Una vez creado correctamente el balanceador de cargas, cree el oyente y los grupos (por ejemplo, L1, P1 y P2) y agregue miembros y monitores a los grupos. Por ejemplo, P1 es el grupo predeterminado para L1, mientras que P2 es el grupo vinculado a LB1 y que administra los servidores de aplicaciones.

Para obtener más información sobre cómo configurar LBaaS V2 mediante la línea de comandos, consulte Configuración de LBaaS V2 mediante la línea de comandos.

Los siguientes comandos crean las directivas y definen las acciones específicas:

Crear directiva L7 para eliminar solicitudes

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action<action-name>
```

Ejemplo:

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

El comando anterior crea y vincula la policy11, una directiva de respuesta, al servidor de conmutación de contenido para rechazar las solicitudes. Como no se creó ninguna regla para esta directiva, la directiva se evalúa como “falsa”y la solicitud se rechaza.

Crear una directiva L7 para redirigir solicitudes a una URL determinada

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-url <redirect-url>
```

Ejemplo:

neutron lbaas-l7policy-create –name policy12 –action REDIRECT_TO_URL –listener admin-list1 –redirect-url `http://example-sports/about-us.html`

El comando anterior crea una acción de respuesta para redirigir las solicitudes a una dirección URL, crea una directiva de respuesta con acción y vincula esta directiva al servidor virtual de conmutación de contenido.

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --
    value <value-string> <L7 policy name>

neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value
     <value-string> <L7 policy name>
```

Las dos reglas anteriores se pueden conectar con un operador AND para derivar la expresión de la directiva de respuesta.

Crear una directiva L7 para redirigir solicitudes a un grupo

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-pool <redirect-pool
    >
```

Ejemplo:

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2

Si esta es la primera directiva de L7, el comando anterior implementa P2 junto con LB1, crea la acción de redireccionamiento de cambio de contenido y redirige las solicitudes a LB1. Si P2 ya existe, el comando crea la acción de redirección de conmutación de contenido y redirige las solicitudes a LB1.

Provisioning manual de la instancia NetScaler ADC VPX en OpenStack

January 30, 2024

En algunas redes empresariales, las instancias de Citrix ADC VPX no pueden conectarse al servidor de licencias de Citrix para descargar automáticamente las licencias, por motivos de seguridad. En este caso, debe implementar manualmente instancias de NetScaler ADC VPX en la plataforma OpenStack. Con el código de activación de licencia (LAC) que recibió de Citrix, descargue la licencia Citrix ADC VPX correspondiente y guárdela en su sistema local.

Para aprovisionar manualmente la instancia NetScaler ADC VPX en OpenStack:

1. Instale el software Citrix ADC Driver y registre Citrix Application Delivery Management (ADM) en OpenStack

    a) En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack**.

    b) Haga clic en **Configurar los ajustes de OpenStack.** En la página **Configurar opciones de OpenStack** , puede establecer los parámetros para configurar OpenStack en Citrix ADM. Aquí tiene dos opciones: **Predeterminado** y **Personalizado**.

    c) Seleccione **Predeterminado**si los servicios de OpenStack se ejecutan en los puertos predeterminados.

2. **Vaya a**Orquestación > Orquestación**en la nube** > **OpenStack**y haga clic en Configuración de implementación.**

    a) **Red**de administración : seleccione la red de administración en OpenStack a la que está conectado el Citrix ADC VPX de aprovisionamiento automático.

b) **Nombre del perfil**: Seleccione el perfil en la lista desplegable. NetScaler ADM utiliza la contraseña contenida en este perfil para configurar nuevas instancias de NetScaler ADC VPX aprovisionadas automáticamente.

c) Imagen de Citrix ADC VPX de un vistazo: seleccione la imagen de Citrix ADC VPX disponible en OpenStack Glance que se utiliza para crear una instancia de Citrix ADC VPX. La lista desplegable mostrará solo las imágenes que están presentes en OpenStack Glance.

3. En Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > **OpenStack** > **Service Packages** y, a continuación, haga clic en **Agregar**.
4. En la página **del paquete de servicios**, especifique los siguientes parámetros:

a) **Nombre**: nombre del paquete de servicios. Por ejemplo, escriba SVC-PKG-GOLD.

b) **Asignación**de instancias de Citrix ADC : seleccione **Dedicada** o **Particionada** como el tipo de asignación de instancias definido en el paquete de servicios.

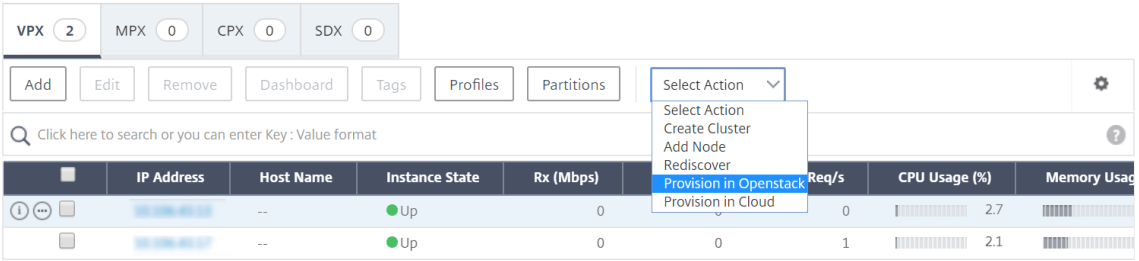
c) **Provisioning**de instancias de Citrix ADC : seleccione **Create Instance OnDemand** para crear instancias de Citrix ADC durante la propia configuración.

d) **Plataforma de aprovisionamiento automático**: Seleccione **OpenStack Compute**. De forma predeterminada, se seleccionará Citrix ADC VPX como tipo de instancia.

e) **Asigne arrendatarios de OpenStack y directivas de ubicación**: en la sección Arrendatarios de OpenStack, haga clic en **Agregar**y seleccione el arrendatario.

f) Haga clic en **Continue** y, a continuación, en **Done**.

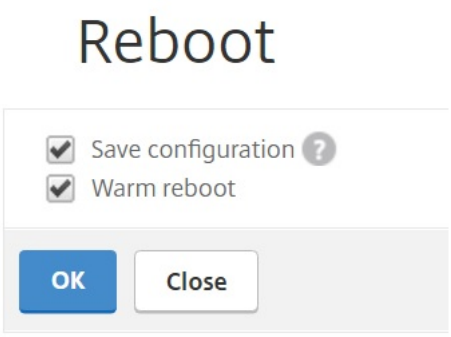
5. Vaya a **Sistema** > **Administración del sistema** > **Cambiar configuración del sistema** y seleccione **http** en la lista desplegable.
6. Vaya a **Redes** > **Instancias** > **Citrix ADC VPX** .
7. En la página **NetScaler ADC VPX**, haga clic en la lista desplegable **Administrador** y seleccione **Aprovisionar dispositivo**.



a) En la página **Provisioning de dispositivos**, escriba el nombre del dispositivo y seleccione el paquete de servicio que creó en el paso anterior.

b) Haga clic en **Aceptar**.

8. **Vaya a la ficha**Orquestación > Orquestación****en la nube**>**OpenStack > Solicitudes**.** Seleccione la solicitud y haga clic en **Tareas** para ver las tareas. Cuando el estado de la tarea cambia a **Finalizado**, significa que NetScaler ADC VPX se aprovisiona en NetScaler ADM.
9. Vaya a **Redes** > **Instancias** > **Citrix ADC VPX** para comprobar que la instancia de Citrix ADC VPX aparece en la página Citrix ADC VPX.
10. Haga clic en la instancia de NetScaler ADC VPX. Cuando la instancia de Citrix ADC VPX se abra en la ventana del explorador, inicie sesión en la instancia. Vaya a **Configuración** > **Sistema** > **Licencias** y agregue manualmente la nueva licencia. Para obtener más información sobre cómo agregar una nueva licencia, consulteDescripción general de licencias de NetScaler ADC.
11. Reinicie la instancia de NetScaler ADC VPX.



12. Después de unos minutos, puede iniciar sesión en OpenStack y, en**System** >**Instancias**, puede ver que la instancia de NetScaler ADC VPX se implementa en OpenStack.
13. Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron. Conéctese a cualquier cliente de Neutron y ejecute las tareas de configuración. Para obtener más información sobre cómo ejecutar los comandos de configuración, consulte Configuración de LBaaS V2 mediante la línea de comandos.

Aprovisionamiento de la instancia NetScaler ADC VPX en OpenStack mediante StyleBook

January 30, 2024

En el flujo de trabajo de orquestación de OpenStack, Citrix Application Delivery Management (ADM) ahora usa el StyleBook «os-cs-lb-mon» para implementar configuraciones de LBaaS en las instancias de Citrix ADC asignadas al inquilino de OpenStack. Se crea un paquete de configuración para cada equilibrador de carga creado por el usuario de OpenStack.

El uso de StyleBooks para la configuración en el flujo de trabajo de OpenStack ofrece las siguientes ventajas:

- Mejor visualización viendo todos los objetos de configuración.
- Fiabilidad a través de la reversión.
- Compatibilidad con varios tipos de instancias de NetScaler ADC (NetScaler ADC HA, particiones, VPX, CPX, MPX y otros).
- Personalización mediante el uso de sus propios StyleBooks para implementar la configuración de los arrendatarios de OpenStack.

Como administrador de NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** para ver el paquete de configuración implementado en la instancia de NetScaler ADC.
Puede realizar las siguientes tareas:

- Desplázate para ver el paquete de configuración «os-cs-lb-mon» implementado para el balanceador de cargas.
- Haga clic en **Ver definición** en el panel StyleBook «os-cs-lb-mon» para comprobar la configuración implementada en las instancias.
- Haga clic en **Ver objeto** para ver la lista de objetos o entidades de NetScaler ADC implementados en las instancias.

Puntos a tener en cuenta antes de Provisioning instancias mediante StyleBooks

A partir de la compilación 49.23 de Citrix ADM 12.1, se actualizó la arquitectura del flujo de trabajo de orquestación de OpenStack. El flujo de trabajo utiliza ahora los StyleBooks de Citrix ADM para configurar instancias de Citrix ADC. Si va a actualizar a Citrix ADM 12.1 compilación 49.23 desde la versión 12.0 o desde la versión 12.1 compilación 48.18, debe ejecutar la siguiente script de migración:

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

- Al ejecutar el script de migración, se crean paquetes de configuración del StyleBook «os-cs-lb-mon» correspondientes a las configuraciones de OpenStack existentes.
- La ejecución de este script de migración es obligatoria si tenía configuraciones de OpenStack implementadas a partir de estas compilaciones anteriores.
- Puede implementar nuevas configuraciones en las instancias con el StyleBook «os-cs-lb-mon» solo después de ejecutar el script de migración desde la versión 12.1, compilación 49.23.
- Todas las configuraciones que se intenten desde OpenStack fallarán hasta que se ejecute el script de migración.

> **Nota**
>
> - Una vez que ejecute el script de migración, no podrá volver a la versión anterior de NetScaler ADM.
> - Asegúrese de que ha actualizado los controladores NetScaler ADC para OpenStack LBaaS V2 a la versión más reciente. Utilice los archivos del paquete Citrix ADC que se proporcionan junto con la versión 49.23 más reciente de Citrix ADM 12.1.

Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron. Conéctese a cualquier cliente de Neutron y ejecute las tareas de configuración. Para obtener más información sobre cómo ejecutar los comandos de configuración, consulte Configuración de LBaaS V2 mediante la línea de comandos.

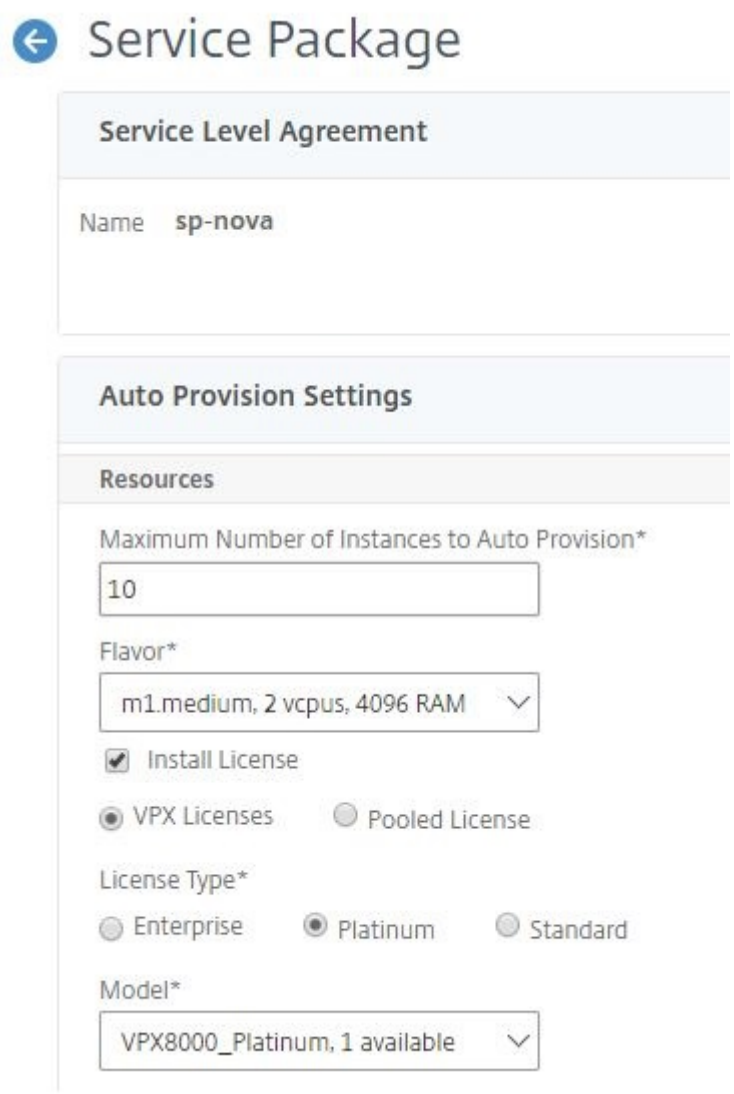
Licencia de check-in y check-out VPX y soporte de licencias agrupadas para el entorno OpenStack

January 30, 2024

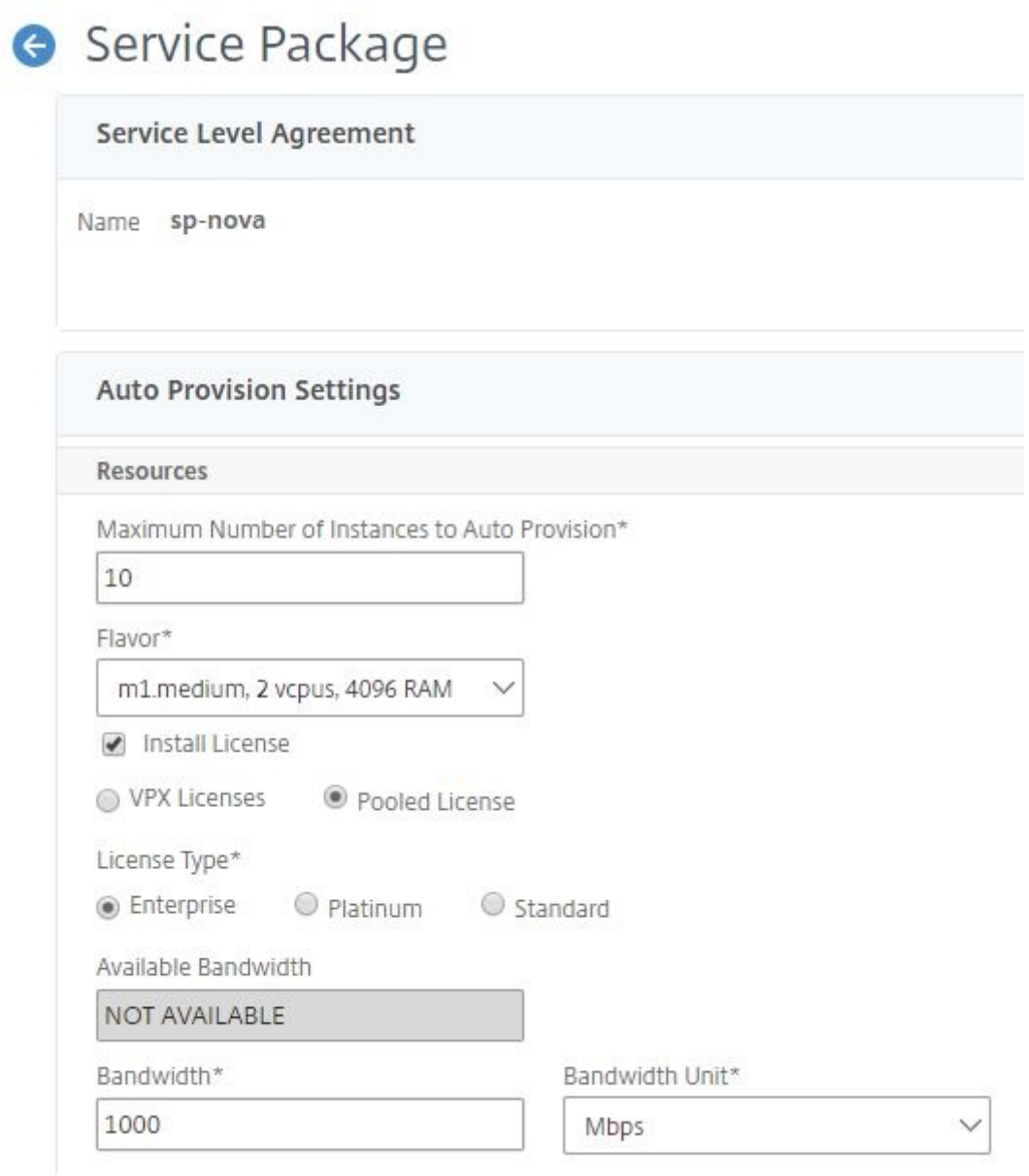
En el flujo de trabajo de orquestación de OpenStack, Citrix Application Delivery Management (ADM) crea instancias de Citrix ADC VPX bajo demanda al seleccionar el paquete de servicios con **OpenStack Compute**. Ahora, la página del paquete de servicios de la función Orchestration de Citrix ADM está mejorada para proporcionar la licencia necesaria para instalarse en las instancias de Citrix ADC VPX que se crean bajo demanda. Las licencias proporcionadas pueden ser licencias de registro y salida VPX o licencias agrupadas.

Para utilizar esta función, primero debe cargar las licencias en Citrix ADM y, a continuación, crear paquetes de servicios que utilicen OpenStack Compute.

- Si se trata de una licencia de check-in y check-out, puede elegir la licencia que se va a instalar entre las distintas licencias disponibles.



- Si se trata de una licencia de grupo, puede seleccionar tanto el ancho de banda como el tipo de edición de licencia que se va a instalar.



Cada vez que implementa el primer equilibrador de carga con NetScaler ADM como proveedor, NetScaler ADM crea la instancia NetScaler ADC VPX e instala la licencia especificada en el paquete de servicio en la instancia recién creada.

Además, cuando eliminas una instancia de equilibrio de carga existente, esa instancia ya no es necesaria. La instancia se retira del servicio y la licencia se devuelve a Citrix ADM. Esto permite un uso óptimo de las licencias disponibles en Citrix ADM.

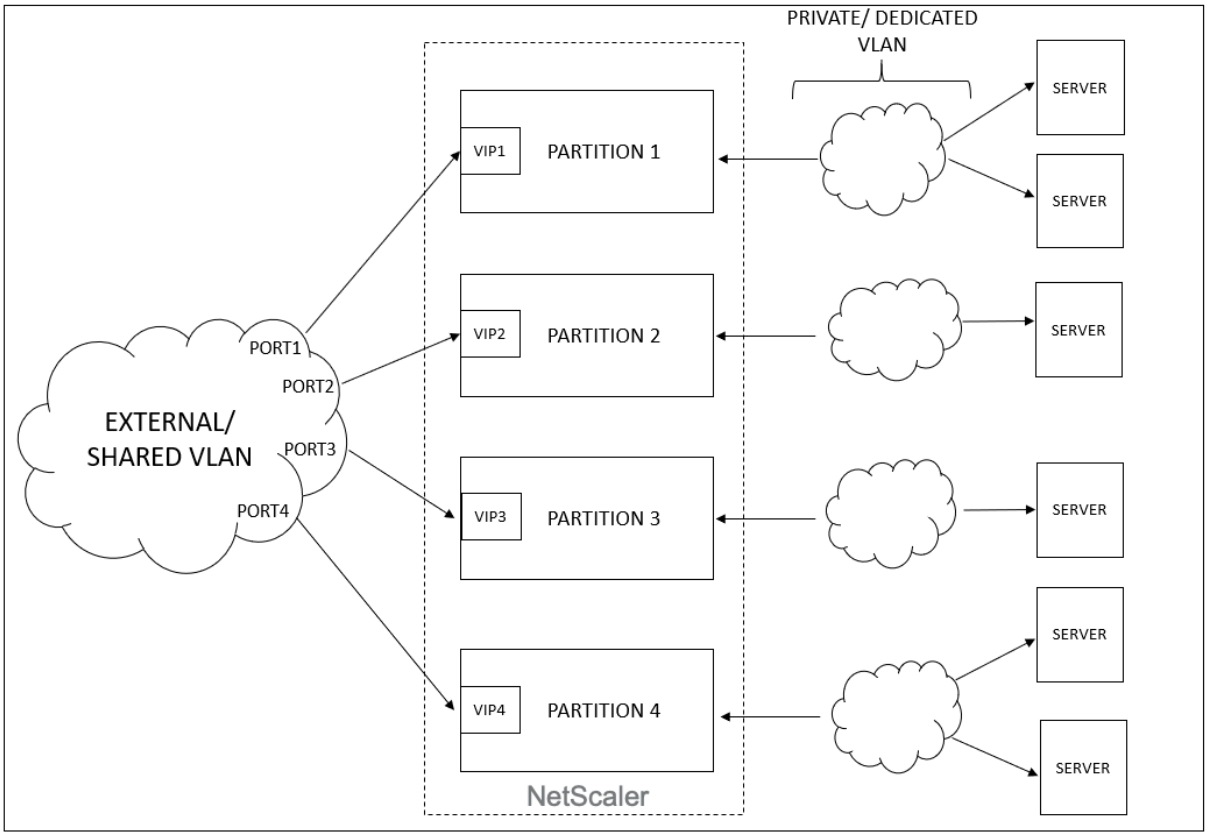
> **Nota**
>
> Cuando Citrix ADM se implementa en modo de alta disponibilidad, tenga en cuenta que las licencias se cargan en el Citrix ADM principal o activo actual, MAS-HA-1. Cuando implementa la

> primera solicitud y Citrix ADM crea las instancias de Citrix ADC VPX, la instancia comprueba las licencias necesarias de MAS-HA-1. En un momento posterior, suponga que el dispositivo secundario de NetScaler ADM, MAS-HA-2, que no tiene las licencias, está activo ahora. La instancia ADC VPX no puede extraer la licencia de MAS-HA-2 ahora y, por lo tanto, la instancia no se puede crear para usuarios nuevos.
>
> En tal caso, asegúrese de que el MAS-HA-1 esté activo y que ahora sea el nodo principal actual. Es decir, conmute por error manualmente el Citrix ADM de MAS-HA-2 a MAS-HA-1. Después de esto, debe volver a intentar la configuración de OpenStack y las instancias se volverán a crear con las licencias adecuadas. Para obtener más información sobre la compatibilidad con licencias en la implementación de alta disponibilidad de NetScaler ADM, consulte Alta disponibilidad.

Compatibilidad con VLAN compartida para particiones de administración

January 30, 2024

Para los inquilinos que se conectan desde redes privadas, Citrix Application Delivery Management (ADM) admite la política de aislamiento para que cada inquilino tenga su propia partición dedicada, una VLAN dedicada y servidores dedicados. Para los arrendatarios que se conecten desde redes públicas, una VLAN dedicada requerirá el uso de demasiadas direcciones IP. Una VLAN compartida evita este problema creando una dirección IP virtual en cada partición, creando así una única subred IP.



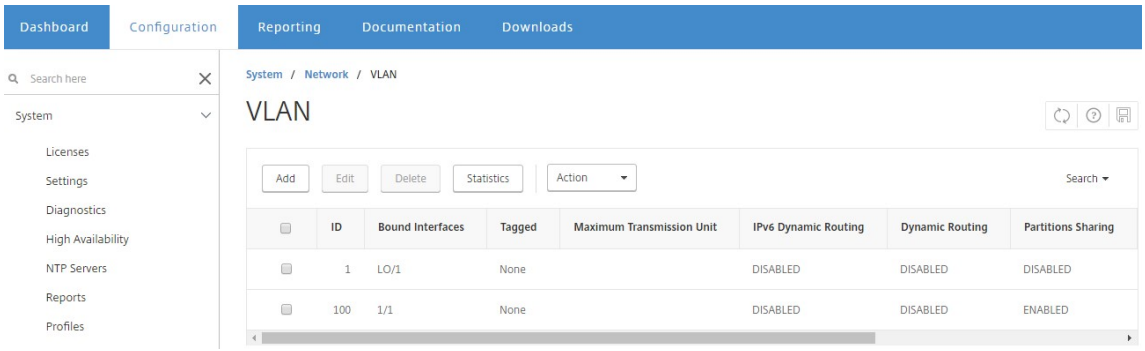
Cuando un arrendatario configura un VIP o un listener, se crea una partición admin en el dispositivo NetScaler ADC para ese arrendatario. Toda la configuración del balanceador de carga se envía a la partición de administración que se ha creado. Si el arrendatario utiliza una red compartida o una red externa para crear un balanceador de carga, se agrega la VLAN de esa red y se habilita la función de uso compartido. Cuando otro inquilino utiliza la misma red compartida para crear su balanceador de carga, la VLAN no se vuelve a agregar al Citrix ADC, sino que también se enlaza a la segunda partición. Por lo tanto, cualquier arrendatario que utilice la misma red compartida obtiene una partición enlazada a la misma VLAN.

El Citrix ADM admite la dirección MAC de destino virtual. Cuando los inquilinos comparten una VLAN, Citrix ADM asigna diferentes direcciones MAC a la partición del dispositivo Citrix ADC. Esto permite compartir una VLAN entre particiones o entre todos los arrendatarios y todos los dominios de tráfico.

Configuración de una VLAN compartida desde una instancia de Citrix ADC

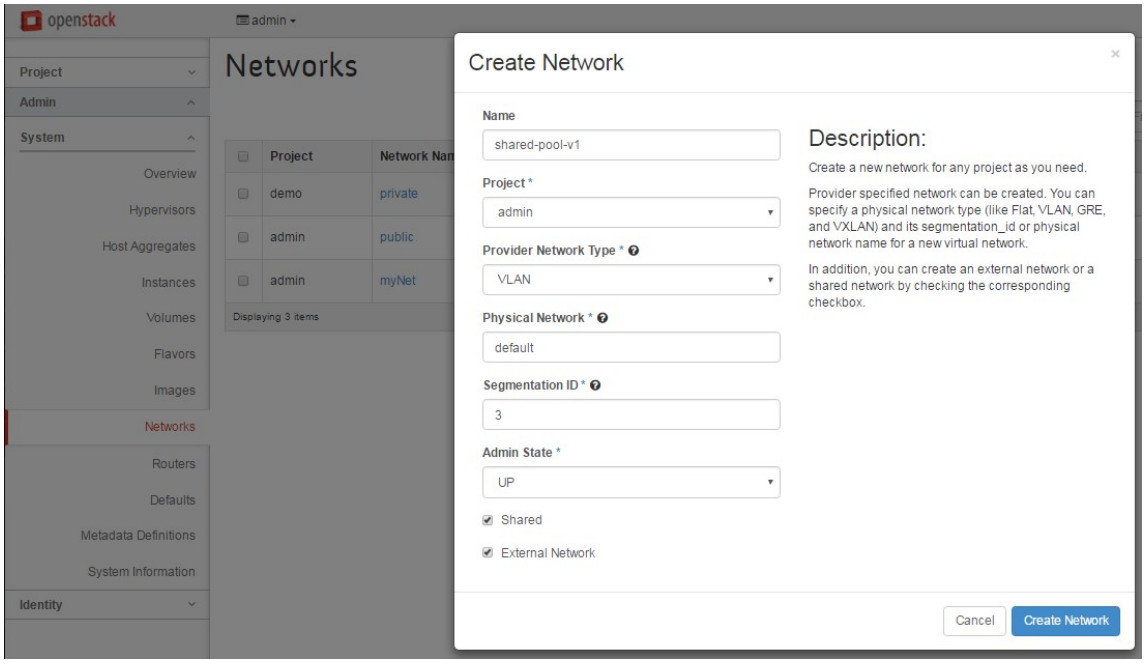
1. En una instancia de Citrix ADC, vaya a **Configuración** > **Sistema** > **Red** > **VLAN**, seleccione un perfil de VLAN y haga clic en **Editar** para establecer el parámetro de partición compartida.
2. En la página **Configurar VLAN**, active la casilla **Compartir particiones**.

3. Haga clic en **Aceptar**.



Configuración de VLAN compartida desde OpenStack Orchestration

1. En OpenStack, vaya a **Administración** > **Sistema** > **Redes**y, a continuación, haga clic en **Crear red**.
2. En **Crear red**, defina los siguientes parámetros:
   a) Nombre: introduzca el nombre de la red
   b) Proyecto: seleccione un proyecto de la lista desplegable
   c) Tipo de red del proveedor: seleccione **VLAN** en la lista desplegable. Esto define que la red virtual se establece como VLAN.
   d) Red física: aquí se selecciona la red física predeterminada. Puede modificar esto.
   e) Estado de administrador: de forma predeterminada, el estado administrativo de la red es ACTIVADO
   f) Seleccione Red **compartida** y **externa** para definir que la VLAN es compartida y utiliza una red externa.
3. Haga clic en **Crear red**.



Flujo de trabajo de licencias de prueba

January 30, 2024

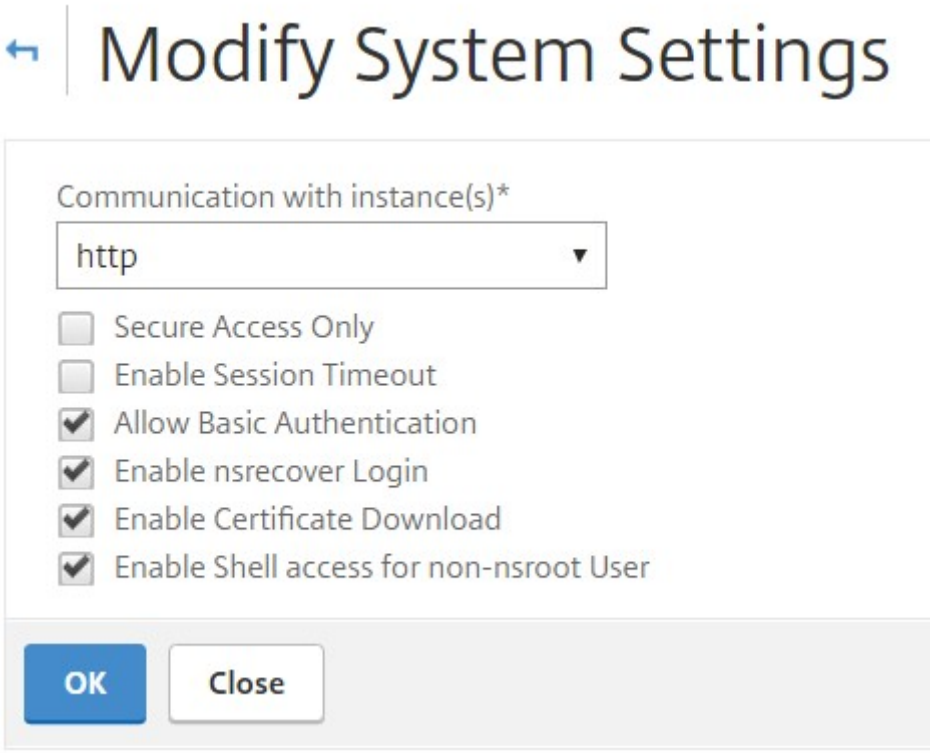
Durante el aprovisionamiento automático de la instancia de NetScaler ADC VPX mediante la orquestación de OpenStack, NetScaler Application Delivery Management (ADM) utiliza OpenStack Compute para iniciar una instancia de NetScaler ADC VPX. La instancia de Citrix ADC VPX recién aprovisionada se pone en contacto con el portal de licencias de Citrix durante la configuración y utiliza el código de activación de licencias (LAC) para descargar e instalar automáticamente los archivos de licencia.

Licencias de prueba

El personal de soporte técnico utiliza licencias de prueba cuando instala dispositivos Citrix ADM y Citrix ADC VPX in situ. Una licencia de prueba o evaluación para Citrix ADC VPX es válida durante 90 días. Si es necesario evaluar más de un Citrix ADC o extender las pruebas después de 90 días, se debe solicitar una nueva licencia de evaluación. En lugar de la instalación automática de los archivos de licencias de prueba, Citrix ADM le ofrece una solución alternativa. Puede descargar manualmente los archivos de licencia e instalarlos en Citrix ADC VPX para completar la instalación de la instancia.

Si el Citrix ADC VPX no puede conectarse a Internet, configure Citrix ADM para que actúe como servidor proxy para el portal de licencias de Citrix e instale los archivos de licencia.

Las instancias de Citrix ADC VPX que tienen una licencia de prueba solo pueden comunicarse con Citrix ADM en HTTP. Para configurar la comunicación HTTP en Citrix ADM, vaya a **Sistema** > **Administración del sistema** y haga clic en **Cambiar la configuración del sistema** . Seleccione **http** en la lista desplegable para establecer el método de comunicación y haga clic en**Aceptar**.



Integración con los servicios de OpenStack Heat

January 30, 2024

OpenStack Neutron LBaaS permite servicios de equilibrio de carga central, como equilibrio de carga, descarga SSL y conmutación de contenido, para aplicaciones. El LBaaS se administra a través de una API RESTful, y la API permite a los inquilinos realizar llamadas REST para crear, actualizar y eliminar objetos de LBaaS. Dado que LBaaS proporciona servicios de equilibrio de carga, no permite el uso de las funciones más avanzadas de NetScaler ADC durante el proceso de orquestación. El complemento Citrix ADC Heat supera esta limitación.

Servicio de orquestación de calor

El servicio de orquestación térmica de OpenStack permite la implementación de aplicaciones en la nube complejas sobre la base de plantillas. La plantilla de orquestación térmica (HOT) describe la infraestructura de una aplicación en la nube en archivos de texto que los humanos pueden leer y escribir, y que pueden gestionarse mediante herramientas de control de versiones. YAML, un lenguaje estructurado, se utiliza para escribir estas plantillas. La plantilla HOT permite crear la mayoría de los tipos de recursos de OpenStack y especifica las relaciones entre los recursos definidos en ella. El complemento Citrix ADC Heat permite configurar las funcionalidades avanzadas del controlador de entrega de aplicaciones (ADC) en cualquier instancia de Citrix ADC.

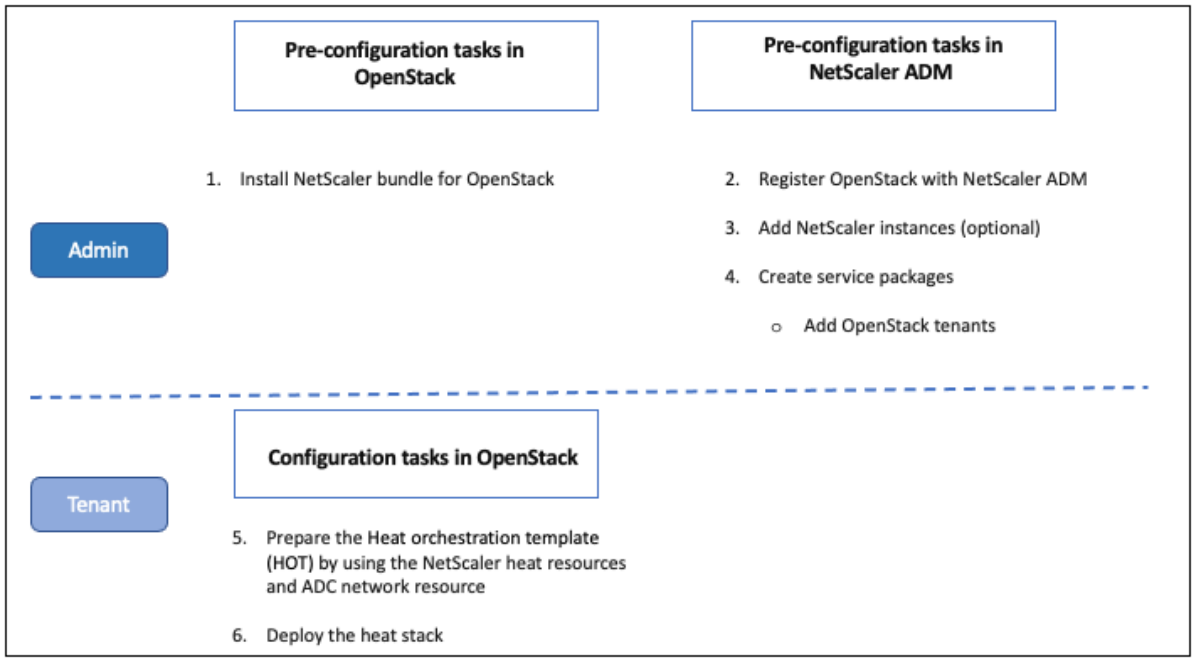
Libros de estilo Citrix ADC

Los StyleBooks de Citrix Application Delivery Management (ADM) se pueden utilizar para crear y configurar las funcionalidades de Citrix ADC. Al igual que las plantillas de Heat, los StyleBooks también están escritos en YAML. Se pueden crear StyleBooks independientes para cada funcionalidad y se puede usar un único StyleBooks para implementar configuraciones en varias instancias de Citrix ADC.

Durante la integración de Citrix ADC con OpenStack, Citrix ADM publica todos los StyleBooks de Citrix ADM como recurso en el servicio Heat. Esto incluye tanto los StyleBooks que se envían con Citrix ADM como los StyleBooks que crea el usuario en un momento posterior. La plantilla Heat le permite configurar las funciones avanzadas de los ADC de Citrix mediante estos recursos de StyleBooks.

Flujo de trabajo para configurar instancias de Citrix ADC mediante Heat

El siguiente diagrama de flujo ilustra el flujo de trabajo para implementar el Heat Stack:



Realice las siguientes tareas como administrador de la nube:

Para configurar los servicios de calefacción en OpenStack:

1. Descargue los paquetes Citrix ADC para OpenStack

   Instale los paquetes Citrix ADC en OpenStack. En Citrix ADM, vaya a **Descargas** y descargue los paquetes de controladores Citrix ADC, descomprima los paquetes y copie el contenido de la carpeta Heat del paquete en el directorio de recursos del motor Heat de OpenStack. La ruta del directorio es la siguiente:

   /opt/stack/heat/heat/engine/resources/netscaler_resources

2. Cree una sección “netscaler_plugin”en el archivo heat.conf y actualice los siguientes parámetros en esa sección:

   [netscaler_plugin]

   a) Cuando la comunicación es http, los parámetros se actualizan de la siguiente manera:

   NMAS_BASE_URI=<http://10.146.103.45:80>

   NMAS_USERNAME=

   NMAS_PASSWORD=

   b) Cuando la comunicación es https, los parámetros se actualizan de la siguiente manera:

   NMAS_BASE_URI=https://common_name_used_in_certificate

   NMAS_USERNAME=<openstack_driver_username

NMAS_PASSWORD=<openstack_driver_password>

SSL_CERT_VERIFY=<True_or_False>

CERT_FILE_PATH=<path_of_the_certificate_file>

Si el usuario establece ssl_cert_verify en «False», Citrix ADM envía verify=False en las llamadas de solicitud, lo que inhabilita la validación del certificado SSL. Si ssl_cert_verify se establece en «True» y la entrada cert_file_path está presente, Citrix ADM envía esta ruta en el parámetro verify de la solicitud; de lo contrario, Citrix ADM envía Verify=true.

> **Nota**
>
> Para implementar Citrix ADM en modo «Alta disponibilidad», actualice los siguientes parámetros en el archivo heat.conf:
>
> NMAS_BASE_URI= <ip address of the front-end virtual server>

3. Reinicie el servicio Heat en OpenStack.

   Al reiniciar los servicios Citrix ADC Heat en OpenStack, todos los StyleBooks Citrix ADM definidos se importan a Heat como recursos. Además, el recurso de red Citrix ADC y el recurso de certificado se importan a OpenStack como recursos Citrix ADC Heat.

4. Registre Citrix ADM en OpenStack.

   a) En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** y haga clic en **Configurar opciones de OpenStack**.

   b) En la página **Configurar los ajustes de OpenStack**, puede establecer los parámetros para configurar OpenStack. Aquí tiene dos opciones: Predeterminado y Personalizado.

   c) Seleccione **Predeterminado** si los servicios de OpenStack se ejecutan en los puertos predeterminados. Introduzca los parámetros siguientes:

      i. Dirección IP del controlador OpenStack

      ii. Nombre de usuario de administrador

      iii. Contraseña

      iv. Arrendatario de administrador de OpenStack

      v. Controlador Citrix ADC y contraseña de Heat

      > **Nota**
      >
      > Esta es la misma contraseña (NMAS_PASSWORD) que introdujo en el archivo heat.conf.

5. Cree paquetes de servicios y defina los SLA con su arrendatario.

Se crea un inquilino en Citrix ADM para cada usuario durante el registro de OpenStack, y tanto el controlador LBaaS como el complemento Heat utilizan la información del inquilino. El complemento Heat utiliza esta información para ponerse en contacto con NetScaler ADM para importar StyleBooks como recursos de Heat en OpenStack.

> **Nota**
>
> Para obtener más información sobre la creación de paquetes de servicios y otras tareas previas a la configuración en NetScaler ADM y OpenStack, consulte Integración de NetScaler ADM con OpenStack Platform.

6. Observe que todos los Stylebooks relevantes de Citrix ADM se importan a OpenStack Heat como recursos. Además, observe que el recurso de red NetScaler ADC y el recurso de certificado NetScaler ADC se importan a OpenStack Heat como recursos.

   > **Nota**
   >
   > Actualmente, solo puede usar los StyleBooks que se envían con Citrix ADM.

   Su arrendatario ahora puede crear la plantilla de Heat en OpenStack, introducir los valores de los parámetros de Heat requeridos e implementar la pila de calor. Cuando se implementa la pila Heat, la configuración se envía a Citrix ADM y se configuran las instancias de Citrix ADC necesarias.

Para preparar la plantilla Heat e iniciar Heat Stack:

1. En OpenStack, el arrendatario puede crear una plantilla de orquestación de calor (HOT) mediante los recursos de Heat.
2. En OpenStack Horizon, el administrador del arrendatario puede ir a **Proyecto** > **Orquestación** > **Pilas para crear la plantilla Heat e iniciar la Heat Stack**. Hay dos formas de crear HOT:

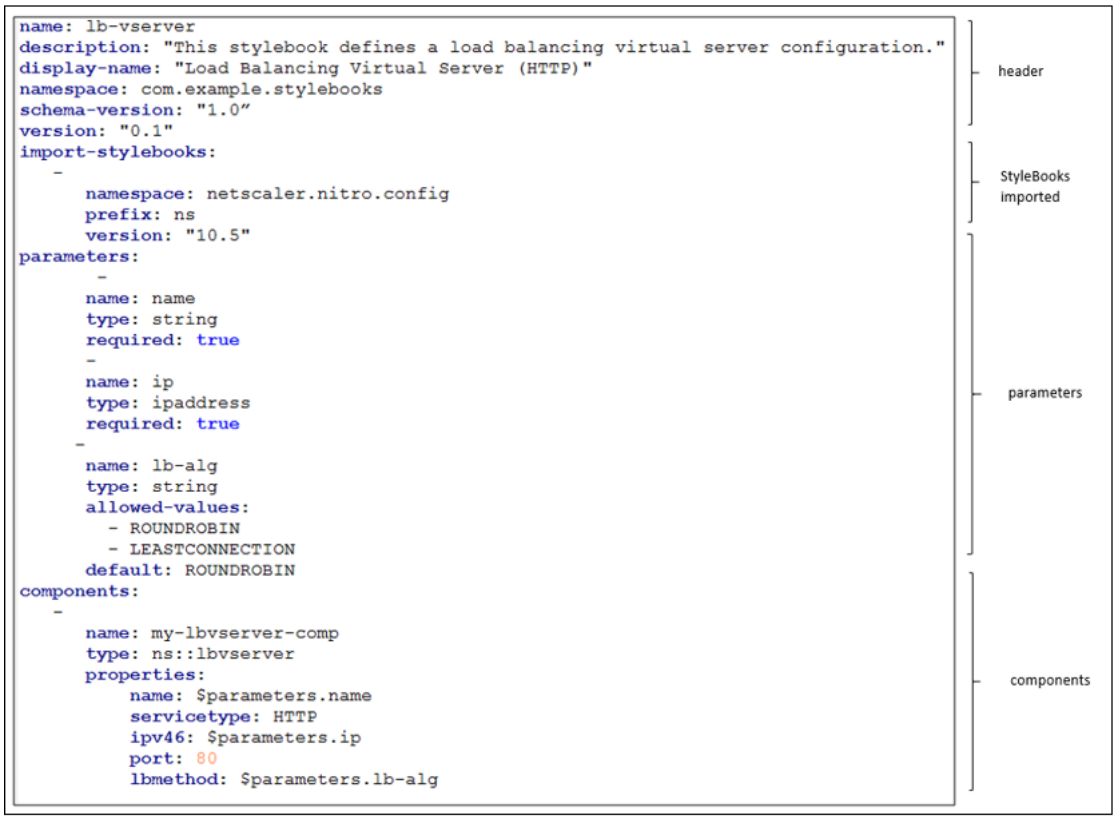
   - **Archivo**: Seleccione la plantilla actualizada del directorio local
   - **Entrada directa**: Copia y pega el contenido de YAML de la plantilla en la ventana

   > **Nota:**
   >
   > Después de implementar correctamente la pila, el arrendatario puede actualizarla mediante la plantilla de cambio de pila. Sin embargo, la información de subred y la dirección IP virtual (VIP) que se proporcionaron inicialmente durante la creación de la pila no se pueden modificar.

   Una vez que el inquilino implemente la pila, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Requests** in Citrix ADM para observar las listas de tareas. Además, vaya a **Aplicaciones** > **Configuración** en Citrix ADM para observar que las instancias de Citrix ADC se configuran correctamente en forma de paquetes de configuración de StyleBooks.

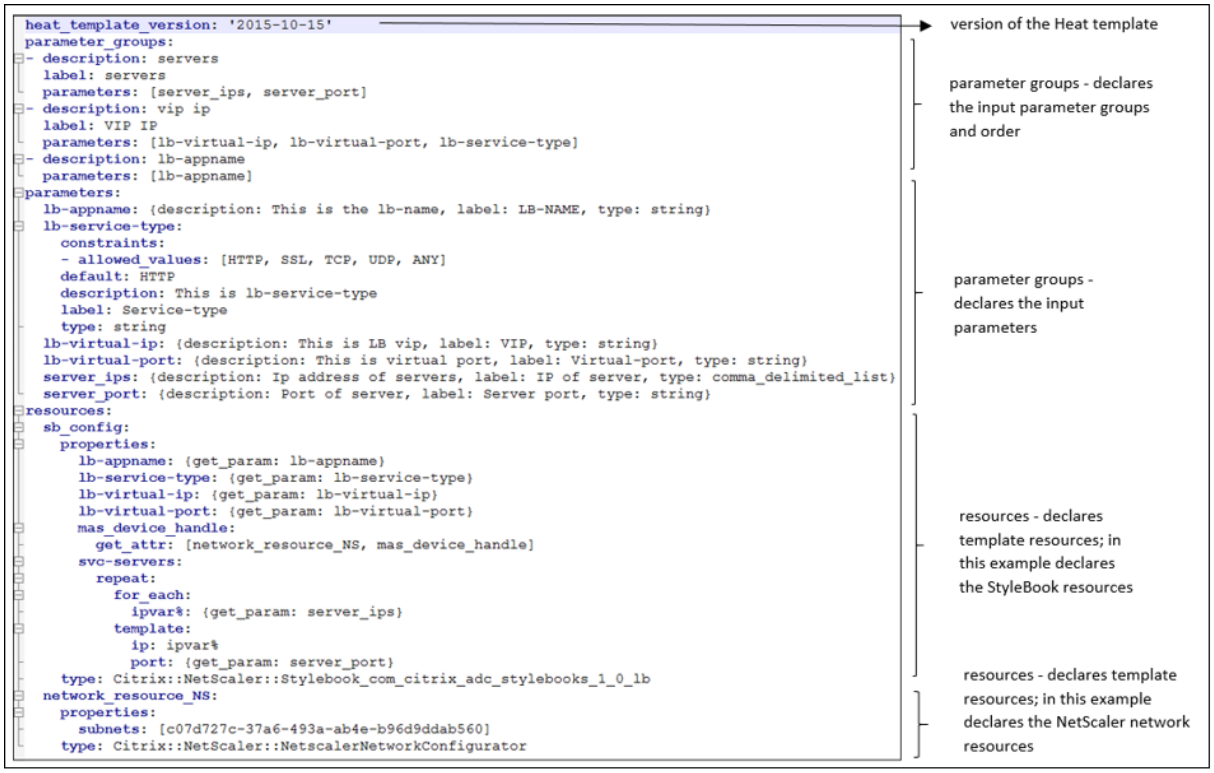
Ejemplo de un NetScaler ADM StyleBooks:

La siguiente imagen muestra un ejemplo de cómo se construye un NetScaler ADM StyleBooks y explica brevemente los componentes. Para obtener más información sobre NetScaler ADM StyleBooks y cómo usar los StyleBooks enviados, consulte StyleBooks.



Un ejemplo de plantilla de calor:

La siguiente imagen muestra la estructura de una plantilla de calor definida en YAML y señala los recursos de StyleBooks y NetScaler ADC que se importan como recursos de calor.



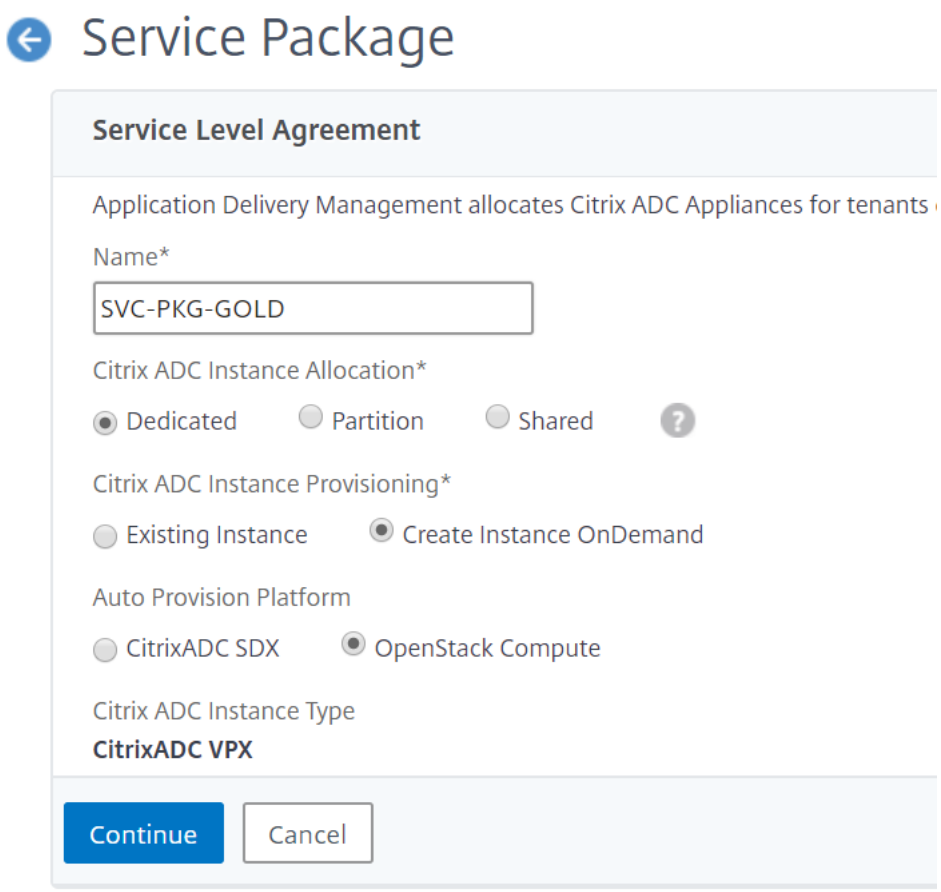
Para obtener más información sobre los servicios de Heat y cómo crear plantillas, consulte ladocumentación de OpenStack Heat.

Directivas de aislamiento de paquetes de servicio

January 30, 2024

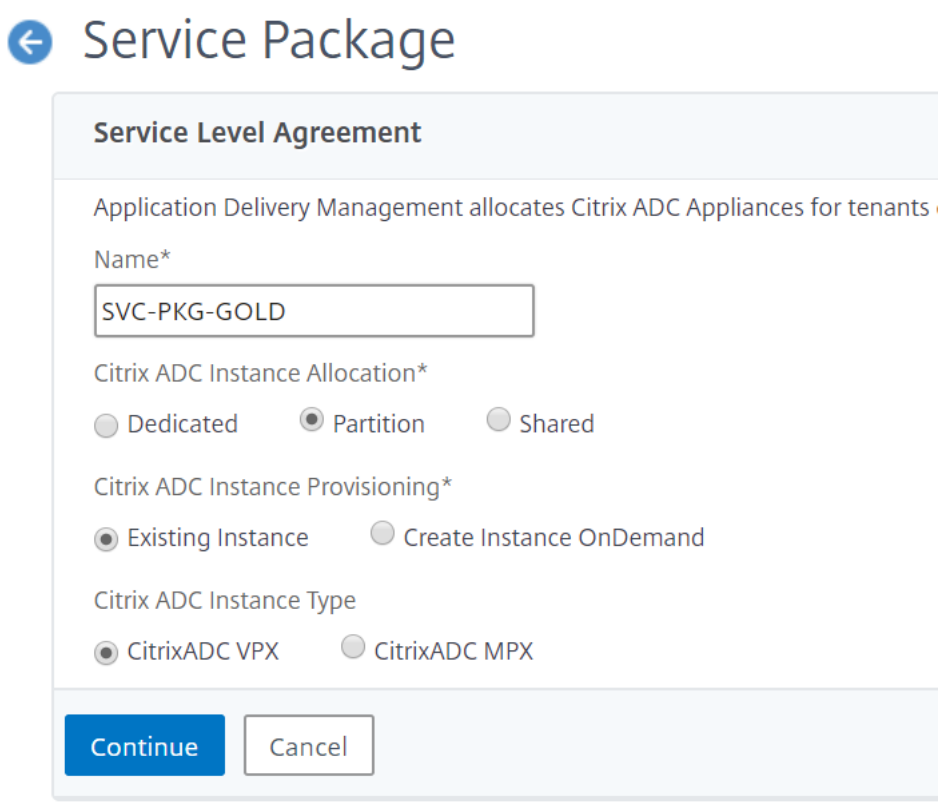
Directiva de aislamiento dedicada

A cada inquilino asociado al paquete de servicios Citrix Application Delivery Management (ADM) de una política dedicada se le asigna una instancia de Citrix ADC de entre las instancias que forman parte de este paquete de servicios. Esta instancia de NetScaler ADC asignada no se comparte con otros arrendatarios.



Directiva de aislamiento de particiones

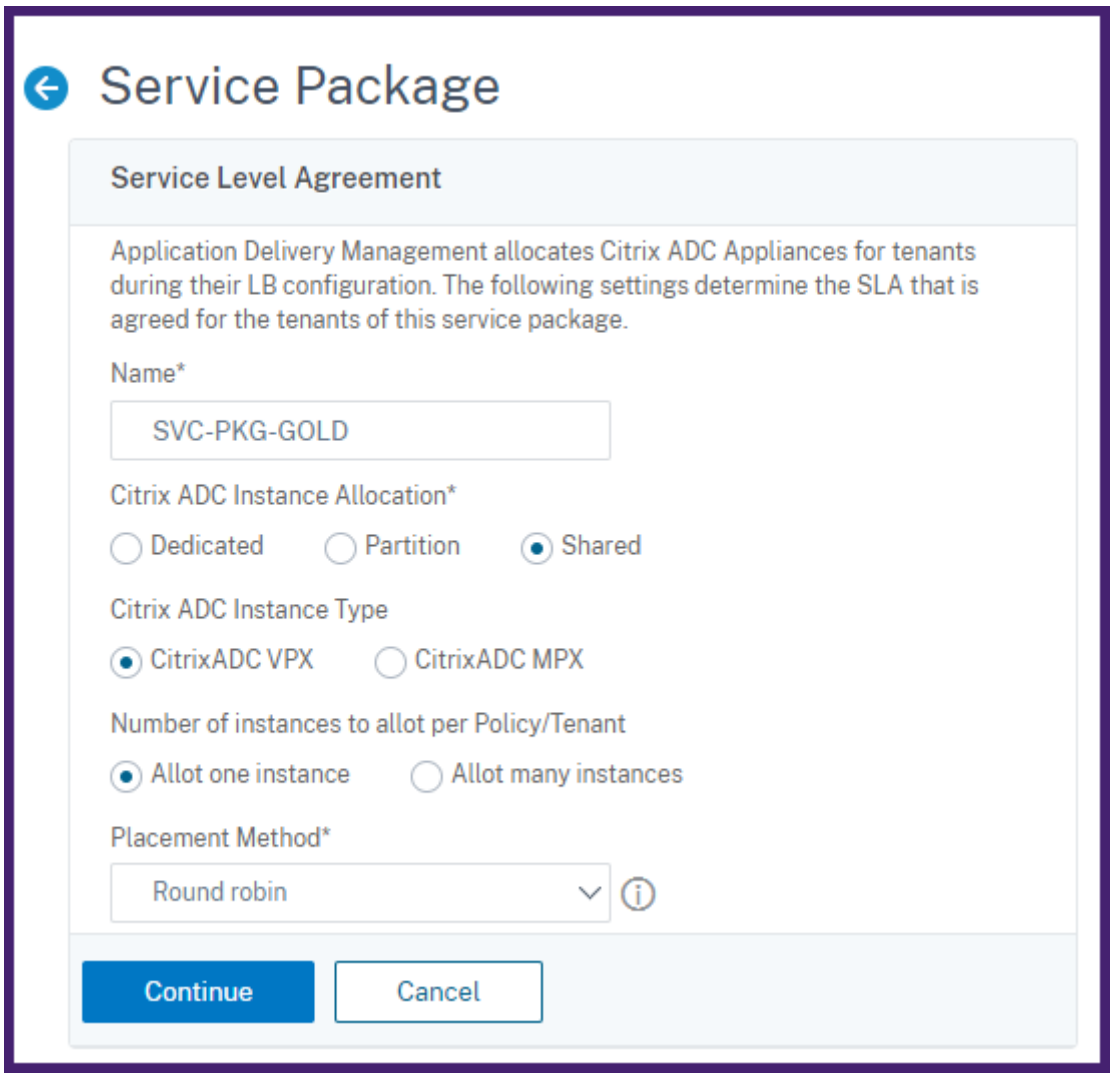
A cada arrendatario asociado al paquete de servicios de la directiva de partición se le asigna una partición de administración lógica dedicada de una instancia NetScaler ADC que forma parte del paquete de servicios.



Directiva de aislamiento compartido

Los inquilinos asociados al paquete de servicios comparten las instancias de Citrix ADC que forman parte del paquete de servicios. Todas las configuraciones de un inquilino se asignan a una instancia de Citrix ADC. En este modo, las configuraciones de varios inquilinos se pueden alojar en la misma instancia de Citrix ADC. Puede seleccionar **Citrix ADC VPX** o **Citrix ADC MPX** como tipo de dispositivo. Puede optar por asignar solo una instancia de Citrix ADC o varias instancias al paquete de servicios. Es decir, varios inquilinos pueden compartir una o varias instancias virtuales del dispositivo Citrix ADC.

> **Nota**
>
> Agregue instancias de NetScaler ADC SDX en los paquetes de servicios como instancias de NetScaler ADC VPX solamente, ya que un NetScaler ADC SDX tiene un NetScaler ADC VPX aprovisionado en él.



Nota

También puede crear políticas de colocación flexibles, en las que las políticas no solo se basen en el nombre o la identificación del inquilino, sino también en otros atributos personalizados. Para obtener más información sobre las directivas de ubicaciónflexible, consulte Asignación flexible de dispositivos basada en directivas.

Asignación flexible de dispositivos basada en directivas

January 30, 2024

Citrix Application Delivery Management (ADM) asigna instancias virtuales de Citrix ADC a los arrendatarios, según los SLA acordados con los arrendatarios. La asignación de instancias virtuales a los

arrendatarios crea una relación de uno a uno entre la instancia y el arrendatario, en la que solo se puede asignar un arrendatario a un paquete de servicios en el centro de datos.

En algunas situaciones, es posible que los arrendatarios requieran más de una instancia o que la asignación de instancias no se base en los arrendatarios como criterio, sino en otros factores, como el ID de red o la aplicación. En estos casos, Citrix ADM permite definir con precisión las políticas de ubicación en función de expresiones definidas por el usuario para asignar una configuración de balanceador de carga a una de las instancias administradas.

Las políticas de ubicación brindan la flexibilidad de decidir qué instancia de Citrix ADC se usa en cada configuración de balanceador de carga creada por los usuarios. Las políticas de colocación flexibles de Citrix ADM ofrecen una opción adicional al método existente de asignación de instancias de Citrix ADC en función de los inquilinos.

> **Nota**
>
> Puede asignar instancias a los arrendatarios de forma manual o utilizar directivas de ubicación para asignar instancias en función de las expresiones creadas. No puede utilizar ambos métodos simultáneamente en un único paquete de servicios.

Las directivas de ubicación se basan en expresiones booleanas definidas sobre las propiedades de los principales objetos de configuración de LBaaS, como los grupos y los balanceadores de carga. La interfaz de usuario de la política de colocación de Citrix ADM proporciona expresiones predefinidas entre las que puede elegir para definir una política personalizada. Puede crear varias directivas de ubicación para diferentes expresiones. Por lo tanto, cada arrendatario puede tener varios dispositivos que se definen según los requisitos del arrendatario.

Primero debe seleccionar una expresión para que coincida con un objeto raíz que se debe configurar más adelante. El objeto raíz puede ser un objeto de grupo en el caso de LBaaS V1 y un objeto de balanceador de carga en el caso de LBaaS V2. Por lo tanto, las ubicaciones basadas en políticas de Citrix ADM son compatibles con las API V1 y V2 de LBaaS. Estas directivas de ubicación se asocian luego a los paquetes de servicios. Una vez que el objeto raíz se coloca en una instancia, los objetos sucesivos del modelo se agregan a la instancia.

Por ejemplo, el objeto de configuración del grupo puede tener las siguientes propiedades:

- tenant_id
- name
- description
- protocol
- método lb_
- identificador_de_subred

- nombre_de_subnombre
- admin_state_up
- estado
- id_de_red
- tipo_de_red
- identificación_de_segmentación
- subnet_cidr
- subnet_gateway_ip

Los siguientes son ejemplos que muestran algunas de las expresiones que utilizan propiedades de grupo para definir una expresión para la directiva:

1. Expresión de directiva basada en nombre de grupo

   config [“pools”] [“nombre”] ==”pool de gama alta»

2. Expresión de directiva basada en nombre de subred del grupo

   config [“pools”] [“subnet_name”] == «us-west-payment-subnet1”

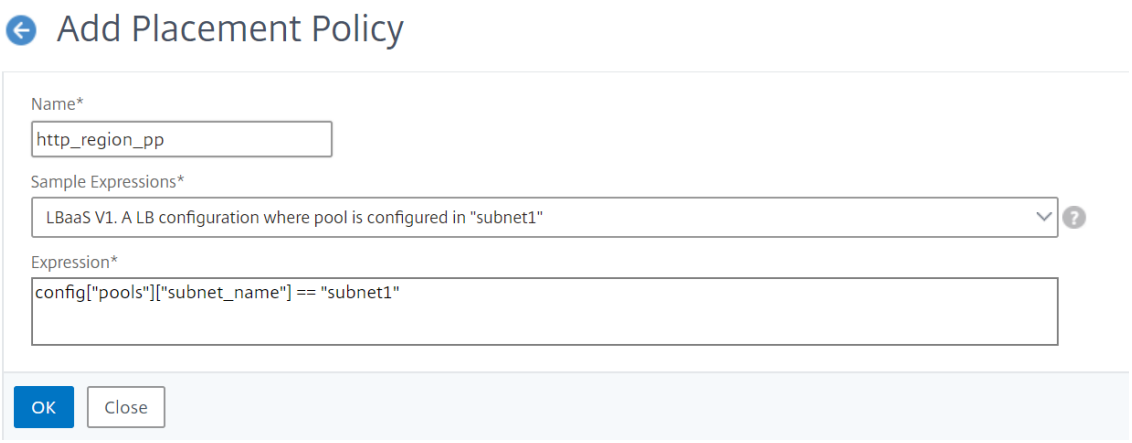
3. Expresión de directiva basada en nombre de subred del equilibrador de carga

   config [“balanceadores de carga”] [“nombre_subred”] == «mas-subnet»

Adición de directiva de ubicación

1. En la página principal de Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > **Placement Policy** y, a continuación, haga clic en **Agregar**.
2. En la página **Agregar directiva de ubicación**, defina los siguientes parámetros:
   a) Nombre: escriba un nombre para la directiva de colocación
   b) Expresiones de uso frecuente: seleccione una expresión de la lista desplegable.
   c) Expresión: en este campo se rellena una expresión lógica (booleana) en función de la expresión que ha seleccionado en el campo anterior. Modifique los nombres de los campos según sea necesario.

> **Nota**
>
> Al crear varias directivas, asegúrese de que las directivas son exclusivas entre sí.



3. Haga clic en **Aceptar**.
4. **Vaya a**Orquestación > Orquestación**en la**nube**>**OpenStack**>**Paquetes de servicios**y, a continuación, haga clic en Agregar.**
5. En la página **del paquete de servicios**, defina los siguientes parámetros:

   a) Nombre: escriba un nombre para el paquete de servicios

   b) Directiva de aislamiento: seleccione Directiva **compartida**

   En la directiva de aislamiento compartido, la configuración del balanceador de carga de un arrendatario coexiste con la configuración del balanceador de carga de otros arrendatarios en el dispositivo asignado al arrendatario.

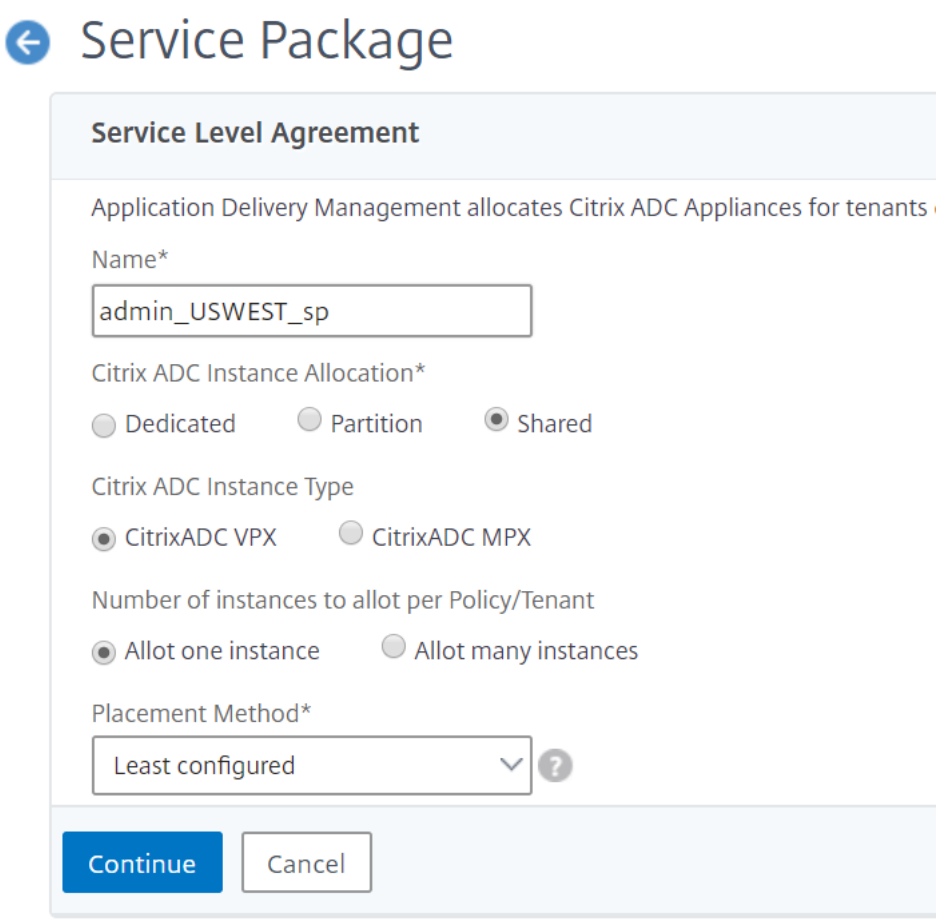
   c) Tipo de dispositivo: seleccione un **Citrix ADC VPX** o **Citrix ADC MPX** previamente aprovisionado

   Seleccione **Asignar un dispositivo** si desea que todas las configuraciones del balanceador de carga de un arrendatario estén vinculadas a un dispositivo. Seleccione **Asignar muchos dispositivos** si desea que cada configuración de balanceador de carga de un arrendatario se distribuya en varios dispositivos según las directivas de ubicación.

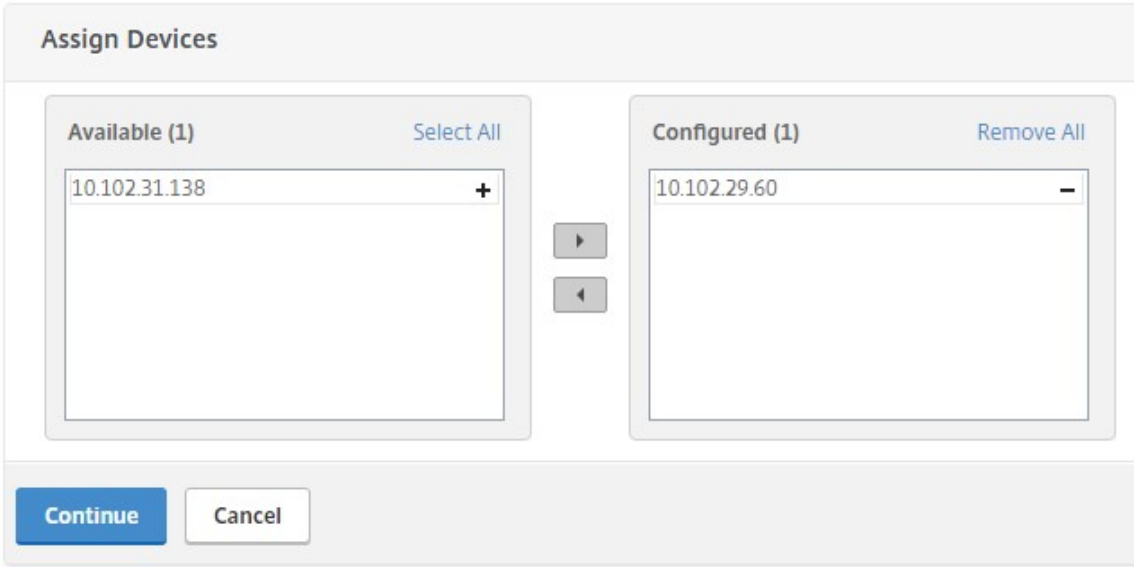
   > **Nota** Citrix ADC SDX debe agregarse a los paquetes de servicios únicamente como instancias de Citrix ADC VPX, ya que un Citrix ADC SDX tiene un Citrix ADC VPX aprovisionado.

   d) Método de colocación: seleccione el **menos configurado**

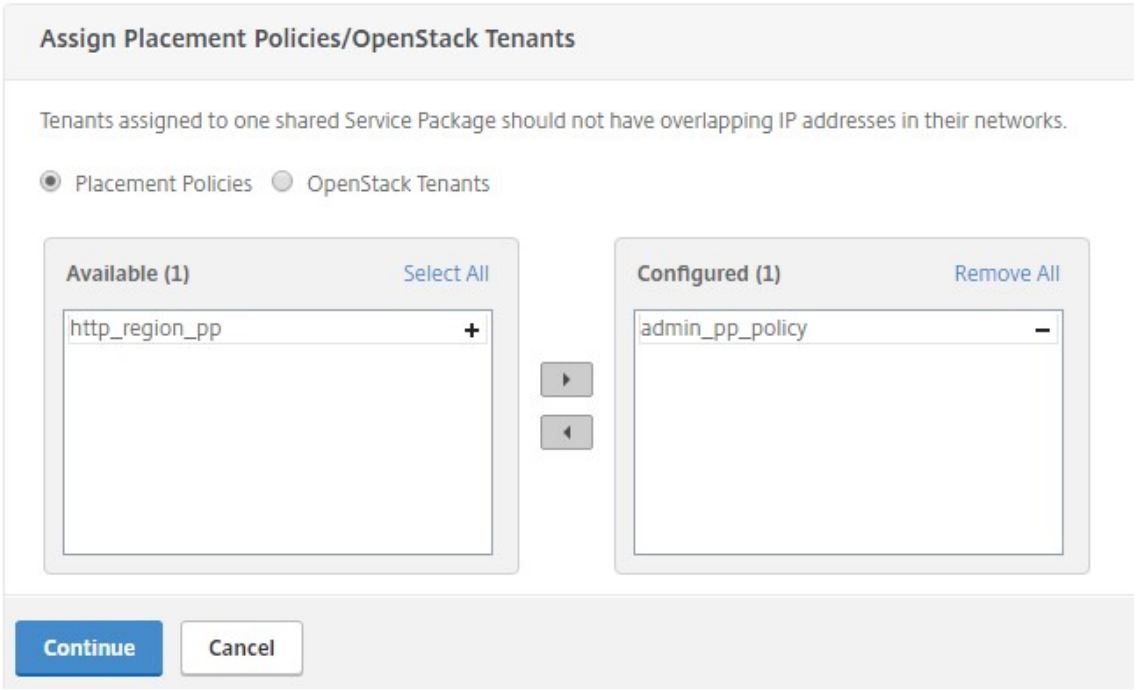
   Cuando se selecciona Menos configurado, se elige como dispositivo para el arrendatario la instancia de NetScaler ADC que tiene el menor número de miembros del grupo configurados en ese momento.



6. Haga clic en **Continuar**.
7. En la sección **Asignar dispositivos**, agregue los dispositivos NetScaler ADC disponibles a la lista de dispositivos configurados.



8. Haga clic en **Continuar**.
9. En la sección **Asignar directivas de ubicación/arrendatarios de OpenStack**, agregue la directiva de ubicación que creó anteriormente.



> **Nota**
>
> Si no se encuentra la directiva, se reviva el mecanismo de reserva y NetScaler ADM asigna instancias de NetScaler ADC basadas en arrendatarios. Si el arrendatario no forma parte de ningún paquete de servicios, NetScaler ADM muestra un mensaje de error que dice: "Tenant\ <admin\ > no forma parte de ningún paquete de servicios y no hay un paquete de servicios predeterminado. "

10. Haga clic en **Continue** y, a continuación, en **Done**.

NSX Manager: Provisioning manual de instancias de NetScaler ADC

January 30, 2024

Citrix Application Delivery Management (ADM) se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios Citrix ADC. Esta integración elimina las complejidades tradicionales asociadas con la topología de la red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios Citrix ADC de forma programática con mayor rapidez.

En este artículo se proporciona una lista de las tareas que debe realizar tanto en VMware NSX Manager como en Citrix ADM.

> **Nota**
>
> Asegúrese de que VMware NSX para vSphere 6.2 y versiones posteriores estén instalados y configurados, y que las puertas de enlace perimetrales, el DLR y las máquinas virtuales que deben tener un equilibrio de carga ya estén creados.

Requisitos previos

- Instale VMware ESXi versión 4.1 o posterior con hardware que cumpla los requisitos mínimos.
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Instale VMware OVF Tool (necesaria para la versión 4.1 de VMware ESXi) en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.
- Instale NetScaler ADM en cualquiera de los hipervisores compatibles.

  Para ver las tareas de instalación de NetScaler ADM compilación 12.1, en cualquiera de los hipervisores compatibles, consulte Implementación de NetScaler ADM.

Requisitos de hardware de VMware ESXi

En la siguiente tabla se enumeran los recursos informáticos virtuales que necesita en el servidor VMware ESXi para instalar un dispositivo virtual Citrix ADM.

Componente	Requisito
RAM	8 GB
CPU virtual	8
Espacio de almacenamiento	500 GB
Interfaces de red virtual	1
Rendimiento	1 Gbps

> **Nota**
>
> Los requisitos de memoria y disco duro especificados anteriormente son para implementar Citrix ADM en el servidor VMware ESXi, teniendo en cuenta que no hay otras máquinas virtuales

> ejecutándose en el host. Los requisitos de hardware del servidor VMware ESXi dependen de la cantidad de máquinas virtuales que se ejecuten en él.

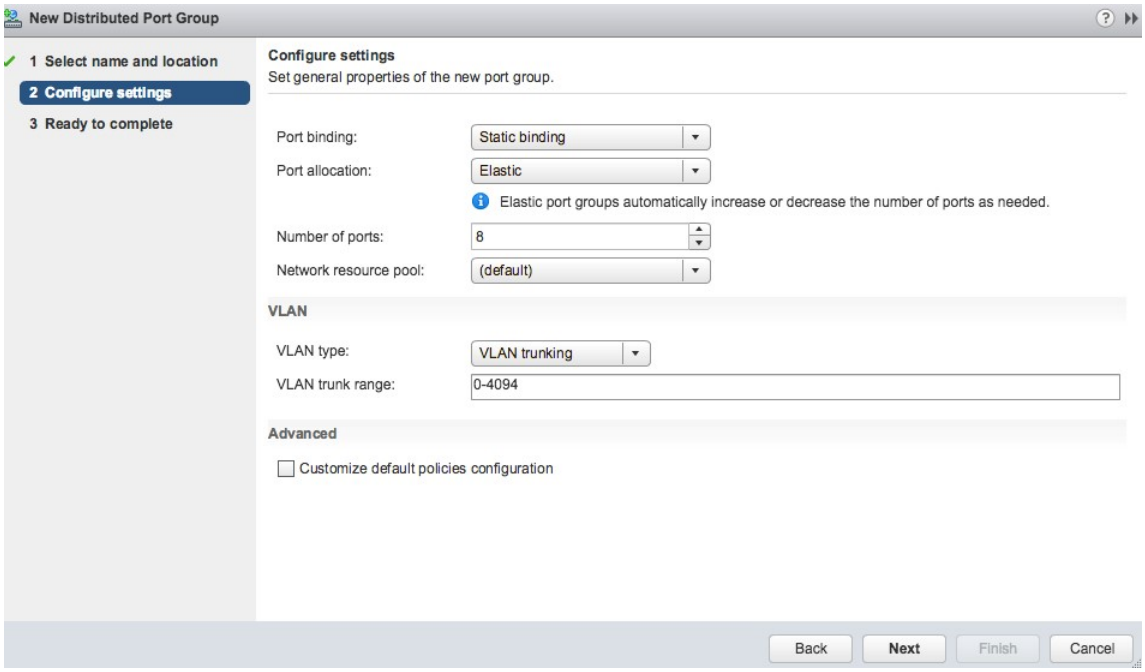
Configuración de VMware NSX

- Cree un grupo de instancias de Citrix ADC VPX de diferentes capacidades, que se agreguen a los diferentes paquetes de servicios.

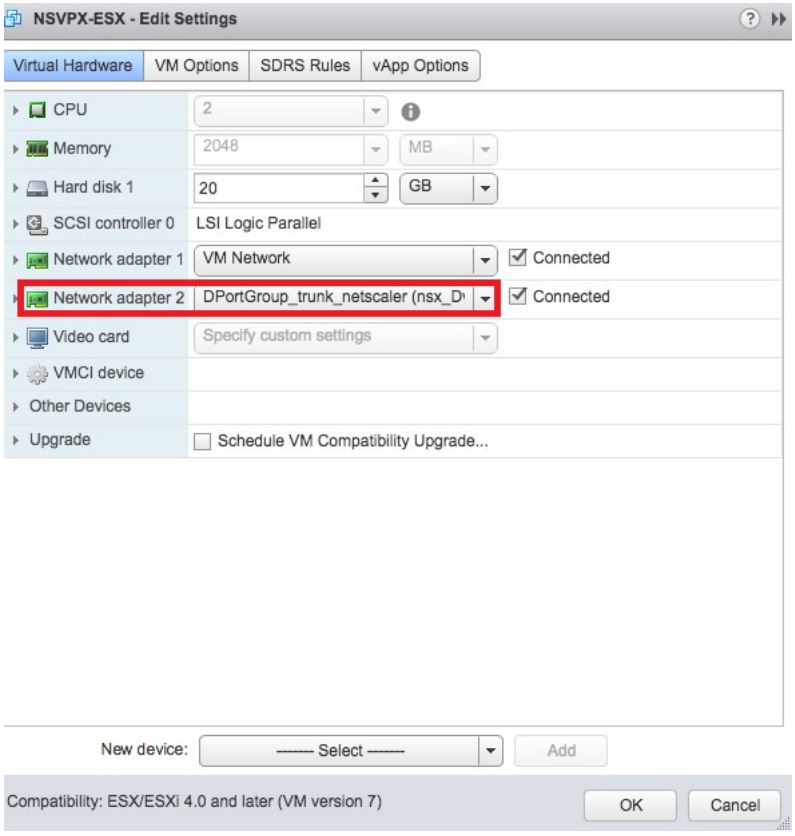
Por ejemplo:

- Cree cinco instancias Citrix ADC VPX de VPX1000 (1 Gbps). Estas instancias se agregan al paquete de servicios Gold.
- Cree cinco instancias Citrix ADC VPX de VPX10 (10 Mbps). Estas instancias se agregan al paquete de servicios Bronze.

1. En el cliente vSphere, vaya a **Redes**y cree un grupo de puertos del tipo VLAN troncal con un rango, por ejemplo, 101-105 (incluso puede proporcionar el rango completo, pero crear un grupo de puertos de tipo VLAN únicamente para las VLAN necesarias).

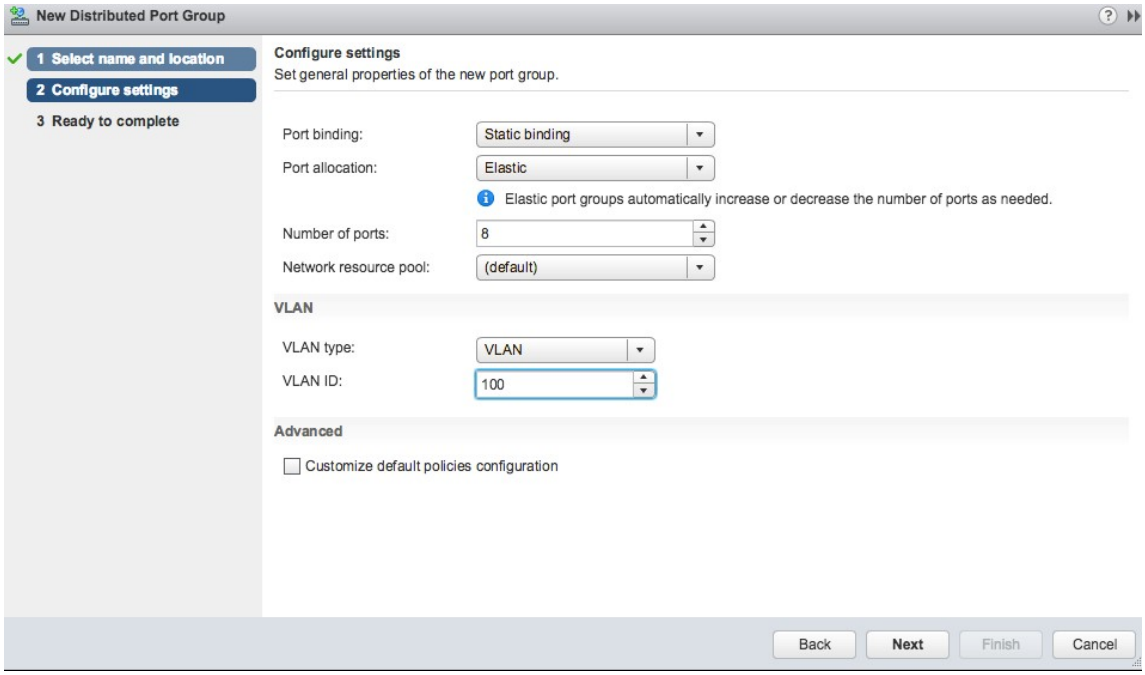


2. Cree una nueva interfaz para cada instancia de NetScaler ADC VPX y conéctela al grupo de puertos troncal de rango de VLAN creado anteriormente.



3. En el cliente vSphere, vaya a **Redes**y cree un grupo de puertos de tipo VLAN.

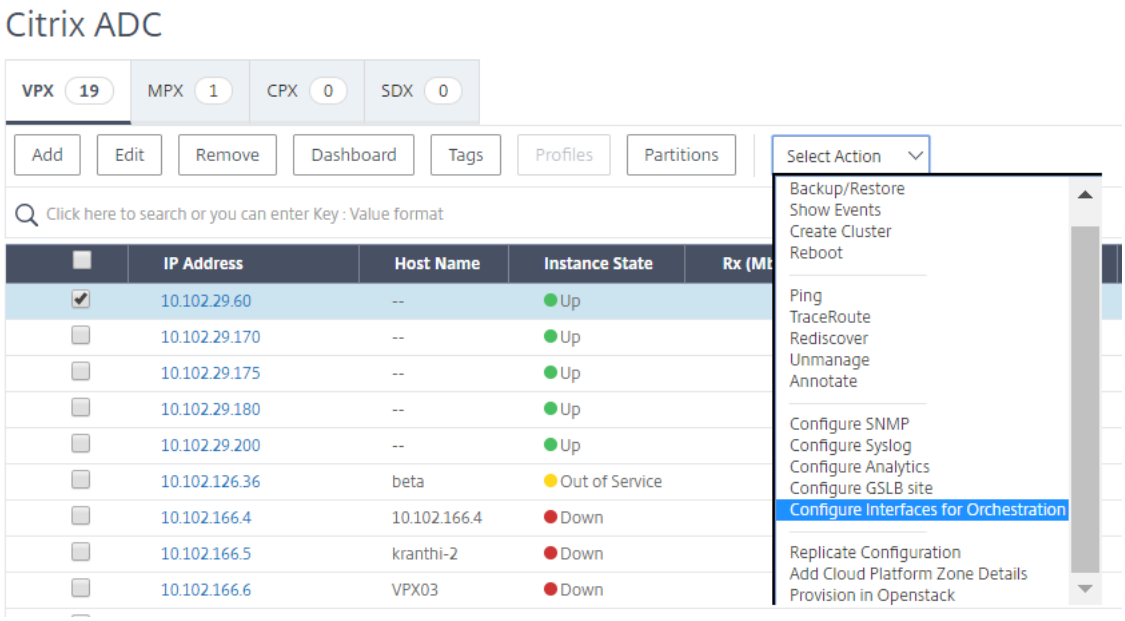
   Por ejemplo, si el grupo de puertos troncal inicial se creó con el rango 101-105, cree cinco grupos de puertos VLAN uno por VLAN, es decir, un grupo de puertos con VLAN 101, otro con VLAN102, etc., hasta VLAN 105.



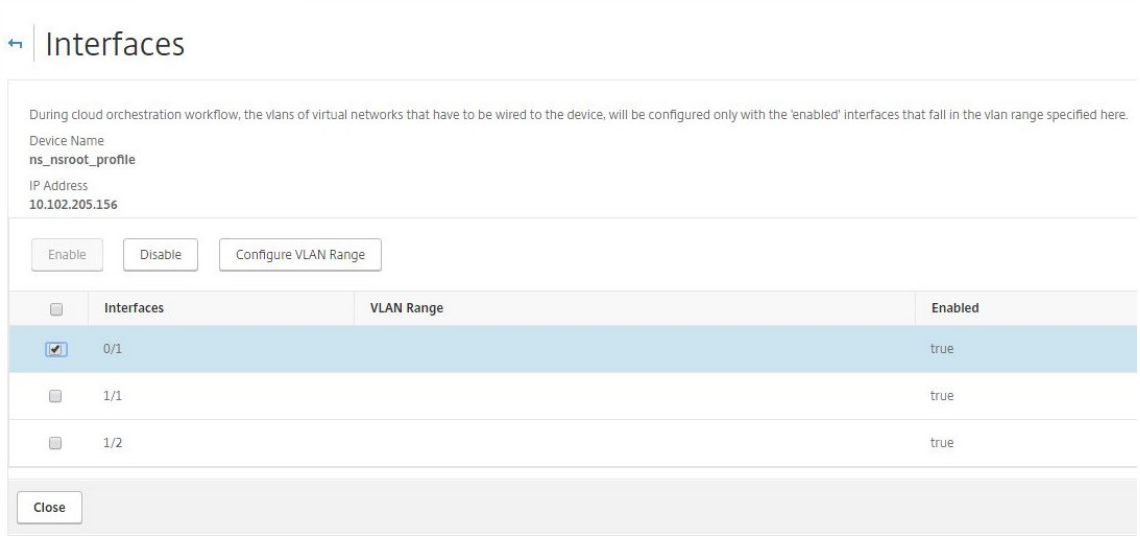
Adición de una instancia NetScaler ADC VPX en NetScaler ADM

Agregue instancias de Citrix ADC VPX en Citrix ADM y especifique el rango de VLAN del grupo troncal para cada dispositivo.

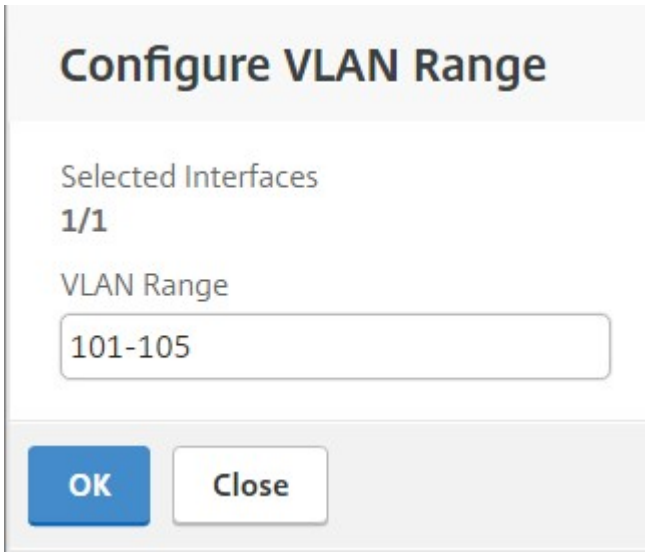
1. En Citrix ADM, vaya a **Infraestructura** > **Instancias** > **Citrix ADC VPX** y haga clic en **Agregar**.
2. En la página **Agregar Citrix ADC VPX** , especifique los nombres de host de las instancias, la dirección IP de cada instancia o un rango de direcciones IP y, a continuación, seleccione un perfil de instancia en la lista de **nombres** de perfil de IP. También puede crear un nuevo perfil de instancia haciendo clic en el icono +.
3. Haga clic en **Aceptar**.
4. Seleccione la instancia de Citrix ADC VPX recién agregada de la lista de la página **Citrix ADC VPX** y haga clic en el botón de flecha hacia abajo del campo **Acción**. Seleccione **Configurar interfaces para orquestación**.



5. En la página **Interfaces**, seleccione la interfaz de administración y haga clic en **Desactivar**para impedir que la VLAN se enlace a la interfaz de administración.



6. En la página **Interfaces**, seleccione la interfaz requerida y haga clic en **Configurar rango de VLAN**.
7. **Introduzca el rango de VLAN configurado en NSX Manager, haga clic en**Aceptar**y, a continuación, en Cerrar.**



Registro de VMware NSX Manager con NetScaler ADM

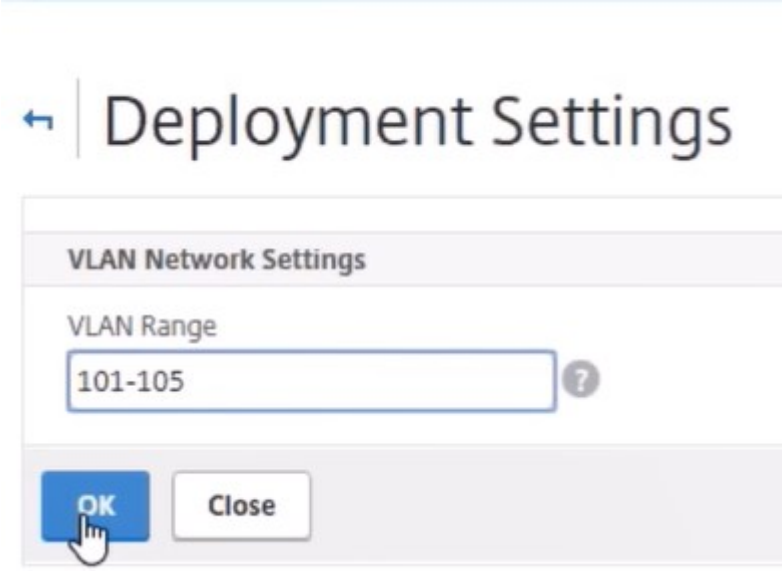
Registre VMware NSX Manager en Citrix ADM para crear un canal de comunicación entre ellos.

1. En Citrix ADM, vaya a **Orchestration** > **SDN OrchestrationVMware NSX Manager**en la lista desplegable y haga clic en**Configurar parámetros de NSX Manager**.
2. En la página **Configurar los ajustes de NSX Manager**, defina los siguientes parámetros:
   a) Dirección IP de NSX Manager: dirección IP de NSX Manager.

b) Nombre de usuario de NSX Manager: nombre de usuario administrativo de NSX Manager.

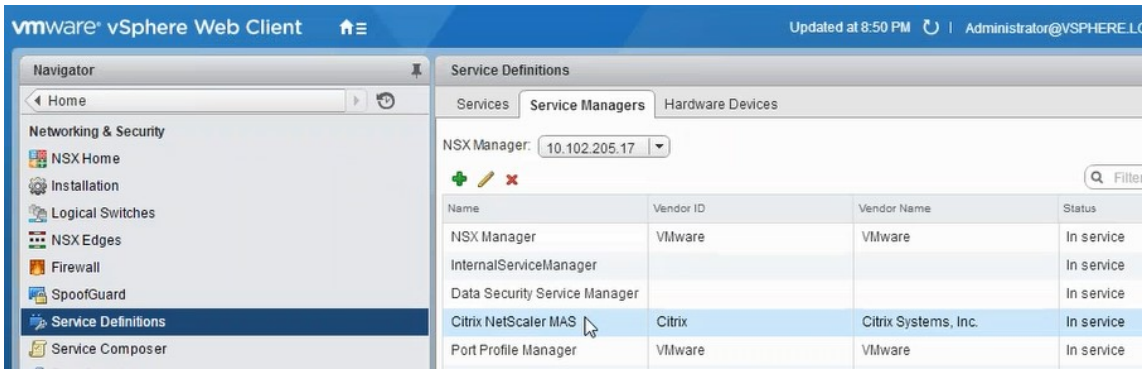
c) Contraseña: Contraseña del usuario administrativo de NSX Manager.

3. En la sección **Cuenta Citrix ADM utilizada por NSX Manager** , defina el nombre de usuario y la contraseña del controlador Citrix ADC para NSX Manager. NetScaler ADM autentica las solicitudes de configuración del equilibrador de carga desde NSX Manager mediante estas credenciales de inicio de sesión.
4. Haga clic en **Aceptar**.
5. Diríjase a **Orquestación** > **Sistema** > **Configuración de implementación.** Proporcione el rango de VLAN que se configuró en el grupo de puertos troncales.



6. Inicie sesión en NSX Manager en vSphere Web Client y vaya a **Definiciones de servicio** > **Administradores de servicio**.

   Puede ver Citrix ADM como uno de los administradores de servicios. Esto indica que el registro es correcto y que se establece un canal de comunicación entre NSX Manager y NetScaler ADM.

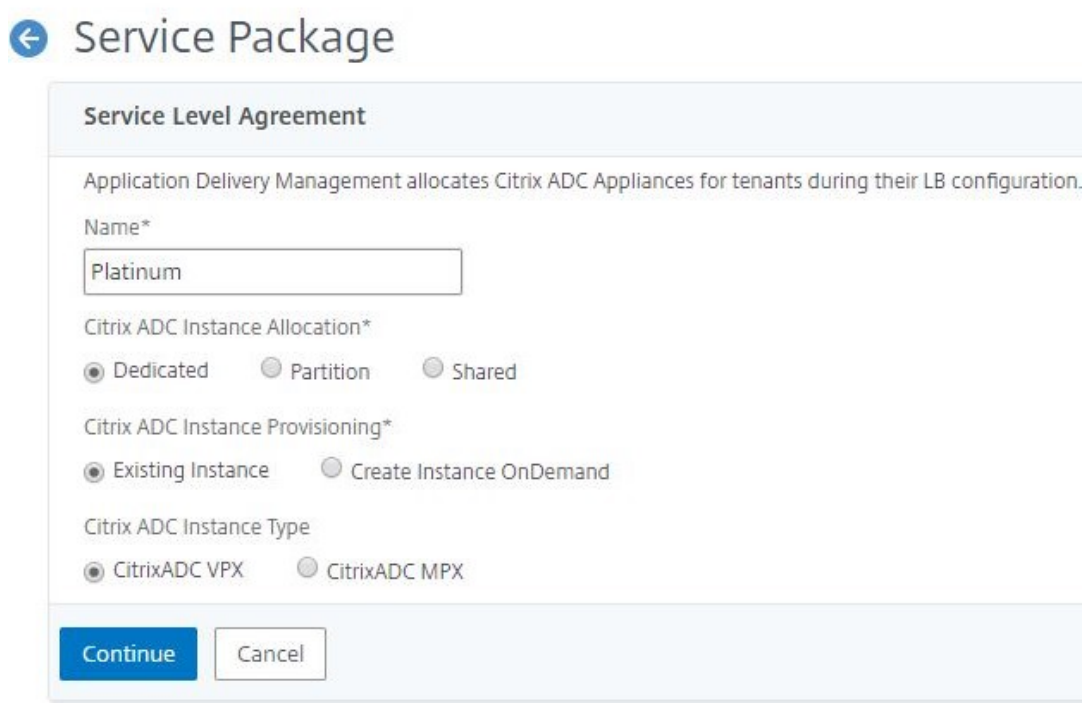


Creación de un Service Package en NetScaler ADM

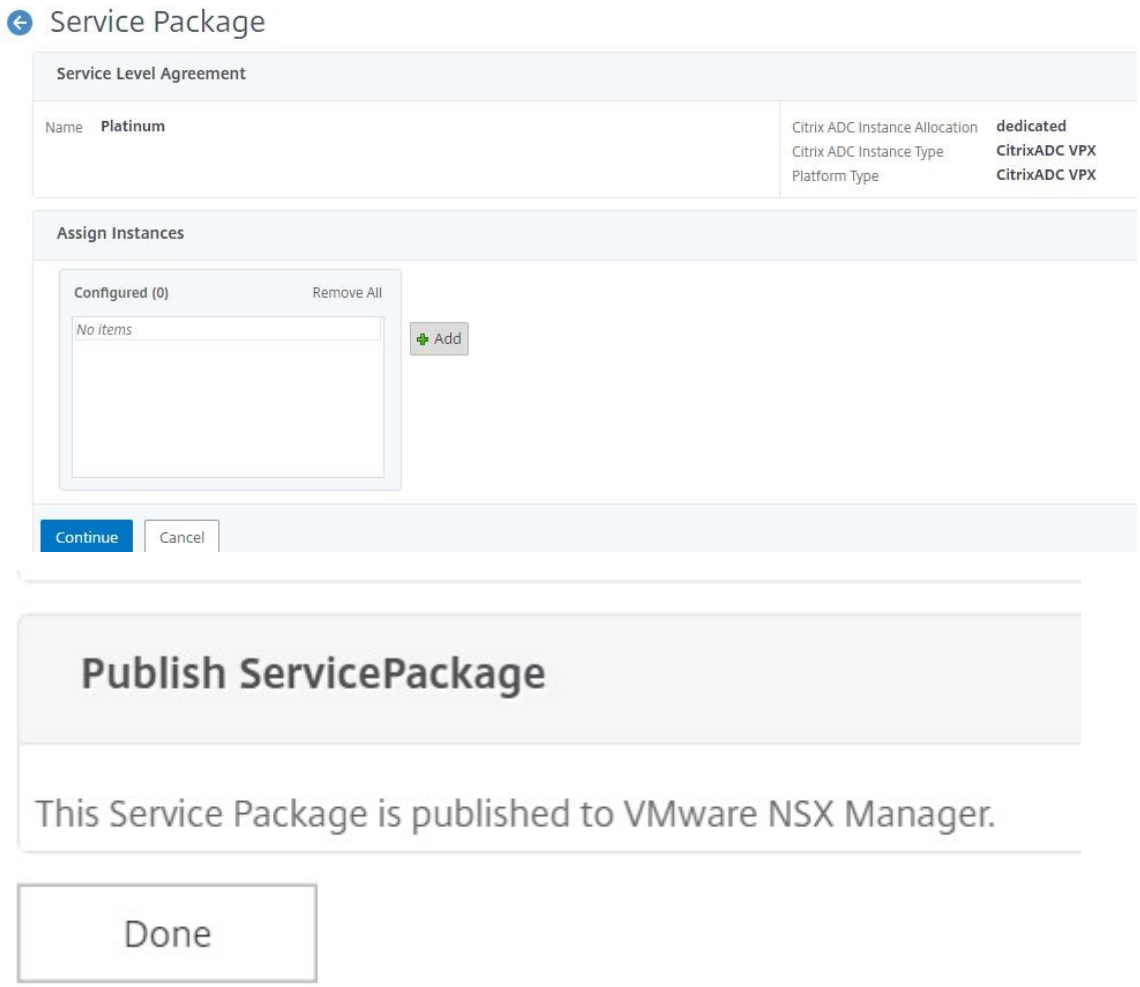
1. En Citrix ADM, vaya a **Orchestration** > **SDN OrchestrationVMware NSX Manager**>**Service Packages**y haga clic en**Agregar** para agregar un nuevo paquete de servicios.
2. En la página **Paquete de servicio**, en la sección **Parámetros básicos**, establezca los siguientes parámetros:
   a) Nombre: escriba el nombre de un paquete de servicios
   b) Directiva de aislamiento: de forma predeterminada, la directiva de aislamiento está configurada como Dedicada
   c) Tipo de dispositivo: de forma predeterminada, el tipo de dispositivo se establece en Citrix ADC VPX

      > **Nota:**
      >
      > Estos valores están configurados de forma predeterminada en esta versión y no se pueden modificar.

   d) Haga clic en **Continuar**.



3. En la sección **Asignar dispositivos**, seleccione el VPX preaprovisionado para este paquete y haga clic en **Continuar**.
4. En la sección **Publicar paquete de servicios**, haga clic en **Continuar** para publicar el paquete de servicios en VMware NSX y, a continuación, haga clic en **Listo**.



Este procedimiento configura un paquete de servicio en NSX Manager. A un servicio se le pueden agregar varios dispositivos y varios bordes pueden usar el mismo paquete de servicios para descargar la instancia de Citrix ADC VPX a Citrix ADM.

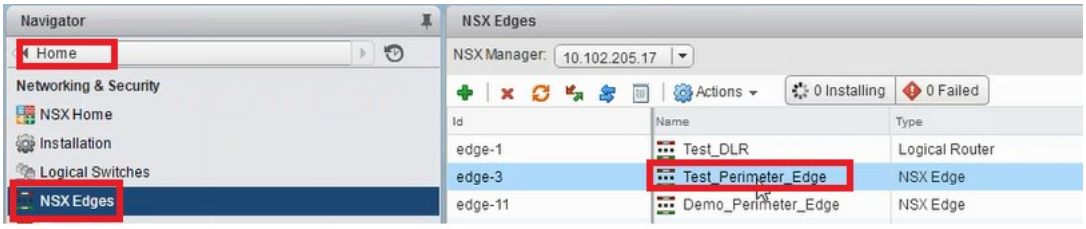
5. **Inicie sesión en NSX Manager en vSphere Web Client y vaya a**Definiciones de servicios**> Servicios.**

   Puede ver que el paquete de servicio NetScaler ADM está registrado.

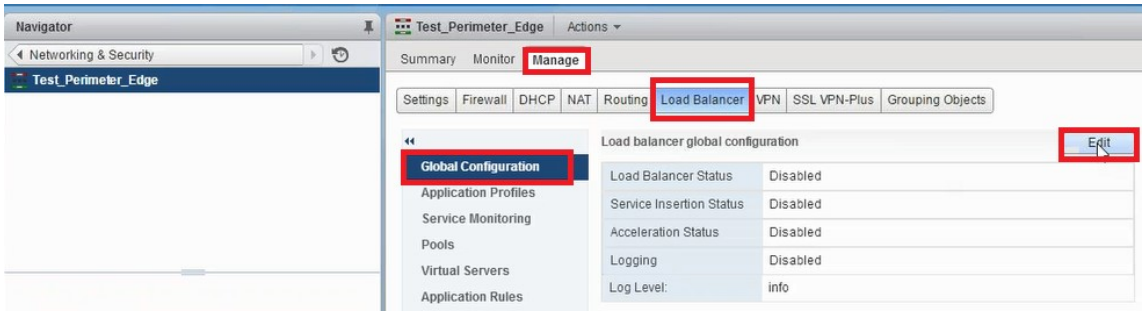
Realización de la inserción del servicio de equilibrador de carga para Edge

Inserte el servicio de equilibrador de carga en la puerta de enlace NSX Edge creada anteriormente (transfiera la función de equilibrio de carga de NSX LB a Citrix ADC).

1. En NSX Manager, vaya a **Inicio** > **NSX Edges**y seleccione la puerta de enlace perimetral que haya configurado.

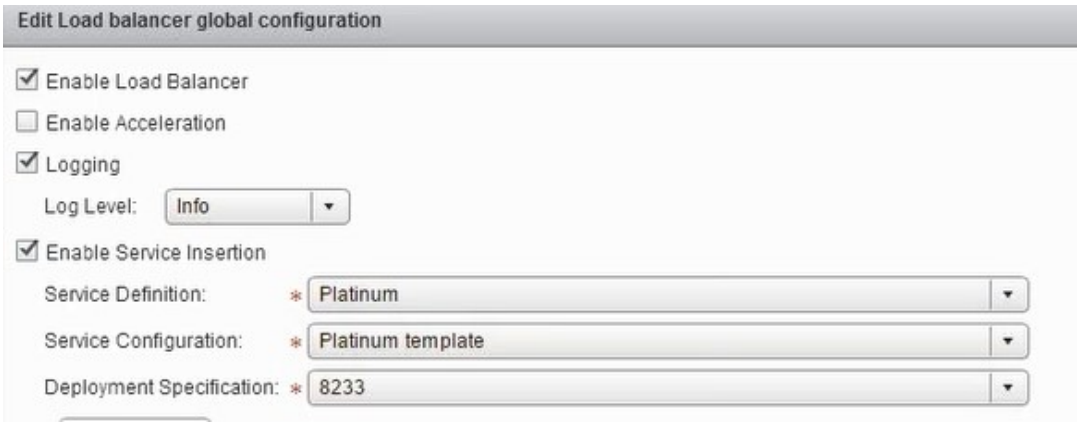


2. Haga clic en **Administrar**y, en la ficha **Equilibrador de carga**, seleccione **Configuración global**y, a continuación, en **Editar**.

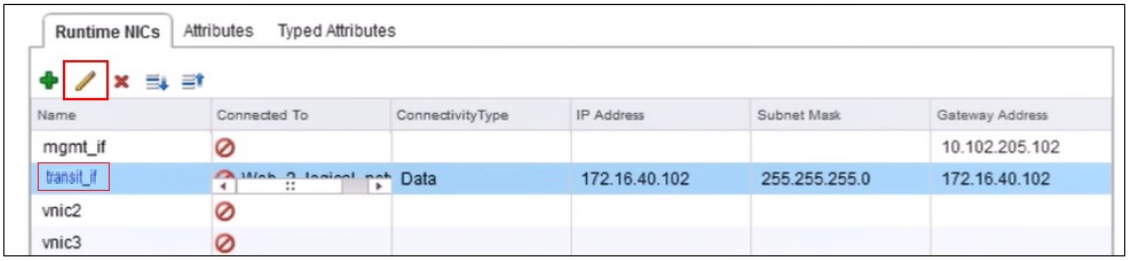


3. Seleccione **Habilitar equilibrador de carga**, **Registro**, **Habilitar inserción de servicios** para habilitarlos.

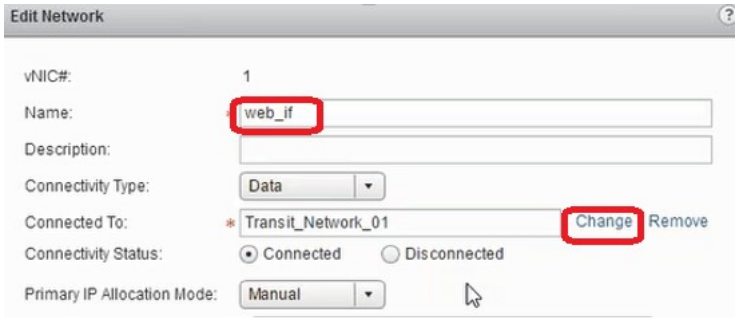
   a) En **Definición de servicio,** seleccione el paquete de servicio creado en NetScaler ADM y publicado en NSX Manager.



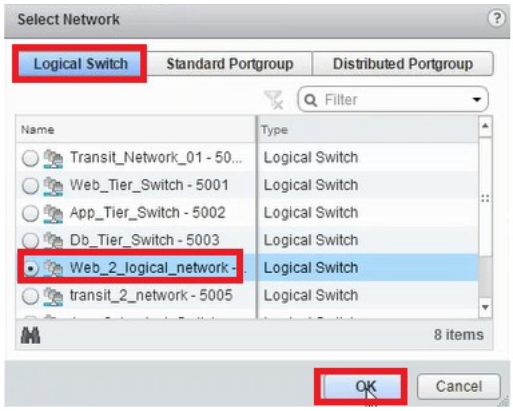
4. Seleccione las NIC en tiempo de ejecución existentes y haga clic en el icono Editar para editar las NIC en tiempo de ejecución que deben conectarse cuando se asigna Citrix ADC VPX.



5. Modifique el nombre de la NIC, especifique el tipo de conectividad como **dato**y haga clic en **Cambiar**.

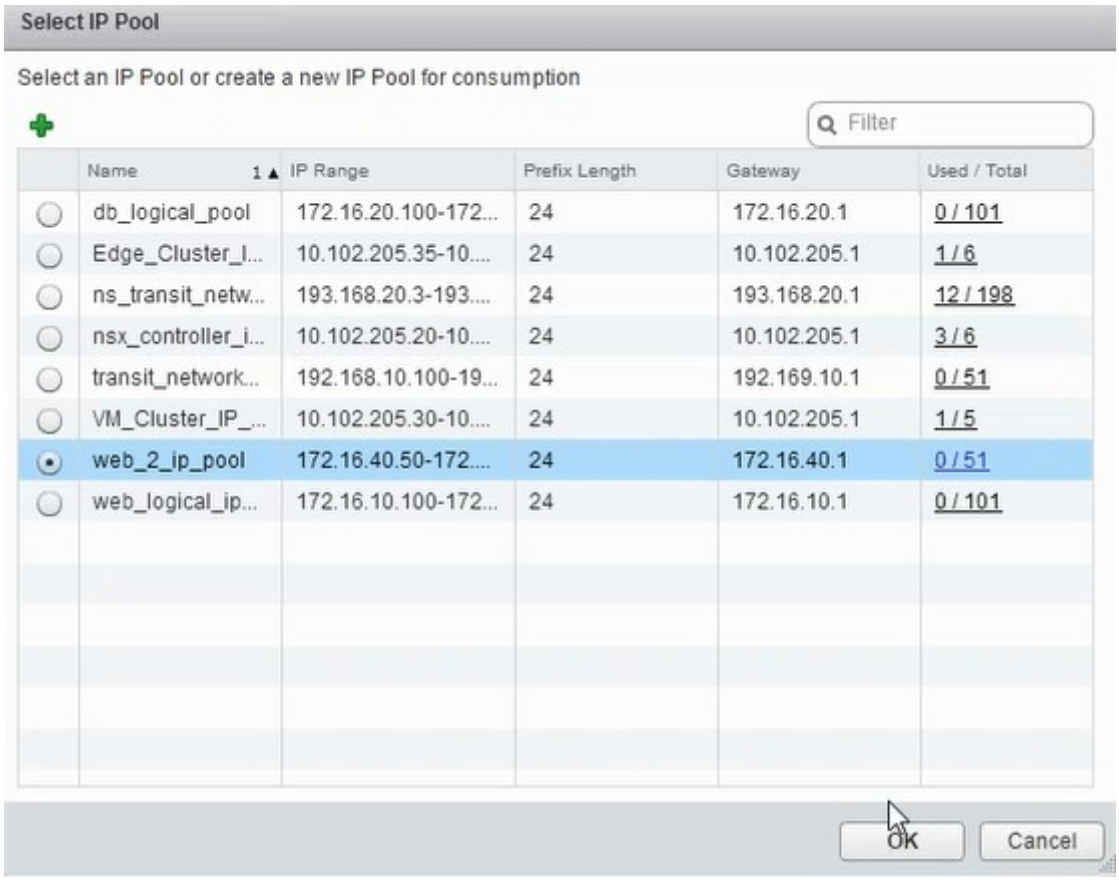


6. Seleccione el conmutador lógico web adecuado.



7. En **Modo de asignación de IP principal**, seleccione Grupo de IP en la lista desplegable y haga clic en el botón de flecha hacia abajo en el campo Grupo de IP.

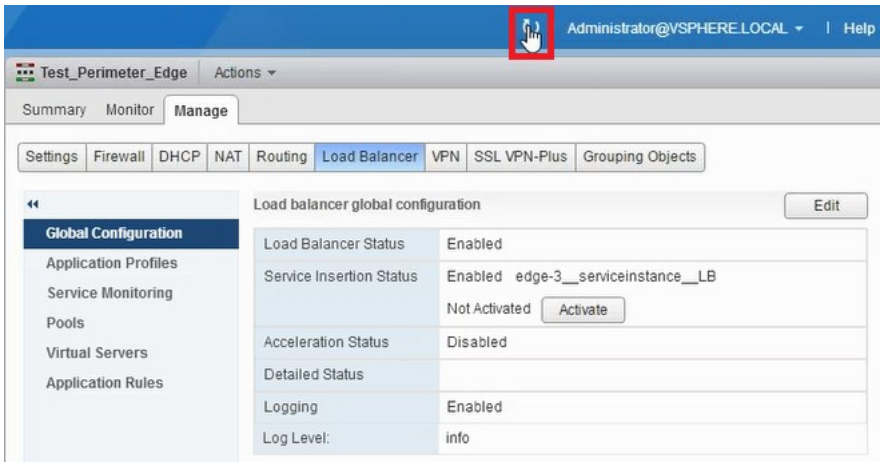
8. En la ventana **Seleccionar grupo de IP**, seleccione el grupo de IP apropiado y haga clic en **Aceptar**.

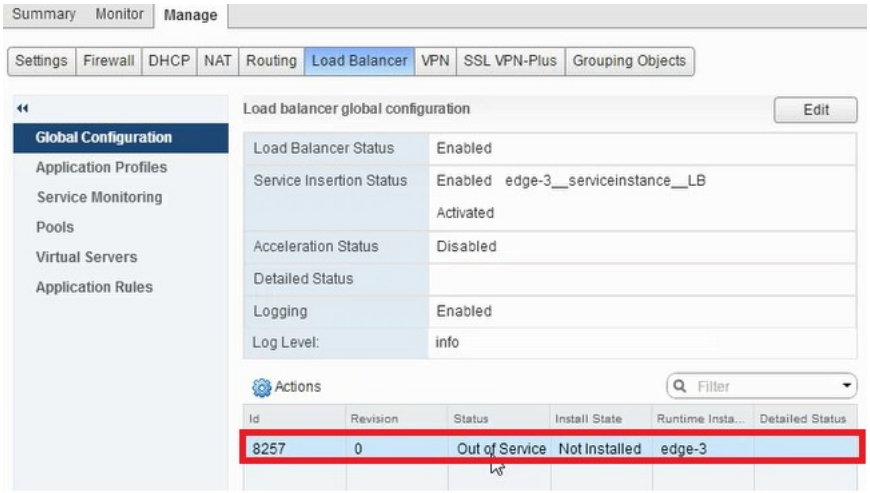


La dirección IP se adquiere y se establece como dirección IP de red de origen en el dispositivo NetScaler ADC VPX. Se crea una Gateway L2 en NSX Manager para asignar la VXLAN a VLAN.

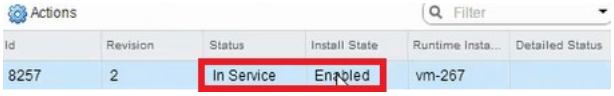
> **Nota** Todas las interfaces de datos están conectadas como NIC en tiempo de ejecución y deben formar parte de las interfaces del DLR.

9. Actualice la vista para ver la creación del tiempo de ejecución.





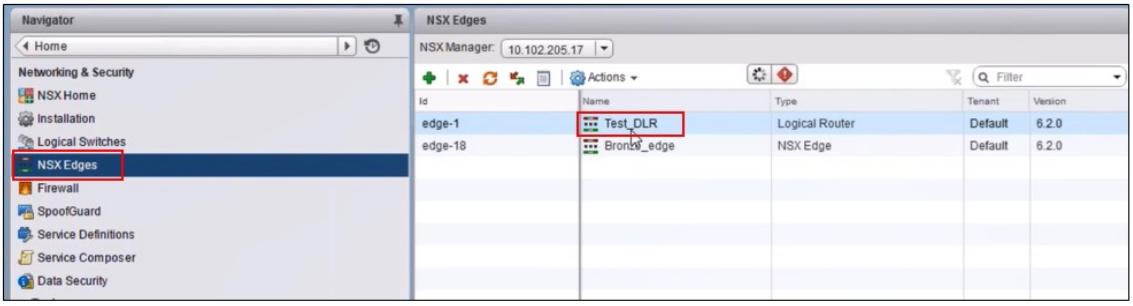
10. Una vez iniciada la máquina virtual, el valor de Estado cambia a **En servicio** y el de Estado de instalación cambia a **Habilitado**.



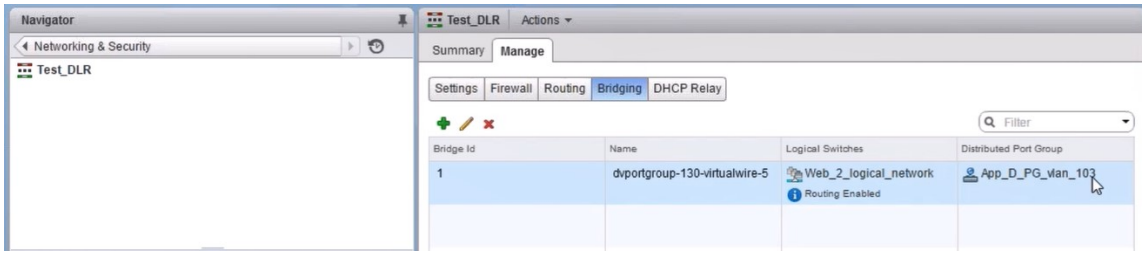
> **Nota**
>
> En NetScaler ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la inserción del servicio LB.

Visualización de L2 Gateway en NSX Manager

1. Inicie sesión en NSX Manager en vSphere Web Client, vaya a **NSX Edges**y seleccione el DLR creado.



2. En la página DLR, vaya a **Administrar** > **Bridging**. Puede ver la Gateway L2 mostrada en la lista.

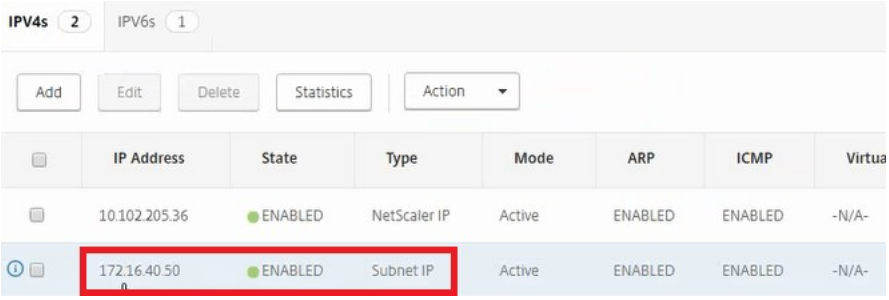


> **Nota**
>
> Se crea una Gateway L2 para cada interfaz de datos.

Visualización de Citrix ADC asignado

1. Inicie sesión en la instancia de Citrix ADC VPX con la dirección IP que se muestra en Citrix ADM. A continuación, vaya a **Configuración** > **Sistema** > **Redes**. En el panel derecho, puede ver que se han agregado las dos direcciones IP. Haga clic en el hipervínculo de dirección IP para ver los detalles.

   La dirección IP de la subred es la misma que la dirección IP de la interfaz web agregada en NSX.



2. Vaya a **Configuración** > **Sistema** > **Licencias** para ver las licencias que se aplican a esta instancia.

Configuración de la instancia de Citrix ADC VPX mediante Stylebook

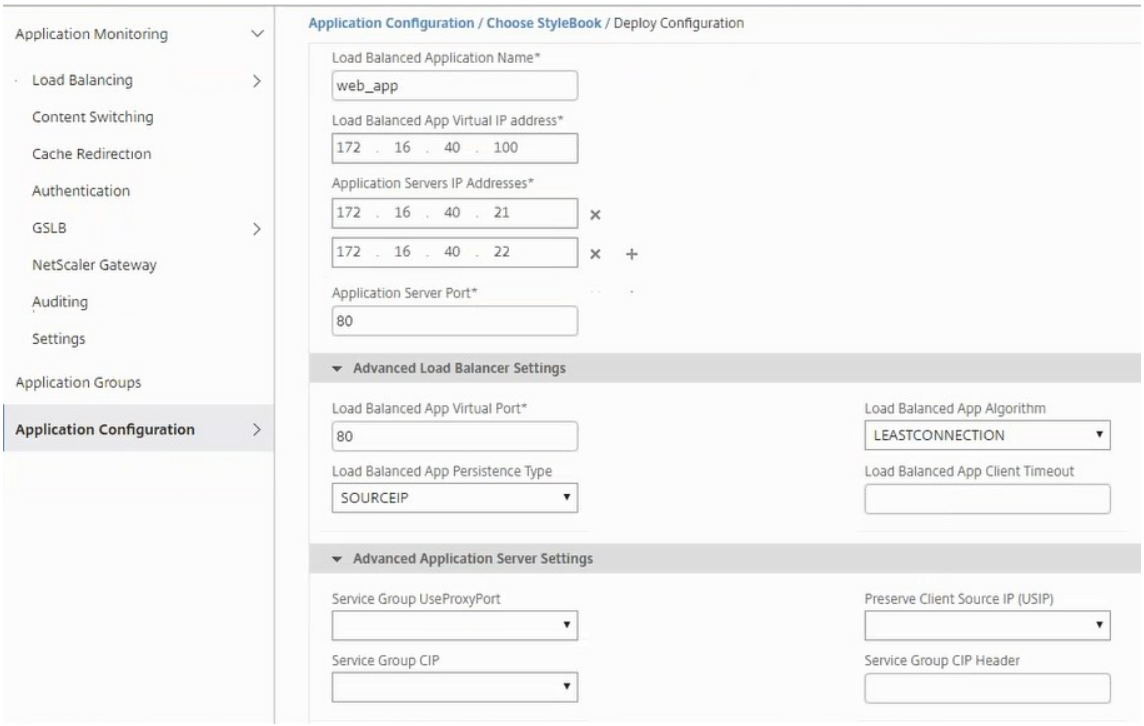
1. En NetScaler ADM, vaya a**Orchestration** >**SDN Orchestration**>**Configure NSX Manager** > **Edge Gateways**.

   Anote la IP de la instancia de Citrix ADC asignada a la puerta de enlace perimetral correspondiente en la que se debe aplicar la configuración de equilibrio de carga a través de Stylebooks.

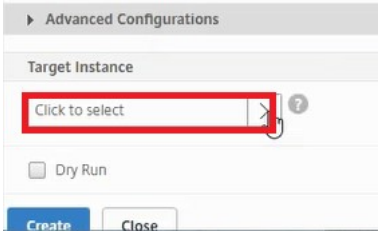
2. Crea un nuevo Stylebook. Vaya a **Aplicaciones** > **Configuración** , importe el StyleBook y seleccione el StyleBook de la lista.

   Para crear un nuevo libro de estilos, consulte Crear su propio libro de estilos.

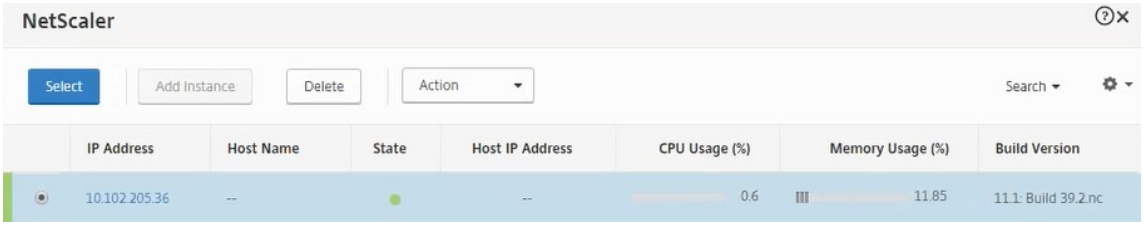
3. Especifique valores para todos los parámetros requeridos.



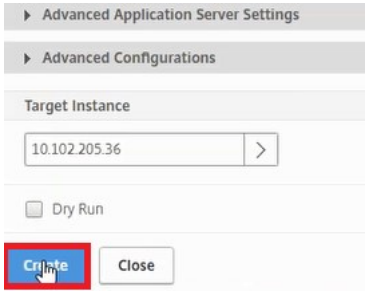
4. Especifique la instancia de Citrix ADC VPX en la que quiere ejecutar estos parámetros de configuración.



5. Seleccione la instancia IP mencionada anteriormente y haga clic en **Seleccionar**.

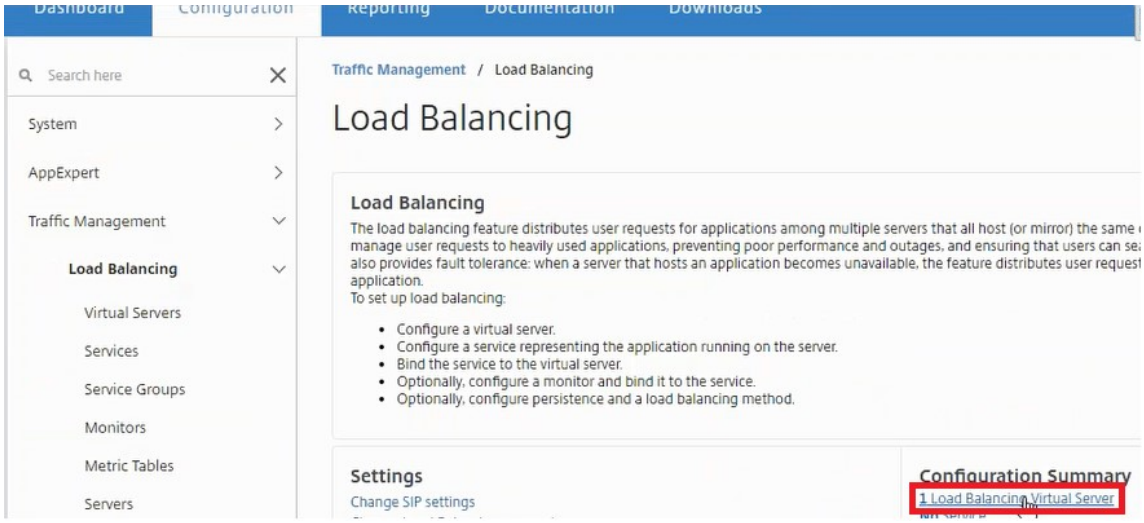


6. Haga clic en **Crear** para aplicar la configuración en el dispositivo seleccionado.

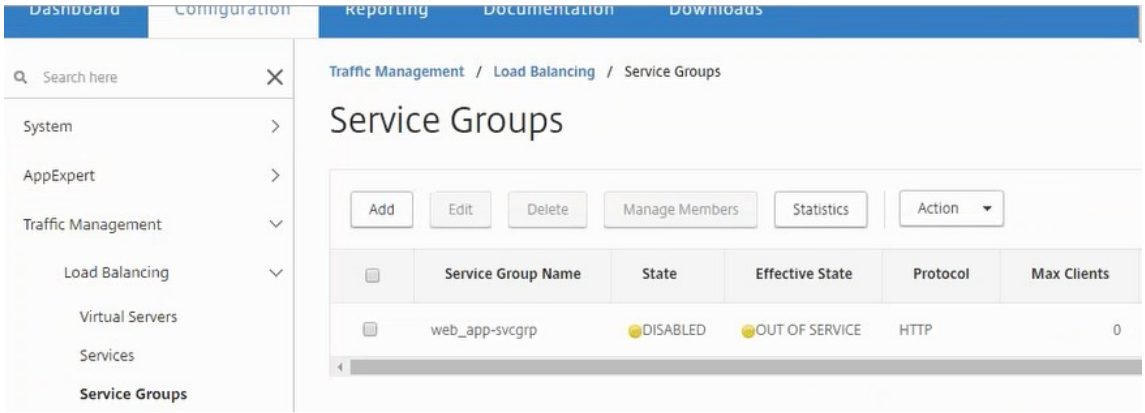


Visualización de la configuración del equilibrador de carga

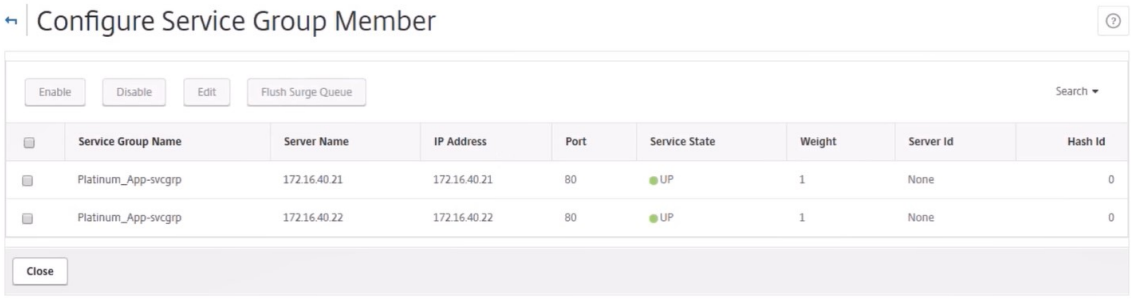
1. Inicie sesión en la instancia de NetScaler ADC VPX, vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** para ver el servidor virtual de equilibrio de carga que se crea.



También puede ver los grupos de servicios que se crean.



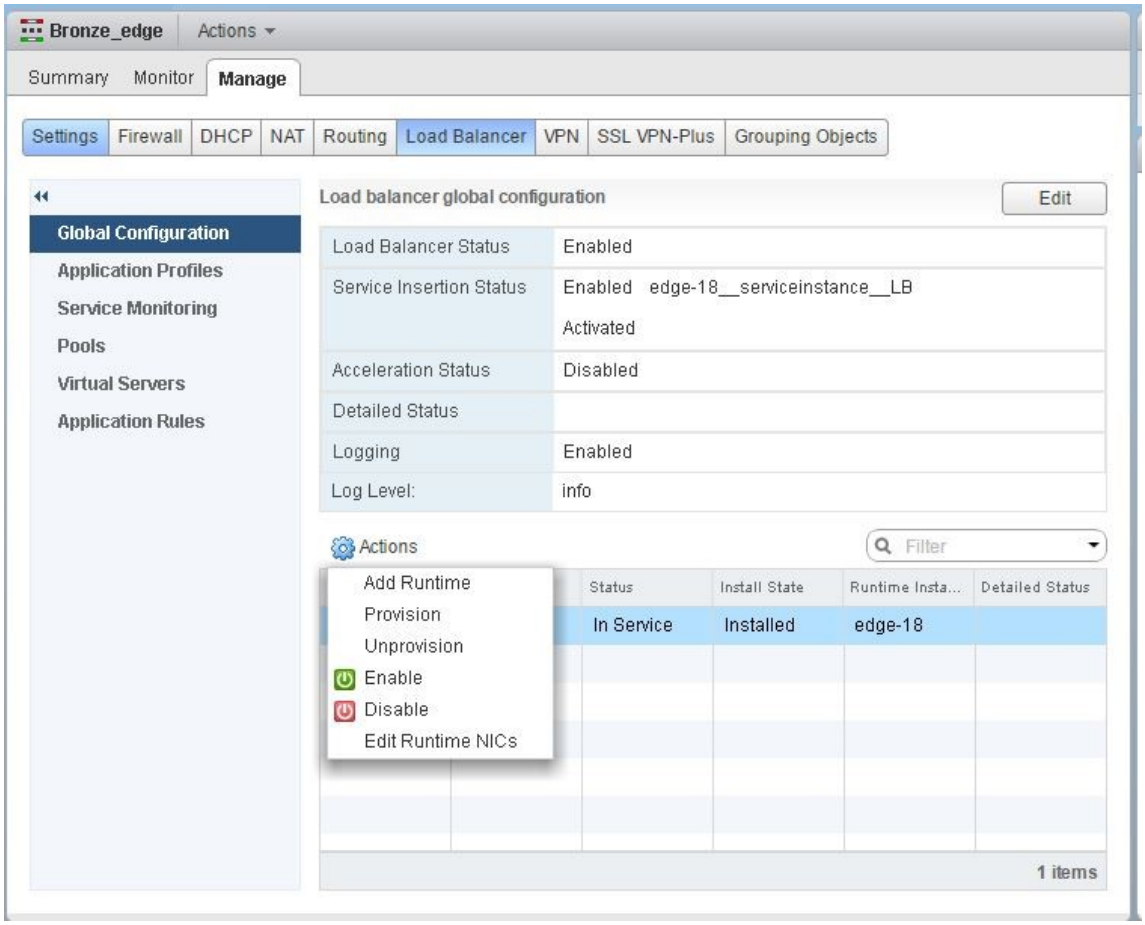
2. Seleccione el grupo de servicios y haga clic en **Administrar miembros**. La página **Configurar Miembro de Grupo de Servicio** muestra los miembros asociados al grupo de servicios.



Eliminación del servicio de equilibrador de carga

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración** y haga clic en el icono **X** para eliminar la configuración de la aplicación.
2. Inicie sesión en NSX Manager en vSphere Web Client y navegue hasta la puerta de enlace perimetral a la que está conectada la instancia de Citrix ADC VPX.
3. Desplácese hasta **Administrar** > **Equilibrador de carga** > **Configuración global**, haga clic con el botón derecho en la entrada de tiempo de ejecución y haga clic en **Anular aprovisionamiento**.

> **Nota** Las puertas de enlace perimetrales de NetScler MAS corresponden a las entradas de tiempo de ejecución de NSX Manager.



La instancia de NetScaler ADC VPX se representa fuera de servicio.

4. En NetScaler ADM, vaya a**Orchestration** >**SDN Orchestration**>**Configure NSX Manager** > **Edge Gateways**. Compruebe que la asignación respectiva de la puerta de enlace perimetral a la instancia eliminada no esté presente.

NSX Manager: Provisioning automático de instancias de NetScaler ADC

January 30, 2024

Overview

Citrix Application Delivery Management (ADM) se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios Citrix ADC. Esta integración elimina las complejidades tradicionales asociadas con la topología de la

red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios Citrix ADC de forma programática con mayor rapidez.

Durante la inserción y eliminación del servicio de equilibrio de carga en VMware NSX Manager, Citrix ADM aprovisiona y destruye dinámicamente las instancias de Citrix ADC. Este aprovisionamiento dinámico requiere que las asignaciones de licencias de Citrix ADC VPX se automaticen en Citrix ADM. Cuando las licencias de Citrix ADC se cargan en Citrix ADM, Citrix ADM desempeña la función de servidor de licencias.

Requisitos previos

> **Nota**
>
> Esta integración solo se admite para **VMware NSX para vSphere 6.1 o versiones anteriores**.

- Citrix ADM, versión 12.1, configurado en alta disponibilidad e instalado en ESX.
- Citrix ADC VPX, versión 12.1
- Licencias de Citrix ADC VPX para instancias de Citrix ADC VPX, versión 12.1
- Instale VMware ESXi versión 4.1 o posterior con hardware que cumpla los requisitos mínimos.
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Instale VMware OVF Tool (necesaria para la versión 4.1 de VMware ESXi) en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.

Implementación de alta disponibilidad de instancias Citrix ADM y Citrix ADC

Para aprovisionar la configuración de NetScaler ADM HA, instale el archivo de imagen NetScaler ADM que ha descargado del sitio de descarga de Citrix. Para obtener más información sobre cómo aprovisionar la configuración de alta disponibilidad de NetScaler ADM, consulte Implementación de NetScaler ADM en alta disponibilidad.

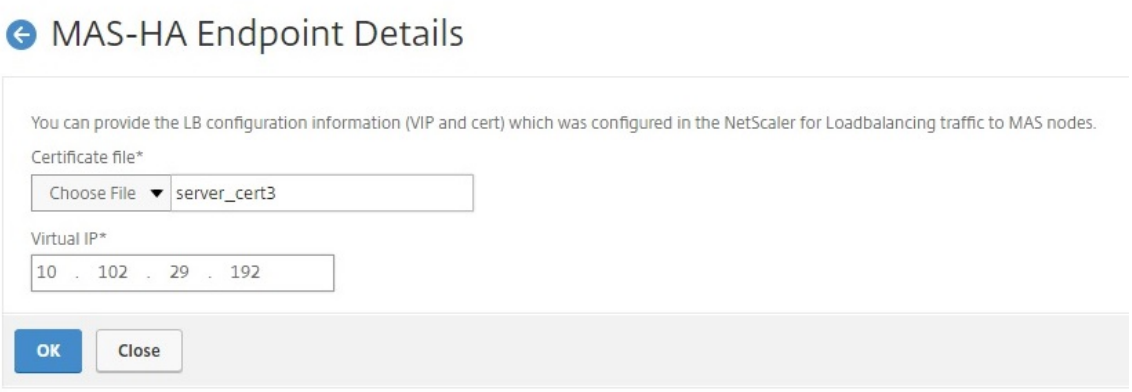
Configuración de detalles de NetScaler ADM HA Endpoint

Para integrar VMware NSX Manager con Citrix ADM implementado en modo HA, primero debe introducir la dirección IP virtual de la instancia de Citrix ADC de equilibrio de carga. También debe cargar el archivo de certificado que está presente en el servidor virtual de equilibrio de carga Citrix ADC al sistema de archivos Citrix ADM.

Para proporcionar información de configuración de equilibrio de carga en Citrix ADM:

1. En el nodo Citrix ADM HA, vaya a **Sistema** > **Implementación**.
2. Haga clic en **Configuración de HA** en la esquina superior derecha y, en la página **Configuración de MAS-HA**, haga clic en **Detalles de extremo de MAS-HA**.

3. En la página **MAS-HA Endpoint Details**, cargue el mismo certificado que ya está presente en la instancia de NetScaler ADC de equilibrio de carga.
4. Introduzca la dirección IP virtual de la instancia de NetScaler ADC de equilibrio de carga y haga clic en **Aceptar**.



Registro de VMware NSX Manager con NetScaler ADM

Al configurar dos servidores Citrix ADM en alta disponibilidad, los dos nodos del servidor están en modo activo-pasivo. Inicie sesión en el nodo principal del servidor Citrix ADM para registrar VMware NSX Manager con Citrix ADM en HA y crear un canal de comunicación entre ellos.

Para registrar VMware NSX Manager con Citrix ADM en HA:

1. En el nodo principal del servidor Citrix ADM, vaya a **Orchestration** > **SDN Orchestration** > **VMware NSX Manager**.
2. Haga clic en **Configurar los ajustes de NSX Manager.**
3. En la página **Configurar los ajustes de NSX Manager**, defina los siguientes parámetros:
   a) Dirección IP de NSX Manager: dirección IP de NSX Manager.
   b) Nombre de usuario de NSX Manager: nombre de usuario administrativo de NSX Manager.

c) Contraseña: Contraseña del usuario administrativo de NSX Manager.

4. En la sección Cuenta Citrix ADM utilizada por NSX Manager, establezca la contraseña del controlador Citrix ADC para NSX Manager.
5. Haga clic en **Aceptar**.

Cargar licencias en Citrix ADM

Cargue las licencias de NetScaler ADC VPX en NetScaler ADM, de modo que NetScaler ADM pueda asignar licencias automáticamente a las instancias durante la orquestación con NSX.

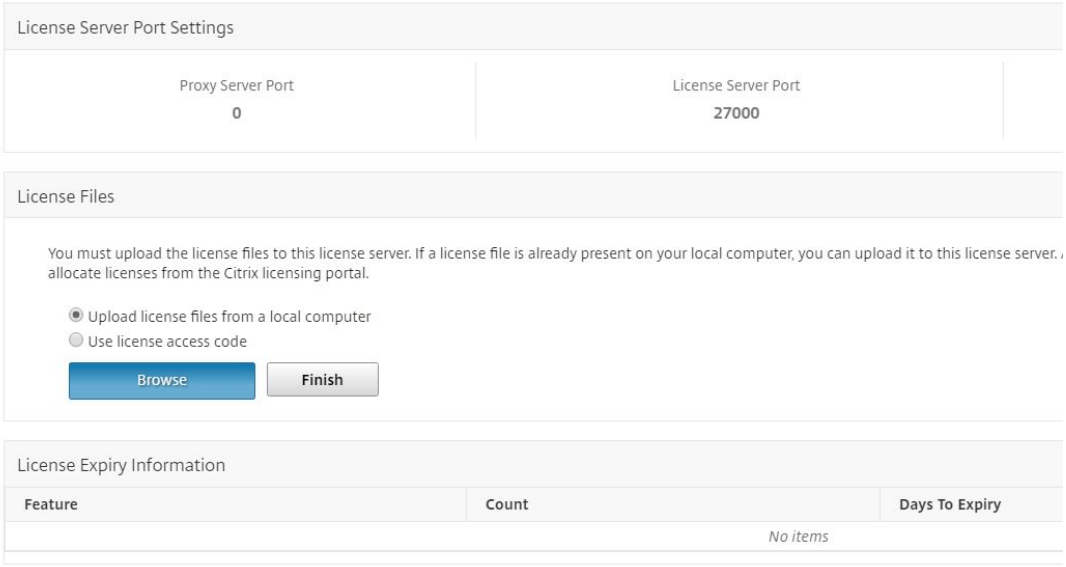
Para instalar archivos de licencia en NetScaler ADM:

1. En Citrix ADM, vaya a **Redes** > **Licencias.**
2. En la sección **Archivos de licencia**, seleccione una de las siguientes opciones:

   a) **Cargar archivos de licencias desde un equipo**local : si ya hay un archivo de licencias en su equipo local, puede cargarlo en Citrix ADM. Para agregar archivos de licencia, haga clic **en**Examinar y seleccione el archivo de licencia (.lic) que desee agregar. Luego haga clic en **Finalizar**.

   b) **Utilice el código**de acceso a la licencia : Citrix envía por correo electrónico el código de acceso a la licencia (LAC) de las licencias que compre. Para agregar archivos de licencia, introduzca el LAC en el cuadro de texto y, a continuación, haga clic en **Obtener licencias** .

   > **Nota**
   >
   > En cualquier momento, puede agregar más licencias a NetScaler ADM desde la Configuración de licencias.



Cargar imágenes de Citrix ADC VPX en Citrix ADM

Agregue las imágenes de NetScaler ADC a NetScaler ADM, de modo que NetScaler ADM utilice estas imágenes tal y como se definen en el paquete de servicio.

Para cargar imágenes de Citrix ADC VPX en Citrix ADM:

1. En NetScaler ADM, vaya a **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Imágenes ESX NSVPX**.
2. Haga clic en **Cargar** y seleccione el paquete zip NetScaler ADC VPX de la carpeta de almacenamiento local.

Crear paquetes de servicios en Citrix ADM

Cree paquetes de servicio en NetScaler ADM para definir el conjunto de SLA, que indica cómo se asignan los recursos de NetScaler ADC.

Para crear paquetes de servicios en Citrix ADM:

1. En Citrix ADM, vaya a **Orchestration** > **SDN OrchestrationVMware NSX Manager**>**Service Packages**y haga clic en**Agregar** para agregar un nuevo paquete de servicios.
2. En la página **Paquete de servicio**, en la sección **Parámetros básicos**, establezca los siguientes parámetros:
   a) Nombre: nombre de un paquete de servicios
   b) Directiva de aislamiento: seleccione **Dedicado**

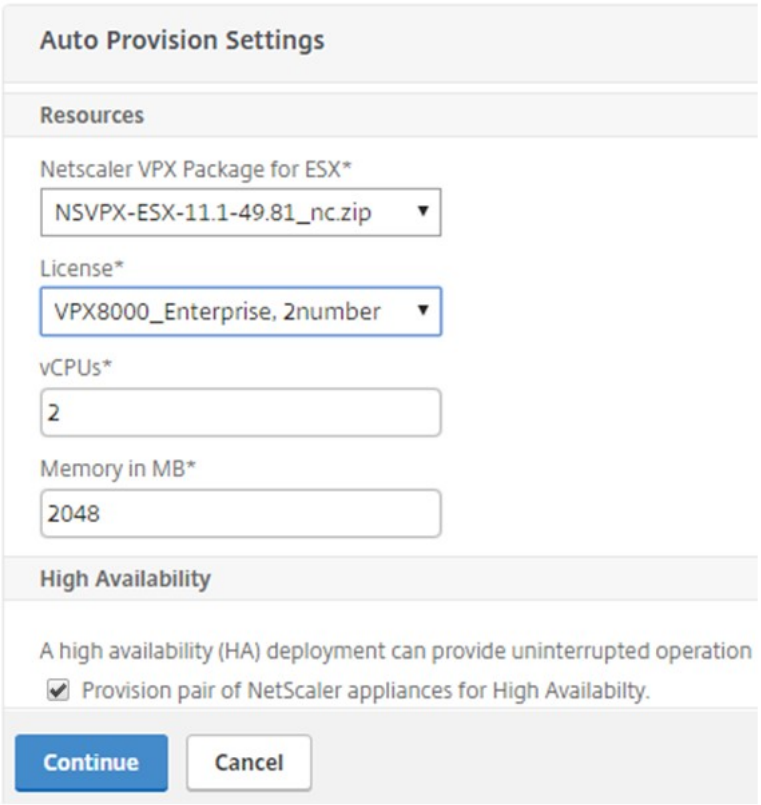
c) Provisioning de instancias de Citrix ADC: seleccione **Crear instancia bajo demanda**

d) Plataforma de aprovisionamiento automático: seleccione **CitrixADC SDX**

e) Haga clic en **Continuar**.

3. En la sección **Configuración de aprovisionamiento automático** , seleccione el paquete zip Citrix ADC VPX cargado recientemente para implementarlo en la plataforma NSX, seleccione la licencia correspondiente y haga clic en **Continuar**.

> **Nota**
>
> En la sección **Alta disponibilidad**, marque la casilla para aprovisionar instancias de NetScaler ADC para alta disponibilidad.



> **Nota**
>
> El nombre de la licencia que aparece en el cuadro de lista que se muestra en la figura anterior, VPX8000_Enterprise, 2number, es un ejemplo y se explica a continuación:
>
> - VPX: La licencia es implementar instancias de NetScaler ADC VPX
> - 8000: el ancho de banda consumible es de 8 GB

> - Enterprise: Citrix ofrece tres tipos de licencias: Standard, Enterprise y Platinum
> - 2number: Se pueden implementar dos instancias de NetScaler ADC VPX mediante esta licencia
>
> **El nombre de la licencia que se muestra en el cuadro de lista Licencia depende de la licencia que haya adquirido en Citrix.**

4. Haga clic en **Continuar**.
5. El paquete de servicios se publica en NSX Manager. En NSX Manager, vaya a **Definiciones de servicios** > **Administradores de servicios**. Puede ver Citrix ADM como uno de los administradores de servicios. Esto indica que el registro se ha realizado correctamente y que se ha establecido una comunicación bidireccional entre NSX Manager y Citrix ADM.

> **Nota**
>
> Para Citrix ADM en una implementación de alta disponibilidad, las licencias solo se cargan en el nodo del servidor de licencias Citrix ADM. Los nodos NetScaler ADM están en modo activo-pasivo.

Realice la inserción del servicio de balanceador de carga para Edge

Realice la inserción del servicio de equilibrador de carga en la puerta de enlace NSX Edge existente, es decir, descargue la función de equilibrio de carga del equilibrador de carga de NSX a NetScaler ADC.

Para insertar el servicio de equilibrio de carga en NSX Edge Gateway:

1. En NSX Manager, vaya a **Inicio** > **Redes y seguridad** > **NSX Edges**y haga doble clic para seleccionar la puerta de enlace perimetral que ha configurado.
2. Haga clic en **Administrar**y, en la ficha **Equilibrador de carga**, seleccione **Configuración global**y, a continuación, en **Editar**.
3. Seleccione **Habilitar balanceador de carga** y **Habilitar inserción de servicios** para habilitarlas.
4. En **Definición de servicio**, seleccione el paquete de servicios que se publicó en NSX Manager.
5. Configure una NIC virtual para la interfaz de administración y una o más NIC virtuales para las interfaces de datos. Seleccione las redes para la administración y los datos en consecuencia.

> **Nota**
>
> Seleccione la opción Grupo de direcciones IP en el modo de asignación de IP principal. Citrix ADM no admite la asignación manual o DHCP de direcciones IP.

6. Haga clic en el icono de actualización para ver la creación del tiempo de ejecución.

> **Nota**
>
> Como se implementan dos instancias de Citrix ADC VPX en una implementación de alta disponibilidad, se crean dos tiempos de ejecución en NSX Manager.
>
> Puede que tengas que actualizar la pantalla para ver los tiempos de ejecución que aparecen en la pantalla.

7. Seleccione el tiempo de ejecución, haga clic en **Acciones**y, en el menú emergente, seleccione **Instalar**. Para HA, repita esto también para el otro tiempo de ejecución.
8. Cuando se inician ambas máquinas virtuales, el valor de Estado cambia a "En servicio"y el de Estado de instalación cambia a "Habilitado".

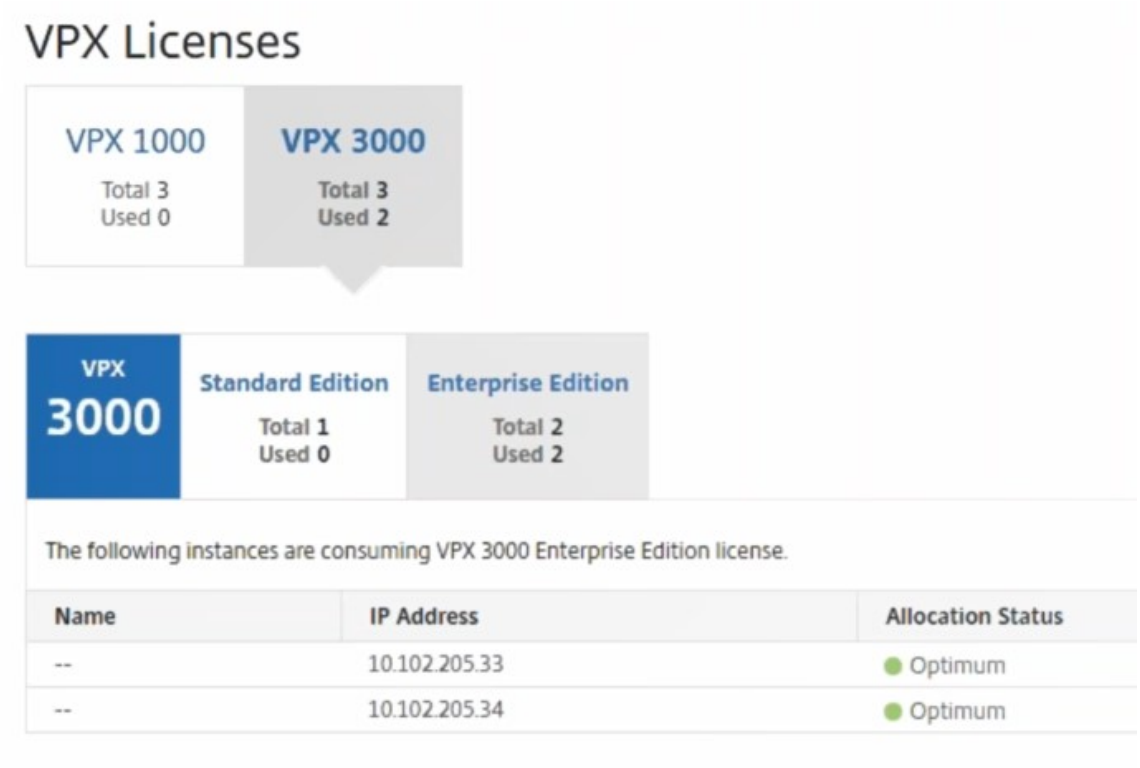
   > **Nota**
   >
   > Puede que tenga que actualizar la pantalla para ver el cambio de estado.

9. En Citrix ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la inserción del servicio. Puede ver que ha llegado a Citrix ADM una solicitud para crear y actualizar el tiempo de ejecución. Cuando se haya actualizado el tiempo de ejecución, seleccione la solicitud y haga clic en el botón **Tareas** para ver si Citrix ADM se ha agregado a NSX Manager.

   Para HA, habrá dos solicitudes para crear y actualizar dos tiempos de ejecución en Citrix ADM. Cuando se hayan actualizado ambos tiempos de ejecución, seleccione ambas solicitudes y haga clic en el botón **Tareas** para ver si se han agregado dos nodos Citrix ADM HA en NSX Manager.
10. En Citrix ADM, vaya a **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Edge Gateways**. En el panel lateral derecho, puede ver que el Citrix ADC VPX se ha agregado a NSX Edge Gateway.

    Para HA, puede ver que se han agregado dos instancias de NetScaler ADC VPX en modo HA a NSX Edge Gateway.
11. En Citrix ADM, vaya a **Redes** > **Licencias** > **Licencias VPX** . Seleccione la licencia NetScaler ADC VPX y la edición que haya instalado.

    Las instancias de NetScaler ADC VPX que están en modo HA consumen dos licencias y el estado se muestra en la pantalla como se muestra a continuación.



Una vez completada la inserción del servicio, puede utilizar StyleBooks para configurar las instancias de NetScaler ADC en uno de los dos métodos siguientes:

- Configurar los servicios de equilibrio de carga en Citrix ADC VPX en la GUI de VMware NSX Manager
- Configurar los servicios de equilibrio de carga en Citrix ADC VPX en la GUI de Citrix ADM

Configurar los servicios de equilibrio de carga en Citrix ADC VPX en la GUI de VMware NSX Manager

Realice la siguiente tarea para habilitar la configuración de los servicios de equilibrio de carga en el dispositivo de Gateway de NSX Edge mediante StyleBooks integrados.

En NSX Manager, vaya a **Inicio** > **Redes y seguridad** > **NSX Edges**y haga doble clic para seleccionar la puerta de enlace perimetral que ha configurado.

Creación de grupos y miembros de grupos

Cree un grupo de servidores y miembros de diferentes capacidades.

1. Haga clic en **Administrar**y, en la ficha **Equilibrador de cargas**, seleccione **Grupos**y, a continuación, haga clic en el icono "**+**"para agregar un nuevo grupo y configurar los siguientes

parámetros:

a) Nombre: nombre del nuevo grupo

b) Algoritmo: seleccione un algoritmo de la base de la lista desplegable en el que se seleccionará el grupo.

c) Monitores: asegúrese de que el monitor de servicio esté configurado en default_http_monitor

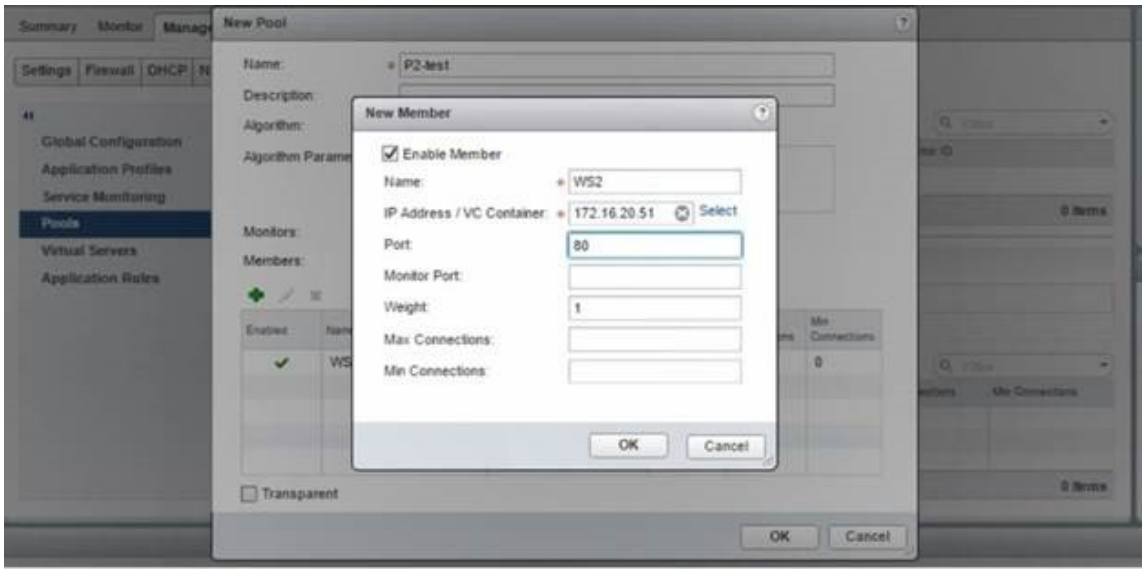
d) Miembros: haga clic en "+"para agregar miembros al grupo e introduzca los parámetros necesarios en la ventana Nuevo miembro.

i. Nombre: nombre del miembro

ii. Dirección IP/contenedor VC: haga clic en Seleccionar para seleccionar el objeto de la lista disponible o introducir la dirección IP del objeto.

2. Haga clic en **Aceptar**.

Agregue tantos miembros como sea necesario.



Creación de servidores virtuales

Cree un conjunto de servidores virtuales y asigne un grupo a cada servidor virtual.

1. Haga clic en **Administrar**y, en la ficha Equilibrador de carga, seleccione **Servidores virtuales**y, a continuación, haga clic en el icono "**+**"para agregar un servidor virtual y establezca los siguientes parámetros:

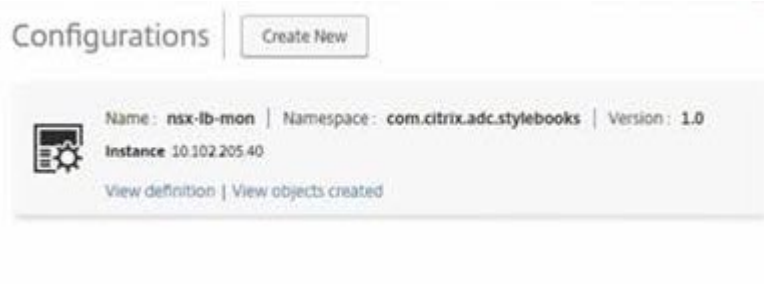
a) Perfil de aplicación: de forma predeterminada, se muestra el perfil de servicio que creó en Citrix ADM.

b) Nombre: nombre del servidor virtual.

c) Dirección IP: haga clic en Seleccionar para seleccionar un grupo de direcciones IP existente o crear un grupo nuevo de direcciones IP.

d) Grupo predeterminado: seleccione el grupo predeterminado de la lista desplegable.

2. Haga clic en **Aceptar**.
3. En NetScaler ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la creación del servicio en una o más instancias de NetScaler ADC seleccionadas.
4. En Citrix ADM, vaya a **Aplicaciones** > **Configuración** y compruebe que se ha creado el paquete de configuración «nsx-lb-mon».



Configurar los servicios de equilibrio de carga en Citrix ADC VPX en la GUI de Citrix ADM

Implemente configuraciones del equilibrador de carga en la instancia de NetScaler ADC mediante NetScaler ADM StyleBooks. Para HA, la configuración se implementa en las dos instancias de Citrix ADC que están en HA.

Para crear paquetes de configuración mediante StyleBooks:

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración** > **Crear nuevo** y seleccione el **StyleBook HTTP/SSL LoadBalancing (con monitores)** de la lista. El StyleBook se abre como una página de interfaz de usuario en la que se introducen los valores de todos los parámetros definidos en este StyleBook.
2. Especifique valores para todos los parámetros requeridos.
3. Seleccione la instancia Citrix ADC VPX de destino que está aprovisionada en el entorno NSX y haga clic en **Crear** para aplicar la configuración en el dispositivo seleccionado. Para la implementación de alta disponibilidad, seleccione las instancias que están en modo de alta disponibilidad.

Verifique la creación de servidores virtuales y grupos de servicios en instancias de Citrix ADC VPX

Puede ver que los grupos de servicios y los servidores virtuales se crean iniciando sesión en la instancia de Citrix ADC VPX.

Para ver los grupos de servicios y los servidores virtuales:

1. Inicie sesión en la instancia de NetScaler ADC VPX. Para la implementación de HA, debe iniciar sesión en las dos instancias de Citrix ADC que estén en HA.
2. Vaya a **Configuración** > **Sistema** > **Redes**. En el panel derecho, puede ver las direcciones IP que se han agregado. Haga clic en el hipervínculo de dirección IP para ver los detalles. Puede ver que la dirección IP de la subred es la misma que la dirección IP de la interfaz web que se agregó a NSX.
3. A continuación, vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y consulte los detalles del servidor virtual.
4. A continuación, vaya a **Grupos de servicios** y consulte los detalles del grupo de servicios.
5. Por último, vaya a **Configuración** > **Sistema** > **Licencias** para ver las licencias que se aplican a esta instancia.

Eliminar los servicios de equilibrio de carga

Cuando los servicios de equilibrio de carga ya no son necesarios en las instancias de NetScaler ADC VPX implementadas en NSX Manager, puede eliminar las inserciones de servicio realizadas anteriormente.

Para eliminar la configuración y la inserción de servicios:

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración**, seleccione la configuración de la aplicación creada y, a continuación, elimínela haciendo clic en el icono «X».
2. En NSX Manager, navegue hasta la puerta de enlace perimetral a la que está conectada la instancia de Citrix ADC VPX. Vaya a **Administrar** > **Equilibrador de carga** > **Configuración global**, haga clic con el botón secundario en la entrada de tiempo de ejecución y, a continuación, haga clic en **Anular aprovisionamiento**. La máquina virtual está fuera de servicio.
3. En NetScaler ADM, vaya a **Orchestration** > **Cloud Orchestration** > **Edge Gateways**. Compruebe que la asignación respectiva de la Gateway perimetral a la instancia eliminada no debe estar presente.

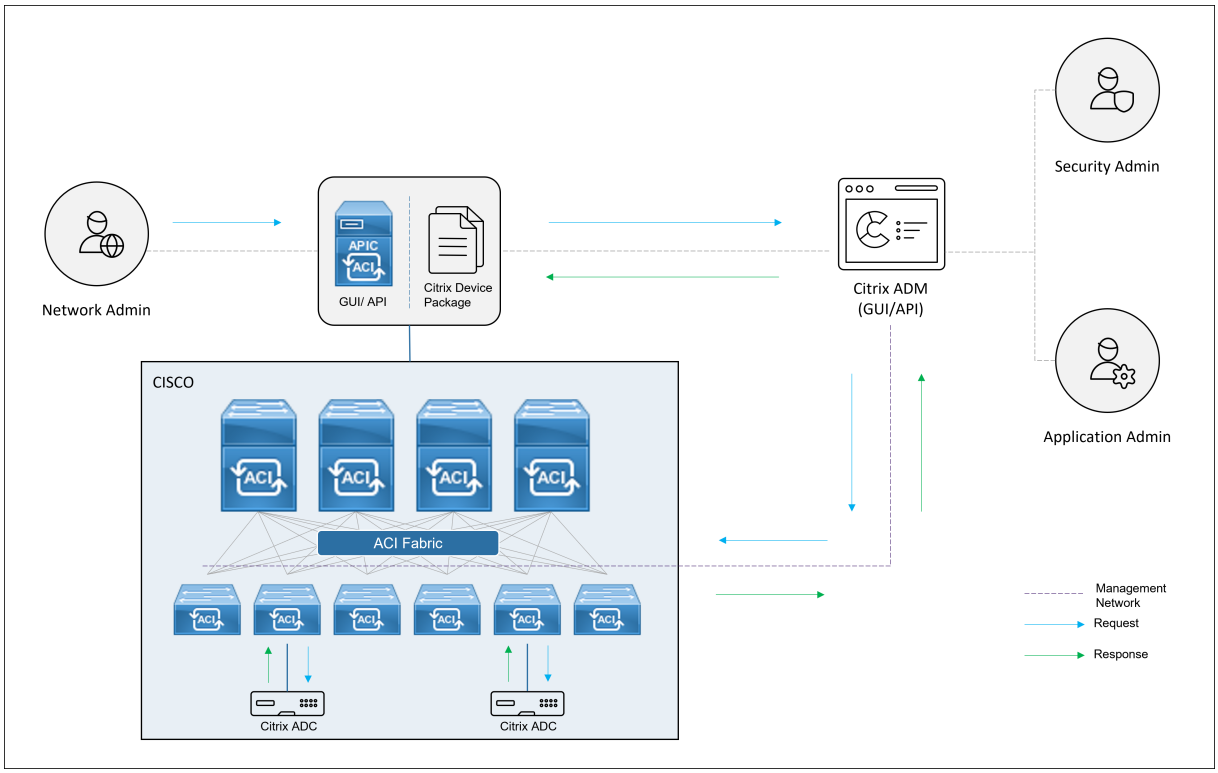
Automatización de Citrix ADC mediante Citrix ADM en el modo híbrido ACI de Cisco

January 30, 2024

Cisco ACI introdujo la compatibilidad con el modo híbrido en la versión 1.3 (2f). En el modo híbrido, puede realizar la automatización de la red a través del controlador de infraestructura de directivas de aplicaciones (APIC) y, al mismo tiempo, delegar la configuración L4-L7 a Citrix Application Delivery Management (ADM), que actúa como administrador de dispositivos en el APIC.

La solución Citrix ADC Hybrid Mode es compatible con un paquete de dispositivos de modo híbrido y Citrix ADM. Debe cargar el paquete de dispositivos de modo híbrido en la APIC. Este paquete proporciona todas las entidades configurables de red L2-L3 de Citrix ADC. StyleBook asigna la paridad de las aplicaciones desde Citrix ADM al APIC. En otras palabras, StyleBook actúa como referencia entre las configuraciones L2-L3 y L4-L7 para una aplicación determinada. Debe proporcionar un nombre de StyleBook al configurar las entidades de red desde el APIC para Citrix ADC.

La siguiente ilustración proporciona una descripción general de Citrix ADC en una solución de modo híbrido:



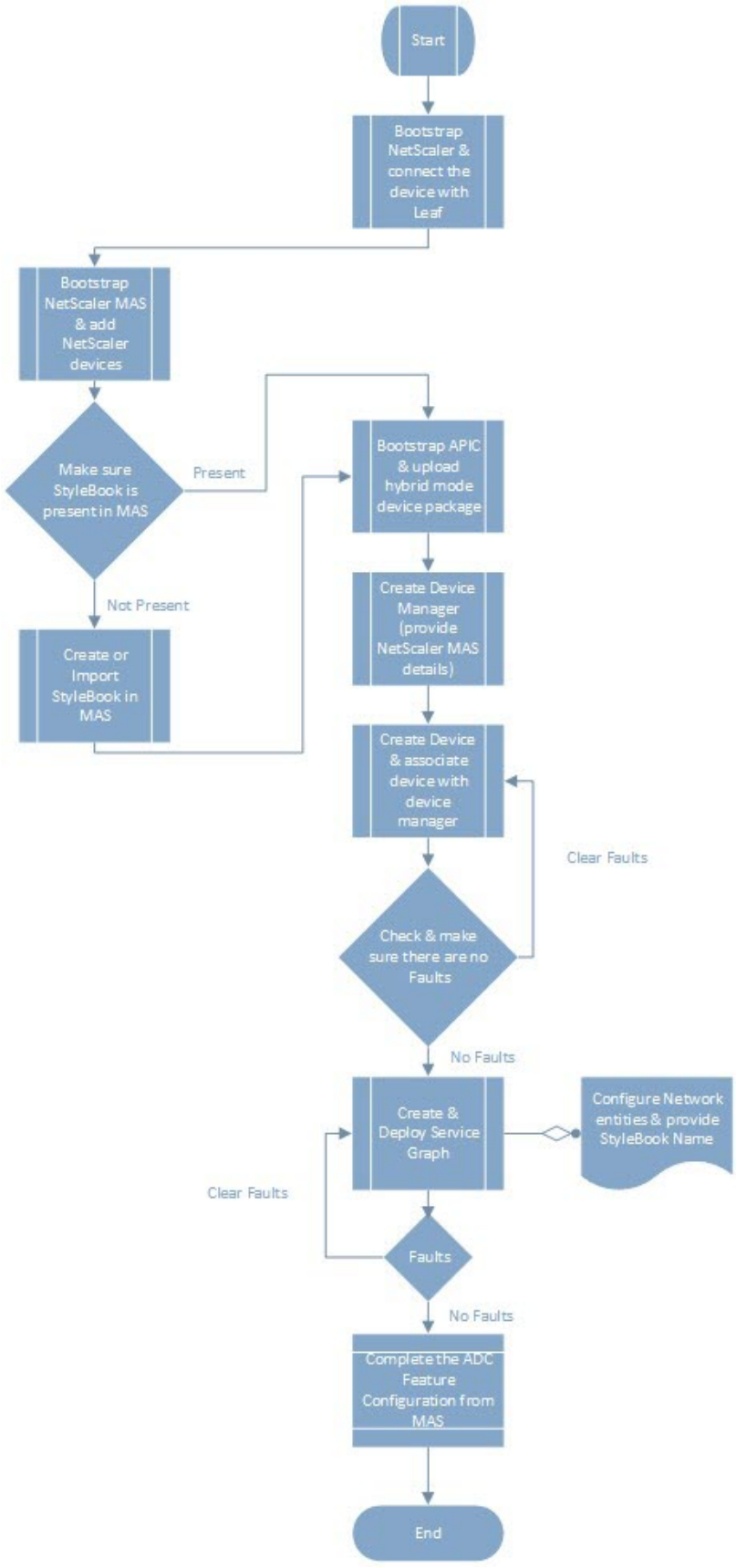
En el modo híbrido, la configuración de Citrix ADC se realiza en las dos fases siguientes:

1. La unión de redes se realiza desde el APIC de Cisco

2. La configuración se realiza desde Citrix ADM

Para cualquier aplicación determinada, el administrador de red debe proporcionar detalles específicos de la red, como las direcciones IP, el puerto, la VLAN (automatizada), etc., como parte de la creación e implementación del gráfico de servicios en el APIC de Cisco. A continuación, estos detalles de configuración se envían a Citrix ADM a través del paquete del dispositivo, y Citrix ADM los procesa internamente y configura el Citrix ADC. Un administrador de aplicaciones crea la configuración relacionada con el ADC de la aplicación mediante StyleBook en Citrix ADM y, a continuación, estas configuraciones se transfieren de Citrix ADM al Citrix ADC. Cisco APIC y Citrix ADM se comunican con el ADC a través de la red de administración.

El siguiente diagrama muestra un flujo de trabajo de Citrix ADC en la solución híbrida:



Requisitos previos

January 30, 2024

Asegúrese de que:

- Tiene conocimientos conceptuales sobre los componentes ACI de Cisco y los ADC de Citrix.
  - Para obtener más información sobre Cisco ACI y sus componentes, consulte la documentación del producto en: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Para obtener más información sobre los ADC de Citrix, consulte la documentación del producto NetScaler ADC en:http://docs.citrix.com/.
- Todos los componentes requeridos de Cisco ACI, incluido un Cisco APIC en el centro de datos, se configuran y configuran. Para obtener más información sobre Cisco ACI y sus componentes, consulte la documentación del producto en: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
- Ha instalado Citrix ADC 11.1 o posterior.
- Ha configurado los ADC de Citrix en Cisco ACI para que puedan administrarse mediante el APIC de Cisco.
- Ha implementado NetScaler Application Delivery Management (ADM) en su entorno. Para obtener más información, consulte Citrix ADM 12.1.
- Se establece la conectividad de administración de APIC a NetScaler ADM y ADC.
- Tome nota de:
  - Las interfaces de conexión y las direcciones IP que se utilizan para la administración y la conectividad de rutas de datos.
  - Detalles del conmutador Leaf: direcciones IP, puertos, interfaces, etc. de Citrix ADC.

> **Nota**
>
> En esta versión, la solución de modo híbrido admite NetScaler ADC en un contexto único, es decir, no se admiten particiones administrativas.

Configurar NetScaler ADC en modo híbrido mediante Cisco APIC y NetScaler ADM

January 30, 2024

Realice las siguientes tareas para configurar un Citrix ADC en modo híbrido mediante Cisco APIC y Citrix Application Delivery Management (ADM):

1. Agregue instancias de NetScaler ADC en su estructura a NetScaler ADM. Para obtener instrucciones, consulte Agregar una instancia a NetScaler ADM.
2. Utilice NetScaler ADM para crear un StyleBook para la aplicación. Para obtener instrucciones, consulte Creación de un StyleBook para la aplicación mediante NetScaler ADM.
3. Importe el paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC. Para obtener instrucciones, consulte Importación del paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC
4. Agregue NetScaler ADM como administrador de dispositivos en Cisco APIC. Para obtener instrucciones, consulte Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC
5. Utilice Cisco APIC para agregar un dispositivo NetScaler ADC en Cisco ACI. Para obtener instrucciones, consulte Agregar NetScaler ADC como dispositivo en Cisco ACI
6. Crear e implementar una plantilla de gráfico de servicio. Para obtener instrucciones, consulte Creación e implementación de un gráfico de servicio
7. Configure los parámetros L4-L7 mediante StyleBook en NetScaler ADM. Para obtener instrucciones, consulte Configurar el parámetro L4-L7 mediante StyleBook de NetScaler ADM
8. Adjuntar o desconectar eventos de punto final de la APIC de Cisco. Para obtener más información, consulte Adjuntar o separar eventos de punto final de APIC

Crear un StyleBook para una aplicación mediante NetScaler ADM

January 30, 2024

Un StyleBook es una plantilla de configuración que puede utilizar para crear y administrar configuraciones de Citrix ADC para cualquier aplicación. Puede crear un StyleBook para configurar una función específica de Citrix ADC, como el equilibrio de carga, la descarga de SSL o la conmutación de contenido. Puede diseñar un StyleBook para crear configuraciones para una implementación de aplicaciones empresariales como Microsoft Exchange o Lync. Para obtener más información, consulte StyleBooks.

Puede crear su propio StyleBook para su aplicación o modificar y utilizar el StyleBook APIC-HTTP-LB suministrado con NetScaler Application Delivery Management (ADM).

Para crear su propio StyleBook para su aplicación en NetScaler ADM, consulte Cómo crear sus propios StyleBooks.

Al crear el StyleBook, asegúrese de seguir el modelo de gráfico de servicio de APIC en el StyleBook. En otras palabras, el gráfico de servicios de la APIC para cualquier aplicación sigue el modelo de consumidor y proveedor conectados a través de una función ADC. El consumidor y el proveedor se representan como un grupo de puntos finales (EPG) y tienen una relación de 1:1. También se debe seguir el mismo modelo en StyleBook, donde el proveedor EPG debe representarse como un grupo de servicios y cada punto final como un miembro del grupo de servicios. El nodo de la función ADC debe estar representado por un servidor virtual (por ejemplo, un servidor virtual de equilibrio de carga) y debe haber una relación 1:1 entre el servidor virtual y el grupo de servicios.

Básicamente, esto captura la esencia del gráfico de servicios y permite gestionar el evento de adjuntar o desconectar de la APIC, donde un evento de adjuntación vincula el punto final al grupo de servicios correspondiente y un evento de desvinculación lo desvincula. Debe asegurarse de que el gráfico de servicio y el StyleBook estén en paridad para una automatización perfecta desde las configuraciones de red L2-L3 a L4-L7 con función ADC.

Importar paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC

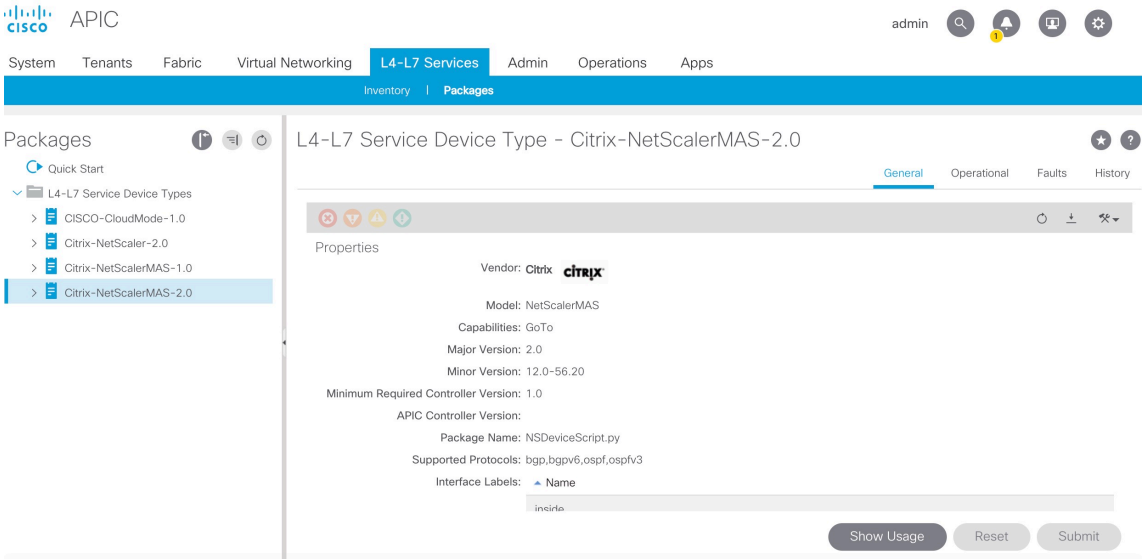
January 30, 2024

El paquete de dispositivos en modo híbrido es un paquete ligero en comparación con un modo totalmente gestionado. Solo los parámetros de red L2-L3 están disponibles en el modelo de dispositivo. El modelo de dispositivo solo tiene definida una función ADC genérica y cuatro perfiles de función basados en la implementación de Citrix ADC en la estructura (por ejemplo, un brazo y dos brazos y lo mismo con RHI). El nombre del paquete Dispositivo de modo híbrido es **NetScaler Hybrid Mode Device package 12.0 Build 56.20**. Busque el paquete de dispositivos Hybrid Mode en el sitio de descargas de Citrix, descárguelo e importe el paquete de dispositivos a la APIC.

> **Nota**
>
> El paquete de dispositivos de modo híbrido puede coexistir con un paquete de dispositivos de modo totalmente gestionado.

Para importar el paquete de dispositivos en modo híbrido a la APIC mediante la GUI de APIC:

1. **En la barra de menús, haga clic en la ficha**Servicios de nivel 4 a nivel 7**y seleccione el panel Paquetes.**
2. **En el panel de**navegación**, haga clic con el botón derecho en**Tipos de dispositivos de nivel 4 a nivel 7 y seleccione Importar paquete de dispositivos**.**
3. En el cuadro de diálogo **Importar paquete de dispositivos** , haga clic **en**Examinar para seleccionar el paquete de dispositivos de modo híbrido Citrix ADC descargado.
4. Haga clic en **Submit**.
   Tras importar correctamente el paquete del dispositivo a la APIC, en el panel de **navegación**, puede ver los detalles del paquete del dispositivo haciendo clic en el nombre del dispositivo.



> **Importante**
>
> Después de importar el paquete del dispositivo, asegúrese de que no haya errores en el APIC. Puede ver los errores haciendo clic en la ficha **Errores** de la ventana Tipos de dispositivos.

Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC

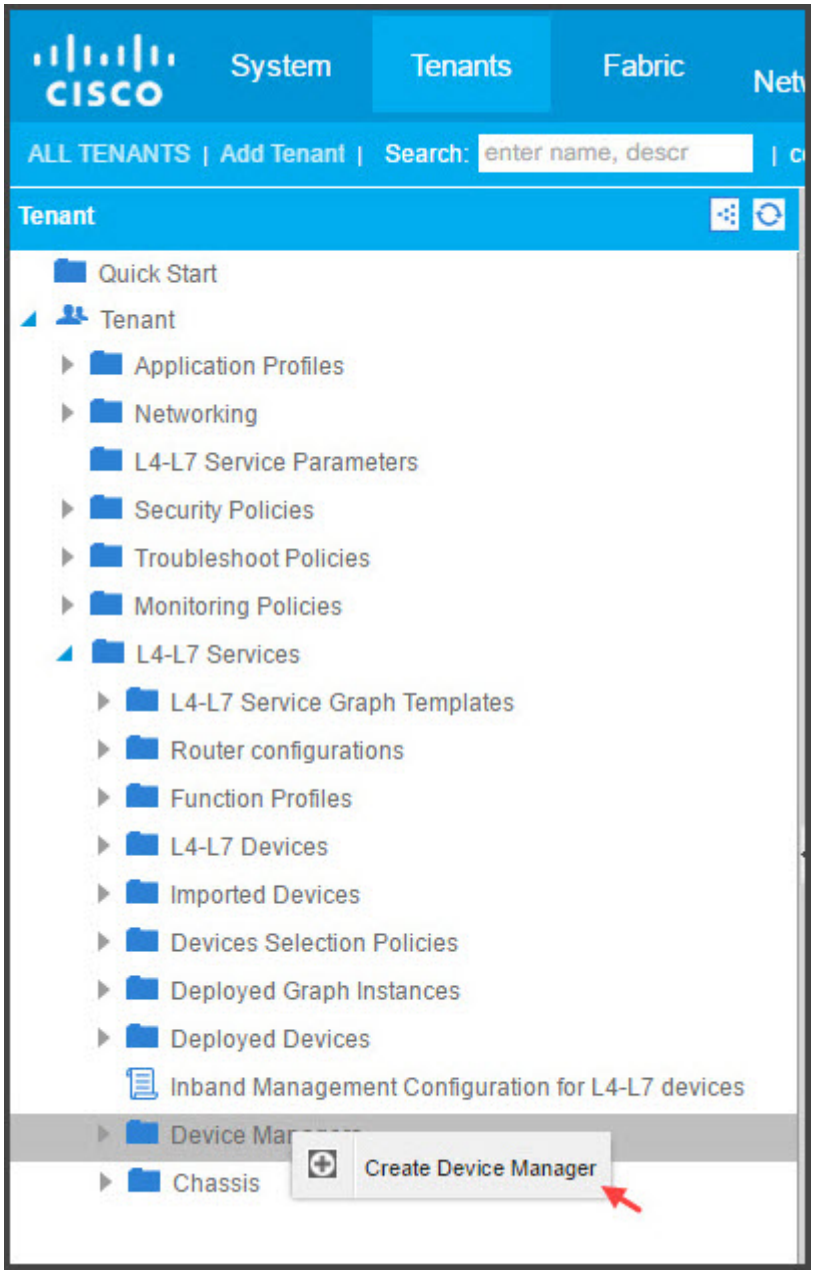
January 30, 2024

24 de mayo de 2018

Citrix Application Delivery Management (ADM) actúa como un administrador de dispositivos centralizado para Citrix ADC implementado en Cisco ACI. Debe agregar Citrix ADM como administrador de dispositivos en la APIC de Cisco.

Para agregar Citrix ADM como administrador de dispositivos en la APIC mediante la GUI de APIC:

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de **navegación**, seleccione ***nombre_de_arrendatario* > Servicios L4-L7.**
4. Haga clic con el botón derecho en **Administradores de dispositivos** y haga clic en **Crear administrador de dispositivos**.



5. En el cuadro de diálogo **Crear administrador de dispositivos**, haga lo siguiente:

a) En el campo **Nombre del administrador de dispositivos** , introduzca un nombre para la implementación de Citrix ADM que desea registrar como administrador de dispositivos.

b) En la lista desplegable **EPG de administración**, seleccione la EPG de administración.

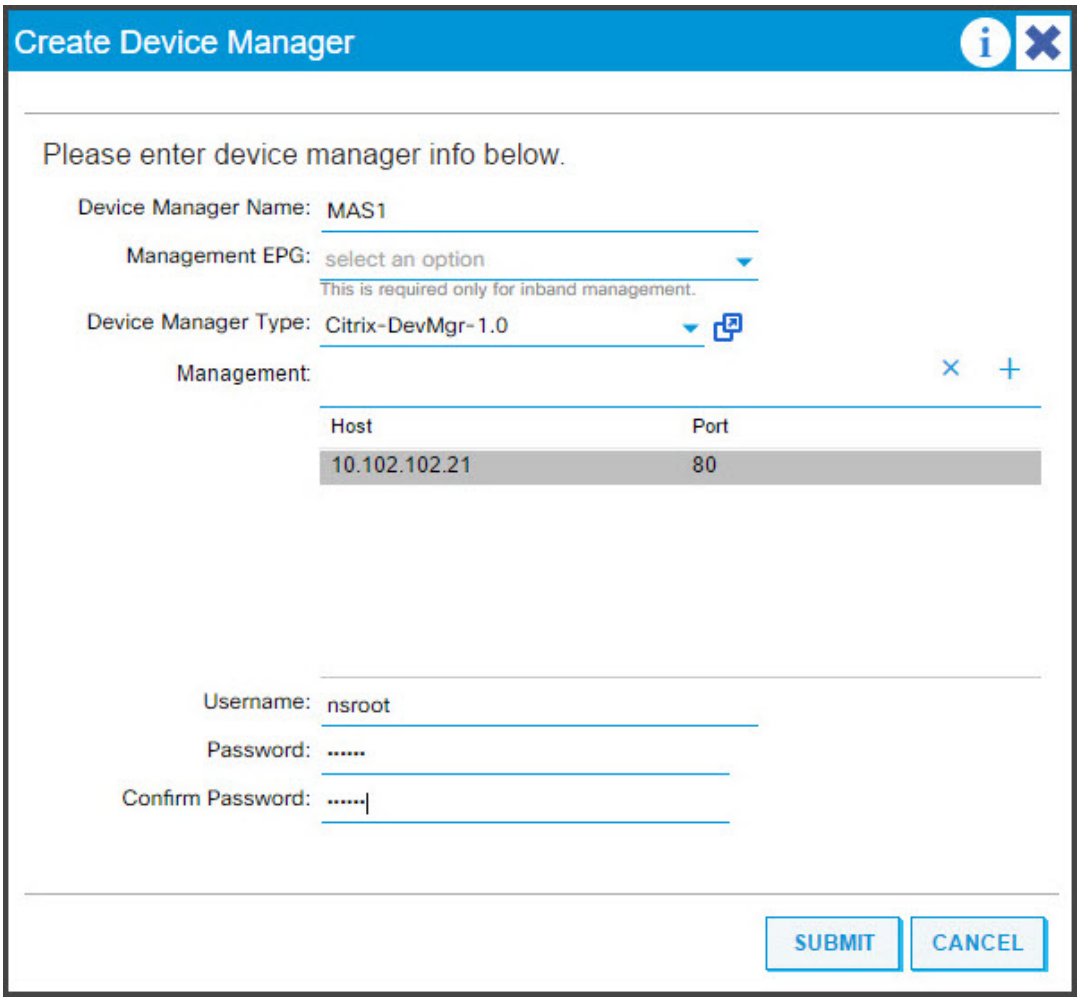
c) En la lista desplegable **Tipo de administrador de dispositivos**, seleccione **Citrix-DevMgr-1.0**.

d) En el campo **Administración** , haga clic en **+** y añada la dirección IP y los detalles del puerto de la implementación de Citrix ADM.

e) En el campo **Nombre** de usuario , introduzca el nombre de usuario para acceder a Citrix ADM.

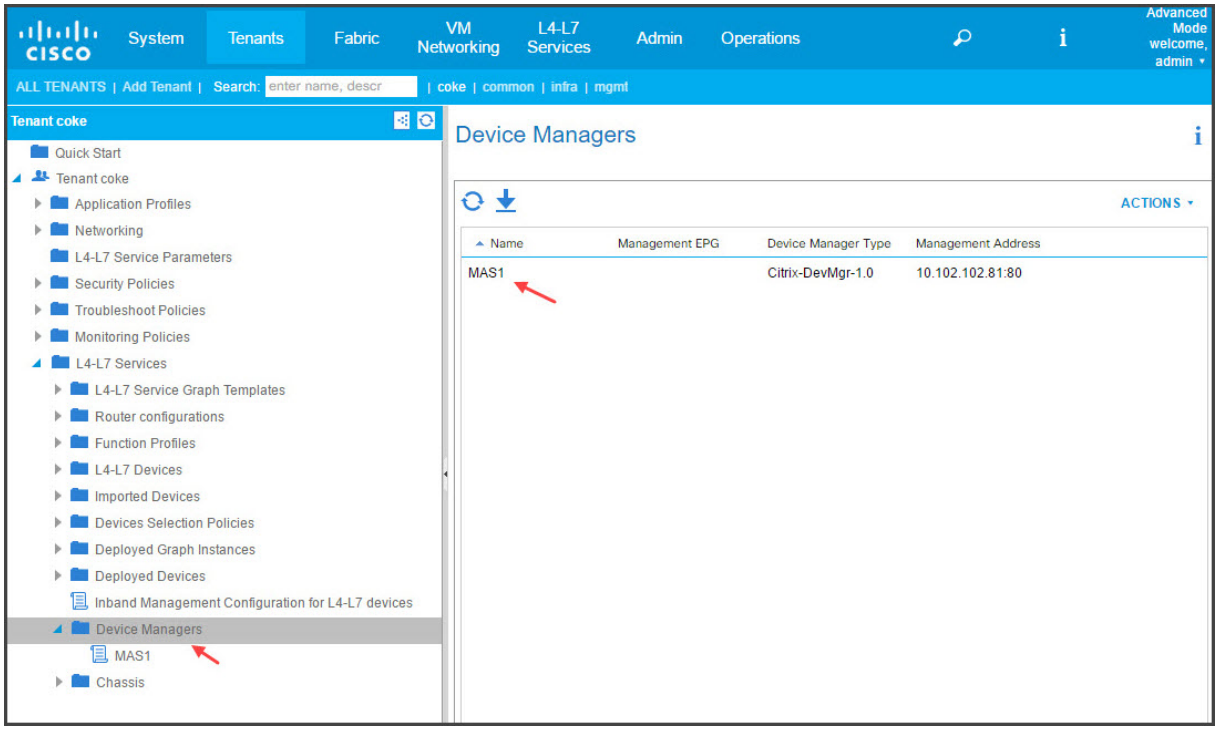
f) En los campos **Contraseña** y **Confirmar contraseña** , introduzca la contraseña para acceder a Citrix ADM.

g) Haga clic en **ENVIAR**.



Una vez que Citrix ADM se haya registrado correctamente como administrador de dispositivos en la APIC, se agrega el administrador de dispositivos y se muestra en el panel de **navegación**. Para ver el

administrador de dispositivos registrado, en el panel de navegación, vaya a ***tenant_name* > Servicios L4-L7 > Administrador de dispositivos.**



> **Nota**
>
> Asegúrese de que no haya problemas de conectividad entre Cisco APIC y Citrix ADM y de proporcionar las mismas credenciales que utiliza para acceder al Citrix ADM. Asegúrese también de que la cuenta tenga privilegios de administrador.
>
> **Importante**
>
> Después de importar el paquete del dispositivo, asegúrese de que no haya errores en el APIC. Puede ver los errores haciendo clic en la ficha **Errores** de la ventana Tipos de dispositivos.

También puede registrar Citrix ADM como administrador de dispositivos mediante las API. A continuación se muestra una carga XML de ejemplo que muestra cómo puede utilizar las API para agregar NetScaler ADM como administrador de dispositivos.

```
<polUni>
    <fvTenant name="coke">
        <vnsDevMgr name="MAS1">
            <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0" />
            <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="*****("/>
        </vnsDevMgr>
    </fvTenant>
```



```
</polUni>
```

Agregar NetScaler ADC como dispositivo en Cisco ACI mediante APIC

January 30, 2024

Debe agregar un Citrix ADC como dispositivo L4-L7 a la APIC para la automatización de la red. La APIC realiza la unión de red entre Leaf y el dispositivo Citrix ADC, según el gráfico de servicios implementado. Debe configurar los ajustes básicos de la configuración del dispositivo, como las direcciones IP de administración de la configuración, el administrador de dispositivos y las credenciales.

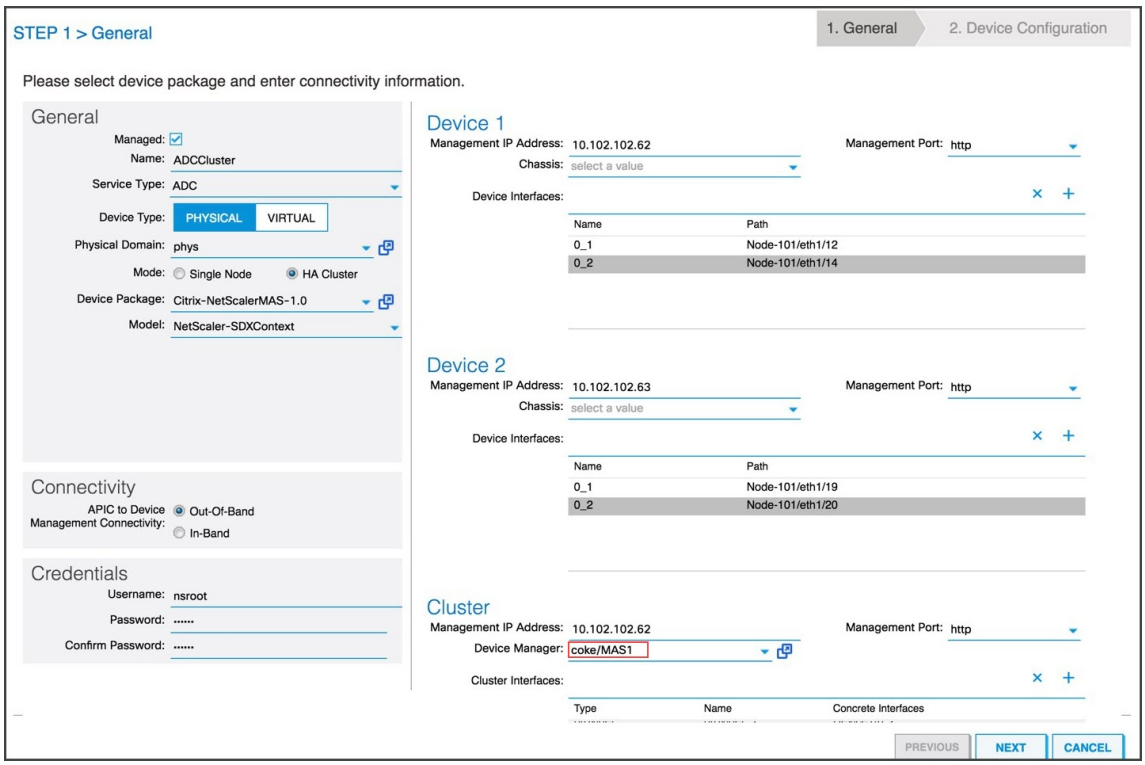
Para registrar el Citrix ADC como dispositivo en la APIC mediante la GUI de APIC:

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de **navegación**, seleccione ***nombre_arrendatario* > Servicios L4-L7 > Dispositivos L4-L7.**
4. En el panel Trabajo, seleccione **Acciones > Crear dispositivos L4-L7**.
5. En el cuadro de diálogo **Crear dispositivos L4-L7**, en la sección **General**, haga lo siguiente:
   a) Seleccione la casilla **Administrado**.
   b) En el campo **Nombre**, introduzca un nombre para el dispositivo.
   c) En la lista desplegable **de tipos de servicio**, seleccione **ADC**.
   d) En el campo **Tipo de dispositivo**, selecciona **Físico**.

      > **Nota**
      >
      > Asegúrese de que, para VMware ESX, seleccione Virtual y asocie el dominio de Virtual Machine Manager (VMM) correspondiente.

   e) En la lista desplegable **Dominio físico**, seleccione el dominio físico.
   f) En el campo **Modo**, seleccione **Nodo único** o **Clúster HA**, según sus necesidades.
   g) En la lista desplegable del **paquete de dispositivos**, seleccione **Citrix-NetScalerMAS-1.0**.
   h) En la lista desplegable **Modelo**, selecciona el modelo del dispositivo. Por ejemplo, Citrix ADC-MPX o Citrix ADC-VPX.
6. En la sección **Conectividad** , seleccione Fuera **de banda** o Dentro de **banda en** el campo **Conectividad de APIC a administración de dispositivos** , según cómo esté configurado Citrix ADC en la estructura.

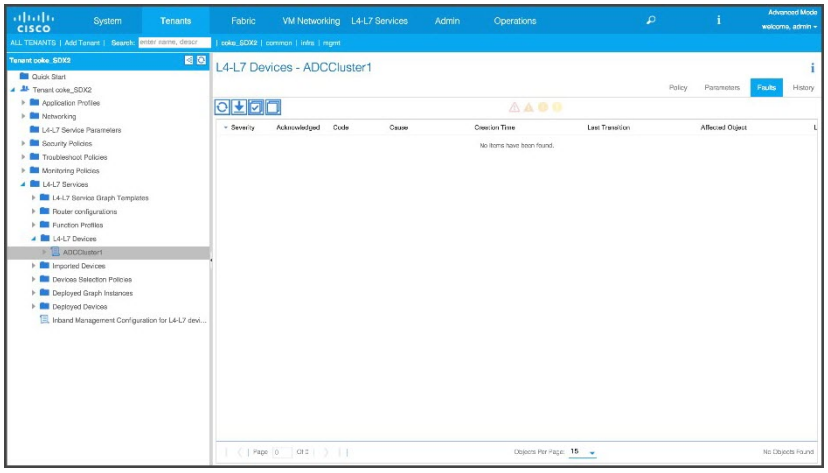
7. En la sección **Credenciales**, especifique el nombre de usuario y la contraseña para acceder al dispositivo.
8. En las secciones **Dispositivo 1** y **Dispositivo 2**, respectivamente, complete la configuración relacionada con la administración.
9. En la sección **Cluster**, complete la configuración relacionada con la administración del clúster. Asegúrese de que en la lista desplegable **Administrador de dispositivos**, seleccione el administrador de dispositivos que creó en Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC



10. Haga clic en **SIGUIENTE**. Aparece la página Configuración del dispositivo. El paquete de dispositivos en modo híbrido no proporciona detalles de configuración específicos del dispositivo y el clúster, como la alta disponibilidad, las funciones y modos de habilitación/desactivación, la configuración de NTP, SNMP, alarmas SNMP, etc. Estas configuraciones deben realizarse mediante Citrix ADM.
11. Haga clic en **FINALIZAR**. Cuando haya registrado correctamente el dispositivo en la APIC, se agregará el dispositivo y se mostrará en el panel de navegación. Para ver el dispositivo registrado, en el panel de navegación, vaya a ***nombre_arrendatario* > Servicios L4-L7 > Dispositivos L4-L7 > nombre_dispositivo.**

> **Importante**
>
> Después de registrar el dispositivo, asegúrese de que no haya errores en el APIC. Puede ver

> los errores haciendo clic en la ficha **Errores** del panel **Trabajo**.



También puede registrar un dispositivo Citrix ADC mediante API. A continuación se muestra una carga útil XML de ejemplo para agregar dispositivo L4-L7:

```
<polUni>

    <fvTenant name="coke">

    <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

     <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

     <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

     <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

     <vnsCCred name="username" value="nsroot"/>

     <vnsCCredSecret name="password" value="****"/>

     <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

     <vnsCDev name="ADC1" devCtxLbl="C1">

     <vnsCIf name="1_1">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /33]"/>

     </vnsCIf>

     <vnsCIf name="1_2">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /35]"/>

```



```
31        </vnsCIf>
32
33        <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
34
35        <vnsCCred name="username" value="nsroot"/>
36
37        <vnsCCredSecret name="password" value="****"/>
38
39        </vnsCDev>
40
41        <vnsCDev name="ADC2" devCtxLbl="C1">
42
43        <vnsCIf name="1_1">
44
45        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
              /34]"/>
46
47        </vnsCIf>
48
49        <vnsCIf name="1_2">
50
51        <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
              /36]"/>
52
53        </vnsCIf>
54
55        <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57        <vnsCCred name="username" value="nsroot"/>
58
59        <vnsCCredSecret name="password" value="****"/>
60
61        </vnsCDev>
62
63        <vnsLIf name="outside">
64
65        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
              mIfLbl-outside"/>
66
67        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
              cIf-1_1"/>
68
69        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
              cIf-1_1"/>
70
71        </vnsLIf>
72
73        <vnsLIf name="inside">
74
75        <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
              mIfLbl-inside"/>
76
77        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
```



```
            cIf-1_2"/>
78
79          <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
               cIf-1_2"/>
80
81          </vnsLIf>
82
83          </vnsLDevV
84
85          </fvTenant>
86
87          </polUni>
```

Crear e implementar un gráfico de servicio

January 30, 2024

Debe usar las plantillas de gráficos de servicio APIC de Cisco en APIC para crear e implementar los ADC de Citrix. Asegúrese de utilizar el perfil de función ADC al crear e implementar un gráfico de servicio.

Una vez configurado el gráfico en el APIC, el APIC automatiza la configuración del dispositivo basándose en las definiciones de las funciones, la conectividad del dispositivo con la estructura y las entidades configuradas como parte de la implementación del gráfico. La APIC también automatiza la configuración de la red, como la asignación de VLAN y su enlace, como parte de la creación del gráfico de servicio, y la configuración se elimina una vez que se elimina el gráfico del APIC.

Un gráfico de servicio se representa como dos o más niveles de una aplicación, con la función de servicio correspondiente insertada entre ellos. Un contrato inserta un gráfico de servicio entre las EPG de origen y destino.

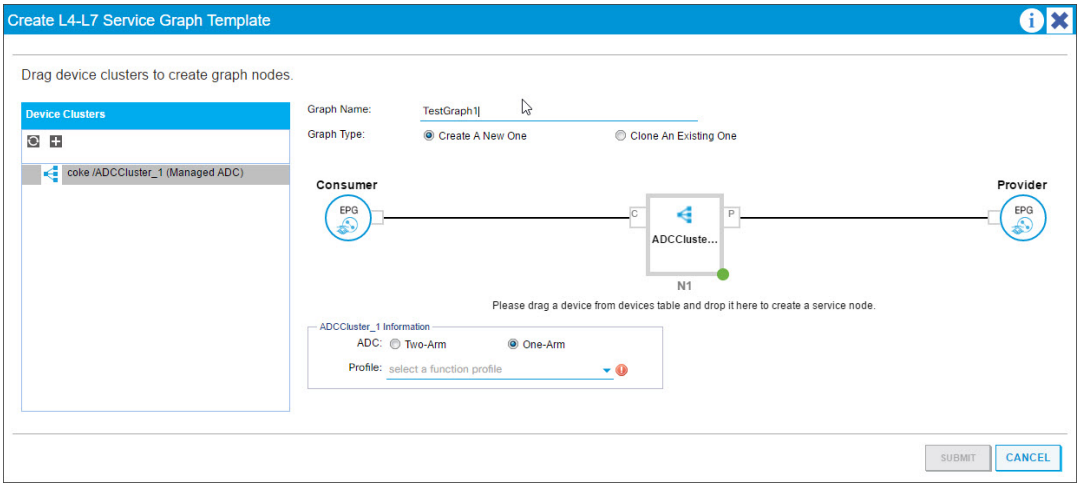
Para crear un gráfico de servicio mediante la interfaz gráfica de usuario de APIC:

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de **navegación**, seleccione ***tenant_name* > Servicios L4-L7 > Plantillas de gráficos de servicios L4-L7.**
4. En el panel **Trabajo**, seleccione **Acciones > Crear una plantilla de gráfico de servicio L4-L7**.
5. En el cuadro de diálogo **Crear una plantilla de gráficos de servicio L4-L7**, en la sección Clústeres de dispositivos, seleccione un clúster de dispositivos y haga lo siguiente:

    a) En el campo **Nombre del gráfico**, introduzca el nombre de la plantilla de gráfico de servicio.

b) En el campo **Tipo de gráfico**, seleccione **Crear uno nuevo**.

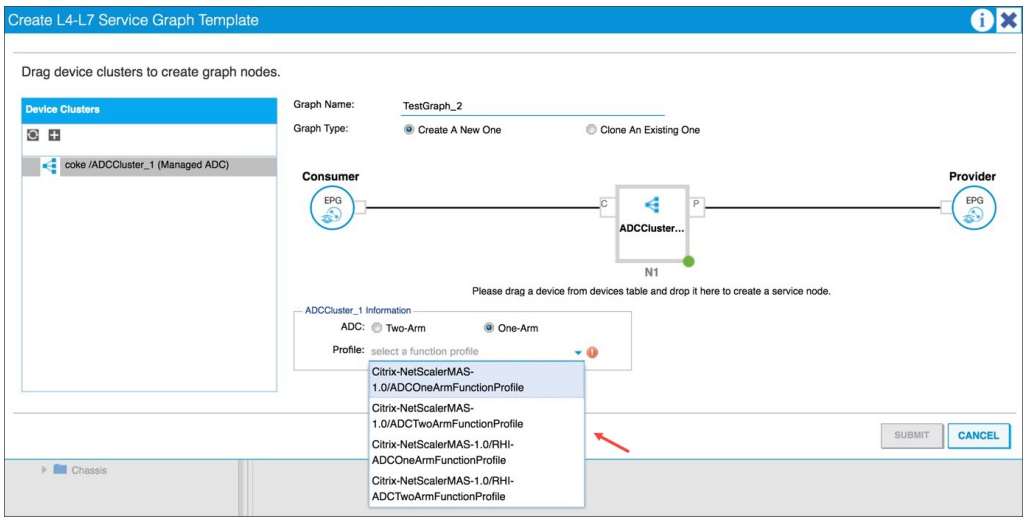
c) En la sección **Clúster de dispositivos**, arrastre el dispositivo y suéltelo entre el grupo de puntos finales del consumidor y el grupo de puntos finales del proveedor para crear un nodo de servicio.



d) En la sección < L4-L7Device_name information >**, haga lo siguiente:

i. En el campo **ADC** , seleccione **One-Arm** o **Two-Arm** , según cómo esté implementado el Citrix ADC en la estructura.

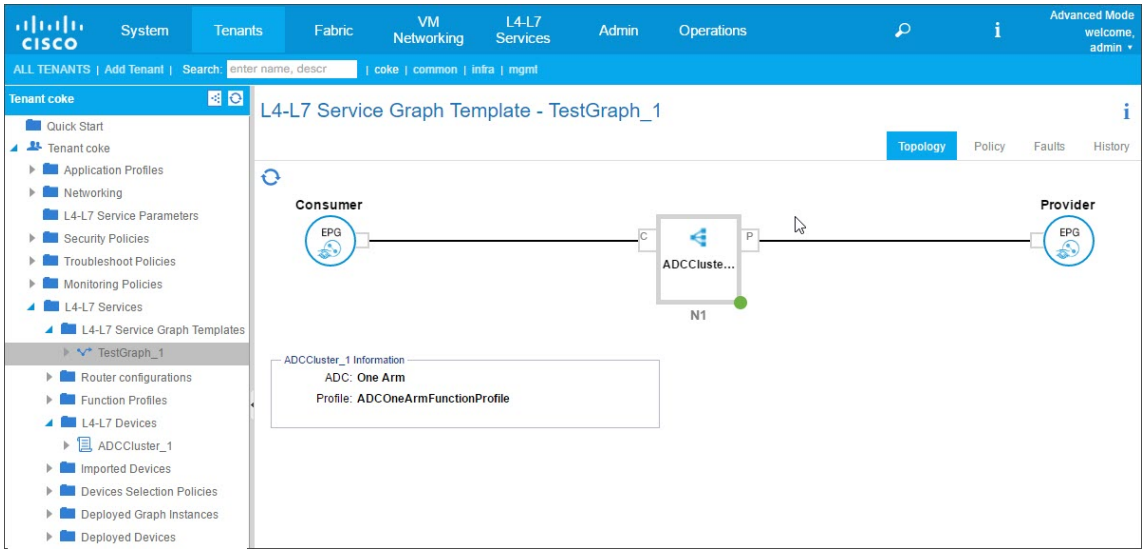
ii. En la lista desplegable **de perfiles**, seleccione el perfil de función que se proporciona en el paquete del dispositivo.



iii. Haga clic en **ENVIAR**.

6. En el panel **de navegación**, haga clic en la plantilla del gráfico de servicios. La pantalla presenta una topología gráfica de la plantilla de gráficos de servicios.

> **Nota**
>
> El APIC de Cisco admite la noción de conectores, y estos conectores están visibles en el nodo ADCCluster. Los conectores definen la dirección del tráfico de red y el script del dispositivo que vincula dinámicamente la VLAN asignada a una dirección IP virtual (VIP) o IP de subred (SNIP), dependiendo de si la conexión es externa o interna. Las VLAN también están enlazadas a interfaces específicas que se utilizan para el tráfico entrante y saliente.

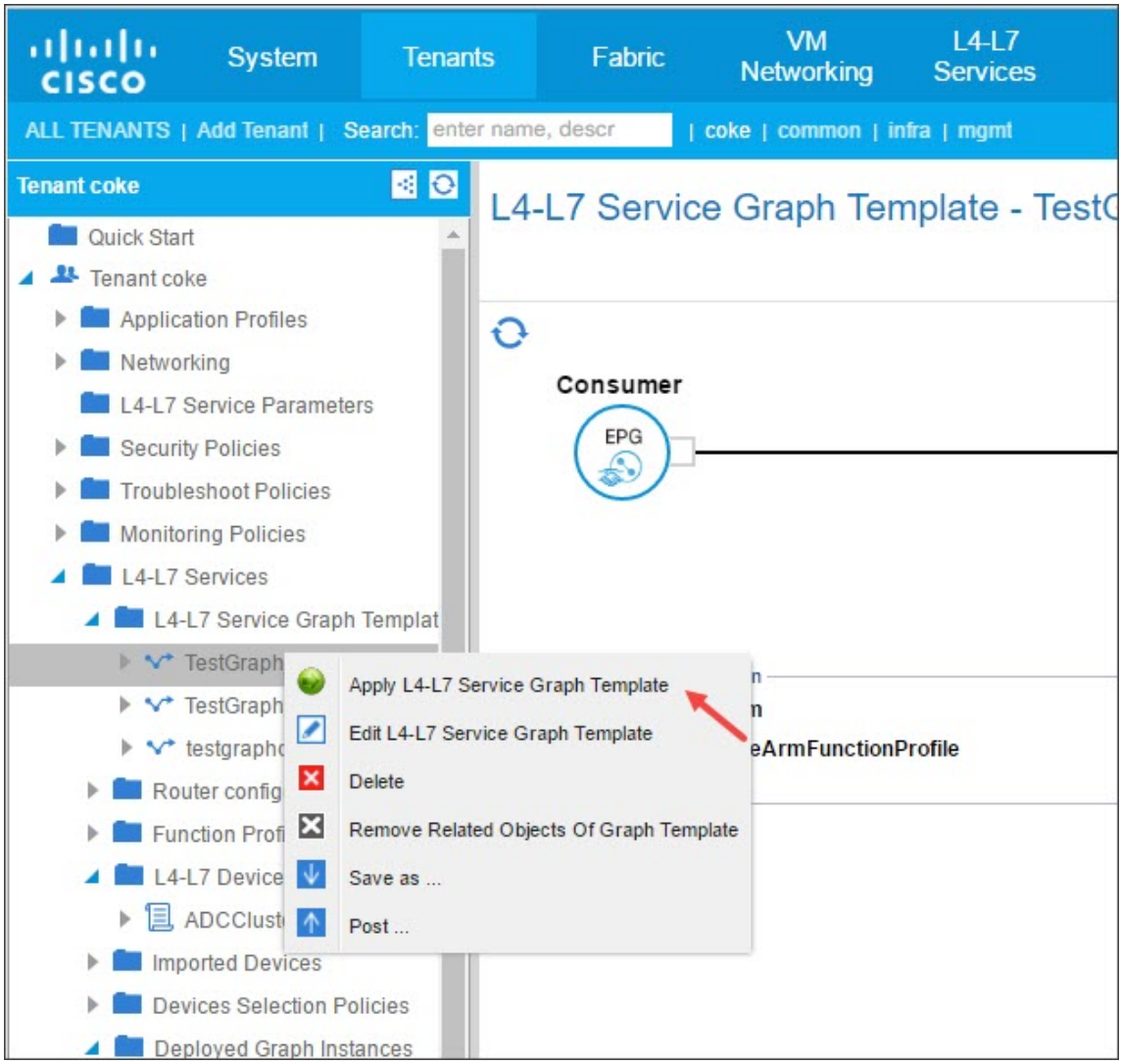


Aplicación de la plantilla de gráficos de servicio a grupos de terminales

Una vez creada la plantilla de gráfico de servicio, debe aplicar la plantilla de gráfico de servicio creada mediante la interfaz gráfica de usuario de APIC.

Para aplicar la plantilla de gráficos de servicios:

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de navegación, elija ***tenant_name* > Servicios L4-L7 > Plantillas de gráficos de servicios L4-L7.**
4. Haga clic con el botón derecho en el ***nombre de la plantilla y haga clic en*Aplicar plantilla de gráfico de servicio L4-L7**.

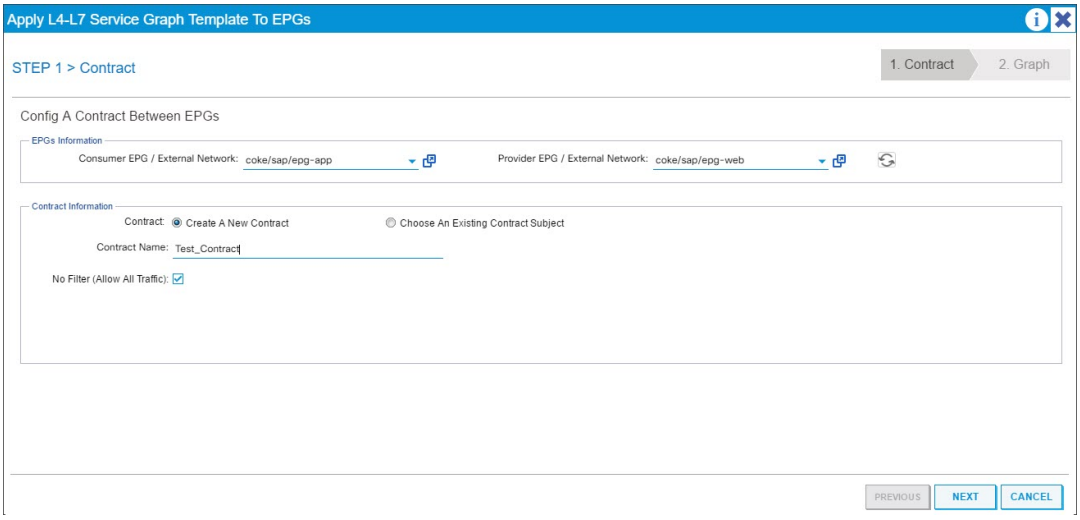


5. En el cuadro de diálogo **Aplicar plantilla de gráfico de servicio L4-L7 a las EPG**, en la sección **Información de la EPG**, complete los siguientes campos:

    a) En la lista desplegable **Consumer EPG/External Network**, seleccione el grupo de terminales de consumo.

    b) En la lista desplegable **Provider EPG/External Network**, seleccione el grupo de puntos de conexión proporcionado.

    c) En la sección **Información del contrato**, complete los campos correspondientes. La información del contrato es específica de la APIC de Cisco y está configurada como parte de las directivas de seguridad asociadas a las EPG.



d) Haga clic en **Siguiente**.

e) En la lista desplegable **de plantillas de gráficos**, seleccione la plantilla de gráficos de servicio que creó.

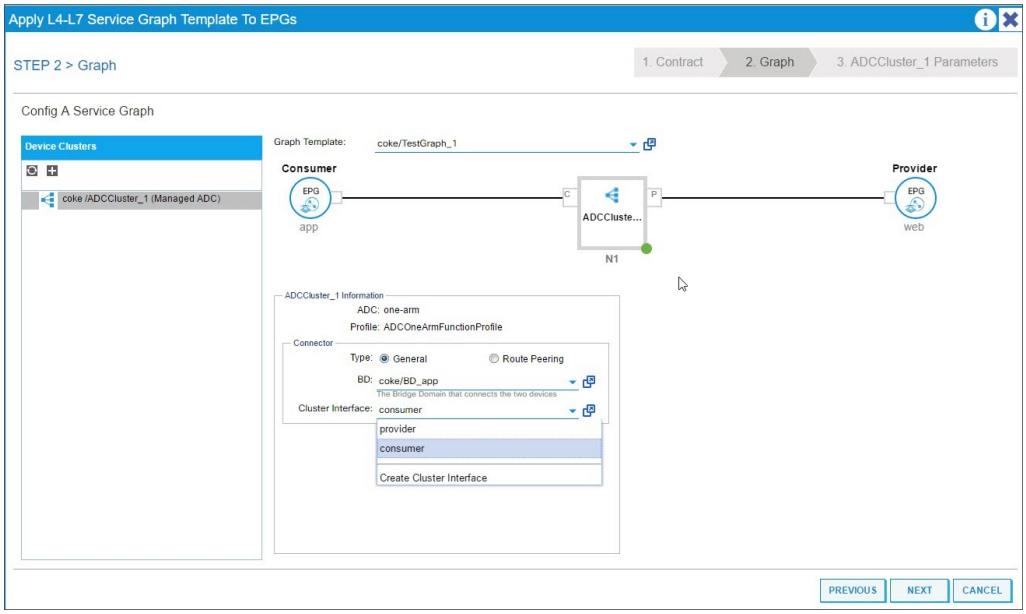
f) En la sección **Conector**, haga lo siguiente:

   i. En el campo **Tipo**, seleccione General.

   ii. En la lista desplegable de **BD**, seleccione el dominio puente. Los detalles del conector forman parte del dominio puente que forma parte del modelo de infraestructura APIC de Cisco.

   iii. En la lista desplegable **Interfaz de clúster**, seleccione la interfaz de clúster adecuada para el dominio puente seleccionado.

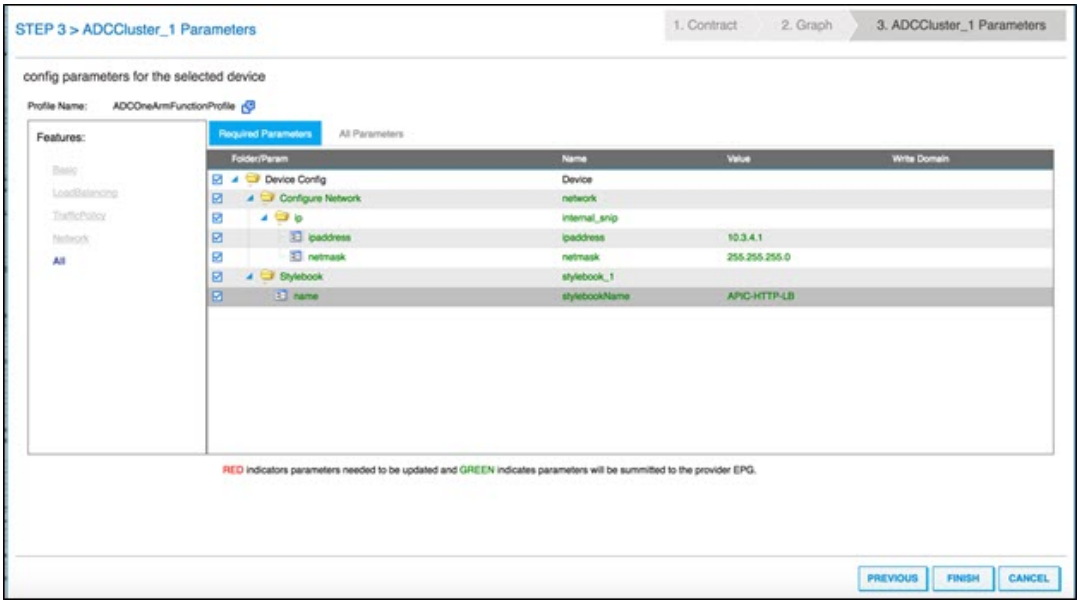
   El APIC de Cisco utiliza los dominios puente seleccionados para el tráfico de rutas de datos entre el dispositivo Citrix ADC y la estructura, según lo exige la plantilla de gráfico de servicio seleccionada.



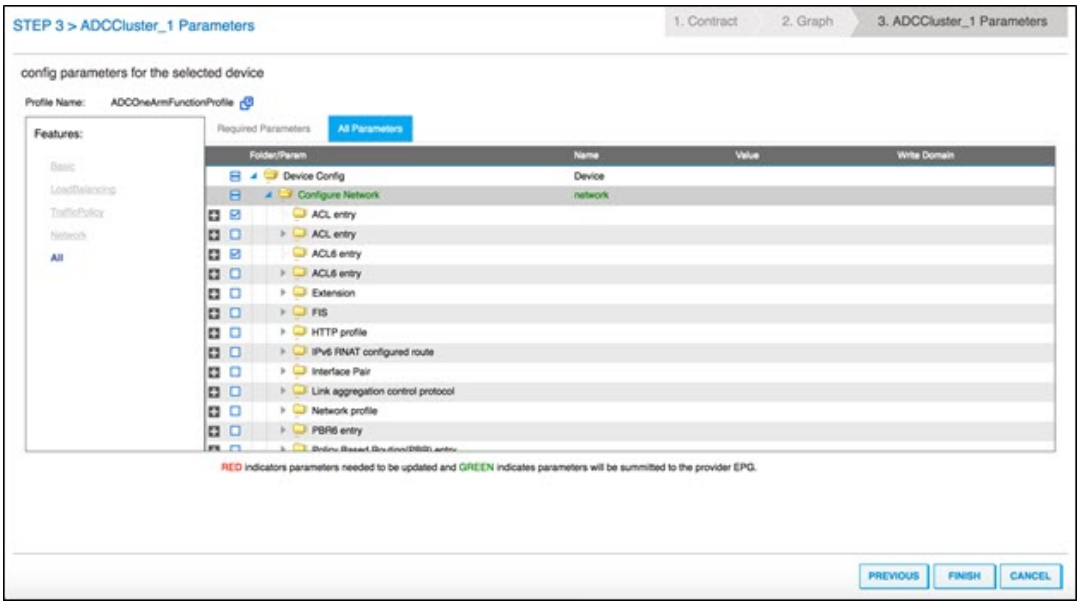
iv. Haga clic en **Siguiente**.

En la pantalla **Parámetros**, en la ficha **Parámetros obligatorios**, introduzca los detalles específicos de L2-L3, como la dirección IP que exige el perfil. El otro parámetro clave es el nombre de StyleBook. Puede ser el StyleBook **APIC-HTTP-LB** integrado que se proporciona en NetScaler Application Delivery Management (ADM) o puede proporcionar el nombre del StyleBook que creó en Creación de un StyleBook para la aplicación con NetScaler ADM

> **Nota**
>
> El nombre StyleBook vincula los detalles de Service Graph con la configuración L4-L7 creada con Citrix ADM para una aplicación determinada.



La GUI de Cisco APIC le permite filtrar los parámetros en función de las características (por ejemplo, el equilibrio de carga). Puede ver y configurar todos los parámetros obligatorios en la ficha **Parámetros obligatorios**, y puede ver y configurar todos los demás parámetros relacionados con la función en la ficha **Todos los parámetros**.

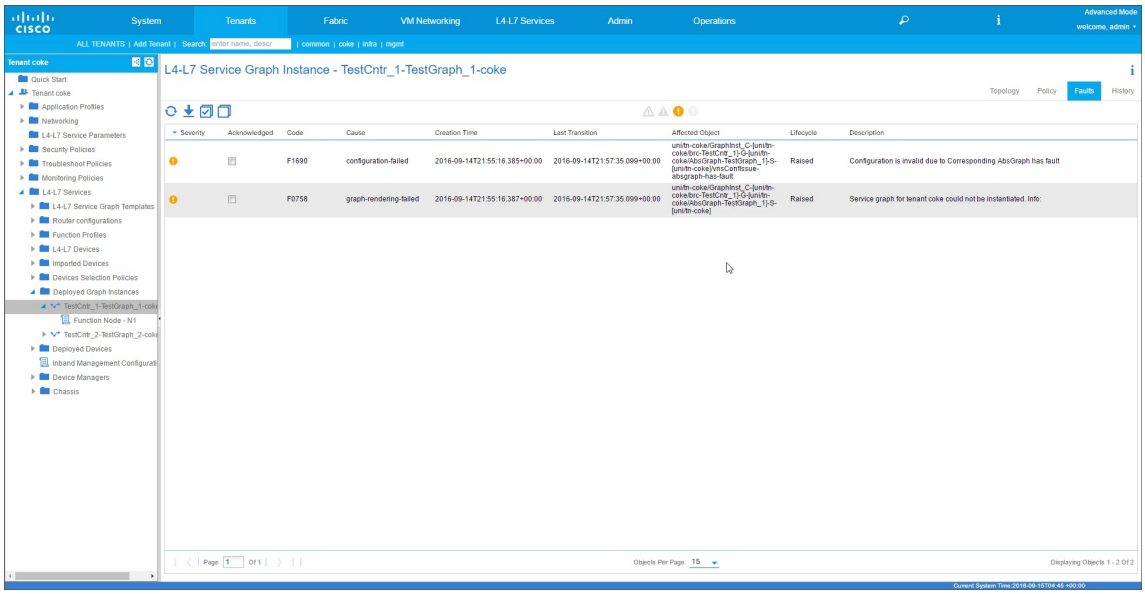


> **Nota**
>
> De forma predeterminada, un perfil integrado de un solo brazo requiere que proporciones detalles del SNIP, como la dirección IP y la máscara de red. Puede ver otros parámetros de red haciendo clic en **Todos los parámetros** y expandiendo el árbol **Configurar red** en la GUI de Cisco APIC. Aquí se enumeran todos los parámetros de red admitidos por Citrix ADC. Puede crear una instancia de cualquier entidad y pro-

> porcionar valores para los atributos enumerados desde la GUI de Cisco APIC.

6. Haga clic en **Finalizar**.

> **Importante**
>
> Después de aplicar la plantilla de gráfico de servicio, asegúrese de que no haya errores en el gráfico implementado. Puede ver los errores haciendo clic en la ficha **Errores** del panel **Trabajo**.



Como parte de la implementación de Service Graph, el paquete Hybrid Mode Device envía los detalles de configuración del APIC de Cisco al Citrix ADM. El Citrix ADM procesa internamente estas configuraciones en el Citrix ADC correspondiente y devuelve la respuesta a la APIC. Una implementación de gráficos exitosa no tendrá ningún error y el Citrix ADC se conectará correctamente en red con la estructura del gráfico correspondiente.

La APIC admite diferentes formas de configurar e implementar gráficos mediante el uso de API, y la implementación de gráficos incluye varias dependencias de algunas construcciones específicas de la API, como Tenant, contract, VLAN y namespace.

El siguiente enfoque de ejemplo ilustra una de las formas de utilizar las API de la APIC para crear e implementar gráficos L4-L7, suponiendo que los artefactos específicos de la APIC ya están configurados en la APIC.

> **Importante**
>
> Asegúrese de utilizar estas cargas XML como referencia y realice los cambios adecuados en el XML antes de utilizarlas en su entorno.

A continuación se muestra un ejemplo de cómo crear e implementar el gráfico de servicios mediante API:

a) Crear perfil de aplicación

b) Crear detalles del gráfico de servicios

c) Adjunte el gráfico de servicio a un contrato

A continuación se muestra un ejemplo de carga XML para crear un AppProfile. El AppProfile contiene las EPG y la EPG del proveedor contiene las entidades, los atributos y sus valores específicos de Citrix ADC. En el siguiente ejemplo de carga útil XML, se crean entidades de red específicas de Citrix ADC, como el NSIP, con un conjunto de atributos y un nombre de StyleBook.

```
<polUni>
    <fvTenant name="coke">
        <!-- Application Profile -->
        <fvAp dn="uni/tn-coke/ap-sap" name="sap">
            <!-- EPG 1  -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
                <fvRsBd tnFvBDName="BD_web" />
                <!-- --------- CONFIG PAYLOAD ---------------- -->
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name=
    "Network">
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip1">
                        <vnsParamInst key="ipaddress" name="ip1"
    value="110.110.110.2"/>
                        <vnsParamInst key="netmask" name="netmask1
    " value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip2">
                        <vnsParamInst key="ipaddress" name="ip2"
    value="220.220.220.2"/>
                        <vnsParamInst key="netmask" name="netmask2
    " value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                </vnsFolderInst>
```



```
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
    name="stylebook_1">
                    <vnsParamInst name="stylebookName" key="name"
    value="APIC-HTTP-LB"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    internal_network" name="internal_network">
                    <vnsCfgRelInst name="internal_network_key" key
    ="internal_network_key" targetName="Network/snip1"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    external_network" name="external_network">
                    <vnsCfgRelInst name="external_network_key" key
    ="external_network_key" targetName="Network/snip2"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
    " name="mFCngStylebook_1">
                    <vnsCfgRelInst name="Stylebook_key" key="
    Stylebook_key" targetName="stylebook_1"/>
                </vnsFolderInst>
                <!-- ------- END CONFIG PAYLOAD -------------- -->
                <fvSubnet ip="110.110.110.110/24" scope="shared"/>
                <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
                <fvRsDomAtt tDn="uni/phys-sepg" />
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
            </fvAEPg>
            <!-- EPG 2 -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
                <fvRsCons tnVzBrCPName="Ctrct1"/>
                <fvRsBd tnFvBDName="BD_app" />
                <fvSubnet ip="220.220.220.220/24" scope="shared"/>
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
                <fvRsDomAtt tDn="uni/phys-sepg" />
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

A continuación se muestra un ejemplo de carga XML para crear detalles de gráficos de servicios:

```
<polUni>
    <fvTenant name="coke">
        <vnsAbsGraph name = "Graph1">
            <vnsAbsTermNodeProv name = "Input1">
                <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
            </vnsAbsTermNodeProv>
```



```
            <vnsAbsNode name="ADC" funcType="GoTo">
                <vnsAbsFuncConn name = "outside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
                </vnsAbsFuncConn>
                <vnsAbsFuncConn name = "inside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
                </vnsAbsFuncConn>
                <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction"/>
                <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/outtmnl"/>
                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix
    -NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
    ADCOneArmServiceProfileGroup/absFuncProf-A
DCOneArmFunctionProfile"/>
                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-
    ADCCluster1"/>
            </vnsAbsNode>
            <vnsAbsTermNodeCon name = "Output1">
                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
            </vnsAbsTermNodeCon>
            <vnsAbsConnection name = "CON1">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeCon-Output1/AbsTConn" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-outside" />
            </vnsAbsConnection>
            <vnsAbsConnection name = "CON2">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-inside" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/AbsTConn" />
            </vnsAbsConnection>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

A continuación se muestra una carga útil XML de ejemplo para adjuntar el gráfico de servicio a un contrato:

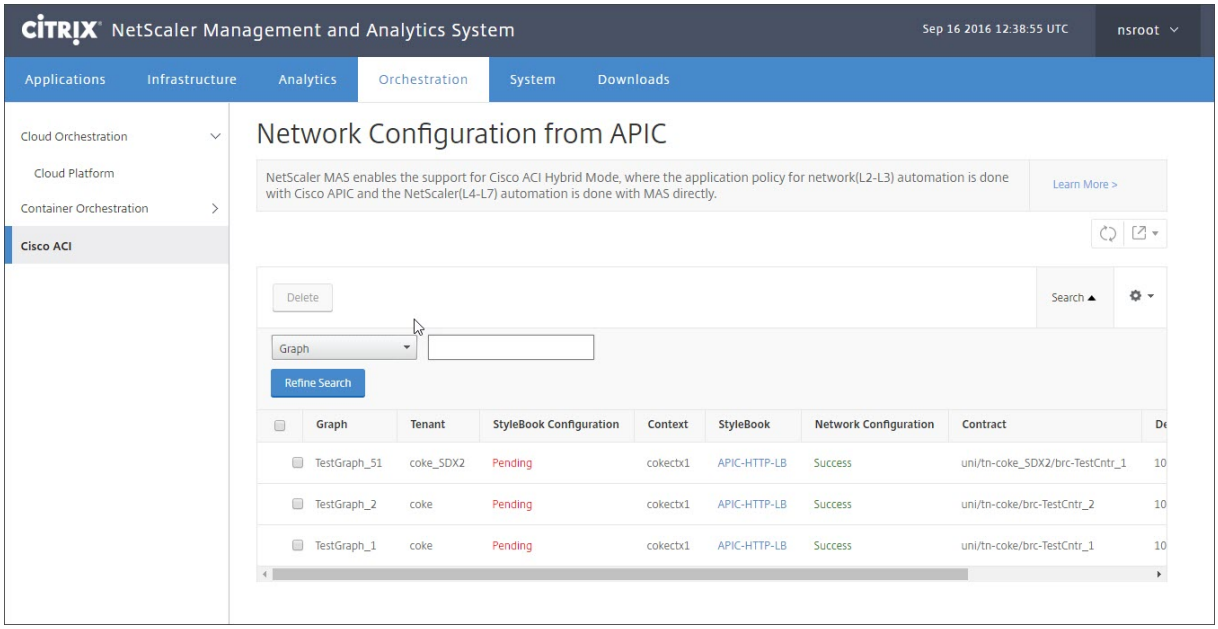
```
<polUni>
    <fvTenant name="coke">
        <vzBrCP name="Ctrct1">
            <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```


Configure los parámetros L4-L7 desde NetScaler ADM con StyleBook

January 30, 2024

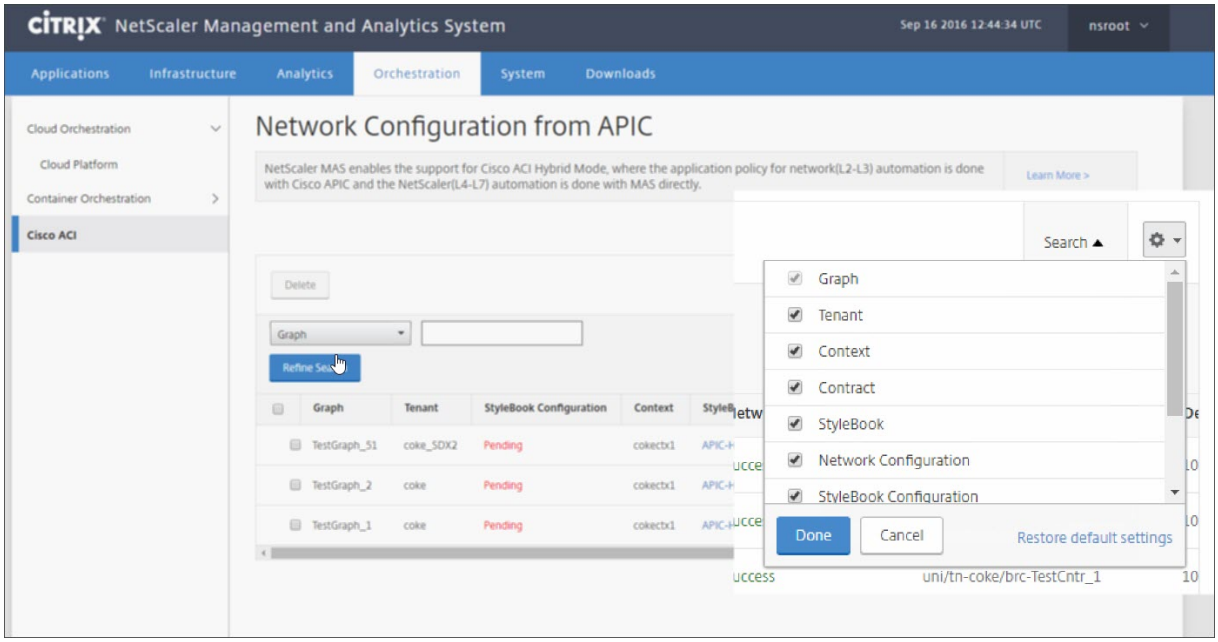
24 de mayo de 2018

En Citrix Application Delivery Management (ADM), puede ver los detalles del gráfico del servicio implementado en la pestaña **Orchestration** , en **Cisco ACI**. La vista tabular muestra los detalles del gráfico de servicio, como el nombre del gráfico, el nombre del arrendatario, el contexto, el nombre de StyleBook y el estado de la configuración de la red.



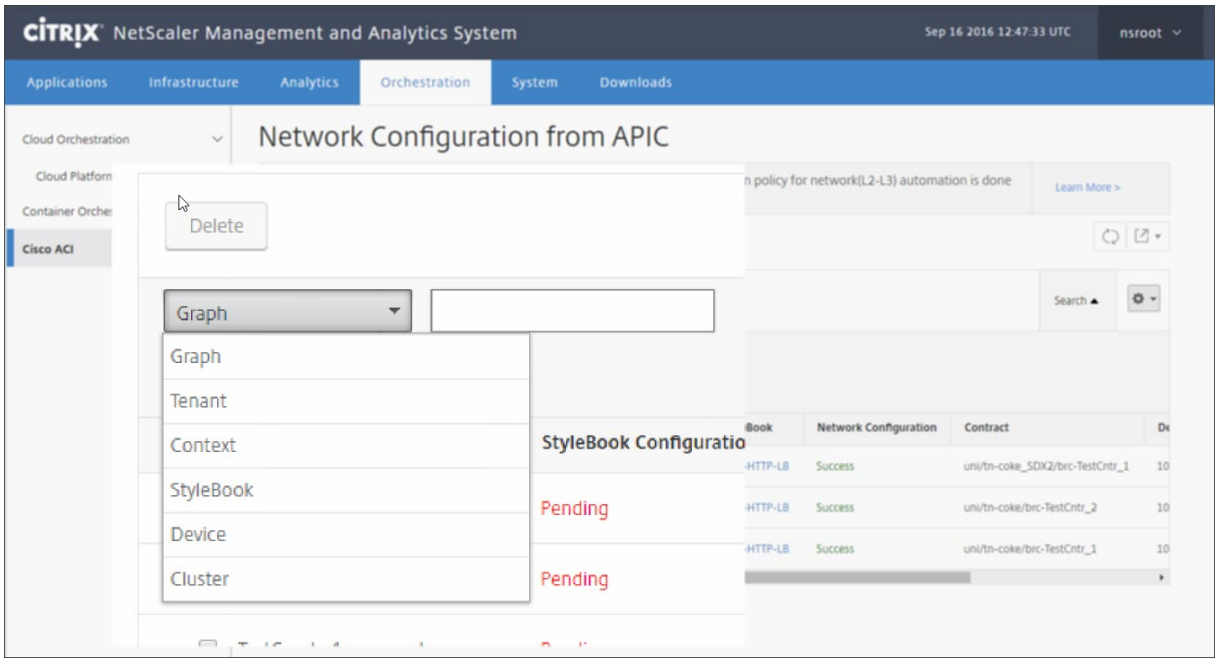
> **Nota**
>
> Si el gráfico se elimina del APIC de Cisco, se elimina la configuración correspondiente del dispositivo, incluida la configuración L4-L7.

Además, la vista tabular permite ordenar cualquier columna de la tabla y filtrar los datos mediante la opción Buscar. También puede personalizar los detalles de las columnas seleccionando o deseleccionando los nombres de las columnas en la lista desplegable de columnas:



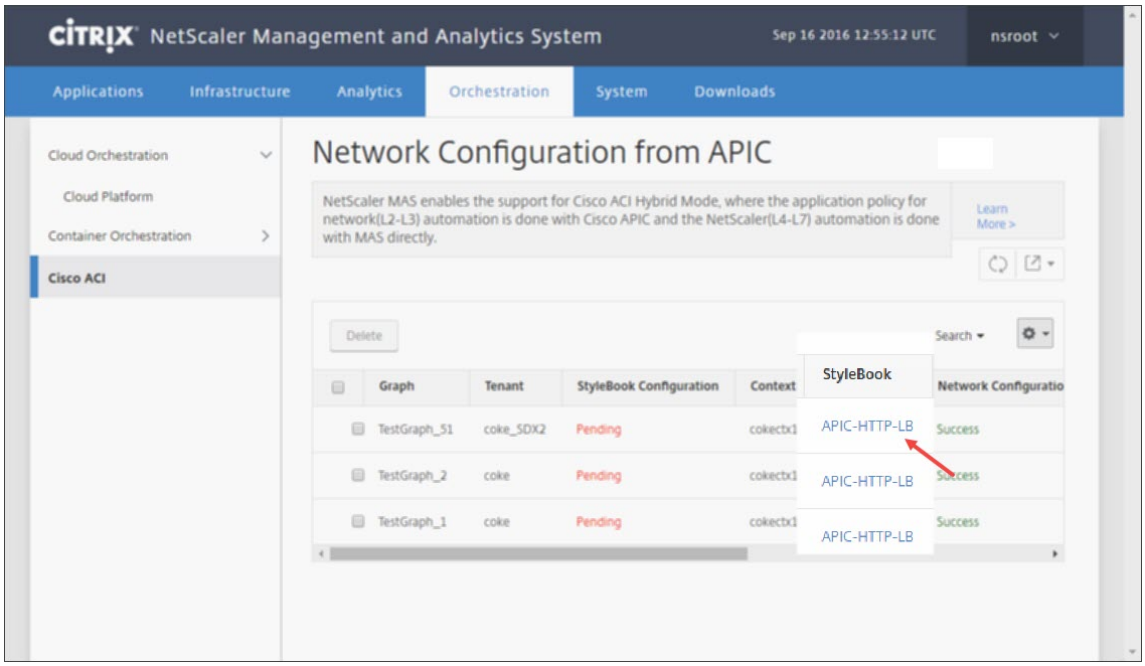
Además, puede hacer clic en el botón **Buscar** y utilizar las opciones de búsqueda para filtrar los datos. Puede seleccionar cualquier columna del cuadro desplegable e introducir el valor correspondiente para filtrar los datos que se muestran en la tabla.

> **Nota**
>
> La función de búsqueda distingue mayúsculas de minúsculas y debe proporcionar los criterios de búsqueda exactos.

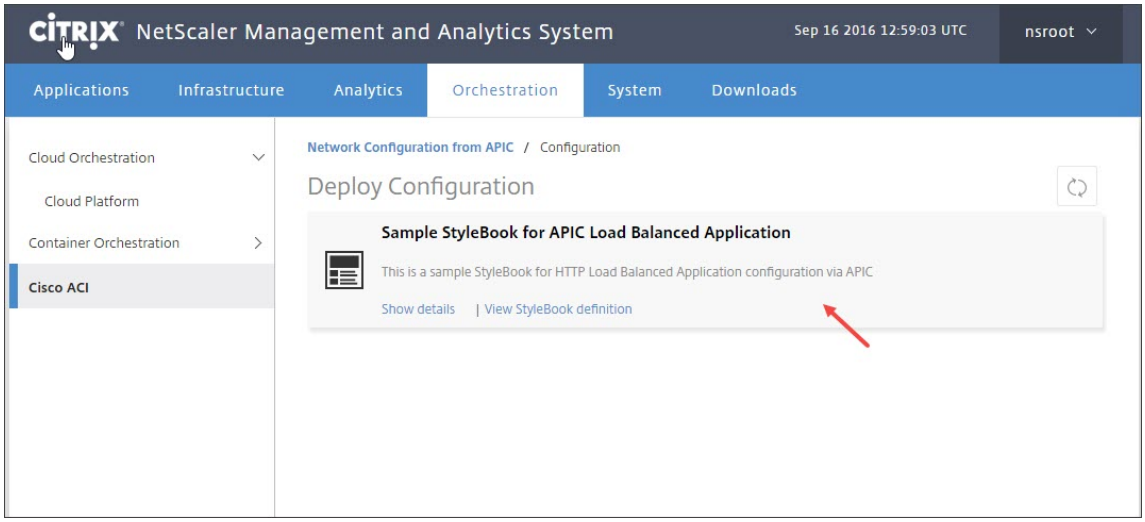


Para implementar la configuración L4-L7 mediante StyleBook en Citrix ADM:

1. Haga clic en el nombre del StyleBook que aparece como URL en la vista tabular.



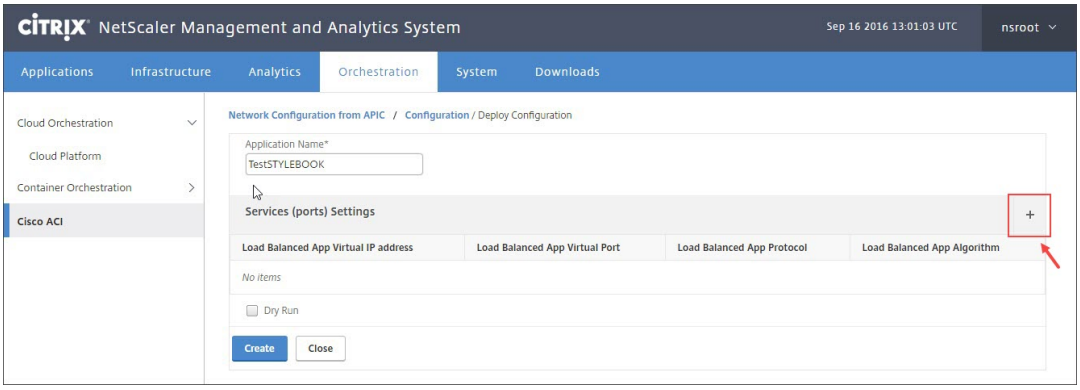
2. En la ventana de configuración, haga doble clic en **StyleBook**.



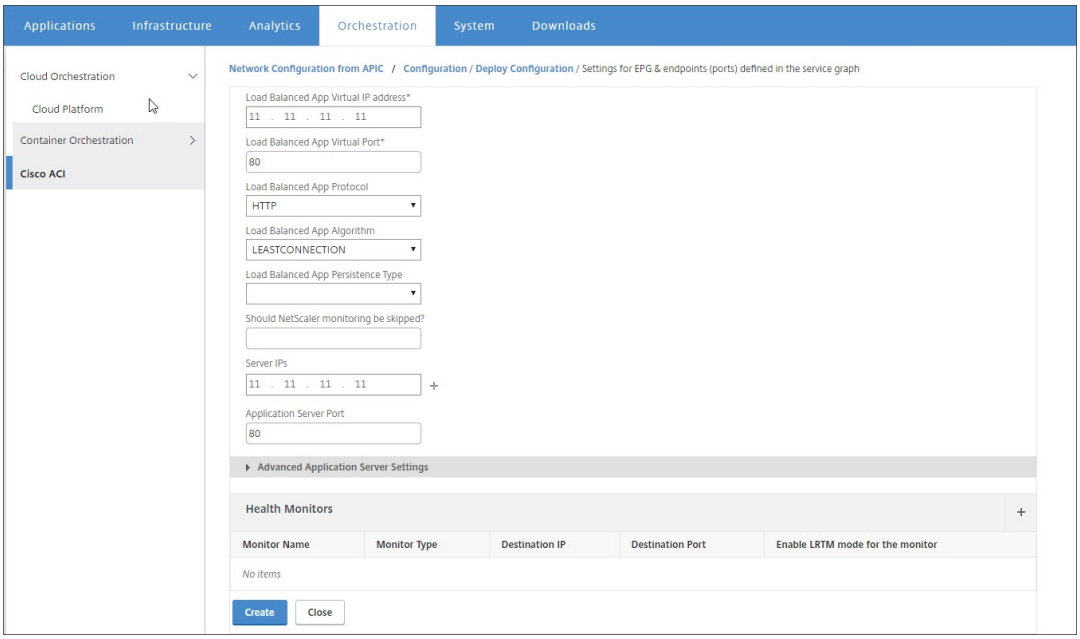
3. En la ventana Configuración de implementación, haga lo siguiente:

   a) En el campo **Nombre de la aplicación**, introduzca el nombre de la configuración de funciones del ADC que corresponda al gráfico de servicios de la aplicación en el APIC.

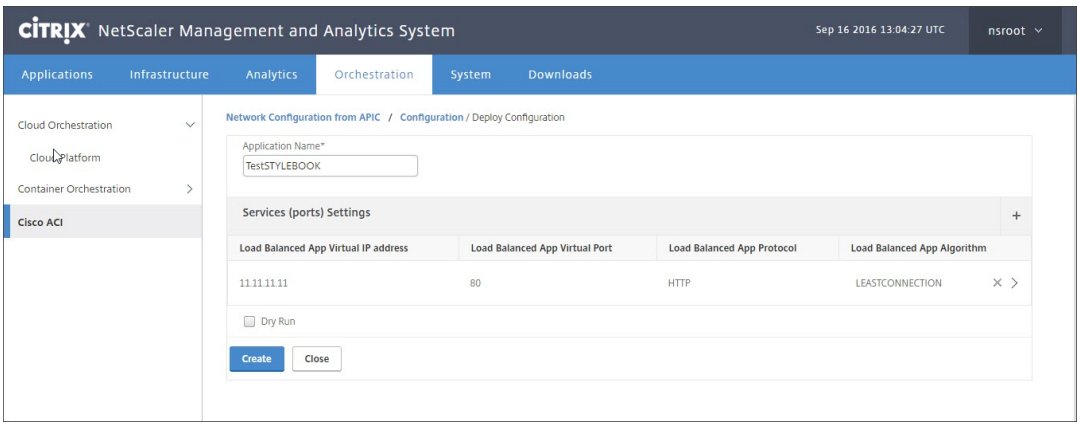
   b) En la sección Configuración del servicio (puertos), haga clic en **+**.



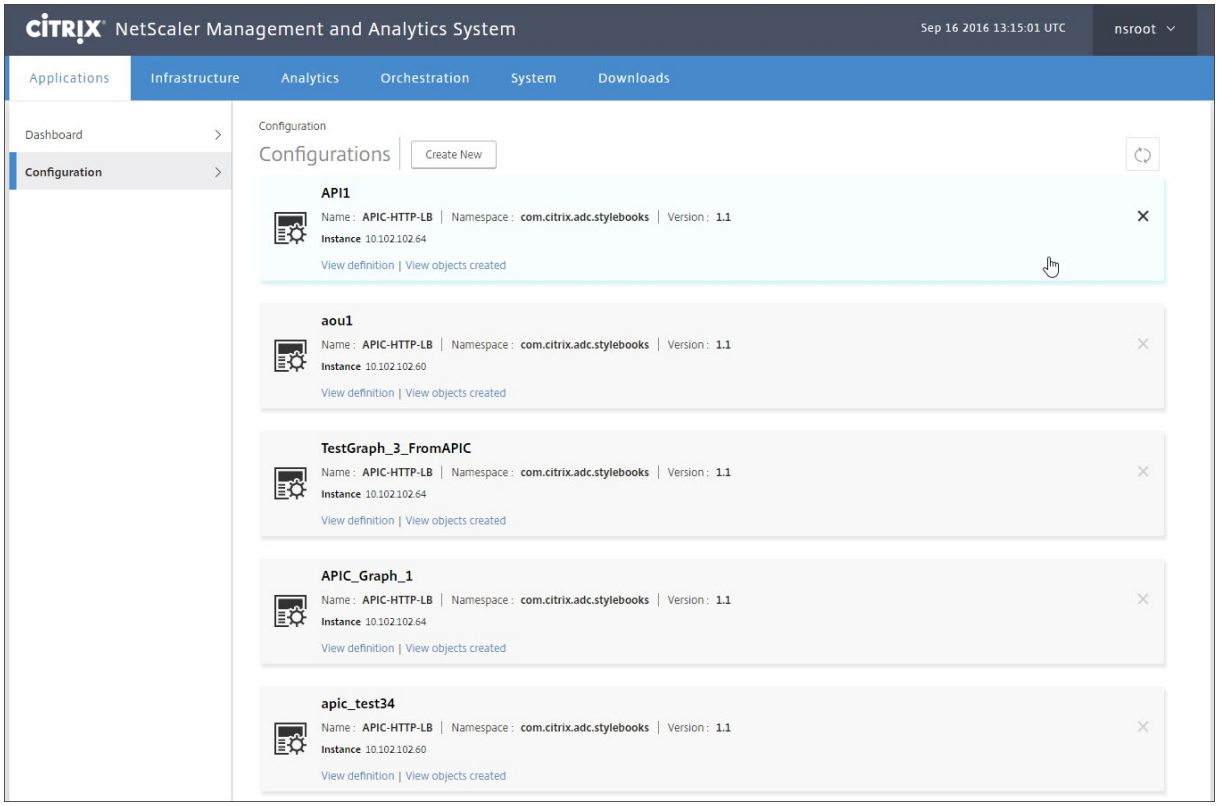
c) **En la**configuración de EPG y puntos finales (puertos) definida en la ventana del gráfico de servicios**, introduzca los valores del parámetro rellenado en el StyleBook y haga clic en Crear.**



d) Haga clic en **Crear**.



La configuración L4-L7 especificada en el StyleBook está implementada en Citrix ADM. **Puede ver la configuración de StyleBoook desde la ficha**Aplicación**, accediendo a Aplicación > Configuración.**



Adjuntar y desenlazar eventos de punto final de APIC

January 30, 2024

La solución de modo híbrido gestiona implícitamente los eventos de conexión o desconexión de terminales de la APIC de Cisco. Cuando la APIC de Cisco desencadena un evento de conexión de punto final, el StyleBook de Citrix Application Delivery Management (ADM) activa automáticamente el servicegroup_servicegroupmember_binding y el punto final se desvincula durante el evento de desconexión del punto final.

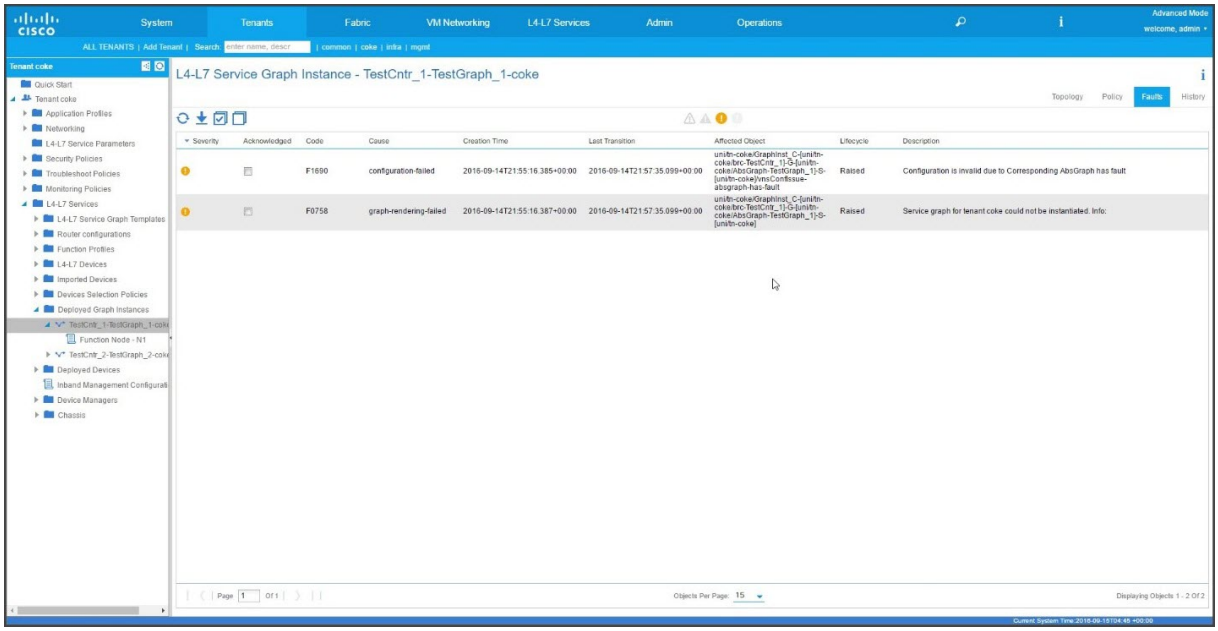
Además, si no ha implementado la configuración L4-L7 en Citrix ADM antes de que se active el evento de conexión o desconexión del punto final en la APIC de Cisco, la solución conservará las direcciones IP adjuntas en la base de datos. Estas direcciones IP se enlazan al grupo de servicios correspondiente una vez creado el grupo de servicios mediante StyleBook.

Informes de fallos de APIC

January 30, 2024

Cuando implementa un paquete de dispositivos Citrix ADC en Cisco ACI, Cisco APIC informa de cualquier error. Puede ver los informes de errores en cualquier nivel de la APIC (por ejemplo, el gráfico de dispositivo, arrendatario, EPG o servicio). La captura de pantalla siguiente muestra un informe de errores a nivel de dispositivo. Para obtener más información sobre los errores, consulte http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html.

Seleccione cualquier entidad de APIC y haga clic en la ficha Errores para mostrar los errores notificados por la APIC para esa entidad.



Registros generados por NetScaler ADM

January 30, 2024

Citrix Application Delivery Management (ADM) proporciona un registro exhaustivo que puede ayudar a solucionar problemas. Los registros generados (**admin.log**) se encuentran en: **/var/controlcenter/log/**

Puede iniciar sesión en Citrix ADM y utilizar el shell para navegar hasta la estructura de directorios de Citrix ADM. A continuación se muestra un fragmento de ejemplo de un registro NetScaler ADM para la implementación de gráficos de APIC.


```
    2016-06-29 10:58:33,816 DEBUG APIC Config  = {
(0, '', 5230): {
'dn': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant': 'coke_SDX2', 'ctxName': 'cokectx1', 'value': {
(10, '', 'ADCHybridMode_1_Consumer_1'): {
'state': 1, 'transaction': 0, 'cifs': {
'ADCHybridMode_1_Device_1': '1_1' }
, 'ackedstate': 0 }
, (7, '', '2129920_32778'): {
'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
, (1, '', 5790): {
'transaction': 0, 'ackedstate': 0, 'value': {
(3, 'ADCFunction', 'N1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'mFCngNetwork', 'mFCngnetwork'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Network_key', 'network_key'): {
'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
 }
 }
, (4, 'internal_network', 'internal_network'): {
'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'internal_network_key', 'internal_network_key'): {
'state': 1, 'transaction': 0, 'target': 'network/internal_snip', 'ackedstate': 0 }
 }
 }
, (2, 'external', 'consumer'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
, (4, 'mFCngStylebook', 'mFCngStylebook'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Stylebook_key', 'Stylebook_key'): {
'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
    }
 }
 }
, (2, 'internal', 'provider'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
 }
 }
```



```
 }
, 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, (4, 'Network', 'network'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'nsip', 'internal_snip'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'type', 'type'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
, (5, 'hostroute', 'hostroute'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
, (5, 'ipaddress', 'ipaddress'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
, (5, 'dynamicrouting', 'dynamicRouting'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
, (5, 'netmask', 'netmask'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0' }
 }
 }
 }
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', 'ackedstate': 0, 'encap': '2129920_32778' }
, (4, 'Stylebook', 'stylebook_1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB' }
 }
 }
 }
, 'txid': 10000 }
 }

   2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', 'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', 'graphInstanceId': 5790 }

   2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
   2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
   2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
   2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
   2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
```



```
            Details  = 10.102.102.62 +++++++++++++++++
88      2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89      2016-06-29 10:58:33,867 DEBUG Host name from device =
           ADCHybridMode_1
90      "InProgress","message":null,"replication_status":"","target":"
           10.102.102.81","operation":"POST","entity_type":"apic","
           entity_id":null }
91    }
92
93      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
94    "errorcode": 0, "message": "Done", "severity": "NONE"  }
95
96      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
97      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
           Config ++++++
98      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99    'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
         }
100   ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102   }
103   collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
           0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
107   ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108   'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790),
         (3, 'ADCFunction', 'N1')], 0) }
109   }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
           []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
113   'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
         : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116   "errorcode": 0, "message": "Done", "severity": "NONE"  }
117   , sessionId = ##
         D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764

118     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {
119   '10.102.102.62': {
120   '10.102.102.62': {
121   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
122   }
123   , (7, '', '2129920_32778'): {
124   'vlan': {
125   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
126   }
```



```
127   , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
          internal', 'provider')), 'nsip'): {
128   'vlan_nsip_binding': {
129   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
130    }
131   , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
          internal_snip')): {
132   'nsip': {
133   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'add_op' }
134    }
135   , (): {
136    }
137   , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
138   'vlan_interface_binding': {
139   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
          u'NONE', 'operation_name': 'bind_op' }
140    }
141    }
142
143      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
144      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
145      2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
          erMsg = Done, statusCode = bind_op
146      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
             = Done, statusCode = add_op
147      2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
          erMsg = Done, statusCode = bind_op
148      2016-06-29 10:58:44,238 DEBUG +++++++++++++++ ServiceAudit response
          = {
149   'faults': [], 'state': 0, 'health': [] }
150
151      2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
152   'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
          uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
153   'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
          coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
          HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
154   , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
          graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
          graphInstanceId': 5790 }
155
156      2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task:
          create apic_graph
157      2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
158      2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
159      2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector
          collection from Config with type 22 for attach & detach event
          ++++++
160      2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
```



```
161   0: [], 1: [], 3: [] }
162
163      2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList
             = []
164      2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
            attachIpList = [] dettachIpList = []
165      2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
166    'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni
        /vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-
        coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName
        ': None, 'configPackId': None, 'tenantName': u'coke_SDX2', '
        styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'
        HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort':
        None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP'
        : None }
167
168  <!--NeedCopy-->
```

Registros generados por el paquete de dispositivos de modo híbrido

January 30, 2024

El paquete de dispositivos Citrix ADC Hybrid Mode genera registros relacionados con la configuración y con la supervisión. Los registros generados se encuentran en **/data/devicescript/Citrix.NetScalerMAS.1.0/logs**.

A continuación se muestra un fragmento de ejemplo de un **debug.log** de Cisco APIC:

```
1      2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
          24063] Device manager details ip = 10.102.102.81, port = 80
2      2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
          24063] +++++++++++++++ serviceAudit  request +++++++++++++++++
3      2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
          24063] ++++++++++ getStyleBookObjects ++++++++++++
4      2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
          24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
           {
5    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6    (5, 'name', 'stylebookName'): {
7    'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
         }
8     }
9     }
10
11     2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
          24063] NMAS collection styleBookName= APIC-HTTP-LB
12     2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
          24063] NMAS collection retCol= {
```



```
13  'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
        'stylebook_1')) }
14
15     2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
          24063]  ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
          /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
          HTTP-LB
16     2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
          24063]  ++++ Response from styleBookresCode serviceAudit = {
17  u'stylebook': {
18  u'uses_builtin_namespaces': {
19  u'netscaler.nitro.config': u'10.5' }
20  , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
       'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
       nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
       : "Sample StyleBook for APIC Load Balanced Application"\
       ndescription: "This is a sample StyleBook for HTTP Load Balanced
       Application configuration via APIC"\nschema-version: "1.0"\nimport-
       stylebooks: \n  - \n    namespace: netscaler.nitro.config\n
       prefix: ns\n    version: "10.5"\n  - \n    namespace: "com.citrix.
       adc.stylebooks"\n    prefix: "stlb"\n    version: "1.1"\nparameters
       -default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n  lb-name(
       appname, port): $appname + "-" + str($port) + "-lb"\n  sg-name(
       appname, port): $appname + "-" + str($port) + "-sg"\n
       healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n
        - \n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
       $parameters.app-services\n    repeat-item: app\n    properties: \
       n      name: $substitutions.lb-name($parameters.appname, $app.
       virtual-port)\n      ipv46: $app.virtual-ip\n      port: $app.
       virtual-port\n      servicetype: $app.protocol\n      lbmethod?:
       $app.algorithm\n      persistencetype?: $app.persistence\n  - \n
        name: svcgrp\n    type: ns::servicegroup\n    repeat: $parameters.
       app-services\n    repeat-item: app\n    properties: \n      name:
       $substitutions.sg-name($parameters.appname, $app.virtual-port)\
       n      servicetype: $app.protocol\n      useproxyport?: $app.sg-
       advanced.useproxyport\n      usip?: $app.sg-advanced.usip\n
       cip?: $app.sg-advanced.cip\n      cipheader?: $app.sg-advanced.
       cipheader\n      healthmonitor?: $substitutions.healthmonitor($app.
       skip_healthmonitor)\n    components: \n      -\n        name:
       lbvserver-svg-binding\n        type: ns::
       lbvserver_servicegroup_binding\n        properties: \n
       name: $substitutions.lb-name($parameters.appname, $app.virtual-port
       )\n          servicegroupname: $parent.properties.name\n      - \
       n        name: svg-members\n        type: ns::
       servicegroup_servicegroupmember_binding\n        condition: $app.
       server-ips\n        repeat: $app.server-ips\n        repeat-item:
       serverip\n        properties: \n          ip: $serverip\n
       port: $app.server-port\n          servicegroupname: $parent.
       properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
       $components.lbvserver\n  - \n    name: servicegroups\n    value:
       $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21  u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
       ': u'APIC-ROOT' }
```



```
22  ] }
23   }
24
25      2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
           24063]  ++++ Dev Mgr request details devMgrUrl = http://
           10.102.102.81/admin/v1/apic
26      2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
           24063]  ++++ Response from Device Mgr serviceAudit = {
27  "APIC":[] }
28
29      2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response = {
30  "APIC":[] }
31
32      2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers content type
           = application/json; charset=utf-8
33      2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers = {
34  'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
       c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
        'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
       10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
       application/json; charset=utf-8' }
35
36      2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
           24063] ++++++++++++++ pollingURL = http://10.102.102.81/admin/v1
           /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37      2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 0
38      2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
39  u'journalcontext': {
40  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
        u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
       service_name': u'admin', u'start_time': u'2016-06-29T10
       :58:33.760565', u'is_default': u'false', u'end_time': None, u'
       target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
       -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41   }
42
43      2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
           24063] ++++++++++++++ pollingStatus = True, pollingTime = 1
44      2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
           24063] ++++++++++++++ pollingResponse json = {
45  u'journalcontext': {
46  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
        u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
       service_name': u'admin', u'start_time': u'2016-06-29T10
       :58:33.760565', u'is_default': u'false', u'end_time': None, u'
       target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
       -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47   }
```



```
48
49      2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
           24063] +++++++++++++++ pollingStatus = True, pollingTime = 2
50      2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
           24063] +++++++++++++++ pollingResponse json = {
51   u'journalcontext': {
52   u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
        Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
        T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
        , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
        replication_status': u'' }
53    }
54
55      2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
           24063] Attempts 1
56      2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
           24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
            '', 5230)), transaction: 0
57      2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
           24063] Attempts for {
58   'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
        'devs': {
59   'ADCHybridMode_1_Device_1': {
60   'state': 0, 'virtual': False, 'manager': {
61   'hosts': {
62   '10.102.102.81': {
63   'port': 80 }
64    }
65   , 'name': 'NMAS_1', 'creds': {
66   'username': 'nsroot', 'password': '<hidden>' }
67    }
68   , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69   'username': 'nsroot', 'password': '<hidden>' }
70    }
71    }
72   , 'manager': {
73   'hosts': {
74   '10.102.102.81': {
75   'port': 80 }
76    }
77   , 'name': 'NMAS_1', 'creds': {
78   'username': 'nsroot', 'password': '<hidden>' }
79    }
80   , 'contextaware': True, 'port': 80, 'creds': {
81   'username': 'nsroot', 'password': '<hidden>' }
82    }
83    is 0
84      2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
           24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
           (0, '', 5230))
85      2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
```



```
           24063] pending: False, delete: False, txId: None
86      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
           24063] Faults: []
87      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
           24063] Health: []
88      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
           24063] Send num: 761, type: 220, len: 382
89  <!--NeedCopy-->
```

Paquete de dispositivos NetScaler ADC en el modo de orquestación de nube de ACI de Cisco

January 30, 2024

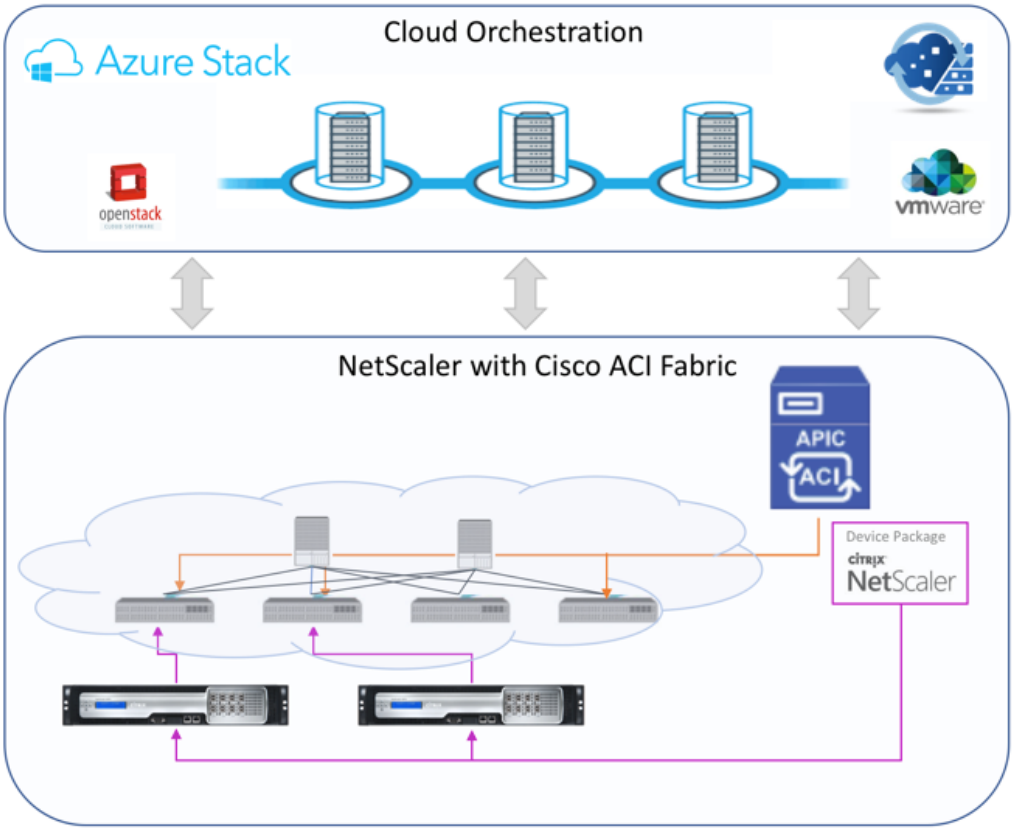
Con Application Policy Infrastructure Controller (APIC) versión 3.1, Citrix NetScaler ADC y Cisco ACI amplían la cartera de integración conjunta para proporcionar una nueva solución que aborde las necesidades del cliente. El nuevo modo de integración, ACI Cloud Orchestrator Mode*, simplifica las integraciones L4-L7 al abstraer la complejidad de la configuración a través de parámetros estandarizados. La solución funciona a la perfección para automatizar los servicios L4-L7, logrando los objetivos de implementaciones ágiles de aplicaciones, flexibilidad operativa y simplicidad.

El modo Cloud Orchestrator de Cisco ACI mediante la solución NetScaler ADC proporciona los siguientes beneficios:

- La automatización de los servicios L4-L7 reduce el error humano.
- La integración prediseñada de la solución Cisco ACI lo ayuda a reducir el tiempo de implementación y aumenta el rendimiento de las aplicaciones, como las aplicaciones web, las máquinas virtuales y SQL.
- Visibilidad totalmente integrada del estado de las aplicaciones, como aplicaciones web, máquinas virtuales y SQL en componentes de red físicos y virtuales.

El modo de orquestador en la nube de ACI ahora le ofrece más opciones para utilizar la nueva GUI de APIC simplificada directamente o seleccionando cualquier orquestador de nube, como Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize o cualquier otro según sus preferencias. Este nuevo cambio se logra al exponer un conjunto de atributos ADC como esquema ADC. Estos atributos se asignan en los perfiles de función de los paquetes de dispositivos. Puede proporcionar valores para estos atributos mientras el orquestador de la nube aprovisiona el servicio ADC (Cisco Cloud Center o Wireless Application Protocol (WAP)).

La siguiente ilustración proporciona una descripción general de NetScaler ADC en una solución de orquestación en la nube:

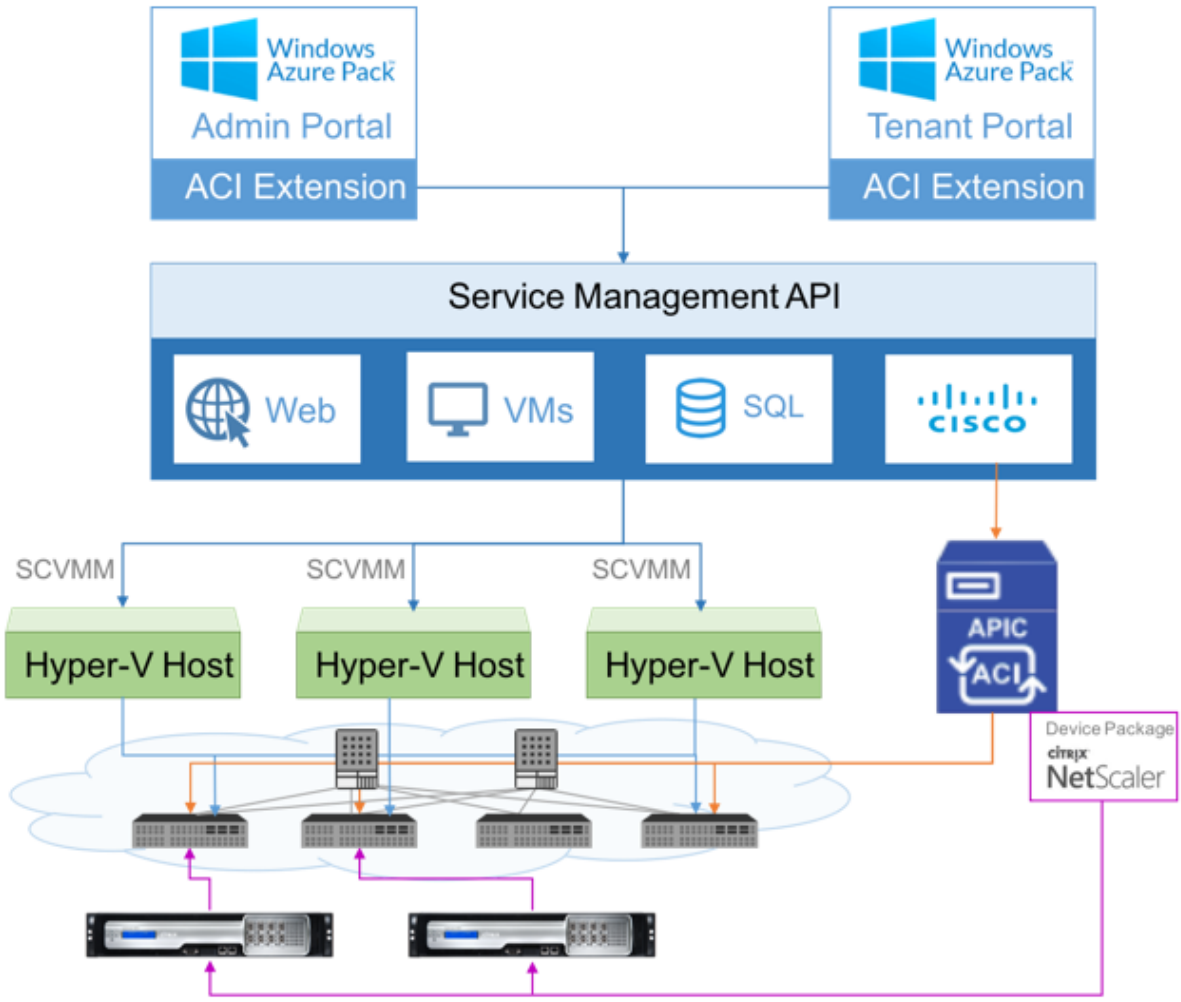


La solución de modo de orquestación en la nube que utiliza Microsoft Azure Pack implica muchos puntos de integración, como Azure Pack a Cisco APIC, Cisco APIC a System Central máquina virtual Manager (SCVMM) y Cisco APIC a NetScaler ADC. Como arrendatario en la nube privada, puede habilitar NAT, aprovisionar servicios de red y agregar un equilibrador de carga.

Azure Pack admite portales de arrendatarios y administradores, y cada uno de ellos tiene su propio conjunto de operaciones que se pueden realizar.

- Como administrador, puede realizar tareas administrativas como el registro de ACI, el rango VIP, la asociación de dispositivos NetScaler ADC con la nube de máquinas virtuales y la creación de cuentas de usuario arrendatario.
- Como arrendatario, puede realizar tareas como iniciar sesión en el portal de arrendatarios de Azure Pack y configurar la red, los dominios de puente y el enrutamiento y reenvío virtuales (VRF), y puede usar las funciones de equilibrio de carga y RNAT de NetScaler ADC.

La siguiente ilustración proporciona información general sobre Azure Pack en una solución de modo de nube:



Importante

- El administrador de la nube puede facilitar con el esquema L4-L7 compatible con APIC y el administrador de APIC puede realizar cualquier cambio adicional directamente en el APIC. Esto le permite configurar e implementar NetScaler ADC a la par del conjunto de funciones admitidas.
- Los arrendatarios pueden implementar varias direcciones VIP con diferentes puertos para la misma red. Debe asegurarse de que la combinación de IP y puerto sea única.
- El paquete de dispositivos NetScaler ADC solo admite la implementación de un solo contexto. Cada arrendatario recibe una instancia de NetScaler ADC dedicada.
- El Protocolo de aplicaciones inalámbricas (WAP) admite dispositivos NetScaler ADC MPX y dispositivos NetScaler ADC VPX (incluye instancias NetScaler ADC VPX implementadas en la plataforma NetScaler ADC SDX).

El paquete de dispositivos en modo de orquestador de nube admite tanto el modo completamente administrado como el modo de administrador de servicios. El paquete de modo completamente administrado admite una amplia variedad de perfiles de función, como el equilibrio de carga simple, el cambio de contenido, la descarga SSL y otros perfiles. Estos perfiles de función cubren un conjunto de funciones y un modo de implementación completos de NetScaler ADC. Del mismo modo, el paquete de dispositivos en modo administrador de servicios admite la configuración e implementación de un brazo y dos brazos de NetScaler ADC mediante APIC. NetScaler Application Delivery Management (ADM) actúa como administrador de servicios para APIC y puede usar NetScaler ADM para configurar los parámetros de NetScaler ADC L4-L7.

> **Nota**
>
> En el modo administrador de servicios (modo híbrido), no puede reutilizar ni reasignar la misma dirección IP del servidor, que ya está presente en el dispositivo NetScaler ADC.

El perfil de función del modo de orquestador de nube tiene un conjunto de parámetros asignados al esquema ADC de APIC y el orquestador usa estos parámetros. El orquestador en la nube proporciona los valores para los parámetros ADC (VIP, mientras se aprovisiona NetScaler ADC a través de APIC). El orquestador se comunica con las API de APIC y pasa los detalles específicos del ADC como parte de la carga útil para un perfil de función específico. Internamente, APIC extrae los valores y los pasa al paquete de dispositivos que configura internamente el NetScaler ADC.

Para obtener más información sobre la lista completa de esquemas ADC, que son compatibles con Cisco APIC, consulte Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, versión 3.x y anteriores).

El paquete de dispositivos de modo completamente administrado admite los siguientes perfiles de función:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC

11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

El paquete de dispositivos en modo de gestión de servicios admite los siguientes perfiles de función en modo nube:

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler ADC admite los perfiles de función mencionados anteriormente. El APIC admite un subconjunto de estos parámetros en el esquema ADC. Si hay algún atributo no admitido por Cisco ACI presente en el perfil de función, debe clonar el perfil de función del modo de orquestador de la nube y proporcionar los valores para todos los atributos no admitidos por APIC y debe guardar los atributos. Más adelante, el orquestador puede usar el perfil de función recién clonado.

El paquete de dispositivos de Citrix Cloud Mode admite NetScaler ADC 12.0 y el modo administrador de servicios también usa NetScaler ADM 12.0. El paquete de dispositivos ha cambiado la versión del modelo de 1.0 a 2.0 y se puede usar como una nueva instalación. El paquete de dispositivos Cloud

Orchestrator Mode no se puede actualizar desde versiones anteriores de paquetes de dispositivos ya que se ha cambiado la versión del modelo.

Los paquetes de dispositivos de Cloud Orchestrator Mode también se pueden usar en implementaciones normales. El paquete no obliga al usuario a aprovisionar NetScaler ADC a través de ningún orquestador en la nube. El paquete de dispositivos es compatible solo con APIC y APIC con Cloud Orchestrator.

Capacidad agrupada de NetScaler ADC

January 30, 2024

La capacidad agrupada de NetScaler ADC le permite compartir licencias de instancia o ancho de banda entre diferentes factores de forma ADC. Para las instancias basadas en suscripciones de CPU virtuales, puede compartir la licencia de CPU virtual en todas las instancias. Use esta capacidad agrupada para las instancias que se encuentran en el centro de datos o en las nubes públicas. Cuando una instancia ya no requiere los recursos, comprueba la capacidad asignada de nuevo en el grupo común. Reutilice la capacidad liberada en otras instancias de ADC que necesiten recursos.

Puede usar las licencias agrupadas para maximizar la utilización del ancho de banda al garantizar la asignación de ancho de banda necesaria a una instancia y no más de lo que necesita. Aumente o reduzca el ancho de banda asignado a una instancia en tiempo de ejecución sin afectar el tráfico. Con las licencias de capacidad agrupadas, puede automatizar el Provisioning de instancias.

Cómo funcionan las licencias de capacidad agrupada de NetScaler ADC

La capacidad agrupada de NetScaler ADC tiene los siguientes componentes:

- Instancias de NetScaler ADC, que se pueden clasificar en:
  - Hardware de capacidad cero
  - Instancias VPX independientes o instancias CPX
- Grupo de ancho de banda
- Grupo de instancias
- Citrix ADM configurado como servidor de licencias

Hardware de capacidad cero

Cuando se administran a través de la capacidad agrupada de NetScaler ADC, las instancias MPX y SDX se denominan “hardware de capacidad cero”porque estas instancias no pueden funcionar hasta que

saquen recursos del ancho de banda y los grupos de instancias. Por lo tanto, estas plataformas también se denominan dispositivos MPX-Z y SDX-Z.

El hardware de capacidad cero requiere una licencia de plataforma para poder obtener ancho de banda y una licencia de instancia del grupo común. Sin embargo, no puede utilizar la capacidad agrupada de NetScaler ADC en otra instancia de hardware NetScaler ADC.

Gestione e instale las licencias de plataforma. Debe instalar manualmente una licencia de plataforma mediante el número de serie del hardware o el código de acceso a la licencia. Una vez que se instala una licencia de plataforma, se bloquea en el hardware y no se puede compartir en las instancias de hardware de NetScaler ADC a pedido. Sin embargo, puede mover manualmente la licencia de plataforma a otra instancia de hardware de NetScaler ADC.

Las instancias ADC MPX que ejecutan la versión 11.1 del software ADC compilación 54.14 o posterior y las instancias SDX de ADC que ejecutan 11.1 compilación 58.13 o posterior admiten la capacidad agrupada de ADC. Para obtener más información, consulte **la Tabla 1. Capacidad agrupada compatible para instancias MPX y SDX**.

Instancias independientes de NetScaler ADC VPX

Las instancias de NetScaler ADC VPX que ejecutan el software NetScaler ADC versión 11.1 compilación 54.14 y posteriores en los siguientes hipervisores admiten la capacidad agrupada:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Las instancias de Citrix ADC VPX que ejecutan la versión 12.0, compilación 51.24 y versiones posteriores del software Citrix ADC en los siguientes hipervisores y plataformas en la nube admiten la capacidad agrupada

- Microsoft Hyper-V
- AWS
- Microsoft Azure

> **Nota**
>
> Para habilitar la comunicación entre NetScaler ADM y Microsoft Azure o AWS, se debe configurar un túnel IPSEC. Para obtener más información, consulte Agregar instancias de Citrix ADC VPX implementadas en la nube a Citrix ADM.
> A diferencia del hardware de capacidad cero, VPX no requiere licencia de plataforma. Para procesar el tráfico, debe desproteger el ancho de banda y una licencia de instancia del grupo.

Instancias CPX independientes de NetScaler ADC

Las instancias CPX de NetScaler ADC implementadas en un host Docker admiten capacidad agrupada. A diferencia del hardware de capacidad cero, el CPX no requiere licencia de plataforma. Para procesar el tráfico, debe retirar una licencia de instancia del grupo.

Grupo de ancho de banda

El grupo de ancho de banda es el ancho de banda total que pueden compartir las instancias de NetScaler ADC, tanto físicas como virtuales. El grupo de ancho de banda comprende grupos separados para cada edición de software (Standard, Enterprise y Platinum). Una instancia determinada de NetScaler ADC no puede tener ancho de banda de diferentes grupos retirados simultáneamente. El conjunto de ancho de banda desde el que puede comprobar el ancho de banda depende de la edición de software para la que se licencia.

Grupo de instancias

El grupo de instancias define el número de instancias VPX o CPX que se pueden administrar mediante la capacidad agrupada de NetScaler ADC o el número de instancias VPX en una instancia SDX-Z.

Cuando se desactiva del grupo, una licencia desbloquea los recursos de las instancias MPX-Z, SDX-Z, VPX y CPX, incluidos CPUs/PE, núcleos SSL, paquetes por segundo y ancho de banda.

> **Nota**
>
> El servicio de administración de un SDX-Z no consume una instancia.

Servidor de licencias NetScaler ADM

La capacidad agrupada de Citrix ADC utiliza el software Citrix ADM configurado como un servidor de licencias para administrar las licencias de capacidad agrupada: licencias de grupo de ancho de banda y licencias de grupo de instancias. Puede usar Citrix ADM para administrar licencias de capacidad agrupada sin una licencia de ADM.

Al retirar licencias del ancho de banda y del grupo de instancias, el factor de forma y el número de modelo de hardware de NetScaler ADC en un hardware de capacidad cero determina

- El ancho de banda mínimo y la cantidad de instancias que una instancia de NetScaler ADC debe desproteger antes de funcionar.
- El ancho de banda máximo y el número de instancias que puede desproteger un dispositivo NetScaler ADC.

- La unidad de ancho de banda mínima para cada check-out de ancho de banda. La unidad de ancho de banda mínimo es la unidad de ancho de banda más pequeña que un dispositivo NetScaler ADC tiene que sacar de un grupo. Cualquier check-out debe ser un múltiplo entero de la unidad mínima de ancho de banda. Por ejemplo, si la unidad de ancho de banda mínima de un NetScaler ADC es de 1 Gbps, se pueden proteger 100 Gbps, pero no 200 Mbps o 150.5 Gbps. La unidad de ancho de banda mínimo es diferente del requisito de ancho de banda mínimo. Una instancia de NetScaler ADC solo puede funcionar después de obtener licencia con al menos el ancho de banda mínimo. Una vez que se alcanza el ancho de banda mínimo, la instancia puede obtener más ancho de banda con la unidad de ancho de banda mínima.

En las tablas 1, 2 y 3 se resumen el ancho de banda máximo y las instancias, el ancho de banda mínimo y la unidad de ancho de banda mínima para todas las instancias de NetScaler compatibles. En la tabla 4 se resumen los requisitos de licencia para los diferentes formatos. Para todas las instancias de Citrix ADC compatibles:

Tabla 1. Capacidad agrupada admitida para instancias MPX y SDX

Línea de productos	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
MPX 5900Z	10	1	N/D	N/D	1 Gbps
MPX 8005Z	15	5	NA	NA	1 Gbps
MPX 8900Z	33	5	NA	NA	1 Gbps
Serie MPX-14000Z	100	20	NA	NA	1 Gbps
Serie MPX-15000Z	100	20	NA	NA	1 Gbps
MPX-25000Z-40G	200	100	NA	NA	1 Gbps
Serie MPX-24000Z	150	100	40	80	1 Gbps
SDX 8015Z	15	2	1	5	1 Gbps
Serie SDX 89XX	33	10	2	7	1 Gbps

Línea de productos	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
Serie SDX-115XX	42	7	2	20	1 Gbps
Serie SDX-14000Z	100	10	2	25	1 Gbps
SDX 15000Z-50G	100	10 (Nota: 20 Gbps para versiones inferiores a 12.1 54.x)	2 (Nota: 5 instancias para versiones inferiores a 12.1 54.x)	55	1 Gbps
SDX- 1500 Z	100	10 (Nota: 20 Gbps para versiones inferiores a 12.1 54.x)	2 (Nota: 5 instancias para versiones inferiores a 12.1 54.x)	55	1 Gbps
Serie SDX-22XXX	120	20	10	80	1 Gbps
SDX-25000Z-40G	200	50	10	115	1 Gbps
SDX 2600Z-100G	200	50	10	115	1 Gbps
SDX 26000Z	200	50	10	115	1 Gbps
SDX 2600Z-50S	200	50	10	115	1 Gbps
SDX 8005Z	15	2	1	2	1 Gbps
Serie SDX-24000Z	150	50	10	80	1 Gbps

> Nota
>
> El ancho de banda y las instancias mínimos se aplican a las instancias SDX que ejecuten las sigu-

> ientes versiones y superiores: 11.1 64.x, 12.0 63.x y 12.1 54.x.
>
> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

Tabla 2. Capacidad agrupada admitida para instancias CPX

	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
CPX	10	1	1	1	10 Mbps

Tabla 3. Capacidad agrupada compatible para instancias VPX en hipervisores y servicios en la nube

Hipervisor/servicio en la nube	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Mbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXi	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	5 Gbps	10 Mbps	1	1	10 Mbps
Azure	3 Gbps	10 Mbps	1	1	10 Mbps

> Nota
>
> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

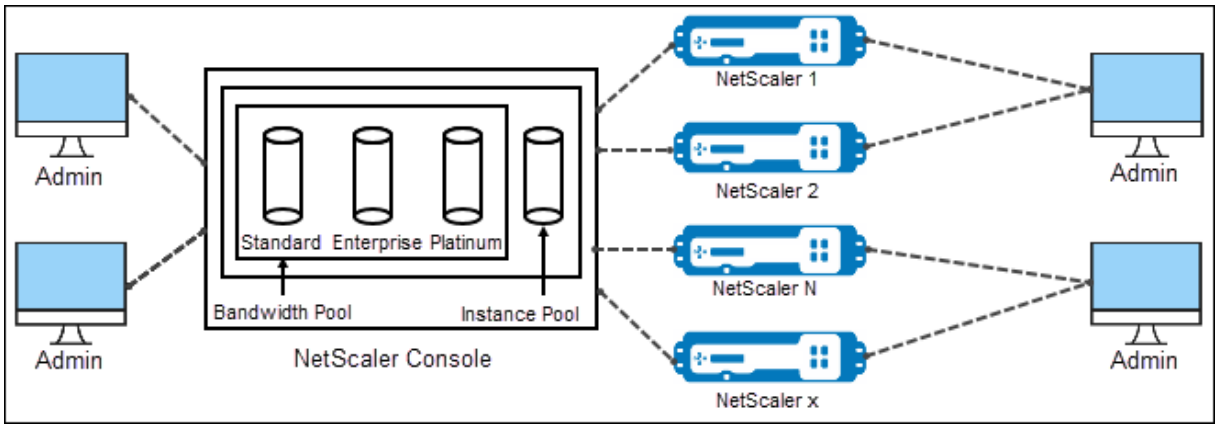
Tabla 4. Requisito de licencia para diferentes factores de forma

Línea de productos	Compra de hardware de capacidad cero	Suscripción Bandwidth & Edition	Suscripción de instancias
MPX	Se requiere licencia	Se requiere licencia	-
SDX	Se requiere licencia	Se requiere licencia	Se requiere licencia
VPX	-	Se requiere licencia	Se requiere licencia
CPX	-	-	Se requiere licencia

Configurar la capacidad agrupada de Citrix ADC

January 30, 2024

Citrix Application Delivery Management (ADM) es el servidor de licencias para todas las instancias de Citrix ADC agregadas a ADM. Puede cargar los archivos de licencia de capacidad agrupados (grupo de ancho de banda o grupo de instancias) al servidor de licencias. Puede asignar licencias del grupo de licencias a instancias de Citrix ADC a petición. Puede asignar las licencias desde Citrix ADM o puede retirar las licencias de las instancias de Citrix ADC (MPX-Z /SDX-Z/VPX/CPX) según la capacidad mínima y máxima de la instancia.



Versiones de hardware y software compatibles

Versión del software Citrix ADC	Hardware Citrix ADC MPX de capacidad cero	Hardware Citrix ADC SDX de capacidad cero	Hipervisores compatibles con Citrix ADC VPX
11.1 Compilación 54.14 y versiones posteriores 12.0 Build 51.24 y posterior	MPX-14000Z, MPX-14000Z-40G, MPX-25000Z-40G	SDX-14000Z, SDX-14000Z-40G, SDX-25000Z-40G	VMware ESX 6.0, Citrix Hypervisor, Linux KVM Microsoft Hyper-V, Amazon AWS, Microsoft Azure

Configurar Citrix ADM como servidor de licencias

Puede configurar Citrix ADM como servidor de licencias para la capacidad agrupada de Citrix ADC. Hay dos formas de que una instancia de Citrix ADC obtenga ancho de banda o licencia de instancia, o ambas:

- Una instancia de Citrix ADC puede iniciar la solicitud de salida a Citrix ADM para obtener su ancho de banda o sus licencias de instancia.
- Las licencias se pueden asignar a una instancia de Citrix ADC a través de Citrix ADM.

> **Nota**
>
> La capacidad agrupada se muestra en Citrix ADM solo si se agregan licencias agrupadas al Citrix ADM.

Los siguientes son los modos de funcionamiento de las instancias de Citrix ADC que utilizan la capacidad agrupada de Citrix ADC:

- **Óptimo**: la instancia se ejecuta con la capacidad de licencia adecuada.
- **Discordancia**de capacidad : la instancia se ejecuta con una capacidad inferior a la configurada por el usuario.
- **Grace**: la instancia se ejecuta con una licencia Grace.
- **Gracia y falta de coincidencia**: la instancia se ejecuta en estado de gracia, pero con una capacidad inferior a la configurada por el usuario.
- **No disponible**: la instancia no está registrada en Citrix ADM para su administración o la comunicación Nitro de Citrix ADM a la instancia no funciona.
- **No asignada**: la licencia no está asignada en la instancia.

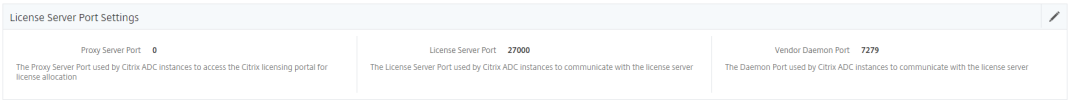
Para instalar archivos de licencia en NetScaler ADM:

1. En un explorador web, escriba la dirección IP del **Citrix ADM** (por ejemplo, http://192.168.100.1).

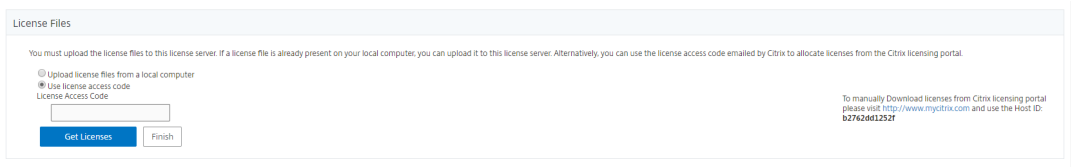
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes > Licencias** .
4. En la sección **Archivos de licencias**, seleccione una de las siguientes opciones:

   - **Cargar archivos de licencias desde un equipo**local : si ya hay un archivo de licencias en su equipo local, puede cargarlo en Citrix ADM. Para agregar archivos de licencia, haga clic **en**Examinar y seleccione el archivo de licencia (.lic) que desee agregar. Luego haga clic en **Finalizar**.

     > **Nota**
     >
     > Si los archivos de licencias cargados no agregan las licencias en la capacidad agrupada de Citrix ADC, puede seleccionar los archivos de licencias y hacer clic en **Aplicar licencias** para agregar las licencias al grupo.



   - **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso de licencia (LAC) para las licencias que compra. Para agregar archivos de licencia, introduzca el LAC en el cuadro de texto y, a continuación, haga clic en **Obtener licencias** .



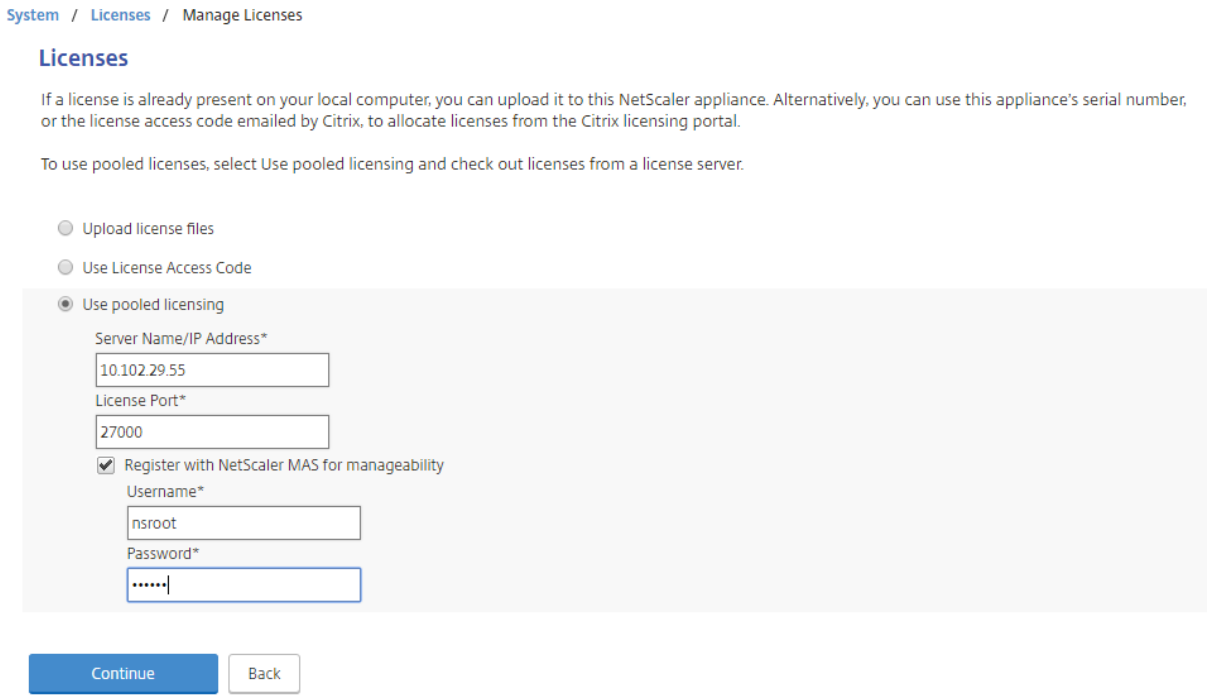
     > **Nota**
     >
     > En cualquier momento, puede añadir más licencias a Citrix ADM desde la configuración de licencias.

Para asignar licencias de capacidad agrupada de Citrix ADC desde Citrix ADM:

> **Nota**
>
> Si no ha registrado la instancia de Citrix ADC en Citrix ADM, puede retirar las licencias de Citrix ADM, pero no puede asignarlas desde Citrix ADM a la instancia de Citrix ADC con capacidad agrupada habilitada.

Asegúrese de cumplir los siguientes requisitos previos antes de asignar licencias de capacidad agrupada a las instancias de ADC.

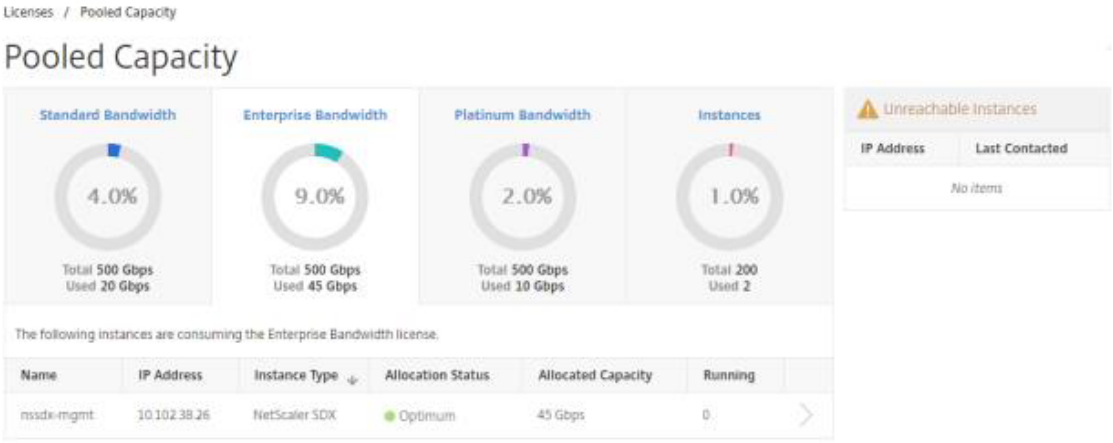
> **Requisito**
>
> previo Antes de poder administrar las licencias del grupo de instancias a través de Citrix ADM, debe registrar la instancia de Citrix ADC en Citrix ADM. En la GUI de Citrix ADC, vaya a **Sistema** > **Licencias** > **Administrar licencias** y seleccione la casilla **Registrarse en Citrix ADM para facilitar la administración** al agregar la IP de Citrix ADM.



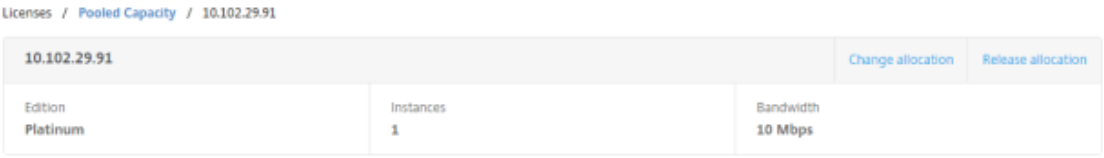
> **Nota**
>
> En los campos **Nombre** de usuario y **Contraseña** de la pantalla anterior, introduzca las credenciales de Citrix ADM.

Una vez registrada la instancia en el servidor de licencias, asigne las licencias de la siguiente manera:

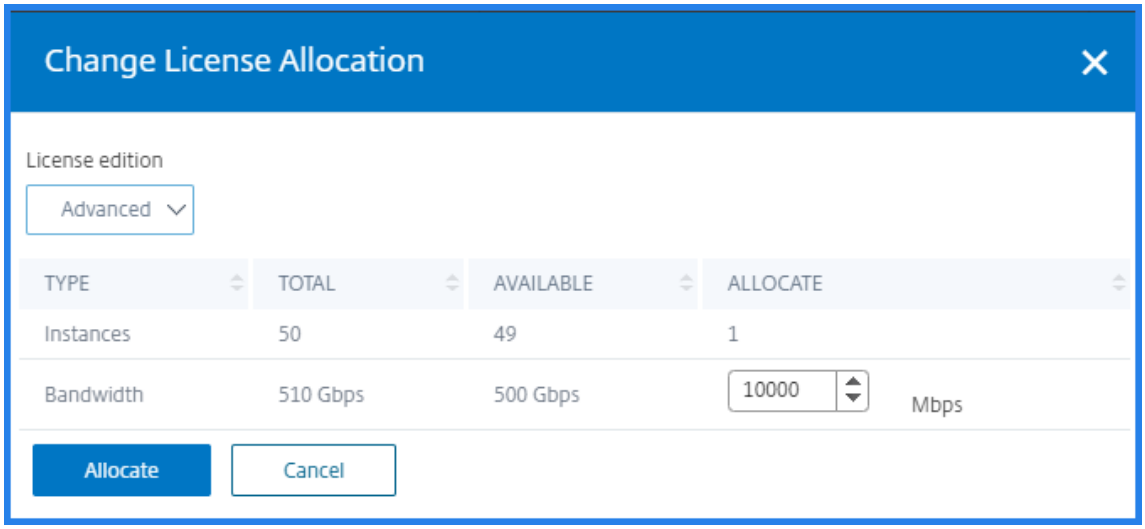
1. En un explorador web, escriba la dirección IP de **Citrix ADM** (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la pestaña Configuración, vaya a **Redes > Licencias > Capacidad** agrupada .
4. Haga clic en el grupo de licencias que quiere administrar.
5. Seleccione una instancia de Citrix ADC de la lista de instancias disponibles haciendo clic en el **botón.**



6. Si desea cambiar o liberar una asignación de licencias, haga clic en **Cambiar asignación** o **Liberar asignación** .



7. Si hace clic en **Cambiar asignación** , aparece una ventana emergente con las licencias disponibles en el servidor de licencias.



8. Puede elegir el ancho de banda o la asignación de instancias a la instancia de Citrix ADC configurando las opciones desplegables **Asignar** . Después de hacer las selecciones, haga clic en **Asignar**.

9. También puede cambiar la edición de licencia asignada en las opciones desplegables de la ventana Cambiar asignación de licencias.

Configuración de la capacidad agrupada de Citrix ADC en MPX-Z

MPX-Z es el dispositivo Citrix ADC MPX con capacidad agrupada de Citrix ADC. El MPX-Z admite la agrupación de ancho de banda para las licencias de las ediciones Platinum, Enterprise o Standard.

El MPX-Z requiere sus licencias de plataforma antes de poder conectarse al servidor de licencias. Puede instalar la licencia de la plataforma MPX-Z cargando el archivo de licencia desde un equipo local o utilizando el número de serie del hardware de la instancia o el código de acceso a la licencia de la sección **Sistema** > **Licencias** de la GUI de la instancia Citrix ADC. Si quita la licencia de la plataforma MPX-Z, la función de capacidad agrupada se deshabilita y todas las licencias retiradas se registran en el servidor de licencias.

Puede modificar dinámicamente el ancho de banda de una instancia MPX-Z sin necesidad de reiniciar. Solo se requiere un reinicio si quiere cambiar la edición de la licencia.

> **Nota**
>
> Cuando reinicias la instancia, comprueba automáticamente las licencias agrupadas necesarias para la capacidad configurada.

Configuración de la capacidad agrupada de Citrix ADC en una instancia de Citrix ADC VPX

Una instancia de Citrix ADC VPX con capacidad agrupada puede extraer licencias de un grupo de ancho de banda (ediciones Platinum/Enterprise/Standard). Puede utilizar la GUI de Citrix ADC para extraer las licencias del servidor de licencias.

Puedes modificar dinámicamente el ancho de banda de una instancia VPX sin necesidad de reiniciar. Solo se requiere un reinicio si quiere cambiar la edición de la licencia.

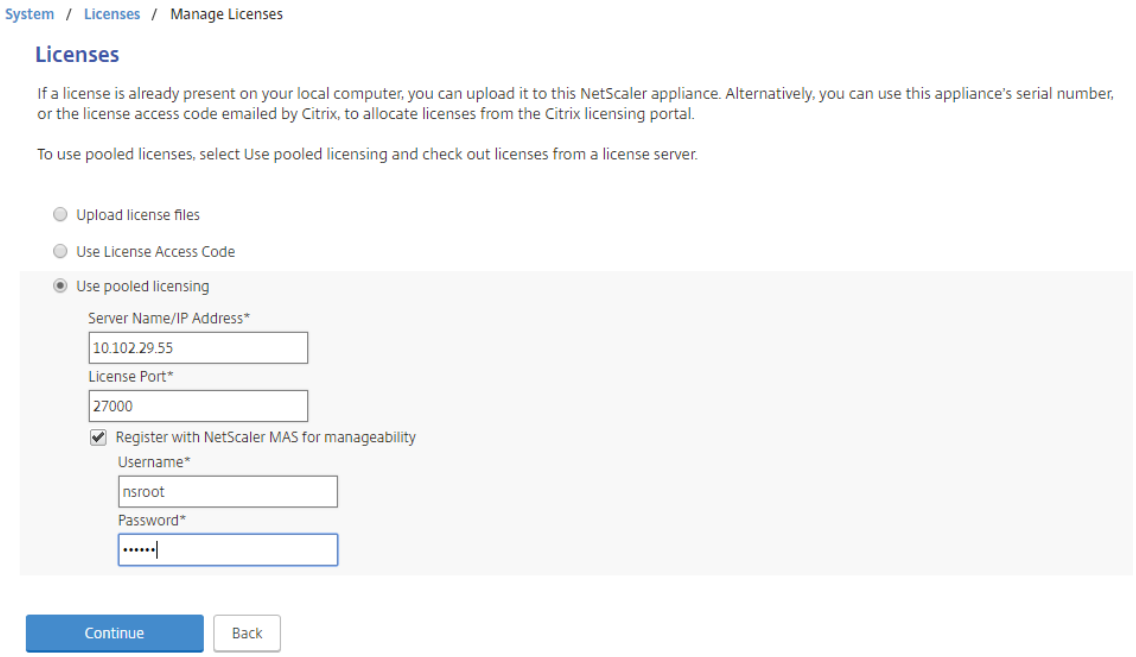
> **Nota**
>
> Cuando reinicies la instancia, eliminará automáticamente las licencias agrupadas necesarias para la capacidad configurada.

Asignación de licencias de grupo a una instancia Citrix ADC MPX-Z o Citrix ADC VPX

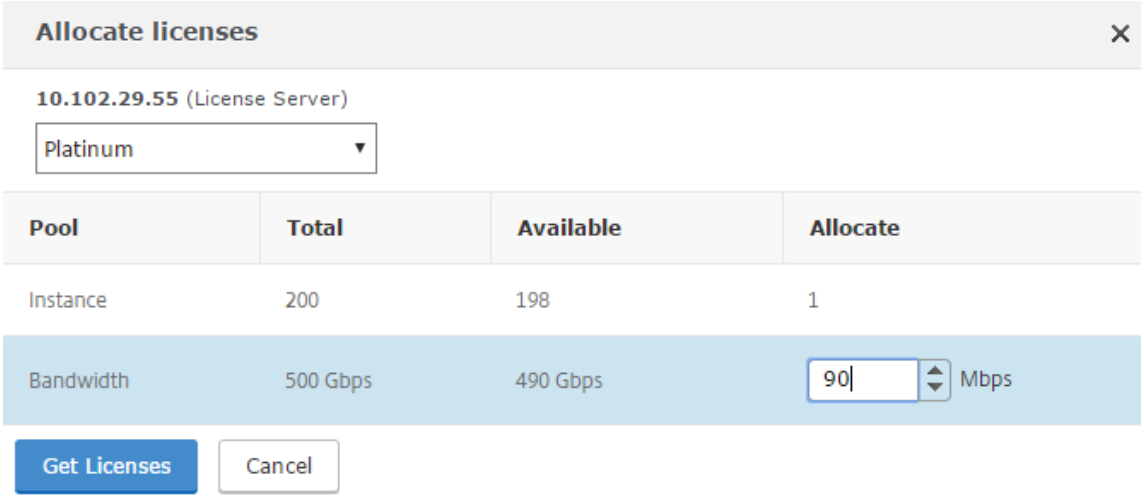
Para asignar sus licencias:

1. En un explorador web, escriba la dirección IP de la instancia de NetScaler ADC (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.

3. En la pestaña Configuración, vaya a **Sistema > Licencias > Administrar licencias** , haga clic en **Agregar nueva licencia** y seleccione **Usar licencias agrupadas** .

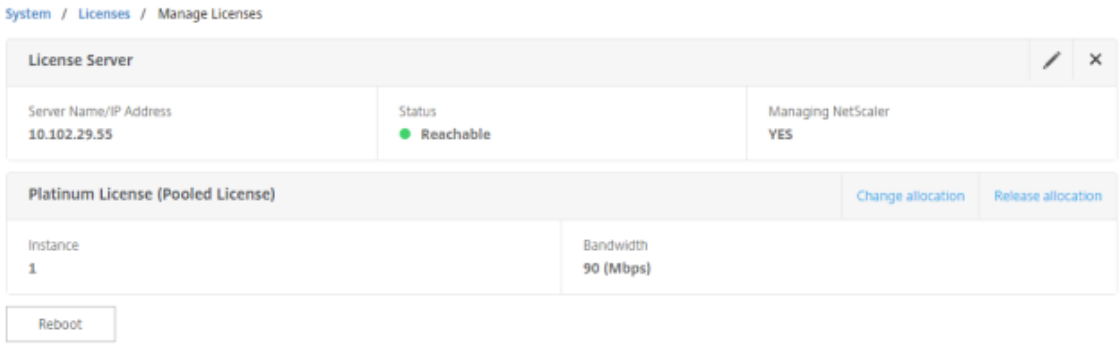


4. Introduzca los detalles del servidor de licencias en el campo **Nombre del servidor/dirección IP**.
5. Si quiere administrar las licencias del grupo de instancias a través de Citrix ADM, seleccione la casilla **Registrarse en Citrix ADM para facilitar la administración** e introduzca las credenciales de ADM .
6. Seleccione la edición de la licencia y el ancho de banda requerido y haga clic en **Obtener licencias** .



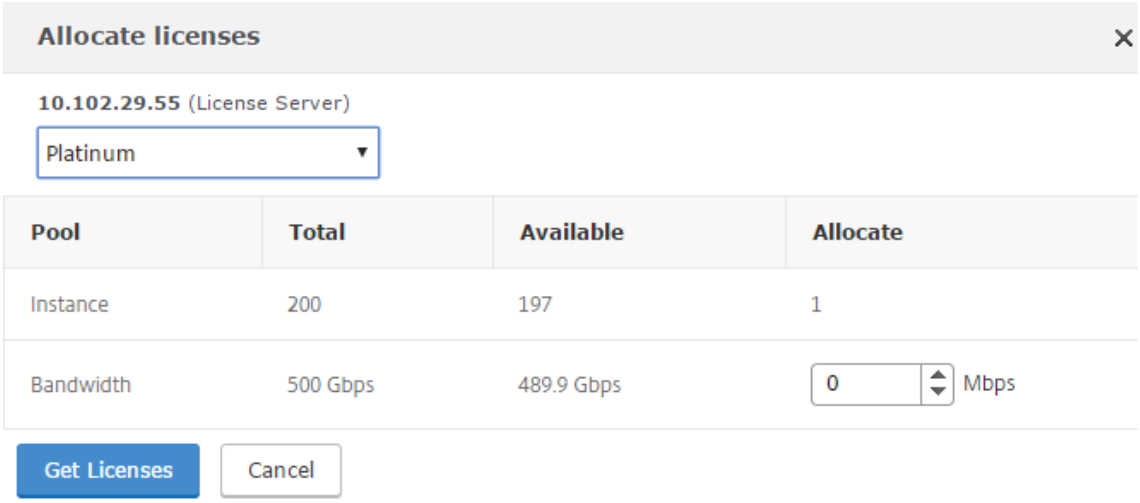
7. Puede cambiar o liberar la asignación de licencias seleccionando **Cambiar asignación** o **Lib-**

erar asignación.



8. Si hace clic en **Cambiar asignación**, una ventana emergente muestra las licencias disponibles en el servidor de licencias.

> **Nota**
>
> No es necesario reiniciar si cambia la asignación de ancho de banda, pero es necesario reiniciar en caliente si cambia la edición de la licencia.



9. Puede asignar ancho de banda o instancias a la instancia de Citrix ADC desde la lista desplegable **Asignar** . A continuación, haga clic en **Obtener licencias**.
10. Puede elegir la edición de licencia y el ancho de banda requerido en las listas desplegables de la ventana emergente.

> **Nota**
>
> La asignación de ancho de banda debe ser un múltiplo de la unidad mínima de ancho

Configuración de la capacidad agrupada de Citrix ADC en SDX-Z

Una instancia SDX-Z es una instancia de Citrix ADC SDX con capacidad agrupada habilitada. SDX-Z admite la agrupación de ancho de banda para las ediciones Platinum, Enterprise y Standard, y la agrupación de instancias. Tras aplicar la licencia de la plataforma SDX-Z, el servicio de administración ofrece opciones para extraer
y devolver las licencias al servidor de licencias y para asignar capacidad de ancho de banda a las instancias de Citrix ADC que se ejecutan en la plataforma SDX-Z.

> **Nota**
>
> Las instancias de NetScaler ADC VPX que se ejecutan en SDX-Z no pueden sacar licencias directamente desde o hacia el servidor de licencias. Esto lo puede hacer el servicio de gestión de SDX.

Puede instalar la licencia de la plataforma SDX-Z cargando el archivo de licencia desde el ordenador local o utilizando el número de serie del hardware de la instancia o el código de acceso a la licencia.

Si quita la licencia de la plataforma SDX-Z, la función de capacidad agrupada se deshabilita y todas las licencias se vuelven a registrar en el servidor de licencias.

> **Nota**
>
> Si reinicias la instancia, comprueba las licencias agrupadas necesarias para la capacidad configurada.

Capacidad de agrupamiento en Citrix ADC SDX

Grupo de instancias:

Un dispositivo SDX puede aprovisionar la misma cantidad de instancias que están disponibles en el grupo de instancias del dispositivo SDX.

Grupo de ancho debanda:

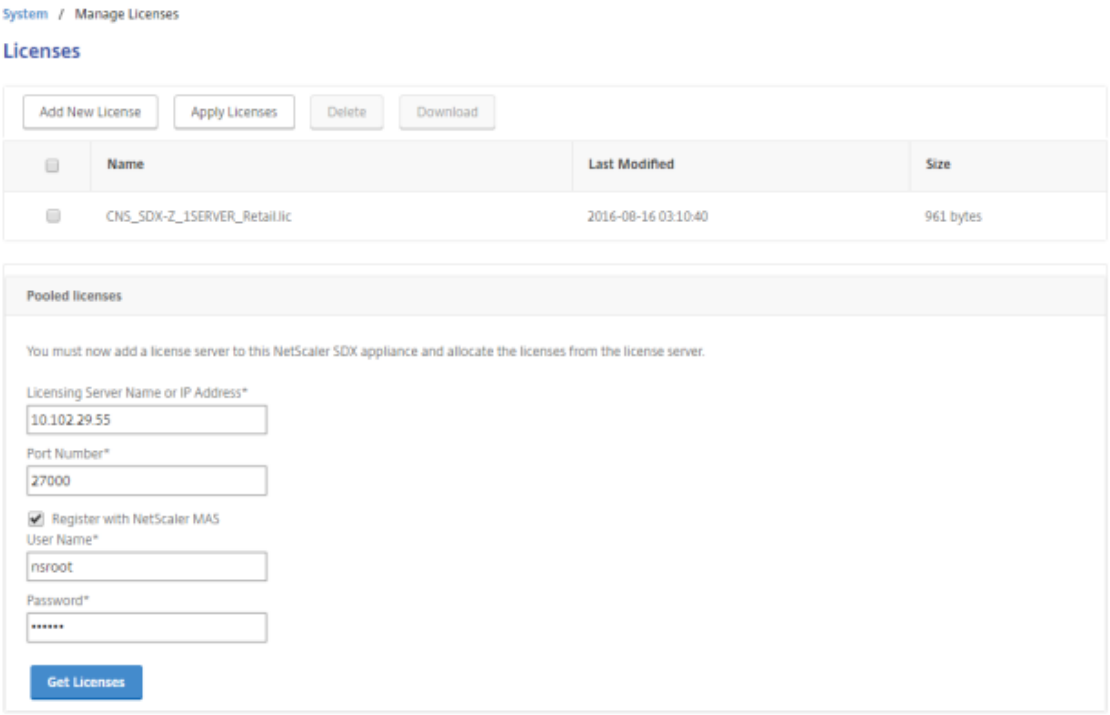
Durante el aprovisionamiento de instancias de NetScaler ADC, el ancho de banda se asigna a la instancia. Puede seleccionar la edición y el ancho de banda requerido para aprovisionar una instancia virtual de Citrix ADC. Management Service permite que el aprovisionamiento continúe solo si la instancia tiene suficiente ancho de banda para la edición solicitada. Se le notifica si el ancho de banda es insuficiente.

> **Nota**
>
> La modificación del ancho de banda no requiere reiniciar la instancia.

Asignación de licencias de grupo a una instancia SDX-Z de Citrix ADC

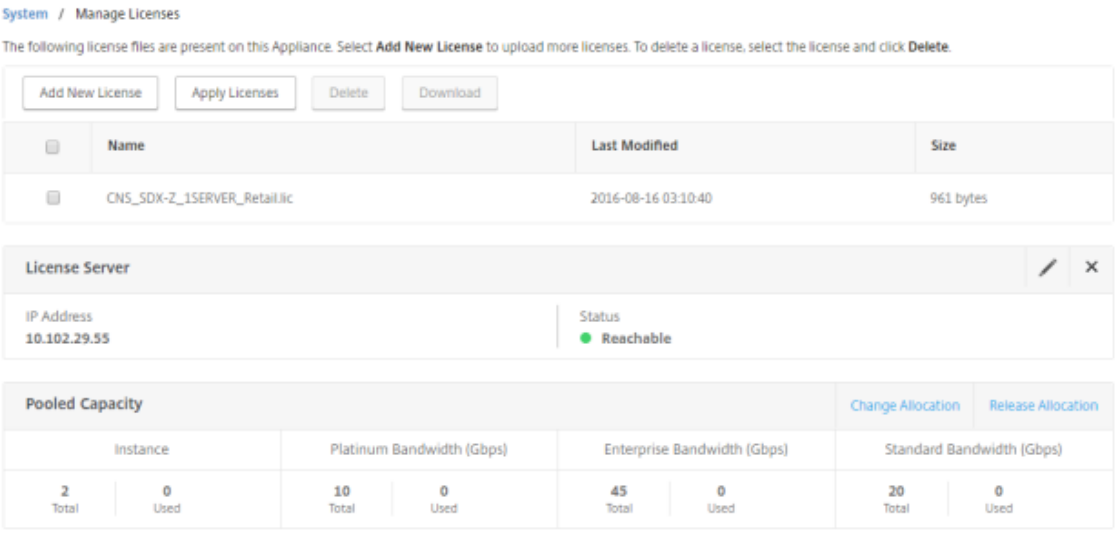
Para asignar sus licencias:

1. En un explorador web, escriba la dirección IP de la instancia SDX-Z de Citrix ADC (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la pestaña Configuración, vaya a **Sistema > Licencias** y vaya a **Capacidad** agrupada .

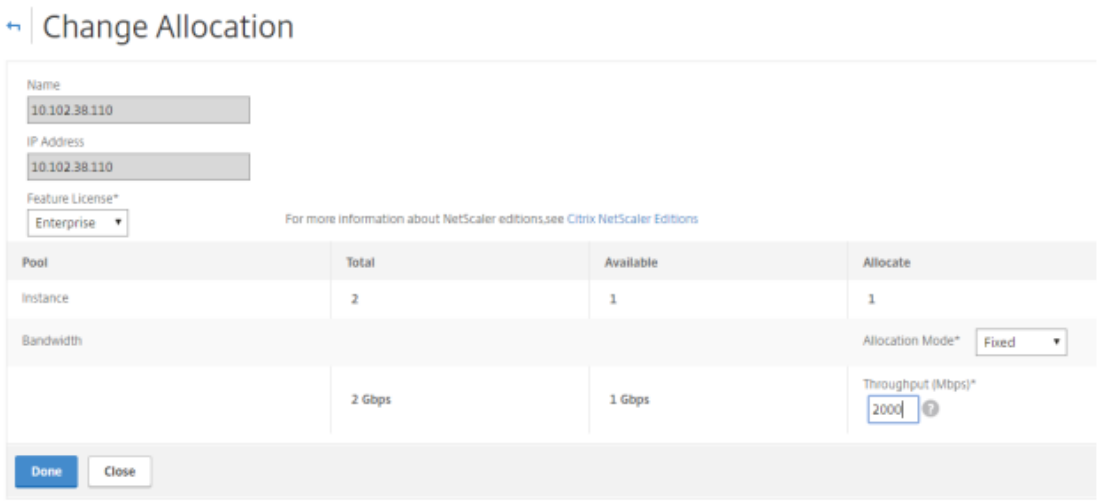


4. Introduzca los detalles del servidor de licencias en el campo **Nombre del servidor/dirección IP**.
5. Si quiere administrar las licencias del grupo de instancias a través de NetScaler ADM, active la casilla de verificación **Registrar con NetScaler ADM** e introduzca las credenciales de ADM.
6. Puede cambiar o liberar la asignación de licencias seleccionando **Cambiar asignación** o **Liberar asignación**.

> **Nota**
>
> El ADM almacena las licencias retiradas en un grupo independiente.



7. Para cambiar la asignación de licencias para una instancia VPX específica en la instancia SDX-Z, seleccione la instancia en la sección **Instancias** y haga clic en **Cambiar asignación.** En una ventana nueva se muestran las licencias disponibles.



8. Puedes cambiar la edición de ancho de banda de la instancia en la lista **desplegable Licencia** de funciones y el ancho de banda requerido en el campo **Rendimiento (mbps)** . Luego haga clic en **Done**.

> **Nota**
>
> La asignación de ancho de banda debe ser un múltiplo entero de la unidad de ancho de banda mínima del factor de forma correspondiente.

Configuración de la capacidad agrupada de Citrix ADC en una instancia de Citrix ADC CPX

Al aprovisionar la instancia Citrix ADC CPX, puede configurar la instancia Citrix ADC CPX para que utilice Citrix ADC Pooled Capacity. En el comando ***docker run*** , debe proporcionar los detalles del servidor de licencias Citrix ADC. La instancia CPX de Citrix ADC extrae las licencias del grupo de instancias.

> **Nota**
>
> De forma predeterminada, la instancia CPX de Citrix ADC extrae una licencia de instancia del grupo de instancias y el rendimiento se establece automáticamente en 1000 Mbps. No puedes modificar el ancho de banda de 1000 Mbps asignado a la instancia.

Puede descargar NetScaler ADC CPX desde Docker App Store. En el host Docker, para descargar NetScaler ADC CPX, ejecute el siguiente comando:

```
docker pull store/citrix/netscalercpx: <version>

<!--NeedCopy-->
```

Para configurar la capacidad agrupada de Citrix ADC mientras se aprovisiona la instancia CPX de Citrix ADC:

Al aprovisionar una instancia CPX de Citrix ADC, defina el servidor de licencias de Citrix como una variable de entorno en el comando ***docker run*** , como se muestra a continuación:

```
docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name
    <container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --
    cap-add=NET_ADMIN <REPOSITORY>:<TAG>

<!--NeedCopy-->
```

Donde:

- <LS_IPADDRESS>es la dirección IP del servidor de licencias de Citrix.
- <LS_PORT>es el puerto del servidor de licencias de Citrix. De forma predeterminada, el puerto es 27000.

Actualice una licencia perpetua en Citrix ADC MPX a Citrix ADC Pooled Capacity

January 30, 2024

El dispositivo NetScaler ADC MPX con licencia perpetua se puede actualizar a la licencia NetScaler ADC Pooled Capacity. La actualización a la licencia NetScaler ADC Pooled Capacity le permite asignar licencias del grupo de licencias a dispositivos NetScaler ADC bajo demanda. También puede configurar la licencia de capacidad agrupada de NetScaler ADC para instancias de ADC configuradas en modo de alta disponibilidad. Para configurar la licencia de capacidad agrupada de Citrix ADC para instancias de Citrix ADC MPX en modo de alta disponibilidad, consulte Actualizar la licencia perpetua en el par de alta disponibilidad de Citrix ADC MPX a Citrix ADC Pooled Capacity.

> **Importante**
>
> Para actualizar el dispositivo Citrix ADC MPX a la licencia Citrix ADC Pooled Capacity, debe cargar la licencia MPX-Z en el dispositivo.

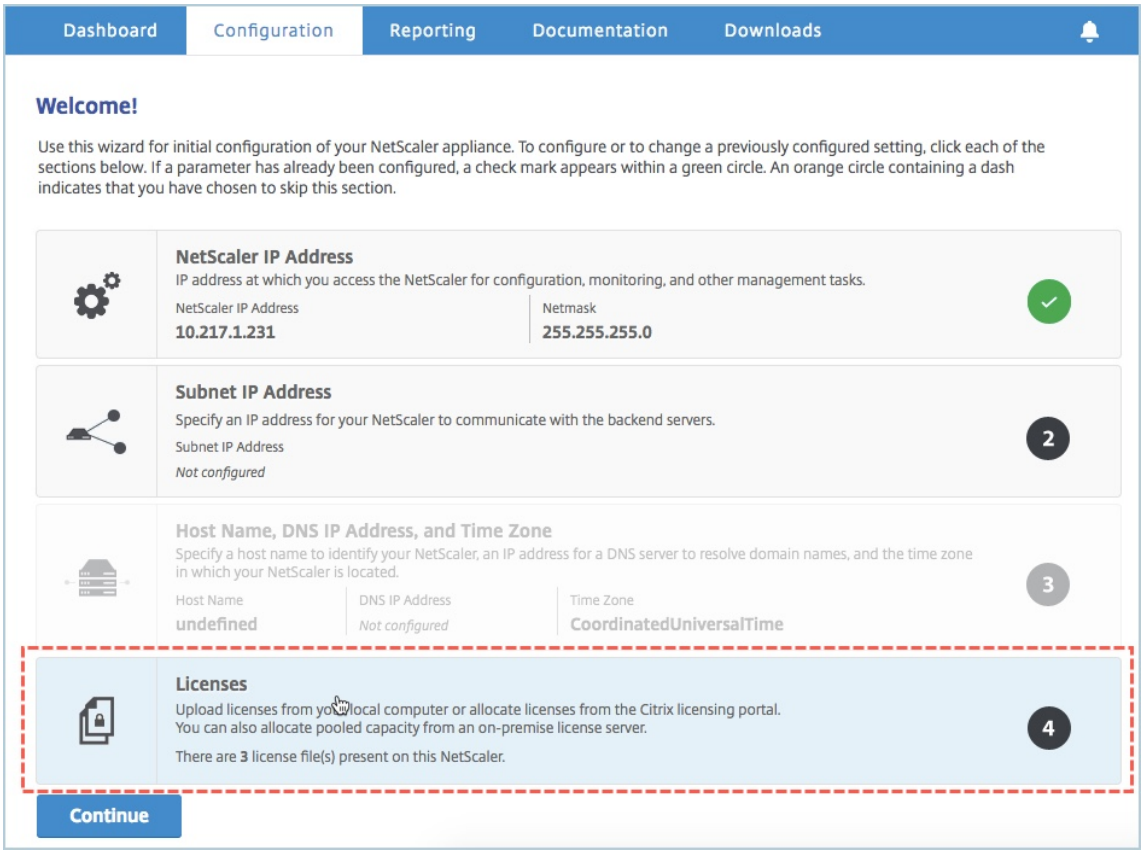
Para actualizar a Citrix ADC Pooled Capacity:

1. En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha Configuración, vaya a **Sistema** > **Licencias**.
5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en Agregar **nueva licencia** .
6. En la página **Licencias**, seleccione **Cargar archivos de licencia** y haga clic en **Examinar** para seleccionar la licencia de capacidad cero de su equipo local.
7. Después de cargar la licencia, haga clic en **Reiniciar** para reiniciar el dispositivo.

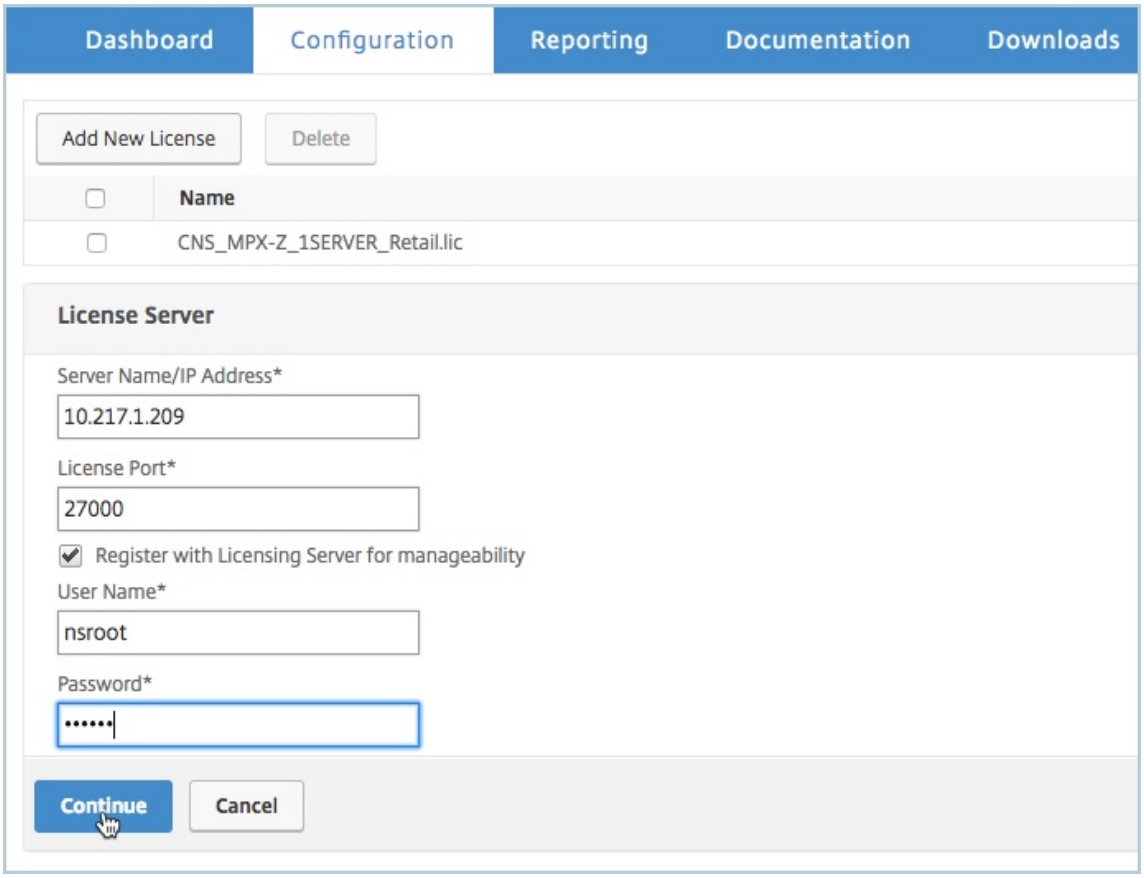
   Asegúrese de que no haya ninguna configuración guardada antes de reiniciar el dispositivo.

   > **Advertencia**
   >
   > Después de aplicar la licencia MPX-Z, las funciones, incluida la descarga de SSL en el dispositivo, quedan sin licencia. El dispositivo deja de procesar solicitudes HTTPS.
   >
   > Si la opción **Solo acceso seguro** está habilitada en el dispositivo antes de la actualización, no podrá conectarse al dispositivo a través de la GUI de NetScaler ADM mediante HTTPS.

8. En la página de **confirmación** , haz clic en **Sí** .
9. Una vez reiniciado el dispositivo, inicie sesión en el dispositivo.
10. En la página de bienvenida, haga clic en la sección **Licencias** .



11. En la sección **Servidor de licencias**, haga lo siguiente:



a) En el campo **Nombre del servidor/Dirección IP**, introduzca los detalles del servidor de licencias.

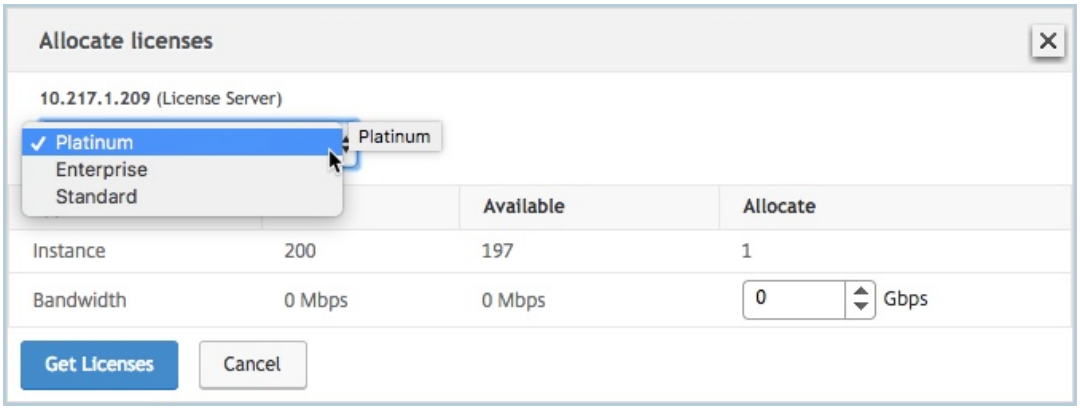
b) En el campo **Puerto** de licencia , introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Si quiere administrar las licencias del grupo de instancias a través de Citrix ADM, seleccione la casilla **Registrarse en el servidor de licencias para facilitar la administración** e introduzca las credenciales de ADM.

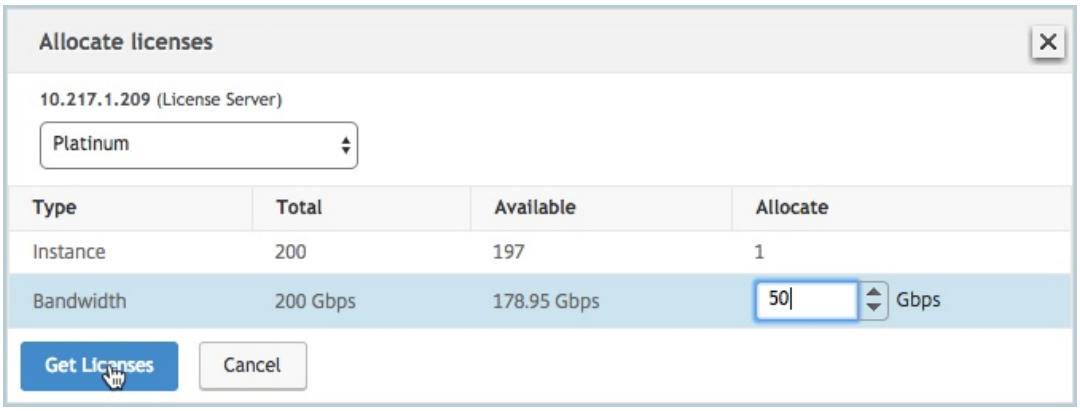
d) Haga clic en **Continuar**.

12. En la ventana Asignar licencias, haga lo siguiente:

a) Seleccione la edición de licencia en la lista desplegable.



b) Asigne el ancho de banda al dispositivo NetScaler ADC desde el menú **Asignar** y haga clic en **Obtener licencias**.



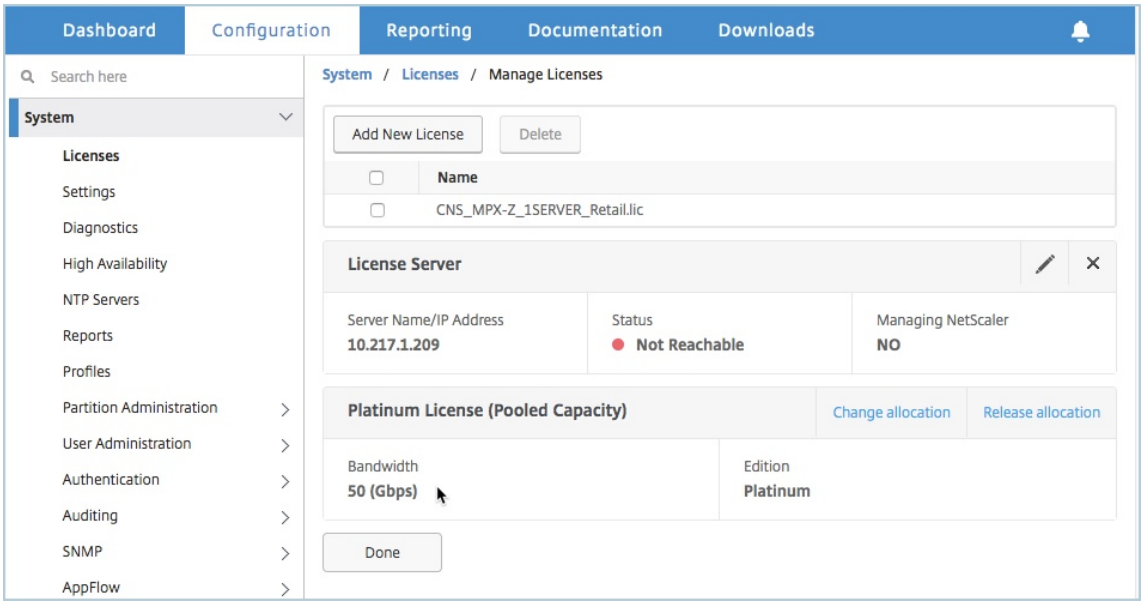
c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.

13. Una vez que se reinicie el dispositivo NetScaler ADC MPX, inicie sesión en el dispositivo NetScaler ADC MPX. En la página de **bienvenida**, haga clic en **Continuar**.

    La página **Licencias** muestra todas las funciones con licencia.

14. Vaya a **Sistema > Licencias** y haga clic en **Administrar licencias**.

    En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y el ancho de banda asignado.



Actualice la licencia perpetua del par de alta disponibilidad Citrix ADC MPX a Citrix ADC Pooled Capacity

Para NetScaler ADC MPX Appliances configurados en modo de alta disponibilidad, debe configurar NetScaler ADC Pooled Capacity en las instancias primarias y secundarias de NetScaler ADC en el par HA. Debe asignar licencias de la misma capacidad a las instancias primarias y secundarias de NetScaler ADC en el par HA. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia del par HA, debe asignar una capacidad de 2 Gbps del grupo común para poder asignar una capacidad de 1 Gbps a cada una de las instancias de NetScaler ADC principales y secundarias del par HA.

> **Importante**
>
> Para actualizar el dispositivo NetScaler ADC MPX para usar la licencia NetScaler ADC Pooled Capacity, debe cargar el MPX-Z al dispositivo.

Requisitos previos

Asegúrese de cargar la licencia MPX-Z en las instancias principales y secundarias del par de HA.

Para cargar la licencia MPX-Z a las instancias MPX de NetScaler ADC en el par HA:

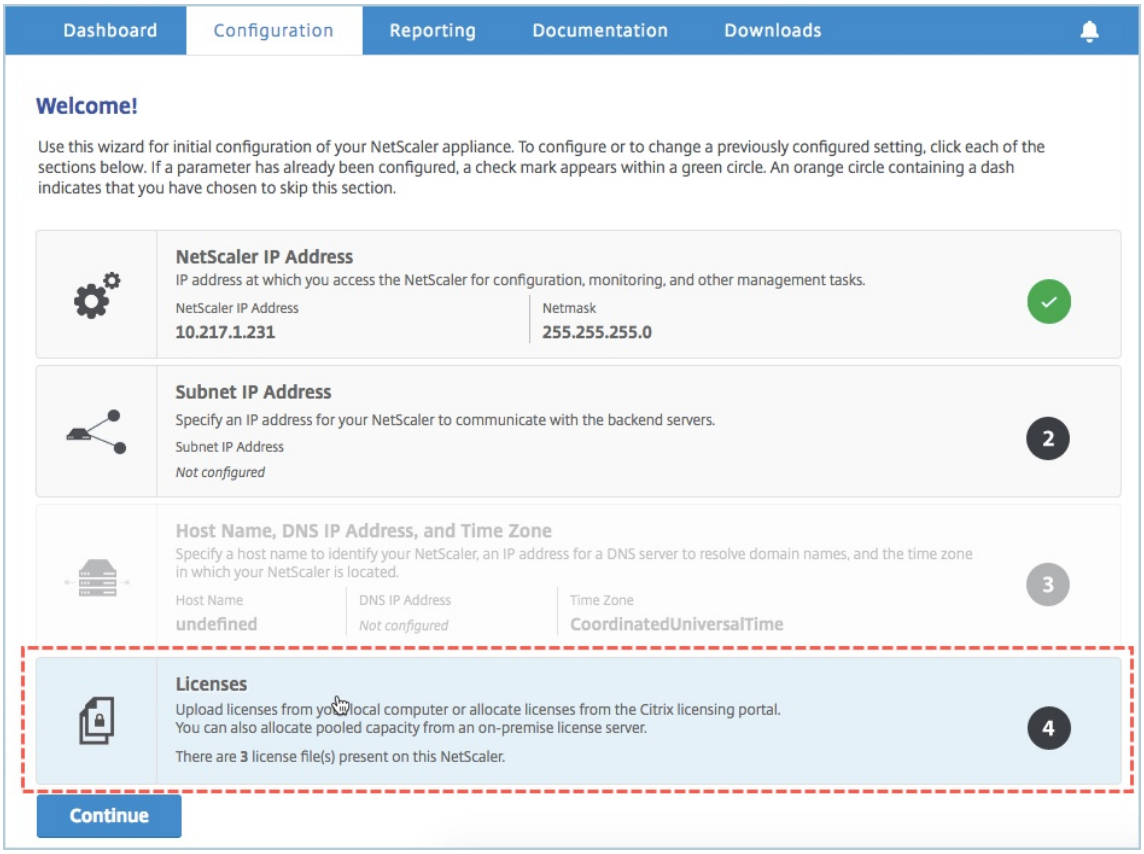
1. En un explorador web, escriba la dirección IP del dispositivo. Por ejemplo: http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha **Configuración**, vaya a **Sistema > Licencias**.

5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en **Agregar nueva licencia** .
6. En la página **Licencias**, seleccione **Cargar archivos de licencia** y haga clic en **Examinar** para seleccionar la licencia de capacidad cero de su equipo local.

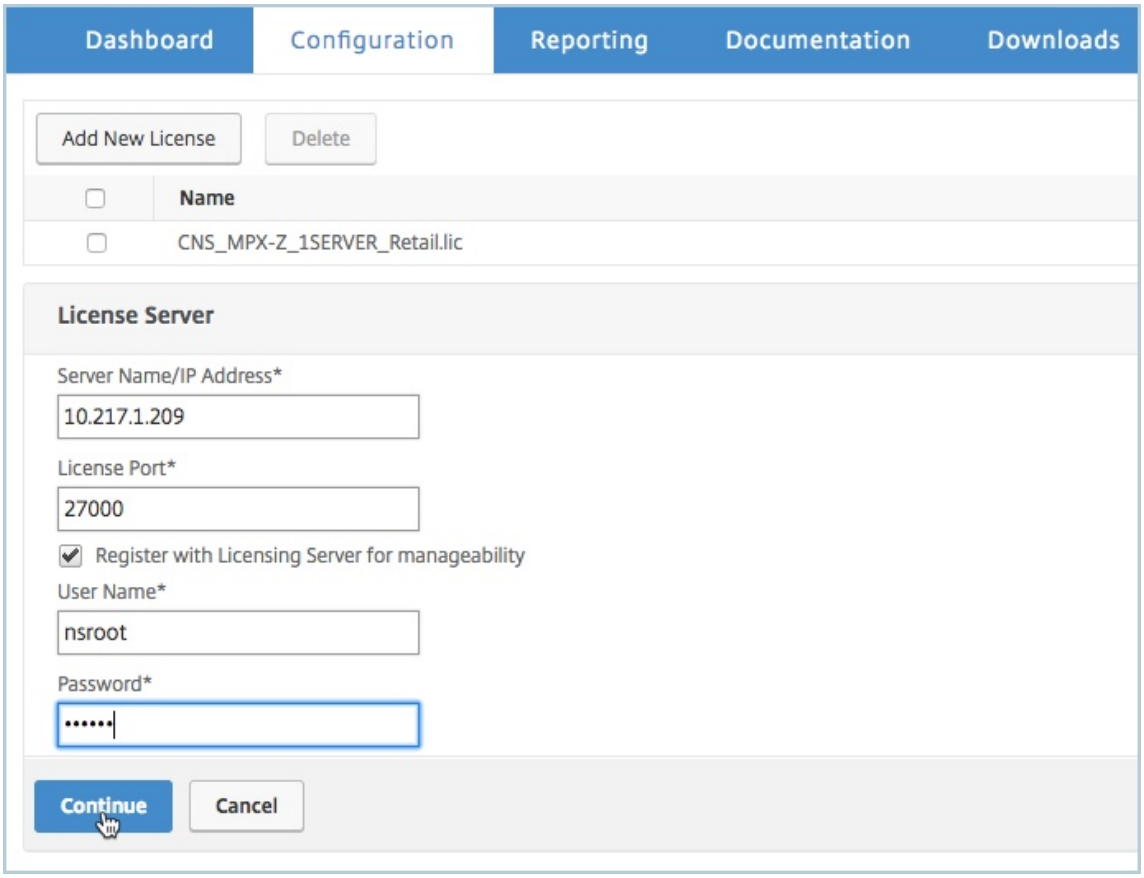
   Una vez cargada la licencia, se le pedirá que reinicie el dispositivo.
7. Haga clic en **Reiniciar** para reiniciar el dispositivo.
8. En la página de **confirmación** , haz clic en **Sí** .

Para actualizar una configuración de alta disponibilidad existente a la capacidad agrupada de NetScaler ADC:

1. Inicie sesión en la instancia MPX de NetScaler ADC secundaria. En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida** , haga clic en la sección **Licencias** .



4. En la sección **Servidor de licencias**, haga lo siguiente:



a) En el campo **Nombre del servidor/Dirección IP**, introduzca los detalles del servidor de licencias.

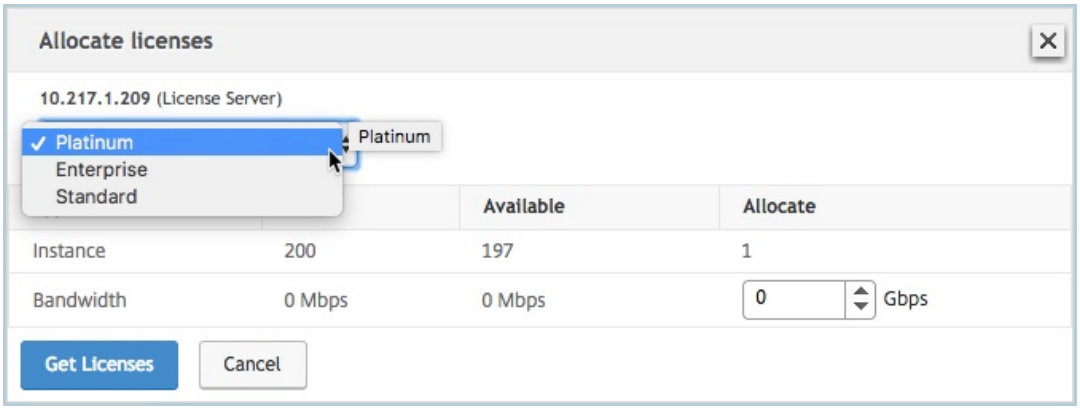
b) En el campo **Puerto** de licencia , introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Si quiere administrar las licencias del grupo de instancias a través de Citrix ADM, seleccione la casilla **Registrarse en el servidor de licencias para facilitar la administración** e introduzca las credenciales de ADM.

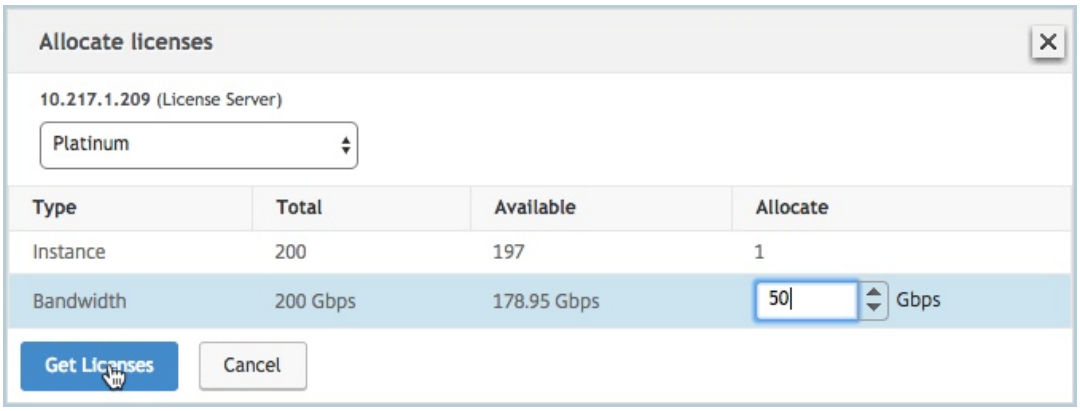
d) Haga clic en **Continuar**.

5. En la ventana **Asignar licencias**, haga lo siguiente:

a) Seleccione la edición de licencia en la lista desplegable.



b) Asigne el ancho de banda al dispositivo NetScaler ADC desde el menú **Asignar** y haga clic en **Obtener licencias**.



c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.

Después de que se reinicie el dispositivo NetScaler ADC MPX secundario, se convierte en el dispositivo NetScaler ADC MPX principal en el par HA.

6. Inicie sesión en el dispositivo Citrix ADC MPX principal existente y reinicie el dispositivo. Lleve a cabo lo siguiente:

a) En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.

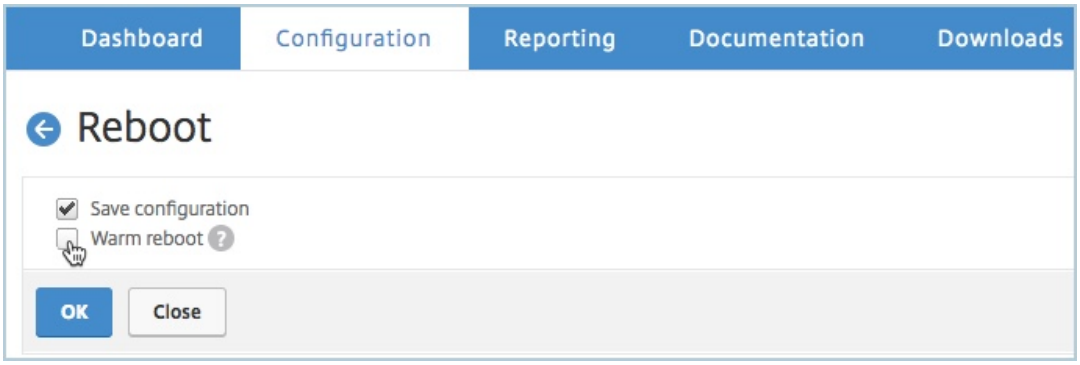
b) En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.

c) En la página de **bienvenida**, haga clic en **Continuar**.

d) En la ficha **Configuración**, haga clic en **Sistema**.

e) En la página **Sistema**, haga clic en **Reiniciar**.

f) En la página **Reiniciar**, seleccione **Reiniciar en caliente** y haga clic en **Aceptar**.



Una vez que se reinicie el dispositivo NetScaler ADC MPX principal, se convierte en el dispositivo NetScaler ADC MPX secundario en el par HA. Si es necesario, puede cambiar la instancia principal y secundaria del par HA a la configuración original del par HA mediante el siguiente comando en cualquier instancia del par HA:

```
> force ha failover
<!--NeedCopy-->
```

Actualizar una licencia perpetua en un NetScaler ADC SDX a la capacidad agrupada de NetScaler ADC

January 30, 2024

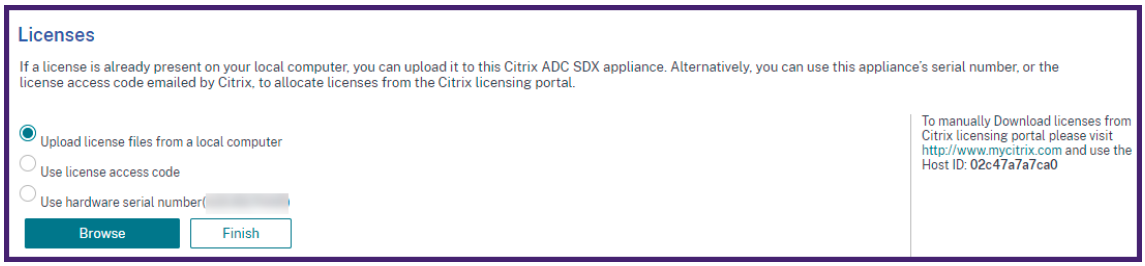
Un dispositivo NetScaler ADC SDX con licencia perpetua se puede actualizar a la licencia NetScaler ADC Pooled Capacity. La actualización a la licencia Citrix ADC Pooled Capacity le permite asignar licencias del grupo de licencias a los dispositivos Citrix ADC bajo demanda. También puede configurar la licencia de capacidad agrupada de NetScaler ADC para instancias de ADC configuradas en modo de alta disponibilidad.

> **Importante**
>
> Para actualizar el dispositivo SDX a la licencia Citrix ADC Pooled Capacity, debe cargar la licencia SDX-Z en el dispositivo.

Para actualizar a la capacidad agrupada de NetScaler ADC:

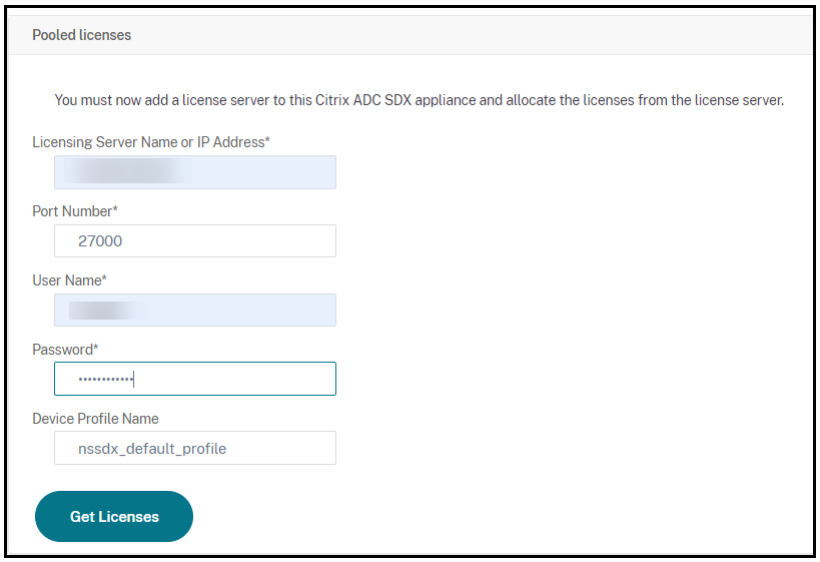
1. En un navegador web, escriba la dirección IP del dispositivo SDX ADC, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.

4. Cargue la licencia de capacidad cero. En la ficha Configuración, vaya a **Sistema** > **Licencias**.
5. Vaya a **Sistema** > **Licencias**.
6. En la página **Licencias** , haga clic en **Administrar licencias** y, a continuación, en **Agregar nueva licencia** .
7. En la página **Licencias** , seleccione **Cargar archivos de licencia** y haga clic **en**Examinar para seleccionar la licencia de capacidad cero de su máquina local. A continuación, haga clic en **Finalizar**.



Una vez que la licencia de capacidad cero se aplica correctamente, la sección **Licencias agrupadas** aparece en la página **Licencias**.

8. En la sección **Licencias agrupadas**, haga lo siguiente:



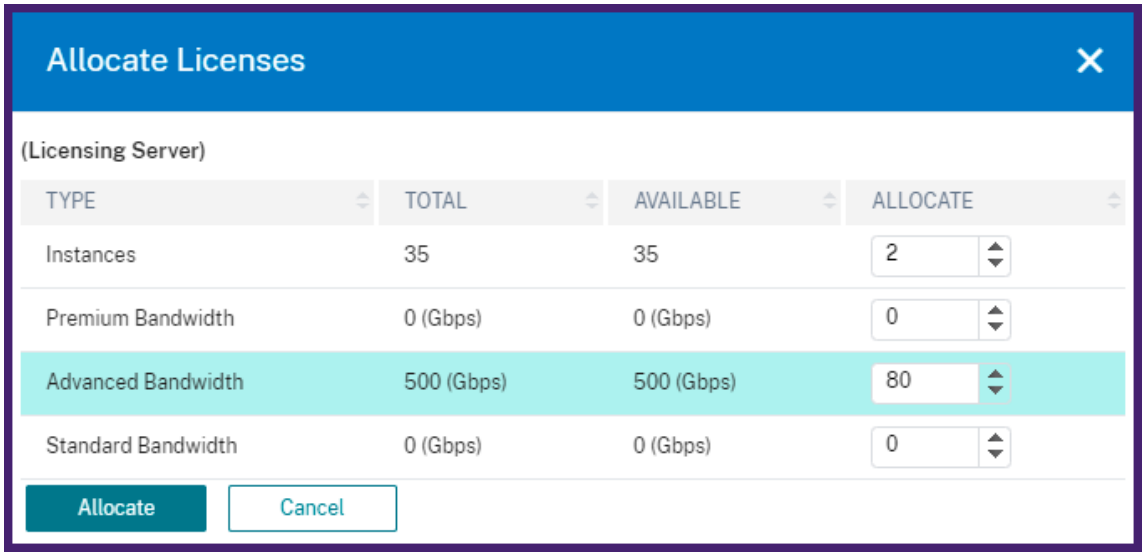
a) En el campo **Nombre del servidor de licencias o Dirección IP**, introduzca los detalles del servidor de licencias.

b) En el campo **Número de puerto**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

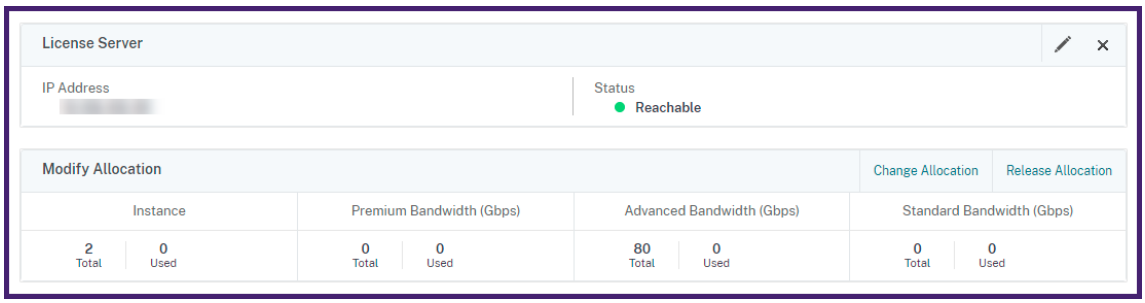
c) Si quiere administrar las licencias del grupo de instancias a través de NetScaler ADM, active la casilla de verificación **Registrar con NetScaler ADM** e introduzca las credenciales de ADM.

d) Haga clic en **Obtener licencias**.

9. En la ventana **Asignar licencias**, especifique las instancias y el ancho de banda necesarios y haga clic en **Asignar**.



En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y las instancias asignadas y el ancho de banda desde el grupo.



Capacidad agrupada de NetScaler ADC en instancias de NetScaler ADC en modo de clúster

January 30, 2024

Puede configurar la capacidad agrupada de NetScaler ADC en las instancias de NetScaler ADC configuradas como un clúster. Los siguientes son los requisitos previos para configurar la capacidad agrupada en las instancias de Citrix ADC en modo clúster:

- Las instancias deben ejecutarse individualmente en un modo de licencia de capacidad agrupada para formar el clúster.

- Todas las instancias deben ejecutarse con el mismo ancho de banda.
- Todas las instancias deben comprobar la capacidad agrupada del mismo Citrix Application Delivery Management (ADM).
- Las nuevas instancias no se pueden agregar a un clúster de NetScaler ADC existente a menos que su capacidad y las configuraciones de NetScaler ADM sean las mismas que las de las instancias existentes en el clúster.

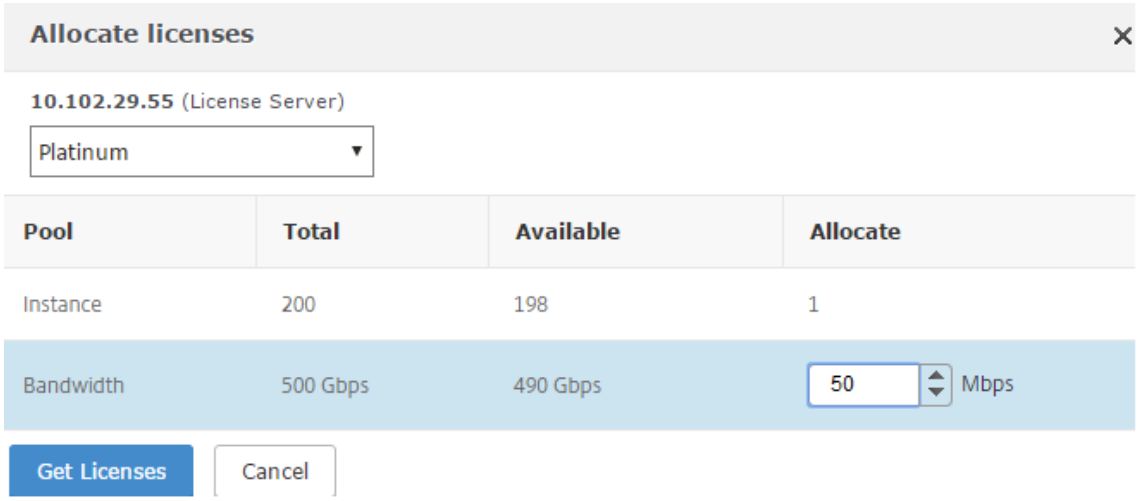
Cualquier retirada de capacidad del clúster de Citrix ADC asignará la misma capacidad a todos los nodos del clúster y al ancho de banda de salida = ancho de banda proporcionado * número de nodos.

Por ejemplo, si retira 50 Mbps de ancho de banda del clúster Citrix ADC y el clúster incluye 12 instancias, cada instancia recibe automáticamente 50 Mbps y se retiran 600 mbps del grupo.

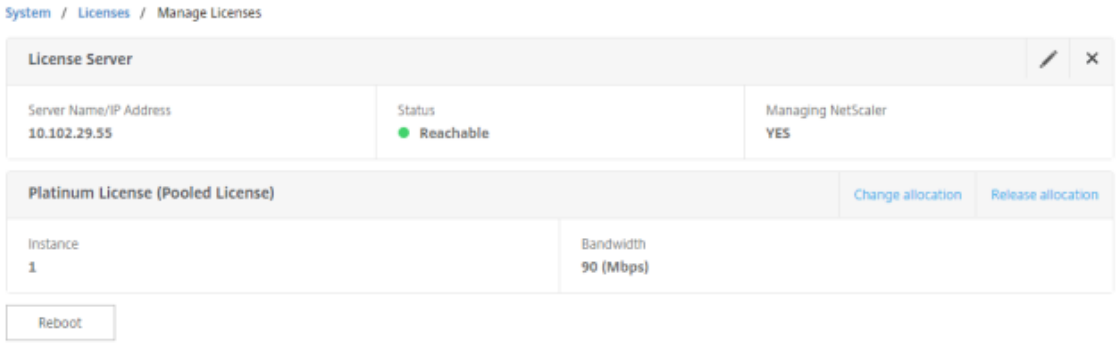
> **Nota**
>
> Si una o más instancias del clúster dejan de responder, el clúster sigue funcionando con la capacidad de las instancias restantes.

Para asignar la capacidad agrupada de Citrix ADC a las instancias de Citrix ADC en modo clúster:

1. En un navegador web, escriba la dirección IP de la dirección **IP del clúster** (CLIP) (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema > Licencias > Administrar licencias**, haga clic en **Agregar nueva licencia** y seleccione **Usar licencias agrupadas**.
4. Introduzca el nombre o la dirección del servidor de licencias en el campo **Nombre del servidor/Dirección IP**.
5. Si quiere administrar las licencias del grupo de instancias a través de Citrix ADM, seleccione la casilla **Registrarse en Citrix ADM para facilitar la administración** e introduzca las credenciales de ADM.
6. Seleccione la edición de licencia y el ancho de banda requerido y haga clic en **Obtener licencias**.

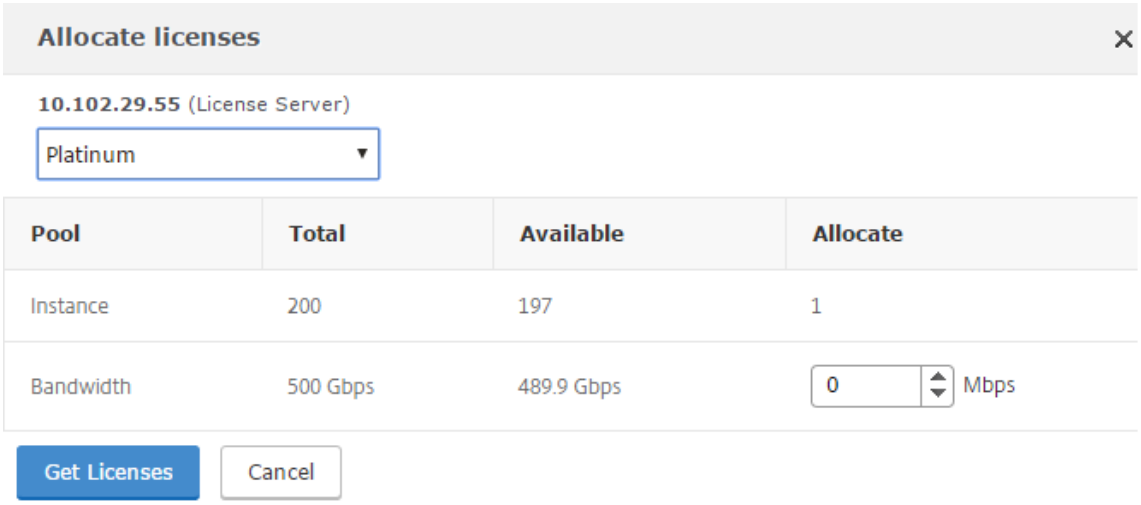


7. Puede cambiar o liberar la asignación de licencias seleccionando **Cambiar asignación** o **Liberar asignación**.



8. Si hace clic en **Cambiar asignación**, una ventana emergente muestra las licencias disponibles en el servidor de licencias.

> **Nota**
>
> La asignación de ancho de banda debe ser un múltiplo integral de la unidad de ancho de banda mínima del factor de forma correspondiente.



9. Puede asignar ancho de banda o instancias a la instancia de Citrix ADC desde la lista desplegable **Asignar** . A continuación, haga clic en **Obtener licencias**.
10. Puede elegir la edición de licencia y el ancho de banda requerido en las listas desplegables de la ventana emergente.

> **Nota**
>
> No es necesario reiniciar si cambia la asignación de ancho de banda, pero es necesario reiniciar en caliente si cambia la edición de la licencia.

Supervisión de estado

January 30, 2024

El servidor de licencias supervisa continuamente el estado de la instancia habilitada para la capacidad agrupada de Citrix ADC. Las instancias se comunican mediante mensajes periódicos con el servidor de licencias. Si no se reciben algunos mensajes consecutivos, el servidor de licencias informa de que se ha perdido la conectividad.

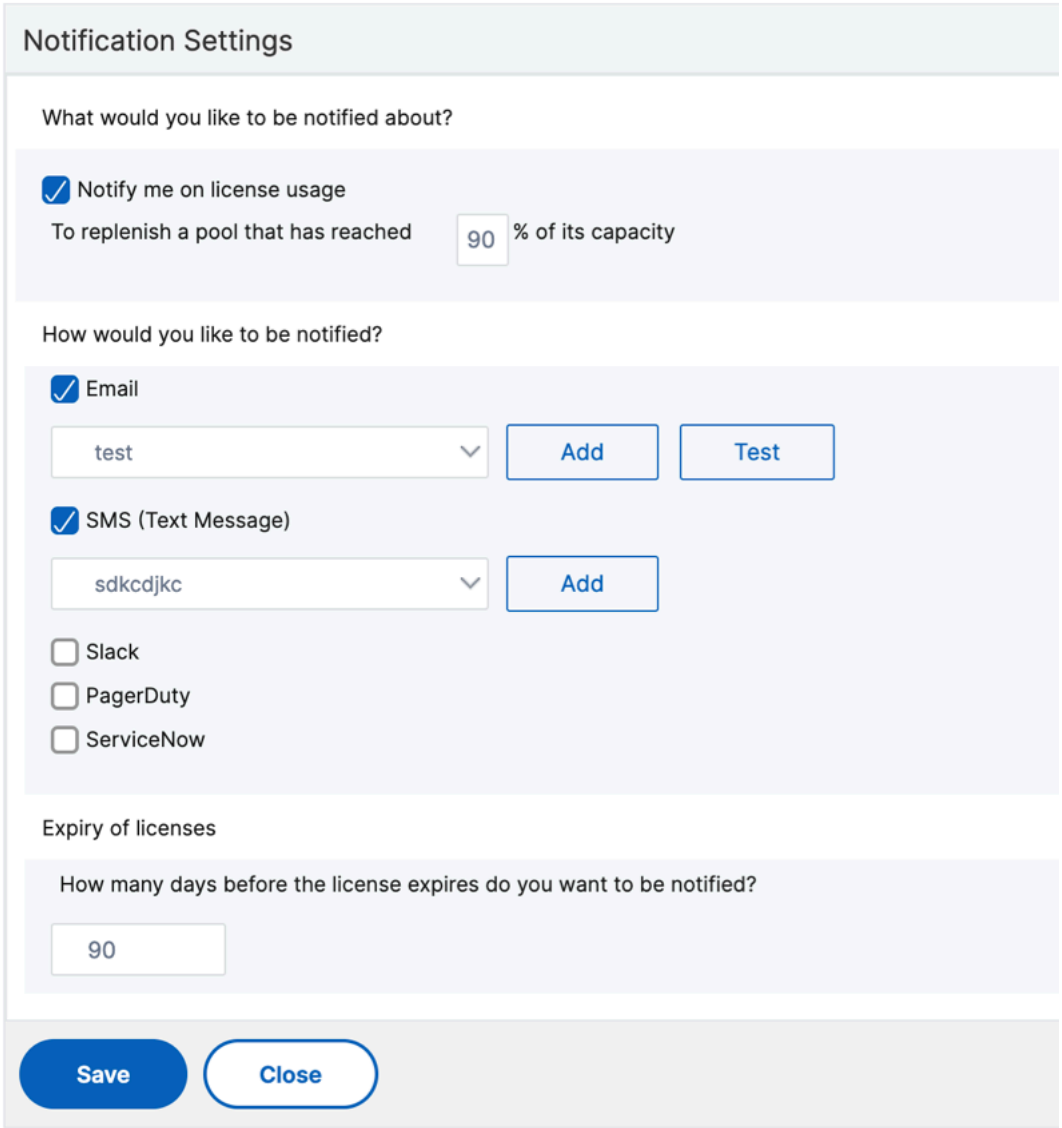
Puede crear notificaciones personalizadas para complementar las alarmas predeterminadas.

Período de gracia

Cuando una instancia habilitada para la capacidad agrupada de Citrix ADC se encuentra en buen estado y el servidor de licencias deja de responder, la instancia sigue funcionando con la capacidad actual durante 30 días. Si la conectividad con el servidor de licencias no se restaura transcurridos 30 días, la instancia pierde su capacidad y deja de procesar el tráfico.

Notificaciones y alarmas

Las notificaciones se pueden habilitar desde Citrix Application Delivery Management (ADM) para cualquier acción realizada en la instancia. Además de la configuración de notificación personalizada, algunas alarmas están configuradas de forma predeterminada. Por ejemplo: para configurar una alarma para reponer un grupo que ha agotado un determinado porcentaje de su capacidad, vaya a **Infraestructura** > **Licencia** > Configuración > **Configuración** de **notificaciones** y haga clic en el botón de edición.



Comportamientos esperados cuando surgen problemas

January 30, 2024

Los siguientes son los comportamientos esperados de los servidores de licencias y las instancias de Citrix ADC cuando experimentan los problemas descritos:

El servidor de licencias deja de responder

> **Advertencia**
>
> El servidor de licencias no responde. Citrix ADC seguirá funcionando con la capacidad actual durante 30 días. Transcurridos 30 días, si no se restaura la conectividad con el servidor de licencias, el Citrix ADC perderá su capacidad actual y dejará de procesar el tráfico.

Si el servidor de licencias deja de responder, la instancia de NetScaler ADC entra en el período de gracia hasta que se restaure la conectividad.

La instancia habilitada para capacidad agrupada de Citrix ADC deja de responder

Si la instancia habilitada para la capacidad agrupada de NetScaler ADC deja de responder y el servidor de licencias está en buen estado, el servidor de licencias comprueba todas las licencias de la instancia de NetScaler ADC después de 10 minutos. Cuando la instancia se reinicia, envía una solicitud para retirar todas las licencias del servidor de licencias.

Tanto el servidor de licencias como la instancia habilitada para la capacidad agrupada de NetScaler ADC dejan de responder

Si tanto el servidor de licencias como la instancia habilitada para la capacidad agrupada de Citrix ADC se reinician y restablecen la conexión, el servidor de licencias registra todas sus licencias después de 10 minutos y las instancias habilitadas para la capacidad agrupada de Citrix ADC retiran automáticamente las licencias una vez finalizado el reinicio.

La instancia habilitada para la capacidad agrupada de NetScaler ADC se cierra correctamente

Durante un cierre agraciado, puede optar por registrar las licencias o conservar las licencias asignadas antes del cierre agraciado. Si decide registrar las licencias, la instancia habilitada para la capacidad agrupada de Citrix ADC no tendrá licencia una vez reiniciada. Si decide conservar las licencias, se

registrarán en el servidor de licencias cuando se cierre la instancia. Una vez reiniciado la instancia, restablece la conexión con el servidor de licencias y retira las licencias tal como se especifica en la configuración guardada.

Si el sistema se reinicia y la extracción falla debido a que no hay capacidad disponible en el grupo, el Citrix ADC comprobará el inventario de las licencias del grupo de Citrix Application Delivery Management (ADM) y retirará cualquier capacidad disponible. Se activa una alarma SNMP para notificar esta condición al usuario si Citrix ADC no se ejecuta a plena capacidad según la configuración. Si no hay capacidad disponible en el grupo de ancho de banda, la instancia con capacidad de grupo habilitada dejará de tener licencia.

La red pierde conectividad

> **Mensaje de error (syslog)**
>
> El servidor de licencias no responde.

Si el servidor de licencias y las instancias habilitadas para la capacidad agrupada de NetScaler ADC están en estado correcto, pero la conectividad de red se pierde, las instancias seguirán funcionando con su capacidad actual durante 30 días. Transcurridos 30 días, si no se restablece la conectividad con el servidor de licencias, las instancias pierden su capacidad y dejan de procesar el tráfico, y el servidor de licencias registra todas sus licencias. Después de que el servidor de licencias restablece la conectividad con las instancias de NetScaler ADC, las instancias vuelven a desproteger las licencias.

Configurar comprobaciones de caducidad para licencias de capacidad agrupadas

January 30, 2024

Ahora puede configurar el umbral de caducidad de las licencias de capacidad agrupada de NetScaler ADC. Al establecer los umbrales, Citrix Application Delivery Management (ADM) envía notificaciones por correo electrónico o SMS cuando una licencia está a punto de caducar. Una captura SNMP y una notificación también se envían cuando la licencia ha expirado en NetScaler ADM.

Se genera un evento cuando se envía una notificación de caducidad de licencia y este evento se puede ver en NetScaler ADM.

Para configurar comprobaciones de caducidad de licencias:

1. Vaya a **Redes** > **Licencias** .

2. En la página de **configuración de licencias**, en la sección**Información sobre la caducidad de la licencia**, encontrará los detalles de las licencias que van a caducar:

    - **Función**: Tipo de licencia que va a caducar.
    - **Recuento**: número de servidores o instancias virtuales que se verán afectados.
    - **Días para caducar**: Número de días antes de la expiración de la licencia.

3. En la sección **Configuración de notificaciones** , haga clic en el icono **Editar** y especifique el umbral de alerta. Puede establecer un porcentaje de la capacidad de licencias agrupadas que se utilizará para notificar a los administradores.
4. Seleccione el tipo de notificación que quiere enviar marcando la casilla correspondiente. Los tipos de notificación son los siguientes:

    a) **Perfil de correo electrónico**: especifique un servidor de correo y los detalles del perfil. Se activa un correo electrónico cuando las licencias están a punto de caducar.

    b) **Perfil SMS**: especifique un servidor del servicio de mensajes cortos (SMS) y los detalles del perfil. Se activa un mensaje SMS cuando las licencias están a punto de caducar.

5. A continuación, especifique cuándo quiere enviar la notificación en términos de número de días antes de la caducidad de la licencia.
6. Haga clic en **Guardar**.

> **Nota**
>
> Cuando agrega nuevas licencias al grupo, las instancias NetScaler ADC utilizan las nuevas licencias al vencimiento de sus licencias existentes.

Licencias de registro y salida de NetScaler ADC VPX

January 30, 2024

Puede asignar licencias VPX a instancias de NetScaler ADC VPX a petición desde NetScaler Application Delivery Management (ADM). NetScaler ADM almacena y administra las licencias, que cuenta con un marco de licencias que proporciona un aprovisionamiento de licencias escalable y automatizado. Una instancia de NetScaler ADC VPX puede retirar la licencia del NetScaler ADM cuando se aprovisiona una instancia de NetScaler ADC VPX, o volver a registrar su licencia en NetScaler ADM cuando se quita o destruye una instancia.

Requisitos previos

Asegúrese de que se cumplen los siguientes requisitos previos:

- Está mediante una imagen de NetScaler ADC VPX que ejecuta la versión 12.0 del software.
  Por ejemplo: NSVPX-ESX-12.0-xx.xx_nc.zip
- Ha instalado Citrix ADM con la versión 12.0.
  Por ejemplo: MAS-ESX-12.0-xx.xx.zip

> **Nota**
>
> Para administrar las licencias VPX existentes mediante Citrix ADM, debe volver a alojar las licencias en Citrix ADM.

Instalación de licencias en Citrix ADM

> **Nota**
>
> Antes de instalar las licencias, reinicie el dispositivo virtual Citrix ADM si ha cambiado la edición del software o el ancho de banda.

Para instalar archivos de licencia en NetScaler ADM:

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Licencias** .
4. En la sección **Archivos de licencias**, seleccione una de las siguientes opciones:

   - **Cargar archivos de licencias desde un equipo**local : si ya hay un archivo de licencias en su equipo local, puede cargarlo en Citrix ADM.
     Para agregar archivos de licencia, haga clic **en**Examinar y seleccione el archivo de licencia (.lic) que desee agregar. Luego haga clic en **Finalizar**.
   - **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso de licencia (LAC) para las licencias que compra.
     Para agregar archivos de licencia, introduzca el LAC en el cuadro de texto y, a continuación, haga clic en **Obtener licencias** .

   > **Nota**
   >
   > Asegúrese de que está conectado a Internet antes de usar el código LAC para instalar las licencias.

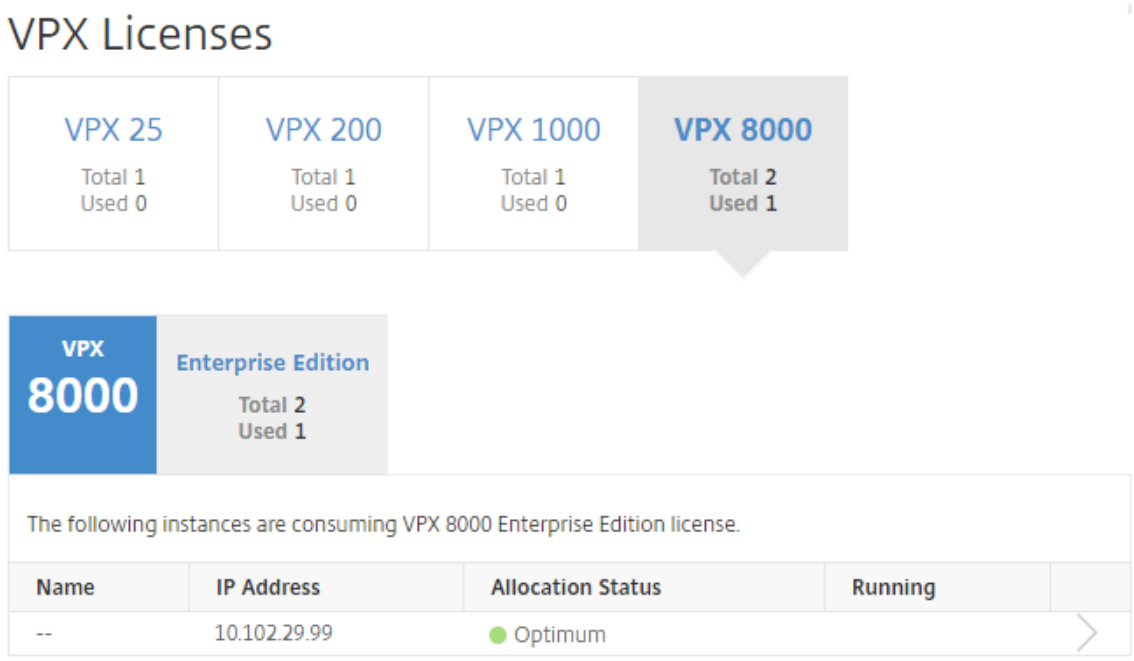
   En cualquier momento, puede agregar más licencias a NetScaler ADM desde la Configuración de licencias.

Verificación

Puede ver las licencias disponibles y asignadas en la GUI de Citrix ADM.

Para mostrar las licencias:

1. En un explorador web, escriba la dirección IP de NetScaler ADM (por ejemplo,http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha Configuración, vaya a **Redes**> **Licencias > Licencias > LicenciasVPX.**

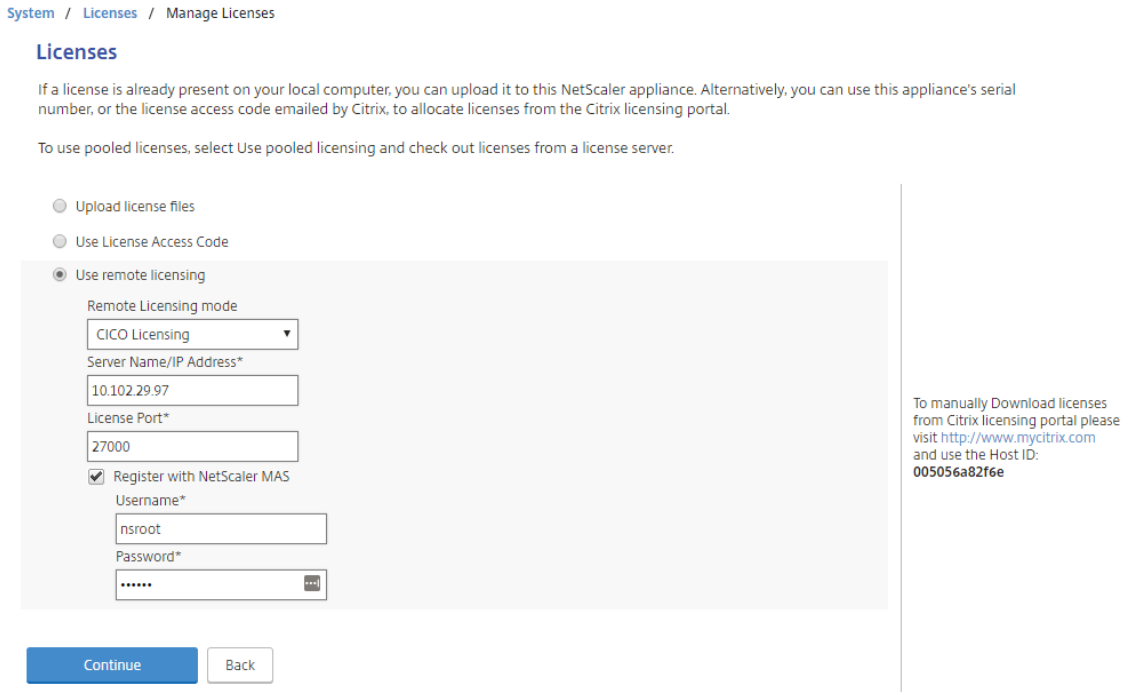


4. Puede ver las licencias asignadas en la tabla de la sección de licencias disponibles.

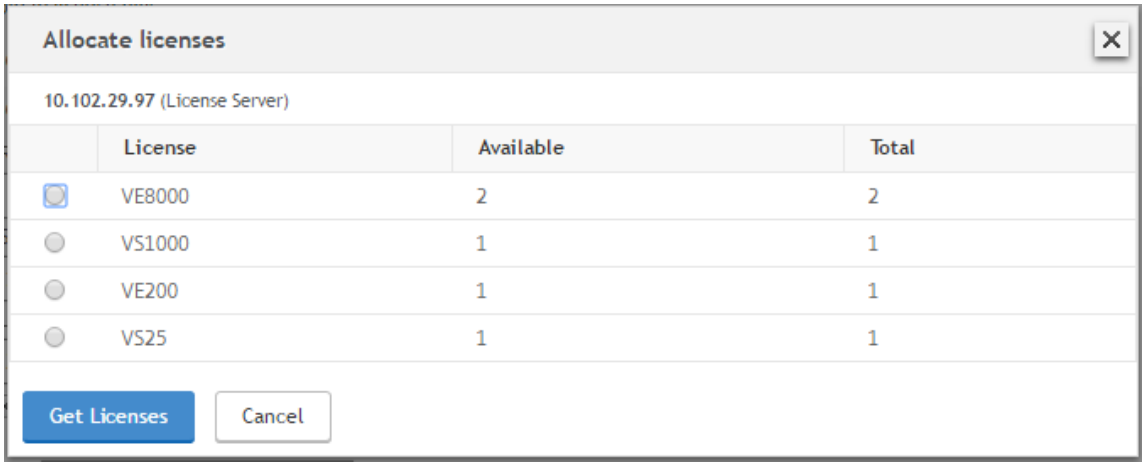
Asignación de licencias VPX a una instancia de Citrix ADC VPX mediante la GUI de Citrix ADC

1. En un explorador web, escriba la dirección IP de la instancia de NetScaler ADC (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la pestaña Configuración, vaya a **Sistema** > **Licencias** > **Administrar licencias** , haga clic en **Agregar nueva licencia** y seleccione **Usar licencias remotas** .
4. Introduzca los detalles del servidor de licencias en el **campo**Nombre del servidor**/Dirección IP** .

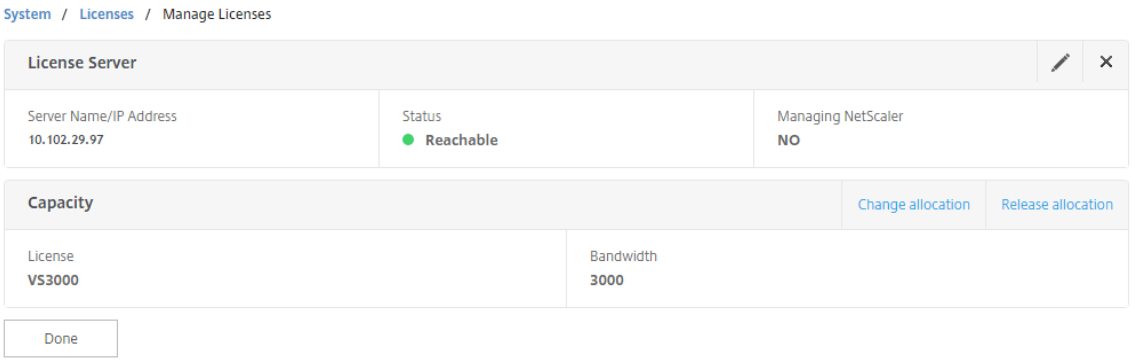
5. Si quiere administrar las licencias VPX de la instancia a través de Citrix ADM, seleccione la casilla **Registrar con Citrix ADM** e introduzca las credenciales de Citrix ADM.



6. Seleccione la edición de licencia con el ancho de banda requerido, haga clic en **Obtener licencias**.



7. Haga clic en **Reiniciar** y la instancia de Citrix ADC VPX se reiniciará.
8. Para cambiar o liberar la asignación de licencias, vaya a **Sistema** > **Licencias** > **Administrar licencias** y seleccione **Cambiar asignación** o **Liberar asignación.**



9. Si hace clic en **Cambiar asignación**, una ventana emergente muestra las licencias disponibles en el servidor de licencias. Seleccione la licencia requerida, haga clic en **Obtener licencias**.

Asignación de licencias VPX a una instancia NetScaler ADC VPX mediante la CLI de NetScaler ADC

1. En un cliente SSH, introduzca la dirección IP de la instancia de Citrix ADC e inicie sesión con las credenciales de administrador.
2. Para agregar un servidor de licencias, escriba el siguiente comando:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Para mostrar las licencias disponibles en el servidor de licencias, escriba el siguiente comando:

```
sh licenseserverpool
<!--NeedCopy-->
```



```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. Para asignar una licencia al dispositivo NetScaler ADC VPX, escriba el siguiente comando:

```
set capacity  –platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

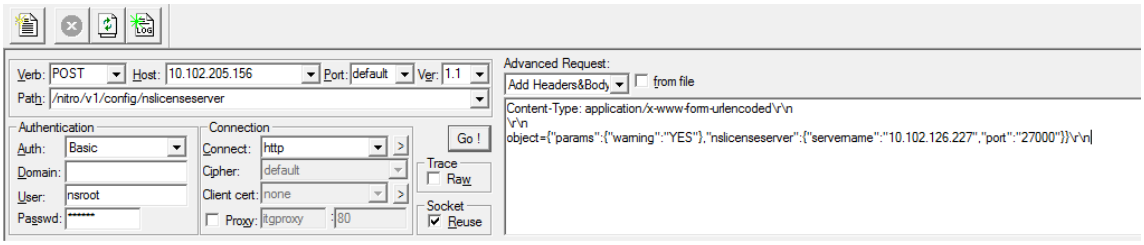
Asignación de licencias VPX a una instancia NetScaler ADC VPX mediante API

En un navegador web o un cliente de API, inicie sesión en la instancia de Citrix ADC VPX con las credenciales de administrador.

Para agregar un servidor de licencias:

1. Establezca el tipo de solicitud en **Publicar**.
2. Establezca la ruta en /nitro/v1/config/nslicensingserver.
3. Establezca la carga útil de la siguiente manera:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  “ params ” ;{
 warning ” : ” yes ”  }
 , ” nslicensing server ” ;{
 servername ” : ” <Citrix ADM IP> ” ,  “ port ” : ” 27000 ”  }
  }
 \r\n
<!--NeedCopy-->
```

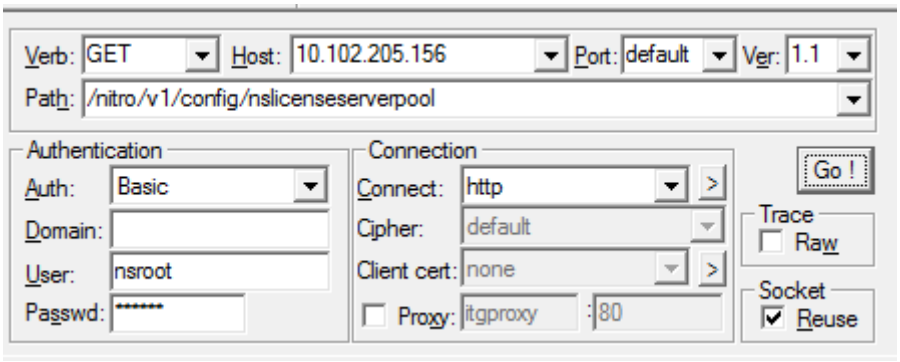



NetScaler ADM responde a la solicitud. La siguiente respuesta muestra éxito.

```
RESPONSE: **************\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

Para ver las licencias disponibles en el servidor de licencias:

1. Defina el tipo de solicitud en **Get**.
2. Establezca la ruta en /nitro/v1/config/nslicenseserverpool



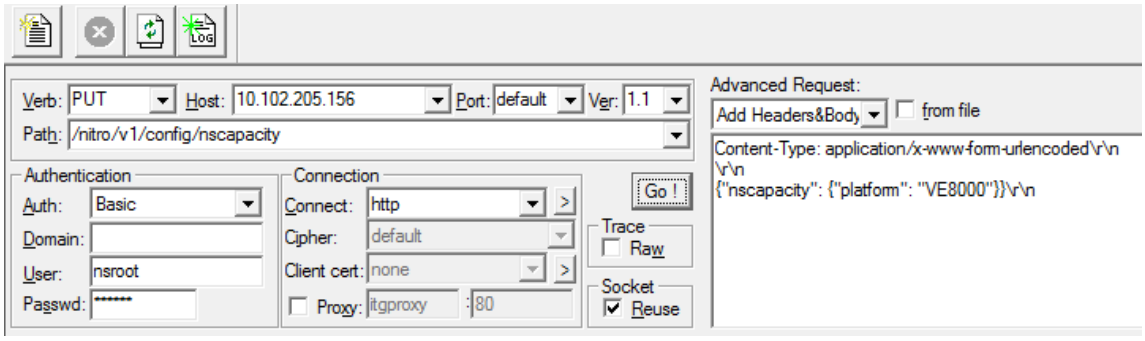
NetScaler ADM responde a la solicitud. La respuesta de ejemplo siguiente muestra el éxito y la lista de licencias disponibles en el servidor de licencias.

RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

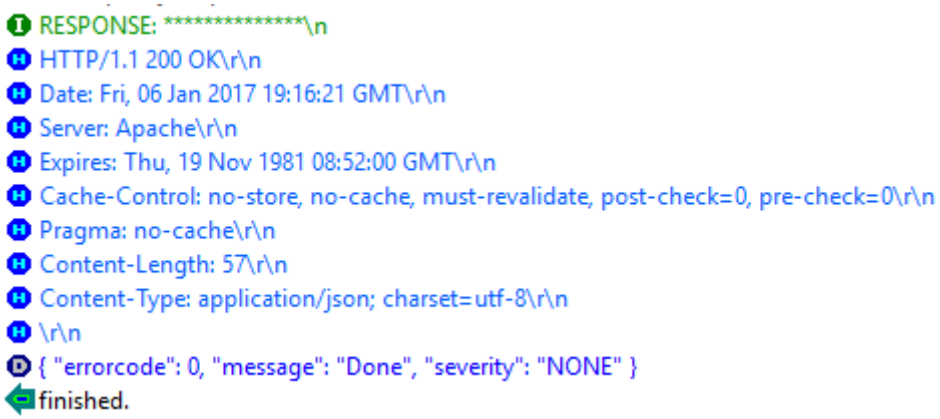
Para asignar una licencia al dispositivo NetScaler ADC VPX:

1. Establezca el tipo de solicitud en **Publicar**.
2. Establezca la ruta en /nitro/v1/config/nscapacity.
3. Establezca la carga útil de la siguiente manera:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  " nscapacity:{
  " platform " : " VE8000 "  }
   }
  \r\n
<!--NeedCopy-->
```



NetScaler ADM responde a la solicitud. La siguiente respuesta muestra éxito.



Configurar comprobaciones de caducidad para licencias de registro y salida de NetScaler ADC VPX

Ahora puede configurar el umbral de caducidad de licencia para las licencias NetScaler ADC VPX. Al establecer umbrales, NetScaler ADM envía notificaciones por correo electrónico o SMS cuando una licencia caduca. Una captura SNMP y una notificación también se envían cuando la licencia ha expirado en NetScaler ADM.

Se genera un evento cuando se envía una notificación de caducidad de licencia y este evento se puede ver en NetScaler ADM.

Para configurar comprobaciones de caducidad de licencias:

1. Vaya a **Redes** > **Licencias** .
2. En la página de **configuración** de la **licencia, en la sección Información de caducidad** de la licencia, puede encontrar los detalles de las licencias que van a caducar:
   - **Función**: Tipo de licencia que va a caducar.
   - **Recuento**: número de instancias o servidores virtuales que se verán afectados.
   - **Días para caducar**: Número de días antes de la expiración de la licencia.
3. En la sección**Configuración de notificaciones**, haga clic en el icono**Modificar** y especifique el umbral de alerta. Puede establecer un porcentaje de la capacidad de licencias agrupadas que se utilizará para notificar a los administradores.
4. Seleccione el tipo de notificación que quiere enviar marcando la casilla correspondiente. Los tipos de notificación son los siguientes:
   a) **Perfil de correo electrónico**: especifique un servidor de correo y los detalles del perfil. Se activa un correo electrónico cuando las licencias están a punto de caducar.

b) **Perfil SMS**: especifique un servidor del servicio de mensajes cortos (SMS) y los detalles del perfil. Se activa un mensaje SMS cuando las licencias están a punto de caducar.

5. A continuación, especifique cuándo quiere enviar la notificación en términos de número de días antes de la caducidad de la licencia.
6. Haga clic en **Guardar**.

Licencias de CPU virtual NetScaler ADC

January 30, 2024

Los administradores de centros de datos como usted están adoptando tecnologías más nuevas que simplifican las funciones de la red y ofrecen costes más bajos y una mayor escalabilidad. La arquitectura de centro de datos más reciente debe incluir, como mínimo, las siguientes funciones:

- Redes definidas por software (SDN)
- Virtualización de funciones de red (NFV)
- Virtualización de red (NV)
- Microservicios

Este movimiento también requiere que los requisitos de software sean dinámicos, flexibles y ágiles para satisfacer las necesidades empresariales en constante cambio. También se espera que las licencias sean administradas por una herramienta de administración central con plena visibilidad del uso.

Licencias de CPU virtuales para NetScaler ADC VPX

Anteriormente, las licencias de NetScaler ADC VPX se asignaban en función del consumo de ancho de banda de las instancias. Un NetScaler ADC VPX está restringido a usar un ancho de banda específico y otras métricas de rendimiento según la edición de licencia a la que está vinculado. Para aumentar el ancho de banda disponible, debe actualizar a una edición de licencia que proporcione más ancho de banda. En ciertos casos, el requisito de ancho de banda puede ser menor, pero el requisito es más para otro rendimiento de L7, como SSL TPS, rendimiento de compresión, etc. Es posible que la actualización de la licencia NetScaler ADC VPX no sea adecuada en estos casos. Pero es posible que tenga que comprar una licencia con gran ancho de banda para desbloquear los recursos del sistema necesarios para el procesamiento intensivo de la CPU. NetScaler ADM ahora admite la asignación de licencias a la instancia de NetScaler ADC en función de los requisitos de la CPU virtual.

En la función de licencia basada en el uso de CPU virtual, la licencia especifica el número de CPU a las que tiene derecho un NetScaler ADC VPX determinado. Por lo tanto, el Citrix ADC VPX puede

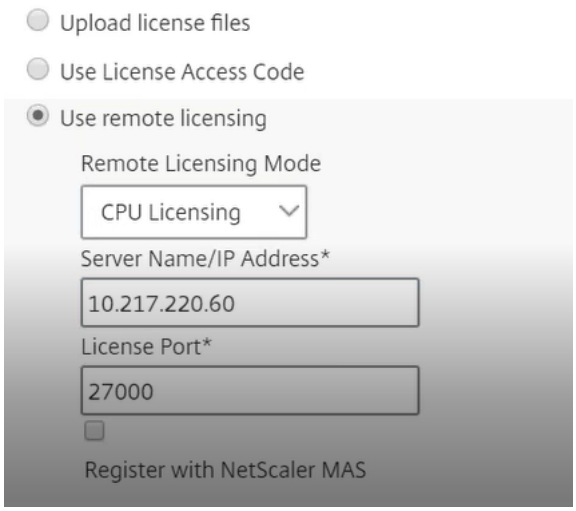
extraer licencias solo para la cantidad de CPU virtuales que se ejecutan en él desde el servidor de licencias. NetScaler ADC VPX extrae licencias en función del número de CPU que se ejecutan en el sistema. NetScaler ADC VPX no considera las CPU inactivas al retirar las licencias.

Al igual que la capacidad de licencias agrupadas y las funcionalidades de licencias CICO, el servidor de licencias NetScaler ADM administra un conjunto independiente de licencias de CPU virtuales. También en este caso, las tres ediciones administradas para las licencias de CPU virtuales son Standard, Enterprise y Platinum. Estas ediciones desbloquean el mismo conjunto de funciones que las desbloqueadas por las ediciones para licencias de ancho de banda.

Es posible que se produzca un cambio en la cantidad de CPU virtuales o que se produzca un cambio en la edición de la licencia. En tal caso, siempre debe cerrar la instancia antes de iniciar una solicitud de un nuevo conjunto de licencias. Debe reiniciar el Citrix ADC VPX después de retirar las licencias.

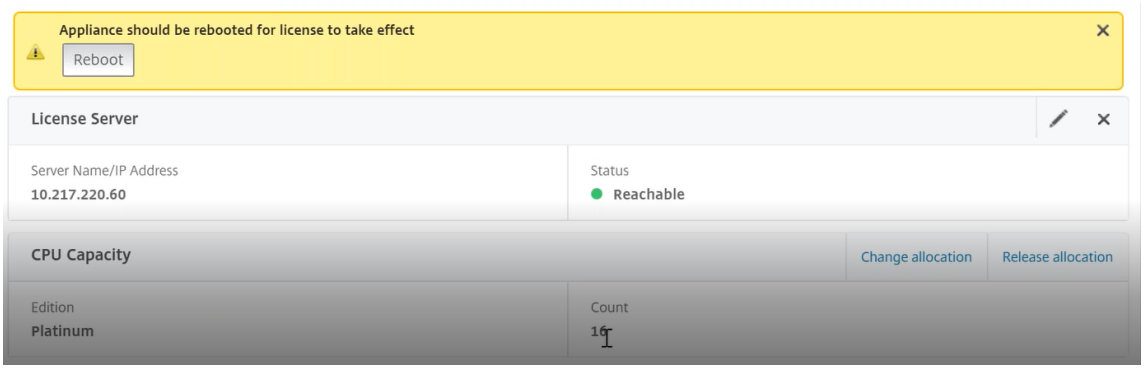
Para configurar el servidor de licencias en NetScaler ADC VPX mediante GUI:

1. En NetScaler ADC VPX, vaya a **Sistema** > **Licencias** y haga clic en **Administrar licencias**.
2. En la página **Licencia**, haga clic en **Agregar nueva licencia**.
3. En la página **Licencias**, seleccione la opción **Usar licencias remotas**.
4. Seleccione las **licencias de CPU** en la lista **de modos de licencia remota**.
5. Escriba la dirección IP del servidor de licencias y el número de puerto.
6. Haga clic en **Continuar**.



> **Nota:**
>
> Siempre debe registrar la instancia de NetScaler ADC VPX en NetScaler ADM. Si aún no lo ha hecho, habilite **Registrarse con NetScaler ADM** y escriba las credenciales de inicio de sesión de NetScaler ADM.

7. En la ventana **Asignar licencias**, seleccione el tipo de licencia. La ventana muestra el total de las CPU virtuales disponibles y también las CPU que se pueden asignar. Haga clic en **Obtener licencias**.
8. Haga clic en **Reiniciar** en la página siguiente para solicitar las licencias.



> **Nota**También
>
> puede liberar la licencia actual y salir de una edición diferente. Por ejemplo, ya está ejecutando una licencia de edición estándar en su instancia. Puede liberar esa licencia y, a continuación, retirarla de la edición Enterprise.

Configuración del servidor de licencias en la licencia NetScaler ADC VPX mediante CLI

En la consola NetScaler ADC VPX, escriba los siguientes comandos para las dos tareas siguientes:

1. Para agregar el servidor de licencias al NetScaler ADC VPX:

```
add licenseserver <IP address of the license server>
<!--NeedCopy-->
```

2. Para solicitar las licencias:

```
set capacity -vcpu - edition platinum
<!--NeedCopy-->
```

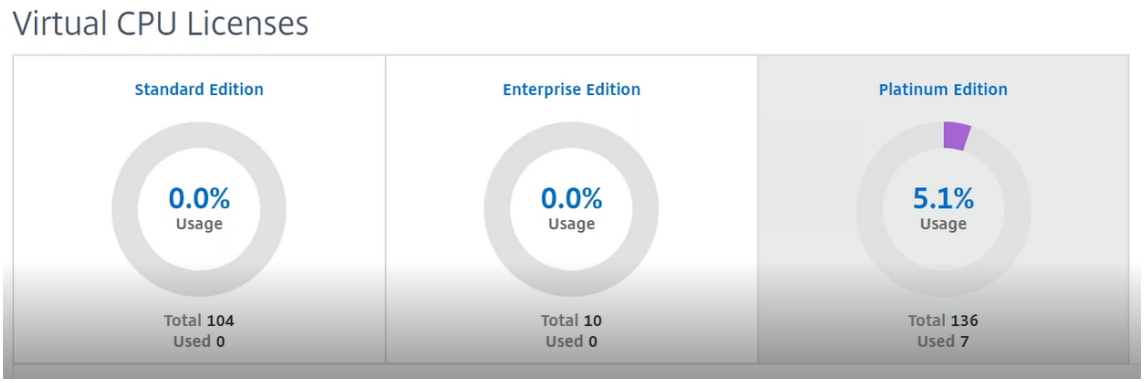
   Cuando se le solicite, reinicie la instancia escribiendo el siguiente comando:

```
reboot -w
<!--NeedCopy-->
```

Administración de licencias de CPU virtual en NetScaler ADM

1. En Citrix ADM, vaya a **Redes** > **Licencias** > Licencias de **CPU virtuales** .
2. La página muestra las licencias asignadas para cada tipo de edición de licencia.

3. Haga clic en el número de cada anillo para ver las instancias de Citrix ADC que utilizan esta licencia.



Licencias de CPU virtual para NetScaler ADC CPX

Al aprovisionar la instancia CPX de NetScaler ADC, puede configurar la instancia CPX de NetScaler ADC para que extraiga las licencias del servidor de licencias en función del uso de la CPU de la instancia.

NetScaler ADC CPX depende del servidor de licencias, que se ejecuta en NetScaler ADM, para administrar las licencias. NetScaler ADC CPX extrae las licencias del servidor de licencias cuando se inicia. Las licencias se archivan de nuevo en el servidor de licencias cuando se cierra el NetScaler ADC CPX.

Puede descargar NetScaler ADC CPX desde Docker App Store. En el host Docker, para descargar NetScaler ADC CPX, ejecute el siguiente comando:

```
docker pull store/citrix/netscalercpx:<version>
<!--NeedCopy-->
```

Existen tres tipos de licencia disponibles para las licencias CPX:

1. Licencias de suscripción de CPU virtual compatibles con CPX y VPX
2. Licencias de capacidad agrupada
3. Licencias CP1000 que admiten vCPU de una a varias vCPU para CPX solamente

Para configurar licencias de suscripción de vCPU al Provisioning la instancia CPX de NetScaler ADC:

Debe especificar el número de licencias de vCPU que utiliza la instancia CPX de Citrix ADC.

- Este valor se introduce como una variable de entorno a través de Docker, Kubernetes o Mesos/-Marathon.
- La variable de destino es “CPX_CORES”. El CPX puede admitir de 1 a 7 núcleos.

Para especificar 2 núcleos, puede ejecutar el comando docker run de la siguiente manera:


```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2
<!--NeedCopy-->
```

Al aprovisionar una instancia de Citrix ADC CPX, defina el servidor de licencias Citrix ADC como una variable de entorno en el comando **docker run** , como se muestra a continuación:

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> cpx:11.1
<!--NeedCopy-->
```

Donde:

- < LS_IP_ADDRESS >*es la dirección IP del servidor de* licencias de NetScaler ADC.
- *<LS_PORT>* es el puerto del servidor de licencias NetScaler ADC. De forma predeterminada, el puerto es 27000.

> **Nota**De forma
>
> predeterminada, la instancia de NetScaler ADC CPX extrae la licencia del grupo de suscripciones de vCPU. La instancia CPX extrae "n"el número de licencias si la instancia se está ejecutando con "n"CPU.

Para configurar las licencias de NetScaler ADC Pooled Capacity o CP1000 al Provisioning la instancia de NetScaler ADC CPX:

Si desea obtener las licencias de la instancia de CPX mediante las licencias agrupadas (basadas en el ancho de banda) o el grupo privado de CPX (CP1000 o basadas en un grupo privado), debe proporcionar las variables de entorno correspondientes.

Por ejemplo,

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e PLATFORM=CP1000 cpx:11.1
<!--NeedCopy-->
```

CP1000. Este comando desencadena la extracción desde el grupo CP1000 (grupo privado CPX). A continuación, la instancia CPX de Citrix ADC recupera el número «n» de instancias para el número «n» de núcleos especificado para CPX_CORES. El caso de uso más común es especificar n = 1 para una extracción de una sola instancia. Los casos de uso de CPX multinúcleo comprueban «n» vCPU (donde «n» va de 1 a 7).

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
<!--NeedCopy-->
```


Capacidad agrupada. Este comando extrae una licencia del grupo de instancias y consume 1000 Mbps de ancho de banda del grupo de ancho de banda platino, pero permite que CPX ejecute hasta 2000 Mbps.En Pooled Licensing, los primeros 1000 Mbps no se cobran.

> **Nota:**
>
> Especifique el número correspondiente de vCPU para el ancho de banda objetivo deseado al retirar el grupo de ancho de banda, tal como se detalla en la siguiente tabla:

Número de núcleos (vCPU)	Ancho de banda máximo
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps
5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

Administrar instancias de Citrix SD-WAN

January 30, 2024

Citrix ADM le permite supervisar, administrar y ver los análisis de los dispositivos Citrix SD-WAN de su red. La siguiente tabla de interoperabilidad proporciona información sobre las funciones de Citrix ADM que se admiten actualmente en cada una de las ediciones de la plataforma Citrix SD-WAN.

Matriz de interoperabilidad de las ediciones de la plataforma Citrix SD-WAN de Citrix y funciones de NetScaler ADM

Modificación de plataforma	Detección	Configuración	Supervisión	Informes (informes de red)	Gestión de eventos	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Modificación de plataforma	Detección	Configuración	Supervisión	Informes (informes de red)	Gestión de eventos	HDX Insight	WAN Insight
Citrix SD-WAN SE	Sí	No	No	No	No	No	No
Citrix SD-WAN PE	Sí	No	No	No	No	Sí	No

Versiones de Citrix SD-WAN compatibles con Citrix ADM

Modificación de plataforma	Versión Citrix SD-WAN	Versión Citrix ADM
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 y versiones posteriores	Citrix ADM 11.0 y versiones posteriores
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 y posterior	NetScaler ADM 12.0.53.8 y posterior
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 y posterior	NetScaler ADM 12.0.53.8 y posterior

Puede agregar un dispositivo Citrix SD-WAN WANOP como instancia administrada en NetScaler ADM. Para obtener más información, consulte Agregar instancias a NetScaler ADM. Puede ver la información WAN, HDX, los informes de red y los informes de eventos para las instancias de Citrix SD-WAN WANOP.

NetScaler ADM permite que los dispositivos Citrix SD-WAN Standard Edition (SE) y Enterprise Edition (EE) se registren como instancias administradas en NetScaler ADM.

Para agregar un dispositivo Citrix SD-WAN SE/PE/AE a NetScaler ADM, configure NetScaler ADM como un recopilador AppFlow en los dispositivos Citrix SD-WAN SE/PE/AE. El dispositivo Citrix SD-WAN SE/PE/AE se agrega como instancia administrada en NetScaler ADM. El dispositivo SD-WAN SE/PE/AE envía los datos de análisis a NetScaler ADM.

Puede configurar NetScaler ADM como un recopilador AppFlow en cada dispositivo SD-WAN SE/PE/AE individualmente, o utilizar Citrix SD-WAN Center para exportar la configuración a los dispositivos administrados.

Para obtener más información, consulte Agregar instancias de Citrix SD-WAN SE/PE/AE en NetScaler ADM.

Para un dispositivo Citrix SD-WAN PE, puede ver registros de datos HDX o datos de varios saltos, dependiendo de la configuración de AppFlow. Un dispositivo Citrix SD-WAN SE proporciona solo datos de salto múltiple. Para obtener más información, consulte Visualización de informes y métricas de HDX Insight y Visualización de datos de análisis para la implementación de varios saltos.

Esta página proporciona vínculos de acceso rápido a los temas a los que puede hacer referencia para configurar NetScaler ADM y administrar los dispositivos WANOP SD-WAN mediante NetScaler ADM.

Descripción general de Citrix ADM

Acerca de Citrix ADM

Architecture

Cómo descubre Citrix ADM las instancias

Cómo se comunica Citrix ADM con las instancias administradas

Implementación de Citrix ADM

Implemente Citrix ADM con Citrix Hypervisor

Implementación de NetScaler ADM con Microsoft Hyper-V

Implemente Citrix ADM con VMware ESXi

Implementación de NetScaler ADM con Linux KVM Server

Implemente Citrix ADM en modo de alta disponibilidad

Migrate from NetScaler Insight Center to NetScaler ADM

Integración de NetScaler ADM con Director

Administración de instancias

Cómo agregar instancias a Citrix ADM

Cómo crear grupos de instancias en Citrix ADM

Cómo hacer una copia de seguridad y restaurar una instancia mediante Citrix ADM

Administración de configuración

Cómo crear trabajos de configuración a partir de comandos correctivos en Citrix ADM

Cómo programar los trabajos creados mediante plantillas integradas en Citrix ADM

Cómo reprogramar los trabajos que se configuraron mediante plantillas integradas en Citrix ADM

Cómo reutilizar los trabajos de configuración ejecutados

Análisis

WAN Insight

HDX Insight

Cómo ver los informes de red de las instancias de Citrix SD-WAN WANOP

Cómo configurar los umbrales adaptativos

Cómo configurar el resumen de bases de datos para análisis

Cómo crear umbrales y alertas mediante Citrix ADM

Gestión de eventos

Cómo establecer la antigüedad de los eventos en Citrix ADM

Cómo programar un filtro de eventos mediante Citrix ADM

Cómo configurar notificaciones de correo electrónico repetidas para eventos de Citrix ADM

Cómo suprimir eventos mediante Citrix ADM

Cómo ver informes de eventos para instancias de Citrix SD-WAN WANOP

Cómo modificar la gravedad notificada de los eventos que se producen en las instancias de NetScaler

Cómo ver el resumen de eventos en NetScaler ADM

Cómo mostrar la gravedad de los eventos y los sesgos de las trampas de SNMP en el panel de infraestructura de Citrix ADM

Autenticación

Cómo conectar en cascada servidores de autenticación externos

Cómo agregar servidores de autenticación RADIUS

Cómo agregar servidores de autenticación LDAP

Cómo agregar servidores de autenticación TACACS

Cómo extraer el grupo de servidores de autenticación en Citrix ADM

Cómo habilitar la autenticación local alternativa

Sistema NetScaler ADM

Administración del sistema Citrix ADM

Cómo actualizar Citrix ADM

Cómo generar un archivo de soporte técnico para Citrix ADM

Cómo hacer copias de seguridad y restaurar el servidor Citrix ADM en una implementación de un solo servidor

Cómo hacer una copia de seguridad y restaurar una configuración de Citrix ADM en un par HA

Cómo habilitar el acceso a Shell para usuarios no predeterminados en Citrix ADM

Cómo configurar el servidor NTP en Citrix ADM

Cómo configurar los parámetros de SSL para Citrix ADM

Cómo configurar el intervalo de purga de Syslog para Citrix ADM

Cómo ver la información de auditoría de NetScaler ADM

Cómo configurar las opciones de notificación del sistema de NetScaler ADM

Cómo supervisar el uso de la CPU, la memoria y el disco de Citrix ADM

Cómo configurar un grupo de cifrado para Citrix ADM

Cómo crear trampas, administradores y usuarios de SNMP en Citrix ADM

Cómo asignar un nombre de host a un servidor Citrix ADM

Cómo configurar los parámetros de poda del sistema para Citrix ADM

Cómo configurar los ajustes de copia de seguridad del sistema mediante Citrix ADM

Cómo configurar y ver alarmas del sistema en NetScaler ADM

Agregar instancias de Citrix SD-WAN

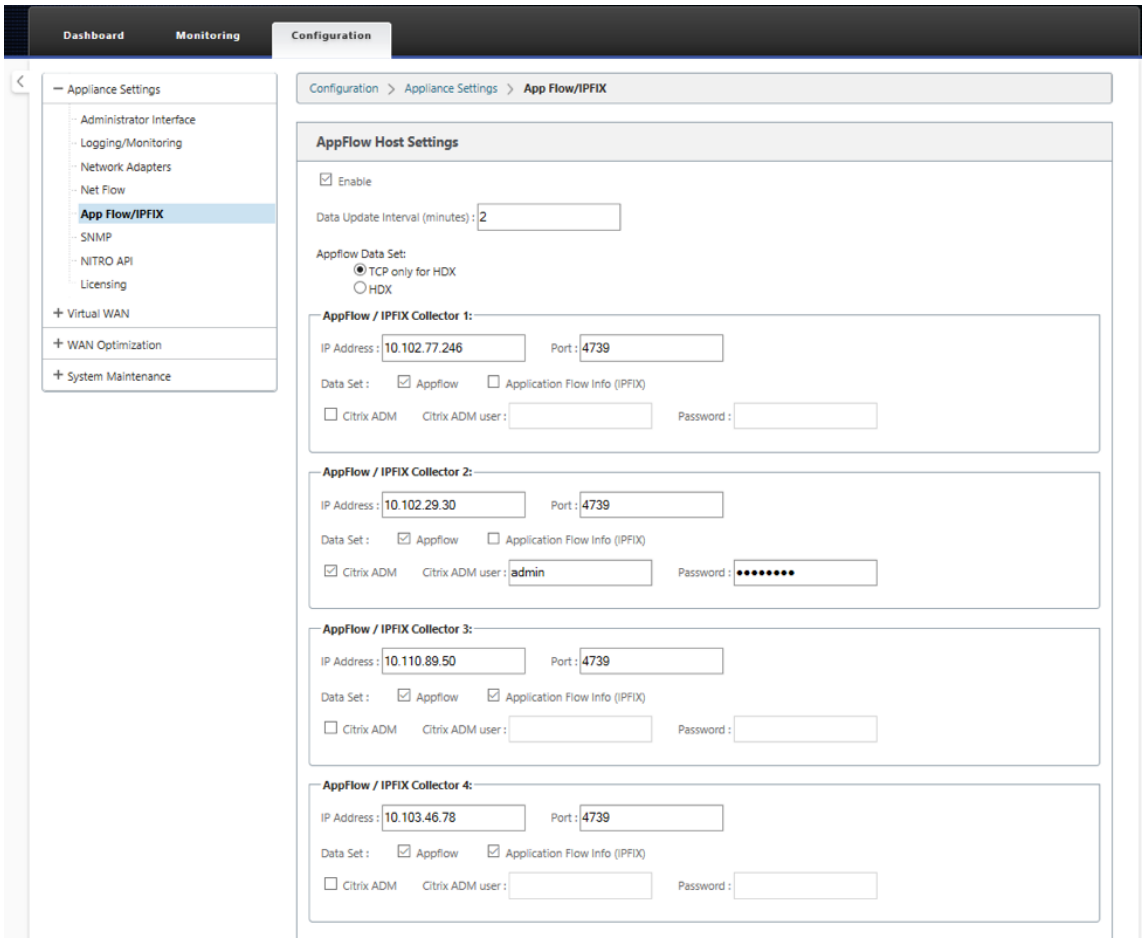
January 30, 2024

Configure NetScaler ADM como el recopilador AppFlow en el dispositivo Citrix SD-WAN SE/PE para agregar estas instancias en NetScaler ADM. Los dispositivos Citrix SD-WAN SE/PE se registran como instancias administradas en Citrix ADM y se recopilan sus registros de AppFlow. Para un dispositivo Citrix SD-WAN PE, puede habilitar la plantilla **TCP solo para HDX** o la plantilla **HDX** . La plantilla **TCP solo para HDX** proporciona datos de saltos múltiples. La plantilla **HDX** proporciona datos HDX, debe habilitarse únicamente en el dispositivo del centro de datos.

Puede configurar NetScaler ADM como un recopilador AppFlow en el dispositivo SD-WAN SE/PE/AE individual, o puede configurar NetScaler ADM como el recopilador AppFlow mediante SD-WAN Center y exportar la configuración a los dispositivos administrados por él.

Para configurar NetScaler ADM como un recopilador AppFlow en un dispositivo Citrix SD-WAN SE/PE/AE:

1. En la interfaz web SD-WAN SE/PE/AE, vaya a **Configuración** > **AppFlow/IPfix**
2. Elija **Activar**.



3. En el campo **Intervalo de actualización de datos** , especifique el intervalo de tiempo, en minutos, en el que los informes de AppFlow se exportan al recopilador de AppFlow.

> **Nota**
>
> Si Citrix ADM es el recopilador de AppFlow, el intervalo de actualización de datos debe ser de 1 minuto.

4. Lleve a cabo una de las siguientes acciones:

- Elija **HDX** para enviar datos de HDX Insight al recopilador de AppFlow. Esto debe estar habilitado en los dispositivos de la sucursal.
- Elija **TCP solo para HDX** para enviar datos de varios saltos al recopilador de AppFlow.

> **Nota**
>
> **La opción de plantilla HDX**solo está disponible para el dispositivo Citrix SD-WAN PE; debe estar habilitada en el dispositivo Data Center

5. En el campo **Dirección IP** , escriba la dirección IP del sistema recopilador AppFlow externo (Citrix ADM Server).
6. En el campo **Puerto** , escriba el número de puerto en el que escucha el sistema recopilador AppFlow externo. El valor predeterminado es 4739.
7. Seleccione la casilla **Citrix ADM** para especificar que Citrix ADM es el recopilador de AppFlow.

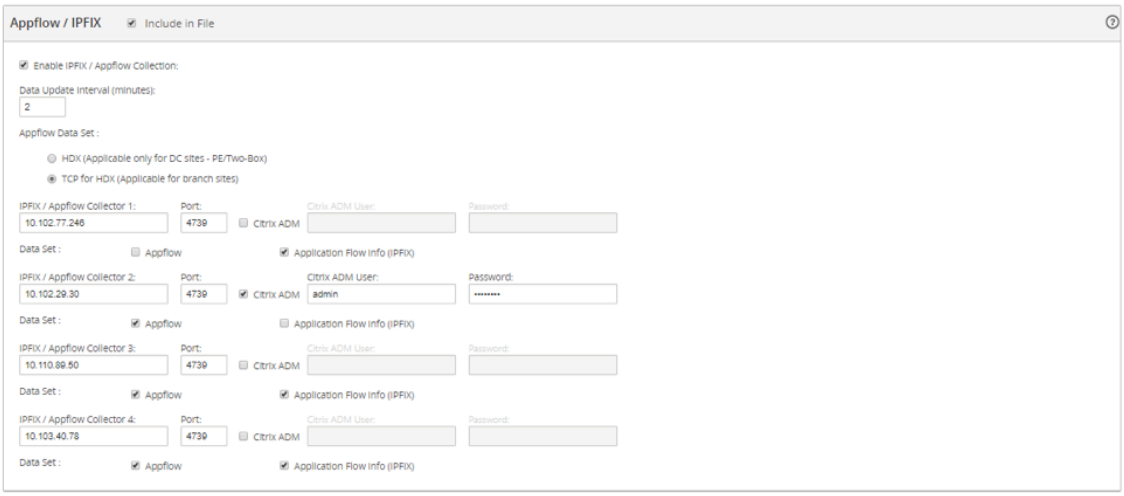
> **Nota**
>
> - Actualmente, NetScaler ADM no admite la recopilación IPFIX.
> - Puede añadir hasta cuatro recopiladores de AppFlow. Citrix ADM o cualquier recopilador de AppFlow que admita el protocolo IPFIX.

8. Introduzca las credenciales del servidor Citrix ADM
9. Haga clic en **Aplicar configuración**.

Los dispositivos Citrix SD-WAN SE/PE se descubren y se enumeran en Citrix ADM. Los dispositivos Citrix SD-WAN SE/PE envían los datos de análisis a NetScaler ADM. Para obtener más información, consulte AppFlow e IPFIX.

Para configurar NetScaler ADM como un recopilador de AppFlow mediante Citrix SD-WAN Center:

1. En la interfaz de usuario de administración de Citrix SD-WAN Center, vaya a **Configuración** > **Configuración del**dispositivo.
2. Navegue hasta la sección **AppFlow/IPFIX** y seleccione **Incluir en archivo**.
3. Seleccione **Habilitar colección IPFIX/AppFlow**.



4. En el campo **Intervalo de actualización de datos**, especifique el intervalo de tiempo, en minutos, en el que se exportan los informes de AppFlow al recopilador AppFlow.

> **Nota**
>
> Si Citrix ADM es el recopilador de AppFlow, el intervalo de actualización de datos debe ser de 1 minuto.

5. Lleve a cabo una de las siguientes acciones:

   - Elija **HDX** para enviar datos de HDX Insight al recopilador de AppFlow.
   - Elija **TCP para HDX** para enviar datos de información de varios saltos al recopilador de AppFlow. Esto debe estar habilitado en los dispositivos de la sucursal.

> **Nota**
>
> **La opción de plantilla HDX**solo está disponible para el dispositivo Citrix SD-WAN PE; debe estar habilitada en el dispositivo Data Center.

6. En el campo **IPFIX/AppFlow Collector**, escriba la dirección IP del sistema recopilador AppFlow externo (Citrix ADM Server).
7. En el campo **Puerto** , escriba el número de puerto en el que escucha el sistema recopilador AppFlow externo. El valor predeterminado es 4739.
8. Seleccione la casilla **Citrix ADM** para especificar que Citrix ADM es el recopilador de AppFlow.
9. Introduzca las credenciales del servidor Citrix ADM.

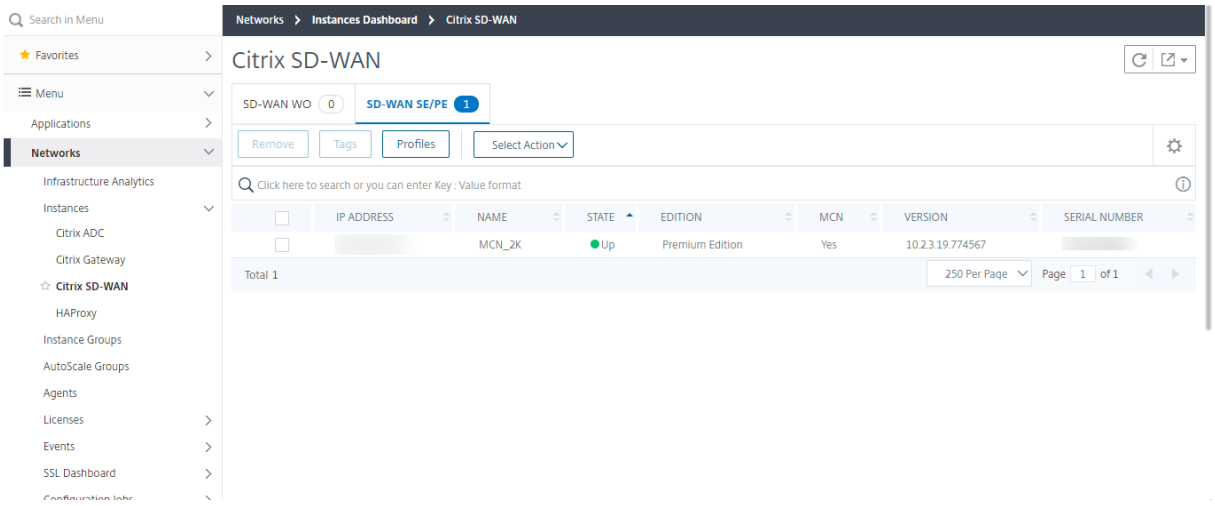
> **Nota**
>
> Puede añadir hasta cuatro recopiladores de AppFlow. Citrix ADM o cualquier recopilador de AppFlow que admita el protocolo IPFIX.

10. Guarde y exporte la configuración a los dispositivos administrados.

    Para obtener más información, consulte Cómo configurar y exportar la configuración del dispositivo a los dispositivos administrados.

Para obtener más información sobre cómo configurar NetScaler ADM como recopilador de AppFlow mediante Citrix SD-WAN Center, AppFlow e IPFIX.

NetScaler ADM detecta y enumera los dispositivos Citrix SD-WAN SE/PE.Los dispositivos Citrix SD-WAN SE/PE se detectan y aparecen en NetScaler ADM. Para ver los dispositivos Citrix SD-WAN SE/PE detectados, en la interfaz web de NetScaler ADM, vaya a **Redes** > **Instancias** > **Citrix SD-WAN** y seleccione **SD-WAN SE/PE/AE**.



Puede ver la dirección IP, el nombre, el estado actual, la edición del software y la versión de los dispositivos descubiertos. También puede comprobar si el dispositivo es un nodo de controlador maestro (MCN) o no.

Puede realizar las siguientes acciones:

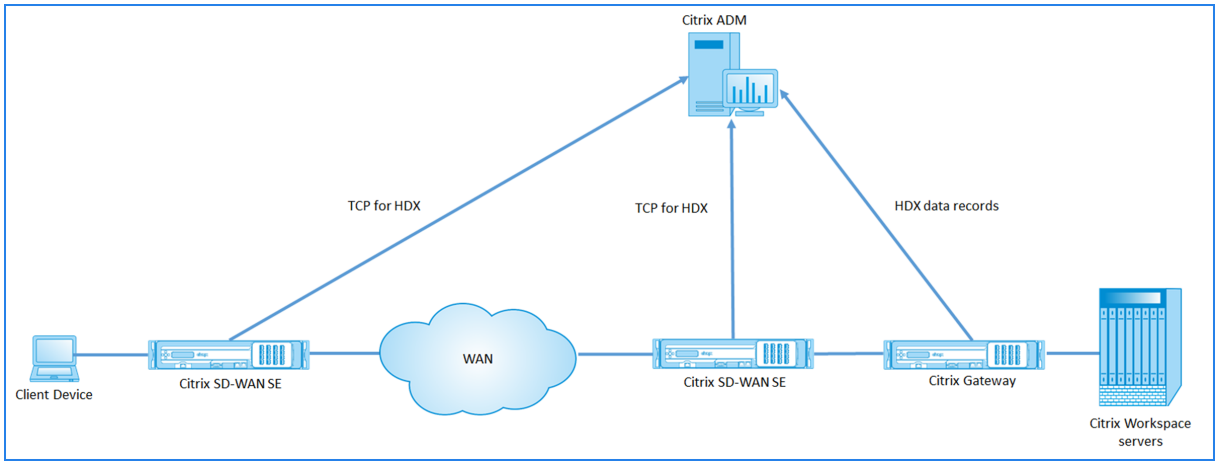
- Ver y eliminar los perfiles de instancia.
- Elimine instancias de Citrix ADM.
- Redescubra instancias.

Para un dispositivo Citrix SD-WAN PE, puede ver registros de datos HDX o datos de varios saltos, dependiendo de la configuración de AppFlow. Un dispositivo Citrix SD-WAN SE proporciona solo datos de salto múltiple. Para obtener más información, consulte Visualización de informes y métricas de HDX Insight y Visualización de datos de Citrix SD-WAN Analytics para la implementación de varios saltos.

Ver los datos de análisis de Citrix SD-WAN para la implementación de varios saltos

January 30, 2024

Una implementación de red de varios saltos tiene varios dispositivos entre el cliente y el servidor, como se muestra en la ilustración siguiente. En este tipo de implementación, los dispositivos Citrix SD-WAN SE y Citrix Gateway se agregan a Citrix ADM y AppFlow está habilitado.



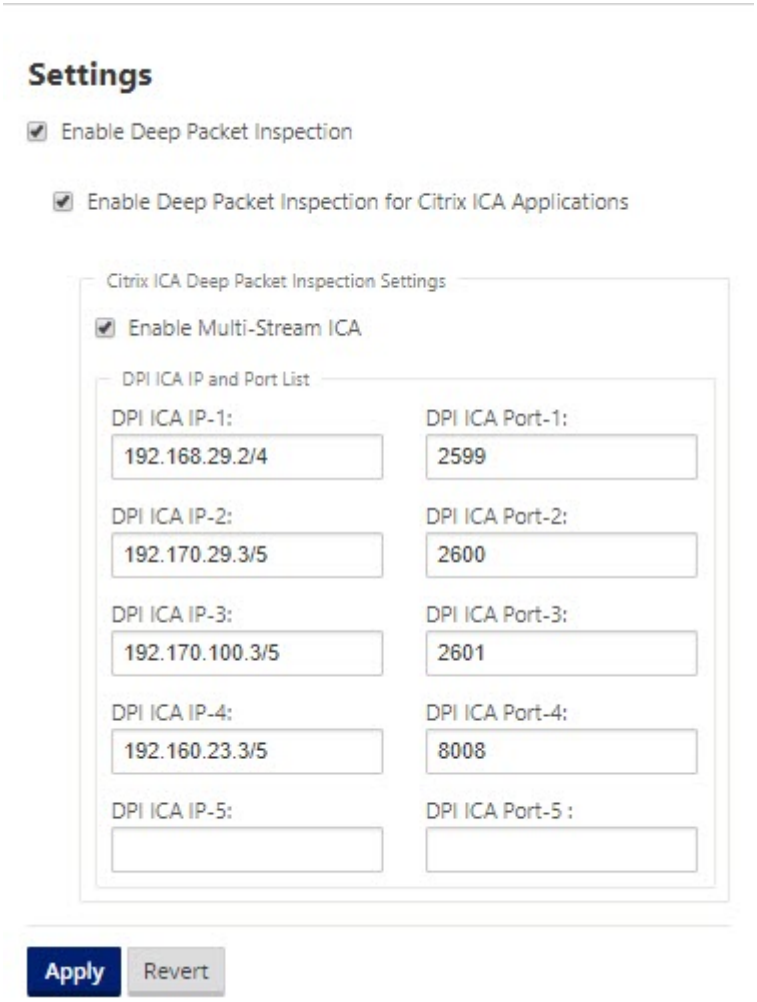
Citrix ADM identifica el dispositivo del que recibe los datos en función del recuento de saltos y el ID de la cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos a través de los cuales fluye el tráfico del cliente al servidor. El ID de la cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos y genera los informes.

Para que los dispositivos Citrix SD-WAN SE envíen los datos de análisis a Citrix ADM, debe configurar la dirección IP virtual de Citrix Gateway como IP ICA de DPI y establecer el número de puerto ICA de DPI en 443.

Para configurar los ajustes de DPI de ICA:

1. En la interfaz de usuario del dispositivo Citrix SD-WAN SE, vaya al **Editor de configuración** > **Avanzado** > **Global** > **Aplicaciones** > **Configuración**.
2. Seleccione **Habilitar la inspección profunda de paquetes** > **Habilitar la inspección profunda de paquetes para aplicaciones ICA de Citrix** > **Habilitar ICA de transmisión múltiple**



3. En el campo **DPI ICA IP-1**, introduzca la dirección IP virtual y el prefijo de Citrix Gateway.
4. En el campo **DPI ICA Port-1**, introduzca el número de puerto 443.
5. Haga clic en **Aplicar** y exporte la configuración al dispositivo mediante el proceso de gestión de cambios.

En Citrix ADM, para cada sesión ICA activa, puede ver un diagrama de sesión en HDX Insight. Los diagramas de sesión proporcionan detalles sobre los dispositivos de la ruta de conexión. También proporcionan información sobre la latencia del lado del cliente y del lado del servidor entre un dispositivo de red y su siguiente salto inmediato. Esta información le permite identificar la causa raíz del retraso y solucionar los problemas de rendimiento.

Citrix SD-WAN SE no envía registros de datos HDX. Solo proporciona información de TCP para HDX. Los datos de HDX Insight los proporcionan los dispositivos habilitados para HDX Insight de la red (por ejemplo, Citrix ADC o Citrix Gateway).

El dispositivo Citrix SD-WAN PE puede enviar TCP para datos HDX o datos HDX Insight, dependiendo de la configuración de AppFlow del dispositivo.La plantilla HDX debe estar habilitada en el dispositivo

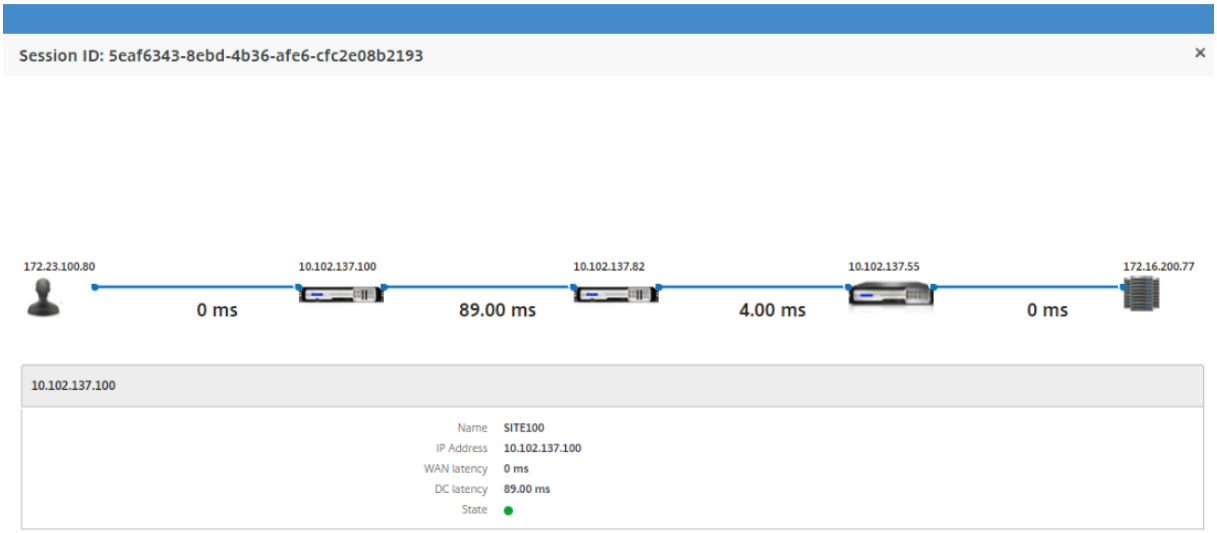
del centro de datos.

> **Nota**
>
> En una implementación de varios saltos, asegúrese de que solo uno de los dispositivos de red envíe datos de HDX Insight. El resto de los dispositivos de red pueden enviar datos TCP para HDX.

Para ver los datos de varios saltos:

En la interfaz web Citrix ADM, vaya a **HDX Insight** > **Usuarios** > **Sesiones actuales** o **HDX Insight** > **Aplicaciones** > **Sesiones actuales** y haga clic en el icono **Diagrama**.

Aparece el diagrama de topología de red.



Haga clic en cualquier elemento de la red para ver más información.

> **Nota**
>
> La información que se muestra depende del elemento de red seleccionado.

Aparecen los siguientes parámetros para los dispositivos Citrix:

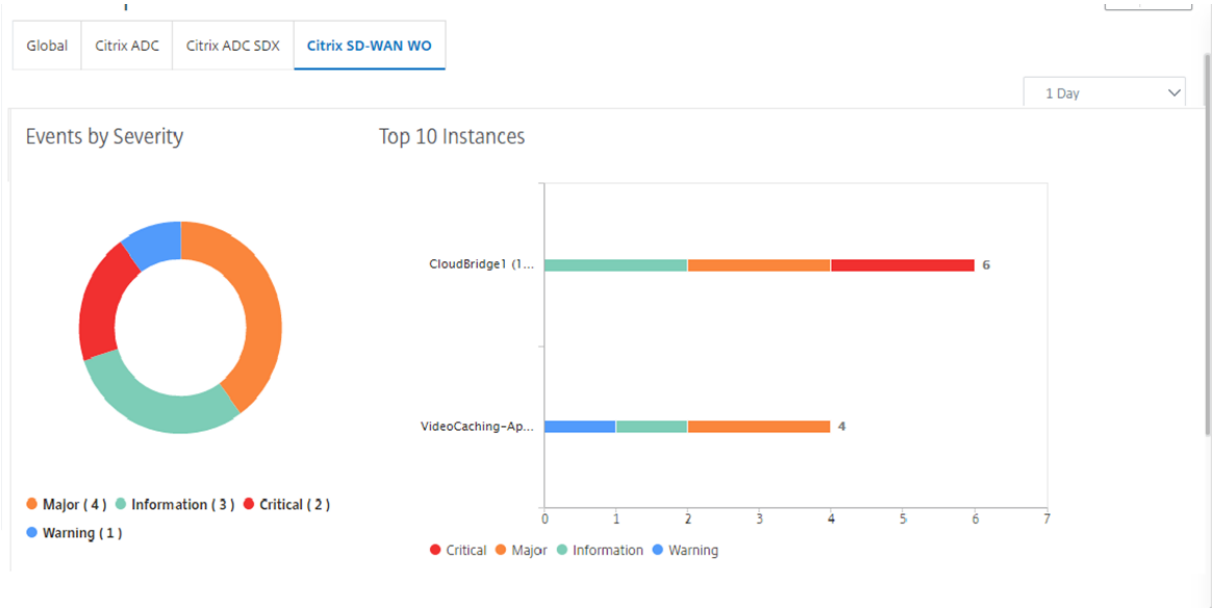
- **Nombre**: nombre del dispositivo Citrix.
- **Dirección IP**: dirección IP del dispositivo.
- **Latencia WAN**: latencia causada por el lado del cliente de la red. Es decir, desde el dispositivo Citrix hasta el usuario final.
- **Latencia DC**: latencia causada por el lado del servidor de la red. Es decir, desde el dispositivo Citrix hasta los servidores back-end.
- **Estado: Estado**de accesibilidad del dispositivo.

Ver informes de eventos para instancias de Citrix SD-WAN WANOP

January 30, 2024

Para ver los eventos de las 10 instancias principales de SD-WAN WANOP como representación gráfica, vaya a **Redes** > **EventosInformes**y seleccione**Citrix SD-WAN WO**.

Los eventos se muestran en función de su gravedad para cada instancia, puede hacer clic en cada gravedad para obtener más información sobre el número de eventos, cuándo ocurrió y a qué categoría pertenece.



Ver informes de red para instancias de Citrix SD-WAN WANOP

January 30, 2024

Puede ver los informes relacionados con la red de optimización de WAN en Citrix ADM. Con estos datos, puede solucionar problemas de red o analizar el comportamiento de sus dispositivos Citrix SD-WAN WAN WANOP. Puede ver los informes de las estadísticas de red de sus dispositivos de optimización de WAN durante la última hora, un día, una semana o un mes.

Puede ver los siguientes informes:

Informes	Descripción
Aceleración	Utilice este informe para analizar el patrón de tráfico acelerado (KBPS por clase de servicio) y el número de conexiones TCP aceleradas que pasan por el dispositivo de optimización de WAN. Esto incluye la cantidad de conexiones TCP que pasan por el dispositivo de optimización de WAN y que se aceleran, la cantidad de conexiones abiertas y semicerradas que se han seleccionado para la aceleración y la cantidad de conexiones medio abiertas que son candidatas a la aceleración.
Conexión de paso	Utilice este informe para ver las conexiones no aceleradas del dispositivo de optimización de WAN.
Clase de servicio	Utilice este informe para ver los ahorros de ancho de banda enviados y recibidos según el tipo de clase de servicio definido para el dispositivo de optimización de WAN.
Aplicación	Utilice este informe para ver el volumen de datos enviados y recibidos en bits por segundo para las aplicaciones que se ejecutan en el dispositivo de optimización de WAN.
Utilización de CPU	Utilice este informe para ver la utilización de la CPU del dispositivo de optimización de WAN como porcentaje.

Informes	Descripción
Incremento de capacidad	Utilice este informe para ver la relación de compresión de envío acumulada para el dispositivo de optimización de WAN.
Reducción de datos	Utilice este informe para ver el ahorro de ancho de banda de transmisión y recepción como porcentaje. También puede analizar el ancho de banda de transmisión y recibir valores de ahorro de ancho de banda por separado para el dispositivo de optimización de WAN.
Utilización de enlaces	Utilice este informe para ver la utilización de los enlaces de transmisión y recepción para la optimización de la WAN como porcentaje.
Uso del plugin	Utilice este informe para ver la cantidad de complementos conectados al dispositivo de optimización de WAN.
Pérdida de paquetes	Utilice este informe para ver los paquetes enviados por enlace interrumpido y los paquetes recibidos por enlace interrumpido para los enlaces definidos en el dispositivo de optimización de WAN.
Rendimiento	Utilice este informe para ver el volumen del enlace enviado y el volumen del enlace recibido en bits por segundo para el dispositivo de optimización de WAN.
QoS	Utilice este informe para ver el volumen de QOS enviado y de recepción de QOS en bits por segundo para el dispositivo de optimización de WAN.

Para ver los informes de red WANOP de Citrix SD-WAN:

1. En Citrix ADM, vaya a **Redes** > **Informes de red** > **Citrix SD-WAN WO** .
2. En la lista desplegable **Nombre** del informe, seleccione un informe que quiera ver.
3. En la lista desplegable **Instancias** , seleccione la instancia de Citrix SD-WAN WANOP para la que desea ver el informe.
4. En la lista desplegable **Duración** , seleccione el intervalo de tiempo.

5. Haga clic en **Ejecutar**.

Respaldar instancias de Citrix SD-WAN WANOP

January 30, 2024

Puede hacer una copia de seguridad del estado actual de una instancia y, más adelante, usar los archivos de la copia de seguridad para restaurar la instancia al mismo estado. Es una buena práctica hacer una copia de seguridad de una instancia antes de actualizarla o por motivos de precaución. Una copia de seguridad de un sistema estable le permite restaurar el sistema a un punto estable en caso de que se vuelva inestable. Hay varias formas de realizar copias de seguridad y restauraciones en una instancia de Citrix SD-WAN WANOP. Puede realizar copias de seguridad y restaurar instancias manualmente mediante la GUI, la CLI o utilizar Citrix ADM para realizar copias de seguridad. Citrix ADM realiza copias de seguridad del estado actual de las instancias SD-WAN WANOP administradas de Citrix mediante llamadas NITRO, el protocolo Secure Shell (SSH) y el protocolo Secure Copy (SCP).

Configuración de los ajustes de backup de instancias

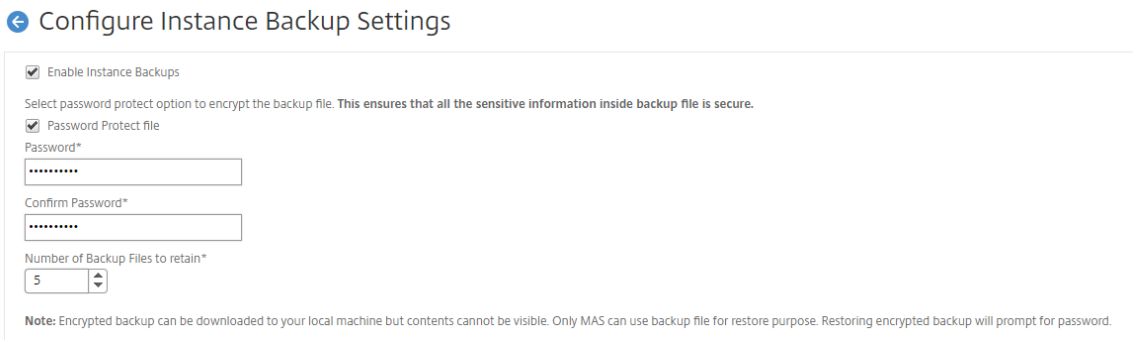
Antes de realizar una copia de seguridad de la instancia Citrix SD-WAN WANOP en Citrix ADM, debe configurar la configuración de copia de seguridad de la instancia en Citrix ADM.

Para configurar los ajustes de copia de seguridad de la instancia:

1. En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**. En el panel derecho, en Configuración de copia de **seguridad, selecciona Configuración** de copia de **seguridad de la instancia** .
2. Seleccione **Habilitar copias de seguridad de instancias** . Esta opción está habilitada de forma predeterminada.
3. Seleccione **Proteger archivo con contraseña** para cifrar el archivo de respaldo. El cifrado del archivo de respaldo garantiza que la información confidencial del archivo de respaldo esté segura.
4. En el campo **Número de archivos de copia de seguridad que retener**, especifique el número de archivos de copia de seguridad que se deben conservar en NetScaler ADM. Puede conservar hasta 50 archivos de respaldo.

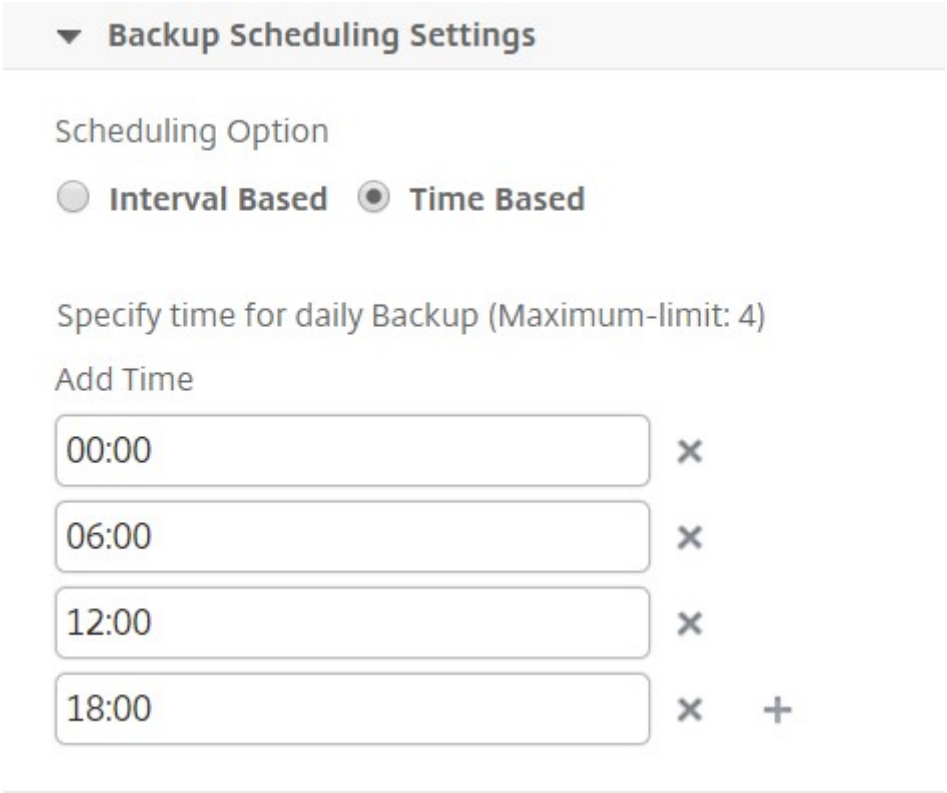
   > **Nota**
   >
   > Cada archivo de respaldo requiere algún requisito de almacenamiento. Citrix recomienda almacenar una cantidad óptima de archivos de respaldo en Citrix ADM según sus necesi-

> dades.



5. Establezca la configuración de programación de copias de seguridad. Elija una de las siguientes opciones:

   - **Basado en intervalos**: Se crea un archivo de copia de seguridad en NetScaler ADM una vez transcurrido el intervalo especificado. El intervalo de copia de seguridad predeterminado es de 12 horas.
   - **Basado**en el tiempo : puede especificar la hora en formato «horas:minutos» a la que debe realizarse la copia de seguridad. Citrix ADM permite realizar hasta cuatro copias de seguridad diarias en las instancias.

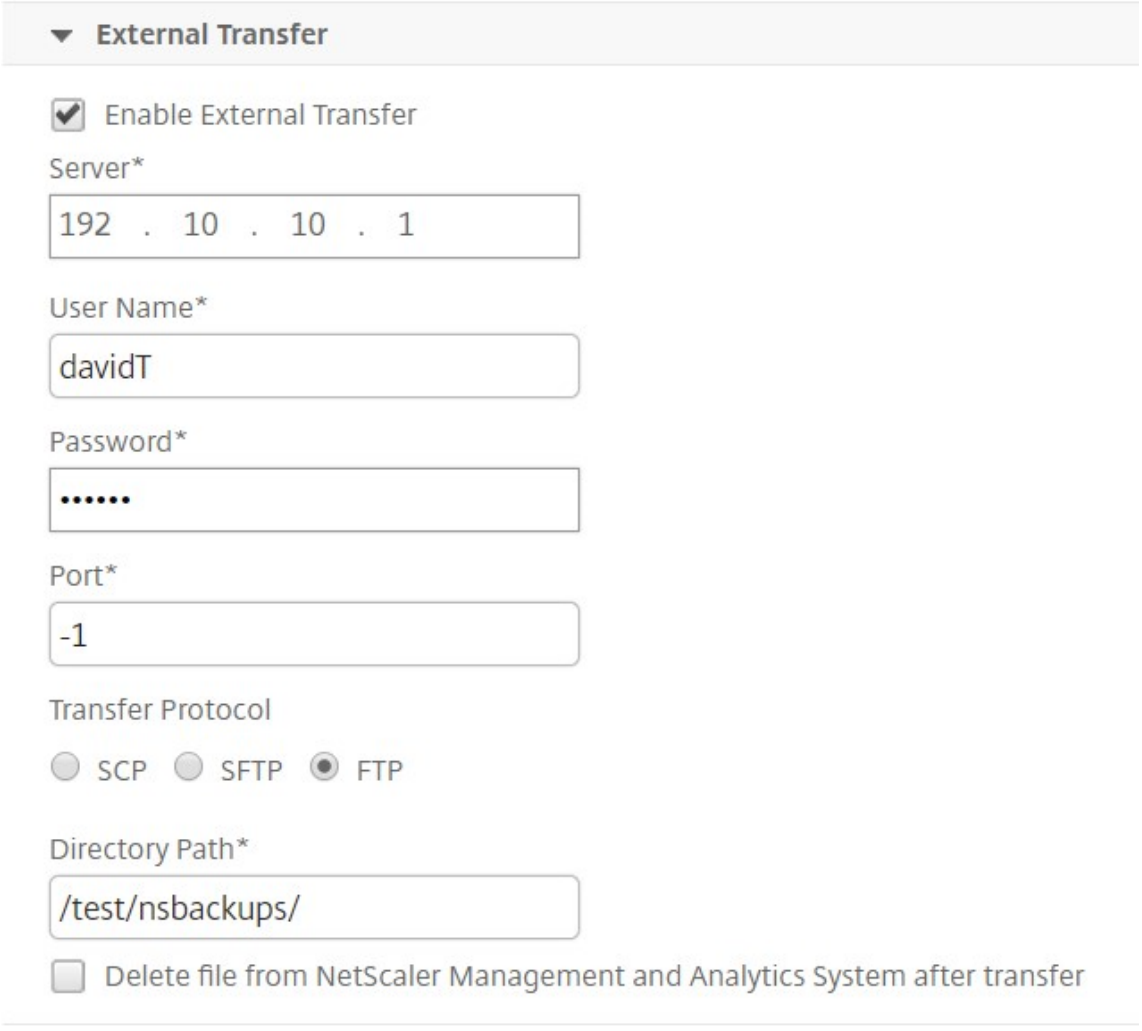


> **Nota**
>
> Omita la sección **Configuración de Citrix ADC**; esta configuración no se aplica a las instancias de SD-WAN WANOP de Citrix.

6. Seleccione **Habilitar transferencia externa para transferir** los archivos de respaldo de la instancia a una ubicación externa. Introduzca los valores de los campos siguientes:

   - **Servidor**: dirección IP del servidor externo.
   - **Nombre**de usuario: nombre de usuario del servidor externo
   - **Contraseña**: contraseña del servidor externo.
   - **Puerto**: número de puerto utilizado para comunicarse con el servidor externo.
   - **Protocolo**de transferencia : protocolo que se utilizará para transferir los archivos de copia de seguridad de Citrix ADM al servidor externo.

   También puede eliminar el archivo de copia de seguridad de Citrix ADM después de transferirlo al servidor externo.



7. Haga clic en **Aceptar**.

> **Nota**
>
> Citrix ADM se envía una captura de SNMP o una notificación de Syslog cuando se produce un error de respaldo en alguna de las instancias de SD-WAN WANOP de Citrix seleccionadas.

Creación de una copia de seguridad de una instancia de Citrix SD-WAN WANOP

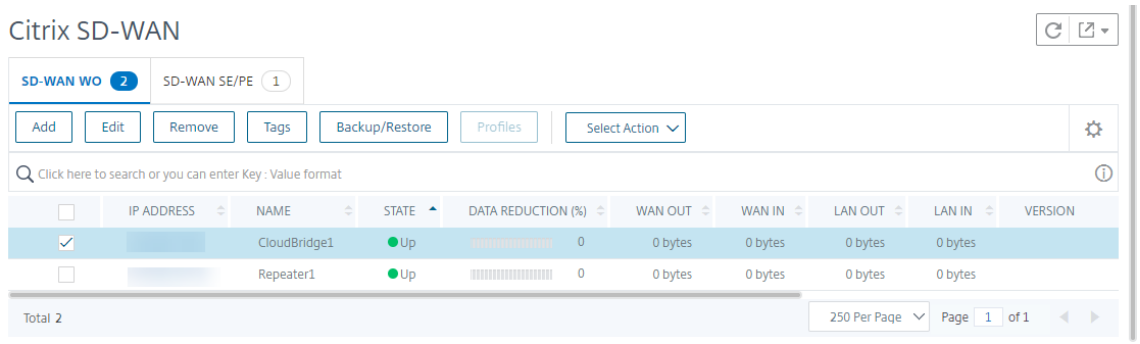
El procedimiento para crear una copia de seguridad para la instancia SD-WAN WANOP de Citrix se aplica a un usuario administrador que utilice el perfil nsroot predeterminado.

Para obtener información sobre cómo un usuario personalizado puede realizar una copia de seguridad de una instancia de Citrix SD-WAN WANOP, consulte la sección Creación de una copia de seguridad de una instancia WANOP de Citrix SD-WAN para usuarios personalizados de este tema.

Asegúrese de que se agregue una instancia de Citrix SD-WAN WANOP a NetScaler ADM para obtener más información, consulte Agregar instancias a NetScaler ADM.

Para crear una copia de seguridad para la instancia de Citrix SD-WAN WANOP:

1. En Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix SD-WAN** .
2. En **SD-WAN WO**, seleccione la instancia de Citrix SD-WAN WANOP de la que quiere realizar una copia de seguridad y, a continuación, haga clic en**Copia de seguridad/restauración**.



3. En la página **Archivos** de copia de seguridad , haga clic en **Realizar copia de** seguridad .
4. Cifre el archivo de respaldo mediante cualquiera de las siguientes opciones:
   - Seleccione **Archivo protegido con contraseña** e introduzca una contraseña para cifrar los archivos de respaldo.

- Selecciona **Usar contraseña global** para usar la contraseña global que especificaste en la página de configuración de la copia de seguridad de la instancia.

5. Haga clic en **Crear copia de seguridad**

Creación de una copia de seguridad de una instancia de Citrix SD-WAN WANOP para usuarios personalizados

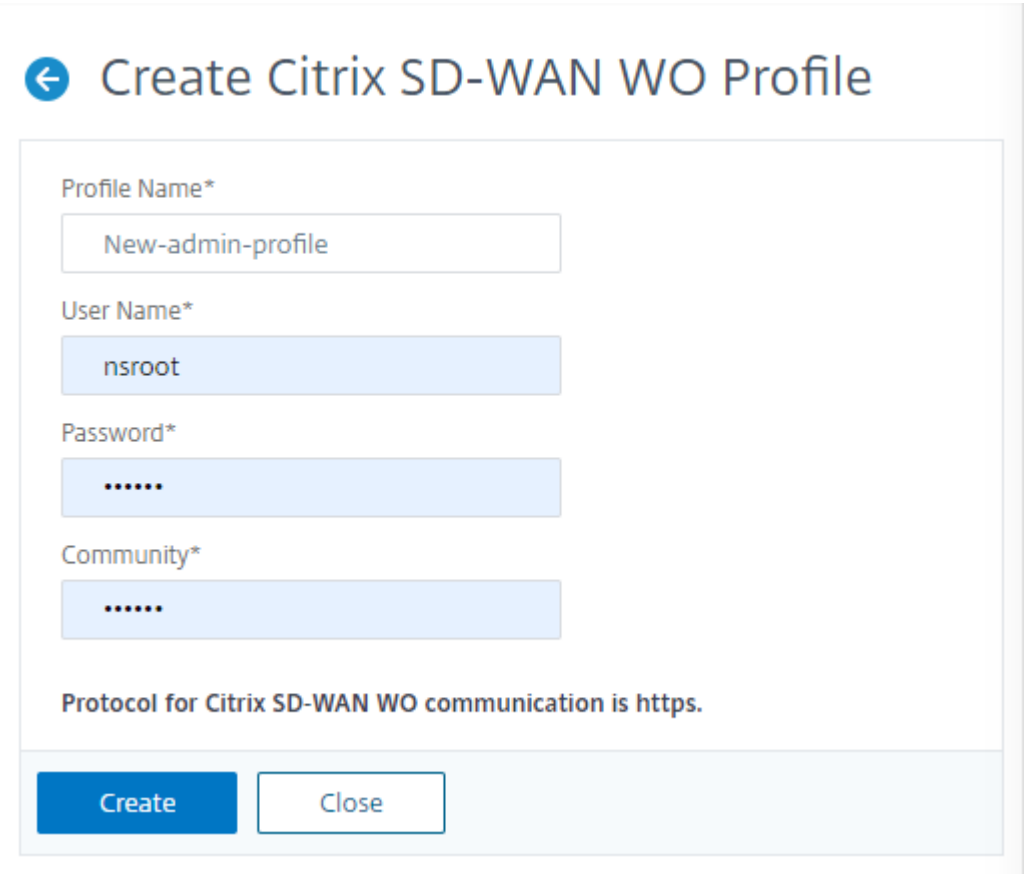
Si ha creado un usuario personalizado con privilegios de administrador en la instancia WANOP de Citrix SD-WAN, utilice el siguiente procedimiento para agregar una instancia y realizar una copia de seguridad de esa instancia mediante Citrix ADM.

La operación de respaldo por parte de usuarios personalizados no es compatible con las plataformas SD-WAN WANOP 400/800/1000WS/2000/2000WS/3000/4000/5000/4100/5100.

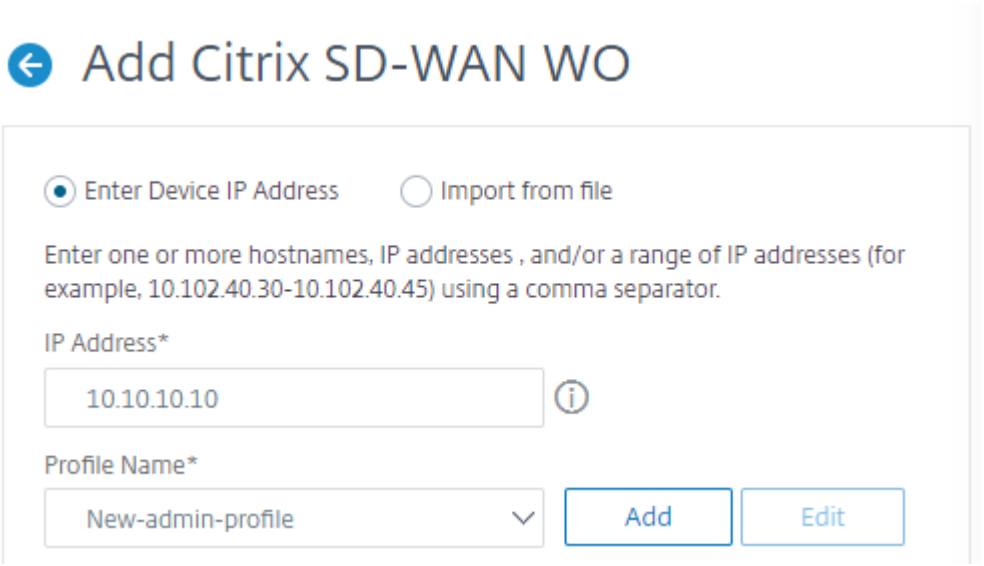
> **Nota**
>
> Citrix recomienda utilizar el perfil nsroot predeterminado al crear copias de seguridad de las plataformas avanzadas Citrix SD-WAN en Citrix ADM.

Para agregar una instancia de Citrix SD-WAN WANOP y realizar una copia de seguridad para un usuario personalizado:

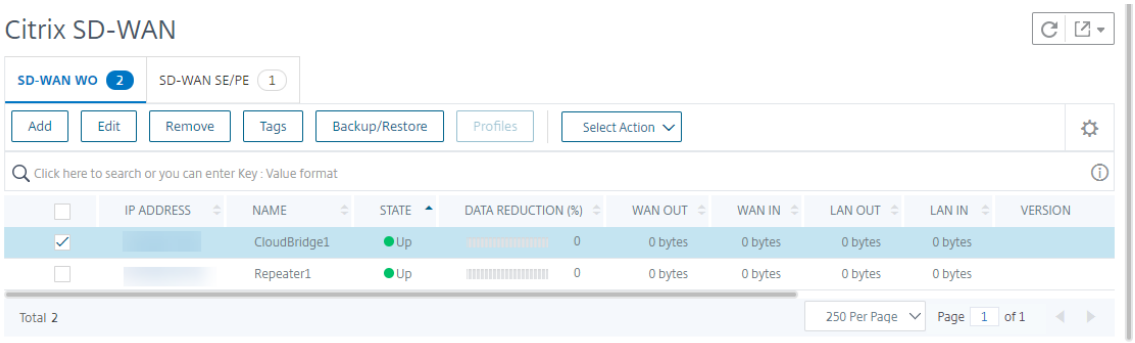
1. En Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix SD-WAN** y seleccione **SD WAN WO**.
2. Haga clic en **Agregar**.
3. En el campo **Dirección IP** , introduzca la dirección IP de la instancia de Citrix SD-WAN WANOP.
4. Haga clic en **Agregar** junto al campo **Nombre del perfil** para crear un perfil nuevo. Aparece la ventana **Crear perfil WO de Citrix SD-WAN** .



5. En el **campo Nombre del perfil** , introduzca un nombre para el perfil.
6. En el campo **Nombre de usuario** , introduzca el nombre de usuario del usuario personalizado que creó en la instancia de SD-WAN WANOP.
7. En el **campo Contraseña** , introduzca la contraseña que estableció para el usuario personalizado en la instancia de SD-WAN WANOP.
8. En el campo **Comunidad** , introduzca la cadena de comunicación SNMP configurada en el dispositivo SD-WAN WANOP. (por ejemplo: pública)
9. Haga clic en **Crear**.
10. En el campo **Nombre del perfil** , seleccione el perfil recién creado **y** haga clic en Aceptar .



11. Vaya a **Redes** > **Instancias** > **Citrix SD-WAN** .
12. En **SD-WAN WO**, seleccione la instancia de Citrix SD-WAN WANOP que acaba de agregar y, a continuación, haga clic en**Copia de seguridad/restauración**.



13. En la página **Archivos** de copia de seguridad , haga clic en **Realizar copia de** seguridad .
14. Cifre el archivo de respaldo mediante cualquiera de las siguientes opciones:

    - Seleccione **Archivo protegido con contraseña** e introduzca una contraseña para cifrar los archivos de respaldo.
    - Selecciona **Usar contraseña global** para usar la contraseña global que especificaste en la página de configuración de la copia de seguridad de la instancia.

Nota

Puede descargar el archivo de respaldo cifrado a su máquina local, pero no puede ver su contenido. Solo Citrix ADM puede usar estos archivos de respaldo con fines de restauración. Al restaurar la copia de seguridad cifrada, se solicitará la contraseña.

15. Haz clic en **Crear copia** de seguridad .

Importante

```
1. Para un dispositivo Citrix SD-WAN WANOP VPX, Citrix ADM solo hace copias de seguridad del archivo de configuración del broker CB.
```

a) Para una plataforma Citrix SD-WAN WANOP avanzada, Citrix ADM hace copias de seguridad de lo siguiente: ·

- Archivo de configuración de CB Broker
- Archivo de configuración NTP
- DNS
- Archivo de configuración SNMPD
- Archivo de configuración de Syslog
- Certificado SSL, claves y políticas
- Archivo de base de datos SVM
- Componentes (en formato XML)
- Recursos (en formato XML)

Los archivos de los que se ha hecho una copia de seguridad en las carpetas correspondientes se enumeran en la tabla siguiente. Tenga en cuenta que si el nombre de una carpeta va seguido de un «*», se realizará una copia de seguridad de todos los archivos de esa carpeta.

Directorio	Subdirectorio o archivos
/br_corredor/	CB-6BBB660a/ ws.conf
/etc/	resolv.conf
/mps/	mps_devices.xml
/mpsconfig/	ssl/*, ntp.conf, snmpd.conf, syslog.conf
/mpsdb/	mpsdb_dump.sql
/ns/	NS-6CBB660A/*

/var/	mps/policy/, *mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/*

Administrar instancias de HAProxy

January 30, 2024

HAProxy es un balanceador de cargas de código abierto que puede balancear la carga de cualquier servicio TCP o HTTP. Para obtener más información sobre HAProxy, consulte http://www.haproxy.org/.

Citrix Application Delivery Management (Citrix ADM) admite la versión 1.4.24 o posterior de HAProxy. Cuando agrega un host en el que ha aprovisionado las instancias de HAProxy a Citrix ADM, Citrix ADM descubre las instancias de HAProxy en el host y le permite supervisarlas. Muestra los siguientes tipos de información sobre la configuración de HAProxy en las instancias:

- Interfaz: cómo se deben reenviar las solicitudes al back-end.
- Backend: el conjunto de servidores que reciben las solicitudes reenviadas.
- Servidores: Servidores entre los que la carga HAProxy equilibra el tráfico.

Para obtener más información, consulte http://www.haproxy.org/download/1.7/doc/configuration.txt.

Además, NetScaler ADM proporciona un panel de aplicaciones HAProxy en el que puede supervisar las interfaces en tiempo real. Para obtener más información, consultePanel de control de aplicaciones HAProxy.

Agregar instancias de HAProxy a NetScaler ADM

January 30, 2024

En Citrix Application Delivery Management (Citrix ADM), debe agregar manualmente los detalles del host en el que ha aprovisionado la instancia de HAProxy. Después de agregar esos detalles, NetScaler ADM descubre automáticamente las instancias de HAProxy aprovisionadas en el host y las agrega al Inventario de NetScaler ADM. También descubre todas las interfaces, los backends y los servidores configurados en las instancias de HAProxy y trata las interfaces como aplicaciones descubiertas.

Requisitos previos

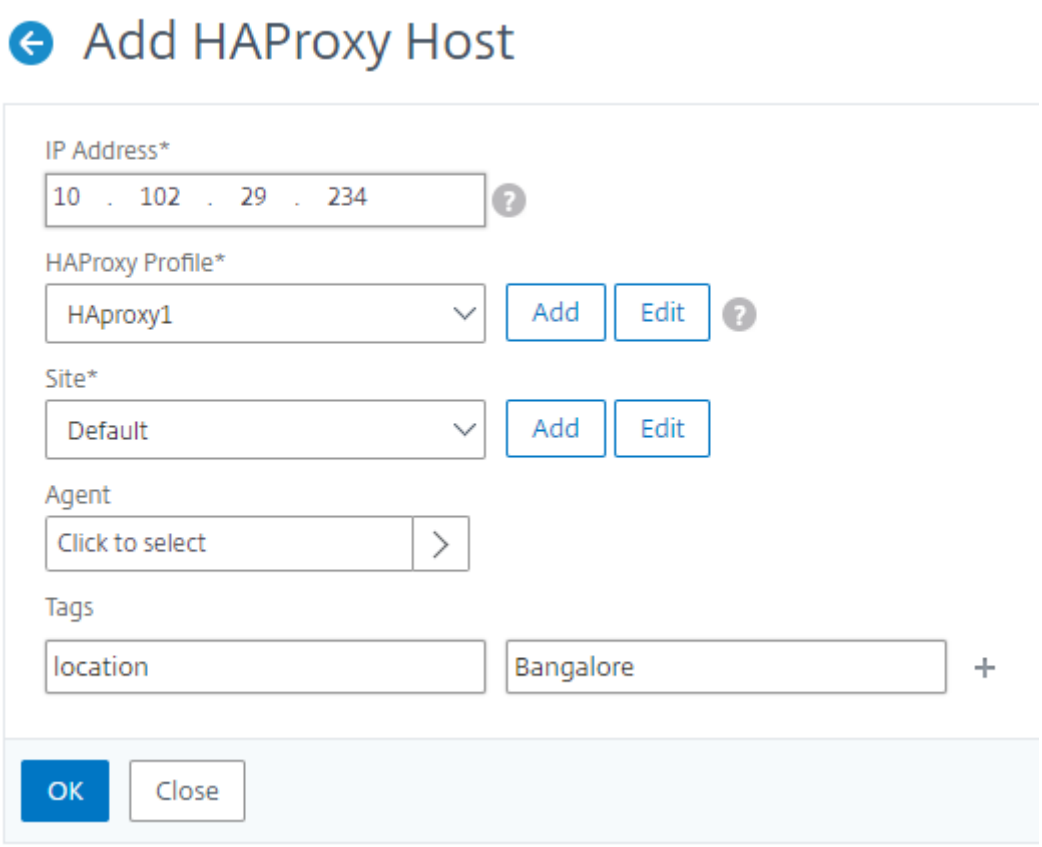
Asegúrese de lo siguiente:

- Implementó una instancia de HAProxy en un host de su implementación. Para obtener más información, consulte http://www.haproxy.org/#docs.
- Identificó y decidió la cantidad de interfaces para las que desea ver las estadísticas de la aplicación en el panel de aplicaciones de HAProxy. De forma predeterminada, el panel de control de aplicaciones HAProxy muestra las estadísticas de 30 aplicaciones detectadas. Para obtener más información sobre el panel de aplicaciones HAProxy, consulte Panel de control de aplicaciones HAProxy Si desea ver las estadísticas de más de 30 aplicaciones descubiertas, debe comprar una licencia independiente. Para obtener más información, consulte Licencias de terceros.

> **Importante**
>
> Citrix ADM requiere acceso al host para detectar las instancias de HAProxy que contiene. Puede proporcionar acceso a Citrix ADM proporcionando el par de claves SSH del host o mediante la contraseña del host. Si desea proporcionar acceso mediante el par de claves SSH, asegúrese de generar el par de claves privadas y públicas de SSH en el host y de agregar la clave pública a las claves autorizadas del host. Además, la cuenta de usuario SSH debe tener permisos de superusuario.

Para agregar una instancia de HAProxy a NetScaler ADM:

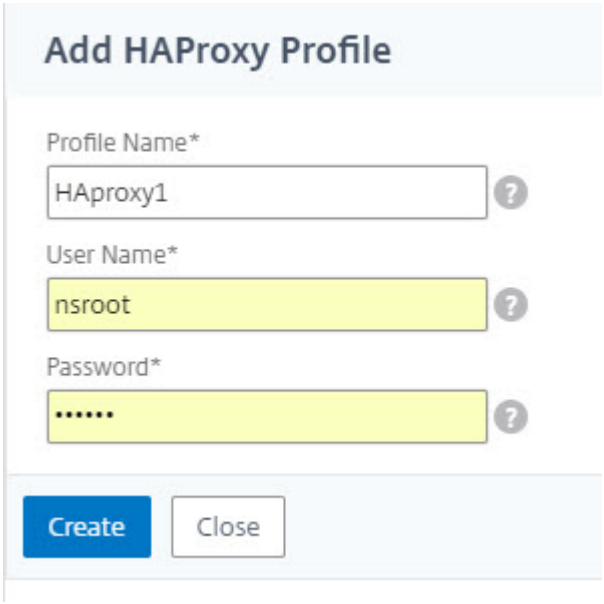
1. En un explorador web, escriba la dirección IP de **Citrix Application Delivery Management** (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de administrador . Las credenciales de administrador predeterminadas son «nsroot» y «nsroot».
3. Navegue hasta **Redes** > **Instancias** . En **Instancias** , seleccione **HAProxy** y haga clic en **Agregar** .
4. En el cuadro de diálogo **Agregar host HAProxy**, haga lo siguiente:



1. En el campo **Dirección IP**, introduzca la dirección IP del host en el que ha aprovisionado las instancias de HAProxy.

    a) En el menú **Perfil de HAProxy** , seleccione un perfil de HAProxy existente o cree y seleccione un nuevo perfil de HAProxy. Para crear un perfil de HAProxy, haga clic en **Agregar** .

        i. En el cuadro de diálogo **Agregar perfil de HAProxy**, haga lo siguiente:



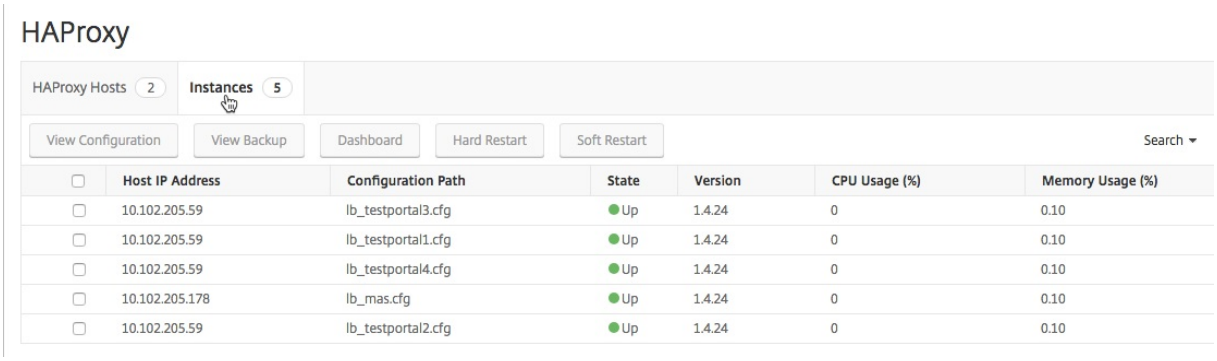
i. En el campo **Nombre del perfil**, introduzca el nombre del perfil.

ii. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de usuario del host.

iii. Haga clic en **Crear**.

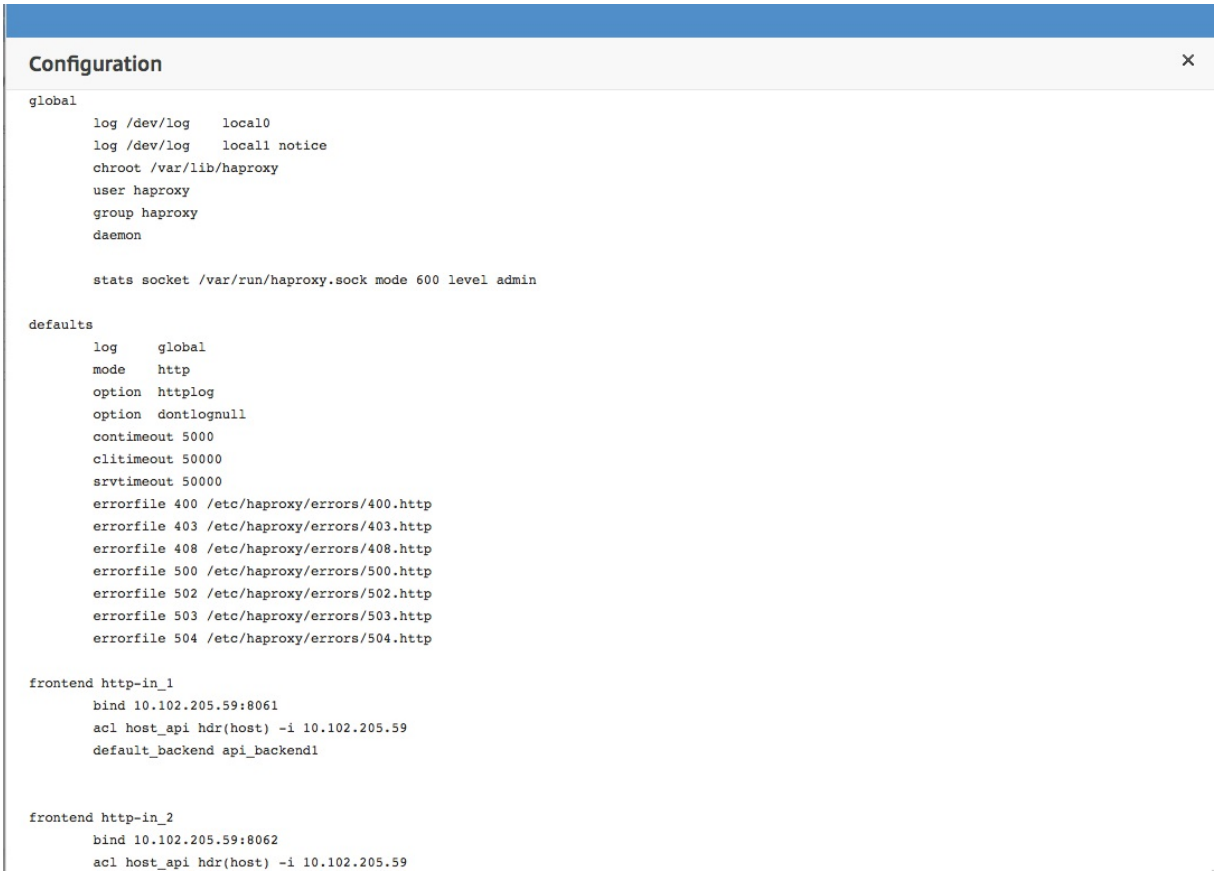
2. En el menú **Sitio** , seleccione un sitio de HAProxy. Para crear y agregar un sitio nuevo al menú, haga clic en **Agregar** .
3. En el menú **Agente** , seleccione un agente.
4. En los campos Etiquetas, introduzca los valores de forma adecuada.
5. Haga clic en **Aceptar**.

NetScaler ADM descubre las instancias de HAProxy aprovisionadas en el host y puede ver todas las instancias de HAProxy en la ficha **Instancias**.



Visualización de la configuración de una instancia HAProxy

Para ver la configuración de una instancia HAProxy en NetScaler ADM, vaya a **Redes** > **Instancias** > **HAProxy** y, en la ficha **Instancias**, seleccione la instancia HAProxy y haga clic en **Ver configuración**.



Panel de aplicación HAProxy

January 30, 2024

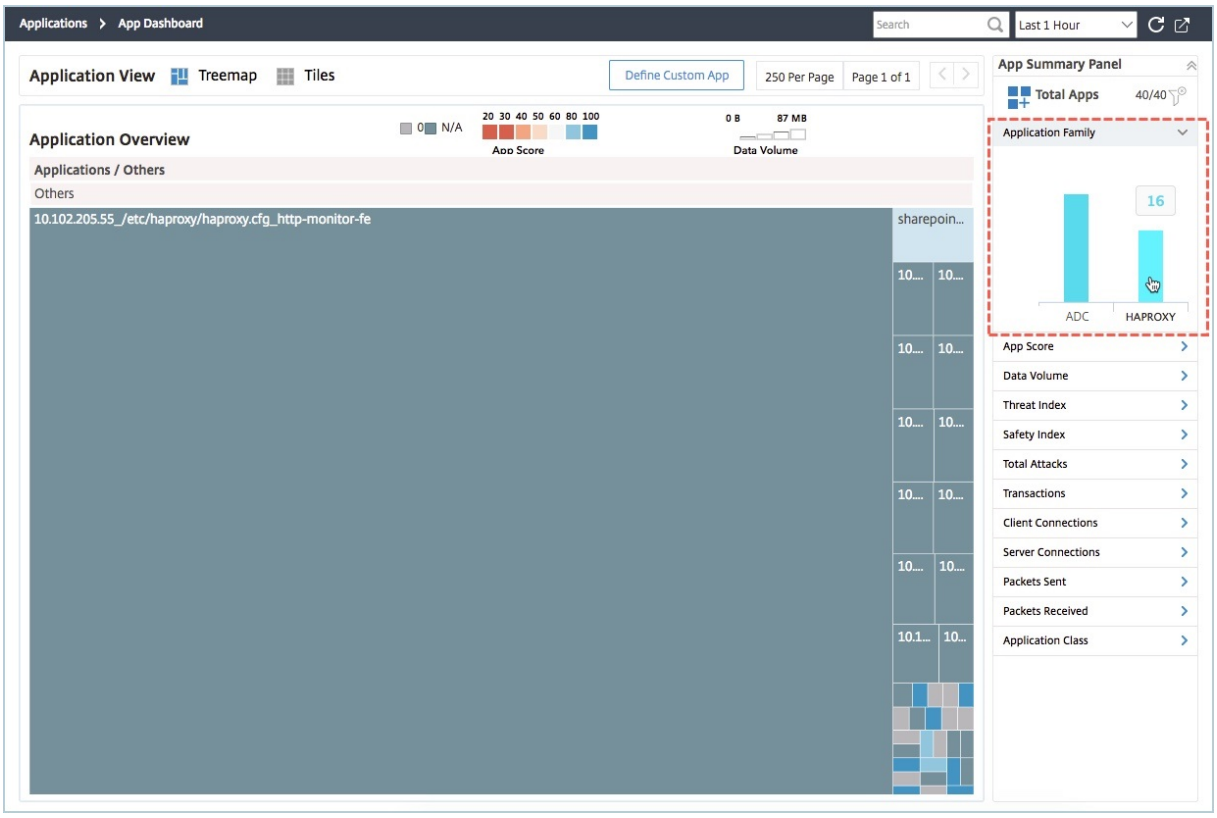
El panel de aplicaciones proporciona estadísticas en tiempo real de todas las interfaces de HAProxy supervisadas por Citrix Application Delivery Management (Citrix ADM). Enumera las interfaces como aplicaciones discretas y proporciona información sobre las transacciones, el rendimiento y las sesiones sobre las aplicaciones.

> **Importante**
>
> Asegúrese de habilitar las **estadísticas** en el archivo de configuración de la instancia de HAProxy.

> Para habilitar las **estadísticas** , edite el archivo de configuración de HAProxy y, después de la sección de valores predeterminados, añada una entrada similar a la del siguiente ejemplo:

```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
<!--NeedCopy-->
```

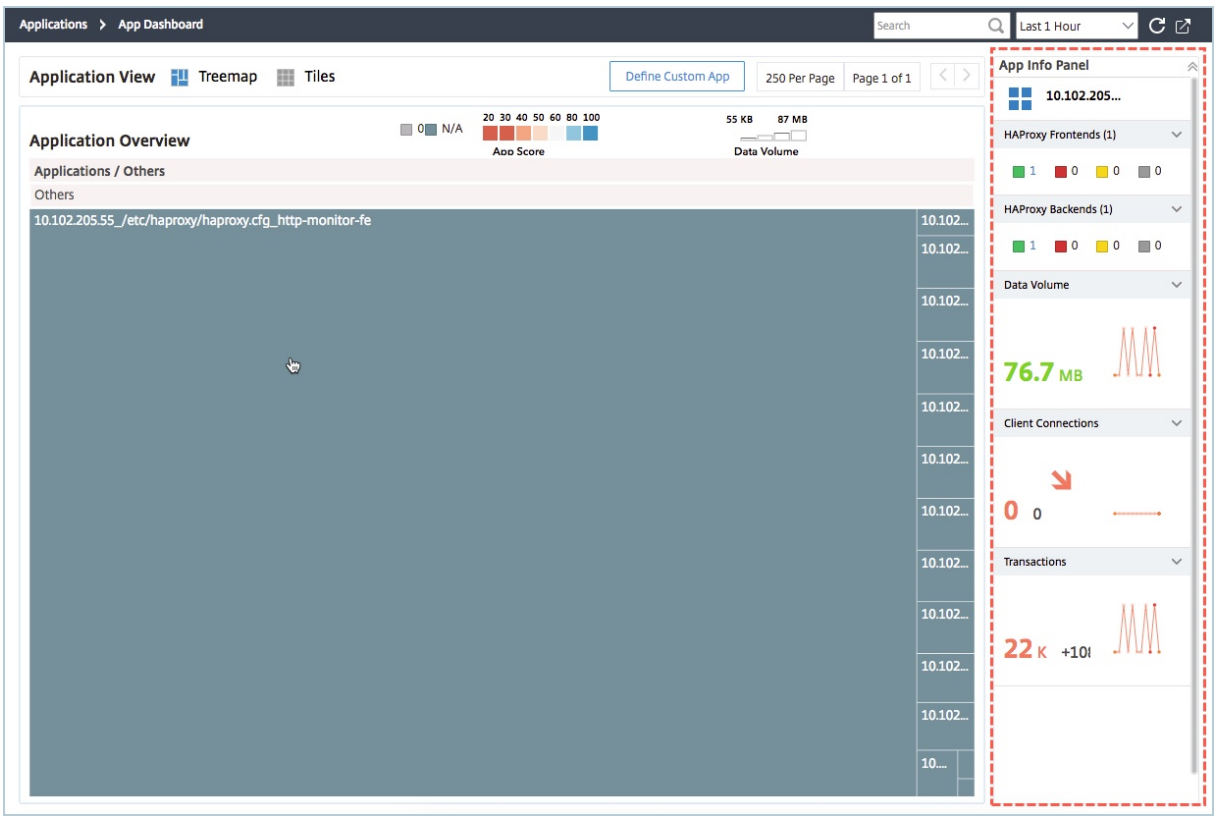
Para acceder a la aplicación HAProxy en el panel de aplicaciones de Citrix ADM, después de agregar las instancias de HAProxy a Citrix ADM, vaya a **Aplicaciones** > **Panel**. Puede filtrar el panel para que muestre solo la aplicación HAProxy. Para filtrar el panel, seleccione **HAPROXY** que se muestra en la sección **Familia de aplicaciones del panel de información resumida de la aplicación**.



Ver métricas clave de la aplicación HAProxy

El panel Información de la aplicación se encuentra en el primer nivel cuando se profundiza en una aplicación HAProxy. Muestra las métricas y componentes clave de la aplicación, junto con su estado. Por ejemplo, para cualquier aplicación HAProxy seleccionada, el panel Información de la aplicación

muestra la cantidad total de interfaces de HAProxy, la cantidad total de backends de HAProxy, el volumen de datos, la tendencia de las conexiones de los clientes y las transacciones. Para ver las métricas clave de la aplicación HAProxy, haga clic en el icono de la aplicación HAProxy en el panel de control de la aplicación. El panel Información de la aplicación reemplaza al panel Resumen de la aplicación.

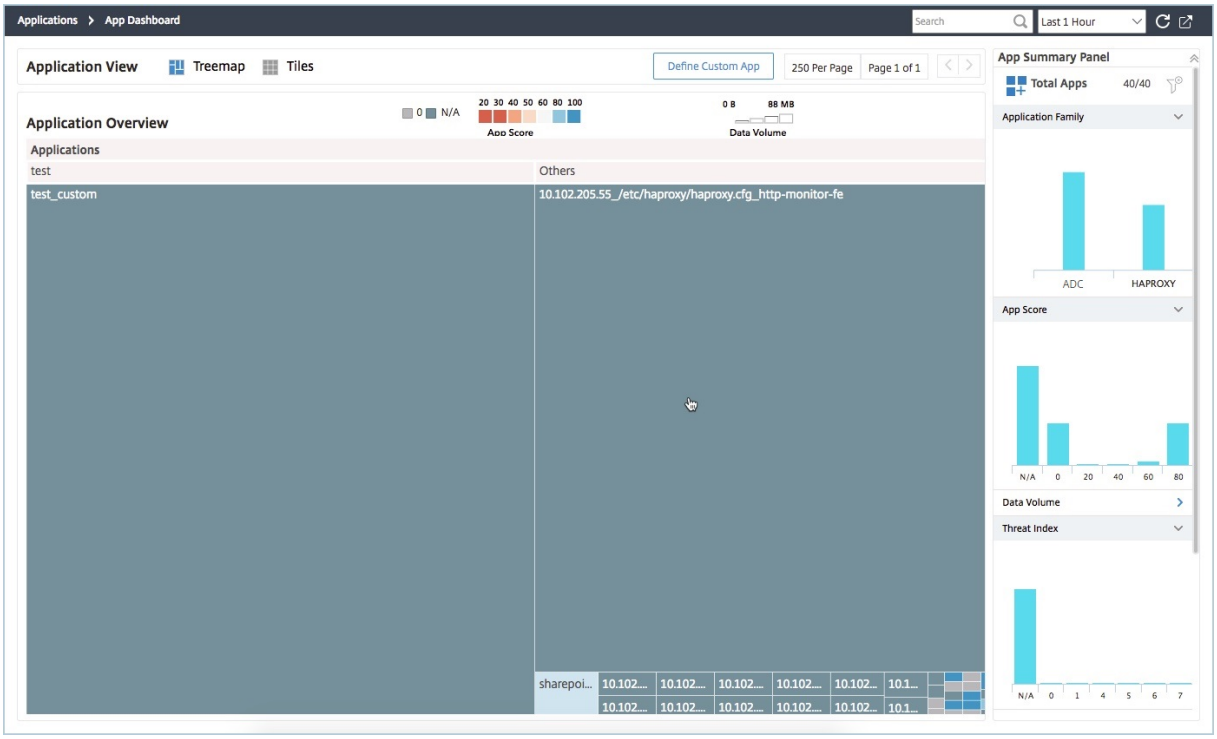


Ver el rendimiento en tiempo real de la aplicación HAProxy

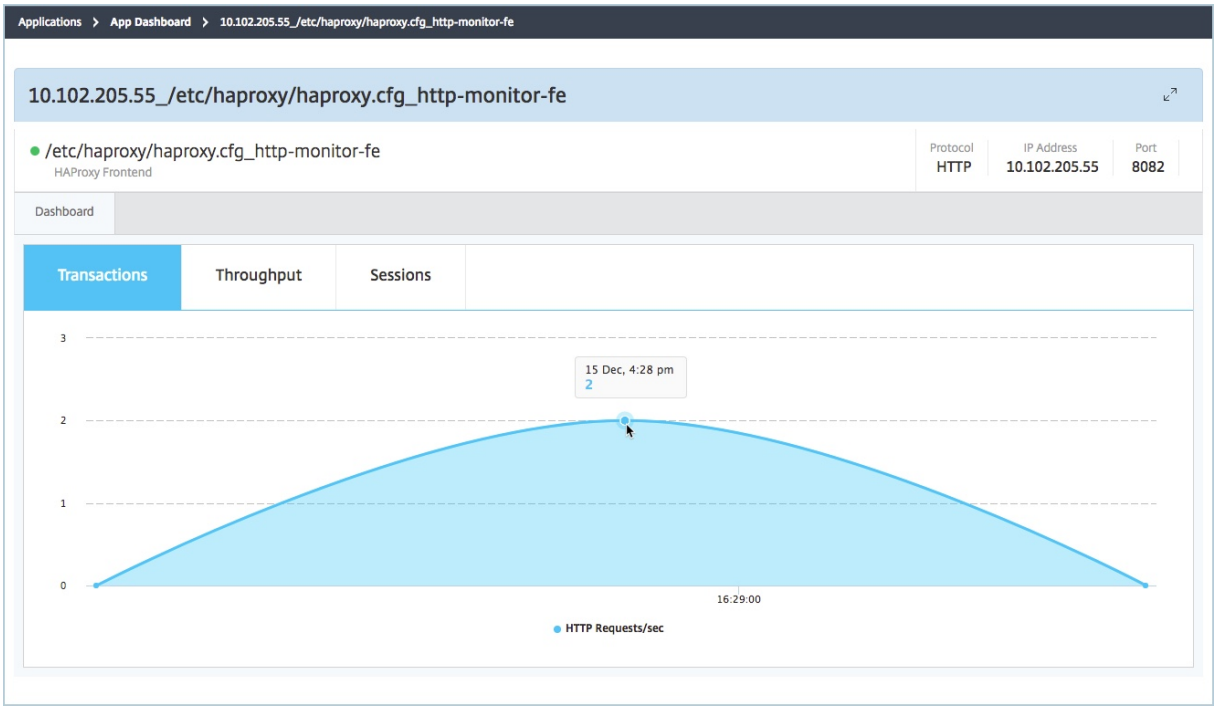
Citrix ADM le permite ver el rendimiento en tiempo real de sus aplicaciones HAProxy. Proporciona los siguientes detalles en tiempo real de la aplicación HAProxy seleccionada:

- **Transacciones.** Transacciones realizadas por la aplicación.
- **Rendimiento.** Rendimiento de la aplicación.
- **Sesiones.** Número de sesiones establecido por la aplicación.

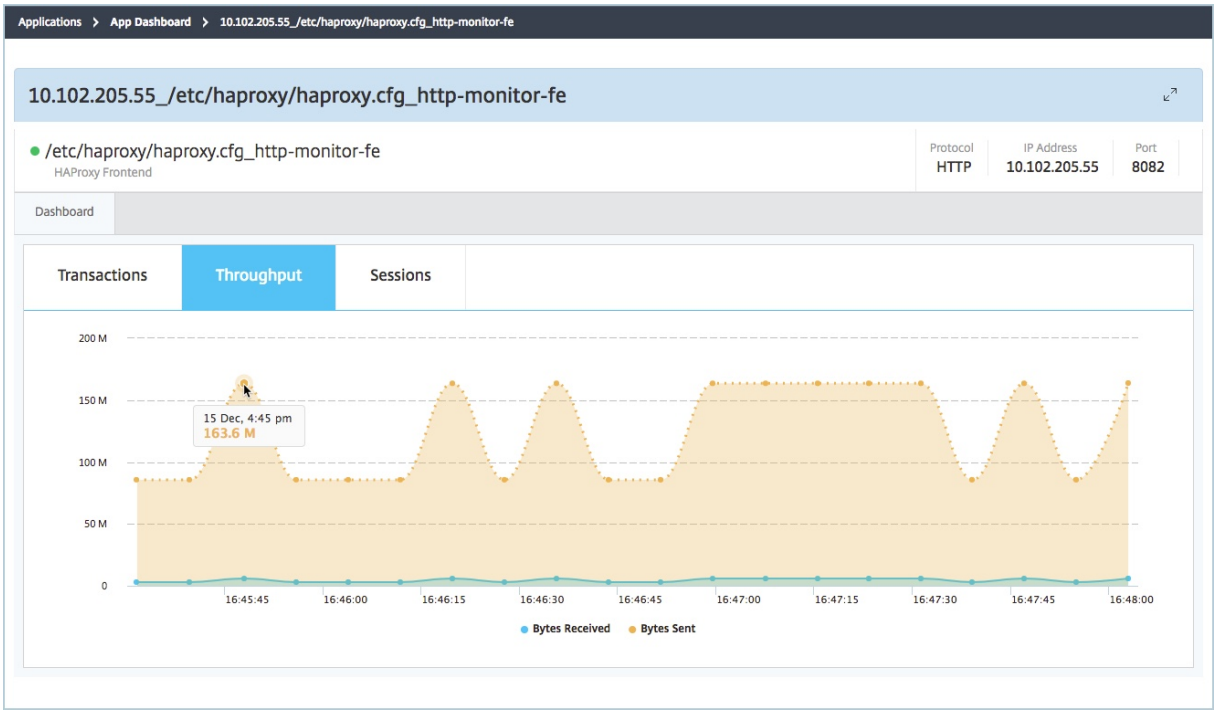
Para ver el rendimiento en tiempo real de la aplicación HAProxy, en el **Panel de aplicaciones**, haga doble clic en el icono de la aplicación HAProxy.



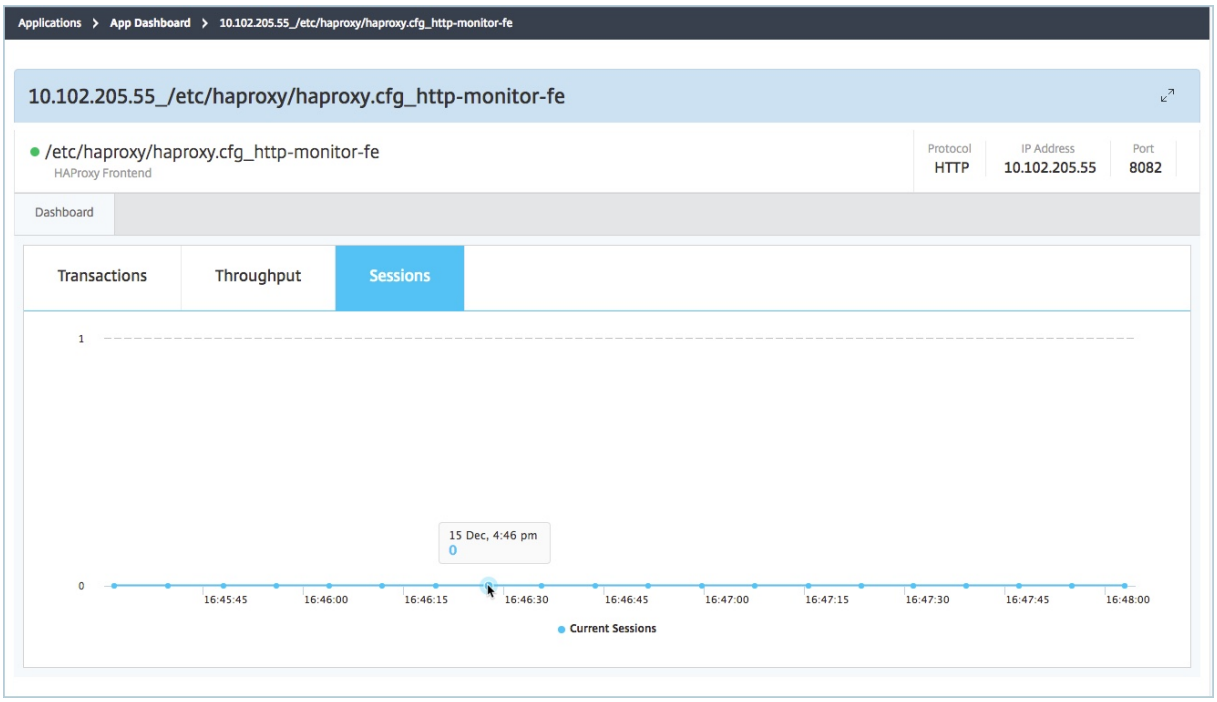
De forma predeterminada, la pestaña **Transacciones** está seleccionada y se muestran las transacciones en tiempo real realizadas por la aplicación.



Para ver el rendimiento en tiempo real de la aplicación, haga clic en la ficha **Rendimiento**.



Puede hacer clic en la ficha **Sesiones** para ver el número de sesiones establecidas por la aplicación en tiempo real.

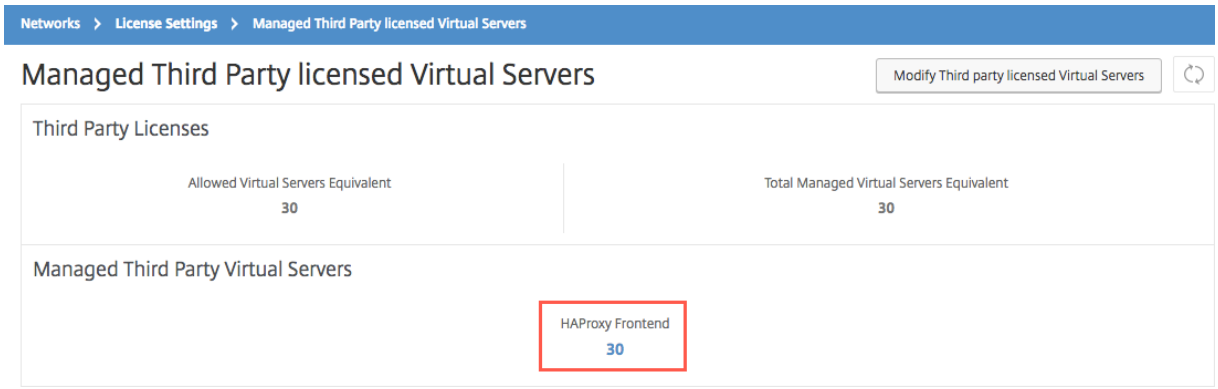


Licencias de terceros

January 30, 2024

Después de agregar los hosts a NetScaler Application Delivery Management (NetScaler ADM), NetScaler ADM descubre automáticamente las instancias de HAProxy aprovisionadas en los hosts y las agrega a NetScaler ADM Inventory. También descubre todas las interfaces, los backends y los servidores configurados en las instancias de HAProxy y considera las interfaces como aplicaciones descubiertas.

Puede administrar y supervisar todas las aplicaciones detectadas, pero, de forma predeterminada, el panel de aplicaciones HAProxy muestra las estadísticas de la aplicación para 30 aplicaciones detectadas. Para obtener más información sobre el panel de aplicaciones HAProxy, consulte Panel de control de aplicaciones HAProxy Si desea ver las estadísticas de aplicaciones de más de 30 aplicaciones descubiertas, debe comprar una licencia independiente.



Las licencias para interfaces adicionales están disponibles en paquetes de 100 servidores virtuales. Puede obtener una licencia válida e instalarla mediante la GUI de NetScaler ADM.

Instalación de las licencias de terceros

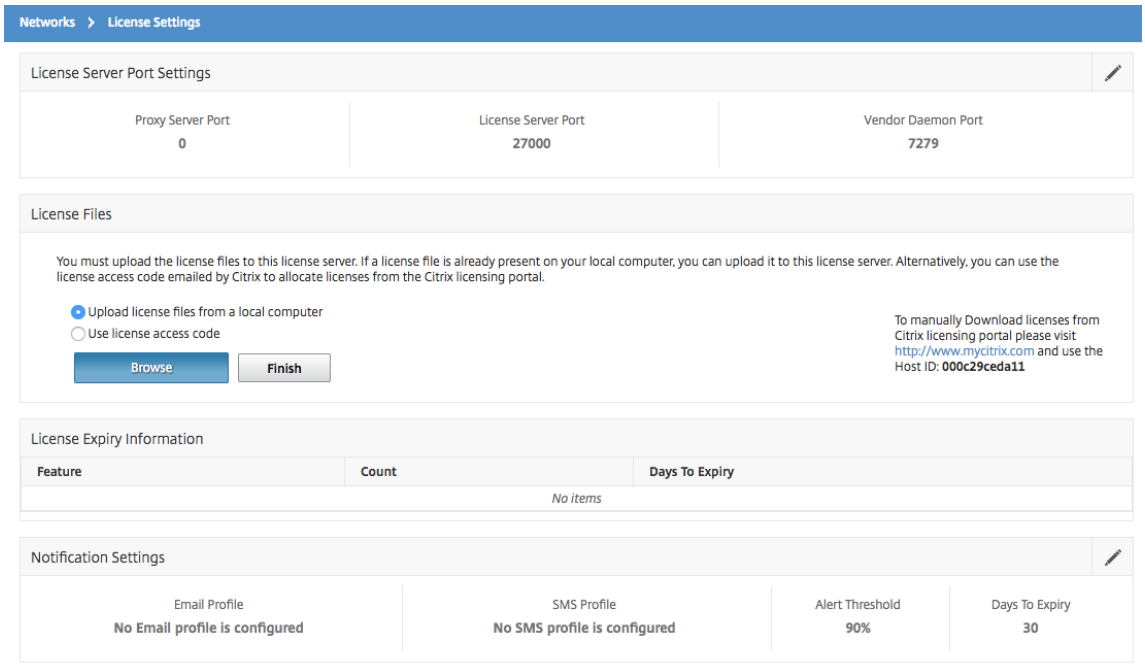
Puede instalar una licencia en NetScaler ADM para ver las estadísticas de aplicaciones de más de 30 aplicaciones descubiertas.

Para instalar una licencia:

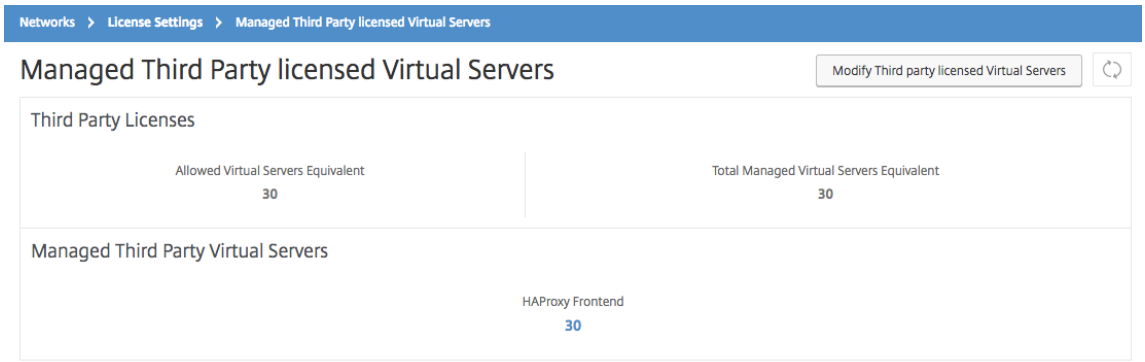
1. En un explorador web, escriba la dirección IP de **NetScaler Management and Analytics System** (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Licencias** .
4. En la sección **Archivos de licencias**, seleccione una de las siguientes opciones:

- **Cargue los archivos de licencia desde un equipo local.** Si ya hay una licencia en su equipo local, haga clic en Examinar y seleccione el archivo de licencia (.lic) que quiere usar para asignar sus licencias. Haga clic en **Finalizar**.
- **Utilice el código**de activación de la licencia : Citrix envía un correo electrónico a la LAC para solicitar la licencia que ha adquirido. Introduzca el LAC en el cuadro de texto y, a continuación, haga clic en **Obtener licencias** .

> **Nota**
>
> Si selecciona esta opción, el sistema de administración y análisis de NetScaler debe estar conectado a Internet o debe haber un servidor proxy disponible.



Puede verificar las licencias instaladas en su NetScaler ADM navegando a **Redes** > **Licencias > Licencias** de **terceros**.

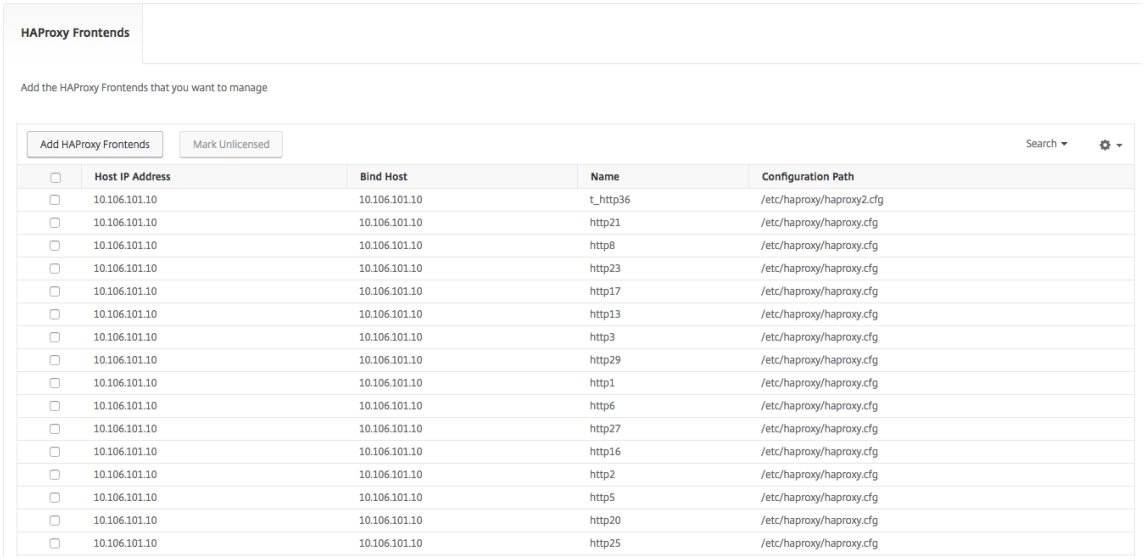


Administración de las licencias de terceros

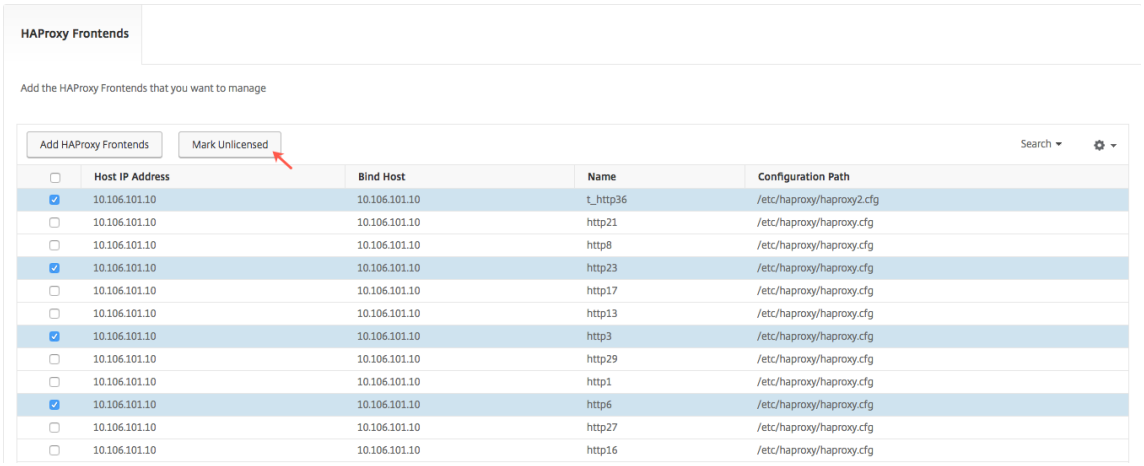
NetScaler ADM selecciona aleatoriamente las aplicaciones detectadas en las instancias de HAProxy y las otorga automáticamente licencias. Si desea cambiar las aplicaciones detectadas seleccionadas, debe anular manualmente la licencia de las aplicaciones descubiertas con licencia y, a continuación, asignar las licencias a las aplicaciones descubiertas para las que desea licenciar.

Para administrar las licencias de terceros:

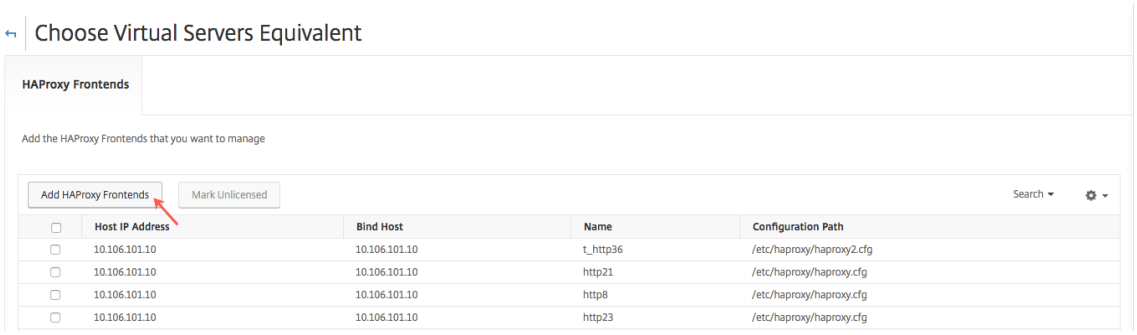
1. Vaya a **Redes** > **Licencias > Licencias** > **Licencias de terceros** y haga clic en **Modificar Servidores virtuales con licencia de terceros**. El panel muestra las interfaces administradas.



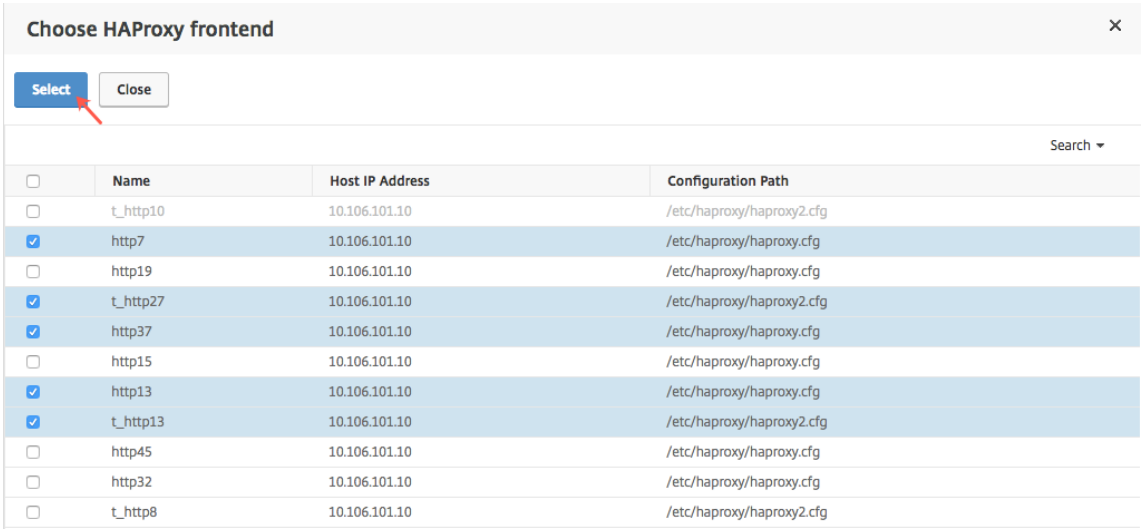
2. Seleccione las interfaces de la lista, **marque como no licenciadas** y haga clic en **Finalizar** para liberar las licencias.



3. Después de liberar las licencias, o si ya tiene licencias disponibles, haga clic en **Agregar frontend HAProxy**.



4. En el cuadro de diálogo **Elegir interfaz de HAProxy** , seleccione las interfaces sin licencia de la lista y haga clic en **Seleccionar**.



5. Haga clic en **Finalizar ahora**.

Control de acceso basado en roles para instancias de HAProxy

January 30, 2024

Citrix Application Delivery Management (Citrix ADM) utiliza un control de acceso detallado basado en roles (RBAC) para controlar el acceso a los objetos de configuración. Por ejemplo, puede crear usuarios y darles acceso a instancias concretas de HAProxy, y puede especificar permisos de ver/solo lectura para el panel de aplicación HAProxy. Para obtener más información, consulte Control de acceso basado en funciones en NetScaler ADM.

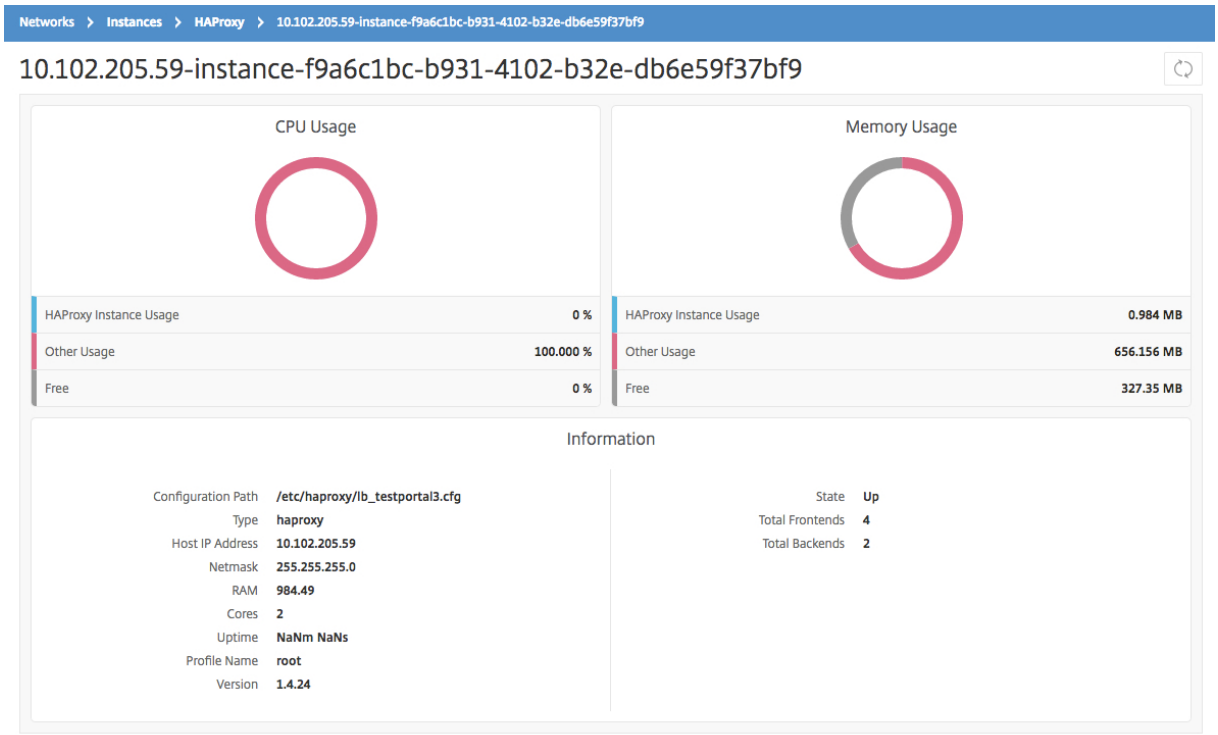
Supervisar instancias de HAProxy

January 30, 2024

El panel de HAProxy de Citrix Application Delivery Management (Citrix ADM) muestra gráficos que ayudan a realizar un seguimiento del uso de la CPU y la memoria de una instancia de HAProxy. El panel también muestra gráficos que indican lo siguiente:

- Porcentaje de CPU utilizada por la instancia de HAProxy en el host.
- Porcentaje de CPU utilizada por otras entidades del host.
- Porcentaje de CPU restante en el host.
- Porcentaje de memoria utilizada por la instancia HAProxy en el host.
- Porcentaje de memoria utilizada por otras entidades del host.
- Porcentaje de memoria restante en el host.

Para supervisar una instancia de HAProxy en Citrix ADM, vaya a la ficha **Redes** > **Instancias** > **HAProxyInstancias**, **seleccione**la instancia de HAProxy y haga clic en **Panel de control**.



Ver los detalles de las interfaces configuradas en instancias de HAProxy

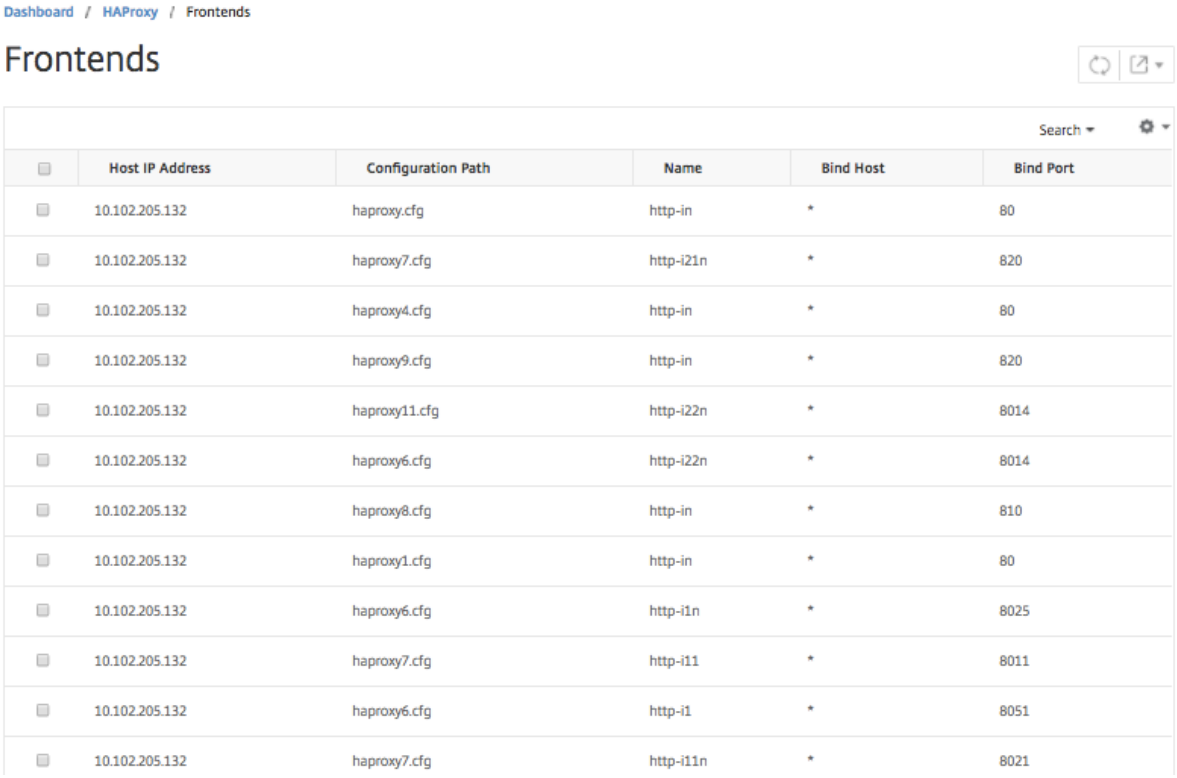
January 30, 2024

Citrix Application Delivery Management (Citrix ADM) informa de los siguientes detalles de la interfaz configurada en una instancia de HAProxy:

- **Dirección IP del host**. Dirección IP del host
- **Ruta**de configuración . Ruta de configuración absoluta de la instancia de HAProxy en el host.
- **Nombre**. Nombre de la interfaz que gestiona el tráfico entrante.
- **Enlazar host**. Dirección IP a la que está vinculada la interfaz.
- **Puerto de enlace**. Puerto al que está vinculada la interfaz.

Para ver la interfaz configurada en las instancias de HAProxy:

En NetScaler ADM, vaya a **Redes > Funciones de red > HAProxy > Frontend**.



Ver los detalles de los backends configurados en instancias de HAProxy

January 30, 2024

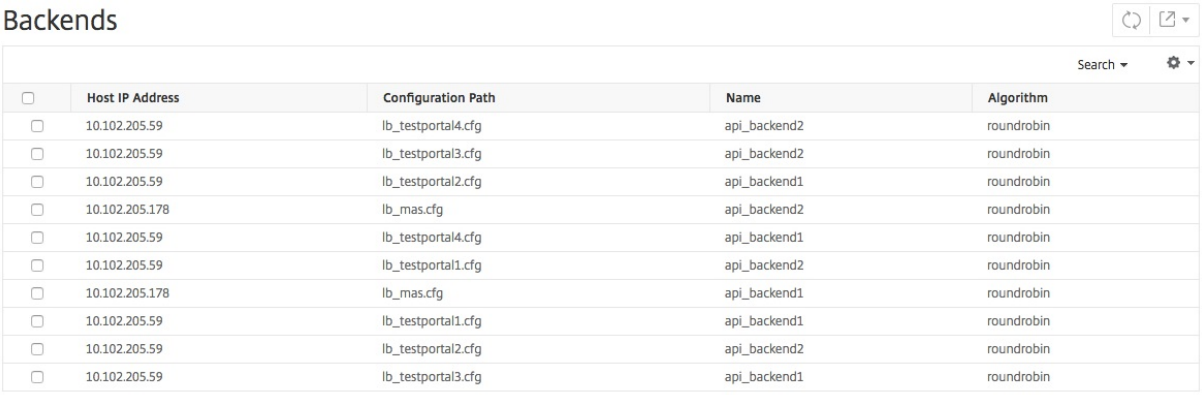
Citrix Application Delivery Management (Citrix ADM) informa de los siguientes detalles de una aplicación de fondo configurada en una instancia de HAProxy:

- **Dirección IP del host**. Dirección IP del host.
- **Ruta**de configuración . Ruta de instancia de HAProxy en el host.

- **Nombre**. Nombre del backend al que se reenvía el tráfico.
- **Algoritmo**. Algoritmo de equilibrio de carga utilizado para equilibrar el tráfico.

Para ver el backend configurado en las instancias de HAProxy:

En NetScaler ADM, vaya a **Redes** > **Funciones de red** > **HAProxy** > **Backends**.



Ver los detalles de los servidores configurados en instancias HAProxy

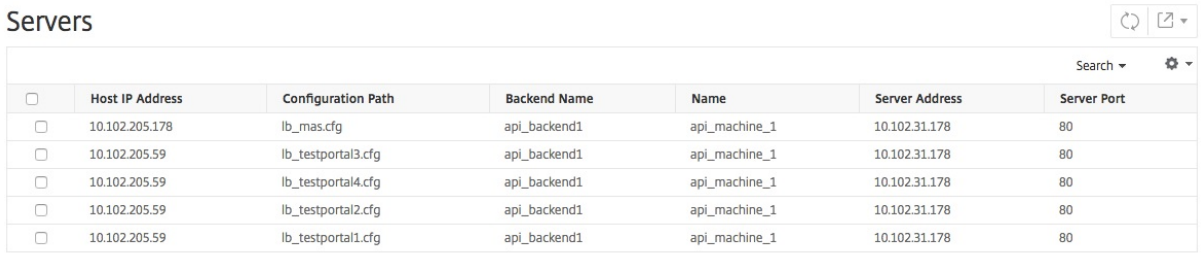
January 30, 2024

Citrix Application Delivery Management (Citrix ADM) informa de los siguientes detalles de los servidores configurados en una instancia de HAProxy:

- **Dirección IP del host**. Nombre del anfitrión.
- **Ruta**de configuración . Ruta absoluta del archivo de configuración de la instancia de HAProxy en el host.
- **Nombre del back-end**. Nombre del backend en la configuración de HAProxy.
- **Nombre**. Nombre del servidor en la configuración de HAProxy.
- **Dirección**del servidor . Dirección IP del servidor.
- **Puerto**de servidor . Puerto utilizado por el servidor.

Para ver los servidores configurados en las instancias de HAProxy:

En NetScaler ADM, vaya a **Redes** > **Funciones de red** > **HAProxy** > **Servidores**.

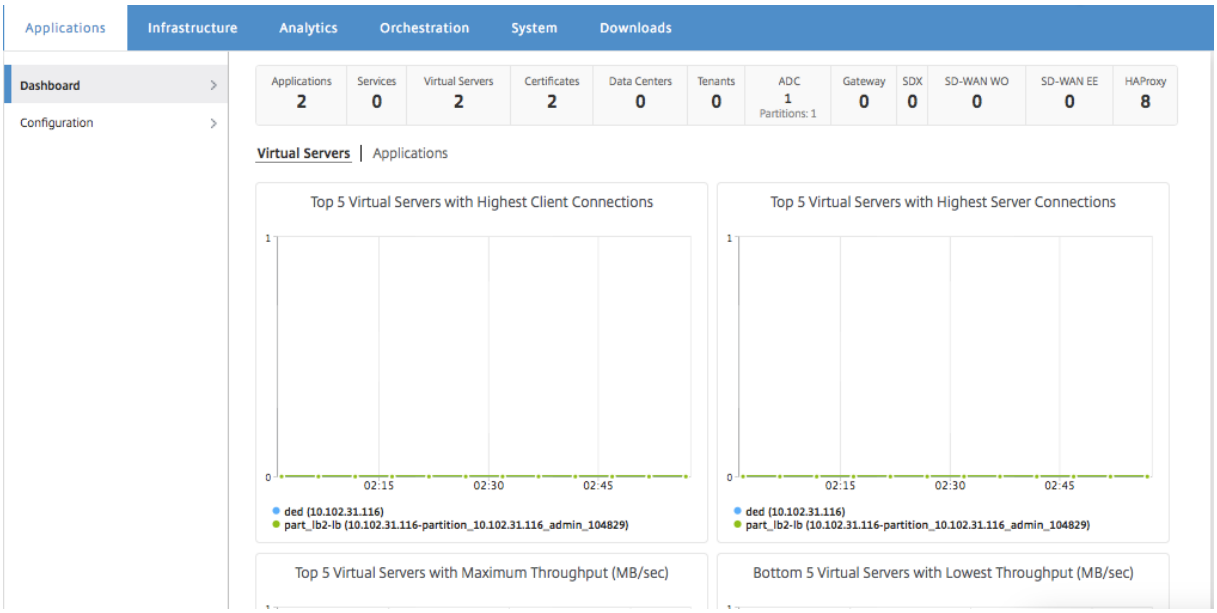


Ver las instancias HAProxy con el mayor número de frontend o servidores

January 30, 2024

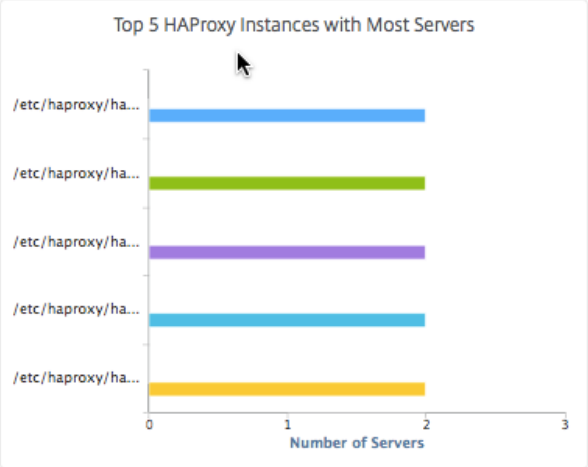
En el panel de aplicaciones, Citrix Application Delivery Management (Citrix ADM) muestra el número de instancias de HAProxy que descubre y enumera las cinco instancias principales de HAProxy que están configuradas con el mayor número de interfaces o servidores.

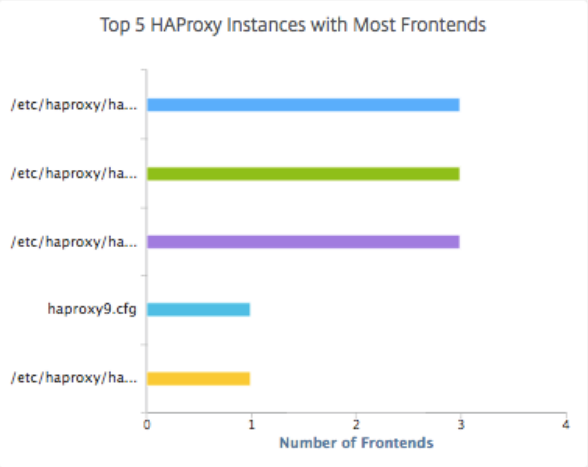
Para ver el panel de aplicaciones, en Citrix ADM, vaya a **Aplicaciones** > **Panel**.



El número de instancias de HAProxy descubiertas por Citrix ADM se muestra en la fila superior, como se muestra a continuación:

Para ver la lista de las cinco principales instancias de HAProxy que están configuradas con el mayor número de interfaces o el mayor número de servidores, desplázate hacia abajo en el panel de control:





Reiniciar una instancia de HAProxy

January 30, 2024

Para reiniciar una instancia de HAProxy desde la GUI de Citrix Application Delivery Management (Citrix ADM), puede seleccionar un reinicio completo o un reinicio suave.

Reinicio duro

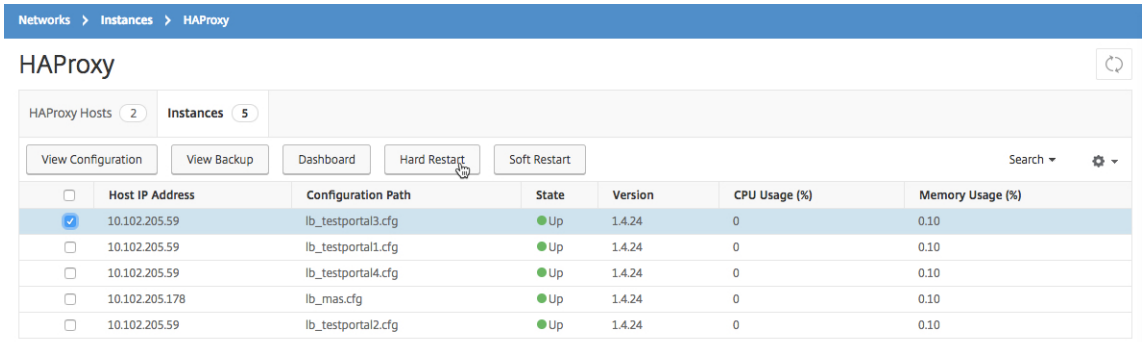
El reinicio completo finaliza el proceso HAProxy en la instancia y cierra todas las conexiones establecidas. Tras el reinicio, se crea un nuevo proceso haproxy y el nuevo proceso HAproxy procesa las nuevas conexiones subsiguientes.

Reinicio suave

El reinicio parcial desvincula el proceso HAProxy del puerto de escucha, pero el proceso HAProxy continúa procesando las conexiones existentes hasta que se cierren. Se crea un nuevo proceso HAProxy para procesar las nuevas conexiones.

Para reiniciar una instancia de HAProxy, haga lo siguiente:

1. Vaya a **Redes** > **Instancias** > **HAProxy** y haga clic en la pestaña **Instancia** .
2. En la ficha **Instancia**, seleccione la instancia HAProxy que quiere reiniciar.
3. Haga clic en **Reiniciar** duro para reiniciar la instancia HAProxy o haga clic en **Reiniciar** suave para reiniciar la instancia HAProxy.



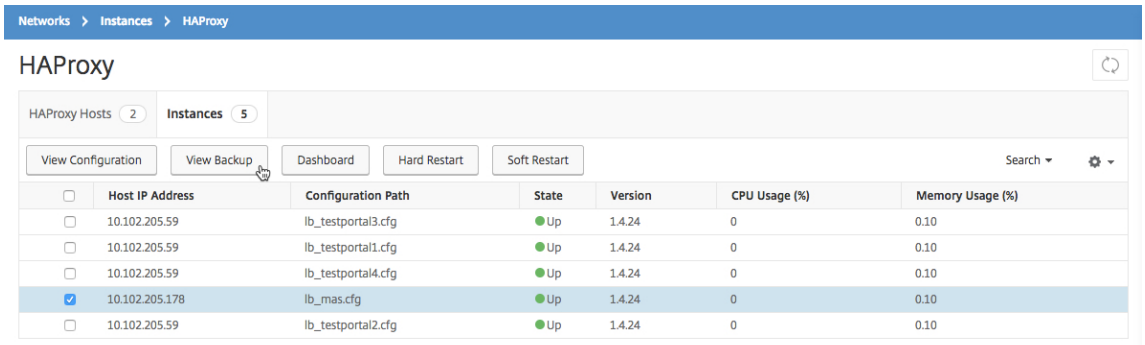
Realizar una copia de seguridad y restaurar una instancia de HAProxy

January 30, 2024

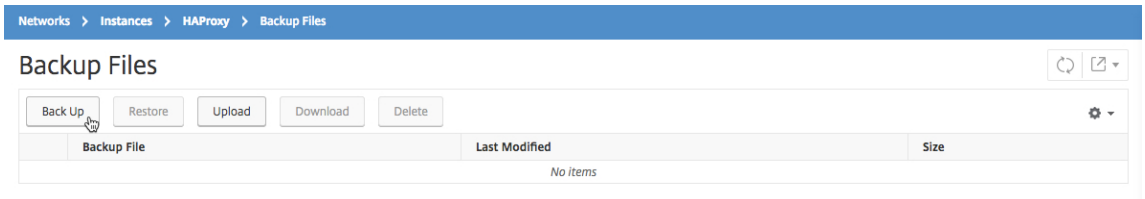
Puede realizar una copia de seguridad del estado actual de una instancia de HAProxy en un archivo de configuración de HAProxy. Si la instancia se vuelve inestable, puede usar el archivo de copia de seguridad para restaurar la instancia al estado estable.

Para realizar una copia de seguridad de una instancia HAProxy mediante NetScaler ADM:

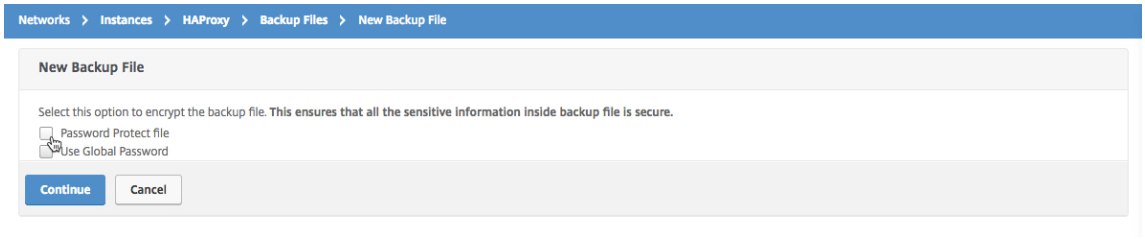
1. En Citrix Application Delivery Management (Citrix ADM), vaya a **Redes > Instancias > HAProxy** .
2. En la página **HAProxy**, haga clic en la ficha **Instancias**.
3. Seleccione la instancia de HAProxy de la que desea hacer una copia de seguridad y, a continuación, haga clic en **Ver copia de seguridad** .



4. En la página **Archivos** de copia de seguridad , haga clic en **Realizar copia de seguridad.**



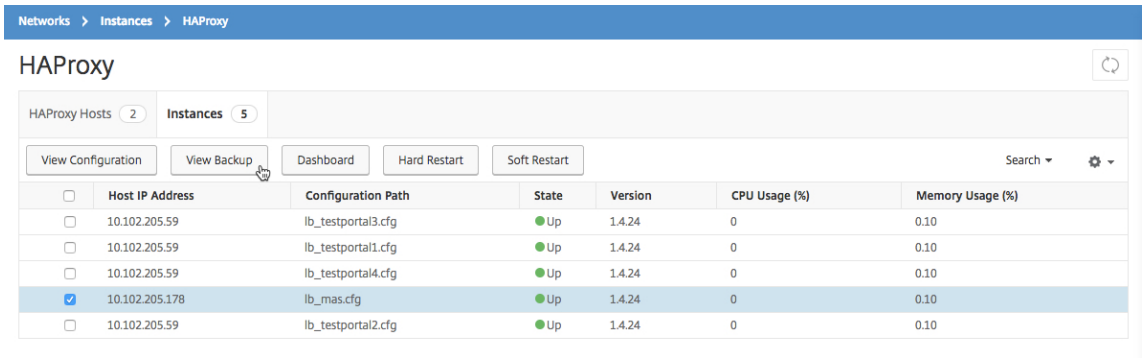
5. Puede optar por cifrar el archivo de copia de seguridad para mayor seguridad.



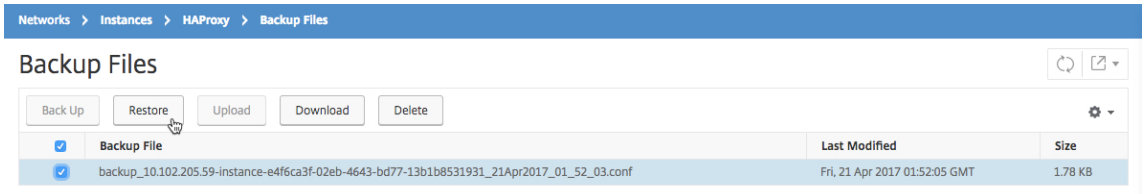
6. Haga clic en **Continuar**.

Para restaurar una instancia mediante NetScaler ADM:

1. Vaya a **Redes** > **Instancias** > **HAProxy** .
2. En la página **HAProxy**, haga clic en la ficha **Instancias**.
3. Selecciona la instancia que quieres restaurar y, a continuación, haz clic en Ver copia de **seguridad** .



4. En la página **Archivos** de copia de seguridad, seleccione el archivo de copia de seguridad que desea restaurar y, a continuación, haga clic en **Restaurar** .



> **Nota**
>
> Al restaurar una instancia, NetScaler ADM reinicia la instancia HAProxy.

Modificar el archivo de configuración HAProxy

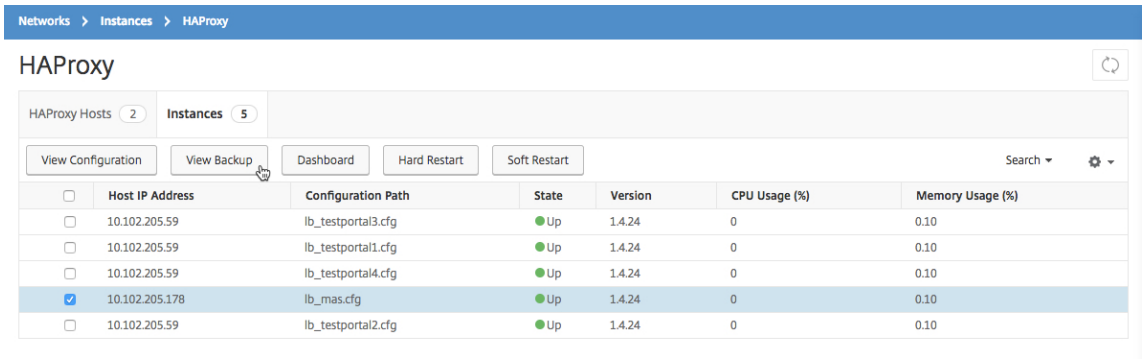
January 30, 2024

Puede actualizar la interfaz, el backend, el servidor y otras configuraciones en el archivo de configuración de HAProxy existente. Para editar el archivo de configuración de HAProxy:

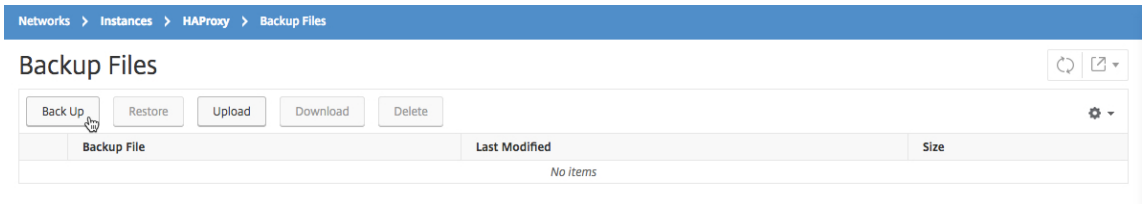
- Haga una copia de seguridad del archivo de configuración de HAProxy.
- Descargue el archivo de configuración HAProxy de copia de seguridad y edítelo sin conexión.
- Cargue el archivo de configuración de HAProxy actualizado en Citrix Application Delivery Management (Citrix ADM)
- Restaure la instancia de HAProxy con el archivo de respaldo actualizado.

Para modificar el archivo de configuración HAProxy mediante NetScaler ADM:

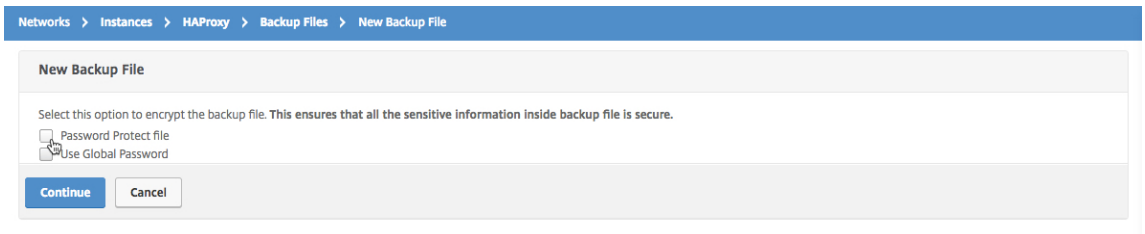
1. En Citrix ADM, vaya a **Redes** > **Instancias** > **HAProxy**.
2. En la página **HAProxy**, haga clic en la ficha **Instancias**.
3. Seleccione la instancia de HAProxy de la que desea hacer una copia de seguridad y, a continuación, haga clic en **Ver copia de seguridad** .



4. En la página **Archivos de copia de seguridad**, haga clic en **Hacer copia de seguridad**.



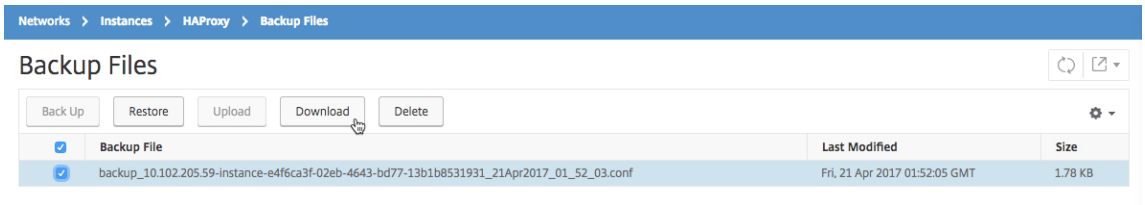
5. Haga clic en **Continuar**.



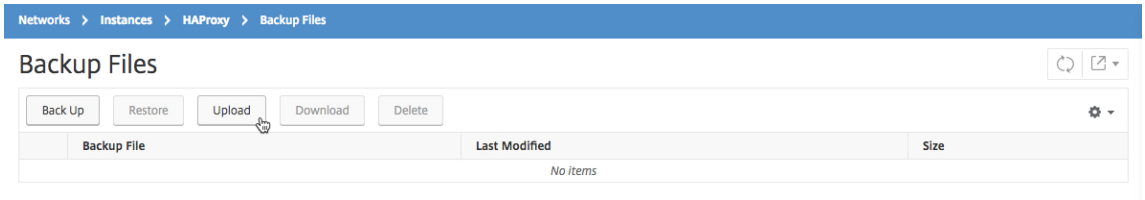
Nota

> No cifre el archivo de respaldo.

6. En la página **Archivos de copia** de seguridad, seleccione el archivo de copia de seguridad y haga clic en **Descargar**.



7. Con un editor de texto, edite el archivo de configuración de HAProxy.
8. En la página **Archivos de copia** de seguridad, haga clic en **Cargar** para examinar y seleccionar el archivo de configuración HAProxy actualizado.



   Después de cargar el archivo de configuración HAProxy actualizado, aparece en la página **Archivos de copia de seguridad**.

9. Seleccione el archivo de configuración HAProxy actualizado y haga clic en **Restaurar**.

Administrar la configuración del sistema

January 30, 2024

En la siguiente tabla se describe cómo configurar los ajustes del sistema en su Citrix ADM.

Si quieres…	Haz esto…
Configurar el mensaje del día	Ahora puede crear un mensaje de bienvenida en Citrix ADM. Puede utilizar esta función para establecer mensajes de recordatorio para usted o para el usuario que inicia sesión en NetScaler ADM. Vaya a **Sistema** > **Configuración del sistema** y haga clic en **Configurar mensaje del día** . Haga clic en **Habilitar mensaje** , escriba el mensaje en el cuadro de mensajes **y** haga clic en Aceptar .
Cierre Citrix ADM	Vaya a **Sistema** > **Administración del sistema**. Puede hacer clic en **Apagar Citrix ADM** para cerrar Citrix ADM por completo. **Nota**Una vez que cierre Citrix ADM, solo podrá

volver a iniciar Citrix ADM desde el hipervisor en el que lo haya instalado.|
Configurar los ajustes del asistente de configuración	Vaya a **Sistema** > **Administración del sistema**. **En Configurar Citrix ADM** , seleccione **Configuración del asistente de configuración** . Puede seleccionar la opción **Citrix ADM Network** para modificar la configuración de la red, como la dirección IP de Citrix ADM y su contraseña. Puede hacer clic en **Configuración del sistema** para modificar el nombre de host, el modo de comunicación con las instancias o la zona horaria local.
Configurar parámetros de red	Vaya a **Sistema** > **Administración del sistema**. **En Configurar Citrix ADM** , seleccione **Configuración de red** . La GUI muestra los certificados y claves SSL instalados en Citrix ADM.
Ver certificado SSL	Vaya a **Sistema** > **Administración del sistema**. **En Configurar Citrix ADM** , seleccione **Ver certificado SSL** . La GUI muestra los certificados y claves SSL instalados en Citrix ADM.
Cambiar zona horaria	Vaya a **Sistema** > **Administración del sistema** . En **Configuración del sistema** , selecciona **Cambiar zona** horaria . En la lista desplegable **Zona** horaria , seleccione la zona horaria del reloj del dispositivo Citrix ADM.
Cambiar nombre de host	Vaya a **Sistema** > **Administración del sistema**. En **Configuración del sistema** , selecciona **Cambiar nombre de host** . Introduzca un nombre de host que se utilizará para identificar su Citrix ADM, de modo que cuando genere la licencia universal para Citrix ADM Gateway, el nombre de host aparezca en la licencia.
Cambiar la configuración del sistema	Vaya a **Sistema** > **Administración del sistema** . En **Configuración del sistema** , selecciona **Cambiar configuración del sistema** . A continuación, active o desactive las casillas de verificación para habilitar o deshabilitar las siguientes funciones: Solo acceso seguro, Habilitar el tiempo de espera de la sesión, Permitir la autenticación básica, Habilitar el inicio de sesión de nsrecover, Habilitar la descarga de certificados, Habilitar el acceso a Shell para usuarios que no sean de nsroot, Solicitar las credenciales de usuario para el inicio de sesión de la instancia
Configurar los ajustes de SSL	Vaya a **Sistema** > **Administración del sistema**. En **Configuración del sistema** , seleccione **Configurar opciones de SSL** para mostrar la configuración del protocolo actual y los conjuntos de cifrado aplicados. Si desea modificar alguna de las configuraciones, en **Editar configuración, seleccione Configuración** de **protocolo** o Conjuntos de **cifrado** .
Habilite la función de configuración de mejora de la experiencia del usuario	Vaya a **Sistema** > **Administración del sistema**. En **Configuración del sistema** , seleccione **Configurar las opciones de mejora de la experiencia del usuario** y, a continuación, active la casilla **Habilitar CUXIP** . Si selecciona esta casilla, las estadísticas de uso se recopilan con el único propósito de mejorar la interfaz gráfica de usuario. Los datos recibidos solo los utilizan los ingenieros de Citrix y no se comparten con nadie.
Actualizar Citrix ADM	Vaya a **Sistema** > **Administración del sistema**. En el subtítulo **Administración del sistema** , seleccione **Actualizar Citrix ADM** y, a continuación, seleccione el nuevo

archivo de imagen. Puede seleccionar un archivo que ya esté en el dispositivo virtual Citrix ADM o puede cargar un archivo desde su equipo local. |
Reiniciar Citrix ADM	Vaya a **Sistema** > **Administración del sistema**. En el subtítulo **Administración del sistema** , seleccione **Reiniciar Citrix ADM** . Aparece un cuadro de diálogo en el que se le pide que confirme la acción. Haga clic en **Sí**.
Configurar los ajustes de poda del sistema (para eliminar datos antiguos)	Vaya a **Sistema** > **Administración del sistema**. En **Configuración de poda**, seleccione Configuración de **poda del sistema** . En el campo Datos a conservar (días), introduzca el número de días durante los que desea conservar los datos en el sistema.
Configurar los ajustes de copia de seguridad del sistema	Vaya a **Sistema** > **Administración del sistema**. En **Configuración de copia** de seguridad, seleccione **Configuración de copia de seguridad del sistema** y, a continuación, introduzca el número de copias de seguridad del sistema que se van a conservar en el dispositivo Citrix ADM. También puede optar por cifrar los archivos de respaldo y especificar una ubicación externa a la que transferirlos. Los archivos de respaldo transferidos se pueden conservar o eliminar del sistema.
Configurar los ajustes de copia de seguridad de la instancia	Vaya a **Sistema** > **Administración del sistema**. En **Configuración de copia** de seguridad, seleccione **Configuración de copia de seguridad de instancia** e introduzca el intervalo de tiempo (en horas) en el que desea crear un archivo de copia de seguridad que haga una copia de seguridad de todas las instancias administradas por Citrix ADM. Puede especificar el número de archivos de respaldo que desea conservar y si desea cifrarlos para que no se pueda acceder a ellos sin una contraseña.
Ver las estadísticas del sistema	Vaya a **Sistema** > **Estadísticas**. Un gráfico de líneas muestra información como el uso de la CPU, el uso de la memoria y el uso del disco.
Ver y administrar sesiones	Vaya a **Sistema** > **Sesiones** . A continuación, puede ver todas las sesiones activas, con detalles. Para terminar una sesión, seleccione su casilla de verificación y haga clic en **Cancelar sesión** .
Agregar o modificar un inquilino	Vaya a **Sistema** > **Inquilinos** y agregue un nuevo inquilino o modifique la configuración de un inquilino existente. Puedes proporcionar información adicional, como el nombre de la unidad organizativa, el departamento y la URL del inquilino.
Cambiar la política de bloqueo de usuarios	Vaya a **Sistema** > **Administración de usuarios** . En **Configuración de usuario** , seleccione **Configuración de bloqueo** de usuarios y, a continuación, active la casilla **Habilitar bloqueo de usuarios** . Puede especificar el número de intentos no válidos que puede realizar un usuario antes de deshabilitar su cuenta y durante cuánto tiempo estará activa la política de bloqueo de usuarios.
Cambiar la complejidad de la contraseña	Vaya a **Sistema** > **Administración de usuarios** . En **Configuración de usuario** , seleccione **Política de contraseñas** y, a continuación, active la casilla **Habilitar complejidad de contraseñas** . En el campo **Longitud mínima de contraseña** , introduzca el número mínimo de caracteres necesario para una contraseña en Citrix ADM.
Agregar o modificar un usuario	Vaya a **Sistema** > **Administración** de usuarios > Usuarios. En

Usuarios, añada un usuario nuevo o modifique la configuración de un usuario existente. Al agregar un usuario, puede habilitar opciones como la autenticación externa , el tiempo de espera de la sesión y la asignación del usuario a grupos específicos. |
Agregar o modificar un grupo de usuarios	Vaya a **Sistema** > **Administración de usuarios** > **Grupos** . En **Grupos** , agrega un grupo nuevo o edita la configuración de un grupo existente. Al agregar un grupo, puede habilitar opciones como asignar permisos para el grupo, configurar el tiempo de espera de la sesión, asignar usuarios al grupo y permitir el acceso a aplicaciones concretas o a todas las aplicaciones del Citrix ADM.
Cambiar la configuración de autenticación	Vaya a **Sistema** > **Autenticación** > **Autenticación**. En **Autenticación** , seleccione **Configuración de autenticación** y seleccione el tipo de servidor de autenticación.
Agregar o modificar un servidor RADIUS	Vaya a **Sistema** > **Autenticación** > **RADIUS** . En **RADIUS** , agregue un nuevo servidor RADIUS o edite la configuración de un servidor RADIUS existente introduciendo o modificando los parámetros de red.
Agregar o modificar un servidor LDAP	Vaya a Sistema > Autenticación > LDAP. En LDAP, añada un nuevo servidor LDAP o modifique la configuración de un servidor LDAP existente introduciendo o modificando los parámetros de red.
Agregar o modificar un servidor TACACS	Vaya a **Sistema** > **Autenticación** > **TACACS** . En **TACACS** , agregue un nuevo servidor TACACS o edite la configuración de un servidor TACACS existente introduciendo o modificando los parámetros de la red.
Agregar o modificar un servidor syslog	Vaya a **Sistema** > **Auditoría** > **Servidores Syslog**. En **Servidores syslog** , agregue un nuevo servidor syslog o modifique la configuración de un servidor syslog existente introduciendo o modificando los parámetros de red . Puede proporcionar información adicional seleccionando el tipo de niveles de registro que desea supervisar.
Leer mensajes de syslog	Vaya a **Sistema** > **Auditoría** . En **Mensajes de auditoría** , seleccione **Mensajes de Syslog**. Los resúmenes de todos los archivos de registro del sistema se muestran en el Visor de Syslog. Puede seleccionar el archivo syslog que desea ver en la opción desplegable Archivo. Además, los archivos syslog se pueden filtrar aún más por módulo, tipo de evento y gravedad.
Configurar los ajustes de purga de syslog	Vaya a **Sistema** > **Auditoría** . En **Configuración**, seleccione **Syslog Purge Settings** y, a continuación, introduzca el número de días que se conservarán los datos de syslog antes de que se eliminen del Citrix ADM.
Ver eventos del sistema	Navegue hasta **Sistema** > **Eventos** . A continuación, puede ver todos los eventos actuales, con detalles.
Agregar o modificar un servidor NTP	Vaya a **Sistema** > **Servidores NTP**. Agregue un nuevo servidor NTP o modifique la configuración de un servidor NTP existente.
Configurar los parámetros de NTP	Vaya a **Sistema** > **Servidores NTP**. Haga clic en **Parámetros NTP** e introduzca los detalles de configuración del servidor en los campos proporcionados.
Habilitar la sincronización de NTP	Vaya a **Sistema** > **Servidores NTP**. Para sincronizar la hora

que se muestra en el servidor NTP con el reloj local, seleccione la casilla **Habilitar la sincronización NTP** . |
Agregar o modificar grupos de cifrado	Navegue hasta **Sistema** > **Grupos de cifrado** para agregar un nuevo grupo de cifrado o editar la configuración de un grupo de cifrado existente. Debe introducir una descripción de su grupo de cifrado y asignarlo a un conjunto de cifrado.
Configurar las opciones de notificación	Vaya a **Sistema** > **Notificaciones**. En **Configuración** , selecciona **Cambiar configuración de notificaciones** . Elige las acciones para las que quieres enviar las notificaciones y selecciona **Correo** electrónico , **SMS** o ambos.
Configurar los ajustes del resumen de eventos	Vaya a **Sistema** > **Notificaciones**. En **Configuración** , seleccione **Configurar opciones de resumen de eventos** . Después de **desactivar la casilla de verificación Desactivar resumen de eventos** , puede establecer un período de repetición y elegir una lista de distribución de correo electrónico para enviar las notificaciones de resumen de eventos.
Agregar o modificar servidores de correo electrónico	Vaya a **Sistema** > **Notificaciones** > Correo **electrónico** . En **Correo** electrónico , seleccione la pestaña **Servidores de correo** electrónico para agregar un nuevo servidor de correo electrónico o editar la configuración de un servidor de correo electrónico existente. Puede habilitar comprobaciones adicionales para asegurarse de que la autenticación es necesaria para acceder al servidor de correo electrónico o para especificar que su servidor de correo electrónico admite la autenticación SSL.
Agregar o modificar listas de distribución de correo electrónico	Vaya a **Sistema** > **Notificaciones** > Correo **electrónico** . En **Correo** electrónico , seleccione la pestaña **Lista de distribución de correo** electrónico para agregar una nueva lista de distribución de correo electrónico o editar la configuración de una lista de distribución de correo electrónico existente.
Agregar o modificar servidores de SMS	Vaya a **Sistema** > **Notificaciones** > **SMS** . En **SMS** , seleccione la pestaña **Servidor SMS** para agregar un nuevo servidor SMS o editar la configuración de un servidor SMS existente.
Agregar o modificar listas de distribución de SMS	Vaya a **Sistema** > **Notificaciones** > **SMS** . En **SMS** , seleccione la pestaña **Lista de distribución de SMS** para agregar una nueva lista de distribución de SMS o editar la configuración de una lista de distribución de SMS existente.
Configurar el ID del motor SNMP	Navegue hasta **Sistema** > **SNMP** . En **Configuración** , seleccione **Configurar ID del motor** y especifique el ID del motor.
Configurar SNMP MIB	Navegue hasta **Sistema** > **SNMP** . En **Configuración** , seleccione **Configurar SNMP MIB** e introduzca los detalles de SNMP MIB.
Configurar trampas SNMP	Vaya a **Sistema** > **SNMP** > **Destinos de captura**. En **Capturas SNMP** , agregue un nuevo destino de captura SNMP o modifique la configuración de un destino de captura SNMP existente.
Agregar o modificar un administrador de SNMP	Vaya a **Sistema** > **SNMP** > **Gestores**. En **SNMP Manager** , agregue un nuevo administrador SNMP o modifique la configuración de un administrador SNMP existente.

Agregar o modificar un usuario de SNMP	Vaya a **Sistema** > **SNMP** > **Usuarios**. En **Usuario de SNMP** , agregue un nuevo usuario de SNMP o modifique la configuración de un usuario de SNMP existente.
Agregar o modificar vistas SNMP	Vaya a **Sistema** > **SNMP** > **Vistas** . En la **vista SNMP** , agregue una nueva vista SNMP o modifique la configuración de una vista SNMP existente.
Modificar alarmas	Vaya a **Sistema** > **Alarmas** y seleccione la alarma cuya configuración desee modificar. Las alarmas le ayudan a supervisar el estado del servidor Citrix ADM.
Ver el registro de tareas	Vaya a **Sistema** > **Diagnóstico** > **Registros de tareas** . A continuación, puede ver todos los registros de tareas con detalles. Para ver información adicional, seleccione un registro de tareas y consulte su registro de dispositivos y, a continuación, consulte el registro de comandos del registro de dispositivos seleccionado.
Generar el archivo de soporte técnico	Vaya a **Sistema** > **Diagnóstico** > **Soporte técnico** . En **Soporte técnico** , haga clic en **Generar archivo de soporte técnico** para generar un archivo (archivo TAR) con los datos y las estadísticas de Citrix ADM, que puede enviar al soporte de Citrix para obtener ayuda con la depuración de un problema.
Configurar los ajustes de la zona horaria de los informes del panel	Vaya a **Sistema** > **Configuración de análisis** . En **Configuración de análisis** , seleccione **Configurar los ajustes de zona horaria de los informes del panel** para establecer la hora local o la zona GMT como la predeterminada para los informes que se muestran en el panel.
Configurar el tiempo de espera de la sesión ICA	Vaya a **Sistema** > **Configuración de análisis** . En **Configuración de análisis** , seleccione **Configurar el tiempo de espera de la sesión** ICA e introduzca la cantidad de tiempo durante el cual una sesión ICA puede permanecer inactiva antes de finalizar.
Configurar las funciones de análisis	Vaya a **Sistema** > **Configuración de análisis** . En **Configuración de análisis** , seleccione **Configurar** funciones para habilitar la configuración de saltos múltiples y la configuración de umbral adaptativo. Si selecciona la casilla **Habilitar multisalto** , Citrix ADM recopila y correlaciona los registros de AppFlow de todos los dispositivos implementados con más de una instancia de Citrix ADC entre un cliente y un servidor. Si selecciona la casilla **Habilitar umbral adaptativo** , se envía un mensaje de syslog al servidor de syslog cada vez que el número de visitas a una URL supera su valor de umbral.
Configurar los ajustes de base de datos	Vaya a **Sistema** > **Configuración de análisis** . En Configuración de **análisis** , seleccione **Configurar** funciones para habilitar la configuración del índice de la base de datos y la configuración de limpieza de la base de datos. Al seleccionar la casilla **Habilitar la indexación de bases de datos**, puede facilitar la consulta eficiente de la base de datos Citrix ADM. Si selecciona la casilla **Habilitar limpieza de base de datos**, se repetirá el intento de limpiar la base de datos si una carga excesiva en Citrix ADM impide la limpieza a la hora programada normalmente.
Configurar los ajustes de la caché de la base	Vaya a **Sistema** > **Configuración de análisis** . En Configuración de **análisis** , seleccione **Configurar ajustes de caché de base de datos** para

almacenar localmente el contenido de la base de datos en la caché, de modo que pueda ver este contenido sin necesidad de acceder al servidor de bases de datos. |
Configurar los ajustes del registro de datos	En **Configuración de análisis** , seleccione **Configurar ajustes de registro de datos** . Puede habilitar las funciones para las siguientes configuraciones: configuración de registro de datos, configuración de persistencia de la duración de los datos, configuración de informes de Web Insight, configuración de recopilación de datos de SLA de Web Insight, configuración de recopilación de datos de URL de Web Insight, configuración de parámetros de URL
Configurar la administración de SLA para direcciones IP específicas de Citrix ADC	Vaya a **Sistema** > **Configuración de Analytics** > **Administración de SLA**. En la lista que se muestra, seleccione la dirección IP de Citrix ADC de un dispositivo en el que quiera administrar el SLA en función del tiempo de respuesta del servidor, las visitas por segundo y el uso del ancho de banda.
Configure el tiempo durante el cual se conservarán los registros de la base de datos para cada nivel de resumen de Insight	Vaya a **Sistema** > **Configuración de Analytics** > **Resumen de base de datos**. Especifique el tiempo durante el que desea conservar los datos de Insight en Citrix ADM. Puede optar por almacenar estos datos por hora, a diario o una vez por minuto.
Agregar o modificar umbrales adaptativos	Vaya a **Sistema** > **Configuración de análisis** > **Umbrales adaptativos** . En **Umbrales** adaptativos , añada un nuevo umbral adaptativo o modifique la configuración de un umbral adaptativo existente. La funcionalidad de umbral adaptativo establece el valor de umbral para el número máximo de visitas en cada URL. Si el número máximo de visitas a una URL es superior al valor de umbral establecido para la URL, se envía un mensaje de syslog a un servidor syslog externo. El intervalo de valores límite puede ser de días o semanas.
Agregar o modificar umbrales y alertas	Vaya a **Sistema** > **Configuración de Analytics** > **Umbrales**. En **Umbrales** , agrega un límite nuevo o edita la configuración de un umbral existente. Puede proporcionar elementos de acción adicionales al crear o modificar un umbral, como habilitarlo, enviar notificaciones por correo electrónico o SMS o configurar una regla para el umbral.
Cargue archivos de certificados SSL y claves SSL	Vaya a **Sistema** > **Configuración avanzada** > **Archivos de certificado SSL** . En **Archivos de certificados SSL** , selecciona la pestaña **Certificados SSL** para cargar un certificado SSL nuevo. Del mismo modo, en **Archivos de certificados****SSL , selecciona la pestaña Claves** SSL para cargar una nueva clave SSL.
Ver o editar los calendarios de exportación de informes	Vaya a **Sistema** > **Configuración avanzada** > **Exportar programaciones** . A continuación, puede ver todos los cronogramas de exportación, con detalles. Puede editar cualquier programa de exportación de la lista que se muestra aquí.
Programar la exportación de un informe	Vaya a **Sistema** > **Configuración avanzada** > **Exportar programaciones** . Para agregar un nuevo cronograma, haga clic en el botón del extremo derecho y seleccione la pestaña **Exportar cronograma** . Especifique los detalles y haga clic en **Programar** .
Utilice las funciones de copia de seguridad y restauración	Vaya a **Sistema** > **Configuración

avanzada** > **Archivos** de copia de seguridad para crear una copia de seguridad de la configuración actual de Citrix ADM. Más adelante, puede utilizar estos archivos de copia de seguridad para restaurar el Citrix ADM al estado en el que hizo la copia de seguridad. Citrix recomienda usar esta función antes de realizar una actualización y, en general , como medida de precaución. |
Instalar un certificado SSL	Vaya a **Sistema** > **Administración del sistema**. **En Configurar Citrix ADM** , seleccione **Instalar certificado SSL** . Puede seleccionar un archivo de certificado y un archivo de clave SSL que ya estén en el dispositivo virtual Citrix ADM, o puede cargar los archivos desde su equipo local. Debe introducir la contraseña de Citrix ADM en el campo Contraseña para instalar correctamente el certificado SSL.
Credenciales rápidas para iniciar sesión en la instancia	Vaya a **Sistema** > **Cambiar la configuración del sistema** . Habilite **Prompt Credentials for Instance Login para** solicitar a los usuarios sus credenciales de instancia en cualquier operación de configuración en instancias de Citrix ADC.
Habilitar la purga automática de datos	Vaya a **Sistema** > **Administración del sistema**. En **Configuración de poda**, seleccione Configuración de **poda del sistema** . Seleccione la casilla **Habilitar la purga automática de datos** para permitir que Citrix ADM purgue los datos cuando el uso del disco alcance el valor umbral establecido. Cuando esta función está habilitada, Citrix ADM purga los datos relacionados con eventos, syslogs, informes de rendimiento y análisis hasta que el uso del disco esté por debajo del valor umbral establecido. Haga clic en el icono de edición para modificar el valor límite de uso del disco.

Configurar las opciones de copia de seguridad del sistema

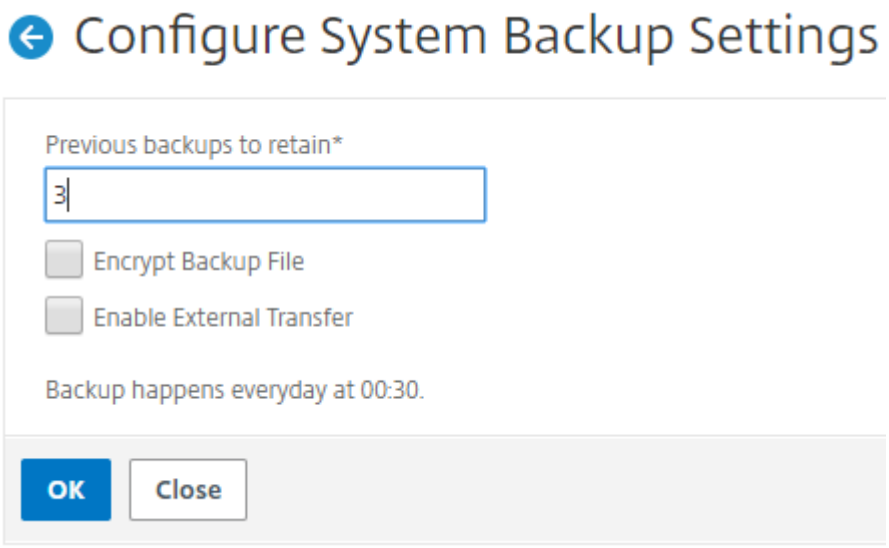
January 30, 2024

Debe establecer la configuración inicial de copia de seguridad del sistema antes de tener que hacer una copia de seguridad y restaurar el sistema Citrix Application Delivery Management (ADM).

1. Vaya a **Sistema**>**Administración del sistema**. En**Configuración de copia de seguridad**, haga clic en**Configuración de copia de seguridad del sistema**.
2. En la página **Configurar la configuración de copia de seguridad del sistema**, especifique lo siguiente:
    - Número de copias de seguridad que se deben conservar. Solo puede conservar hasta 10 copias de seguridad.
    - Cifrar el archivo de copia de seguridad.
    - Habilita la transferencia externa. Puede transferir una copia de una copia del archivo de respaldo a otro sistema como medida de precaución. Para restaurar la configuración,

primero debe cargar el archivo en el servidor Citrix ADM y, a continuación, realizar la operación de restauración. Especifique el servidor, el nombre de usuario y la contraseña, el puerto, el protocolo de transferencia que se va a utilizar y la ruta de acceso del directorio. Para obtener más información sobre la transferencia externa, consulte Transferir un archivo de respaldo Citrix ADM a un sistema externo.

3. Haga clic en **Aceptar**.



Configurar un servidor NTP

January 30, 2024

Puede configurar un servidor de Protocolo de hora de red (NTP) en NetScaler Application Delivery Management (ADM) para sincronizar su reloj con el servidor NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

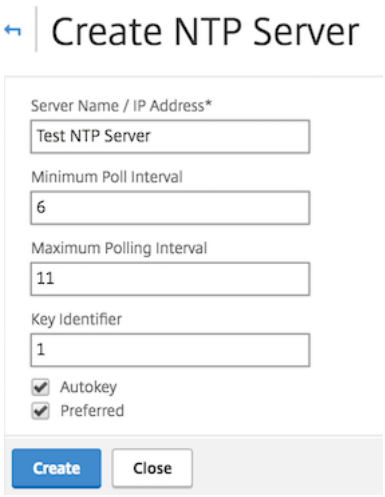
Para configurar un servidor NTP en NetScaler ADM:

1. Vaya a **Sistema** > **Servidores NTP** y, a continuación, haga clic en **Agregar** .
2. En la página **Crear servidor NTP**, introduzca los siguientes detalles:
   - **Nombre del servidor/dirección IP**: Introduzca el nombre de dominio o la dirección IP del servidor NTP. El nombre o la dirección IP no se pueden cambiar después de agregar el servidor NTP.
   - **Intervalo mínimo de sondeo**: Especifique el valor mínimo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que

el intervalo mínimo de sondeo sea de 64 segundos, que se puede expresar como 2^6, introduzca 6

- **Intervalo máximo de sondeo**: Especifique el valor máximo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que el intervalo máximo de sondeo sea de 256 segundos, que se puede expresar como 2^8, introduzca 8.
- **Identificador de clave**: introduzca el identificador de clave que se puede utilizar para la autenticación de clave simétrica con el servidor NTP. No añada un identificador de clave si decide seleccionar Autokey.
- **Clave automática**: Seleccione **Autokey** si desea utilizar la autenticación de clave pública con el servidor NTP. No seleccione si desea agregar un identificador de clave.
- **Preferido**: Seleccione esta opción si desea especificar este servidor NTP como servidor preferido para la sincronización de relojes. Esto solo se aplica si hay más de un servidor configurado.

3. Haga clic en **Crear**.



Para habilitar la sincronización NTP en NetScaler ADM:

1. Vaya a **Sistema** > **Servidores NTP**.
2. Haga clic en **Sincronización NTP** y active la casilla de verificación **Habilitar sincronización NTP**.
3. Haga clic en **Aceptar**.

> Nota
>
> Puede encontrar los mensajes de registro NTP en el directorio /var/log en el archivo de `/var/log/ntpd.log` archivo.

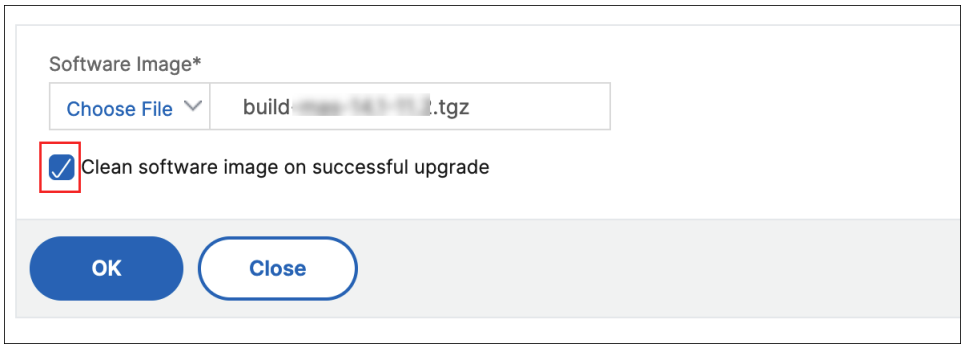
Actualizar Citrix ADM

January 30, 2024

Cada versión de Citrix Application Delivery Management (ADM) ofrece funciones nuevas y actualizadas con una mayor funcionalidad. En las notas de la versión que acompañan al anuncio de la versión se incluye una lista completa de mejoras. Tómese un momento para leer las notas de la versión antes de actualizar el software. Es importante entender el marco de licencias y los tipos de licencias antes de empezar a actualizar.

Para actualizar Citrix ADM:

1. Vaya a **Sistema** > **Administraciones del Sistema**. En el subtítulo **Administración del sistema** , haga clic en **Actualizar Citrix ADM** .
2. En la página Actualizar Citrix ADM, cargue un nuevo archivo de imagen seleccionando **Local** (su máquina local) o **Dispositivo**(el archivo del certificado debe estar presente en el dispositivo virtual Citrix ADM).
   De formapredeterminada, la imagen de software se limpia después de una actualización correcta.
3. Haga clic en **Aceptar**.



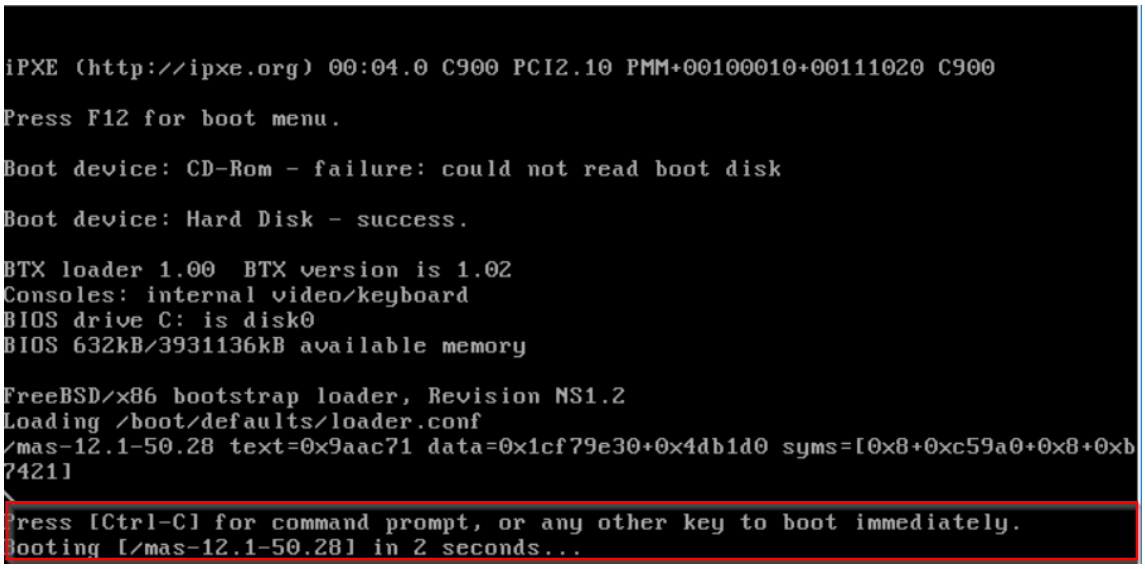
Cómo restablecer la contraseña para Citrix ADM

January 30, 2024

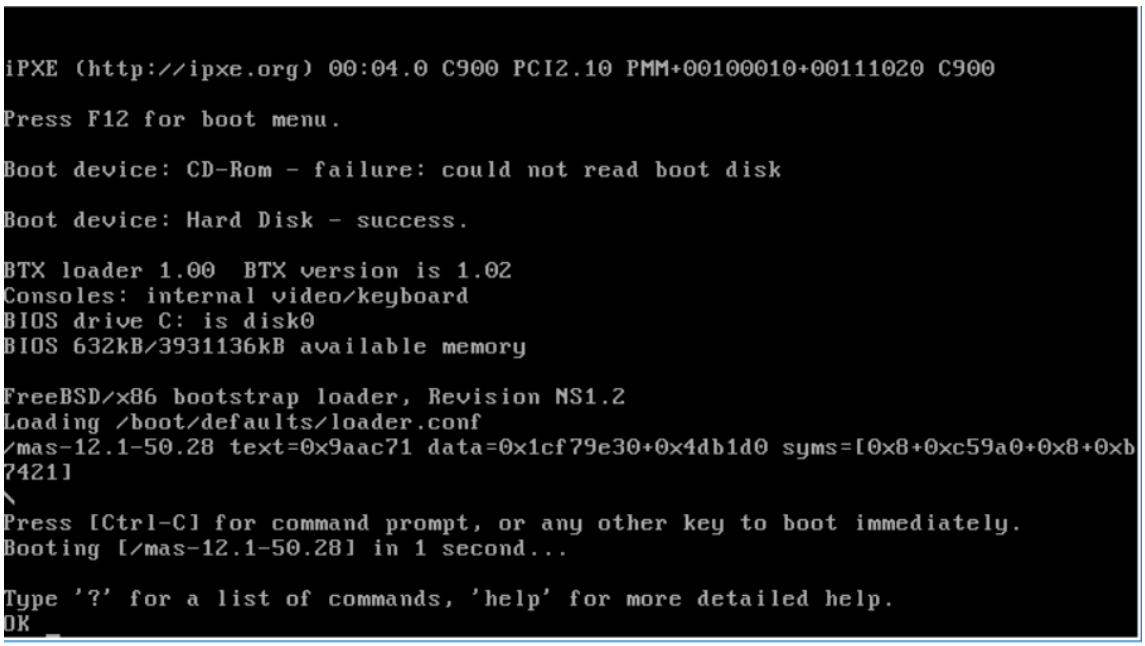
El procedimiento para restablecer la contraseña de Citrix ADM puede diferir en los hipervisores en los que está alojado. Si ha cambiado la contraseña predeterminada y quiere restablecerla, puede restablecerla reiniciando el nodo Citrix ADM.

Citrix Hypervisor con XenCenter:

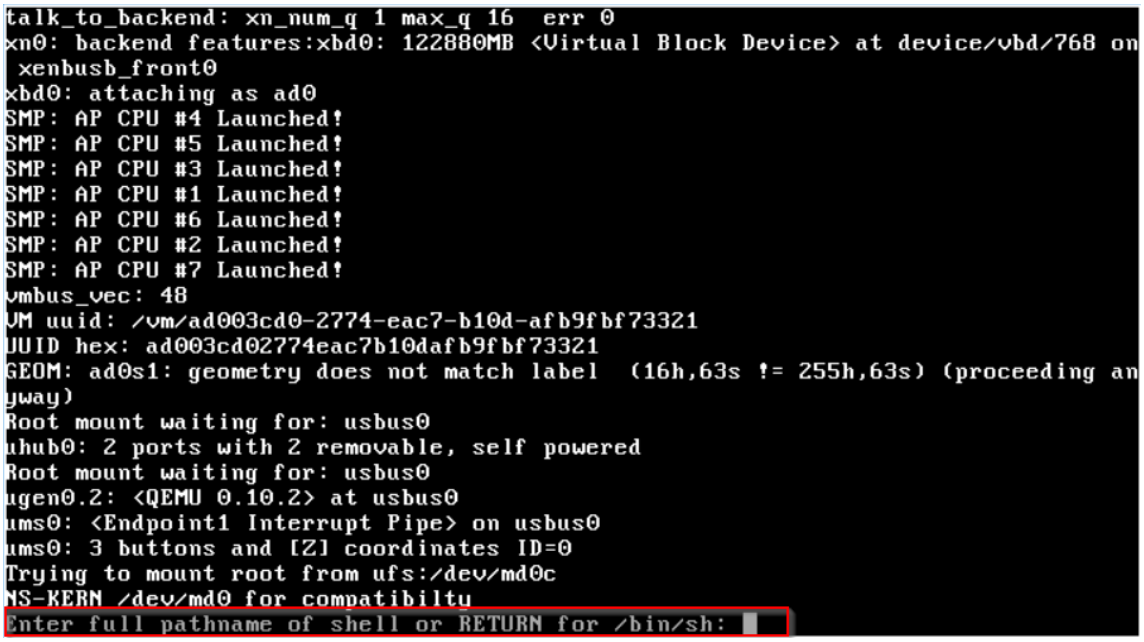
1. Inicie sesión en Citrix Hypervisor mediante XenCenter.
2. Seleccione el nodo Citrix ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.



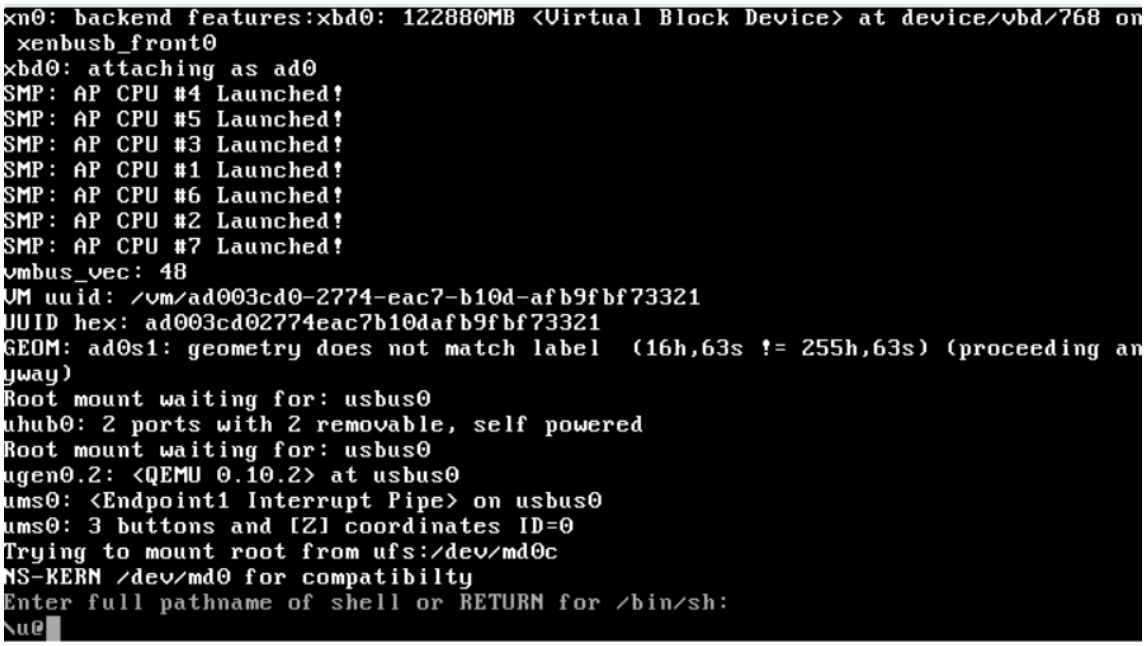
4. Ejecute el comando **boot -s** en la línea de comandos OK.



Citrix ADM se reinicia y muestra el siguiente mensaje:

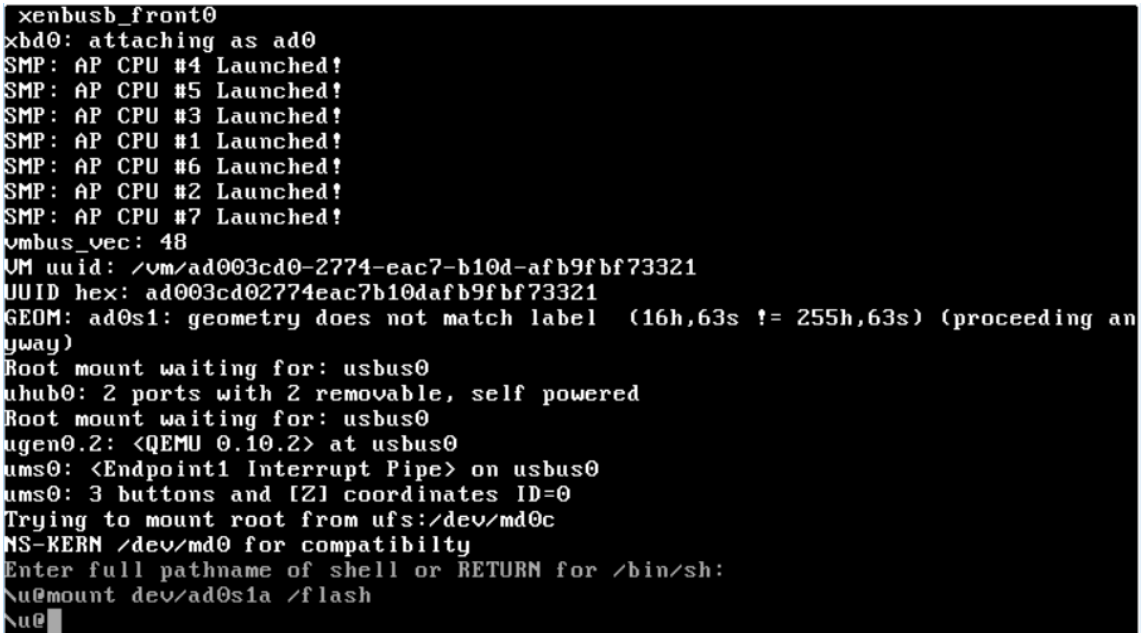


5. Presiona **Entrar** para que aparezca el mensaje /u @.



6. Monte la partición flash con el siguiente comando:

```
mount dev/ad0s1a /flash
```

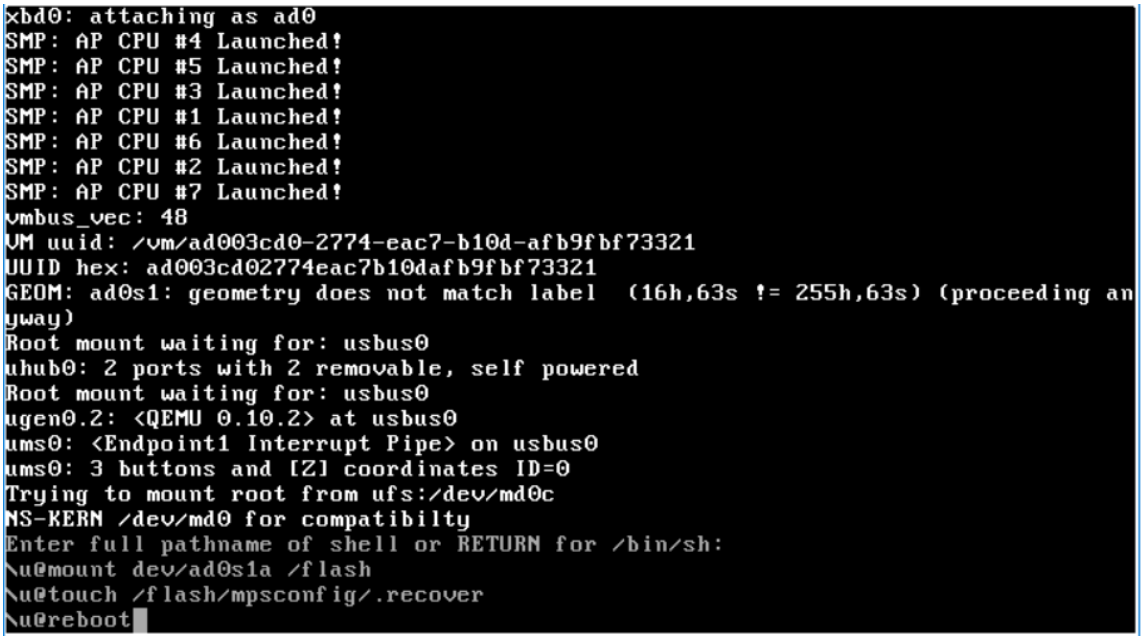



7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm –rf /etc/passwd`
9. Cree un archivo con el siguiente comando:

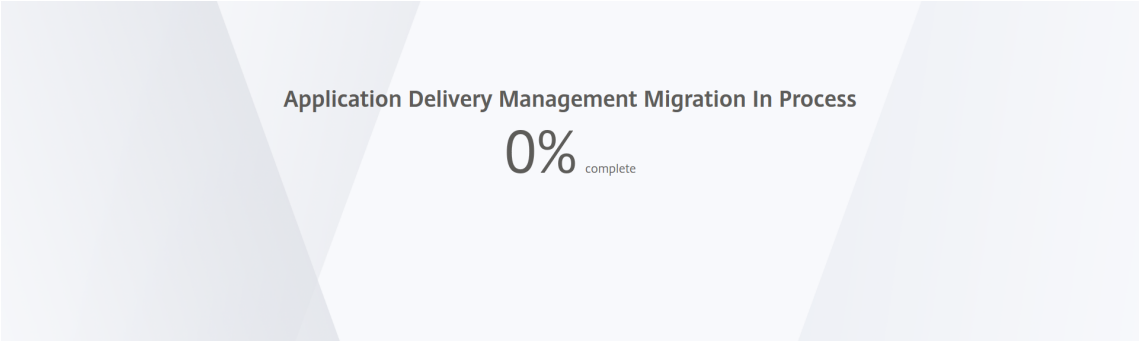
   `touch /flash/mpsconfig/.recover`

   La contraseña ahora se restablece a la contraseña predeterminada.

10. Ejecute el comando **Reboot** para reiniciar Citrix ADM.



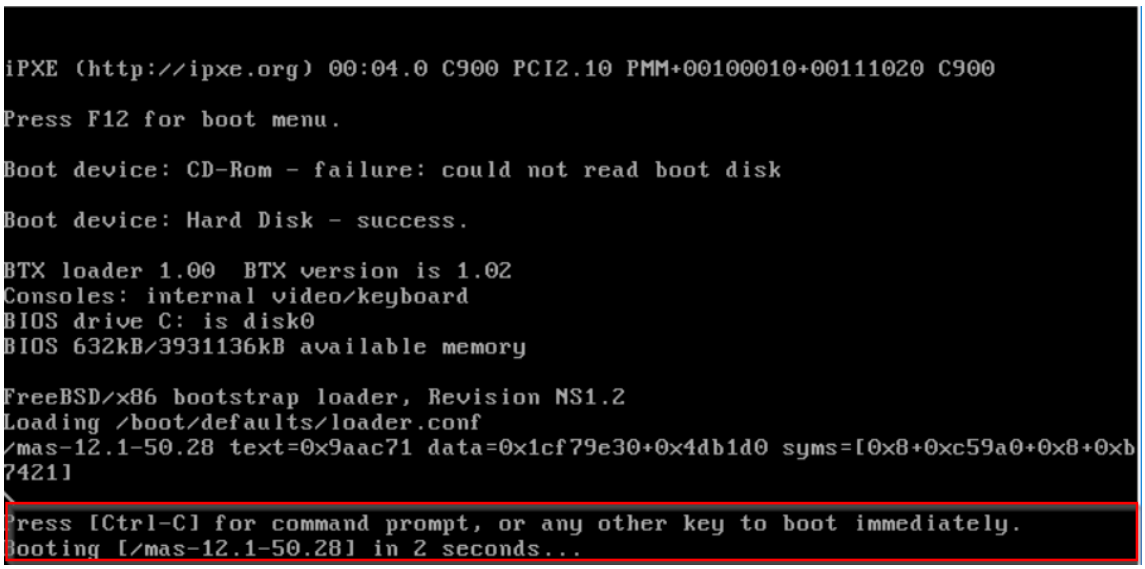
11. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.



Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el Hypervisor.

Esx mediante vSphere:

1. Inicie sesión en ESX con vSphere.
2. Seleccione el nodo Citrix ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.



4. Ejecute el comando **boot -s** en la línea de comandos OK.

   El Citrix ADM se reinicia.
5. Presiona **Entrar** para que aparezca el mensaje /u @.
6. Monte la partición flash con el siguiente comando:

   ```
   mount dev/da0s1a /flash
   ```
7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm –rf /etc/passwd`

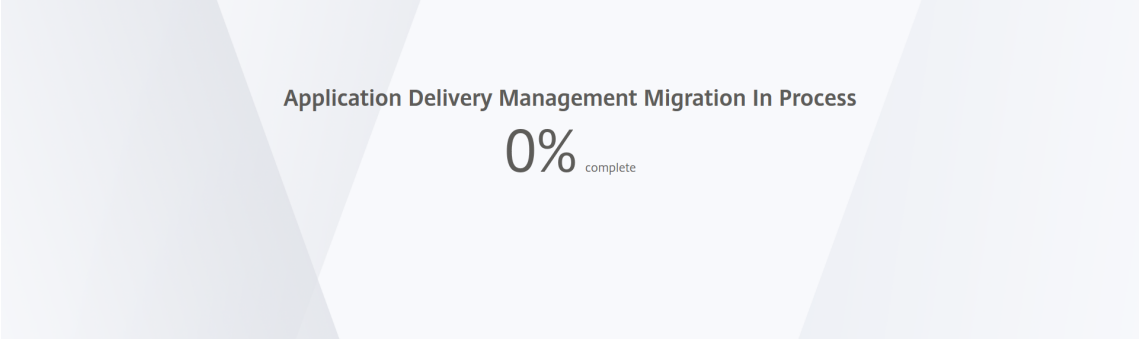
9. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.

10. Ejecute el comando **Reboot** para reiniciar Citrix ADM.

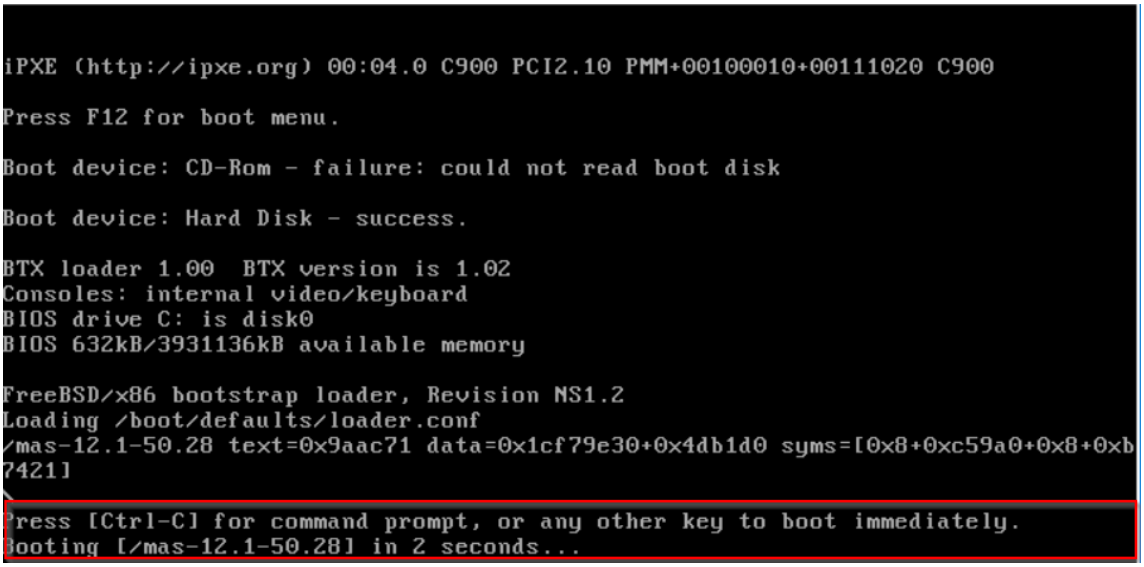
11. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.



   Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el servidor ESX.

Hyper-V mediante el administrador Hyper-V:

1. Inicie sesión en hyper-v con el administrador de hyper-v.
2. Seleccione el nodo Citrix ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.



4. Ejecute el comando **boot -s** en la línea de comandos OK.

   El Citrix ADM se reinicia.

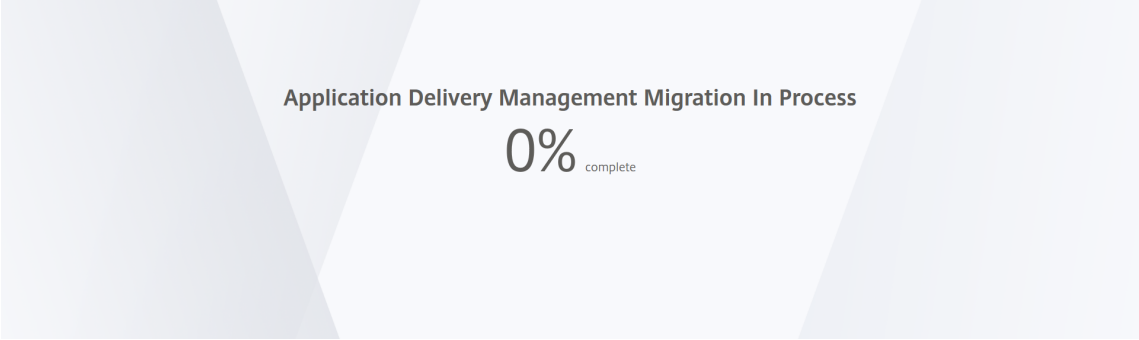
5. Presiona **Entrar** para que aparezca el mensaje /u @.
6. Monte la partición flash con el siguiente comando:

   ```
   mount dev/ad0s1a /flash
   ```

7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm –rf /etc/passwd`
9. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.
10. Ejecute el comando **Reboot** para reiniciar Citrix ADM.
11. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.



Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el administrador de hyper-v.

Servidor KVM Linux (SSH a servidor KVM mediante cualquier cliente SSH):

1. Inicie sesión en Citrix ADM mediante un cliente SSH en el servidor KVM.
2. Reinicie Citrix ADM.
3. Presione **CTL + C** para interrumpir la secuencia de arranque poco después de que aparezca el mensaje **Loading /boot/defaults/loader.conf**.
4. En el símbolo OK, ejecute el comando siguiente:

   ```
   set console='comconsole,vidconsole'
   ```

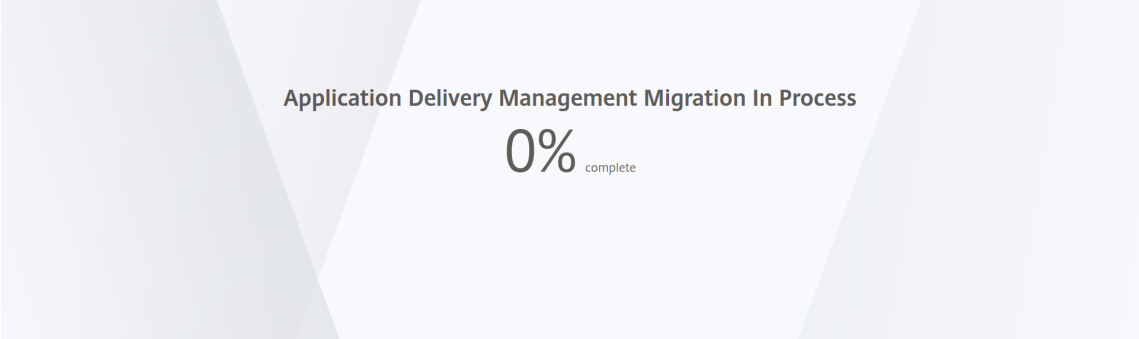
5. Ejecute el comando **boot -s** para reiniciar Citrix ADM.
6. Después de que aparezca el mensaje **Enter full path of shell o RETURN for /bin/sh:**, presione **Entrar** para obtener el mensaje /u@.
7. Monte la partición flash con el siguiente comando:

   ```
   mount dev/vtbd0s1a /flash
   ```


8. `Delete /flash/mpsconfig/master.passwd`
9. `Delete rm –rf /etc/passwd`
10. Cree un archivo con el siguiente comando:

    `touch /flash/mpsconfig/.recover`

    La contraseña ahora se restablece a la contraseña predeterminada.
11. Ejecute el comando **Reboot** para reiniciar Citrix ADM.
12. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.



Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde la GUI y *nsrecover/nsroot* para iniciar sesión desde la consola SSH.

Configurar el intervalo de depuración de syslog

January 30, 2024

Syslog es un protocolo estándar para el registro. Tiene dos componentes: el módulo de auditoría Syslog, que se ejecuta en la instancia Citrix Application Delivery Controller (ADC), y el servidor Syslog, que puede ejecutarse en el sistema operativo (SO) FreeBSD subyacente de la instancia Citrix ADC o en un sistema remoto. SYSLOG utiliza el Protocolo de datagramas de usuario (UDP) para la transferencia de datos.

Syslog permite el aislamiento del sistema que genera la información y del sistema que almacena la información. Puede consolidar la información de registro y obtener información de los datos recopilados. También puede configurar syslog para registrar diferentes tipos de eventos.

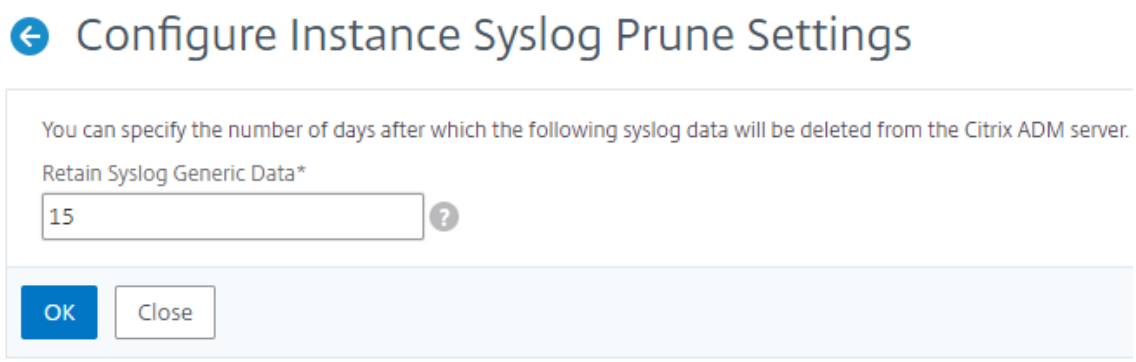
Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog.Puede especificar el número de días después de los cuales se eliminarán los siguientes datos de syslog de NetScaler Application Delivery Management (ADM):

- Datos genéricos de Syslog
- Datos de AppFirewall
- Datos de NetScaler Gateway

También puede configurar el intervalo de purga de Citrix Gateway por tipo de syslog. Este intervalo de purga tiene prioridad sobre el intervalo de purga configurado para retener los datos de Citrix Gateway.

Para configurar los intervalos de purga de syslog para Citrix ADM:

1. Vaya a **Sistema** > **Administración del sistema**. En **Configuración de poda**, haga clic en Configuración de **poda de Syslog de instancia** .
2. En la página **Configurar los ajustes de depuración de Syslog de la instancia** , especifique **Conservar datos genéricos de Syslog** . Escriba el número de días durante los cuales NetScaler ADM retiene mensajes genéricos de syslog.



Configurar las opciones de poda del sistema

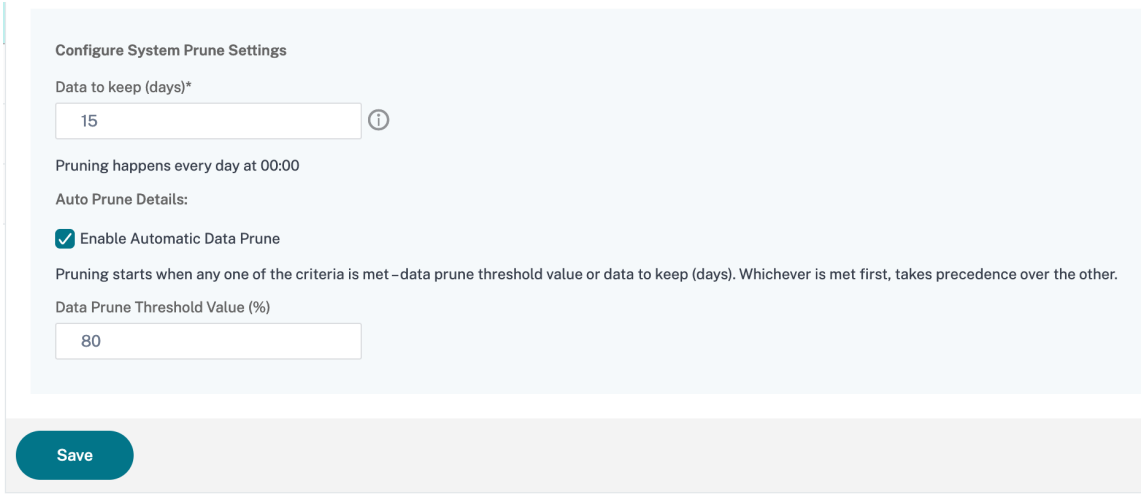
January 30, 2024

Para limitar la cantidad de datos de informes que se almacenan en la base de datos del software Citrix Application Delivery Management (ADM), puede eliminarlos. Puede especificar el intervalo para el que quiere que NetScaler ADM conserve datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

> **Nota**
>
> El valor que especifique no puede superar los 30 días ni ser inferior a 15 días.

Para configurar las opciones de poda del sistema para los informes de rendimiento mediante NetScaler ADM:

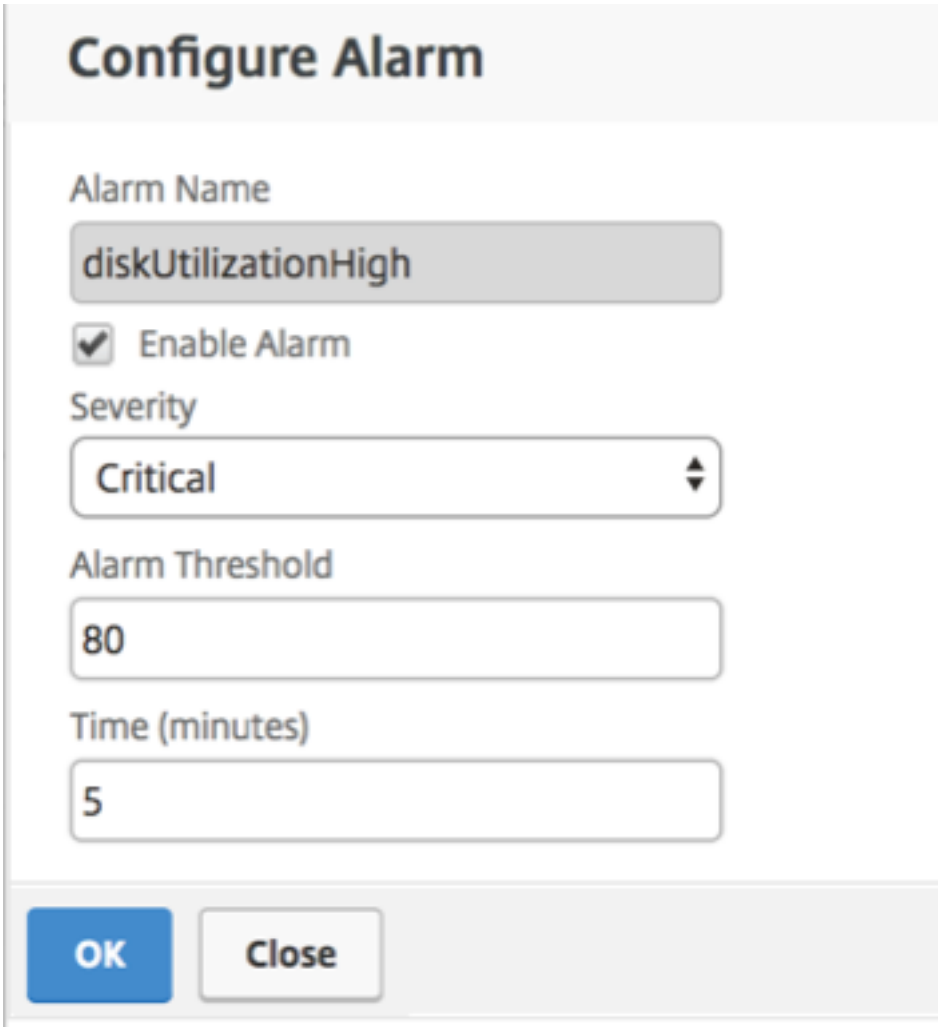
1. Vaya a **Sistema**>**Administración del sistema**. En **Configuración de poda**, haga clic en Configuración de **poda del sistema** .
2. En la página**Configurar configuración de ciruela del sistema**, especifique el número de días durante los que quiere conservar los datos y haga clic en**Aceptar**.



Puede activar la depuración automática seleccionando la casilla **Activar depuración automática de datos** . Se activa una alarma cuando el uso del disco supera el **valor umbral de purga de datos configurado .**

Puede configurar y habilitar la alarma**DiskUtilizationHigh**(de forma predeterminada) y especificar lo siguiente:

- **Gravedad,** como Crítica.
- **Umbral**de alarma . Escriba el valor para el que se calcula la gravedad del evento.
- **Hora**. Duración (en minutos) tras la cual desea activar la alarma.



Habilitar el acceso al shell para usuarios no predeterminados

January 30, 2024

Puede habilitar el acceso al shell para usuarios no predeterminados en Citrix Application Delivery Management (ADM). Puede utilizar esta función para habilitar y configurar el modo de comunicación con las instancias.

> **Nota**
>
> De forma predeterminada, el acceso a la consola está inhabilitado para los usuarios no predeterminados.

Para habilitar el acceso al shell para usuarios no predeterminados en Citrix ADM:

1. En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**.

2. En **Configuración del sistema**, haga clic en **Cambiar configuración del sistema**.
3. En la página **Modificar la configuración del sistema**, configure los siguientes parámetros:

    - **Comunicación con instancias**: Seleccione el protocolo de comunicación.
    - **Acceso**seguro : habilite el acceso seguro para Citrix ADM.
    - **Habilitar el tiempo de espera de la sesión**: Especifique el período de tiempo durante el cual se mantendrá una sesión inactiva.
    - **Permitir la autenticación básica**: Permita que el servicio de administración acepte las credenciales proporcionadas mediante el Protocolo de autenticación básica.
    - **Habilitar el inicio de sesión**en nsrecover : habilite el inicio de sesión en nsrecover Service.
    - **Habilitar la descarga**de certificados : le permite descargar certificados del Citrix ADC agregado.
    - **Habilitar el acceso al shell para usuarios**que no son de nsroot : habilite el acceso al shell para los usuarios no predeterminados en Citrix ADM.
    - **Solicitar credenciales de usuario para iniciar sesión en la instancia :**permita a los usuarios introducir sus credenciales de usuario al iniciar sesión en las instancias desde Citrix ADM.

4. Haga clic en **Aceptar**.

Recuperar servidores NetScaler ADM inaccesibles

January 30, 2024

Citrix Application Delivery Management (ADM) ahora proporciona una herramienta de mantenimiento de bases de datos para realizar la limpieza de la base de datos del sistema. Ahora puede iniciar la herramienta Citrix ADM Utility para conectarse al sistema de archivos, eliminar algunos componentes y hacer que la base de datos sea accesible. El script de recuperación Citrix ADM es una herramienta que ayuda a recuperar espacio en el sistema de archivos borrando tablas y archivos de bases de datos antiguos o no utilizados. La herramienta le ayuda a navegar por las tablas y archivos de la base de datos en pasos sucesivos y muestra el espacio actual ocupado en el sistema de archivos por los elementos respectivos. Una vez que haya seleccionado las tablas y los archivos de la base de datos que se van a eliminar, la herramienta los elimina del sistema de archivos después de la confirmación.

Cómo utilizar el script de recuperación de bases de datos de NetScaler ADM para una implementación independiente de NetScaler ADM

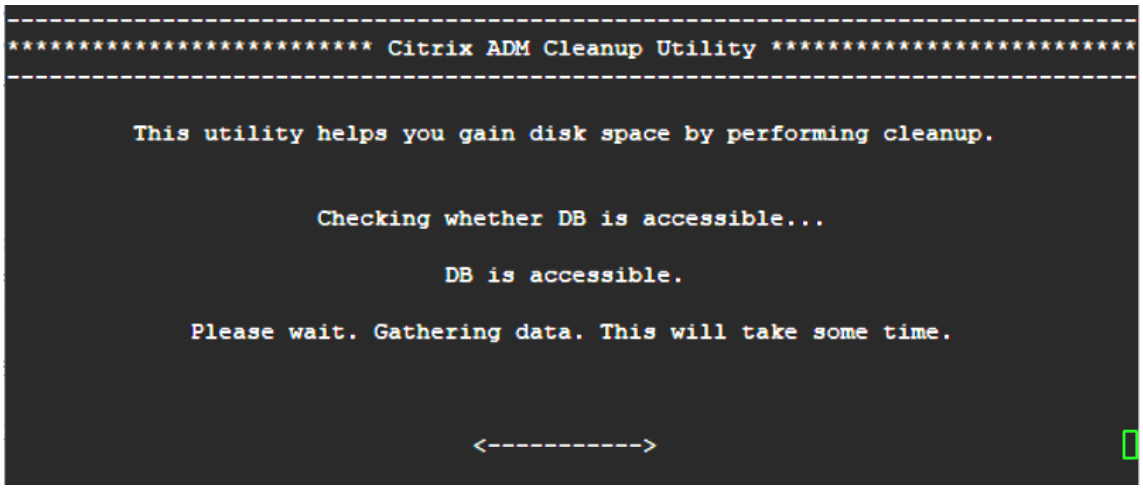
Utilice el procedimiento siguiente en un único servidor de implementación de NetScaler ADM para conectarse al sistema de archivos, eliminar algunos componentes y hacer accesible la base de datos y, a continuación, realizar las operaciones de recuperación.

1. Con un cliente SSH o la consola del hipervisor, inicie sesión en Citrix ADM y escriba el siguiente comando:

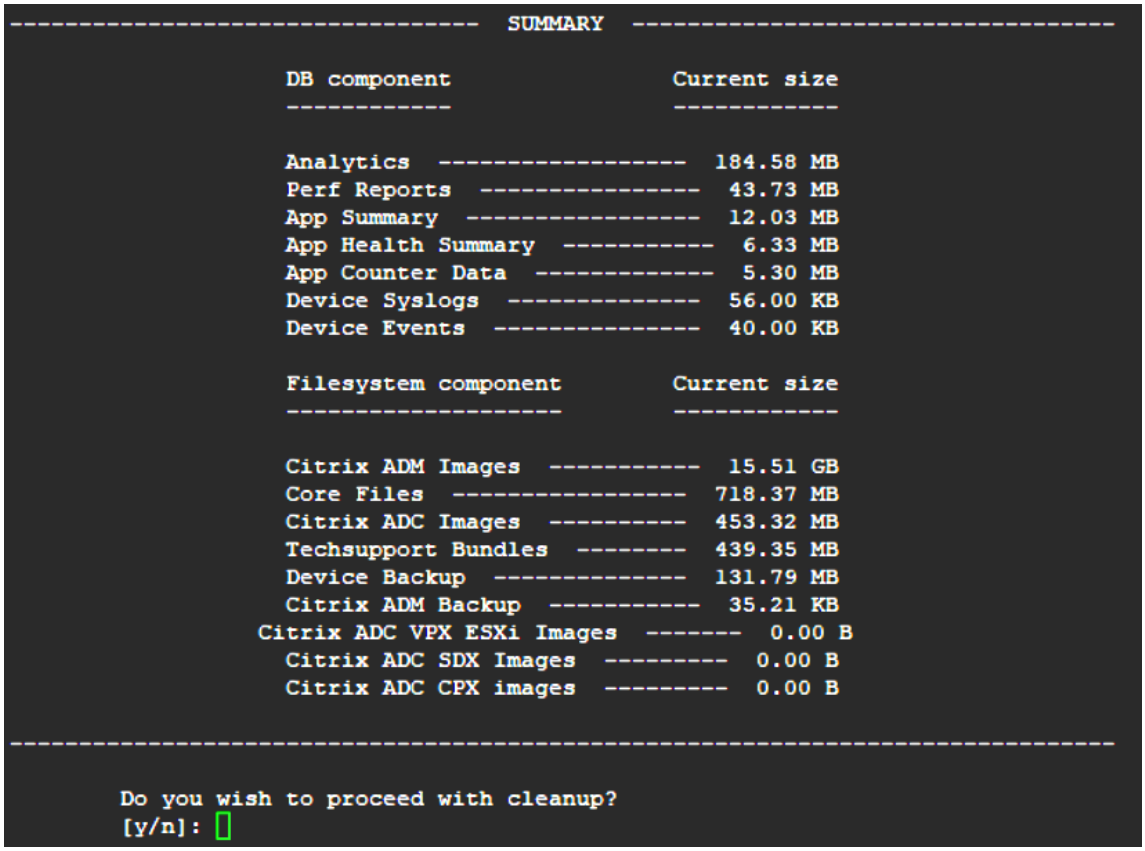
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. Cuando la pantalla muestre un mensaje de advertencia para detener algunos procesos NetScaler ADM, escriba "y"y presione la tecla **Intro**.

   La siguiente pantalla aparece mientras el sistema determina qué componentes de la base de datos puede eliminar sin afectar a los archivos principales del sistema.



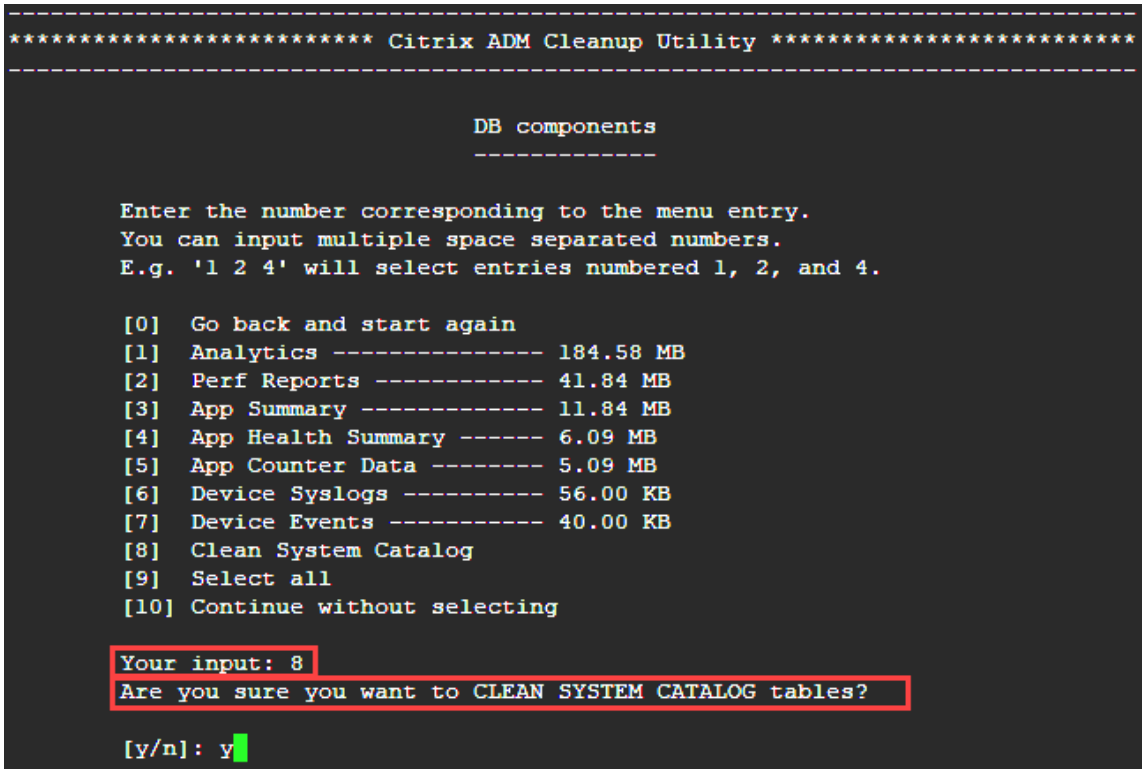
3. La pantalla muestra la lista de archivos de la base de datos. Escriba "y"y pulse la tecla Enter para iniciar el proceso de limpieza.



4. Puede seleccionar el componente específico de la base de datos que debe limpiarse y escribir el número correspondiente. Presiona la tecla **Enter**.

   Por ejemplo, para limpiar el catálogo de sistemas, seleccione la opción 8 en el menú de selección **de componentes** de la base de datos, escriba "y"y pulse la tecla **Enter** para continuar con la limpieza del catálogo del sistema.

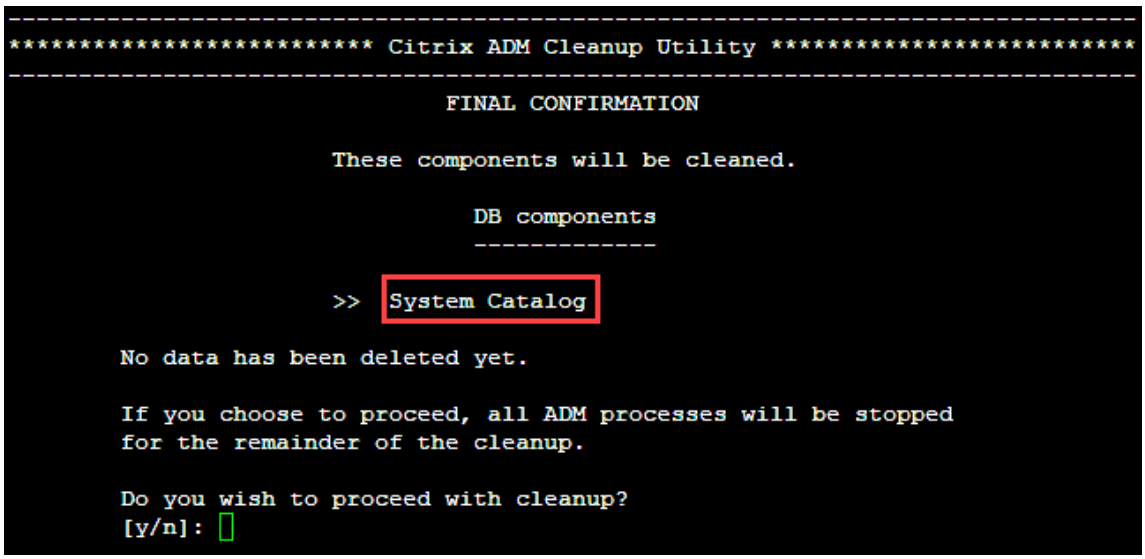
   > **Nota** Citrix ADM incluye tablas de usuarios conocidas como catálogo del sistema. El catálogo del sistema es una ubicación de la base de datos Citrix ADM donde un sistema de administración de bases de datos relacionales almacena los metadatos del esquema, como la información sobre tablas y columnas y los registros internos. Las tablas del catálogo del sistema son como las tablas normales que pueden acumular filas infladas y muertas con el tiempo y, por lo tanto, necesitan limpiarse periódicamente para obtener un rendimiento óptimo. Es una buena práctica mantener estas tablas con regularidad. La actividad no solo libera espacio en disco, sino que también mejora el rendimiento general de la base de datos y, por lo tanto, del Citrix ADM.



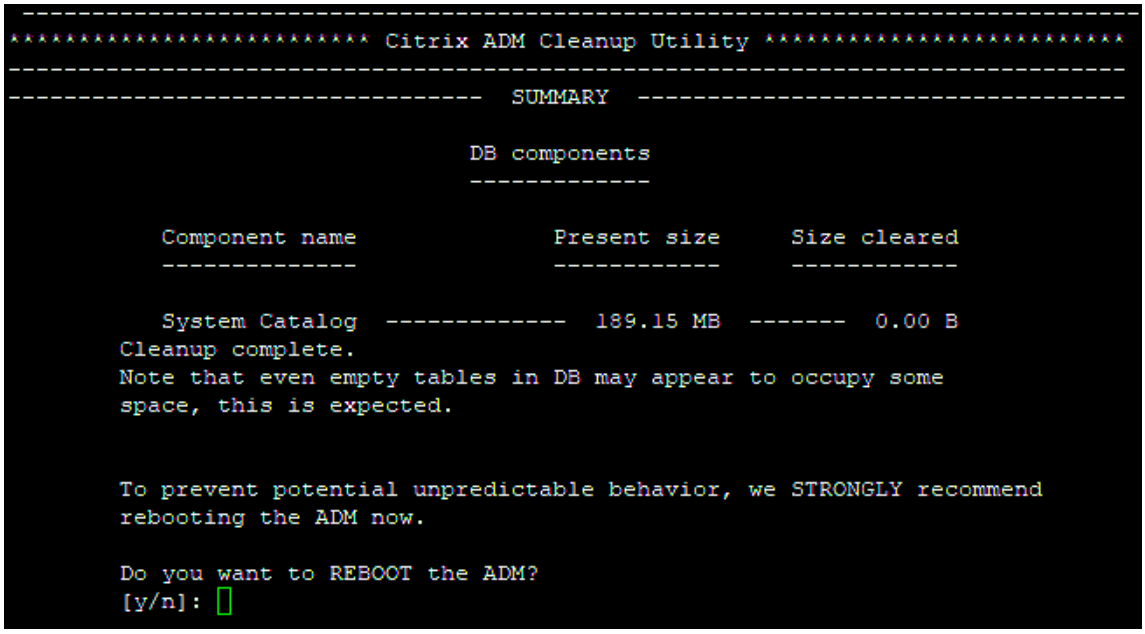
La utilidad de limpieza ofrece la opción de limpiar los componentes de la base de datos y los componentes de archivos. Puede seleccionar cualquier componente del archivo escribiendo un número entre "1"y "9", o escribir "11"y pulsar la tecla Enter para limpiar el componente de la base de datos.

> **Nota:**
>
> El número "11"indica que no ha seleccionado ningún componente de archivo para limpiarlo y que continúa limpiando el componente de base de datos anterior que había seleccionado anteriormente. En este ejemplo, es "catálogo del sistema".

5. Escriba "y"y vuelva a pulsar la tecla **Enter** en la pantalla de confirmación final.



Se limpia el catálogo del sistema, lo que puede llevar tiempo según el tamaño de la tabla del catálogo del sistema. Una vez finalizado el proceso, aparece una pantalla de resumen.



6. Escriba «y» y pulse la **tecla**Intro para reiniciar Citrix ADM.

   Asegúrese de reiniciar Citrix ADM después de limpiar el sistema. Espere unos 30 minutos para que las operaciones internas de la base de datos se completen después de que NetScaler ADM se haya reiniciado. A continuación, debe poder conectarse a la base de datos Citrix ADM. Si no es así, vuelva a ejecutar el script de recuperación para liberar más espacio. Cuando Citrix ADM está en funcionamiento, debe funcionar según lo esperado.

   > **Nota**
   >
   > El tamaño actual de la tabla de catálogo del sistema nunca es igual a cero después de la limpieza. Esto se debe a que solo se eliminan las filas vacías de la tabla y es posible que la tabla tenga algunas entradas válidas incluso después de limpiarlas.

Cómo utilizar el script de recuperación de bases de datos Citrix ADM para una implementación de alta disponibilidad de Citrix ADM

El sistema de bases de datos para los servidores Citrix ADM en una implementación de alta disponibilidad está en modo de sincronización continua. Al utilizar la nueva herramienta de recuperación de bases de datos, no es necesario replicar el procedimiento en ambos servidores Citrix ADM.

1. Con un cliente SSH o la consola de un hipervisor, inicie sesión en el nodo principal.
2. Ejecute este comando:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. Siga el procedimiento del paso 2 disponible para el script de recuperación de implementación independiente de NetScaler ADM

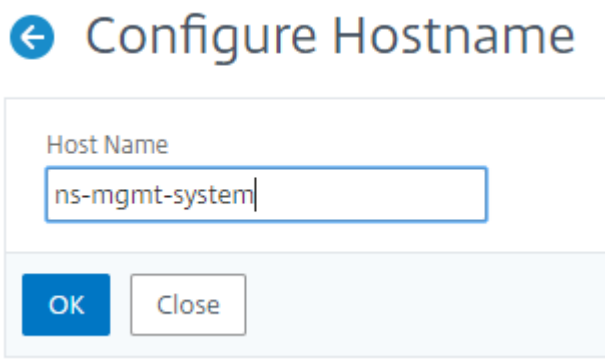
Asignar un nombre de host a un servidor NetScaler ADM

January 30, 2024

Para identificar un servidor de NetScaler Application Delivery Management (ADM), puede asignarle un nombre de host. El nombre del host se muestra en la licencia universal de NetScaler ADM.

Para asignar un nombre de host a un servidor de NetScaler ADM:

1. En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**.
2. En **Configuración del sistema**, haga clic en **Cambiar nombre de host**.
3. En la página **Configurar nombre de host**, escriba un nombre de host y haga clic en **Aceptar**.



Copia de seguridad y restauración del servidor NetScaler ADM

January 30, 2024

Puede realizar copias de seguridad periódicas de su servidor Citrix ADM. Puede realizar copias de seguridad y restaurar los archivos de configuración, los detalles de la instancia, los datos del sistema, etc. Antes de actualizar, realice una copia de seguridad de los archivos de configuración del servidor ADM por razones de precaución.

La copia de seguridad incluye los siguientes componentes:

- Archivos de configuración de Citrix ADM:
  - SNMP
  - Archivos de configuración del servidor Syslog
  - archivos NTP

  - Certificados de SSL
  - Archivos del Centro de control
- Copias de seguridad de las instancias de Citrix ADC que administra el servidor Citrix ADM.
- Plantillas de auditoría de configuración.
- Datos del sistema almacenados en la base de datos:
  - Lista de arrendatarios y usuarios creada.
  - Configuración del servidor de autenticación externo (LDAP, RADIUS y otros).
  - Se crearon trabajos de configuración y plantillas de trabajo.
- Datos de infraestructura y aplicaciones almacenados en la base de datos:
  - Datos de instancias de Citrix ADC agregadas y administradas.
  - Detalles del perfil de la instancia, detalles de la versión, detalles del grupo de instancias, etc.
  - Aplicación estática (grupo de servidores virtuales) creada por el administrador.
- Configuración SNMP.

> **Nota**
>
> Los datos de Analytics, los eventos y los mensajes de syslog se excluyen de la copia de seguridad.

Respaldar la configuración de NetScaler ADM

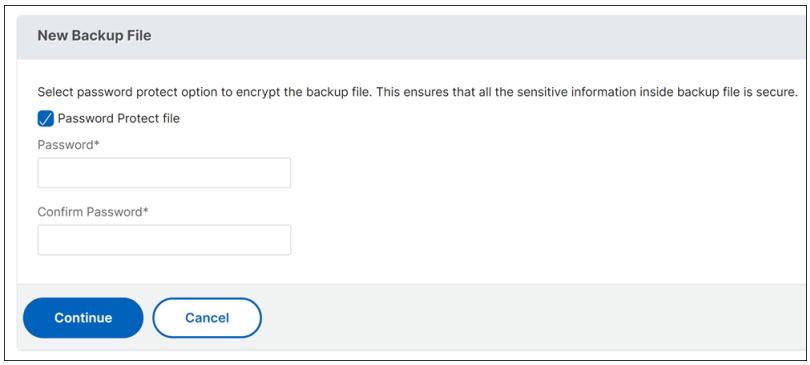
De forma predeterminada, el servidor Citrix ADM hace copias de seguridad de la configuración cada 24 horas (a las 00:30 horas). También puede programar y seleccionar la hora de la copia de seguridad. Además, puede mover una copia del archivo de la copia de seguridad a otro sistema.

La copia de seguridad se almacena como un archivo TAR comprimido que también se puede cifrar. De forma predeterminada, se conservan tres archivos de respaldo en el servidor. Para evitar problemas de espacio bajo en disco, puede almacenar un máximo de 10 archivos de copia de seguridad en el servidor NetScaler ADM. Sin embargo, Citrix recomienda almacenar algunas copias de los archivos de copia de seguridad en el servidor o transferir los archivos a otro sistema como medida de precaución.

Para realizar una copia de seguridad de una configuración de NetScaler ADM:

1. Vaya a **Sistema** > **Configuración avanzada** > **Archivos de copia de seguridad**y, a continuación, haga clic en Realizar **copia de**seguridad.

2. Para cifrar el archivo de copia de seguridad, active la casilla de verificación **Archivo Proteger con contraseña** y, a continuación, proporcione una contraseña para cifrar el archivo.



> **Nota**
>
> También puede configurar un archivo de respaldo para el cifrado; para ello, vaya a **Sistema** > **Configuración de copia de seguridad del sistema** y, a continuación, seleccione **Cifrar archivo** de copia de seguridad.

Transferir un archivo de copia de seguridad NetScaler ADM a un sistema externo

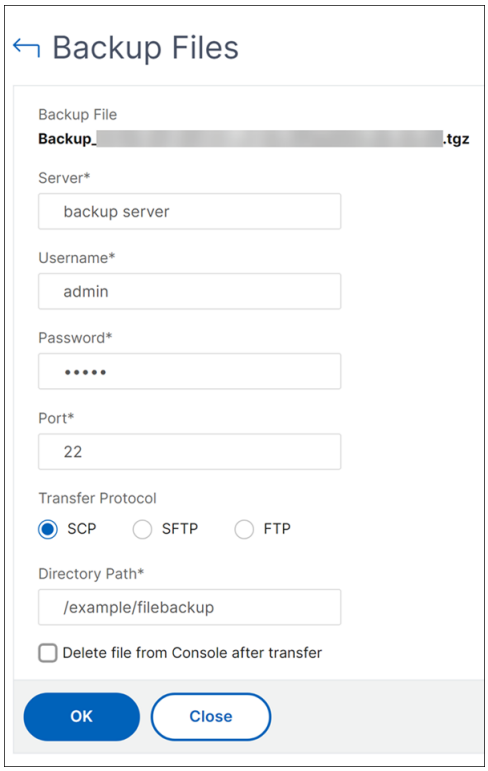
Puede transferir una copia del archivo de copia de seguridad a otro sistema como medida de precaución. Cuando quiera restaurar la configuración, primero cargue el archivo en el servidor NetScaler ADM y, a continuación, realice la operación de restauración.

Para transferir un archivo de copia de seguridad de Citrix ADM:

1. Vaya a **Sistema** > **Configuración avanzada** > **Archivos** de respaldo .
2. Seleccione el archivo de copia de seguridad que quiere mover a otro sistema y, a continuación, haga clic en**Transferir**.
3. En la página **Archivos de respaldo**, especifique los siguientes parámetros:
   - **Servidor**: Dirección IP del sistema al que desea transferir el archivo de la copia de seguridad.
   - **Nombre de usuario y contraseña**: Credenciales de usuario del nuevo sistema en el que se copian los archivos de la copia de seguridad.
   - **Puerto**: Número de puerto del sistema al que se transfieren los archivos.
   - **Protocolo de transferencia**: Protocolo que se utiliza para realizar la transferencia del archivo de respaldo. Puede seleccionar los protocolos SCP, SFTP o FTP para transferir el archivo de la copia de seguridad.
   - **Ruta del directorio**: La ubicación a la que se transfiere el archivo de copia de seguridad en el nuevo sistema.

Como alternativa, también puede configurar los detalles del sistema externo navegando hasta **Sistema**> Configuración de copia de seguridad del **sistema** .

4. Puede eliminar el archivo de copia de seguridad de NetScaler ADM después de la transferencia activando la casilla de verificación **Eliminar archivo de Administración de entrega de aplicaciones después de la transferencia**.
5. Haga clic en **Aceptar** para realizar la transferencia.



> **Nota**
>
> Para guardar una copia del archivo de respaldo en su sistema local, vaya a **Sistema** > **Configuración avanzada** > Archivos de **respaldo** , seleccione el archivo que desea copiar y, a continuación, haga clic en **Descargar** .

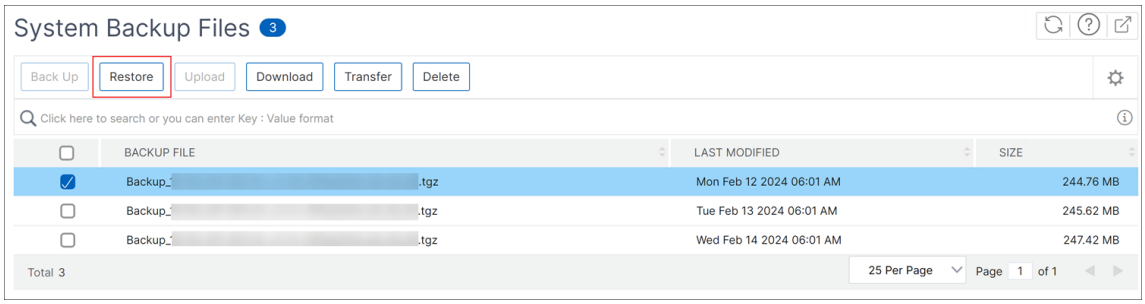
Restaurar la configuración de NetScaler ADM desde un archivo de copia de seguridad

Al restaurar la configuración de Citrix ADM a partir de un archivo del que se hizo una copia de seguridad anteriormente, la operación de restauración desactiva el archivo de copia de seguridad y, a continuación, restaura la configuración. La operación de restauración elimina la configuración existente y la reemplaza por la configuración del archivo de copia de seguridad.

> **Nota**
>
> La operación de restauración falla si se cambia el nombre del archivo de copia de seguridad o si se modifica el contenido del archivo de respaldo.

Para restaurar una configuración de NetScaler ADM a partir de un archivo de copia de seguridad:

1. Vaya a **Sistema** > **Configuración avanzada** > **Archivos de copia de seguridad**.
2. Seleccione el archivo de copia de seguridad que quiere restaurar y, a continuación, haga clic en **Restaurar**.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.



> **Nota**
>
> Para restaurar la configuración a partir de un archivo de copia de seguridad almacenado en un sistema externo, cargue el archivo de copia de seguridad en el servidor ADM antes de realizar la operación de restauración. Para cargar el archivo, vaya a **Sistema** > **Configuración avanzada** > **Archivos de copia**de seguridad y, a continuación, haga clic en **Cargar**.

Ver información de auditoría

January 24, 2024

Syslog es un protocolo estándar para el registro. Tiene dos componentes: el módulo de auditoría Syslog, que se ejecuta en la instancia Citrix Application Delivery Controller (ADC), y el servidor Syslog, que puede ejecutarse en el sistema operativo (SO) FreeBSD subyacente de la instancia Citrix ADC o en un sistema remoto. SYSLOG utiliza el Protocolo de datagramas de usuario (UDP) para la transferencia de datos.

Syslog permite el aislamiento del sistema que genera la información y del sistema que almacena la información. Puede consolidar la información de registro y obtener información de los datos recopilados. También puede configurar syslog para registrar diferentes tipos de eventos.

Puede supervisar los mensajes de syslog que genera un dispositivo Citrix ADC si configura el dispositivo para redirigir los mensajes de syslog a Citrix Application Delivery Management (ADM). Puede programar un trabajo para crear servidores syslog que generen diferentes tipos de datos syslog mediante la función de plantillas integradas de Citrix ADM.

Primero, configure un servidor syslog al que la instancia pueda enviar información de registro. A continuación, especifique el formato de fecha y hora para grabar los mensajes de registro.

Para configurar un servidor syslog en Citrix ADM:

1. Vaya a**Sistema**>**Auditoría.** En **Resumen de configuración**, seleccione Servidores **Syslog.** O puede ir a **Sistema** > **Auditoría > ServidoresSyslog**.
2. **En la página del**servidor Syslog**, haga clic en Agregar.**
3. En la página **Crear servidor de Syslog**, introduzca los siguientes valores:

    - **Nombre**: Nombre del servidor syslog.
    - **Dirección IP**: Dirección IP del servidor syslog.
    - **Puerto: puerto** del servidor Syslog.

4. Elija los niveles de registro (Todos, Ninguno o Personalizado). En consecuencia, seleccione los niveles de gravedad.
5. Haga clic en **Create**.

Para configurar el formato de fecha y hora de syslog en Citrix ADM:

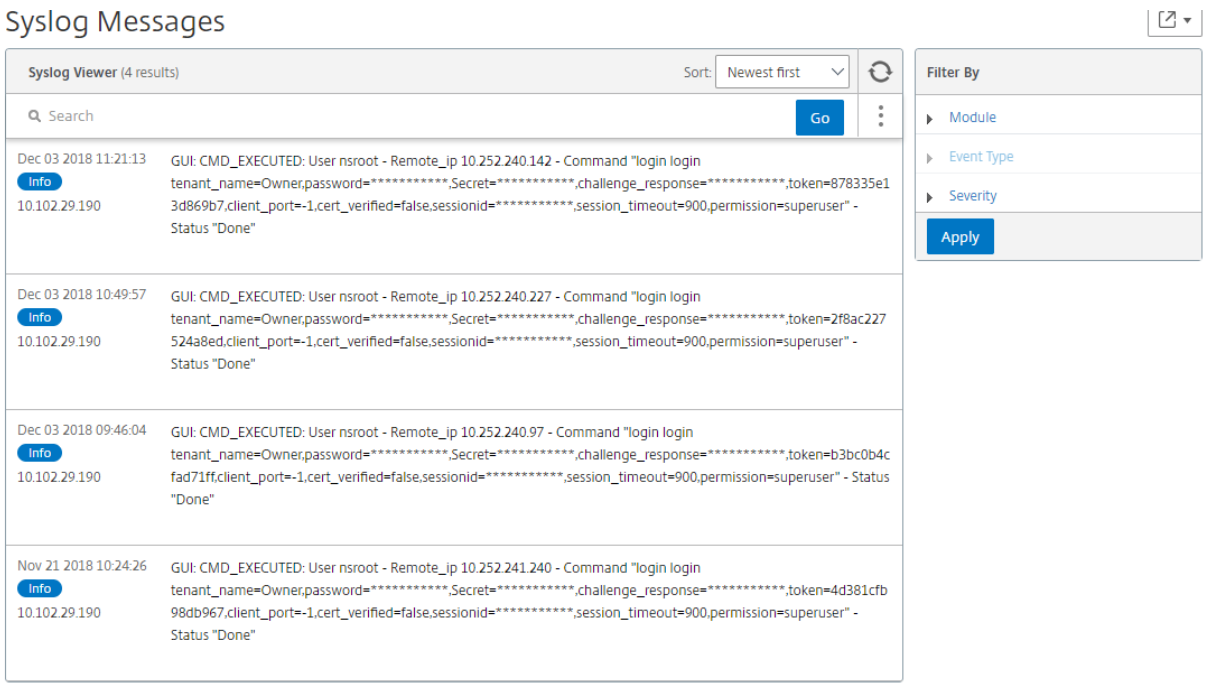
1. Vaya a**Sistema**>**Auditoría.** En**Resumen de configuración**, seleccione Servidores**Syslog.**
2. **En la página**Servidor Syslog, seleccione un servidor**syslog y, a continuación, haga clic en Parámetros de Syslog.**
3. En la página**Configurar parámetros de Syslog**, especifique el formato de fecha y hora.
4. Haga clic en **Aceptar**.

Para ver los mensajes de syslog en Citrix ADM:

Ahora puede ver todos los mensajes de syslog generados en las instancias administradas de Citrix ADC si ha configurado la instancia para redirigir los mensajes de syslog al servidor Citrix ADM. Los mensajes de syslog se almacenan en la base de datos del servidor Citrix ADM de forma centralizada y estarán disponibles en el Visor de Syslog para fines de auditoría. Puede consolidar esta información de registro y obtener informes para el análisis a partir de los datos recopilados.

Puede filtrar esta información por módulo, tipo de evento y gravedad. También puede configurar syslog para registrar diferentes tipos de eventos.

Para ver elvisor de Syslog**, vaya a**Sistema**> Auditoría.** En la página**de auditoría**, en Mensajes de**auditoría, seleccione Mensajes**de**Syslog**. Elija los filtros adecuados para ver los mensajes de registro del sistema.



Configurar la configuración de SSL

January 30, 2024

SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de redes de seguridad de uso común que proporcionan una comunicación cifrada entre los usuarios y los servidores. Puede configurar los parámetros de SSL en Citrix Application Delivery Management (ADM) y especificar el tipo de clientes que se conectan al sistema.

Para configurar los parámetros de SSL para Citrix ADM:

1. Vaya a **Sistema** > **Administración del sistema**. En **Configuración del sistema**, haga clic en **Configurar la configuración de SSL**.
2. En la página de **configuración SSL**, revise la configuración actual del protocolo y los conjuntos de cifrado aplicados al sistema.
3. Para modificar la configuración del protocolo, vaya a **Editar configuración** > **Configuración de protocolo** y realice los cambios que desee.
4. Para modificar los conjuntos de cifrado aplicados, vaya a **Editar configuración** > **Suites de cifrado** y realice los cambios que desee.
5. Haga clic en Aceptar **y**, a continuación, en **Cerrar** .

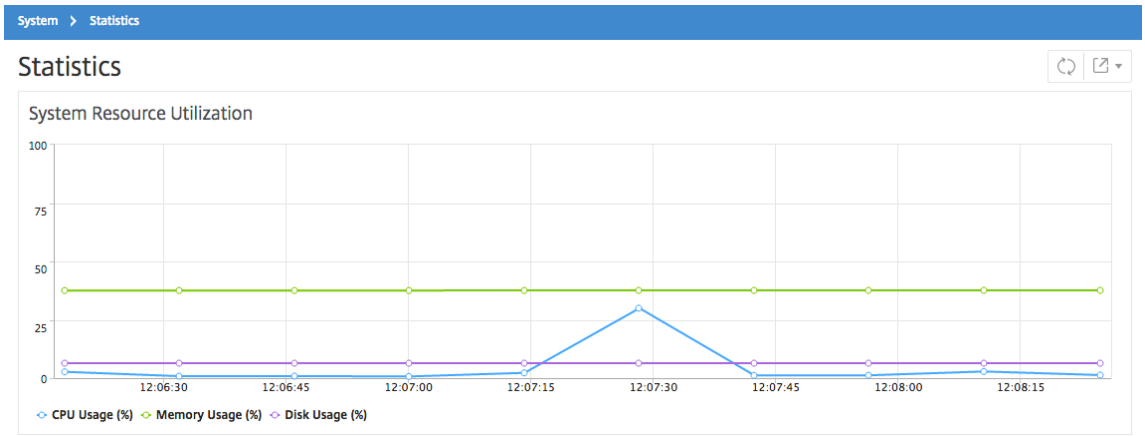
Supervisar el uso de CPU, memoria y disco

January 24, 2024

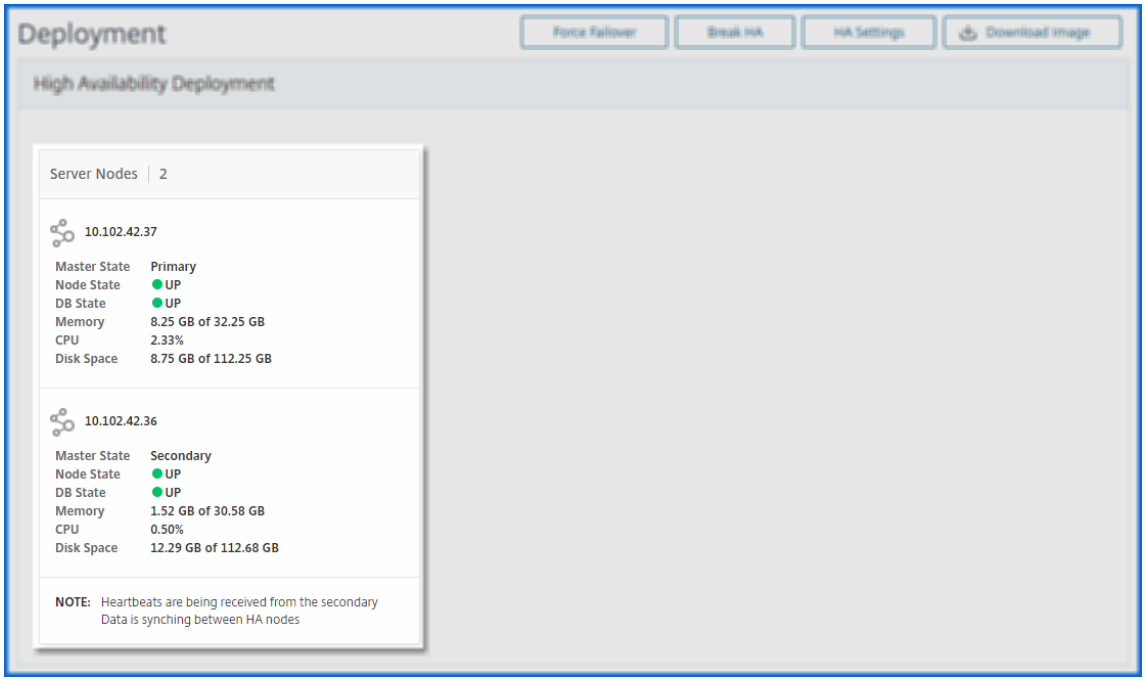
Puede utilizar la información mantenida en los registros y las estadísticas. Esta información también se muestra en los informes que ayudan a configurar y mantener Citrix Application Delivery Management (ADM).

Para supervisar el uso de la CPU, la memoria y el disco,

- **Implementación independiente.** Vaya a **Sistema** > **Estadísticas**. Puede ver gráficos de utilización de CPU, memoria y disco en tiempo real.



- **Implementación de alta disponibilidad.** Navegue hasta **Sistema** > **Implementación** . Las estadísticas de la memoria, la CPU, el espacio en disco y las instancias administradas se muestran numéricamente como se muestra en la siguiente ilustración:



Configurar las opciones de notificación del sistema

January 30, 2024

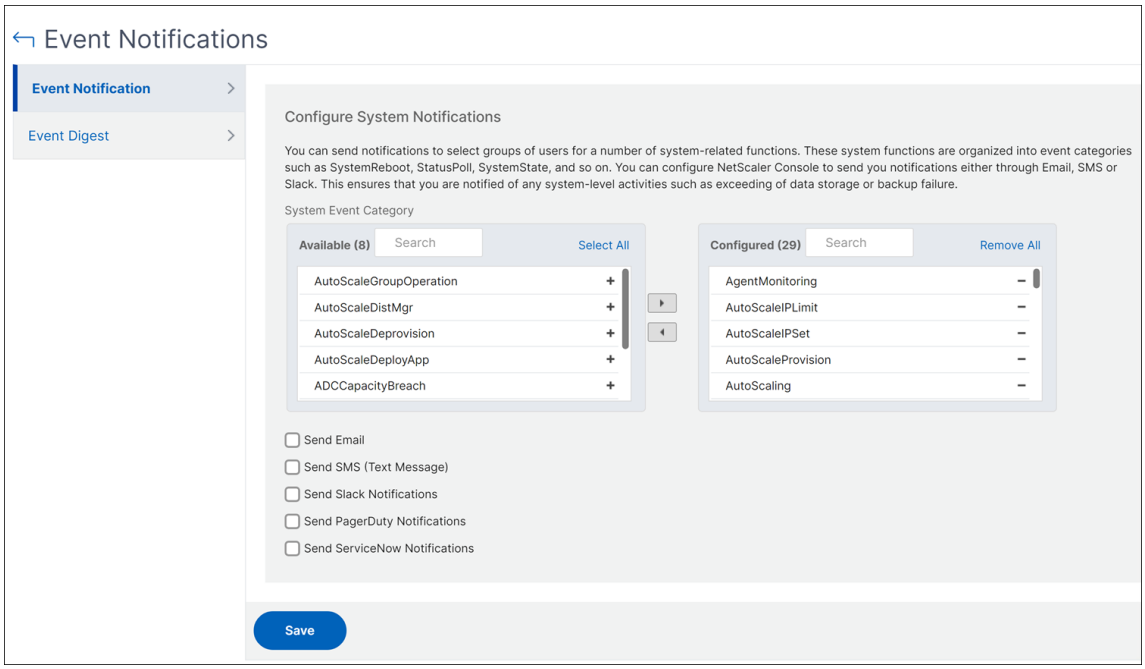
Puede enviar notificaciones a grupos de usuarios seleccionados para una serie de funciones relacionadas con el sistema. Estas funciones del sistema se organizan en categorías de eventos como SystemReboot, StatusPoll, SystemState, etc. Puede configurar NetScaler Application Delivery Management (ADM) para que le envíe notificaciones por correo electrónico o SMS. Debe configurar un servidor de correo electrónico o un servidor de puerta de enlace del servicio de mensajes cortos (SMS) para enviar notificaciones por correo electrónico y texto a los usuarios.Esto garantiza que se le notifique cualquier actividad a nivel del sistema, como el inicio de sesión del usuario o el reinicio del sistema.

Por ejemplo, es posible que desee enviar una notificación por correo electrónico a dos usuarios cuando alguien intente iniciar sesión en Citrix ADM mediante la CLI y el intento de inicio de sesión falle. Debe configurar la notificación del sistema seleccionando la categoría UserLogin y crear un servidor de notificaciones por correo electrónico o elegir una lista de distribución de correo electrónico existente a la que enviar la notificación.

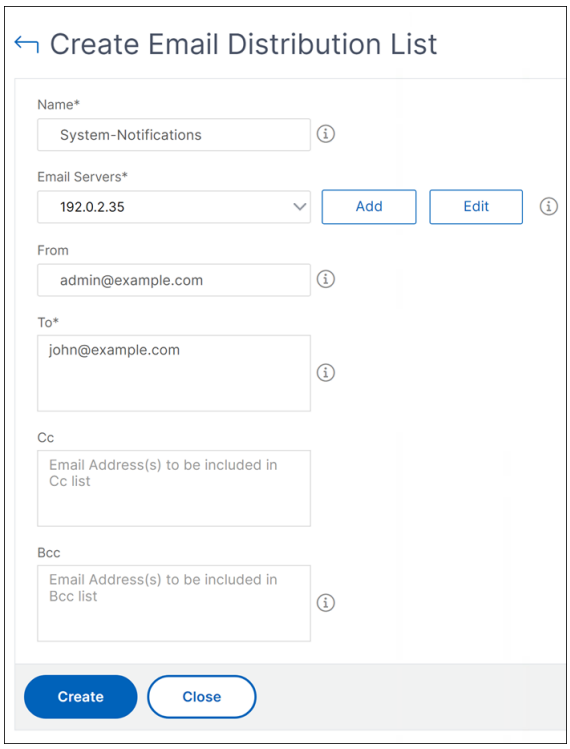
Para configurar los ajustes de notificación del sistema en Citrix ADM:

1. Vaya a **Sistema** > **Notificaciones**. En**Configuración**, haga clic en **Cambiar la configuración de notificaciones**.

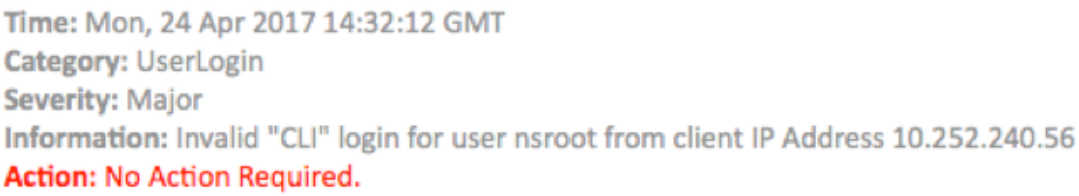
2. En la página **Configurar configuración de notificación del sistema**, en**Categoría**, seleccione una categoría como**UserLogin**.



3. Seleccione **Enviar correo** electrónico y seleccione una distribución de correo electrónico de la lista desplegable o haga clic en el icono « **+** » para crear una nueva lista de distribución de correo electrónico, como se muestra en la figura siguiente. Si quieres enviar notificaciones por texto, selecciona **Enviar SMS (mensaje de texto)**y crea una lista de distribución de SMS haciendo clic en el icono "**+**"y especificando los detalles del servidor de SMS.



Después de establecer las notificaciones para determinadas categorías de eventos, siempre que se produzca un evento perteneciente a esa categoría, se envía una notificación a los destinatarios mediante correo electrónico o SMS. En este ejemplo, puede ver una notificación por correo electrónico cuando un usuario no puede iniciar sesión en Citrix ADM mediante la CLI.



Las notificaciones del sistema se envían para los siguientes eventos:

Categoría	Causa
Fallo en la copia de seguridad	La copia de seguridad del sistema falla
Se ha superado el almacenamiento de datos	El almacenamiento de la base de datos supera el límite especificado en la licencia
DeviceBackupFailure	Se produce un error en la copia de seguridad de la instancia

Categoría	Causa
Supervisión de la HA	Se produce la conmutación por error de alta disponibilidad del sistema, no hay latidos del nodo del mismo nivel y se produce un error de sincronización de la base de datos
HealthMontoring	La utilización de la CPU, la RAM o el disco supera el valor umbral
Pool de licencias	El conjunto de licencias supera el valor umbral
Licencias	La licencia falla cuando se aplica
Recuperación de contraseña	La recuperación de la contraseña falla o se realiza correctamente
Umbral alto de PerfCounter	El valor del contador de rendimiento supera el límite
Umbral PerfCounter Normal	El valor del contador de rendimiento es normal
Directiva fallida	Se produce un error en alguna de las directivas del sistema
Fallo en la copia de seguridad del dispositivo remoto	La copia de seguridad de la instancia remota falla
RemoteSystemBackupFailure	La copia de seguridad remota del sistema falla
RemoteSystemBackupNormal	La copia de seguridad remota del sistema se realiza correctamente
SSLCertThreshold	Se ha superado el umbral de un certificado
StatusPoll	Cualquier cambio en el estado de una instancia
Estado del subsistema	Cualquier cambio en el estado del subsistema
Reinicio del sistema	Se reinicia el sistema
Estado del sistema	Cualquier cambio en el estado del sistema
Fallo de TrapConfig	Se produce un error al agregar una captura SNMP en una instancia
Inicio de sesión de usuario	Error en la autenticación de usuario

Generar un archivo de soporte técnico

January 30, 2024

Citrix recomienda generar un archivo de datos y estadísticas de NetScaler Application Delivery Management (ADM) antes de ponerse en contacto con el soporte técnico para solucionar un problema. El archivo es un archivo TAR que puede enviar al equipo de soporte técnico.

> **Nota**
>
> Para los servidores Citrix ADM en modo de alta disponibilidad, puede generar un archivo de soporte técnico desde cualquiera de los servidores. Citrix recomienda no utilizar la dirección IP del servidor virtual de equilibrio de carga para generar el archivo de soporte técnico.

Para configurar y enviar un archivo de soporte técnico desde NetScaler ADM:

1. Vaya a **Sistema** > **Diagnóstico** > **Soporte técnico y, a**continuación, haga clic en **Generar archivo de soporte técnico**.
2. En la página **Generar archivo de soporte**, seleccione las siguientes opciones:

- **Recopilar registros de depuración : seleccione esta opción para recopilar los registros del decodificador**.
- **Duración**: introduzca la duración durante la que se deben recopilar los registros de depuración. Solo verá esta opción si activa la opción **Recopilar registros de depuración**.
- **Recopilar distribución de datos**: Seleccione esta opción para recopilar registros distintos y diversos de la base de datos.

```
The archive file is created as a TAR file.

For example, the archive file that is created might be named as
   follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
   tar.gz
```

1. Puede enviar los archivos de soporte técnico al equipo de soporte de dos maneras:

   a) Puede descargar el archivo de la GUI de ADM a su almacenamiento local y, a continuación, utilizar un navegador web para cargarlo en CIS.

   b) También puede cargar los archivos de soporte técnico al sitio web de Citrix Insight Services (CIS) ejecutando un script en la consola ADM.

      i. Mediante SSH, inicie sesión en la consola ADM.

      ii. Cambie a la línea de comandos de Shell y escriba:

      /mps/collector_upload.pl

El comando completo se muestra a continuación con los atributos que debe proporcionar:

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
   proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
    <sr>] [-description <description>] [-debug] <file>
```



```
<!--NeedCopy-->
```

La ventaja de ejecutar el script de Perl es que no tiene que descargar el archivo de soporte técnico de ADM a su sistema local y luego subirlo a CIS. Como opción, puede cargar el archivo en CIS directamente mediante un proxy de la consola ADM.

Asegúrese de tener una cuenta en CIS. Puede usar las credenciales de su cuenta de Citrix para cargar archivos a CIS.

¿Qué pasa si no tiene un servidor proxy? ¿O qué pasa si tiene algunos problemas con los proxies de reenvío SSL? (Esto puede ocurrir si el script de Perl no confía en el certificado raíz del servidor proxy) . Aún puede cargar el archivo directamente desde el shell ADM a CIS.

> **Nota:**
>
> Puede seguir descargando el archivo y enviarlo por correo electrónico al equipo de soporte técnico de Citrix en caso de que ADM no pueda cargar el archivo a CIS desde la consola. O bien, puede descargar el archivo de ADM a su almacenamiento local y, a continuación, utilizar un navegador web para cargarlo en CIS.

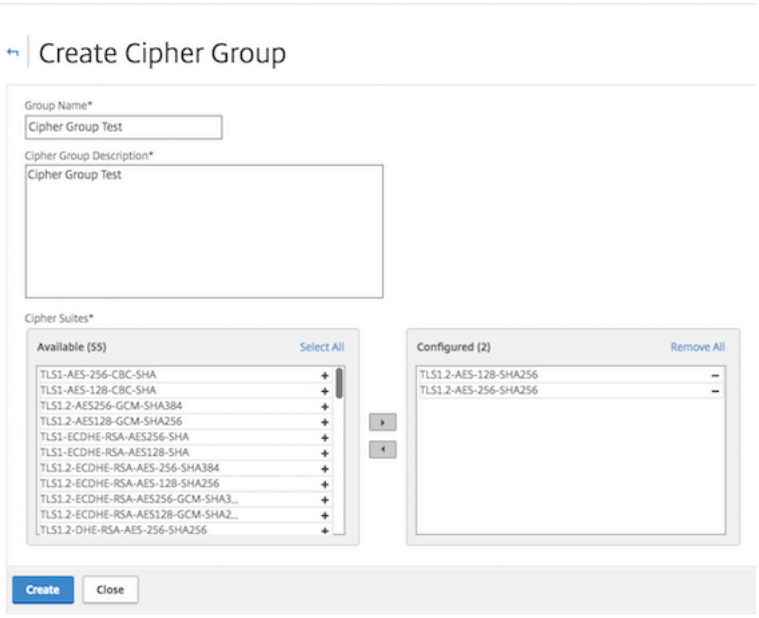
Configurar un grupo de cifrado

January 24, 2024

Un grupo de cifrado es un conjunto de conjuntos de cifrado que se vincula a un servidor virtual SSL, servicio o grupo de servicios en la instancia de Citrix Application Delivery Controller (ADC). Un conjunto de cifrado comprende un protocolo, un algoritmo de intercambio de claves (Kx), un algoritmo de autenticación (Au), un algoritmo de cifrado (Enc) y un algoritmo de código de autenticación de mensajes (Mac).

Para agregar un grupo de cifrado en NetScaler ADM:

1. Vaya a **Sistema** > **Grupos de cifrado** y, a continuación, haga clic en **Agregar** .
2. En la página **Crear Grupo de Cifrados**, introduzca los siguientes detalles:
    - **Nombre del grupo**: Nombre del grupo de cifrado.
    - **Descripción del grupo de cifrado**: Proporcione una descripción del grupo de cifrado.
    - Conjuntos de**cifrado: haga clic en Agregar para seleccionar los conjuntos** de cifrado de la lista Disponible y, a continuación, mover los conjuntos de cifrado seleccionados (o todos) a la lista configurados.
3. Haga clic en **Crear**.



Crear destino de capturas SNMP, comunidad de administradores y usuarios

January 30, 2024

Siempre que se produce una condición anormal en el Citrix ADM, se genera una captura de SNMP. A continuación, las capturas se envían a un dispositivo remoto denominado servidor de destino de capturas o *destino de capturas SNMP* . Puede consultar al agente SNMP para obtener información específica del sistema desde un dispositivo remoto denominado *administrador SNMP*. A continuación, el agente busca en la base de información de administración (MIB) los datos solicitados y los envía al administrador SNMP.

Para crear un destino de captura SNMP en Citrix ADM:

1. Vaya a **Sistema** > **SNMP** > **Destinos de captura**.
2. En **CapTURAS SNMP**, haga clic en **Agregar** para crear una captura SNMP y, a continuación, especifique los siguientes detalles:
   - **Versión.** Seleccione la versión de SNMP que desee utilizar.
   - **Servidor de destino.** Nombre o dirección IP del destino de la trampa.
   - **Puerto.** Introduzca el puerto de destino de la trampa. El puerto está configurado en 162 de forma predeterminada.

- **Comunidad.** Especifique la cadena de comunidad que se utilizará al enviar una trampa al oyente de la trampa.

3. Haga clic en **Crear**.

> **Nota**
>
> Si está creando un destino de captura SNMP v3, especifique las credenciales de usuario de SNMP a las que desea vincular la captura. Para agregar una credencial de usuario de SNMP, haga clic en **Insertar** y, a continuación, agregue el usuario de la lista de usuarios de SNMP disponibles.

Para crear una comunidad de administradores de SNMP:

1. Vaya a **Sistema** > **SNMP** > **Gestores**.
2. En **SNMP Manager**, haga clic en **Agregar** para crear una comunidad de administradores de SNMP y, a continuación, especifique los siguientes detalles:
   - **Gestor SNMP.** Introduzca el nombre o la dirección IP del administrador SNMP.
   - **Comunidad.** Especifique la cadena de comunidad que se utilizará al enviar las trampas al oyente de trampas.
3. Si lo desea, puede seleccionar la casilla **Habilitar red de administración** para especificar la máscara de **red, que es la máscara**de subred de la red del administrador de SNMP.
4. Haga clic en **Crear**.

Para crear un usuario SNMP:

1. Vaya a **Sistema** > **SNMP** > **Usuarios**.
2. En **Usuario SNMP**, haga clic en **Agregar**.
3. Introduzca el nombre de usuario y asigne un nivel de seguridad al usuario desde el menú.
4. En función del nivel de seguridad asignado al usuario, proporcione protocolos de autenticación adicionales, como protocolos de autenticación, contraseñas de privacidad y asigne vistas SNMP.

Configurar y ver alarmas del sistema

January 30, 2024

Puede habilitar y configurar un conjunto de alarmas para supervisar el estado de sus servidores NetScaler Application Delivery Management (ADM). Debe configurar las alarmas del sistema para

asegurarse de estar al tanto de cualquier problema crítico o importante del sistema. Por ejemplo, es posible que quiera recibir una notificación si el uso de CPU es alto o si hay varios errores de inicio de sesión en el servidor. Para algunas categorías de alarmas, como cpuUsageHigh o memoryUsageHigh, puede establecer umbrales y definir la gravedad (como Crítica o Mayor) de cada una. Para algunas categorías, como InventoryFailed o LoginFailure, solo puede definir la gravedad. Cuando se supera el umbral de una categoría de alarma (por ejemplo, MemoryUsageHigh) o cuando se produce un evento correspondiente a la categoría de alarma (por ejemplo, **LoginFailure**), se graba un mensaje en el sistema y puede verlo como mensaje de syslog. Además, puede configurar las notificaciones para recibir un correo electrónico o un SMS correspondiente a la configuración de la alarma.

Puede asignar o modificar la gravedad de una alarma. Los niveles de gravedad que puede asignar son Crítico, Principal, Menor, Advertencia e Informativo.

Considere un caso en el que desee supervisar cada vez que se produzca un intento fallido de copia de seguridad. Puede activar la alarma BackupFailed y asignarle una gravedad, como Mayor. Siempre que NetScaler ADM intente realizar una copia de seguridad de los archivos del sistema y cuando el intento falla, se activa una alarma. Puede ver el mensaje en Citrix ADM u recibir notificaciones por correo electrónico o SMS.

Para configurar la alarma, debe seleccionar la alarma BackupFailed y especificar el nivel de gravedad como Principal. La alarma está activada de forma predeterminada.

Para configurar y ver una alarma del sistema mediante NetScaler ADM:

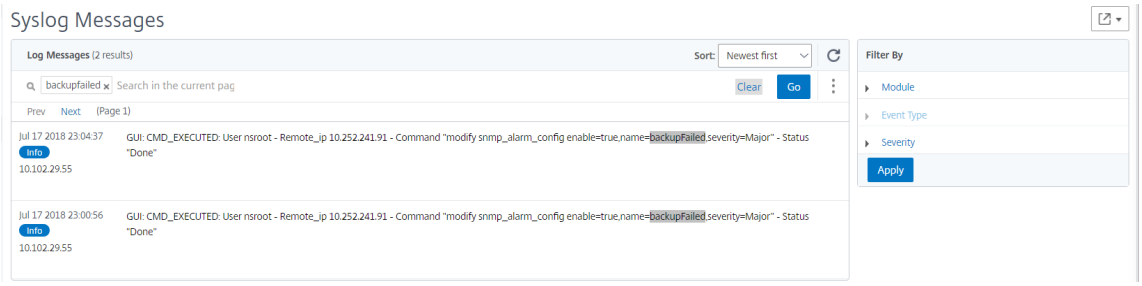
1. Navegue hasta **Sistema** > **Alarmas** .

2. Seleccione la alarma que desee configurar (por ejemplo, BackupFailed) y haga clic en **Editar** para modificar su configuración.
3. La alarma está activada de forma predeterminada. Asigne un nivel de gravedad (ejemplo: Principal) y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Para algunas alarmas, no puede establecer un umbral.
> Cuando se activa la alarma, puede ver el evento generado como un mensaje de syslog.

Para ver el evento generado por la alarma BackupFailed mediante Citrix ADM:

1. Vaya a**Sistema**>**Auditoría.**
2. En la página**de auditoría**, en Mensajes de**auditoría, seleccione Mensajes**de**Syslog**.
3. En el campo de búsqueda, escriba el nombre de la alarma.
   En este ejemplo, puede ver que se generó un evento para un intento de copia de seguridad fallido.



   También puede configurar notificaciones para enviarle un correo electrónico o un texto SMS (Servicio de mensajes cortos) cuando se activa una alarma. Para obtener información sobre cómo configurar las notificaciones del sistema, consulte Cómo configurar los valores de notificación del sistema de NetScaler ADM.

NetScaler ADM como servidor proxy API

January 30, 2024

Además de poder recibir solicitudes de API REST de NITRO para sus propias funciones de administración y análisis, Citrix Application Delivery Management (Citrix ADM) puede funcionar como un servidor proxy de API REST para sus instancias administradas. En lugar de enviar solicitudes de API directamente a las instancias administradas, los clientes de API REST pueden enviar las solicitudes de API a Citrix ADM. Citrix ADM puede diferenciar entre las solicitudes de API a las que debe responder y las solicitudes de API que debe reenviar sin cambios a una instancia administrada.

Como servidor proxy de API, Citrix ADM le ofrece las siguientes ventajas:

- **Validación de solicitudes de API**. Citrix ADM valida todas las solicitudes de API comparándolas con las políticas configuradas de seguridad y control de acceso basado en roles (RBAC). Citrix ADM también reconoce a los inquilinos y garantiza que la actividad de las API no sobrepase los límites de los inquilinos.
- **Auditoría centralizada**. Citrix ADM mantiene un registro de auditoría de toda la actividad de la API relacionada con sus instancias administradas.
- **Administración de sesiones**. NetScaler ADM libera a los clientes de API de la tarea de mantener sesiones con instancias administradas.

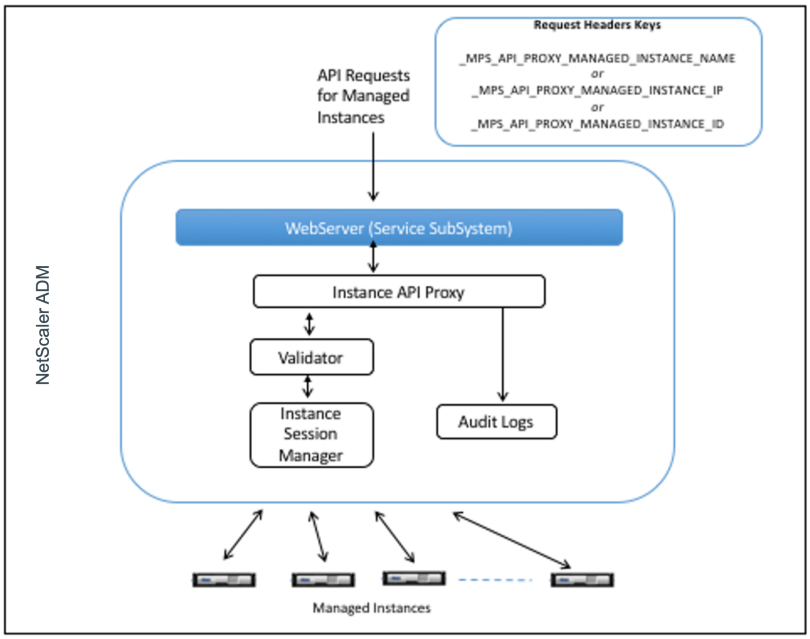
Cómo funciona Citrix ADM como servidor proxy de API

Cuando quiere que NetScaler ADM reenvíe una solicitud a una instancia administrada, configure el cliente de API para que incluya cualquiera de los siguientes encabezados HTTP en la solicitud de API:

- _MPS_API_PROXY_MANAGED_INSTANCE_NAME. Nombre de la instancia administrada.
- _MPS_API_PROXY_MANAGED_INSTANCE_IP. Dirección IP de la instancia administrada.
- _MPS_API_PROXY_MANAGED_INSTANCE_ID. ID de la instancia administrada.

La presencia de cualquiera de estos encabezados HTTP ayuda a NetScaler ADM a identificar una solicitud de API como una que debe reenviar a una instancia administrada. El valor del encabezado ayuda a Citrix ADM a identificar la instancia administrada a la que debe reenviar la solicitud.

Este flujo se representa en la siguiente ilustración:



Como se muestra en la ilustración anterior, cuando uno de estos encabezados HTTP aparece en una solicitud, NetScaler ADM procesa la solicitud de la siguiente manera:

1. Sin modificar la solicitud, Citrix ADM la reenvía al motor proxy de la API de la instancia.
2. El motor proxy de la API de instancia reenvía la solicitud de API a un validador y registra los detalles de la solicitud de API en el registro de auditoría.
3. El validador se asegura de que la solicitud no infrinja las directivas de seguridad configuradas, las directivas de RBAC, los límites de arrendamiento, etc. Realiza comprobaciones adicionales, como una comprobación para determinar si la instancia administrada está disponible.

Si la solicitud de API es válida y se puede reenviar a la instancia administrada, Citrix ADM identifica una sesión que mantiene el administrador de sesiones de la instancia y, a continuación, envía la solicitud a la instancia administrada.

Cómo usar NetScaler ADM como servidor proxy API

En los siguientes ejemplos se muestran las solicitudes de API REST que un cliente de API envía a un servidor Citrix ADM que tiene una dirección IP de 192.0.2.5. Se requiere Citrix ADM para reenviar las solicitudes, sin cambios, a una instancia gestionada con la dirección IP 192.0.2.10. Todos los ejemplos utilizan el encabezado _MPS_API_PROXY_MANAGED_INSTANCE_IP.

Antes de enviar a Citrix ADM las solicitudes de API, el cliente de API debe:

- Inicie sesión en Citrix ADM
- Obtener un identificador de sesión
- Incluye el ID de sesión en las solicitudes de API posteriores.

La solicitud de la API de inicio de sesión tiene el siguiente formato:

```
    POST /nitro/v2/config/login HTTP/1.1
    Host: 192.0.2.5
    Content-Type: application/json
    Accept: application/json
    Cache-Control: no-cache

    {

        "login":
        {

            "username":"******",
            "password":"*******"
         }

     }

<!--NeedCopy-->
```

Citrix ADM responde a la solicitud de inicio de sesión con una respuesta que incluye el identificador de sesión. El siguiente ejemplo de cuerpo de respuesta muestra un identificador de sesión:

```
{


  "errorcode": 0,
  "message": "Done",
  "operation": "add",
  "resourceType": "login",
  "username": "***********",
```



```
  "tenant_name": "Owner",
  "resourceName": "******",
  "login": [
    {

      "tenant_name": "Owner",
      "permission": "superuser",
      "session_timeout": "36000",
      "challenge_token": "",
      "username": "",
      "login_type": "",
      "challenge": "",
      "client_ip": "",
      "client_port": "-1",
      "cert_verified": "false",
      "sessionid": "##
     D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
      "token": "b2f3f935e93db6a"
     }

   ]

 }

<!--NeedCopy-->
```

Ejemplo 1: Recuperar las estadísticas del servidor virtual de equilibrio de carga

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
    GET /nitro/v1/stat/lbvserver HTTP/1.1
    Host: 192.0.2.5
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    Accept: application/json
    Cache-Control: no-cache
<!--NeedCopy-->
```

Ejemplo 2: Crear un servidor virtual de equilibrio de carga

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
    POST /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
    Host: 192.0.2.5
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    Content-Type: application/json
```



```
6      Accept: application/json
7      Cache-Control: no-cache
8
9      {
10   "lbvserver":{
11   "name":"sample_lbvserver","servicetype":"HTTP","ipv46":"10.102.1.11","
        port":"80" }
12    }
13
14 <!--NeedCopy-->
```

Ejemplo 3: Modificar un servidor virtual de equilibrio de carga

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
1      PUT /nitro/v1/config/lbvserver HTTP/1.1
2      Host: 192.0.2.5
3      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5      Content-Type: application/json
6      Accept: application/json
7      Cache-Control: no-cache
8
9      {
10   "lbvserver":{
11   "name":"sample_lbvserver","appflowlog":"DISABLED" }
12    }
13
14 <!--NeedCopy-->
```

Ejemplo 4: Eliminar un servidor virtual de equilibrio de carga

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
1      DELETE /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
2      Host: 192.0.2.5
3      Cookie: SESSID=##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
4      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5      Cache-Control: no-cache
6
7  <!--NeedCopy-->
```


Preguntas frecuentes

January 30, 2024

En esta sección se proporcionan las preguntas frecuentes sobre las siguientes funciones de NetScaler Application Delivery Management (NetScaler ADM). Haga clic en el nombre de una función en la siguiente tabla para ver la lista de preguntas frecuentes de esa función.

Análisis	Autenticación	Administración de configuración
Administración de certificados	Implementación	Implementación (recuperación ante desastres)
Gestión de eventos	Administración de instancias	StyleBooks
Administración del sistema		

Análisis

¿Debo habilitar el canal virtual EUEM en las instancias de Citrix Gateway implementadas en modo de salto único?

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el Citrix ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual de EUEM no está habilitado, los datos restantes de HDX Insight se mostrarán en Citrix ADM.

Un canal virtual EUEM es un servicio predeterminado que se ejecuta en las aplicaciones de escritorio virtual (VDA) de Citrix. Si no se está ejecutando, inicie el proceso "Citrix End User Experience Monitoring"en los servicios de VDA.

¿Cómo puedo habilitar NetScaler ADM para supervisar el tráfico de aplicaciones web y escritorios virtuales?

1. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia de Citrix Application Delivery Controller (Citrix ADC) en la que quiere habilitar el análisis.
2. Seleccione **Activar/desactivar Insight** en la lista desplegable **Acción** .
3. En la página **Configure Insight** que se abre, seleccione todos los servidores virtuales en los que quiera habilitar el análisis y haga clic en **Habilitar AppFlow** . Para obtener más información, consulte Cómo habilitar el análisis en instancias.

> **Nota**
>
> Para las instancias NetScaler ADC de la versión 11.0, versión 65.30 y versiones posteriores, no hay ninguna opción en NetScaler ADM para habilitar Security Insight explícitamente. Asegúrese de configurar los parámetros de AppFlow en las instancias NetScaler ADC, de modo que NetScaler ADM comience a recibir el tráfico de Security Insight junto con el tráfico de Web Insight. Para obtener más información sobre cómo establecer los parámetros de AppFlow en las instancias de NetScaler ADC, consultePara establecer los parámetros de AppFlow mediante la utilidad de configuración.

Después de agregar las instancias NetScaler ADC, ¿NetScaler ADM comienza automáticamente a recopilar información analítica?

No. Primero debe habilitar el análisis en los servidores virtuales alojados en instancias de Citrix ADC administradas por Citrix ADM. Para obtener más información, consulte Cómo habilitar el análisis en las instancias.

¿Necesito acceder al dispositivo Citrix ADC individual para habilitar el análisis?

No. Toda la configuración se realiza desde la interfaz de usuario de NetScaler ADM, que enumera los servidores virtuales alojados en la instancia específica de NetScaler ADC. Para obtener más información, consulte Cómo habilitar el análisis en las instancias.

¿Cuáles son los tipos de servidores virtuales que se pueden enumerar en una instancia de NetScaler ADC para habilitar el análisis?

Actualmente, la interfaz de usuario de NetScaler ADM incluye los siguientes servidores virtuales para permitir el análisis:

- Servidor virtual de equilibrio de carga
- Servidor virtual de conmutación de contenido
- Servidor virtual VPN
- Servidor virtual de redirección de caché

¿Cómo puedo conectar un disco adicional a Citrix ADM?

Para adjuntar un disco adicional a NetScaler ADM:

1. Apague la máquina virtual NetScaler ADM.

2. En el Hypervisor, conecte un disco adicional del tamaño de disco requerido a la máquina virtual NetScaler ADM.

   Por ejemplo, Consideremos que quiere aumentar el espacio en disco a 200 GB, en una máquina virtual NetScaler ADM de 120 GB. En este escenario, debe conectar un espacio en disco de 200 GB en lugar de 80 GB. Los 200 GB de espacio en disco recién conectados se utilizarán para almacenar datos de base de datos, archivos de registro NetScaler ADM. El espacio de disco actual de 120 GB se utilizará para almacenar los archivos principales, los archivos de registro del sistema operativo, etc.

3. Inicie la máquina virtual NetScaler ADM.

¿Qué quiere decir con que los recopiladores no están configurados en las instancias de NetScaler ADC?

Un recopilador recibe los registros de AppFlow generados por el dispositivo NetScaler ADC.

NetScaler ADM recibe tráfico de Security Insight y Web Insight de las instancias de NetScaler ADC cuando la función AppFlow está habilitada. Cuando habilita la función AppFlow en una instancia de NetScaler ADC, debe especificar al menos un recopilador al que se envían los registros de AppFlow. Si los recopiladores no están configurados en las instancias de NetScaler ADC, NetScaler ADM no recibe el tráfico de las instancias.

Por ejemplo, se agregan cinco instancias de NetScaler ADC a NetScaler ADM. Si no se especifican recopiladores para dos instancias, no fluye tráfico a NetScaler ADM. Los diagnósticos de autoservicio detectan el problema y lo muestran como "Los recopiladores no están configurados en 2 instancias. "

Para obtener más información sobre cómo configurar la función AppFlow, consulte Configuración de la función AppFlow.

Autenticación

¿Qué es el equilibrio de carga de las solicitudes de autenticación?

La función de equilibrio de carga del servidor de autenticación permite a NetScaler ADM equilibrar la carga de las solicitudes de autenticación que se dirigen a los servidores de autenticación externos. El equilibrio de carga de los servidores de autenticación garantiza que la carga de autenticación se divida entre varios servidores de autenticación y, por lo tanto, evita que un servidor de autenticación se sobrecargue. Puede crear un servicio de autenticación para conectarse y obtener información de usuario de su servidor de autenticación externo existente mediante protocolos de autenticación como LDAP, RADIUS o TACACS.

¿Por qué necesitamos conectar servidores de autenticación externos en cascada?

Los servidores de autenticación externos en cascada proporcionan un procesamiento de autenticación ininterrumpido, lo que permite el acceso a usuarios legítimos en caso de que falle un servidor de autenticación. No hay límite en cuanto a los tipos de servidores de autenticación que se pueden aplicar en cascada. Puede tener todos los servidores de RADIUS, todos los servidores de LDAP o una combinación de servidores de RADIUS y LDAP.

¿Cuántos servidores de autenticación externos puedo conectar en cascada?

Puede conectar en cascada hasta 32 servidores de autenticación externos en NetScaler ADM.

¿Tengo una alternativa cuando falla la autenticación externa?

Puede producirse una situación en la que la autenticación externa falle por completo, incluso si ha conectado varios servidores en cascada. Por ejemplo, es posible que no se pueda acceder a los servidores externos o que no se hayan introducido las credenciales de un usuario nuevo en ninguno de los servidores de autenticación externos. Para evitar el bloqueo de usuarios en tal situación, puede habilitar la autenticación local de reserva. Para obtener más información, consulteAutenticación local alternativa.

¿Qué es la autenticación local de reserva?

La autenticación local alternativa es una opción para autenticar a los usuarios localmente cuando la autenticación externa falla. Si falla la autenticación externa, NetScaler ADM accede a la base de datos de usuarios local para autenticar a los usuarios.

En Citrix ADM, vaya a **Sistema** > **Autenticación** > **Configuración de autenticación** . En esta página, puede agregar varios servidores de autenticación externos en una cascada y seleccionar la opción **Habilitar autenticación local de reserva**.

¿Qué es la extracción de grupos de usuarios externos?

Si ha agregado servidores externos para autenticar a los usuarios, puede importar (extraer) grupos de usuarios existentes en NetScaler ADM. Debe importar los grupos de usuarios una vez y proporcionar un permiso de grupo a un grupo de usuarios en lugar de importar usuarios individuales y darles permisos individuales. No tiene que volver a crear los usuarios en NetScaler ADM.

¿Por qué necesitamos asignar permisos de grupo?

Cuando utiliza la función de equilibrio de carga de NetScaler ADC, puede integrar NetScaler ADM con servidores de autenticación externos e importar información de grupos de usuarios desde los servidores de autenticación. Inicie sesión en Citrix ADM y cree manualmente la misma información de grupo en Citrix ADM y asigne permisos a esos grupos. El permiso de usuario y grupo de usuarios se administra en NetScaler ADM y no en el servidor externo. Los usuarios tienen diferentes permisos de acceso basados en funciones en los servidores externos. Configure los mismos permisos para los usuarios de NetScaler ADM también. En lugar de configurar los permisos individualmente para cada usuario, puede configurar un permiso de nivel de grupo para que los miembros del grupo de usuarios puedan acceder a servicios específicos en los servidores virtuales con equilibrio de carga. Los permisos típicos que puede asignar son permisos para administrar instancias de NetScaler ADC, instancias de Citrix SDX, servidores virtuales, etc., de modo que los usuarios de ese grupo puedan administrar solo esas instancias o servidores virtuales. Más adelante podrá modificar los permisos otorgados a los usuarios a nivel de grupo. Incluso puede eliminar uno o más grupos de usuarios; otros usuarios del grupo seguirán funcionando en NetScaler ADM.

Administración de configuración

¿Puedo realizar la configuración en varias instancias de NetScaler ADC simultáneamente con NetScaler ADM?

Sí, puede usar trabajos de configuración para realizar la configuración en varias instancias de NetScaler ADC.

¿Qué son los trabajos de configuración en NetScaler ADM?

Un trabajo es un conjunto de comandos de configuración que puede crear y ejecutar en una o más instancias administradas. Puede crear trabajos para realizar cambios de configuración en todas las instancias, replicar configuraciones en varias instancias de la red y realizar tareas de configuración de grabación y reproducción mediante la GUI de NetScaler ADM. También puede convertir las tareas grabadas en comandos de CLI.

Puede utilizar la función Trabajos de configuración de NetScaler ADM para crear un trabajo de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados.

¿Puedo programar trabajos con plantillas integradas en NetScaler ADM?

¡Sí! Puede programar un trabajo mediante la opción de plantilla integrada. Un trabajo es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Por ejemplo, puede utilizar la opción de plantilla integrada para programar un trabajo para configurar servidores syslog. Puede optar por ejecutar el trabajo inmediatamente o programar el trabajo para que se ejecute más tarde.

Puede guardar la configuración de un trabajo creado previamente y volver a ejecutar el trabajo después de modificar los comandos, los parámetros, el origen de configuración y las instancias de destino. Esto resulta útil cuando el mismo conjunto de comandos tiene que ejecutarse en una instancia diferente, o cuando el trabajo encuentra un error y detiene la ejecución posterior.

Administración de certificados

¿La eliminación de certificados SSL de Citrix ADM conduce a la eliminación de certificados de las instancias de Citrix ADC?

No

Implementación

¿Cuáles son el nombre de usuario y la contraseña predeterminados?

- Después de completar la configuración de red inicial, puede iniciar sesión en NetScaler ADM desde el hipervisor o la consola SSH, con el nombre de usuario y la contraseña predeterminados (nsrecover/nsroot).
- El nombre de usuario y la contraseña predeterminados para iniciar sesión desde la GUI son *nsroot/nsroot*.

¿Cómo cambiar la contraseña predeterminada?

Para cambiar la contraseña:

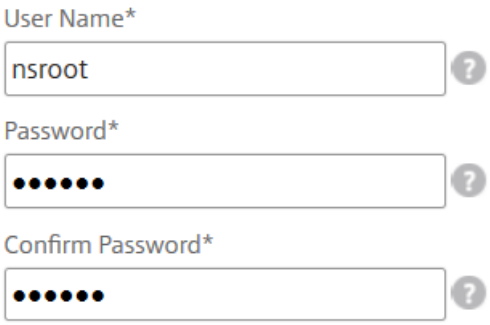
1. En Citrix ADM, vaya a **Sistema** > **Administración** de **usuarios > Usuarios**.

   Se muestra la página Usuarios.

2. Seleccione el nombre de usuario **nsroot** y haga clic en **Modificar**.

Se muestra la página Configurar usuario del sistema.

3. Seleccione **Cambiar contraseña** y cree una contraseña de su elección.



4. Haga clic en **Aceptar**.

   Ahora puede usar la nueva contraseña para iniciar sesión desde la GUI y el hipervisor o la consola SSH.

   > Nota
   >
   > No puede modificar el nombre de usuario.

¿Cómo restablecer la contraseña?

Puede ver esta documentación para restablecer la contraseña.

En un par HA, si la contraseña se cambia en el nodo principal y si la opción Romper el par HA se selecciona más adelante, ¿cuál es el comportamiento?

Puede iniciar sesión en ambos nodos independientes con su nueva contraseña.

Si dos servidores independientes tienen contraseñas diferentes, ¿cuál es el impacto de la implementación de estos dos servidores en un par de alta disponibilidad?

Se recomienda tener una contraseña predeterminada para ambos servidores cuando implemente dos servidores independientes en el par de alta disponibilidad.

La configuración de HA está completa, pero no se puede acceder a la GUI del nodo principal. ¿Cuál puede ser la razón?

La configuración tarda unos minutos en surtir efecto. Puede intentar acceder de nuevo después de unos minutos.

La configuración de HA está completa, pero no se puede acceder a la GUI de la dirección IP flotante. ¿Cuál puede ser la razón?

Después de la configuración de alta disponibilidad, primero debe acceder a la GUI del nodo principal y completar la implementación. Para obtener más información, consulte Implementar el nodo principal y el secundario como un par de alta disponibilidad. Una vez completada la implementación, el servidor se reinicia y se prepara para la implementación de alta disponibilidad. A continuación, puede acceder a la GUI de la dirección IP flotante.

¿Qué base de datos admite NetScaler ADM independiente y NetScaler ADM HA?

Tanto NetScaler ADM independiente como NetScaler ADM HA admiten PostgreSQL.

¿Cuál es la posible pérdida de datos en el nodo secundario?

El nodo secundario escucha los mensajes de latido que el nodo principal envía a través de la base de datos NetScaler ADM. Si el nodo secundario no recibe los latidos durante más de 180 segundos, el nodo secundario realiza una comprobación basada en SSH en el nodo principal. Si el latido y la comprobación basada en SSH fallan, se considera que el nodo principal está inactivo.

En este caso, el nodo secundario pasa a ser el nodo principal y el período de 180 segundos se puede considerar como la posible pérdida de datos en el nodo secundario.

¿Qué ocurre si el nodo principal está inactivo?

El nodo secundario se hace cargo y se convierte en el nodo principal.

¿Cómo volver a instalar el nodo que ha fallado?

Se recomienda instalar una compilación de VM nueva. Para volver a instalar:

1. Rompe el par de alta disponibilidad. Navegue hasta **Sistema** > **Implementación**

   Se muestra la página de implementación. Haga clic en **Romper alta disponibilidad**.

2. Elimine el nodo fallido del Hypervisor.
3. Importe el archivo de imagen.xva al hipervisor.
4. En la ficha Consola, configure Citrix ADM con las configuraciones de red iniciales. Para obtener más información, consulte Registrar e implementar el primer servidor (nodo principal) y Registrar e implementar el segundo servidor (nodo secundario).
5. Reimplemente el par de alta disponibilidad.

¿NetScaler ADM admite almacenamiento SAN?

Citrix recomienda hospedar NetScaler ADM VHD en un almacenamiento local. Cuando se aloja en dispositivos de almacenamiento en una SAN, es posible que NetScaler ADM no funcione como se esperaba.

¿Citrix ADM admite discos adicionales?

Sí. Una nueva instalación del par NetScaler ADM HA asigna 120 GB de almacenamiento de forma predeterminada. Para más de 120 GB de almacenamiento, puede agregar un disco adicional para un almacenamiento máximo de 3 TB. No se admite la adición de más de un disco adicional.

Después de inhabilitar el par de alta disponibilidad, ¿qué sucede con la dirección IP flotante configurada?

Ya no se podrá acceder a la dirección IP flotante y tendrá que volver a implementar el par de alta disponibilidad.

¿Puedo dar una dirección IP flotante diferente al volver a implementar?

Sí. Puede configurar una nueva dirección IP flotante.

¿Por qué no es accesible la GUI del nodo secundario?

El nodo secundario es solo un servidor de réplicas de lectura y actúa como nodo principal solo si el nodo principal está inactivo por cualquier motivo. Citrix recomienda acceder a la GUI del nodo principal o a la GUI de direcciones IP flotantes.

Si el nodo principal está inactivo durante un período prolongado, ¿se pueden realizar las configuraciones con la GUI de direcciones IP flotantes?

Sí. Puede seguir realizando configuraciones y las configuraciones se guardan en el nodo secundario. Cuando el nodo principal regresa, se sincronizarán todas las configuraciones.

Si es necesario cambiar la dirección IP del nodo principal o la dirección IP del nodo secundario o la dirección IP flotante en el futuro (por ejemplo, cambiarla a IPv6), ¿cuáles son las soluciones recomendadas?

No se admite el cambio de direcciones IP en el par de alta disponibilidad sin romper el par de alta disponibilidad.

Para actualizar la dirección IP del nodo principal o del nodo secundario:

1. Rompe el par de alta disponibilidad. Navegue hasta **Sistema** > **Implementación** .

   Aparecerá la página Implementación. Haga clic en **Romper alta disponibilidad**.

   a) Inicie sesión en el nodo principal mediante un cliente SSH o desde el hipervisor.

   b) Use `nsrecover` como nombre de usuario e introduzca la contraseña que ha establecido.

   c) Introduzca **networkconfig**. Realice el procedimiento del **paso 3** disponible en Register e implemente el primer servidor (nodo principal).

      Durante la configuración de red inicial, puede proporcionar una dirección IP diferente.

   d) Realice el mismo procedimiento para el nodo secundario y continúe con el procedimiento del **paso 3** disponible en Registrar e implementar el segundo servidor (nodo secundario).

Para actualizar la dirección IP flotante:

1. Navegue hasta **Sistema** > **Implementación** .

   Aparecerá la página Implementación.

   a) Haga clic en **Configuración de HA**.

   b) Haga clic en **Configurar dirección IP flotante para el modo de alta disponibilidad**.

   c) Introduzca la dirección IP flotante y haga clic en **Aceptar**.

¿ADM admite procesadores AMD?

No. ADM no admite procesadores AMD

Implementación (recuperación ante desastres)

¿Con qué frecuencia se produce la replicación entre el sitio principal y el sitio de recuperación ante desastres?

La replicación entre el sitio principal y el sitio de recuperación ante desastres es en tiempo real.

Después de iniciar el script de reserva en el sitio de recuperación ante desastres, ¿el sitio de recuperación ante desastres se convierte en el sitio primario temporal hasta que el sitio principal se recupera y funciona completamente?

No. El sitio de recuperación ante desastres se convertirá ahora en el sitio principal.

Si se selecciona la opción Pareja de HA, ambos nodos funcionan como un servidor independiente. Dado que la compatibilidad con DR no se aplica al servidor independiente, ¿qué ocurre con el sitio de recuperación ante desastres si se selecciona Romper par de alta disponibilidad?

Si selecciona la opción Romper par de alta disponibilidad, se termina la replicación entre el sitio principal y el sitio de DR. Debe volver a configurar el sitio de recuperación ante desastres como parte de la reimplementación del par de alta disponibilidad.

Gestión de eventos

¿Cómo puedo hacer un seguimiento de todos los eventos que se han generado en mis instancias de NetScaler ADC administradas con NetScaler ADM?

Como administrador de red, puede ver detalles como cambios de configuración, condiciones de inicio de sesión, errores de hardware, violaciones de umbrales y cambios de estado de la entidad en sus instancias de NetScaler ADC, junto con los eventos y su gravedad en instancias específicas. Puede usar el panel de eventos de NetScaler ADM para ver los informes generados para los detalles de gravedad de eventos críticos en todas las instancias de NetScaler ADC.

¿Qué son las reglas del evento?

Con NetScaler ADM, puede configurar reglas para supervisar eventos específicos. Las reglas de eventos facilitan la supervisión de una gran cantidad de eventos generados en la infraestructura de Citrix ADM.

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, instancias NetScaler ADC, categorías y objetos de error. Las acciones que puede asignar a los eventos son el envío de una notificación por correo electrónico, el reenvío de capturas SNMP desde las instancias administradas de NetScaler ADC a NetScaler ADM y el envío de una notificación por SMS.

Administración de instancias

¿Qué son los centros de datos en NetScaler ADM?

Un centro de datos NetScaler ADM es una agrupación lógica de las instancias de NetScaler ADC en una ubicación geográfica específica. Cada servidor puede supervisar y administrar varias instancias de NetScaler ADC dentro de un centro de datos. Puede usar el servidor Citrix ADM para administrar datos como el syslog, el flujo de tráfico de aplicaciones y las capturas de SNMP de las instancias administradas. Para obtener más información sobre la configuración de centros de datos, consulte Cómo configurar centros de datos para geomapas en Citrix ADM.

¿Cuáles son los diferentes dispositivos Citrix compatibles con NetScaler ADM?

Las instancias son los dispositivos Citrix o los dispositivos virtuales que quiere descubrir, administrar y supervisar desde NetScaler ADM. Debe agregar estas instancias al servidor de NetScaler ADM. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a Citrix ADM:

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

Puede agregar instancias al configurar el servidor Citrix ADM por primera vez o más adelante.

¿Qué es un perfil de instancia?

Citrix ADM utiliza un perfil de instancia para acceder a una instancia en particular.

Un perfil de instancia contiene el nombre de usuario y la contraseña para acceder a una o más instancias. Hay un perfil predeterminado disponible para cada tipo de instancia. Por ejemplo, ns-root-profile es el perfil predeterminado para las instancias de Citrix ADC. Contiene las credenciales de administrador de NetScaler ADC predeterminadas. Cuando cambias las credenciales necesarias para acceder a las instancias, puede definir perfiles de instancia personalizados para esas instancias.

¿Podemos agregar instancias de SD-WAN ilimitadas en NetScaler ADM? ¿NetScaler ADM puede gestionar todos los contadores escalares y vectoriales para SD-WAN?

Actualmente, no hay límite de licencias para las instancias de SD-WAN que se pueden agregar a NetScaler ADM. NetScaler ADM tiene un conjunto de informes integrados que sondea internamente los contadores escalares y vectoriales.

¿Puedo detectar de nuevo varias instancias de Citrix VPX en NetScaler ADM?

Sí, puede redescubrir varias instancias de Citrix **VPX** en NetScaler ADM para conocer los estados y configuraciones más recientes de las instancias.

Vaya a **Redes** > **Instancias** > **NetScaler VPX,**seleccione las instancias que quiere redescubrir y, en la lista desplegable **Acción**, haga clic en **Redescubrir**. Para obtener más información, consulte Cómo redescubrir varias instancias VPX.

¿Se puede instalar NetScaler ADM en Citrix SDX?

No

StyleBooks

¿Se pueden usar StyleBooks para configurar diferentes instancias de NetScaler ADC que se ejecutan en diferentes versiones del software NetScaler ADC?

Sí, puede utilizar StyleBooks para configurar diferentes instancias de NetScaler ADC que se ejecuten en versiones diferentes si no hay discrepancia entre los comandos entre diferentes versiones.

Cuando se utiliza un StyleBook para configurar varias instancias de NetScaler ADC al mismo tiempo y se produce un error en la configuración de una instancia de NetScaler ADC, ¿qué sucede?

Si se produce un error al aplicar la configuración a una instancia de NetScaler ADC, la configuración no se aplica más instancias y las configuraciones ya aplicadas se revierten.

¿Las copias de seguridad de NetScaler ADC realizadas a través de NetScaler ADC incluyen configuraciones aplicadas a través de StyleBooks?

Sí

Administración del sistema

¿Puedo asignar un nombre de host a mi servidor Citrix ADC?

Sí, puede asignar un nombre de host para identificar su servidor NetScaler ADM. Para asignar un nombre de host, vaya a **Sistema** > **Administración del sistema** > **Configuración del sistema** y haga clic en **Cambiar nombre de host** .

El nombre del host se muestra en la licencia universal de NetScaler ADM. Para obtener más información, consulteCómo asignar un nombre de host a un servidor NetScaler ADM.

¿Puedo realizar una copia de seguridad y restaurar mi configuración de NetScaler ADM?

Sí, puede realizar copias de seguridad de los archivos de configuración (archivos NTP y certificados SSL), de los datos del sistema, de la infraestructura y de las aplicaciones, y de todas las configuraciones SNMP. Si su NetScaler ADM se vuelve inestable, puede utilizar los archivos de copia de seguridad para restaurar su NetScaler ADM a un estado estable.

Para hacer una copia de seguridad y restaurar la configuración de Citrix ADM, vaya a **Sistema** > Configuración **avanzada** > **Archivos** de copia de seguridad y haga clic **en Realizar** copia de seguridad o **restaurar** , según sea el caso. Para obtener más información, consulte Cómo hacer copias de seguridad y restaurar la configuración en Citrix ADM.

Citrix recomienda utilizar esta función antes de realizar una actualización o por motivos de precaución.

¿Qué son los umbrales y las alertas en NetScaler ADM?

Puede establecer umbrales y alertas para supervisar el estado de una instancia de NetScaler ADC y supervisar las entidades de las instancias administradas.

Cuando el valor de un contador supera el umbral, NetScaler ADM genera una alerta para indicar un problema relacionado con el rendimiento. Cuando el valor del contador vuelve al valor de borrado especificado en el umbral, el evento se borra.

¿Puedo generar un archivo de asistencia técnica para NetScaler ADM?

Sí. Citrix recomienda generar un archivo de datos y estadísticas de NetScaler ADM antes de ponerse en contacto con la asistencia técnica para solucionar un problema. El archivo es un archivo TAR que puede enviar al equipo de soporte técnico.

Puede generar un archivo de soporte técnico que contenga registros de depuración, la duración durante la cual se recopilaron los registros de depuración y registros distintos y diversos de la base de datos de NetScaler ADM.

Para configurar y enviar un archivo de soporte técnico, vaya a **Sistema** > **Diagnóstico** > **Soporte técnico** y, a continuación, haga clic en Generar archivo de soporte técnico. Para obtener más información, consulteCómo generar un archivo de soporte técnico para NetScaler ADM.

¿Qué es la depuración de syslog?

Syslog es un protocolo estándar para el registro. Syslog permite el aislamiento del sistema que genera la información y del sistema que almacena la información. Puede consolidar la información de registro y obtener información de los datos recopilados. También puede configurar syslog para registrar diferentes tipos de eventos.

Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog. Puede especificar el número de días tras los cuales se eliminarán de Citrix ADM todos los datos genéricos de Syslog, AppFirewall y Citrix Gateway.

¿Puedo configurar el servidor NTP en NetScaler ADM?

Puede configurar un servidor de Protocolo de hora de red (NTP) en NetScaler ADM para sincronizar el reloj de NetScaler ADM con el servidor de NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

Para configurar un servidor NTP, vaya a **Sistema** > **Servidores NTP** y, a continuación, haga clic en **Agregar**. Para obtener más información, consulteCómo configurar el servidor NTP en NetScaler ADM.

¿A partir de qué versión se admite la implementación de alta disponibilidad activa-pasiva de NetScaler ADM?

El modo de implementación de alta disponibilidad activa-pasiva de NetScaler ADM es compatible con la versión 12.0, compilación 51.24, de NetScaler ADM.

Tenía una configuración de alta disponibilidad activa-activa de NetScaler ADM y había configurado un dispositivo NetScaler ADC con un servidor virtual de equilibrio de carga para un acceso unificado a la GUI. ¿Cómo actualizo esta configuración?

Después de actualizar el par NetScaler ADM HA al modo activo-pasivo, debe ejecutar el siguiente comando en el dispositivo NetScaler ADC para actualizar la configuración de equilibrio de carga:

add lb monitor MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n" "-recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

¿Puedo configurar el equilibrio de carga del par de alta disponibilidad de NetScaler ADM en una instancia de NetScaler ADC mediante el puerto 443?

No, no puede configurar el equilibrio de carga del par de NetScaler ADM HA en una instancia de NetScaler ADC mediante el puerto 443.

Cuando configura `http-ecv` y `https-ecv` supervisa en NetScaler ADC, no supervisa correctamente los nodos de NetScaler ADM HA.

¿Se puede utilizar un archivo de copia de seguridad del servidor NetScaler ADM para restaurar la configuración de otro servidor NetScaler ADM?

Sí

Después de que NetScaler ADM realice una copia de seguridad de una instancia de NetScaler ADC, ¿se puede usar ese archivo de copia de seguridad para restaurar la configuración de otra instancia de NetScaler ADC a través de NetScaler ADM?

Sí. Descargue el archivo de respaldo de Citrix ADM, cárguelo en el repositorio de respaldo de otra instancia de Citrix ADC y restaure esa instancia. Asegúrese de que la información de red y la información de autenticación no entren en conflicto. Por ejemplo, compruebe si hay conflictos de direcciones IP o puertos, perfiles de contraseña que no coincidan. Asegúrese también de que la instancia VPX restaurada tenga la misma dirección NSIP y licencia NetScaler ADC que la que se realizó la copia de seguridad.

Antes de restaurar una instancia en un par de alta disponibilidad, asegúrese de que las direcciones IP y el estado (principal o secundario) almacenados en el archivo de respaldo coincidan con los de la configuración de alta disponibilidad original. Compruebe también que el nuevo primario y secundario tengan el mismo tipo de licencia NetScaler ADC.

¿Podemos obligar a Citrix ADM a utilizar una dirección SNIP para comunicarse con las instancias de Citrix ADC, en lugar de utilizar la dirección NSIP del servidor Citrix ADM?

Sí, puede agregar una dirección SNIP (con administración habilitada) en NetScaler ADM para comunicarse con instancias de NetScaler ADC.

Cuando hago copias de seguridad de instancias de NetScaler ADC en NetScaler ADM, ¿el resultado es una copia de seguridad completa o básica?

Las copias de seguridad de las instancias de NetScaler ADC de NetScaler ADM son copias de seguridad completas.

¿Existe una guía de solución de problemas para NetScaler ADM?

Sí. Consulte https://support.citrix.com/article/CTX224502.

¿Cómo se administran las instancias de NetScaler ADC cuando se produce una conmutación por error de alta disponibilidad de NetScaler ADM?

Si la comprobación basada en latidos y SSH falla, se considera que el nodo principal está inactivo y el nodo secundario pasa a ser el nodo principal. Todas las instancias de NetScaler ADC se actualizan con los últimos detalles del nodo principal como destino de captura SNMP de forma predeterminada.

El nuevo nodo Citrix ADM principal (activo) comprueba si el nodo anteriormente activo estaba configurado como recopilador de AppFlow o servidor syslog. Si lo estaba, el nuevo nodo principal agrega los detalles del recopilador de AppFlow o del servidor syslog a la información enviada a las instancias.

Para syslog reemplaza los detalles del servidor antiguo.

¿Qué ocurre cuando el nodo NetScaler ADM HA que se no funcionaba vuelve a funcionar?

Después de volver al servicio, el nodo NetScaler ADM permanece pasivo a menos que el nodo activo conmute por error.

¿Cómo se distribuyen las instancias de NetScaler ADC en los nodos de alta disponibilidad de NetScaler ADM?

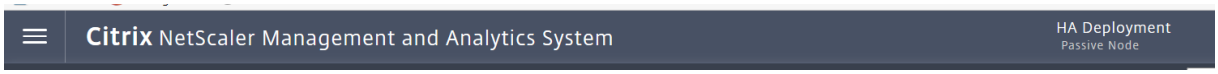
Todas las instancias de NetScaler ADC son administradas por el nodo principal de NetScaler ADM.

¿Cómo se administran las licencias de servidores virtuales en caso de conmutación por error de Citrix ADM HA?

Si el nodo principal de NetScaler ADM en el que se aplican las licencias de servidor virtual falla, el nuevo nodo principal administra las licencias de servidor virtual durante un período de gracia de 30 días. Las licencias deben volver a solicitarse en la nueva escuela primaria antes de que finalice el período de gracia. Para obtener alternativas, póngase en contacto con el soporte técnico de Citrix.

¿Es obligatorio un equilibrador de carga para la configuración de NetScaler ADM HA?

No, pero si no hay un equilibrador de carga, se debe acceder a los nodos NetScaler ADM a través de sus propias direcciones IP. El nodo pasivo está marcado con la etiqueta «Pasivo» y Citrix recomienda no crear ninguna configuración en el nodo pasivo.



¿NetScaler ADM admite una base de datos externa?

No

¿Se puede usar una instancia de NetScaler ADC que administra NetScaler ADM como equilibrador de carga para la alta disponibilidad de NetScaler ADM?

Sí

¿Qué datos se sincronizan entre los nodos de HA de NetScaler ADM?

Se sincroniza la base de datos completa de NetScaler ADM y se sincronizan las siguientes carpetas:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/

- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/