NetScaler Application Delivery Management 14.1

Machine translated content

Disclaimer

Contents

Notas de la versión

January 30, 2024

Las notas de la versión de NetScaler Application Delivery Management (ADM) 14.1 describen las nuevas funciones, las mejoras de las funciones existentes y los problemas conocidos de una compilación. El documento de notas de la versión 14.1 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.

> **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.

Notas de versión de NetScaler ADM 14.1-12.34 Build

January 30, 2024

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas conocidos y resueltos que existen en la versión 14.1-12.34 de NetScaler ADM.

Notas

- Este documento de notas de la versión no incluye correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.
- La compilación 14.1-12.34 reemplaza a la compilación 14.1-12.30.
- La compilación 14.1-12.34 incluye la nueva función NSADM-98483 y un problema conocido NSADM-106497, junto con todas las mejoras y correcciones de errores disponibles en la compilación 14.1-12.30.

Novedades

Las mejoras y los cambios que están disponibles en la compilación 14.1-12.34.

Sistema de licencias

Licenciamiento de NetScaler Flexed El licenciamiento Flexed de NetScaler es el nuevo marco de licenciamiento destinado a simplificar el proceso de administración de licencias. Su licencia Flexed incluye licencias de instancias de software (VPX/CPX/BLX, SDX, MPX y VPX FIPS) y licencias de capacidad de ancho de banda. Debe aplicar las licencias Flexed en el servicio NetScaler Console o NetScaler ADM local. También debe aplicar la licencia MPX Z-Cap y SDX Z-Cap en el hardware NetScaler MPX y el hardware NetScaler SDX, respectivamente. A continuación, puede asignarlos a todos los formatos de NetScaler implementados en la nube o de forma local.

Para obtener más información, consulte
Licencia flexible.

Las licencias flexibles se admiten oficialmente en las versiones locales 14.1 y 13.1 de NetScaler ADM. En la versión 14.1-12.x local de ADM y versiones posteriores, está disponible la asignación por paquetes de usuarios VIP de ADM ilimitados para el análisis y puede administrar las licencias Flexed a través de la interfaz de usuario de Flexed Dashboard (**NetScaler Licensing > Flexed Licensing**).

En el caso de las versiones 13.1 y 14.1 locales de ADM anteriores a 14.1-12.x, al aplicar las licencias Flexed, ADM las trata de la misma manera que las licencias agrupadas y muestra los detalles en la interfaz de usuario del panel agrupado (**Infraestructura > Licencias** agrupadas). En estas versiones, no está disponible el derecho combinado de un número ilimitado de VIP de ADM para realizar análisis.

Para disfrutar de una mejor experiencia con el producto, con una GUI flexible y derechos agrupados, le recomendamos que actualice su ADM local a la versión 14.1-12.x o posterior.

> **Nota:**
>
> Para cumplir con los requisitos actuales de licencia de Flexed, habilite ADM On-Prem Cloud Connector. Esta función conecta su ADM local con el servicio ADM para la recopilación de telemetría. Le recomendamos que habilite la recopilación de telemetría cuando utilice las licencias Flexed. Para habilitar ADM On-Prem Cloud Connector, consulte ADM On-Prem Cloud Connector.

[NSADM-98483]

Análisis

Detección de anomalías en las métricas clave de la aplicación Como administrador, debe asegurarse de que sus aplicaciones se administren de manera eficiente para obtener información que le

permita priorizar mejor y solucionar problemas. En algunos escenarios, es posible que también desee ver y analizar la desviación inusual en el rendimiento de las aplicaciones que puede producirse durante un período específico.

En el **Panel de aplicaciones**, cuando selecciona una aplicación, la ficha **Métricas clave** le permite ver cómo se utilizan sus aplicaciones. NetScaler ADM supervisa el patrón de tráfico y analiza si las métricas clave se encuentran en el rango esperado. Ahora puede ver las anomalías de las siguientes métricas clave si hay desviaciones del rango esperado:

- Tiempo de respuesta
- Rendimiento
- Volumen de datos
- Solicitudes por segundo

Para obtener más información, consulte Uso y anomalíasde las aplicaciones

[NSADM-97531]

Exporta datos a Splunk y New Relic solo desde instancias seleccionadas Al crear una suscripción para exportar datos a Splunk y New Relic, ahora puede seleccionar instancias. Si creas una suscripción con instancias específicas, los datos se exportan a Splunk y New Relic solo desde las instancias seleccionadas.

Para obtener más información, consulte Integración con Splunk e Integración con New Relic.

[NSADM-94371]

Tareas y recomendaciones prácticas Ahora se han agregado las siguientes mejoras a la función **Tareas** :

- Se presenta una nueva ficha de **tareas** en la que puede ver las tareas procesables que requieren su atención inmediata. Estas tareas se muestran en función de su utilización actual. Como administrador, la realización de estas tareas prácticas garantiza que la implementación de NetScaler sea segura, compatible y eficiente. Estas tareas procesables se basan en la gravedad de los problemas (críticos y medios).
- La ficha Tareas **pendientes** pasa a llamarse **Recomendaciones**. En **Recomendaciones**, puede seguir revisando las tareas existentes y hacer clic en **Guide Me** para completar la tarea.
- La ficha **Archivo** ya no está disponible. En su lugar, puede optar **por descartar** una recomendación de la lista.

Para obtener más información, consulte Recomendaciones y tareas prácticas.

[NSADM-91870]

Infraestructura

Usa el almacén de certificados para actualizar los certificados SSL Al actualizar un certificado SSL en **Infraestructura > Panel de control SSL > Actualizar,** ahora puede seleccionar el certificado en el almacén de certificados. Antes, tenías que cargar el archivo de certificado y el archivo de clave para actualizar un certificado SSL.

Para obtener más información, consulta Cómo actualizar un certificado instalado.

[NSADM-101303]

Soporte de registro de escaneo en Security Advisory En **Security Advisory** , ahora puede ver una nueva opción llamada **Scan Log** . Con el registro de **escaneo** , puede:

- Vea el informe de los últimos cinco escaneos CVE. El informe incluye tanto el análisis predeterminado del sistema como el análisis a petición iniciado por el usuario.
- Descarga el informe de cada escaneo en formato CSV y PDF.
- Vea el estado del análisis bajo demanda que está actualmente en curso.

Para obtener más información, consulte Aviso de seguridad.

[NSADM-101142]

Lista actualizada de trampas SNMP La lista de capturas SNMP ahora se actualiza con nuevas trampas, así como con algunas trampas que faltaban anteriormente. Para ver la lista completa, vaya a **Infraestructura > Eventos > Configuración de eventos > NetScaler.**

[NSADM-99798]

Administre los certificados y cifrados personalizados de bases de datos en una implementación de alta disponibilidad NetScaler ADM ahora le permite reemplazar los certificados de base de datos integrados predeterminados por sus propios certificados de una entidad de certificación de confianza. También puede configurar sus propios conjuntos de cifrado para la base de datos ADM. Para usar esta función, vaya a **Configuración > Implementación de alta disponibilidad > Certificados de bases de datos**.

Para obtener más información, consulte Administrar cifrados y certificados personalizados de bases de datos en una implementación de alta disponibilidad.

[NSADM-96583]

Uso compartido de la información de la licencia de suscripción entre ADM local y el servicio ADM El servidor local de ADM ahora envía la información de la licencia de suscripción de NetScaler al servicio ADM a través del ADM On-Prem Cloud Connector.

[NSADM-93820]

Uso compartido de información de licencia agrupada entre ADM local y el servicio ADM El servidor local de ADM ahora envía la información de licencia agrupada de NetScaler al servicio ADM a través del ADM On-Prem Cloud Connector.

[NSADM-93812]

Seguridad

Panel de seguridad unificada En NetScaler ADM, ahora puede usar un panel de control de un solo panel para configurar las protecciones, habilitar los análisis e implementarlos en sus aplicaciones. Vaya a **Seguridad > Panel de seguridad** y, a continuación, haga clic en **Administrar aplicación** para:

- Vea todas las aplicaciones seguras y no seguras.
- Seleccione una aplicación no segura, configure las protecciones a partir de varias opciones de plantillas, habilite el análisis de las protecciones e impleméntelas en su aplicación para protegerla.

Anteriormente, tenía que configurar todas las protecciones en las instancias de NetScaler y solo podía ver los análisis de las protecciones configuradas en NetScaler ADM. Como administrador, este panel de un solo panel le permite configurar las protecciones para la aplicación en un único flujo de trabajo.

Para obtener más información, consulte Panel de seguridad unificada.

[NSADM-92678]

StyleBooks

Use certificados del almacén de certificados NetScaler ADM en StyleBooks Ahora puede definir StyleBooks para usar certificados del almacén de certificados ADM de NetScaler. Al crear paquetes de configuración, puede seleccionar los certificados que ya existen en el almacén de certificados o agregar otros nuevos al almacén de certificados.

Para obtener más información, consulte Administrar los certificados SSL del almacén de certificados con StyleBooks.

[NSADM-101515]

Definir un menú desplegable en StyleBooks NetScaler ADM ahora le permite definir un menú desplegable en los «parámetros-condiciones» de la definición de StyleBook.

Para obtener más información, consulte Condiciones de parámetros.

[NSADM-99543]

Descargue paquetes de soporte para StyleBooks y paquetes de configuración Ahora puede descargar un paquete de soporte para solucionar problemas de cualquier operación de StyleBook o paquete de configuración. Puede compartir estos paquetes de soporte con el equipo de NetScaler al abrir un ticket de soporte para StyleBooks. Para descargar un paquete de soporte, vaya a **Aplicaciones > Configuración > Paquetes de configuración > Paquetes de soporte**.

Para obtener más información, consulte Descargar el paquete de soporte.

[NSADM-97838]

Modificar el estado y el estado ARP de los servidores virtuales en StyleBooks En **Aplicaciones > Configuración > Paquetes de configuración > Migrar la configuración de NetScaler**, ahora puede ver y editar el estado (habilitado/inhabilitado) y el estado de ARP de cualquier servidor virtual migrado a un nuevo NetScaler.

Para obtener más información, consulte Crear un StyleBook para migrar la configuración de la aplicación NetScaler.

[NSADM-97827]

Migre configuraciones sin un paquete de configuración NetScaler ADM ahora ofrece la opción de migrar configuraciones de aplicaciones entre NetScalers sin crear un paquete de configuración en NetScaler ADM. De forma predeterminada, la migración crea un paquete de configuración en ADM que se utiliza para seguir administrando la configuración a través de StyleBooks. Si solo quiere migrar la configuración de la aplicación de un NetScaler a otro sin administrarla posteriormente mediante StyleBooks, desactive la casilla **Administrar la configuración mediante ADM durante la migración en Aplicaciones > Configuraciones**** > Paquetes de configuración > Migrar la configuración de NetScaler **Migrar.

Para obtener más información, consulte Migración de la configuración de la aplicación NetScaler con StyleBooks Configuration Builder.

[NSADM-97802]

Problemas resueltos

Los problemas que se abordan en la compilación 14.1-12.34.

Análisis

- En ocasiones, el agente ADM de NetScaler puede bloquearse y generar archivos de volcado principales después de una actualización.

  [NSHELP-36428]

Infraestructura

- En determinadas condiciones, es posible que se pierdan las configuraciones de expresiones regulares aplicadas a algunos grupos de usuarios.

  [NSADM-104565]

- En **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**, al seleccionar una instancia vulnerable de NetScaler con un CVE y **hacer clic en Continuar con el flujo de trabajo de actualización**, aparece el siguiente mensaje de error:

  «La instancia de NetScaler seleccionada no requiere este flujo de trabajo de corrección»

  [NSADM-103649]

- En **Infraestructura > Eventos > Mensajes de eventos**, NetScaler ADM no muestra si las trampas de uso de la CPU de NetScaler son para la CPU de paquetes o la CPU de administración.

  [NSADM-103391]

- Cuando NetScaler ADM se instala en un clúster de Kubernetes, es posible que determinadas páginas, como **Infrastructure Analytics**, **Events**, **Syslog Events** y **Data Storage Management**, no aparezcan en la GUI de NetScaler ADM.

  [NSADM-103180]

- Cuando se exporta un informe de una página desplazable en NetScaler ADM, el informe exportado puede truncar el contenido que se extiende más allá de la altura de la ventana visible.

  [NSADM-102765]

- Se observa un bloqueo del subsistema mas_service en las implementaciones escaladas.

  Este problema se produce si tiene permisos de RBAC y pertenece a un grupo que tiene las siguientes configuraciones en **Configuración > Usuarios y funciones > Grupo > Configuración de autorización**:

  - Se selecciona una instancia específica en **Instancias**
  - **Todas las aplicaciones** se seleccionan en **Aplicaciones**

  [NSADM-99873]

- Cuando, como administrador raíz, inicie sesión en la GUI o API de NetScaler ADM con las credenciales predeterminadas por primera vez, se le pedirá que cambie la contraseña predeterminada.

  [NSADM-95328]

Administración y supervisión

- Cuando un usuario de RBAC envía una solicitud de API NITRO a NetScaler ADM para recuperar la lista de servidores de NetScaler, la respuesta indica incorrectamente que no hay servidores disponibles. Sin embargo, al navegar a la GUI de NetScaler ADM**(Infraestructura > Funciones de red > Equilibrio de carga > Servidores), se muestran todos los servidores**de NetScaler vinculados a ese usuario.

  [NSHELP-36645]

- La operación de restauración de NetScaler ADM **en Configuración > Archivos de copia de seguridad > Restaurar no se completa de forma** intermitente.

  [NSHELP-36527]

- NetScaler ADM no puede comprimir ciertos archivos principales, lo que aumenta el consumo de espacio en disco.

  [NSHELP-36434]

- Cuando un administrador crea un grupo con acceso a todas las aplicaciones y un usuario que pertenece a ese grupo intenta acceder a la página **Infraestructura > Funciones de red > Equilibrio de carga > Servidores**, no se puede acceder a la GUI de NetScaler ADM.

  [NSHELP-36426]

- Durante la sincronización de archivos entre los nodos principal y secundario en la configuración de NetScaler ADM HA, el subsistema de inventario se bloquea de forma intermitente.

  [NSHELP-36357]

- En los agentes integrados de NetScaler, las alertas o mensajes de eventos no se generan incluso después de que la antigüedad del evento supere la duración establecida **en Infraestructura > Eventos > Reglas > Agregar**.

  [NSHELP-35706]

- Al aprovisionar una instancia VPX en SDX en **Infraestructura > Instancias > NetScaler > SDX > Seleccione una acción > Aprovisionar VPX**, no aparece la opción **Administrar a través de la red**.

  [NSHELP-36328]

StyleBooks

- Los archivos de registro de NetScaler ADM StyleBook no se comprimen automáticamente incluso después de superar el límite de tamaño del archivo, lo que aumenta el consumo de espacio en disco.

  [NSHELP-36680]

- Cuando los paquetes de configuración con caracteres especiales en sus parámetros se actualizan o eliminan, NetScaler ADM muestra un mensaje de éxito a pesar de que las operaciones de actualización o eliminación están incompletas en NetScaler. Con esta corrección, NetScaler ADM ahora muestra con precisión los errores de cualquier configuración incompleta que se deba a la presencia de caracteres especiales en la definición del paquete de configuración.

  [NSADM-104423]

Problemas conocidos

Los problemas que existen en la versión 14.1-12.34.

Análisis

- En **Aplicaciones > Panel de control**, al hacer clic en una aplicación alojada en el par NetScaler HA, la ficha **Rendimiento** de la página de detalles de la aplicación no muestra ningún dato en **Todos los servicios**.

  Solución alternativa: actualice la página o vaya a otra ficha dentro de la página de detalles de la aplicación y, a continuación, vuelva a la ficha **Rendimiento** para ver los servicios asociados al servidor virtual de equilibrio de carga.

  [NSADM-105613]

Infraestructura

- El panel de licencias flexible muestra los detalles de NetScaler solo después de haber retirado al menos un NetScaler del grupo de licencias de ancho de banda Premium.

  [NSADM-106497]

- Cuando se eliminan licencias de NetScaler ADM para VMware ESXi, es posible que el **recuento de licencias en Configuración > Configuración de licencias y** análisis no refleje inmediatamente el número actualizado.

  [NSADM-105851]

- El informe de diferencias no se genera para un trabajo de actualización en **Infraestructura > Trabajos de actualización > Informes** de diferencias.

  [NSADM-10677]

- Después de configurar un NetScaler ADM nuevo, puede aparecer el siguiente mensaje de error: «Error en la operación: no se encontraron las métricas. «

  Este problema se produce porque el trabajo de purga automática de datos aún no se ha ejecutado, lo que provoca la ausencia de datos. El trabajo está programado para ejecutarse durante 3 horas y, una vez ejecutado, se generan los datos necesarios y el mensaje de error ya no aparece.

  [NSADM-103157]

- Al intentar instalar un certificado en una instancia de NetScaler BLX, se produce un error en la instalación y la página **Infraestructura > Panel de control de SSL > Registros de auditoría de SSL muestra el** siguiente mensaje de error:

  «SCP: La autenticación mediante contraseña falla en la *dirección IP*. «

  [NSADM-102202]

- El agente de NetScaler no se registra en NetScaler ADM si alguna de sus contraseñas tiene el símbolo «#».

  [NSADM-100613]

Sistema de licencias

- Una vez aplicada la licencia Flexed o Pooled, la página de **configuración de Analytics** (**Ajustes > Configuración de Analytics**) no se actualiza con los detalles correctos.

  Soluciónalternativa : actualice la página para obtener los detalles correctos.

  [NSADM-10665]

- El panel de licencias flexibles de **NetScaler Licensing > Flexed Licensing Dashboard** aparece en blanco.

  Soluciónalternativa : aplique una licencia de ancho de banda Premium.

  [NSADM-106561]

Administración y supervisión

- El agente ADM de NetScaler genera trampas SNMP «NetScalerLoginFailure». Este problema se produce porque las credenciales que utiliza el agente ADM para iniciar sesión en NetScaler se truncan debido a un carácter de nueva línea.

[NSHELP-36804]

- En un par ADM HA, se observó que el estado de la base de datos estaba **inactivo** y no se sincronizaba, incluso después de intentar varias veces con la opción **Sincronizar base de datos** en la GUI.

  [NSHELP-29626]

Notas de la versión 14.1—8.50 de NetScaler ADM

January 30, 2024

Este documento de notas de la versión describe las mejoras y los cambios, así como los problemas resueltos y conocidos que existen en la versión 14.1—8.50 de NetScaler ADM.

Notas

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

Novedades

Las mejoras y los cambios que están disponibles en las compilaciones 14.1—8.50.

Administración y supervisión

Soporte para la identificación y corrección de CVE-2023-4966 y CVE-2023-4967

> **Nota:**
>
> Puede ver los detalles del CVE-2023-4966 y del CVE-2023-4967 solo si ha habilitado el asesoramiento de seguridad a través de ADM On-Prem Cloud Connector. Para obtener más información, consulte ADM On-Prem Cloud Connector

El asesoramiento de seguridad de NetScaler ADM ahora admite la identificación y corrección de CVE-2023-4966 y CVE-2023-4967.

- La identificación requiere una combinación de análisis de versión y configuración.
- La solución requiere una actualización de las instancias vulnerables de NetScaler a una compilación recomendada que tenga la solución.

> **Nota:**
>
> Security Advisory no admite compilaciones de NetScaler que hayan llegado al final de su vida útil (EOL). Le recomendamos que actualice a las compilaciones o versiones compatibles con NetScaler.

Para obtener más información sobre cómo usar NetScaler ADM para actualizar las instancias de NetScaler, consulte Usar trabajos para actualizar las instancias de NetScaler.

Para obtener más información, consulte el Boletín de seguridad.

[NSADM-101092]

Análisis

Función para configurar la exportación de métricas de NetScaler a Prometheus a través de StyleBook Para exportar métricas de NetScaler a Prometheus, debe crear un perfil de análisis en NetScaler y especificar el archivo de esquema. Para obtener más información, consulte Supervisar NetScaler, las aplicaciones y la seguridad de las aplicaciones mediante Prometheus.

En **Aplicaciones > Configuración > StyleBooks > StyleBook predeterminado**, ahora puede usar el StyleBook **Prometheus TimeSeries Analytics Configuration** y ejecutar la configuración en todas las instancias administradas.

Para obtener más información, consulte StyleBook de análisis de Prometheus.

[NSADM-97698]

Ver la causa principal de la latencia de las aplicaciones La lentitud de las aplicaciones es una preocupación importante para cualquier organización, ya que tiene como resultado un impacto en el negocio o productividad. En **Applications > Web Insight**, ahora puede ver una nueva métrica llamada **Aplicaciones con anomalías en el tiempo de respuesta**. Con esta métrica, como administrador, puede analizar si la latencia de la aplicación se debe a las siguientes causas:

- Latencia de red del cliente
- Latencia de red del servidor
- Tiempo de procesamiento del servidor

Para obtener más información, consulte Ver la causa principal de la latencia de las aplicaciones.

[NSADM-97530]

Trabajo de configuración: Función para crear un trabajo para configurar la exportación de métricas de NetScaler a Prometheus Para exportar métricas de NetScaler a Prometheus, debe crear un perfil de análisis en NetScaler y especificar el archivo de esquema. Para obtener más información, consulte Supervisar NetScaler, las aplicaciones y la seguridad de las aplicaciones mediante Prometheus.

En **Configuration Job**, ahora puede crear un trabajo con la plantilla **NSConfigurePrometheusAnalyticsProfile** de la **plantilla incorporada**, especificar los parámetros necesarios y ejecutar el trabajo en todas las instancias administradas.

Para obtener más información, consulte Programar trabajos creados mediante plantillas integradas.

[NSADM-97251]

Asigne un perfil de red para el NetScaler administrado desde NetScaler ADM Al habilitar el análisis para los servidores virtuales en NetScaler ADM, los datos de AppFlow de NetScaler se exportan a NetScaler ADM a través de la dirección IP de subred de NetScaler (SNIP). En algunos casos, es posible que el SNIP esté bloqueado debido al firewall de la red. En estos casos, es posible que tenga que usar una dirección IP diferente a la del SNIP. Para obtener más información sobre el perfil de red, consulte Usar una IP de origen especificada para la comunicación del back-end.

Ahora puede asignar perfiles de red a una instancia de NetScaler mediante NetScaler ADM. Vaya a **Infraestructura > Instancias > NetScaler ADC**, seleccione la instancia y, en la lista **Seleccionar** acción, **haga clic en Configurar perfiles de red para asignar un perfil de red** a la instancia.

> **Nota:**
>
> Asegúrese de haber desactivado los análisis en todos los servidores virtuales antes de asignar un perfil de red a la instancia.

Con esta mejora, puede asignar un perfil de red para exportar datos de AppFlow de NetScaler a NetScaler ADM.

[NSADM-91836]

Infraestructura

Mejoras en el escenario de error de la actualización Cuando se produce un error en un trabajo de**actualización (Infraestructura > Trabajos**de actualización), el trabajo defectuoso provoca problemas de espacio en disco debido a la presencia de los archivos de compilación y otros archivos extraídos. Como resultado, el siguiente trabajo de actualización también falla.

Ahora se ha mejorado el escenario de error del trabajo de actualización. Si se produce un error en un trabajo de actualización, NetScaler ADM elimina el archivo de compilación anterior de la instancia de NetScaler.

[NSADM-97383]

Cambios de cambio de marca NetScaler ADM pasa a llamarse NetScaler ADM. Para alinearse con la nueva marca, también se actualiza la GUI de ADM.

[NSADM-97365]

Directiva de acceso para agentes locales Al crear una **directiva de acceso** con acceso de **edición** para el agente de ADM en **Configuración > Usuarios y roles > Directivas de acceso**, los usuarios asociados a esta directiva ahora pueden registrar el agente con sus credenciales.

[NSADM-97337]

Panel de administración de almacenamiento de datos disponible en la GUI de NetScaler ADM En **Configuración > Administración del almacenamiento de datos**, ahora puede ver y administrar la información de almacenamiento de datos en las diferentes funciones de su implementación actual. El panel de administración del almacenamiento de datos le ayuda a visualizar cómo se consume el almacenamiento en todas las funciones y le ayuda a controlar si el consumo de almacenamiento está dentro del umbral especificado.

El panel de control ofrece las siguientes funciones:

- Mosaicos**de ingestión de datos, almacenamiento, consumo**y **acciones** : los mosaicos proporcionan:
  - Estado de la actividad de ingesta de datos
  - Información sobre los datos consumidos y el espacio total disponible en disco
  - Opciones para revisar la directiva de retención de datos, realizar una depuración de datos y revisar las notificaciones del sistema
- **Tendencia de consumo de almacenamiento**: le ayuda a visualizar cómo se almacenan los datos en las diferentes funciones durante un período de tiempo
- **Consumo de almacenamiento por características**:
  - Muestra la distribución del almacenamiento de datos por diferentes funciones
  - Le permite realizar depuraciones de datos, ver el historial de las depuraciones de datos y ver las funciones eliminadas en cada depuración de datos

Para obtener más información, consulte Usar el panel de almacenamiento de datos.

[NSADM-97320]

Compatibilidad con el almacén de certificados SSL en NetScaler ADM Ahora puede administrar sus certificados SSL en **Infraestructura > Panel de control SSL > Almacén de certificados**.

Utilice el **almacén de certificados** para:

- Agregar, actualizar y eliminar certificados
- Instalar certificados en instancias de NetScaler
- Importación de certificados desde instancias de NetScaler

Para obtener más información, consulte Cómo usar el almacén de certificados.

[NSADM-97257]

El límite de sesiones de usuario ha cambiado a 40 En **Configuración > Usuarios y roles > Grupos**, puede configurar hasta 40 sesiones de usuario. De forma predeterminada, se le asignan 20 sesiones de usuario. Sin embargo, si pertenece a los grupos de usuarios de administración y de solo lectura, se le asignan 40 sesiones de usuario de forma predeterminada y este valor no se puede cambiar.

[NSADM-95314]

Reintentar trabajos de actualización fallidos En **Infraestructura > Trabajos de actualización**, ahora puede seleccionar el trabajo de actualización fallido y realizar una de las siguientes acciones:

- Haga clic en **Reintentar** junto al trabajo de actualización fallido.
- Vaya a **Seleccionar acción > Reintentar el trabajo de actualización**.

Para obtener más información, consulte Reintentar trabajos de actualización fallidos.

[NSADM-93439]

Cloud Connector ADM On-Prem Puede utilizar la función Cloud Connector para establecer una conexión entre ADM On-Prem y el servicio ADM. Esta conectividad le permite aprovechar la función de asesoramiento de seguridad de ADM On-Prem. El asesoramiento de seguridad le permite realizar un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE), evaluar el impacto de las CVE, comprender las soluciones y resolver las vulnerabilidades. Como administrador, puede supervisar las instancias de NetScaler en busca de nuevos CVE mediante un análisis periódico o un análisis manual, y tomar las medidas necesarias para solucionarlo.

Para obtener más información, consulte ADM On-Prem Cloud Connector.

[NSADM-92204]

Asesoramiento de seguridad sobre NetScaler ADM Puede configurar ADM On-Prem Cloud Connector y permitir que Security Advisory utilice la versión completa de la función Security Advisory en ADM on-prem. Anteriormente, el aviso de seguridad solo estaba disponible en la versión preliminar.

Para obtener más información, consulte Aviso de seguridad.

> **Nota:**
>
> Si no ha configurado o si ha desactivado el ADM On-Prem Cloud Connector, solo puede utilizar el aviso de seguridad como versión preliminar.

Para obtener más información sobre ADM On-Prem Cloud Connector, consulte ADM On-PremCloud Connector.

[NSADM-91726]

Administración y supervisión

Se requiere autenticación para que las operaciones de StyleBook accedan a las instancias de NetScaler Como administrador, ahora puede solicitar a los usuarios que proporcionen credenciales para todas las operaciones de StyleBook y del paquete de configuración realizadas en las instancias de NetScaler. Para activar esta función, sigue estos pasos:

- Vaya a **Configuración > Administración > Configuración del sistema, zona horaria, URL permitidas y del agente > Configuración básica**
- Seleccione **Solicitar credenciales para el inicio de sesión de la instancia**
- Seleccione **Prompt Credenciales para las operaciones de Stylebook**

Como alternativa, si selecciona **Solicitar credenciales para el inicio de sesión de la instancia** y desactiva **Solicitar credenciales para las operaciones de Stylebook**, no se solicitará un nombre de usuario ni una contraseña a las operaciones de Stylebook y del paquete de configuración realizadas en las instancias de NetScaler.

Para obtener más información, consulte Cómo habilitar el acceso al shell para usuarios no predeterminados.

[NSHELP-35432]

Acceso de solo lectura a los archivos de backup y las sesiones de usuario de NetScaler ADM Los usuarios con acceso de solo lectura ahora pueden ver las siguientes páginas:
Configuración > Usuarios y funciones > Sesiones*
**Configuración **Archivos de copia de seguridad

[NSHELP-35431]

Configurar el umbral de ingesta de datos Ahora puede configurar un umbral de ingesta de datos en **Configuración > Administración del almacenamiento de datos > Directiva de retención de datos > Sistema > Configuración de ingesta de datos**. Con esta configuración, puede configurar el proceso a nivel del sistema para que se detenga cuando el almacenamiento de datos alcance el valor umbral. Los valores límite aceptados son del 50% al 80%.

Para obtener más información, consulte Directiva de retención de datos.

[NSHELP-35237]

La versión de ADM y la dirección IP están disponibles en el archivo de soporte técnico La versión de ADM y la dirección IP ahora están disponibles en el archivo de soporte técnico desde **Configuración > Diagnóstico > Generar archivo de soporte técnico**.

[NSHELP-33551]

StyleBooks

Las siguientes funciones ya están disponibles en StyleBooks:

- Fuentes de datos: utilice instancias de NetScaler ADC como fuentes de datos o cree fuentes de datos personalizadas.
- GitHub Enterprise: importa y sincroniza StyleBooks y paquetes de configuración desde su servidor de GitHub Enterprise.
- Funciones integradas: se agregan las siguientes funciones integradas:
  - `match()`
  - `contains()`
  - `select()`
  - `hash_sha256()`
  - `relate()`
  - `splat()`
- Definiciones de StyleBook: actualice las definiciones de StyleBook personalizadas directamente desde la GUI de NetScaler ADM.
- Paquetes de configuración del repositorio de GitHub: Importa y sincroniza los paquetes de configuración de un repositorio de GitHub. Anteriormente, solo se permitían los StyleBooks.
- Atributo: `botinsight`Configure el tipo `botinsight` en la sección `insights` de StyleBooks.

[NSADM-97841]

Compatibilidad con atributos adicionales en análisis de StyleBooks La sección de análisis de StyleBooks ahora se ha mejorado para:
- Aceptar parámetros para configurar el modo de transporte (`transport-mode`)
- Configurar HDX Insight para diferentes tipos de tráfico (`enable-hdxinsight-for`)
- Habilitar la opción HTTP X-Forwarded-For () - Habilitar las mediciones del lado del cliente (`http-x-forwarded-for`)
`client-side-measurements`

Para obtener más información, consulte Gramática de StyleBooks.

[NSADM-97839]

Problemas resueltos

Los problemas que se abordan en las compilaciones 14.1—8.50.

Análisis

- La reducción periódica de los datos del panel de control de la aplicación no funcionó como se esperaba. Como resultado, NetScaler ADM consumió más espacio en disco.

  [NSHELP-36184]

- Cuando NetScaler ADM pierde las licencias del servidor virtual, se espera que el estado de análisis de los servidores virtuales que utilizan esas licencias esté inhabilitado. Este escenario no funcionaba como se esperaba para los servidores virtuales VPN.

  [NSHELP-36183]

Infraestructura

- En **Gateway > HDX Insight** y **Gateway > Gateway Insight**, el eje X de los gráficos muestra fechas en lugar de hora.

  [NSHELP-36043]

- El par ADM HA de NetScaler no se recupera del escenario de cerebro dividido debido a un fallo de sincronización en la comunicación de los latidos.

  [NSHELP-35934]

- La función del Programa de mejora de la experiencia de usuario del cliente (CUXIP) está habilitada para los usuarios y sus datos de uso se recopilan incluso después de que el administrador haya desactivado CUXIP en **Configuración > Administración > Configuración**de CUXIP.

  [NSADM-101771]

- Cuando usted, como administrador raíz, inició sesión en la GUI o API de NetScaler ADM con las credenciales predeterminadas por primera vez, no se le pidió que cambiara la contraseña predeterminada. Con esta solución, se ve obligado a cambiar la contraseña predeterminada.

  [NSADM-95328]

- Cuando se crean varios usuarios SNMP simultáneamente mediante un script, las solicitudes SNMP a ADM fallan.

  [NSADM-83924]

Administración y supervisión

- Las carpetas creadas en el directorio de copias de seguridad ADM de NetScaler no se eliminan durante la operación de eliminación de copias de seguridad que se programa cada 2 horas.

  [NSHELP-35911]

- La autenticación con LDAP externo falla de forma intermitente en NetScaler ADM y solo se resuelve reiniciando NetScaler ADM.

  [NSHELP-35733]

- El subsistema mas_perf de ADM se bloquea y aparece un mensaje de evento en **Configuración** > Eventos del sistema ADM.

  [NSHELP-35711]

- Los usuarios no pueden ver sus aplicaciones autorizadas en **Aplicaciones > Panel de control de aplicaciones**. Este problema se produce cuando los usuarios pertenecen a muchos grupos y cada grupo tiene muchas aplicaciones.

  [NSHELP-35165]

- Un análisis de Qualys realizado en NetScaler ADM informó de una débil vulnerabilidad activa de intercambio de claves SSL/TLS en los puertos de PostgreSQL.

  [NSHELP-34487]

- Si NetScaler se desconecta del servidor de licencias y vuelve a conectarse en 10 minutos, es posible que la licencia extraída por NetScaler aparezca dos veces en el servidor de licencias. Reinicie el servidor de licencias para liberar esta entrada obsoleta.

  [NSHELP-35420]

Provisioning

- Al aprovisionar NetScaler VPX en la nube (**Infraestructura > Instancias > NetScaler > VPX > Provision) mediante ESXi o VMware vCenter**, se ignora la configuración de licencias.

[NSHELP-35984]

- La provisión de NetScaler VPX en VMware vCenter**(Infrastructure > Instance > NetScaler > VPX > Provision) falla debido al mismo nombre que se usó en la instancia VPX**eliminada anteriormente.

  [NSHELP-35983]

StyleBooks

- Si crea un paquete de configuración a partir de una definición de StyleBook que tiene un servidor virtual de autenticación y enlaces de políticas de caché integrados y, a continuación, elimina el paquete de configuración, la eliminación se realiza correctamente. Sin embargo, si intenta volver a crear el paquete de configuración con los mismos parámetros, aparece el siguiente mensaje de error:
  `Resource already exists`.

  [NSHELP-35646]

- Cuando intenta migrar una configuración de ADC de una instancia de ADC de origen a una instancia de destino en **Aplicaciones > Configuración > Paquetes de configuración > Migrar ADC > Comenzar > Especificar configuración** y hace clic en **Siguiente**, aparece el siguiente mensaje de error de forma intermitente:

  `No Job found`.

  [NSADM-97948]

Problemas conocidos

Los problemas que existen en las versiones 14.1—8.50.

Infraestructura

- En **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**, al seleccionar una instancia vulnerable de NetScaler con un CVE y **hacer clic en Continuar con el flujo de trabajo de actualización**, aparece el siguiente mensaje de error:

  «La instancia de NetScaler seleccionada no requiere este flujo de trabajo de corrección»

  Solución alternativa: actualice manualmente la instancia de NetScaler **desde**Infraestructura > Trabajos de actualización.

  [NSADM-103649]

- Después de configurar un nuevo ADM de NetScaler, puede aparecer el siguiente mensaje de error: `Error in operation - Metrics not found`.

  Este problema se produce porque el trabajo de purga automática de datos aún no se ha ejecutado, lo que provoca la ausencia de datos. El trabajo está programado para ejecutarse durante 3 horas y, una vez ejecutado, se generan los datos necesarios y el mensaje de error ya no aparece.

  [NSADM-103157]

- Cuando se exporta un informe de una página desplazable en NetScaler ADM, el informe exportado puede truncar el contenido que se extiende más allá de la altura de la ventana visible.

  [NSADM-102765]

- Al intentar instalar un certificado en una instancia de NetScaler BLX, se produce un error en la instalación y la página **Infraestructura > Panel de control de SSL > Registros de auditoría de SSL muestra el** siguiente mensaje de error:

  `SCP: Authentication by password fails on _<ip-address>_.`

  [NSADM-102202]

- El agente de NetScaler no se registra en NetScaler ADM si alguna de sus contraseñas tiene el símbolo %23.

  [NSADM-100613]

Administración y supervisión

- En un par ADM HA, se observó que el estado de la base de datos estaba **inactivo** y no se sincronizaba, incluso después de intentar varias veces con la opción **Sincronizar base de datos** en la GUI.

  [NSHELP-29626]

Notas de lanzamiento de la versión 14.1-4.42 de NetScaler ADM

January 30, 2024

Este documento de notas de la versión describe las mejoras y los cambios, los problemas corregidos y conocidos que existen en la versión 14.1-4.42 de NetScaler ADM.

Notas

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

Novedades

Las mejoras y los cambios que están disponibles en la compilación 14.1-4.42.

Análisis

Web Insight: soporte para ver la distribución porcentual en función de las solicitudes En **Web Insight**, ahora puede ver la **distribución porcentual por solicitudes** en las siguientes métricas:

- Clientes
- Servidores
- Ubicaciones geográficas
- URLs

Como administrador, esta mejora le permite comprender la distribución porcentual recibida en función del total de solicitudes durante la duración seleccionada. Por ejemplo, puede comparar la forma en que los servidores reciben las solicitudes durante la duración seleccionada.

Para obtener más información, consulte Web Insight.

[NSADM-96158]

Soporte para exportar desde cada widget en Web Insight En **Web Insight**, la opción de exportación ahora está incluida en todos los widgets y permite exportar datos en formato tabular. Con esta mejora, puede:

- Exporte los datos necesarios de forma individual desde cualquier widget.
- Desglosa cualquier métrica y exporta también los datos necesarios desde cualquier widget.

Anteriormente, los datos de exportación solo proporcionaban el informe consolidado.

> **Nota:**
>
> También puede seguir utilizando la opción de exportación existente para generar el informe consolidado.

[NSADM-94140]

Un panel unificado para ver los detalles de las métricas clave de la instancia Como administrador, ahora puede visualizar un panel que proporciona una descripción general de los detalles de las métricas clave en función de:

- Aplicaciones
- Infraestructura ADC
- Seguridad de las aplicaciones
- Gateway

Este panel de control de un solo panel le permite ver los detalles para una mejor experiencia de supervisión del uso y el rendimiento de la instancia.

Para obtener más información, consulte Panel unificado

[NSADM-94137]

Exporte datos de métricas y eventos de ADM a Splunk y New Relic Al crear una nueva suscripción en **Configuración > Integración del ecosistema** para la integración de NetScaler ADM con Splunk y New Relic, ahora puede seleccionar la opción **Eventos de ADM** y **métricas** de ADM. Después de configurar la suscripción con una de estas opciones o ambas, puede ver los datos correspondientes en el panel de control de Splunk y New Relic.

Para obtener más información, consulte Integración con Splunk e Integración con New Relic.

[NSADM-93765]

Ver la calificación SSL de una aplicación En **Aplicaciones > Panel de control**, ahora puede ver la calificación SSL de una aplicación. Puedes revisar los problemas de SSL y actualizar la aplicación para obtener una calificación A+ . Sin embargo, si observa alguna caída en el tráfico debido a esta actualización, puede deshacer el perfil de front-end seguro configurado en su aplicación. Esta acción revierte la calificación A+ a una calificación anterior.

Para obtener más información, consulte Análisis de calificación SSL A+.

[NSADM-92025]

Web Insight: soporte para ver valores nulos en gráficos En **Web Insight** , al desglosar cualquier métrica en **Aplicaciones** , clientes, URL o instancias, la vista de análisis ahora proporciona la visibilidad de los valores nulos (por ejemplo, 0 ms y 0 solicitudes) en el gráfico durante la duración seleccionada.

Anteriormente, si no se recibía tráfico ni transacciones durante el período seleccionado, Web Insight mostraba los gráficos omitiendo esos valores nulos. Como administrador, ahora puede ver el gráfico completo con estos valores nulos.

[NSADM-88686]

Infraestructura

Compatibilidad con contraseñas de nodos RPC para la implementación de alta disponibilidad de NetScaler Ahora puede configurar la contraseña del nodo RPC al crear los nodos principal y secundario en una implementación de alta disponibilidad. Vaya a **Infraestructura > Trabajos de actualización > Crear trabajo > Configurar un par de instancias de NetScaler de alta disponibilidad** para introducir las contraseñas de los nodos de RPC para los nodos de alta disponibilidad.

Para obtener más información, consulte Programar la configuración de un par de instancias de NetScalerde alta disponibilidad.

[NSADM-93912]

El agente ADM de NetScaler almacena en caché las imágenes de NetScaler El tiempo necesario para la actualización de NetScaler ahora se reduce considerablemente, ya que las imágenes de NetScaler se almacenan en caché en el agente NetScaler ADM después de descargarlas. Por lo tanto, no es necesario descargar las imágenes para los trabajos de actualización posteriores.

> **Nota:**
>
> Esto solo se aplica a los ADC que se agregan mediante el agente NetScaler ADM.

Para obtener más información, consulte Crear un trabajo de actualización de ADC.

[NSADM-76343]

Ver la cadena de certificados completa Ahora puede ver la cadena completa de enlaces de un certificado, incluidos los certificados intermedios hasta el certificado de CA raíz.

Para ver la cadena de certificados, vaya a **Infraestructura > Panel de control SSL**, elija un certificado SSL y haga clic en **Detalles**.

Para obtener más información, consulte Ver cadena de certificados SSL.

[NSADM-52467]

StyleBooks

Soporte para tipos de argumentos adicionales en la función replace() La función integrada «replace ()» también puede aceptar una lista de los siguientes tipos integrados:

- `string`

- `ipaddress`
- `tcp-port`
- `number`
- **`boolean`**

Para obtener más información, consulte Funciones integradas.

[NSADM-96802]

Soporte para la función multiple () Las funciones integradas de StyleBooks ahora admiten la función multiple (). La función multiple (argument1, argument2) toma dos argumentos y devuelve una lista con muchas copias del argumento 1. El número de copias es igual al número pasado al argumento 2.

Para obtener más información, consulte Funciones integradas.

[NSADM-95973]

Soporte para secciones opcionales en los paquetes de configuración de StyleBook Las secciones `targets` y `stylebook` ahora son opcionales en la carga útil del paquete de configuración. Si no especifica estas secciones para actualizar un paquete de configuración, las últimas secciones `targets` y `stylebook` utilizadas se obtienen de la base de datos ADM de NetScaler y se actualiza el paquete de configuración.

[NSADM-92377]

Especifique el acceso del grupo de usuarios a los paquetes de configuración Como administrador, ahora puede impedir que los grupos de usuarios accedan a los paquetes de configuración creados por otros grupos de usuarios. Para seleccionar esta opción, vaya a Configuración **> Usuarios y funciones > Grupos > Configuración de autorización > Paquetes de configuración > Todas las configuraciones creadas por el grupo de usuarios** .

Para obtener más información, consulta la sección **Paquetes de configuración** en Crear un grupo de usuarios.

[NSADM-92374]

Problemas resueltos

Los problemas que se abordan en la compilación 14.1-4.42.

Análisis

- El par NetScaler ADM HA puede provocar un escenario de cerebro dividido de forma intermitente.

  [NSHELP-35430]

- Las transacciones web HTTP que no tienen un valor de parámetro de consulta en la URL no se muestran en el panel de NetScaler ADM Web Insight (**Applications**Web Insight).

  Por ejemplo, si la URL `https://www.google.com/search?q=abstract%20api` no tiene el valor del parámetro de consulta y está disponible como `https://www.google.com/search?q=`, las transacciones HTTP se descartan y no están disponibles en el panel.

  [NSADM-99448]

- En **Web Insight**, al desglosar cualquier métrica para ver los detalles y, a continuación, profundizar en cualquier métrica, el gráfico permanece en la vista anterior, pero todos los demás detalles aparecen como se esperaba.

  Como resultado, esto crea la suposición de que el desglose adicional no funciona como se esperaba.

  [NSADM-98995]

Infraestructura

- Faltan instancias MPX en la página **Infraestructura > Inventario de NetScaler > NetScaler (MPX/VPX/CPX/BLX**).

  [NSHELP-35593]

- Cuando inicia sesión en la GUI de NetScaler ADM con autenticación de usuario LDAP y utiliza «dominio\ nombre de usuario», las preferencias del usuario no se guardan.

  [NSADM-100995]

- Al ejecutar comandos en una partición para cualquier trabajo de configuración, aparece el siguiente mensaje de error: «Comando bloqueado para el dispositivo de partición de administración».

  Este problema aparece en las versiones 13.1-42.47 de NetScaler y versiones posteriores.

  [NSADM-100416]

- Tras realizar una conmutación por error para un par de HA de ADM en **Configuración > Implementación > Forzar la conmutación por error**, no verá los detalles del nodo secundario en la página **Configuración > Implementación**.

[NSADM-98674]

- Cuando intenta agregar un perfil de Slack en **Configuración > Notificaciones > Slack > Agregar**, el perfil no se agrega y aparece el siguiente mensaje de error:

  `Please check internet connectivity`.

  [NSADM-98633]

- Cuando usted, como administrador raíz, inició sesión en la GUI o API de NetScaler ADM con las credenciales predeterminadas por primera vez, no se le pidió que cambiara la contraseña predeterminada. Con esta solución, se ve obligado a cambiar la contraseña predeterminada.

  [NSADM-95328]

Administración y supervisión

- Al hacer una copia de seguridad de una instancia de NetScaler o restaurarla, no se hace copia de seguridad del directorio /var/metrics_conf.

  [NSHELP-35724]

- Cuando exporta los informes de caducidad de SSL para una semana, 30 o 90 días desde **Infraestructura > Panel de control SSL > Certificados SSL > Exportar informes** y selecciona **Tabular** , el informe resultante muestra una columna de dominio vacía.

  [NSHELP-35592]

- En **Infraestructura > Panel de control SSL > Certificados SSL**, el par de alta disponibilidad de NetScaler no muestra los superíndices “P”y “S”para los dispositivos principales y secundarios.

  [NSHELP-35523]

- El estado de NetScaler ADM aparece como **Inactivo** de forma intermitente incluso después de que todos los procesos estén activos y en ejecución.

  [NSHELP-35408]

- En el caso de varias direcciones IP de clúster (CLIP) en un clúster, al agregar un CLIP entre corchetes en **Infraestructura > Instancias > NetScaler Agregar**, la configuración falla y el CLIP no se agrega a NetScaler ADM.

  [NSHELP-35323]

- En **Infraestructura > Configuración > Trabajos de configuración > Crear trabajo > Seleccionar configuración**, al introducir una variable de contraseña (`$password$`) y conservar el campo **Escribir** como **texto en lugar del campoContraseña**y hacer clic en**Siguiente**, la página no se carga.

  [NSHELP-35266]

- El proceso de inventario de NetScaler ADM se bloquea de forma intermitente cuando se envían solicitudes a otros procesos de ADM.

  [NSHELP-35048]

- NetScaler ADM no responde debido a varios bloqueos de subsistemas.

  [NSHELP-34633]

- El sitio principal (el par NetScaler ADM HA) sigue intentando sincronizar los datos con el nodo de recuperación ante desastres de NetScaler ADM y falla.
  Este problema se produce cuando el sitio principal tiene datos de gran tamaño (>1 GB).

  [NSHELP-32750]

Provisioning

- La provisión de NetScaler VPX en SDX (Infraestructura**> Instancias > NetScaler ADC > VPX) falla en NetScaler ADM**.

  [NSHELP-35347]

StyleBooks

- La implementación de los paquetes de configuración puede fallar cuando la definición de StyleBook incluye la `operations`sección.

  [NSHELP-35588]

- Cuando agrega algunas versiones de Infoblox como proveedor de IPAM en **Configuración > IPAM > Agregar** , aparece el siguiente mensaje de error:

  ```
  Invalid provider information: Invalid attributes for registering provider.
  ```

  [NSHELP-35302]

Problemas conocidos

Los problemas que existen en la versión 14.1-4.42.

Infraestructura

- El agente de NetScaler no se registra en NetScaler ADM si alguna de sus contraseñas tiene un símbolo. #

[NSADM-100613]

- En **Configuración > Administración > Instalar certificados SSL**, si el nombre del archivo de certificado que carga está entre paréntesis, se produce un error al instalar el certificado SSL en NetScaler. Aparece el siguiente mensaje de error:

  «Solicitud POST no válida, la carga útil debe comenzar con object=».

  [NSADM-99531]

Administración y supervisión

- En un par ADM HA, se observó que el estado de la base de datos estaba **inactivo** y no se sincronizaba, incluso después de intentar varias veces con la opción **Sincronizar base de datos** en la GUI.

  [NSHELP-29626]

Migración local de NetScaler ADM a Citrix Cloud

January 30, 2024

Puede migrar **NetScaler ADM 13.0 64.35 local o una versión posterior** a Citrix Cloud. Si su ADM tiene 12.1 o una versión anterior, primero debe actualizar a **13.0 64.35 o una versión posterior** y, a continuación, migrar a Citrix Cloud. Para obtener más información, consulte la sección Actualización.

> **Nota:**
>
> El servicio NetScaler ADM ahora pasa a llamarse servicio NetScaler Console. La interfaz de usuario y la documentación de nuestro producto se están actualizando actualmente para reflejar estos cambios. Durante este tiempo, es posible que encuentre que los nombres más antiguos y más nuevos se hacen referencia indistintamente. Le agradecemos su comprensión durante esta transición.

El servicio NetScaler Console a través de Citrix Cloud le permite obtener:

- Lanzamientos más rápidos, aproximadamente cada dos semanas con las últimas actualizaciones de funciones.
- Análisis basado en aprendizaje automático para seguridad de aplicaciones y bot, rendimiento y uso.

- Otras funciones que actualmente solo se admiten en el servicio NetScaler Console, como el análisis de los períodos de mayor actividad y escasez, el análisis basado en el aprendizaje automático para la seguridad de las aplicaciones y los bots, el análisis de la CPU de las aplicaciones y muchas más.

Para una migración correcta, debe:

- Asegúrese de tener conexión a Internet en ADM local para la accesibilidad de Citrix Cloud
- Configurar el agente de NetScaler
- Obtenga el cliente y el archivo CSV secreto de Citrix Cloud
- Valide la licencia de NetScaler Console
- Migrar mediante un script

Tras migrar de ADM local al servicio de consola de NetScaler, si desea volver a continuar con ADM local, puede usar el script de reversión. Para obtener más información, consulte Volver a ADM local.

Configurar el agente de NetScaler

Para habilitar las comunicaciones entre las instancias de NetScaler y NetScaler ADM, debe configurar un agente. De forma predeterminada, los agentes de NetScaler ADM se actualizan automáticamente a la versión más reciente. También puede seleccionar una hora específica para la actualización del agente. Para obtener más información, consulte Configuración de los valores de actualización del agente.

- Si su ADM local actual (par independiente o de alta disponibilidad) no tiene ningún agente local configurado, debe configurar al menos un agente para el servicio de consola de NetScaler.
- Si su ADM local existente (par independiente o de alta disponibilidad) se ha configurado con agentes locales para implementaciones en varios sitios, debe configurar la misma cantidad de agentes para el servicio NetScaler Console.

Para obtener más información sobre la configuración de un agente, consulte la sección Introducción.

Obtenga el cliente y el archivo CSV secreto de Citrix Cloud

Después de configurar el agente, obtenga el cliente y el archivo CSV secreto de la página de Citrix Cloud:

1. Inicie sesión en citrix.cloud.com
2. Haga clic en el icono **Inicio** y seleccione **Administración de identidades y accesos**.

3. En la ficha **Acceso API**, introduzca un nombre de cliente seguro y haga clic en **Crear cliente**.
4. Se generan ID y Secret. Haga clic en **Descargar** y guarde el archivo CSV en el ADM local.

   Por ejemplo, guarde el archivo CSV en el directorio /var.

Valide las licencias de servicio de NetScaler Console

Debe obtener licencias para el servicio NetScaler.

- Las licencias VIP del servicio NetScaler Console deben ser superiores o iguales a las licencias VIP locales.

  > **Nota**
  >
  > Si las licencias VIP son inferiores, los servidores virtuales se seleccionan de forma aleatoria y se produce un error en la configuración de nivel VIP para el servicio NetScaler Console.

- Si utiliza la implementación local de ADM como servidor de licencias, reasigne las licencias al servicio NetScaler Console antes de la migración. Para obtener más información, consulte Configurar un servidor ADM solo como servidor de licencias agrupado y Cómo reasignar un archivo de licencias.
- Si utiliza las licencias agrupadas en ADM local, debe obtener las licencias agrupadas para el servicio NetScaler Console y, a continuación, asignar las licencias a las instancias de ADC. Para obtener más información, consulte Configurar licencias agrupadas. Las siguientes versiones admitidas de ADC permiten modificar la asignación de licencias desde ADM:
  - NetScaler SDX: 13.0 74.11 o versiones posteriores.
  - NetScaler VPX y MPX: 13.0 47.24 o versiones posteriores, 12.1 58.14 o versiones posteriores y 11.1 65.10 o versiones posteriores.

Migrar mediante un script

- Con la compilación ADM 82.x, puede seleccionar la función y, a continuación, migrar.
- Para las compilaciones ADM 76.x o posteriores, los scripts de migración (`servicemigrationtool.py` y `config_collect_onprem.py`) están disponibles como parte de la compilación, disponible en `cd /mps/scripts`.
- Para compilaciones de ADM anteriores a 76.x, debe descargar los scripts de migración y copiar los scripts en ADM local.

> Nota
>
> Asegúrese de que el ADM local tenga conectividad a Internet durante la migración.

1. Con un cliente SSH, inicie sesión en el ADM local.

   > Nota
   >
   > Para un par ADM HA, inicie sesión en el nodo principal.

2. Escribe **shell** y presiona **Entrar** para cambiar al modo bash.
3. Copie el ID de cliente y el archivo CSV secreto. Por ejemplo, copie el archivo en el directorio /var.

   Después de copiar el archivo CSV, puede validar si el archivo CSV está presente.

   ```
   bash-3.2# cd /var
   bash-3.2# pwd
   /var
   bash-3.2# ls -ltr secureclient.csv
   -rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
   bash-3.2#
   ```

   > Nota
   >
   > Para un par ADM HA, copie el archivo CSV en el nodo principal.

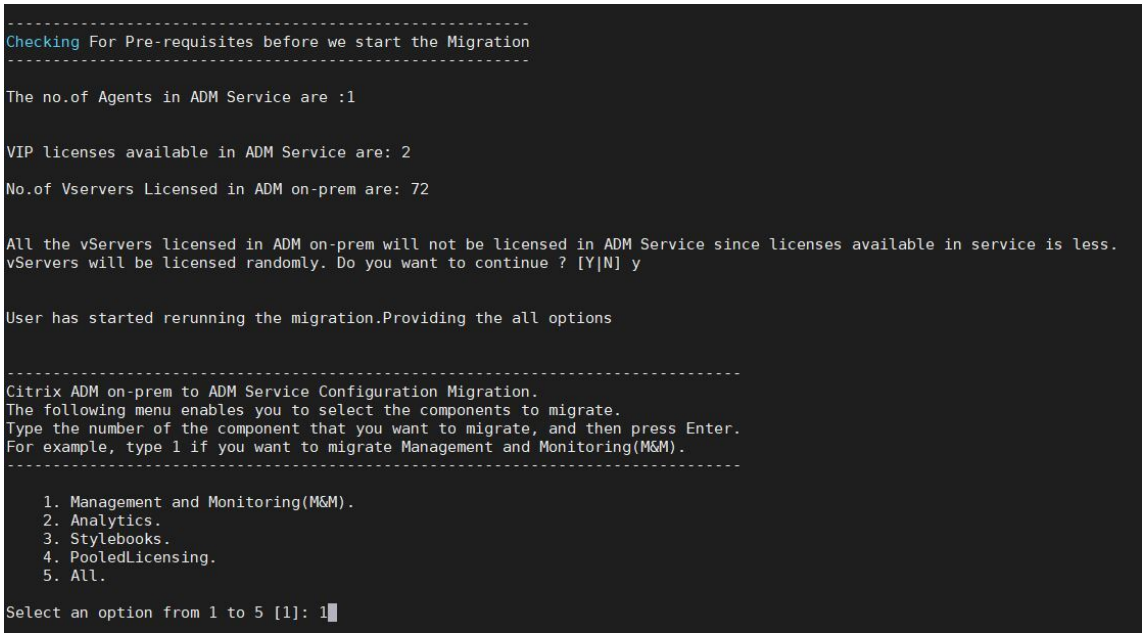
4. Para la **versión ADM 13.0 82.xx**, ejecute los siguientes comandos para completar la migración:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler ADM VM>`

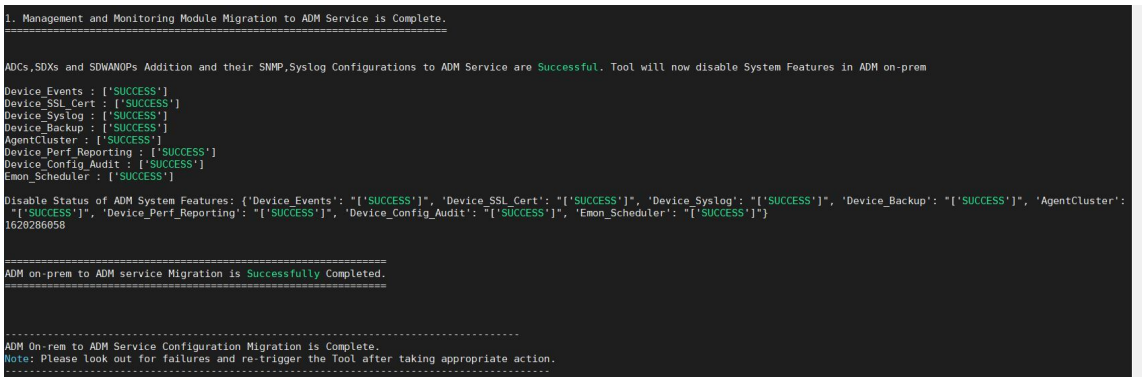
   Por ejemplo, `python servicemigrationtool.py /var/secureclient.csv`

   Después de ejecutar el script de migración, la herramienta muestra las siguientes opciones:



Según la opción que proporcione, solo esa función se migrará al servicio NetScaler Console.

En el ejemplo, se selecciona la opción 1. La herramienta completa la migración de Administración y supervisión (M&M) y muestra el siguiente mensaje:



La función **de gestión y supervisión (M&M)** incluye:

- Instancias ADC, etiquetas, grupos de instancias, perfiles, aplicaciones personalizadas, trabajos de configuración, SNMP, configuraciones de syslog.
- Sitios, bloqueos de IP, informes de red, umbrales de análisis, configuración de notificaciones, configuración de eliminación de datos.
- Configura plantillas de auditoría, intervalos de sondeo, reglas de eventos y ajustes.
- Grupos, roles y directivas de RBAC

La función de **análisis** incluye:

- Configuración de Appflow por servidor virtual desde instancias de ADC.

- Configuración de Appflow por dispositivo SD-WAN.

> Nota:
>
> - La función Administración y supervisión (M&M) se migra automáticamente, incluso si selecciona cualquier otra función (2, 3 o 4).
> - Solo puede especificar una función a la vez.
> - Después de completar la migración de cualquier función, si quiere migrar cualquier otra función más adelante, la función que ya se ha migrado no se muestra en la lista. Por ejemplo, si primero completa la migración de la función de **Analytics**, la próxima vez que ejecute el script de migración, solo podrá ver las opciones **StyleBooks**, **Licencias agrupadas** y **Todo**.
> - Al migrar las licencias agrupadas, migran todos los tipos, incluidos los servidores virtuales.

5. Para la **versión de ADM 13.0 76.xx**, ejecute los siguientes comandos para completar la migración:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises NetScaler ADM VM>`

   Por ejemplo, `python servicemigrationtool.py /var/secureclient.csv`

6. Para ADM anterior a 13.0 76.xx versión:

   a) Descargue el script de migración desde la siguiente ubicación: `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

   b) Guarde los dos scripts en ADM local. Por ejemplo, guarde en el directorio /var

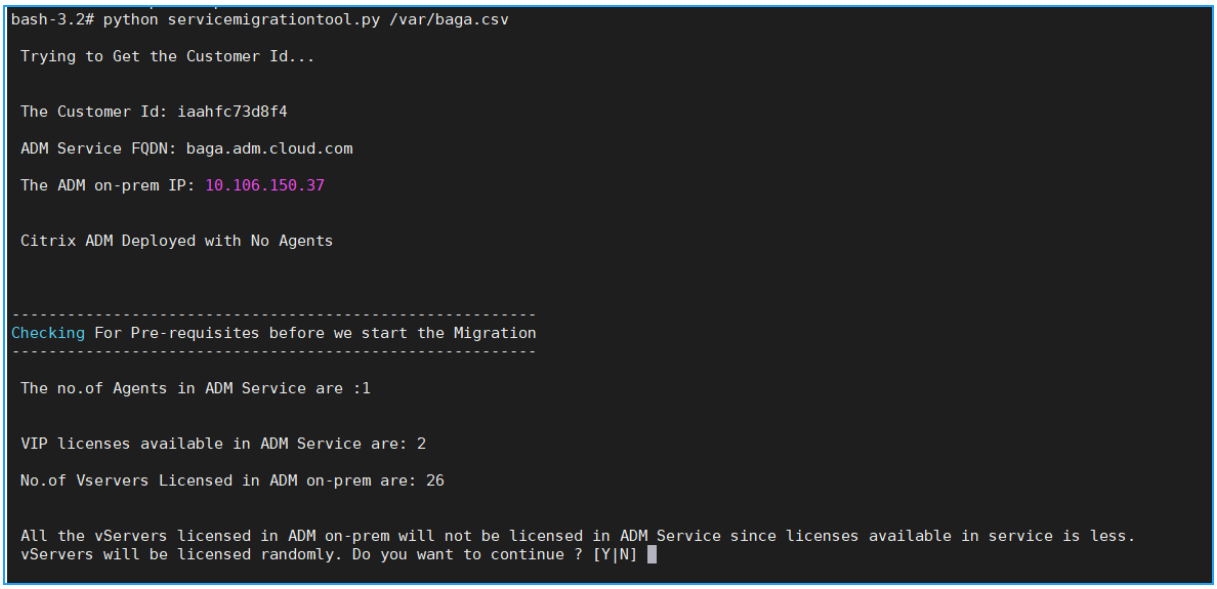
   c) Ejecute los siguientes comandos para migrar:

      i. `cd /var`

      ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

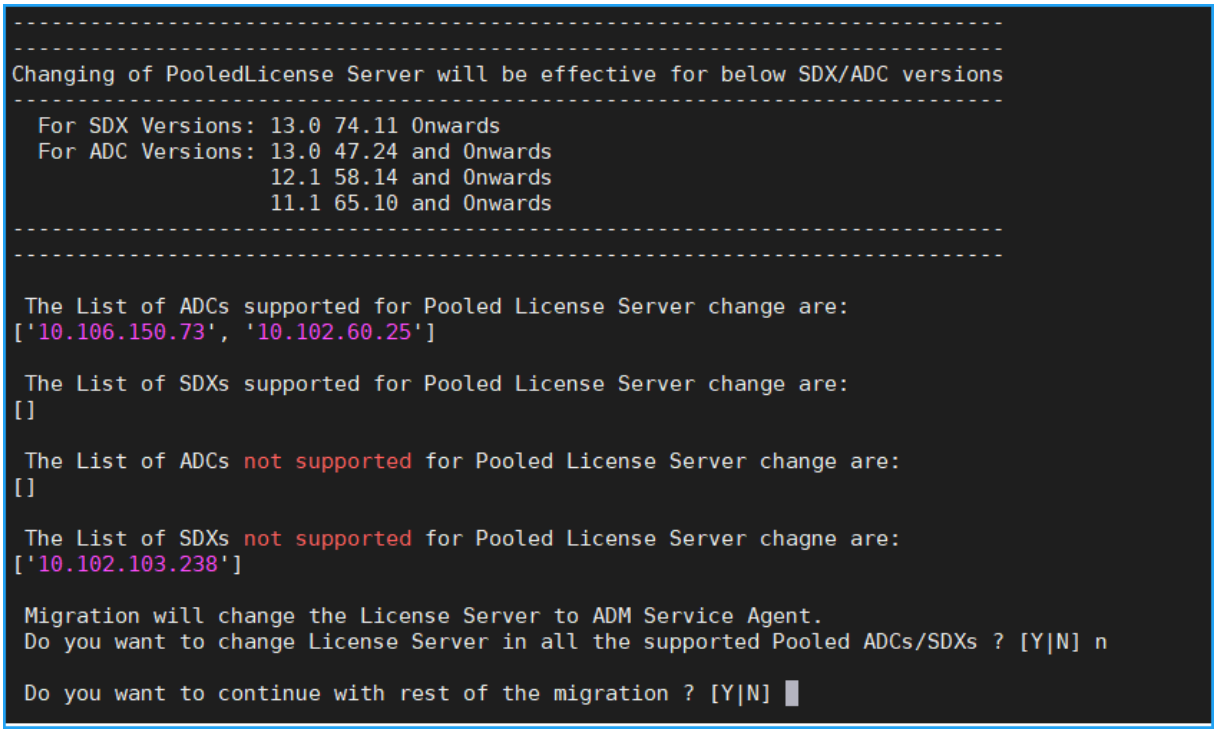
      Por ejemplo, `python servicemigrationtool_27.py /var/secureclient.csv`

Después de ejecutar el script, comprueba los requisitos previos y, a continuación, procede con la migración. En primer lugar, el script comprueba la disponibilidad de la licencia. El siguiente mensaje solo aparece si tiene una licencia de servicio de NetScaler Console inferior a la licencia local.



Si selecciona **Y**, la migración continúa otorgando licencias al VIP aleatoriamente. Si selecciona **N**, el script detiene la migración.

Si tiene la versión de instancia ADC no compatible para el servidor de licencias agrupado, aparecerá el siguiente mensaje:



Si selecciona **Y**, el proceso de migración continúa cambiando el servidor de licencias. Si selecciona **N**, el script le preguntará si quiere continuar con el resto de la migración. El script detiene la migración si selecciona **N**.

Dependiendo de la configuración local, el tiempo aproximado para completar la migración es entre unos minutos y unas horas. Una vez completada la migración, verá el siguiente mensaje:

```
--------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
--------------------------------------------------------------------------------
```

La migración se realiza correctamente una vez que todas las instancias de ADC y sus respectivas configuraciones se transfieren correctamente al servicio NetScaler Console. Después de la migración correcta, NetScaler ADM local deja de procesar los siguientes eventos de instancia:

- Certificados de SSL
- Mensajes de Syslog
- Backup
- Cluster de agentes
- Informes de rendimiento
- Auditoría de configuración
- Emon programador

Volver a ADM local

Si quiere volver a ADM local, asegúrese de que se cumplan los requisitos previos.

Requisitos previos

Si su ADM local (antes de migrar al servicio de consola NetScaler) es:

- Si se utiliza como servidor de licencias agrupadas, asegúrese de tener las licencias agrupadas necesarias en la ADM local.
- Configurado con agentes ADM locales, asegúrese de que los agentes estén disponibles en estado “ACTIVO”.

Usar el script de reversión

> Nota
>
> Después de la reversión, las mismas configuraciones (antes de la migración) en Analytics, SNMP y las licencias agrupadas vuelven a estar disponibles en ADM local. Si ha realizado algún cambio en estas configuraciones después de la migración, estos cambios no se reflejan en ADM local.

- Para compilaciones de **ADM 82.xx o posteriores**, el script de reversión está disponible como parte de la compilación y se puede acceder a él en `/mps/scripts`.
- Para compilaciones de **ADM anteriores a 79.xx**, puede actualizar a la compilación 82.x y usar el script de rollback o puede descargar el script de rollback y copiar el script en ADM local.

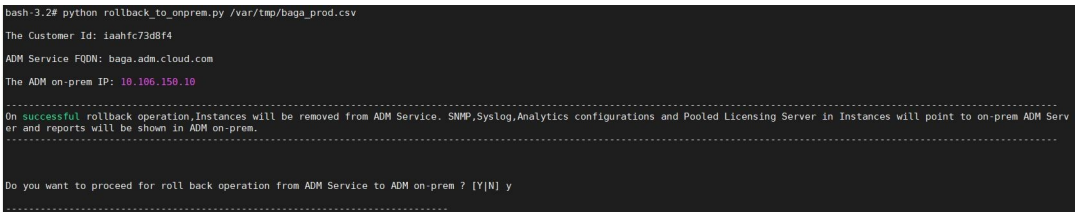
1. Con un cliente SSH, inicie sesión en el ADM local.
2. Escribe shell y presiona Enter para cambiar al modo bash.
3. Para la compilación ADM **13.0 82.xx**, ejecute los siguientes comandos para completar la reversión:

   a) cd /mps/guiones

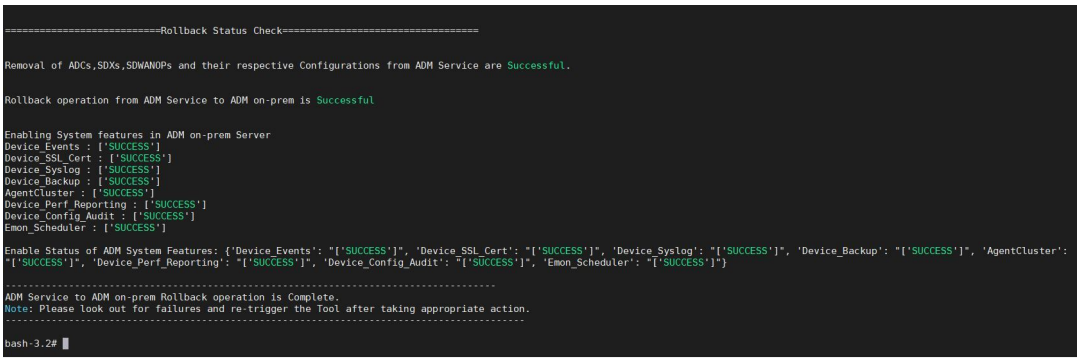
   b) python rollback_to_onprem.py <`path of ClientID/Secret File in ADM on-prem VM`>

   Por ejemplo, `python rollback_to_onprem.py /var/ secureclient.csv.csv`

   La herramienta inicia la operación de reversión y un mensaje le pregunta si quiere continuar. Escriba **Y** para continuar.



   Puede ver el siguiente mensaje después de que se complete la reversión.



4. Para la compilación ADM anterior a la versión 82.xx:

a) Descargue el script de reversión desde la siguiente ubicación:

```
https://download.citrixnetworkapi.net/root/download/v1/public
/software?product=admonprem&build=migrationtool&model=servicemigration
.tgz
```

b) Para las compilaciones de ADM 79.xx y 76.xx, guarde el script `/mps/scripts` y ejecute los siguientes comandos para la reversión:

   i. `cd /mps/scripts`

   ii. `python rollback_to_onprem.py < path of client/secret csv file in ADM on-prem>`

   Por ejemplo, `python rollback_to_onprem.py /var/ secureclient.csv`

c) Para compilaciones de ADM anteriores a 76.xx, guarde el script en ADM local. Por ejemplo, guárdelo en la ubicación `/var` y ejecute los siguientes comandos para la reversión:

   i. `cd /var`

   ii. `python rollback_to_onprem_27.py < path of client/secret csv file in ADM on-prem>`

   Por ejemplo, `python rollback_to_onprem_27.py /var/secureclient.csv`

La herramienta inicia la operación de reversión y un mensaje le pregunta si quiere continuar. Escriba **Y** para continuar.

Preguntas frecuentes

January 30, 2024

Servicio ADM

¿El agente de servicio ADM es opcional similar al agente de NetScaler ADM local?

No. El agente de servicio ADM es obligatorio para el servicio ADM y todas las comunicaciones entre instancias y el servicio ADM se producen a través del agente de servicio ADM. El agente ADM local es opcional; sin embargo, puede configurar el agente local solo para ahorrar el consumo de ancho de banda.

¿Por qué el servicio ADM?

El servicio ADM a través de Citrix Cloud ofrece las siguientes ventajas, sin necesidad de nuevas compilaciones periódicas:

- Oferta SaaS basada en la nube con incorporación más fácil y menor coste de propiedad que el NetScaler ADM local.
- Lanzamientos más rápidos, aproximadamente cada dos semanas con las últimas actualizaciones de funciones.
- Análisis basado en aprendizaje automático para la seguridad, el rendimiento y el uso de las aplicaciones.
- Varias otras funciones que actualmente solo se admiten en el servicio ADM, como análisis de períodos pico y lean, análisis de seguridad de aplicaciones basadas en aprendizaje automático para WAF y bot, análisis de CPU de aplicaciones y muchas más.

También puede unirse al seminario web mensual del servicio NetScaler ADM para conocer las últimas funciones y soluciones del producto. Regístrese en el seminario web mediante el siguiente enlace:

`https://www.citrix.com/events/2022/whats-new-with-citrix-application-delivery-management.html`

¿Qué ocurre después de la migración si NetScaler ADM local es un par HA?

Todas las configuraciones se mueven a Citrix Cloud. No es necesario configurar un nodo de recuperación ante desastres.

¿Qué pasa si el agente cae por alguna razón?

Puede esperar una posible pérdida de datos hasta que el agente esté en funcionamiento. Sin embargo, también puede configurar agentes ADM para implementaciones multisitio para garantizar la continuidad si hay una conmutación por error del agente. Para obtener más información, consulte Configurar agentes ADM para la implementación en varios sitios.

¿También se migra la copia de seguridad de instancias?

La copia de seguridad no se incluye en la migración.

¿También se migran los datos históricos?

Los datos históricos no se migran. Puede exportar los datos desde el ADM local.

¿También se migran las licencias locales?

No. El archivo de licencia local no se puede utilizar para el servicio ADM. Debe obtener licencias para el servicio ADM. Para obtener más información, consulte Licencias. Si utiliza licencias agrupadas en ADM local, debe obtener licencias agrupadas para el servicio ADM y, a continuación, asignar licencias a instancias.

¿Qué no se migra desde NetScaler ADM local?

Las siguientes funciones no se pueden migrar al servicio ADM:

- **RBAC**: En el servicio ADM, el acceso del usuario se basa en la invitación del administrador. Los usuarios del servicio ADM deben tener una cuenta en Citrix Cloud. Como resultado, los usuarios de ADM locales no se migran.
- **Exportar programas**: Las programaciones de exportación incluyen detalles como desglose y programaciones de varias páginas. Todas estas programaciones detalladas de exportación no se migran.
- **Certificados/claves/CSR SSL**: El servicio ADM solo puede mostrar los certificados/claves/-claves/CSR ADC SSL. Como resultado, los certos/claves SSL cargados en NetScaler ADM local no se migrarán al servicio ADM.

NetScaler ADM local está integrado con Citrix Director. ¿Qué pasa con la integración?

Actualmente, la integración de Director con ADM solo se admite en ADM local.

Después de la migración, ¿se requiere de nuevo la licencia de la instancia o habilitar el análisis?

Debe asegurarse de que las licencias del servicio ADM sean superiores o iguales a las licencias VIP locales. Si las licencias ya son superiores a la VIP local de NetScaler ADM, los servidores virtuales se otorgan automáticamente a los servidores virtuales. De lo contrario, las licencias se asignan aleatoriamente.

Herramienta de migración

Después de ejecutar el script de migración, se muestran los mensajes de error. ¿Cuál puede ser el problema?

Se muestra un archivo de registro con motivos de error. Puede realizar las acciones correctivas adecuadas y ejecutar de nuevo el script de migración. En general, antes de ejecutar el script de migración,

asegúrese de:

- Configurar el agente de servicio ADM
- Obtener las licencias de servicio ADM
- Copie la ruta correcta donde ha almacenado el cliente y archivo CSV seguro

Las instancias de ADC tienen versiones inferiores a la limitación mencionada para licencias agrupadas. ¿Qué sucede si se selecciona la opción "Y"para cambiar el servidor de licencias?

El cambio del servidor de licencias solo se realiza para las versiones de NetScaler MPX, VPX y SDX compatibles.

¿Qué ocurre si el script de migración ha fallado en la configuración de las instancias de ADC?

Las instancias de ADC siguen funcionando en la configuración de ADM local. Puede tomar las medidas necesarias a partir del motivo de error sugerido y volver a ejecutar el script de migración.

Qué ocurre si algunas de las instancias de ADC no se mueven al servicio ADM. ¿Ayudará la reejecución del script de migración?

Sí. Después de volver a ejecutar el script, solo se migran las instancias fallidas. Supongamos que dos de cada cinco instancias no han podido moverse. Después de realizar acciones correctivas y volver a ejecutar el script de migración, tres instancias que se movieron correctamente anteriormente muestran el mensaje "El dispositivo ya existe". Y las otras dos instancias que fallaron anteriormente se migran correctamente.

¿Hay un archivo de registro para comprobar el estado de la migración?

Sí, se genera un archivo de registro en el `/var/mps/log/` directorio. ADM con python3.7 tiene el archivo de registro como `servicemigrationtool.py.log` y ADM con python 2.7 tiene el archivo de registro como `servicemigrationtool_27.py.log`.

¿Qué sucede si la sesión termina mientras se ejecuta el script de migración?

Puede volver a ejecutar el script de migración. En la nueva sesión, las instancias ya agregadas de la última sesión se muestran como "El dispositivo ya existe"y la migración continúa aún más.

¿Qué ocurre si el servicio ADM tiene licencias inferiores a las de NetScaler ADM local y se inicia el script de migración?

Después de ejecutar el script de migración, aparece una sugerencia, mencionando que las licencias son menores y se solicita que continúe o detenga. Si quiere continuar con licencias menores, los servidores virtuales se otorgan licencias aleatoriamente a partir de las licencias disponibles.

¿Qué ocurre cuando NetScaler ADM local se migra a la cuenta Express del servicio ADM?

La cuenta Express del servicio ADM solo tiene dos licencias de servidor virtual, dos paquetes de configuración de StyleBook y dos trabajos de configuración. Si su ADM local tiene más de estas configuraciones e inicia la migración con Express Account, el script solo puede migrar las configuraciones mencionadas aplicables a Express Account (dos licencias de servidor virtual, dos paquetes de configuración de StyleBook y dos trabajos de configuración)

¿Qué sucede si un usuario invitado de Citrix Cloud (que no sea el usuario administrador que creó una cuenta de Citrix Cloud) intenta migrar la configuración de ADM local?

Se recomienda que el administrador ejecute el script de migración. Un usuario invitado no tiene privilegios de administrador (AdminExceptSystem_Group). Como resultado, se produce un error en la migración de grupos, roles y directivas y se muestra el mensaje "El usuario no tiene permiso".

Como solución, el administrador (que creó la cuenta de Citrix Cloud) puede cambiar el grupo asociado con el usuario invitado como "admin_group".

Guión de reversión

¿Qué ocurre si el script de reversión se utiliza en el par ADM HA local?

El par ADM HA local se restaura con todas las configuraciones que estaban disponibles antes de la migración.

¿Qué ocurre con el nodo de recuperación ante desastres después de usar el script de reversión?

El nodo de recuperación ante desastres también se restaura con todas las configuraciones antes de la migración

Solución de problemas

January 30, 2024

Cuando ejecuta el script de migración por primera vez, comprueba los requisitos previos y continúa con la migración. Si se cumplen todos los requisitos previos, la migración se completa sin ningún error. Si falla algún requisito previo, el script muestra mensajes de error con motivos. Después de corregir los errores, debe volver a ejecutar el script.

> Nota
>
> Si aparece un mensaje de error que muestra "ya existe", significa que:
>
> - Es posible que haya ejecutado el script de migración durante más de una vez y algunas configuraciones ya se han migrado al servicio ADM.
> - Es posible que haya creado manualmente la misma configuración en el servicio ADM antes de ejecutar el script de migración.

Consulte algunos de los siguientes mensajes de error:

Perfil manual agregado al servicio ADM

```
==================Profiles Addition to ADM Service====================


60.26 : FAILURE : Profile 60.26 already exists

 The list of ADC profiles added to ADM Service are :
{'60.26': "['FAILURE']"}
```

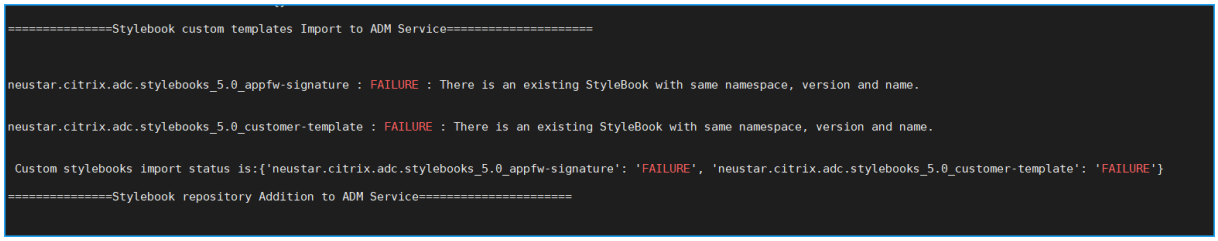
Solución alternativa: Si ha creado perfiles de administrador en el servicio NetScaler ADM antes de ejecutar el script de migración, asegúrese de eliminar esos perfiles y volver a ejecutar el script de migración.

Se agregó el dispositivo NetScaler al servicio ADM

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

Solución alternativa: en ADM local, asegúrese del estado de la instancia y vea si puede acceder a la instancia sin ningún problema. Si persiste algún problema, solucione el problema y vuelva a ejecutar el script de migración.

Importación de plantillas personalizadas de StyleBook al servicio ADM



Solución alternativa: este mensaje de error es un ejemplo para el StyleBook ya migrado. También puede ver este error si ha creado manualmente un StyleBook con el mismo nombre, versión y espacio de nombres, en el servicio NetScaler ADM antes de ejecutar el script de migración.

Trabajos de configuración agregados al servicio ADM

```
==============Config Jobs Addition to ADM Service====================


config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

Solución alternativa: Este error se produce si se ha suscrito a Express Account y tiene más de dos trabajos de configuración. Debe obtener una suscripción válida para poder migrar todos los trabajos de configuración.

Bloques IP agregados al servicio ADM

```
====================IP Blocks Addition in ADM Service=======================


ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

Solución alternativa: elimine el bloque IP que se crea manualmente en el servicio ADM y vuelva a ejecutar el script de migración.

Estado de adición del informe del panel de red

```
================Network Dashboard Reports Addition to ADM Service================


new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

Solución alternativa: Elimine el panel que se crea manualmente en el servicio ADM y vuelva a ejecutar el script de migración.

Todos los artículos

January 30, 2024

Los “artículos prácticos”de NetScaler Application Delivery Management (NetScaler ADM) son artículos sencillos, relevantes y fáciles de implementar sobre las funciones de NetScaler 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 certificados	Sistema NetScaler ADM
	Administración de la configuración	Autenticación	Análisis	Funciones de red

Administración de instancias

Cómo supervisar sitios distribuidos globalmente

Cómo administrar las particiones de administración de las instancias de NetScaler

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 mediante NetScaler ADM

Cómo forzar que una instancia secundaria de NetScaler 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 modificar el archivo de configuración de HAProxy mediante NetScaler ADM

Cómo redescubrir varias instancias de NetScaler VPX

Cómo sondear instancias y entidades de NetScaler 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 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 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 a otra 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

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 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

StyleBooks

Cómo ver diferentes grupos de StyleBooks

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 análisis desde NetScaler 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 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 NetScaler ADM

Cómo modificar la gravedad reportada de los eventos que ocurren en 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 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 habilitar servidores de autenticación externos alternativos y en cascada

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 NetScaler 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

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

NetScaler Application Delivery Management (ADM) es una solución de administración centralizada que simplifica las operaciones al proporcionar a los administradores una visibilidad en toda la empresa y automatizar las tareas de administración que deben ejecutarse en varias instancias. Puede gestionar y supervisar los productos de NetScaler que incluyen NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX y NetScaler Gateway. 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 páginas 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 aplicaciones también muestra información relacionada con los ataques, como ataques SYN, ataques de ventanas pequeñas y ataques de inundación DNS para las instancias de ADC descubiertas.

Redes

Instances

Le permite administrar las instancias de NetScaler y NetScaler Gateway.

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

NetScaler 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 comenzar a usar el panel SSL de ADM y sus funcionalidades, debe comprender qué es un certificado SSL y cómo puede usar 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 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. 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 supervisar todas las aplicaciones web seguras que ofrece NetScaler 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 supervisar las métricas de las técnicas de optimización de vídeo utilizadas por las instancias de NetScaler a fin de mejorar la experiencia del cliente y la eficiencia operativa.

WAN Insight

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

Orchestration

Orquestación en la nube

Permite la integración de los productos NetScaler 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 con la orquestación en la nube de OpenStack.

Orchestration

NetScaler ADM admite SDN en la red empresarial mediante la integración con controladores SDN de diferentes proveedores. ADM admite VMware NSX Manager y Cisco Application Policy Infrastructure Controller (APIC).

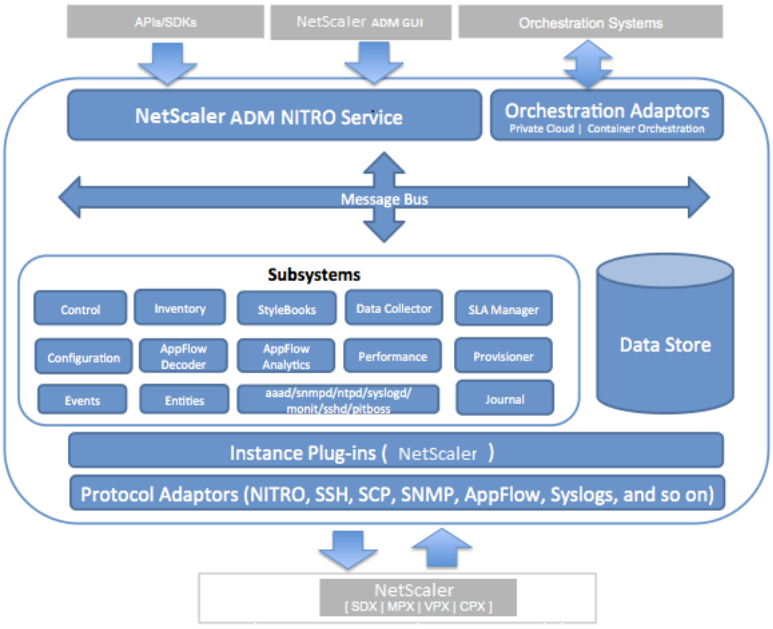
Arquitectura

January 30, 2024

La base de datos NetScaler 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 a 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 Servicio en ADM actúa como un servidor web que gestiona las solicitudes y respuestas HTTP que se envían a subsistemas dentro de ADM desde la GUI o 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 otros subsistemas (Inventory, StyleBooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Rendimiento, Eventos, Entidades, Administrador de SLA, Aprovisionador y Diario) 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 NetScaler ADC o dispositivos virtuales que desea descubrir, administrar y supervisar desde NetScaler Application Delivery Management (ADM). Para administrar y supervisar estas instancias, debe agregarlas al servidor NetScaler ADM. Puede agregar los siguientes dispositivos NetScaler ADC y dispositivos virtuales a ADM:

- Instancias de NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- Instancias de NetScaler Gateway

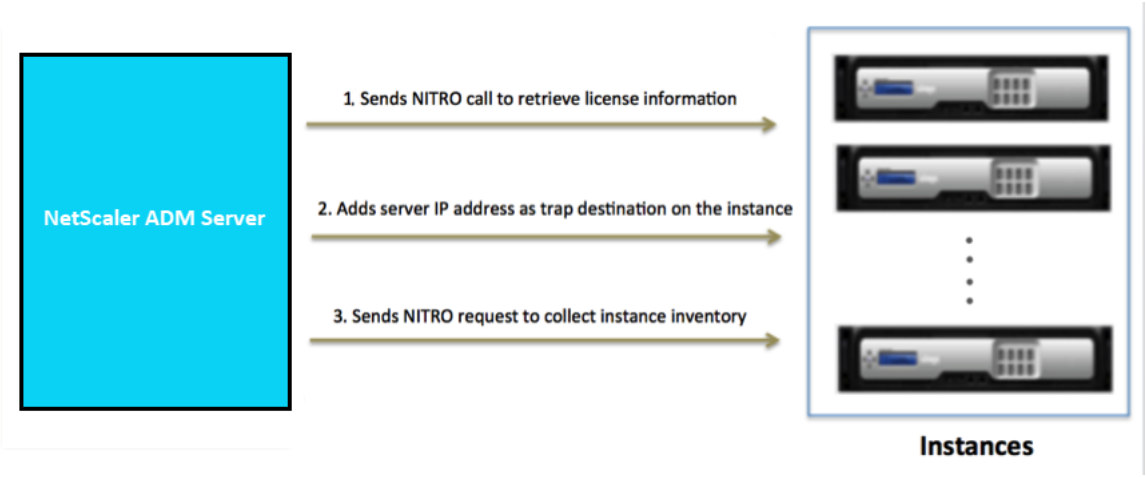
Puede agregar instancias mientras configura el servidor NetScaler ADM por primera vez o más tarde.

> **Nota**
>
> NetScaler ADM utiliza la dirección IP de NetScaler (NSIP) de las instancias ADC para la comunicación. ADM también puede detectar instancias ADC con una dirección IP de subred (SNIP) que tiene habilitado el acceso de administración en ella. Para obtener información sobre los puertos

> que deben estar abiertos entre las instancias de ADC y ADM, consulte Puertos.
>
> Si quiere agregar un par ADC HA mediante SNIP, asegúrese de habilitar el modo Configuración de red independiente (INC) en el par ADC HA. Para obtener más información sobre cómo agregar instancias, consulta Agregar instancias.

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, NetScaler ADM realiza implícitamente los siguientes pasos.

1. NetScaler ADM utiliza los detalles del perfil de instancia para iniciar sesión en la instancia. Mediante una llamada 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 de ADC (por ejemplo, NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX o NetScaler Gateway). Al detectar correctamente la instancia, se agrega a la base de datos de ADM.

   Este paso puede fallar si el perfil de instancia no incluye las credenciales correctas. En el caso de las instancias de NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler BLX y NetScaler 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.

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

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

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

Cómo NetScaler ADM sondea las instancias y entidades administradas

De forma predeterminada, NetScaler ADM sondea automáticamente a intervalos regulares. NetScaler 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
Encuesta de inventario	Cada 60 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. Vaya a **Infraestructura > Instancias > NetScaler**. 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 **Infraestructura > 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.

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

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
				Puede sondear los certificados SSL manualmente y agregar todos los certificados de las instancias inmediatamente a NetScaler ADM. Para hacerlo, vaya a **Infraestructura > Panel de control SSL** y haga clic en **Sondear ahora**. La página **Encuesta 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 60 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. Para habilitar el sondeo de entidades, consulte Habilitar o inhabilitar las funciones de ADM.	NITRO llama.	Sí, pero no se puede establecer en menos de 10 minutos. Para configurar, vaya a **Infraestructura > Funciones de red**. En la página Función de redes, haga clic en **Configuración** para configurar el intervalo de sondeo.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
				Puede sondear entidades manualmente y agregar todas las entidades de las instancias inmediatamente a NetScaler ADM. Para hacerlo, vaya a **Infraestructura > Funciones de red** y haga clic en **Sondear ahora**. La página **Encuesta ahora** le permite sondear todas las instancias o seleccionadas de la red

Nota

Además del sondeo, NetScaler 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 NetScaler 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 NetScaler se almacena internamente en la base de datos.

Diferentes formas de sondear instancias

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

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

Sondeo global de instancias

NetScaler 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 establecer el intervalo en función de sus requisitos si navega a **Infraestructura > Funciones de red** > **Configuración**.

Sondeo manual de instancias

Cuando NetScaler 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 NetScaler ADM, hay un período mínimo de intervalo de sondeo en el que no se realiza el sondeo automático. Si agrega una nueva instancia de NetScaler o si se actualiza una entidad, NetScaler 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, NetScaler ADM ahora le permite sondear solo instancias y entidades seleccionadas en un momento dado.

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

Para sondear instancias específicas en NetScaler ADM:

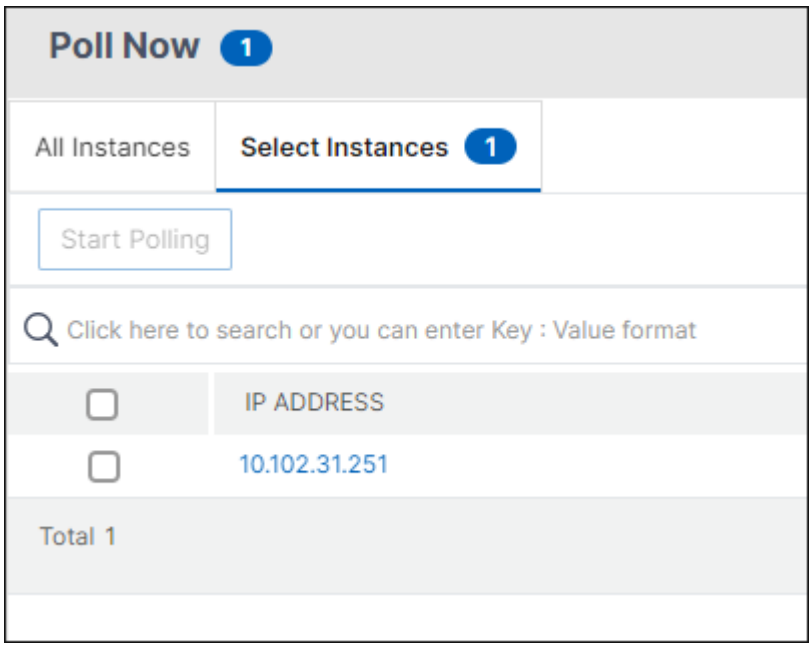
1. En NetScaler ADM, vaya a **Infraestructura > Funciones de red**.
2. En la página **Funciones de red**, en la esquina superior derecha, haga clic en **Sondear ahora**.

3. La página emergente **Poll Now** ofrece la opción de sondear todas las instancias de NetScaler 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**.



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

Encuesta manual de entidades

NetScaler ADM también le permite sondear solo algunas 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, NetScaler ADM sondea solo esa entidad y actualiza el estado en la GUI de NetScaler 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 NetScaler 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 NetScaler ADM, vaya a**Infraestructura > 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

ADM On-Prem Cloud Connector permite a Citrix Cloud recopilar datos de licencia, configuración y uso para cumplir con las licencias y administrar, medir y mejorar el servicio. A partir de la versión 14.1 8.x o posterior, puede configurar Cloud Connector para habilitar una conexión entre el servicio ADM y ADM On-Prem. Al habilitar ADM On-Prem Cloud Connector:

- Se recopilan la licencia obligatoria y los datos de uso para el cumplimiento de Flexed Licensing.
- Puede obtener la función de **asesoramiento de seguridad** en ADM On-Prem. Para obtener más información, consulte Cloud Connector local de ADM.

Tras habilitar Cloud Connector, se habilita la recopilación de métricas de datos.

Categorías de datos

En las tablas siguientes se proporcionan los detalles de los parámetros que se recopilan después de habilitar Cloud Connector:

Categorías	Descripción	¿Para qué lo utilizamos?
Implementación y uso de funciones de NetScaler	Información sobre la implementación y el uso de NetScaler, como el nombre del cliente, el ID del cliente, el total de dispositivos administrados y el total de dispositivos administrados activos.	Gestionar, medir y mejorar el servicio.
Implementación de NetScaler ADM	Información sobre NetScaler	Gestionar, medir y mejorar el servicio.
Licencias, derechos y uso de NetScaler y NetScaler ADM	Derechos, licencias	Cumplimiento de licencias y para administrar, medir y mejorar el servicio.

NetScaler y NetScaler ADM: parámetros de implementación y uso de funciones

Parámetros	Descripción
onprem_ip	La dirección IP del ADM
t_ten	El recuento total de arrendatarios que está conectado a ADM
deploy	Comprueba si el tipo de implementación de ADM es independiente o de par HA
is_dr	Comprueba si el nodo de recuperación ante desastres está configurado o no
is_agt	Comprueba si el agente local de ADM está configurado o no
is_cloud	Comprueba si la implementación de ADM es un servicio de ADM o de ADM local
is_cntr	Comprueba si la implementación de ADM está en el clúster de Kubernetes
platform	La plataforma en la que se aloja el ADM. Por ejemplo, Citrix Hypervisor
total_users	El recuento total de usuarios locales de ADM
total_gui_requests	El total de usuarios que iniciaron sesión en la GUI de ADM en las últimas 24 horas

Parámetros	Descripción
total_api_requests	El total de solicitudes a ADM a través de la API en las últimas 24 horas. Esto también incluye a los usuarios de proxy remotos (solicitudes del agente).
total_api_external_requests	El total de solicitudes a ADM a través de la API que excluyen las solicitudes del agente
total_custom_apps	El total de aplicaciones personalizadas en ADM
total_managed_apps	El total de aplicaciones administradas en ADM
total_apps	El total de aplicaciones en ADM
total_custom_sites	El total de sitios personalizados configurados en ADM
total_managed_devices	El total de instancias de NetScaler administradas en ADM
total_active_managed_devices	El total de instancias de NetScaler que están en estado UP
total_ns_device	El total de instancias MPX administradas en ADM
total_ngvpx_device	El total de instancias VPX de Gateway administradas en ADM
total_nswg_device	El total de instancias de Web Gateway administradas en ADM
total_nswgvpx_device	El total de instancias VPX de Web Gateway administradas en ADM
total_nsvpx_device	El total de instancias VPX administradas en ADM
total_cpx_device	El total de instancias CPX administradas en ADM
total_nsap_device	El total de instancias de partición de administración en ADM
total_nssdx_device	El total de instancias SDX administradas en ADM
total_agents	El total de agentes locales de ADM configurados
total_active_agents	El total de agentes locales de ADM que están en estado UP
total_custom_event_rules	El total de reglas de eventos personalizados creadas en ADM
total_event_rules	El total de reglas de eventos creadas en ADM
total_stylebook_config_store_count	El total de paquetes de configuración creados en ADM

Parámetros	Descripción
total_user_sb_stylebook_count	El total de paquetes de configuración personalizados creados en ADM
total_waf_devices	El total de instancias de NetScaler que están habilitadas con infracciones de WAF
total_gw_devices	El total de instancias de NetScaler que están habilitadas con SSL VPN
total_icaproxy_devices	El total de instancias de NetScaler habilitadas con HDX Insight en ADM
total_bot_devices	El total de instancias de NetScaler que están habilitadas con violaciones de bots
total_pooled_devices	El total de instancias de NetScaler (administradas y no administradas) con licencias agrupadas
total_config_audit	La plantilla de auditoría de configuración total configurada en ADM
total_config_job	El total de trabajos de configuración creados en ADM
total_ssl_certs	El total de certificaciones SSL que se crean, modifican o eliminan de ADM
total_network_report	El informe de red total creado en ADM
total_k8s	El ADM de NetScaler alojado en el clúster de Kubernetes. El total de clústeres de Kubernetes.
total_ipam	El total de proveedores de IPAM agregados en ADM
total_rbac_groups	El total de grupos RBAC configurados en ADM
total_ingress_deployed	El total de controladores de ingreso en Kubernetes.
total_ipam_configured	El total de redes IPAM agregadas en ADM
total_web_transaction_analytics	El total de instancias de NetScaler habilitadas con el análisis de transacciones web
total_pager_duty_profile	El total de perfiles de PagerDuty agregados en ADM
total_slack_profile	El total de perfiles de Slack añadidos en ADM
total_api_discovery	El total de instancias de NetScaler que reciben solicitudes de API
total_lb_devices	El total de instancias de NetScaler configuradas con servidores virtuales de equilibrio de carga

Parámetros	Descripción
total_lb_devices_http	El total de instancias de NetScaler configuradas con servidores virtuales HTTP de equilibrio de carga
total_lb_devices_ssl	El total de instancias de NetScaler configuradas con servidores virtuales SSL de equilibrio de carga
total_cs_devices	El total de instancias de NetScaler configuradas con servidores virtuales de conmutación de contenido
total_gslb_devices	El total de instancias de NetScaler configuradas con servidores virtuales de equilibrio de carga de servidores globales
total_aaa_devices	El total de instancias de NetScaler configuradas con servidores virtuales AAA
t_radius_svr	El total de servidores de autenticación RADIUS configurados en ADM
t_ldap_svr	El total de servidores de autenticación LDAP configurados en ADM
t_tacacs_svr	El total de servidores de autenticación TACACS configurados en ADM
agent_id	El identificador único del agente implementado
platform	La plataforma en la que está alojado el agente. Por ejemplo, Citrix Hypervisor
version	La versión del agente ADM
city	La ciudad donde se implementa el agente ADM
country	El país en el que se implementa el agente ADM
region	La región en la que se implementa el agente ADM
device_id	El ID único de la instancia VPX
version	La versión de compilación de la instancia VPX
state	El estado actual (ACTIVO o INACTIVO) de la instancia VPX
device_platform	La plataforma donde está alojada la instancia VPX
root	Los detalles de uso del disco ADM en los directorios /var, /root, /flash, /var/mps

Parámetros	Descripción
total	El espacio total en disco ADM (unidad: bytes)
used	El espacio total en disco ADM utilizado
free	El espacio total disponible en disco ADM
Adm_analt_dx - Función	El tipo de análisis (Bot, WAF, Web Insight, Service Graph, etc.) para el que se identifican los problemas.
Adm_analt_dx - issue_type	La categoría de problema a la que pertenece el problema identificado. Por ejemplo, licencias, configuración
Adm_analt_dx - sub_issue_type	La subcategoría del problema identificado. La subedición puede ser NO_VIPS_LICENSED, BOT_INSIGHT_IN_ACTION_DISABLED, NS_FEATURE_DISABLED, VSERVER_WITHOUT_BOT_POLICY_BINDING, NO_COLLECTORS_PRESENT, APPFLOWPARAM_DISABLED, ICA_APPFLOW_POLICY_BINDING, VSERVER_WITHOUT_APPFIREWALL_POLICY_BINDING, SECURITY_INSIGHT_IN_ACTION_DISABLED, NO_CPX_VIPS_PRESENT, COLLECTOR_UNBOUND_IN_VSERVER, VSERVER_WITHOUT_APPFLOW_POLICY_BINDING
feature	La función de análisis que está habilitada en los servidores virtuales de equilibrio de carga y conmutación de contenido
total_lbvserver_ft_enabled	Los servidores virtuales de equilibrio de carga total en los que está habilitada al menos una función de análisis
total_csvserver_ft_enabled	El total de servidores virtuales de conmutación de contenido en los que está habilitada al menos una función de análisis
feature_enabled_on_vpn	La función de análisis que está habilitada en los servidores virtuales VPN
total_vpnvserver_ft_enabled	El total de servidores virtuales VPN en los que está habilitada al menos una función de análisis

Elementos de datos de uso, derechos y licencias de NetScaler y NetScaler ADM

Parámetros	Descripción
pool_instances_entitled	El total de instancias del grupo tituladas
pool_instances_used	El total de instancias agrupadas utilizadas
pool_fips_instances_entitled	El conjunto total de instancias FIPS tituladas
pool_fips_instances_used	El total de instancias FIPS del grupo utilizadas
pool_entvcpu_entitled	El conjunto total de vCPU empresariales titulado
pool_entvcpu_used	El grupo total utilizado de vCPU empresariales
pool_entbw_entitled	El ancho de banda empresarial total del pool denominado [MBps]
pool_entbw_used	El ancho de banda empresarial total utilizado en el pool [MBps]
pool_pltbw_entitled	El ancho de banda Platinum total del pool denominado [MBps]
pool_pltbw_used	El ancho de banda Platinum total utilizado en el pool [MBps]
pool_pltvcpu_entitled	El conjunto total de vCPU Platinum titulado
pool_pltvcpu_used	El conjunto total de vCPU Platinum utilizadas
pool_stdbw_entitled	El ancho de banda estándar total del pool denominado
pool_stdbw_used	El ancho de banda estándar total utilizado
pool_stdvcpu_entitled	El conjunto total de vCPU estándar denominado
pool_stdvcpu_used	El conjunto total de CPU virtuales estándar utilizadas
pool_cpxvcpu_entitled	El conjunto total de vCPU CPX titulado
pool_cpxvcpu_used	El conjunto total de CPU virtuales CPX utilizadas
pool_perc_instances_used	El% de instancias utilizadas
pool_perc_vcpu_used	El% de vCPU utilizadas
pool_perc_bw_used	El% de ancho de banda utilizado
total_entitled_vservers	El total de servidores virtuales autorizados
total_used_vservers	El total de servidores virtuales utilizados
total_discovered_vservers	El total de servidores virtuales descubiertos

Parámetros	Descripción
perc_used_vservers	El% de servidores virtuales utilizados/autorizados
perc_discovered_vservers	El% de servidores virtuales descubiertos o autorizados
is_local_license	Comprueba si la licencia está alojada en NetScaler ADM
license_edition	El tipo de licencia (Platinum/Standard/Enterprise)
is_pooled_license	Comprueba si la licencia es una licencia agrupada
model_id	El ID de modelo de la instancia
plt_license_allocation	La asignación de licencias de platino
ent_license_allocation	La asignación de licencias empresariales
std_license_allocation	La asignación de licencias estándar
license_end_date	Número total de días para que caduque la licencia
platform	El tipo de dispositivo
instance_id	El identificador único de la instancia
instance_mode	Comprueba si la instancia es un par independiente o de alta disponibilidad
instance_state	El estado de la instancia (activo/inactivo)
flex_vpx_inst_titled	El total de instancias VPX autorizadas
flex_vpx_inst_allocated	El total de instancias VPX asignadas
flex_sdx_inst_titled	El total de instancias SDX autorizadas
flex_sdx_inst_allocated	El total de instancias SDX asignadas
flex_mpx_inst_titled	El total de instancias MPX autorizadas
flex_mpx_inst_allocated	El total de instancias MPX asignadas
flex_plt_bw_titled	El ancho de banda platino autorizado
flex_plt_bw_allocated	El ancho de banda de platino asignado
flex_ent_bw_titled	El ancho de banda empresarial autorizado
flex_ent_bw_allocated	El ancho de banda empresarial asignado
flex_std_bw_titled	El ancho de banda estándar autorizado

Parámetros	Descripción
flex_std_bw_allocated	El ancho de banda estándar asignado
flex_vpx_fips_inst_titled	El total de instancias FIPS autorizadas
flex_vpx_fips_inst_allocated	El total de instancias FIPS asignadas

Si su dispositivo NetScaler ADM es 14.1 4.x o una versión inferior, puede crear una identidad de cliente en Citrix Cloud para enviar estadísticas importantes sobre el estado, el estado y otras métricas de la implementación de ADM On-Prem a la cuenta de Citrix Cloud. Citrix recopila estadísticas para comprender el uso de NetScaler ADM. Para obtener más información, consulte Gobernanza de datos para la identidad del cliente.

Sistema de licencias

January 30, 2024

NetScaler Application Delivery Management (ADM) requiere una licencia de NetScaler verificada para administrar y supervisar las instancias de NetScaler, cuando las instancias se detectan a través del protocolo `https`.

NetScaler ADM admite las siguientes ediciones de licencia. Póngase en contacto con su representante de ventas o socio de NetScaler para comprar una licencia de ADM.

Edición Express: Puede administrar y supervisar cualquier cantidad de instancias con la licencia de la edición Express. De forma predeterminada, se aplica la licencia de la edición Express.

Edición avanzada: Permite administrar las aplicaciones descubiertas y ver el análisis de los servidores virtuales comprados junto con los servidores virtuales gratuitos.

Puntos a tener en cuenta:

- Para la compilación **13.1-9.x o anterior**, puede administrar hasta 30 aplicaciones descubiertas o servidores virtuales y ver análisis. Más allá de las 30 aplicaciones descubiertas o de los 30 servidores virtuales, debe comprar y aplicar una licencia Advanced. Por ejemplo, si compra 100 licencias de servidor virtual, tiene derecho a usar hasta 130 licencias de servidor virtual.
- Para la compilación **13.1-12.x o posterior**, puede administrar hasta dos aplicaciones descubiertas o servidores virtuales y ver los análisis. Más allá de las dos aplicaciones descubiertas o de los dos servidores virtuales, debe comprar y aplicar una licencia Advanced. Por ejemplo, si compra 100 licencias de servidor virtual, tiene derecho a usar hasta 102 licencias de servidor virtual.

Después de la actualización a la compilación 13.1-12.x:

- Todos los servidores virtuales gratuitos predeterminados de Express permanecen en funcionamiento durante 30 días. Puede seleccionar los 2 servidores virtuales y aplicar las 2 licencias predeterminadas dentro del período de gracia de 30 días. Si el usuario no realiza ninguna acción 30 días después de la actualización, ADM aplica la licencia de forma aleatoria a 2 servidores virtuales y anula la licencia de los servidores virtuales restantes. Debe comprar y aplicar nuevas licencias avanzadas para habilitar estos servidores virtuales.
- Tras la actualización, los siguientes son los cambios en el comportamiento de ADM:
  - ADM aplica un período de gracia de 30 días.
  - Dentro del período de gracia de 30 días, se bloquea la asignación de nuevos servidores virtuales para los 30 servidores virtuales gratuitos exprés.
    * Por ejemplo, si el número de licencias de servidores virtuales disponibles antes de actualizar a la versión 12.x era de 30 y solo se utilizaban 20 servidores virtuales con licencia, solo podrá usar los 20 servidores virtuales y no podrá licenciar los 10 servidores virtuales restantes durante el período de gracia de 30 días.
  - Sin embargo, dentro del período de gracia de 30 días, como administrador, aún puede aplicar licencias ADM avanzadas y asignar nuevos servidores virtuales.

Funciones	Opciones	Edición express	Edición anticipada	Licencia NetScaler
Aplicaciones	Panel de aplicaciones	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.	La información relacionada con NetScaler Web App Firewall en App Dashboard necesita una licencia Premium (o) Advanced con App Firewall.

Funciones	Opciones	Edición express	Edición anticipada	Licencia NetScaler
		Información web	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.
		Gráfico de servicio	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.
		Configuración > StyleBooks	Sin límite	Sin límite
Seguridad	Panel de seguridad	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.	La información relacionada con NetScaler Web App Firewall en el Panel de seguridad necesita una licencia Premium (o) Advanced con App Firewall.
		Infracciones de seguridad	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.

Funciones	Opciones	Edición express	Edición anticipada	Licencia NetScaler
		Usuarios y puntos finales	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.
Gateway	HDX Insight	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.	Avanzado (informes < 1 hora) Premium (informes = Ilimitado)
		Gateway Insight	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas y dos servidores virtuales adicionales.
Infraestructura	Análisis de infraestructura	Sin límite	Sin límite	NA
		Instancias	Sin límite	Sin límite
		Tablero SSL	Sin límite	Sin límite
		Eventos	Sin límite	Sin límite
		Funciones de red	Sin límite	Sin límite
		Informes de red	Sin límite	Sin límite
		Licencias agrupadas	Sin límite	Sin límite

Funciones	Opciones	Edición express	Edición anticipada	Licencia NetScaler
		Configuración > Trabajos de configuración, plantillas de configuración y consejos de configuración	Sin límite	Sin límite
		Trabajos de actualización	Sin límite	Sin límite
		Orchestration	Sin límite	Sin límite
		WAN Insight	Sin límite	Sin límite
Parámetros	RBAC y autenticación externa (nivel de instancia)	Sin límite	Sin límite	NA
		RBAC y autenticación externa	Sin límite	Sin límite

*Para la integración de Citrix Director con el soporte de NetScaler 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 NetScaler ADM a través de la GUI de NetScaler ADM.

Alta disponibilidad

El servidor NetScaler 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, NetScaler ADM admite la asignación de los mismos archivos de licencia a ambos servidores.

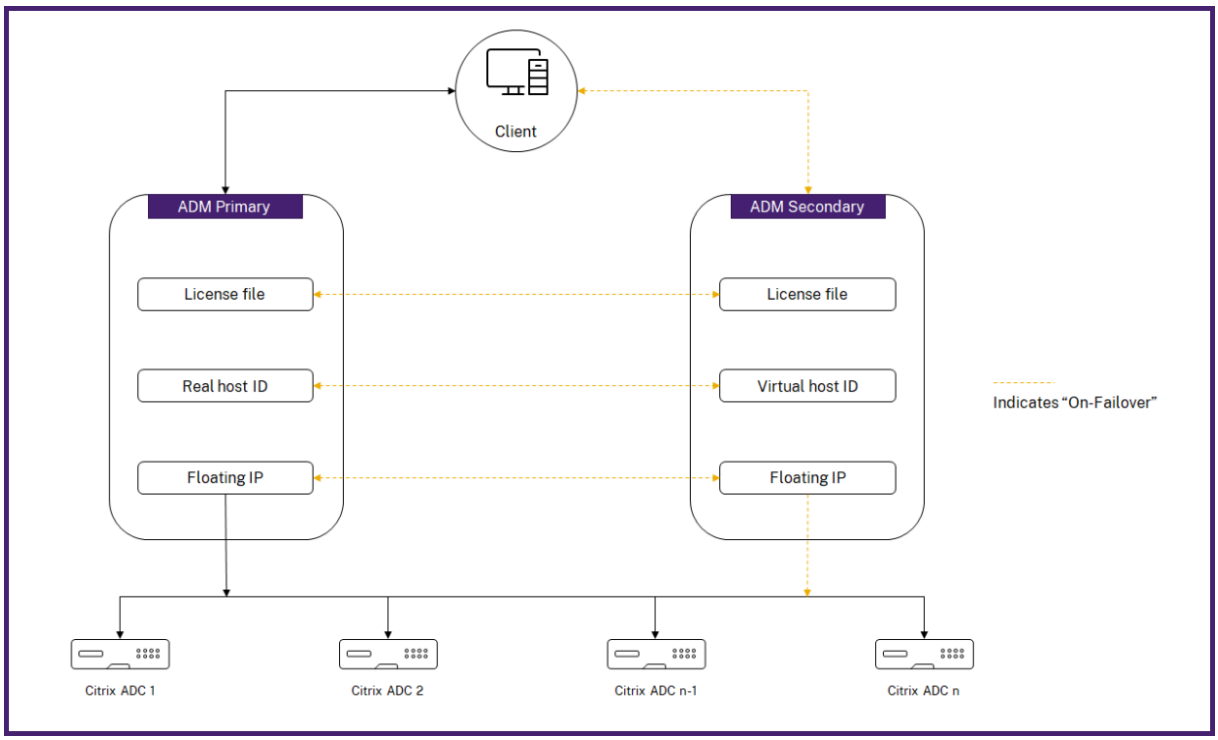
Nota

- Si ha instalado NetScaler 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 NetScaler 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 ID 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 NetScaler retiran las licencias del Node-1 mediante la dirección IP flotante.

Las licencias están bloqueadas para instancias de ADC. Para obtener licencias de un NetScaler ADM HA, las instancias requieren la dirección IP del dispositivo específico. Cuando aplicas las licencias en un servidor principal, este se encargará de las licencias y este aplicará todas las licencias futuras a 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.

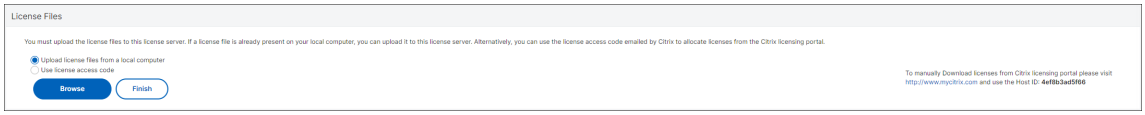
Actualización de las licencias de servidor virtual

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

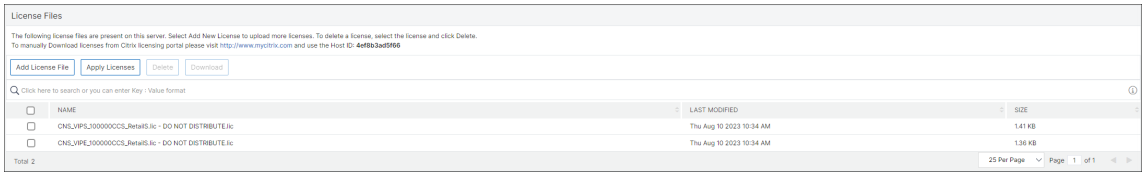
Para actualizar las licencias del dispositivo:

1. Inicie sesión en NetScaler ADM con las credenciales de administrador.
2. Vaya a**Infraestructura > Licencias agrupadas**.
3. Vaya a **Archivos de licencia**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 quiere usar para asignar sus licencias. Haga 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, NetScaler 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 verificar las licencias instaladas en su NetScaler ADM navegando a **Configuración > Configuración de licencias y análisis**.

Administrar servidores virtuales

Puede seleccionar los servidores virtuales o los servidores virtuales de terceros que desee administrar y supervisar a través de NetScaler ADM.

> **Puntos que tener en cuenta**
>
> - De forma predeterminada, NetScaler 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 NetScaler ADM es inferior al número de licencias de servidor virtual instaladas, NetScaler ADM, de forma predeterminada, otorga licencias a todos los servidores virtuales.

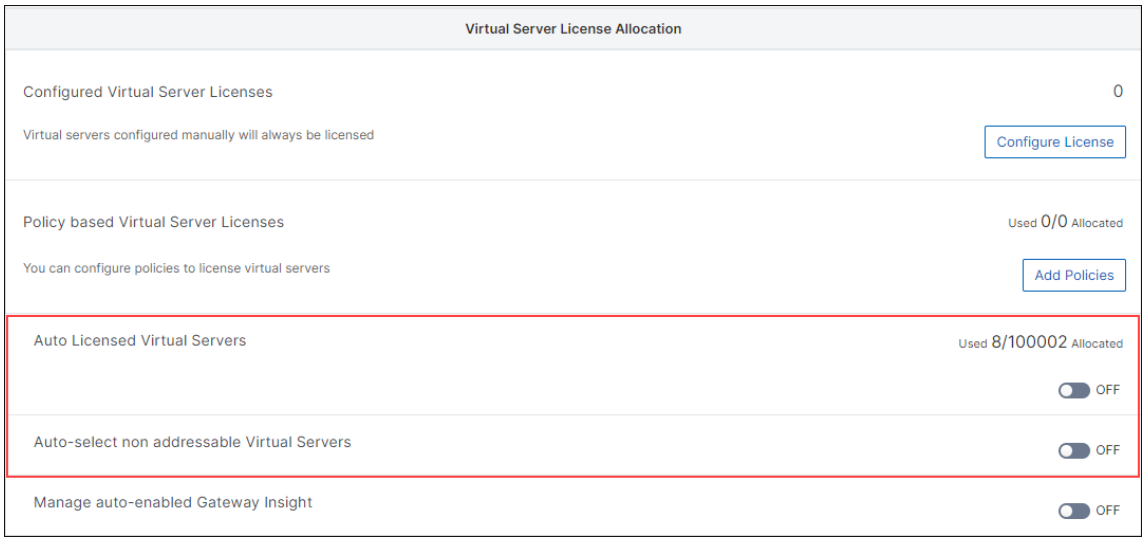
Para seleccionar manualmente los servidores virtuales o para restringir las licencias a los servidores virtuales limitados, primero debe inhabilitar la concesión automática de licencias de los servidores virtuales y, a continuación, seleccionar los servidores virtuales que quiere administrar.

Inhabilitar la concesión de licencias automáticas de servidores virtuales

1. Vaya a **Configuración > Configuración de licencias y análisis**.

   El panel muestra las licencias de servidor virtual disponibles, los servidores virtuales administrados junto con el tipo de servidor virtual e información sobre la caducidad de la licencia.

2. En **Asignación de licencias de servidor virtual**, inhabilite **los servidores virtuales con licencia automática** y **seleccione automáticamente los servidores virtuales no direccionables**.

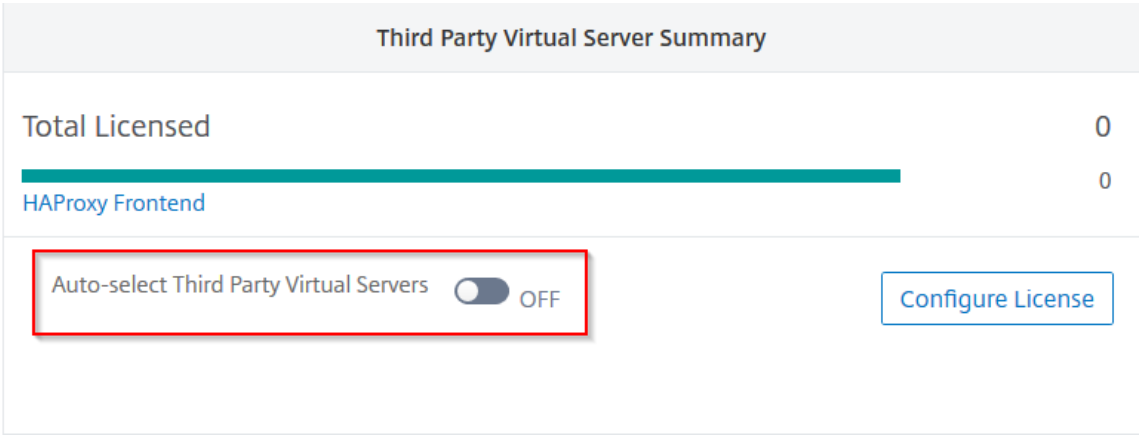


Seleccionar servidores virtuales de terceros para obtener licencias

1. Vaya a **Configuración > Configuración de licencias y análisis**.

   El panel muestra las licencias de servidor virtual disponibles, los servidores virtuales administrados junto con el tipo de servidor virtual e información sobre la caducidad de la licencia.

2. En **Resumen de servidores virtuales de terceros**, desactive la **selección automática de servidores virtuales de terceros**.



Aplicar licencias de servidor virtual manualmente

Puede aplicar licencias manualmente a un servidor virtual individual.

1. En **Asignación de licencias de servidor virtual**, seleccione **Configurar licencias**.

   Aparece la página **Todos los servidores** virtuales.
2. Filtrar servidores virtuales sin licencia mediante la propiedad:`Licensed: No`.
3. Seleccione el servidor virtual que quiere licenciar.
4. Haga clic en **Licencia**.

Configurar licencias de servidor virtual basadas en directivas

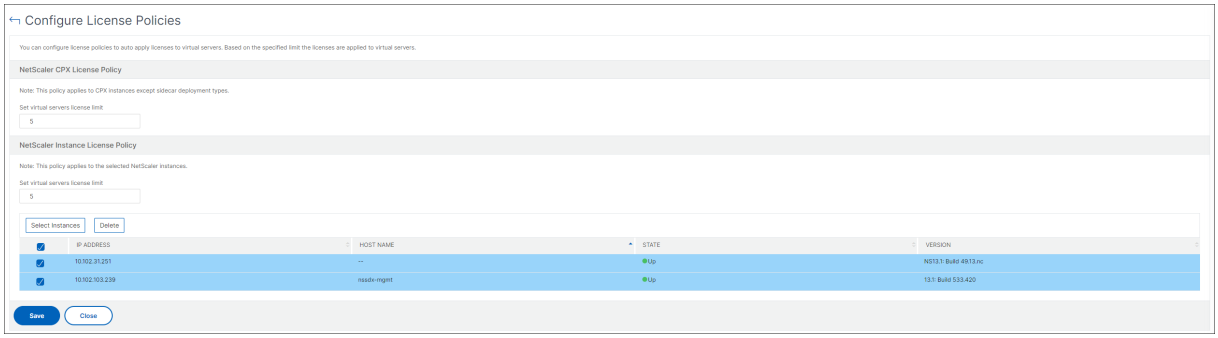
Puede configurar una directiva para aplicar la licencia a los servidores virtuales. Esta directiva controla la cantidad de servidores virtuales a los que quiere licenciar automáticamente. También aplica licencias solo a los servidores virtuales de las instancias seleccionadas.

Haga clic en **Modificar directivas** y puede especificar lo siguiente:

- Establezca el límite de servidores virtuales en instancias CPX por separado para aplicar licencias. ADM aplica licencia a servidores virtuales en instancias CPX hasta un límite especificado.

  > **Importante**
  >
  > Este límite se aplica a las instancias CPX, excepto a los tipos de implementación sidecar.
  >
  > Para ver las instancias CPX de los tipos de implementación de sidecar, filtre los servidores virtuales mediante la propiedad: `License Type: Freely Managed`.

- Establezca el límite de servidores virtuales en instancias ADC seleccionadas (MPX/VPX/BLX) para aplicar licencias. El ADM aplica licencias a los servidores virtuales en las instancias de ADC hasta un límite especificado.
- Seleccione las instancias de ADC prioritarias para aplicar las licencias de servidor virtual. Por lo tanto, ADM solo puede aplicar licencia a los servidores virtuales de instancias seleccionadas.



Ver los servidores virtuales con licencia

Después de aplicar las licencias a los servidores virtuales, puede ver los servidores virtuales con licencia o los servidores virtuales de terceros.

1. Vaya a **Configuración > Configuración de licencias y análisis**.
2. Haga clic en el tipo de servidor virtual en la sección **Total de licencias** del **Resumen de licencias de servidores virtuales**.

Configurar la compatibilidad con licencias automáticas para servidores virtuales no direccionables

NetScaler 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.

NetScaler ADM proporciona una opción en NetScaler ADM en **Asignación de licencias de servidor virtual**. Si activa la opción **Seleccionar automáticamente servidores virtuales no direccionables**, aplique automáticamente licencias de servidores virtuales no direccionables.

> **Nota**
>
> - NetScaler ADM, de forma predeterminada, sigue sin seleccionar automáticamente los servi-

> dores virtuales no direccionables para las licencias.
>
> - Application Analytics (App Dashboard) es la única analítica admitida actualmente en servidores virtuales con licencia no direccionables.

Comprobaciones de caducidad de licencias de servidores virtuales

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

Para ver el estado de las licencias:

1. Vaya a **Infraestructura > Licencias agrupadas > Licencias del 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 **Infraestructura > Licencias agrupadas > 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.
    - **SMS (mensaje de texto):** perfil SMS o lista de distribución para enviar notificaciones cuando las licencias alcanzan el umbral o van a caducar.
    - **Slack**: Especifique los detalles del perfil Slack.
    - **Alertas de PagerDuty**: Especifique un perfil de PagerDuty. Según la configuración de notificaciones configurada en su portal de PagerDuty, se envía una notificación cuando sus certificados están a punto de caducar.
    - **Notificarme:** defina 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.
    - **Caducidad de licencias:** Número de días restantes antes de la expiración.

Requisitos del sistema

January 30, 2024

Antes de instalar NetScaler ADM, debe comprender los requisitos del software, los requisitos del navegador, la información de los puertos, la información de la licencia y las limitaciones.

Requisitos de NetScaler ADM

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs **Nota:**Recomendamos usar la tecnología de unidades de estado sólido (SSD) para las implementaciones de NetScaler ADM.
Espacio de almacenamiento	El espacio de almacenamiento predeterminado requerido es 120 GB. Los requisitos de almacenamiento reales dependen de la estimación del tamaño de NetScaler ADM. Usa la calculadora de tamaño para calcular las estimaciones de almacenamiento. Póngase en contacto con su representante de NetScaler para acceder a la calculadora de tamaños. Si el requisito de almacenamiento NetScaler ADM supera los 120 GB, debe adjuntar un disco adicional. Solo se puede agregar un disco adicional. Le recomendamos que calcule el almacenamiento y adjunte discos adicionales en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a NetScaler ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps

Requisitos para el agente de NetScaler ADM on-prem

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs
Espacio de almacenamiento	30 GB
Interfaces de red virtual	1
Rendimiento	1 Gbps

> **Nota**
>
> El procesador AMD es compatible con:
>
> - **NetScaler ADM 13.1, compilación 4.43, o una versión posterior**.
> - **Agente NetScaler ADM 13.1, compilación 17.42, o una versión posterior**.

Se requiere una versión mínima de NetScaler para las funciones de NetScaler ADM

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

Función NetScaler ADM	Versión del software NetScaler
StyleBooks	10.5 y versiones posteriores
Compatibilidad con OpenStack/CloudStack	11.0 y posteriores, si se requiere una partición
	11.1 y versiones 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 NetScaler, 10.1 y posteriores
	Para NetScaler SDX, 11.0 y versiones posteriores

Función NetScaler ADM	Versión del software NetScaler
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
Infracciones de seguridad de WAF	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 NetScaler ADM, ya que las instancias de NetScaler ejecutan la versión 11.0, compilación 66.x.

Requisitos para el análisis de NetScaler ADM

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

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

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

NetScaler ADM puede generar informes para las aplicaciones que se publican en Citrix Virtual Apps o Citrix Virtual Desktops y a las que se accede a través de Citrix Workspace. Sin embargo, esta capacidad depende del sistema operativo en el que esté instalado Workspace. Actualmente, un NetScaler no analiza el tráfico ICA en busca de aplicaciones o escritorios a los que se accede a través de Citrix Workspace 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 Dell Wyse basados en Linux
- Clientes ligeros basados en Dell Wyse ThinOS
- Clientes ligeros basados en Ubuntu de 10 ZiG
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

Se requiere una licencia de instancia de NetScaler para HDX Insight

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

Licencia y duración de NetScaler	5 minutos	1 hora	1 día	1 semana	1 mes
Estándar	No	No	No	No	No
Avanzado	Sí	Sí	No	No	No
Premium	Sí	Sí	Sí	Sí	Sí

Hipervisores compatibles

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

Hipervisor	Versiones
Citrix Hypervisor	7.1 y 7.4
VMware ESX	6.0, 6.5, 6.7 y 7.0
Microsoft Hyper-V	2012 R2 y 2016
KVM genérico	RHEL 7.4, RHEL 8.0, Ubuntu 16.04 y Ubuntu 18.04

Sistemas operativos y versiones de Workspace compatibles

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

Sistema operativo	Versión Workspace
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

Exploradores web compatibles

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

Explorador web	Versión
Microsoft Edge	79 y versiones posteriores
Google Chrome	51 y versiones posteriores
Safari	10 y versiones posteriores
Mozilla Firefox	52 y versiones posteriores

Puertos compatibles

NetScaler ADM utiliza la dirección IP de NetScaler (conocida como NSIP) para comunicarse con NetScaler. Puede usar un agente como intermediario entre la instancia de ADC y ADM. Para establecer una comunicación con estos servidores, abra los puertos necesarios.

> **Nota**
>
> Si ha configurado NetScalers en modo de alta disponibilidad, NetScaler ADM utiliza NSIP para comunicarse con NetScaler y los puertos necesarios siguen siendo los mismos.

Diagrama de puertos de red para la implementación sin agentes:

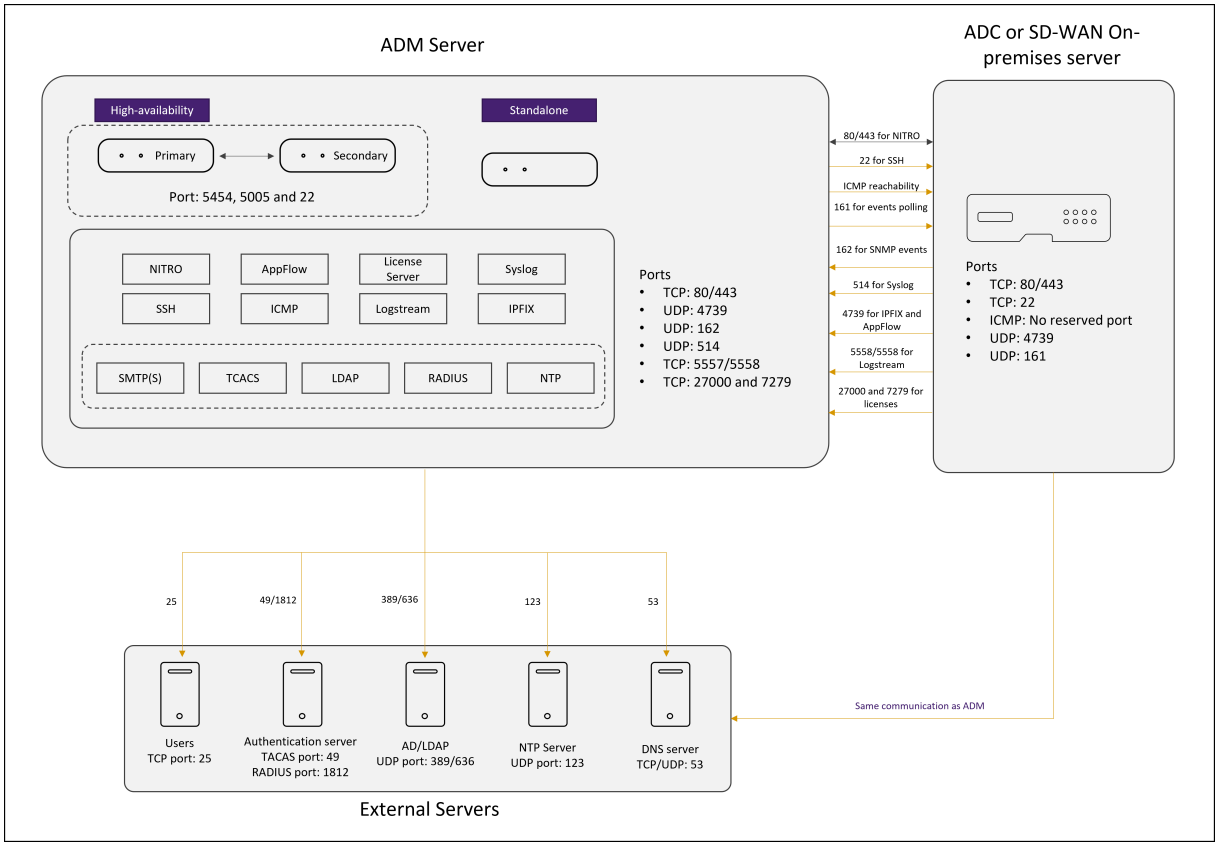


Diagrama de puertos de red para la implementación que incluye el agente ADM:

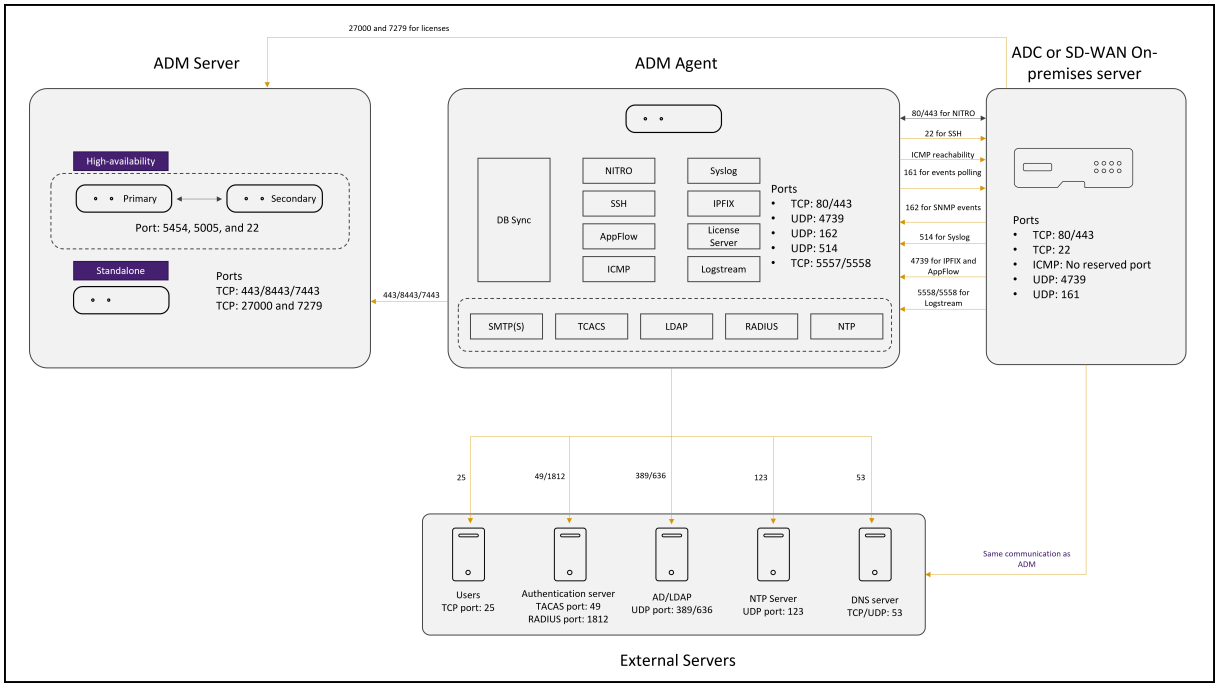


Diagrama de puertos de red para la implementación de alta disponibilidad de NetScaler ADM:

Si hay dos servidores NetScaler ADM configurados en modo de alta disponibilidad, al agregar una

instancia:

- NetScaler ADM se comunica con NetScaler a través de la dirección IP principal.
- NetScaler establece la conectividad con NetScaler ADM a través de la dirección IP flotante de ADM. Esto implica que NetScaler dirige todo el tráfico de SNMP, Syslog y Analytics a la dirección IP flotante de ADM.

Las siguientes secciones explican los puertos requeridos y su finalidad:

- Servidor ADM
- Agente ADM
- instancia de ADC
- Servidores externos

Puertos para el servidor ADM

En la siguiente tabla se explican los puertos necesarios que deben estar abiertos en el servidor de ADM.

Puerto	Tipo	Detalles	Dirección de comunicación
80/443/5454/22	TCP	Puerto predeterminado para la comunicación y sincronización de bases de datos entre nodos NetScaler ADM en modo de alta disponibilidad.	Nodo principal de NetScaler ADM a nodo secundario de NetScaler ADM
443/8443/7443	TCP	Puerto para la comunicación entre el agente NetScaler ADM y NetScaler ADM.	El agente NetScaler ADM inicia la comunicación con NetScaler ADM. A continuación, NetScaler ADM y el agente interactúan entre sí.

Puerto	Tipo	Detalles	Dirección de comunicación
27000 y 7279	TCP	Puertos de licencia para la comunicación entre el servidor de licencias de NetScaler ADM y la instancia de ADC. Estos puertos también se utilizan para licencias agrupadas de ADC.	NetScaler a NetScaler ADM
5005	UDP	Puerto para intercambiar latidos entre los nodos HA.	De nodo principal a nodo secundario de NetScaler ADM. De nodo secundario a nodo principal de NetScaler ADM.

Si las instancias de NetScaler ADM y NetScaler no utilizan un agente para la comunicación, abra los siguientes puertos en el servidor NetScaler ADM:

Puerto	Tipo	Detalles	Dirección de comunicación
80/443	TCP	Para la comunicación NITRO desde NetScaler ADM a la instancia de NetScaler.	Agente de NetScaler ADM a NetScaler y NetScaler a NetScaler ADM agente
4739	UDP	Para la comunicación de AppFlow desde la instancia de NetScaler a NetScaler ADM.	NetScaler a agente NetScaler ADM
162	UDP	Para recibir eventos SNMP desde la instancia de NetScaler a NetScaler ADM.	NetScaler a agente NetScaler ADM

Puerto	Tipo	Detalles	Dirección de comunicación
514	UDP	Para recibir mensajes de syslog desde la instancia de NetScaler a NetScaler ADM.	NetScaler a agente NetScaler ADM
5557/5558	TCP	Para la comunicación de flujo de registros (para infracciones de seguridad de WAF, Web Insight y HDX Insight) desde NetScaler a NetScaler ADM.	NetScaler a NetScaler ADM
5563	TCP	Para recibir métricas ADC (contadores), eventos del sistema y mensajes de registro de auditoría de la instancia de NetScaler a NetScaler ADM	NetScaler a NetScaler ADM

Puertos para el agente ADM

En la siguiente tabla se explican los puertos necesarios que deben estar abiertos en el agente de ADM.

Puerto	Tipo	Detalles	Dirección de comunicación
80/443	TCP	Para la comunicación NITRO desde NetScaler ADM a la instancia de NetScaler.	Agente de NetScaler ADM a NetScaler y NetScaler a NetScaler ADM agente
4739	UDP	Para la comunicación de AppFlow desde la instancia de NetScaler a NetScaler ADM.	NetScaler a agente NetScaler ADM

Puerto	Tipo	Detalles	Dirección de comunicación
162	UDP	Para recibir eventos SNMP desde la instancia de NetScaler a NetScaler ADM.	NetScaler a agente NetScaler ADM
514	UDP	Para recibir mensajes de syslog desde la instancia de NetScaler a NetScaler ADM.	NetScaler a agente NetScaler ADM
5557/5558	TCP	Para la comunicación de flujo de registros (para infracciones de seguridad de WAF, Web Insight y HDX Insight) desde NetScaler a NetScaler ADM.	NetScaler a NetScaler ADM

Puertos para instancias de ADC

En la siguiente tabla se explican los puertos necesarios que deben estar abiertos en las instancias de NetScaler.

Puerto	Tipo	Detalles	Dirección de comunicación
80/443	TCP	Para la comunicación NITRO desde NetScaler ADM a la instancia de NetScaler. Para la comunicación NITRO entre servidores NetScaler ADM en modo de alta disponibilidad.	NetScaler ADM a NetScaler y NetScaler a NetScaler ADM

Puerto	Tipo	Detalles	Dirección de comunicación
22	TCP	Para la comunicación SSH desde NetScaler ADM a la instancia de NetScaler. Para la sincronización entre los servidores NetScaler ADM implementados en modo de alta disponibilidad. Además, este puerto es necesario para la comunicación SSH entre el agente ADM y NetScaler.	NetScaler ADM a NetScaler. O bien, el agente de NetScaler ADM a NetScaler.
Sin puerto reservado	ICMP	Para detectar la accesibilidad de la red entre las instancias de NetScaler ADM y NetScaler, o el servidor NetScaler ADM secundario implementado en modo de alta disponibilidad.	NetScaler ADM a NetScaler
161	UDP	Para sondear eventos de instancias de ADC.	NetScaler ADM a NetScaler

Puertos para el agente ADC integrado

En la siguiente tabla se explican los puertos necesarios que deben estar abiertos para un agente integrado de NetScaler.

Puerto	Tipo	Detalles	Dirección de comunicación
443	TCP	Para todas las comunicaciones entre NetScaler ADM y el agente integrado NetScaler	De NetScaler ADM al agente integrado de NetScaler y del agente integrado de NetScaler a NetScaler ADM

> **Nota:**
>
> En la implementación de alta disponibilidad de ADM, todas las comunicaciones de ADM utilizan la dirección IP del nodo principal.

Puertos para servidores externos

En la siguiente tabla se explican los puertos necesarios que deben estar abiertos en los servidores externos:

Puerto	Tipo	Detalles	Dirección de comunicación
25	TCP	Para enviar notificaciones SMTP desde NetScaler ADM a los usuarios.	NetScaler ADM a los usuarios.
389/636	TCP	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre NetScaler ADM y el servidor de autenticación externo LDAP.	Servidor de autenticación externa de NetScaler ADM a LDAP
123	UDP	Puerto de servidor NTP predeterminado para sincronizar con varias fuentes de tiempo.	NetScaler ADM a servidor NTP

Puerto	Tipo	Detalles	Dirección de comunicación
1812	RADIUS	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre NetScaler ADM y el servidor de autenticación externo RADIUS.	NetScaler ADM a servidor de autenticación externa RADIUS
49	TACACS	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre NetScaler ADM y el servidor de autenticación externo TACACS.	NetScaler ADM a servidor de autenticación externa TACACS

Limitaciones

Desde NetScaler ADM 12.1 o una versión posterior, las siguientes funciones admiten el formato IPv6 de las direcciones IP:

1. Acceso de administración para la GUI de NetScaler ADM
2. Acceso de administración para NetScaler
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 NetScaler

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

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 destinado a los administradores de redes y aplicaciones que administran dispositivos de red Citrix (NetScaler y NetScaler Gateway). 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 NetScaler ADM en su centro de datos, revise los requisitos de software, los requisitos del navegador, la información de puertos, la información de licencias y las limitaciones.

- **Información sobre la licencia**. Puede agregar cualquier cantidad de instancias y entidades sin licencia. Sin embargo, solo puede ver la información de análisis de dos servidores virtuales sin aplicar una licencia. Para ver los análisis de más de dos servidores virtuales, debe adquirir las licencias correspondientes. 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 necesarios estén abiertos para que NetScaler ADM se comunique con las instancias de NetScaler. Obtenga más información.
- **Requisitos de instancia de NetScaler**. Las diferentes versiones del software NetScaler admiten diferentes funciones de NetScaler ADM. Revise esta información para asegurarse de que ha actualizado las instancias de NetScaler a la versión correcta. 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 Insight Center, puede migrar a NetScaler ADM y aprovechar las funciones de administración, supervisión, 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:
  - NetScaler 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 independiente. Para obtener más información, consulteConfigurar en una implementación de alta disponibilidad.

Paso 3: Agregar instancias a NetScaler ADM

En NetScaler ADM, puede descubrir, administrar y supervisar todas las instancias de NetScaler que se implementan en las instalaciones o en la nube. Debe agregar instancias al servidor NetScaler ADM si quiere administrar y supervisar estas instancias. Puede agregar las siguientes instancias a NetScaler ADM:

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler Gateway

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

Debe configurar un servidor de Network Time Protocol (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**. Configure 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, 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 cuales 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 supervisar sus instancias y aplicaciones.

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

Implementar

January 30, 2024

Antes de usar NetScaler ADM para administrar y supervisar las aplicaciones y la infraestructura de red, primero debe instalarlo en uno de los hipervisores o en un clúster de Kubernetes. Si implementa NetScaler ADM en un hipervisor, puede implementarlo como un único servidor o en modo de alta disponibilidad. El modo de alta disponibilidad no se aplica a un clúster de Kubernetes. Si utiliza NetScaler Insight Center, puede migrar a NetScaler ADM y aprovechar las funciones de administración, supervisión, orquestación y administración de aplicaciones, además de las funciones de análisis.

- **Implementación de un solo servidor**: en el caso de un ADM independiente implementado en un hipervisor, 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:
  - NetScaler ADM en Citrix Hypervisor
  - NetScaler ADM en Microsoft Hyper-V
  - NetScaler ADM en VMware ESXi
  - NetScaler ADM en el servidor KVM Linux
  - NetScaler ADM en el clúster de Kubernetes
- **Implementación de alta disponibilidad (HA)**: una implementación de alta disponibilidad de dos servidores NetScaler ADM proporciona operaciones ininterrumpidas. En una configuración de HA, los dos nodos NetScaler ADM deben implementarse en modo activo-pasivo, en la misma subred con 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 NetScaler ADM elimina la necesidad de un equilibrador de carga independiente de NetScaler. Consulte:Configurar en una implementación de alta disponibilidad.

> Nota La
>
> alta disponibilidad no es aplicable para ADM implementado en un clúster de Kubernetes.

- **Migre de NetScaler Insight Center a NetScaler ADM**: puede migrar su implementación de NetScaler Insight Center a NetScaler ADM sin perder la configuración, los ajustes ni los datos existentes. Con NetScaler ADM, no solo puede ver los distintos análisis generados por 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 NetScaler ADM con Director: Director**se integra con NetScaler ADM para el análisis de red 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 NetScaler Application Delivery Management (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 específicos de la plataforma y los pasos detallados para instalar NetScaler ADM, consulte los siguientes temas:

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

Requisitos generales para NetScaler ADM

Componente	Requisito
RAM	32 GB
CPU virtual	8 CPUs
Espacio de almacenamiento	Citrix recomienda utilizar la tecnología Solid State Drive (SSD) para las implementaciones de NetScaler ADM. El espacio de almacenamiento predeterminado requerido es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de NetScaler ADM. Use la calculadora de tamaño que se menciona en la sección **Límites máximos** (página número 7) de la Guía de implementación de NetScaler 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 de NetScaler ADM supera los 120 GB, debe conectar un disco adicional. Citrix recomienda que estime el almacenamiento y conecte un disco adicional en el momento de la implementación inicial. Solo puede agregar un disco adicional. Para obtener más información, consulte Cómo conectar un disco adicional a NetScaler ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps

> Nota:
>
> Citrix recomienda alojar el VHD de NetScaler ADM en un almacenamiento local. Cuando se aloja en dispositivos de almacenamiento en una SAN, es posible que NetScaler ADM no funcione como se esperaba. Por lo tanto, no se admite la implementación de ADM en SAN.

NetScaler ADM en Citrix Hypervisor

January 30, 2024

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

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

Requisitos previos

Antes de instalar NetScaler 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 usar XenCenter para instalar NetScaler ADM en Citrix Hypervisor.
- Ha descargado el archivo de imagen XVA de NetScaler ADM.

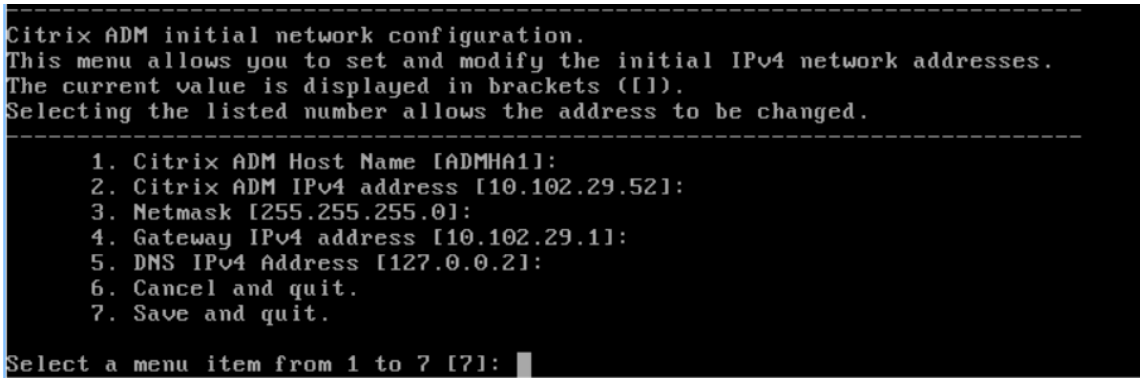
requisitos del sistema de XenCenter

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.

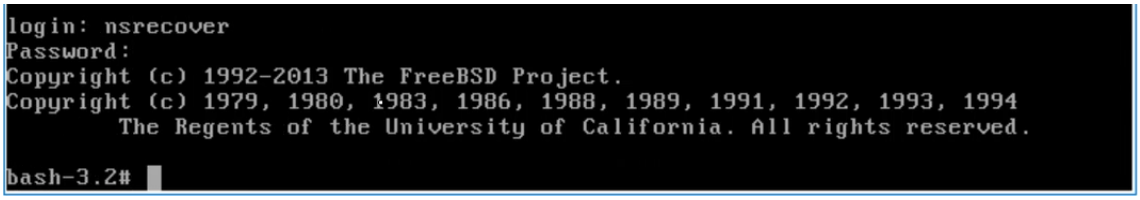
Componente	Requisito
Sistema operativo	Windows 7, Windows Server 2003 o Windows 10
.NET framework	Versión 2.0 o posterior
CPU	750 MHz (MHz), recomendado: 1 gigahercio (GHz) o más rápido
RAM	1 GB, Recomendado: 2 GB
NIC	NIC de 100 megabits por segundo (Mbps) o más rápido

Instale NetScaler 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.

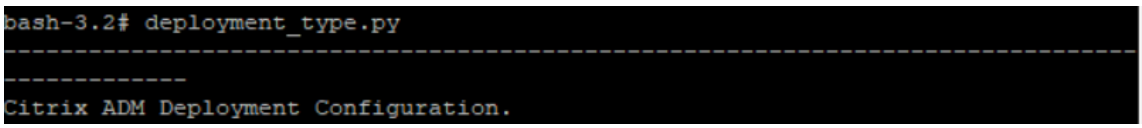


2. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.
3. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.



> **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 el símbolo del shell: `/mps/deployment_type.py`



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

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

> **Nota**
>
> Después de instalar NetScaler 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 NetScaler 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 NetScaler ADM.

NetScaler ADM en 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 NetScaler 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 ADM de NetScaler.

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.

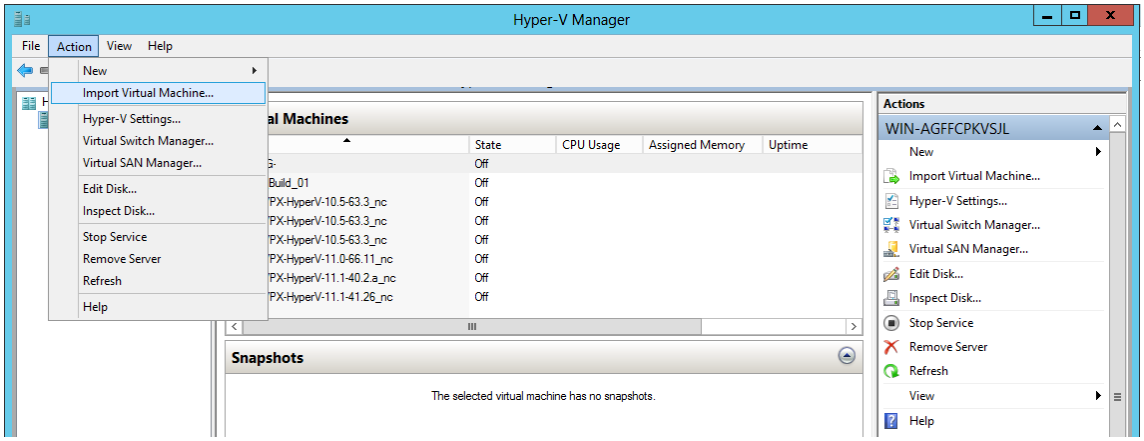
Componente	Requisito
Sistema operativo	Windows Server 2012 R2
.NET framework	Versión 2.0 o posterior
CPU	750 MHz (MHz), recomendado: 1 gigahercio (GHz) o más rápido
RAM	1 GB, Recomendado: 2 GB
NIC	NIC de 100 megabits por segundo (Mbps) o más rápido

Instalación de NetScaler Application Delivery Management

La cantidad de servidores NetScaler 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:

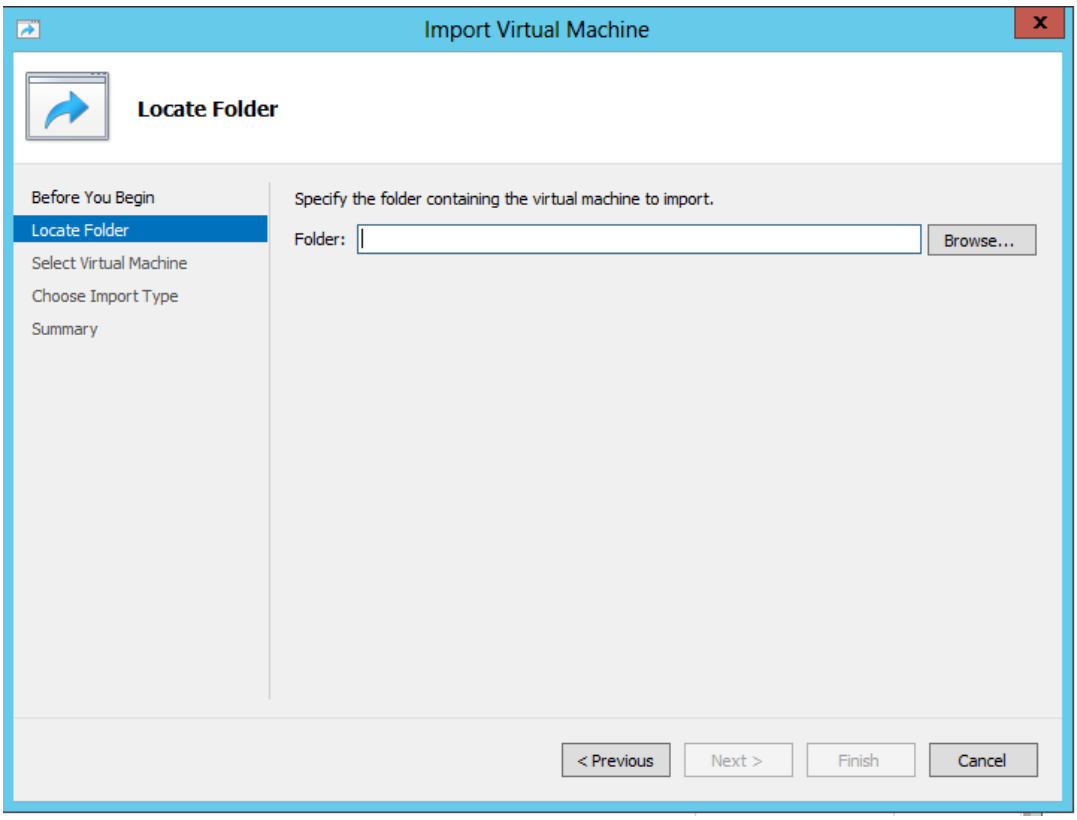
   a) **En el cuadro de diálogo Importar máquina virtual, en la sección**Localizar carpeta**, busque la carpeta en la que guardó la imagen de NetScaler ADM Hyper-V, seleccione la carpeta y haga clic en Siguiente.**

   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.

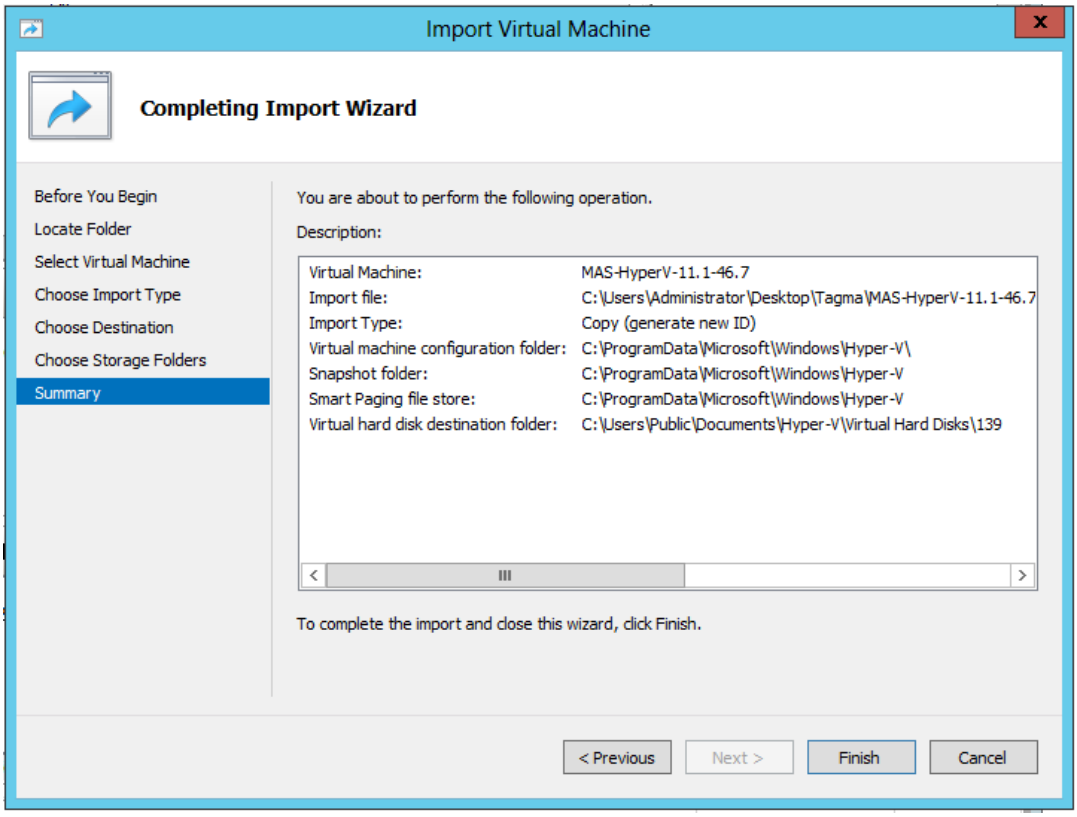
   d) En la sección **Elegir destino**, puede especificar las carpetas para almacenar los archivos de la máquina virtual.

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



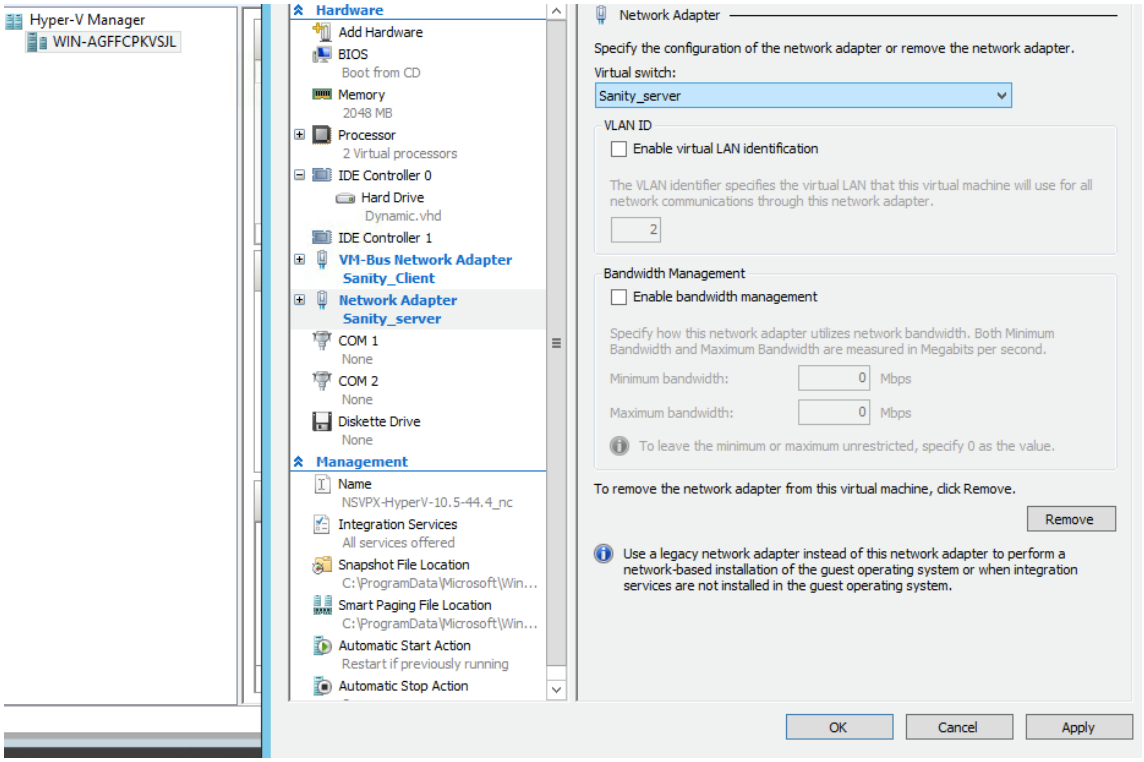
e) En la sección **Elegir carpetas de almacenamiento**, puede seleccionar la ubicación en la que desea almacenar los discos duros virtuales y, a continuación, hacer clic en **Siguiente**.

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

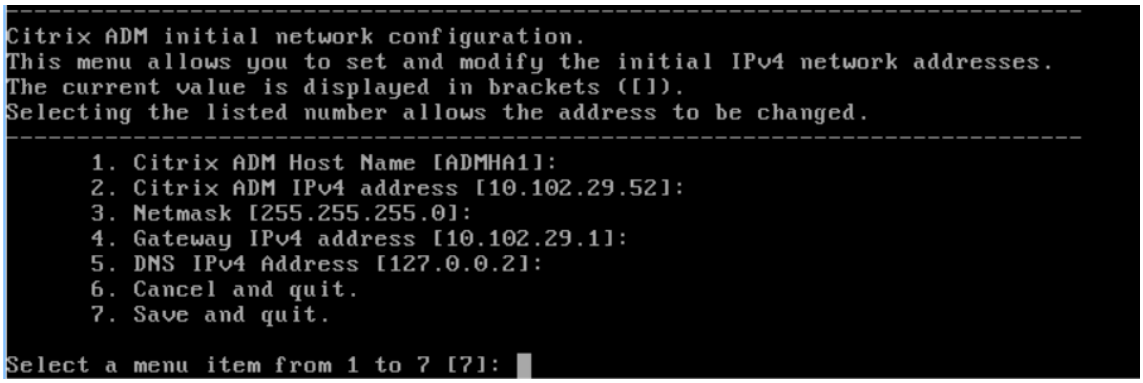


La imagen de NetScaler ADM Hyper-V se muestra en el panel derecho.

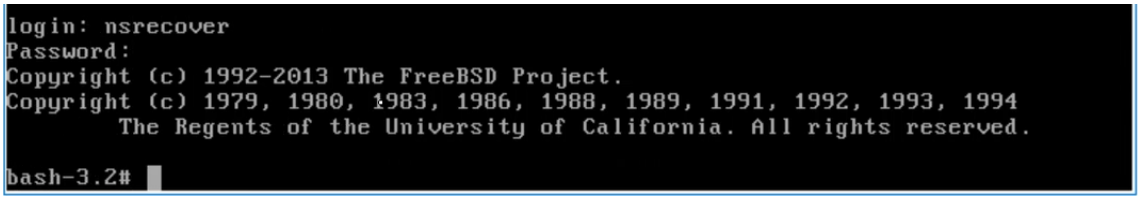
4. Haga clic con el botón secundario en la imagen de NetScaler ADM Hyper-V y, a continuación, haga clic en **Configuración**.
5. En el panel izquierdo del cuadro de diálogo que aparece, vaya a **Hardware** > **Adaptador de red VM_Bus**y, en el panel derecho, en la lista de redes, seleccione la red correspondiente.



6. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7. **Haga clic con el botón derecho en la imagen de NetScaler ADM Hyper-V y, a continuación, 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.



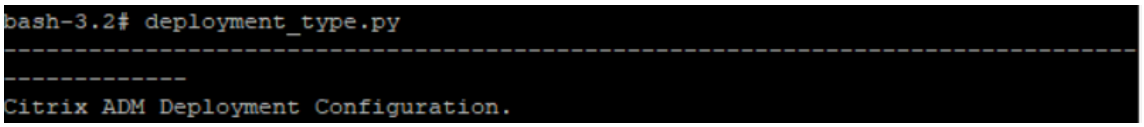
10. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.
11. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.



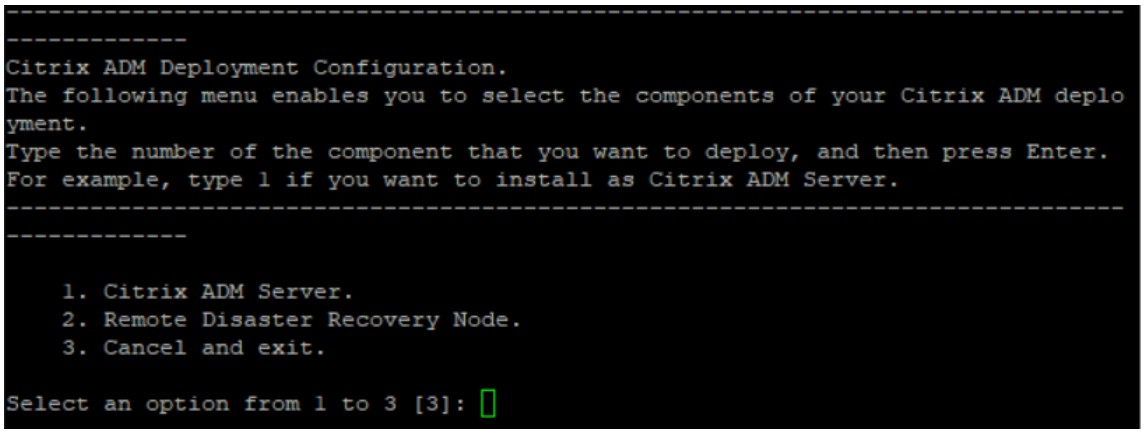
> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

12. Ejecute el script de implementación escribiendo el comando en la línea de comandos:

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



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



14. Escriba**Sí** para implementar NetScaler ADM como una implementación independiente.
15. Escriba**Sí**para reiniciar el servidor NetScaler ADM.

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

Verificación

Una vez instalado el servidor, puede acceder a la interfaz gráfica de usuario escribiendo la dirección IP del servidor NetScaler ADM en la barra de direcciones del explorador. Las credenciales de admin-

istrador predeterminadas para iniciar sesión en el servidor son nsroot/nsroot.

El explorador muestra la utilidad de configuración NetScaler ADM.

NetScaler ADM en VMware ESXi

January 30, 2024

Este documento describe cómo instalar dispositivos virtuales NetScaler ADM en VMware ESXi, mediante el cliente VMware vSphere.

Requisitos previos

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

- Instale una versión de VMware ESXi compatible (6.0, 6.5, 6.7 y 7.0).
- 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
>
> - VMotion solo es compatible con **NetScaler ADM 13.0 Build 47.22 o posterior**. Puede programar y automatizar la migración del servidor ADM implementado en un hipervisor ESXi, incluidas las configuraciones de vSphere de alta disponibilidad y vSphere DRS.
> - VMware Tools for NetScaler ADM se entrega como parte de la compilación de software y no se pueden actualizar ni modificar por separado.

Para instalar NetScaler ADM

Siga estos pasos para instalar un dispositivo virtual ADM en VMware ESXi.

> **Nota**
>
> Los pasos y las capturas de pantalla se basan en la versión 6.0 de VMware ESXi. La GUI puede diferir en otras versiones de ESXi. VMware ESXi versión 7.0.1c número de compilación 17325551 con adaptador VMXNET3 se admite en **NetScaler ADM 13.0 71.40 o posterior**. Consulte la documentación de VMware para conocer los pasos específicos de la versión.

1. Inicie el cliente de VMware vSphere en su estación de trabajo.

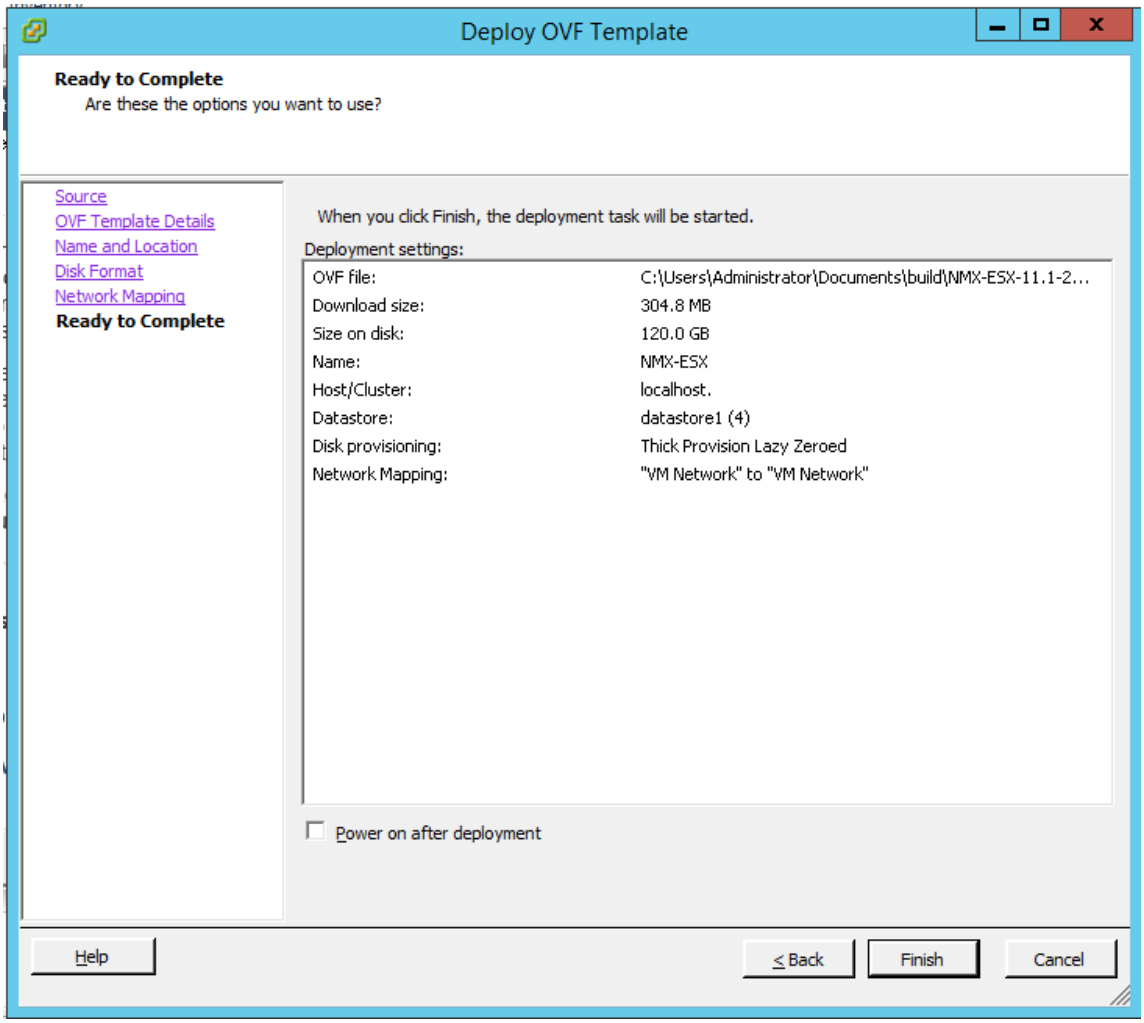
2. En el cuadro de texto **Dirección IP/Nombre**, escriba la dirección IP del servidor de VMware ESXi al que desea conectarse.
3. En los cuadros de texto **Nombre de usuario** y **Contraseña** , escriba las credenciales de administrador y, a continuación, haga clic **en**Iniciar sesión .
4. En el menú **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 soporta el sistema operativo FreeBSD. "Haga clic en **Sí**.

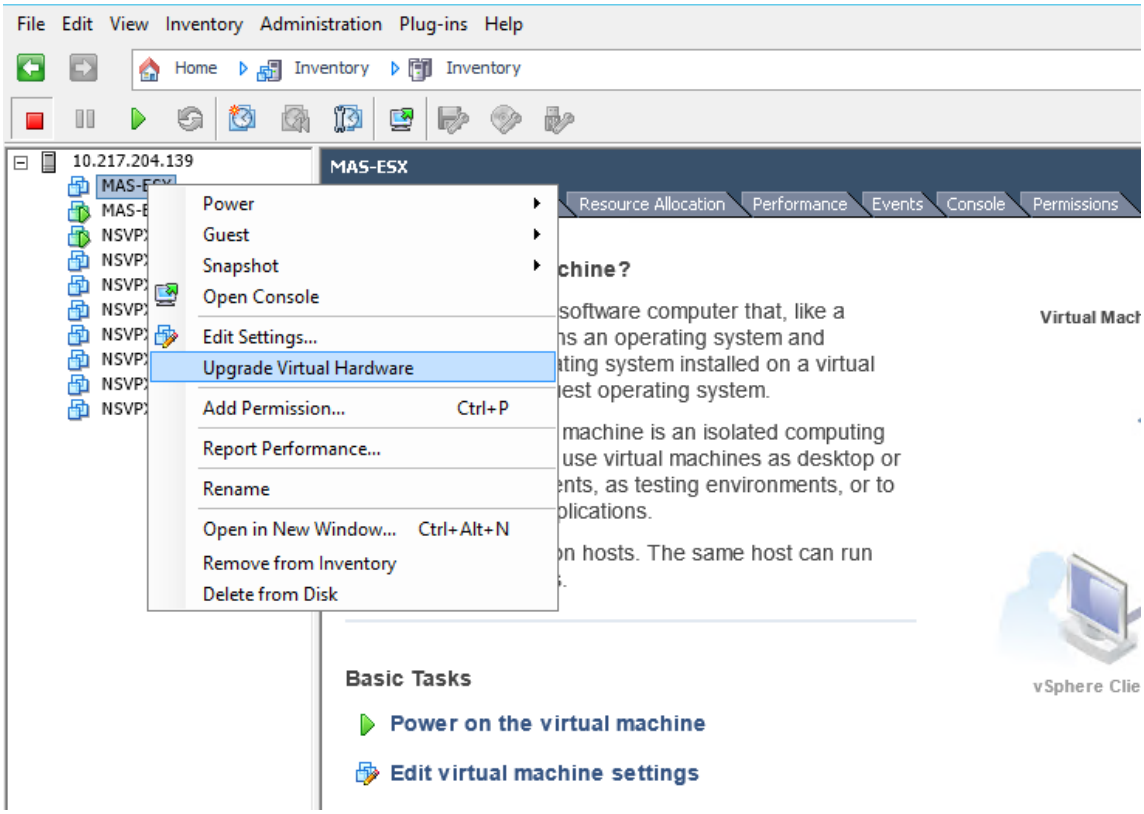
6. En la página **Detalles de plantilla de OVF**, haga clic en **Siguiente**.
7. Escriba un nombre para el dispositivo virtual NetScaler ADM y, a continuación, haga clic en **Siguiente**.
8. Especifique el formato de disco seleccionando Formato de aprovisionamiento fino o Formato de aprovisionamiento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

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

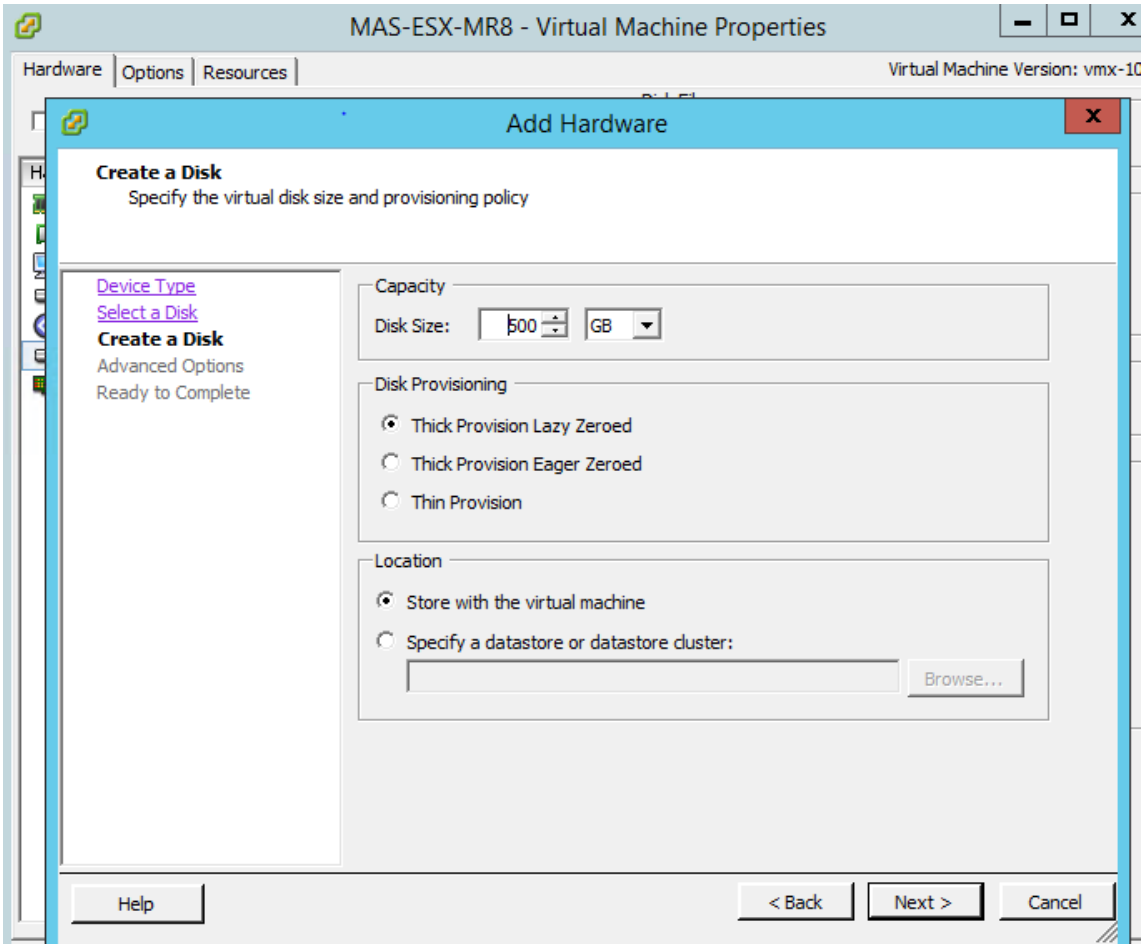
9. Haga clic en **Finalizar** para iniciar el proceso de instalación.



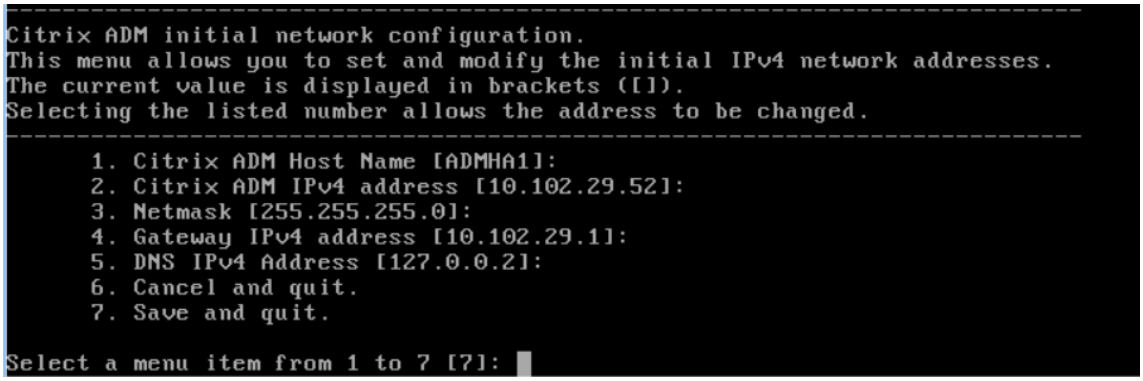
10. Ya tiene todo listo para iniciar el dispositivo virtual NetScaler ADM.
11. En el panel de navegación, seleccione el dispositivo virtual que instaló. En el menú **Inventario**, haga clic con el botón derecho en la **máquina virtual** y, a continuación, haga clic en **Actualizar hardware virtual**.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



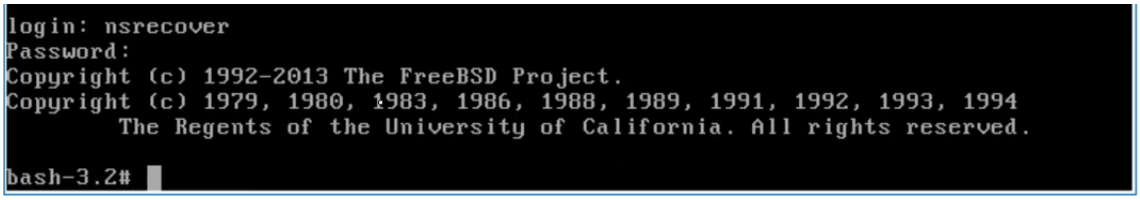
12. En el menú **Inventario**, haga clic en **Máquina virtual** y, a continuación, en **Modificar configuración**.
13. En el cuadro de diálogo **Propiedades de la máquina virtual**, en la ficha **Hardware**, haga clic en **Memoria** y, a continuación, en el panel derecho, especifique el **Tamaño de memoria** 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.



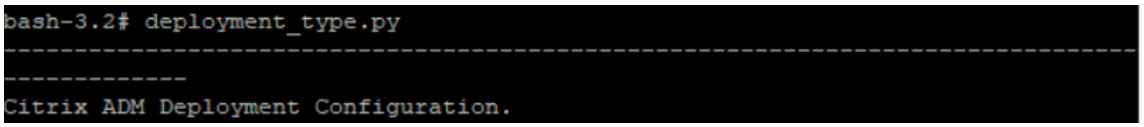
18. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.
19. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.



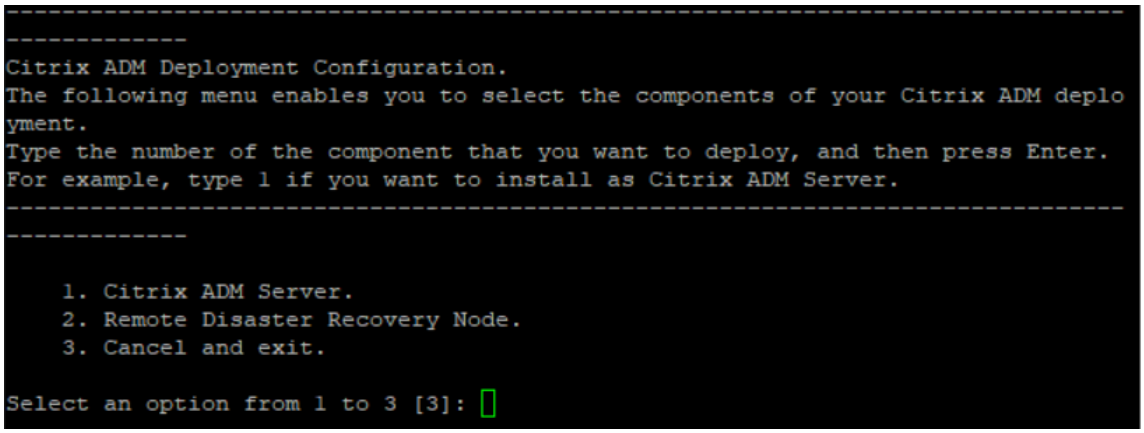
> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

20. Ejecute el script de implementación escribiendo el comando en la línea de comandos:

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



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



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

> **Nota**
>
> Después de instalar NetScaler 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 NetScaler ADM.

> **Nota**
>
> El tiempo de instalación típico de ADM es de unos 10 minutos en VMware ESXi, pero puede tardar más en algunos sistemas.

Automatice la implementación del agente ADM de NetScaler en VMware ESXi

January 30, 2024

NetScaler ADM le permite automatizar la implementación de agentes NetScaler ADM en VMware ESXi.

Como administrador, puede automatizar las siguientes acciones:

- Configurar el agente ADM de NetScaler
- Registre el agente ADM de NetScaler y cambie la contraseña predeterminada del agente.

Configurar el agente ADM de NetScaler

Para automatizar la configuración del agente, agregue los valores de los siguientes parámetros en el archivo.ovf:

1. Dirección IP
2. Máscara de red
3. Gateway
4. Servidor de nombres
5. Nombre de host

> **Nota**
>
> El archivo.ovf está disponible en el archivo de imagen del agente. Para descargar el archivo del agente ADM de NetScaler, vaya a. https://www.citrix.com/downloads/citrix-application-management/ El patrón de nomenclatura del archivo de imagen del agente es el siguiente: **MASAGENT-ESX-releasenumber-buildnumber.zip**

Registre el agente ADM de NetScaler y cambie la contraseña predeterminada

> **Nota**
>
> Antes de registrar y cambiar la contraseña predeterminada, asegúrese de haber agregado los parámetros especificados en Configurar el agente ADM de NetScaler.

Para automatizar el registro del agente ADM de NetScaler y el cambio de la contraseña predeterminada, agregue los valores de los siguientes parámetros en el mismo archivo.ovf:

1. IP del servidor ADM
2. Nombre de usuario ADM
3. Contraseña ADM
4. Contraseña nueva del agente

Requisitos previos

Antes de empezar a instalar un dispositivo virtual, asegúrese de:

- Instale VMware vSphere 8.x en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.
- Descargue los archivos de configuración de NetScaler ADM.

Cómo configurar y registrar un agente ADM de NetScaler

1. Descargue y modifique el archivo.OVF
2. Instale el dispositivo virtual NetScaler ADM en VMware ESXi
3. Verificar

Descargue y modifique el archivo.OVF

1. Extraiga los archivos del archivo MASAGENT-ESX-releasenumber-buildnumber.zip a la ubicación deseada. Están disponibles los siguientes archivos:
    - archivo.ovf
    - archivo.vmdk
    - archivo.ova
    - archivo.mf
2. Abra el archivo.ovf en cualquier editor y agregue el siguiente código de <ProductSection>..</ProductSection> ejemplo después de la etiqueta </VirtualHardwareSection>


```
<ProductSection>
    <Info>Information about the installed software</Info>
    <Product>Application Delivery management</Product>
    <Vendor>Citrix</Vendor>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.netmask">
    <Label>Netmask</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.gateway">
    <Label>Gateway</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.nameserver">
    <Label>Nameserver</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.hostname">
    <Label>Hostname</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.ServerIP">
    <Label>ADM Server IP</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.ServerUname">
    <Label>ADM Username</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
        ="VALUE"
    ovf:type="string" ovf:key="eth0.ServerPassword">
    <Label>ADM Password</Label>
    </Property>

```



```
46      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
47      ovf:type="string" ovf:key="eth0.NewPassword">
48      <Label>Agent New Password</Label>
49      </Property>
50
51  </ProductSection>
52  <!--NeedCopy-->
```

1. Para los parámetros que desee configurar, agregue sus valores correspondientes en ovf:value=” VALUE”

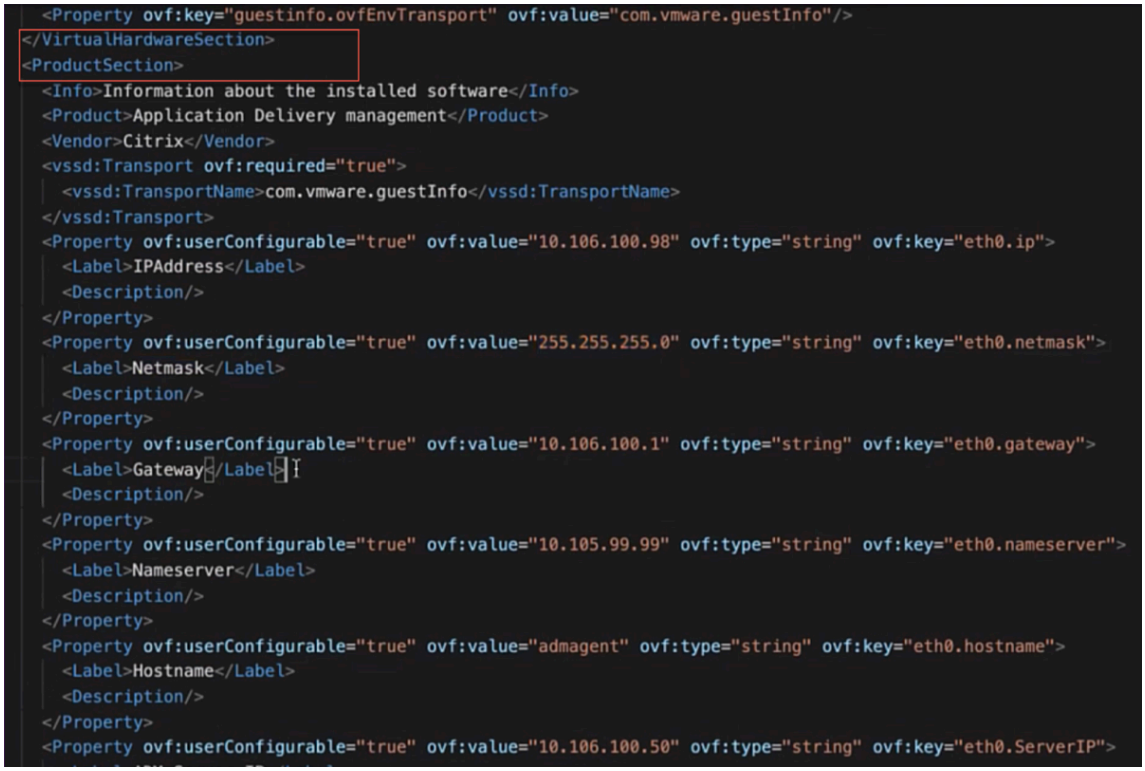
   - Para configurar el agente ADM de NetScaler, agregue los valores a los siguientes parámetros:

     - Dirección IP
     - Máscara de red
     - Gateway
     - Servidor de nombres
     - Nombre de host

   - Para registrar y cambiar la contraseña predeterminada del agente ADM de NetScaler, agregue los valores a los siguientes parámetros:

     - IP del servidor ADM
     - Nombre de usuario ADM
     - Contraseña ADM
     - Contraseña nueva del agente

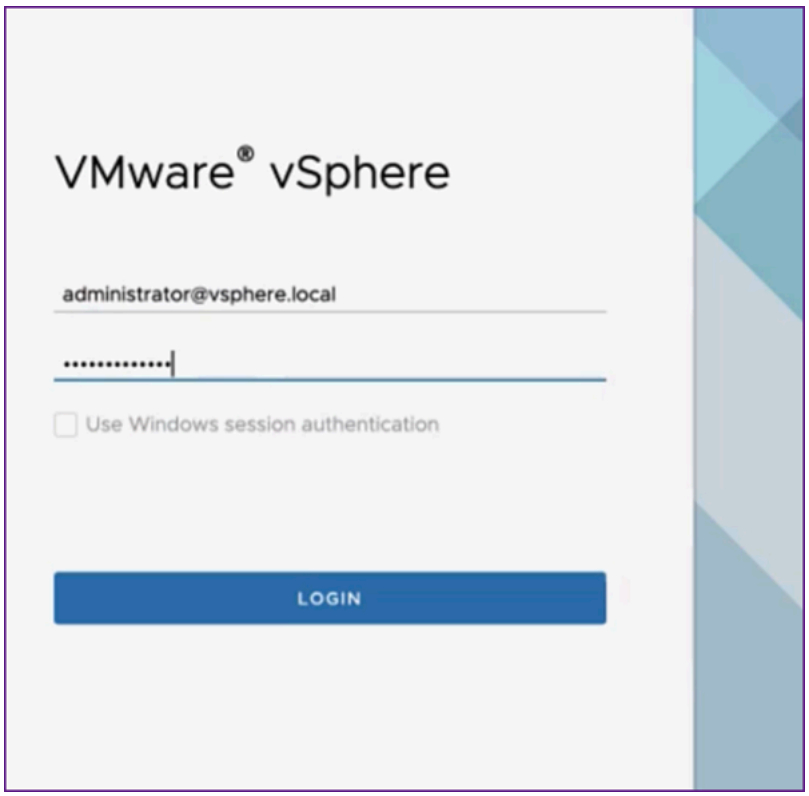
   > **Nota**
   >
   > - Debe configurar el agente ADM de NetScaler antes de registrarse y cambiar la contraseña predeterminada del agente.
   > - Si no se registra ni cambia la contraseña predeterminada en el archivo .ovf, debe realizar estas acciones manualmente después de implementar la máquina virtual.



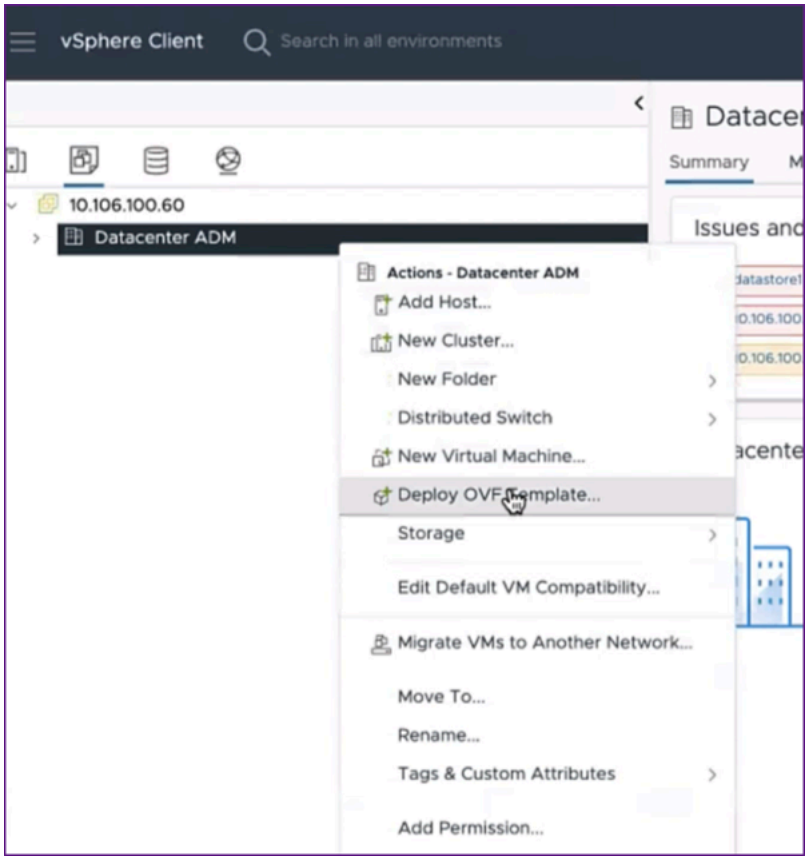
2. Tras agregar los parámetros y sus valores, guarde el archivo.ovf.

Instale el dispositivo virtual NetScaler ADM en VMware ESXi

1. Inicie sesión en **VMware vSphere Client** y escriba las credenciales de administrador. Haga clic en **Login**.

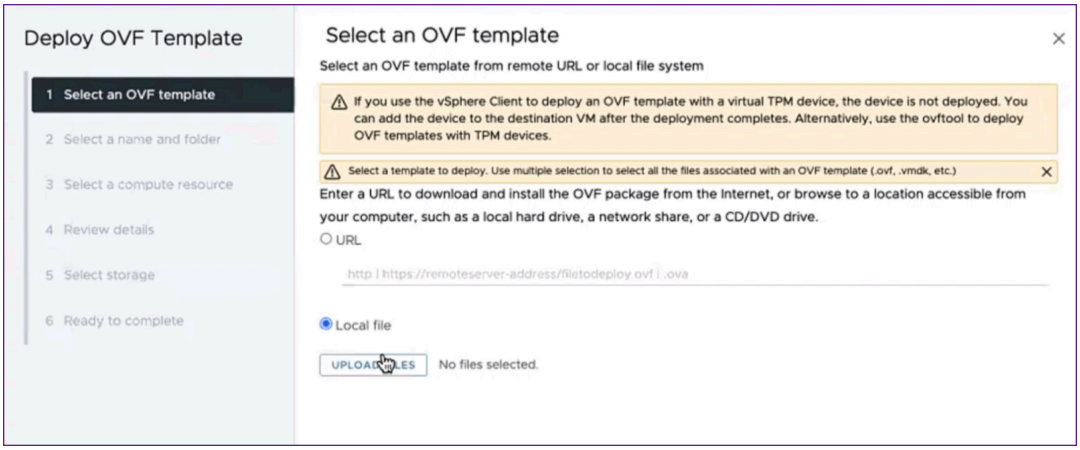


2. Seleccione su servidor ESXi y haga clic con el botón derecho para seleccionar **Implementar plantilla de OVF**.

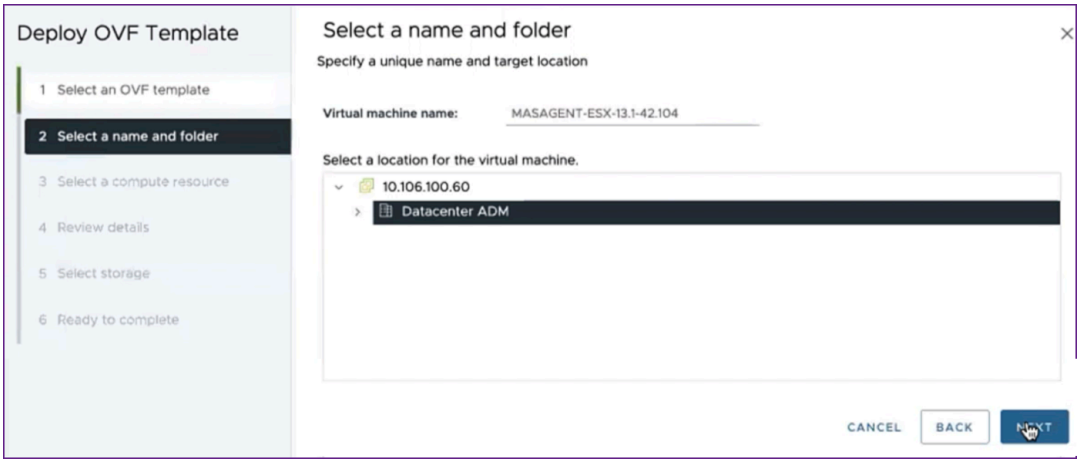


3. En la página **de plantillas Deploy OVF** :

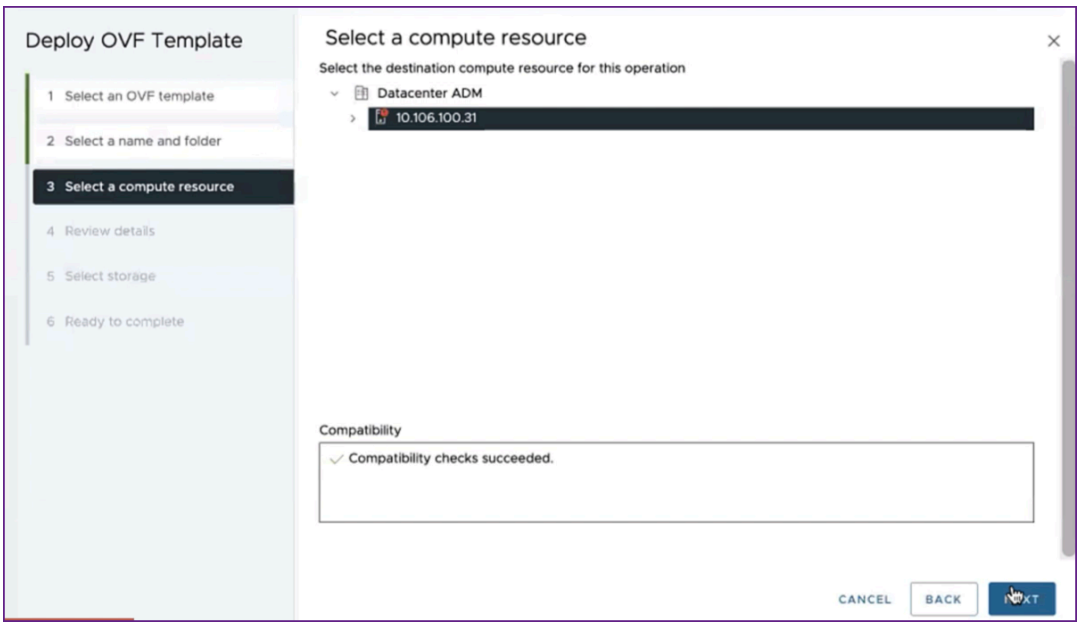
   a) **Seleccione una plantilla de OVF**: seleccione **Archivo local** y navegue hasta donde ha guardado el archivo.ovf y el archivo.vmdk editados. Seleccione los archivos y haga clic en **Abrir** para cargarlos. Haga clic en **Siguiente**.



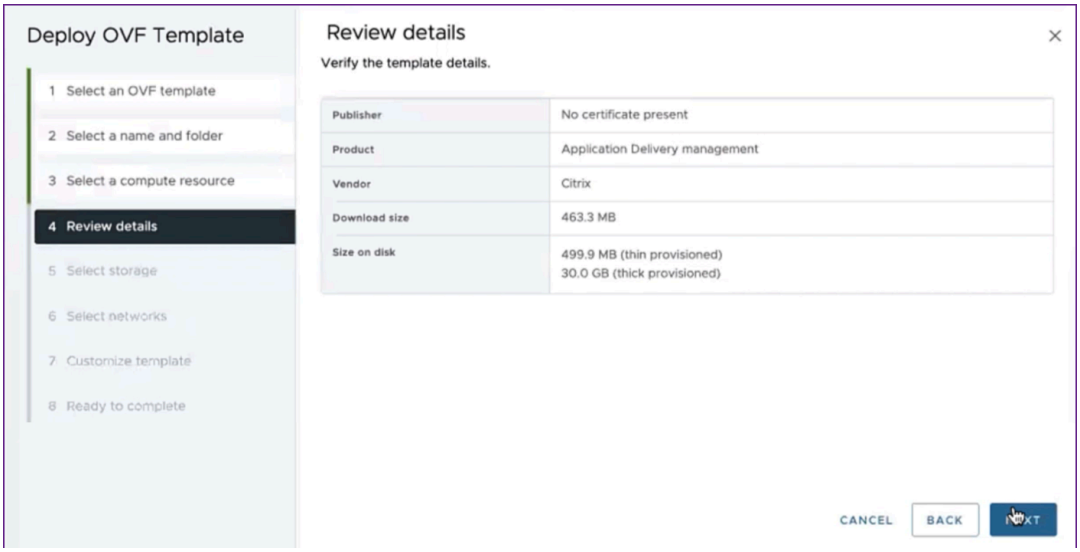
   b) **Seleccione un nombre y una carpeta**: agregue un nombre para el dispositivo virtual y seleccione la ubicación del ESXi en la que quiere implementar la máquina virtual. Haga clic en **Siguiente**.



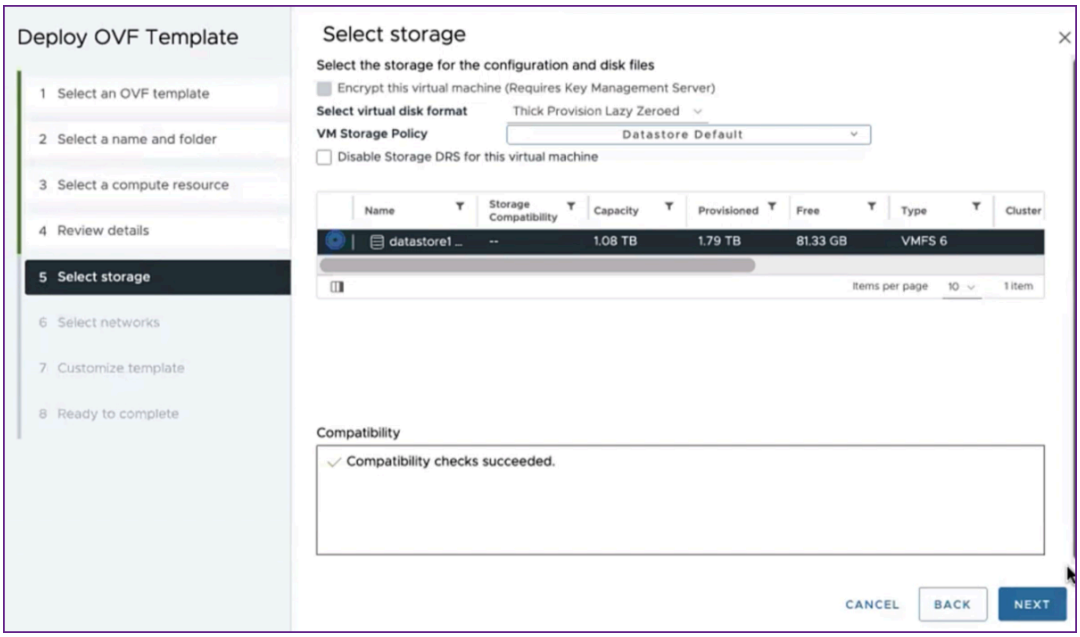
c) **Seleccione un recurso de cómputo**: seleccione un recurso en el que ejecutar la plantilla después de implementarla. Haga clic en **Siguiente**.



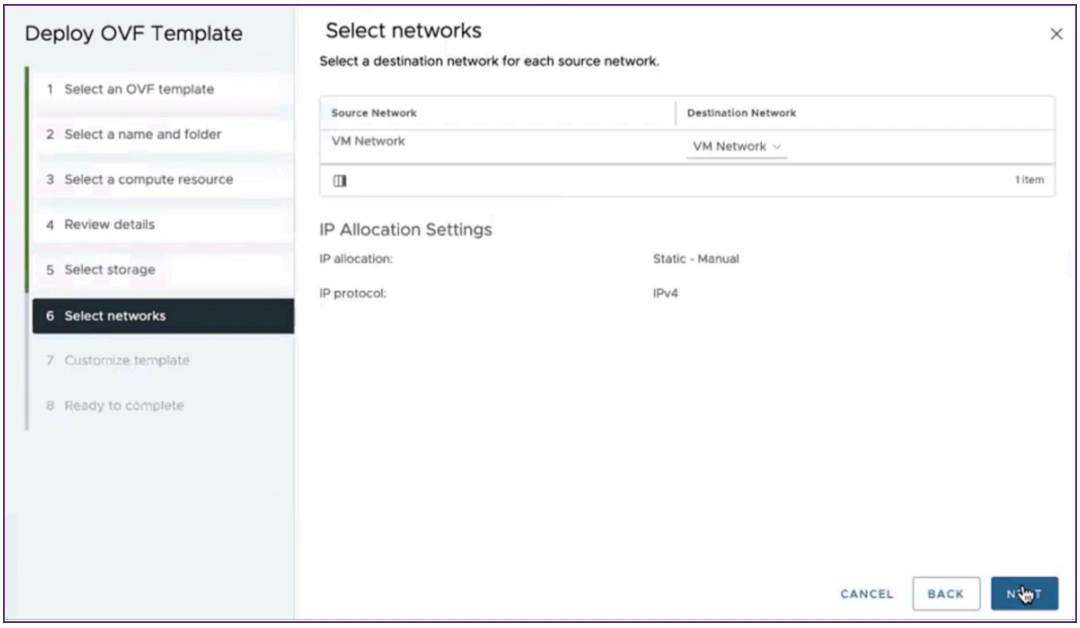
d) **Detalles de revisión**: compruebe los detalles de la plantilla de OVF. Haga clic en **Siguiente**.



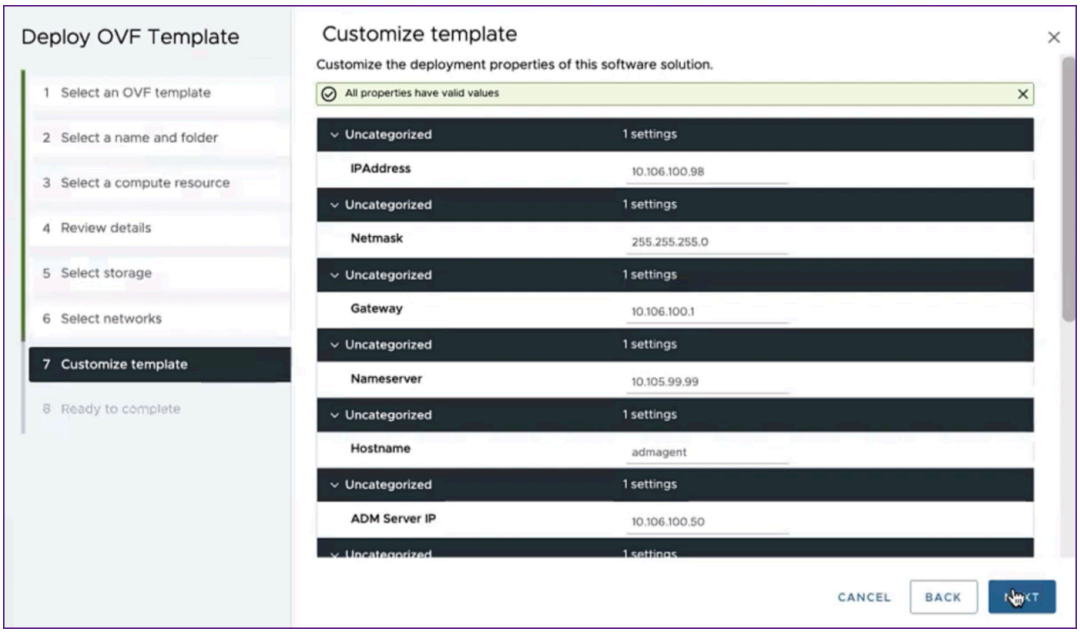
e) **Seleccione el almacenamiento**: seleccione un almacén de datos para almacenar la plantilla de OVF. Haga clic en **Siguiente**.



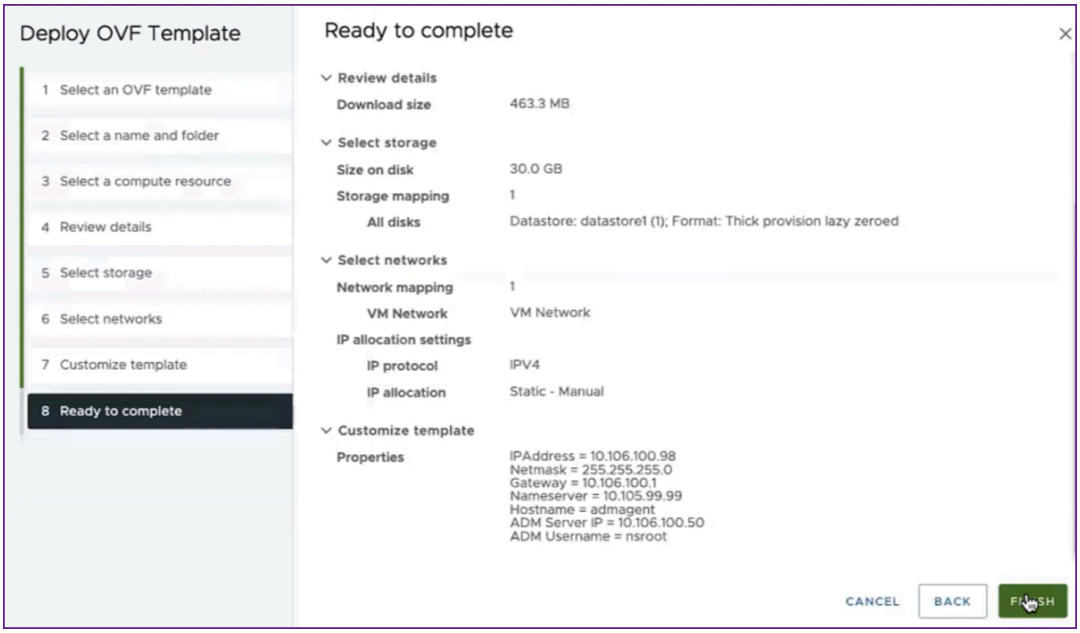
f) **Seleccione redes**: continúe con la configuración predeterminada. Haga clic en **Siguiente**.



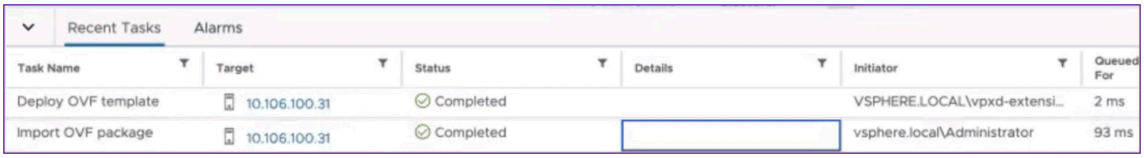
g) **Personalice la plantilla**: revise todas las propiedades de la plantilla de OVF. Se muestran todos los parámetros y valores que ha agregado al archivo.ovf en la sección Descargar y modificar el archivo OVF.



h) **Listo para completar**: para guardar la configuración e iniciar el proceso de implementación, haga clic en **Finalizar**.

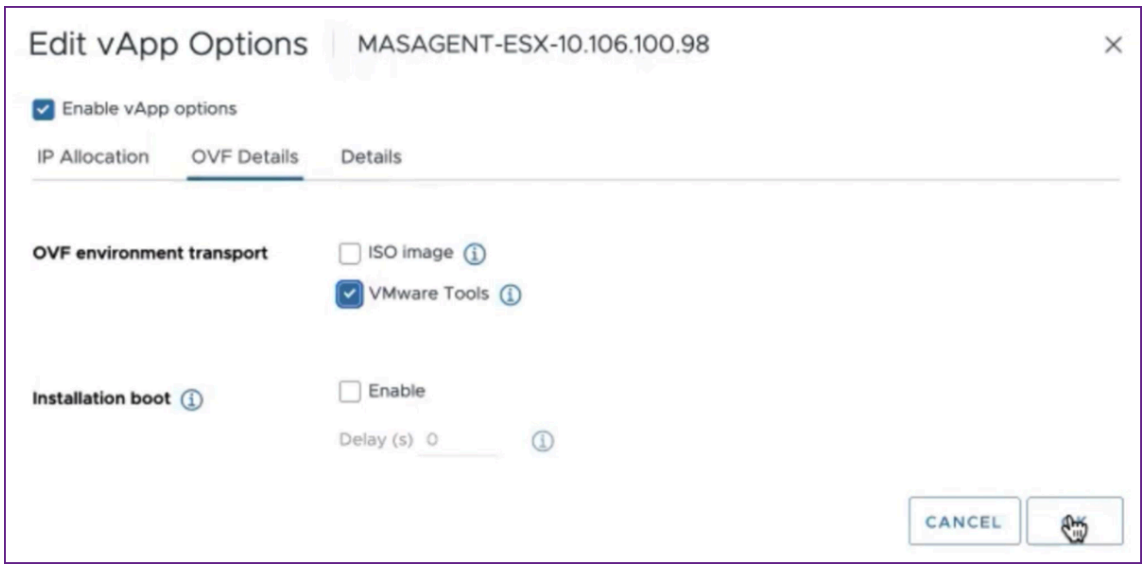


Espere a que se complete la implementación. Cuando el estado de la operación de **implementación de la plantilla de OVF** se haya completado al 100%, se implementará su agente.

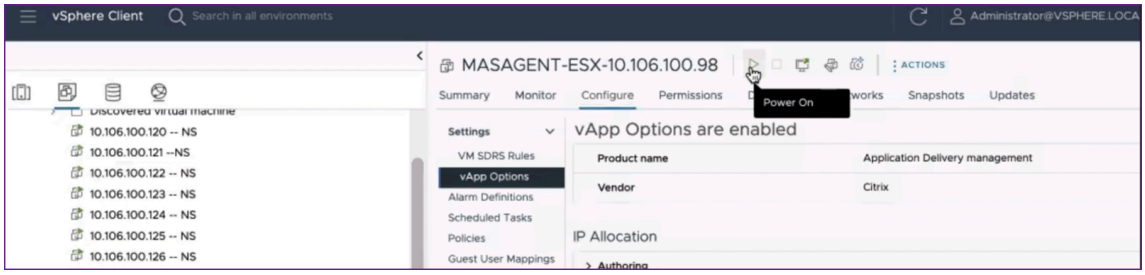


> **Importante**
>
> No encienda el dispositivo virtual antes de modificar la configuración.

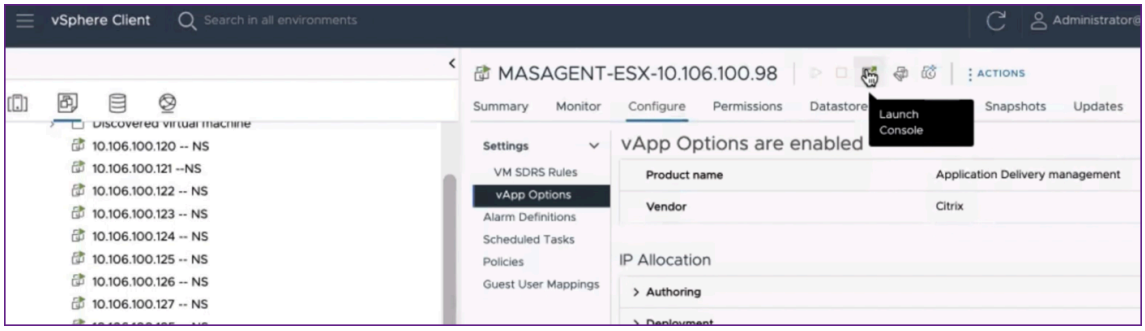
4. Haga clic en el nuevo dispositivo virtual que ha instalado y vaya a **Configurar > Configuración > Opciones de vApp > Modificar**.
5. En la ventana **Modificar opciones de vApp**, vaya a **En detalles de OVF > Transporte del entorno de OVF**y seleccione **VMware Tools**. Haga clic en **Aceptar**.

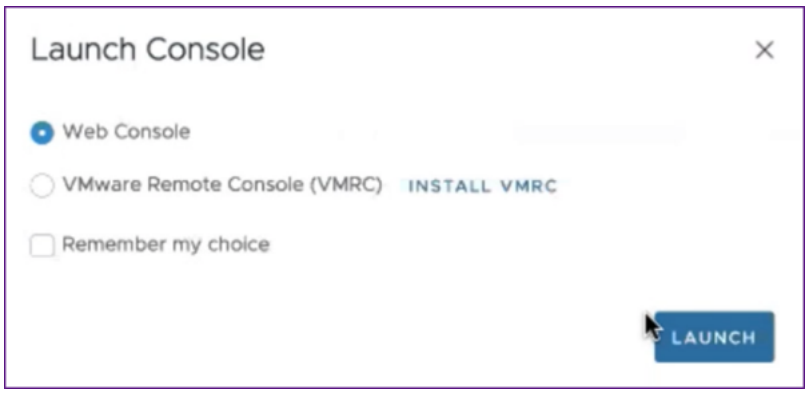


6. Haga clic con el botón derecho en la máquina virtual y, a continuación, en **Encender**. Como alternativa, puede seleccionar la ficha **Resumen** de la máquina virtual y hacer clic **en Encender**.

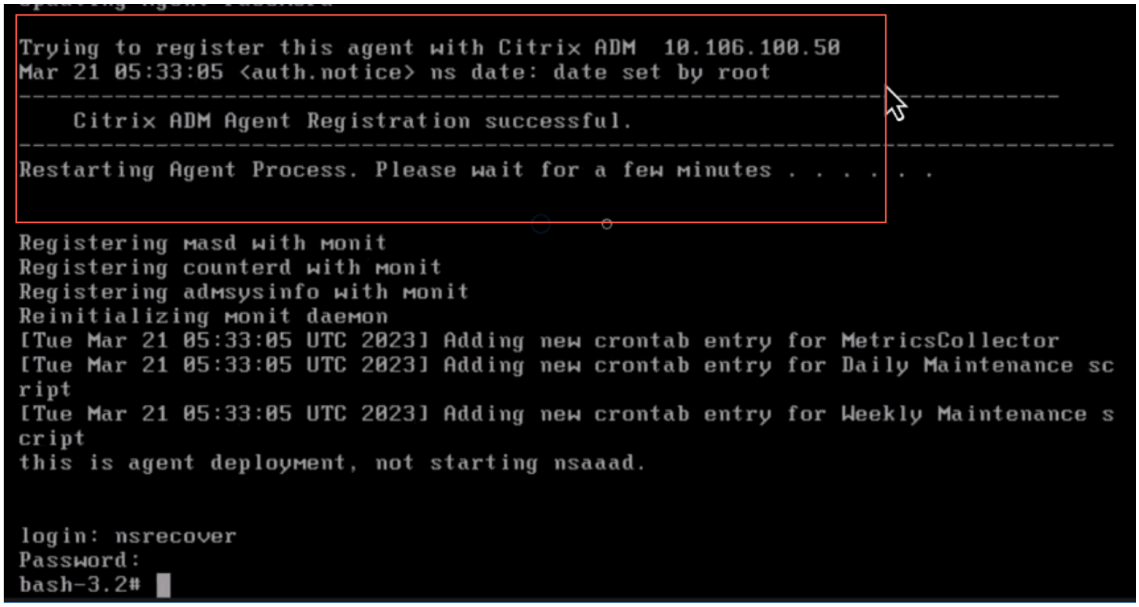


7. En la ficha **Resumen**, selecciona **Launch Web Console**.
   En la ventana **Launch Console**, seleccione **Web Console**. Haga clic en **Iniciar**.





8. En la consola, aparece un mensaje de registro correcto después de registrar el agente NetScaler ADM en el servidor NetScaler ADM. Para comprobar que se ha implementado el agente ADM de NetScaler y que se ha cambiado la contraseña predeterminada, inicie sesión con el nombre de usuario del agente NetScaler ADM y la nueva contraseña.



Verificar

Para comprobar que el agente ADM de NetScaler esté implementado:

1. Una vez implementado el agente NetScaler ADM, acceda a la GUI de NetScaler ADM escribiendo la
   dirección IP del servidor NetScaler ADM en el navegador.
2. Inicie sesión en el servidor con sus credenciales.
3. Vaya a **Infraestructura > Instancias > Agentes**.
   El agente recién implementado se muestra en la plataforma ESX.

NetScaler ADM en clúster de Kubernetes

January 30, 2024

Antes de instalar dispositivos virtuales NetScaler ADM en un clúster de Kubernetes, lea la sección de requisitos previos.

Requisitos previos

Asegúrese de que se cumplen los siguientes requisitos previos antes de instalar ADM.

Clúster de Kubernetes

- El clúster de Kubernetes debe ser de la siguiente versión o superior:
  - Versión del servidor v1.20
  - Versión de cliente v1.20

  Escriba el comando `kubectl version` para comprobar la versión.
- La aplicación Helm instalada en el clúster debe tener la versión de cliente v3.4.0 o superior.

  Use el comando `helm version` para comprobar la versión.
- El clúster de Kubernetes CNI (Container Network Interface) debe ser la versión de Calico v3.21.1 o superior.
- Todos los nodos subordinados del clúster deben tener instalado un cliente NFS. Esto se debe a que la aplicación ADM persiste los datos y la configuración en volúmenes montados en un servidor de archivos de red. Para instalar un cliente NFS en un subordinado basado en Ubuntu, escriba los siguientes comandos:

```
apt-get update
apt install nfs-common
```

- La aplicación ADM necesita 32 GB de memoria y 8 vCPU en el clúster y 120 GB de espacio en NFS.

Compartición de NFS

La aplicación ADM necesita volúmenes persistentes para almacenar datos como la configuración, los certificados, las imágenes y otros. Para ello, ADM requiere montajes NFS. La aplicación requiere dos carpetas de los montajes de red compartidos:

- Uno para almacenar archivos como certificados, imágenes y otros
- El otro para la base de datos

> Nota
>
> Se recomienda tener un NFS con una SSD.

Estas dos carpetas pueden ser diferentes o iguales. Ambas carpetas deben tener 777 permisos. La primera carpeta debe tener un espacio mínimo de 10 GB. El tamaño de la segunda carpeta depende de la cantidad de datos que deben ser persistentes en la base de datos. El tamaño mínimo es de 100 GB.
Para el entorno de producción, recomendamos tener una solución NFS de grado de producción.

Dispositivo NetScaler

Se requiere el dispositivo NetScaler como dispositivo de entrada. ADC hace que los servicios de aplicaciones requeridos estén disponibles fuera del
clúster de Kubernetes. El dispositivo NetScaler debe estar fuera del clúster de Kubernetes y los nodos de trabajo deben ser accesibles desde el ADC. Siga estos pasos:

- Configure un SNIP en el ADC. ADC usa este SNIP para llegar a los nodos de trabajo del clúster de Kubernetes.
- Identifique una dirección IP gratuita que se utilizará como dirección IP del servidor virtual para que los servicios de aplicaciones requeridos estén disponibles fuera del clúster de Kubernetes.

Instalar ADM en el clúster de Kubernetes

Siga estos pasos para instalar un dispositivo ADM en un clúster de Kubernetes:

1. Vaya al sitio de NetScaler y descargue el archivo del gráfico de mandos ADM de NetScaler para Kubernetes.
2. Extraiga el tarball descargado del gráfico de Helm en el directorio /var del nodo principal del clúster de Kubernetes.
3. Abra el`values.yaml` archivo bajo el`/var/citrixadm` directorio.
4. Introduzca una contraseña para la base de datos en el campo `dbpasswd` del archivo.
5. Cambie los valores siguientes. La aplicación ADM utiliza estos valores para configurar el dispositivo NetScaler de modo que los servicios estén expuestos al mundo externo:
    - `ingressIP`: una IP virtual configurada en NetScaler para acceder a la aplicación.

- `applicationID`: un identificador único para distinguir la configuración de ingreso del resto de la configuración en el dispositivo NetScaler.
- `ingressADCIP`: la dirección IP NetScaler (NSIP), que se utiliza como ingreso para la aplicación ADM.
- `ingressADCUsername`: un nombre de usuario para acceder al dispositivo NetScaler. Este usuario debe tener privilegios de escritura.
- `ingressADCPassword`: Contraseña para el nombre de usuario.

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. Cambie los siguientes valores en la sección de **almacenamiento**. Estos valores especifican la persistencia requerida para almacenar los archivos requeridos por la aplicación ADM.
   - `nfsServer`: nombre de host o dirección IP del servidor NFS
   - `path`: monta la ruta de la carpeta para almacenar los archivos de la aplicación.
   - `size`: al menos 10 GB.

   > Nota
   >
   > La unidad de este valor es Gi. Por ejemplo, 10Gi, 20Gi.

7. Vaya a la sección **de almacenamiento** en`pg-datastore` y cambie los siguientes valores. Estos valores especifican la persistencia utilizada para crear una base de datos.
   - `nsfServer`: nombre de host o dirección IP del servidor NFS.
   - `size`: monte una ruta para la carpeta utilizada para el almacén de datos.
   - `path`: al menos 100 GB.

   > Nota
   >
   > La unidad de este valor es Gi. Por ejemplo, 100Gi, 200Gi.

8. Vaya al directorio /var/citrix en el nodo principal y ejecute el siguiente comando para instalar una aplicación ADM:
   `helm install -n citrixadm --namespace <name> ./citrixadm`

> Nota
>
> Este comando helm no se admite en la versión 3.x de helm.

Este comando también instala los pods necesarios en el clúster. El argumento de espacio de nombres es opcional. Si no se proporciona un espacio de nombres, Helm instala ADM en el espacio de nombres predeterminado. Para facilitar la administración, instale ADM en un espacio de nombres independiente.

9. Abra su explorador y escriba `http://< virtual server IP address >` e inicie sesión en el ADM utilizando `nsroot`/`nsroot` como credenciales. Para un acceso seguro escriba `https://< virtual server IP address >`.

> Nota
>
> Durante la implementación, la aplicación ADM crea tablas en el almacén de datos, lo que puede tardar un poco. Dependiendo de los recursos asignados por Kubernetes a varios pods de la aplicación ADM, el servicio puede tardar entre 5 y 15 minutos en aparecer.

NetScaler ADM en el 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 NetScaler ADM en su plataforma Linux-KVM y configúrelo para su red.

Requisitos previos

Antes de instalar el dispositivo virtual NetScaler ADM, compruebe que la versión 3.6.11-4 de Linux-KVM y versiones posteriores estén instaladas 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 mayor es la velocidad, mejor será el rendimiento del 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 NetScaler ADM requiere 120 GB de espacio en disco.

> **Nota**
>
> Los requisitos de memoria y disco duro especificados son para implementar NetScaler ADM en la plataforma OpenStack, teniendo en cuenta que no hay otras máquinas virtuales en ejecución 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 NetScaler ADM solo admite una interfaz de red paravirtualizada de virtIO. Asegúrese de conectar esta interfaz a la red de administración del host Linux-KVM para que NetScaler 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 de **descargas**, seleccione **NetScaler Application Delivery Management**.
5. En la página **NetScaler Application Delivery Management**, seleccione la versión. Por ejemplo, seleccione la **versión 13.0**.
6. Haga clic en **Software de producto** para expandirlo y haga clic en la versión más reciente. Por ejemplo, seleccione **NetScaler MAS Release (Feature Phase) 13.0**Build 36.27.

   Se muestra la página de creación seleccionada.
7. En la lista **Jump to Download**, seleccione **NetScaler MAS image for KVM, 13.0 Build xx.xx**
8. Haga clic en **Descargar archivo**, acepte el CLUF 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.

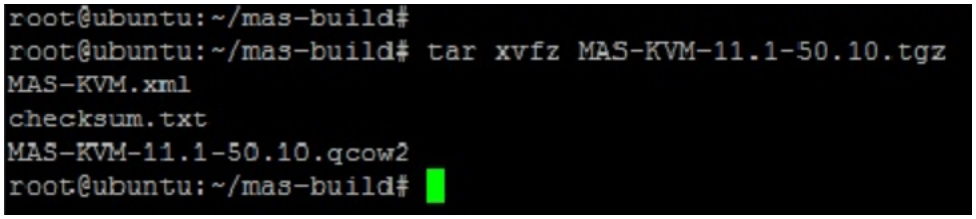
   b) Utilice el comando tar para descomprimir el archivo de imagen de NetScaler Application Delivery Management. El paquete descomprimido contiene los siguientes componentes:

      i. Un archivo XML de dominio que especifica los atributos ADM de NetScaler

      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. `name` - Especifique el nombre.

   B. `mac` - Especifique la dirección MAC.

   C. `source file`: Especifique la ruta de origen de la imagen de disco absoluta. La ruta del archivo tiene que ser absoluta.

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

   D. `mode` - Especifique el modo.

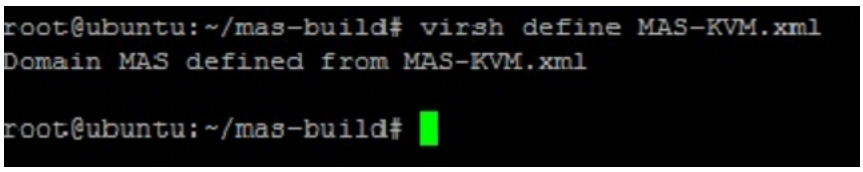
   E. `model type` - Establece Virtio.

   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-->
```

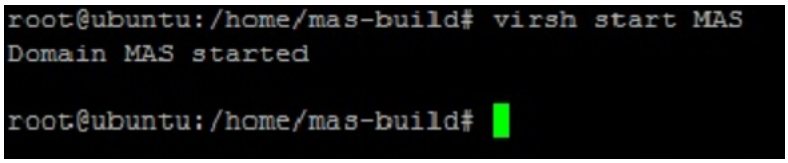
vi. Defina los atributos de VM en el archivo MAS1-KVM.xml mediante el siguiente comando: `virsh define \<FileName\>.xml`

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

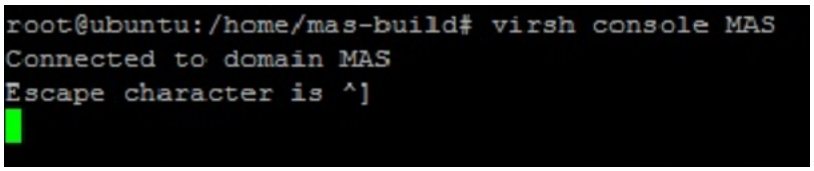
vii. Inicie NetScaler ADM escribiendo el siguiente comando: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

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



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

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



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 NetScaler ADM, la CLI y la GUI de NetScaler 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. Retire el módulo kvm_intel con el siguiente comando:
>   `rmmod kvm\\_intel`

2. Desactive **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.

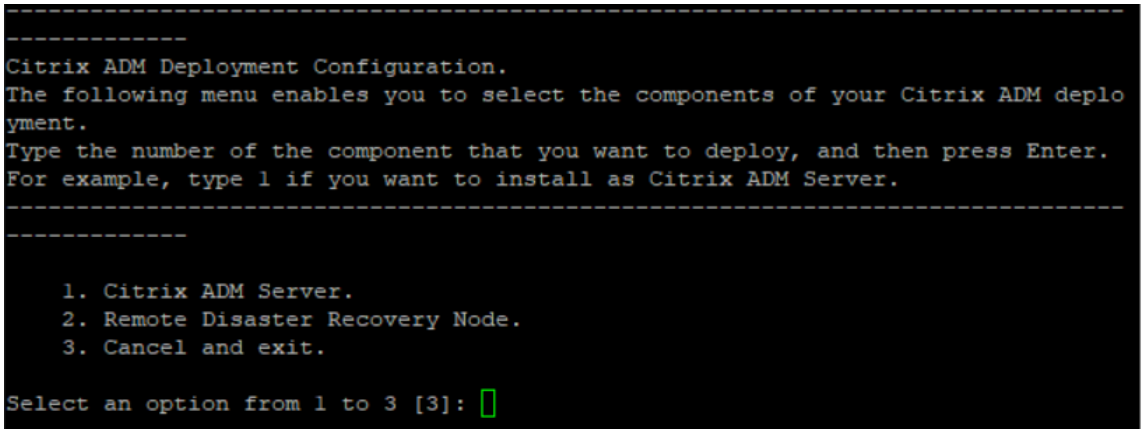
Después de instalar NetScaler ADM, espere unos 10 minutos para que los servicios estén disponibles y, a continuación, inicie sesión en NetScaler ADM.

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

   Después de iniciar sesión por primera vez, cambie 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 NetScaler ADM, vaya a **Configuración > 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 entrar en el menú de configuración de red inicial de NetScaler ADM. Configure la dirección IP de administración.
4. Para completar la configuración de red inicial de NetScaler ADM, siga las instrucciones. La consola muestra las opciones de configuración de red inicial de NetScaler ADM para configurar los siguientes parámetros para el NetScaler ADM. El nombre del host se rellena de forma predeterminada.
   a) Introduzca **2** para actualizar la dirección IPv4 de NetScaler ADM: Dirección IP de administración desde la que accede a NetScaler 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 Gateway: La dirección IP de la puerta de enlace predeterminada para la subred de la dirección IP de administración de NetScaler ADM.
   d) Escriba **7** para guardar y salir: Guarda los cambios de configuración y sale del sistema.

5. Ejecute el script de implementación escribiendo el comando en el símbolo del shell: `deployment_type.py`
6. En la pantalla de implementación que aparece, seleccione el tipo de implementación como **servidor de NetScaler ADM**.



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

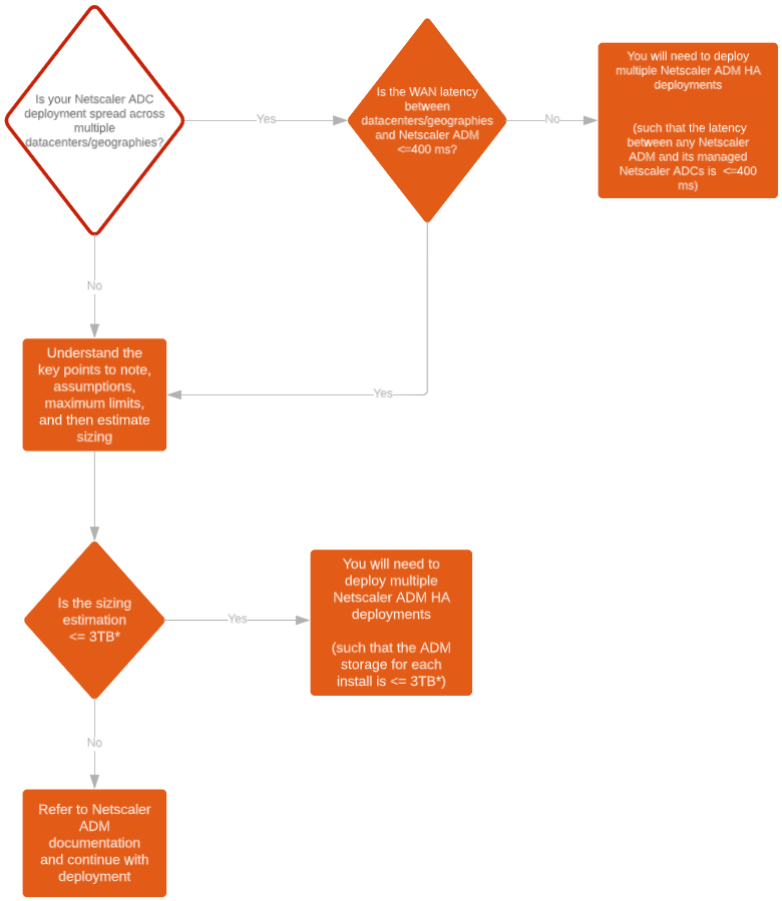
   Más adelante, puede acceder al NetScaler ADM escribiendo la dirección IP del servidor NetScaler ADM en la barra de direcciones del navegador. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son *nsroot/nsroot* .

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 NetScaler 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 NetScaler ADM HA es de 3 TB. Para obtener más información, consulte la guía de implementación.
>
> **Importante**
>
> **Para acceder a NetScaler ADM 12.1, build 48.18 o versiones posteriores mediante HTTPS:**
>
> Si ha configurado una instancia de NetScaler para equilibrar la carga de NetScaler ADM en un modo de alta disponibilidad, primero elimine la instancia de NetScaler. A continuación, configure una dirección IP flotante para acceder a NetScaler ADM en modo de alta disponibilidad.

Los siguientes son los beneficios de la implementación de alta disponibilidad en NetScaler 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.
- Posibilidad de configurar la dirección IP flotante en el nodo principal para eliminar la necesidad de un balanceador de carga de NetScaler independiente.
- Proporciona un fácil acceso a la interfaz de usuario de NetScaler ADM mediante la dirección IP flotante.
- La interfaz de usuario NetScaler 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.

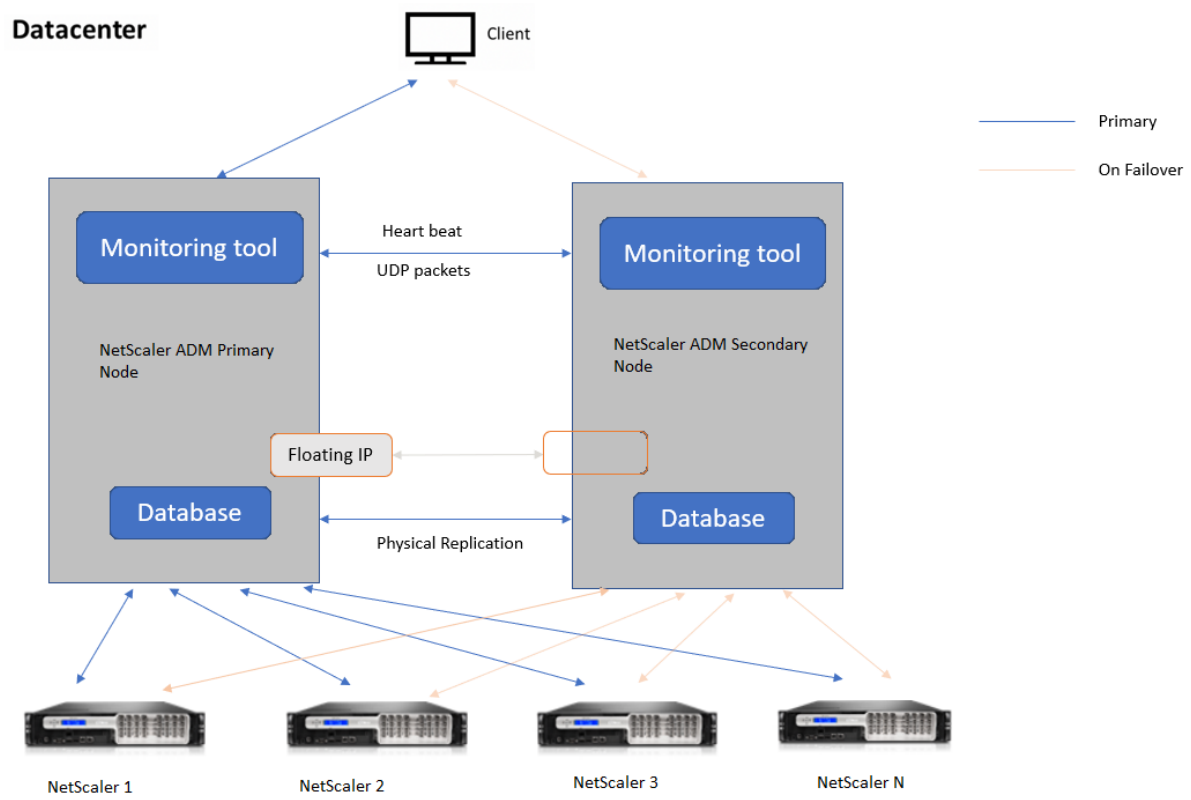
Términos y condiciones	Descripción
Nodo principal	Primer nodo registrado en la implementación de alta disponibilidad.
Nodo secundario	Segundo nodo registrado en la implementación de alta disponibilidad.
Latido	Mecanismo utilizado para intercambiar mensajes entre el nodo principal y el secundario en la 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 NetScaler ADM implementados en modo de alta disponibilidad.



En la implementación de alta disponibilidad, un nodo NetScaler 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 ADM de NetScaler 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 NetScaler 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 NetScaler ADM y la base de datos para intercambiar información sobre el estado del nodo, el estado, los procesos, etc. 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 que se asigna a la dirección IP del nodo principal y que el cliente puede usar para conectarse a NetScaler 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 ADM de NetScaler se implementan en modo activo y 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.

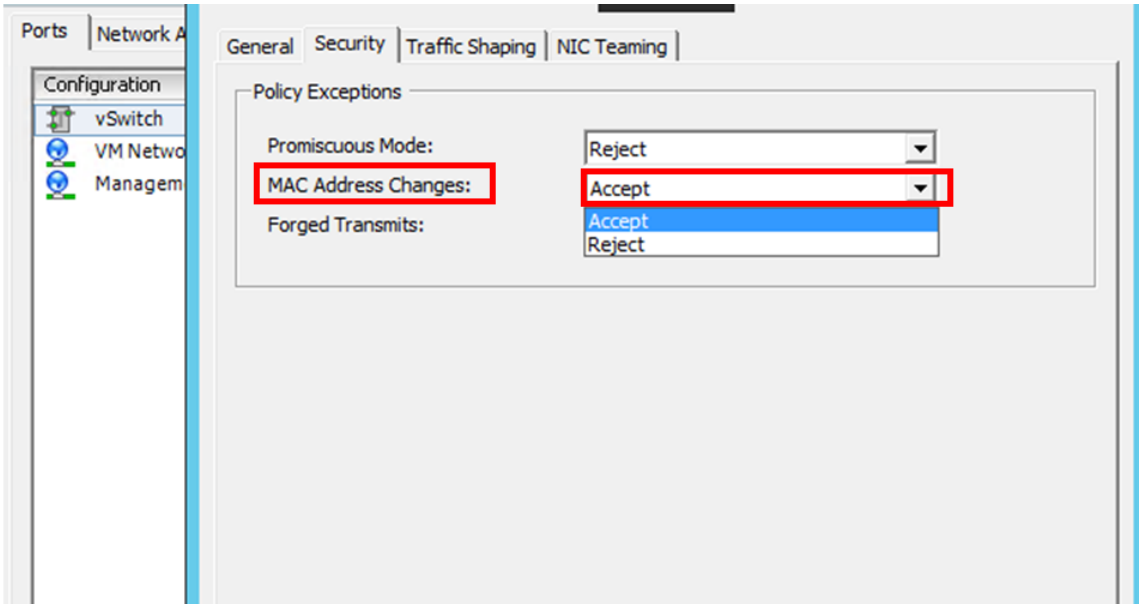
- Base de datos:
  - En una configuración de alta disponibilidad, todos los archivos de configuración se sincronizan automáticamente del nodo principal al nodo secundario en un intervalo de un minuto.
  - La sincronización de bases de datos se realiza al instante mediante la replicación física de la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

- Actualización de NetScaler ADM:
  - Los procesos internos actualizan implícitamente NetScaler ADM con respecto a 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 NetScaler ADM en un entorno de 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.

> **Nota**
>
> Para NetScaler ADM implementado en la versión 6.7 de ESXI, puede configurar la opción de **cambios de dirección MAC** como **Rechazar** también. Tras la conmutación por error, el tráfico fluye al nuevo nodo principal sin problemas, independientemente de la configuración de **cambios de dirección MAC**. Por lo tanto, aceptar los cambios en la dirección MAC no es obligatorio.
>
> Si el ADM de NetScaler se implementa en la versión de ESXI inferior a 6.7, asegúrese de que la opción **Cambios de dirección MAC** esté configurada en **Aceptar** únicamente.



Requisitos previos

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

- La implementación de alta disponibilidad de NetScaler ADM es compatible con la versión 12.0, compilación 51.24 de NetScaler ADM.
- Descargue el archivo de imagen de NetScaler Application Delivery Management (.xva) del sitio de NetScaler: 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**
Espacio de almacenamiento	Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de NetScaler ADM. El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de NetScaler ADM. Si sus requisitos de almacenamiento de NetScaler 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 NetScaler 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 NetScaler 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.

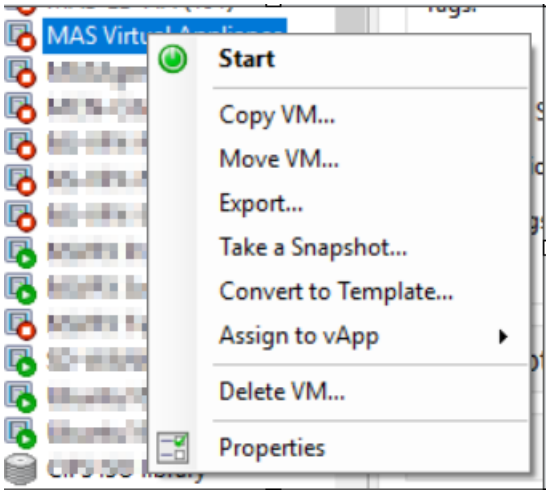
Registrar e implementar el primer servidor (nodo principal)

Para registrar el primer nodo:

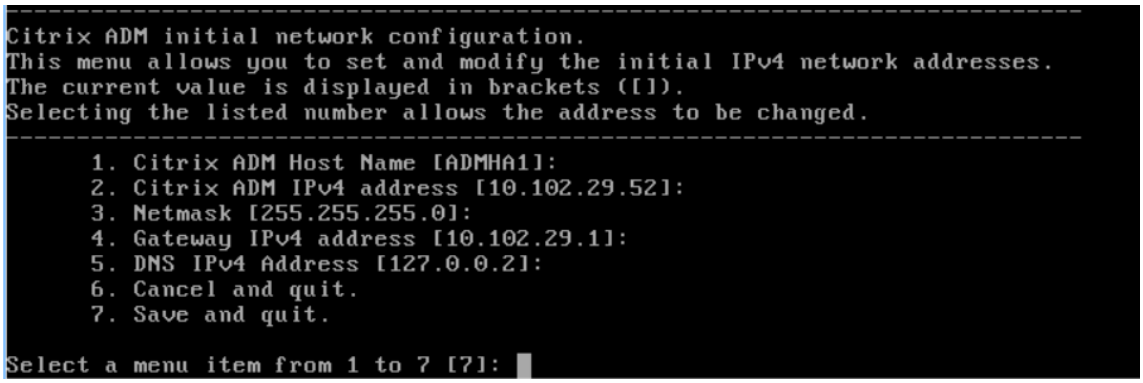
1. Utilice el archivo de imagen.xva descargado del sitio de NetScaler e impórtelo al hipervisor.

   > **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 NetScaler ADM con las configuraciones de red iniciales.

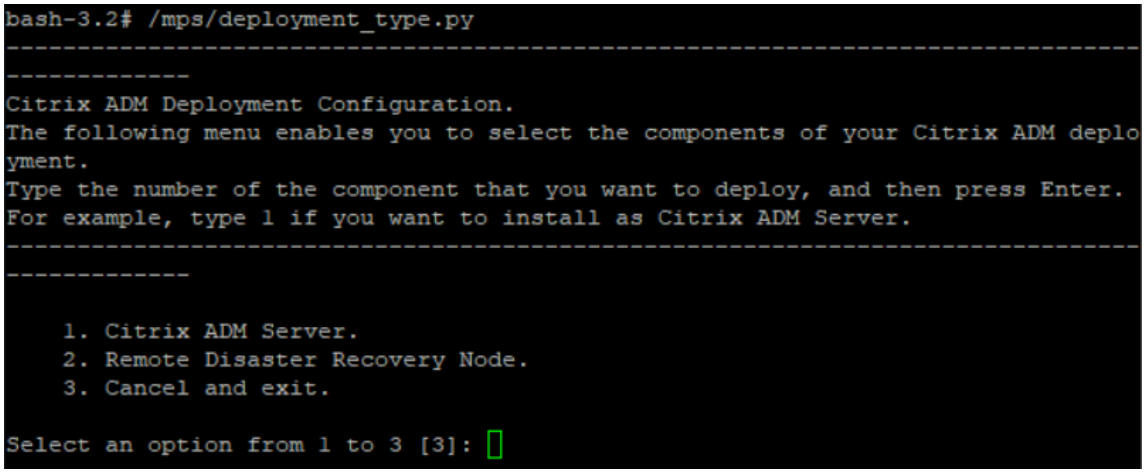
   

4. Una vez completada la configuración de red inicial, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: *nsrecover/nsroot*.

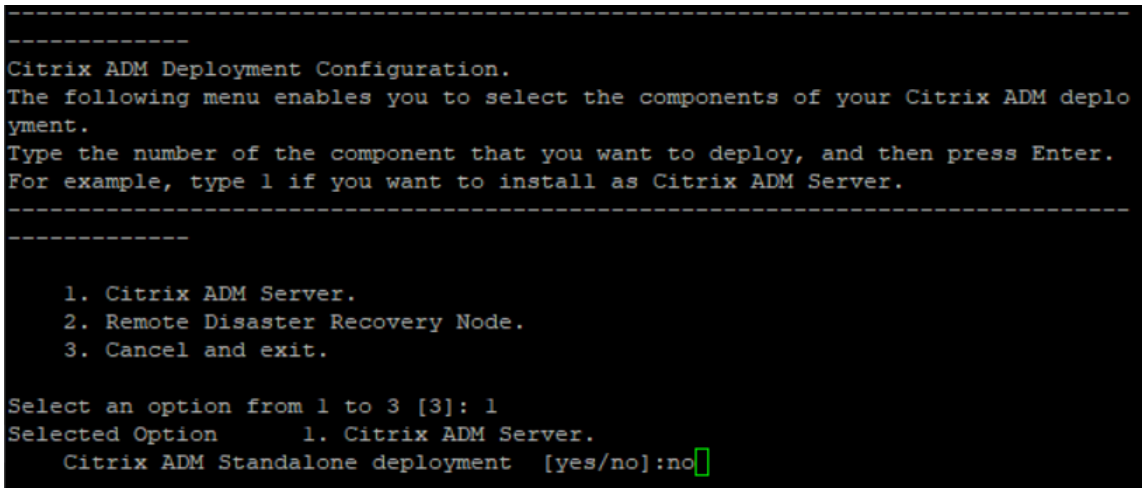
   > **Nota**
   >
   > Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

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

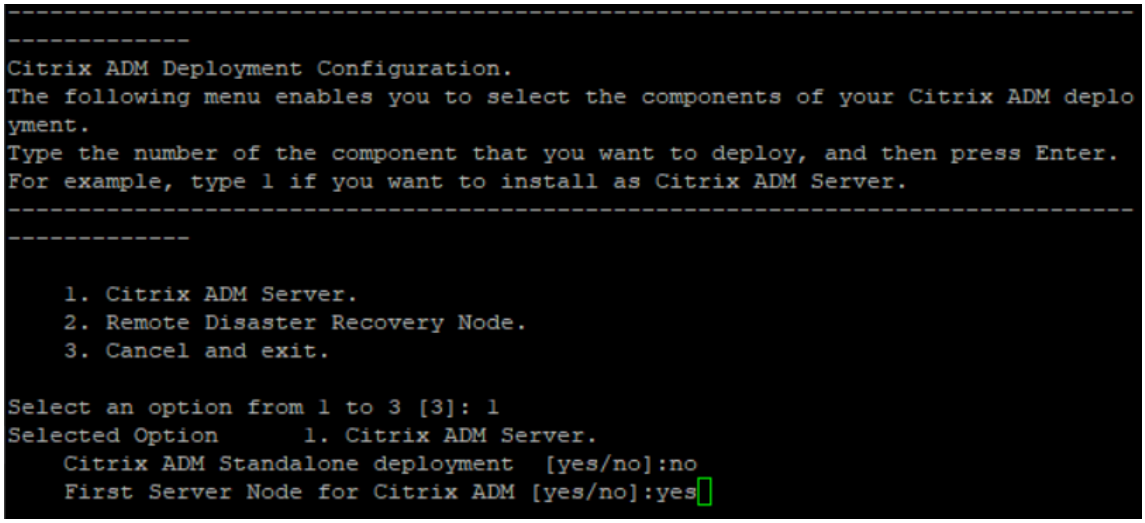
6. Seleccione **1** para registrar el servidor NetScaler ADM como nodo principal.



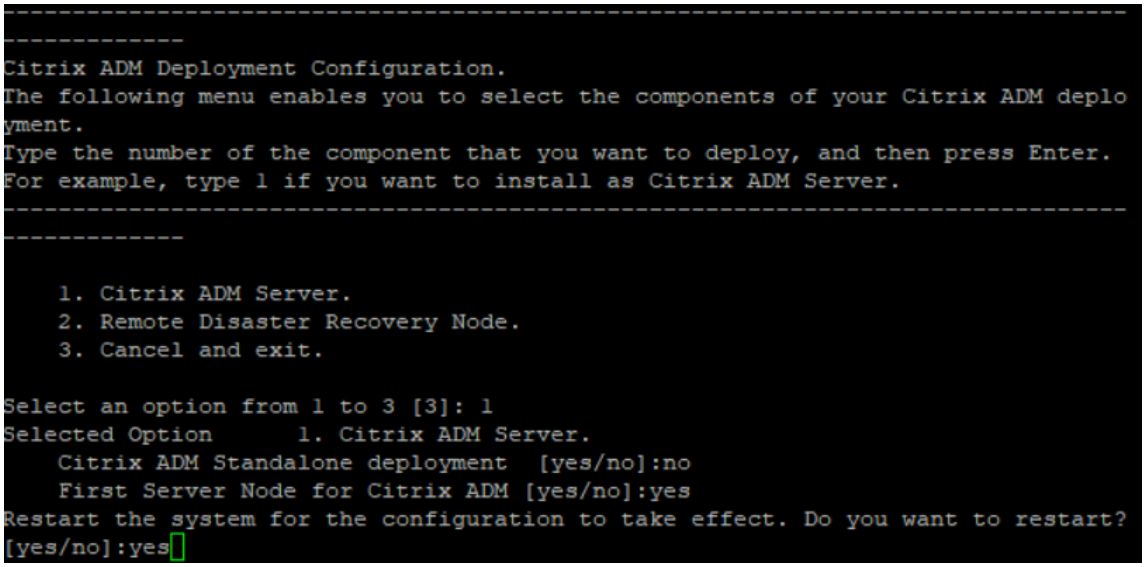
7. La consola le pide que seleccione la implementación independiente de NetScaler ADM. Introduzca**No** para confirmar la implementación como alta disponibilidad.



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.



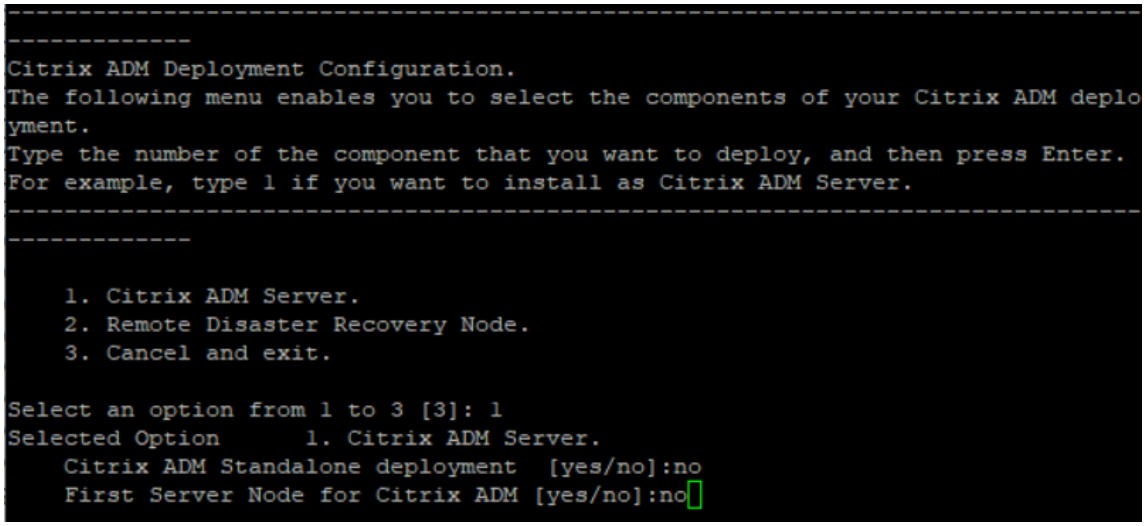
El sistema se reinicia y se muestra como nodo principal en la interfaz de usuario de NetScaler ADM.

Registrar e implementar el segundo servidor (nodo secundario)

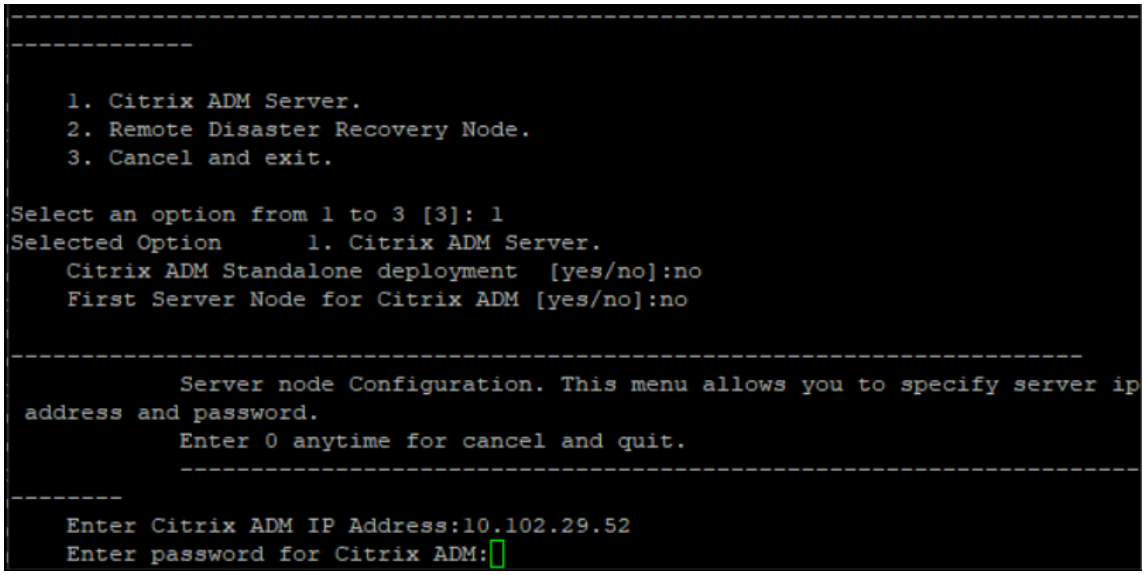
1. Utilice el archivo de **imagen.xva** descargado del sitio de NetScaler e impórtelo al hipervisor.
2. En la ficha **Consola**, configure NetScaler ADM con las configuraciones de red iniciales, tal como se muestra en la siguiente imagen.
3. Una vez completada la configuración inicial de la red, el sistema 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.

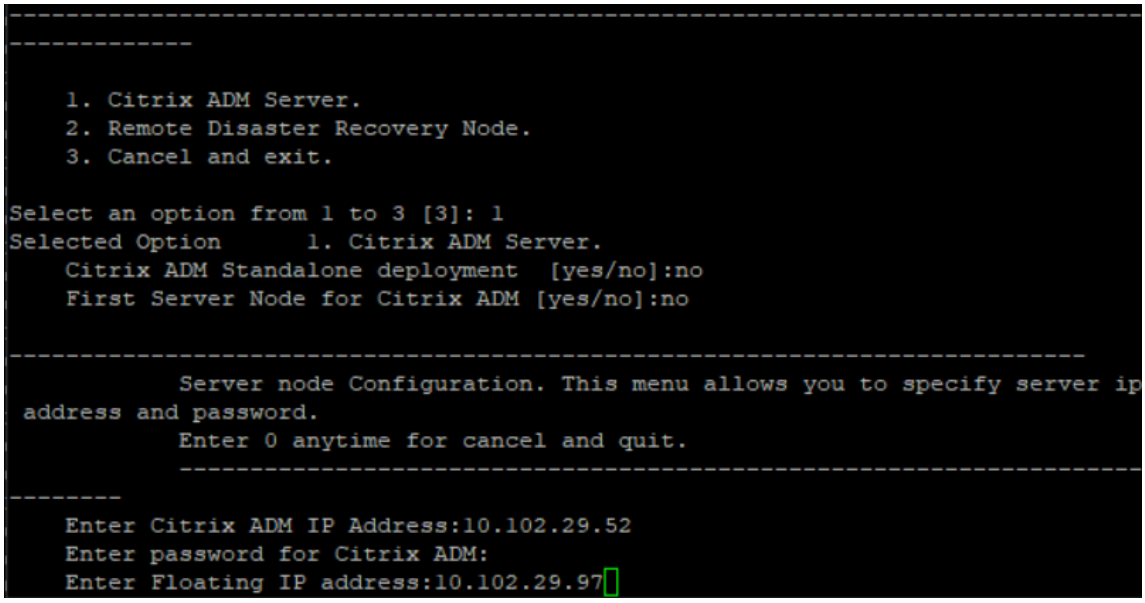
4. Para implementar el nodo secundario, escriba **/mps/deployment_type.py**. Aparece el menú de configuración de implementación de NetScaler ADM.
5. Seleccione **1** para registrar el servidor NetScaler ADM como nodo secundario.
6. La consola le pide que seleccione NetScaler ADM como implementación independiente. 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 NetScaler 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 NetScaler ADM.

Para implementar nodos como un par de alta disponibilidad:

1. Abra un navegador web e introduzca la dirección IP del primer nodo del servidor NetScaler 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**.

   NetScaler 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 NetScaler ADM con las credenciales de administrador, haga clic en **Comenzar** en la página principal y, si lo quiere, complete lo siguiente:

   a) Agregar instancias de NetScaler

   b) Configurar la identidad del cliente

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

8. Vaya a **Configuración > 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 NetScaler ADM y convertir los nodos en servidores NetScaler ADM independientes.

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

Para inhabilitar la alta disponibilidad:

1. En un navegador web, introduzca la dirección IP del nodo principal del servidor NetScaler 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

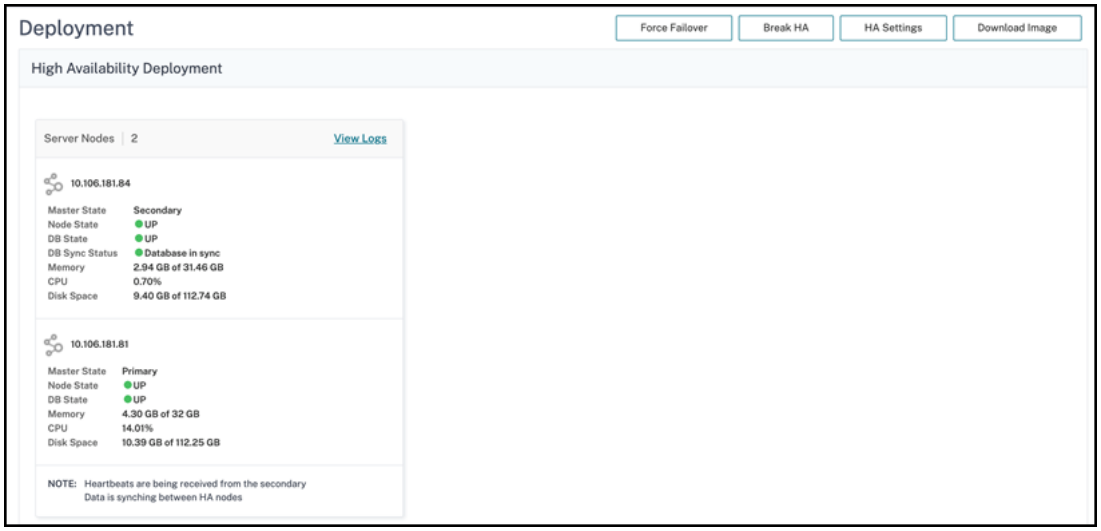
Se produce una conmutación por error si se da una de las siguientes condiciones:

- **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 NetScaler ADM está inactivo.

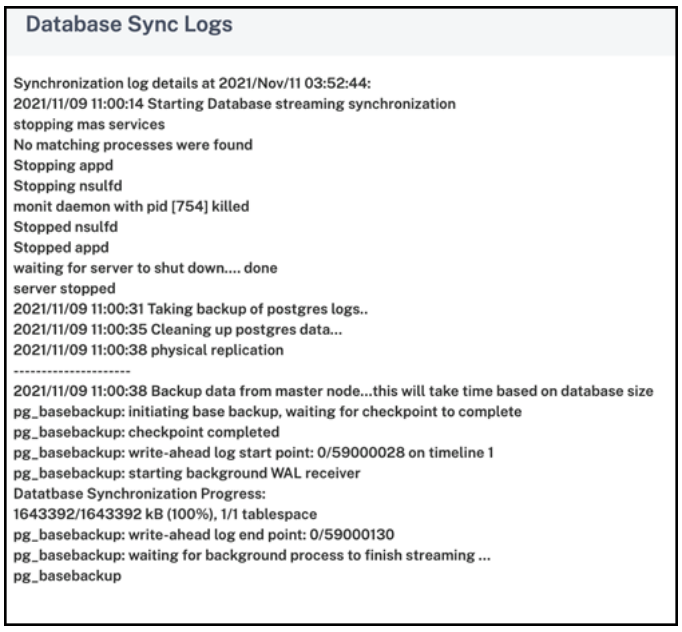
Ver mensajes del registro de sincronización de bases

En el par NetScaler ADM HA, los archivos de configuración se sincronizan automáticamente desde el nodo principal al nodo secundario y se produce la replicación de transmisión física de la base de datos.

Sin embargo, si se produce un error de replicación de transmisión, aparece el botón **Sincronizar base** de datos. Puede hacer clic en el botón **Sincronizar base** de datos para iniciar el proceso de sincronización de la base



Para ver el progreso de la sincronización de la base de datos, haga clic en **Ver registros**. Aparece el mensaje **Registros de sincronización de base** de datos y puede ver los detalles del progreso de la sincronización en tiempo real.



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 NetScaler ADM como principales y secundarios. Debido a un posible tiempo de inactividad del enlace de red, la comunicación entre los dos nodos ADM de NetScaler 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.

A partir de NetScaler ADM 12.1 o de una versión posterior, esta situación de cerebro dividido se gestiona correctamente una vez que se restablecen el enlace de red y los latidos 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 NetScaler ADM proporciona funciones completas de copia de seguridad y recuperación del sistema para NetScaler 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.

La siguiente tabla describe los términos utilizados al configurar la recuperación ante desastres en NetScaler ADM.

Términos y condiciones	Descripción
Sitio principal (centro de datos A)	El sitio principal tiene nodos NetScaler ADM implementados en modo de alta disponibilidad.

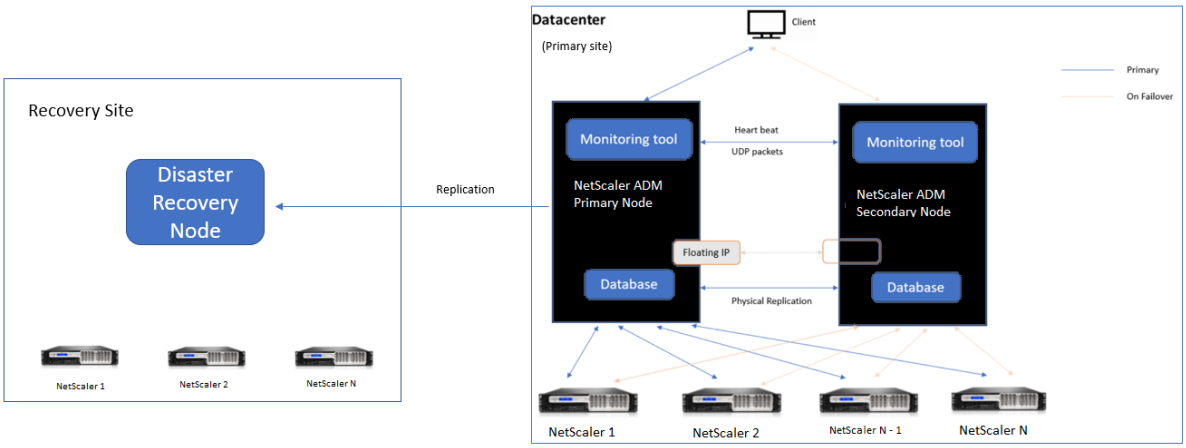
Términos y condiciones	Descripción
Sitio de recuperación (centro de datos B)	El sitio de recuperación tiene un nodo de recuperación ante desastres implementado en modo independiente. Este nodo está en modo de solo lectura y no estará operativo hasta que el sitio principal esté inactivo.
Nodo de recuperación ante desastres	El nodo de recuperación es un nodo independiente implementado en el sitio de recuperación. Este nodo se hace operativo (al nuevo primario) en caso de que se produzca un desastre en el sitio primario 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 NetScaler 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 NetScaler 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 NetScaler en el sitio de recuperación, pero no reciben tráfico 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 nodos NetScaler ADM configurados en modo de alta disponibilidad.
- La implementación independiente de NetScaler ADM en el sitio principal no admite la función de recuperación ante desastres.
- El par ADM HA de NetScaler (en el sitio principal) y el nodo independiente (en el sitio de DR) 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

Componente	Requisito
Espacio de almacenamiento	Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de NetScaler ADM. El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de NetScaler ADM. Si sus requisitos de almacenamiento de NetScaler ADM superan los 120 GB, debe conectar un disco adicional. **Nota** Solo puede agregar un disco más. Citrix recomienda estimar el almacenamiento y adjuntar más disco en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a NetScaler 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 NetScaler ADM en modo de alta disponibilidad
- Implementar y registrar el nodo de recuperación ante desastres de NetScaler ADM
- Habilitar y inhabilitar la configuración de recuperación ante desastres desde la interfaz de usuario

Implementar NetScaler ADM en modo de alta disponibilidad

Para configurar la configuración de recuperación ante desastres, asegúrese de que NetScaler ADM se implementa en modo de alta disponibilidad. Para obtener información sobre la implementación de NetScaler ADM en alta disponibilidad, consulteImplementación de alta disponibilidad

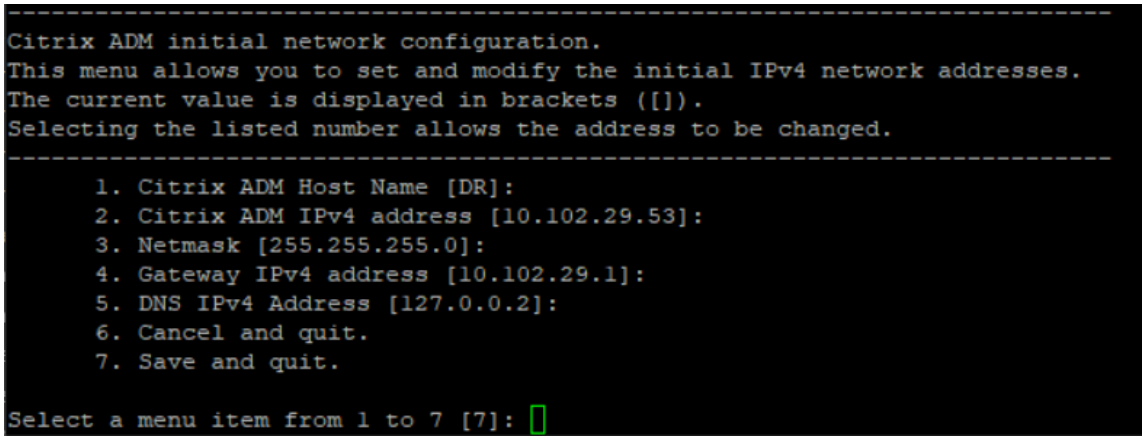
> **Nota**
>
> - NetScaler ADM implementado en modo de alta disponibilidad debe actualizarse a la versión 13.1 de NetScaler ADM.
> - **La dirección IP flotante es obligatoria** para registrar el nodo de recuperación ante desastres con el nodo principal.

Implemente y registre el nodo de recuperación ante desastres ADM de NetScaler mediante la consola DR

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

1. Descargue el archivo de imagen `.xva` del sitio de NetScaler e impórtelo a su hipervisor.
2. En la ficha **Consola**, configure NetScaler 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`.

   > **Importante** No cambie las credenciales del nodo DR (`nsrecover`/`nsroot`) durante el registro. Puede cambiar las credenciales del nodo DR después de registrar el nodo DR correctamente.

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 NetScaler ADM.


```
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]:
```

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

```
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]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

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.

```
------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    ------------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

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.
> - Una vez que el registro se ha realizado correctamente, las credenciales de administrador predeterminadas para iniciar sesión en el servidor son `nsroot`/`nsroot`.

8. Si quiere cambiar la contraseña del nodo DR, ejecute la siguiente script:

```
/mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Ejemplo:

```
/mps/change_freebsd_password.sh nsroot new_password
<!--NeedCopy-->
```

Implementar el nodo de recuperación ante desastres mediante la GUI de NetScaler ADM

Una vez que el nodo de recuperación ante desastres se haya registrado correctamente mediante la consola DR, implemente el nodo DR desde la GUI ADM de NetScaler. Este paso habilita la configuración de recuperación ante desastres desde el sitio principal de NetScaler ADM.

1. Vaya a **Sistema > Administración del sistema > Configuración de recuperación ante desastres.**
2. En la página de **recuperación ante desastres**, seleccione **Deploy DR Node**.
3. Se muestra un cuadro de diálogo de confirmación. Haga clic en **Sí** para continuar.

> **Nota**
>
> El tiempo necesario para la copia de seguridad del sistema depende del tamaño de los datos y de la velocidad del enlace WAN.

Tras implementar correctamente el nodo DR en la GUI ADM de NetScaler, puede supervisar el estado de la base de datos, la memoria, la CPU y el uso del disco del nodo DR.

Para inhabilitar la configuración de recuperación ante desastres, seleccione **Eliminar nodo de recuperación ante desastres**. Se muestra un cuadro de diálogo de confirmación. Haga clic en **Sí** para continuar.

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

1. Inicie sesión en el nodo DR mediante un Hypervisor o una consola SSH.
2. Configure el nodo de DR siguiendo el procedimiento disponible en Implementar y registrar el nodo de recuperación ante desastres de NetScaler ADM mediante la consola de DR.

3. Implemente el nodo de recuperación ante desastres mediante la GUI de NetScaler ADM.

Para obtener más información, consulte las preguntas frecuentes.

> **Importante**
>
> - Es responsabilidad del administrador detectar que se ha producido un desastre en el sitio principal.
> - El flujo de trabajo de recuperación ante desastres lo inicia manualmente el administrador después de que el sitio principal se apaga.
> - Un administrador debe iniciar manualmente el proceso ejecutando un script de recuperación en el nodo de recuperación ante desastres en el sitio de recuperación.
> - Si actualiza el par HA en el sitio primario, también debe actualizar manualmente el nodo independiente en el sitio DR.

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 uno de los siguientes scripts de recuperación en el nodo de recuperación ante desastres según su requisito (en el sitio de recuperación):

   - Configure SNMP, Syslog y Analytics en el nodo DR:

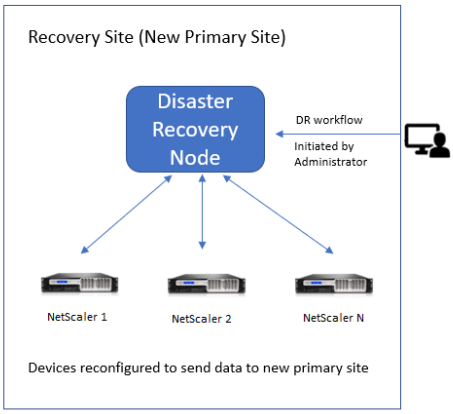
   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

   <!--NeedCopy-->
   ```

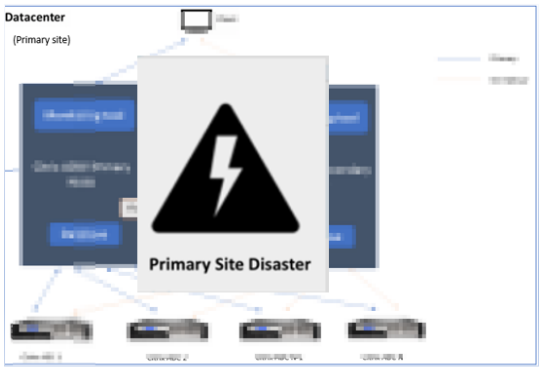
   - Configure también el nodo DR como servidor de licencias:

   ```
   /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
      ls <IP-address-of-the-primary-site>

   <!--NeedCopy-->
   ```

4. Internamente, las instancias NetScaler 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

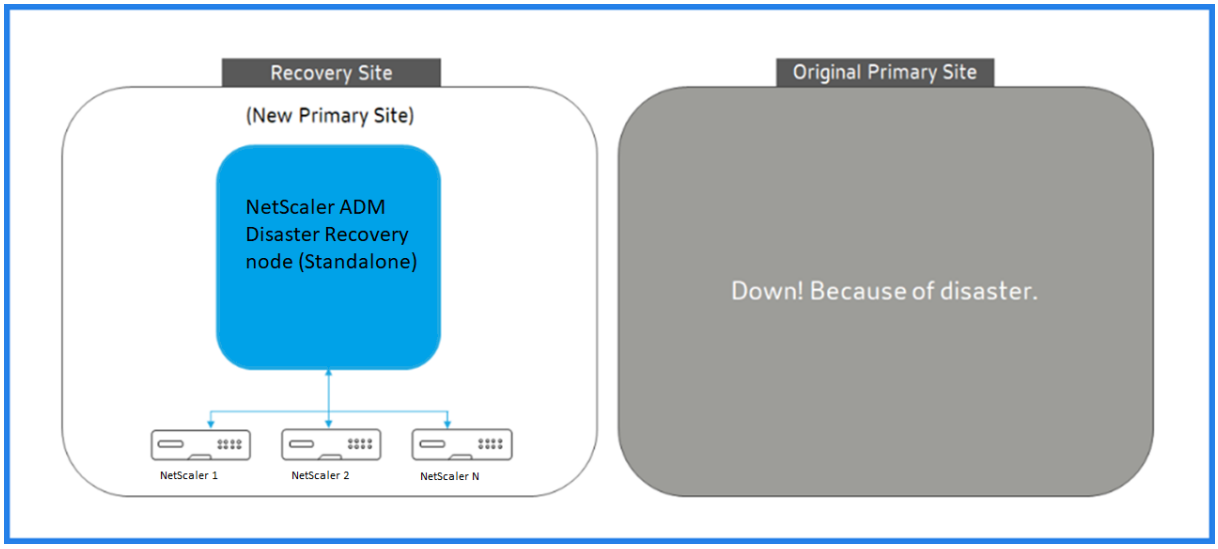
Una vez que se ha producido el desastre y el administrador inicia el script de recuperación, el sitio de recuperación ante desastres se convierte ahora en el nuevo sitio principal.

Si quiere revertir las configuraciones al sitio original más adelante, consulte Revertir configuraciones al sitio principal original.

> **Importante**
>
> - Si ha instalado NetScaler ADM 12.1.49.x o versiones anteriores, dispone de un período de gracia de 30 días para ponerse en contacto con Citrix y volver a alojar la licencia original en NetScaler ADM (en el sitio de DR).
> - Para las versiones 12.1.50.x o posteriores, la licencia ADM de NetScaler se sincroniza automáticamente con el sitio de DR (no es necesario ponerse en contacto con Citrix para obtener la licencia).
> - Si ha aplicado licencias agrupadas para las instancias, NetScaler con la versión **11.1 65.x o posterior**, **12.1 58.x o posterior**, **13.0 47.x o posterior** y **NetScaler SDX 13.0 76.x o posterior** admiten la actualización automática del servidor de licencias en el sitio de DR. En el resto de versiones, debe reconfigurar manualmente las instancias en el sitio de DR.

Revertir las configuraciones al sitio principal original

Tras un desastre, el nodo de recuperación ante desastres (DR) configurado se convierte en el nuevo sitio principal y el tráfico del cliente fluye a través de este nodo.



Para obtener más información, consulte Flujo de trabajo después del desastre.

Cuando el sitio primario original esté libre de desastres y decida mover todas las operaciones al sitio primario, vuelva a configurar el sitio primario original para que coincida con las configuraciones del nodo DR.

Antes de empezar, asegúrese de que tanto el sitio principal como el sitio de DR estén activos.

Para revertir los cambios en el sitio principal original desde el sitio de DR, lleve a cabo los siguientes pasos:

1. Inicie sesión en el sitio principal original y ejecute el siguiente comando:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
    password> -L <primary-node-password> &
<!--NeedCopy-->
```

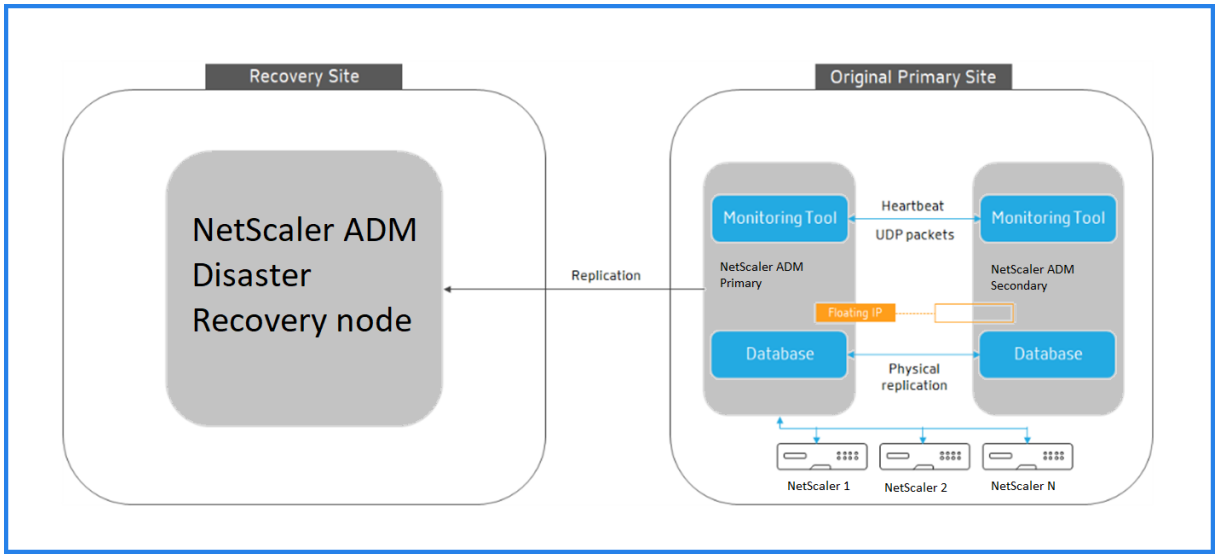
   Este comando configura solo Syslog, SNMP y Analytics en el sitio principal.

   Si quiere configurar el sitio principal como un servidor de licencias agrupado para instancias de ADC, ejecute el siguiente comando:

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
    password> -L <primary-node-password>  -O yes &
<!--NeedCopy-->
```

   El comando `-O` recupera la dirección IP del sitio DR y reconfigura el sitio primario como servidor de licencias agrupado.

2. Vuelva a configurar el sitio de recuperación ante desastres. Consulte Implementar la configuración de recuperación ante desastres.



Después de revertir correctamente las configuraciones del sitio de recuperación ante desastres al sitio principal original, el tráfico del cliente fluye a través del nodo principal de NetScaler ADM.

Configurar agentes en prem para la implementación en varios sitios

January 30, 2024

En las versiones anteriores de NetScaler ADM, las instancias de NetScaler implementadas en centros de datos remotos se pueden administrar y supervisar desde NetScaler ADM que se ejecuta en un centro de datos principal. Las instancias de NetScaler enviaron datos directamente al dispositivo principal de NetScaler ADM, lo que provocó el consumo de ancho de banda de la red WAN. Además, el procesamiento de datos de análisis utiliza recursos de CPU y memoria del dispositivo principal de NetScaler ADM.

Puede tener centros de datos ubicados en todo el mundo. Los agentes desempeñan un papel vital en los siguientes casos:

- Instalar agentes en centros de datos remotos para reducir el consumo de ancho de banda WAN.
- Limitar el número de instancias que envían tráfico directamente al NetScaler 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 NetScaler a NetScaler ADM principal.

> - Si ha instalado agentes para uno o más 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 uno o más centros de datos remotos. En este caso, la comunicación entre el sitio principal y uno o más centros de datos remotos se realiza a través de la dirección IP flotante.
> - El agente local de NetScaler ADM no admite licencias agrupadas.

Desde NetScaler ADM 12.1 o posterior, las instancias se pueden configurar con agentes para que se comuniquen con el NetScaler ADM principal ubicado en un centro de datos diferente.

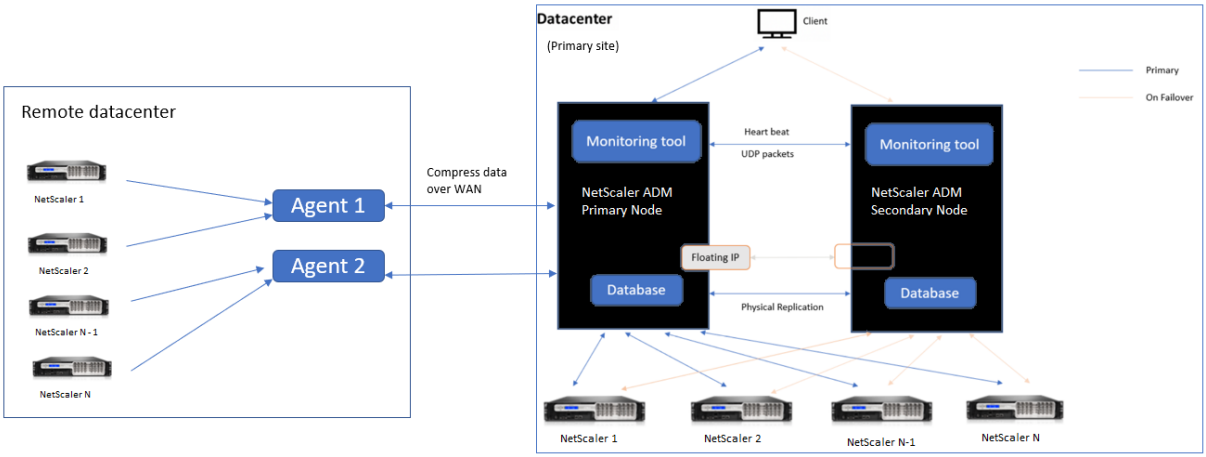
Los agentes funcionan como intermediarios entre la instancia principal de NetScaler ADM y las instancias descubiertas en diferentes centros de datos. Los siguientes son los beneficios de instalar agentes:

- 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 NetScaler ADM. Los agentes realizan el primer nivel de procesamiento de datos y envían los datos procesados en formato comprimido al NetScaler 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 NetScaler en caso de conmutación por error del agente. Cuando un agente de un sitio falla, el tráfico de las instancias de NetScaler 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.

Arquitectura

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



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

En el sitio secundario, los agentes se implementan y registran con el servidor NetScaler 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 NetScaler del sitio secundario se registran en el servidor NetScaler 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 NetScaler ADM. Los agentes procesan los datos recibidos de las instancias y los envían a la instancia principal de NetScaler ADM en un formato comprimido. Los agentes se comunican con el servidor de NetScaler 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
  - Adjuntar el agente a un sitio
- Agregar instancias de NetScaler
  - 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 NetScaler ADM y las instancias administradas de NetScaler 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 NetScaler 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	32 GB
CPU virtual	8 CPUs
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 NetScaler ADM on-prem.

Tipo	Puerto	Detalles	Dirección de comunicación
TCP	8443, 7443, 443	Para la comunicación saliente y entrante entre el agente y el servidor local de NetScaler ADM.	Agente de NetScaler ADM a NetScaler ADM

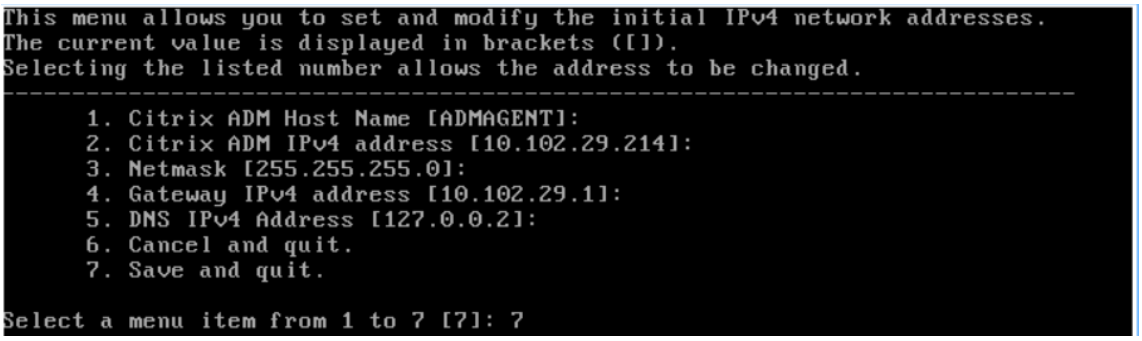
Los siguientes puertos deben estar abiertos entre el agente y las instancias de NetScaler.

Tipo	Puerto	Detalles	Dirección de comunicación
TCP	80	Para la comunicación NITRO entre el agente y la instancia de NetScaler.	NetScaler ADM a NetScaler y NetScaler a NetScaler ADM
TCP	22	Para la comunicación SSH entre el agente y la instancia de NetScaler. Para la sincronización entre los servidores NetScaler ADM implementados en modo de alta disponibilidad.	NetScaler ADM a NetScaler y agente de NetScaler ADM a NetScaler
UDP	4739	Para la comunicación de AppFlow entre el agente y la instancia de NetScaler.	NetScaler a NetScaler ADM
ICMP	Sin puerto reservado	Para detectar la accesibilidad de la red entre las instancias de NetScaler ADM y NetScaler, o el servidor NetScaler ADM secundario implementado en modo de alta disponibilidad.	
UDP	161, 162	Para recibir eventos SNMP desde la instancia de NetScaler al agente.	Puerto 161 - NetScaler ADM a NetScaler Puerto 162 - NetScaler a NetScaler ADM

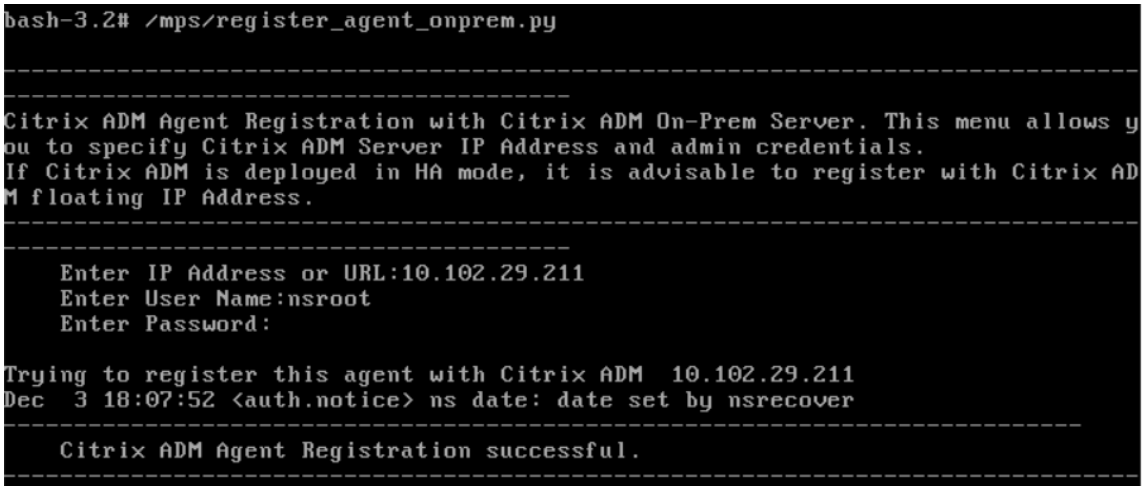
Tipo	Puerto	Detalles	Dirección de comunicación
UDP	514	Para recibir mensajes de syslog desde la instancia de NetScaler al agente.	NetScaler a NetScaler ADM
TCP	5557	Para la comunicación de Logstream entre el agente y las instancias de NetScaler.	NetScaler a NetScaler ADM

Registrar el agente

1. Utilice el archivo de imagen del agente descargado del sitio de NetScaler e impórtelo al hipervisor. El patrón de denominación del archivo de imagen del agente es el siguiente, **MASAGENT-<HYPERVISOR>-<n.º de versión>** Por ejemplo: **MASAGENT-XEN-13.0-xy.xva**
2. En la ficha **Consola**, configure NetScaler ADM con las configuraciones de red iniciales.
3. Introduzca el nombre de host de NetScaler 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, introduzca **/mps/register_agent_onprem.py**. Las credenciales de registro del agente NetScaler ADM se muestran como se muestra en la siguiente imagen.
6. Introduzca la dirección IP flotante NetScaler ADM y las credenciales de usuario.



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

Después de que el agente se reinicie, acceda a la GUI de NetScaler ADM, desde el menú principal, vaya a la página **Infraestructura > Instances > Agents** para verificar el estado del agente. El agente recién agregado se muestra en estado **activo**.

> **Nota**
>
> NetScaler 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 NetScaler ADM.

Adjuntar un agente a un 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 un sitio con el botón de signo 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 NetScaler asignadas se conmutan automáticamente a otros agentes en funcionamiento en el mismo sitio.

Acciones del agente

Puede aplicar varias acciones a un agente en **Infraestructura > Agentes > Seleccionar acciones**.

En **Seleccionar acción**, puede utilizar las siguientes funciones:

Instale un certificado nuevo: si necesita un certificado de agente diferente para cumplir con sus requisitos de seguridad, puede agregar uno.

Cambie la contraseña predeterminada: para garantizar la seguridad de su infraestructura, cambie la contraseña predeterminada de un agente.

Generar un archivo de soporte técnico: genere un archivo de soporte técnico para un agente de NetScaler ADM seleccionado. Puede descargar este archivo y enviarlo al soporte técnico de Citrix para su investigación y solución de problemas.

Agregar instancias de NetScaler

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

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Proxy de reenvío SSL de Citrix

Para obtener más información, consulte Agregar instancias a NetScaler ADM.

Adjuntar una instancia existente al agente

Si ya se ha agregado una instancia al dispositivo principal de NetScaler ADM, puede adjuntarla a un agente modificando un agente.

1. Vaya a **Infraestructura > Instancias** y seleccione el tipo de instancia. Por ejemplo, NetScaler.
2. Haga clic en **Modificar** para modificar una instancia existente.
3. Haga clic para seleccionar el agente.
4. En la página **Agente**, seleccione el agente con el 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

Después de agregar las instancias y configurar el agente, acceda a la GUI de una instancia para comprobar si el destino de la captura está configurado.

En NetScaler ADM, vaya a **Infraestructura**> Instancias. En **Instancias**, seleccione el tipo de instancia a la que quiere acceder (por ejemplo, NetScaler 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 NetScaler en centros de datos remotos, pero no es obligatorio.
>
> En caso de que desee agregar la instancia directamente al MAS principal, no seleccione **un agente** mientras agrega instancias.

Conmutación por error del agente de NetScaler ADM

La conmutación por error del agente puede producirse en un sitio que tiene dos o más agentes registrados. Cuando un agente pasa a estar inactivo (estado INACTIVO) en el sitio, NetScaler ADM redistribuye las instancias de ADC del agente inactivo con otros agentes activos.

> **Importante**
>
> - Asegúrese de que la función de **conmutación por error del agente** esté habilitada en su cuenta. Para habilitar esta función, consulte Habilitar o inhabilitar las funciones de ADM.
> - Si un agente está ejecutando un script, asegúrese de que el script está presente en todos los agentes del sitio. Por lo tanto, el agente modificado puede ejecutar el script después de la conmutación por error del agente.

Para adjuntar un sitio a un agente en la GUI de ADM, consulte Adjuntar un agente a un sitio.

Para lograr una conmutación por error del agente, seleccione agentes NetScaler ADM uno por uno y adjunte al mismo sitio.

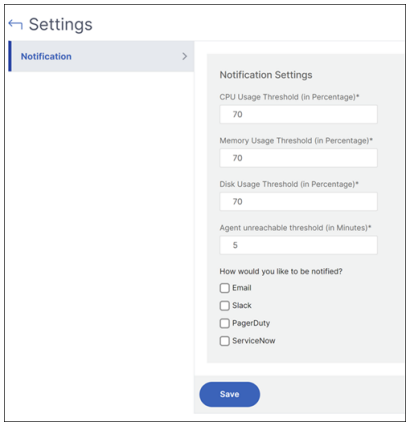
Por ejemplo, dos agentes 10.106.1xx.2x y 10.106.1xx.3x están conectados y operativos en el sitio de Bangalore. Si un agente queda inactivo, NetScaler ADM lo detecta y muestra el estado como inactivo.

Cuando un agente NetScaler ADM pasa a estar inactivo (estado Inactivo) en un sitio, NetScaler ADM espera cinco minutos a que el agente se active (estado Activo). Si el agente permanece inactivo, NetScaler ADM redistribuye automáticamente las instancias entre los agentes disponibles en el mismo sitio.

NetScaler ADM desencadena la redistribución de instancias cada 30 minutos para equilibrar la carga entre los agentes activos del sitio.

Configurar el umbral inalcanzable del agente y la notificación

Si un agente está inactivo o no se puede contactar durante un tiempo determinado, puede recibir una notificación sobre el estado del agente por correo electrónico, Slack, PagerDuty y ServiceNow. En **Infraestructura > Instancias > Agentes**, haga clic en **Configuración**, especifique la duración entre 5 minutos y 60 minutos y seleccione el método de notificación que quiere que se le notifique.



Instalar un agente ADM como microservicio en un clúster de Kubernetes

January 30, 2024

La implementación de un agente de NetScaler ADM como microservicio es útil para administrar NetScaler CPX. Los procedimientos disponibles en este documento solo son aplicables si el clúster de NetScaler ADM y Kubernetes están configurados en una red diferente. En este caso, puede configurar un agente ADM como un microservicio, donde se aloja el clúster de Kubernetes.

> Nota
>
> También puede configurar un agente local y registrarlo en la red, donde se aloja el clúster de Kubernetes.

Introducción

1. En NetScaler ADM, vaya a **Infraestructura > Instancias > Agentes**.
2. En la lista **Seleccionar acción**, seleccione la opción **Descargar microservicio del agente**.
3. En la página **Descargue Agent Microservicio**, especifique los siguientes parámetros:
   a) **ID de aplicación**: Un ID de cadena para definir el servicio para el agente en el clúster de Kubernetes y distinguir este agente de otros agentes del mismo clúster.
   b) **Contraseña**: Especifique una contraseña para que CPX utilice esta contraseña para incorporarla CPX a ADM a través del agente.
   c) **Confirmar contraseña**: Especifique la misma contraseña para la confirmación.

      > Nota
      >
      > No debe usar la contraseña predeterminada (`nsroot`).

   d) Haga clic en **Descargar archivo Yaml**.

Instalar el agente NetScaler ADM en el clúster de Kubernetes

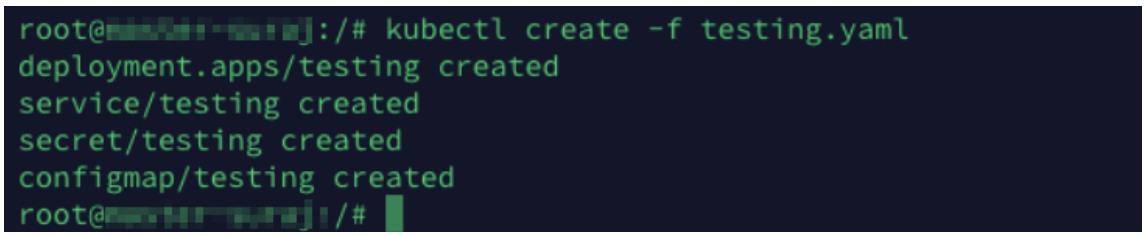
En el nodo principal de Kubernetes:

1. Guardar el archivo YAML descargado
2. Ejecute este comando:

   `kubectl create -f <yaml file>`

   Por ejemplo, `kubectl create -f testing.yaml`

   El agente se ha creado correctamente.



En NetScaler ADM, vaya a **Infraestructura > Instancias > Agentes** para ver el estado del agente.

Después de configurar el agente, puede agregar las instancias de NetScaler CPX y ver los análisis en Service Graph. Para obtener más información, consulte:

- Agregar instancias CPX de NetScaler a NetScaler ADM.
- Configuración del gráfico de servicio.

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

January 30, 2024

Puede actualizar su único servidor NetScaler ADM a una implementación de alta disponibilidad de dos servidores NetScaler ADM. Un par de servidores NetScaler 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 NetScaler 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 NetScaler ADM a un par de alta disponibilidad, debe aprovisionar un nuevo nodo de servidor NetScaler ADM, configurarlo como el segundo servidor único de NetScaler ADM e implementar ambos servidores NetScaler ADM como un par de alta disponibilidad.

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

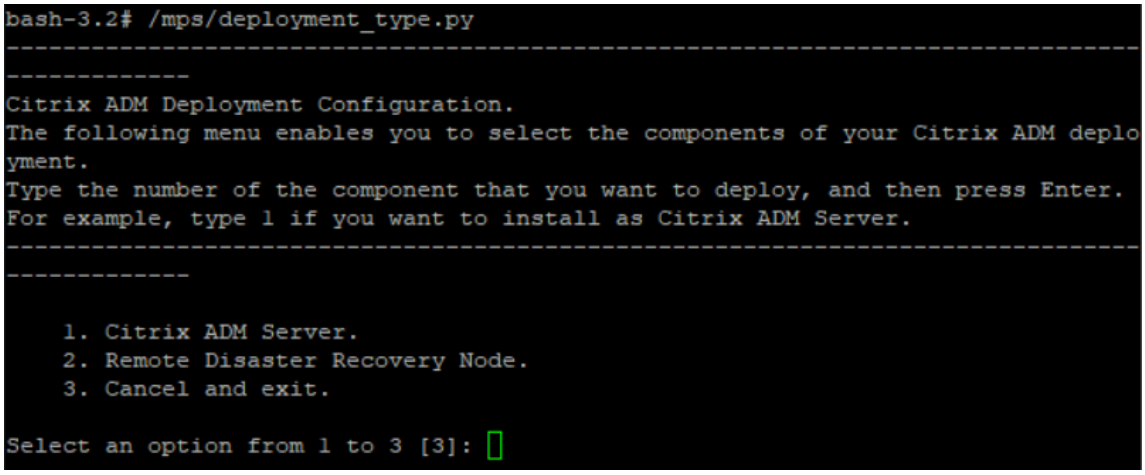
1. Modificación del nodo de servidor existente
2. Provisioning del segundo nodo del servidor
3. Implementación de los dos nodos en modo HA
4. Configuración del par de alta disponibilidad

Modificar el nodo de servidor NetScaler ADM existente

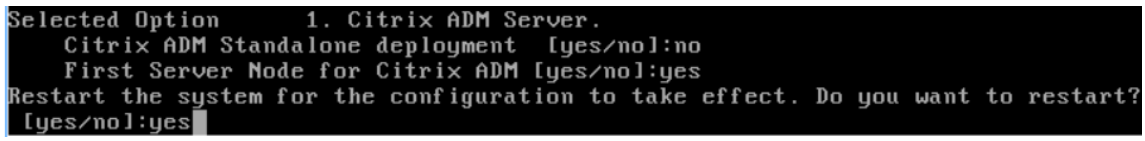
Para migrar el ADM de NetScaler del modo de servidor único al modo de alta disponibilidad, debe cambiar el tipo de implementación inicial del nodo del servidor al modo de alta disponibilidad.

1. En una estación de trabajo o portátil, abra la consola del nodo del servidor NetScaler ADM existente. Por ejemplo, considere que ha implementado un ADM de NetScaler con la dirección IP 10.106.171.17 como servidor independiente.

2. Inicie sesión en NetScaler ADM. Las credenciales predeterminadas son `nsroot` y `nsroot`.
3. En el símbolo del shell `/mps/deployment_type.py`, escriba y presione **Entrar**.
4. Seleccione el tipo de implementación como servidor NetScaler 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 del sitio de NetScaler.

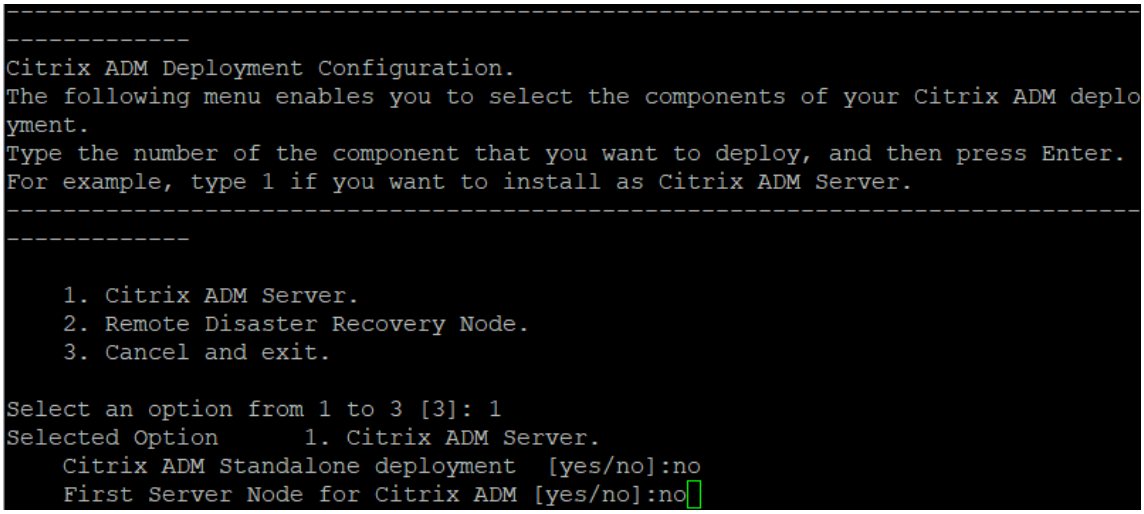
1. Importe el archivo de imagen al Hypervisor y, a continuación, desde la ficha Consola, configure las opciones de configuración de red iniciales como se explica en la siguiente pantalla:


```
--------------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------------
      1. Citrix ADM Host Name [CitrixADM]:
      2. Citrix ADM IPv4 address [10.102.29.211]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

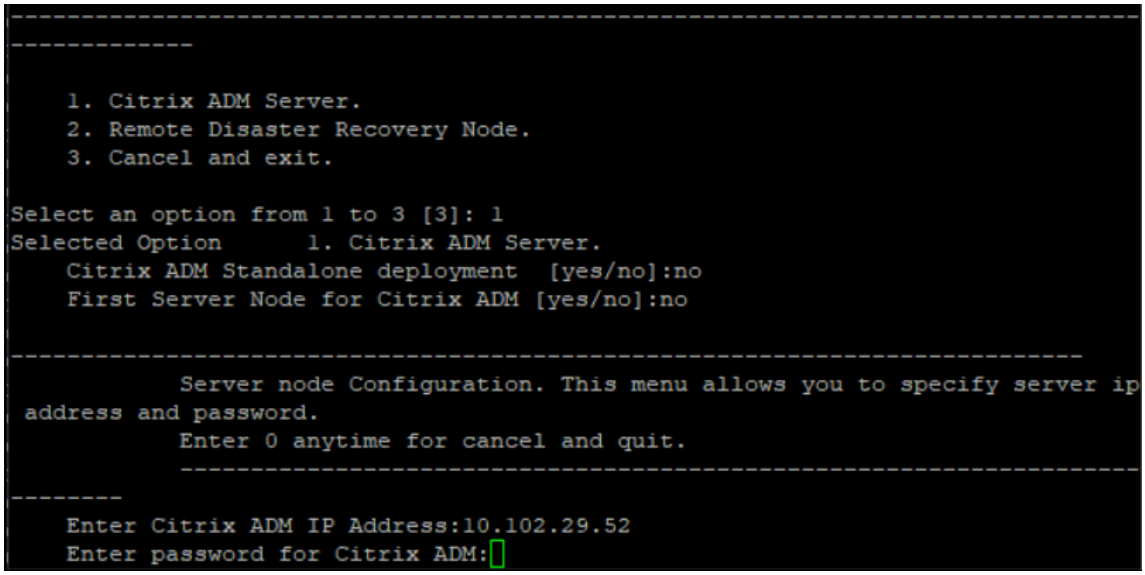
2. Tras especificar las direcciones IP necesarias, en la línea de comandos, escriba /mps/deployment_type.py y pulse enter.
3. Seleccione el tipo de implementación como servidor **NetScaler ADM.**
4. La consola de implementación le pide que seleccione la implementación del servidor (como independiente). 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
```

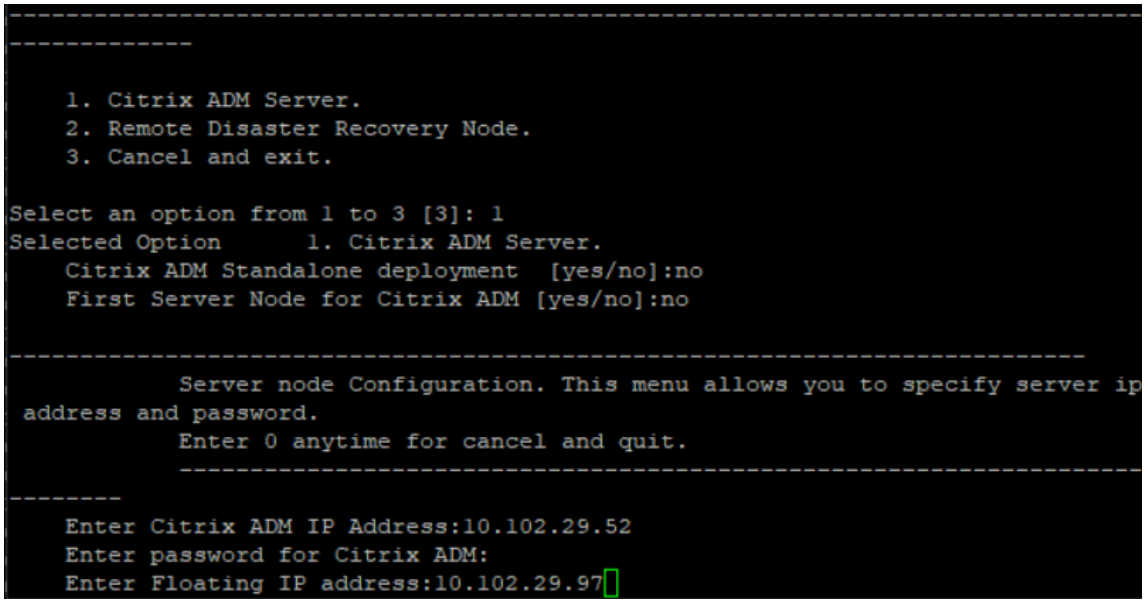
5. A continuación, la consola le pide que seleccione el (primer nodo del servidor). Escriba **No** para confirmar el nodo como el segundo nodo del servidor.



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

> **Importante**
>
> Antes de implementar nodos de alta disponibilidad, asegúrese de cambiar la contraseña predeterminada.

1. En un explorador web, escriba la dirección IP del nodo del servidor NetScaler 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**
>
> Tras implementar NetScaler ADM en alta disponibilidad, puede acceder al nodo principal o a la dirección 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**.

Migre de NetScaler Insight Center a 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 NetScaler ADM, no solo puede ver los diversos 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 NetScaler 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 NetScaler ADM 12.0 compilación 57.24 y, a continuación, actualizar a la versión más reciente de NetScaler ADM 13.1. Para obtener más información, consulte Actualizar.

- Ha descargado el archivo de imagen.tgz de compilación más reciente de NetScaler ADM 13.1.

Requisitos 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 NetScaler 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 símbolo del shell 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. Después de instalar NetScaler ADM 12.0 compilación 57.24, debe actualizar a la versión más reciente de NetScaler ADM 13.1 realizando los pasos anteriores.

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

> **Nota**
>
> En NetScaler ADM, de forma predeterminada, no hay ningún coste de licencia para administrar y supervisar dos servidores virtuales creados dentro de las instancias de NetScaler detectadas. Para supervisar y administrar más de dos servidores virtuales, instale las licencias NetScaler ADM necesarias. Para obtener más información, consulteLicencias de NetScaler 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 NetScaler 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 NetScaler ADM.
Interfaces de red virtual	1
Rendimiento	1 Gbps o 100 Mbps

Requerimientos mínimos

Antes de configurar la integración de red, asegúrese de crear un usuario de RBAC con acceso a HDX Insights.

Requisitos 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 NetScaler ADM son compatibles con la versión 7.0 y posteriores de Citrix VDA
- Citrix Workspace es compatible con Citrix Virtual Apps and Desktops versión 7.0 y posterior
- Asegúrese de que MAC, Citrix Workspace para Mac (versión 11.8 y posteriores) y Windows Citrix Workspace para Windows 14.0 y posteriores estén disponibles para mostrar métricas de RTT de ICA 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.

- La sesión ICA Round Trip Time (RTT) muestra los datos correctamente para Citrix Workspace para Windows 3.4 o posterior y para Citrix Workspace para Mac 11.8 o posterior. En las versiones anteriores de estos espacios de trabajo, 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, consultehttps://docs.citrix.com/en-us/citrix-virtual-apps-desktops/director/install-and-configure/hdx-insight.html.
> - Para obtener más información sobre HDX Insight, consultehttp://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

Conecte 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 sus datos, puede conectar un disco adicional.

> **Nota:**
>
> - Calcule los requisitos de almacenamiento y adjunte un disco adicional al servidor.
> - 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 NetScaler ADM, debe adjuntar un disco adicional a cada nodo. El tamaño de ambos discos debe ser el mismo.
> - Si existe un disco externo de menor capacidad, debe quitarlo antes de conectar uno nuevo.
> - Se recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de NetScaler ADM.

En este documento se explican los siguientes casos acerca de adjuntar un disco nuevo adicional, crear particiones y cambiar el tamaño de los discos adicionales:

1. Conecte un disco adicional en un NetScaler ADM independiente
2. Inicie la herramienta de partición de disco
3. Crear particiones en el nuevo disco adicional
4. Cambiar el tamaño de las particiones en el disco adicional existente
5. Elimine las particiones en el disco adicional

Conecte un disco adicional en un NetScaler ADM independiente

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

Inicie la herramienta de partición de disco

NetScaler ADM ahora proporciona la **herramienta de partición de disco NetScaler ADM**, una nueva herramienta de línea de comandos.

1. Con la herramienta, puede crear particiones en el disco adicional recién agregado.
2. También puede cambiar el tamaño de los discos adicionales existentes con la herramienta. Pero el disco externo existente no debe ser mayor que 2 terabytes.

   > **Nota:**
   >
   > - Cambiar el tamaño de los discos existentes a más de 2 terabytes puede provocar la pérdida de datos. Esto se debe a una limitación conocida en 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 ADM de NetScaler. No puede crear particiones en el disco principal (predeterminado) con esta herramienta.

Para iniciar la herramienta de partición de disco:

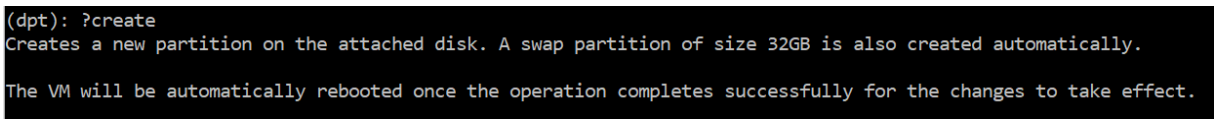
1. Abra una conexión SSH a NetScaler ADM mediante un cliente SSH, como PuTTY.
2. Inicie sesión en NetScaler ADM con las credenciales `nsrecover`/`nsroot`.
3. Cambie al símbolo del shell y escriba:

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

> **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".

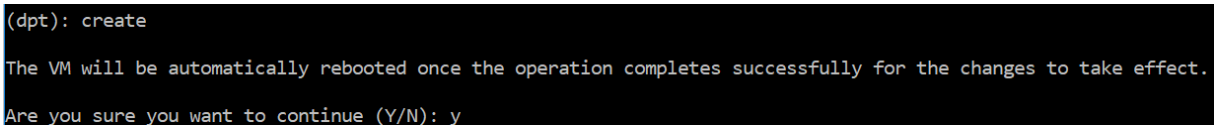


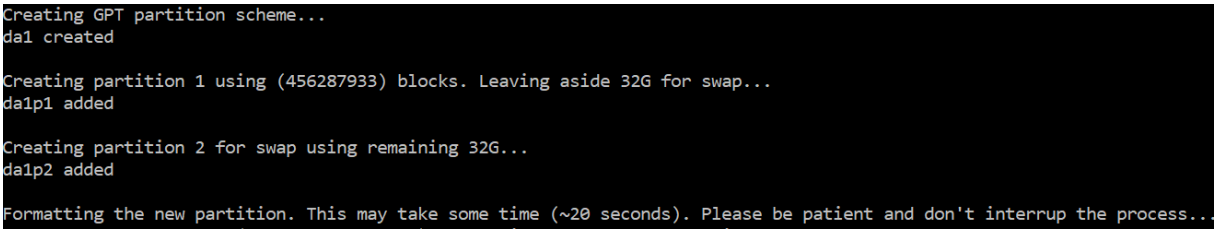
> **Nota:**
>
> No hay un límite de tamaño de 2 terabytes al crear particiones con la herramienta de partición de disco. La herramienta puede crear particiones de más de 2 terabytes. Al particionar el disco, se agrega automáticamente una partición de intercambio de 32 GB de tamaño. A continuación,

> la partición principal utiliza todo el espacio restante en el disco.

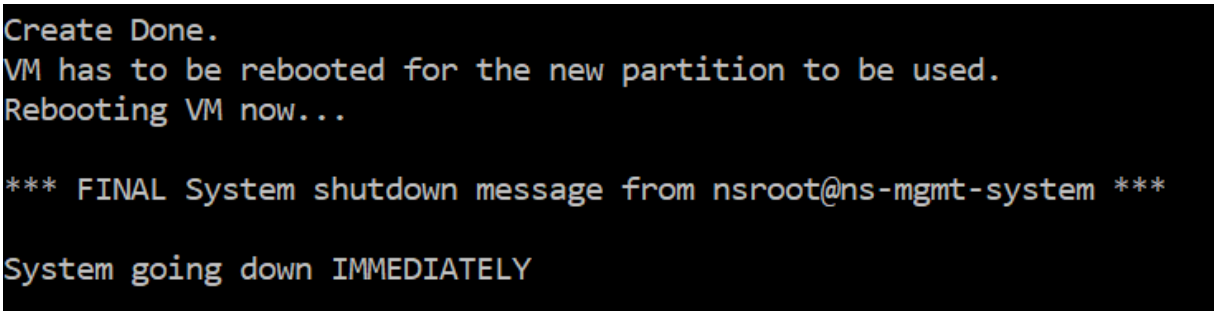
Una vez ejecutado el comando, se crea un esquema de particiones de tabla de particiones GUID (GPT). También se crean una partición de intercambio de 32 GB y una partición de datos para utilizar el resto del espacio. A continuación, se crea un nuevo sistema de archivos en la partición principal.

> **Nota:**
>
> Este proceso puede tardar unos segundos y no debe interrumpirlo.

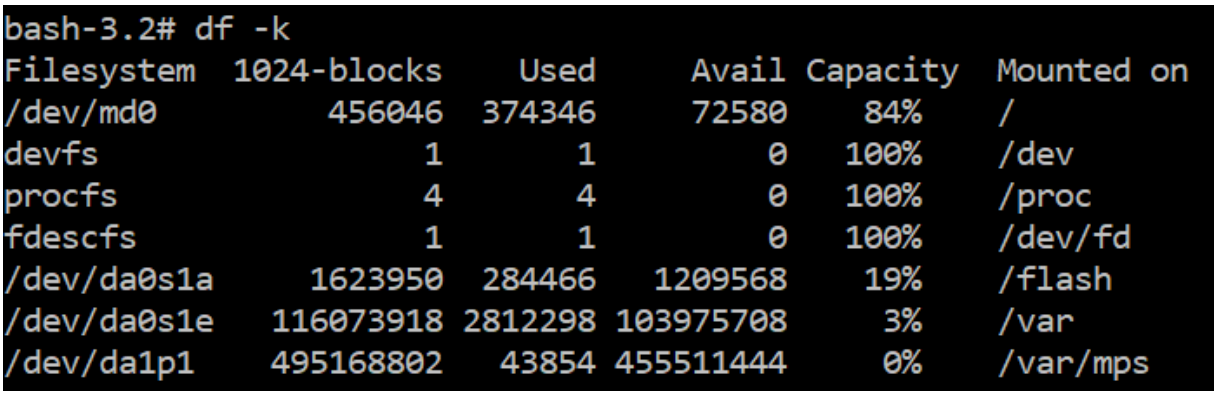




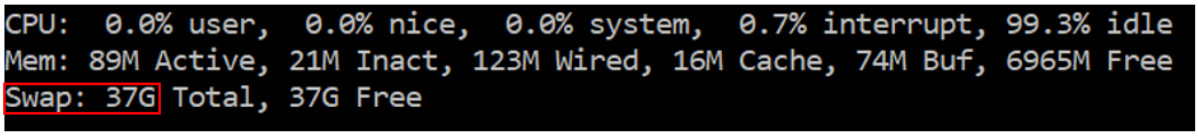
Una vez que se completa el comando create, la máquina virtual se reinicia automáticamente para que la nueva partición se monte.



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



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

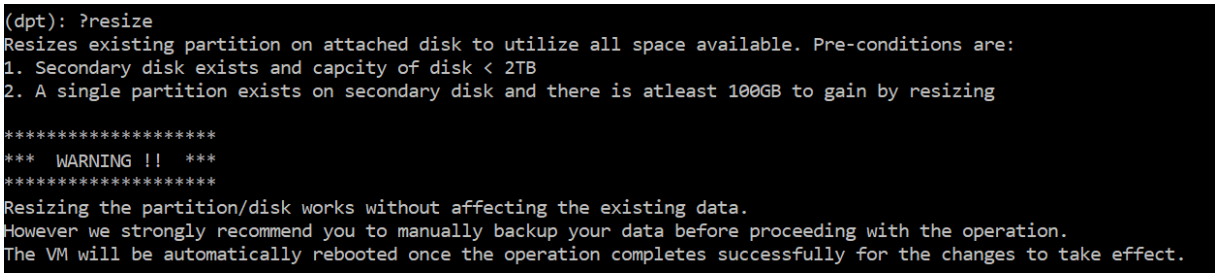


> **Nota:**
>
> La herramienta reinicia la máquina virtual después de crear la partición.

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 esquema `master boot record` (`MBR`) o GPT. El tamaño del disco debe ser inferior a 2 terabytes.

> **Nota:**
>
> - El comando `resize` está diseñado para funcionar sin perder ningún dato existente. Sin embargo, le recomendamos que haga una copia de seguridad de los datos críticos de este disco en un almacenamiento externo antes de 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 al cambiar el tamaño de las particiones. Un aumento gradual de este tipo garantiza que no tendrá que cambiar el tamaño con más frecuencia.



El comando `resize` comprueba todas las condiciones previas y procede si se cumplen todas las condiciones previas y después de que usted haya dado su consentimiento para cambiar el tamaño. Detiene los procesos que acceden al disco, que incluyen los subsistemas de 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 «crecimiento del sistema de archivos» puede tardar un poco en completarse y tenga cuidado de no interrumpirlo mientras esté 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`. Estos son los detalles del antes y el después de aumentar la talla:

```
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. Este problema 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.
```

Al ejecutar el comando «remove», se le pide confirmación y, una vez confirmado, detiene todos los procesos (como los subsistemas de ADM, los procesos de PostgreSQL y los monitores de 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...
```

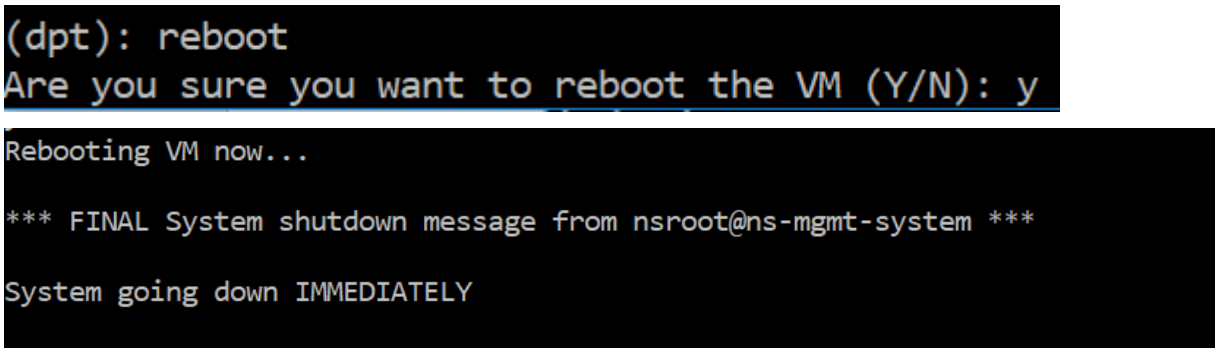
> **Nota:**
>
> La herramienta reinicia la máquina virtual después de eliminar la partición.

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 pedirá confirmación y, tras la confirmación, se detendrán todos los procesos (como los subsistemas de ADM, los procesos de PostgreSQL y los monitores de ADM). A continuación, se reinicia la máquina virtual.



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

> **Nota:**
>
> La creación de un archivo de respaldo requiere espacio en disco. Asegúrese de que haya suficiente espacio en disco (50% o más) antes de ejecutar los comandos de respaldo.

Para hacer una copia de seguridad de los datos de NetScaler ADM antes de cambiar el tamaño de las particiones o eliminarlas:

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 según el tamaño de los datos de los que se va a hacer una copia de seguridad.

5. Genera una suma de verificación.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--NeedCopy-->
```

6. Copie los archivos tarball y de suma de comprobación en un servidor remoto.
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.

```
cd /var/mps/
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:

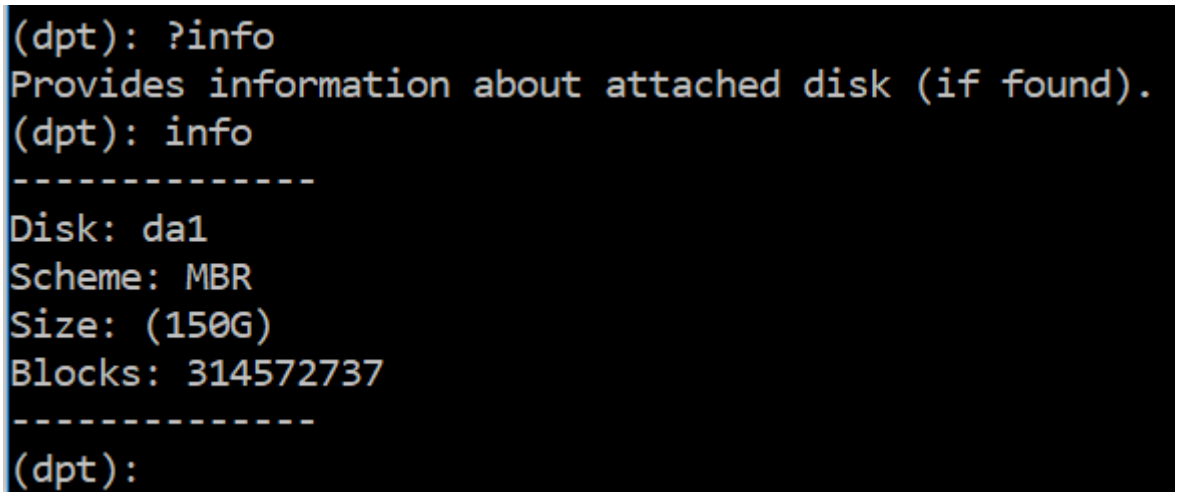
Para enumerar los comandos admitidos, escriba **help** o **?** y presione Entrar. Para obtener más ayuda sobre cada uno de los comandos, pulse **ayuda** o **?** seguido del nombre del comando y pulse la tecla **Enter**.

```
(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 particiones GPT significa que el disco se particionó con NetScaler ADM 12.1 o una versión 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. Este problema es una limitación conocida de la plataforma.



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. Se utiliza una partición de intercambio 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 dis-

eñado para discos secundarios creados con versiones anteriores de NetScaler 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

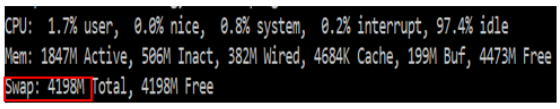
El comando `create_swapfile` es útil solo cuando la memoria es mayor o igual a 16 GB y no cuando la memoria es baja. Por lo tanto, este comando también comprueba la memoria antes de continuar con la creación del archivo de intercambio.

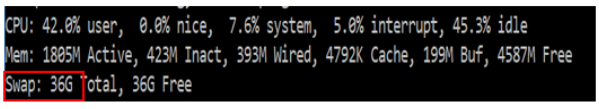
```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

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 da su consentimiento para 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

Tenga en cuenta que ha configurado un par de servidores NetScaler ADM en una configuración de alta disponibilidad sin discos secundarios. Además, tenga en cuenta que ha agregado 2 o más instancias de NetScaler, ha comprobado y comprobado que todos los procesos están en ejecución. 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. Apague el nodo secundario.
2. Agregue un disco a través del hipervisor.

   > **Nota:**
   >
   > Asegúrese de no extender el disco principal del nodo secundario.

3. Inicie el nodo secundario.
4. Ejecute la herramienta de particiones en el nodo secundario.
5. Después de agregar el disco, se reinicia el nodo secundario.
6. Apague el nodo secundario después de que se reinicie.
7. Cierre el nodo principal.
8. Agregue un disco a través del hipervisor.

   > **Nota:**
   >
   > Asegúrese de no extender el disco principal del nodo principal.

9. Inicie el nodo principal.
10. Ejecute la herramienta de partición en el nodo principal.
11. Después de agregar el disco, se reinicia el nodo principal.
12. Una vez que el nodo principal esté en funcionamiento, inicie el nodo secundario.
13. Asegúrese de que el nodo secundario esté en funcionamiento y de que las bases de datos estén sincronizadas.
14. Confirme que todos los datos aún existen.

Para aumentar la capacidad de RAM en ambos nodos:

1. Cierre ADM_Secondary y aumente el tamaño de RAM según sea necesario. No reinicies 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. Una vez reiniciado el ADM_Primary, compruebe si es el nodo principal.
5. Inicie el nodo ADM_Secondary. Cuando se reinicie, asegúrese de que aparezca como secundario y de que la sincronización de la base de datos funcione.
6. Confirme que todos los datos aún existen.

   > **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.

Cloud Connector ADM On-Prem

January 30, 2024

Puede usar la función ADM On-Prem Cloud Connector para establecer una conexión entre ADM On-Prem y el servicio NetScaler Console.

> **Nota:**
>
> El servicio NetScaler ADM ahora pasa a llamarse servicio NetScaler Console. La interfaz de usuario y la documentación de nuestro producto se están actualizando actualmente para reflejar estos cambios. Durante este tiempo, es posible que encuentre que los nombres más antiguos y más nuevos se hacen referencia indistintamente. Le agradecemos su comprensión durante esta transición.

Esta conectividad le permite seleccionar la siguiente función para utilizarla en ADM On-Prem:

Asesoramiento de seguridad: el asesoramiento de seguridad permite la identificación automática de NetScaler vulnerable y proporciona beneficios en el flujo de trabajo de remediación. El asesoramiento de seguridad le permite realizar un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE), evaluar el impacto de las CVE, comprender las soluciones y resolver las vulnerabilidades. Como administrador, puede supervisar las instancias de NetScaler en busca de nuevos CVE mediante un análisis periódico o un análisis manual, y tomar las medidas necesarias para solucionarlo. Para obtener más información, consulte Aviso de seguridad.

Recopilaciónautomatizada de telemetría : si utiliza licencias Flexed, le recomendamos que habilite Cloud Connector, que es el modo automatizado de recopilación de datos de telemetría. Para obtener más información, consulte Licencia de capacidad flexible.

> **Notas:**
>
> - No necesita agregar ni migrar las instancias de NetScaler al servicio NetScaler Console.
> - ADM On-Prem Cloud Connector requiere que se conecte al servicio NetScaler Console mediante la configuración de una cuenta de servicio de NetScaler Console (si aún no se ha creado).
> - A partir de la versión 14.1 8.x, ADM On-Prem Cloud Connector reemplaza la función de identidad del cliente.
> - Tras configurar ADM On-Prem Cloud Connector, permitirá a Citrix Cloud recopilar datos de licencia, configuración y uso para cumplir con las licencias y administrar, medir y mejorar el servicio. Para obtener más información, consulte Gobierno de datos.

Requisitos previos

Antes de configurar ADM On-Prem Cloud Connector, asegúrese de cumplir los siguientes requisitos previos:

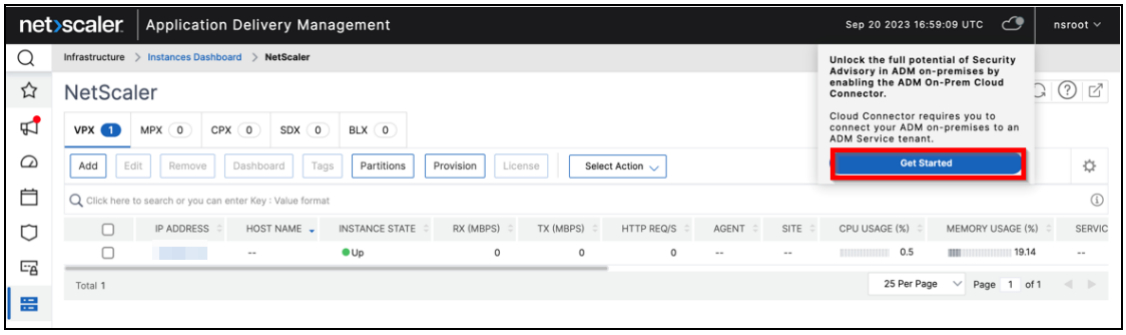
- Asegúrese de tener conexión a Internet o de tener un servidor proxy configurado en ADM on-prem para la accesibilidad de Citrix Cloud.
- Asegúrese de que se permita el acceso a las siguientes URL de puntos de conexión:
  - Servicio de descarga:
    `https://download.citrixnetworkapi.net`
  - Servicio de confianza:
    `*.citrixnetworkapi.net`
  - URL de servicios
    - `*.agent.adm.cloud.com`
    - `*.adm.cloud.com`
    - `adm.cloud.com`
  - Conectividad con Citrix Cloud:
    - `Citrix.cloud.com`
    - `Accounts.cloud.com`

- Asegúrese de haber desactivado el bloqueador de ventanas emergentes en el navegador desde el que accede a la GUI local de ADM.

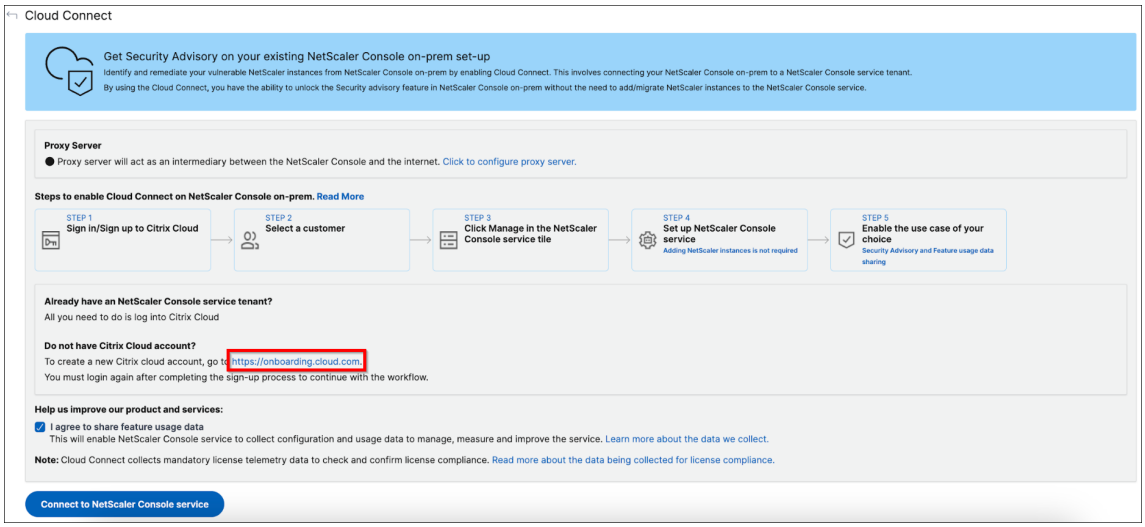
Configuración del ADM On-Prem Cloud Connector

Flujo de trabajo 1: si es un usuario nuevo sin una cuenta de Citrix Cloud ni un inquilino del servicio NetScaler Console

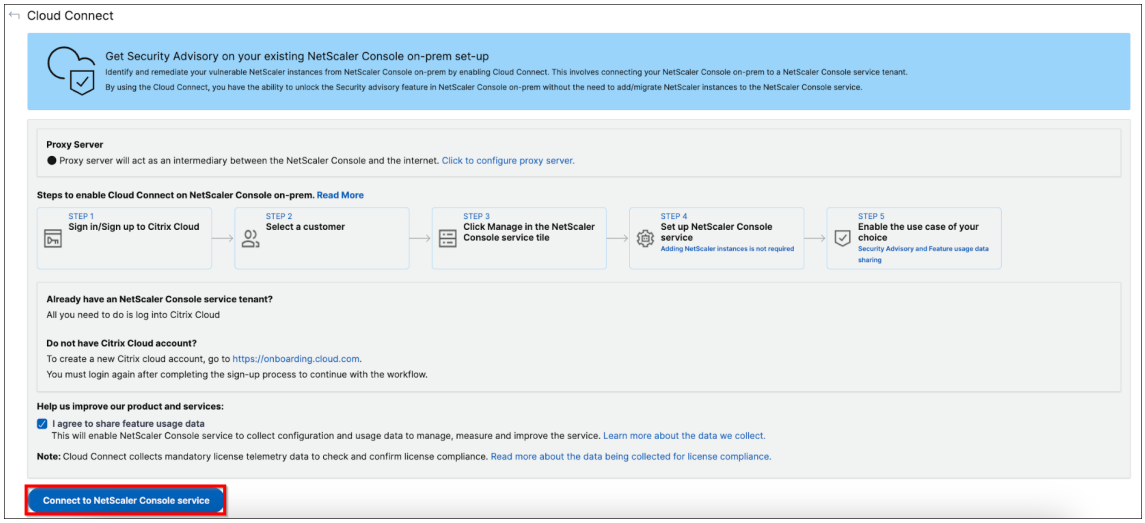
1. En NetScaler ADM, haga clic en el icono de la **nube** > **Comenzar**.



2. En la página de configuración de ADM On-Prem Cloud Connector, haga clic en el enlace. `https://onboarding.cloud.com`

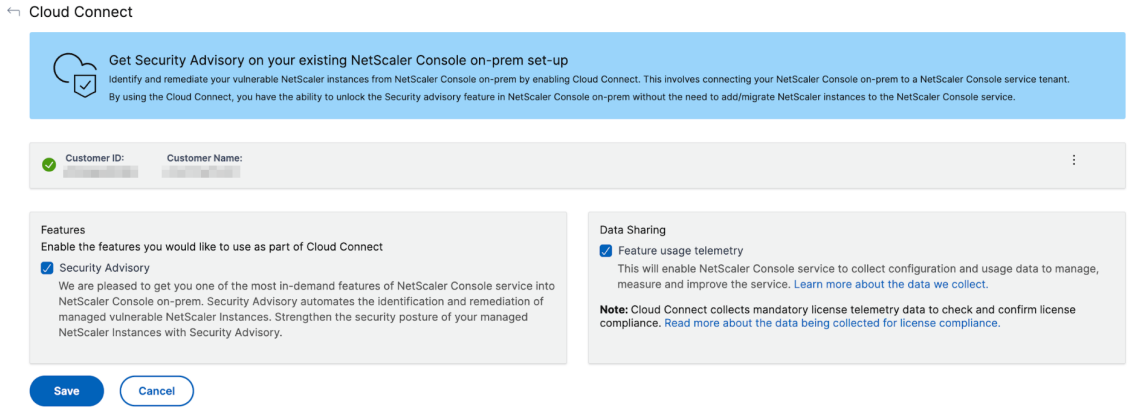


3. Siga el procedimiento de este documento para crear una cuenta de Citrix Cloud.
4. Tras crear una cuenta de Citrix Cloud, debe volver a iniciar sesión haciendo clic en **Conectar al servicio NetScaler Console** en NetScaler ADM. Tras iniciar sesión correctamente, la página redirige a los pasos de creación de arrendatarios del servicio de NetScaler Console.

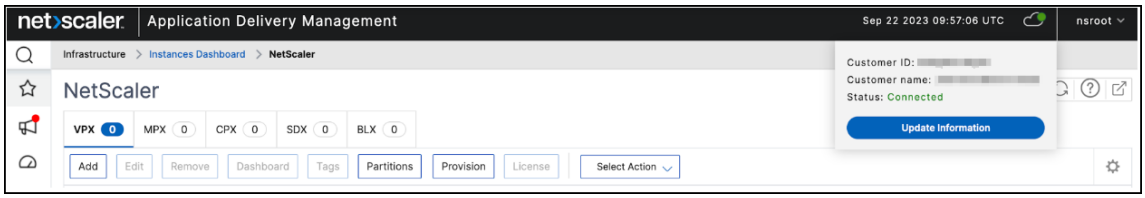


5. Seleccione una región que se adapte a las necesidades de su empresa y haga clic en **Listo**.
6. Seleccione un rol y finalice la configuración.

   La configuración puede tardar unos minutos en completarse. En ADM, puede ver la pantalla de **activación del conector ADM On-Prem Cloud en curso**. Puede hacer clic en **Actualizar** y esperar hasta que aparezca la página de configuración actualizada o hacer clic en **Cancelar** para omitir esta pantalla y buscar más adelante la página de configuración actualizada.
7. La configuración del ADM On-Prem Cloud Connector está completa. Puede continuar para habilitar el aviso de seguridad desde la página de configuración de ADM On-Prem Cloud Connector.
8. Seleccione **Aviso de seguridad** y haga clic en **Guardar**.

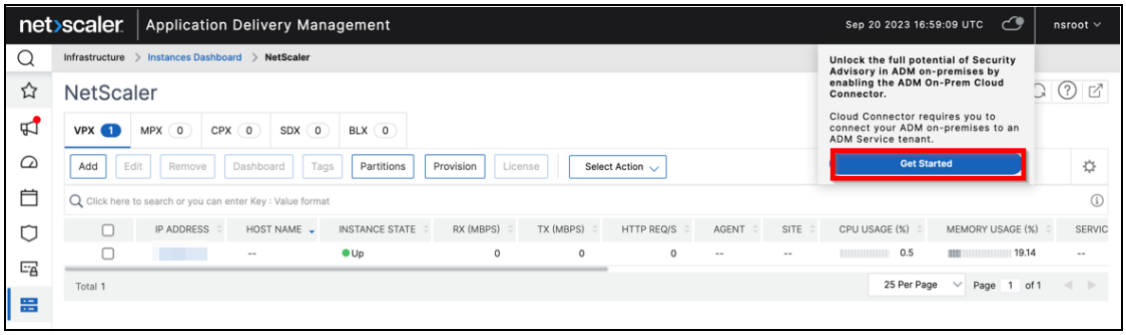


Puede ver el estado como conectado.

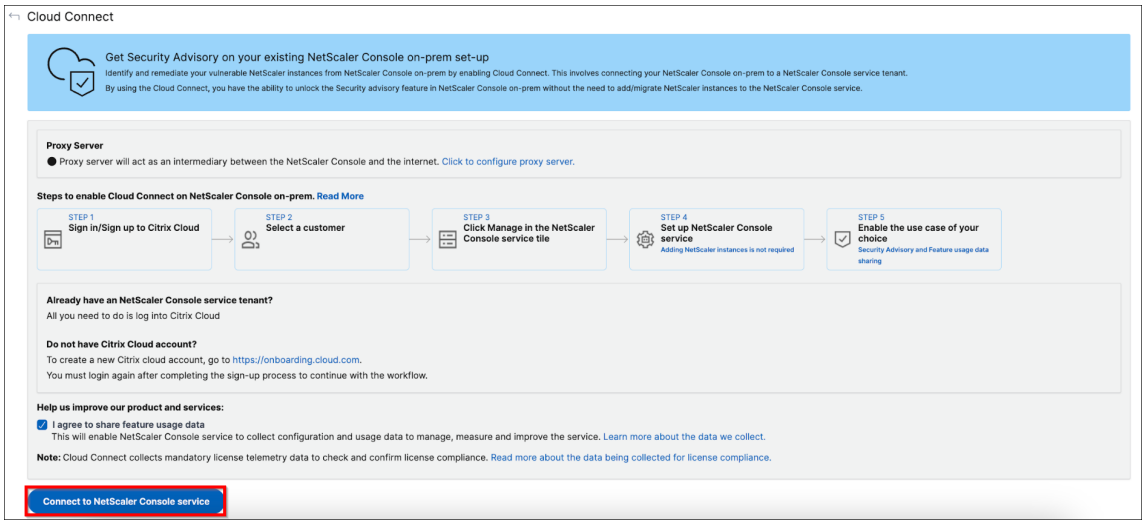


Flujo de trabajo 2: si tiene una cuenta de Citrix Cloud pero no tiene un inquilino del servicio NetScaler Console

1. En NetScaler ADM, haga clic en el icono de la **nube** > **Comenzar**.



2. Haga clic en **Conectarse al servicio NetScaler Console**.

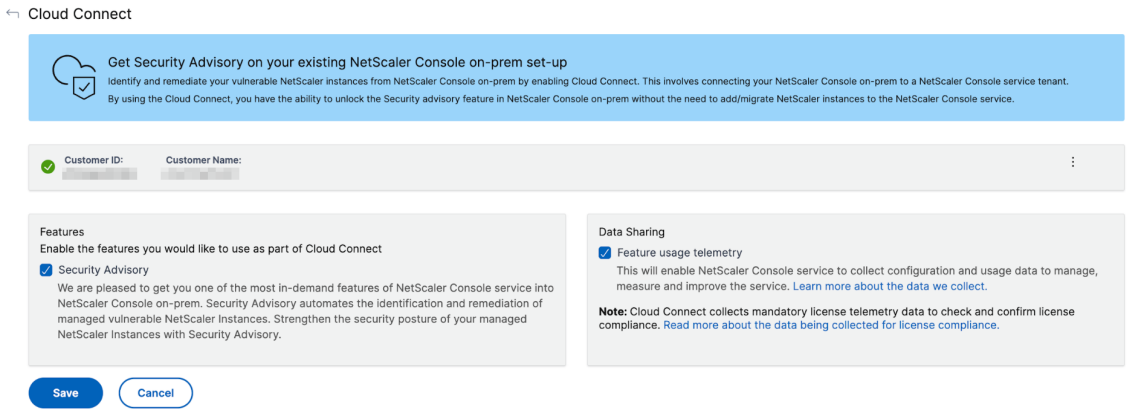


3. Se le redirigirá a una nueva ficha. Inicie sesión en Citrix Cloud.
4. Una vez que reciba el mensaje de inicio de sesión correcto, la página redirigirá a los pasos de incorporación de ADM.
5. Seleccione una región que se adapte a las necesidades de su empresa y haga clic en Listo.
6. Seleccione un rol y finalice la configuración.

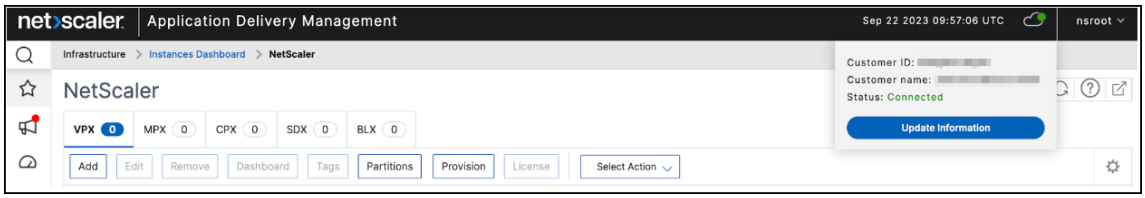
   La configuración puede tardar unos minutos en completarse. En ADM, puede ver la pantalla de **activación del conector ADM On-Prem Cloud en curso**. Puede hacer clic en **Actualizar** y esperar hasta que aparezca la página de configuración actualizada o hacer clic en **Cancelar** para omitir esta pantalla y buscar más adelante la página de configuración actualizada.

7. La configuración del ADM On-Prem Cloud Connector está completa. Puede continuar para habilitar el aviso de seguridad desde la página de configuración de ADM On-Prem Cloud Connector.

8. Seleccione **Aviso de seguridad** y haga clic en **Guardar**.

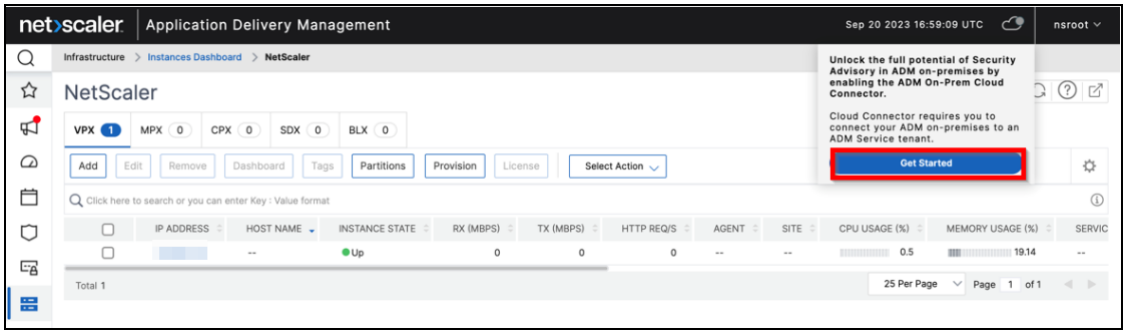


Puede ver el estado como conectado.

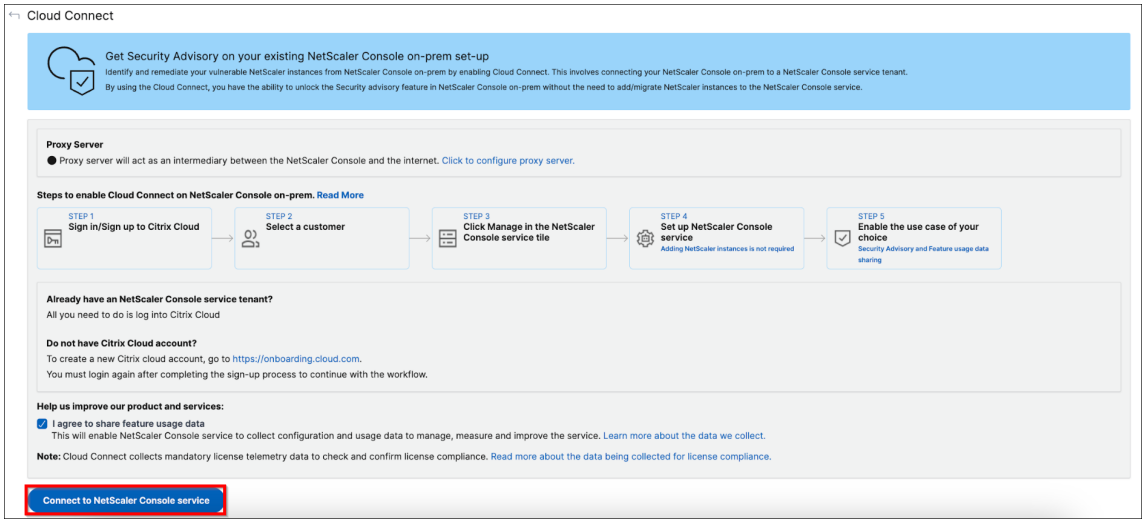


Flujo de trabajo 3: si ya es usuario y tiene una cuenta de Citrix Cloud y un inquilino del servicio NetScaler Console

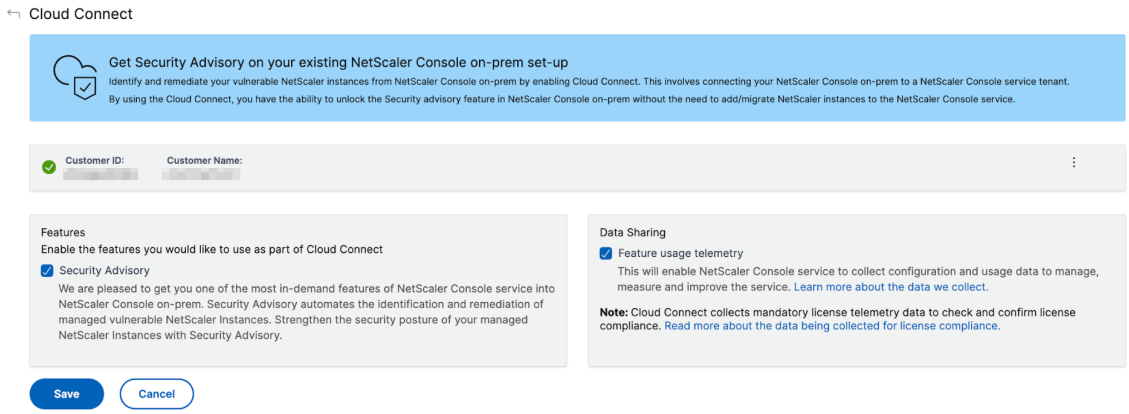
1. En NetScaler ADM, haga clic en el icono de la **nube** > **Comenzar**.



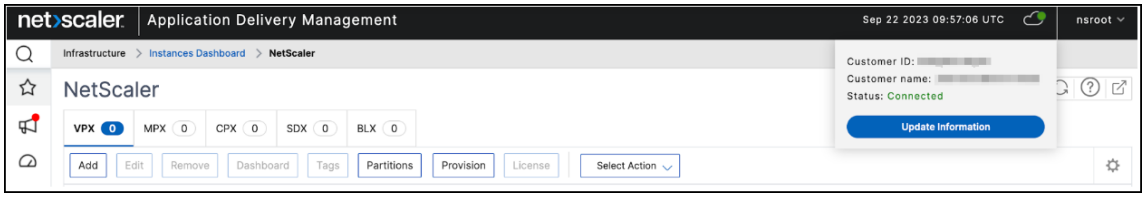
2. Haga clic en **Conectarse al servicio NetScaler Console**.



3. Se le redirigirá a una nueva ficha. Inicie sesión en Citrix Cloud y seleccione un arrendatario. Después de seleccionar el arrendatario, recibirá un mensaje de inicio de sesión correcto.
4. La configuración del ADM On-Prem Cloud Connector está completa. Puede continuar para habilitar el aviso de seguridad desde la página de configuración de ADM On-Prem Cloud Connector.
5. Seleccione **Aviso de seguridad** y haga clic en **Guardar**.



Puede ver el estado como conectado.



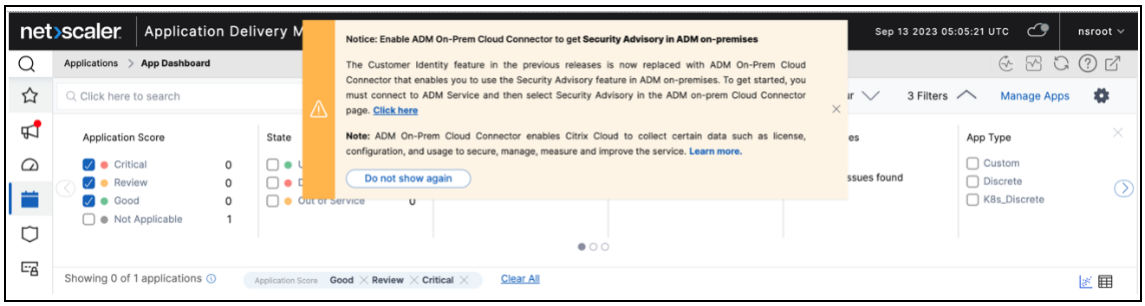
¿Qué sucede si la identidad del cliente ya está habilitada?

Si ya es un usuario de una versión anterior con Customer Identity habilitada, ha seleccionado el intercambio de datos y ha actualizado a la versión más reciente (14.1 8.x), se aplican los siguientes esce-

narios:

- Si tiene un inquilino del servicio de NetScaler Console, ADM On-Prem Cloud Connector se habilita automáticamente en su ADM local. Permitirá a Citrix Cloud recopilar datos de licencia, configuración y uso para gestionar, medir y mejorar el servicio. Para obtener más información, consulte Gobierno de datos. En la página de configuración de Cloud Connector, puede seleccionar **Security Advisory** para usar la función.

  La siguiente notificación aparece si ADM On-Prem Cloud Connector se configura automáticamente en el ADM de NetScaler.

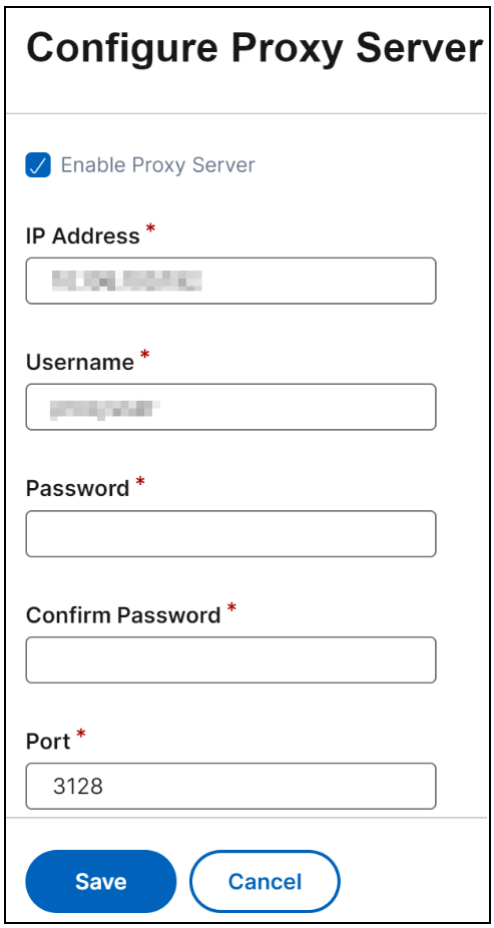


- Si no tiene un inquilino de servicio de NetScaler Console o el uso compartido de datos no está habilitado como parte de la identidad del cliente, el ADM On-Prem Cloud Connector no se habilita automáticamente y debe configurar Cloud Connector manualmente. Tras la configuración, permitirá a Citrix Cloud recopilar datos de licencia, configuración y uso para gestionar, medir y mejorar el servicio. Obtenga más información sobre la recopilación de datos.

Otras opciones

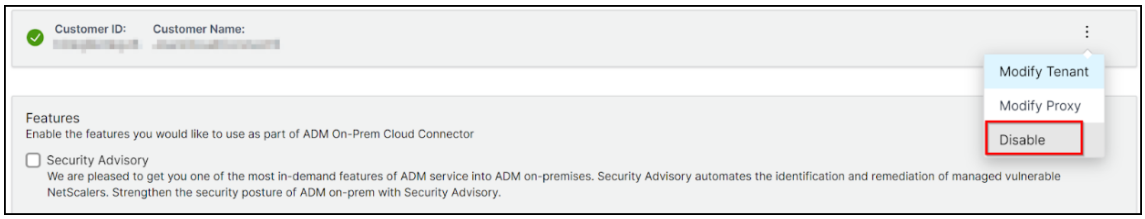
Tras activar ADM On-Prem Cloud Connector, puede utilizar las siguientes opciones:

- **Modificar arrendatario**: le permite cambiar el arrendatario existente. Al hacer clic en **Modificar arrendatario**, se le redirigirá a una nueva ficha y deberá iniciar sesión en Citrix Cloud. Después de iniciar sesión correctamente, puede seleccionar un arrendatario diferente.
- **Modificar proxy**: le permite configurar los ajustes del proxy en ADM on-prem. Esto es necesario cuando NetScaler ADM no tiene acceso directo a Internet a través de la red de administración. Haga clic en **Modificar proxy** de la lista, actualice los detalles y, a continuación, haga clic en **Guardar**.



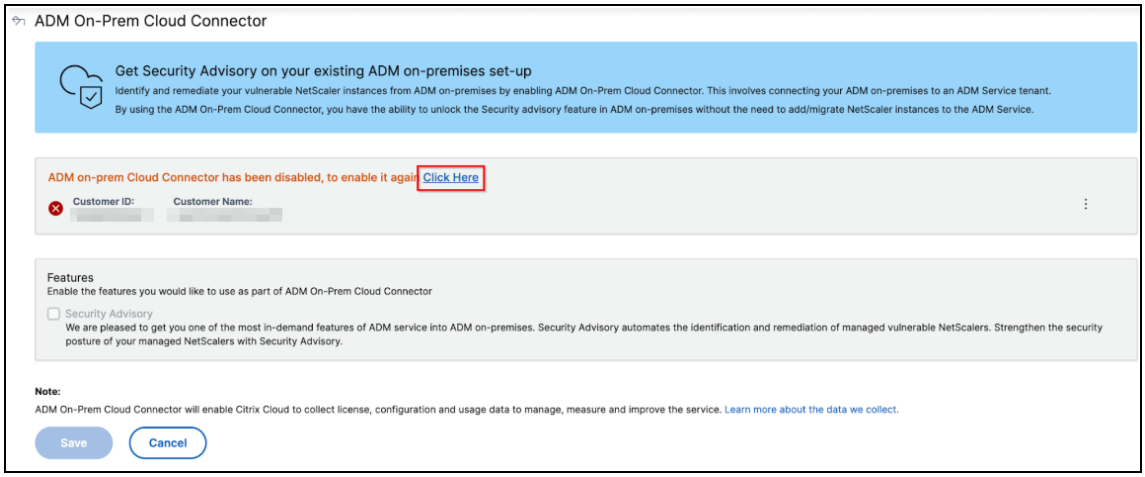
- **Desactivar**: desactiva la función ADM On-Prem Cloud Connector. Si decide inhabilitarla, la recopilación de métricas de datos estará inhabilitada y no podrá usar la versión completa del aviso de seguridad.

  Para inhabilitarlo, haga clic en **Desactivar** en la lista.



  Aparece un mensaje de confirmación. Haga clic en **Sí** para inhabilitarlo.

  Puede volver a activar ADM On-Prem Cloud Connector más adelante sin necesidad de realizar ningún paso adicional.



Desactivar el aviso de seguridad

En la página de configuración del ADM On-Prem Cloud Connector, también puede desactivar la casilla de verificación **Aviso de seguridad para inhabilitar la función de asesoramiento** de seguridad. Las métricas de datos aún se recopilan.

Configuración

January 30, 2024

Puede acceder a un servidor NetScaler ADM únicamente mediante la GUI. Debe acceder a la GUI para agregar instancias, administrar y supervisar sus instancias y aplicaciones, ver análisis y configurar el servidor NetScaler 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.

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

Para acceder a la GUI de NetScaler ADM:

Inicie sesión en NetScaler ADM con las credenciales de administrador.

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

- Agregue instancias a NetScaler ADM. Debe agregar instancias al servidor NetScaler ADM si desea 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 Network Time Protocol (NTP) en NetScaler 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 NetScaler ADM para administrar y supervisar sus instancias y aplicaciones, se recomienda configurar algunos ajustes del sistema para garantizar un rendimiento óptimo de su servidor NetScaler ADM.

Agregar instancias a NetScaler ADM

January 30, 2024

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

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

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

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

Cómo crear un perfil NetScaler

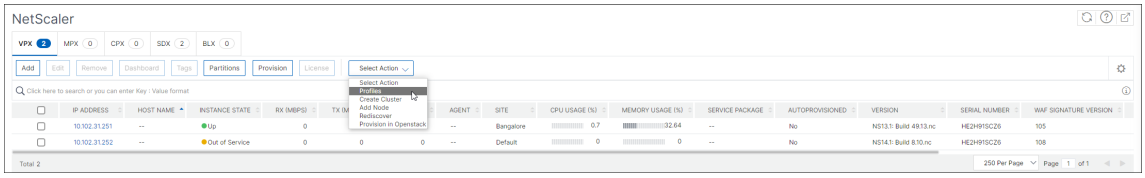
El perfil de NetScaler incluye las credenciales, los puertos y los tipos de autenticación para agregar instancias a NetScaler ADM. Para cada tipo de instancia, está disponible un perfil predeterminado. Por ejemplo, `nsroot` es el perfil predeterminado para las instancias de NetScaler. El perfil predeterminado se define mediante las credenciales de administrador predeterminadas de NetScaler. 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 NetScaler desde la página **Instancia** o al agregar o cambiar una instancia.

> **Nota:**
>
> Asegúrate de usar la cuenta de superadministrador para crear un perfil de instancia.

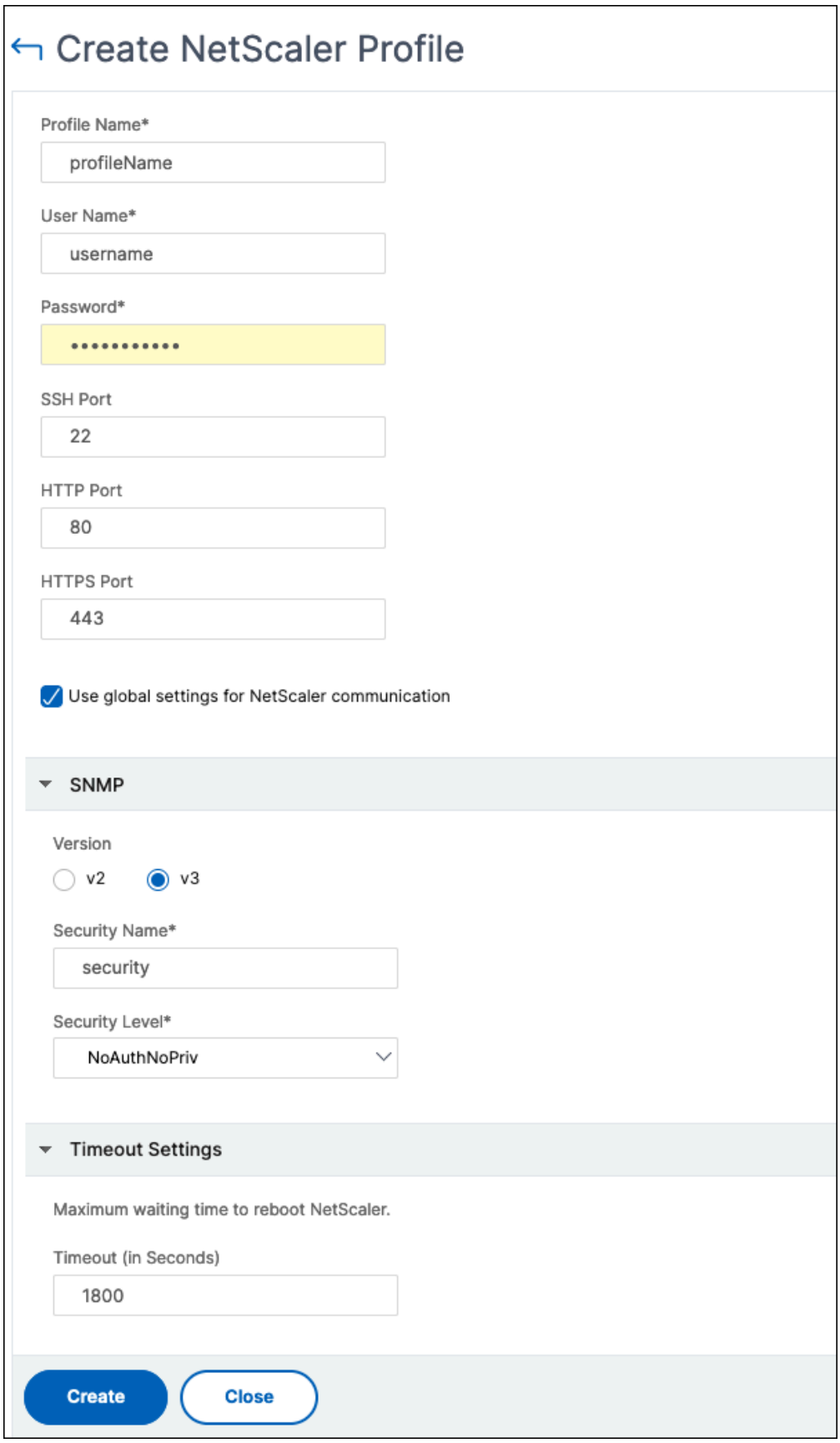
Para crear un perfil de NetScaler desde la página Instancia:

1. Vaya a **Infraestructura > Instancias**.
2. Seleccione una instancia. Por ejemplo, NetScaler.
3. En la página NetScaler, en **Seleccionar acción**, seleccione **Perfiles**.



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

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



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

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

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

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

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

> **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 NetScaler CPX. El puerto HTTP personalizado solo se puede utilizar para la comunicación entre NetScaler ADM y NetScaler CPX.

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

> **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 NetScaler CPX. El puerto HTTPS personalizado solo se puede utilizar para la comunicación entre NetScaler ADM y NetScaler CPX.

g) **Usar la configuración global para la comunicación de NetScaler**: Seleccione esta opción si quiere utilizar la configuración del sistema para la comunicación entre NetScaler ADM y la instancia de NetScaler; 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 NetScaler SDX, solo se admite **SNMPv2**.

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

j) Seleccione **Create**.

Agregar instancias de ADC a NetScaler ADM

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

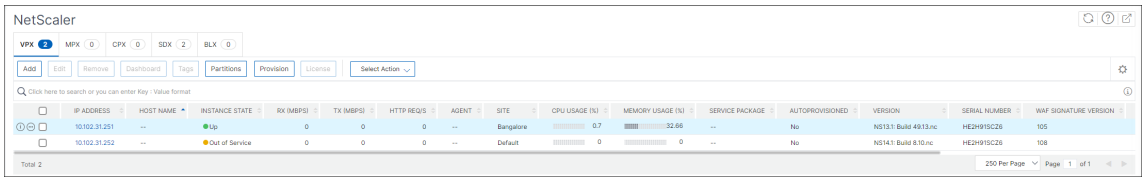
Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de NetScaler, o un intervalo de direcciones IP.

> **Nota:**
>
> - Para agregar instancias de NetScaler configuradas en un clúster, debe especificar la dirección IP del clúster o cualquiera de los nodos individuales de la configuración del clúster. Sin embargo, en NetScaler ADM, el clúster se representa únicamente mediante la dirección IP del clúster.
> - Para las instancias de NetScaler configuradas como un par de HA, cuando agrega una instancia, la otra instancia del par se agrega automáticamente.

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 NetScaler ADM:

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



3. Seleccione una de estas opciones:

   - **Escriba la dirección IP del dispositivo**: Para las instancias NetScaler, especifique el nombre de host o la dirección IP de cada instancia, o un rango de direcciones IP.

     Si quiere descubrir un par ADC HA mediante SNIP, asegúrese de que el modo de configuración de red independiente (INC) esté activado. Además, especifique las direcciones SNIP en el siguiente formato:

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     <!--NeedCopy-->
     ```

     Por ejemplo, `10.10.10.11#10.10.10.12`

   - **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.

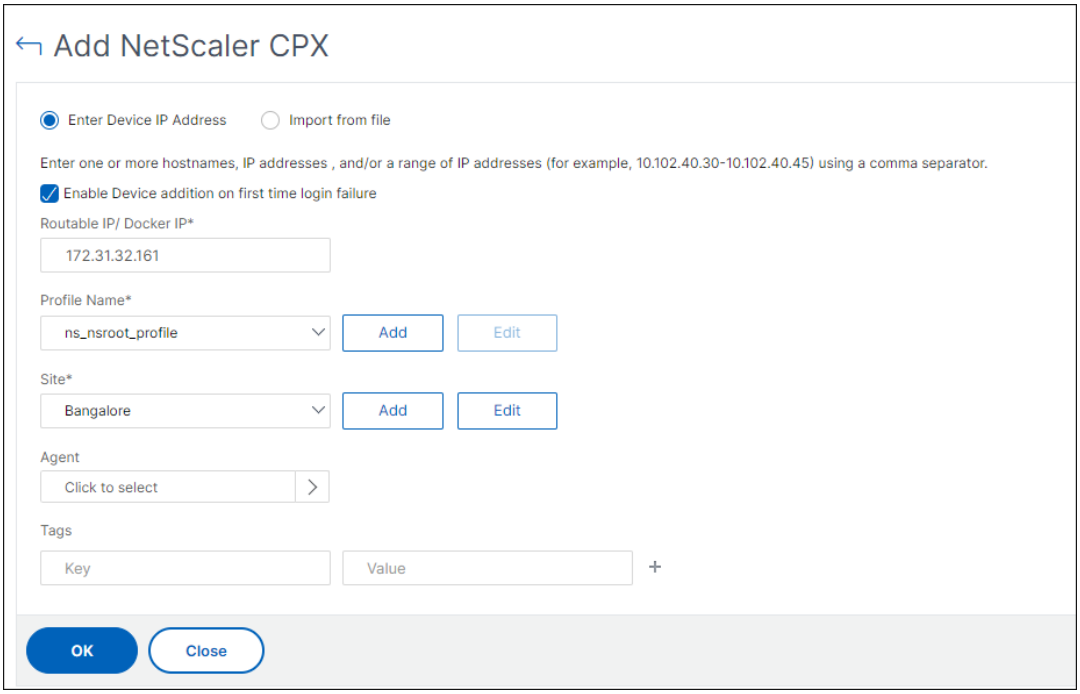
4. En **Nombre de perfil** , selecciona el perfil de instancia apropiado o crea un perfil haciendo clic en el icono + .
5. En **Sitio** , selecciona la ubicación en la que quieres agregar la instancia o crea una ubicación haciendo clic en el icono **+** .
6. Haga clic **en** Aceptar para iniciar el proceso de agregar instancias a NetScaler ADM.

> **Nota:**
>
> Si quiere volver a descubrir una instancia, vaya a **Infraestructura > Instancias > NetScaler**. Seleccione el tipo de instancia (por ejemplo, VPX) y seleccione la instancia que quiere volver a descubrir y, a continuación, en la lista **Seleccionar acción**, haga clic en **Redescubrir**.

Agregar instancias de NetScaler CPX a NetScaler ADM

NetScaler ADM se ha mejorado para brindar soporte a las mejoras que se han logrado en las funcionalidades de CPX. La instancia CPX de NetScaler ahora se agrega a NetScaler 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, NetScaler ADM descubre y registra automáticamente la instancia CPX. Ya no se descubre una instancia de CPX a través del host Docker.

1. Vaya a **Infraestructura > Instancias > NetScaler** y haga clic en **CPX**.
2. Haga clic en **Agregar** para agregar nuevas instancias CPX en NetScaler ADM.
3. Se abrirá la página **Add NetScaler 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. La incorporación de un par clave-valor facilita la búsqueda de la instancia más adelante.



> **Nota:**
>
> Para las instancias CPX de NetScaler, 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 una instancia independiente de NetScaler BLX en NetScaler ADM

Una instancia independiente de NetScaler BLX es una instancia única que se ejecuta en el servidor host Linux dedicado.

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. En la ficha **BLX**, haga clic en **Agregar**.
3. Seleccione la opción **Independiente** de la lista **Tipo de Instancia**.
4. En el campo **Dirección IP**, especifique la dirección IP de la instancia de BLX.
5. En el campo **Dirección IP del host**, especifique la dirección IP del servidor Linux en el que está alojada la instancia de BLX.
6. En la lista **de nombres de perfil**, seleccione el perfil adecuado para una instancia de BLX o cree un perfil.

   Para crear un perfil, haga clic en **Agregar**.

> **Importante:**
>
> Asegúrese de haber especificado el nombre de usuario del host y la contraseña correctos del servidor Linux en el perfil.

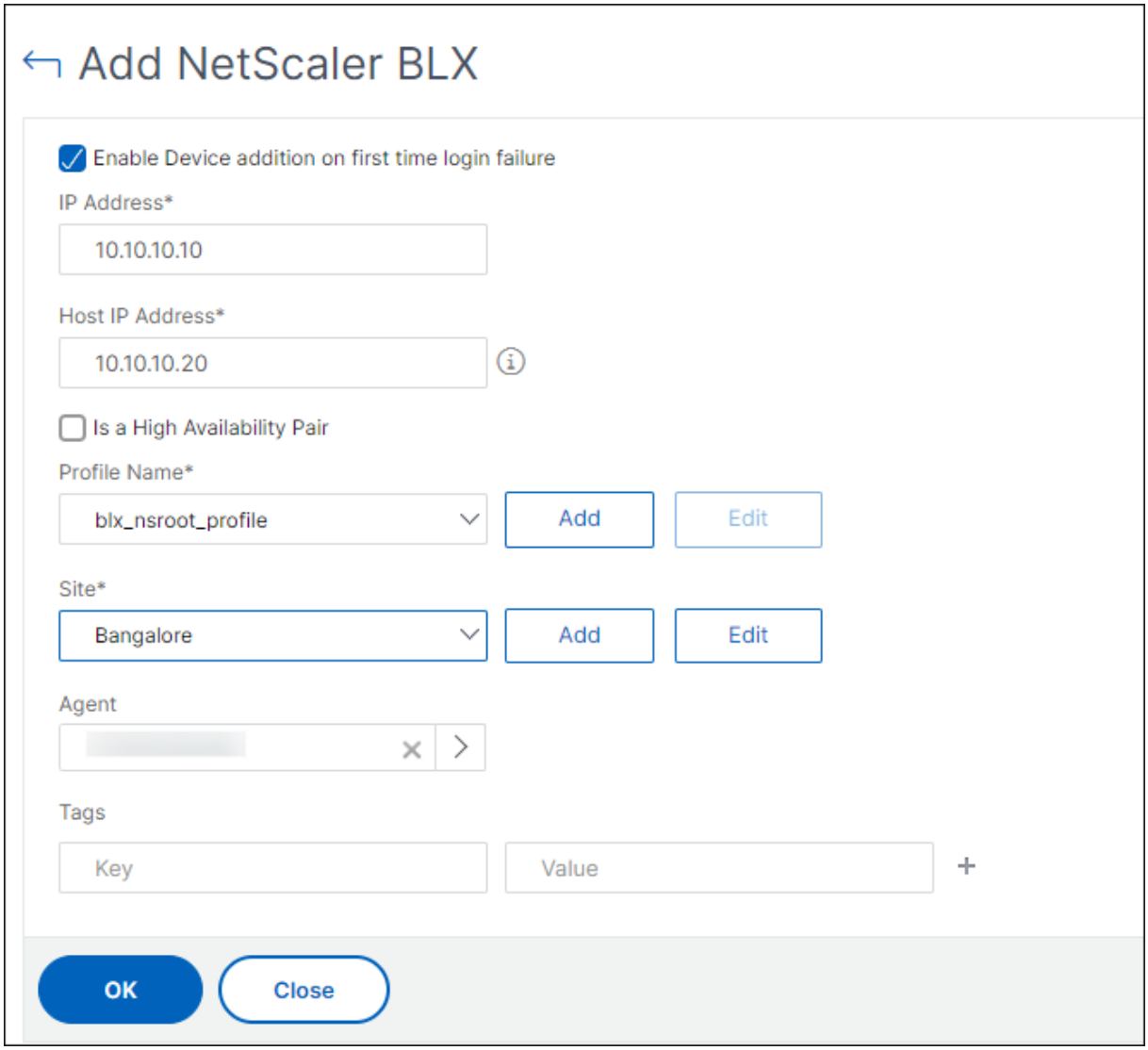
7. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

   Si quieres agregar un sitio, haga clic en **Agregar**.

8. En la lista de **agentes**, seleccione el agente NetScaler ADM al que quiere asociar la instancia.

   Si solo hay un agente configurado en su NetScaler ADM, ese agente se selecciona de forma predeterminada.

9. Haga clic en **Aceptar**.



Agregue instancias de NetScaler BLX de alta disponibilidad en NetScaler ADM

Las instancias de NetScaler BLX de alta disponibilidad que se ejecutan en diferentes servidores host Linux. Un servidor Linux no puede hospedar más de una instancia BLX.

1. En la ficha **BLX**, haga clic en **Agregar**.
2. Seleccione la opción **Alta disponibilidad** en la lista **Tipo de instancia**.
3. En el campo **Dirección IP**, especifique la dirección IP de la instancia de BLX.
4. En el campo **Dirección IP del host**, especifique la dirección IP del servidor Linux en el que está alojada la instancia de BLX.
5. En el campo **Dirección IP del mismo** nivel, especifique la dirección IP de la instancia BLX homóloga.
6. En el campo **Dirección IP del host del mismo** nivel, especifique la dirección IP del servidor Linux en el que está alojada la instancia BLX del mismo nivel.
7. En la lista **de nombres de perfil**, seleccione el perfil adecuado para una instancia de BLX o cree un perfil.

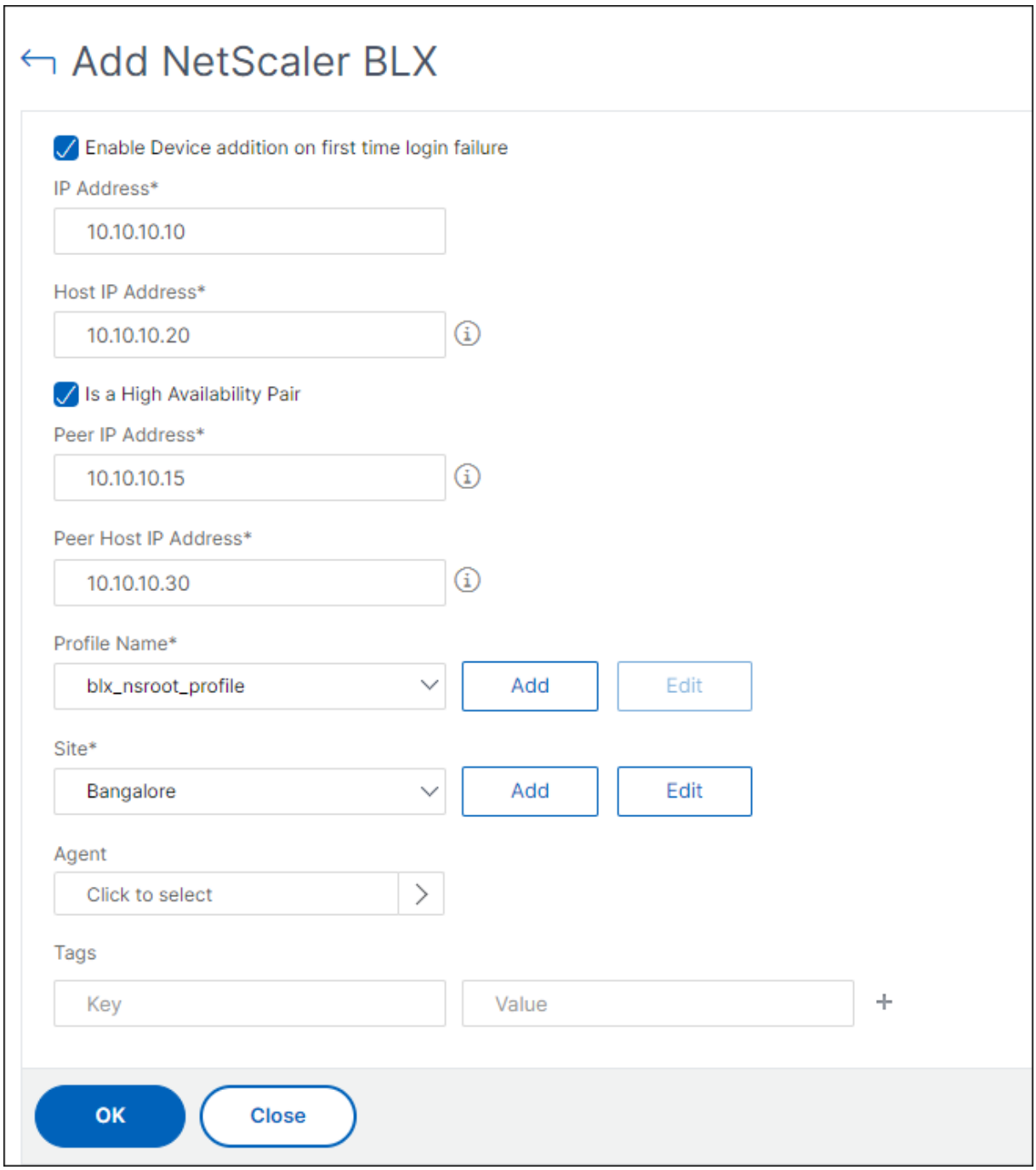
   Para crear un perfil, haga clic en **Agregar**.

   > **Importante:**
   >
   > Asegúrese de especificar el nombre de usuario del host y la contraseña correctos del servidor Linux en el perfil.

8. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

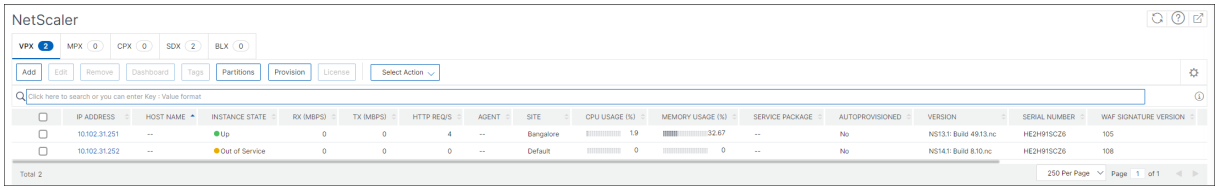
   Si quieres agregar un sitio, haga clic en **Agregar**.
9. En la lista de **agentes**, seleccione el agente NetScaler ADM al que quiere asociar la instancia.

   Si solo hay un agente configurado en su NetScaler ADM, ese agente se selecciona de forma predeterminada.
10. Haga clic en **Aceptar**.



Acceder a una GUI de instancia desde NetScaler ADM

1. Vaya a **Infraestructura > InstanciasNetScaler**.
2. Seleccione el tipo de instancia al que desea acceder (por ejemplo, VPX, MPX, CPX, SDX o BLX).
3. Haga clic en la dirección IP de NetScaler requerida o en el nombre de host.



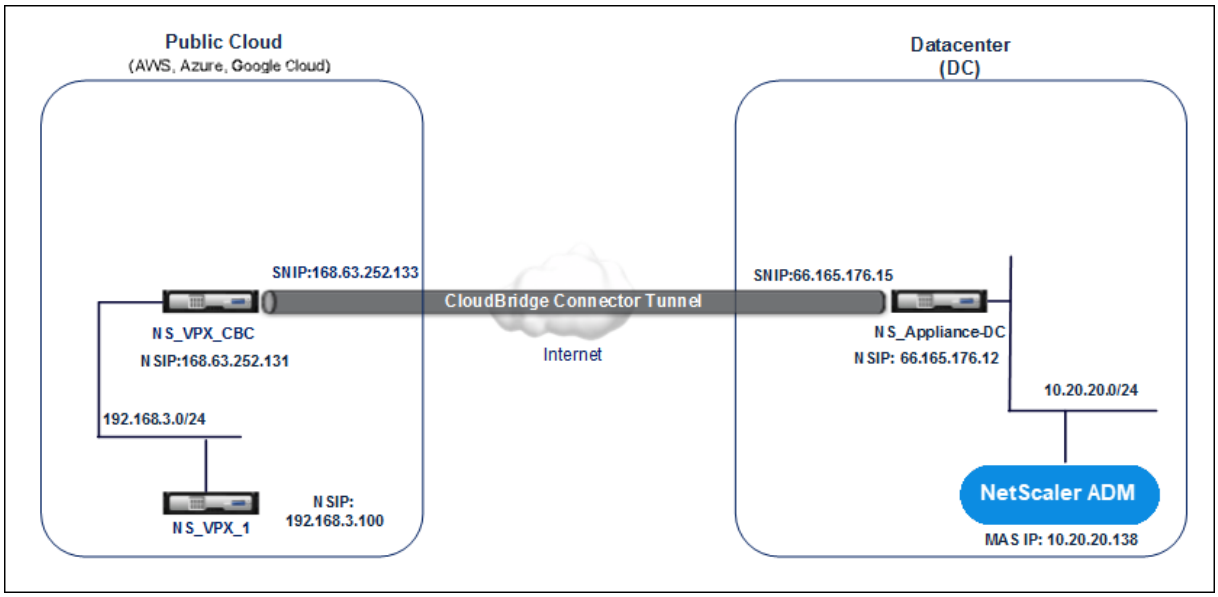
La GUI de la instancia seleccionada aparece en una ventana emergente.

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

January 30, 2024

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

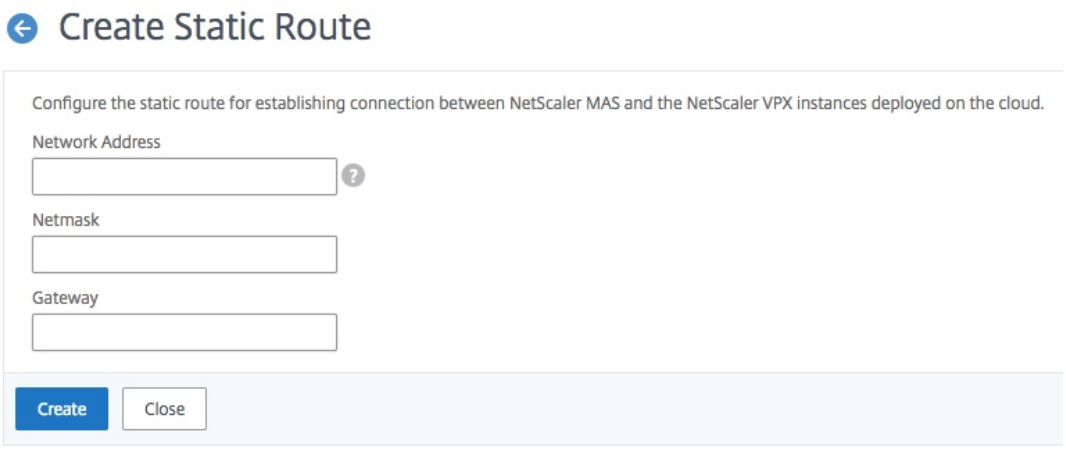
La siguiente topología de ejemplo utiliza la conectividad de Citrix CloudBridge Connector para la capa 3 entre NetScaler ADM y las instancias de NetScaler VPX implementadas en la nube.



Se configura un túnel de Citrix CloudBridge Connector entre el dispositivo NetScaler NS_Appliance-DC, en un centro de datos de centro de datos, y el dispositivo virtual NetScaler (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 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 VPX en la nube pública.
   - Para obtener instrucciones, consulteInstalar NetScaler VPX en AWS.
   - Para obtener instrucciones, consulte Instalar NetScaler VPX en Microsoft Azure.
   - Para obtener instrucciones, consulte Instalar NetScaler VPX en Google Cloud.
2. Implemente y configure un dispositivo físico NetScaler o aprovisionar y configurar un dispositivo virtual (VPX) de NetScaler en una plataforma de virtualización del centro de datos.
   - Para obtener instrucciones, consulte Instalar una instancia de NetScaler VPX en Citrix Hypervisor.
   - Para obtener instrucciones, consulte Instalar dispositivos virtuales Citrix en VMware ESXi.
   - Para obtener instrucciones, consulte Instalar dispositivos virtuales NetScaler en Microsoft Hyper-V.
3. Configure Citrix CloudBridge Connector entre el centro de datos y la nube pública. Para obtener instrucciones, consulte Configuración de Citrix CloudBridge Connector.
4. Configure la ruta estática para establecer la conexión entre NetScaler ADM y las instancias de NetScaler VPX implementadas en la nube, de la siguiente manera:
   a) Inicie sesión en NetScaler 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 NetScaler 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 VPX al NetScaler ADM especificando el rango de direcciones IP de las instancias de NetScaler VPX en la nube pública. Para obtener instrucciones detalladas, consulte Agregar instancias a NetScaler ADM.

Administrar licencias y habilitar análisis en servidores virtuales

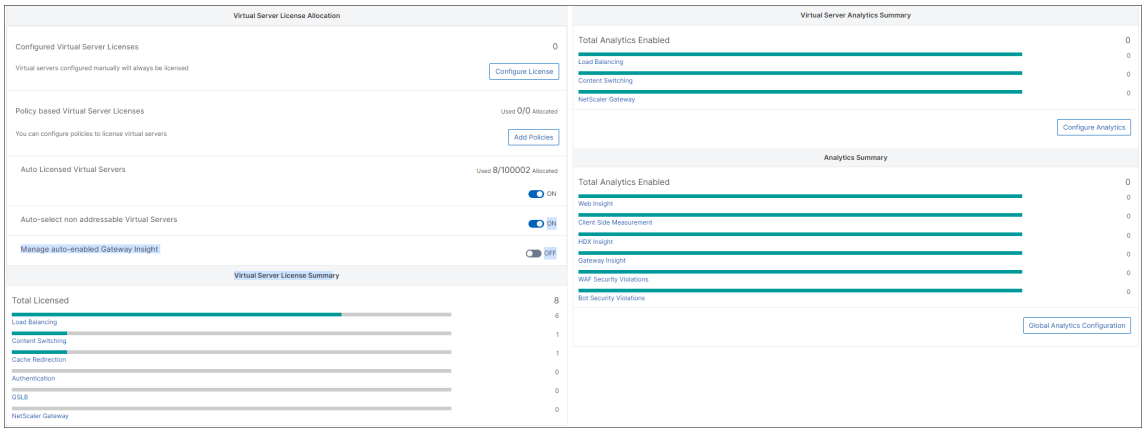
January 30, 2024

> **Nota**
>
> - De forma predeterminada, la opción **Servidores virtuales con licencia automática** está habilitada. Debe asegurarse de tener licencias suficientes para licenciar los servidores virtuales. Si tiene licencias limitadas y quiere licenciar solo los servidores virtuales selectivos según sus requisitos, inhabilite la opción **Servidores virtuales con licencia automática**. Vaya a **Configuración > Configuración de licencias y análisis** y inhabilite la opción **Servidores virtuales con licencia automática en Asignación de licencias de servidoresvirtuales**.

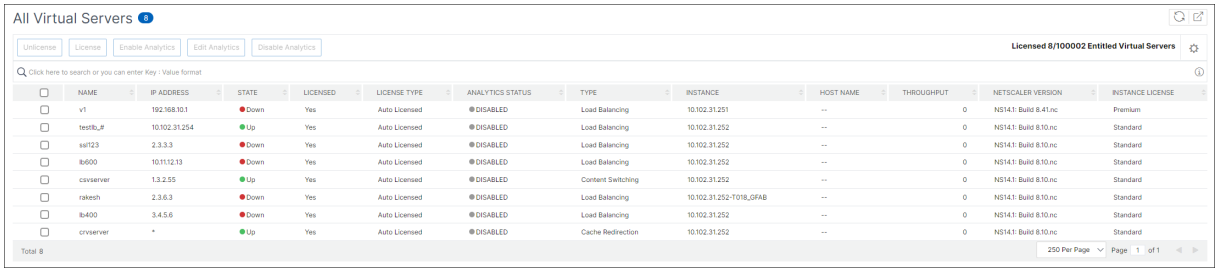
El proceso de habilitación de análisis se simplifica. Puede obtener una licencia del servidor virtual y habilitar el análisis en un único flujo de trabajo.

Vaya a **Configuración > Configuración de licencias y análisis** para:

- Ver el **resumen de licencia del servidor virtual**
- Ver el **resumen de análisis del servidor virtual**



Al hacer clic en **Configurar licencia** o **Configurar análisis**, aparece la página **Todos los servidores virtuales**.



En la página **Todos los servidores virtuales**, puede:

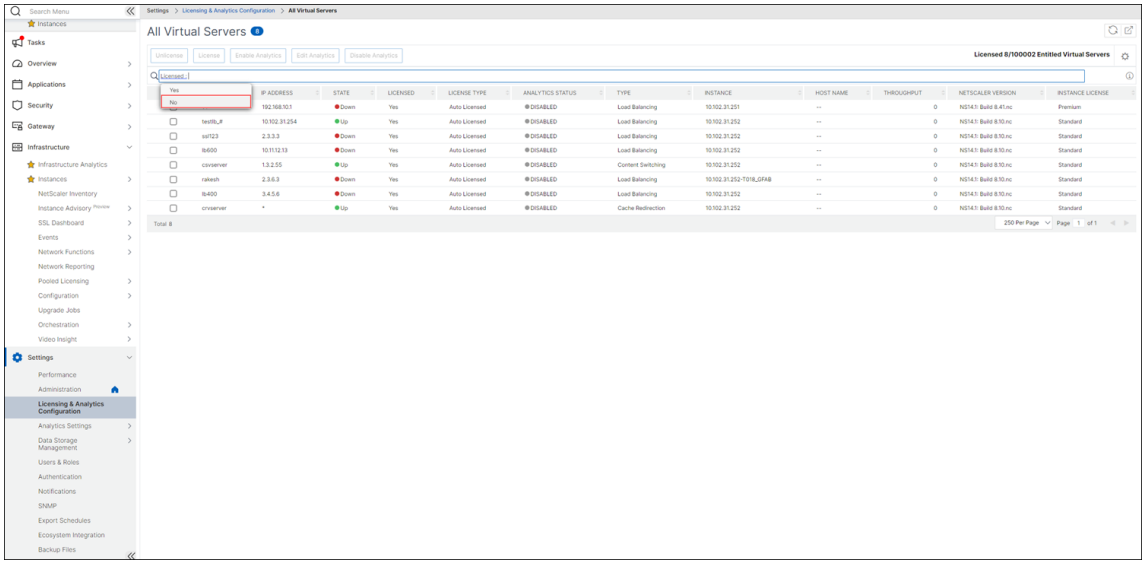
- Solicitar licencia para servidores virtuales sin licencia
- Eliminar la licencia de los servidores virtuales con licencia
- Habilite el análisis en servidores virtuales con licencia
- Modificar análisis
- Desactivar la analítica

> **Nota**
>
> Los servidores virtuales compatibles que permiten el análisis son el equilibrio de carga, la conmutación de contenido y NetScaler Gateway.

Administrar licencias en servidores virtuales

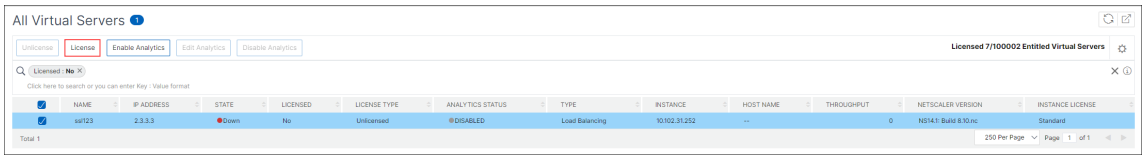
Para licenciar los servidores virtuales, desde la página **Todos los servidores virtuales** :

1. Haga clic en la barra de búsqueda, seleccione **Con licencia** y seleccione **No**.



   Ahora se aplica el filtro y solo se muestran los servidores virtuales sin licencia.

2. Seleccione los servidores virtuales y, a continuación, haga clic en **Licencia**.



Para anular la licencia de los servidores virtuales, desde la página **Todos los servidores virtuales** :

1. Haga clic en la barra de búsqueda, seleccione **Licencia** y seleccione **Sí**.
2. Seleccione los servidores virtuales y haga clic en **Anular licencia**.

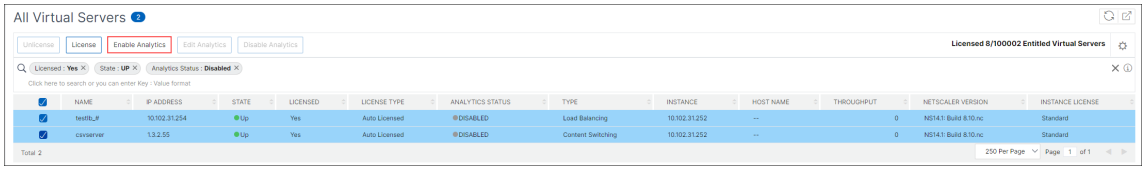
Habilitar análisis

Los siguientes son los requisitos previos para habilitar el análisis de los servidores virtuales:

- Asegúrese de que los servidores virtuales tengan **licencia**
- Asegúrese de que el estado de los análisis **esté**
- Asegúrese de que los servidores virtuales estén en estado **UP**

Puede filtrar los resultados para identificar los servidores virtuales que se mencionan en los requisitos previos.

1. Haga clic en la barra de búsqueda, seleccione **Estado** y, a continuación, seleccione **UP**.
2. Haga clic en la barra de búsqueda, seleccione **Licencia** y, a continuación, seleccione **Sí**.
3. Haga clic en la barra de búsqueda, seleccione **Estado de análisis**y, a continuación, seleccione **Desactivado**.
4. Tras aplicar los filtros, seleccione los servidores virtuales y, a continuación, haga clic en **Habilitar análisis**.



> **Nota**
>
> Alternativamente, puede habilitar el análisis para una instancia concreta:
>
> ```
> 1.  Vaya a **Infraestructura > Instances > NetScaler** y, a continuación, seleccione el tipo de instancia. Por ejemplo, VPX.
>
> 1.  Seleccione la instancia y, en **la lista Seleccionar acción**, seleccione **Configurar análisis**
> ```



```
4
5  1.  En la página Configurar análisis en servidores virtuales,
       seleccione el servidor virtual y haga clic en **Habilitar
       análisis**.
```

5. En la ventana **Habilitar análisis**:

   a) Seleccione los tipos de conocimientos (Web Insight o WAF Security Violations)

   b) Seleccione **Logstream** como modo de transporte

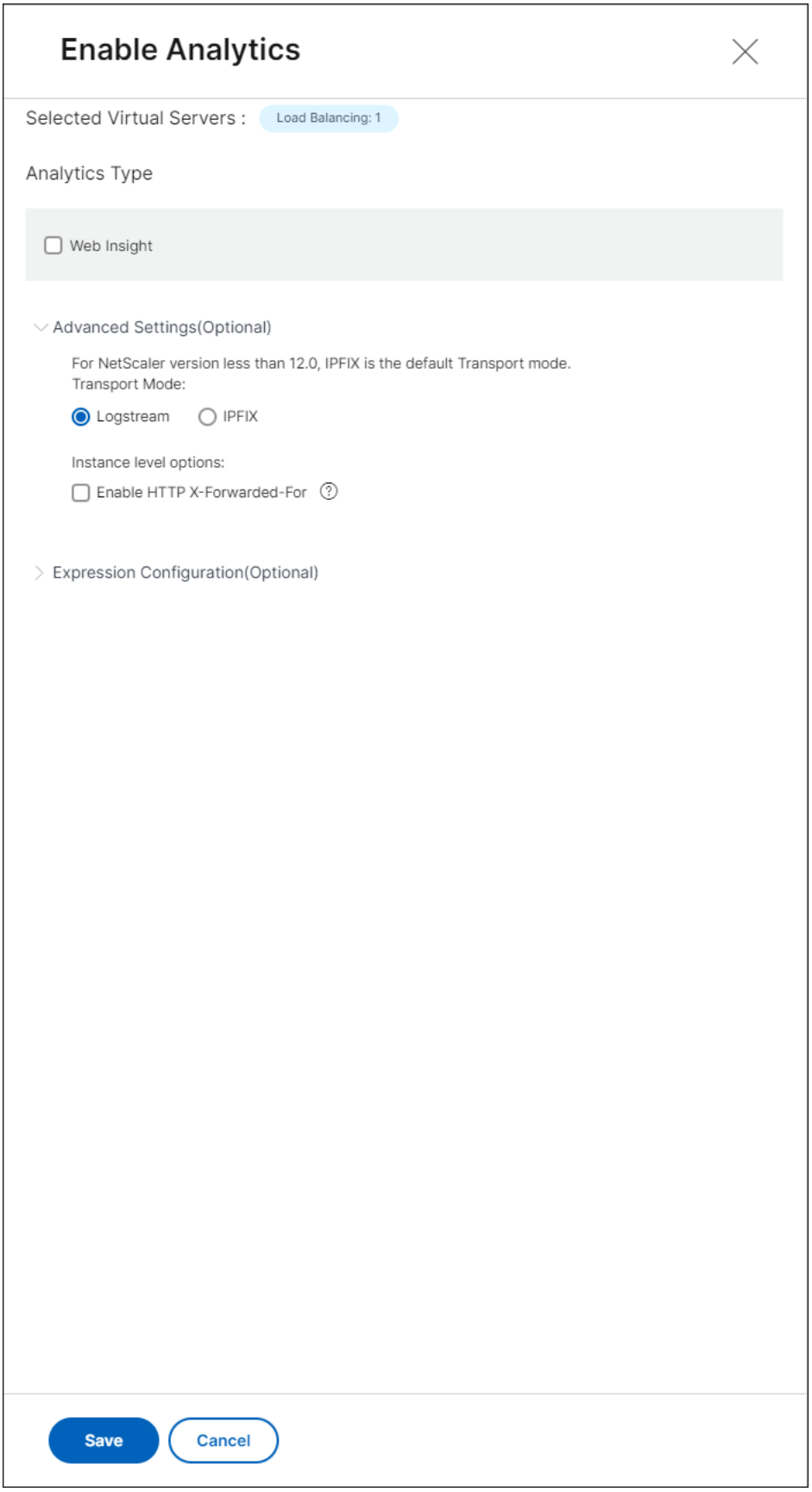
   > **Nota**
   >
   > Para NetScaler 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para NetScaler 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
   >
   > Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

   c) En **Opciones a nivel de instancia**:

   - **Habilitar HTTP X-Forwarded-For**: Seleccione esta opción para identificar la dirección IP para la conexión entre el cliente y la aplicación, a través del proxy HTTP o el equilibrador de carga.
   - **NetScaler Gateway**: Seleccione esta opción para ver los análisis de NetScaler Gateway.

   d) La expresión es verdadera por defecto

   e) Haga clic en **OK**.



> **Nota**
>
> - Si selecciona servidores virtuales que no tienen licencia, NetScaler ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
> - Para las particiones de administración, solo se admite **Web Insight**
> - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, NetScaler ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

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

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

Modificar análisis

Para modificar los análisis en los servidores virtuales:

1. Seleccione los servidores virtuales

   > Nota
   >
   > Alternativamente, también puede modificar análisis para una instancia concreta:

   ```
   1.  Vaya a **Infraestructura > Instances > NetScaler** y, a
   continuación, seleccione el tipo de instancia. Por ejemplo,
    VPX.
   2
   3  1.  Seleccione la instancia y haga clic en **Modificar aná
   lisis**.
   ```

2. Haga clic en **Modificar análisis**
3. Modifique los parámetros que quiere aplicar en la ventana **Modificar configuración de Analytics**
4. Haga clic en **Aceptar**.

Desactivar la analítica

Para inhabilitar los análisis en los servidores virtuales seleccionados:

1. Seleccione los servidores virtuales
2. Haga clic en **Desactivar**

NetScaler ADM desactiva los análisis en los servidores virtuales seleccionados

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

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

Un proceso unificado para permitir el análisis en servidores virtuales

January 30, 2024

Además del proceso existente para habilitar el análisis, también puede utilizar un flujo de trabajo de panel único para configurar el análisis en:

- Todos los servidores virtuales con licencia existentes
- Los servidores virtuales con licencia posteriores

Después de la configuración, esta función elimina la necesidad de habilitar manualmente el análisis en los servidores virtuales existentes y posteriores.

Puntos a tener en cuenta:

Antes de configurar los análisis, debe comprender los siguientes comportamientos de NetScaler ADM:

- Al configurar esta función por primera vez, debe asegurarse de que se cumplen los requisitos previos mencionados en este documento.
- Modifique la configuración de análisis más adelante.

  Tenga en cuenta que ha configurado los ajustes de análisis por primera vez al seleccionar Web Insight, HDX Insight y Gateway Insight. Si quiere modificar la configuración de análisis más adelante y anular la selección de Gateway Insight, los cambios no afectan a los servidores virtuales que ya están habilitados con análisis.
- Los servidores virtuales que ya están habilitados con análisis.

  Tenga en cuenta que tiene 10 servidores virtuales con licencia y dos de ellos ya están habilitados con análisis. En este caso, esta función permite el análisis solo para los ocho servidores virtuales restantes.
- Los servidores virtuales que se inhabilitan manualmente con análisis.

  Tenga en cuenta que tiene 10 servidores virtuales con licencia y que ha inhabilitado manualmente el análisis para dos servidores virtuales. En este caso, esta función permite el análisis solo para los ocho servidores virtuales restantes y omite los servidores virtuales que se inhabilitan manualmente con el análisis.
- Las opciones**Infracciones de seguridad de bots** e **Infracciones de seguridad de WAF** solo se admiten en servidores virtuales con licencia premium. Si los servidores virtuales no tienen licencia premium, las violaciones de **seguridad de bots y las violaciones** de **seguridad de WAF** no están habilitadas.

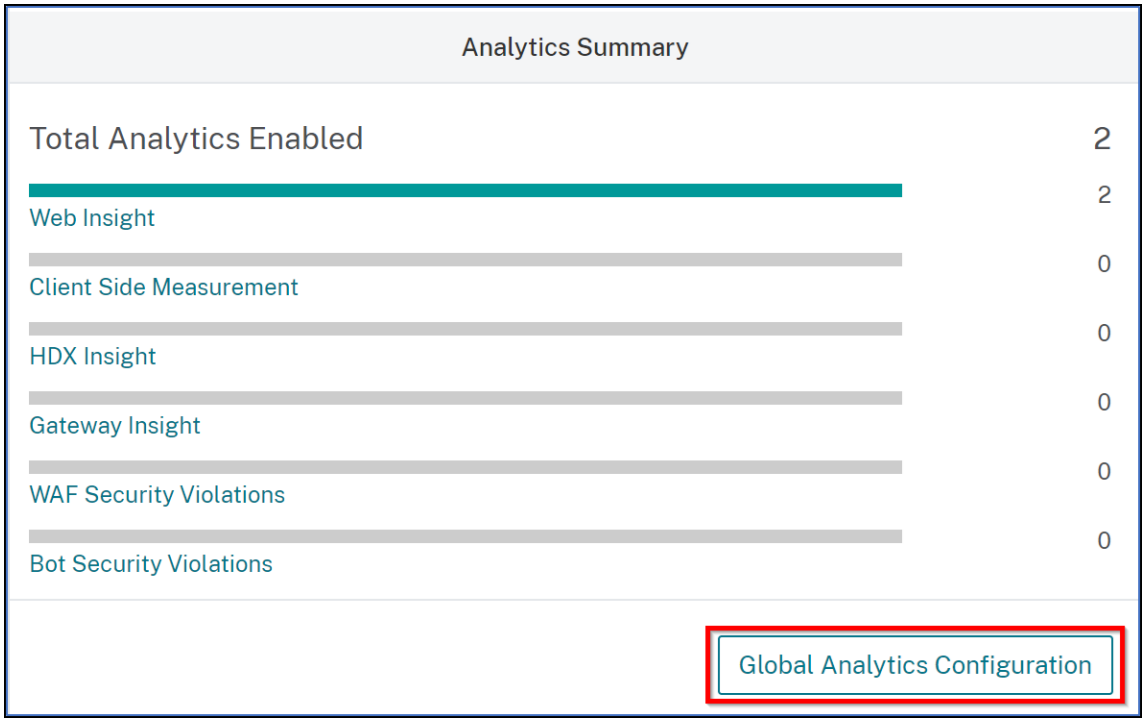
Requisitos previos

Compruebe que:

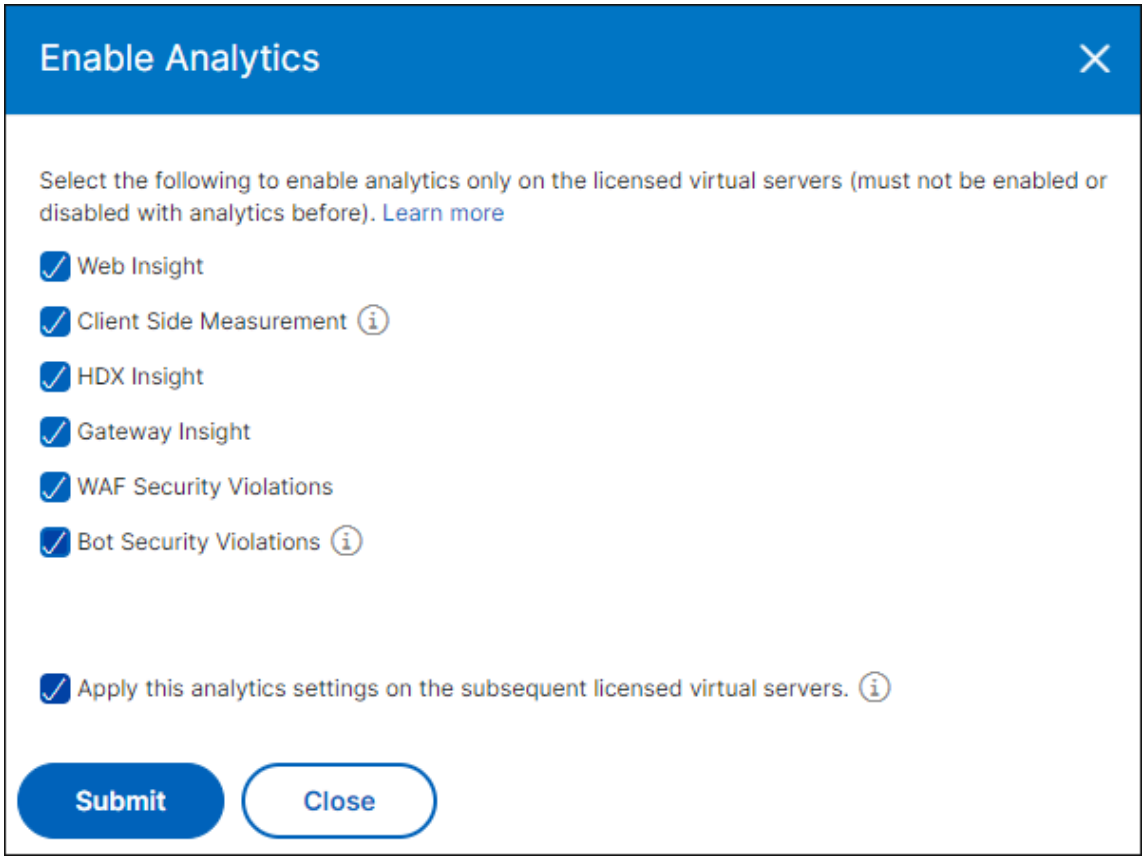
- Todos los servidores virtuales existentes tienen licencia.
- La opción de licencia automática está habilitada para licenciar todos los servidores virtuales posteriores. Vaya a **Configuración > Configuración de licencias y análisis** y, en **Asignación de licencias de servidores virtuales**, active la opción **Servidores virtuales con licencia automática**.

Habilitar análisis

1. Vaya a **Configuración > Configuración de licencias y análisis**.
2. En **Resumen de análisis**, haga clic en **Configuración de análisis global**.



3. Seleccione las funciones de análisis que quiere habilitar para el análisis en los servidores virtuales.
4. Para habilitar el análisis en los servidores virtuales posteriores, seleccione la casilla **Aplicar esta configuración de análisis en los servidores virtuales con licencia posteriores**.
5. Haga clic en **Submit**.



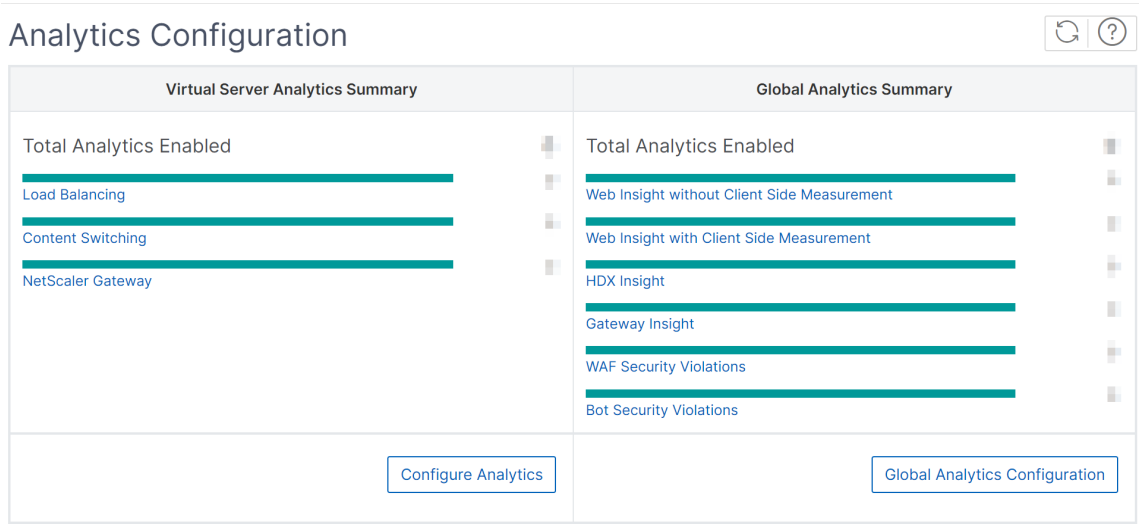
Configure el análisis en servidores virtuales con licencia flexible

January 30, 2024

El requisito previo para habilitar el análisis es que los servidores virtuales tengan licencia. Si utiliza una licencia flexible, todos los servidores virtuales existentes y los servidores virtuales posteriores se licencian automáticamente. Puede continuar con la configuración de los análisis.

Puede configurar los análisis de dos maneras. Vaya a Configuración **> Configuración de análisis** para ver:

- **Resumen**de análisis de servidores virtuales : le permite configurar los análisis en los servidores virtuales existentes.
- **Resumen de análisis global**: le permite configurar los análisis en los servidores virtuales existentes y posteriores.



Configurar los análisis en los servidores virtuales existentes

> **Nota:**
>
> Asegúrese de que los servidores virtuales en los que desea habilitar el análisis estén en **estado**ACTIVO.

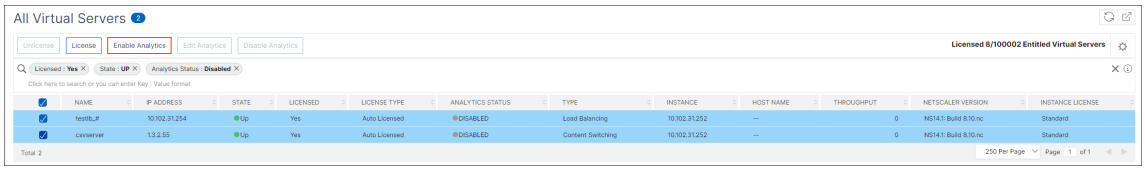
1. En **Resumen de análisis de servidores virtuales**, haga clic en **Configurar análisis**.

   Aparece la página **Todos los Servidores Virtuales**. Puede hacer lo siguiente:

   - Habilitar análisis
   - Modificar análisis
   - Desactivar la analítica

   > **Nota:**
   >
   > Los servidores virtuales compatibles que permiten el análisis son el equilibrio de carga, la conmutación de contenido y NetScaler Gateway.

2. Seleccione los servidores virtuales y, a continuación, haga clic en **Habilitar análisis**.



> **Nota**
>
> Como alternativa, puedes habilitar los análisis para una instancia:

```
1. Vaya a **Infraestructura > Instances > NetScaler** y, a
```



```
continuación, seleccione el tipo de instancia. Por ejemplo,
 VPX.

1.  Seleccione la instancia y, en la lista **Seleccionar acció
n** , seleccione **Configurar análisis**

1.  En la página Configurar análisis en servidores virtuales,
seleccione el servidor virtual y haga clic en **Habilitar
análisis**.
```

3. En la ventana **Habilitar análisis**:

   a) Seleccione los tipos de información.

   b) Seleccione **Logstream** como modo de transporte.

   > **Nota:**
   >
   > Para NetScaler 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para NetScaler 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
   >
   > Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

   c) En **Opciones a nivel de instancia**:

   - **Habilitar HTTP X-Forwarded-For**: Seleccione esta opción para identificar la dirección IP para la conexión entre el cliente y la aplicación, a través del proxy HTTP o el equilibrador de carga.
   - **NetScaler Gateway**: Seleccione esta opción para ver los análisis de NetScaler Gateway.

   d) La expresión es true de forma predeterminada.

   e) Haga clic en **Aceptar**.

   > **Nota:**
   >
   > - Para las particiones de administración, solo se admite **Web Insight** .
   > - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, NetScaler ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

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

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

Modificar análisis

Para modificar los análisis en los servidores virtuales:

1. Seleccione los servidores virtuales.

   > **Nota:**
   >
   > Como alternativa, también puedes editar los análisis de una instancia:
   >
   > ```
   > 1.  Vaya a **Infraestructura > Instances > NetScaler** y, a continuación, seleccione el tipo de instancia. Por ejemplo, VPX.
   > 
   > 1.  Seleccione la instancia y haga clic en **Modificar análisis**.
   > ```

2. Haga clic en **Modificar análisis**
3. Edite los parámetros que desea aplicar en la ventana **Editar configuración de análisis** .
4. Haga clic en **Aceptar**.

Desactivar la analítica

Para inhabilitar los análisis en los servidores virtuales seleccionados:

1. Seleccione los servidores virtuales.
2. Haz clic en **Desactivar análisis** .

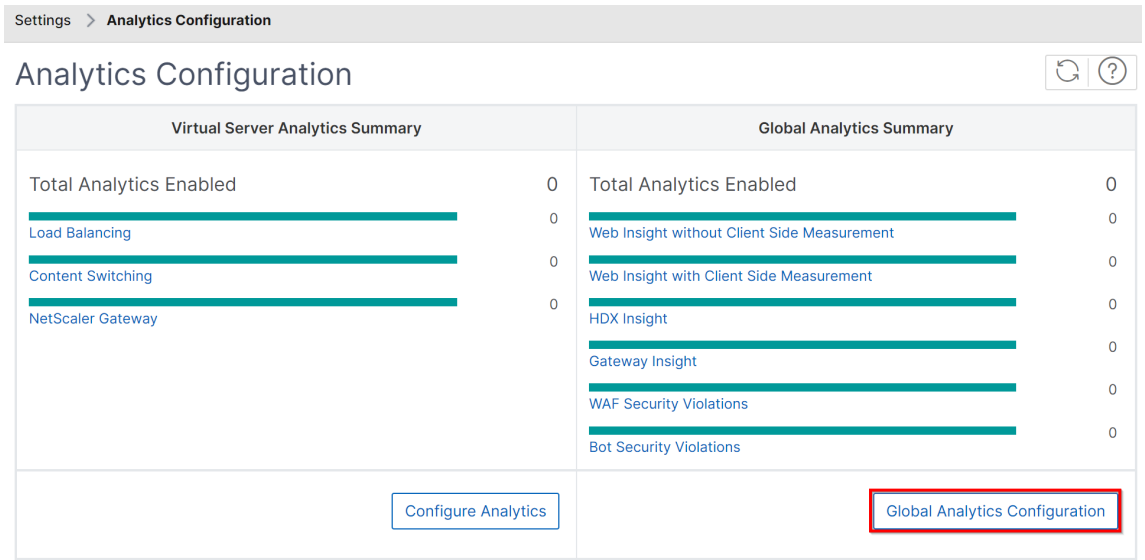
NetScaler ADM desactiva los análisis en los servidores virtuales seleccionados.

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

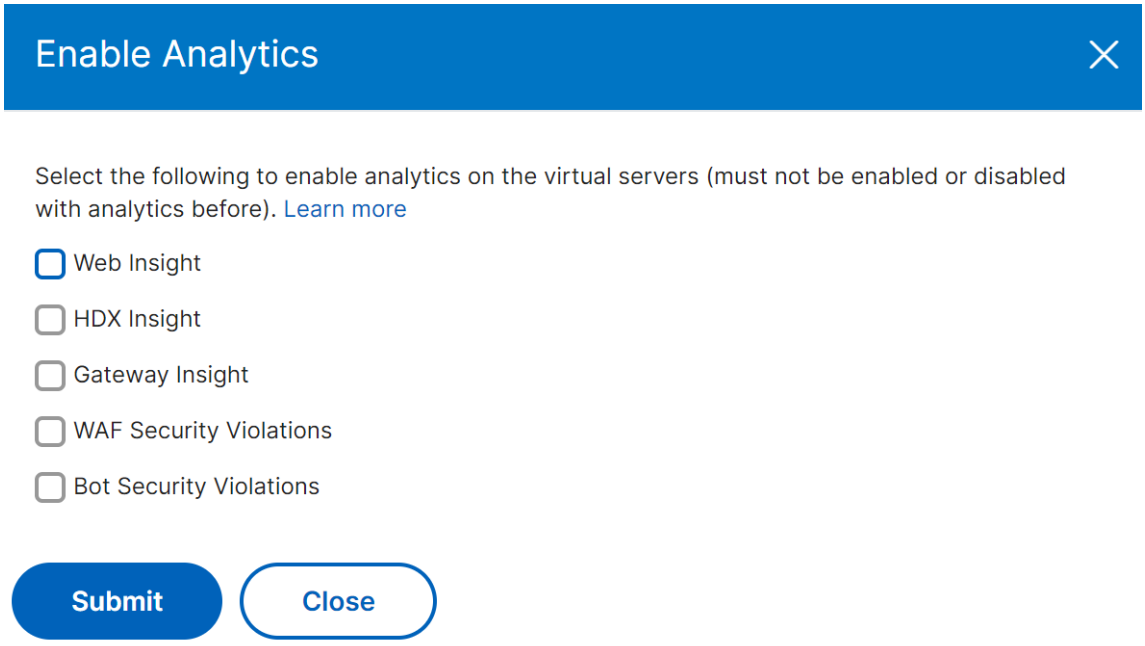
Función	IPFIX	Flujo de registro
Información web	•	•
Infracciones de seguridad de WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
Insight SSL	No compatible	•
CR Insight	•	•
Reputación IP	•	•
AppFirewall	•	•
Medición del lado del	•	•
Syslog/Auditlog	•	•

Configure los análisis de forma global

1. En **Resumen de análisis global** , haga clic en **Configuración de análisis global** .



2. Seleccione las funciones de análisis que quiere habilitar para el análisis en los servidores virtuales.
3. Haga clic en Submit.



Tras la configuración, el análisis se habilita en los servidores virtuales existentes y posteriores.

Puntos que tener en cuenta

- Tenga en cuenta que ha configurado la configuración de Global Analytics por primera vez seleccionando Web Insight , HDX Insight y Gateway Insight . Si vuelve a cambiar la configuración de análisis más adelante y deselecciona Gateway Insight , los cambios no afectarán a los servidores virtuales que ya están habilitados con análisis.
- Tenga en cuenta que tiene 10 servidores virtuales con licencia y dos de ellos ya están habilitados con análisis mediante la opción **Configurar análisis** . En este escenario, al configurar la configuración de análisis global, los análisis se aplican solo en los ocho servidores virtuales restantes.
- Tenga en cuenta que tiene 10 servidores virtuales con licencia y que ha inhabilitado manualmente el análisis para dos servidores virtuales. En este escenario, al configurar la configuración de análisis global, los análisis se aplican solo en los ocho servidores virtuales restantes y se omiten los servidores virtuales que se deshabilitan manualmente con los análisis.

Asignar un perfil de red para la instancia de NetScaler gestionada

January 30, 2024

Al habilitar el análisis para los servidores virtuales en NetScaler ADM, los datos de AppFlow de NetScaler se exportan a NetScaler ADM a través de la dirección IP de subred de NetScaler (SNIP).

En algunos casos, es posible que el SNIP esté bloqueado debido al firewall de la red. En estos casos, es posible que tenga que usar una dirección IP diferente a la del SNIP. Para obtener más información sobre el perfil de red, consulte Usar una IP de origen especificada para la comunicación del back-end.

Puede asignar un perfil de red a una instancia de NetScaler mediante NetScaler ADM para exportar datos de AppFlow de NetScaler a NetScaler ADM.

Requisitos previos

Compruebe que:

- La versión de la instancia de NetScaler es **13.0-48.4 o posterior**.
- El perfil de red se configura en las instancias de NetScaler.

Para asignar un perfil de red en NetScaler ADM:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Configurar perfiles de red** para asignar un perfil de red a la instancia.
3. Seleccione un perfil de red de la lista y haga clic en **Aplicar**.

> **Nota:**
>
> Asegúrese de inhabilitar los análisis para todos los servidores virtuales antes de asignar un perfil de red a la instancia.

Configurar servidor NTP

January 30, 2024

Puede configurar un servidor de Network Time Protocol (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.

Para configurar un servidor NTP en NetScaler ADM:

1. En la GUI de ADM, vaya a **Configuración > Administración**. En la página **Administración del sistema**, en **Configuraciones de red**, haga clic en **Servidores NTP**. 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**.

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 algunos ajustes del sistema para garantizar un rendimiento óptimo de su servidor NetScaler ADM.

Configurar alarmas del sistema

Configure 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. 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 se puede ver el mensaje como un mensaje de syslog.

Para configurar alarmas del sistema:

1. Vaya a **Configuración > SNMP**y, a continuación, haga clic en la ficha **Alarmas** en la esquina superior derecha.
2. Seleccione la alarma que quiere configurar y haga clic en **Modificar**.
3. En la página **Configurar alarma**, seleccione la gravedad de la alarma y establezca el umbral.
4. Para ver las alarmas que han superado el umbral o para las que se ha producido un evento, vaya a **Configuración > Auditoría** y haga clic en **Mensajes de syslog**.

Configurar 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. La configuración de la notificación 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 **Configuración > Administración**. En la página **Administración del sistema**, en **Notificaciones de eventos**, haga clic en **Configurar notificación de eventos y resumen > Notificación de eventos**.
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 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).

Para configurar la configuración de poda delsistema :

1. Vaya a **Configuración > Administración del sistema**. En **Reproducción de datos**, haga clic en **Reproducción de datos del sistema y de la instancia**.
2. En la página **Sistema**, especifique el número de días durante los que desea conservar los datos y haga clic en **Guardar**.

Configurar la configuración de syslog prune 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 después de los cuales los datos genéricos de syslog se eliminarán de NetScaler ADM.

Para configurar los ajustes de purga delsyslog de la instancia :

1. Vaya a **Configuración > Administración > Eliminación de datos**.
2. Haga clic en **Poda de datos de sistema e instancia > Syslog**de instancia.
3. En la **página Configurar la configuración de Syslog Prune de la instancia**, especifique el número de días comprendido entre 1 y 180 en el campo Retain **Syslog Generic** Data.
4. Haga clic en **Guardar**.

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 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).

Para configurar los ajustes de poda deeventos de instancia :

1. Vaya a **Configuración > Administración**.
2. En la página **Administración del sistema**, en **Poda de datos, haga clic en Podade datos del sistema y de la instancia**.

3. En la página **de eliminación de datos**, haga clic en **Eventos de instancia**.
4. **En el campo**Datos para conservar (días)**, introduzca el intervalo de tiempo, en días, durante el que quiere conservar los datos en el servidor NetScaler ADM y haga clic en Guardar.**

Configurar 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. 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 **Configuración > Administración**.
2. En **Copia de seguridad**, haga clic en **Configurar copia de seguridad del sistema y de la instancia**.
3. Haga clic en **Sistema** y, en la página **Configurar la configuración de respaldo del sistema**, especifique los valores requeridos.

Configurar las opciones de copia de seguridad de instancia

Si realiza una copia de seguridad del estado actual de una instancia de NetScaler, puede usar los archivos de respaldo para restaurar la estabilidad si la instancia se vuelve 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 **Configuración > Administración**.
2. En **Copia de seguridad**, haga clic en **Configurar copia de seguridad del sistema y de la instancia**.
3. Haga clic en **Instancia**, en **Configurar la configuración de copia de seguridad de la instancia**, y especifique los valores requeridos.

Habilitar o inhabilitar funciones de ADM

Como administrador, puede habilitar o inhabilitar las siguientes funciones en la página **Configuración > Administración > Funciones configurables** :

- **Failover** del agente: La conmutación por error del agente puede producirse en un sitio que tiene dos o más agentes activos. Cuando un agente se vuelve inactivo (estado DOWN) en el sitio, el servicio NetScaler ADM redistribuye las instancias ADC del agente inactivo con otros agentes activos. Para obtener más información, consulte Configurar agentes locales para la implementación en varios sitios.
- **Función de red de sondeo** de entidad: Una entidad es una directiva, un servidor virtual, un servicio o una acción asociada a una instancia de ADC. De forma predeterminada, NetScaler ADM sondea automáticamente las entidades de función de red configuradas cada 60 minutos. Para obtener más información, consulte Descripción general de sondeos.
- **Copia de seguridad de instancia: Realice** una copia de seguridad del estado actual de una instancia de NetScaler y, posteriormente, utilice los archivos de copia de seguridad para restaurar la instancia de ADC al mismo estado. Para obtener más información, consulte Realizar copias de seguridad y restaurar instancias de NetScaler.
- **Auditoría de configuración de instancias**: Supervise los cambios de configuración en las instancias administradas de NetScaler, solucione los errores de configuración y recupere las configuraciones no guardadas. Para obtener más información, consulte Crear plantillas de auditoría.
- **Eventos de instancia**: Los eventos representan ocurrencias de eventos o errores en una instancia de NetScaler administrada. Los eventos recibidos en NetScaler ADM se muestran en la página de **resumen de eventos** (**Infraestructura > Eventos**) y todos los eventos activos se muestran en la página Mensajes de eventos (**Infraestructura > Eventos > Mensajes de eventos**). Para obtener más información, consulte Eventos.
- **Informes de red de instancias**: Puede generar informes para instancias a nivel global. Además, para entidades como los servidores virtuales y las interfaces de red. Para obtener más información, consulte Informes de red.
- **Certificados SSL de instancia**: NetScaler ADM proporciona una vista centralizada de los certificados SSL instalados en todas las instancias administradas de NetScaler. Para obtener más información, consulte Panel de control SSL.
- **Syslog de instancias**: Puede supervisar los eventos syslog generados en sus instancias NetScaler si ha configurado el dispositivo para redirigir todos los mensajes syslog a NetScaler ADM.

Para habilitar una función, lleve a cabo los siguientes pasos:

1. Seleccione la función de la lista que quiere habilitar.
2. Haga clic en **Activar**.

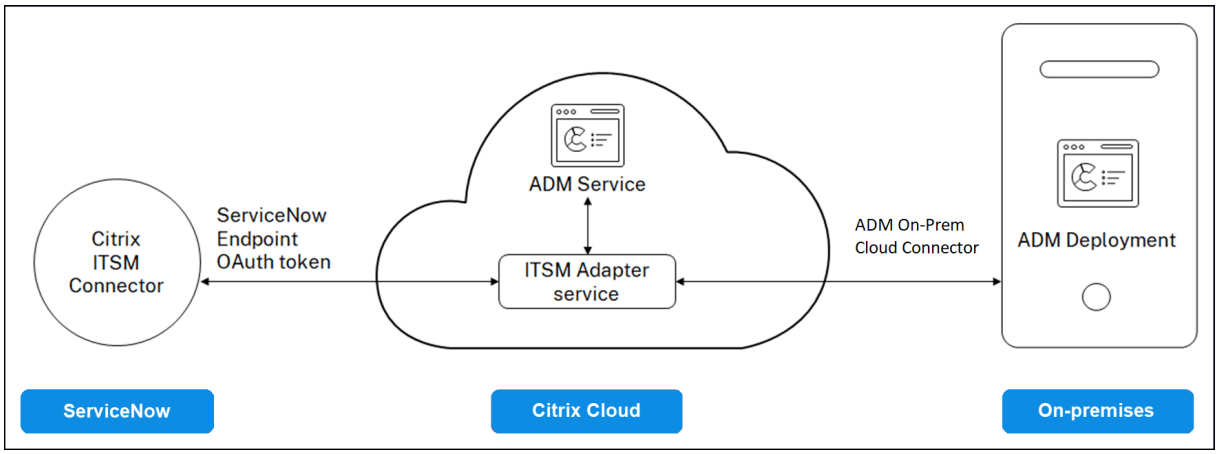
> **Importante**
>
> Si una función está inhabilitada, el usuario no puede realizar las operaciones asociadas a esa función.

Integre NetScaler ADM con la instancia de ServiceNow

January 30, 2024

Cuando quiera habilitar las notificaciones de ServiceNow para los eventos de NetScaler y ADM, integre NetScaler ADM con la instancia de ServiceNow. Esta integración utiliza el conector ITSM de Citrix para comunicarse entre NetScaler ADM y la instancia de ServiceNow.

La integración de ServiceNow con ADM utiliza el servicio de adaptador ITSM para la autenticación basada en tokens. Para hacerlo, crea una instancia de punto final en ServiceNow. Para obtener más información, consulte Cómo funciona el adaptador ITSM.



Para conectar su implementación local de ADM con un adaptador ITSM, asegúrese de haber configurado ADM On-Prem Cloud Connector. Para obtener más información, consulte ADM On-Prem Cloud Connector.

Para la integración de ServiceNow con ADM, versión 14.1 4.x o anterior, asegúrese de configurar la identidad del cliente. Para obtener más información, consulte Configurar la identidad del cliente.

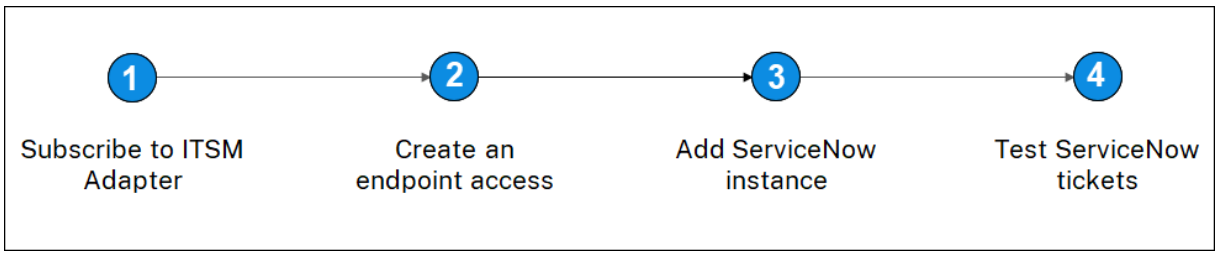
Requisitos previos

Antes de integrar ADM con ServiceNow, asegúrese de lo siguiente:

1. Inscríbase en Citrix Cloud. Asegúrese de tener acceso para administrar los administradores de Citrix Cloud. Para obtener más información, consulte Administrar administradores de Citrix Cloud.

¿Cómo integrar ADM con ServiceNow?

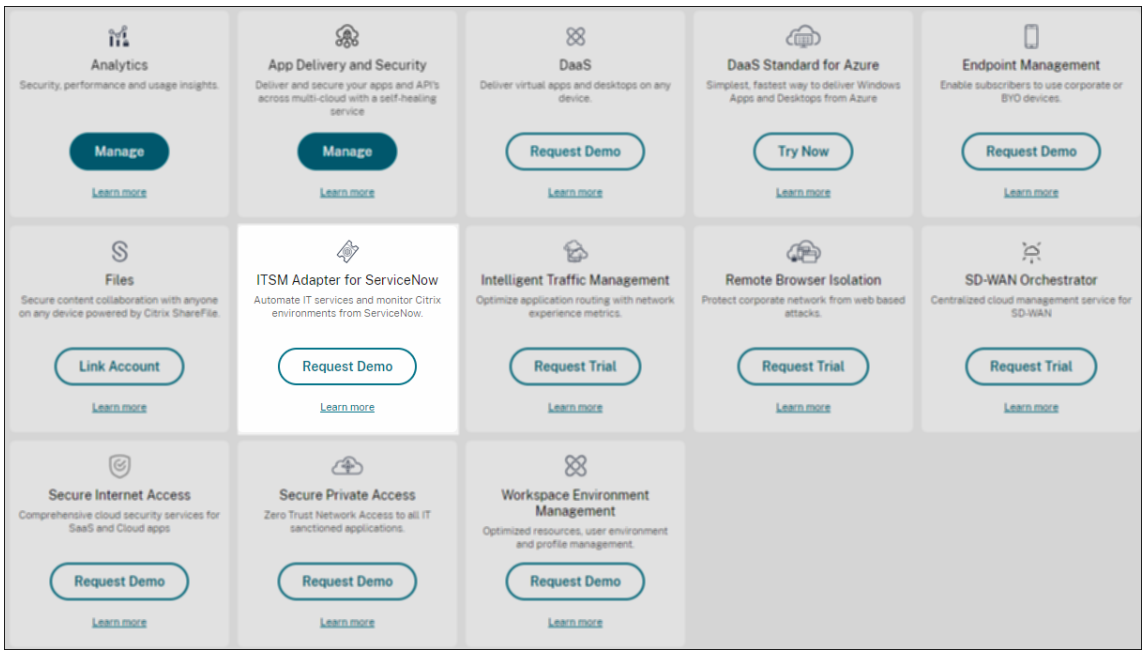
Realice los siguientes pasos para integrar NetScaler ADM con ServiceNow mediante el conector ITSM:



1. Suscríbase al servicio Adaptador ITSM en Citrix Cloud.
2. Crea un acceso de punto final en la instancia de ServiceNow.
3. Agregue una instancia de ServiceNow.
4. Pruebe la generación automática de tíquets de ServiceNow en ADM.

Paso 1: Suscríbase al servicio de adaptador ITSM en Citrix Cloud

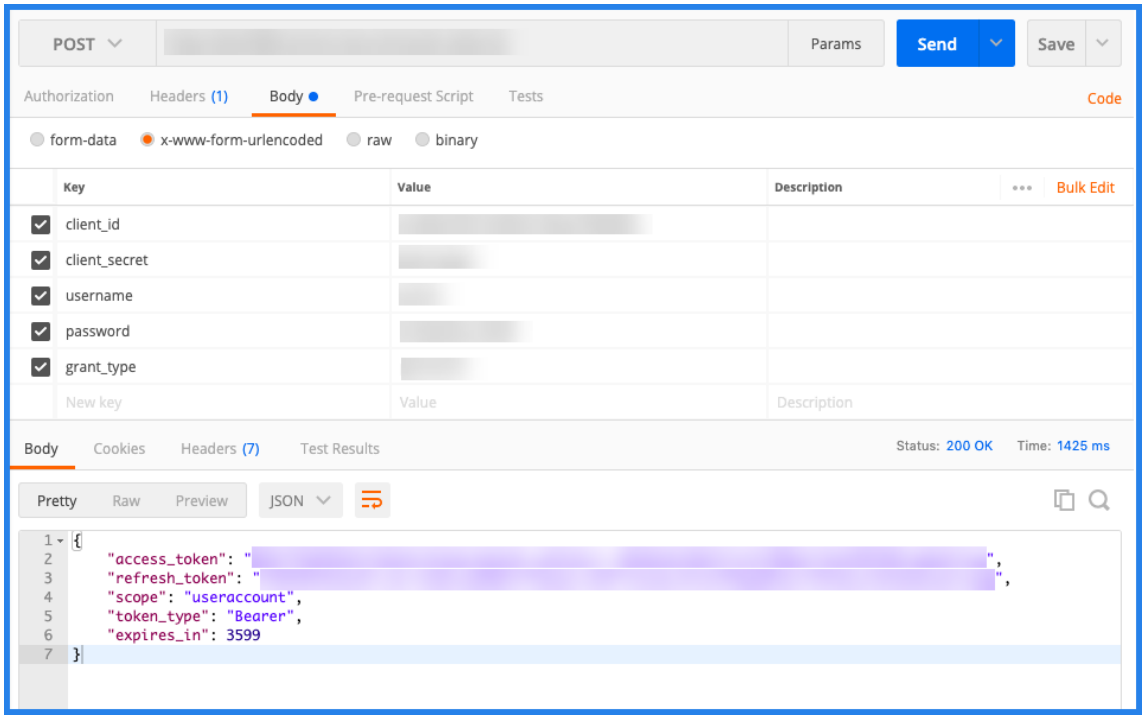
1. En el icono **Adaptador ITSM**, haga clic en **Solicitar prueba**.



2. Desplácese hasta **Identity Access and Management** > **API Access** y anote la información de **Client ID** y **Client Secret**.

Paso 2: crear un acceso de punto final en la instancia de ServiceNow

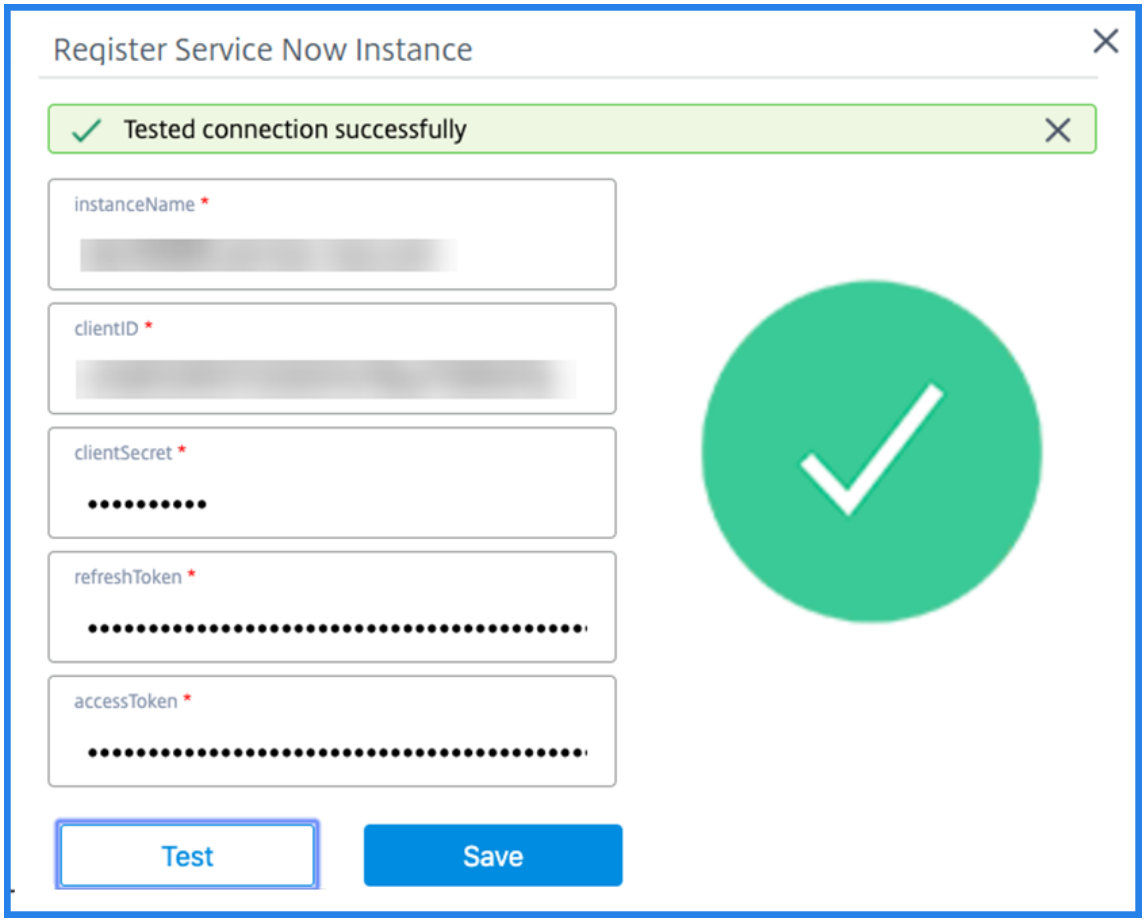
1. Inicie sesión en su instancia de ServiceNow con credenciales de administrador.
2. Vaya a la tienda de ServiceNow. Descargue e instale el **conector ITSM de Citrix**.
3. En el panel **Citrix ITSM Connector**, seleccione **Inicio** y, a continuación, haga clic en **Autenticar**. Escriba el ID de cliente y el secreto que ha anotado en Citrix Cloud.
4. Pruebe la conexión.
5. Guarde la configuración. Aparece un acuse de recibo de ServiceNow que indica que la conexión está activa.
6. Cree un endpoint para acceder a una instancia de ServiceNow. Consulte Crear un punto de enlace para que los clientes accedan a la instancia.
7. Obtenga los tokens de acceso y actualización utilizando el ID de cliente y el secreto de cliente. Consulte Tokens de OAuth.



Paso 3: Agregar una instancia de ServiceNow

1. En la ficha **Administrar**, seleccione Agregar instancia de ServiceNow.

2. Especifique el **nombre de la instancia**, el **ID del cliente, el secreto**del cliente, el**token de actualización**y el**token de acceso**.
3. Haga clic en **Test**.



La instancia de ServiceNow ahora está conectada al servicio ITSM Adapter.

4. Después de probar correctamente la conexión, haga clic en **Guardar** para agregar una instancia de ServiceNow.

Paso 4: Probar la generación automática de tíquets de ServiceNow en ADM

1. Inicie sesión en NetScaler ADM.
2. Vaya a **Cuenta > Notificaciones** y selecciona **ServiceNow**.
3. Seleccione el perfil ServiceNow de la lista.
4. Haga clic en **Probar** para generar automáticamente un tíquet de ServiceNow y verificar la configuración.

   Si quiere ver los tíquets de ServiceNow en la GUI de NetScaler ADM, seleccione **Tíquets de ServiceNow**.

Configurar las notificaciones de ServiceNow en ADM

Después de registrar la instancia de ServiceNow en el adaptador ITSM, puede configurar notificaciones de ServiceNow para los siguientes eventos en la GUI de NetScaler ADM:

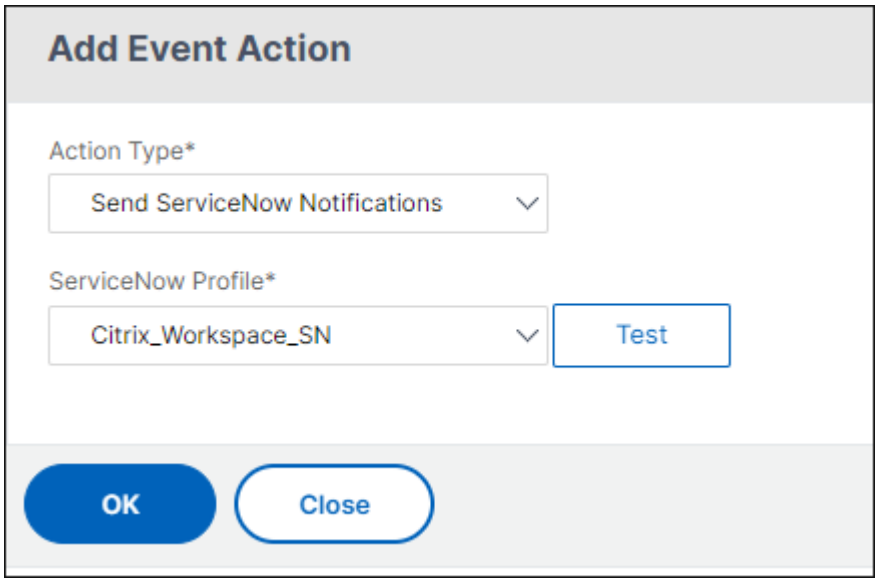
> **Importante**
>
> Esta función es compatible con ServiceNow Cloud.

- **Eventos de NetScaler**: NetScaler ADM puede generar los incidentes de ServiceNow para el conjunto seleccionado de eventos de NetScaler a partir de instancias de NetScaler administradas seleccionadas.

  Para enviar notificaciones de ServiceNow para eventos de NetScaler desde las instancias administradas, debe configurar una regla de evento y asignar la acción de regla como **Enviar notificaciones de ServiceNow**.

  Cree una regla de eventos en el ADM navegando a **Infraestructura > Eventos > Reglas**. Para obtener más información, consulte Enviar notificaciones de ServiceNow.

- **Análisis de aplicaciones**: NetScaler ADM puede generar incidentes de ServiceNow para las aplicaciones que sobrepasen el umbral especificado.



  En este ejemplo, se genera un incidente de ServiceNow cuando la puntuación de aplicaciones de la aplicación cae por debajo de 90.

- **Los eventos del certificado SSL y de la licencia ADM**: NetScaler ADM puede generar los incidentes de ServiceNow para los eventos de caducidad del certificado SSL y de caducidad de la licencia ADM.

  Para enviar notificaciones de ServiceNow sobre la caducidad de un certificado SSL, consulte Caducidad del certificado SSL.

Para enviar notificaciones de ServiceNow sobre la caducidad de una licencia ADM, consulte Caducidad de la licencia de NetScaler ADM.

Exportar o programar informes de exportación

January 30, 2024

En NetScaler ADM, puede exportar un informe completo para la función NetScaler ADM seleccionada. Este informe proporciona una visión general de la asignación entre las instancias, las particiones y los detalles correspondientes.

NetScaler ADM muestra informes de exportación programados específicos de funciones bajo funciones de ADM individuales, que puede ver, modificar o eliminar. Por ejemplo, para ver los informes de exportación de instancias de NetScaler, vaya a **Red > Instancias > NetScaler** y haga clic en el icono de exportación. Puede exportar estos informes en formato PDF, JPEG, PNG y CSV.

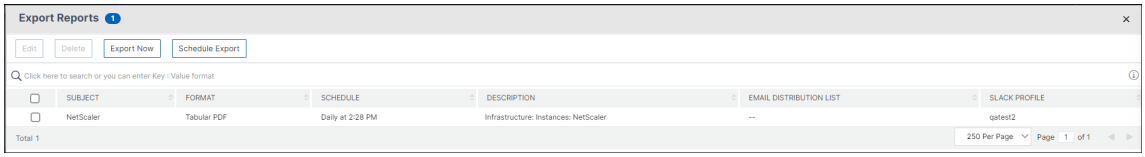
En **Exportar informes**, puede realizar las siguientes acciones:

- Exportar un informe a un equipo local
- Programar informes de exportación
- Ver, modificar o eliminar los informes de exportación programados

Exportar un informe

Para exportar un informe del ADM al equipo local, realice los siguientes pasos:

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.
2. Seleccione **Exportar ahora**.
3. Seleccione una de las siguientes opciones de exportación:
    - **Instantánea**: Esta opción exporta informes ADM como una instantánea.
    - **Tabular**: Esta opción exporta informes ADM en formato tabular. También puede elegir cuántos registros de datos exportar en formato tabular



4. Seleccione el formato de archivo que quiere guardar el informe en el equipo local.
5. Haga clic en **Exportar**.

Programar informe de exportación

Para programar el informe de exportación a intervalos regulares, especifique el intervalo de recurrencia. NetScaler ADM envía el informe exportado al perfil de correo electrónico o de Slack configurado.

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.
2. Seleccione **Programar exportación** y especifique lo siguiente:
    - **Asunto**: De forma predeterminada, este campo rellena automáticamente el nombre de la función seleccionada. Sin embargo, puede reescribirlo con un título significativo.
    - **Opción Exportar** - Exportar informes ADM en una instantánea o un formato tabular. También puede elegir cuántos registros de datos exportar en formato tabular
    - **Formato**: Seleccione el formato de archivo que quiere recibir el informe en el perfil de correo electrónico o slack configurado.
    - **Recurrencia**: Seleccione **Diaria**, **Semanal**o **Mensual** de la lista.
    - **Descripción**: Especifique la descripción significativa de un informe.
    - **Hora de exportación**: Especifique a qué hora quiere exportar el informe.
    - **Correo electrónico**: A ctive la casilla de verificación y seleccione el perfil en el cuadro de lista. Si quiere agregar un perfil, haga clic en **Agregar**.
    - **Slack**: Seleccione la casilla de verificación y selecciona el perfil en el cuadro de lista. Si quiere agregar un perfil, haga clic en **Agregar**.
3. Haga clic en **Programar**.

Ver y modificar los informes de exportación programados

Para ver los informes de exportación, realice lo siguiente:

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.

   La página **Exportar informe** muestra todos los informes de exportación específicos de cada función.

2. Seleccione el informe que quiere modificar y haga clic en **Modificar**.

Actualizaciones

January 30, 2024

Cada versión de NetScaler ADM ofrece funciones nuevas y actualizadas con mayor funcionalidad. Citrix recomienda actualizar NetScaler 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 comenzar a actualizar. Para obtener información sobre las licencias de NetScaler ADM, consulte Licencias.

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 NetScaler ADM y siga las instrucciones de este artículo para actualizar el sistema a la versión 14.1 más reciente. Una vez que comienza el proceso de actualización, ADM se reinicia y las conexiones existentes finalizan y vuelven a conectarse cuando finaliza la actualización. La configuración existente se conserva, pero NetScaler ADM no procesa ningún dato hasta que se completa la actualización.

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

Puntos a tener en cuenta antes de actualizar a 14.1:

- Si actualiza desde la versión 11.1 o 12.0 56.x y versiones anteriores, realice los siguientes pasos:

  1. Actualice de la versión existente a 12.0 compilación 57.24.
  2. Actualice a la última versión de la versión 12.1.

3. Actualice a la versión 13.1.
4. Actualice a la versión 14.1.

- Si actualiza desde la compilación 12.0 57.24 y versiones posteriores, actualice primero a la 12.1, luego a la 13.1 y, por último, a la 14.1.
- Si actualiza desde la versión 12.1, primero debe actualizar a la versión 13.0 64.xx y, a continuación, directamente a la versión 14.1
- Si actualiza desde versiones anteriores a 13.0 64.xx, para una mejor experiencia de usuario, actualice primero a 13.0 64.xx y, después, a 14.1.
- Tras la actualización correcta a la versión 14.1 e iniciar sesión en la GUI, se recomienda cambiar la contraseña si utiliza la contraseña predeterminada.

Puntos importantes a tener en cuenta antes de actualizar a 14.1 xx.xx y posteriores

Al actualizar el software ADM a la versión 14.1 xx.xx, también se migra la base de datos ADM. Esta migración de datos se produce porque ADM ahora utiliza PostgreSQL versión 10.11.

> **Nota**
>
> No se admite la reclasificación del software ADM. No intente rebajar de categoría.

Precauciones recomendadas:

- Realice una instantánea del servidor ADM de NetScaler para cada actualización, si va a actualizar a la versión 14.1 xx.xx o posterior.
- Realice una copia de seguridad del servidor NetScaler ADM antes de actualizar.
- Después de la actualización, es posible que deba restablecer las conexiones entre el servidor NetScaler ADM y las instancias administradas. Un mensaje de confirmación le avisa de que las conexiones pueden fallar si continúa.
- Si actualiza a cualquier versión entre 13.1.9.x y 13.1.30.x, NetScaler ADM revierte el paquete de configuración de StyleBooks existente a su versión anterior.

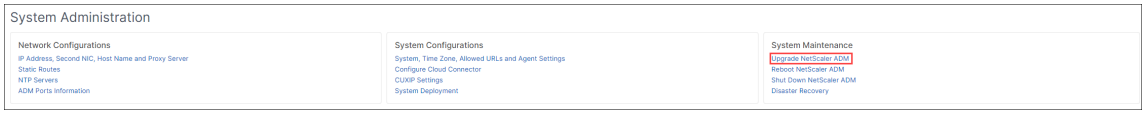
  Para evitar este problema, actualice a la versión 13.1.33.50.
- Para los servidores de NetScaler ADM en configuración de alta disponibilidad, al actualizar la versión, no realice ningún cambio de configuración en ninguno de los nodos.

  > **Advertencia**
  >
  > No actualice el explorador hasta que el proceso de actualización se haya completado cor-

> rectamente. Compruebe la GUI para conocer el tiempo aproximado para completar la actualización.

Actualice un único servidor NetScaler ADM a 14.1 4.x

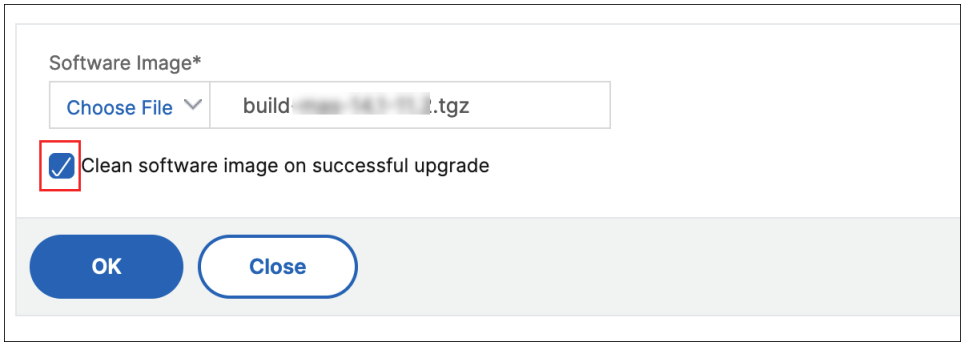
1. Inicie sesión en NetScaler ADM con credenciales de administrador.
2. Vaya a **Configuración** > **Administración** . En **Mantenimiento del sistema**, haga clic en **Actualizar NetScaler ADM**.



3. En la página **Actualizar NetScaler** ADM, seleccione la casilla **Limpiar imagen de software al realizar una actualización correcta para eliminar los archivos de imagen** después de la actualización. Al seleccionar esta opción, se quitan automáticamente los archivos de imagen NetScaler ADM tras la actualización.

> **Nota**
>
> Esta opción está seleccionada de forma predeterminada. Si no selecciona esta casilla de verificación antes de iniciar el proceso de actualización, debe eliminar las imágenes manualmente.

4. A continuación, puede cargar un nuevo archivo de imagen seleccionando **Local** (su máquina local) o **Dispositivo**. El archivo de compilación debe estar presente en el dispositivo virtual NetScaler ADM.



5. Haga clic en **Aceptar**.
   Aparece el cuadro de diálogo Confirmar. Haga clic en **Sí**.

   Se inicia el proceso de actualización.

Después de migrar la configuración, puede iniciar sesión en la GUI de ADM. Al iniciar sesión, los datos históricos comienzan a migrarse en segundo plano mientras se puede continuar trabajando en ADM.

Durante la migración de datos históricos, es posible que algunos de los datos antiguos no estén disponibles. El tiempo necesario para migrar la base de datos depende del tamaño de los datos y del número de tablas.

Puede supervisar la migración de la base de datos mediante la GUI de ADM. Haga clic en **Ver progreso de actualización** y aparecerá el **estado de migración de la base de datos**.

Actualice un par de alta disponibilidad a la versión 14.1

Para los servidores NetScaler ADM en modo de alta disponibilidad, puede actualizar accediendo al nodo activo o a la dirección IP flotante. Ambos servidores NetScaler ADM se actualizan automáticamente a la versión más reciente una vez que se inicia el proceso de actualización en cualquiera de los servidores.

Actualice la implementación de recuperación ante desastres de NetScaler ADM

> **Nota:**
>
> Asegúrese de que la contraseña sea la misma para el par HA y el nodo de recuperación ante desastres.

Actualizar la implementación de recuperación ante desastres de NetScaler ADM es un proceso de dos pasos:

- Actualice los nodos de NetScaler ADM configurados en modo de alta disponibilidad en el sitio principal. Más adelante, debe actualizar el nodo de recuperación ante desastres.
- Asegúrese de haber actualizado los servidores NetScaler ADM que se implementan en alta disponibilidad, antes de actualizar el nodo de recuperación ante desastres.

Actualizar el nodo de recuperación ante desastres de NetScaler ADM

1. Descargue el archivo de imagen de actualización de NetScaler ADM del sitio de NetScaler.
2. Cargue este archivo al nodo de recuperación ante desastres con las credenciales de `nsrecover`.
3. Inicie sesión en el nodo de recuperación ante desastres con las credenciales de `nsrecover`.
4. Desplácese hasta la carpeta donde colocó el archivo de imagen y descomprima el archivo.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Wed May 15 05:27:10 2019 from 10.252.241.103
bash-3.2# cd /var/mps/mps_images
bash-3.2# tar xvfz build-mas-13.0-36.25.tgz
```


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 NetScaler ADM es un proceso de tres pasos. Asegúrese de haber realizado las siguientes tareas antes de actualizar los agentes locales:

1. Actualice los servidores NetScaler ADM implementados en alta disponibilidad.
2. Actualice el nodo de recuperación ante desastres de NetScaler ADM.

   Para obtener más información, consulte Actualizar la implementación de recuperación ante desastres de NetScaler ADM.

Actualizar el agente on-prem

1. Descargue el archivo de imagen de actualización del agente ADM de NetScaler desde el sitio de NetScaler.
2. Cargue este archivo en el nodo del agente mediante `nsrecover` credenciales.
3. Asegúrese de descargar la imagen de actualización del agente correcta.
4. Inicie sesión en el agente on-prem mediante las`nsrecover` credenciales.
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:

   `./installmasagent`

   ```
   bash-3.2# ./installmasagent
   ```


Agregar un disco adicional al servidor NetScaler ADM

Si el requisito de almacenamiento de NetScaler ADM excede el espacio en disco predeterminado (120 GB), puede conectar un disco adicional. Puede conectar más disco en implementaciones de un solo servidor y de alta disponibilidad.

Al actualizar NetScaler ADM desde las versiones 12.1 a 13.10, las particiones que había creado en el disco adicional en la versión anterior siguen siendo las mismas. Las particiones no se eliminan ni se redimensionan.

El procedimiento para conectar más discos sigue siendo el mismo en la compilación actualizada. Ahora puede utilizar la nueva herramienta de partición de discos en NetScaler ADM para crear particiones en el disco recién agregado. También puede utilizar la herramienta para cambiar el tamaño de las particiones en el disco más existente. Para obtener más información sobre cómo conectar más discos y utilizar la nueva herramienta de particionamiento de disco, consulte Cómo conectar un disco adicional a NetScaler ADM.

Autenticación

January 30, 2024

Los usuarios pueden autenticarse internamente mediante NetScaler 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 NetScaler ADM. Si el usuario se autentica externamente, el "nombre externo"del usuario debe coincidir con la identidad de usuario externo registrada en el servidor de autenticación, según el protocolo de autenticación seleccionado.

NetScaler ADM admite la autenticación externa mediante servidores RADIUS, LDAP y TACACS. Este soporte unificado proporciona una interfaz común para autenticar y autorizar a todos los usuarios locales y externos del servidor Autenticación, Autorización y Contabilidad que están accediendo al sistema. NetScaler 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 NetScaler ADM que está 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 la autenticación. Si la autenticación se realiza correctamente, se concede al usuario acceso a NetScaler ADM.

Servidores de autenticación externos

NetScaler ADM envía todas las solicitudes de servicio de autenticación, autorización y auditoría al servidor remoto RADIUS, LDAP o TACACS. El servidor de autenticación, autorización y auditoría remo-

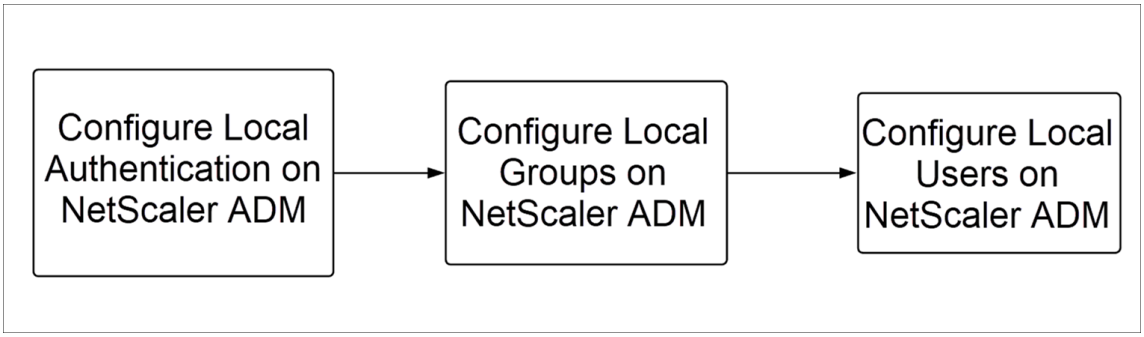
tos recibe la solicitud, valida la solicitud y envía una respuesta a NetScaler ADM. Cuando se configura para utilizar un servidor remoto RADIUS, TACACS o LDAP para la autenticación, NetScaler ADM se convierte en un cliente RADIUS, TACACS o LDAP. En cualquiera de estas configuraciones, los registros de autenticación se almacenan en la base de datos del servidor host remoto. El nombre de cuenta, los permisos asignados y los registros de contabilidad de tiempo también se almacenan en el servidor de autenticación, autorización y auditoría de cada usuario.

Además, puede utilizar la base de datos interna de NetScaler ADM para autenticar a los usuarios localmente. Crear entradas en la base de datos para los usuarios y sus contraseñas y roles predeterminados. También puede seleccionar el orden de autenticación 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 para que incluyan la base de datos interna como copia de seguridad de autenticación de reserva en la lista configurada de servidores de autenticación, autorización y auditoría.

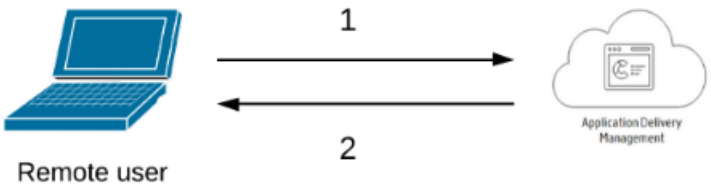
Autenticar usuarios en NetScaler ADM

Puede autenticar a sus usuarios en NetScaler ADM de dos maneras:

- Usuarios locales configurados en NetScaler ADM



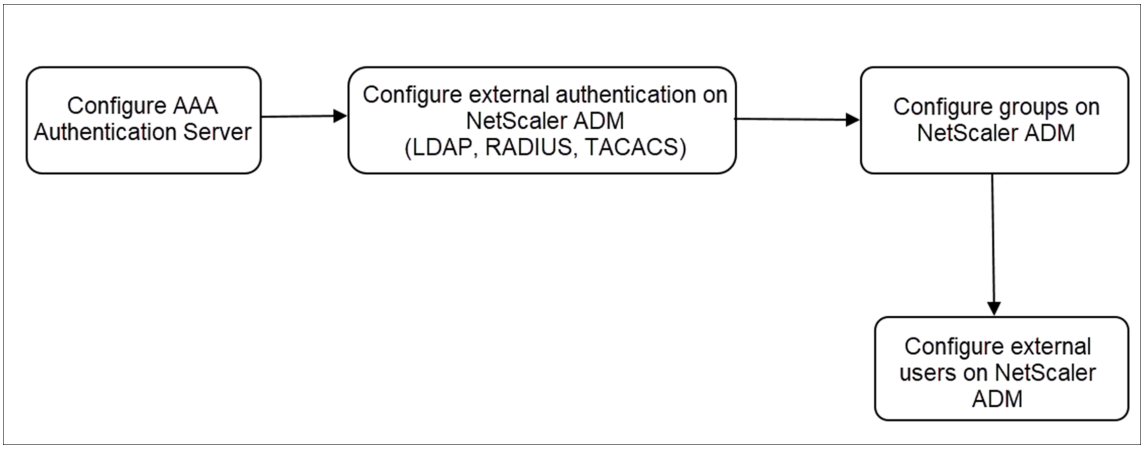
Después de la configuración, el siguiente es el flujo de trabajo para la autenticación de usuario en el servidor local.



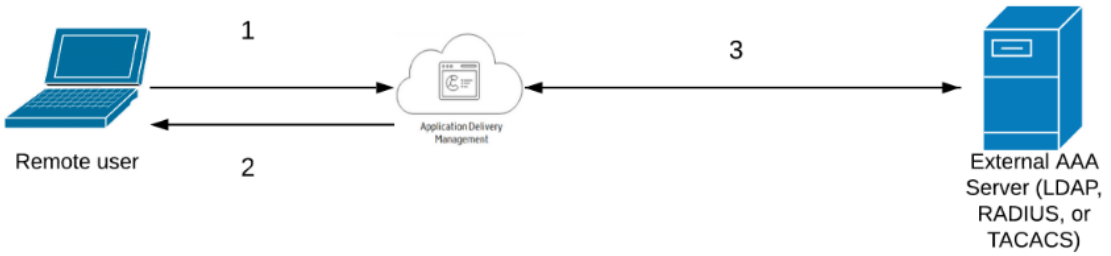
1 —El usuario inicia sesión en NetScaler ADM

2 —NetScaler ADM solicita a los usuarios las credenciales de autenticación y comprueba si las credenciales coinciden en la base de datos de ADM.

- Uso de servidores de autenticación externos



Después de la configuración, el siguiente es el flujo de trabajo para la autenticación de usuario en el servidor externo de autenticación, autorización y auditoría:



1 —El usuario se conecta con NetScaler ADM

2 —NetScaler ADM solicita al usuario las credenciales

3 —NetScaler ADM valida las credenciales de usuario con el servidor externo de autenticación, autorización y auditoría. Si la validación se realiza correctamente, el usuario puede continuar iniciando sesión

Configurar servidores de autenticación externos en NetScaler ADM

January 30, 2024

Después de configurar el servidor LDAP, RADIUS o TACACS, puede agregar estos servidores en NetScaler ADM.

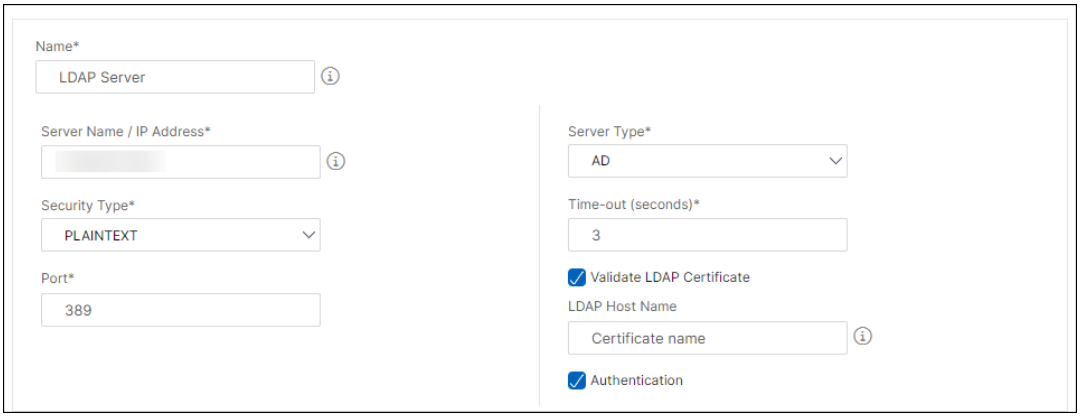
Agregar servidor de autenticación LDAP

January 30, 2024

Al integrar el protocolo LDAP con los servidores de autenticación RADIUS y TACAS, puede utilizar ADM para buscar y autenticar credenciales de usuario desde directorios distribuidos.

1. Vaya a **Configuración > 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/TLS
   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 NetScaler 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, ahora puede obtener la lista de claves públicas almacenadas en el objeto de usuario en el servidor LDAP a través de SSH.



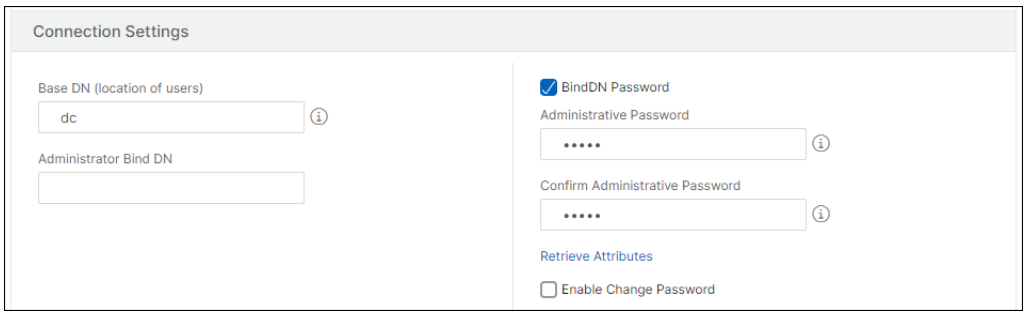
En Configuración de conexión, especifique los siguientes parámetros:

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.

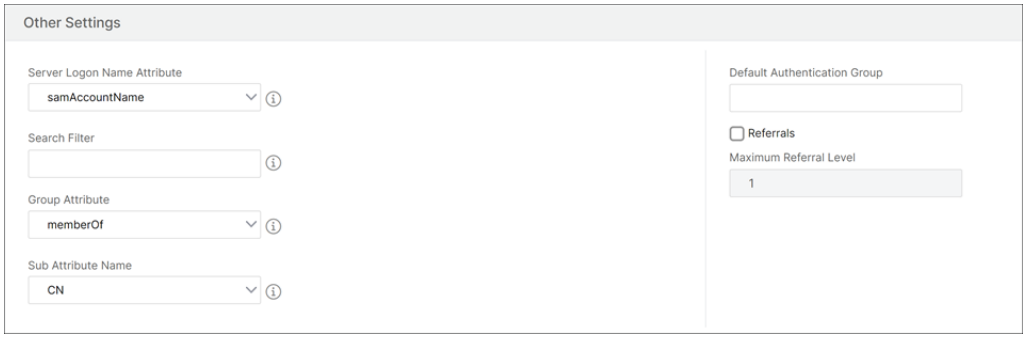
ii. **Filtro de búsqueda**: Configure usuarios externos para la autenticación de dos factores según el filtro de búsqueda configurado en el servidor LDAP. Por ejemplo, vpnallowed=true con ldaploginame `samaccount` y el nombre de usuario proporcionado por el usuario bob produciría una cadena de búsqueda LDAP de: `&(vpnallowed=true)(samaccount=bob)`.

> Nota
>
> De forma predeterminada, los valores del filtro de búsqueda se encierran entre corchetes.

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 NetScaler ADM deben tener los mismos nombres de los miembros del grupo de Active Directory.

5. Habilite los servidores de autenticación externos.

   Para obtener más información sobre cómo habilitar servidores de autenticación externos, consulte Habilitar servidores de autenticación externos y opciones alternativas.

Agregar servidor de autenticación RADIUS

January 30, 2024

1. Vaya a **Configuración > Autenticación**.
2. Seleccione la ficha **RADIUS** y, a continuación, haga clic en **Agregar**.

   En la página **Crear servidor RADIUS**, especifique los siguientes parámetros:

   a) **Nombre**: Especifique un nombre de servidor RADIUS

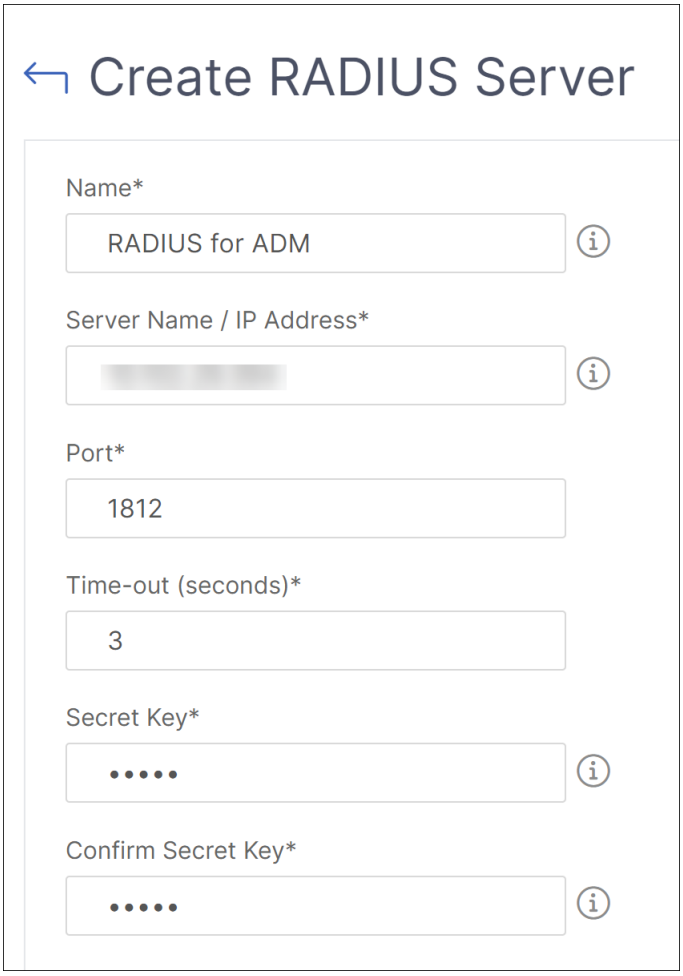
   b) **Nombre del servidor/Dirección IP**: Especifique la dirección IP del servidor RADIUS

   c) **Puerto**: Especifique el número de puerto en el que está alojado el servidor RADIUS. El puerto predeterminado es 1812

   d) Tiempo de**espera (segundos)**: Tiempo en segundos durante el que el sistema NetScaler ADM espera una respuesta del servidor RADIUS

   e) **Clave secreta**: Especifique la clave secreta RADIUS para la autenticación

f) **Confirmar la clave secreta**: Vuelva a especificar la clave para confirmarla



En **Detalles**, especifique los siguientes parámetros:

i. **ID de NAS**: Especifique el ID para enviar el identificador al servidor RADIUS

ii. **Identificador de proveedor de grupo**: Especifique el ID del proveedor para utilizar la extracción de grupos RADIUS

iii. **Prefijo de grupo**: Cadena que precede a los nombres de grupo dentro de un atributo RADIUS para la extracción de grupos RADIUS

iv. **Tipo de atributo de grupo**: Especifique el tipo de atributo para la extracción del grupo RADIUS

v. **Separador de grupos**: Cadena que delimita los nombres de grupos dentro de un atributo RADIUS para la extracción de grupos RADIUS

vi. **Identificador del proveedor de la dirección IP**: El ID del proveedor en RADIUS indica la IP de la intranet. Un valor de 0 indica que el atributo no está codificado por el proveedor.

vii. **Identificador de proveedor de contraseña**: Contraseña de ID de proveedor en la respuesta de RADIUS para extraer la contraseña del usuario

viii. **Tipo de atributo de dirección IP**: Atributo de dirección IP remota para que el RADIUS responda

ix. **Tipo de atributo de contraseña**: El atributo de contraseña para que el RADIUS responda

x. **Codificación de contraseñas**: Seleccione pap, chap, mschapv1 o mschapv2 de la lista. Esto indica cómo se deben codificar las contraseñas en los paquetes RADIUS que viajan del sistema al servidor RADIUS.

xi. **Grupo de autenticación predeterminado**: Grupo predeterminado para elegir cuando la autenticación se realiza correctamente, además de los grupos extraídos

Seleccione Contabilidad si quiere que el dispositivo registre la información de auditoría con el servidor RADIUS.

3. Haga clic en **Crear**.

   El servidor RADIUS ahora está configurado.

4. Habilite los servidores de autenticación externos.

   Para obtener más información sobre cómo habilitar servidores de autenticación externos, consulte Habilitar servidores de autenticación externos y opciones alternativas.

Agregar servidor de autenticación TACACS

January 30, 2024

1. Vaya a **Configuración > Autenticación**.
2. Seleccione la ficha **TACACS** y, a continuación, haga clic en **Agregar**.
3. En la página **Crear TACACS**, especifique los siguientes parámetros:

   a) **Nombre**: Especifique un nombre de servidor TACACS

   b) **Dirección IP**: Especifique la dirección IP del TACACS

   c) **Puerto**: Especifique el número de puerto en el que está alojado el servidor TACACS. El puerto predeterminado es 49

   d) Tiempo de**espera (segundos)**: Tiempo en segundos durante el que el sistema NetScaler ADM espera una respuesta del servidor LDAP

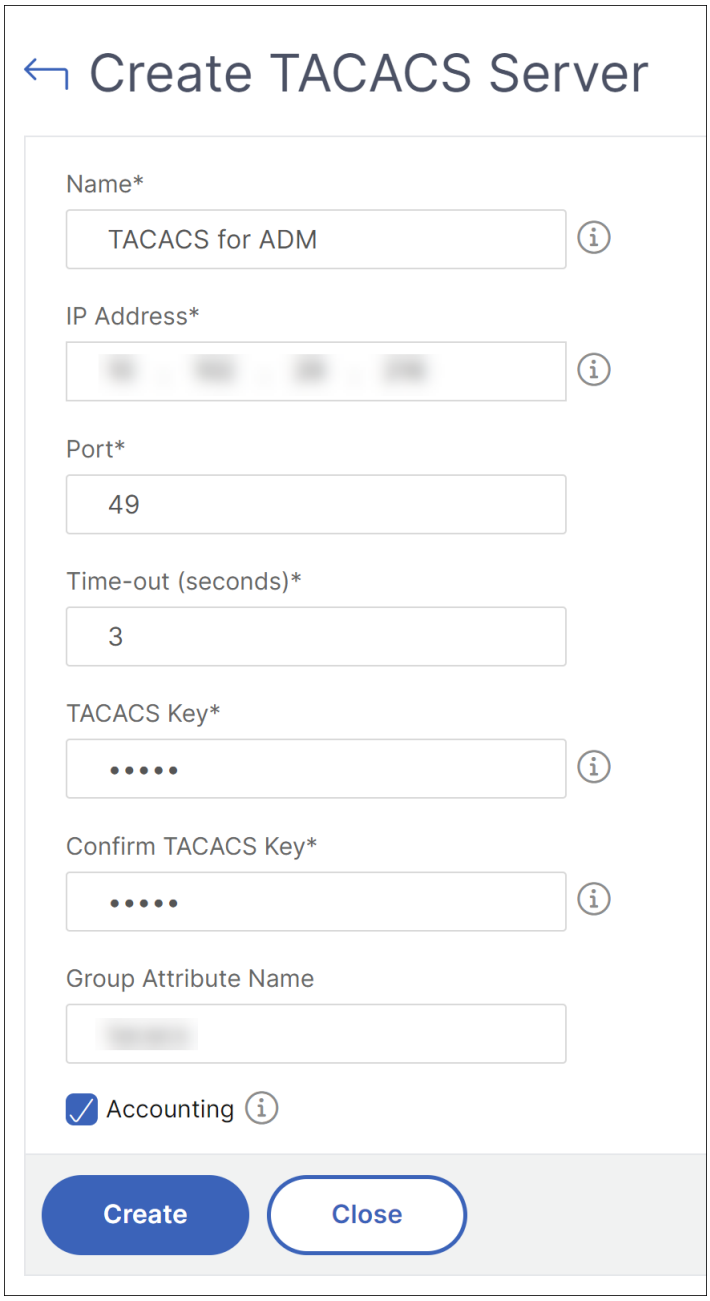
e) Clave**TACACS: especifique la clave** TACACS para la autenticación

f) **Confirme la clave TACACS**: Vuelva a especificar la clave TACACS para confirmarla

g) **Nombre de atributo de grupo**: Especifique el nombre del grupo

Seleccione **Contabilidad** si quiere que el dispositivo registre la información de auditoría con el servidor TACACS.

4. Haga clic en **Crear**.



5. Habilite los servidores de autenticación externos.

Para obtener más información sobre cómo habilitar servidores de autenticación externos, consulte Habilitar servidores de autenticación externos y opciones alternativas.

Usuarios en NetScaler ADM

January 30, 2024

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.

Para obtener más información sobre la configuración de usuarios, consulte Configurar usuarios.

> Nota
>
> Si los usuarios están en Active Directory, asegúrese de que el nombre del grupo en NetScaler ADM sea el mismo que el del grupo Active Directory del servidor externo.

Grupos de usuarios en NetScaler 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 NetScaler ADM:

- Un grupo se define como un conjunto de usuarios que tienen permisos similares.
- Un grupo puede tener una o varias funciones
- 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 NetScaler 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.
Si utiliza la autenticación local, cree usuarios y agréguelos a los grupos configurados en NetScaler ADM. A continuación, los usuarios heredan la configuración de esos grupos.

Para obtener más información sobre la configuración de grupos y la asignación de permisos de grupos, consulte Configurar grupos.

Extraer un grupo de servidores de autenticación

January 30, 2024

> **Nota**
>
> La extracción del servidor TACACS se admite desde **NetScaler**ADM 13.0.

NetScaler ADM le permite:

- Extraiga la lista de grupos a los que pertenece un usuario en el servidor de autenticación externo.
- Asignarlos a la configuración de grupo que coincida con los grupos configurados en el servidor externo.

Ventajas:

- No es necesario crear usuarios en NetScaler ADM, ya que se administran en el servidor externo.
- NetScaler 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.

Habilite los servidores de autenticación externos y las opciones de respaldo

January 30, 2024

La opción alternativa permite que la autenticación local se sustituya si se produce un error en la autenticación del servidor externo. Un usuario configurado tanto en NetScaler ADM como en el servidor de autenticación externo puede iniciar sesión en NetScaler ADM, incluso si los servidores de autenticación externos configurados están inactivos o no se puede acceder a ellos. Para garantizar que la autenticación alternativa funcione:

- Los usuarios que no sean nsroot deben poder acceder a NetScaler ADM si el servidor externo está inactivo o no se puede acceder a él

- Debe agregar al menos un servidor externo

NetScaler ADM también admite un sistema unificado de protocolos de autenticación, autorización y contabilidad (AAA) (LDAP, RADIUS y TACACS), junto con la autenticación local. Este soporte unificado proporciona una interfaz común para autenticar y autorizar a todos los usuarios y clientes AAA externos que acceden al sistema.

NetScaler 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, NetScaler 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 en NetScaler ADM. Puede agregar cualquier tipo de servidores de autenticación externos compatibles (RADIUS, LDAP y TACACS).

Por ejemplo, considere que quiere agregar cuatro servidores de autenticación externos y configurar dos servidores RADIUS, un servidor LDAP y un servidor TACACS. NetScaler ADM intenta autenticarse con los servidores externos en función de las configuraciones. En este caso de ejemplo, NetScaler ADM intenta:

- Conéctese con el primer servidor RADIUS
- Conéctese con el segundo servidor RADIUS, si la autenticación ha fallado con el primer servidor RADIUS
- Conéctese con el servidor LDAP, si la autenticación ha fallado con ambos servidores RADIUS
- Conéctese con el servidor TACACS si la autenticación ha fallado tanto con los servidores RADIUS como con el servidor LDAP.

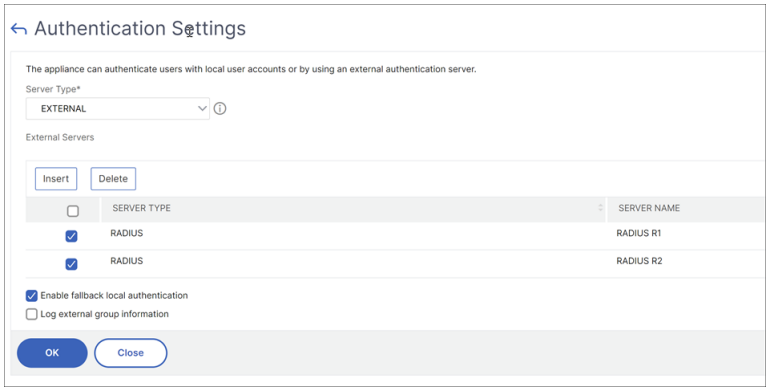
> Nota
>
> Puede configurar hasta 32 servidores de autenticación externos en NetScaler ADM.

Configurar servidores externos de reserva y cascada

1. Vaya a **Configuración > Autenticación**.
2. En la página **Autenticación**, haga clic en **Configuración**
3. En la página **Configuración de autenticación**, seleccione **EXTERNO** en la lista de **tipos de servidor** (solo se pueden conectar en cascada los servidores externos).
4. Haga clic en **Insertar**, en la página **Servidores externos**, seleccione uno o varios servidores de autenticación para conectarlos en cascada.

5. Seleccione la casilla **Habilitar la autenticación local alternativa** si quiere que la autenticación local se sustituya si se produce un error en la autenticación externa.
6. Seleccione la casilla **Registrar la información del grupo externo** si quiere capturar la información del grupo de usuarios externos en el registro de auditoría del sistema.
7. Haga clic en **Aceptar** para cerrar la página.

   Los servidores seleccionados se muestran en Servidores externos:



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.

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, un usuario ya debe tener una cuenta creada en un sistema que pueda ser interrogada por el mecanismo de autenticación, o debe crearse 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, NetScaler ADM admite la autenticación externa con 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 requerido para identificar al usuario en NetScaler 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 y qué programas que se ejecutan en nombre de los usuarios pueden hacer. De esta manera, el control de acceso busca evitar actividades que puedan conducir a una infracción 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. NetScaler ADM permite un control de acceso (RBAC) detallado y basado en funciones mediante el cual los administradores pueden proporcionar permisos de acceso a los usuarios en función de las funciones de los usuarios individuales de una empresa. El RBAC en NetScaler ADM se logra mediante la creación de directivas de acceso, roles, grupos y usuarios.

Control de acceso por roles

January 30, 2024

NetScaler ADM proporciona un control de acceso (RBAC) detallado y basado en roles, con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales de su 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, se puede permitir a un usuario realizar todas las operaciones de red, mientras que otro 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 los usuarios o grupos en función de condiciones específicas. En NetScaler ADM, la creación de roles y directivas es específica de la función RBAC en NetScaler. 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. Un administrador de aplicaciones debe poder acceder únicamente a los recursos dentro del ámbito.

Ejemplo:

Chris, el jefe del grupo ADC, es el superadministrador de NetScaler ADM en su organización. Chris 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 también tener acceso de solo lectura para las operaciones de administración del sistema.

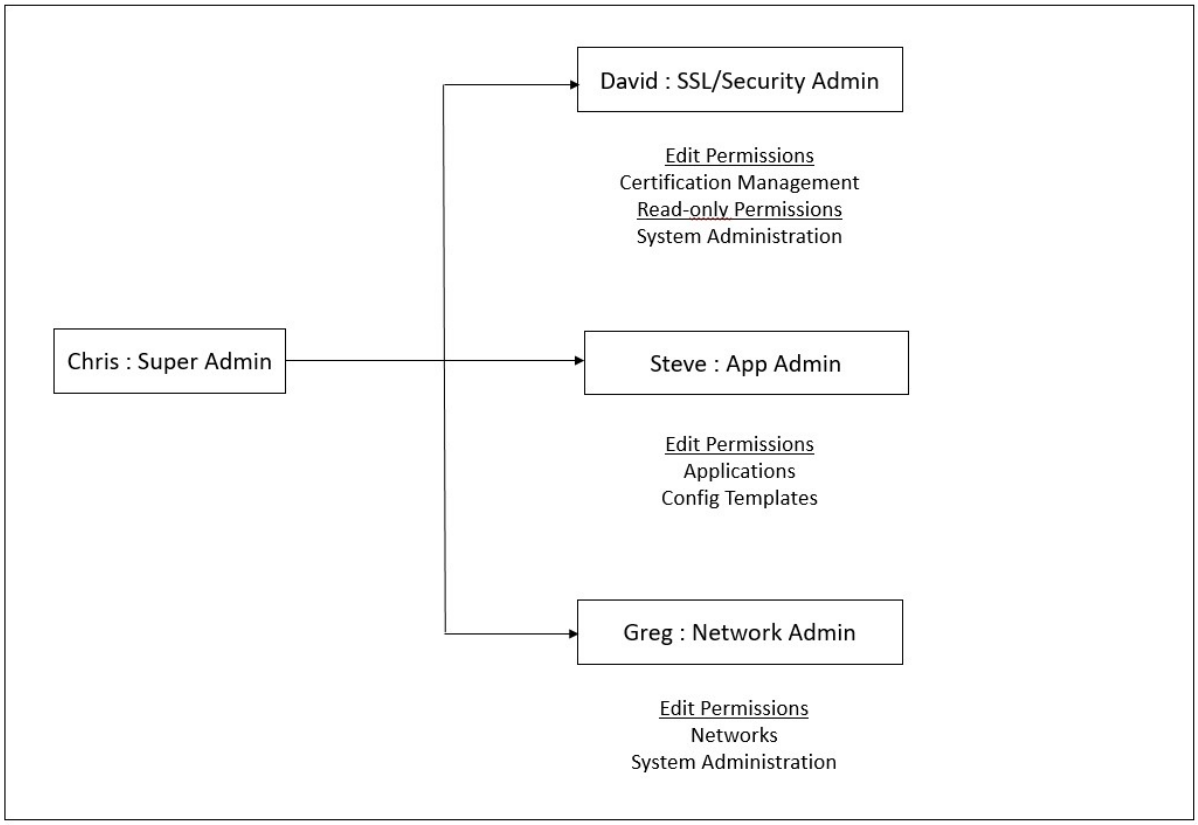
Steve, un administrador de aplicaciones, necesita acceso solo a aplicaciones específicas y a plantillas de configuración específicas.

Greg, un administrador de red, necesita acceso a la administración de sistemas y redes.

Chris también debe proporcionar RBAC para todos los usuarios, independientemente del hecho de que sean locales o externos.

Los usuarios de NetScaler ADM pueden autenticarse localmente o se pueden autenticar 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 NetScaler ADM:

- **Analytics**: RBAC no es totalmente compatible con los módulos de análisis. La compatibilidad con RBAC se limita al nivel de instancia y no se aplica a nivel de aplicación en los módulos de análisis Web Insight, SSL Insight, Gateway Insight, HDX Insight y WAF Security Violations. 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 NetScaler 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 los paquetes de configuración.
  - No se admite el permiso de acceso para StyleBook o paquetes de configuración específicos
    Ejemplo: Si ya hay un paquete de configuración en la instancia, los usuarios pueden modificar la configuración en una instancia de NetScaler 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. NetScaler Application Delivery Management (ADM) proporciona cuatro directivas de acceso predefinidas:

1. **adminpolicy**. Permite el acceso a todas las funciones de NetScaler ADM. El usuario tiene permisos de visualización y edición, puede ver todo el contenido de NetScaler 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 NetScaler ADM, pero no está autorizado a realizar ninguna operación.
3. **appAdminPolicy**. Otorga permisos administrativos para acceder a las funciones de la aplicación en NetScaler 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 NetScaler ADM, vaya a **Configuración > Usuarios y roles > 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**.

   La sección **Permisos** enumera todas las funciones de NetScaler ADM, con opciones para especificar el acceso de solo lectura, habilitar-inhabilitar o modificar.
4. Haga clic en el icono (+) para expandir cada grupo de entidades en varias entidades.

   a) Seleccione la casilla de verificación de permisos situada junto al nombre de la función para conceder permisos a los usuarios.

   - **Ver:** Esta opción permite al usuario ver la función en NetScaler ADM.
   - **Activar-Inhabilitar:** Esta opción solo está disponible para las **funciones Funciones de red** que permiten habilitar o inhabilitar acciones en NetScaler ADM. El usuario puede habilitar o inhabilitar la función. Además, el usuario también puede realizar la acción **Encuestar ahora**.

     Cuando se concede el permiso **Habilitar-Inhabilitar** a un usuario, también se concede el permiso **Ver**. No puede anular la selección de esta opción.

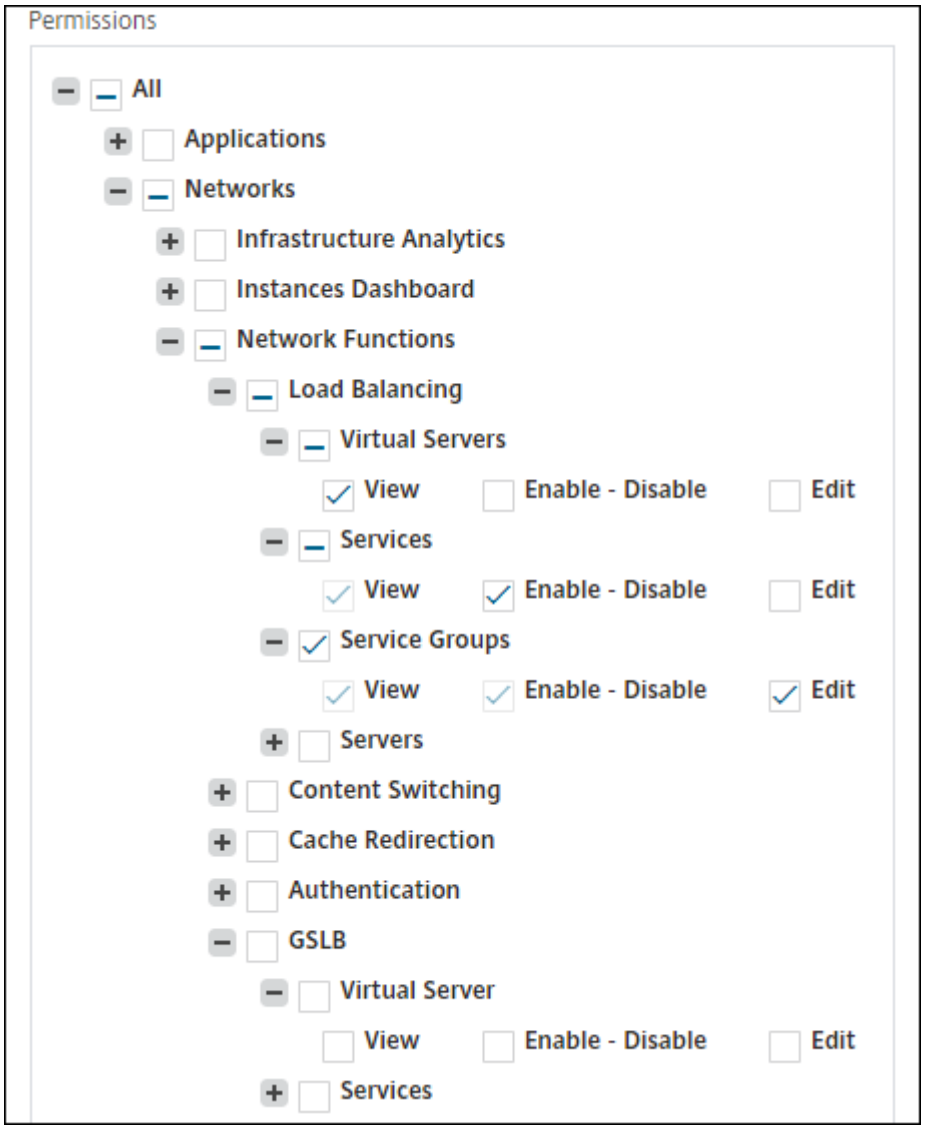
- **Modificar:** esta opción otorga el acceso total al usuario. El usuario puede modificar la función y sus funciones.

  Si concedes el permiso de **edición**, se concederán los permisos de **visualización** y de **activación y desactivación**. No puede anular la selección de las opciones seleccionadas automáticamente.

Si selecciona la casilla de verificación de la función, se seleccionan todos los permisos de la función.

> **Nota:**
>
> Amplíe Equilibrio de carga y GSLB para ver más opciones de configuración.

En la imagen siguiente, las opciones de configuración de la función Equilibrio de carga tienen permisos diferentes:



El permiso de **visualización** se concede a un usuario para la función **Servidores virtuales**. El usuario puede ver los servidores virtuales de equilibrio de carga en NetScaler ADM. Para ver los servidores virtuales, vaya a **Infraestructura > Funciones de red > Equilibrio de carga** y seleccione la ficha **Servidores virtuales**.

El permiso **Habilitar-Inhabilitar** se concede a un usuario para la función **Servicios**. Este permiso también otorga el permiso de **visualización**. El usuario puede habilitar o inhabilitar los servicios enlazados a un servidor virtual de equilibrio de carga. Además, el usuario puede realizar **la acción de encuesta ahora** en los servicios. Para habilitar o inhabilitar los servicios, vaya a **Infraestructura > Funciones de red > Equilibrio de carga** y seleccione la ficha **Servicios**.

> **Nota:**
>
> Si un usuario tiene el permiso **Habilitar-Inhabilitar**, la acción de habilitación o inhabilitación de un servicio está restringida en la página siguiente:
>
> a) Vaya a **Infraestructura > Funciones de red**.
>
> b) Seleccione un servidor virtual y haga clic en **Configurar**.
>
> c) Seleccione la página **Vinculación del servicio de servidor virtual de equilibrio de carga**.
> Esta página muestra un mensaje de error si selecciona **Activar** o **Desactivar**.

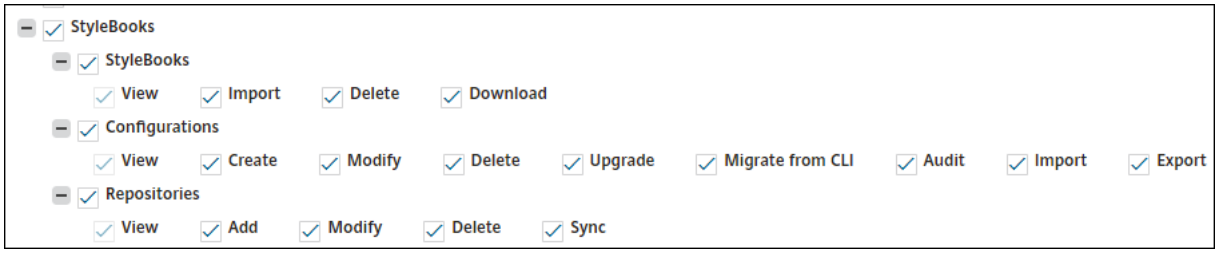
El permiso de **edición** se concede a un usuario para la función **de grupos de servicios**. Este permiso otorga el acceso completo cuando se otorgan los permisos de **visualización** y **activación y desactivación**. El usuario puede modificar los grupos de servicios enlazados a un servidor virtual de equilibrio de carga. Para modificar grupos de servicios, vaya a **Infraestructura > Funciones de red > Equilibrio de carga** y seleccione la ficha **Grupos de servicios**.

5. Haga clic en **Crear**.

Otorgar permisos de StyleBook a los usuarios

Puede crear una directiva de acceso para conceder permisos de StyleBook, como importar, eliminar, descargar, etc.

> **Nota:**
>
> El permiso Ver se activa automáticamente al conceder otros permisos de StyleBook.



Configurar grupos

January 30, 2024

En NetScaler ADM, un grupo puede tener acceso tanto a nivel de entidad como a nivel de recursos. Por ejemplo, un grupo de usuarios puede tener acceso solo a instancias seleccionadas de NetScaler; otro grupo con solo 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 NetScaler ADM.

Puede administrar el acceso de un usuario en NetScaler ADM a nivel individual de las entidades de funciones de red. Puede asignar dinámicamente permisos específicos al usuario o al grupo a nivel de entidad.

NetScaler ADM trata el servidor virtual, los servicios, los grupos de servicios y los servidores como entidades de función de red.

- **Servidor virtual (aplicaciones)**: Equilibrio de carga (lb), GSLB, conmutación de contexto (CS), redirección de caché (CR), autenticación () y NetScaler Gateway (VPN`Auth`)
- **Servicios**: Equilibrio de carga y servicios GSLB
- **Grupo de servicios: grupos** de servicios GSLB y equilibrio de carga
- **Servidores: servidores** de equilibrio de carga

Crear un grupo de usuarios

1. En NetScaler ADM, vaya a **Configuración > Usuarios y funciones > Grupos** .
2. Haga clic en **Agregar**.

   Aparece la página **Crear grupo de sistemas**.
3. En el campo **Nombre de grupo**, escriba el nombre del grupo. La longitud máxima permitida es de 64 caracteres.

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 funciones. También puede ir a **Configuración > Usuarios y funciones > Usuarios** y crear o modificar usuarios.

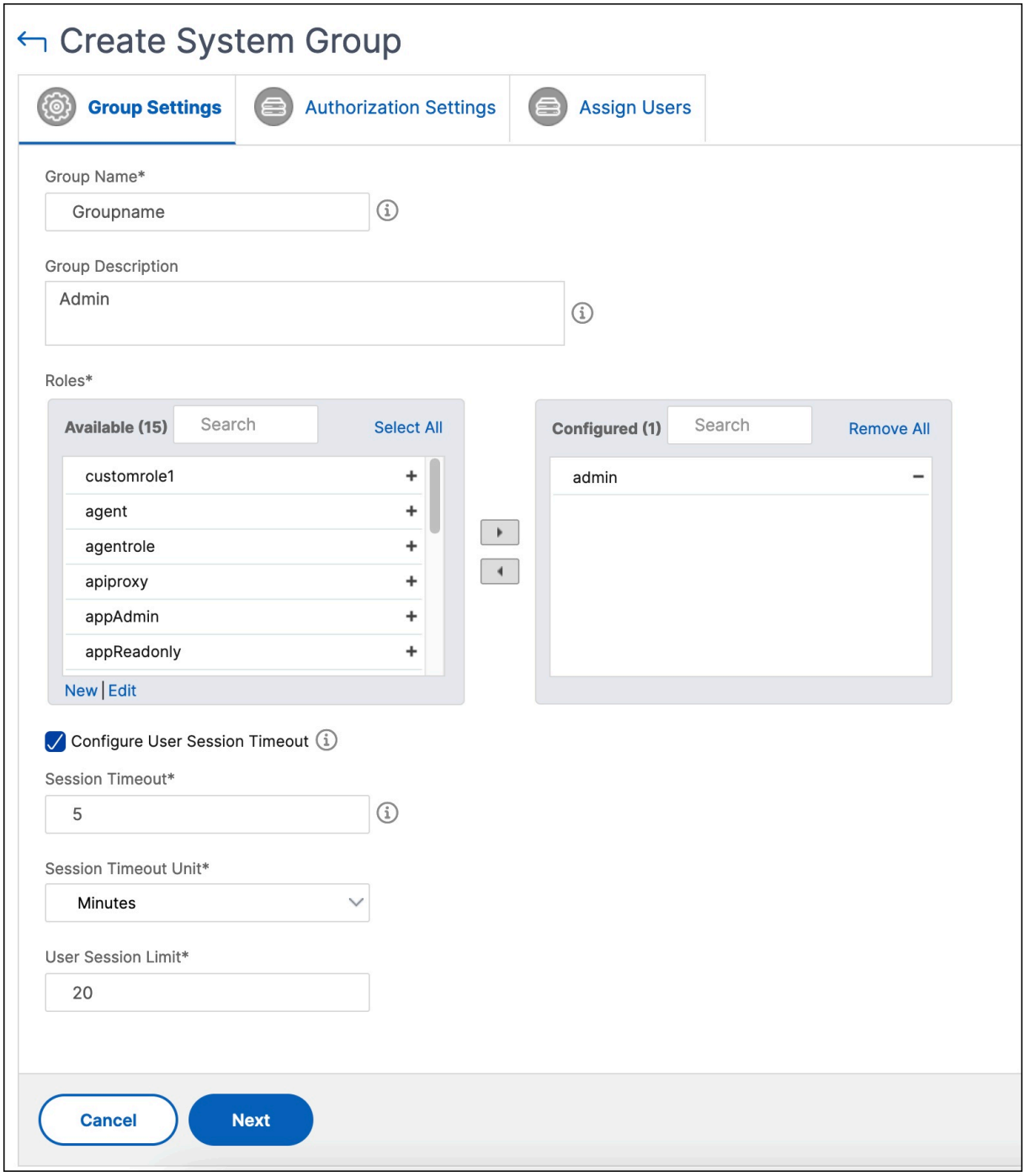
6. Seleccione **Configurar el tiempo de espera de la sesión de usuario** para configurar el período de tiempo que debe permanecer activo un usuario.

   Cuando esté habilitada, especifique los siguientes parámetros:

   - Tiempo de**espera de la sesión**: introduzca el período de tiempo durante el que una sesión de usuario debe permanecer activa. El valor predeterminado es 15.
   - **Unidad de tiempo de espera de sesión**: Seleccione la unidad de tiempo de espera de la lista, en minutos u horas. El valor predeterminado es minutos.

7. En el campo **Límite de sesión de usuario**, introduzca la cantidad máxima de sesiones permitidas por usuario.

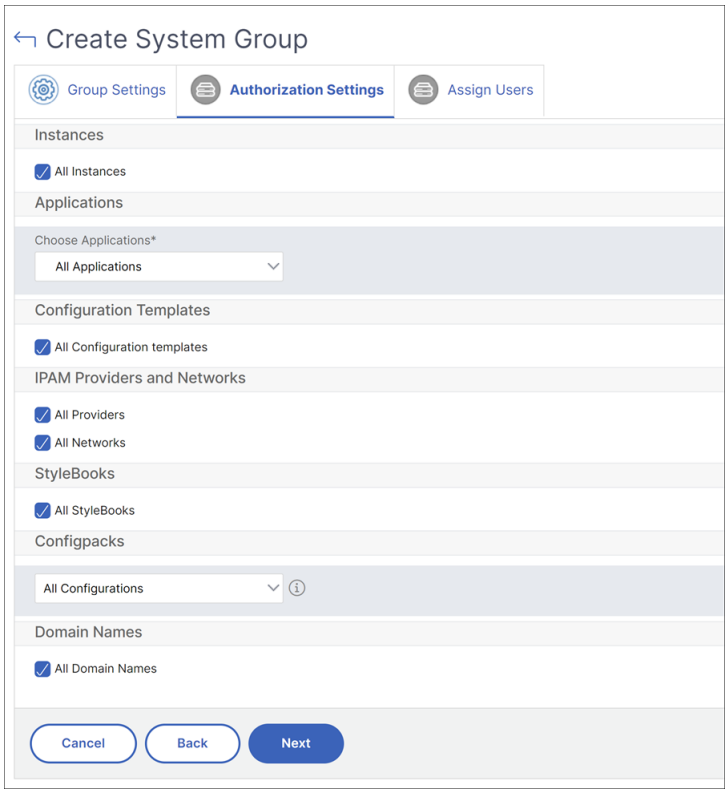
> **Nota:**
>
> Puede configurar hasta 40 sesiones de usuario. De forma predeterminada, se le asignan 20 sesiones de usuario. Sin embargo, si pertenece a los grupos de usuarios de administración y de solo lectura, se le asignan 40 sesiones de usuario de forma predeterminada y este valor no se puede cambiar.



1. Haga clic en **Siguiente**. En la ficha **Configuración de autorización**, puede proporcionar la configuración de autorización para los siguientes recursos:

   - Grupos de Autoscale
   - Instancias
   - Aplicaciones
   - Plantillas de configuración

- StyleBooks
- Paquetes de configuración
- Nombres de dominio



Es posible que quiera seleccionar recursos específicos de las categorías a las que los usuarios pueden tener acceso.

Grupos de Autoscale:

Si quiere seleccionar los grupos de Autoscale específicos que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla de verificación **Todos los grupos de AutoScale** y haga clic en **Agregar grupos de AutoScale**.

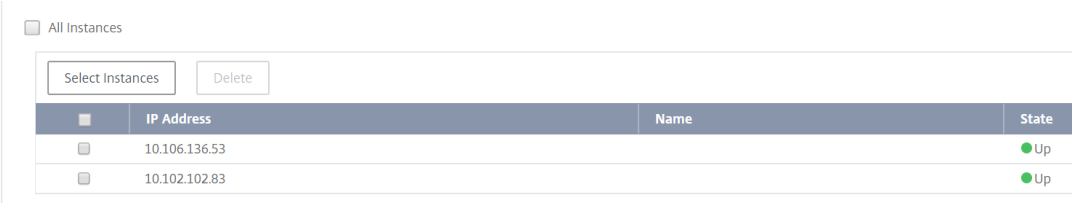
b) Seleccione los grupos de Autoscale necesarios de la lista y haga clic en **Aceptar**.

Instancias:

Si quiere seleccionar las instancias específicas que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todas las instancias** y haga clic en **Seleccionar instancias**.

b) Seleccione las instancias necesarias de la lista y haga clic en **Aceptar**.



Aplicaciones:

La lista **Elegir aplicaciones** le permite conceder acceso a un usuario a las aplicaciones necesarias.

Puede conceder acceso a las aplicaciones sin seleccionar sus instancias. Al conceder a un usuario acceso a una aplicación, el usuario está autorizado a acceder solo a esa aplicación, independientemente de la selección de instancias.

Las siguientes opciones están disponibles:

- **Todas las aplicaciones:** Esta opción está seleccionada por defecto. Agrega todas las aplicaciones que están presentes en el NetScaler ADM.
- **Todas las aplicaciones de instancias seleccionadas:** Esta opción solo aparece si selecciona instancias de la categoría **Todas las instancias**. Agrega todas las aplicaciones presentes en la instancia seleccionada.
- **Aplicaciones específicas:** esta opción le permite agregar las aplicaciones necesarias a las que quiere que accedan los usuarios. Haga clic en **Agregar aplicaciones** y seleccione las aplicaciones necesarias de la lista.
- **Seleccione el tipo de entidad individual:** esta opción le permite seleccionar un tipo específico de entidad de función de red y las entidades correspondientes.

  Puede agregar entidades individuales o seleccionar todas las entidades del tipo de entidad requerido para conceder acceso a un usuario.

  La opción **Aplicar también en entidades enlazadas** autoriza las entidades enlazadas al tipo de entidad seleccionado. Por ejemplo, si selecciona una aplicación y selecciona **Aplicar también en entidades enlazadas**, NetScaler ADM autoriza todas las entidades enlazadas a la aplicación seleccionada.

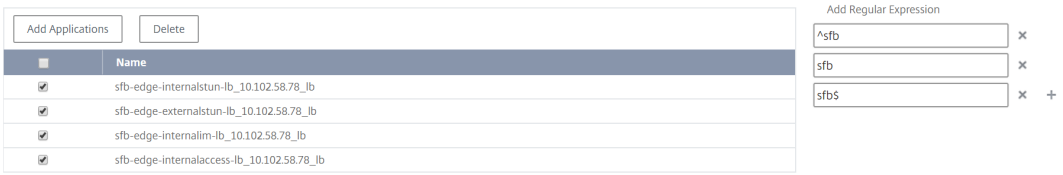
  > **Nota:**
  >
  > Para autorizar entidades vinculadas, seleccione solo un tipo de entidad.

Puede usar expresiones regulares para buscar y agregar las entidades de funciones de red que cumplan con los criterios de expresiones regulares de los grupos. La expresión de expresiones regulares especificada se conserva en NetScaler ADM. Para agregar una expresión regular, lleve a cabo los siguientes pasos:

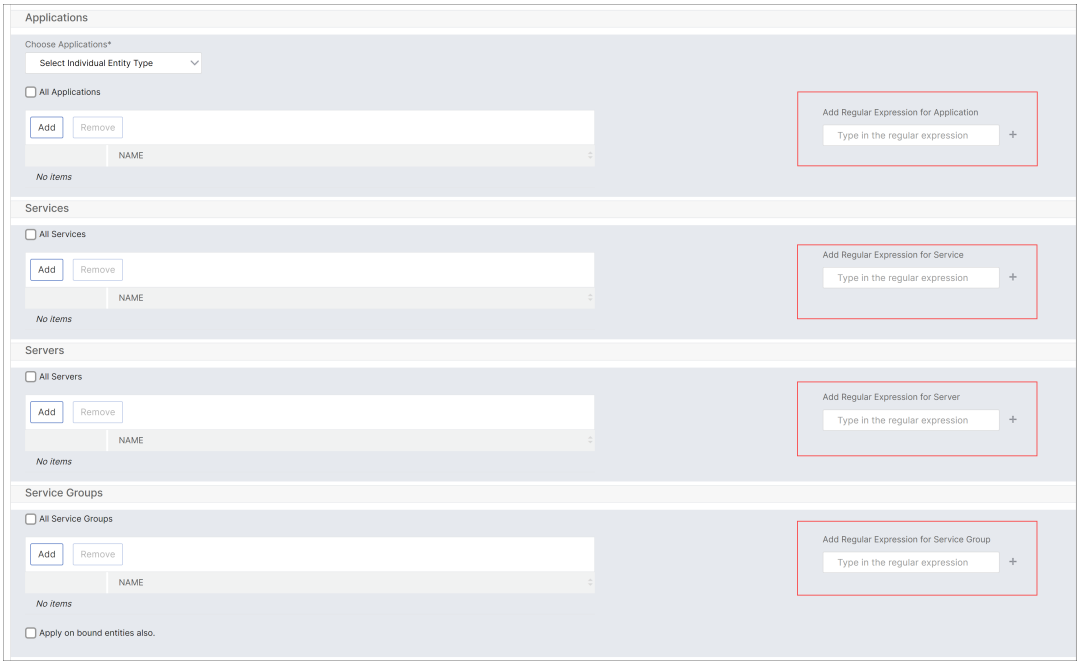
a) Haga clic en **Agregar expresión regular**.

b) Especifique la expresión regular en el cuadro de texto.

En la siguiente imagen se explica cómo usar una expresión regular para agregar una aplicación cuando se selecciona la opción **Aplicaciones específicas** :



En la siguiente imagen se explica cómo utilizar la expresión regular para agregar entidades de función de red al elegir la opción **Seleccionar el tipo de entidad individual** :



Si quiere agregar más expresiones regulares, haga clic en el icono **+**.

> **Nota:**
>
> La expresión regular solo coincide con el nombre del servidor para el tipo de entidad del **servidor** y no con la dirección IP del servidor.

Si selecciona la opción **Aplicar también a las entidades enlazadas** para una entidad detectada, el usuario puede acceder automáticamente a las entidades que están enlazadas a la entidad descubierta.

La expresión regular se almacena en el sistema para actualizar el alcance de la autorización. Cuando las nuevas entidades coinciden con la expresión regular de su tipo de entidad, NetScaler ADM actualiza el alcance de la autorización para las nuevas entidades.

Plantillas de configuración:

Si quiere seleccionar la plantilla de configuración específica que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla de verificación **Todas las plantillas de configuración** y haga clic en **Agregar plantilla de configuración**.

b) Seleccione la plantilla necesaria de la lista y haga clic en **Aceptar**.

StyleBooks:

Si quiere seleccionar el StyleBook específico que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los StyleBooks** y haga clic en **Agregar StyleBook**al grupo. Puede seleccionar StyleBooks individuales o especificar una consulta de filtro para autorizar StyleBooks.

Si quiere seleccionar los StyleBooks individuales, seleccione los StyleBooks en el panel **Individuales StyleBooks** y haga clic en **Guardar selección**.

Si quiere utilizar una consulta para buscar StyleBooks, seleccione el panel **Filtros personalizados**. Una consulta es una cadena de pares clave-valor donde las claves son `name`, `namespace`, y `version`.

También puede utilizar expresiones regulares como valores para buscar y agregar StyleBooks que cumplan los criterios de expresiones regulares para los grupos. Una consulta de filtro personalizada para buscar StyleBooks admite las dos operaciones `And` y `Or`.

Ejemplo :

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
   version=1.0
<!--NeedCopy-->
```

Esta consulta enumera los StyleBooks que cumplen las condiciones siguientes:

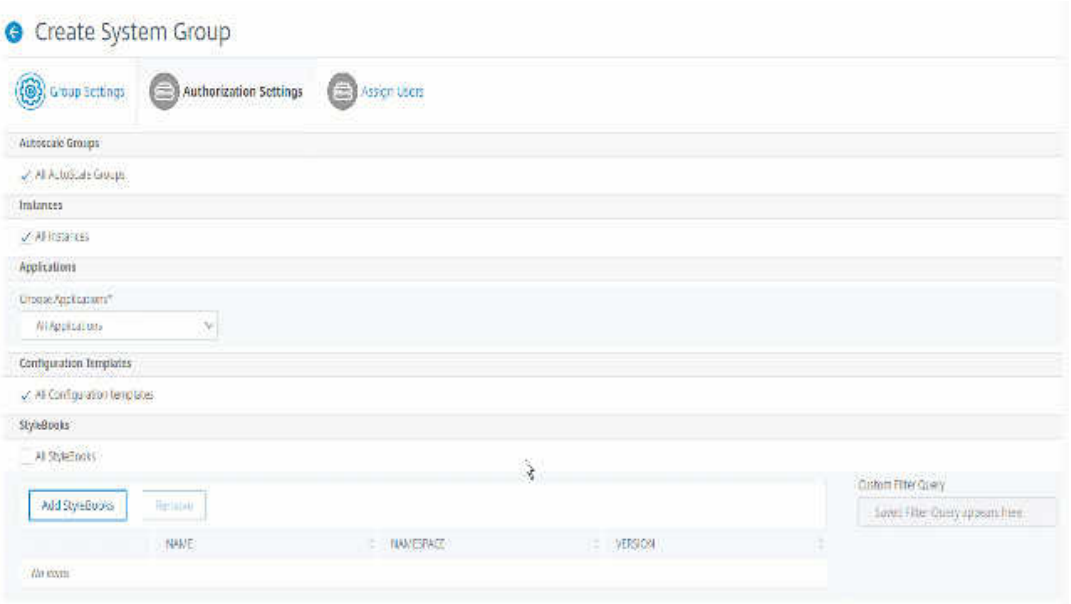
- El nombre de StyleBook es `lb-mon` o `lb`.
- El espacio de nombres StyleBook es `com.citrix.adc.stylebooks`.
- La versión de StyleBook es `1.0`.

Utilice una operación `Or` entre expresiones de valor definidas para la expresión clave.

Ejemplo :

- La consulta `name=lb-mon|lb` es válida. Devuelve los StyleBooks que tienen un nombre `lb-mon` o `lb`.
- La consulta `name=lb-mon | version=1.0` no es válida.

Presione `Enter` para ver los resultados de la búsqueda y haga clic en **Guardar consulta**.



La consulta guardada aparece en la **consulta de filtros personalizados**. Basado en la consulta guardada, el ADM proporciona acceso de usuario a esos StyleBooks.

b) Seleccione los StyleBooks necesarios de la lista y haga clic en **Aceptar**.

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.

Paquetes de configuración:

En los **paquetes de configuración** , selecciona una de las siguientes opciones:

- **Todas las configuraciones**: Esta opción está seleccionada de forma predeterminada. Permite a los usuarios administrar todas las configuraciones que están en ADM.
- **Todas las configuraciones de los StyleBooks**seleccionados : esta opción agrega todos los paquetes de configuración del StyleBook seleccionado.
- **Configuraciones específicas**: Esta opción le permite agregar configuraciones específicas de cualquier StyleBook.
- **Todas las configuraciones creadas por el grupo de usuarios**: esta opción permite a los usuarios acceder únicamente a las configuraciones creadas por los usuarios del mismo grupo.

  Puede seleccionar los paquetes de configuración aplicables al crear grupos y asignar usuarios a ese grupo.

Nombres de dominio:

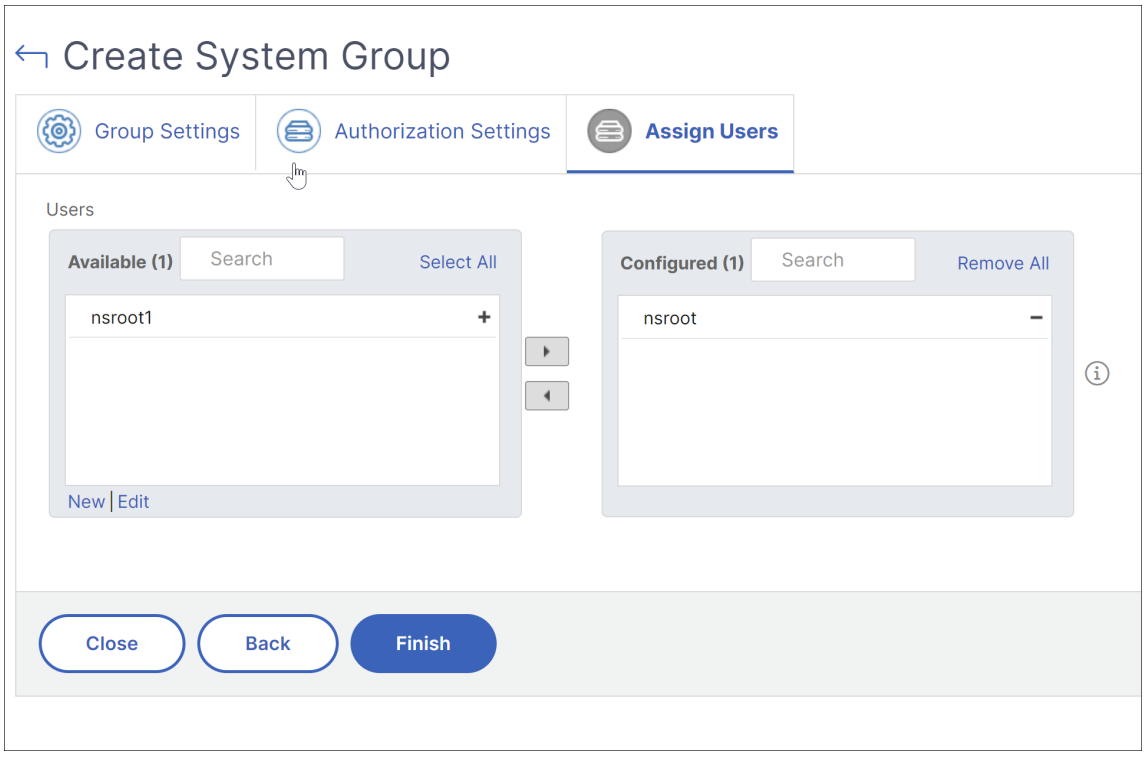
Si quiere seleccionar el nombre de dominio específico que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los nombres de dominio** y haga clic en **Agregar nombre de dominio**.

b) Seleccione los nombres de dominio necesarios de la lista y haga clic en **Aceptar**.

2. Haga clic en **Crear grupo**.
3. En la sección **Asignar usuarios** , seleccione el usuario en la lista **Disponible** y añada el usuario a la lista **Configurado** .

> **Nota:**
>
> También puede agregar usuarios haciendo clic en **Nuevo**.



4. Haga clic en **Finalizar**.

Gestione el acceso de los usuarios a través de múltiples entidades de funciones de red

Como administrador, puede administrar el acceso de los usuarios a nivel individual de las entidades de funciones de red en NetScaler ADM. Además, puede asignar de forma dinámica permisos específicos al usuario o a un grupo a nivel de entidad mediante el filtro de expresiones regulares.

Este documento describe cómo definir la autorización de usuario a nivel de entidad.

Antes de comenzar, cree un grupo. Consulte Configurar grupos en NetScaler ADM para obtener más información.

Caso de uso:

Considere un caso en el que una o más aplicaciones (servidores virtuales) están alojadas en el mismo servidor. Un superadministrador (George) quiere conceder a Steve (un administrador de aplicaciones) acceso solo a App1 y no al servidor de alojamiento.

La siguiente tabla ilustra este entorno, en el que el Servidor-A aloja las aplicaciones App-1 y App-2.

Servidor anfitrión	Aplicación (servidor virtual)	Servicio	Grupo de servicios
Servidor A	App1	App-service-1	App-service-group-1
Servidor A	App2	App-service-2	App-service-group-2

> **Nota:**
>
> NetScaler ADM trata los servidores virtuales, los servicios, los grupos de servicios y los servidores como entidades de funciones de red. El servidor virtual del tipo de entidad se denomina aplicación.

Para asignar permisos de usuario a las entidades de funciones de red, George define la autorización de usuario de la siguiente manera:

1. Vaya a **Cuenta > Administración de usuarios > Grupos** y agrega un grupo.
2. En la ficha **Configuración de autorización**, seleccione Elegir aplicaciones.
3. Elija **Seleccionar tipo de entidad individual**.
4. Seleccione el tipo de entidad **Todas las aplicaciones** y agregue la entidad App-1 de la lista disponible.
5. Haga clic en **Crear grupo**.
6. En **Asignar usuarios**, seleccione los usuarios que requieren el permiso. Para este caso, George selecciona el perfil de usuario de Steve.
7. Haga clic en **Finalizar**.

Con esta configuración de autorización, Steve solo puede administrar App-1 y no otras entidades de funciones de red.

> **Nota:**
>
> Asegúrese de que la opción **Aplicar también a entidades enlazadas** esté desactivada. De lo contrario, NetScaler ADM concede acceso a todas las entidades de funciones de red enlazadas a

> App-1. Como resultado, también otorga acceso al servidor de alojamiento.

Un superadministrador puede especificar las expresiones regulares (expresiones regulares) para cada tipo de entidad. La expresión regular se almacena en el sistema para actualizar el ámbito de autorización del usuario. Cuando las nuevas entidades coinciden con la expresión regular de su tipo de entidad, NetScaler ADM puede conceder a los usuarios acceso de forma dinámica a las entidades de funciones de red específicas.

Para conceder permisos a los usuarios de forma dinámica, el superadministrador puede agregar expresiones regulares en la ficha **Configuración de autorización**.

En este caso, George agrega App* como expresión regular el tipo de entidad Aplicaciones y las aplicaciones que coinciden con los criterios de expresiones regulares aparecen en la lista. Con esta configuración de autorización, Steve puede acceder a todas las aplicaciones que coincidan con la expresión regular App*. Sin embargo, su acceso está limitado solo a las aplicaciones, no al servidor alojado.

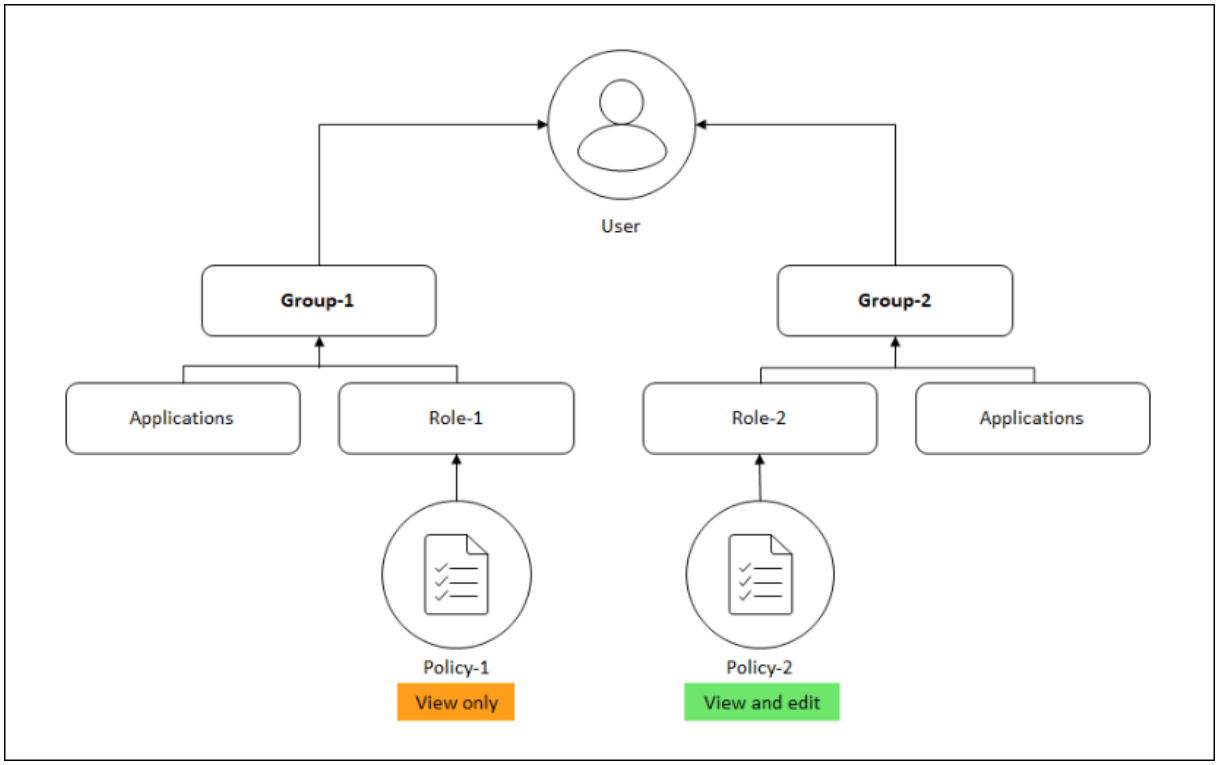
Cómo cambia el acceso de usuario en función del ámbito de autorización

Cuando un administrador agrega un usuario a un grupo que tiene diferentes configuraciones de directiva de acceso, el usuario se asigna a más de un ámbito de autorización y directivas de acceso.

En este caso, el ADM concede al usuario acceso a las aplicaciones según el alcance de autorización específico.

Considere un usuario asignado a un grupo que tiene dos directivas de directiva 1 y directiva 2.

- **Directiva 1**: solo se muestran los permisos para las aplicaciones.
- **Directiva 2**: Ver y modificar los permisos de las aplicaciones.



El usuario puede ver las aplicaciones especificadas en la Directiva 1. Además, este usuario puede ver y modificar las aplicaciones especificadas en la directiva 2. El acceso de edición a las aplicaciones Group-1 está restringido ya que no está en el ámbito de autorización Group-1.

Asignación de RBAC al actualizar NetScaler ADM de 12.0 a versiones posteriores

Cuando actualiza NetScaler ADM de 12.0 a 13.1, no ve las opciones para proporcionar permisos de "lectura y escritura"o "lectura"al crear grupos. Estos permisos se sustituyen por "funciones y directivas de acceso", que ofrecen más flexibilidad para proporcionar permisos basados en funciones a los usuarios. En la siguiente tabla se muestra cómo se asignan los permisos de la versión 12.0 a la versión 13.1:

12.0	Permitir solo aplicaciones	13.1
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 NetScaler Application Delivery Management (ADM), cada rol está vinculado 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 podría conceder permiso para agregar instancias de NetScaler en NetScaler ADM y la otra directiva podría conceder permisos para crear e implementar StyleBooks y configurar instancias de NetScaler.

Cuando varias directivas definen permisos de edición y solo lectura para una sola función, los permisos de edición tienen prioridad.

NetScaler ADM proporciona cuatro funciones predefinidas:

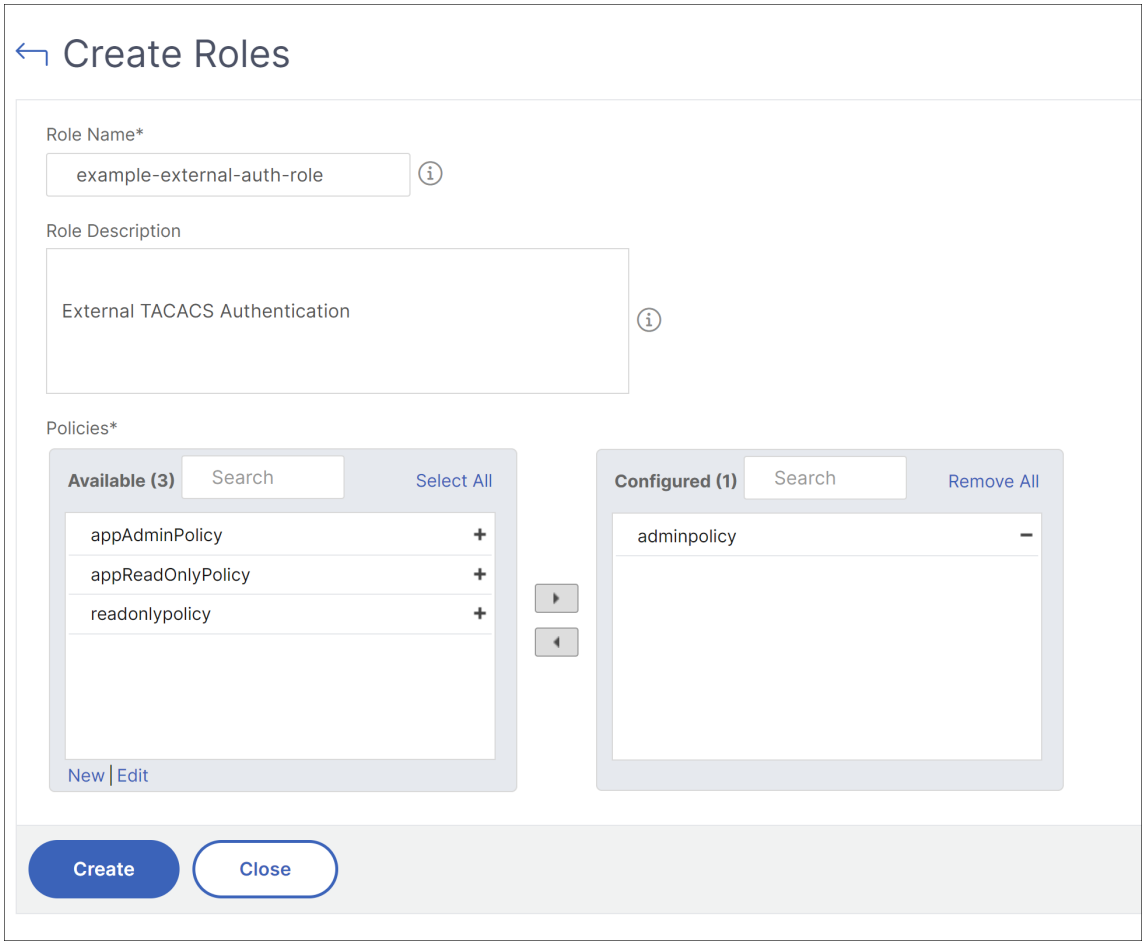
- **administrador**. Tiene acceso a todas las funciones de NetScaler ADM. (Este rol está vinculado a adminpolicy).
- **solo lectura**. Tiene acceso de solo lectura. (Este rol está vinculado a readonlypolicy).
- **appAdmin**. Tiene acceso administrativo solo a las funciones de la aplicación en NetScaler 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 NetScaler ADM, vaya a **Configuración > Usuarios y roles**.
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, NetScaler Application Delivery Management (ADM) tiene un usuario:

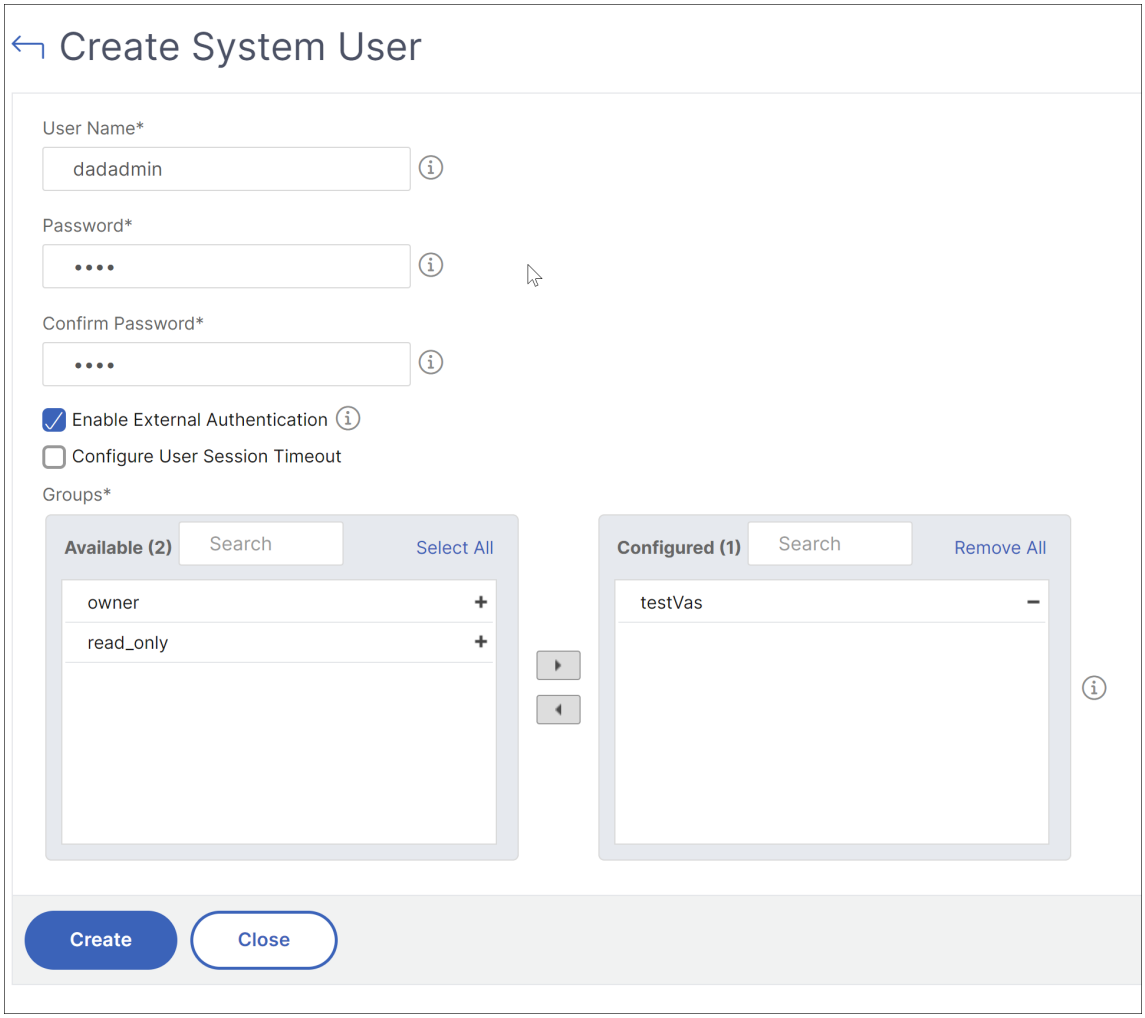
nsroot: el usuario root (nsroot) tiene todos los privilegios administrativos en el dispositivo. El usuario nsroot es el superadministrador de NetScaler ADM.

Puede crear usuarios adicionales configurando cuentas para ellos. Al agregar nuevos usuarios a NetScaler ADM, puede definir sus permisos asignando los grupos, roles 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 NetScaler ADM:

1. En NetScaler ADM, vaya a **Configuración > Usuarios y roles**.
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 NetScaler 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**.

Tareas y recomendaciones prácticas

January 30, 2024

> **Nota:**
>
> - La ficha Tareas **pendientes** pasa a llamarse **Recomendaciones**. En **Recomendaciones**, puede seguir revisando las tareas existentes y hacer clic en **Guide Me** para completar la tarea.
> - La ficha **Archivo** ya no está disponible. En su lugar, puede optar **por descartar** una recomendación de la lista.

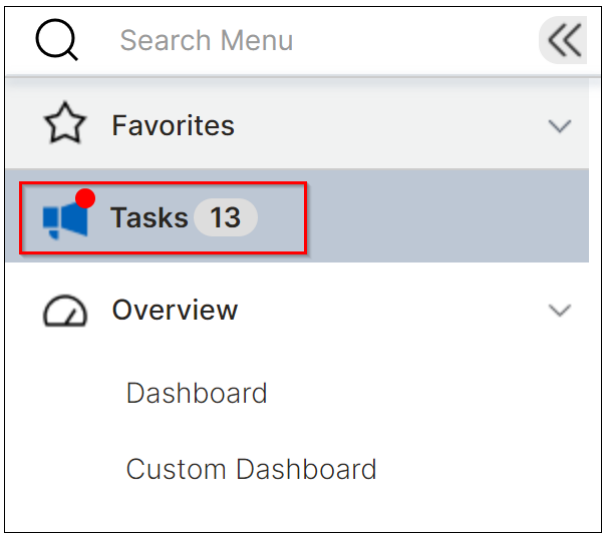
Es posible que haya descubierto cientos de instancias de NetScaler y que haya configurado varios servidores virtuales (aplicaciones) desde cada instancia. Como administrador, debe asegurarse de que todas las instancias de NetScaler y sus aplicaciones se administren de manera eficiente para obtener información que permita priorizar mejor y solucionar problemas.

A medida que amplíes más su infraestructura, es posible que también tengas que concentrarte en los problemas críticos que afectan a sus instancias y aplicaciones y que requieren su atención inmediata. También debe asegurarse de que la implementación de NetScaler ADM sea eficiente, segura y compatible. En función de su uso y suscripción actuales, la función **Tareas** de NetScaler ADM le permite ver tanto las **tareas** procesables en las que debe tomar medidas inmediatas como las **recomendaciones** para garantizar una implementación eficiente.

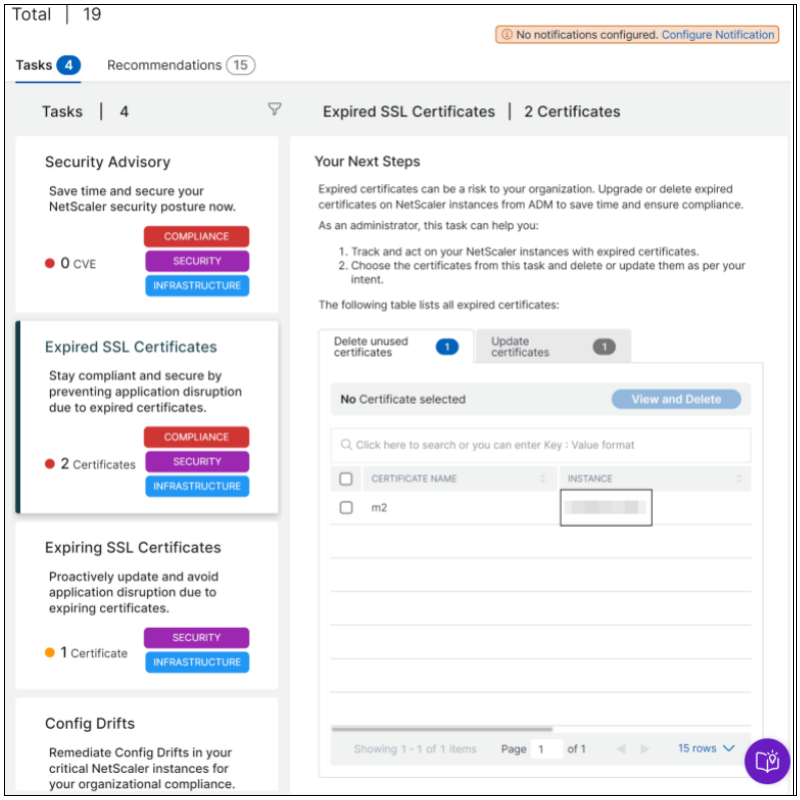
Como administrador, al hacer uso de estas **recomendaciones** y **tareas**prácticas, puede:

- Obtenga visibilidad instantánea de cualquier observación o problema que requiera su acción inmediata.
- Configure las notificaciones para recibir notificaciones cada vez que NetScaler ADM detecte alguna tarea y tome medidas de forma proactiva.
- Logre una implementación eficiente de las instancias de NetScaler ADM y NetScaler.
- Reduzca el tiempo y el esfuerzo cruciales para identificar los problemas críticos.
- Asegúrese de utilizar todas las capacidades de NetScaler ADM, habilite el descubrimiento de productos y las funcionalidades recomendadas por el producto para una administración eficiente de la implementación.

En la GUI de NetScaler ADM, haga clic en **Tareas** para ver tanto las **tareas** como las **recomendaciones**.

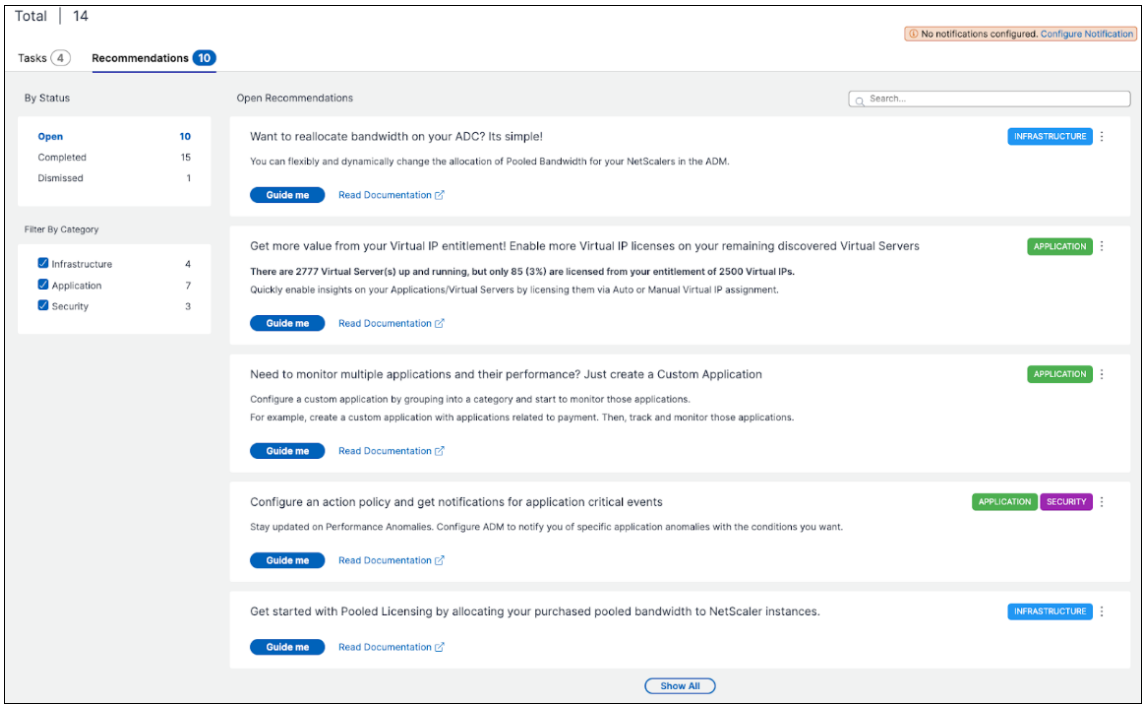


- **Tareas**: Le permite ver una lista de tareas que requieren su atención y acción inmediatas. A medida que amplíe su infraestructura, es posible que algunos problemas críticos pasen desapercibidos y provoquen brechas de seguridad. Por ejemplo, las instancias de NetScaler con CVE requieren atención inmediata y debe tomar medidas inmediatas para garantizar que las instancias se ejecuten en la versión y compilación recomendadas. En **Tareas**, puede obtener esos conocimientos de forma inmediata. En función de su utilización actual, puede ver un total de 4 tareas. Las tareas se muestran en función de la gravedad (crítica y media).



- **Recomendaciones**: Proporciona ciertas recomendaciones basadas en su uso actual para mejorar la implementación de NetScaler ADM. Puede usar la opción **Guíame** para completar cualquier recomendación. Cualquier recomendación que complete con la opción **Guíame** se mueve a Completada. También puede descartar cualquier recomendación, que pasará a la categoría **Rechazada**. Para ver las recomendaciones rechazadas, usa el filtro **Por estado** y selecciona **Rechazadas** para ver las recomendaciones rechazadas.

  También puede usar el **filtro por categoría** para filtrar recomendaciones específicas en función de las categorías (infraestructura, aplicación y seguridad). Como alternativa, también puede usar la barra de **búsqueda**, escribir los primeros caracteres para profundizar en la tarea.



Tareas

En **Tareas**, puede ver las cuatro tareas siguientes en función de la implementación actual de ADM.

- **Certificados SSL caducados**: Proporciona información sobre los certificados SSL caducados instalados en su NetScaler ADM. Seleccione esta tarea para ver las siguientes fichas:

  - **Eliminar certificados no utilizados**: muestra los certificados que no se utilizan en ninguna instancia de NetScaler. Para completar la tarea, revise los certificados no utilizados, seleccione el certificado y haga clic en **Ver y eliminar**.

    Acción recomendada: Se le redirige a **Infraestructura > Panel de control SSL > Certificados SSL: caducados**. Para eliminar un certificado, haga clic en **Eliminar**. Si quiere

actualizar el certificado, selecciónelo y haga clic en **Actualizar**. Para obtener más información, consulta Cómo actualizar un certificado instalado.

- **Actualizar certificados**: muestra los certificados que ya han caducado. Para completar la tarea, revise los certificados, selecciónelos y haga clic en **Ver y actualizar**.

  Acción recomendada: Se le redirige a **Infraestructura > Panel de control SSL > Certificados SSL: caducados**. Seleccione el certificado y haga clic en **Actualizar** o **Eliminar**. Para obtener más información, consulta Cómo actualizar un certificado instalado.

- **Certificados SSL que están a punto de caducar**: Proporciona información sobre los certificados SSL que están a punto de caducar.

  Acción recomendada: seleccione esta tarea para ver las fichas en función del número total de días que faltan para la fecha de caducidad. Para completar la tarea, seleccione el certificado en la ficha y haga clic en **Ver y actualizar**. Se le redirigirá a la página correspondiente en **Infraestructura > Panel de control SSL**. Seleccione el certificado y haga clic en **Actualizar**. Para obtener más información, consulta Cómo actualizar un certificado instalado.

- Diferencias de**configuración:** proporciona información sobre las desviaciones de configuración (diferencia guardada frente a diferencia de ejecución y diferencia de plantilla frente a diferencia de ejecución) en las instancias de NetScaler. Seleccione esta tarea para ver las siguientes fichas:

  - **Instancias con configuración sin guardar**: puede ver las instancias que tienen la configuración sin guardar. Para completar la tarea, seleccione la instancia y haga clic en **Ver y guardar la configuración**.

    Acción recomendada: se le redirigirá a **Infraestructura > Configuración > Auditoría de configuración > Informes de auditoría** y podrá ver las instancias que tienen configuraciones sin guardar. Haga clic en **Guardar configuración** para completar esta tarea. Para obtener más información, consulte la documentación.

  - **Instancias con desviaciones de la plantilla**: puede ver las instancias que tienen desviaciones de plantilla. Para completar la tarea, seleccione la instancia y haga clic en **Ver y ejecutar los comandos correctos**.

    Acción recomendada: se le redirigirá a **Infraestructura > Configuración > Auditoría de configuración > Informes de auditoría** y podrá ver las instancias que tienen desviaciones de plantilla. Siga la documentación para completar la tarea.

- **Asesoramiento de seguridad**: Proporciona información sobre las CVE que afectan a las instancias de NetScaler. Seleccione esta tarea para ver las siguientes fichas:

  - **CVE detectados**: muestra los CVE detectados y las instancias de NetScaler que afectan a los CVE. Para completar esta tarea, seleccione una CVE y haga clic en **Ver y corregir**.

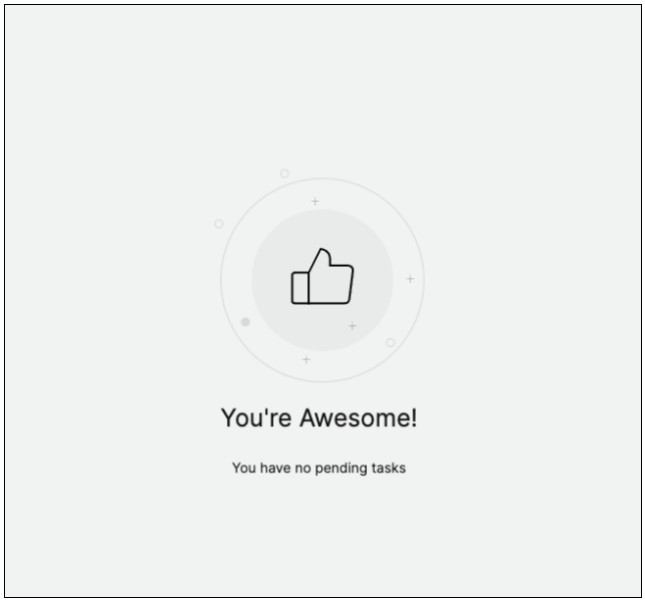
Acción recomendada: se le redirigirá a la página de **consejos de seguridad** en **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**. Siga la documentación para completar la tarea.

- **Instancias afectadas: muestra las instancias**de NetScaler afectadas por los CVE. Para completar la tarea, seleccione la instancia y haga clic en **Ver y corregir.**

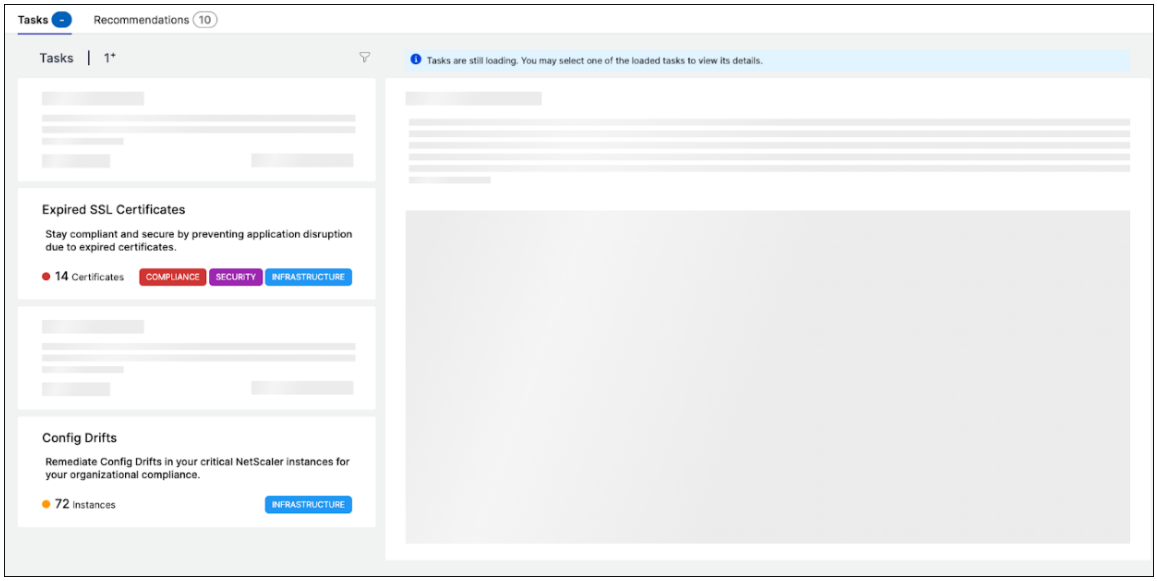
  Acción recomendada: se le redirigirá a la página de **consejos de seguridad** en **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**. Siga la documentación para completar la tarea.

Nota:

- Puede ver la página siguiente si su NetScaler ADM no tiene ninguna tarea pendiente:



- En algunos escenarios, las comprobaciones se realizan en todas las instancias y es posible que se necesite más tiempo para cargar todas las tareas.



Recomendaciones

En la siguiente tabla se describen las recomendaciones que puede ver en la GUI de NetScaler ADM:

> **Nota**
>
> En el caso de las licencias agrupadas, recibirá recomendaciones basadas en sus derechos de licencia agrupados existentes.

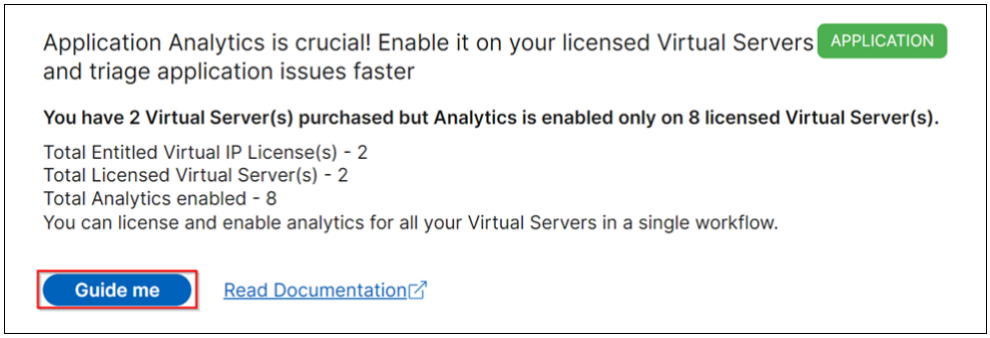
Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
Agregar un ADC	Después de la integración en NetScaler ADM y si no se detecta ninguna instancia de ADC.
Agregue un agente de ADM externo para utilizar al máximo las funciones de NetScaler ADM	Si no hay un agente externo configurado. Puede empezar con un agente integrado. Sin embargo, se requiere un agente externo para utilizar todas las funciones, como los análisis, las licencias agrupadas, etc.
Registrar un ADC de un agente integrado a un agente externo	Tras la integración en NetScaler ADM mediante el flujo de trabajo de Service Connect, las instancias de ADC se incorporan mediante el agente integrado. Puede registrar esas instancias de ADC en un agente externo para utilizar todas las funciones, como el análisis, las licencias agrupadas, etc.

Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
¡El análisis de aplicaciones es crucial! Habilítelo en sus servidores virtuales con licencia y clasifique los problemas de las aplicaciones con mayor rapidez.	Si tiene varios servidores virtuales con licencia pero no tiene habilitados los análisis.
¿Quiere reasignar ancho de banda en su ADC? ¡Es sencillo!	Si las licencias agrupadas se asignan en la GUI de ADC y esas instancias de ADC se descubren en NetScaler ADM, puede realizar la reasignación mediante NetScaler ADM.
¡Saque más provecho de sus derechos de uso de IP virtuales! Habilite más licencias de IP virtuales en los servidores virtuales restantes descubiertos	Si tiene las licencias necesarias, pero no las de todos los servidores virtuales.
Habilite el acceso granular basado en roles para sus usuarios empresariales clave	Si el control de acceso basado en roles (RBAC) aún no está configurado en NetScaler ADM.
Configure reglas y no se pierda ningún evento crítico en sus instancias de ADC	Si aún no se ha configurado una regla de eventos personalizada.
¿Necesita supervisar varias aplicaciones y su rendimiento? Simplemente cree una aplicación personalizada	Si la aplicación personalizada aún no está configurada.
Notifique y nunca se pierda eventos críticos en sus aplicaciones	Si la directiva de acción no está configurada para la desviación de la puntuación de la aplicación, el tiempo de procesamiento del servidor, la latencia de la red del cliente, la latencia de la red del servidor o el tiempo de respuesta.
Evite las interrupciones de uso de las aplicaciones y nunca se pierda los certificados SSL que caducan en una aplicación	Si no hay alertas o notificaciones configuradas para los certificados SSL que vencen.
Asesoramiento de seguridad: Mantenga sus ADC actualizados con los CVEs y las mitigaciones	Si las instancias de ADC tienen algún impacto en el CVE.
Configurar una directiva empresarial y supervisar desviaciones	Si la configuración empresarial de SSL no ha cambiado o sigue siendo la predeterminada.
¿Repite tareas manuales? Cree trabajos de configuración y aplíquelos a varios ADC	Si la tarea **Config Job** aún no está configurada.
Administre y supervise la puntuación de la instancia seleccionando los indicadores personalizados que prefiera.	Si la configuración y los umbrales predeterminados de la **configuración de puntuación de instancia** no se modifican.

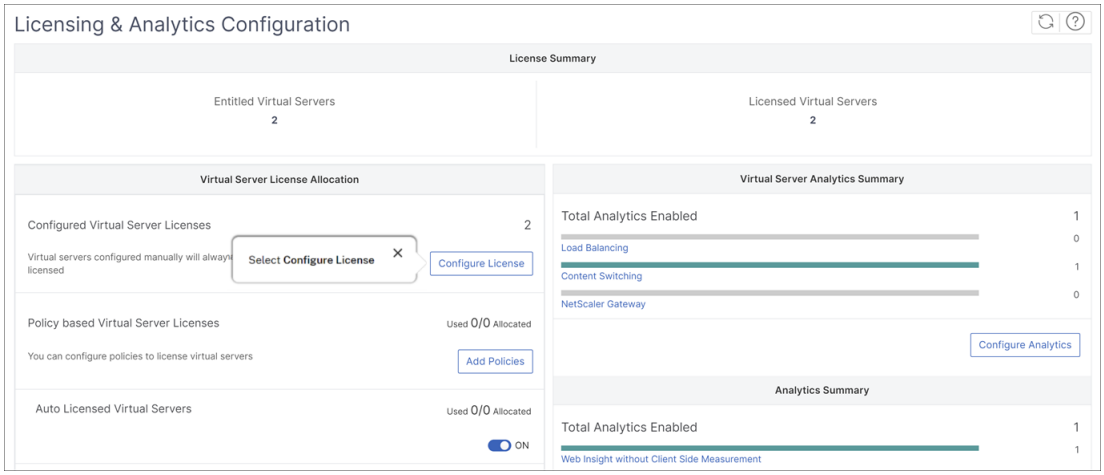
Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
Realice un seguimiento de la puntuación de su solicitud seleccionando los indicadores personalizados de su elección.	Si los componentes de App Score del Panel de control de la aplicación se utilizan de forma predeterminada y no se realiza ninguna personalización.
Agregue bloques de IP privados para visualizar las solicitudes de los clientes en el mapa geográfico	Si los bloques de IP no están configurados. Puede crear bloques de IP para mapear y visualizar las solicitudes de los clientes en un mapa geográfico en función de su IP o rango privados.
Suscríbase y exporte sus infracciones de AppSec a Splunk en tiempo real	Si la integración de Splunk en NetScaler ADM aún no está configurada.
Personalice el umbral predeterminado o crea uno para sus servicios de Kubernetes	Si solo se utilizan los umbrales predeterminados en el gráfico de servicios y no se aplica ningún umbral simple o doble a los servicios.
Configure proactivamente los perfiles de notificación y reciba notificaciones en sus destinos de comunicación	Si aún no se ha configurado un perfil de notificación.
Programe exportaciones periódicas y reciba notificaciones sobre los detalles de la infraestructura	Si aún no se han configurado programas de exportación en **Infraestructura > Instancias**.
¿Tiene ServiceNow y quiere integrarlo en ADM?	Si la integración de ServiceNow en NetScaler ADM aún no está configurada.
Automatice la administración de certificados SSL con Venafi y ADM	Si el servidor Venafi aún no está configurado en NetScaler ADM.
Renueva su licencia agrupada antes de que caduque.	Si su licencia actual está a punto de caducar en 30 días.
Comience a utilizar las licencias agrupadas asignando el ancho de banda agrupado que haya adquirido a las instancias de NetScaler.	Si aún no ha empezado a asignar sus derechos de licencia agrupados.
Considere la posibilidad de adquirir más capacidad de ancho de banda agrupada.	Si ha utilizado el 90% o más de sus derechos de ancho de banda agrupados.
Su permiso de ancho de banda agrupado actual está infrautilizado. Revisa y considera la posibilidad de asignar más	Si el uso de la asignación de licencias agrupadas es inferior al 70%.

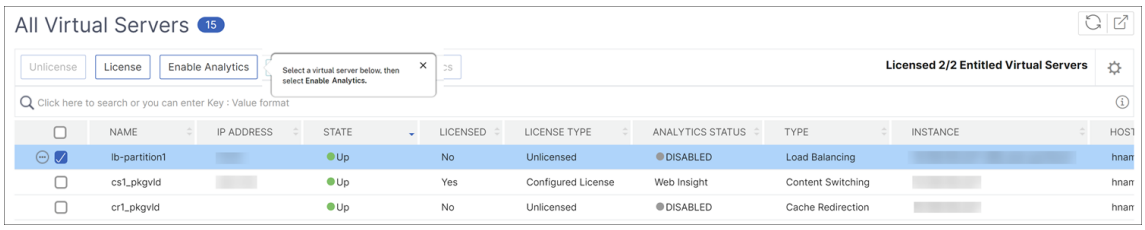
¿Cómo utilizar el flujo de trabajo de Guide me y completar la recomendación?

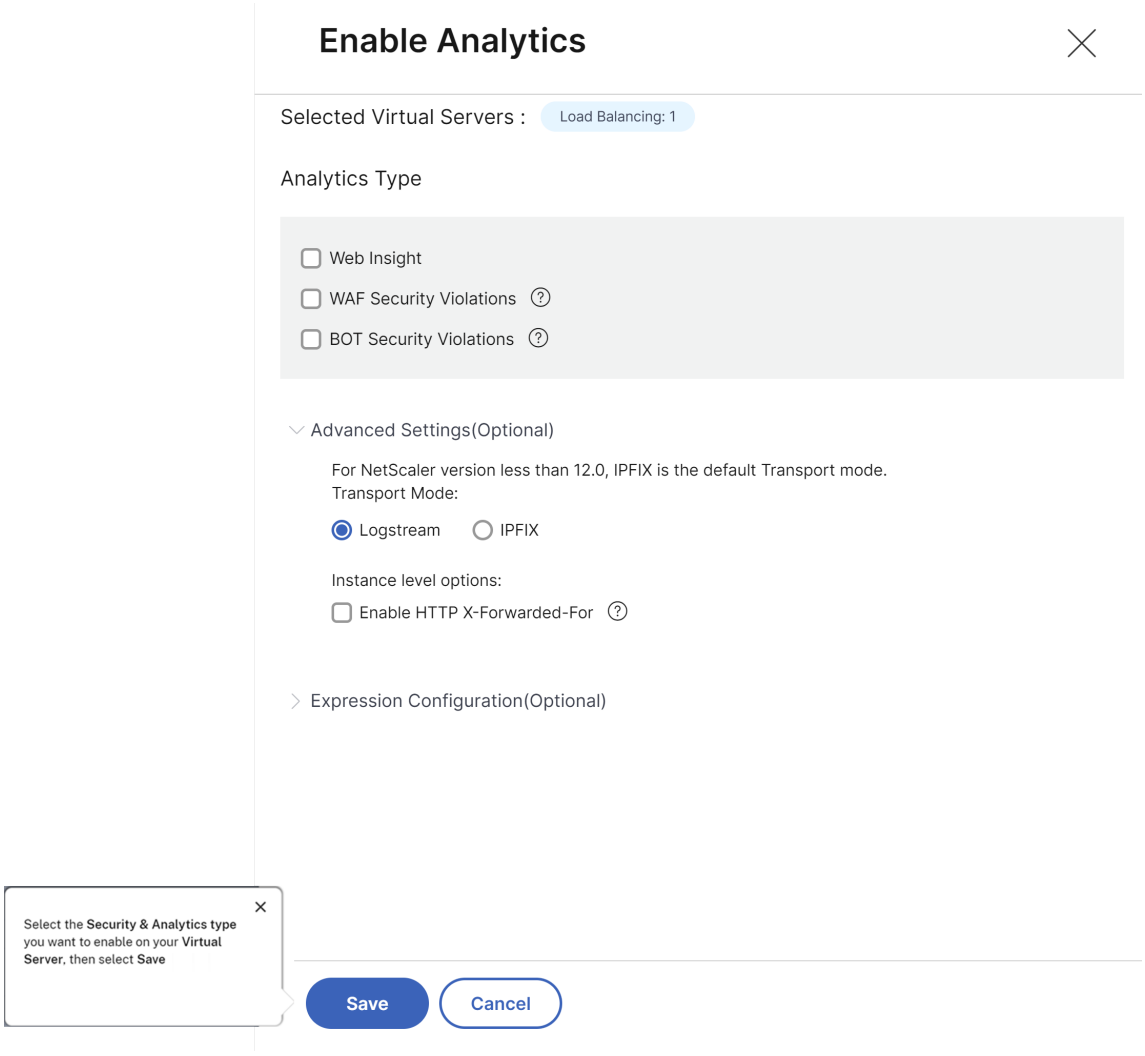
Pongamos que quiere habilitar el análisis para todos los servidores virtuales con licencia. Haga clic en **Guiarme** para realizar la siguiente tarea:



El flujo de trabajo proporciona las sugerencias necesarias para completar la tarea. En este ejemplo, después de hacer clic en **Guiarme**, siga las sugerencias de información sobre herramientas que se proporcionan:

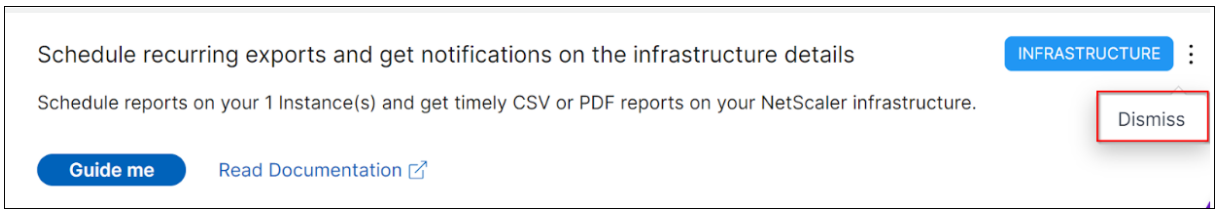
1. 

2. 

3. 

Tras seleccionar el tipo de análisis y hacer clic en **Guardar análisis**, la recomendación estará completa y pasará a Completado.

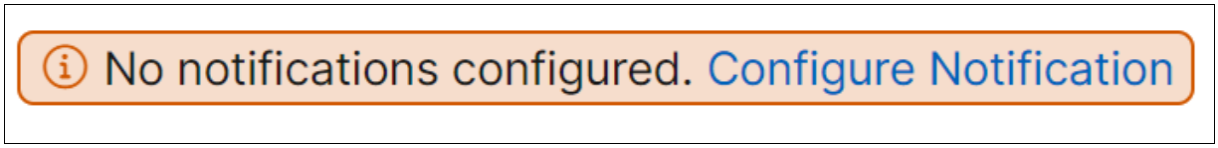
Del mismo modo, si quiere completar alguna recomendación más adelante, puede seleccionar **Descartar** en la lista y se moverá a **Descartada**.



Configurar notificaciones

Puede configurar y recibir notificaciones cada vez que NetScaler ADM identifique cualquier tarea abierta que requiera su acción inmediata. Si no ha configurado las notificaciones, puede hacer clic

en **Configurar notificación** en la esquina superior derecha.



En la página **Notificaciones**, puede configurar los perfiles de **Correo electrónico** y **Slack**y, a continuación, hacer clic en **Guardar** para recibir notificaciones. Para cada tipo de notificación, la GUI de NetScaler ADM muestra la lista o el perfil de distribución configurados. El NetScaler ADM envía notificaciones a la lista o perfil de distribución seleccionado.

Preguntas frecuentes

1. ¿Por qué tipo de recomendaciones están presentes para los administradores?

   Actualmente, las recomendaciones son específicas para las implementaciones y ayudan a los administradores a realizar más configuraciones y tareas de configuración para que la implementación sea eficiente. También permite descubrir mejor los productos y los administradores pueden saber qué hace una tarea y cómo puede ayudar sin ningún conocimiento previo ni saber si la función existe en ADM o no.

2. ¿Qué ocurre si rechazo alguna recomendación?

   Las recomendaciones que desestime se trasladan a **Rechazadas**. Puede completar estas recomendaciones más adelante.

3. ¿La recomendación pasa a **Completada** si empiezo una guía y la dejo en el medio?

   No, la recomendación no se completa a menos que se guarde o complete la acción.

4. ¿Puedo realizar búsquedas o filtros?

   ¡Sí! Puede utilizar la barra de búsqueda o limitarse a tareas específicas seleccionando la categoría de la lista.

5. ¿Recibiré tareas para realizar acciones en eventos dinámicos?

   ¡Sí! Actualmente puede ver un total de 4 tareas procesables. Para obtener más información, consulte Tareas.

6. ¿Aparecerán todas las tareas prácticas y más de 20 recomendaciones aunque no haya agregado instancias de NetScaler en NetScaler ADM?

   No. Debe tener servidores virtuales e instancias de NetScaler disponibles en NetScaler ADM para mostrar todas las tareas y recomendaciones.

7. ¿Con qué frecuencia se actualizarán las tareas?

Al hacer clic en **Tareas** en el panel de navegación izquierdo, se actualizan y están disponibles en su estado más reciente. Los detalles se obtienen y actualizan.

Un panel unificado para ver los detalles de las métricas clave de la instancia

January 30, 2024

En NetScaler ADM, puede ver varios datos sobre el uso y el rendimiento de las aplicaciones, la infraestructura de ADC, las infracciones de seguridad (bots y WAF), etc. Como administrador, es posible que tenga que navegar hasta varias opciones de la GUI de ADM para ver varios datos. Por ejemplo, para comprobar la información sobre los servidores virtuales (aplicaciones) y las instancias de ADC:

- Primero debe ir a **Aplicaciones > Panel de control** para ver información sobre las aplicaciones.
- A continuación, debe ir a **Infraestructura > Análisis de infraestructura** para ver información sobre las instancias de ADC.

Para una mejor experiencia de supervisión, es necesario que tenga un privilegio que contenga una descripción general de todos los datos requeridos. Vaya a **Descripción general > Panel de control** para visualizar un panel de control de un solo panel con una descripción general de los detalles de las métricas clave en función de las siguientes categorías:

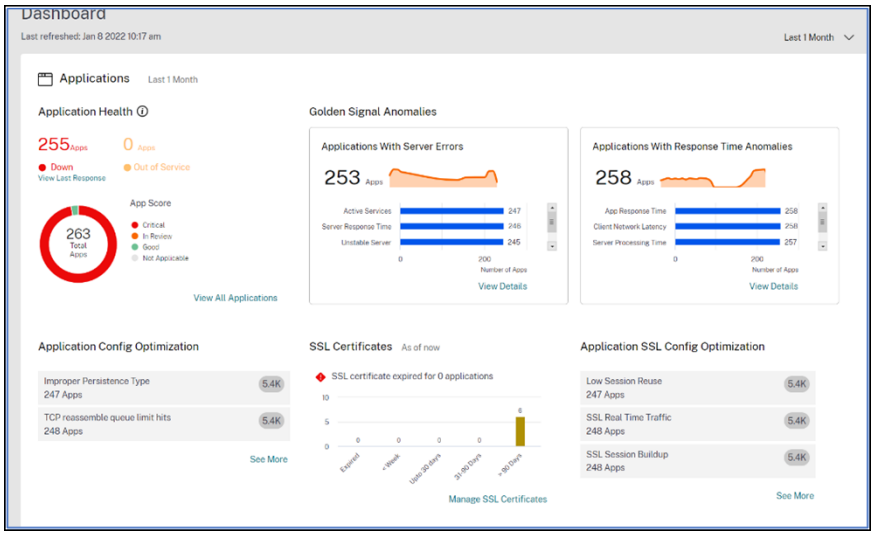
- Aplicaciones
- Infraestructura ADC
- Seguridad de las aplicaciones
- Gateway

Aplicaciones

En **Aplicaciones**, puede ver:

- Estado de**la aplicación**: proporciona una descripción general de las aplicaciones que están **inactivas** o **fuera de servicio**y en función de su estado, como **Crítico**, **En revisión**, En **buen**estado y **No aplicable**. Haga clic en **Ver todas las aplicaciones** para ver los detalles en el panel de aplicaciones
- **Anomalías de Golden Signal**: proporciona una descripción general de las aplicaciones que tienen errores de servidor y anomalías en el tiempo de respuesta. Haga clic en **Ver detalles** para obtener más información.

- **Optimización de la configuración de aplicaciones**: proporciona una descripción general del total de aplicaciones que tienen problemas de rendimiento. Haga clic en **Ver más** para ver los detalles del problema en el panel de control
- **Certificados SSL**: proporciona una descripción general de los certificados SSL junto con su validez. Haga clic en **Administrar certificados SSL** para ver más información en el panel de control SSL.
- **Optimización de la configuración SSL** de aplicaciones: proporciona una descripción general del total de aplicaciones que tienen problemas relacionados con SSL. Haga clic en **Ver más** para ver los detalles del problema.



Infraestructura ADC

En **ADC Infrastructure**, puede ver las siguientes métricas clave relacionadas con la instancia de ADC:

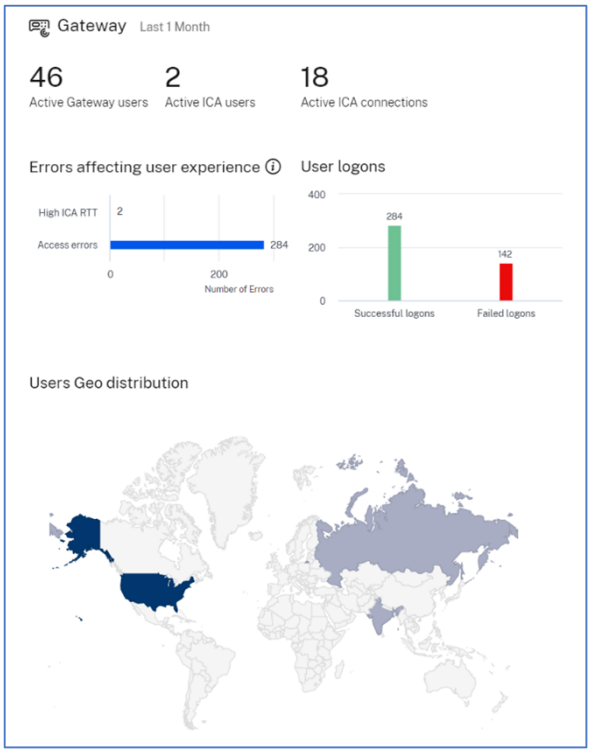
- Estado de**la instancia de ADC**: proporciona una descripción general del total de instancias de ADC en función de la puntuación de la instancia.
- **Instancias de ADC afectadas por los CVE**: proporciona una descripción general del total de instancias de ADC que se ven afectadas por vulnerabilidades y exposiciones comunes (CVE).
- **Problemas de instancias de ADC**: proporciona una descripción general de los problemas de las instancias de ADC en función de la categoría de problema. Para obtener más información, consulte Análisis de infraestructura.
- **Resumen de actualización de instancias de ADC**: proporciona una descripción general del total de instancias de ADC que no están en la versión más reciente. Haga clic en Ver panel de instancias de ADC para obtener más información.

Seguridad de las aplicaciones

Proporciona una descripción general del total de aplicaciones afectadas y del total de infracciones (bots y WAF) notificadas durante el período seleccionado. Haga clic en **Ver panel de seguridad** para ver los detalles de las infracciones de seguridad y de bots

Gateway

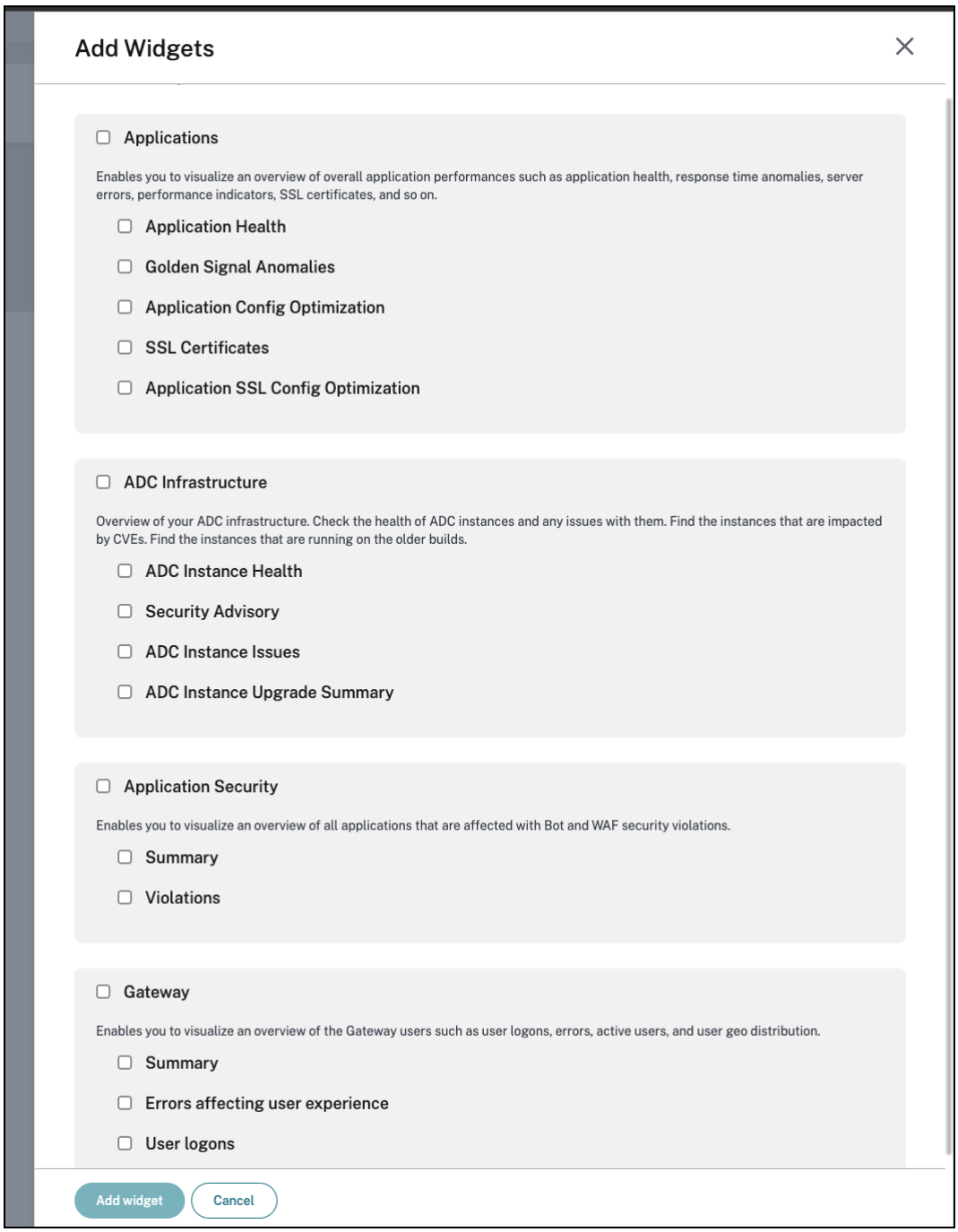
Proporciona una descripción general del total de usuarios de gateway activos, el total de usuarios de ICA activos y el total de conexiones ICA activas. También puede ver los errores, los detalles de inicio de sesión de los usuarios y un mapa geográfico que proporciona detalles sobre las ubicaciones de los usuarios.



Personaliza el panel

Puede usar la opción **Modificar panel** y personalizar la vista del panel según su elección. Con la opción **Modificar panel** de control, puede:

- Arrastrar widgets
- Elimine todo el widget (aplicaciones, infraestructura ADC, Gateway o seguridad de aplicaciones).
- Elimine los widgets más pequeños presentes debajo de cada widget.
- Haga clic en **Agregar widget** y seleccione las métricas clave necesarias que quiere ver en cada widget.



- Restablecer los valores predeterminados
- Restablecer la última vez que se guardó

Tras realizar los cambios, haga clic en **Guardar**.

> **Nota**
>
> - De forma predeterminada, se muestran todos los widgets. Si personaliza el panel, guarde

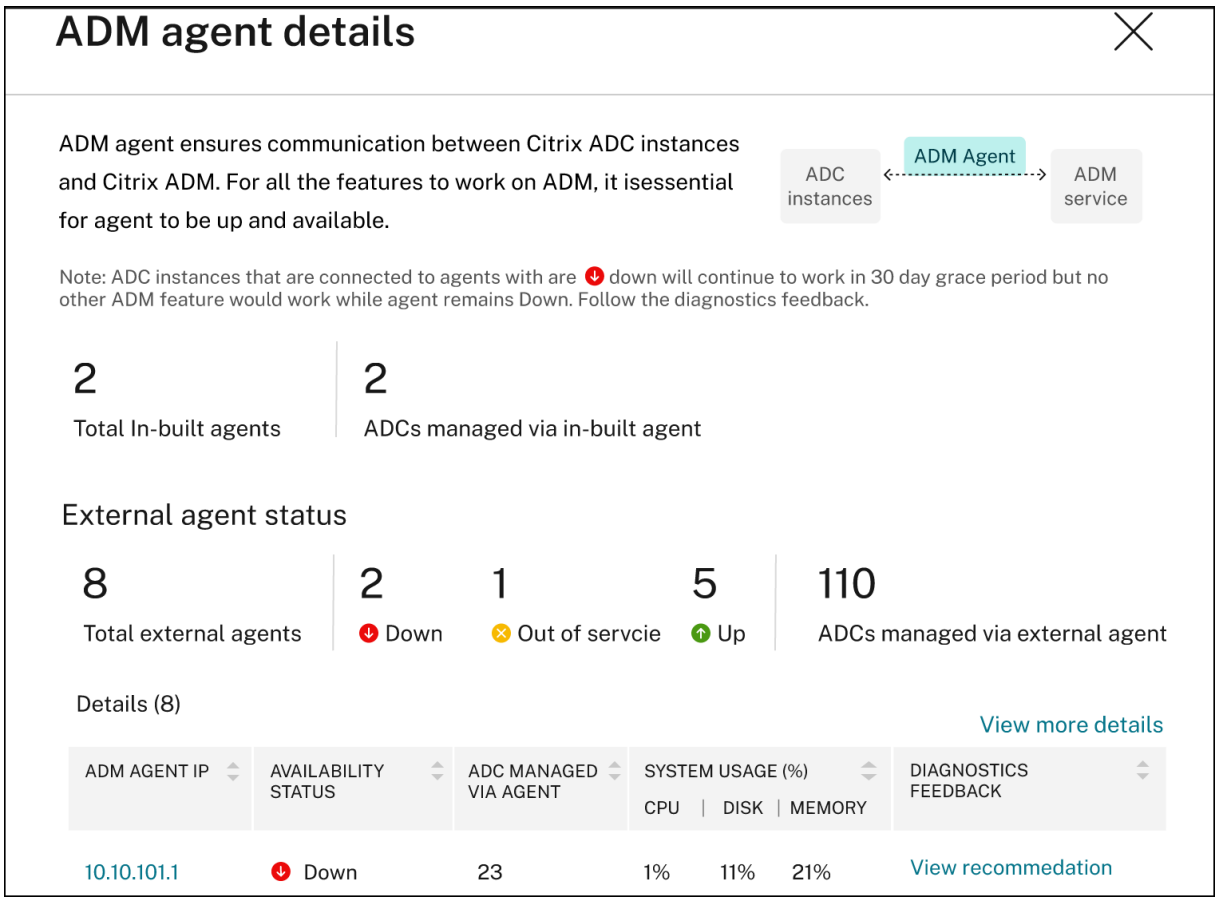
> los cambios y utilice de nuevo la opción **Restablecer los valores predeterminados**, todos los widgets se agregarán al panel.
>
> - La opción **Restablecer la última vez guardada** carga la configuración guardada anteriormente.

Ver detalles del agente

En el panel unificado, puede visualizar una descripción general de los detalles del agente de ADM. En **Descripción general > Panel de control**, junto al **estado del agente de ADM**, puede ver el siguiente estado que le permite analizar la disponibilidad general de los agentes:

- **Todos disponibles**. Indica que todos los agentes están en funcionamiento.
- **Todo no está disponible**. Indica que todos los agentes están fuera de servicio y no están disponibles.
- **[número de agentes] no disponible**. Indica que algunos agentes están inactivos y no se puede acceder a ellos.
- **Todo fuera de servicio**. Indica que todos los agentes están fuera de servicio.
- **[número de agentes] fuera de servicio**. Indica que algunos agentes están fuera de servicio.
- **No se ha encontrado el agente externo**. Indica que no hay ningún agente configurado (a través de ningún hipervisor).

Haga clic en **Ver detalles** para ver una descripción general de los detalles del agente de ADM, como el total de agentes integrados, el total de agentes externos, la IP del agente, el estado, el uso del sistema, las comprobaciones de diagnóstico, etc.



Crear y aplicar filtros

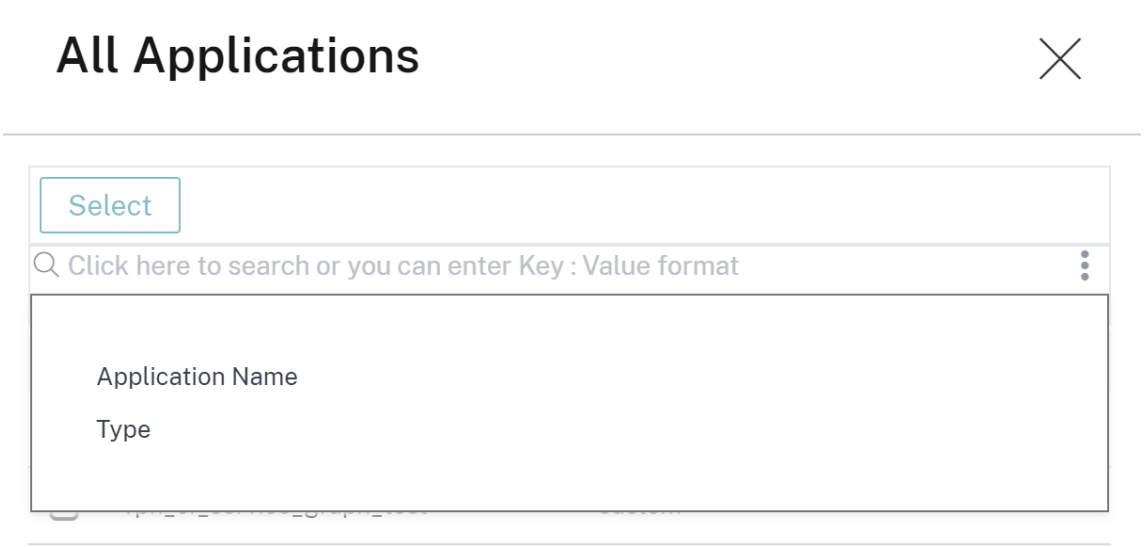
Puede aplicar filtros y ver la información solo para las instancias o aplicaciones seleccionadas de la siguiente manera:

- Aplicaciones
- Infraestructura ADC
- Seguridad de las aplicaciones

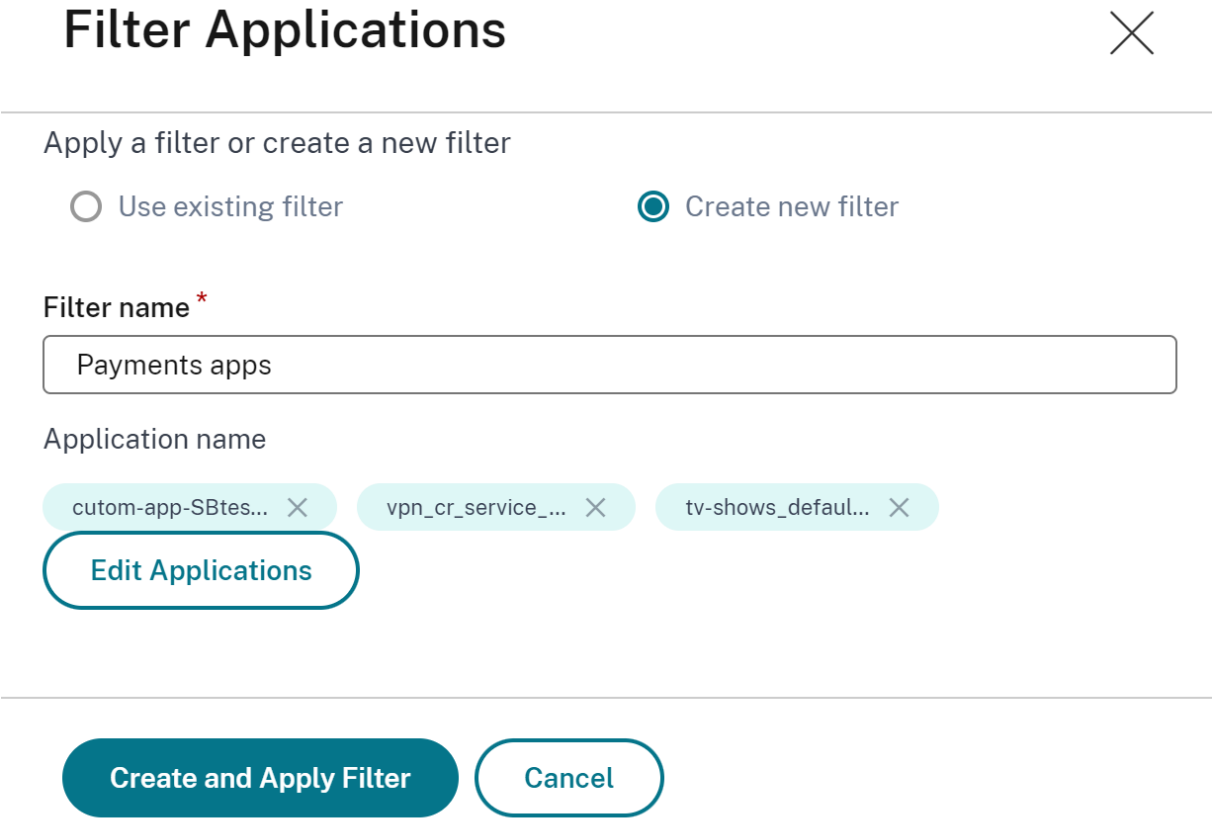
De forma predeterminada, se seleccionan todas las aplicaciones. Puede crear un archivador personalizado desde el panel de control haciendo clic en el icono de filtros disponible en el mosaico.

En la ventana **Filtrar aplicaciones**:

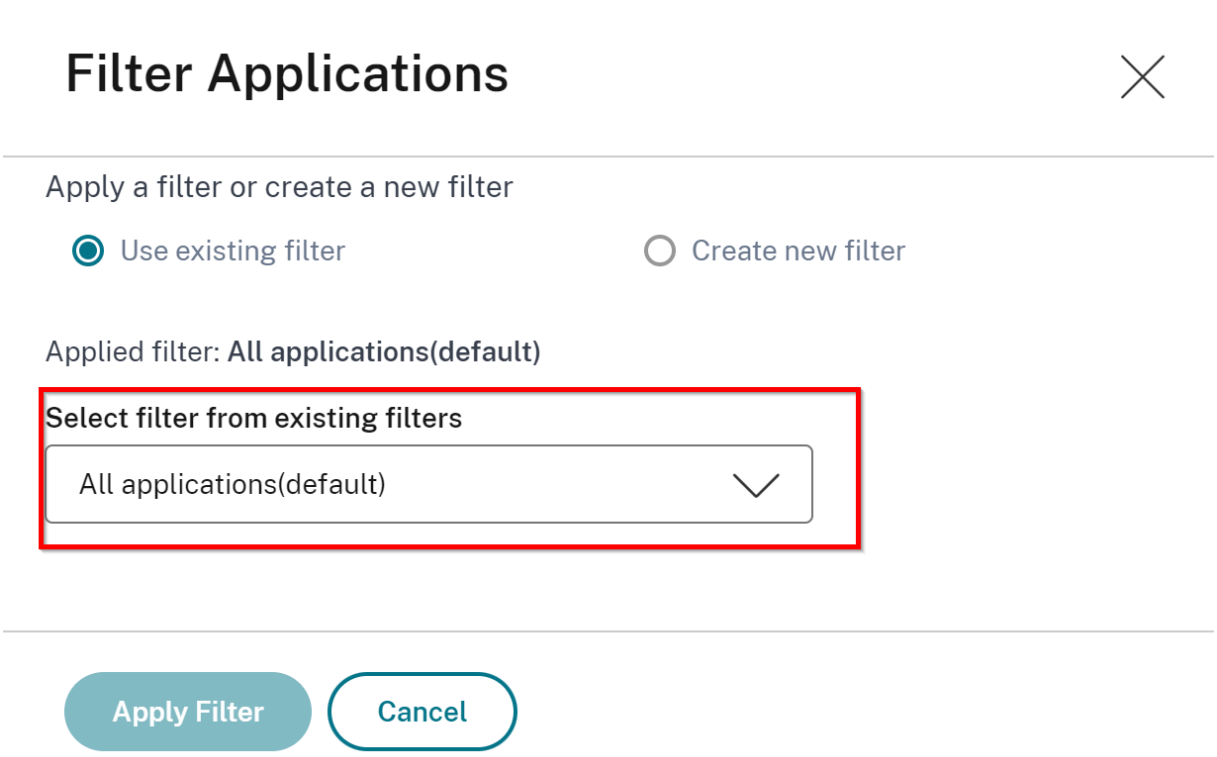
1. Seleccione **Crear filtro nuevo**.
2. Proporcione un nombre de filtro según su elección.
3. Haga clic en **Seleccionar aplicaciones** y agregue todas las aplicaciones necesarias para el filtro. Al seleccionar aplicaciones, también puede utilizar los filtros (**nombre** y **tipo de aplicación**) y, a continuación, seleccionar las aplicaciones.



4. Haga clic en **Crear y aplicar filtro**.

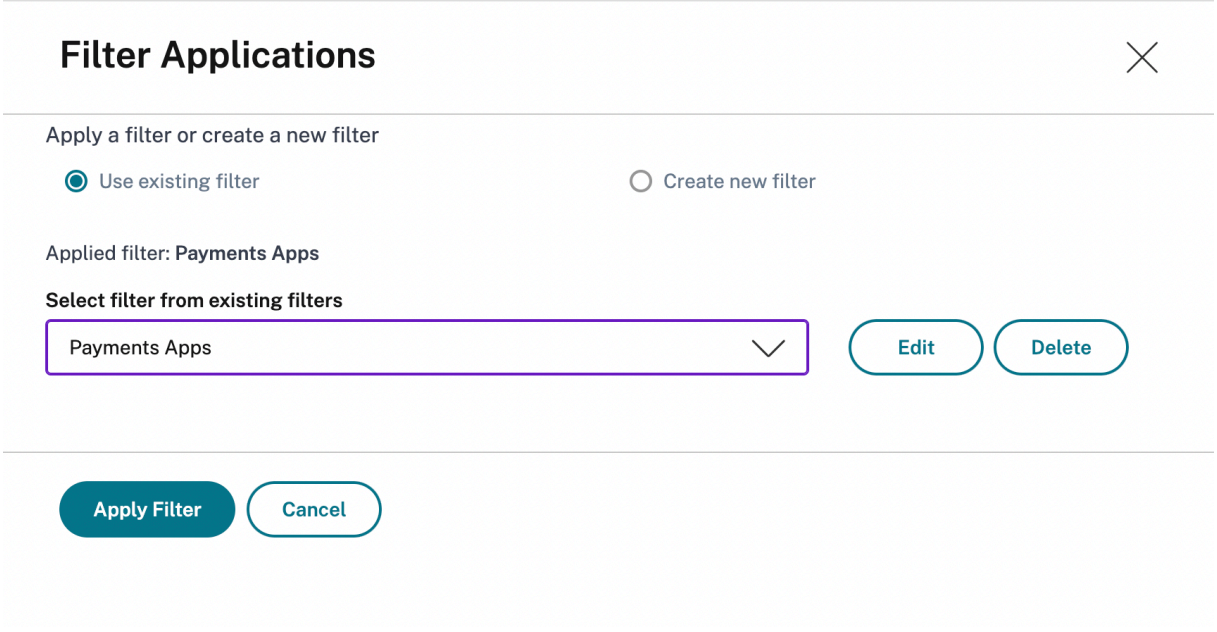


El filtro ya está creado y aplicado. Puede crear más filtros siguiendo el mismo procedimiento. Después de crear filtros, puede seleccionar y aplicar filtros a través de la lista **Seleccionar un filtro de entre los filtros existentes**.



Modificar filtros

Para modificar un filtro, seleccione el filtro de la lista y haga clic en **Modificar**. Con la opción de edición, puede agregar o eliminar aplicaciones y, a continuación, actualizar el filtro.



Para eliminar un filtro, selecciónelo de la lista y haga clic en **Eliminar**.

> **Nota**
>
> Al crear un filtro con aplicaciones y si se elimina una de las aplicaciones en el panel de aplicaciones, los detalles de la aplicación se eliminan inmediatamente del panel unificado.

Aplicaciones

January 30, 2024

La función de análisis y administración de aplicaciones de NetScaler ADM le permite supervisar las aplicaciones mediante un enfoque centrado en las aplicaciones. Este enfoque le ayuda a:

- Compruebe la puntuación y analice el rendimiento general de las aplicaciones
- Compruebe si hay algún problema que persista con el servidor o el cliente
- Detecte anomalías en los flujos de tráfico de la aplicación y tome medidas correctivas

> **Nota**
>
> Las aplicaciones hacen referencia a uno o más servidores virtuales que están configurados en las instancias (NetScaler).

Puede supervisar las aplicaciones durante el tiempo que dure, por ejemplo, 1 hora, 1 día, 1 semana y 1 mes.

Requisitos previos

- Asegúrese de haber agregado instancias de NetScaler en NetScaler ADM
- Asegúrese de tener una licencia válida para sus instancias NetScaler. Para obtener más información, consulte Licencias
- Asegúrese de haber aplicado una licencia para servidores virtuales. Para obtener más información, consulte Administrar licencias en servidores virtuales

Descripción general de la aplicación

Las aplicaciones pueden ser:

- Aplicaciones discretas
- Aplicaciones personalizadas
- Aplicaciones de microservicios (k8s_discrete)

Aplicaciones discretas

Todos los servidores virtuales con licencia se denominan aplicaciones discretas.

Aplicaciones personalizadas

Los servidores virtuales de una categoría se denominan aplicaciones personalizadas. Como administrador, debe agregar aplicaciones personalizadas basadas en una categoría. A continuación, puede gestionar y supervisar las aplicaciones a través del panel de control. Obtiene la facilidad de supervisar aplicaciones específicas que se agrupan en una categoría.

Por ejemplo, puede crear una categoría para su centro de datos1 y agregar sus instancias de ADC. Tras definir una categoría y agregar la instancia para el centro de datos1, el panel de la aplicación se muestra con una categoría independiente, que incluye todas las aplicaciones relacionadas con el centro de datos1.

Puntos que tener en cuenta

- Las aplicaciones discretas que se agregan a las aplicaciones personalizadas se eliminan de las aplicaciones discretas.
- Todas las aplicaciones que no se agregan a ninguna categoría están disponibles como **"otras"**.
- De forma predeterminada, NetScaler ADM le permite agregar licencias para hasta 2 aplicaciones. Dependiendo de su licencia, puede seleccionar y aplicar licencias para las aplicaciones que quiere supervisar.

Aplicaciones de microservicios

En un clúster de Kubernetes, NetScaler proporciona un Ingress Controller para NetScaler MPX (hardware), NetScaler VPX (virtualizado) y NetScaler CPX (en contenedores). Para obtener más información, consulte NetScaler Ingress Controller.

Las aplicaciones discretas que se configuran mediante las instancias de NetScaler CPX se denominan aplicaciones de microservicios.

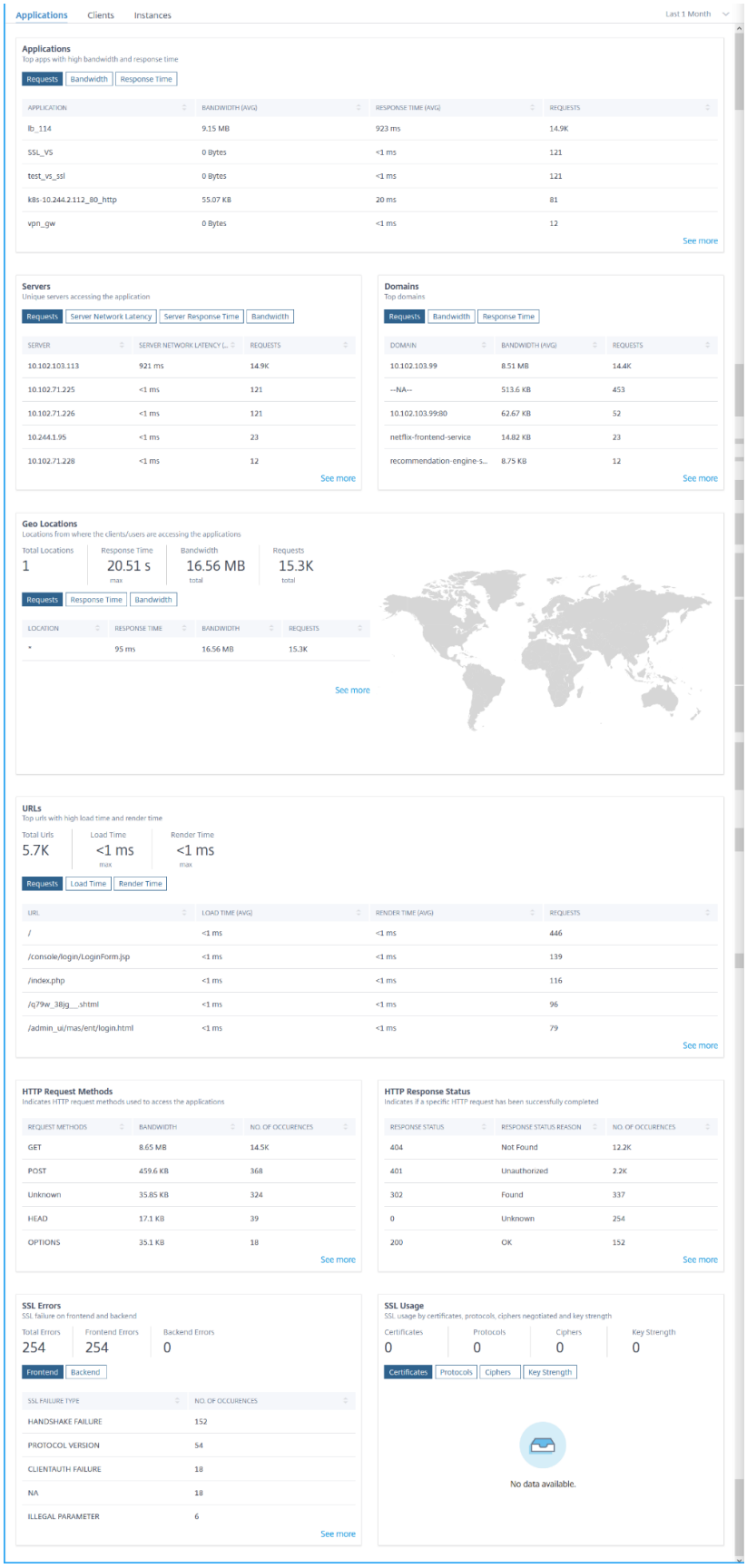
Panel de control Web Insight

January 30, 2024

La función de Web Insight mejorada se incrementa y proporciona visibilidad de métricas detalladas para aplicaciones web, clientes e instancias de NetScaler. Esta Web Insight mejorada le permite evaluar y visualizar la aplicación completa desde las perspectivas de rendimiento y uso juntos. Como administrador, puede ver Web Insight para:

- Una aplicación. Vaya a **Aplicaciones > Panel**, haga clic en una aplicación y seleccione la ficha **Web Insight** para ver las métricas detalladas. Para obtener más información, consulte Análisis de uso de aplicaciones.
- Todas las aplicaciones. Vaya a **Aplicaciones > Web Insight** y haga clic en cada ficha (Aplicaciones, Clientes, Instancias) para ver las siguientes métricas:

Aplicaciones	Clientes	Instancias
Aplicaciones	Clientes	Métricas de Instancia
Servidores	Ubicaciones geográficas	Aplicaciones
Dominios	Métodos de solicitud HTTP	Dominios
Ubicaciones geográficas	Estado de respuesta HTTP	URLs
URLs	URLs	Métodos de solicitud HTTP
Métodos de solicitud HTTP	Sistema operativo	Estado de respuesta HTTP
Estado de respuesta HTTP	Exploradores web	Clientes
Errores SSL	Errores SSL	Servidores
Uso SSL	Uso SSL	Sistema operativo
		Exploradores web

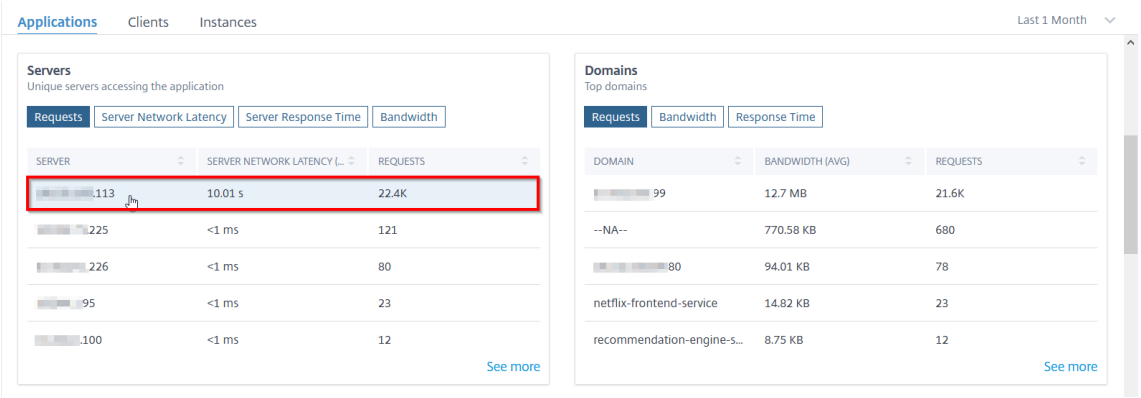


En cada métrica, puede ver los 5 resultados principales. Puede hacer clic para profundizar más para analizar el problema y realizar acciones de solución de problemas más rápido.

> **Nota:**
>
> - A partir de la versión **14.1-4.x** , al desglosar una métrica, la vista de análisis del gráfico de series temporales muestra valores nulos (por ejemplo, 0 ms y 0 solicitudes) durante la duración seleccionada. Antes, si no se recibía tráfico ni transacción durante el período seleccionado, la vista de análisis mostraba los gráficos omitiendo los valores nulos.
> - En algunos casos, es posible que NetScaler no pueda calcular los valores de RTT para algunas transacciones. Para este tipo de transacciones, NetScaler ADM muestra los valores de RTT como
>
> - **NA**: Se muestra cuando la instancia de ADC no puede calcular el RTT.
> - **< 1 ms**: Se muestra cuando la instancia de ADC calcula el RTT en decimales entre 0 ms y 1 ms. Por ejemplo, 0,22 ms.

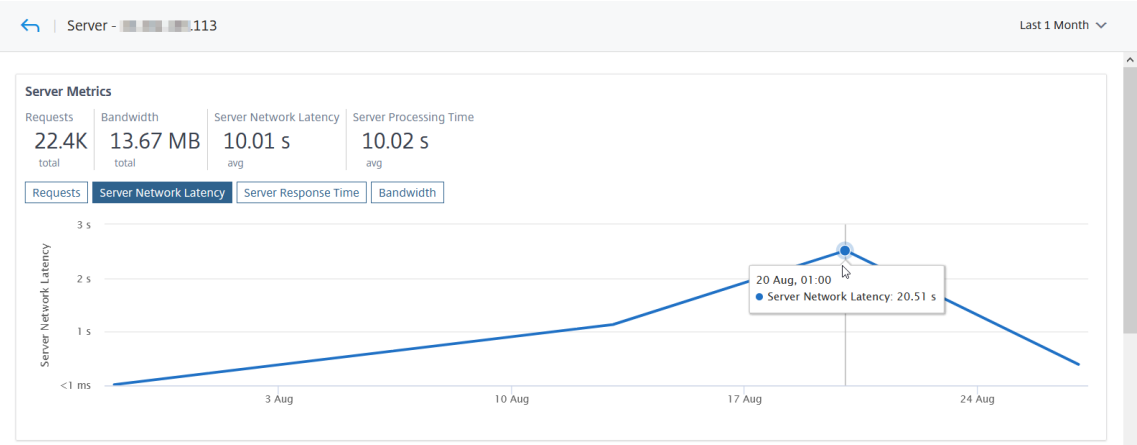
Por ejemplo, considere que quiere analizar la latencia de la red del servidor durante un mes de duración y tomar la decisión de escalar o reducir el entorno de producción. Para analizar esto:

1. Seleccione Último mes de la lista y, en la ficha **Aplicaciones**, desplácese hacia abajo hasta **Servidores**y haga clic en un servidor.



   Se muestran los detalles de las métricas del servidor seleccionado.

2. Seleccione la ficha **Latencia de red del servidor** para analizar la latencia.

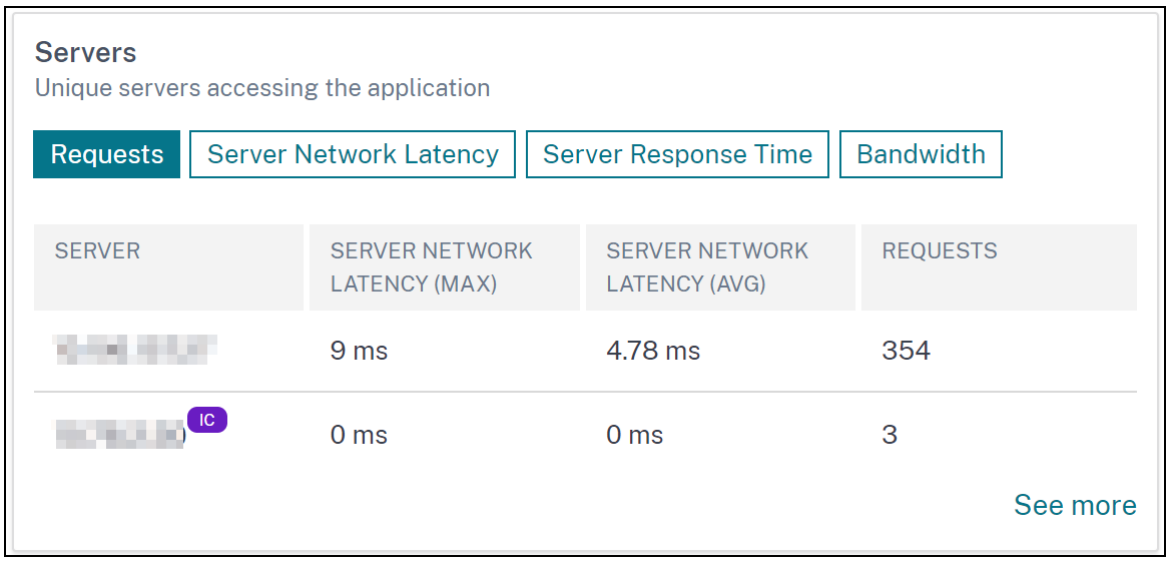


La latencia media indica 10.01 s y, a partir del gráfico, puede analizar que la latencia de la red del servidor durante el último 1 mes parece ser alta. Como administrador, puede tomar la decisión de escalar el entorno de producción.

Solicitudes de caché integradas

La caché integrada proporciona almacenamiento en memoria en el dispositivo NetScaler y ofrece contenido web a los usuarios sin necesidad de un viaje de ida y vuelta a un servidor de origen.

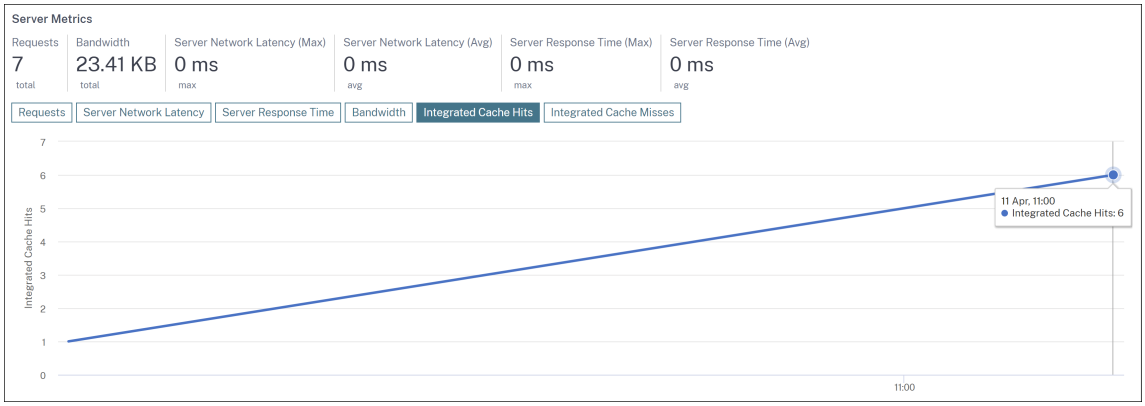
Las solicitudes de caché de integración están visibles actualmente en **Servidores** con una notificación de IC junto a la dirección IP del servidor virtual ADC. Todas las demás solicitudes están visibles con la dirección IP del servidor de origen.



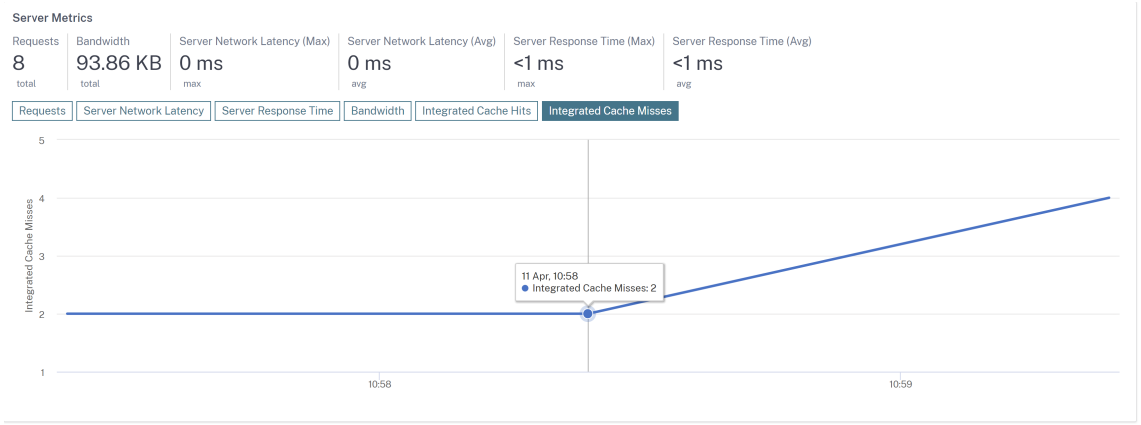
Al analizar un servidor para ver más detalles, **las métricas del servidor muestran las** fichas integradas de aciertos y errores de la memoria caché.

La vista gráfica en:

- La ficha **Respuestas de la memoria caché integrada** le permite ver el total de respuestas que el dispositivo NetScaler proporciona desde la memoria caché.



- La ficha **Errores de la memoria caché integrada** le permite ver el total de respuestas que el dispositivo NetScaler proporciona desde el servidor de origen.



Solucionar problemas de Web Insight

Para obtener más información, consulte el documento de solución de problemas Solucionar problemas de Web Insight.

Ver la causa principal de la latencia de las aplicaciones

January 30, 2024

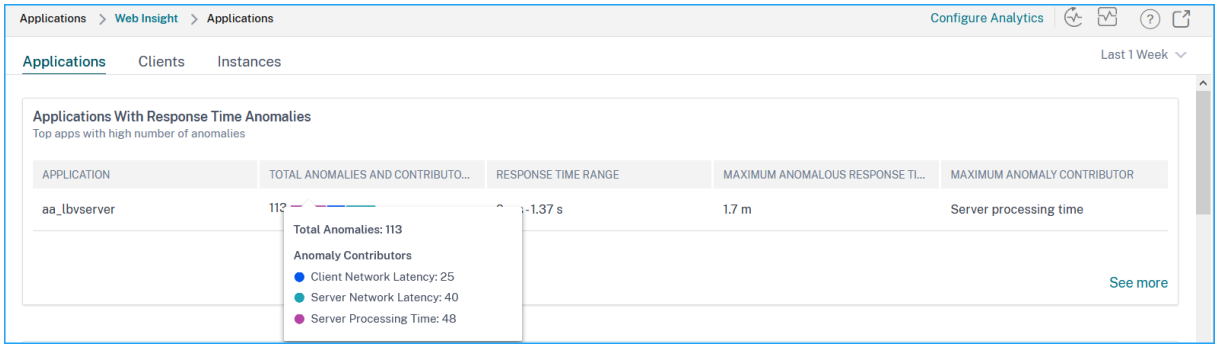
La lentitud de las aplicaciones es una preocupación importante para cualquier organización, ya que tiene como resultado un impacto en el negocio o productividad. En **Applications > Web Insight**, ahora puede ver una nueva métrica llamada **Aplicaciones con anomalías en el tiempo de respuesta**.

Con esta métrica, como administrador, puede analizar si la latencia de la aplicación se debe a las siguientes causas:

- Latencia de red del cliente
- Latencia de red del servidor
- Tiempo de procesamiento del servidor

NetScaler ADM realiza comprobaciones de anomalías cada hora e informa de las anomalías del tráfico de la última hora, en función de determinados requisitos previos. Por ejemplo, para evitar resultados falsos positivos, si el tiempo de respuesta es < 1 ms, se omiten las comprobaciones de anomalía para esos resultados.

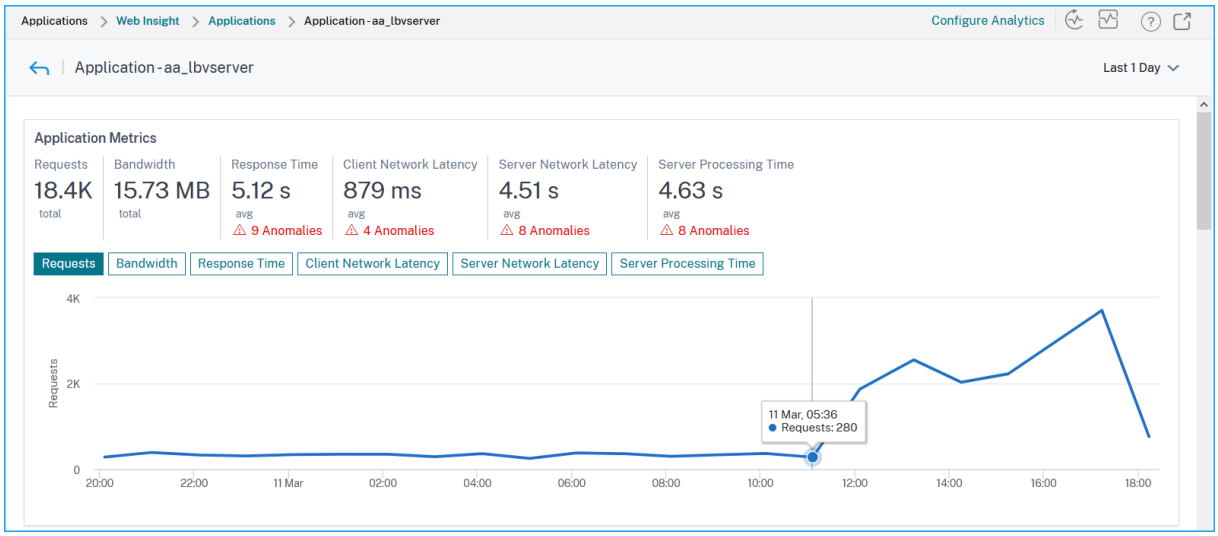
La página **Aplicaciones > Web Insight** permite ver las aplicaciones con anomalías de tiempo de respuesta durante la duración seleccionada. La métrica **Aplicaciones con anomalías de tiempo de respuesta** muestra las cinco aplicaciones principales en función de las anomalías totales. Haga clic en **Ver más** para ver todas las aplicaciones.



- **Aplicación**: indica el nombre de la aplicación.
- **Anomalías totales y colaboradores**: Denota las anomalías totales de la aplicación. Al pasar el puntero del mouse (ratón), puede ver las anomalías totales que provienen de la latencia de red del cliente, la latencia de red del servidor y el tiempo de procesamiento del servidor respectivamente.
- **Rango de tiempo de respuesta**: indica el intervalo de tiempo de respuesta esperado de la aplicación.
- **Tiempo máximo de respuesta anómala**: Denota el tiempo de respuesta más alto de la aplicación.
- **Colaborador máximo de anomalías**: indica si el número máximo de anomalías para la aplicación proviene de latencia de red cliente, latencia de red del servidor o tiempo de procesamiento del servidor.

Desenlaje de aplicaciones

Haga clic en una aplicación para ver los detalles de **Métricas de aplicación** para la duración seleccionada.



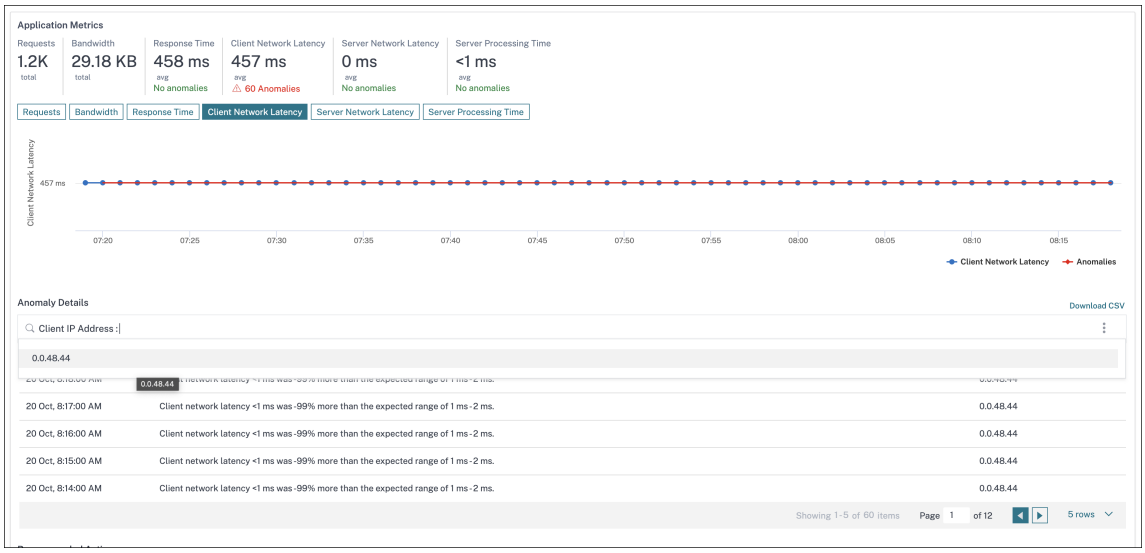
Las **Métricas de la Aplicación** le permiten ver:

- **Resumen**: una descripción general para visualizar el rendimiento de la aplicación, como el tiempo de respuesta, las solicitudes y el ancho de banda.
- **Solicitudes**: El total de solicitudes recibidas por la aplicación. También puede ver las solicitudes de los 5 clientes principales en función del total de solicitudes.
- **Ancho de banda**: Ancho de banda total procesado por la aplicación. También puede ver el consumo de ancho de banda de los 5 servidores principales en función del consumo total de ancho de banda.
- **Tiempo de respuesta**: descripción general para visualizar la latencia de la red del cliente, la latencia de la red del servidor y el tiempo de procesamiento del servidor en el mismo gráfico.
- Latencia de la**red del cliente: latencia** media de la red del cliente (del cliente al ADC).
- Latencia de la**red del servidor: latencia** media de la red del servidor (del ADC al servidor).
- **Tiempo de procesamiento del servidor: tiempo** medio de procesamiento del servidor (del servidor al ADC).

Si la aplicación tiene anomalías, puede ver si las anomalías provienen de latencia de red cliente, latencia de red del servidor o tiempo de procesamiento del servidor. Haga clic en cada ficha para ver los detalles.

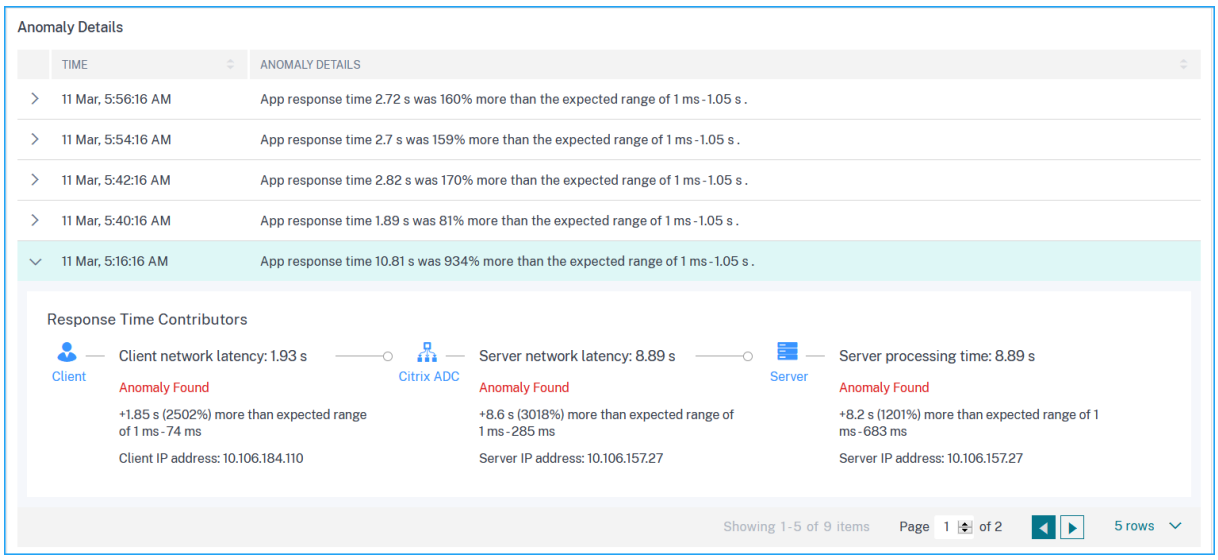
En las fichas **Latencia de la red del cliente** y **Latencia de la red del servidor**, puede ver:

- **Una barra de búsqueda**: Haga clic en la barra de búsqueda para ver la dirección IP de todos los clientes (en Latencia de red de clientes) y servidores (en Latencia de red de servidores). Puede seleccionar la dirección IP para filtrar los resultados.
- **Una opción**de exportación : haz clic en **Descargar CSV** para exportar los detalles en formato CSV.

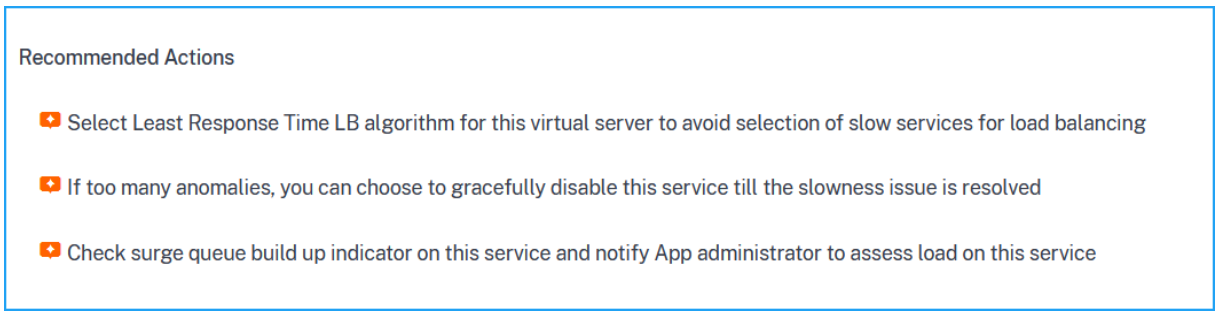


Tiempo de respuesta

En **Detalles de anomalía**, haga clic para ver los detalles de los contribuyentes de tiempo de respuesta (del cliente al servidor). En el ejemplo siguiente se presenta una anomalía para la latencia de red del cliente, la latencia de red del servidor y el tiempo de procesamiento del servidor. También puede ver los rangos esperados y la brecha que ha ocurrido más allá del rango esperado.



Las Acciones Recomendadas le sugieren las posibles resoluciones para las anomalías.



Del mismo modo, puede hacer clic en las fichas **Latencia de red del cliente, Latencia de**red**del servidor y Tiempo de procesamiento** del servidor para ver:

- Anomalía que ha infringido el rango esperado.
- Acciones recomendadas que sugieren las posibles resoluciones.

Si la aplicación está funcionando bien, puede ver las métricas de la aplicación como ninguna anomalía.

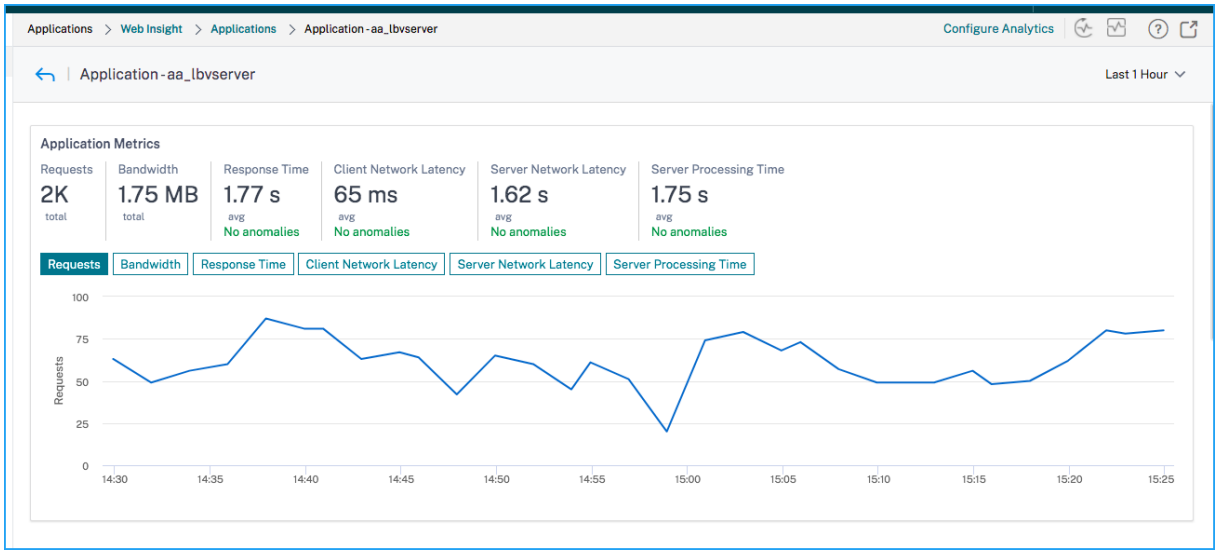


Gráfico de servicio

January 30, 2024

La función de gráfico de servicio de NetScaler ADM permite supervisar todos los servicios de una representación gráfica. Esta función también le permite ver un análisis detallado y métricas accionables de los servicios. Puede ver el gráfico de servicio para:

- Aplicaciones configuradas en todas las instancias de NetScaler
- Aplicaciones de Kubernetes

- Aplicaciones web de 3 niveles

Gráfico de servicio para aplicaciones en todas las instancias de NetScaler

La función de gráfico de servicio global le permite obtener una visualización holística de la `clients to infrastructure to application` vista. Desde esta vista gráfica de servicio de un solo panel, como administrador, puede:

- Comprender desde qué región están accediendo los usuarios a las aplicaciones específicas (aplicaciones web de 3 niveles y aplicación de microservicios)
- Visualice la vista de infraestructura (instancia de NetScaler) en la que se procesa la solicitud del cliente
- Comprender si los problemas ocurren desde el cliente, la infraestructura o la aplicación
- Más detalles para solucionar el problema

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Global** para ver:

- Detalles integrales de todas las aplicaciones conectadas desde el cliente a los servidores backend
- Todas las instancias de NetScaler conectadas a sus respectivos centros de datos

  > **Nota**
  >
  > Puede ver los centros de datos solo si tiene aplicaciones GSLB.

- Información de métricas del cliente
- Información de métricas de NetScaler
- Todas las instancias de NetScaler que tienen aplicaciones discretas, aplicaciones personalizadas y aplicaciones de microservicio discretas
- Las 4 principales aplicaciones de puntuación baja que pertenecen a aplicaciones personalizadas, aplicaciones discretas y aplicaciones de microservicios
- Información de métricas para los 4 principales servidores virtuales de puntuación baja
- El estado de las aplicaciones (aplicaciones discretas, aplicaciones personalizadas y aplicaciones de microservicios) como **Crítica**, **Revisión**, **Buena** y **No Aplicable**.

Para obtener más información, consulte Vista holística de las aplicaciones en el gráfico de servicio.

Gráfico de servicio para aplicaciones Kubernetes

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Microservicios** para ver:

- Garantice el performance general de las aplicaciones end-to-end
- Identifique los cuellos de botella creados por la interdependencia de los diferentes componentes de sus aplicaciones
- Reúna información sobre las dependencias de los diferentes componentes de sus aplicaciones
- Supervise los servicios dentro del clúster de Kubernetes
- Supervisa qué servicio tiene problemas
- Compruebe los factores que contribuyen a los problemas de rendimiento
- Ver la visibilidad detallada de las transacciones HTTP del servicio
- Analizar las métricas HTTP, TCP y SSL

Al visualizar estas métricas en NetScaler ADM, puede analizar la causa raíz de los problemas y realizar las acciones necesarias para solucionar problemas más rápidamente. El gráfico de servicio muestra sus aplicaciones en varios servicios de componentes. Estos servicios que se ejecutan dentro del clúster de Kubernetes pueden comunicarse con varios componentes dentro y fuera de la aplicación. Para empezar, consulta Configurar el gráfico de servicios.

Gráfico de servicios para aplicaciones web de 3 niveles

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Aplicaciones Web** para ver:

- Detalles sobre cómo se configura la aplicación (con el servidor virtual de conmutación de contenido y el servidor virtual de equilibrio de carga)

  Para las aplicaciones GSLB, puede ver los servidores virtuales de centros de datos, instancias de ADC, CS y LB.
- Transacciones de extremo a extremo desde el cliente hasta el servicio
- La ubicación desde la que el cliente accede a la aplicación
- El nombre del centro de datos donde se procesan las solicitudes de cliente y las métricas NetScaler del centro de datos asociadas (solo para aplicaciones GSLB)
- Detalles de métricas para clientes, servicios y servidores virtuales
- Si los errores son del cliente o del servicio
- El estado del servicio, como **Crítico**, **Revisado**y **Bueno**. NetScaler ADM muestra el estado del servicio según el tiempo de respuesta del servicio y el recuento de errores.
  - **Crítico (rojo)**: Indica cuándo el tiempo promedio de respuesta del servicio es superior a 200 ms Y el recuento de errores es > 0

  - **Revisión (naranja)**: Indica si el tiempo promedio de respuesta del servicio es > 200 ms O el recuento de errores es > 0
  - **Bueno (verde)**: Indica que no hay errores y que el tiempo medio de respuesta del servicio es inferior a 200 ms

- El estado del cliente, como **Crítico**, **Revisado**y **Bueno**. NetScaler ADM muestra el estado del cliente en función de la latencia de la red del cliente y el recuento de errores.
  - **Crítico (rojo)**: indica si la latencia promedio de la red del cliente es > 200 ms Y el recuento de errores es > 0
  - **Revisión (naranja)**: Indica si la latencia promedio de la red del cliente es > 200 ms O el recuento de errores es > 0
  - **Bueno (verde)**: Indica que no hay ningún error y que la latencia media de la red del cliente es < 200 ms.
- El estado del servidor virtual, como **Crítico**, **Revisado**y **Correcto**. NetScaler ADM muestra el estado del servidor virtual en función de la puntuación de la aplicación.
  - **Crítico (rojo)**: Indica si la puntuación de la aplicación es inferior < 40
  - **Reseña (naranja)**: Indica si la puntuación de la aplicación está entre 40 y 75
  - **Bueno (verde)**: Indica cuando la puntuación de la aplicación es > 75

Puntos a tener en cuenta:

- En el gráfico de servicios solo se muestran los servidores virtuales de equilibrio de carga, conmutación de contenido y GSLB.
- Si ningún servidor virtual está enlazado a una aplicación personalizada, los detalles no son visibles en el gráfico de servicio de la aplicación.
- Puede ver las métricas de los clientes y servicios en el gráfico de servicios solo si se producen transacciones activas entre los servidores virtuales y la aplicación web.
- Si no hay transacciones activas disponibles entre los servidores virtuales y la aplicación web, solo puede ver los detalles en el gráfico de servicios en función de los datos de configuración, como el equilibrio de carga, el cambio de contenido, los servidores virtuales GSLB y los servicios.
- Si se realizan cambios en la configuración de la aplicación, puede tardar 10 minutos en reflejarse en el gráfico de servicio.

Para obtener más información, consulte Gráfico de servicio para aplicaciones.

StyleBooks

January 30, 2024

Los StyleBooks simplifican la tarea de administrar configuraciones complejas de NetScaler para sus aplicaciones. Un StyleBook es una plantilla que puede utilizar para crear y administrar configuraciones de NetScaler. Puede crear un StyleBook para configurar una función específica de NetScaler, 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. NetScaler Application Delivery Management (ADM) calcula la diferencia entre el estado existente en un NetScaler y el estado deseado que usted 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 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 NetScaler. 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 NetScalers y también se puede mover entre instancias.

- **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 NetScaler. 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 NetScaler o en otra diferente. Se crea un nuevo paquete de configuración para esta configuración. Se guarda un paquete de configuración tanto en NetScaler ADM como en la instancia de NetScaler 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

Panel de seguridad de aplicaciones

January 30, 2024

El panel **de seguridad de aplicaciones** proporciona información general sobre las métricas de seguridad para las aplicaciones detectadas/con licencia. Este panel muestra la información sobre los ataques de seguridad de las aplicaciones descubiertas o con licencia, como los ataques de sincronización, los ataques de ventanas pequeñas, los ataques de inundación de DNS, etc.

Para ver las métricas de seguridad en el panel de seguridad de la aplicación:

1. Vaya a **Seguridad** > **Panel de seguridad** .
2. Seleccione la dirección IP de la instancia en la lista Instancia.

   Los informes incluyen la siguiente información para cada aplicación:

   - **Índice**de amenazas . Sistema de clasificación de un solo dígito que indica la importancia de los ataques a la aplicación. 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.

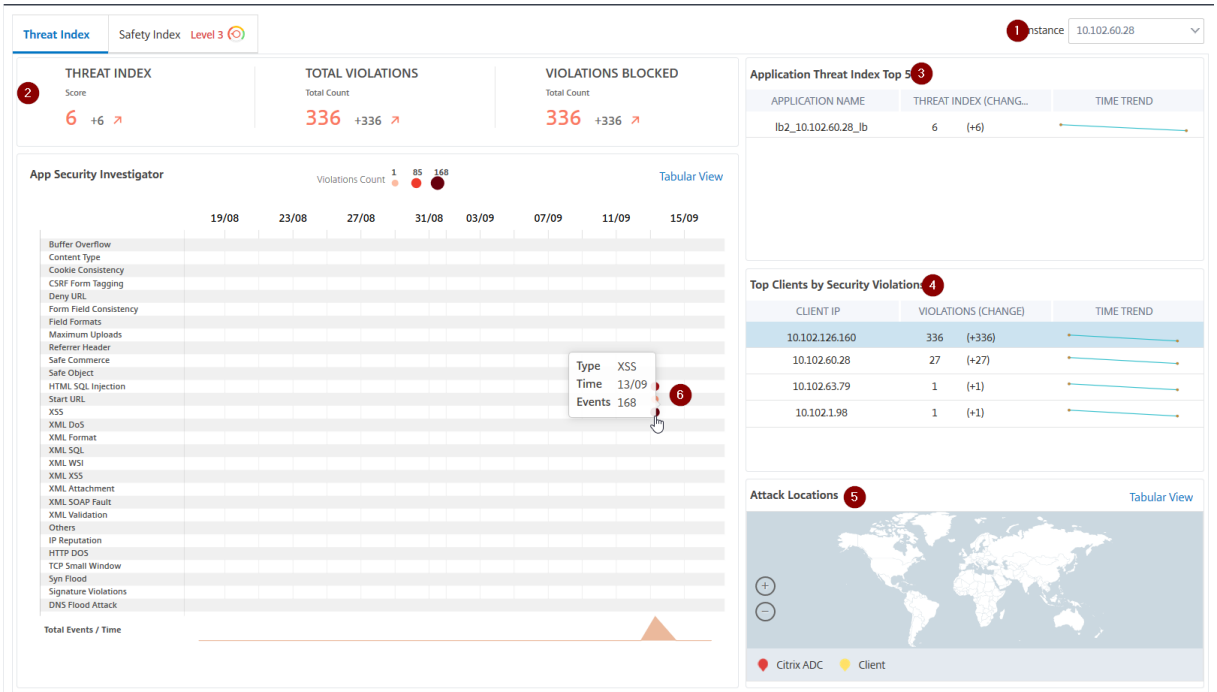
     El índice de amenazas se basa en la información de ataque. La información relacionada con el ataque, como el tipo de infracción, la categoría del ataque, la ubicación y los detalles del cliente, proporciona una visión de los ataques a la aplicación. La información de infracción se envía a NetScaler ADM 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 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. Para un valor de índice de seguridad elevado, ambas configuraciones deben ser fuertes. Por ejemplo, si se realizan comprobaciones rigurosas del firewall de aplicaciones, pero no se proporcionan medidas de seguridad del sistema NetScaler, como una contraseña segura para el usuario `nsroot`, a las aplicaciones se les asigna un valor de índice de seguridad bajo.

Puede ver las discrepancias reportadas en el **investigador de seguridad de aplicaciones**.

Detalles del índice de amenazas



1: Muestra la dirección IP de la instancia NetScaler para la que puede ver detalles.

2: Muestra detalles como la puntuación del índice de amenazas, el total de infracciones ocurridas y el total de infracciones bloqueadas.

3: muestra el servidor virtual de la instancia seleccionada.

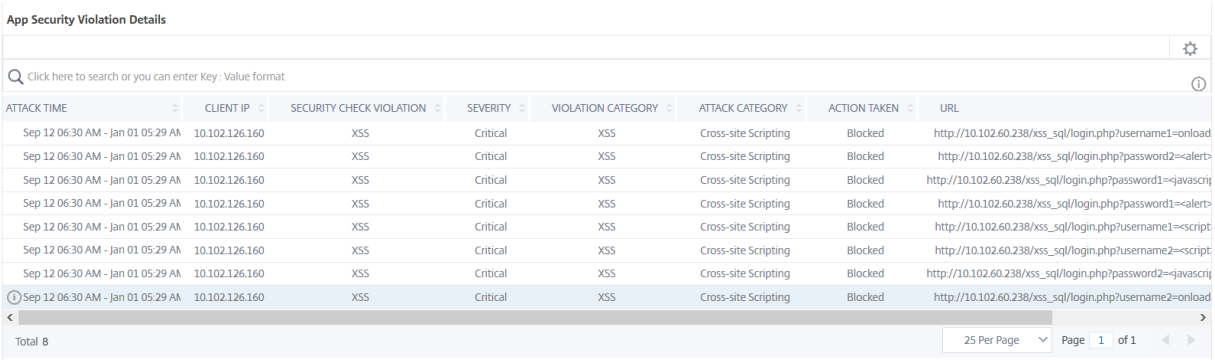
4: muestra las violaciones de seguridad según los clientes. Se muestra el gráfico App Security Investigator para cada cliente. Puede hacer clic en cada IP de cliente para ver los resultados.

5: Muestra las infracciones en la vista de mapa y en la vista tabular.

6: muestra los detalles de la infracción. Al situar el puntero del mouse sobre el gráfico, se muestran los detalles como el tipo de infracción, la hora del ataque y el total de eventos.

Al hacer clic en un gráfico de burbujas, los detalles se muestran en la página **Detalles de infracción de seguridad de aplicaciones**. Por ejemplo, si quiere ver más detalles de la infracción de scripts entre sitios (scripts entre sitios), haga clic en el gráfico rellenado para **XSS** en **App Security Investigator**.

Los detalles de infracción de seguridad de la aplicación se muestran con detalles de infracción como tiempo de ataque, categoría de ataque, gravedad, URL, etc.



También puede hacer clic en la opción **Configuración** para seleccionar las opciones que quiere que se muestren.

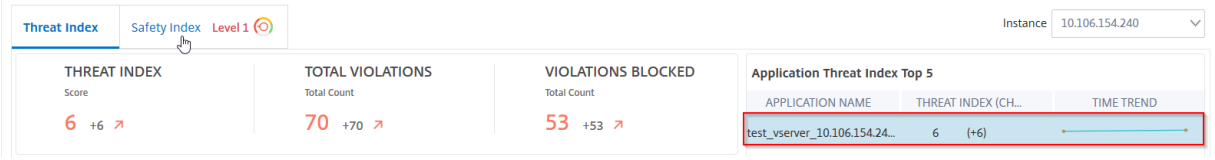
Detalles del índice de seguridad

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.

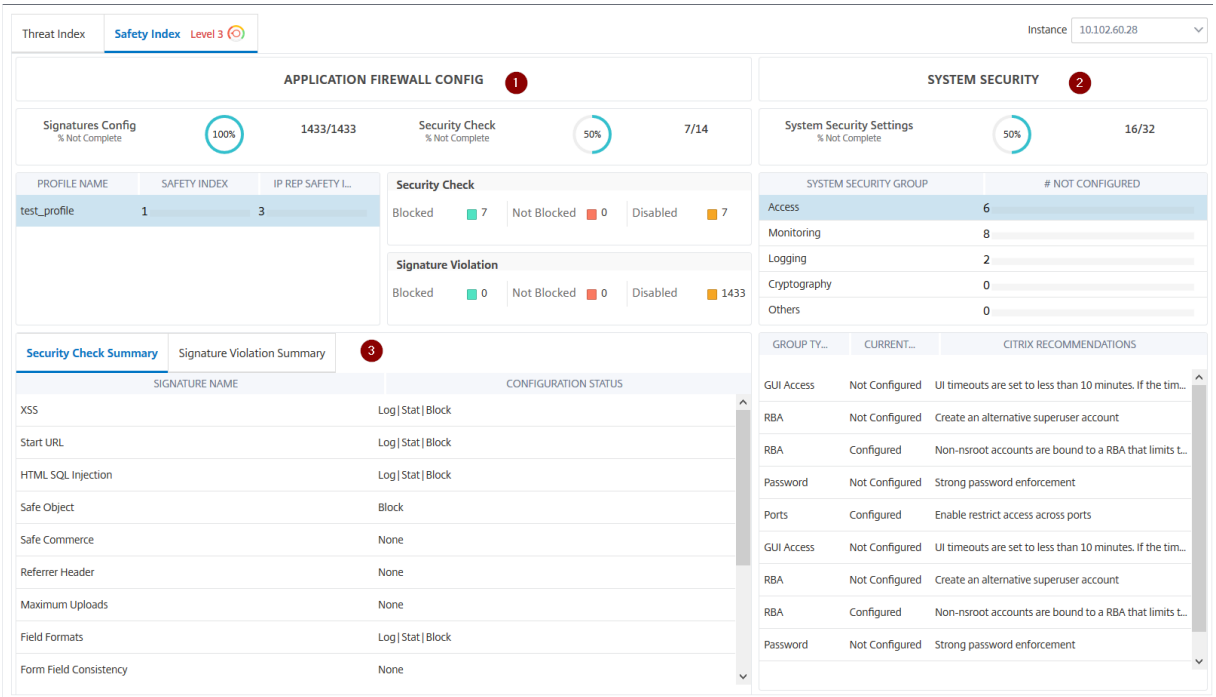
El resumen del índice de seguridad proporciona información sobre la eficacia de las siguientes configuraciones de seguridad:

- **Configuración**del firewall de aplicaciones . Muestra cuántas entidades de firma y seguridad no están configuradas.
- Seguridad del**sistema NetScaler ADM.** Muestra cuántas opciones de seguridad del sistema no están configuradas.

Para ver los detalles del **índice de seguridad**, seleccione un servidor/aplicación virtual y haga clic en la ficha **Índice de seguridad**.



Se muestran los detalles.



1: Muestra la información detallada de las configuraciones de Application Firewall.

2: Muestra la información detallada de Seguridad del sistema. Haga clic en cada grupo de seguridad para obtener detalles sobre el estado actual y las recomendaciones de Citrix.

3: Muestra el resumen de comprobación de seguridad e infracción de firma.

También puede ver un resumen del entorno de amenazas si habilita las **Infracciones de seguridad de WAF** para servidores virtuales y, a continuación, navega a **Seguridad** > **Infracciones de seguridad**.

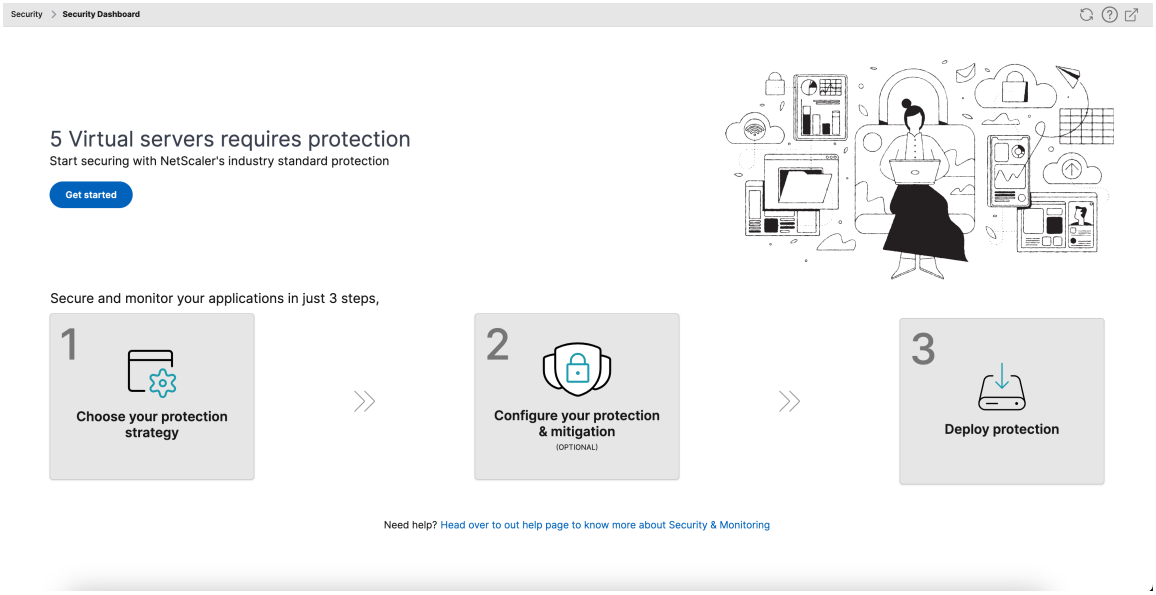
Panel de seguridad unificada

January 30, 2024

El panel **de seguridad unificada** es un panel único en el que puede configurar las protecciones, habilitar el análisis e implementar las protecciones en su aplicación. En este panel, puede elegir entre varias opciones de plantilla y completar todo el proceso de configuración en un único flujo de trabajo. Para empezar, vaya a **Seguridad > Panel de seguridad** y, a continuación, haga clic en **Administrar aplicación**. En la página **Administrar aplicaciones**, puede ver los detalles de sus aplicaciones seguras y no seguras.

> **Nota:**
>
> - Si es un usuario nuevo o si no ha configurado ninguna protección mediante StyleBooks o

directamente en instancias de NetScaler, aparecerá la siguiente página después de **hacer clic**en Seguridad > Panel de seguridad.

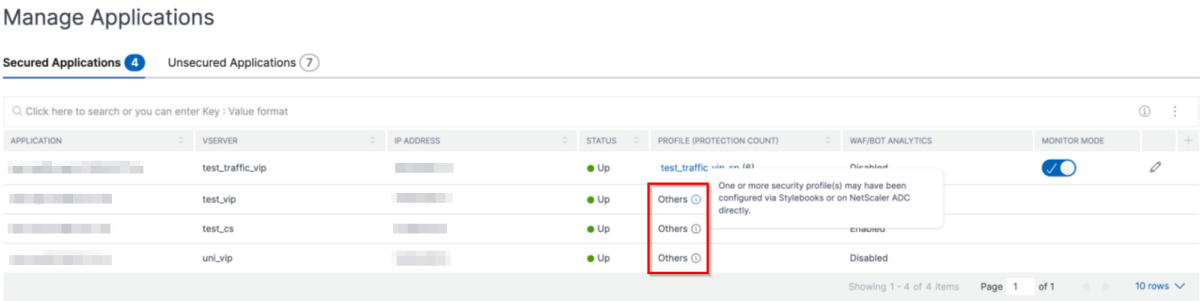


- Puede ver la cantidad total de servidores virtuales que requieren protección. Haga clic en **Comenzar** para ver los detalles en **Aplicaciones no seguras.**
- Los tipos de servidores virtuales aptos para configurar las protecciones son el equilibrio de carga y la conmutación de contenido.

Aplicaciones seguras

Puede ver los detalles después de configurar las protecciones mediante el panel de seguridad unificado. Para obtener más información, consulte Configurar protecciones para aplicaciones no seguras.

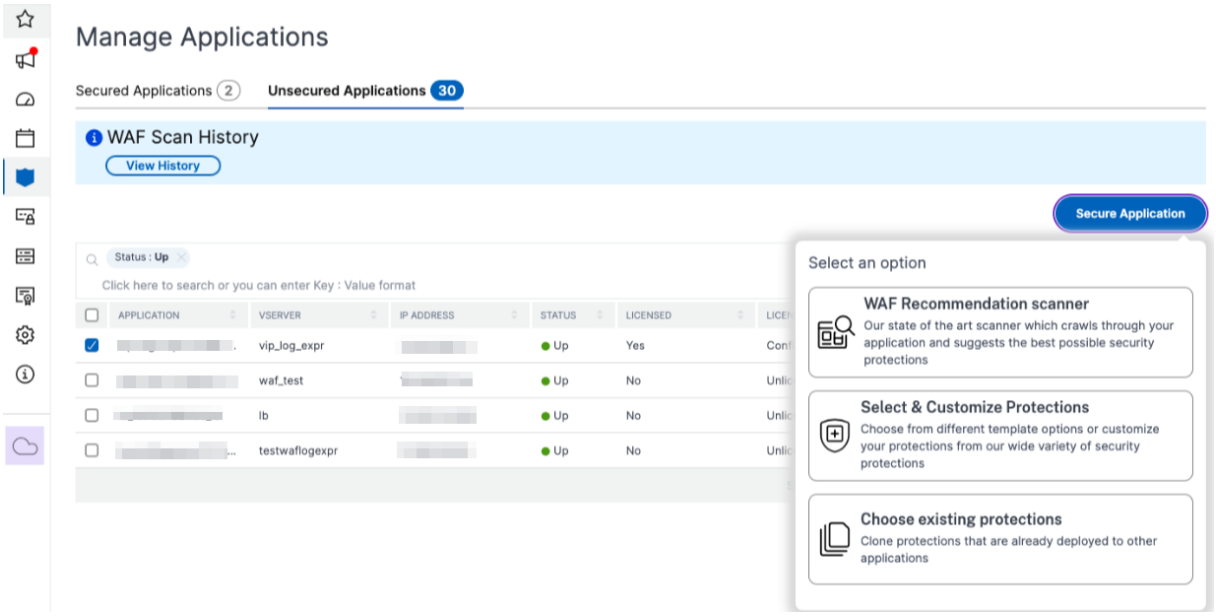
Si ya ha configurado las protecciones directamente en las instancias de NetScaler o mediante StyleBooks, puede ver las aplicaciones en la ficha **Aplicaciones seguras** marcada como **Otras** en **Perfil**.



Configurar protecciones para aplicaciones no seguras

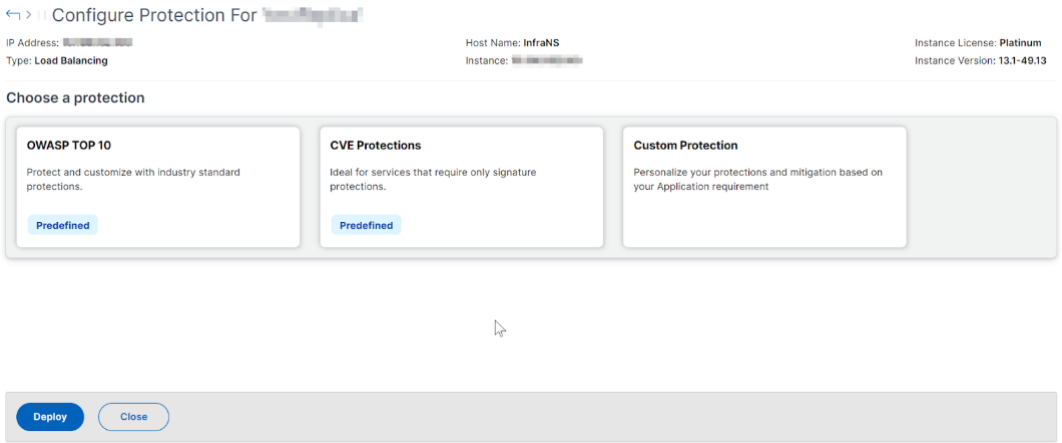
> **Nota:**
>
> El número máximo de entidades de configuración (reglas) admitidas en la lista de bloques es 32.

En la ficha **Aplicaciones no seguras**, seleccione una aplicación y haga clic en **Aplicación segura**.



Puede seleccionar cualquiera de las siguientes opciones para proteger su aplicación:

- **Escáner de recomendaciones WAF**: Esta opción le permite ejecutar un análisis en su aplicación. En función de ciertos parámetros del escaneo, el resultado le sugiere las protecciones para su aplicación. Podría considerar aplicar esas recomendaciones.
- **Seleccione y personalice las protecciones**: Esta opción le permite elegir entre diferentes opciones de plantillas o personalizar sus protecciones e implementarlas.



- **OWASP Top 10**: Una plantilla predefinida que cuenta con las protecciones estándar de la industria contra los 10 principales riesgos de seguridad de OWASP. Para obtener más información, consulte https://owasp.org/www-project-top-ten/.
- **Protecciones CVE**: Puede crear el conjunto de firmas a partir de la lista de reglas de firma preconfiguradas clasificadas en categorías de vulnerabilidades conocidas. Puede seleccionar firmas para configurar la acción de registro o bloqueo cuando un patrón de firma coincida con el tráfico entrante. El mensaje de registro contiene los detalles de la vulnerabilidad.
- **Protecciones personalizadas**: Seleccione las protecciones e impleméntelas según sus requisitos.

- **Elija las protecciones existentes**: Esta opción clona las protecciones que se implementan en una aplicación existente. Si quiere implementar esas mismas protecciones en otra aplicación, puede seleccionar esta opción e implementarla en otra aplicación tal como está. También puede seleccionar esta opción como plantilla, modificar las protecciones y, a continuación, implementarlas.

Escáner de recomendaciones WAF

> **Nota:**
>
> - Solo puede ejecutar un análisis a la vez para una aplicación. Para iniciar un nuevo análisis para la misma aplicación o para una aplicación diferente, debe esperar hasta que finalice el análisis anterior.
> - Puede hacer clic en **Ver historial** para ver el historial y el estado de los escaneos anteriores. También puede hacer clic en **Ver informe** y aplicar las recomendaciones más adelante.

Requisitos previos:

- La instancia de NetScaler debe ser 13.0 41.28 o posterior (para las comprobaciones de seguridad) y 13.0 o posterior (para las firmas).
- Debe tener la licencia premium.
- Debe ser el servidor virtual de equilibrio de carga.

Para comenzar con el análisis de recomendaciones de WAF, debe proporcionar la siguiente información:

1. En **Parámetros de escaneo**:
   - **Nombre de dominio**: Especifique una dirección IP accesible válida o el nombre de dominio accesible públicamente asociado a la aplicación. Por ejemplo: www.example.com.

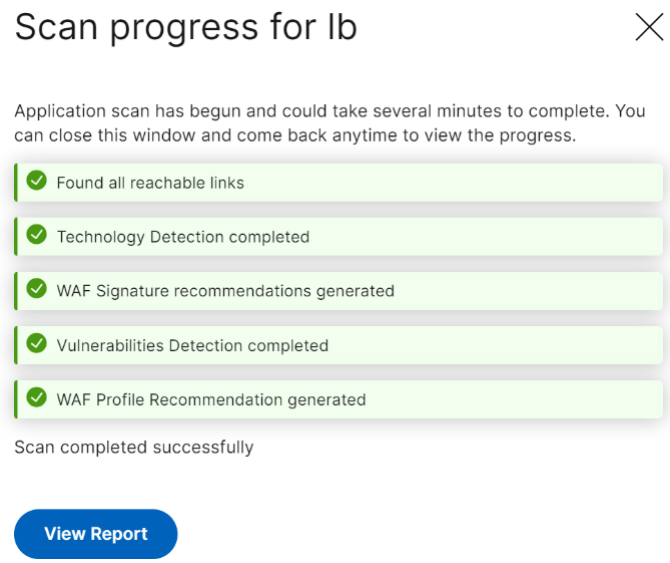
- **Protocolo HTTP/HTTPS**: Seleccione el protocolo de la aplicación.
- **Tiempo de espera del tráfico**: El tiempo de espera (en segundos) de una sola solicitud durante el escaneo. El valor debe ser superior a 0.
- **URL desde la que iniciar el escaneo**: La página principal de la aplicación para iniciar el escaneo. Por ejemplo: `https://www.example.com/home`. La URL debe ser una dirección IPv4 válida. Si las direcciones IP son privadas, debe asegurarse de que se pueda acceder a la dirección IP privada desde la IP de administración de NetScaler ADM.
- **URL de inicio** de sesión: URL a la que se envían los datos de inicio de sesión para la autenticación. En HTML, esta URL se conoce comúnmente como URL de acción.
- **Método de autenticación**: Seleccione el método de autenticación compatible (basado en formularios o encabezados) para su aplicación.
  - La autenticación basada en formularios requiere enviar un formulario a la URL de inicio de sesión con las credenciales de inicio de sesión. Estas credenciales deben tener la forma de campos de formulario y sus valores. A continuación, la aplicación comparte la cookie de sesión que se utiliza para mantener las sesiones durante el análisis.
  - La autenticación basada en encabezados requiere el encabezado de autenticación y su valor en la sección de encabezados. El encabezado de autenticación debe tener un valor válido y se usa para mantener las sesiones durante el escaneo. Los campos del formulario deben dejarse vacíos si están basados en encabezados.
- **Método de solicitud**: Seleccione el método HTTP utilizado al enviar los datos del formulario a la URL de inicio de sesión. Los métodos de solicitud permitidos son **POST**, **GET**y **PUT**.
- **Campos de formulario**: Especifique los datos del formulario que se enviarán a la URL de inicio de sesión. Los campos de formulario solo son obligatorios si selecciona la autenticación basada en formularios. Debe especificar en los pares clave-valor, donde el **nombre del campo** es la clave y el valor del **campo es el valor**. Asegúrese de que todos los campos del formulario necesarios para iniciar sesión se agreguen correctamente, incluidas las contraseñas. Los valores se cifran antes de almacenarlos en la base de datos. Puede hacer clic en **Agregar** para agregar varios campos de formulario. Por ejemplo, Nombre de **campo (nombre** de usuario) y **Valor de campo** (admin).
- **URL de cierre de sesión**: Especifique la URL que finaliza la sesión después de acceder. Por ejemplo: `https://www.example.com/customer/logout`.

2. En **Configuraciones de escaneo**:
   - **Vulnerabilidades que comprobar**: Seleccione las vulnerabilidades para que el analizador las detecte. Actualmente, esto se hace por la inyección de SQL y las infracciones de scripts

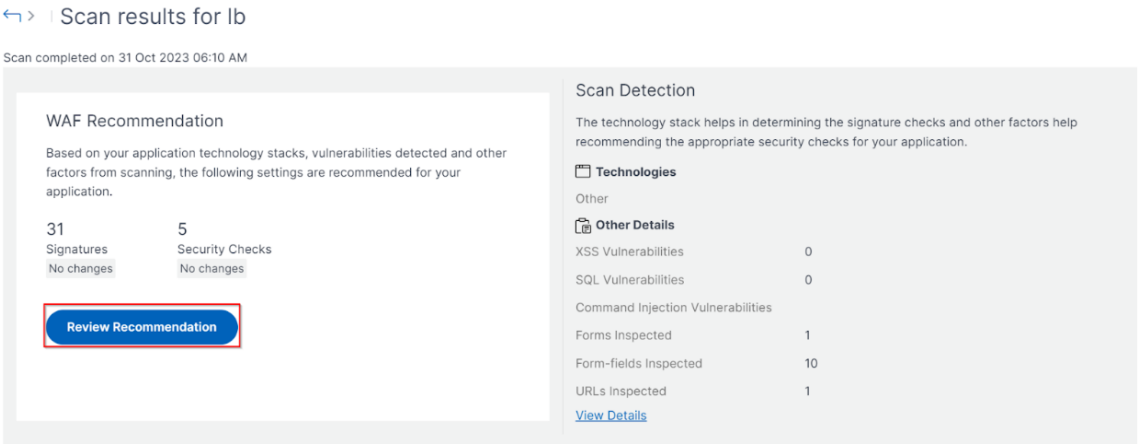
entre sitios. De forma predeterminada, se seleccionan todas las infracciones. Tras seleccionar las vulnerabilidades, simula estos ataques a la aplicación para informar de la posible vulnerabilidad. Se recomienda habilitar esta detección si no se encuentra en el entorno de producción. También se informa de todas las demás vulnerabilidades, sin simular estos ataques a la aplicación.

- **Límite de tamaño de respuesta**: El límite máximo del tamaño de la respuesta. No se escanean las respuestas que superen el valor mencionado. El límite recomendado es de 10 MB (1000000 bytes).
- **Simultaneidad** de solicitudes: el total de solicitudes enviadas a la aplicación web en paralelo.

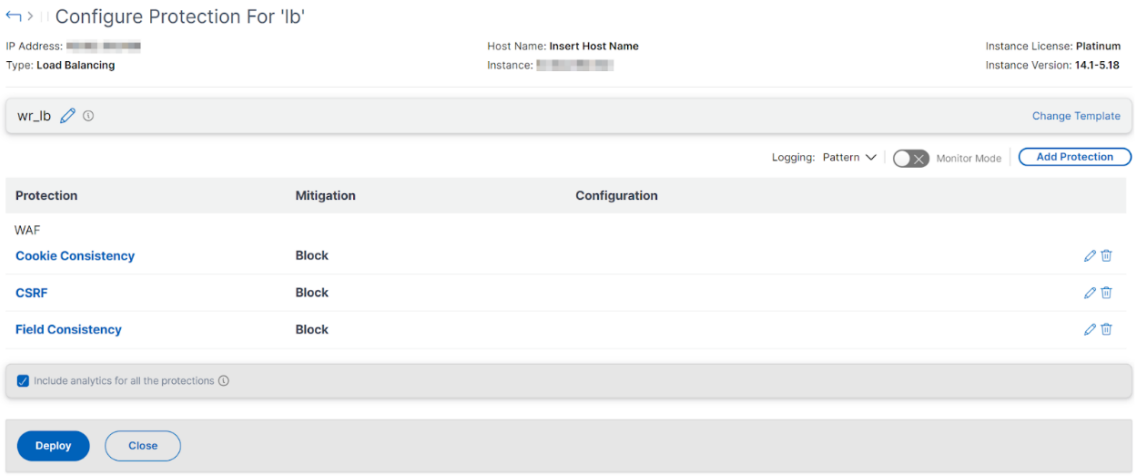
3. La configuración de los ajustes de escaneo del WAF está completa. Puede hacer clic en **Iniciar escaneo** para comenzar el proceso de escaneo y esperar a que finalice el progreso. Una vez finalizado el escaneo, haga clic en **Ver informe**.



4. En la página de resultados del análisis, haga clic en **Revisar recomendación**.



5. Revise las protecciones, o bien modifique o agregue cualquier otra protección y haga clic en **Implementar**.

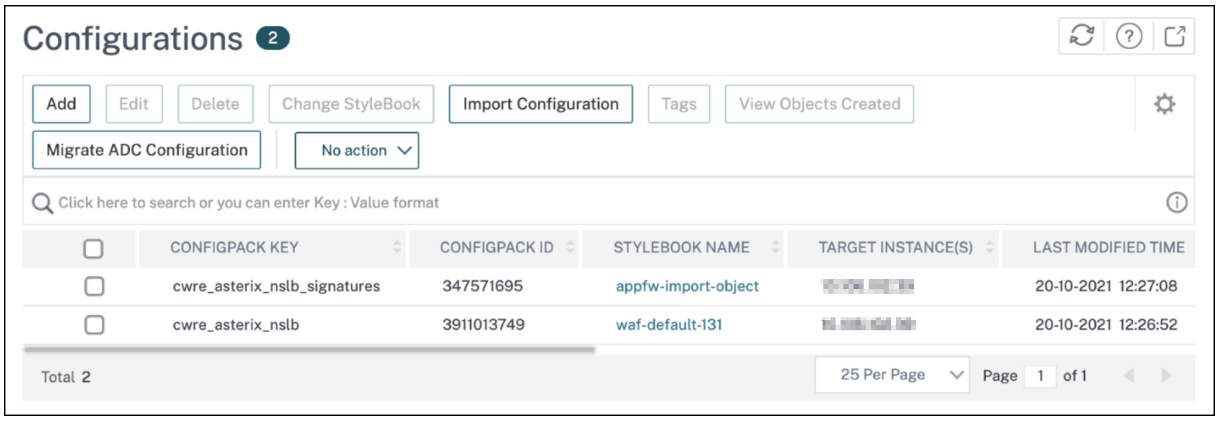


Si aplica correctamente las comprobaciones de seguridad:

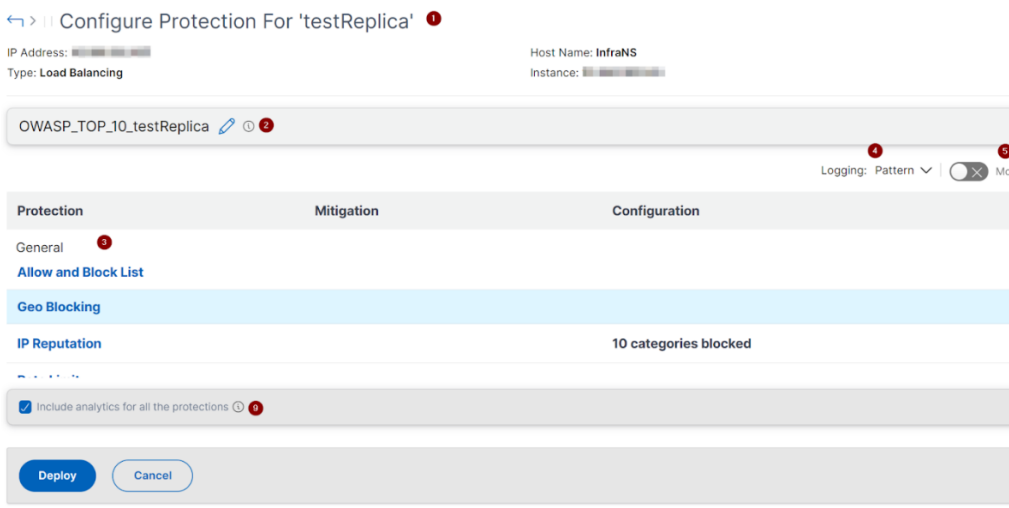
- La configuración se aplica a la instancia de NetScaler a través de StyleBooks, según la versión.
  - Para NetScaler 13.0 `unified-appsec-protection-130`, se usa StyleBook.
  - Para NetScaler 13.1 `unified-appsec-protection-131`, se usa StyleBook.
  - Para NetScaler 14.1 `unified-appsec-protection-141`, se usa StyleBook.
- El perfil `Appfw` se crea en NetScaler y se enlaza a la aplicación mediante `policylabel`.
- Las firmas están enlazadas al perfil appfw, si las firmas recomendadas ya están aplicadas.

> **Nota**
>
> Las comprobaciones de seguridad se admiten en NetScaler 13.0 41.28 o una versión posterior.

Para comprobar que los perfiles y las firmas WAF se aplican a través de los StyleBooks predeterminados, vaya a **Aplicaciones > Configuración > Paquetes de configuración**.



Seleccione y personalice las protecciones



Los 10 mejores de OWASP

1: Proporciona información sobre la aplicación, como la dirección IP, el tipo de servidor virtual, el tipo de licencia, desde qué instancia está configurada la aplicación, etc.

2: Muestra la plantilla seleccionada. Puede cambiarle el nombre según lo que elijas.

3 - Muestra las protecciones. Algunas protecciones requieren información adicional.

4 - Muestra el tipo de registro detallado. Puede seleccionar las siguientes opciones:

- **Patrón**. Registra solo el patrón de infracción.
- **Carga útil del patrón**. Registra el patrón de infracción y 150 bytes de carga adicional de JSON.
- **Patrón, carga útil, cabecera**. Registra el patrón de infracción, 150 bytes de información adicional sobre la carga útil de JSON y el encabezado HTTP.

5 - Permite activar el modo monitor. Si habilita el modo Monitor, el tráfico solo se registra y las mitigaciones no se activan.

6 - Le permite agregar más protecciones. Haga clic en **Agregar protecciones** y revíselas para agregarlas.

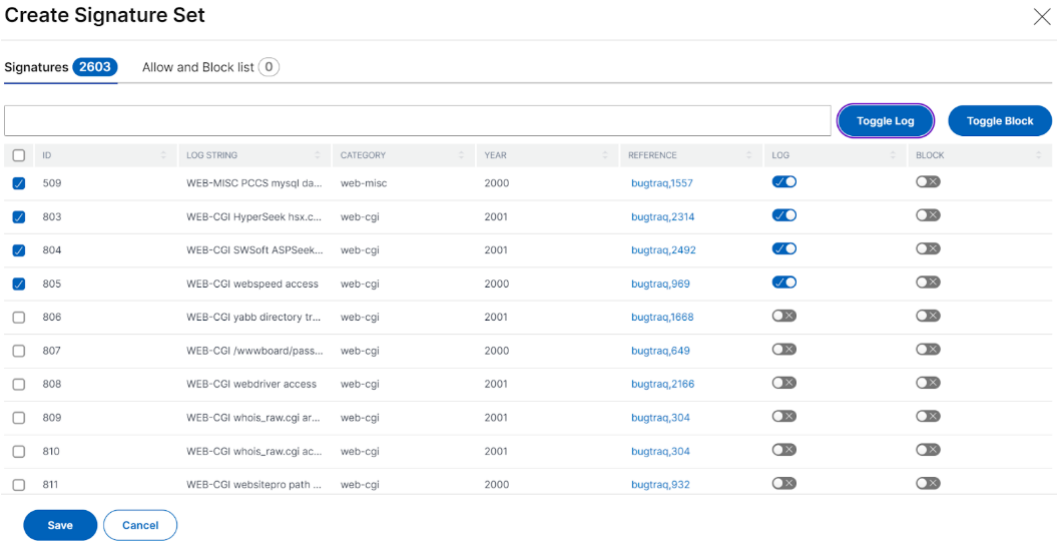
7 - Le permite elegir una nueva plantilla mediante la opción Cambiar plantilla.

8: Permite modificar o eliminar la protección.

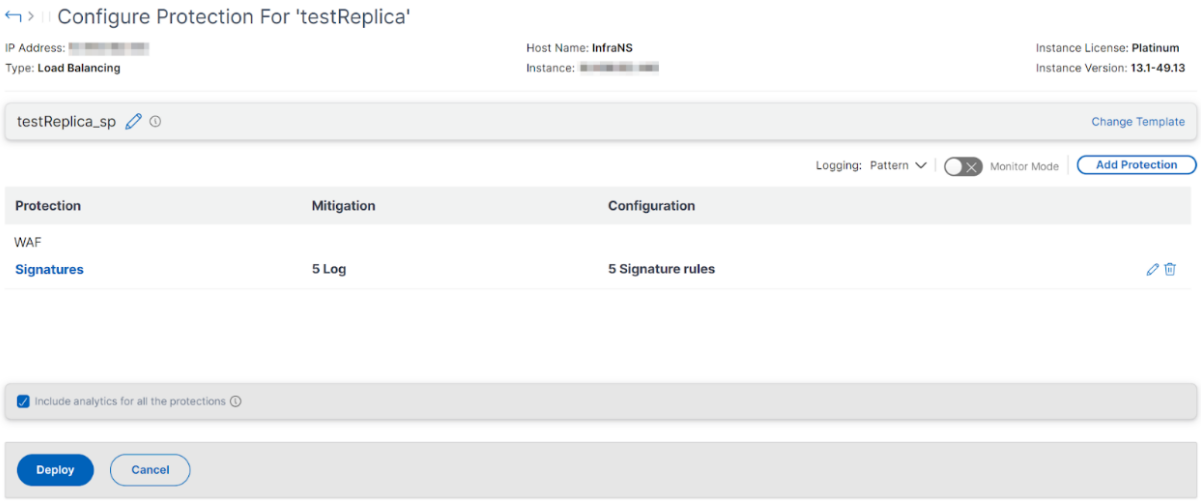
9: Habilita el análisis para las protecciones que seleccione. Esta opción está seleccionada de forma predeterminada. Puede ver los análisis de las protecciones configuradas en **Seguridad > Violaciones de seguridad**.

Después de configurar las protecciones, haga clic en **Implementar**.

Protecciones CVE Para implementar las protecciones de CVE, haga clic en **Crear protección de CVE.** En la página **Crear conjunto de firmas**, seleccione las firmas de la lista para configurar la acción de registro o bloqueo y, a continuación, haga clic en **Guardar**.

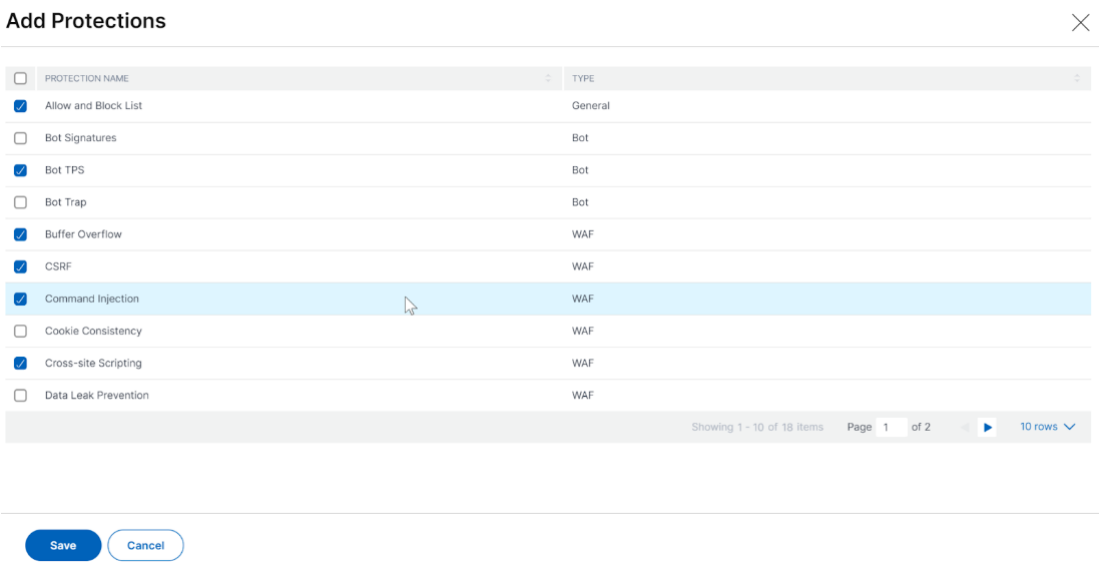


Después de hacer clic en **Guardar**, puede ver las firmas agregadas a la página de configuración.



También puede hacer clic en **Agregar protección** para agregar más protecciones a la aplicación. Después de configurar todas las protecciones, haga clic en **Implementar**.

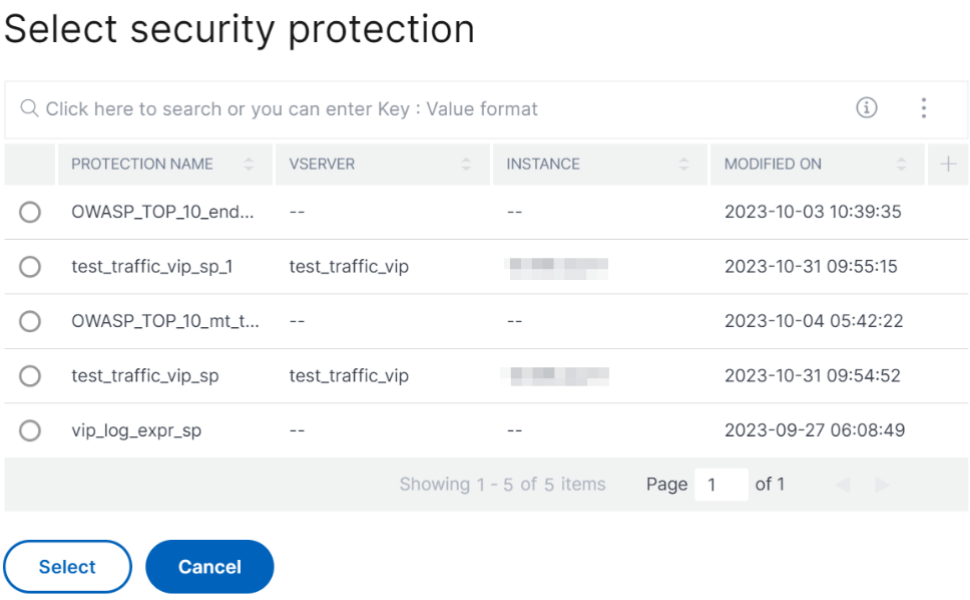
Protección personalizada Para realizar la implementación con protecciones según sus necesidades, haga clic en **Crear nueva protección**. En la página **Agregar protecciones**, seleccione las protecciones que quiere implementar y haga clic en **Guardar**.



Después de hacer clic en **Guardar**, revise las protecciones seleccionadas en la página de configuración y, a continuación, haga clic en **Implementar**.

Elija las protecciones existentes

Para implementar las protecciones existentes de una aplicación a otra, seleccione una protección existente de la lista.



Tras seleccionar una protección, las protecciones existentes se clonan y se muestran en la página de configuración. Puede modificarlos en función de sus necesidades y, a continuación, hacer clic en **Implementar**.

Ver detalles de infracciones de seguridad de la aplicación

January 30, 2024

Las aplicaciones web que están expuestas a Internet se han vuelto vulnerables a los ataques drásticamente. NetScaler ADM le permite visualizar detalles de infracciones accionables para proteger las aplicaciones contra ataques. Navegue hasta **Seguridad** > **Violaciones de seguridad** para obtener una solución de panel único para:

- Visualice las aplicaciones con visibilidad completa de los detalles de las amenazas asociadas tanto en las infracciones de seguridad de WAF como en las infracciones de seguridad
- Acceda a las infracciones de seguridad de la aplicación en función de sus categorías como **Network**, **Bot** y **WAF**
- Tomar medidas correctivas para proteger las aplicaciones

La página **Infracciones de Seguridad** tiene las siguientes opciones:

- **Descripción general de la aplicación**: muestra una descripción general de las aplicaciones que tienen infracciones totales, infracciones de WAF y bot totales, infracciones por país, etc. Para obtener más información, consulte Descripción general de la aplicación.
- **Todas las infracciones**: muestra los detalles de infracción de seguridad de la aplicación. Para obtener más información, consulte Todas las infracciones.

Requisito previo

Asegúrese de que el **recopilador de métricas** esté habilitado. De forma predeterminada, **Metrics Collector** está habilitado en la instancia de NetScaler. Para obtener más información, consulte Configurar el análisis inteligente de aplicaciones.

Integración con Splunk

January 30, 2024

Ahora puede integrar NetScaler ADM con Splunk para ver los análisis de:

- Violaciones de WAF
- Infracciones de bots
- Información sobre certificados SSL

- Eventos y métricas

El complemento Splunk le permite:

- Combine todas las demás fuentes de datos externas.
- Proporcione una mayor visibilidad de los análisis en un lugar centralizado.

NetScaler ADM recopila eventos de Bot, WAF y SSL y los envía a Splunk periódicamente. El complemento del modelo de información común (CIM) de Splunk convierte los eventos en datos compatibles con CIM. Como administrador, utilizando los datos compatibles con CIM, puede ver los eventos en el panel de control de Splunk.

Para que la integración tenga éxito, debe:

- Configurar Splunk para recibir datos de NetScaler ADM
- Configurar NetScaler ADM para exportar datos a Splunk
- Ver paneles en Splunk

Configurar Splunk para recibir datos de NetScaler ADM

En Splunk, debes:

1. Configure el extremo del recopilador de eventos HTTP de Splunk y genere un token
2. Instale el complemento del modelo de información común (CIM) de Splunk
3. Instale el normalizador CIM (aplicable solo para información sobre WAF y bots)
4. Prepare un panel de ejemplo en Splunk

Configure el extremo del recopilador de eventos HTTP de Splunk y genere un token

Primero debes configurar el recopilador de eventos HTTP en Splunk. Esta configuración permite la integración entre el ADM y Splunk para enviar los datos. A continuación, debes generar un token en Splunk para:

- Habilite la autenticación entre ADM y Splunk.
- Reciba datos a través del extremo del recopilador de eventos.

1. Inicia sesión en Splunk.
2. Vaya a **Configuración > Entradas de datos > Recopilador de eventos HTTP** y haga clic en **Agregar nuevo**.
3. Especifique los siguientes parámetros:

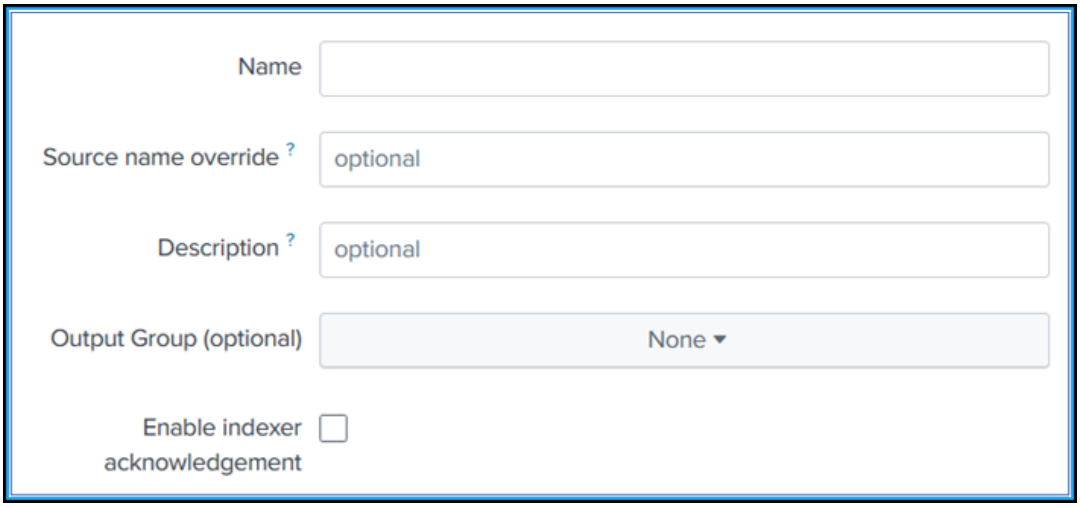
a) **Nombre**: especifique un nombre de su elección.

b) **Anulación del nombre de origen (opcional)**: si establece un valor, anula el valor de origen del recopilador de eventos HTTP.

c) **Descripción (opcional)**: especifique una descripción.

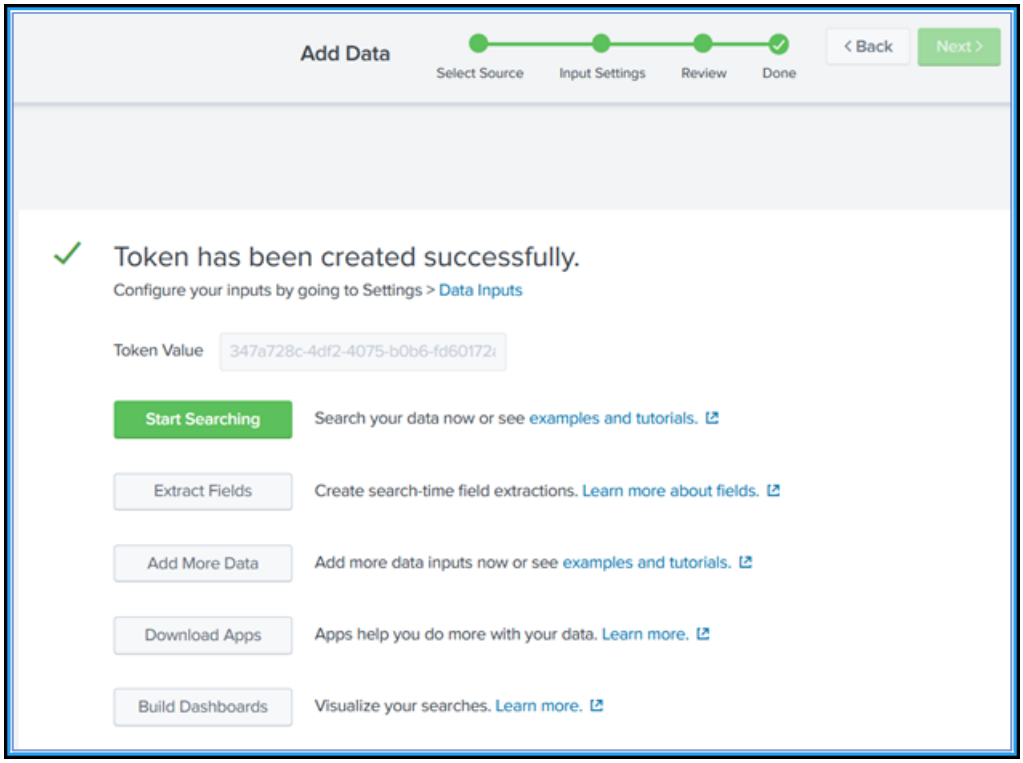
d) **Grupo de salida (opcional)**: de forma predeterminada, esta opción aparece seleccionada como Ninguna.

e) **Habilitar el reconocimiento del indexador**: de forma predeterminada, esta opción no está seleccionada.



4. Haga clic en **Siguiente**.
5. Si lo quiere, puede establecer parámetros de entrada adicionales en la página **Configuración de entrada**.
6. Haga clic en **Revisar** para comprobar las entradas y, a continuación, en **Enviar**.

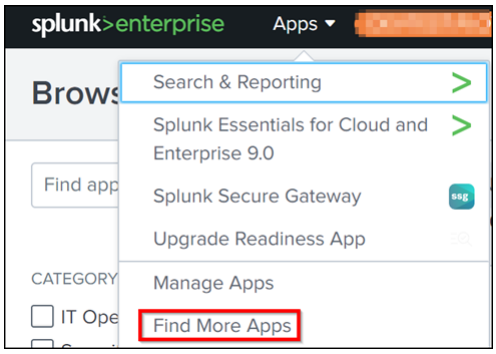
   Se genera un token. Debe usar este token cuando agregue detalles en NetScaler ADM.



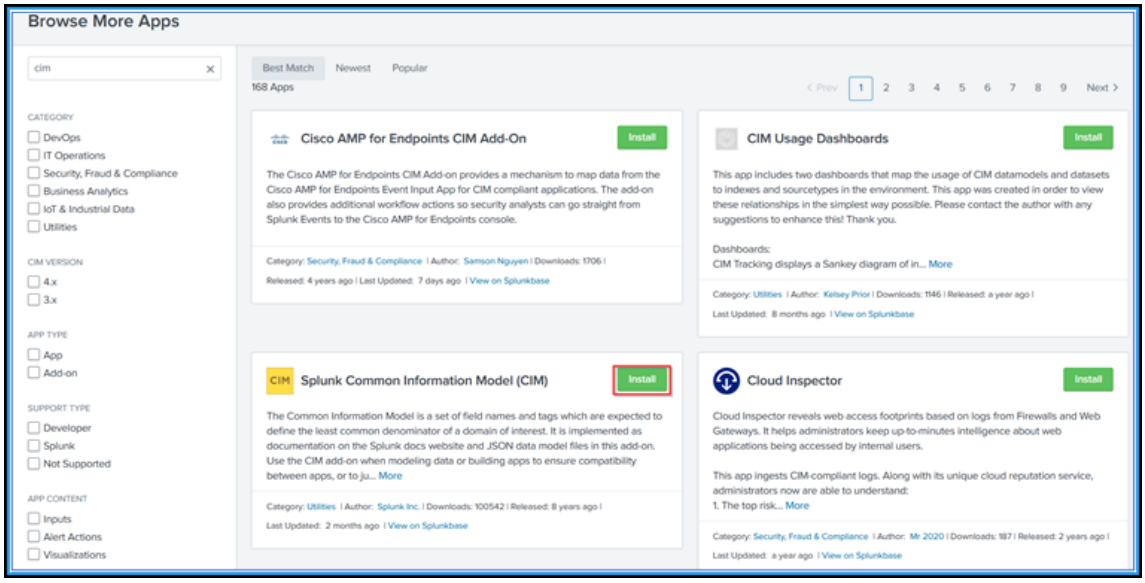
Instale el modelo de información común de Splunk

En Splunk, debes instalar el complemento CIM de Splunk. Este complemento garantiza que los datos recibidos de NetScaler ADM normalicen los datos ingeridos y coincidan con un estándar común, ya que utilizan los mismos nombres de campo y etiquetas de eventos para eventos equivalentes.

1. Inicia sesión en Splunk.
2. Vaya a **Aplicaciones > Buscar más aplicaciones**.



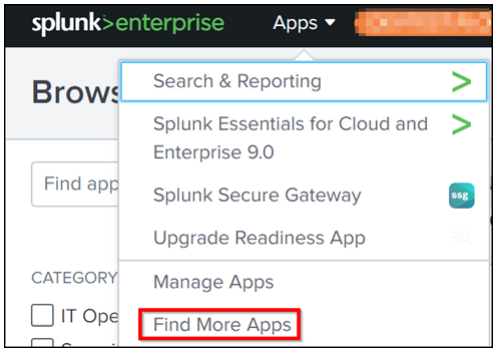
3. Escriba **CIM** en la barra de búsqueda y pulse **Entrar** para obtener el complemento del **modelo de información común (CIM) de Splunk** y haga clic en **Instalar**.



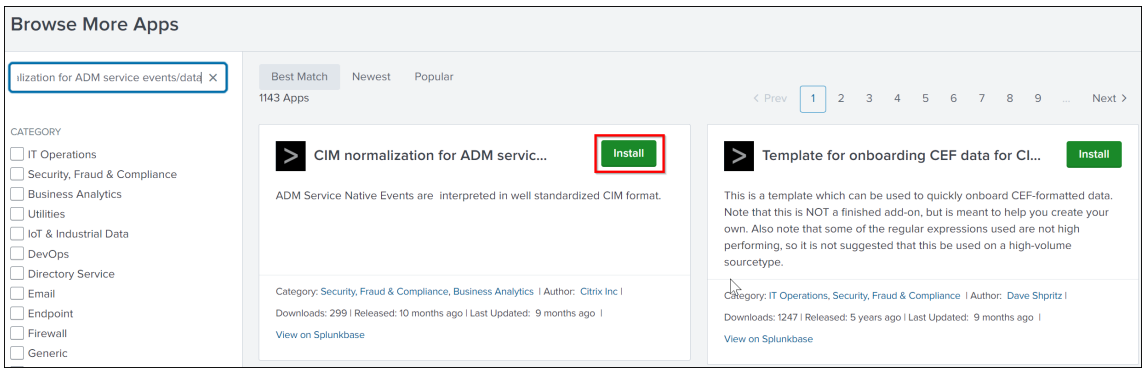
Instale el normalizador CIM

El normalizador CIM es un complemento adicional que debes instalar para ver la información sobre el WAF y los bots en Splunk.

1. En el portal de Splunk, vaya a **Aplicaciones > Buscar más aplicaciones**.



2. Escriba **normalización CIM para eventos o datos del servicio ADM** en la barra de búsqueda, presione **Entrar** para obtener el complemento y haga clic en **Instalar**.



Prepare un panel de ejemplo en Splunk

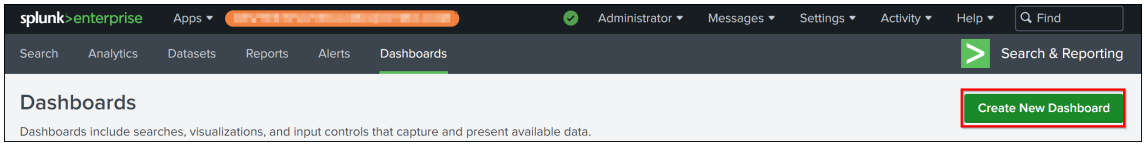
Después de instalar el CIM de Splunk, debe preparar un panel de ejemplo con una plantilla para WAF y Bot, información sobre los certificados SSL y eventos y métricas. Puede descargar el archivo de plantilla del panel (`.tgz`), usar cualquier editor (por ejemplo, el bloc de notas) para copiar su contenido y crear un panel pegando los datos en Splunk.

> **Nota:**
>
> El siguiente procedimiento para crear un panel de ejemplo se aplica a todos los casos de uso. Debe utilizar el archivo `json` requerido.

1. Inicie sesión en la página de descargas de Citrix y descargue el panel de ejemplo disponible en Paneles de ejemplo para terminales de terceros.
2. Extraiga el archivo, abra el archivo `json` con cualquier editor y copie los datos del archivo.

   Después de extraer, obtendrá tres `json` archivos. Usa el:

   - `adm_splunk_security_violations.json` archivo para crear un panel de ejemplo de WAF y Bot.
   - `adm_splunk_ssl_certificate.json` archivo para crear un panel de muestra de información sobre certificados SSL.
   - `adm_splunk_events_and_metrics_history.json` archivo para crear un panel de métricas y eventos de ADM.
3. En el portal de Splunk, vaya a **Búsqueda e informes > Paneles** y, a continuación, haga clic en **Crear panel de mandos**.



4. En la página **Crear panel de mandos**, especifique los siguientes parámetros:

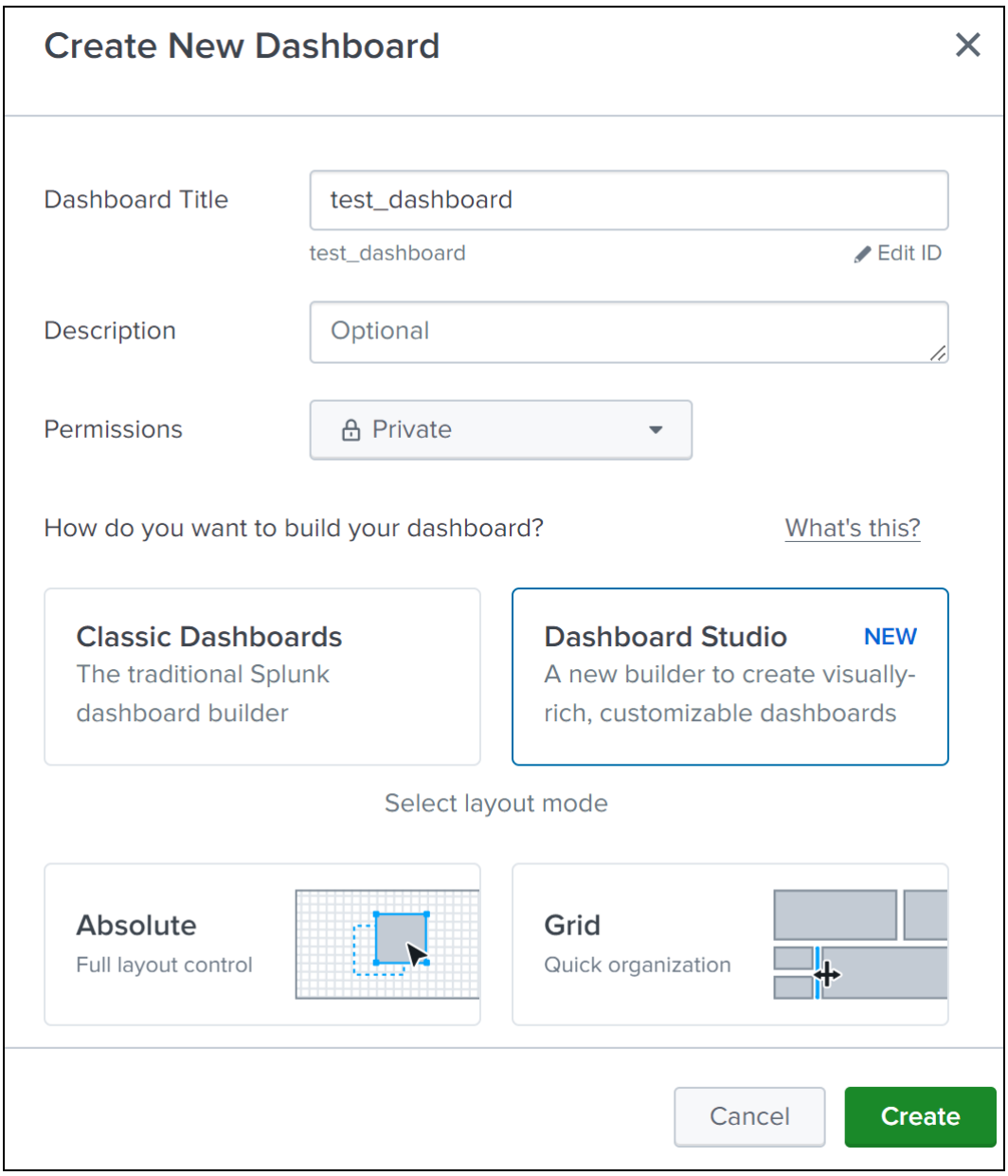
   a) **Título del panel**: Proporcione un título.

   b) **Descripción**: Si lo quiere, puede proporcionar una descripción como referencia.

   c) **Permiso**: Seleccione **Privado** o **Compartido en la aplicación** según sus necesidades.

   d) Seleccione **Panel de mandos de Studio**.

   e) Seleccione cualquier diseño (**Absoluto** o **Cuadrícula**) y, a continuación, haga clic en **Crear**.

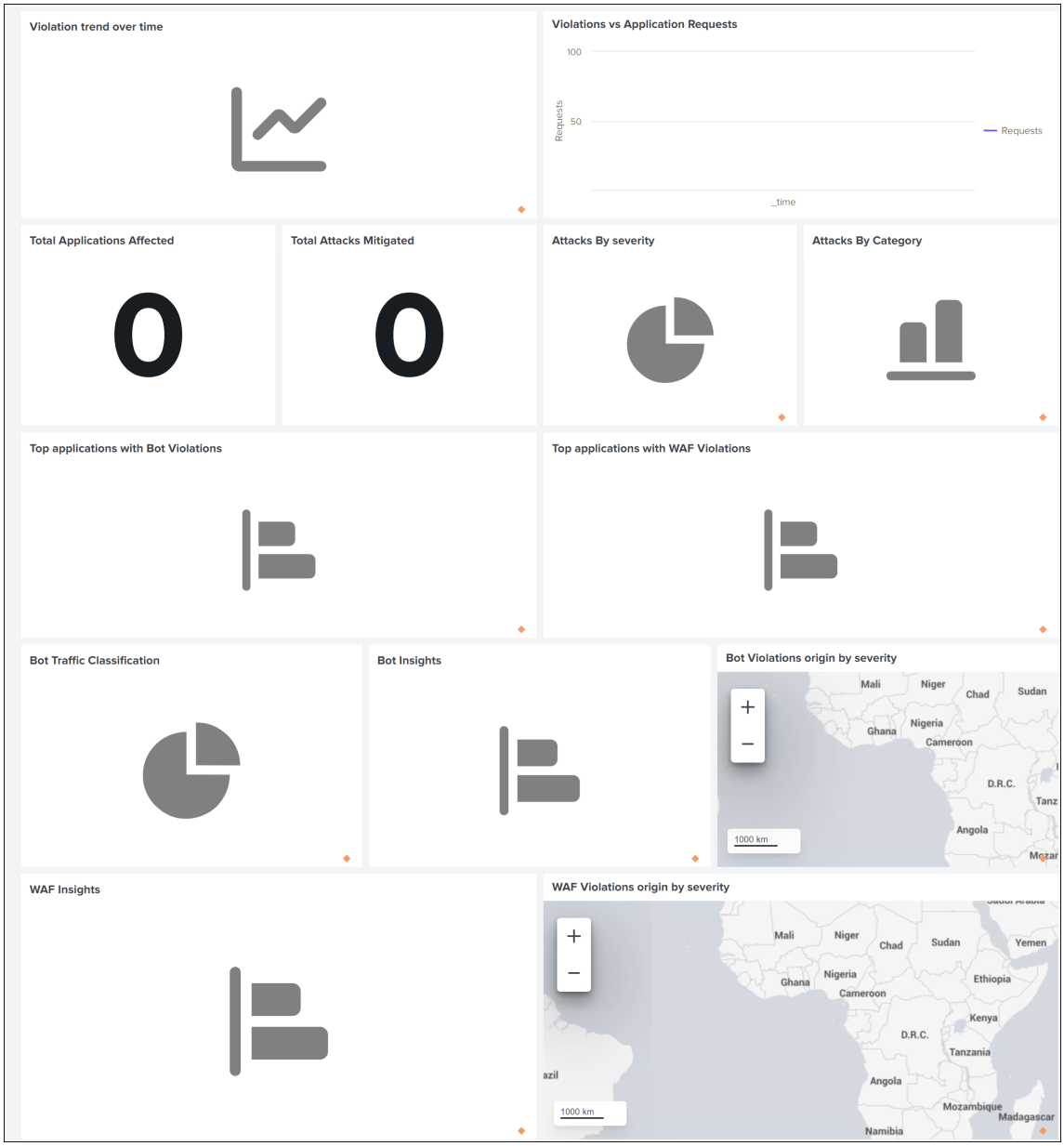


Después de hacer clic en **Crear**, seleccione el icono **Origen** en el diseño.

5. Elimine los datos existentes, pegue los datos que copió en el paso 2 y haga clic en **Atrás**.
6. Haga clic en **Guardar**.

   Puede ver el panel de ejemplo.

   A continuación se muestra un ejemplo de panel de control para WAF y bot.



Configurar NetScaler ADM para exportar datos a Splunk

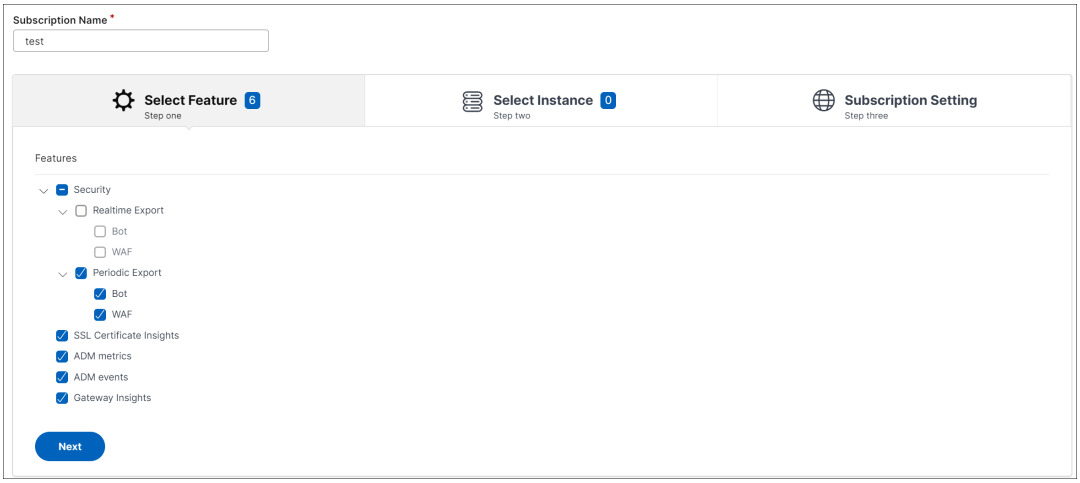
Ya lo tienes todo preparado en Splunk. El último paso consiste en configurar NetScaler ADM mediante la creación de una suscripción y la adición del token.

Al completar el siguiente procedimiento, podrá ver el panel actualizado en Splunk que está disponible actualmente en su NetScaler ADM:

1. Inicie sesión en NetScaler ADM.
2. Vaya a **Configuración > Integración de ecosistemas**.

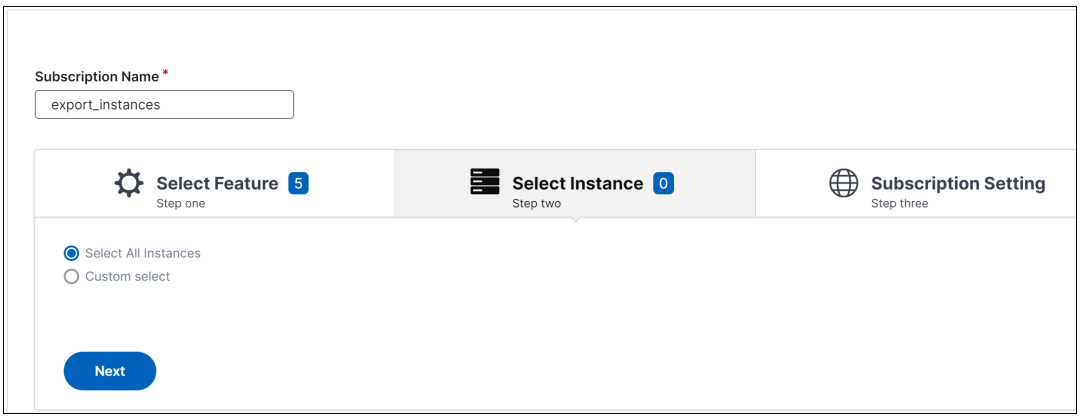
3. En la página **Suscripciones**, haga clic en **Agregar**.
4. Especifique un nombre de su elección en el campo **Nombre de la suscripción**.
5. En la ficha **Seleccionar función**, puede seleccionar las funciones que quiere exportar y hacer clic en **Siguiente**.

    - **Exportación en tiempo real**: Las infracciones seleccionadas se exportan inmediatamente a Splunk.
    - **Exportación periódica**: Las infracciones seleccionadas se exportan a Splunk en función de la duración que seleccione.



6. En la ficha **Seleccionar instancia**, puede elegir **Seleccionar todas las instancias** o Selección **personalizada**y, a continuación, hacer clic en **Siguiente**.

    - **Seleccione Todas las instancias**: Exporta datos a Splunk desde todas las instancias de NetScaler.
    - **Selección personalizada: permite seleccionar** las instancias de NetScaler de la lista. Si selecciona instancias específicas de la lista, los datos se exportarán a Splunk solo desde las instancias de NetScaler seleccionadas.



7. En la ficha **Configuración de suscripción** :

   a) **Tipo de punto final**: Seleccione **Splunk**.

   b) **URL del punto final**: Especifique los detalles del punto final de Splunk. El punto final debe estar en el formato https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event.

   > **Nota**
   >
   > Se recomienda utilizar HTTPS por motivos de seguridad.

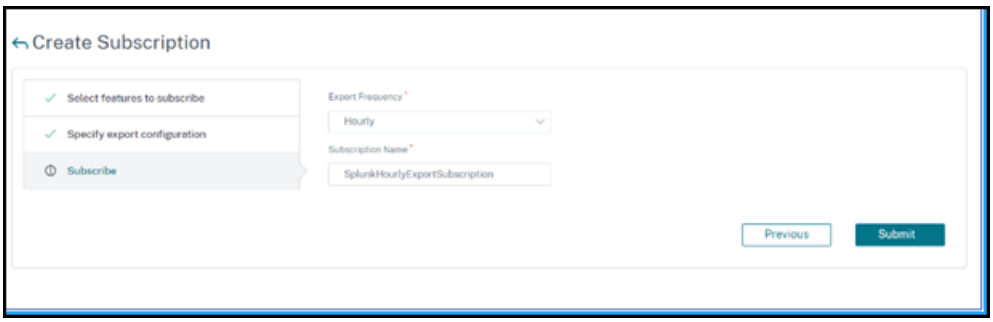
   - **SPLUNK_PUBLIC_IP**: Una dirección IP válida configurada para Splunk.
   - **SPLUNK_HEC_PORT**: Indica el número de puerto que especificó durante la configuración del punto final del evento HTTP. El número de puerto predeterminado es 8088.
   - **Servicios/coleccionador/evento**: Indica la ruta de la aplicación HEC.

   c) **Token de autenticación**: Copie y pegue el token de autenticación de la página de Splunk.

   d) **Seleccione Frecuencia**: Seleccione **Diaria** u **Horaria** de la lista. Según la selección, NetScaler ADM exporta los detalles a Splunk.

   > **Nota**
   >
   > Aplicable solo si ha seleccionado infracciones en la **exportación periódica**.

   e) Haga clic en **Submit**.



   > **Nota**
   >
   > - Cuando se configura con la opción de **exportación periódica** por primera vez, los datos de las funciones seleccionadas se envían a Splunk inmediatamente. La siguiente frecuencia de exportación se realizará en función de su selección (diaria u horaria).
   > - Cuando se configura con la opción **Realtime Export** por primera vez, los datos de las funciones seleccionadas se envían a Splunk inmediatamente tan pronto como se detectan las infracciones en NetScaler ADM.

Ver paneles en Splunk

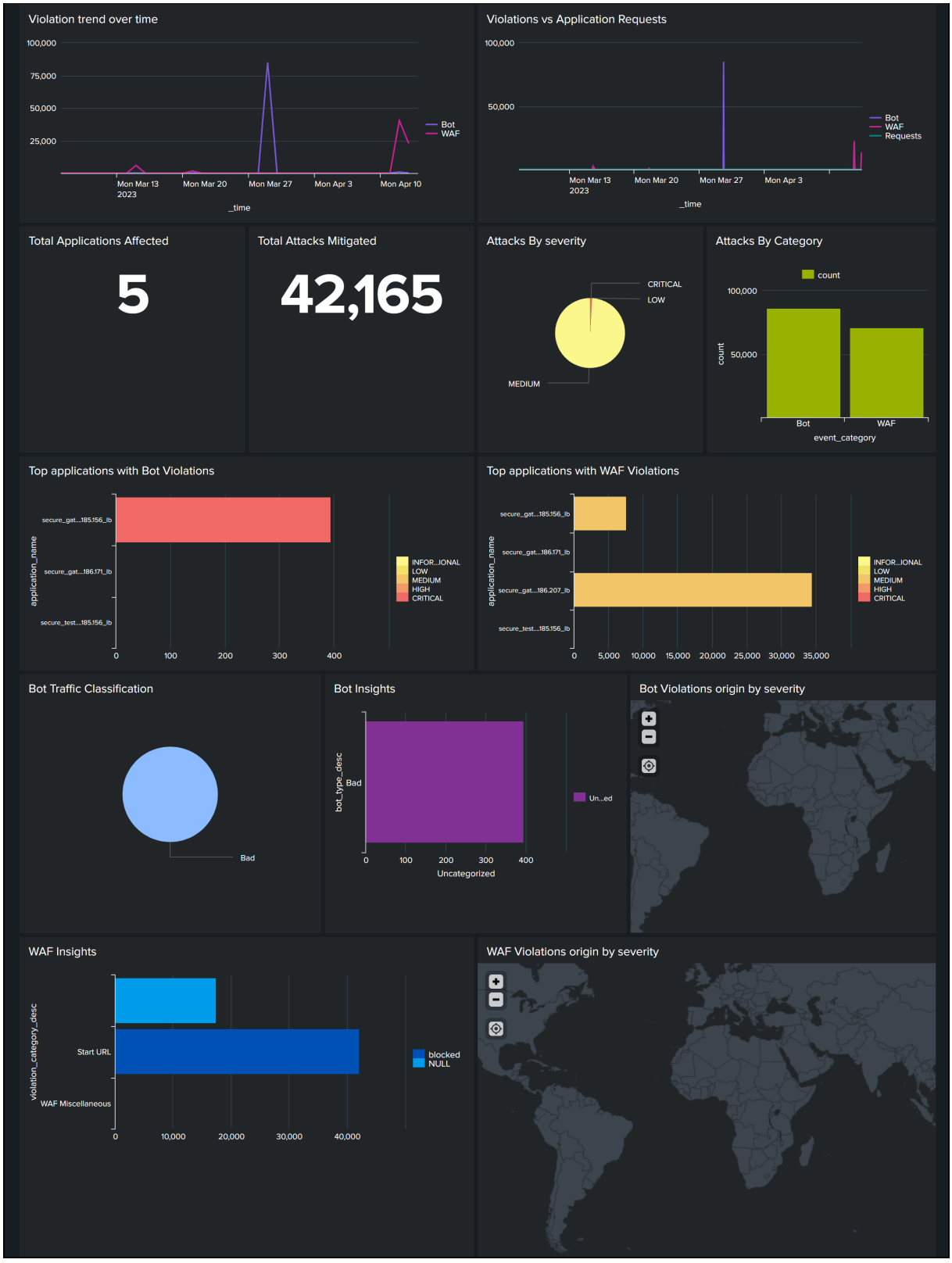
Tras completar la configuración en NetScaler ADM, los datos se exportan desde NetScaler ADM y los eventos aparecen en Splunk.

> **Nota:**
>
> Para ver inmediatamente los datos actualizados de información sobre los certificados SSL en Splunk, haga clic en **Poll Now** en el panel SSL de NetScaler ADM**(**Infraestructura > Panel SSL).

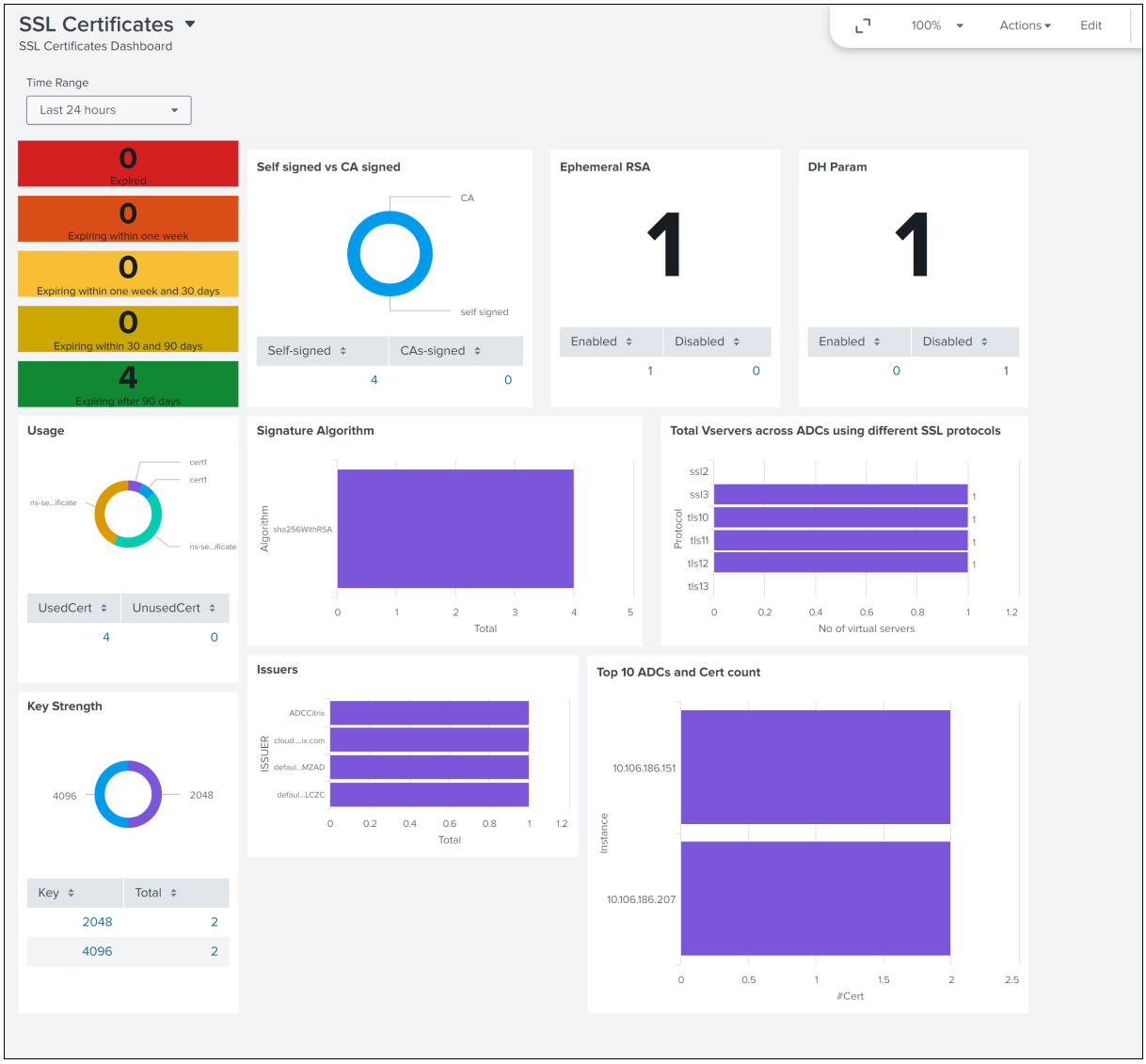
Ya está todo listo para ver el panel actualizado en Splunk sin ningún paso adicional.

Vaya a Splunk y haga clic en el panel que ha creado para ver el panel actualizado.

El siguiente es un ejemplo del panel actualizado de WAF y Bot:

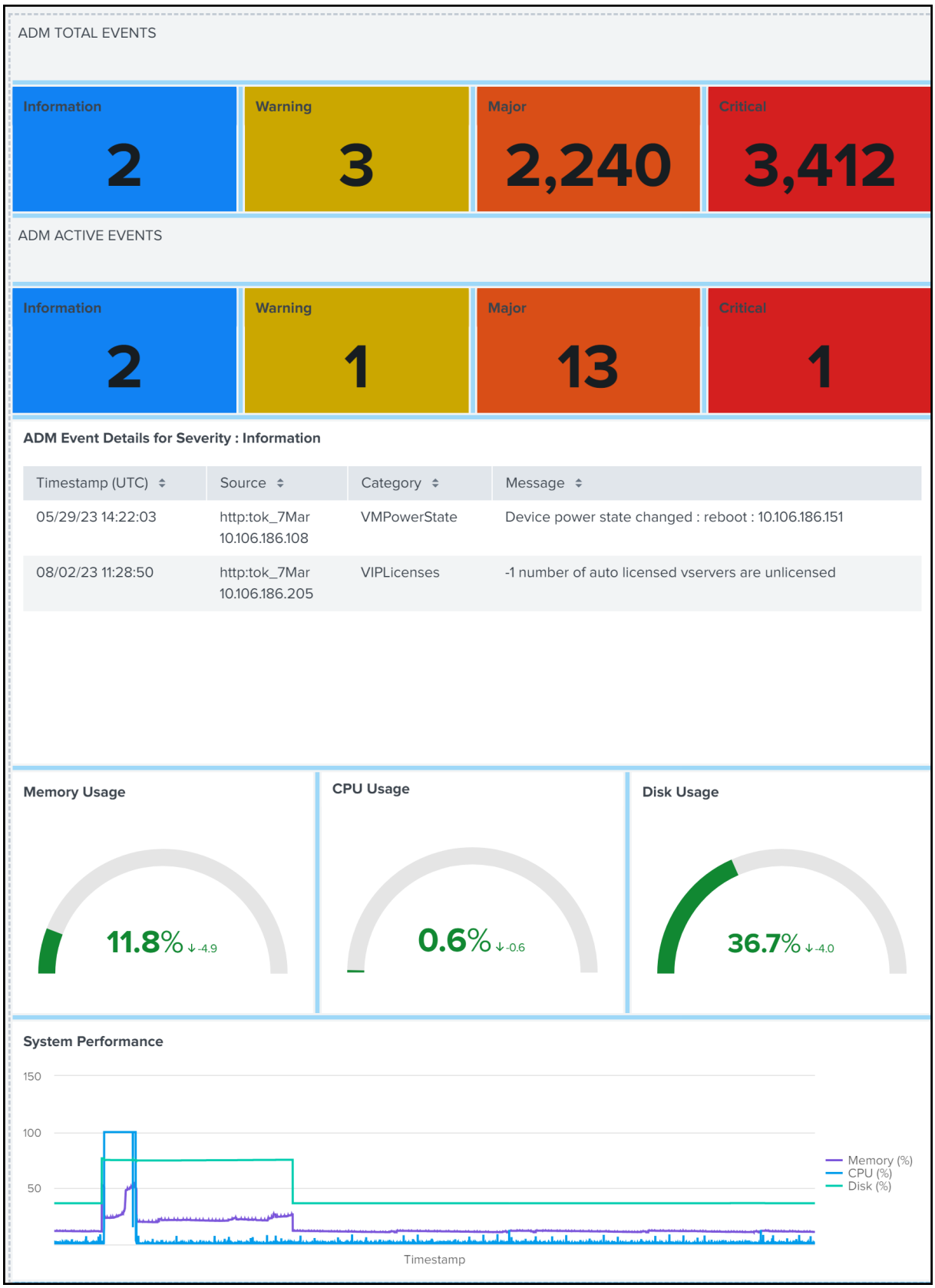


El siguiente panel es un ejemplo del panel de información actualizado sobre los certificados SSL.



El siguiente panel es un ejemplo del panel de estadísticas y eventos actualizado.

> **Nota:**
>
> Los datos de uso de la memoria, la CPU y el disco muestran el valor actual del NetScaler ADM. La tendencia al alza y a la baja de estos valores se muestra en función de la comparación del valor anterior cada 5 minutos.



Además del panel de control, también puede ver los datos en Splunk después de crear la suscripción.

1. En Splunk, haga clic en **Buscar e informes**.
2. En la barra de búsqueda:
    - Escriba `sourcetype="metrics"` y seleccione la duración en la lista para ver los datos de las métricas de ADM.
    - Escriba `sourcetype="event"` y seleccione la duración en la lista para ver los datos de los eventos de ADM.
    - Escriba `sourcetype="bot"` o `sourcetype="waf"` y seleccione la duración en la lista para ver los datos del bot/WAF.
    - Escriba `sourcetype="ssl"` y seleccione la duración en la lista para ver los datos de información del certificado SSL.

Integración de New Relic

January 30, 2024

Ahora puede integrar NetScaler ADM con New Relic para ver los análisis de las infracciones de WAF y Bot en su panel de control de New Relic. Con esta integración, puede:

- Combine todas las demás fuentes de datos externas en su panel de control de New Relic.
- Obtenga visibilidad de los análisis en un lugar centralizado.

NetScaler ADM recopila los eventos de Bot y WAF y los envía a New Relic en tiempo real o de forma periódica, según su elección. Como administrador, también puede ver los eventos de Bot y WAF en su panel de control de New Relic.

Requisitos previos

Para que la integración tenga éxito, debe:

- Obtén un punto final del evento New Relic con el siguiente formato:

  `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`

  Para obtener más información sobre la configuración de un punto final de eventos, consulte la documentación de New Relic.

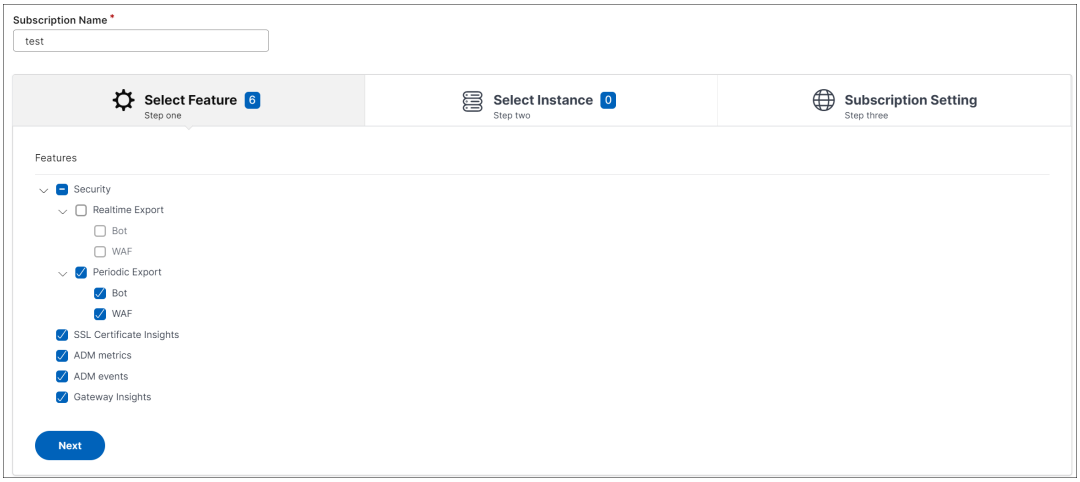
Para obtener más información sobre cómo obtener un ID de cuenta, consulte la documentación de New Relic.

- Obtenga una nueva clave de reliquia. Para obtener más información, consulte la documentación de New Relic.
- Agregar los detalles clave en NetScaler ADM

Agregar los detalles clave en NetScaler ADM

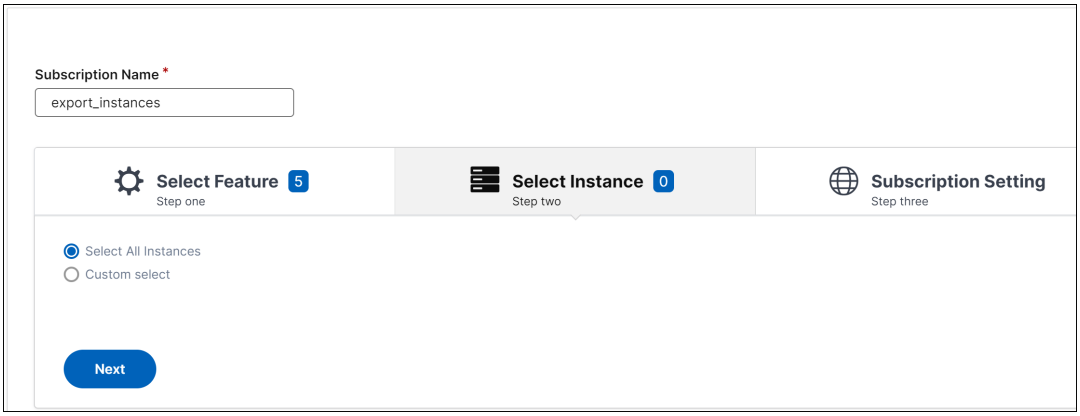
Después de generar un token, debe agregar detalles en NetScaler ADM para integrarlo con New Relic.

1. Inicie sesión en NetScaler ADM.
2. Vaya a **Configuración > Integración de ecosistemas**.
3. En la página **Suscripciones**, haga clic en **Agregar**.
4. En la ficha **Seleccionar función**, seleccione las funciones que desee exportar y haga clic en **Siguiente**.
    - **Exportación en tiempo real**: Las infracciones seleccionadas se exportan inmediatamente a New Relic.
    - **Exportación periódica**: Las infracciones seleccionadas se exportan a New Relic en función de la duración que seleccione.



5. En la ficha **Seleccionar instancia**, puede elegir **Seleccionar todas las instancias** o Selección **personalizada**y, a continuación, hacer clic en **Siguiente**.
    - **Seleccione Todas las instancias**: Exporta datos a New Relic desde todas las instancias de NetScaler.

- **Selección personalizada: permite seleccionar** las instancias de NetScaler de la lista. Si selecciona instancias específicas de la lista, los datos se exportarán a New Relic solo desde las instancias de NetScaler seleccionadas.



6. En la ficha **Configuración de suscripción** :

   a) **Tipo de punto final**: Seleccione **Nueva reliquia**.

   b) **URL del punto final**: Especifique los detalles del punto final de New Relic. El punto final debe estar en el formato `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`.

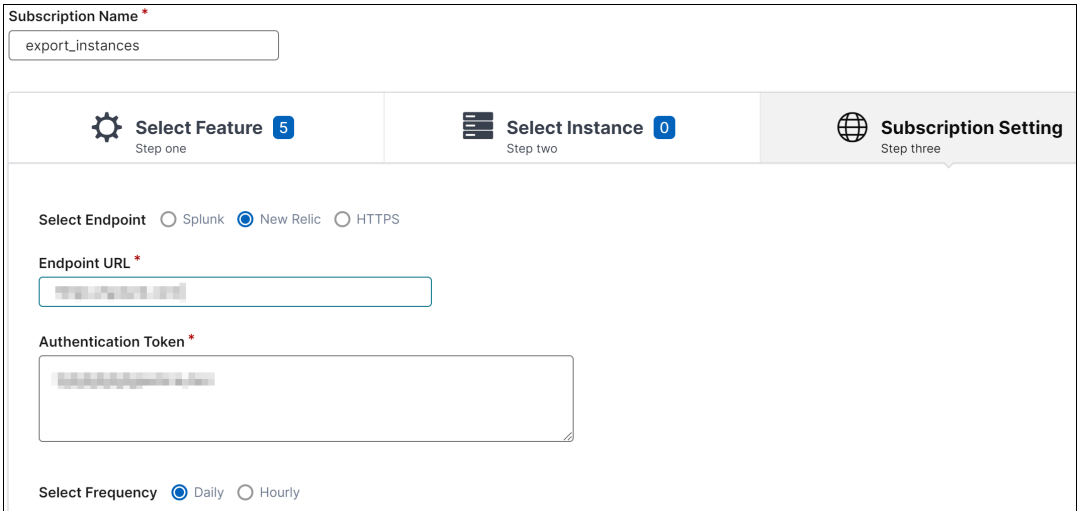
   > **Nota**
   >
   > Se recomienda utilizar HTTPS por motivos de seguridad.

   c) **Token de autenticación**: Copie y pegue el token de autenticación de la página New Relic.

   d) **Seleccione Frecuencia**: Seleccione **Diaria** u **Horaria** de la lista. Según la selección, NetScaler ADM exporta los detalles a New Relic.

   > **Nota**
   >
   > Aplicable solo si ha seleccionado infracciones en la **exportación periódica**.

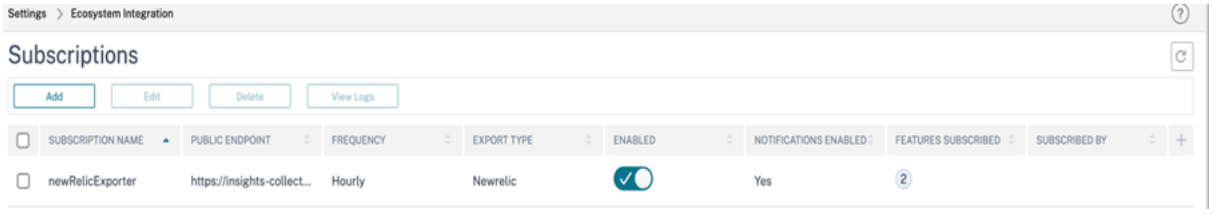
   e) Haga clic en **Submit**.



Nota

- Cuando se configura con la opción **Exportación periódica** por primera vez, los datos de las funciones seleccionadas se envían inmediatamente a New Relic. La siguiente frecuencia de exportación se realizará en función de su selección (diaria u horaria).
- Al configurar con la opción **Exportación en tiempo real** por primera vez, los datos de las funciones seleccionadas se envían a New Relic inmediatamente en cuanto se detectan las infracciones en NetScaler ADM.

La configuración está completa. Puede ver los detalles en la página **Suscripciones**.

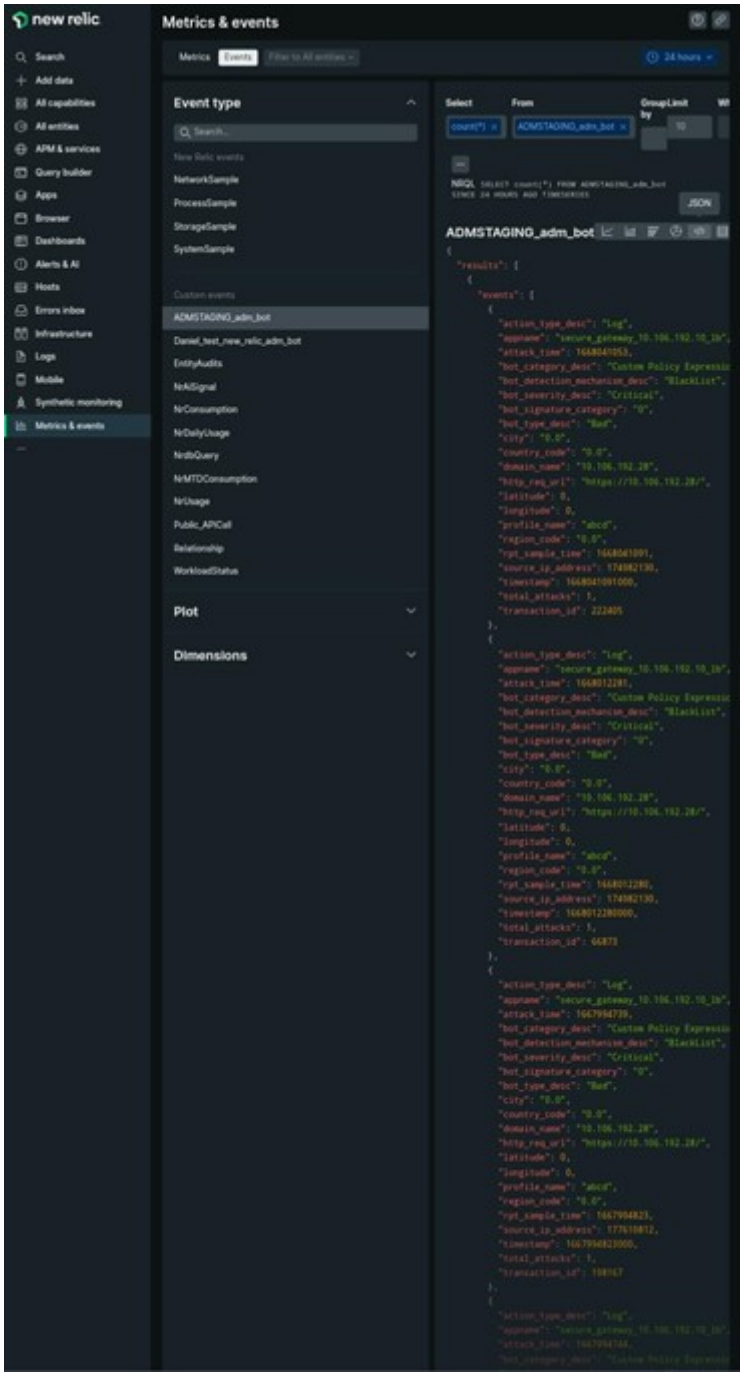


Panel de mandos de New Relic

Cuando los eventos se exportan a New Relic, puede ver los detalles de los eventos en **Métricas y eventos** en el siguiente formato JSON:

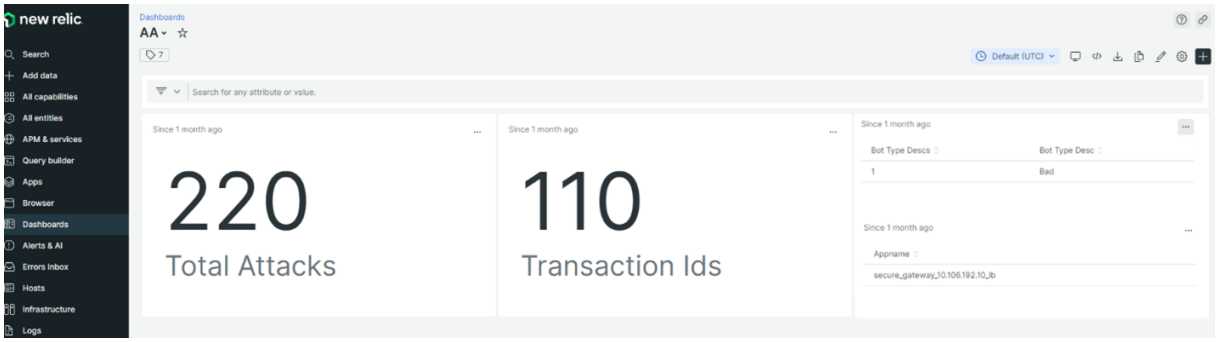
<subsription_name>_adm_<event name> donde el nombre del evento puede ser Bot, WAF, etc.

En el siguiente ejemplo, ADMSTAGING es <subscription_name> y bot es <event_name>.



Una vez que hayas incorporado los datos JSON a su panel de control de New Relic, como administrador, puede usar el NRQL (lenguaje de consulta de New Relic) y crear un panel personalizado con facetas y widgets según su elección mediante la creación de consultas en torno a los datos ingeridos. Para obtener más información, consulte `https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/`

El siguiente es un ejemplo de panel creado con el NRQL:



Para crear este panel, se requieren las siguientes consultas:

- Widget 1: Total de ataques únicos en la tabla de eventos

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- Widget 2: ID de transacción únicos en la tabla de eventos

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days
   ago
  ```

- Widget 3: Total de tipos de bots únicos y sus recuentos

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <
  event_name> since 30 days ago
  ```

- Widget 4: Total de nombres de aplicaciones únicos que detectan infracciones de bots

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

Gateway Insight

January 30, 2024

En una implementación de NetScaler 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 NetScaler Gateway y conocer la actividad del usuario y los motivos del error de inicio de sesión. Por lo general, esta información 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 NetScaler 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 la cantidad de aplicaciones iniciadas, la cantidad de sesiones totales y activas, la cantidad de bytes totales y el ancho de banda consumido 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 NetScaler 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 NetScaler 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 NetScaler ADM deben ser iguales o posteriores a las del dispositivo NetScaler Gateway.
- Se puede ver una hora de informes de Gateway Insight para instancias de NetScaler con licencia Advanced. Una licencia Premium es imprescindible para ver los informes de Gateway Insight más allá de una hora.

Limitaciones

- NetScaler 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 NetScaler.

- 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 las fallas en el dispositivo NetScaler 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
  - Conexión de OAuth-OpenID

    Para la autenticación de OAuth-OpenID Connect, NetScaler puede actuar como una parte de confianza de conexión (RP) de OAuth-OpenID o proveedor de identidad de conexión (IdP) de OAuth-OpenID. Cuando la autenticación se realiza correctamente, el nombre de usuario se informa en la ficha Usuarios en el informe Gateway Insight. Sin embargo, no puede identificar si la sesión se creó en el IdP o en el RP.

    Nota: La autenticación OAuth-OpenID Connect se admite en NetScaler ADM versión 13.1 compilación 4.xx y posteriores.

Habilitar Gateway Insight

Para habilitar Gateway Insight para su dispositivo NetScaler Gateway, primero debe agregar el dispositivo NetScaler Gateway a NetScaler ADM. A continuación, debe habilitar AppFlow para el servidor virtual que representa la aplicación VPN. Para obtener información sobre cómo agregar dispositivos a NetScaler ADM, consulte Agregar dispositivos.

> **Nota**
>
> Para ver los errores del análisis de punto final (EPA) en NetScaler ADM, debe habilitar la autenticación, la autorización y el registro de nombres de usuario de auditoría de AppFlow en el dispositivo NetScaler Gateway.

El siguiente procedimiento para habilitar la información de Gateway es aplicable si NetScaler ADM es **13.0 Build 36.27**:

1. Vaya a **Infraestructura > Instancias**y seleccione la instancia para la que quiere habilitar AppFlow.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. En la página **Configurar Insight**, en **Configurar Analytics**, seleccione **NetScaler Gateway**.
4. Seleccione el servidor virtual y, a continuación, haga clic en **Habilitar AppFlow**.
5. En la pantalla **Habilitar AppFlow**, en la lista **Seleccionar expresión**, haga clic en true.
6. Junto a **Modo de transporte**, active la casilla de verificación **Logstream**.

   > **Nota**
   >
   > Puede elegir **IPFIX** o **Logstream** como modo de transporte.
   >
   > Para obtener más información sobre **IPFIX** y **Logstream**, consulte **Descripción general de Logstream**.

7. Haga clic en **Aceptar**.

Para NetScaler ADM versión 13.0 Build 41.x o posterior

1. Vaya a **Infraestructura > Instancias**y seleccione la instancia.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione el servidor virtual y haga clic en **Habilitar análisis**.
4. En **Opciones avanzadas**:
   a) Seleccione **Logstream**
   b) Seleccione **NetScaler Gateway**
5. Haga clic en **Aceptar**.

Habilitar la autenticación, autorización y auditoría de AppFlow el registro de nombres de usuario en un dispositivo NetScaler 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**

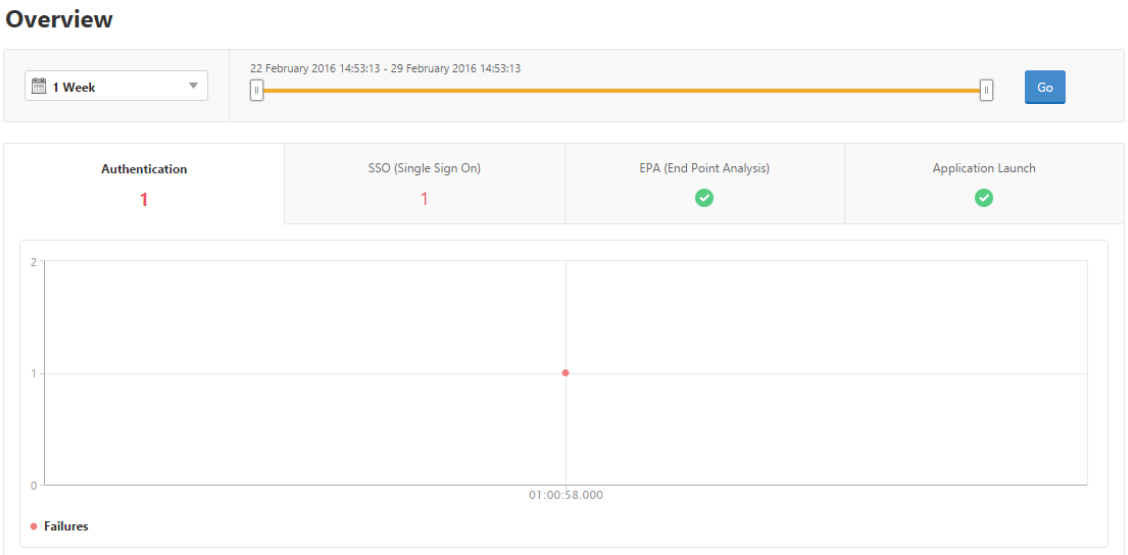
Ver los informes de Gateway Insight

En NetScaler ADM, puede ver los informes de todos los usuarios, aplicaciones y puertas de enlace asociados a los dispositivos NetScaler 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.

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso de nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de NetScaler ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos.

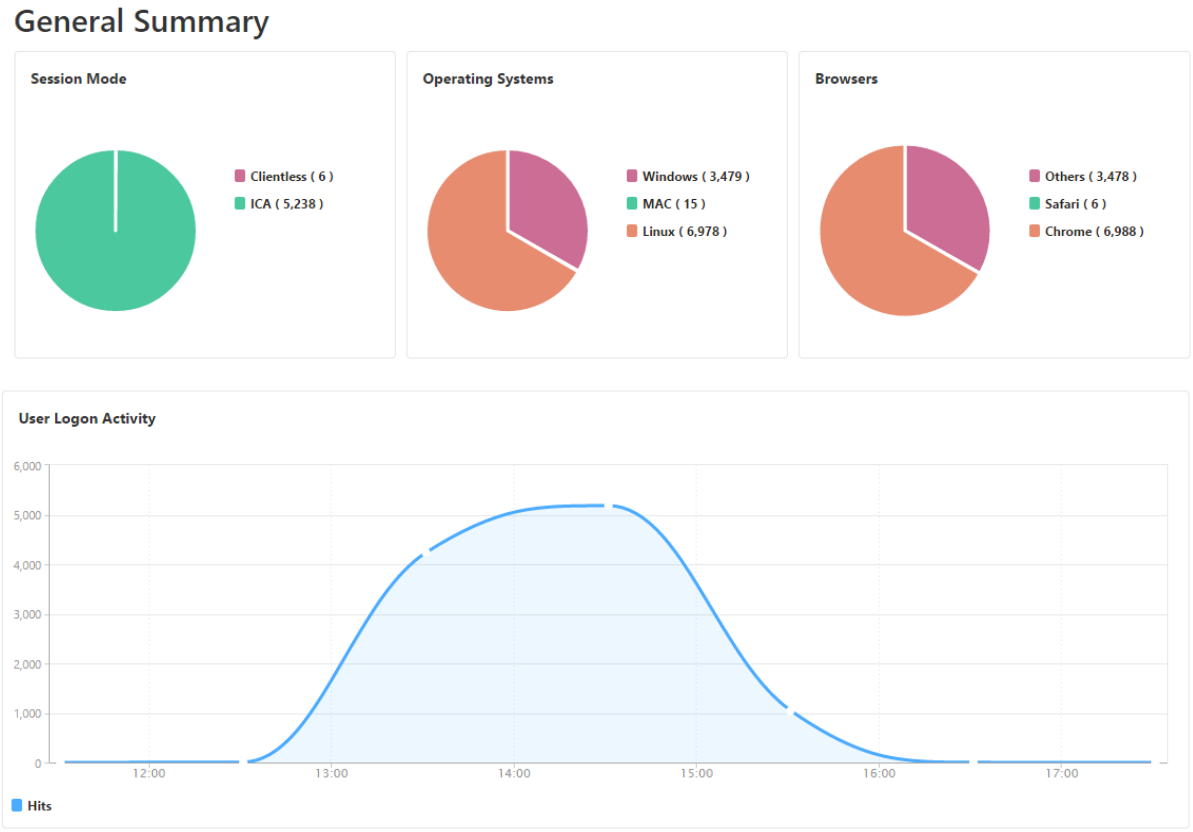
Para ver los errores de EPA, SSO, autenticación, autorización y lanzamiento de aplicaciones

1. En NetScaler ADM, vaya a **Gateway > 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 NetScaler ADM, vaya a **Gateway > Gateway Insight**, desplácese hacia abajo para ver los informes.



Visualización de informes de Gateway Insight para usuarios

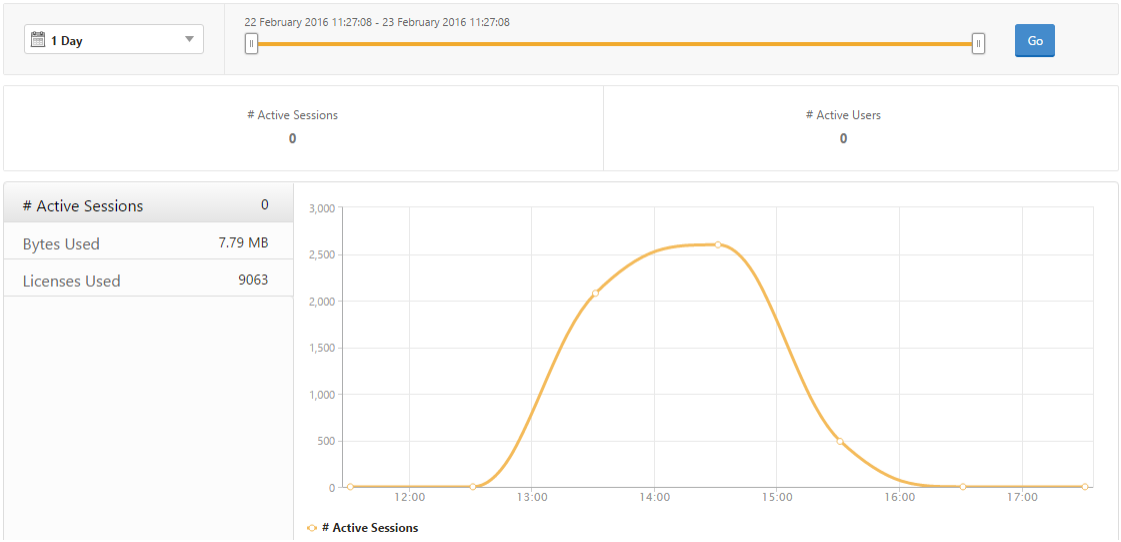
Puede ver los informes de:

- Todos los usuarios asociados con los dispositivos NetScaler Gateway.
- La EPA, autenticación, inicio de sesión único y errores de inicio de aplicación para un usuario.
- Los detalles de las sesiones activas y terminadas de un usuario.
- Los tipos de modos de sesión como Túnel completo, VPN sin cliente y Proxy ICA.

Para ver los detalles del usuario

1. En NetScaler ADM, vaya a **Gateway > 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. 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.

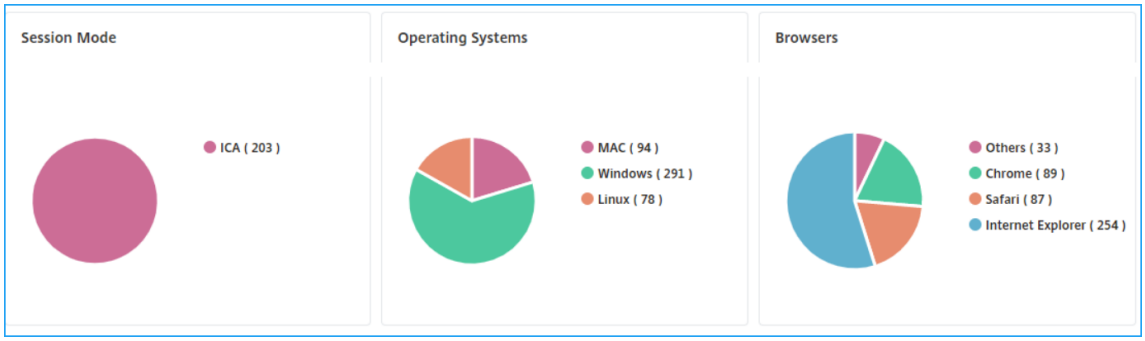


Desplácese hacia abajo para ver una lista de usuarios disponibles y usuarios activos.

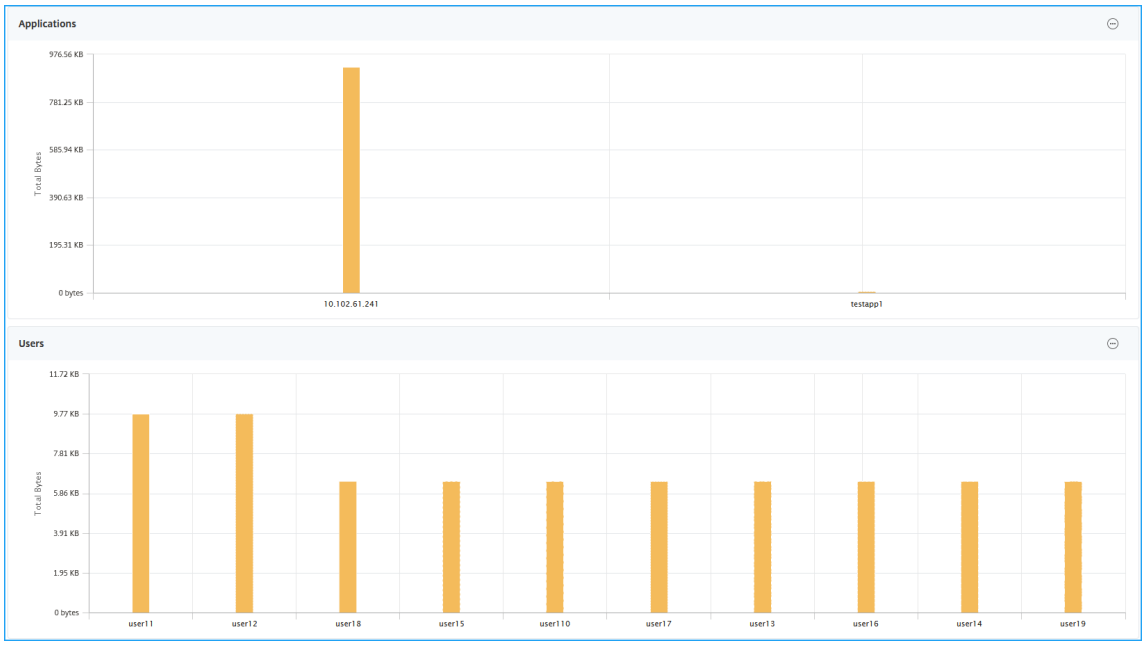
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

En la ficha **Usuarios** o **Usuarios activos**, haga clic en un usuario para ver los siguientes detalles de usuario:

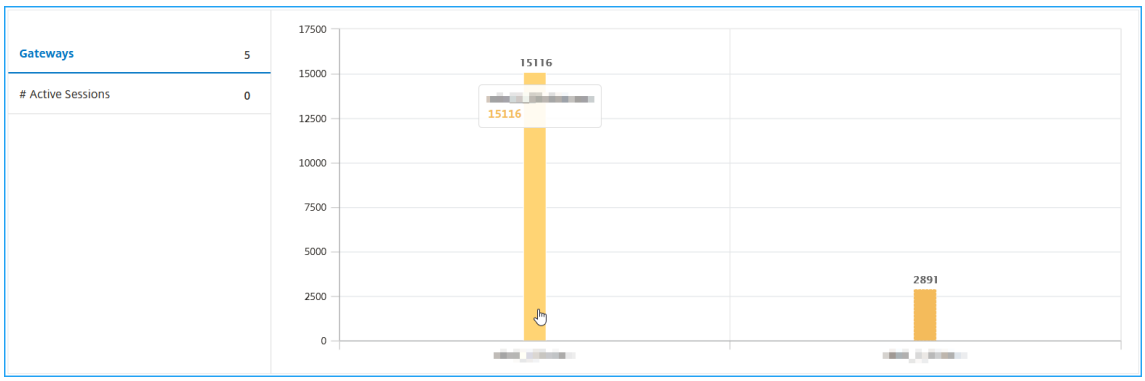
- **Detalles del usuario**: puede ver información sobre cada usuario asociado con los dispositivos de puerta de enlace de ADC. Vaya a **Gateway** > **Gateway Insight** > **Usuarios** y haga clic en un usuario para ver las perspectivas del usuario seleccionado, como el modo de sesión, el sistema operativo y los exploradores.



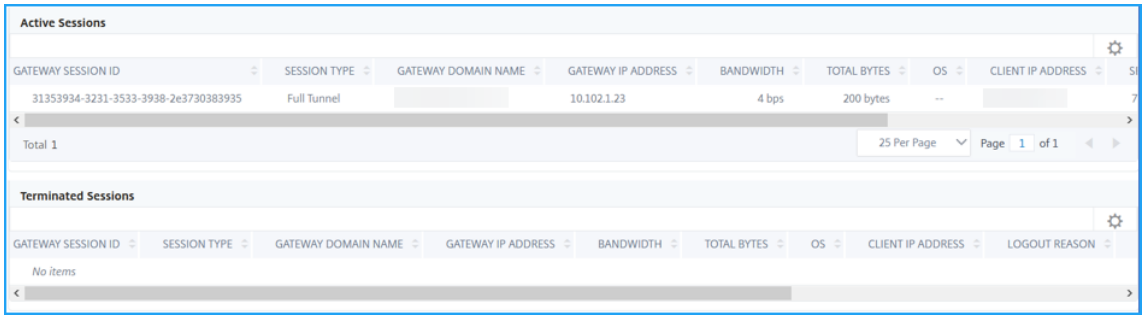
- **Usuarios y aplicaciones para la puerta de enlace seleccionada**: vaya a Puerta de **enlace > GatewayInsight**>**Puerta de enlace** y haga clic en el nombre de dominio de una puerta de enlace para ver las 10 aplicaciones principales y los 10 usuarios principales que están asociados a la puerta de enlace seleccionada.



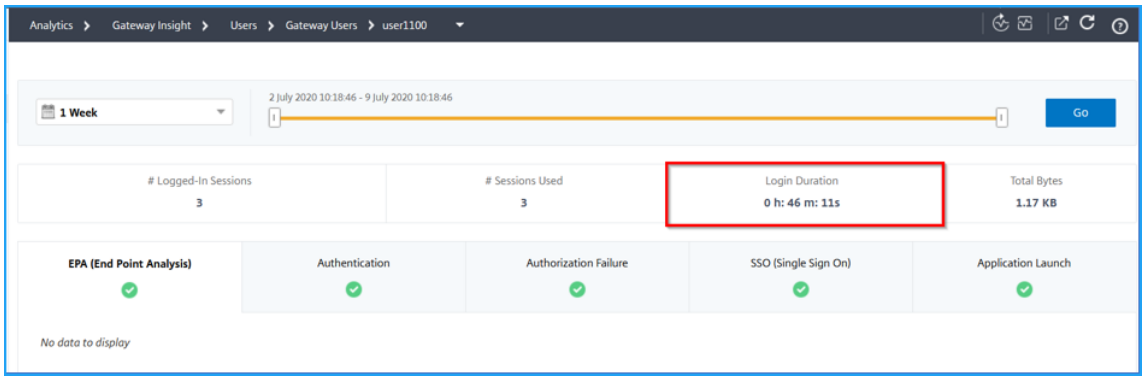
- **Ver más opción para aplicaciones y usuarios**: para más de 10 aplicaciones y usuarios, puede hacer clic en el icono más en Aplicaciones y Usuarios para ver todos los detalles de usuarios y aplicaciones asociados a la puerta de enlace seleccionada.
- **Ver detalles haciendo clic en el gráfico de barras**: al hacer clic en un gráfico de barras, puede ver los detalles relevantes. Por ejemplo, vaya a **Gateway > Gateway Insight > Gateway** y haga clic en el gráfico de barras de gateway para ver los detalles de la puerta de enlace



- El usuario **Sesiones Activas y SesionesTerminadas**.



- El nombre del dominio de puerta de enlace y la dirección IP de la puerta de **enlace en Sesiones**
- Duración del inicio de sesión del usuario.



- El motivo de la sesión de cierre de sesión del usuario. Los motivos de cierre de sesión pueden ser:
  - Tiempo de espera excedido
  - Se cerró la sesión debido a un error interno
  - Se ha cerrado la sesión debido al tiempo de espera de la sesión inactiva
  - El usuario ha cerrado sesión
  - El administrador ha detenido la sesión

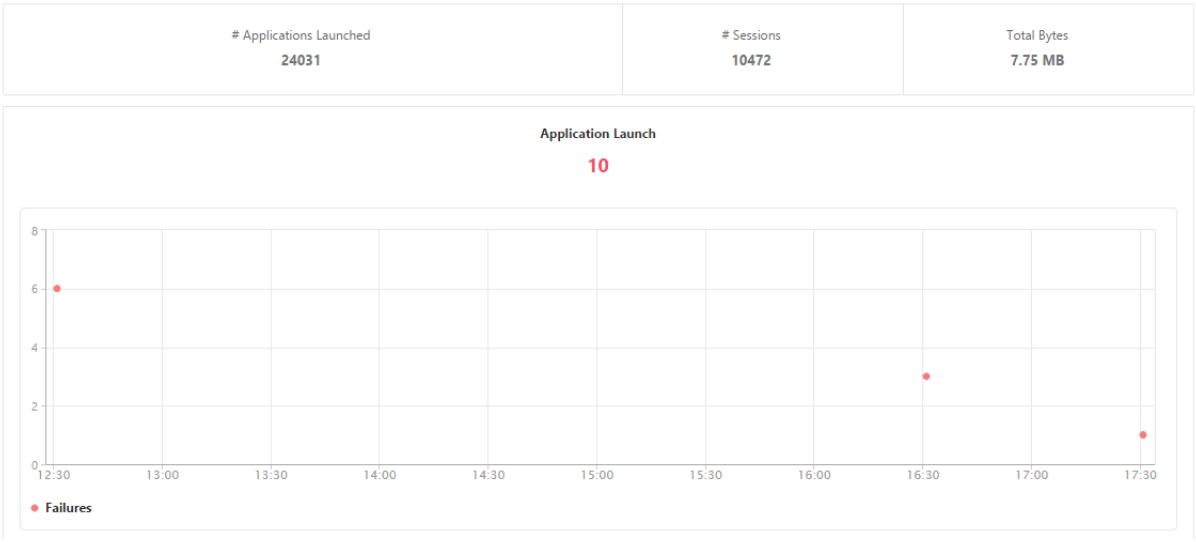
Visualización de informes de Gateway Insight para aplicaciones

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 **Gateway > 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.

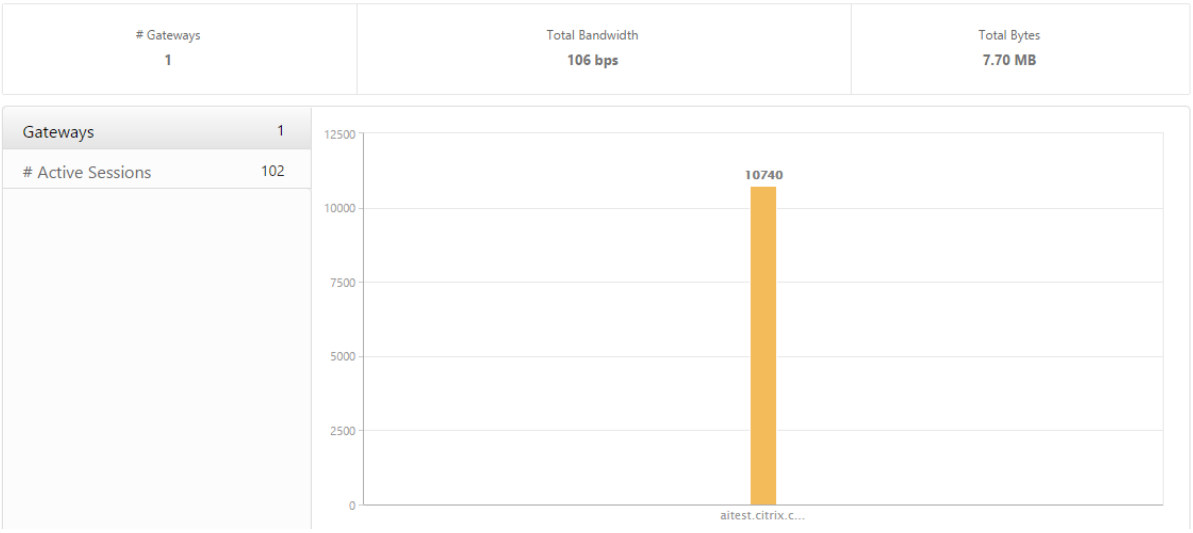
Visualización de informes de Gateway Insight para puertas de enlace

Puede ver la cantidad de puertas de enlace, la cantidad de sesiones activas, el total de bytes y el ancho de banda que utilizan todas las puertas de enlace asociadas a un dispositivo NetScaler 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.

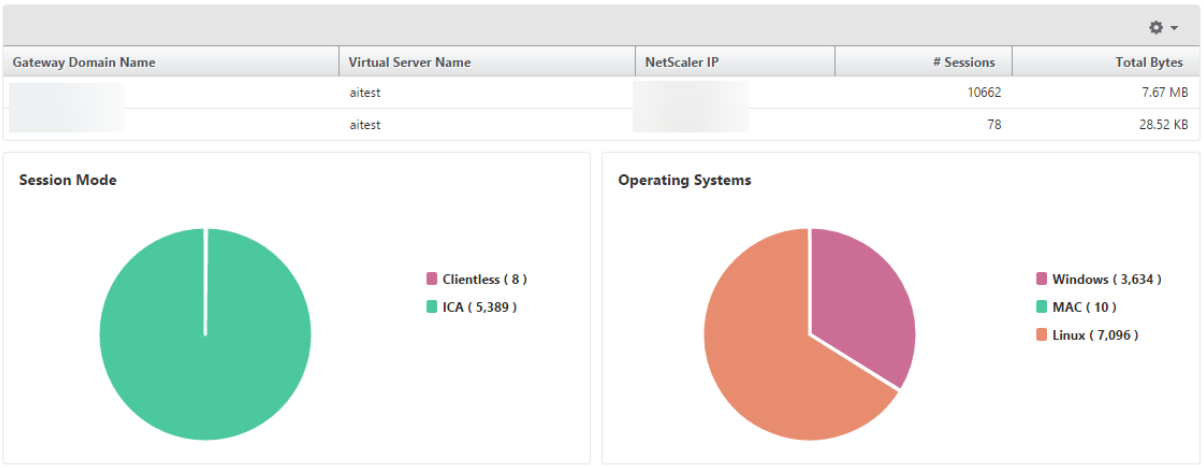
Para ver los detalles de la Gateway

1. En **NetScaler ADM**, vaya a **Gateway > Gateway Insight > Gateways** .
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 NetScaler 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 NetScaler 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 **Configuración > 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 NetScaler Gateway.

Un usuario no puede iniciar sesión en el dispositivo NetScaler Gateway ni en los servidores web internos

Usted es un administrador de NetScaler Gateway que supervisa los dispositivos NetScaler Gateway a través de NetScaler ADM y quiere comprobar por qué un usuario no puede iniciar sesión o en qué fase del proceso de inicio de sesión se ha producido el error.

NetScaler 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 NetScaler ADM, puede buscar un usuario en particular y, a continuación, ver todos los detalles de ese usuario.

Para buscar un usuario:

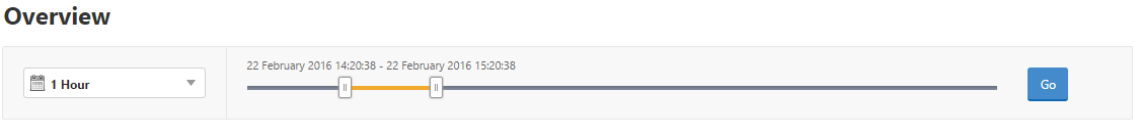
En NetScaler ADM, vaya a **Gateway > Gateway Insight** y, en el cuadro de texto **Buscar usuarios**, especifique el usuario en el que quiere buscar.

Fallos de autenticación

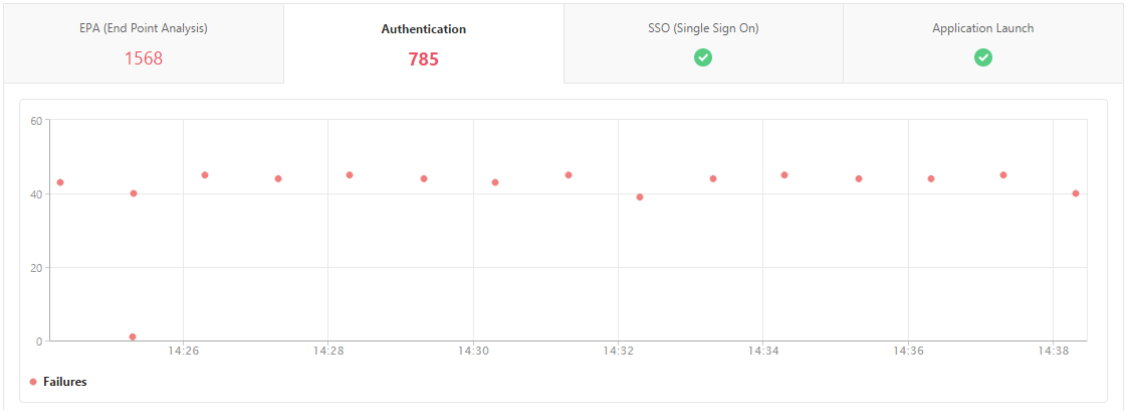
Puede ver errores de autenticación, como credenciales incorrectas o ninguna respuesta del servidor de autenticación. También puede ver el factor por el que falló la autenticación.

Para ver los detalles del error de autenticación:

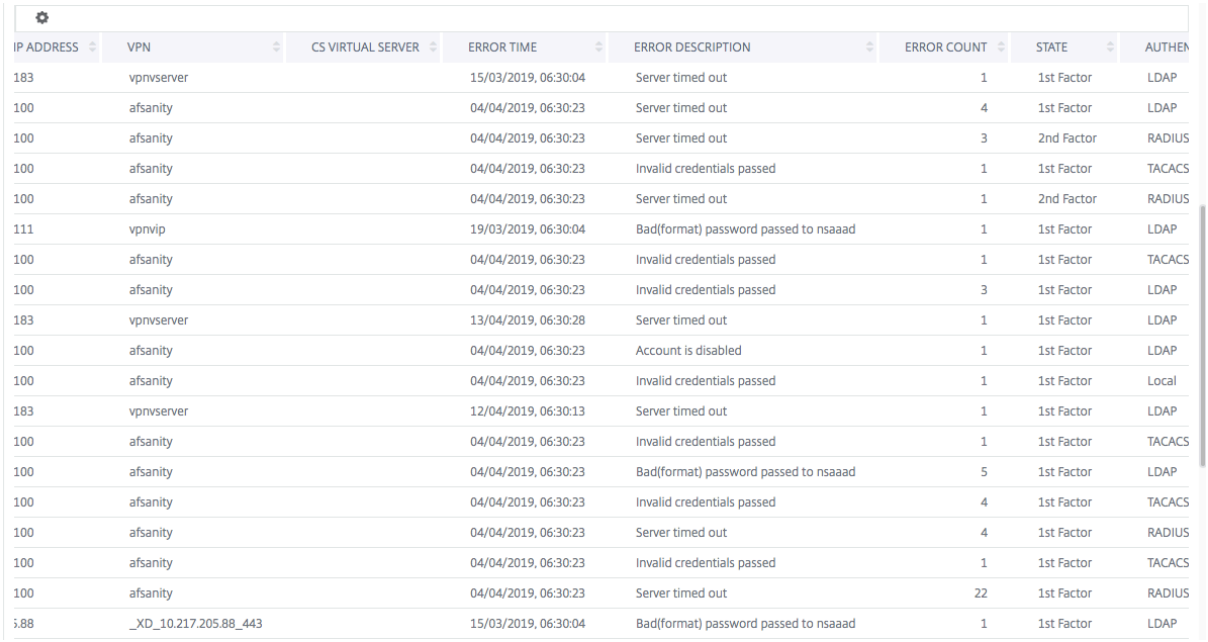
1. En NetScaler ADM, vaya a **Gateway > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de autenticación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **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 el enésimo factor en el que se produjo el error.



IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

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 el icono de configuración.

> **Importante:**
>
> Si la autenticación de OAuth-OpenID Connect falla, el nombre de usuario se muestra como **NA** en el informe de Gateway Insight para algunos de los errores, por ejemplo, "Error de verificación de token". En este error, los nombres de usuario no están disponibles para el error de autenticación debido a un "error de verificación de token"en la parte de confianza de conexión de OAuth-OpenID.

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth req
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-	[redacted]	[redacted]	[redacted]	gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token verification failed
-NA-	[redacted]	[redacted]	[redacted]	vpnvserver		Relying party: Token decryption failure

Errores de EPA

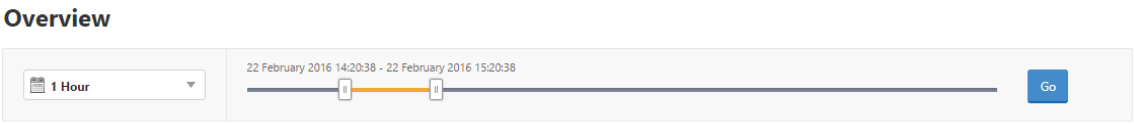
Puede ver los errores de EPA en la etapa previa o posterior a la autenticación.

> **Importante:**
>
> NetScaler Gateway notifica los errores de la EPA a NetScaler ADM para las expresiones clásicas y avanzadas. Para las expresiones avanzadas, los nombres de las directivas no se muestran en

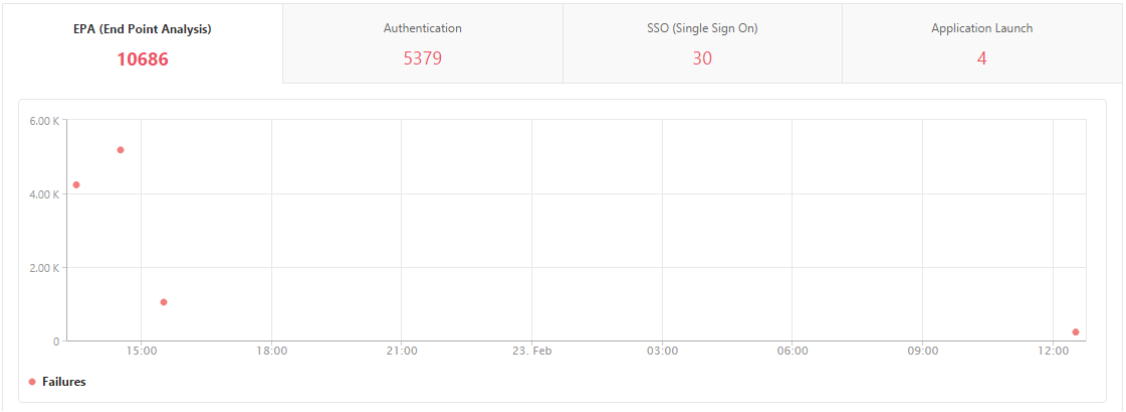
> el panel de control de Gateway Insight. Los errores se notifican si la EPA está configurada como uno de los factores del flujo de autenticación de nFactor.

Para ver los detalles de fallo de EPA:

1. En NetScaler ADM, vaya a **Gateway > 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 fallo de la EPA. Por ejemplo, el mensaje de error «Fallos en la comprobación previa a la autenticación de la EPA» aparece cuando se produce un error en una comprobación de la EPA debido a errores de nFactor EPA.

La columna **Nombre** de la directiva muestra la directiva que provocó el 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. El identificador del caso se muestra en las entradas que no tienen un nombre de usuario asignado si se utiliza la EPA como factor en el flujo de autenticación de nFactor.

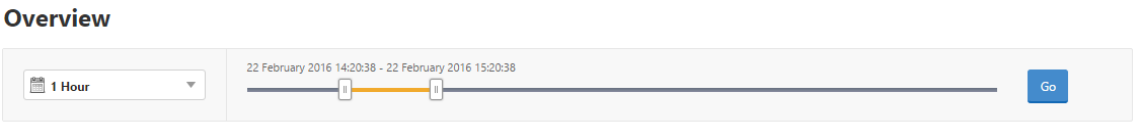
> **Nota**
>
> NetScaler Gateway no informa de los errores de la EPA cuando la expresión "clientSecurity"se configura como una regla de directiva de sesión de VPN.

Errores de SSO

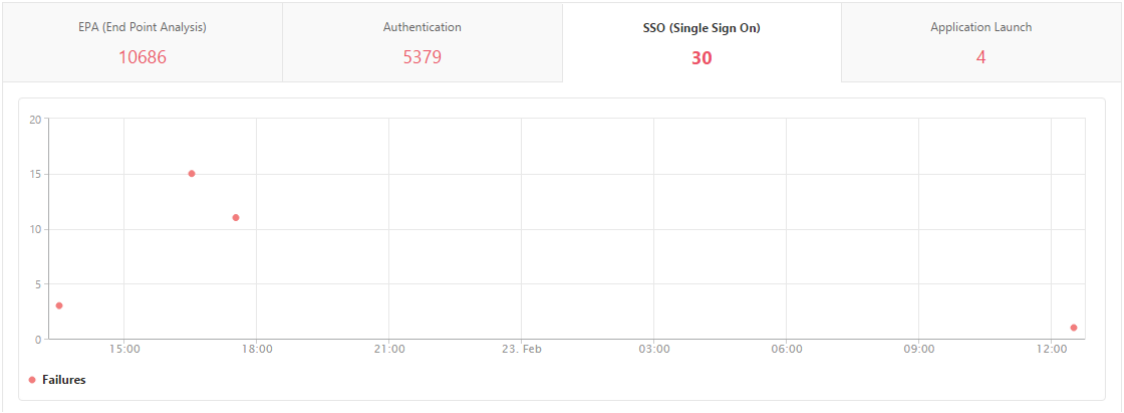
Puede ver todos los errores de SSO en cualquier etapa de los usuarios que acceden a cualquier aplicación a través del dispositivo NetScaler Gateway.

Para ver los detalles del error de inicio de SSO:

1. En NetScaler ADM, vaya a **Gateway > 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

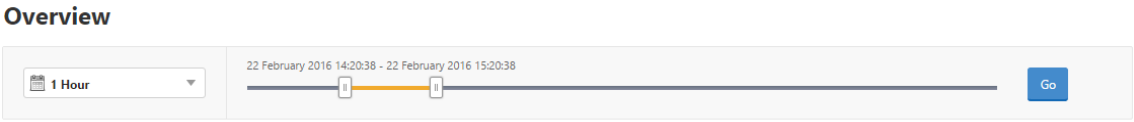
Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de SSO y otros detalles de ese usuario. Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

Después de iniciar sesión correctamente en NetScaler Gateway, un usuario no puede iniciar ninguna aplicación virtual

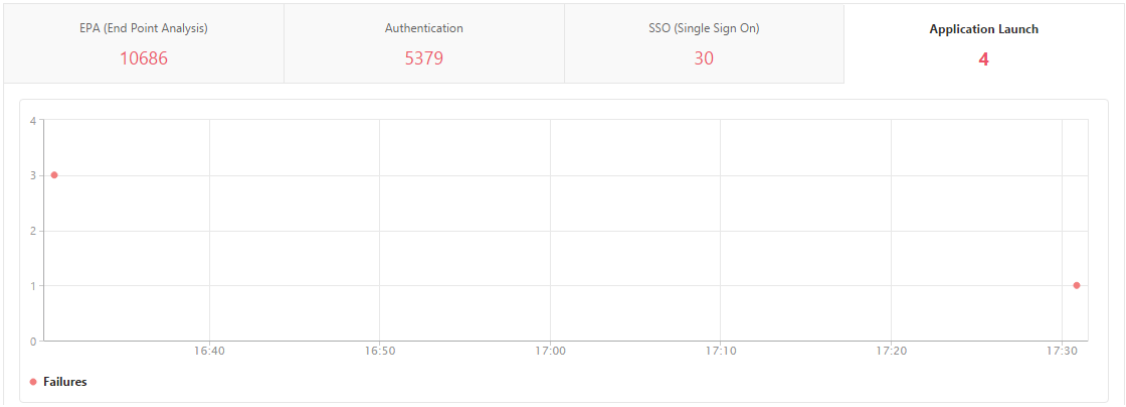
Si se produce un error en el inicio de la aplicación, puede obtener visibilidad de los motivos, como Secure Tíquet Authority (STA) o Citrix Virtual App Server, o un tíquet STA no válido. Puede ver la hora en que se produjo el error, los detalles del error y el recurso para el que falló la validación STA.

Para ver los detalles del error de inicio de la aplicación:

1. En NetScaler ADM, vaya a **Gateway > 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

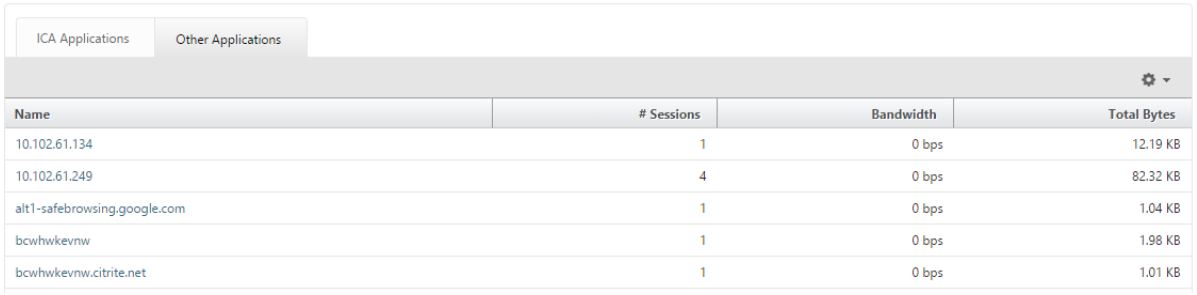
Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de inicio de la aplicación y otros detalles de ese usuario. Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

Después de iniciar correctamente una nueva aplicación, un usuario quiere ver el total de bytes y ancho de banda consumidos por esa aplicación

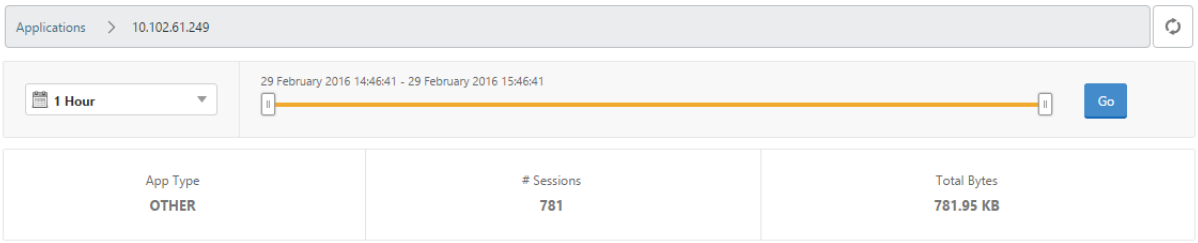
Después de haber iniciado correctamente una nueva aplicación, en NetScaler ADM, puede ver el total de bytes y ancho de banda consumidos por esa aplicación.

Para ver el total de bytes y ancho de banda consumidos por una aplicación:

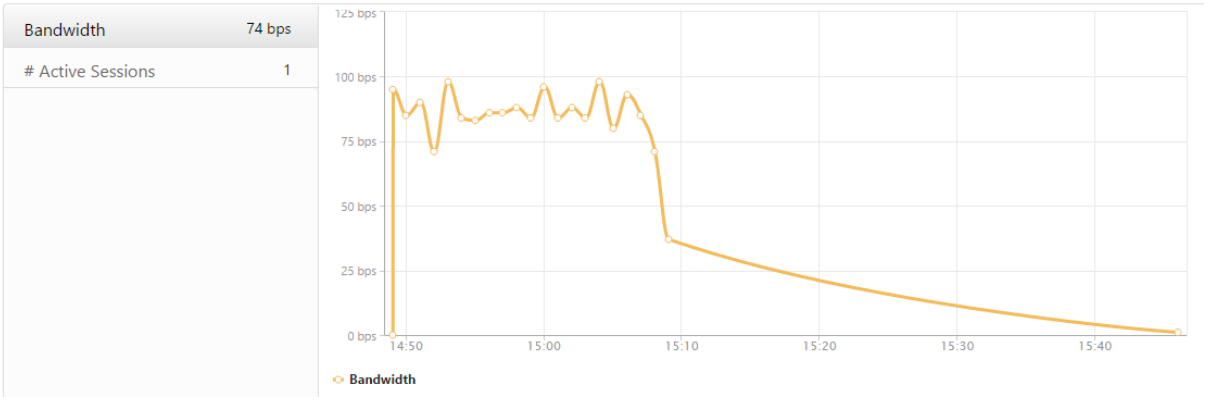
En NetScaler ADM, vaya a **Gateway > Gateway Insight > Aplicaciones**, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, haga clic en la aplicación de la que quiere ver los detalles.



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.

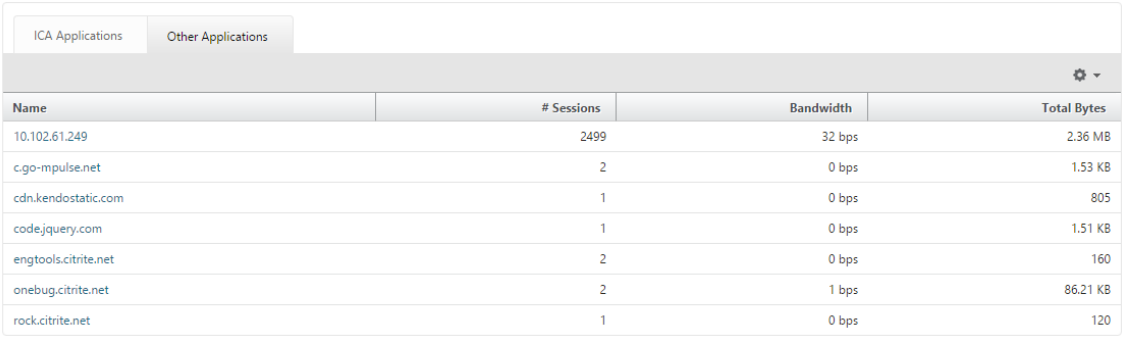


Un usuario ha iniciado sesión correctamente en NetScaler Gateway, pero no puede acceder a determinados recursos de red de la red interna

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 NetScaler ADM , **vaya a Gateway > Gateway Insight > Applications** .
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

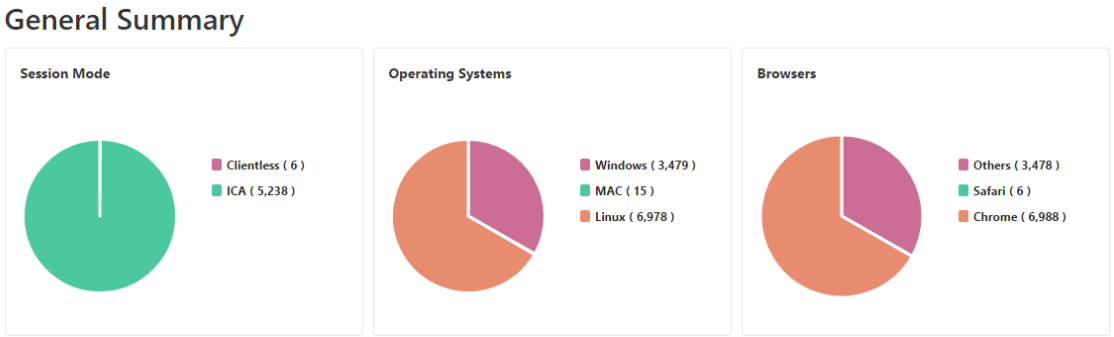
3. Desplácese hacia abajo y, en la tabla **Usuarios**, se muestran todos los usuarios que tienen acceso a esa aplicación.

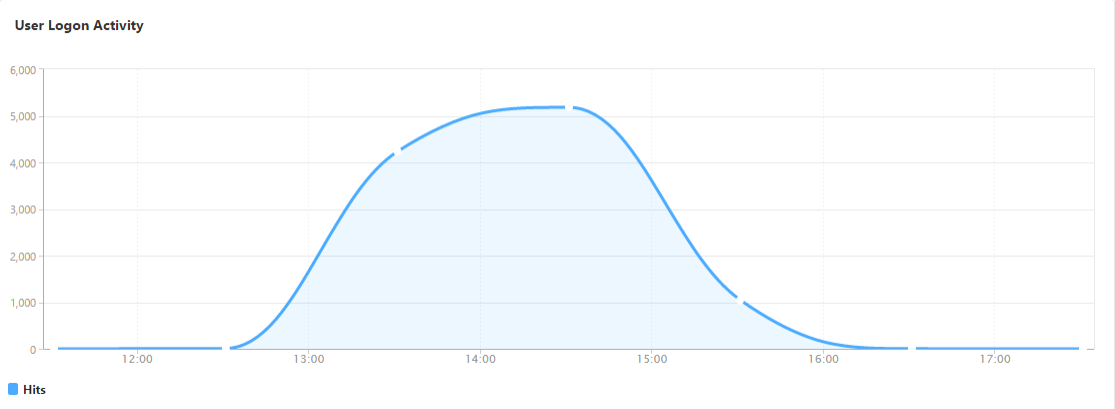
Es posible que diferentes usuarios usen distintas implementaciones de NetScaler Gateway o que inicien sesión en NetScaler Gateway a través de diferentes modos de acceso. El administrador debe poder ver detalles sobre los tipos de implementación y los modos de acceso

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 NetScaler 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 el número de usuarios que han iniciado sesión:

1. En NetScaler ADM, vaya a **Gateway > 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 y NetScaler ADM.
- Generación de registros en NetScaler.
- Validaciones en NetScaler ADM.

Lista de comprobación de configuración de Gateway Insight

- Asegúrese de que la función AppFlow está habilitada en el dispositivo NetScaler. Para obtener más información, consulte Habilitar AppFlow.
- Compruebe la configuración de Gateway Insight en la configuración en ejecución de NetScaler.

  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:

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  2  <!--NeedCopy-->
  ```

  El tipo de enlace OTHERTCP_REQUEST también es necesario para Gateway Insight.

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type
       OTHERTCP_REQUEST
  ```



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

- 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
- Para el doble salto, Gateway Insight debe configurarse en ambos saltos.
- Compruebe el parámetro `appflowlog` en el servidor virtual NetScaler Gateway/VPN. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.

Lista de comprobación de conectividad entre NetScaler y NetScaler ADM

- Compruebe el estado del recopilador AppFlow en NetScaler. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler 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 AppFlow.

  También puede navegar a **Configuración > AppFlow > Directivas** en la GUI para comprobar las visitas a la directiva de AppFlow.
- Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

Generación de registros en la lista de comprobación de NetScaler

- Ejecute el comando `nsconmsg -d stats -g ai_tot` y compruebe si hay incrementos de estadísticas en NetScaler.
- Capture `nstrace logs` y compruebe si hay paquetes CFLOW para confirmar que NetScaler exporta registros de AppFlow.

> **Nota:**
>
> Los `nstrace logs` son necesarios solo para IPFIX. Para Logstream, los registros de nstrace no confirman si el dispositivo ADC exportó los registros AppFlow.

Validación de registros en NetScaler ADM

- Ejecute el `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` comando para comprobar los registros para confirmar que NetScaler ADM está recibiendo registros de AppFlow.
- Asegúrese de que la instancia de NetScaler se ha agregado a NetScaler ADM.
- Asegúrese de que el servidor virtual NetScaler Gateway/VPN tiene licencia en NetScaler ADM.

Validación de registros Logstream en NetScaler ADM

La validación de los datos Logstream recibidos por NetScaler ADM se puede realizar mediante los siguientes métodos:

- **Habilitar el registro de datos en NetScaler ADM**

  Una vez habilitado, los registros se pueden ver en el archivo /var/mps/log/mps_afdecoder.log

- **Habilitar el registro de bibliotecas ULFD**

  Ejecute el comando `/mps/decoder_enable_debug`

  Los registros se capturan en `/var/ulflog/libulfd.log`

  Puede inhabilitar el registro mediante el comando `/mps/decoder_disable_debug`

Contadores de Gateway Insight

Los siguientes contadores de Gateway Insight están disponibles.

- 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
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

Registros de AppFlow en el registro de NetScaler

A partir de la versión 13.0 compilación 71.x, puede comprobar los registros de NetScaler para confirmar si se exportan los registros de AppFlow. El nivel de registro predeterminado de `syslogparams` captura todos los registros de errores e información. En caso de que no encuentre una pista sobre

los errores, habilite todos los niveles de registro, incluido DEBUG in, `syslogparams` para capturar incluso los registros de DEPURACIÓN.

Registros de muestra

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
   GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
   =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
   Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
   vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
   AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
   CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
   =16777219 Deviceid=0 email="
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
   : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
   zero"
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
   : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
   =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
   CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
   =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
   SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
   BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
   GwInsight: Sent session update record Func=
   ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
   Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
   =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
```



```
      SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
      BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
      GwInsight: Sent session update record Func=
      ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
      Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
      =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
      SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
      BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

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 y NetScaler ADM.
- Paquete de soporte técnico para NetScaler y NetScaler ADM.
- `nstrace` durante el problema.

Problemas conocidos

Consulte las notas de la versión de ADC para conocer los problemas conocidos en Gateway Insight.

HDX Insight

January 30, 2024

HDX Insight proporciona una visibilidad integral del tráfico de HDX a Citrix Virtual Apps and Desktop que pasa por NetScaler. También permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento. La disponibilidad de datos de visibilidad históricos y en tiempo real permite a NetScaler Application Delivery Management (ADM) soportar una amplia variedad de casos de uso.

Para que aparezca cualquier dato, debe habilitar AppFlow en sus servidores virtuales de NetScaler 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, active la siguiente configuración de directivas

- 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 HDX, activa o terminada, que el usuario haya realizado dentro del período de tiempo seleccionado. Otra información incluye varias estadísticas de latencia y ancho de banda consumido durante la sesión. También puede obtener información sobre el ancho de banda de los canales virtuales individuales, como el audio, la asignación de impresoras y la asignación de unidades del cliente.

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso a nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de NetScaler ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos.

También puede ir a **Puerta de enlace > HDX Insight > Aplicaciones** y hacer clic en **Duración del lanzamiento**para ver el tiempo que tardó la aplicación en iniciarse. También puede ver el agente de usuario de todos los usuarios conectados en**Gateway > HDX Insight > Usuarios.**

> **Nota**HDX Insight admite Particiones de administración configuradas en instancias de NetScaler 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 10 ZiG

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.

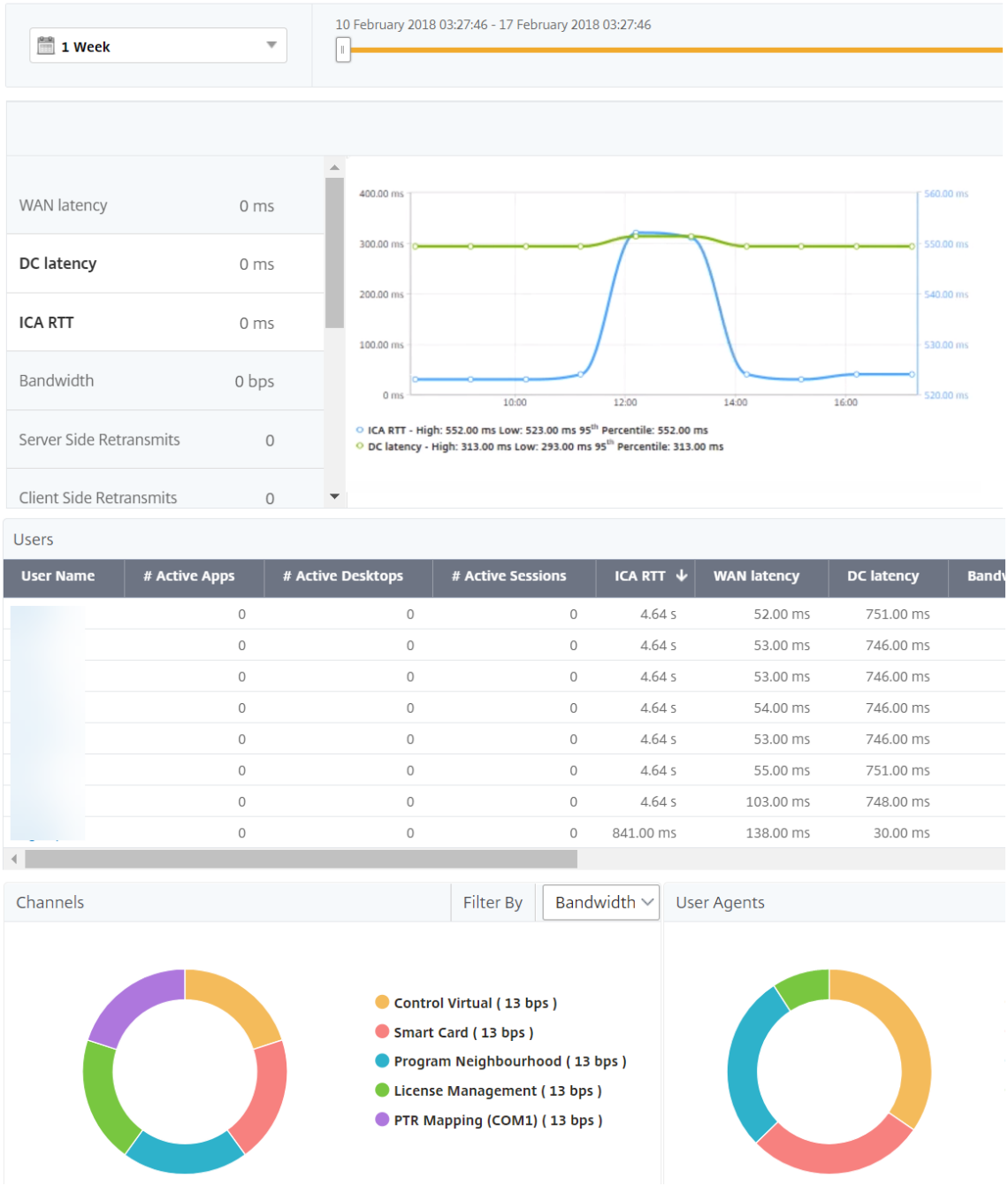
Los retrasos pueden deberse a la latencia en la red del servidor, retrasos en el tráfico ICA causados por la red del servidor o latencia en la red del cliente.

Para identificar la causa principal del problema, analice las siguientes métricas:

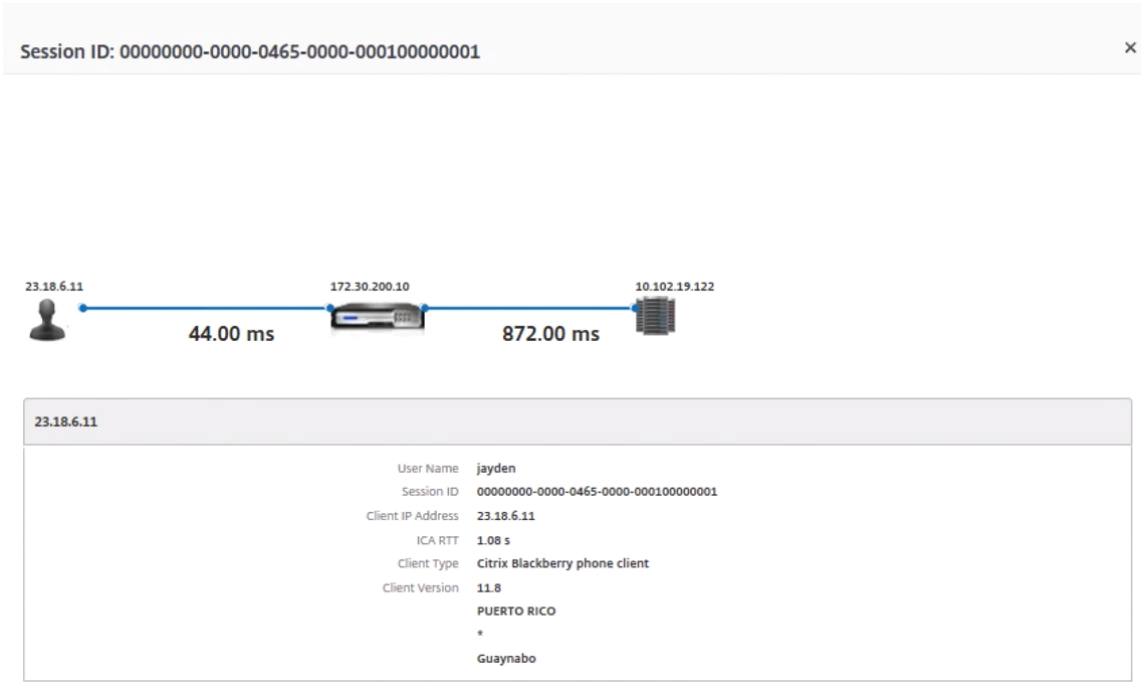
- Latencia de WAN
- Latencia de DC
- Demora de host

Para ver las métricas del cliente:

1. Vaya a **Puerta de enlace > HDX Insight > Usuarios**.
2. Desplácese hacia abajo y seleccione el nombre de usuario y seleccione 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 del 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 App o Desktop

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.

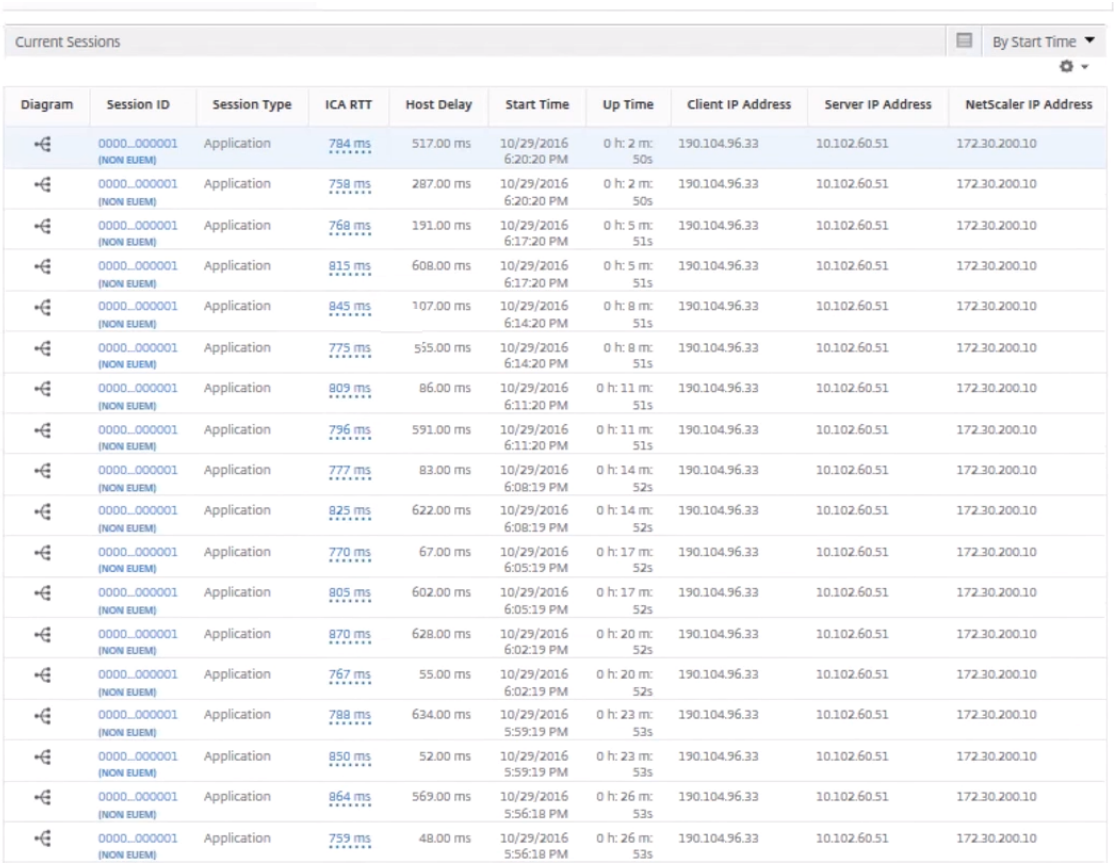
Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia de WAN
- Latencia de DC
- Demora del host

Para ver las métricas de usuario:

1. Vaya a **Gateway > HDX Insight > Usuarios .**
2. Desplácese hacia abajo y haga clic en el nombre de usuario.
3. En la representación gráfica, anote los valores de latencia WAN, latencia de DC y RTT de 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 más métricas de usuario, como la fluctuación de WAN y las retransmisiones del lado del servidor si utiliza NetScaler ADM ejecutando el software 11.1 compilación 51.21 o posterior. Para ver estas métricas, vaya a **Gateway > 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 ADM de NetScaler muestra el uso de las 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 NetScaler ADM para que muestre los mapas geográficos de una ubicación geográfica o LAN determinada especificando el rango de IP privado (dirección IP inicial 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 **Gateway > HDX Insight**y, en la sección **Mundo** del mapa, haga clic en el país o la región para 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:

Vaya a **Configuración > Configuración de Analytics > Bloques de IP** para configurar geomapas para una ubicación en particular.

Caso de uso

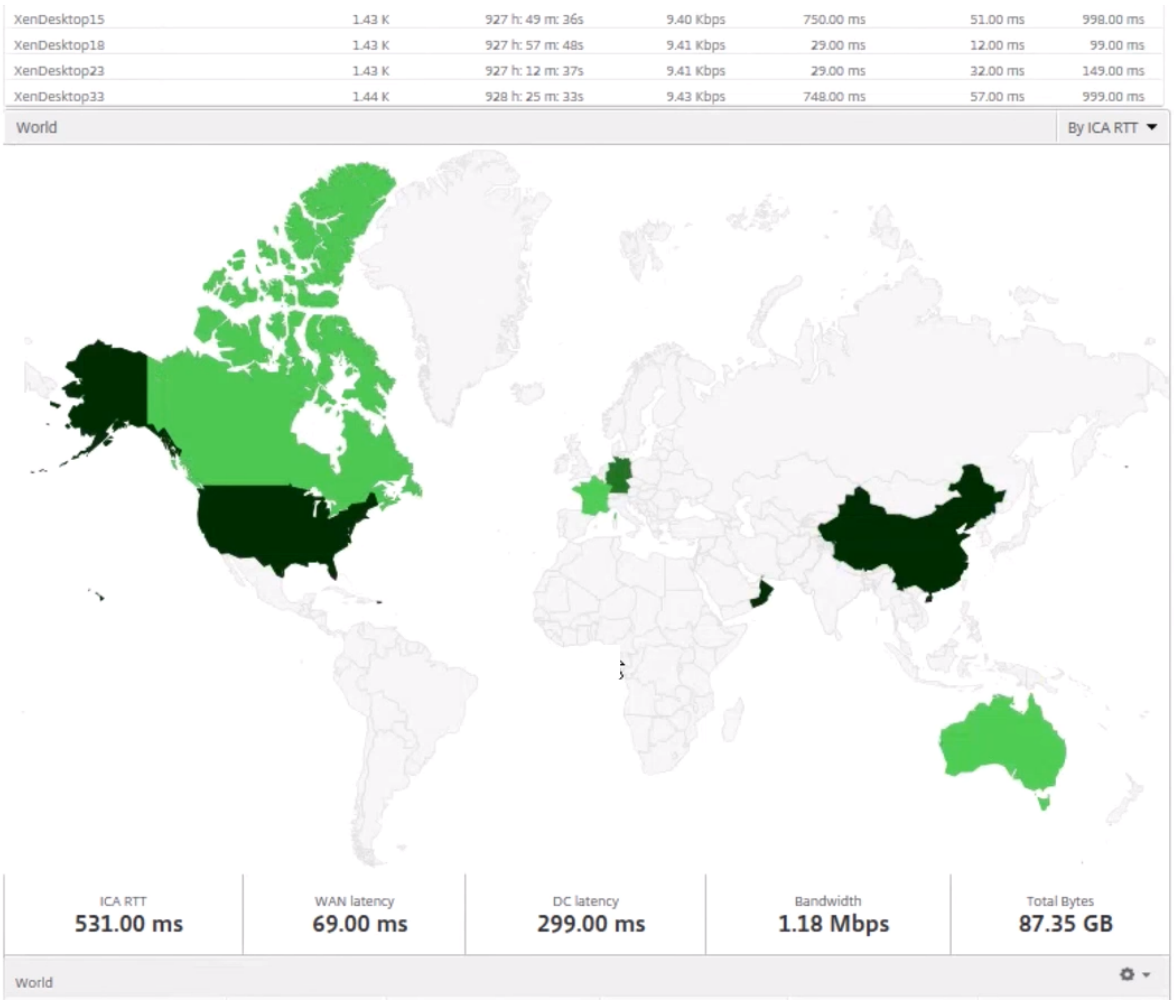
Considere un caso en el que la organización ABC tiene 2 sucursales, una en Santa Clara y la otra en India.

Los usuarios de Santa Clara utilizan el dispositivo NetScaler Gateway en SClara.x.com para acceder al tráfico VPN. Los usuarios indios utilizan el dispositivo NetScaler 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 NetScaler 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 NetScaler que analice el tráfico puede utilizar la funcionalidad de mapa geográfico 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 alto, porque la oficina de Santa Clara solo tiene un dispositivo NetScaler Gateway a través del cual los usuarios pueden acceder al tráfico de VPN. Por lo tanto, es posible que el administrador decida instalar otro NetScaler Gateway, de modo que los usuarios dispongan de dos dispositivos NetScaler Gateway locales a través de los cuales acceder a la VPN.



Limitaciones

Si las instancias NetScaler tienen licencia Advanced, los umbrales establecidos en NetScaler 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

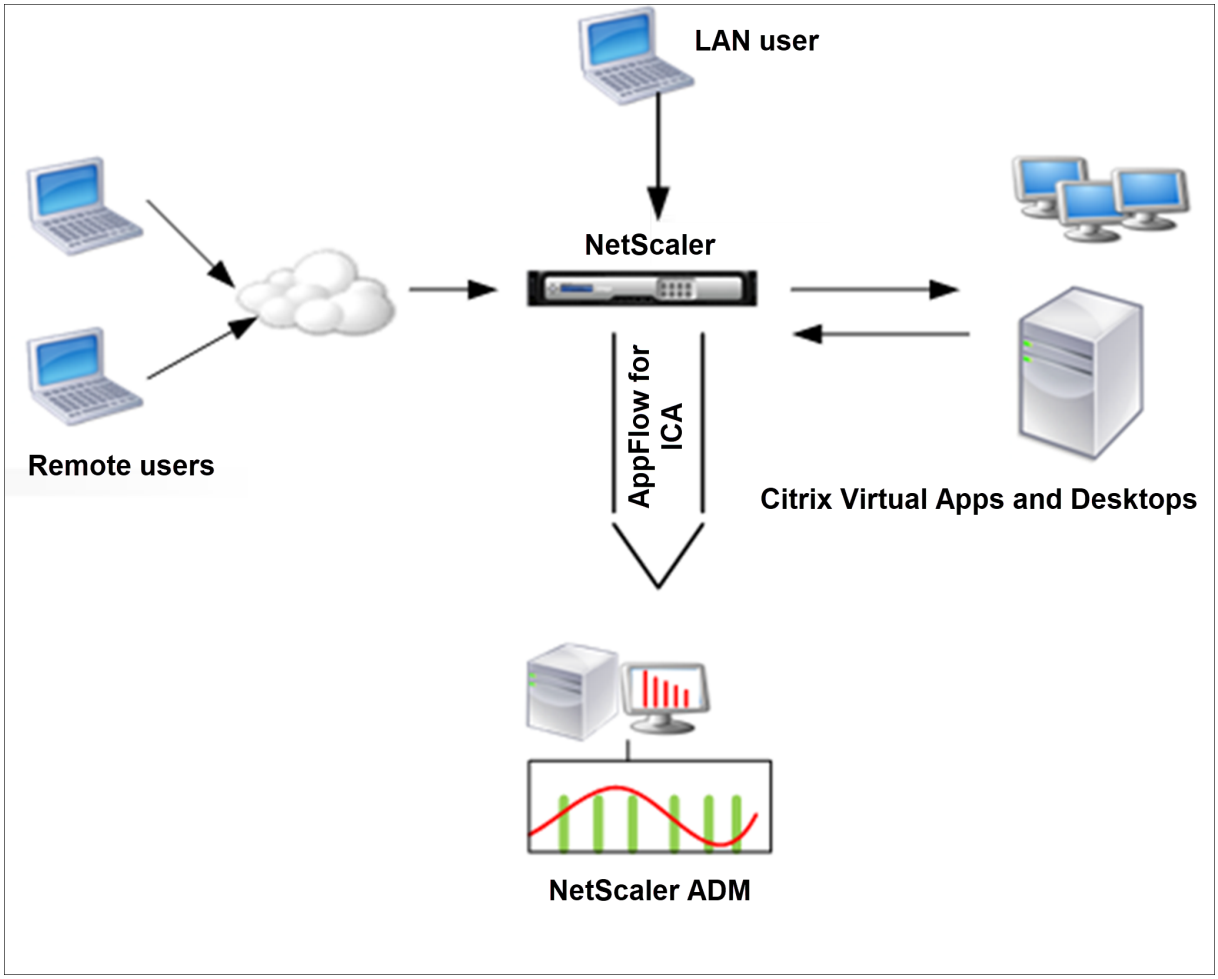
HDX Insight permite al departamento de TI ofrecer una experiencia de usuario excepcional al proporcionar una visibilidad integral sin precedentes del tráfico ICA que pasa por las instancias de NetScaler y forma parte de NetScaler Application Delivery Management (ADM) Analytics. HDX Insight ofrece capacidades de análisis de fallos y de inteligencia empresarial atractivas y potentes 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 NetScaler difiere según la postura del dispositivo en la topología de implementación.

Habilitar la recopilación de datos para supervisar los NetScalers implementados en modo de usuario de LAN

Los usuarios externos que accedan a las aplicaciones de escritorio y aplicaciones virtuales de Citrix deben autenticarse en NetScaler Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a NetScaler 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 App y Desktop, puede implementar el dispositivo NetScaler en modo de usuario LAN configurando un servidor virtual de redirección de caché, que actúa como proxy SOCKS en el dispositivo NetScaler Gateway.



> **Nota** NetScaler ADM y el dispositivo NetScaler Gateway residen en la misma subred.

Para supervisar los dispositivos NetScaler implementados en este modo, primero agregue el dispositivo NetScaler al inventario de NetScaler Insight, habilite AppFlow y, a continuación, consulte los informes en el panel.

Después de agregar el dispositivo NetScaler al inventario de NetScaler ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - En una instancia de ADC, puede ir a **Configuración > AppFlow > Recopiladores**para comprobar si el recopilador (es decir, NetScaler ADM) está activo o no. La instancia NetScaler envía registros AppFlow a NetScaler ADM mediante NSIP. Sin embargo, la instancia usa su SNIP para verificar la conectividad con NetScaler ADM. Por lo tanto, asegúrese de que el SNIP esté configurado en la instancia.
> - No puede habilitar la recopilación de datos en un NetScaler implementado en modo de usuario de LAN mediante la utilidad de configuración de NetScaler 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.

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 NetScaler Gateway, agregue una acción que se aplicará mediante una directiva que coincida con el tráfico de la VPN.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or 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 NetScaler ADM como un recopilador AppFlow en el dispositivo NetScaler.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

‘‘‘

add appflow collector MyInsight -IPAddress 192.168.1.101

‘‘‘

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string>
```

Ejemplo :

```
add appflow action act -collectors MyInsight
```

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
```

Ejemplo :

```
add appflow policy pol true act
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
```

Ejemplo :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Nota**
>
> El valor de tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicar 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
```

8. Guarde la configuración. Tipo: `save ns config`

Habilitar la recopilación de datos para los dispositivos NetScaler Gateway implementados en modo de salto único

Cuando implementa NetScaler 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 NetScaler a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo NetScaler Gateway al inventario de NetScaler Application Delivery Management (ADM) y habilitar AppFlow en ADM.

Para habilitar la función AppFlow desde NetScaler ADM:

1. En un explorador web, escriba la dirección IP del NetScaler 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 la lista **Seleccionar acción**, seleccione **Configurar análisis**.
5. Seleccione los servidores virtuales VPN y haga clic en **Habilitar análisis**.
6. Seleccione **HDX Insight** y, a continuación, **ICA**.
7. Haga clic en **Aceptar**.

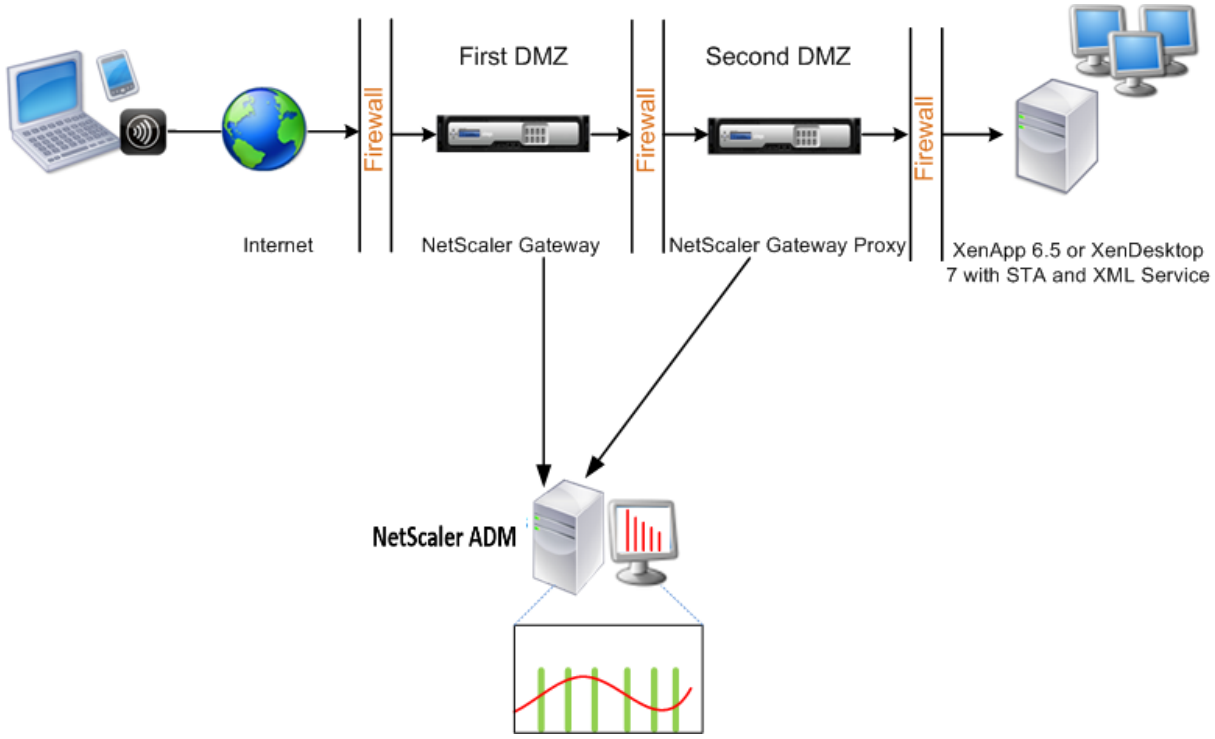
> **Nota**
>
> cuando habilita AppFlow en modo de salto único, los siguientes comandos se ejecutan en segundo plano. Estos comandos se especifican explícitamente aquí para solucionar problemas.

```
1  -  add appflow collector <name> -IPAddress <ip_addr>
2
3  -  add appflow action <name> -collectors <string>
4
5  -  set appflow param -flowRecordInterval <secs>
6
7  -  disable ns feature AppFlow
8
9  -  enable ns feature AppFlow
10
11 -  add appflow policy <name> <rule> <expression>
12
13 -  set appflow policy <name> -rule <expression>
14
15 -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
      positive_integer>
16
17 -  set vpn vserver <name> -appflowLog ENABLED
18
19 -  save ns config
```

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el NetScaler 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 NetScaler ADM.

Habilitar la recopilación de datos para los dispositivos NetScaler Gateway implementados en modo de doble salto

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 NetScaler 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 NetScaler ADM para que los dispositivos NetScaler Gateway reportar estas estadísticas vitales.



NetScaler Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Este NetScaler Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

NetScaler Gateway en la segunda DMZ sirve como dispositivo proxy de NetScaler Gateway. Este NetScaler Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores.

El NetScaler ADM se puede implementar en la subred que pertenece al dispositivo NetScaler Gateway en la primera DMZ o en la subred que pertenece a la segunda DMZ del dispositivo NetScaler Gateway. En la imagen de arriba, NetScaler ADM y NetScaler Gateway de la primera DMZ se implementan en la misma subred.

En modo de salto doble, NetScaler ADM recopila los registros TCP de un dispositivo y los registros ICA

del otro dispositivo. Después de agregar los dispositivos NetScaler Gateway al inventario de NetScaler ADM y habilitar la recopilación de datos, cada uno de los dispositivos exporta los informes realizando un seguimiento del recuento de saltos y del ID de la cadena de conexiones.

Para que NetScaler 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 NetScaler 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.

NetScaler ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos NetScaler Gateway y generar los informes.

Para supervisar los dispositivos NetScaler Gateway implementados en este modo, primero debe agregar NetScaler Gateway al inventario de NetScaler ADM, habilitar AppFlow en NetScaler ADM y, a continuación, ver los informes en el panel de NetScaler ADM.

Configure HDX Insight en los servidores virtuales utilizados para Optimal Gateway

Pasos para configurar HDX Insight en servidores virtuales utilizados para Optimal Gateway:

1. Vaya a **Infraestructura > Instancias** y seleccione la instancia de NetScaler en la que desea habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione el servidor virtual VPN configurado para la autenticación y haga clic en **Habilitar análisis**.
4. Seleccione **HDX Insight** y, a continuación, **ICA**.
5. Seleccione otras opciones avanzadas según sea necesario.
6. Haga clic en **Aceptar**.
7. Repita los pasos 3 a 6 en el otro servidor virtual VPN.

Habilitar la recopilación de datos en NetScaler ADM

Si habilita NetScaler 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 NetScaler 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 NetScaler ADM:

1. En un explorador web, escriba la dirección IP del NetScaler 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 la lista **Seleccionar acción**, seleccione **Configurar análisis**.
5. Seleccione los servidores virtuales VPN y haga clic en **Habilitar análisis**.
6. Seleccione **HDX Insight** y, a continuación, seleccione **ICA** o **TCP** para el tráfico ICA o el 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 NetScaler ADM no muestra los registros, incluso si la columna Insight muestra Habilitado.

7. Haga clic en **Aceptar**.

Configuración de dispositivos NetScaler Gateway para exportar datos

Después de instalar los dispositivos NetScaler Gateway, debe configurar las siguientes opciones en los dispositivos NetScaler Gateway para exportar los informes a NetScaler ADM:

- Configure los servidores virtuales de los dispositivos NetScaler Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlace el servidor virtual NetScaler Gateway de la segunda DMZ al servidor virtual NetScaler Gateway de la primera DMZ.
- Habilite el salto doble en NetScaler Gateway en la segunda DMZ.
- Inhabilite la autenticación en el servidor virtual de NetScaler Gateway en la segunda DMZ.
- Habilite uno de los dispositivos NetScaler Gateway para exportar registros ICA
- Habilite el otro dispositivo NetScaler Gateway para exportar registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos NetScaler Gateway.

Configure NetScaler Gateway mediante la interfaz de línea de comandos:

1. Configure el servidor virtual de NetScaler Gateway en la primera DMZ para comunicarse con el servidor virtual de NetScaler Gateway en la segunda DMZ.


```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON
```

2. Enlace el servidor virtual NetScaler Gateway de la segunda DMZ al servidor virtual NetScaler Gateway de la primera DMZ. Ejecute el siguiente comando en NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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
```

6. Habilite el otro dispositivo NetScaler 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 NetScaler Gateway:

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

Configurar NetScaler Gateway mediante la Utilidad de configuración:

1. Configure NetScaler Gateway en la primera DMZ para comunicarse con NetScaler Gateway en

la segunda DMZ y enlazar NetScaler Gateway en la segunda DMZ a NetScaler Gateway en la primera 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 Avanzado, expanda **Aplicaciones publicadas**.

c) Haga clic en**Servidor de siguiente salto** y vincule un servidor de siguiente salto al segundo dispositivo NetScaler Gateway.

2. Habilite el salto doble en NetScaler 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) Amplíe más, seleccione**Double Hop**y haga clic en**Aceptar**.

3. Inhabilite la autenticación en el servidor virtual de NetScaler Gateway en la segunda DMZ.

a) En la pestaña **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) Amplíe**más**y desactive la opción**Habilitar autenticación**.

4. Habilite uno de los dispositivos NetScaler Gateway para exportar registros TCP.

a) En la pestaña **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**Elegir directiva**, seleccione**AppFlow**y, en la lista **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 NetScaler Gateway para exportar registros ICA:

a) En la pestaña **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**Elegir directiva**, seleccione AppFlow y, en la lista 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 NetScaler Gateway.

a) En la ficha **Configuración**, vaya a **Sistema** > **Appflow**.

b) En el panel derecho, en el grupo**Configuración**, haga doble clic en**Cambiar la configuración de Appflow**.

c) Seleccione **Conexión encadenamiento** y haga clic en **Aceptar**.

7. Configure NetScaler Gateway en la primera DMZ para comunicarse con NetScaler Gateway en la segunda DMZ y enlazar NetScaler Gateway en la segunda DMZ a NetScaler Gateway en la primera DMZ.

a) En la pestaña 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 **Aplicaciones publicadas** .

c) Haga clic en**Servidor de siguiente salto**y vincule un servidor de siguiente salto al segundo dispositivo NetScaler Gateway.

8. Habilite el salto doble en NetScaler Gateway en la segunda DMZ.

a) En la pestaña 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) Amplíe Más, seleccione**Double Hop**y pulse**Aceptar**.

9. Inhabilite la autenticación en el servidor virtual de NetScaler Gateway en la segunda DMZ.

a) En la pestaña 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) Amplíe**más**y desactive la opción**Habilitar autenticación**.

10. Habilite uno de los dispositivos NetScaler Gateway para exportar registros TCP.
    a) En la pestaña 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 Elegir directiva, seleccione AppFlow y, en la lista **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 NetScaler Gateway para exportar registros ICA.
    a) En la pestaña 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**Elegir directiva**, seleccione AppFlow y, en la lista **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 NetScaler Gateway.

Habilite la recopilación de datos para supervisar los NetScalers implementados en modo transparente

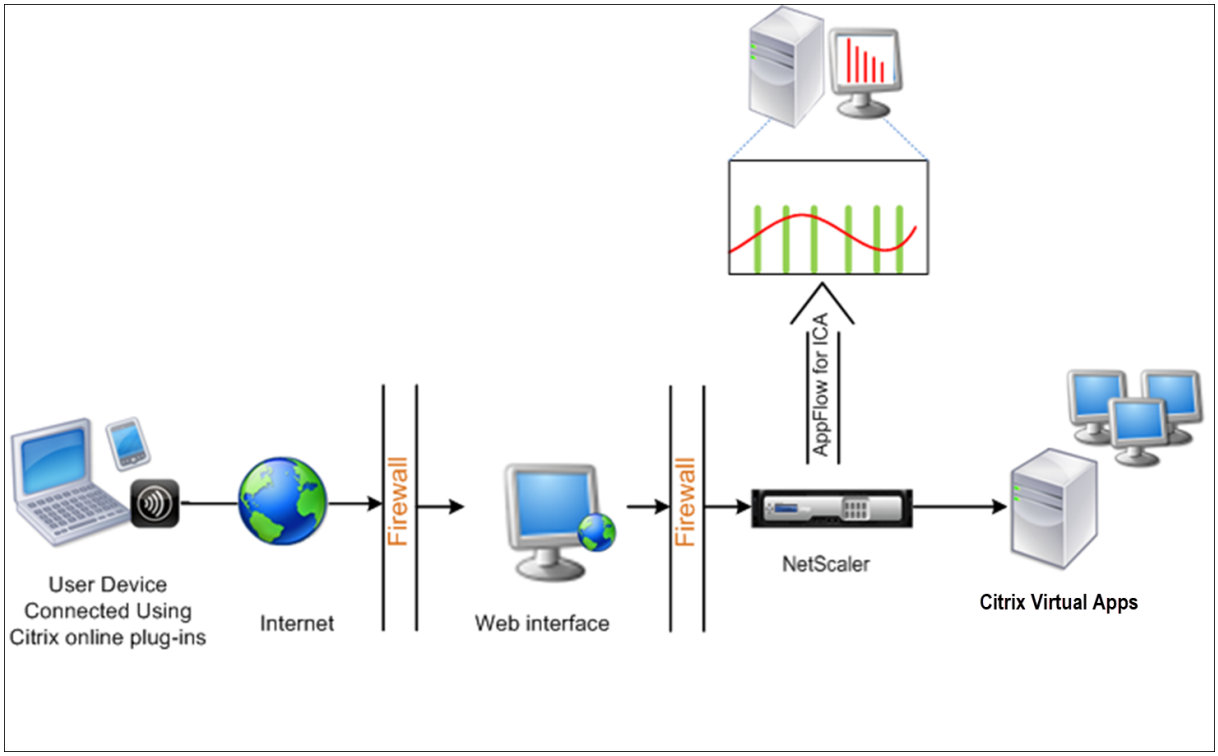
Cuando un NetScaler se implementa en modo transparente, los clientes pueden acceder a los servidores directamente, sin que intervenga ningún servidor virtual. Si un dispositivo NetScaler se implementa en modo transparente en un entorno de Citrix Virtual Apps and Desktop, el tráfico ICA no se transmite a través de una VPN.

Después de agregar NetScaler al inventario NetScaler 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 NetScaler ADM como un recopilador de AppFlow en cada dispositivo NetScaler y debe configurar una directiva de AppFlow para recopilar todo o el tráfico ICA específico que fluye a través del dispositivo.

Nota

- No puede habilitar la recopilación de datos en un NetScaler implementado en modo transparente mediante la utilidad de configuración de NetScaler 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 NetScaler ADM cuando un NetScaler se implementa 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>...
```

Ejemplo:

```
set ns param -icaPorts 2598 1494
```


> **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 un recopilador AppFlow en el dispositivo NetScaler.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Ejemplo:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> **Nota** Para ver los recopiladores AppFlow configurados en el dispositivo NetScaler, utilice el comando**show appflow collector**.

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string> ...
```

Ejemplo:

agregar acción AppFlow act-colectores MyInsight

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
```

Ejemplo:

```
add appflow policy pol true act
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
```

Ejemplo:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Nota**
>
> El valor de **tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarlo 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
```

8. Guarde la configuración. Tipo: `save ns config`

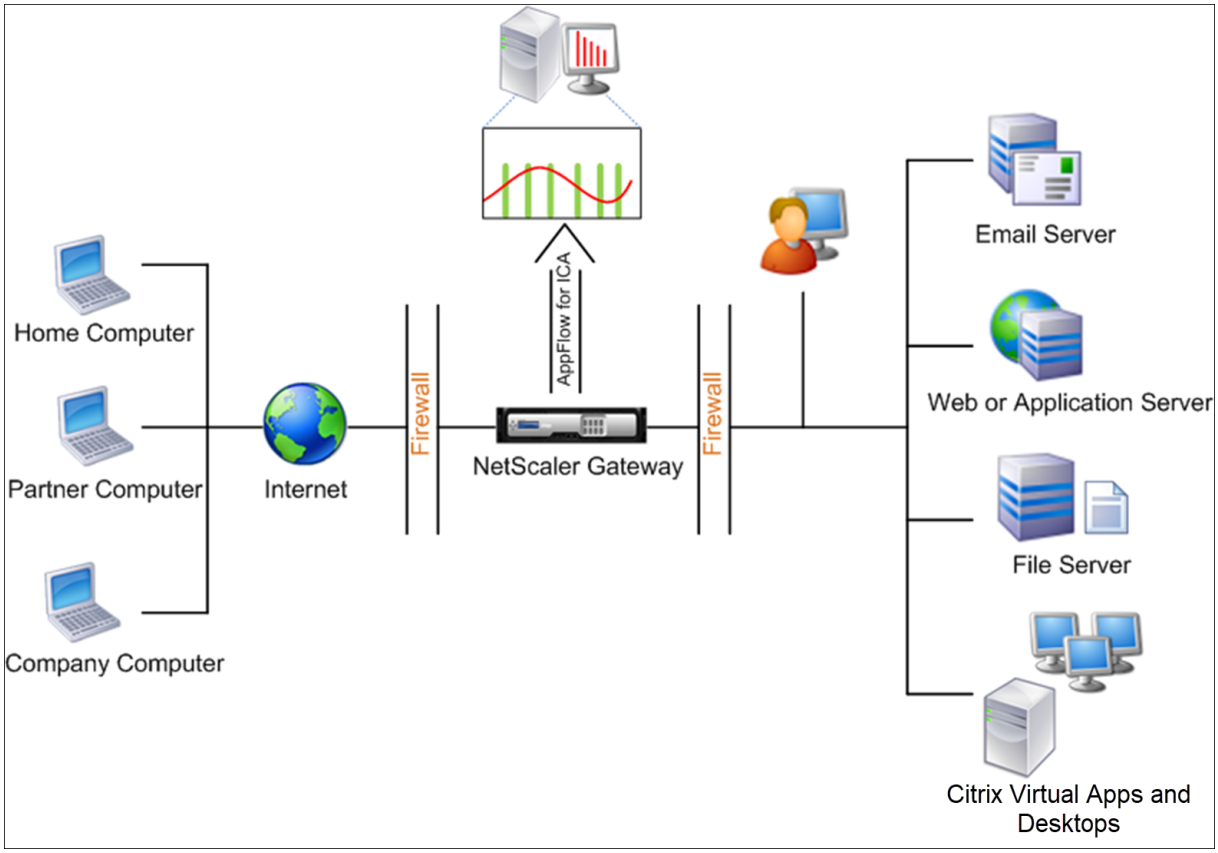
‘‘‘

Habilitar la recopilación de datos para dispositivos NetScaler Gateway implementados en modo de salto único

January 30, 2024

Cuando implementa NetScaler 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 NetScaler a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo NetScaler Gateway al inventario de NetScaler Application Delivery Management (ADM) y habilitar AppFlow en ADM.



Para habilitar la función AppFlow desde ADM:

1. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia de NetScaler en la que desea habilitar el análisis.
2. En la lista **Acción**, seleccione **Activar/Desactivar Insight**.
3. Seleccione los **servidores virtuales VPN** y haga clic en **Habilitar AppFlow** .
4. En el campo **Habilitar AppFlow**, escriba **true** y seleccione **ICA**.
5. Haga clic en **Aceptar**.

> **Nota**
>
> Cuando habilita AppFlow en modo de salto único, los siguientes comandos se ejecutan en segundo plano. 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 NetScaler 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 NetScaler ADM.

Habilite la recopilación de datos para supervisar los NetScalers implementados en modo transparente

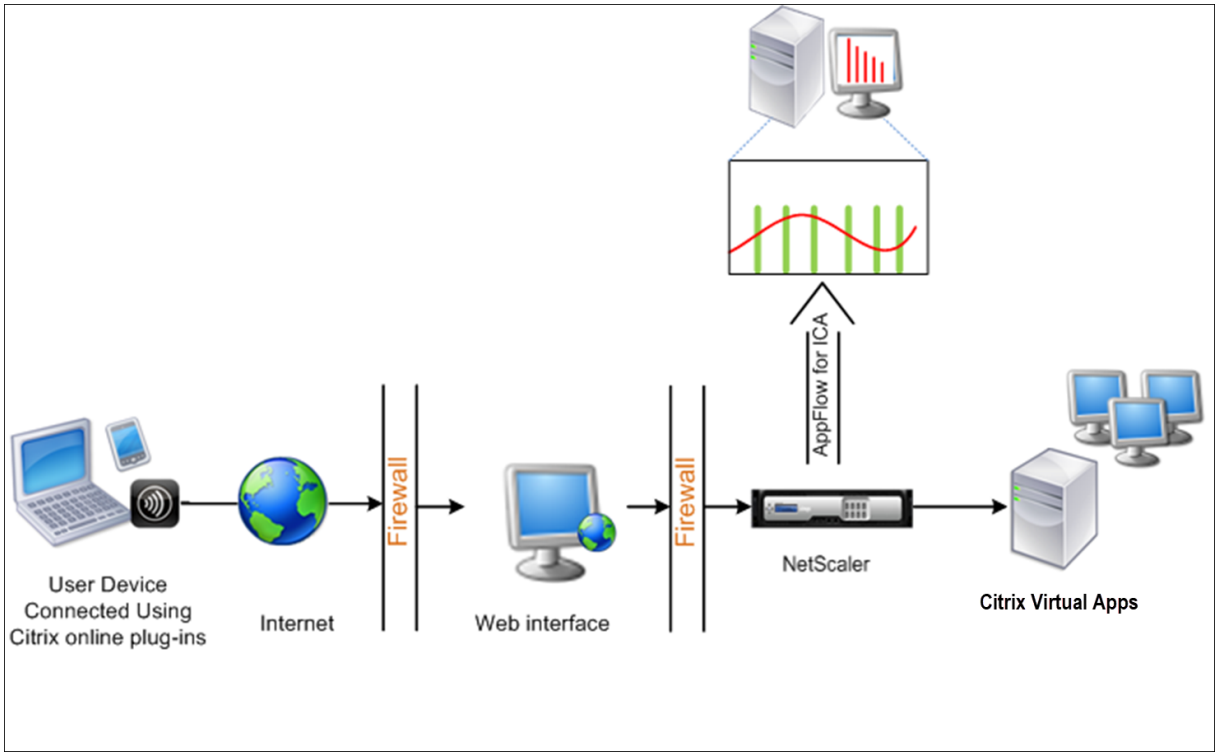
January 30, 2024

Cuando un NetScaler se implementa en modo transparente, los clientes pueden acceder a los servidores directamente, sin que intervenga ningún servidor virtual. Si un 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 NetScaler al inventario NetScaler 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 NetScaler ADM como recopilador de AppFlow en cada instancia de NetScaler y configurar una directiva de AppFlow para recopilar todo el tráfico ICA, o uno específico, que fluye a través del dispositivo.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un NetScaler implementado en modo transparente mediante la utilidad de configuración de NetScaler 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 NetScaler ADM cuando un NetScaler se implementa 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 un recopilador de AppFlow en la instancia de 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 AppFlow configurados en la instancia de NetScaler, utilice el comando**show appflow collector**.

4. Cree una acción AppFlow 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 AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlace la directiva de AppFlow 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 de **tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarlo 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.

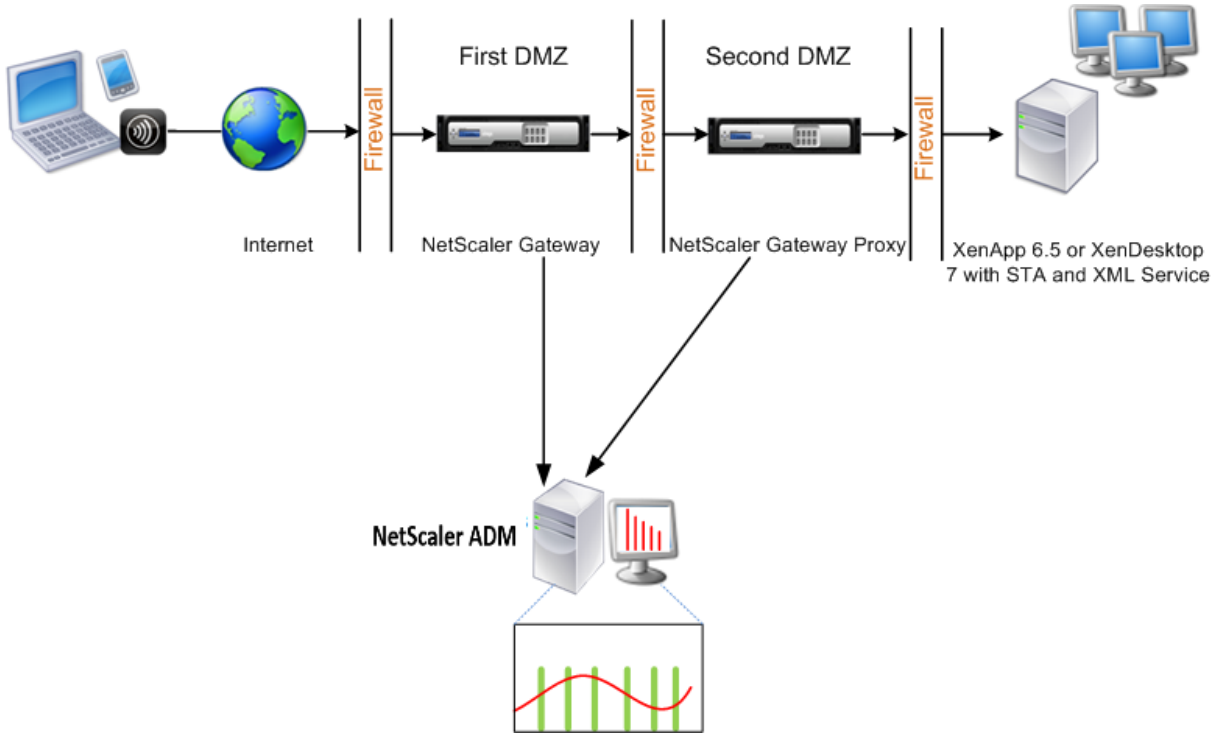
```
save ns config
<!--NeedCopy-->
```


Habilitar la recopilación de datos para dispositivos NetScaler Gateway implementados en modo de salto doble

January 30, 2024

El modo de doble salto de NetScaler Gateway proporciona protección adicional a la red interna de una organización, ya que un atacante tendría que penetrar en varias zonas de seguridad o zonas desmilitarizadas (DMZ) para llegar a los servidores de la red segura. Si quiere analizar la cantidad de saltos (dispositivos NetScaler Gateway) por los que pasan las conexiones ICA y también los detalles sobre la latencia de cada conexión TCP y su comparación con la latencia ICA total percibida por el cliente, debe instalar NetScaler ADM para que los dispositivos NetScaler Gateway generen estas estadísticas vitales.

Figura 3 . NetScaler ADM implementado en modo de salto doble



NetScaler Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Este NetScaler Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

NetScaler Gateway en la segunda DMZ sirve como dispositivo proxy de NetScaler Gateway. Este NetScaler Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores.

El NetScaler ADM se puede implementar en la subred que pertenece al dispositivo NetScaler Gateway

en la primera DMZ o en la subred que pertenece a la segunda DMZ del dispositivo NetScaler Gateway. En la imagen de arriba, NetScaler ADM y NetScaler Gateway de la primera DMZ se implementan en la misma subred.

En modo de salto doble, NetScaler ADM recopila los registros TCP de un dispositivo y los registros ICA del otro dispositivo. Después de agregar los dispositivos NetScaler Gateway al inventario de NetScaler ADM y habilitar la recopilación de datos, cada dispositivo exporta los informes haciendo un seguimiento del recuento de saltos y el ID de cadena de conexión.

Para que NetScaler 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 NetScaler 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.

NetScaler ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos NetScaler Gateway y generar los informes.

Para supervisar los dispositivos NetScaler Gateway implementados en este modo, primero debe agregar NetScaler Gateway al inventario de NetScaler ADM, habilitar AppFlow en NetScaler ADM y, a continuación, ver los informes en el panel de NetScaler ADM.

Habilitar la recopilación de datos en NetScaler ADM

Si habilita NetScaler 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 NetScaler 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 NetScaler ADM:

1. Vaya a **Infraestructura > Instancias** y seleccione la instancia de NetScaler en la que desea habilitar el análisis.
2. En la lista **Acción**, seleccione **Activar/Desactivar Insight**.
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 el tráfico ICA un tráfico TCP respectivamente.

   > **Nota**
   >
   > Si el registro de AppFlow no está habilitado para los servicios o grupos de servicios del dis-

> positivo NetScaler, el panel de control de NetScaler ADM no muestra los registros, incluso si la columna Insight muestra Habilitado.

5. Haga clic en **Aceptar**.

Configurar los dispositivos de NetScaler Gateway para exportar datos

Después de instalar los dispositivos NetScaler Gateway, debe configurar las siguientes opciones en los dispositivos NetScaler Gateway para exportar los informes a NetScaler ADM:

- Configure los servidores virtuales de los dispositivos NetScaler Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlace el servidor virtual NetScaler Gateway de la segunda DMZ al servidor virtual NetScaler Gateway de la primera DMZ.
- Habilite el salto doble en NetScaler Gateway en la segunda DMZ.
- Inhabilite la autenticación en el servidor virtual de NetScaler Gateway en la segunda DMZ.
- Habilite uno de los dispositivos NetScaler Gateway para exportar registros ICA
- Habilite el otro dispositivo NetScaler Gateway para exportar registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos NetScaler Gateway.

Configure NetScaler Gateway mediante la interfaz de línea de comandos:

1. Configure el servidor virtual de NetScaler Gateway en la primera DMZ para comunicarse con el servidor virtual de NetScaler 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. Enlace el servidor virtual NetScaler Gateway de la segunda DMZ al servidor virtual NetScaler Gateway de la primera DMZ. Ejecute el siguiente comando en NetScaler 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 NetScaler 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 NetScaler Gateway en la segunda DMZ.

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Habilite uno de los dispositivos NetScaler 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 NetScaler 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
<!--NeedCopy-->
```

7. Habilite el encadenamiento de conexiones en ambos dispositivos NetScaler Gateway:

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Configuración de NetScaler Gateway mediante la utilidad de configuración:

1. Configure NetScaler Gateway en la primera DMZ para comunicarse con NetScaler Gateway en la segunda DMZ y enlazar NetScaler Gateway en la segunda DMZ a NetScaler Gateway en la primera 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 Avanzado, expanda **Aplicaciones publicadas**.

c) Haga clic en**Servidor de siguiente salto** y vincule un servidor de siguiente salto al segundo dispositivo NetScaler Gateway.

2. Habilite el salto doble en NetScaler 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**, seleccione **Doble salto** y haga clic en **Aceptar**.

3. Inhabilite la autenticación en el servidor virtual de NetScaler Gateway en la segunda DMZ.

a) En la pestaña **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) Amplíe**más**y desactive la opción**Habilitar autenticación**.

4. Habilite uno de los dispositivos NetScaler Gateway para exportar registros TCP.

a) En la pestaña **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**Elegir directiva**, seleccione**AppFlow**y, en la lista desplegable**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 NetScaler Gateway para exportar registros ICA:

a) En la pestaña **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 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 NetScaler Gateway.

a) En la ficha**Configuración**, vaya a**Configuración > 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**.

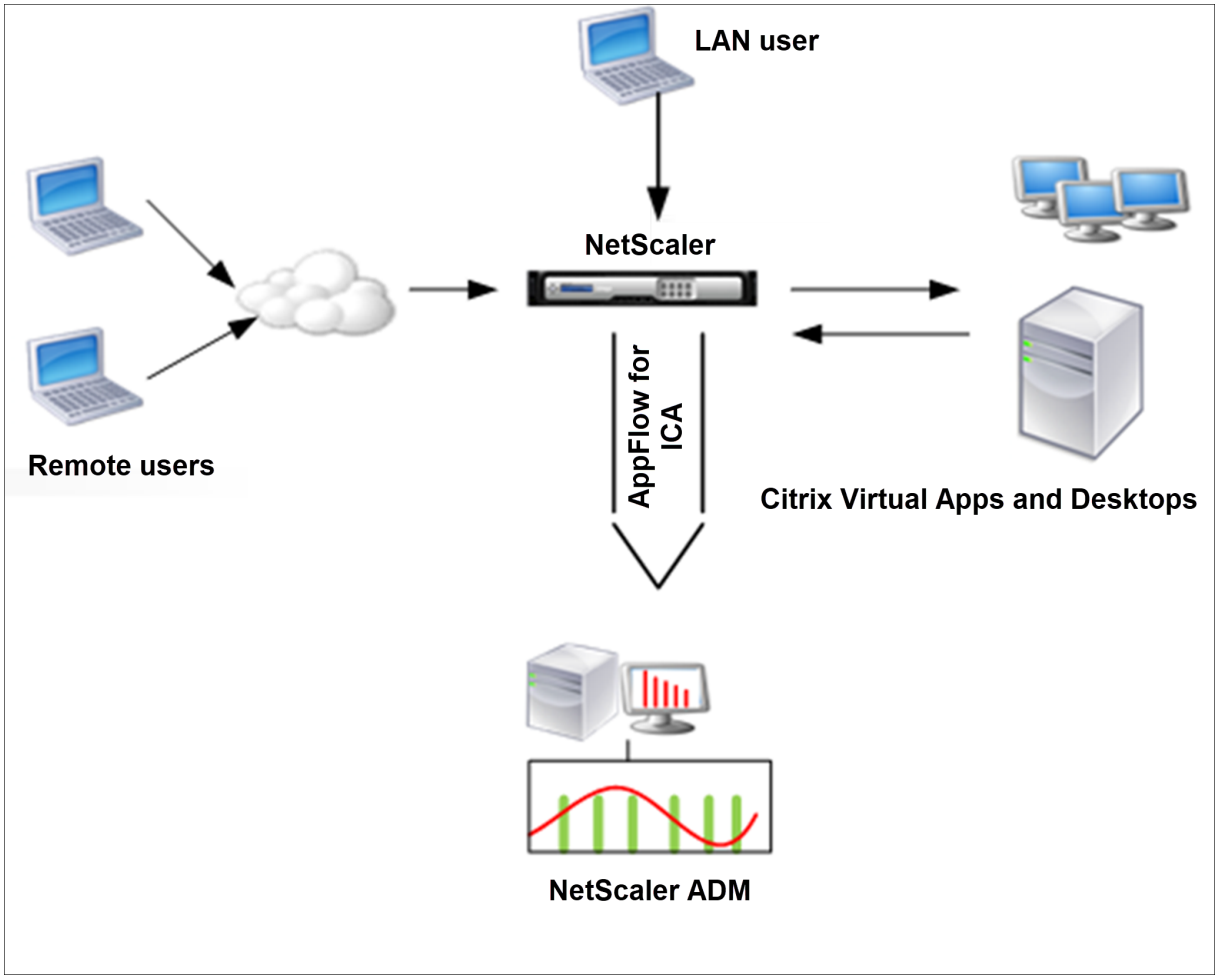
Habilite la recopilación de datos para supervisar los NetScalers implementados en modo de usuario de LAN

January 30, 2024

Los usuarios externos que acceden a las aplicaciones de Citrix Virtual App o Desktop deben autenticarse en NetScaler Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a NetScaler 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 aplicaciones de 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 NetScaler Gateway.

Figura 4 . NetScaler ADM implementado en modo de usuario de LAN



Nota NetScaler ADM y el dispositivo NetScaler Gateway residen en la misma subred.

Para supervisar los dispositivos NetScaler implementados en este modo, primero agregue el dispositivo NetScaler al inventario de NetScaler Insight, habilite AppFlow y, a continuación, consulte los informes en el panel.

Después de agregar el dispositivo NetScaler al inventario de NetScaler ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un NetScaler implementado en modo de usuario de LAN mediante la utilidad de configuración de NetScaler 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 NetScaler 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 NetScaler ADM como un recopilador AppFlow en el dispositivo NetScaler.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
   \\>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Cree una acción AppFlow 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 AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlace la directiva de AppFlow 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 de tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicar 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 on NetScaler Application Delivery Management (ADM) le permite supervisar el tráfico de HDX que pasa por las instancias de NetScaler. NetScaler ADM le permite establecer umbrales en varios contadores utilizados para supervisar el tráfico de Insight. También puede configurar reglas y crear alertas en NetScaler 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 aplicación está asociada con varios accesos, ancho de banda consumido por la aplicación y 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 NetScaler 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 NetScaler 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: ICA RTT (métrica) para usuarios (entidad) debe ser <= 100 ms
- Regla de umbral2: La latencia 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, NetScaler 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 NetScaler ADM o recibir la alerta por 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 NetScaler ADM.

Los grupos de umbral también se pueden vincular a las geolocalizaciones para el supervisión geo-específico 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 NetScaler 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 para optimizar la entrega de aplicaciones y escritorios para acceder 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 algunos se encuentran en 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 ICA RTT para una ubicación cercana al centro de datos puede ser de 5 a 10 ms, mientras que el mismo para una ubicación remota puede ser de unos 100 ms.

Con la administración 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 sobre las 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 NetScaler ADM:

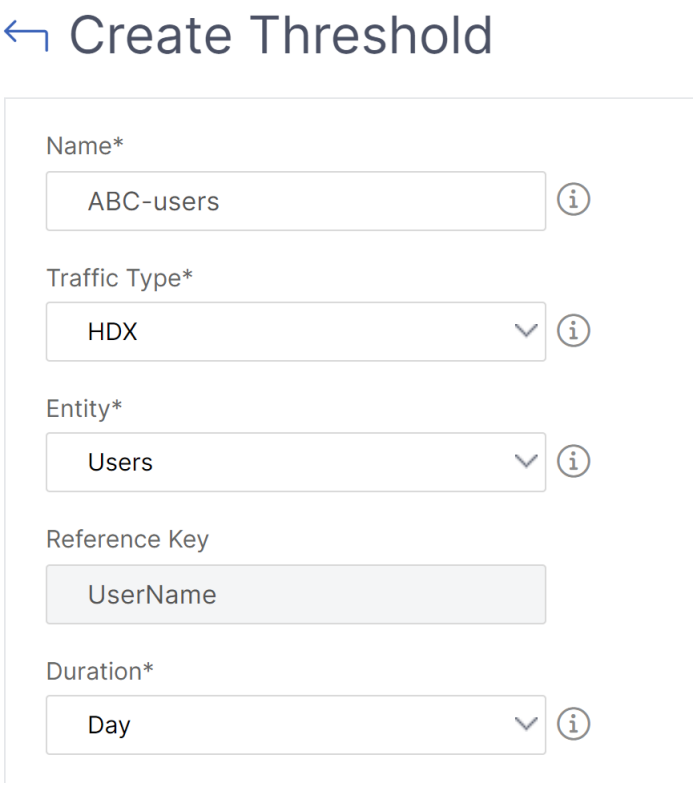
1. En NetScaler ADM, vaya a **Configuración > Configuración de Analytics > Umbrales**. En la página **Umbrales** que se abre, haga clic en **Agregar**.
2. En la página **Crear umbrales y alertas**, especifique los siguientes detalles:
    a) **Nombre**. Escriba un nombre para crear un evento para el que NetScaler ADM genere una alerta.

b) **Tipo de tráfico**. En el cuadro de lista, selecciona HDX.

c) **Entidad**. En el cuadro de lista, seleccione la categoría o el tipo de recurso. Las entidades difieren para cada tipo de tráfico seleccionado anteriormente.

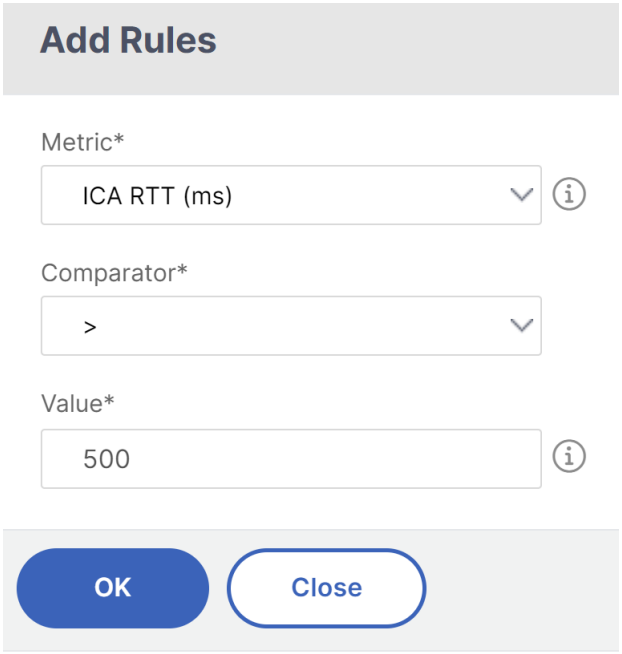
d) **Clave de referencia**. Se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.

e) **Duración**. En el cuadro de lista, 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.

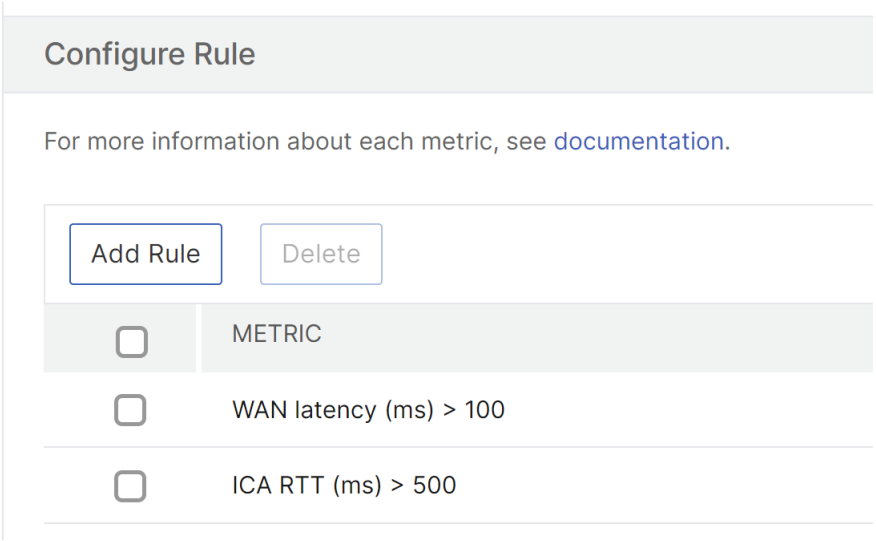


3. Creación de grupo de reglas de umbral para todas las entidades:

   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.

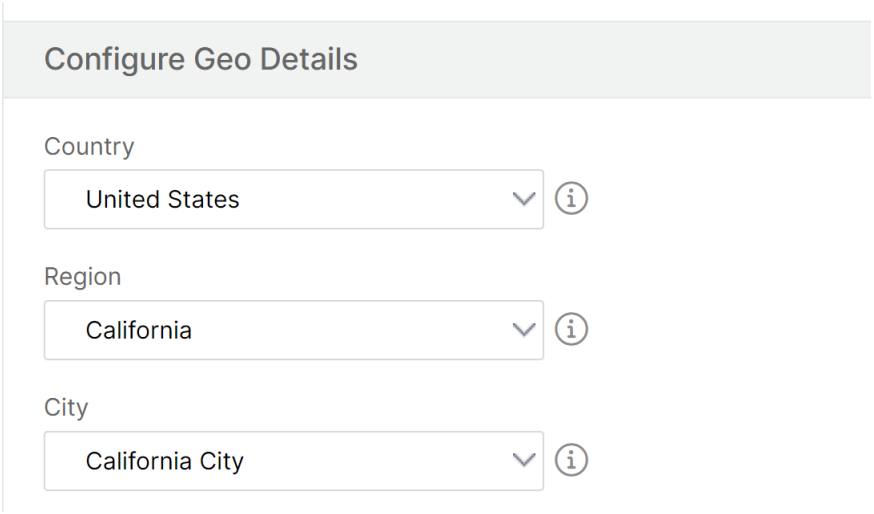


Puede crear varias reglas para supervisar cada entidad. La creación de varias reglas en un solo grupo le permite supervisar las entidades como un grupo de reglas de umbral en lugar de reglas individuales. Haga clic en **Aceptar** para cerrar la ventana.



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 NetScaler 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.

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 App o Desktop 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 que actúan como puertas de enlace para el tráfico entrante.
- **Escritorios**: muestra los informes de los escritorios utilizados en el período de tiempo seleccionado.

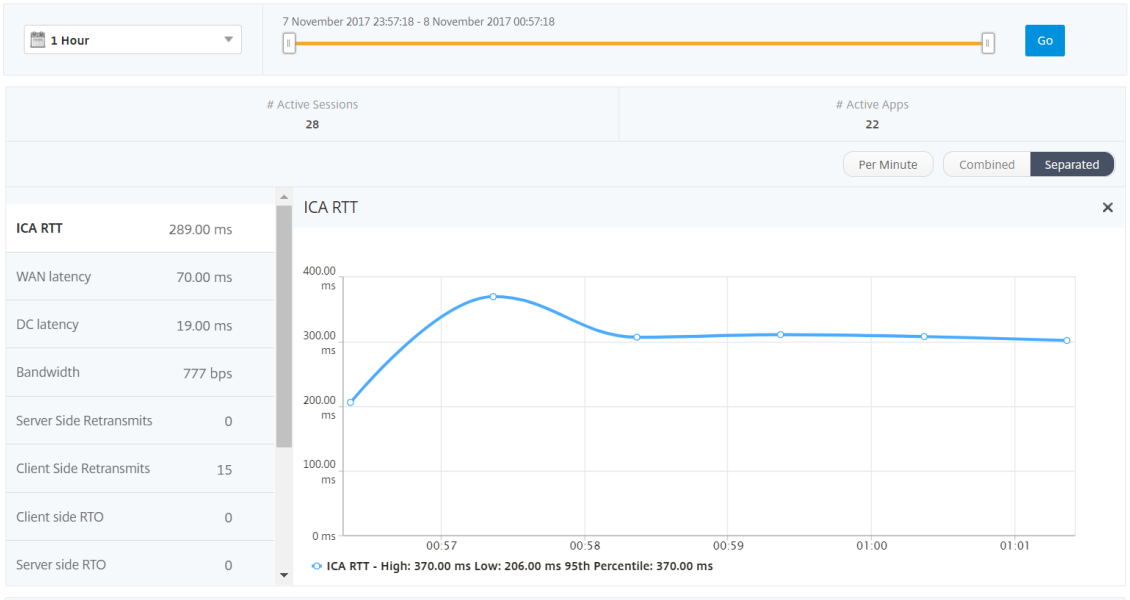
- **Licencias**: muestra los informes del total de licencias de VPN con SSL utilizadas dentro del intervalo de tiempo especificado.

Informes y métricas de visualización de usuarios

Los informes y las métricas de esta vista se muestran por usuario de Citrix Virtual Apps and Desktops.

Para navegar a la vista de usuarios:

1. Vaya a **Gateway > HDX Insight > Usuarios**



Los informes de vista de usuario y las métricas 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 e 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:

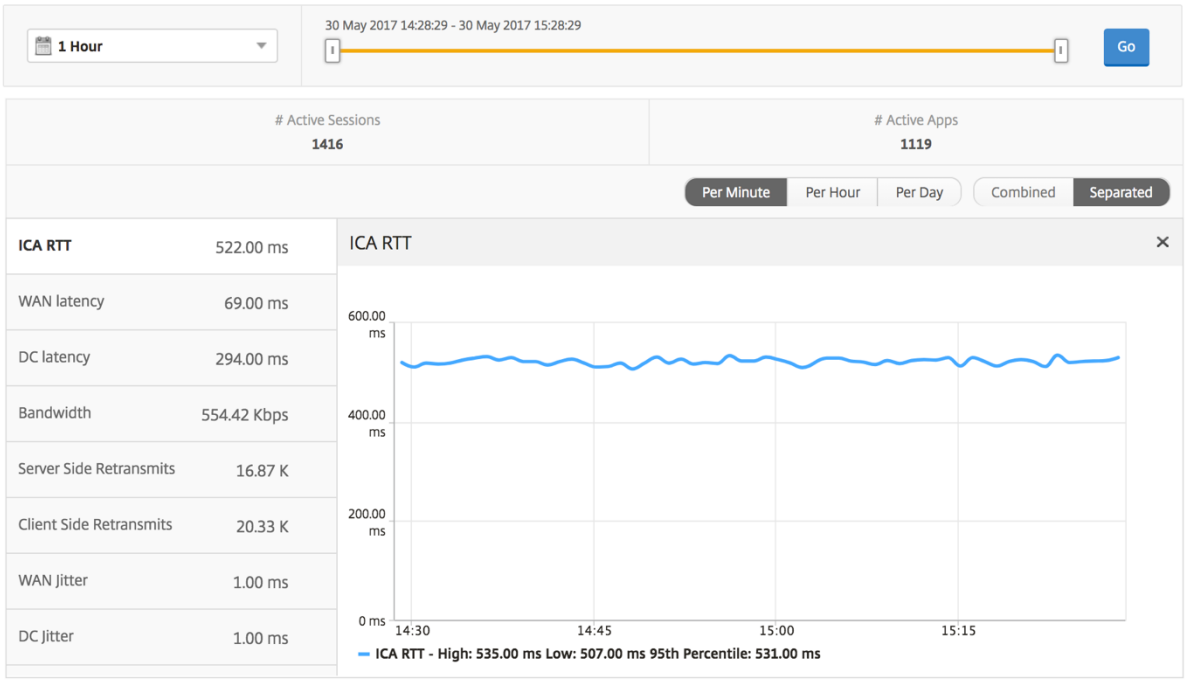
1. Utilice la lista de períodos de tiempo o el control deslizante de tiempo para establecer el intervalo de tiempo deseado.

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 App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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 y el servidor back-end.
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 ha producido 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 resumido 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 escritorio alojado en Citrix Virtual App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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.

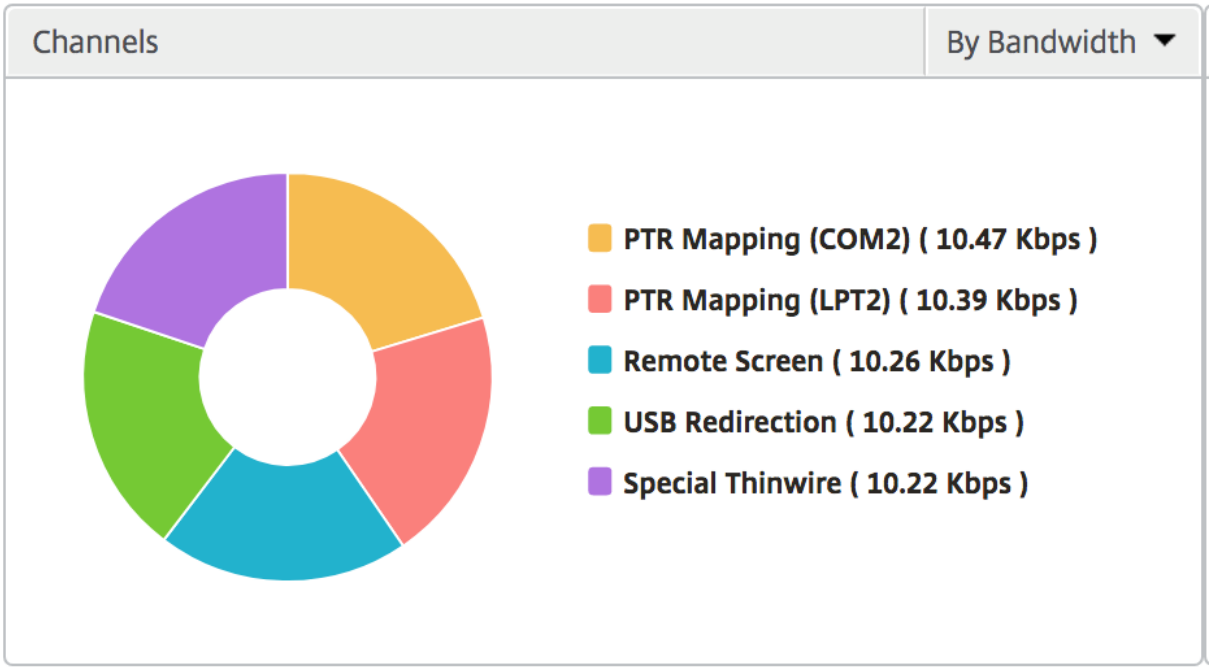
Métricas	Descripción
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Retransmisiones del lado del servidor	El número de paquetes retransmitidos en la conexión entre NetScaler y el servidor back-end.
Retransmisiones 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 ha producido 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

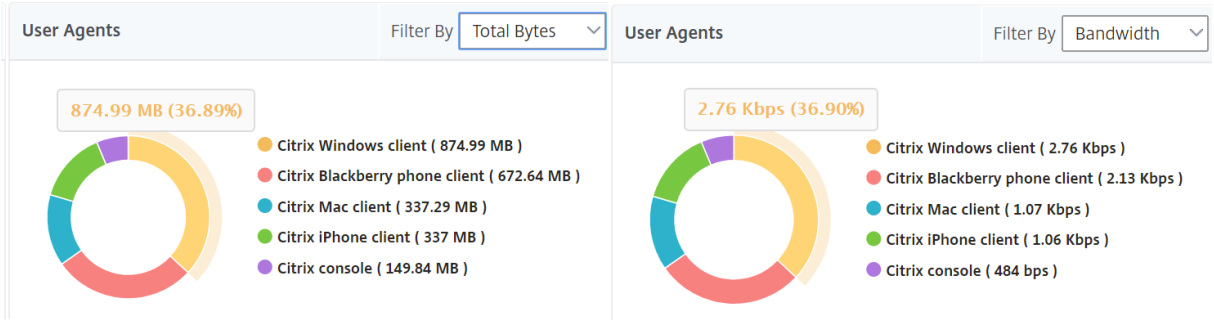
Search

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	

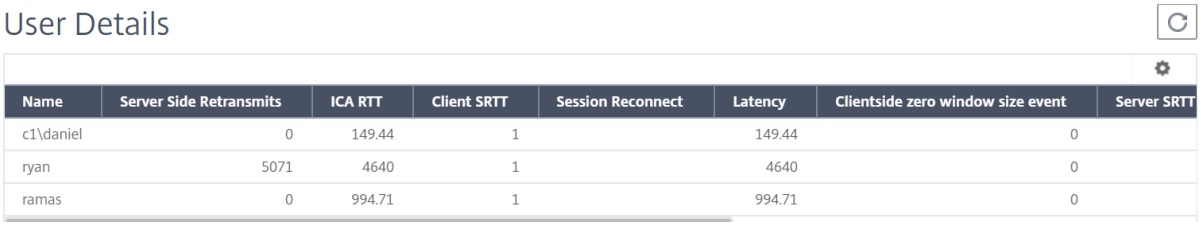
Canales Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.



Agentes de usuario Los agentes de usuario representan el ancho de banda total y el total de bytes consumidos por cada cliente del espacio de trabajo en forma de gráfico de anillos. Cada segmento coloreado del gráfico representa un cliente del espacio de trabajo. La longitud del segmento depende del número de usuarios que lancen sus aplicaciones en ese cliente de espacio de trabajo. 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 de espacio de trabajo.



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	

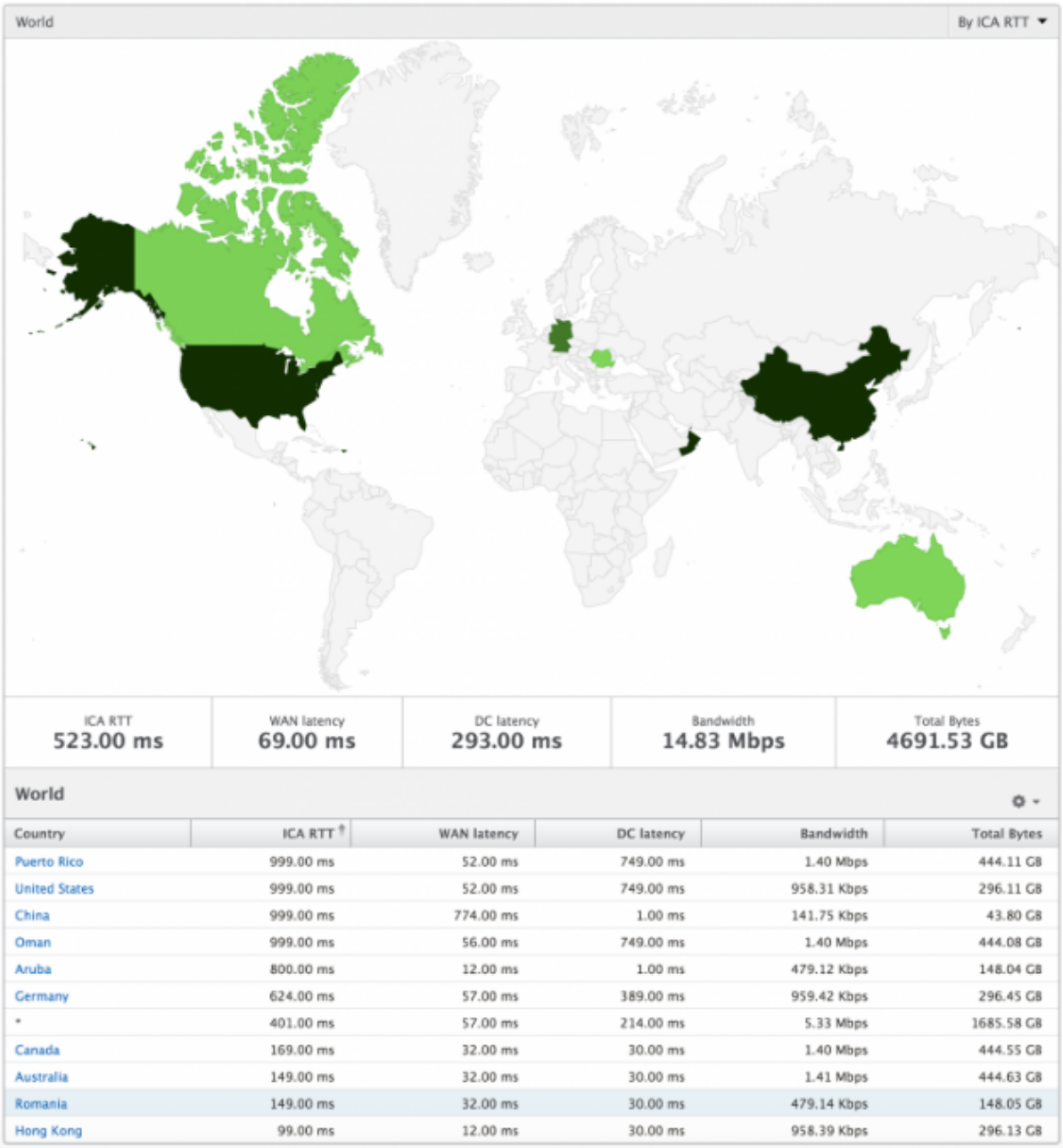
Recuento de infracciones de umbrales Las métricas de recuento de infracciones de Umbrales representan el recuento de umbrales incumplidos en el período de tiempo seleccionado.

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, simplemente haciendo 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 **Gateway > 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 por los NetScalers 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 espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.

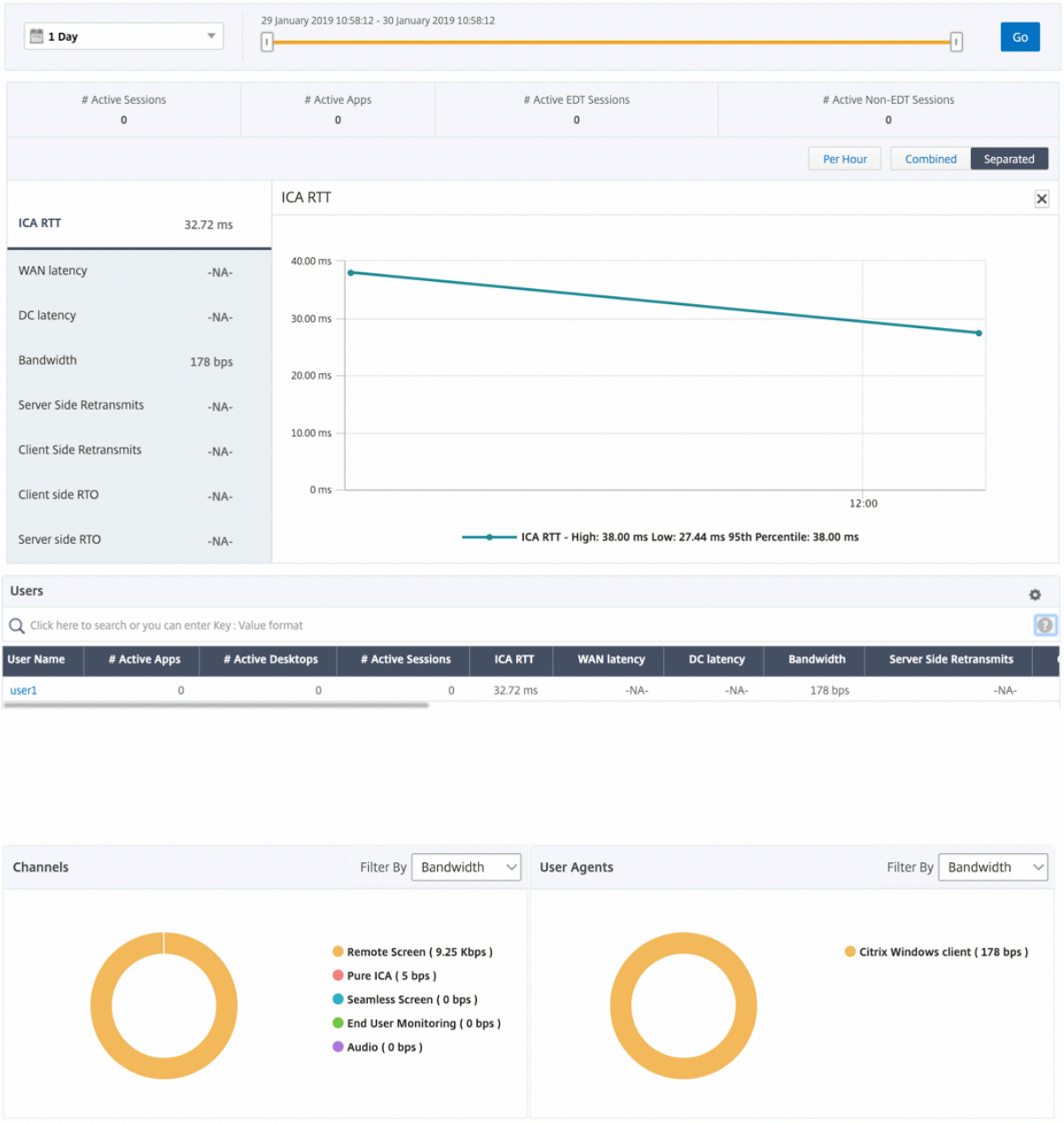
Métricas	Descripción
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que 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 App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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 y el servidor back-end.

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 ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.

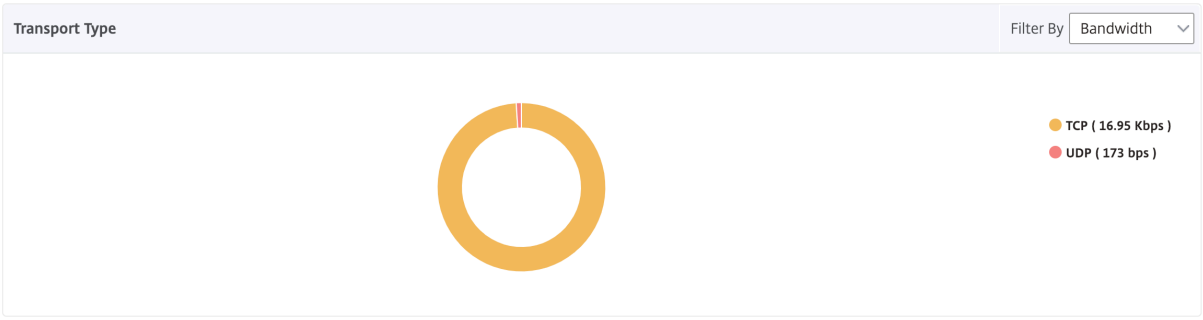
Soporte para EDT en HDX insights

NetScaler Application Delivery Management (ADM) ahora admite el transporte de datos avanzado (EDT) para mostrar los análisis de 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 Workspace.

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, aparecen como "NA".



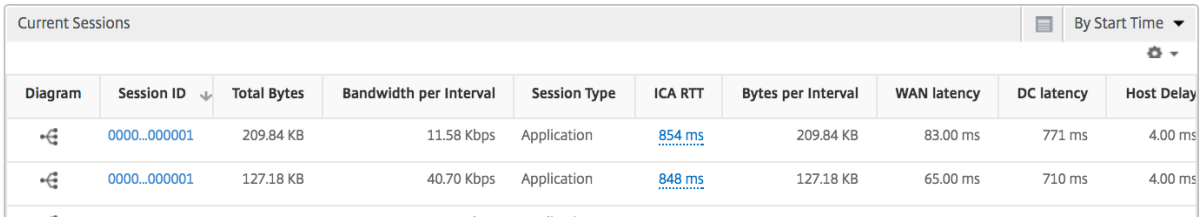
Se ha introducido un nuevo gráfico de donut para permitirle ver el ancho de banda consumido por el usuario y también el número total de bytes según el tipo de protocolo utilizado por los usuarios.

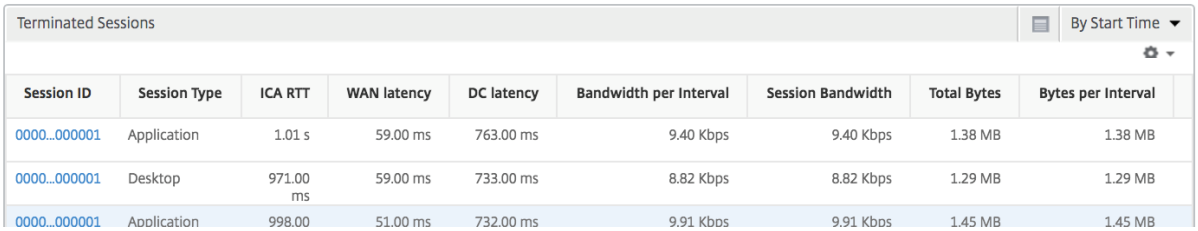


> **Nota**
>
> EDT en HDX Insight es compatible con NetScaler ADM desde la versión 12.1 compilación 50.28 y está disponible en instancias ADC desde la versión 12.1 compilación 49.23.

Métricas de HDX Insight disponibles en NetScaler ADM 12.0 y versiones posteriores:

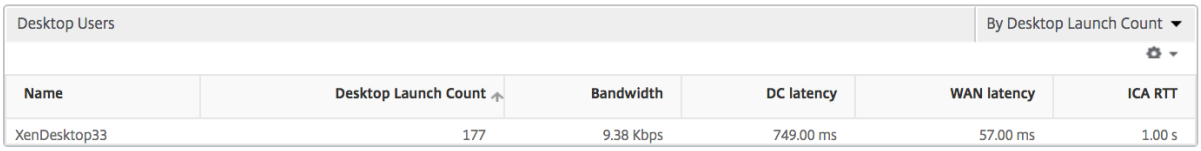
Latencia del lado del cliente L7	Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega.
Latencia L7 del lado del servidor	La latencia media de L7 observada entre el dispositivo NetScaler y Citrix Virtual App. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén 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.



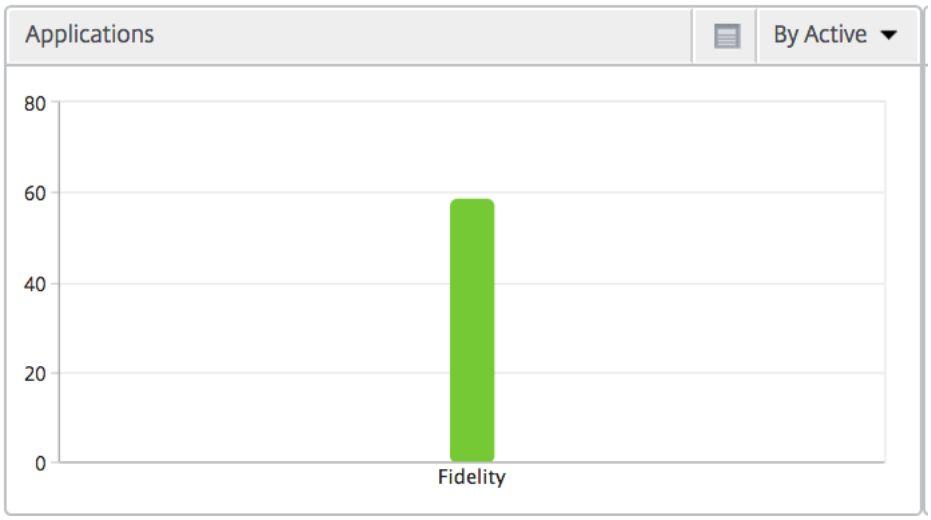


Usuarios de escritorio Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

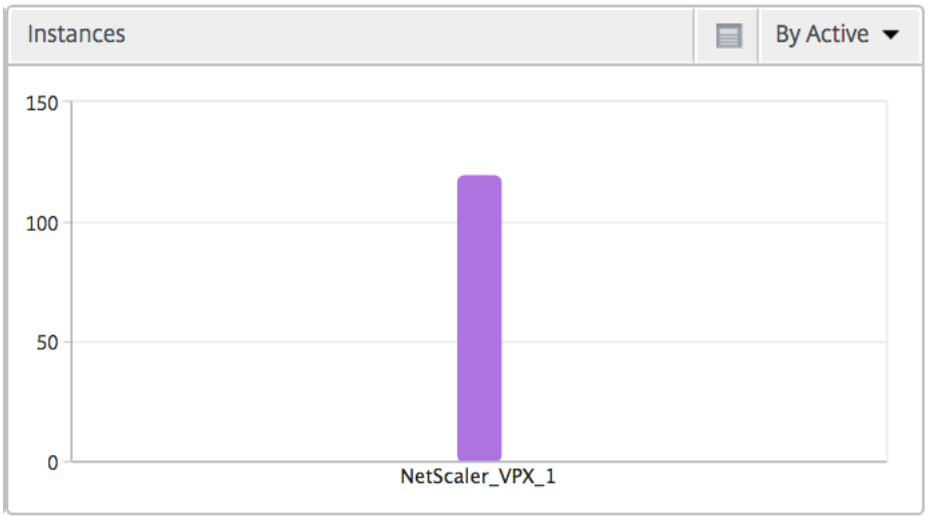
Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia causada por el lado del servidor de la red 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 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 App o Desktop, respectivamente.



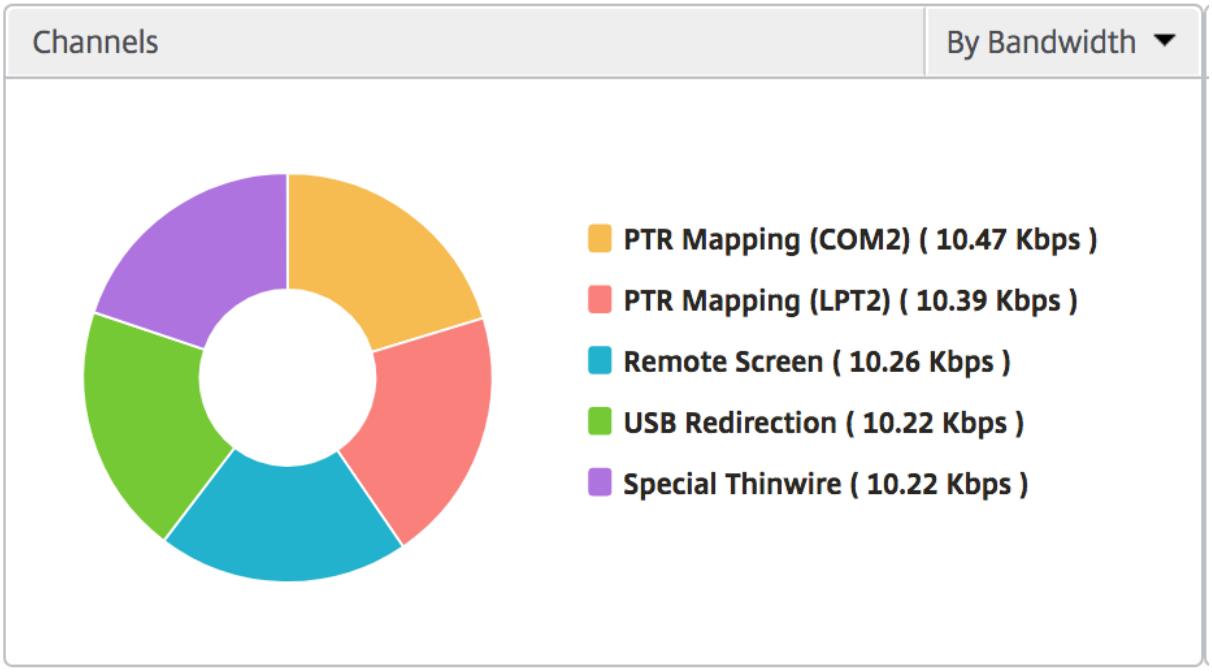
Aplicaciones Gráfico de barras que representa las aplicaciones ordenadas por Activo, recuento total de inicio de sesión, recuento total de inicio de aplicaciones y duración del lanzamiento.



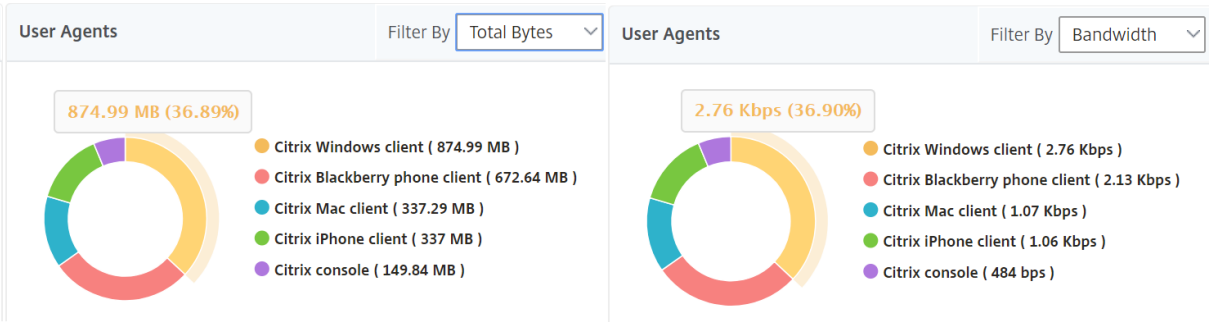
Instancias Un gráfico de barras que representa las instancias de NetScaler ordenadas por aplicaciones activas y totales



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.



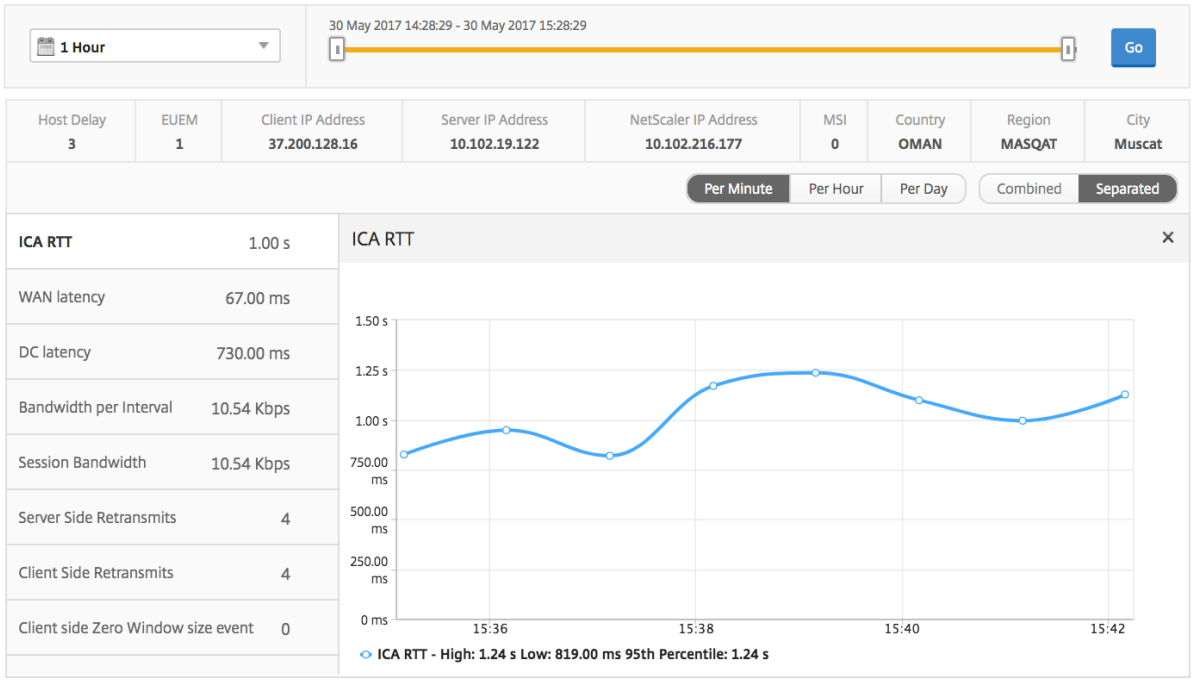
Vista de sesión por usuario La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

Para ver las métricas de la sesión de un usuario seleccionado:

1. Vaya a **Gateway > 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**.

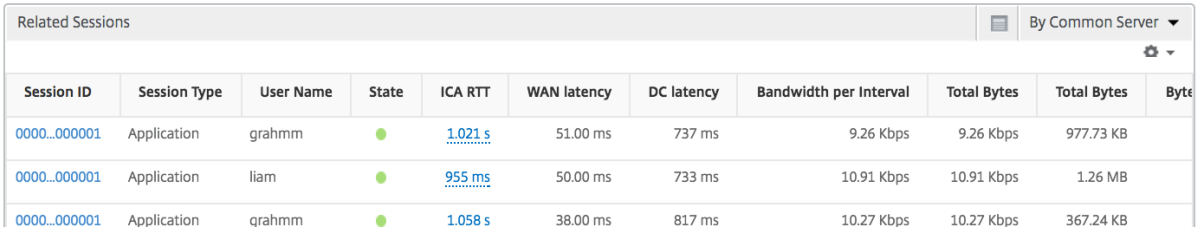
Gráfico cronológico

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	El RTT de ICA es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps o Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red 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 y el servidor back-end.
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 ha producido 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.



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 aplicaciones

Los informes y métricas de esta vista se centran en Citrix Virtual Apps.

Para desplazarse a la vista Aplicación:

1. Vaya a **Gateway > HDX Insight > Aplicaciones** .

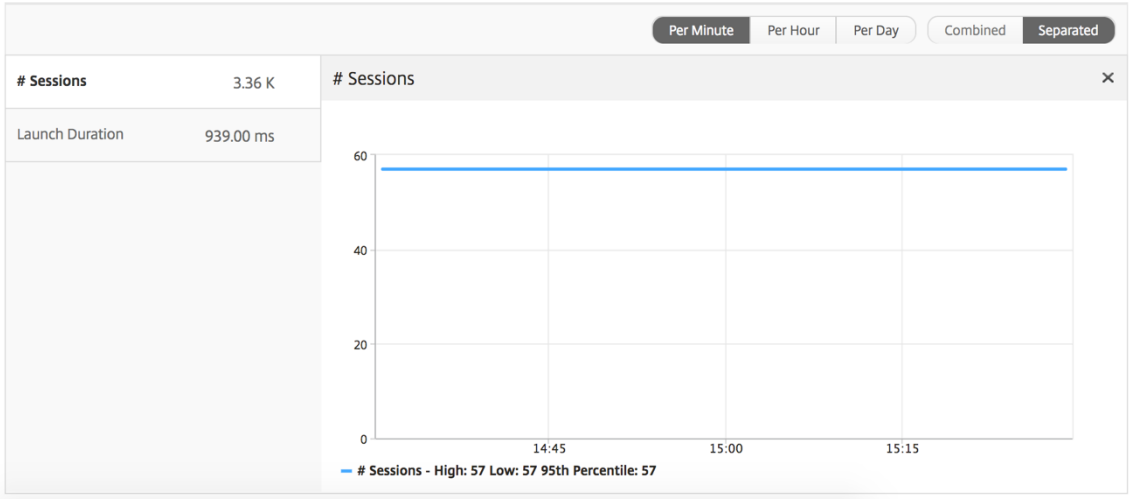
Vista de resumen

La vista de resumen muestra los informes de todas las aplicaciones que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas/informes, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

Gráfico de líneas

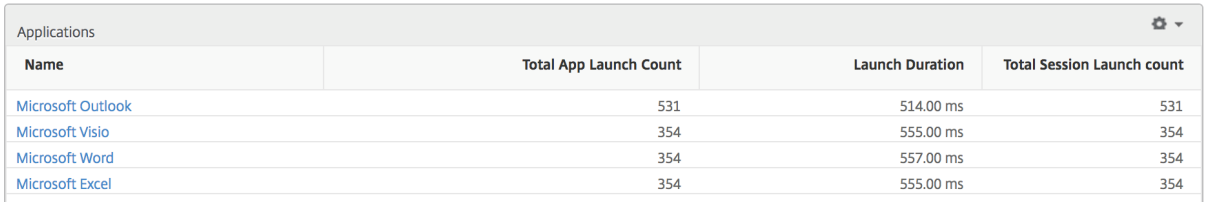
Métricas	Descripción
N.º de sesiones	Número total de sesiones durante un intervalo de tiempo determinado.
Duración de inicios	Promedio de tiempo necesario para iniciar una aplicación.



Informe resumido de las aplicaciones

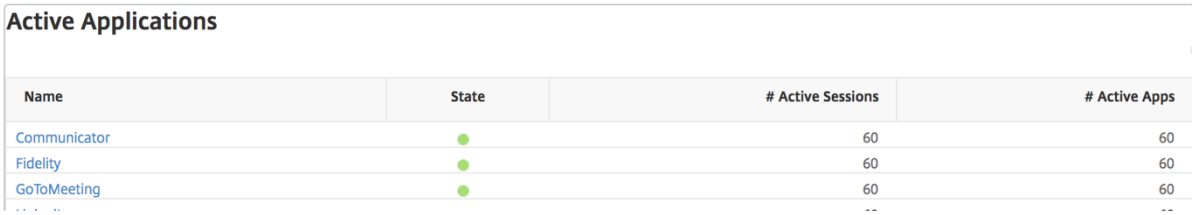
Métricas	Descripción
Nombre	Nombre de la aplicación virtual Citrix.
Recuento total de sesiones iniciadas	Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado.

Métricas	Descripción
Recuento total de aplicaciones iniciadas	Número total de aplicaciones de Citrix Virtual App lanzadas durante el intervalo de tiempo dado.
Duración de inicios	Tiempo promedio que se tarda en iniciar la aplicación virtual de Citrix.



Informe de aplicación activa

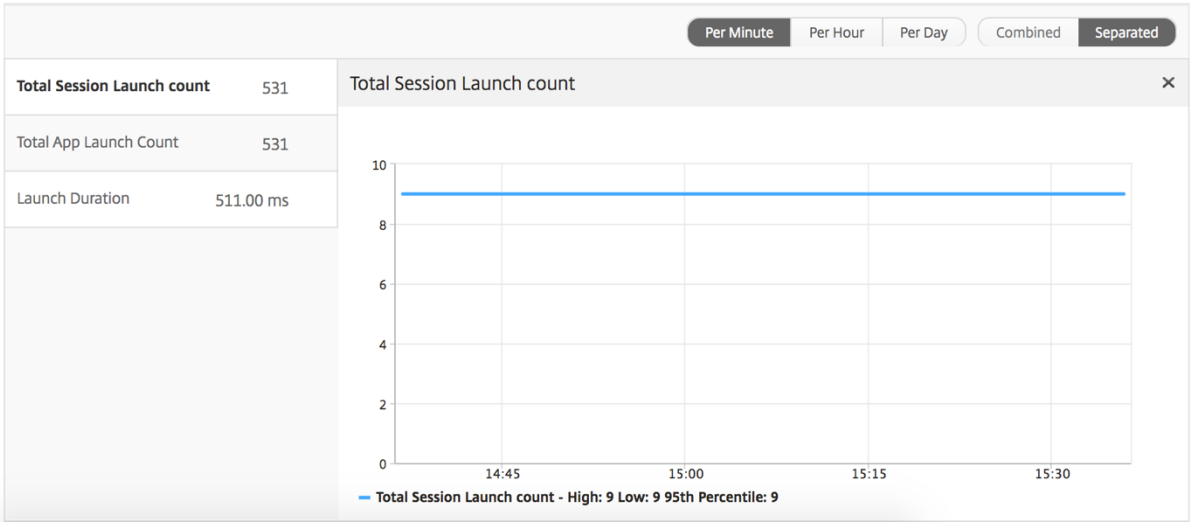
Métricas	Descripción
Nombre	Nombre de la aplicación virtual Citrix.
State	Muestra el estado de la aplicación: Verde-Activa, Rojo-Inactiva
N.º de sesiones activas	Número de sesiones de usuario activas que utilizan esta aplicación durante un intervalo de tiempo determinado.
Aplicaciones #Active	Número de sesiones activas para esta aplicación.



Informe Umbral El informe de umbrales representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Aplicación 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.



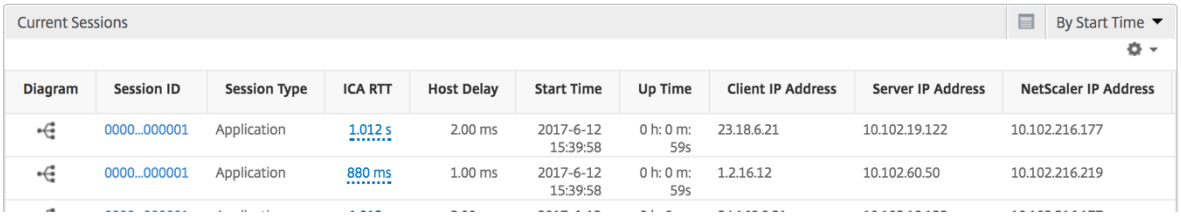
Informe sobre sesiones actuales

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 NetScalers 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.

Métricas	Descripción
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 espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
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.
RTT de ICA	El RTT de ICA es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps o Desktops, respectivamente.

Métricas	Descripción
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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 y el servidor back-end.
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 ha producido 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 aplicación virtual de Citrix 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.
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.

Métricas	Descripción
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 el caso de que los dispositivos que no son Citrix estén presentes 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 el caso de que los dispositivos que no son Citrix estén presentes 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. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Gateway > 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, desde NetScaler hasta el 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 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 back-end.
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 ha producido 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.

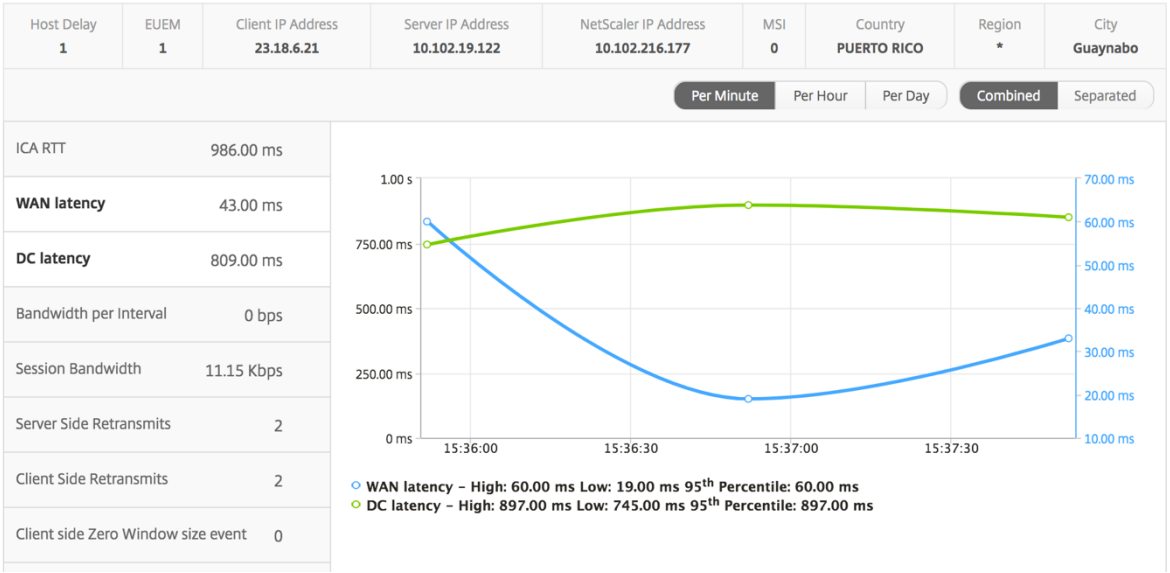
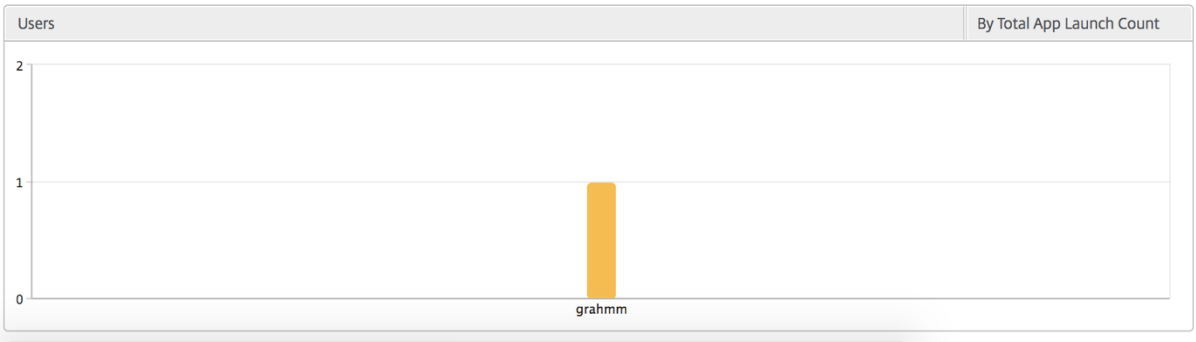


Gráfico de barras de usuario El gráfico de barras del usuario representa a los usuarios que han iniciado sesión en esta aplicación en particular.



Informes y métricas de vista de escritorio

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 **Gateway > HDX Insight > Escritorio** .

Vista de resumen

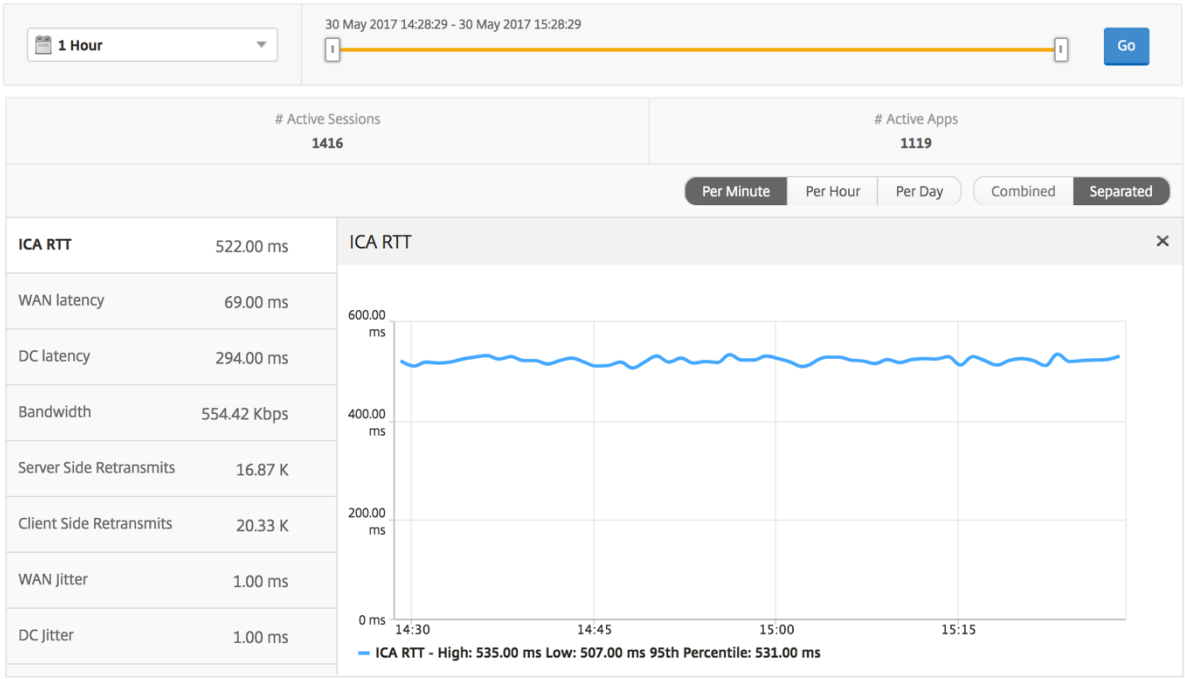
La vista de resumen muestra los informes de todos los Citrix Virtual Desktops que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas/informes, a menos que se mencione 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, desde NetScaler 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 y el servidor back-end.
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 ha producido 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.

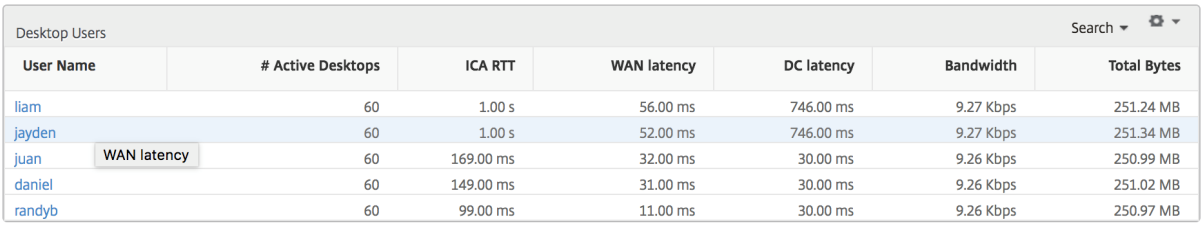
Métricas	Descripción
Evento de ventana cero en el lado del servidor	Este contador indica el número de veces que el servidor anunció una ventana TCP cero.



Informe de resumen de escritorio

Métricas	Descripción
Sesiones activas	Número total de sesiones activas de Citrix Virtual Desktop 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 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.

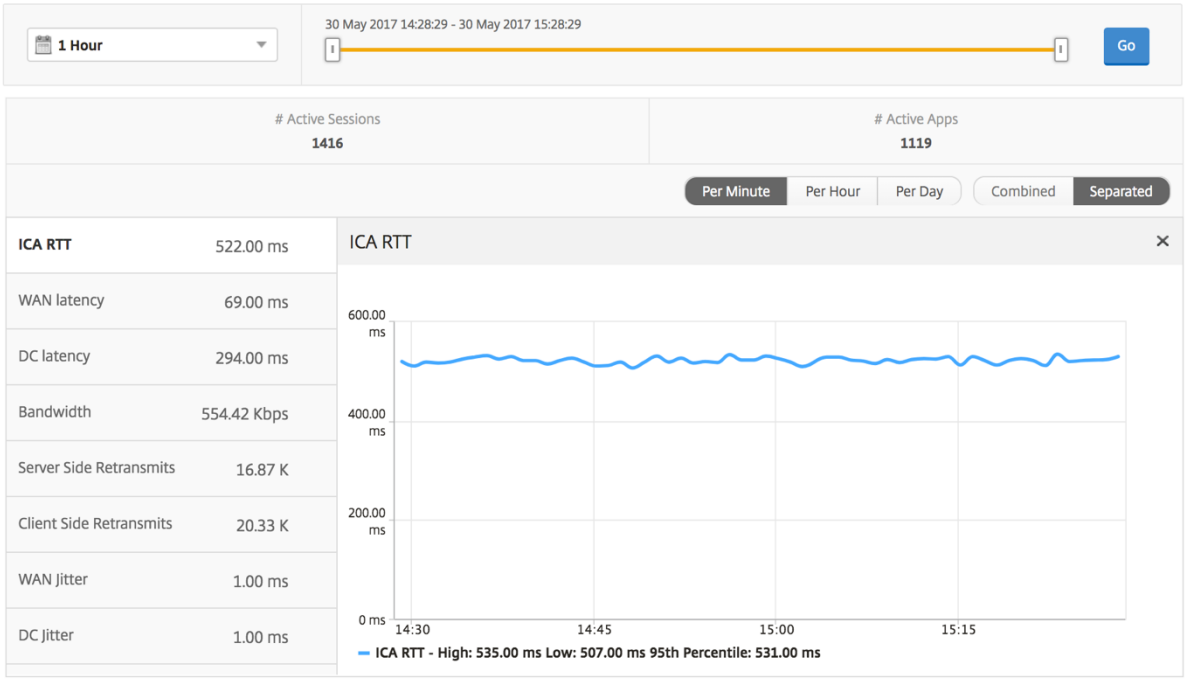
Para navegar a la vista Escritorio en particular:

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

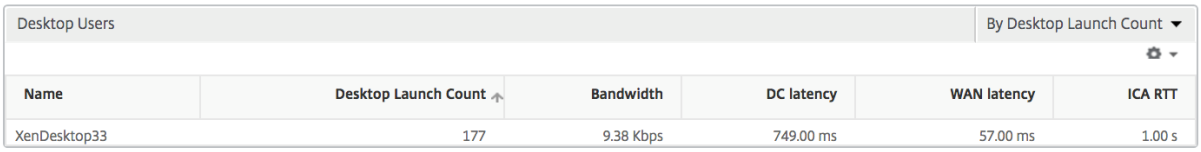
Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.

Métricas	Descripción
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual 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 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 y el servidor back-end.
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 ha producido 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 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 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.

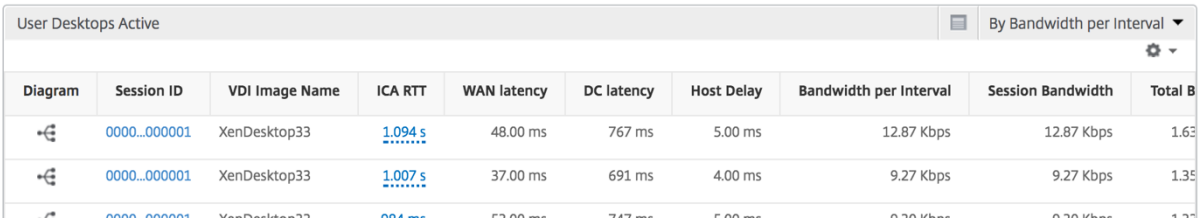


Informe de escritorios de usuario activos e inactivos Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

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 por los NetScalers 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 espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
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 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 y el servidor back-end.
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.

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.
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 ha producido 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	



Por vista de 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.

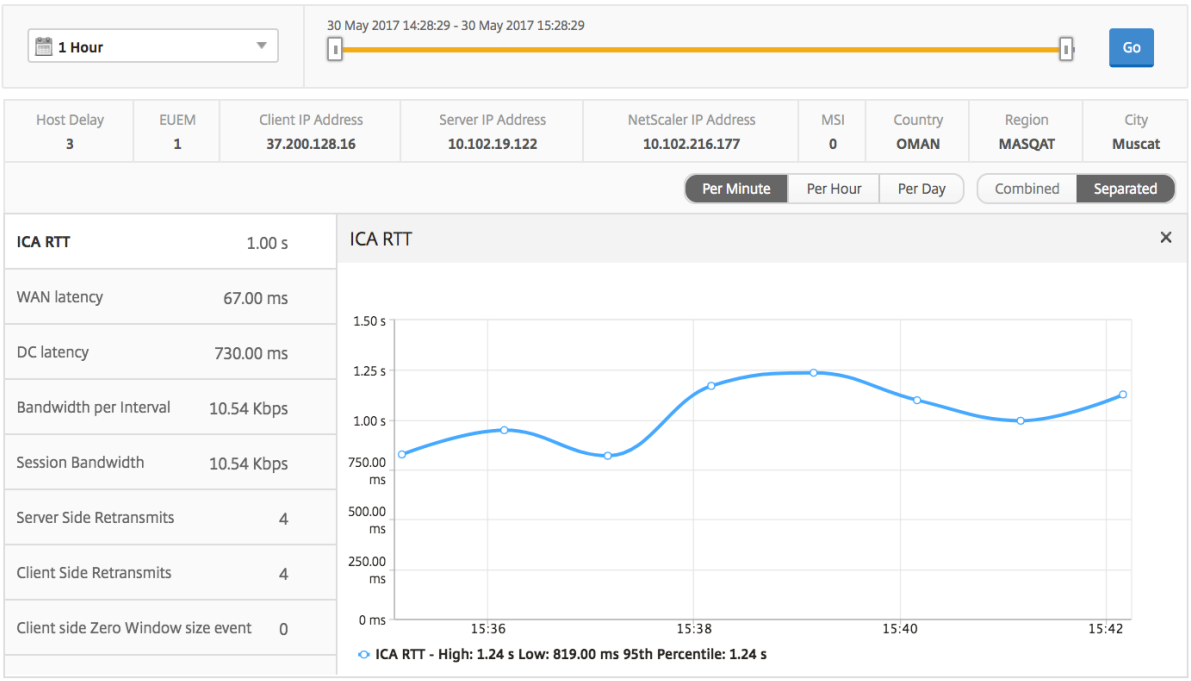
Para ver las métricas de la sesión de un usuario seleccionado:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.

2. Vaya a **Gateway > 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 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 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 y el servidor back-end.
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 ha producido 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.

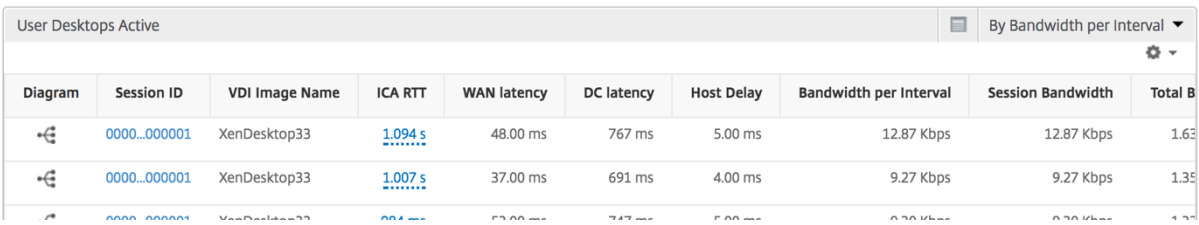


Informe de sesiones de escritorio relacionadas Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

Métricas	Descripción
ID de sesión	Una identidad única para una sesión ICA.
Tipo de sesión	Aplicación/escritorio.
State	Verde/rojo para las sesiones activas/inactivas.
Demora de host	Retraso promedio en el tráfico ICA que pasa por los NetScalers 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.

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 App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
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 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 y el servidor back-end.
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 ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.



Informes y métricas de vista de instancias

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 Insight > Instancias**.

Los informes y las métricas de vistas de instancias constan de las siguientes secciones:

- Vista resumida de la instancia
- Vista por instancia

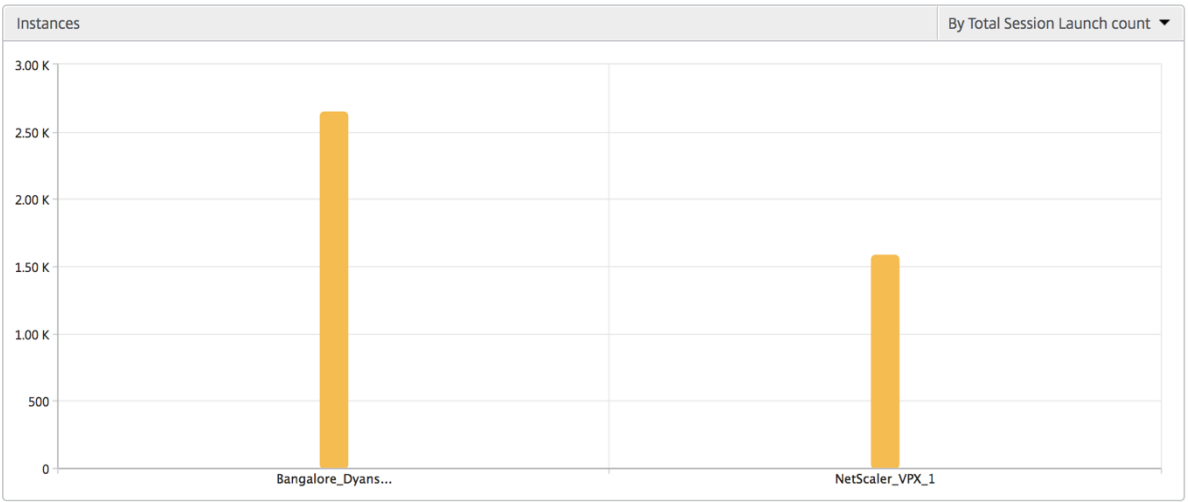
Vista de resumen de instancia

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.

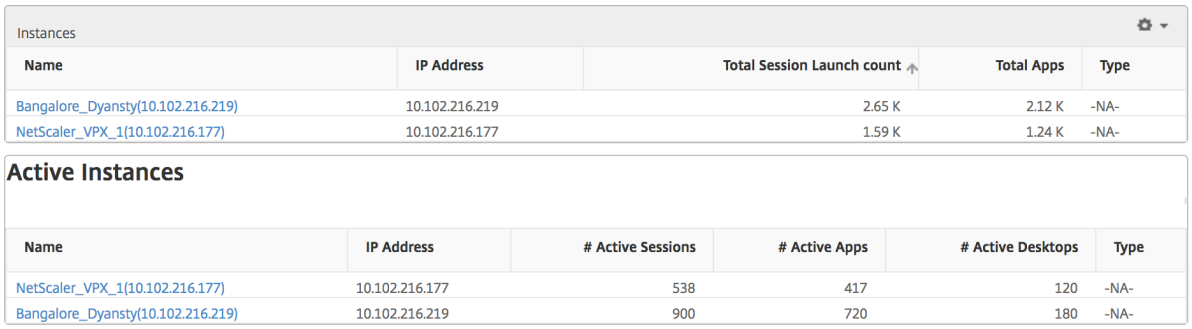
Gráfico de barras de instancia

Este gráfico muestra la instancia frente al recuento de inicio total de sesión	Total de aplicaciones que se pueden seleccionar de la lista en la parte superior derecha del lienzo gráfico.



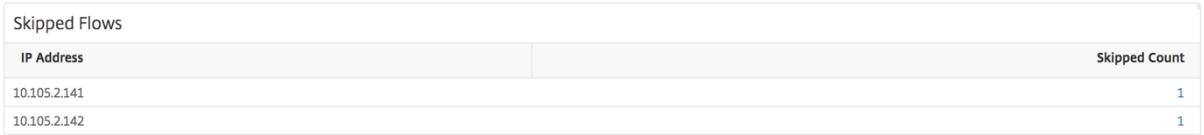
Informe de resumen de instancia/instancias activas

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, consulte cómo crear umbrales.

Flujos omitidos Un flujo omitido es un registro que omitió el análisis de la conexión ICA. Esto puede ocurrir por varios motivos, como el uso de versiones no compatibles de Citrix Virtual Apps and Desktops, una versión no compatible del espacio de trabajo o tipo de espacio de trabajo, etc. Esta tabla muestra la dirección IP y el recuento de flujos omitidos. Es posible que estos espacios de trabajo no formen parte de los espacios de trabajo de la lista de permitidos. Por lo tanto, estas sesiones se saltan de la supervisión.

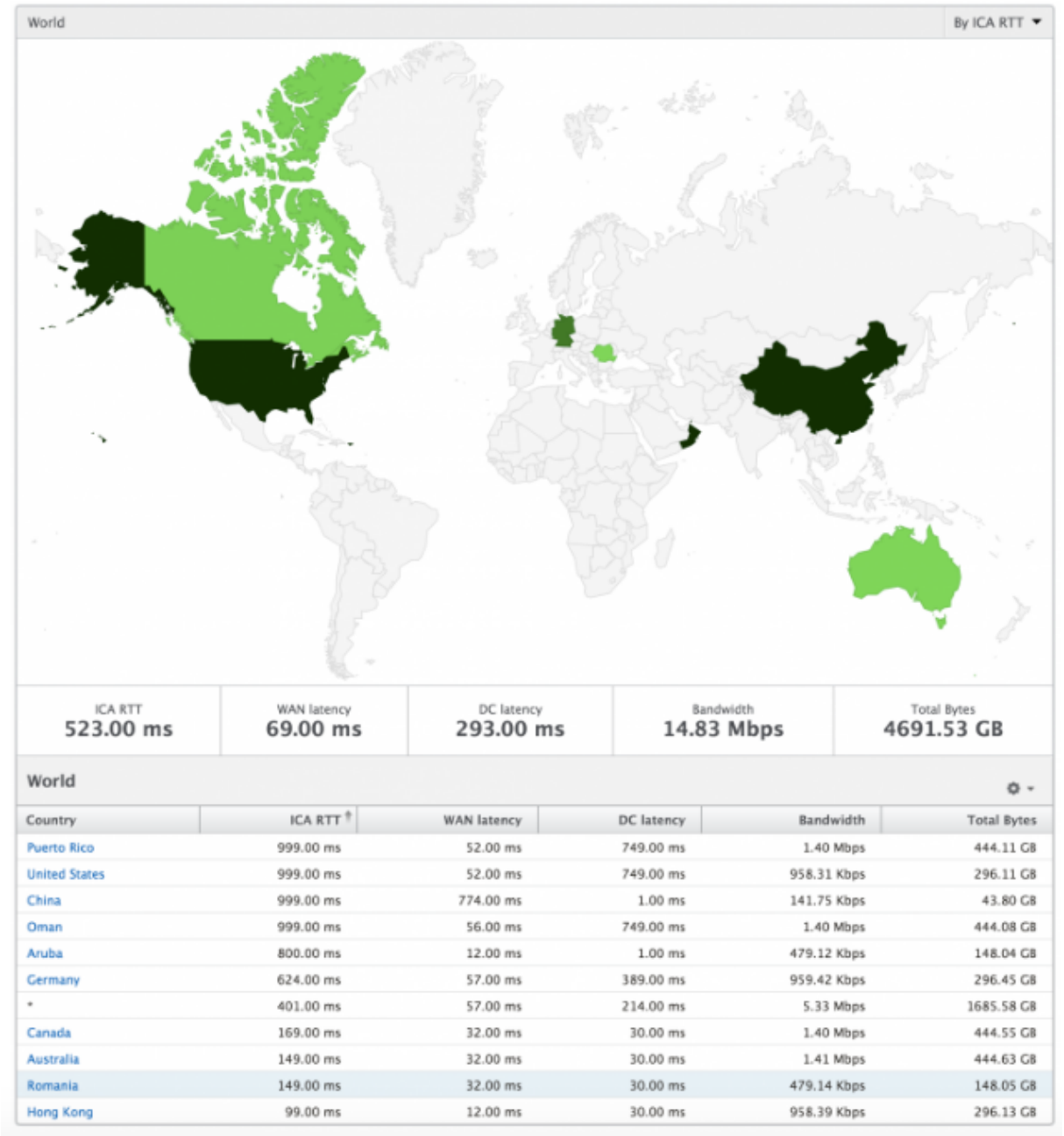


Visión del mundo La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores

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 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

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 de instancia:

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Instancias**.

3. Seleccione una instancia concreta en el **informe Resumen de Instancia**.

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 App durante el intervalo de tiempo dado.
Total de aplicaciones	Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado.

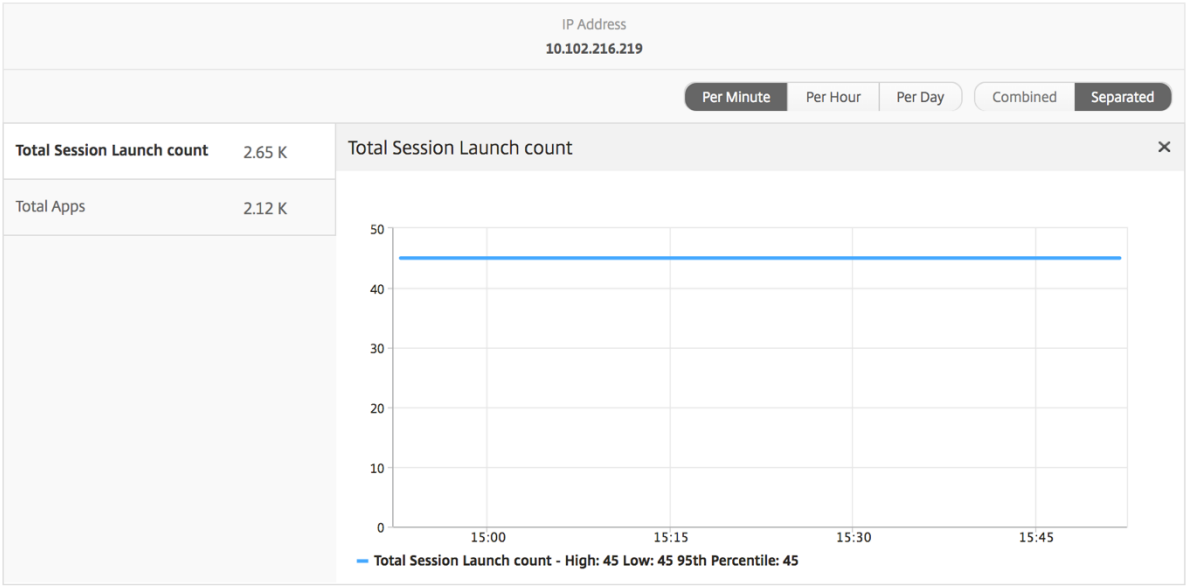


Gráfico de barras de aplicaciones Muestra las 5 aplicaciones principales según los siguientes criterios: por aplicaciones activas, recuento total de inicios de sesiones, recuento total de inicios de aplicaciones o duración del lanzamiento.

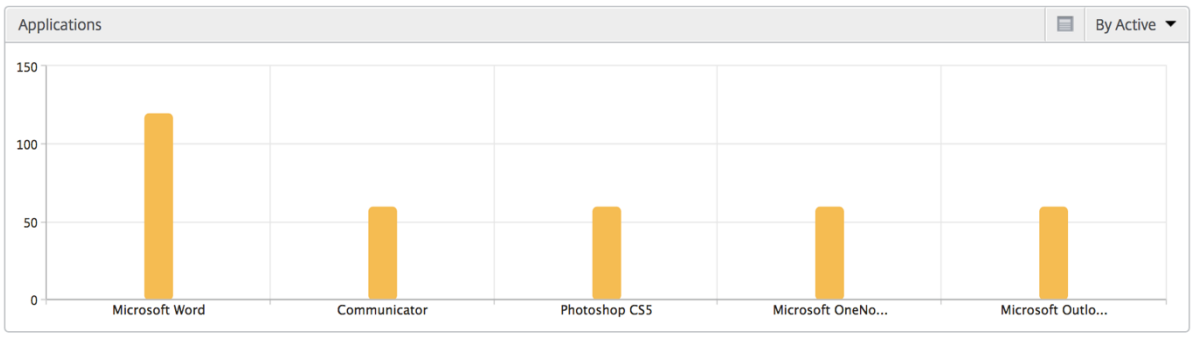
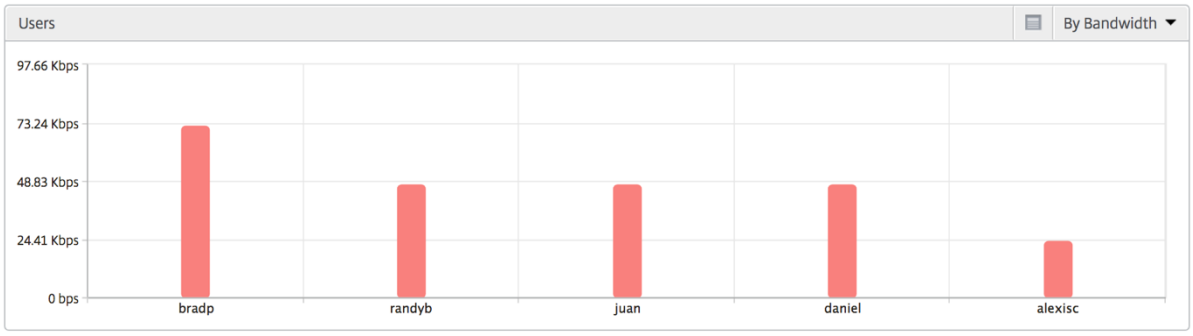


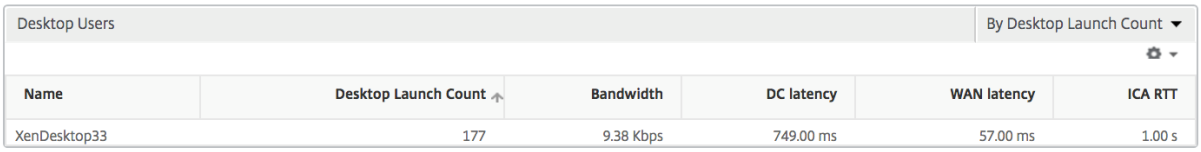
Gráfico de barras de usuarios El gráfico de barras Usuarios muestra los 5 usuarios principales en función de los siguientes criterios

- 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.

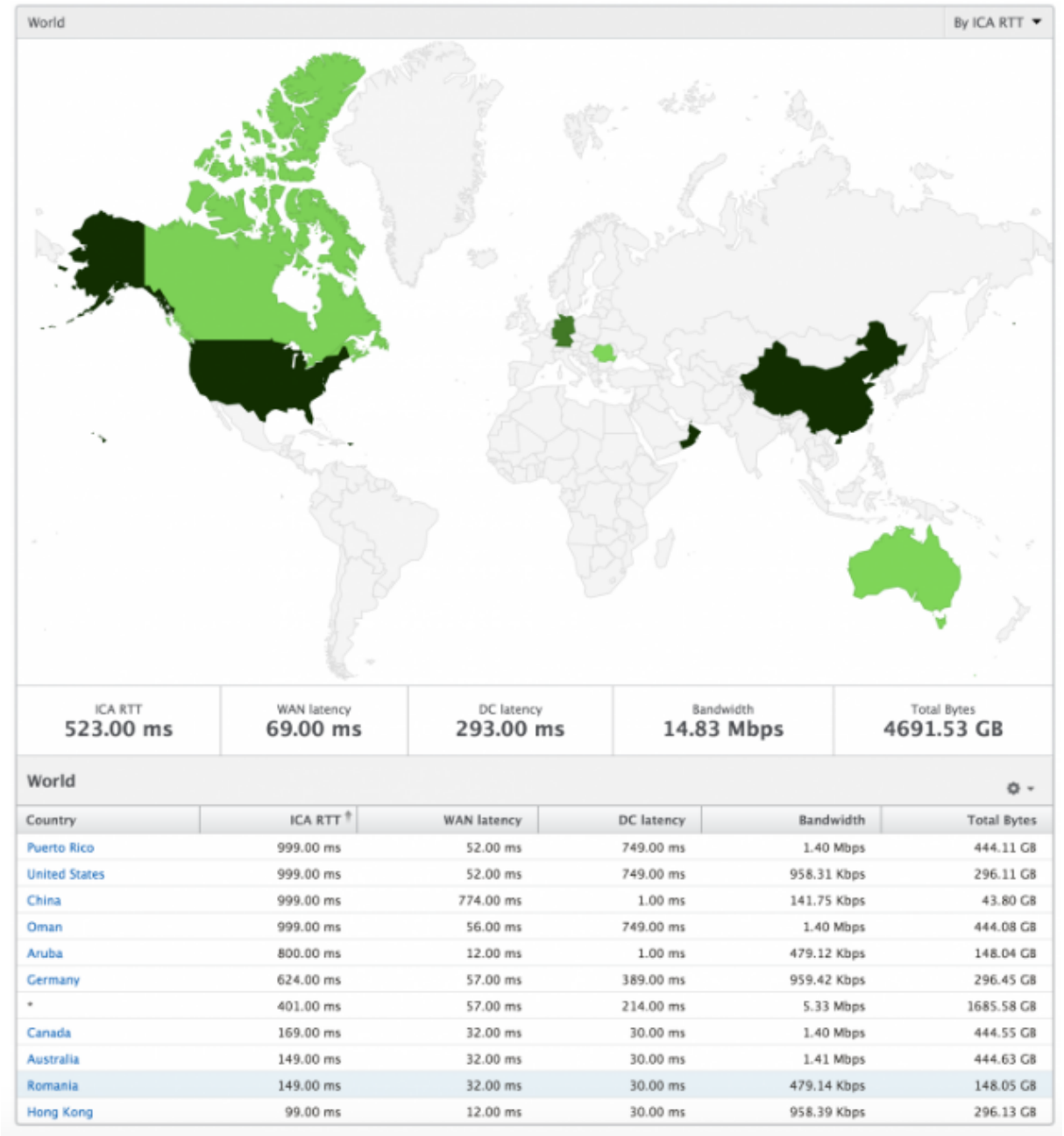
Métricas	Descripción
Nombre	Nombre del escritorio virtual de Citrix.
Recuento de lanzamientos	Número de veces que se ha iniciado el escritorio.
Ancho de banda	Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado.
Latencia de DC	Latencia 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 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 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 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 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



Informes y métricas de vista de licencias

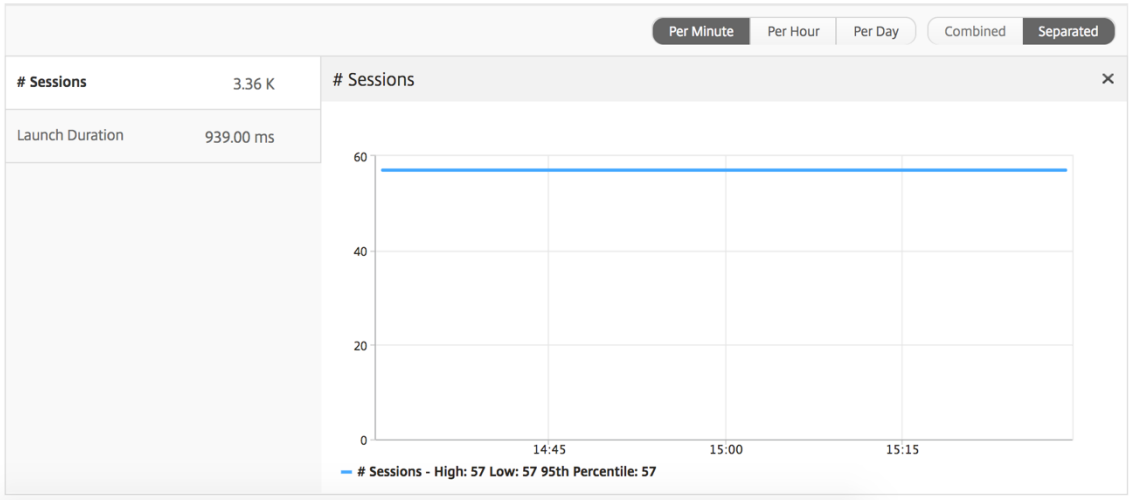
La vista de licencia proporciona detalles sobre la información de licencia de NetScaler Gateway.

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. Vaya a **Gateway > HDX Insight > Aplicaciones** .

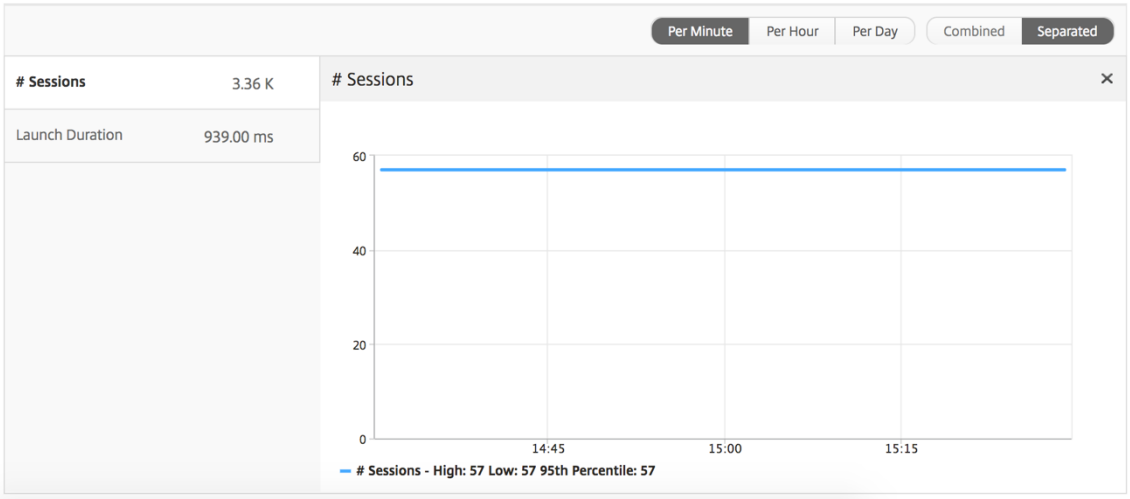
Vista de resumen

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

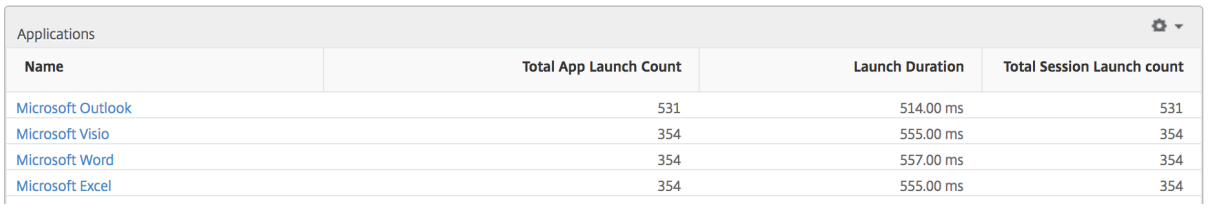
Métricas	Descripción
N.º de sesiones	Número total de sesiones durante un intervalo de tiempo determinado.
Duración de inicios	Promedio de tiempo necesario para iniciar una aplicación.



Informe resumido de las aplicaciones

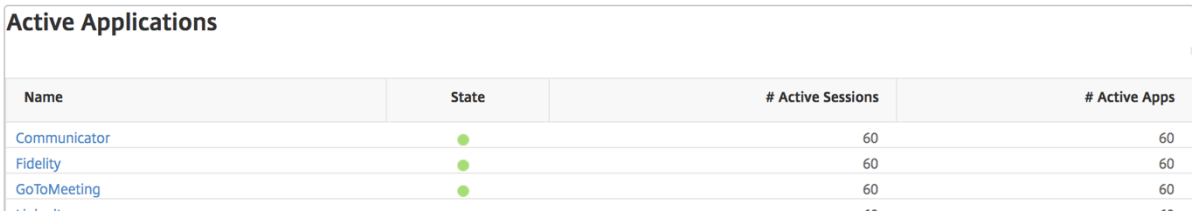
Métricas	Descripción
Nombre	Nombre de la aplicación virtual Citrix.
Recuento total de sesiones iniciadas	Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado.

Métricas	Descripción
Recuento total de aplicaciones iniciadas	Número total de aplicaciones de Citrix Virtual App lanzadas durante el intervalo de tiempo dado.
Duración de inicios	Tiempo promedio que se tarda en iniciar la aplicación virtual de Citrix.



Informe de aplicación activa

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.

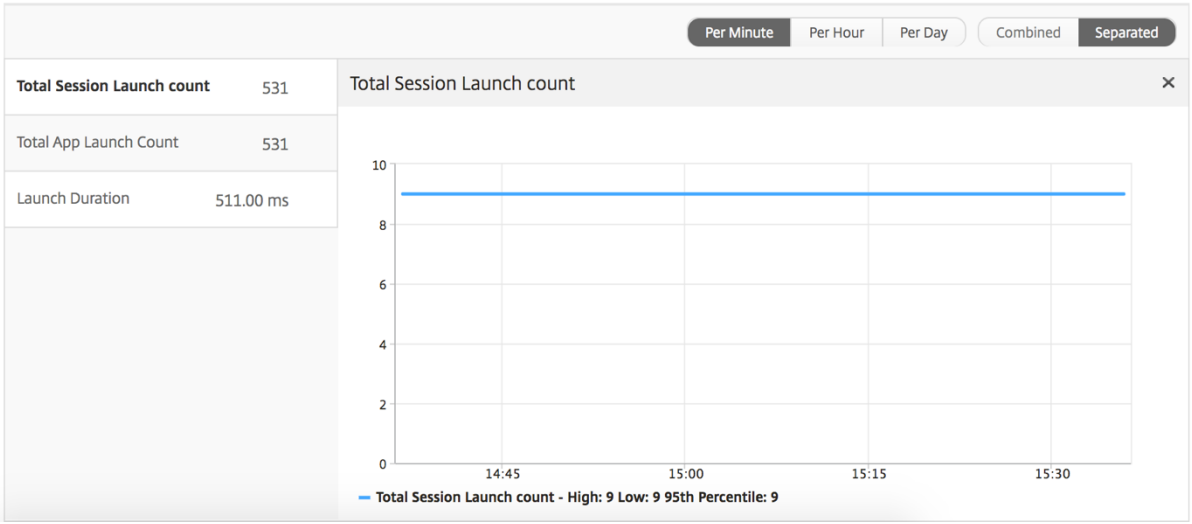


Informe Umbral

El informe de umbrales representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Aplicación 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.



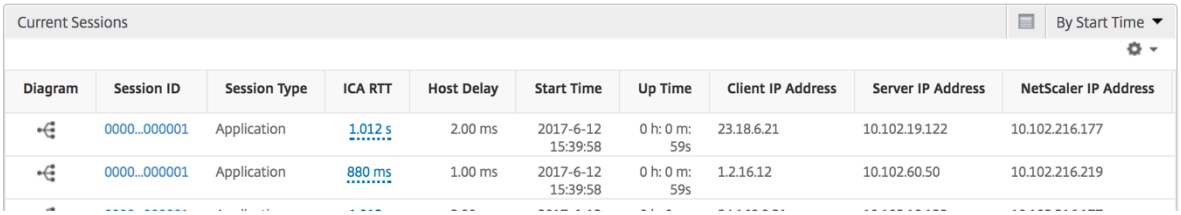
Informe sobre sesiones actuales

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 NetScalers 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.

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 App.
Dirección IP de NetScaler	IP de administración de NetScaler (NSIP).
Tipo de cliente	Tipo de espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
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 hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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 back-end.
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 ha producido 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 aplicación virtual de Citrix 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 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 y Citrix Virtual App. Esta métrica es útil en dispositivos que no son Citrix que están presentes 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 **Gateway > 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, desde NetScaler hasta el 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 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 back-end.
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 ha producido 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.

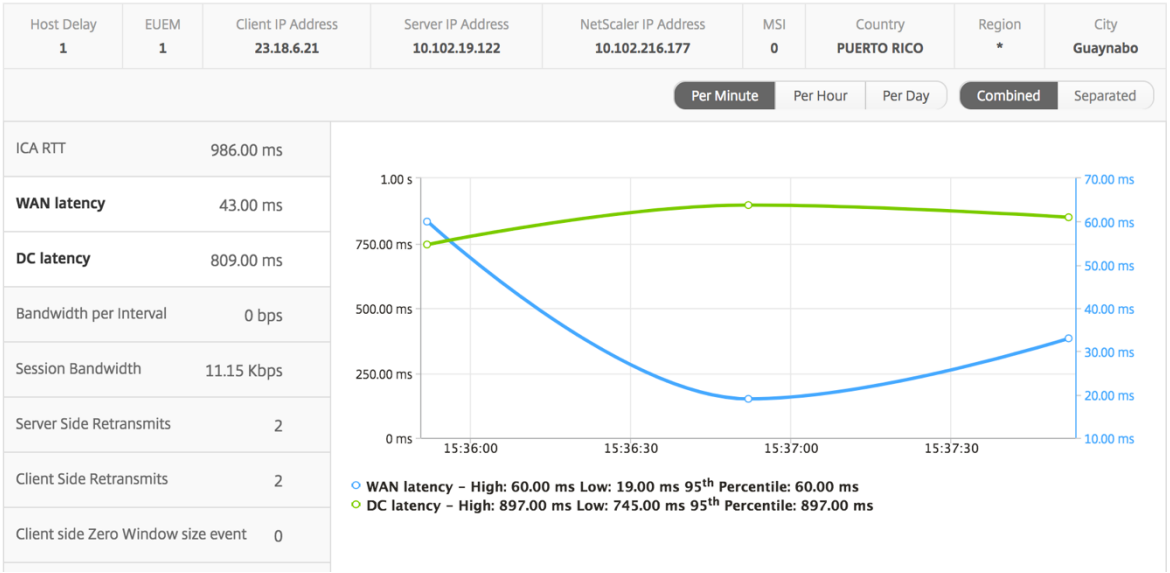
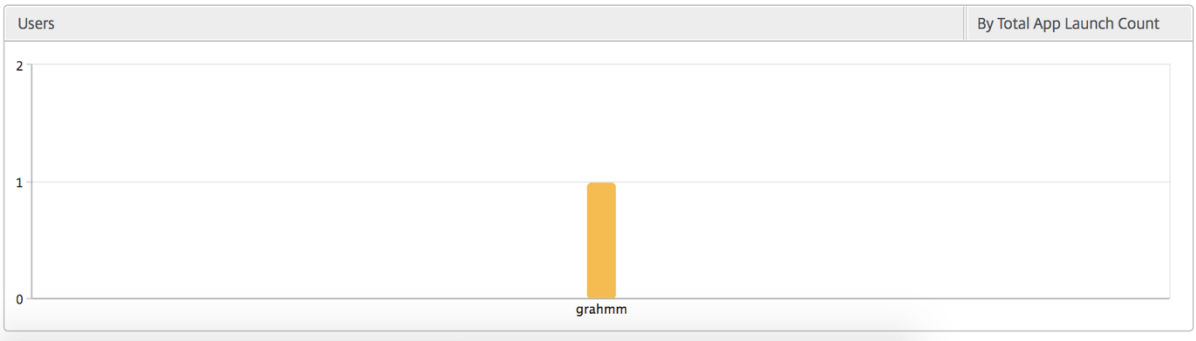


Gráfico de barras de usuario

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 Citrix Virtual Desktops.

Para desplazarse a la vista Escritorio:

1. Vaya a **Gateway > HDX Insight > Escritorio** .

Vista de resumen

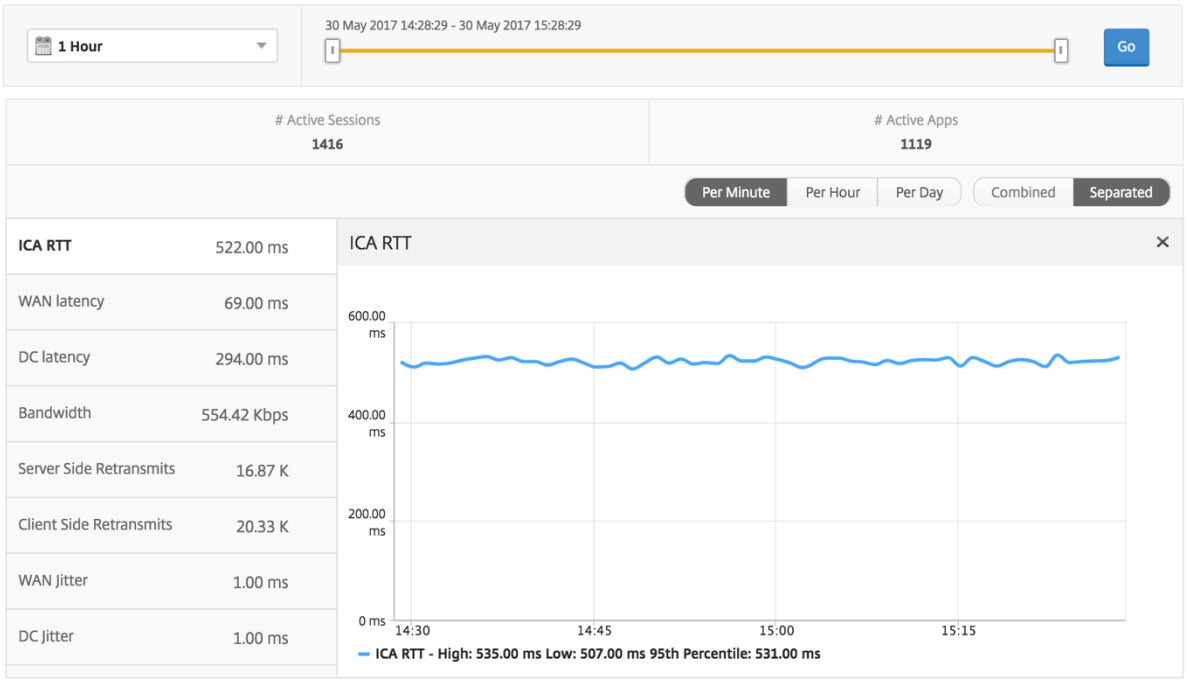
La vista de resumen muestra los informes de todos los Citrix Virtual Desktops que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas/informes, a menos que se mencione 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, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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 back-end.
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.

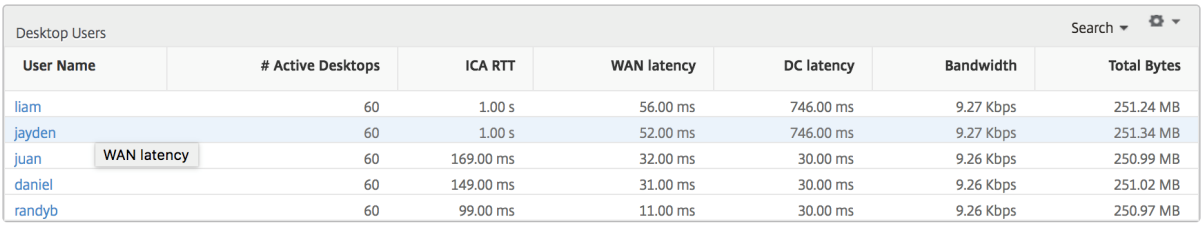
Métricas	Descripción
RTO rápido del lado del servidor	Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler y el servidor back-end.
Evento de ventana cero en el lado del cliente	Este contador indica el número de veces que el cliente anunció una ventana 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, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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.

Por vista de escritorio

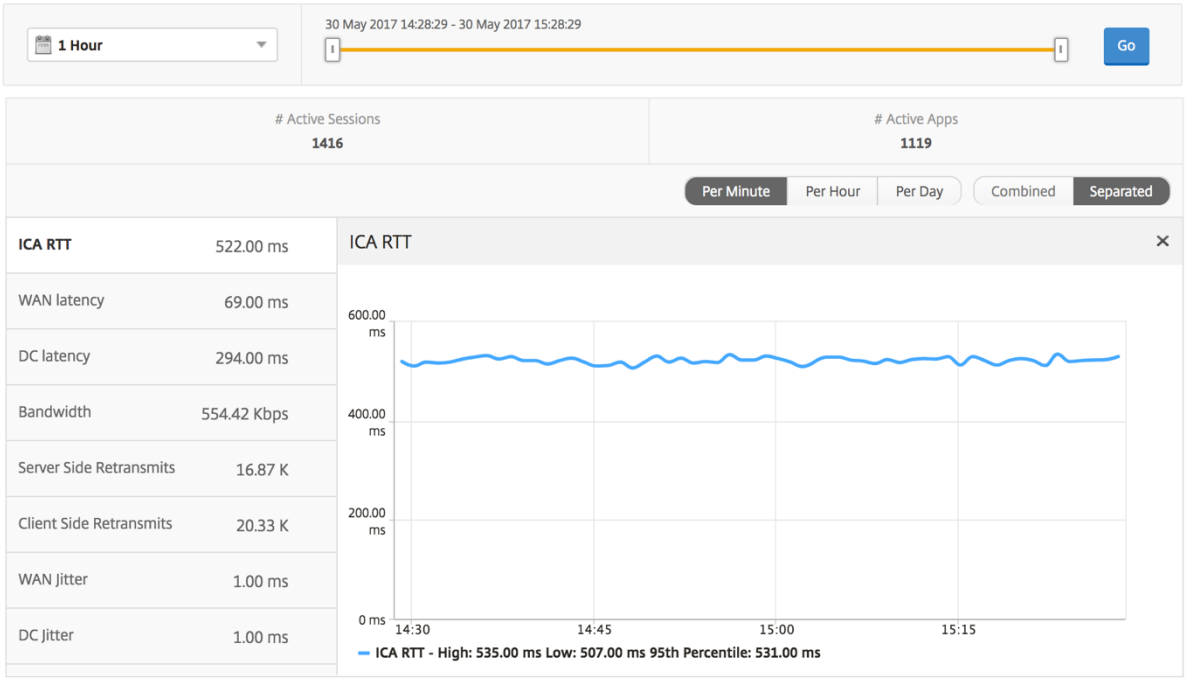
Por vista de escritorio proporciona informes detallados de la experiencia del usuario final para un escritorio virtual de Citrix seleccionado.

Para navegar a la vista Escritorio en particular:

1. Vaya a **Analytics > HDX Insight > Escritorio**.
2. Seleccione un **escritorio** concreto en el **informe de resumen de escritorios**.

Gráfico de líneas

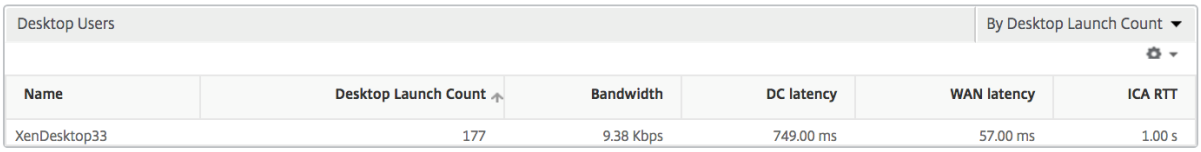
Métricas	Descripción
N.º de sesiones activas	Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops.
N.º de aplicaciones activas	Este número indica el recuento de sesiones activas de Citrix Virtual App.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario 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 hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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 back-end.
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 ha producido 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 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 servidores back-end.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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.



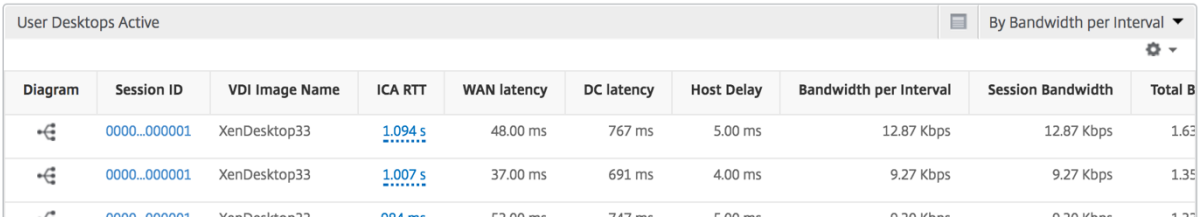
Informe de escritorios de usuario activos e inactivos

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 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 espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
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	El RTT de ICA es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps o Desktops, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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 back-end.

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 ha producido 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	



Por vista de 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 **Gateway > HDX Insight > Escritorio** .
2. Seleccione un escritorio concreto en el **informe de resumen de escritorios**.
3. Seleccione una sesión del informe de sesiones actuales.

Gráfico cronológico

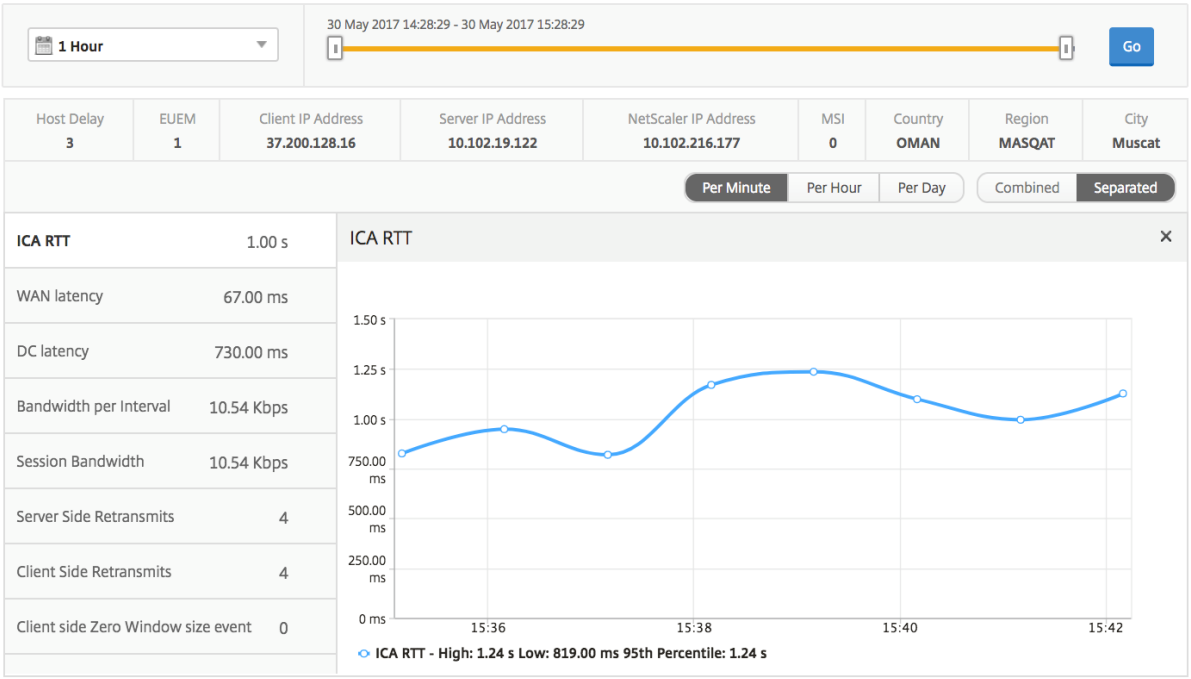
La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

Para ver las métricas de la sesión de un usuario seleccionado:

1. Vaya a **Gateway > 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 App and Desktop.
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 un escritorio alojados en Citrix Virtual App y Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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 back-end.
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 ha producido 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.



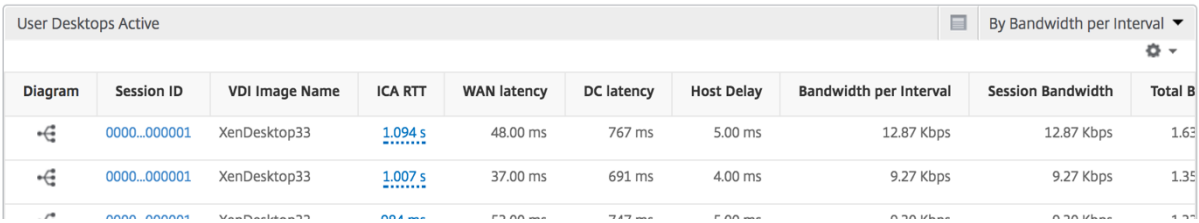
Informe de sesiones de escritorio relacionadas

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 NetScalers 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.
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 App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta 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 back-end.
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 ha producido 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



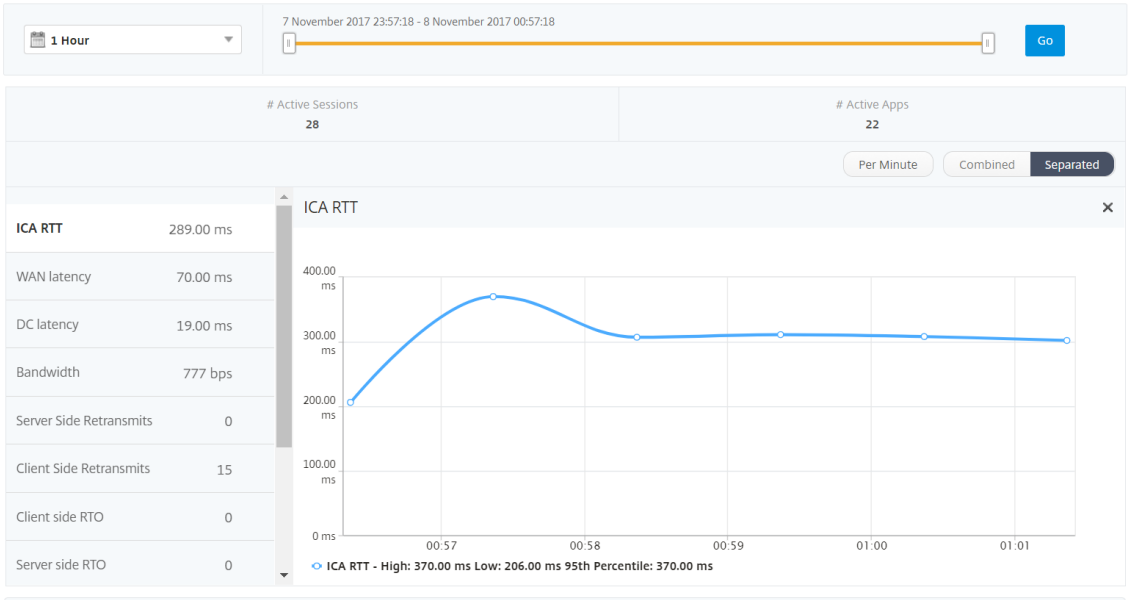
Informes y métricas de visualización de usuarios

January 30, 2024

Los informes y métricas de esta vista se muestran por usuarios de Citrix Virtual Apps y Desktop.

Para navegar a la vista Usuarios:

1. Vaya a **Gateway > 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 e 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:

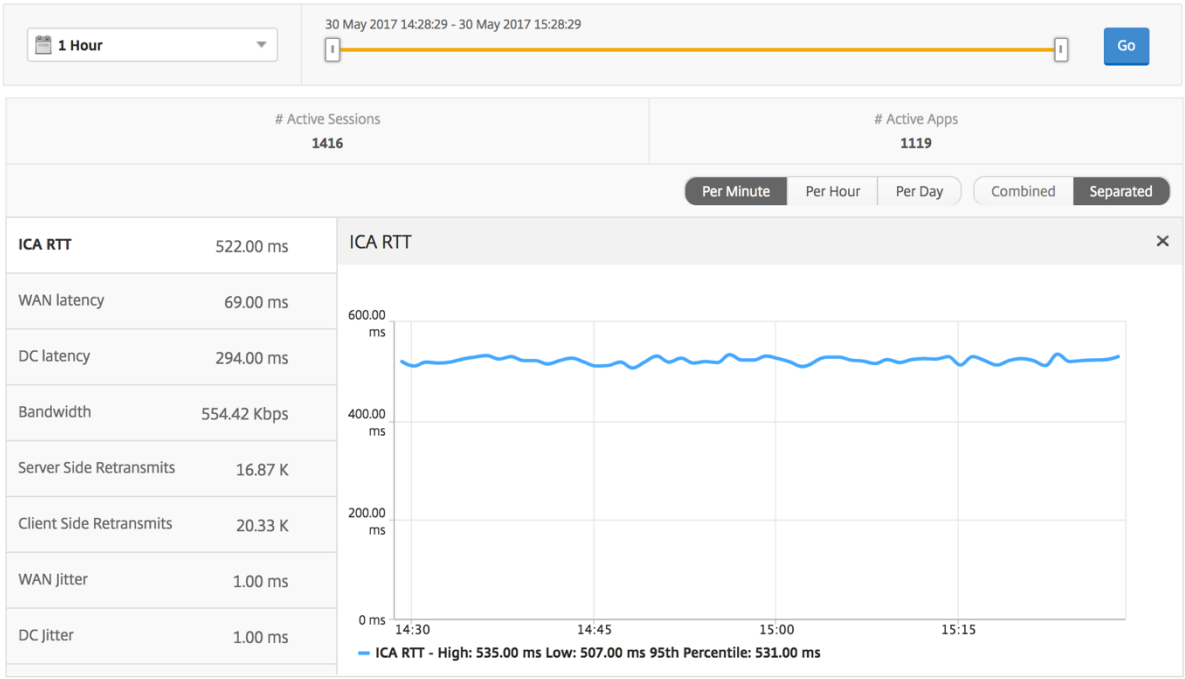
1. Utilice la lista de períodos de tiempo o el control deslizante de tiempo para establecer el intervalo de tiempo deseado.

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 App and Desktop.
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 App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta servidores de fondo.
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.

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 resumido 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 App and Desktop.
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 App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.

Métricas	Descripción
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta servidores de fondo.
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.
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.

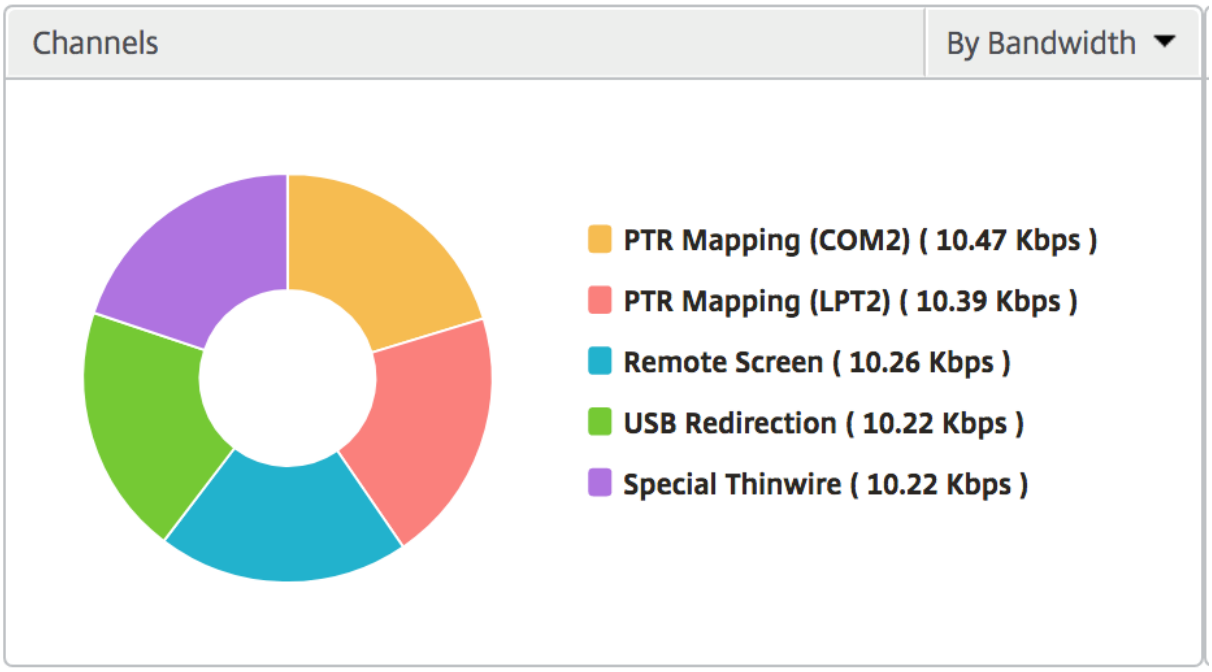
Users

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	

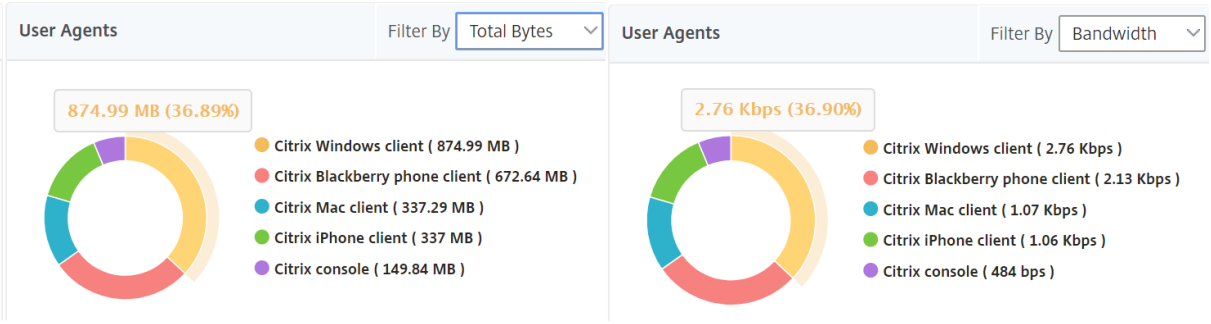
Canales

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 infracciones de umbrales

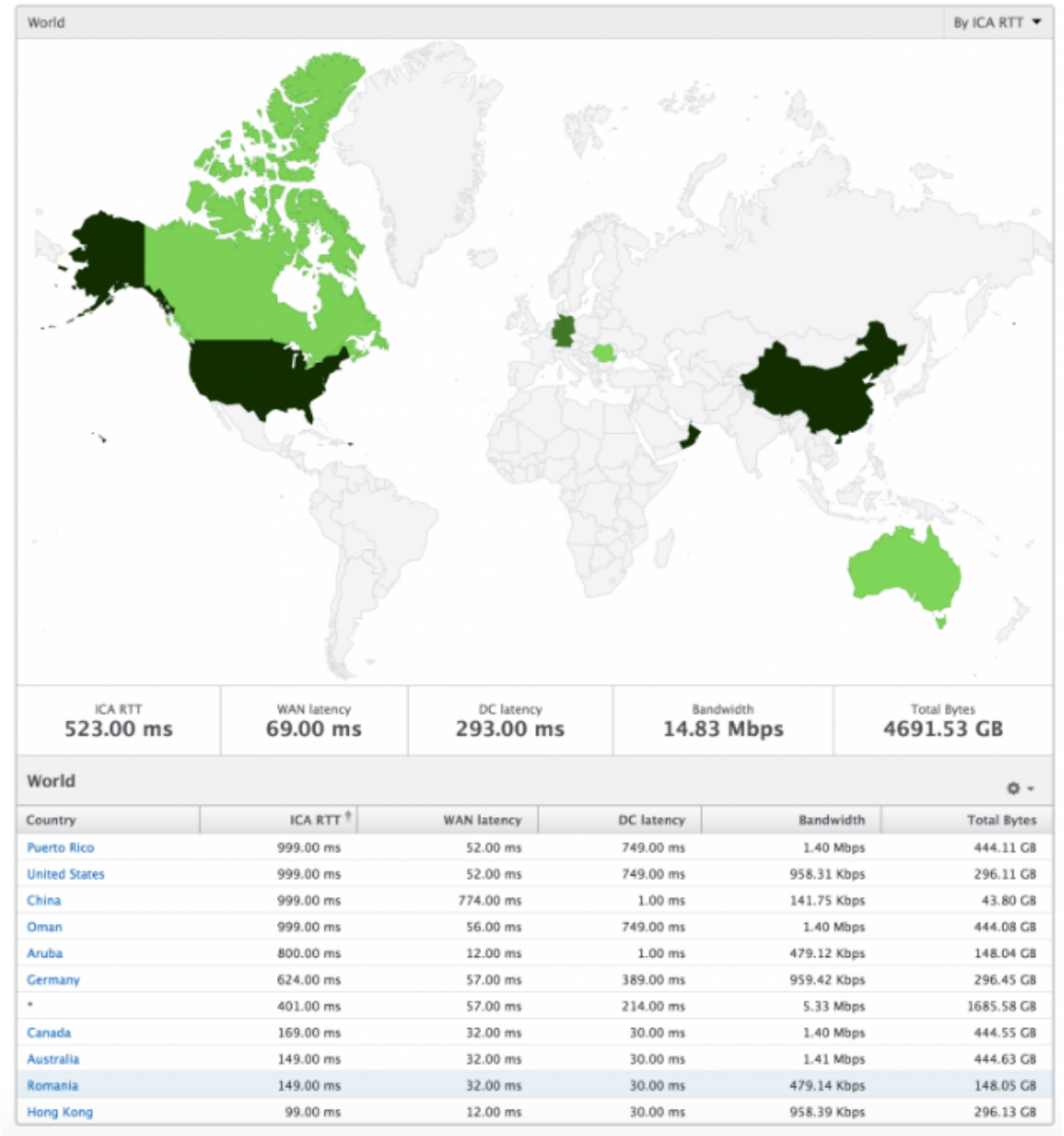
Las métricas de recuento de infracciones de Umbrales representan el recuento de umbrales incumplidos en el período de tiempo seleccionado. Para obtener más información, consulta cómo crear umbrales y alertas.

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 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 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 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. Vaya a **Gateway > 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 espacio de trabajo: Citrix Windows Client, etc.
Versión del cliente	Versión Workspace.
MSI	Booleano (sí/no). Indica si la sesión es ICA multisecuencia.
Reconexiones de sesión	Número de veces que se volvió a conectar la sesión.

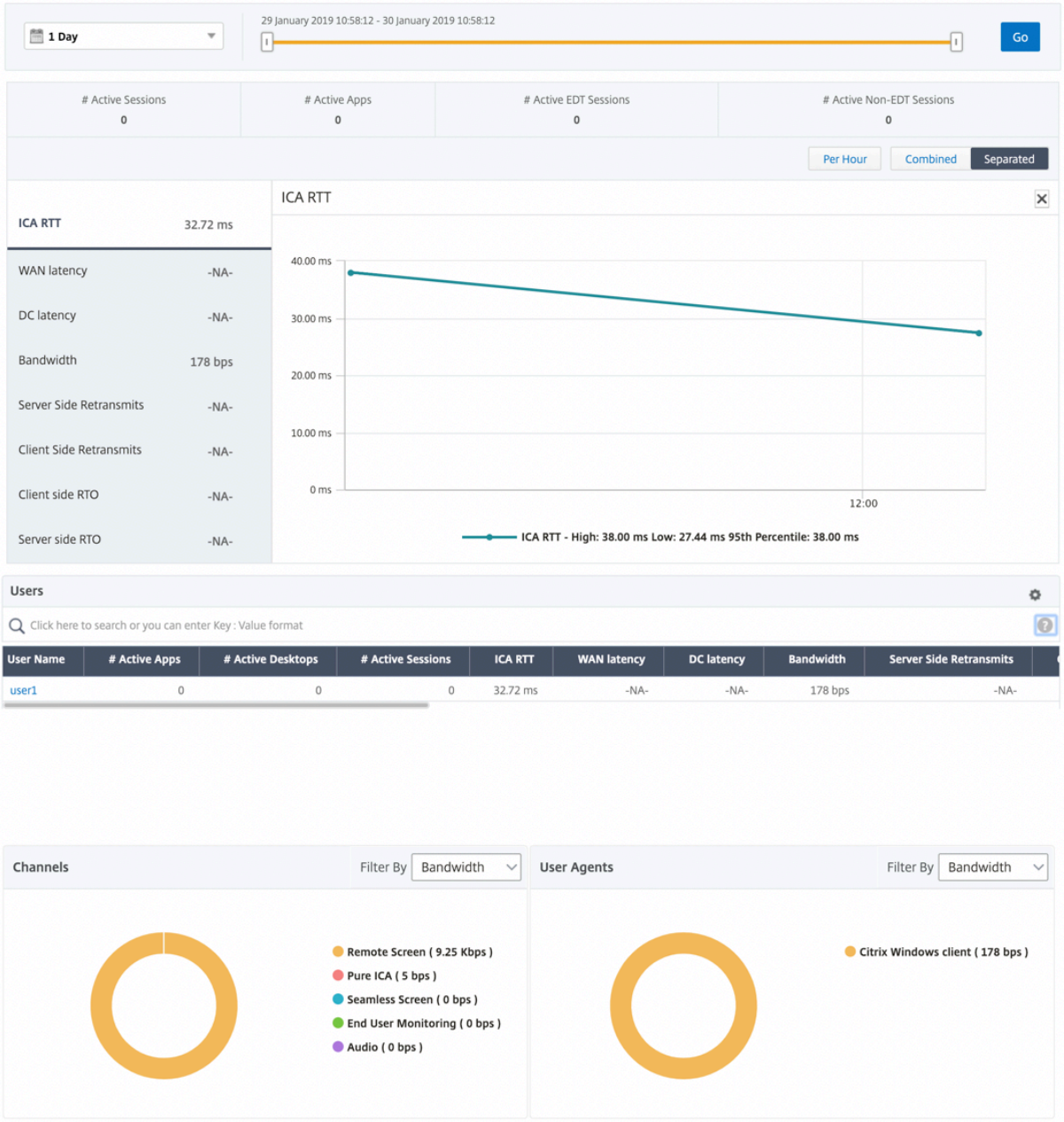
Métricas	Descripción
Recuento de ACR	Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas.
Tipo de acceso de usuario	Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway.
País	País desde el que 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 App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta servidores de fondo.
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.

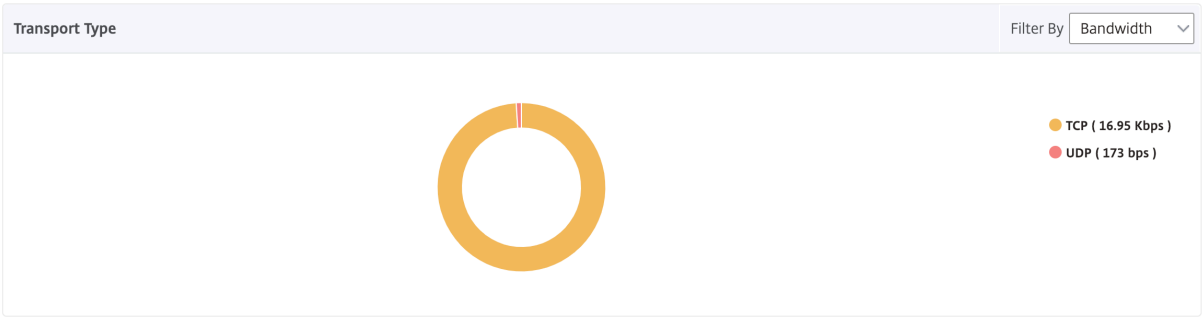
Soporte para EDT en HDX insights

NetScaler Application Delivery Management (ADM) ahora admite el transporte de datos avanzado (EDT) para mostrar los análisis de 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 Workspace.

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 y los RTO. Algunas de estas métricas no están disponibles para los usuarios que sí tienen sesiones de EDT, ya que actualmente se calculan a partir de la pila de TCP. Por lo tanto, aparecen como "NA".

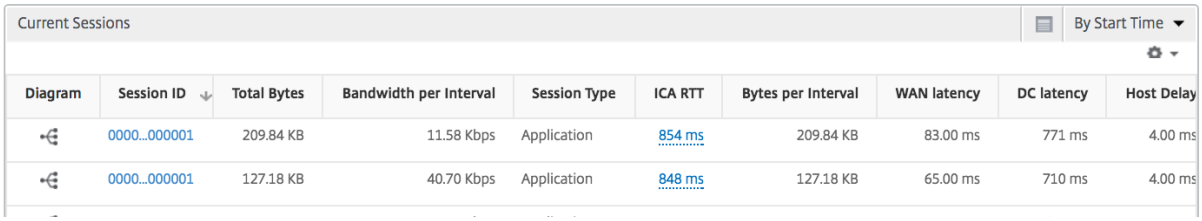


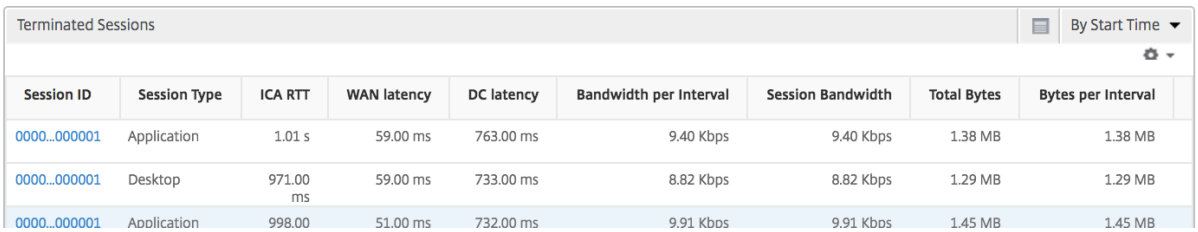
Se ha introducido un nuevo gráfico de donut para permitirle ver el ancho de banda consumido por el usuario y también el número total de bytes según el tipo de protocolo utilizado por los usuarios.



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 el caso de que los dispositivos que no son Citrix estén presentes 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 el caso de que los dispositivos que no son Citrix estén 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.

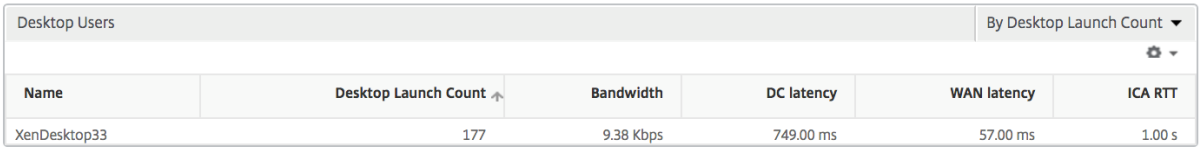




Usuarios de escritorio

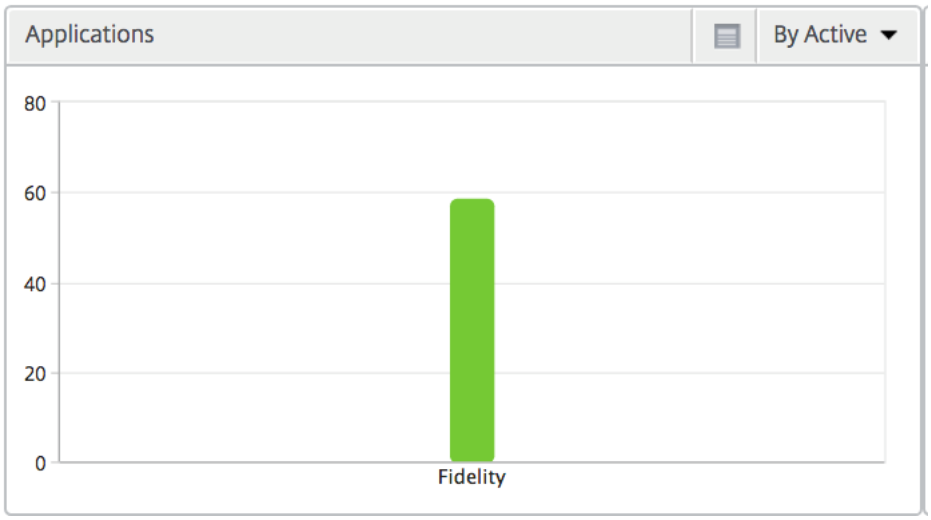
Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

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, desde NetScaler hasta servidores de fondo.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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 App o Desktop, respectivamente.



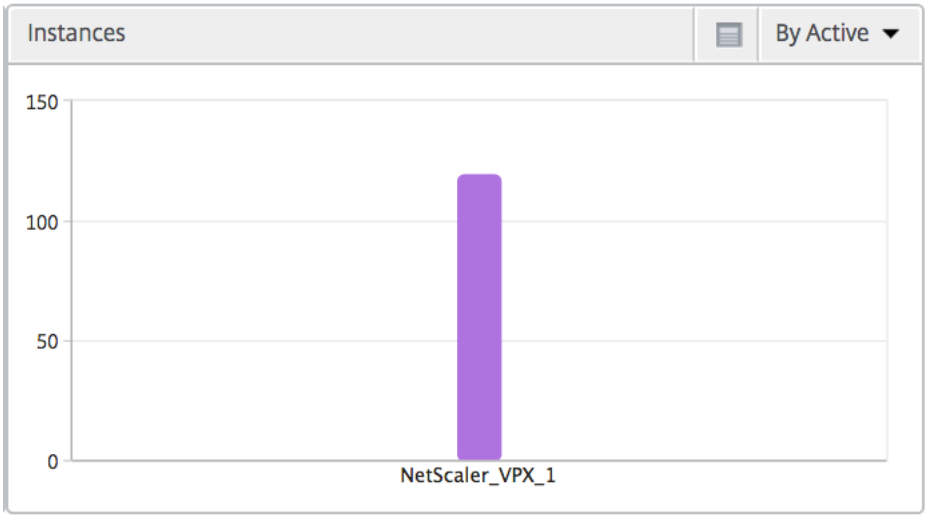
Aplicaciones

Gráfico de barras que representa las aplicaciones ordenadas por Activo, recuento total de inicio de sesión, recuento total de inicio de aplicaciones y duración del lanzamiento.



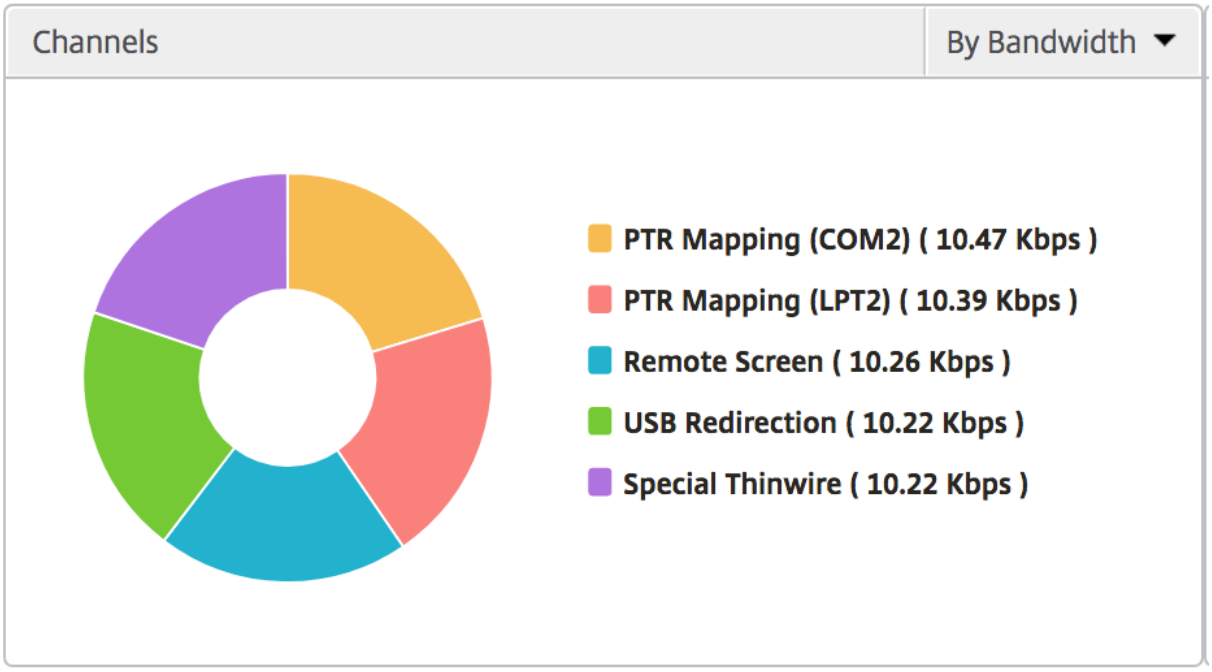
Instancias

Un gráfico de barras que representa las instancias de NetScaler ordenadas por aplicaciones activas y totales



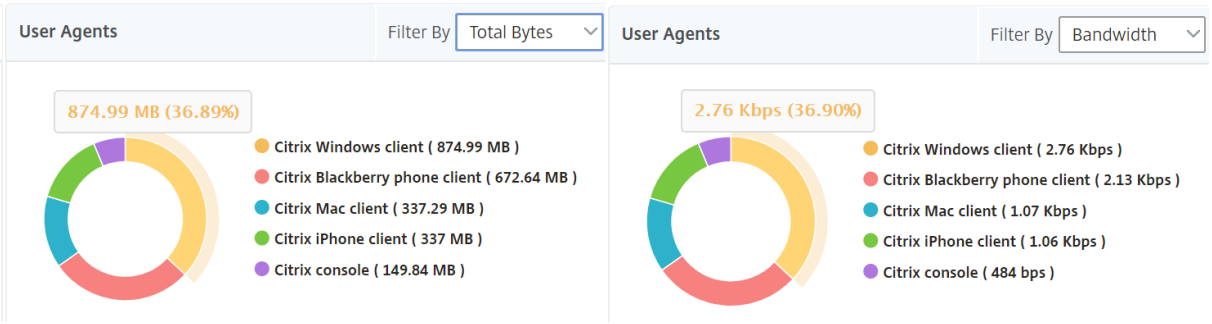
Canales

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:

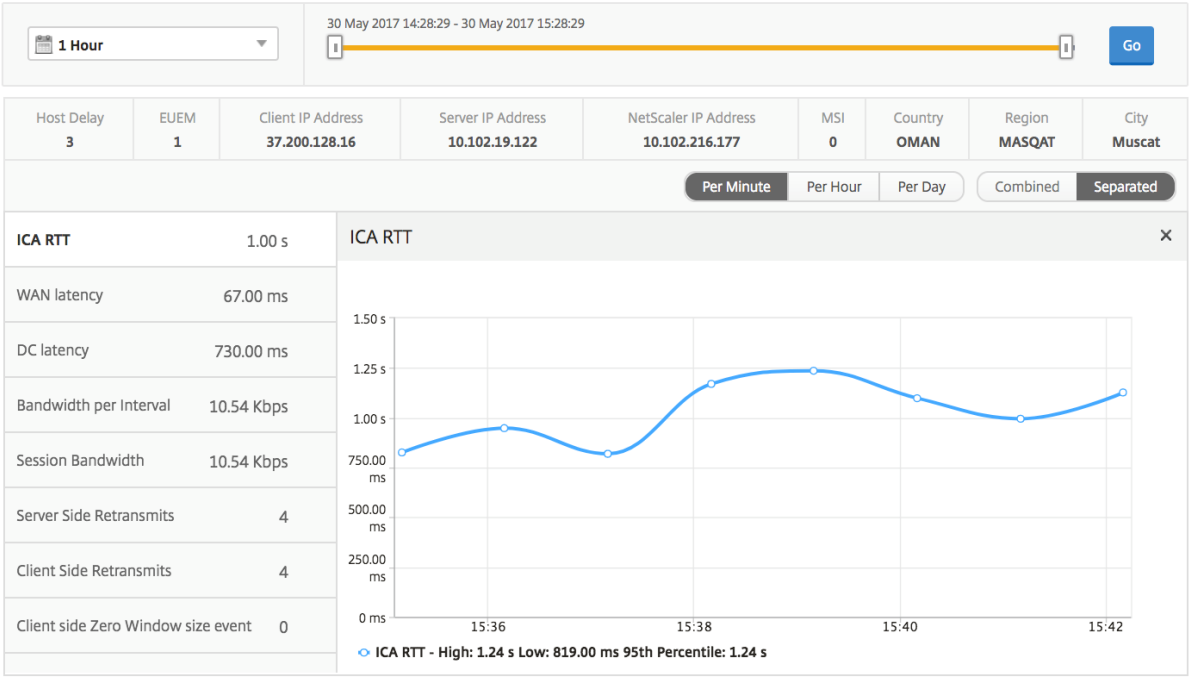
1. Vaya a **Gateway > HDX Insight > Usuarios** .
2. Select un usuario concreto en la sección **Informe de resumen de usuario**.

3. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

Gráfico cronológico

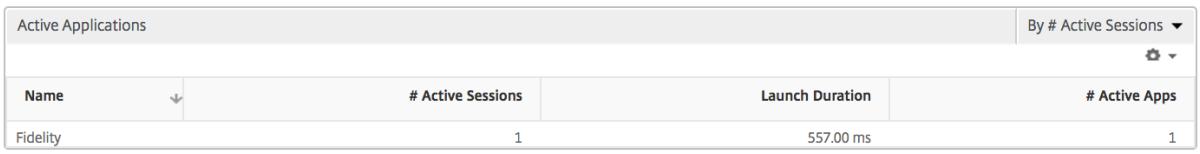
Métricas	Descripción
Reconexiones de sesión	Este número indica el recuento de sesiones activas de Citrix Virtual App and Desktop.
Recuento de ACR	Este número indica el recuento de sesiones activas de Citrix Virtual App.
RTT de ICA	ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler hasta el usuario final.
Latencia de DC	Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler hasta servidores de fondo.
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.



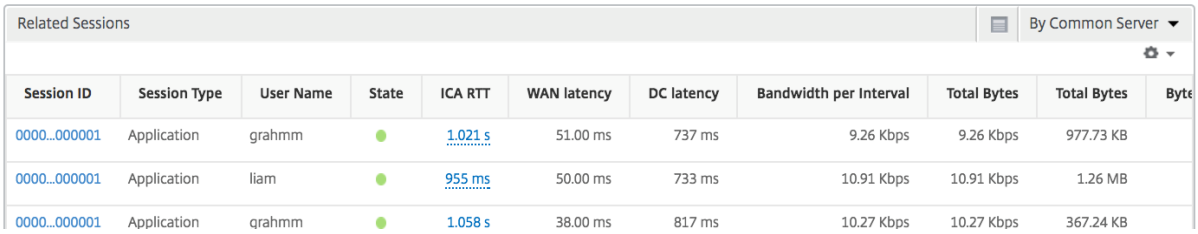
Aplicación activa

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 de instancia:

1. Vaya a **Gateway > HDX Insight > Instancias** .

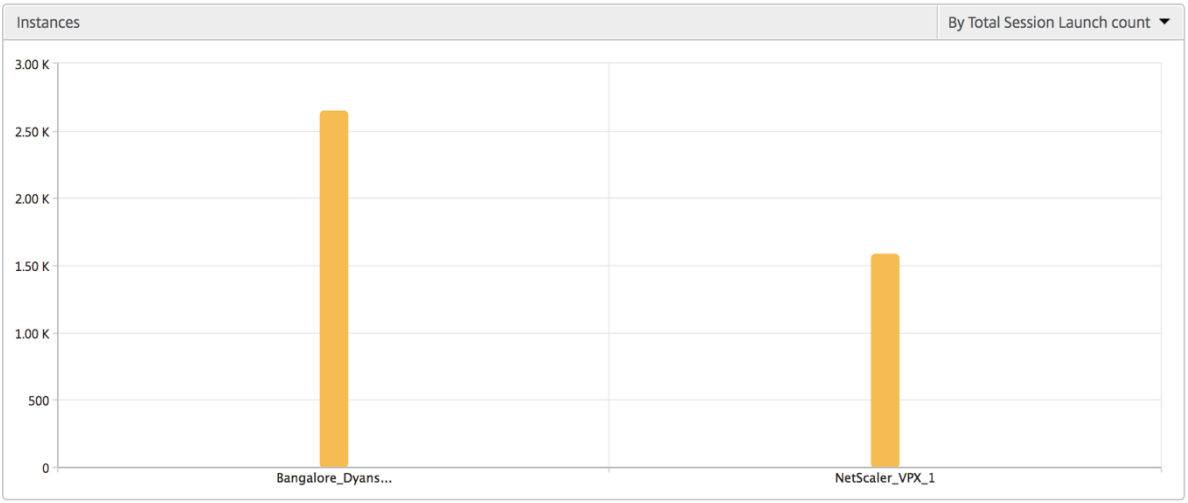
Vista de resumen de instancia

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 menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

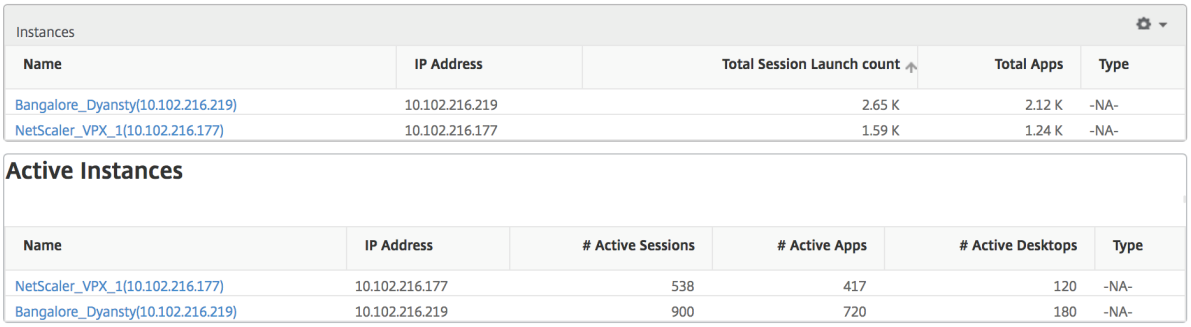
Gráfico de barras de instancia

Este gráfico muestra la instancia frente al recuento total de inicio de sesión y Total de aplicaciones que se pueden seleccionar de la lista en la parte superior derecha del lienzo del gráfico.



Informe de resumen de instancia/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


Instances

Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

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 ocurrir por varios motivos, como el uso de versiones no compatibles de Citrix Virtual Apps and Desktops, una versión no compatible del espacio de trabajo o tipo de espacio de trabajo, etc. Esta tabla muestra la dirección IP y el recuento de flujo omitido. Es posible que estos espacios de trabajo no formen parte de los espacios de trabajo de la lista de permitidos. Por lo tanto, estas sesiones se saltan de la supervisión.

¡Ver **error! La referencia de hipervínculo no es válida** para obtener más detalles sobre problemas relacionados con el análisis ICA.


Skipped Flows

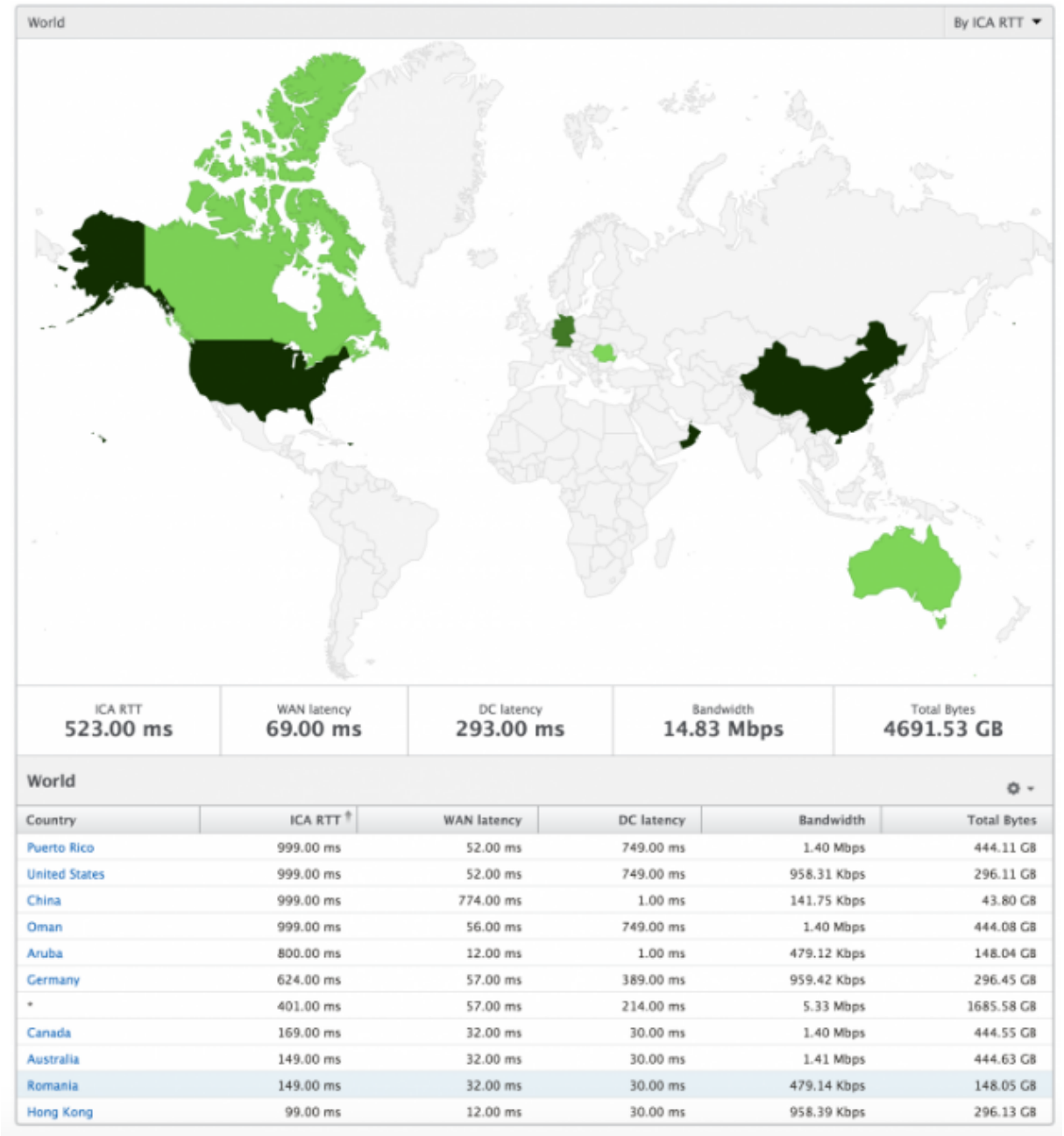
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

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 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 versión 12.0 y posterior, puede profundizar en 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

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 de instancia:

1. Vaya a **Gateway > HDX Insight > Instancias** .
2. Seleccione una instancia concreta en el **informe Resumen de Instancia**.

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 App durante el intervalo de tiempo dado.
Total de aplicaciones	Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado.

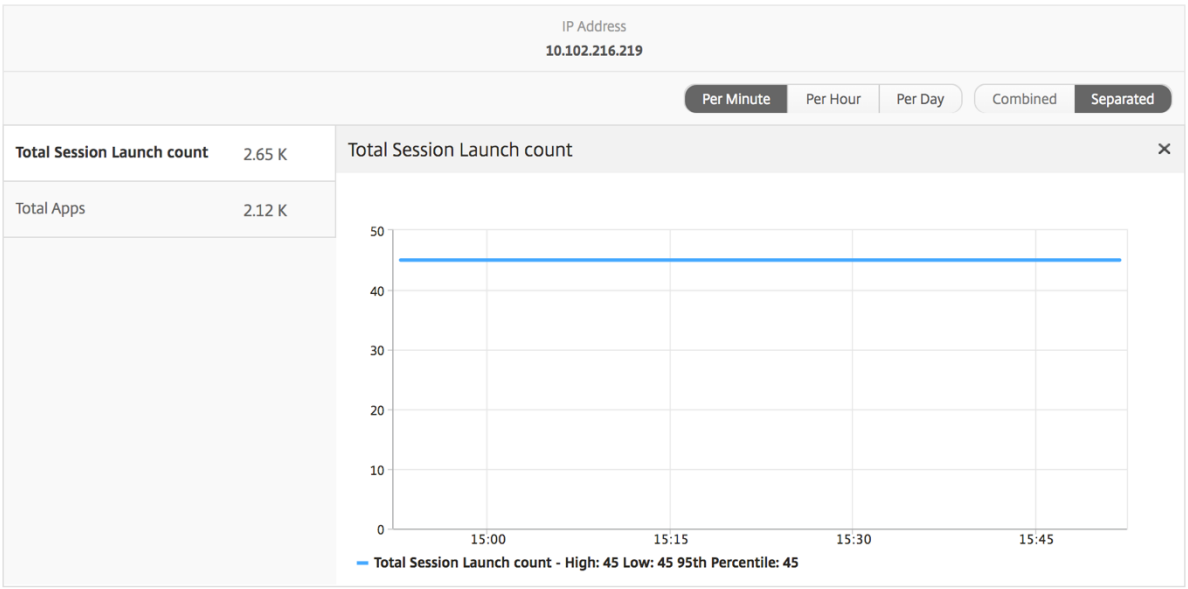


Gráfico de barras de aplicaciones

Muestra las 5 aplicaciones principales según los siguientes criterios: por aplicaciones activas, recuento total de inicios de sesiones, recuento total de inicios de aplicaciones o duración del lanzamiento.

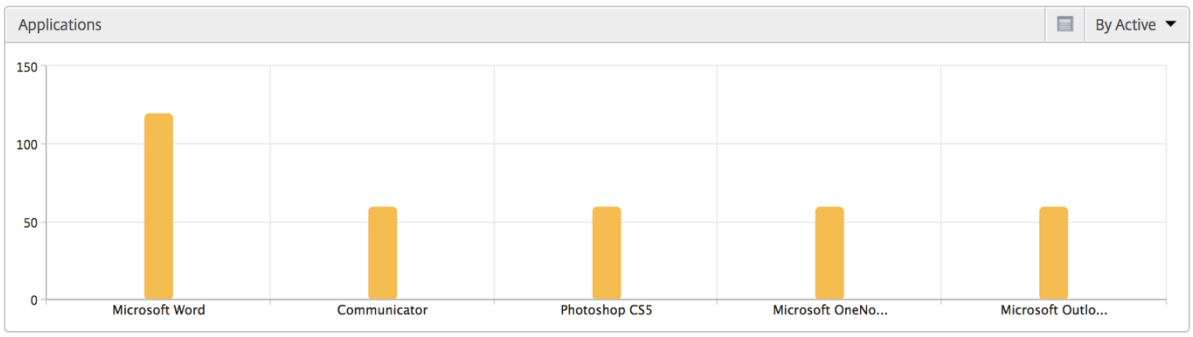
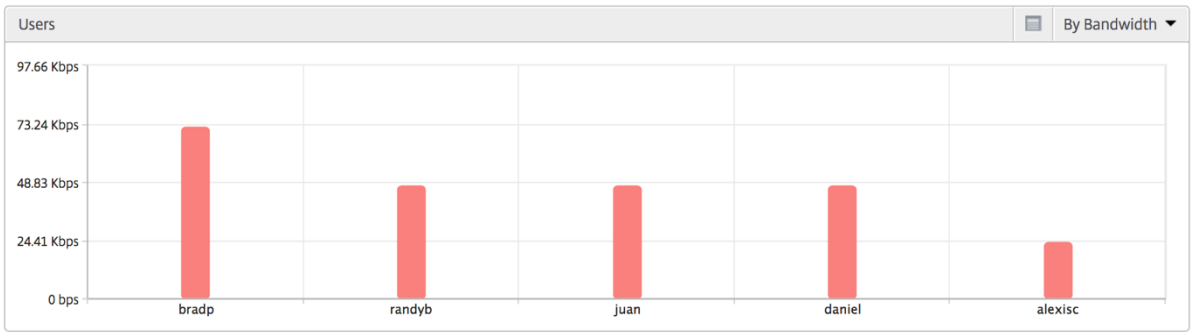


Gráfico de barras de usuarios

El gráfico de barras Usuarios muestra los 5 usuarios principales en función de los siguientes criterios

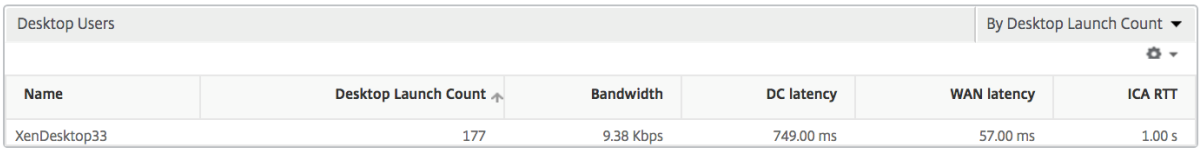
- Ancho de banda
- Latencia de WAN
- Latencia de DC
- RTT de ICA



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, desde NetScaler hasta servidores back-end.
Latencia de WAN	Latencia causada por el lado cliente de la red. Es decir, desde NetScaler 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 App o Desktop, respectivamente.



Desktop Users — By Desktop Launch Count

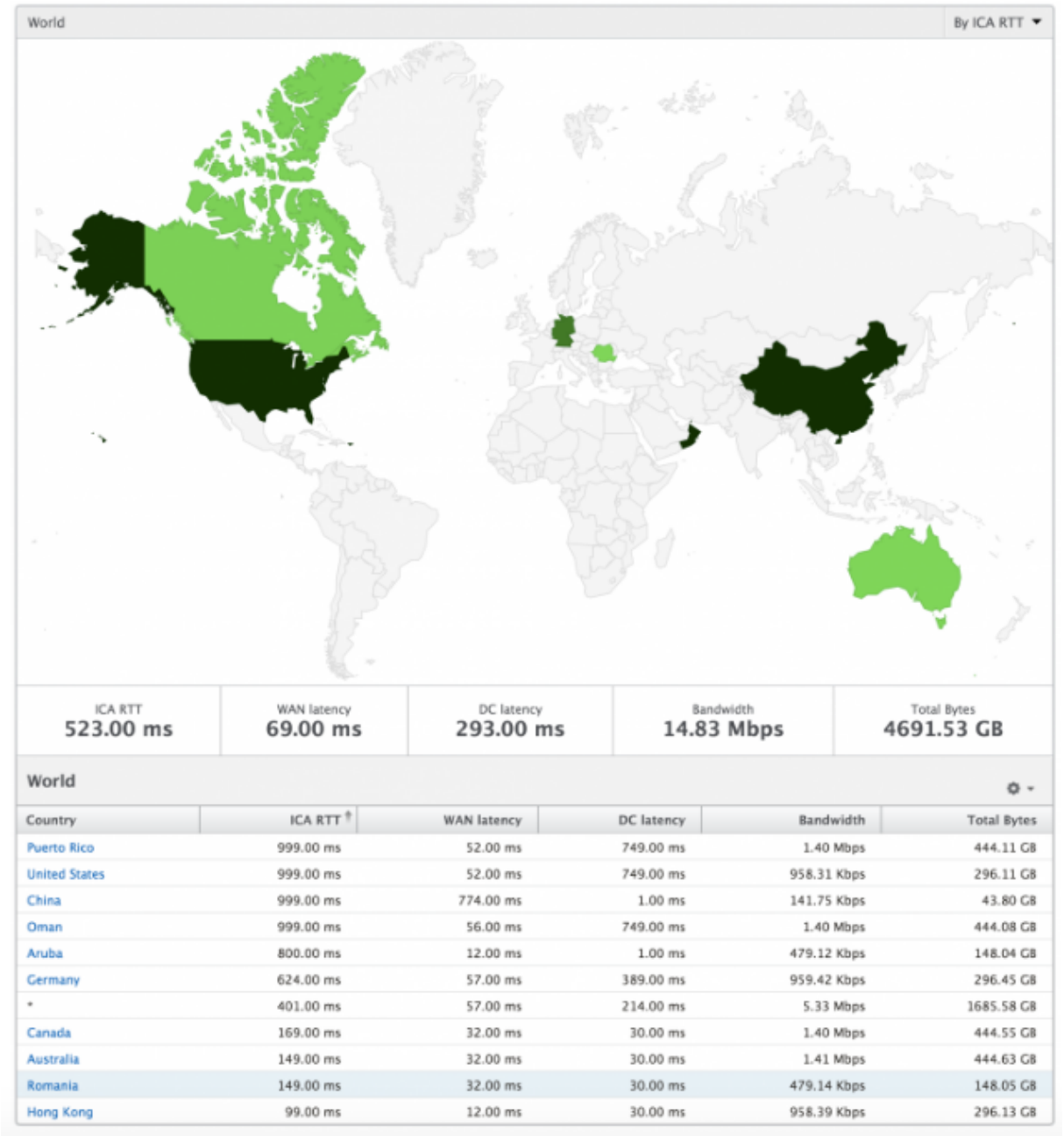
Name	Desktop Launch Count	Bandwidth	DC latency	WAN latency	ICA RTT
XenDesktop33	177	9.38 Kbps	749.00 ms	57.00 ms	1.00 s

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 mundial del sistema, profundizar en un país en particular y más hacia las ciudades también haciendo 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

Informes y métricas de vista de licencias

January 30, 2024

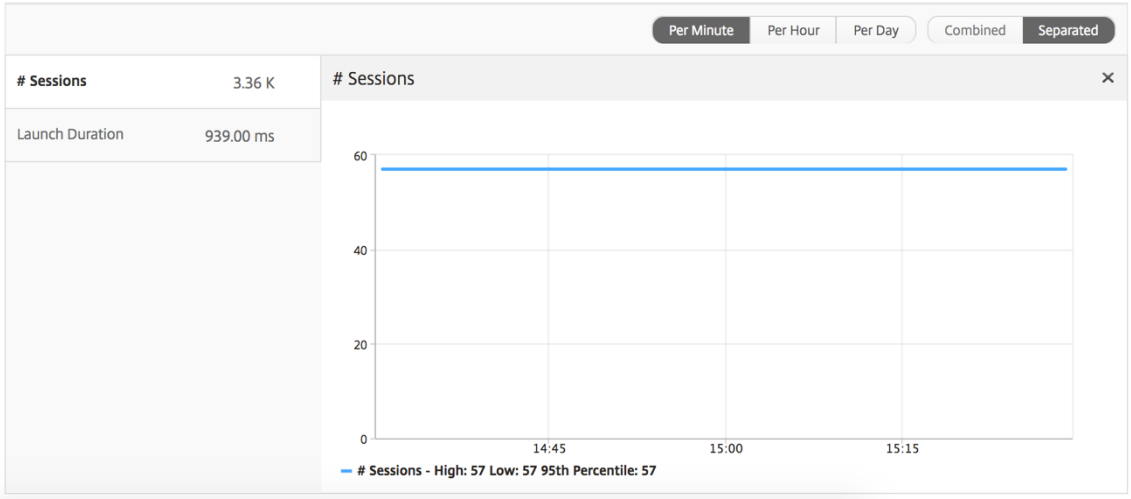
La vista de licencia proporciona detalles sobre la información de licencia de NetScaler Gateway.

Para navegar a la vista de licencia:

1. Vaya a **Gateway > 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, 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 y NetScaler ADM.
- Generación de registros para el tráfico HDX/ICA en NetScaler.
- Población de registros en NetScaler ADM.

Lista de comprobación de configuración de HDX Insight

- Asegúrese de que la función AppFlow esté habilitada en NetScaler. Para obtener más información, consulte Habilitar AppFlow.
- Compruebe la configuración de HDX Insight en la configuración de NetScaler 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 ICA_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 NetScaler Gateway o el servidor virtual VPN esté habilitado para Access Gateway o implementación de doble salto. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.
- Compruebe que “Encadenamiento de conexiones”está activado en NetScaler 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.

Lista de comprobación de conectividad entre NetScaler y NetScaler ADM

- Compruebe el estado del recopilador AppFlow en NetScaler. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler 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 AppFlow.

  También puede navegar a **Configuración > AppFlow > Directivas** en la GUI para comprobar las visitas a la directiva 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

Ejecute el comando `tail -f /var/log/ns.log | grep -i "default ICA Message"` para validar el 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 Citrix Workspace

  Solución: Actualice 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.

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

Omitir código	Mensaje de error	Causa del error
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
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

Omitir código	Mensaje de error	Causa del error
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_LEN0	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
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, se ve con espacios de trabajo 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

Omitir código	Mensaje de error	Causa del error
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_RECONNECT_VERSION	Se omitió el análisis ICA para este espacio de trabajo (cliente) porque no está en la lista de permitidos
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	No se puede detectar el estado de análisis de la cookie de reconexión del cliente
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	Se detectó una longitud de cookie de reconexión no válida después de la
145	NS_ICA_ERR_INVALID_RECONNECT_ID	El cliente reconecta la cookie omitió la restricción necesaria
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	Cadena de versión de espacio de trabajo 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

Omitir código	Mensaje de error	Causa del error
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_INVALIDSTATE	Estado no válido para un comando crypt en el cifrado básico
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_X3	El VDA no admite la versión 3 de Reducer
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_X3	Workspace no admite la versión 3 de Reducer
168	NS_ICA_ERR_ICAP_INSUFFBYTE	Número inesperado de bytes en el protocolo de enlace ICA
169	NS_ICA_ERR_HIGHER_RECONSEQ	Mayor número de secuencia de reanudación de CGP de reconexiones de postes del 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

Omitir código	Mensaje de error	Causa del error
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
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 recuperar el servicio reconecta el tíquet 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 inhabilitar HDX Insight para conexiones que no son 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 la PCB de un 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

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
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
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
hdx_dbg_reconnected_session	Número total de solicitudes de reconexión del cliente sin ningún error de NetScaler	Estados/Diagnósticos
hdx_dbg_host_rejected_ns_reconnect	Número total de hosts rechazados de solicitudes de reconexión por cliente	Estados/Diagnósticos

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_euem_available	Indica el número de conexiones que tienen disponible el canal de supervisión de la experiencia del usuario final. Se requiere el canal de Supervisión de la experiencia del usuario final para recopilar estadísticas como el RTT de ICA.	Estados/Diagnósticos
hdx_err_disabled_sr	La fiabilidad de la sesión se desactiva mediante el control `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 y HDX Insight omite esta conexión.	Error
hdx_err_skip_old_server	Versión de servidor antigua no compatible	Error
hdx_err_clnt_not_whitelist	El espacio de trabajo del cliente no está en la lista de permitidos, HDX Insight omite esta conexión	Error
hdx_sm_ica_cam_channel_disabled	Número total de NS_ICA_CAM_CHANNEL inhabilitados mediante la directiva 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

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_sm_ica_ccm_channel_disabled	Número total de NS_ICA_CCM_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_cdm_channel_disabled	Número total de NS_ICA_CDM_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_com1_channel_disabled	Número total de NS_ICA_COM1_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_com2_channel_disabled	Número total de NS_ICA_COM2_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_cpm_channel_disabled	Número total de NS_ICA_CPM_CHANNEL inhabilitados mediante la directiva 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

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/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
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.

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 NetScaler ADM está recibiendo registros de AppFlow.
- Confirme que la instancia de NetScaler 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 y NetScaler ADM.
- Versiones del servidor Citrix Virtual Apps and Desktops.
- Versiones de Client Workspace.
- Número de sesiones ICA activas cuando se produjo el problema.
- Paquete de soporte técnico capturado ejecutando el comando `show techsupport` en el símbolo del sistema de NetScaler.
- Paquete de soporte técnico capturado para NetScaler ADM.
- Rastreos de paquetes capturados en todos los NetScaler.
  Para iniciar un seguimiento de paquete, escriba,`start nstrace -size 0'`
  Para detener un seguimiento de paquete, escriba,`stop nstrace`
- Recopilar entradas en la tabla ARP del sistema ejecutando el comando `show arp`.

Problemas conocidos

Consulte las notas de la versión de ADC para conocer los problemas conocidos en HDX Insight.

Análisis de infraestructura

January 30, 2024

Un objetivo clave para los administradores de red es supervisar las instancias de NetScaler. Las instancias de ADC ofrecen información interesante sobre el uso y el rendimiento de las aplicaciones y escritorios a los que se accede mediante ellas. Los administradores deben supervisar la instancia de ADC y analizar los flujos de aplicación procesados por cada instancia de ADC. Pueden remediar cualquier problema probable de configuración, configuración, conectividad, certificados y otros que puedan afectar el uso o el rendimiento de las aplicaciones. Por ejemplo, un cambio repentino en el patrón de tráfico de la aplicación puede deberse a un cambio en la configuración SSL, como la desactivación de un protocolo SSL. Los administradores deben poder identificar rápidamente la correlación entre estos puntos de datos para garantizar lo siguiente:

- La disponibilidad de las aplicaciones se encuentra en un estado óptimo
- No hay problemas de consumo de recursos, hardware, capacidad o cambio de configuración
- No hay inventarios no utilizados
- No hay certificados caducados

La función de análisis de infraestructura simplifica el proceso de análisis de datos al correlacionar varias fuentes de datos y cuantificarlas en una puntuación medible que define el estado de una instancia. Con esta función, los administradores tienen un único punto de contacto para saber si hay un problema, el origen del problema y las posibles soluciones que pueden realizar.

Análisis de infraestructura

La función de análisis de la infraestructura de gestión de entrega de aplicaciones (ADM) de NetScaler recopila todos los datos recopilados de las instancias de NetScaler y los cuantifica en una **puntuación de instancias que define el estado de las instancias**. La puntuación de la instancia se resume en una vista tabular o como visualización de paquetes circulares. La función Análisis de infraestructura le ayuda a visualizar los factores que provocaron o podrían provocar un problema en las instancias. Esta visualización también le ayuda a determinar las acciones que deben realizarse para evitar que el problema se repita.

Puntuación de instancia

La puntuación de la instancia indica el estado de una instancia de ADC. Una puntuación de 100 significa una instancia perfectamente sana sin problemas. La puntuación de la instancia captura diferentes niveles de posibles problemas en la instancia. Es una medida cuantificable de la salud de las instancias y múltiples "indicadores de salud"contribuyen a la puntuación.

Los**indicadores de salud son los** componentes básicos de la puntuación de la instancia, donde la puntuación se calcula periódicamente para un "período de supervisión"predefinido, en función de todos los indicadores detectados en esa ventana de tiempo. Actualmente, Infrastructure Analytics calcula la puntuación de la instancia una vez cada hora en función de los datos recopilados de las instancias.
Un indicador se puede definir como cualquier actividad (un evento o un problema) que pertenezca a una de las siguientes categorías de las instancias.

- Indicadores de recursos del sistema
- Indicadores de eventos críticos
- Indicadores de configuración SSL
- Indicadores de desviación de configuración

Indicadores de salud

- Indicadores de recursos del sistema

Los siguientes son los problemas críticos de recursos del sistema que pueden ocurrir en las instancias de NetScaler y que NetScaler ADM puede supervisar.

- Uso**elevado de la CPU**. El uso de la CPU ha superado el valor de umbral más alto en la instancia de NetScaler.
- **Alto uso de memoria**. El uso de memoria ha superado el valor de umbral superior en la instancia de NetScaler.
- **Uso elevado del disco**. El uso del disco ha superado el valor umbral superior en la instancia de NetScaler.
- **Errores de disco**. Hay errores en el disco duro 0 o en el disco duro 1 del hipervisor en el que está instalada la instancia de ADC.
- **Fallo de alimentación**. La fuente de alimentación ha fallado o se ha desconectado de la instancia de ADC.
- **Fallo en la tarjeta SSL**. La tarjeta SSL instalada en la instancia ha fallado.
- **Errores de flash**. Se observan errores de Compact Flash en la instancia de NetScaler.
- La**NIC descarta**. Los paquetes descartados por la tarjeta NIC han cruzado el valor de umbral más alto en la instancia de NetScaler.

Para obtener más información sobre estos errores de recursos del sistema, consulta El panel de instancias.

- Indicadores de eventos críticos

  Los siguientes eventos críticos se identifican mediante la función de administración de eventos de ADM, que se configura con una gravedad crítica.

  - **Fallo de sincronización de HA**. La sincronización de la configuración entre las instancias de ADC en alta disponibilidad falló en el servidor secundario.
  - **No tiene latidos**. El servidor principal de un par de instancias de ADC en alta disponibilidad no recibe los latidos del servidor secundario.
  - **Tiene un mal estado secundario**. El servidor secundario de un par de instancias de ADC con alta disponibilidad se encuentra en estado secundario Inactivo, Desconocido o Permanecer.
  - **La versión HA no coincide**. La versión de las imágenes del software ADC instaladas en un par de instancias de ADC en alta disponibilidad no coincide.
  - **Fallo de sincronización del clúster**. La sincronización de la configuración entre las instancias de ADC en el modo de clúster ha fallado.

- **La versión del clúster no coincide**. La versión de las imágenes del software ADC instaladas en las instancias de ADC en modo de clúster no coincide.
- **Fallo de propagación del clúster**. Se produjo un error al propagar las configuraciones a todas las instancias de un clúster.

> **Nota**
>
> Puede tener la lista de eventos SNMP críticos cambiando los niveles de gravedad de los eventos. Para obtener más información sobre cómo cambiar los niveles de gravedad, consulte Modificar la gravedad informada de los eventos que se producen en las instancias de NetScaler.

Para obtener más información sobre los eventos de NetScaler ADM, consulte Eventos.

- Indicadores de configuración SSL
  - **No se recomienda la fuerza clave**. La fortaleza clave de los certificados SSL no cumple con los estándares de NetScaler.
  - **Emisor no recomendado**. Citrix no recomienda el emisor del certificado SSL.
  - **Los certificados SSL han caducado**. El certificado SSL instalado en la instancia ADC ha caducado.
  - **Los certificados SSL están vencidos**. El certificado SSL instalado en la instancia ADC está a punto de caducar en la próxima semana.
  - **Algoritmos no recomendados**. Los algoritmos de firma de los certificados SSL instalados en la instancia de ADC no cumplen con los estándares de NetScaler.

Para obtener más información sobre los certificados SSL, consulte Panel de control SSL.

- Indicadores de desviación de configuración
  - **Plantilla Config Drift**. Hay una desviación (cambios sin guardar) en la configuración con respecto a las plantillas de auditoría que ha creado con configuraciones específicas que quiere auditar en determinadas instancias.
  - **Desviación de configuración predeterminada**. Hay una desviación (cambios no guardados) en la configuración de los archivos de configuración predeterminados.

Para obtener más información sobre las desviaciones de la configuración y cómo ejecutar informes de auditoría para comprobar las desviaciones de la configuración, consulte Ver informes de auditoría.

Ver problemas de capacidad ADC

Cuando una instancia ADC ha consumido la mayor parte de su capacidad disponible, puede producirse la caída de paquetes al procesar el tráfico del cliente. Este problema provoca un bajo

rendimiento en una instancia de ADC. Al comprender estos problemas de capacidad del ADC, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento del ADC.

Para ver las cuestiones relativas a la capacidad de los CCA,

1. Vaya a **Infraestructura > Análisis de infraestructura**.
2. Expanda la instancia para la que quiere ver los problemas de capacidad.

El ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra las caídas de paquetes o incrementos de contador de límite de velocidad, si existe. Los problemas se clasifican según los siguientes parámetros de capacidad:

- **Límite de rendimiento alcanzado**: El número de paquetes descartados en la instancia una vez alcanzado el límite de rendimiento.
- **Se alcanzó el límite de CPU PE**: La cantidad de paquetes descartados en todas las NIC una vez alcanzado el límite de CPU PE.
- **Se alcanzó el límite de PPS**: El número de paquetes descartados en la instancia una vez alcanzado el límite de PPS.
- **Límite de velocidad de procesamiento de SSL**: Número de veces que se ha alcanzado el límite de rendimiento de SSL
- **Límite de velocidad SSL TPS**: El número de veces que se ha alcanzado el límite de SSL TPS.

El ADM calcula la puntuación de la instancia en el umbral de capacidad definido.

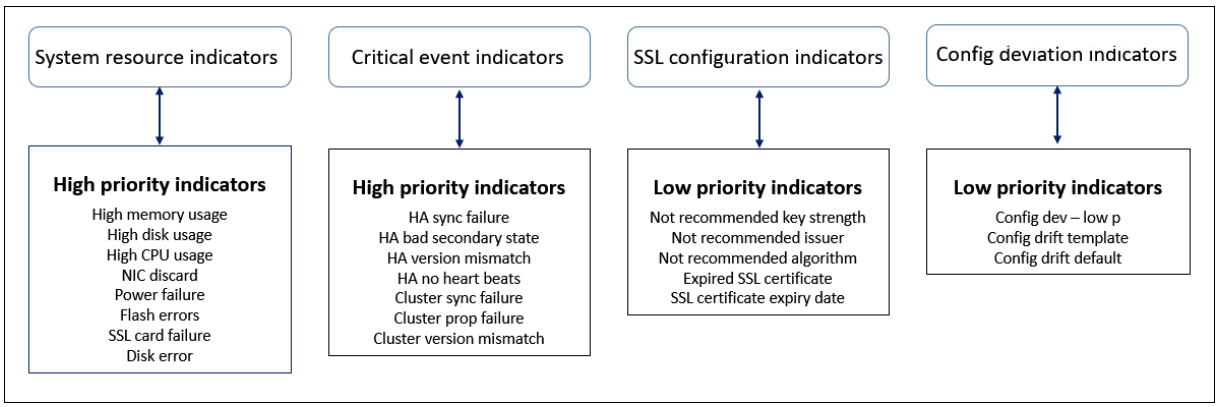
- Umbral bajo: 1 incremento del contador de límite de velocidad o caída de paquetes
- Umbral alto: Incremento del contador de límite de velocidad o caída de 10000 paquetes

Por lo tanto, cuando una instancia de ADC supera el umbral de capacidad, la puntuación de la instancia se ve afectada.

Cuando los paquetes caen o el contador de límite de velocidad aumenta, se genera un evento bajo la categoría `ADCCapacityBreach`. Para ver estos eventos, vaya a **Cuentas > Eventos del sistema**.

Valor de los indicadores de salud

Los indicadores se clasifican en indicadores de alta prioridad e indicadores de baja prioridad sobre la base de sus valores de la siguiente manera:



Los indicadores de salud dentro del mismo grupo de indicadores tienen diferentes pesos asignados a ellos. Un indicador podría contribuir más a reducir la puntuación de la instancia que otro indicador. Por ejemplo, un uso elevado de memoria reduce la puntuación de la instancia más que el uso elevado del disco, el uso elevado de la CPU y el descarte de NIC. Si una instancia tiene un mayor número de indicadores detectados, menor será la puntuación de la instancia.

El valor de un indicador se calcula según las siguientes reglas. Se dice que el indicador se detecta de una de las tres formas siguientes:

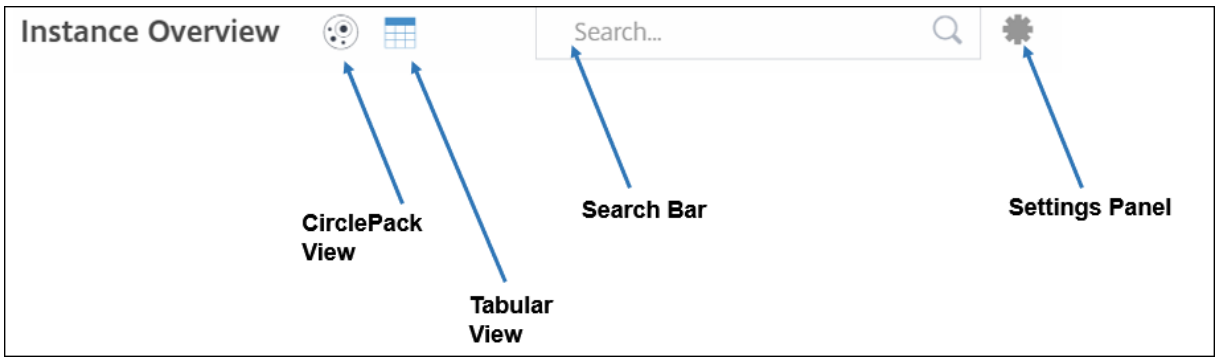
1. **Basado en una actividad**. Por ejemplo, un indicador de recursos del sistema se activa cada vez que se produce un corte de energía en la instancia y este indicador reduce el valor de la puntuación de la instancia. Cuando se borra el indicador, se elimina la penalización y la puntuación de la instancia aumenta.
2. **Basado en la violación del valor umbral**. Por ejemplo, se activa un indicador de recursos del sistema cuando la tarjeta NIC descarta paquetes y se infringe el nivel de umbral.
3. **Basado en la brecha de valor de umbral bajo y alto**. En este caso, un indicador se puede activar de dos maneras:
    - Cuando el valor del indicador se encuentra entre los umbrales más bajo y más alto, en cuyo caso se aplica una penalización parcial a la puntuación de la instancia.
    - Cuando el valor supera el umbral alto, en cuyo caso se aplica una penalización total a la puntuación de la instancia.
    - No se aplicará ninguna penalización a la puntuación de la instancia si el valor cae por debajo de un umbral bajo.

Por ejemplo, el uso de la CPU es un indicador de recursos del sistema que se activa cuando el valor de uso cruza el umbral inferior y también cuando el valor cruza el umbral alto.

Panel de análisis de infraestructura

Vaya a **Infraestructura > Análisis de infraestructura**.

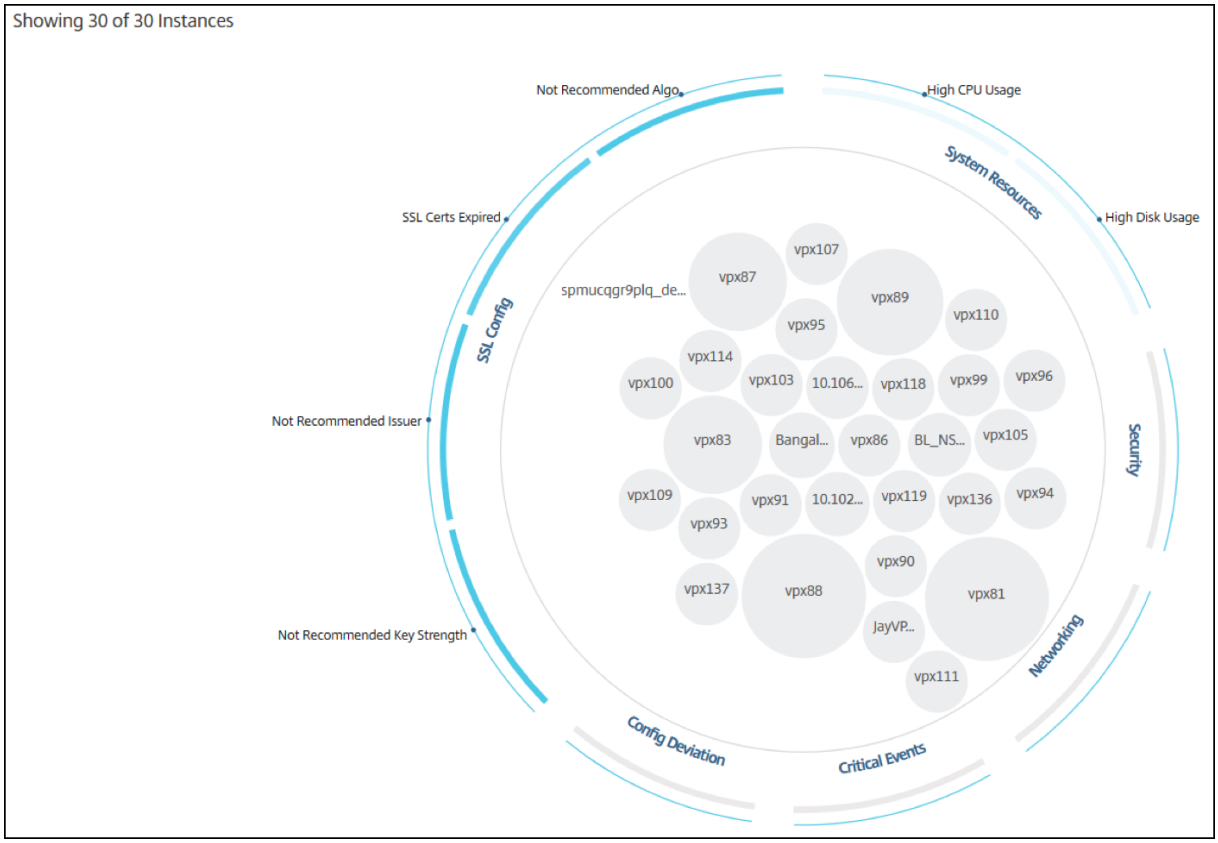
Infrastructure Analytics se puede ver en formato **Circle Pack** o **Tabular**. Puede alternar entre los dos formatos.



- En la vista Tabular, puede buscar una instancia escribiendo el nombre de host o la dirección IP en la barra de búsqueda.
- De forma predeterminada, la página Infrastructure Analytics muestra el panel de resumen en la parte derecha de la página.
- Haga clic en el icono de **configuración** para mostrar el panel de **configuración**.
- En ambos formatos de vista, el panel de resumen muestra los detalles de todas las instancias de la red.

Vista circular del paquete

Los diagramas de empaquetado circular muestran los grupos de instancias como círculos muy organizados Suelen mostrar jerarquías en las que los grupos de instancias más pequeños tienen un color similar al de otros grupos de la misma categoría o están anidados dentro de grupos más grandes. Los paquetes de círculo representan conjuntos de datos jerárquicos y muestran diferentes niveles en la jerarquía y cómo interactúan entre sí.



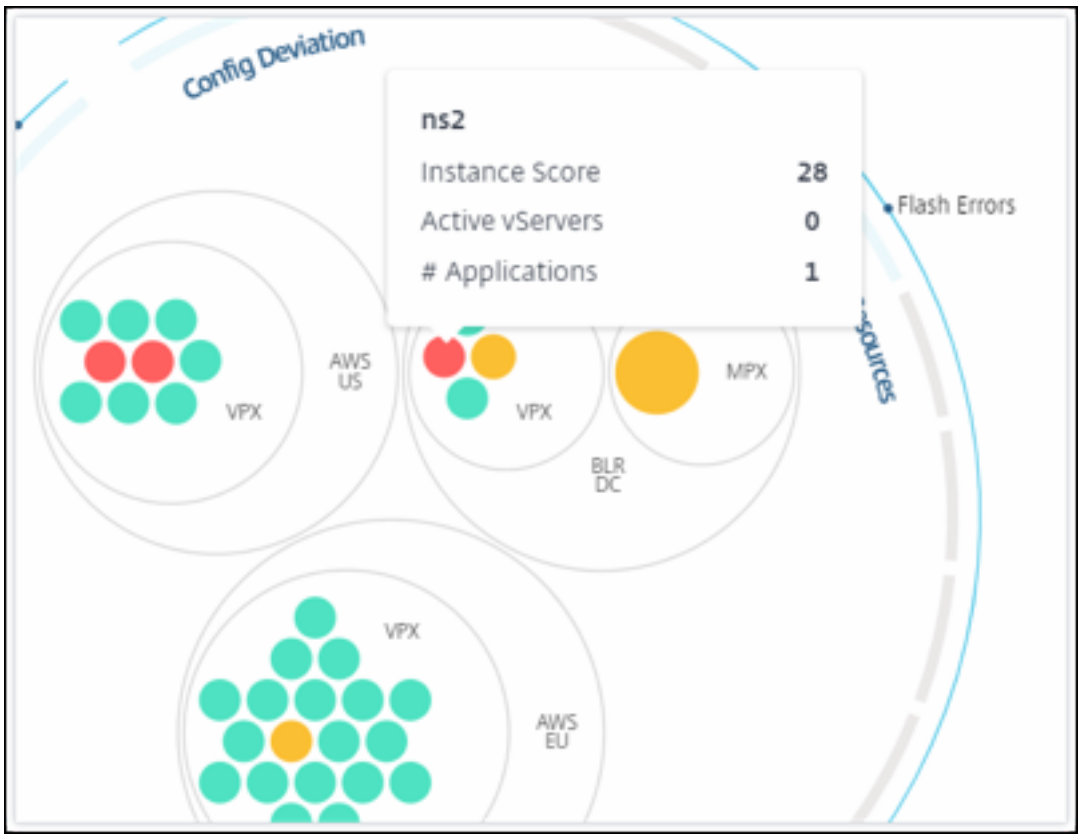
Círculos de instancia

Color. Cada instancia se representa en Circle Pack como un círculo coloreado. El color del círculo indica el estado de la instancia.

- **Verde**: la puntuación de la instancia está entre 100 y 80. La instancia está en buen estado.
- **Amarillo**: La puntuación de la instancia está entre 80 y 50; se han detectado algunos problemas que deben revisarse.
- **Rojo**: la puntuación de la instancia es inferior a 50. La instancia se encuentra en una etapa crítica, ya que se han observado varios problemas en esa instancia.

Talla El tamaño de estos círculos de colores indica la cantidad de servidores virtuales configurados en esa instancia. Un círculo más grande indica que hay un mayor número de servidores virtuales.

Puede pasar el puntero del mouse sobre cada uno de los círculos de la instancia (círculos de colores) para ver un resumen. La sugerencia de la herramienta al pasar el mouse muestra el nombre de host de la instancia, el número de servidores virtuales activos y el número de aplicaciones configuradas en esa instancia.

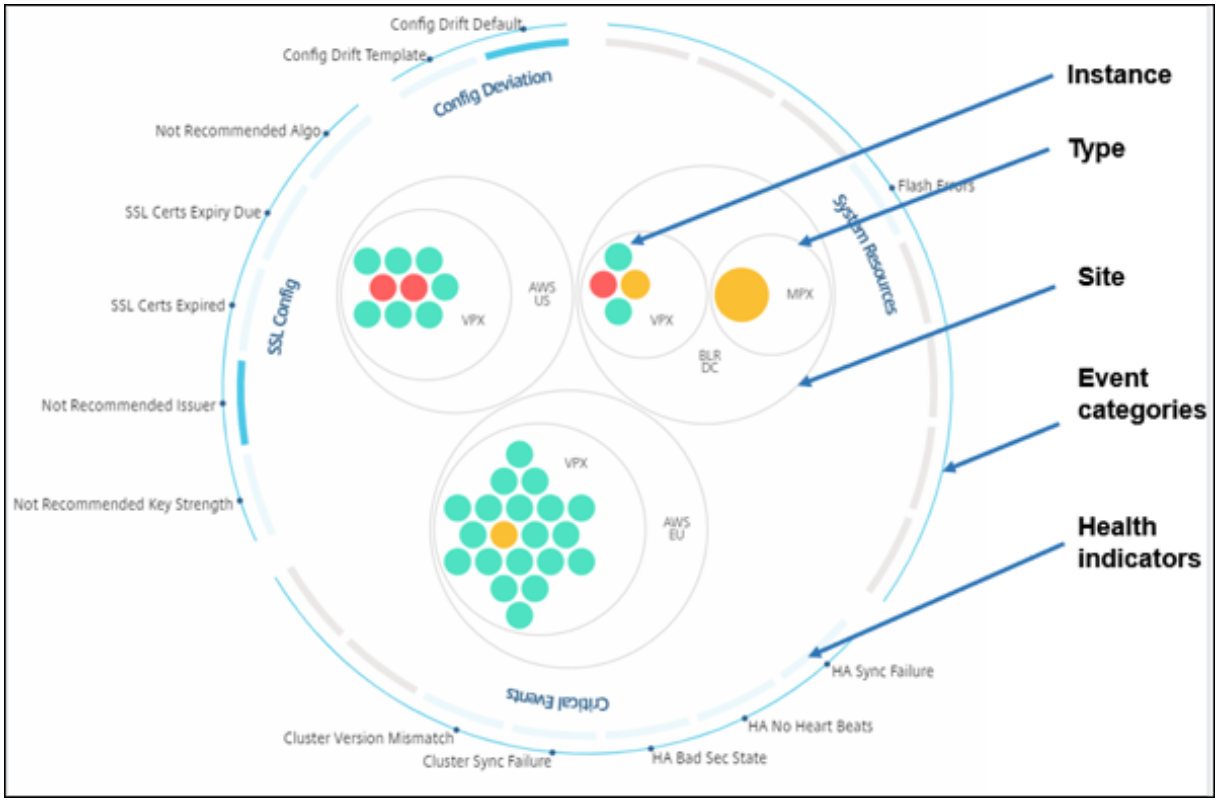


Círculos de instancia agrupados

El paquete circular, al principio, comprende círculos de instancias que se agrupan, anidan o empaquetan dentro de otro círculo según los siguientes criterios:

- el sitio en el que se implementan
- el tipo de instancias implementadas: VPX, MPX, SDX y CPX
- el modelo virtual o físico de la instancia de ADC
- la versión de la imagen ADC instalada en las instancias

La siguiente imagen muestra un paquete de círculo donde las instancias se agrupan primero por el sitio o centro de datos donde se implementan y, a continuación, se agrupan en función de su tipo, VPX y MPX.

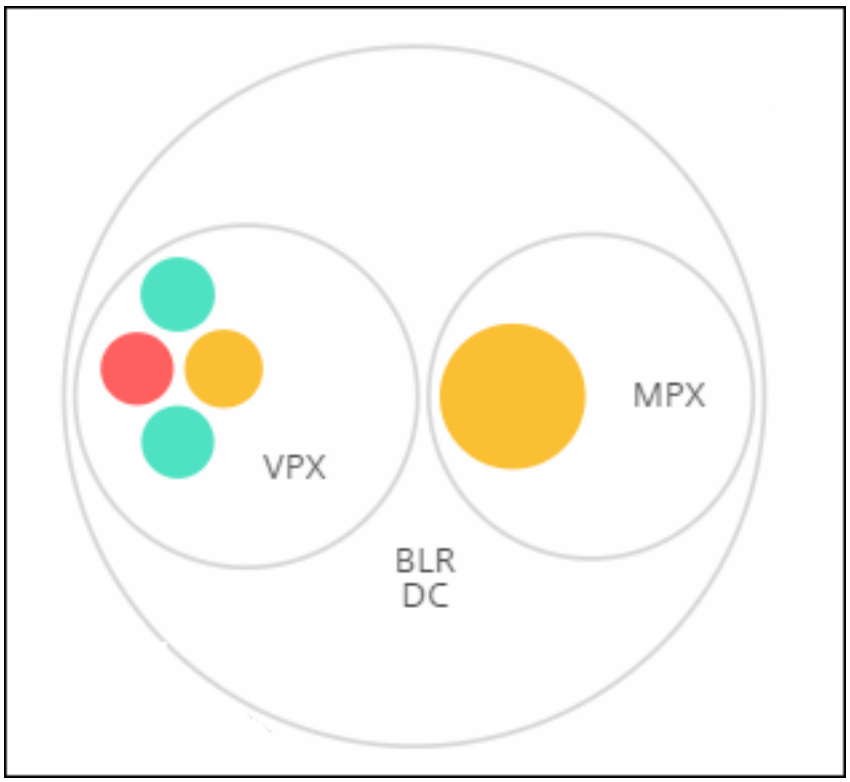


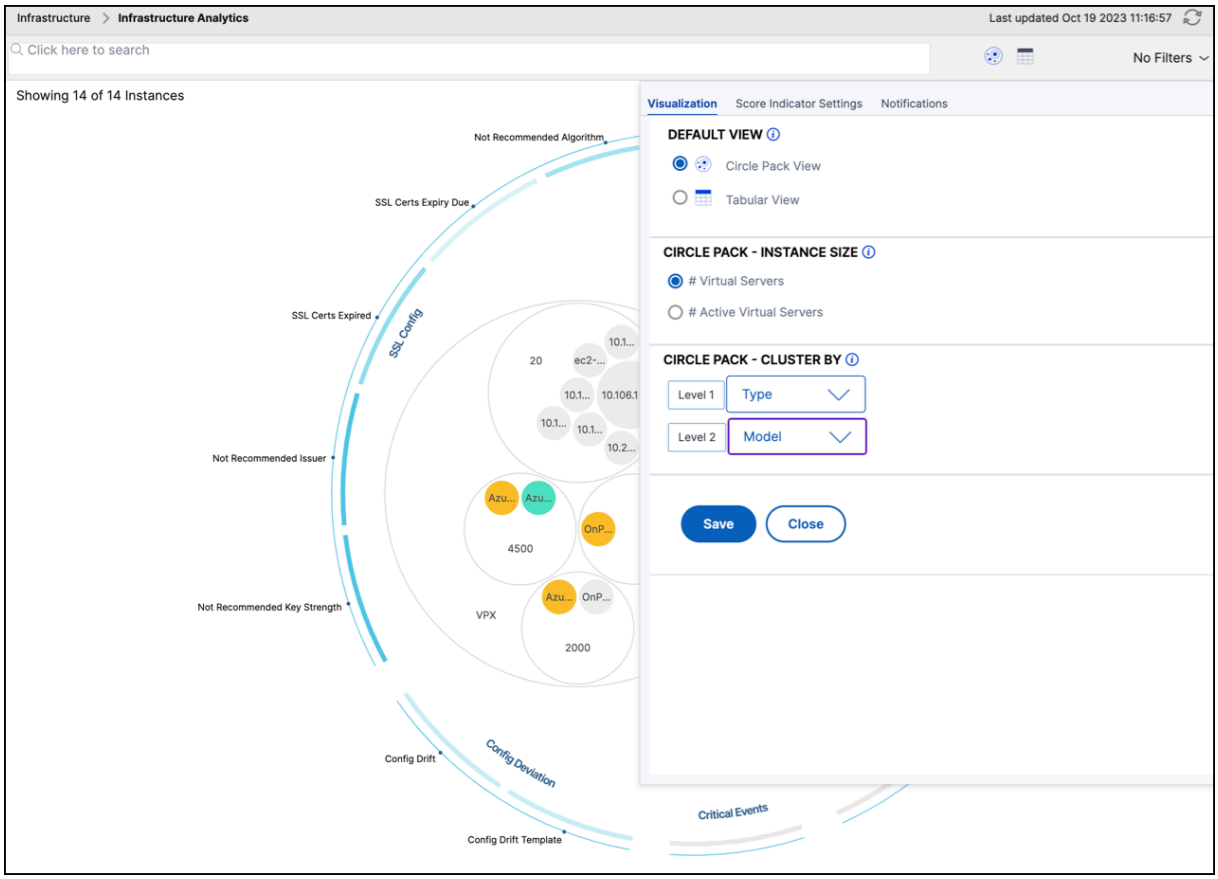
Todos estos círculos anidados están delimitados por dos círculos exteriores. Los dos círculos exteriores representan las cuatro categorías de eventos supervisados por el NetScaler ADM (recursos del sistema, eventos críticos, configuración de SSL y desviación de configuración) y los indicadores de estado que contribuyen.

Círculos de instancia agrupados

NetScaler ADM supervisa muchas instancias. Para facilitar la supervisión y el mantenimiento de estas instancias, Infrastructure Analytics permite agruparlas en dos niveles. Es decir, las agrupaciones de instancias se pueden anidar dentro de otra agrupación.

Por ejemplo, el centro de datos de BLR tiene dos tipos de instancias de ADC: VPX y MPX, implementadas en él. Primero puede agrupar las instancias de ADC por su tipo y, a continuación, agrupar todas las instancias por el sitio en el que están agrupadas. Ahora puede identificar fácilmente cuántos tipos de instancias se implementan en los sitios que está administrando.

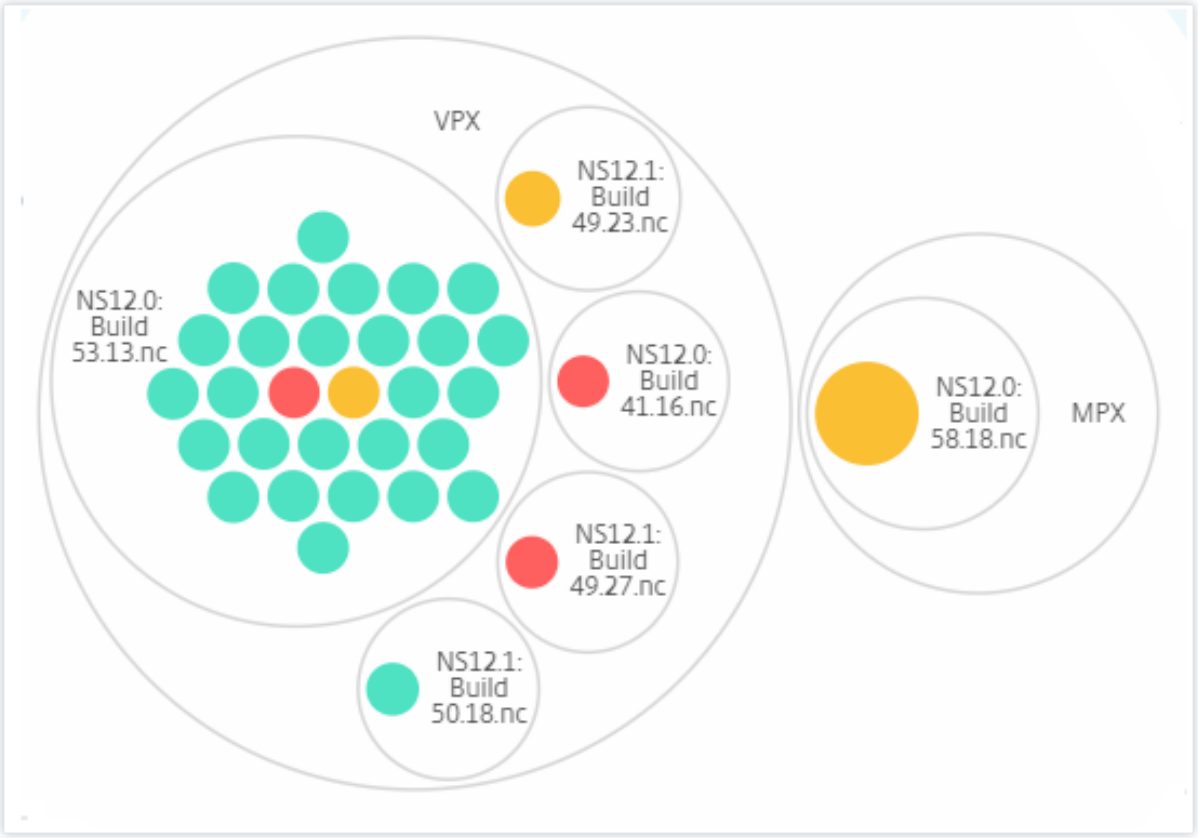




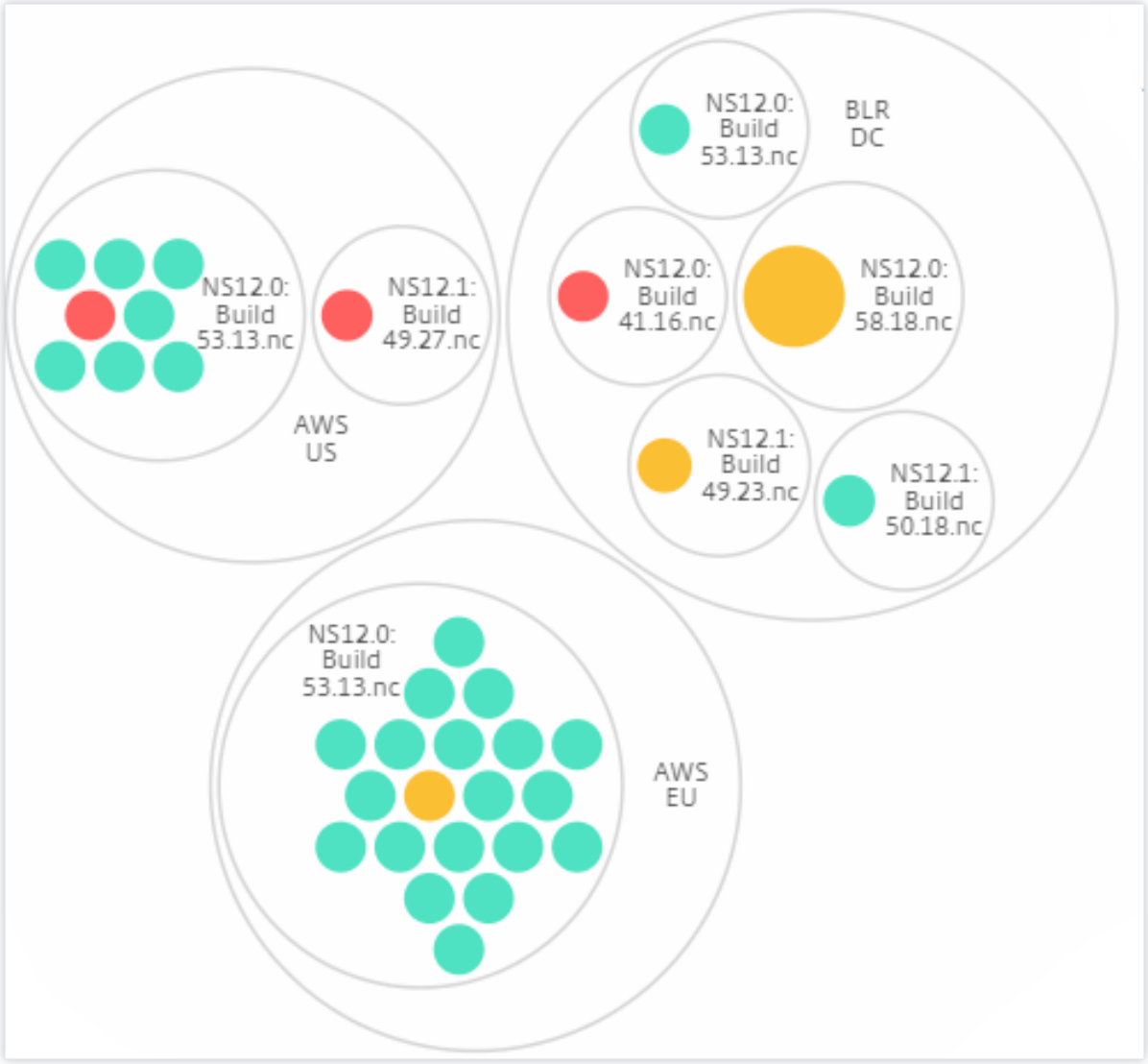
Algunos ejemplos más de clustering de dos niveles son los siguientes:

Sitio y modelo:

Tipo y versión:

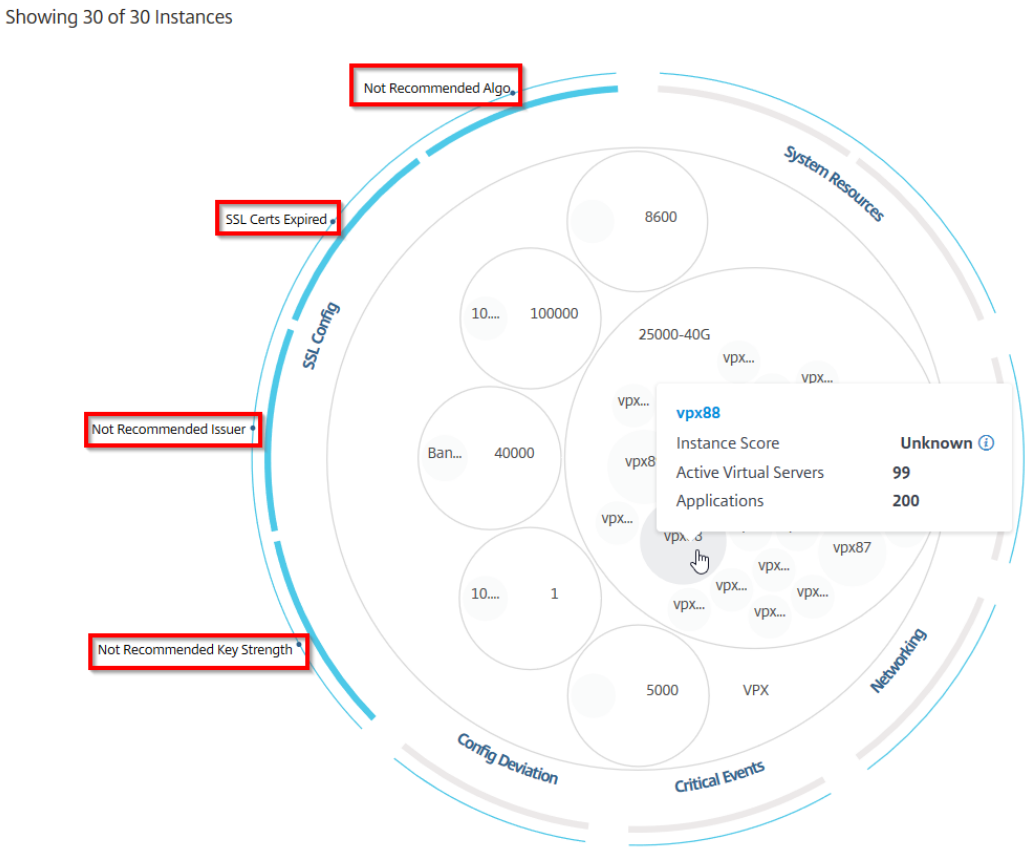


Sitio y versión:



Cómo usar Circle Pack

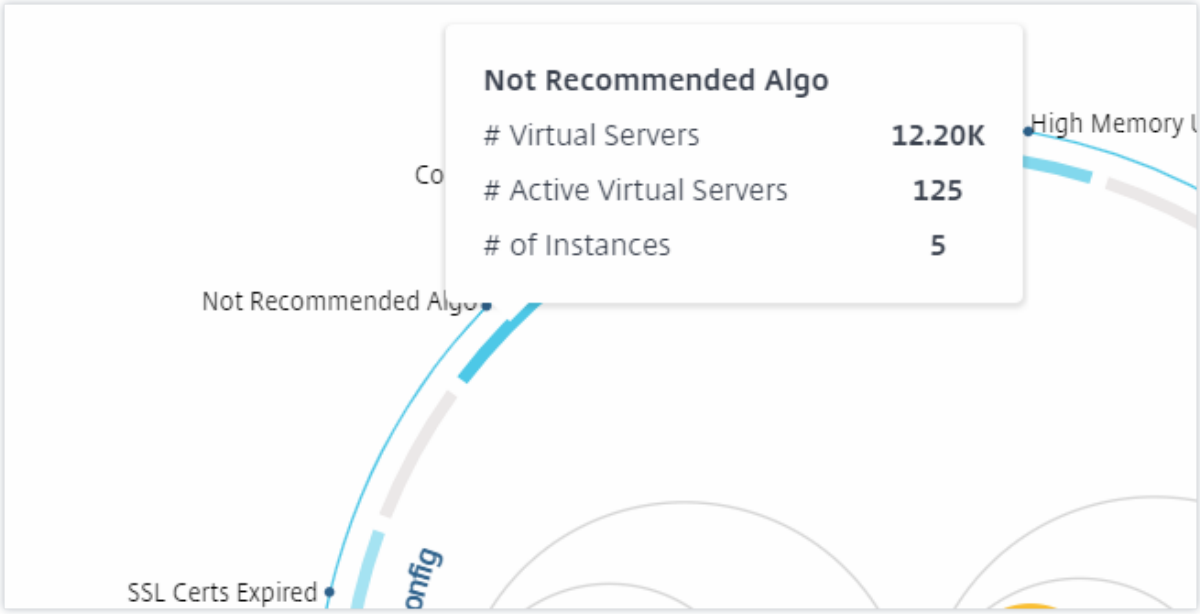
Haga clic en cada uno de los círculos coloreados para resaltar esa instancia.



Dependiendo de los eventos que se hayan producido en ese caso, solo los indicadores de salud aparecen resaltados en los círculos exteriores. Por ejemplo, las dos imágenes siguientes de Circle Pack muestran diferentes conjuntos de indicadores de riesgo, aunque ambas instancias se encuentran en un estado crítico.

También puede hacer clic en los indicadores de estado para obtener más detalles sobre el número de instancias que han informado de ese indicador de riesgo. Por ejemplo, haga clicNot recommended

`Algo` para ver el informe resumido de ese indicador de riesgo.

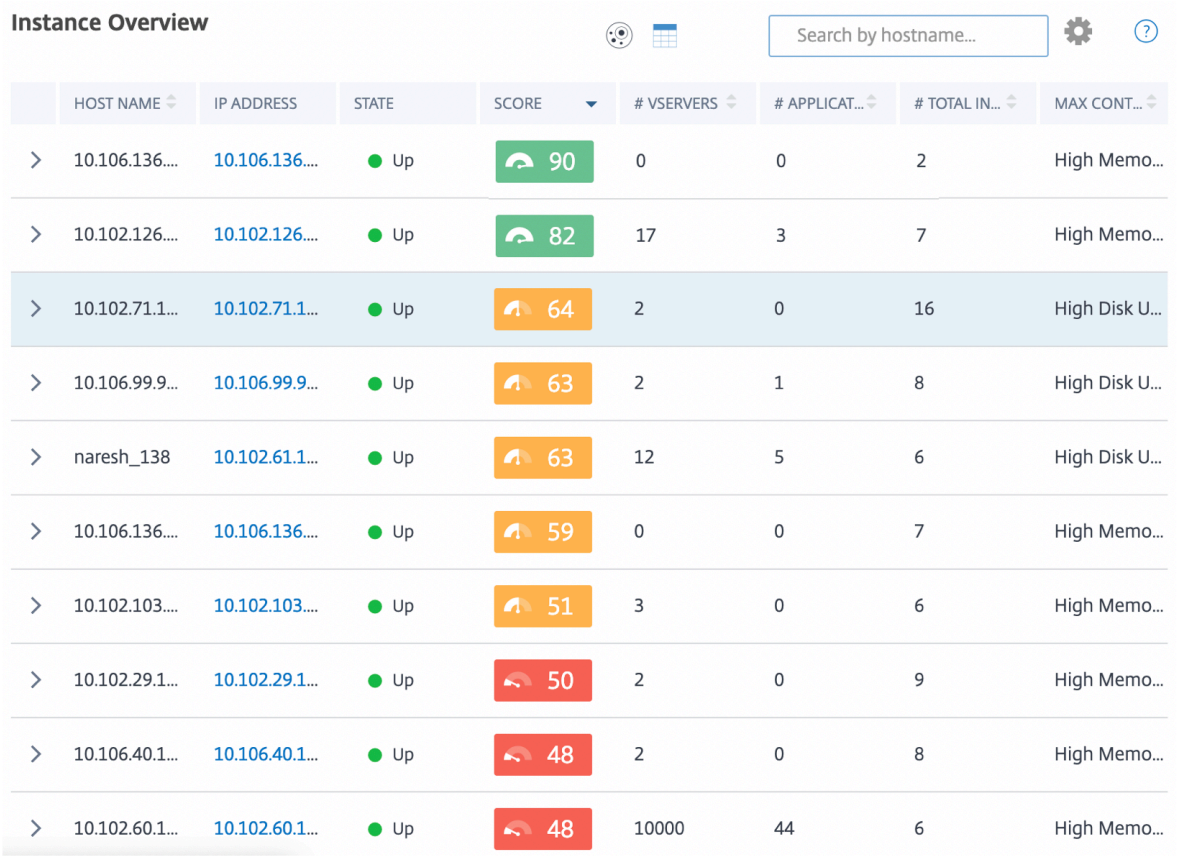


Vista tabular

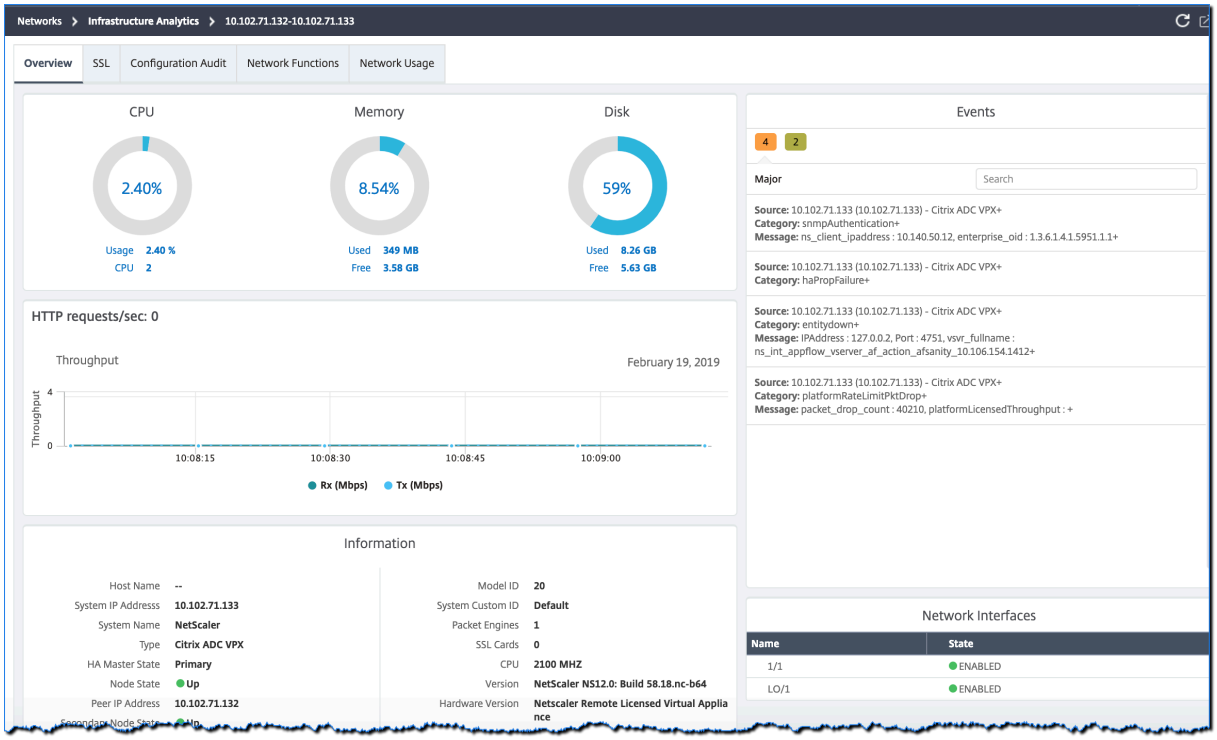
La vista tabular muestra las instancias y los detalles de esas instancias en un formato tabular. Los detalles que se muestran son los siguientes:

- Nombre de host de la instancia
- La dirección IP de la instancia
- Estado de la instancia
- Puntuación de instancia
- Número de servidores virtuales configurados en esa instancia
- Número de aplicaciones configuradas en esa instancia
- Número total de indicadores de riesgo
- El evento que contribuye más a reducir la puntuación de la instancia

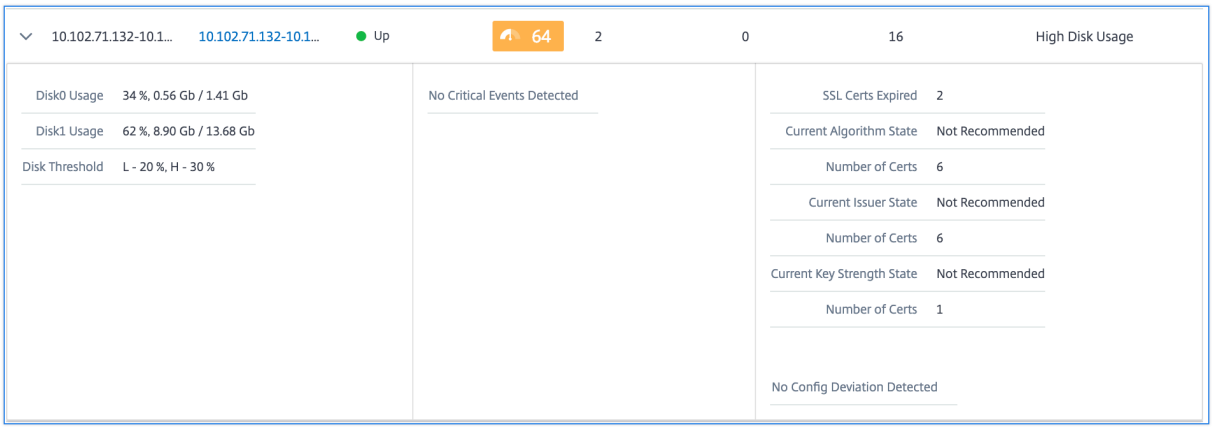
Las instancias que se encuentran en estado crítico aparecen en la parte superior de la tabla, seguidas de las instancias que deben revisarse y, a continuación, las instancias en buen estado.



Haga clic en la dirección IP de la instancia en la vista tabular para ver más detalles de esa instancia en el panel de control. El panel de instancias presenta una descripción general de la instancia en la que puede ver la CPU, la memoria y el uso del disco de la instancia. También puede ver detalles relacionados con la administración de certificados SSL, auditoría de configuración, funciones de red y un informe de red que muestra el uso detallado de la red de la instancia. Desplázate hacia abajo para ver la lista de las funciones y los modos habilitados en esta instancia.



También puede hacer clic en la flecha situada al principio de cada fila para expandir la fila y obtener más detalles.



La fila de la tabla expandida muestra los errores que se han producido en la instancia en todas las categorías. En el ejemplo anterior, puede ver que se han producido errores en los recursos del sistema, en la configuración de SSL y en los archivos de configuración. Sin embargo, no se ha informado de ningún evento crítico en la instancia.

Cómo utilizar el panel de resumen

El **Panel de resumen** le ayuda a centrarse de manera eficiente y rápida en las instancias que necesitan revisión o estado crítico. El panel se divide en tres fichas: descripción general, información de

la instancia y perfil de tráfico. Los cambios que realice en este panel modifican la visualización en los formatos de vista Circle Pack y Tabular. En las siguientes secciones se describen estas fichas con más detalle. Los ejemplos de las siguientes secciones le ayudan a utilizar los diferentes criterios de selección de manera eficiente para analizar los problemas reportados por las instancias.

Descripción general:

La ficha **Descripción general** permite supervisar las instancias en función de los errores de hardware, el uso, los certificados caducados y otros indicadores similares que pueden ocurrir en las instancias. Los indicadores que puede supervisar aquí son los siguientes:

- Uso de CPU
- Uso de memoria
- Uso del disco
- Fallos del sistema
- Eventos críticos
- Caducidad de los

Los ejemplos siguientes ilustran cómo puede interactuar con el panel **Visión general** para aislar las instancias que informan de errores.

Ejemplo 1: Ver las instancias que se encuentran en estado de revisión:

Seleccione la casilla **Revisar** para ver solo las instancias que no informan de errores críticos, pero que aún requieren atención.

Los histogramas del panel **Descripción general** representan un número agregado de instancias en función de los eventos de uso elevado de la CPU, alto uso de memoria y uso elevado del disco. Los histogramas se califican en 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% y 100%. Pase el puntero del mouse sobre uno de los gráficos de barras. La leyenda de la parte inferior del gráfico muestra el rango de uso y el número de instancias en ese rango. También puede hacer clic en el gráfico de barras para mostrar todas las instancias de ese rango.

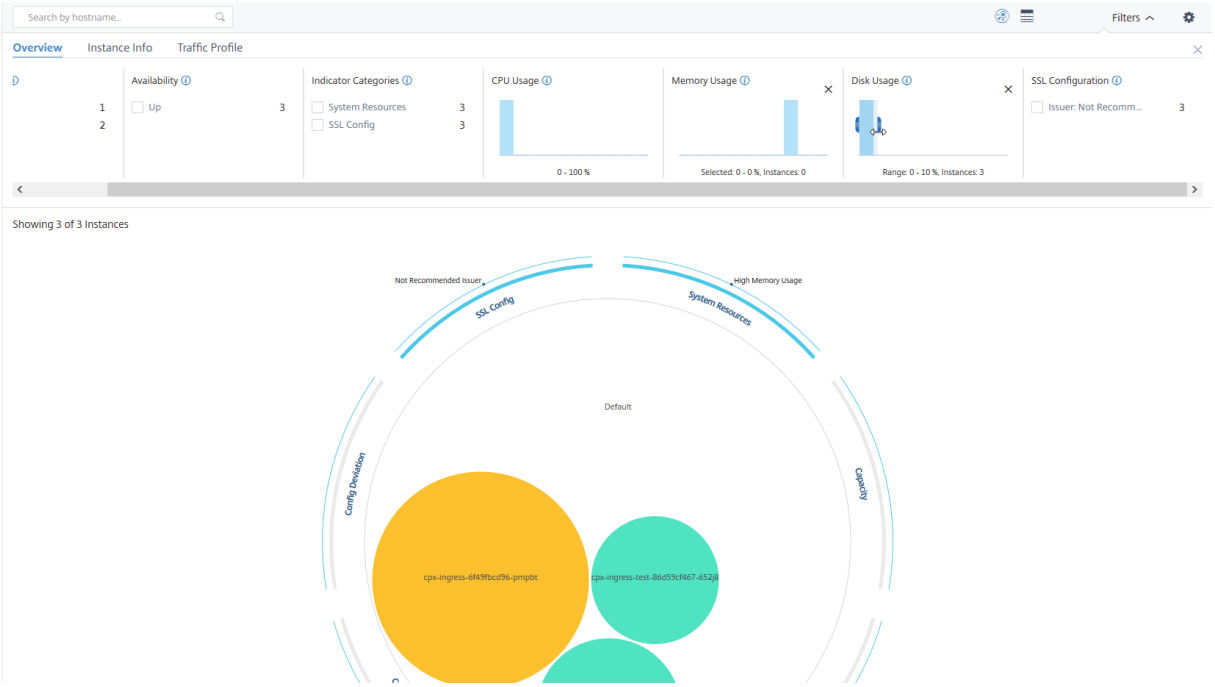
Ejemplo 2: Vea las instancias que consumen entre el 10 y el 20% de la memoria asignada:

En la sección de uso de memoria, haga clic en el gráfico de barras. La leyenda muestra que el rango seleccionado es del 10 al 20% y que hay 29 instancias que funcionan en ese rango.

También puede seleccionar varios rangos en estos histogramas.

Ejemplo 3: Vea las instancias que consumen mucho espacio en disco en varios rangos:

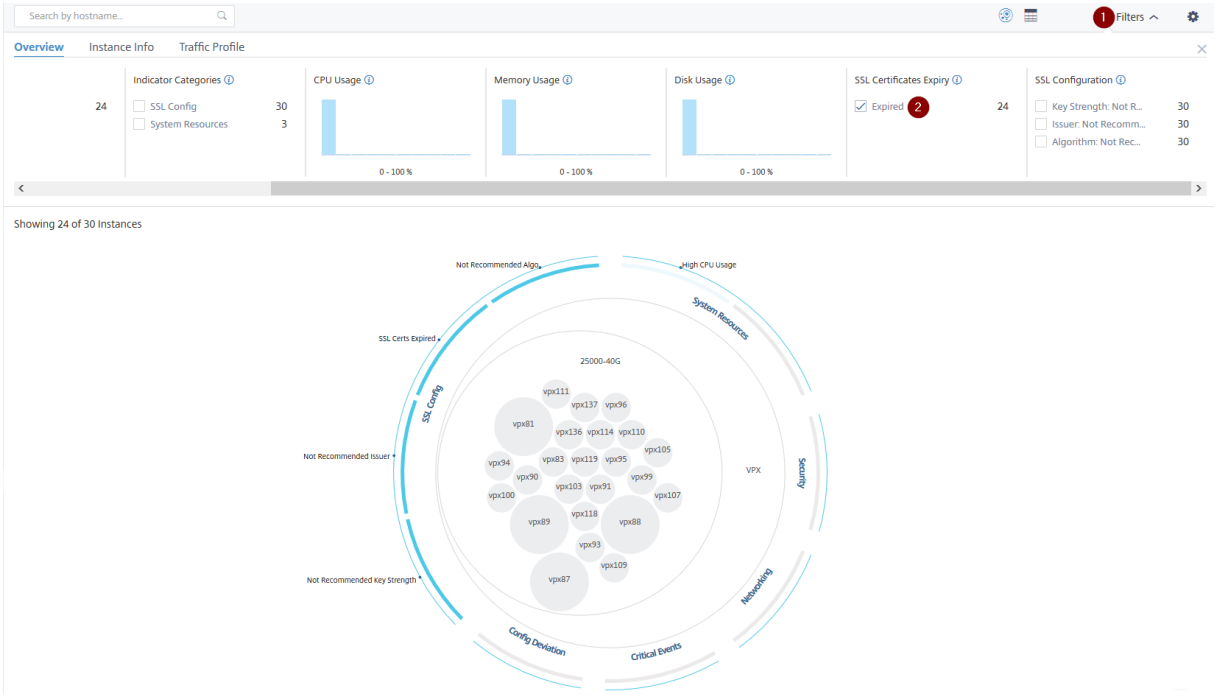
Para ver las instancias que han consumido espacio en disco entre un 0 y un 10%, arrastre el puntero del mouse sobre los dos rangos.



> **Nota**
>
> Haga clic en "X"para eliminar la selección. También puede hacer clic en **Restablecer** para eliminar varias selecciones.

Los gráficos de barras horizontales del panel **Descripción general** indican el número de instancias que informan de errores del sistema, eventos críticos y estado de caducidad de los certificados SSL. Seleccione la casilla de verificación para ver esas instancias.

Ejemplo 4: Ver instancias de certificados SSL caducados:



1: Haga clic en la lista **Filtro**.

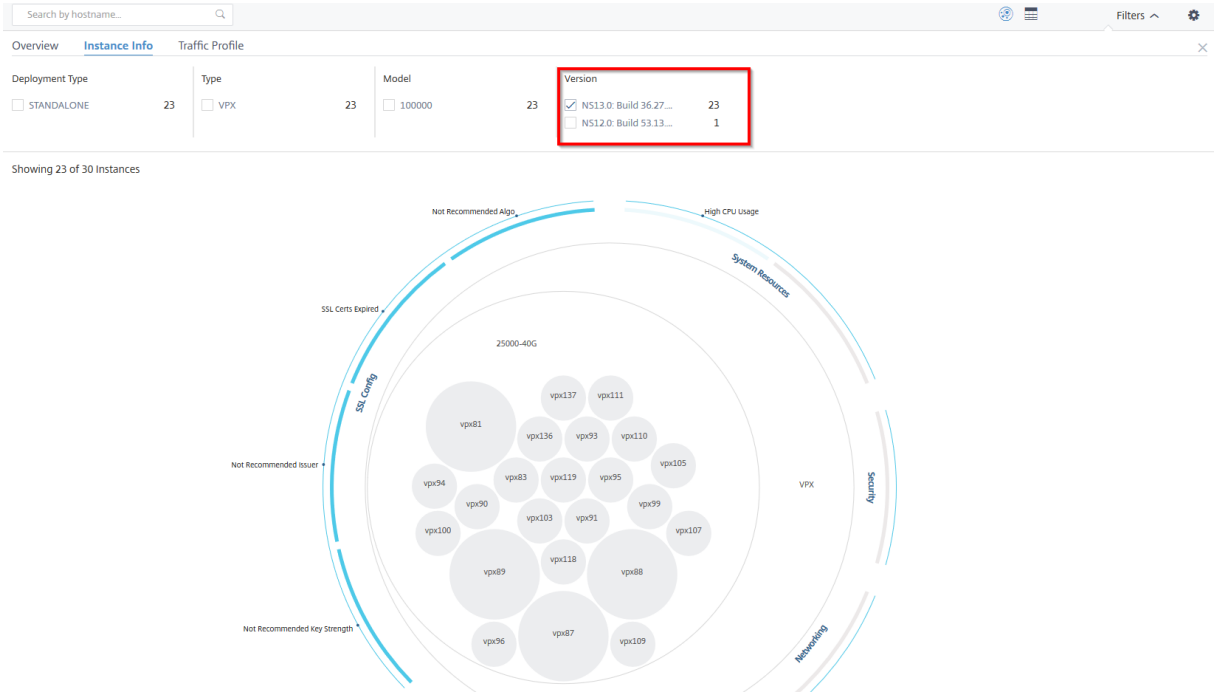
2 - En la sección **Caducidad de los certificados SSL**, seleccione la casilla de verificación **Vencidos** para ver las instancias.

Información de la instancia

El panel de **información de la instancia** le permite ver las instancias según el tipo de implementación, el tipo de instancia, el modelo y la versión de software. Puede seleccionar varias casillas de verificación para reducir la selección.

Ejemplo 5: Ver instancias de NetScaler VPX con un número de compilación específico:

Seleccione la versión que quiere ver.



Perfil de tráfico

Los histogramas del panel **de perfil de tráfico** representan un número agregado de instancias en función del rendimiento con licencia de las instancias, el número de solicitudes, conexiones y transacciones gestionadas por las instancias. Seleccione el gráfico de barras para ver las instancias de ese rango.

Ejemplo 6: Ver instancias que admiten conexiones TCP:

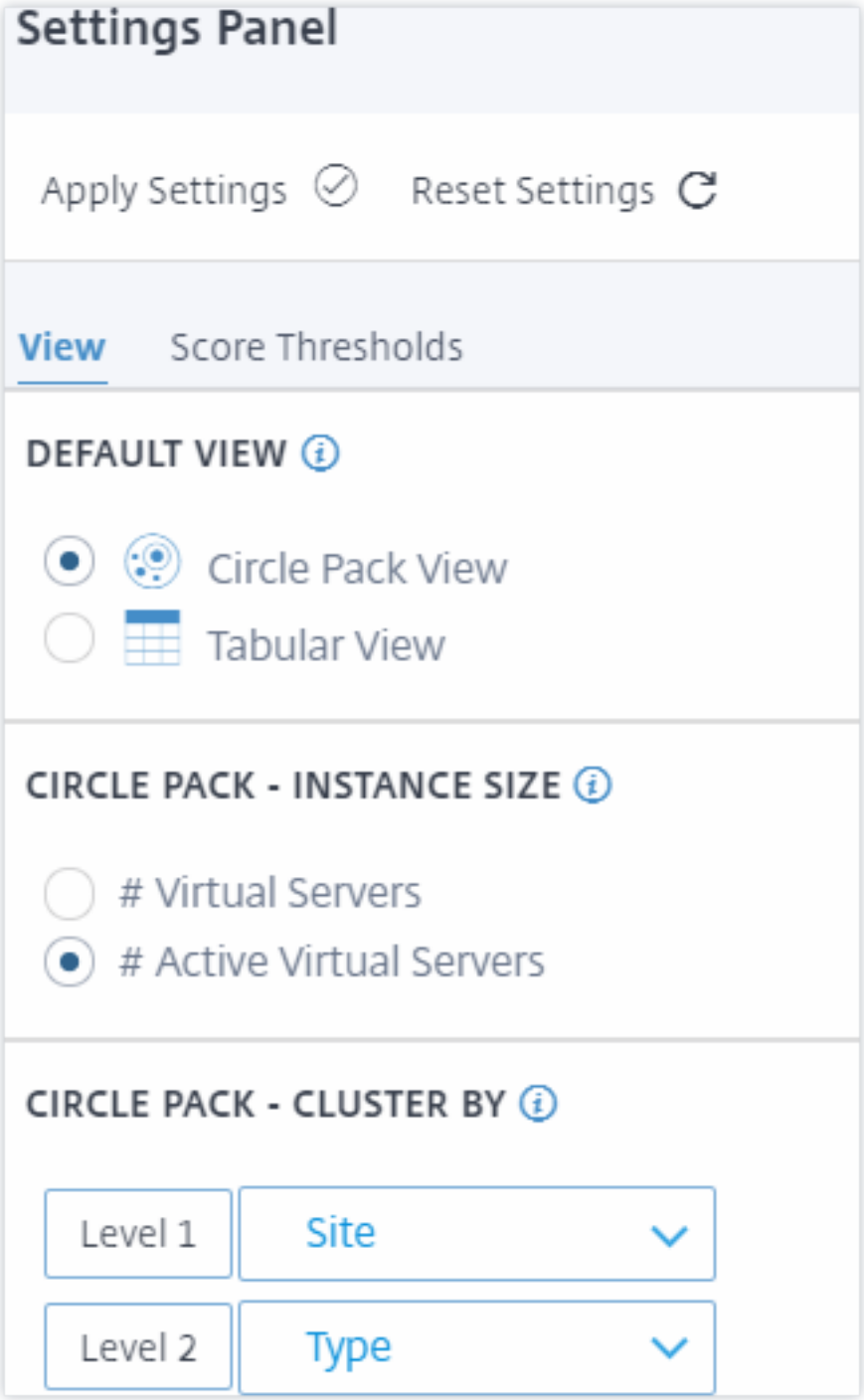
La siguiente imagen muestra el número de instancias que admiten conexiones TCP.

Cómo usar el panel de configuración

El panel de **configuración** le permite configurar la vista predeterminada de Infrastructure Analytics. También le permite establecer los valores de umbral bajos y altos para un uso elevado de la CPU, un uso elevado del disco y un uso elevado de la memoria. El panel de ajustes está dividido en dos fichas: Umbrales de visualización y puntuación.

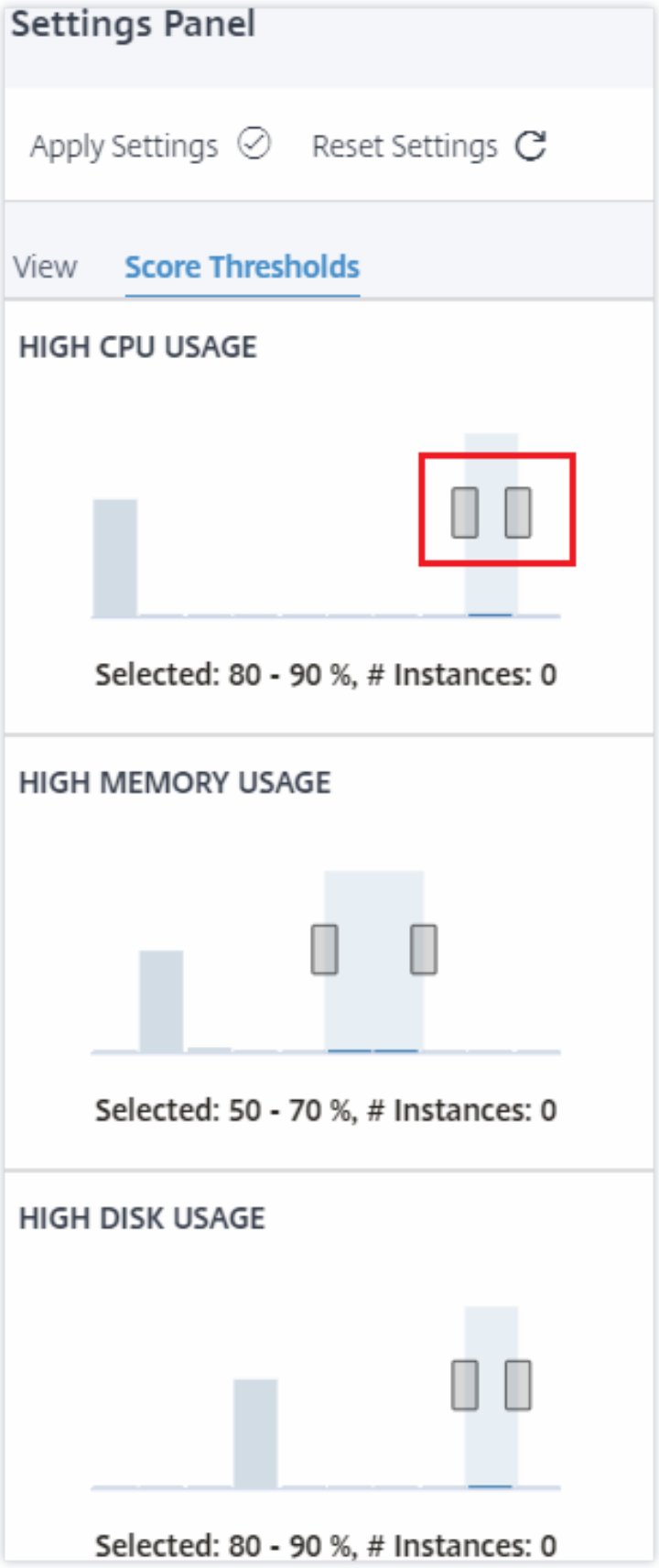
Ver

- **Vista predeterminada**. Seleccione el formato **Circle Pack** o Tabular como vista predeterminada en la página de análisis. El formato que selecciona es el que aparece cada vez que accede a la página en NetScaler ADM.
- **Paquete circular: tamaño de instancia**. Permita que el tamaño del círculo de instancias sea igual al número de servidores virtuales o al número de servidores virtuales activos.
- **Paquete Circle, Cluster By**. Decida el agrupamiento de dos niveles de los círculos de instancia. Para obtener más información sobre la agrupación en clústeres de instancias, consulta Círculos de instancias en clústeres.



Umbrales de puntuación

Puede modificar los valores de umbral bajo y alto para un uso elevado de CPU, memoria y disco en función de los requisitos de tráfico de su organización. Arrastre los controladores de cada uno de los Histograma de selección para establecer los valores.



> **Nota**
>
> Haga clic en **Aplicar configuración** para aplicar estos cambios o haga clic en **Restablecer** para eliminar todos los cambios.

Cómo visualizar los datos en el panel

Con Infrastructure Analytics, los administradores de red ahora pueden identificar las instancias que necesitan más atención en cuestión de segundos. Para entender la visualización de datos con más detalle, consideremos el caso de Chris, un administrador de red de ExampleCompany.

Chris mantiene muchas instancias de NetScaler en la organización. Algunas de las instancias procesan mucho tráfico y Chris necesita supervisarlas de cerca. Chris observa que algunas instancias con mucho tráfico ya no procesan todo el tráfico que pasa por ellas. Antes, para analizar esta reducción, Chris tuvo que leer varios informes de datos procedentes de diversas fuentes. Chris tuvo que pasar más tiempo tratando de correlacionar los datos manualmente y determinar qué instancias no están en un estado óptimo y necesitan atención.

Chris usa la función de análisis de infraestructura para ver visualmente el estado de todas las instancias.

Los dos ejemplos siguientes ilustran cómo Infrastructure Analytics ayuda a Chris en la actividad de mantenimiento:

Ejemplo 1: Para supervisar el tráfico SSL:

Chris observa en el Circle Pack que una instancia tiene una puntuación de instancia baja y que esa instancia se encuentra en estado "Crítico". Chris hace clic en esa instancia para ver cuál es el problema. El resumen de la instancia muestra que hay un error en la tarjeta SSL en esa instancia y que la instancia no puede procesar el tráfico SSL (el tráfico SSL se ha reducido). Chris extrae esa información y envía un informe al equipo para investigar el problema inmediatamente.

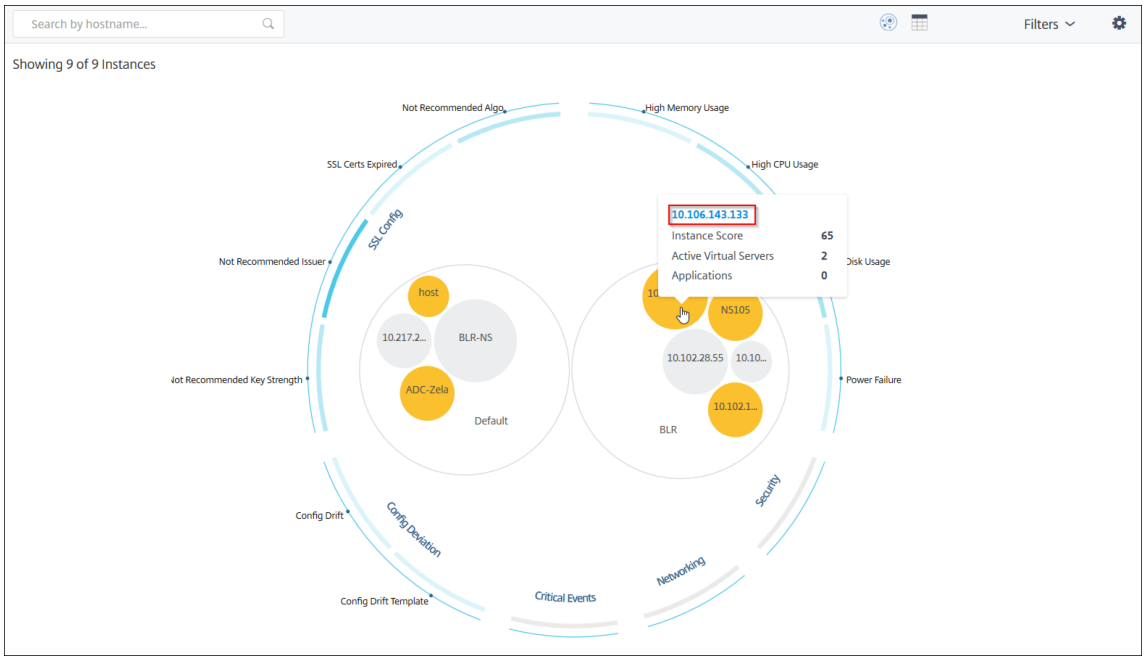
Ejemplo 2: Para supervisar los cambios de configuración:

Chris también observa que otra instancia está en estado "Revisar"y que recientemente se ha producido una desviación de configuración. Cuando Chris hace clic en el indicador de riesgo de desviación de configuración, se da cuenta de que se han realizado cambios de configuración relacionados con RC4 Cipher, SSL v3, TLS 1.0 y TLS 1.1, que podrían deberse a problemas de seguridad. Chris también observa que el perfil de tráfico de transacciones SSL de esta instancia ha disminuido. Chris exporta este informe y lo envía al administrador para indagar más.

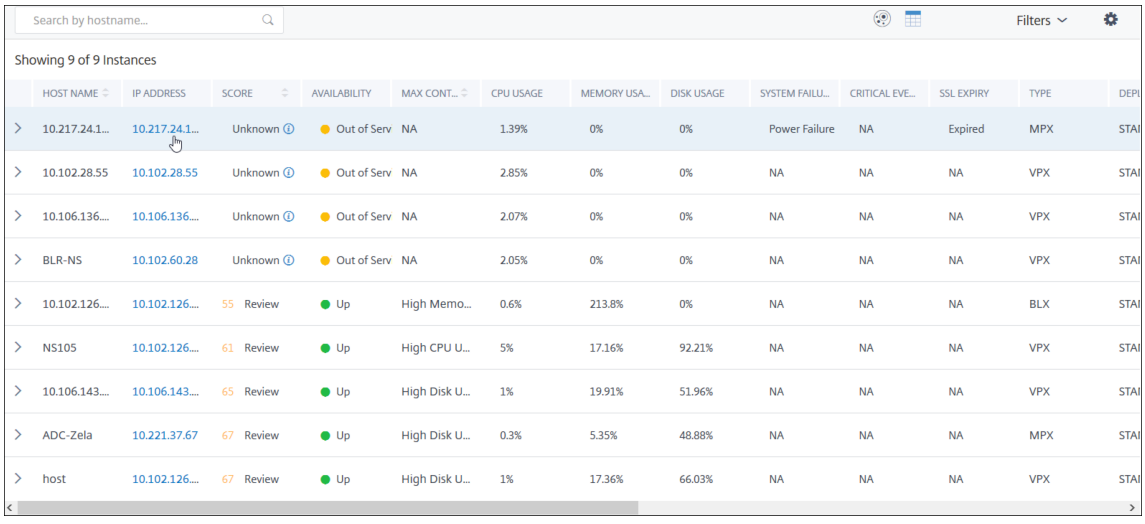
Ver detalles de instancia en Infrastructure Analytics

January 30, 2024

1. Vaya a **Infraestructura > Análisis de infraestructura**
2. Haga clic en la vista de paquete de círculo y seleccione la dirección IP.



También puede hacer clic en una dirección IP en la vista de tabla.



- **Nombre de host**: indica el nombre de host asignado a la instancia de ADC
- **Dirección IP**: indica la dirección IP de la instancia de ADC

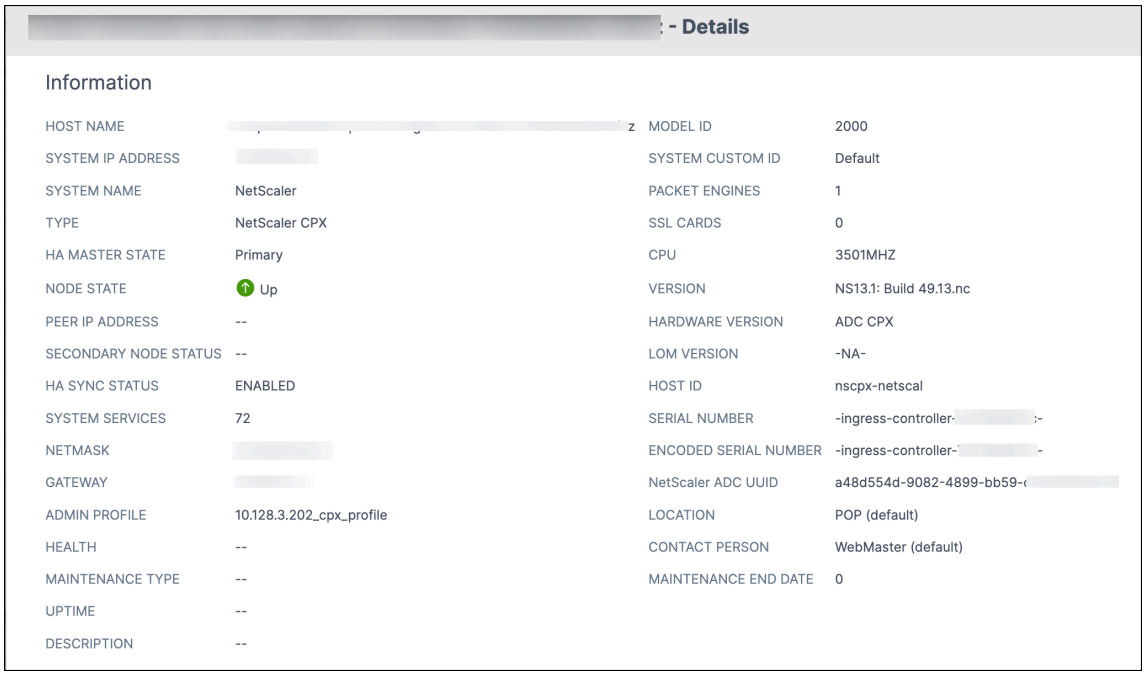
- **Puntuación**: Denota la puntuación de instancia ADC y el estado como Crítico, Bueno y Justo
- **Disponibilidad**: Indica el estado de la instancia de ADC, como **Activo**, **Inactivo**o **Fuera de servicio**.
- **Contribución máxima**: Indica la categoría de problema en la que la instancia de ADC tiene el número máximo de errores.
- **Uso de la CPU**: indica el% de CPU actual que utiliza la instancia
- **Uso de memoria**: indica el% de memoria actual que utiliza la instancia
- **Uso del disco**: indica el% de disco actual utilizado por la instancia
- **Fallo del sistema**: indica el número total de errores del sistema de instancias
- **Eventos críticos**: Indica la categoría de eventos en la que la instancia NetScaler tiene el máximo de eventos
- **Caducidad del SSL**: Indica el estado del certificado SSL instalado en la instancia de ADC
- **Tipo**: Indica el tipo de instancia ADC como VPX, SDX, MPX o CPX
- **Implementación**: indica si la instancia de ADC se implementa como una instancia independiente o un par de HA
- **Modelo**: indica el número de modelo de la instancia de ADC
- **Versión**: indica la versión y el número de compilación de la instancia ADC
- **Rendimiento**: indica el rendimiento de la red actual desde la instancia de ADC.
- **Solicitud de HTTPS por segundo**: indica las solicitudes HTTPS actuales por segundo recibidas por la instancia de ADC
- **Conexión TCP**: indica las conexiones TCP actuales establecidas
- **Transacción SSL**: indica las transacciones SSL actuales procesadas por la instancia de ADC
- **Sitio**: indica el nombre del sitio en el que está implementada la instancia de ADC.

> **Nota**
>
> Cada 5 minutos, se actualizan los valores actuales de uso de la CPU, de memoria, de disco, de rendimiento, etc.

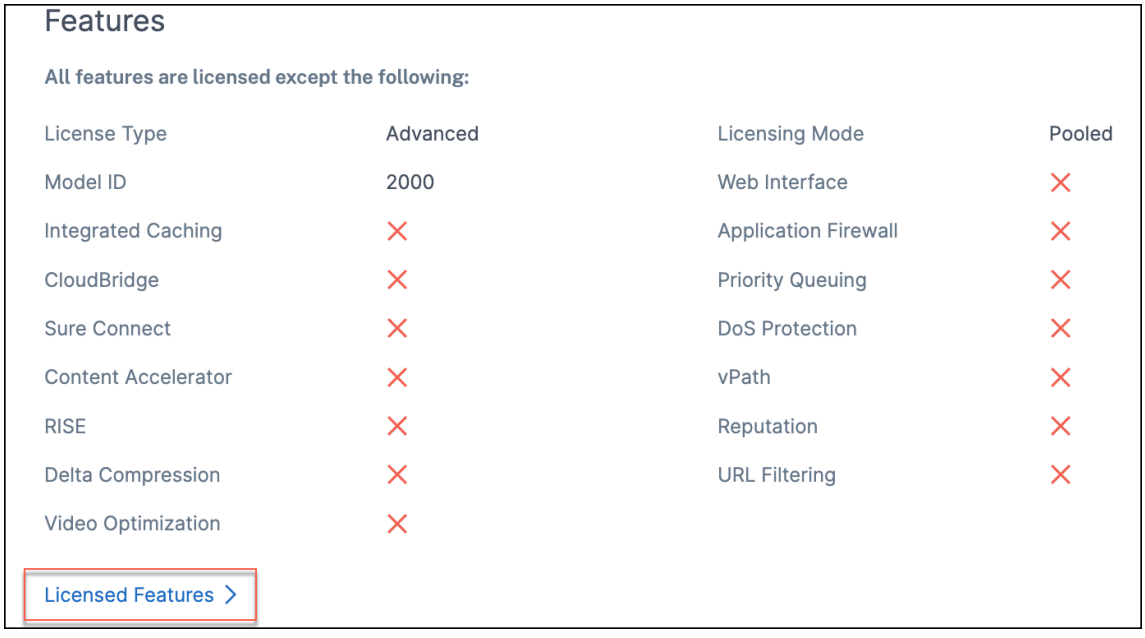
Haga clic en **Detalles de ejemplar** para ver los detalles.

Se muestran los siguientes detalles:

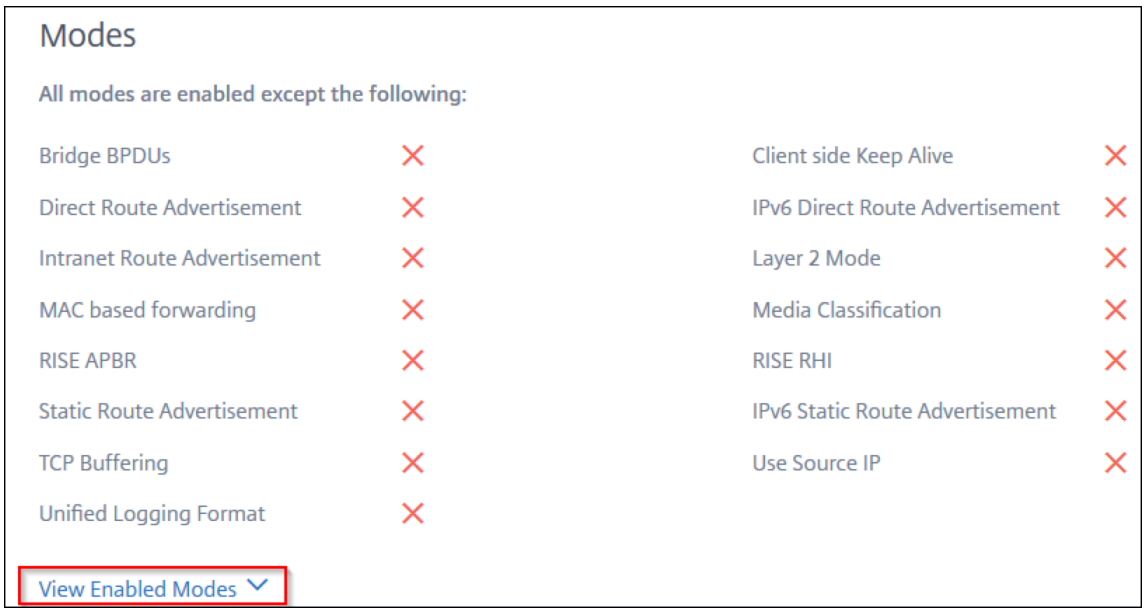
- **Información**: Detalles de la instancia, como el tipo de instancia, el tipo de implementación, la versión o el modelo.



- **Funciones**: de forma predeterminada, se muestran las funciones que no tienen licencia. Haga clic en **Funciones con licencia** para ver las funciones que tienen licencia.

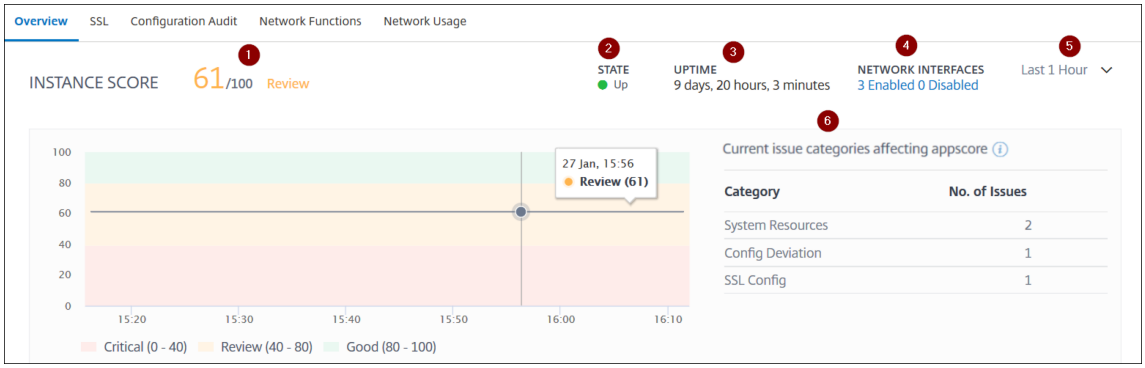


- **Modos**: de forma predeterminada, se muestran todos los modos que están inhabilitados en la instancia. Haga clic en **Ver modos habilitados** para ver los modos habilitados en la instancia.



El panel de instancias presenta una descripción general de la instancia en la que puede ver los siguientes detalles:

- **Puntuación de instancia**



1: indica la puntuación actual de la instancia de NetScaler durante el tiempo seleccionado. La puntuación final se calcula en **100 menos el total de penaltis**. El gráfico muestra los rangos de puntuación para la duración de tiempo seleccionada.

2: Indica el estado de la instancia de NetScaler, como **Activo**, **Inactivo** y **Fuera de servicio**.

3: indica el tiempo que la instancia de NetScaler está activa y en ejecución.

4: indica el total de interfaces de red habilitadas y inhabilitadas para la instancia. Haga clic para ver los detalles, como el nombre de la interfaz de red y el estado (habilitada o inhabilitada).

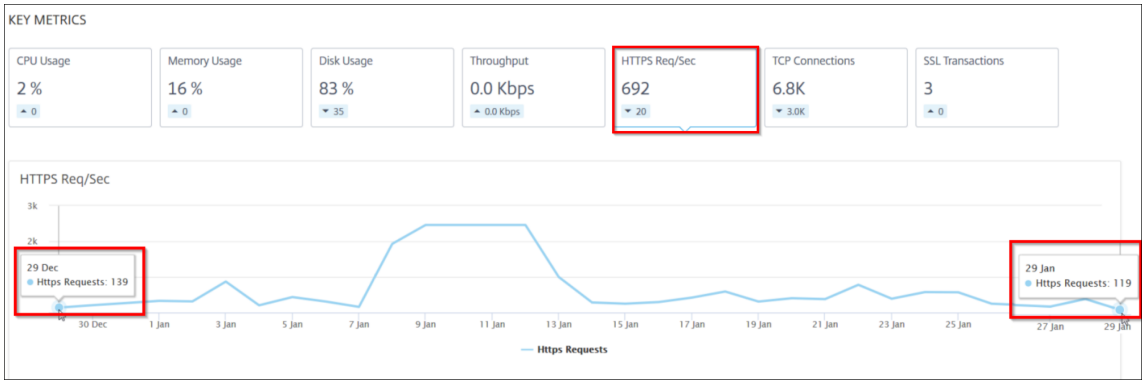
5 —Seleccione la duración del tiempo de la lista para ver los detalles de la instancia.

6: muestra el total de problemas y la categoría de problemas de la instancia de ADC.

- **Métricas clave**

Haga clic en cada ficha para ver los detalles. En cada métrica, puede ver el valor medio y el valor de diferencia para el tiempo seleccionado.

La siguiente imagen es un ejemplo de HTTPS Req/Sec y la duración seleccionada es de 1 hora. El valor **692** es la media de las Req/Sec de HTTPS para el mes de duración y el valor **20** es el valor de la diferencia. En el gráfico, el primer valor es **139** y el último valor es **119**. El valor de la diferencia es **139** —**119 = 20**.



Puede ver las siguientes métricas de instancia en un formato de gráfico para la duración de tiempo seleccionada:

- **Uso de CPU**: el% de CPU promedio de la instancia durante el tiempo seleccionado (se muestra tanto para la CPU de paquetes como para la CPU de administración).
- **Uso de memoria**: el% promedio de uso de memoria de la instancia durante el tiempo seleccionado.
- **Uso del disco**: el% medio de espacio en disco de la instancia durante el tiempo seleccionado.
- **Rendimiento**: el rendimiento de red promedio procesado por la instancia durante el tiempo seleccionado.
- **Solicitud de HTTPS por segundo**: el promedio de solicitudes HTTPs recibidas por la instancia durante el tiempo seleccionado.
- **Conexiones TCP**: el promedio de conexiones TCP establecidas por el cliente y el servidor durante el tiempo seleccionado.
- **Transacciones SSL**: el promedio de transacciones SSL procesadas por la instancia durante el tiempo seleccionado.

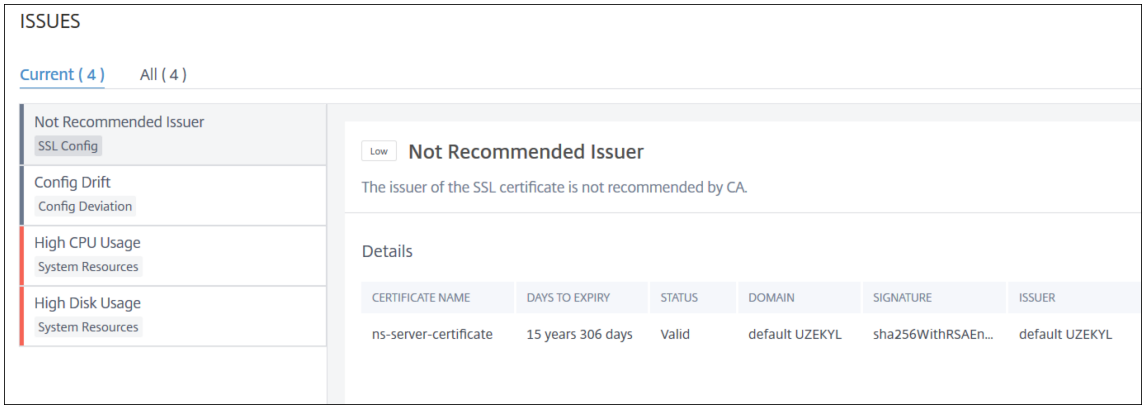
- **Problemas**

  Puede ver los siguientes problemas que se producen en la instancia de NetScaler:

Categoría de problema	Descripción	Problemas
Recursos del sistema	Muestra todos los problemas relacionados con los recursos del sistema NetScaler, como la CPU, la memoria y el uso del disco.	– Alto uso de CPU – Alto uso de memoria – Uso elevado del disco – Fallos en la tarjeta SSL – Fallo de alimentación – Error de disco – Error de flash – Descartes de NIC
Configuración SSL	Muestra todos los problemas relacionados con la configuración de SSL en la instancia de NetScaler.	– Los certificados SSL han caducado – Emisor no recomendado – Algoritmo no recomendado – No se recomienda la fuerza de la llave
desviación de configuración	Muestra todos los problemas relacionados con los trabajos de configuración aplicados en la instancia de NetScaler.	– Deriva de configuración – Ejecución vs plantilla
Eventos críticos	Muestra todos los eventos críticos relacionados con las instancias de NetScaler configuradas en el par HA y en el clúster.	– Fallo de Cluster Prop – Fallo de sincronización del clúster – Las versiones del clúster no coinciden

Categoría de problema	Descripción	Problemas
Redes	Muestra los problemas operativos que se producen en las instancias.	– HA: Estado secundario incorrecto – HA No Heat Beats – Fallo de sincronización de HA – No coincide la versión de HA Para obtener más información, consulte Análisis de infraestructura mejorados con nuevos indicadores.

Haga clic en cada ficha para analizar y solucionar el problema. Por ejemplo, considere que una instancia tiene los siguientes errores durante el tiempo seleccionado:



- La ficha **Actual** muestra los problemas que afectan actualmente a la puntuación de la instancia.
- La ficha **Todo** muestra todos los problemas de infraestructura detectados durante la duración seleccionada.

Ver los problemas de capacidad en una instancia de ADC

January 30, 2024

Cuando una instancia ADC ha consumido la mayor parte de su capacidad disponible, puede producirse la caída de paquetes al procesar el tráfico del cliente. Este problema provoca un bajo

rendimiento en una instancia de ADC. Al comprender estos problemas de capacidad del ADC, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento del ADC.

En la **vista Circle Pack**, puede ver los problemas de capacidad de la instancia de ADC si existe.

Para ver las cuestiones relativas a la capacidad de los CCA,

1. Vaya a **Infraestructura > Análisis de infraestructura**.
2. Seleccione la vista de paquete de círculos.

> **Nota**
>
> En **Infrastructure Analytics**, el paquete circular y las vistas tabulares muestran los eventos y problemas que ocurrieron en la última hora.

La siguiente ilustración sugiere los problemas de capacidad existentes en la instancia seleccionada:

Los problemas se clasifican según los siguientes parámetros de capacidad:

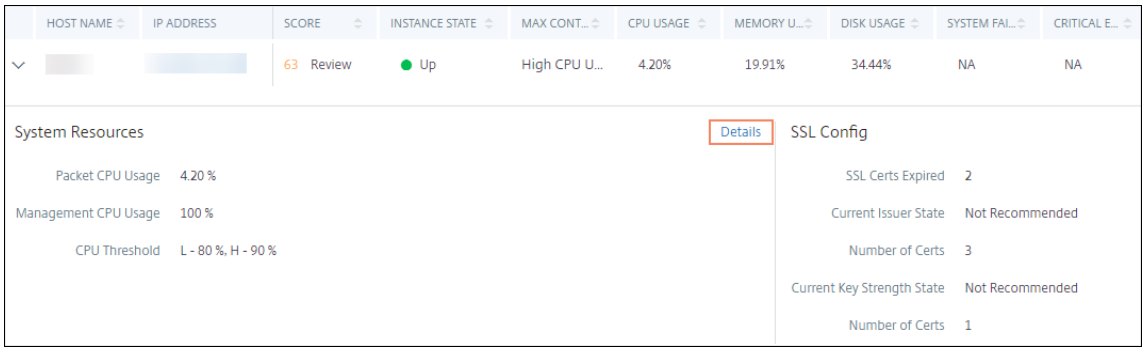
- **Límite de rendimiento alcanzado**: El número de paquetes descartados en la instancia una vez alcanzado el límite de rendimiento.
- **Se alcanzó el límite de CPU PE**: La cantidad de paquetes descartados en todas las NIC una vez alcanzado el límite de CPU PE.
- **Límite de PPS alcanzado**: la cantidad de paquetes descartados en la instancia después de alcanzar el límite de PPS.

- **Límite de velocidad de procesamiento de SSL**: Número de veces que se ha alcanzado el límite de rendimiento de SSL
- **Límite de velocidad SSL TPS**: El número de veces que se ha alcanzado el límite de SSL TPS.

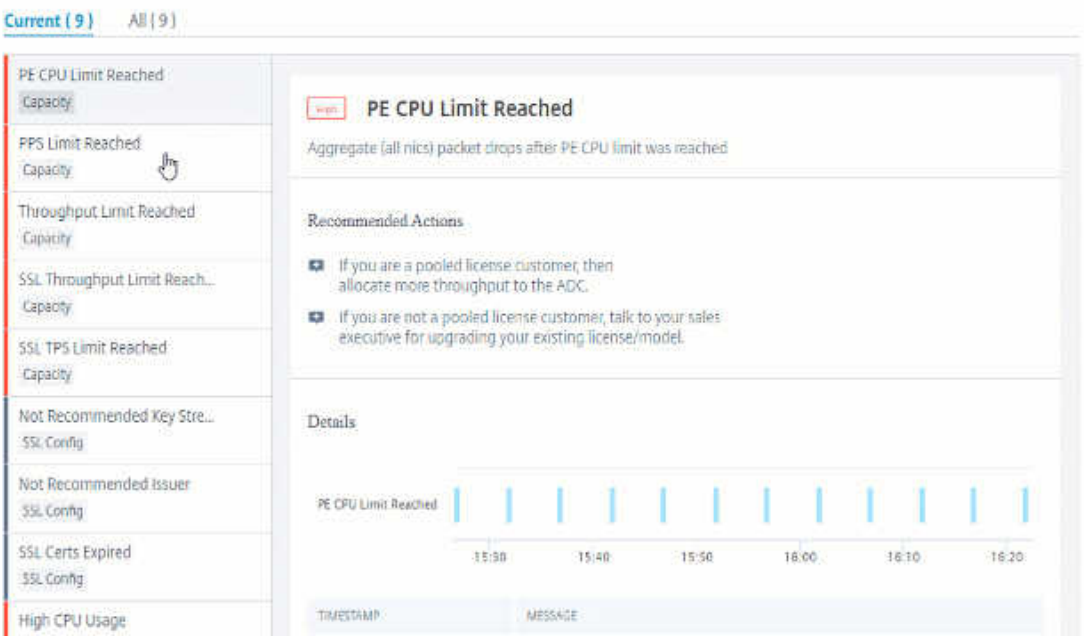
Vea las acciones recomendadas para resolver problemas de capacidad

El ADM recomienda acciones que puedan resolver problemas de capacidad. Para ver las acciones recomendadas, realice los siguientes pasos:

1. En **Infraestructura > Análisis de infraestructura**, seleccione la vista tabular.
2. Seleccione la instancia que tiene problemas de capacidad y haga clic en **Detalles**.



3. En la página de instancias, desplázate hacia abajo hasta la sección **Problemas**.
4. Seleccione cada problema y consulte las acciones recomendadas para resolver los problemas de capacidad.



El ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra las caídas de paquetes o incrementos de contador de límite de velocidad, si existe.

El ADM calcula la puntuación de la instancia en el umbral de capacidad definido.

- **Umbral bajo**: 1 incremento del contador de límite de velocidad o caída de paquetes
- **Umbral alto**: Incremento del contador de límite de velocidad o caída de 10000 paquetes

Por lo tanto, cuando una instancia de ADC infringe el umbral de capacidad, la puntuación de la instancia se ve afectada.

Cuando los paquetes caen o el contador de límite de velocidad aumenta, se genera un evento bajo la categoría `ADCCapacityBreach`. Para ver estos eventos, vaya a **Cuentas > Eventos del sistema**.

Análisis de infraestructura mejorado con nuevos indicadores

January 30, 2024

Con NetScaler ADM Infrastructure Analytics, puede:

- Vea un nuevo conjunto de problemas operativos que se producen en las instancias de NetScaler.
- Consulta los mensajes de error y consulta las recomendaciones para solucionar los problemas.

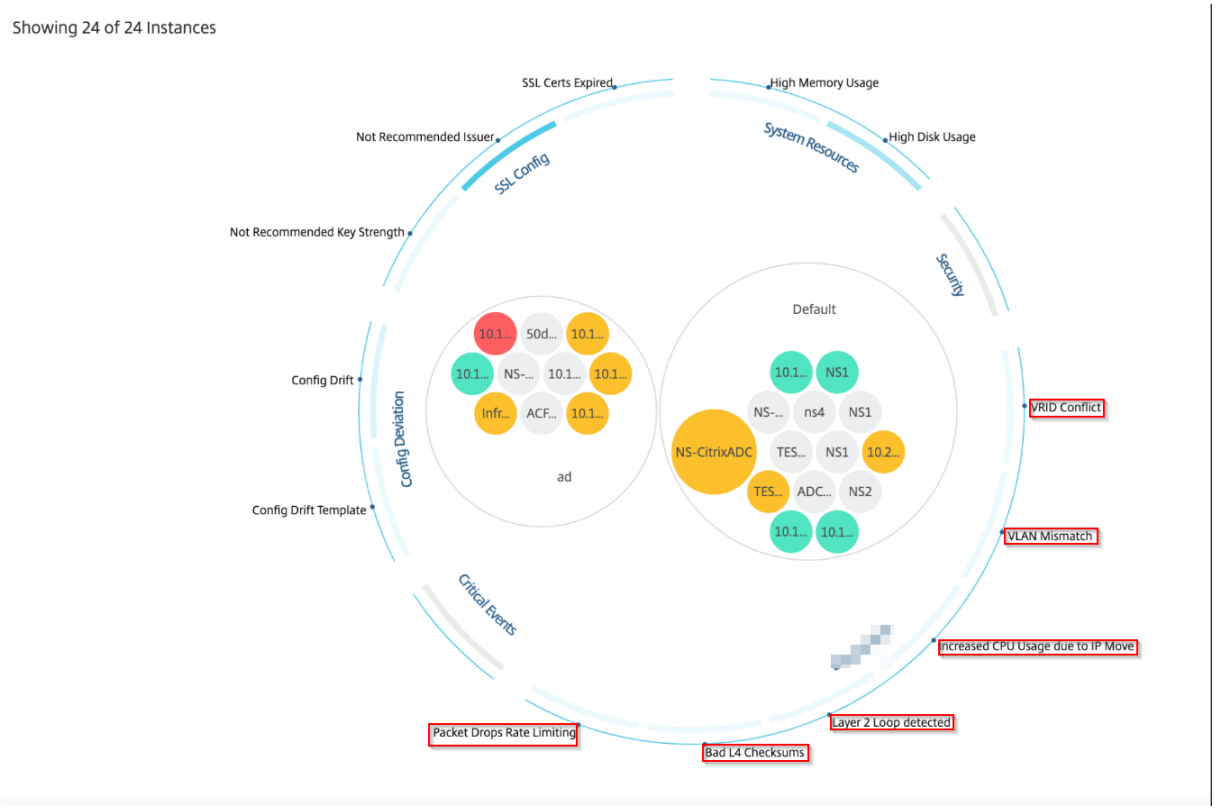
Como administrador, puede identificar rápidamente la causa principal del análisis de los problemas.

> **Nota**
>
> Los indicadores de reglas no son compatibles con:
>
> - Instancias de NetScaler configuradas en modo de clúster.
> - Instancias NetScaler configuradas con particiones de administración.

En NetScaler ADM, vaya a **Infraestructura > Análisis de infraestructura** para ver los indicadores de:

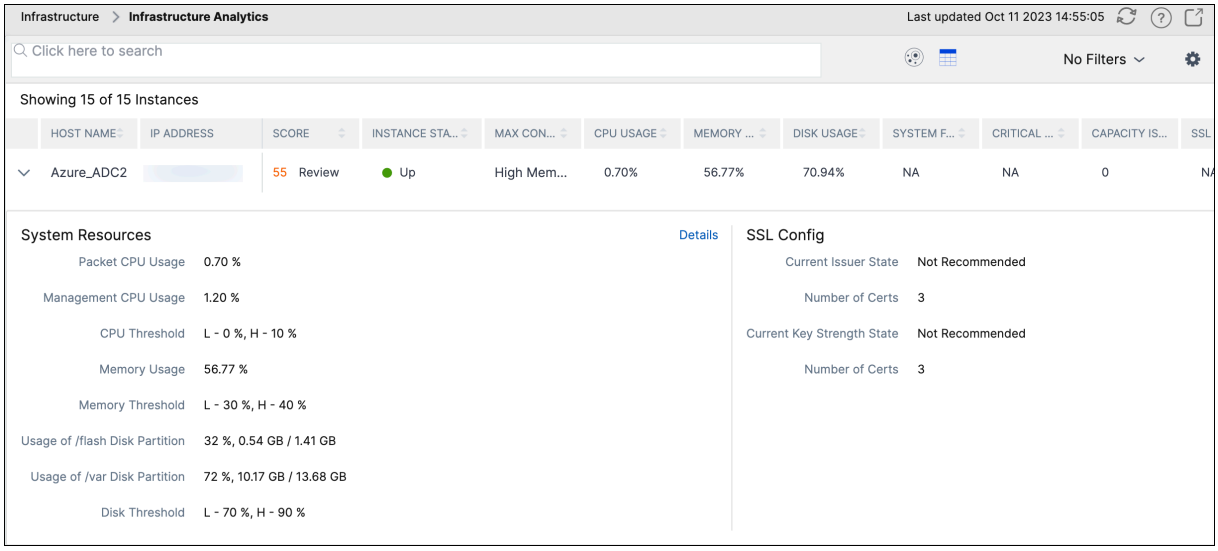
Nombre del indicador en Infrastructure Analytics	Descripción
Error de asignación de puertos	Detecta cuándo NetScaler usa SNIP para comunicarse con una nueva conexión de servidor y el total de puertos disponibles en ese SNIP está agotado. La acción recomendada es agregar otro SNIP en la misma subred.

Nombre del indicador en Infrastructure Analytics	Descripción
No hay configuración de ruta predeterminada	Detecta cuándo se interrumpe el tráfico debido a la falta de disponibilidad de rutas.
Conflicto de IP	Detecta si se configura o se aplica una misma dirección IP en dos o más instancias de una red.
Conflicto de VRID	Detecta cuando se producen problemas de acceso intermitentes para el VRID especificado.
Discordancia de VLAN	Detecta si se produce algún error durante la configuración de la VLAN enlazada a las subredes IP.
Ataque de ventana pequeña TCP	Detecta si hay un posible ataque a una ventana pequeña en curso. Esta alerta es solo a título informativo, porque ADC ya mitiga este ataque.
umbral de control de velocidad	Detecta cuándo se descartan paquetes según el umbral de control de velocidad configurado.
Límite de persistencia	Detecta cuándo se impone el máximo de visitas a la memoria NetScaler.
No coincide el nombre del sitio de GSLB	Detecta cuándo se producen errores de sincronización de la configuración de GSLB debido a una falta de coincidencia en
Encabezado IP con formato incorrecto	Detecta cuándo fallan las comprobaciones de seguridad de los paquetes IPv4.
Sumas de comprobación L4 incorrectas	Detecta si la validación de la suma de comprobación para los paquetes TCP falla.
Mayor uso de CPU debido al movimiento de IP	Detecta si es necesario actualizar un gran número de equipos Mac.
Dirección excesiva de paquetes	Detecta altos niveles de dirección de paquetes de software debido al uso del tipo de clave rss asimétrica.
Loop de capa 2	Detecta la presencia de bucles de capa 2 en la red.
Discordancia de VLAN etiquetada	Detecta cuándo se reciben paquetes de VLAN etiquetados en una interfaz sin etiquetar.



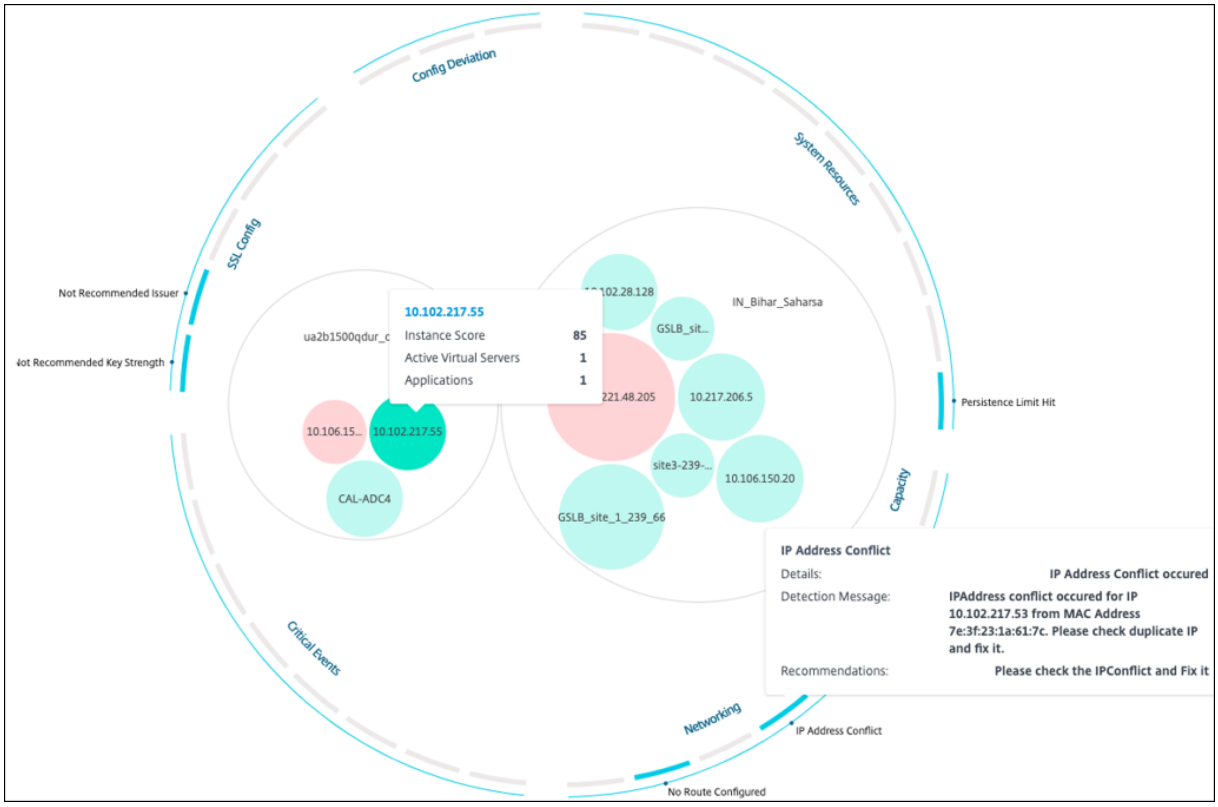
Vista tabular

También puede ver anomalías mediante la opción de vista tabular en **Infrastructure Analytics**. Vaya a **Infraestructura > Análisis de infraestructura** y, a continuación, haga clic en  para mostrar todas las instancias administradas. Haga clic en › para ampliar y obtener más información



Ver detalles de una anomalía

Por ejemplo, si desea ver los detalles del **conflicto de direcciones IP** en la red, haga clic en la anomalía que aparece en relación con el conflicto de direcciones IP para ver los detalles.



- **Detalles**: Indica qué anomalía se ha detectado
- **Mensaje de detección**: Indica la dirección MAC para la que la dirección IP tiene el conflicto
- **Recomendaciones**: Indica el elemento de acción para resolver este conflicto de direcciones IP

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 NetScaler ADM o una versión posterior. 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 mientras configura el servidor NetScaler ADM por primera vez o más tarde. Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de NetScaler, 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.

Una vez que haya agregado una instancia, puede eliminarla navegando a **Infraestructura > Instancias y haciendo** clic en **Todas las instancias**. En la página Instancias, seleccione la instancia que quiere eliminar y haga clic en **Quitar**.

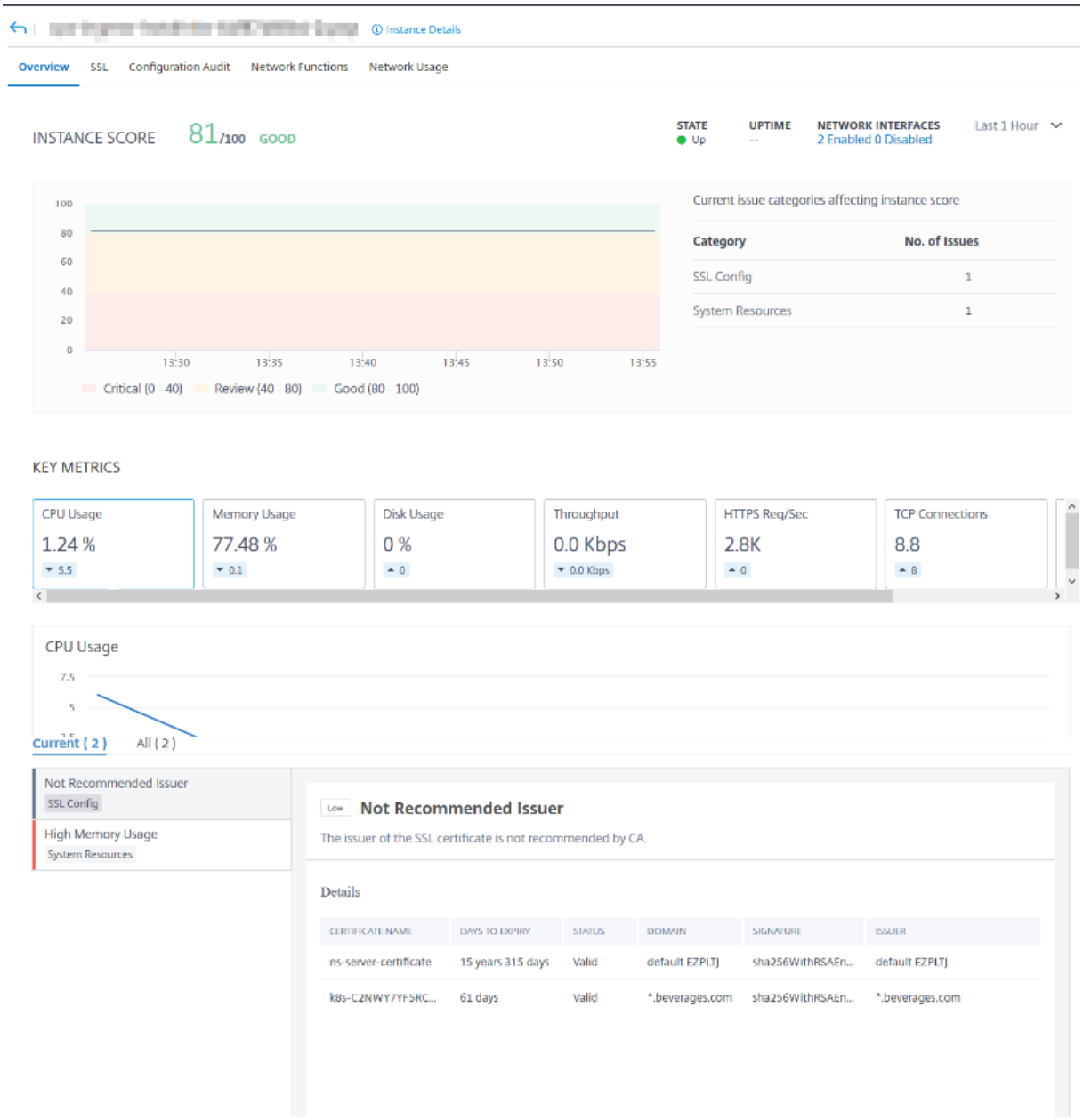
Cómo usar el panel de instancias

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 **Infraestructura > 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.

  Para obtener más información, consulte Detalles de la instancia.

- **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 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 puede hacer clic en el icono "más"situado en la esquina inferior derecha de la pantalla para agregar 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.

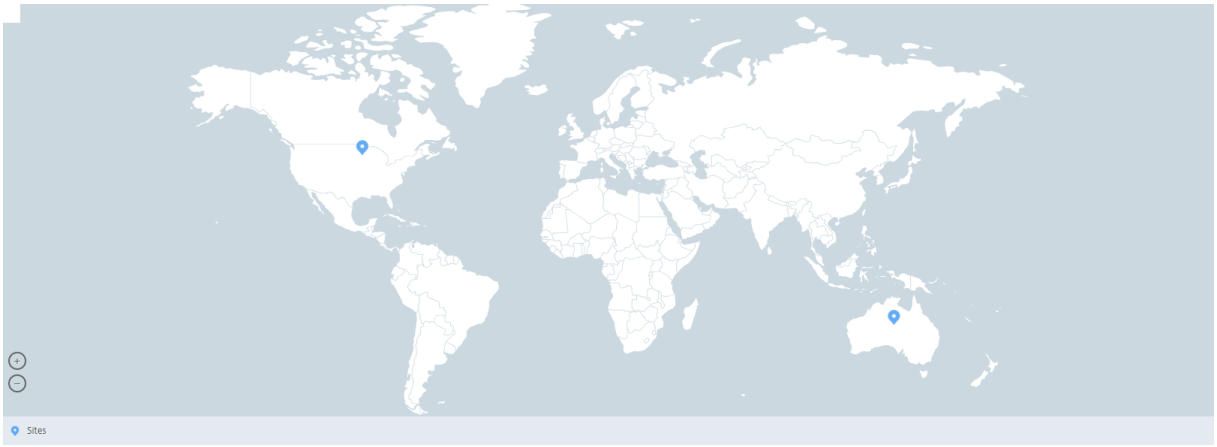
En la siguiente sección se explica cómo puede supervisar los centros de datos en NetScaler ADM.

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 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.

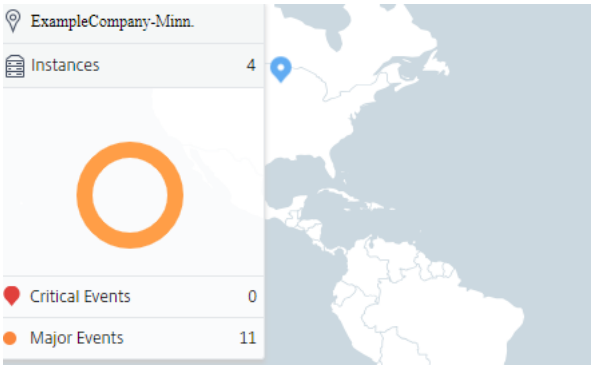
Geomaps en NetScaler ADM le proporciona una representación gráfica de sus sitios. Geomaps también desglosa su experiencia de supervisión de red por área geográfica. Con las geometrías, puede visualizar la distribución de instancias de red por ubicación y supervisar todos los problemas de red. Puede navegar a la página **Infraestructura > Instancias** 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.

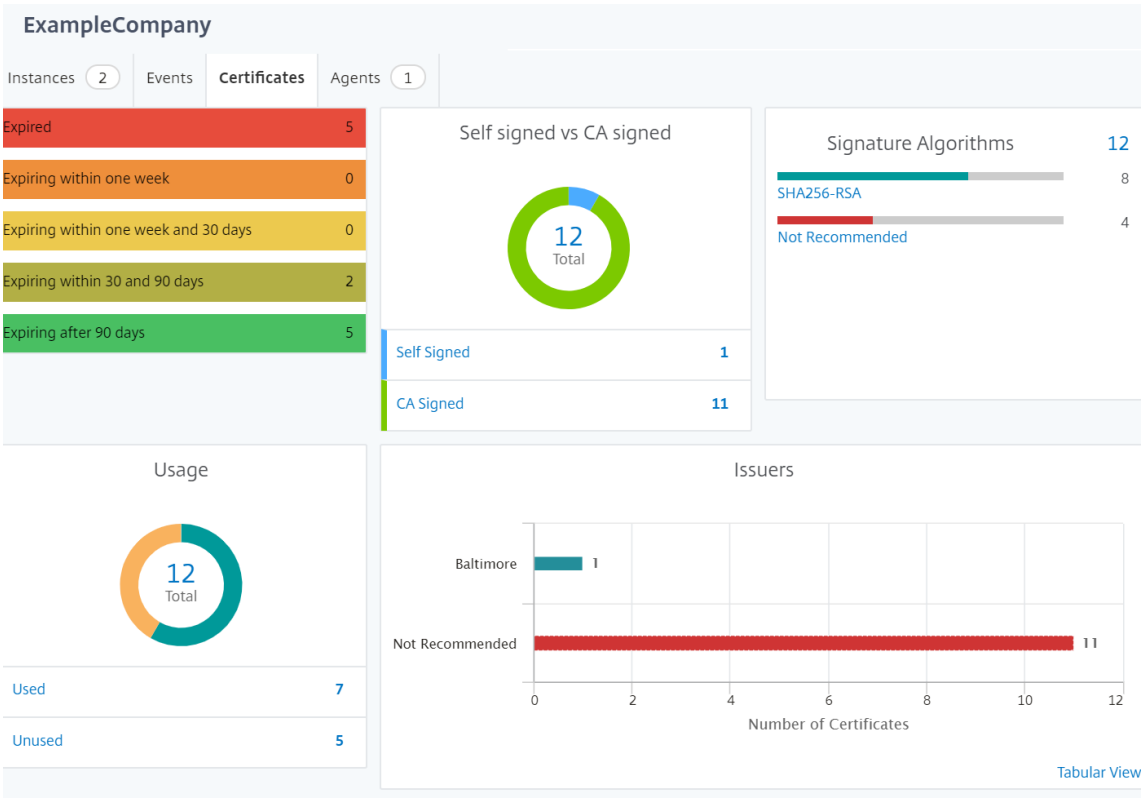


Haga clic en las fichas para ver más información:

- 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.

- 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 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 y el agente.

Para obtener más información sobre cómo agregar instancias de NetScaler, consulte Agregar instancias.

Para crear sitios:

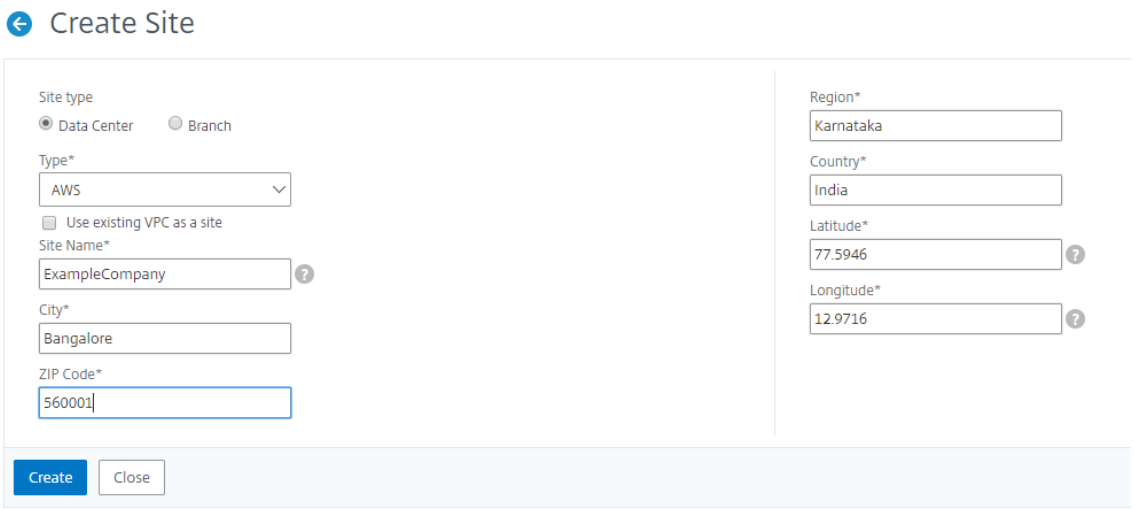
Cree sitios antes de agregar instancias en NetScaler ADM. Proporcionar información de ubicación le permite localizar el sitio con precisión.

Vaya a**Infraestructura > Instancias > 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.
    i) **Longitud**: Escriba la longitud de la ubicación.
2. Haga clic en **Create**.

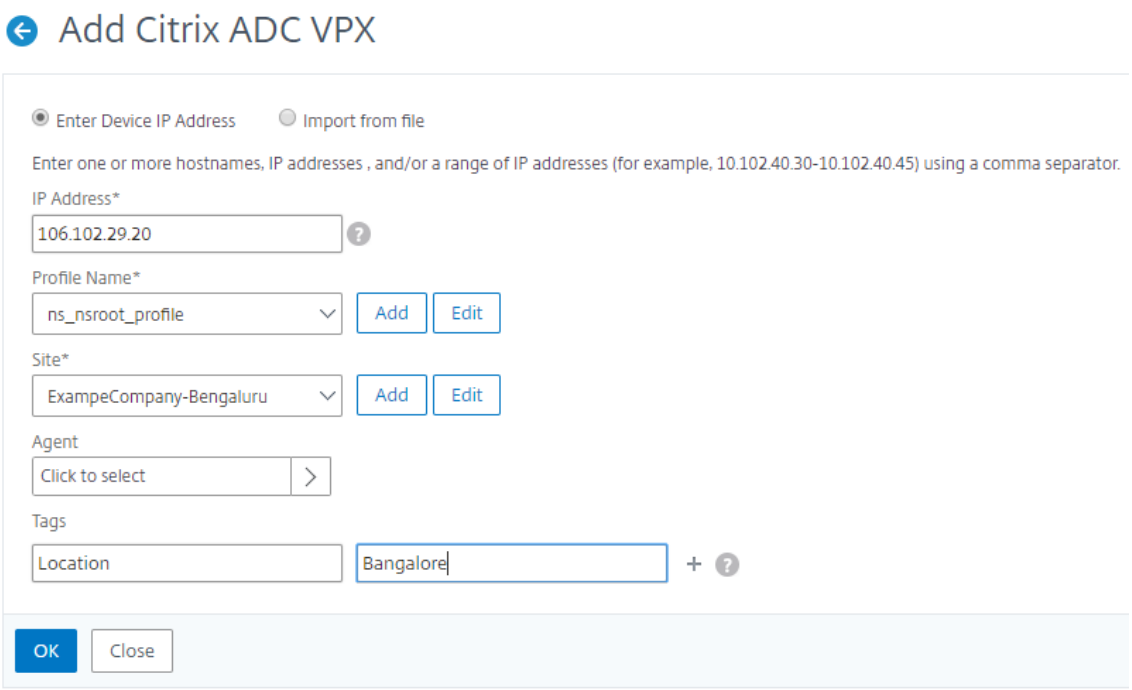


Para agregar instancias y seleccionar sitios:

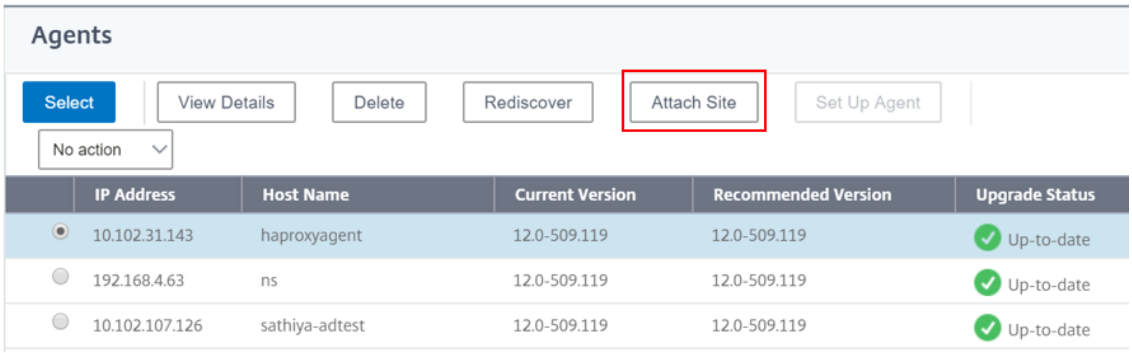
Tras crear los sitios, debe agregar instancias en NetScaler ADM. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

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 NetScaler ADM, vaya a **Infraestructura**> Instancias.
2. Seleccione el tipo de instancia que quiere crear y haga clic en **Agregar**.
3. En la página **Agregar NetScaler 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**.



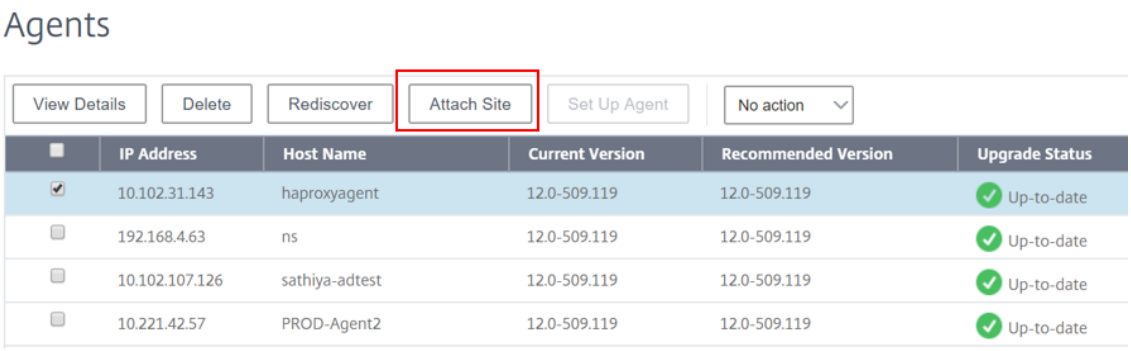
1. Seleccione el sitio de la lista y haga clic en **Guardar**.

1. Haga clic en **Aceptar**.

También puede adjuntar un agente a un sitio navegando a **Infraestructura > Instancias > Agentes**.

Para asociar un agente NetScaler ADM al sitio:

1. En NetScaler ADM, vaya a **Infraestructura > Instancias > 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 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

NetScaler Application Delivery Management (ADM) ahora le permite asociar sus instancias de Citrix Application Delivery Controller (ADC) a 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 comprender cómo el etiquetado de instancias le ayuda a supervisarlas mejor.

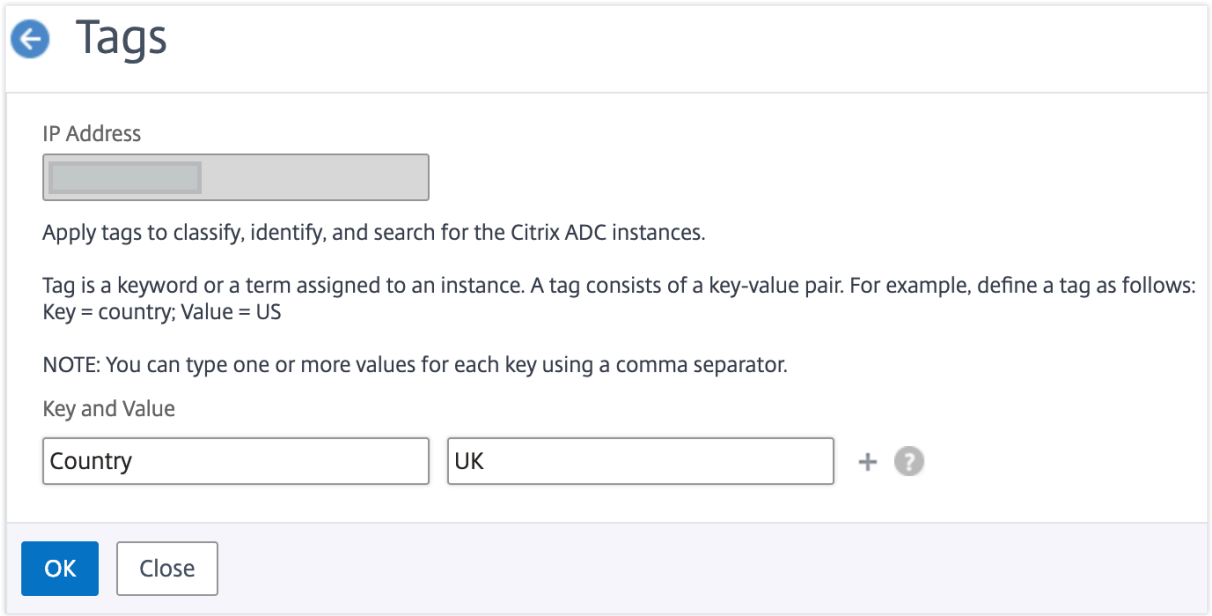
- **Caso de uso 1**: puede crear una etiqueta para identificar todas las instancias en el Reino Unido. Aquí, puede crear una etiqueta con la clave como "País"y el valor como "Reino Unido". Esta etiqueta le ayuda a buscar y supervisar todas esas instancias en el Reino Unido.
- **Caso de uso 2**: Quiere buscar instancias que se encuentran en el entorno provisional. Aquí, puede crear una etiqueta con la clave como "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 de uso 3**: considere una situación en la que quiera conocer la lista de instancias de NetScaler que se encuentran en el área "Swindon"en el Reino Unido y que son propiedad de usted, David T. Puede crear etiquetas para todos estos requisitos y asignarlas a todas las instancias que cumplan estas condiciones.

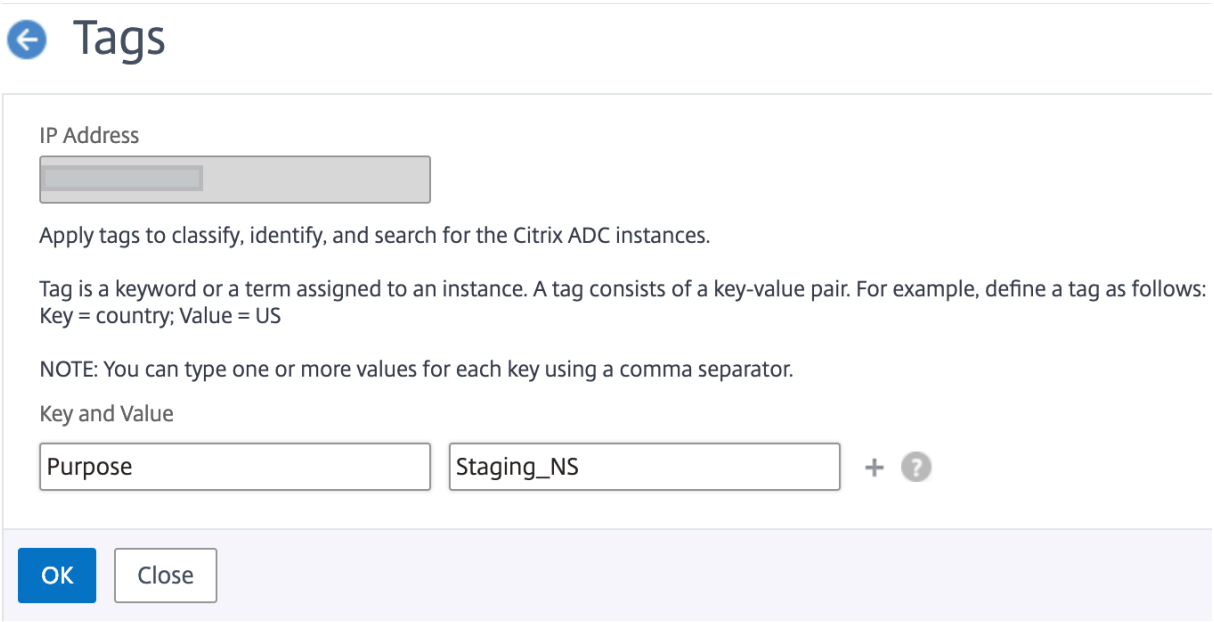
Para asignar etiquetas a la instancia de NetScaler VPX:

1. En NetScaler ADM, vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione la ficha **NetScaler VPX**.
3. Seleccione el NetScaler VPX requerido.
4. Haga clic en **Etiquetas**.
5. Cree etiquetas y haga clic en **Aceptar**.

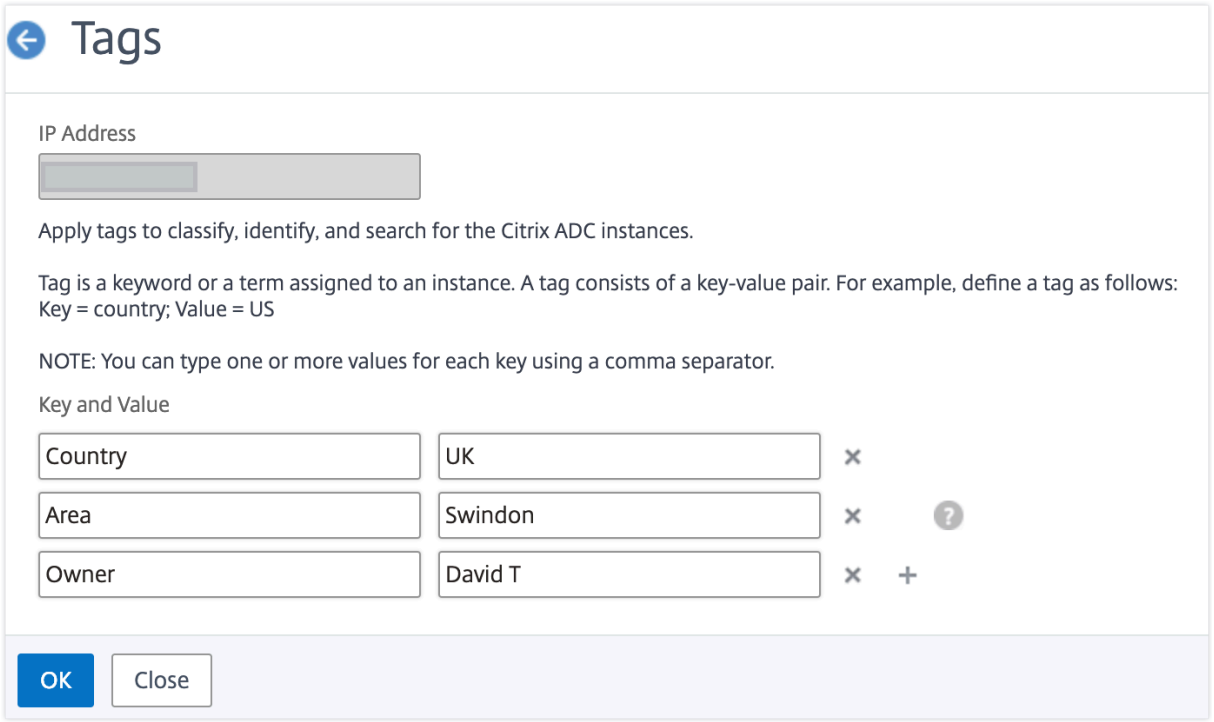
La ventana de **etiquetas** que aparece le permite crear sus propios pares de "clave-valor"asignando valores a cada palabra clave que cree.

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.



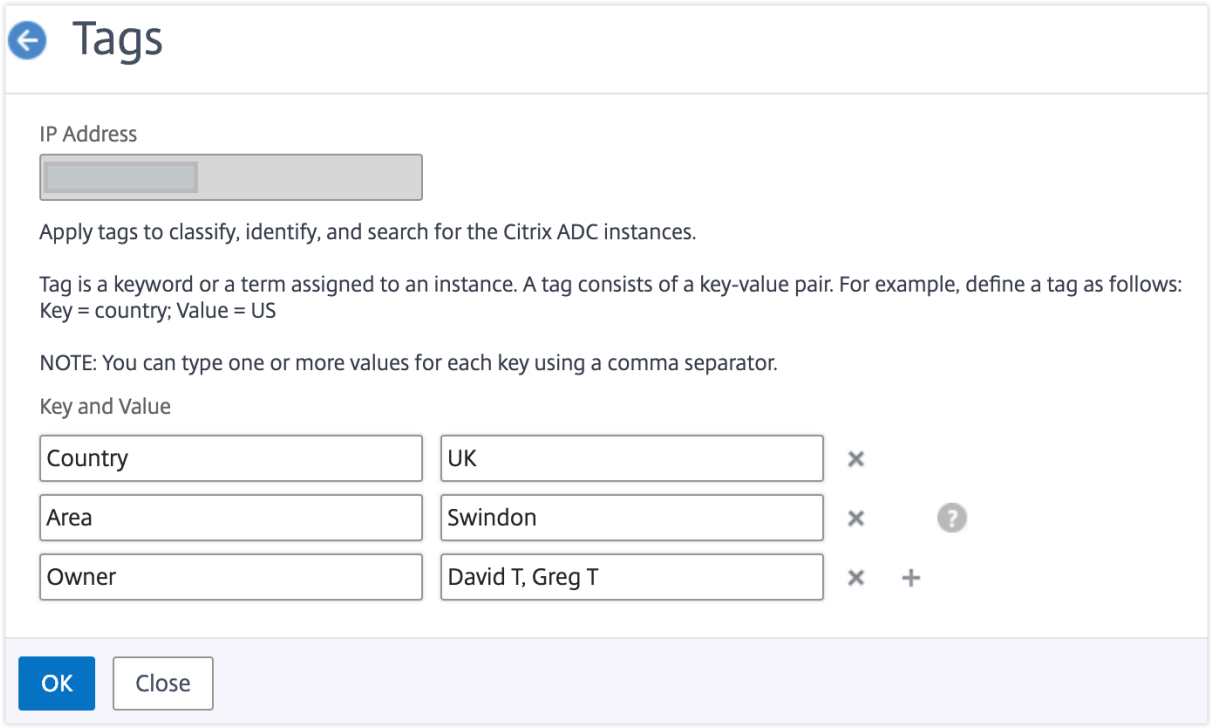


También puede agregar varias etiquetas haciendo clic en "+. "La adición de etiquetas múltiples y significativas le permite buscar de manera eficiente las instancias.



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 en función de etiquetas, consulte Cómo buscar instancias mediante 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 haber una situación en la que NetScaler Application Delivery Management (ADM) administre muchas instancias de NetScaler. 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 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 para agregar alguna descripción adicional sobre la instancia de NetScaler. Ahora puede asociar sus instancias de NetScaler con etiquetas. Estas etiquetas se pueden usar para identificar y buscar mejor las instancias de NetScaler.

- **Propiedades**. Cada instancia de NetScaler 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 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.

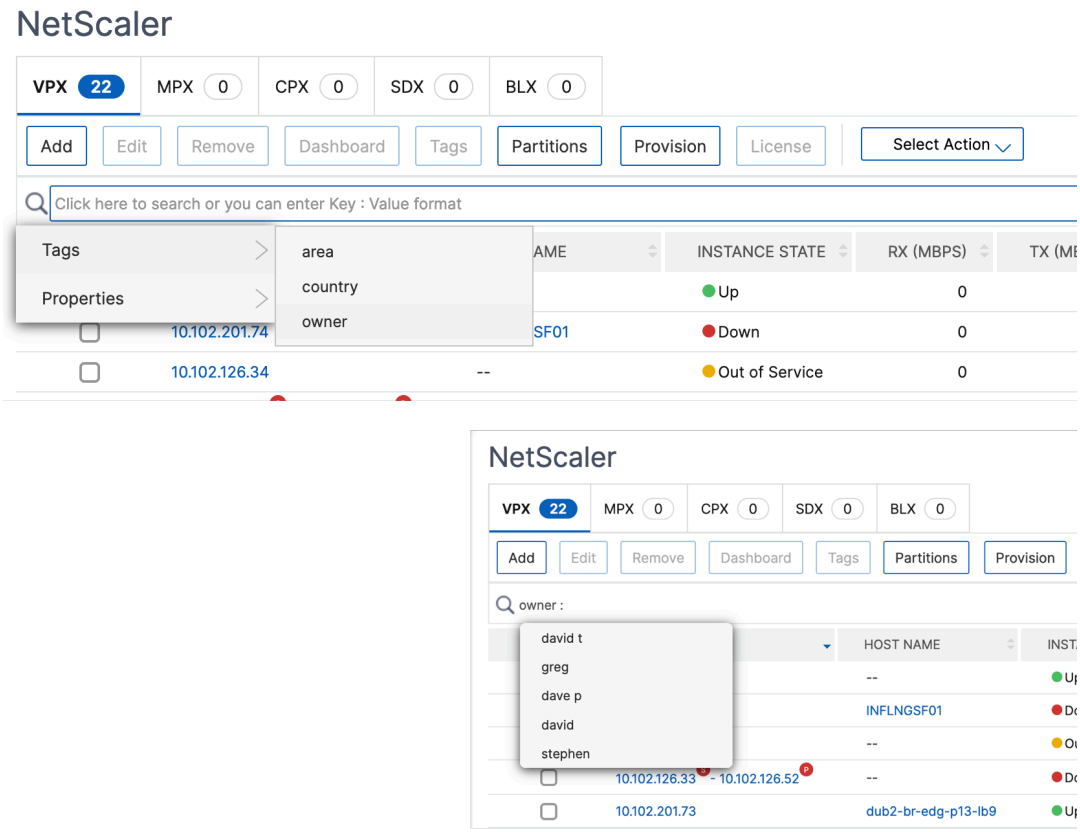
Puede utilizar una combinación de etiquetas y propiedades para crear sus propios criterios de búsqueda.

Para buscar instancias de NetScaler VPX

1. En NetScaler ADM, vaya a la ficha **Infraestructura > Instancias > NetScaler** > **VPX**.
2. Haga clic en el campo de búsqueda. Puede crear una expresión de búsqueda mediante etiquetas o propiedades o combinando ambas.

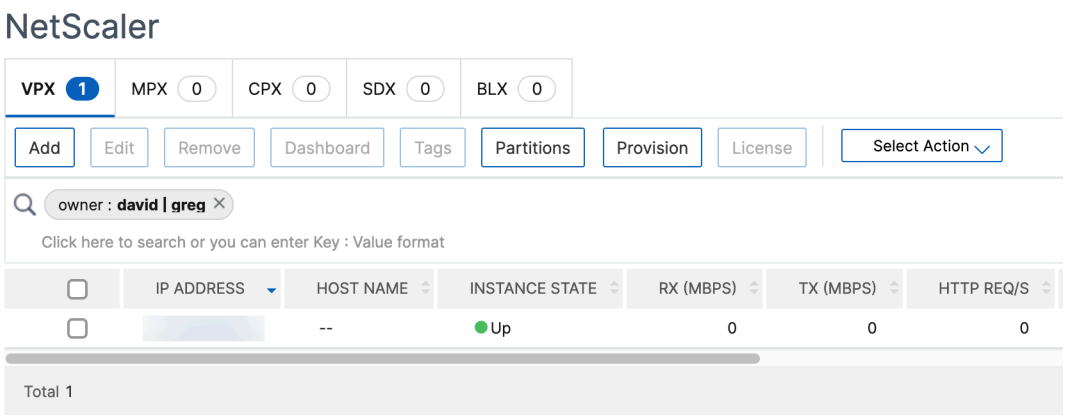
   Los siguientes ejemplos muestran cómo puede utilizar la expresión de búsqueda de manera eficiente para buscar la instancia.

   a) Seleccione la opción **Etiquetas** y seleccione **Propietario**. Selecciona "David T."

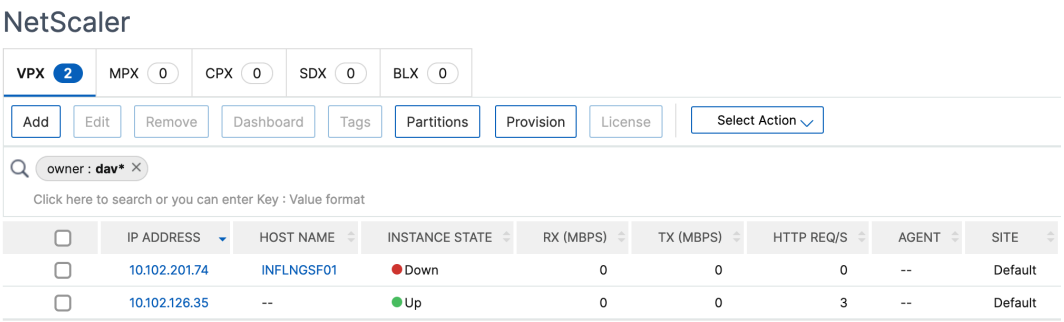


NetScaler ADM admite expresiones regulares y caracteres comodín en las expresiones de búsqueda.

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 propiedad de 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

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 particiones diferentes en la misma instancia de NetScaler. Se puede asignar un administrador de red para administrar varias particiones en varias instancias de NetScaler.

NetScaler Application Delivery Management (ADM) proporciona una forma sencilla de administrar todas las particiones que son propiedad de 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, las particiones de administración configuradas en esa instancia de NetScaler se agregan al sistema automáticamente.

Tenga en cuenta que tiene dos instancias de NetScaler 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 10.102.29.120 tiene p1 y p2 como se muestra en la imagen siguiente.

Para ver las particiones, vaya a**Infraestructura > Instancias > NetScaler > 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.

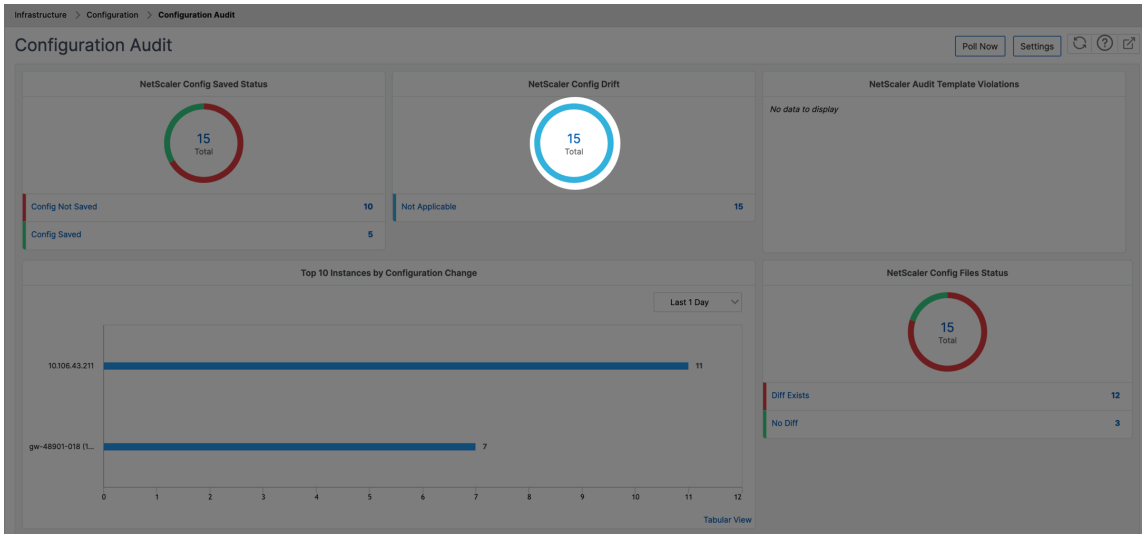
En primer lugar, debe crear dos grupos con los permisos adecuados (por ejemplo, permisos de administrador) e incluir las instancias de partición de administración necesarias en cada grupo. Por ejemplo, cree el grupo de sistemas partition1-admin y añada las particiones de administración de NetScaler 10.102.29.120-p1 y 10.102.216.49-Partition_1 a este grupo. Cree también el grupo de sistemas partition2-admin y añada las particiones de administración de NetScaler 10.102.29.120-p2, 10.102.216.49-Partition_2 y 10.102.216.49-Partition_3 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.

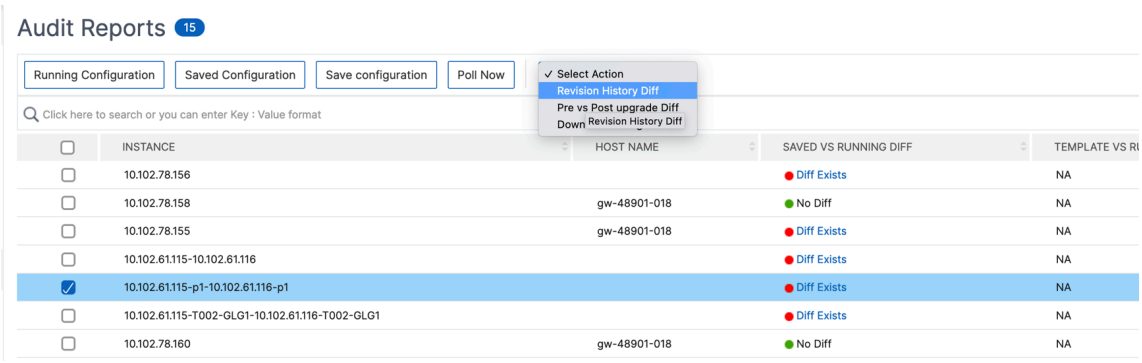
La diferencia en el historial de revisiones de la partición de administración le permite ver la diferencia entre los cinco archivos de configuración más recientes de una instancia de NetScaler particionada. Puede comparar los archivos de configuración entre sí (por ejemplo, la revisión de configuración 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:

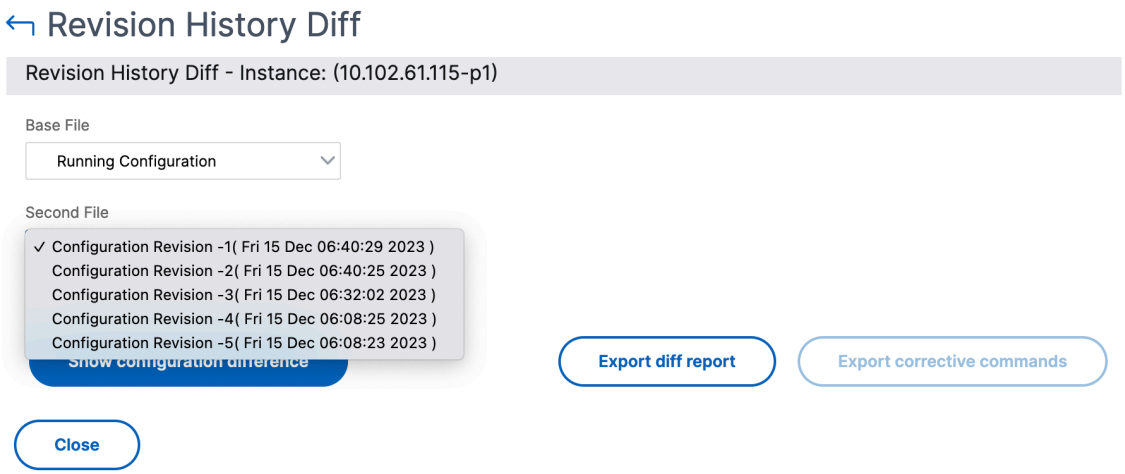
1. Vaya a **Infraestructura > Auditoría de configuración.** Haga clic dentro del gráfico de donut que representa el estado de configuración de instancia. En la página **Informes de auditoría** que se abre, haga clic en la instancia de NetScaler particionada.



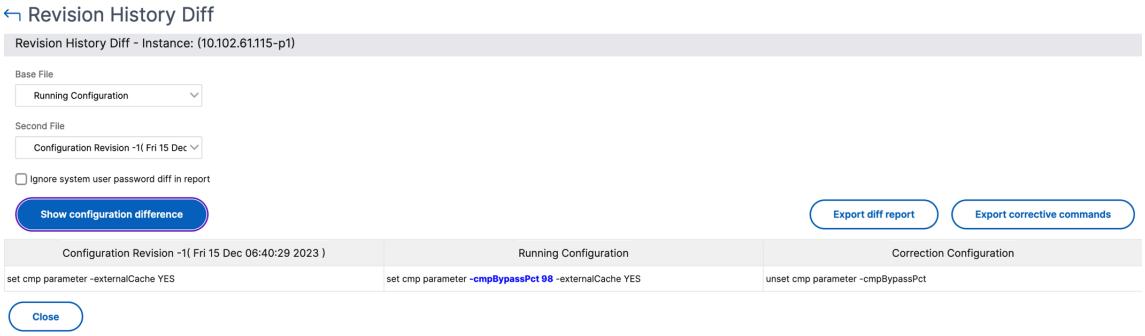
2. En el menú **Acción**, haga clic en Diferencia del **historial de revisiones.**



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**.



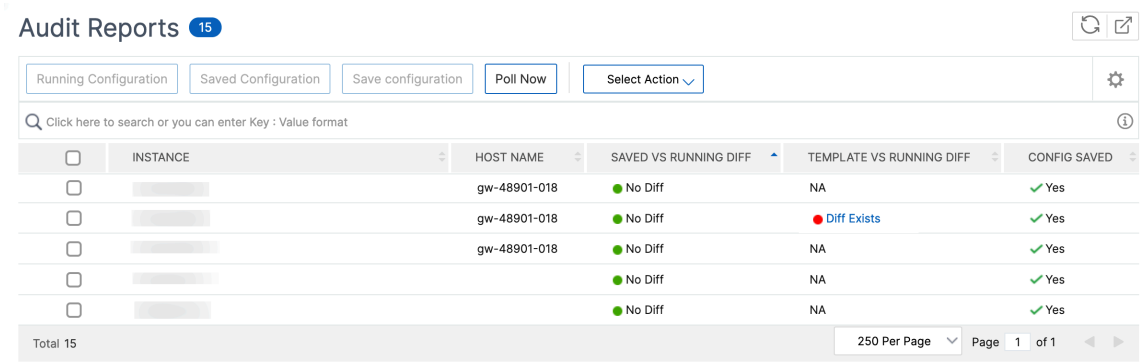
4. A continuación, puede ver la diferencia entre los cinco archivos de configuración más recientes para la instancia de NetScaler con particiones seleccionada, como se muestra a continuación. También puede ver los comandos de configuración correctiva y exportar estos comandos correctivos a la carpeta local. Estos comandos correctivos son los comandos que deben ejecutarse en el archivo base para obtener la configuración al estado deseado (archivo de configuración que se está utilizando 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 con particiones.



2. Si hay alguna diferencia entre la plantilla de auditoría y la diferencia 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.

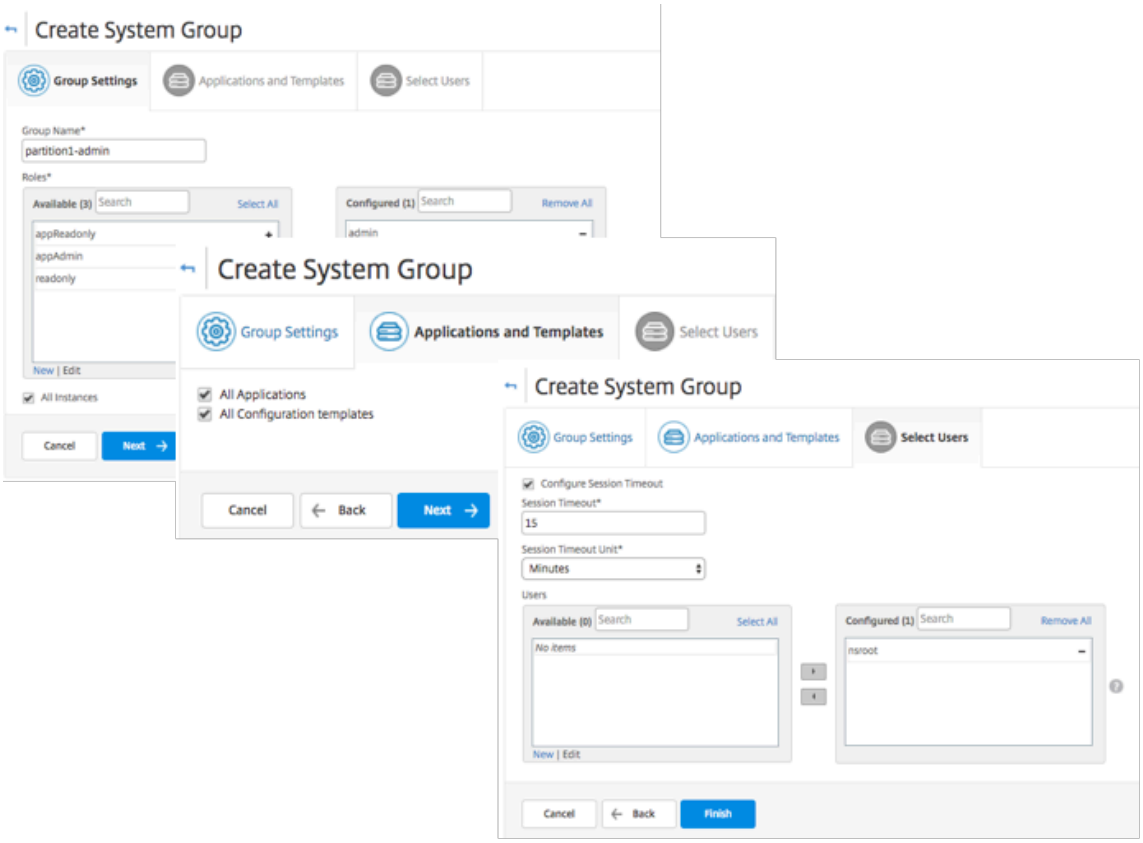
Para crear grupos:

1. Vaya a **Configuración > 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 vínculo **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**Configuración > 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.

Crear un par de alta disponibilidad de NetScaler

January 30, 2024

Un par de alta disponibilidad (HA) de NetScaler puede proporcionar un funcionamiento ininterrumpido durante el tiempo de inactividad o las fallas de la red. Puede crear un par de instancias de ADC de alta disponibilidad mediante NetScaler ADM. Para obtener más información, consulte Alta disponibilidad de NetScaler.

Realice los siguientes pasos para crear un par de instancias de ADC de alta disponibilidad en NetScaler ADM:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione una instancia ADC de la lista con la que quiere crear un par HA.

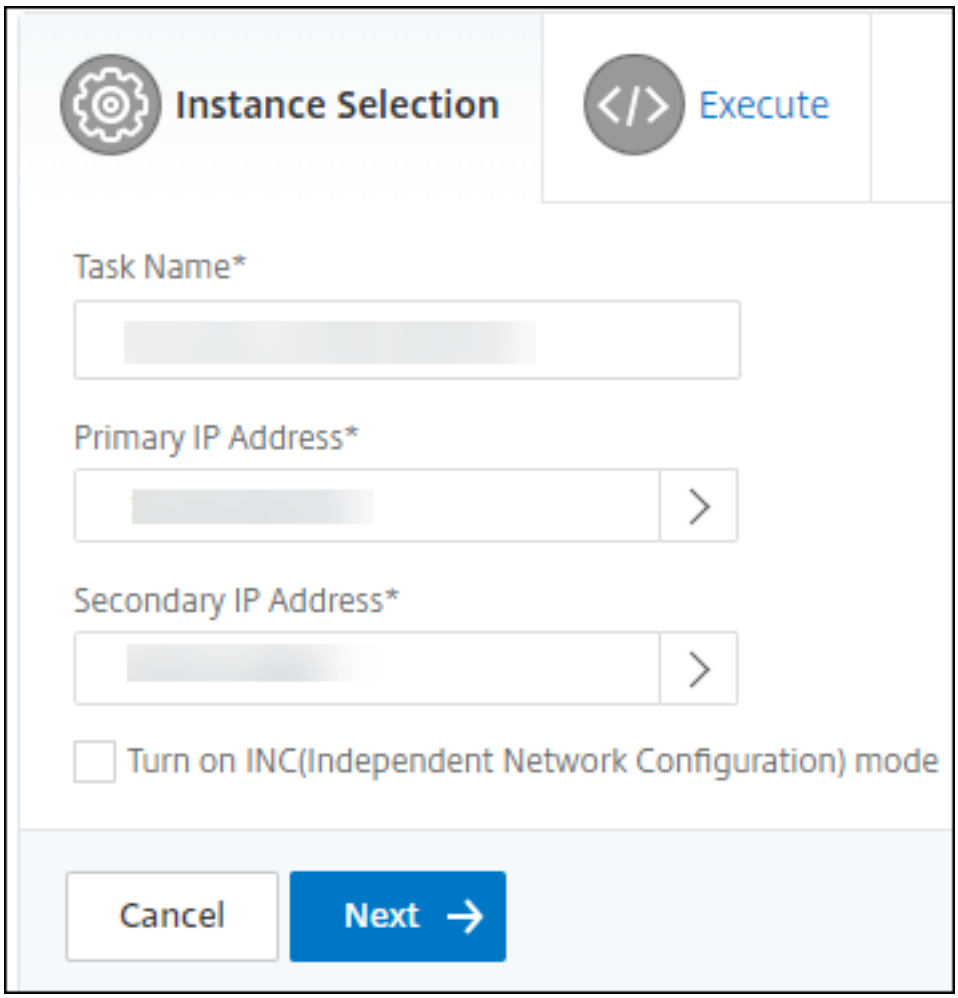
   La instancia seleccionada se convierte en la instancia principal del par HA.
3. Haga clic en Seleccionar **acción > Crear par HA**.
4. En **Selección de instancias**, realice los siguientes pasos:

   a) En **Dirección IP secundaria**, haga clic para seleccionar una instancia secundaria.

   b) Seleccione una instancia de ADC que desee configurar como secundaria en el par HA.

   c) Si lo desea, seleccione **Activar el modo INC (Configuración de red independiente)** si tiene las instancias del par HA en dos subredes.

   d) Haga clic en **Siguiente**.



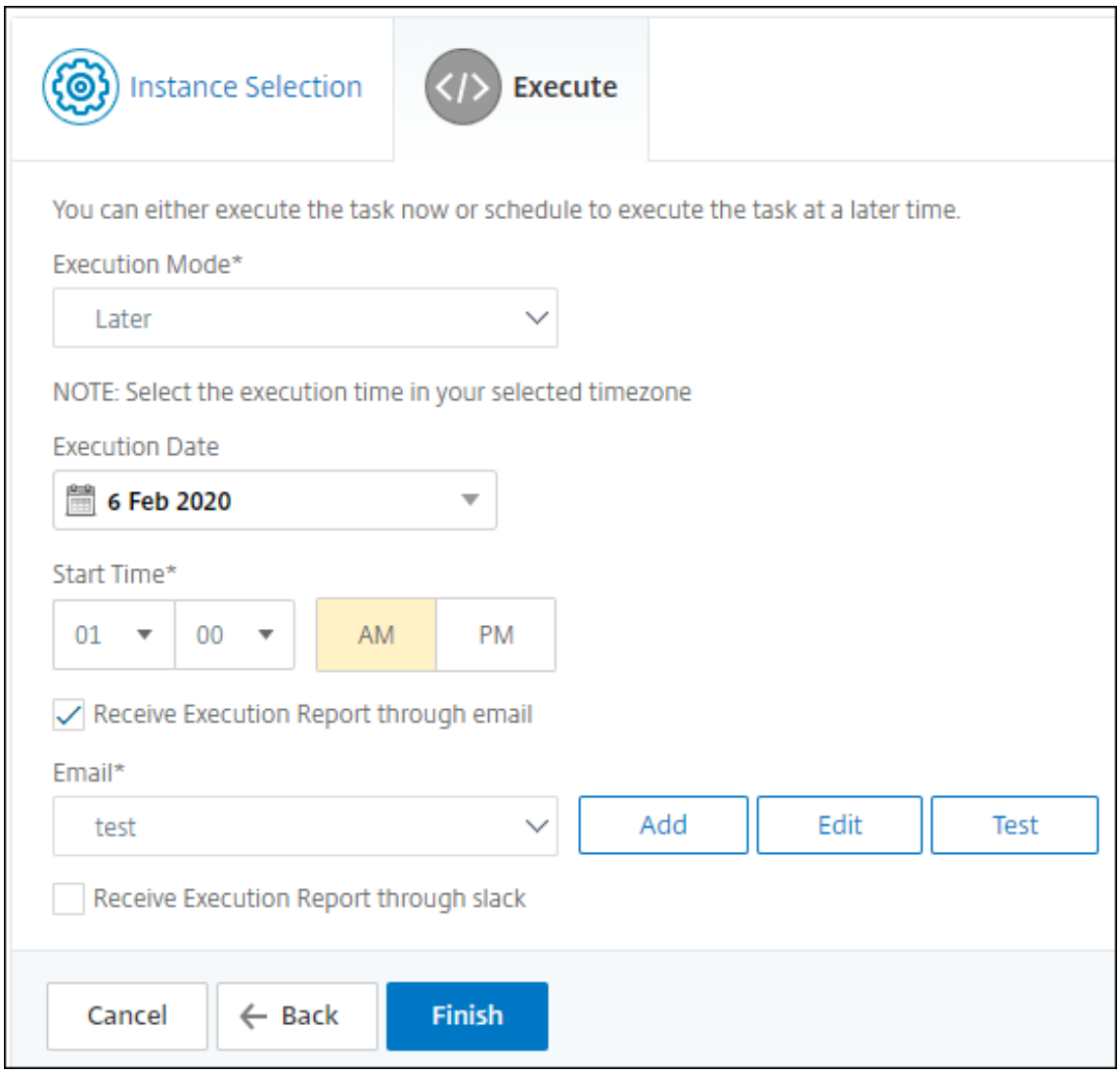
5. En **Execute**, puede decidir crear un par HA ahora o más adelante.

   a) En **Modo de ejecución**, seleccione uno de los siguientes modos de ejecución:

      - **Ahora**: Seleccione esta opción para crear un par HA ahora.
      - **Más adelante**: Seleccione esta opción para crear un par HA en una fecha y hora específicas.

   b) Si ha seleccionado **Más tarde** en la lista **Modo de ejecución**, seleccione **Fecha de ejecución** y **Hora de inicio** cuando quiera ejecutar esta tarea.

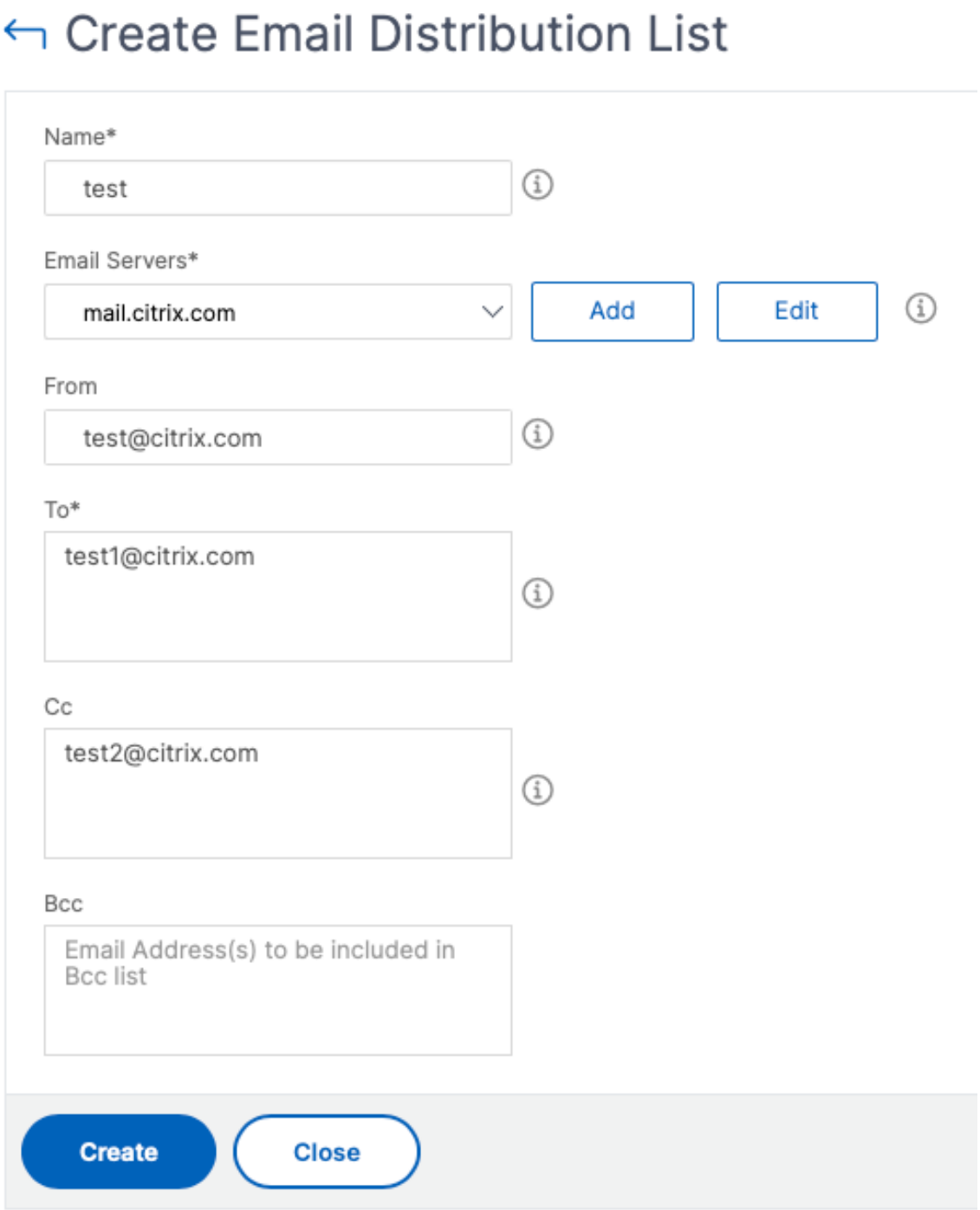
      > **Nota**
      >
      > El tiempo de ejecución se muestra en la zona horaria establecida en NetScaler ADM.



Puede recibir un informe de ejecución de esta tarea a través de lo siguiente:

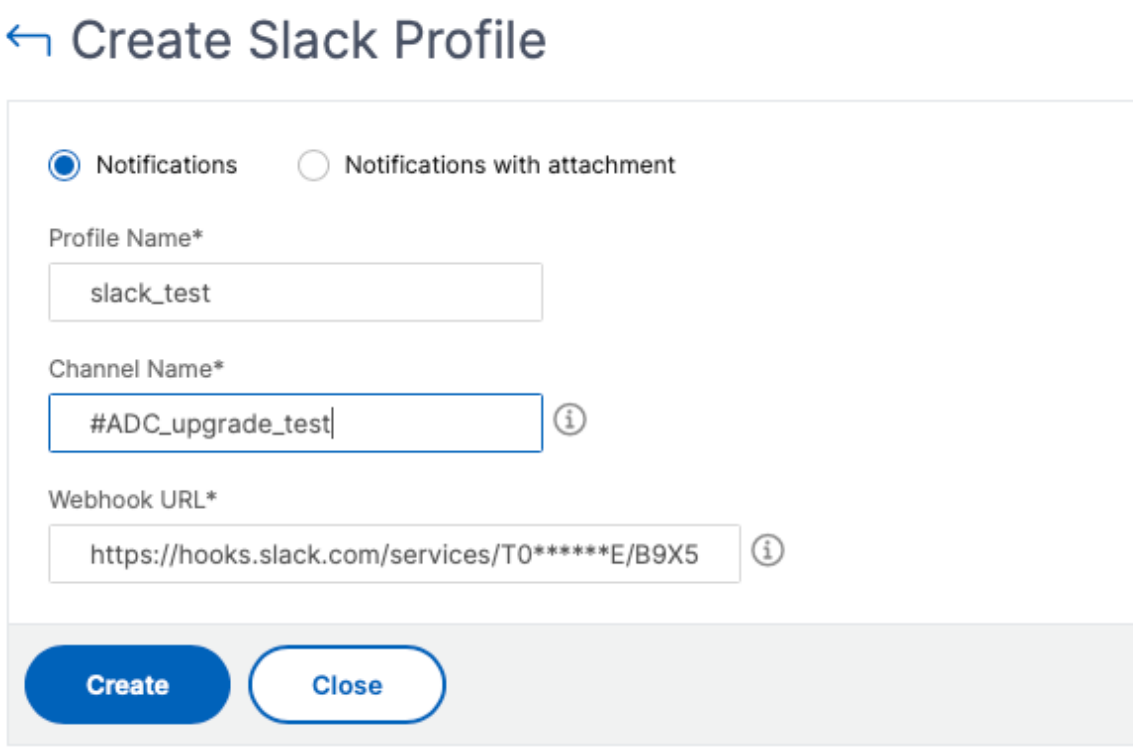
- **Correo electrónico**: Seleccione la distribución del correo electrónico de la lista.

  Para agregar una lista de distribución, haga clic en **Agregar**. Especifique los parámetros necesarios para agregar la lista de distribución y haga clic en **Crear**.



- **Slack**: Selecciona el perfil de Slack de la lista.

  Para agregar un perfil de Slack, haga clic en **Agregar**. Especifique el **nombre del perfil**, **el nombre del canal**y el **token** y haga clic en **Crear**.



Realizar copias de seguridad y restaurar instancias de NetScaler

January 30, 2024

Puede realizar una copia de seguridad del estado actual de una instancia de NetScaler y posteriormente utilizar los archivos de copia de seguridad para restaurarla al mismo estado. Realice siempre 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. Puede realizar copias de seguridad y restaurar manualmente las configuraciones de NetScaler mediante la GUI y la CLI. También puede utilizar NetScaler 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 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:

- NetScaler SDX

- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

> **Nota:**
>
> - Asegúrese de que el perfil ADM de NetScaler tenga acceso de administrador para hacer copias de seguridad y restaurar las instancias de ADC.
> - Desde NetScaler ADM, no puede realizar la operación de copia de seguridad y restauración en un clúster de NetScaler.
> - 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 respaldo por instancia de ADC en este directorio.

Para realizar copias de seguridad y restaurar instancias de NetScaler, primero debe configurar las opciones de copia de seguridad en NetScaler ADM. Después de configurar los parámetros, puede seleccionar una sola instancia de NetScaler 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 NetScaler 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 seleccionada o varias instancias:

1. En NetScaler ADM, vaya a **Configuración** > **Administración**.
2. En **Copia de seguridad**, seleccione **Configurar copia de seguridad del sistema y de la instancia**.
3. Seleccione **Instancia** y especifique lo siguiente:
    - **Habilitar copias de seguridad de instancias**: De forma predeterminada, NetScaler ADM está habilitado para realizar copias de seguridad de instancias de NetScaler. Desactive esta opción si no quiere crear archivos de respaldo para las instancias.

- **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 respaldo cifrado a su equipo local, pero no puede abrir el archivo con la GUI ADM de NetScaler ni con ningún editor de texto. 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.

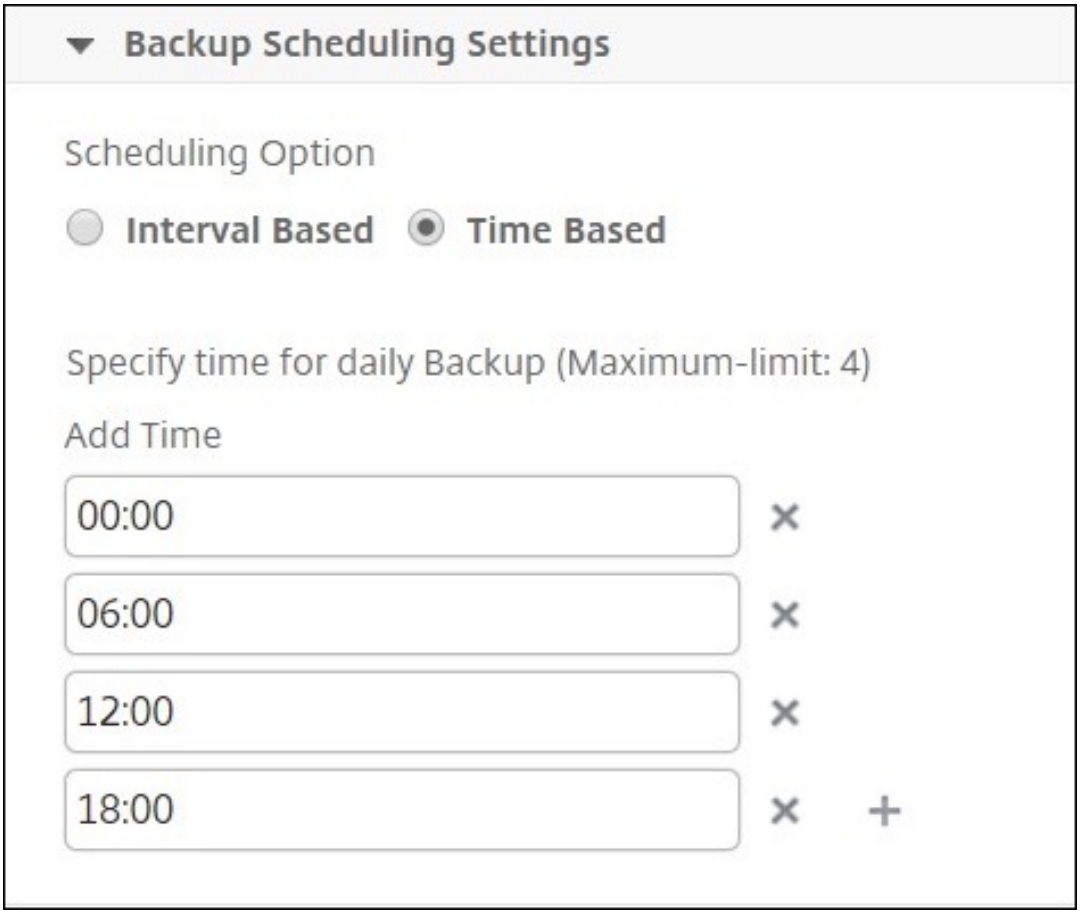
- **Número de archivos de copia de seguridad que se deben conservar**: Especifique el número de archivos de copia de seguridad que se deben conservar en NetScaler ADM. Puede conservar hasta 50 archivos de respaldo por instancia de ADC. El valor predeterminado es tres archivos de copia de seguridad.

  > **Nota:**
  >
  > Cada archivo de respaldo tiene en cuenta algunos requisitos de almacenamiento. Le recomendamos que almacene una cantidad óptima de archivos de respaldo de NetScaler en NetScaler ADM según sus necesidades.

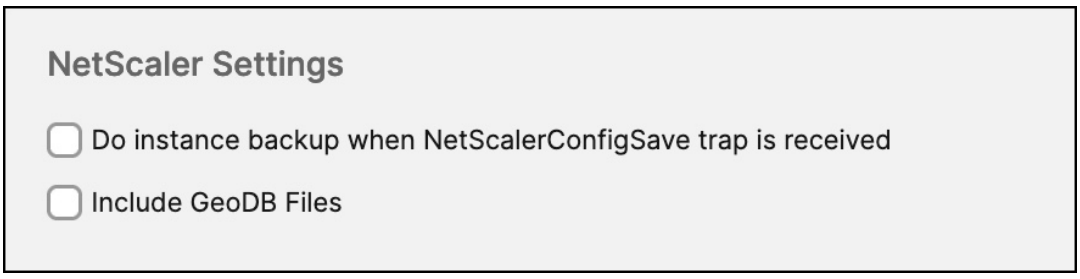
- **Configuración de programación de copias**de seguridad: (opcional) Hay dos opciones disponibles para crear archivos de copia de seguridad, aunque solo se puede utilizar una opción a la vez:

  a) La opción de programación de copias de seguridad predeterminada es "basada en intervalos". Se crea un archivo de respaldo en NetScaler 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, especifique la hora en `hours:minutes` formato para realizar copias de seguridad de las instancias a la hora especificada. NetScaler ADM permite realizar un máximo de cuatro copias de seguridad diarias en las instancias.



- **Configuración de NetScaler**: (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 NetScaler envíe una captura "NetScalerConfigSave"a NetScaler ADM. Una instancia de NetScaler envía "NetScalerConfigSave"cada vez que se guarda la configuración de la instancia.
- **Archivos de geodatabase**: (opcional) De forma predeterminada, NetScaler ADM no realiza copias de seguridad de los archivos de la geodatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.



- **Transferencia externa:**(opcional) NetScaler ADM le permite transferir los archivos de copia de seguridad de instancias de NetScaler a una ubicación externa:

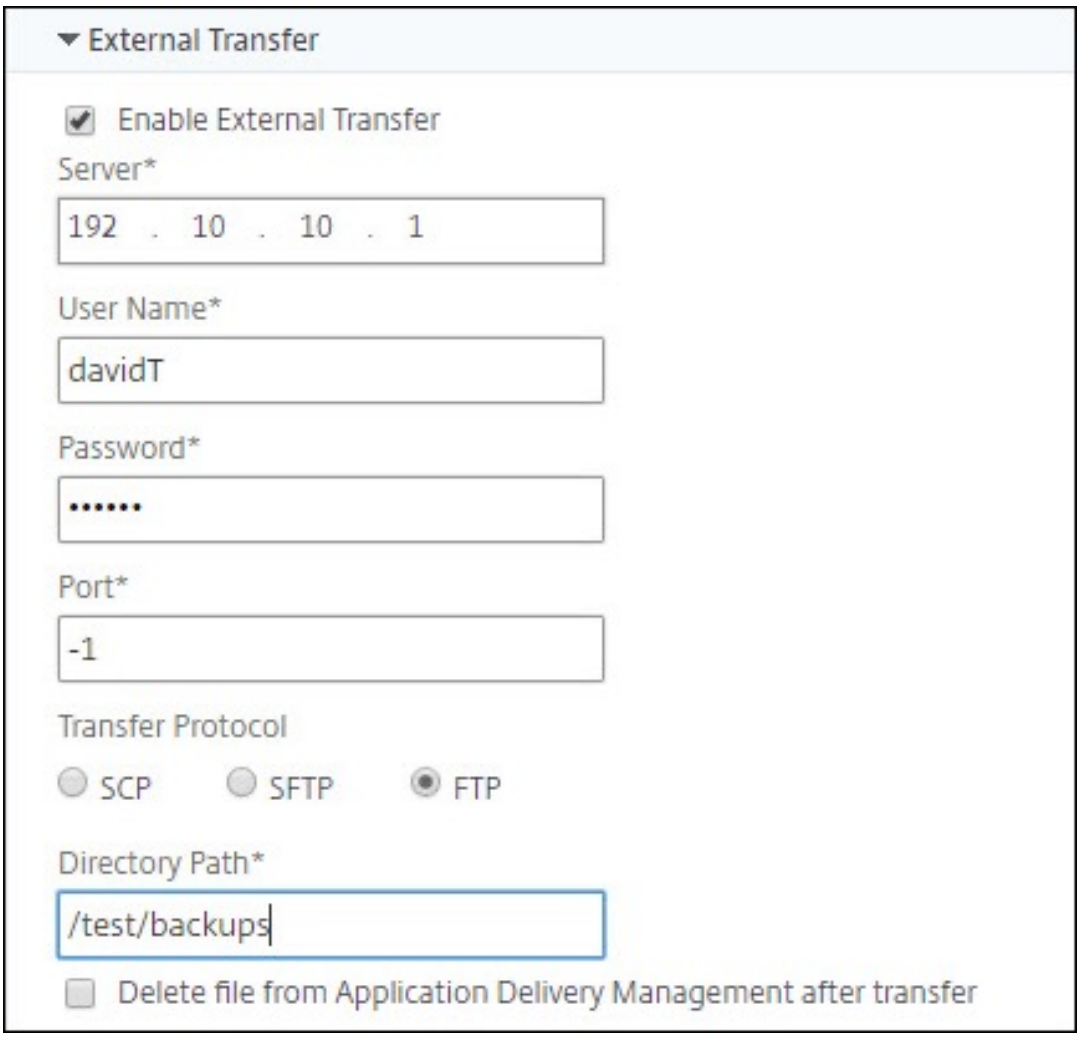
a) Especifique la dirección IP de la ubicación.

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 donde debe almacenarse el archivo.

e) Si lo quiere, también puede eliminar el archivo de respaldo de NetScaler ADM después de transferirlo al servidor externo.



Nota:

NetScaler ADM se envía una captura SNMP o una notificación de Syslog cuando se produce un error de respaldo en cualquiera de las instancias de NetScaler seleccionadas.

Crear una copia de seguridad para una instancia de NetScaler seleccionada mediante NetScaler ADM

Realice esta tarea si quiere realizar una copia de seguridad de una instancia de NetScaler seleccionada o de varias instancias:

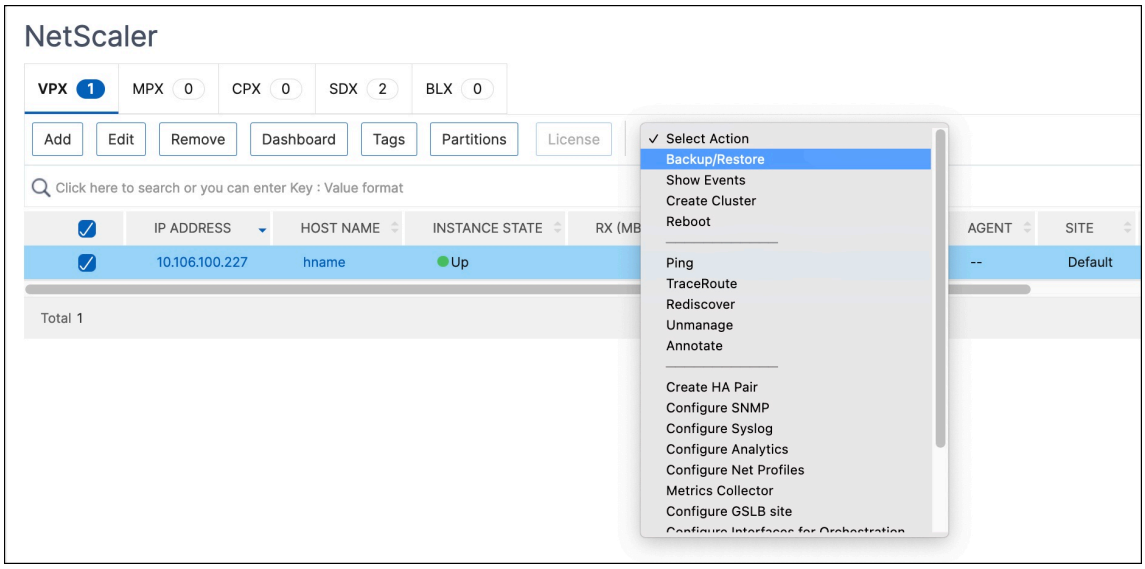
1. **En NetScaler ADM, vaya a Infraestructura > Instancias.** En**Instancias**, seleccione el tipo de instancias (por ejemplo, NetScaler VPX) que se mostrarán en la pantalla.
2. Seleccione la instancia de la que quiere realizar una copia de seguridad.
    - Para las instancias de MPX, VPX y BLX, seleccione **Respaldar/Restaurar** 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 quiere cifrar el archivo de copia de seguridad para obtener más 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 con NetScaler ADM

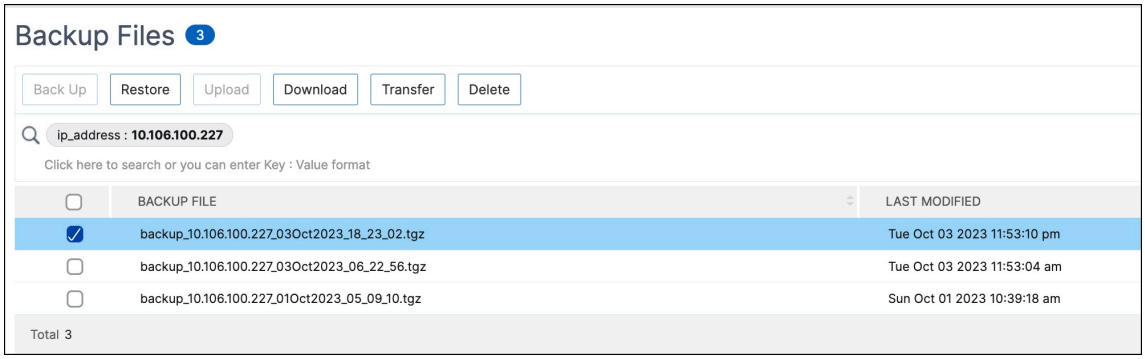
> **Nota:**
>
> Si tiene instancias de NetScaler en un par de alta disponibilidad, debe tener en cuenta lo siguiente:
>
> - Restaure la misma instancia desde la que se creó el archivo de copia de seguridad. Por ejemplo, consideremos un caso en el que se tomó una copia de seguridad de la instancia principal 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 mediante el archivo de reserva que creó anteriormente:

1. Vaya a**Infraestructura > Instancias**, seleccione la instancia que quiere restaurar y, a continuación, haga clic en**Seleccionar acción > Copia de seguridad/restauración**.



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 SDX con NetScaler ADM

En NetScaler ADM, la copia de seguridad del dispositivo NetScaler SDX incluye lo siguiente:

- Instancias de NetScaler 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 de los dispositivos presentes en SDX
- Imágenes de creación de NetScaler

- Imágenes de NetScaler 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)

Restaure el dispositivo NetScaler SDX a la configuración disponible en el archivo de respaldo. Durante la restauración del dispositivo, se elimina toda la configuración actual.

Si va a restaurar el dispositivo NetScaler SDX mediante una copia de seguridad de otro dispositivo NetScaler SDX, asegúrese de agregar las licencias y configurar la configuración de red del Servicio de administración del nuevo dispositivo para que coincida con la configuración del archivo de respaldo antes de iniciar el proceso de restauración. Es decir, el nuevo dispositivo debe contar con una licencia y cumplir los requisitos mínimos de licencia del archivo de respaldo. Por ejemplo, si la copia de seguridad tenía cinco instancias VPX con un total de 5 GB, el nuevo dispositivo también debe poder cumplir estos requisitos. O bien, si el dispositivo de respaldo tenía una licencia platino, el nuevo dispositivo debe tener la misma licencia o una superior. La configuración de red, como la dirección IP, la máscara de red, la puerta de enlace, la dirección IP de XenServer y el servidor DNS, debe configurarse correctamente en el nuevo dispositivo.

Antes de restaurar el dispositivo SDX, asegúrese de que la variante de plataforma del dispositivo SDX de la que se hizo una copia de seguridad sea la misma que la del dispositivo. 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 RMA.

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

1. En la GUI de NetScaler ADM, vaya **a Infraestructura > Instancias > NetScaler > SDX**. Selecciona una instancia.
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

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:

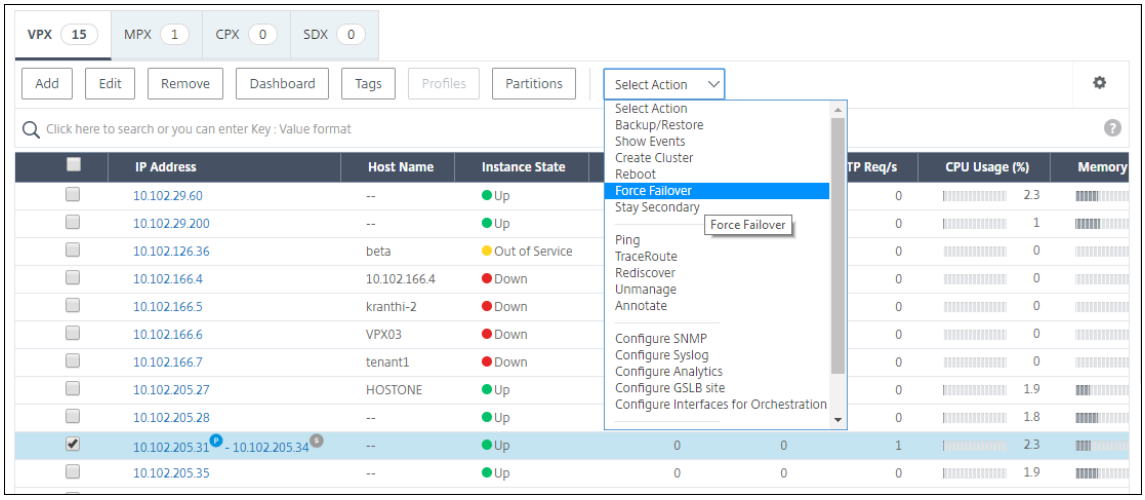
- Se fuerza la conmutación por error en un sistema independiente.
- La instancia secundaria está inhabilitada o inactiva. Si la instancia secundaria se encuentra en un estado inactivo, debe esperar a que su estado sea ACTIVO para forzar una conmutación por error.
- La instancia secundaria está configurada para permanecer secundaria.

La instancia de NetScaler 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 mediante NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a la ficha **Infraestructura > Instancias > NetScaler > 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 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 desaparezca durante unos segundos, pero no quiere que el nodo secundario asume el control. Desea que siga siendo el nodo secundario incluso si detecta un error en el nodo principal.

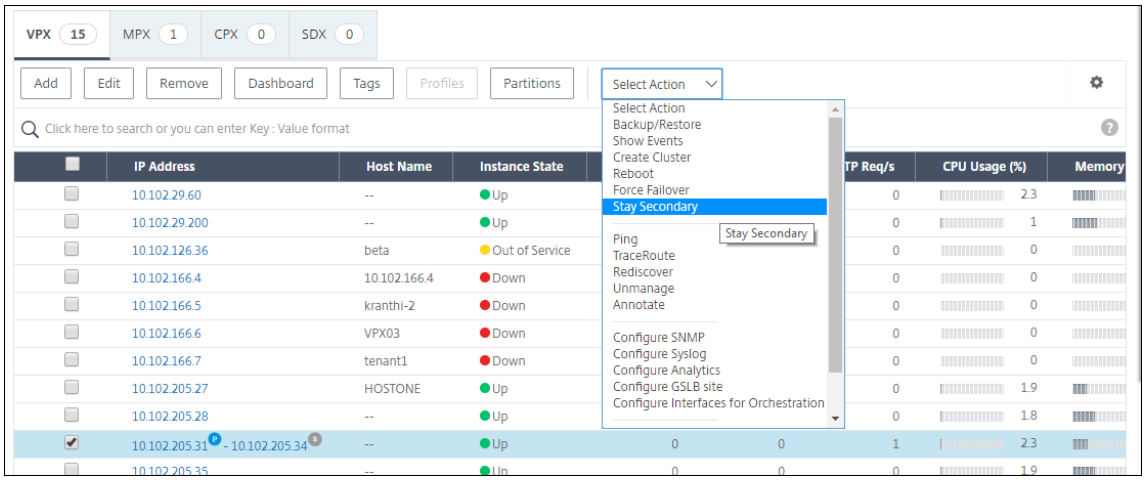
Cuando obliga al nodo secundario a permanecer secundario, seguirá siendo secundario incluso si el nodo principal se desactiva. Además, cuando se fuerza el estado de un nodo de un par de HA a permanecer secundario, no participa en las transiciones de la máquina de estado HA. El estado del nodo se muestra 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 para que permanezca secundaria mediante NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a la ficha **Infraestructura > Instancias** > **NetScaler** > **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

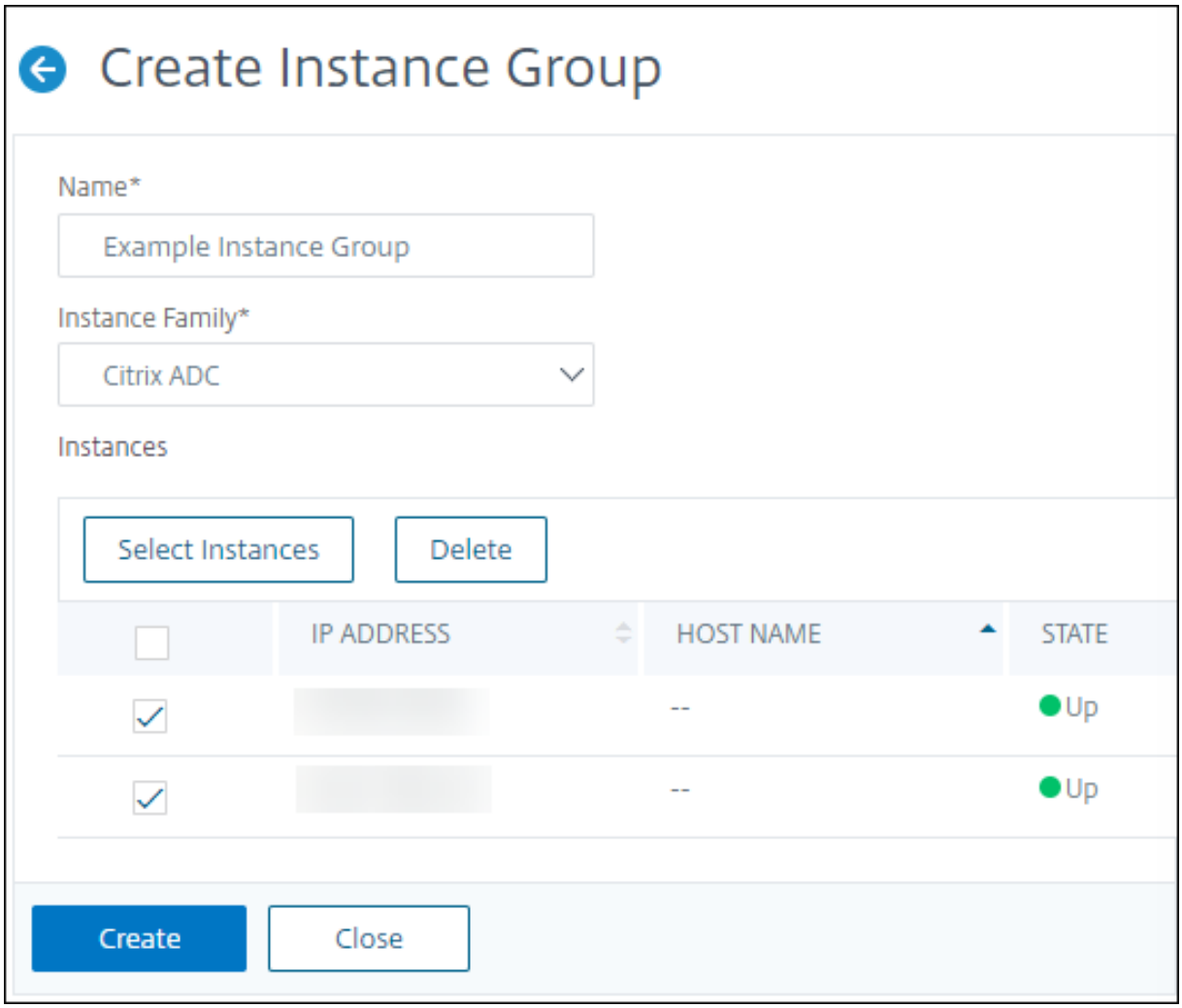
Para crear un grupo de instancias, primero debe agregar todas las instancias de NetScaler a NetScaler ADM. Una vez que hayas agregado las instancias correctamente, crea grupos de instancias según su familia de instancias. La creación de un grupo de instancias le ayuda a actualizar, hacer copias de seguridad o restaurar las instancias agrupadas al mismo tiempo.

Para crear un grupo de instancias con NetScaler ADM

1. En NetScaler ADM, vaya a **Infraestructura > Grupos de instancias**y, a continuación, haga clic en **Agregar**.
2. Especifique un nombre para el grupo de instancias y seleccione **NetScaler** en la lista **Familia de instancias**.
3. Haga clic en **Seleccionar instancias**. En la página **Seleccionar instancias**, seleccione las instancias que quiere agrupar y haga clic en **Seleccionar**.

   La tabla muestra las instancias seleccionadas y sus detalles. Si quieres eliminar alguna instancia del grupo, selecciona la instancia de la tabla y haz clic en **Eliminar** .

4. Haga clic en **Crear**.



Aprovisione instancias de NetScaler VPX en SDX mediante ADM

January 30, 2024

Puede aprovisionar una o más instancias de NetScaler VPX en el dispositivo SDX mediante NetScaler ADM. El número de instancias que puede implementar depende de la licencia que haya adquirido. Si el número de instancias agregadas es igual al especificado en la licencia, ADM le impide aprovisionar más instancias de NetScaler.

Antes de comenzar, asegúrese de agregar una instancia SDX en ADM donde quiera aprovisionar instancias VPX.

Para aprovisionar una instancia VPX, haga lo siguiente:

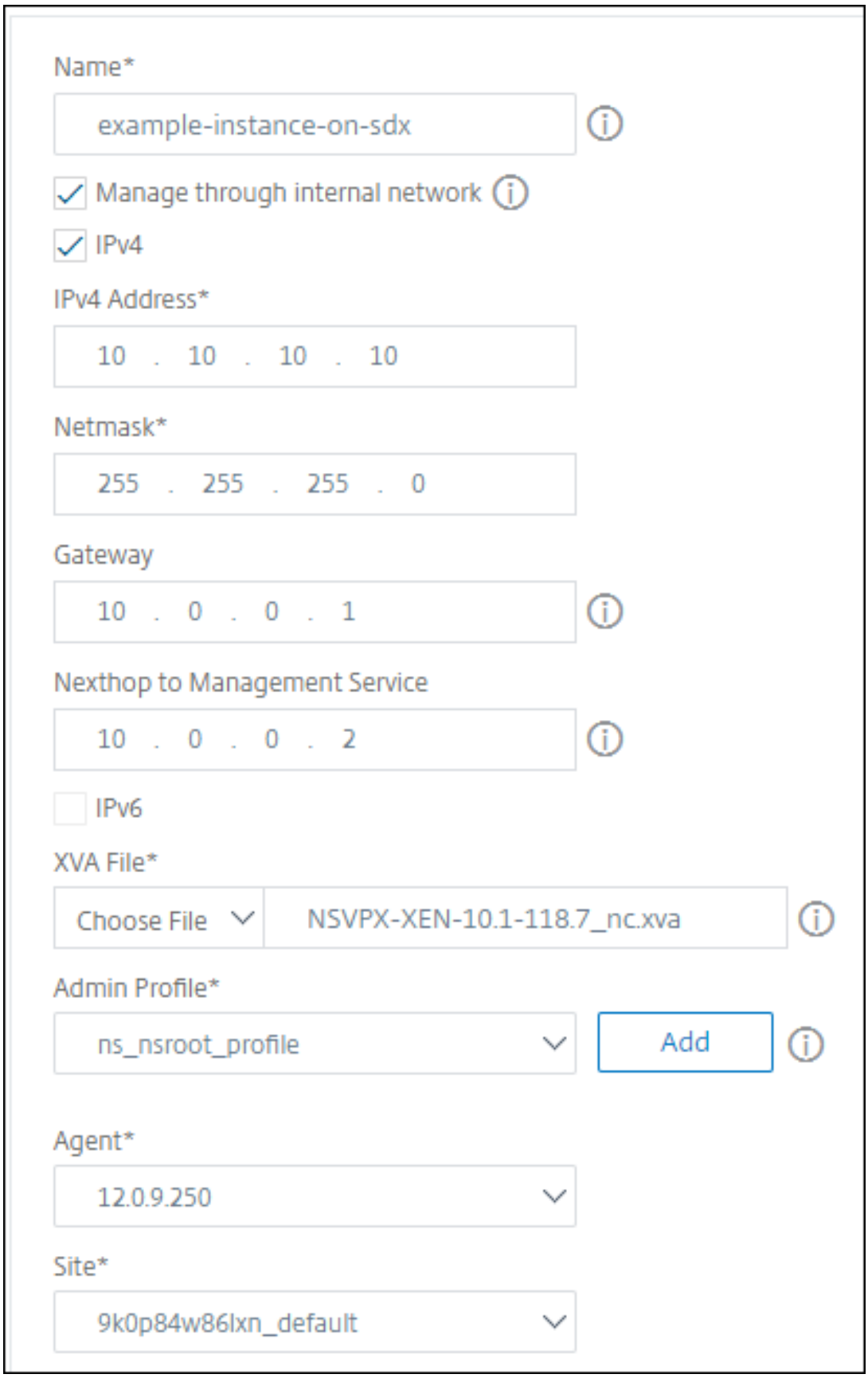
1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. En la ficha **SDX**, seleccione una instancia SDX en la que quiera aprovisionar una instancia VPX.
3. En **Seleccionar acción**, seleccione **Aprovisionar VPX**.

Paso 1: Agregar una instancia VPX

El ADM utiliza la siguiente información para configurar instancias VPX en un dispositivo SDX:

- **Nombre**: especifique un nombre para una instancia de ADC.
- Establezca una red de comunicación entre SDX y VPX. Para ello, seleccione las opciones necesarias de la lista:
  - **Administrar a través de una red interna**: Esta opción establece una red interna para la comunicación entre el ADM y una instancia VPX.
  - **Dirección IP**: puede seleccionar una dirección **IPv4 o**IPv6**, o ambas, para administrar la instancia de NetScaler VPX. Una instancia VPX solo puede tener una IP de administración (también denominada IP de NetScaler). No puede quitar la dirección IP de NetScaler.

    Para la opción seleccionada, asigne una máscara de red, una puerta de enlace predeterminada y un salto siguiente al servidor ADM para la dirección IP.
- **Archivo XVA**: Seleccione el archivo XVA desde el que quiere aprovisionar una instancia VPX. Utilice una de las siguientes opciones para seleccionar el archivo XVA.
  - **Local**: seleccione el archivo XVA de su equipo local.
  - **Dispositivo**: Seleccione el archivo XVA en un explorador de archivos ADM.
- **Perfil de administrador**: este perfil proporciona acceso para aprovisionar instancias VPX. Con este perfil, ADM recupera los datos de configuración de una instancia. Si tiene que agregar un perfil, haga clic en **Agregar**.
- **Agente**: Seleccione el agente al que quiere asociar las instancias
- **Sitio**: Seleccione el sitio donde quiere agregar la instancia.



Paso 2: Asignar licencias

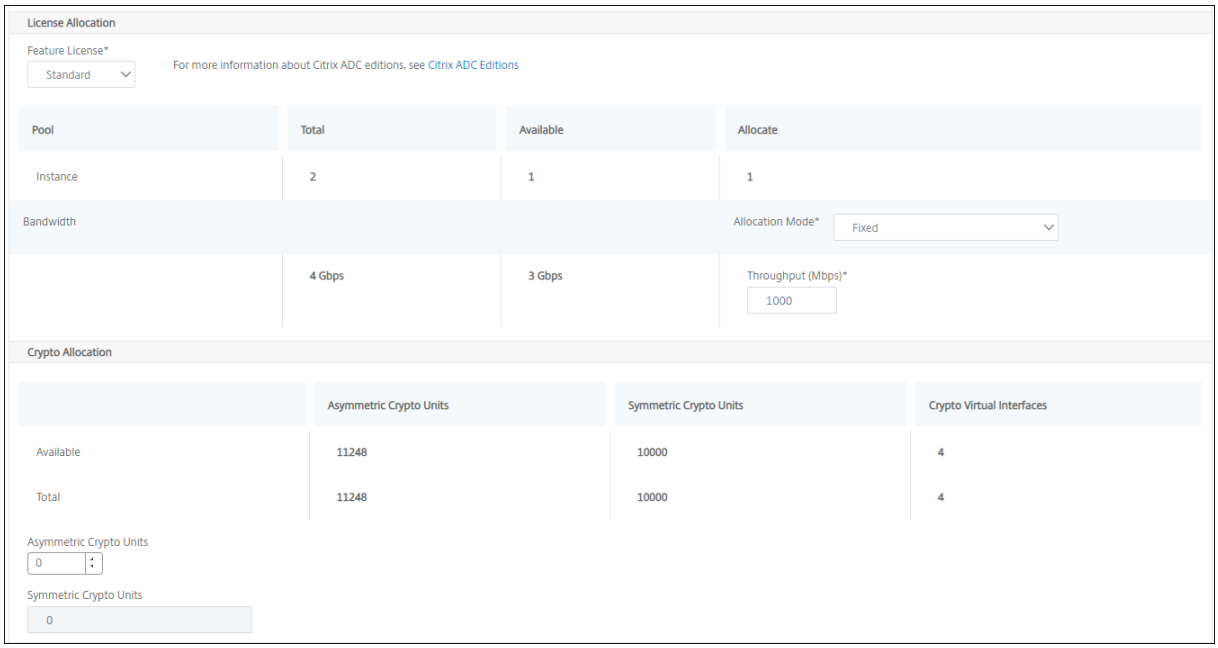
En la sección **Asignación de licencias**, especifique la licencia VPX. Puede utilizar las licencias Standard, Advanced y Premium.

- **Modo de asignación**: puede elegir los modos **fijo** o de **ráfaga** para el conjunto de ancho de banda.

  Si elige el modo **Burstable**, puede usar ancho de banda adicional cuando se alcanza el ancho de banda fijo.

- **Rendimiento**: asigne el rendimiento total (en Mbps) a una instancia.

> **Nota**
>
> Compre una licencia independiente (SDX 2-Instance Add-On Pack para Secure Web Gateway) para instancias de Citrix Secure Web Gateway (SWG) en dispositivos SDX. Este paquete de instancias es diferente de la licencia de plataforma SDX o del paquete de instancias SDX.
>
> Para obtener más información, consulte Implementación de una instancia de Citrix Secure Web Gateway en un dispositivo SDX.



A partir de la versión 12.0 57.19 de SDX, la interfaz para administrar la capacidad de cifrado ha cambiado. Para obtener más información, consulte Administrar la capacidad de cifrado.

Paso 3: Asignar recursos

En la sección **Asignación de recursos**, asigne recursos a una instancia VPX para mantener el tráfico.

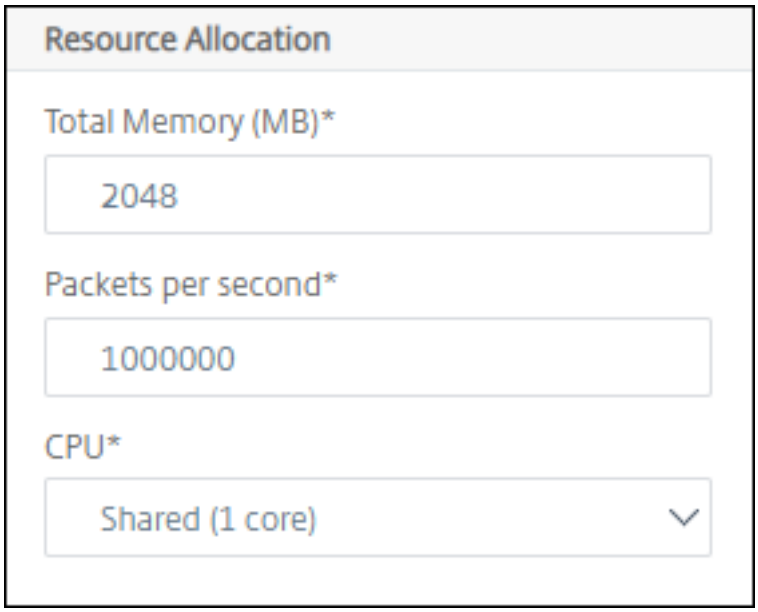
- **Memoria total (MB)**: asigna la memoria total a una instancia. El valor mínimo es 2048 MB.
- **Paquetes por segundo**: especifique la cantidad de paquetes que se van a transmitir por segundo.
- **CPU**: especifique el número de núcleos de CPU de una instancia. Puede utilizar núcleos de CPU compartidos o dedicados.

  Cuando selecciona un núcleo compartido para una instancia, las demás instancias pueden utilizar el núcleo compartido en el momento de escasez de recursos.

  Reinicie instancias en las que se reasignan núcleos de CPU para evitar cualquier degradación del rendimiento.

  Si utiliza la plataforma SDX 25000xx, puede asignar un máximo de 16 núcleos a una instancia. Además, si utiliza la plataforma SDX 2500xxx, puede asignar un máximo de 11 núcleos a una instancia.

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



En la siguiente tabla se enumeran las versiones de VPX admitidas, la imagen de un solo paquete y el número de núcleos que puede asignar a una instancia:

Nombre de la plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una única instancia
SDX 8015, SDX 8400 y SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 y SDX 20500	12	10	5
SDX 11515, SDX 11520, SDX 11530, SDX 11540 y SDX 11542	12	10	5
SDX 17500, SDX 19500 y SDX 21500	12	10	5
SDX 17550, SDX 19550, SDX 20550 y SDX 21550	12	10	5
SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 y SDX 14100	12	10	5
SDX 22040, SDX 22060, SDX 22080, SDX 22100 y SDX 22120	16	14	7
SDX 24100 y SDX 24150	16	14	7
SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G y SDX 14100 40G	12	10	10
SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS y SDX 14100. FIPS	12	10	5
SDX 14040 40S, SDX 14060 40S, SDX 14080 40S y SDX 14100 40S	12	10	5

Nombre de la plataforma	Núcleos totales	Total de núcleos disponibles para el aprovisionamiento de VPX	Núcleos máximos que se pueden asignar a una única instancia
SDX 25100A, 25160A, 25200A	20	18	9
SDX 25100-40G, 25160-40G, 25200-40G	20	18	16 (si la versión es 11.1-51.x o superior); 9 (si la versión es 11.1-50.x o inferior; todas las versiones de 11.0 y 10.5)
SDX 26100, 26160, 26200, 26250	28	26	13
15000-50G	16	14	7
SDX 16000	64	30	16
SDX 9100	20	9	9

Nota

En la plataforma SDX 26xxx, se puede asignar un máximo de 26 núcleos de CPU a una instancia VPX. Si se asignan unidades criptográficas a la instancia, el número máximo de núcleos depende del número de unidades criptográficas e interfaces de datos.

Por ejemplo, si asigna 24000 unidades criptográficas a una instancia, puede asignar 24 núcleos de CPU y un máximo de dos interfaces de datos a la instancia. El dispositivo SDX considera las interfaces de datos y las unidades criptográficas como dispositivos PCI. Para las unidades criptográficas 26000, el aprovisionamiento de instancias VPX falla debido a que no hay espacio para agregar interfaces de datos.

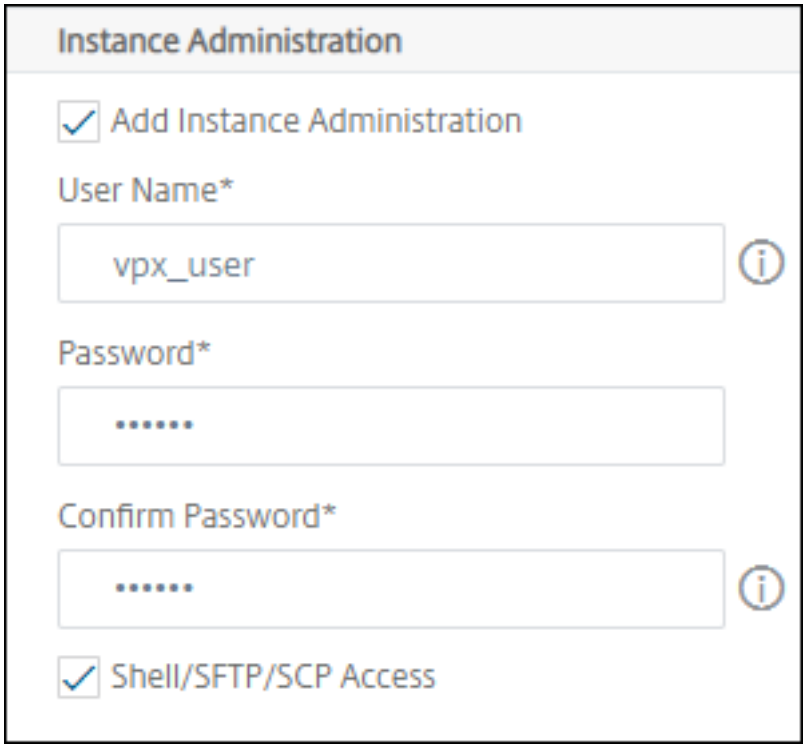
Paso 4: Agregar la administración de instancias

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

Especifique los siguientes detalles:

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

- **Contraseña**: especifique la contraseña del nombre de usuario.
- Acceso a**Shell/Sftp/Scp: el acceso permitido al administrador de instancias de NetScaler**. Esta opción está seleccionada de forma predeterminada.



Paso 5: Especificar la configuración de red

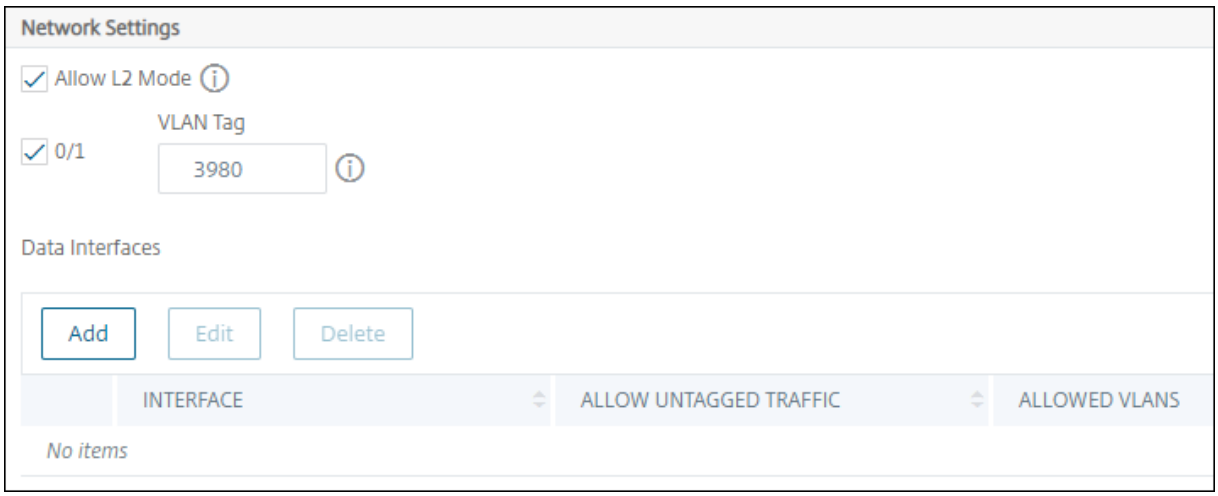
Seleccione la configuración de red requerida para una instancia:

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

  > **Nota**
  >
  > Si inhabilita el modo L2 para una instancia, debe iniciar sesión en la instancia e inhabilitar el modo L2 desde esa instancia. De lo contrario, podría provocar que todos los demás modos de NetScaler se desactiven después de reiniciar la instancia.

- **0/1**: en **la etiqueta VLAN**, especifique un ID de VLAN para la interfaz de administración.
- **0/2**: en **la etiqueta VLAN**, especifique un ID de VLAN para la interfaz de administración.

De forma predeterminada, se seleccionan las interfaces **0/1** y **0/2**.



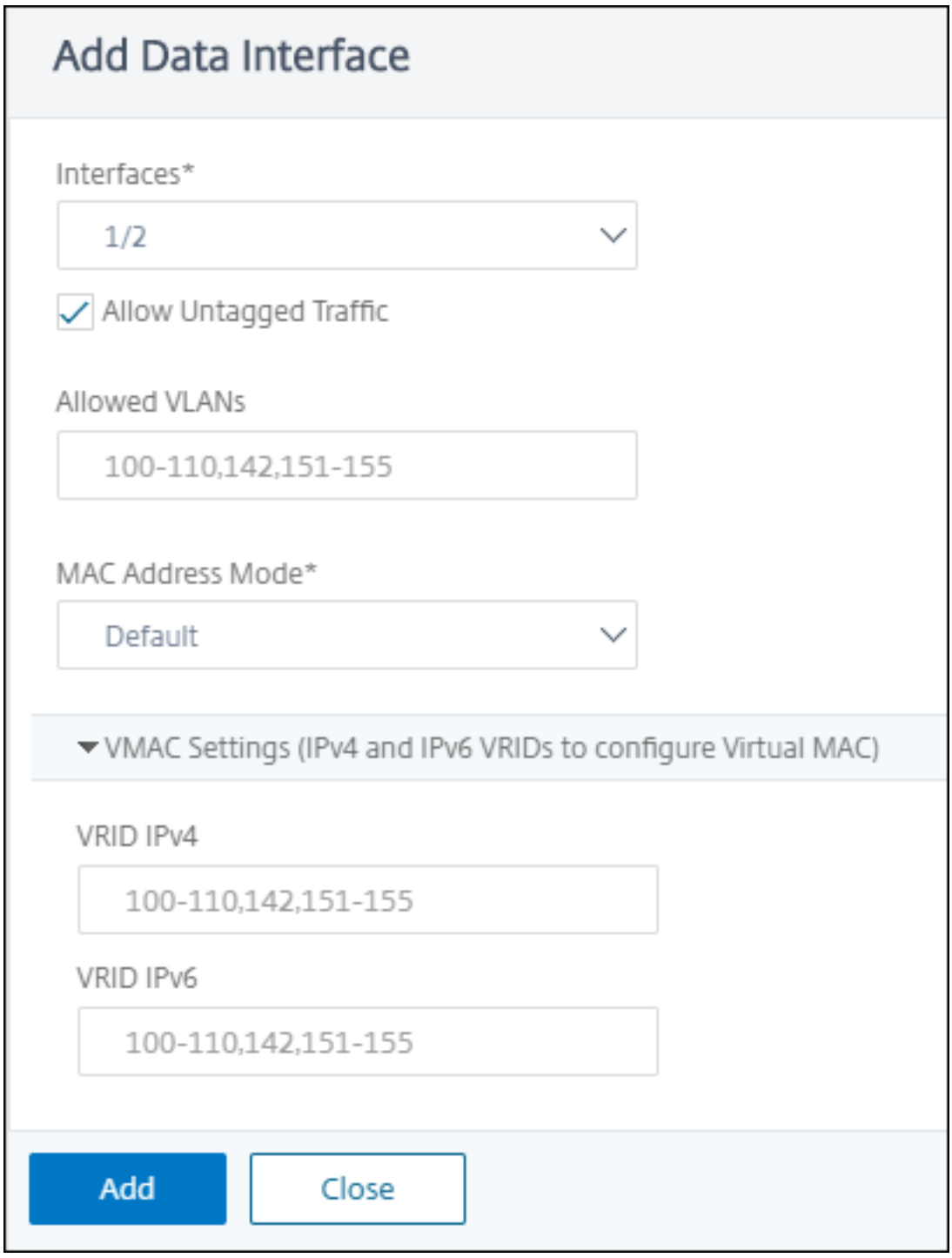
En **Interfaces de datos**, haga clic en **Agregar** para agregar interfaces de datos y especifique lo siguiente:

- **Interfaces**: seleccione la interfaz de la lista.

  > **Nota**
  >
  > Los identificadores de interfaz de las interfaces que se agregan a una instancia no se corresponden necesariamente con la numeración de la interfaz física en el dispositivo SDX.
  >
  > Por ejemplo, la primera interfaz que asocia con la instancia -1 es la interfaz SDX 1/4, aparece como interfaz 1/1 cuando ve la configuración de la interfaz en esa instancia. Esta interfaz indica que es la primera interfaz que asoció con instance-1.

- **VLAN permitidas**: especifique una lista de identificadores de VLAN que se pueden asociar a una instancia de NetScaler.
- **Modo de dirección MAC**: asigna una dirección MAC a una instancia. Seleccione una de estas opciones:
  - **Predeterminado**: Citrix Workspace asigna una dirección MAC.
  - **Personalizado**: elija este modo para especificar una dirección MAC que anule la dirección MAC generada.
  - **Generado: Genera** una dirección MAC mediante la dirección MAC base establecida anteriormente. Para obtener información sobre cómo configurar una dirección MAC base, consulte Asignación de una dirección MAC a una interfaz.
- **Configuración de VMAC (VRID IPv4 e IPv6 para configurar Virtual MAC)**
  - **VRID IPV4**: el VRID de IPv4 que identifica el VMAC. Valores posibles: 1-255. Para obtener más información, consulte Configuración de VMAC en una interfaz.

- VRID IPV6: el VRID IPv6 que identifica el VMAC. Valores posibles: 1-255. Para obtener más información, consulte Configuración de VMAC en una interfaz.



Haga clic en **Agregar**.

Paso 6 - Especificar la configuración de VLAN de administración

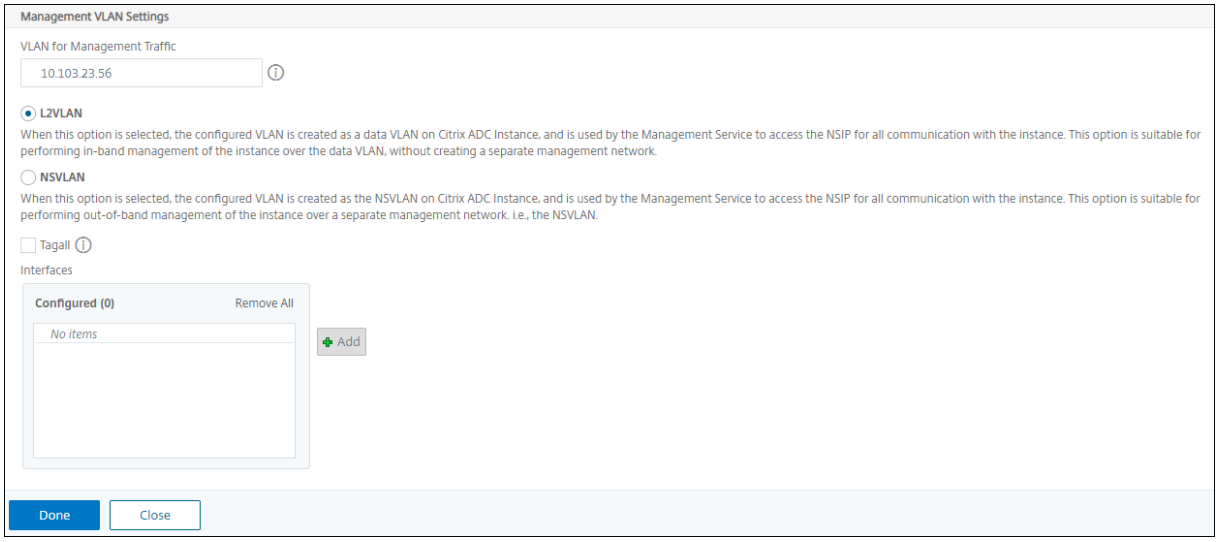
El Servicio de administración y la dirección de administración (NSIP) de la instancia VPX se encuentran en la misma subred y la comunicación se realiza a través de una interfaz de administración.

Si el Servicio de administración y la instancia se encuentran en subredes diferentes, especifique un ID de VLAN mientras aprovisione una instancia VPX. Por lo tanto, la instancia es accesible a través de la red cuando está activa.

Si su implementación requiere que solo se pueda acceder al NSIP a través de la interfaz seleccionada mientras se aprovisiona la instancia VPX, seleccione **NSVLAN**. Y, el NSIP se vuelve inaccesible a través de otras interfaces.

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

> **Importante**
>
> - No puede cambiar esta configuración después de aprovisionar la instancia VPX.
> - El comando `clear config full` de la instancia VPX elimina la configuración de la VLAN si no se selecciona **NSVLAN**.

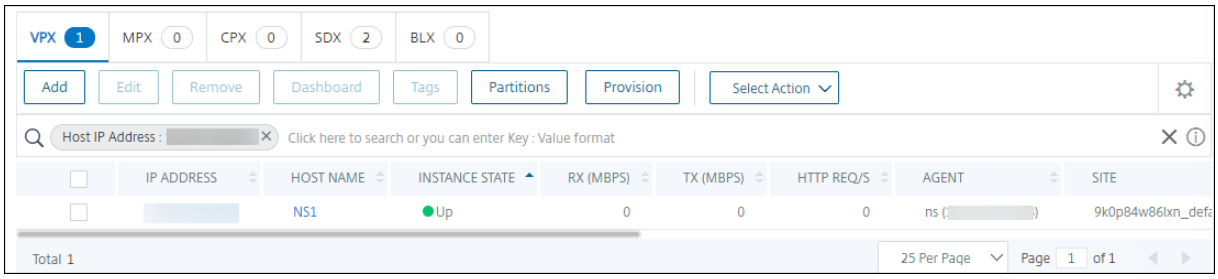


Haga clic en **Listo** para aprovisionar una instancia VPX.

Ver la instancia VPX aprovisionada

Para ver la instancia recién aprovisionada, haga lo siguiente:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. En la ficha **VPX**, busque una instancia por la propiedad **Dirección IP del host y especifique la dirección** IP de la instancia SDX en ella.



Volver a detectar varias instancias de NetScaler VPX

January 30, 2024

Puede redescubrir varias instancias de NetScaler VPX en su configuración de NetScaler Application Delivery Management (ADM). Además, puede volver a descubrir varias instancias de NetScaler VPX cuando desee ver los estados y configuraciones más recientes de esas instancias. El servidor NetScaler ADM vuelve a descubrir todas las instancias de NetScaler VPX y comprueba si se puede acceder a las instancias de Citrix Application Delivery Controller (ADC).

Para volver a descubrir varias instancias de NetScaler VPX:

1. En un navegador web, escriba la dirección IP del servidor NetScaler 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 ficha **Infraestructura > Instancias > NetScaler** > **VPX** y seleccione las instancias que quiere redescubrir.
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 del redescubrimiento de cada una de las instancias de NetScaler VPX.

Desadministrar una instancia

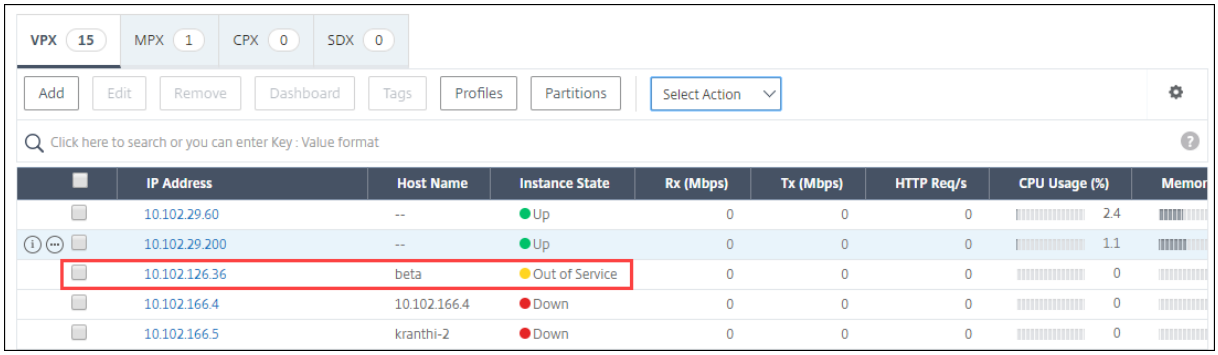
January 30, 2024

Si desea detener el intercambio de información entre NetScaler Application Delivery Management (ADM) y las instancias de su red, puede desadministrarlas.

Para anular la gestión de una instancia:

Vaya a la ficha **Infraestructura > Instancias > NetScaler** > **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 NetScaler Application Delivery Management (ADM) a una instancia, puede encontrar información como el número 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.

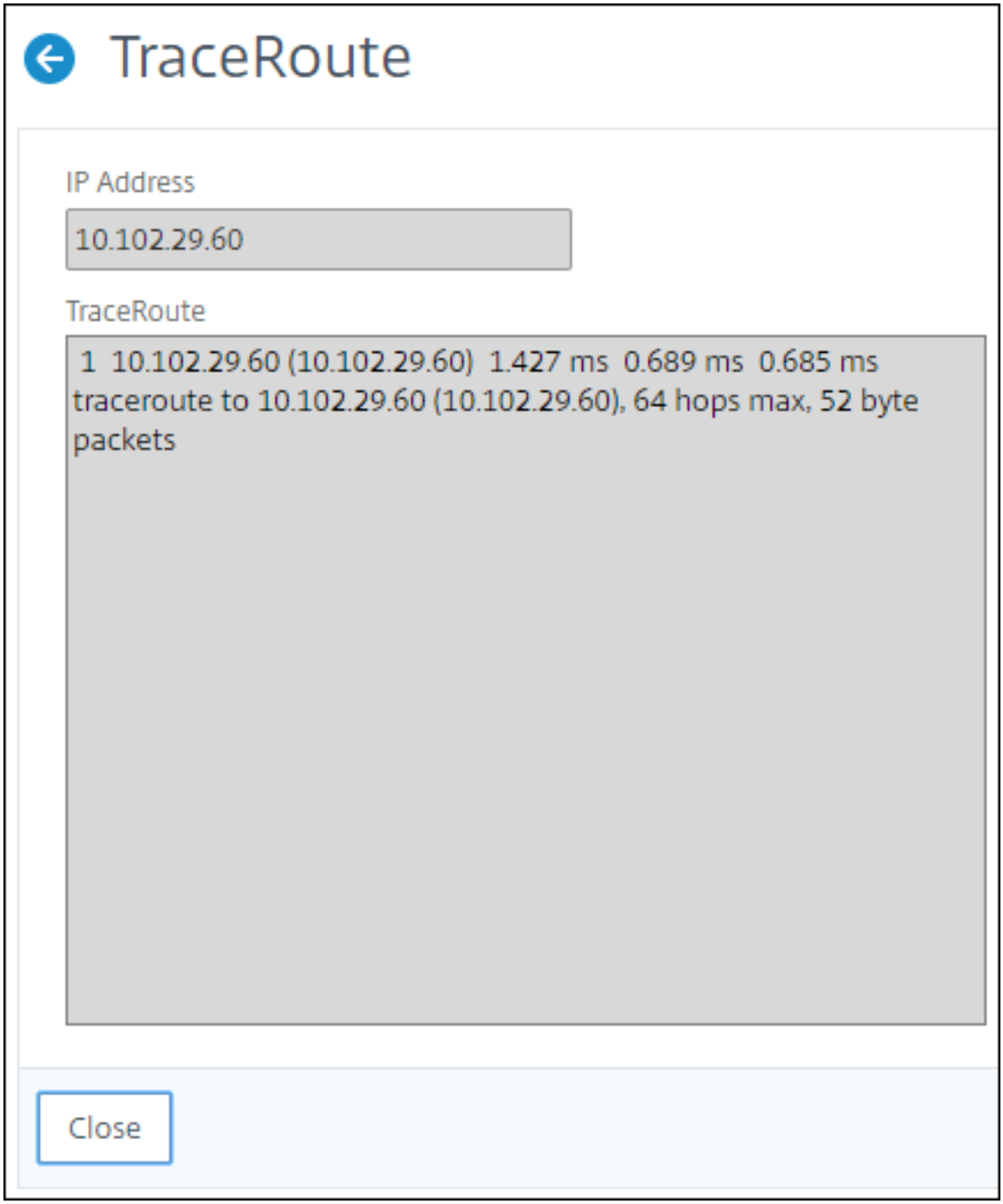
Traceroute también registra el tiempo que tarda un paquete en viajar de un salto a otro. Si hay alguna interrupción en la transferencia de paquetes, traceroute muestra dónde existe el problema.

Para rastrear la ruta de una instancia:

1. En NetScaler ADM, vaya a la ficha **Infraestructura > Instancias > NetScaler** > **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 mensajes de **TraceRoute** muestra la ruta a la instancia y la cantidad de tiempo, en milisegundos, que consume cada salto.



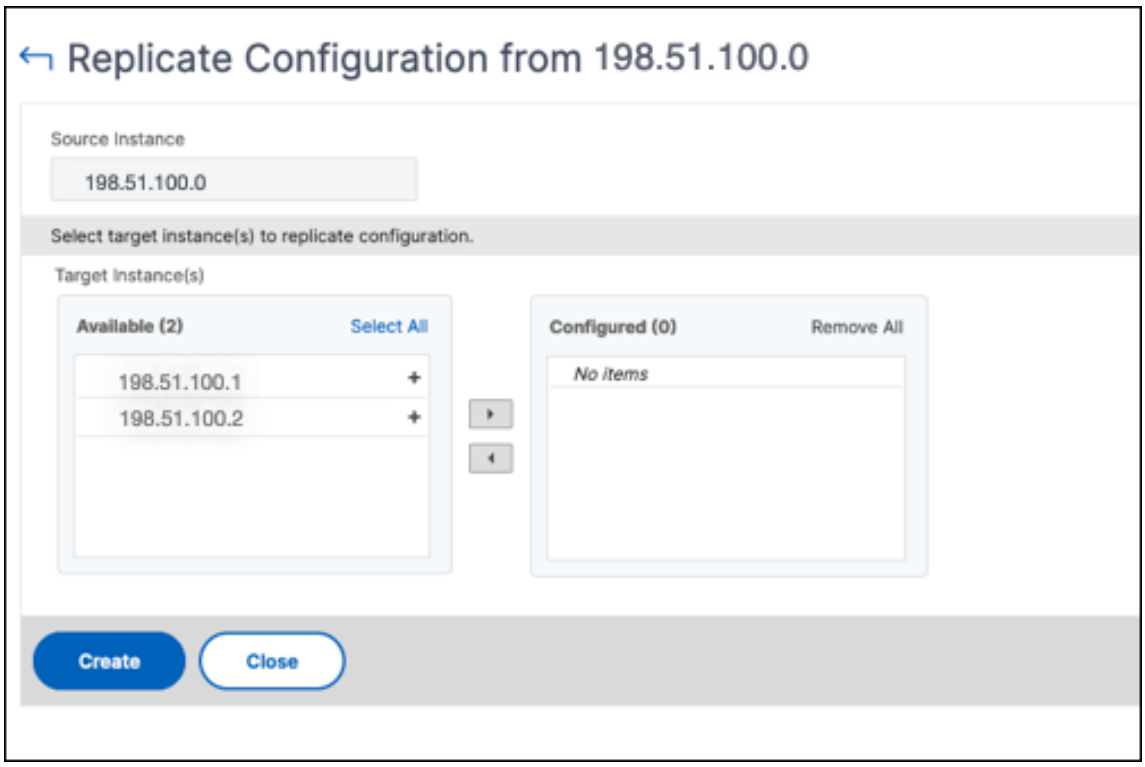
Replique las configuraciones de una instancia de NetScaler a otra

January 30, 2024

Puede usar la función Replicar configuración de NetScaler ADM para copiar configuraciones de una instancia de NetScaler y replicarla en una o varias instancias.

Para replicar configuraciones de una instancia a otras instancias de NetScaler

1. Vaya a **Infraestructura > Instancias > NetScaler**. Seleccione la instancia de origen cuyas configuraciones quiere replicar en otras instancias y, en la lista **Seleccionar acción**, haga clic en **Replicar configuración**.
2. En **Replicar configuración**, seleccione la instancia de destino en la que quiere aplicar las configuraciones de la instancia de origen. Puede replicar las configuraciones de una única instancia de origen a una única instancia o a varias instancias de destino.



3. Haga clic en **Crear**.

Las configuraciones replicadas se agregan a la lista de instancias de NetScaler. Para ver el estado de las instancias replicadas, haga clic en el icono de actualización.

> **Nota:**
>
> Durante la replicación, todas las IP de red de la instancia de origen se replican en la instancia de destino. Si la instancia de destino se encuentra en una red diferente de la instancia de origen, es posible que no se pueda acceder a las IP de la instancia de destino. Cuando no se puede acceder a las IP, el estado de las entidades de la instancia de destino se muestra como Inactivo.
>
> Para ver el estado de las entidades configuradas en la instancia de NetScaler administrada, vaya a **Infraestructura > Funciones de red**.

Administración de certificados SSL

January 30, 2024

Cualquier organización o sitio web individual que requiera el manejo de información confidencial o confidencial debe tener un certificado SSL. El certificado SSL en un servidor web ayuda a garantizar la autenticidad del servidor web al cliente conectado. No solo autentica la identidad de un sitio web, sino que también ayuda a generar la clave de sesión, que se utiliza posteriormente para el cifrado de toda la sesión.

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).

NetScaler Application Delivery Management (ADM) le proporciona una consola unificada para automatizar la instalación, la actualización, la eliminación, la vinculación y la descarga de los certificados SSL. Ayuda a conservar la reputación del sitio web y la confianza del cliente. NetScaler ADM ahora optimiza todos los aspectos de la administración de certificados por usted. A través de una consola unificada, puede configurar directivas automatizadas para garantizar el emisor recomendado, la fuerza de clave, el protocolo y los algoritmos según las directivas de TI de la organización. Al hacerlo, puede vigilar de cerca los certificados que no se utilizan o que están a punto de caducar.

Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

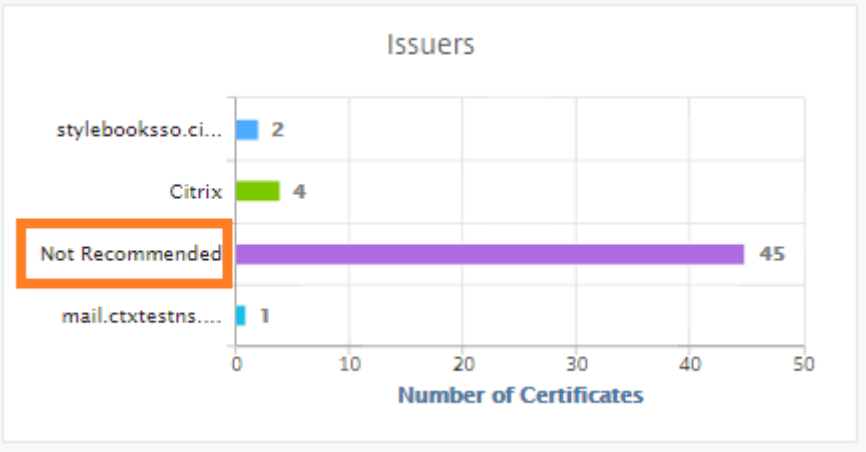
- De una entidad emisora de certificados (CA) autorizada, como Verisign
- Al generar un nuevo certificado SSL y una clave en el dispositivo NetScaler

Configuración de directiva SSL empresarial

Cada empresa tiene su propia directiva SSL y define los requisitos a los que deben cumplir todos los certificados SSL. La seguridad siempre ha sido una de las principales prioridades de todos los usuarios empresariales y, por lo tanto, la configuración SSL desempeña un papel importante.

Por ejemplo, una empresa ABC ordena que todos los certificados deben tener fortalezas clave mínimas de 2.048 bits o superiores. Los certificados deben ser autorizados por entidades emisoras o entidades emisoras de confianza. Los administradores deben comprobar todos estos parámetros SSL para asegurarse de que los certificados cumplen con la directiva de la empresa. Es un trabajo tedioso verificar cada certificado manualmente. Para superar este caso, NetScaler ADM le ayuda a configurar la configuración de la directiva SSL empresarial y muestra cualquier certificado de incumplimiento con la etiqueta "No recomendado".

Puede ver el resumen de los certificados de incumplimiento (no recomendados) en el Panel de control de SSL.



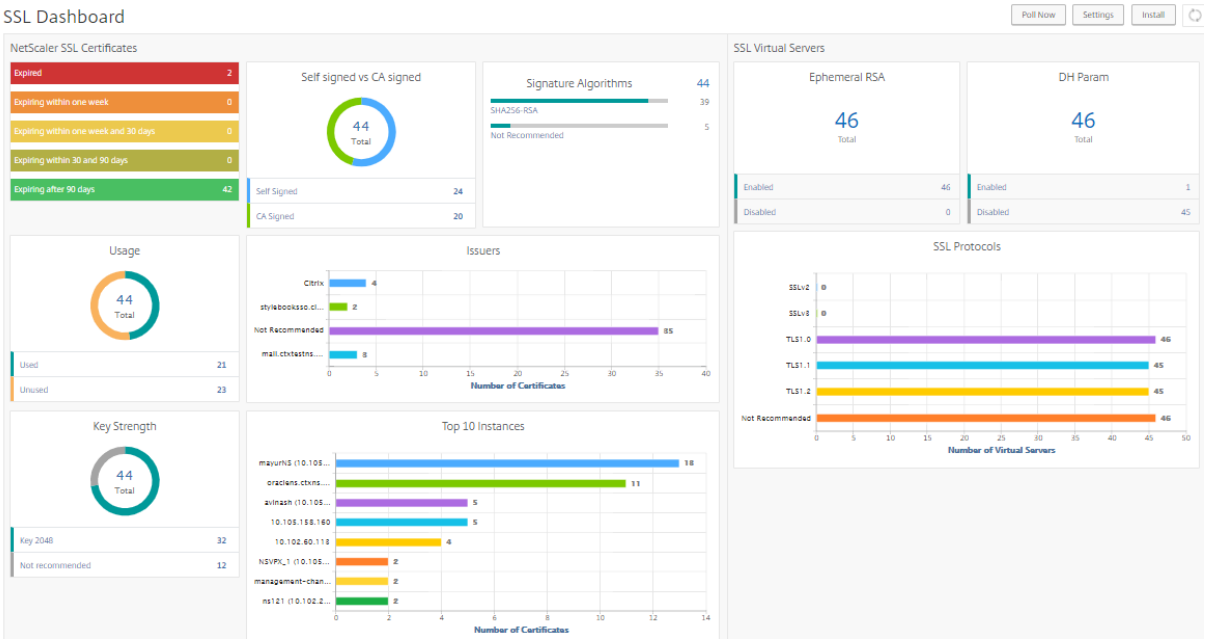
> **Nota**
>
> Los certificados "No recomendados"se clasifican en función de diferentes parámetros, y puede verlos en componentes relevantes.

Cómo funciona el certificado NetScaler ADM

SSL Dashboard proporciona una presentación visual de todos los certificados SSL instalados en diferentes instancias de NetScaler. El panel SSL incluye la siguiente información para cada certificado instalado en instancias de NetScaler. Se clasifica en función de lo siguiente:

- **Autofirmada frente a CA firmada.** La sección autofirmada frente a la firma de CA le ayuda a segregar los certificados en certificados autofirmados y certificados firmados por CA.
- **Algoritmos de firma.** Esta sección segrega los certificados SSL en función de los algoritmos de firma que se utilizan para el cifrado.

- **Uso.** Esta sección segrega los certificados SSL en función de certificados usados y no utilizados. Los certificados no utilizados exigen una atención especial, ya que es posible que no se hayan podido enlazar a los servidores virtuales.
- **Emisores.** Esta sección separa los certificados SSL en función del emisor de los certificados.
- **Fuerza de la clave.** Esta sección segrega los certificados SSL en función de la intensidad de clave de una clave privada.
- **Las 10 instancias principales.** Esta sección proporciona los detalles de las 10 instancias principales de NetScaler en función del número de certificados SSL instalados.



Casos de uso de administración de certificados SSL

Los siguientes casos de uso describen cómo puede utilizar el certificado SSL para administrar y supervisar los certificados en varias instancias de NetScaler.

Instalar certificados SSL

Imagine que tiene una flota de instancias de NetScaler en las que debe implementar los certificados SSL requeridos. NetScaler ADM proporciona una consola unificada para implementar los certificados SSL en varias instancias de NetScaler en un solo intento.

Por ejemplo, es posible que quiera instalar algunos certificados SSL en una o más instancias de NetScaler. Con este enfoque, puede minimizar la intervención manual de instalar el certificado SSL

en cada instancia de NetScaler. Puede realizar una instalación masiva de certificados SSL en una o más instancias de NetScaler.

Para obtener un resumen de los certificados SSL, inicie sesión en **NetScaler ADM**y, a continuación, vaya a **Infraestructura > Panel de control SSL**.

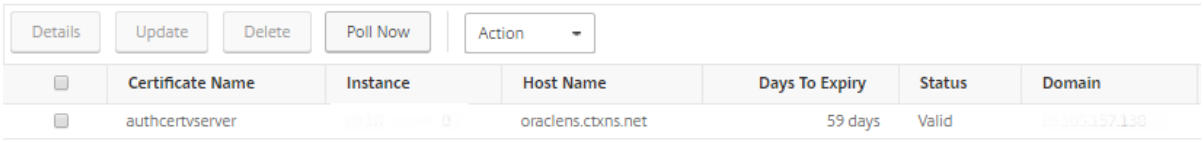
Configuración de notificación para caducidad del certificado

En este caso de uso, es posible que tenga muchos certificados en varias instancias de NetScaler y se convierte en una sobrecarga para realizar el seguimiento de la caducidad de cada certificado. Es un trabajo tedioso para usted realizar un seguimiento manual de cada certificado y actualizarlo antes de que caduque. Para evitar estos casos, puede configurar NetScaler ADM para que envíe las notificaciones o alertas a los perfiles configurados de correo electrónico, buscapersonas, Slack o ServiceNow configurados. De esta forma, puede mantenerse al tanto de las fechas de caducidad de los certificados y renovarlos mucho antes de las fechas de caducidad.

Por ejemplo, puede olvidarse de realizar un seguimiento del certificado que está a punto de caducar. Y el certificado caduca causando una interrupción del servicio, lo que podría afectar a numerosas aplicaciones para los usuarios. Con la configuración de notificación de caducidad de certificado ADM, puede evitar estos casos imprevistos.

Puede ver el resumen y realizar un seguimiento de los certificados que están a punto de caducar en el **panel SSL**.

Para ver el informe de certificados que caducan en cualquier duración, puede hacer clic en el mosaico para obtener los detalles de todos los certificados que caducan en esa ventana.



Renovación de certificados

Ahora puede renovar los certificados desde NetScaler ADM. Puede renovar los certificados existentes o crear los certificados basándose en lo siguiente:

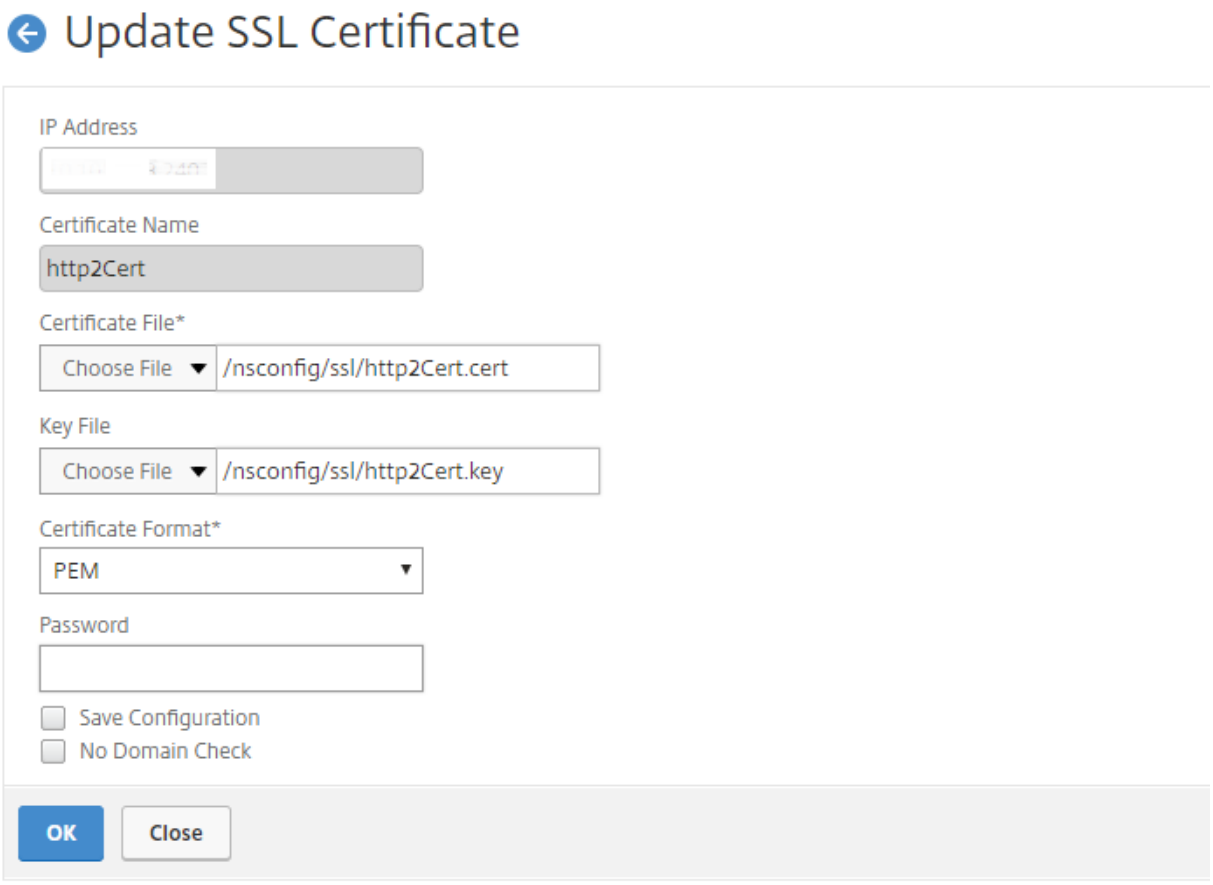
Actualizar el certificado existente En este caso de uso, debe actualizar un certificado existente una vez que reciba un certificado renovado de la entidad emisora de certificados (CA). Ahora puede actualizar los certificados existentes desde NetScaler ADM sin iniciar sesión en las instancias de NetScaler.

Por ejemplo, puede haber algunos cambios o modificaciones en los certificados existentes. La CA emite certificados renovados. En lugar de ir al dispositivo NetScaler, ahora puede actualizar el certificado SSL desde NetScaler ADM.

Para actualizar cualquier certificado, inicie sesión en NetScaler ADM y, a continuación, vaya a **Infraestructura > Panel SSL**.

Seleccione el certificado que quiere actualizar y haga clic en **Actualizar**.

Tiene la opción de actualizar los campos relevantes del certificado seleccionado de NetScaler ADM.

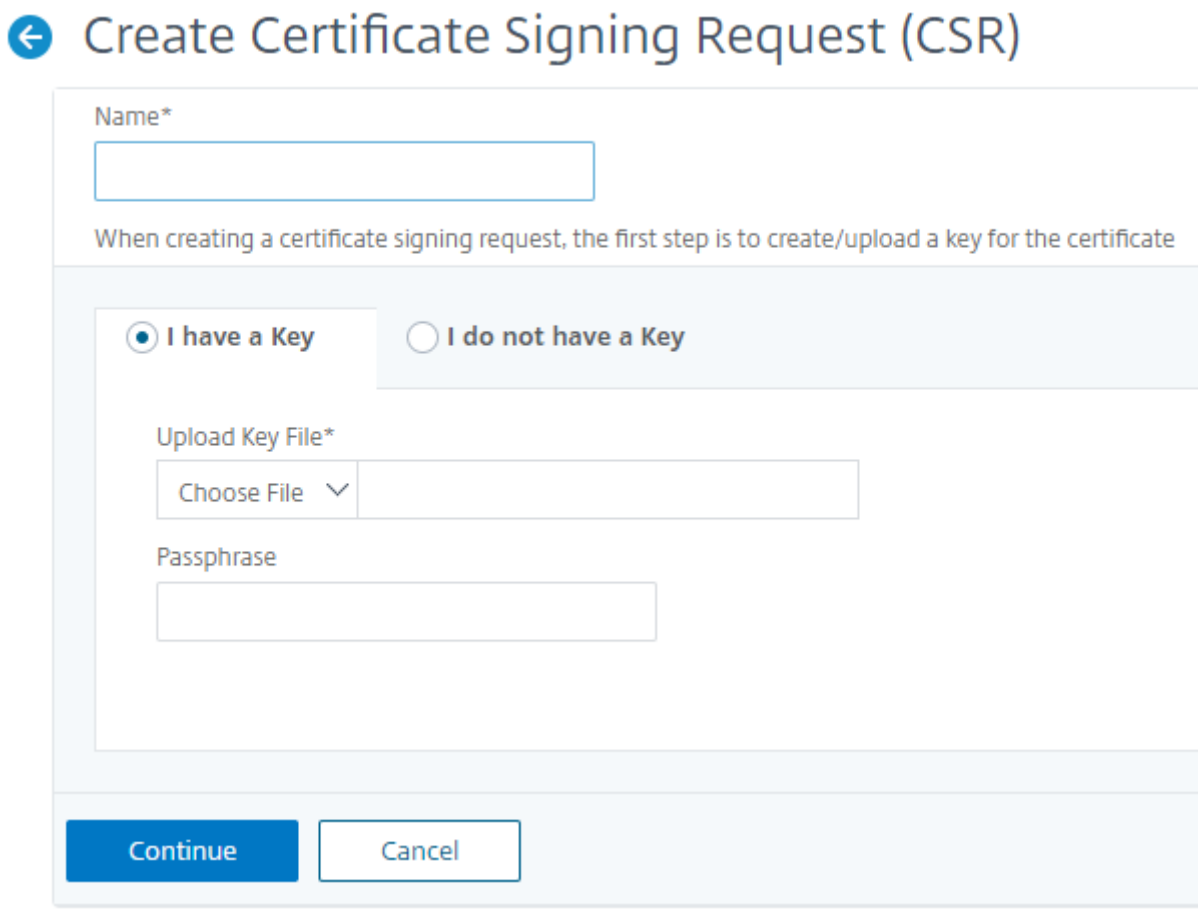


Crear solicitud de firma de certificado Imagine un caso de uso en el que uno de los certificados SSL no cumple con las directivas de la organización. Desea obtener un certificado nuevo de la entidad emisora de certificados. Ahora puede generar una solicitud de firma de certificado (CSR) desde NetScaler ADM. Una CSR y una clave pública se pueden enviar a una entidad emisora de certificados para obtener el certificado SSL.

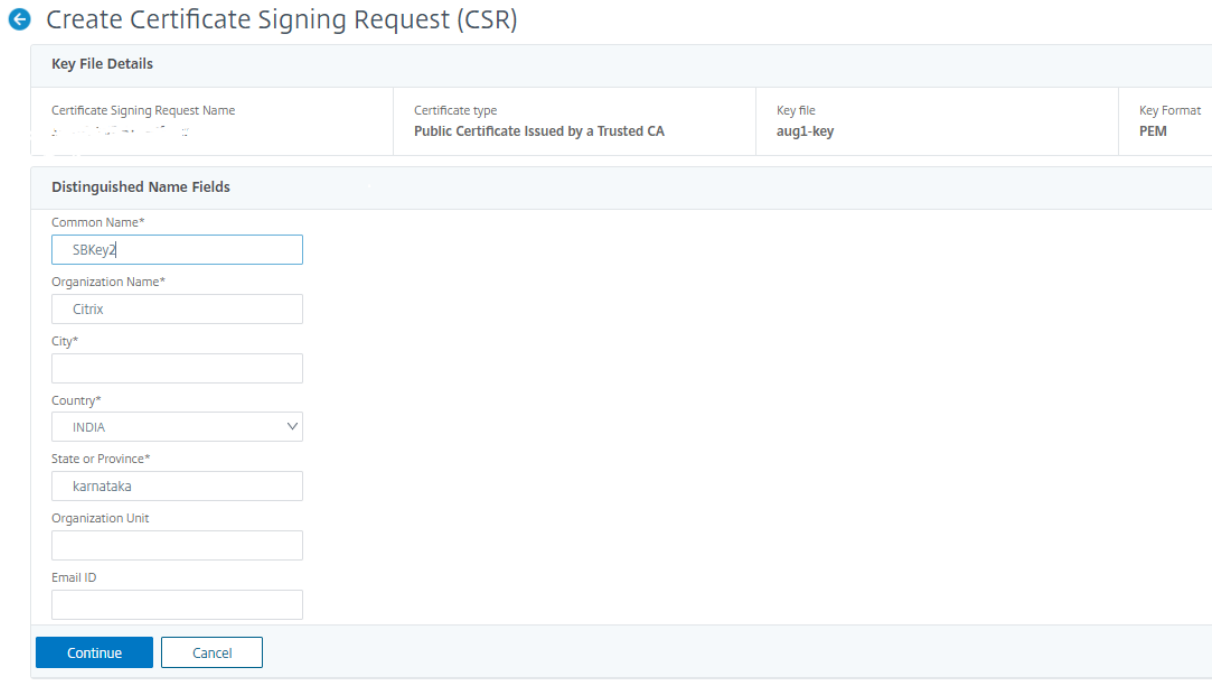
Para determinar y crear CSR, seleccione el certificado deseado y haga clic en **Crear CSR**.

Necesita tener un par de valores de clave pública o privada. Para cargar una clave, haga clic en **Elegir archivo** y selecciónelo en la lista. Para crear una clave, seleccione **No tengo una opción Clave** y

especifique los parámetros relevantes.

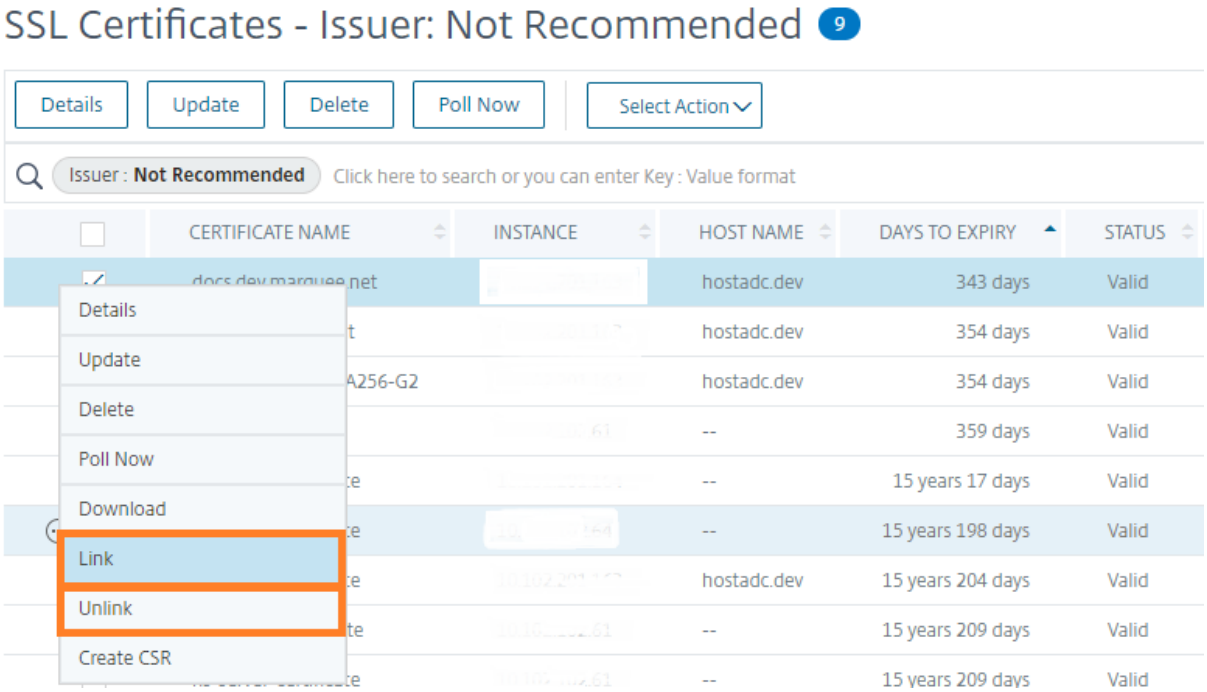


Para proporcionar más detalles de la clave seleccionada, como Nombre común, Nombre de organización, Ciudad, País, Estado, Unidad organizativa e ID de correo electrónico para crear la CSR.



Vincular y desvincular certificados SSL

Puede enlazar varios certificados SSL entre sí para crear un paquete de certificados. Para vincular un certificado a otro certificado, el emisor del primer certificado debe coincidir con el dominio del segundo certificado.

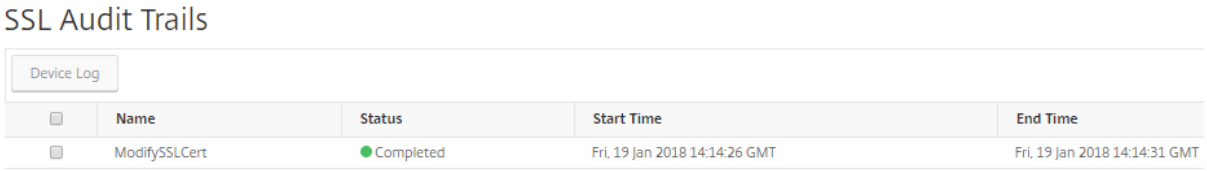


Registros de auditoría

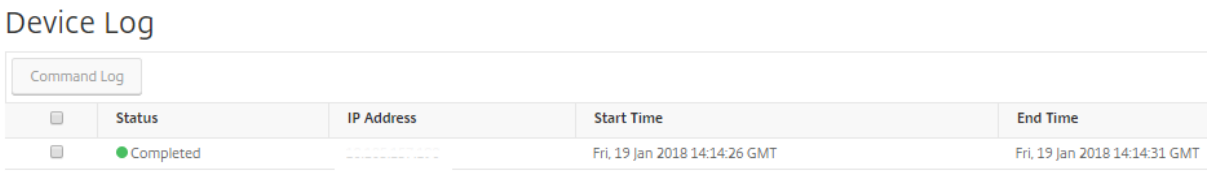
Registros de auditoría es una colección de archivos de registro de texto generados por NetScaler ADM. Muestra un historial de certificados SSL que se agregan, modifican y modifican mediante NetScaler ADM al dispositivo NetScaler específico. Los registros de auditoría también muestran la dirección IP del dispositivo NetScaler, el estado, la hora de inicio y la hora de finalización de la operación concreta.

En este ejemplo, es posible que quiera comprobar el cambio que se ha producido durante un período en el certificado concreto. Además, tiene una opción para ver el historial de cambios en el certificado a través del registro de dispositivos y el registro de comandos.

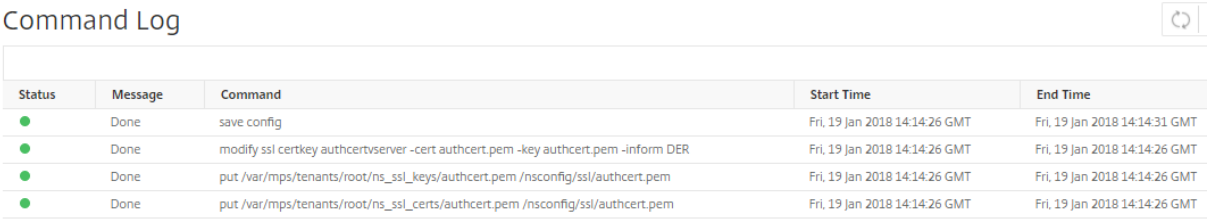
Para determinar la información de los certificados SSL, en el **Panel de control de SSL**, haga clic en **Registro de auditoría**. El resumen de la aplicación incluye el estado de los certificados SSL con Hora de inicio y Hora de finalización.



Para determinar la información del dispositivo NetScaler de un certificado SSL determinado, seleccione la casilla de verificación Certificado correspondiente que quiera. Haga clic en **Registro del dispositivo**.



Para ver la información del tipo de comando y el mensaje, haga clic en **Registro de comandos**.



Usar el panel SSL

January 30, 2024

Puede utilizar el panel de certificados SSL de NetScaler 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:

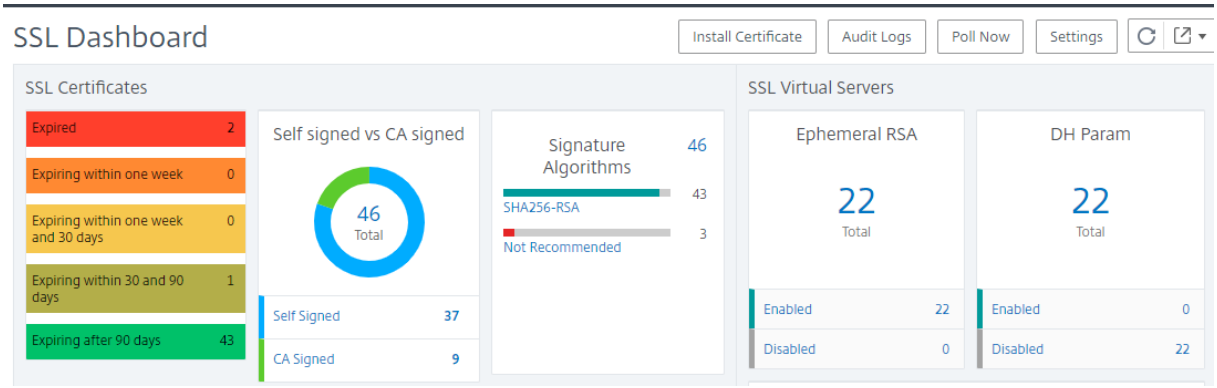
- Número de días después de los cuales caducan los certificados
- Número de certificados usados y no utilizados
- Número de certificados autofirmados y firmados por una CA
- Número de emisores
- algoritmos de firma
- Protocolos SSL
- Las 10 instancias principales por número de certificados en uso

Para supervisar certificados SSL

Puede utilizar el panel SSL de NetScaler ADM para supervisar sus certificados si su empresa tiene una directiva de SSL en la que ha definido ciertos requisitos de certificados SSL, como que todos los certificados deben tener un nivel de clave mínimo de 2048 bits y una autoridad de CA de confianza debe autorizarlo.

En otro ejemplo, puede que haya cargado un certificado nuevo pero se haya olvidado de enlazarlo 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 hacer clic en el gráfico para ver el nombre de los certificados, la instancia en la que se está utilizando, su validez, su algoritmo de firma, etc.

Para supervisar los certificados SSL en NetScaler ADM, vaya a **Infraestructura > Panel de control SSL**.



NetScaler ADM le permite sondear certificados SSL y agregar todos los certificados SSL de las instancias inmediatamente a NetScaler ADM. Para hacerlo,

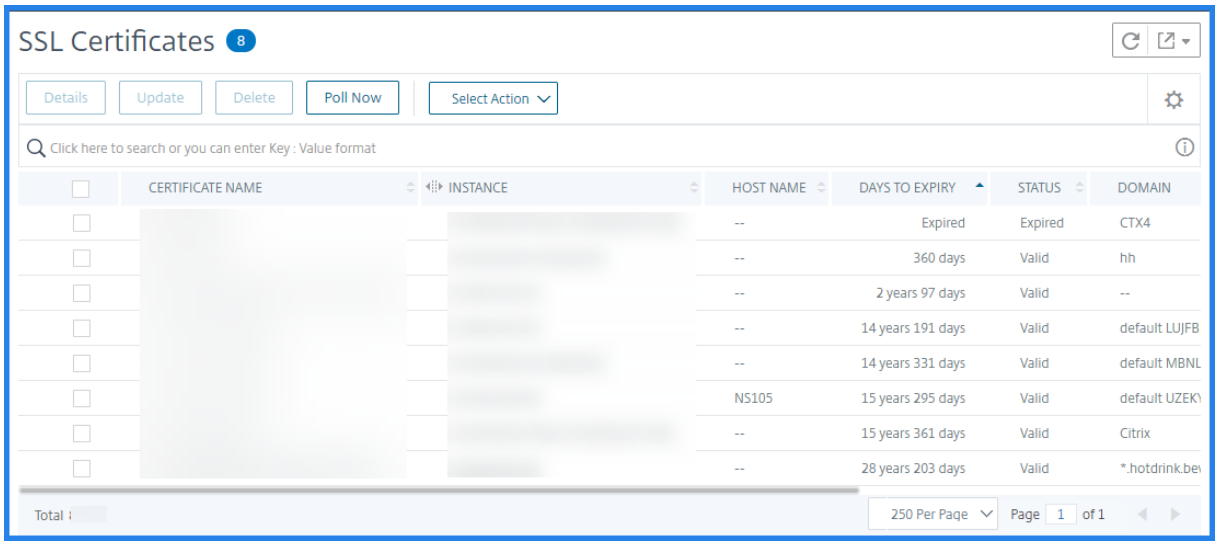
1. Vaya a **Infraestructura > Panel de control SSL**.
2. Haga clic en **Encuesta ahora**.

   En la página **Sondear ahora**, puede sondear todas las instancias de ADC gestionadas o seleccionar instancias específicas.
3. Haga clic en **Iniciar sondeo**.

En el **panel SSL**, puede supervisar los certificados SSL de ADC, los servidores virtuales SSL y los protocolos SSL.

Puede hacer clic en las métricas del panel para ver los detalles relacionados con los certificados SSL, los servidores virtuales SSL o los protocolos SSL.

Por ejemplo, cuando hace clic en el número bajo **Self signed vs CA signed** en el panel, la GUI de ADM muestra todos los certificados SSL en las instancias NetScaler.



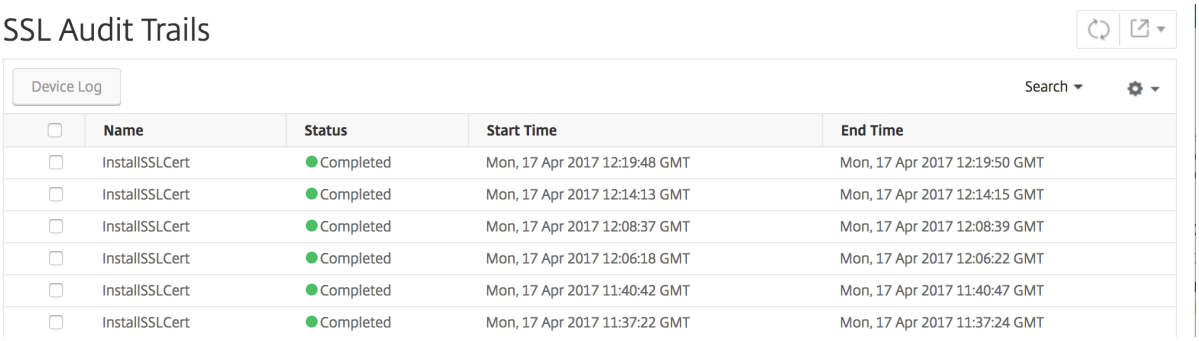
El panel de control SSL de NetScaler ADM también muestra la distribución de los protocolos SSL que se ejecutan en los servidores virtuales. Como administrador, puede especificar los protocolos que quiere supervisar a través de la directiva SSL; para obtener más información, consulte Configuración de directivas SSL. Los protocolos admitidos son SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3. 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 inhabilitar las teclas Diffie-Hellman (DH) o RSA efímera 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 apropiado se muestra una lista de los servidores virtuales en los que están habilitadas las claves RSA de DH o efímero.

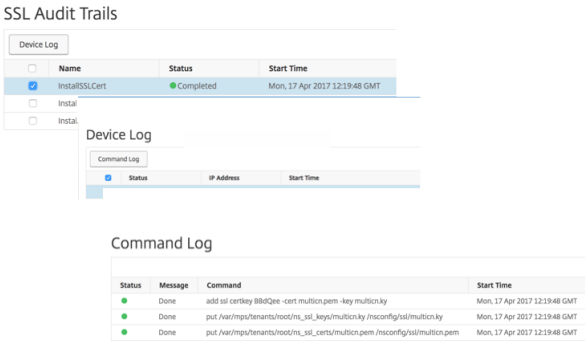
Para ver pistas de auditoría de certificados SSL

Ahora puede ver los detalles de registro de certificados SSL en NetScaler ADM. Los detalles del registro muestran las operaciones realizadas con certificados SSL en NetScaler 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 para una operación en particular realizada en NetScaler ADM mediante certificados SSL, vaya a **Infraestructura > Panel de control SSL** > y haga clic en **Registros de auditoría**.



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.

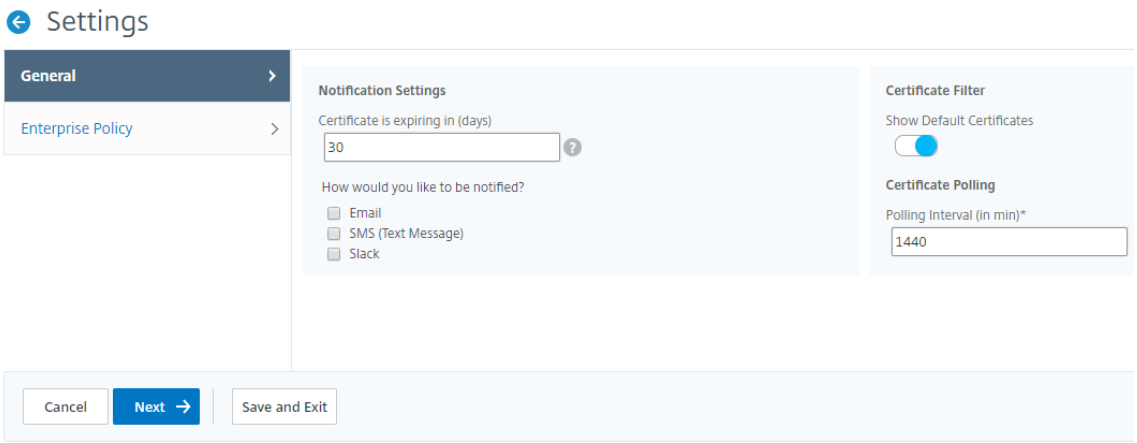


Para excluir certificados NetScaler predeterminados en el panel SSL

NetScaler ADM le permite mostrar u ocultar los certificados predeterminados de NetScaler 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 **Infraestructura > Panel SSL** en la GUI de NetScaler 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 **Mostrar certificados predeterminados** y haga clic en **Guardar y salir**.



Ver, cargar y descargar archivos SSL

Para ver los archivos SSL en NetScaler ADM, vaya a **Infraestructura > Panel de control SSL > Archivos SSL en NetScaler ADM**.

Puede ver, cargar y descargar los siguientes archivos en NetScaler ADM:

- Certificados de SSL
- Claves SSL
- CSR SSL

Para ver y descargar archivos SSL en una instancia de NetScaler, vaya a **Infraestructura > Panel de control SSL > Archivos SSL en NetScaler**.

Puede acceder a los archivos SSL solo después de realizar una copia de seguridad de las instancias de NetScaler, ya sea manualmente o mediante un proceso de copia de seguridad programado.

> **Importante:**
>
> Para habilitar la descarga de archivos SSL desde instancias ADC, habilite la función **Certificados SSL de instancia**. Para obtener más información, consulte Habilitar o inhabilitar las funciones

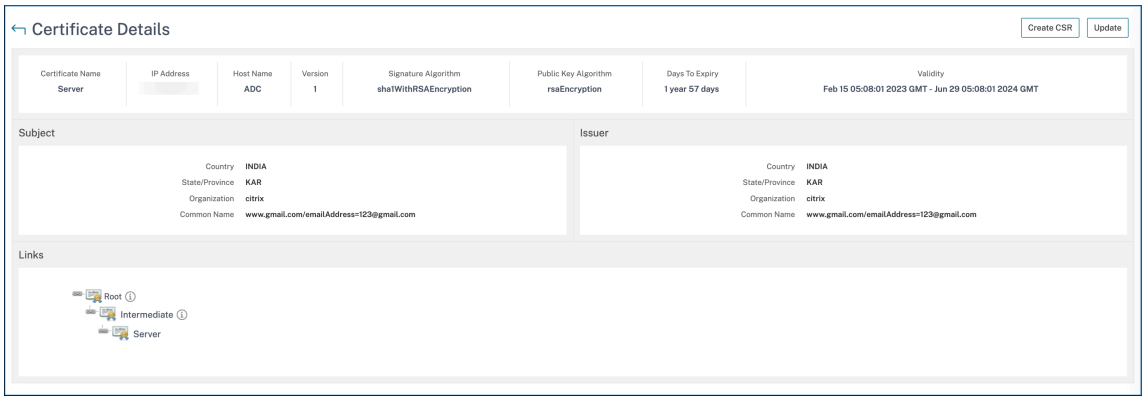
de ADM.

Ver cadena de certificados SSL

Puede ver la cadena de certificados completa, desde los certificados intermedios hasta el certificado de la CA raíz.

Para ver una cadena de certificados:

1. Vaya a **Infraestructura > Panel de control SSL** y haga clic en los certificados SSL de cualquier icono.
2. En la página **Certificados SSL**, seleccione un certificado y haga clic en **Detalles**. La cadena de certificados se muestra en **Vínculos**.



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.

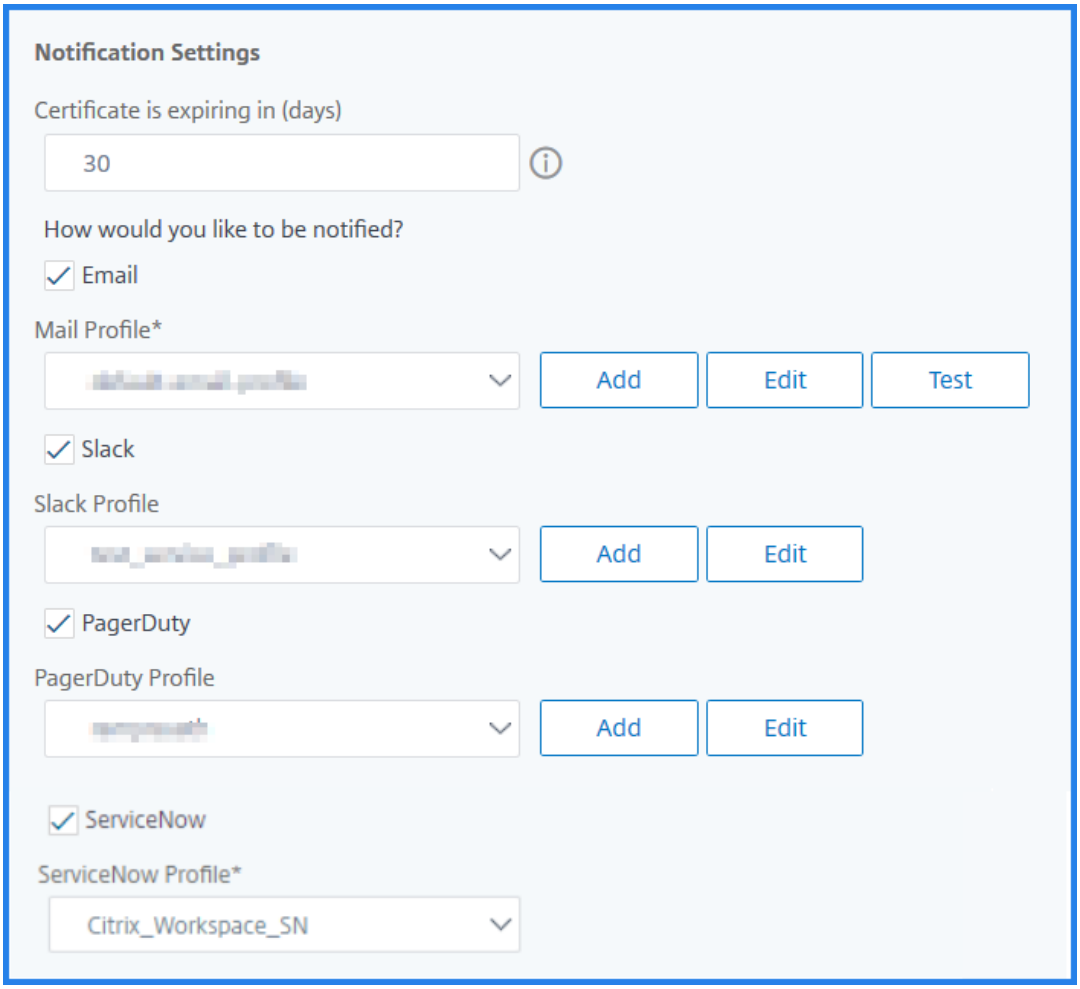
Para configurar notificaciones desde NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a **Infraestructura**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.
    - **Alertas de PagerDuty**: Especifique un perfil de PagerDuty. Según la configuración de notificaciones configurada en su portal de PagerDuty, se envía una notificación cuando sus certificados están a punto de caducar.
    - **ServiceNow**: se envía una notificación al perfil predeterminado de ServiceNow cuando los certificados están a punto de caducar.

      > **Importante**
      >
      > Asegúrese de que Citrix Cloud ITSM Adapter esté configurado para ServiceNow e integrado con NetScaler ADM. Para obtener más información, consulte Integrar NetScaler ADM con la instancia de ServiceNow.



6. Haga 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. NetScaler 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.

Puede configurar los destinos de capturas si va a **Configuración > SNMP > Destinos de capturas**. 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.

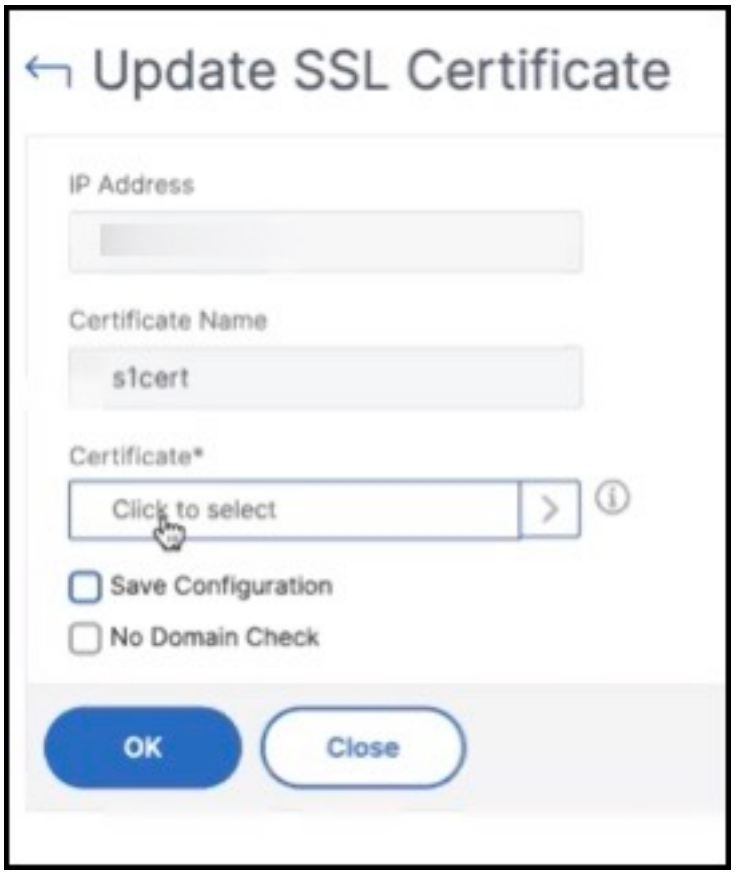
Actualizar un certificado instalado

January 30, 2024

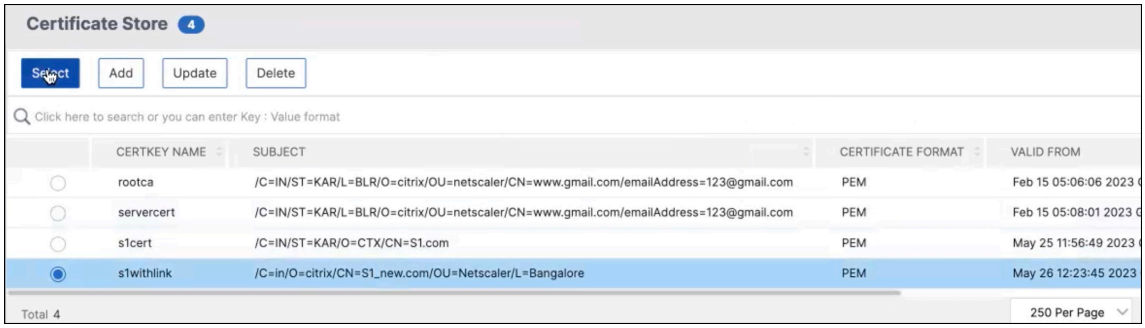
Después de recibir un certificado renovado de la entidad de certificación (CA), no tiene que iniciar sesión en instancias individuales de NetScaler para actualizar los certificados. Puede actualizar los certificados existentes en NetScaler ADM con certificados del almacén de certificados.

Para actualizar un certificado SSL desde NetScaler ADM:

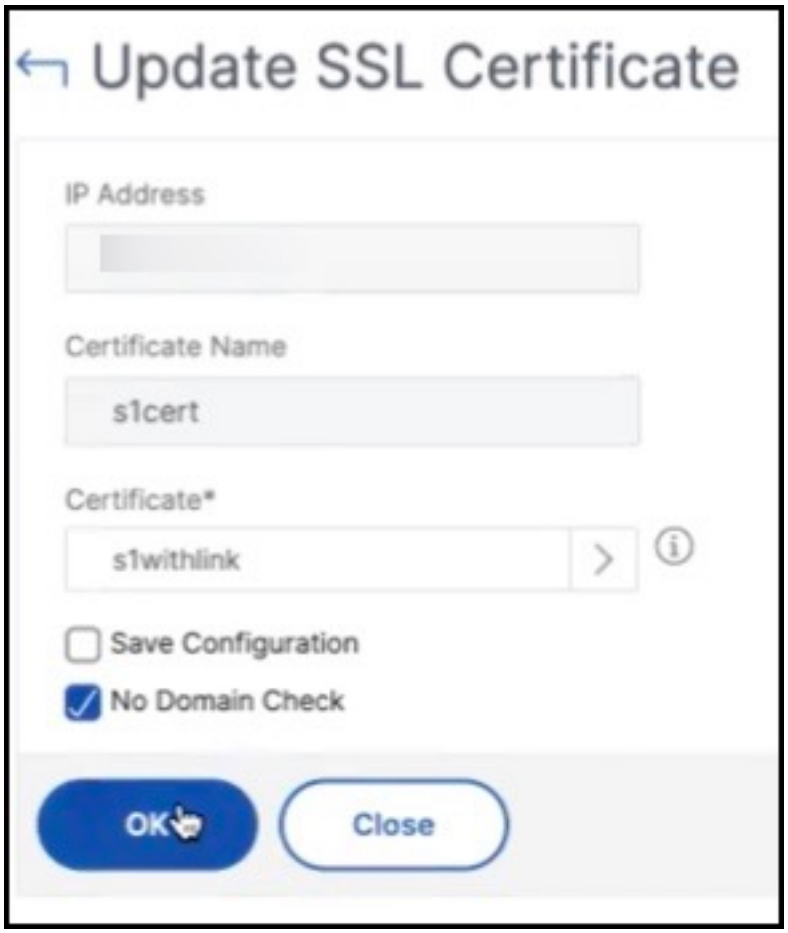
1. En NetScaler ADM, vaya a **Infraestructura > Panel SSL**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. En la página **Certificados SSL**, seleccione un certificado y haga clic en **Actualizar**. También puede hacer clic en el certificado SSL para ver sus detalles y, a continuación, haga clic en **Actualizar** en la esquina superior derecha de la página **Certificado SSL**.
4. En la página **Actualizar certificado SSL**, seleccione **Certificado** para ver la página del **almacén de certificados**.



5. En la página **Almacén de certificados**, seleccione el archivo de certificado que desee agregar. Haga clic en **Seleccionar**.



6. Si el nombre de dominio del nuevo certificado no coincide con el certificado anterior, seleccione **Sin comprobación de dominio** si quiere que el servidor aloje el nuevo dominio.



Haga clic en **Aceptar**. Todos los servidores virtuales SSL a los que está vinculado este certificado se actualizan automáticamente.

> **Nota:**
>
> Al actualizar un certificado SSL existente con una cadena de certificados del almacén de certificados, el certificado existente se actualiza con los certificados vinculados. Seleccione el certificado y haga clic en **Detalles** para ver la cadena de certificados.

Instalar certificados SSL en una instancia de NetScaler

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:

También puede importar un certificado de una instancia de NetScaler seleccionada y aplicarlo a otras instancias de NetScaler específicas desde la GUI de NetScaler Application Delivery Management (ADM).

1. Vaya a **Infraestructura > Panel de control 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:

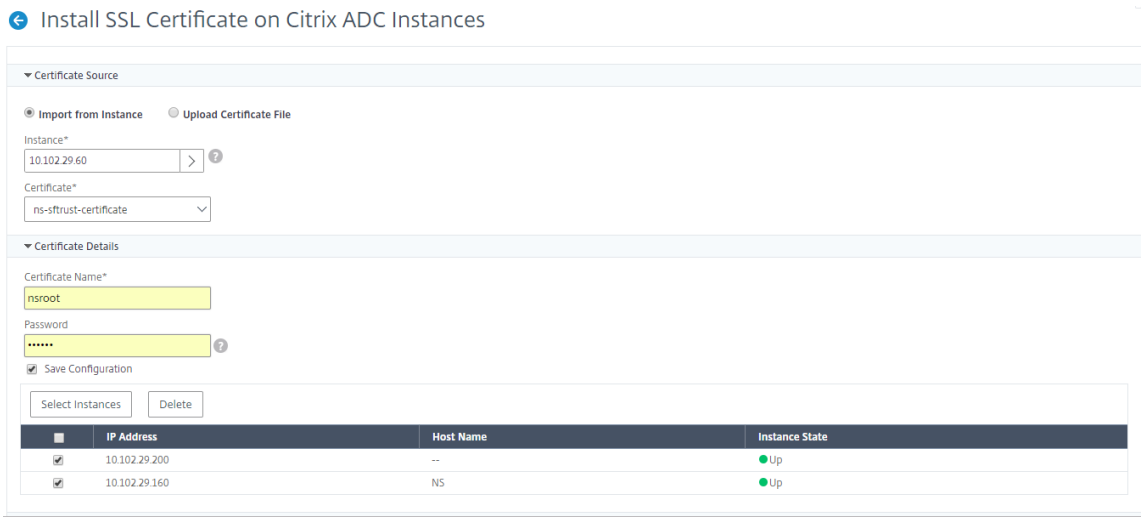
    a) Origen de certificado
    Seleccione la opción **Importar desde instancia**.

    - 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

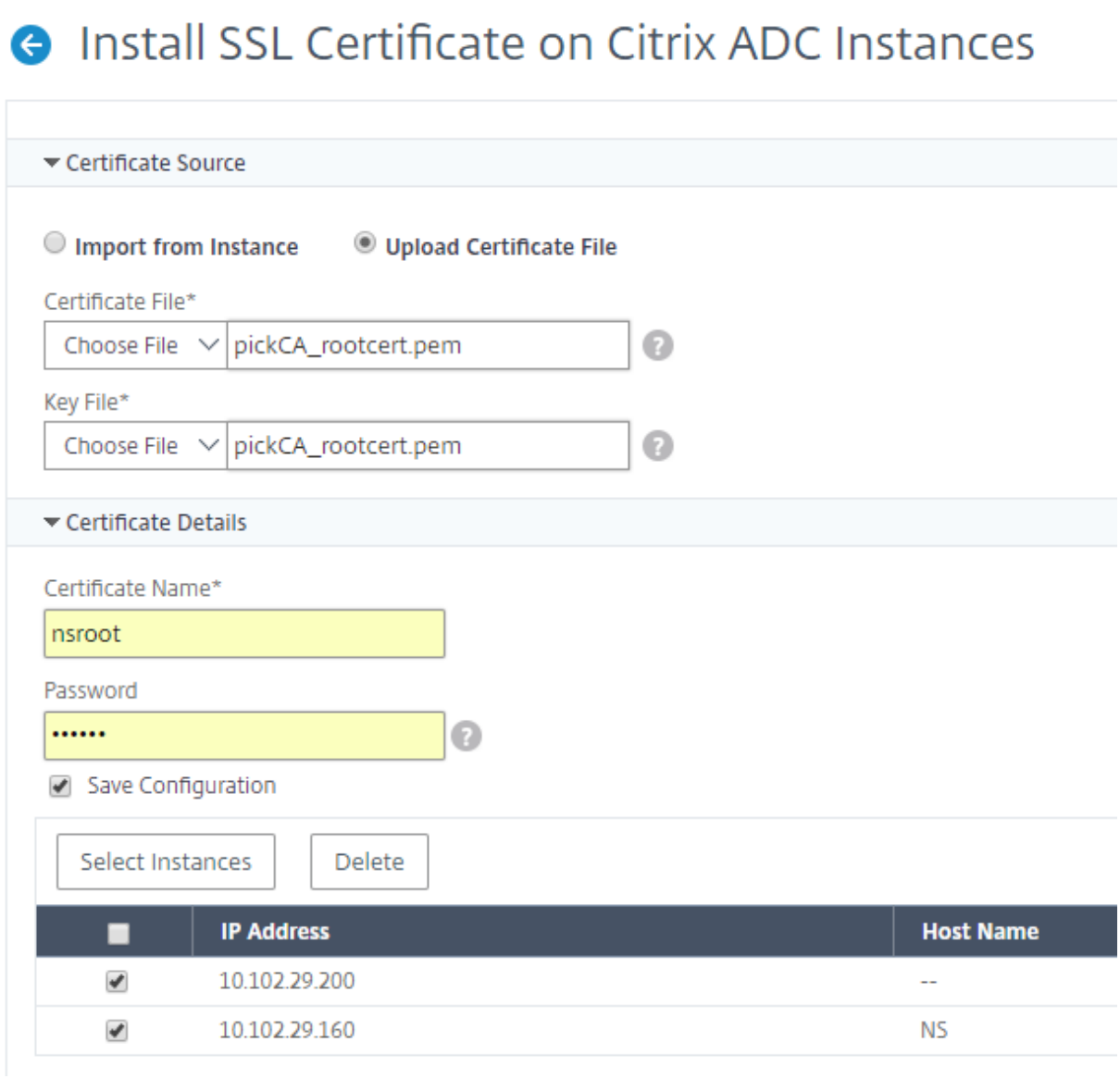
    - **Nombre del certificado**. Especifique un nombre para la clave del certificado.
    - **Contraseña**. Contraseña para cifrar la clave privada. Puede utilizar esta opción para cargar claves privadas cifradas.

4. Haga clic en **Seleccionar instancias** para seleccionar las instancias de NetScaler en las que quiere instalar sus certificados.
5. Haga clic en **Aceptar**.



Para instalar un certificado SSL desde NetScaler ADM:

1. En NetScaler ADM, vaya a **Infraestructura > Panel SSL**.
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 equipo local) o **Appliance** (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 NetScaler ADM en las que desea 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 **Infraestructura**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.

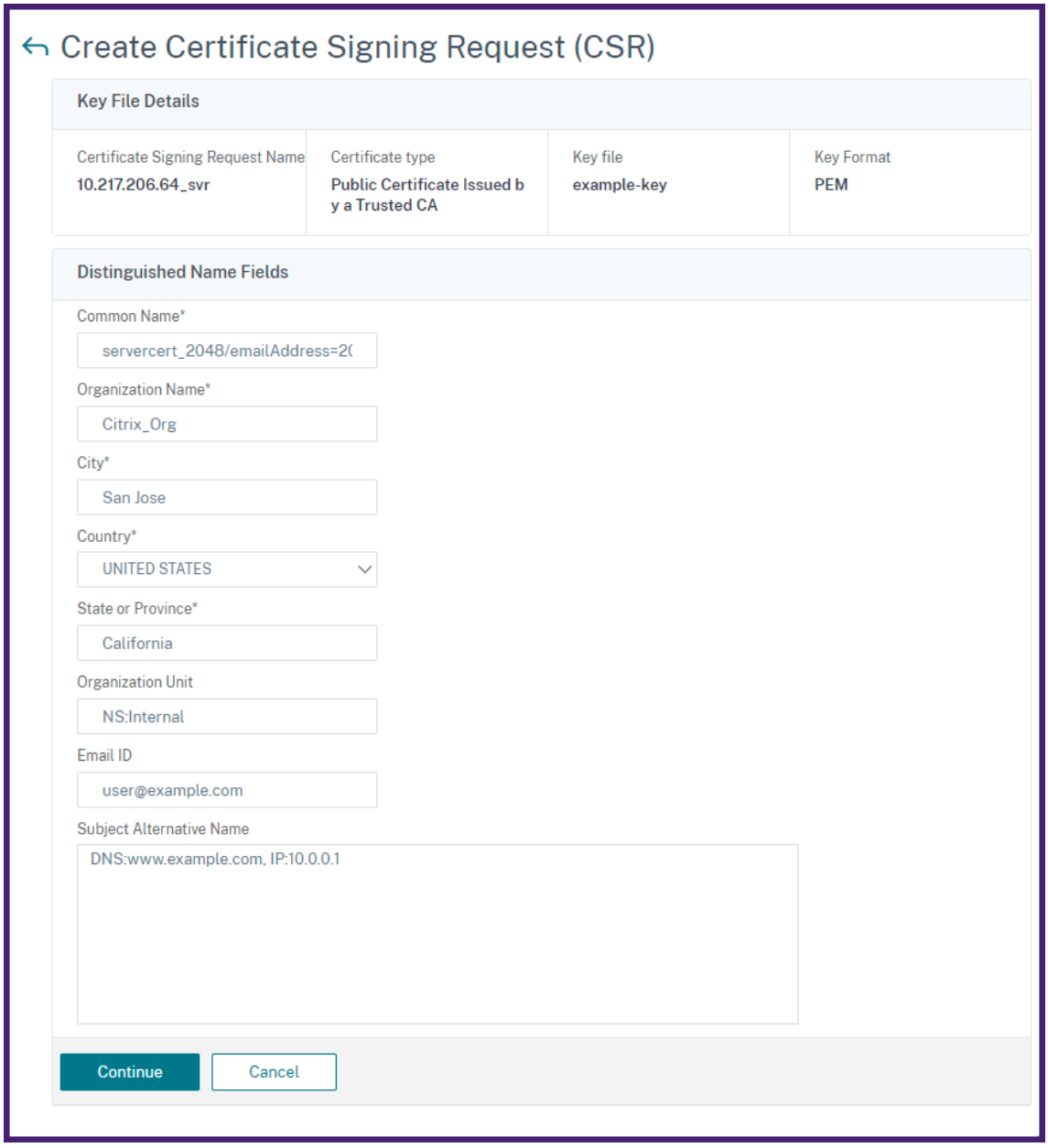
5. Haga clic en **Continuar**.
6. En la siguiente página, proporcione más detalles.

   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.

En el campo **Nombre alternativo del sujeto**, puede especificar varios valores, como nombres de dominio y direcciones IP con un único certificado. Los nombres alternativos del sujeto ayudan a proteger varios dominios con un único certificado.

Especifique los nombres de dominio y las direcciones IP en el siguiente formato:

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```



En este ejemplo, asegura `10.0.0.1` y `www.example.com`.

Revise los campos y haga clic en **Continuar**.

> **Nota**
>
> La mayoría de los CA aceptan envíos de certificados por correo electrónico. La CA devuelve un certificado válido a la dirección de correo electrónico desde la que envía 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 **Infraestructura**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 NetScaler ADM, vaya a **Infraestructura > Panel SSL**.
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 fortaleza de la clave del certificado no coincide con la seguridad de la clave recomendada en la política 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 NetScaler 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.

> **Nota**
>
> El panel de control de SSL solo muestra los **algoritmos de firma** que se seleccionan a través de la opción **Configuración** y otros se muestran como **No recomendado**.

Encuesta de certificados SSL de instancias NetScaler

January 30, 2024

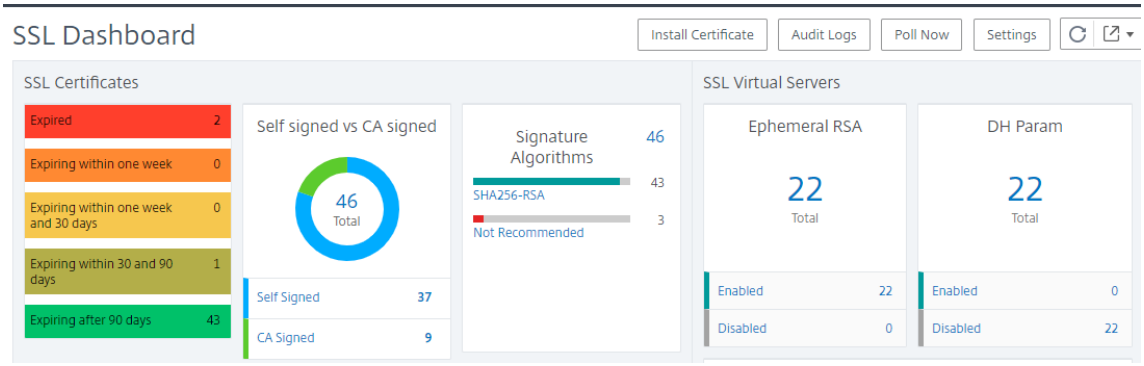
NetScaler Application Delivery Management (ADM) sondea automáticamente los certificados SSL una vez cada 24 horas mediante las llamadas de NITRO y el protocolo Secure Copy (SCP). También puede sondear manualmente los certificados SSL para descubrir los certificados SSL recién agregados en las

instancias de Citrix Application Delivery Controller (ADC). El sondeo de todos los certificados SSL de instancias NetScaler coloca una carga pesada en la red.

En lugar de sondear todos los certificados SSL de las instancias de NetScaler, puede sondear manualmente solo los certificados SSL de una o varias instancias seleccionadas.

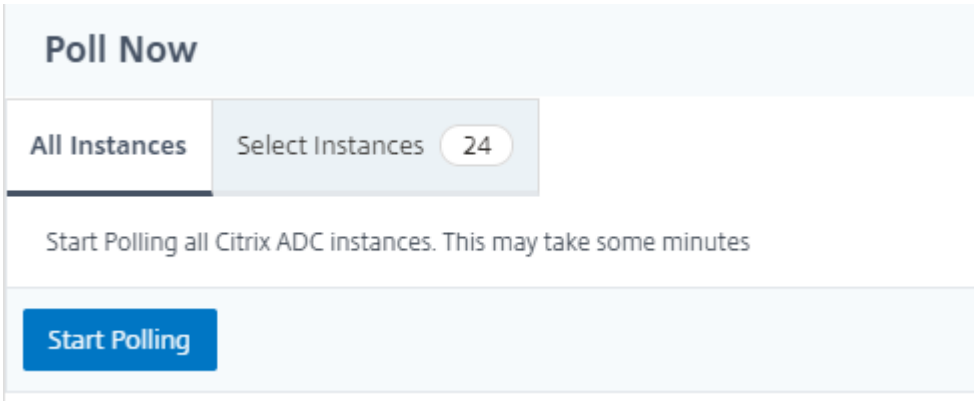
Para sondear certificados SSL en instancias NetScaler:

1. En NetScaler ADM, vaya a **Infraestructura > Panel SSL**.
2. En la página **SSL Dashboard**, en la esquina superior derecha, haga clic en **Sondear ahora**.

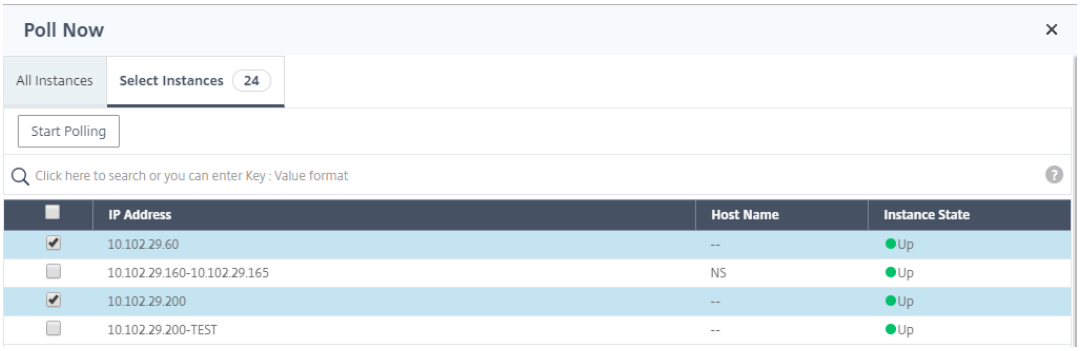


3. Aparece la página **Encuesta ahora**, que le da la opción de sondear todas las instancias de NetScaler en la red o sondear las instancias seleccionadas.

   a) Para sondear los certificados SSL de todas las instancias de NetScaler, 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**.



Utilice el almacén de certificados ADM de NetScaler para administrar los certificados SSL

January 30, 2024

El almacén de certificados NetScaler ADM le ayuda a almacenar y administrar sus certificados SSL en una sola ubicación. Más adelante, podrá utilizar los certificados almacenados para configurar los ajustes de NetScaler.

El almacén de certificados le permite añadir, actualizar y eliminar certificados SSL. También puede usar el almacén de certificados para importar un certificado de una instancia de NetScaler y aplicarlo a otras instancias de NetScaler de destino.

Agregar certificados SSL al almacén de certificados

1. Vaya a **Infraestructura > Panel de control de SSL > Almacén de certificados**. Haga clic en **Agregar**.
2. En la página **Agregar certificado**, introduzca los siguientes detalles:
    - **Nombre de la clave de certificado**: introduzca un nombre para el certificado. El nombre debe tener únicamente caracteres alfanuméricos, guiones bajos y caracteres ASCII y debe tener menos de 30 caracteres. No puede cambiar el nombre después de crear el certificado.
    - **Archivo de certificado**: navegue hasta su unidad local y cargue el archivo de certificado.
    - **Archivo clave**: cargue el archivo clave desde su equipo local.
    - **Contraseña**: si tiene una clave privada cifrada en formato PEM, escriba la frase de contraseña que se utilizó para cifrar la clave privada.

- **Agregar cadena de certificados**: seleccione esta opción para añadir el certificado a una cadena de certificados.
- **Cadena de certificados**: busque su unidad local y cargue el archivo de certificado.
- Haga clic en **Crear**.

Actualizar los certificados SSL en el almacén de certificados

1. Vaya a **Infraestructura > Panel de control de SSL > Almacén de certificados**. Seleccione el certificado que desee actualizar y haga clic en **Actualizar**.
2. En la página **Actualizar certificado**, introduzca los siguientes detalles:
   - **Nombre de la clave de certificado**: muestra el nombre del certificado que ha seleccionado para actualizar.
   - **Archivo de certificado**: para actualizar el archivo de certificado, cargue un archivo de certificado.
   - **Archivo clave**: para actualizar el archivo clave, cargue un archivo clave desde su computadora local.
   - **Contraseña**: si tiene una clave privada cifrada en formato PEM, escriba la frase de contraseña que se utilizó para cifrar la clave privada.
   - **Agregar cadena de certificados**: seleccione esta opción para añadir el certificado a una cadena de certificados.
   - **Cadena de certificados**: busque su unidad local y cargue el archivo de certificado.
   - Haga clic en **Aceptar**.

Eliminar los certificados SSL del almacén de certificados

1. Vaya a **Infraestructura > Panel de control de SSL > Almacén de certificados**. Haga clic en **Agregar**.
2. Cuando se le solicite, haga clic en **Sí** para eliminar el certificado.

Instalar certificados SSL en instancias de NetScaler

1. Vaya a **Infraestructura > Panel de control de SSL > Almacén de certificados**. Seleccione el certificado que desee instalar en una instancia de NetScaler.

2. En la página **Instalar el certificado SSL en las instancias de NetScaler**, introduzca los siguientes detalles:

   a. **Origen del certificado**

   - **Certificado**: muestra el nombre del certificado que ha seleccionado.

   b. **Detalles del certificado**

   - **Nombre del certificado**: muestra el nombre del certificado.
   - **Guardar configuración**: seleccione esta opción para guardar la configuración de NetScaler. La configuración de NetScaler se guarda después de instalar el certificado.

3. Haga clic en **Seleccionar instancias** para seleccionar las instancias de NetScaler en las que quiere instalar sus certificados.

Haga clic en **Aceptar**.

Importación de certificados desde instancias de NetScaler

1. Vaya a **Infraestructura > Panel de control de SSL > Almacén de certificados**. Haga clic en **Importar certificados ADC**.
2. En la página **Importar certificados ADC**, puede seleccionar una de las siguientes fichas:

   - **Importar certificados ADC**: haga clic en **Iniciar sondeo** para sondear todos los certificados SSL de todas las instancias de NetScaler.
   - **Seleccionar instancias**: seleccione una instancia de NetScaler y **haga clic en Importar certificados ADC** para sondear los certificados SSL solo en la instancia de NetScaler seleccionada.

   Tras el sondeo, los certificados SSL y los archivos de claves se descargan y se añaden al almacén de certificados.

   > **Nota:**
   >
   > La operación de importación no se realiza correctamente para los certificados si existen nombres de certificados idénticos en el almacén. Sin embargo, la operación de importación continúa sondeando los certificados restantes y agrega los certificados de NetScaler, si están disponibles, al almacén.

Administre los certificados y cifrados personalizados de bases de datos en una implementación de alta disponibilidad

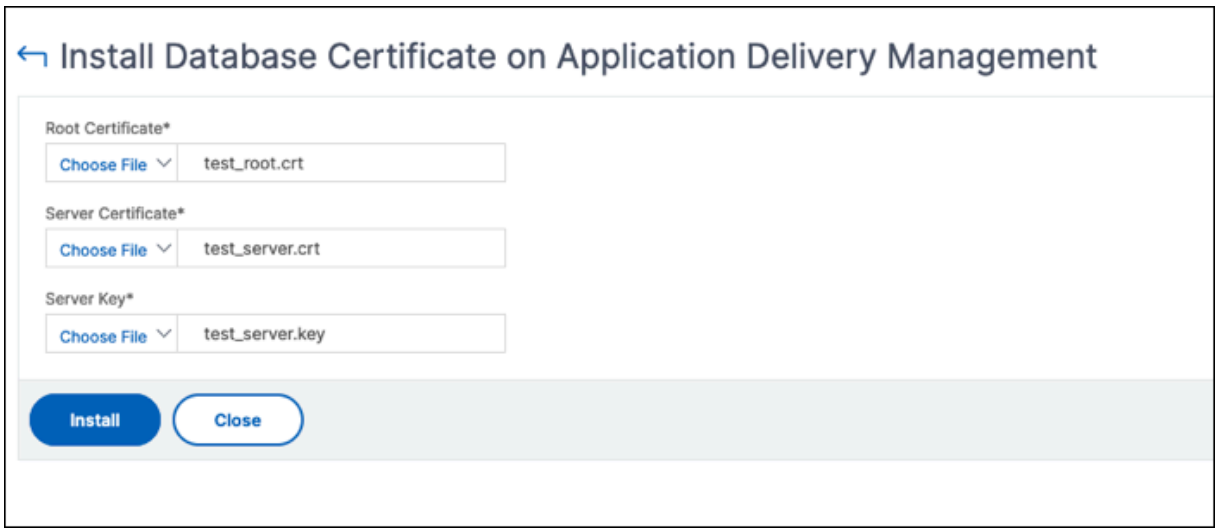
January 30, 2024

NetScaler ADM le permite reemplazar los certificados de base de datos integrados predeterminados por sus propios certificados de una entidad de certificación de confianza. También puede configurar sus propios conjuntos de cifrado en la base de datos ADM de NetScaler. Esta función proporciona una mayor flexibilidad y seguridad para sus necesidades de administración de certificados y protege todas las comunicaciones entre sus nodos de alta disponibilidad con certificados SSL de confianza.

Instale los certificados de base de datos en NetScaler ADM

Para instalar sus certificados en una configuración de alta disponibilidad:

1. Vaya a **Configuración > Implementación de alta disponibilidad** y haga clic en **Certificados de base de datos**.
2. Haga clic en la ficha **Certificado instalado** y, a continuación, en **Instalar nuevo certificado**.
3. En la página **Instalar el certificado de base de datos en Application Delivery Management**, cargue un certificado raíz, un certificado de servidor y una clave de servidor. Puede realizar una de las siguientes acciones:
    - **Seleccione Archivo > Local** para cargar un archivo de certificado o clave desde su máquina local.
    - **Elija Archivo > Dispositivo** para cargar un archivo de certificado o clave que esté presente en NetScaler ADM.
4. Haga clic en **Instalar**.

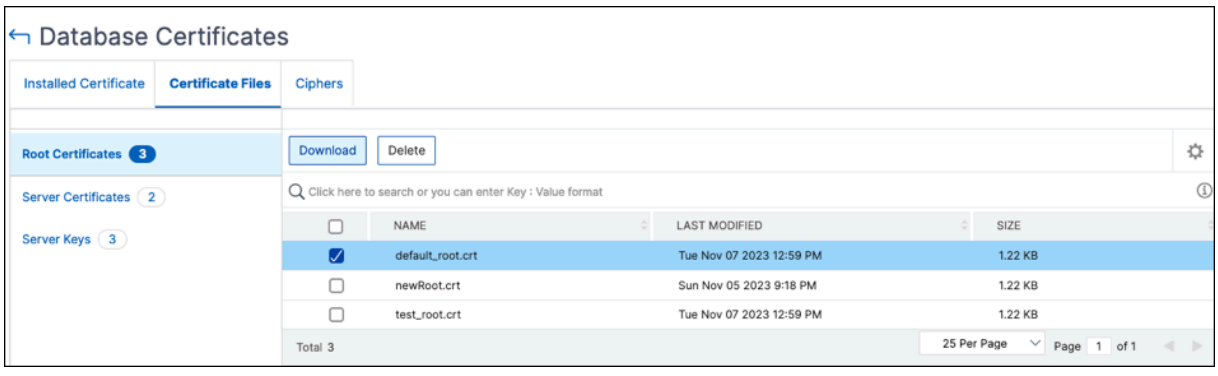


> **Nota:**
>
> Si hay varios certificados en cadena, debe combinarlos en un único archivo. Asegúrese de que el orden de concatenación sea correcto, con los certificados intermedios primero y luego el certificado raíz. Este orden es esencial para que la cadena de certificados se reconozca correctamente.
>
> Por ejemplo, el siguiente comando agrega el contenido de cada archivo de certificado (intermediate_certificate1.crt, intermediate_certificate2.crt y root_certificate.crt) al archivo denominado combined_certs.crt:
>
> ```
> cat intermediate_certificate1.crt >> combined_certs.crt
> cat intermediate_certificate2.crt >> combined_certs.crt
> cat root_certificate.crt >> combined_certs.crt
> ```

Administre los certificados de bases de datos instalados

Para ver, descargar y eliminar los certificados instalados:

1. Vaya a **Configuración > Implementación de alta disponibilidad** y haga clic en **Certificados de base de datos**.
2. Haga clic en la ficha **Archivos de certificados** y seleccione **Certificados raíz, Certificados**de **servidor o Claves** de servidor para ver los archivos correspondientes.
3. Para descargar un archivo a su máquina local, haga clic en **Descargar**.
4. Para eliminar un archivo de certificado, selecciónelo y haga clic en **Eliminar**. En el cuadro de diálogo de confirmación que aparece, haga clic en **Aceptar**.

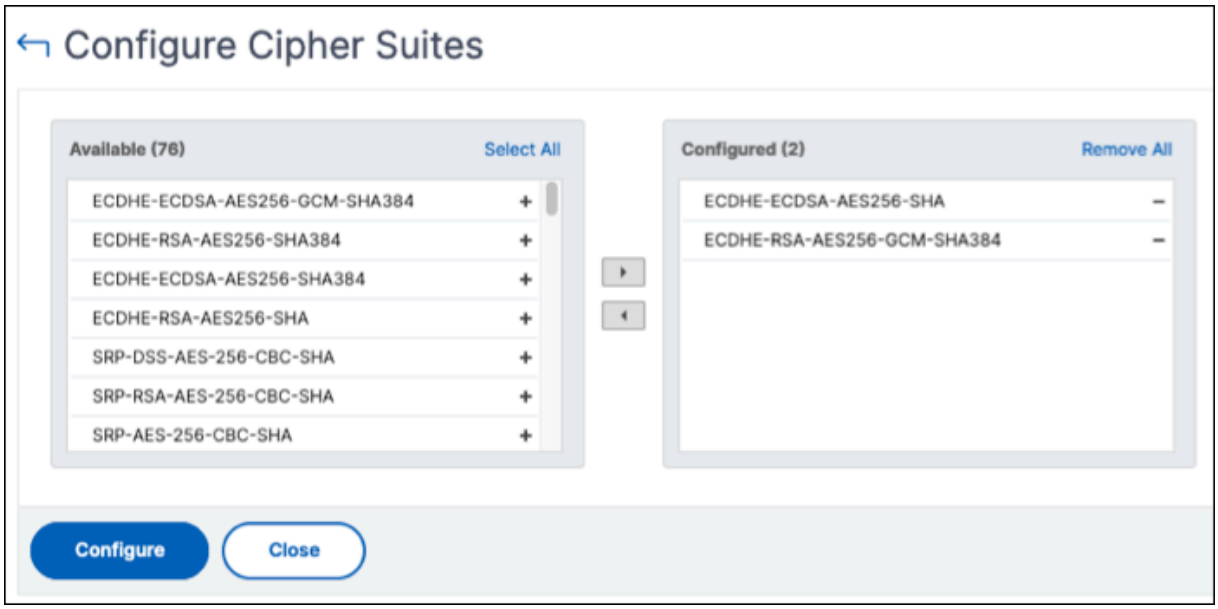


Configurar conjuntos de cifrado de bases de datos

Para configurar conjuntos de cifrado para una implementación de alta disponibilidad:

1. Vaya a **Configuración > Implementación de alta disponibilidad** y haga clic en **Certificados de base de datos**.

2. Haga clic en la ficha **Cifrados** y, a continuación, en **Configurar cifrado**.
3. En la página **Configurar conjuntos de cifrado**, seleccione uno o más cifrados de la lista de cifrados disponibles.
4. Haga clic en **Configurar**. En el cuadro de diálogo de confirmación que aparece, haga clic en **Sí** para cambiar la configuración de cifrado.



> **Nota:**
>
> Al cambiar la configuración de cifrado, se reinician los nodos secundarios y de recuperación ante desastres de NetScaler ADM.

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 a NITRO y se agrega implícitamente como destino de captura para que la instancia reciba sus trampas o eventos.

Los eventos representan ocurrencias de eventos o errores en una instancia administrada de NetScaler. 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 de resumen de eventos (**Infraestructura > Eventos**) y todos los eventos activos se muestran en la página Mensajes de eventos (**Infraestructura > Eventos > Mensajes de eventos**).

NetScaler ADM también comprueba los eventos generados en las instancias para formar alarmas de diferentes niveles de gravedad. Estas alarmas se muestran como mensajes, algunos de los cuales

pueden requerir atención inmediata. Por ejemplo, la falla del sistema se puede clasificar como una gravedad de evento "Crítica"y debería abordarse inmediatamente.

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de los eventos, que pueden ser muchos, generados en toda la infraestructura de NetScaler.

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, categoría, objetos de error, comandos de configuración y mensajes.

También puede asegurarse de que se activan varias notificaciones para un evento durante un intervalo de tiempo específico, hasta que se borre el evento. Como medida adicional, puede personalizar su correo electrónico con una línea de asunto y un mensaje de usuario específicos, y cargar un archivo adjunto.

Usar panel de eventos

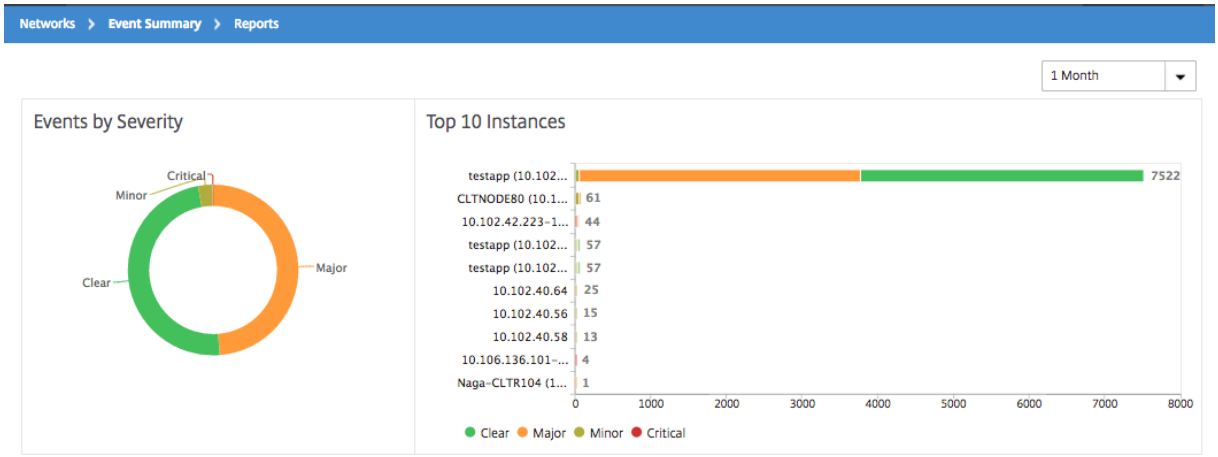
January 30, 2024

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.

Para ver los detalles en el panel de eventos:

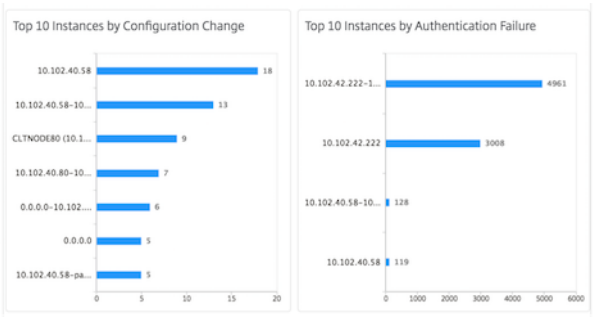
Vaya a **Infraestructura > Eventos > Informes**.

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 de la gravedad del evento.

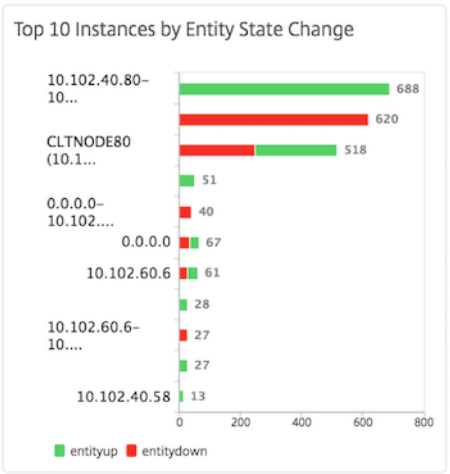


Para ver más detalles, vaya al tipo de instancia de NetScaler (**Infraestructura > Eventos > Informes** > **NetScaler/ NetScaler SDX**) para ver lo siguiente:

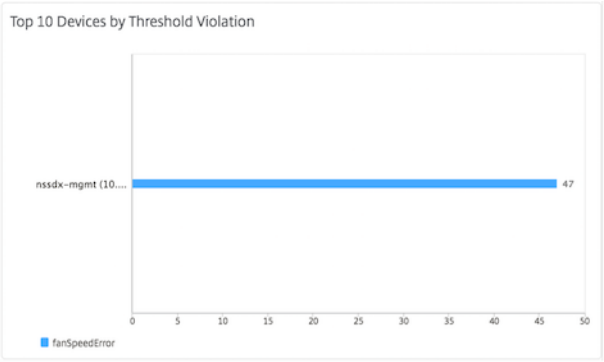
- Los 10 dispositivos principales por fallo de hardware
- Los 10 dispositivos principales por cambio de configuración
- Los 10 dispositivos principales por error de autenticación



- 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

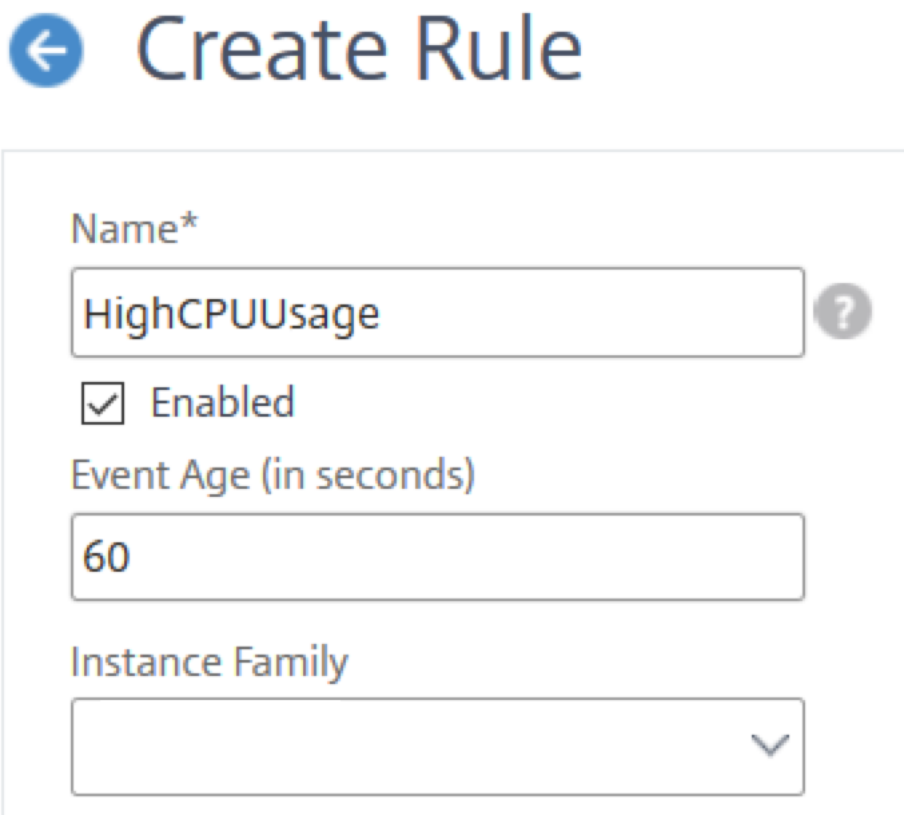
Puede configurar la opción de antigüedad del evento para especificar el intervalo de tiempo (en segundos). NetScaler ADM supervisa los dispositivos hasta la duración establecida y genera un evento solo si la antigüedad del evento supera la duración establecida.

> 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. A continuación, siempre 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 NetScaler ADM, vaya a **Infraestructura > 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 capturas `entityup`, `entitydown` y `entityofs`.

Programar un filtro de eventos

January 30, 2024

Tras crear un filtro para su regla, si no desea que el servidor NetScaler Application Delivery Management (ADM) envíe una notificación cada vez que el evento generado cumpla con los criterios del filtro, puede programar el filtro para que se active únicamente en intervalos de tiempo específicos, como diario, semanal o mensual.

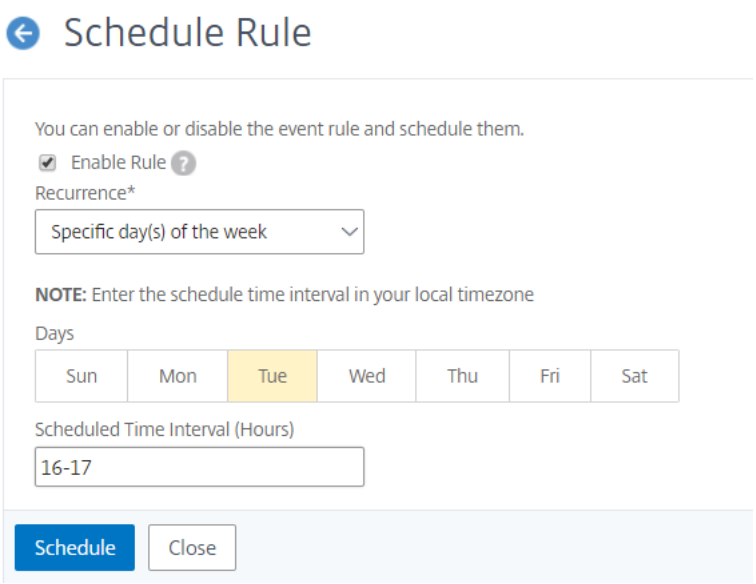
Por ejemplo, si ha programado una actividad de mantenimiento del sistema para diferentes aplicaciones en las instancias en diferentes momentos, las instancias pueden generar varias alarmas.

Si ha configurado un filtro para estas alarmas y ha habilitado las notificaciones por correo electrónico para estos filtros, el servidor envía una gran cantidad de notificaciones por correo electrónico cuando NetScaler 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 NetScaler ADM, vaya a **Infraestructura > 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**: Active esta casilla de verificación para habilitar la regla de evento programado.
   - **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)**: Horas en las 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

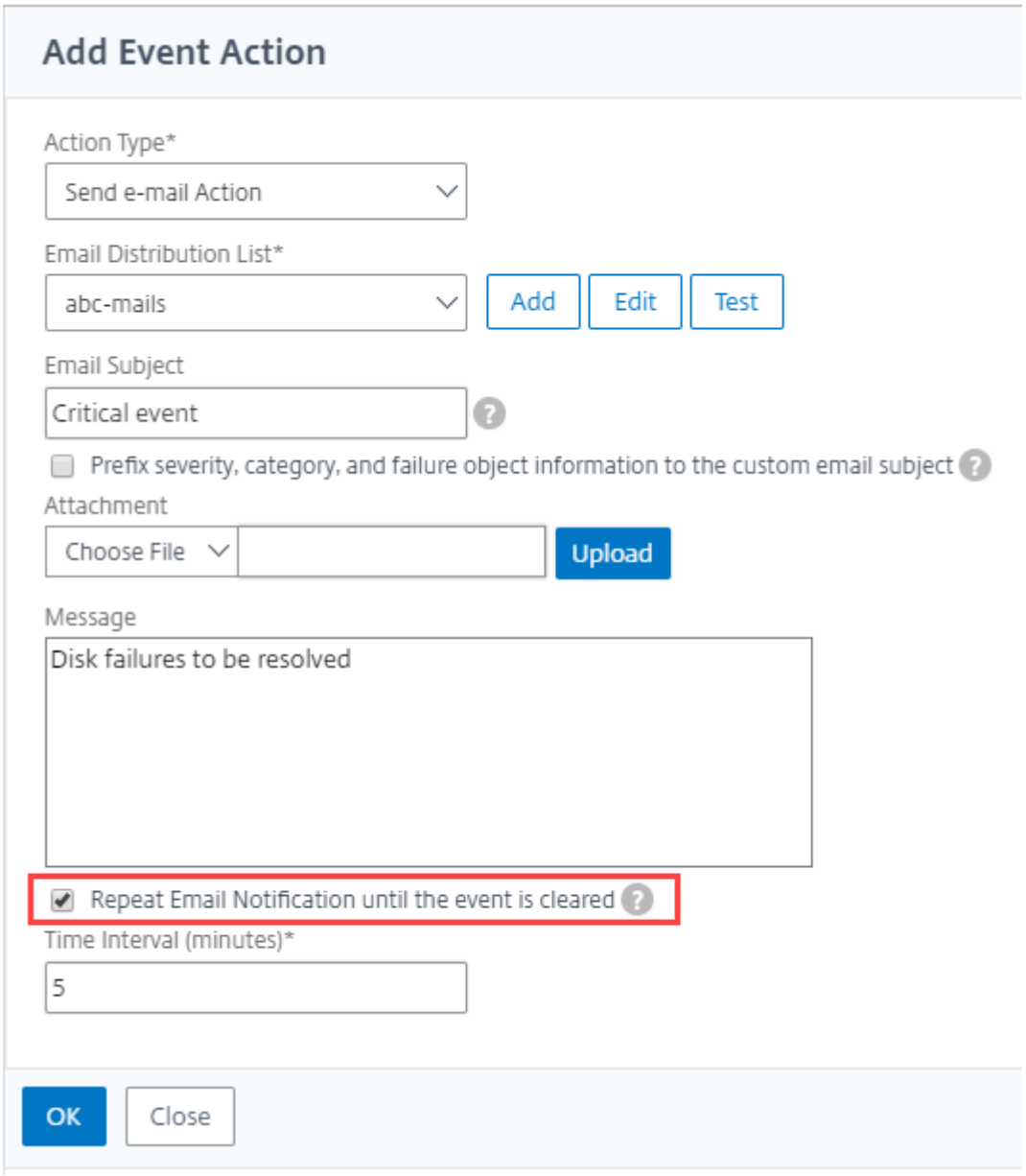
Para garantizar que se aborden todos los eventos críticos y no se omita ninguna notificación importante por correo electrónico, puede optar por enviar notificaciones por correo electrónico repetidas para las reglas de eventos que cumplan con los criterios que has seleccionado. Por ejemplo, si ha creado 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 **Infraestructura > Eventos > Resumen de eventos**, elija una **categoría**, seleccione un evento en la categoría y haga clic en **Borrar**.
> - O bien, vaya a **Infraestructura > 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 NetScaler Application Delivery Management (ADM), vaya a **Infraestructura > 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

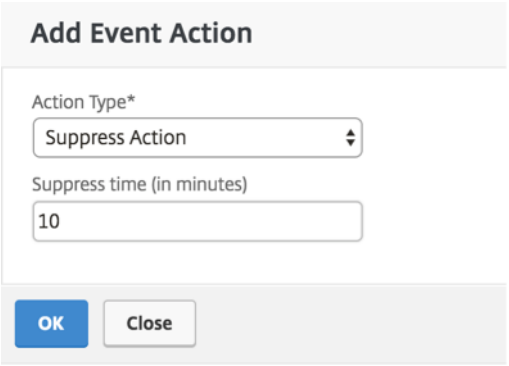
January 30, 2024

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.

> Nota:
>
> También puede configurar el tiempo de supresión como 0 minutos y significa tiempo infinito. Si no especifica ninguna duración de tiempo, NetScaler ADM considerará el tiempo de supresión como cero y nunca caduca.

Para suprimir eventos mediante NetScaler ADM:

1. En NetScaler Application Delivery Management (ADM), vaya a **Infraestructura > 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 la lista desplegable **Tipo de acción** y especifique el período de tiempo, en minutos, para el que debe suprimirse un evento.
5. Haga clic en **Aceptar**.



Crear reglas de eventos

January 30, 2024

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de un gran número de eventos generados en toda la infraestructura.

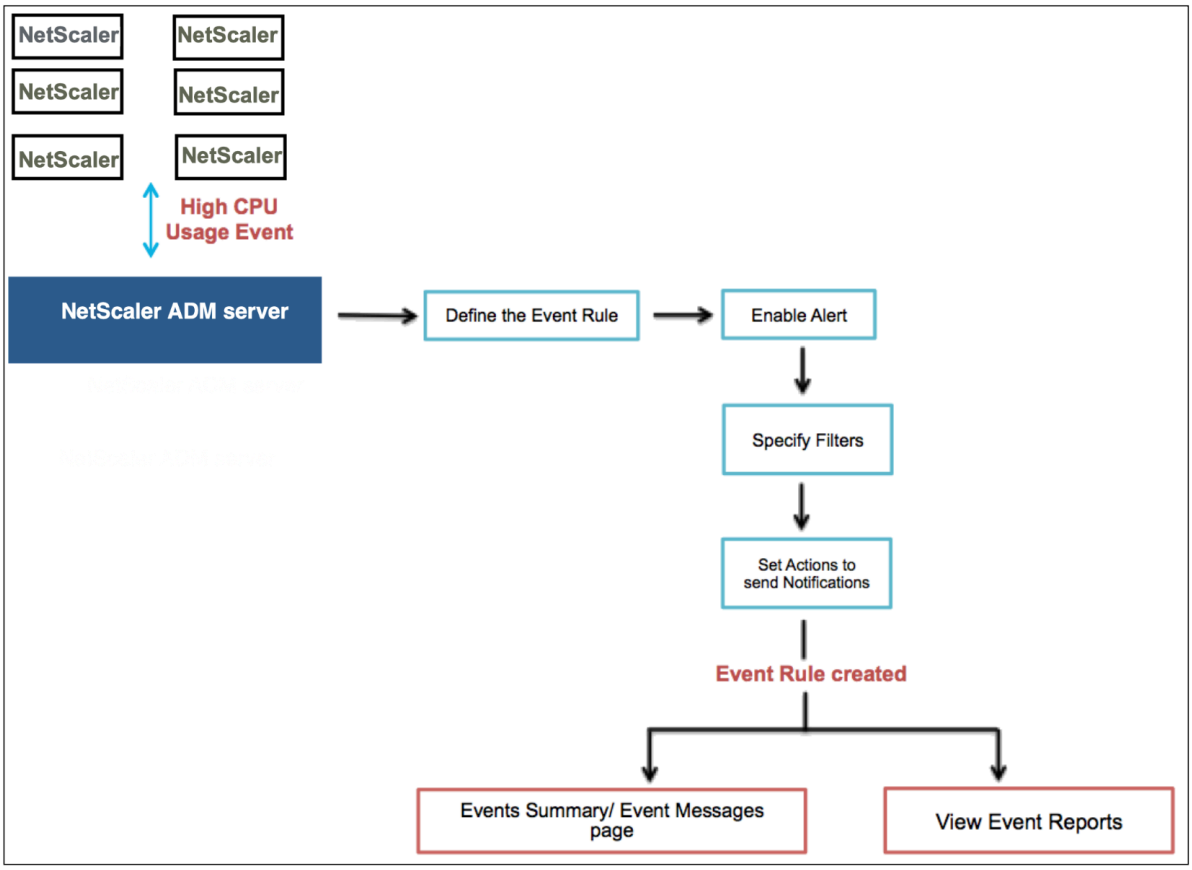
Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen los criterios de filtro de la regla, se ejecuta la acción asociada a la regla. Las condiciones para las que puede crear filtros son: gravedad, instancias de Citrix Application Delivery Controller (NetScaler), 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
- **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 especificados.
- **Suprimir acción**: Suprime la eliminación de un evento durante un período de tiempo específico.
- **Enviar notificaciones de Slack**: envía notificaciones en el canal de Slack configurado para los eventos que coincidan con los criterios del filtro.
- **Enviar notificaciones de PagerDuty**: Envíe notificaciones de eventos basadas en las configuraciones de PagerDuty para los eventos que coincidan con los criterios de filtro.
- **Enviar notificaciones de ServiceNow**: Generar automáticamente incidentes de ServiceNow para un evento que coincida con los criterios de filtro.

Para obtener más información, consulte Agregar acciones de reglas de eventos

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 una línea de asunto específica, un mensaje de usuario y un archivo adjunto.



Por ejemplo, como administrador, puede que quiera supervisar los eventos de "alto uso de CPU"para instancias específicas de NetScaler si esos eventos pueden provocar una interrupción de las instancias de NetScaler. Puede hacer lo siguiente:

- Crea una regla para supervisar las instancias y especifica una acción que te envíe una notificación por correo electrónico cuando se produzca un evento de la categoría "uso elevado de la CPU".
- Programe la regla para que se ejecute a una hora específica, por ejemplo, entre las 11:00 y las 23:00 horas, 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 a las que se aplica la regla
5. Seleccionar objetos de error
6. Especificar filtros avanzados

7. Especificar las acciones que se deben realizar cuando la regla detecta un evento

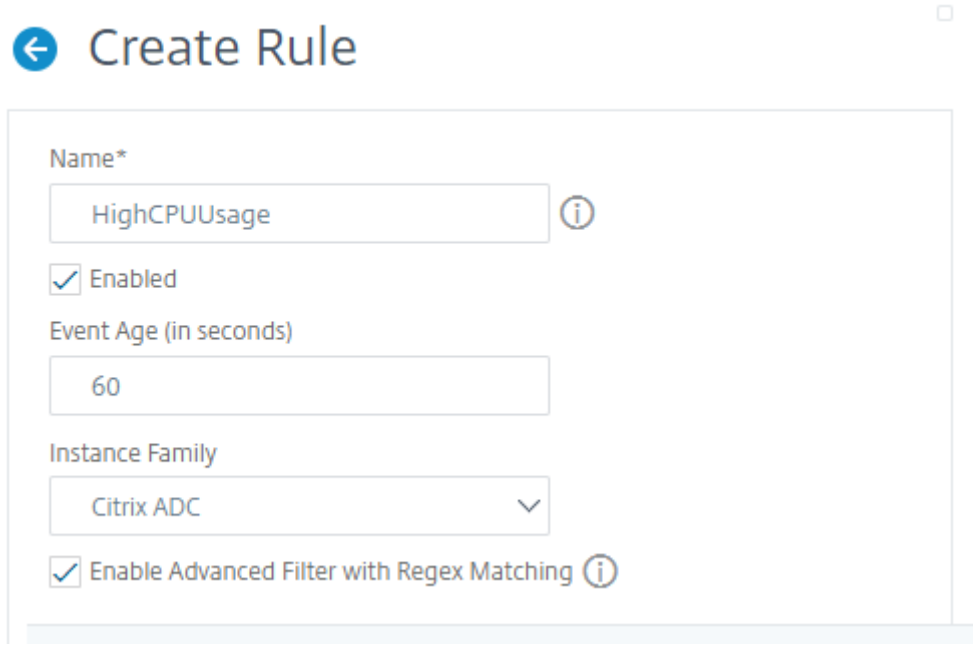
Paso 1: Definir una regla de evento

Vaya a **Infraestructura > 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 NetScaler ADM actualiza una regla de eventos.

> 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 NetScaler tenga un evento de "uso elevado de la CPU"durante 60 segundos o más. Puede establecer la antigüedad del evento en 60 segundos, de modo que cada vez que su instancia de NetScaler tenga un evento de "uso elevado de la CPU"durante 60 segundos o más, reciba una notificación por correo electrónico con los detalles del evento.



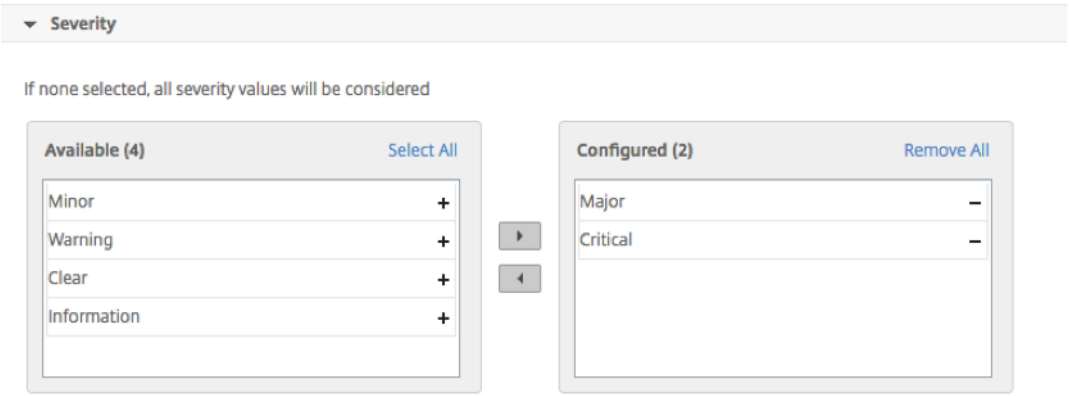
También puede filtrar las reglas de eventos por **familia de instancias** para rastrear la instancia de NetScaler desde la que NetScaler ADM recibe un evento.

Si quiere incluir una expresión regular distinta de la coincidencia de patrones de asterisco (*), seleccione **Habilitar filtro avanzado con coincidencia de expresiones regulares**.

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.

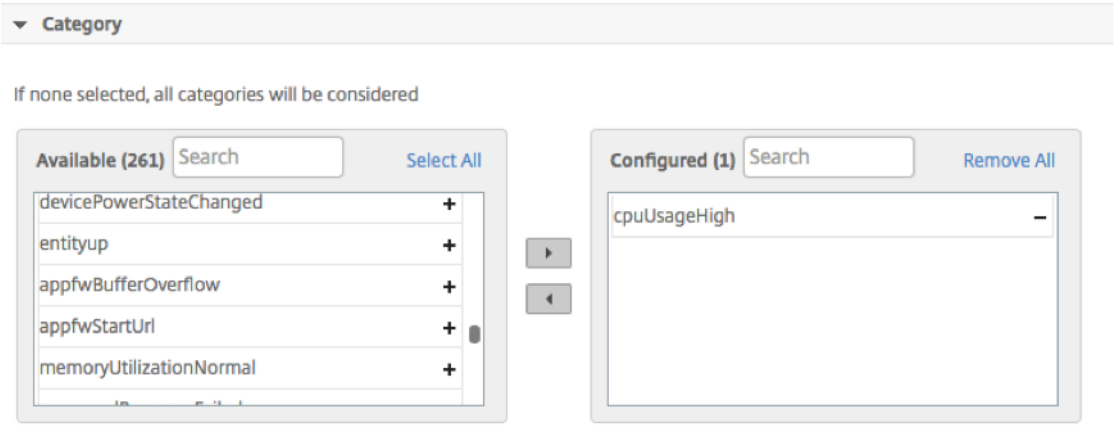


> **Nota**
>
> Puede configurar la gravedad para eventos genéricos y específicos de Advanced. Para modificar la gravedad de los eventos de las instancias de NetScaler administradas en NetScaler ADM, vaya a **Infraestructura > Eventos > Configuración de eventos**. Elija la **categoría** para la que quiere configurar la gravedad del evento y haga clic en **Configurar gravedad**. Asigne un nuevo nivel de gravedad y haga clic en **Aceptar**.

Paso 3: Especifica la categoría del evento

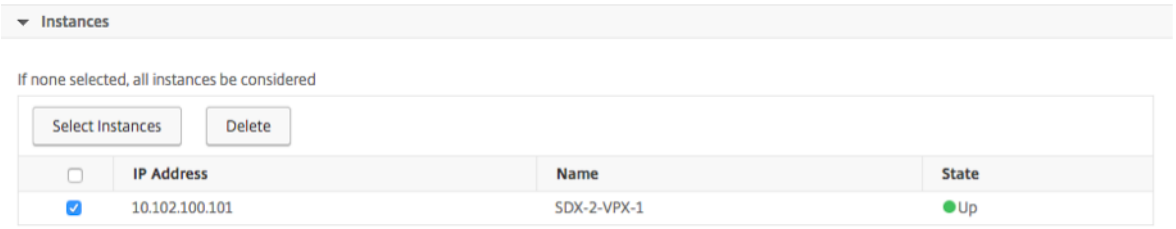
Puede especificar la categoría o las categorías de los eventos generados por las instancias NetScaler. Todas las categorías se crean en instancias de NetScaler. A continuación, estas categorías se mapean con NetScaler ADM, que se puede utilizar para definir reglas de eventos. Seleccione la categoría que quiera considerar y muévalo de la tabla **Disponible** a la tabla **Configurada**.

En el ejemplo anterior, debe elegir “cpuUsageHigh”como categoría de eventos de la tabla que se muestra.



Paso 4: Especificar instancias de NetScaler

Seleccione las direcciones IP de las instancias de NetScaler 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**.



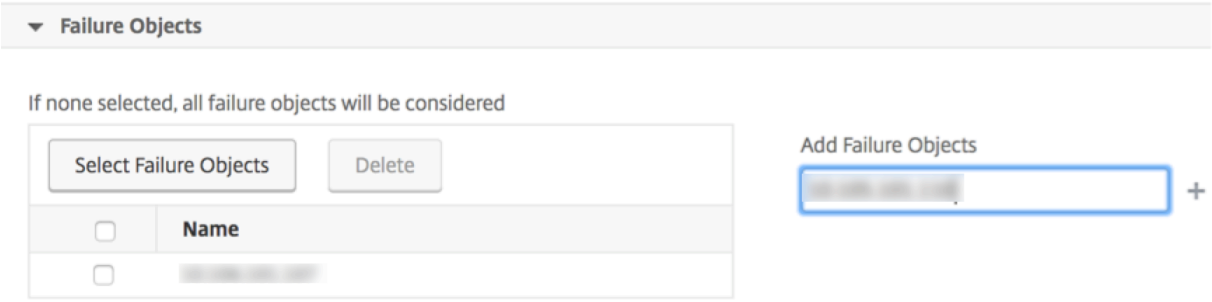
Paso 5: Seleccione objetos de error

Puede seleccionar un objeto de error de la lista proporcionada o agregar un objeto de fallo para el que se haya generado un evento. También puede especificar una expresión regular para agregar objetos de error. Según la expresión regular especificada, los objetos de error se agregan automáticamente a la lista. Los objetos de error son instancias de entidad o contadores para los que se ha generado un evento.

> **Importante**
>
> Para enumerar objetos con errores mediante expresiones regulares, seleccione **Habilitar filtro avanzado con coincidencia de expresiones** regulares en el paso 1.

El objeto de error afecta a la forma en que se procesa un evento y garantiza que refleje el problema exacto tal como se notificó. Con este filtro, puede realizar un seguimiento rápido de los problemas en los objetos de falla e identificar la causa de un problema. Por ejemplo, si un usuario tiene problemas para iniciar sesión, el objeto de error aquí es el nombre de usuario o la contraseña, por ejemplo `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.

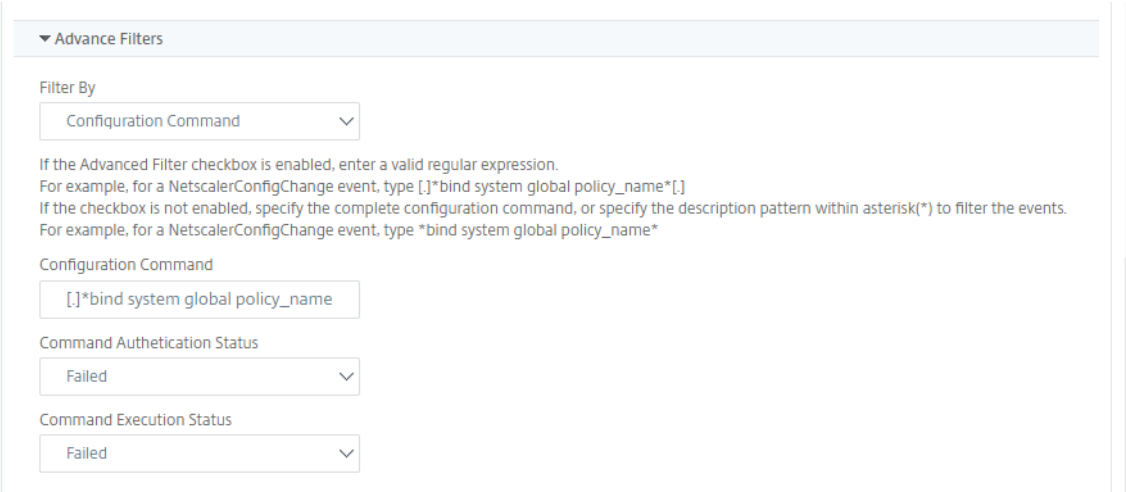


Paso 6: Especificar filtros avanzados

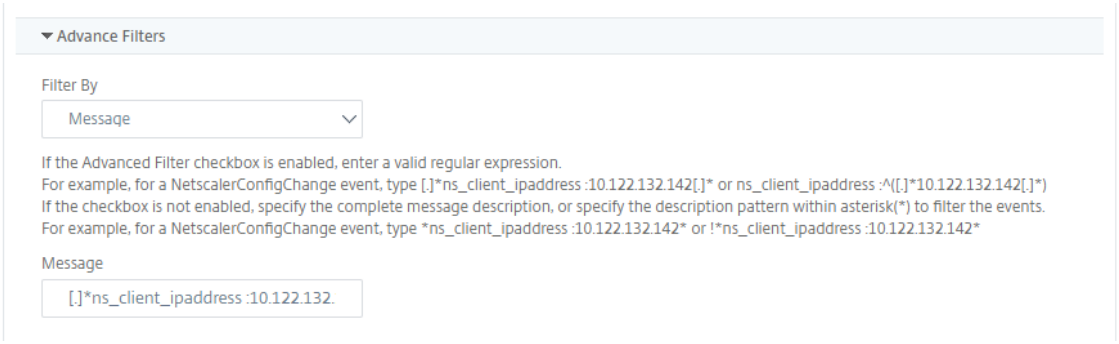
Puede filtrar aún más una regla de evento por:

- **Comandos de configuración**: puede especificar el comando de configuración completo o especificar una expresión regular para filtrar los eventos.

  Puede filtrar aún más la regla de eventos según el estado de autenticación y/o el estado de ejecución del comando. Por ejemplo, para a `NetscalerConfigChange event`, escriba `[.]*bind system global policy_name[.]*`.



- **Mensajes**: puede especificar la descripción completa del mensaje o especificar una expresión regular para filtrar los eventos.
  Por ejemplo, para un evento `NetscalerConfigChange`, escriba `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)` .



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:

- Enviar correo electrónico Action
- Acción de captura de envío
- Ejecutar acción de comando
- Ejecutar acción de trabajo
- Acción de supresión
- Enviar notificaciones de Slack
- Enviar notificaciones de PagerDuty
- Enviar notificaciones de ServiceNow

Para establecer la acción de regla de evento de correo electrónico

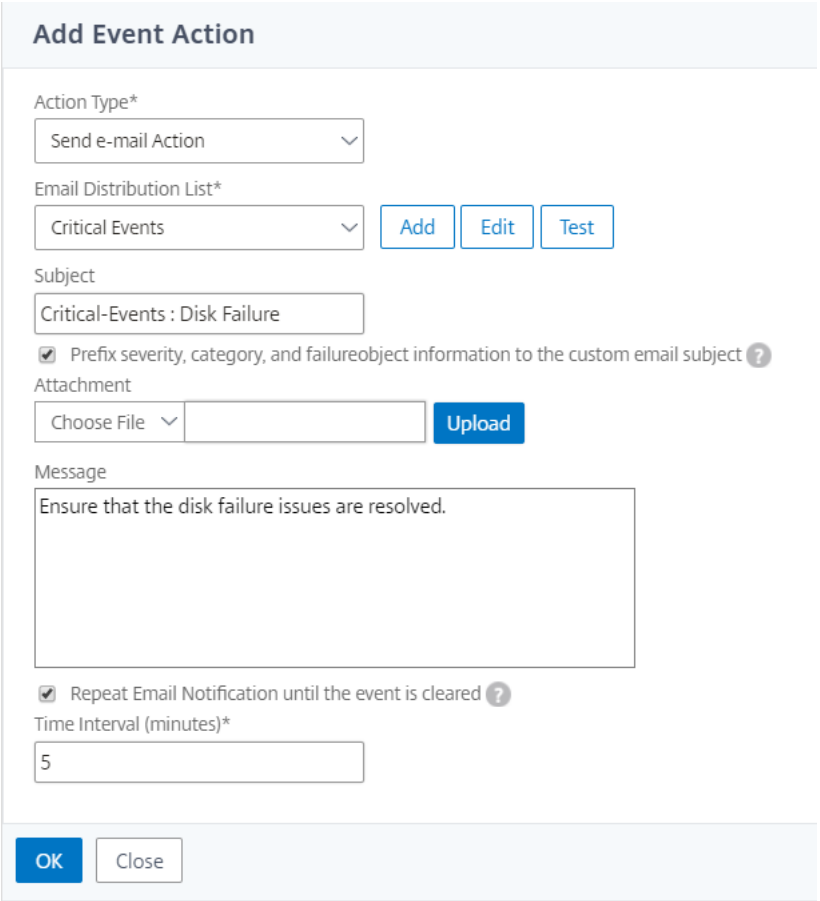
Al elegir el tipo de acción de evento Enviar correo electrónico, se activa un correo electrónico cuando los eventos cumplen con los criterios de filtro definidos. Debe crear una lista de distribución de correo electrónico proporcionando detalles del servidor de correo o del perfil de correo o puede seleccionar una lista de distribución de correo electrónico que haya creado anteriormente.

Debido a la gran cantidad de servidores virtuales que se configuran en NetScaler ADM, es posible que reciba un gran número de correos electrónicos cada día. Los correos electrónicos tienen una línea de asunto predeterminada que proporciona información sobre la gravedad del evento, la categoría del evento y el objeto de error. Sin embargo, la línea de asunto no contiene información sobre el nombre del servidor virtual en el que se originan estos eventos. Ahora tiene la opción de incluir información adicional, como el nombre de la entidad afectada o el nombre del objeto de error.

También puede agregar una línea de asunto personalizada y un mensaje de usuario, y cargar un archivo adjunto a su correo electrónico cuando un evento entrante coincida con la regla configurada.

Al enviar correos electrónicos para notificaciones de eventos, es posible que quiera enviar un correo electrónico de prueba para probar los ajustes configurados. El botón "Probar"ahora le permite enviar un correo electrónico de prueba después de configurar un servidor de correo electrónico, las listas distribuidas asociadas y otros ajustes. Esta función garantiza que la configuración funcione bien.

También puede asegurarte de que se aborden todos los eventos críticos y no se omita ninguna notificación importante por correo electrónico. Para ello, selecciona la casilla **Repetir notificación por correo electrónico hasta que se desactive el evento** para enviar notificaciones repetidas por correo electrónico sobre 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.



Para establecer la acción de regla de evento de reventado

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 el destino de las trampas y los detalles del perfil de las trampas), los mensajes de captura se envían a detectores de trampas específicos cuando los eventos cumplen con los criterios de filtro definidos.

Para establecer la acción Ejecutar comando

Al elegir la acción del evento **Ejecutar acción de comando**, puede crear un comando o un script que se pueda ejecutar en NetScaler ADM para eventos que coincidan con un criterio de filtro determinado.

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 refleje el problema exacto tal como se notificó. 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 reemplazan con valores reales.

Por ejemplo, considere que quiere establecer una acción de comando de ejecución cuando el estado de un servidor virtual de equilibrio de carga es **Inactivo**. Como administrador, puede considerar la posibilidad de ofrecer una solución rápida agregando otro servidor virtual. En NetScaler ADM, puede:

- Escriba un archivo de script (.sh).

  A continuación se muestra un archivo de script (.sh) de ejemplo:

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- Guarde el archivo .sh en cualquier ubicación persistente del agente NetScaler ADM. Por ejemplo: `/var`.
- Proporcione la ubicación del archivo.sh en NetScaler ADM que se ejecutará cuando se cumplan los criterios de regla.

Para configurar la acción **Ejecutar comando** para crear un nuevo servidor virtual:

1. Defina la regla
2. Seleccione la gravedad del evento
3. Selecciona la categoría de eventos **entitydown**
4. Seleccione la instancia que tiene configurado el servidor virtual
5. Seleccione o cree un objeto de error para el servidor virtual
6. En **Acciones de reglas de eventos**, haga clic en **Agregar acción** y seleccione **Ejecutar acción de comando** en la lista de **tipos de acciones**.

7. En **Lista de ejecución de comandos**, haga clic en **Agregar**.

   Aparece la página Crear lista de distribución de comandos.

   a) En **Nombre del perfil**, especifique un nombre de su elección

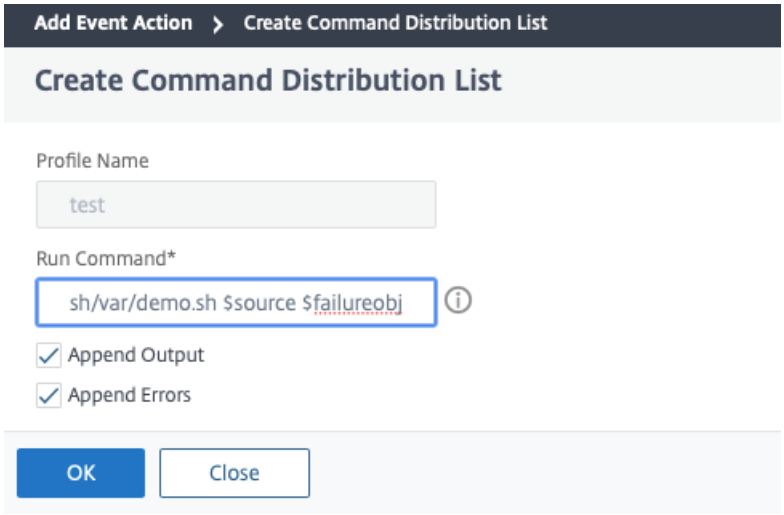
   b) En **Ejecutar comando**, especifique la ubicación del agente de NetScaler ADM, donde debe ejecutarse el script. Por ejemplo: `/sh/var/demo.sh $source $failureobj`.

   c) Seleccione **Anexar salida** y **Anexar errores**

   > **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 descarta todas las salidas y errores generados al ejecutar el script.

   d) Haga clic en **Crear**.

8. En la página **Agregar acción de evento**, haga clic en **Aceptar**.



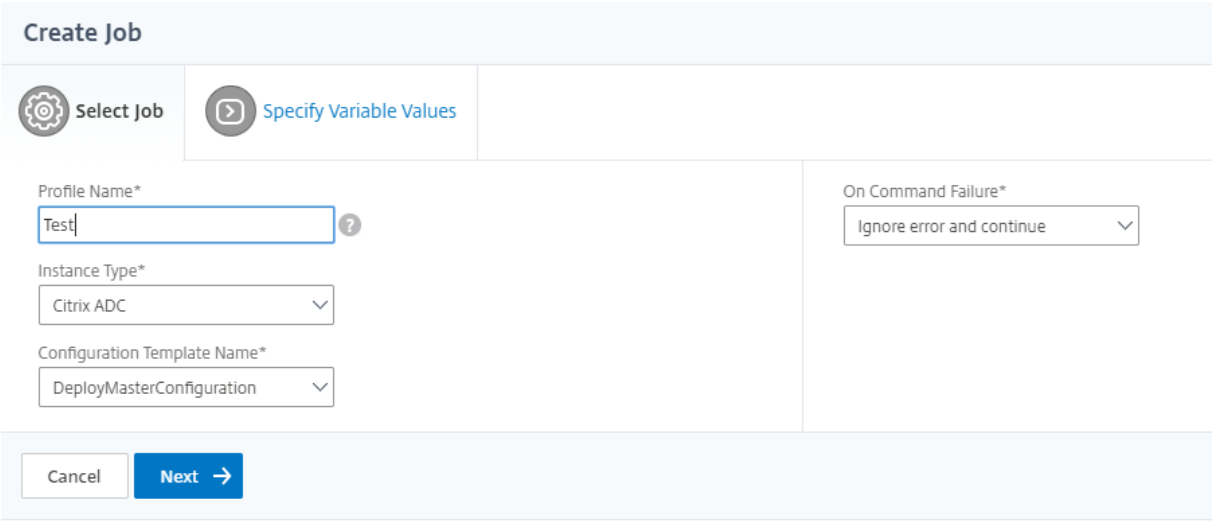
> **Nota**
>
> Puede habilitar las opciones **Anexar salida** y **Anexar errores** si quiere almacenar la salida y los errores generados (si los hay) al ejecutar un script en los archivos de registros del servidor NetScaler ADM. Si no habilita estas opciones, NetScaler ADM descarta todas las salidas y errores generados al ejecutar el script.

Para establecer la acción de trabajo `Execute`

Al crear un perfil con trabajos de configuración, un trabajo se ejecuta como un trabajo integrado o un trabajo personalizado para las instancias de NetScaler y NetScaler SDX, para eventos y alarmas que

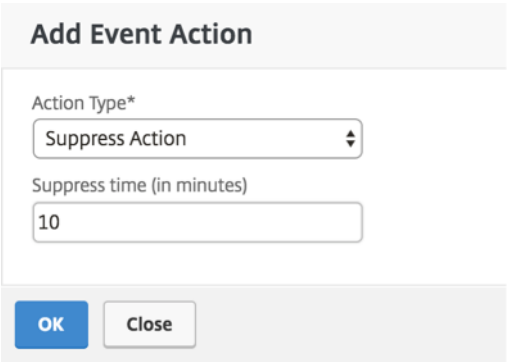
coincidan con los criterios de filtro que ha especificado.

1. En **Acciones de regla de evento**, haga clic en **Agregar acción** y seleccione **Ejecutar acción de trabajo** en la lista desplegable **Tipo de acción**.
2. Cree un perfil con un trabajo que quiera 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 establecer 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.



Para configurar notificaciones de Slack desde NetScaler ADM

Configure el canal de Slack requerido proporcionando el nombre del perfil y la URL de webhook en la GUI de NetScaler ADM. Las notificaciones de eventos se envían a este canal. Puede configurar varios canales de Slack para recibir estas notificaciones

1. En NetScaler ADM, vaya a**Infraestructura > Eventos > Reglas**y haga clic en**Agregar**para crear una regla.
2. En la página **Crear regla**, defina los parámetros de la regla, como la gravedad y la categoría. Seleccione las instancias y también los objetos de error que se deben monitorear.
3. En**Acciones de reglas de eventos**, haga clic en**Agregar acción**. A continuación, selecciona**Enviar notificaciones de Slack**en la lista de**tipos de acción** y selecciona Lista de **perfiles de Slack**.
4. También puede agregar una lista de perfiles de Slack haciendo clic en **Agregar** junto al campo **Lista de perfiles de Slack**.
5. Escriba los siguientes parámetros para crear una lista de perfiles:
    a) **Nombre del perfil**. Escriba un nombre para la lista de perfiles que se configurará en NetScaler ADM
    b) **Nombre del canal**. Escribe el nombre del canal de Slack al que se van a enviar las notificaciones de eventos.
    c) **URL del webhook**. Escribe la URL del Webhook del canal que has introducido anteriormente. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal y todas las notificaciones de eventos se envían a esta URL para que se publiquen en el canal de Slack designado. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Haga clic en **Crear** y haga clic en **Aceptar** en la ventana **Agregar acción de evento**.

> **Nota:**
>
> También puede agregar los perfiles de Slack desde **Sistema** > **Notificaciones** > **Perfiles de Slack**. Haga clic en **Agregar** y cree el perfil como se describe en la sección anterior.

Puede ver el estado de los perfiles de Slack que ha creado.

La regla de evento se crea ahora con filtros apropiados y acciones de regla de evento bien definidas.

Para establecer notificaciones de PagerDuty desde NetScaler ADM

Puede agregar un perfil de PagerDuty como opción en NetScaler ADM para supervisar las notificaciones de incidentes en función de las configuraciones de PagerDuty. PagerDuty le permite configurar notificaciones por correo electrónico, SMS, notificaciones push y llamadas telefónicas a un número registrado.

Antes de agregar un perfil de PagerDuty en NetScaler ADM, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para obtener más información, consulte la documentación de PagerDuty.

Puede seleccionar su perfil de PagerDuty como una de las opciones para recibir notificaciones de las siguientes funciones:

- **Eventos**: lista de eventos que se generan para las instancias de NetScaler.
- **Licencias**: lista de licencias que están actualmente activas, a punto de caducar, etc.
- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias NetScaler.

Para agregar un perfil de PagerDuty en ADM:

1. Inicie sesión en NetScaler ADM mediante credenciales de administrador.
2. Vaya a **Configuración > Notificaciones > Perfiles de PagerDuty**.
3. Haga clic en **Agregar** para crear un nuevo perfil.
4. En la página Crear Perfil de PagerDuty:
   a) Proporcione un nombre de perfil de su elección.
   b) Introduzca la **clave de integración**.
      Puede obtener la clave de integración en su portal de PagerDuty.
   c) Haga clic en **Crear**.

   Caso de uso:

   Considere un caso que:

   - quiere enviar notificaciones a su perfil de PagerDuty.
   - han configurado la llamada telefónica como una opción en PagerDuty para recibir notificaciones.
   - quiere recibir alertas de llamadas telefónicas para eventos de NetScaler.

   Para llevar a cabo la configuración:

   a) Diríjase a **Eventos** > **Reglas**

b) En la página **Crear regla**, configure todos los demás parámetros para crear una regla.

c) En **Crear acciones de regla**, haga clic en **Agregar acción**.

Aparece la página **Agregar acción de evento**.

i. En **Tipo de acción**, seleccione **Enviar notificaciones de PagerDuty**.

ii. Seleccione su perfil de PagerDuty y haga clic en **Aceptar**.

Una vez completada la configuración, cada vez que se genere un nuevo evento para la instancia de NetScaler, recibirá una llamada telefónica. Desde la llamada telefónica, puede decidir:

- Reconoce el evento
- Marcarlo como resuelto
- Escalar a otro miembro del equipo

Para generar automáticamente incidentes de ServiceNow desde NetScaler ADM

Puede generar automáticamente incidentes de ServiceNow para eventos de NetScaler ADM seleccionando el perfil de ServiceNow en la GUI de NetScaler ADM. Debe elegir el perfil ServiceNow en NetScaler ADM para configurar una regla de eventos.

Antes de configurar una regla de evento para generar automáticamente incidentes de ServiceNow, integre NetScaler ADM con una instancia de ServiceNow. Para obtener más información, consulte Configurar el adaptador ITSM para ServiceNow.

Para configurar una regla de evento, vaya a **Eventos** > **Reglas**.

1. En la página **Crear regla**, configure todos los demás parámetros para crear una regla.
2. En **Crear acciones de regla**, haga clic en **Agregar acción**.

   Aparece la página **Agregar acción de evento**.

   a) En **Tipo de acción**, seleccione **Enviar notificaciones de ServiceNow**.

   b) En el **perfil de ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.

   c) Haga clic en **Aceptar**.

Modificar la gravedad reportada de los eventos que se producen en instancias de NetScaler

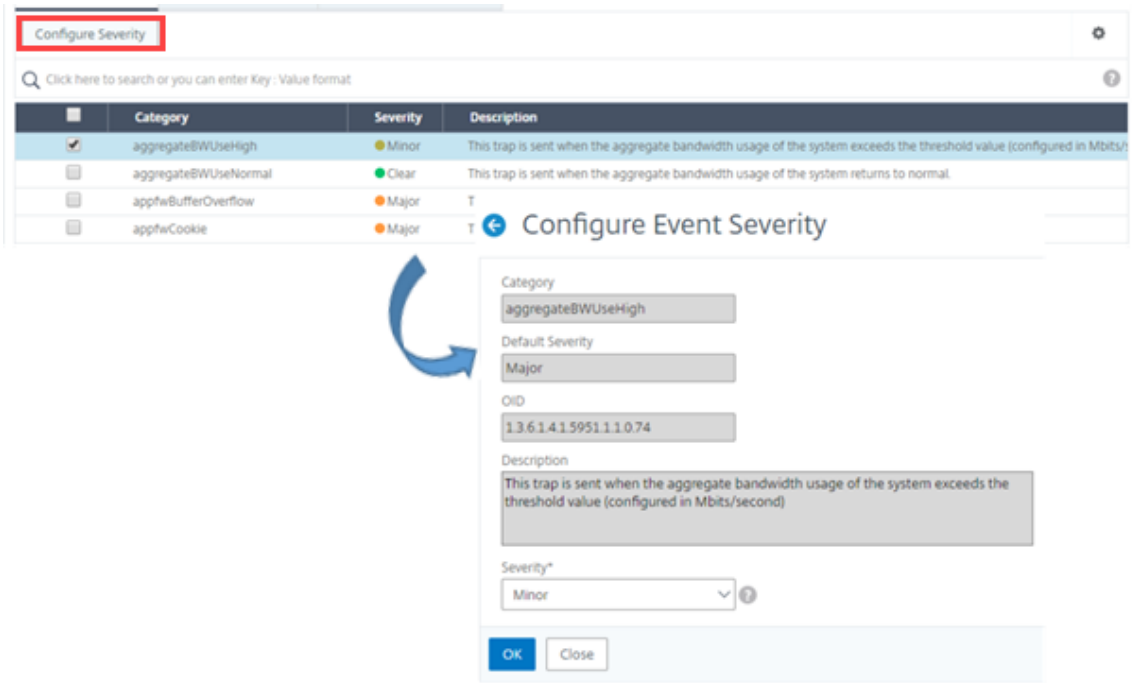
January 30, 2024

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 **Infraestructura > 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**.

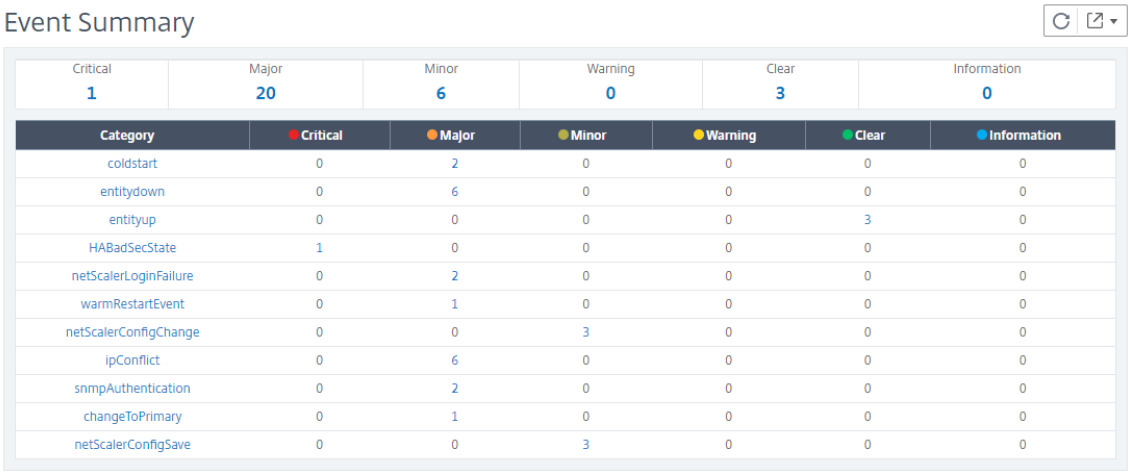


Ver resumen de eventos

January 30, 2024

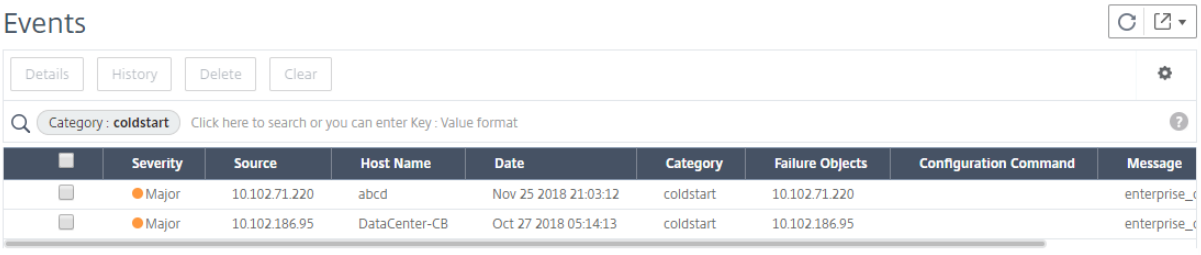
Ahora puede ver una página Resumen de eventos para supervisar los eventos y las capturas recibidas en el servidor NetScaler Application Delivery Management (ADM). Vaya a **Infraestructura > Eventos**. La página Resumen de Eventos muestra la siguiente información en formato de tabla:

- **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 ha estado 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 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 una captura, se le lleva a la página **Eventos**, en la que se preseleccionan filtros como Categoría y Gravedad. Esta página muestra más información sobre el evento, como la dirección IP y el nombre del host de la instancia de NetScaler, 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 NetScaler Application Delivery Management (ADM), puede ver el evento inmediatamente en la página de 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 NetScaler ADM con todo detalle en el panel de infraestructura.

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 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, se le dirigirá a la página **Eventos basados en gravedad**, donde puede ver todos los detalles sobre cuándo se produjo un evento crítico durante el tiempo que ha seleccionado: el origen de la instancia, la fecha, la categoría y la notificación de mensaje enviada cuando se produjo el evento crítico.

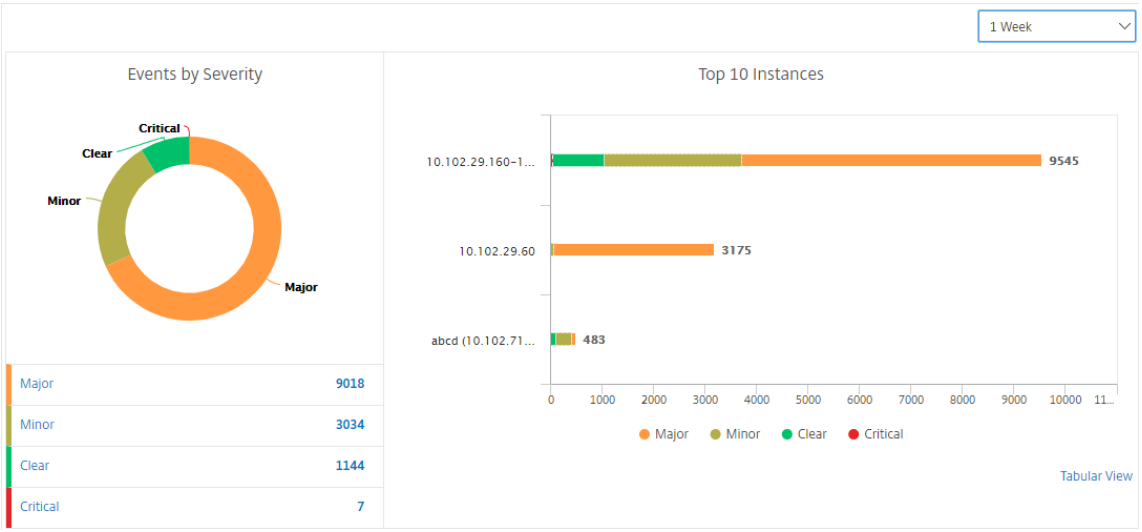
Del mismo modo, puede ver el estado de una instancia de NetScaler VPX en el panel de control. Puede enmascarar el tiempo durante el cual la instancia estaba en funcionamiento y en ejecución, y mostrar solo las veces que la instancia estuvo fuera de servicio. Al hacer clic en el gráfico, se le lleva a 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 ver el panel de control de la instancia de Citrix en particular para obtener más detalles.

Para seleccionar eventos específicos por gravedad en NetScaler ADM:

1. Inicie sesión en NetScaler ADM con sus credenciales de administrador.
2. Vaya a **Infraestructura > Panel de control**.

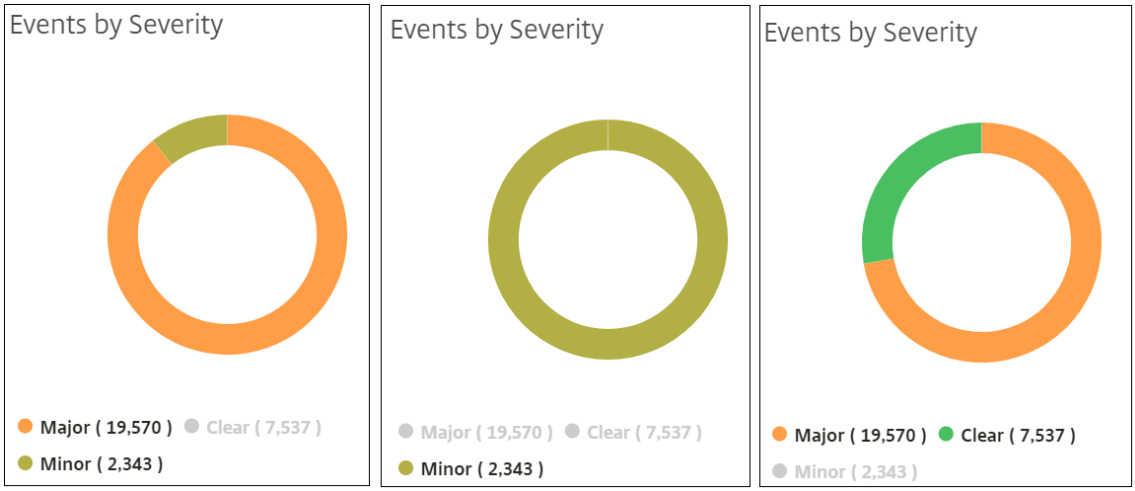
   O bien:

   Vaya a **Infraestructura > 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 donut para mostrar la página de **eventos basados en gravedad** correspondiente, que muestra los siguientes detalles de la gravedad seleccionada para la duración seleccionada:
    - Origen de instancia
    - Datos del evento
    - Categoría de eventos generados por la instancia de NetScaler
    - 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 en NetScaler ADM:

Ahora puede ver los detalles de cada captura SNMP recibida de sus instancias de NetScaler administradas en el servidor NetScaler ADM en la página **Configuración de eventos**. Vaya a **Infraestructura > 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".

Ver y exportar mensajes syslog de NetScaler

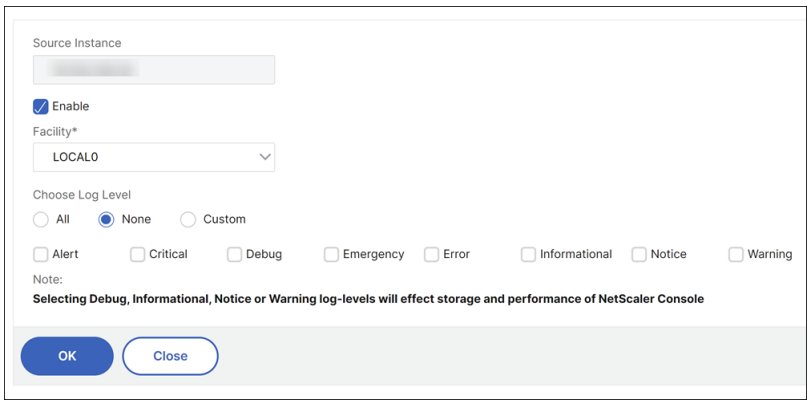
January 30, 2024

Desde el software ADM, puede supervisar los eventos syslog generados en las instancias de Citrix Application Delivery Controller (ADC). Para ello, debe configurar ADM como servidor syslog para las instancias de NetScaler. Después de configurar ADM, todos los mensajes syslog se redirigen de las instancias de ADC a ADM.

Configurar ADM como servidor syslog

Siga estos pasos para configurar ADM como el servidor syslog:

1. En la GUI de ADM, vaya a **Infraestructura > Instancias**.
2. Seleccione la instancia de NetScaler desde la que quiere que se recopilen y muestren los mensajes syslog en NetScaler ADM.
3. En la lista **Seleccionar acción**, seleccione **Configurar Syslog**.
4. Haga clic en **Activar**.
5. En la lista desplegable de **instalaciones**, seleccione una instalación local o a nivel de usuario.
6. Seleccione el nivel de registro requerido para los mensajes de syslog.
7. Haga clic en **Aceptar**.

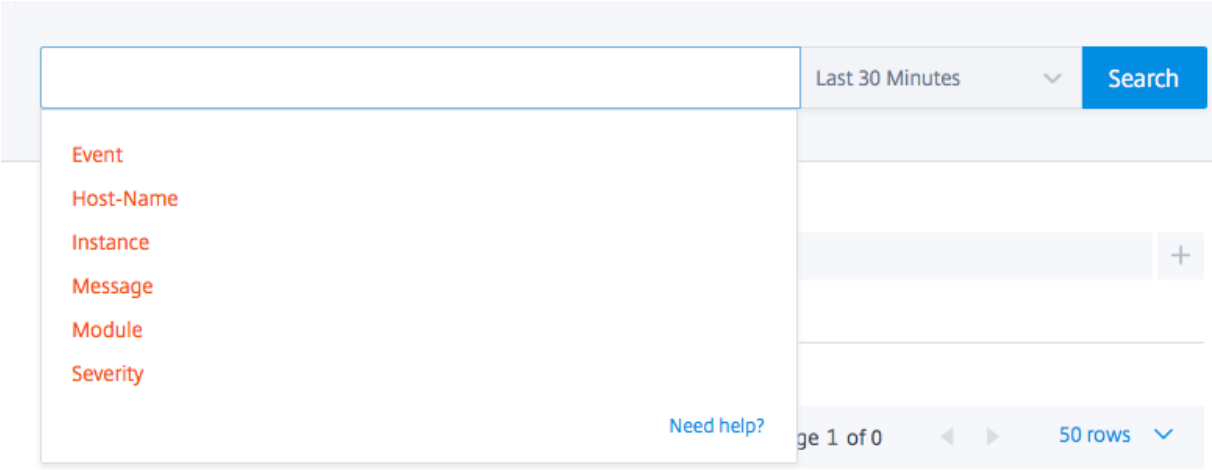


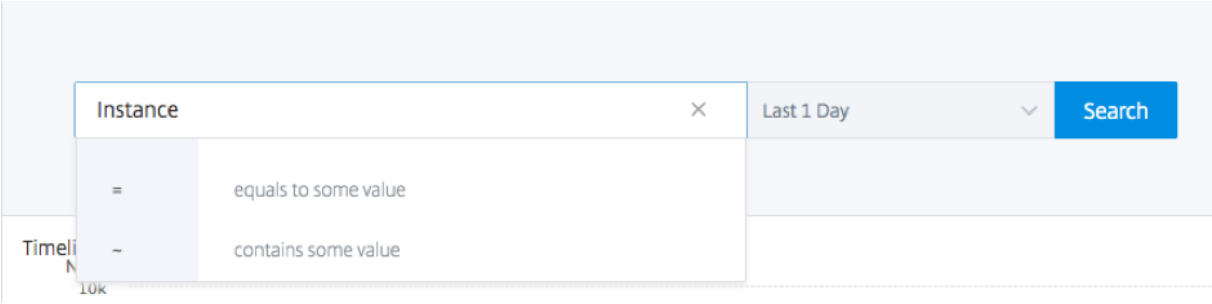
Estos pasos configuran todos los comandos syslog en la instancia de NetScaler y NetScaler ADM comienza a recibir los mensajes syslog.

Ver y buscar mensajes de syslog

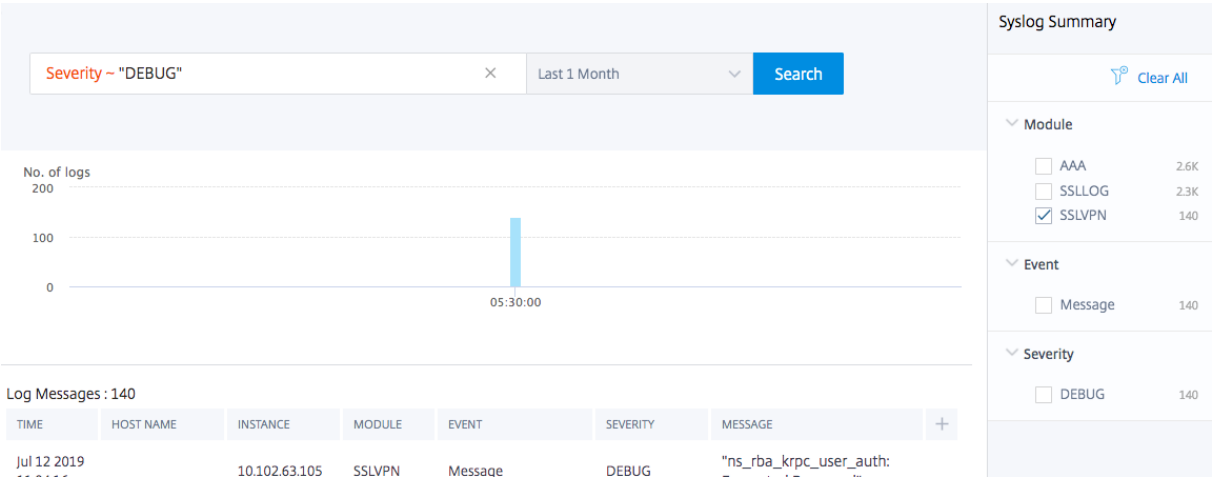
Puede ver todos los mensajes de syslog generados en las instancias administradas de NetScaler. Los mensajes de syslog se almacenan en la base de datos de forma centralizada y están disponibles en **Infraestructura > Eventos > Mensajes de syslog** para fines de auditoría. Puede combinar esta información de registro y derivar informes para análisis a partir de los datos recopilados.

Además, puede usar filtros para reducir los resultados de búsqueda de mensajes syslog y encontrar exactamente lo que está buscando y en tiempo real. Haga clic en **¿Necesita ayuda?** para abrir la ayuda de búsqueda integrada.





A continuación, agregue el término de búsqueda. Para algunas categorías, se muestra una lista precompletada de términos de búsqueda. De forma predeterminada, el tiempo de búsqueda es de 1 día. Puede cambiar la hora y el intervalo de fechas haciendo clic en la flecha hacia abajo. Puede restringir aún más la búsqueda seleccionando opciones en el panel **Resumen de Syslog**.

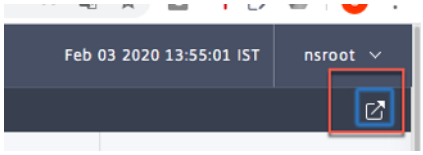


Exportar y programar mensajes syslog

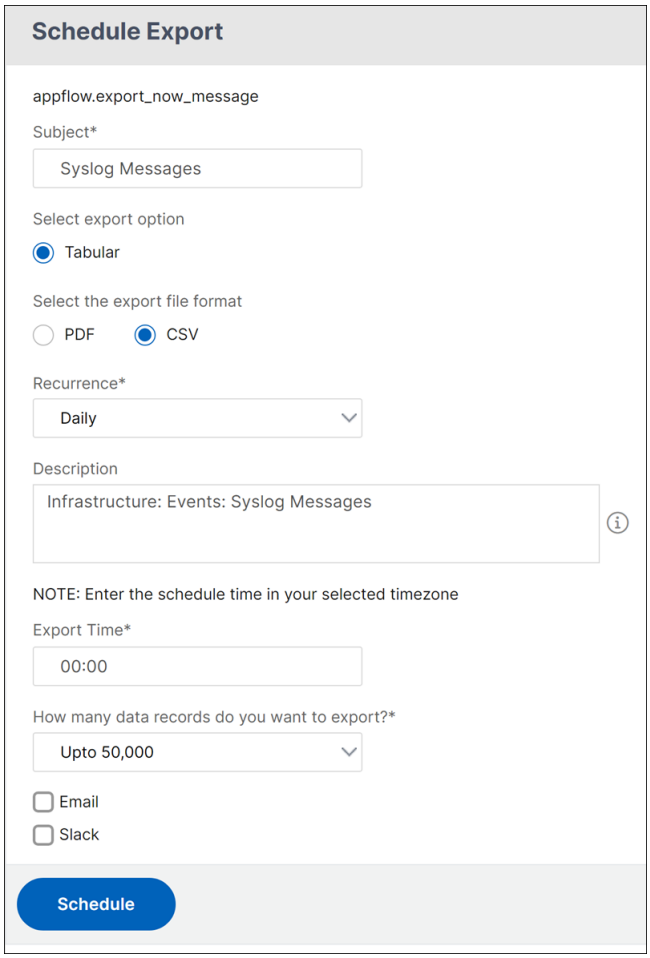
Puede ver los mensajes syslog sin iniciar sesión en ADM, programando una exportación de todos los mensajes syslog recibidos en el servidor. Puede exportar mensajes syslog generados en las instan-

cias de ADC en formatos PDF, CSV, PNG y JPEG. Puede programar la exportación de estos informes a direcciones de correo electrónico o cuenta de Slack especificadas a intervalos diferentes.

Para exportar y programar los mensajes de registro, haga clic en el icono de flecha situado en la esquina superior derecha.



- Para exportar los mensajes de registro, haga clic en **Exportar informes > Exportar ahora**, seleccione el formato requerido y, a continuación, haga clic en **Exportar**.
- Para programar la exportación de mensajes syslog, haga clic en **Exportar informes > Programar informe**y defina los parámetros necesarios. Puede recibir el informe por correo electrónico o Slack.



Suprimir mensajes de syslog

January 30, 2024

Cuando se configura como servidor syslog, NetScaler Application Delivery Management (ADM) recibe todos los mensajes de 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. NetScaler ADM elimina todos los mensajes que coincidan 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 o de varias instancias. También puede proporcionar un patrón de texto para que NetScaler ADM busque y suprima mensajes. NetScaler ADM elimina todos los mensajes que coincidan 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)

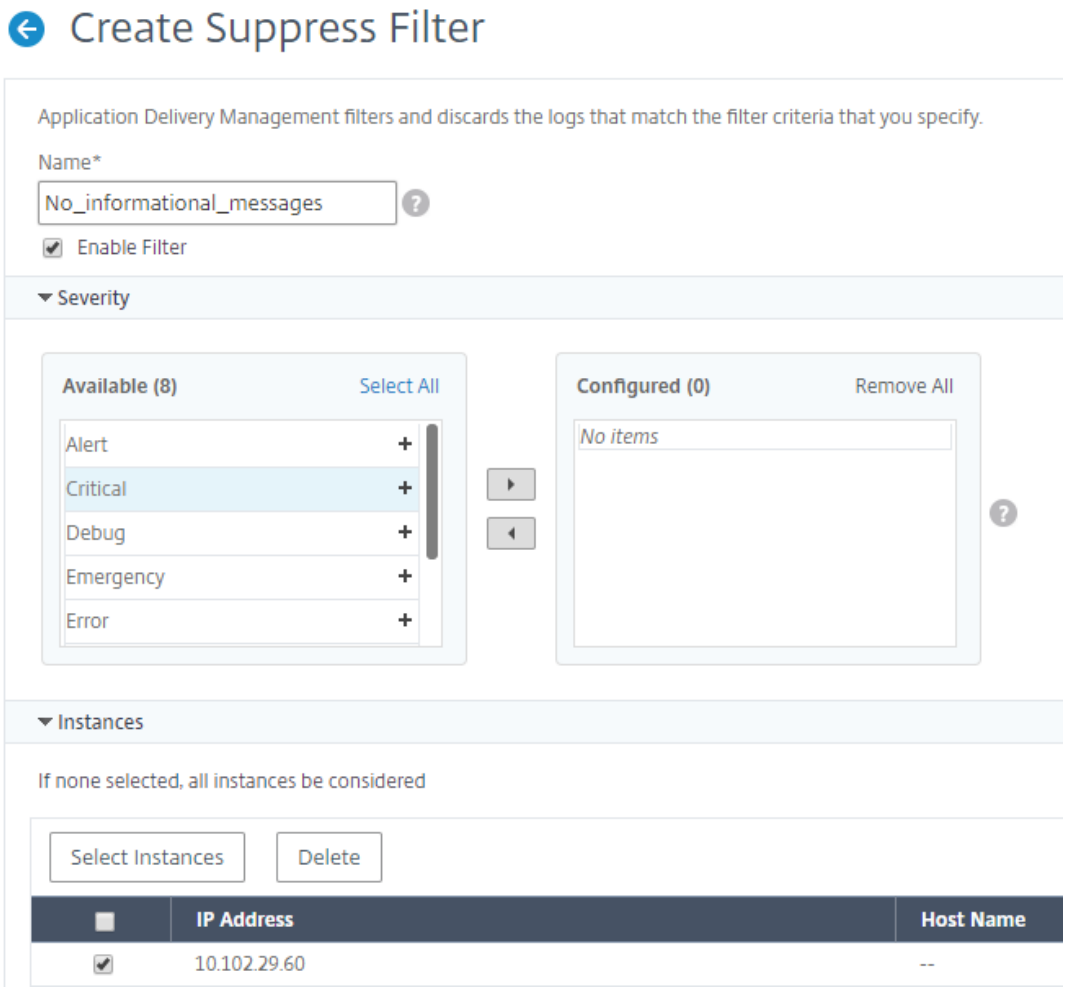
Supresión de mensajes de syslog mediante la creación de filtros

1. En NetScaler ADM, vaya a **Infraestructura > Eventos > Mensajes de Syslog** > **Suprimir filtro**.
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, 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.

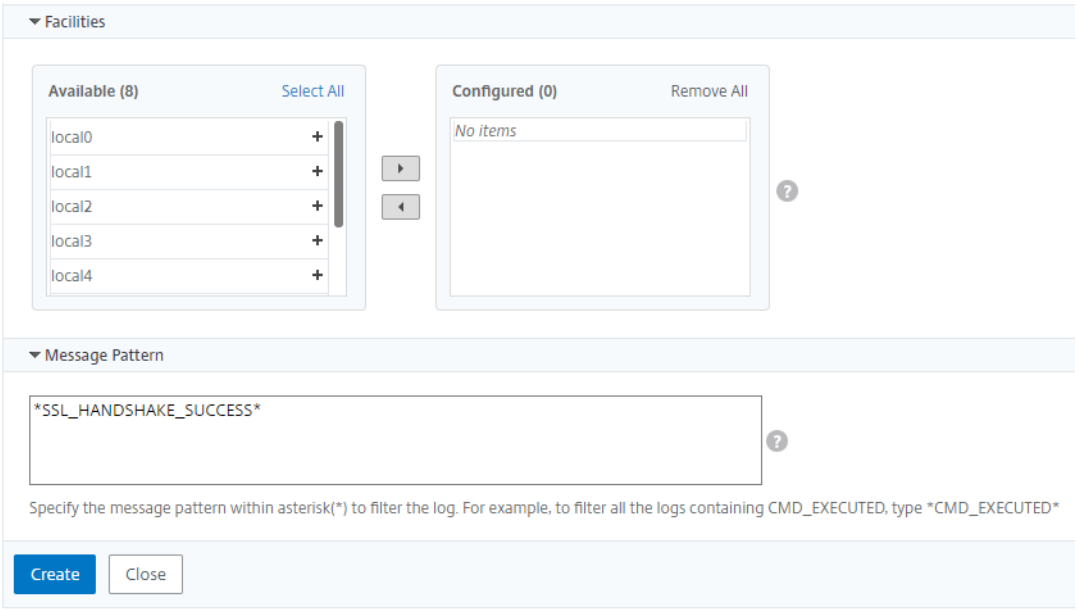
b) **Gravedad**: Seleccione y agregue los niveles de registro para los que debe suprimir los mensajes. Por ejemplo, si no quiere ver ningún mensaje informativo que llegue, puede seleccionar Informativo para suprimirlos.

c) **Instancias**: Seleccione las instancias NetScaler 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 **Infraestructura > Eventos > Mensajes de Syslog** > **Suprimir filtro**y, en la página **Suprimir filtro**, seleccione el filtro y haga clic en **Modificar**.
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

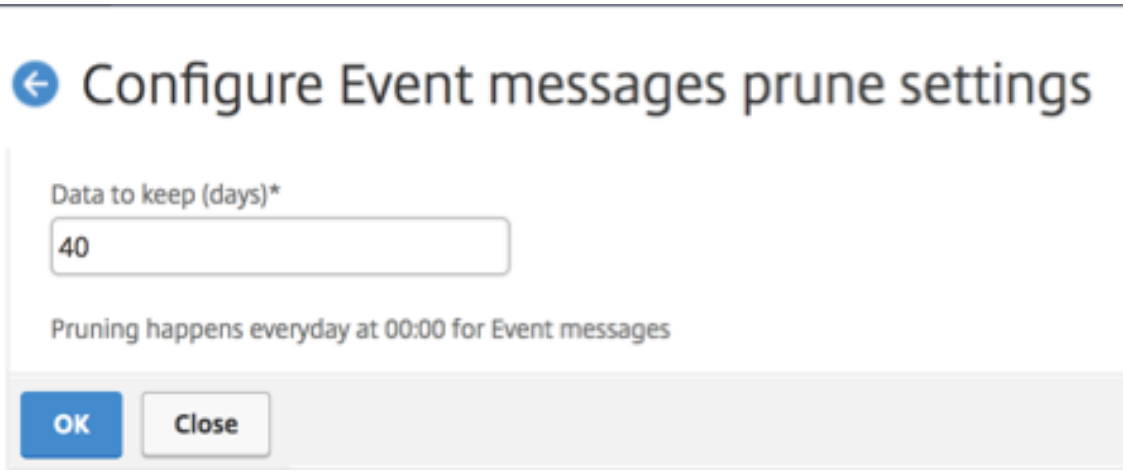
January 30, 2024

Las instancias de Citrix Application Delivery Controller (ADC) administradas por su servidor NetScaler Application Delivery Management (ADM) envían datos de mensajes de eventos de forma continua para almacenarlos en NetScaler 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, durante el que desea conservar los datos en el servidor NetScaler ADM y haga clic en Aceptar.**



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

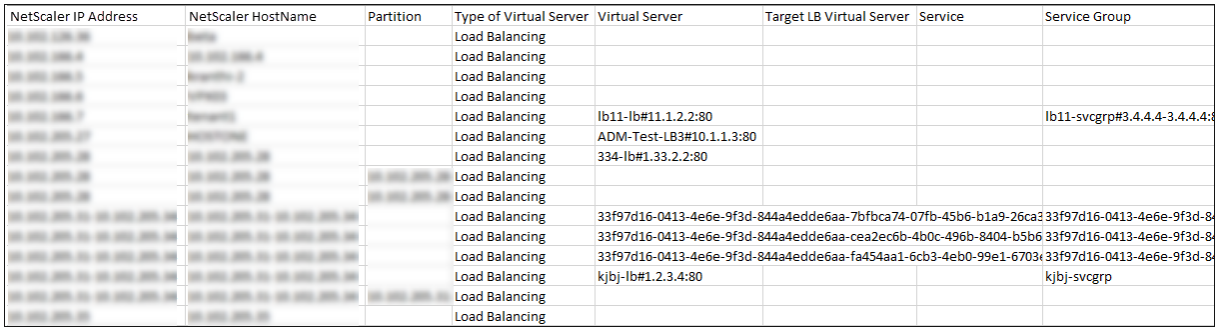
January 30, 2024

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 NetScaler 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 NetScaler.

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 NetScaler que están presentes en la red.

La siguiente imagen muestra un ejemplo de un informe resumido.



NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		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 NetScaler 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 NetScaler.

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.

NetScaler 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 NetScaler ADM, vaya a **Infraestructura > Funciones de red > Equilibrio de carga.**
2. En la página **Equilibrio de carga**, 
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 NetScaler ADM, vaya a **Infraestructura > 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 NetScaler 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 el equilibrio de carga, la conmutación de contenido, la redirección de caché, el equilibrio de carga global del servidor (GSLB), la autenticación y NetScaler Gateway en NetScaler Application Delivery Management (ADM). Este informe le permite tener una vista de alto nivel de la asignación entre las instancias de NetScaler, las particiones y las entidades enlazadas correspondientes (servidores virtuales, grupos de servicios y servicios) 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.

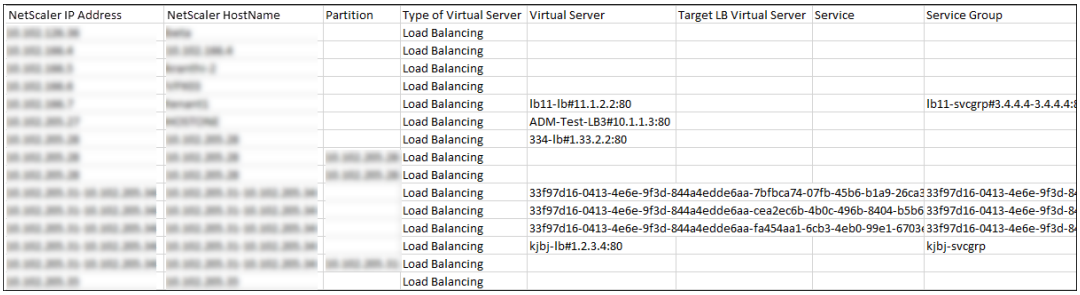
> **Nota**
>
> - Para los servidores virtuales GSLB, el informe de funciones de red muestra solo los servidores virtuales GSLB y los servicios asociados.
> - Para los servidores virtuales de conmutación de contenido y redirección de caché, el informe muestra solo los enlaces a los servidores LB asociados.
> - Los servidores virtuales SSL no aparecen en este informe porque NetScaler 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 **Infraestructura > 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 IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

   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 **Habilitar programación**, puede generar los informes seleccionados.

Informes de red

January 30, 2024

Puede optimizar el uso de los recursos supervisando los informes de su red en NetScaler Application Delivery Management (NetScaler ADM). Es posible que tenga una implementación distribuida con muchas aplicaciones implementadas en varias ubicaciones. Para garantizar un rendimiento óptimo de sus aplicaciones, también ha implementado varias instancias de Citrix Application Delivery Controller (NetScaler) para equilibrar la carga, cambiar el contenido o comprimir el tráfico. El rendimiento

de la red puede afectar al rendimiento de la aplicación. Para continuar manteniendo el rendimiento de sus aplicaciones, debe supervisar regularmente el rendimiento de la red y asegurarse de que todos los recursos se utilizan de manera óptima.

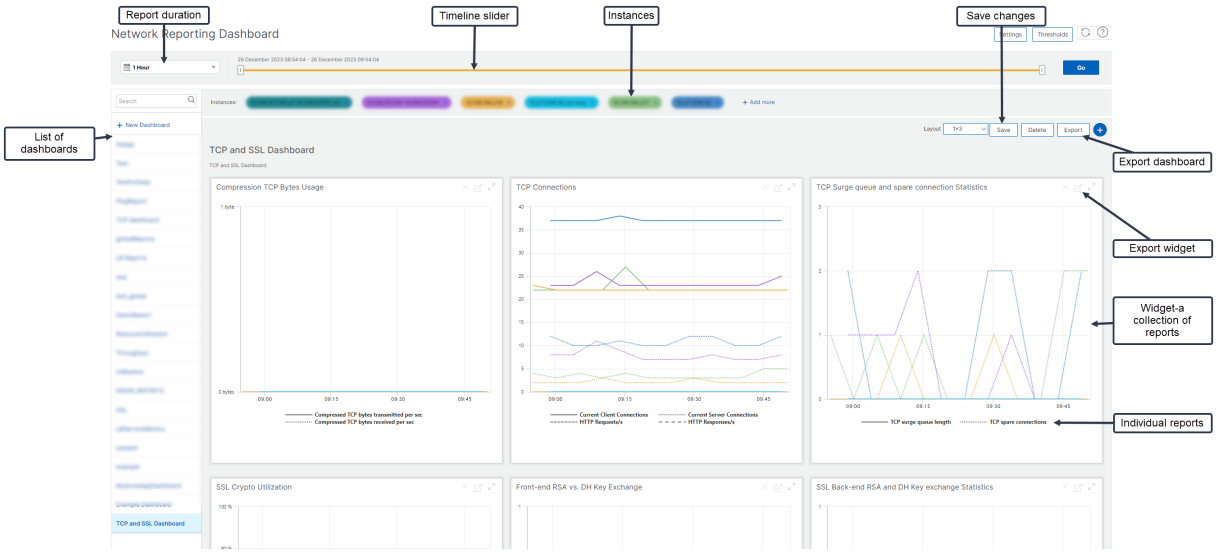
NetScaler ADM ahora le permite generar informes no solo para instancias a nivel global, sino también para entidades como los servidores virtuales y las interfaces de red. La familia de instancias incluye instancias de NetScaler. Los servidores virtuales para los que puede generar informes son los siguientes:

- Servidores, servicios y grupos de servicios de equilibrio de carga
- Servidores de conmutación de contenido
- Servidores de redirección de caché
- Equilibrio de carga de servicio global (GSLB)
- Autenticación
- NetScaler 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:



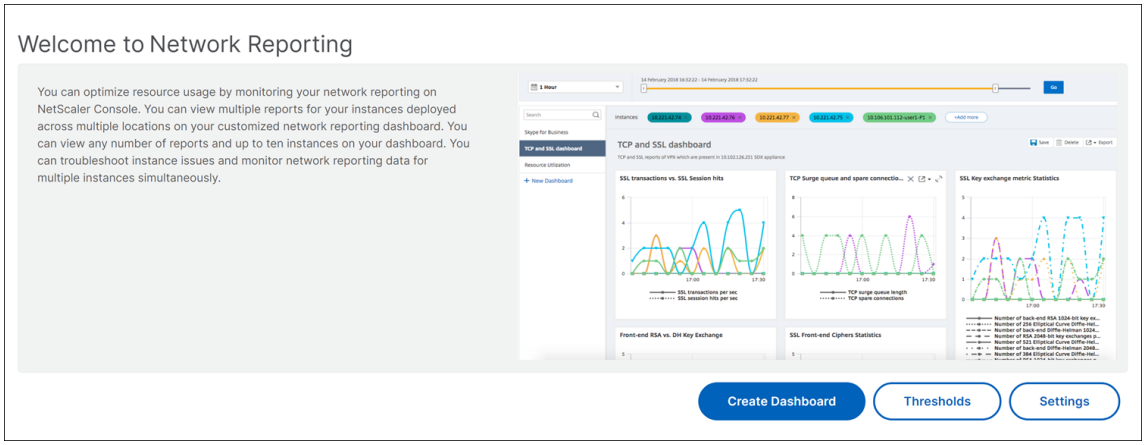
- El panel del lado izquierdo muestra todos los paneles personalizados creados en NetScaler ADM. Puede hacer clic en uno de ellos para ver los diversos informes de los que está compuesto el panel. Por ejemplo, un panel TCP y SSL contiene varios informes relacionados con protocolos TCP y SSL.

- Puede personalizar cada panel con varios widgets para mostrar varios 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 una periodicidad 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 NetScaler ADM le permite ver informes de 10 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.

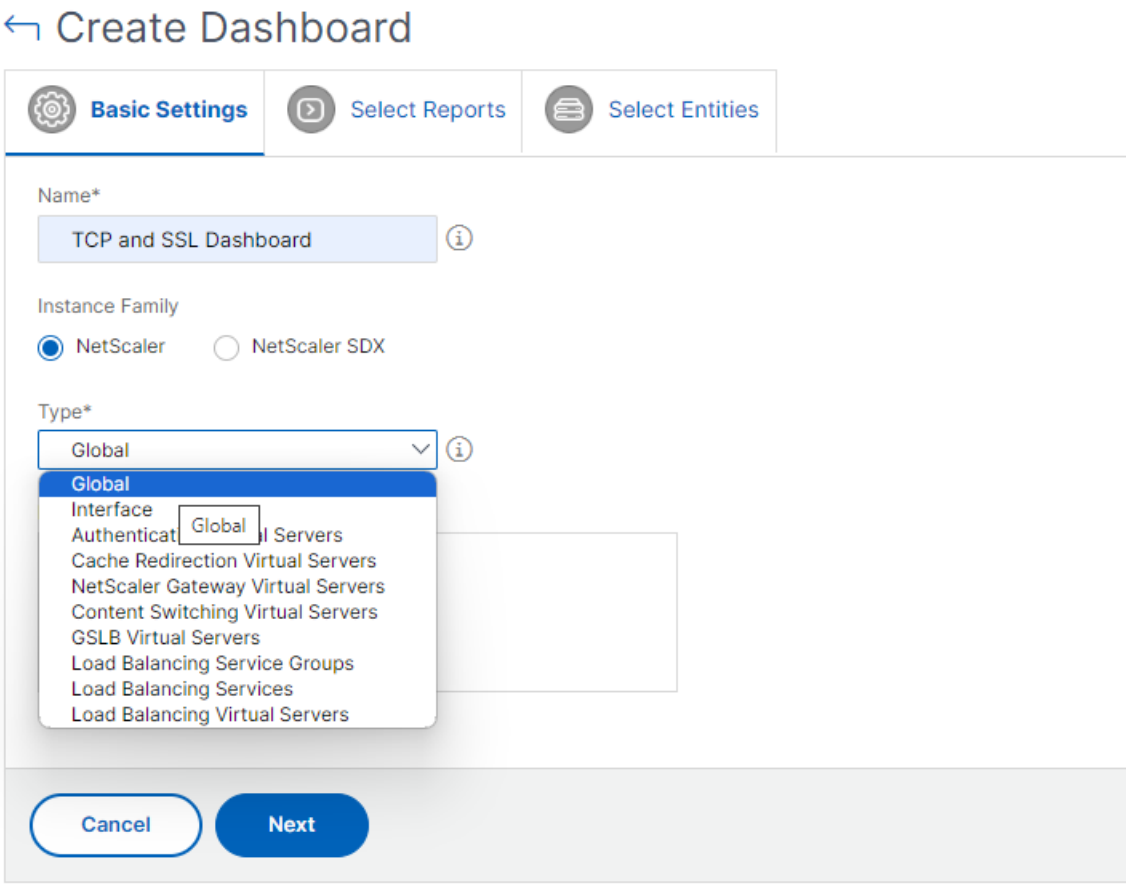
En la siguiente sección se explican en detalle las tareas para crear un panel, generar informes y exportar informes.

Para ver o crear un tablero de mandos:

1. En NetScaler ADM, vaya a **Infraestructura > Informes de red**.



2. 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.
3. Para crear un panel, haga clic en **Nuevo panel**. Se abre la página Crear panel.



4. En la ficha Configuración básica, introduzca los siguientes detalles:

   a) **Nombre**. Escriba el nombre del panel de control.

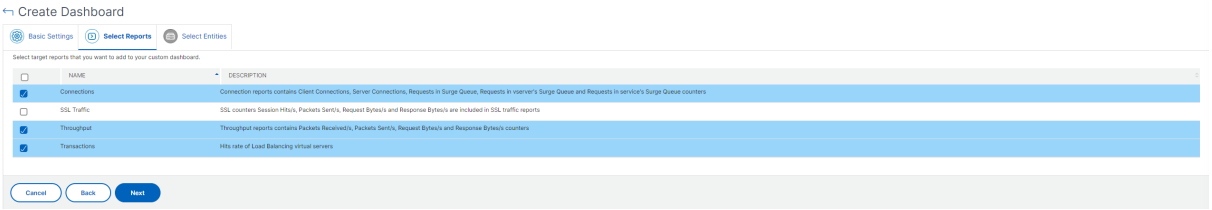
   b) **Familia**de instancias . Seleccione el tipo de instancia: NetScaler o NetScaler SDX.

   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.

5. Haga clic en **Siguiente**. Aparecen todos los informes compatibles para la instancia y la entidad específica.

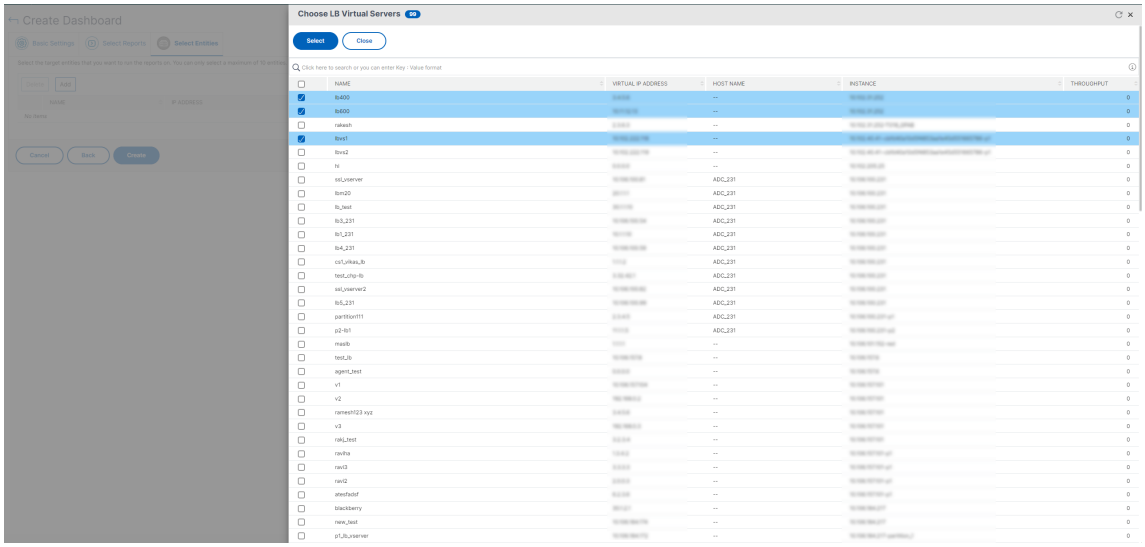
6. En la ficha **Seleccionar informes**, seleccione los informes necesarios. En este ejemplo, puede seleccionar las transacciones, las conexiones y el rendimiento. Haga clic en **Siguiente**.



1. En la ficha **Seleccionar entidades**, haga clic en **Agregar**.

   Aparecerá una ventana con la lista de entidades en función del tipo de entidad seleccionado en la ficha **Configuración básica**. En este ejemplo, aparece la ventana **Choose LB Virtual Servers**.

2. Seleccione las entidades que quiere supervisar.



3. Haga clic en **Crear**.

Se crea el panel de control 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 **Infraestructura > 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**.

   En la página **Exportar**, puede realizar una de las siguientes acciones:

6. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.

7. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

   Puede programar una exportación de la página del panel de control de **Network Reporting** de forma recurrente. Por ejemplo, puede establecer una opción para generar un informe de panel cada semana durante la hora anterior en un momento determinado. A continuación, el informe se genera cada semana y muestra el estado del panel de control. El informe anula la marca de fecha y hora, si lo establece el usuario.

> **Nota**
>
> - si selecciona Periodicidad semanal, asegúrese de seleccionar los días de la semana 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.

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 tiene esta cadena como nombre.

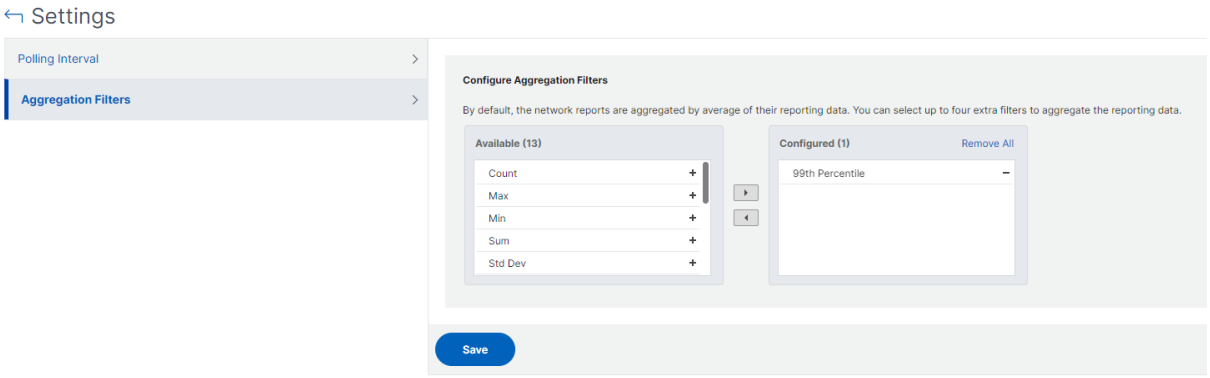
Por ejemplo, para los informes de red que se originan en un servidor virtual concreto, puede escribir el asunto "authentication-reports-10.106.118.120", donde 10.106.118.120 es la dirección IP del servidor virtual supervisado.

> **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.

Ver datos de informes de red mediante la aplicación de agregaciones

Puede aplicar agregaciones a los datos de rendimiento de la red y ver el rendimiento de las aplicaciones en el panel. También puede exportar los resultados en función de sus necesidades. Al usar estas agregaciones aplicadas a los datos, puede analizar y asegurarse de que todos los recursos se utilizan de manera óptima. Vaya a **Red > Informes de red** y seleccione la duración de 1 día o más para **ver la opción Ver por**.

En los datos medios existentes, puede aplicar agregaciones seleccionando la opción de la lista **Ver por**. Cuando se aplica la agregación, los datos se actualizan para cada métrica en el tablero de mandos. Haga clic en **Configuración** y seleccione **Filtros de agregación**.



Las siguientes son las agregaciones que puede agregar:

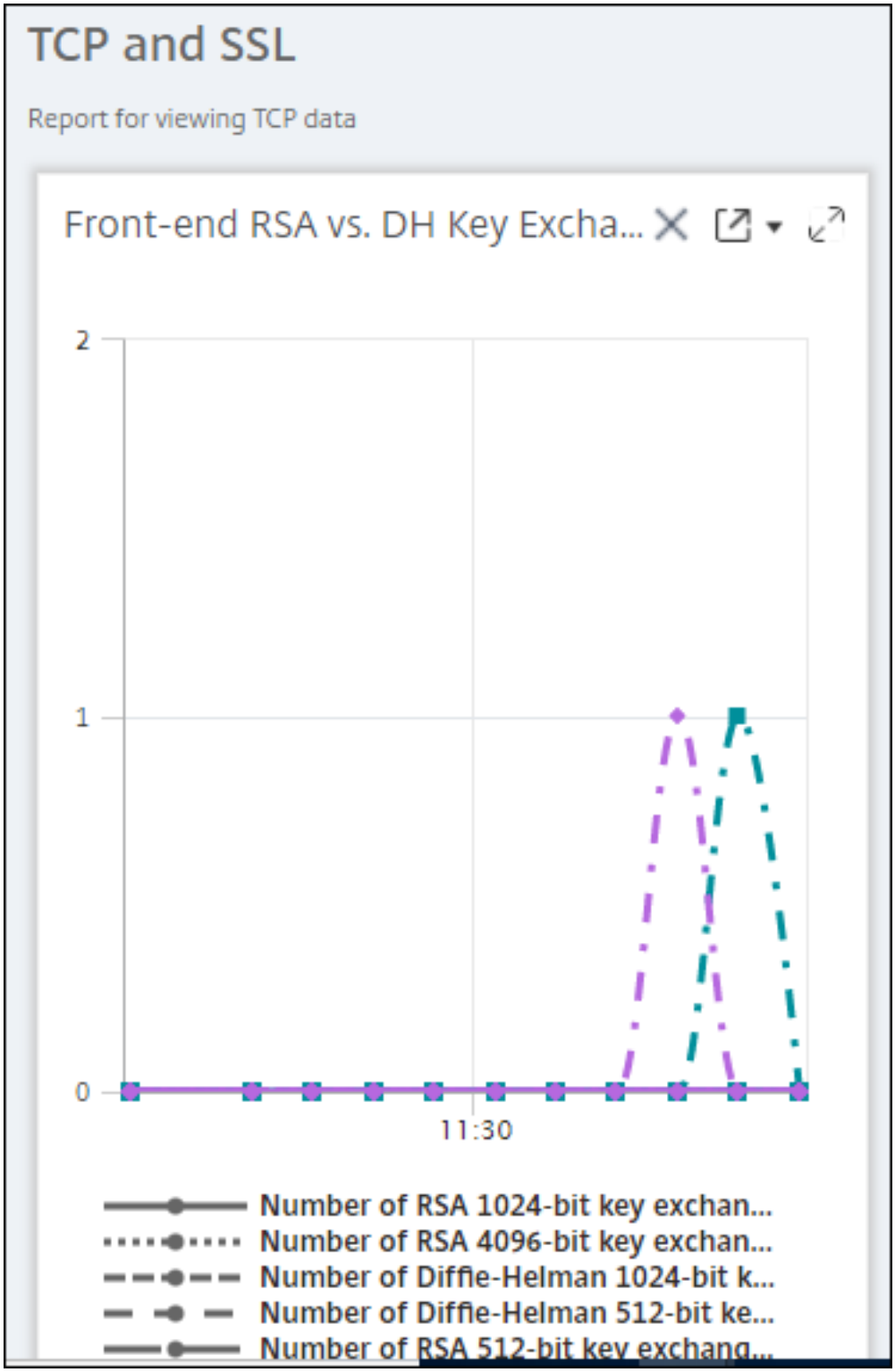
- Recuento
- Máx.
- Mín.
- Suma
- Desarrollo de Std
- Desviación
- Modo
- Mediana
- Percentil 25
- Percentil 75
- Percentil 95
- Percentil 99
- Primera
- Última

Puede agregar hasta 4 opciones de agregación al panel. Después de agregar las opciones de agregación, NetScaler ADM tarda aproximadamente 1 hora en generar informes para las opciones de agregación seleccionadas.

Para exportar informes de widgets:

1. Vaya a **Infraestructura > 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, también haga clic en **Skype Empresarial**.
4. Seleccione un widget. Por ejemplo, seleccione **Load Balancing Virtual Server Transactions**.
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, 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. Para ver estos eventos, vaya a **Infraestructura > 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 NetScaler ADM, vaya a **Infraestructura > Informes de red > Umbrales**. En **Umbrales**, haga clic en **Agregar**.
2. En la página **Crear umbral**, especifique los siguientes detalles:
    - **Nombre**. Nombre del umbral.
    - **Tipo de instancia**. Elija NetScaler.
    - **Nombre del informe**. Nombre del informe de rendimiento que proporciona información sobre este umbral.
3. 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. Puede ver los eventos de "gravedad crítica"en **Infraestructura > Eventos > Informes**. En la página Informes, puede hacer clic en el anillo **Eventos por gravedad** para ver los eventos según su gravedad.

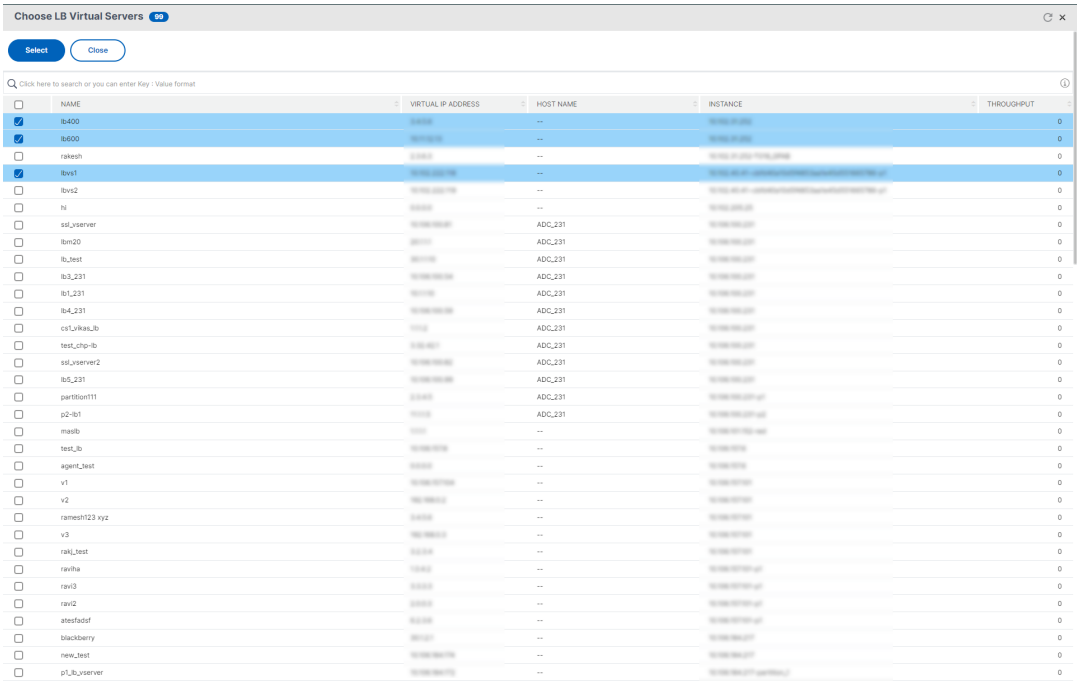
- **Valor claro**. Escriba el valor que indica cuándo borrar el valor. Por ejemplo, puede que quiera borrar el umbral de conexiones de clientes actuales cuando el valor supervisado alcance el 50 por ciento. En este caso, escriba 50 como valor de borrado.
- **Gravedad del evento** Seleccione el nivel de seguridad que quiera establecer para el valor del umbral.

4. Puede elegir las instancias y entidades que se establecerán con el valor umbral. En la sección **Instancias**, elija una de las siguientes opciones:

   - **Todas las instancias**. El umbral se establece para todas las instancias.
   - **Instancias específicas**. El umbral se establece para instancias específicas. Utilice la flecha derecha para mover las instancias de la lista **Disponible** a la lista **Configurados**. El umbral se establece para las instancias de la lista **Configurados**.
   - **Entidades específicas**. El umbral se establece para entidades específicas.

     Haga clic en **Agregar** para seleccionar las entidades.

     Aparece una ventana con la lista de entidades según el tipo de informe seleccionado en el campo **Nombre del informe**. En este ejemplo, aparece la ventana **Elegir servidores virtuales LB**.



     Seleccione las entidades para las que quiera establecer un umbral. Haga clic en **Seleccionar**. Las entidades seleccionadas aparecen en la sección **Instancias**.

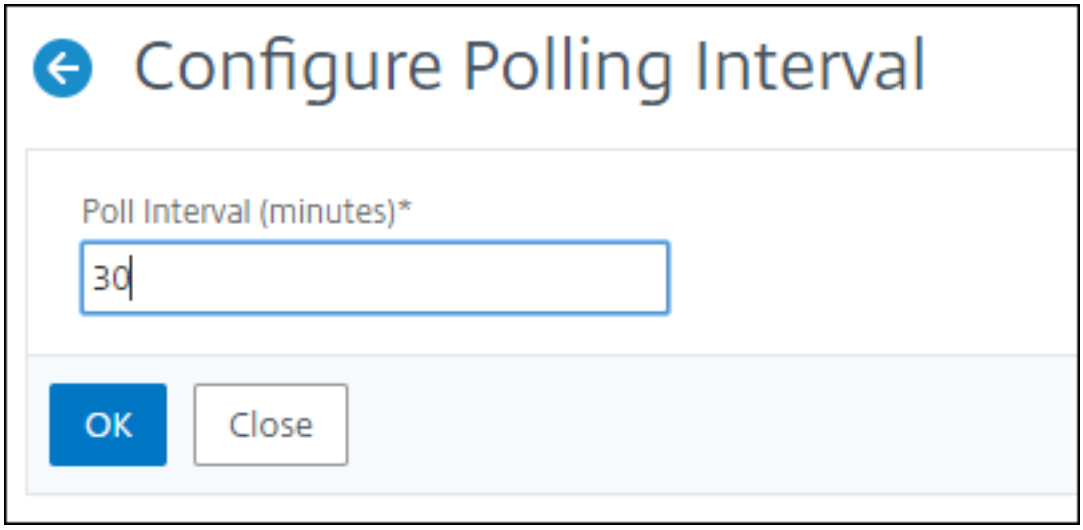
> **Nota:**
>
> La opción **Entidades específicas** solo aparece si selecciona informes basados en vserver en el **nombre del informe**. Por ejemplo, si selecciona **LB Service Statistics**

5. También puede agregar 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.
6. Seleccione**Activar**para habilitar el umbral para generar alarmas.
7. Opcionalmente, puede configurar **Acciones** como notificaciones de correo electrónico o Slack, o ambas notificaciones de correo electrónico y Slack.
8. 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. ADM recupera estadísticas de instancia como información de contadores y las agrega en función de 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 **Infraestructura > 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. Esta configuración limita la cantidad de datos de informes de red que se almacenan en la base de datos del servidor NetScaler 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 exceder los 30 días ni ser inferior a 1 día.

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) de la red.

NetScaler 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 uno de estos para crear un origen reutilizable de comandos e instrucciones para el sistema para ejecutar 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 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 .

> **Nota**
> La opción **Cambiar nombre** está inhabilitada para las plantillas de configuración predeterminadas. Sin embargo, puede cambiar el nombre de las plantillas de configuración personalizadas.

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 el trabajo para que se ejecute en una etapa posterior.

Instancia

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. También puede actualizar una instancia de NetScaler extrayendo la configuración en ejecución o una configuración guardada y ejecutando los comandos en otra instancia de NetScaler 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

Mediante Crear trabajo, puede introducir sus propios comandos CLI o utilizar el botón Grabar y reproducir para obtener comandos de una sesión de NetScaler. 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 todas 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 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 **Infraestructura > Trabajos de configuración**.
2. Haga clic en **Crear trabajo**.
3. En la página **Crear trabajo**, en la ficha **Seleccionar configuración**, especifique el nombre del trabajo y seleccione el **tipo de instancia** de la lista.

4. En la lista de **fuentes** de configuración, seleccione la plantilla de trabajo de configuración que quiere 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 de **fuentes de configuración**, seleccione las diferentes plantillas y, a continuación, arrástrelas al editor de configuración. Los tipos de plantillas pueden ser **Plantilla de configuración**, **Plantilla integrada**, **Configuración maestra**, **Grabar y reproducir**, **Instancia** y **Archivo**.

    > **Nota**
    >
    > Si agrega la `Deploy Master Configuration Job` plantilla por primera vez, agregue una plantilla de otro tipo y, a continuación, toda la plantilla de trabajo se convierte en un `Master Configuration` tipo.

    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 mientras modifica el trabajo de configuración.

    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 ficha**Previsualizar variables**para obtener una vista previa de las variables en una única vista consolidada que haya definido al crear o modificar un trabajo de configuración.

    Puede personalizar los comandos de reversión para cada comando del editor de configuración. Para especificar los comandos personalizados, habilite la opción de reversión personalizada.

    > **Importante**
    >
    > Para que la reversión personalizada surta efecto, complete el asistente de **creación de trabajos**. Y en la ficha **Ejecutar**, seleccione la opción **Revertir comandos correctos** de la lista **Al fallar un comando**.

5. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración.

    a) En un par de alta disponibilidad de NetScaler, puede ejecutar un trabajo de configuración local en un nodo primario o secundario. Seleccione en qué nodo quiere ejecutar el trabajo.

- **Ejecutar en nodos primarios**: seleccione esta opción para ejecutar el trabajo solo en nodos primarios.
- **Ejecutar en nodos secundarios**: seleccione esta opción para ejecutar el trabajo solo en nodos secundarios.

También puede elegir tanto el nodo principal como el secundario para ejecutar el mismo trabajo de configuración. Si no selecciona nodo principal o secundario, el trabajo de configuración se ejecuta automáticamente en el nodo principal.

6. 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.
   c) Haga clic en **Siguiente**.

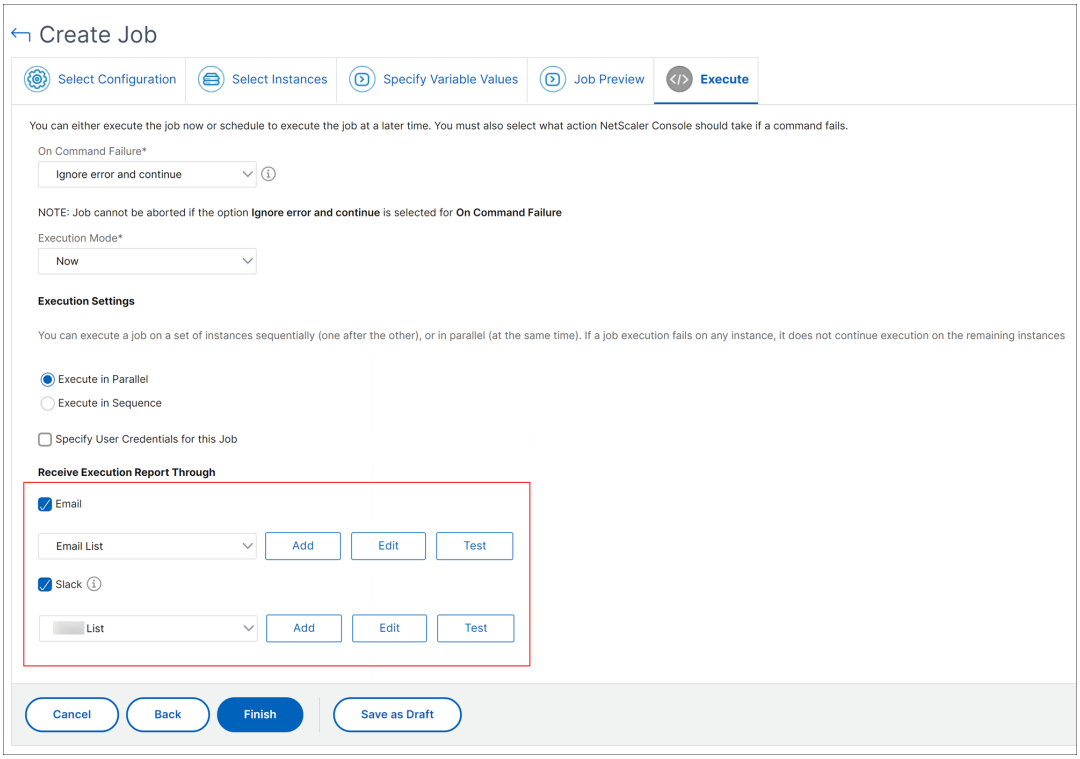
Para enviar un correo electrónico y una notificación de Slack para un trabajo:

Ahora se envía un correo electrónico y una notificación de Slack cada vez que se ejecuta o se programa un trabajo. La notificación incluye detalles como el éxito o fracaso del trabajo junto con los detalles relevantes.

1. Vaya a **Infraestructura > Trabajos de configuración**.
2. Seleccione el trabajo que quiere habilitar la notificación de correo electrónico y Slack y haga clic en **Modificar**.
3. En la ficha **Ejecutar**, vaya al panel **Recibir informe de ejecución mediante** :
   - Seleccione la casilla **Correo electrónico** y elija la lista de distribución de correo electrónico a la que quiere enviar el informe de ejecución.

     Si quiere agregar una lista de distribución de correo electrónico, haga clic en **Agregar** y especifique los detalles del servidor de correo electrónico.
   - Selecciona la casilla de verificación de **Slack** y elige el canal de Slack al que quieres enviar el informe de ejecución.

     Si quiere agregar un perfil de Slack, haga clic en **Agregar** y especifique el **nombre del perfil**, el **nombre del canal** y el **token** del canal de Slack requerido.



4. Haga clic en **Finalizar**.

Para enviar un correo electrónico y una notificación de Slack para un trabajo:

Ahora se envía un correo electrónico y una notificación de Slack cada vez que se ejecuta o se programa un trabajo. La notificación incluye detalles como el éxito o fracaso del trabajo junto con los detalles relevantes.

1. Vaya a **Infraestructura > Trabajos de configuración**.
2. Seleccione el trabajo que quiere habilitar la notificación de correo electrónico y Slack y haga clic en **Modificar**.
3. En la ficha **Ejecutar**, vaya al panel **Recibir informe de ejecución mediante** :
    - Seleccione la casilla **Correo electrónico** y elija la lista de distribución de correo electrónico a la que quiere enviar el informe de ejecución.

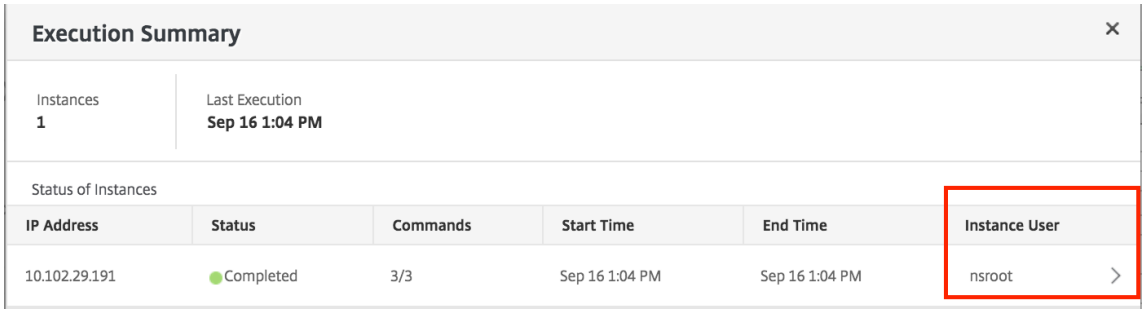
      Si quiere agregar una lista de distribución de correo electrónico, haga clic en **Agregar** y especifique los detalles del servidor de correo electrónico.
    - Selecciona la casilla de verificación de **Slack** y elige el canal de Slack al que quieres enviar el informe de ejecución.

      Si quiere agregar un perfil de Slack, haga clic en **Agregar** y especifique el **nombre del perfil**, el **nombre del canal** y el **token** del canal de Slack requerido.

4. Haga clic en **Finalizar**.

Para ver los detalles del resumen de ejecución:

1. Vaya a **Infraestructura > Trabajos de configuración**.
2. Seleccione el trabajo que quiere ver el resumen de ejecución y haga clic en **Detalles**.
3. Haga clic en **Resumen de ejecución** para ver:
    - El estado de la instancia en la que se ejecuta el trabajo
    - Los comandos se ejecutan en el trabajo
    - La hora de inicio y finalización del trabajo, y
    - Nombre del usuario de la instancia



Ver informes de auditoría

January 30, 2024

(NetScaler 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:

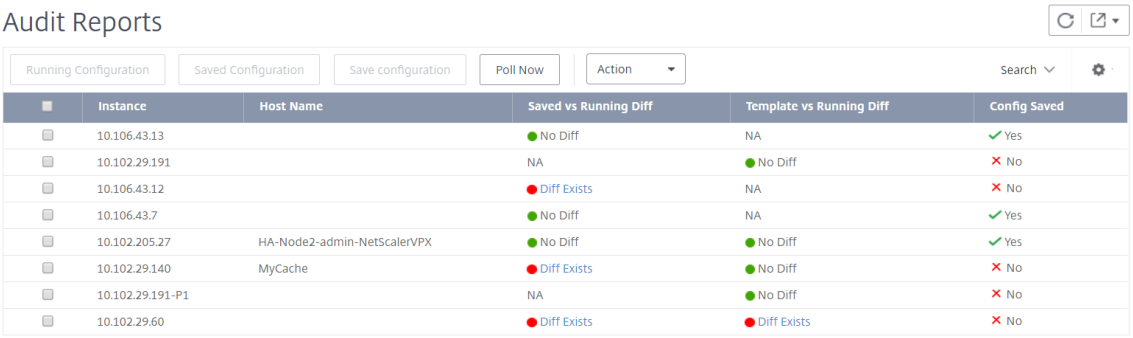
- Informe resumido de todas las instancias por instancia
- Informe diferencial granular (diff) para cada par instancia-plantilla

Las plantillas de auditoría de las **plantillas de auditoría** se ejecutan a la hora programada con respecto a 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 **NetScaler Config Drift**, la página de **informes de auditoría** que aparece a continuación muestra una lista de instancias que muestra tanto «Diff Exists» como «No Diff». « Puede descargar los informes de diferencias que muestra NetScaler ADM.

NetScaler ADM también ofrece la opción de programar la exportación automática de un informe de diferencias como archivo adjunto 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 NetScaler ADM, vaya a **Infraestructura > Configuración > 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.

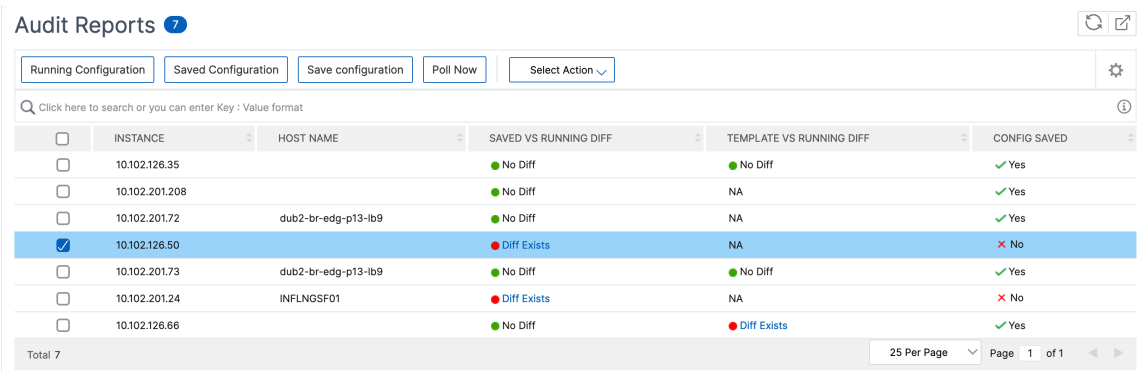


En la imagen puede ver que para algunos casos un diff está presente solo en **Saved Vs Running Diff** y para algunos casos, un diff está presente solo en **Template vs Running Diff**. En algunos casos, existen diferencias entre **Saved Vs Running Diff** y **Template vs Running Diff.**

Diferencia guardada frente a ejecución

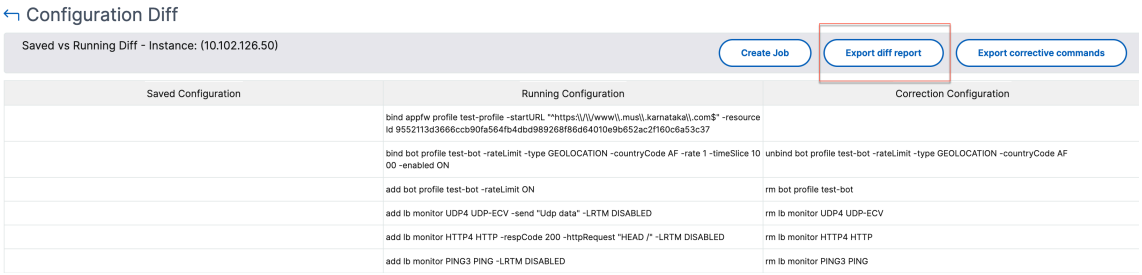
Puedes ver un informe de la diferencia entre la configuración guardada en la instancia y la configuración que se está ejecutando actualmente en la instancia.

1. Haz clic en **Diff Exists** para una instancia en **Saved Vs Running Diff.**



Puedes ver el informe de la configuración guardada comparándolo con la configuración diferencial en ejecución para esa instancia.

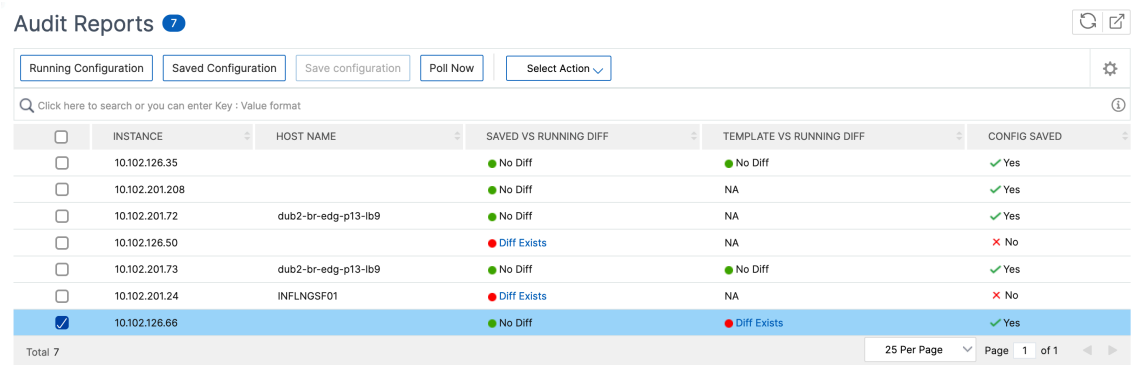
2. Haga clic en **Exportar informe de diferencias** para descargar un archivo CSV del informe de diferencias. También puede hacer clic en **Exportar comandos correctivos** para exportar los comandos a un archivo.txt. A continuación, puede ejecutar los comandos en la instancia ADM de NetScaler asociada desde Configuration Jobs para corregir la configuración de esa instancia.



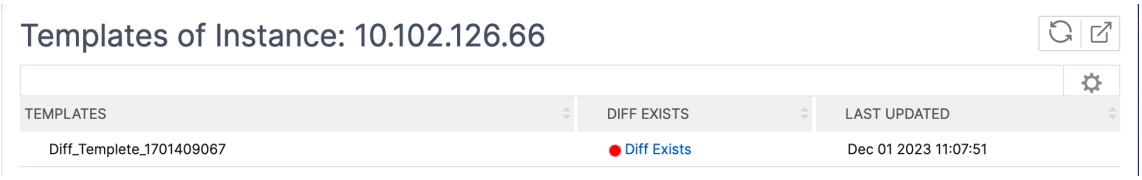
Plantilla vs Diff Running

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.

1. Haga clic en **Diff Exists** para una de las instancias de **Template vs Running Diff.**

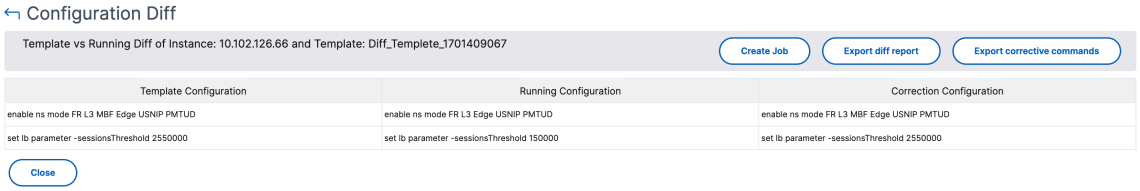


2. Las plantillas revelan las diferencias cuando la instancia de NetScaler ADM se desvía de la configuración especificada en la plantilla.



3. Haga clic de nuevo en**Diff Exists**. La siguiente imagen muestra la configuración que busca la plantilla, las configuraciones en ejecución y las configuraciones de corrección o los comandos

que se deben ejecutar para corregir la configuración. Si la **configuración** en ejecución está en blanco, significa que los comandos no están configurados o que se han eliminado.



4. 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 CLI para corregir la configuración de la instancia.

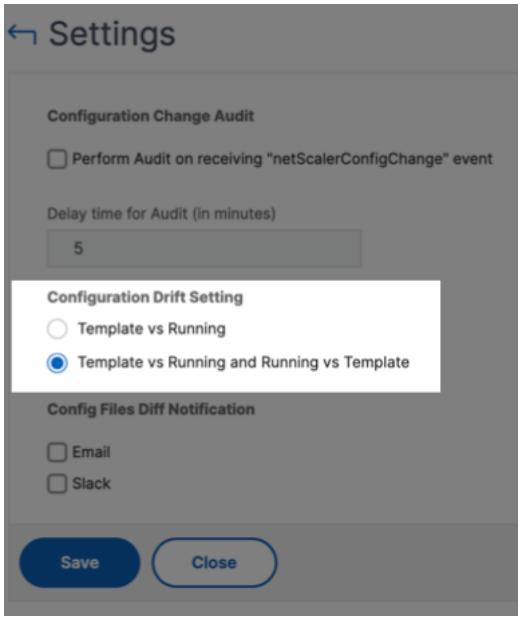
Template_vs_Running_Diff_of_Instance _10.102.126.66_and_Template _Diff_Templete_1701409067

Template Configuration	Running Configuration	Correction Configuration	
enable ns mode FR L3 MBF Edge USNIP PMTUD	enable ns mode FR L3 Edge USNIP PMTUD	enable ns mode FR L3 MBF Edge USNIP PMTUD	
set lb parameter -sessionsThreshold 2550000	set lb parameter -sessionsThreshold 150000	set lb parameter -sessionsThreshold 2550000	

También puede utilizar la configuración Plantilla frente a Ejecución y Ejecución frente a la plantilla, para comparar la configuración de ambos modos:

- Compara la configuración de la plantilla de auditoría con la configuración en ejecución en la instancia.
- Compara la configuración en ejecución de la instancia con la plantilla de auditoría.

De forma predeterminada, la plantilla vs. Se selecciona la configuración Running Drift. Para modificar la configuración de deriva, seleccione **Configuración**en la página **Auditoría de configuración** .



Ver los informes de auditoría de estado de archivo

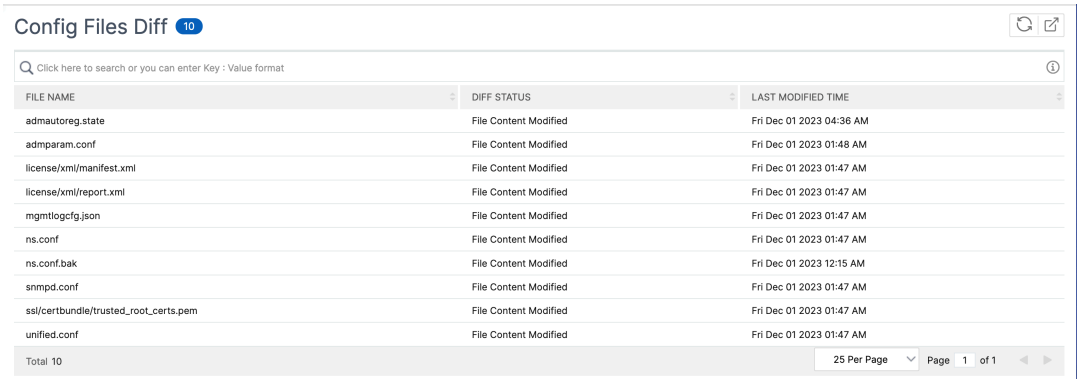
Utilice la tabla de estado de **archivos de NetScaler** para supervisar si se agrega, modifica o elimina algún archivo de la carpeta `nsconfig`. Por ejemplo, si el archivo de licencia se actualiza en una instancia de NetScaler, puede comprobar cuándo se actualizó por última vez este archivo y tomar las medidas necesarias.

1. Vaya a **Infraestructura > Configuración > Auditoría de configuración**.
2. En la página **Auditoría de configuración** , haga clic en el gráfico de estado del **archivo de configuración de NetScaler** .

   La página **Informes de auditoría** muestra las instancias con el estado Diff.

   El **estado** de la diferencia se calcula para el intervalo entre la **hora de la encuesta anterior** y la **última hora de la encuesta**. El **estado** de la diferencia puede ser uno de los siguientes:

   - **La diferencia existe**: este estado indica que los archivos han cambiado en la carpeta `nsconfig` de una instancia desde la **hora de la encuesta anterior**. Para ver lo que ha cambiado en el archivo, haga clic en **Diff Exists**.



- **Sin diferencias**: Este estado indica que los archivos de la`nsconfig` carpeta no han cambiado desde la hora de la encuesta anterior.
- **NA**: este estado indica que la supervisión del estado del archivo no es aplicable. Este estado aparece cuando el NetScaler ADM no sondea la instancia. Por ejemplo, cuando se agrega una instancia recientemente o el estado de la instancia está inactivo, no se realiza el sondeo de la instancia.

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 quiere supervisar los cambios de configuración en las instancias administradas de NetScaler, solucionar los errores de configuración y recuperar configuraciones no guardadas después de un apagado repentino del sistema.

Puede crear plantillas de auditoría con configuraciones específicas para auditar en determinadas instancias. NetScaler ADM compara estas instancias con la plantilla de auditoría e informa si hay una discrepancia en la configuración. El informe de diferencias de configuración le permite solucionar problemas y rectificar los cambios de configuración no deseados.

Puede automatizar la ejecución de la plantilla de auditoría de la siguiente manera:

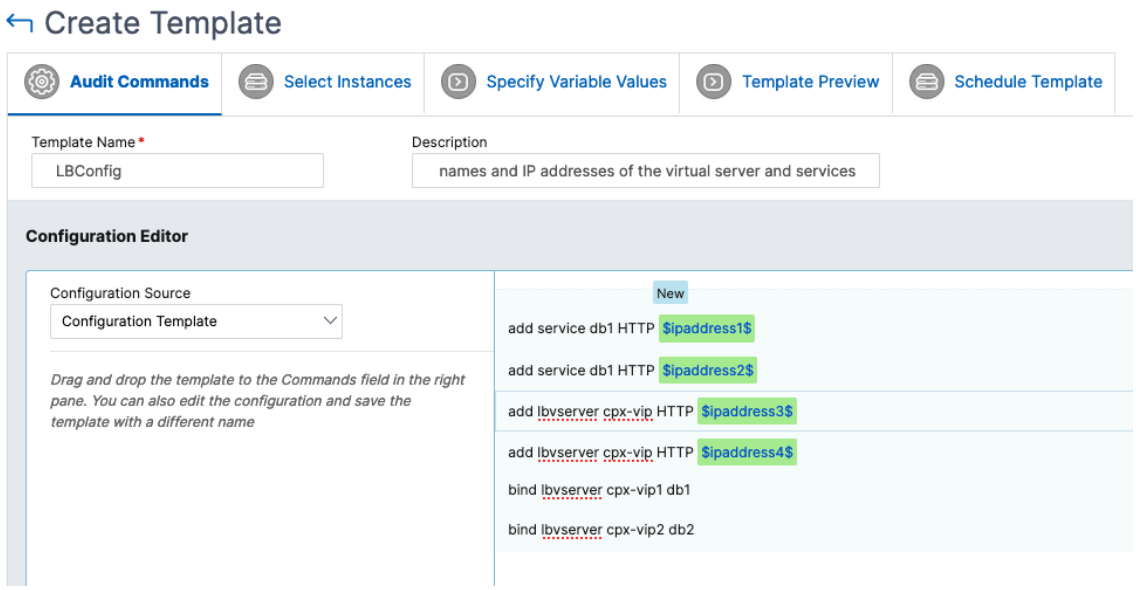
- Programar la hora a la que se debe ejecutar la plantilla.
- Establecer la frecuencia con la que NetScaler ADM debe ejecutar la plantilla. Puede ejecutar la plantilla diariamente, en un día específico de una semana o en una fecha específica de un mes.

También tiene la opción de enviar el informe de diferencias generado por NetScaler ADM a las direcciones de correo electrónico especificadas que puede configurar. Con esta opción, los usuarios pueden recibir el informe como un archivo adjunto de correo o una notificación de Slack. No tienen que iniciar sesión en NetScaler ADM para exportar los informes manualmente.

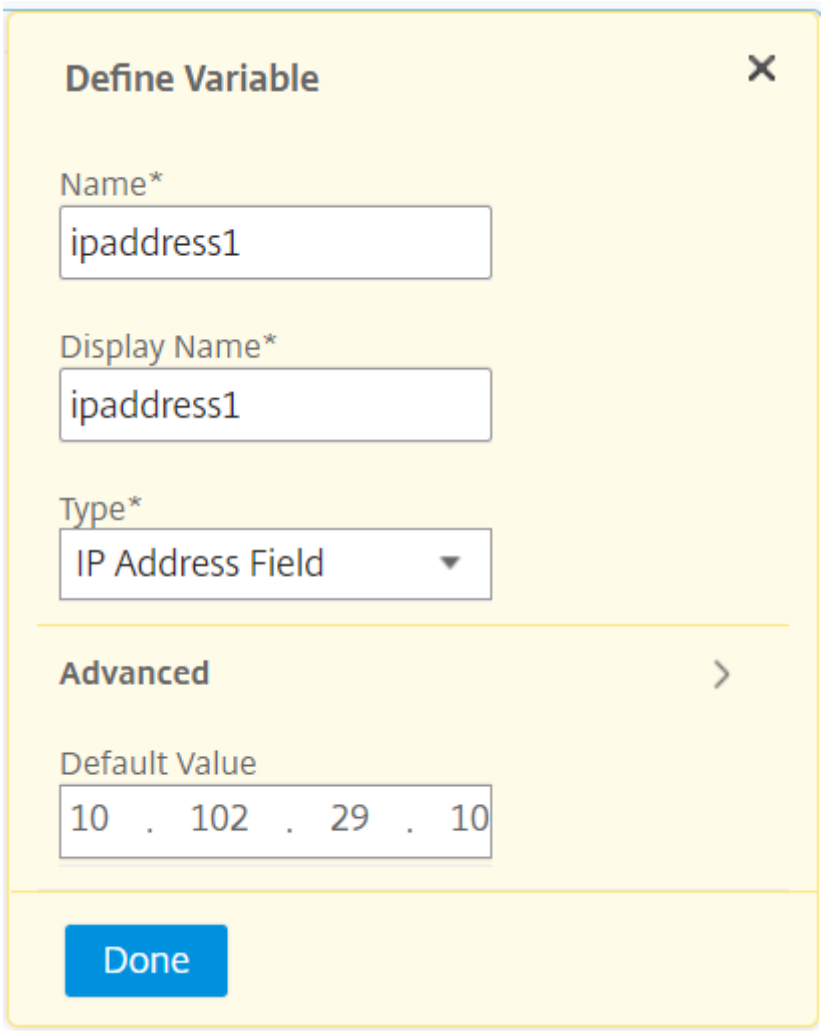
> **Nota:**
>
> La opción **Cambiar** nombre está deshabilitada para las plantillas de configuración predeterminadas. Sin embargo, puede cambiar el nombre de las plantillas de configuración personalizadas.

Para crear plantillas de auditoría:

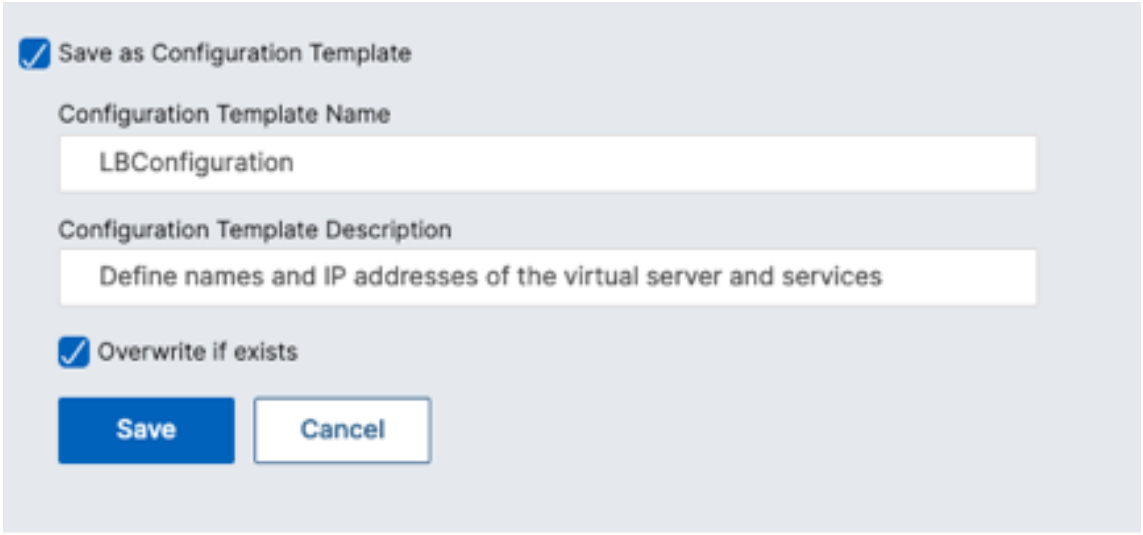
1. Vaya a **Infraestructura > Configuración > Auditoría de configuración > Plantillas de auditoría** y haga clic en **Agregar** .
2. En la página **Crear plantilla** y en la pestaña **Comandos de auditoría** , especifique el nombre de la plantilla y su descripción.
3. En la página **Editor de configuración**, 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 está encerrada con «$».



   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.

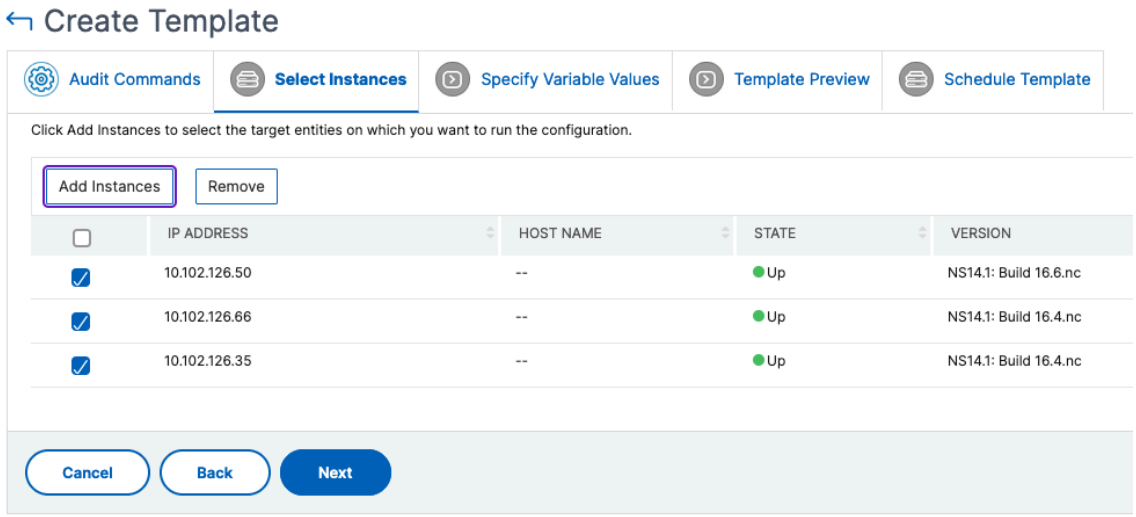


También puede guardar los comandos como una plantilla de configuración.



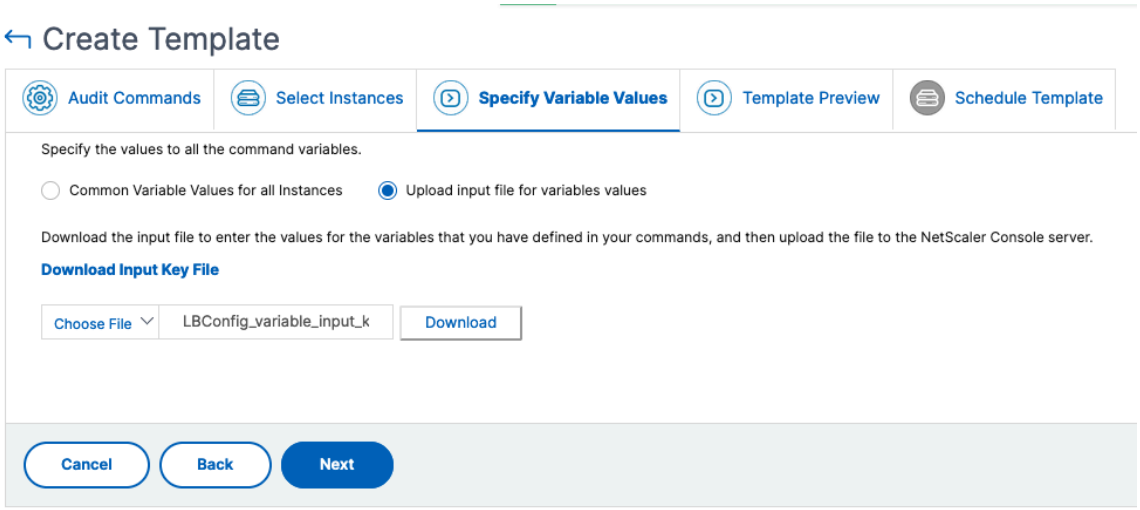
5. Haga clic en **Guardar** y, a continuación, en **Siguiente** .

6. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración y haga clic en **Siguiente**.

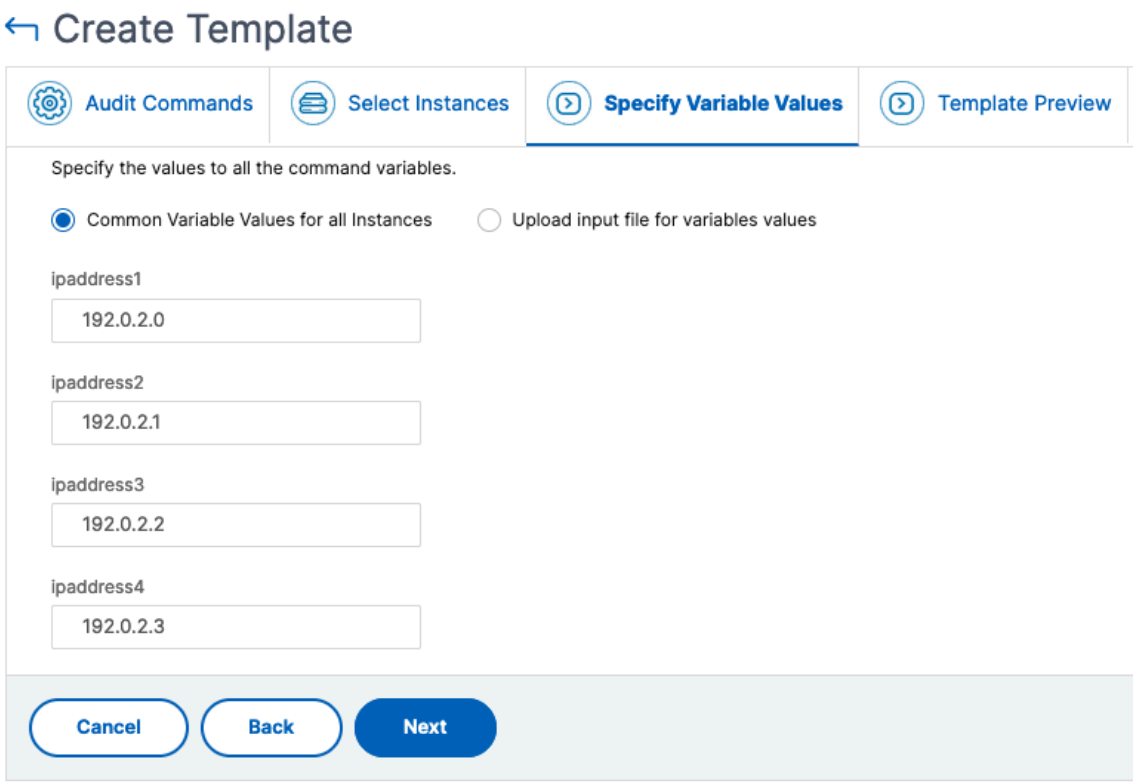


7. En la ficha **Especificar valores de variable**, tiene dos opciones:

   a) Descargue el archivo de entrada para introducir los valores de las variables que ha definido en los comandos. Tras introducir las variables, cargue el archivo en el servidor NetScaler ADM.

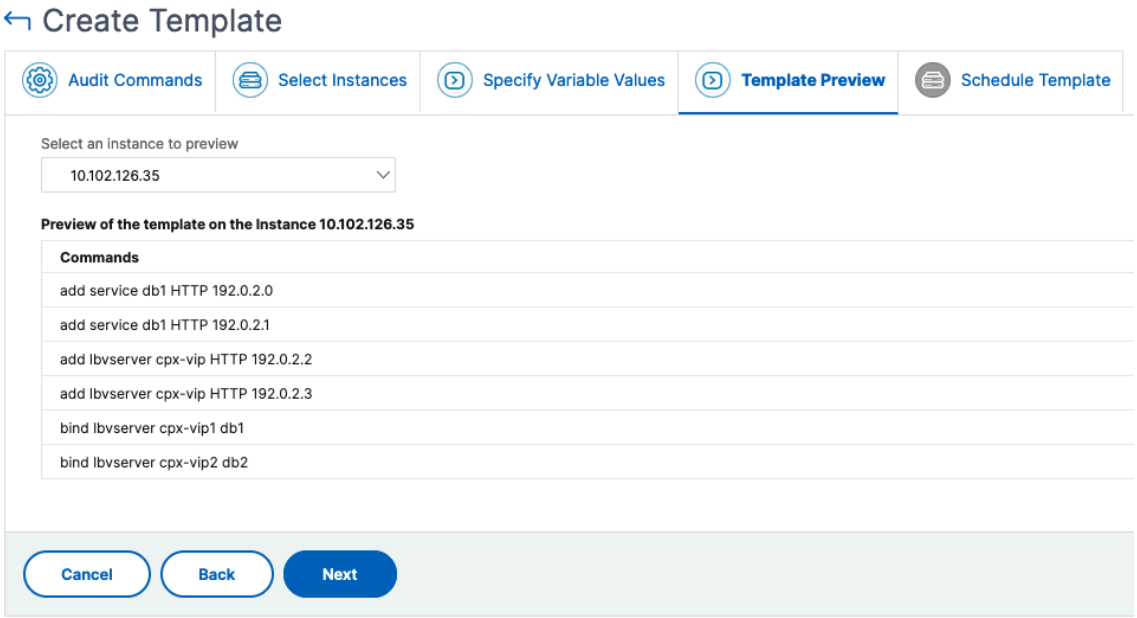


   a) Introduzca valores comunes para las variables que ha definido para todas las instancias.



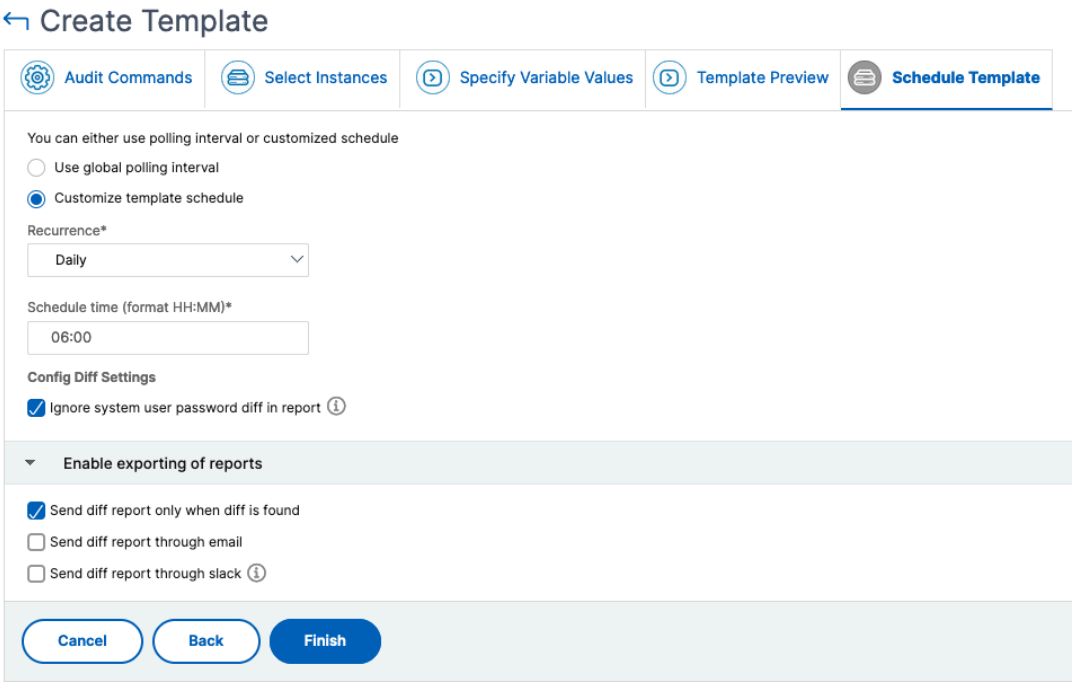
> **Nota:**
>
> Si quieres auditar cada instancia con valores diferentes, debes crear variables independientes en el archivo de entrada para cada instancia.

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.
    - **Personalizar la planificación de plantillas**. Utilice esta opción para configurar la hora y la frecuencia con las que se deben ejecutar las plantillas.
        - Especifique la frecuencia y el momento de ejecución de las plantillas de auditoría.
    - **Habilite la exportación de informes**. Utilice esta opción para:
        - **Enviar informe de diferencias: solo se encuentra la diferencia**
        - **Envíe el informe de diferencias por correo**electrónico . Configure el perfil de correo al que se debe enviar el informe de diferencias como archivo adjunto de correo.
        - **Envía un informe de diferencias a través de Slack**. Configura el canal de Slack al que se debe enviar el informe de diferencias como notificación.



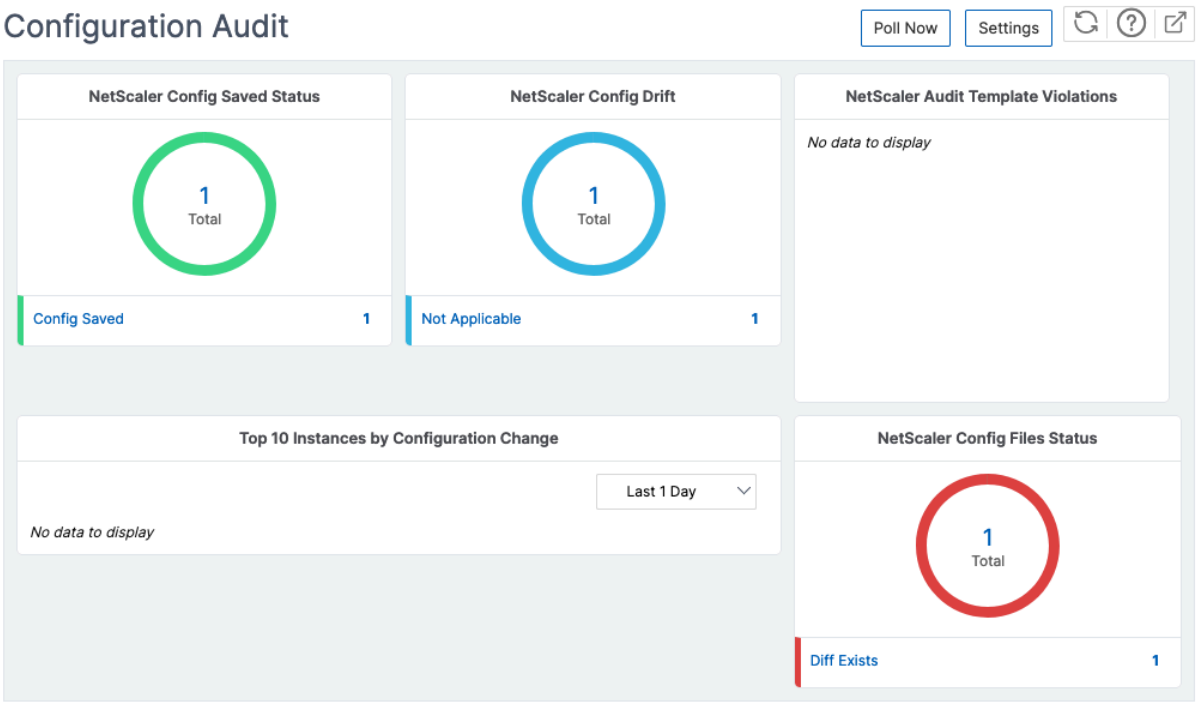
11. Haga clic en **Finalizar**.

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 los 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 10 instancias principales por cambio de configuración
- El número de configuraciones guardadas y no guardadas
- El archivo agregado, eliminado o modificado en la`nsconfig` carpeta

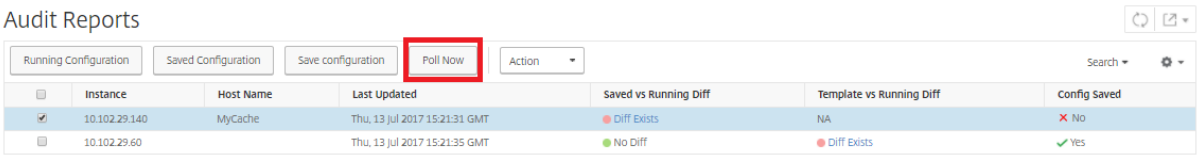


NetScaler ADM también le permite sondear auditorías de configuración manualmente y agrega todas las auditorías de configuración de las instancias inmediatamente al NetScaler ADM. Para hacerlo, vaya a **Infraestructura > Configuración > Auditoría de configuración**, haga clic en **Sondear ahora**. La página emergente **Sondear ahora** le ofrece la opción de sondear todas las instancias de NetScaler de la red o sondear las instancias seleccionadas.

También puede forzar una auditoría en una instancia. Para ello, haga clic en cualquiera de los gráficos siguientes:

- **Estado guardado de la configuración de NetScaler**
- **Deriva de configuración de NetScaler**

En la página **Informes de auditoría**, seleccione la instancia y, en la lista **Acción**, seleccione **Encuesta ahora**.



El gráfico de **estado del archivo de configuración de NetScaler** proporciona el estado de los archivos NetScaler presentes en la`nsconfig` carpeta. NetScaler ADM registra y compara los cambios en los archivos dentro de la`nsconfig` carpeta y muestra las diferencias. Consulte Ver los informes de auditoría del estado de los archivos.

Establecer notificaciones de auditoría de configuración

1. Vaya a **Infraestructura > Configuración > 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. Selecciona la **casilla**Activado . 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.

Obtener consejos de configuración sobre la configuración de la red

January 30, 2024

Puede configurar las instancias de NetScaler con configuraciones óptimas para que pueda lograr un rendimiento óptimo en sus aplicaciones. Sin embargo, algunas configuraciones pueden no ser configuraciones estándar, lo que podría afectar al rendimiento de sus aplicaciones.

Para ayudarlo a optimizar el rendimiento de la aplicación, NetScaler ADM analiza la configuración de la instancia de NetScaler y le ofrece recomendaciones. Puede aplicar las configuraciones recomendadas desde NetScaler ADM.

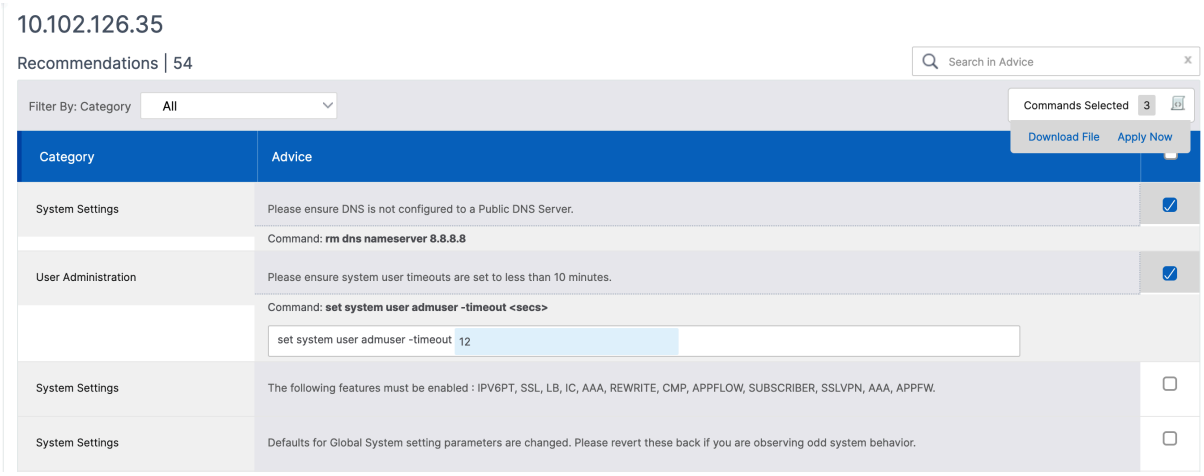
Para analizar la instancia de NetScaler:

1. Vaya a **Infraestructura > Configuración > Auditoría de configuración > Consejos 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 NetScaler que desee analizar.

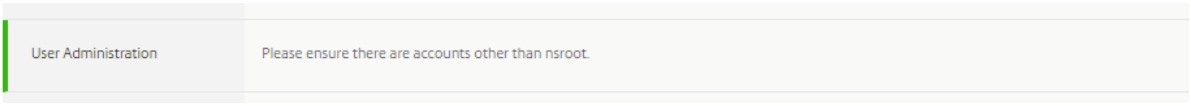
NetScaler ADM analiza la configuración de la instancia y proporciona una lista de recomendaciones de configuración como se muestra en la imagen siguiente. Haga clic en la casilla de verificación situada junto a un consejo de configuración para ver los comandos correctivos.



Si desea actualizar la configuración, especifique los valores de las variables en los comandos correctivos y haga clic en **Aplicar ahora** .

> **Nota:**
>
> Los comandos que se enumeran aquí son solo recomendaciones. Un usuario con acceso de lectura y escritura puede editar cualquier comando con esta función. Asegúrese de conceder un acceso privilegiado limitado a los usuarios que considere que no deben modificar 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 **Infraestructura > Instancias ><Instance_Type>**, seleccione la dirección IP de la instancia y, a continuación, haga clic en **Mostrar eventos** en la lista desplegable **Acciones**.

En la página **Eventos** , consulte los detalles del cambio de configuración.

Auditoría de configuración de sondeo de instancias NetScaler

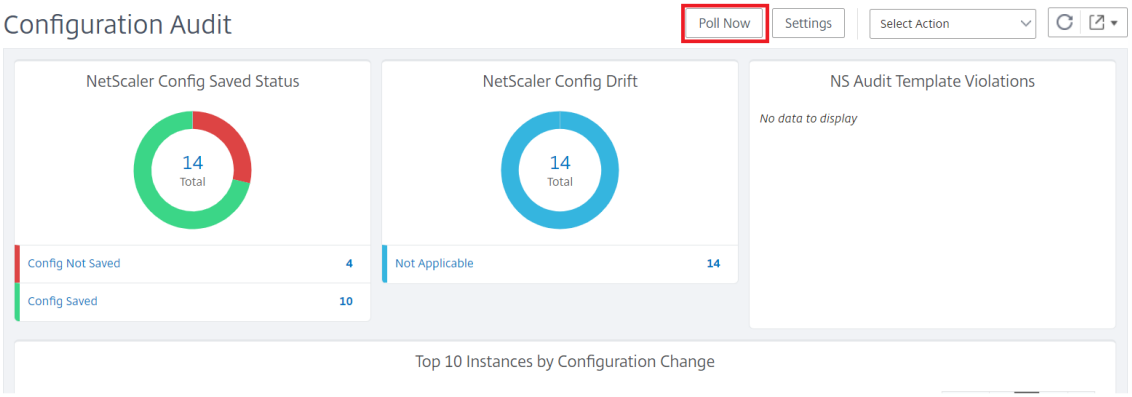
January 30, 2024

NetScaler ADM sondea automáticamente las auditorías de configuración cada 10 horas para buscar los cambios de configuración que se producen en las instancias de NetScaler. También puede sondear manualmente las auditorías de configuración para detectar cambios recientes, pero sondear todas las instancias de configuración de NetScaler coloca una carga pesada en la red.

En lugar de sondear toda la auditoría de configuración de instancias de NetScaler, puede sondear manualmente solo las auditorías de configuración de una instancia o instancias seleccionadas.

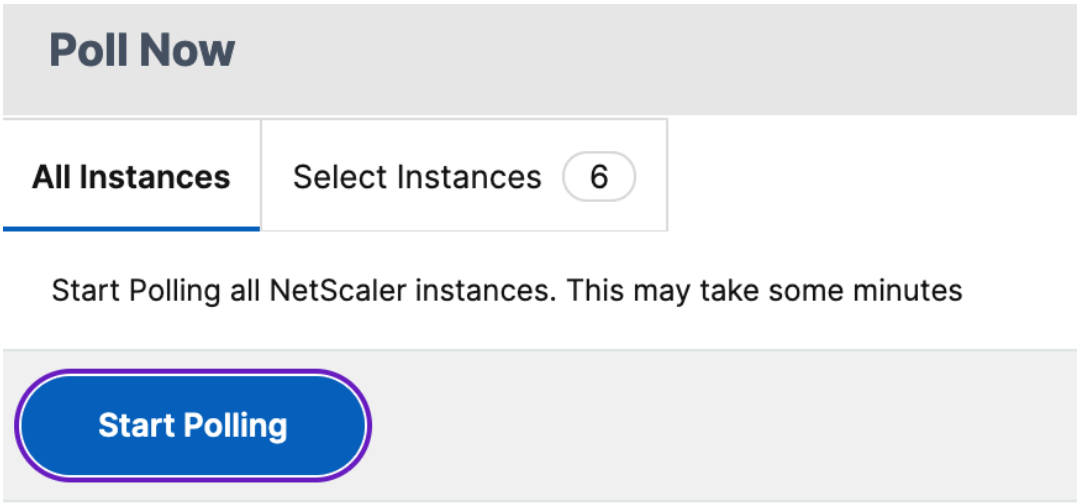
Para sondear auditorías de configuración de instancias NetScaler:

1. En NetScaler ADM, vaya a **Infraestructura > Configuración > Auditoría de configuración**.
2. En **Auditoría de configuración** , haga clic en **Sondear ahora** .

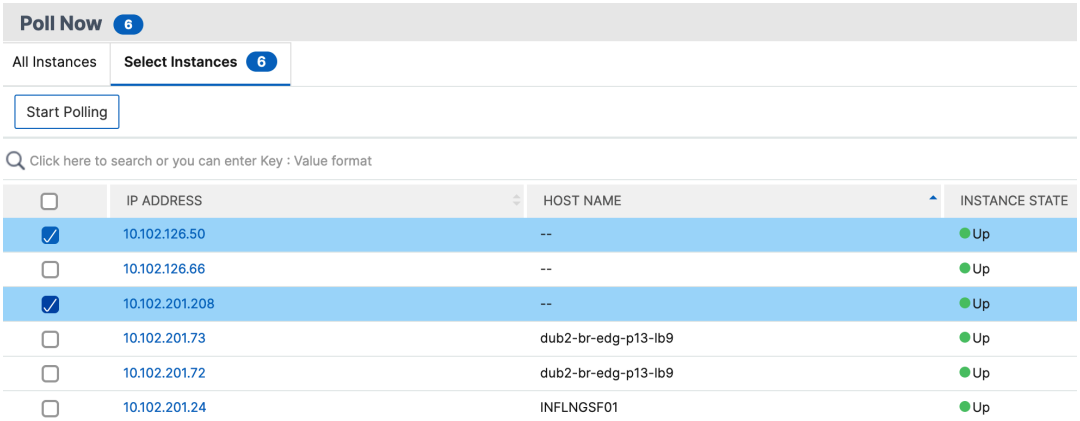


3. Aparece la página **Encuesta ahora**, que le da la opción de sondear todas las instancias de NetScaler en la red o sondear las instancias seleccionadas.

   a) Para sondear todas las instancias de NetScaler, 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

Cada vez que se produce un cambio de configuración en una instancia de NetScaler de la red, se actualiza el archivo de configuración. La instancia envía una captura SNMP de ConfigChange a NetScaler ADM. Puede habilitar NetScaler ADM para que realice una auditoría de configuración en esa instancia cuando la instancia envíe una captura SNMP de ConfigChange.

Si hay alguna diferencia entre la configuración de la plantilla de auditoría y la configuración en ejecución, aparece un mensaje de estado Diff Exists en la página **Informe de auditoría** . Haga clic en el enlace **Diff Exists** para ir a la página **Configuration Diff** , donde puede ver el comando correctivo. Puede utilizar estos comandos correctivos para crear un trabajo de configuración y ejecutarlo en las instancias específicas de NetScaler. Cuando ejecuta el trabajo de configuración, las instancias vuelven a la configuración deseada.

Para obtener más información sobre cómo crear trabajos 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 NetScaler ADM, vaya a **Infraestructura > Configuración > Auditoría de configuración**.
2. Haga clic **en **Configuración en la página Auditoría** de configuración .

3. Seleccione **Realizar auditoría al recibir el evento «NetScalerConfigChange** ».

> **Nota:**
>
> NetScaler ADM realiza una auditoría de configuración para cada instancia que reciba las trampas 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 después de este retraso de tiempo cuando recibe la captura de ConfigChange SNMP por esa instancia.

Auditoría de configuración

January 30, 2024

Este documento incluye temas sobre cómo:

- Ver informes de auditoría
- Auditar los cambios de configuración en todas las instancias
- Obtener consejos de configuración sobre la configuración de la red
- Auditoría de configuración de sondeo de instancias NetScaler
- Genere una diferencia de auditoría de configuración para las trampas SNMP de ConfigChange

Trabajos de actualización de versiones

January 30, 2024

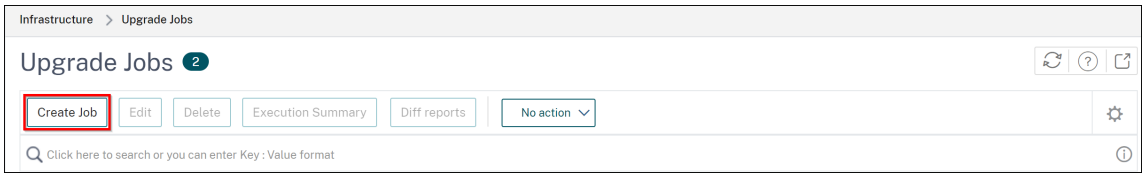
Puede crear las siguientes tareas de mantenimiento mediante NetScaler ADM. A continuación, puede programar las tareas de mantenimiento en una fecha y hora específicas.

- Actualizar instancias de NetScaler
- Actualizar instancias SDX de NetScaler
- Actualización de instancias NetScaler BLX
- Actualización de instancias de NetScaler en el grupo de Autoscale
- Configurar el par HA de instancias NetScaler
- Convertir un par de instancias de HA en clúster

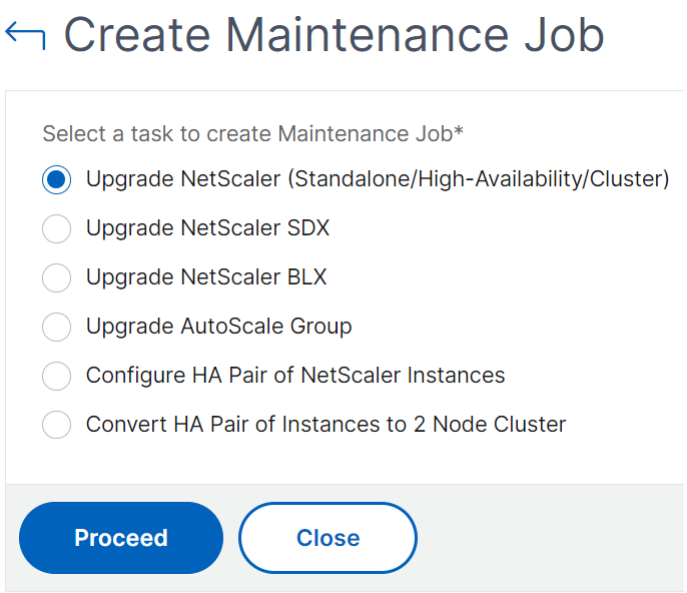
> **Nota:**
>
> Si se produce un error en un trabajo de actualización, NetScaler ADM elimina los archivos de compilación y otros archivos extraídos para garantizar que las instancias de NetScaler tengan suficiente espacio en disco para el siguiente intento de actualización.

Programar la actualización de instancias NetScaler

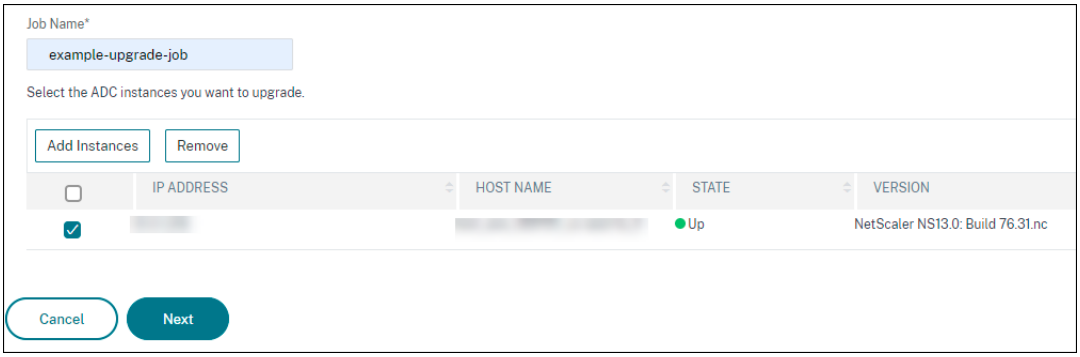
1. Vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.



2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar NetScaler (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.



3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar instancias ADC que quiera actualizar.
    - Para actualizar un par HA, especifique la dirección IP de un nodo principal o secundario. Sin embargo, se recomienda utilizar la instancia principal para actualizar el par HA.
    - Para actualizar un clúster, especifique la dirección IP del clúster.



5. Haga clic en **Siguiente** para seleccionar la imagen. Seleccione una de las siguientes opciones de la lista **Imagen de software**:

   - **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
   - **Dispositivo**: Seleccione el archivo de actualización de instancias en el explorador de archivos de NetScaler ADM. La GUI de NetScaler ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.
     - **Omitir la carga de imágenes a ADC si la imagen seleccionada ya está disponible**: Seleccione esta opción si la imagen ya está presente en la instancia de NetScaler.
     - **Limpiar la imagen de software de NetScaler en una actualización correcta**: Seleccione esta opción para borrar la imagen cargada en la instancia de ADC después de la actualización de la instancia.

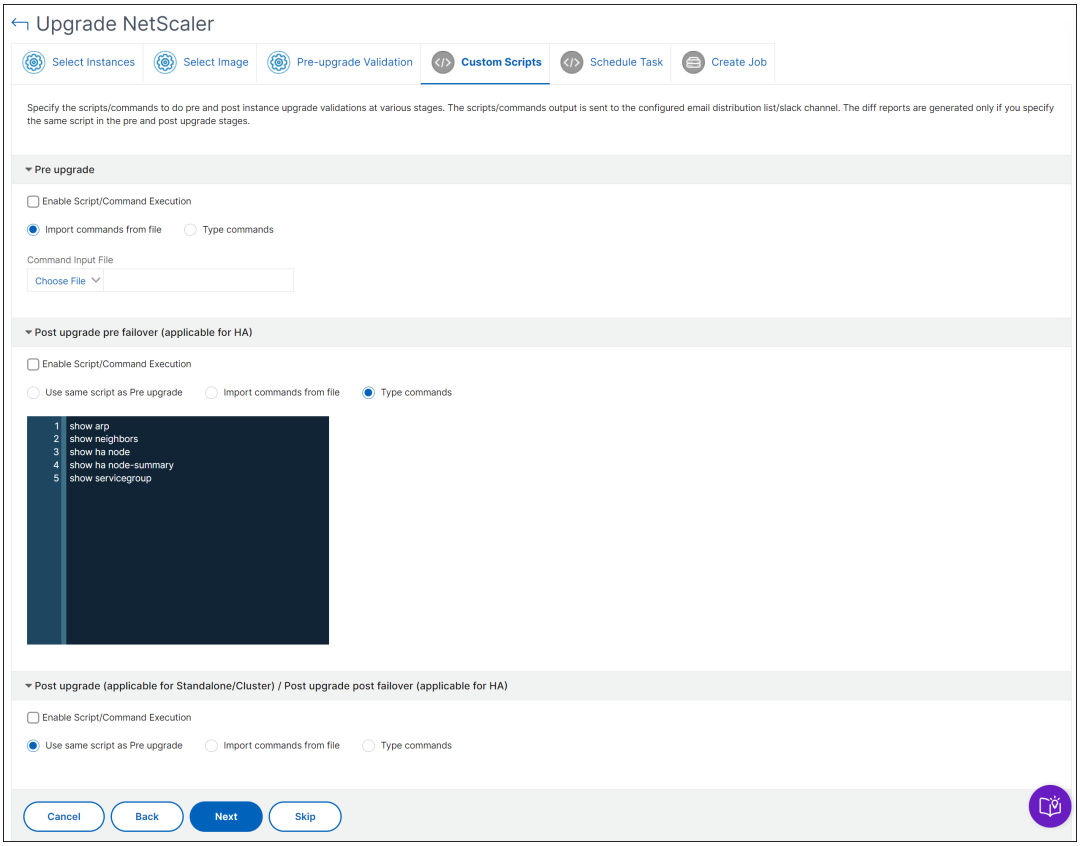
6. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   La ficha **Validación previa a la actualización** muestra las instancias fallidas. Quite las instancias con errores y haga clic en **Siguiente**.

   > **Importante**
   >
   > Si especifica la dirección IP del clúster, NetScaler ADM realiza la validación previa a la actualización solo en la instancia especificada, no en los otros nodos del clúster.

7. Opcional, en **Scripts personalizados**, especifique los scripts que se ejecutarán antes y después de una actualización de instancia. Utilice una de las siguientes formas de ejecutar los comandos:

   - **Importar comandos del archivo**: Seleccione el archivo de entrada de comandos del equipo local.
   - **Escribir comandos**: Introduzca comandos directamente en la GUI.



Puede usar scripts personalizados para comprobar los cambios antes y después de una actualización de la instancia. Por ejemplo:

- La versión de la instancia antes y después de la actualización.
- El estado de las interfaces, los nodos de alta disponibilidad, los servidores virtuales y los servicios antes y después de la actualización.
- Las estadísticas de los servicios y servidores virtuales.
- Las rutas dinámicas.

8. Haga clic en **Siguiente**. En **Planificar tarea**, seleccione una de las siguientes opciones:

   - **Actualizar ahora**: El trabajo de actualización se ejecuta inmediatamente.
   - **Programar más tarde**: Seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.

     Si quiere actualizar un par ADC HA en dos etapas, seleccione **Realizar actualización de dos etapas para nodos en HA**.

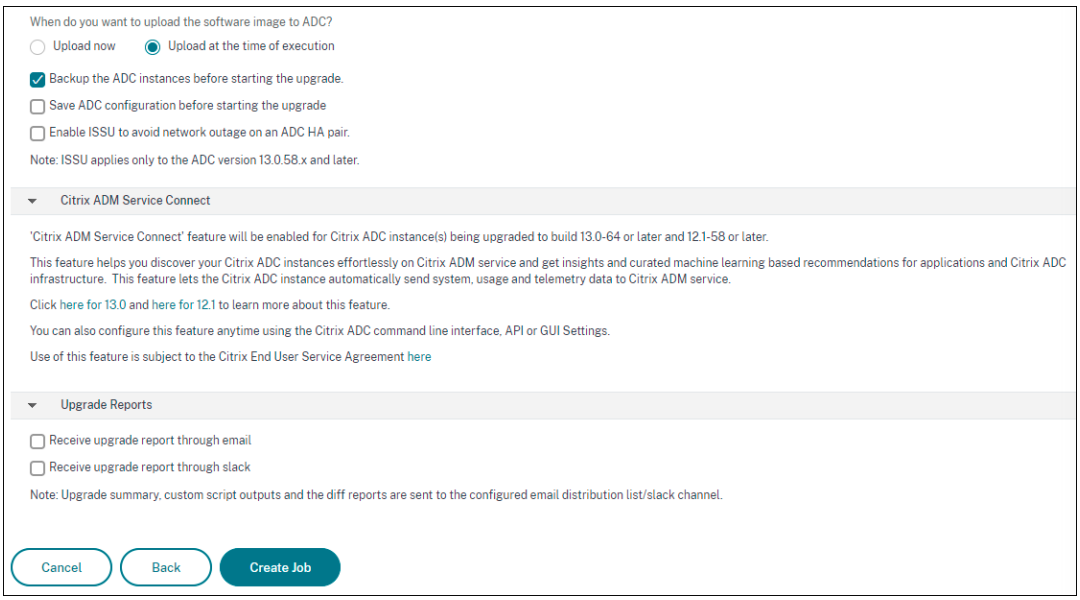
     Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia en el par HA.

9. Haga clic en **Siguiente**. En **Crear trabajo**, especifique los siguientes detalles:

    a) Especifique cuándo quiere cargar la imagen en una instancia:

    - **Cargar ahora**: Seleccione esta opción para cargar la imagen inmediatamente. Sin embargo, el trabajo de actualización se ejecuta a la hora programada.
    - **Cargar en el momento de la ejecución**: Seleccione esta opción para cargar la imagen en el momento de la ejecución del trabajo de actualización.
    - **Realice una copia de seguridad de las instancias ADC antes de iniciar la actualización.** - Crea una copia de seguridad de las instancias ADC seleccionadas.
    - **Guardar la configuración de ADC antes de iniciar la actualización**: Guarda los trabajos de configuración que están configurados en la instancia antes de la actualización.
    - **Habilite ISSU para evitar cortes de red en el par ADC HA**: ISSU garantiza la actualización de tiempo de inactividad cero en un par de alta disponibilidad de ADC. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par ADC HA sin tiempo de inactividad. Especifique el tiempo de espera de migración ISSU en minutos.

- **NetScaler ADM Service Connect**: Si piensa actualizar a las **compilaciones 13.0-64 o posterior** y **12.1-58 o posterior**, NetScaler ADM Service Connect se habilita automáticamente. Para obtener más información, consulte Incorporación con poco toque de instancias NetScaler mediante NetScaler ADM service connect.
- **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.
- **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.



10. Haga clic en **Crear trabajo**.

Programar la actualización de instancias de NetScaler SDX

1. Vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Actualizar NetScaler SDX** y haga clic en **Continuar**.
3. En la página **Actualizar NetScaler SDX**, en la ficha **Selección de instancias** :
   a) Agregue un **nombre de tarea**.
   b) En la lista **Imagen de software**, seleccione **Local** (su máquina local) o **Dispositivo** (el archivo de compilación debe estar presente en el dispositivo virtual NetScaler ADM).

      Comienza el proceso de carga.
   c) Agregue las instancias de NetScaler SDX en las que quiere ejecutar el proceso de actualización.
   d) Haga clic en **Siguiente**.
4. En la ficha **Programar tarea**, seleccione **Ahora** en la lista de **modos de ejecución** para actualizar una instancia de NetScaler SDX ahora y haga clic en **Finalizar**.
5. Para actualizar una instancia de NetScaler 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 y hacer clic en **Finalizar**.
6. También puede habilitar las notificaciones de correo electrónico y de demora para recibir el informe de ejecución de la instancia de NetScaler SDX de actualización. Haz clic en la casilla

Recibir informe de ejecución por correo electrónico y en la casilla **Recibir informe de ejecución a través de Slack** para activar las notificaciones.

Para obtener más información sobre cómo configurar la lista de distribución de correo electrónico y el canal de Slack, consulte el **paso 8** de Programar la actualización de instancias de NetScaler.

Programar la actualización de las instancias BLX de NetScaler

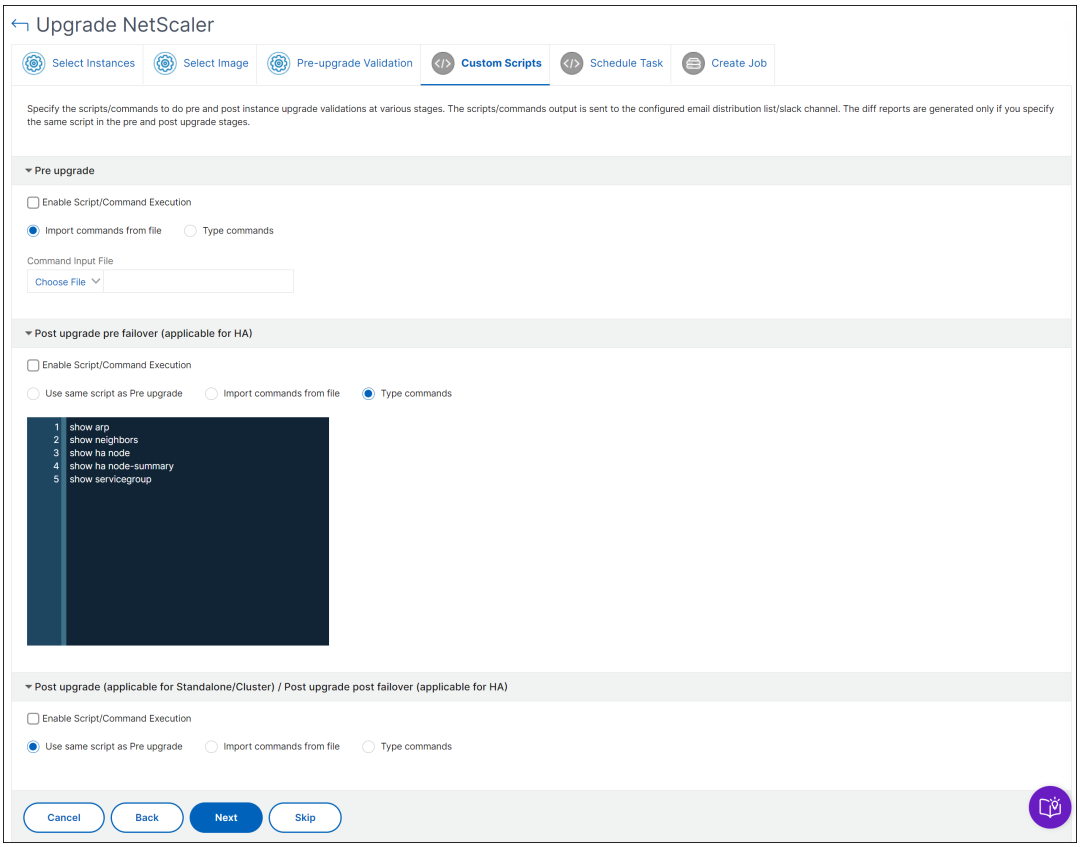
1. Vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar NetScaler BLX** y haga clic en **Continuar**.
3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar las instancias BLX que quiera actualizar.
   - Para actualizar un par HA, especifique la dirección IP de un nodo principal o secundario. Sin embargo, se recomienda utilizar la instancia principal para actualizar el par HA.
   - Para actualizar un clúster, especifique la dirección IP del clúster.
5. Haga clic en **Siguiente** para seleccionar la imagen. Seleccione una de las siguientes opciones en la lista **Imagen de software**:
   - **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
   - **Dispositivo**: Seleccione el archivo de actualización de instancias en el explorador de archivos de NetScaler ADM. La GUI de NetScaler ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.
     - **Omitir la carga de imágenes a ADC si la imagen seleccionada ya está disponible**: Seleccione esta opción si la imagen ya está presente en la instancia de NetScaler.
     - **Limpiar la imagen de software de NetScaler en una actualización correcta**: Seleccione esta opción para borrar la imagen cargada en la instancia de ADC después de la actualización de la instancia.
6. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   La ficha **Validación previa a la actualización** muestra las instancias fallidas. Quite las instancias con errores y haga clic en **Siguiente**.

> **Importante**
>
> Si especifica la dirección IP del clúster, NetScaler ADM realiza la validación previa a la actualización solo en la instancia especificada, no en los otros nodos del clúster.

7. Opcional, en **Scripts personalizados**, especifique los scripts que se ejecutarán antes y después de una actualización de instancia. Utilice una de las siguientes formas de ejecutar los comandos:

   - **Importar comandos del archivo**: Seleccione el archivo de entrada de comandos del equipo local.
   - **Escribir comandos**: Introduzca comandos directamente en la GUI.



   Puede usar scripts personalizados para comprobar los cambios antes y después de una actualización de la instancia. Por ejemplo:

   - La versión de la instancia antes y después de la actualización.
   - El estado de las interfaces, los nodos de alta disponibilidad, los servidores virtuales y los servicios antes y después de la actualización.
   - Las estadísticas de los servicios y servidores virtuales.
   - Las rutas dinámicas.

8. Haga clic en **Siguiente**. En **Planificar tarea**, seleccione una de las siguientes opciones:

    - **Actualizar ahora**: El trabajo de actualización se ejecuta inmediatamente.
    - **Programar más tarde**: Seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.

      Si quiere actualizar un par de HA en dos etapas, seleccione **Realizar actualización de dos etapas para los nodos de HA**.

      Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia en el par HA.

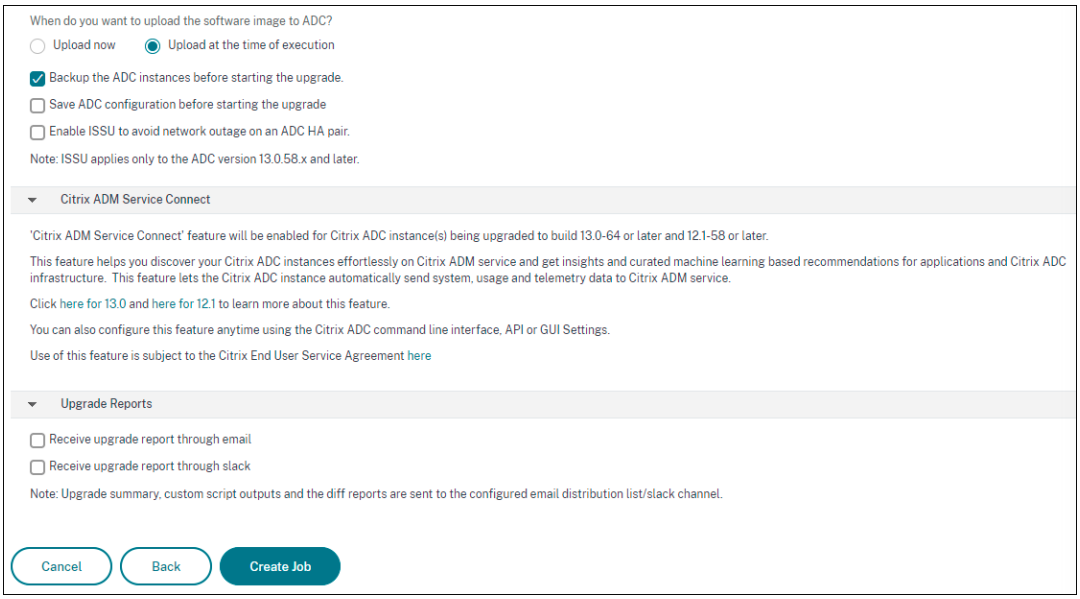
9. Haga clic en **Siguiente**. En **Crear trabajo**, especifique los siguientes detalles:

    a) Especifique cuándo quiere cargar la imagen en una instancia:

        - **Cargar ahora**: Seleccione esta opción para cargar la imagen inmediatamente. Sin embargo, el trabajo de actualización se ejecuta a la hora programada.
        - **Cargar en el momento de la ejecución**: Seleccione esta opción para cargar la imagen en el momento de la ejecución del trabajo de actualización.
        - **Copia de seguridad de las instancias de ADC antes de iniciar la actualización**: Crea una copia de seguridad de las instancias de ADC seleccionadas.
        - **Guardar la configuración de ADC antes de iniciar la actualización**: Guarda los trabajos de configuración que están configurados en la instancia antes de la actualización.
        - **Habilite ISSU para evitar cortes de red en el par ADC HA**: ISSU garantiza la actualización de tiempo de inactividad cero en un par de alta disponibilidad de ADC. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par ADC HA sin tiempo de inactividad. Especifique el tiempo de espera de migración ISSU en minutos.

    - **NetScaler ADM Service Connect**: Si piensa actualizar a las **compilaciones 13.0-64 o posterior** y **12.1-58 o posterior**, NetScaler ADM Service Connect se habilita automáticamente. Para obtener más información, consulte Incorporación con poco toque de instancias NetScaler mediante NetScaler ADM service connect.
    - **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.

- **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.



10. Haga clic en **Crear trabajo**.

Programar la actualización del grupo de Autoscale

Realice los siguientes pasos para actualizar todas las instancias de los servicios en la nube que forman parte del grupo de Autoscale:

1. Vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Actualizar grupo de Autoscale** y haga clic en **Continuar**.
3. En la ficha **Configuración de actualización** :
   a) Seleccione el **grupo de escalabilidad automática** que quiere actualizar.
   b) En **Imagen**, seleccione la versión de NetScaler. Esta imagen es la versión existente de las instancias de NetScaler en el grupo de Autoscale.
   c) En **NetScaler Image**, examine el archivo de versión de NetScaler al que quiere actualizar.

      Si marca **Actualización de gracia**, la tarea de actualización espera hasta que caduque el período de conexión de drenaje especificado.
   d) Haga clic en **Siguiente**.
4. En la ficha **Programar tarea**:
   a) Seleccione una de las siguientes opciones de la lista Modo de ejecución:

- **Ahora:**Para iniciar las instancias de NetScaler, actualice inmediatamente.
- **Más tarde:** Para iniciar la actualización de las instancias de NetScaler más adelante.

b) Si selecciona la opción **Más tarde**, seleccione Fecha de ejecución y Hora de inicio cuando quiera iniciar la tarea de actualización.

También puede habilitar las notificaciones de correo electrónico y de demora para recibir el informe de ejecución del grupo de escalado automático de actualización. Haz clic en la casilla **Recibir informe de ejecución por correo** electrónico y en la casilla **Recibir informe de ejecución a través de Slack** para activar las notificaciones.

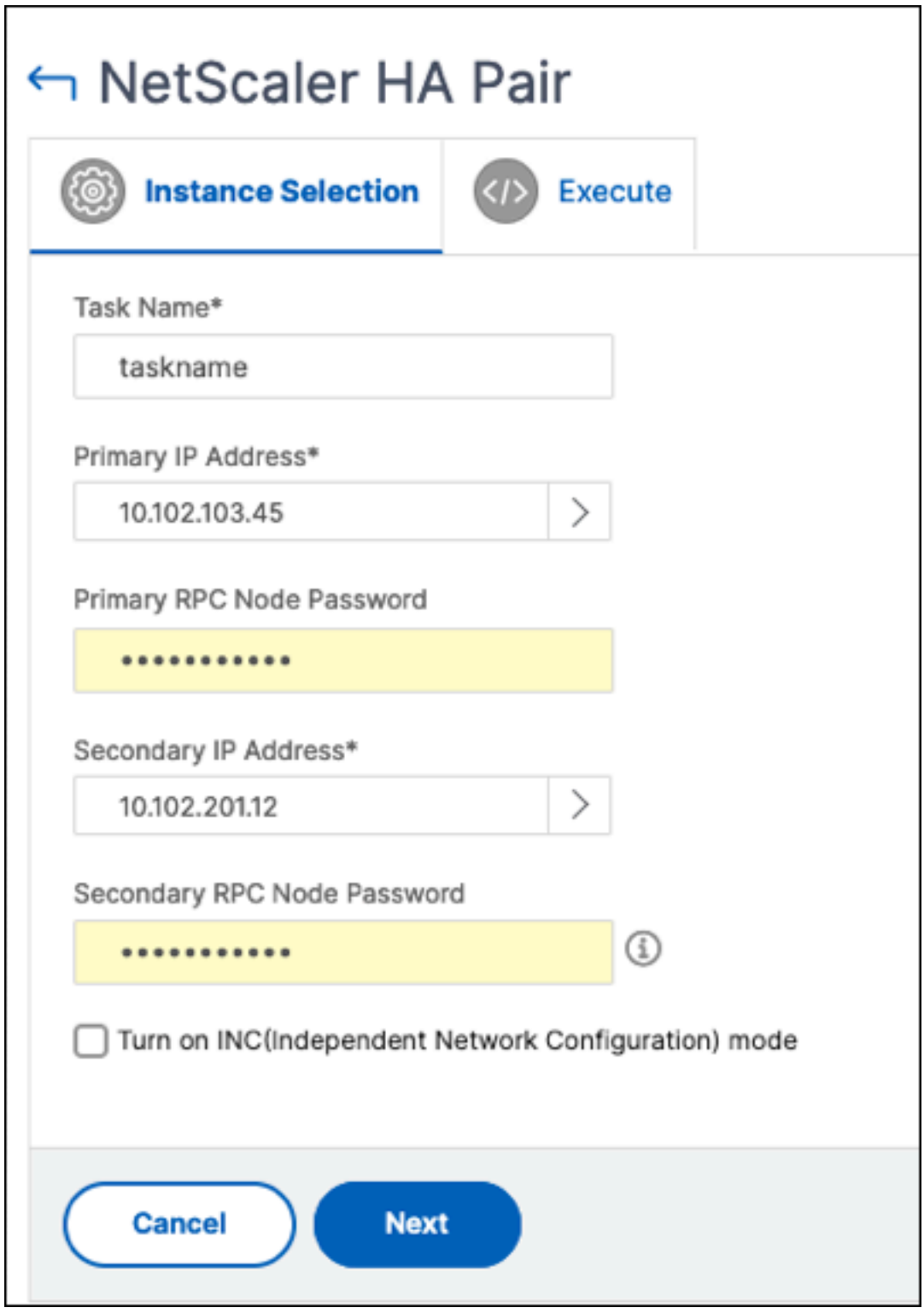
5. Haga clic en **Finalizar**.

Programar la configuración del par de instancias de NetScaler de HA

1. Vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Configurar Par HA de Instancias de NetScaler** y haga clic en **Continuar**.
3. En la página **NetScaler HA Pair**, en la ficha **Selección de instancias** :
   a) Agregue un **nombre de tarea**.
   b) Seleccione la dirección IP principal. Haga clic en **Aceptar**.
   c) Introduzca la contraseña del nodo RPC principal.
   d) Seleccione la dirección IP secundaria. Haga clic en **Aceptar**.

> **Nota:**
>
> Los campos de contraseña del nodo RPC están disponibles en la versión 14.1 y posteriores de NetScaler.

   e) Introduzca la contraseña del nodo RPC secundario.
   f) Haga clic para **activar el modo Activar INC (Configuración de red independiente)** si tiene las instancias de par HA en dos subredes.
   g) Haga clic en **Siguiente**.



4. En la ficha **Programar tarea**, seleccione **Ahora** en la lista **Modo de ejecución** para actualizar una instancia de NetScaler ahora y haga clic en **Finalizar**.
5. Para actualizar un par de NetScaler HA más tarde, 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 y hacer clic en **Finalizar**.

6. También puede habilitar las notificaciones de correo electrónico y de demora para recibir el informe de ejecución de la creación del par ADC HA. Haz clic en la casilla **Recibir informe de ejecución por correo** electrónico y en la casilla **Recibir informe de ejecución a través de Slack** para activar las notificaciones.

   Para obtener más información sobre cómo configurar la lista de distribución de correo electrónico y el canal de Slack, consulte el **paso 8** de Programar la actualización de instancias de NetScaler.

Programar la conversión del par de instancias de HA en clúster

1. Vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Convertir par de instancias HA en clúster de 2 nodos** y haga clic en **Continuar**.
3. En la página **Migrar NetScaler HA a Cluster**, en la ficha **Selección de Instancia**, agregue un **nombre de tarea**. Especifique la dirección IP principal, la dirección IP secundaria, el ID del nodo principal, el ID del nodo secundario, la dirección IP del clúster, el ID del clúster y el plano posterior y, a continuación, haga clic en **Siguiente**.
4. En la ficha **Programar tarea**, seleccione **Ahora** en la lista **Modo de ejecución** para actualizar una instancia de NetScaler ahora y haga clic en **Finalizar**.
5. Para actualizar más tarde, 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 par HA de NetScaler y hacer clic en **Finalizar**.
6. También puede habilitar las notificaciones de correo electrónico y de demora para recibir el informe de ejecución de la actualización de una instancia de NetScaler SDX. Haz clic en la casilla **Recibir informe de ejecución por correo** electrónico y en la casilla **Recibir informe de ejecución a través de Slack** para activar las notificaciones.

   Para obtener más información sobre cómo configurar la lista de distribución de correo electrónico y el canal de Slack, consulte el **paso 8** de Programar la actualización de las instancias de NetScaler.

Usar trabajos para actualizar instancias de NetScaler

January 30, 2024

Puede utilizar NetScaler Application Delivery Management (ADM) para actualizar una o más instancias de NetScaler. Debe conocer el marco de licencias y los tipos de licencias antes de actualizar una instancia.

Cuando actualice la instancia de NetScaler creando un trabajo de mantenimiento, realice la comprobación previa a la validación de las instancias que quiere actualizar.

1. **Comprobar si hay personalizaciones**: Haga una copia de seguridad de sus personalizaciones y elimínelas de las instancias. Puede volver a aplicar las personalizaciones de copia de seguridad después de la actualización de la instancia.
2. **Comprobar el uso del disco**: Si la carpeta `/var` tiene menos de 6 GB de espacio y la carpeta `/flash` tiene menos de 200 MB de espacio, limpie el espacio en disco. Compruebe las siguientes rutas de carpetas para limpiar el espacio en disco:
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **Compruebe si hay problemas de hardware de disco**: Resuelva los problemas de hardware si los hay.

Puede actualizar un par de NetScaler HA en dos etapas:

1. Cree un trabajo de actualización y ejecute en uno de los nodos inmediatamente o programe más tarde.
2. Programe el trabajo de actualización para que se ejecute en el nodo restante más adelante. Asegúrese de programar este trabajo después de la actualización del nodo inicial.

Cuando actualice un par de NetScaler HA, tenga en cuenta lo siguiente:

- El nodo secundario se actualiza primero.
- La sincronización y propagación de los nodos se desactivan hasta que ambos nodos se actualizan correctamente.
- Tras la actualización correcta del par HA, aparece un mensaje de error en el historial de ejecución. Este mensaje aparece si los nodos del par HA están en compilaciones o versiones diferentes. Este mensaje indica que la sincronización entre el nodo primario y secundario está inhabilitada.

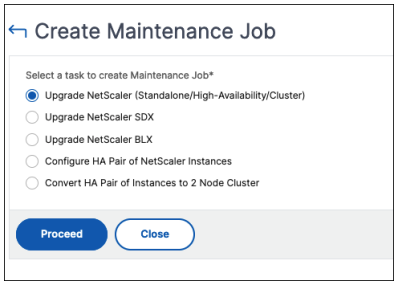
Al actualizar un clúster de NetScaler, el ADM realiza la validación previa a la actualización únicamente en la instancia especificada. Antes de realizar la actualización, compruebe y resuelva los problemas de personalización, uso del disco y hardware en los nodos del clúster.

Cree un trabajo de mantenimiento de actualizaciones para actualizar las instancias de NetScaler

> **Nota**
>
> No se admite la actualización de NetScaler de una versión superior a una versión inferior. Por ejemplo, si su instancia de NetScaler es 13.0 82.x, no puede degradar la instancia de NetScaler a 13.0 79.x ni a ninguna otra versión anterior.

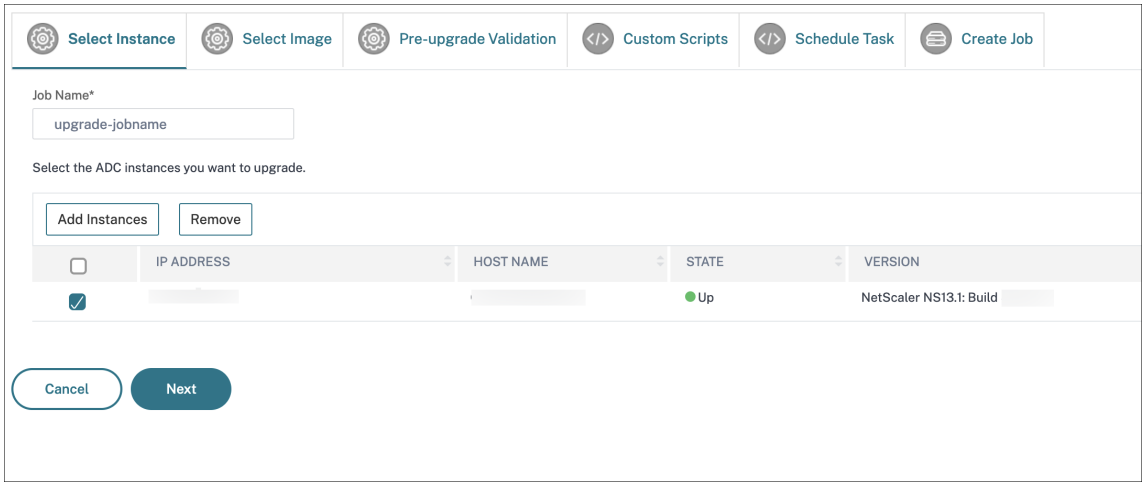
1. En NetScaler ADM, vaya a **Infraestructura > Trabajos de actualización**. Haga clic en el botón **Crear trabajo**.

2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar NetScaler (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.



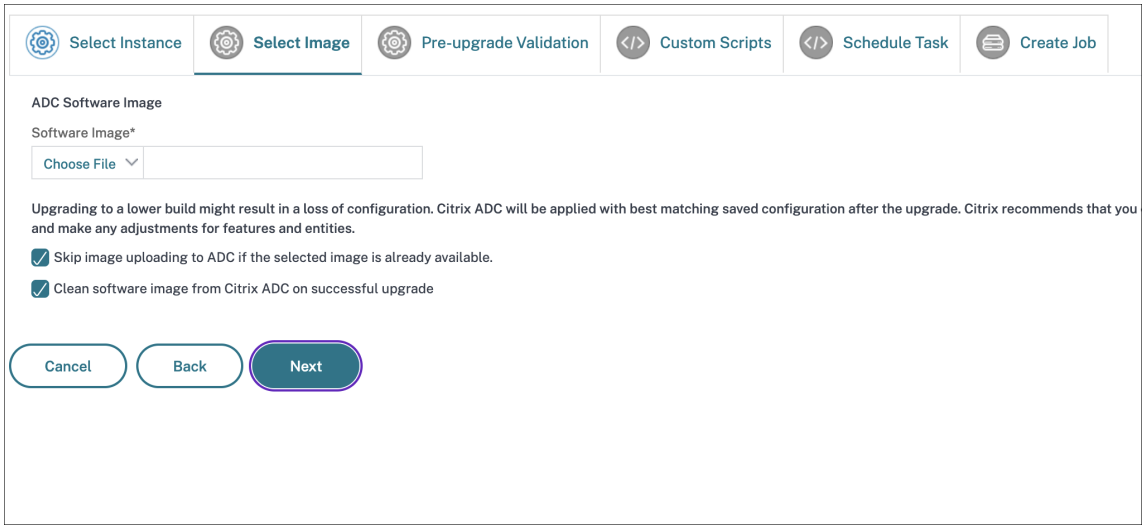
3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar las instancias de NetScaler que desee actualizar.
    - Para actualizar un par de alta disponibilidad de NetScaler, seleccione las direcciones IP del par de alta disponibilidad (indicadas por los superíndices “S”y “P”).

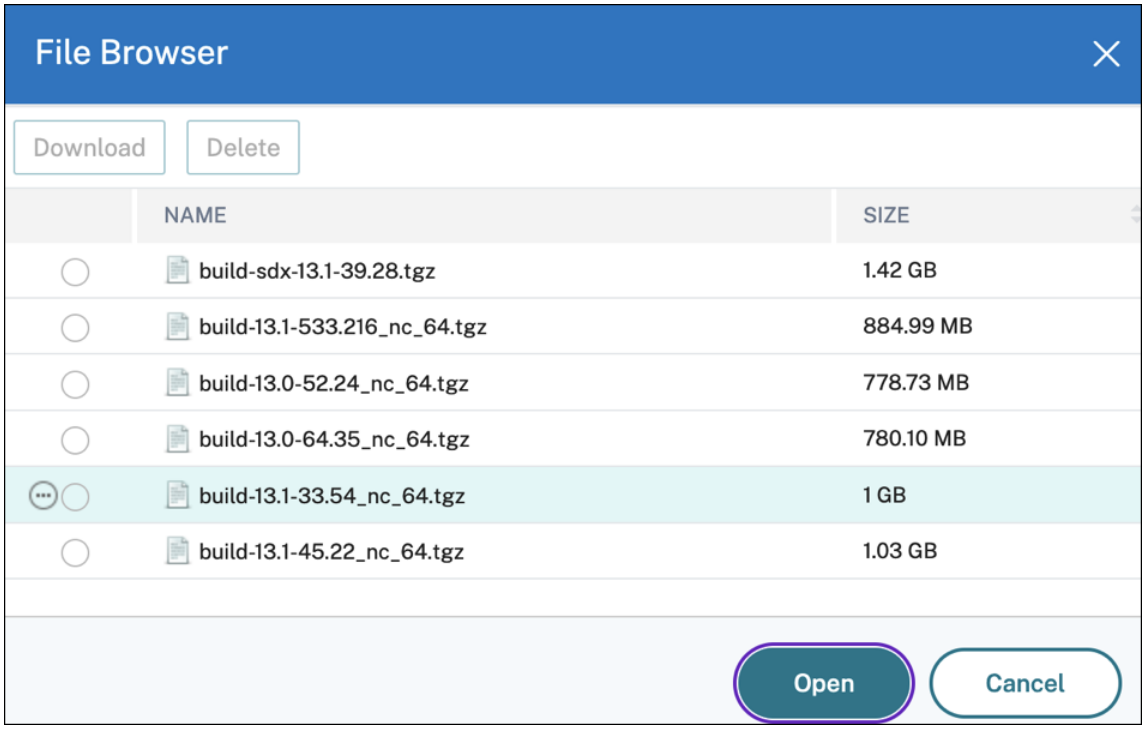
- Para actualizar un clúster, seleccione la dirección IP del clúster (indicada con el superíndice “C”).



5. En la ficha **Seleccionar imagen**, seleccione una imagen de NetScaler de la unidad local o de las imágenes de compilación.

   - **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
   - **Dispositivo**: Seleccione el archivo de actualización de instancias en un explorador de archivos ADM de NetScaler. La GUI de NetScaler ADM muestra los archivos de instancia que están presentes en `/var/mps/ns_images`.





- **Omitir la carga de imágenes a NetScaler si la imagen seleccionada ya está** disponible: esta opción comprueba si la imagen seleccionada está disponible en NetScaler. El trabajo de actualización omite la carga de una imagen nueva y usa la imagen disponible en NetScaler.
- **Limpiar la imagen del software de NetScaler si la actualización se realiza correctamente**: esta opción borra la imagen cargada en la instancia de NetScaler tras la actualización de la instancia.

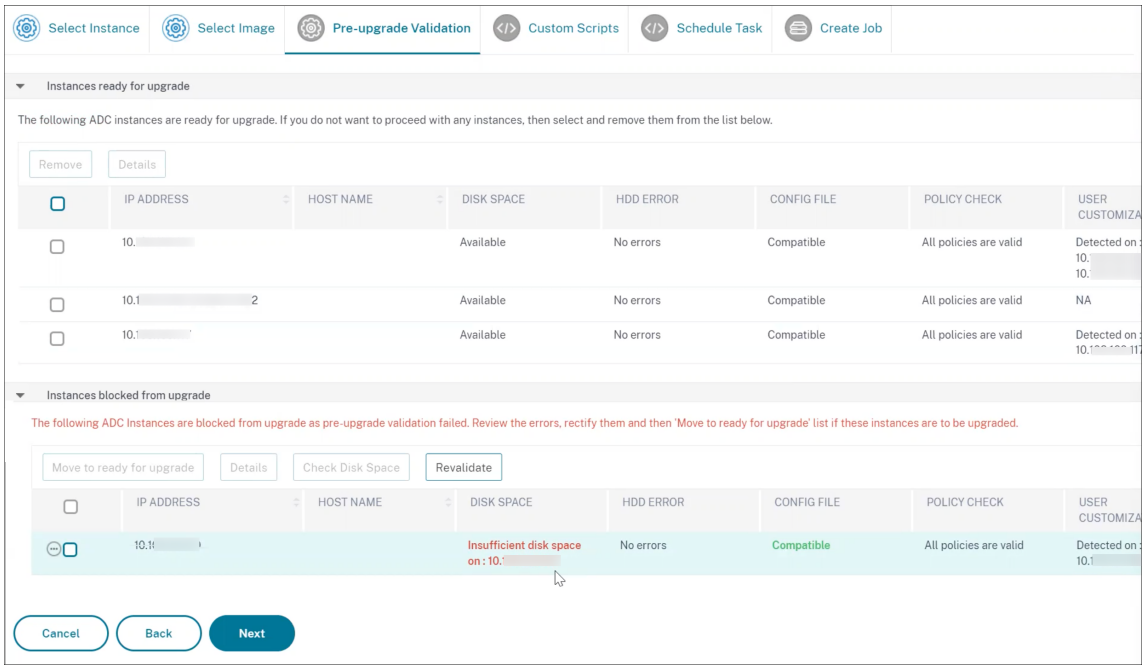
Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

> **Nota:**
>
> - Las imágenes de NetScaler descargadas se almacenan en el agente NetScaler ADM y están presentes en `/var/mps/adcimages`. Estas imágenes almacenadas en caché se pueden usar para varias actualizaciones de NetScaler, lo que elimina la necesidad de descargar una imagen cada vez que se realiza una actualización.
> - NetScaler ADM borra las imágenes de NetScaler almacenadas en caché cada tres días en función de la última hora de modificación de las imágenes. Solo los dos archivos de imagen más recientes se almacenan en caché en el agente ADM de NetScaler a la vez.

6. La ficha **Validación previa a la actualización** muestra las siguientes secciones:

- **Instancias listas para la actualización**. Puede continuar con la actualización de estas instancias.
- **Instancias bloqueadas para la actualización**. Se ha bloqueado la actualización de estas instancias de NetScaler debido a errores de validación previos a la actualización.

  Puede revisar, corregir los errores y, a continuación, hacer clic en **Mover a listo para la actualización** para actualizarlos. Si no tiene suficiente espacio en disco en una instancia, puede comprobar y limpiar el espacio en disco. Consulte Limpiar espacio en disco de NetScaler.



- **Verificación de directivas**: si NetScaler ADM encuentra directivas clásicas no compatibles, puede eliminarlas para crear un trabajo de actualización.

> **Importante**
>
> Si especifica la dirección IP del clúster, ADM realiza la validación previa de la actualización solo en la instancia especificada, no en los otros nodos del clúster.

7. Opcional, en **Scripts personalizados**, especifique los scripts que se ejecutarán antes y después de una actualización de instancia. Utilice una de las siguientes formas de ejecutar los comandos:

   Los scripts personalizados se utilizan para comprobar los cambios antes y después de la actualización de una instancia de NetScaler. Por ejemplo:

   - La versión de la instancia antes y después de la actualización.

- El estado de las interfaces, los nodos de alta disponibilidad, los servidores virtuales y los servicios antes y después de la actualización.
- Las estadísticas de los servicios y servidores virtuales.
- Las rutas dinámicas.

Una actualización de instancia tiene varias etapas. Ahora puede especificar estos scripts para ejecutarse en las siguientes etapas:

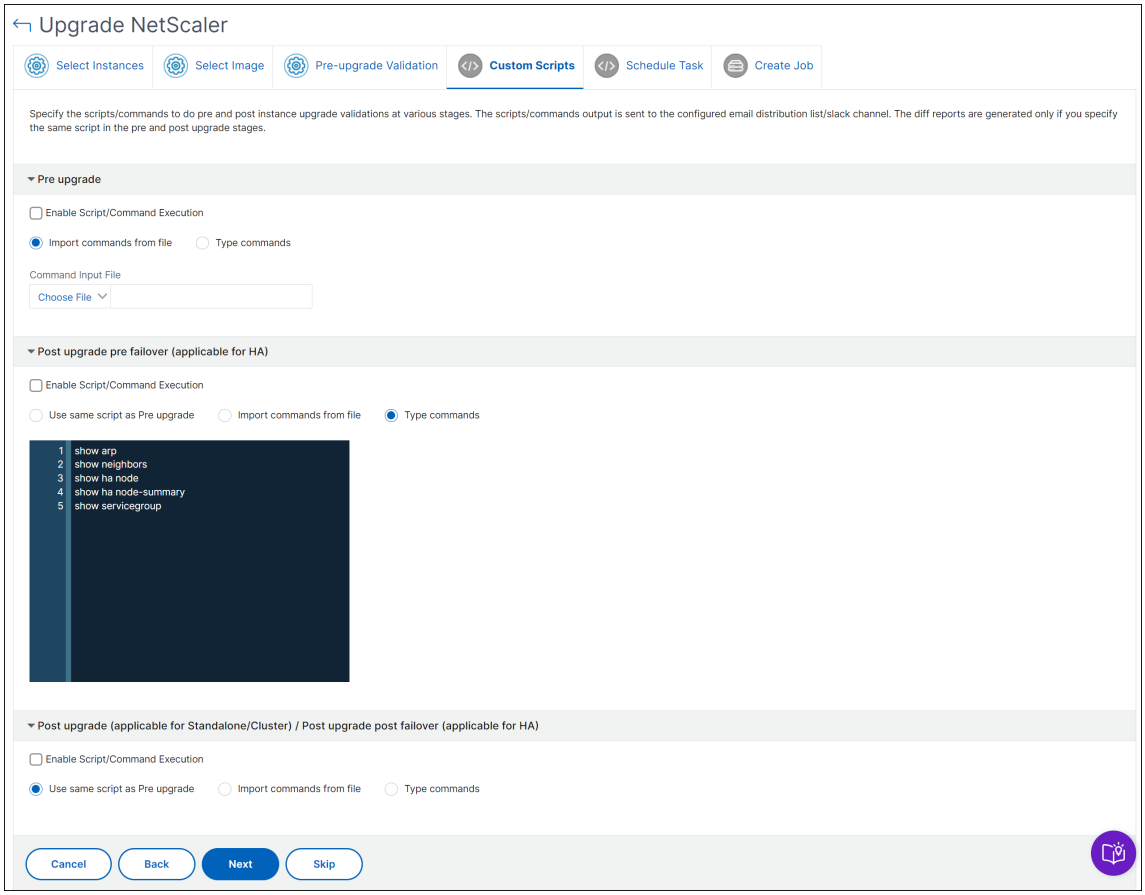
- **Preactualización**: el script especificado se ejecuta antes de actualizar una instancia.
- **Después de la actualización previa a la conmutación por error (aplicable para HA)**: esta etapa solo se aplica a la implementación de alta disponibilidad. El script especificado se ejecuta después de actualizar los nodos, pero antes de su conmutación por error.
- **Post upgrade (aplicable para independiente)/Conmutación por error posterior a la actualización (aplicable para HA)**: el script especificado se ejecuta después de actualizar una instancia en la implementación independiente. En la implementación de alta disponibilidad, el script se ejecuta después de actualizar los nodos y su conmutación por error.

> **Nota**
>
> Asegúrese de habilitar la ejecución del script en las etapas requeridas. De lo contrario, los scripts especificados no se ejecutan.

Puede importar un archivo de script o escribir comandos directamente en la GUI de ADM.

- **Importar comandos de archivo**: seleccione el archivo de entrada de comandos desde el equipo local.
- **Comandos de tipo**: introduzca los comandos directamente en la GUI.

En las etapas posteriores a la actualización, puede utilizar el mismo script especificado en la etapa previa a la actualización.



8. En **Planificar tarea**, seleccione una de las siguientes opciones:

   - **Actualizar ahora**: El trabajo de actualización se ejecuta inmediatamente.
   - **Programar más tarde**: Seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.

     Si quiere actualizar un par de NetScaler HA en dos etapas, **seleccione Realizar una actualización en dos etapas para los nodos**de HA.

     Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia en el par HA.

9. En **Crear trabajo**, especifique los siguientes detalles:

   a) Seleccione una de las siguientes opciones de la lista **Imagen de software**:

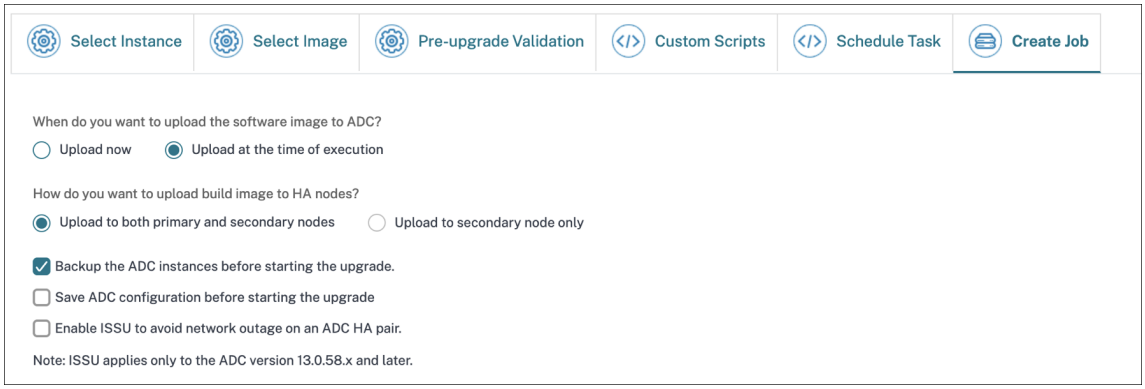
      - **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
      - **Dispositivo**: Seleccione el archivo de actualización de instancias en un explorador de archivos ADM. La GUI de ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.

b) Especifique cuándo quiere cargar la imagen en una instancia:

- **Cargar ahora**: Seleccione esta opción para cargar la imagen inmediatamente. Sin embargo, el trabajo de actualización se ejecuta a la hora programada.
- **Cargar en el momento de la ejecución**: Seleccione esta opción para cargar la imagen en el momento de la ejecución del trabajo de actualización.

Para un par de alta disponibilidad, puede especificar los nodos en los que quiere cargar la imagen:

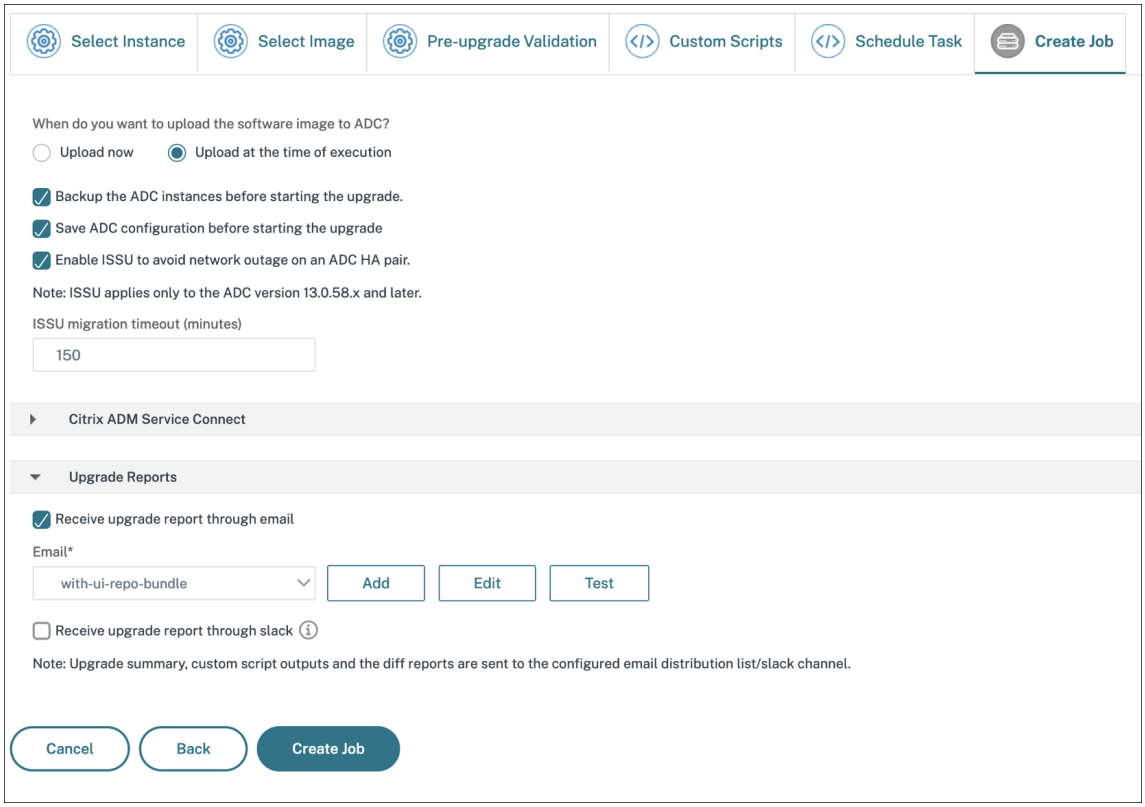
- **Carga a los nodos principal y secundario**: sube el archivo de imagen de compilación a los nodos principal y secundario.
- **Subir solo al nodo secundario**: suba el archivo de imagen de compilación únicamente al nodo secundario. Tras actualizar el nodo secundario, se produce una conmutación por error y el archivo de imagen de compilación se carga en el nuevo nodo secundario, que anteriormente era el nodo principal.



Para obtener más información sobre los casos de programación disponibles para el par de alta disponibilidad, consulte Programar trabajos de actualización para el par de alta disponibilidad.

- **Limpiar la imagen del software de NetScaler si la actualización se realiza correctamente**: seleccione esta opción para borrar la imagen cargada en la instancia de NetScaler tras la actualización de la instancia.
- **Realice una copia de seguridad de las instancias de NetScaler antes de iniciar la actualización.** - Crea una copia de seguridad de las instancias de NetScaler seleccionadas.
- **Mantenga el estado principal y secundario de los nodos de alta disponibilidad después de la actualización**: seleccione esta opción si quiere que el trabajo de actualización inicie una conmutación por error después de la actualización de cada nodo. De esta manera, el trabajo de actualización mantiene el estado primario y secundario de los nodos.
- **Guardar la configuración de NetScaler antes de iniciar la actualización: guarda la configuración** de NetScaler en ejecución antes de actualizar las instancias de NetScaler.

- **Habilite ISSU para evitar la interrupción de la red en un par NetScaler HA: ISSU garantiza la actualización sin tiempo de inactividad en un par de alta disponibilidad de NetScaler**. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par de NetScaler HA sin tiempo de inactividad. Especifique el tiempo de espera de migración ISSU en minutos.
- **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.
- **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.

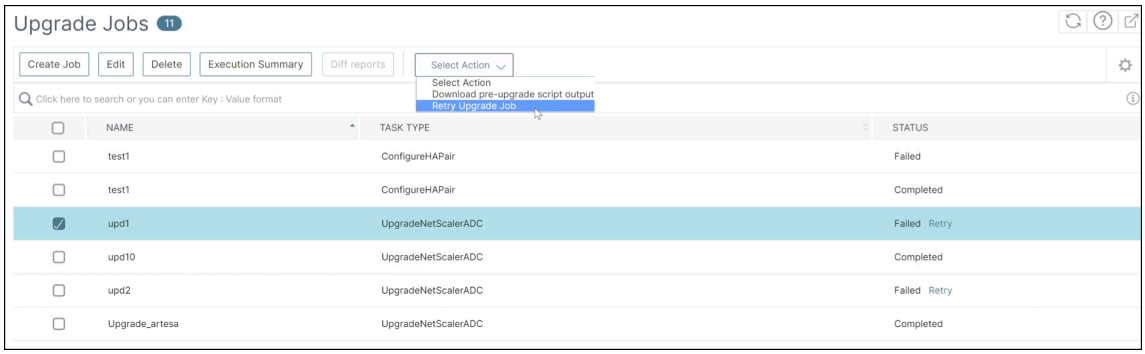


10. Haga clic en **Crear trabajo**.

El trabajo de actualización aparece en **Infraestructura > Trabajos de actualización**. Cuando modifique un trabajo existente, puede cambiar a cualquier ficha si los campos obligatorios ya están rellenados. Por ejemplo, si se encuentra en la ficha **Seleccionar configuración**, puede cambiar a la ficha **Vista previa del trabajo**.

Reintentar trabajos de actualización fallidos

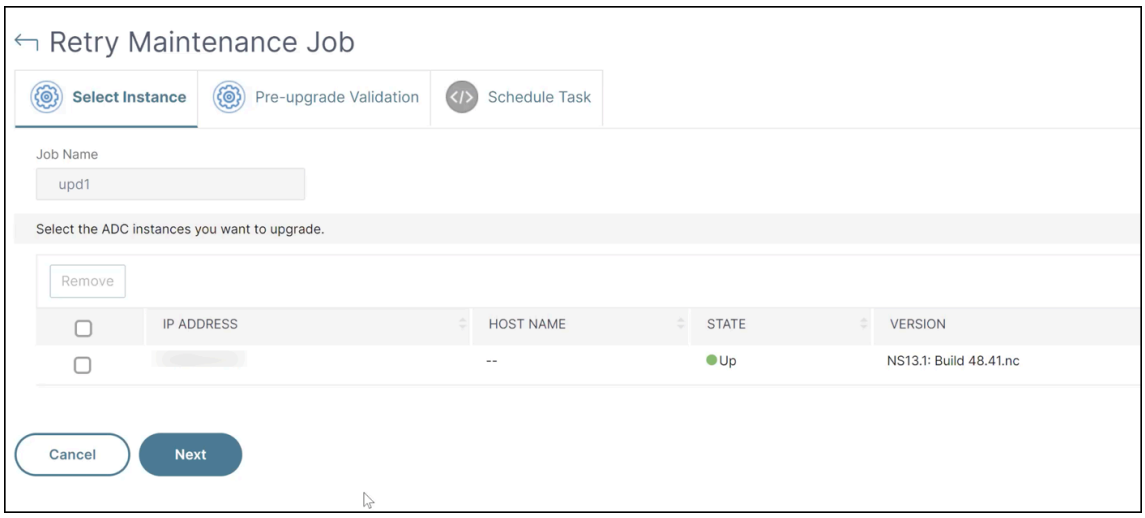
1. En **Infraestructura > Trabajos de actualización**, seleccione el trabajo de actualización fallido y haga clic en **Reintentar**. Como alternativa, también puede ir a **Seleccionar acción > Reintentar un trabajo de actualización** para volver a intentar un trabajo fallido.



2. En **Seleccionar instancia**, especifique los siguientes detalles:

   - **Nombre del trabajo**: Introduzca un nombre para la actualización.
   - Seleccione en la lista las instancias de NetScaler que quiera actualizar. Para eliminar una instancia, haga clic en **Eliminar**.

   Haga clic en **Siguiente** para iniciar el proceso de validación.

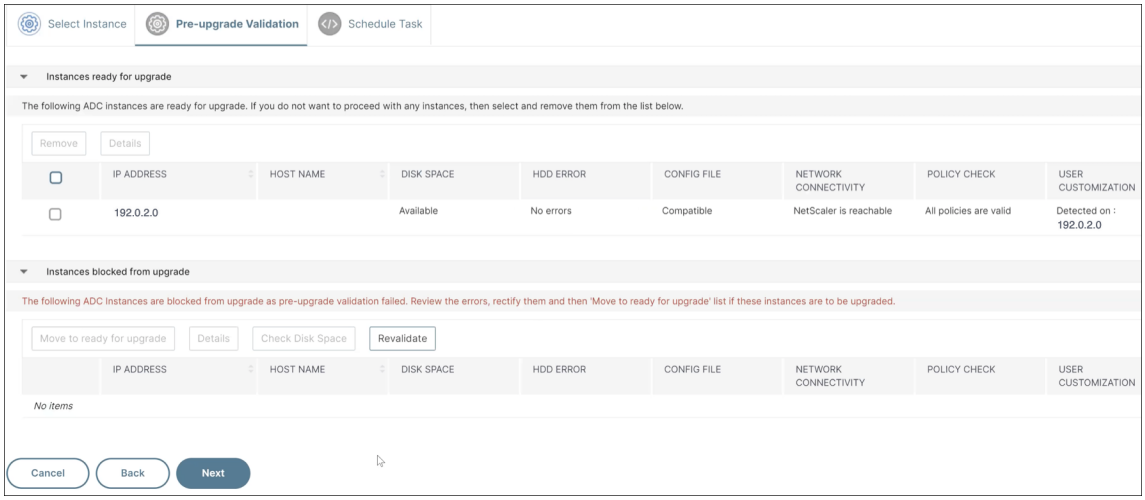


3. La ficha **Validación previa a la actualización** muestra las siguientes secciones:

   - **Instancias listas para la actualización**. Puede continuar con la actualización de estas instancias.
   - **Instancias bloqueadas para la actualización**. Se ha bloqueado la actualización de estas instancias de NetScaler debido a errores de validación previos a la actualización.

Puede revisar, corregir los errores y, a continuación, hacer clic en **Mover a listo para la actualización** para actualizarlos. Si no tiene suficiente espacio en disco en una instancia, puede comprobar y limpiar el espacio en disco. Consulte Limpiar el espacio en disco de NetScaler.

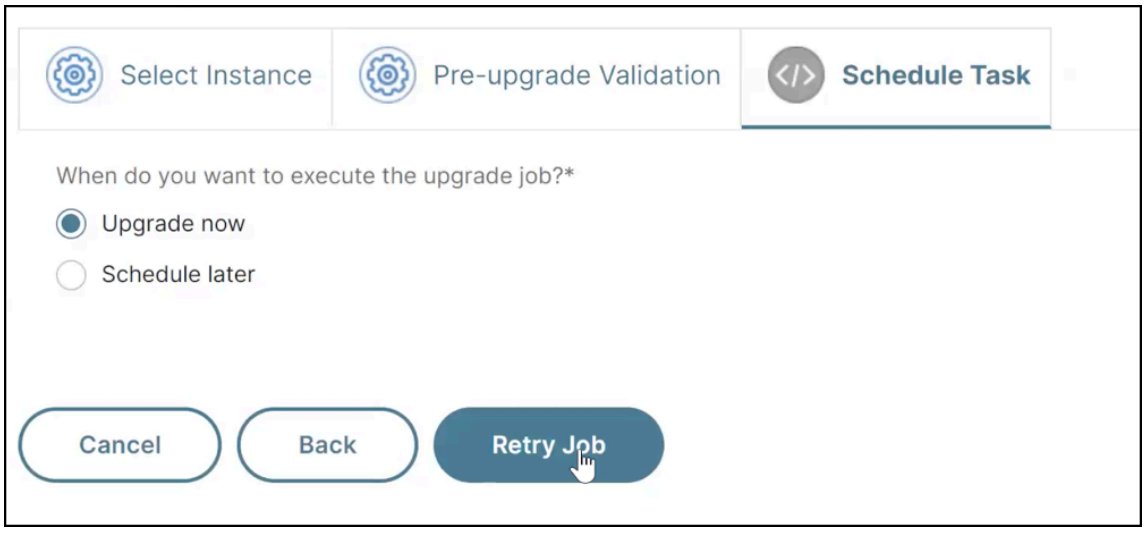
- **Verificación de directivas**: si NetScaler ADM encuentra directivas clásicas no compatibles, puede eliminarlas para crear un trabajo de actualización.



Haga clic en **Siguiente**.

4. En **Planificar tarea**, seleccione una de las siguientes opciones:

   - **Actualizar ahora**: el trabajo de actualización se ejecuta inmediatamente.
   - **Programar más tarde**: seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.



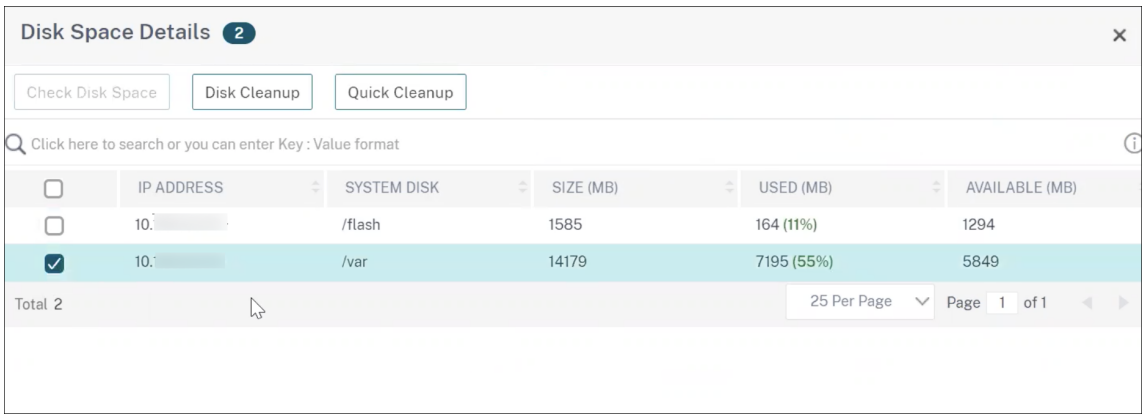
Haga clic en **Reintentar**.

Limpie el espacio en disco de NetScaler

Si se enfrenta al problema de falta de espacio en disco al actualizar una instancia de NetScaler, libere el espacio en disco de la propia GUI de NetScaler ADM.

1. En la ficha **Validación previa a la actualización**, la sección **Instancias bloqueadas para la actualización** muestra las instancias en las que no se pudo realizar la actualización por falta de espacio en disco. Seleccione la instancia que tiene problemas de espacio en disco.
2. Haga clic en **Comprobar espacio en disco**.

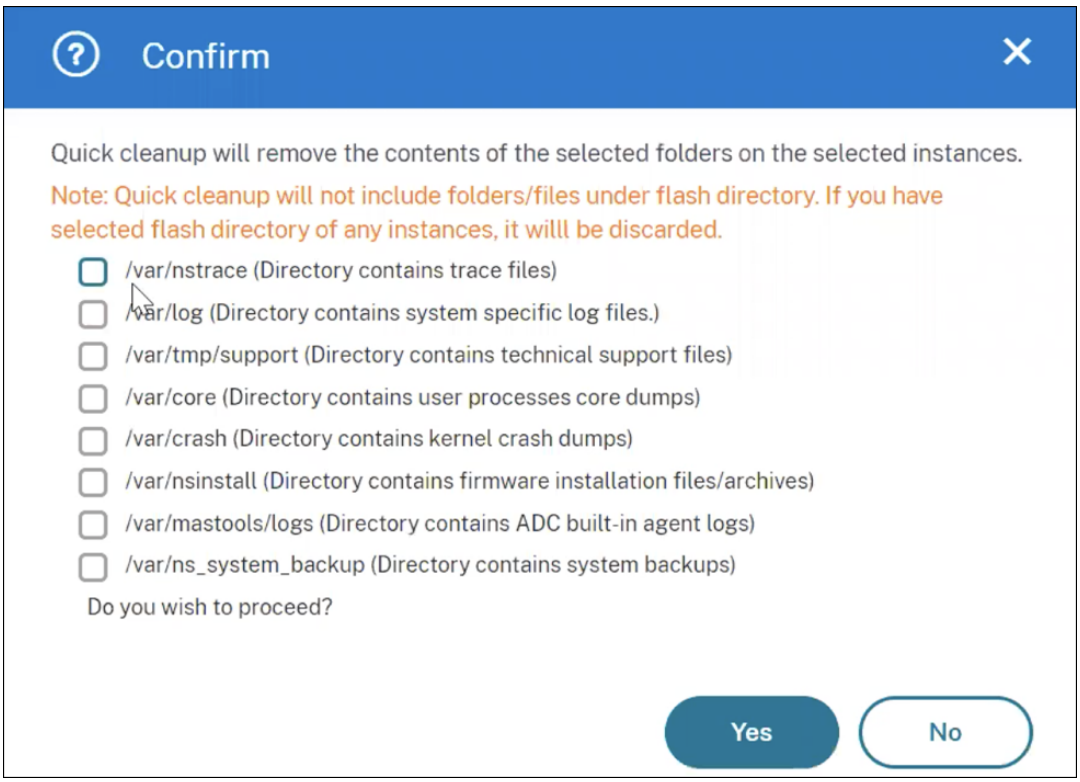
   Aparece el panel **Detalles del espacio en disco**. Este panel muestra las instancias, la memoria utilizada y la memoria disponible.



3. En el panel **Detalles del espacio en disco**, seleccione la instancia que deba limpiarse y realice una de las siguientes acciones:

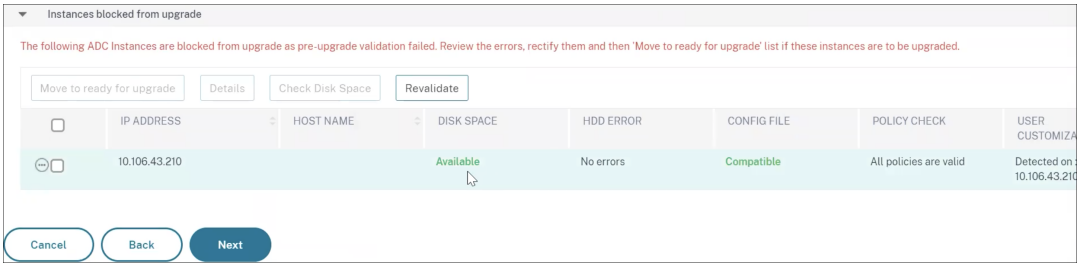
   a) **Liberador de espacio en disco**: Vaya hasta las carpetas o directorios necesarios y elimínelos para liberar espacio en disco.

   b) **Limpieza rápida**: Borre rápidamente el espacio en disco mediante la eliminación de varias carpetas. En el panel **Confirmar** que aparece, seleccione las carpetas que quiera eliminar y haga clic en **Sí**.



c) Después de liberar espacio en disco, puede comprobar si hay suficiente espacio en disco disponible para actualizar la instancia. En la sección **Instancias bloqueadas por la actualización**, haga clic en **Revalidar**.

En el ejemplo siguiente, hay espacio en disco disponible. Ahora puede hacer clic en **Mover a lista para la actualización para** actualizar la instancia o hacer clic en **Siguiente** para continuar con el siguiente paso.



Programar trabajos de actualización para un par de alta disponibilidad de NetScaler

La siguiente tabla muestra los diferentes casos de programación en la página **Programar tareas** y las opciones de actualización correspondientes disponibles en la página **Crear trabajo** :

¿Cuándo quiere ejecutar el trabajo de actualización?	¿Cuándo quiere cargar la imagen del software en NetScaler?	¿Cómo quiere cargar la imagen de compilación a los nodos HA?
Actualiza ahora	No aplicable	**Cargar a los nodos principal y secundario** (opción predeterminada)
Programe más tarde	**Cargar en el momento de la ejecución** (opción predeterminada)	**Cargar a los nodos principal y secundario** (opción predeterminada)
Programar más adelante (cuando esté seleccionada la opción **Realizar una actualización en dos etapas para los nodos de HA**)	**Cargar en el momento de la ejecución** (opción predeterminada)	**Cargar ahora** **Subir solo al nodo secundario** (opción predeterminada y única) **Cargar ahora**

Descargar un informe de diferencias combinado de un trabajo de actualización de NetScaler

Puede descargar un informe de diferencias de un trabajo de actualización de NetScaler si se especifican scripts personalizados. Un informe diff contiene las diferencias entre las salidas del script previo a la actualización y posterior a la actualización. Con este informe, puede determinar qué cambios se produjeron en la instancia de NetScaler después de la actualización.

> **Nota**
>
> El informe diff solo se genera si especifica el mismo script en las etapas anterior a la actualización y posterior a la actualización.

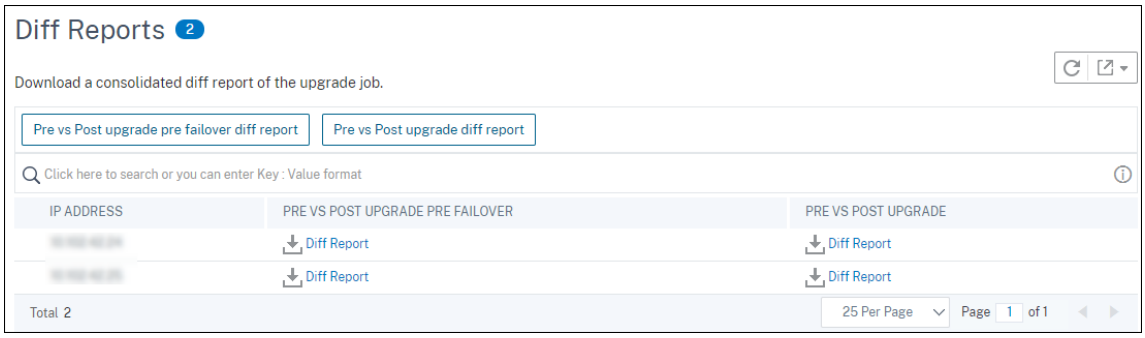
Para descargar un informe diff de un trabajo de actualización, haga lo siguiente:

1. Vaya a **Infraestructura > Trabajos de configuración > Trabajos de mantenimiento**.
2. Seleccione el trabajo de actualización para el que quiere descargar un informe de diferencias.
3. Haga clic en **Diff Reports**.

4. En **Informes de diferencias**, descargue un informe diff consolidado del trabajo de actualización seleccionado.

   En esta página, puede descargar cualquiera de los siguientes tipos de informes diff:

   - **Informe de diferencia de conmutación por error anterior a posterior a la actualización**
   - **Informe de diferencia anterior y posterior a la actualización**



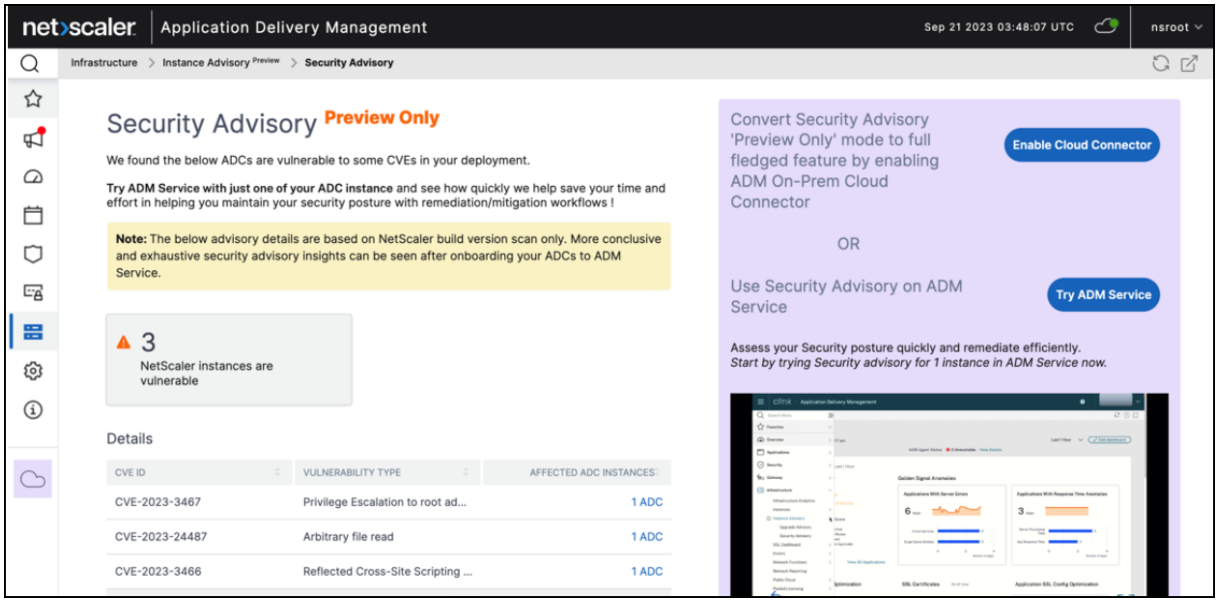
Asesoramiento de seguridad

January 30, 2024

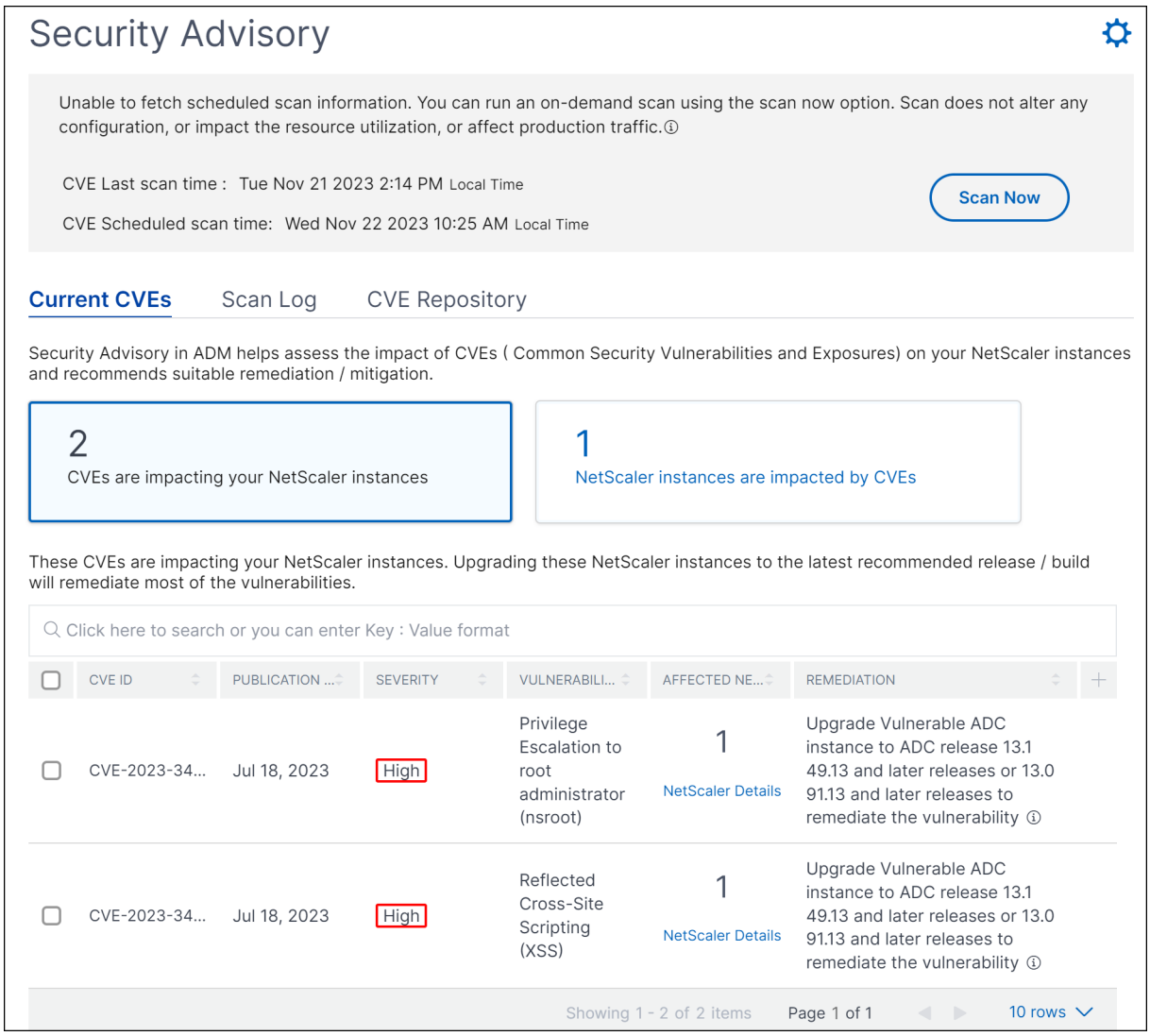
Una infraestructura segura, segura y resistente es la línea vital de cualquier organización. Las organizaciones deben realizar un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE) y evaluar el impacto de las CVE en su infraestructura. También deben comprender y planificar la remediación para resolver las vulnerabilidades. La función de asesoramiento de seguridad de NetScaler ADM le permite identificar los CVE que ponen en riesgo sus instancias de NetScaler y recomienda soluciones.

A partir de la versión 14.1 8.x, puede usar la versión completa del aviso de seguridad configurando **ADM On-Prem Cloud Connector** y habilitando el **aviso de seguridad**.

Si no ha configurado ADM On-Prem Cloud Connector, solo puede ver la versión preliminar de Security Advisory. Puede hacer clic en **Habilitar Cloud Connector** y completar la configuración para usar la versión completa del aviso de seguridad. Para obtener más información, consulte ADM On-Prem Cloud Connector.



Después de configurar ADM On-Prem Cloud Connector y habilitar el aviso de seguridad, puede ver la página de consejos de seguridad actualizada.



Como administrador, debe asegurarse de realizar un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE), evaluar el impacto de las CVE, comprender las soluciones y resolver las vulnerabilidades.

Funciones de asesoramiento de seguridad

Las siguientes funciones de asesoramiento de seguridad le ayudan a proteger su infraestructura:

Funciones	Descripción
Análisis del sistema	Analiza todas las instancias administradas de forma predeterminada una vez a la semana. NetScaler ADM decide la fecha y la hora de los escaneos del sistema y no puede cambiarlos.

Funciones	Descripción
Escaneo bajo demanda	Puede analizar manualmente las instancias cuando sea necesario. Si el tiempo transcurrido desde el último análisis del sistema es significativo, puede ejecutar un análisis bajo demanda para evaluar la situación de seguridad actual. O escanee después de aplicar una corrección para evaluar la postura revisada.
Análisis de impacto de CVE	Muestra los resultados de todas las CVE que afectan a su infraestructura y de todas las instancias de NetScaler que se ven afectadas, y sugiere soluciones. Utilice esta información para aplicar medidas correctivas a fin de corregir los riesgos de seguridad.
Registro de análisis	Almacena las copias de los últimos cinco escaneos. Puede descargar estos informes en formato CSV y PDF y analizarlos.
Repositorio CVE	Ofrece una vista detallada de todos los CVE relacionados con NetScaler que Citrix ha anunciado desde diciembre de 2019 y que podrían afectar a su infraestructura de NetScaler. Puede utilizar esta vista para comprender los CVE en el ámbito del asesoramiento de seguridad y para obtener más información sobre los CVE. Para obtener información sobre los CVE no compatibles, consulte los CVE no compatibles en el Aviso de seguridad.

Puntos que tener en cuenta

- Security Advisory no admite compilaciones de NetScaler que hayan llegado al final de su vida útil (EOL). Le recomendamos que actualice a las compilaciones o versiones compatibles con NetScaler.
- Instancias compatibles con la detección de CVE: Todas las instancias de NetScaler (SDX, MPX, VPX) y Gateway.
- CVE compatibles: todos los CVE posteriores a diciembre de 2019.

> **Nota:**
>
> El aviso de seguridad de NetScaler ADM no admite la detección y la corrección de las vulnerabilidades que afectan al complemento de NetScaler Gateway para Windows. Para obtener información sobre los CVE no compatibles, consulte los CVE no compatibles en el Aviso de seguridad.

- El aviso de seguridad de NetScaler ADM no tiene en cuenta ningún tipo de configuración incorrecta de la función al identificar la vulnerabilidad.
- El aviso de seguridad de NetScaler ADM solo permite identificar y corregir los CVE. No permite la identificación y la solución de los problemas de seguridad que se destacan en el artículo sobre seguridad.
- Alcance de las versiones de NetScaler y Gateway: La función se limita a las compilaciones principales. El aviso de seguridad no incluye ninguna versión especial en su alcance.
  - La partición de administración no admite el asesoramiento de seguridad.
- Los siguientes tipos de escaneo están disponibles para los CVE:
  - **Análisis de versiones**: este análisis necesita NetScaler ADM para comparar la versión de una instancia de NetScaler con las versiones y compilaciones en las que está disponible la corrección. Esta comparación de versiones ayuda al aviso de seguridad de NetScaler ADM a identificar si NetScaler es vulnerable a la CVE. Por ejemplo, si un CVE está fijo en una versión y compilación xx.yy de NetScaler, el aviso de seguridad considera vulnerables todas las instancias de NetScaler en compilaciones inferiores a xx.yy. El análisis de versiones se admite actualmente en el asesoramiento de seguridad.
  - **Análisis de configuración**: Este análisis necesita que NetScaler ADM coincida con un patrón específico del análisis de CVE con el archivo de configuración de NetScaler (nsconf). Si el patrón de configuración específico está presente en el archivo ns.conf de NetScaler, la instancia se considera vulnerable para ese CVE. Este análisis se utiliza normalmente con el análisis de versiones.
    El análisis de configuración se admite actualmente en el asesoramiento de seguridad.
  - **Análisis personalizado**: Este análisis necesita que NetScaler ADM se conecte con la instancia de NetScaler gestionada, le envíe un script y lo ejecute. La salida del script ayuda a NetScaler ADM a identificar si NetScaler es vulnerable al CVE. Los ejemplos incluyen el resultado específico de un comando shell, el resultado específico de un comando de CLI, ciertos registros y la existencia o el contenido de ciertos directorios o archivos. El aviso de seguridad también usa escaneos personalizados para encontrar coincidencias de varios patrones de configuración, si el escaneo de configuración no puede ayudar con lo mismo. En el caso de los CVE que requieren escaneos personalizados, el script se ejecuta cada vez

que se ejecuta el análisis programado o bajo demanda. Obtenga más información sobre los datos recopilados y las opciones para escaneos personalizados específicos en la documentación de asesoramiento de seguridad de ese CVE.

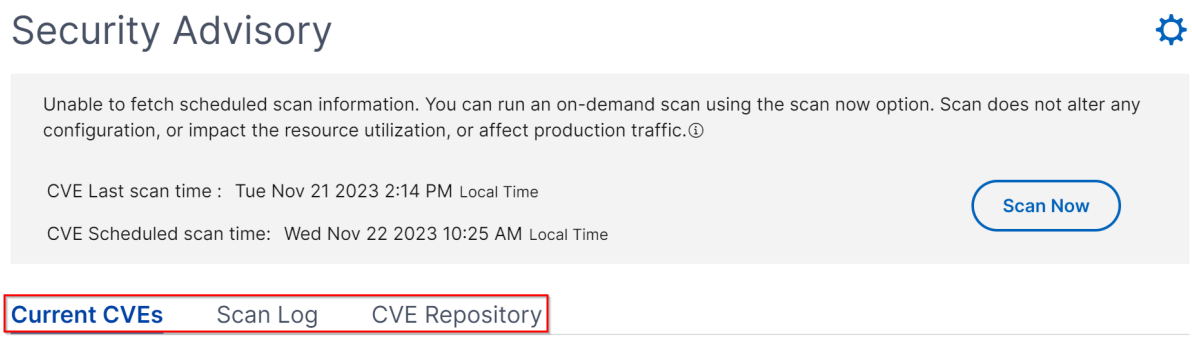
- Los escaneos no afectan al tráfico de producción en NetScaler y no alteran ninguna configuración de NetScaler en NetScaler.
- El aviso de seguridad de NetScaler ADM no admite la mitigación de CVE. Si ha aplicado una mitigación (solución temporal) a la instancia de NetScaler, ADM seguirá identificando el NetScaler como un NetScaler vulnerable hasta que haya completado la corrección.
- Para las instancias FIPS, no se admite el escaneo CVE.

Cómo utilizar el panel de asesoría de seguridad

Para acceder al panel **de asesoramiento de seguridad**, desde la GUI de NetScaler ADM, vaya a **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**.

El tablero incluye tres fichas:

- CVE actuales
- Registro de análisis
- Repositorio CVE



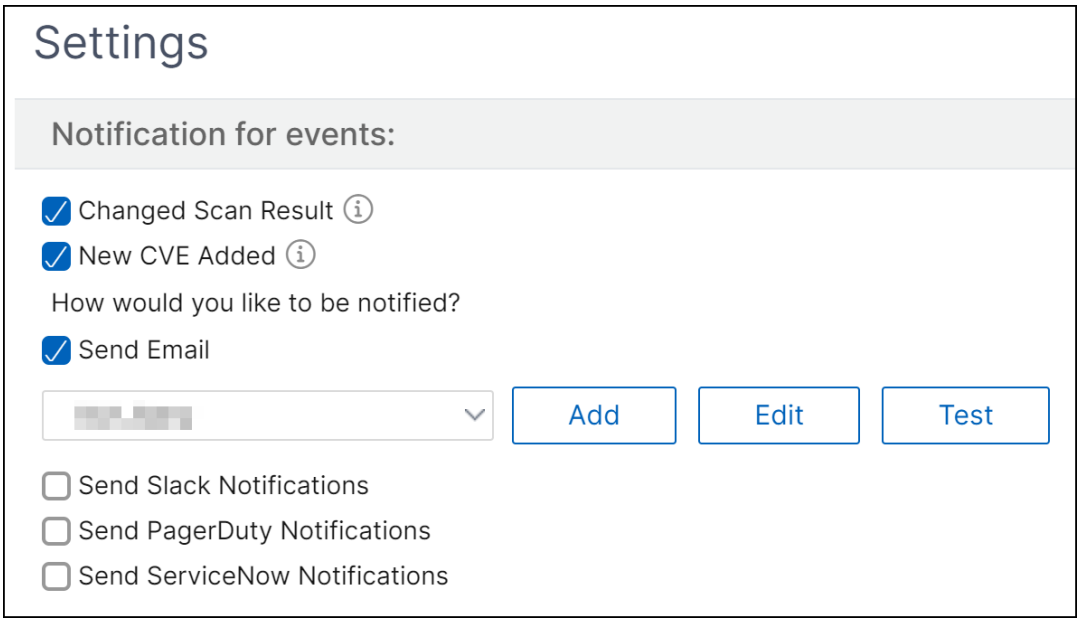
> **Importante:**
>
> En la GUI o en el informe del **asesor de seguridad**, es posible que no aparezcan todas las CVE y es posible que solo vea un CVE. Como solución alternativa, haga clic en **Analizar ahora** para ejecutar un análisis bajo demanda. Una vez finalizado el análisis, todas las CVE del ámbito (aproximadamente 15) aparecen en la interfaz de usuario o informe.

En la esquina superior derecha del panel de control se encuentra el icono de configuración, que le permite:

- Activa y desactiva las notificaciones.

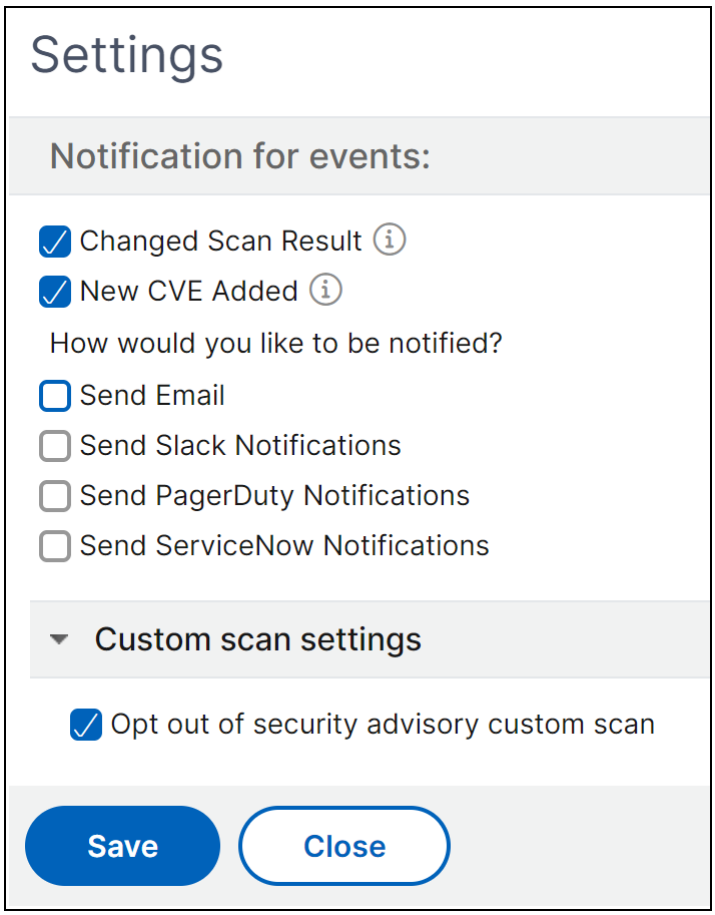
  Puede recibir las siguientes notificaciones sobre el impacto de las CVE.

  - Notificaciones por correo electrónico, Slack, PagerDuty y ServiceNow sobre los cambios en los resultados del escaneo de CVE y los nuevos CVE que se agreguen al repositorio de CVE.
  - Notificación en la nube para los cambios en los resultados del escaneo de impacto de CVE.



- Configurar los ajustes de escaneo personalizados

  Puede hacer clic en la lista **Configuración de digitalización personalizada** para ver la casilla de verificación de la configuración adicional. Tiene la opción de seleccionar la casilla de verificación y excluirse de estos escaneos personalizados de CVE. El impacto de las CVE que necesitan un análisis personalizado no se evaluará para sus instancias de NetScaler en el aviso de seguridad.



CVE actuales

Esta ficha muestra el número de CVE que afectan a sus instancias y también las instancias que se ven afectadas por los CVE. Las fichas no son secuenciales, y como administrador, puede cambiar entre estas fichas dependiendo de su caso de uso.

La tabla que muestra la cantidad de CVEs que afectan a las instancias de NetScaler contiene los siguientes detalles.

ID de CVE: el ID del CVE que afecta a las instancias.

Fecha de publicación: la fecha en que se publicó el boletín de seguridad de ese CVE.

Puntuación de gravedad: el tipo de gravedad (alta/media/crítica) y la puntuación. Para ver la puntuación, pase el cursor sobre el tipo de gravedad.

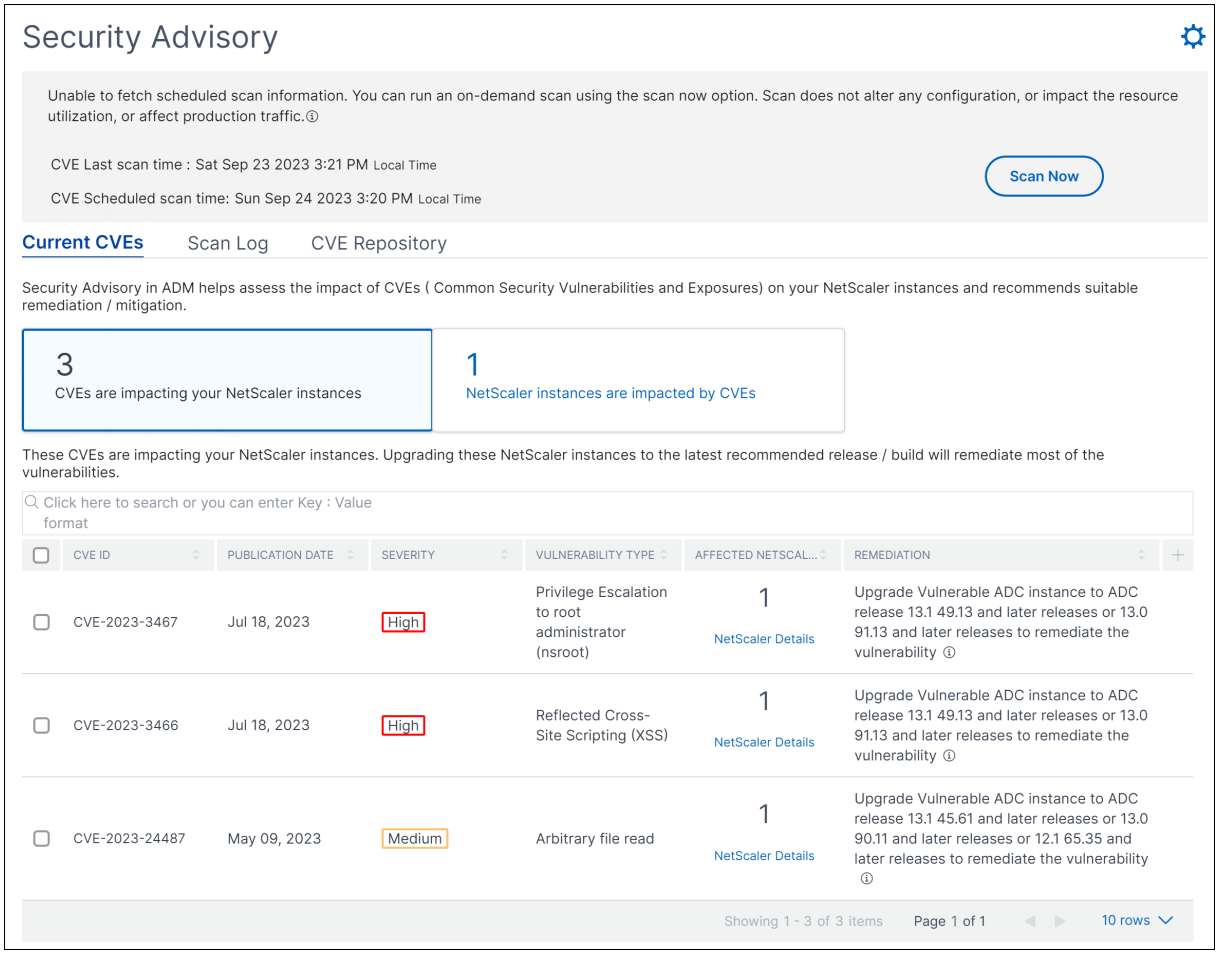
Tipo de vulnerabilidad: el tipo de vulnerabilidad de este CVE.

Instancias de NetScaler afectadas: El recuento de instancias al que afecta el ID de CVE. Al pasar el ratón por encima, aparece la lista de instancias de NetScaler.

Corrección: las soluciones disponibles, que consisten en actualizar la instancia (normalmente) o aplicar paquetes de configuración.

La misma instancia puede verse afectada por múltiples CVE. Esta tabla le ayuda a ver cuántas instancias están afectando a un CVE determinado o a varios CVE seleccionados. Para comprobar la dirección IP de la instancia afectada, coloque el cursor sobre los detalles de NetScaler en la sección **Instancias de NetScaler afectadas**. Para comprobar los detalles de la instancia afectada, haga clic en **Ver instancias afectadas** en la parte inferior de la tabla.
También puede agregar o quitar columnas de la tabla haciendo clic en el signo más.

En esta pantalla, el número de CVE que afectan a sus instancias es de 3 CVE y las instancias que se ven afectadas por estos CVE son una.

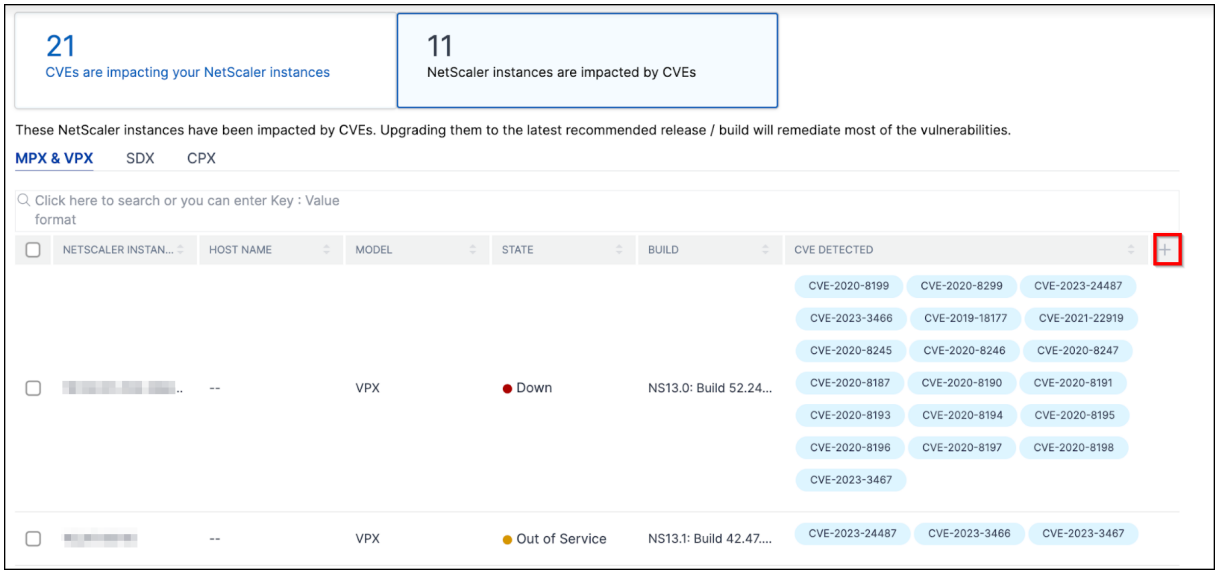


La ficha **<number of>Las instancias de NetScaler se ven afectadas por los CVE** muestra todas las instancias de NetScaler ADM de NetScaler afectadas. La tabla muestra los siguientes detalles:

- Dirección IP de NetScaler
- Nombre de host
- Número de modelo de NetScaler
- Estado de NetScaler

- Versión y compilación del software
- Lista de CVEs que afectan al NetScaler.

Puede agregar o eliminar cualquiera de estas columnas según sus necesidades haciendo clic en el signo +.



Para corregir el problema de vulnerabilidad, seleccione la instancia de NetScaler y aplique la corrección recomendada. La mayoría de los CVE necesitan una actualización como solución, mientras que otros necesitan una actualización y un paso adicional como solución.

- Para obtener información sobre la solución del CVE-2020-8300, consulte Solucionar vulnerabilidades para el CVE-2020-8300.
- Para CVE-2021-22927 y CVE-2021-22920, consulte Solucionar vulnerabilidades de CVE-2021-22927 y CVE-2021-22920.
- Para CVE CVE-2021-22956, consulte Identificar y corregir vulnerabilidades para CVE-2021-22956
- Para CVE CVE-2022-27509, consulte Solucionar vulnerabilidades para CVE-2022-27509

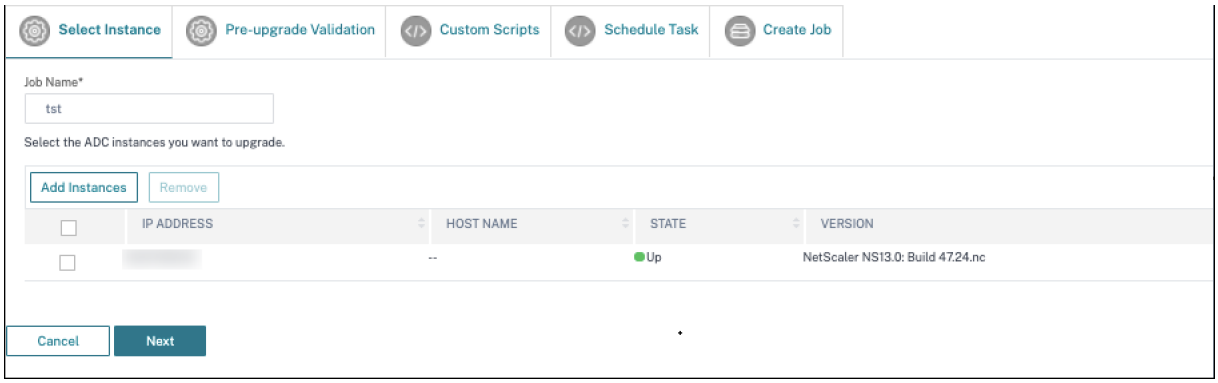
> **Nota**
>
> Si las instancias de NetScaler tienen personalizaciones, consulte Consideraciones de actualización para obtener configuraciones de NetScaler personalizadas antes de planificar la actualización de NetScaler.

Actualización: Puede actualizar las instancias vulnerables de NetScaler a una versión y compilación que tenga la solución. Este detalle se puede ver en la columna de corrección. Para actualizar, seleccione la instancia y, a continuación, haga clic en **Continuar para actualizar el flujo de trabajo**. En el flujo de trabajo de actualización, el NetScaler vulnerable se rellena automáticamente como el NetScaler de destino.

> **Nota**
>
> Las versiones 12.0, 11,0, 10.5 e inferiores ya están al final de la vida (EOL). Si sus instancias de NetScaler se ejecutan en alguna de estas versiones, actualice a una versión compatible.

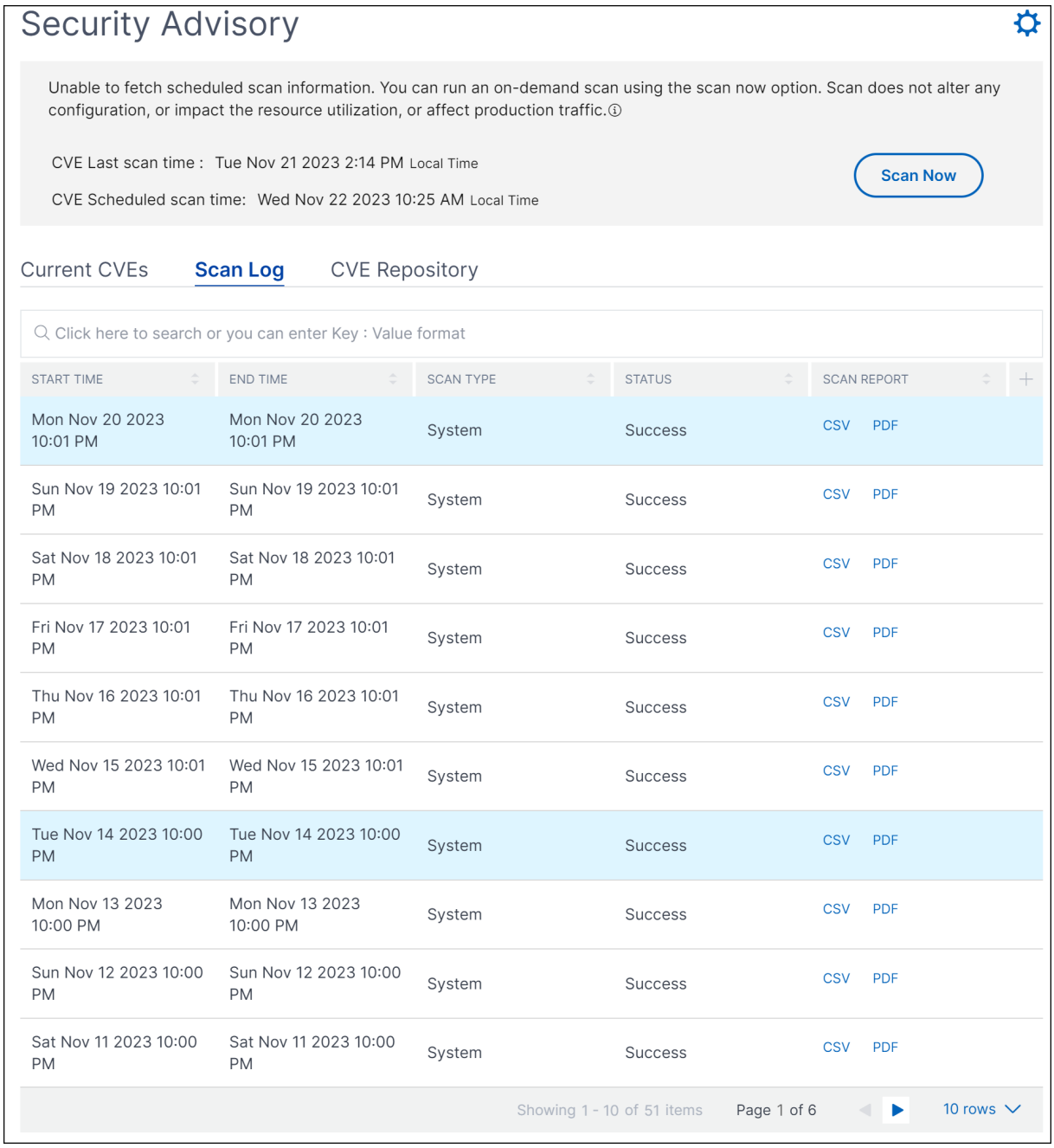
Se inicia el flujo de trabajo de actualización. Para obtener más información sobre cómo usar NetScaler ADM para actualizar las instancias de NetScaler, consulte Usar trabajos para actualizar las instancias de NetScaler.

> **Nota**
>
> La versión y compilación a la que quiere actualizar está a su discreción. Consulta los consejos de la columna de corrección para saber qué versión y qué compilaciones tienen la corrección de seguridad. Y, en consecuencia, seleccione una versión y una compilación compatibles que aún no hayan llegado al final de su vida útil.



Registro de análisis

La ficha muestra los informes de los últimos cinco escaneos de CVE, que incluyen escaneos del sistema predeterminados y escaneos iniciados por el usuario bajo demanda. Puede descargar el informe de cada escaneo en formato CSV y PDF. Si hay un análisis bajo demanda en curso, también puede ver el estado de finalización.

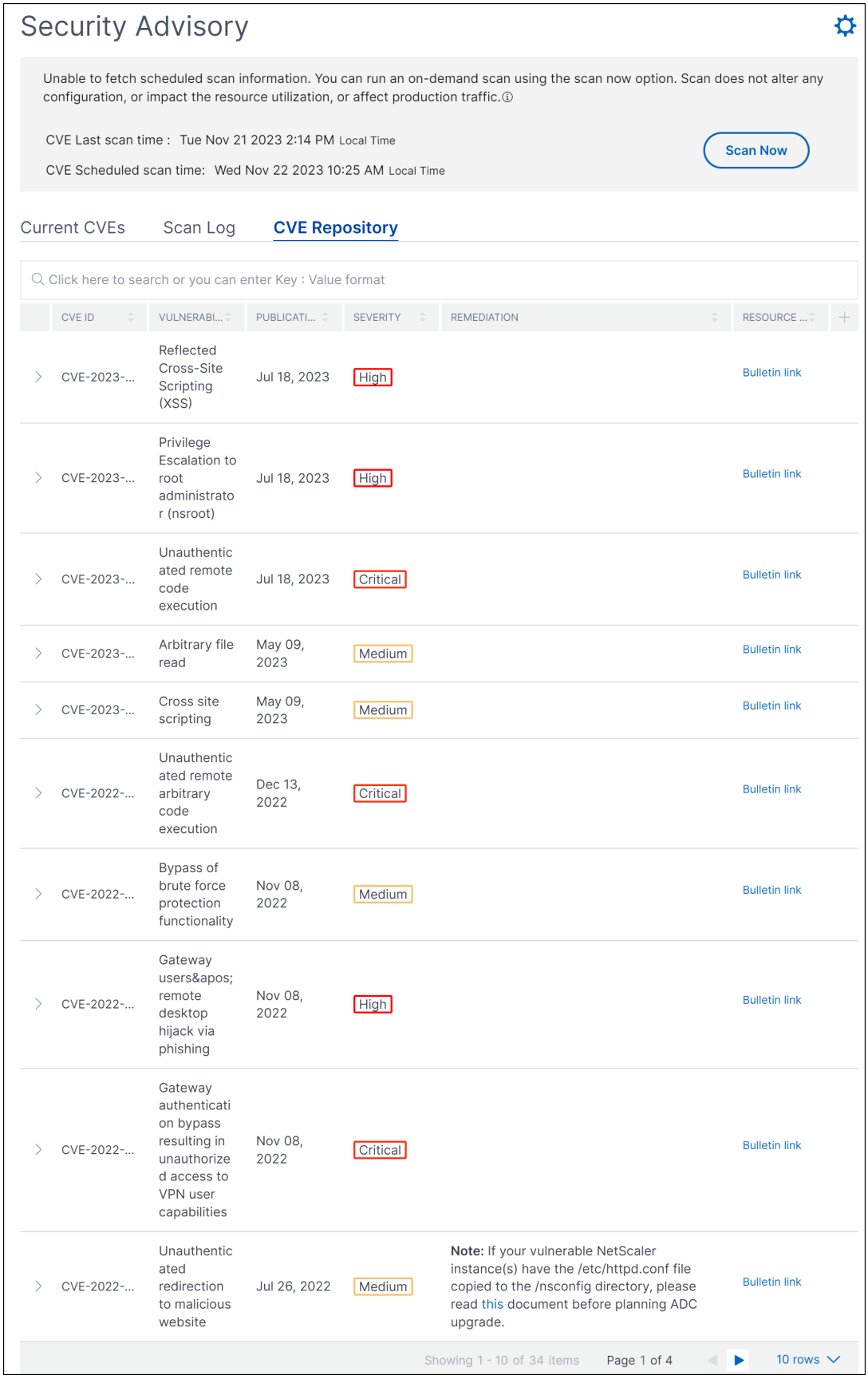


Repositorio CVE

Esta ficha incluye la información más reciente de todos los CVE de diciembre de 2019, junto con los siguientes detalles:

- Identificadores CVE
- Tipo de vulnerabilidad
- Fecha de publicación

- Nivel de gravedad
- Remediación
- Enlaces a boletines de seguridad



Security Advisory

Unable to fetch scheduled scan information. You can run an on-demand scan using the scan now option. Scan does not alter any configuration, or impact the resource utilization, or affect production traffic.

CVE Last scan time : Tue Nov 21 2023 2:14 PM Local Time

CVE Scheduled scan time: Wed Nov 22 2023 10:25 AM Local Time

Scan Now

Current CVEs | Scan Log | CVE Repository

Click here to search or you can enter Key : Value format

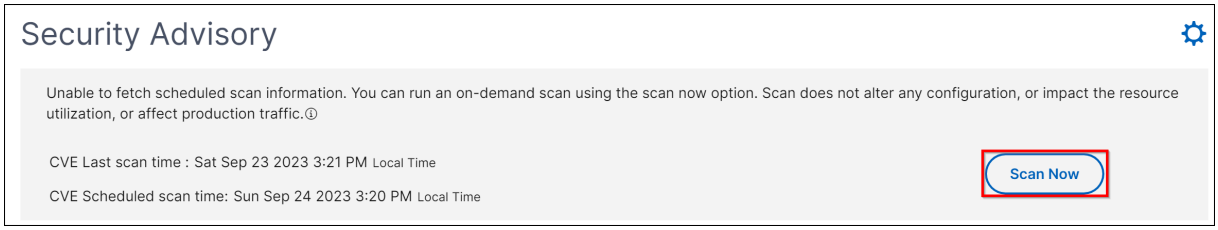
CVE ID	VULNERABI...	PUBLICATI...	SEVERITY	REMEDIATION	RESOURCE ...
CVE-2023-...	Reflected Cross-Site Scripting (XSS)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Privilege Escalation to root administrator (nsroot)	Jul 18, 2023	High		Bulletin link
CVE-2023-...	Unauthenticated remote code execution	Jul 18, 2023	Critical		Bulletin link
CVE-2023-...	Arbitrary file read	May 09, 2023	Medium		Bulletin link
CVE-2023-...	Cross site scripting	May 09, 2023	Medium		Bulletin link
CVE-2022-...	Unauthenticated remote arbitrary code execution	Dec 13, 2022	Critical		Bulletin link
CVE-2022-...	Bypass of brute force protection functionality	Nov 08, 2022	Medium		Bulletin link
CVE-2022-...	Gateway users' remote desktop hijack via phishing	Nov 08, 2022	High		Bulletin link
CVE-2022-...	Gateway authentication bypass resulting in unauthorized access to VPN user capabilities	Nov 08, 2022	Critical		Bulletin link
CVE-2022-...	Unauthenticated redirection to malicious website	Jul 26, 2022	Medium	**Note:** If your vulnerable NetScaler instance(s) have the /etc/httpd.conf file copied to the /nsconfig directory, please read this document before planning ADC upgrade.	Bulletin link

Showing 1 - 10 of 34 items Page 1 of 4 10 rows

Escanear ahora

Puede escanear las instancias en cualquier momento, según sus necesidades.

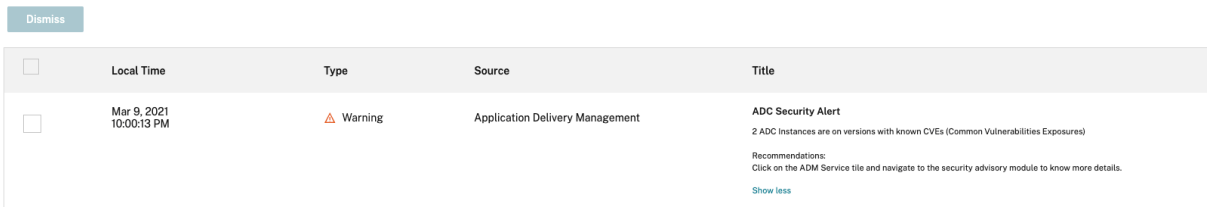
Haga clic en **Escanear ahora** para buscar los CVE que afecten a sus instancias de NetScaler. Una vez finalizado el análisis, los detalles de seguridad revisados aparecen en la GUI de asesoramiento de seguridad.



NetScaler ADM tarda unos minutos en completar el escaneo.

Notificación

Como administrador, recibe notificaciones de Citrix Cloud, que indican cuántas instancias de NetScaler son vulnerables a los CVE. Para ver las notificaciones, haga clic en el icono de campana en la esquina superior derecha de la GUI de NetScaler ADM.



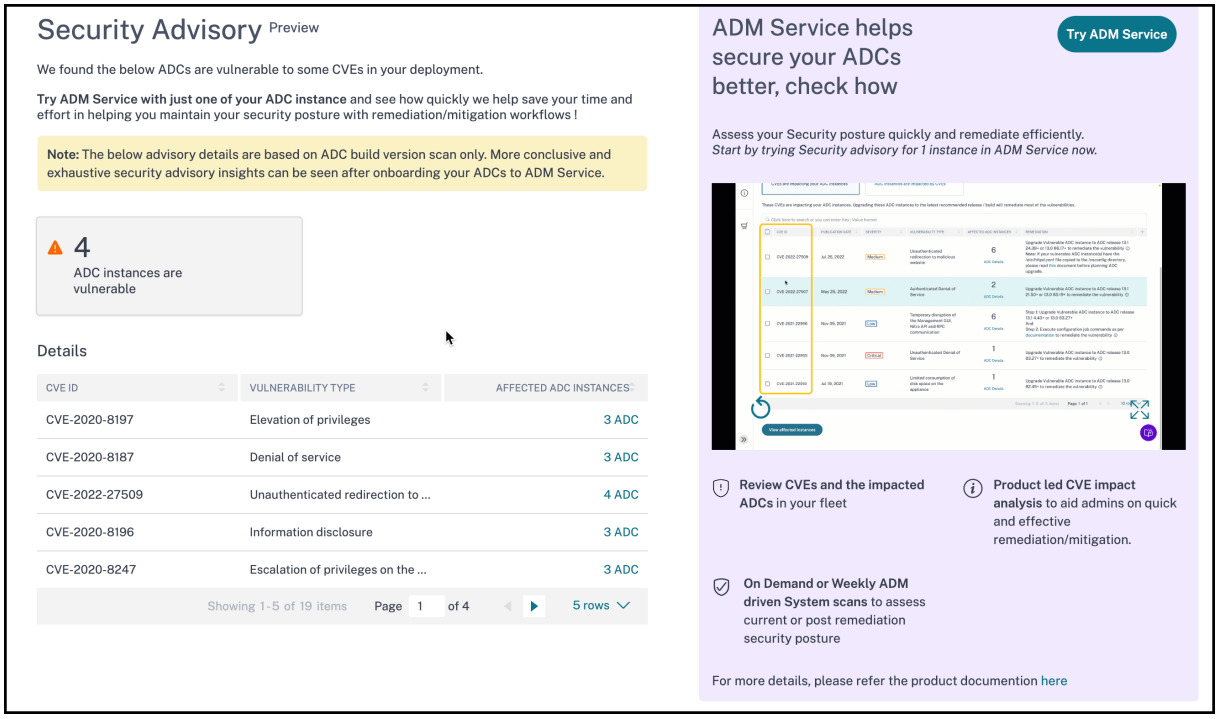
Aviso de seguridad en versiones 14.1 4.x o anteriores

Si está en las versiones anteriores, solo puede usar la versión preliminar de la función de asesoramiento de seguridad. La versión preliminar solo destaca los CVE de NetScaler y las instancias de ADC incorporadas a ADM Service que están en riesgo. Si quiere utilizar la versión completa de la función de asesoramiento de seguridad, debe habilitar ADM On-Prem Cloud Connector.

> **IMPORTANTE**
>
> Para obtener un análisis detallado del impacto de la CVE, información concluyente sobre los escaneos personalizados y los escaneos del sistema y los flujos de trabajo de corrección y mitigación, **pruebe NetScaler ADM Service**.

Ver asesoramiento de seguridad

Para acceder al **asesoramiento de seguridad**, vaya a **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**. Puede ver el estado de vulnerabilidad de todas las instancias de ADC que administra a través de NetScaler ADM.



El aviso de seguridad local de NetScaler ADM solo escanea la versión ADC para comprobar si hay CVE y se muestra la siguiente información.

- **ID de CVE**: el ID del CVE que afecta a las instancias.
- **Tipo de vulnerabilidad**: el tipo de vulnerabilidad de este CVE.
- Instancias de**ADC afectadas: el recuento de instancias**a las que afecta el ID de CVE.

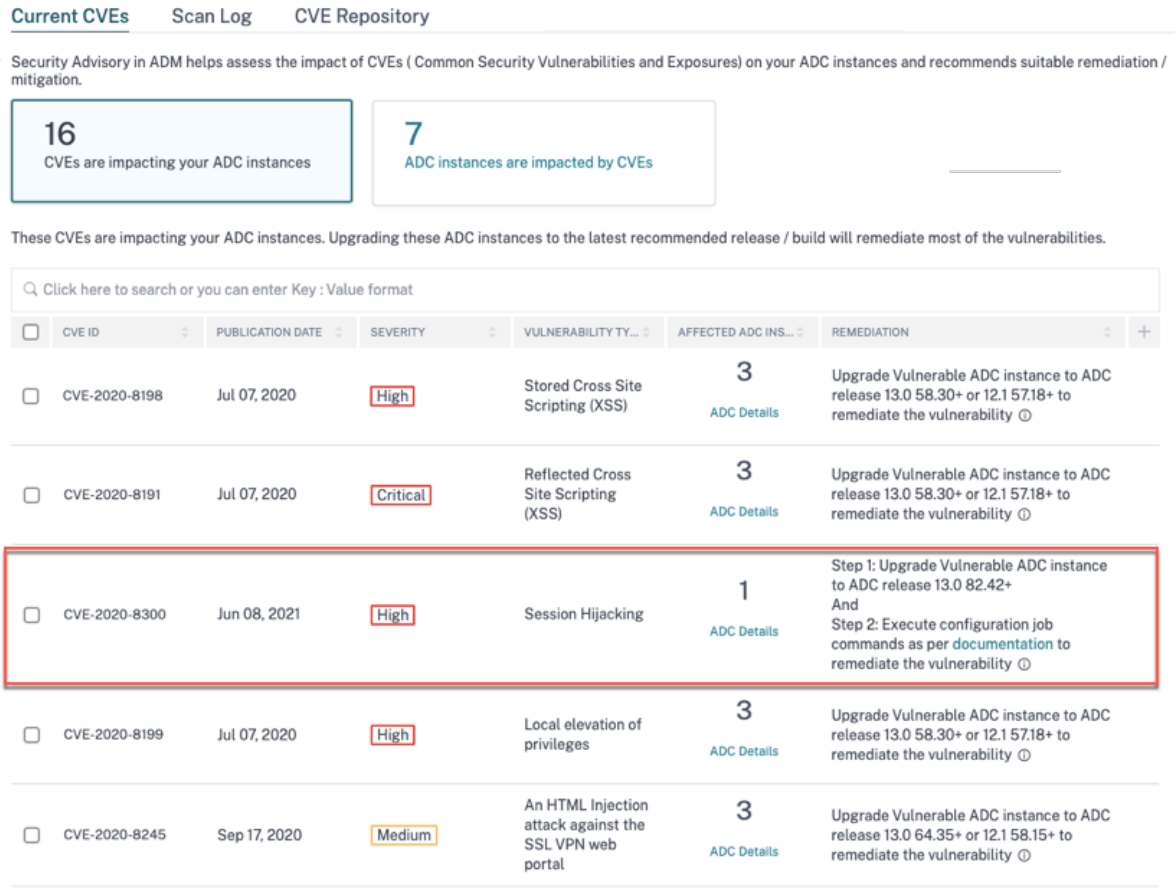
El aviso de seguridad local de NetScaler ADM también le permite seleccionar una de las instancias de ADC e incorporarla al servicio ADM. Haga clic en **Probar el servicio ADM** e incorpore la instancia de ADC al servicio ADM. El aviso de seguridad del servicio ADM le permite comprobar el tipo de vulnerabilidad de una CVE en particular y obtener información sobre la mitigación y la corrección para resolver la vulnerabilidad.

Para obtener más información sobre el aviso de seguridad del servicio ADM, consulte la animación GIF en la página del **aviso de seguridad**.

Corrija las vulnerabilidades del CVE-2020-8300

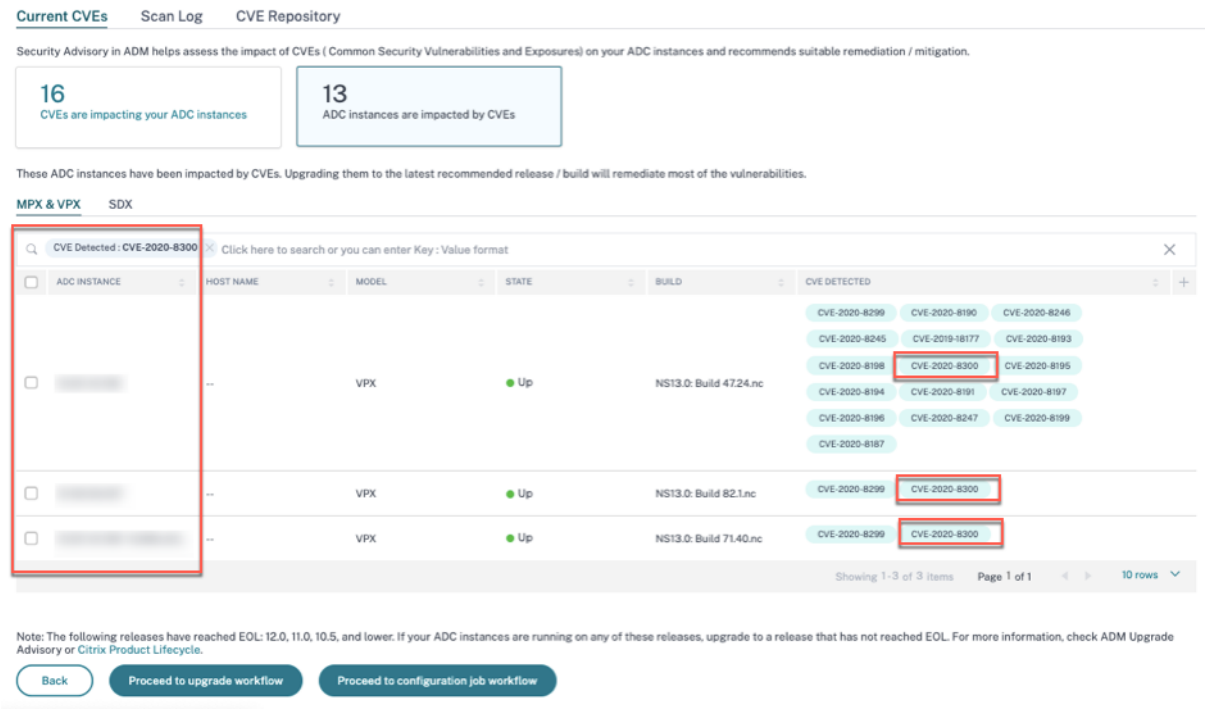
January 30, 2024

En el panel de consejos de seguridad de NetScaler ADM, en **CVE actuales > Las instancias de <number of> ADC se ven afectadas por las CVE**, puede ver todas las instancias vulnerables debido a este CVE específico. Para comprobar los detalles de las instancias afectadas por el CVE-2020-8300, seleccione **CVE-2020-8300** y haga clic en **Ver instancias afectadas**.



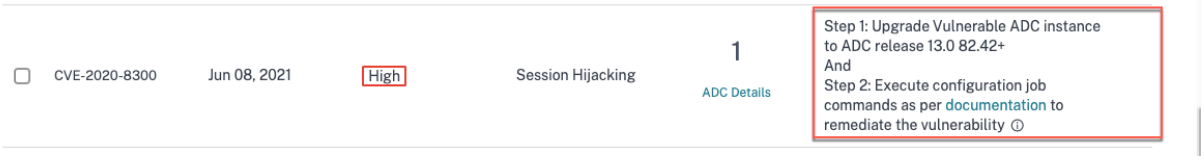
> **Nota**
>
> Para obtener más información sobre el panel de asesoramiento de seguridad, consulte Asesoramiento de seguridad .

Aparece la ventana **<number of>Instancias de ADC afectadas por los CVE**. Aquí puede ver el recuento y los detalles de las instancias de ADC afectadas por el CVE-2020-8300.



Corrija el CVE-2020-8300

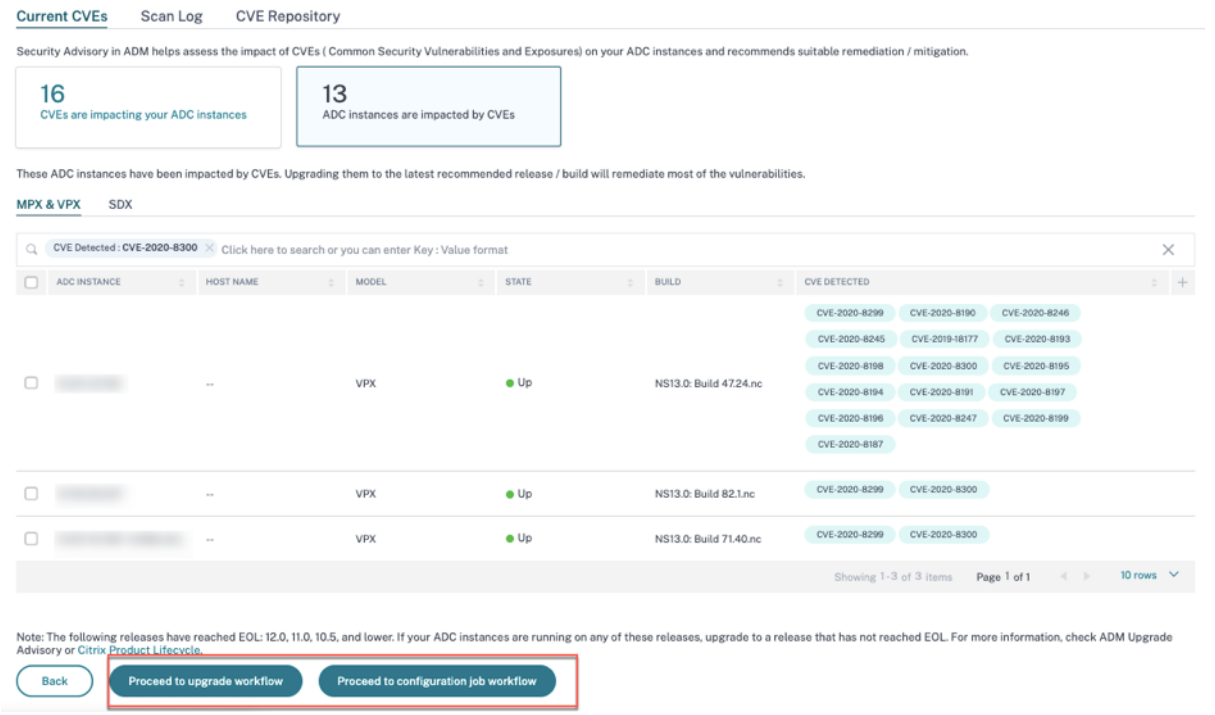
Para las instancias de ADC afectadas por el CVE-2020-8300, la corrección consiste en un proceso de dos pasos. En la GUI, en los **CVE actuales > Las instancias de ADC se ven afectadas por los CVE**, puede ver los pasos 1 y 2.



Los dos pasos incluyen:

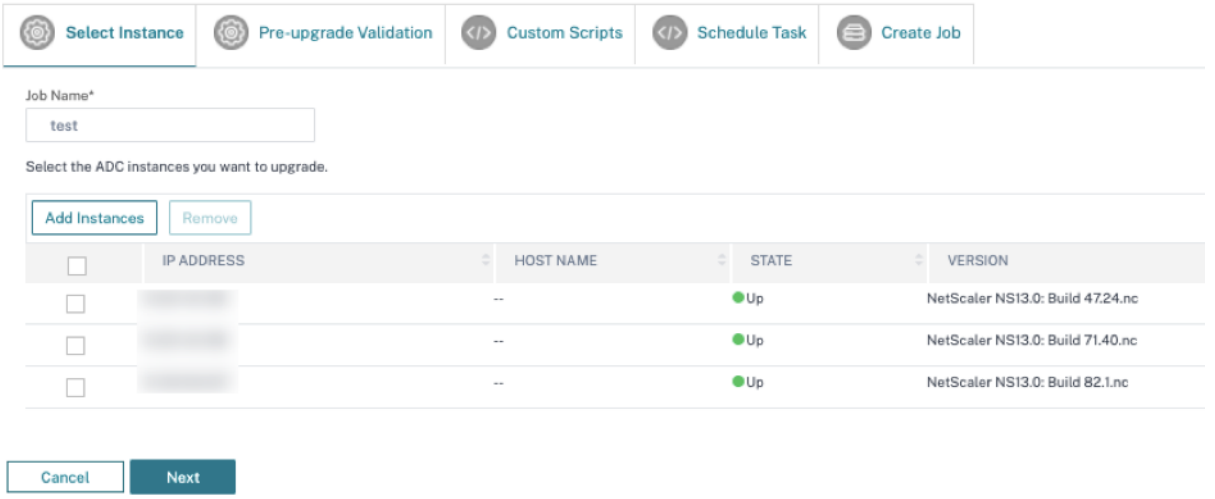
1. Actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.
2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración. Siga este paso para cada ADC vulnerable de uno en uno e incluya todas las acciones de SAML y los perfiles de SAML para ese ADC.

En **CVE actuales > Instancias de ADC afectadas por las CVE**, verá dos flujos de trabajo independientes para este proceso de corrección de 2 pasos: **Proceder a actualizar el flujo de trabajo** y **Proceder al flujo de trabajo de configuración**.



Paso 1: Actualizar las instancias de ADC vulnerables

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.



Para obtener más información sobre cómo usar NetScaler ADM para actualizar las instancias de ADC, consulte Crear un trabajo de actualización de ADC.

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de ADC vulnerables.

Paso 2: Aplicar los comandos de configuración

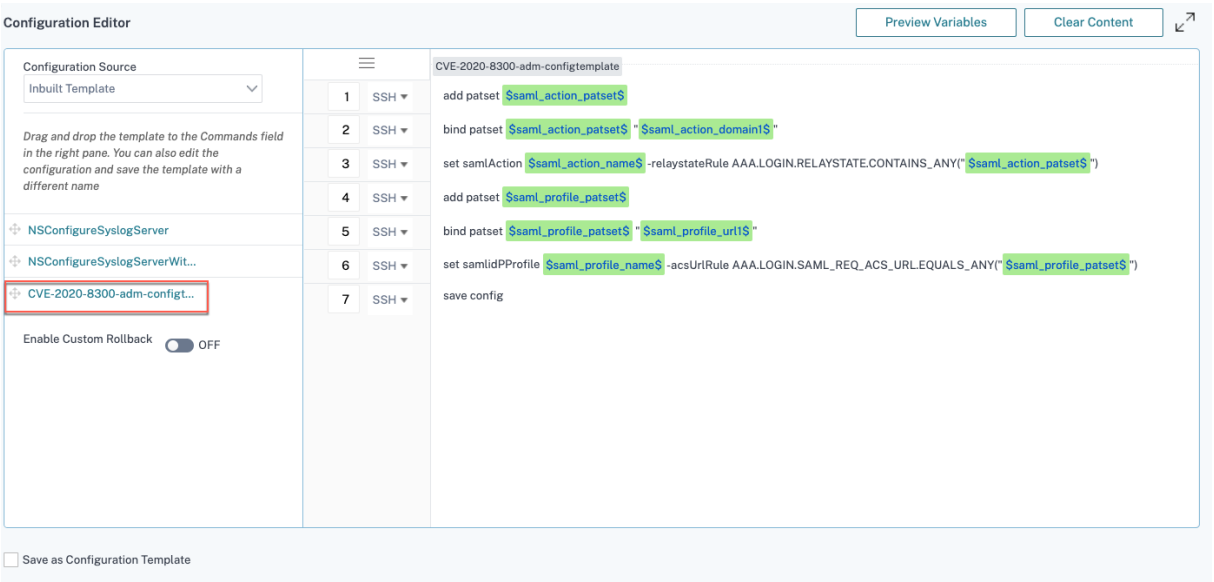
Tras actualizar las instancias afectadas, en la ventana **<number of> Instancias de ADC afectadas por los CVE**, seleccione una instancia afectada por el CVE-2020-8300 y haga clic en **Continuar con el flujo de trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.
5. Ejecutar el trabajo.

Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**:

- Para una instancia de ADC afectada por varios CVE (como CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 y CVE-2021-22956): al seleccionar la instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**, la plantilla de configuración integrada no se rellena automáticamente en Seleccionar configuración. Arrastre y suelte la plantilla de trabajo de configuración correspondiente en la sección **Plantilla de asesoramiento de seguridad** manualmente en el panel de tareas de configuración del lado derecho.
- Para varias instancias de ADC que se ven afectadas únicamente por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene ADC 1, ADC 2 y ADC 3, y todos ellos se ven afectados únicamente por el CVE-2021-22956. Seleccione todas estas instancias y haga clic en **Continuar con el flujo de trabajo de configuración**, y la plantilla de configuración integrada se rellenará automáticamente en **Seleccionar configuración**.
- Para varias instancias de ADC afectadas por CVE-2021-22956 y uno o más CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren una corrección para aplicarla a cada ADC a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo de configuración**, se produce un error aparece un mensaje que le indica que ejecute el trabajo de configuración en cada ADC a la vez.

Paso 1: Seleccione la configuración En el flujo de trabajo de configuración, la plantilla de configuración integrada se rellena automáticamente en **Seleccionar configuración**.



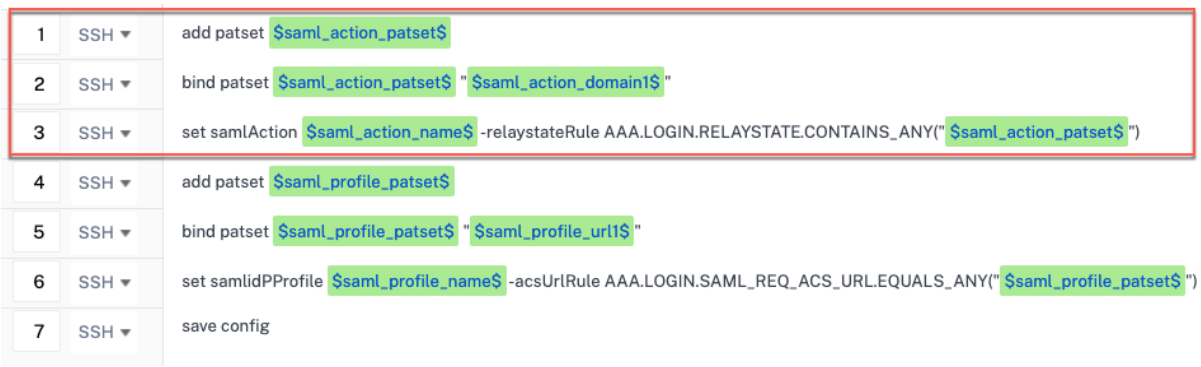
Ejecute un trabajo de configuración independiente para cada instancia de ADC afectada, de una en una, e incluya todas las acciones de SAML y los perfiles de SAML para ese ADC. Por ejemplo, si tiene dos instancias de ADC vulnerables, cada una con dos acciones de SAML y dos perfiles de SAML, debe ejecutar este trabajo de configuración dos veces. Una vez por ADC, cubriendo todas sus acciones de SAML y perfiles de SAML.

ADC 1	ADC2
Trabajo 1: dos acciones SAML+dos perfiles SAML	Trabajo 2: dos acciones SAML+dos perfiles SAML

Asigne un nombre al trabajo y personalice la plantilla para las siguientes especificaciones. La plantilla de configuración integrada es solo un esquema o una plantilla base. Personalice la plantilla en función de su implementación para cumplir con los siguientes requisitos:

a. **Acciones de SAML y sus dominios asociados**

Según la cantidad de acciones de SAML que tenga en su implementación, debe replicar las líneas 1 a 3 y personalizar los dominios para cada acción de SAML.

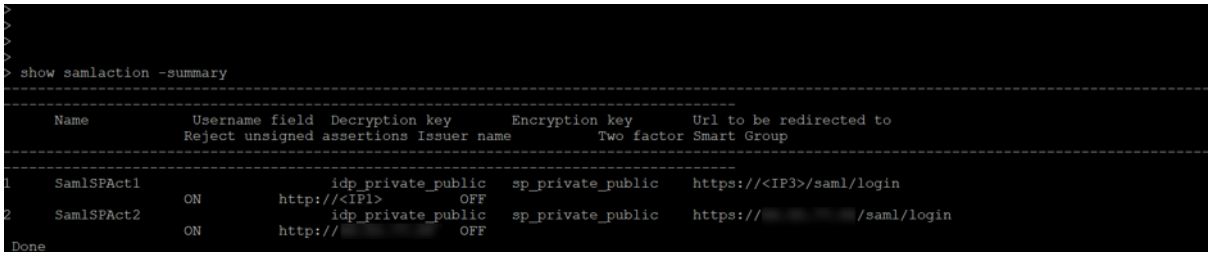


Por ejemplo, si tiene dos acciones de SAML, repita las líneas 1 a 3 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_action_patset$ "$saml_action_domain1$"` manualmente varias veces para asegurarse de que la línea aparezca N veces para esa acción de SAML. Y cambie los siguientes nombres de definición de variables:

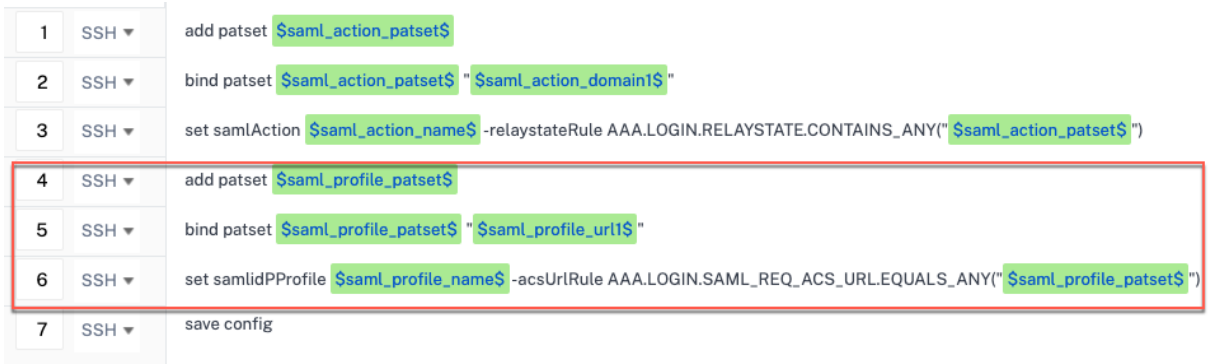
- `saml_action_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) de la acción SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.
- `saml_action_domain1`: es la variable de plantilla de configuración y representa el nombre de dominio de esa acción SAML específica. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

Para buscar todas las acciones de SAML de un dispositivo, ejecute el comando `show samlaction`.



b. **Perfiles SAML y sus URL asociadas**

Según la cantidad de perfiles SAML que tenga en su implementación, replique las líneas de 4 a 6. Personalice las URL de cada perfil de SAML.



Por ejemplo, si tiene dos perfiles SAML, introduzca manualmente las líneas 4 a 6 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

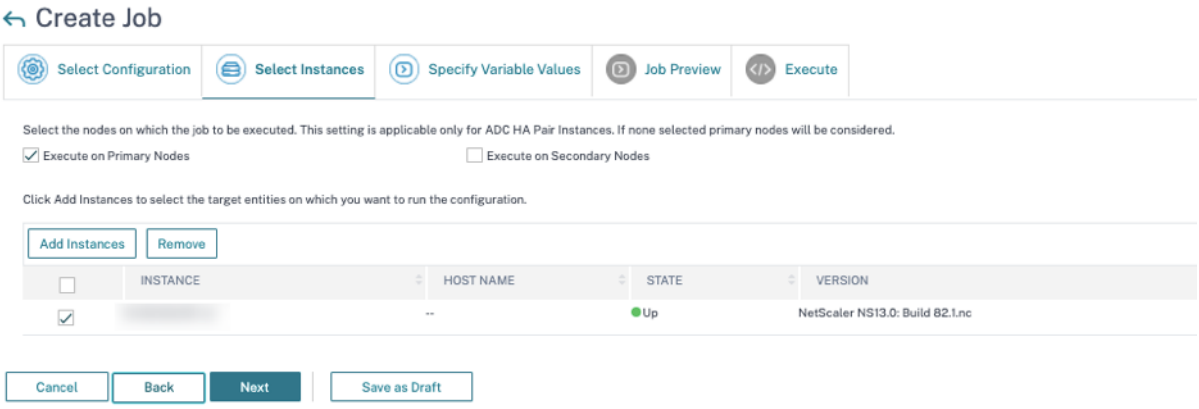
Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_profile_patset "$saml_profile_url1$"` manualmente varias veces para asegurarse de que la línea aparezca N veces para ese perfil de SAML. Y cambie los siguientes nombres de definición de variables:

- `saml_profile_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) del perfil SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.
- `saml_profile_url1`: es la variable de plantilla de configuración y representa el nombre de dominio de ese perfil SAML específico. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

Para buscar todos los perfiles SAM de un dispositivo, ejecute el comando `show samlidpProfile` .

Paso 2: selecciona la instancia

La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia y haga clic en **Siguiente**.

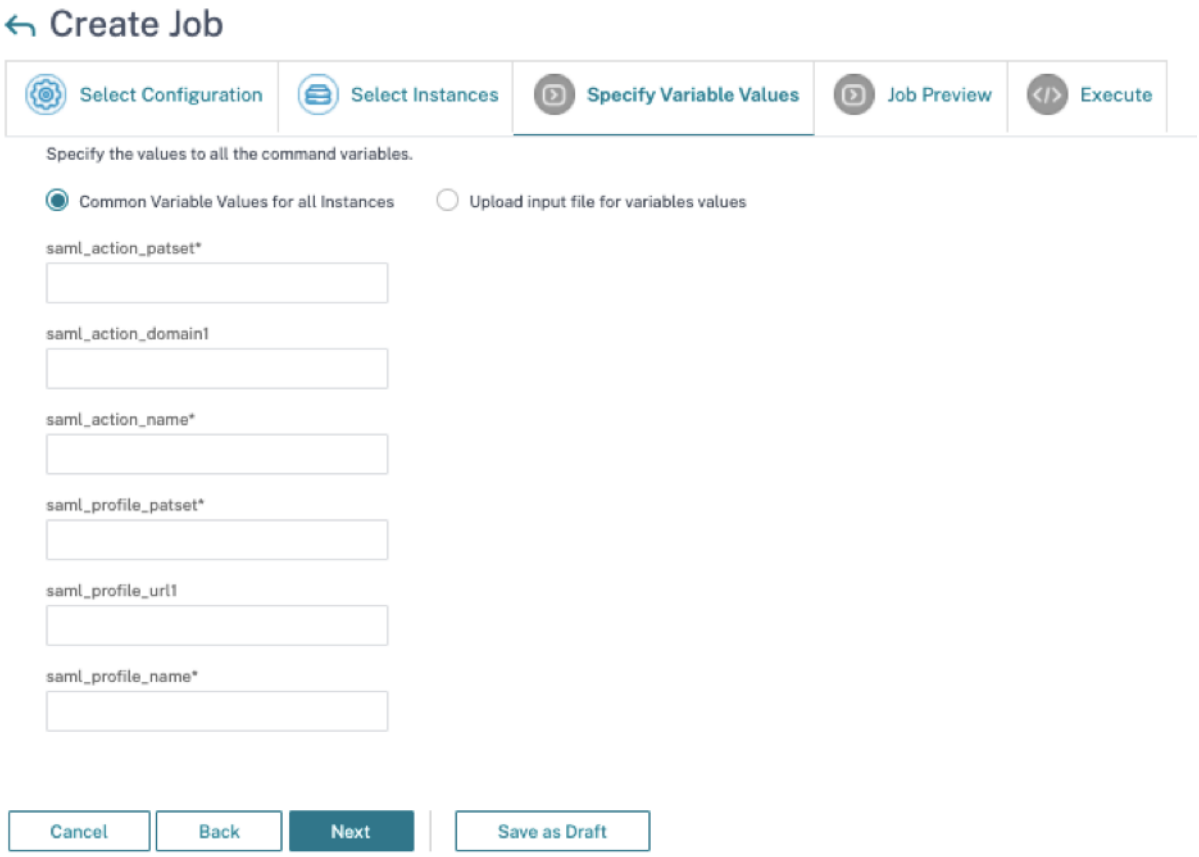


Paso 3: especificar los valores de las variables Introduzca los valores de las variables.

- `saml_action_patset`: agregar un nombre para la acción SAML

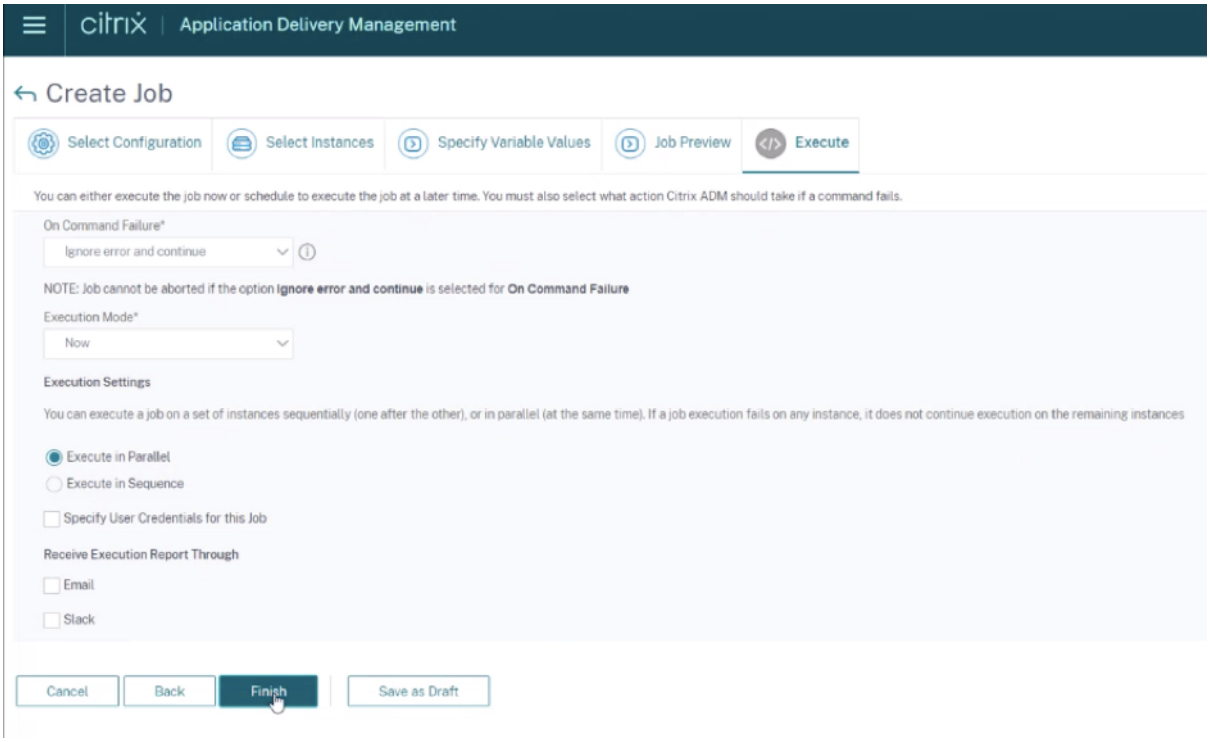
- `saml_action_domain1`: introduzca un dominio con el formato `https://<example1.com>/`
- `saml_action_name`: introduzca lo mismo de la acción SAML para la que está configurando el trabajo
- `saml_profile_patset`: agregue un nombre para el perfil SAML
- `saml_profile_url1`: introduzca la URL en este formato `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: introduzca el mismo perfil SAML para el que está configurando el trabajo

> **Nota**
>
> En el caso de las URL, la extensión no siempre es así `cgi/samlauth`. Depende de la autorización de terceros que tenga y, en consecuencia, debe colocar la extensión.



Paso 4: Vista previa de la configuración Previsualiza los valores de las variables que se han insertado en la configuración y haga clic en **Siguiente**.

Paso 5: Ejecute el trabajo Haga clic en **Finalizar** para ejecutar el trabajo de configuración.



Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para todos los ADC vulnerables, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Puntos a tener en cuenta sobre la cuenta NetScaler ADM Express

La cuenta NetScaler ADM Express tiene funciones limitadas, que incluyen la limitación de dos trabajos de configuración únicamente.

Para corregir el CVE-2020-8300, debe ejecutar tantos trabajos de configuración como el número de instancias de ADC vulnerables. Por lo tanto, si tiene una cuenta Express y necesita ejecutar más de dos trabajos de configuración, siga esta solución alternativa.

Solución alternativa: ejecute dos trabajos de configuración para dos instancias de ADC vulnerables y, a continuación, elimine ambos trabajos para seguir ejecutando los dos trabajos siguientes para las dos siguientes instancias de ADC vulnerables. Continúe con esto hasta que haya cubierto todos los casos vulnerables. Antes de eliminar los trabajos, puede descargar el informe para consultarlo en el futuro. Para descargar el informe, en **Red > Trabajos**, seleccione los trabajos y haga clic en **Descargar** en **Acciones**.

Ejemplo: Si tiene seis instancias de ADC vulnerables, ejecute dos trabajos de configuración en dos instancias vulnerables respectivamente y, a continuación, elimine ambos trabajos de configuración.

Repite este paso otras dos veces. Al final, habría ejecutado seis trabajos de configuración para seis instancias de ADC, respectivamente. En la interfaz de usuario de NetScaler ADM, **en Infraestructura > Trabajos**, solo verá los dos últimos trabajos de configuración.

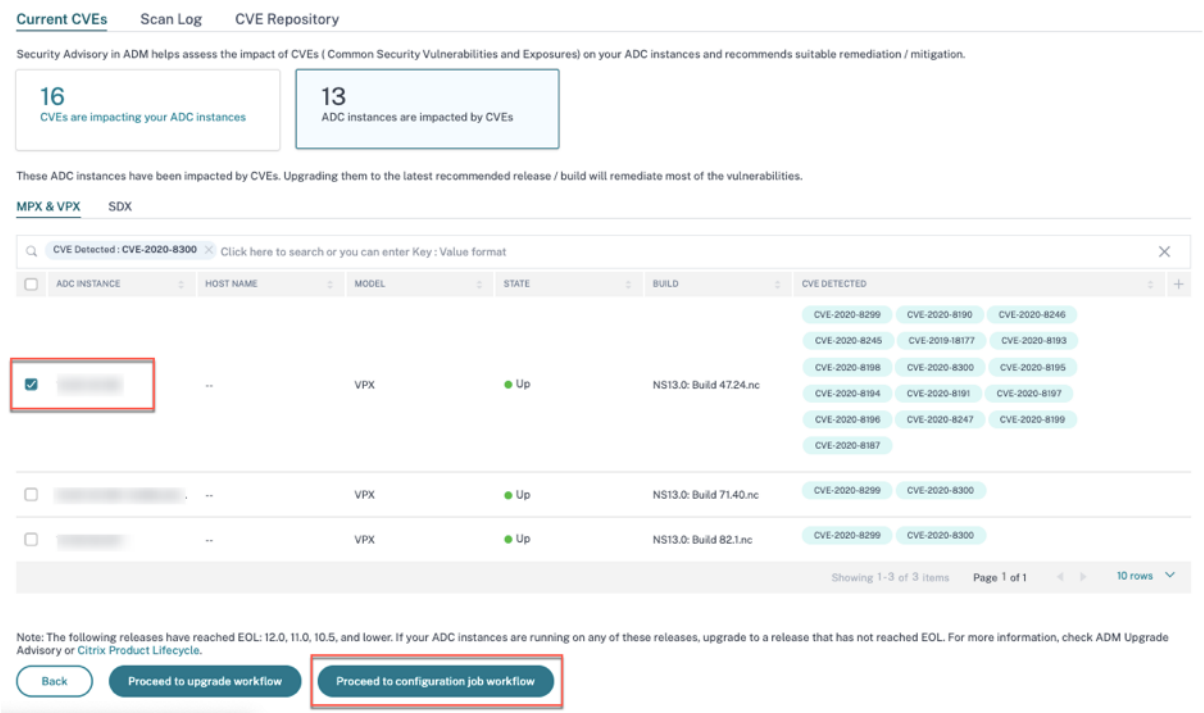
Escenario

En este escenario, tres instancias de ADC son vulnerables a CVE-2020-8300 y debe corregir todas las instancias. Siga estos pasos:

1. Actualice las tres instancias de ADC siguiendo los pasos que se indican en la sección **Actualizar una instancia** de este documento.
2. Aplique el parche de configuración a un ADC a la vez, mediante el flujo de trabajo de configuración. Consulte los pasos que se indican en la sección **Aplicar comandos de configuración** de este documento.

El ADC 1 vulnerable tiene la siguiente configuración:

Dos acciones SAML	Dos perfiles SAML
La acción 1 de SAML tiene un dominio y la acción 2 de SAML tiene dos dominios	El perfil SAML 1 tiene una URL y el perfil SAML 2 tiene dos URL



Seleccione ADC 1 y haga clic en **Continuar con el flujo de trabajo de configuración**. La plantilla integrada se rellena automáticamente. A continuación, asigne un nombre a la tarea y personalice la plantilla de acuerdo con la configuración dada.

En las tablas siguientes se enumeran las definiciones de variables para los parámetros personalizados.

Tabla 1. Definiciones de variables para la acción SAML

Configuración ADC	Definición de variable para patset	Definición de variable para el nombre de la acción SAML	Definición de variable para dominio
La acción 1 de SAML tiene un dominio	saml_action_patset1	saml_action_name1	saml_action_domain1
La acción 2 de SAML tiene dos dominios	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Tabla 2. Definiciones de variables para el perfil SAML

Configuración ADC	Definición de variable para patset	Definición de variable para el nombre de perfil SAML	Definición de variable para URL
El perfil SAML 1 tiene una URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
El perfil SAML 2 tiene dos URL	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

En **Seleccionar instancias**, seleccione ADC 1 y haga clic en **Siguiente**. Aparece la ventana **Especificar valores variables**. En este paso, debe proporcionar valores para todas las variables definidas en el paso anterior.

A continuación, revise las variables.

Haga clic en **Siguiente** y, después, en **Finalizar** para ejecutar el trabajo.

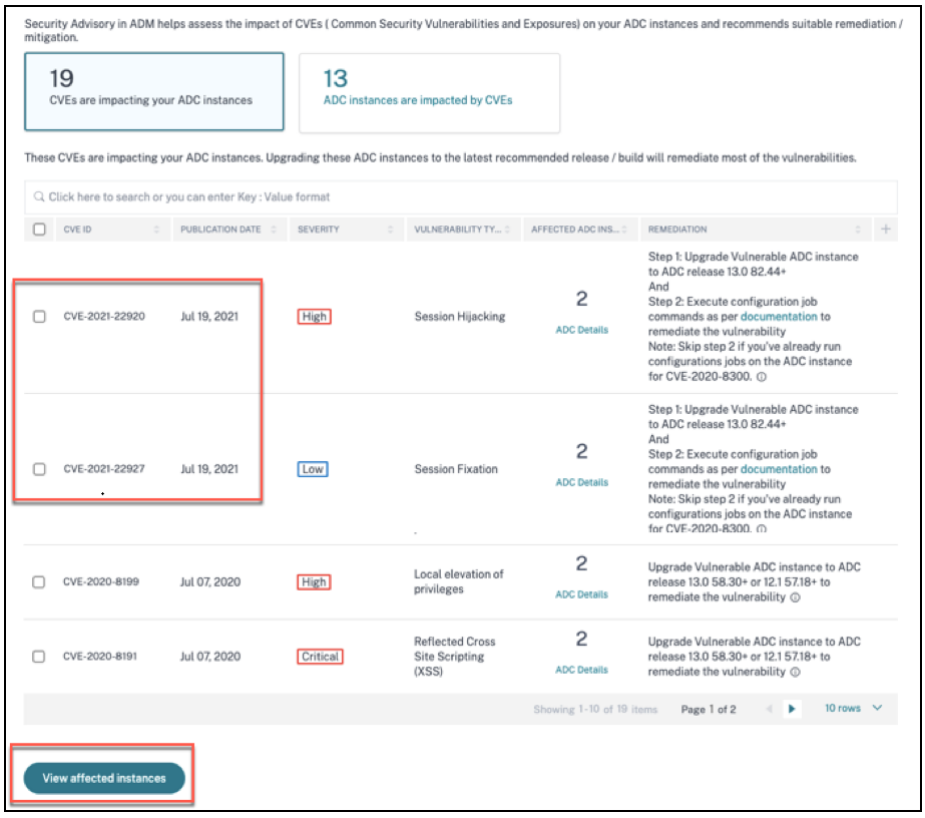
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para ADC1, siga los mismos pasos para corregir el ADC 2 y el ADC 3. Una vez finalizada la corrección, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Corrija las vulnerabilidades de los CVE-2021-22927 y CVE-2021-22920

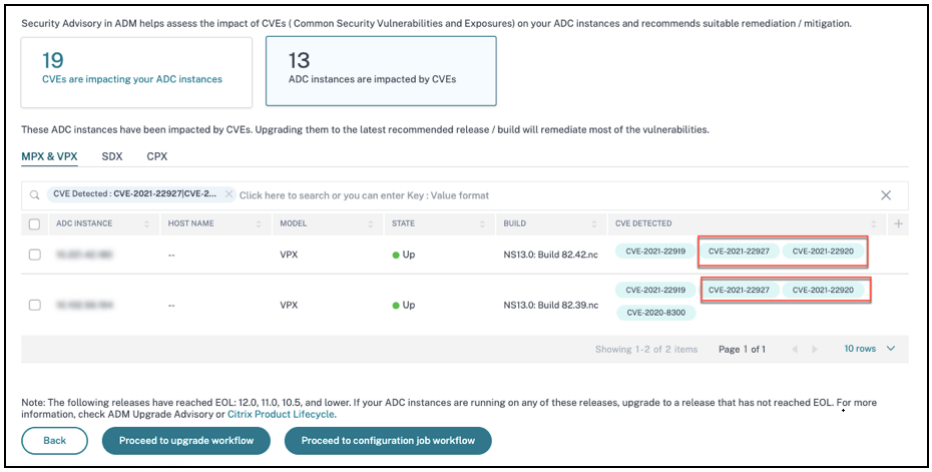
January 30, 2024

En el panel de consejos de seguridad de NetScaler ADM, en **CVE actuales > Las instancias de < `number of`> ADC se ven afectadas por las CVE**, puede ver todas las instancias vulnerables debido a los CVE-2021-22927 y CVE-2021-22920. Para comprobar los detalles de las instancias afectadas por estos dos CVE, seleccione uno o más CVE y haga clic en **Ver instancias afectadas**.



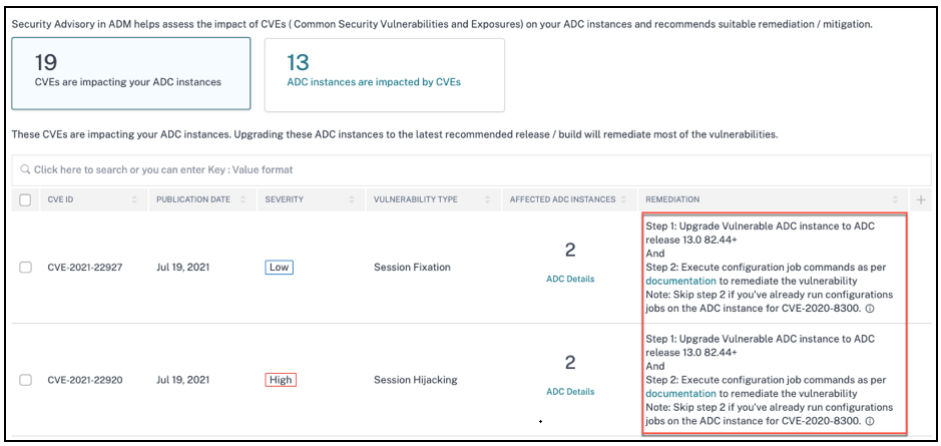
> **Nota**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde un par de horas en concluir y reflejar el impacto de los CVE-2021-22927 y CVE-2021-22920 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, inicie un análisis bajo demanda haciendo clic en **Escanear ahora**.
>
> Para obtener más información sobre el panel de asesoramiento de seguridad, consulte Asesoramiento de seguridad .

Aparece la ventana **<number of>Instancias de ADC afectadas por los CVE**. En la siguiente captura de pantalla, puede ver el recuento y los detalles de las instancias de ADC afectadas por los CVE-2021-22927 y CVE-2021-22920.



Corrija los CVE-2021-22927 y CVE-2021-22920

Para las instancias de ADC afectadas por los CVE-2021-22927 y CVE-2021-22920, la corrección consiste en un proceso de dos pasos. En la GUI, en los **CVE actuales > Las instancias de ADC se ven afectadas por los CVE**, puede ver los pasos 1 y 2.

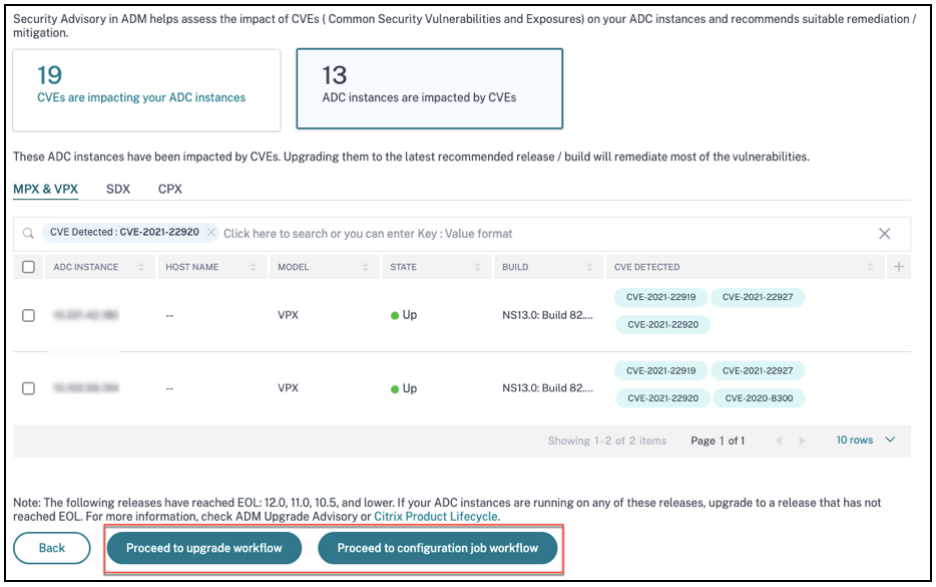


Los dos pasos incluyen:

1. Actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.
2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración. Siga este paso para cada ADC vulnerable, uno a la vez, e incluya todas las acciones de SAML para ese ADC.

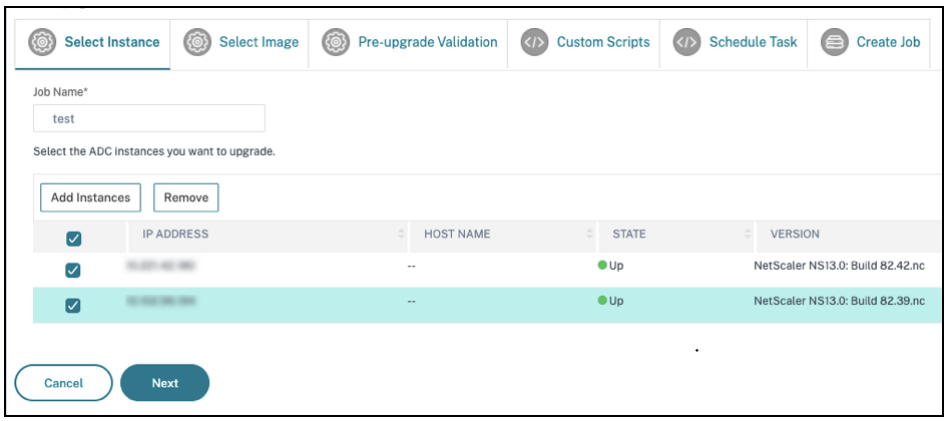
> **Nota**
>
> Omita el paso 2 si ya ha ejecutado trabajos de configuración en la instancia ADC para el CVE-2020-8300.

En **CVE actuales > Instancias de ADC afectadas por las CVE**, verá dos flujos de trabajo independientes para este proceso de corrección de 2 pasos: **Proceder a actualizar el flujo de trabajo** y **Proceder al flujo de trabajo de configuración**.



Paso 1: Actualizar las instancias de ADC vulnerables

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.



Para obtener más información sobre cómo usar NetScaler ADM para actualizar las instancias de ADC, consulte Crear un trabajo de actualización de ADC.

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de ADC vulnerables.
>
> **Nota**
>
> Tras completar el paso 1 para todas las instancias de ADC vulnerables a los CVE-2021-22920 y CVE-2021-22927, realice un análisis a petición. La postura de seguridad actualizada en los **CVE actuales** le ayuda a comprender si las instancias de ADC siguen siendo vulnerables a alguno de estos CVE. Desde la nueva postura, también puede comprobar si necesita ejecutar trabajos de configuración.
>
> Si ya ha aplicado los trabajos de configuración adecuados a la instancia de ADC para CVE-2020-8300 y ahora ha actualizado la instancia de ADC, después de realizar el análisis bajo demanda, la instancia ya no se muestra como vulnerable para CVE-2020-8300, CVE-2021-22920 y CVE-2021-22927.

Paso 2: Aplicar los comandos de configuración

Tras actualizar las instancias afectadas, en la ventana **<number of> Instancias de ADC afectadas por los CVE**, seleccione una instancia afectada por los CVE-2021-22927 y CVE-2021-22920 y haga clic en **Continuar con el flujo de trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

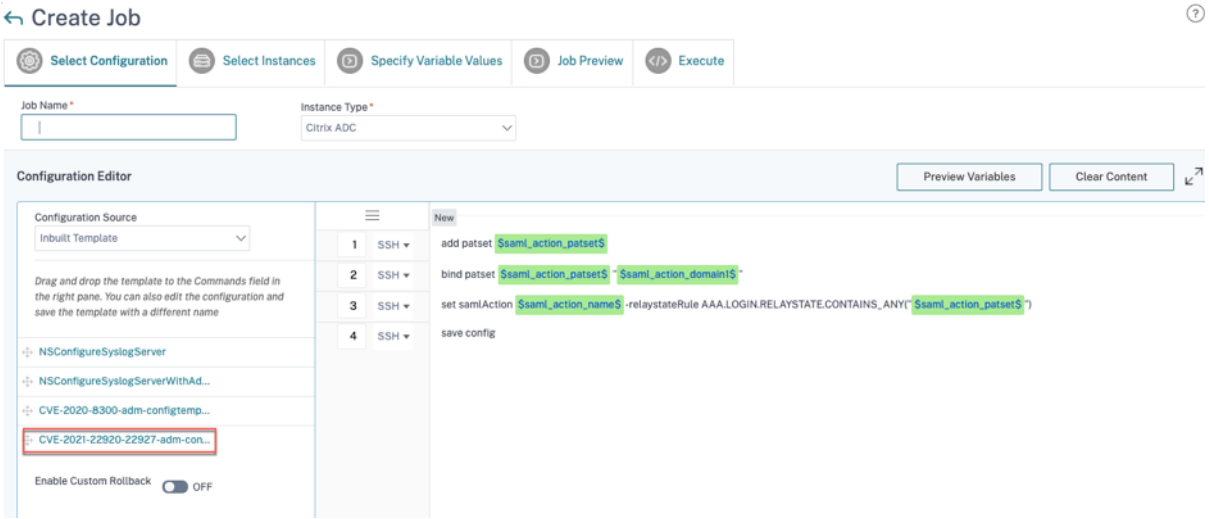
1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.
5. Ejecutar el trabajo.

Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar**

con el flujo de trabajo de configuración:

- Para una instancia de ADC afectada por varios CVE (como CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 y CVE-2021-22956): al seleccionar la instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**, la plantilla de configuración integrada no se rellena automáticamente en Seleccionar configuración. Arrastre y suelte la plantilla de trabajo de configuración correspondiente en la sección **Plantilla de asesoramiento de seguridad** manualmente en el panel de tareas de configuración del lado derecho.
- Para varias instancias de ADC que se ven afectadas únicamente por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene ADC 1, ADC 2 y ADC 3, y todos ellos se ven afectados únicamente por el CVE-2021-22956. Seleccione todas estas instancias y haga clic en **Continuar con el flujo de trabajo de configuración**, y la plantilla de configuración integrada se rellenará automáticamente en **Seleccionar configuración**.
- Para varias instancias de ADC afectadas por CVE-2021-22956 y uno o más CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren una corrección para aplicarla a cada ADC a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo de configuración**, se produce un error aparece un mensaje que le indica que ejecute el trabajo de configuración en cada ADC a la vez.

Paso 1: Seleccione la configuración En el flujo de trabajo de configuración, la plantilla base de configuración integrada se rellena automáticamente en **Seleccionar configuración**.



> **Nota**
>
> Si la instancia de ADC seleccionada en el paso 2 para aplicar los comandos de configuración es vulnerable a CVE-2021-22927, CVE-2021-22920 y también a CVE-2020-8300, la plantilla base de CVE-2020-8300 se rellena automáticamente. La plantilla CVE-2020-8300 es un superconjunto

> de comandos de configuración necesarios para los tres CVE. Personalice esta plantilla base de acuerdo con la implementación y los requisitos de su instancia de ADC.

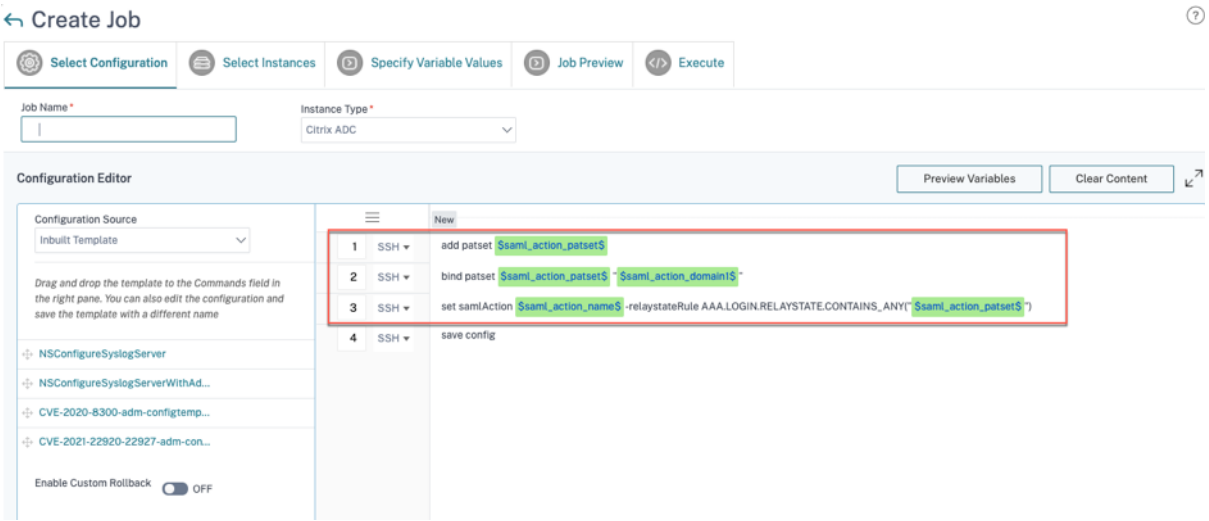
Debe ejecutar un trabajo de configuración independiente para cada instancia de ADC afectada, una a la vez, e incluir todas las acciones de SAML para ese ADC. Por ejemplo, si tiene dos instancias de ADC vulnerables, cada una con dos acciones de SAML, debe ejecutar este trabajo de configuración dos veces. Una vez por ADC cubriendo todas sus acciones de SAML.

ADC 1	ADC2
Trabajo 1: dos acciones de SAML	Trabajo 2: dos acciones de SAML

Asigne un nombre al trabajo y personalice la plantilla para las siguientes especificaciones. La plantilla de configuración integrada es solo un esquema o una plantilla base. Personalice la plantilla en función de su implementación para cumplir con los siguientes requisitos:

a. **Acciones de SAML y sus dominios asociados**

Según la cantidad de acciones de SAML que tenga en su implementación, debe replicar las líneas 1 a 3 y personalizar los dominios para cada acción de SAML.



Por ejemplo, si tiene dos acciones de SAML, repita las líneas 1 a 3 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_action_patset$ "$saml_action_domain1$"` manualmente varias veces para asegurarse de que la línea aparezca N veces para esa acción de SAML. Y cambie los siguientes nombres de definición de variables:

- `saml_action_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) de la acción SAML. Puede especificar el valor real en el

paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

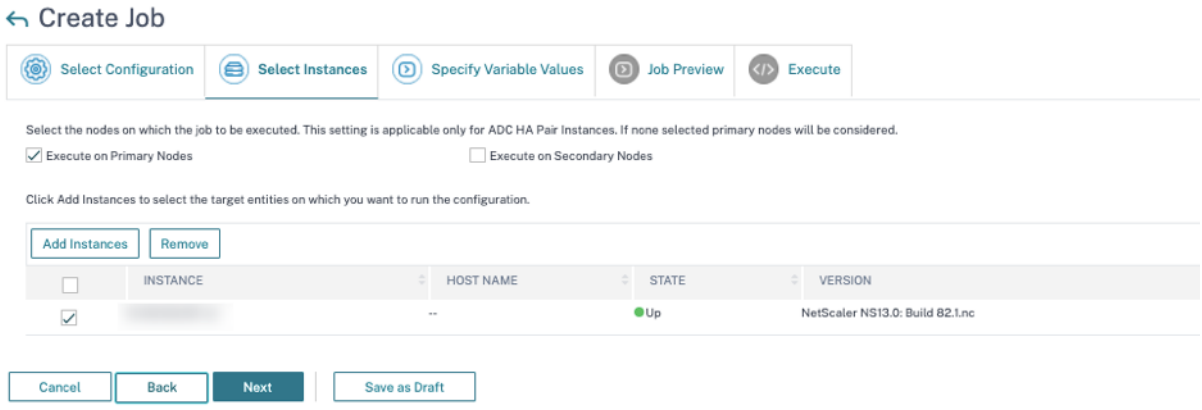
- `saml_action_domain1`: es la variable de plantilla de configuración y representa el nombre de dominio de esa acción SAML específica. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

Para buscar todas las acciones de SAML de un dispositivo, ejecute el comando `show samlaction` .

```
> show samlaction -summary
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
     Name           Username field  Decryption key       Encryption key       Url to be redirected to
                    Reject unsigned assertions Issuer name          Two factor Smart Group
-------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------
1    SamlSPAct1                     idp_private_public   sp_private_public    https://<IP3>/saml/login
                ON          http://<IP1>          OFF
2    SamlSPAct2                     idp_private_public   sp_private_public    https://[redacted]/saml/login
                ON          http://[redacted]     OFF
 Done
```

Paso 2: selecciona la instancia

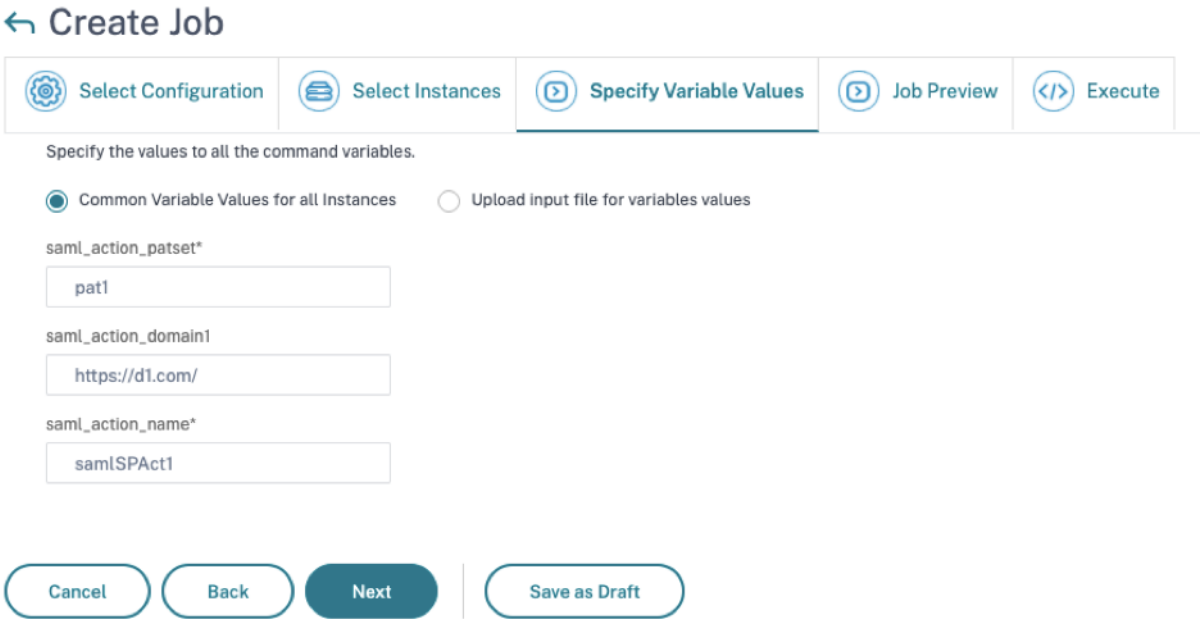
La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia y haga clic en **Siguiente**.



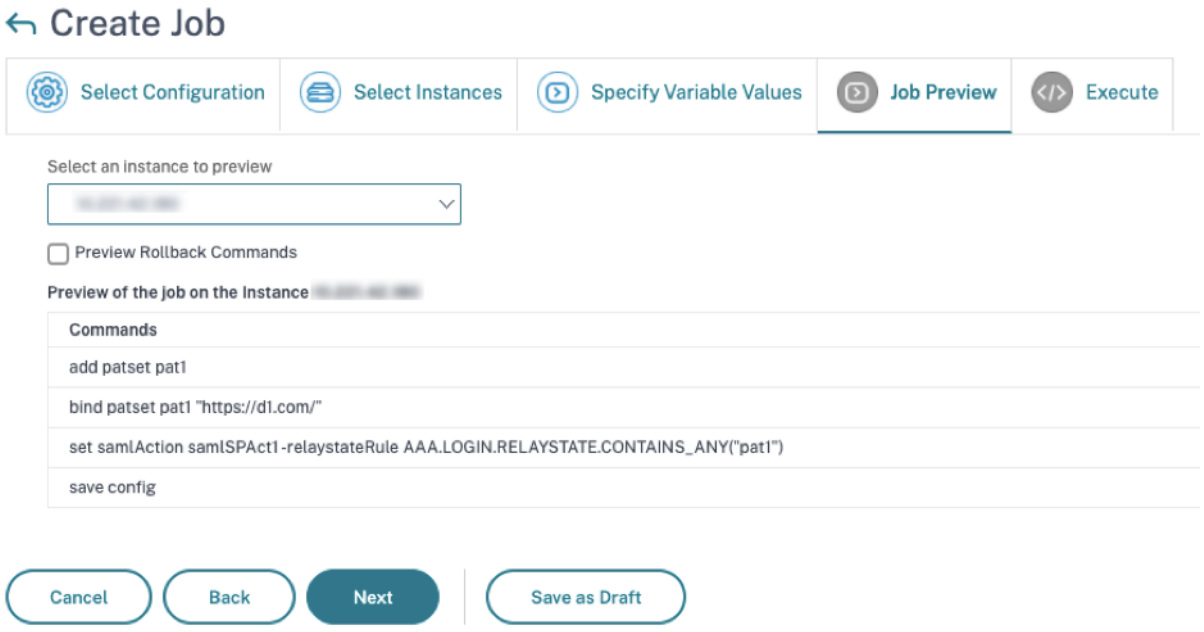
Paso 3: especificar los valores de las variables Introduzca los valores de las variables.

- `saml_action_patset`: agregar un nombre para la acción SAML
- `saml_action_domain1`: introduzca un dominio con el formato `https://<example1.com>/`

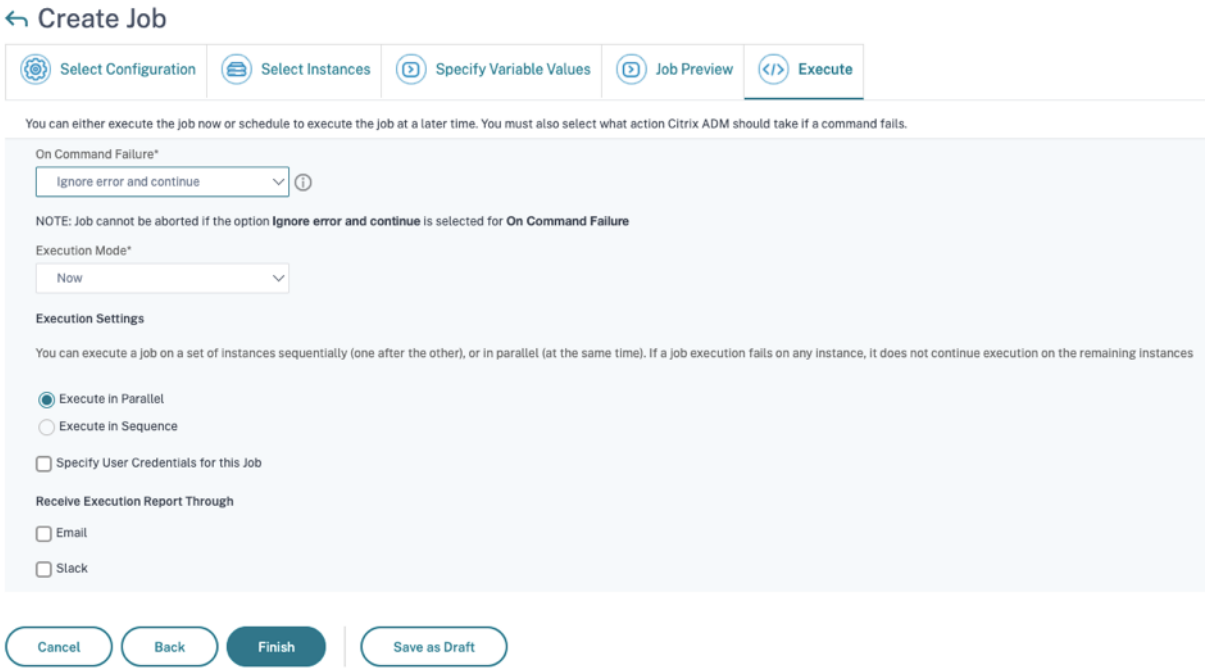
- `saml_action_name`: introduzca lo mismo de la acción SAML para la que está configurando el trabajo



Paso 4: Vista previa de la configuración Previsualiza los valores de las variables que se han insertado en la configuración y haga clic en **Siguiente**.



Paso 5: Ejecute el trabajo Haga clic en **Finalizar** para ejecutar el trabajo de configuración.



Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para todos los ADC vulnerables, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

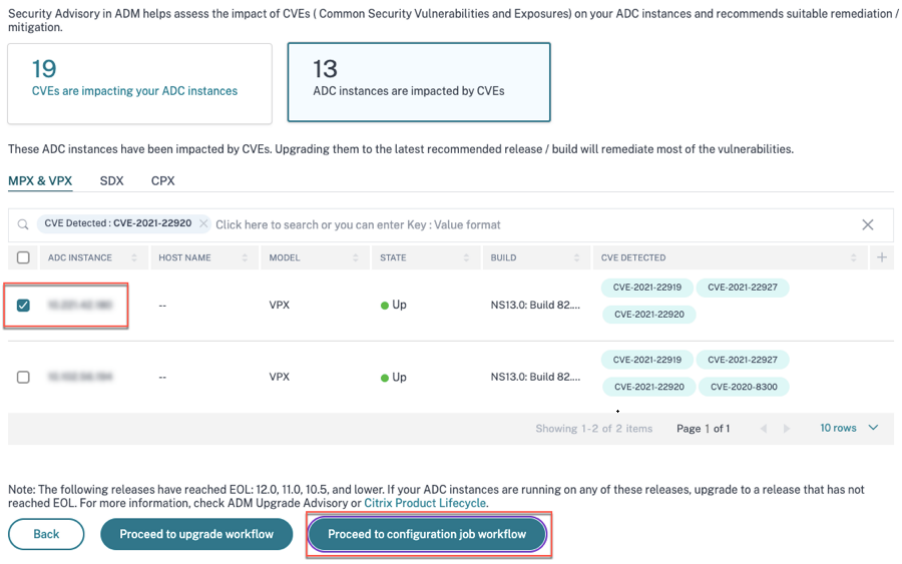
Escenario

En este escenario, dos instancias de ADC son vulnerables a CVE-2021-22920 y debe corregir todas las instancias. Siga estos pasos:

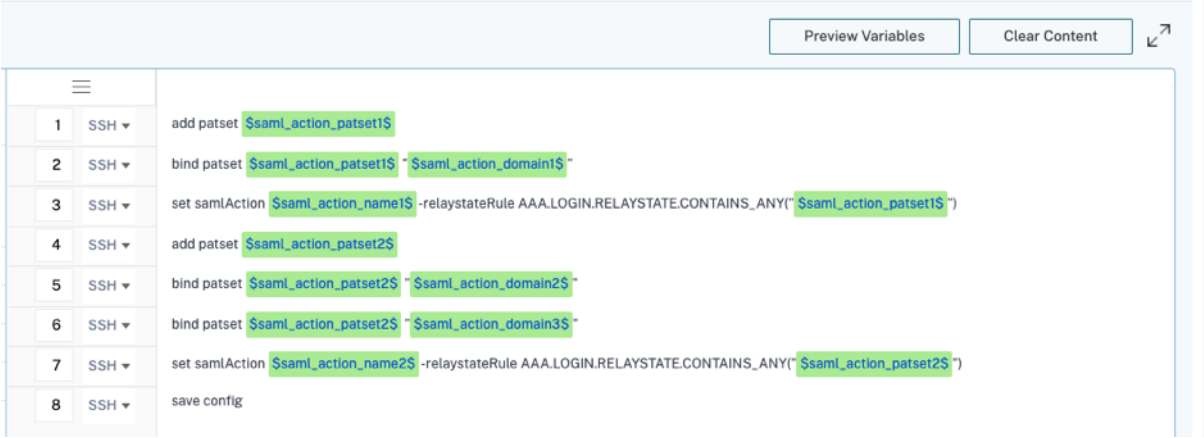
1. Actualice las tres instancias de ADC siguiendo los pasos que se indican en la sección "Actualizar una instancia"de este documento.
2. Aplique el parche de configuración a un ADC a la vez, mediante el flujo de trabajo de configuración. Consulte los pasos que se indican en la sección "Aplicar comandos de configuración"de este documento.

El ADC 1 vulnerable tiene dos acciones de SAML:

- La acción 1 de SAML tiene un dominio
- La acción 2 de SAML tiene dos dominios



Seleccione ADC 1 y haga clic en **Continuar con el flujo de trabajo de configuración**. La plantilla base integrada se rellena automáticamente. A continuación, asigne un nombre a la tarea y personalice la plantilla de acuerdo con la configuración dada.

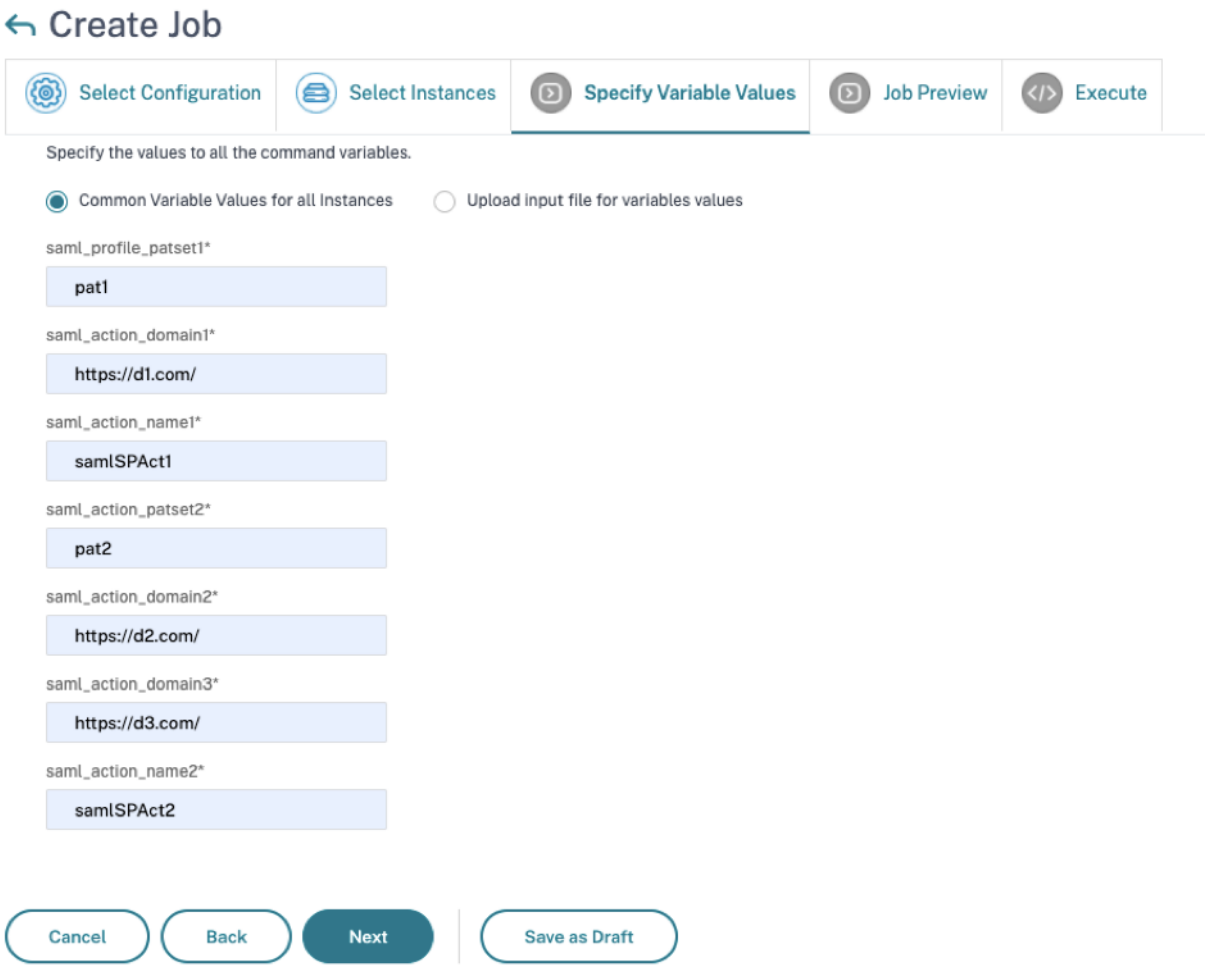


En la tabla siguiente se enumeran las definiciones de variables para los parámetros personalizados.

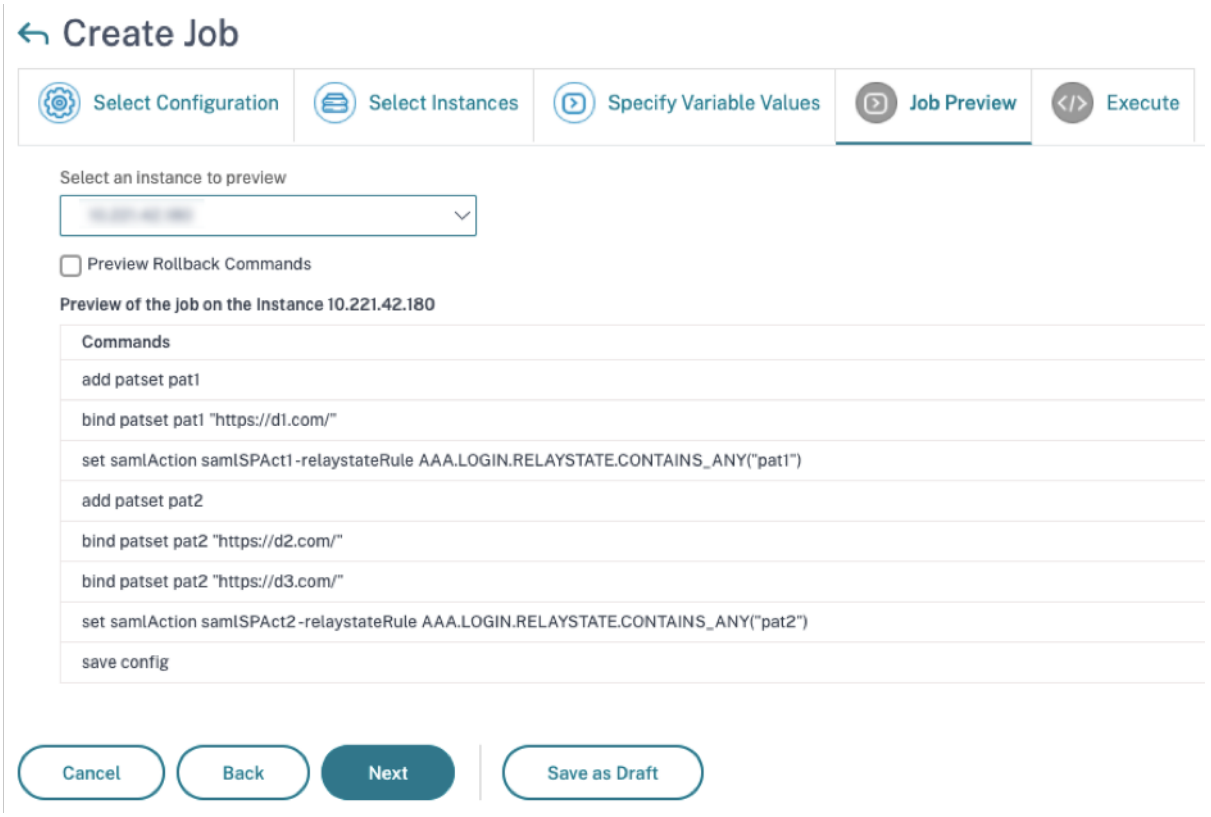
Tabla. Definiciones de variables para la acción SAML

Configuración ADC	Definición de variable para patset	Definición de variable para el nombre de la acción SAML	Definición de variable para dominio
La acción 1 de SAML tiene un dominio	saml_action_patset1	saml_action_name1	saml_action_domain1
La acción 2 de SAML tiene dos dominios	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

En **Seleccionar instancias**, seleccione ADC 1 y haga clic en **Siguiente**. Aparece la ventana **Especificar valores variables**. En este paso, debe proporcionar valores para todas las variables definidas en el paso anterior.



A continuación, revise las variables.



Haga clic en **Siguiente** y, después, en **Finalizar** para ejecutar el trabajo.

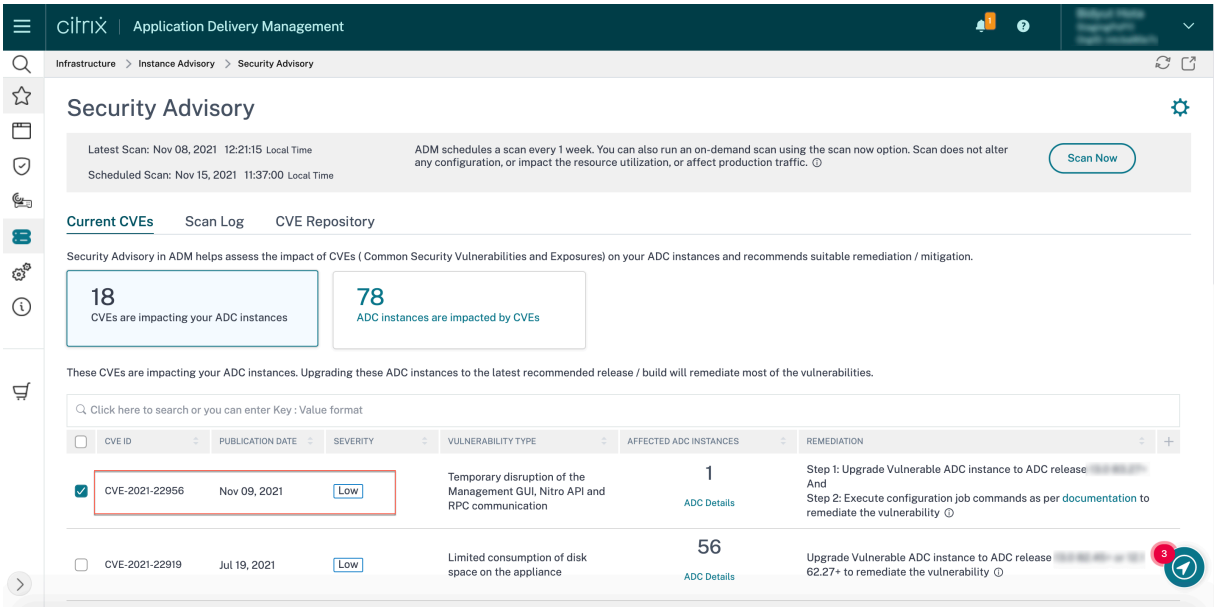
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para ADC1, siga los mismos pasos para corregir el ADC 2 y el ADC 3. Una vez finalizada la corrección, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

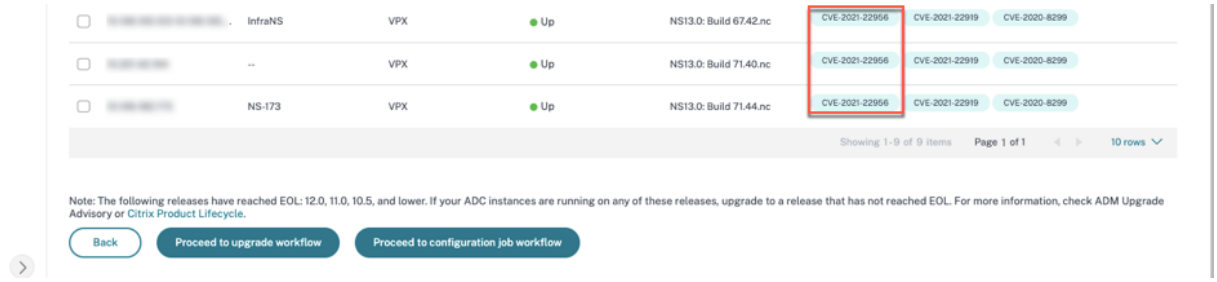
Identificar y corregir las vulnerabilidades del CVE-2021-22956

January 30, 2024

En el panel de asesoramiento de seguridad de NetScaler ADM, en CVE**actuales > Las instancias de< number of>**ADC se ven afectadas por vulnerabilidades y exposiciones (CVE) comunes, puede ver todas las instancias vulnerables debido a este CVE específico. Para comprobar los detalles de las instancias afectadas por el CVE-2021-22956, seleccione CVE-2021-22956 y haga clic en **Ver instancias afectadas**.



Aparecen las instancias de<number of>ADC afectadas por la ventana CVE. Aquí puede ver el recuento y los detalles de las instancias de ADC afectadas por el CVE-2021-22956.



Para obtener más información sobre el panel de asesoramiento de seguridad, consulte Asesoramiento de seguridad .

> **Nota**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde algún tiempo en concluir y reflejar el impacto del CVE-2021-22956 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, inicie un análisis bajo demanda haciendo clic en **Escanear ahora**.

Identifique las instancias afectadas por el CVE-2021-22956

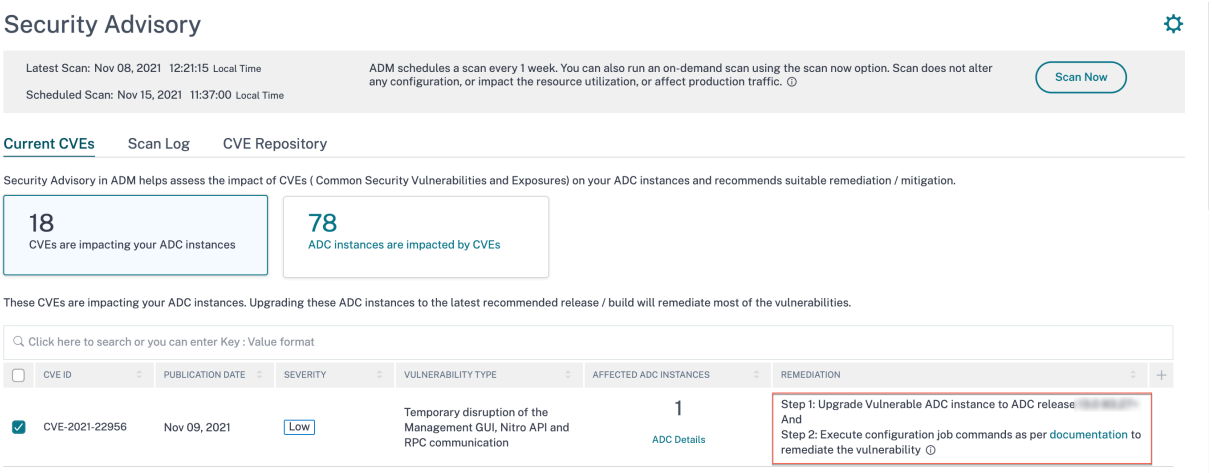
El CVE-2021-22956 requiere un escaneo personalizado, en el que el servicio ADM se conecta con la instancia ADC administrada y envía un script a la instancia. El script se ejecuta en la instancia ADC y comprueba los parámetros del archivo de configuración de Apache (`httpd.conf file`) y del número máximo de conexiones de cliente (`maxclient`) para determinar si una instancia es vulnerable o no. La información que el script comparte con el servicio ADM es el estado de la vulnerabilidad

en formato booleano (verdadero o falso). El script también devuelve al servicio ADM una lista de recuentos de max_clients para diferentes interfaces de red, por ejemplo, host local, NSIP y SNIP con acceso de administración.

Este script se ejecuta cada vez que se ejecutan los análisis programados bajo demanda. Una vez finalizado el escaneo, el script se elimina de la instancia de ADC.

Remediar CVE-2021-22956

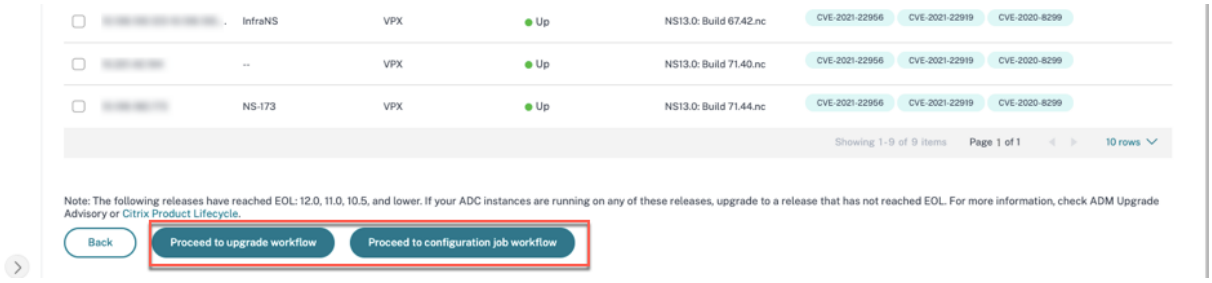
Para las instancias de ADC afectadas por el CVE-2021-22956, la corrección consiste en un proceso de dos pasos. En la GUI, en los**CVE actuales > Las instancias de ADC se ven afectadas por los CVE**, puede ver los pasos 1 y 2.



Los dos pasos incluyen:

1. Actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.
2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración.

En CVE actuales > Instancias de ADC afectadas por las CVE, verá dos flujos de trabajo independientes para este proceso de corrección de 2 pasos: Proceder a actualizar el flujo de trabajo y Proceder al flujo de trabajo de configuración.



Paso 1: Actualizar las instancias de ADC vulnerables

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.

Para obtener más información sobre cómo usar NetScaler ADM para actualizar las instancias de ADC, consulte Crear un trabajo de actualización de ADC.

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de ADC vulnerables.

Paso 2: Aplicar los comandos de configuración

Tras actualizar las instancias afectadas, en la ventana **<number of> Instancias de ADC afectadas por los CVE**, seleccione la instancia afectada por el CVE-2021-2295 y haga clic en **Continuar con el flujo de trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

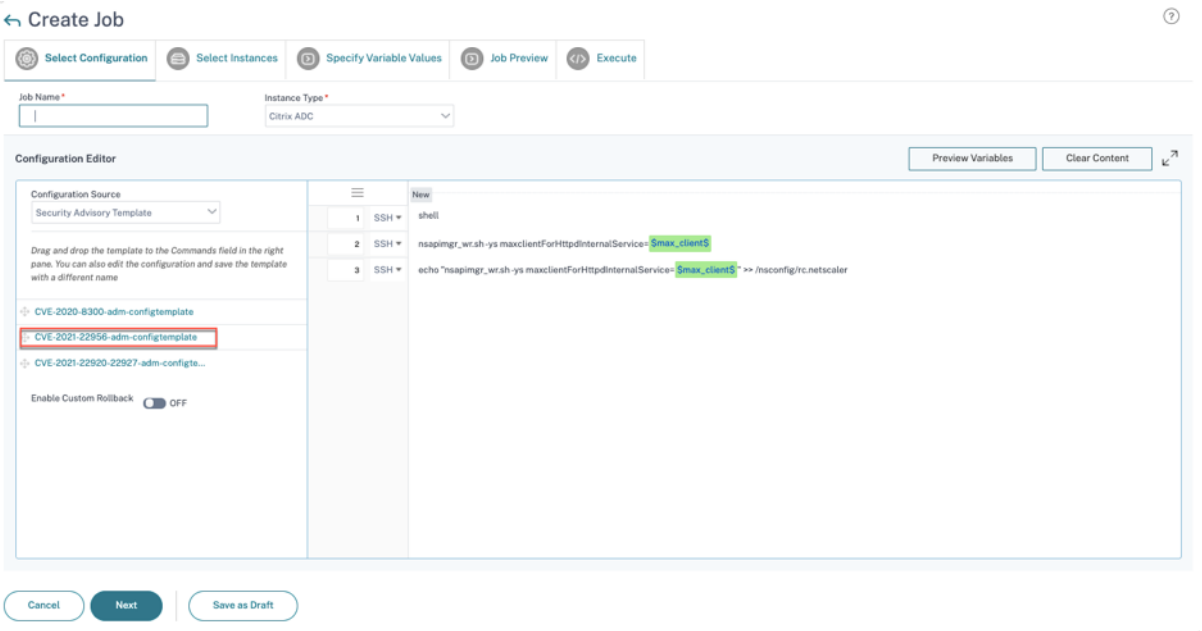
1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.
5. Ejecutar el trabajo.

Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**:

- Para una instancia de ADC afectada por varios CVE (como CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 y CVE-2021-22956): al seleccionar la instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**, la plantilla de configuración integrada no se rellena automáticamente en Seleccionar configuración. Arrastre y suelte la plantilla de trabajo de configuración correspondiente en la sección **Plantilla de asesoramiento de seguridad** manualmente en el panel de tareas de configuración del lado derecho.
- Para varias instancias de ADC que se ven afectadas únicamente por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene ADC 1, ADC 2 y ADC 3, y todos ellos se ven afectados únicamente por el CVE-2021-22956. Seleccione todas estas instancias y haga clic en **Continuar con el flujo de trabajo de configuración**, y la plantilla de configuración integrada se rellenará automáticamente en **Seleccionar configuración**. Consulte el problema conocido NSADM-80913 en las notas de la versión.
- Para varias instancias de ADC afectadas por CVE-2021-22956 y uno o más CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren una corrección para aplicarla a cada

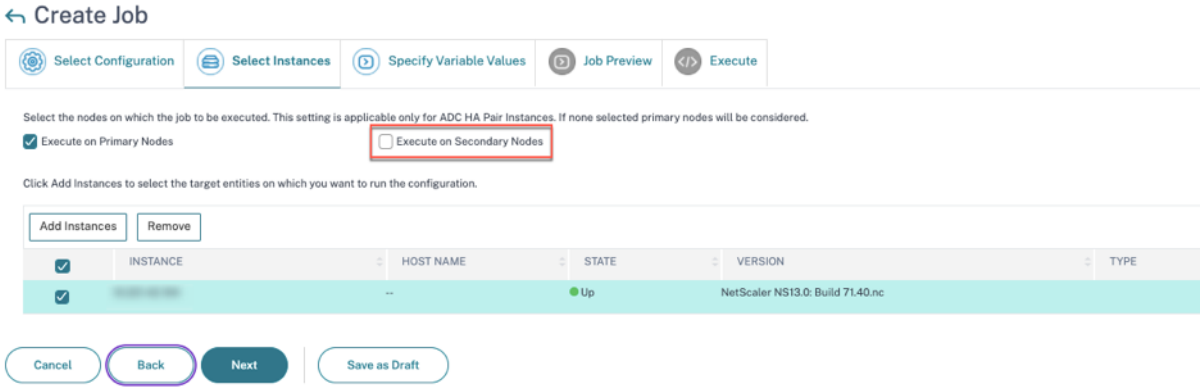
ADC a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo de configuración**, se produce un error aparece un mensaje que le indica que ejecute el trabajo de configuración en cada ADC a la vez.

Paso 1: Seleccione la configuración En el flujo de trabajo de configuración, la plantilla base de configuración integrada se rellena automáticamente en **Seleccionar configuración**.



Paso 2: selecciona la instancia

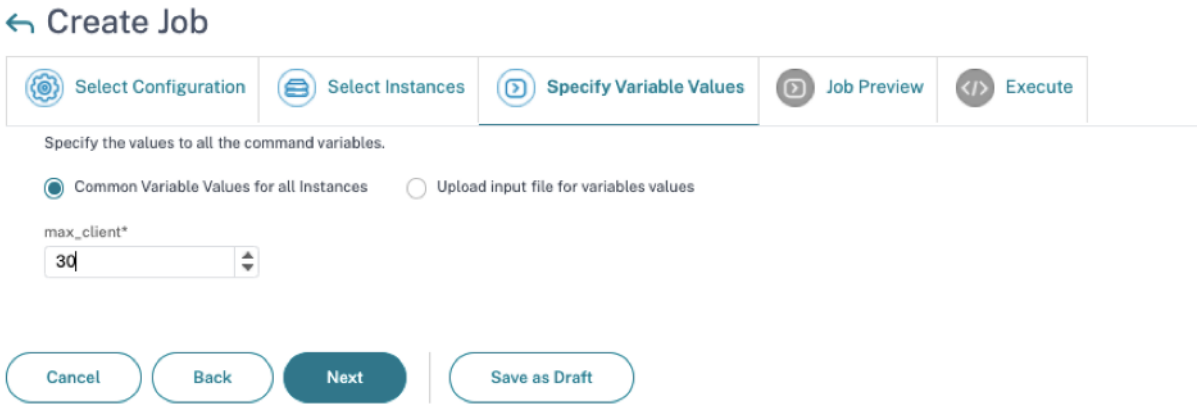
La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia. Si esta instancia forma parte de un par de HA, seleccione **Ejecutar en nodos secundarios**. Haz clic en **Siguiente** .



> **Nota**
>
> Para las instancias de ADC en modo clúster, mediante el asesoramiento de seguridad de ADM, ADM permite ejecutar el trabajo de configuración solo en el nodo del coordinador de configuración del clúster (CCO). Ejecute los comandos en nodos que no sean de CCO por separado.

`rc.netscaler` se sincroniza en todos los nodos de alta disponibilidad y del clúster, lo que hace que la corrección sea persistente después de cada reinicio.

Paso 3: especificar los valores de las variables Introduzca los valores de las variables.



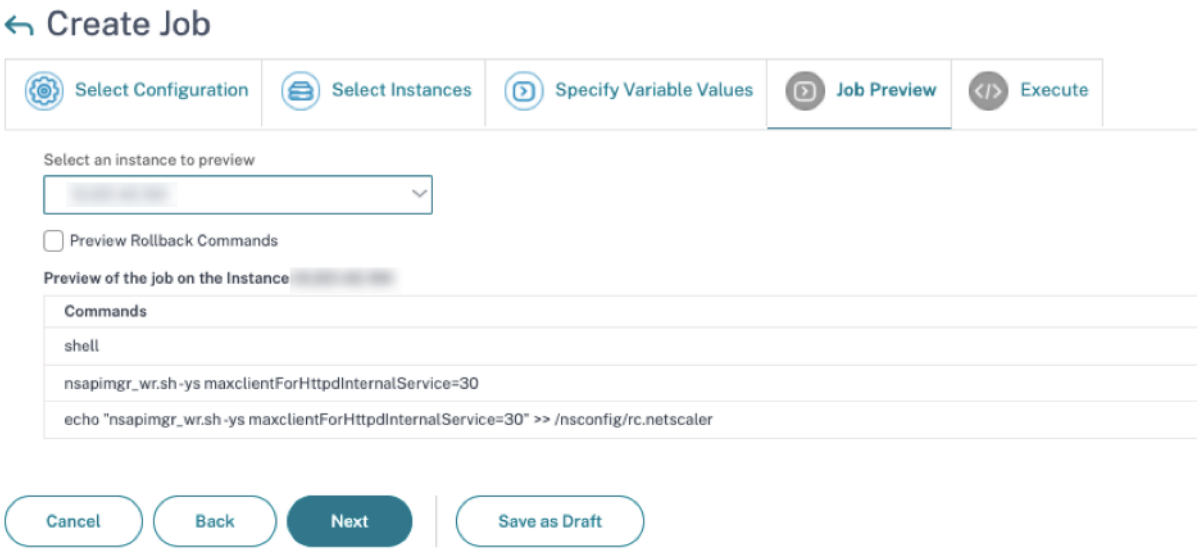
Seleccione una de las siguientes opciones para especificar las variables de sus instancias:

Valores de variables comunes para todas las instancias: introduzca un valor común para la variable `max_client`.

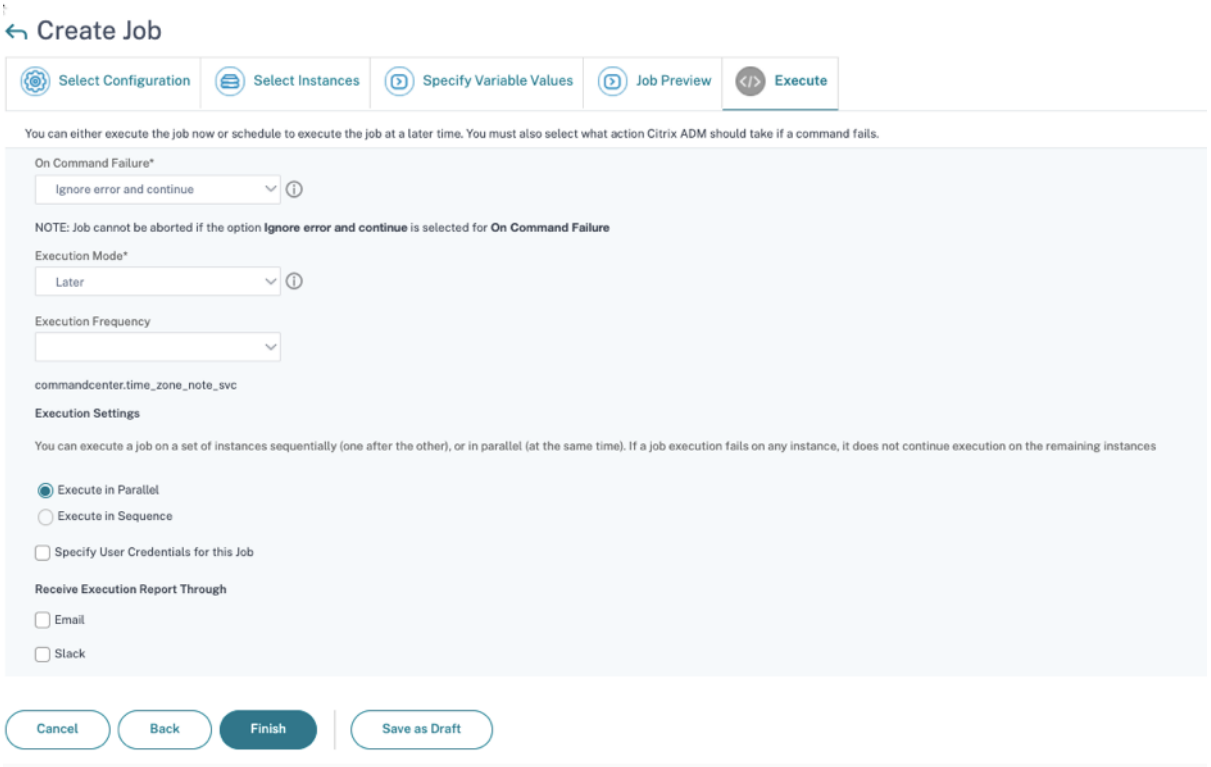
Cargar archivo de entrada para valoresde variables : haga clic en **Descargar archivo de claves** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca los valores de la variable `max_client` y, a continuación, suba el archivo al servidor ADM. Consulte el problema conocido NSADM-80913 en las notas de la versión, notas sobre un problema relacionado con esta opción.

> **Nota**
>
> Para las dos opciones mencionadas anteriormente, el valor `max_client` recomendado es 30. Puede establecer el valor de acuerdo con su valor actual. Sin embargo, no debe ser cero y debe ser inferior o igual al conjunto max_client del archivo `/etc/httpd.conf`. Puede comprobar el conjunto de valores actuales en el archivo de configuración `/etc/httpd.conf` del servidor HTTP Apache buscando la cadena `MaxClients`, en la instancia de ADC.

Paso 4: Vista previa de la configuración Previsualiza los valores de las variables que se han insertado en la configuración y haga clic en **Siguiente**.



Paso 5: Ejecute el trabajo Haga clic en **Finalizar** para ejecutar el trabajo de configuración.



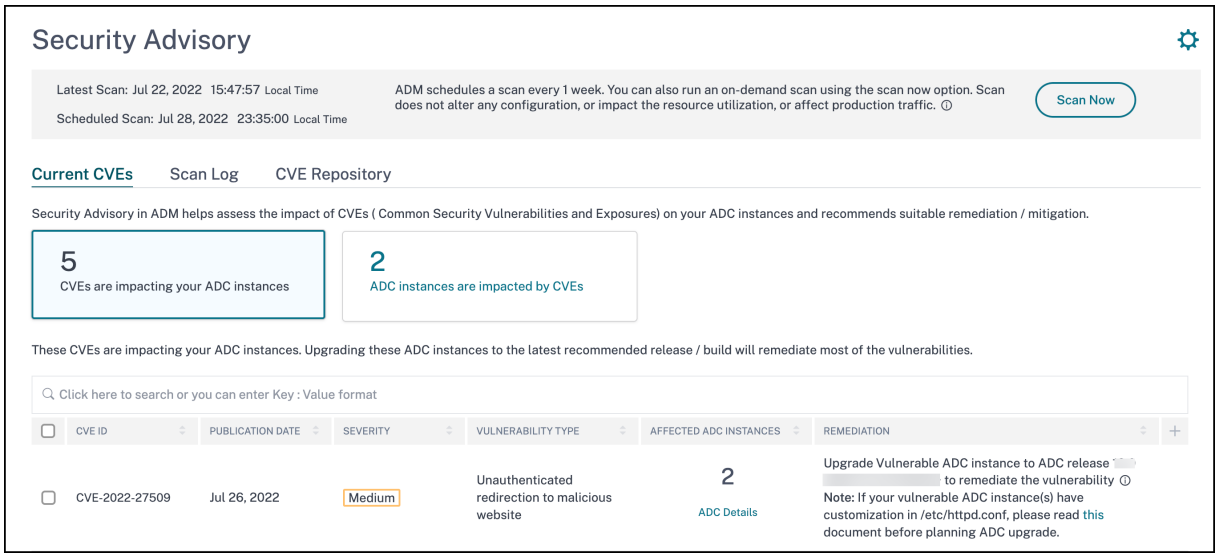
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para todos los ADC vulnerables, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Identificar y corregir las vulnerabilidades del CVE-2022-27509

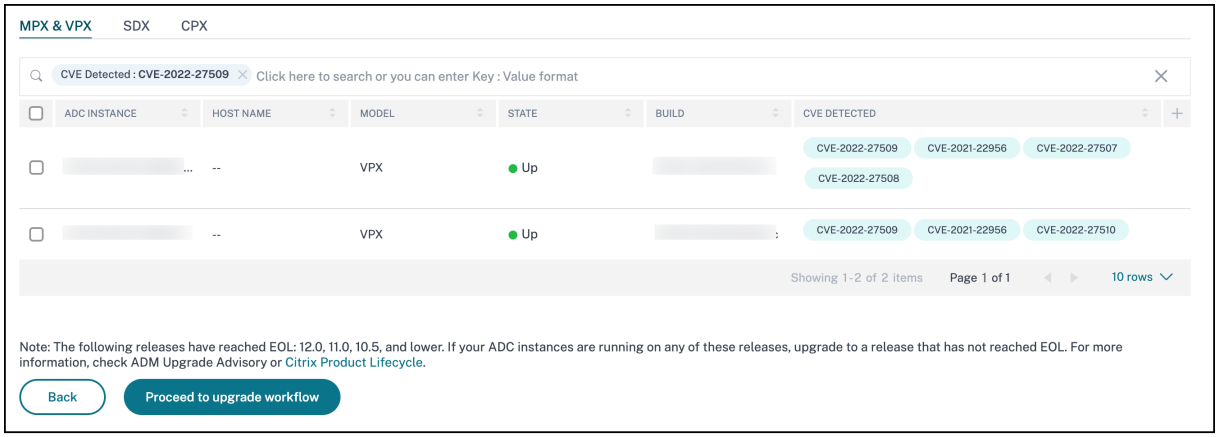
January 30, 2024

En el panel de consejos de seguridad de NetScaler ADM, en **CVE actuales Las instancias de <number of> ADC se ven afectadas por las CVE**, puede ver todas las instancias vulnerables debido a CVE-2022-27509. Para comprobar los detalles de las instancias afectadas por los CVE, seleccione CVE-2022-27509 y haga clic en **Ver instancias afectadas**.



> **Nota**
>
> Para entender el motivo de la vulnerabilidad de ADC, descargue el informe CSV en la ficha Registros de escaneo del Aviso de seguridad.

Aparece la ventana **<number of>Instancias de ADC afectadas por los CVE**. En la siguiente captura de pantalla, puede ver el recuento y los detalles de las instancias de ADC afectadas por el CVE-2022-27509.



Para obtener más información sobre el panel de asesoramiento de seguridad, consulte Asesoramiento de seguridad .

> **Nota**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde un par de horas en concluir y reflejar el impacto del CVE-2022-27509 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, inicie un análisis bajo demanda haciendo clic en **Escanear ahora**.

Identifique las instancias afectadas por el CVE-2022-27509

El CVE-2022-27509 requiere una combinación de escaneo personalizado y escaneo de versiones. Como parte del escaneo personalizado, el servicio ADM se conecta con la instancia de ADC administrada y envía un script a la instancia. El script se ejecuta en la instancia de ADC y determina si la instancia es vulnerable. Este script se ejecuta cada vez que se ejecuta el análisis programado o bajo demanda.

Una vez finalizado el escaneo, el script se elimina de la instancia de ADC.

También puede optar por no recibir estos escaneos personalizados de asesoramiento de seguridad. Para obtener más información sobre la configuración de escaneo personalizado y la inhabilitación de los escaneos personalizados, consulte la sección **Configurar la configuración del escaneo personalizado** en la página de **consejos de seguridad**.

Remediar CVE-2022-27509

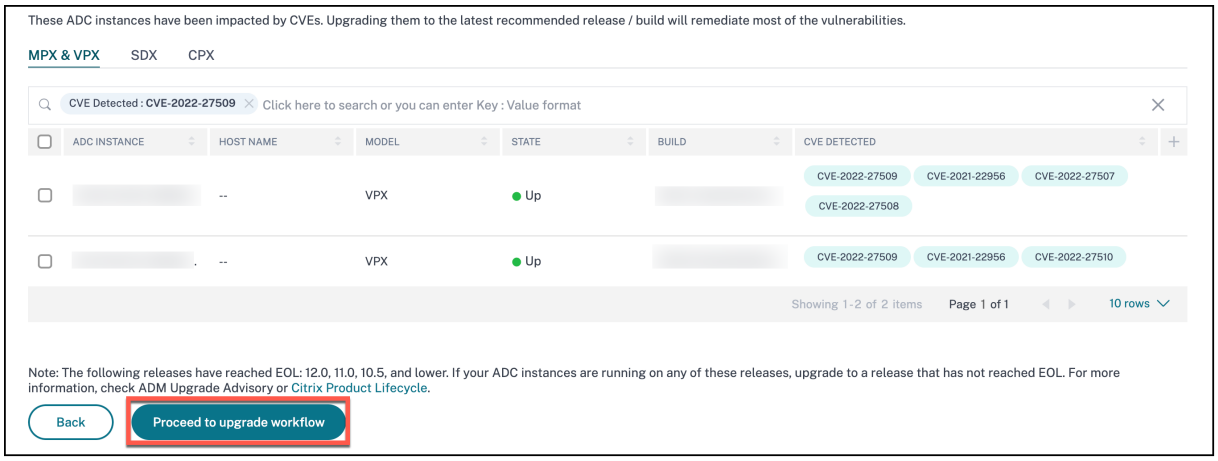
Para las instancias de ADC afectadas por el CVE-2022-27509, la corrección es un proceso de un solo paso y es necesario actualizar las instancias de ADC vulnerables a una versión y una compilación que tengan la solución. En la GUI, en los **CVE actuales > Las instancias de ADC se ven afectadas por las CVE**, puede ver el paso a seguir para solucionarlo.

En **CVE actuales > Instancias de ADC afectadas por las CVE**, verá el siguiente flujo de trabajo para este proceso de corrección de un solo paso, que es **Proceder a actualizar el flujo de trabajo**.

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.

> **IMPORTANTE**
>
> Si sus instancias de ADC vulnerables tienen el archivo /etc/httpd.conf copiado al directorio /nsconfig, consulte Consideraciones de actualización para configuraciones de ADC personalizadas antes de planificar la actualización del ADC.

Para obtener más información sobre cómo usar NetScaler ADM para actualizar las instancias de ADC, consulte Crear un trabajo de actualización de ADC.



CVE no compatibles en el asesoramiento de seguridad

January 30, 2024

El asesoramiento de seguridad de NetScaler ADM hace un seguimiento de todas las nuevas vulnerabilidades y exposiciones comunes (CVE) y evalúa el impacto de las CVE en la infraestructura. Puede revisar las recomendaciones y tomar las medidas adecuadas. Sin embargo, hay algunos CVE que no son compatibles y la detección y la corrección de las vulnerabilidades están fuera del alcance del asesoramiento de seguridad de NetScaler ADM.

- **CVE-2022-21827**:

  El CVE-2022-21827 afecta al complemento de NetScaler Gateway para las versiones compatibles con Windows anteriores a la 21.9.1.2.

  NetScaler ADM no admite la detección y la corrección de las vulnerabilidades que afectan al complemento de NetScaler Gateway para Windows. Además, las vulnerabilidades de los complementos de NetScaler Gateway no se pueden evaluar realizando comprobaciones en el ADC, verificando la versión de ADC o comprobando la configuración del ADC. La detección y la corrección de este CVE solo se pueden evaluar en función de la versión del complemento NetScaler Gateway para Windows implementada en el cliente.

  Como resultado, la detección y la corrección de esta vulnerabilidad están fuera del alcance del asesoramiento de seguridad de NetScaler ADM.

Aviso de actualización (versión preliminar)

January 30, 2024

Como administrador de red, puede administrar muchas instancias de ADC que se ejecutan en diferentes compilaciones de ADC en NetScaler ADM. Supervisar el ciclo de vida de cada instancia de ADC puede ser una tarea engorrosa. Debe visitar la matriz de productos de NetScalere identificar las instancias de ADC que están llegando o han llegado al final de su vida útil (EOL) o al final del mantenimiento (EOM). Luego, planea su actualización.

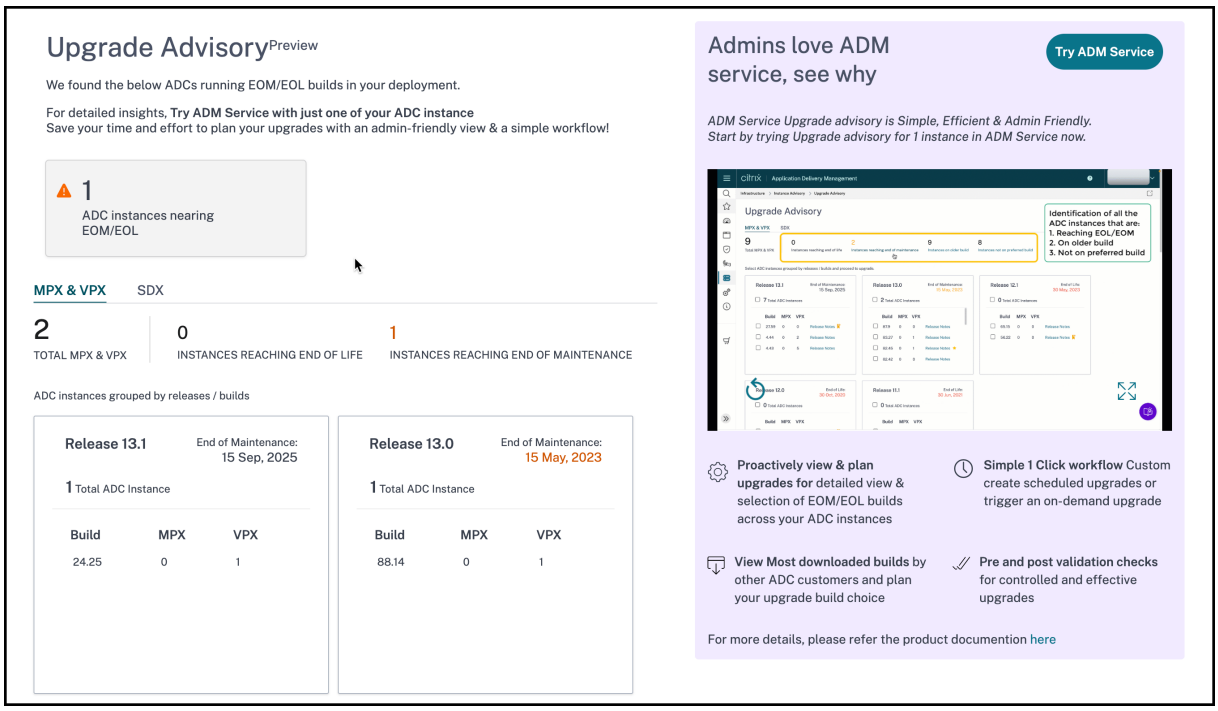
El aviso de actualización local de NetScaler ADM realiza un escaneo de versiones en los ADC y proporciona una vista de las compilaciones de EOM/EOL en todas sus instancias de ADC.

> **IMPORTANTE**
>
> Para obtener información detallada y el flujo de trabajo necesario para actualizar las instancias de ADC, **pruebe NetScaler ADM Service**.

Consultar el aviso de actualización

Vaya a **Infraestructura > Asesoramiento de instancias > Asesoramiento de actualizaciones** y consulte la siguiente información:

- Recuento total de instancias de ADC.
- Instancias que llegan al final de la vida.
- Instancias que llegan al final del mantenimiento.



La página **Asesor de Actualización** agrupa las instancias de ADC por sus versiones.

El aviso de actualización local de NetScaler ADM también le permite seleccionar una de las instancias de ADC e incorporarla al servicio ADM. Haga clic en **Probar el servicio ADM** e incorpore la instancia de ADC al servicio ADM. El aviso de actualización del servicio de ADM le proporciona el flujo de trabajo para actualizar según la instancia de ADC seleccionada.

Para obtener más información sobre el aviso de actualización del servicio ADM, consulte la animación gif en la página de consejos de **actualización**.

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

NetScaler Application Delivery Management (ADM) admite el SDN en la red empresarial mediante la integración con los controladores SDN de diferentes proveedores. NetScaler ADM es compatible con VMware NSX Manager y Cisco Application Policy Infrastructure Controller (APIC).

VMware NSX Manager

NetScaler ADM se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios de NetScaler. Esta integración elimina las complejidades tradicionales asociadas a la topología de red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios de NetScaler mediante programación 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 NetScaler ADM permite la integración de los productos de NetScaler con VMware NSX y proporciona las siguientes capacidades:

- 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, 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 un VPX de una determinada puerta de enlace Edge 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 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 usuarios y modelo de consumo de autoservicio, al tiempo que proporciona 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 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 directivas de aplicaciones (APIC) y, al mismo tiempo, delegar la configuración L4-L7 a NetScaler ADM, que actúa como administrador de dispositivos en el APIC.

La solución NetScaler Hybrid Mode es compatible con un paquete de dispositivos de modo híbrido y NetScaler ADM. Debe cargar el paquete de dispositivos de modo híbrido en la APIC. Para obtener más información, consulteNetScaler Automation Using NetScaler ADM in Cisco ACI Hybrid Mode.

OpenStack: Integración de instancias NetScaler

January 30, 2024

La función Cloud Orchestration de NetScaler Application Delivery Management (ADM) permite la integración de los productos de NetScaler 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. Después de esto, los usuarios de OpenStack pueden implementar sus configuraciones de balanceador de carga desde OpenStack en la instancia de NetScaler.

Las siguientes secciones proporcionan una breve descripción de las funciones del flujo de trabajo de integración de NetScaler ADM y OpenStack.

Controlador NetScaler para OpenStack Neutron LBaaS

El complemento LBaaS de OpenStack Neutron incluye un controlador de NetScaler que permite a OpenStack comunicarse con NetScaler ADM. OpenStack utiliza este controlador para reenviar

cualquier configuración 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 deseadas. OpenStack también usa el controlador para llamar a NetScaler ADM a intervalos regulares a fin de recuperar el estado de las diferentes entidades (como los VIP y los grupos) de todas las configuraciones de equilibrio de carga de NetScaler. El software de controlador NetScaler para la plataforma OpenStack se incluye junto con el ADM de NetScaler. Para descargar e instalar los controladores, primero debe instalar NetScaler ADM e iniciar la aplicación.

Registrar NetScaler 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 en la nube, así como las credenciales de usuario del controlador OpenStack NetScaler. Más adelante, puede especificar las mismas credenciales de inicio de sesión en la sección NetScaler_Driver del archivo de configuración de Neutron (neutron.conf) para que el controlador NetScaler de OpenStack pueda conectarse a NetScaler ADM durante las configuraciones de LB.

Una vez que OpenStack y NetScaler ADM se hayan registrado entre sí, 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 ADM de NetScaler y comprobar el rendimiento de sus configuraciones de LB en NetScalers.

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 directivas de ubicación ofrecen la flexibilidad necesaria para decidir la instancia de NetScaler que se utiliza en cada configuración de balanceador de carga creada por los usuarios. Como alternativa, el ADM de NetScaler también ofrece una opción para asignar una instancia de NetScaler en función de los arrendatarios 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 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 NetScaler ADM con OpenStack Workflow
- Prerequisites
- Tareas previas a la configuración en NetScaler ADM y OpenStack
- Pasos de configuración de LBaaS V1 con Horizon
- Pasos de configuración para LBaaS V2 mediante línea de comandos
- Provisioning manual de una instancia de NetScaler VPX en OpenStack
- Integración de NetScaler ADM con OpenStack Heat Services
- Supervisión de aplicaciones OpenStack en NetScaler ADM

Escenario de caso de uso

En el siguiente caso de uso se explica el flujo de trabajo de integración 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 dedicado para equilibrar la carga entre los servidores S1 y S2 en la plataforma OpenStack.

Para cumplir con este requisito, Steve tiene que instalar y configurar tanto OpenStack como NetScaler ADM, y prepararlos para que sean compatibles 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 NetScaler ADM y configurar el controlador LBaaS de NetScaler en el componente de red de OpenStack, Neutron. Una vez finalizado el registro, NetScaler ADM muestra los detalles de todos los arrendatarios de OpenStack. Steve puede seleccionar Example-SportsOnline de la lista de personas que desean las funciones de NetScaler LBaaS y configurar a Tom para que asigne un NetScaler dedicado a sus configuraciones de balanceador de carga en NetScaler ADM.

Para ello, Steve puede aprovisionar una instancia de NetScaler VPX en la capa informática (Nova) de OpenStack mediante la interfaz de usuario ADM de NetScaler o permitir que MAS aprovisione automáticamente una instancia de NetScaler VPX a pedido, cuando Tom realice su configuración de LB en OpenStack. En cualquier caso, NetScaler ADM administra la instancia VPX. Para lograrlo, Steve crea un paquete de servicios en NetScaler 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 NetScaler VPX al paquete de servicios y asocia Example-SportsOnline, junto con otros arrendatarios, que necesitan un NetScaler dedicado al paquete de servicios. Como resultado, cuando Tom realiza su primera configuración de balanceador de carga, NetScaler ADM asigna una de las instancias de NetScaler VPX del paquete de servicios a Example-SportsOnline y también implementa su configuración en ese NetScaler.

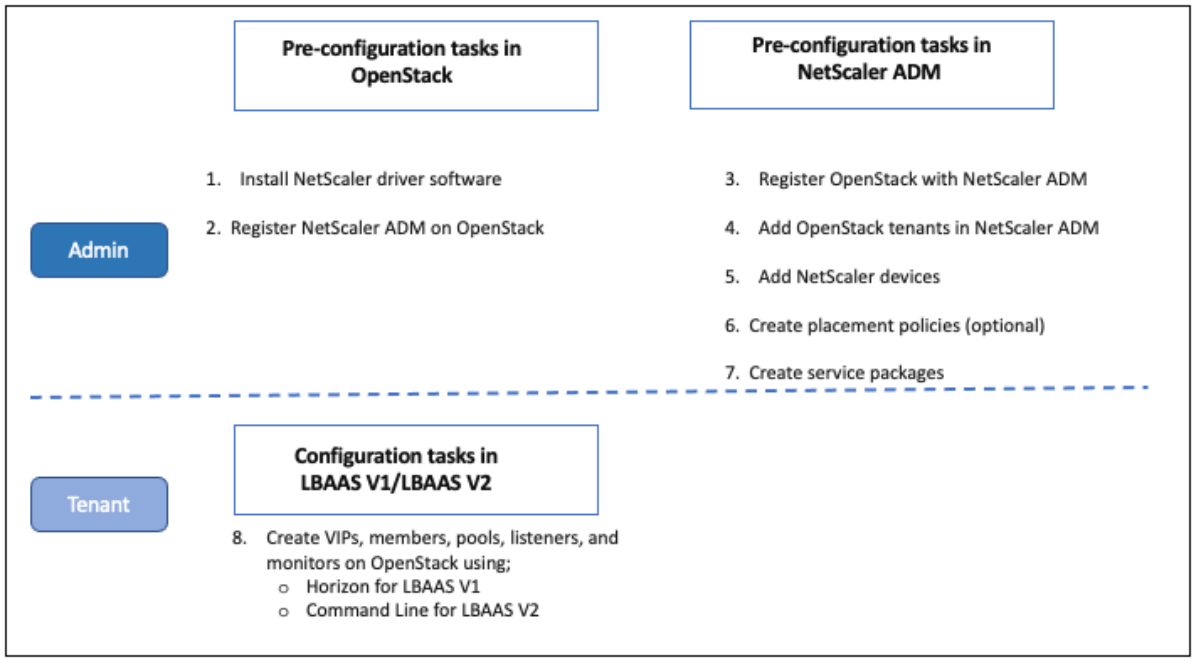
Tom ahora puede crear configuraciones de equilibrio de carga mediante la creación de grupos, IP virtuales (VIP) y monitores de salud mediante OpenStack LBaaS/UI. Los grupos y los VIP de OpenStack se implementan como grupos de servicios y servidores virtuales en la instancia de NetScaler. Tom

también puede crear monitores de estado para supervisar los servidores y enviar el tráfico de aplicaciones únicamente a los servidores que estén activos en cualquier momento y a los que se pueda acceder desde NetScaler.

La configuración de equilibrio de carga creada en OpenStack ahora se implementa en la instancia de NetScaler. Una vez configurada completamente, la instancia de NetScaler 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 NetScaler ADM con OpenStack Workflow

El siguiente diagrama de flujo muestra el flujo de trabajo que debe seguir al configurar LBaaS V1 y LBaaS V2.



NSX Manager: Provisioning manual de instancias de NetScaler

January 30, 2024

NetScaler 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 de NetScaler. Esta integración elimina las complejidades tradicionales asociadas a la topología de red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios de NetScaler mediante programación con mayor rapidez.

En este artículo se proporciona una lista de las tareas que debe realizar tanto en VMware NSX Manager como en NetScaler 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 13.1, en cualquiera de los hipervisores compatibles, consulte Implementación de NetScaler ADM.

Requisitos de hardware de VMware ESXi

La siguiente tabla muestra los recursos informáticos virtuales que necesita en su servidor VMware ESXi para instalar un dispositivo virtual NetScaler 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 NetScaler ADM en el servidor VMware ESXi, teniendo en cuenta que no hay otras máquinas

> virtuales en ejecución en el host. Los requisitos de hardware del servidor VMware ESXi dependen de la cantidad de máquinas virtuales que se ejecuten en él.

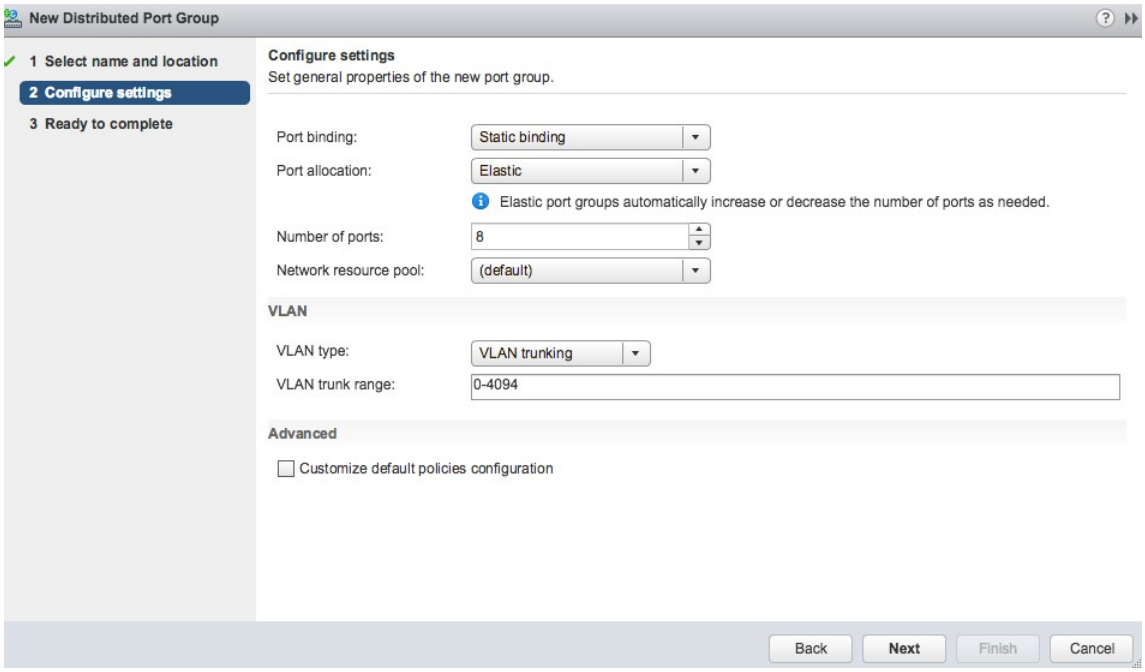
Configuración de VMware NSX

- Cree un grupo de instancias de NetScaler VPX de diferentes capacidades, que se agregarán a los diferentes paquetes de servicios.

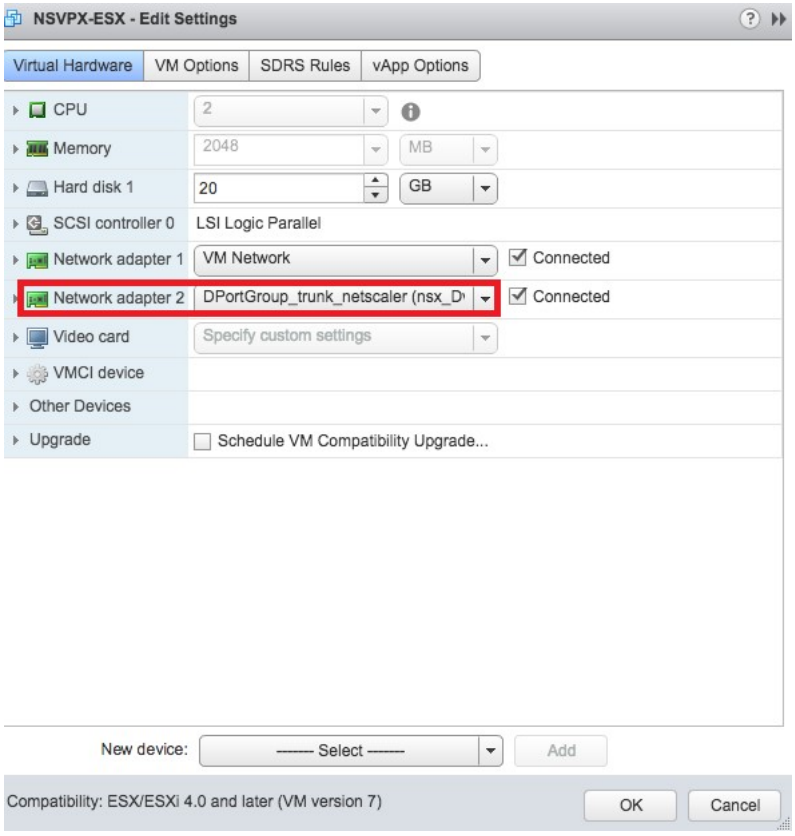
Por ejemplo:

- Cree cinco instancias VPX de VPX1000 de NetScaler (1 Gbps). Estas instancias se agregan al paquete de servicios Gold.
- Cree cinco instancias VPX de VPX10 (10 Mbps) de NetScaler. 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).

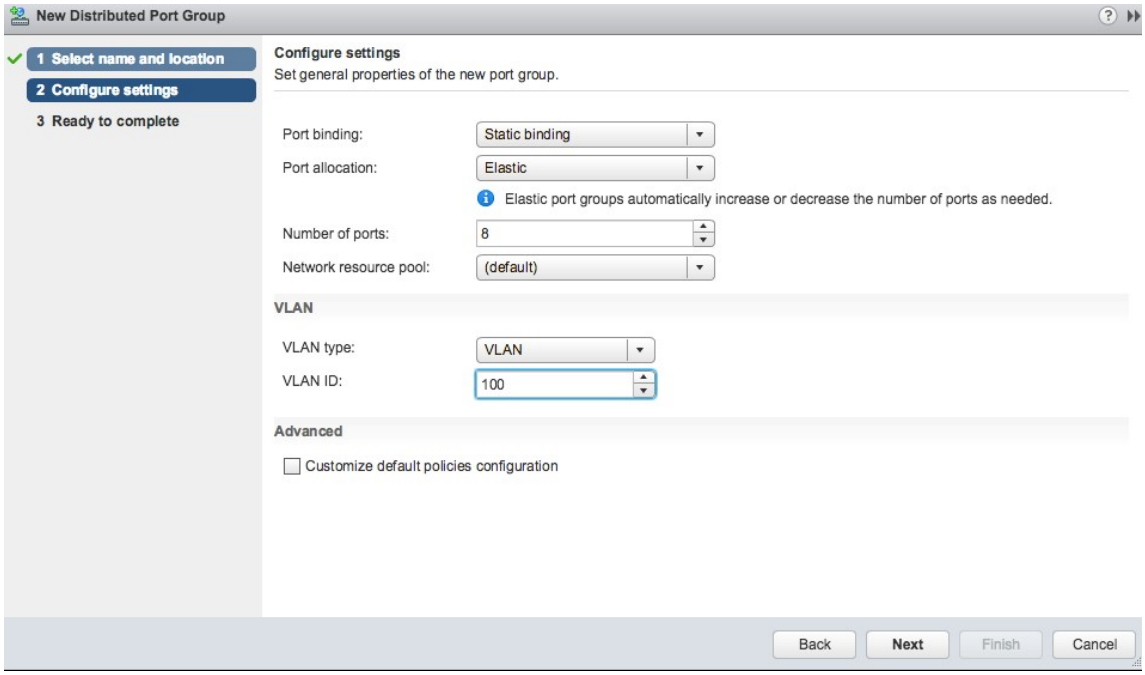


2. Cree una nueva interfaz para cada instancia de NetScaler VPX y conéctela al grupo de puertos troncal de rango de VLAN creado anteriormente.



3. En el cliente vSphere, vaya a **Redes**y cree un grupo de puertos de tipo VLAN.

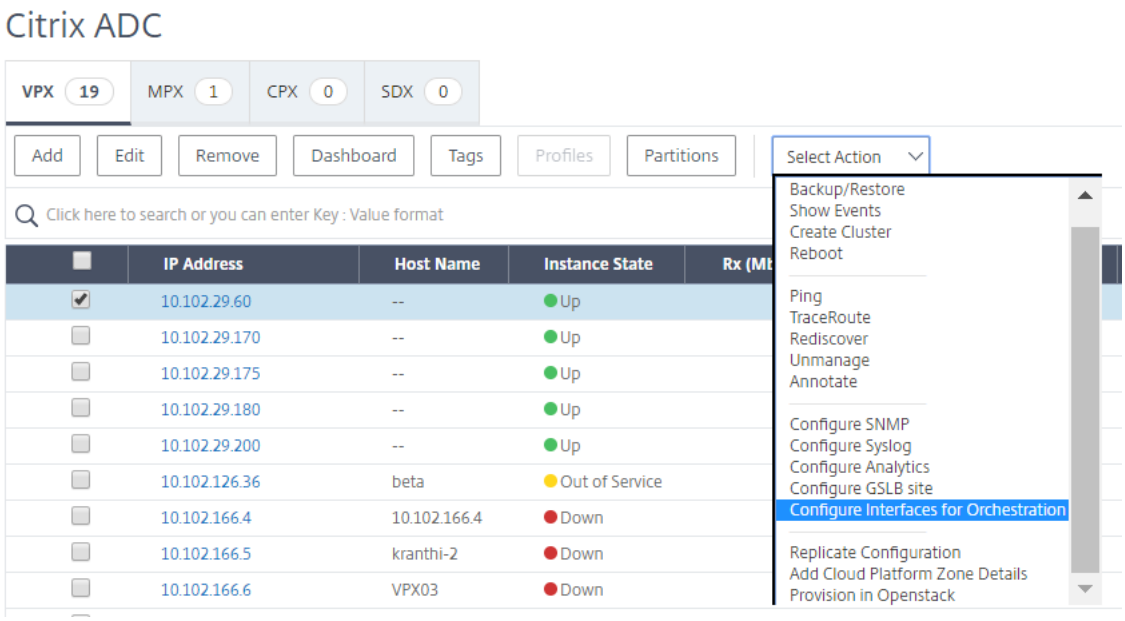
   Por ejemplo, si el grupo de puertos troncal inicial se creó con el rango 101-105, cree cinco grupos de puertos VLAN uno por VLAN, es decir, un grupo de puertos con VLAN 101, otro con VLAN102, etc., hasta VLAN 105.



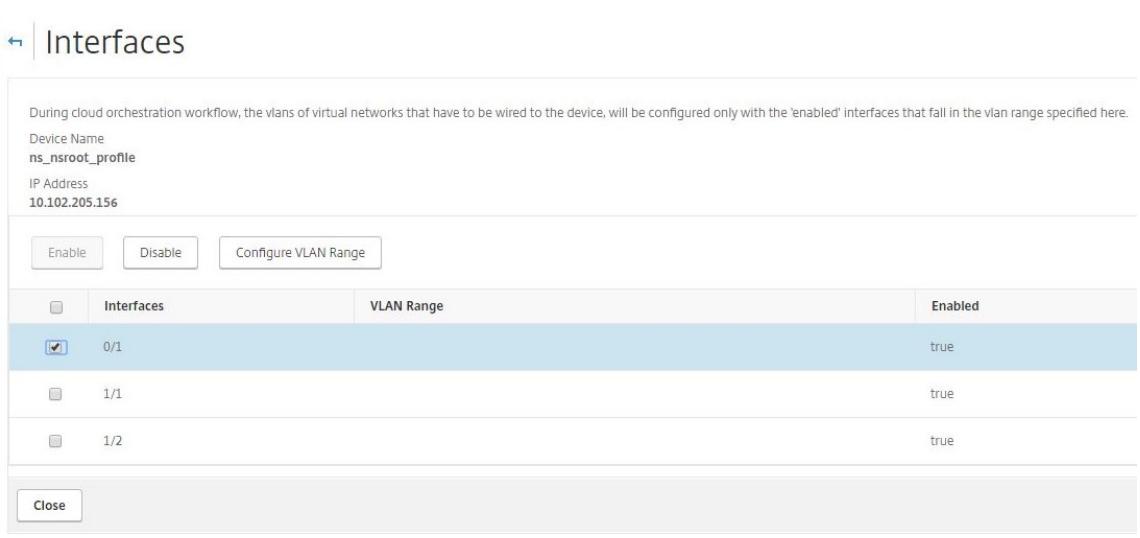
Adición de una instancia NetScaler VPX en NetScaler ADM

Agregue instancias de NetScaler VPX en NetScaler ADM y especifique el rango de VLAN del grupo troncal para cada dispositivo.

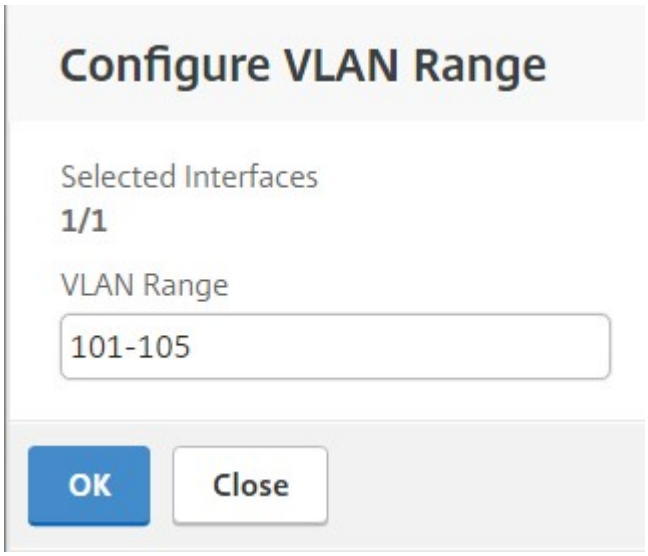
1. **En NetScaler ADM, vaya a**Infraestructura**>**Instancias**>**NetScaler VPX**y haga clic en Agregar.**
2. En la página **Agregar NetScaler VPX**, especifique los nombres de host de las instancias, la dirección IP de cada instancia o un rango de direcciones IP y, a continuación, seleccione un perfil de instancia de 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 NetScaler VPX recién agregada de la lista de la página de**NetScaler 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

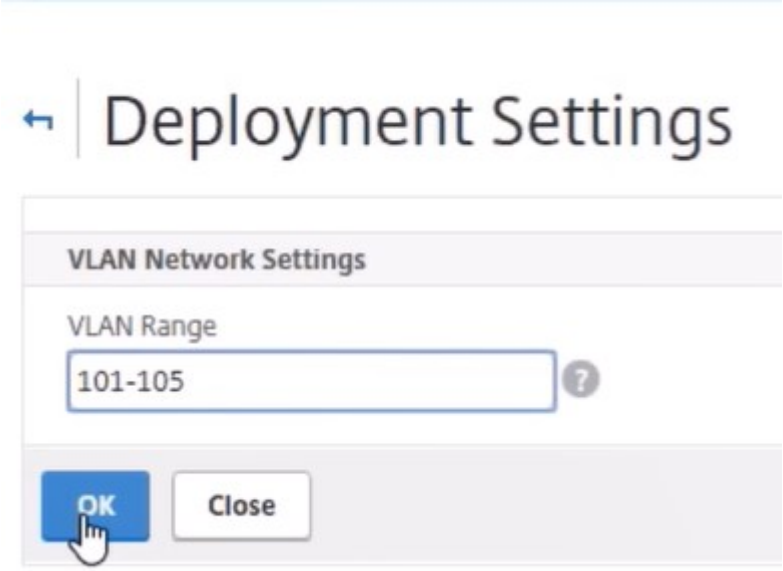
Registre VMware NSX manager con NetScaler ADM para crear un canal de comunicación entre ellos.

1. **En NetScaler ADM, vaya a**Orchestration >**SDN Orchestration>**VMware NSX Manager en la lista desplegable y haga clic en Configurar los ajustes 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.

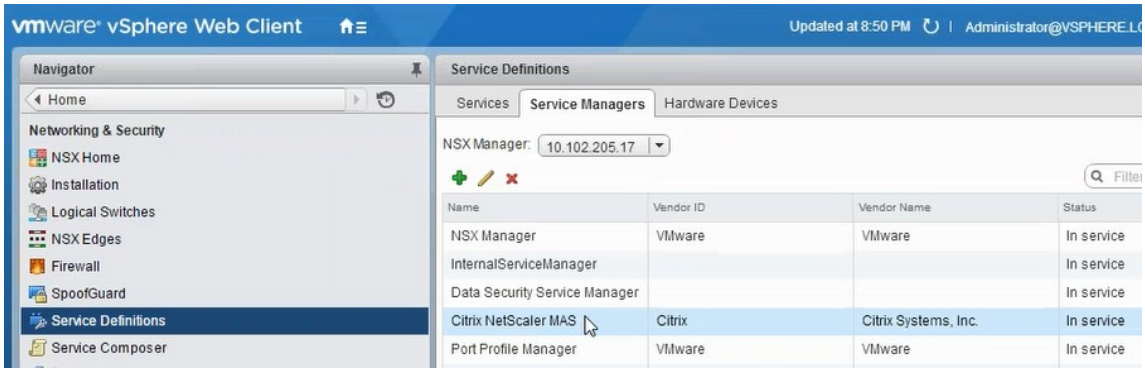
c) Contraseña: Contraseña del usuario administrativo de NSX Manager.

3. En la sección **Cuenta de NetScaler ADM utilizada por NSX Manager**, establezca el nombre de usuario y la contraseña de NetScaler Driver 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 NetScaler 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.

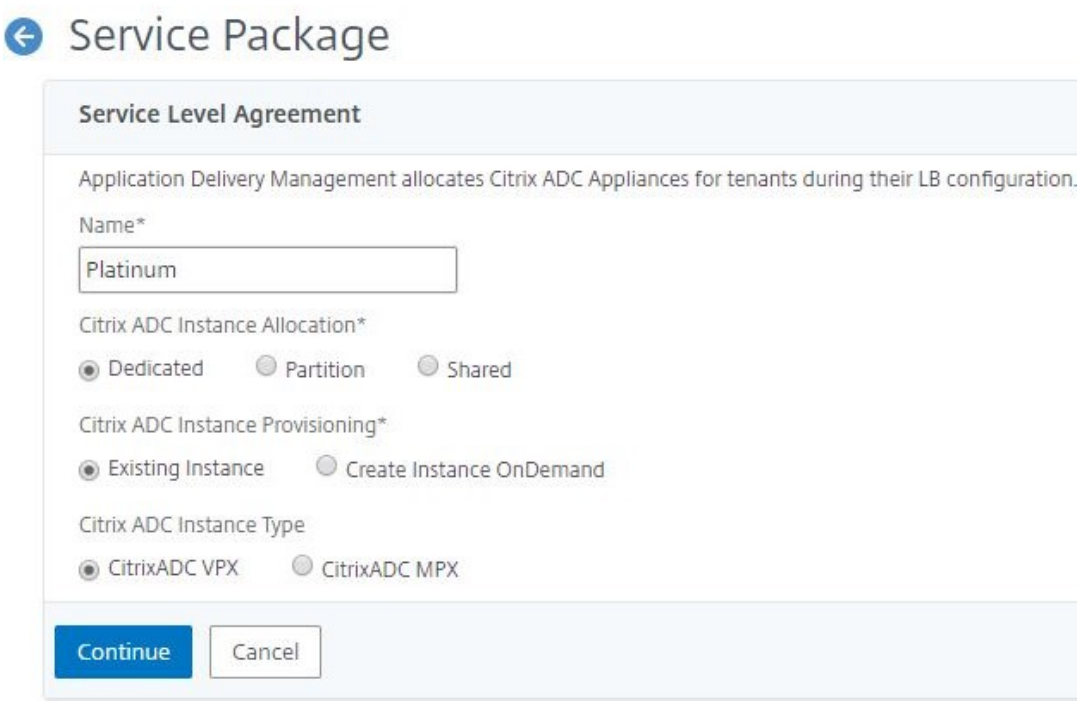


Creación de un Service Package en NetScaler ADM

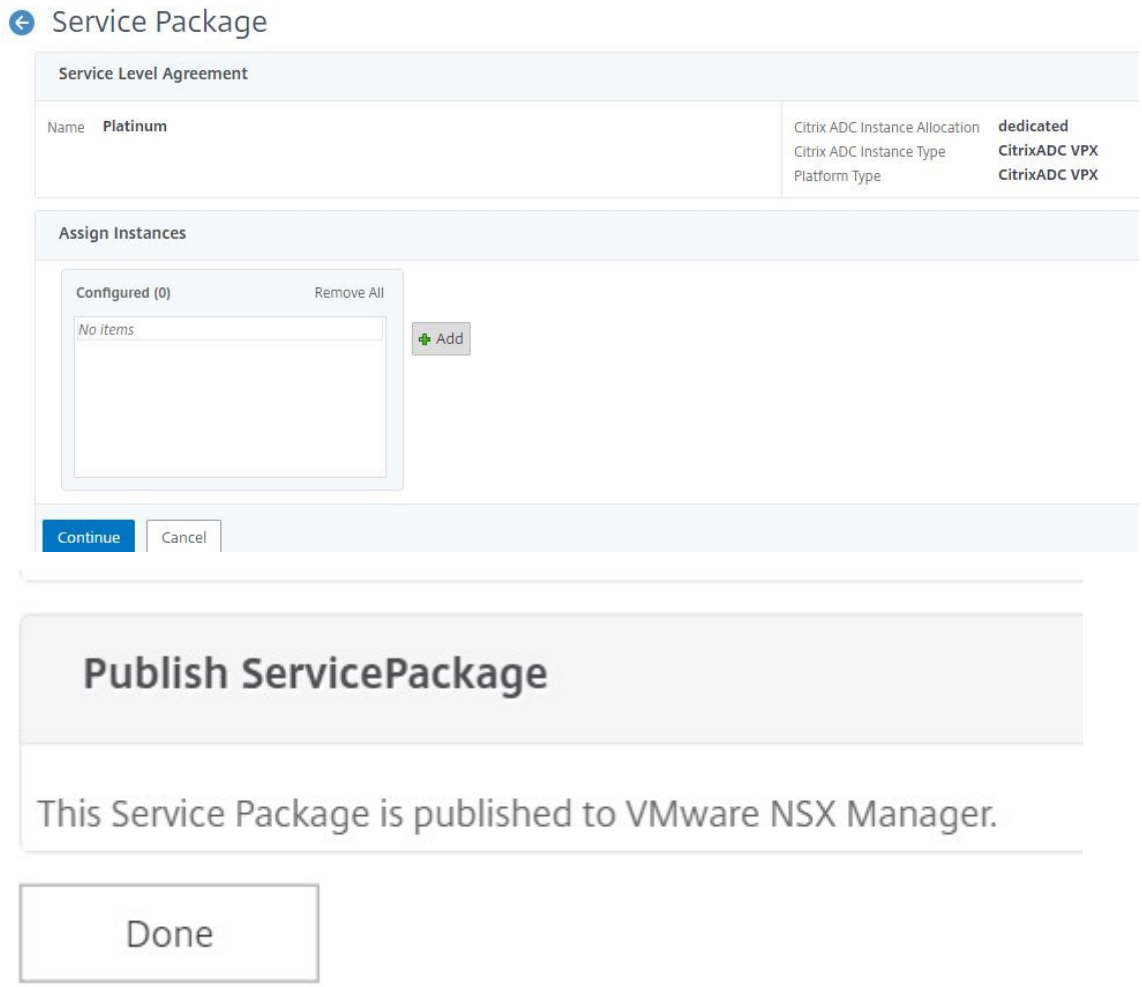
1. En NetScaler ADM, vaya a**Orchestration >**SDN Orchestration****>**VMware NSX Manager**> **Paquetes de servicios**y haga clic en **Agregar para agregar** un nuevo paquete de servicios.
2. En la página **Paquete de servicio**, en la sección **Parámetros básicos**, establezca los siguientes parámetros:
   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 NetScaler 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 NetScaler VPX a NetScaler ADM.

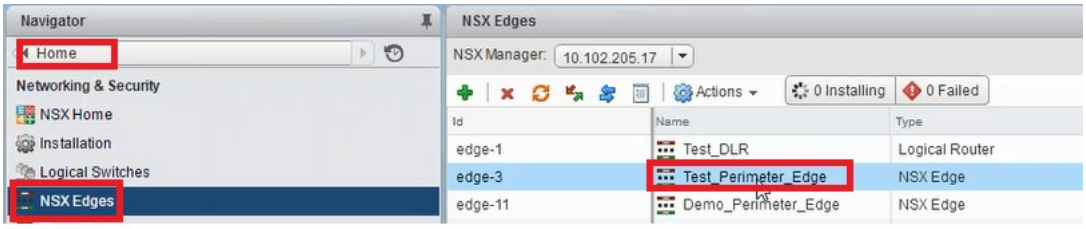
5. **Inicie sesión en NSX Manager en vSphere Web Client y vaya a**Definiciones de servicios**> Servicios.**

   Puede ver que el paquete de servicio NetScaler ADM está registrado.

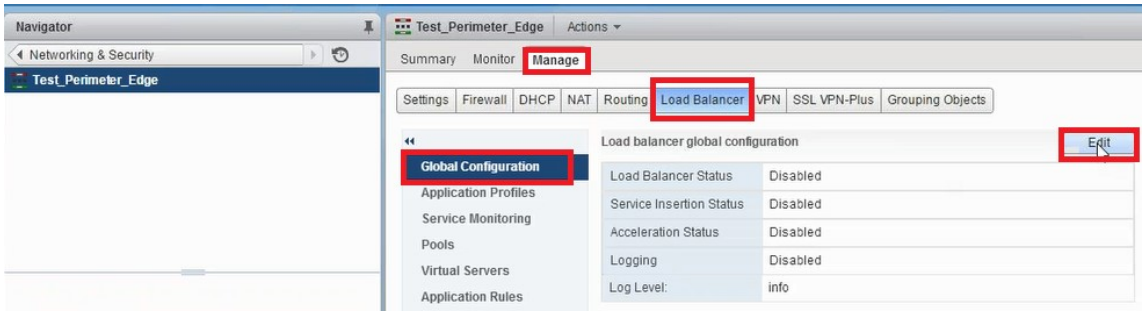
Realización de la inserción del servicio de equilibrador de carga para Edge

Inserte el servicio de balanceador de carga en la puerta de enlace de NSX Edge creada anteriormente (descargue la función de equilibrio de carga de NSX LB a NetScaler).

1. En NSX Manager, vaya a **Inicio** > **NSX Edges**y seleccione la puerta de enlace perimetral que haya configurado.

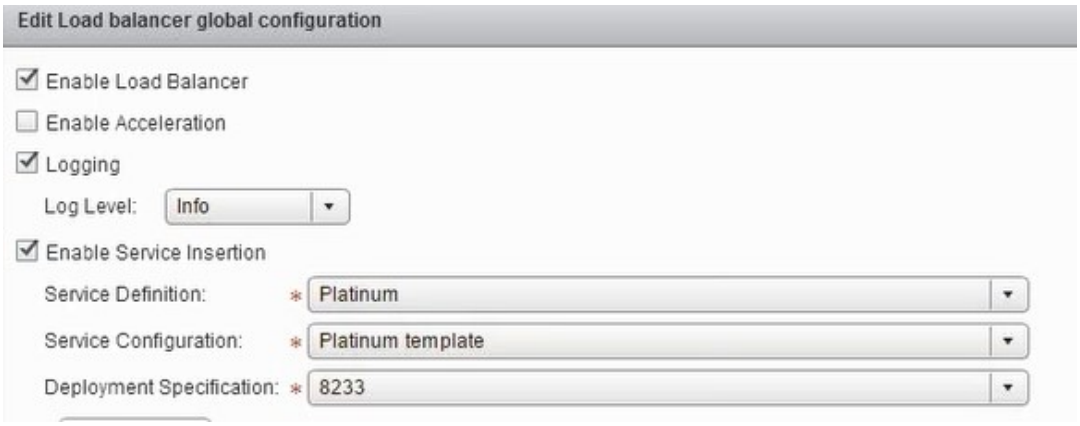


2. Haga clic en **Administrar**y, en la ficha **Equilibrador de carga**, seleccione **Configuración global**y, a continuación, en **Editar**.

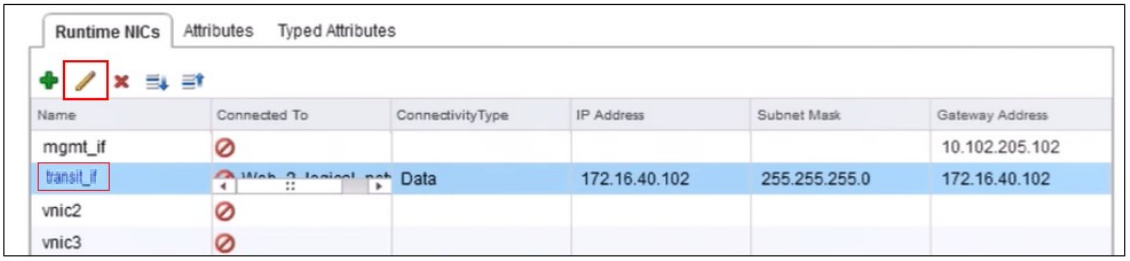


3. Seleccione **Habilitar equilibrador de carga**, **Registro**, **Habilitar inserción de servicios** para habilitarlos.

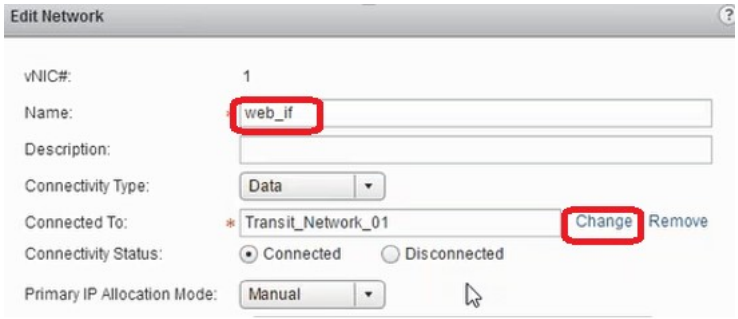
   a) En **Definición de servicio,** seleccione el paquete de servicio creado en NetScaler ADM y publicado en NSX Manager.



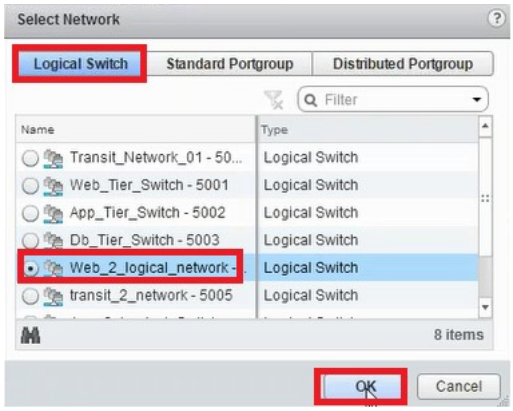
4. Seleccione las NIC de tiempo de ejecución existentes y haga clic en el icono Editar para modificar las NIC de tiempo de ejecución que deben conectarse al asignar NetScaler VPX.



5. Modifique el nombre de la NIC, especifique el tipo de conectividad como **dato**y haga clic en **Cambiar**.

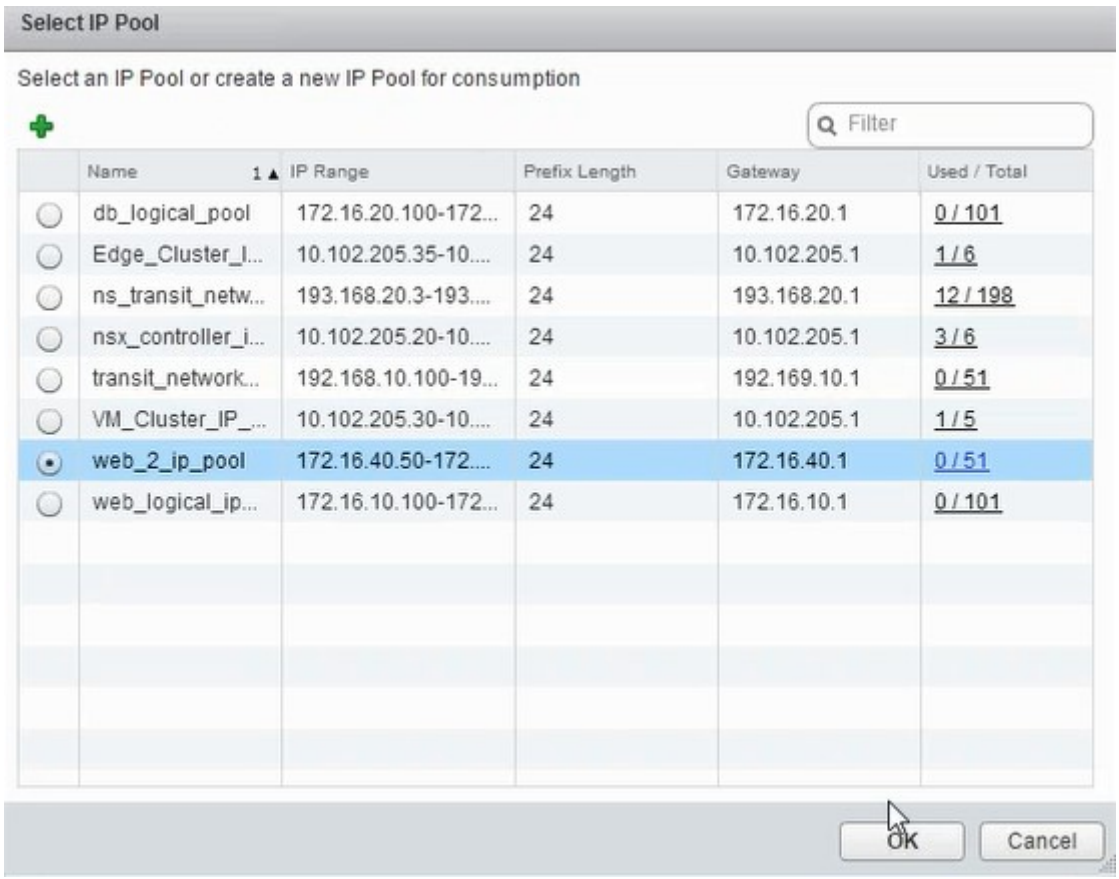


6. Seleccione el conmutador lógico web adecuado.



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.

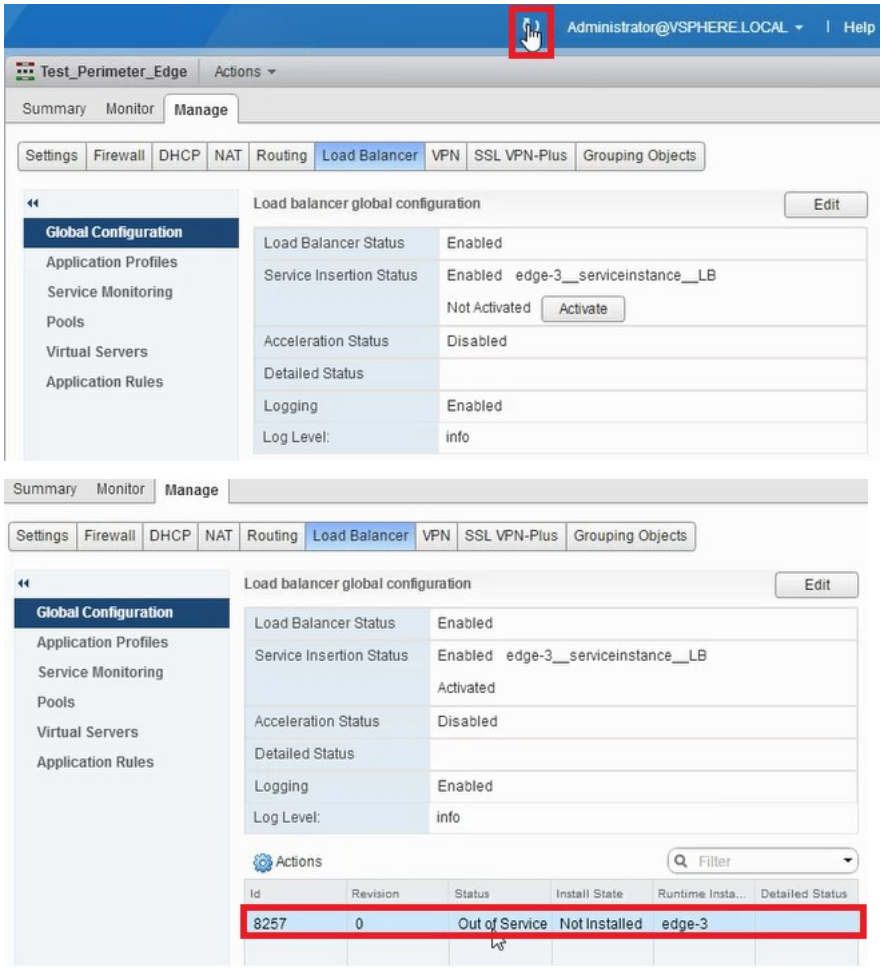
8. En la ventana **Seleccionar grupo de IP**, seleccione el grupo de IP apropiado y haga clic en **Aceptar**.



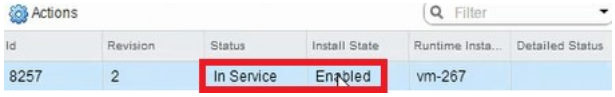
La dirección IP se adquiere y se establece como dirección IP de red de origen en el dispositivo NetScaler VPX. Se crea una Gateway L2 en NSX Manager para asignar la VXLAN a VLAN.

> **Nota**
>
> Todas las interfaces de datos están conectadas como NIC en tiempo de ejecución y forman parte de interfaces para DLR.

9. Actualice la vista para ver la creación del tiempo de ejecución.



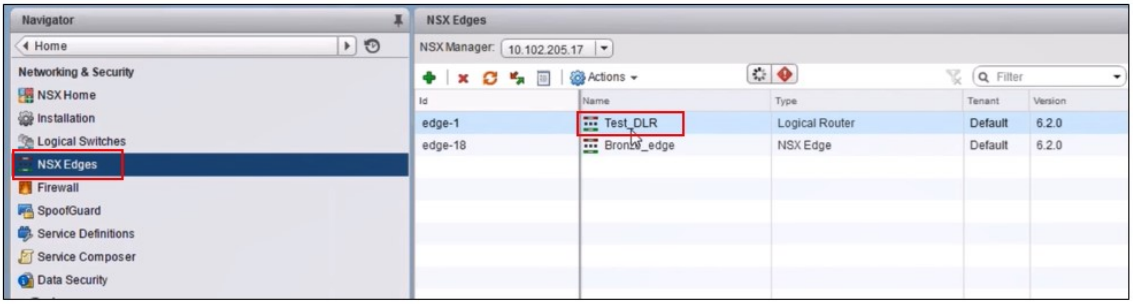
10. Una vez iniciada la máquina virtual, el valor de Estado cambia a **En servicio** y el de Estado de instalación cambia a **Habilitado**.



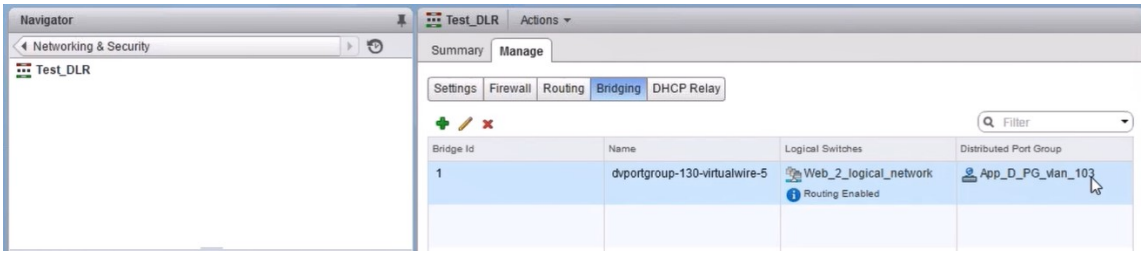
> **Nota**
>
> En NetScaler ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la inserción del servicio LB.

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.



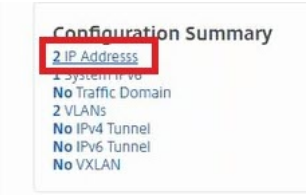
2. En la página DLR, vaya a **Administrar** > **Bridging**. Puede ver la Gateway L2 mostrada en la lista.



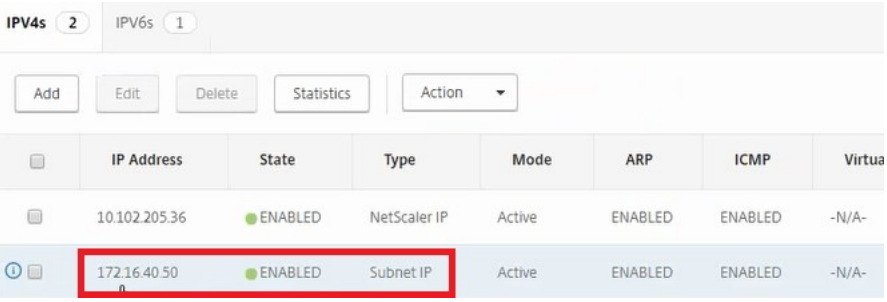
> **Nota**
>
> Se crea una Gateway L2 para cada interfaz de datos.

Visualización de NetScaler asignado

1. Inicie sesión en la instancia de NetScaler VPX con la dirección IP que se muestra en NetScaler 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 NetScaler VPX mediante StyleBook

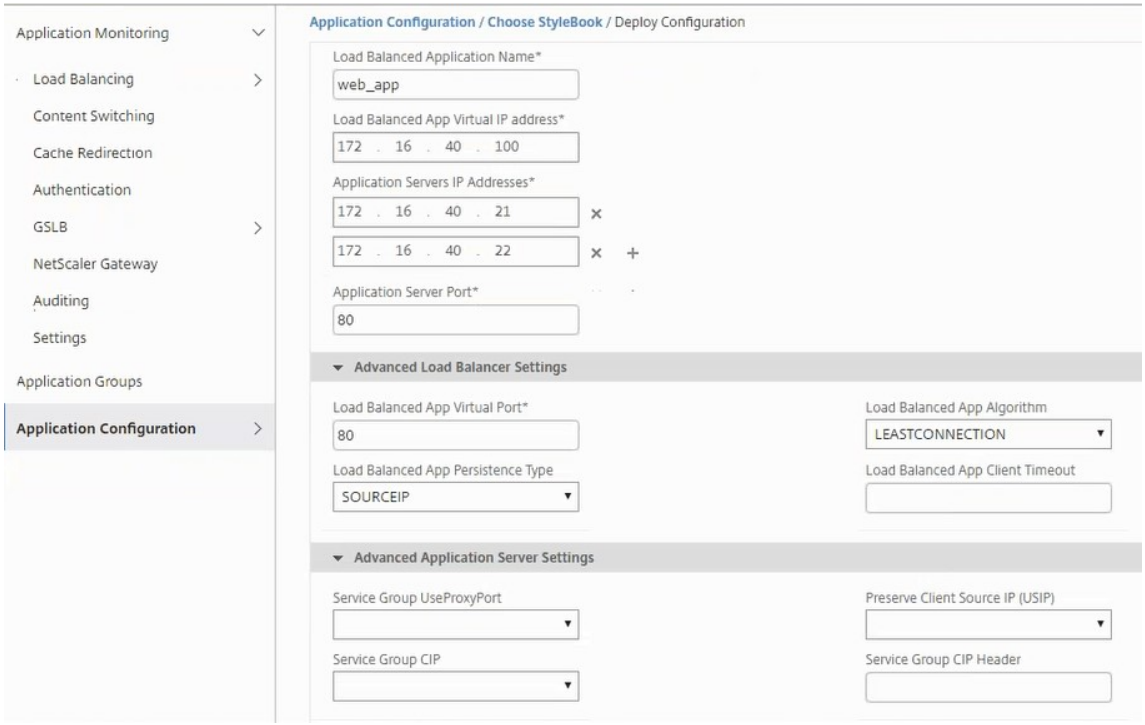
1. En NetScaler ADM, vaya a**Orchestration** >**SDN Orchestration**>**Configure NSX Manager** > **Edge Gateways**.

   Tome nota de la dirección IP de instancia de NetScaler que se asigna a la puerta de enlace perimetral respectiva en la que debe aplicarse la configuración de equilibrio de carga a través de StyleBooks.

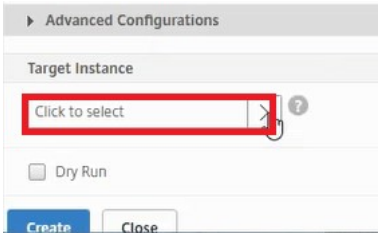
2. Cree un nuevo StyleBook. Vaya a **Aplicaciones** > **Configuración**, importe el StyleBook y seleccione el StyleBook de la lista.

   Para crear un StyleBook nuevo, consulta Crea su propio StyleBook.

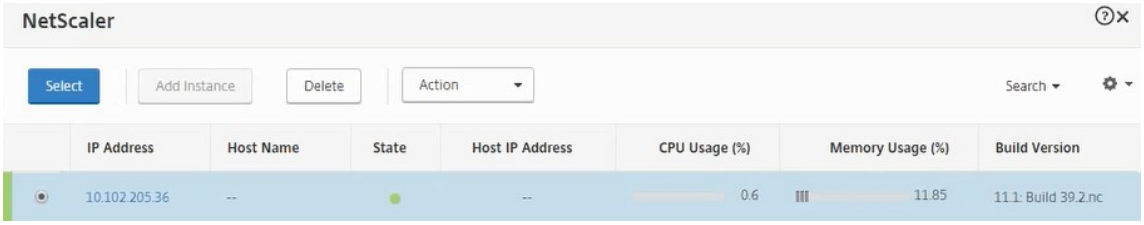
3. Especifique valores para todos los parámetros requeridos.



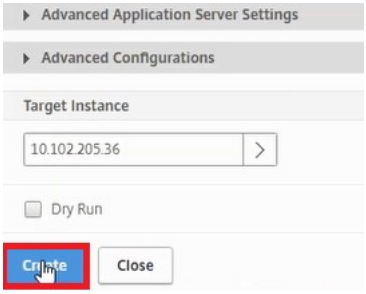
4. Especifique la instancia de NetScaler VPX en la que desea ejecutar estos ajustes de configuración.



5. Seleccione la instancia IP mencionada anteriormente y haga clic en **Seleccionar**.

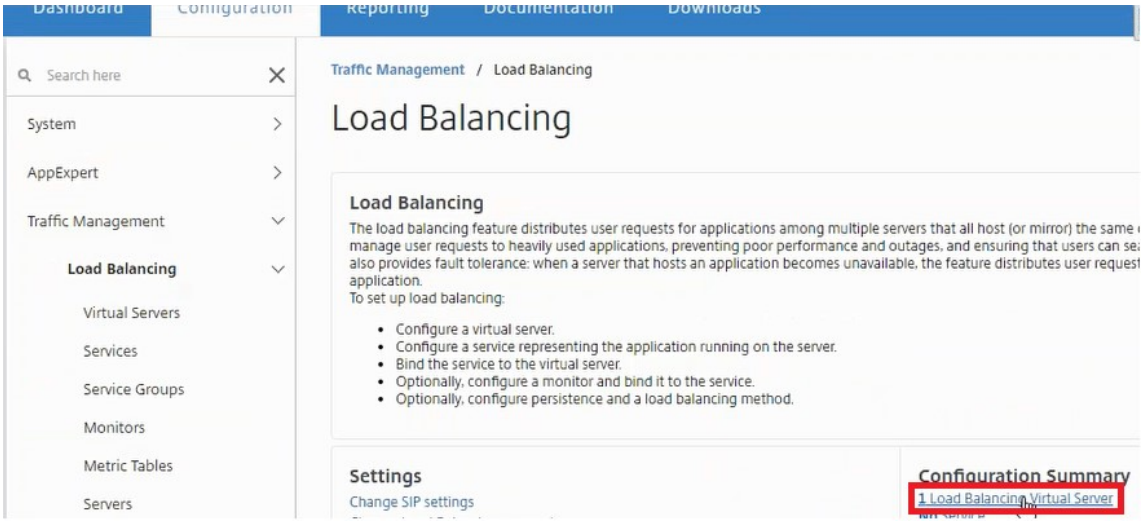


6. Haga clic en **Crear** para aplicar la configuración en el dispositivo seleccionado.

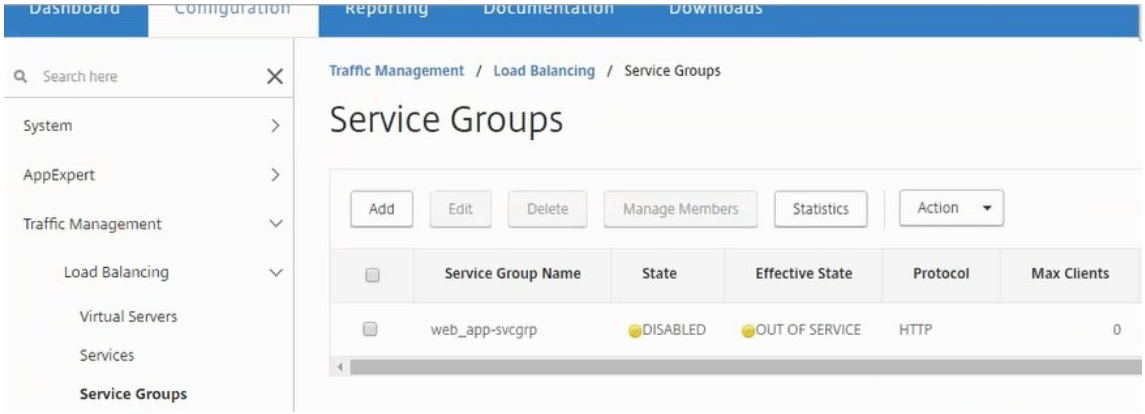


Visualización de la configuración del equilibrador de carga

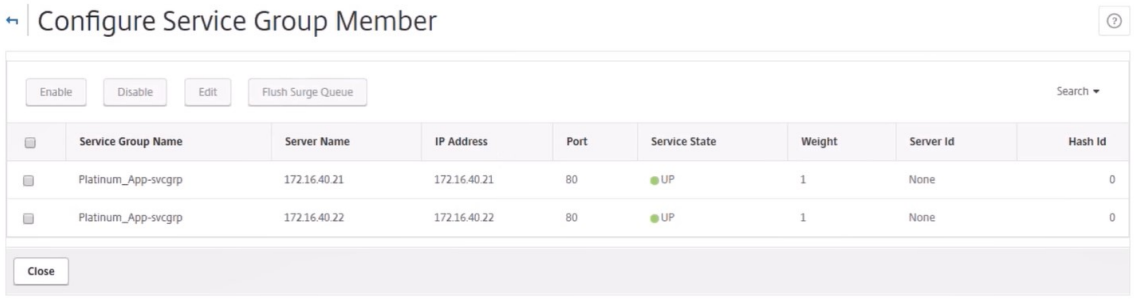
1. Inicie sesión en la instancia de NetScaler VPX, vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** para ver el servidor virtual de equilibrio de carga que se crea.



También puede ver los grupos de servicios que se crean.



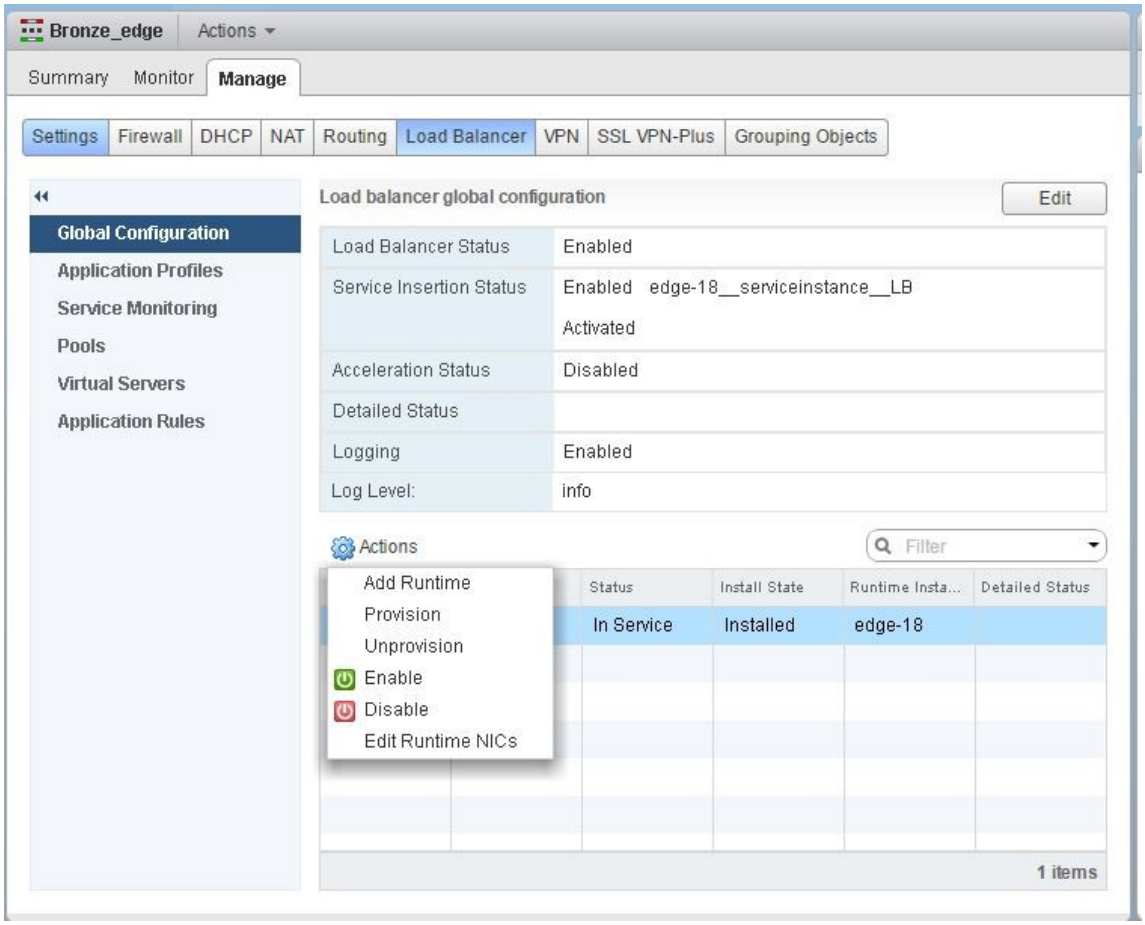
2. Seleccione el grupo de servicios y haga clic en **Administrar miembros**. La página **Configurar Miembro de Grupo de Servicio** muestra los miembros asociados al grupo de servicios.



Eliminación del servicio de equilibrador de carga

1. En NetScaler 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 NetScaler 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 Edge en NetScaler ADM corresponden a las entradas en tiempo de ejecución en NSX Manager.



La instancia de NetScaler 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

January 30, 2024

Overview

NetScaler 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 de NetScaler. Esta integración elimina las complejidades tradicionales asociadas a la topología

de red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios de NetScaler mediante programación con mayor rapidez.

Durante la inserción y eliminación del servicio de equilibrio de carga en VMware NSX Manager, NetScaler ADM aprovisiona y destruye las instancias de NetScaler de forma dinámica. Este aprovisionamiento dinámico requiere que las asignaciones de licencias de NetScaler VPX se automaticen en NetScaler ADM. Cuando las licencias de NetScaler se cargan en NetScaler ADM, NetScaler 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**.

- NetScaler ADM, versión 13.0, configurado en alta disponibilidad e instalado en ESX.
- NetScaler VPX, versión 13.0
- Licencias de NetScaler VPX para instancias de NetScaler VPX, versión 13.0
- 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 instancias de NetScaler ADM y NetScaler de alta disponibilidad

Para aprovisionar la configuración de NetScaler ADM HA, instale el archivo de imagen de NetScaler ADM que ha descargado del sitio de NetScaler. Para obtener más información sobre cómo aprovisionar la configuración de alta disponibilidad de NetScaler ADM, consulte Implementación de NetScaler ADM en alta disponibilidad.

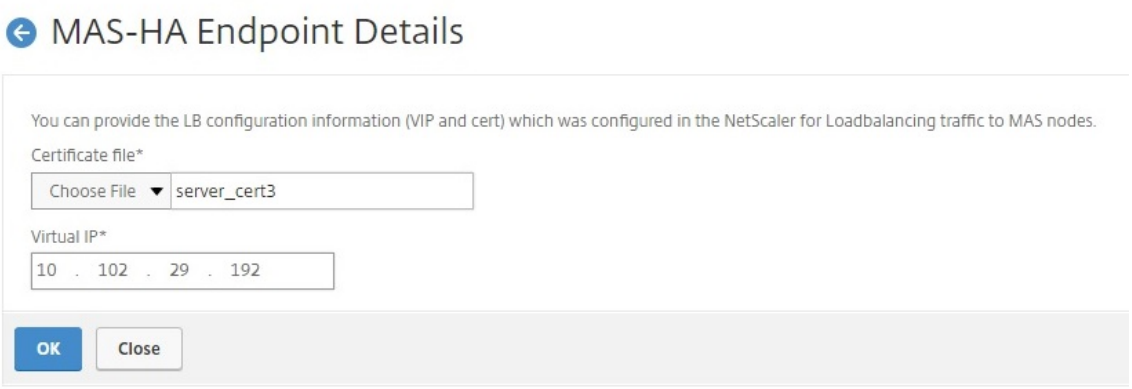
Configuración de detalles de NetScaler ADM HA Endpoint

Para integrar VMware NSX manager con NetScaler ADM que se implementa en modo HA, primero debe introducir la dirección IP virtual de la instancia de NetScaler de equilibrio de carga. También debe cargar el archivo de certificado que está presente en el servidor virtual de equilibrio de carga de NetScaler al sistema de archivos ADM de NetScaler.

Para proporcionar información de configuración de equilibrio de carga en NetScaler ADM:

1. **En el nodo NetScaler 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 de equilibrio de carga.
4. Introduzca la dirección IP virtual de la instancia de NetScaler de equilibrio de carga y haga clic en **Aceptar**.



Registro de VMware NSX Manager con NetScaler ADM

Al configurar dos servidores NetScaler ADM en alta disponibilidad, los dos nodos del servidor se encuentran en modo activo-pasivo. Inicie sesión en el nodo del servidor NetScaler ADM principal para registrar VMware NSX manager con NetScaler ADM en HA y crear un canal de comunicación entre ellos.

Para registrar VMware NSX manager con NetScaler ADM en HA:

1. **En el nodo principal del servidor NetScaler 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 ADM de NetScaler utilizada por NSX Manager, defina la contraseña del controlador de NetScaler para NSX Manager.
5. Haga clic en **Aceptar**.

Carga de licencias en NetScaler ADM

Cargue las licencias de NetScaler VPX en NetScaler ADM para que NetScaler ADM pueda asignar licencias automáticamente a las instancias durante la orquestación con NSX.

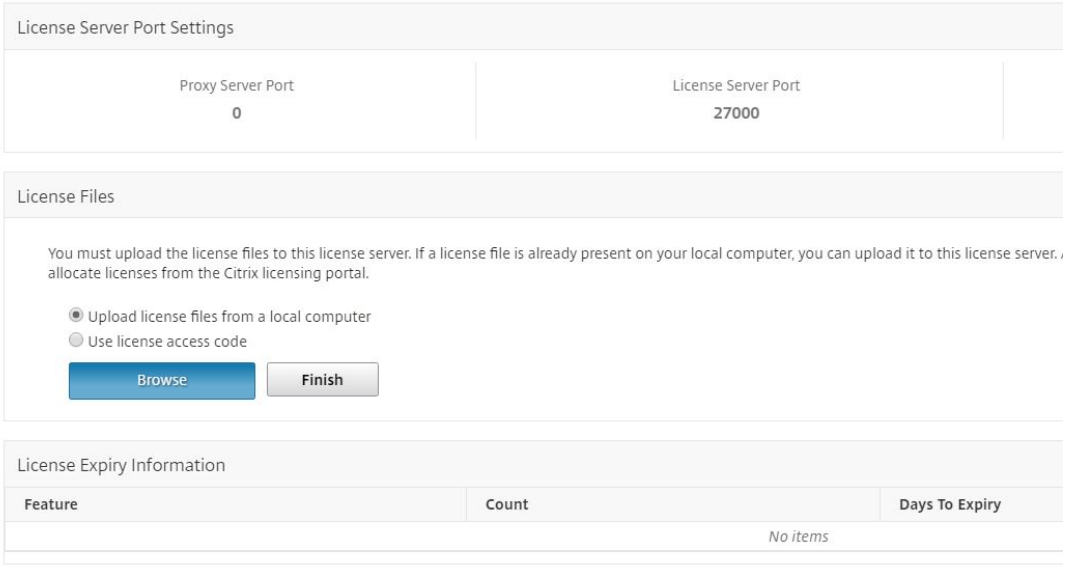
Para instalar archivos de licencia en NetScaler ADM:

1. En NetScaler ADM, vaya a **Infraestructura > Licencias agrupadas**.
2. En la sección **Archivos de licencia**, seleccione una de las siguientes opciones:

   a) **Cargue archivos de licencia desde un equipo local**: Si ya hay un archivo de licencia en su equipo local, puede cargarlo en NetScaler 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) **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso a licencias de las licencias que adquiera. Para añadir archivos de licencia, introduzca el código de acceso a la licencia 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.



Carga de imágenes de NetScaler VPX en NetScaler ADM

Agregue las imágenes de NetScaler 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 NetScaler VPX en NetScaler 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 VPX de la carpeta de almacenamiento local.

Creación de paquetes de servicios en NetScaler ADM

Cree paquetes de servicio en NetScaler ADM para definir el conjunto de SLA, que indica cómo se asignan los recursos de NetScaler.

Para crear paquetes de servicios en NetScaler ADM:

1. En NetScaler ADM, vaya a**Orchestration >**SDN Orchestration****>**VMware NSX Manager**> **Paquetes de servicios**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**

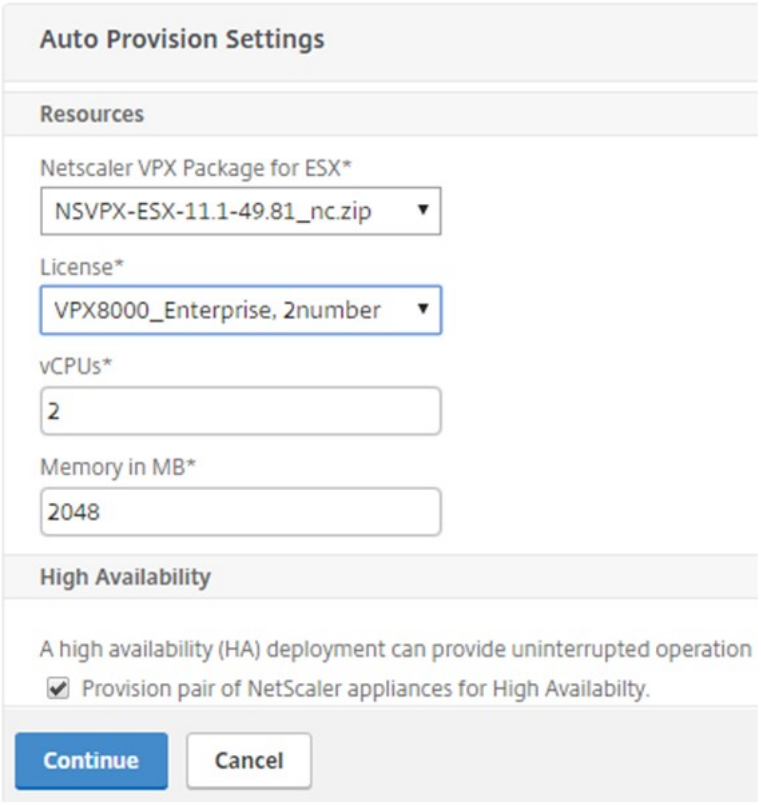
c) **Provisioning de instancias de NetScaler: seleccione Crear instancia bajo demanda**

d) Plataforma de aprovisionamiento automático: seleccione **CitrixNetScaler**SDX

e) Haga clic en **Continuar**.

3. **En la sección**Configuración de aprovisionamiento automático**, seleccione el paquete zip de NetScaler 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 para alta disponibilidad.



> **Nota**
>
> El nombre de la licencia que se muestra en el cuadro de lista que se muestra en la ilustración anterior, VPX8000_Advanced, número 2 es un ejemplo y se explica de la siguiente manera:
>
> - VPX: La licencia es implementar instancias de NetScaler VPX
> - 8000: el ancho de banda consumible es de 8 GB

- Avanzado: NetScaler ofrece tres tipos de licencias: Standard, Advanced y Premium
- Número 2: se pueden implementar dos instancias de NetScaler 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 a NetScaler 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 NetScaler ADM.

> **Nota**
>
> Para NetScaler ADM en implementaciones de alta disponibilidad, las licencias solo se cargan en el nodo del servidor de licencias de NetScaler ADM. Los nodos NetScaler ADM están en modo activo-pasivo.

Realización de la inserción del servicio de equilibrador 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.

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. NetScaler 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:**
>
> dado que está implementando dos instancias de NetScaler VPX en una implementación de HA, se crean dos tiempos de ejecución en el administrador de NSX.
>
> 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 NetScaler 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 NetScaler 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 que NetScaler ADM se ha agregado a NSX Manager.

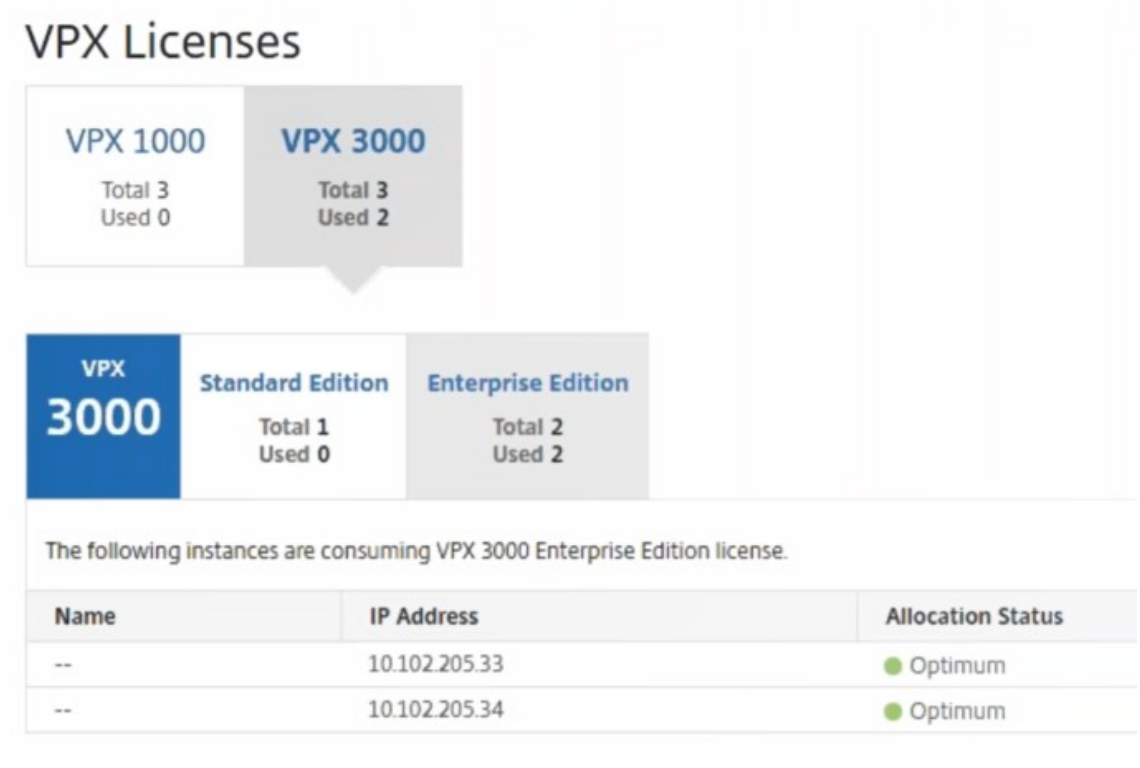
   Para HA, habrá dos solicitudes para crear y actualizar dos tiempos de ejecución en NetScaler ADM. Cuando se hayan actualizado ambos tiempos de ejecución, seleccione ambas solicitudes y haga clic en el botón **Tareas** para ver que se han agregado dos nodos HA de NetScaler ADM a NSX Manager.

10. **En NetScaler ADM, vaya a**Orchestration > SDN Orchestration****> **VMware** NSX Manager > Edge Gateways**.** En el panel lateral derecho, puede ver que el NetScaler VPX se ha agregado al NSX Edge Gateway.

    Para HA, puede ver que se han agregado dos instancias de NetScaler VPX en modo HA a NSX Edge Gateway.

11. En NetScaler ADM, vaya a **Infraestructura > Licencias agrupadas > Licencias VPX**. Seleccione la licencia NetScaler VPX y la edición que haya instalado.

    Las instancias de NetScaler 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 en uno de los dos métodos siguientes:

- Configuración de los servicios de equilibrio de carga en NetScaler VPX en la GUI de VMware NSX Manager
- Configuración de Load Balancing Services en NetScaler VPX en NetScaler ADM GUI

Configuración de los servicios de equilibrio de carga en NetScaler 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

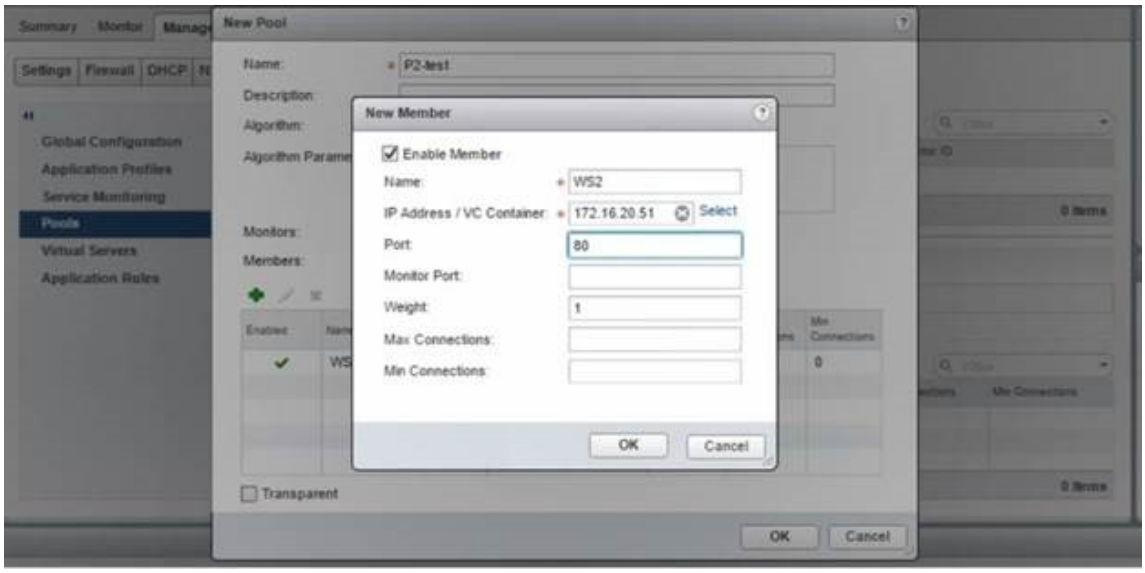
d) Miembros: haga clic en "+"para agregar miembros al grupo e introduzca los parámetros necesarios en la ventana Nuevo miembro.

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:

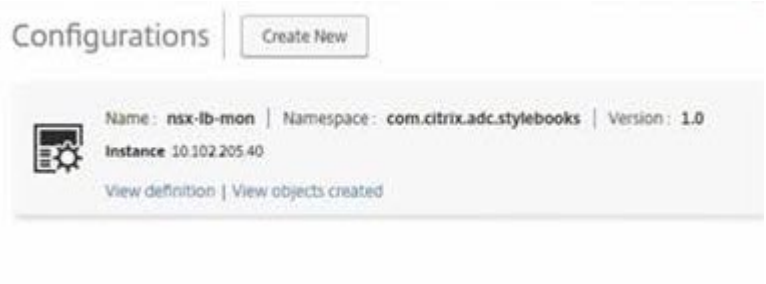
a) Perfil de aplicación: de forma predeterminada, se muestra el perfil de servicio que creó en NetScaler ADM.

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 seleccionadas.
4. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración**y compruebe que se ha creado el paquete de `nsx-lb-mon` configuración.



Configuración de Load Balancing Services en NetScaler VPX en NetScaler ADM GUI

Implemente configuraciones del equilibrador de carga en la instancia de NetScaler mediante NetScaler ADM StyleBooks. Para HA, la configuración se implementa en las dos instancias de NetScaler que se encuentran en HA.

Para crear paquetes de configuración a través de StyleBooks:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración** > **Crear nuevo**y seleccione el StyleBook de **equilibrio de carga HTTP/SSL (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 de NetScaler VPX de destino que se aprovisiona 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.

Verificación de la creación de servidores virtuales y grupos de servicios en instancias de NetScaler VPX

Puede ver que los grupos de servicios y los servidores virtuales se crean iniciando sesión en la instancia de NetScaler VPX.

Para ver los grupos de servicios y los servidores virtuales:

1. Inicie sesión en la instancia de NetScaler VPX. Para la implementación de HA, debe iniciar sesión en las dos instancias de NetScaler 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 servicios de equilibrio de carga

Cuando los servicios de equilibrio de carga ya no son necesarios en las instancias de NetScaler VPX implementadas en NSX Manager, puede eliminar las inserciones de servicio realizadas anteriormente.

Para eliminar la configuración y la inserción de servicios:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración, seleccione la configuración**de la aplicación creada y, a continuación, elimine la configuración 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 NetScaler 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**. Asegúrese de que no existe una asignación respectiva de la puerta de enlace Edge a la instancia eliminada.

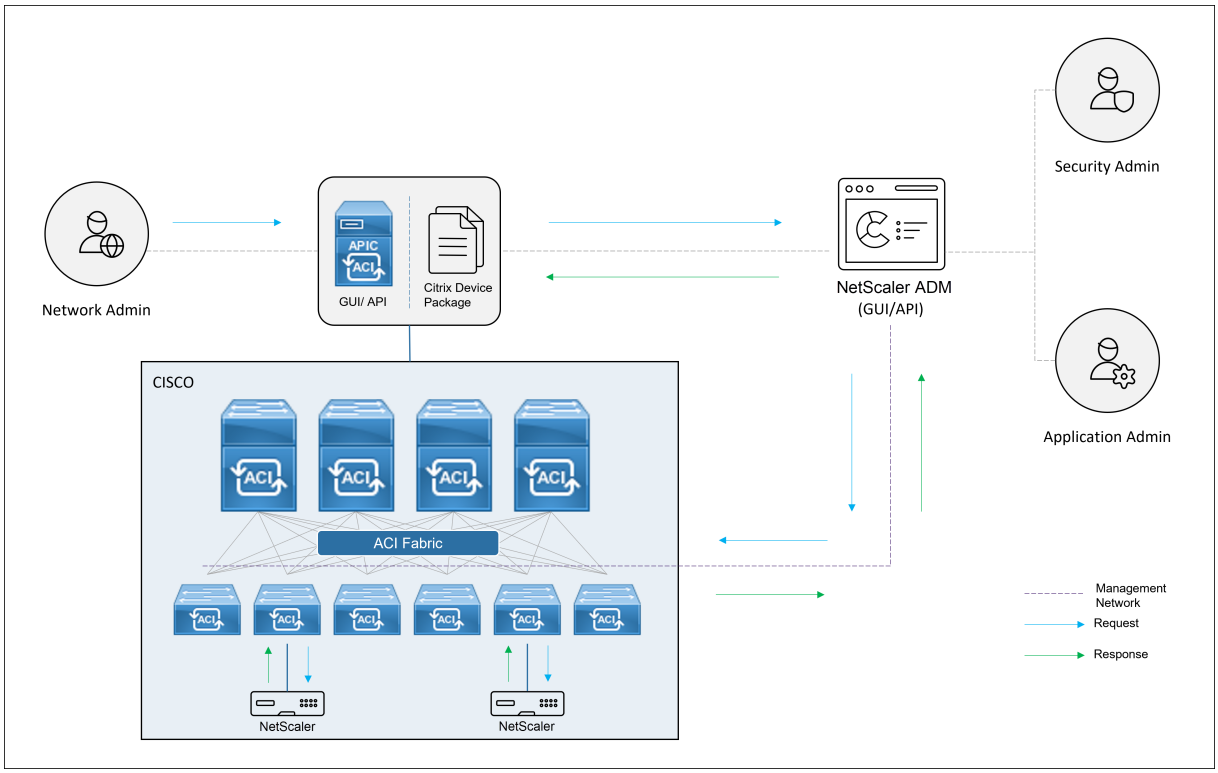
Automatización de NetScaler mediante NetScaler ADM en el modo híbrido ACI de Cisco

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 NetScaler Application Delivery Management (ADM), que actúa como administrador de dispositivos en el APIC.

La solución NetScaler Hybrid Mode es compatible con un paquete de dispositivos de modo híbrido y NetScaler 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 NetScaler. StyleBook mapea la paridad de las aplicaciones desde NetScaler 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 NetScaler.

La siguiente ilustración proporciona una descripción general de NetScaler en una solución de modo híbrido:



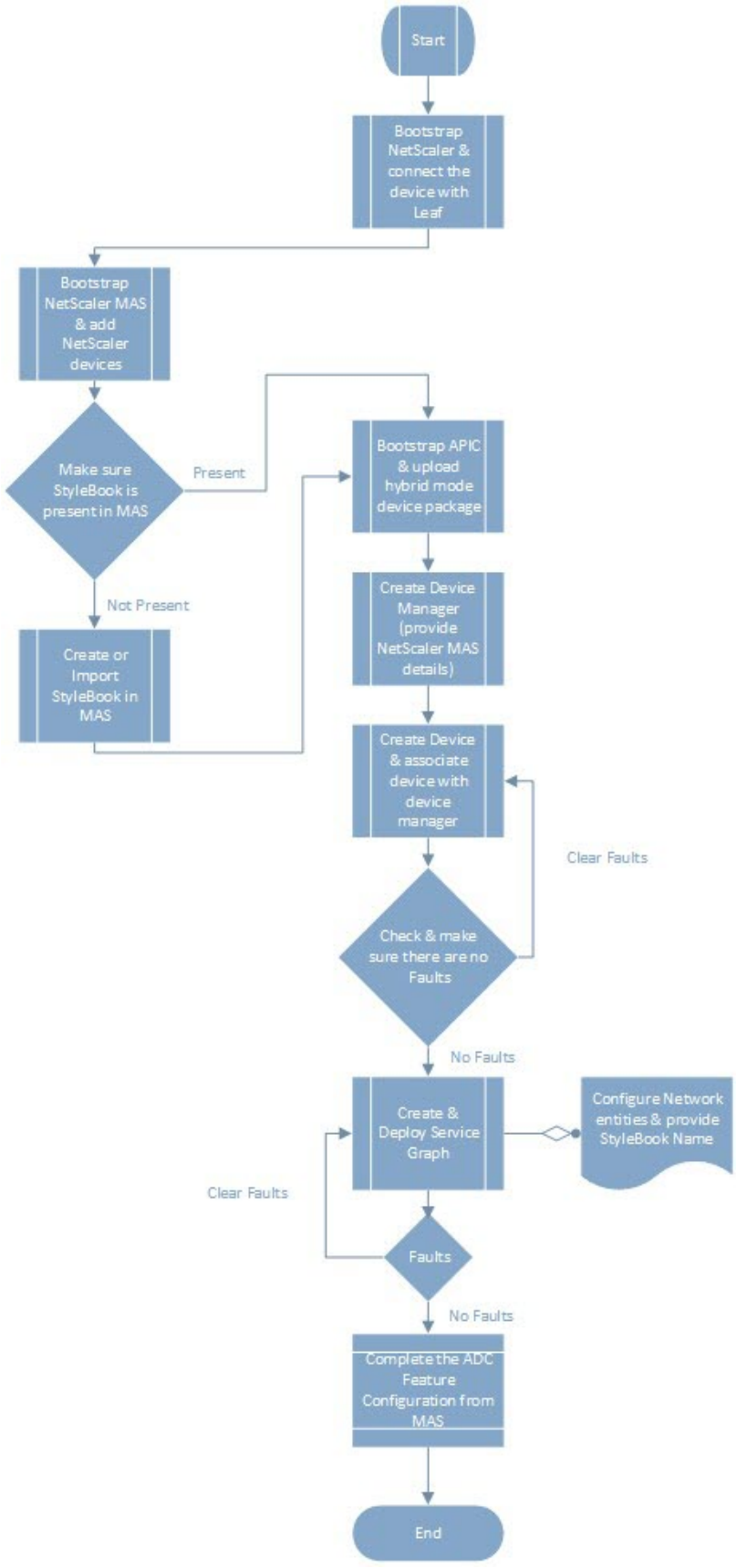
En el modo híbrido, la configuración de NetScaler se realiza en las dos fases siguientes:

1. La unión de redes se realiza desde el APIC de Cisco

2. La configuración se realiza desde NetScaler 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 NetScaler ADM a través del paquete del dispositivo, y NetScaler ADM los procesa internamente y configura el NetScaler. Un administrador de aplicaciones crea la configuración relacionada con el ADC de la aplicación mediante StyleBook en NetScaler ADM y, a continuación, estas configuraciones se envían de NetScaler ADM a NetScaler. El APIC de Cisco y el ADM de NetScaler se comunican con el ADC a través de la red de administración.

El siguiente diagrama muestra un flujo de trabajo de NetScaler en la solución híbrida:



Paquete de dispositivos NetScaler en el modo de orquestación de nube de ACI de Cisco

January 30, 2024

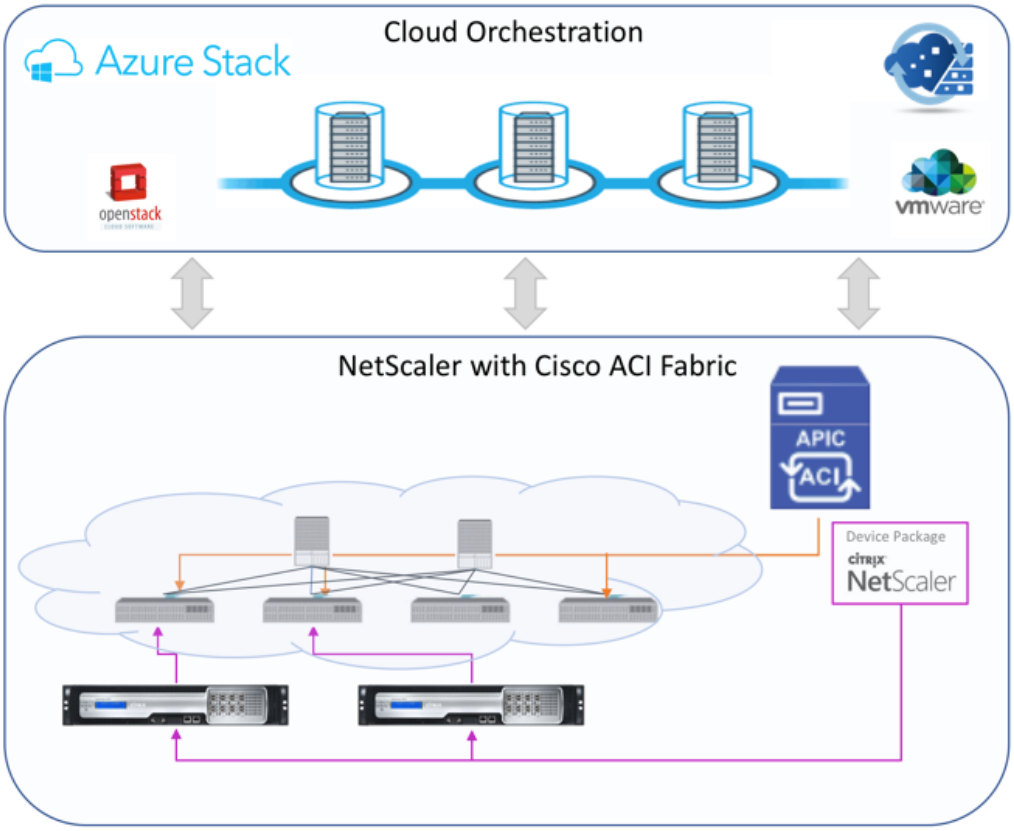
Con Application Policy Infrastructure Controller (APIC) versión 3.1, Citrix NetScaler y Cisco ACI amplían la cartera de integración conjunta para proporcionar una nueva solución que aborde las necesidades del cliente. El nuevo modo de integración, ACI Cloud Orchestrator Mode*, simplifica las integraciones 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 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 en una solución de orquestación en la nube:

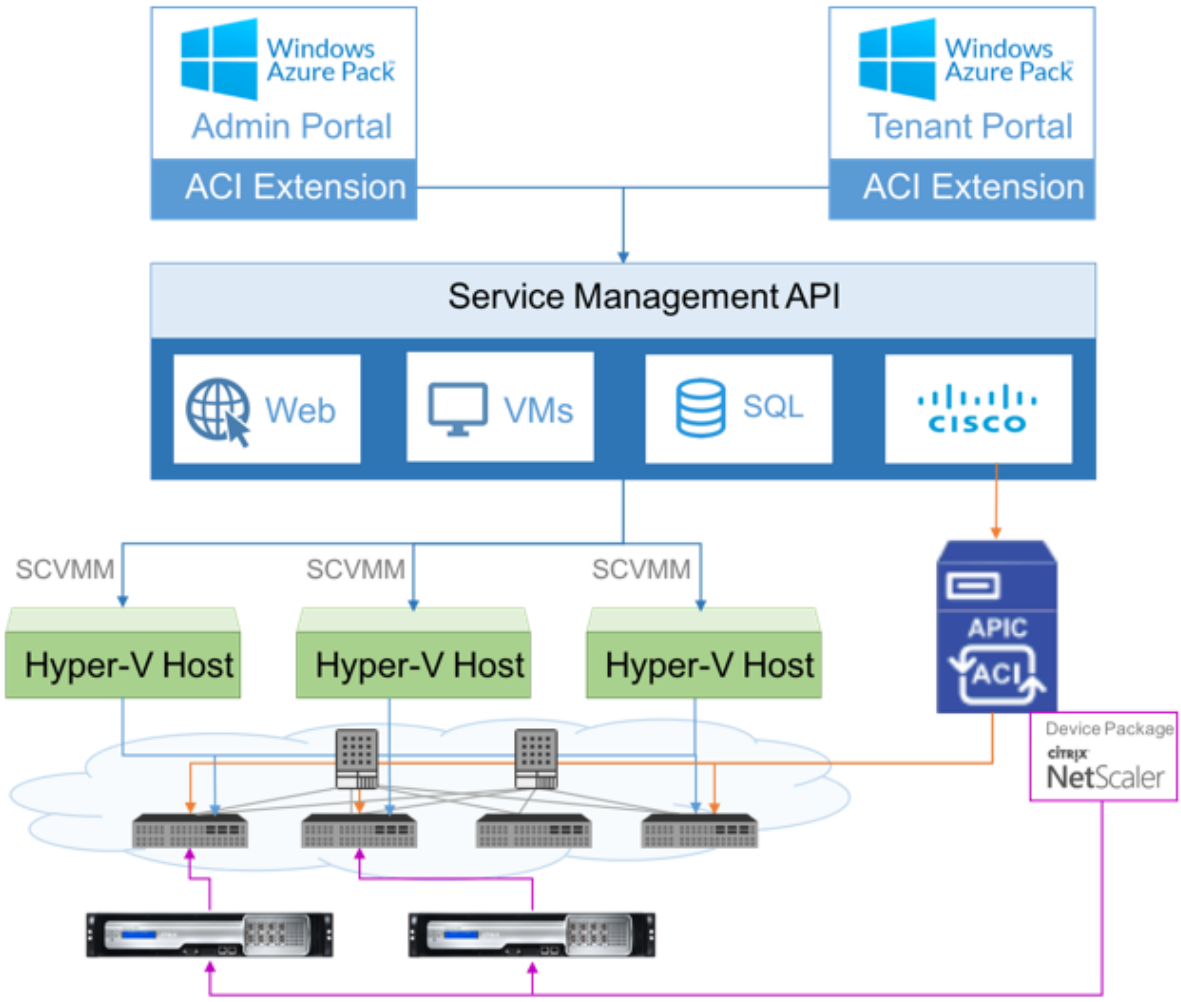


La solución de modo de orquestación en la nube que utiliza Microsoft Azure Pack implica muchos puntos de integración, como Azure Pack a Cisco APIC, Cisco APIC a System Central máquina virtual Manager (SCVMM) y Cisco APIC a NetScaler. Como arrendatario en la nube privada, puede habilitar NAT, aprovisionar 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 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.

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 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 solo admite la implementación de un solo contexto. Cada arrendatario recibe una instancia de NetScaler dedicada.
- El Protocolo de aplicaciones inalámbricas (WAP) admite dispositivos NetScaler MPX y dispositivos NetScaler VPX (incluye instancias NetScaler VPX implementadas en la plataforma NetScaler 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. 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 mediante APIC. NetScaler Application Delivery Management (ADM) actúa como administrador de servicios para APIC y puede utilizar NetScaler ADM para configurar los parámetros de NetScaler 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.

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 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.

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 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 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 a través de ningún orquestador en la nube. El paquete de dispositivos es compatible solo con APIC y APIC con Cloud Orchestrator.

Administrar la configuración de Kubernetes Ingress en NetScaler ADM

January 30, 2024

Kubernetes (K8s) es una plataforma de orquestación de contenedores de código abierto que automatiza la implementación, el escalado y la administración de aplicaciones nativas de la nube.

Kubernetes proporciona la función Ingress, que permite que el tráfico de clientes fuera del clúster acceda a los microservicios de una aplicación que se ejecuta dentro del clúster de Kubernetes. Las instancias de ADC pueden actuar como entrada a las aplicaciones que se ejecutan dentro de un clúster de Kubernetes. Las instancias de ADC pueden equilibrar la carga y enrutar el tráfico de norte a sur desde los clientes a cualquier microservicio dentro del clúster de Kubernetes.

> **Nota**
>
> - NetScaler ADM admite la función Ingress en los clústeres con Kubernetes versión 1.14 a 1.21.
> - NetScaler ADM admite dispositivos NetScaler VPX y MPX como dispositivos de ingreso.
> - En el entorno de Kubernetes, la carga de instancia de NetScaler equilibra solo el tipo de servicio "NodePort".

Puede configurar varias instancias ADC para que actúen como dispositivos de ingreso en el mismo clúster o en distintos clústeres o espacios de nombres. Después de configurar las instancias, puede asignar cada instancia a diferentes aplicaciones en función de la directiva de Ingress.

Puede crear e implementar una configuración de Ingress con API o `kubectl` de Kubernetes. También puede configurar e implementar un Ingress desde NetScaler ADM.

Puede especificar los siguientes aspectos de la integración de Kubernetes en ADM:

- **Clúster**: Puede registrar o anular el registro de clústeres de Kubernetes para los que ADM puede implementar configuraciones de Ingress. Cuando registre un clúster en NetScaler ADM, especifique la información del servidor de la API de Kubernetes. A continuación, seleccione un agente de ADM que pueda llegar al clúster de Kubernetes e implementar configuraciones de Ingress.

- **Directivas: las** directivas de entrada se utilizan para seleccionar la instancia de ADC en función del clúster o el espacio de nombres para implementar una configuración de entrada. Especifique la información del clúster, el sitio y la instancia cuando agregue una directiva.
- **Configuración de ingreso**: Esta configuración es la configuración de ingreso de Kubernetes, que incluye las reglas de conmutación de contenido y las rutas URL correspondientes de los microservicios y sus puertos. También puede especificar los certificados SSL/TLS (para descargar el procesamiento SSL en la instancia de ADC) con los recursos secretos de Kubernetes.

NetScaler ADM asigna automáticamente las configuraciones de ingreso a instancias de ADC mediante directivas de ingreso.

Para cada configuración de Ingress correcta, NetScaler ADM genera un StyleBook ConfigPack. El ConfigPack representa la configuración ADC aplicada a la instancia de ADC que corresponde a la configuración de Ingress. Para ver el ConfigPack, vaya a **Aplicaciones > StyleBooks > Configuraciones**.

Antes de comenzar

Para usar instancias de NetScaler como dispositivos de entrada en clústeres de Kubernetes, asegúrese de tener:

- Kubernetes agrupamiento en su lugar.
- Cluster Kubernetes registrado en NetScaler ADM.

Configurar NetScaler ADM con un token secreto para administrar un clúster de Kubernetes

Para que NetScaler ADM pueda recibir eventos de Kubernetes, debe crear una cuenta de servicio en Kubernetes para NetScaler ADM. Además, configure la cuenta de servicio con los permisos RBAC necesarios en el clúster.

1. Cree una cuenta de servicio para NetScaler ADM. Por ejemplo, el nombre de la cuenta de servicio puede ser`citrixadm-sa`. Para crear una cuenta de servicio, consulte Usar varias cuentas de servicio.
2. Utilice el`cluster-admin` rol para enlazar la cuenta de servicio NetScaler ADM. Este enlace concede un valor `ClusterRole` en todo el clúster a una cuenta de servicio. A continuación, se muestra un comando de ejemplo para vincular un rol `cluster-admin` a la cuenta de servicio.

```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```


Después de vincular la cuenta de servicio NetScaler ADM al rol `cluster-admin`, la cuenta de servicio tiene acceso en todo el clúster. Para obtener más información, consulte `kubectl Createclusterrolebinding`.

3. Obtenga el token de la cuenta de servicio creada.

   Por ejemplo, ejecute el siguiente comando para ver el token de la cuenta de servicio `citrixadm-sa`:

```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. Ejecute el siguiente comando para obtener la cadena secreta del token:

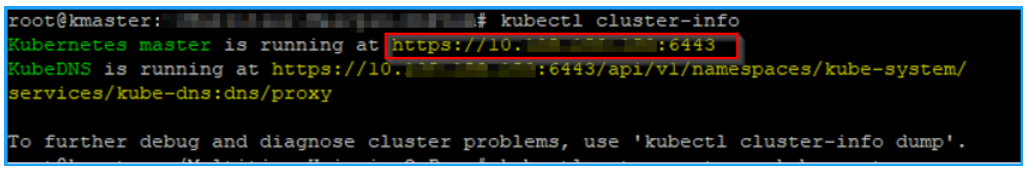
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

Agregar el clúster de Kubernetes en NetScaler ADM

Después de configurar un agente NetScaler ADM y configurar rutas estáticas, debe registrar el clúster de Kubernetes en NetScaler ADM.

Para registrar el clúster de Kubernetes:

1. Inicie sesión en NetScaler ADM con credenciales de administrador.
2. Vaya a **Orchestration** > **Kubernetes** > **Clúster**.
   Se muestra la página Clústeres.
3. Haga clic en **Agregar**.
4. En la página **Agregar clúster**, especifique los siguientes parámetros:
   a) **Nombre**: especifique un nombre de su elección.
   b) **URL del servidor API** - Puede obtener los detalles de la URL del servidor API desde el nodo principal de Kubernetes.
      i. En el nodo principal de Kubernetes, ejecute el comando `kubectl cluster-info` .



      ii. Introduzca la URL que aparece para **“Kubernetes master se está ejecutando en. “**

c) **Token de autenticación**: especifique la cadena de token de autenticación que se obtiene al configurar NetScaler ADM para administrar un clúster de Kubernetes. El token de autenticación es necesario para validar el acceso para la comunicación entre el clúster de Kubernetes y NetScaler ADM. Para generar un token de autenticación:

i. En el nodo principal de Kubernetes, ejecute los siguientes comandos:

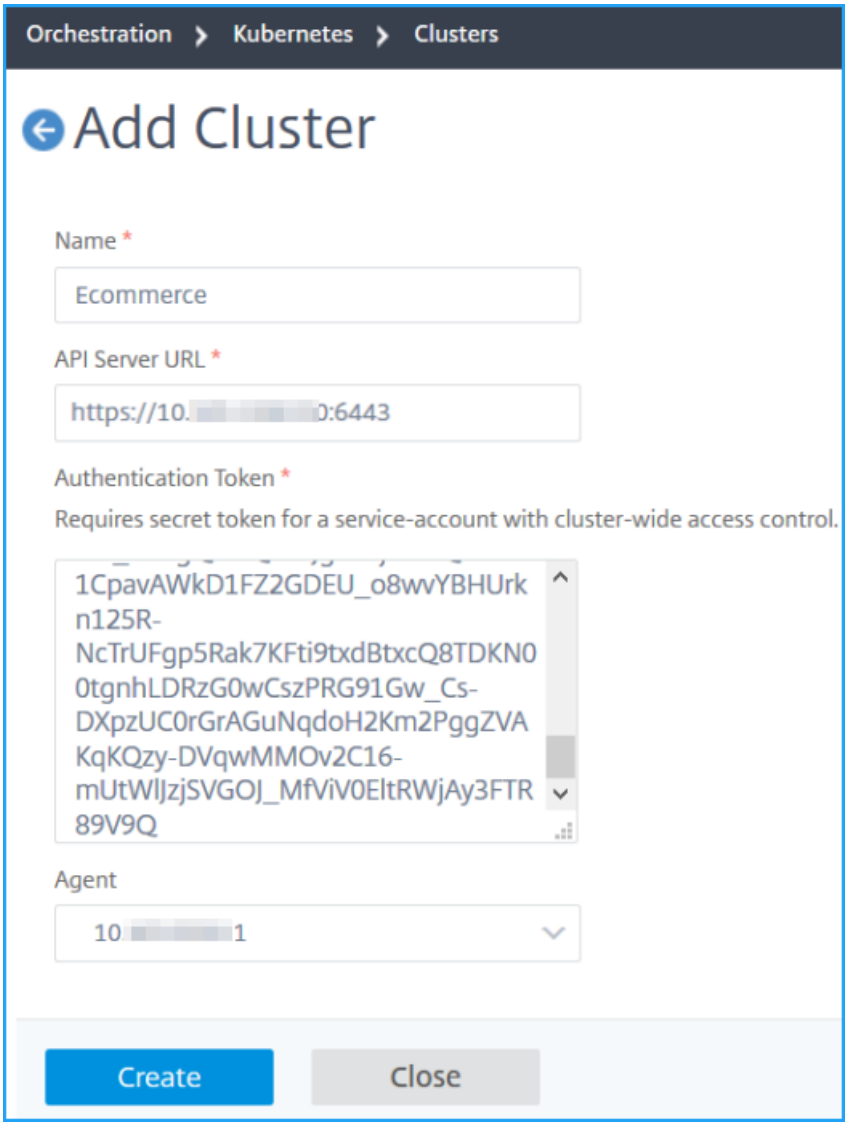
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Copie el token que se genera y péguelo como token de autenticación

Para obtener más información, consulte la documentación de Kubernetes.

d) Seleccione el agente de la lista.

e) Haga clic en **Crear**.



Definir una directiva de ingreso

La directiva Ingress decide qué NetScaler se utiliza para implementar una configuración de Ingress, basada en el clúster de entrada o el espacio de nombres.

1. Vaya a **Orchestration > Kubernetes > Policy**.
2. Haga clic en **Add** para crear una directiva.
    a) Especifique el nombre de la directiva.
    b) Defina **las condiciones** para implementar la configuración de Ingress en un clúster de Kubernetes. Estas condiciones suelen basarse en el clúster de entrada y el espacio de nombres.
    c) En el panel Infraestructura,
        - **Sitio**: Seleccione un sitio de la lista.
        - **Instancia**: Seleccione la instancia de ADC de la lista.

        Las listas de **sitios** e **instancias** rellenan las opciones en función de la selección de clústeres en el panel **Condiciones**.

        Estas listas muestran los sitios o las instancias que están asociados con el agente NetScaler ADM configurado con el clúster de Kubernetes.
    d) En **Elegir red**, seleccione la red desde la que ADM asigna automáticamente las direcciones IP virtuales a una configuración de entrada.

        Esta lista muestra las redes creadas en **Infraestructura > IPAM**.
    e) Haga clic en **Crear**.

Implementar la configuración de Ingress

Puede implementar la configuración de Ingress desde Kubernetes mediante `kubectl`, la API de Kubernetes u otras herramientas. También puede implementar la configuración de Ingress directamente desde NetScaler ADM.

1. Vaya a **Orchestration > Kubernetes > Entradas**.
2. Haga clic en **Agregar**.
3. En el campo **Crear entrada**, especifique los siguientes detalles:
    a) Especifique el nombre del Ingress.
    b) En **Clúster**, selecciona el clúster de Kubernetes en el que quieres implementar un Ingress.

c) Seleccione el Espacio de **nombres de clúster** en la lista. En este campo se enumeran los espacios de nombres que están presentes en el clúster de Kubernetes especificado.

d) Si lo desea, seleccione **Asignar dirección IP frontend automáticamente**.

e) Seleccione **Protocolo de entrada** en la lista. Si selecciona **HTTPS**, especifique el **secreto de TLS**.

Este secreto incrusta el recurso secreto de Kubernetes que incorpora el certificado HTTPS y la clave privada.

Una entrada HTTPS requiere un secreto basado en TLS configurado en el clúster de Kubernetes. Especifique los campos `tls.crt` y `tls.key` para incluir el certificado del servidor y la clave del certificado, respectivamente.

f) Para el enrutamiento de contenido, especifique los siguientes detalles:

- **Rutas de URL**: Especifique la ruta que se asocia con el servicio y el puerto de Kubernetes.
- **Servicio de Kubernetes**: Especifique el servicio deseado.
- **Puerto**: Especifique el puerto de servicio.
- **Método LB**: Seleccione el método de equilibrio de carga preferido para el servicio de Kubernetes seleccionado.

  El método seleccionado actualiza la especificación de entrada con una anotación apropiada. Por ejemplo, si selecciona el método **ROUNDROBIN**, la anotación de Citrix aparece como sigue:

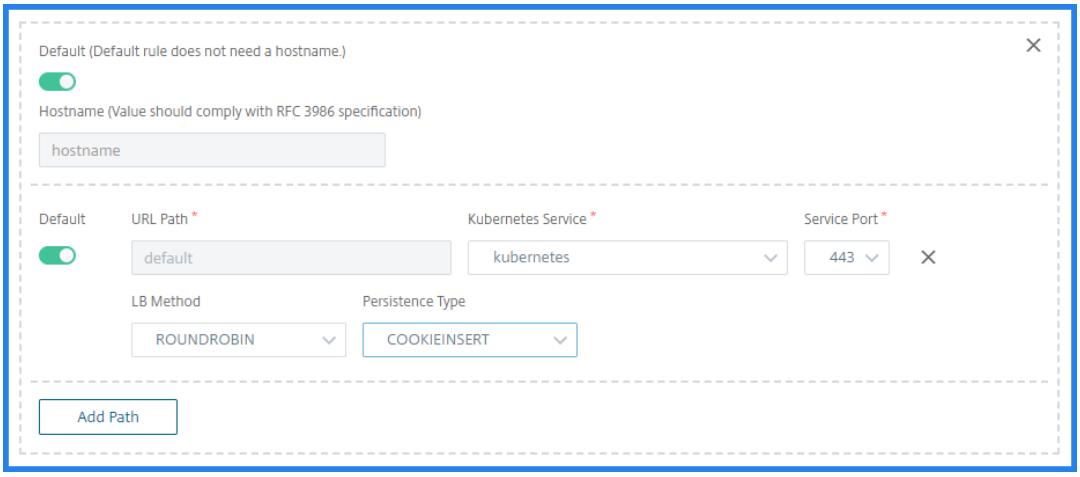
  ```
  "lbmethod":"ROUNDROBIN"
  <!--NeedCopy-->
  ```

- **Tipo de persistencia**: Seleccione el tipo de persistencia de equilibrio de carga preferido para el servicio de Kubernetes seleccionado.

  El tipo de persistencia seleccionado actualiza la especificación de entrada con una anotación apropiada. Por ejemplo, si selecciona **COOKIEINSERT**, la anotación de Citrix aparece de la siguiente manera:

  ```
  "persistenceType":"COOKIEINSERT"
  <!--NeedCopy-->
  ```

Haga clic en **Agregar** para agregar más rutas de URL y puertos a la configuración de Ingress.



Después de la implementación, la configuración de Ingress redirige el tráfico del cliente a un servicio específico en función de lo siguiente:

- La ruta URL y el puerto solicitados.
- El método LB y el tipo de persistencia definidos.

> **Nota**
>
> Se espera que los servicios de Kubernetes utilizados en una configuración de ingreso sean de tipo NodePort.

g) Si lo desea, especifique una **descripción de entrada**.

h) haga clic en **Implementar**

Si quiere revisar la configuración antes de implementar, haga clic en **Generar especificación de ingreso**. La configuración de Ingress especificada aparece en formato YAML. Después de revisar la configuración, haga clic en **Implementar**.

> **Nota**
> Aplique licencias a los servidores virtuales que se crean mediante configuraciones de Ingress. Para aplicar la licencia, lleve a cabo los siguientes pasos:
>
> 1. Vaya a **Configuración > Configuración de licencias y análisis**.
> 2. En **Resumen de licencia del servidor virtual**, habilite la **selección automática de servidores virtuales**.

Video Insight

January 30, 2024

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 NetScaler 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 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, consulte Optimización de vídeo. Al integrar el dispositivo NetScaler con NetScaler Application Delivery Management (ADM), se recopila información clave de los datos de vídeo que fluyen por el dispositivo NetScaler. 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 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 con licencia NetScaler Premium. La licencia NetScaler Premium es compatible con las plataformas NetScaler Telco (VPX T1000 y VPX-T).

Para configurar Video Insight en una instancia de NetScaler, primero habilite la función AppFlow, configure un recopilador, una acción y una directiva de AppFlow y vincule la directiva globalmente. Al configurar el recopilador, debe especificar la dirección IP del servidor NetScaler ADM en el que desea supervisar los informes.

Para configurar la información de vídeo en una instancia de NetScaler, 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`

enable feature AppFlow

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-->
```

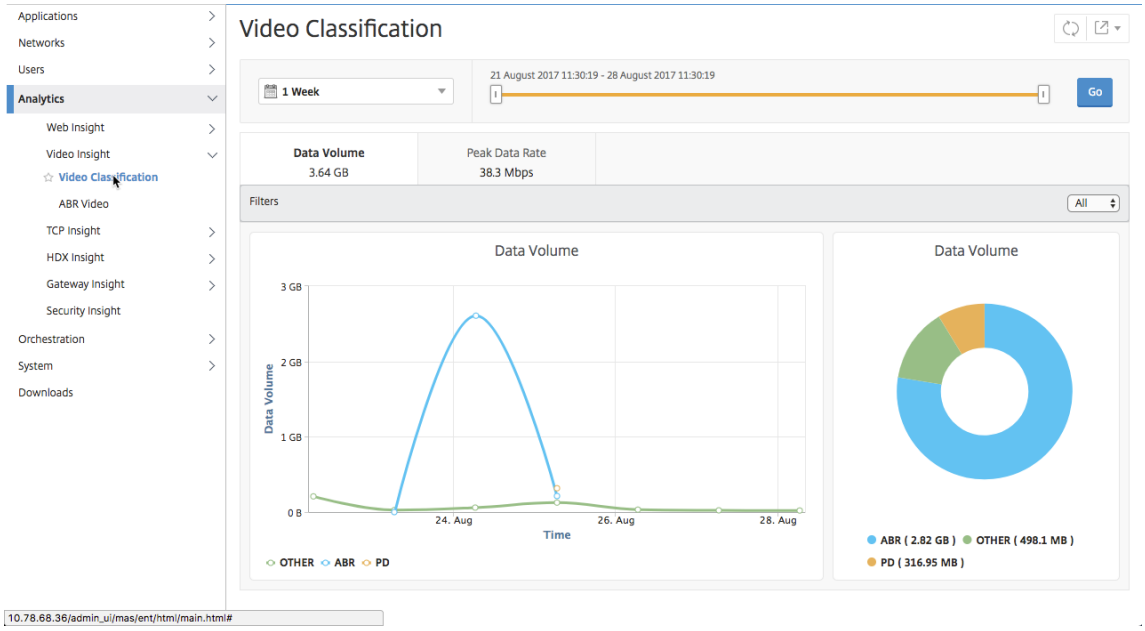
Visualización de las métricas de Video Insight en NetScaler ADM

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 NetScaler 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 que no son ABR ni PD en el tráfico de vídeo, según el 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

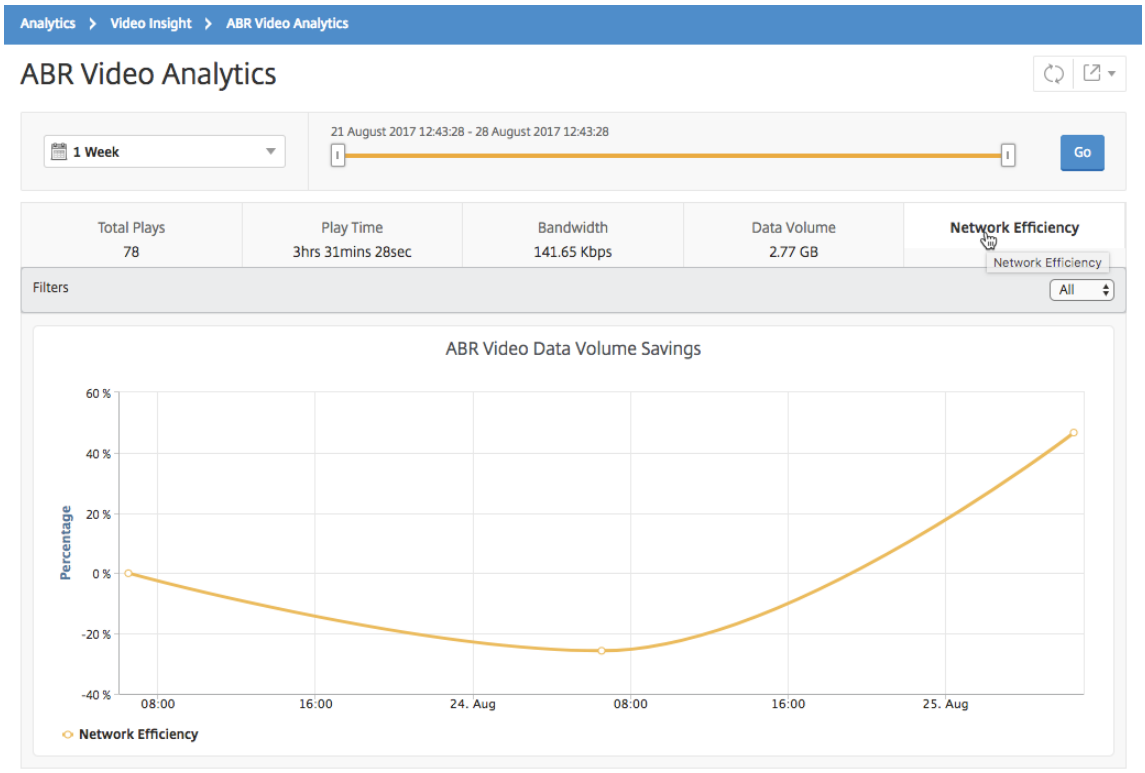
January 30, 2024

Para un período de tiempo determinado, NetScaler Application Delivery Management (ADM) proporciona un gráfico que muestra la proporción de sesiones de vídeo optimizadas y no optimizadas en el período de tiempo. 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 ahorrado por la optimización:

1. Vaya a **Analytics > Video Insight**y haga clic en **ABR Video.**
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. 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

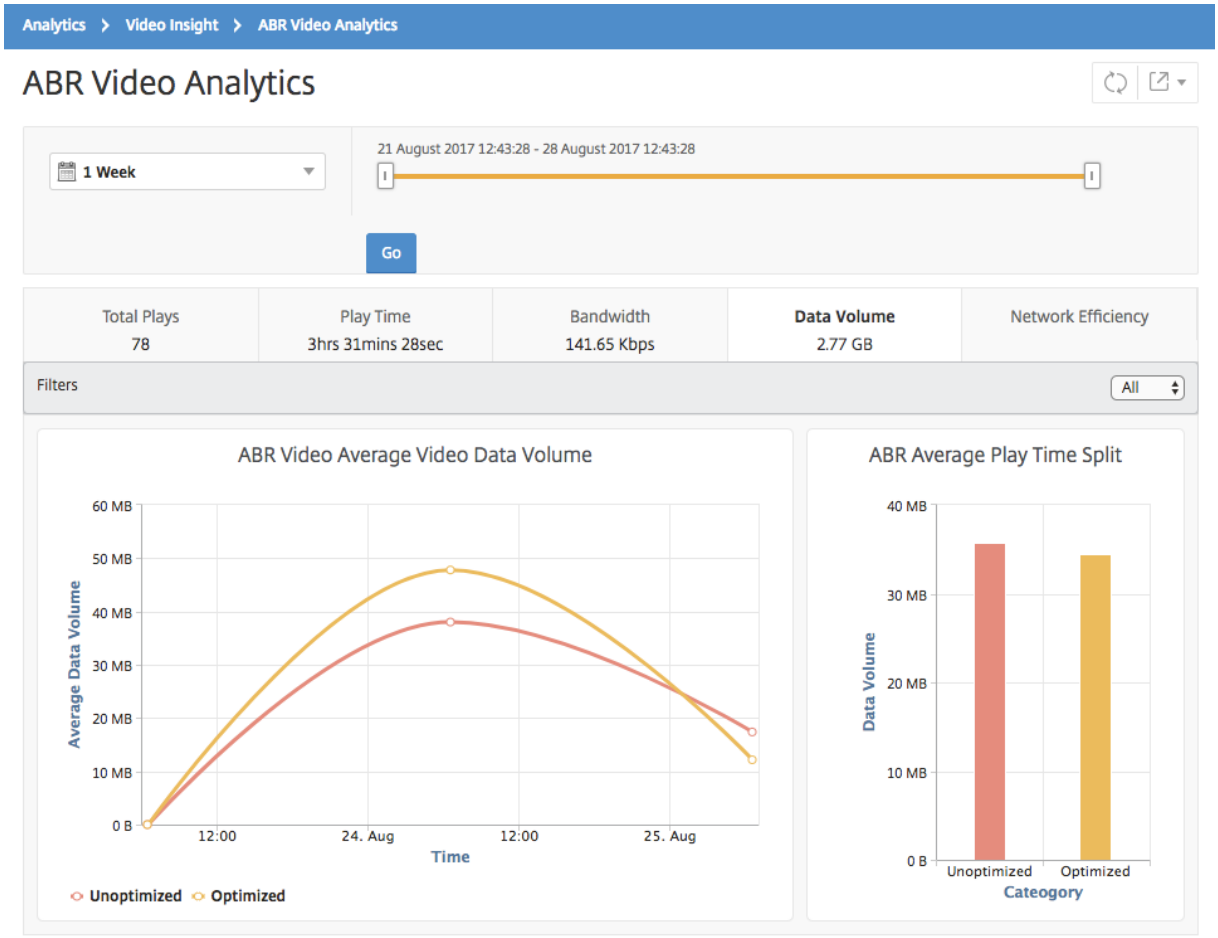
Durante un período de tiempo determinado, NetScaler Application Delivery Management (ADM) muestra el volumen de datos utilizado en los vídeos de ABR optimizados y no optimizados, para que pueda comparar los dos volúmenes.

Para ver el volumen de datos que utilizan los vídeos de ABR:

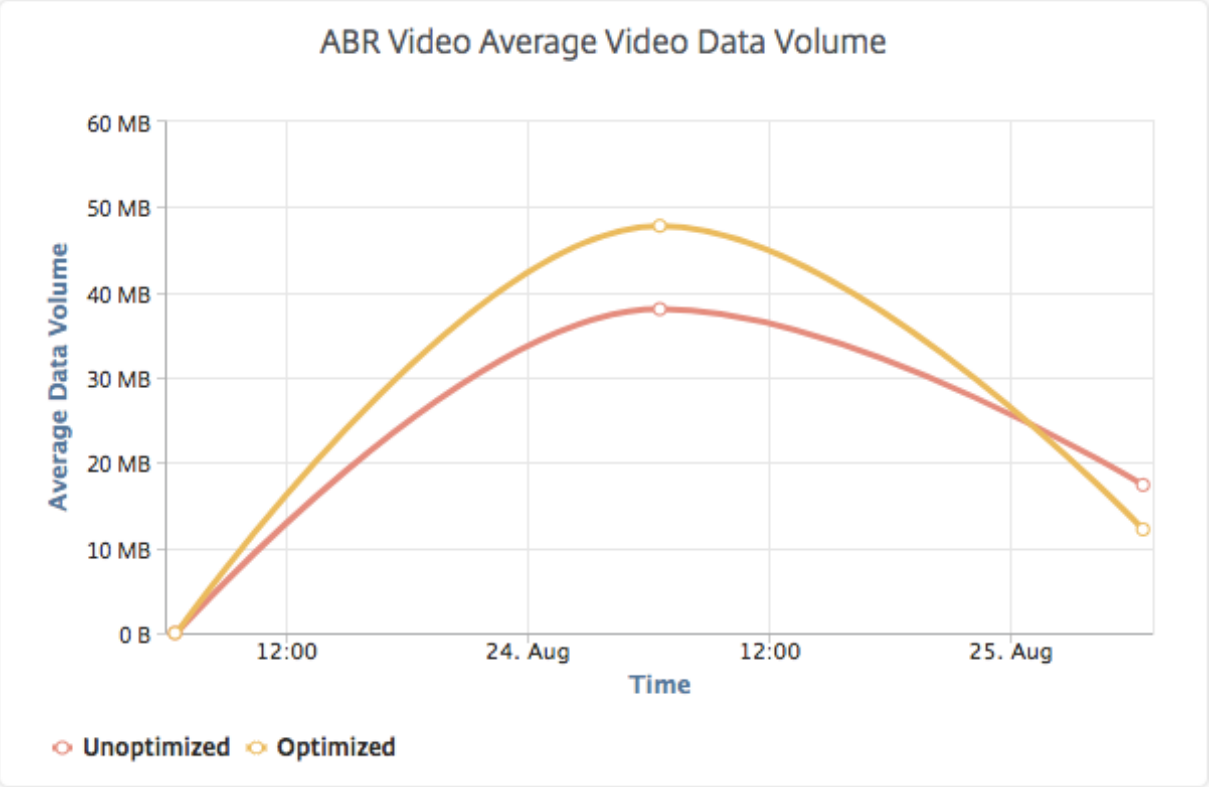
1. Vaya a **Analytics > Video Insight**y haga clic en **ABR Video.**
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.

3. Haga clic en **Ir** y seleccione la ficha **Volumen de datos**.

Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR 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

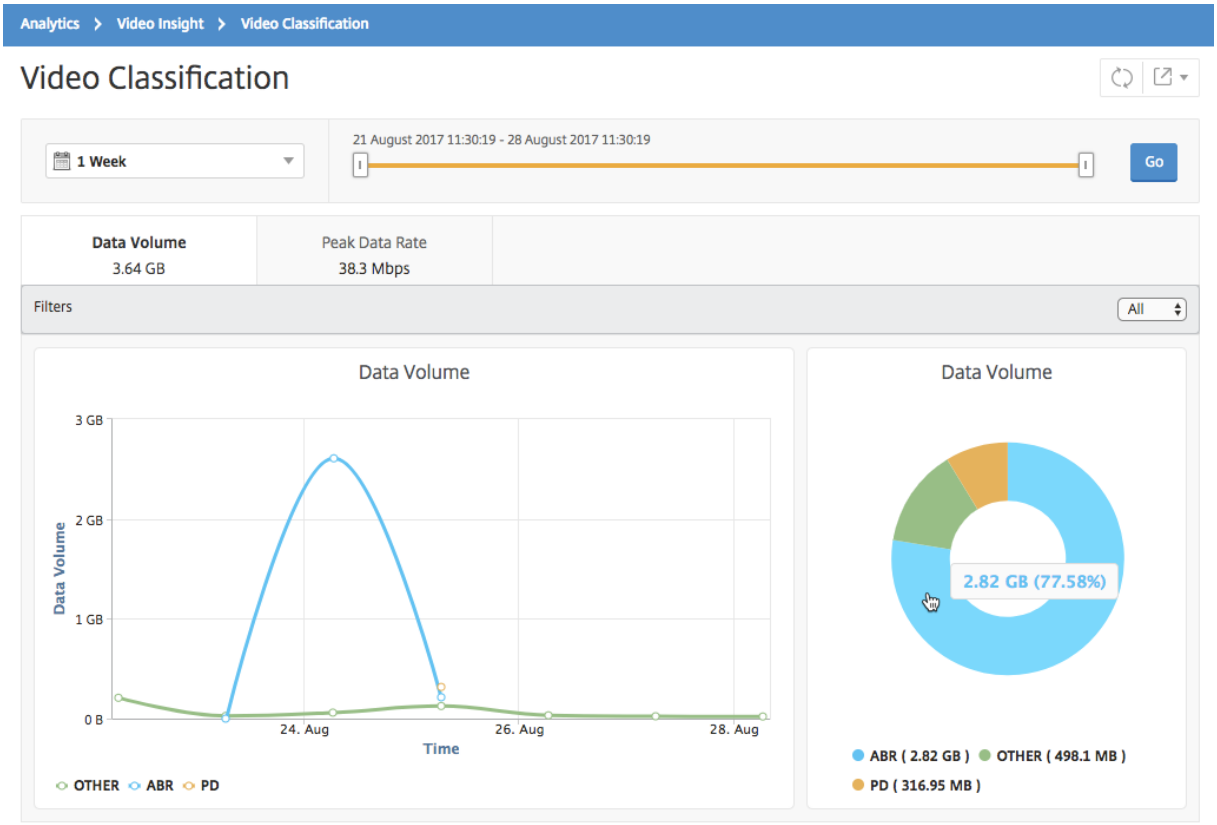
January 30, 2024

El dispositivo NetScaler 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.

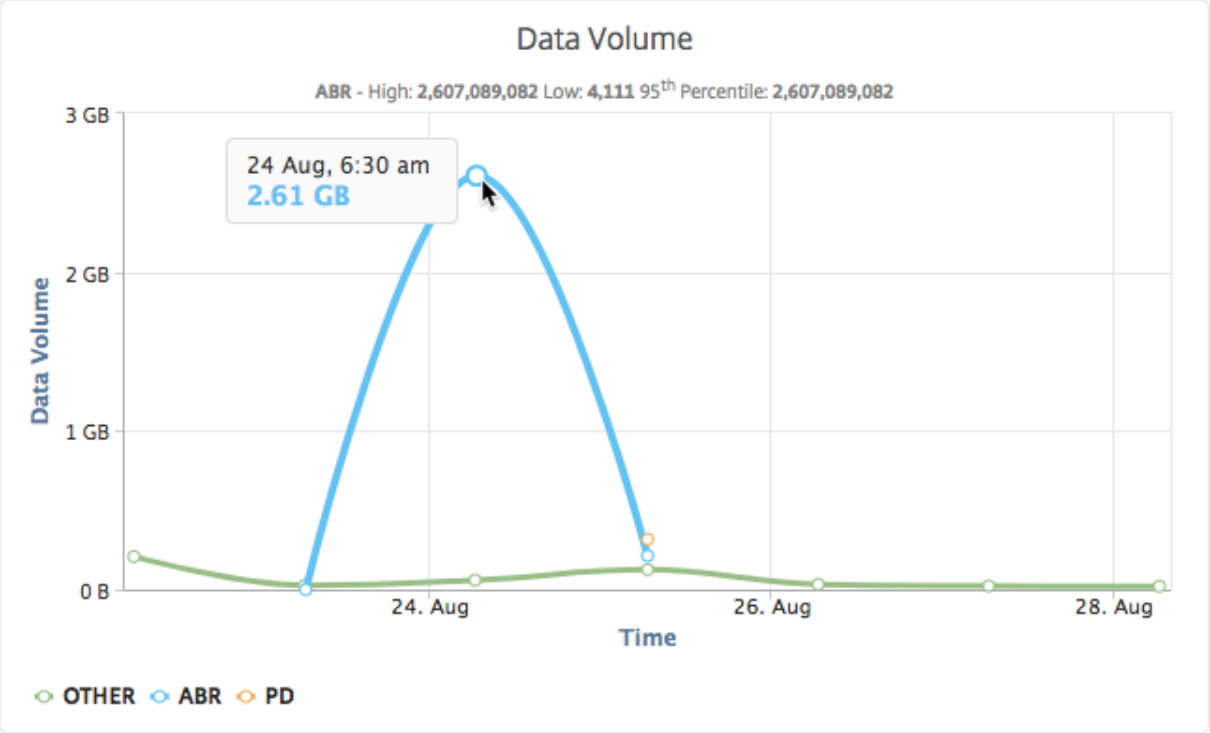
Para ver los tipos de vídeos y el volumen de datos consumido:

1. Vaya a **Analytics > Video Insight** y haga clic en **Clasificación de vídeos**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir**.

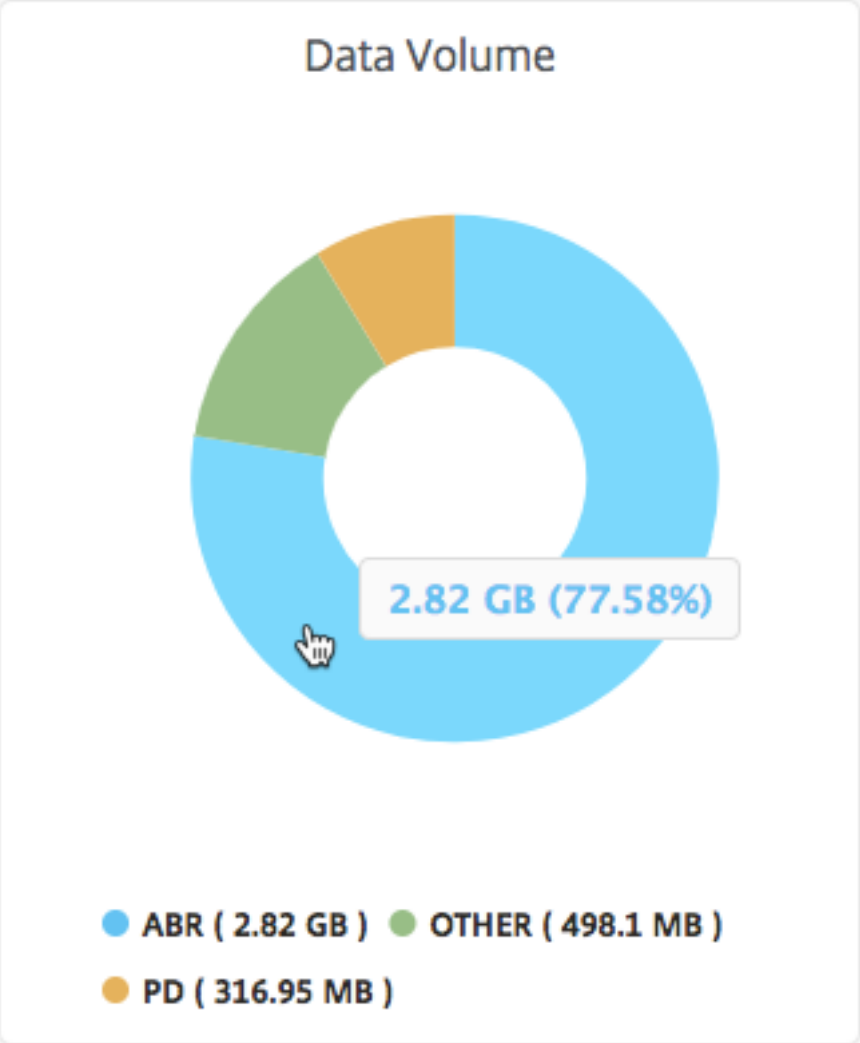
Puede utilizar la lista **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.



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

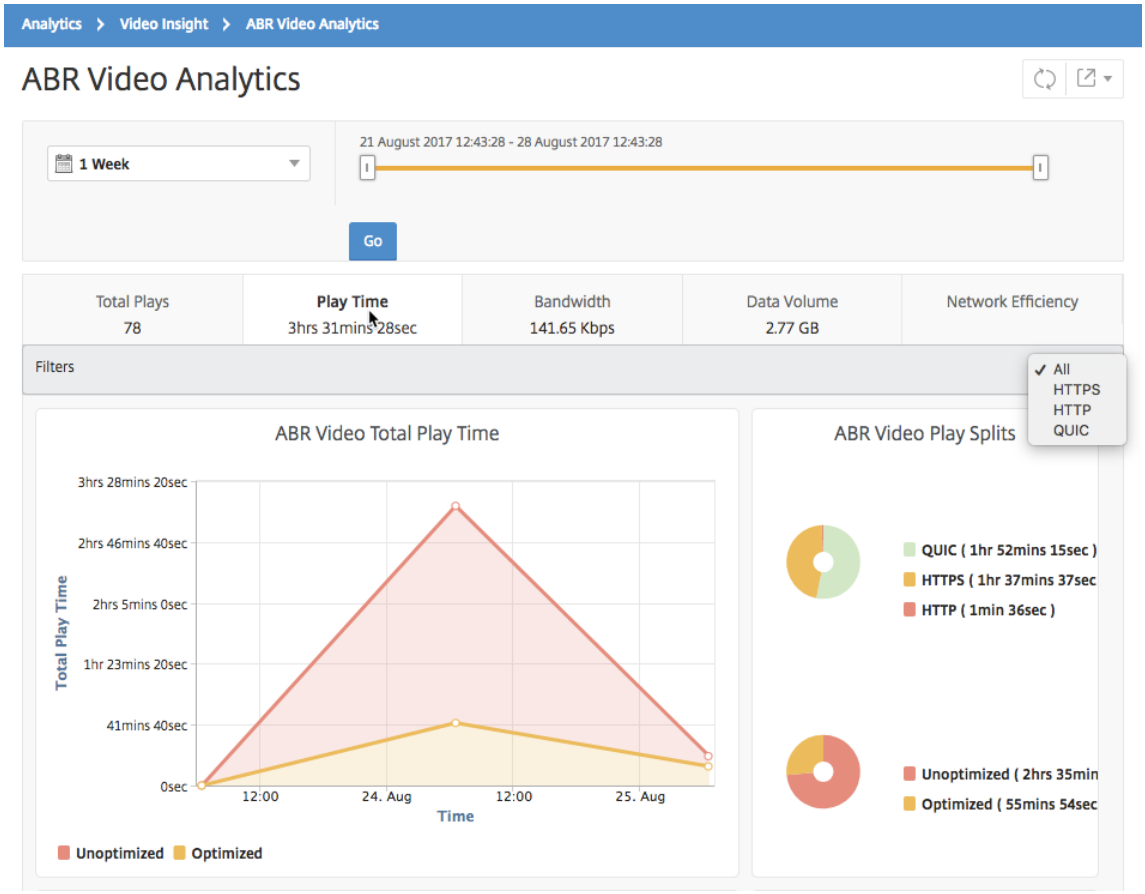
Durante un período de tiempo determinado, NetScaler Application Delivery Management (ADM) proporciona el tiempo de reproducción de los vídeos ABR y también le permite comparar el tiempo de reproducción de los vídeos ABR optimizados y no optimizados en su red.

Para ver el tiempo de juego:

1. Vaya a **Analytics > Video Insight** y haga clic en **ABR Video.**
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.

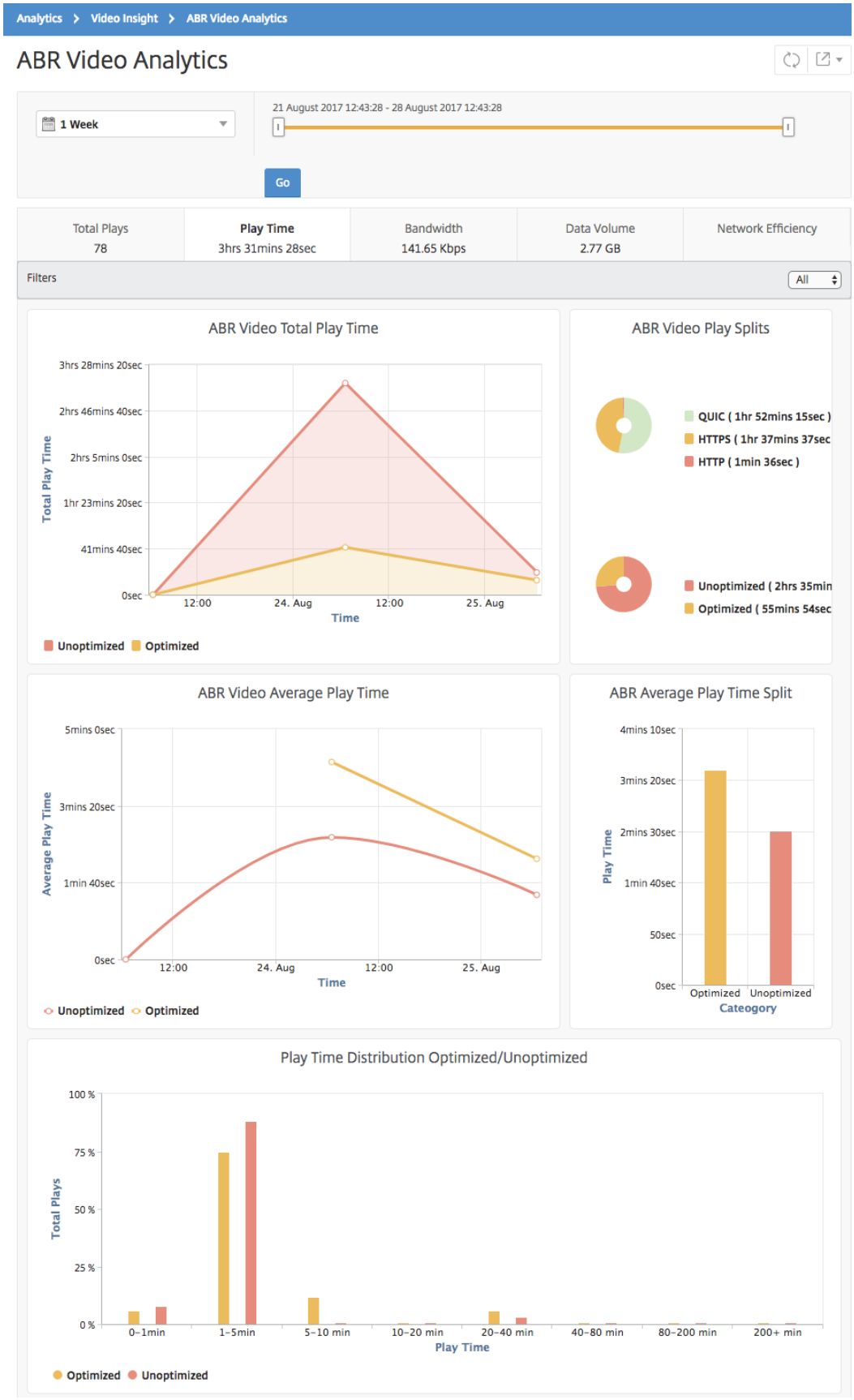
3. Haga clic en **Ir** y seleccione la ficha **Tiempo de reproducción**.

   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR 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

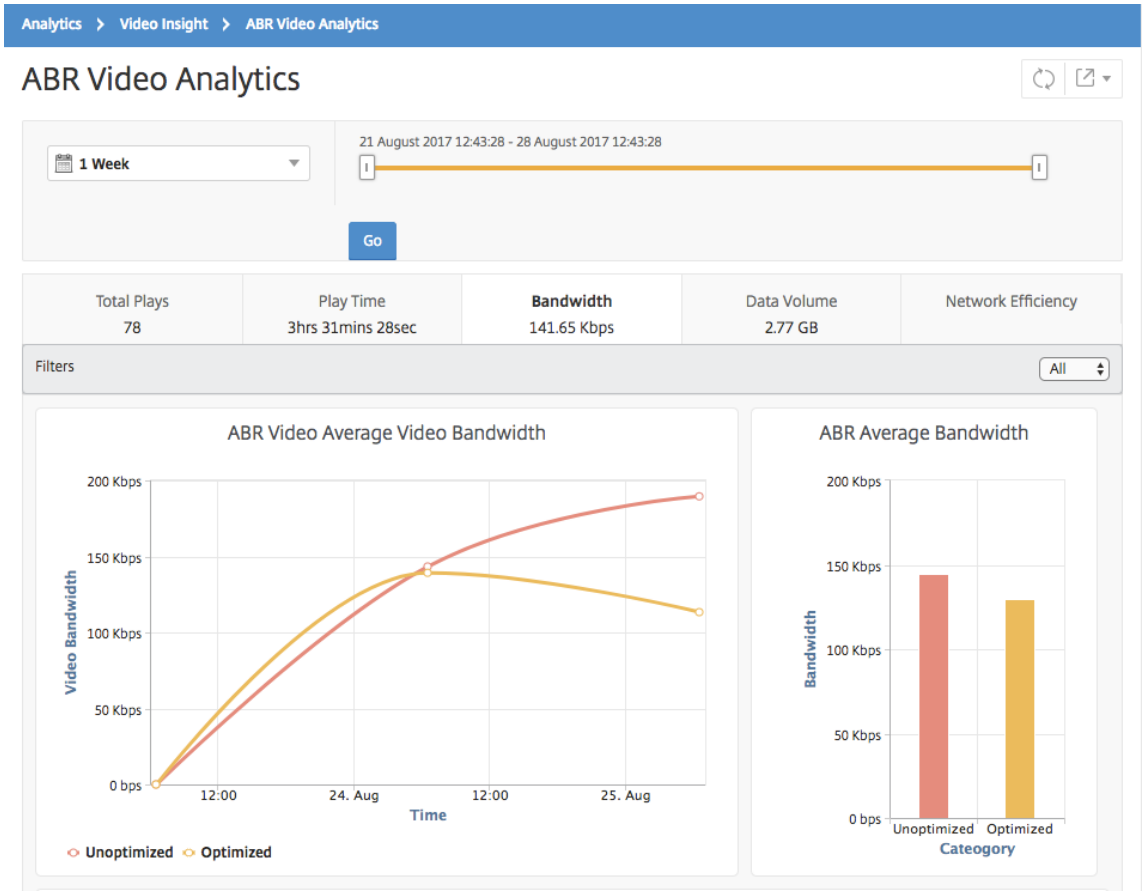
Durante un período de tiempo determinado, NetScaler Application Delivery Management (ADM) proporciona el ancho de banda que consumen los vídeos ABR optimizados y no optimizados y también le permite comparar el ancho de banda consumido por los vídeos ABR optimizados y no optimizados de su red en función de:

- Tiempo de reproducción
- Volumen de datos

Para ver el consumo de ancho de banda:

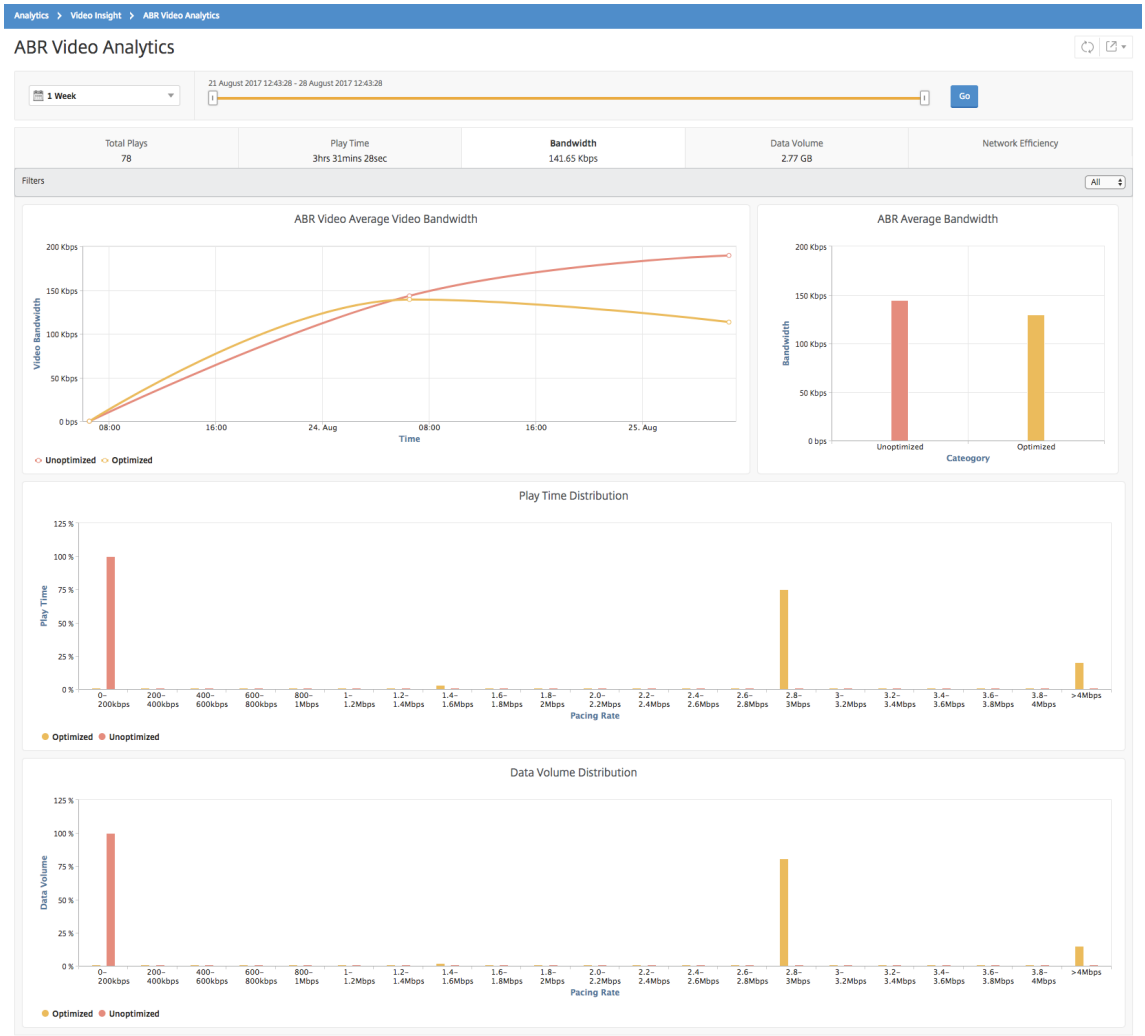
1. Vaya a **Analytics > Video Insight** y haga clic en **ABR Video Analytics**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Ancho de banda**.

   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR 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

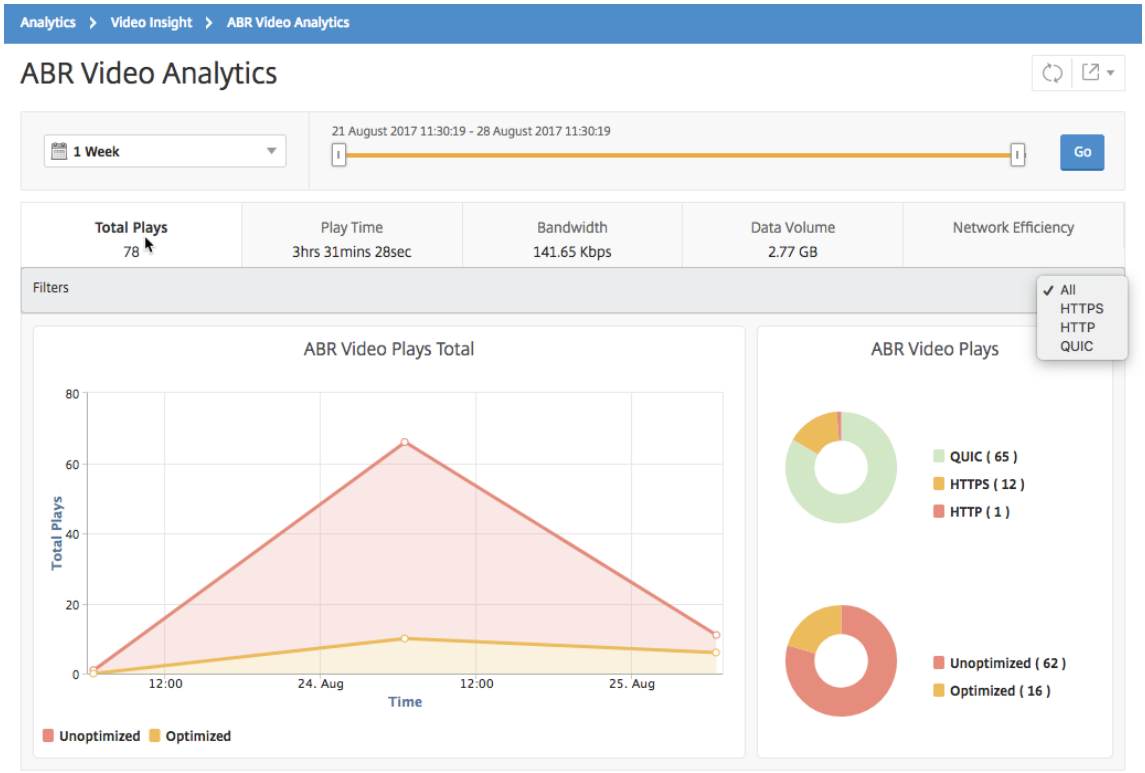
Durante un período de tiempo determinado, NetScaler Application Delivery Management (ADM) muestra el número de reproducciones de vídeos ABR y le permite comparar el número de reproducciones optimizadas y no optimizadas en su red.

Para ver el número de jugadas:

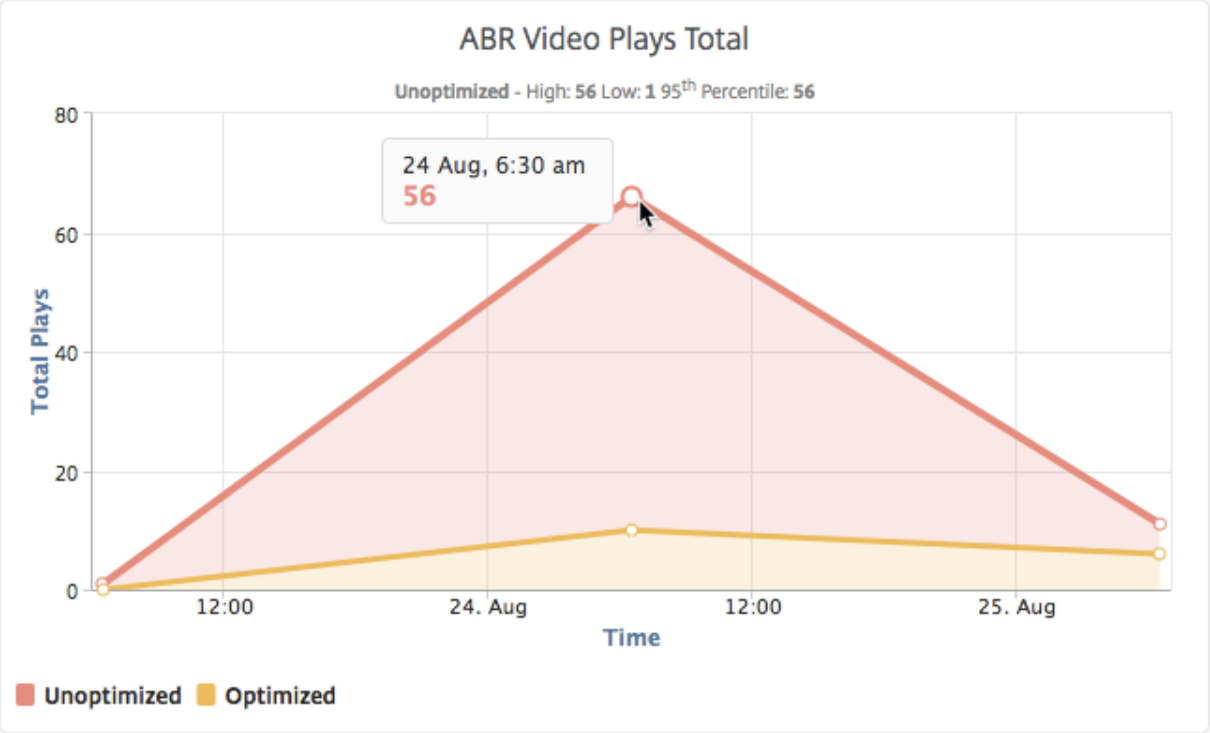
1. Vaya a **Analytics > Video Insight**y haga clic en **ABR Video Analytics**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.

3. Haga clic en **Ir** y seleccione la ficha **N.º de reproducciones**.

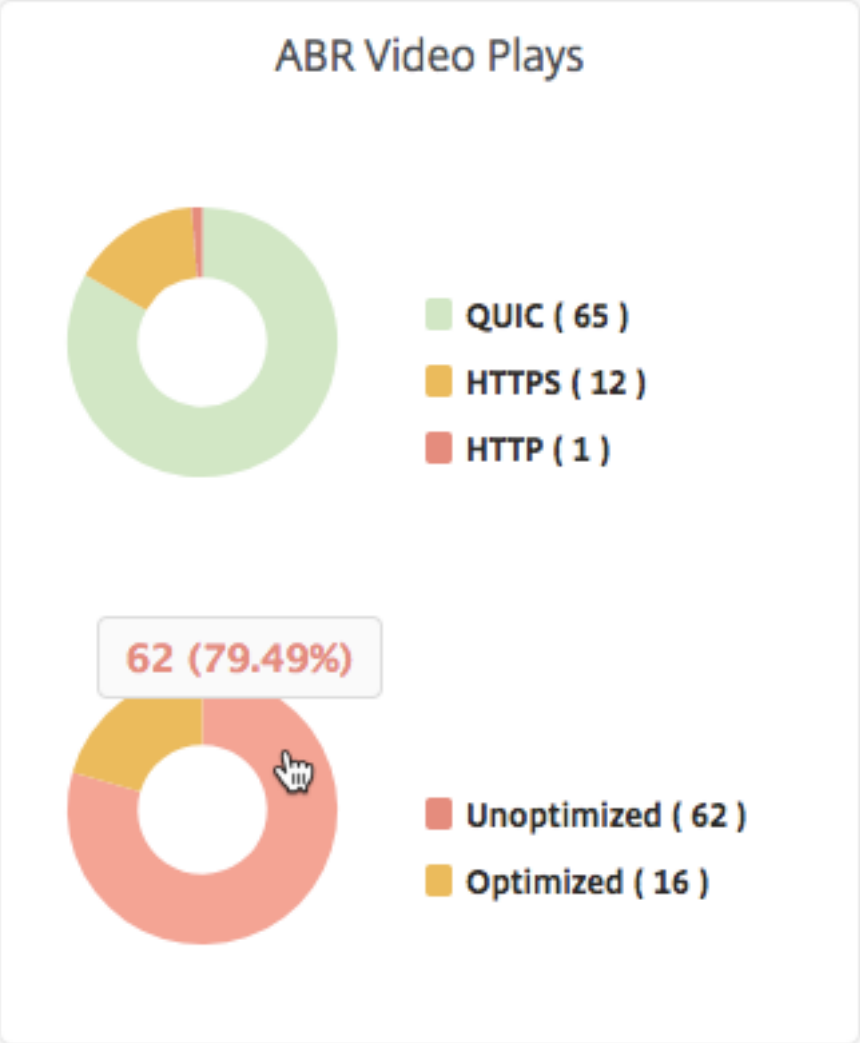
   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.



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

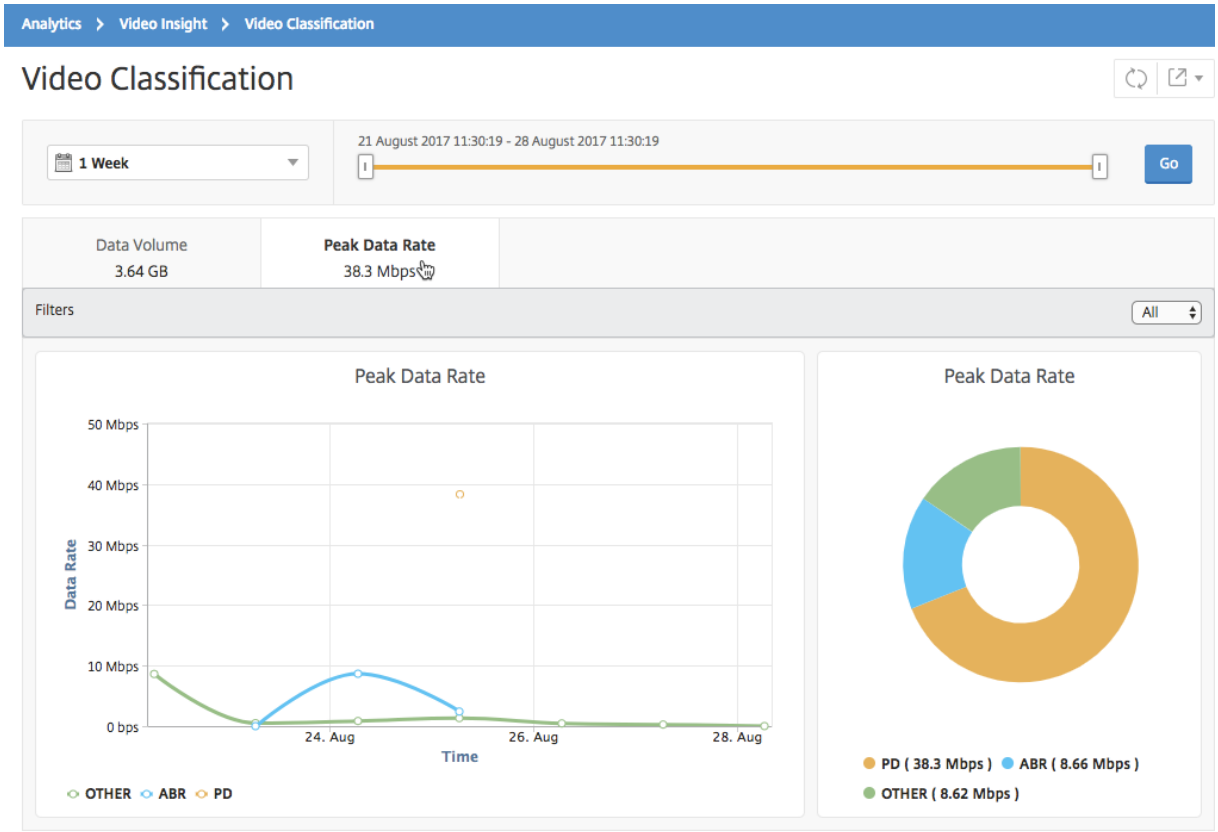
January 30, 2024

NetScaler Application Delivery Management (ADM) le muestra el rendimiento máximo o la velocidad de datos del tráfico de vídeo de su red.

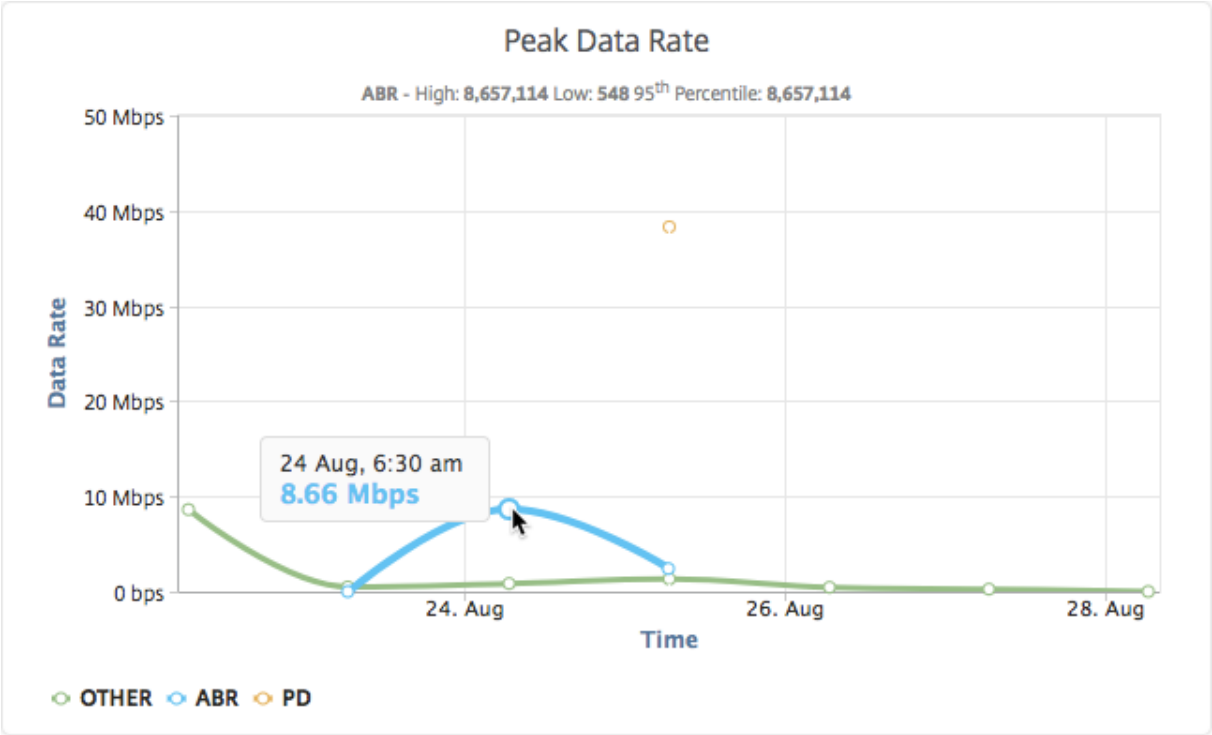
Para ver la velocidad máxima de datos del tráfico de vídeo:

1. Vaya a **Analytics > Video Insight**y haga clic en **Clasificación de vídeos**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Tasa de datos máxima**.

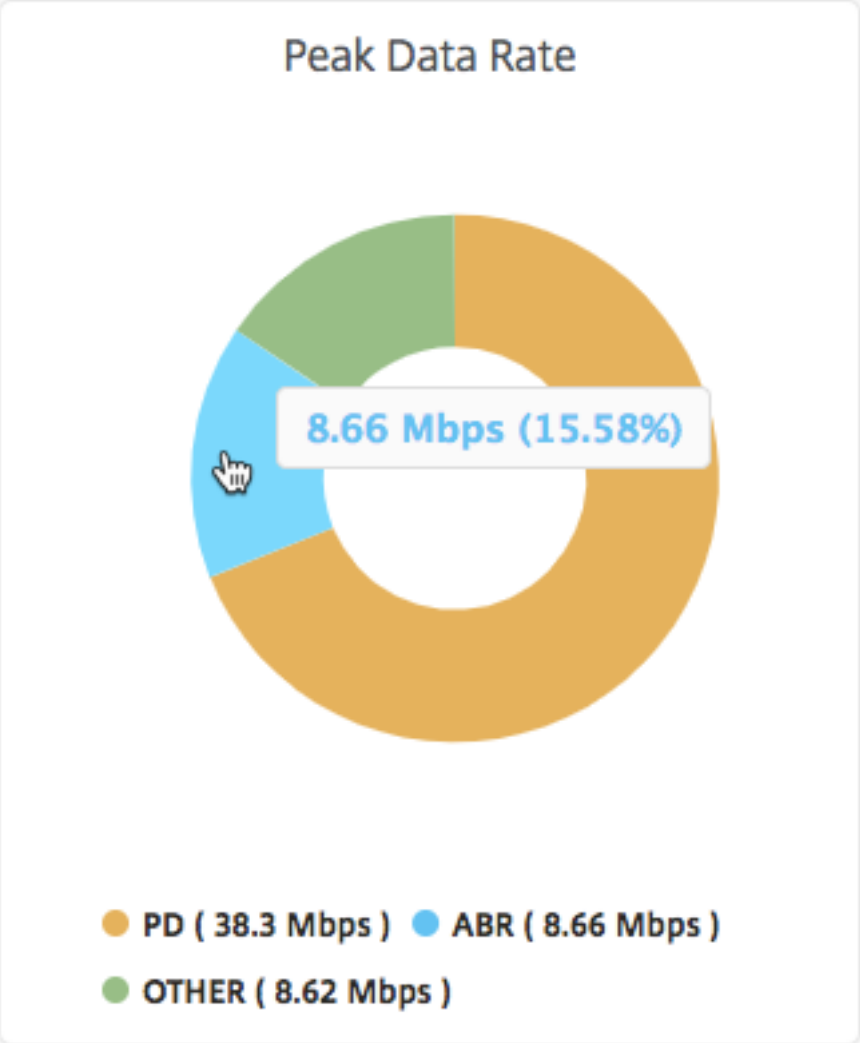
Puede utilizar la lista **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.



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.



Configurar la administración de direcciones IP (IPAM)

January 30, 2024

NetScaler ADM IPAM le permite asignar y liberar automáticamente direcciones IP en las configuraciones administradas de NetScaler ADM. Puede asignar direcciones IP desde redes o rangos de IP definidos mediante los siguientes proveedores de IP:

- Proveedor de IPAM integrado de NetScaler ADM.
- Solución IPAM de Infoblox.

Puede utilizar NetScaler ADM IPAM en:

- **StyleBooks**: asigna automáticamente las IP a los servidores virtuales al crear configuraciones.

- Puerta de**enlace de API**: Asigne automáticamente una dirección IP al proxy de API.

También puede realizar un seguimiento de las direcciones IP de cada red o del rango de IP administrado por NetScaler ADM.

Agregar un proveedor de direcciones IP externo

NetScaler ADM tiene un proveedor de IPAM integrado para administrar las IP y los rangos de IP. También puede utilizar un proveedor de direcciones IP externo para NetScaler ADM.

> **Importante:**
>
> Antes de empezar, asegúrese de que los siguientes permisos estén habilitados en el proveedor de direcciones IP externo:
>
> - Capacidad para consultar redes que están presentes en el proveedor.
> - Reserve una dirección IP en la red.
> - Libere una dirección IP de la red.
> - Recupere las direcciones IP usadas de una red.
> - Recuperar direcciones IP disponibles de una red.

Realice los siguientes pasos para agregar una solución de proveedor de IPAM externo en NetScaler ADM:

1. Vaya a **Configuración > IPAM**.
2. En **Proveedores**, haga clic en **Agregar**.
3. Especifique los siguientes detalles para agregar un proveedor de IPAM:
   - **Nombre**: especifique el nombre del proveedor de IP que se utilizará en NetScaler ADM.
   - **Proveedor**: Seleccione un proveedor IPAM de la lista.
   - **URL**: especifique la URL de la solución de IPAM que asigna direcciones IP en un entorno NetScaler ADM. Asegúrese de especificar la dirección URL en el siguiente formato:

     ```
     https://<host name>
     <!--NeedCopy-->
     ```

     Ejemplo:`https://myinfoblox.example.com`
   - **Nombre de usuario**: especifique el nombre de usuario para iniciar sesión en la solución IPAM.
   - **Contraseña**: especifique la contraseña para iniciar sesión en la solución IPAM.
4. Haga clic en **Agregar**.

Infoblox DDI como proveedor externo

Actualmente, NetScaler ADM admite Infoblox DDI como proveedor externo.

Puede usar NetScaler ADM IPAM con el proveedor de Infoblox para realizar las siguientes acciones:

- Listar redes IPAM
- Crear, actualizar y eliminar redes IPAM
- Reservar y liberar una dirección IP de las redes IPAM

Crear una red IPAM Para crear una red ADM IPAM de NetScaler mediante el proveedor Infoblox, debe existir una red con el mismo rango de IP CIDR en Infoblox.

Cuando crea una red IPAM en NetScaler ADM, solo registra el uso de la red Infoblox en NetScaler ADM. Luego, ADM trabaja junto con Infoblox para administrar las direcciones IP asignadas desde la red. La red InfoBlox puede seguir utilizándose fuera de NetScaler ADM.

Del mismo modo, si elimina la red NetScaler ADM IPAM, NetScaler ADM anula el registro de la red Infoblox. Esto significa que NetScaler ADM ya no interactúa con Infoblox para la administración de direcciones IP en esa red.

API de Infoblox DDI NetScaler ADM IPAM utiliza las siguientes API de Infoblox para realizar las acciones respectivas:

- (/network): Enumera todas las redes Infoblox disponibles
- (/network?network={id}): Recupera detalles de una red Infoblox específica
- (/ipv4address): Enumera todas las IP de una red Infoblox
- (/record:host): Recupera los detalles de una dirección IP específica
- (/{IP}): Reserva y libera direcciones IP en una red Infoblox

Para obtener más información sobre las API de Infoblox, consulte la guía de referencia de la API REST de Infoblox, disponible en Infoblox DDI.

Agregar una red

Agregue una red para usar IPAM con las configuraciones administradas de NetScaler ADM.

1. Vaya a **Configuración > IPAM**.
2. En **Redes**, haga clic en **Agregar**.
3. Especifique los siguientes detalles:
    - **Nombre de red**: especifique el nombre de la red para identificar la red en NetScaler ADM.

- **Proveedor**: Seleccione el proveedor de la lista.

  En esta lista se muestran los proveedores agregados a NetScaler ADM.

- **Tipo de red**: Seleccione el **intervalo de direcciones IP** o **CIDR** de la lista según sus requisitos.

- **Valor de red**: Especifique el valor de la red.

  > **Nota:**
  >
  > NetScaler ADM IPAM solo admite direcciones IPv4.

  Para el **intervalo de IP**, especifique el valor de red en el siguiente formato:

  ```
  <first-IP-address>-<last-IP-address>
  <!--NeedCopy-->
  ```

  Ejemplo :

  ```
  10.0.0.20-10.0.0.100
  <!--NeedCopy-->
  ```

  Para **CIDR**, especifique el valor de la red en el siguiente formato:

  ```
  <IP-address>/<subnet-mask>
  <!--NeedCopy-->
  ```

  Ejemplo :

  ```
  10.70.124.0/24
  <!--NeedCopy-->
  ```

4. Haga clic en **Crear**.

Ver direcciones IP asignadas

Para ver más detalles acerca de las direcciones IP asignadas desde la red IPAM, siga estos pasos:

1. Vaya a **Configuración > IPAM**.
2. En la ficha **Redes**, haga clic en **Ver todas las IP asignadas**.

   Este panel muestra la dirección IP, el nombre del proveedor, el proveedor del proveedor y la descripción. También muestra los detalles del recurso que reservaron esta dirección IP:

   - **Módulo**: muestra el módulo NetScaler ADM que reservó la dirección IP. Por ejemplo, si StyleBooks reservó la dirección IP, esta columna muestra StyleBooks como módulo.

- **Tipo de Recurso**: Muestra el tipo de recurso de ese módulo. Para el módulo StyleBooks, solo el tipo de recurso de configuraciones utiliza la red IPAM. Por lo tanto, muestra Configuraciones bajo esta columna.
- **ID de recurso**: muestra el ID de recurso exacto con un enlace. Haga clic en este vínculo para acceder al recurso que está utilizando la dirección IP. Para el tipo de recurso de configuración, muestra el ID del paquete de configuración como el ID del recurso.

> **Nota:**
>
> Si quiere liberar la dirección IP, seleccione la dirección IP que quiera liberar y haga clic en Liberar **direcciones IP asignadas**.

Utilice los registros de auditoría de ADM para administrar y supervisar su infraestructura

January 30, 2024

Puede utilizar el servicio ADM de NetScaler para realizar un seguimiento de todos los eventos de ADM y syslog generados en las instancias de ADC administradas por ADM. Estos mensajes pueden ayudarlo a administrar y supervisar su infraestructura. Sin embargo, los mensajes de registro son una excelente fuente de información solo si los revisas, y ADM simplifica la forma de revisar los mensajes de registro.

Puede usar filtros para buscar mensajes de registro de auditoría y syslog de ADM. Los filtros ayudan a acotar los resultados y a encontrar exactamente lo que busca en tiempo real. La Ayuda de búsqueda integrada le guía para filtrar los registros. Otra forma de ver los mensajes de registro es exportarlos en formato PDF, CSV, PNG y JPEG. Puede programar la exportación de estos informes a direcciones de correo electrónico especificadas en distintos intervalos.

Puede revisar los siguientes tipos de mensajes de registro desde la GUI de ADM:

- Registros de auditoría relacionados con instancias de ADC
- Registros de auditoría relacionados con ADM
- Registros de auditoría de aplicaciones

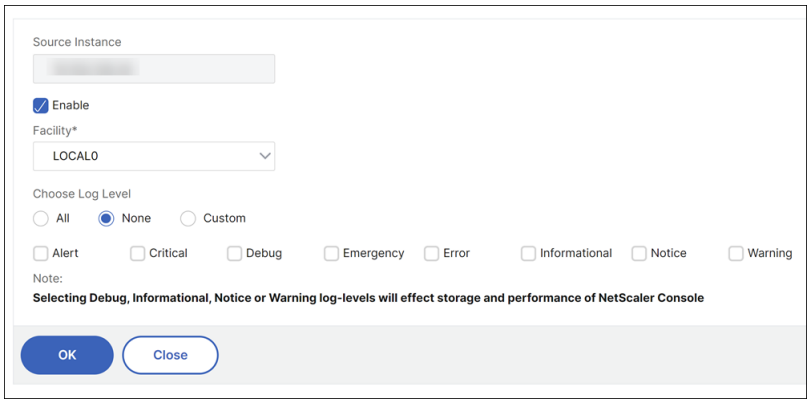
Registros de auditoría relacionados con instancias de ADC

Antes de poder ver los mensajes de syslog relacionados con la instancia de ADC desde ADM, configure el servicio ADM de NetScaler como el servidor syslog de su instancia de NetScaler. Una vez completada la configuración, todos los mensajes syslog se redirigen desde la instancia a ADM.

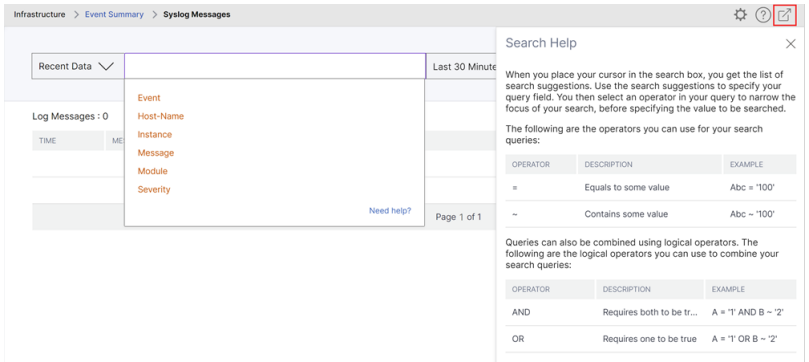
Configurar el servicio ADM como servidor syslog

Siga estos pasos para configurar ADM como el servidor syslog:

1. En la GUI de ADM, vaya a **Infraestructura > Instancias**.
2. Seleccione la instancia de NetScaler desde la que quiere que se recopilen y muestren los mensajes syslog en NetScaler ADM.
3. En la lista **Seleccionar acción**, seleccione **Configurar Syslog**.
4. Haga clic en **Activar**.
5. En la lista desplegable de **instalaciones**, seleccione una instalación local o a nivel de usuario.
6. Seleccione el nivel de registro requerido para los mensajes de syslog.
7. Haga clic en **Aceptar**.



Estos pasos configuran todos los comandos syslog en la instancia de NetScaler y NetScaler ADM comienza a recibir los mensajes syslog. Para ver los mensajes, vaya a **Infraestructura > Eventos > Mensajes de Syslog**. Haga clic en **¿Necesita ayuda?** para abrir la ayuda de búsqueda integrada. Para obtener más información, consulte Ver y exportar mensajes de syslog.



Para exportar los mensajes de registro, haga clic en el icono de flecha de la esquina superior derecha.

A continuación, haga clic en **Exportar ahora** o **Planificar exportación**. Para obtener más información, consulte Ver y exportar mensajes de syslog.

Registros de auditoría relacionados con ADM

Según reglas preconfiguradas, ADM genera mensajes de registro de auditoría para todos los eventos en, lo que le ayuda a supervisar el estado de la infraestructura. Para ver todos los mensajes del registro de auditoría presentes en el ADM, vaya a **Configuración > Mensajes del registro de auditoría de ADM**.

Para exportar los mensajes de registro, haga clic en el icono de flecha de la esquina superior derecha.

Registros de auditoría relacionados con aplicaciones

Puede ver los mensajes de registro de auditoría para todas las aplicaciones ADM o para una aplicación específica.

- Para ver todos los mensajes de registro de auditoría de todas las aplicaciones presentes en el ADM, vaya a **Infraestructura > Funciones de red > Auditoría**.
- Para ver los mensajes de registro de auditoría de cualquier aplicación específica en ADM, vaya a **Aplicaciones > Panel de control**, haga clic en un servidor virtual y seleccione **Registro de auditoría**.

Administración de licencias de NetScaler para licencias flexibles y agrupadas

January 30, 2024

> **Nota:**
>
> Para obtener información sobre los diferentes tipos de licencias de NetScaler, consulte Descripción general de las licencias.

Todos los detalles relacionados con sus licencias, como la configuración de los puertos, los archivos de licencias, la información de caducidad y la configuración de las notificaciones, se enumeran en esta página. Puede aplicar licencias, configurar las comprobaciones de caducidad de las licencias y establecer notificaciones para el uso de las licencias y los días de caducidad.

Configuración del puerto del servidor de licencias

Las instancias de NetScaler utilizan los puertos para comunicarse con el servidor de licencias. Haga clic en el icono **Editar** y especifique los valores de los siguientes parámetros:

- **Puerto**del servidor de licencias: el puerto del servidor proxy que utilizan las instancias de NetScaler para acceder al portal de licencias de Citrix para la asignación de licencias. Valor predeterminado: 27000.
- **Puerto**daemon del proveedor: el puerto del servidor de licencias que utilizan las instancias de NetScaler para comunicarse con el servidor de licencias. Valor predeterminado: 7279.
- **Puerto**de servidor proxy : NetScaler ADM se puede usar como un proxy HTTP de reenvío para que las instancias de NetScaler accedan al portal MyCitrix para la recuperación automática de licencias. Para habilitar esta función, especifique un puerto TCP en el que el proxy escuche.

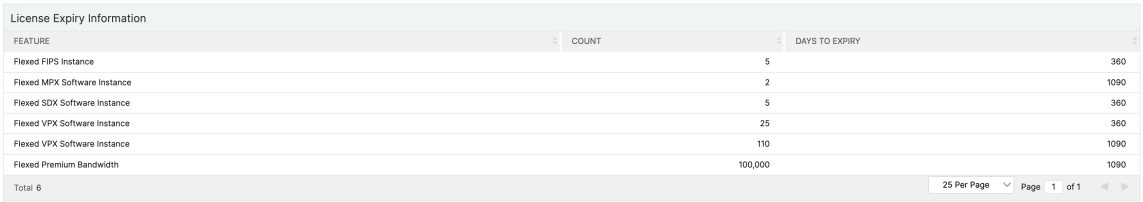
Archivos de licencias

Los archivos de licencia presentes en su NetScaler se enumeran en esta sección. Puede añadir, eliminar y descargar licencias. Debe aplicar las licencias antes de poder utilizarlas.

Aplicar un archivo de licencia

1. Vaya a **NetScaler Licensing > License Management** .
2. En la sección **Archivos de licencia** , haga clic en **Agregar archivo de licencia** y seleccione una de las siguientes opciones:
   - **Cargar archivos de licencia desde un equipo**local : si ya hay un archivo de licencia en su equipo local, puede cargarlo en NetScaler ADM.
   - **Usar código**de acceso a la licencia: especifique el código de acceso a la licencia que ha comprado en Citrix. Haga clic en **Obtener licencias** y, a continuación, en **Finalizar** .
3. Haga clic en **Finalizar**.
   Los archivos de licencia se agregan a NetScaler ADM.
   En la sección **Información de caducidad** de licencias se enumeran las licencias presentes en NetScaler ADM, el recuento y los días que faltan para que caduquen.

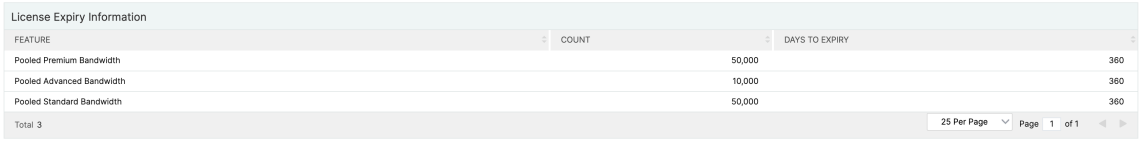
   La siguiente captura de pantalla muestra el número de licencias de instancias de software FIPS de Flexed NetScaler VPX, NetScaler MPX, NetScaler SDX y NetScaler VPX, la capacidad de ancho de banda premium de Flexed actual y los días que faltan para su caducidad.

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Flexed FIPS Instance	5	360
Flexed MPX Software Instance	2	1090
Flexed SDX Software Instance	5	360
Flexed VPX Software Instance	25	360
Flexed VPX Software Instance	110	1090
Flexed Premium Bandwidth	100,000	1090

   Total 6 — 25 Per Page — Page 1 of 1

   La siguiente captura de pantalla muestra el ancho de banda agrupado estándar, avanzado y premium disponible y los días que faltan para su vencimiento.



4. Seleccione un archivo de licencia y haga clic en **Aplicar licencias** .

Eliminar un archivo de licencia

Para eliminar un archivo de licencia, seleccione uno o más archivos y haga clic en **Eliminar** . Al eliminar una licencia, primero debe agregarla y solo entonces podrá aplicarla.

Descargar un archivo de licencia

Para descargar un archivo de licencia, seleccione un archivo y haga clic en **Descargar** . Puede guardar el archivo de licencia sin conexión como copia de seguridad.

Información de caducidad de la licencia

Ahora puede configurar el umbral de caducidad de las licencias de capacidad flexible o agrupada. Cuando se establece el umbral, NetScaler ADM envía notificaciones por correo electrónico o SMS cuando una licencia está a punto de caducar. También se envían una captura SNMP y una notificación cuando la licencia ha caducado 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 desde **Infraestructura > Eventos**.

Ver la caducidad de la licencia

1. Vaya a **NetScaler Licensing > License Management** .
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:
    - **Funcionalidad**: tipo de licencia que va a caducar.
    - **Recuento**: número de instancias o servidores virtuales afectados.
    - **Días hasta la caducidad**: número de días antes de que caduque la licencia.

> **Nota:**
>
> Al agregar nuevas licencias al grupo, las instancias de NetScaler utilizan las nuevas licencias cuando caducan las licencias existentes.

Configuración de notificaciones

Especifique la configuración en función de la cual se enviarán las notificaciones sobre el uso de la licencia y los días que faltan para su caducidad.

1. En la sección **Configuración de notificaciones** , haga clic en el icono **Editar** y seleccione **Notificarme sobre el uso de la licencia** . Establezca el umbral de alerta, que es un porcentaje de la capacidad de las licencias flexibles o agrupadas que se utilizará para enviar una notificación.
2. Seleccione el tipo de notificación que desea enviar cuando las licencias alcancen el umbral o vayan a caducar; para ello, seleccione la casilla correspondiente. Los tipos de notificación son los siguientes. Selecciona un tipo de notificación y haz clic en **Agregar** para agregar detalles. También puedes comprobar que cada notificación se entrega antes de guardar la configuración.

    - **Correo**electrónico : perfil de correo electrónico o lista de distribución para enviar notificaciones. Para obtener más información, consulte Crear una lista de distribución de correo electrónico.
    - **SMS**: perfil de SMS o lista de distribución para enviar notificaciones.
    - **Slack**: detalles del perfil de Slack para enviar notificaciones.
    - **PagerDuty**: perfil de PagerDuty para enviar notificaciones.
    - **ServiceNow**: el perfil Citrix ServiceNow se especifica de forma predeterminada y es la única opción disponible actualmente.
      Para obtener más información sobre la creación de estos perfiles, consulte Configurar notificaciones

3. Especifique los días de caducidad , que es el número de días antes de los que desea recibir una notificación sobre el vencimiento de la licencia.
4. Haga clic en **Guardar**.

Crea una lista de distribución de correo electrónico

Realice los siguientes pasos para crear una lista de distribución de correo electrónico:

1. Selecciona Correo **electrónico** y haz clic en **Agregar** .
2. En **Crear lista de distribución de correo electrónico**, especifique los siguientes detalles:

    - **Nombre**: Especifique el nombre de la lista de distribución.
    - **Servidor**de correo electrónico : seleccione el servidor de correo electrónico que envía una notificación por correo electrónico. Para agregar un servidor de correo electrónico, haga clic en Agregar. Especifique el nombre del servidor/la dirección IP y el puerto. Seleccione Autenticación para exigir la autenticación para acceder al servidor de correo electrónico. Seleccione Seguro si el servidor de correo electrónico admite la autenticación SSL. Haga clic en Crear.

- **De**: especifique la dirección de correo electrónico desde la que NetScaler ADM envía el mensaje.
- **Para**: especifique las direcciones de correo electrónico a las que NetScaler ADM envía el mensaje.
- **Cc**: especifique las direcciones de correo electrónico en las que NetScaler ADM copia el mensaje.
- **Bcc**: especifique las direcciones de correo electrónico en las que el NetScaler ADM copia a ciegas (no muestra la dirección de correo electrónico) el mensaje.

3. Haga clic en **Crear**.

Crea una lista de distribución de SMS

Realice los siguientes pasos para configurar los ajustes de notificación SMS:

1. En **SMS**, haga clic en **Agregar**.
2. En **Crear lista de distribución de SMS**, especifique los siguientes detalles:
   - **Nombre**: Especifique el nombre de la lista de distribución.
   - **Servidor**SMS : seleccione el servidor SMS que envía las notificaciones SMS. Para agregar un servidor de SMS, haga clic en **Agregar** . Especifique los detalles del servidor y haga clic en **Crear** .
   - **Para**: especifique el número de teléfono al que NetScaler ADM envía el mensaje.
3. Haga clic en **Crear**.

Crear un perfil de Slack

Realice los siguientes pasos para crear un perfil de Slack:

1. En **Slack**, haga clic en **Agregar**.
2. En **Crear perfil de Slack**, especifica los siguientes detalles:
   - **Nombre de perfil**: especifique el nombre del perfil. Este nombre aparece en la lista de perfiles de Slack.
   - **Nombre**del canal : especifique el nombre del canal de Slack al que el ADM de NetScaler envía la notificación.
   - **URL del webhook**: especifique la URL del webhook del canal. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal. Todas las notificaciones de eventos que se envían a esta URL se publican en el canal de Slack designado. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK.

Crear un perfil de PagerDuty

PagerDuty le permite configurar las notificaciones por correo electrónico, SMS, notificaciones push y llamadas telefónicas en un número registrado. Antes de añadir un perfil de PagerDuty en NetScaler Application Delivery and Management, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para empezar a usar PagerDuty, consulte la documentación de PagerDuty.

Realice los siguientes pasos para crear un perfil de PagerDuty:

1. En **PagerDuty**, haga clic en **Agregar**.
2. En **Crear perfil de PagerDuty**, especifique los siguientes detalles:
    - **Nombre**de perfil : especifique un nombre de perfil. Este nombre lo utilizan distintos módulos, como las reglas de eventos y las notificaciones SSL, para enviar alertas de PagerDuty.
    - **Clave de integración**: especifique la clave de integración. Puede obtener esta clave en su portal PagerDuty.
3. Haga clic en **Crear**.

Para obtener más información, consulte Servicios e integraciones en la documentación de PagerDuty.

Ver el perfil de ServiceNow

Para habilitar las notificaciones de ServiceNow para los eventos de NetScaler y los eventos de NetScaler ADM, debe integrar la entrega y la administración de aplicaciones de NetScaler con ServiceNow mediante el conector ITSM. Para obtener más información, consulte Integrar NetScaler ADM con la instancia de ServiceNow.

Realice los siguientes pasos para ver y verificar el perfil ServiceNow:

1. En **ServiceNow** , el perfil **Citrix_Workspace_SN** está seleccionado de forma predeterminada .
2. Haga clic en **Probar** para generar automáticamente un tíquet de ServiceNow y verificar la configuración.

Licencia de capacidad flexible

January 30, 2024

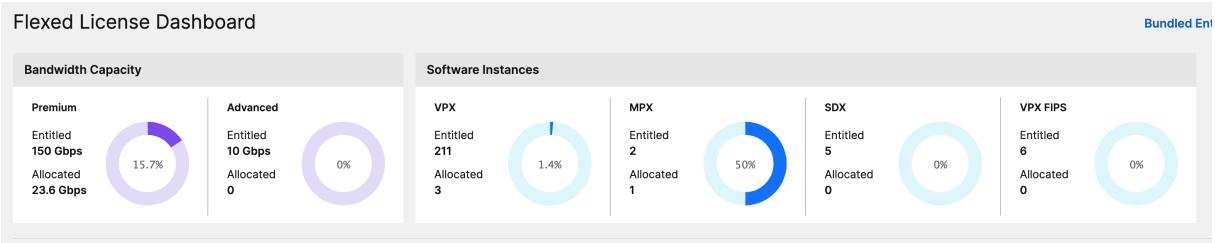
El licenciamiento Flexed de NetScaler es el nuevo marco de licenciamiento destinado a simplificar el proceso de administración de licencias. Su licencia Flexed incluye licencias de instancias de software (VPX/CPX/BLX, SDX, MPX y VPX FIPS) y licencias de capacidad de ancho de banda. Debe aplicar

la licencia Flexed en el servicio NetScaler Console o NetScaler ADM local. También debe aplicar la licencia MPX Z-Cap y SDX Z-Cap en el hardware NetScaler MPX y NetScaler SDX, respectivamente. A continuación, puede asignarlos a todos los formatos de NetScaler implementados en la nube o de forma local.

Una licencia Flexed también ofrece análisis para servidores virtuales ilimitados.

Si tiene una licencia agrupada y ahora ha comprado una licencia Flexed, puede ver los detalles de su licencia en el panel de licencias Flexed. El ancho de banda y las instancias combinados aparecen en el panel de licencias de Flexed.

La licencia de ancho de banda normalmente incluye solo la edición Premium, a menos que anteriormente tuviera una licencia Pooled Standard o Advanced, en cuyo caso las ediciones Standard, Advanced y Premium aparecen en el panel de licencias Flexed.



Para obtener más información, consulte el panel de licencias Flexed.

Puede usar las licencias Flexed 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.

Recopilación de telemetría con licencia Flexed

Para cumplir con los requisitos actuales de licencia de Flexed, habilite ADM On-Prem Cloud Connector. Esta función conecta su ADM local con el servicio ADM (ahora renombrado como servicio NetScaler Console) para la recopilación de telemetría. Le recomendamos que habilite la recopilación de telemetría cuando utilice las licencias Flexed. Para habilitar ADM On-Prem Cloud Connector, consulte Cloud Connector.

El Cloud Connector local de ADM permitirá a Citrix Cloud recopilar datos de licencia, configuración y uso para cumplir con las licencias y administrar, medir y mejorar el servicio. Obtenga más información sobre los datos que recopilamos.

> **Nota:**
>
> Además de este modo automatizado de recopilación de datos, en una versión futura estará disponible un modo manual para habilitar y compartir los datos de telemetría. Puede compartir los datos de telemetría a través del modo automático o manual. Una vez que ambos modos

> estén disponibles, es obligatorio compartir los datos de telemetría y, si no lo hace, el soporte y el mantenimiento se suspenderán después de 90 días.

Hardware de capacidad cero

Cuando se administran mediante las licencias Flexed de NetScaler, las instancias MPX y SDX se denominan «hardware de capacidad cero» porque no pueden funcionar hasta que extraigan los recursos del grupo de ancho de banda. Por lo tanto, estas plataformas también se conocen como dispositivos MPX-Z y SDX-Z.

El hardware de capacidad cero requiere una licencia Z-cap para comprobar el ancho de banda del grupo común.

> **Nota:**
>
> - La instalación de licencias de capacidad cero funciona de la misma manera que otras licencias locales de NetScaler. Para obtener más información sobre cómo obtener e instalar una licencia de capacidad cero, consulte la guía de licencias de NetScaler.

Gestione e instale las licencias de Z-cap

Debe instalar una licencia Z-cap manualmente, utilizando el número de serie del hardware o el código de acceso a la licencia. Una vez instalada la licencia Z-cap, se bloquea en el hardware y no se puede compartir entre instancias de hardware de NetScaler a petición. Sin embargo, puede mover manualmente la licencia Z-cap a otra instancia de hardware de NetScaler.

Las instancias MPX de NetScaler que ejecutan la versión 11.1, compilación 54.14 o posterior del software NetScaler, y las instancias SDX de NetScaler que ejecutan la versión 11.1, compilación 58.13 o posterior, admiten las licencias NetScaler Flexed. Para obtener más información, consulte **la Tabla 1. Licencias Flexed compatibles para instancias**MPX y SDX.

Instancias independientes de NetScaler VPX

Las instancias de NetScaler VPX que ejecutan la versión 11.1 Build 54.14 del software NetScaler y versiones posteriores de los siguientes hipervisores admiten las licencias Flexed:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Las instancias de NetScaler VPX que ejecutan la versión 12.0 Build 51.24 del software NetScaler y versiones posteriores en los siguientes hipervisores y plataformas de nube admiten las licencias Flexed:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Las instancias de NetScaler VPX que ejecutan las versiones 13.0 y 13.1 del software NetScaler (todas las versiones) en los siguientes hipervisores y plataformas en la nube admiten las licencias Flexed:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **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 NetScaler VPX implementadas en la nube a NetScaler ADM. A diferencia del hardware de capacidad cero, NetScaler VPX no requiere una licencia de capacidad cero. Para procesar el tráfico, debe desproteger el ancho de banda y una licencia de instancia del grupo.

Instancias CPX independientes de NetScaler

Las instancias CPX de NetScaler implementadas en un host Docker admiten las licencias Flexed. A diferencia del hardware de capacidad cero, NetScaler CPX no requiere una licencia Z-cap. Una sola instancia de NetScaler CPX que consume hasta 1 Gbps de rendimiento extrae solo 1 instancia y no tiene ancho de banda del grupo de licencias. Por ejemplo, considere que tiene 20 instancias de NetScaler CPX con un grupo de ancho de banda de 20 Gbps. Si una de las instancias de NetScaler CPX consume un rendimiento de 500 Mbps, el grupo de ancho de banda sigue siendo de 20 Gbps para las 19 instancias de NetScaler CPX restantes.

Si la misma instancia de NetScaler CPX comienza a consumir 1500 Mbps de rendimiento, el grupo de ancho de banda tendrá 19,5 Gbps para las 19 instancias de NetScaler CPX restantes.

En el caso de las licencias Flexed, solo puede añadir más ancho de banda en múltiplos de 10 Mbps.

Instancias independientes de NetScaler BLX

Las instancias BLX de NetScaler admiten las licencias Flexed. Una instancia de NetScaler BLX no requiere una licencia Z-cap. Para procesar el tráfico, una instancia de NetScaler BLX debe desproteger el ancho de banda y 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, tanto físicas como virtuales. El grupo de ancho de banda comprende un grupo para la edición de software Premium. Si cambia de licencias agrupadas a licencias flexibles, es posible que encuentre una combinación de ediciones de software Standard, Advanced y Premium. Una instancia determinada de NetScaler MPX/VPX/CPX/BLX no puede tener ancho de banda de diferentes grupos comprobados 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

Hay tres tipos de grupos de instancias de software:

- Instancia de software VPX/CPX/BLX
- Instancia de software MPX (se aplica el mismo grupo para MPX FIPS)
- Instancia de software SDX (se aplica el mismo grupo para SDX FIPS)
- Instancia de software VPX FIPS

Cuando se retira del grupo, una licencia desbloquea los recursos de la instancia de software, incluidas las CPU/PE, los núcleos SSL, los paquetes por segundo y el ancho de banda.

Servidor de licencias NetScaler ADM

Las licencias Flexed de NetScaler utilizan NetScaler ADM configurado como servidor de licencias para administrar las licencias Flexed: licencias de grupos de ancho de banda y licencias de grupos de instancias.

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 en un hardware de capacidad cero determina

- El ancho de banda mínimo y la cantidad de instancias que una instancia de NetScaler debe desproteger antes de funcionar.

- El ancho de banda máximo y el número de instancias que puede desproteger un dispositivo NetScaler.
- 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 NetScaler debe desproteger 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 es de 1 Gbps, se pueden comprobar 1000 Mbps, 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 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.

Las tablas 1, 2, 3 y 4 resumen el ancho de banda máximo/instancias, el ancho de banda mínimo y la unidad mínima de ancho de banda para todas las instancias NetScaler admitidas. En la tabla 5 se resumen los requisitos de licencia para los diferentes formatos de todas las instancias de NetScaler compatibles. Las tablas siguientes hacen referencia a los requisitos del sistema.

> **Nota:**
>
> La unidad de comprobación de ancho de banda mínimo para NetScaler CPX/BLX/VPX es de 10 Mbps. El ancho de banda mínimo de la unidad de pago para NetScaler MPX/SDX es de 1 Gbps.

Tabla 1A. Capacidad flexible compatible para MPX

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Unidad mínima de ancho de banda
MPX 5900Z	1	10	1 Gbps
MPX 8900Z	5	30	1 Gbps
MPX 8900Z FIPS	5	20	1 Gbps
MPX 9100Z	10	95	1 Gbps
MPX 9100Z FIPS	10	95	1 Gbps
MPX 14000Z	20	100	1 Gbps
MPX 14000Z-40G	20	100	1 Gbps
MPX 14000Z-40S	40	100	1 Gbps
MPX 14000Z FIPS	30	80	1 Gbps
MPX 15000Z	20	120	1 Gbps

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Unidad mínima de ancho de banda
MPX 15000Z-50G	20	120	1 Gbps
MPX 15000Z FIPS	30	120	1 Gbps
MPX 16000Z	30	250	1 Gbps
MPX 22000Z	40	120	1 Gbps
MPX 2400Z	100	150	1 Gbps
MPX 25000Z	100	160	1 Gbps
MPX 25000Z-40G	100	200	1 Gbps
MPX 2600Z	100	200	1 Gbps
MPX 26000Z-50S	100	200	1 Gbps
MPX 26000Z-100G	100	200	1 Gbps

Tabla 1A. Capacidad flexible compatible para la versión de NetScaler SDX anterior a la compilación 13.0-47.x

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 8900Z	10	30	2	7	1 Gbps
SDX 1400 Z	20	100	5	25	1 Gbps
SDX 14000Z-40G	40	100	20	25	1 Gbps
SDX 15000Z	20	120	5	55	1 Gbps
SDX 15000Z-50G	20	120	5	55	1 Gbps
SDX 2000Z	40	120	80	80	1 Gbps
SDX 2400 Z	100	150	80	80	1 Gbps
SDX 2500 Z	100	200	20	115	1 Gbps
SDX 25000Z-40G	100	200	20	115	1 Gbps

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 26000Z	100	200	20	115	1 Gbps
SDX 2600Z-50S	100	200	20	115	1 Gbps
SDX 2600Z-100G	100	200	20	115	1 Gbps

Tabla 1B. Capacidad flexible compatible con NetScaler SDX versión 13 (compilación 13.0-47.x y posteriores), versión 13.1 (compilación anterior a 51.x) y versión 14.1 (compilación anterior a 12.x) de NetScaler SDX

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	2	7	1 Gbps
SDX 1400 Z	10	100	2	25	1 Gbps
SDX 14000Z-40G	20	100	10	25	1 Gbps
SDX 15000Z	10	120	2	55	1 Gbps
SDX 15000Z-50G	10	120	2	55	1 Gbps
SDX 1600Z	15	250	10	55	1 Gbps
SDX 2000Z	20	120	40	80	1 Gbps
SDX 2400 Z	50	150	40	80	1 Gbps
SDX 2500 Z	50	200	10	115	1 Gbps
SDX 25000Z-40G	50	200	10	115	1 Gbps
SDX 26000Z	50	200	10	115	1 Gbps

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 2600Z-50S	50	200	10	115	1 Gbps
SDX 2600Z-100G	50	200	10	115	1 Gbps

Tabla 1C. Capacidad flexible compatible para NetScaler SDX versión 13.1 (compilación 51.x y posteriores) y versión 14.1 (compilación 12.x y posteriores) de NetScaler SDX

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	1	7	1 Gbps
SDX 1400 Z	10	100	1	25	1 Gbps
SDX 14000Z-40G	20	100	1	25	1 Gbps
SDX 15000Z	10	120	1	55	1 Gbps
SDX 15000Z-50G	10	120	1	55	1 Gbps
SDX 1600Z	15	250	1	55	1 Gbps
SDX 2000Z	20	120	1	80	1 Gbps
SDX 2400 Z	50	150	1	80	1 Gbps
SDX 2500 Z	50	200	1	115	1 Gbps
SDX 25000Z-40G	50	200	1	115	1 Gbps
SDX 26000Z	50	200	1	115	1 Gbps
SDX 2600Z-50S	50	200	1	115	1 Gbps

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 2600Z-100G	50	200	1	115	1 Gbps

> **Notas:**
>
> - La cantidad mínima de compra puede diferir del requisito mínimo del sistema.
> - En NetScaler SDX con la compilación 14.1-12.x y versiones posteriores, con una licencia Flexed, se elimina la restricción de retirar un número mínimo de licencias de instancia. Es decir, puede obtener como mínimo una licencia de instancia.

Tabla 2. Ancho de banda mínimo/máximo e instancias mínimo/máximo admitidas para las instancias CPX de NetScaler

Línea de productos	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Mbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
CPX	10	10	1	1	10 Mbps

Tabla 3. Ancho de banda mínimo/máximo e instancias mínimo/máximo admitidas para instancias de NetScaler 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

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
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

> Nota
>
> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

Tabla 4. Ancho de banda mínimo/máximo e instancias mínimo/máximo admitidas para las instancias de NetScaler BLX

Línea de productos	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Mbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
BLX	100	10	1	1	10 Mbps

Tabla 5. Requisito de licencia de capacidad cero para diferentes formatos

Línea de productos	Hardware de capacidad cero
MPX	Se requiere licencia
SDX	Se requiere licencia
VPX	-
CPX	-
BLX	-

Configurar las licencias Flexed

January 30, 2024

> **Nota:**
>
> Si ha agrupado licencias y ya ha comprado y aplicado licencias Flexed, el derecho combinado aparece en el panel de licencias Flexed.

Las licencias Flexed de NetScaler le permiten compartir licencias de instancia o ancho de banda en diferentes formatos de NetScaler. Utilice esta capacidad flexible 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 NetScaler que necesiten recursos.

Puede usar las licencias Flexed 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.

Puede realizar las siguientes tareas en NetScaler ADM:

1. Cargue los archivos de licencia Flexed (grupo de ancho de banda o grupo de instancias de software) al servidor de licencias.

   > **Nota:**
   >
   > El servidor de licencias es el servidor local NetScaler ADM.

2. Cargue las licencias SDX o MPX de capacidad cero en el hardware SDX o MPX y asigne licencias del grupo de licencias a las instancias de NetScaler a pedido.

   - Consulte las licencias de las instancias de NetScaler en función de la capacidad mínima y máxima de la instancia.

Puede descargar las licencias Flexed, incluidas las licencias de ancho de banda, de instancia y Z-cap, desde citrix.com. Para obtener más información, consulte la Guía de licencias de NetScaler.

Estados de licenciamiento de NetScaler Flexed

Los estados de licencia Flexed indican el requisito de licencia en una instancia de NetScaler. Las instancias de NetScaler configuradas con licencias Flexed muestran uno de los siguientes estados:

- **Asignado**: la instancia se está ejecutando con la capacidad de licencia adecuada.
- **Grace**: La instancia se ejecuta en una licencia de gracia.
- **Conexión perdida**: la comunicación de NetScaler ADM con la instancia no funciona.

Antes de comenzar

Asegúrese de que se cumplen los siguientes requisitos previos antes de configurar las licencias Flexed:

- Se puede acceder a los puertos `27000` y `7279` desde NetScaler a NetScaler ADM para comprobar las licencias. Consulte Requisitos del sistema.

Paso 1: Aplicar licencias en NetScaler ADM

1. Vaya a **NetScaler Licensing > License Management** .
2. En la sección **Archivos de licencia**, seleccione **Agregar archivo de licencia** y seleccione una de las siguientes opciones:
   - **Cargue los archivos de licencia desde un equipo local**. Si ya hay un archivo de licencia en su equipo local, puede subirlo a NetScaler ADM.
   - **Utilice el código de acceso de licencia**. Especifique el código de acceso a la licencia de la licencia que ha adquirido en Citrix. A continuación, seleccione **Obtener licencias**. A continuación, selecciona **Finalizar**.

   > **Nota:**
   >
   > En cualquier momento, puede agregar más licencias a NetScaler ADM desde **Parámetros de licencias.**

3. Haga clic en **Finalizar**.

   Los archivos de licencia se agregan a NetScaler ADM. En la sección **Información de caducidad** de licencias se enumeran las licencias presentes en NetScaler ADM y los días que faltan para que caduquen.
4. En **Archivos de licencia**, seleccione el archivo de licencia que quiera aplicar y haga clic en **Aplicar licencias**.

   Esta acción permite a las instancias de NetScaler utilizar la licencia seleccionada como licencia flexible.

Paso 2: Registrar NetScaler ADM como servidor de licencias y asignar licencias

Puede registrar NetScaler ADM como servidor de licencias en una instancia de NetScaler.

Registrar un servidor NetScaler ADM mediante la GUI

En la GUI de NetScaler ADM, registre el servidor NetScaler ADM asociado a una instancia de NetScaler.

1. Inicie sesión en la GUI de NetScaler.
2. Vaya a **Sistema > Licencias > Administrar licencias** .
3. Haga clic en **Agregar licencia nueva**.
4. Seleccione **Usar licencias remotas** y seleccione el modo de licencia remota de la lista.
5. En el campo **Nombre del servidor/dirección IP**, especifique la dirección IP del servidor NetScaler ADM asociado que está registrada en el NetScaler ADM.
6. Seleccione **Registrar con NetScaler ADM**.
7. Introduzca las credenciales del servidor NetScaler ADM para registrar una instancia en NetScaler ADM y haga clic en **Continuar**. En NetScaler ADM, uno de los servidores es el servidor de licencias.
8. En **Asignar licencias**, seleccione la edición de la licencia y especifique el ancho de banda requerido.

   Por primera vez, asigne licencias en NetScaler. Más adelante, puede cambiar o liberar la asignación de licencias desde la GUI de NetScaler ADM.
9. Haga clic en **Obtener licencias**.

   > **Importante**
   >
   > Reinicie la instancia en caliente si cambia la edición de la licencia. Los cambios de configuración no surtirán efecto hasta que reinicie la instancia.

Agregar un servidor NetScaler ADM mediante la CLI

Si una instancia de NetScaler no tiene ninguna GUI, utilice los siguientes comandos de la CLI para agregar un servidor NetScaler ADM asociado a una instancia:

1. Inicie sesión en la consola de NetScaler.
2. Agregue la dirección IP del servidor NetScaler ADM asociado que está registrada en NetScaler ADM. El puerto de licencia predeterminado es 27000.

```
1 > add ns licenseserver <adm-server-IP-address> -port <adm-server-
     license-port-number>
2 <!--NeedCopy-->
```

3. Ver el ancho de banda de licencia disponible en el servidor de licencias:


```
> sh ns licenseserverpool
<!--NeedCopy-->
```

4. Asigne el ancho de banda de licencia desde la edición de licencia requerida:

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
<!--NeedCopy-->
```

> **Importante**
>
> Warm reinicie la instancia si cambia la edición de la licencia.
>
> `reboot -w`
>
> Los cambios de configuración no surtirán efecto hasta que reinicie la instancia.

Paso 3: Editar el ancho de banda flexible para las instancias de NetScaler

1. Vaya a **NetScaler Licensing > Flexed Licensing > Dashboard** .
2. En la sección **NetScalers con licencia** , seleccione una instancia y haga clic en **Editar ancho** de banda.
3. En la página **Editar ancho** de banda, introduzca un número en la columna **Asignar** .
4. Haga clic en **Submit**.

NetScaler MPX-Z

MPX-Z es el dispositivo NetScaler MPX con capacidad flexible. El MPX-Z admite la agrupación de ancho de banda solo para las licencias de la edición Premium.

El MPX-Z necesita una licencia para poder conectarse al servidor de licencias. Puede instalar la licencia MPX-Z de una de las siguientes maneras:

- Carga del archivo de licencia desde un equipo local.
- Usar el número de serie del hardware de la instancia.
- El código de acceso a licencias de la sección **Sistema** > **Licencias** de la GUI de la instancia.

Si quita la licencia MPX-Z, MPX deja de tener licencia. Las licencias se liberan 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 Flexed necesarias para la capacidad configurada.

NetScaler SDX-Z

SDX-Z es el dispositivo NetScaler SDX con capacidad flexible. SDX-Z admite ancho de banda y grupo de instancias para las licencias de la edición Premium.

SDX-Z requiere una licencia para poder conectarse al servidor de licencias. Puede instalar la licencia SDX-Z de una de las siguientes maneras:

- Carga del archivo de licencia desde un equipo local.
- Usar el número de serie del hardware de la instancia.
- El código de acceso a licencias de la sección **Sistema** > **Licencias** de la GUI de la instancia.

Si eliminas la licencia SDX-Z, SDX deja de tener licencia. Las licencias se liberan en el servidor de licencias.

Puede modificar dinámicamente el ancho de banda de una instancia SDX-Z sin necesidad de reiniciar.

> **Nota:**
>
> Cuando reinicias la instancia, comprueba automáticamente las licencias Flexed necesarias para la capacidad configurada.

Par de alta disponibilidad NetScaler

Antes de empezar, asegúrese de que el servidor NetScaler ADM esté configurado como servidor de licencias. Para obtener más información, consulte Configurar NetScaler ADM como servidor de licencias.

Al asignar el ancho de banda a un par de NetScaler HA, el ADM de NetScaler comprueba el ancho de banda asignado a la instancia principal. Debe repetir el proceso para la instancia secundaria.

Para asignar licencias de grupo a un par de NetScaler HA, consulte Asignar licencias flexibles a instancias de NetScaler

La página **Flexed Capacity** muestra las instancias y su capacidad asignada por separado.

Panel de licencias flexible

January 30, 2024

El panel de licencias Flexed le ofrece una visión completa de la capacidad de ancho de banda y las instancias que ha adquirido.

En esta página se muestran la capacidad de ancho de banda en todas las ediciones y los detalles de las instancias para diferentes formatos, como MPX, VPX y SDX. NetScaler MPX y NetScaler MPX FIPS tienen el mismo archivo de licencia. Del mismo modo, NetScaler SDX y NetScaler SDX FIPS tienen el mismo archivo de licencia. Sin embargo, NetScaler VPX FIPS tiene un archivo diferente al de NetScaler VPX y se muestra por separado. Además, NetScaler BLX y NetScaler CPX requieren licencias de NetScaler VPX y forman parte de los derechos y la asignación de VPX. Una licencia Flexed solo admite la edición premium. Sin embargo, si ha adquirido licencias Flexed y anteriormente tenía capacidad de ancho de banda estándar o avanzada agrupada, los detalles relacionados con la capacidad de ancho de banda (estándar o avanzada) también aparecen en el panel de licencias Flexed.

Los detalles sobre las instancias de NetScaler con licencia están disponibles en la sección de **NetScalers con licencia**. Puedes seleccionar una instancia y editar el ancho de banda o liberar la licencia en esa instancia.

Puede filtrar los resultados en función de los siguientes parámetros:

- Filtrar por ancho de banda
  - Premium
  - Avanzado
  - Estándar
- Factor de forma
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- Estado de la licencia
  - Conexión perdida
  - ¡Grace
  - Asignado

Editar el ancho de banda asignado en una instancia de NetScaler

1. Vaya a **NetScaler Licensing > Flexed Licensing > Dashboard** .

2. En la sección **NetScalers con licencia** , seleccione una instancia y haga clic en **Editar ancho** de banda.
3. En la página **Editar ancho** de banda, introduzca un número en la columna **Asignar** .
4. Haga clic en **Submit**.

Libere licencias en una instancia de NetScaler

Para transferir licencias a otra instancia, debe liberar la licencia en la instancia actual y, a continuación, aplicar la licencia a la nueva instancia. Al seleccionar **Release License** , se hace lo siguiente:

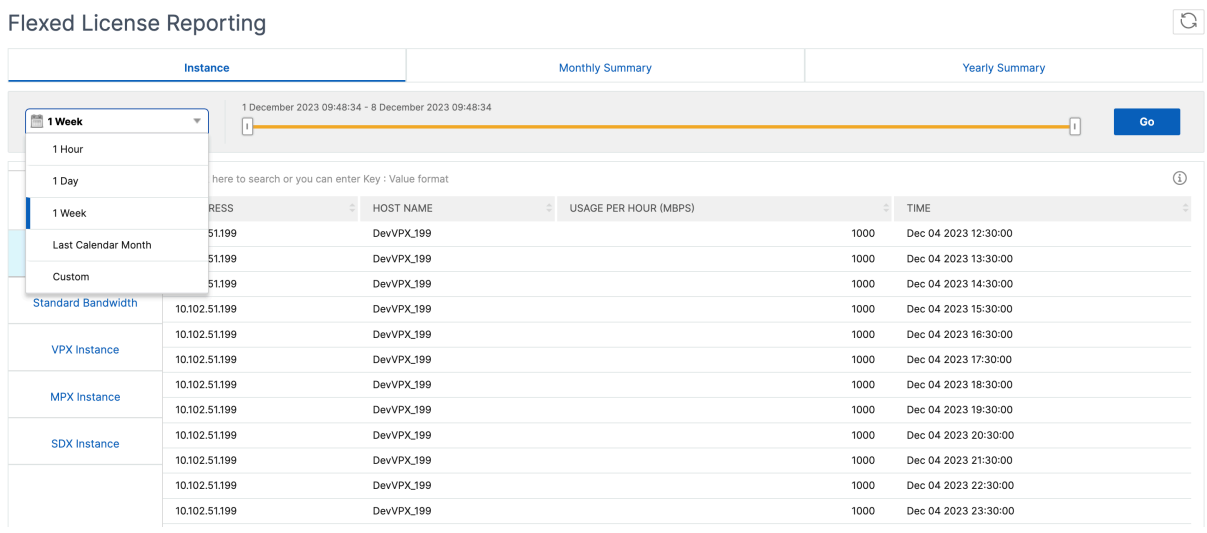
- Libera todas las licencias retiradas en esa instancia en el servidor de licencias.
- Elimina la configuración del servidor de licencias de esa instancia.

Si selecciona **Sí**, la instancia de NetScaler deja de tener licencia y no puede procesar ningún tráfico.

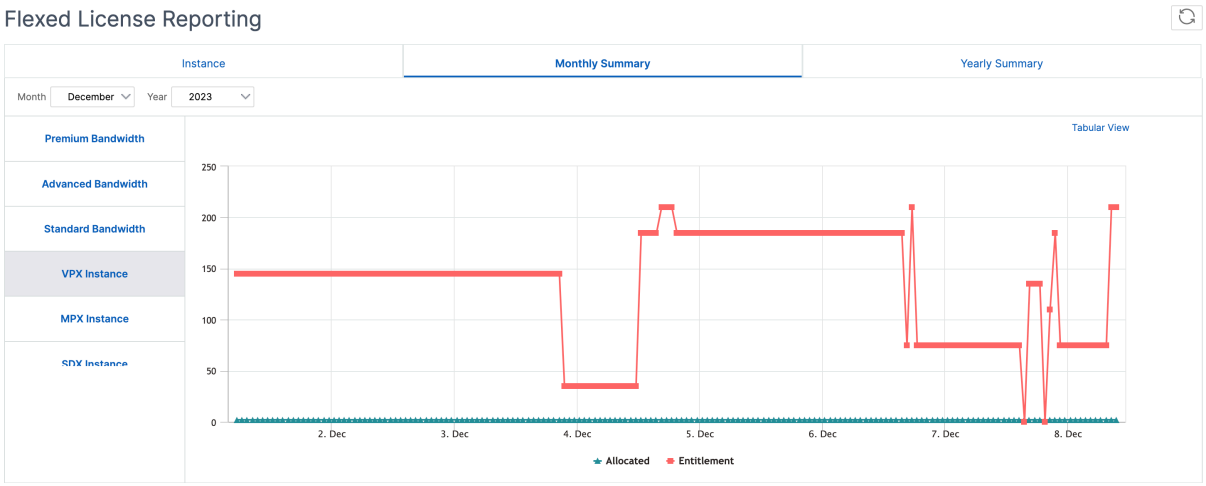
Informes de licencias flexibles

January 30, 2024

Puede ver los detalles sobre la asignación y los derechos de su instancia de software y licencias de ancho de banda para saber cuánto se asigna de la autorización. Puedes ver los detalles de la instancia, como qué instancia consume cuánto ancho de banda (uso por hora) y el momento en que lo hace. Puede especificar el período de tiempo desde una hora hasta un período de tiempo personalizado.



Las vistas gráficas están disponibles en las pestañas **Resumenmensual y Resumen** anual . Los gráficos siguientes son algunos ejemplos de asignación y asignación de instancias de software.



Capacidad agrupada de NetScaler

January 30, 2024

La capacidad agrupada de NetScaler le permite compartir ancho de banda o licencias de instancia en diferentes formatos de NetScaler. Para las instancias basadas en suscripción de CPU virtual, puede compartir la licencia de CPU virtual en todas las instancias. Utilice 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 para otras instancias de NetScaler 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 del 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 agrupada, puede automatizar el aprovisionamiento de instancias.

Cómo funcionan las licencias de capacidad agrupadas de NetScaler

La capacidad agrupada de NetScaler tiene los siguientes componentes:

- Instancias de NetScaler, que se pueden clasificar en:
  - Hardware de capacidad cero
  - Instancias de NetScaler VPX independientes o instancias de NetScaler CPX o instancias de NetScaler BLX
- Grupo de ancho de banda

- Grupo de instancias
- NetScaler ADM configurado como servidor de licencias

Hardware de capacidad cero

Cuando se administran mediante la capacidad agrupada de NetScaler, las instancias MPX y SDX se denominan «hardware de capacidad cero» porque estas instancias no pueden funcionar hasta que eliminen los recursos del ancho de banda y los grupos de instancias. Por lo tanto, estas plataformas también se conocen como 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.

> **Nota**
>
> - La suscripción de licencia de instancia no es necesaria para las instancias MPX. Consulte la tabla 1 de esta página para ver la capacidad agrupada compatible para las instancias MPX y SDX. Consulte la tabla 5 para ver los requisitos de licencia para los diferentes formatos MPX y SDX.
> - La instalación de licencias de capacidad cero funciona de la misma manera que otras licencias locales de NetScaler. Para obtener más información sobre cómo obtener e instalar una licencia de capacidad cero, consulte la guía de licencias de NetScaler.

Administrar e instalar 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 a pedido. Sin embargo, puede mover manualmente la licencia de plataforma a otra instancia de hardware de NetScaler.

Las instancias MPX de NetScaler que ejecutan la versión 11.1, compilación 54.14 o posterior del software NetScaler, y las instancias SDX de NetScaler que ejecutan la versión 11.1, compilación 58.13 o posterior, admiten la capacidad agrupada de NetScaler. Para obtener más información, consulte **la Tabla 1. Capacidad agrupada compatible para instancias**MPX y SDX.

Instancias independientes de NetScaler VPX

Las instancias de NetScaler VPX que ejecutan la versión 11.1, compilación 54.14 del software NetScaler y versiones posteriores de los siguientes hipervisores admiten la capacidad agrupada:

- VMware ESX 6.0

- Citrix Hypervisor
- Linux KVM

Las instancias de NetScaler VPX que ejecutan la versión 12.0 Build 51.24 del software NetScaler y versiones posteriores en los siguientes hipervisores y plataformas de nube admiten la capacidad agrupada:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

Las instancias de NetScaler VPX que ejecutan las versiones 13.0 y 13.1 del software NetScaler (todas las versiones) en los siguientes hipervisores y plataformas de nube admiten la capacidad agrupada:

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **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 NetScaler VPX implementadas en la nube a NetScaler ADM.
> A diferencia del hardware de capacidad cero, NetScaler VPX no requiere una 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

Las instancias CPX de NetScaler implementadas en un host Docker admiten la capacidad agrupada. A diferencia del hardware de capacidad cero, NetScaler CPX no requiere una licencia de plataforma. Una sola instancia de NetScaler CPX que consume hasta 1 Gbps de rendimiento extrae solo 1 instancia y no tiene ancho de banda del grupo de licencias. Por ejemplo, considere que tiene 20 instancias de NetScaler CPX con un grupo de ancho de banda de 20 Gbps. Si una de las instancias de NetScaler CPX

consume un rendimiento de 500 Mbps, el grupo de ancho de banda sigue siendo de 20 Gbps para las 19 instancias de NetScaler CPX restantes.

Si la misma instancia de NetScaler CPX comienza a consumir 1500 Mbps de rendimiento, el grupo de ancho de banda tendrá 19,5 Gbps para las 19 instancias de NetScaler CPX restantes.

Para licencias de grupo, puede agregar más ancho de banda solo en múltiplos de 10 Mbps.

Instancias independientes de NetScaler BLX

Las instancias BLX de NetScaler admiten licencias de capacidad agrupada. Una instancia de NetScaler BLX no requiere una licencia de plataforma. Para procesar el tráfico, una instancia de NetScaler BLX debe desproteger el ancho de banda y 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, tanto físicas como virtuales. El conjunto de ancho de banda comprende grupos separados para cada edición de software (Standard, Advanced y Premium). Una instancia determinada de NetScaler 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 de NetScaler VPX o instancias de NetScaler CPX o instancias de NetScaler BLX que se pueden administrar mediante la capacidad agrupada de NetScaler o el número de instancias de NetScaler VPX en una instancia SDX-Z.

Cuando se retira del grupo, una licencia desbloquea los recursos de la instancia MPX-Z, SDX-Z, VPX, NetScaler CPX y NetScaler BLX, incluidos CPU/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 NetScaler utiliza el ADM de NetScaler configurado como servidor de licencias para administrar las licencias de capacidad agrupada: licencias de grupos de ancho de banda y

licencias de grupos de instancias. Puede usar el software NetScaler ADM para administrar las licencias de capacidad agrupada sin una licencia NetScaler 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 en un hardware de capacidad cero determina

- El ancho de banda mínimo y la cantidad de instancias que una instancia de NetScaler debe desproteger antes de funcionar.
- El ancho de banda máximo y el número de instancias que puede desproteger un dispositivo NetScaler.
- 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 NetScaler debe desproteger 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 es de 1 Gbps, se pueden comprobar 1000 Mbps, 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 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.

Las tablas 1, 2, 3 y 4 resumen el ancho de banda máximo/instancias, el ancho de banda mínimo y la unidad mínima de ancho de banda para todas las instancias NetScaler admitidas. En la tabla 5 se resumen los requisitos de licencia para diferentes factores de forma para todas las instancias de NetScaler compatibles:

Tabla 1. Capacidad agrupada compatible 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 8900Z	30	5	NA	NA	1 Gbps
MPX 9100Z	30	10	NA	NA	1 Gbps
MPX 8900Z FIPS	33	5	NA	NA	1 Gbps
Serie MPX 14000Z	100	20	NA	NA	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 MPX 14000Z 40G	100	20	N/D	N/D	1 Gbps
MPX 14000Z serie FIPS	100	20	N/D	N/D	1 Gbps
Serie MPX 14000Z 40S	100	20	N/D	N/D	1 Gbps
Serie MPX 15000Z	120	20	N/D	N/D	1 Gbps
MPX 15000Z serie FIPS	120	20	N/D	N/D	1 Gbps
Serie 50G de MPX 15000Z	120	20	N/D	N/D	1 Gbps
Serie MPX 16000Z	200	30	N/D	N/D	1 Gbps
Serie MPX 22000Z	120	40	N/D	N/D	1 Gbps
Serie MPX 24000Z	150	100	N/D	N/D	1 Gbps
MPX 25000Z 40G	200	100	N/D	N/D	1 Gbps
MPX 25000ZA	200	100	N/D	N/D	1 Gbps
Serie MPX 26000Z	200	100	N/D	N/D	1 Gbps
Serie MPX 26000Z 100G	200	100	N/D	N/D	1 Gbps
Serie MPX 26000Z 50S	200	100	N/D	N/D	1 Gbps
SDX 8900Z	30	10	1	7	1 Gbps
SDX 9100Z	95	20	1	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 14000Z	100	10	1	25	1 Gbps
Serie SDX 14000Z 40G	100	1	2	25	1 Gbps
Serie SDX 14000Z 40S	100	20	1	25	1 Gbps
Serie SDX 14000Z FIPS	100	10	1	25	1 Gbps
SDX 15000Z 50G	120	10	1	55	1 Gbps
SDX 15000Z	120	10	1	55	1 Gbps
Serie SDX 16000Z	200	15	1	55	1 Gbps
Serie SDX 22000Z	120	20	1	80	1 Gbps
SDX 25000Z 40G	200	50	1	115	1 Gbps
SDX 25000ZA	200	50	1	115	1 Gbps
SDX 26000Z 100 G	200	50	1	115	1 Gbps
SDX 26000Z	200	50	1	115	1 Gbps
SDX 26000Z 50	200	50	1	115	1 Gbps
Serie SDX 24000Z	150	50	1	80	1 Gbps

> Nota
>
> El ancho de banda mínimo y las instancias se aplican a las instancias SDX que ejecutan las siguientes versiones y versiones superiores: 11.1 64.x, 12.0 63.x, 12.1 54.x y 13.0 41.x.

> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

Tabla 2. Capacidad agrupada compatible para instancias CPX de NetScaler

Línea de productos	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Mbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
CPX	10	10	1	1	10 Mbps

Tabla 3. Capacidad agrupada compatible para instancias de NetScaler 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	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

> Nota
>
> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

Tabla 4. Capacidad agrupada compatible para instancias BLX de NetScaler

Línea de productos	Ancho de banda máximo (Gbps)	Ancho de banda mínimo (Mbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
BLX	100	10	1	1	10 Mbps

Tabla 5. Requisito de licencia para diferentes factores de forma

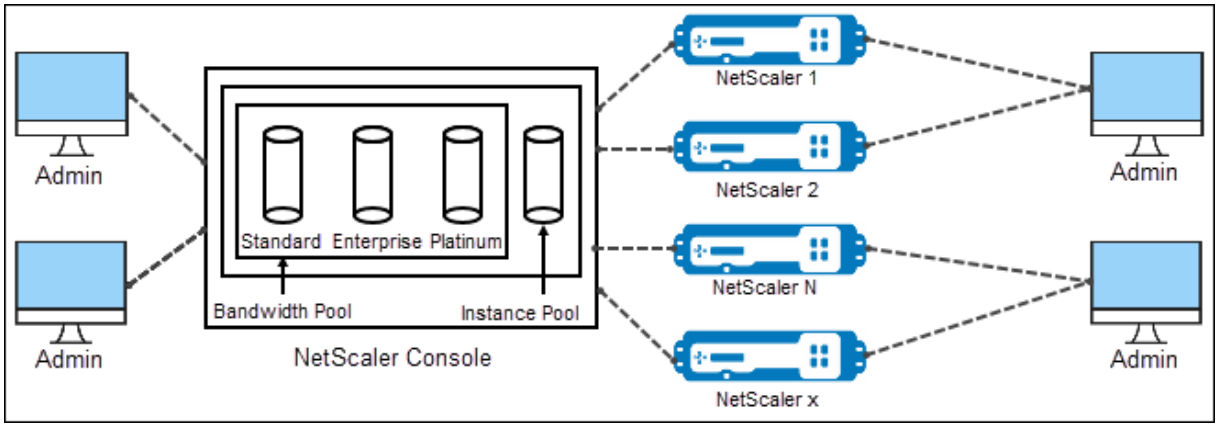
Línea de productos	Compra de hardware de capacidad cero	Suscripción a ancho de banda y edición	Suscripción de instancias
MPX	Se requiere licencia	Se requiere licencia	-
SDX	Se requiere licencia	Se requiere licencia	Se requiere licencia
VPX	-	Se requiere licencia	Se requiere licencia
CPX	-	-	Se requiere licencia
BLX	-	Se requiere licencia	Se requiere licencia

Configurar la capacidad agrupada de NetScaler

January 30, 2024

Para usar la capacidad agrupada de NetScaler, configure NetScaler ADM como un servidor de licencias para las instancias de NetScaler necesarias. Las instancias de NetScaler registran y retiran licencias del NetScaler ADM. Puede realizar las siguientes tareas en la GUI de administración y entrega de aplicaciones de NetScaler:

- Cargue los archivos de licencia de capacidad agrupada (ancho de banda y grupo de instancias) al servidor de licencias.
- Asigne licencias del grupo de licencias a instancias de NetScaler bajo demanda.
- Consulte las licencias de las instancias de NetScaler (MPX-Z /SDX-Z/VPX/CPX/BLX) en función de la capacidad mínima y máxima de la instancia.
- Configure la capacidad agrupada de las instancias FIPS de NetScaler para registrar o retirar licencias.



Versiones de hardware y software compatibles

Para ver las versiones de hardware y software compatibles con la capacidad agrupada, consulte Capacidad agrupada de NetScaler.

Estados de capacidad agrupada de NetScaler

Los estados de capacidad agrupada indican el requisito de licencia en una instancia de NetScaler. Las instancias de NetScaler configuradas con capacidad agrupada muestran uno de los siguientes estados:

- **Óptimo**: la instancia se ejecuta con la capacidad de licencia adecuada.
- **Discrepancia de capacidad**: la instancia se ejecuta con una capacidad inferior a la configurada por el usuario.
- **Grace**: La instancia se ejecuta en una licencia de gracia.
- **Grace & Mismatch**: La instancia se ejecuta en gracia pero con una capacidad inferior a la configurada por el usuario.
- **No disponible**: la instancia no está registrada en NetScaler ADM para su administración o la comunicación NITRO desde NetScaler ADM a las instancias no funciona.
- **No asignada**: la licencia no está asignada en la instancia.

Paso 1: Aplicar licencias en NetScaler ADM

1. En NetScaler ADM, vaya a **NetScaler Licensing > Pooled Licensing** .
2. En la sección **Archivos de licencia**, seleccione **Agregar archivo de licencia** y seleccione una de las siguientes opciones:

- **Cargue los archivos de licencia desde un equipo local**. Si ya hay un archivo de licencia en su equipo local, puede subirlo a NetScaler ADM.
- **Utilice el código de acceso de licencia**. Especifique el código de acceso a la licencia de la licencia que ha adquirido en Citrix. A continuación, seleccione **Obtener licencias**. A continuación, selecciona **Finalizar**.

> **Nota:**
>
> En cualquier momento, puede agregar más licencias a NetScaler ADM desde la **configuración de licencias**.

3. Haga clic en **Finalizar**.

   Los archivos de licencia se agregan a NetScaler ADM. La pestaña **Información de caducidad** de la licencia muestra las licencias presentes en NetScaler ADM y los días que faltan para que caduquen.

4. En **Archivos de licencia**, seleccione el archivo de licencia que quiera aplicar y haga clic en **Aplicar licencias**.

   Esta acción permite a las instancias de NetScaler utilizar la licencia seleccionada como capacidad agrupada.

Para obtener más información sobre cómo aplicar las licencias agrupadas a la administración y entrega de aplicaciones de NetScaler, consulte el vídeo relacionado:

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Paso 2: Registrar NetScaler ADM como servidor de licencias

Para registrar NetScaler ADM como servidor de licencias en una instancia de NetScaler, siga uno de los procedimientos siguientes:

- Usar GUI
- Usar CLI

Utilice la GUI para registrar NetScaler ADM como servidor de licencias

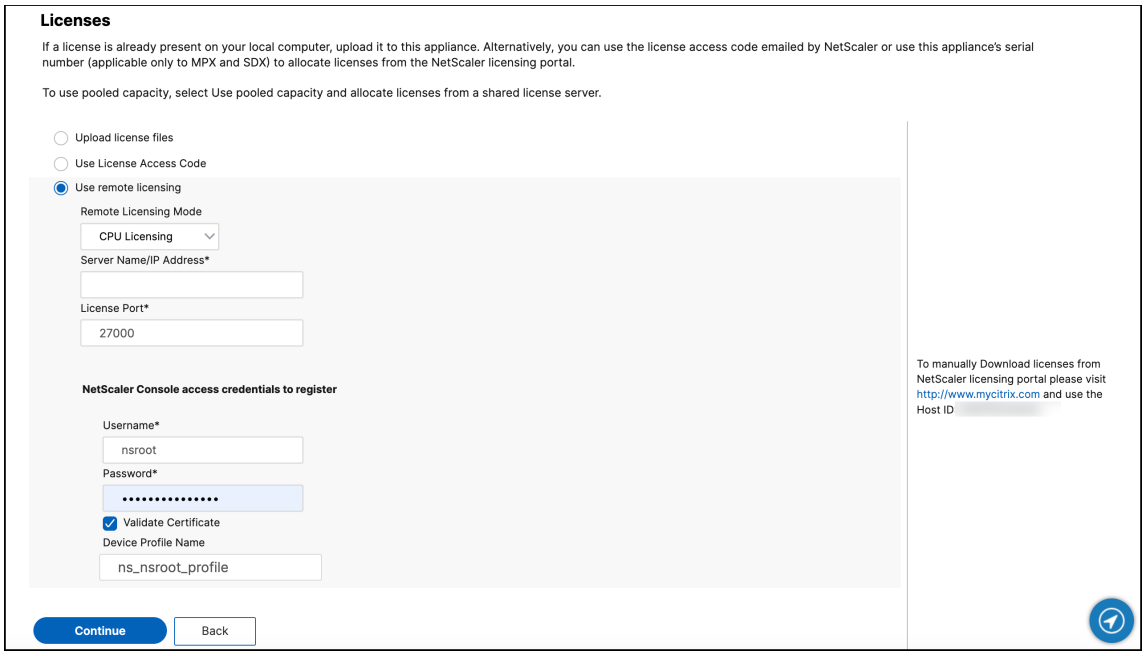
En la GUI de NetScaler, registre el servidor NetScaler ADM como servidor de licencias.

1. Inicie sesión en la GUI de NetScaler.
2. Vaya a **Sistema** > **Licencias** > **Administrar licencias** .
3. Haga clic en **Agregar licencia nueva**.

4. Seleccione **Usar licencias remotas** y seleccione el modo de licencia remota de la lista.
5. En el campo **Nombre del servidor/dirección IP**, especifique la dirección IP del servidor NetScaler ADM.

   > Para una implementación de HA, utilice una IP flotante. Para obtener más información sobre la configuración, consulte Configurar la implementación de alta disponibilidad.
   >
   > Para una implementación que utilice un NetScaler ADM independiente o un agente, consulte Descripción general de licencias

6. Seleccione **Registrar con NetScaler ADM**.
7. Introduzca sus credenciales de NetScaler ADM para registrar una instancia con NetScaler ADM y haga clic en **Continuar**.



8. En **Asignar licencias**, seleccione la edición de la licencia y especifique el ancho de banda requerido.

   Por primera vez, asigne licencias en NetScaler. Más adelante, puede cambiar o liberar la asignación de licencias desde la GUI de NetScaler ADM.

   a) Haga clic en **Obtener licencias**.

   > **Importante:**
   >
   > Reinicie la instancia en caliente si cambia la edición de la licencia. Los cambios de configuración no surtirán efecto hasta que reinicie la instancia.

Use la CLI para agregar NetScaler ADM como servidor de licencias

Si una instancia de NetScaler no tiene ninguna GUI, utilice los siguientes comandos de la CLI para agregar el servidor NetScaler ADM como servidor de licencias:

1. Inicie sesión en la consola de NetScaler.
2. Agregue la dirección IP del servidor NetScaler ADM:

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number> -licensemode <license-mode>
<!--NeedCopy-->
```

   Para obtener más información, consulte Descripción general de las licencias.

3. Vea el ancho de banda de licencias disponible en el servidor de licencias.

```
> sh ns licenseserverpool
<!--NeedCopy-->
```

   Este comando enumera las licencias según el modo de licencia especificado al agregar el servidor de licencias.

   Ejemplo 1:

   Si el modo de licencia especificado es `CICO`, la salida solo contiene licencias de CICO.

```
> add licenseserver [redacted] -licensemode CICO
 Done
> sh licenseserverpool
        VPX8000P Total                  : 1
        VPX8000P Available              : 1
```

   Ejemplo-2:

   Si el modo de licencia especificado es `Pooled`, la salida solo contiene licencias de capacidad agrupada.

```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                  : 40
        Instance Available              : 38
        Standard Bandwidth Total        : 210.00 Gbps
        Standard Bandwidth Available    : 210.00 Gbps
        Enterprise Bandwidth Total      : 50.00 Gbps
        Enterprise Bandwidth Available  : 50.00 Gbps
        Platinum Bandwidth Total        : 210.00 Gbps
        Platinum Bandwidth Available    : 205.00 Gbps
```

   Ejemplo-3:

   Si el modo de licencia especificado es `vCPU`, la salida solo contiene licencias de CPU virtuales.


```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

Para ver todas las licencias juntas, ejecute el siguiente comando:

```
1  > sh ns licenseserverpool -getallLicenses
2  <!--NeedCopy-->
```

Ejemplo de salida:

```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. Asigne el ancho de banda de licencia desde la edición de licencia requerida:

```
1  > set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
       -amount-license-bandwidth> -edition <specify-license-edition>
2  <!--NeedCopy-->
```

La edición de licencia puede ser **Standard**, **Enterprise** o **Platinum**.

> **Importante**
>
> Warm reinicie la instancia si cambia la edición de la licencia.
>
> `reboot -w`
>
> Los cambios de configuración no surtirán efecto hasta que reinicie la instancia.

Paso 3: Asignar licencias agrupadas a instancias de NetScaler

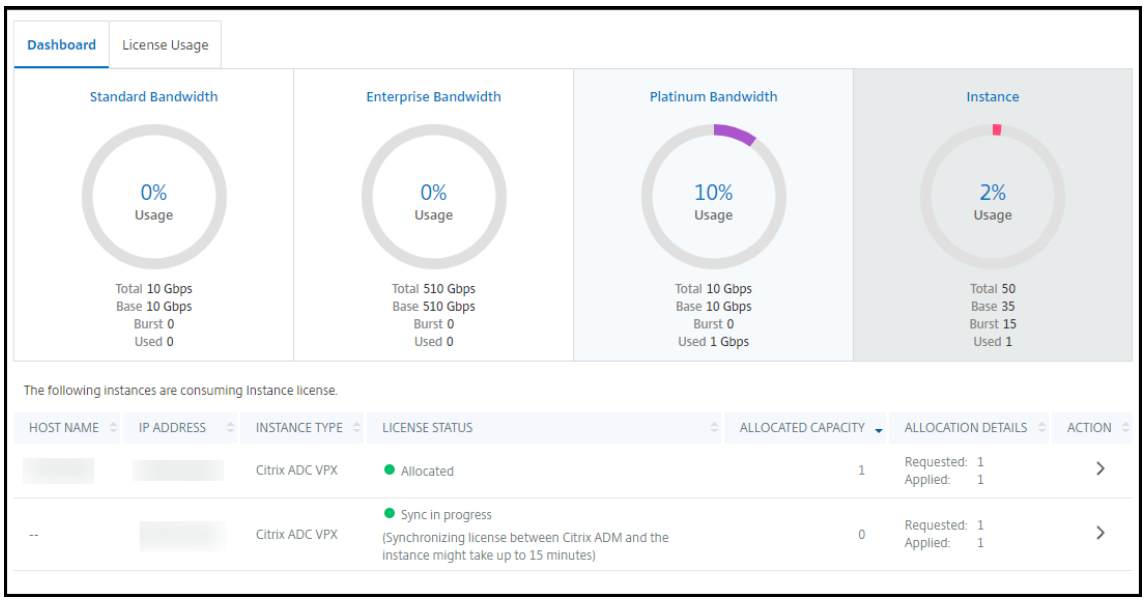
Para asignar licencias de capacidad agrupada desde la GUI de NetScaler ADM:

1. Inicie sesión en NetScaler ADM.
2. Vaya a **Infraestructura > Licencias > Licencias de ancho de banda > Capacidad agrupada**.

   La capacidad de la instancia FIPS solo aparece si carga licencias de instancias FIPS a NetScaler ADM.
3. Haga clic en el grupo de licencias que quiere administrar.

   > **Nota**
   >
   > El campo **Capacidad asignada** no refleja el ancho de banda modificado de forma inmediata. El cambio de ancho de banda se aplica tras el reinicio en caliente de NetScaler.
   >
   > En **Detalles de asignación, los**campos **Solicitado** y **Aplicado se** actualizan cuando cambias la asignación de ancho de banda de la instancia.

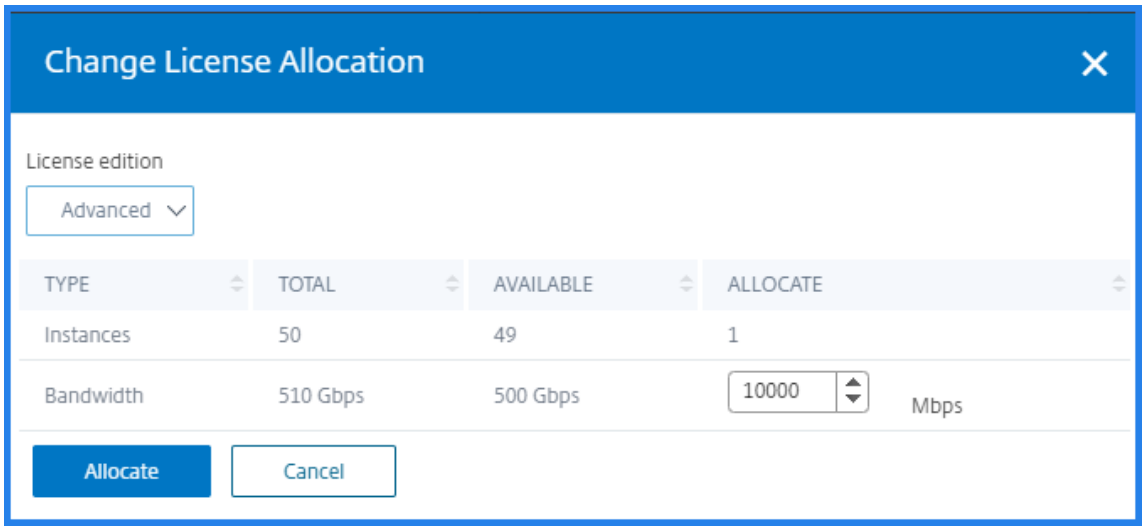
4. Seleccione una instancia de NetScaler de la lista de instancias disponibles haciendo clic en el botón **>**.



La columna **ESTADO DE LA LICENCIA** muestra los mensajes de estado de asignación de licencias correspondientes.

> **Nota:**
>
> La ficha **Instancias no administradas** muestra las instancias que se detectan pero no se administran en NetScaler ADM.

5. Haga clic en **Cambiar asignación** o **Liberar asignación** para modificar la asignación de licencias.
6. Aparecerá una ventana emergente con las licencias disponibles en el servidor de licencias.
7. Puede elegir el ancho de banda o la asignación de instancias a la instancia configurando las opciones de la lista **Asignación**. Después de hacer las selecciones, haga clic en **Asignar**.
8. También puede cambiar la edición de licencia asignada desde las opciones de lista en la **ventana Cambiar asignación de licencias**.



> **Nota**
>
> Reinicia una instancia en caliente si cambias la edición de la licencia.

Para obtener más información sobre cómo cambiar la asignación de ancho de banda, consulte el vídeo relacionado:

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Configurar la capacidad agrupada en instancias de NetScaler

Puede configurar licencias de capacidad agrupada en las siguientes instancias de NetScaler:

- Instancias de NetScaler
- Instancias de NetScaler VPX
- Par de alta disponibilidad NetScaler

Instancias de NetScaler MPX

MPX-Z es el dispositivo NetScaler MPX con capacidad agrupada. MPX-Z admite la agrupación de ancho de banda para licencias de edición Premium, Advanced o Standard.

MPX-Z requiere licencias de plataforma antes de poder conectarse al servidor de licencias. Puede instalar la licencia de plataforma MPX-Z de las siguientes maneras:

- Carga del archivo de licencia desde un equipo local.
- Usar el número de serie del hardware de la instancia.
- El código de acceso a licencias de la sección **Sistema** > **Licencias** de la GUI de la instancia.

Si quita la licencia de la plataforma MPX-Z, la función de capacidad agrupada se desactiva. Las licencias de instancia se entregan al 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.

Instancias de NetScaler VPX

Una instancia de NetScaler VPX con capacidad agrupada puede extraer licencias de un grupo de ancho de banda (ediciones Premium/Advanced/Standard). Puede usar la GUI de NetScaler para consultar las licencias del servidor de licencias.

Puede 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:**
>
> Al reiniciar la instancia, las licencias de capacidad agrupada configuradas se retiran automáticamente del servidor NetScaler ADM.

Par de alta disponibilidad NetScaler

Antes de empezar, asegúrese de que el servidor NetScaler ADM esté configurado como servidor de licencias. Para obtener más información, consulte Configurar NetScaler ADM como servidor de licencias.

Para las instancias de NetScaler configuradas en un modo de alta disponibilidad, debe configurar la capacidad agrupada en cada nodo del par de alta disponibilidad. Tanto para el nodo principal como para el secundario, debe asignar licencias de la misma capacidad. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia en el par de alta disponibilidad, necesita el doble de capacidad (2 Gbps) del grupo común. A continuación, puede asignar una capacidad de 1 Gbps a cada nodo.

Para asignar una licencia de grupo a cada nodo del par, siga los pasos que se indican en Asignar licencias agrupadas a instancias de NetScaler. Primero asigne la licencia al primer nodo y, a continuación, repita los mismos pasos para asignar la licencia al segundo nodo.

Actualice una licencia perpetua en NetScaler VPX a NetScaler Pooled capacity

January 30, 2024

Las instancias de NetScaler VPX con licencia perpetua se pueden actualizar a una licencia de capacidad agrupada de ADC. La actualización a una licencia de capacidad agrupada le permite asignar licencias del grupo de licencias a las instancias VPX a pedido. También puede configurar la licencia de capacidad agrupada para instancias de ADC configuradas en un modo de alta disponibilidad. Para configurar la licencia de capacidad agrupada para instancias VPX en modo de alta disponibilidad, consulte Actualización de la licencia perpetua del par de alta disponibilidad de NetScaler VPX a NetScaler Pooled Capacity.

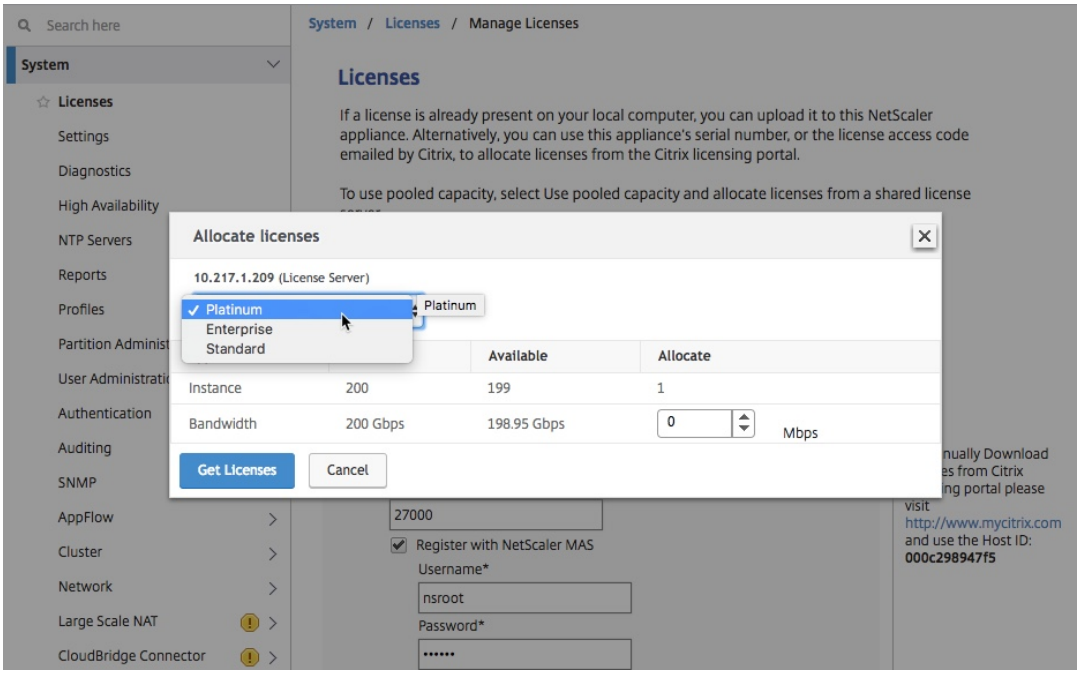
Requisitos previos

Para actualizar a la capacidad agrupada de NetScaler:

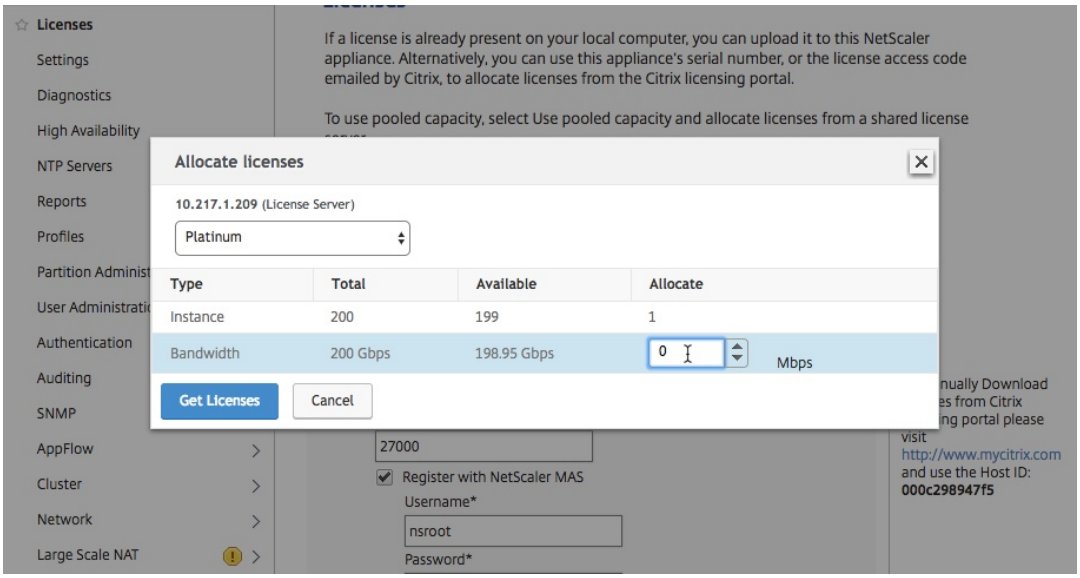
1. En un explorador web, escriba la dirección IP de la instancia VPX, como http://192.168.100.1.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. En la **pestaña Configuración** , vaya a **Sistema > Licencias** y haga clic en **Administrar licencias** .
5. En la página **Licencias**, haga clic en **Agregar nueva licencia**.
6. En la página **Licencias**, elija **Usar licencias remotas** y haga lo siguiente:
    a) En la lista desplegable del **modo de licencia remota**, seleccione Licencias **agrupadas.**
    b) En el campo **Nombre del servidor/Dirección IP**, Introduzca los detalles del servidor de licencias.
    c) Asegúrese de que la casilla **Registrar con NetScaler ADM** esté seleccionada e introduzca las credenciales de NetScaler ADM si desea administrar las licencias de grupo de su instancia a través de NetScaler ADM.
    d) Haga clic en **Continuar**.

7. En **Asignar licencias**, haga lo siguiente:

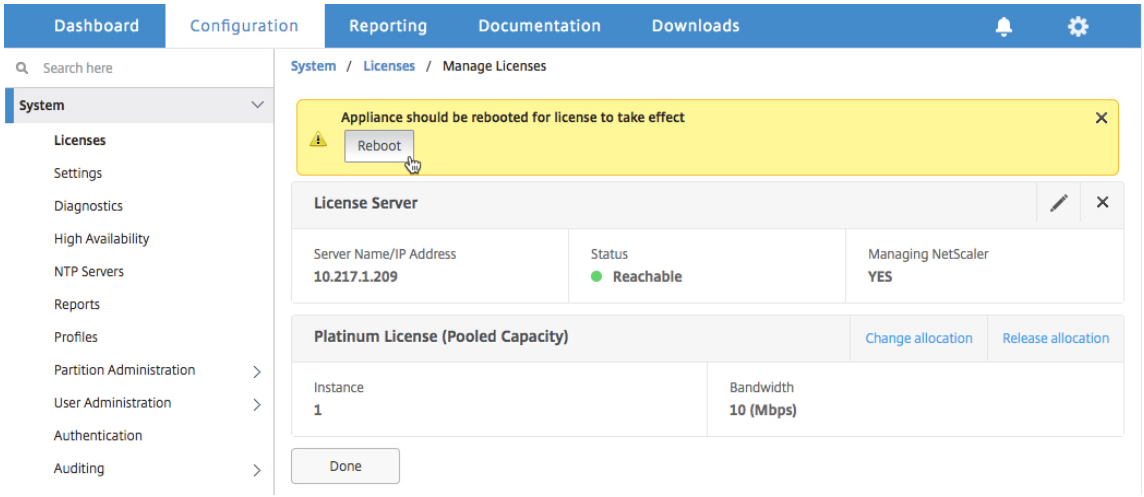
   a) Seleccione la edición de licencia en la lista desplegable.



   b) Asigne el ancho de banda al dispositivo NetScaler desde el menú **Asignar** y haga clic en **Obtener licencias**.



8. Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.



9. En el cuadro de diálogo Confirmar, haga clic en **Sí** .
10. Después de que se reinicie la instancia VPX, inicie sesión en la instancia. En la página de **bienvenida**, haga clic en **Continuar**.

    La página **Licencias** muestra todas las funciones que tienen licencia en el dispositivo NetScaler VPX. Haga clic en **X**.
11. 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.

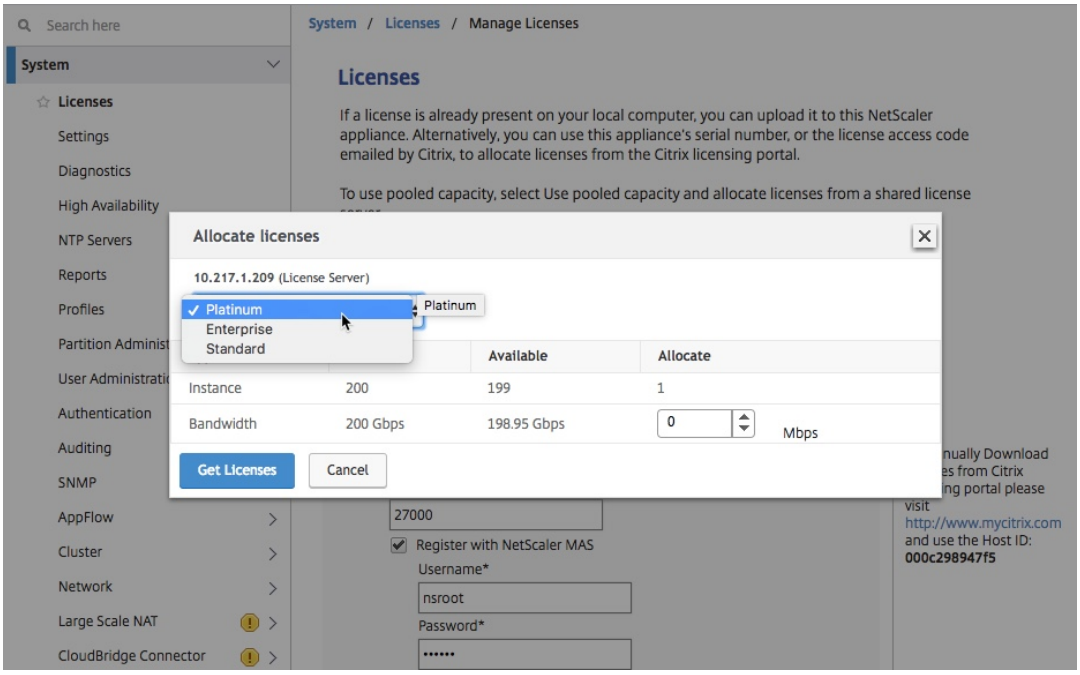
Actualice la licencia perpetua del par de alta disponibilidad de NetScaler VPX a la capacidad agrupada de NetScaler

Para las instancias VPX configuradas en un modo de alta disponibilidad, debe configurar la capacidad agrupada en las instancias principales y secundarias del par HA. Tanto para las instancias principales como para las secundarias, debe asignar licencias de la misma capacidad. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia en el par de alta disponibilidad, necesita el doble de capacidad (2 Gbps) del grupo común. A continuación, puede asignar una capacidad de 1 Gbps a cada una de las instancias principal y secundaria del par de alta disponibilidad.

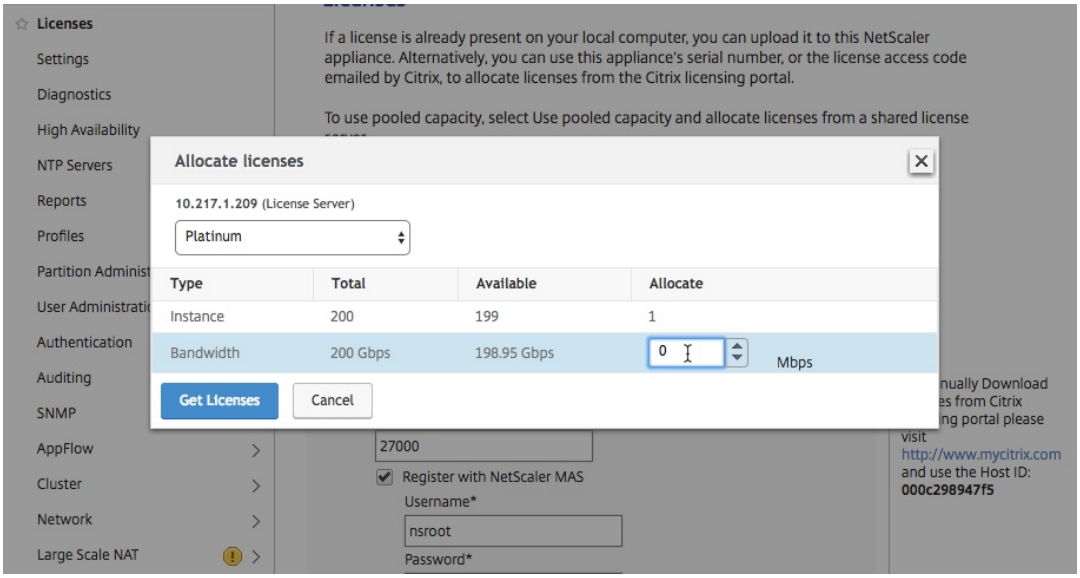
Para actualizar una configuración existente de NetScaler VPX HA a la capacidad agrupada de NetScaler:

1. Inicie sesión en la instancia VPX secundaria (nodo 2). En un explorador web, escriba la dirección IP del dispositivo NetScaler, como `http://192.168.100.1`.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.

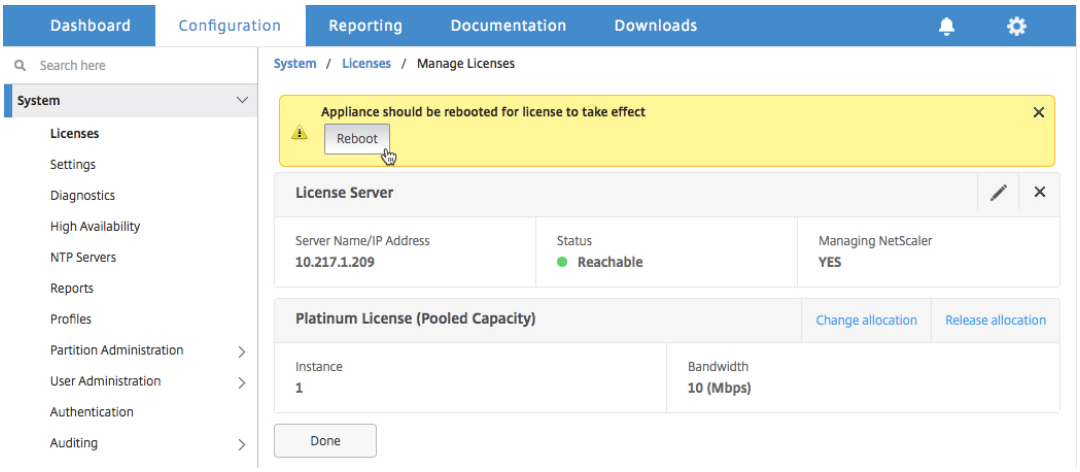
4. En la pestaña Configuración, vaya a **Sistema > Licencias** y haga clic en **Administrar licencias** .
5. En la página **Licencias**, haga clic en **Agregar nueva licencia**.
6. Elija **Usar licencias remotas** y haga lo siguiente:
   a) En la lista desplegable del **modo de licencia remota**, seleccione Licencias **agrupadas.**
   b) En el campo **Nombre del servidor/Dirección IP**, Introduzca los detalles del servidor de licencias.
   c) Asegúrese de que la casilla **Registrar con NetScaler ADM** esté seleccionada e introduzca las credenciales de NetScaler ADM si desea administrar las licencias de grupo de su instancia a través de NetScaler ADM.
   d) Haga clic en **Continuar**.
7. En **Asignar licencias**, haga lo siguiente:
   a) Seleccione la edición de licencia en la lista desplegable.



   b) Asigne el ancho de banda al dispositivo NetScaler desde el menú **Asignar** y haga clic en **Obtener licencias**.



c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar en caliente la instancia.



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

   La instancia VPX se reinicia.

   Cuando se le solicite, haga clic en **Reiniciar para reiniciar** el dispositivo. Una vez que el dispositivo esté en funcionamiento con la nueva licencia, fuerce una conmutación por error escribiendo `force ha failover`. Esta conmutación por error garantiza que el par de alta disponibilidad esté en buen estado.

9. Después de la conmutación por error, inicie sesión en la nueva instancia VPX secundaria (nodo 1) y repita el mismo proceso para agregar la nueva instancia secundaria al grupo.

   Si desea cambiar las instancias principales y secundarias del par HA a la configuración original del par HA, fuerce una conmutación por error. Ejecute el siguiente comando en cualquier instancia del par de alta disponibilidad:


```
  > force ha failover
<!--NeedCopy-->
```

10. Para comprobar que la instancia VPX se ha actualizado a la licencia de capacidad agrupada, inicie sesión en las instancias principal y secundaria y complete los siguientes pasos.

    a) En la página de **bienvenida**, haga clic en **Continuar**.

    b) En la pestaña Configuración, 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.

Actualización de una licencia perpetua en NetScaler MPX a la capacidad agrupada de NetScaler

January 30, 2024

El NetScaler MPX con licencia perpetua se puede actualizar a la licencia NetScaler Pooled Capacity. La actualización a la licencia NetScaler Pooled Capacity le permite asignar licencias del grupo de licencias a dispositivos NetScaler bajo demanda. También puede configurar la licencia de capacidad agrupada de NetScaler para las instancias de NetScaler configuradas en modo de alta disponibilidad. Para configurar la licencia de capacidad agrupada de NetScaler para instancias MPX de NetScaler en modo de alta disponibilidad, consulte Actualización de la licencia perpetua del par de alta disponibilidad de NetScaler MPX a NetScaler Pooled capacity.

> **Nota**
>
> La conversión de una licencia perpetua a una licencia de capacidad agrupada es un proceso unidireccional para la obtención de derechos de licencia. No puede revertir la licencia de capacidad agrupada a perpetua.
>
> **Importante**
>
> Para actualizar la licencia de NetScaler MPX a la licencia de capacidad agrupada de NetScaler, debe cargar la licencia MPX-Z en el dispositivo.

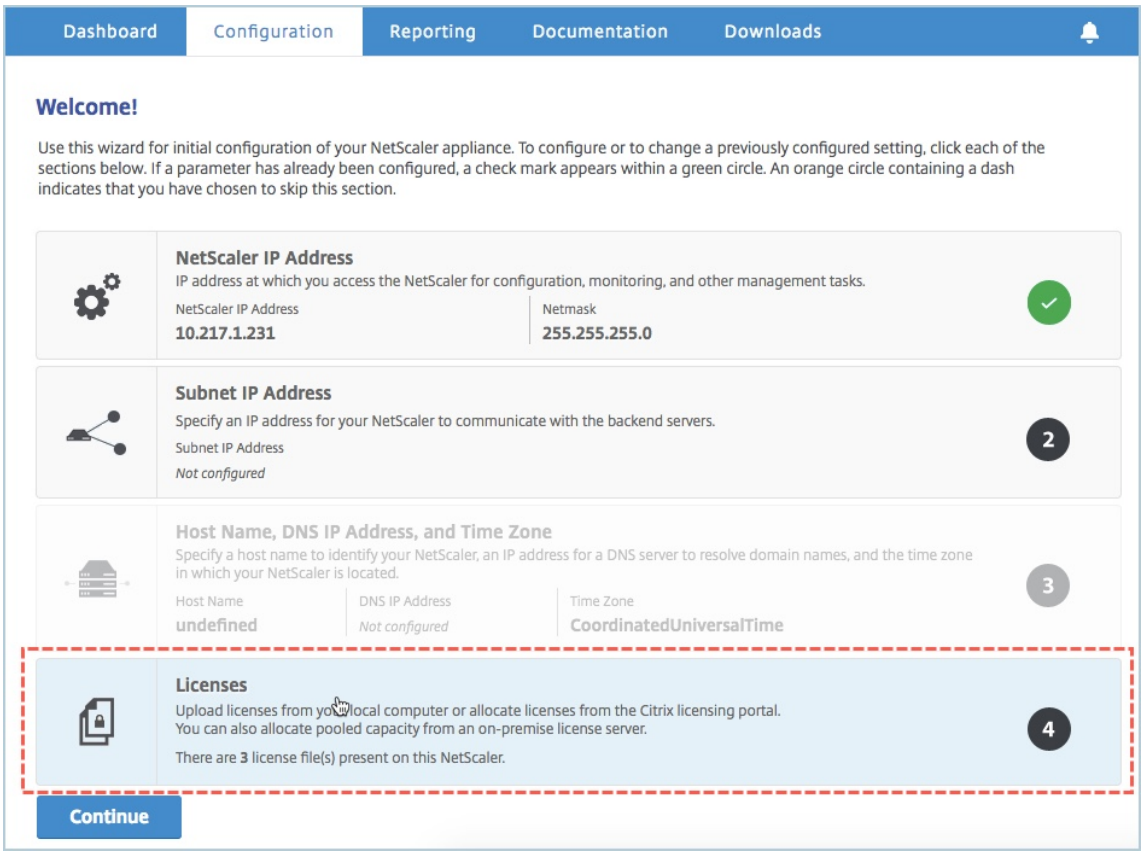
Para actualizar a la capacidad agrupada de NetScaler:

1. En un navegador web, escriba la dirección IP del NetScaler, como http://192.168.100.1.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.

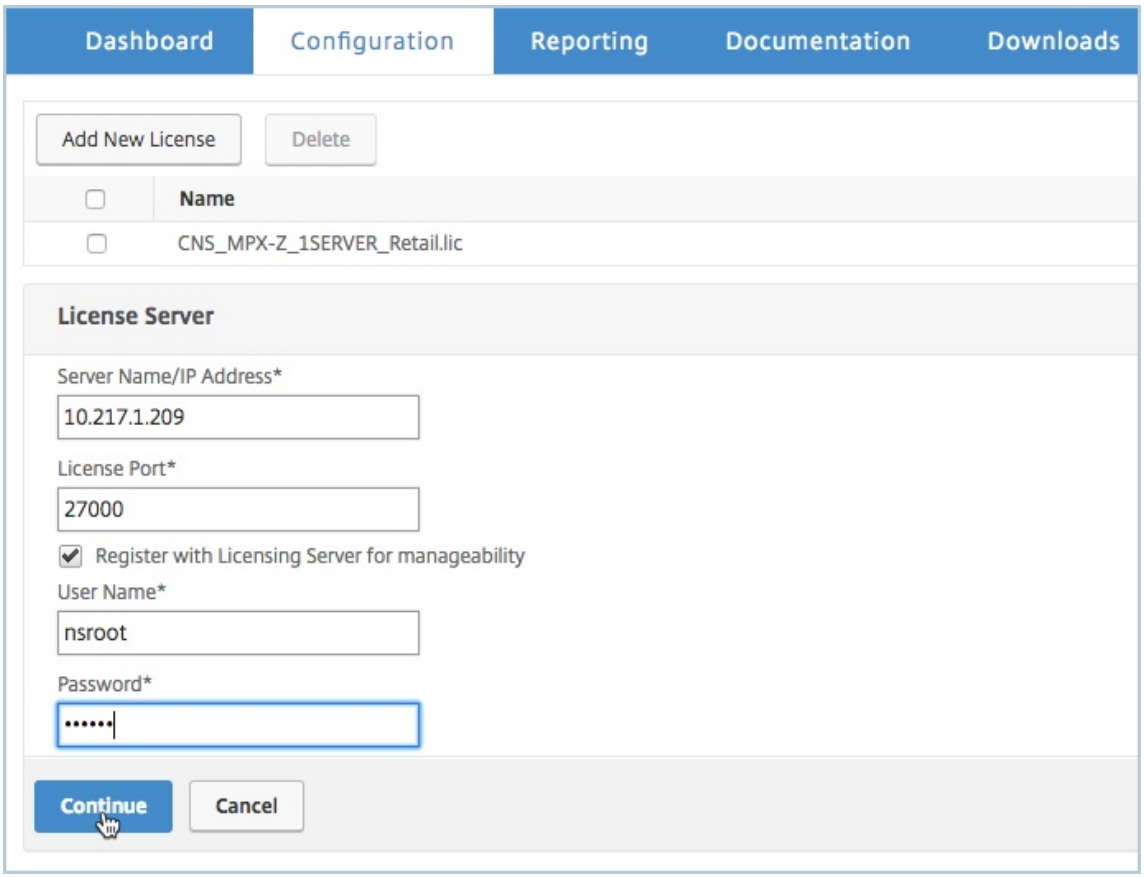
4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha Configuración, vaya a **Sistema** > **Licencias**.
5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en Agregar **nueva licencia** .
6. En la página **Licencias** , seleccione Cargar **archivos de licencia** y haga clic **en**Examinar para seleccionar la licencia de capacidad cero de su máquina local.
7. Después de cargar la licencia, haga clic en **Reiniciar** para 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.

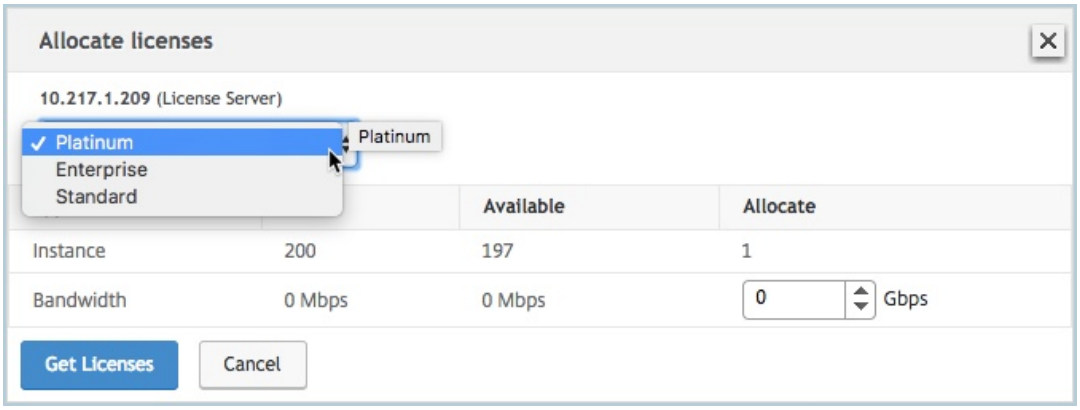
b) En el campo **Puerto de licencias**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Si desea administrar las licencias del grupo de instancias a través de NetScaler ADM, seleccione la casilla **Registrarse en el servidor de licencias para facilitar la administración** e introduzca las credenciales de NetScaler ADM.

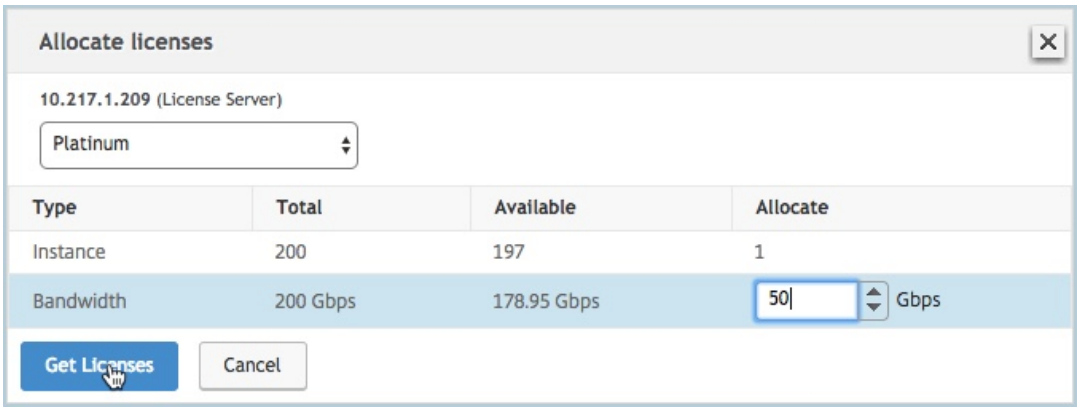
d) Haga clic en **Continuar**.

12. En **Asignar licencias**, haga lo siguiente:

a) Seleccione la edición de licencia en la lista desplegable.



b) Asigne el ancho de banda a NetScaler desde el menú **Asignar** y haga clic en **Obtener licencias**.



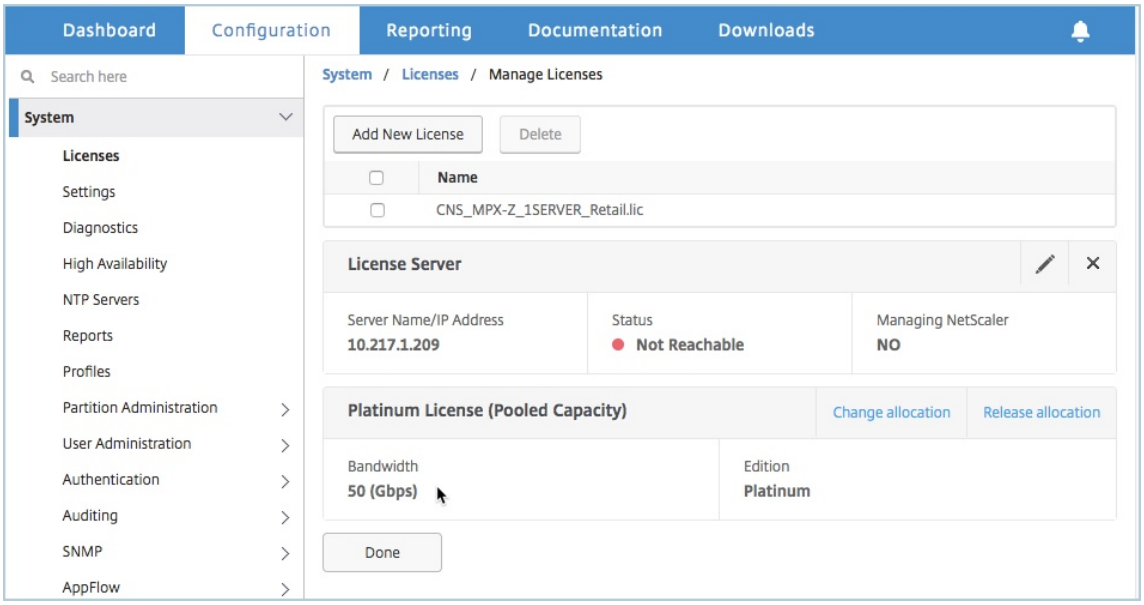
c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.

13. Cuando se reinicie NetScaler MPX, inicie sesión en el NetScaler 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.



Actualización de la licencia perpetua del par de alta disponibilidad de NetScaler MPX a la capacidad agrupada de NetScaler

Para los dispositivos MPX configurados en modo de alta disponibilidad, debe configurar la capacidad agrupada en las instancias de NetScaler principales y secundarias del par HA. Asigne licencias de la misma capacidad a las instancias de NetScaler principales y secundarias en el par de alta disponibilidad. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia en el par de alta disponibilidad, debe asignar una capacidad de 2 Gbps del grupo común. Con una capacidad de 2 Gbps, puede asignar 1 Gbps cada una a las instancias de NetScaler principal y secundaria en el par de alta disponibilidad.

> **Importante**
>
> Para actualizar NetScaler MPX para usar la licencia de capacidad agrupada de NetScaler, debe cargar el MPX-Z en el 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 de NetScaler MPX en el par de HA:

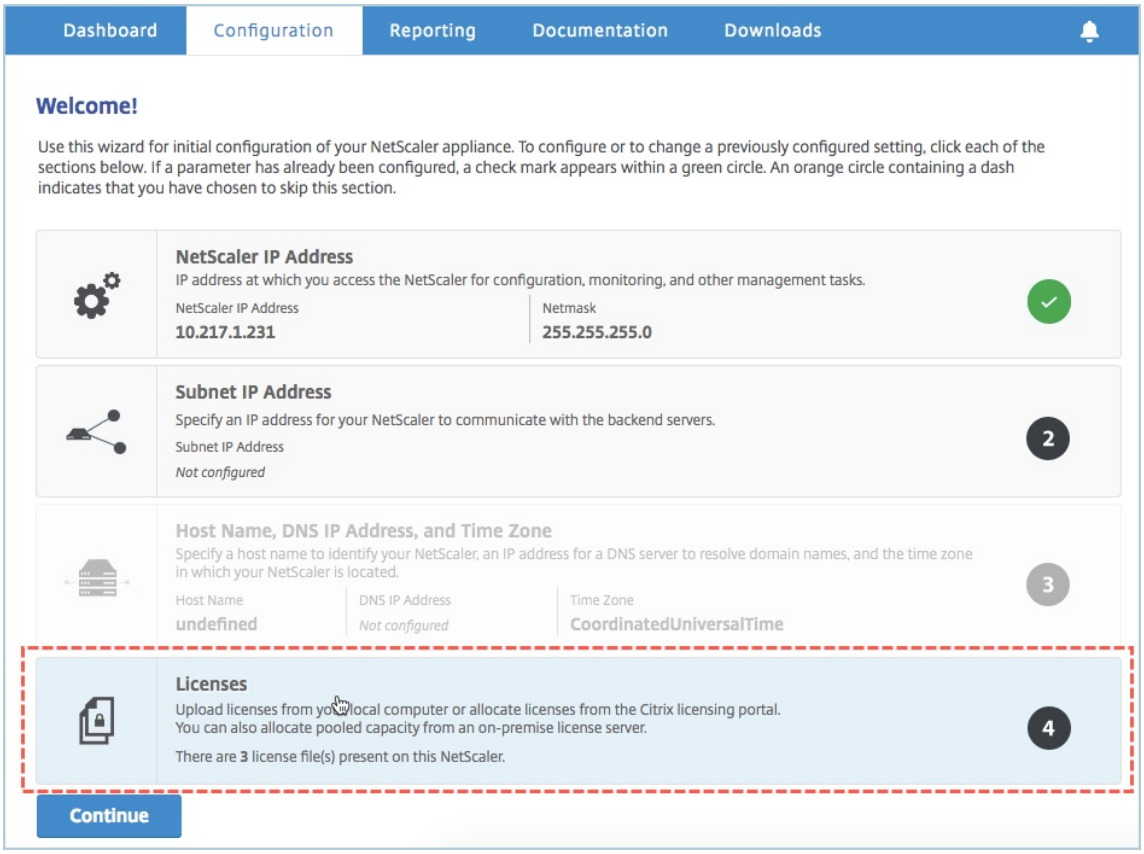
1. En un explorador web, escriba la dirección IP del dispositivo. Por ejemplo: http://192.168.100.1.
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero (licencia 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 máquina local.

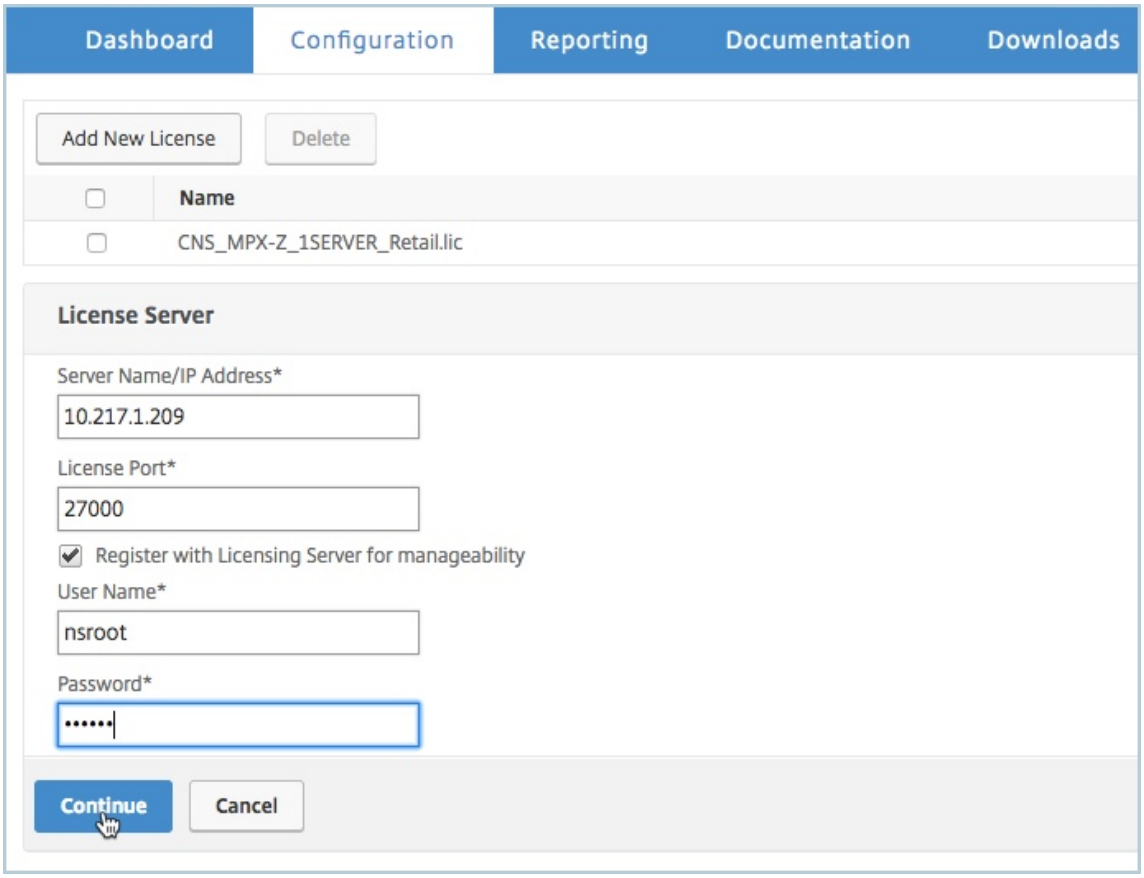
   Una vez cargada la licencia, se le pedirá que reinicie el dispositivo.
7. Haga clic en **Reiniciar** para reiniciar el dispositivo.
8. En la página de **confirmación** , haz clic en **Sí** .

Para actualizar una configuración de alta disponibilidad existente a la capacidad agrupada de NetScaler:

1. Inicie sesión en la instancia de NetScaler MPX secundaria. En un navegador web, escriba la dirección IP de NetScaler, como http://192.168.100.1.
2. En **Nombre de usuario** y **Contraseña**, introduzca 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.

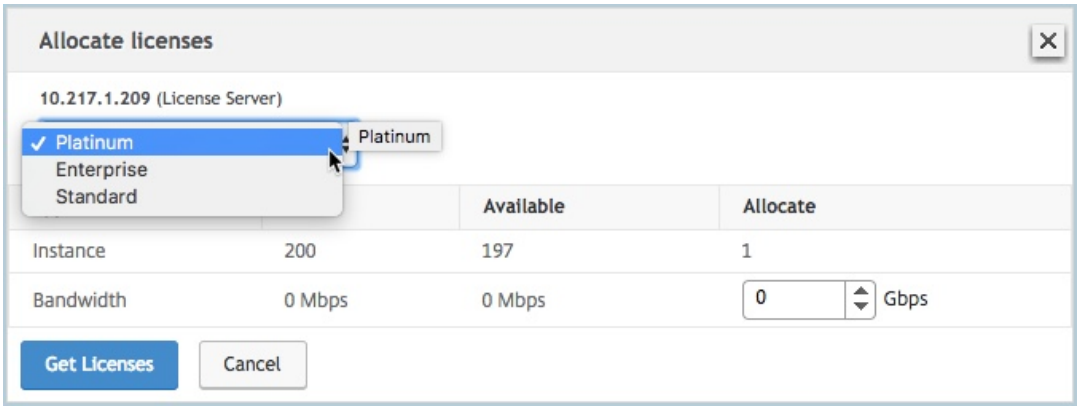
b) En el campo **Puerto de licencias**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Si desea administrar las licencias del grupo de instancias a través de NetScaler ADM, seleccione la casilla **Registrarse en el servidor de licencias para facilitar la administración** e introduzca las credenciales de NetScaler ADM.

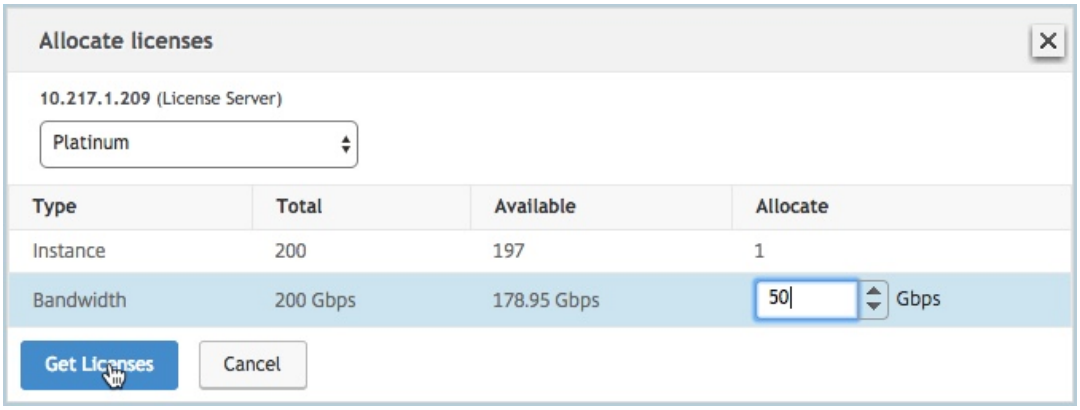
d) Haga clic en **Continuar**.

5. En **Asignar licencias**, haga lo siguiente:

a) Seleccione la edición de licencia en la lista desplegable.



b) Asigne el ancho de banda a NetScaler desde el menú **Asignar** y haga clic en **Obtener licencias**.



c) Cuando se le solicite, haga clic en **Reiniciar para reiniciar** el dispositivo. Una vez que el dispositivo esté en funcionamiento con la nueva licencia, fuerce una conmutación por error escribiendo `force ha failover`. Esta conmutación por error garantiza que el par de alta disponibilidad esté en buen estado.

6. Inicie sesión en el NetScaler MPX principal existente y reinicie el dispositivo. Lleve a cabo lo siguiente:

   a) En un navegador web, escriba la dirección IP del NetScaler, como http://192.168.100.1.

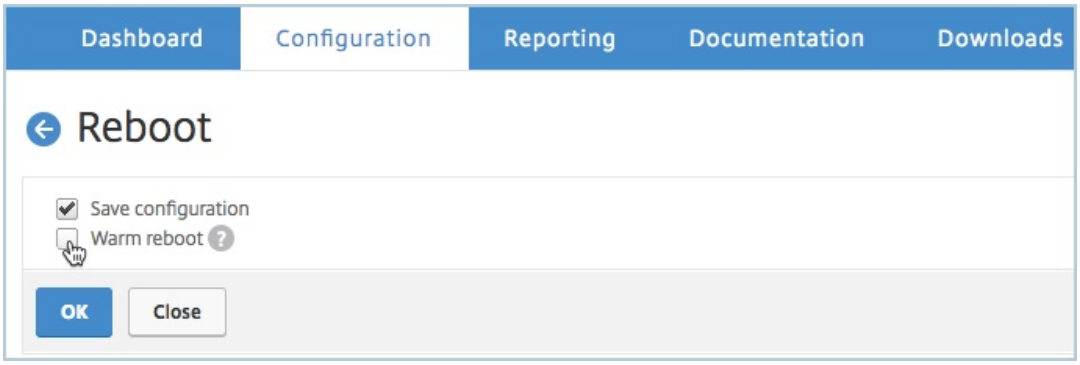
   b) En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.

   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**.



Tras reiniciarse el NetScaler MPX principal, pasa a ser el NetScaler MPX secundario del par HA. Si desea cambiar las instancias principales y secundarias del par HA a la configuración original del par HA, fuerce una conmutación por error. Ejecute el siguiente comando en cualquier instancia del par de alta disponibilidad:

```
> force ha failover
<!--NeedCopy-->
```

Actualice una licencia perpetua en un NetScaler SDX a la capacidad agrupada de NetScaler

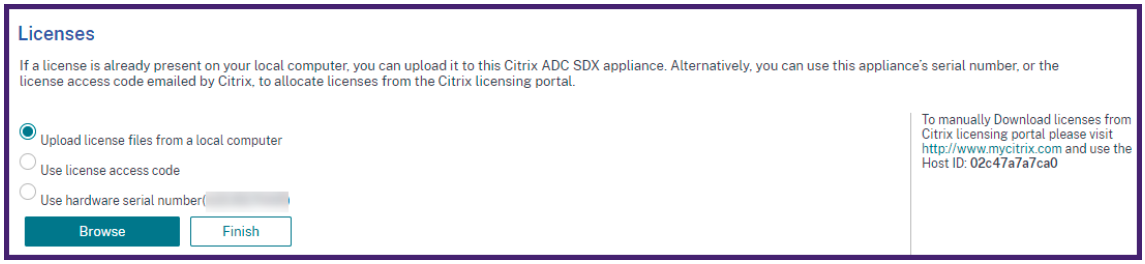
January 30, 2024

El NetScaler SDX con licencia perpetua se puede actualizar a la licencia de capacidad agrupada de NetScaler. La actualización a la licencia NetScaler Pooled Capacity le permite asignar licencias del grupo de licencias a NetScaler a pedido. También puede configurar la licencia de capacidad agrupada de NetScaler para las instancias de NetScaler configuradas en modo de alta disponibilidad.

> **Importante**
>
> La conversión de una licencia perpetua a una licencia de capacidad agrupada es un proceso de asignación de derechos de licencia unidireccional. No puede revertir la licencia de capacidad agrupada a perpetua.
>
> - Para actualizar la licencia de NetScaler SDX a la licencia NetScaler Pooled Capacity, debe cargar la licencia SDX-Z en el dispositivo.
> - Asegúrese de tener el permiso para agregar instancias de NetScaler en NetScaler ADM.
> - Para garantizar que no haya ningún impacto en las licencias actuales, el cliente debe asignar la misma cantidad de instancias y ancho de banda que están disponibles como parte de la licencia perpetua.

Para actualizar a la capacidad agrupada de NetScaler:

1. En un navegador web, escriba la dirección IP de NetScaler SDX, por ejemplo: http://192.168.100.1.
2. En **Nombre de usuario** y **Contraseña**, introduzca 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. En la página **Administrar licencias**, haga clic en **Agregar archivo de licencia**.
6. En la página **Licencias** , seleccione **Cargar archivos de licencia desde un equipo local** y haga clic **en**Examinar para seleccionar la licencia de capacidad cero de su máquina local. A continuación, haga clic en **Finalizar**.



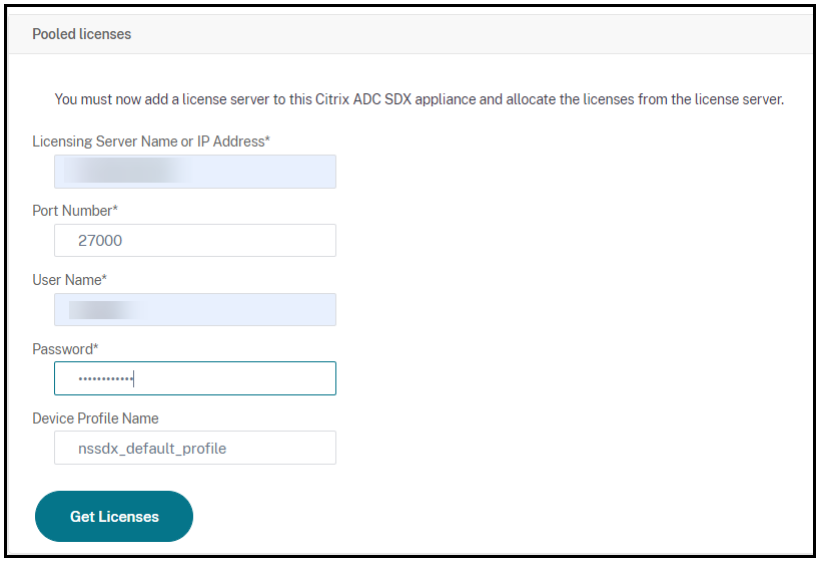
Una vez que la licencia de capacidad cero se haya aplicado correctamente, la sección **Licencias** agrupadas aparece en la página **Licencias** .

> **Nota**
>
> Para eliminar el archivo de licencia anterior, no es necesario reiniciar el NetScaler SDX, por lo que no hay tiempo de inactividad. Para obtener más ayuda, póngase en contacto con el servicio de asistencia de NetScaler.

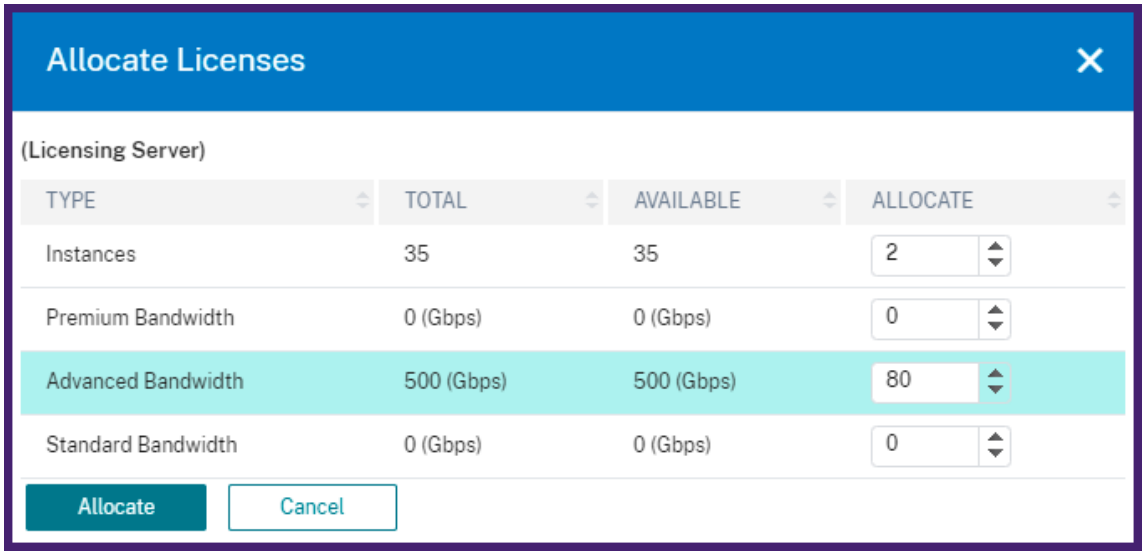
7. En la sección **Licencias agrupadas**, haga lo siguiente:
   a) En el campo **Nombre del servidor de licencias o Dirección IP**, introduzca los detalles del servidor de licencias.
      - Si desea configurar el servidor NetScaler ADM como servidor de licencias, especifique la dirección IP del servidor NetScaler ADM.
      - Si utiliza un agente para comunicarse con el servidor NetScaler ADM, especifique la dirección IP del agente NetScaler ADM.
   b) En el campo **Número de puerto**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.
   c) Especifique **el nombre de usuario** y la **contraseña** del servidor de licencias.
      - Para el servidor NetScaler ADM, introduzca las credenciales de administrador.

- Para el agente ADM de NetScaler, introduzca las credenciales del agente.

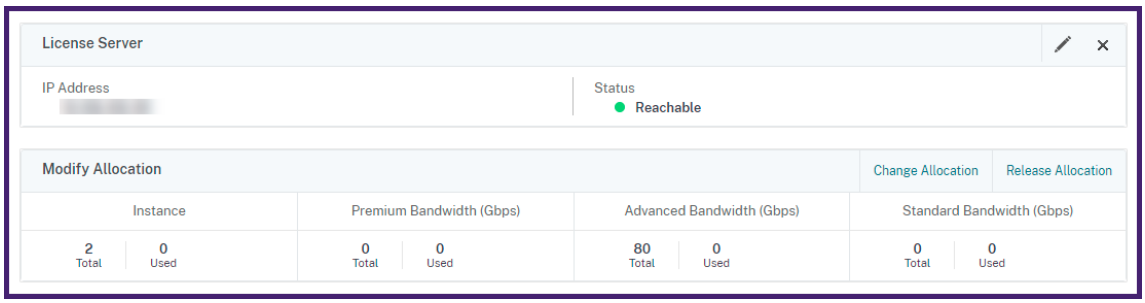
d) Haga clic en **Obtener licencias**.



8. 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.



> **Nota**
>
> La actualización de una licencia perpetua a capacidad agrupada no requiere reiniciar el dispositivo SDX.

Capacidad agrupada de NetScaler en instancias de NetScaler en modo clúster

January 30, 2024

Puede configurar la capacidad agrupada de NetScaler en las instancias de NetScaler configuradas como clúster. Los siguientes son los requisitos previos para configurar la capacidad agrupada en las instancias de NetScaler en modo clúster:

- Las instancias se ejecutan 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 comprobaron la capacidad agrupada de la misma administración y entrega de aplicaciones de NetScaler.
- No se pueden agregar nuevas instancias a un clúster de NetScaler 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 reducción de capacidad del clúster de NetScaler asigna la misma capacidad a todos los nodos del clúster y el ancho de banda de salida = ancho de banda proporcionado * cantidad de nodos.

Por ejemplo, si desactiva 50 Mbps de ancho de banda del clúster NetScaler y el clúster incluye 12 instancias, cada instancia recibe automáticamente 50 Mbps. Y 600 Mbps es extraen de la agrupación.

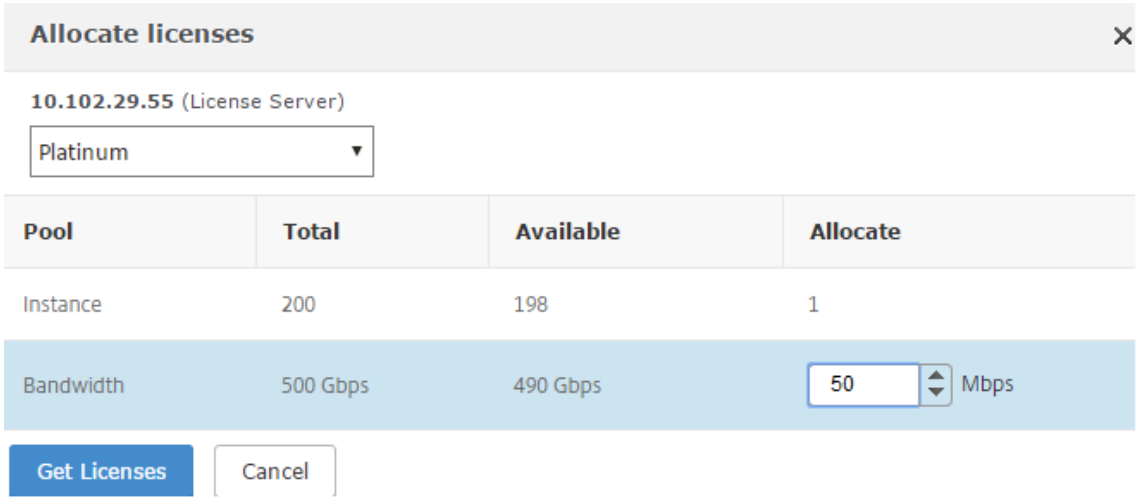
> **Nota**
>
> Si una o más instancias del clúster dejan de responder, el clúster continúa procesando el tráfico con la capacidad de las instancias restantes.

Asigne la capacidad agrupada de ADC a un clúster de ADC

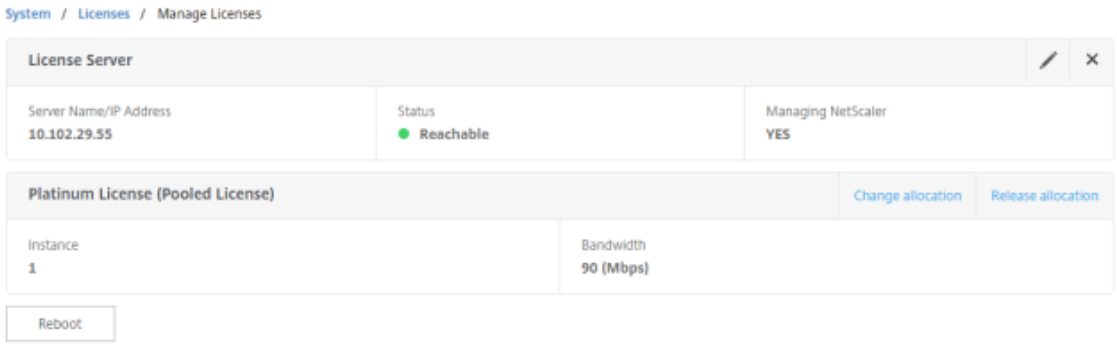
Asigne licencias a cada nodo del clúster por separado. Porque los comandos para propagar y sincronizar las licencias en los nodos del clúster están inhabilitados.

Repita el siguiente procedimiento en cada nodo del clúster:

1. En un navegador web, escriba la dirección IP de NetScaler (NSIP). 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 el nombre o la dirección del servidor de licencias en el campo **Nombre del servidor/Dirección IP**.
5. Si desea administrar las licencias del grupo de instancias a través de NetScaler ADM, seleccione la casilla **Registrarse en NetScaler ADM para obtener capacidad de administración** e introduzca las credenciales de NetScaler ADM .
6. Seleccione la edición de licencia y el ancho de banda requerido y haga clic en **Obtener licencias**.

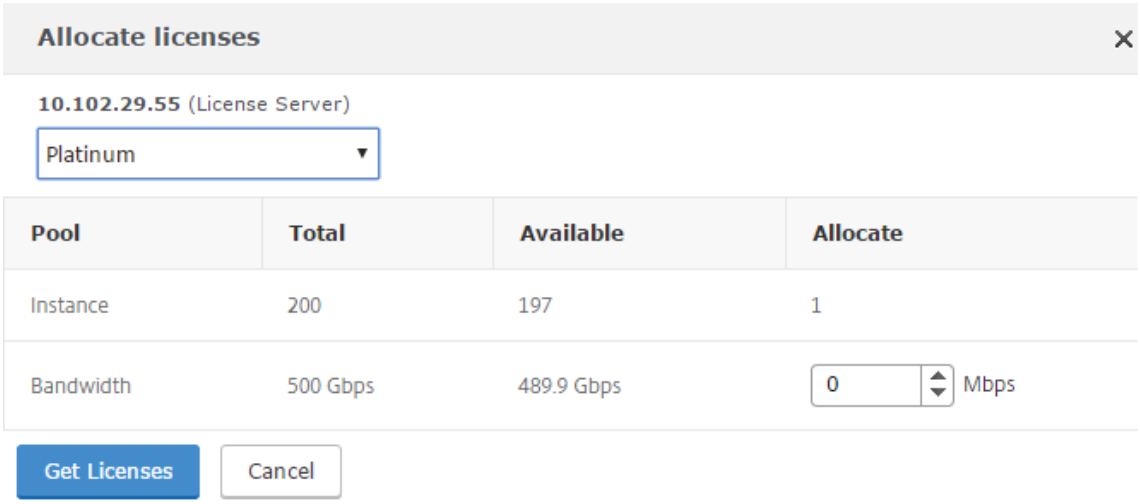


7. Puede cambiar o liberar la asignación de licencias seleccionando **Cambiar asignación** o **Liberar asignación**.



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 NetScaler 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.

Asigne la capacidad agrupada de ADC a un clúster de ADC mediante la CLI

Asigne licencias a cada nodo del clúster por separado. Porque los comandos para propagar y sincronizar las licencias en los nodos del clúster están inhabilitados.

Repita el siguiente procedimiento en cada nodo del clúster:

1. En un cliente SSH, introduzca la dirección IP de NetScaler (NSIP) 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 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
```


Comportamientos esperados cuando surgen problemas

January 30, 2024

Los siguientes son los comportamientos esperados de los servidores de licencias y las instancias de NetScaler cuando experimentan los problemas descritos:

El servidor de licencias deja de responder

> **Advertencia**
>
> El servidor de licencias no responde. NetScaler continúa operando con la capacidad actual durante 30 días. Después de 30 días, si no se restaura la conectividad con el servidor de licencias, NetScaler pierde su capacidad actual y detiene el procesamiento del tráfico.

Si el servidor de licencias deja de responder, la instancia de NetScaler entra en el período de gracia hasta que se restaure la conectividad.

La instancia agrupada de NetScaler deja de responder

Si la instancia agrupada de NetScaler 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 transcurridos 10 minutos. Cuando la instancia se reinicia, envía una solicitud para desproteger todas las licencias del servidor de licencias.

Tanto el servidor de licencias como la instancia agrupada de NetScaler dejan de responder

Si tanto el servidor de licencias como la instancia de NetScaler Pooled se reinician y restablecen la conexión, el servidor de licencias registra todas sus licencias transcurridos 10 minutos y las instancias de NetScaler Pooled las extraen automáticamente una vez finalizado el reinicio.

La instancia agrupada de NetScaler se cierra correctamente

Durante un cierre agraciado, puede optar por registrar las licencias o conservar las licencias asignadas antes del cierre agraciado. Si decide comprobar que las licencias de la instancia agrupada de NetScaler no tienen licencia después de reiniciarse. 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 el proceso de pago falla debido a que no hay capacidad disponible en el grupo, NetScaler comprueba el inventario de las licencias del grupo de administración y entrega de aplicaciones de NetScaler y comprueba cualquier capacidad disponible. Se genera una alarma SNMP para notificar esta condición al usuario si el NetScaler no se ejecuta con plena capacidad según la configuración. Si no hay capacidad disponible en el grupo de ancho de banda, la instancia del grupo deja 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 agrupadas de NetScaler están en buen estado pero se pierde la conectividad de red, 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, las instancias vuelven a desproteger las licencias.

Período de gracia

Cuando una instancia agrupada de NetScaler está 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.

Escenarios de caducidad de licencias flexibles o agrupadas y comportamiento de problemas de conectividad

January 30, 2024

Este documento presenta diferentes escenarios de caducidad de licencias y comportamiento de problemas de conectividad en NetScaler MPX, NetScaler SDX y NetScaler VPX/NetScaler BLX/NetScaler CPX.

Tipos de licencias flexibles

- Instancia de software (VPX/BLX/CPX, SDX, MPX, VPX FIPS)
- Capacidad de ancho de banda

MPX FIPS usa una licencia del grupo de software MPX. SDX FIPS usa una licencia del grupo de software SDX. VPX FIPS usa una licencia del grupo de software VPX FIPS.

Escenario: formato MPX

Está utilizando licencias Flexed/Pooled y las licencias caducarán pronto. Los siguientes escenarios explican el comportamiento cuando se carga una nueva licencia en NetScaler Application Delivery and Management antes y después de que caduque el plazo, o cuando no hay un archivo de licencia.

Antes de que venza el plazo

Si la nueva licencia se carga antes de que venza el plazo y la licencia anterior sigue siendo válida, hay dos grupos de capacidad diferentes (antiguo y nuevo) disponibles.

- Si NetScaler está en funcionamiento, cambia a la nueva licencia Flexed/Pooled sin problemas una vez que caduque la licencia anterior.
- No es necesario reiniciar.
- NetScaler no requiere una reconfiguración manual de la capacidad.

Después de que venza el plazo

En este caso, el conjunto de capacidad existente ha caducado.

- NetScaler sigue funcionando con licencia hasta que se reinicie.
- Si NetScaler se reinicia y no hay ningún archivo de licencia válido, deja de tener licencia.
- Si NetScaler permanece activo para obtener la nueva licencia, se debe reconfigurar manualmente (reasignar la capacidad).

Escenario: formato SDX

Está utilizando licencias Flexed/Pooled y las licencias caducarán pronto. Los siguientes escenarios explican el comportamiento cuando se carga una nueva licencia en NetScaler Application Delivery and Management antes y después de que caduque el plazo, o cuando no hay un archivo de licencia.

Antes de que venza el plazo

Si la nueva licencia se carga antes de que venza el plazo y la licencia anterior sigue siendo válida, hay dos grupos de capacidad diferentes (antiguo y nuevo) disponibles.

- Si NetScaler está en funcionamiento, cambia a la nueva licencia Flexed/Pooled sin problemas una vez que caduque la licencia anterior.
- No es necesario reiniciar.
- NetScaler no requiere una reconfiguración manual de la capacidad.

Después de que venza el plazo

En este caso, el conjunto de capacidad existente ha caducado.

- NetScaler sigue funcionando con licencia hasta que se reinicie.
- Si el servicio de administración se reinicia y no hay ningún archivo de licencia válido, el rendimiento de todos los VPX se reduce a 1 Mbps.
- Si el servicio de administración permanece activo para recoger la nueva licencia, se debe reconfigurar manualmente (reasignar la capacidad).

Escenario: factor de forma VPX/BLX/CPX

Está utilizando licencias Flexed/Pooled y las licencias caducarán pronto. Los siguientes escenarios explican el comportamiento cuando se carga una nueva licencia en NetScaler Application Delivery and Management antes y después de que caduque el plazo, o cuando no hay un archivo de licencia.

Antes de que venza el plazo

Si la nueva licencia se carga antes de que venza el plazo y la licencia anterior sigue siendo válida, hay dos grupos de capacidad diferentes (antiguo y nuevo) disponibles.

- Si NetScaler está en funcionamiento, cambia a la nueva licencia Flexed/Pooled sin problemas una vez que caduque la licencia anterior.
- No es necesario reiniciar.
- NetScaler no requiere una reconfiguración manual de la capacidad.

Después de que venza el plazo

En este caso, el conjunto de capacidad existente ha caducado.

- NetScaler sigue funcionando con licencia hasta que se reinicie.

- Si NetScaler se reinicia y no hay ningún archivo de licencia válido, VPX y BLX dejarán de tener licencia y CPX pasará a ser CPX Express.
- Si NetScaler permanece activo para obtener la nueva licencia, se debe reconfigurar manualmente (reasignar la capacidad).

Resumen

La siguiente tabla resume el comportamiento de todos los formatos de NetScaler si no se aplica una nueva licencia a NetScaler Application Delivery and Management:

Factor de forma	Después de que caduque la licencia	Tras el reinicio de NetScaler
VPX/CAJA	Sigue funcionando hasta que se reinicie	VPX/BLX deja de tener licencia
CPX	Sigue funcionando hasta que se reinicie	CPX se convierte en CPX Express
MPX	Sigue funcionando hasta que se reinicie	MPX deja de tener licencia
SDX	Sigue funcionando hasta que se reinicie	El rendimiento de todos los VPX se reduce a 1 Mbps (lo que los hace inutilizables)

Escenarios de comportamiento de problemas de conectividad

Si se interrumpe la conectividad entre NetScaler y el servidor local de entrega y administración de aplicaciones de NetScaler, el comportamiento es el siguiente:

- NetScaler entra en vigor durante 30 días.
- Durante este período de gracia, la funcionalidad de licenciamiento continúa funcionando hasta el trigésimo día.
- En el trigésimo primer día,
  - NetScaler VPX/NetScaler CPX/NetScaler BLX y NetScaler MPX se reinician forzosamente y dejan de tener licencia.
  - El rendimiento de todos los VPX de NetScaler SDX se reduce a 1 Mbps.

Configure el servidor de entrega y administración de aplicaciones de NetScaler como servidor de licencias flexible o agrupado

January 30, 2024

Como administrador, puede configurar el servidor de entrega y administración de aplicaciones de NetScaler solo como servidor de licencias flexible o agrupado. Con esta configuración, el servidor NetScaler ADM solo recibe datos de licencias de las instancias de NetScaler.

En ocasiones, es posible que tenga un mandato reglamentario que exija restringir los datos de las instancias de NetScaler para que no salgan de la zona reguladora. En tales situaciones, puede implementar una instancia local del servidor local ADM en su zona reguladora para utilizar las capacidades de administración, supervisión y análisis. Si sigue el mismo enfoque para utilizar la función de licencias flexibles o agrupadas, debe dividir las licencias flexibles o agrupadas en varios servidores de licencias NetScaler ADM. Este enfoque no le brinda la flexibilidad de asignar licencias flexibles o agrupadas entre las instancias de NetScaler implementadas en todo el mundo.

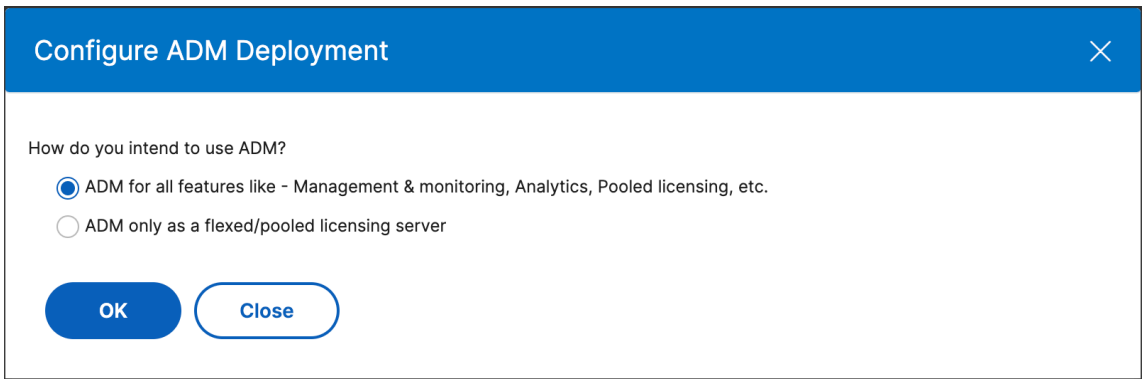
Por lo tanto, configure el servidor NetScaler ADM solo como servidor de licencias Flexed o Pooled. El servidor NetScaler ADM solo recibe datos de licencias de todas las instancias de NetScaler. Por lo tanto, puede cumplir con el mandato reglamentario y asignar de forma dinámica licencias de capacidad flexible o agrupada en todas las instancias de NetScaler implementadas en todo el mundo.

Cómo configurar el servidor NetScaler ADM solo como servidor de licencias Flexed o Pooled

Antes de empezar, asegúrese de que no se haya agregado ninguna instancia de NetScaler al servidor NetScaler ADM. Agregue instancias de NetScaler solo después de completar el paso 4.

Haga lo siguiente para configurar el servidor NetScaler ADM solo para el servidor de licencias Flexed o Pooled:

1. Vaya a **Configuración > Administración**.
2. En la sección **Configuraciones del sistema**, seleccione **Implementación del sistema**.
3. En **ADM Deployment** , seleccione **ADM solo como servidor de licencias flexibles** o agrupadas .



4. Haga clic en **Aceptar**.

   Esta acción conserva solo la función de licencias flexibles o agrupadas y desactiva las siguientes funciones de NetScaler ADM:

   - Respaldo de NetScaler ADM
   - Gestión de eventos
   - Administración de certificados SSL
   - Informes de red
   - Funciones de red
   - Auditoría de configuración

   > **Nota:**
   >
   > De forma predeterminada, la función de análisis de NetScaler ADM está inhabilitada. Asegúrese de inhabilitar esta función si la ha habilitado.

   En el cuadro de confirmación, haga clic en **Sí**.

   La GUI de NetScaler ADM ahora solo muestra la función de licencias flexibles o agrupadas. Y las funciones restantes no aparecen.

5. Después de configurar NetScaler ADM solo para la función de licencias, agregue instancias de NetScaler en la página **Infraestructura > Instancias**.

> **Nota**
>
> - Puede agregar una instancia de NetScaler en uno o varios servidores NetScaler ADM. Al cambiar la contraseña de dichas instancias de NetScaler, asegúrese de actualizar la contraseña en todos los servidores NetScaler ADM en los que se descubra la instancia.
> - Un usuario aún puede realizar algunas operaciones con las funciones inhabilitadas en la GUI de NetScaler ADM. Por ejemplo, el sondeo de eventos y el backup de NetScaler. Como superadministrador, si desea restringir estas operaciones, deshabilite el acceso de los usuarios para otros administradores mediante una política de acceso adecuada. Para

> obtener más información, consulte Configurar directivas de acceso en NetScaler ADM.

Regístrese y compruebe las licencias de NetScaler VPX y NetScaler BLX

January 30, 2024

Puede asignar licencias de NetScaler VPX y NetScaler BLX a instancias de NetScaler bajo demanda desde NetScaler Application Delivery and Management. El software NetScaler ADM almacena y administra las licencias, que tienen un marco de licencias que proporciona un aprovisionamiento de licencias escalable y automatizado. Una instancia puede retirar la licencia de NetScaler ADM cuando se aprovisiona. Cuando se quita o destruye una instancia, la instancia vuelve a comprobar su licencia en el software NetScaler ADM.

Requisitos previos

Asegúrese de que se cumplen los siguientes requisitos previos:

- Está mediante una imagen de NetScaler VPX que ejecuta la versión 12.0 del software.
  Por ejemplo: NSVPX-ESX-12.0-xx.xx_nc.zip
- Ha instalado NetScaler ADM con la versión 12.0.
  Por ejemplo: MAS-ESX-12.0-xx.xx.zip

> **Nota**
>
> Para administrar las licencias de NetScaler VPX existentes mediante NetScaler ADM, debe volver a alojar las licencias en NetScaler ADM.

Instalación de licencias en NetScaler ADM

> **Nota**
>
> Antes de instalar las licencias, reinicie el dispositivo virtual NetScaler 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 NetScaler ADM (por ejemplo, http://192.168.100.1).
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. Vaya a**Infraestructura > Licencias agrupadas**.

4. En la sección **Archivos de licencias**, seleccione una de las siguientes opciones:

   - **Cargue archivos de licencia desde un equipo local**: Si ya hay un archivo de licencia en su equipo local, puede cargarlo en NetScaler ADM.
     Para agregar archivos de licencia, haga clic en **Examinar** y seleccione el archivo de licencia (.lic) que quiera agregar. Luego haga clic en **Finalizar**.
   - **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso a la licencia de las licencias que adquiera.
     Para agregar archivos de licencias, introduzca el código de acceso a la licencia en el cuadro de texto y, a continuación, haga clic en **Obtener licencias**.

   > **Nota**
   >
   > Asegúrese de estar conectado a Internet antes de usar el código de acceso de la licencia para instalarlas.

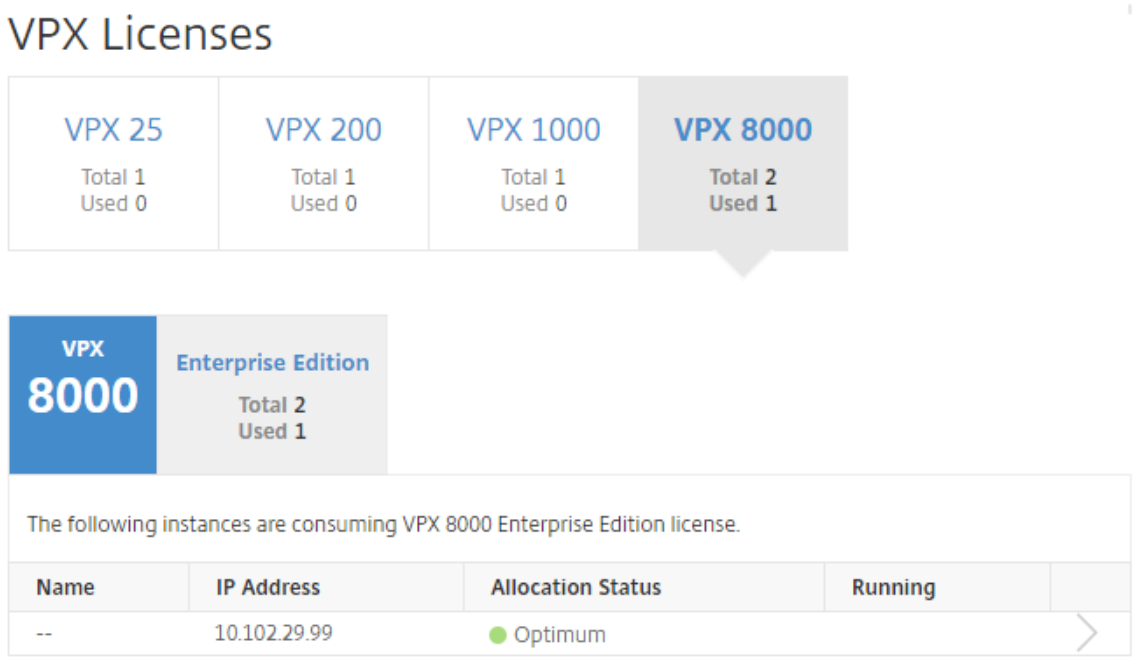
   En cualquier momento, puede agregar más licencias a NetScaler ADM desde la página **Configuración de licencias**.

Verificación

Puede ver las licencias disponibles y asignadas en la GUI de NetScaler ADM.

Para mostrar las licencias:

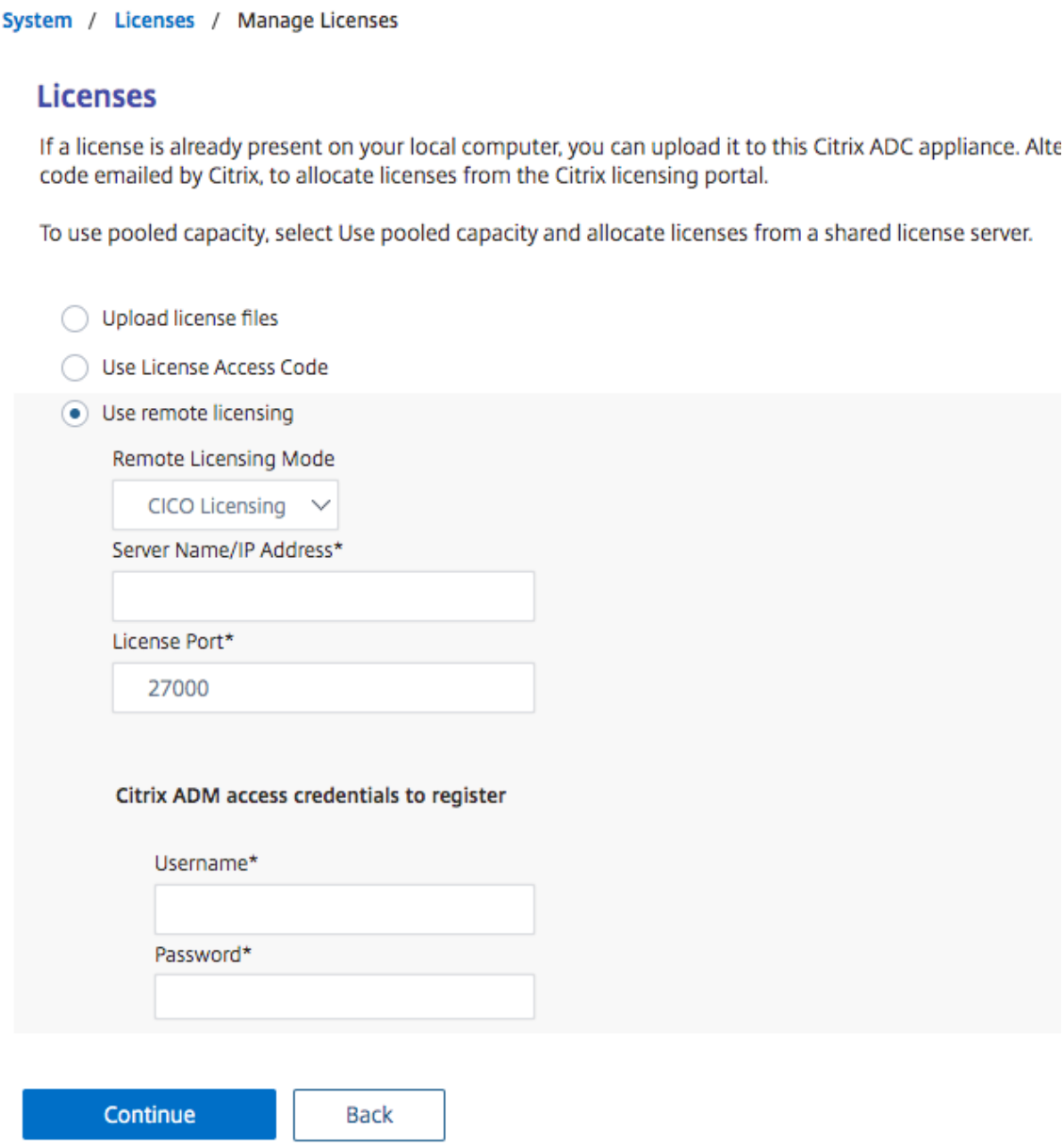
1. En un explorador web, escriba la dirección IP de NetScaler ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha Configuración, vaya a **Infraestructura > Licencias agrupadas > Licencias VPX**.



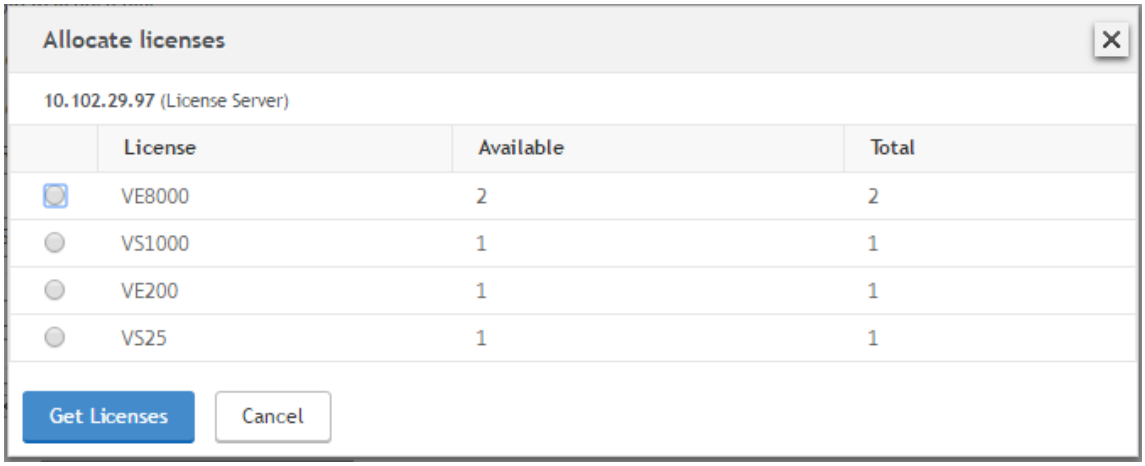
4. Puede ver las licencias asignadas en la tabla de la sección de licencias disponibles.

Asigne licencias de NetScaler VPX y NetScaler BLX a una instancia de NetScaler mediante la GUI de NetScaler

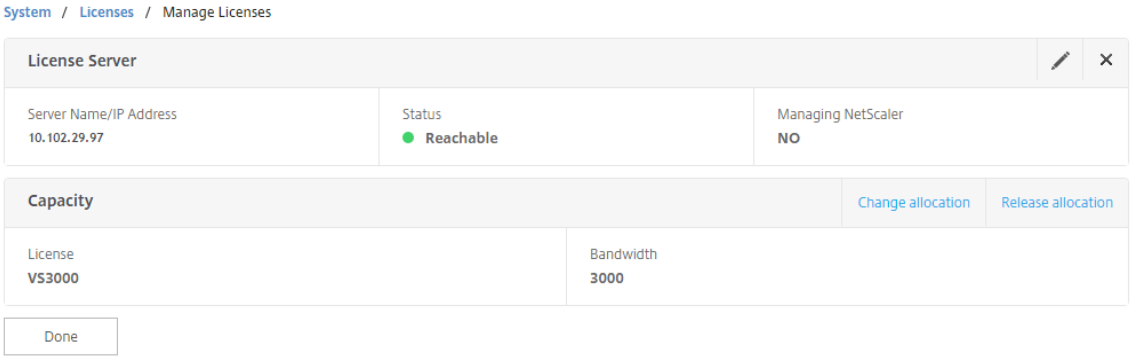
1. En un explorador web, escriba la dirección IP de la instancia de NetScaler (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha Configuración, vaya a **Configuración > Licencias > Administrar licencias**, haga clic en **Agregar nueva licencia**y seleccione **Usar licencias remotas > Licencias de CICO**.
4. Introduzca los detalles del servidor de licencias en el **campo Nombre del servidor/dirección IP**.
5. En **Nombre** de usuario y **contraseña** , introduzca las credenciales de NetScaler ADM y haga clic en **Continuar**.



6. Seleccione la edición de licencia con el ancho de banda requerido, haga clic en **Obtener licencias**.



7. Haga clic en **Reiniciar**, la instancia de NetScaler se reiniciará.
8. Para cambiar o liberar la asignación de licencias, vaya a **Sistema > Licencias > Administrar licencias** y seleccione **Cambiar asignación o Asignación** de **versiones .**



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**.

Asigne licencias de NetScaler VPX y NetScaler BLX a una instancia de NetScaler mediante la CLI de NetScaler

1. En un cliente SSH, introduzca la dirección IP de la instancia de NetScaler e inicie sesión mediante 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, introduzca 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
```

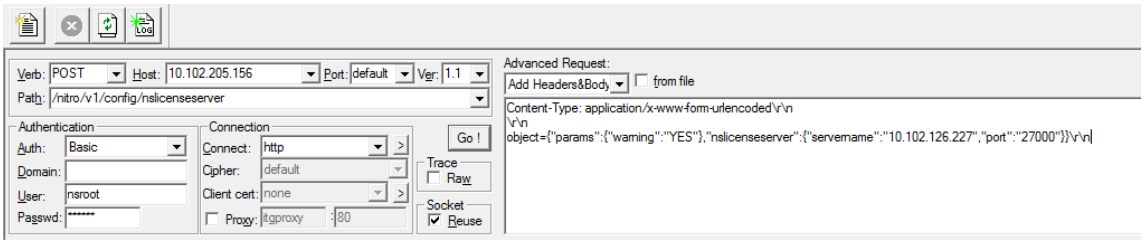
Asigne licencias de NetScaler VPX y NetScaler BLX a una instancia de NetScaler mediante la API

En un explorador web o un cliente de API, inicie sesión en la instancia de NetScaler 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 " : " <NetScaler ADM IP> " , " port " : " 27000 "  }
  }
 \r\n
<!--NeedCopy-->
```

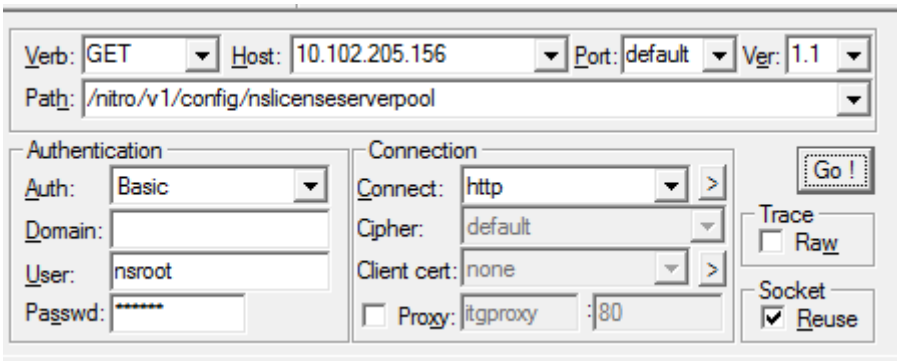


NetScaler ADM responde a la solicitud. La siguiente respuesta muestra éxito.

```
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



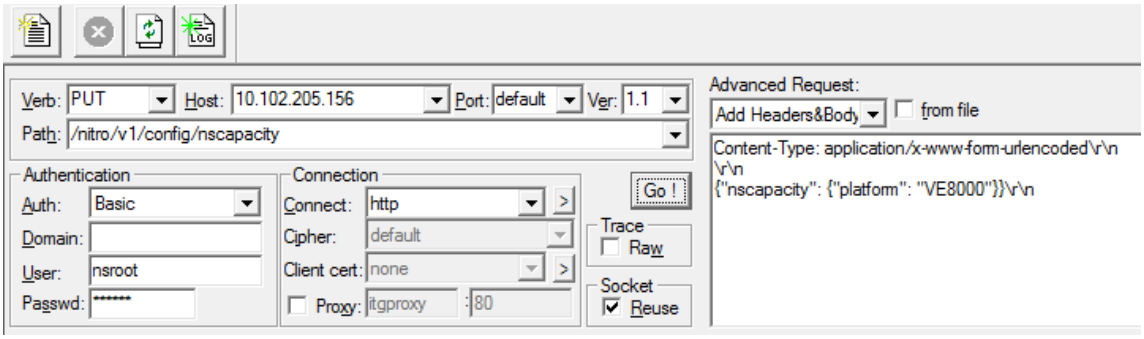
NetScaler ADM responde a la solicitud. La respuesta de ejemplo siguiente muestra el éxito y la lista de licencias disponibles en el servidor de licencias.

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:

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.

Actualizar una dirección IP del servidor de licencias

Puede actualizar la dirección IP del servidor de licencias en las instancias de NetScaler VPX y NetScaler BLX sin que ello afecte al ancho de banda de licencia asignado a la instancia ni a la pérdida de datos.

Actualización mediante la CLI: para actualizar la dirección IP del servidor de licencias mediante la CLI, escriba el siguiente comando en la instancia:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Este comando se conecta al nuevo servidor y libera los recursos asociados al servidor de licencias anterior.

Actualización mediante la GUI: Para actualizar la dirección IP del servidor de licencias mediante la GUI, vaya a **Sistema > Licencias > Administrar licencias** y haga clic en **Agregar nueva licencia**. Para obtener más información, consulte Asignar licencias de NetScaler VPX y NetScaler BLX a una instancia de NetScaler mediante la GUI de NetScaler.

Configure las comprobaciones de caducidad de las licencias de entrada y salida de NetScaler VPX y NetScaler BLX

Ahora puede configurar el umbral de caducidad de las licencias de NetScaler VPX y NetScaler BLX. Al establecer umbrales, NetScaler ADM envía notificaciones por correo electrónico o SMS cuando una licencia caduca. También se envían una captura SNMP y una notificación cuando la licencia ha caducado 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**Infraestructura > Licencias agrupadas**.
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 servidores virtuales o instancias afectadas.
    - **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 para que se utilice para notificar a los administradores.
4. Seleccione el tipo de notificación que desea enviar seleccionando 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 desea enviar la notificación en términos del número de días antes de que caduque la licencia.
6. Haga clic en **Guardar**.

Licencias de CPU virtual NetScaler

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 necesita 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 VPX

Anteriormente, las licencias de NetScaler VPX se asignaban en función del consumo de ancho de banda de las instancias. Un NetScaler 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 escenarios, el requisito de ancho de banda puede ser menor, pero el requisito es mayor para otros rendimientos de L7, como SSL, TPS y rendimiento de compresión. Es posible que la actualización de la licencia NetScaler 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 en función de los requisitos de la CPU virtual.

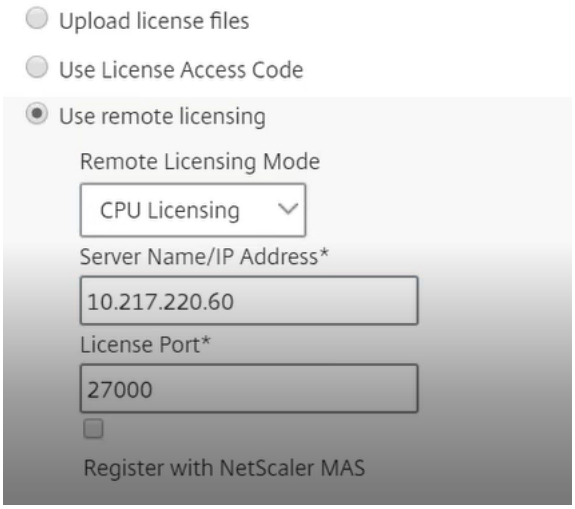
En la función de licencia basada en el uso de CPU virtual, la licencia especifica el número de CPU a las que tiene derecho un NetScaler VPX determinado. Por lo tanto, NetScaler VPX puede desproteger licencias solo para el número de CPU virtuales que se ejecutan en él desde el servidor de licencias. NetScaler VPX extrae licencias en función del número de CPU que se ejecutan en el sistema. NetScaler VPX no considera las CPU inactivas al retirar las licencias.

Al igual que las funcionalidades de licencias agrupadas y CICO, el servidor de licencias ADM de NetScaler administra un conjunto independiente de licencias de CPU virtuales. También en este caso, las tres ediciones gestionadas para las licencias de CPU virtuales son Standard, Advanced y Premium. 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. Reinicie NetScaler VPX después de retirar las licencias.

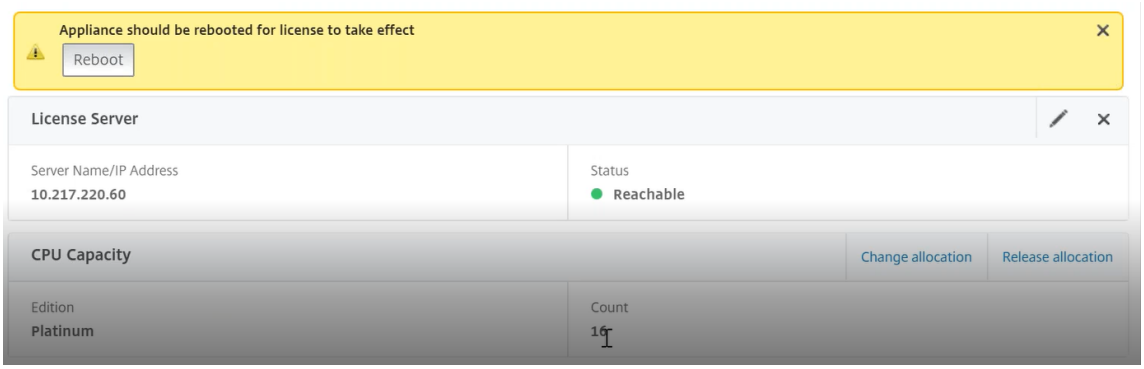
Para configurar el servidor de licencias en NetScaler VPX mediante GUI:

1. En NetScaler 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 VPX con NetScaler ADM. Si aún no lo ha hecho, active **Registrar 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 la licencia.



> **Nota**También
>
> puede liberar la licencia actual y salir de una edición diferente. Por ejemplo, ya tiene una licencia de edición estándar en su instancia. Puede liberar esa licencia y luego echar un vistazo a la edición avanzada.

Configuración de un servidor de licencias en la licencia de NetScaler VPX mediante la CLI

En la consola NetScaler VPX, escriba los siguientes comandos para las dos tareas siguientes:

1. Para agregar el servidor de licencias al NetScaler VPX:

```
add licenseserver <IP address of the license server>
<!--NeedCopy-->
```

2. Para solicitar las licencias:

```
set capacity -vcpu - edition premium
<!--NeedCopy-->
```

   Cuando se le solicite, reinicie la instancia escribiendo el siguiente comando:

```
reboot -w
<!--NeedCopy-->
```

Actualizar una dirección IP del servidor de licencias

Puede actualizar la dirección IP del servidor de licencias en la instancia de NetScaler VPX sin que ello afecte al ancho de banda de licencia asignado a la instancia ni a la pérdida de datos. Para actualizar la dirección IP del servidor de licencias, escriba el siguiente comando en la instancia de NetScaler VPX:

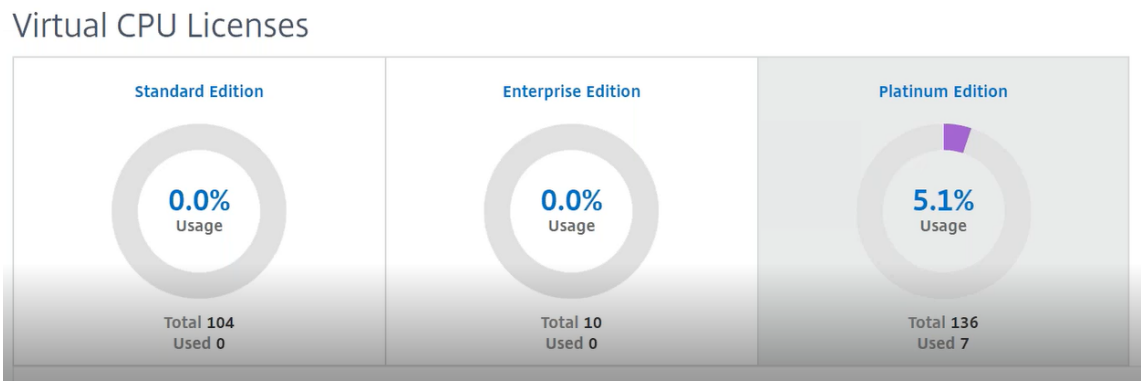
```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Este comando se conecta al nuevo servidor y libera los recursos asociados al servidor de licencias anterior.

Administración de licencias de CPU virtual en NetScaler ADM

1. En NetScaler ADM, vaya a **Infraestructura > Licencias agrupadas > VCPU agrupadas**.
2. La página muestra las licencias asignadas para cada tipo de edición de licencia.

3. Haga clic en el número que aparece dentro de cada anillo para ver las instancias de NetScaler que utilizan esta licencia.



Licencias de CPU virtual para NetScaler CPX

Al aprovisionar la instancia CPX de NetScaler, puede configurar la instancia CPX de NetScaler para que extraiga las licencias del servidor de licencias en función del uso de la CPU de la instancia.

NetScaler CPX depende del servidor de licencias, que se ejecuta en NetScaler ADM, para administrar las licencias. NetScaler 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 CPX.

Puede descargar la imagen CPX de NetScaler del registro de contenedores de Quay mediante el comando "docker pull"e implementarla en su entorno.

Hay tres tipos de licencia disponibles para las licencias de NetScaler CPX:

1. Licencias de suscripción a CPU virtuales compatibles con NetScaler CPX y VPX
2. Licencias de capacidad agrupada
3. Licencias CP1000 que admiten una o varias vCPU solo para NetScaler CPX

Para configurar licencias de suscripción de vCPU al Provisioning la instancia CPX de NetScaler:

Especifique la cantidad de licencias de vCPU que utiliza la instancia CPX de NetScaler.

- 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 NetScaler CPX puede admitir de 1 a 16 núcleos.

Para especificar 2 núcleos, puede ejecutar el comando docker run de la siguiente manera:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```


Al aprovisionar una instancia CPX de NetScaler, defina el servidor de licencias de NetScaler 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.
- <*LS_PORT*> es el puerto del servidor de licencias NetScaler. De forma predeterminada, el puerto es 27000.

> **Nota**De forma
>
> predeterminada, la instancia de NetScaler CPX extrae la licencia del grupo de suscripciones de vCPU. La instancia CPX de NetScaler comprueba un número «n» de licencias si la instancia se ejecuta con «n» CPU.

Para configurar la capacidad agrupada de NetScaler o las licencias CP1000 mientras se aprovisiona la instancia de NetScaler CPX:

Si desea comprobar la licencia de la instancia de NetScaler CPX mediante las licencias agrupadas (basadas en el ancho de banda) o el grupo privado de NetScaler CPX (CP1000 o basado en grupos privados), 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 activa la extracción desde el grupo CP1000 (grupo privado de NetScaler CPX). A continuación, la instancia CPX de NetScaler recupera un 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 NetScaler 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 Premium, pero permite que NetScaler CPX ejecute hasta 2000 Mbps. En las licencias agrupadas, no se cobran los primeros 1000 Mbps.

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 la configuración del sistema

January 30, 2024

En la siguiente tabla se describe la lista de opciones disponibles en **Configuración** > **Administración**:

Configuraciones de red

Configuraciones de red	Opciones	Descripción
Dirección IP, segunda NIC, nombre de host y servidor proxy	Dirección IP	Muestra los detalles de la dirección IP de configuración de red de NetScaler ADM que se utilizan para implementar NetScaler ADM

Configuraciones de red	Opciones	Descripción
	Segunda NIC	Permite configurar una segunda NIC para aislar el acceso de administración de NetScaler ADM. Para obtener más información, consulte Configurar una NIC doble para acceder a NetScaler ADM
	Nombre de host	Permite asignar un nombre de host a NetScaler ADM. Para obtener más información, consulte Asignar un nombre de host a un servidor NetScaler ADM
	Servidor proxy	Permite configurar ADM como servidor proxy. Para obtener más información, consulte NetScaler ADM como servidor proxy de API
Rutas estáticas		Le permite configurar rutas estáticas para establecer una conexión entre las instancias de NetScaler ADM y NetScaler VPX
Servidores NTP		Garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red. Para obtener más información, consulte Configurar el servidor NTP
Información de puertos ADM		Le permite comprender qué puerto debe estar abierto para la comunicación entre las instancias ADM y ADC. Para obtener más información, consulte Puertos compatibles

Configuraciones del sistema

Configuraciones del sistema	Opciones	Descripción
Sistema, zona horaria, URL permitidas y mensaje del día	Parámetros básicos	Permite modificar la configuración del sistema, como habilitar el inicio de sesión de `nsrecover`, habilitar el tiempo de espera de sesión, etc.
	Zona horaria	Le permite modificar la zona horaria que se utilizará en NetScaler ADM. La zona horaria predeterminada es UTC
	Lista de URL permitidas	Permite configurar direcciones URL para enviar solicitudes ininterrumpidas a ADM. Puede configurarlo con el valor "none" si no se agregará ninguna URL
	Mensaje del día	Le permite crear un mensaje de bienvenida en NetScaler ADM. Puede utilizar esta función para establecer mensajes de recordatorio para usted o para el usuario que inicia sesión en NetScaler ADM. Haga clic en **Habilitar mensaje**, escriba el mensaje en el cuadro de mensajes y haga clic en **Guardar**
Ver huella digital de ADM		Le permite copiar el identificador de huella digital único de NetScaler ADM para empezar con el gráfico de servicios

Configuraciones del sistema	Opciones	Descripción
Configurar la identidad del cliente		Permite proteger los recursos de red al permitir que solo los clientes o usuarios autenticados accedan a su red. Para obtener más información, consulte Gobierno de datos
Configuración de CUXIP		Si selecciona esta casilla de verificación, las estadísticas de uso se recopilan con el único propósito de mejorar la GUI. Los datos recibidos solo los utilizan los ingenieros de Citrix y no se comparten con nadie

Mantenimiento del sistema

Mantenimiento del sistema	Descripción
Actualizar NetScaler ADM	Permite actualizar NetScaler ADM a través de GUI. Para obtener más información, consulte Actualización
Reinicie NetScaler ADM	Le permite reiniciar NetScaler ADM
Cierre NetScaler ADM	Le permite cerrar NetScaler ADM
Recuperación ante desastres	Permite ver la información del nodo de recuperación ante desastres. Para obtener más información, consulte Configurar la recuperación ante desastres

Poda de datos

Poda de datos	Opciones	Descripción
Reproducción de datos de sistemas e instancias	Sistema	Permite limitar la cantidad de datos de informes que se almacenan en la base de datos del servidor NetScaler ADM. Para obtener más información, consulte Configurar los ajustes de poda del sistema
	Eventos de instancia	Le permite limitar los mensajes de eventos que informan los datos almacenados en NetScaler ADM
	Syslog de instancia	Permite limitar la cantidad de datos de syslog almacenados en la base de datos. Para obtener más información, consulte Configurar los ajustes de syslog prune de instancia
	Informes de red	Le permite limitar los datos de informes de red almacenados en NetScaler ADM

Backup

Backup	Opciones	Descripción
Configurar la copia de seguridad del sistema y de la instancia	Sistema	Permite configurar la configuración inicial de la copia de seguridad antes de realizar una copia de seguridad del sistema. Para obtener más información, consulte Configuración de respaldo del sistema

Backup	Opciones	Descripción
	Instancia	Permite configurar opciones en NetScaler ADM para realizar copias de seguridad de una instancia de NetScaler seleccionada o varias instancias. Para obtener más información, consulte Configurar los ajustes de respaldo de instancias

Notificaciones de eventos

Notificaciones de eventos	Opciones	Descripción
Configurar la notificación y el resumen de eventos	Notificación de eventos	Puede enviar notificaciones a grupos de usuarios seleccionados para varias 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, SMS o Slack. Esto garantiza que se le notifique cualquier actividad a nivel del sistema, como el exceso de almacenamiento de datos o un error de respaldo.

	Resumen del evento	Le permite obtener un informe consolidado de los eventos importantes del sistema y las funciones

Configuración SSL

Configuración SSL	Descripción
Instalar certificado SSL	Le permite instalar el certificado SSL y el archivo de clave SSL
Ver certificado SSL	Le permite ver los detalles del certificado SSL
Configuración de SSL	Para obtener más información, consulte Configurar los ajustes de SSL
Certificados SSL	Le permite cargar, descargar o eliminar un certificado SSL o un archivo de clave SSL
Grupos de cifrado	Para obtener más información, consulte Configurar grupos de cifrado

Configurar funciones

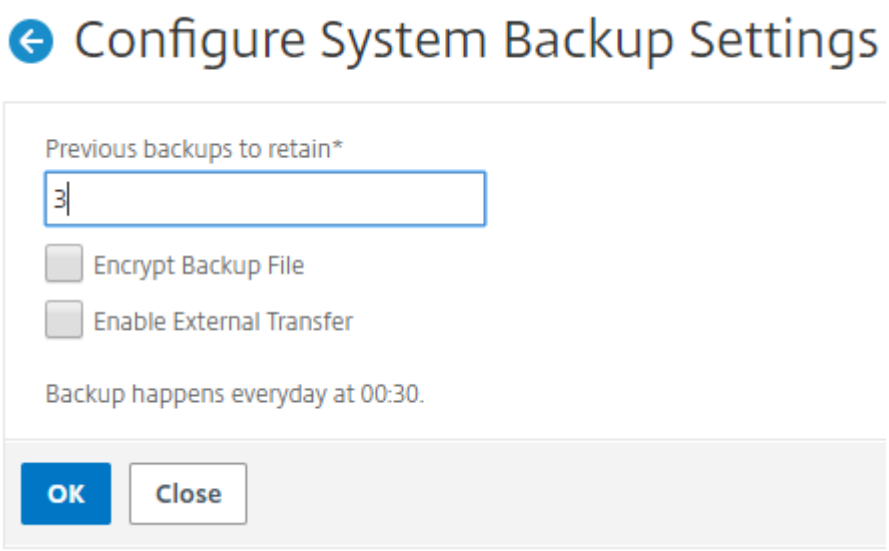
Configurar funciones	Descripción
Habilitar o inhabilitar funciones	Puede habilitar o inhabilitar funciones en NetScaler ADM. Para obtener más información, consulte Habilitar o inhabilitar las funciones de ADM

Configurar las opciones de copia de seguridad del sistema

January 30, 2024

Establezca la configuración inicial de copia de seguridad del sistema antes de que necesite realizar una copia de seguridad y restaurar el sistema NetScaler Application Delivery Management (ADM).

1. Vaya a **Configuración > Administración** . En Copia de **seguridad** , haga clic en **Configurar copia de seguridad del sistema y de la instancia** .
2. En la página **Copia de seguridad > Sistema**, especifique lo siguiente:
   - Copias de seguridad anteriores para conservar. Solo puede retener hasta 10 copias de seguridad.
   - Seleccione **Cifrar archivo de copia de seguridad** para cifrar los archivos de copia de seguridad.
   - Seleccione **Habilitar transferencia externa** para transferir una copia del archivo de respaldo a otro sistema. Cuando desee restaurar la configuración, primero debe cargar el archivo en el servidor NetScaler 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, consulteTransferir un archivo de copia de seguridad de NetScaler ADM a un sistema externo.
3. Haga clic en **Aceptar**.



Configurar un servidor NTP

January 30, 2024

Puede configurar un servidor de Network Time Protocol (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 **Configuración > 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 quiere que el intervalo mínimo de sondeo sea de 64 segundos, que se puede expresar como 2^6, escriba 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 **Configuración > 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.

Actualice NetScaler Application Delivery Management (ADM)

January 30, 2024

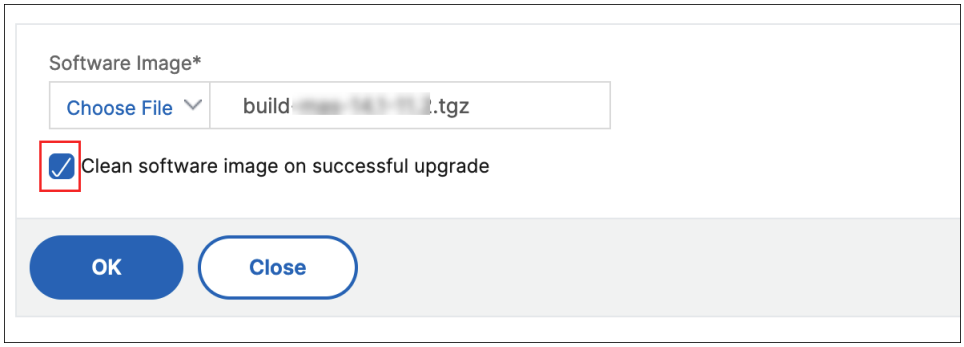
Cada versión de NetScaler ADM ofrece funciones nuevas y actualizadas con mayor funcionalidad. En las notas de la versión que acompañan al anuncio de la versión se incluye una lista completa de mejoras. Tómese un momento para leer las notas de la versión antes de actualizar el software. Es importante entender el marco de licencias y los tipos de licencias antes de empezar a actualizar.

Para actualizar NetScaler ADM:

1. Vaya a **Configuración > Administración**. En **Mantenimiento del sistema**, haga clic en **Actualizar NetScaler ADM**.
2. En la página Actualizar NetScaler ADM, cargue un nuevo archivo de imagen seleccionando **Local** (su equipo local) o **Dispositivo**.

   > **Nota**
   >
   > Al seleccionar **Appliance**, asegúrese de que la imagen de actualización esté disponible en `/var/mps/mps_images` en NetScaler ADM.

   De formapredeterminada, la imagen de software se limpia después de una actualización correcta.
3. Haga clic en **Aceptar**.



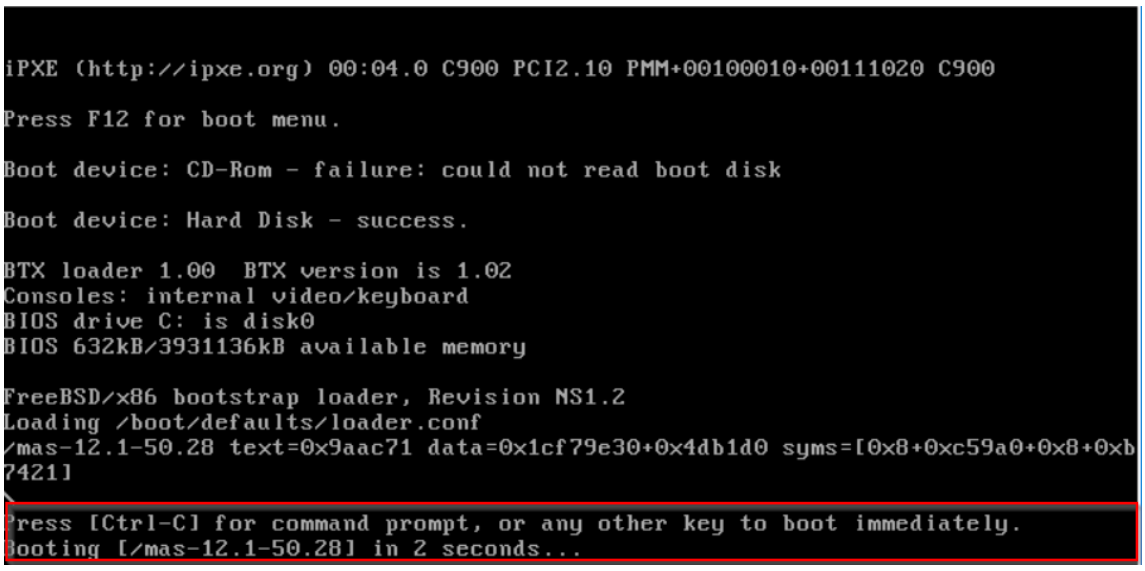
Cómo restablecer la contraseña para NetScaler ADM

January 30, 2024

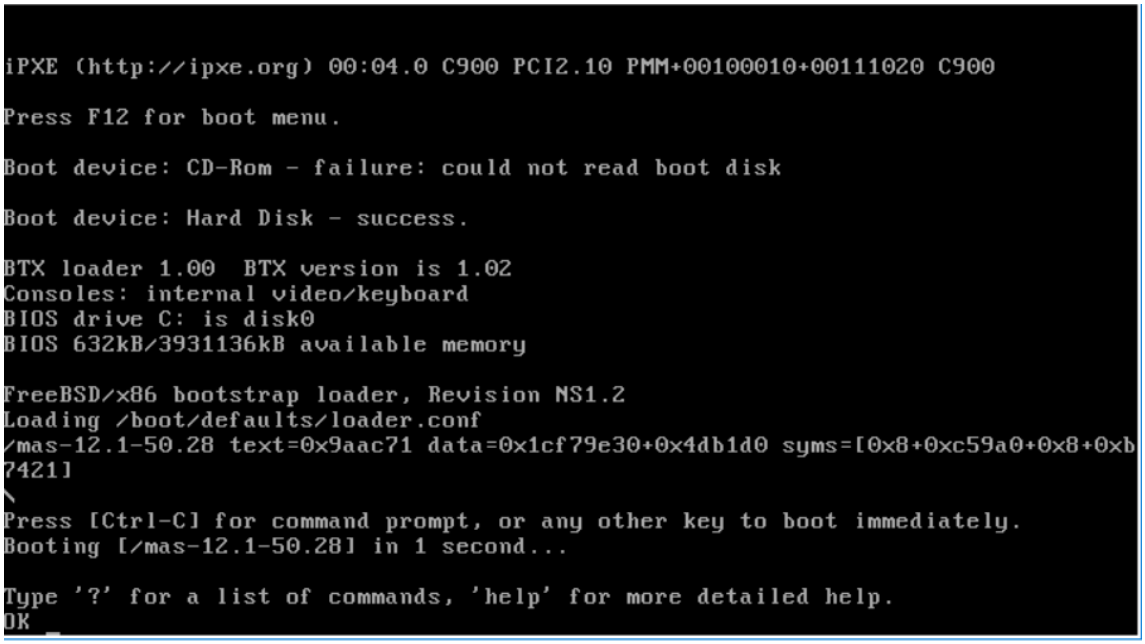
El procedimiento para restablecer la contraseña de NetScaler ADM puede diferir en los hipervisores en los que está alojado. Si ha cambiado la contraseña predeterminada y quiere restablecerla, puede restablecer la contraseña reiniciando el nodo ADM de NetScaler.

Citrix Hypervisor con XenCenter:

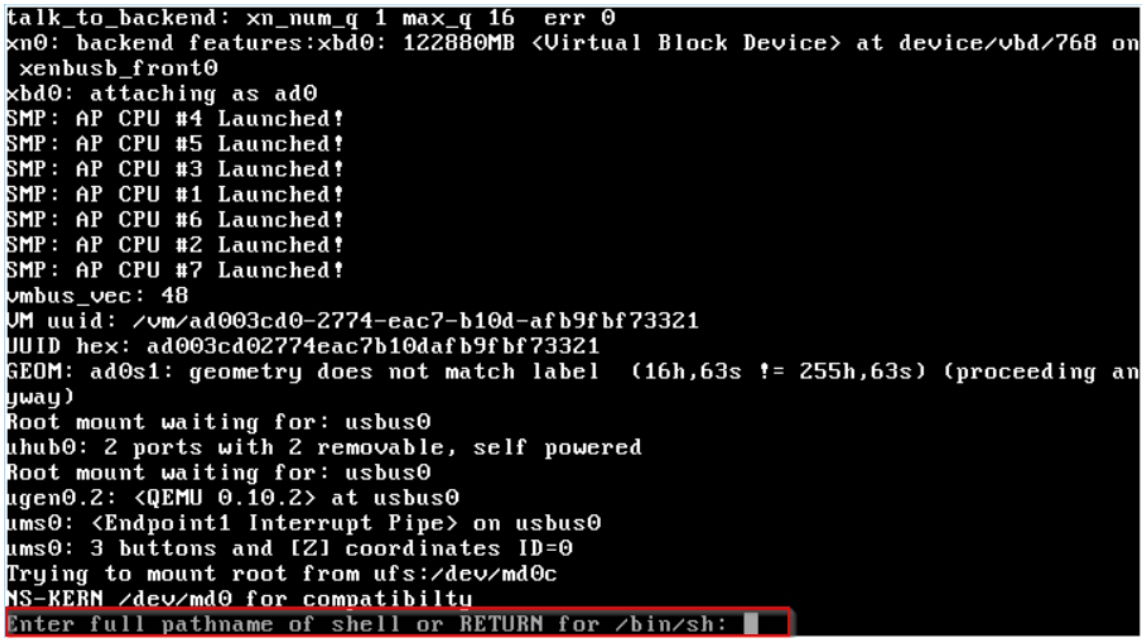
1. Inicie sesión en Citrix Hypervisor mediante XenCenter.
2. Seleccione el nodo NetScaler ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.



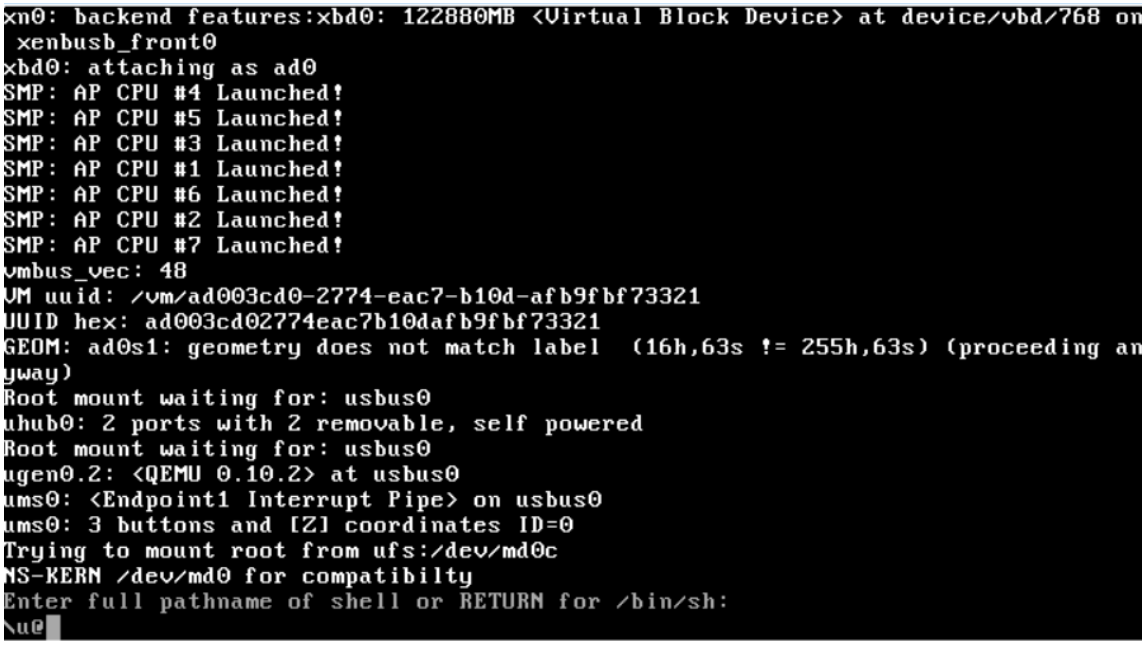
4. Ejecute el comando **boot -s** en la línea de comandos OK.



NetScaler ADM se reinicia y muestra el siguiente mensaje:

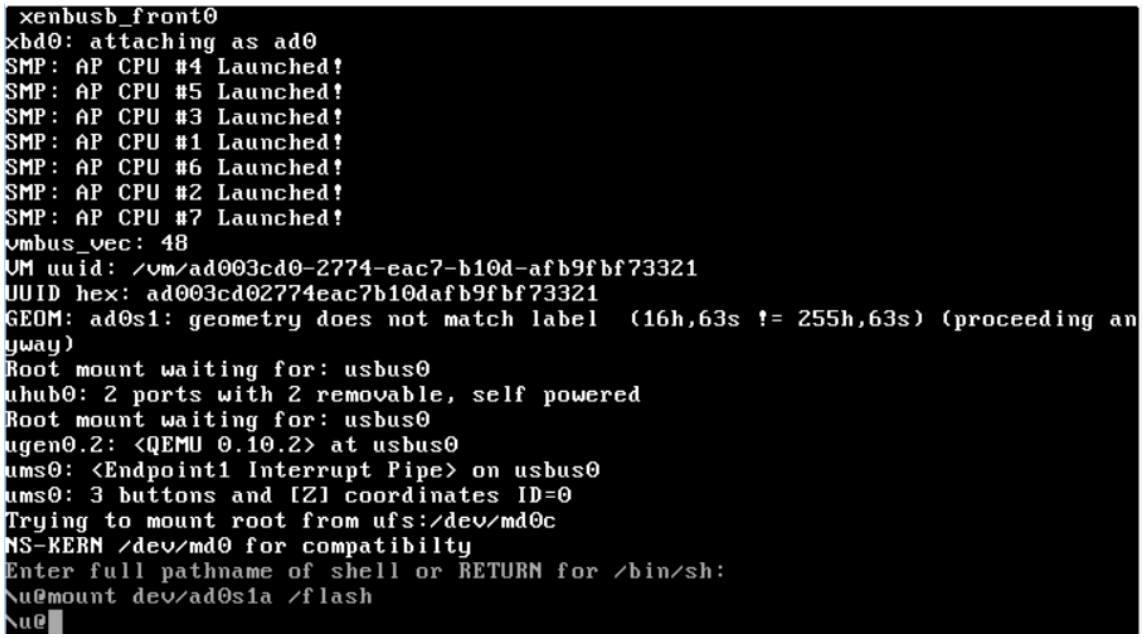


5. Presiona **Entrar** para que aparezca el mensaje /u @.



6. Monte la partición flash con el siguiente comando:

   ```
   mount /dev/da0s1a /flash
   ```



7. Cree un archivo con el siguiente comando:

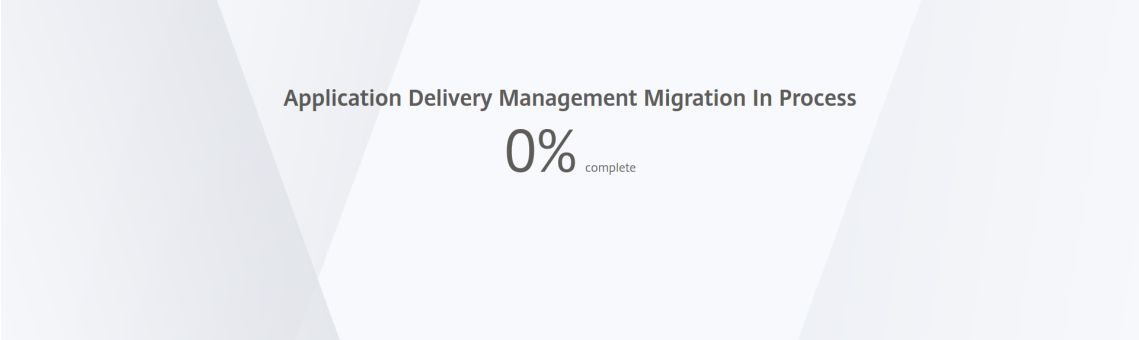
   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.

8. Ejecute el comando **Reboot** para reiniciar NetScaler ADM.


```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@touch /flash/mpsconfig/.recover
\u@reboot
```

9. Acceda a la GUI de NetScaler ADM y espere hasta que se complete el reinicio.



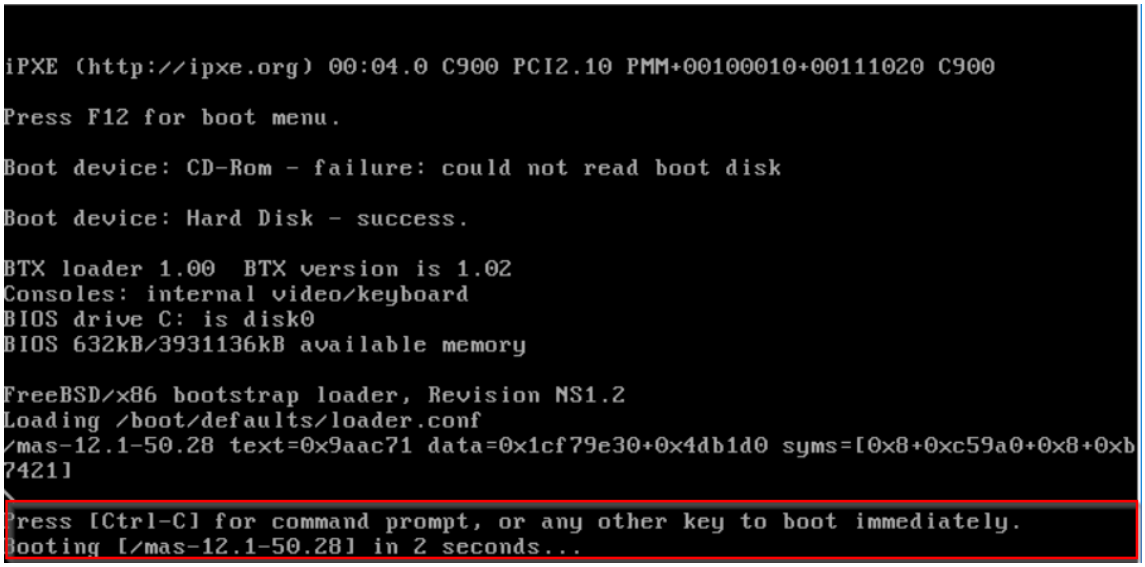
Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el Hypervisor.

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Esx mediante vSphere:

1. Inicie sesión en ESX con vSphere.
2. Seleccione el nodo NetScaler 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 NetScaler 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
   ```

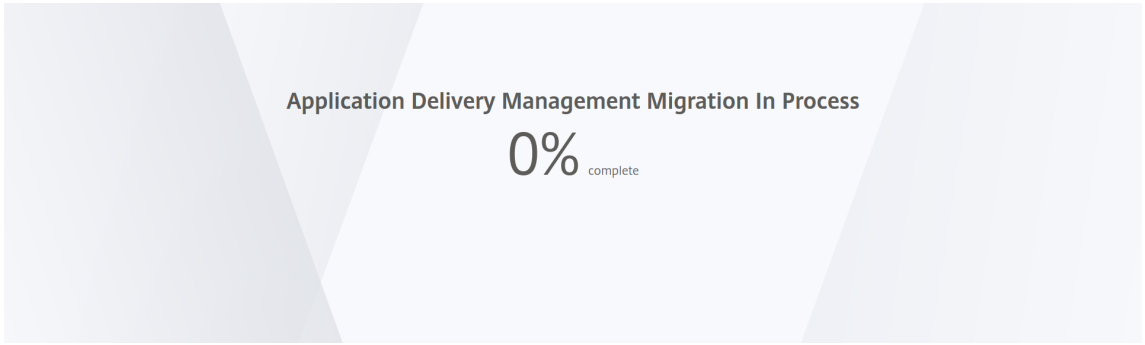
7. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.

8. Ejecute el comando **Reboot** para reiniciar NetScaler ADM.

9. Acceda a la GUI de NetScaler ADM y espere hasta que se complete el reinicio.

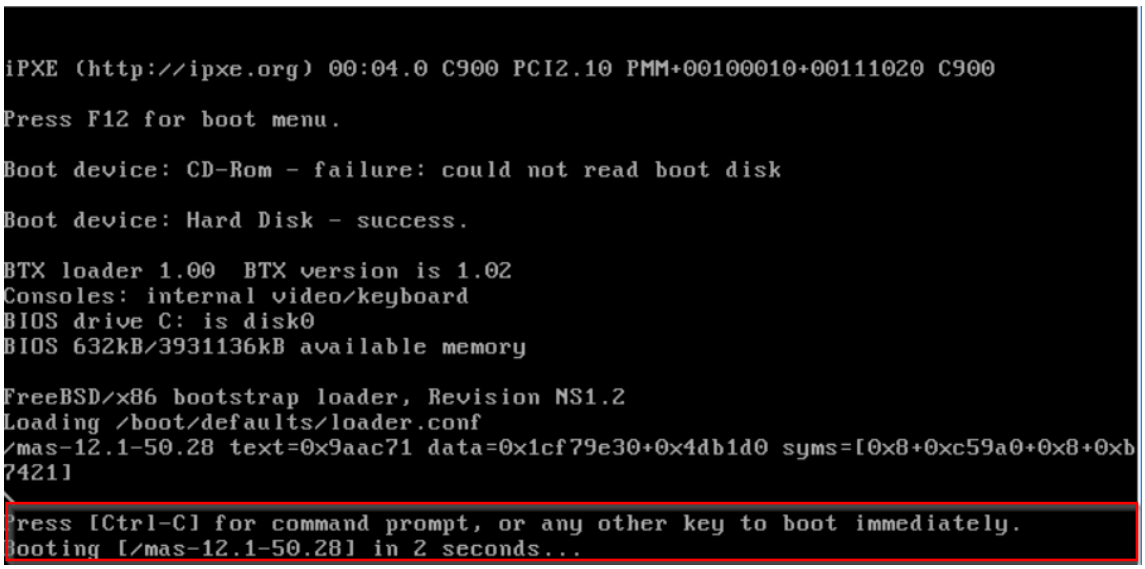


   Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el servidor ESX.

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Hyper-V mediante el administrador Hyper-V:

1. Inicie sesión en hyper-v con el administrador de hyper-v.
2. Seleccione el nodo NetScaler 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.

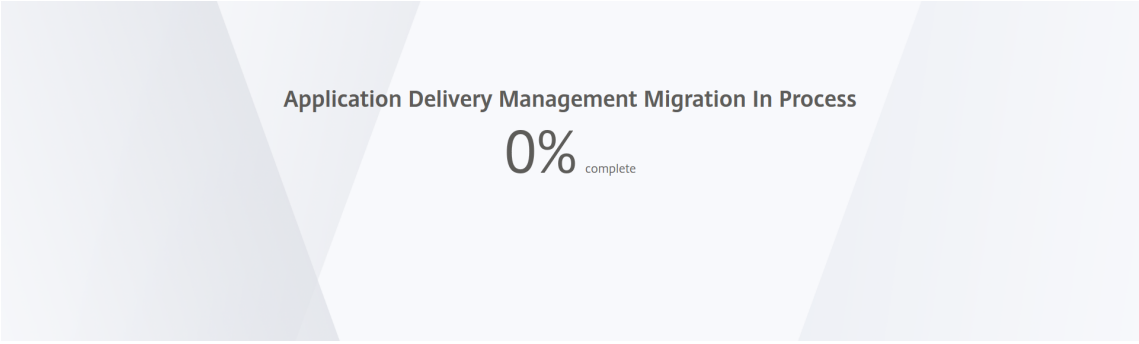
   El NetScaler ADM se reinicia.
5. Presiona **Entrar** para que aparezca el mensaje /u @.
6. Monte la partición flash con el siguiente comando:

   `mount dev/ad0s1a /flash`
7. Cree un archivo con el siguiente comando:

   `touch /flash/mpsconfig/.recover`

   La contraseña ahora se restablece a la contraseña predeterminada.
8. Ejecute el comando **Reboot** para reiniciar NetScaler ADM.

9. Acceda a la GUI de NetScaler 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.

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Servidor KVM Linux (SSH a servidor KVM mediante cualquier cliente SSH):

1. Inicie sesión en NetScaler ADM mediante un cliente SSH en el servidor KVM.
2. Reinicie NetScaler 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 NetScaler 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:

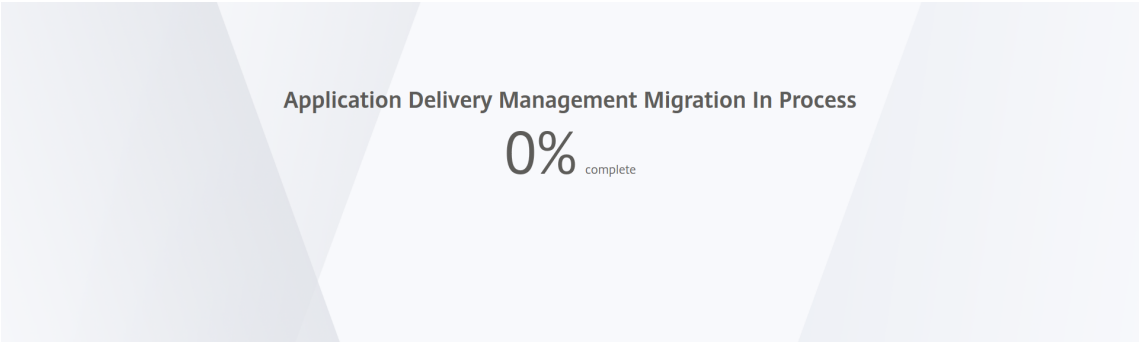
   ```
   mount dev/vtbd0s1a /flash
   ```

8. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.

9. Ejecute el comando **Reboot** para reiniciar NetScaler ADM.
10. Acceda a la GUI de NetScaler 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.

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie NetScaler ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

Configurar una NIC secundaria para acceder a NetScaler ADM

January 30, 2024

Puede configurar una segunda NIC para aislar el acceso de administración a NetScaler ADM. Con esta segunda función de NIC, según sus necesidades, puede elegir cómo desea aislar el tráfico que se recibe y se envía a través del ADM de NetScaler.

Considere un caso en el que desee aislar el tráfico para:

- Tenga todas las comunicaciones entre NetScaler ADM y sus instancias de NetScaler administradas en una sola red.
- Tenga acceso de administración a NetScaler ADM en otra red.

En este caso, como administrador, puede:

- Configure una dirección IP para el tráfico entre NetScaler ADM y sus instancias administradas de NetScaler.

- Configure otra dirección IP para administrar el software NetScaler ADM a fin de realizar todas las tareas administrativas del software.

> **Nota**
>
> Si NetScaler ADM está configurado como un par de HA, la dirección IP de administración configurada en la segunda NIC se asocia al nodo principal.

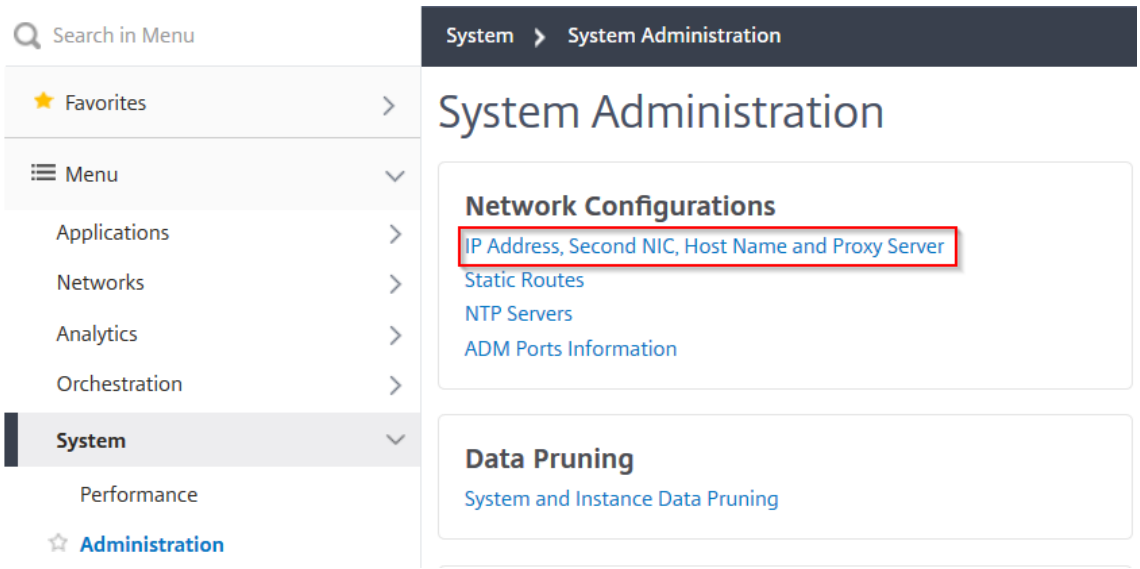
Requisitos previos

- Asegúrese de haber implementado y configurado **NetScaler ADM 13.0 Build 47.x o posterior** en el hipervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM o VMware ESXi).
- Asegúrese de haber agregado la segunda NIC al hipervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM o VMware ESXi).

Para asignar una dirección IP a una NIC en un hipervisor de Citrix y crear una interfaz secundaria, consulte Asignar una dirección IP a una NIC.

Configurar una segunda NIC en NetScaler ADM

1. Inicie sesión en ADM GUI.
2. Vaya a **Configuración > Administración**.
3. En **Configuración de red**, haga clic en **Dirección IP, Segunda NIC, Nombre de host y Servidor proxy**.



Aparece la página de configuración de red.

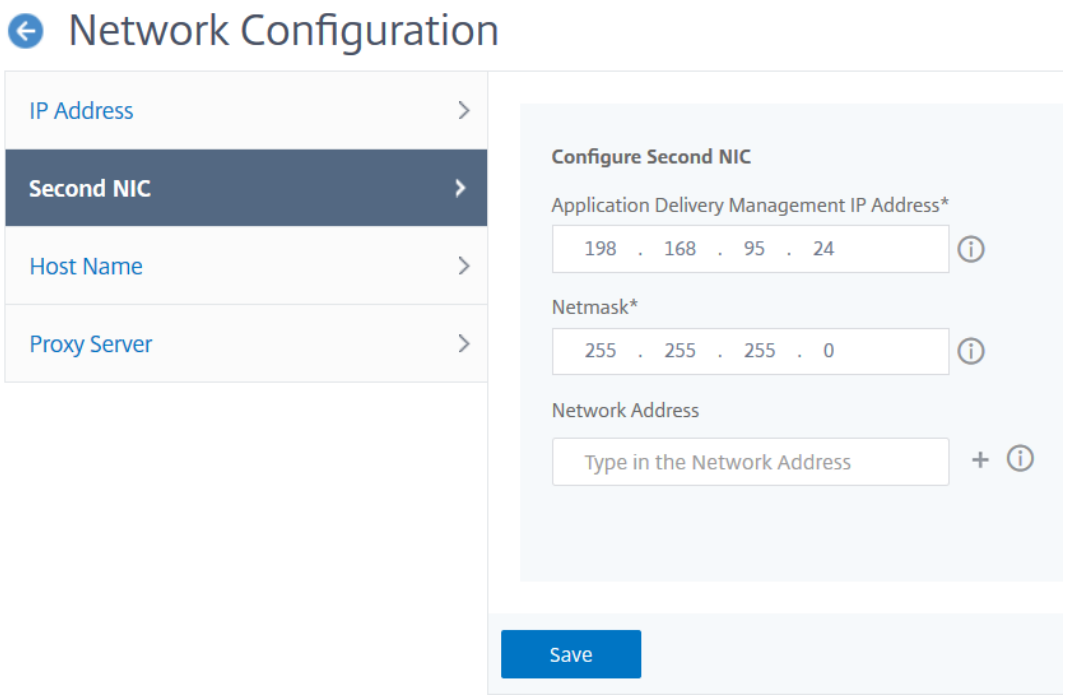
4. Haga clic en la ficha Segunda NIC y configure los siguientes parámetros:

   a) **Dirección IP de administración de entrega de aplicaciones: introduzca una dirección** IP válida para acceder a NetScaler ADM. Puede usar esta dirección IP para acceder a NetScaler ADM, además de la dirección IP de administración existente.

   b) **Máscara de red**: Introduzca la dirección de máscara de red para especificar el host de la red. La dirección predeterminada es 255.255.255.0.

   c) **Dirección de red**: Introduzca una dirección IP para agregar una entrada de ruta para NetScaler ADM. Haga clic en **+** para agregar más direcciones IP. Este campo es opcional.

   d) Haga clic en **Guardar**.



Configurar una NIC secundaria para acceder al agente ADM

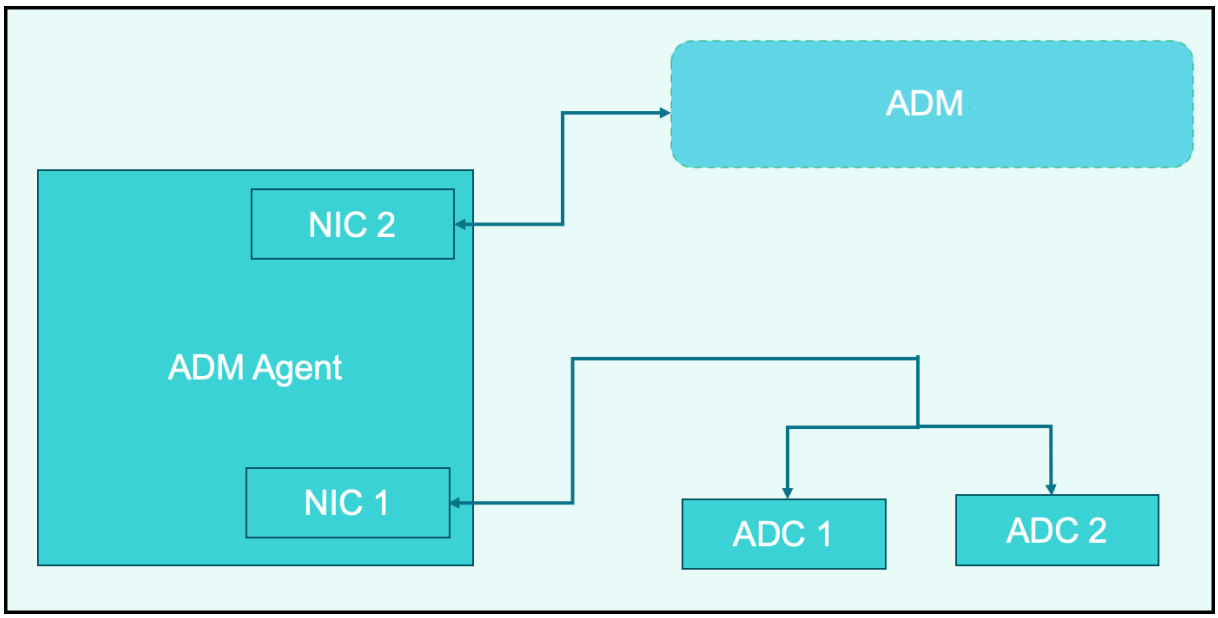
January 30, 2024

Puede configurar dos NIC en un agente de ADM. Mediante la arquitectura de NIC dual, el agente ADM podrá:

- Establezca la comunicación entre el agente de ADM y las instancias de ADC: puede usar la primera NIC para aislar el tráfico que se recibe y envía a través del ADM de Citrix y también para comunicarse entre NetScaler ADM y sus instancias de NetScaler administradas en otra red.

- Establezca la comunicación entre el agente ADM y NetScaler ADM: puede utilizar la segunda NIC para administrar el ADM de NetScaler que está en una red y realizar tareas administrativas

> **Nota**
>
> No puede intercambiar la funcionalidad y la configuración de ambas NIC.



En este caso, como administrador, puede:

- Configure la dirección IP para el tráfico entre NetScaler ADM y sus instancias de NetScaler administradas.
- Configure la dirección IP para administrar el software NetScaler ADM para realizar todas las tareas administrativas del software.

> **Nota**
>
> No es obligatorio configurar dos NIC para un agente de ADM. Es opcional y solo se requiere cuando es necesario separar el tráfico entre el agente ADM, NetScaler ADM y los ADC.

Modifique las direcciones de red NIC IPV4 mediante la CLI

1. Abra una conexión SSH a la consola del agente NetScaler ADM mediante un cliente SSH, como PuTTY.
2. Inicie sesión con las credenciales de **nsrecover/nsroot** y cambie a la línea de comandos de la consola.
3. Ejecute el comando **ifconfig**. Puede ver los detalles de las dos NIC que ha configurado:

- NIC 1: para la comunicación entre el agente de ADM y la comunicación de ADC
- NIC 2: para la comunicación entre ADM Agent y NetScaler ADM

```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Ejecute el comando **networkconfig**. Aparece un menú que le permite configurar o modificar las direcciones de red IPV4.

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
     1. Citrix ADM Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```

> **Nota**
>
> La segunda dirección de red NIC puede tomar varios valores de IP.

5. Seleccione un elemento del menú que quiera modificar. Guarde y cierre la configuración.

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 de Syslog, que se ejecuta en la instancia de Citrix Application Delivery Controller (ADC), y el servidor Syslog, que puede ejecutarse en el sistema operativo (SO) FreeBSD subyacente de la instancia de NetScaler 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.

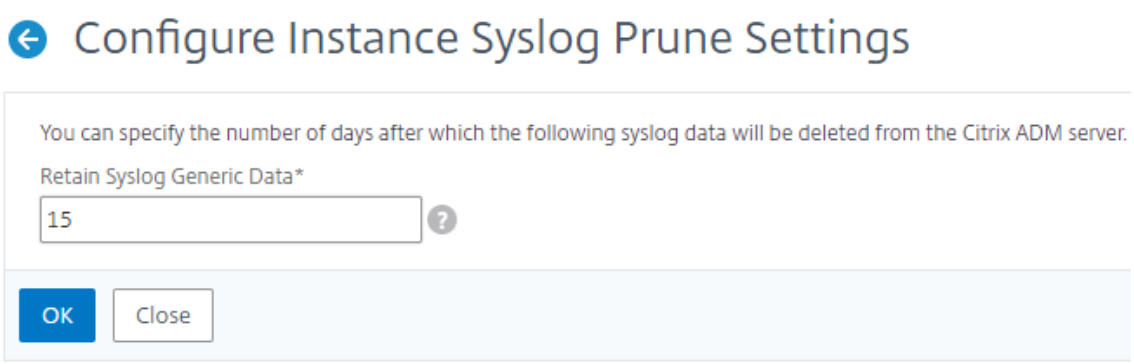
Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que desea eliminar los datos de syslog.Puede especificar el número de días después de los cuales se eliminarán los siguientes datos de syslog de NetScaler Application Delivery Management (ADM):

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

También puede configurar el intervalo de poda de NetScaler Gateway por tipo de syslog. Este intervalo de poda tiene prioridad sobre el intervalo de runas configurado para conservar los datos de NetScaler Gateway.

Para configurar la configuración del intervalo de poda de syslog para NetScaler ADM:

1. Vaya a **Configuración > Administración**.En **Poda de datos**, haga clic en **Poda de datos de sistema e instancia y, a** continuación, haga clic en **Syslog de instancia**.
2. En la página **Configurar la configuración de Syslog Prune de la instancia**, especifique **Conservar datos genéricos de Syslog (días).** Escriba el número de días durante los cuales NetScaler ADM retiene mensajes genéricos de syslog.



Configurar los parámetros de poda del sistema y de poda de eventos

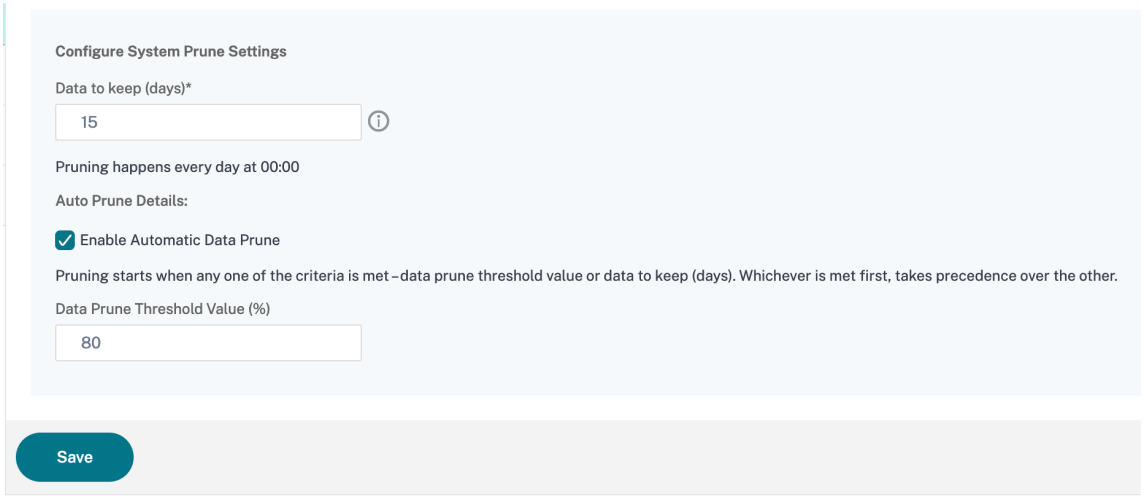
January 30, 2024

Para limitar la cantidad de datos de informes que se almacenan en la base de datos de software NetScaler Application Delivery Management (ADM), puede recortarlos. 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 ser superior a 30 días ni inferior a 15 días.

Para configurar los ajustes de poda del sistema para los informes de rendimiento:

1. Vaya a **Configuración** > **Administración** . En**Reproducción de datos**, haga clic en**Reproducción de datos del sistema y de la instancia**.
2. En la página**Configurar los parámetros de purga del sistema**, especifique lo siguiente:
   - Días para conservar los datos
   - Porcentaje de espacio en disco (umbral de purga)
3. Haga clic en **Aceptar**.



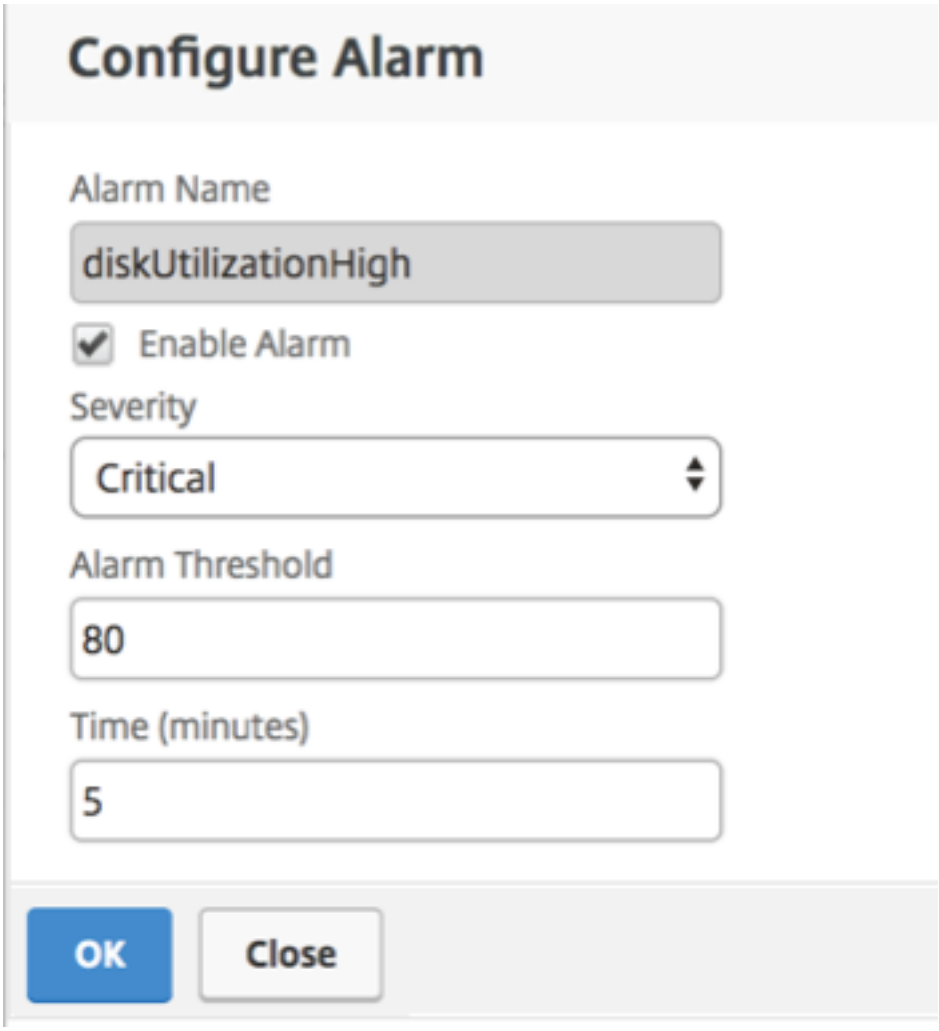
Para habilitar la depuración automática, marque la casilla **Habilitar purga automática de datos**. Se activa una alarma y se envía un correo electrónico cuando el uso del disco supera el **valor umbral de purga de datos** configurado.

> **Nota**
>
> La purga comienza cuando se cumple cualquiera de los criterios: el valor umbral de purga de datos o los datos que se deben conservar (días). Lo que se encuentre primero, tiene prioridad sobre el otro.

Para configurar y habilitar los ajustes de alarma:

1. Vaya a **Configuración** > **SNMP** . Haga clic en **Alarmas** en la esquina superior derecha.
2. Seleccione la alarma que quiera configurar (por ejemplo, diskUtiliationHigh) y haga clic en **Modificar**.
3. En la página **Configurar alarma**, especifique lo siguiente:

- **Gravedad**: Seleccione el nivel de gravedad.
- **Umbral de alarma**: Escriba el valor para el que se calcula la gravedad del evento.
- **Tiempo**: Escriba el tiempo (en minutos) después del cual quiere activar la alarma.



Configurar la configuración de podar eventos mediante NetScaler ADM

Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos de NetScaler ADM, puede especificar el intervalo para el que quiere que NetScaler ADM retenga 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).

1. Vaya a **Configuración > Administración > Eliminación de datos** y haga clic en **Eliminación de datos de sistema e instancia**. Haga clic en **Eventos de instancia**.
2. Introduzca el intervalo de tiempo, en días, durante el que quiere conservar los datos en el servidor NetScaler ADM y haga clic en **Guardar**.

Habilitar el acceso al shell para usuarios no predeterminados

January 30, 2024

Puede habilitar el acceso a la consola para los usuarios no predeterminados en NetScaler 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 a la consola para los usuarios no predeterminados en NetScaler ADM:

1. En NetScaler ADM, vaya a **Configuración > Administración**.
2. En **Configuraciones del sistema**, haga clic en **Sistema, zona horaria, URL permitidas y Configuración del agente**.
3. En la página **Configuraciones del sistema**, configure los siguientes parámetros:
    - **Comunicación con instancias**: Seleccione el protocolo de comunicación.
    - **Acceso seguro**: Habilite el acceso seguro para NetScaler 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 inicio de sesión nsrecover** - Habilitar el inicio de sesión de `nsrecover` en el servicio de administración.
    - **Habilitar la descarga de certificados**: Le permite descargar certificados del NetScaler agregado.
    - **Habilitar el acceso a Shell para usuarios que no sean de nsroot**: Habilite el acceso a shell para usuarios no predeterminados en NetScaler ADM.
    - **Solicitar credenciales de usuario para iniciar sesión en instancias**: Permite a los usuarios introducir sus credenciales de usuario al iniciar sesión en las instancias desde NetScaler ADM.
        - **Solicitar credenciales para las operaciones de Stylebooks**: permita a los usuarios introducir sus credenciales de usuario mientras utilizan las operaciones de StyleBook y del paquete de configuración en las instancias de NetScaler.

          > **Nota:**
          > Si se selecciona **Solicitar credenciales para el inicio de sesión de instancias** y se borra **Solicitar credenciales para las operaciones de Stylebook**, no se so-

> licita a los usuarios que proporcionen credenciales para las operaciones de StyleBook y del paquete de configuración en las instancias de NetScaler.

4. Haga clic en **Aceptar**.

Recuperar servidores NetScaler ADM inaccesibles

January 30, 2024

NetScaler 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 de utilidad NetScaler ADM para conectarse al sistema de archivos, eliminar algunos componentes y hacer que la base de datos sea accesible. El script de recuperación ADM de NetScaler 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

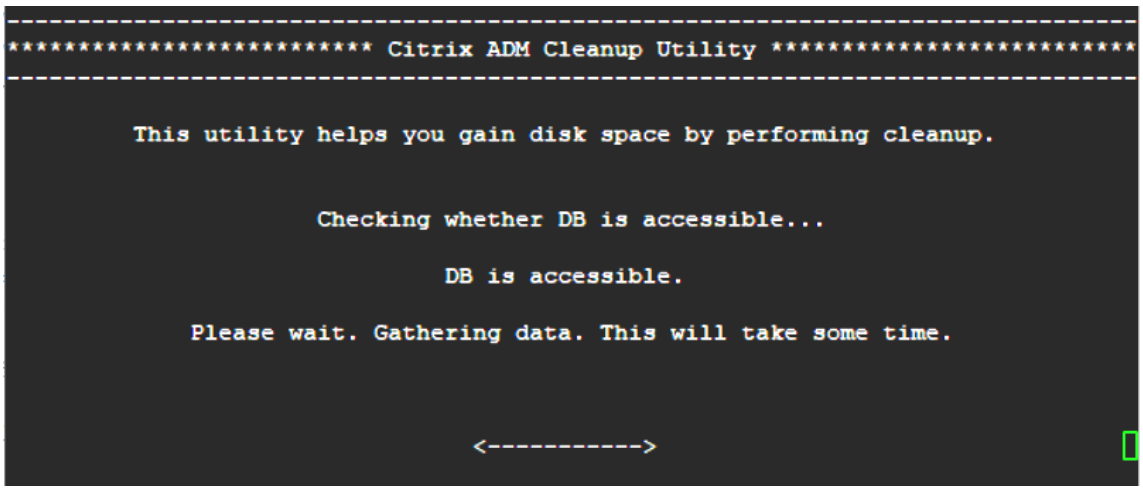
Utilice el procedimiento siguiente en un único servidor de implementación de NetScaler ADM para conectarse al sistema de archivos, eliminar algunos componentes y hacer accesible la base de datos y, a continuación, realizar las operaciones de recuperación.

1. Con un cliente SSH o la consola del hipervisor, inicie sesión en NetScaler ADM y escriba el siguiente comando:

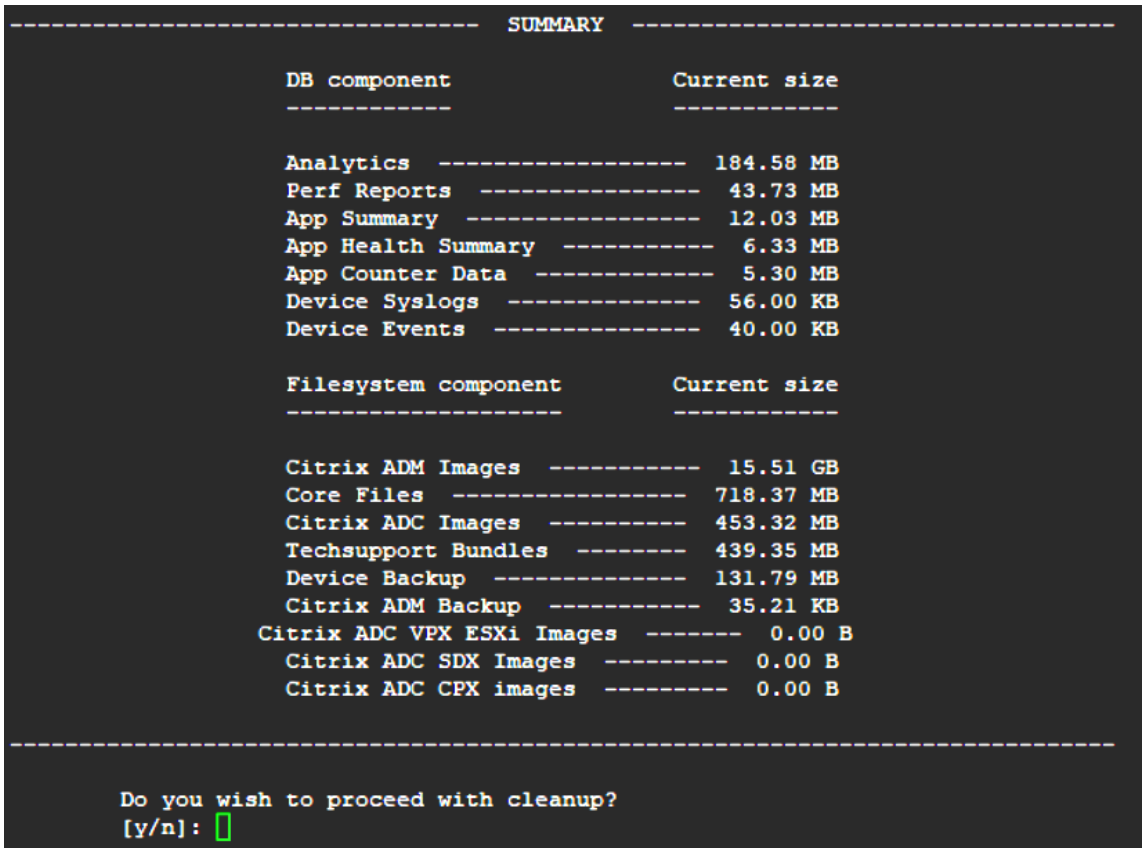
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

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.



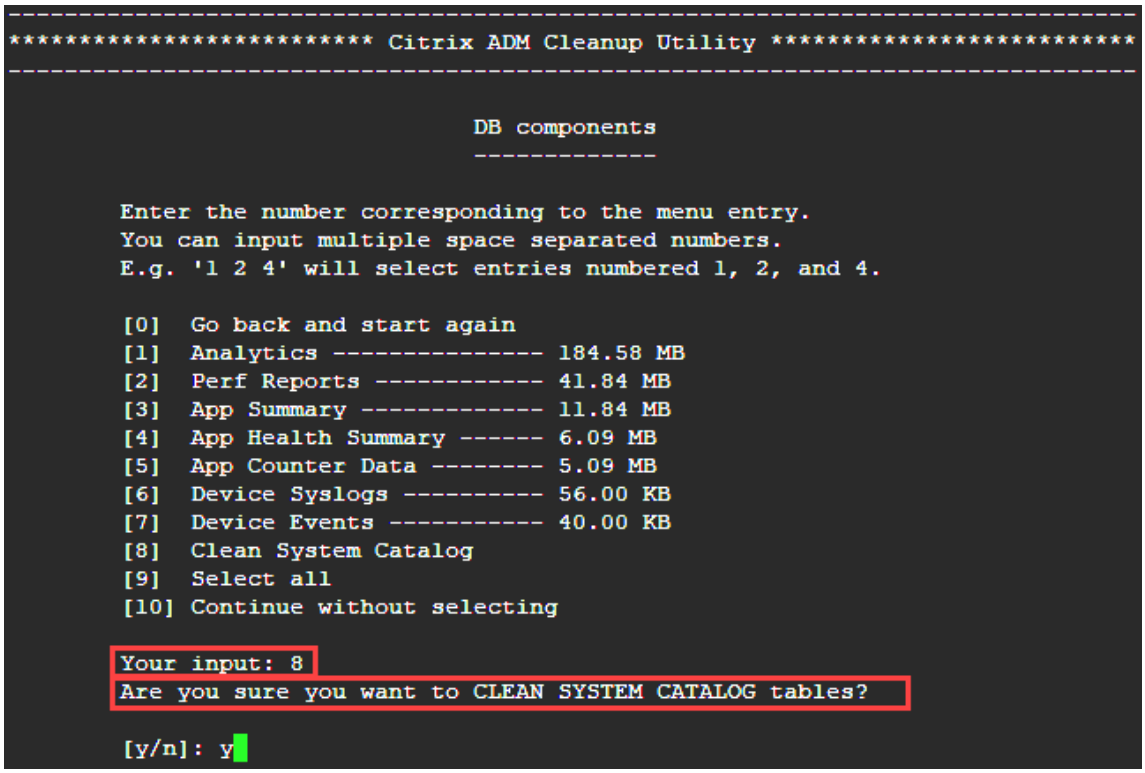
3. La pantalla muestra la lista de archivos de la base de datos. Escriba "y"y pulse la tecla Enter para iniciar el proceso de limpieza.



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.

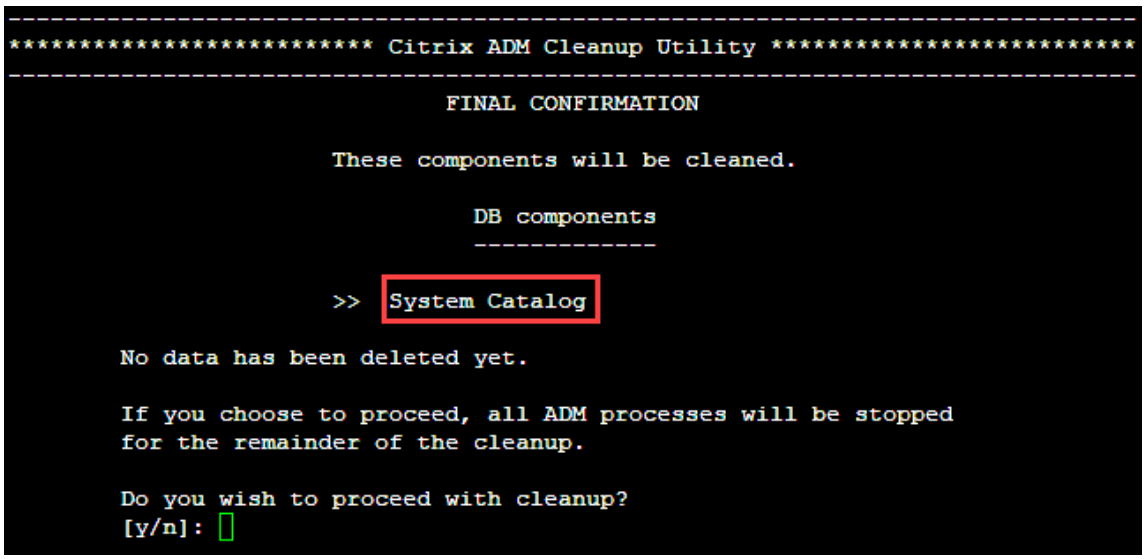
> **Nota:**
>
> NetScaler ADM incluye tablas de usuarios conocidas como catálogo del sistema. El catálogo del sistema es una ubicación en la base de datos ADM de NetScaler donde un sistema de administración de bases de datos relacionales almacena los metadatos del esquema, como información sobre tablas y columnas y 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 ADM de NetScaler.



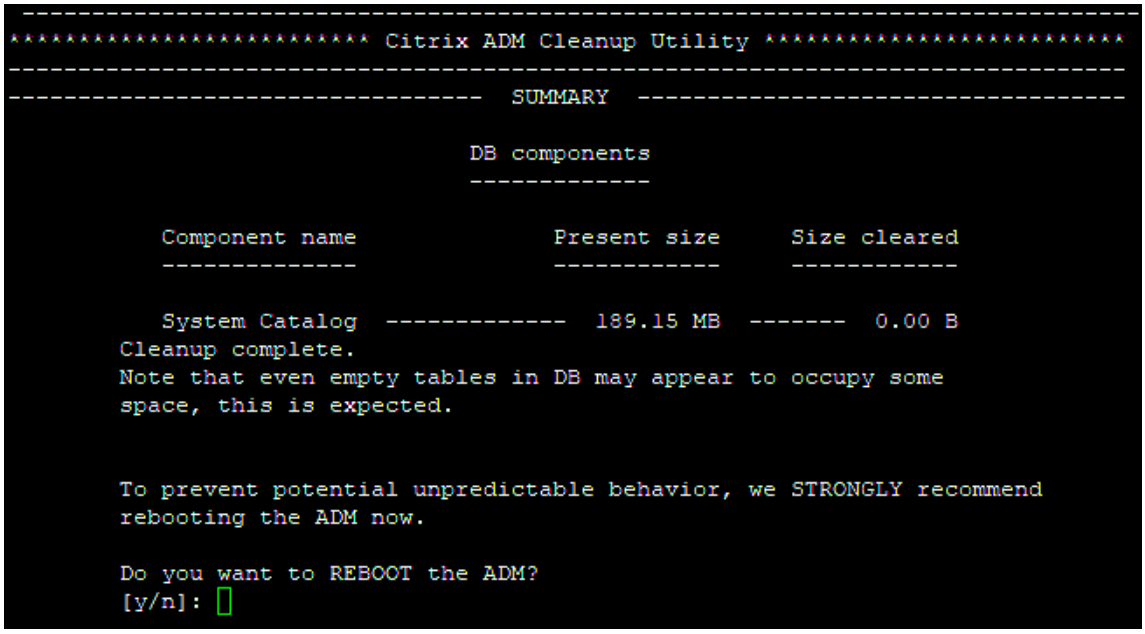
La utilidad de limpieza ofrece la opción de limpiar los componentes de la base de datos y los componentes de archivos. Puede seleccionar cualquier componente del archivo escribiendo un número entre "1"y "9", o escribir "11"y pulsar la tecla Enter para limpiar el componente de la base de datos.

> **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 **Enter** para reiniciar NetScaler ADM.

   Asegúrese de reiniciar NetScaler 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, podrá conectarse a la base de datos NetScaler ADM. Si no es así, vuelva a ejecutar el script de recuperación para liberar más espacio. Cuando NetScaler ADM esté en funcionamiento, debería 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 NetScaler ADM para una implementación de alta disponibilidad de NetScaler ADM

El sistema de base de datos para los servidores NetScaler 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 necesita replicar el procedimiento en los dos servidores NetScaler 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

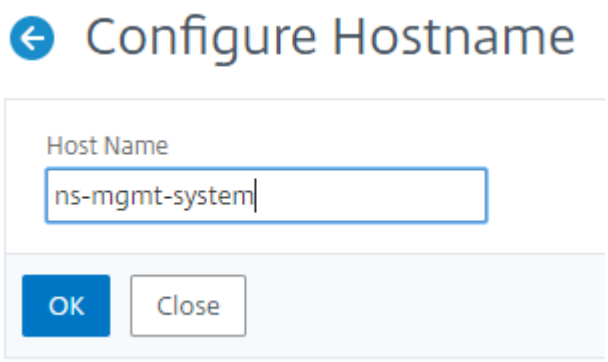
Asignar un nombre de host a un servidor NetScaler ADM

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**.



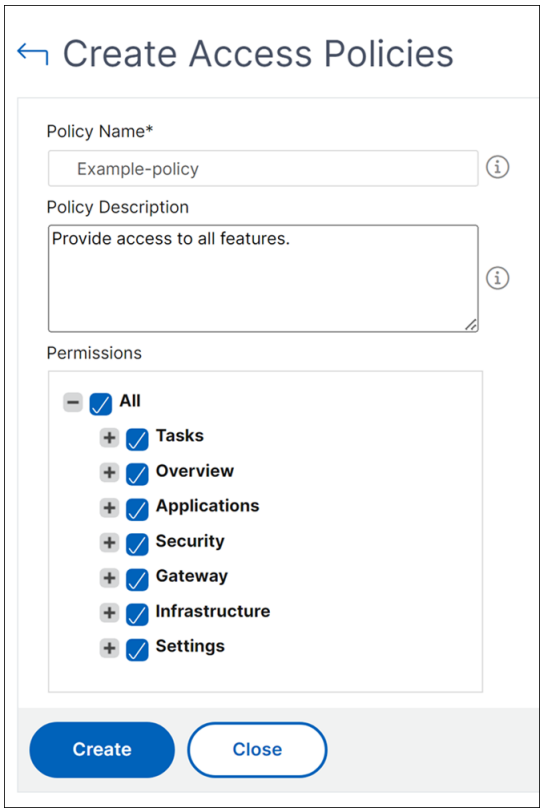
> **Nota**
>
> También puede usar el comando `networkconfig` en el hipervisor y cambiar el nombre del host.

Copia de seguridad y restauración del servidor NetScaler ADM

January 30, 2024

Puede realizar copias de seguridad periódicas de su servidor NetScaler ADM. Puede realizar copias de seguridad y restaurar los archivos de configuración, los detalles de la instancia, los datos del sistema, etc.

> **Importante**
>
> Citrix recomienda restaurar el servidor ADM mediante una copia de seguridad de la misma versión. Por ejemplo, si la versión de ADM es 13.0, use la copia de seguridad de ADM 13.0 para restaurar el servidor.

> El acceso de los usuarios para hacer copias de seguridad y restaurar el servidor ADM es limitado. La página **Configuración > Archivos de copia** de seguridad solo aparece para los usuarios que tienen acceso a todas las funciones de ADM. Un usuario puede acceder a esta página solo si su directiva de acceso tiene todos los permisos. Normalmente, los superusuarios tienen acceso a todas las funciones de ADM.
>
> 
>
>
> Para obtener más información, consulte Configurar directivas de acceso.

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 ADM de NetScaler:
  - SNMP
  - Archivos de configuración del servidor Syslog
  - archivos NTP
  - Certificados de SSL
  - Archivos del Centro de control
- Copias de seguridad de las instancias de NetScaler que administra el servidor NetScaler 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 NetScaler 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, las licencias de ADM y los mensajes de syslog se excluyen de la copia de seguridad.

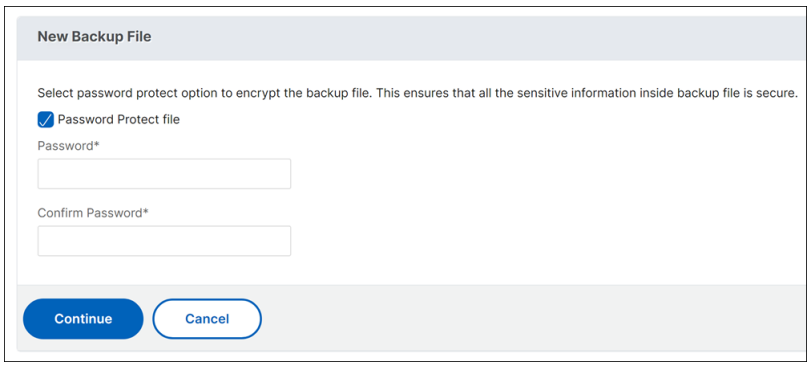
Respaldar la configuración de NetScaler ADM

De forma predeterminada, el servidor NetScaler ADM realiza 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 hacer una copia de seguridad de una configuración NetScaler ADM:

1. Vaya a **Configuración > Archivos de respaldo**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.

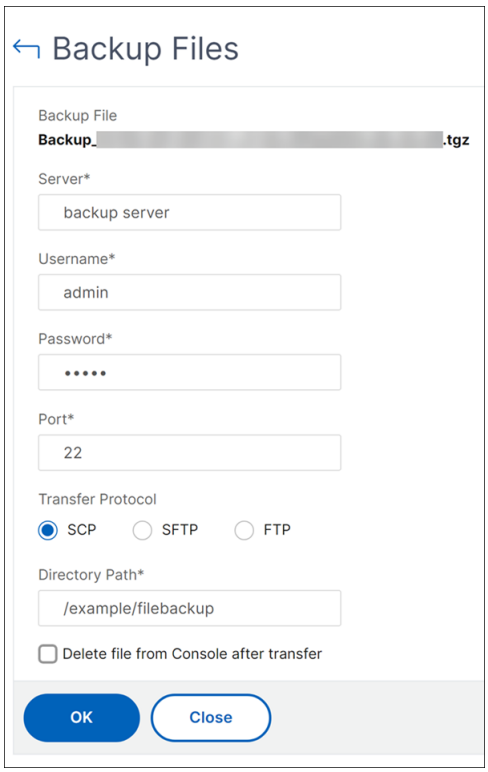


Transferir un archivo de copia de seguridad NetScaler ADM a un sistema externo

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 respaldo de NetScaler ADM:

1. Ve a**Configuración > Archivos de copia de seguridad**.
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.
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 copia de seguridad en su sistema local, vaya a **Configuración > Archivos de copia**de seguridad, seleccione el archivo que quiere copiar y, a continuación, haga clic en **Descargar**.

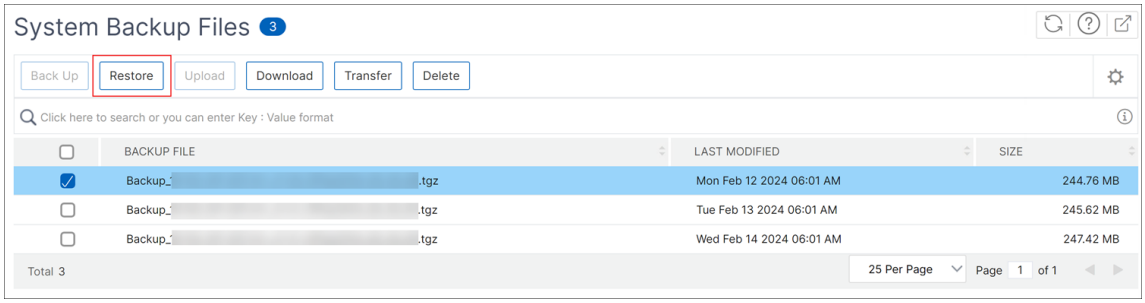
Restaurar la configuración de NetScaler ADM desde un archivo de copia de seguridad

Al restaurar la configuración de NetScaler ADM a partir de un archivo del que se hizo una copia de seguridad anterior, la operación de restauración desactiva el archivo de respaldo 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. Ve a **Configuración > 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 **Configuración > Archivos de copia**de seguridad y, a continuación, haga clic en **Cargar**.

Instantáneas de máquinas virtuales de NetScaler ADM en una implementación de alta disponibilidad

January 30, 2024

Puede tomar instantáneas de los servidores NetScaler ADM en la implementación de HA antes de iniciar la actualización. Las instantáneas capturan todo el estado de la máquina virtual en el momento en que se toman.

Realice una instantánea de los servidores NetScaler ADM

Utilice la siguiente secuencia para tomar instantáneas de los servidores NetScaler ADM:

1. Servidor secundario NetScaler ADM
2. Servidor principal NetScaler ADM

Para tomar una instantánea de los servidores NetScaler ADM:

1. En el hipervisor, seleccione el servidor secundario NetScaler ADM de la lista de máquinas virtuales.
2. Realice una instantánea de la máquina virtual.

> **Nota:**
>
> Le recomendamos que seleccione **Tomar memoria de la máquina virtual** al tomar la instantánea.

3. Asigne a la instantánea un nombre significativo e introduzca una descripción, si es necesario.

   La instantánea se almacena en el directorio de máquinas virtuales predeterminado.

4. Repita los mismos pasos para el servidor principal.

> **Nota:**
>
> No es necesario apagar la máquina virtual mientras se toma una instantánea.

Restaurar una instantánea de los servidores NetScaler ADM

Al restaurar una instantánea, se devuelven la memoria, la configuración y el estado de los discos de la máquina virtual al estado en que se encontraban cuando se tomó la instantánea.

Utilice la siguiente secuencia para restaurar las instantáneas de los servidores NetScaler ADM:

1. Servidor principal NetScaler ADM
2. Servidor secundario NetScaler ADM

Para restaurar la instantánea de los servidores NetScaler ADM:

1. En el hipervisor, seleccione el servidor principal NetScaler ADM de la lista de máquinas virtuales.
2. Haga clic con el botón derecho en la máquina virtual y revierta la instantánea.

   La máquina virtual se revierte a la instantánea más reciente.

3. Repita los mismos pasos para el servidor secundario NetScaler ADM.

Ver información de auditoría

January 30, 2024

Syslog es un protocolo estándar para el registro. Tiene dos componentes: el módulo de auditoría de Syslog, que se ejecuta en la instancia de Citrix Application Delivery Controller (ADC), y el servidor Syslog, que puede ejecutarse en el sistema operativo (SO) FreeBSD subyacente de la instancia de NetScaler 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 NetScaler si configura el dispositivo para redirigir los mensajes de syslog a NetScaler Application Delivery Management (ADM). Puede programar un trabajo para crear servidores syslog que generen diferentes tipos de datos de syslog mediante la función de plantillas integrada en NetScaler 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 NetScaler 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 NetScaler ADM:

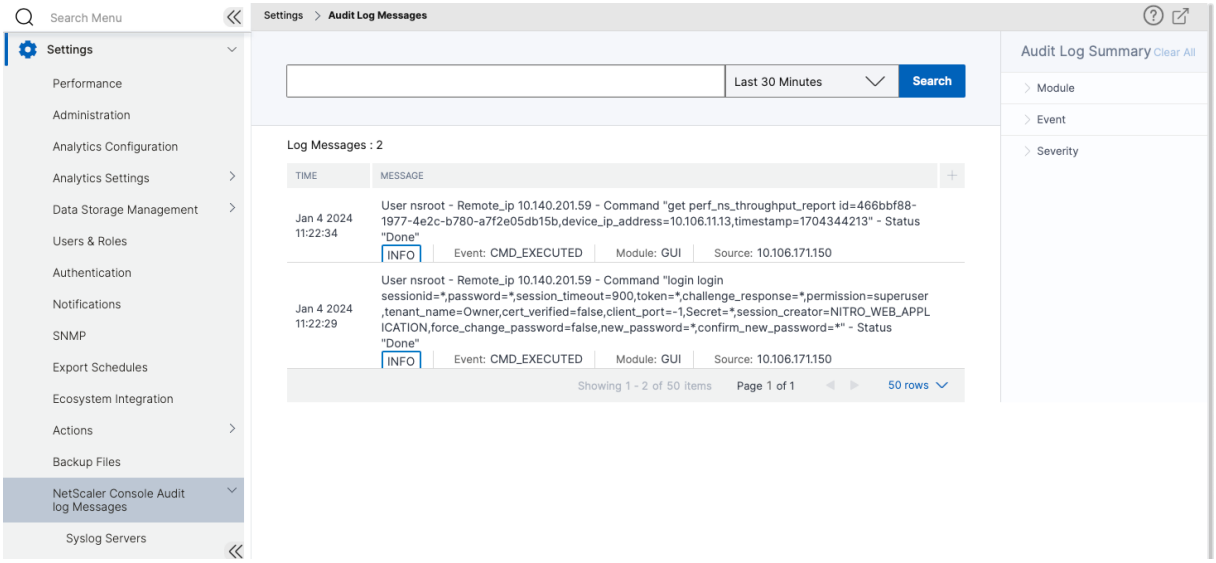
1. Vaya a**Sistema**>**Auditoría.** En**Resumen de configuración**, seleccione Servidores**Syslog.**
2. **En la página**Servidor Syslog, seleccione un servidor**syslog y, a continuación, haga clic en Parámetros de Syslog.**
3. En la página**Configurar parámetros de Syslog**, especifique el formato de fecha y hora.
4. Haga clic en **Aceptar**.

Para ver los mensajes de syslog en NetScaler ADM:

Ahora puede ver todos los mensajes de syslog generados en las instancias de NetScaler gestionadas si ha configurado la instancia para redirigir los mensajes de syslog al servidor NetScaler ADM. Los mensajes de syslog se almacenan en la base de datos del servidor NetScaler 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 ajustes de SSL en NetScaler Application Delivery Management (ADM) y especificar el tipo de clientes que se conectan al sistema.

Para configurar los ajustes de SSL para NetScaler 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** .

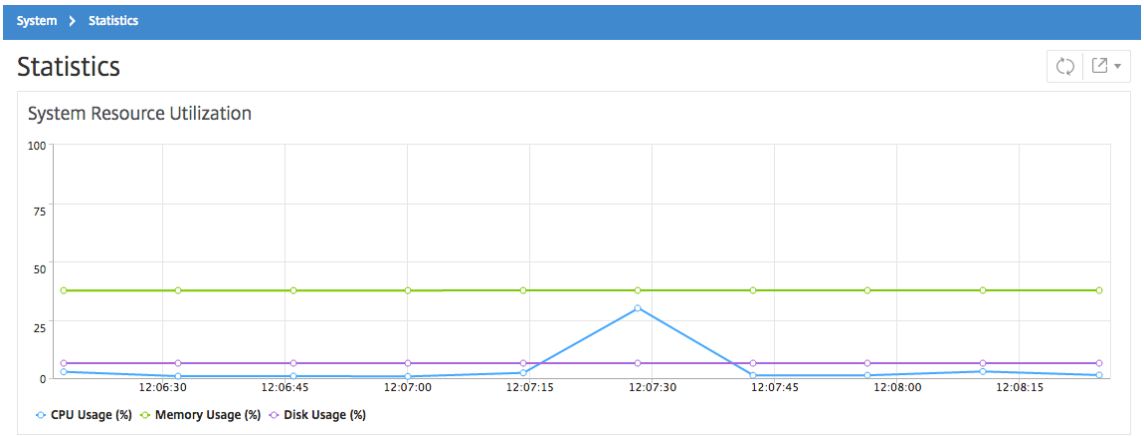
Supervisar el uso de CPU, memoria y disco

January 30, 2024

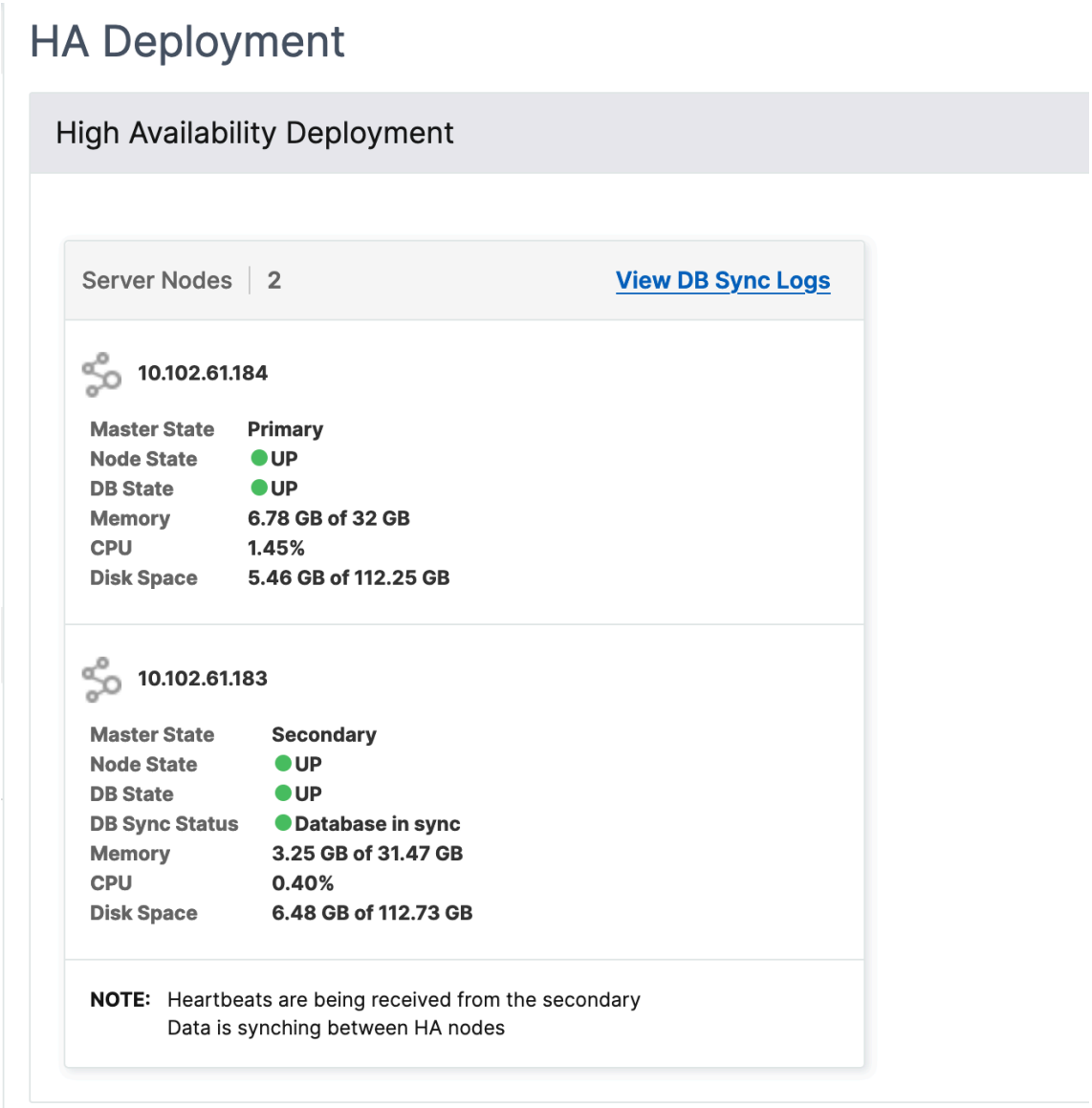
Puede utilizar la información mantenida en los registros y las estadísticas. Esta información también se muestra en los informes que le ayudan a configurar y mantener NetScaler Application Delivery Management (ADM).

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.** Vaya a **Configuración > 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

January 30, 2024

Puede seleccionar un tipo de notificación para recibir notificaciones para las siguientes funciones:

- **Eventos**: lista de eventos que se generan para las instancias de NetScaler. Para obtener más información, consulte Agregar acciones de reglas de eventos.
- **Licencias**: lista de licencias que están actualmente activas, a punto de caducar, etc. Para obtener más información, consulte Caducidad de la licencia de NetScaler ADM.

- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias NetScaler. Para obtener más información, consulte Caducidad del certificado SSL

ADM admite los siguientes tipos de notificación:

- Correo electrónico
- SMS
- Slack
- PagerDuty
- ServiceNow

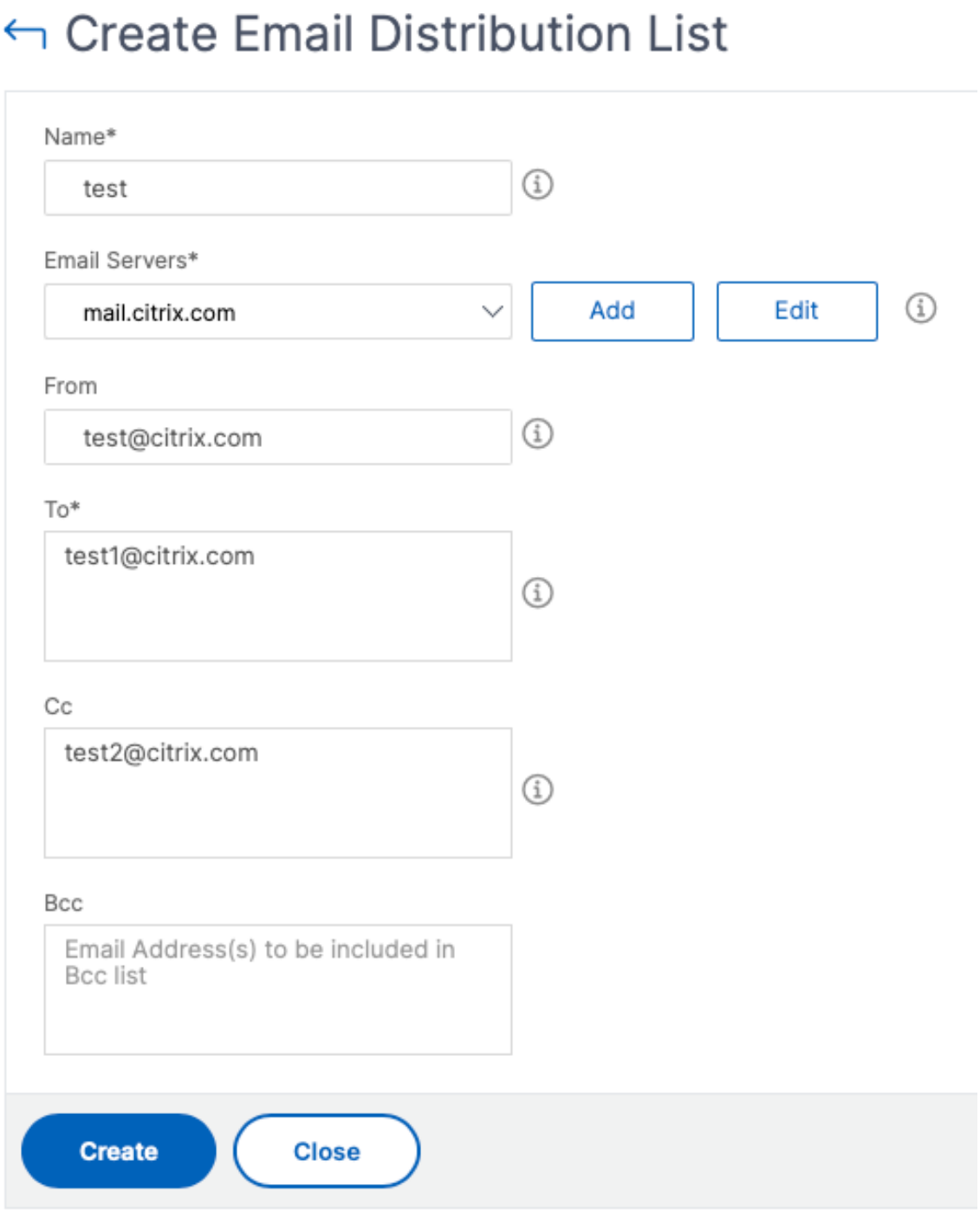
Para cada tipo de notificación, la GUI de ADM muestra la lista de distribución o el perfil configurados. El ADM envía notificaciones a la lista de distribución o perfil seleccionado.

Crea una lista de distribución de correo electrónico

Para recibir notificaciones por correo electrónico para las funciones de ADM, debe agregar un servidor de correo electrónico y una lista de distribución.

Realice los siguientes pasos para crear una lista de distribución de correo electrónico:

1. Vaya a **Configuración > Notificaciones**.
2. En **Correo electrónico**, haga clic en **Agregar**.
3. En **Crear lista de distribución de correo electrónico**, especifique los siguientes detalles:
    - **Nombre**: Especifique el nombre de la lista de distribución.
    - **Servidor de correo electrónico**: Seleccione el servidor de correo electrónico que envía la notificación por correo electrónico. Si desea agregar un servidor de correo electrónico, haga clic en **Agregar**.
    - **Desde**: Especifique la dirección de correo electrónico desde la que ADM debe enviar los mensajes.
    - **Para**: Especifique las direcciones de correo electrónico a las que ADM tiene que enviar mensajes.
    - **Cc**: Especifique las direcciones de correo electrónico a las que ADM debe enviar copias de los mensajes.
    - **Bcc**: Especifique las direcciones de correo electrónico a las que ADM debe enviar copias de los mensajes sin mostrar las direcciones.



4. Haga clic en **Crear**.

Repita este procedimiento para crear varias listas de distribución de correo electrónico. La ficha **Correo electrónico** muestra todas las listas de distribución de correo electrónico presentes en ADM.

Crea una lista de distribución de SMS

Para recibir notificaciones por SMS para las funciones de ADM, debe agregar un servidor SMS y números de teléfono.

Realice los siguientes pasos para configurar los ajustes de notificación SMS:

1. Vaya a **Configuración > Notificaciones**.
2. En **SMS**, haga clic en **Agregar**.
3. En **Crear lista de distribución de SMS**, especifique los siguientes detalles:
    - **Nombre**: Especifique el nombre de la lista de distribución.
    - **Servidor de SMS**: seleccione el servidor de SMS que envía la notificación por SMS.
    - **Para**: Especifique el número de teléfono al que ADM debe enviar mensajes.
4. Haga clic en **Crear**.

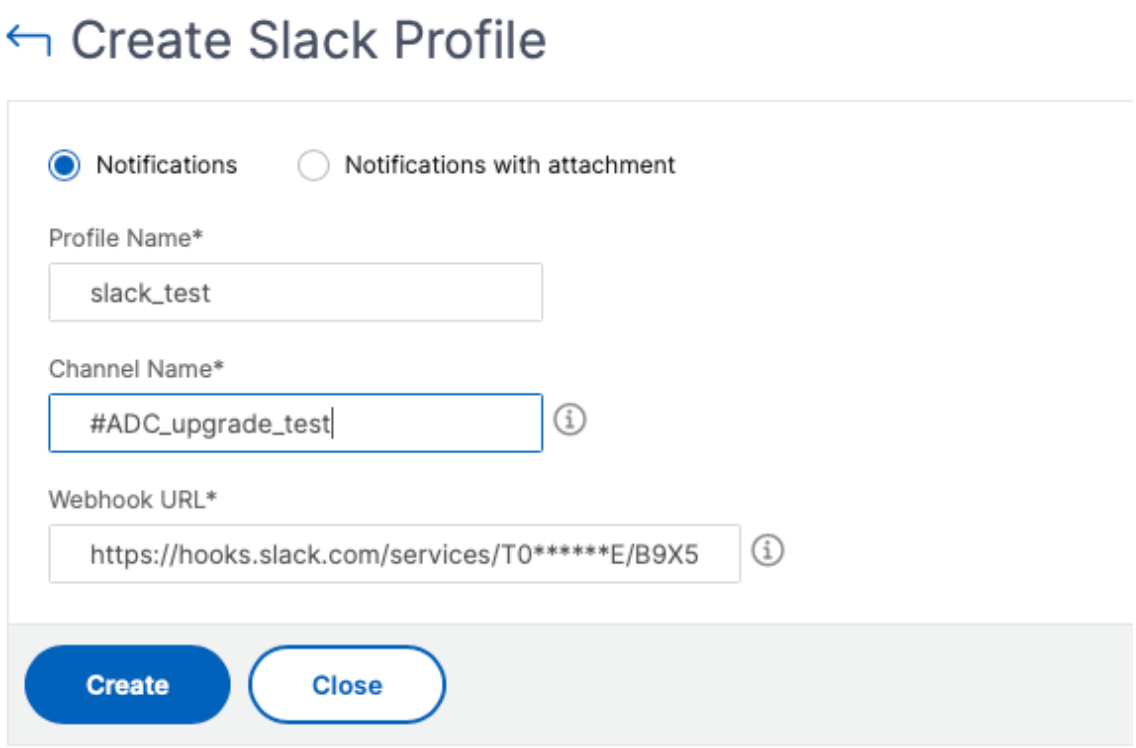
Repita este procedimiento para crear varias listas de distribución de SMS. La ficha **SMS** muestra todas las listas de distribución de SMS presentes en ADM.

Crear un perfil de Slack

Para recibir notificaciones de Slack sobre las funciones de ADM, debes crear un perfil de Slack.

Realice los siguientes pasos para crear un perfil de Slack:

1. Vaya a **Configuración > Notificaciones**.
2. En **Slack**, haga clic en **Agregar**.
3. En **Crear perfil de Slack**, especifica los siguientes detalles:
    - **Nombre de perfil**: especifique el nombre del perfil. Este nombre aparece en la lista de perfiles de Slack.
    - **Nombre del canal**: Especifica el nombre del canal de Slack al que ADM debe enviar las notificaciones.
    - **URL del webhook**: especifique la URL del webhook del canal. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal. Además, todas las notificaciones de eventos se envían a esta URL se publican en el canal Slack designado. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. Haga clic en **Crear**.

Repite este procedimiento para crear varios perfiles de Slack. La ficha **Slack** muestra todos los perfiles de Slack presentes en ADM.

Crear un perfil de PagerDuty

Puede agregar un perfil de PagerDuty para supervisar las notificaciones de incidentes en función de las configuraciones de PagerDuty. PagerDuty le permite configurar notificaciones a través de correo electrónico, SMS, notificaciones push y llamadas telefónicas en un número registrado.

Antes de agregar un perfil de PagerDuty en NetScaler ADM, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para empezar a usar PagerDuty, consulta la documentación de PagerDuty.

Realice los siguientes pasos para crear un perfil de PagerDuty:

1. Vaya a **Configuración > Notificaciones**.
2. En **PagerDuty**, haga clic en **Agregar**.
3. En **Crear perfil de PagerDuty**, especifique los siguientes detalles:
    - **Nombre de perfil**: especifique un nombre de perfil de su elección.

- **Clave de integración**: especifique la clave de integración. Puede obtener esta clave en su portal PagerDuty.

4. Haga clic en **Crear**.

Para obtener más información, consulte Servicios e integraciones en la documentación de PagerDuty.

Repita este procedimiento para crear varios perfiles de PagerDuty. La ficha **PagerDuty** muestra todos los perfiles PagerDuty presentes en ADM.

Ver el perfil de ServiceNow

Si quiere habilitar las notificaciones de ServiceNow para eventos de NetScaler y eventos de ADM, debe integrar NetScaler ADM con ServiceNow mediante el conector ITSM. Para obtener más información, consulte Integrar NetScaler ADM con la instancia de ServiceNow.

Realice los siguientes pasos para ver y verificar el perfil ServiceNow:

1. Vaya a **Configuración > Notificaciones**.
2. En **ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.
3. Haga clic en **Probar** para generar automáticamente un tíquet de ServiceNow y verificar la configuración.

   Si quiere ver los tíquets de ServiceNow en la GUI de NetScaler ADM, seleccione **Tíquets de ServiceNow**.

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 NetScaler 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 `afdecoder` registros.
- **Duración**: Introduzca la duración para 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 Citrix Insight Services (CIS).

   b) También puede cargar los archivos de soporte técnico al sitio web de CIS ejecutando un script en la consola ADM.

      i. Mediante SSH, inicie sesión en la consola ADM.

      ii. Cambie al símbolo del 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 a CIS directamente mediante un proxy desde la consola de 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 suceder si el script de Perl no confía en el certificado raíz del servidor proxy). Aún puede cargar el archivo directamente desde el shell de 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.

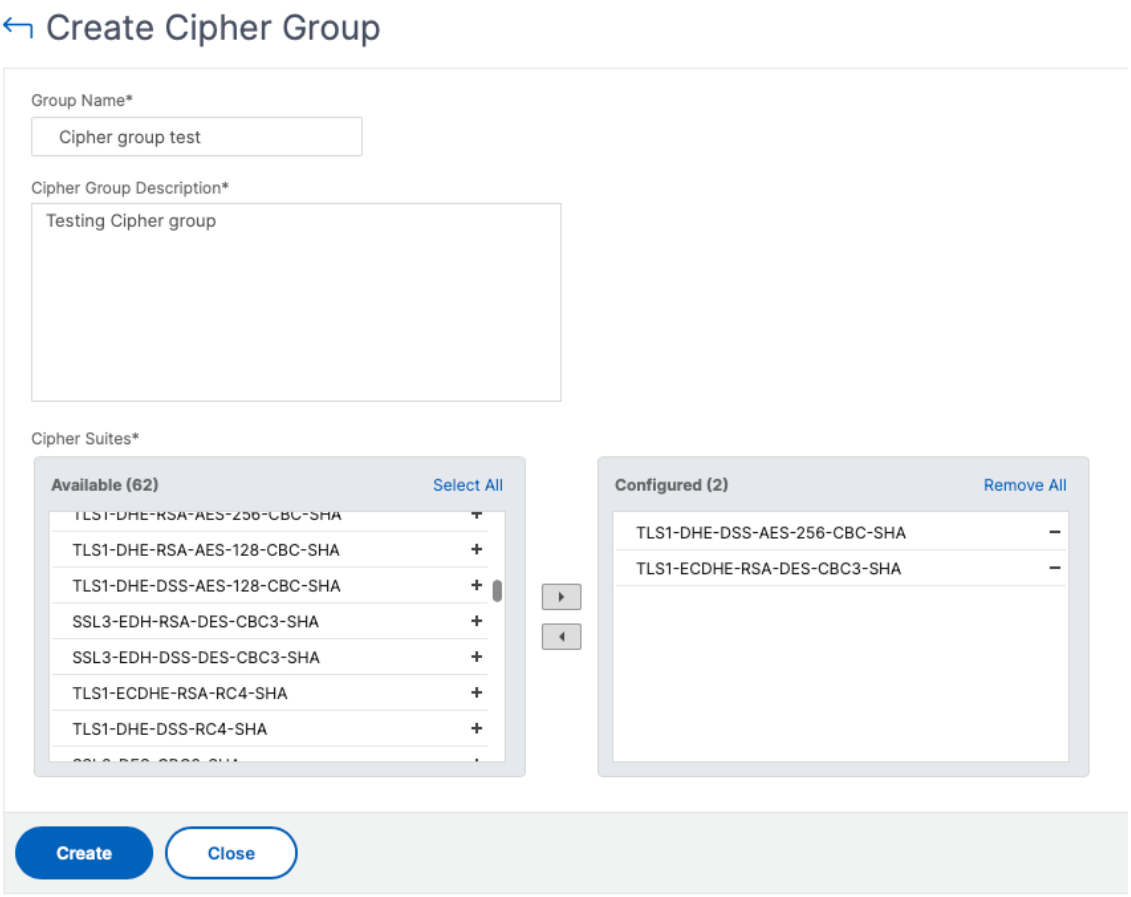
Configurar un grupo de cifrado

January 30, 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 **Configuración > Administración**
2. En **Configuración de SSL**, haga clic en **Grupos de cifrado**
3. Haga clic en **Agregar**.
4. 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.
5. 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 ADM de NetScaler, se genera una captura SNMP. A continuación, las capturas se envían a un dispositivo remoto denominado servidor de destino de capturas o *destino de capturas SNMP* . Aquí, NetScaler ADM se configura como destino de captura. 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 NetScaler 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 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. 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.

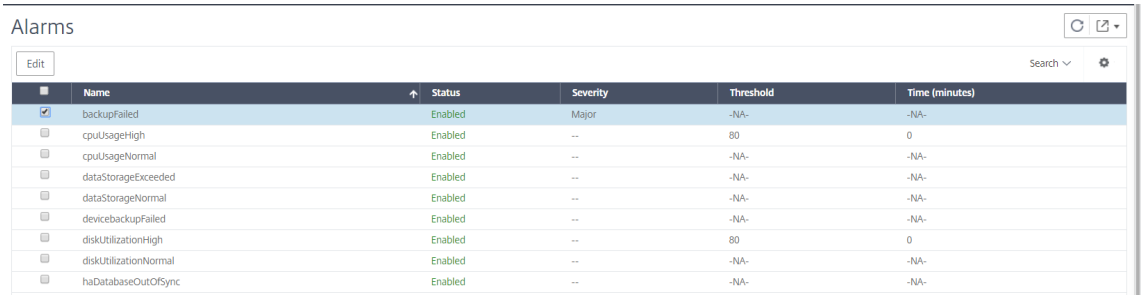
Puede asignar o modificar la gravedad de una alarma. Los niveles de gravedad que puede asignar son Crítico, Principal, Menor, Advertencia e Informativo.

Considere un caso en el que desee supervisar cada vez que se produzca un intento fallido de copia de seguridad. Puede habilitar la alarma BackupFailed y asignarle una gravedad, como Major, a ella. 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 NetScaler 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. Ve a **Configuración > SNMP**. Haga clic en **Alarmas** en la esquina superior derecha.

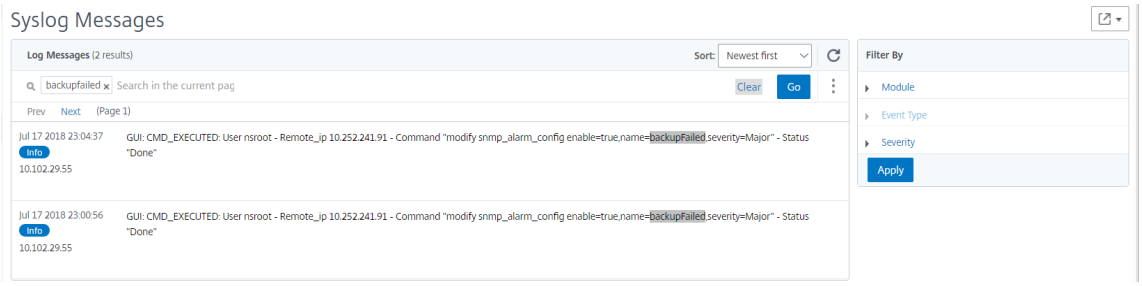


2. Seleccione la alarma que desee configurar (por ejemplo, BackupFailed) y haga clic en **Editar** para modificar su configuración.
3. La alarma está activada de forma predeterminada. Asigne un nivel de gravedad (ejemplo: Principal) y, a continuación, haga clic en **Aceptar**.

> **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 NetScaler 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.

Cree administradores y usuarios de SNMP para el agente NetScaler ADM

January 30, 2024

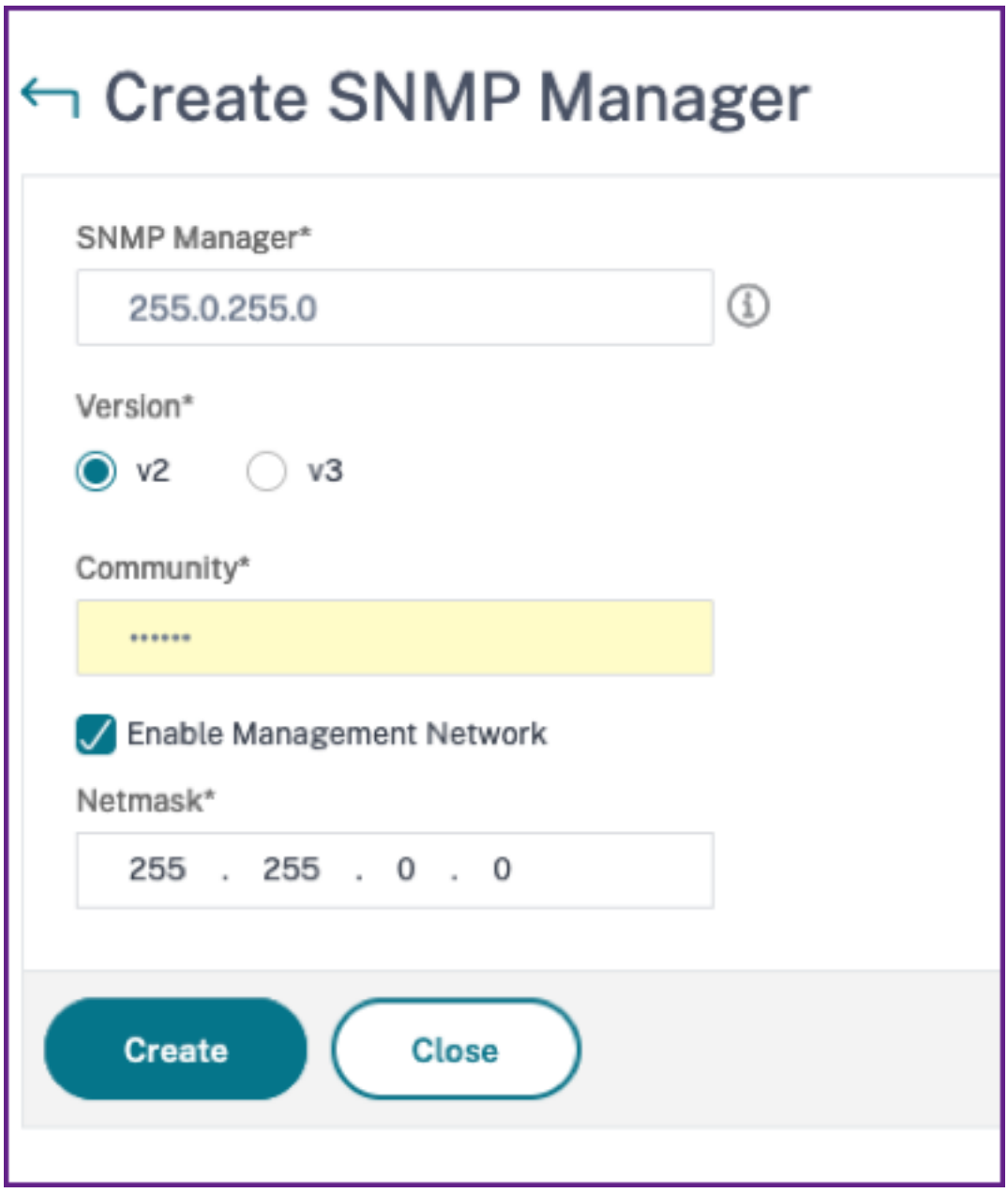
Puede consultar al agente SNMP para obtener información específica del sistema desde un dispositivo remoto denominado administrador SNMP. A continuación, el agente busca en la base de información de administración (MIB) los datos solicitados y los envía al administrador SNMP.

Puede agregar un administrador SNMP para consultar un agente ADM de NetScaler. El administrador cumple con SNMP V2 y V3. Si especifica uno o más administradores SNMP, el agente ADM de NetScaler no acepta consultas SNMP de ningún host, excepto de los administradores SNMP especificados.

Agregar un administrador SNMP v2

Para agregar un administrador SNMP v2 para el agente ADM de NetScaler:

1. Vaya a **Infraestructura > Agentes**, seleccione un agente ADM de NetScaler y haga clic en **Seleccionar acción**> Administrar SNMP.
2. **En la ficha**SNMP> SNMP Manager**, haga clic en Agregar.**
3. En la página **Crear un administrador de SNMP**, especifique los siguientes detalles:
   - **Administrador SNMP**. Introduzca el nombre o la dirección IP del Administrador de SNMP.
   - **Versión**. Selecciona v2.
   - **Comunidad**. Introduzca un nombre de comunidad. Una configuración de comunidad SNMP autentica las consultas SNMP de los administradores de SNMP.
   - **Habilitar red de administración**: active esta casilla de verificación para especificar la máscara de red de la red del administrador SNMP.
   - **Máscara de red**: introduzca la máscara de subred asociada a una dirección IP.
4. Haga clic en **Crear**.



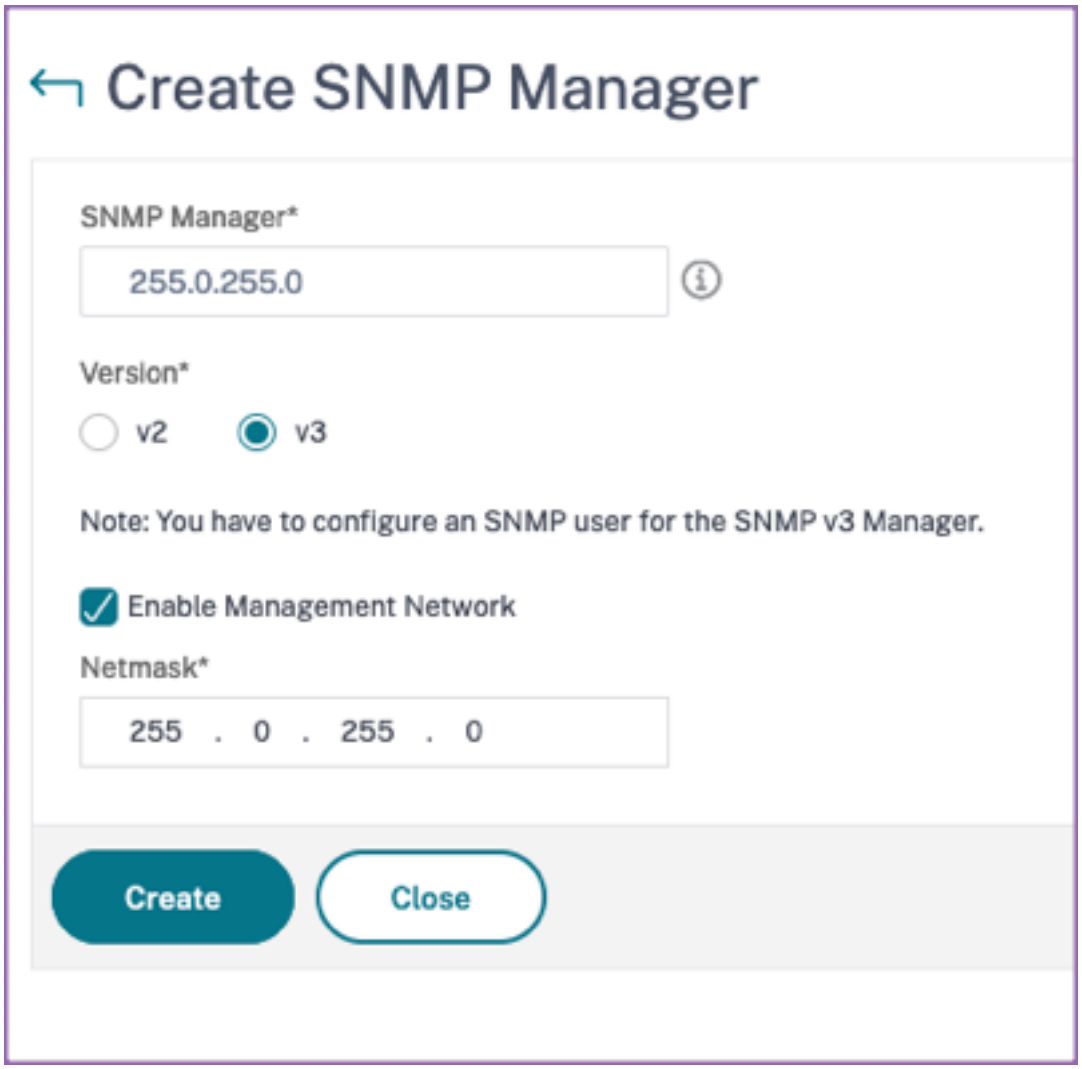
Agregar un administrador SNMP v3

Para agregar un administrador SNMP v3 para el agente ADM de NetScaler:

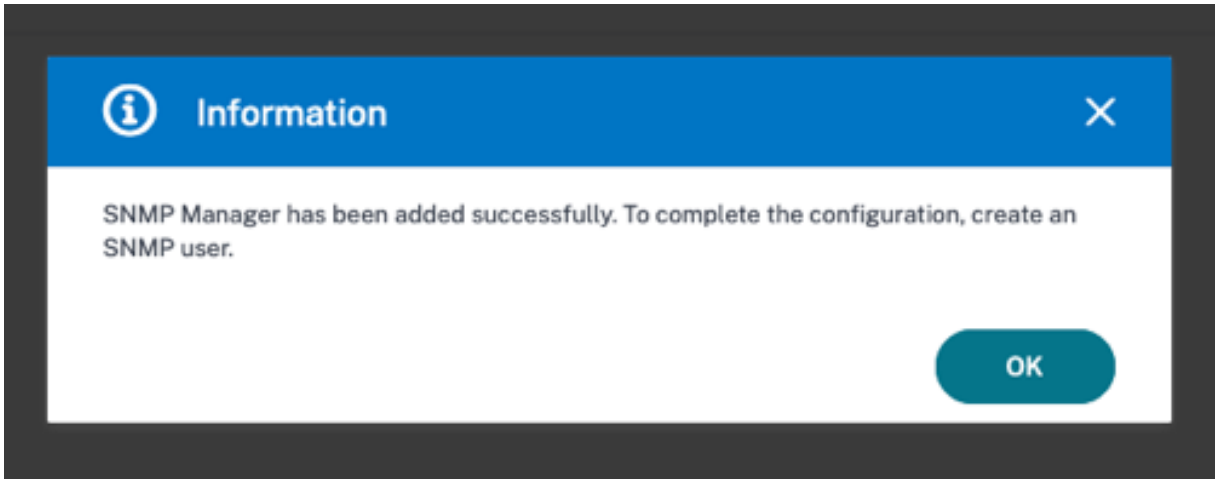
1. Vaya a **Infraestructura > Agentes**, seleccione un agente ADM de NetScaler y haga clic en **Seleccionar acción**> Administrar SNMP.
2. **En la ficha**SNMP> SNMP Manager**, haga clic en Agregar.**
3. En la página **Crear un administrador de SNMP**, especifique los siguientes detalles:

- **Administrador SNMP**. Introduzca el nombre o la dirección IP del Administrador de SNMP.
- **Versión**. Selecciona v3.
- **Habilitar red de administración**: active esta casilla de verificación para especificar la máscara de red de la red del administrador SNMP.
- **Máscara de red**: introduzca la máscara de subred asociada a una dirección IP.

4. Haga clic en **Crear**.



Aparece un cuadro de diálogo que confirma que se ha creado un administrador de SNMP y le solicita que configure un usuario de SNMP.



> **Nota**
>
> Debe configurar un usuario SNMP para un administrador SNMP v3. Para configurar el usuario SNMP, vaya a **SNMP > Usuario SNMP**.

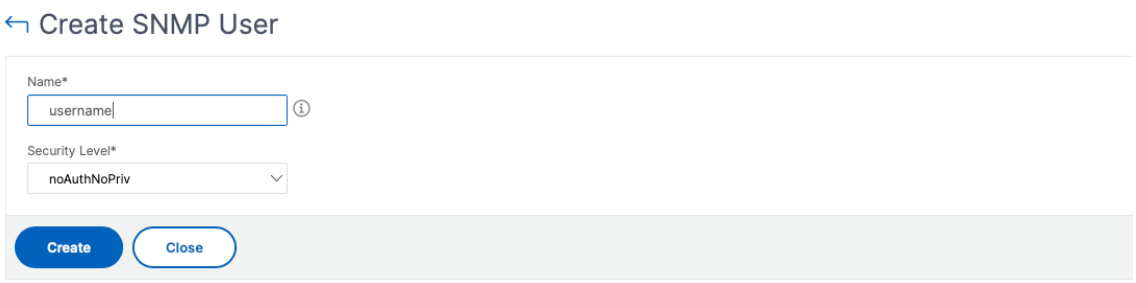
Agregar un usuario SNMP

Agregue un usuario SNMP para responder a las consultas SNMP v3 de un administrador de SNMP.

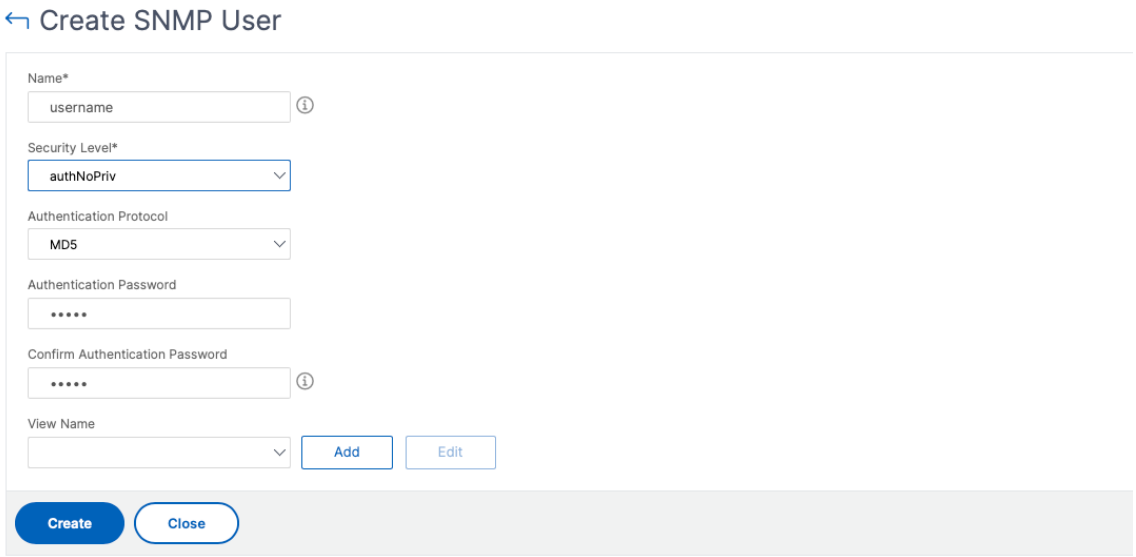
Para agregar un usuario SNMP para el agente ADM de NetScaler:

1. Vaya a **Infraestructura > Agentes**, seleccione un agente ADM de NetScaler y haga clic en **Seleccionar acción**> Administrar SNMP.
2. **En la ficha**SNMP> Usuario SNMP**, haga clic en Agregar.**
3. En la página **Crear usuario SNMP**, añada los siguientes detalles:
   - **Nombre**. Introduzca el nombre de usuario.
   - **Nivel de seguridad**. Nivel de seguridad requerido para la comunicación entre el agente ADM de NetScaler y el administrador SNMP.

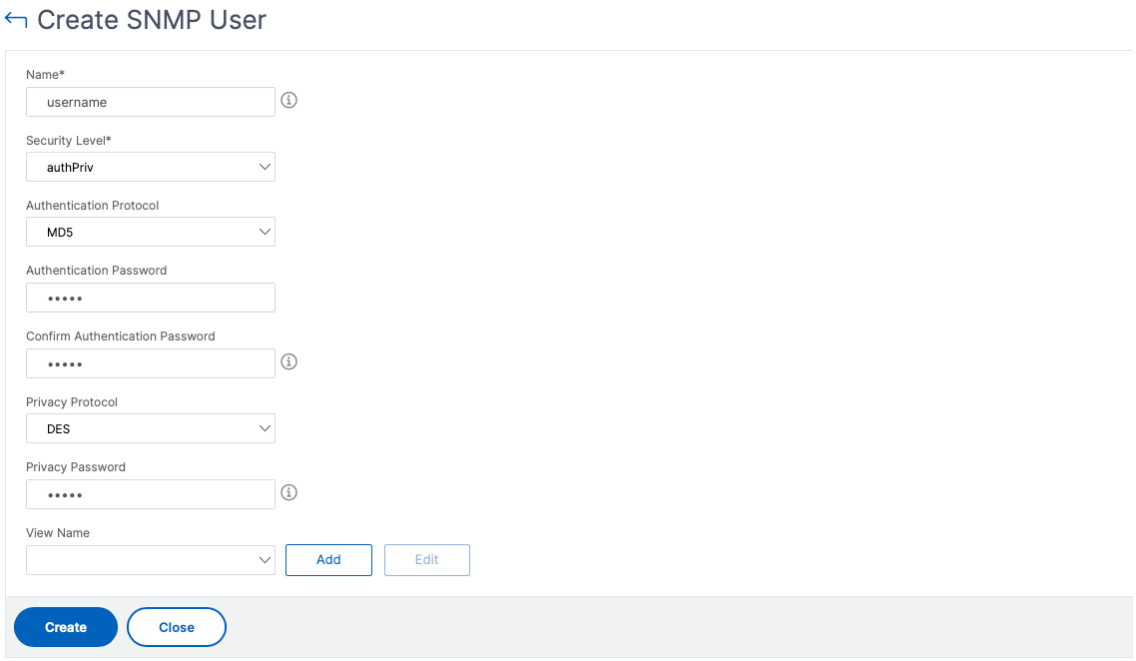
     Seleccione uno de los siguientes niveles de seguridad:
   - **NoAuthNoPriv**. No requieren autenticación ni cifrado.



- **AuthNoPriv**. Requiere autenticación pero no cifrado.



- **AuthPriv**. Exigen autenticación y cifrado.



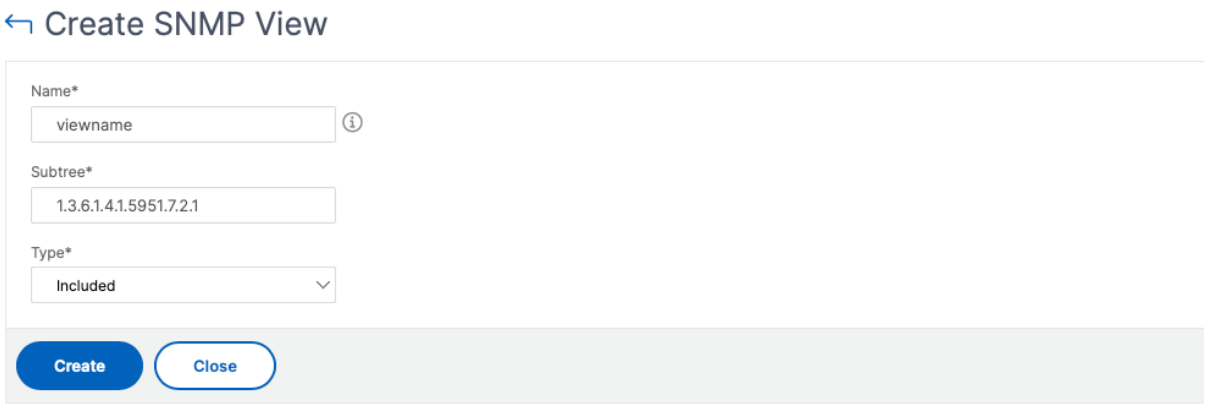
En función del nivel de seguridad asignado al usuario, proporcione protocolos de autenticación adicionales, como protocolos de autenticación, contraseñas de privacidad y asigne vistas SNMP.

Administración de vistas SNMP

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

Para permitir o restringir un OID SNMP para el agente ADM de NetScaler:

1. **Vaya a**Infraestructura > Agentes > Administrar SNMP**y, en la ficha**Vista de SNMP**, haga clic en Agregar.**
2. En la **vista Crear SNMP**, introduzca los siguientes detalles:
   - **Nombre de la vista**: nombre de la vista SNMP. Una instancia puede tener muchas vistas SNMP con el mismo nombre, diferenciadas por la configuración de los parámetros del sub-árbol.
   - **Subárbol**: una rama particular (subárbol) del árbol MIB que desea asociar a esta vista de SNMP. Debe especificar el subárbol como un OID de SNMP.
   - **Tipo**: este campo le permite incluir o excluir subárboles de una vista.
3. Haga clic en **Crear**.



Configurar los ajustes del agente

January 30, 2024

Puede modificar el intervalo de mantenimiento y los requisitos de cambio de contraseña del agente NetScaler ADM.

Establecer el intervalo de mantenimiento-vivo del agente

El servidor y el agente de NetScaler ADM mantienen la misma conexión TCP para el intervalo keep-alive especificado. Un agente usa esta conexión para enviar los datos de las instancias administradas al servidor NetScaler ADM.

1. Vaya a **Configuración > Administración**.
2. Seleccione **Sistema, zona horaria, URL permitidas y Configuración del agente** en **Configuraciones del sistema.**
3. En **Configuración básica > Configuración del agente**, especifique el intervalo de mantenimiento entre 30 y 120 segundos.
4. Haga clic en **Guardar**.

Cambiar la contraseña del agente sin la contraseña actual

Puede permitir que las contraseñas de los agentes se cambien sin su contraseña actual.

1. Vaya a **Configuración > Administración**.
2. Seleccione **Sistema, zona horaria, URL permitidas y Configuración del agente** en **Configuraciones del sistema.**
3. En la casilla **Configuración básica > Configuración del agente > Eliminar el requisito previo de la contraseña actual para cambiar la contraseña del agente**, puede hacer lo siguiente:
   - Seleccione la casilla de verificación para eliminar el campo **Contraseña actual** de la página **Contraseña del agente de cambio**.
   - Desactive la casilla de verificación para conservar el campo **Contraseña actual** en la página **Contraseña del agente de cambio**.
4. Haga clic en **Guardar**.

> **Nota**
>
> Para ver la página **Cambiar contraseña del agente**, vaya a **Infraestructura > Instancias > Agentes**, seleccione un agente y haga clic en **Seleccionar acción > Cambiar contraseña**.

Utilice el panel de administración de almacenamiento de datos

January 30, 2024

Es importante saber qué funciones se utilizan en NetScaler ADM y el uso de datos de cada una de estas funciones. El panel **Administración del almacenamiento de datos** cumple este propósito y funciona como su herramienta de visualización, lo que le permite comprender el total de datos almacenados en la base de datos ADM de NetScaler en varias funciones. El panel también indica si el almacenamiento consumido está dentro de los límites especificados o si supera el almacenamiento autorizado.

Como administrador, puede realizar las siguientes tareas en el panel **Administración del almacenamiento de datos**:

- Consulte el consumo de almacenamiento de datos de los últimos 30 días: Las tendencias de almacenamiento de datos se almacenan en la base de datos de NetScaler ADM durante los últimos 30 días. Estas tendencias están disponibles en forma gráfica o tabular. Estas tendencias muestran la cantidad de datos ingresada y la cantidad de datos que se almacenan después de los ciclos de depuración programados en NetScaler ADM.
- Ver el estado de la ingesta de datos: La actividad de ingesta de datos se produce siempre que el almacenamiento consumido esté dentro de los límites del almacenamiento autorizado. Cuando el almacenamiento consumido es superior al almacenamiento autorizado, la actividad de datos se detiene.
- Enviar notificaciones: Puede configurar las notificaciones para que se envíen cuando el almacenamiento consumido alcance el 75 % o el 100 % del almacenamiento autorizado, lo que permite a los usuarios gestionar su almacenamiento.
- Flexibilidad para administrar el espacio de almacenamiento de datos: Puede crear más espacio dentro de los datos almacenados reduciendo los datos que considere adecuados para su eliminación o reducción.

Vaya a **Configuración > Administración del almacenamiento de datos** para ver su panel de almacenamiento de datos.

En las siguientes secciones se describe cómo utilizar el panel **Administración del almacenamiento de datos** para una administración eficaz del almacenamiento de datos:

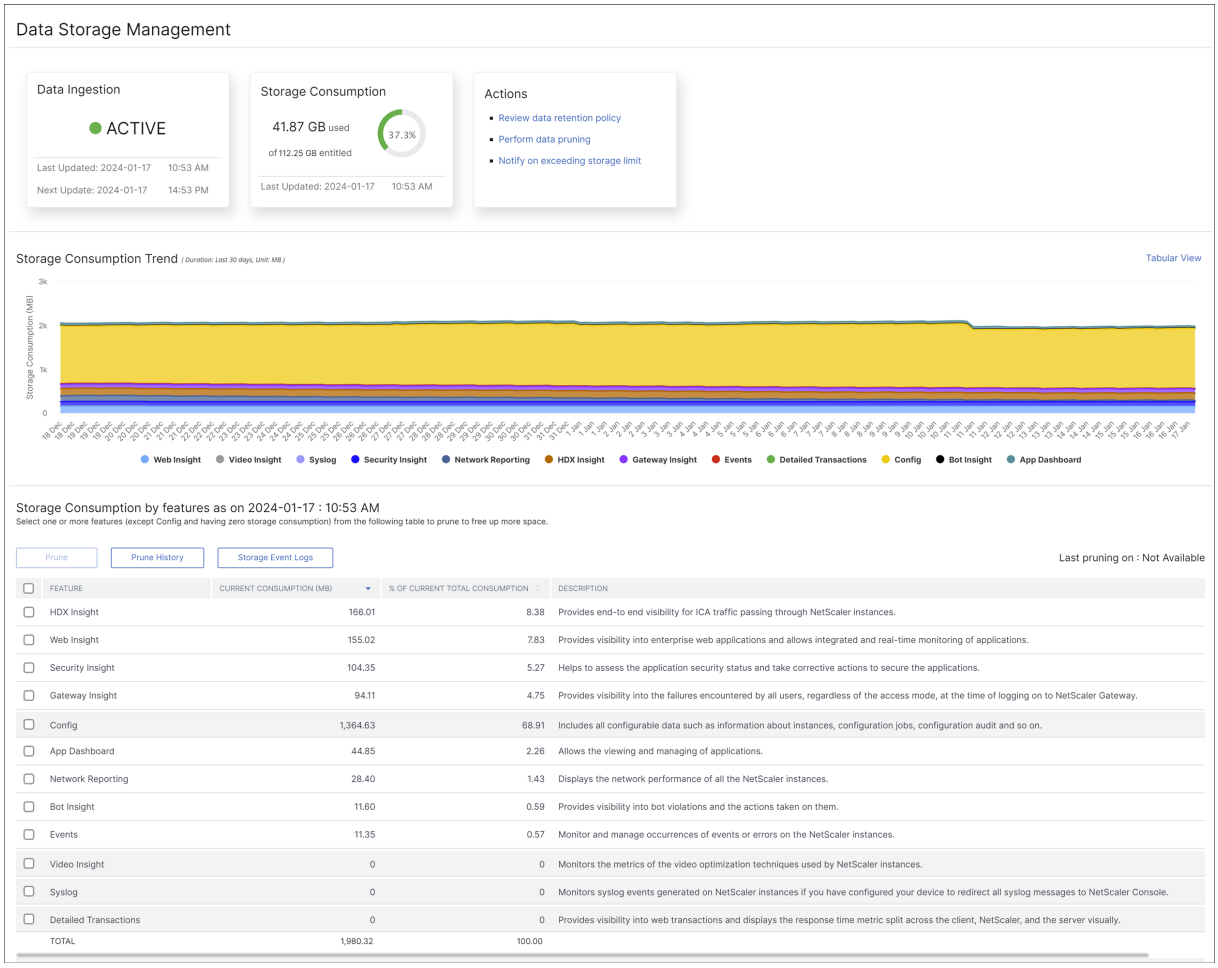
- Comprender su almacenamiento de datos: Esta sección le ayuda a entender cómo puede usar el panel para ver información sobre su almacenamiento de datos.
- Administrar el almacenamiento de datos: En esta sección se proporciona información sobre las acciones que puede realizar en el panel de control para administrar el almacenamiento de datos.

Comprenda su almacenamiento de datos

January 30, 2024

Puede utilizar el panel **Administración de almacenamiento de datos** de NetScaler ADM para ver datos y gráficos que le ayudan a realizar un seguimiento del uso del almacenamiento de datos.

Para controlar el consumo de almacenamiento de datos, vaya a **Configuración > Administración del almacenamiento de datos**.



El panel de administración del almacenamiento de datos indica la siguiente información:

- Estado de su actividad de ingestión de datos
- Consumo total de almacenamiento
- Tendencias de consumo de almacenamiento
- Consumo de almacenamiento por funciones

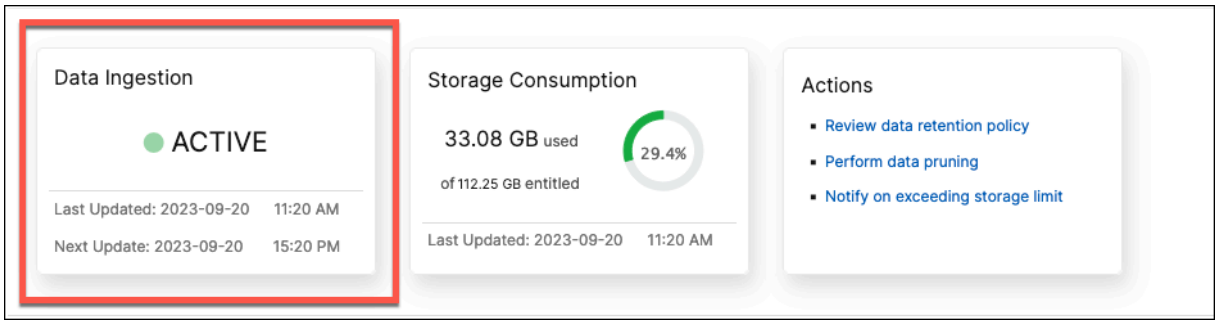
Estado de su actividad de ingestión de datos

La ingesta de datos se refiere al proceso de importar datos grandes y variados de todas las instancias de NetScaler administradas a través de diversas funciones, como eventos, syslogs, informes de red, etc., al almacenamiento ADM de NetScaler.

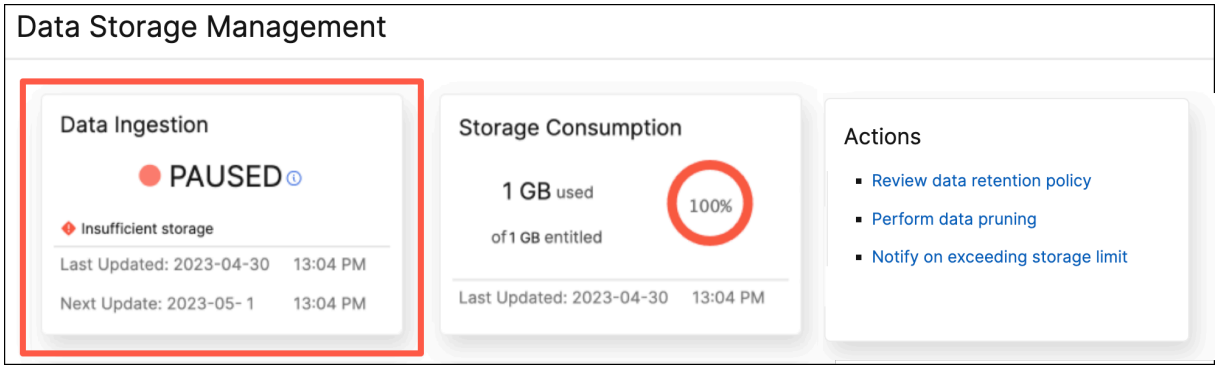
El estado de ingesta de datos indica si NetScaler ADM recopila estadísticas de las instancias de NetScaler. La actividad de ingesta de datos continúa mientras el almacenamiento consumido esté dentro del almacenamiento autorizado. Cuando el consumo es mayor al almacenamiento autorizado, la ingesta de datos se detiene.

Consulte el mosaico **Ingestión de datos** para comprender el estado actual de la ingesta de datos. Este mosaico muestra uno de los dos estados siguientes:

- **Activa**: La actividad de ingesta de datos está en curso.



- **En pausa**: La actividad de ingesta de datos está en pausa porque el almacenamiento consumido supera el almacenamiento autorizado.

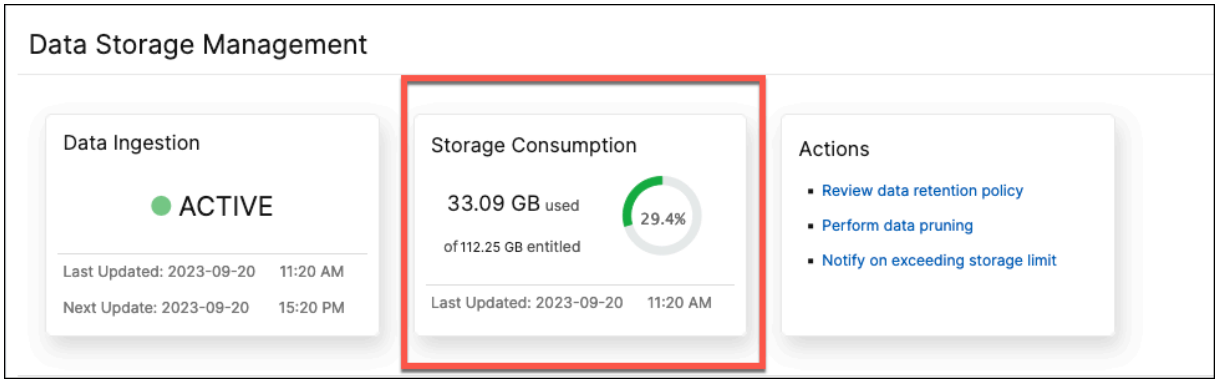


Cómo reanudar la ingesta de datos pausada

Para reanudar la actividad de ingesta de datos, puede realizar una depuración de datos. Para obtener más información, consulte Realizar depuración de datos.

Consumo total de almacenamiento

Para obtener una descripción general rápida de su almacenamiento de datos, consulte el mosaico **Consumo de almacenamiento**.



El mosaico **Consumo de almacenamiento** muestra el almacenamiento total utilizado por todas las funciones de la implementación.

Pase el mouse sobre el gráfico de anillos para ver lo siguiente:

Almacenamiento autorizado

El almacenamiento autorizado es el almacenamiento total disponible para su uso según su licencia. Si tiene una licencia Express, obtendrá 500 MB de almacenamiento autorizado. Si tiene una licencia avanzada, obtiene la suma de 500 MB de almacenamiento por cada VIP comprado y cualquier espacio de almacenamiento adicional que haya comprado directamente sin comprar VIP.

Tenga en cuenta los siguientes escenarios:

- Compró 20 VIP. Obtiene 500 MB de almacenamiento gratuito por cada VIP. El almacenamiento autorizado es de 20*500 = 10 GB.
- Compró 20 VIP y un almacenamiento adicional de 5 GB. Obtiene 500 MB de almacenamiento gratuito por cada VIP. El almacenamiento autorizado es de 20*500 + 5 = 15 GB.

Almacenamiento consumido

El almacenamiento consumido es el almacenamiento total que utilizan todas las funciones de la implementación. Los siguientes criterios de codificación de colores especifican la cantidad de almacenamiento utilizada por las funciones:

- **Verde**: El almacenamiento consumido es inferior al 75 % del almacenamiento autorizado.
- **Ámbar**: El almacenamiento consumido representa entre el 75 y el 99 % del almacenamiento autorizado.
- **Rojo**: El límite de almacenamiento consumido ha alcanzado o está por encima del almacenamiento autorizado actual.

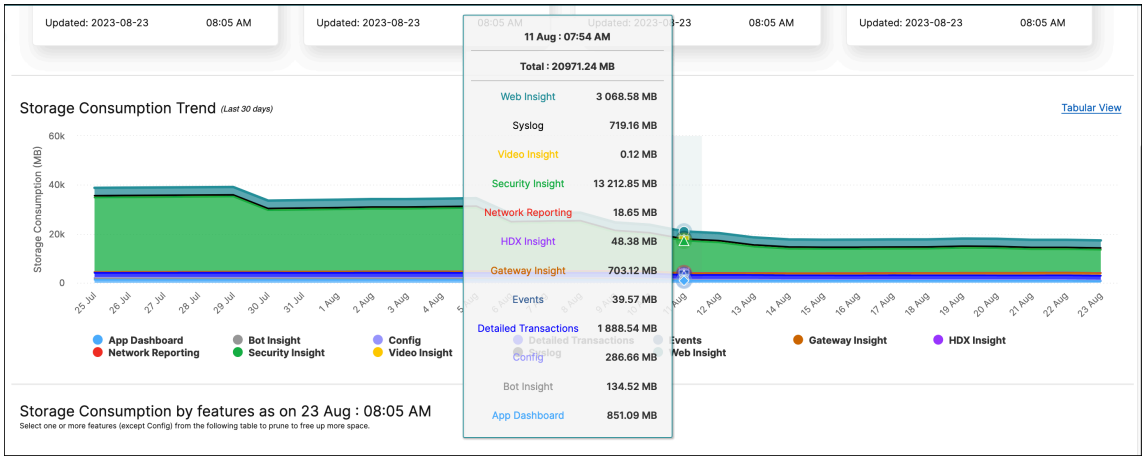
Tendencias de consumo de almacenamiento

Para saber cómo se consumen los datos en los últimos 30 días, consulte la sección **Tendencia del consumo de almacenamiento**.

Las **tendencias de consumo de almacenamiento** proporcionan información sobre qué funciones utilizan más o menos espacio de almacenamiento durante un período de tiempo y le ayudan a gestionar de forma eficaz el consumo de almacenamiento de datos.

Puede ver las tendencias de los datos de almacenamiento de cualquiera de las siguientes formas:

- **Vista gráfica**: Muestra cómo se distribuye el almacenamiento de datos en las diferentes funciones de NetScaler ADM. Pase el ratón sobre la cronología para ver la información de almacenamiento de datos de cualquier día del mes.



> **Nota:**
>
> La **vista gráfica** es la vista predeterminada.

- **Vista tabular**: haga clic en **Vista tabular** para mostrar la información de almacenamiento de datos en forma de tabla.

Storage Consumption Trend *(Last 30 days)* Graphical View

FEATURE	25 JUL	26 JUL	27 JUL	28 JUL	29 JUL	30 JUL	31 JUL	1 AUG	2 AUG	3 AUG	4 AUG
Security Insight	30415.05	30478.90	30535.21	30596.05	30648.76	25069.69	25222.26	25380.30	25552.37	25551.91	2570
Web Insight	3193.42	3200.39	3207.48	3213.02	3219.95	3226.22	3231.98	3238.30	3246.83	3252.87	3258
Detailed Transactions	2007.07	1998.34	1985.43	2046.68	2031.71	2014.52	1995.44	1985.16	2039.65	2025.91	2014
Gateway Insight	248.15	279.05	310.27	342.74	373.78	403.89	434.83	466.64	499.50	499.01	529.
Syslog	775.05	775.54	776.50	686.32	697.56	708.37	719.57	720.30	721.24	721.61	721.5
App Dashboard	1240.54	1237.85	1238.79	1238.08	1238.98	1238.13	1238.94	1238.66	1239.17	1239.24	1238
Config	269.76	270.68	272.41	273.02	274.16	275.49	275.18	272.52	271.13	271.70	271.8
HDX Insight	52.95	52.72	52.49	52.53	52.45	52.64	52.75	52.83	52.80	53.23	52.9
Events	45.06	45.27	44.85	44.49	43.96	43.63	43.24	43.08	43.16	42.95	42.5
Network Reporting	21.80	21.78	21.77	21.77	21.77	21.77	21.77	21.77	21.75	22.07	22.2
Bot Insight	544.23	543.98	544.09	544.32	544.10	544.01	544.10	544.05	544.10	544.10	544.
Video Insight	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
TOTAL	38813.31	38904.75	38989.54	39059.27	39147.42	33598.61	33780.30	33963.85	34231.95	34224.85	3439

Showing 1 - 12 of 12 items Page 1 of 1

> **Nota:**
>
> La vista tabular le permite filtrar los datos mediante el campo de búsqueda.

En la siguiente tabla se describen los campos que se muestran en la sección **Tendencia del consumo de almacenamiento**:

FUNCIÓN	DESCRIPCIÓN
Config	Incluye todos los datos configurables, como información sobre las instancias, los trabajos de configuración, la auditoría de configuración, etc.
HDX Insight	Proporciona visibilidad integral para el tráfico ICA que pasa a través de NetScaler.
Informes de red	Muestra el rendimiento de la red de todas las instancias de NetScaler.
Información web	Proporciona visibilidad de las aplicaciones web empresariales y permite la supervisión integrada y en tiempo real de las aplicaciones.
Security Insight	Ayuda a evaluar el estado de seguridad de las aplicaciones y a tomar medidas correctivas para proteger las aplicaciones.
Gateway Insight	Proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, al iniciar sesión en NetScaler Gateway.

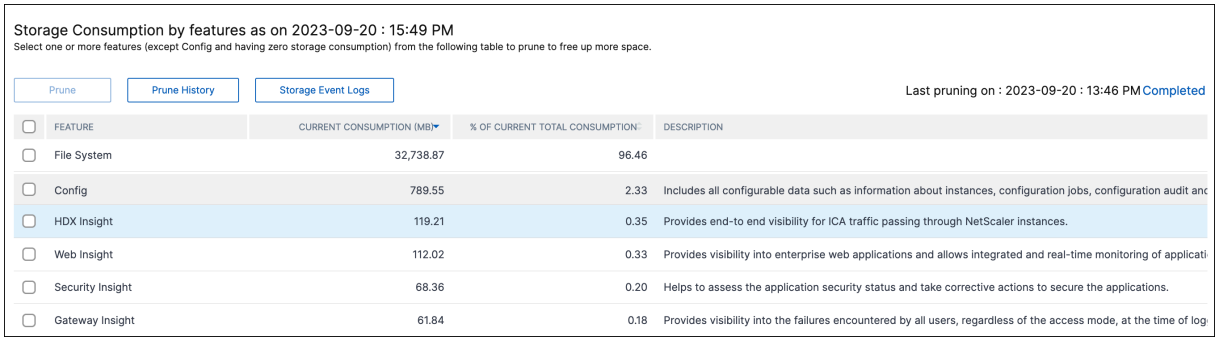
FUNCIÓN	DESCRIPCIÓN
Eventos	Supervise y administre la aparición de eventos o errores en las instancias de NetScaler.
Panel de aplicaciones	Permite la visualización y administración de aplicaciones.
Insight del bot	Proporciona visibilidad sobre las infracciones de los bots y las acciones que se han tomado al respecto.
Syslog	Supervisa los eventos de syslog generados en las instancias de NetScaler si ha configurado su dispositivo para redirigir todos los mensajes de syslog a NetScaler ADM.
Video Insight	Supervisa las métricas de las técnicas de optimización de vídeo utilizadas por las instancias de NetScaler.
Transacciones detalladas	Proporciona visibilidad de las transacciones web y muestra visualmente la métrica del tiempo de respuesta dividida entre el cliente, NetScaler y el servidor.

Consumo de almacenamiento por funciones

Para obtener más información sobre cómo se distribuye el almacenamiento de datos entre las diferentes funciones, consulte **Consumo de almacenamiento por funciones en la sección *dd mmm***.

El consumo de almacenamiento por funciones como *dd mmm* le ayuda a comprender:

- El espacio de almacenamiento utilizado por todas las diferentes funciones de NetScaler ADM
- El porcentaje de espacio que consumen las funciones en un día determinado



Si quiere ordenar las entradas de la tabla, los encabezados de la tabla. NetScaler ADM ordena al-

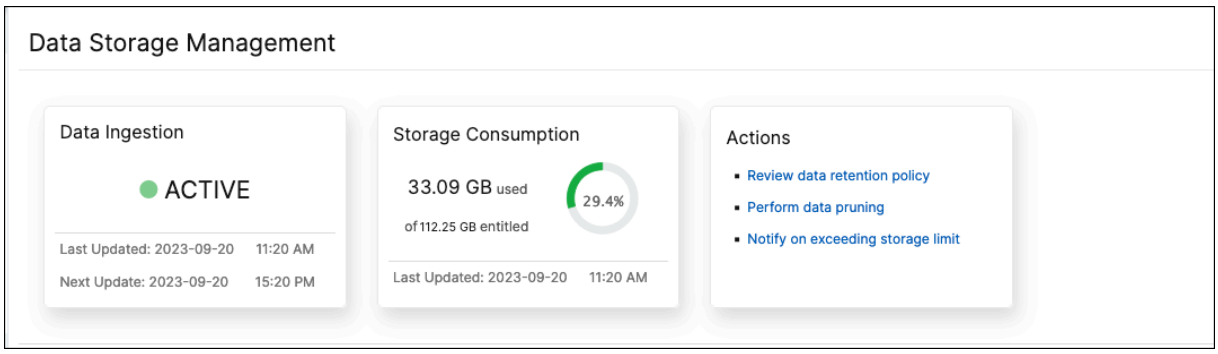
fanuméricamente la tabla de arriba a abajo en función de los datos de la columna elegida. Para ordenar la tabla en orden inverso, vuelva a hacer clic en el encabezado de la columna.

Para obtener información sobre cómo depurar los datos, el historial de depuración y los registros de eventos de almacenamiento, consulte Administrar el almacenamiento de datos

Administra tu espacio de almacenamiento

January 30, 2024

Puede utilizar el panel **Administración del almacenamiento de datos** para observar el uso del almacenamiento de datos y tomar las medidas necesarias para liberar espacio o aumentar el almacenamiento cuando el almacenamiento de datos supere el límite de la licencia.



El **cuadro Acciones** muestra la lista de pasos recomendados que puede realizar para administrar la capacidad de almacenamiento:

- Revisar la directiva de retención de datos
- Realizar una depuración de datos
- Notificar si se supera el límite de almacenamiento

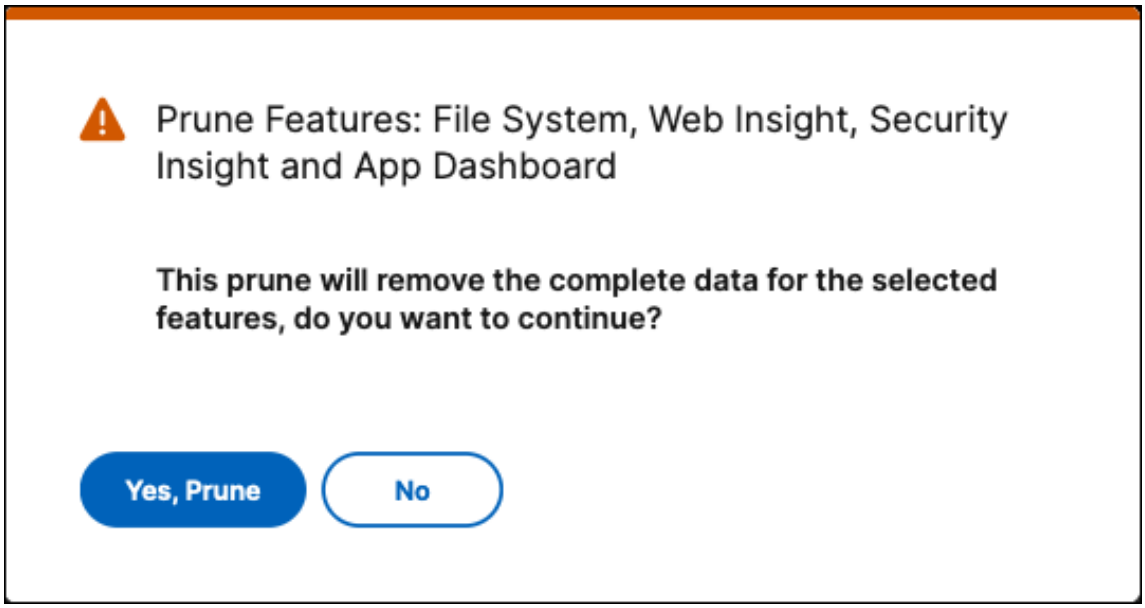
Realizar una depuración de datos

Recorte sus datos para optimizar los recursos de almacenamiento y obtener más espacio de almacenamiento. Además de liberar espacio, la depuración de datos mejora la calidad de los datos y acelera los tiempos de procesamiento. Le recomendamos que revise y purgue los datos innecesarios a intervalos regulares. Este proceso garantiza que sus recursos se utilicen con prudencia y que NetScaler ADM sea ágil y responsivo.

Para reducir sus datos:

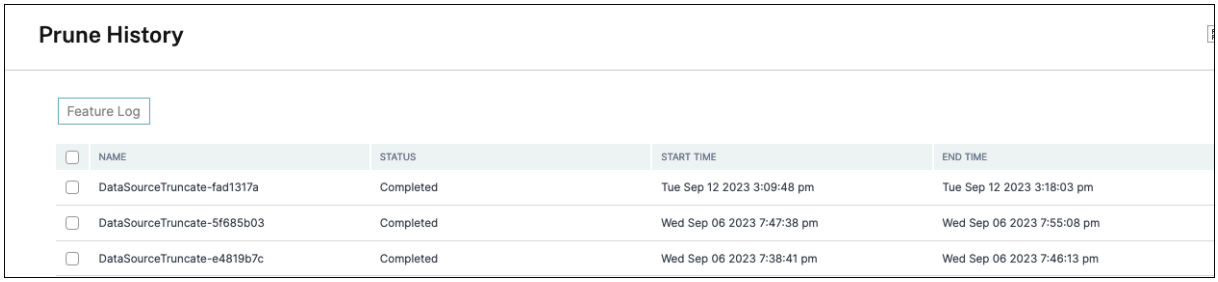
1. En la página **Administración del almacenamiento de datos**, desplácese hacia abajo hasta la sección ***Consumo de almacenamiento por funciones, tal como se muestra en la sección aaaa-mm-dd***.
2. Seleccione una o más funciones y haga clic en **Eliminar.** No puede seleccionar **Config**, ya que incluye todas las configuraciones del sistema.

   Una ventana emergente le pide que confirme si quiere eliminar todos los datos de las funciones seleccionadas. Haga clic en **Sí, podar**.



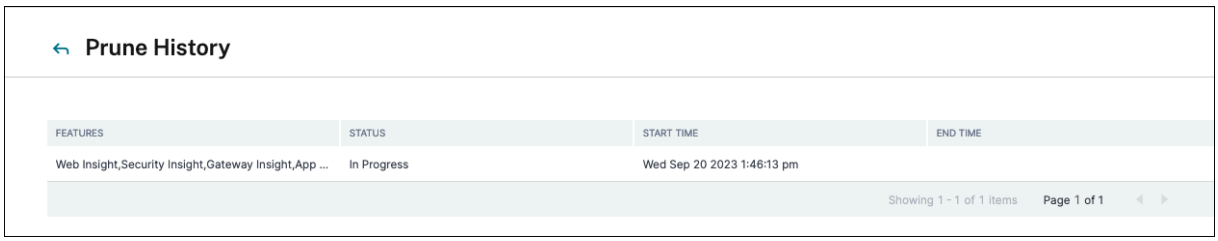
Ver el historial de podas

Haga clic en **Ver historial de podas** para obtener detalles sobre todas las actividades de poda que realizó en NetScaler ADM.



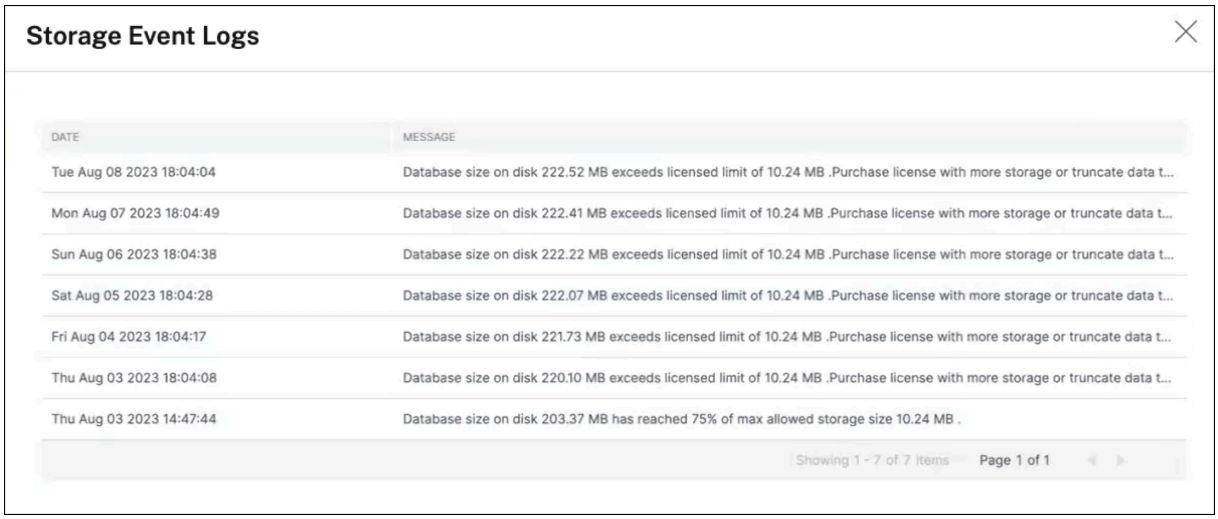
La página **Registros de poda: registros de tareas** muestra la lista de todas las tareas de eliminación, incluidos sus respectivos estados, hora de inicio y hora de finalización.

Para saber qué funciones se eliminaron en cada una de las operaciones de poda, seleccione una tarea y haga clic en **Registro de funciones**.



Ver registros de eventos de almacenamiento

Haga clic en **Registros de eventos de almacenamiento** para obtener información sobre todas las veces que sus datos superaron o alcanzaron el 75 % del límite de su licencia.



Revisar la directiva de retención de datos

La directiva de retención de datos se refiere a un conjunto de reglas y configuraciones que determinan cómo NetScaler ADM administra y mantiene los datos históricos a lo largo del tiempo. Esta directiva describe cuánto tiempo se almacenan los datos antes de que se eliminen automáticamente.

Si quiere reducir el espacio de almacenamiento que utilizan todas las distintas funciones, puede cambiar el tiempo que se guardan los datos en NetScaler ADM.

Utilice la página **Directiva de retención de datos** para modificar la configuración de almacenamiento de datos para:

- Mensajes de eventos
- Mensajes de Syslog
- Datos de informes de red

Para obtener más información sobre la configuración de almacenamiento de datos, consulte Directiva de retención de datos.

Notificar si se supera el límite de almacenamiento

Puede configurar notificaciones para que NetScaler ADM le envíe alertas cuando la capacidad de almacenamiento de datos supere los límites especificados.

Para ver y configurar las notificaciones del sistema:

1. En el mosaico **Acciones**, haga clic en **Notificar si se supera el límite de almacenamiento**.
2. En la página **Configurar notificaciones del sistema**, en la **categoría Eventos del sistema**, asegúrese de seleccionar la categoría **DataStorageExceeded** para recibir las notificaciones.

Puede especificar varios parámetros relacionados con cómo y cuándo se le envían las notificaciones a usted o a otros usuarios. Seleccione el método de comunicación preferido (por ejemplo, notificaciones por correo electrónico, Slack, PagerDuty y ServiceNow) y defina los destinatarios de las notificaciones.

Para obtener más información sobre cómo configurar los perfiles y enviar notificaciones, consulte Configurar notificaciones.

Directiva de retención de datos

January 30, 2024

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, 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 del sistema:

1. Vaya a **Configuración > Administración del almacenamiento de datos > Directiva de retención de**datos.
2. En la página **de depuración de datos**, haga clic en **Sistema**.
3. En la página **Sistema**, introduzca los siguientes detalles:
    - **Datos que se deben conservar (días)**: introduzca el número de días durante los que se deben conservar los datos. Debe especificar un valor entre 1 y 30.
    - **Valor umbral de depuración de datos (%): introduzca un límite umbral (en porcentaje) para establecerlo como condición para los procesos** de depuración o limpieza de datos. Cuando los datos de la base de datos alcanzan este porcentaje especificado de

capacidad de almacenamiento, se activan los procedimientos de depuración de datos para eliminarlos y liberar espacio.

- **Detalles de la eliminación automática**: seleccione **Activar la eliminación automática de datos si** quiere que la depuración de datos se inicie cuando se cumpla alguno de los siguientes criterios:
  - Se alcanza el valor umbral de **datos especificado en el valor umbral de Data Prune (%)**.
  - Se alcanza el número de días especificado en el valor **Datos que se deben conservar (días)**.
- **Configuración de ingesta de datos**: introduzca un límite umbral (en porcentaje) para establecerlo como condición para la ingesta de datos. Cuando los datos de la base de datos alcanzan este porcentaje especificado, la actividad de ingesta de datos se detiene. Debe especificar un límite entre el 50 y el 80%.

4. Haga clic en **Guardar** para guardar la configuración.

Configurar la configuración de syslog prune 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 después de los cuales los datos genéricos de syslog se eliminarán de NetScaler ADM.

Para configurar los valores de depuración de syslog de instancias:

1. Vaya a **Configuración > Administración del almacenamiento de datos > Directiva de retención de**datos.
2. En la página **de eliminación de datos**, haga clic en **Eventos de instancia**.
3. En el campo **Conservar datos genéricos de Syslog**, especifique el número de días entre 1 y 180.
4. Haga clic en **Guardar**.

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 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).

Para configurar los parámetros de poda del evento de instancia:

1. Vaya a **Configuración > Administración del almacenamiento de datos > Directiva de retención de**datos.
2. En la página **de eliminación de datos**, haga clic en **Eventos de instancia**.
3. **En el campo**Datos para conservar (días)**, introduzca el intervalo de tiempo, en días, durante el que quiere conservar los datos en el servidor NetScaler ADM y haga clic en Guardar.**

Configurar los ajustes de reducción de informes de red

Para limitar los datos de informes de red almacenados en NetScaler ADM, puede especificar el intervalo durante el que quiere conservar los datos históricos de informes de red.

Para configurar los parámetros de poda del evento de instancia:

1. Vaya a **Configuración > Administración del almacenamiento de datos > Directiva de retención de**datos.
2. En la página **Data Pruning**, haga clic en **Network Reporting**.
3. En el campo **Datos que se van a conservar (días)**, especifique el número de días comprendido entre 1 y 30.
4. Haga clic en **Guardar**.

NetScaler ADM como servidor proxy API

January 30, 2024

Además de poder recibir solicitudes de la API REST de NITRO para su propia funcionalidad de administración y análisis, NetScaler Application Delivery Management (NetScaler ADM) puede funcionar como un servidor proxy de API REST para sus instancias gestionadas. En lugar de enviar solicitudes de API directamente a las instancias gestionadas, los clientes de la API REST pueden enviar las solicitudes de API a NetScaler ADM. NetScaler 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 gestionada.

Como servidor proxy de API, NetScaler ADM le ofrece las siguientes ventajas:

- **Validación de solicitudes de API**. NetScaler ADM valida todas las solicitudes de API según las directivas configuradas de seguridad y control de acceso basado en roles (RBAC). NetScaler ADM también reconoce a los arrendatarios y garantiza que la actividad de la API no sobrepase los límites de los arrendatarios.

- **Auditoría centralizada**. NetScaler ADM mantiene un registro de auditoría de toda la actividad de la API relacionada con sus instancias gestionadas.
- **Administración de sesiones**. NetScaler ADM libera a los clientes de API de la tarea de mantener sesiones con instancias administradas.

Cómo funciona NetScaler ADM como servidor proxy de API

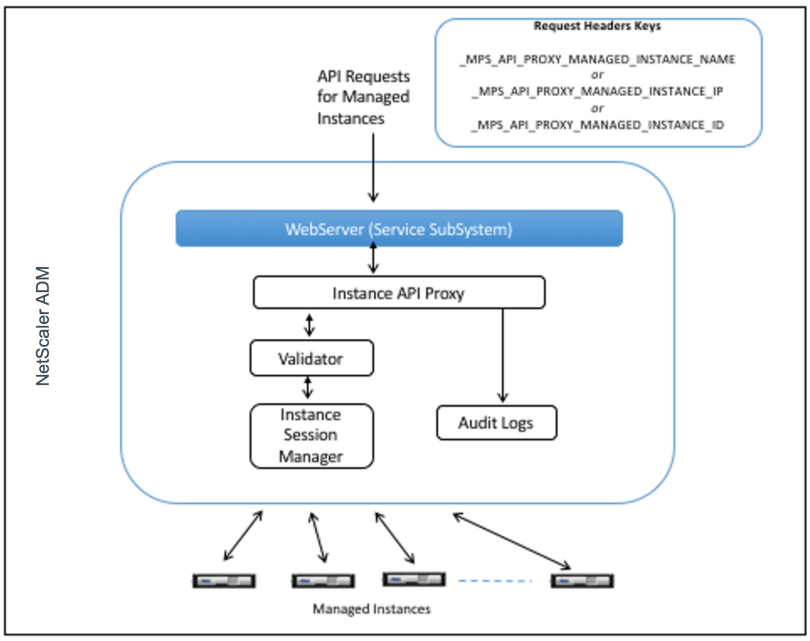
Cuando quiere que NetScaler ADM reenvíe una solicitud a una instancia administrada, configure el cliente de API para que incluya cualquiera de los siguientes encabezados HTTP en la solicitud de API:

valores de encabezado	Descripción
_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.
_MPS_API_PROXY_TIMEOUT	Valor de tiempo de espera para una solicitud de API de NITRO. Establezca el valor de tiempo de espera en segundos. Cuando se establece un tiempo de espera de proxy, ADM espera la duración especificada antes de agotar el tiempo de espera de la solicitud.
_MPS_API_PROXY_MANAGED_INSTANCE_USERNAME	Nombre de usuario para acceder a la instancia de ADC administrada.
_MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD	Contraseña para acceder a la instancia de ADC administrada.
_MPS_API_PROXY_MANAGED_INSTANCE_SESSID	Id. de sesión para acceder a la instancia administrada.

> **Nota:**
>
> En **Configuración > Administración > Configuraciones del sistema > Configuración básica**, si selecciona **Solicitar credenciales para el inicio de sesión de la instancia**, asegúrese de configurar el nombre de usuario y la contraseña de una instancia administrada. Como alternativa, también puede especificar el ID de sesión de instancia.

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 NetScaler ADM a identificar la instancia gestionada 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, NetScaler ADM reenvía la solicitud al motor de 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, NetScaler ADM identifica una sesión mantenida por el Administrador de sesiones de la instancia y, a continuación, envía la solicitud a la instancia administrada.

> **Nota**
>
> Asegúrese de que la opción **Solicitar credenciales para inicio de sesión de instancia** está inhabilitada. Para ello:
>
> 1. Vaya a **Configuración > Administración**.
> 2. En **Configuraciones del sistema**, seleccione **Sistema, Zona horaria, URL permitidas y Mensaje del día**.

Cómo usar NetScaler ADM como servidor proxy API

Los siguientes ejemplos muestran las solicitudes de API REST que un cliente de API envía a un servidor NetScaler ADM que tiene una dirección IP de 192.0.2.5. Se requiere NetScaler 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 las solicitudes de API a NetScaler ADM, el cliente de API debe:

- Inicie sesión en NetScaler 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/v1/config/login
Content-Type: application/json

{

    "login": {

        "username":"nsroot",
        "password":"nsroot"
      }

 }

<!--NeedCopy-->
```

NetScaler ADM responde a la solicitud de inicio de sesión con una respuesta que incluye el ID 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": "nsroot",

  "login": [
```



```
19
20      {
21
22
23        "tenant_name": "Owner",
24
25        "permission": "superuser",
26
27        "session_timeout": "36000",
28
29        "challenge_token": "",
30
31        "username": "",
32
33        "login_type": "",
34
35        "challenge": "",
36
37        "client_ip": "",
38
39        "client_port": "-1",
40
41        "cert_verified": "false",
42
43        "sessionid": "##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45        "token": "b2f3f935e93db6a"
46       }
47
48
49    ]
50
51   }
52
53  <!--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:

```
1      GET /nitro/v1/stat/lbvserver
2      Content-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5   <!--NeedCopy-->
```

Donde el valor del encabezado de cookie es el ID de sesión devuelto por la llamada a la API de inicio de sesión. Y el valor de _MPS_API_PROXY_MANAGED_INSTANCE_IP es la dirección IP del ADC.

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
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

         "lbvserver":{

             "name":"sample_lbvserver",
             "servicetype":"HTTP",
             "ipv46":"10.102.1.11",
             "port":"80"
          }

     }

<!--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:

```
    PUT /nitro/v1/config/lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

       "lbvserver":{

            "name":"sample_lbvserver",
            "appflowlog":"DISABLED"
         }

     }

<!--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
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--NeedCopy-->
```

Ejemplo 5: Descargue la configuración de ejecución de CLI en el ADC

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
1     GET /nitro/v1/config/nsrunningconfig
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6  <!--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

¿Es necesario habilitar el canal virtual EUEM en instancias de NetScaler Gateway implementadas en modo de salto único?

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el NetScaler ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual EUEM no está habilitado, los datos restantes de HDX Insight se seguirán mostrando en NetScaler ADM.

El canal virtual EUEM es un servicio predeterminado que se ejecuta en las aplicaciones Citrix Virtual Desktop (VDA). 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** > **NetScaler** y seleccione la instancia de NetScaler en la que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. En la página **Configurar análisis**, seleccione todos los servidores virtuales en los que quiere 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 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, 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, consultePara establecer los parámetros de AppFlow mediante la utilidad de configuración.

Después de agregar las instancias NetScaler, ¿NetScaler ADM comienza automáticamente a recopilar información analítica?

No. Habilite el análisis en los servidores virtuales alojados en instancias de NetScaler administradas por NetScaler ADM. Para obtener más información, consulte Cómo habilitar el análisis en instancias.

¿Es necesario acceder al dispositivo NetScaler individual para habilitar el análisis?

No. Todas las configuraciones se realizan desde la interfaz de usuario de NetScaler ADM, que enumera los servidores virtuales alojados en la instancia de NetScaler específica. Para obtener más información, consulte Cómo habilitar el análisis en instancias.

¿Cuáles son los tipos de servidores virtuales que se pueden enumerar en una instancia de NetScaler 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 conecto un disco adicional a NetScaler ADM?

Para adjuntar un disco adicional a NetScaler ADM:

1. Apague la máquina virtual NetScaler ADM.
2. En el hipervisor, 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 caso, debe adjuntar 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. Los 120 GB de espacio en disco existentes se utilizan para almacenar archivos principales, 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?

Un recopilador recibe los registros de AppFlow generados por el dispositivo NetScaler.

NetScaler ADM recibe tráfico de Security Insight y Web Insight de las instancias de NetScaler cuando la función AppFlow está habilitada. Cuando habilita la función AppFlow en una instancia de NetScaler,

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, NetScaler ADM no recibe el tráfico de las instancias.

Por ejemplo, se agregan cinco instancias de NetScaler 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.

¿Qué hace la habilitación de mediciones del lado del cliente?

Con las mediciones del lado del cliente habilitadas, ADM captura el tiempo de carga y las métricas de tiempo de representación para páginas HTML, mediante inyección HTML. Mediante estas métricas, los administradores pueden identificar problemas de latencia L7.

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 haber una situación en la que la autenticación externa falle por completo, incluso cuando haya 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 nuevo usuario 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 NetScaler ADM, vaya a **Configuración > 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 una 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, puede integrar NetScaler ADM con servidores de autenticación externos e importar información de grupos de usuarios desde los servidores de autenticación. Inicie sesión en NetScaler ADM y cree manualmente la misma información de grupo en NetScaler 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 los permisos para administrar las instancias de NetScaler, las instancias de NetScaler SDX, los servidores virtuales, etc., de modo que los usuarios de ese grupo solo puedan administrar 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 simultáneamente con NetScaler ADM?

Sí, puede usar trabajos de configuración para realizar la configuración en varias instancias de NetScaler.

¿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 NetScaler ADM conduce a la eliminación de certificados de las instancias de NetScaler?

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 NetScaler ADM, vaya a **Configuración > Administración de usuarios > Usuarios**.

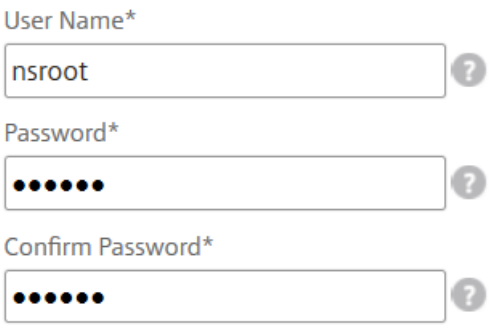
   Se muestra la **página Usuarios**.

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 interfaz gráfica de usuario, 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 de alta disponibilidad, si la contraseña se cambia en el nodo principal y si la opción Romper par de alta disponibilidad 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. Vaya a **Configuración > 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 NetScaler 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. Por lo tanto, no se admite la implementación de ADM en SAN.

¿Admite NetScaler ADM un disco adicional?

Sí. Una nueva instalación del par NetScaler ADM HA asigna 120 GB de almacenamiento de forma predeterminada. Para obtener más de 120 GB de almacenamiento, puede agregar un disco adicional para obtener un máximo de 3 TB de almacenamiento. 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 puede acceder a la dirección IP flotante y debe 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. Vaya a **Configuración > 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. Vaya a **Configuración > 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?

El procesador AMD es compatible con:

- **NetScaler ADM 13.1, compilación 4.43, o una versión posterior**.
- **Agente NetScaler ADM 13.1, compilación 17.42, o una versión posterior**.

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. Para revertir el par de alta disponibilidad como sitio principal, consulte Revertir configuraciones al sitio principal original

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 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, 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.

¿Qué son las reglas del evento?

Con NetScaler ADM, puede configurar reglas para supervisar eventos específicos. Las reglas de eventos facilitan la supervisión de muchos eventos generados en la infraestructura de NetScaler 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, 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 a NetScaler ADM y el envío de una notificación por SMS.

Administración de instancias

¿Qué sucede si una instancia de ADC no puede conectarse a ADM después de la asignación de ancho de banda cuando se utiliza la licencia de capacidad agrupada de NetScaler?

Si falla el latido entre la instancia de ADC y ADM, la instancia entra en un período de gracia de 30 días. Y una vez que se restablece la comunicación, las licencias de capacidad agrupada comienzan a

funcionar. Cuando se encuentra en período de gracia, las funciones ADC no se ven afectadas. Después de 30 días de período de gracia, la instancia de ADC inicia el reinicio en caliente y no tiene licencia.

¿Qué son los centros de datos en NetScaler ADM?

Un centro de datos NetScaler ADM es una agrupación lógica de las instancias de NetScaler en una ubicación geográfica específica. Cada servidor puede supervisar y administrar varias instancias de NetScaler dentro de un centro de datos. Puede usar el servidor NetScaler ADM para administrar datos como syslog, flujo de tráfico de aplicaciones y capturas SNMP de las instancias administradas. Para obtener más información sobre la configuración de centros de datos, consulte Cómo configurar centros de datos para Geomaps en NetScaler ADM.

¿Cuáles son los diferentes dispositivos NetScaler ADC compatibles con NetScaler ADM?

Las instancias son los dispositivos NetScaler ADC o los dispositivos virtuales que desea descubrir, administrar y supervisar desde NetScaler ADM. Debe agregar estas instancias al servidor de NetScaler ADM. Puede agregar los siguientes dispositivos NetScaler ADC y dispositivos virtuales a NetScaler ADM:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

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

¿Qué es un perfil de instancia?

NetScaler ADM utiliza un perfil de instancia para acceder a una instancia.

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, nsroot-profile es el perfil predeterminado para las instancias de NetScaler. Contiene las credenciales de administrador de NetScaler predeterminadas. Cuando cambias las credenciales necesarias para acceder a las instancias, puede definir perfiles de instancia personalizados para esas instancias.

¿Puedo redescubrir varias instancias de NetScaler 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 **Infraestructura > Instancias > NetScaler > VPX**, seleccione las instancias que quiere redescubrir y, en la lista **Acción**, haga clic en **Redescubrir**. Para obtener más información, consulte Cómo redescubrir varias instancias VPX.

¿Se puede instalar NetScaler ADM en NetScaler SDX?

No

¿Puedo agregar una instancia de NetScaler en el software ADM mediante una dirección IP pública?

Sí, puede hacerlo mediante la traducción de direcciones de red (NAT).

- Para agregar una sola instancia: utilice la IP NAT de la dirección IP pública de la instancia de ADC.
- Para agregar un par de HA de ADC: agregue las direcciones IP de NAT del par de HA en este formato:

  `<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`
- Para agregar un clúster de ADC: agregue todas las direcciones IP públicas de NAT de todas las instancias del clúster, cada una separada por una coma, y agregue la IP de NAT de la IP DEL CLÚSTER entre paréntesis o corchetes. Un formato de ejemplo: NAT1, NAT2, NAT3,(NATIP de CLUSTERIP).

Para obtener más información, consulte estos temas:

- Agregar instancias a NetScaler ADM
- Configuración de la traducción de direcciones de red

¿Cómo registrar un nodo de recuperación ante desastres si se cambian las credenciales del nodo de recuperación ante desastres?

Restablezca las credenciales del nodo de recuperación ante desastres (DR) a`nsrecover`/`nsroot` mediante el siguiente comando:

```
./mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

Para registrar un nodo de DR, siga los pasos de Implementar y registrar el nodo de DR de NetScaler ADM mediante la consola de DR.

StyleBooks

¿Se pueden usar StyleBooks para configurar diferentes instancias de NetScaler que se ejecutan en diferentes versiones del software NetScaler?

Sí, puede utilizar StyleBooks para configurar diferentes instancias de NetScaler 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 al mismo tiempo y se produce un error en la configuración de una instancia de NetScaler, ¿qué sucede?

Si se produce un error al aplicar la configuración a una instancia de NetScaler, la configuración no se aplica a más instancias y se deshacen las configuraciones ya aplicadas.

¿Las copias de seguridad de NetScaler realizadas a través de NetScaler incluyen configuraciones aplicadas a través de StyleBooks?

Sí

Administración del sistema

¿Puedo asignar un nombre de host a mi servidor NetScaler ADM?

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 realizar una copia de seguridad y restaurar la configuración de NetScaler 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, consulteCómo realizar una copia de seguridad y restaurar la configuración en NetScaler 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 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 después de los cuales se eliminarán todos los datos genéricos de Syslog, los datos de AppFirewall y los datos de NetScaler Gateway de NetScaler ADM.

¿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 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 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 mediante el puerto 443?

No, no puede configurar el equilibrio de carga del par de NetScaler ADM HA en una instancia de NetScaler mediante el puerto 443.

Cuando configura `http-ecv` y `https-ecv` supervisa en NetScaler, 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, ¿se puede usar ese archivo de copia de seguridad para restaurar la configuración de otra instancia de NetScaler a través de NetScaler ADM?

Sí. Descargue el archivo de copia de seguridad de NetScaler ADM, cárguelo en el repositorio de copias de seguridad de otra instancia de NetScaler 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 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 copia de seguridad 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.

¿Podemos obligar a NetScaler ADM a usar una dirección SNIP para comunicarse con las instancias de NetScaler, en lugar de usar la dirección NSIP del servidor NetScaler ADM?

Sí, puede agregar una dirección SNIP (con administración habilitada) en NetScaler ADM para comunicarse con instancias de NetScaler.

Cuando hago copias de seguridad de instancias de NetScaler en NetScaler ADM, ¿el resultado es una copia de seguridad completa o básica?

Las copias de seguridad de las instancias de NetScaler 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 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 se actualizan con los últimos detalles del nodo principal como destino de captura SNMP de forma predeterminada.

El nuevo nodo principal (activo) de NetScaler ADM comprueba si el nodo activo anteriormente estaba configurado como el recopilador AppFlow o servidor syslog; si lo era, el nuevo primario 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 en los nodos de alta disponibilidad de NetScaler ADM?

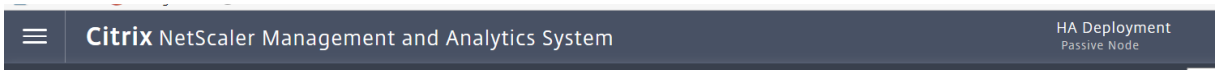
Todas las instancias de NetScaler son administradas por el nodo principal de NetScaler ADM.

¿Cómo se administran las licencias de servidor virtual si hay una conmutación por error de alta disponibilidad de NetScaler ADM?

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. Vuelva a aplicar las licencias en el nuevo primario antes de que finalice el período de gracia. Para obtener alternativas, póngase en contacto con el soporte de NetScaler.

¿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 se marca 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 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/