Servicio NetScaler Console

Machine translated content

Disclaimer

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

Contents

Overview

January 26, 2024

El servicio NetScaler Console (anteriormente denominado servicio NetScaler ADM) es una solución basada en la web para administrar todas las implementaciones de NetScaler, que incluyen NetScaler MPX, NetScaler VPX, NetScaler SDX, NetScaler CPX, NetScaler BLX y NetScaler Gateway er Gateway que se implementan en las instalaciones o en la nube.

Puede utilizar esta solución en la nube para administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada y centralizada basada en la nube. NetScaler Console proporciona todas las capacidades necesarias para configurar, implementar y administrar rápidamente la entrega de aplicaciones en las implementaciones de NetScaler y con análisis detallados del estado, el rendimiento y la seguridad de las aplicaciones.

NetScaler Console ofrece las siguientes ventajas:

- **Ágil**: Fácil de operar, actualizar y consumir. El modelo de servicio de NetScaler Console está disponible en la nube, lo que facilita el funcionamiento, la actualización y el uso de las funciones que ofrece NetScaler Console. La frecuencia de las actualizaciones, combinada con la función de actualización automatizada, mejora rápidamente la implementación de NetScaler.
- **Tiempo de obtención de valor** más rápido: Logro de objetivos empresariales más rápido. A diferencia de la implementación local tradicional, puede usar la consola de NetScaler con unos pocos clics. No solo ahorra el tiempo de instalación y configuración, sino que también evita perder tiempo y recursos en posibles errores.
- **Administración de múltiples sitios**: panel único para instancias en centros de datos de varios sitios. Con la consola de NetScaler, puede administrar y supervisar los NetScaler que se encuentran en varios tipos de implementaciones. Dispone de una gestión integral para los NetScalers implementados en las instalaciones y en la nube.
- **Eficiencia operativa**: Forma optimizada y automatizada de lograr una mayor productividad operativa. Con la consola NetScaler, sus costos operativos se reducen al ahorrar tiempo, dinero y recursos en el mantenimiento y la actualización de las implementaciones de hardware tradicionales.
- **Visibilidad del tráfico de Internet en tiempo real**: Experiencia de usuario mejorada con el análisis del tráfico de Internet en tiempo real. Con la consola de NetScaler, puede recopilar datos reales de monitoreo de usuarios de los clientes a medida que acceden a las aplicaciones en nubes, centros de datos y CDN, y crear una imagen holística del estado de Internet. El tráfico se dirige a las ubicaciones con la latencia más baja y la mejor disponibilidad para garantizar una experiencia de usuario óptima.

- **Aplicaciones en varios sitios**: Cree, configure y entregue una aplicación en varios sitios. Con la consola de NetScaler, puede configurar, entregar y administrar aplicaciones en varios entornos de nube para lograr una alta disponibilidad y confiabilidad.

Cómo funciona NetScaler Console

NetScaler Console está disponible como servicio en Citrix Cloud. Después de registrarse en Citrix Cloud y comenzar a utilizar el servicio, instale agentes en el entorno de red o inicie el agente integrado en las instancias. A continuación, agregue las instancias que quiere administrar al servicio.

Un agente permite la comunicación entre la consola de NetScaler y las instancias administradas del centro de datos. El agente recopila datos de las instancias administradas de la red y los envía a la consola de NetScaler.

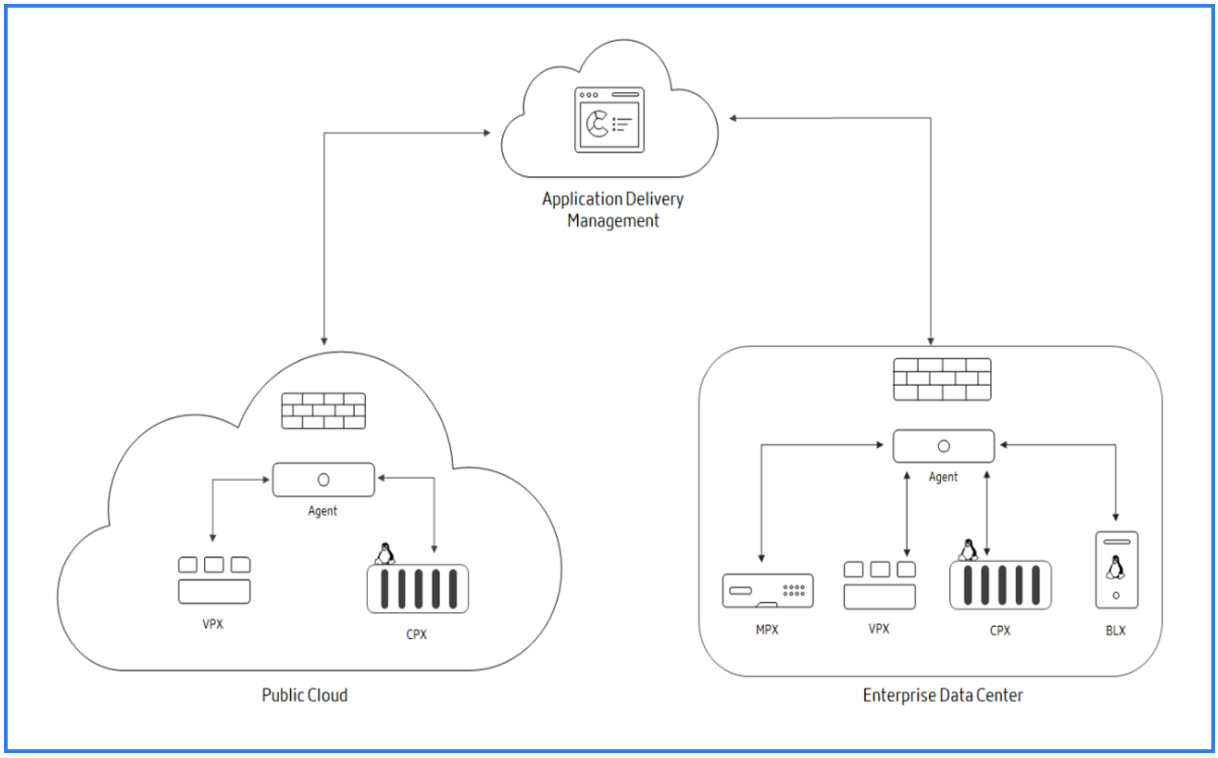
Cuando agrega una instancia a NetScaler Console, se agrega implícitamente como destino de captura y recopila un inventario de la instancia.

El servicio recopila detalles de instancia como:

- Nombre de host
- Versión de software
- Configuración en ejecución y guardada
- Certificados
- Entidades configuradas en la instancia, etc.

NetScaler Console sondea periódicamente las instancias administradas para recopilar información. Para obtener más información, consulte Gobernanza de datos.

La siguiente imagen ilustra la comunicación entre el servicio, los agentes y las instancias (MPX, VPX, CPX, BLX):



Para incorporarse a NetScaler Console y ver cómo funciona, consulte Introducción ysus subtemas.

Funciones y soluciones

January 26, 2024

Este documento describe las funciones que admite la consola de NetScaler.

Análisis y administración de aplicaciones

La función de análisis y administración de aplicaciones de NetScaler Console refuerza el enfoque centrado en las aplicaciones para ayudarlo a abordar diversos desafíos de entrega de aplicaciones. Este enfoque le brinda visibilidad de las puntuaciones de estado de las aplicaciones, le ayuda a determinar los riesgos de seguridad y le ayuda a detectar anomalías en los flujos de tráfico de las aplicaciones y a tomar medidas correctivas.

- Análisis del rendimientode 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 seguridadde aplicaciones: el panel de seguridad de aplicaciones proporciona una vista integral del estado de seguridad de sus aplicaciones. Por ejemplo, muestra métricas de se-

guridad 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 detectadas de NetScaler.

- Análisis inteligente de aplicaciones: la función de análisis inteligente de aplicaciones proporciona una solución fácil y escalable para monitorear y solucionar problemas de las aplicaciones que se entregan a través de los dispositivos NetScaler. Intelligent App Analytics no solo supervisa todos los niveles de las transacciones de las aplicaciones, sino que también utiliza técnicas de aprendizaje automático para definir los patrones de tráfico normales en la red y detectar anomalías. Esta función reduce el tiempo total de entrega y mejora el tiempo de actividad general de la aplicación.

StyleBooks

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 Skype for Business.

Administración de instancias

Le permite administrar las instancias de NetScaler, NetScaler Gateway y Citrix Secure Web Gateway.

Gestión de eventos

Los eventos representan ocurrencias de eventos o errores en una instancia administrada de NetScaler. Por ejemplo, cuando se produce un error del sistema o un cambio en la configuración, se genera un evento y se graba en NetScaler Console. Las siguientes son las funciones relacionadas que puede configurar o ver mediante NetScaler Console:

- Creación de reglas de eventos
- Uso de NetScaler Console para exportar mensajes de syslog

Administración de certificados

NetScaler Console optimiza todos los aspectos de la administración de certificados para 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.

Administración de la configuración

NetScaler Console le permite crear trabajos de configuración que le ayudan a realizar tareas de configuración, como la creación de entidades, la configuración de funciones, la replicación de los cambios

de configuración, las actualizaciones del sistema y otras actividades de mantenimiento con facilidad en varias instancias. Las plantillas y los trabajos de configuración simplifican las tareas administrativas más repetitivas y las convierte en una sola tarea en NetScaler Console.

Auditoría de configuración

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

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

Gestión de licencias

Le permite administrar las licencias de NetScaler configurando NetScaler Console como administrador de licencias.

- Capacidad agrupada de NetScaler: un grupo de licencias común desde el que la instancia de NetScaler puede extraer una licencia de instancia y solo el ancho de banda que necesite. Cuando la instancia ya no requiere estos recursos, vuelve a registrarlos en el grupo común, haciendo que los recursos estén disponibles para otras instancias que los necesiten.
- Licencias de registro y salida deNetScaler VPX : NetScaler Console asigna las licencias a las instancias de NetScaler VPX a pedido. Una instancia de NetScaler VPX puede extraer la licencia de la consola de NetScaler cuando se aprovisiona una instancia de NetScaler VPX o volver a consultar su licencia en NetScaler Console cuando se elimina o destruye una instancia.

Informes de red

Puede optimizar el uso de los recursos supervisando los informes de red en NetScaler Console.

Analytics

Proporciona una forma fácil y escalable de analizar los diversos conocimientos de los datos de las instancias de NetScaler para describir, predecir y mejorar el rendimiento de las aplicaciones. Puede utilizar una o más funciones de análisis simultáneamente.

- HDX Insight: proporciona visibilidad integral del tráfico ICA que pasa por NetScaler. HDX Insight permite a los administradores ver en tiempo real las métricas de latencia de los clientes y de la red, los informes históricos, los datos de rendimiento integrales y la solución de problemas de rendimiento.
- Web Insight: proporciona visibilidad de las aplicaciones web empresariales. 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 procesa los datos de NetScaler mediante un algoritmo de aproximación. Proporciona los 1000 registros principales de las métricas relacionadas con las aplicaciones web de su empresa.

- Gateway Insight: proporciona visibilidad de 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 para ayudarlo a evaluar el estado de seguridad de sus aplicaciones y tomar medidas correctivas para proteger sus aplicaciones.
- SSL Insight: proporciona visibilidad de las transacciones seguras en la web (HTTPs). Permite a los administradores de TI monitorear todas las aplicaciones web que ofrece NetScaler al proporcionar una supervisión histórica, en tiempo real e integrada de las transacciones web. SSL Insight procesa los datos de NetScaler mediante un algoritmo de aproximación. Proporciona los 1000 registros principales de las métricas relacionadas con las transacciones web de su empresa.

Control de acceso por roles

El control de acceso basado en roles (RBAC) le permite conceder permisos de acceso en función de las funciones de los usuarios individuales dentro de su empresa. El primer usuario de una organización que inicia sesión con credenciales de Citrix Cloud tiene la función de superadministrador que, de forma predeterminada, tiene todos los permisos de acceso. A los demás usuarios de esa organización, que posteriormente crea el administrador, se les otorgan funciones que no son de administrador.

Subscriptions

Proporciona una vista del panel de control de las suscripciones que ha adquirido.

De forma predeterminada, se le asigna una cuenta Express. Con esta cuenta, puede administrar los recursos limitados de NetScaler Console. Para obtener más información, consulte Administrar los recursos de NetScaler Console mediante una cuenta Express.

Las siguientes funciones de la consola NetScaler no están disponibles actualmente:

- Implementación
  - Migración de Citrix Insight Center a NetScaler Console
  - Integración de la consola NetScaler con el Director de escritorios virtuales de Citrix
- Análisis: TCP Insight y Video Insight
- Configuración limitada del sistema
- Orchestration
  - Integración con OpenStack y VMware NSX Manager

- Automatización de NetScaler en el modo híbrido de Cisco ACI
- Container Orchestration: Integración con Mesos/Marathon y Kubernetes

Notas de la versión

January 26, 2024

Las notas de la versión de NetScaler Console (anteriormente denominada servicio NetScaler ADM) describen las nuevas funciones, las mejoras de las funciones existentes, los problemas resueltos y los problemas conocidos disponibles en una versión de servicio.

Para obtener más información, consulte:

- Novedades
- Versiones anteriores

De forma predeterminada, el agente de NetScaler se actualiza automáticamente a la última versión de NetScaler Console. Puede ver los detalles del agente en la página **Infraestructura > Instancias > Agentes**. También puede especificar la hora a la que quiere que se realicen las actualizaciones del agente. Para obtener más información, consulte Configurar los ajustes de actualización del agente.

Novedades

September 2, 2024

25 de julio de 2024

Problema resuelto

Infraestructura En **Infraestructura > Trabajos de actualización**, al actualizar una instancia de NetScaler que tiene directivas clásicas, la validación previa a la actualización muestra la instancia como **Instancias cuya actualización está bloqueada** y la actualización no se realiza.

Solución temporal: Antes de actualizar una instancia, le recomendamos que convierta las directivas clásicas en avanzadas para las funciones compatibles con la herramienta NSPEPI. Para obtener más información, consulte Consideraciones de actualización para configuraciones con directivas clásicas.

[NSADM-113851]

Telemetría Como parte del programa de telemetría de NetScaler, NetScaler Console ya no comprueba la siguiente configuración cada 24 horas ni la envía a las instancias de NetScaler. Anteriormente, la configuración se comprobaba cada 24 horas y, si faltaba, se enviaba a las instancias de NetScaler:

```
enable ns feature AppFlow
add analytics profile telemetry_metrics_profile -type timeseries -
    outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "
    ./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency
    300
```

[NSADM-114375]

15 de julio de 2024

Infraestructura

Ver y exportar direcciones IP propiedad de NetScaler en la GUI de NetScaler Console Ahora puede ver y exportar las direcciones IP propiedad de NetScaler (**Infraestructura > Instancias > IP propiedad de NetScaler**) en la GUI de NetScaler Console.

Para obtener más información, consulte Ver direcciones IP propiedad de NetScaler.

[NSADM-88798, NSADM-91769]

Licencias

Consulte los detalles de las instancias VPX aprovisionadas en una instancia SDX en el panel de licencias Flexed En el panel de licencias flexibles (**NetScaler Licensing > Flexed Licensing > Dashboard**), en **Licensed NetScalers**, puede ver la cantidad de instancias VPX que se han retirado para NetScalerSDX. Ahora puede hacer clic en el recuento para ver los detalles de la instancia VPX aprovisionada para ese SDX, como el nombre de la instancia, la dirección IP, el rendimiento (MBPS) y la edición.

Anteriormente, solo podía ver el número total de instancias VPX retiradas para ese SDX.

[NSADM-105358]

Vea los detalles del ID de host y el número de serie de MPX/SDX en las licencias de capacidad cero En **NetScaler Licensing > Licencias de capacidad cero**, ahora puede ver los detalles del **ID de host** y el **número de serie** de las instancias MPX y SDX.

[NSADM-100327]

Problemas resueltos

Los problemas que se abordan en la compilación del 15 de julio de 2024.

Infraestructura

- Al modificar una instancia en NetScaler Console (Infraestructura > Instancias > NetScaler), por ejemplo, al cambiar el sitio o el perfil de administrador, los pares clave-valor de las etiquetas asociadas a la instancia se invierten.

  [NSHELP-38083]

- En Config Job, al ejecutar la plantilla ShowConfiguration simultáneamente en los NetScalers principales y secundarios de un par de alta disponibilidad, al hacer clic en Descargar archivos de resultados, se descarga el archivo solo para la instancia secundaria.

  [NSHELP-37831]

- Cuando no hay ningún panel en Network Reporting (Infraestructura > Network Reporting), aparece el siguiente mensaje de error:

  "No tiene acceso a esta página"

  Este mensaje de error se puede ignorar y no le impide crear paneles.

  [NSADM-113332]

- Las capturas SNMP no se reciben en el servicio NetScaler Console cuando se configura mediante el agente integrado.

  [NSHELP-38191]

StyleBooks En la GUI de NetScaler Console, al editar un paquete de configuración para usar un StyleBook diferente, la actualización no funciona según lo esperado.

[NSADM-110351]

09 de julio de 2024

Función para la identificación y remediación de CVE-2024-5491 y CVE-2024-5492

El asesoramiento de seguridad del servicio NetScaler Console ahora admite la identificación y la corrección de CVE-2024-5491 y CVE-2024-5492.

- La identificación de CVE-2024-5491 requiere una combinación de escaneo de versión y configuración.

- La identificación de CVE-2024-5492 requiere un escaneo de versiones.

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 Console para actualizar las instancias de NetScaler, consulte Usar trabajos para actualizar las instancias de NetScaler.

Para obtener más información, consulte el Boletín de seguridad.

> **Nota:**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde un par de horas en finalizar y reflexionar sobre el impacto de los CVE-2024-5491 y CVE-2024-5492 en el módulo de asesoramiento de seguridad. Para ver el impacto con mayor rapidez, puede iniciar un escaneo bajo demanda haciendo clic en **Escanear ahora**.

18 de junio de 2024

Telemetría

Programa de telemetría de NetScaler Como cliente actual de NetScaler Console, debe cumplir con el programa de telemetría de NetScaler, que exige la recopilación de datos de telemetría de uso de licencias y funciones. Los datos de telemetría se cargan automáticamente cada 24 horas y no es necesaria ninguna acción por su parte.

- Para obtener más información, consulte el programa de telemetría de NetScaler.
- Para obtener más información sobre los parámetros de telemetría, consulte Gobierno de datos.

[NSADM-113300]

11 de junio de 2024

Análisis

El recopilador de métricas y el análisis del uso durante períodos ajustados están habilitados a nivel del servidor virtual El recopilador de métricas y el análisis de uso eficiente ahora están habilitados a nivel de servidor virtual en lugar de a nivel de instancia. Con esta mejora, el recopilador de

métricas y el análisis de uso eficiente permanecen habilitados solo en sus servidores virtuales activos con mucho tráfico.

Para revisar sus servidores virtuales y habilitar el **recopilador de métricas** y el uso eficiente en otros servidores virtuales, vaya a **Configuración > Configuración de análisis** y haga clic en **Configurar métricas** en **Resumen de métricas del servidor virtual**.

Para obtener más información, consulte Configurar el análisis inteligente de aplicaciones.

[NSADM-111609]

Asigne un perfil de red en las instancias de NetScaler para la recopilación de métricas Cuando habilita el recopilador de métricas para los servidores virtuales en NetScaler Console, los datos de métricas de NetScaler se exportan a NetScaler Console a través de la dirección IP de subred (SNIP) de NetScaler. 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. 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 un perfil de red a la instancia de NetScaler para recopilar métricas. Metrics Collector envía los datos del contador de NetScaler a NetScaler Console, que se utiliza para detectar problemas en las aplicaciones. Vaya a **Infraestructura > Instancias > NetScaler**, seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Configurar perfiles de red para Metrics Collector**.

Para obtener más información sobre la asignación de un perfil de red, consulte Asignar un perfil de red para la instancia de NetScaler gestionada.

[NSADM-111138]

Integración de observabilidad: vea los detalles de la suscripción fallida a NetScaler En **Observability Integration**, al configurar una suscripción de NetScaler a Splunk o Prometheus, ahora puede ver los registros detallados de las suscripciones fallidas. Como administrador, al usar estos registros, puede analizar el motivo del error de la suscripción.

Para obtener más información, consulte Ver los registros de configuraciones fallidas

[NSADM-109022]

Eliminación de la opción de exportación periódica para WAF y Bot Insight en Observability Integration La opción de exportación periódica para WAF y Bot Insight ahora se elimina al configurar la exportación de información de NetScaler Console a herramientas de observabilidad (como Splunk, New Relic y Microsoft Sentinel). Dado que las infracciones de WAF y Bot son cruciales, se recomienda utilizar la opción de exportación en tiempo real para exportar la información en tiempo real siempre que se produzca.

Cualquier suscripción existente con una configuración de exportación periódica para WAF y Bot se cambia automáticamente a exportación en tiempo real.

[NSADM-109019]

Infraestructura

Compatibilidad con el aprovisionamiento "basado en aplicaciones" El servicio NetScaler Console introduce el aprovisionamiento "basado en aplicaciones"para AWS y Azure. Esta función optimiza y simplifica las implementaciones de NetScaler en los centros de datos en la nube, lo que permite la entrega eficiente de aplicaciones desde estos entornos.

Para obtener más información, consulte Aprovisionamiento basado en aplicaciones en AWS y Aprovisionamiento basado en aplicaciones en Azure.

[NSADM-108491]

Problemas resueltos

Los problemas que se abordan en la compilación del 11 de junio de 2024.

Análisis

- Un proceso de la Consola/Agente de NetScaler puede bloquearse debido a un daño en la memoria.

  [NSHELP-38032]

- En **Web Insight**, los detalles del servidor virtual de equilibrio de carga configurado detrás del servidor virtual de conmutación de contenido no están visibles en los informes diarios, semanales y mensuales.

  [NSHELP-37713]

Infraestructura

- Cuando los usuarios que no son administradores intentan ver las estadísticas de los servidores virtuales en NetScaler Console (**Infraestructura > Funciones de red**), aparece el siguiente mensaje de error:

  "No está autorizado a acceder "

  [NSHELP-37977]

- En una configuración de alta disponibilidad, cuando se utilizan las "mastools"del agente integradas junto con las particiones, el estado de la instancia secundaria de NetScaler es "desconocido"en el panel SSL (**Infraestructura > Panel SSL**) y en el equilibrio de carga (**Infraestructura > Funciones de red > Equilibrio de carga**).

  [NSHELP-37902]

StyleBooks

- Al editar los paquetes de configuración, no se aplican los cambios que realice en las ACL o en las reglas de enrutamiento basado en políticas (PBR), como agregar, actualizar o eliminar.

  [NSHELP-37656]

5 de junio de 2024

Análisis

Integrar NetScaler Console con Microsoft Sentinel En **Observability Integration**, ahora puede configurar la integración de NetScaler Console con Microsoft Sentinel para exportar y ver información en Microsoft Sentinel. Para una integración exitosa, asegúrese de que se cumplen los siguientes requisitos previos:

- **Suscripción a Azure**: una suscripción a Azure para implementar y usar Microsoft Sentinel.
- **Espacio de trabajo de análisis de registros**: se requiere un espacio de trabajo para almacenar y analizar los datos recopilados.
- **Funciones de IAM**: se deben establecer niveles de permisos como lector y colaborador para el espacio de trabajo.
- **Tablas personalizadas**: para almacenar y enviar los datos de NetScaler Console al espacio de trabajo.

Para obtener más información, consulte Integración con Microsoft Sentinel

[NSADM-108930]

Plataforma

Compatibilidad con la versión 9.x de OpenSSH La versión de OpenSSH de NetScaler ahora se ha actualizado de la 8.x a la 9.x.

[NSPLAT-29640]

StyleBooks

Opción Guardar como borrador en los paquetes de configuración Ahora puede guardar el paquete de configuración como borrador. Para guardar la configuración como borrador, siga estos pasos:

1. Vaya a **Aplicaciones > Configuración > Paquetes de configuración**.
2. En la página **Configuraciones**, haga clic en **Agregar**.
3. Seleccione un libro de estilos y haga clic en **Seleccionar**.
4. En la página **Crear configuración**, haga clic en **Guardar como borrador**.

Los borradores guardados aparecen en la pestaña **Borrador de configuraciones** , en **Configuraciones pendientes**.

Para obtener más información, consulta Guardar un paquete de configuración como borrador.

[NSADM-110734]

Opción de programación en los paquetes de configuración Ahora puede programar la implementación de los paquetes de configuración recién creados. Para crear una programación para un nuevo paquete de configuración, siga estos pasos:

1. Vaya a **Aplicaciones > Configuración > Paquetes de configuración**.
2. En la página **Configuraciones**, haga clic en **Agregar**.
3. Seleccione el libro de estilos y haga clic en **Seleccionar**.
4. En la página **Crear configuración**, en **Ejecución**, seleccione **Más tarde** en la lista **Modo de ejecución**.
5. Seleccione la fecha y hora deseadas para la programación.

En el caso de los paquetes de configuración implementados, puede programar cuándo publicar las actualizaciones y cuándo eliminar el paquete de configuración. Las opciones de programación están disponibles al editar un paquete de configuración implementado.

Para obtener más información, consulte Crear una programación para un paquete de configuración.

[NSADM-110728]

Problemas resueltos

Los problemas que se abordan en la compilación del 5 de junio de 2024.

Análisis

- Los detalles del **estado de la aplicación** en el panel de información **general** no muestran los mismos detalles disponibles en la **puntuación de la aplicación** en el **panel de control de aplicaciones**.

  [NHELP-37720]

- Si se administran más de 25 000 servidores virtuales a través de NetScaler Console, es posible que el panel de aplicaciones tarde más en cargar los detalles.

  [NSADM-111705]

Infraestructura

- Las reglas de eventos no generan las acciones esperadas cuando cambia el estado del grupo de servicios.

  [NSHELP-37616]

StyleBooks

- Al agregar datos de recopilación con valores vacíos para campos de tipo dirección IP, entero o booleano a la fuente de datos personalizada en StyleBooks, la operación puede fallar.

  [NHELP-37826]

- Al crear un paquete de configuración desde la GUI de NetScaler Console, es posible que el sistema devuelva una lista vacía para los parámetros que hacen referencia a la fuente de datos ADC administrada integrada.

  [NHELP-37824]

- Al intentar crear un paquete de configuración o realizar una ejecución en seco, las operaciones pueden fallar si se cumplen las dos condiciones siguientes:

  - La definición de StyleBook hace referencia a otro StyleBook dentro de la sección de componentes.
  - Al asignar parámetros de tipo ‘‘datum’’a las propiedades entre el StyleBook actual y el StyleBook al que se hace referencia.

  [NHELP-37793]

22 de mayo de 2024

Análisis

Actualice de forma masiva los servidores virtuales SSL mediante la tarea Actualización de la calificación SSL A+ En **Tareas**, ahora puede ver la tarea **Actualización de la calificación SSL A+**. El proceso actual de actualización de la calificación SSL a A+ en **Panel de aplicaciones** le permite actualizar solo una aplicación a la vez. Mediante la tarea **Actualización de la calificación SSL A+**, puede realizar una actualización masiva.

NetScaler Console revisa la configuración SSL del servidor virtual de aplicaciones con el perfil de front-end seguro de NetScaler e identifica las aplicaciones que no tienen una calificación A+. La tarea **Actualización de la calificación SSL A+** muestra las aplicaciones que no tienen la calificación A+. Como administrador, puede seleccionar aplicaciones y realizar una actualización masiva para lograr el cumplimiento de SSL.

Para obtener más información, consulte Recomendaciones y tareas prácticas.

[NSADM-108164]

Licencias

Detalles de uso real en Informes de licencias flexibles En el panel **Informes de licencias flexibles** (**NetScaler Licensing > Flexed Licensing > Informes**), ahora puede ver el uso real del ancho de banda y el rendimiento, lo que le permite ver los detalles del consumo (uso máximo y uso promedio). Anteriormente, el panel solo mostraba los detalles de la asignación y los derechos.

Además, las siguientes mejoras también están disponibles en el panel Informes de licencias flexibles:

- Filtre para ver los detalles de las instancias de NetScaler seleccionadas.
- Opción para exportar detalles en formato PDF, PNG y JPEG.
- El ancho de banda pasa a denominarse capacidad de rendimiento.

Para obtener más información, consulte Informes de licencias flexibles

[NSADM-97093]

StyleBooks

Cree expresiones de directivas de NetScaler en StyleBooks La GUI de StyleBooks ahora le permite crear expresiones de directivas de NetScaler seleccionando elementos de las listas, lo que le

ayuda a crear expresiones de forma más rápida y precisa. Para que el editor de expresiones de directiva esté disponible para un parámetro, especifique el atributo `is_policy_expression` GUI en la definición de parámetros de StyleBooks.

Para obtener más información, consulte Expresiones de directiva en StyleBooks.

[NSADM-12651]

Problemas resueltos

Los problemas que se abordan en la compilación del 22 de mayo de 2024.

Infraestructura En **Config Job**, al ejecutar la plantilla **ShowConfiguration** simultáneamente en los NetScalers principales y secundarios de un par de alta disponibilidad, al hacer clic en **Descargar archivos de resultados**, se descarga el archivo solo para la instancia secundaria.

[NSHELP-37831]

StyleBooks Al eliminar una instancia de NetScaler que usa una dirección IP de subred (SNIP) para el acceso de administración desde NetScaler Console y, a continuación, volver a agregar la instancia, las operaciones de los paquetes de configuración creados antes de eliminar la instancia pueden fallar.

[NSHELP-37786]

23 de abril de 2024

Análisis

Compatibilidad con exportación periódica de datos para instancias de NetScaler personalizadas Al crear una suscripción para la exportación de datos de NetScaler Console a Splunk o New Relic, ahora puede seleccionar la **exportación periódica** (diaria o cada hora) y aplicarla a las instancias personalizadas. Anteriormente, no se permitía la exportación periódica de datos a las instancias personalizadas.

[NSADM-109020]

Infraestructura

Alerta de evento adicional para la utilización del disco NetScaler Console ahora le permite establecer un valor umbral adicional para las alarmas de utilización del disco. Con este valor de umbral,

puede establecer un límite de nivel inferior para recibir alertas antes de que se supere un umbral superior. Para configurar el umbral de nivel inferior, vaya a **Parámetros > SNMP > Modificar** y habilite **Configurar un umbral de nivel inferior**.

Para obtener más información, consulte Configurar y ver las alarmas del sistema.

[NSADM-97285]

Problemas resueltos

Los problemas que se abordan en la compilación del 23 de abril de 2024.

Infraestructura

- Cuando intenta exportar el informe de NetScaler Console como una instantánea en **Infraestructura > Instancias > NetScaler**, la página deja de responder.

  [NSHELP-37689]

- Si se administran más de 10 instancias de NetScaler a través de un agente en NetScaler Console, se produce un error en el subsistema de inventario de agentes. Como resultado, NetScaler Console no obtiene los datos de configuración de NetScaler más recientes.

  [NSHELP-37749]

Licencias

- El número de instancias que se muestra en el panel de licencias flexibles es incorrecto.

  [NSHELP-37733]

Seguridad

- Al exportar los registros de infracciones en forma tabular mediante las opciones **Exportar ahora** o **Programar exportación** en **Seguridad > Infracciones de seguridad > Todas las infracciones > Detalles de la infracción**, solo se incluyen en el informe los registros visibles en la vista de página actual, independientemente del número de registros seleccionados en **Número de registros para exportar**.

  [NSHELP-37562]

10 de abril de 2024

Análisis

Integración de observabilidad: Función para configurar la exportación de métricas y registros de auditoría de NetScaler a Splunk En **Parámetros > Integración de observabilidad**, ahora puede configurar la exportación de los registros de auditoría y métricas de NetScaler a Splunk.

Para obtener más información, consulte Configurar la exportación de métricas y registros de auditoría de NetScaler a Splunk.

[NSADM-108858]

Infraestructura

Acceder a la GUI de NetScaler a través del nombre de host Cuando se conecta a NetScaler a través de **Infraestructura > Instancias > NetScaler**, al hacer clic en el nombre del host, se establece ahora la conexión a la GUI de NetScaler a través del nombre del host. Anteriormente, al hacer clic en el nombre del host o en la dirección IP, se iniciaba la conexión a la GUI de NetScaler a través del NSIP.

[NSADM-108790]

Ver las discrepancias entre los nodos de alta disponibilidad durante la actualización de versión Ahora puede ver las discrepancias de configuración entre el nodo principal y el nodo secundario mientras actualiza la implementación de alta disponibilidad de NetScaler. Puede revisar las discrepancias y decidir si quiere continuar o detener la actualización. Para usar esta función, vaya a **Infraestructura > Trabajos de actualización** y consulte las discrepancias en la ficha **Validación previa a la actualización**.

Para obtener más información, consulte Trabajos de actualización.

[NSADM-103826]

Problemas resueltos

Los problemas que se abordan en la compilación del 10 de abril de 2024.

Infraestructura

- La página **Infraestructura > Eventos > Mensajes de Syslog** aparece en blanco cuando los mensajes de Syslog contienen caracteres especiales, como superíndices.

  [NSHELP-37551]

- El recuento de certificados usados y sin usar que se muestra en **Infraestructura > Panel de control de SSL > Uso** es incorrecto cuando los certificados SSL tienen cadenas de certificados.

  [NSHELP-37469, NSADM-106867]

Licencias

- Los puertos 27000 y 7279 necesarios en el agente para las licencias agrupadas o flexibles pueden dejar de estar disponibles tras el reinicio de los procesos del agente. En estos casos, las instancias de NetScaler que usan licencias agrupadas o flexibles pueden entrar en período de gracia.

  [NSADM-110461]

Seguridad

- Al ir a **Seguridad > Recomendación de WAF**, es posible que aparezca el siguiente mensaje de error:

  "**Error HTTP 500 ([objeto Objeto]) al acceder al dispositivo de punto final de datos: "aplicaciones"**"

  [NSHELP-37598]

26 de marzo de 2024

Problemas resueltos

Los problemas que se abordan en la compilación del 26 de marzo de 2024.

Infraestructura

- Al crear o actualizar un trabajo de actualización de versiones, cuando intenta seleccionar una instancia en **Infraestructura > Trabajos de actualización > Crear trabajo > Seleccionar instancia > Agregar instancias**, la página **Agregar instancias** muestra la ficha **Particiones**, que no es aplicable al flujo de trabajo. Si selecciona una partición, la página deja de responder y no puede continuar.

  [NSADM-110118]

- Cuando crea notificaciones de Slack en **Parámetros > Notificaciones > Slack > Crear notificaciones de Slack** y selecciona **Notificaciones con archivos adjuntos**, las notificaciones no se muestran y aparece el siguiente mensaje de error:

  ```
  Invalid token
  ```


[NSHELP-37313]

StyleBooks

- Cuando se selecciona la opción **Solo acceso seguro** en **Configuración > Administración > Configuraciones del sistema > Parámetros básicos** e intenta realizar cualquier operación de proxy de API de dispositivo, la operación falla.

  [NSHELP-37368]

12 de marzo de 2024

Licencias

Función para seleccionar manualmente un agente de NetScaler como LSA en el servicio NetScaler Console Ahora puede seleccionar manualmente un agente de NetScaler como agente de servidor de licencias (LSA) para las licencias de NetScaler Pooled o NetScaler Flexed.

Cuando un LSA está inactivo, el servicio NetScaler Console espera 24 horas antes de seleccionar automáticamente el siguiente LSA. El administrador puede elegir manualmente un nuevo LSA mientras tanto mediante esta función. Sin embargo, el administrador debe asegurarse de que el estado del nuevo LSA elegido sea **ACTIVO** y que su estado de diagnóstico sea **correcto**.

Para obtener más información, consulte Comportamiento de los agentes de NetScaler para licencias Flexed o Pooled.

[NSADM-105168]

Problemas resueltos

Los problemas que se abordan en la compilación del 12 de marzo de 2024.

Análisis

- Cuando habilita **Gateway Insight** para los servidores virtuales de Gateway, la columna **Estado de análisis** en **Parámetros > Configuración de análisis > Todos los servidores virtuales** aparece como **inhabilitada**.

  [NHELP-37400]

- En **Gateway > Gateway Insight**, la ficha **Autenticación** no muestra los detalles de usuario de las autenticaciones fallidas.

  [NSHELP-37465]

Infraestructura

- Cuando se crea una directiva definida por el usuario y se agrega un usuario a esa directiva, las solicitudes de la API GET para recursos específicos presentan problemas de permisos y aparece el siguiente error:

  "No autorizado porque no se otorgaron los permisos necesarios"

  [NSHELP-37331]

28 de febrero de 2024

Infraestructura

Actualizaciones de las licencias VIP y del almacenamiento de NetScaler Console Service

- **VIP ilimitados en el servicio NetScaler Console**: a partir de la versión 14.1-21.x del servicio NetScaler Console, se elimina el concepto de VIP con licencia. Ahora hay un número ilimitado de VIP disponibles en el servicio NetScaler Console. Ya no tiene que comprar licencias de servidores virtuales de NetScaler Console porque el SKU de la licencia VIP finalizará la venta (EOS) y la renovación (EOR) en breve.
- Almacenamiento de**servicios de NetScaler Console**:
  - La SKU de almacenamiento del servicio de NetScaler Console finalizará la venta (EOS) y la renovación (EOR) en breve.
  - El derecho de almacenamiento predeterminado del servicio NetScaler Console ahora es de 5 GB.
  - Todas las licencias de almacenamiento de servicios de NetScaler Console adquiridas en el pasado se respetarán hasta que finalice el plazo.
  - Todas las licencias VIP de NetScaler Console adquiridas en el pasado que le dieron derecho a un derecho proporcional de almacenamiento del servicio NetScaler Console se conservarán hasta que finalice el plazo.
  - Si adquiere cualquier otro paquete de licencias que le dé derecho a un derecho de almacenamiento superior a NetScaler Console, los 5 GB predeterminados se cambian para que coincidan con el derecho.

[NSADM-108300]

Actualizaciones del recopilador de análisis y métricas

- Con la compatibilidad ilimitada de VIP desde la versión 14.1 21.x, todos los servidores virtuales nuevos y existentes ahora tienen licencia automática. Puede habilitar el análisis en los servidores virtuales sin licenciarlos explícitamente.
- El recopilador de métricas ahora está deshabilitado de forma predeterminada para todos los tipos de licencia de NetScaler en las nuevas instancias de NetScaler que se agregaron a NetScaler Console a partir de la versión 14.1 21.x. La configuración del recopilador de métricas para las instancias administradas existentes permanece sin cambios.

[NSADM-108803]

Análisis

Directivas de acción: configurar las notificaciones para el uso de las aplicaciones En Directivas de acción (**Configuración > Acciones > Directivas de acción**), ahora puede configurar una directiva de acción para el uso de las aplicaciones y seleccionar **las opciones Solicitudes por segundo**, **Rendimiento** y **Volumen de datos**. Estas opciones le permiten configurar y recibir notificaciones para el promedio de solicitudes por segundo, las anomalías de solicitudes por segundo, el promedio de rendimiento, las anomalías de rendimiento, el volumen total de datos y las anomalías del volumen de datos. Para obtener más información, consulte Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación.

[NSADM-104833]

Integración de observabilidad El flujo de trabajo de configuración para la integración con Splunk y New Relic ahora está mejorado para mejorar la experiencia del usuario y está disponible en **Configuración > Integración de observabilidad**. Anteriormente, el flujo de trabajo de configuración para la integración con Splunk y New Relic estaba disponible en **Configuración > Integración del ecosistema**.

Para obtener más información, consulte Integración de observabilidad

[NSADM-104702]

Integración de observabilidad: soporte para configurar la exportación de métricas de NetScaler a Prometheus En **Configuración > Integraciones de observabilidad**, ahora puede configurar la exportación de las métricas de NetScaler a Prometheus seleccionando el esquema predeterminado.

Para obtener más información, consulte Integración de Prometheus e Integración de observabilidad.

[NSADM-101426]

Gateway Insight: mejoras en la exportación de informes En **Gateway > Gateway Insight**, ahora puede exportar el informe solo con las opciones seleccionadas mediante el icono de configuración de todas las tablas de cada métrica (EPA, Authentication, Authorization Failure, SSO y Application Launch). Anteriormente, el informe exportado mostraba toda la información independientemente de las opciones seleccionadas.

[NSADM-96821]

StyleBooks

Actualizaciones de los StyleBooks predeterminados Los StyleBooks predeterminados basados en la versión 10.5 de NetScaler dejarán de estar disponibles en las próximas versiones. Ahora hay disponible un nuevo conjunto de StyleBooks predeterminados en **Aplicaciones > Configuración > StyleBooks > StyleBooks predeterminados, basado en la versión 13.0**de NetScaler.

[NSADM-105513]

Opción para clonar un StyleBook NetScaler Console ahora permite a los administradores crear un duplicado de un StyleBook, junto con sus dependencias. Luego, los administradores pueden usar este paquete para realizar personalizaciones adicionales, como actualizar `parameters` y `components` .

Para utilizar esta función, vaya a Aplicaciones > Configuración > Stylebooks, seleccione un StyleBook**predeterminado o personalizado y haga clic en Clonar.**

Para obtener más información, consulte Clonar un StyleBook.

[NSADM-92376]

Problemas resueltos

Los problemas que se abordan en la compilación del 28 de febrero de 2024.

Infraestructura

- La migración del servicio NetScaler Console al servicio NetScaler Console falla y algunos grupos de Azure Active Directory no están disponibles en el servicio NetScaler Console. Este problema se produce debido a la presencia de espacios en los nombres de grupo de Azure Active Directory creados en NetScaler Console.

  [NSHELP-37006]

- Los usuarios no pueden acceder a NetScaler Console si pertenecen a varios grupos de Azure Active Directory.

  [NSHELP-37005]

- En **Web Insight** y **Security Violations**, el flujo de trabajo de exportación programada en la GUI se ha mejorado para mejorar la experiencia del usuario.

  [NSADM-106624]

- En **Infraestructura > Informes de red**, el informe de exportación tabular no incluye detalles como el servicio, el grupo de servicios, el servidor virtual y el nombre de la interfaz.

  [NSHELP-37224]

- 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]

06 de febrero de 2024

Análisis

Panel de aplicaciones: soporte para ver los detalles de las métricas de la aplicación desde la partición de administración de NetScaler En **Panel de aplicaciones**, ahora puede ver los detalles de las métricas de las aplicaciones que se crean a partir de las particiones de administración de NetScaler. Anteriormente, solo se podían ver las aplicaciones de las particiones de administración sin ninguna métrica.

[NSADM-105343]

Infraestructura

Cambio de marca de NetScaler ADM en Citrix Cloud A partir de la versión 14.1 16.x, el servicio NetScaler ADM pasó a llamarse servicio NetScaler Console. A continuación, Application Delivery Management pasa a llamarse NetScaler Console en los siguientes lugares:

- El icono de la página principal de **Mis servicios** en Citrix Cloud.
- El nombre del servicio en el **menú Citrix Cloud > Mis servicios**.
- El nombre del producto que aparece en el flujo de trabajo Agregar administrador en el menú **Establecer acceso > Acceso personalizado** desde **Citrix Cloud > Administración de identidades y accesos > Administradores > Agregar administrador/grupo**.

Ejecute scripts de validación predeterminados en los trabajos de actualización NetScaler Console ahora incluye una opción para los scripts de validación predeterminados en el flujo de trabajo de actualización. Estos scripts predeterminados se ejecutan antes y después de un trabajo de actualización, lo que genera un informe de diferencias. Aún tiene la opción de ejecutar scripts predeterminados personalizados.

Para obtener más información, consulte Actualizar instancias de NetScaler.

[NSADM-100803]

Automatice la implementación de objetos de radar para los sitios de consola de NetScaler NetScaler permite automatizar la implementación de objetos de radar para los sitios de NetScaler Console, lo que elimina la necesidad de una implementación manual en las instancias de NetScaler.

Esta mejora solo está disponible cuando se edita una instancia de NetScaler y solo se aplica al centro dedatos de tipo sitio (con el **tipoprivado) o sucursal.**

Al seleccionar **Implementar en NetScaler** en la lista **Medidas de usuarios reales**, la lista de instancias de **NetScaler** se rellena automáticamente, lo que le permite elegir la instancia específica para implementar el objeto de radar (r20.png).

Para obtener más información, consulte Automatizar el despliegue de objetos de radar.

[NSADM-104691]

Problemas resueltos

Los problemas que se abordan en la compilación del 6 de febrero de 2024.

Análisis

- El ataque **XML SQL** no se notifica ni en el panel de seguridad (**Seguridad > Panel de seguridad) ni en el panel**de infracciones de**seguridad (Seguridad > Violaciones de seguridad**).

  [NSHELP-37159]

Licencias

- 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]

Administración y supervisión

- Cuando se crea un trabajo de configuración, el estado de **Infraestructura > Configuración > Trabajos** muestra **Completado**, pero **Detalles > Resumen de ejecución** muestra un 0% de finalización.

  [NSHELP-37176]

- El estado de un trabajo de actualización en dos etapas para un NetScaler HA muestra «Programado» aunque se haya completado la actualización de NetScaler HA. El nodo principal muestra completado (**Estado de etapa 1: Completado**), pero el nodo secundario muestra programado (**Etapa 2: Programado**).

  [NSHELP-36943]

- Cuando se crea una plantilla de auditoría de configuración con caracteres especiales en su nombre en **Infraestructura > Configuración > Auditoría de configuración > Plantillas de auditoría > Agregar**, la plantilla se genera correctamente. Sin embargo, no se genera un informe diferencial para la plantilla en el panel de **auditoría de configuración** durante el sondeo.

  Este problema se produce cuando se utilizan caracteres especiales distintos de - (guión) y '_' (guión bajo).

  [NSHELP-36438]

24 de enero de 2024

Análisis

Ver detalles del aviso de actualización en Tareas En **Tareas**, ahora puede ver la tarea procesable del **asesoramiento de actualización**. Según su uso actual, si sus instancias de NetScaler ya han alcanzado o están a punto de llegar al final del ciclo de vida (EOL) o al final del mantenimiento (EOM) en un plazo de 90 días, la tarea de asesoramiento sobre actualizaciones muestra **los** detalles de esas instancias. Puede hacer clic en **Tomar medidas** y actualizar esas instancias a una compilación recomendada.

[NSADM-104715]

Infraestructura

Permisos mejorados para usuarios de solo lectura Los usuarios con permisos de solo lectura para las siguientes funciones ahora pueden sondear las instancias de NetScaler:

- Certificados SSL (**Infraestructura > Panel de control SSL > Encuesta ahora**)
- Funciones de red (**Infraestructura > Funciones de red > Encuesta ahora**)

- Auditorías de configuración (**Infraestructura > Configuración > Auditoría de configuración > Sondear ahora**)

[NSADM-104710]

Problemas resueltos

Los problemas que se abordan en la compilación del 24 de enero de 2024.

- El registro de agentes integrado en NetScaler SDX muestra un mensaje de éxito, pero la instancia SDX no aparece en **Infraestructura > Panel de instancias**.

  [NSHELP-37137, NSHELP-37128]

- En **Infraestructura > Funciones de red > Equilibrio de carga**, la ficha **Servidores** indica el número de servidores, pero no muestra ninguna entrada de tabla para los usuarios no predeterminados.

  [NSHELP-36964]

16 de enero de 2024

Soporte para la identificación y remediación de CVE-2023-6548 y CVE-2023-6549

El asesoramiento de seguridad del servicio NetScaler Console ahora admite la identificación y la corrección de los CVE-2023-6548 y CVE-2023-6549.

- La identificación del CVE-2023-6548 requiere un escaneo de versiones.
- La identificación del CVE-2023-6549 requiere una combinación de escaneo 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.

> **Nota:**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde un par de horas en finalizar y reflexionar sobre el impacto de los CVE-2023-6548 y CVE-2023-6549 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, puede iniciar un análisis bajo demanda haciendo clic en **Escanear ahora**.

[NSADM-104763]

09 de enero de 2024

Análisis

Soporte para compartir un panel personalizado con otros usuarios Como administrador, ahora puede compartir el panel personalizado con otros usuarios. En **Descripción general > Panel personalizado**, seleccione un panel y haga clic en **Compartir**. Escriba el nombre de usuario y haga clic en **Invitar** para compartir el panel. Los usuarios asignados pueden ver el panel en modo de solo lectura.

[NSADM-100879]

Infraestructura

Configurar ITM Radar en sitios de consola de NetScaler El ITM Radar mejora las capacidades de monitoreo de la red. Los sitios implementados en centros de datos, máquinas virtuales o proveedores de nube ahora pueden alojar el objeto de radar (r20.png), lo que proporciona información sobre las métricas de rendimiento. El objeto ITM Radar recopila activamente valiosas estadísticas de las aplicaciones de los usuarios finales, proporcionando a los sitios una sólida telemetría de radar ITM para una supervisión de la red más eficaz y decisiones informadas de gestión del tráfico.

Para obtener más información, consulte Configurar ITM Radar .

[NSADM-91686]

Vea los datos de información sobre pasarelas en Splunk y New Relic Al crear una nueva suscripción en **Configuración > Integración del ecosistema** para la integración del servicio NetScaler Console con Splunk y New Relic, ahora puede seleccionar la opción **Gateway Insights**. Tras configurar la suscripción con la opción **Gateway Insights**, puede ver los datos de Gateway Insights en Splunk y New Relic.

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

[NSADM-101036]

Exporte los datos SSL a Splunk y New Relic de forma inmediata Los datos SSL ahora se exportan a Splunk y New Relic inmediatamente después de que un administrador cree una suscripción seleccionando **SSL Certificate Insight** en Splunk y New Relic. Anteriormente, los administradores tenían que hacer clic en Sondear **ahora** (**Infraestructura > Panel de control SSL**) para exportar los datos por primera vez.

[NSADM-101035]

Ver detalles del aviso de actualización en Tareas En **Tareas**, ahora puede ver la tarea procesable del **asesoramiento de actualización**. Según su uso actual, si sus instancias de NetScaler ya han alcanzado o están a punto de llegar al final del ciclo de vida (EOL) o al final del mantenimiento (EOM) en un plazo de 90 días, la tarea de asesoramiento sobre actualizaciones muestra los detalles de esas instancias. Puede hacer clic en **Tomar medidas** y actualizar esas instancias a una compilación recomendada.

[NSADM-104715]

Directiva de acción: configurar las notificaciones para las solicitudes, el ancho de banda y el tiempo de respuesta En **Directivas de acción** (**Configuración > Acciones > Directivas de acción**), al configurar una directiva de acción en Rendimiento de la aplicación, ahora puede seleccionar las opciones **Solicitudes**, **ancho** de banda y **tiempo de respuesta** . Estas opciones le permiten configurar y recibir notificaciones para el total de solicitudes, el ancho de banda total, el tiempo de respuesta promedio y las anomalías del tiempo de respuesta. Para obtener más información, consulte Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación.

Además, ahora también puede configurar una directiva de acción a partir del gráfico de tendencias en **Web Insight** para estas métricas. Como administrador, cuando observa un patrón de tráfico inusual o un aumento repentino en estas métricas en cualquier aplicación, esta mejora le permite crear una directiva de acción relativa haciendo clic en **Crear directiva de acciones** después de colocarla en un punto específico del gráfico.

[NSADM-101273]

Problemas resueltos

Los problemas que se abordan en la compilación del 9 de enero de 2024.

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.

  [NSADM-106665]

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

  [NSADM-106561]

- En **NetScaler Licensing > License Management**, la configuración para la infracción del umbral mediante una notificación por correo electrónico no funciona según lo esperado.

  [NSHELP-36895]

13 de diciembre de 2023

Infraestructura

Cambio de marca del servicio NetScaler ADM El servicio NetScaler Application Delivery Management (ADM Service) ahora pasa a llamarse servicio NetScaler Console.

Otras terminologías que han cambiado de nombre son las siguientes:

- El agente ADM ahora pasa a llamarse agente NetScaler
- ADM Service Connect ahora pasa a llamarse Console Advisory Connect

> **Nota:**
>
> La interfaz de usuario y la documentación de nuestro producto de servicio NetScaler Console se están actualizando actualmente para reflejar estos cambios. Durante este tiempo, es posible que encuentre referencias indistintamente a los nombres anteriores y a los renombrados. Le agradecemos su comprensión durante esta transición.

[NSADM-105125]

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.

> **Nota:**
>
> Asegúrese de que los agentes de NetScaler ejecuten la versión 16.x o una posterior.

Para obtener más información, consulte Licencia flexible.

[NSADM-98483]

Análisis

Licencia flexible: el recopilador de métricas está desactivado de forma predeterminada para las nuevas instancias de NetScaler agregadas a NetScaler Console Si utiliza la licencia Flexed, el recopilador de métricas ahora está deshabilitado de forma predeterminada para las nuevas instancias de NetScaler que se agreguen a NetScaler Console. Debe habilitar manualmente esta opción para enviar los datos de métricas y contadores de NetScaler a la consola. La configuración del recopilador de métricas para las instancias administradas existentes permanece sin cambios.

> **Nota:**
>
> El recopilador de métricas debe estar habilitado para que los datos aparezcan en el panel de control de aplicaciones y sus fichas relacionadas, como Rendimiento, SSL y Métricas clave para todos los servidores virtuales con licencia de esa instancia.

Para obtener más información, consulte Configurar el análisis inteligente de aplicaciones.

[NSADM-106193]

Desaprobación de las funciones de vídeo y TCP Insight Con la última versión, los datos de los informes de **VideoInsight y TCP** Insight ya no están disponibles para su visualización en NetScaler Console.

[NSADM-106597]

Infraestructura

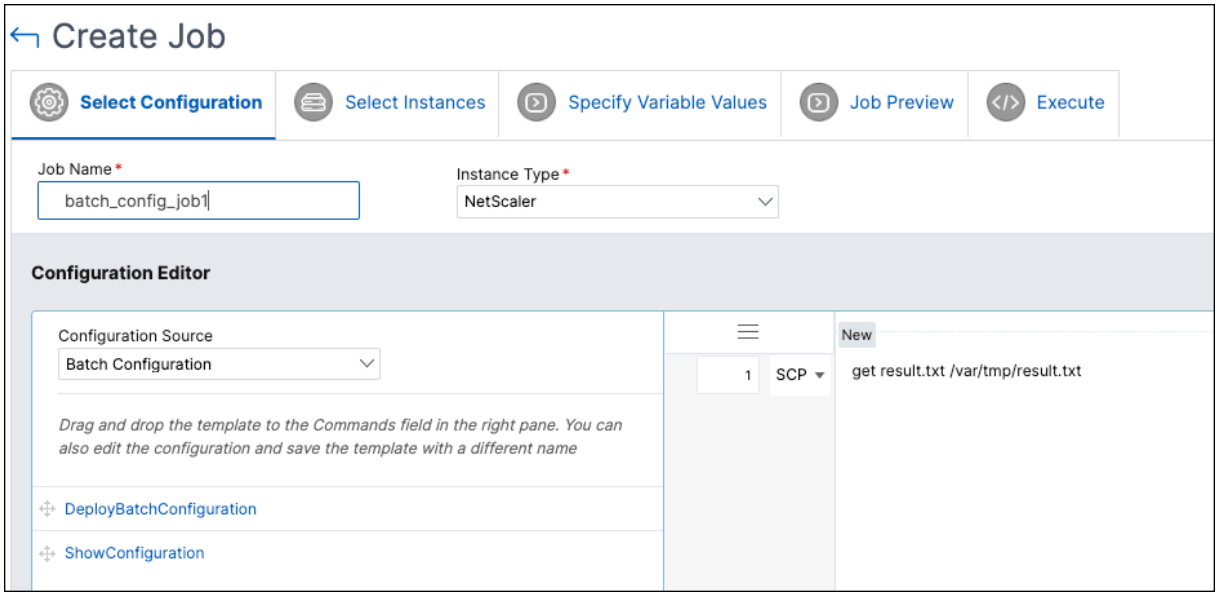
Descargar archivos para trabajos de configuración por lotes Los trabajos de configuración ahora le permiten descargar archivos de un directorio de una instancia de NetScaler a un directorio de su máquina local mediante la GUI de NetScaler ADM.

Para usar esta función, vaya a **Infraestructura > Configuración > Trabajos de configuración**, seleccione un trabajo y haga clic en **Descargar archivos de resultados** .

El botón **Descargar archivos de resultados** solo está disponible si se cumplen las siguientes condiciones:

- El trabajo de configuración que se crea es un trabajo de configuración por lotes. Para crear un trabajo de configuración por lotes, vaya a **Crear trabajo > Seleccionar configuración** y, en el **Editor de configuración**, seleccione **Origen de configuración > Configuración por lotes**
- Se usa un comando `scp get` en el **Editor de configuración**

Para varias instancias de NetScaler, los archivos de resultados descargados están disponibles en carpetas independientes, cada una de las cuales corresponde a una instancia individual.



[NSADM-105442]

Pausar y reanudar un trabajo de actualización programado NetScaler ADM ahora ofrece la opción de pausar el trabajo de actualización programado. Para usar esta función, vaya a **Infraestructura > Trabajos de actualización, seleccione un trabajo** de actualización programado existente y haga clic en **Detener** para pausar el trabajo. Para reanudar el trabajo de actualización programado, haga clic en **Reanudar** .

> **Nota:**
>
> Si el tiempo programado para el trabajo de actualización ha pasado después de haber decidido reanudarlo, debe volver a crear el trabajo de actualización.

Para obtener más información, consulte Trabajos de actualización.

[NSADM-100807, NSADM-97280]

Problemas resueltos

Los problemas que se abordan en Build son el 13 de diciembre de 2023.

Análisis

- En **Aplicaciones > Panel** de control, la exportación de los datos del registro de transacciones al formato tabular o CSV no muestra ningún dato. Este problema se detecta cuando NetScaler ADM está configurado con zonas horarias distintas de las UTC.

  [NSHELP-36817]

- En **Seguridad > Infracciones de seguridad > Detalles de la infracción**, el filtro de búsqueda no reconoce la «IP del cliente! =» consulta.

  [NSHELP-36675]

- Los informes de instantáneas programadas exportados desde **Seguridad > Infracciones de seguridad > Exportar informes > Programar** exportación con el formato de archivo seleccionado como JPEG muestran el siguiente error:

  «Proporcione los parámetros de consulta en el contexto del informe o en csv_export_arr. «

  [NSHELP-36657]

Infraestructura

- Algunos usuarios ven la marca de agua «Solo para fines de desarrollo» en los mapas de la página **Infraestructura > Instancias** .

  [NSHELP-36863]

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]

Seguridad

- Después de configurar las protecciones en el panel de seguridad unificado (**Seguridad > Panel de seguridad > Administrar aplicación**), las protecciones no se implementan en el servidor virtual de conmutación de contenido.

  [NSADM-105544]

29 de noviembre de 2023

Infraestructura

Usa etiquetas para autorizar instancias para grupos de usuarios Como administrador, ahora puedes autorizar a los usuarios a instancias específicas en función de las etiquetas asociadas. Al crear grupos de usuarios, vaya a **Configuración > Usuarios y roles > Agregar > Configuración de autorización > Seleccione etiquetas** y, a continuación, autorice a los usuarios a crear instancias por etiquetas.

Para obtener más información, consulte Configuración del control de acceso basado en funciones.

[NSADM-104798]

Problemas resueltos

Los problemas que se abordan en la compilación del 29 de noviembre de 2023.

- 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]

09 de noviembre de 2023

Análisis

Configurar el tiempo de espera de la sesión de Gateway En **Configuración > Configuración de análisis > Configurar el tiempo de espera de sesión de ICA/Gateway, ahora puede configurar el tiempo**de espera de la sesión para Gateway Insight. De forma predeterminada, el valor es de 30 minutos. Con esta configuración, si NetScaler ADM no recibe el registro de finalización de sesión dentro de la duración configurada, la sesión se graba como finalizada.

[NSADM-101271]

Actualización en el proceso de respaldo de NetScaler y el acceso al firewall Las copias de seguridad de las instancias de NetScaler ahora se cargan directamente desde el agente de NetScaler al servicio ADM de NetScaler y, a continuación, a Amazon S3. Por lo tanto, ya no necesita permitir el acceso a las URL de S3 en su firewall para el servicio de respaldo de NetScaler.

[NSADM-98267]

Soporte para la gestión inteligente del tráfico El servicio ADM de NetScaler ahora admite la administración inteligente del tráfico que le ayuda a mejorar la experiencia del usuario al analizar el tráfico de Internet en tiempo real y dirigir automáticamente el tráfico a las ubicaciones óptimas.

La gestión inteligente del tráfico le permite:

- Entregue aplicaciones en varias ubicaciones para reducir el tiempo de respuesta de las aplicaciones y maximizar su disponibilidad, basándose en datos de servicio en tiempo real.
- Configure el DNS autoritativo para administrar sus zonas.
- Vea información sobre los centros de datos de los clientes o las plataformas y aplicaciones de entrega.
- Identifique las mejores plataformas y ubicaciones.

Haga clic en **Administración inteligente del tráfico** en el panel de navegación izquierdo para comenzar. Para obtener más información, consulte Administración inteligente del tráfico.

[NSADM-91677]

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]

Problemas resueltos

Los problemas que se abordan en la compilación del 9 de noviembre de 2023.

Infraestructura

- Al configurar el agente integrado de NetScaler para administrar instancias, la configuración se bloquea en la página **Agregar instancias, aunque el** registro se haya realizado correctamente, y el agente se puede ver en **la** página Panel de instancias.

  [NSHELP-36614]

StyleBooks

- 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 caracteres especiales en la definición del paquete de configuración.

  [NSADM-104423]

25 de octubre de 2023

Análisis

Crea paneles personalizados para ver los detalles de las métricas clave de la instancia Al igual que en el panel unificado (**Descripción general > Panel de control**), ahora puede ver los detalles de las métricas de la instancia en función de su elección mediante la creación de paneles personalizados. Por ejemplo, si quiere supervisar las métricas clave de las aplicaciones y la seguridad de las aplicaciones, puede crear un panel personalizado seleccionando solo esas dos categorías. Puede crear hasta 20 paneles con un nombre único para cada panel. Como administrador, esta mejora le permite crear varios paneles y supervisar solo la información necesaria sobre las instancias.

Para empezar, dirígete a **Descripción general > Panel de control personalizado**.

Para obtener más información, consulta Crear paneles personalizados para ver los detalles de las métricas clave de la instancia.

[NSADM-91875]

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. También puedes ver estas tareas procesables en función de 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.

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.

[NSADM-101303]

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]

Problemas resueltos

Los problemas que se abordan en la versión del 25 de octubre de 2023.

- 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]

10 de octubre de 2023

Administración y supervisión

Soporte para la identificación y corrección de CVE-2023-4966 y CVE-2023-4967 El asesoramiento de seguridad de NetScaler Console ahora admite la identificación y la corrección de los 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]

26 de septiembre de 2023

Análisis

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 las instancias de NetScaler. Si crea una suscripción con instancias específicas, los datos se exportan a Splunk y New Relic solo desde las instancias de NetScaler seleccionadas.

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

[NSADM-94371]

Infraestructura

Instancias locales de ADM conectadas con el servicio ADM mediante Cloud Connector En **Configuración**, ahora puede ver una nueva opción denominada **ADM On-Prem**. En esta página, puede ver los detalles de las instancias locales de ADM que están conectadas con el arrendatario del servicio de ADM a través de ADM On-Prem Cloud Connector.

Para obtener más información, consulte Instancias locales de ADM conectadas con ADM Service mediante CloudConnector.

[NSADM-94576]

Problemas resueltos

Los problemas que se abordan en la compilación del 26 de septiembre de 2023.

Análisis

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

  [NSHELP-36184]

13 de septiembre de 2023

Infraestructura

Token de autenticación para cargar el paquete de soporte técnico Ahora necesita un token de autenticación para cargar el paquete de soporte técnico generado en su NetScaler al servidor de soporte técnico de Citrix. Anteriormente, cargaba el paquete de soporte técnico con el nombre de usuario y la contraseña de Citrix. Para obtener más información, consulte Cómo generar un paquete de soporte técnico para una instancia de NetScaler.

[NSADM-93351]

Problemas resueltos

Los problemas que se abordan en la versión del 13 de septiembre de 2023.

Análisis

- Cuando NetScaler Console pierde las licencias de servidor virtual, se espera que el estado de análisis de los servidores virtuales que utilizan esas licencias esté deshabilitado. 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 del gráfico muestra las fechas en lugar de la hora.

  [NSHELP-36043]

Administración y supervisión

- Los informes exportados desde **Infraestructura > Informes de red > Exportar** aparecen truncados o incompletos.

  [NSHELP-36252]

- Los usuarios de Azure Active Directory (AD) que pertenecen a muchos grupos de Azure no pueden acceder a NetScaler Console aunque los grupos de AD estén asignados a grupos de ADM.

  [NSHELP-35456]

31 de agosto de 2023

Infraestructura

Consulte la página del almacén de certificados en el panel de control SSL Ahora puede ir a **Infraestructura > Panel de control de SSL > Almacén de certificados** para ver la página **Almacén de certificados**.

[NSADM-97858]

Soporte para la funcionalidad SNMP para los agentes En **Infraestructura > Agentes > Acciones > Administrar SNMP**, ahora puede crear administradores de SNMP, usuarios de SNMP y vistas de SNMP para los agentes.

Para obtener más información sobre los administradores y usuarios de SNMP, consulte Crear administradores y usuarios de SNMP para el agente ADM de NetScaler.

[NSADM-94923]

Mejoras en la experiencia de usuario y la funcionalidad del panel de administración del almacenamiento de datos Para mejorar la experiencia del usuario y hacer que la administración del almacenamiento de datos sea más eficiente, ahora están disponibles las siguientes mejoras para el panel **Administración del almacenamiento de datos**:

- Nuevo diseño de interfaz de usuario para el panel de control:
  - Se agregaron mosaicos de **ingesta de datos**, **consumo de almacenamiento**, **depuración de datos** y **acciones**.
  - El mosaico **Acciones** ofrece opciones para agregar más espacio de almacenamiento, revisar la directiva de retención de datos, depurar los datos y revisar las notificaciones del sistema
- Función de búsqueda en la sección **Tendencias de consumo de almacenamiento** :

  Además de ver las tendencias de almacenamiento, ahora puede buscar funciones y tendencias específicas.
- Realice una depuración de datos:

- Ahora puede seleccionar una o más funciones y reducir sus datos para liberar espacio de almacenamiento.
- Tiene derecho a 10 podas de datos cada mes

Para obtener más información sobre el panel de administración del almacenamiento de datos, consulte Administración del almacenamiento de datos.

[NSADM-93202]

Seguridad

API Gateway ha cambiado su nombre a API Security **API Gateway** pasa a llamarse **API Security**. Puedes ver los cambios en las siguientes páginas:

- **Seguridad > API Security**
- **Seguridad > API Security > Análisis de API > Obtenga ayuda > Documentos de seguridad de API**
- **Configuración > Usuarios y funciones > Grupos > Configuración de autorización > API Security**
- **Configuración > Usuarios y funciones > Directivas de acceso > Permisos > Seguridad > API Security**

[NSADM-102384]

Problemas resueltos

Los problemas que se abordan en la compilación del 31 de agosto de 2023.

Administración y supervisión

- En **Infraestructura > Informes de red,** el panel de informes de red no muestra ningún dato histórico en los informes del servidor virtual. Este problema se produce al seleccionar un par de NetScaler HA en **Seleccionar entidades** al crear el panel.

[NSHELP-36228]

11 de agosto de 2023

Administración y supervisión

Aviso de seguridad: Supervisión de la integridad de los archivos El aviso de seguridad de NetScaler Console ahora le permite escanear los archivos de compilación de NetScaler y ver

los resultados de cualquier modificación o adición a los archivos de compilación originales de NetScaler.

En la Asesoría de seguridad (**Infraestructura > Asesoría de instancias > Asesoría de seguridad**), la opción **Analizar ahora** le permite seleccionar **Analizar CVE**, **Escanear archivos** o **Analizar ambos**. Tras seleccionar **Escanear archivos** o **Escanear ambos**, NetScaler Console compara el hash binario de los archivos de compilación de NetScaler gestionados con los valores hash binarios originales y resalta si hay alguna alteración o adición de archivos en la ficha **Supervisión de la integridad de los archivos**.

Los resultados del análisis muestran las instancias de NetScaler que tienen cualquier cambio potencial en los archivos originales o cualquier otra adición de archivos. Para obtener más información sobre los resultados del escaneo, puede ponerse en contacto con el departamento forense digital de su organización.

Para obtener más información, consulte Aviso de seguridad.

[NSADM-91856]

09 de agosto de 2023

Infraestructura

Consulte los detalles de la plataforma de virtualización de NetScaler VPX En **Infraestructura > Instancias > NetScaler VPX**, ahora puede ver la plataforma en la que está alojado NetScaler VPX seleccionando **Configuración > Cloud Platform**.

[NSADM-97319]

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]

Seguridad

Actualizar una definición de API existente En **Security > API Gateway > API Discovery**, ahora puede actualizar una definición de API existente con recursos de API seleccionados.

Para obtener más información, consulte Actualizar una definición de API existente con puntos de conexión de API detectados.

[NSADM-97433]

Problemas resueltos

Los problemas que se abordan en la compilación del 9 de agosto de 2023.

Provisioning

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

  [NSHELP-35983]

StyleBooks

- 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 se ha encontrado ningún trabajo.

  [NSADM-97948]

- Si crea un paquete de configuración a partir de una definición de StyleBook que tiene un servidor virtual de autenticación y enlaces de directivas 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, aparecerá el siguiente mensaje de error:

  El recurso ya existe.

  [NSHELP-35646]

26 de julio de 2023

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 Supervisión de la consola, las aplicaciones y la seguridad de las aplicaciones de NetScaler con 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]

Asigne un perfil de red para las instancias de NetScaler administradas desde NetScaler Console
Cuando habilita el análisis para los servidores virtuales en NetScaler Console, los datos de AppFlow de NetScaler se exportan a NetScaler Console a través de la dirección IP de subred (SNIP) de NetScaler. 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 a través de NetScaler Console. Vaya a **Infraestructura > Instancias > Citrix 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 Console.

[NSADM-91836]

Infraestructura

Experiencia de usuario mejorada al usar la CLI para configurar el agente de NetScaler como proxy Cuando intenta registrar un agente de NetScaler en el servicio NetScaler Console, la CLI ahora le hace preguntas (y/n) sobre el uso del proxy.

También tiene la opción de configurar el proxy en el mismo script, si es necesario.

[NSADM-96921]

Soporte de CLI para ver las URL de los puntos finales al registrar un agente de NetScaler Después de introducir una URL de servicio en la CLI al registrar un agente de NetScaler en el servicio NetScaler Console, puede ver la lista de todas las URL de punto final a las que se debe permitir el acceso.

[NSADM-96920]

StyleBooks

Compatibilidad con atributos adicionales en análisis de StyleBooks Se ha mejorado la sección de análisis de StyleBooks para:

- Aceptar los 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 (`http-x-forwarded-for`)
  - Habilitar mediciones del lado del cliente (`client-side-measurements`)

Para obtener más información, consulte Análisis de StyleBooks.

[NSADM-97839]

18 de julio de 2023

Administración y supervisión

Soporte para la identificación y corrección de CVE-2023-3519, CVE-2023-3466 y CVE-2023-3467 El asesoramiento de seguridad de NetScaler Console ahora admite la identificación y la corrección de los CVE-2023-3519, CVE-2023-3466 y CVE-2023-3467.

Identificación de:

- El CVE-2023-3519 requiere una combinación de análisis de versión y configuración.
- Los modelos CVE-2023-3466 y CVE-2023-3467 requieren un análisis de versiones.

La corrección de CVE-2023-3519, CVE-2023-3466 y CVE-2023-3467 requiere una actualización de la instancia vulnerable de NetScaler a una versión y compilación que incluyan la corrección.

> **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 Console para actualizar las instancias de NetScaler, consulte Usar trabajos para actualizar las instancias de NetScaler.

Para obtener más información sobre cómo corregir los códigos CVE-2023-3519, CVE-2023-3466 y CVE-2023-3467, consulte el Boletín de seguridad.

> **Nota:**
>
> El análisis del sistema de asesoramiento de seguridad puede tardar un par de horas en finalizar y reflejar el impacto de los códigos CVE-2023-3519, CVE-2023-3466 y CVE-2023-3467 en el módulo de asesoramiento de seguridad. Para ver el impacto con mayor rapidez, puede iniciar un escaneo bajo demanda haciendo clic en **Escanear ahora**.

[NSADM-100103]

12 de julio de 2023

Problemas resueltos

Los problemas que se abordan en Build 12 de julio de 2023.

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

  [NSHELP-35724]

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

  [NSHELP-35588]

03 de julio de 2023

Análisis

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.

Ahora, en **Trabajo de configuración**, puede crear un trabajo con la plantilla `NSConfigurePrometheusAnalyt` de **Plantilla incorporada**, especificar los parámetros necesarios y ejecutar el trabajo en todas las instancias administradas.

Para obtener más información, consulte Programar trabajos para configurar la exportación de métricas de NetScaler a Prometheus.

[NSADM-97251]

Infraestructura

El agente 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 de NetScaler una vez descargadas. Por lo tanto, no es necesario descargar las imágenes para los trabajos de actualización posteriores.

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

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

[NSADM-76343]

Problemas resueltos

- En Web Insight, cuando se profundiza en una métrica para ver los detalles y, a continuación, se profundiza 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]

- 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 se ha encontrado ningún trabajo".

  [NSADM-97948, NSADM-97727]

- En el **Panel de aplicaciones**, al seleccionar una aplicación y navegar a la ficha **SSL** para vincular un certificado, aparece el mensaje de error "**Certificado no encontrado en la base de datos**".

  [NSHELP-35654]

14 de junio de 2023

Seguridad

Soporte para crear una definición de API sin seleccionar puntos finales En la página **Seguridad > API Gateway > Detección de API** > **vserver**, ahora puede crear una definición de API sin seleccionar un punto final. Al hacer clic en **Crear definición de API**, aparece una ventana emergente para confirmar si se debe crear una definición de API para todos los puntos de conexión detectados. Haga clic en **Sí** para crear la definición de API con todos los puntos finales; de lo contrario, haga clic en **No**.

Para obtener más información, consulte Discover API endpoints.

[NSADM-94318]

StyleBooks

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

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

Para obtener más información, consulte replace().

[NSADM-96802]

Problemas resueltos

Los problemas que se abordan en la compilación del 14 de junio de 2023.

- En Upgrade Jobs (**Infraestructura > Upgrade Jobs**), al seleccionar la instancia fallida de validación previa a la actualización y hacer clic en **Revalidar**, aparece un mensaje de error.

  [NSADM-98329]

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

  [NSHELP-35593]

- Al exportar los informes de caducidad de SSL semanales, 30 o 90 días desde **Infraestructura > Panel de control SSL > Certificados SSL > Exportar informes** y selecciona **Tabular**, el informe resultante muestra una columna 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]

- En la versión 13.1 y posteriores de NetScaler, los comandos ISSU no se ejecutan durante la actualización de NetScaler.

  [NSHELP-35391]

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

  [NSHELP-35323]

31 de mayo de 2023

Análisis

Recomendaciones de licencias agrupadas en la función Tareas En **Tasks**, ahora puede ver las recomendaciones y los flujos de trabajo de Guide Me para los derechos de licencia agrupados. Como administrador, estas recomendaciones de licencias agrupadas garantizan que utilice todas las funciones de NetScaler Console.

Para obtener más información, consulte Ver recomendaciones y administrar sus ADC y aplicaciones de manera eficiente.

[NSADM-93988]

Exporte datos de información sobre SSL a Splunk y New Relic Al crear una nueva suscripción en **Configuración > Integración de ecosistemas para la integración** de Citrix ADM con Splunk y New Relic, ahora puede seleccionar la opción **SSL Certificate** Insights. Después de configurar la suscripción con la opción **SSL Certificate Insights**, puedes ver los datos SSL (datos relacionados con el servidor SSL y el certificado SSL) en el panel de control de Splunk y New Relic.

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

[NSADM-92047]

Problemas resueltos

Los problemas que se abordan en la compilación del 31 de mayo de 2023.

- En **Gateway > HDX Insight > Instancias**, al seleccionar una instancia y exportar los datos, la información del nombre de usuario para los usuarios de escritorio no estaba disponible. Con esta corrección, la información del nombre de usuario también está disponible en el informe.

  [NSADM-96024]

- Al seleccionar **Configurar SNMP** para una instancia de SDX en **Infraestructura > Instancias> Citrix ADC > SDX**, aparece un mensaje de error. Este problema se produce si el perfil SDX está configurado con SNMP v3 y **NoAuthNoPriv** como nivel de seguridad.

  [NSHELP-35324]

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

  [NSHELP-35266]

- En Web Insight, al exportar datos mediante la opción de instantánea, los gráficos del informe aparecen en blanco.

  [NSHELP-35147]

- Los análisis no están visibles en HDX Insight. Incluso si se reinicia Citrix ADM, los análisis solo están visibles durante un período breve y se vuelven invisibles más adelante.

  [NSHELP-35128]

- Para una instancia de SDX en **Infrastructure > Instancias > Citrix ADC > SDX > Dasboard**, cuando los valores utilizados y libres de un recurso son cero, el gráfico de **utilización de los recursos del sistema** muestra un espacio en blanco y campos de valores en blanco.

  Con esta corrección, el número cero aparece junto al nombre del recurso si los valores utilizados y libres son cero.

  [NSHELP-35069]

18 de mayo de 2023

Análisis

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]

Infraestructura

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**.

[NSADM-52467]

Soporte para registrar eventos independientemente de la antigüedad del evento NetScaler Console ahora le permite registrar todos los eventos independientemente de la edad de los eventos que haya establecido en las reglas de eventos.

Para configurar esta opción, vaya a **Infraestructura > Reglas > Agregar > Configurar la antigüedad del evento** y seleccione la casilla **Registrar eventos al instante independientemente de la duración del evento** .

[NSHELP-19914]

Problemas resueltos

Los problemas que se abordan en la compilación del 18 de mayo de 2023.

- En **Infraestructura > Trabajos de actualización > Agregar > Programar tarea**, si selecciona **Realizar una actualización en dos etapas para los nodos de HA** y selecciona la misma hora en los dos campos de **hora de inicio**, aparece el siguiente mensaje de error al continuar:

  “common.date_diff_error:Debe haber al menos 1 hora de diferencia entre el tiempo de actualización”

  Incluso si cambia la hora de inicio en los campos, la ficha **Crear trabajo** muestra una página vacía.

  [NSHELP-35016]

- En **Infraestructura > Asesoramiento de instancias > Aviso de actualización**, los detalles sobre el fin del mantenimiento (EOM) y el final de la vida útil (EOL) de la versión 13.0 son incorrectos.

  [NSHELP-34953]

- La alerta por correo electrónico de cualquier evento mostraba la región de forma incorrecta. Con esta corrección, la región no aparece en las alertas de eventos por correo electrónico.

  [NSHELP-34913]

09 de mayo de 2023

Administración y supervisión

Soporte para la identificación y corrección de CVE-2023-24488 y CVE-2023-24487 El asesoramiento de seguridad de NetScaler Console ahora admite la identificación y la corrección de los CVE-2023-24488 y CVE-2023-24487.

Identificación de:

- El CVE-2023-24488 requiere una combinación de análisis de versión y configuración.
- El CVE-2023-24487 requiere un análisis de la versión.

La corrección de CVE-2023-24487 y CVE-2023-24488 requiere actualizar la instancia de ADC vulnerable a una versión y una compilación que tengan la solución.

Para obtener más información sobre los detalles de la versión de compilación fija para CVE-2023-24487 y CVE-2023-24488, consulte Boletín de seguridad.

> **Nota:**
>
> Las compilaciones 13.1—45.63 de ADC sustituyen a las compilaciones 13.1—45.61.

Para obtener más información sobre cómo usar NetScaler Console para actualizar las instancias de ADC, consulte Crear un trabajo de actualización de ADC.

> **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-2023-24488 y CVE-2023-24487 en el módulo de asesoramiento de seguridad. Para ver el impacto con mayor rapidez, puede iniciar un escaneo bajo demanda haciendo clic en **Escanear ahora**.

[NSADM-93570]

25 de abril de 2023

Las mejoras y cambios que están disponibles en la compilación del 25 de abril de 2023.

Análisis

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]

StyleBooks

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** .

[NSADM-92374]

Problemas resueltos

Los problemas que se abordan en la compilación del 25 de abril de 2023.

- En **Aplicaciones > Configuración > Paquetes de configuración**, al introducir una consulta de búsqueda mediante los criterios de búsqueda de **Propiedades > Tecla de visualización**, se muestra el resultado de la búsqueda, pero la barra de búsqueda muestra el número de índice del resultado.

  Con esta corrección, la barra de búsqueda muestra la consulta de búsqueda en texto en lugar de un número.

  [NSADM-96859]

Análisis

- Los datos de ancho de banda de **HDX Insight** y **Gateway Insight** se muestran incorrectamente en bytes por segundo en lugar de bits por segundo.

  [NSHELP-34836]

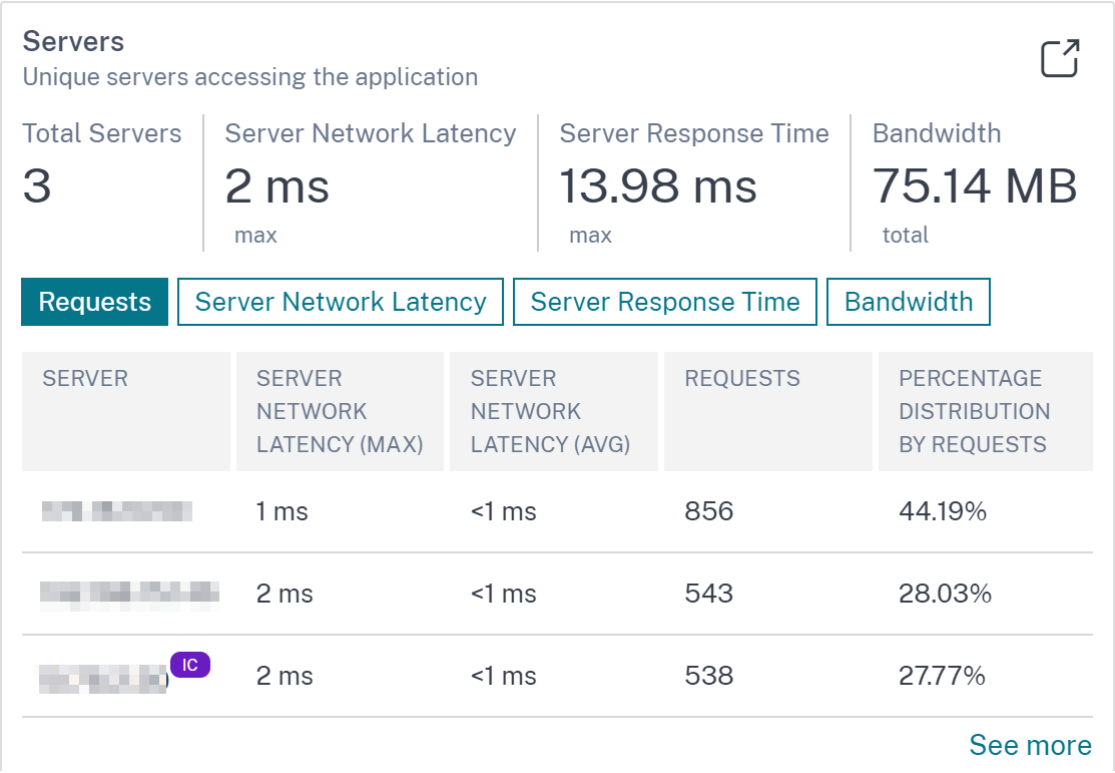
13 de abril de 2023

Las mejoras y cambios que están disponibles en la compilación del 13 de abril de 2023.

Análisis

Notificación de caché integrada en Web Insight Después de habilitar la caché integrada en la instancia de NetScaler, las solicitudes elegibles se procesan sin necesidad de ir de ida y vuelta a un servidor de origen. En **Web Insight**, estas solicitudes de caché integrada están visibles actualmente en **Servidores** con dirección IP de servidor virtual en lugar de en la dirección IP del servidor real.

Para una mejor visibilidad de estas solicitudes de caché integrada, ahora puede ver una notificación de IC junto a la dirección IP del servidor virtual ADC en **Servidores**.



Para las solicitudes que no se procesan con la memoria caché integrada, la dirección IP real del servidor de origen está visible.

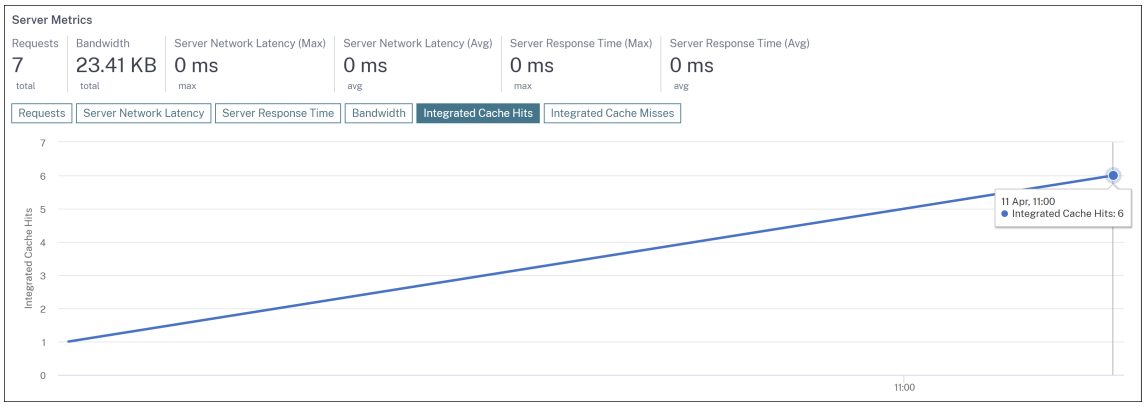
Como administrador, esta notificación le permite identificar rápidamente que la instancia de ADC ha procesado las solicitudes de caché integrada.

[NSADM-91864]

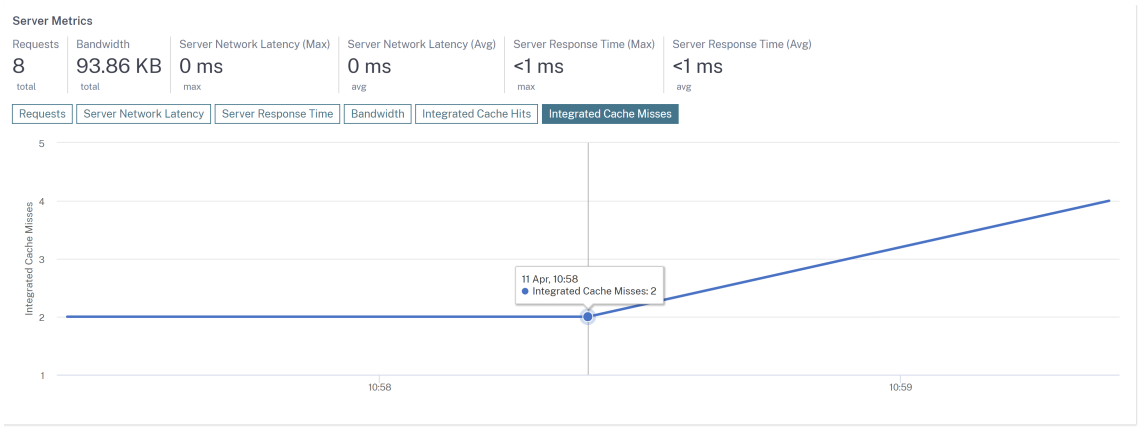
Gráfico de aciertos y errores de caché integrado en Web Insight En **Web Insight**, al analizar un servidor, **las métricas del servidor** ahora muestran las fichas de **aciertos** y errores de **caché integrados**.

Como administrador, la vista gráfica está 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.



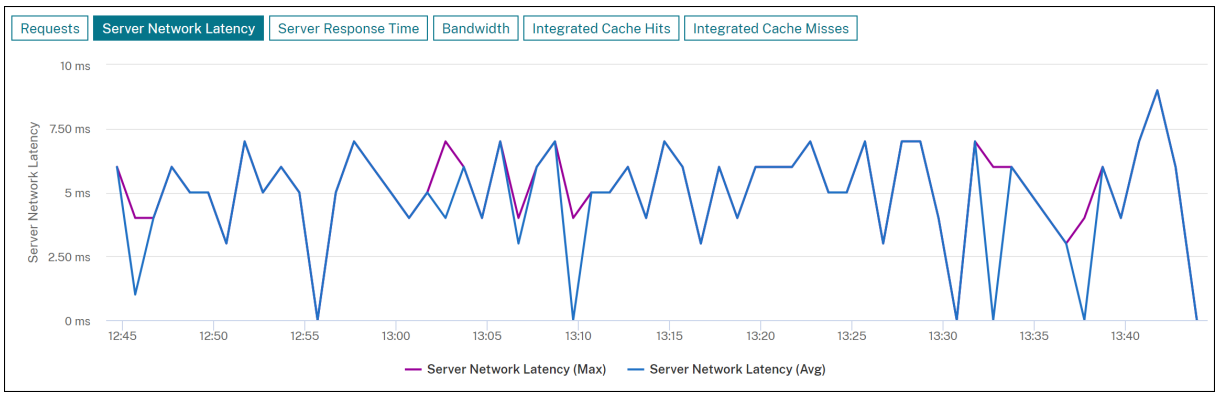
- La ficha **Errores de la memoria caché integrada** le permite ver el total de respuestas que el dispositivo NetScaler proporciona desde el servidor de origen.



[NSADM-93952]

Web Insight: Consulte los valores medios y máximos en gráficos A partir de la 13.1 45.47 o versiones posteriores, la consola **Web Insight** de NetScaler es compatible con la visibilidad de los valores de latencia máxima en **Servidores** y **Clientes**.

Además de esta compatibilidad, al analizar un servidor o un cliente, ahora puede ver los valores promedio y máximo en el panel de resumen y también pasar el puntero del ratón sobre el gráfico de análisis de series temporales en **Latencia de la red del servidor**, **Tiempo de respuesta del servidor** y **Latencia de la red del cliente**.



Como administrador, esta mejora le permite visualizar la latencia máxima en los gráficos durante la duración seleccionada.

[NSADM-93816]

Infraestructura

Vea las tendencias de almacenamiento de datos en la GUI de NetScaler Console En **Configuración > Administración del almacenamiento de datos**, ahora puede ver la información de almacenamiento de datos en las distintas funciones de su implementación actual. El panel **de administración del almacenamiento de datos** le ayuda a visualizar cómo se almacenan los datos y si las funciones funcionan dentro de sus derechos de almacenamiento.

> **Nota**
>
> Se espera que las directivas de almacenamiento de datos cambien en las próximas versiones. Con estos cambios, no podrá almacenar datos históricos después de que superen el límite de almacenamiento.

Para obtener más información, consulte Administrar el almacenamiento de datos.

[NSADM-94623]

Problemas resueltos

Los problemas que se abordan en la compilación del 12 de abril de 2023.

Infraestructura

- En las implementaciones de alta disponibilidad, no existe la opción de cargar archivos de imagen de compilación únicamente en el nodo secundario.

  Como parte de la solución, ahora puede cargar archivos de imagen de compilación en el nodo secundario desde la ficha **Infraestructura > Actualizar trabajos** > **Crear trabajo** > **Cargar solo en el nodo secundario**.

  [NSADM-96079]

- Los informes exportados desde **Infraestructura > Instancias > NetScaler** no muestran el número de serie de los nodos secundarios.

  Los informes ahora muestran los números de serie de los nodos principales y secundarios de las instancias de NetScaler. También puede ver los informes desde **Infraestructura > NetScaler Inventory**.

  [NSHELP-18816]

05 de abril de 2023

Las mejoras y cambios que están disponibles en la compilación del 5 de abril de 2023.

Seguridad

Cree definiciones de API a partir de los puntos finales de API descubiertos en la GUI de NetScaler Console Ahora puede crear definiciones de API a partir de puntos de enlace de API descubiertos en **Seguridad > API Gateway > Detección de API**.

[NSADM-85957]

Panel unificado: vea las métricas clave del análisis de la API En el panel unificado (**Descripción general > Panel)**, ahora puede ver las métricas clave de los puntos finales de la API configurados a través de NetScaler Console.

Para obtener más información, consulta Un panel unificado para ver los detalles de las métricas clave de la instancia.

[NSADM-85954]

Problemas resueltos

Los problemas que se abordan en la compilación del 5 de abril de 2023.

- La opción **Elegir dispositivo** para los campos **Archivo de certificado** y **Archivo clave** aparece en las páginas siguientes:
  - **Infraestructura > Panel de control SSL > Administrar el almacén de certificados > Agregar**
  - **Infraestructura > Panel de control SSL > Certificados SSL > Actualización**

  Como solución, ahora se ha eliminado la opción **Elegir dispositivo**.

  [NSHELP-34566]
- Si NetScaler tiene una consola NetScaler local como servidor de licencias y se modifica un agente en **Infraestructura > Instancias > Agentes**, se produce el siguiente problema:

  `The IP address of the license server on NetScaler changes from the IP address of the on-premises NetScaler Console to the IP address of one of the NetScaler agents`.

  [NSHELP-34483]
- Al modificar la contraseña de un perfil de administrador de SDX configurado con SNMPv3 desde **Infraestructura > Instancias> NetScaler > ficha SDX > Perfil**, aparece el siguiente mensaje de error:

  `Please provide valid authentication protocol. The possible values are MD5, SHA`.

  [NSHELP-34372]

14 de marzo de 2023

Problemas resueltos

En la compilación del 14 de marzo de 2023 se solucionó el siguiente problema:

En **Infraestructura > Panel de control SSL > Instalación de certificados**, al cargar una cadena de certificados que tenga el mismo certificado raíz que una cadena de certificados existente, se produce un error en la instalación del certificado. El siguiente texto aparece en **Infraestructura > Panel de control SSL > Registros de auditoría SSL > Registro de dispositivos > Registro de comandos**:

`Resource Already Exists`

[NSHELP-34233]

Al eliminar una lista de distribución de correo electrónico de **Configuración > Notificaciones > Correo electrónico**, aparece el siguiente error:

`Error: Bad Gateway`

Este problema se produce porque el nombre de la lista de distribución de correo electrónico tiene un espacio en blanco.

Como parte de la solución, NetScaler Console ahora permite eliminar las listas de distribución de correo electrónico con espacios en blanco.

[NSHELP-34545]

02 de marzo de 2023

Análisis

Mejoras en Web Insight En Web Insight, ahora puede ver las siguientes mejoras en **Métricas de la aplicación**:

- Se presenta una nueva ficha **Resumen** que permite visualizar una descripción general del rendimiento de la aplicación, como el tiempo de respuesta, las solicitudes y el ancho de banda. Como administrador, esto le permite obtener una idea del rendimiento de la aplicación durante el período seleccionado. Puede utilizar la opción de conmutación y personalizar la vista.
- En la ficha **Solicitudes**, además del total de solicitudes existentes, también puede ver las solicitudes de los 5 clientes principales en función del total de solicitudes. Como administrador, esto le permite obtener una idea de los clientes que acceden a la aplicación durante el período seleccionado.
- En la ficha **Ancho de banda**, puede ver el consumo de ancho de banda de los 5 servidores principales en función del consumo total de ancho de banda. Como administrador, esto le permite obtener una idea de los servidores que consumen más ancho de banda durante el período seleccionado.
- En la ficha **Tiempo de respuesta**, también puede ver 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. Como administrador, esto le permite obtener información sobre la latencia que se produce en el cliente, el servidor y la aplicación durante el período seleccionado. Puede utilizar la opción de conmutación y personalizar la vista.

  [NSADM-87792]

Infraestructura

Eliminación de cuentas inactivas de NetScaler Console Express Si su cuenta de NetScaler Console Express permanece inactiva durante 45 días, la cuenta se eliminará. Citrix envía un recordatorio después de 30 días de inactividad.

[NSADM-93203]

Administración y supervisión

Resumen de cambios en la ejecución para la actualización de alta disponibilidad de NetScaler En la GUI de NetScaler Console, el resumen de ejecución de **Infraestructura > Trabajos de actualización > Resumen de ejecución** ya no muestra los comandos relacionados con la sincronización de alta disponibilidad.

Esto se debe a que, durante la actualización de alta disponibilidad de NetScaler, si los nodos principal y secundario de NetScaler están en versiones diferentes, NetScaler inhabilita la sincronización de alta disponibilidad entre los nodos. NetScaler Console no realiza esta operación.

[NSADM-93441]

Defina el umbral para las entidades individuales en los informes de red En **Infraestructura > Informes de red > Umbrales**, ahora puede establecer el valor de umbral para entidades específicas al configurar el umbral.

Para obtener más información, consulte Informes de red.

[NSADM-91727]

Función para programar la actualización de agentes individuales En **Infraestructura > Instancias > Agentes > Configuración**, ahora puede programar la actualización de cada agente de NetScaler. Puede optar por actualizar automáticamente un agente a la siguiente compilación o especificar una hora y una zona horaria para programar una actualización.

Para obtener más información, consulte la configuración de actualización del agente.

[NSADM-91719]

Mejoras en la actualización de instancias de NetScaler Los siguientes cambios ya están disponibles en la ficha **Validación previa a la actualización**:

- Sección **Instancias bloqueadas para la actualización**: En esta nueva sección se enumeran las instancias a las que se ha bloqueado la actualización debido a errores de validación previos a la actualización.
- Botón **Limpieza rápida**: Este botón está disponible en el panel **Detalles del espacio en disco** y permite liberar rápidamente el espacio en disco de varias carpetas.

Para obtener más información, consulte Cómo actualizar una instancia de ADC.

[NSADM-91505]

Las imágenes de NetScaler BLX ya están disponibles en la biblioteca de imágenes Al actualizar NetScaler BLX desde **Infraestructura > Actualizar trabajos > Actualizar NetScaler BLX > Seleccionar imagen, ahora puede seleccionar**las imágenes de **NetScaler BLX** de la biblioteca de imágenes.

[NSADM-86864]

Seguridad

Vea las versiones de NetScaler Web App Firewall y las firmas de bots de una instancia de NetScaler Ahora puede ver las versiones de NetScaler Web App Firewall y las firmas de bots de una instancia de NetScaler. Las versiones de firmas más recientes protegen su instancia de los CVE. Para obtener más información, consulte Artículos sobre alertas de firmas y artículos sobre alertas de firmas de bots.

[NSADM-92378]

Análisis del rendimiento de las aplicaciones

Mejoras en Web Insight En **Web Insight**, ahora puede ver los valores máximos de latencia de red tanto en el **servidor** como en el **cliente**. Como administrador, esta mejora le permite identificar el servidor o cliente exacto que funciona con la máxima latencia.

Anteriormente, Web Insight proporcionaba el valor máximo únicamente en función de los valores de latencia promedio de todos los servidores y clientes.

[NSADM-91834]

Otros

Crear y aplicar filtros en el panel unificado En el panel unificado (**Descripción general > Panel de control**), ahora puede crear y aplicar filtros en:

- Aplicaciones
- Infraestructura ADC
- Seguridad de las aplicaciones

Como administrador, puede aplicar filtros y ver la información solo para las instancias o aplicaciones seleccionadas.

Para obtener más información, consulta Un panel unificado para ver los detalles de las métricas clave de la instancia.

[NSADM-91873]

Problemas resueltos

Los problemas que se abordan en la compilación del 2 de marzo de 2023.

- En **Infraestructura > Trabajos de actualización**, al seleccionar un trabajo finalizado que tenga el nombre del archivo de script anterior o posterior a la actualización con caracteres especiales y, a continuación, descarga los scripts de salida de la lista de **selección de acciones**, aparece el mensaje de error **Archivo no encontrado**.

[NSHELP-33854]

07 de febrero de 2023

Análisis

Las violaciones de seguridad muestran las etiquetas OWASP En la GUI de NetScaler Console, las infracciones de seguridad ahora muestran etiquetas OWASP. Es compatible con las listas OWASP 2017 y OWASP 2021. Estas etiquetas ayudan a determinar si la infracción pertenece a la lista de las 10 principales de OWASP.

Seleccione una infracción para ver más detalles. Los detalles ahora incluyen las columnas OWASP 2017 y OWASP 2021. Estas columnas muestran los códigos de OWASP y puede utilizarlos para obtener más información sobre la infracción en el sitio web de OWASP.

[NSADM-92999]

Administración y supervisión

Soporte para cambiar la contraseña del agente sin la contraseña actual Como superadministrador, ahora puede permitir que las contraseñas de los agentes se cambien sin sus contraseñas actuales.

Vaya a **Configuración > Configuraciónglobal**>**Configuraciones del sistema**>**Agente y zona horaria > Agente**y seleccione la casilla**Eliminar el requisito previo de la contraseña actual para cambiar la contraseña del agente**. La página**Cambiar contraseña del agente**ya no tendrá el campo**Contraseña actual**.

Para volver a mostrar el campo **Contraseña actual**, desactive la casilla **Eliminar el requisito previo de la contraseña actual para cambiar la contraseña del agente** .

[NSADM-91826]

Se ha revisado el intervalo de visualización de datos de series temporales para las cuentas de NetScaler Console Express Para los servidores virtuales administrados con la cuenta Express, ahora se ha revisado la visualización de datos de series temporales en los gráficos de análisis y los gráficos de informes de red para la **última hora** de duración.

Función	Intervalo de visualización de datos existente	Nuevo intervalo de visualización de datos
Panel de aplicaciones	1 minuto	5 minutos
Informes de red	5 minutos	10 minutos
Web Insight, HDX Insight, Gateway Insight, Security Insights, BOT Insights, transacciones detalladas	1 minuto	5 minutos

[NSADM-93200]

Problemas resueltos

Estos problemas se abordaron en la compilación del 7 de febrero de 2023.

Al habilitar o inhabilitar la configuración de syslog para la instancia de ADC, ADM no guarda la configuración en la instancia de ADC. Como resultado, los eventos de cambios de configuración no se guardan en NetScaler Console.

[NSHELP-33264]

En **Infraestructura > Instancias > Agente**, tras instalar el certificado SSL con una clave cifrada por contraseña, se produce un error en la conexión con el agente en el puerto 443.

[NSHELP-33614]

24 de enero de 2023

Problemas resueltos

Estos problemas se abordaron en la compilación del 24 de enero de 2023.

Aparece un mensaje de error al habilitar SNMP v3 en una instancia de NetScaler SDX desde la GUI de NetScaler Console. Para ello, vaya a **Infraestructura > Instancias > NetScaler > SDX > Seleccionar acción Configurar SNMP**.

[NSHELP-33852]

10 de enero de 2023

Administración y supervisión

Vea las recomendaciones y administre sus ADC y aplicaciones de manera eficiente como tareas procesables con los flujos de trabajo de Guide Me En la GUI de NetScaler Console, se presenta una nueva opción de **tarea**, en la que ahora puede ver las recomendaciones en función de su suscripción y uso actual. Como administrador, puede:

- Vea las **tareas pendientes** como recomendaciones prácticas para licencias, análisis, eventos, certificados SSL y mucho más
- Complete la tarea mediante la opción **Guíame**, que proporciona instrucciones, herramientas y consejos para completar la tarea correctamente.
- Reconozca las tareas y muévalas al archivo
- Vaya a **Tareas archivadas** y utilice las herramientas guiadas (consejos para necesidades recurrentes)

Estas recomendaciones garantizan que está utilizando todas las capacidades de NetScaler Console, permiten el descubrimiento de productos y las funcionalidades recomendadas por el producto para una administración eficiente de la implementación.

Para obtener más información, consulte Ver recomendaciones y administrar sus ADC y aplicaciones de manera eficiente.

[NSADM-68719]

StyleBooks

Habilitar o inhabilitar la longitud de la máscara de red en la GUI de configuración de StyleBook Al crear un paquete de configuración a partir de StyleBooks con el atributo `type: ipnetwork`, la GUI de configuración de StyleBook ahora muestra el botón **Longitud de la máscara de red** junto al campo **Dirección IP**.

Puede realizar una de las siguientes acciones:

- Habilitar la entrada de longitud de máscara de red
- Inhabilitar la entrada de la dirección IP de la máscara de red

[NSADM-80696]

13 de diciembre de 2022

Administración y supervisión

Función para la identificación y la corrección de CVE-2022-27518 El aviso de seguridad de NetScaler Console ahora admite la identificación y la corrección del CVE-2022-27518.

La identificación de CVE-2022-27518 requiere una combinación de un análisis de versiones y un análisis de configuración, y la corrección requiere actualizar las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.

Para obtener más información sobre cómo corregir el CVE-2022-27518, consulte el Aviso de seguridad.

> **NOTA**
>
> Es posible que el escaneo del sistema de avisos de seguridad tarde un par de horas en concluir y reflejar el impacto de CVE-2022-27518 en el módulo de avisos de seguridad. Para ver el impacto con mayor rapidez, puede iniciar un escaneo bajo demanda haciendo clic en **Escanear ahora**.

09 de diciembre de 2022

Análisis

Suspensión de Advanced Security Analytics para las instancias de ADC con licencia Premium NetScaler Console ya no admite **Advanced Security Analytics** para las instancias de ADC con licencia premium. Con esta actualización, en la GUI de NetScaler Console:

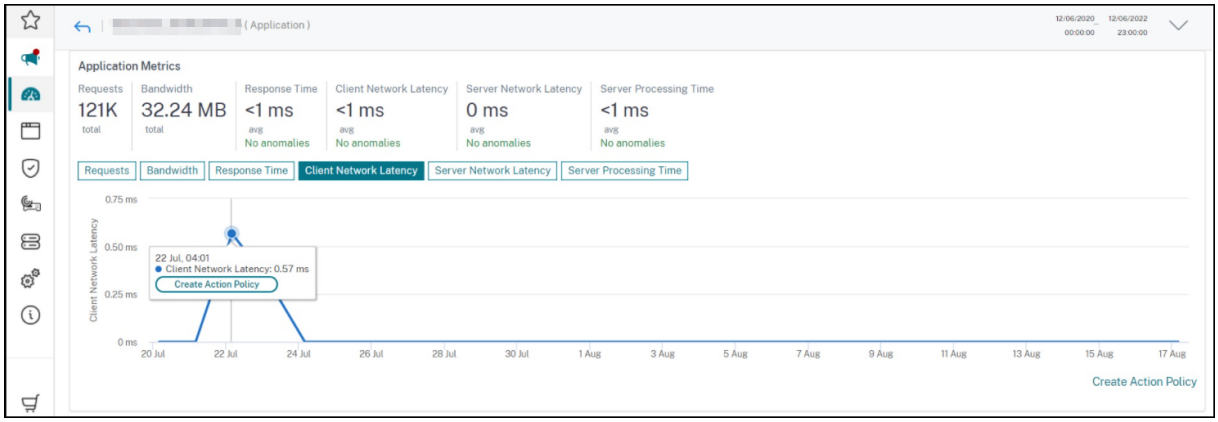
- Las configuraciones existentes en el análisis de seguridad avanzado y las infracciones asociadas basadas en el comportamiento ahora no están visibles.
- La visibilidad de las otras infracciones de bots y de WAF permanece inalterada. Para obtener más información, consulte las Categorías de infracciones.
- La exportación de Splunk y New Relic solo se admite en caso de infracciones de WAF y bots.

[NSADM-92342]

Configurar una directiva de acción desde Web Insight En **Web Insight**, ahora puede configurar una directiva de acción desde Graph Trend para las siguientes métricas:

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

Como administrador, cuando observa un patrón de tráfico inusual o un aumento repentino en estas métricas en cualquier aplicación, esta mejora le permite crear una directiva de acción relativa haciendo clic en **Crear directiva de acciones** después de colocarla en un punto específico del gráfico.



[NSADM-88682]

Directiva de acción: Agregar varias aplicaciones Al configurar una directiva de acciones para **Latencia de la red del cliente**, **Latencia de la red del servidor** y **Tiempo de procesamiento del servidor**, ahora puede seleccionar varias aplicaciones mediante el operador **IN** y aplicarlas en una sola directiva.

Para obtener más información, consulte Directivas de acción.

[NSADM-88680]

29 de noviembre de 2022

Infraestructura

La información de caducidad de la licencia Z se muestra en NetScaler Console Ahora puede ver la información de caducidad de las licencias Z de las instancias MPX y SDX en NetScaler Console. Para ello, vaya a **Infraestructura > Licencias agrupadas > Capacidad agrupada Licencias Z**.

[NSADM-80202]

Administración y supervisión

Funciones de SD-WAN y HAProxy descontinuadas en NetScaler Console NetScaler Console ya no admite las funciones SD-WAN y HAProxy. Como resultado, las funciones asociadas aplicables a SD-WAN y HAProxy ahora no están disponibles en la GUI de NetScaler Console.

[NSADM-90549]

Mejoras en la actualización de SDX: Función para seleccionar imágenes SDX de la biblioteca de recursos Al programar un trabajo de mantenimiento para actualizar una instancia SDX en NetScaler Console, ahora tiene la opción de seleccionar una opción de la biblioteca de imágenes necesaria para la actualización. Vaya a **Infraestructura > Actualizar trabajos > Crear trabajo**, seleccione **Actualizar NetScaler SDX** y haga clic en **Continuar** para actualizar una instancia de SDX.

[NSADM-88832]

Problemas resueltos

Los problemas que se abordan en la compilación del 29 de noviembre de 2022.

- Los usuarios de Azure AD no pueden iniciar sesión en ADM si un administrador los agregó a DaaS u otros productos de NetScaler antes que a ADM.

  [NSHELP-32556]

- En **Infraestructura > Funciones de red > Equilibrio de carga > Servicios**, el total de servicios configurados muestra solo 5000 recuentos, incluso cuando el recuento total de servicios configurados en las instancias de ADC es superior a 5000.

  [NSHELP-32299]

16 de noviembre de 2022

Análisis

Integración de New Relic Ahora puede integrar NetScaler Console con New Relic para ver los análisis de WAF, bots e infracciones basadas en el comportamiento en su panel de control de New Relic. Con esta integración, puede:

- Combinar 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 Console recopila eventos basados en bots, WAF y comportamientos y los envía a New Relic en tiempo real o de forma periódica, según su elección. Como administrador, también puede ver el bot, el WAF y otros eventos basados en el comportamiento en su panel de control de New Relic.

Para obtener más información, consulte Integración de New Relic.

[NSADM-83119]

Infraestructura

Actualización automatizada de grupos de Autoscale La operación de actualización de los grupos de Autoscale ahora está automatizada. Vaya a **Infraestructura > Nube pública > Grupos de Autoscale** y seleccione el grupo de Autoscale que quiere actualizar. NetScaler Console realiza las comprobaciones necesarias y actualiza el grupo Autoscale.

Para obtener más información, consulte Modificar grupos de escalado automático.

[NSADM-84955]

Administración y supervisión

Las métricas de uso de criptomonedas están disponibles en el panel de informes de ADM Service Network Ahora puede agregar y ver las métricas de uso de criptomonedas en el panel de informes de red. Vaya a **Infraestructura > Informes de red > Crear panel**. Seleccione **SSL Crypto Utilización** como entidad y cree un panel para la generación de informes de red.

[NSADM-88416]

Problemas resueltos

Los problemas que se abordan en la compilación del 16 de noviembre de 2022.

Las unidadescriptográficas asimétricas y las **unidades criptográficas simétricas** ahora son campos editables en la GUI de NetScaler Console. Puede introducir el número de ASU y SCU al aprovisionar una instancia de NetScaler VPX en el dispositivo NetScaler SDX con chips Intel Coleto (COL).

Vaya a **Infraestructura** > **Instancias** > **NetScaler**y, en la ficha SDX, seleccione una instancia SDX en **la** que quiera aprovisionar una instancia de NetScaler VPX. En **Seleccionar acción**, seleccione **Aprovisionar VPX** y, en la página que aparece, introduzca la capacidad criptográfica en **Asignación de criptomonedas**

[NSHELP-33297]

8 de noviembre de 2022

Administración y supervisión

Identificación y corrección de los CVE-2022-27510, CVE-2022-27513 y CVE-2022-27516 El aviso de seguridad de NetScaler Console ahora admite la identificación y la corrección de tres nuevos CVE: CVE-2022-27510, CVE-2022-27513 y CVE-2022-27516.

- La identificación del CVE-2022-27510 requiere una combinación de escaneo de configuración y escaneo de versiones, y la corrección requiere actualizar las instancias de ADC vulnerables a una versión y compilación que tengan la solución.
- La identificación del CVE-2022-27513 requiere una combinación de un escaneo de configuración y un escaneo de versiones, y la corrección requiere actualizar las instancias de ADC vulnerables a una versión y compilación que tengan la solución.
- La identificación del CVE-2022-27516 requiere una combinación de un escaneo de configuración y un escaneo de versiones, y la corrección requiere actualizar las instancias de ADC vulnerables a una versión y compilación que tengan la solución.

Para obtener más información sobre cómo corregir los CVE-2022-27510, CVE-2022-27513 y CVE-2022-27516, consulte el Aviso de seguridad.

> **Nota**
>
> El escaneo del sistema de asesoramiento de seguridad puede tardar un par de horas en concluir y reflejar el impacto de los CVE-2022-27510, CVE-2022-27513 y CVE-2022-27516 en el módulo de asesoramiento de seguridad. Para ver el impacto con mayor rapidez, puede iniciar un escaneo bajo demanda haciendo clic en **Escanear ahora**.

Junto con el boletín, también se publica un artículo de seguridad sobre los ataques de contrabando de solicitudes HTTP. Para obtener información sobre los ataques de contrabando de solicitudes HTTP, consulte CTX472830.

> **Nota**
>
> El aviso de seguridad de NetScaler Console solo admite la identificación y la corrección de los CVE. No soluciona los problemas de seguridad que se destacan en el artículo de seguridad. Por lo tanto, no ofrecemos la identificación y la corrección de los ataques de contrabando de solicitudes HTTP.

[NSADM-88525]

28 de octubre de 2022

Infraestructura

Especifique la zona horaria para la actualización del agente En **Infraestructura > Instancias > Agentes > Configuración > Actualización**, la hora de inicio utiliza la zona horaria que eligió en **Configuración global > Configuración del sistema**.

Para obtener más información sobre la configuración de la zona horaria, consulte Establecer la zona horaria de NetScaler Console.

[NSADM-88417]

Problemas resueltos

Los problemas que se abordan en la compilación del 28 de octubre de 2022.

En **Ajustes > Configuración de licencias y análisis > Configurar análisis**, los resultados de la página **Todos los servidores virtuales** desaparecen al aplicar los siguientes filtros:

- Nombre
- Estado
- Tipo

[NSHELP-32807]

Cuando configura una segunda NIC para aislar el acceso de administración a NetScaler Console, a la dirección IP de la segunda NIC se le asigna incorrectamente la misma dirección IP de la NIC principal.

[NSHELP-32567]

12 de octubre de 2022

Análisis

Infracciones de seguridad de WAF: vea los análisis de la gramática de En **Seguridad > Infracciones de seguridad**, en **WAF**, ahora puede ver los registros y los análisis de las infracciones **gramaticales de la inyección de comandos**. Para obtener más información, consulte:

- Verificación de protección de inyección de comandos HTML
- Infracciones de seguridad

[NSADM-85792]

Infraestructura

Valide su perfil de acceso a la nube con permisos adicionales El perfil de acceso a la nube existente del grupo de Autoscale que se conecta a AWS necesita permisos de IAM adicionales. Actualmente, el servicio NetScaler Console invalidaba los perfiles de acceso a la nube debido a la falta de permisos. Para validar los permisos de IAM, haga lo siguiente:

1. Copie los permisos de IAM más recientes mencionados en Crear roles de IAM.

2. Vaya a la consola de AWS y valide la función del perfil de acceso a la nube con los permisos de IAM más recientes.

[NSADM-90096]

27 de septiembre de 2022

Análisis

Infracciones de seguridad de WAF: vea los análisis de la palabra clave En **Seguridad > Infracciones de seguridad**, en **WAF**, ahora puede ver los registros y los análisis de las infracciones de **palabras clave de bloqueo y palabras clave** de **bloqueo de JSON**.

Para obtener más información, consulte:

- Compatibilidad con palabras clave personalizadas para la carga útil HTML
- Infracciones de seguridad

[NSADM-86225]

Configure la administración de bots en las instancias ADC platino En NetScaler Console, ahora puede:

- Configure las técnicas de detección de bots e impleméntelas en las instancias ADC de la versión 13.0 36.27 o posterior con una licencia premium.
- Consulte el análisis de bots activando la opción **Infracciones de seguridad de bots** para los servidores virtuales existentes configurados con técnicas de detección de bots, ya sea a través de StyleBook o directamente desde la instancia de ADC.

Junto con la configuración actual de StyleBook, esta mejora simplifica aún más el proceso de configuración de las técnicas de detección de bots e implementarlas en las instancias de ADC.

Para obtener más información, consulte Configurar las técnicas de detección de bots en NetScaler Console.

[NSADM-80413]

Infraestructura

Nueva opción para crear un trabajo de configuración para aplicaciones de Autoscale En **Grupos de Autoscale > Configuraciones**, ahora puede navegar hasta los trabajos de configuración seleccionando una aplicación de Autoscale. En la página **Crear trabajo**, aparecen comandos de ejemplo

basados en los detalles de configuración de la aplicación seleccionada. Puede modificar valores o comandos. Además, agregue o elimine comandos.

> **Nota**
>
> Puede usar los trabajos de configuración solo para las aplicaciones creadas mediante el modo de comandos CLI de ADC.

Para obtener más información, consulte Implementar una aplicación de Autoscale mediante trabajos de configuración.

[NSADM-85939]

NetScaler Console reprograma los trabajos cuando se producen imprevistos A veces, al ejecutar un trabajo de configuración o actualización, es posible que se enfrente a eventos como los siguientes:

- La actualización del servicio NetScaler Console está en curso.
- Un agente de ADM deja de funcionar. Puede ocurrir si la actualización del agente está en curso.

En estos casos, NetScaler Console reprograma los trabajos para la hora siguiente.

Anteriormente, NetScaler Console no podía identificar la actualización del servicio ADM ni el estado del agente. Como resultado, los trabajos fallaban después del tiempo de espera.

[NSADM-85554]

Ver la información de uso y licencia de las instancias ADC de CICO no administradas Ahora puede ir a **Infraestructura > Licencias agrupadas > Licencias de ancho de banda > CICO** para ver la información de uso y licencia de las instancias ADC de CICO no administradas en ADM Service.

[NSADM-85452]

Administración y supervisión

Genere un paquete de soporte técnico para la instancia ADC secundaria En un par de ADC de alta disponibilidad, ahora puede generar también un paquete de soporte técnico para el nodo secundario, desde la GUI de ADM. Anteriormente, solo se podía generar un paquete de soporte técnico para el nodo principal.

[NSADM-88905]

Vea los puntos de datos de informes de red para cada día del mes En **Infraestructura > Informes de red**, al seleccionar una duración de un mes en el panel, se muestran los puntos de datos de cada día. Anteriormente, mostraba los puntos de datos de cada semana.

[NSADM-88875]

StyleBooks

Los StyleBooks admiten instancias NetScaler BLX Al crear un paquete de configuración, ahora puede elegir instancias de NetScaler BLX como instancias de destino. Anteriormente, StyleBooks admitía instancias NetScaler MPX, SDX, VPX y CPX.

[NSADM-86253]

13 de septiembre de 2022

StyleBooks

StyleBooks predeterminados mejorados para configurar un servidor virtual de equilibrio de carga Con los StyleBooks predeterminados mejorados, ahora puede configurar todas las opciones compatibles en ADC para un servidor virtual de equilibrio de carga. Por ejemplo, ahora puede configurar el patrón IP, la máscara IP, el rango de IP y más. Anteriormente, solo se podían configurar unas pocas opciones desde StyleBooks. Hemos añadido los siguientes StyleBooks a NetScaler Console con sus versiones mejoradas:

Nombre	Versión
lb	2.0
lb-mon	2.0

[NSADM-80663]

Problemas resueltos

Los problemas que se abordan en la compilación del 13 de septiembre de 2022.

- Al invitar a un grupo de IAM seleccionando Azure AD como proveedor de identidades, las funciones de ADM no aparecen en **Acceso personalizado** si tienen espacios en blanco.

  [NSHELP-32557]

- Los usuarios de Azure AD no pueden iniciar sesión en ADM si un administrador los agregó a DaaS u otros productos de NetScaler antes que a ADM.

  [NSHELP-32556]

29 de agosto de 2022

Habilitar automáticamente Gateway Insight y Account Takeover para NetScaler Gateway

Todos los servidores virtuales de NetScaler Gateway con licencia ahora se habilitan automáticamente con **Account Takeover para NetScaler Gateway** y **Gateway Insight**. En NetScaler Console, esto le permite ver información sobre:

- Ataques de apropiación de cuentas para NetScaler Gateway en **Seguridad > Infracciones de seguridad**. La disponibilidad de la página de inicio de sesión de NetScaler Gateway se convierte en un blanco fácil para que los bots malintencionados roben las credenciales de los usuarios y realicen ciberataques, como el uso de credenciales Como administrador, es posible que quiera analizar si bots malintencionados han intentado apoderarse de la cuenta de NetScaler Gateway. Para obtener más información, consulte Adquisición de cuentas para NetScaler Gateway.
- Problemas relacionados con los servidores virtuales NetScaler Gateway en **Gateway > Gateway Insight**. Como administrador, es posible que quiera supervisar las instancias de gateway para obtener información como la actividad de inicio de sesión de los usuarios, los motivos de los errores de inicio de sesión, los usuarios activos, los usuarios disponibles, los ataques de bots, etc. Para obtener más información, consulte Gateway Insight.

> **Nota**
>
> La activación automática de las funciones de Gateway Insight y Account Takeover para NetScaler Gateway se lanzará a los clientes por fases.
>
> - La consola NetScaler debe tener uno o más agentes NetScaler externos configurados y tener uno o más dispositivos Premium o Advanced Gateway.
> - Una vez que se publique esta funcionalidad en NetScaler Console, todos los servidores virtuales NetScaler Gateway con licencia existentes y los servidores virtuales NetScaler Gateway con licencia posterior se habilitarán automáticamente con Gateway Insight y Account Takeover for NetScaler Gateway.
> - Para todos los servidores virtuales de NetScaler Gateway que se inhabiliten manualmente con la opción Gateway Insight, Gateway Insight no se habilitará automáticamente en esos servidores virtuales.
> - Para inhabilitar la opción **Gateway Insight** :

1. Vaya a **Configuración > Configuración de licencias y análisis**.
2. En **Resumen de análisis de servidores virtuales**, haga clic en **Configurar análisis**.
3. En la página **Todos los servidores virtuales**, seleccione el servidor virtual NetScaler Gateway y haga clic en **Modificar análisis**.
4. Deseleccione la opción **Gateway Insight** y haga clic en **Guardar**.

- La **adquisición de cuentas para NetScaler Gateway** se inhabilita automáticamente después de inhabilitar la opción **Gateway Insight**.

[NSADM-82732]

Mejoras en el panel de control unificado

El panel de control unificado en **Descripción general > Panel** de control ahora incluye widgets más pequeños para todas las métricas clave de cada categoría. Al hacer clic en **Modificar panel**, puede:

- 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.

Esta mejora le permite personalizar la vista del panel agregando o eliminando los widgets necesarios en cada categoría.

[NSADM-86337]

Elige un país de la región seleccionada

Al iniciar sesión en el servicio NetScaler Console por primera vez, ahora puede elegir el país que mejor se adapte a las necesidades de su empresa. Los países aparecen según la región seleccionada. Anteriormente, solo se podían seleccionar regiones.

Por ejemplo, si selecciona la región **EMEA**, la GUI muestra los siguientes países:

- Francia
- Reino Unido
- Alemania

Del mismo modo, puede elegir un país adecuado de otras regiones.

[NSADM-83643]

Web Insight: vea los detalles de los problemas relacionados con el cifrado

En **Aplicaciones > Web Insight**, en **Errores de SSL**, ahora puede desglosar la **diferencia de cifrado** para ver detalles como el nombre del cifrado SSL, las acciones recomendadas y los detalles de las aplicaciones y los clientes afectados.

Para obtener más información, consulte Web Insight.

Compatibilidad con la versión 3 de SNMP para la configuración de SDX en ADM

Ahora puede crear un perfil SNMP v3 para la instancia de NetScaler SDX desde la GUI de ADM. Vaya a la ficha **Infraestructura > Instancias > NetScaler > SDX** y, a continuación, haga clic en **Perfiles**. Puede agregar todos los parámetros del perfil, seleccionar la **versión 3** como tipo de perfil SNMP y, a continuación, hacer clic en **Crear** para crear un perfil SDX de NetScaler.

[NSADM-84828]

16 de agosto de 2022

Análisis

Panel de control de aplicaciones: vea información detallada para solucionar los problemas de la aplicación En el **panel de aplicaciones**, al profundizar en una aplicación, ahora puede ver las **acciones recomendadas** para los siguientes problemas de la aplicación, que le permiten ver información detallada para solucionar los problemas:

- Tiempo de respuesta
- Servicios Activos
- Servidor inestable
- Solapas de servicio

Para obtener más información, consulte Indicadores de rendimiento (problemas).

[NSADM-84811]

Infraestructura

Soporte de NIC dual para el agente ADM Puede configurar una segunda NIC en el agente ADM para administrar el acceso a NetScaler Console. Con la arquitectura de NIC dual, el agente ADM ahora podrá:

- Establecer la comunicación entre el agente de ADM y las instancias de ADC
- Establecer la comunicación entre el agente de ADM y el servicio de ADM

Para obtener más información, consulte Compatibilidad con dos NIC en NetScaler Console.

[NSADM-85781]

Recrea un clúster que forme parte del grupo Google Cloud Autoscale Para ver y solucionar los problemas de los clústeres de ADC que forman parte de un grupo de escalabilidad automática de Google Cloud (GCP), ahora puede ir a **Infraestructura > Nube pública > Grupo de escalabilidad automática**y hacer clic en **Ver clústeres**.

Puede seleccionar el **clúster de GCP** y hacer clic en **Recrear** para eliminar el clúster existente y sustituirlo por uno nuevo. Todas las configuraciones de la aplicación se transfieren al nuevo clúster de ADC.

Para obtener más información, consulte Ver y solucionar problemas de clústeres de ADC.

[NSADM-75731]

Administración y supervisión

Vea los detalles del agente de ADM en el panel unificado En el panel unificado, ahora 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 los agentes que están disponibles o no disponibles.

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.

Para obtener más información, consulte Descripción general del panel de control unificado.

[NSADM-83096]

Problemas resueltos

- Después de habilitar los análisis o al modificar los análisis para los servidores virtuales de NetScaler Gateway configurados a partir del par de alta disponibilidad, las **opciones de nivel de instancia** en **Configuración avanzada (opcional)** aparecen inhabilitadas, incluso después de que estas opciones estén habilitadas.

  [NSHELP-32188]

- En **Gateway > HDX Insight > Usuarios**, al seleccionar un usuario, en lugar de mostrar los detalles del usuario seleccionado, ADM muestra los detalles de todos los usuarios.

  [NSHELP-32181]

- En **Gateway > HDX Insight > Instancias**, cuando hace clic en un país para obtener más detalles, los datos de **Sesiones actuales** no se muestran.

  [NSHELP-32125]

13 de julio de 2022

Administración y supervisión

Soporte para la identificación y corrección del CVE-2022-27509 El aviso de seguridad de NetScaler Console ahora permite identificar y corregir el CVE-2022-27509.

La identificación de CVE-2022-27509 requiere una combinación de escaneo de versiones y escaneo personalizado, y la corrección requiere una actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución. Si las instancias de ADC vulnerables tienen el archivo `/etc/httpd.conf` copiado en el directorio `/nsconfig`, consulte [Consideraciones de actualización para configuraciones de ADC personalizadas] antes de planificar la actualización 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.

Para obtener más información sobre cómo ADM identifica los ADC vulnerables a CVE-2022-27509 y los pasos para solucionarlos, consulte Identificar y corregir las vulnerabilidades de CVE-2022-27509.

> **Nota**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde un par de horas en concluir y reflexionar sobre el impacto del CVE-2022-27509 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, puede iniciar un análisis bajo demanda haciendo clic en **Escanear ahora**.

[NSADM-85549]

Configurar una directiva de acceso para los trabajos de actualización Como superadministrador, ahora puede configurar una directiva de acceso, establecer los permisos (ver/editar) para los trabajos de actualización y aplicar la directiva a los usuarios de NetScaler Console. En **Configuración**

> Usuarios y funciones > Directivas de acceso, haga clic en **Agregar** para configurar una directiva de acceso seleccionando **Infraestructura > Trabajos de actualización** en **Permisos**.

Para obtener más información, consulte Configurar directivas de acceso en NetScaler Console.

[NSADM-82494]

Soporte para la auditoría de configuración en instancias de NetScaler BLX en modo compartido Ahora puede crear plantillas de auditoría de configuración con determinadas configuraciones y supervisar los cambios de configuración en las instancias de NetScaler BLX en modo compartido. Para obtener más información, consulte Crear plantillas de auditoría.

[NSADM-82323]

Compatibilidad con el formato CSV y la exportación programada en el análisis de transacciones web En el **análisis de transacciones web**, ahora puede ver las siguientes mejoras al hacer clic en el icono **Exportar** :

- En **Exportar ahora**, puede exportar datos en formato CSV.
- Se introduce la opción **Programar exportación** que le permite programar y exportar los datos en formato CSV a través del correo electrónico y Slack.

Para obtener más información, consulte Análisis de transacciones web.

Problema resuelto

En el servicio NetScaler Console, al ir a **Infraestructura > Instancias Agentes** y hacer clic en **Configuración** para cambiar la configuración de actualización del agente, aparece un mensaje de confirmación **Configuración de actualización del agente modificada** una vez cambiada la configuración.

[NSHELP-32099]

29 de junio de 2022

Aplicaciones

Configurar y asociar una aplicación a varias aplicaciones personalizadas En **Panel de aplicaciones**, ahora puede configurar una aplicación y asociarla a varias aplicaciones personalizadas. Con esta función, puede reutilizar la misma aplicación para varias aplicaciones personalizadas, en lugar de crear una aplicación independiente para cada aplicación personalizada.

Para obtener más información, consulte Configurar y asociar una aplicación a varias aplicaciones personalizadas.

[NSADM-82040]

Administración y supervisión

Navegadores compatibles para acceder a la GUI de NetScaler Console Ahora solo se puede acceder a la GUI de NetScaler Console desde las siguientes versiones de navegadores compatibles:

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

[NSADM-83943]

15 de junio de 2022

Infraestructura

Supervise el uso de los parámetros del sistema del agente NetScaler y solucione los problemas mediante el demonio de reparación automática El agente de NetScaler ahora monitoriza los recursos de su sistema (CPU, memoria y disco) mediante la ejecución automática del daemon de recuperación automática en segundo plano. El demonio de autorreparación comprueba los umbrales y aplica las acciones automáticamente en los siguientes escenarios:

- Si el uso del disco supera el 80% o más durante un período específico, se aplica la acción de limpieza de espacio (registros, registros de respaldo, archivos principales, archivos bloqueados, etc.) para recuperar el espacio en disco.
- Si el uso de la memoria y la CPU supera el 90% o más durante un período específico, los procesos de ADM se reinician para recuperar la CPU y la memoria.

> **Nota**
>
> El demonio de reparación automática no supervisa los umbrales configurados en **Infraestructura > Instancias > Agentes > Configuración > Notificación**.

[NSADM-82558]

07 de junio de 2022

Análisis

Ver análisis de bots y WAF para aplicaciones personalizadas En **Seguridad > Infracciones de seguridad**, en **WAF** y **Bot**, ahora puede seleccionar una aplicación personalizada y ver los detalles de las aplicaciones consolidadas aplicables a una aplicación personalizada. También puede seleccionar una aplicación de la lista y ver los detalles de una aplicación concreta de la aplicación personalizada.

Para obtener más información, consulte Infracciones de seguridad.

[NSADM-77375]

Administración y supervisión

Importe e instale el paquete de certificados SSL (con cadena de certificados) a través del almacén de certificados En **Infraestructura > Panel de control SSL**, al seleccionar **Administrar almacén de certificados** en la lista disponible junto a **Configuración**, puede:

- Haga clic en **Importar certificados ADC > Iniciar sondeo** y el paquete de certificados SSL, junto con la cadena de certificados que vincula el certificado del servidor a su emisor (la CA intermedia), se importarán de la instancia de ADC al almacén de certificados.
- Consulte los certificados en el almacén de certificados, seleccione un certificado y haga clic en **Instalar** para instalar el certificado junto con la cadena de certificados en las instancias de ADC seleccionadas.

[NSADM-82727]

Actualización de versión disponible para instancias BLX de NetScaler En **Infraestructura > Trabajos de actualización**, ahora puede crear un trabajo para actualizar las instancias BLX de NetScaler. Debe seleccionar la imagen de compilación adecuada (aplicable a Ubuntu o Red Hat) para que la actualización se realice correctamente. Para obtener más información, consulte Trabajos de mantenimiento.

[NSADM-82324]

Problema resuelto

En **Infraestructura > Resumen de eventos > Mensajes de Syslog**, los datos solo se han mostrado durante los últimos 30 días. Con esta corrección, los datos se muestran hasta 180 días.

[NSHELP-30961]

10 de mayo de 2022

Análisis

Exportar datos en tiempo real a Splunk La integración de NetScaler Console con Splunk ahora le permite exportar datos en tiempo real a Splunk. En la GUI de ADM, al seleccionar la opción **Exportar en tiempo real** y configurarla, las infracciones seleccionadas en NetScaler Console se envían inmediatamente a Splunk.

Para obtener más información, consulte Integración con Splunk.

[NSADM-84529]

Mejoras en el motor de aprendizaje WAF En NetScaler Console, ahora puede configurar un perfil de aprendizaje e implementar u omitir las reglas de relajación para las siguientes comprobaciones de seguridad adicionales:

- **JSON SQL**
- **inyección de comandos JSON**
- **JSON XSS**

> **Nota**
>
> Para configurar un perfil de aprendizaje mediante estas comprobaciones de seguridad, la instancia de NetScaler debe tener un tamaño de 13.1 a 14.10 o posterior.

Para obtener más información, consulte Motor de aprendizaje WAF.

[NSADM-80921]

Aplicaciones

Mejoras en el panel de control unificado El panel unificado de **Información general > Panel de control** ahora le permite personalizarlo según su elección. Con la opción **Modificar panel** de control, puede:

- Arrastrar widgets
- Eliminar widgets
- Agregar widgets
- Restablecer los valores predeterminados

Tras realizar los cambios, haga clic en **Guardar**.

> **Nota**
>
> De forma predeterminada, se muestran todos los widgets. Si ha personalizado el panel, ha guardado los cambios y ha utilizado la opción Restablecer a la configuración predeterminada, se restaurará el último panel personalizado guardado.

[NSADM-52144]

Infraestructura

Mejoras en la interfaz gráfica de usuario de ADM Ahora puede expandir o contraer el menú de navegación de la GUI de ADM de forma individual. Esta mejora le permite ver todas las opciones de cada sección.

[NSADM-85480]

Soporte para la identificación y corrección de los CVE-2022-27507 y CVE-2022-22508 El aviso de seguridad de NetScaler Console ahora admite la identificación y la corrección de dos nuevas CVE: **CVE-2022-27507** y **CVE-2022-22508**.

- La identificación de **CVE-2022-27507** requiere una combinación de un análisis de versiones y un análisis de configuración, y la corrección requiere una actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.

  El aviso de seguridad de ADM no admite la mitigación. Si ha aplicado la mitigación (solución temporal) a la instancia de ADC, ADM seguirá identificando el ADC como vulnerable hasta que haya completado la corrección.

  Para el **CVE-2022-27507**, incluso si ha aplicado la mitigación y ha desactivado temporalmente HDX Insight para el tráfico de EDT (consulte el boletín de seguridad), el aviso de seguridad de ADM seguirá identificando el ADC como vulnerable hasta que haya completado la corrección (actualización a una versión y la compilación que tenga corregir).

- La identificación de **CVE-2022-27508** requiere una combinación de escaneo de versiones y análisis de configuración, y la corrección requiere una actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.

  Para obtener más información sobre cómo corregir los CVE-2022-27507 y CVE-2022-22508, consulte el Aviso 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 de los **CVE-2022-27507** y **CVE-2022-27508** en el módulo

> de asesoramiento de seguridad. Para ver el impacto antes, puede iniciar un análisis bajo demanda haciendo clic en **Escanear ahora**.

[NSADM-85673]

Problema resuelto

En **Infraestructura > Instancias > NetScaler**, cuando cambia la contraseña de un perfil de administrador e incluye% en la contraseña, aparece un mensaje de error.

[NSHELP-31392]

27 de abril de 2022

Administración y supervisión

Desactualización de ADC a través de la GUI de ADM con el archivo `ns.conf` correcto En **Infraestructura > Trabajos de actualización**, al crear un trabajo de actualización para actualizar la instancia de ADC a una versión inferior, ADM ahora selecciona el archivo `ns.conf` compatible desde el que se aplica la configuración a la instancia de ADC. El archivo `ns.conf` seleccionado debe ser de la misma versión o inferior a la seleccionada por el usuario. Si no hay ningún archivo `ns.conf` adecuado en la instancia de ADC, no se permite la degradación y se muestra el mensaje de error correspondiente.

[NSADM-81421]

Problemas resueltos

- Al habilitar **Advanced Security Analytics**, aplicar un perfil con una o más infracciones basadas en el comportamiento y hacer clic en **Guardar**, los detalles de la tabla no se muestran en **Configuración > Configuración de licencias y análisis > Todos los servidores virtuales**.

  Nota: Las infracciones basadas en el comportamiento son el exceso de conexiones con los clientes, las transacciones de carga inusualmente grandes, las transacciones de descarga inusualmente grandes y la tasa de solicitudes inusualmente alta.

  [NSADM-85020]

- En **Infraestructura > Resumen de eventos > Mensajes de Syslog**, los datos solo se han mostrado durante los últimos 30 días. Con esta corrección, los datos se muestran hasta 180 días.

  [NSHELP-30961]

12 de abril de 2022

Análisis

Se agregaron nuevas infracciones para limitar la velocidad de las infracciones La regla de limitación de velocidad detecta varias solicitudes procedentes del mismo cliente. En **Seguridad > Infracciones de seguridad > Descripción general de la aplicación**, en **Bot**, ahora puede ver los siguientes detalles de la infracción:

- **URL**
- **IP de origen**
- **Ubicación geográfica**
- **Sesión**

Haga clic en **Registros** para ver detalles como la hora, la IP del cliente, el tipo de bot, la detección de bots, etc. Para obtener más información, consulta Ver los detalles de la infracción del bot.

[NSADM-80925]

Función para infracciones de explorador web sin encabezado en infracciones de bots En **Seguridad > Infracciones de seguridad > Descripción general de la aplicación**, en **Bot**, ahora puede ver los detalles de **Infracciones de explorador web sin encabezado**. Haga clic en **Registros** para ver detalles como la hora, la IP del cliente, el tipo de bot, la detección de bots, etc.

Para obtener más información, consulta Ver los detalles de la infracción del bot.

[NSADM-89027]

Administración y supervisión

El CVE-2022-21827 no entra en el ámbito del aviso de seguridad de NetScaler Console El CVE-2022-21827 afecta al complemento NetScaler Gateway para las versiones compatibles con Windows anteriores a la 21.9.1.2.

NetScaler Console no admite la detección y reparación de las vulnerabilidades que afectan al complemento 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 solución de esta vulnerabilidad están fuera del alcance del asesoramiento de seguridad de NetScaler Console.

Para obtener más información, consulte los CVE no compatibles en Security Advisory.

Opción de cancelación de suscripción disponible en los correos electrónicos de productos enviados al cliente Los clientes (clientes nuevos e inactivos) ahora tienen la opción de cancelar la suscripción a todas las notificaciones por correo electrónico incluidas en los correos electrónicos de productos enviados por NetScaler Console. Para obtener más información sobre cómo suscribirse o cancelar la suscripción, consulte Suscripciones por correo

[NSADM-83272]

Conservar filtros en el panel de aplicaciones En **Aplicaciones > Panel de control**, al aplicar filtros a través de la barra de búsqueda y las métricas clave, los filtros ahora se conservan. Puede ver los mismos filtros aunque:

- Vuelva a **Aplicaciones > Panel de control** desde una navegación diferente dentro de la GUI de ADM.
- Cierre el explorador web y abra una nueva sesión desde el mismo explorador.

> **Nota**
>
> Los filtros no se conservan si abre una nueva sesión desde un explorador web diferente o en modo incógnito.

[NSADM-82038]

StyleBooks

Actualización automática de los paquetes de configuración Cuando se actualiza un certificado SSL en el almacén de certificados de NetScaler Console, los paquetes de configuración asociados al certificado SSL se actualizan automáticamente.

[NSADM-80694]

31 de marzo de 2022

Análisis

Mejoras en el análisis de seguridad avanzado en caso de infracciones Como mejora de la función de análisis de seguridad avanzado, ahora se ha simplificado el proceso para habilitar primero el **análisis de seguridad avanzado** y, a continuación, crear un perfil mediante el icono de **configuración**. Ahora puede habilitar **Advanced Security Analytics**, crear un perfil y asignar el perfil a los servidores virtuales en un único flujo de trabajo.

Para obtener más información, consulte Habilitar el análisis de seguridad avanzado.

[NSADM-81383]

Mejoras en el panel de control unificado En **Descripción general > Panel de control**, ahora puede ver las siguientes mejoras:

- Puede hacer clic en los recuentos de métricas clave en todas las categorías para ver los detalles de la instancia de ADC/aplicación/Gateway afectada.
- En **Aplicaciones**, se realizaron cambios menores en la GUI en las métricas clave de SSL para visualizar más información.
- En **Gateway**, la **distribución geográfica de usuarios** muestra los 3 países principales según el recuento de usuarios.

[NSADM-82758]

Administración y supervisión

Compatibilidad con el algoritmo ECDSA en el panel de control SSL Al configurar una directiva empresarial en el **panel SSL > Configuración > Directiva empresarial**, ahora puede seleccionar **ECDSA** en el **Algoritmo de firma recomendado**.

Para obtener más información sobre ECDSA, consulte el soporte de los conjuntos de cifrado ECDSA.

Para obtener más información sobre la configuración de la directiva empresarial, consulte Configurar una directiva empresarial.

[NSADM-71321]

Incorporación

Compatibilidad con ADM para la versión 1.23 de Kubernetes NetScaler Console ahora admite agregar y administrar clústeres con la versión 1.23 de Kubernetes.

[NSADM-83683]

16 de marzo de 2022

Incorporación

Pruebe la preparación para la incorporación de las instancias de ADC Si quiere incorporar una instancia de ADC a NetScaler Console mediante la opción de agente incorporado predeterminada,

puede realizar una prueba de ejecución para asegurarse de que la instancia de ADC esté lista para su incorporación. Para obtener más información, consulte Probar la preparación para la incorporación de las instancias de ADC.

[NSADM-80502]

01 de marzo de 2022

Administración y supervisión

Invitar usuarios o grupos a ADM desde Azure AD Como superadministrador, ahora puede invitar a usuarios o grupos a NetScaler Console desde el Azure AD conectado a NetScaler Console. Antes de hacerlo, asegúrese de que Azure AD esté conectado a Citrix Cloud, consulte Conectar Azure Active Directory a Citrix Cloud. Anteriormente, solo podía invitar a usuarios con Citrix Identity.

Al seleccionar Azure AD como proveedor de identidades, solo puede especificar el acceso personalizado para el usuario o grupo seleccionado. Los usuarios pueden iniciar sesión en NetScaler Console con sus credenciales de Azure AD. Con esta función, no necesita crear una identidad de Citrix para los usuarios que forman parte del Azure AD seleccionado. Si se agrega un usuario al grupo invitado, no es necesario que envíes una invitación para el usuario recién agregado. Este usuario puede acceder a NetScaler Console con las credenciales de Azure AD.

[NSADM-81039]

ADM guarda los certificados y los archivos clave cargados en ADC y la información se almacena en la base de datos de ADM Al cargar certificados y archivos de claves a Cert Store mediante el **panel de control SSL** de la GUI del servicio ADM, solo los metadatos y el contenido cifrado del archivo de certificado se guardan en la base de datos de ADM. La clave y la contraseña utilizadas para descifrar el contenido se guardan en Cloud Wallet.

[NSADM-72475]

Nuevos informes de red en ADM Los siguientes informes de red nuevos se agregan como contadores totales:

- **Autenticación correcta e incorrecta**
- **Autenticación HTTP correcta frente a fallos**
- **Autenticación no HTTP correcta frente a fallos**
- **Sesiones de la AAA**
- **Sesiones actuales de la AAA**

- **Sesiones ICAOnly actuales**
- **Conexiones ICAOnly actuales**
- **Conexiones ICA (Smart Access) actuales**

Puede usar estos contadores para agregar umbrales y recibir notificaciones. Para obtener más información, consulte Informes de red.

[NSADM-62239]

Directiva de acción: configure las notificaciones de bots y WAF con los detalles de la transacción En **Directivas de acción**, al configurar una directiva de acción, ahora puede seleccionar las opciones **Infracción de bots por cliente** e **Infracción de WAF por cliente**. Estas opciones le permiten configurar y recibir notificaciones con detalles de la transacción, como la IP del cliente, el total de ataques, el tipo de infracción, etc.

Para obtener más información, consulte Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación.

[NSADM-80630]

Inhabilitar los escaneos personalizados de Security Advisory La interfaz de usuario de NetScaler Application Delivery Management Service ahora le permite excluirse de los análisis personalizados de asesoramiento de seguridad Si opta por no participar en estos escaneos personalizados de asesoramiento de seguridad, el impacto de los CVE que necesitan un escaneo personalizado no se evaluará para sus instancias de ADC en el Aviso de seguridad.

Para excluirse de los escaneos personalizados de Security Advisory, consulte Configuración de escaneo personalizado.

[NSADM-80288]

StyleBooks

Utilice etiquetas de formato HTML en la descripción y el encabezado del StyleBook En la definición de **StyleBook**, ahora puede incluir un campo de encabezado y utilizar etiquetas de formato HTML para el texto. También puede incluir imágenes como parte del encabezado y se mostrará en la parte superior del formulario de configuración. Esta función permite agregar infografías para los usuarios de StyleBook que ayudan a entender la configuración de StyleBook. Si usa imágenes en el encabezado, asegúrese de usar el formato de imagen codificado en base64 en la etiqueta `image`.

```
name: app-stylebook-with-HTML-tags
namespace: com.examples.stylebooks
version: `1.0`
```



```
4 display-name: `Example App StyleBook`
5 header: 'This <b> StyleBook </b> defines all the app configuration for
     <i>Load Balanced Application </i>. The following image describes the
      target deployment for the app <img id=`b64img` src=`data:image/png;
     base64,` />'
```

[NSADM-80699]

Ofrezca aplicaciones de escalabilidad automática que estén fuera de la red virtual o VPC de las instancias de ADC Cuando los servidores de aplicaciones y las instancias de ADC estén situados en diferentes redes virtuales, redes de VPC y subredes, proporcione el bloque CIDR de una subred o VPC en la que haya servidores de aplicaciones. Especifique el bloque CIDR en el campo **Servidor de origen** al configurar los parámetros de aprovisionamiento. De esta forma, puede entregar aplicaciones desde los servidores de aplicaciones que se encuentran fuera de la red virtual o la red de VPC de las instancias de ADC.

Anteriormente, esta función solo estaba disponible para los grupos de Autoscale en AWS, ahora puede utilizarla también en Azure y Google Cloud.

Para obtener más información, consulte:

- Microsoft Azure.
- Google Cloud.

[NSADM-78617]

10 de febrero de 2022

Administración y supervisión

Compatibilidad con la plantilla ShowConfiguration En el Editor de configuración, al seleccionar **Configuración por lotes**, ahora puede usar la plantilla **ShowConfiguration**. Arrastre la plantilla **ShowConfiguration** al panel derecho e introduzca los comandos show que se ejecutarán en las instancias de NetScaler.

Por ejemplo, puede introducir comandos como `sh ns info`, `sh node`, `sh ns stats`, `sh interface` y `shell ls /var/tmp` y ver el resultado.

Puede descargar el resultado de los comandos como un archivo de texto.

[NSADM-66132]

Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación Además de la vista analítica existente de los eventos de la aplicación, puede configurar una directiva

de acción para recibir notificaciones de eventos de la aplicación a través de Slack, Email, PagerDuty o ServiceNow. Los eventos de la aplicación incluyen problemas de rendimiento, infracciones de bots y WAF e infracciones de gráficos de servicio. Como administrador, mediante la directiva de acción, puede recibir notificaciones de eventos en tiempo real.

Con la directiva de acción, puede:

- Predefina ciertas condiciones para los eventos de la aplicación.
- Recibe notificaciones de los siguientes eventos a través de Slack, Email, PagerDuty y ServiceNow:
  - **Infracción de SQL de WAF**
  - **Infracción de WAF XSS**
  - **WAF deduce una infracción de XML**

    > **Nota**
    >
    > Para recibir la notificación de infracción de la WAF, las transacciones de infracción mínimas deben ser del 20%. Por ejemplo, de cada 100 transacciones, un mínimo de 20 deben ser transacciones de infracción.

  - **Las 3 principales infracciones de WAF**

    (El total de infracciones aportadas por SQL, XSS y XML en conjunto debe ser del 30%. Por ejemplo, de cada 100 transacciones, 30 o más deben ser una combinación de infracciones de SQL, XSS e inferir XML.)
  - **Infracciones de bots**

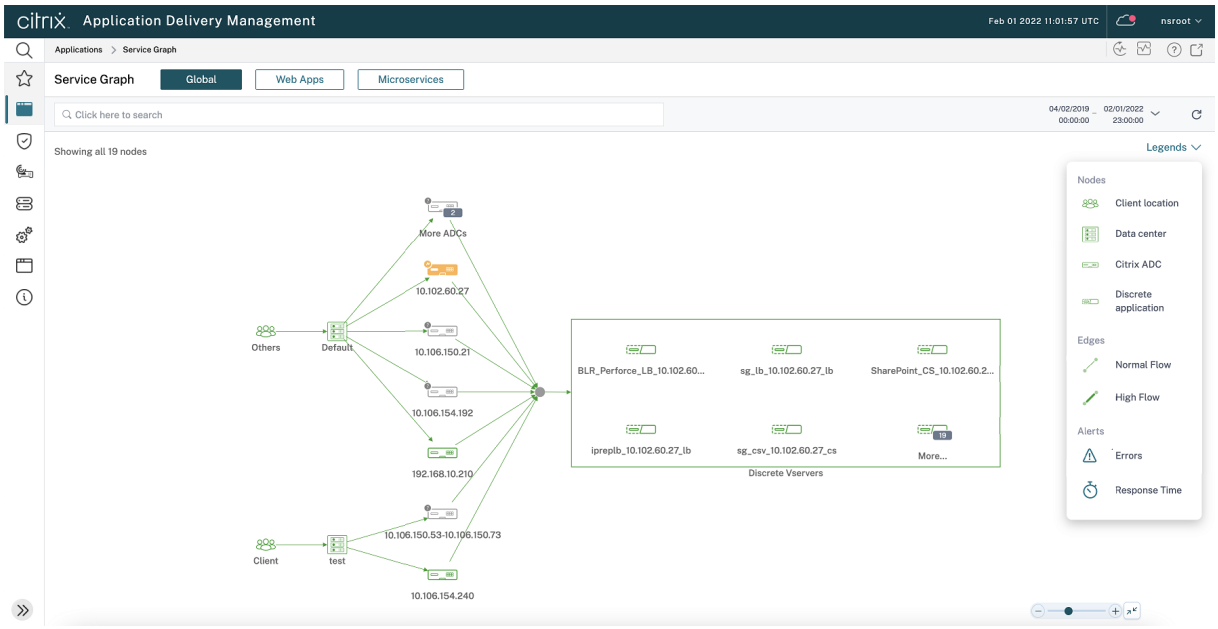
    (Para obtener más información sobre la lista de infracciones de bots, consulta las categorías de infracciones).
  - **Infracción de la puntuación**
  - **Latencia de red del cliente**
  - **Latencia de red del servidor**
  - **Tiempo de procesamiento del servidor**
  - **Infracción del gráfico de**

Para obtener más información, consulte Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación.

[NSADM-70968], [NSADM-76588], [NSADM-72799]

Aplicaciones

Mejoras en el gráfico de servicio En el gráfico de servicios globales y el gráfico de servicios de microservicios, ahora puede ver la leyenda que proporciona la descripción de los símbolos disponibles en el gráfico de servicios.



[NSADM-82077]

Incorporación

Configure los ajustes para los correos electrónicos de flujo de trabajo de incorporación de Como parte del flujo de trabajo de incorporación sencillo basado en ADM Service Connect, recibirá correos electrónicos iniciados por el producto del servicio NetScaler Console. Puede configurar y administrar los correos electrónicos que recibe como parte de este flujo de trabajo de las siguientes maneras:

- Habilitar los correos electrónicos para todos los administradores
- Activar o desactivar los correos electrónicos para los administradores seleccionados
- Desactivar los correos electrónicos para todos los administradores

Para obtener más información sobre cómo configurar y administrar los correos electrónicos, consulte Configuración del correo electrónico.

[NSADM-80289]

Vea los diagnósticos del agente de NetScaler y reciba alertas para la verificación de terminales NetScaler Console ahora realiza una comprobación de diagnóstico periódica (cada una hora) para el agente NetScaler y proporciona la siguiente información:

- **Accesibilidad de puntos finales**
- **sonda de control de salud**
- **Proxy de agente**

Si el estado de accesibilidad del punto final del agente cambia (de **Aceptar** a **Necesita revisión**), el superadministrador recibe una notificación por correo electrónico con los detalles del problema.

Para obtener más información, consulte Ver los diagnósticos de los agentes y recibir alertas para la verificación de terminales.

[NSADM-69407]

StyleBooks

Las actualizaciones del paquete de configuración de StyleBook se concilian automáticamente A veces, la actualización de un paquete de configuración de StyleBook que está implementado en una instancia de ADC puede tener diferencias con respecto a su estado implementado. En esos casos, se produce un error al actualizar el paquete de configuración. El motor StyleBook ahora concilia automáticamente estas diferencias y actualiza el paquete de configuración. Anteriormente, aparecía un mensaje en la GUI que requería su confirmación para conciliar los cambios antes de actualizar el paquete de configuración.

[NSADM-80660]

Gestione las fuentes de datos en ADM Definir una fuente de datos en NetScaler Console le ayuda a utilizar los datos de fuentes externas como entrada al crear o actualizar las configuraciones de StyleBook. De lo contrario, debe proporcionar de forma explícita cada entrada requerida por el StyleBook. En NetScaler Console, puede usar cualquier instancia de ADC administrada como fuente de datos para la entrada a una configuración de StyleBook. En NetScaler Console, puede usar las instancias ADC administradas como fuentes de datos. También puede definir fuentes de datos personalizadas que pueden servir de entrada al crear o actualizar configuraciones. Para ver las fuentes de datos personalizadas, vaya a **Aplicaciones > Configuración > Fuentes de datos**.

Utilice el tipo integrado `datum` en la definición de StyleBook para definir una fuente de datos.

Ejemplo:

```
parameters:
  -
```



```
    name: selected-lb
    label: Select an existing ADC
    type: datum
    required: true
    data-source:
      type: managed-adc
```

En este ejemplo, el parámetro `datum` se utiliza para definir el origen de datos `managed-adc`. Esta fuente de datos le permite recuperar datos de las instancias de ADC administradas por NetScaler Console.

[NSADM-80659]

Compruebe la compatibilidad de StyleBook para obtener un paquete de configuración Al cambiar el StyleBook por un paquete de configuración en la GUI de ADM, ahora puede determinar los cambios a partir de la definición de StyleBook recién seleccionada. Y cómo afectan estos cambios al paquete de configuración. Con esta información, puede realizar las actualizaciones necesarias en la definición de StyleBook antes de cambiarla. O bien, puede decidir continuar con el StyleBook existente.

Por ejemplo, si cambia el StyleBook por un paquete de configuración, el StyleBook existente puede tener un puerto HTTPS permitido, mientras que el StyleBook recién seleccionado puede tener SSL. En este caso, es posible que también tengas que modificar los mismos valores de HTTPS para el puerto SSL.

[NSADM-80664]

25 de enero de 2022

Integración de ADC con baja interacción en ADM: vea los diagnósticos automatizados

La siguiente información solo se aplica a las instancias de ADC que están conectadas al servicio ADM a través de la función de conexión del servicio de ADM.

Anteriormente, existía un proceso manual para utilizar la herramienta de diagnóstico para solucionar los problemas de incorporación con poca interacción. Ahora, también puede ver la información de diagnóstico sobre las instancias de ADC que tienen problemas con la incorporación con poca interacción en la GUI de ADM.

Cuando se encuentra en el flujo de trabajo de incorporación de baja interacción basado en ADM Service Connect, en la página **Inventario de activos** puede ver la opción de **preparación para la incorporación** recientemente agregada que proporciona el estado de preparación para la incorporación de la instancia de ADC, como **Necesita revisión** u **Aceptar**.

También puede ver esta vista yendo a **Infraestructura > Instancias > NetScaler** y haciendo clic en la opción **Inventario de activos**.

A continuación, puede utilizar esta información para comprender y resolver los problemas.

Para obtener más información, consulte Solucionar problemas con la herramienta de diagnóstico o la GUI de ADM.

[NSADM-77245]

Soporte para la incorporación con poca interacción de clientes que aún no están en la nube de Citrix

Como parte de la incorporación sencilla de instancias de NetScaler mediante el flujo de trabajo de ADM Service Connect, los clientes que aún no estén en Citrix Cloud ahora podrán registrarse en la nube de Citrix e incorporar sus instancias de ADC en ADM Service fácilmente. Estos clientes recibirán un correo electrónico del servicio de consola NetScaler que los guiará hacia la incorporación **al servicio ADM**. Al hacer clic en este botón, pueden registrarse en Citrix Cloud e incorporar sus instancias de ADC en el servicio ADM mediante el flujo de trabajo de incorporación de baja interacción. Para obtener más información, consulte Incorporación discreta de instancias de NetScaler mediante service connect.

[NSADM-76466]

Análisis de infraestructura: configure notificaciones para problemas específicos

En **Infrastructure Analytics**, ahora puede seleccionar los problemas necesarios, habilitar las notificaciones de problemas que infrinjan los umbrales configurados y recibir notificaciones solo para los problemas seleccionados. Anteriormente, se recibían notificaciones de todos los problemas. Esta mejora le permite recibir notificaciones solo para los problemas seleccionados que quiera supervisar.

Para obtener más información, consulte Configurar notificaciones.

[NSADM-76361]

17 de enero de 2022

Compatibilidad con ADM para clúster BLX

Ahora puede agregar el clúster BLX en ADM. En la GUI de ADM, se agrega la dirección IP del clúster (CLIP) y el recuento de los nodos del clúster ahora está visible en el panel.

[NSADM-78588]

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, consulta Un panel unificado para ver los detalles de las métricas clave de la instancia.

[NSADM-74075]

Infracción de seguridad: Gramática de inyección SQL JSON

En **Seguridad > Infracciones de seguridad**, en **WAF**, ahora puede ver la infracción de **gramática de inyección JSON SQL** para la aplicación seleccionada. Para obtener más información, consulte Detalles de la infracción.

[NSADM-62909]

Utilice las palabras clave reservadas del StyleBook para los parámetros y las expresiones

Ahora puede utilizar las palabras clave reservadas al definir parámetros y expresiones en una definición de StyleBook. Las palabras clave reservadas son las siguientes:

```
1 "and", "false", "in", "not", "true", "or"
```

Por ejemplo, un parámetro denominado ahora `not` es un parámetro válido (`$parameters.not`).

[NSADM-80657]

Los StyleBooks admiten condiciones de parámetros anidados

En una definición de StyleBook, ahora puede especificar una condición de parámetro dentro de una condición de parámetro. Estas condiciones se denominan condiciones de parámetros anidados y utilizan una construcción de repetición para definir estas condiciones. Las condiciones de los parámetros anidados son útiles cuando se quiere aplicar una acción a cada elemento de un parámetro de la lista.

Ejemplo:

```
parameters-conditions:
  -
    repeat: $parameters.lbvservers
    repeat-item: lbvserver
    parameters-conditions:
      -
        target: $lbvserver.port
        action: set-allowed-values
        condition: $lbvserver.protocol == "HTTPS"
        value: $parameters.ssl-ports
```

En este ejemplo, cuando el usuario selecciona el protocolo HTTPS para un servidor virtual de equilibrio de carga, los valores del puerto se rellenan dinámicamente. Además, se aplica a cada uno de los servidores virtuales de equilibrio de carga de la lista.

Para obtener más información, consulte Condiciones de parámetros anidados.

[NSADM-62747]

Problema resuelto

En una configuración de GSLB, cuando tiene el mismo nombre de dominio para varias instancias de ADC, el sondeo de la entidad actualiza incorrectamente la base de datos.

[NSHELP-29885]

Problemas conocidos

July 17, 2024

NetScaler Application Delivery Management (NetScaler Console) presenta los siguientes problemas conocidos:

Administración y supervisión

En **Infraestructura > Panel de control SSL > Administrar almacén** de certificados, al hacer clic en **Importar certificados** de NetScaler, NetScaler Console no puede importar los certificados de NetScaler en formato PFX.

[NSHELP-34803]

Infraestructura

- 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]

- Cuando se crea una regla de eventos con algunas entidades seleccionadas en **Infraestructura > Eventos > Reglas > Crear regla > Seleccionar objetos de error**, no se muestran todas las entidades seleccionadas. Este problema se produce cuando hay una gran cantidad de servidores, servicios o grupos de servicios virtuales.

  Solución temporal: Contacte con el equipo de asistencia de NetScaler para obtener ayuda con este problema.

  [NSADM-110553]

Cumplimiento de datos

January 26, 2024

Conformidad con PCI DSS

El estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI) es un estándar de seguridad del sector de las tarjetas de crédito que define el nivel de seguridad requerido para las personas, los procesos y la tecnología que debe existir al almacenar, procesar o transmitir datos de tarjetas de crédito. El PCI DSS se aplica a los comerciantes, procesadores y proveedores de servicios, así como a todas las demás entidades que almacenan, procesan o transmiten datos de tarjetas de crédito. La certificación de cumplimiento (AOC) de PCI DSS es, en última instancia, una certificación de una entidad de que se requiere y existe un nivel de seguridad específico.

El servicio de administración de entrega de aplicaciones de NetScaler cumple con PCI DSS

El servicio de gestión de entrega de aplicaciones (ADM) de NetScaler ha alcanzado satisfactoriamente el cumplimiento de PCI DSS mediante una evaluación de los dominios de control de cumplimiento de PCI DSS para los clientes. El servicio NetScaler Console no almacena, procesa ni transmite los datos PCI de los clientes. El servicio de consola NetScaler también se someterá anualmente a una evaluación PCI DSS por parte de un evaluador de seguridad cualificado (QSA) para evaluar nuestros servicios y controles.

Si bien Citrix ayuda a garantizar el cumplimiento de PCI DSS por parte del cliente, el uso de los productos y servicios de NetScaler no permite cumplir con el PCI DSS por sí solo. Los clientes son responsables de garantizar que cuentan con un programa de cumplimiento, procesos internos y controles adecuados para cumplir y mantener sus requisitos de cumplimiento de la PCI DSS.

Haga clic en Certificación de cumplimiento (AOC) de NetScaler Console Service PCI para descargar un informe sin conexión.

Programa de telemetría de NetScaler

September 2, 2024

El programa de telemetría de NetScaler es un programa de recopilación de datos obligatorio que permite cargar los datos de uso de funciones y licencias necesarios para que los clientes cumplan con sus obligaciones de licencia de mantenimiento y soporte. Citrix recopila datos de telemetría de licencias básicos y datos de telemetría de implementación y uso de funciones de NetScaler para sus intereses legítimos, incluido el cumplimiento de las licencias. Los datos de configuración y uso de funciones de la NetScaler Console también se recopilan para administrar, medir y mejorar los productos y servicios de Citrix.
El programa de telemetría de NetScaler se habilita automáticamente a partir de la compilación 14.1-28.x.

> **Notas:**
>
> - La carga de telemetría se realiza automáticamente cada 24 horas.
> - Para recopilar y almacenar las métricas de telemetría en sus instancias de NetScaler, se introdujo la siguiente configuración en sus instancias de NetScaler a través de NetScaler Console como parte del programa de telemetría de NetScaler lanzado el 18 de junio de 2024.

```
1 enable ns feature AppFlow
2 add analytics profile telemetry_metrics_profile -type timeseries -
```



```
outputMode prometheus -metrics ENABLED -serveMode Pull -
schemaFile "./telemetry_collect_ns_metrics_schema.json" -
metricsExportFrequency 300
```

- El archivo `/nsconfig/.telemetry.conf` se actualiza con el siguiente comando para la telemetría de Gateway. NetScaler Console comprueba este comando cada hora y, si falta, lo agrega. Este comando solo se envía a las instancias de NetScaler que tienen una configuración de servidor virtual VPN:

```
1 ns_telemetry_server,<Console IP>,5140
```

- Algunos parámetros de telemetría se recopilan mediante scripts que se envían desde NetScaler Console a las instancias de NetScaler. Estos scripts son de solo lectura y no cambian nada en NetScaler.
- La información recopilada mediante telemetría, como las direcciones de correo electrónico, los nombres de usuario y las direcciones IP, se seudonimiza de forma segura codificando la información en el origen mediante algoritmos hash unidireccionales. Como resultado, Citrix no puede acceder a estos valores ni leerlos. Estos datos de telemetría se usan únicamente con fines de comparación lógica de activos.

La siguiente tabla proporciona los detalles de los parámetros que se recopilan como parte del programa de telemetría de NetScaler:

Categorías	Descripción	Para qué lo utilizamos
Telemetría de uso e implementación de licencias y uso de NetScaler	Información sobre los derechos de licencia, la asignación, el uso y los datos de implementación de NetScaler de alto nivel y el uso de las funciones de NetScaler.	Cumplimiento de licencias y para administrar, medir y mejorar el servicio.
Telemetría de implementación y uso de funciones de NetScaler Console	Información sobre la implementación de Console y el uso de las funciones.	Gestionar, medir y mejorar el servicio.

Para obtener más información sobre la lista de parámetros de telemetría, consulte Gobernanza de datos.

Gobierno de datos

September 2, 2024

El servicio NetScaler Console forma parte de los servicios de Citrix Cloud y utiliza Citrix Cloud como plataforma para el registro, la incorporación, la autenticación, la administración y la concesión de licencias. Citrix recopila y almacena datos en Citrix Cloud como parte del servicio NetScaler Console. Este documento describe qué datos se recopilan y los métodos de recopilación, almacenamiento y transmisión de datos.

Para obtener más información sobre las prácticas de protección de datos de Citrix, consulte Descripción general de la protección de datos de Citrix Cloud Services.

Esta información es para oficiales de seguridad, oficiales de cumplimiento, auditores de información, administradores de infraestructura y operaciones de red y propietarios de líneas de negocio.

Programa de telemetría de NetScaler

El programa de telemetría de NetScaler está habilitado en el servicio NetScaler Console desde la compilación **14.1 a 28.x**. Con este programa, los datos requeridos se cargan automáticamente. Para obtener más información sobre la telemetría requerida recopilada, consulte Gobierno de datos para telemetría de NetScaler.

¿Cómo recopilamos, almacenamos y transmitimos datos?

El servicio NetScaler Console recopila datos de las instancias y los agentes gestionados. Estas instancias se implementan en las instalaciones del cliente y los datos se transmiten desde el agente (implementado en las instalaciones del cliente) de forma segura a través de un canal SSL cifrado mediante el protocolo TLS 1.2 a la nube.

Los datos se almacenan en una base de datos relacional con aislamiento de datos para múltiples usuarios en la capa de base de datos y como archivos en Elastic File System (EFS) alojados en la nube de AWS en los Estados Unidos, EMEA (Fráncfort) y APJ (Sídney), según el punto de presencia (POP) elegido por el cliente. Todos los POP se alojan en las regiones comerciales de AWS.

Las contraseñas, las cadenas comunitarias SNMP, los certificados SSL y la copia de seguridad de la configuración de NetScaler se cifran mediante una clave AES 256 única por arrendatario y se almacenan de forma segura en la base de datos. Para obtener más información sobre las regiones comerciales que utiliza Citrix Cloud y la presencia del servicio NetScaler Console en cada región, consulte Consideraciones geográficas.

Categorías de datos

Para las prácticas de manejo de datos, los datos se clasifican en:

- **Contenido del cliente**: Cualquier dato cargado en la cuenta del cliente para su almacenamiento o datos en el entorno informático del cliente al que NetScaler tenga acceso para prestar determinados servicios.
- **Registros**: Incluye registros de los Servicios, que incluyen, entre otros:
  - Datos e información sobre el rendimiento, la estabilidad, el uso, la seguridad y el soporte
  - Información técnica sobre dispositivos y sistemas

Contenido del cliente

El servicio de consola de NetScaler recopila información de varias fuentes:

- NetScaler
- NetScaler Gateway
- Web App Firewall (WAF) de NetScaler y administración de bots

El servicio de consola de NetScaler también recopila información sobre los detalles de la sesión y la actividad del administrador, además de la información mencionada en los registros.

Registros

Los registros se utilizan para facilitar el aprovisionamiento de actualizaciones de software, la autenticación de licencias, el soporte, el análisis y otros fines de conformidad con los acuerdos de usuario de Citrix.

Los registros de metadatos y telemetría recopilados incluyen:

- NetScaler Service Agent Hypervisor o plataforma de nube pública o tanto hipervisor de agente como plataforma de nube pública
- Ubicación geográfica del agente
- Versión de NetScaler
- Tipo de producto NetScaler
- Información sobre licencias (exprés y de suscripción)
- Uso del servicio en la nube por parte del administrador de NetScaler Console (lo que mejora la experiencia del usuario administrador).

Contenido y registros detallados de los clientes

- **Gestión de eventos (Inicio de sesión > Infraestructura > Eventos)**
  - Las trampas SNMP proporcionan alertas sobre el estado y el rendimiento de la red NetScaler.
  - Syslog de transacciones web que atraviesan la información de estado de la red de NetScaler.
  - Detalles del servidor de SMS, Slack y PagerDuty para activar las notificaciones de eventos por SMS/Slack.
  - Detalles del servidor SMTP para la configuración del correo electrónico.
  - Detalles del perfil de ServiceNow para crear tickets en ServiceNow.
- **Administración de certificados SSL (inicio de sesión > Infraestructura > Panel de control SSL)**
  - Certificados SSL, clave SSL, CSR de SSL, emisor de CA y algoritmos de firma de las aplicaciones web optimizados por la instancia de NetScaler.
- **Auditoría de configuración (inicio de sesión > Infraestructura > Configuración > Auditoría de configuración)**
  - Seguimiento de datos para la auditoría de configuración de NetScaler relacionados con las instancias de NetScaler, que incluyen la dirección IP del servidor de aplicaciones web y los detalles de la dirección IP de NetScaler.
- **Trabajos de configuración (Inicio de sesión > Infraestructura > Configuración > Trabajos de configuración)**
  - Detalles de configuración de NetScaler, dirección IP de la instancia y detalles de la dirección IP del servidor de aplicaciones web.
- **StyleBooks (Iniciar sesión > Aplicaciones > Configuración > StyleBooks)**
  - Las configuraciones de NetScaler se almacenan como una plantilla, que incluyen detalles de la dirección IP del servidor de aplicaciones web.
- **Administración de instancias (inicio de sesión > Infraestructura > Instancias)**
  - La dirección IP de las instancias de NetScaler, el tipo de instancia de NetScaler, la copia de seguridad de la configuración de NetScaler, los eventos críticos de NetScaler y la geolocalización del centro de datos donde se implementa la instancia de NetScaler (si está configurada).

- **Análisis de infraestructura (Inicio de sesión > Infraestructura > Análisis de infraestructura)**
  - Dirección IP de las instancias de NetScaler, tipo de instancia de NetScaler, eventos críticos de NetScaler, número de aplicaciones asociadas y geolocalización del centro de datos donde se implementa la instancia de NetScaler (si está configurada).
- **Aplicaciones (Inicio de sesión > Aplicaciones)**
  - Panel de control de la aplicación: URL de la aplicación, método de solicitud, código de respuesta, total de bytes, detalles del servidor de la aplicación web, direcciones IP del servidor virtual, detalles del cliente, navegador, sistema operativo cliente, protocolo SSL, nivel de cifrado SSL, intensidad de la clave SSL, dirección IP de la instancia de NetScaler, marca de tiempo de las solapas del servidor y tipo de contenido de respuesta.
- **Análisis (AppFlow/ Logstream)**
  - **Web Insights (Inicio de sesión > Aplicaciones)**: dirección IP del servidor virtual, clientes, URL, navegadores, sistemas operativos, métodos de solicitudes, estados de respuesta, dominios, dirección IP del servidor de aplicaciones web, certificados SSL, cifrado SSL negociado, fortaleza de la clave SSL, protocolo SSL y interfaz de fallas SSL.
  - **HDX Insight (Inicio de sesión > Gateway)**: detalles del usuario de ICA, detalles de la aplicación ICA, detalles del servidor VDA, detalles del escritorio en HDX Insight, detalles de geolocalización del cliente de la aplicación, detalles de la sesión activa de HDX, licencias de VPN para HDX, dirección IP de NetScaler del cliente, tipo de cliente y versión.
  - **Gateway Insight (Inicio de sesión > Gateway)**: detalles del usuario, detalles de la aplicación, navegadores, sistemas operativos, modos de sesión, licencias de Gateway, detalles del servidor AAA y directiva AAA configurada en Gateway.
  - **Infracciones de seguridad (inicio de sesión > Seguridad)**: IP del cliente, URL, infracciones de seguridad (WAF y Bot), geolocalización del ataque, fecha y hora del ataque, ID de transacción, WAF y estado de configuración de seguridad de NetScaler.
  - **Análisis de API (inicio de sesión > Seguridad > API Gateway)**: información sobre las instancias de la API, los puntos de conexión de la API, el ancho de banda total, la información sobre el rendimiento de la API, la solicitud total, el tiempo de respuesta y los errores. Posibilidad de profundizar en cada instancia de API para obtener visibilidad de los puntos finales individuales de la API y el rendimiento. Seguridad relacionada con el éxito de la autenticación, los errores, la limitación de velocidad, el cifrado SSL, la información del protocolo y los errores de SSL.
- **Asesoramiento de seguridad (inicio de sesión > Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad)**

- **Análisis**de versiones : este análisis necesita que NetScaler Console compare la versión de una instancia de NetScaler con las versiones y compilaciones en las que está disponible la solución. Esta comparación de versiones ayuda al asesoramiento de seguridad de NetScaler Console a identificar si el NetScaler es vulnerable al CVE. La lógica subyacente de este análisis es que si se corrige un CVE en la versión y la compilación xx.yy de NetScaler, todas las instancias de NetScaler de compilaciones inferiores a xx.yy se consideran vulnerables. El análisis de versiones se admite actualmente en el asesoramiento de seguridad.
- **Análisis de configuración :**este análisis necesita que NetScaler Console haga coincidir un patrón específico del escaneo CVE con el archivo de configuración de NetScaler. 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 hoy en día en el asesoramiento de seguridad.
- **Análisis**personalizado : este análisis necesita que el servicio NetScaler Console se conecte con la instancia de NetScaler gestionada, inserte un script en ella y ejecute el script. La salida del script ayuda a NetScaler Console a identificar si el 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.

Seguridad

La exposición sobre seguridad de Citrix Services describe en profundidad los controles de seguridad que se aplican a los servicios Citrix Cloud, incluidos el acceso y la autenticación, el desarrollo y el mantenimiento del sistema, la gestión de programas de seguridad, la gestión de activos, el cifrado, la gestión de operaciones, la seguridad de los recursos humanos, la seguridad física, la continuidad empresarial y la gestión de incidentes.

La seguridad de los productos Citrix Cloud se controla mediante directivas de cifrado y administración de claves. Consulte el documento técnico sobre los procesos de desarrollo de seguridad para obtener más información sobre cómo Citrix emplea la seguridad a lo largo del ciclo de desarrollo de sus productos.

Política de retención de datos para NetScaler Console Service

Los datos como las medidas estadísticas, los paneles, los informes, las alertas, los eventos y los registros de la consola de NetScaler y los detalles de inicio de sesión se conservan durante el período en que el cliente se suscribe al servicio. A continuación, la cuenta de usuario se convierte en una cuenta Express en la que el usuario solo puede administrar dos servidores virtuales.

La cuenta Express tiene una capacidad de 500 MB o 1 día de datos de análisis e informes, independientemente del límite que alcance primero la cuenta. Si no se utiliza una cuenta Express o el cliente no inicia sesión en la cuenta durante más de 30 días, la cuenta y todo el Contenido del cliente asociado se eliminarán automáticamente.

Para obtener más información sobre la retención y eliminación de datos de las cuentas de Citrix Cloud Services, consulte la descripción general de la protección de datos de Citrix Cloud Services.

> **Nota**
>
> Todos los datos de análisis de NetScaler Console se conservan durante un período máximo de 30 días.

Servicios de terceros

El servicio de consola NetScaler se aloja en los centros de datos de Amazon Web Service (AWS) de las regiones de Estados Unidos, EMEA (Fráncfort) y APJ (Sídney), según el punto de presencia (POP) elegido por el cliente.

En la actualidad, el servicio de consola de NetScaler utiliza servicios y API de varias tecnologías de terceros:

- Servicios utilizados para la funcionalidad del producto:
  - Google Maps, AWS EFS, AWS RDS, AWS Elastic Cache, AWS ALB, AWS Route 53, AWS EKS, AWS Secret Manager, AWS ECR repository y AWS MSK.
- Los servicios y herramientas de terceros que se utilizan para supervisar y operar NetScaler Console incluyen:
  - PagerDuty para rotación de guardia
  - Análisis de registros con Splunk
  - Fluentd para la agregación de registros
  - Slack para la comunicación y las alertas
  - AWS Cloudwatch, SQS
  - S3 como área de almacenamiento en AWS, para almacenar métricas y archivos principales

- Prometheus y Grafana para la monitorización (en implementación de Honeycomb)

Referencias

- Para obtener más información sobre cómo accedemos a los datos recopilados, consulte la exposición sobre seguridad de Citrix Services.
- Para obtener más información sobre cuánto tiempo se conservan los datos recopilados, consulte Descripción general de la protección de datos de Citrix Cloud Services.
- Descripción general de la seguridad técnica de Citrix Cloud.
- Medidas de seguridad de datos técnicas y organizativas de Citrix Cloud.

Introducción

January 26, 2024

Este documento explica cómo empezar a incorporar y configurar NetScaler Console por primera vez. Este documento está dirigido a los administradores de redes y aplicaciones que administran dispositivos de red Citrix (NetScaler, NetScaler Gateway, Citrix Secure Web Gateway, etc.). Siga los pasos de este documento independientemente del tipo de dispositivo que vaya a administrar con NetScaler Console.

Antes de comenzar la incorporación, asegúrese de revisar los requisitos del navegador, los requisitosde instalación del agentey los requisitos de puertos.

Paso 1: Registrarse en Citrix Cloud

Para empezar a usar NetScaler Console, primero debe crear una cuenta empresarial de Citrix Cloud o unirse a una ya existente que haya creado otra persona de su empresa. Para obtener instrucciones y procesos detallados sobre cómo proceder, consulte Registrarse en Citrix Cloud.

Paso 2: Administrar NetScaler Console con una cuenta Express

Después de iniciar sesión en Citrix Cloud, haga lo siguiente:

1. Vaya a la sección **Servicios disponibles**.
2. En el mosaico Administración de **entrega de aplicaciones** , haga clic en **Administrar** .

   El icono **Administración de entrega de aplicaciones** pasa a la sección **Mis servicios**.

3. Seleccione una región que se adapte a las necesidades de su empresa.

   > **Importante**No
   >
   > puede cambiar la región más tarde.

4. Seleccione los roles y los casos de uso que se apliquen a usted.

Puede cerrar la sesión en el explorador mientras la inicialización se completa en segundo plano, lo que puede tardar algún tiempo.

> **Nota**
>
> Citrix asigna una cuenta Express para administrar los recursos de NetScaler Console. Si su cuenta de NetScaler Console Express permanece inactiva durante 45 días, la cuenta se elimina. Para obtener más información, consulte Administrar NetScaler Console mediante una cuenta Express.

Cuando vuelva a iniciar sesión en su cuenta de Citrix Cloud, aparecerá la pantalla **GUI de NetScaler Console** . Haga clic en **Comenzar** para empezar a configurar el servicio por primera vez.

Paso 3: Seleccione un tipo de implementación de NetScaler

Seleccione una de las siguientes opciones de implementación que se adapte a sus requisitos empresariales:

- **Implementación**inteligente : esta opción es una configuración de entorno automatizada para implementar nuevas instancias de NetScaler. Instala automáticamente un agente para permitir la comunicación entre la consola de NetScaler y las instancias administradas.

  Esta opción es compatible con los entornos de AWS, Microsoft Azurey Google Cloud. En tres pasos, puede entregar una aplicación que esté presente en la nube mediante instancias de NetScaler.

- **Implementación personalizada**: esta opción es una implementación de varias etapas. Puede seleccionar cada opción de entorno e implementar o descubrir instancias de NetScaler.

Seleccione una implementación inteligente para AWS

Esta opción de implementación crea la siguiente infraestructura en AWS:

- Una pila de CloudFormation en AWS para crear la infraestructura necesaria que incluye subredes, grupos de seguridad, puertas de enlace NAT, etc.
- Un agente en la VPC para administrar las instancias de NetScaler.

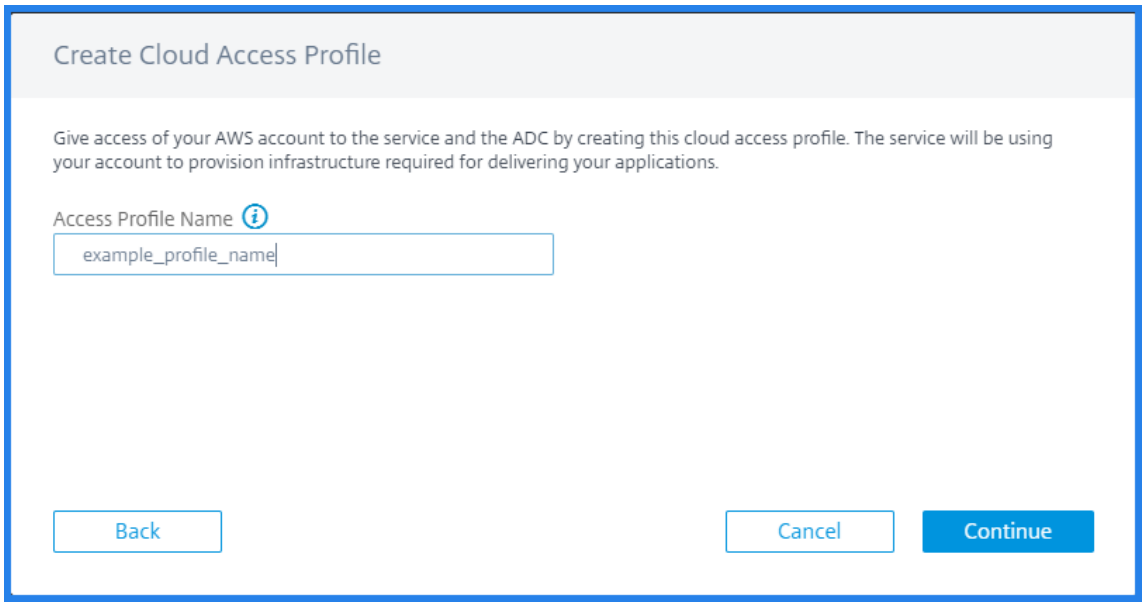
- Un grupo de NetScaler Autoscale. Puede personalizar este grupo más adelante en la página **Infraestructura > Nube pública > Grupos de Autoscale**.

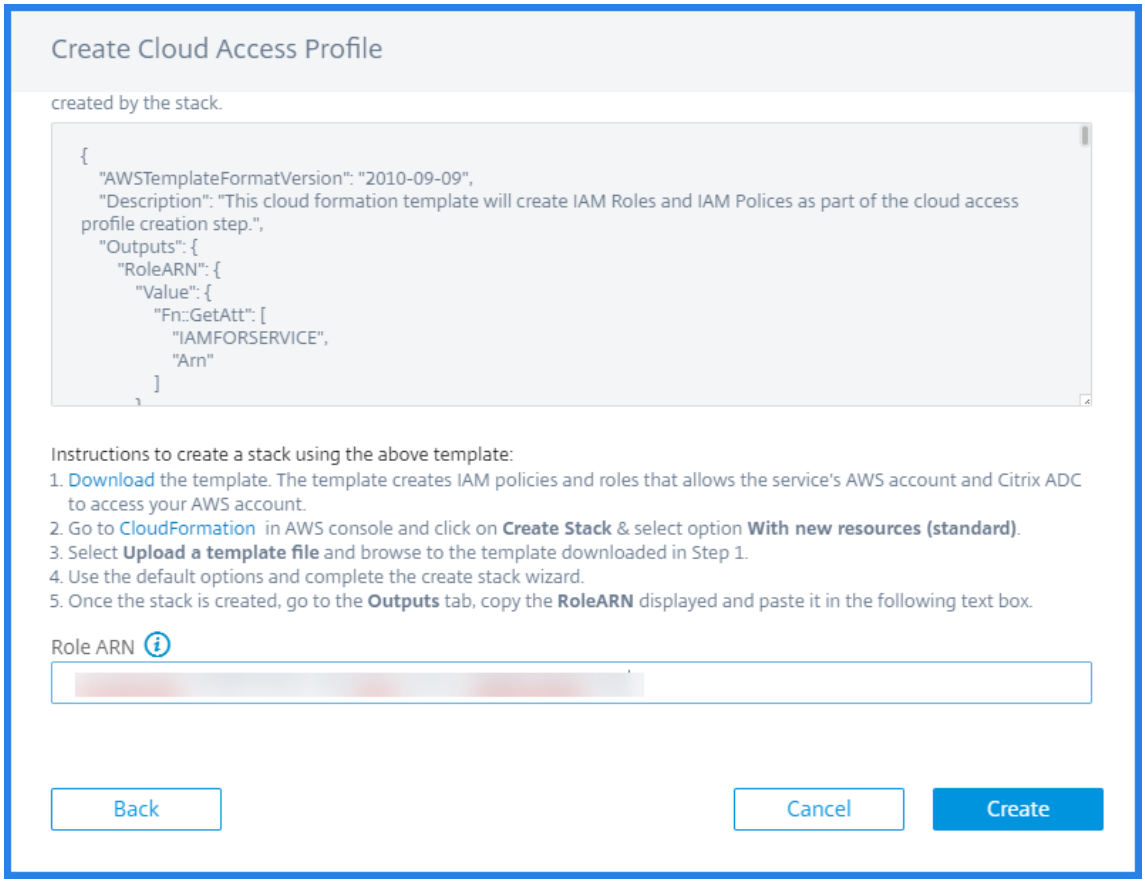
Antes de implementar instancias de NetScaler, asegúrese de lo siguiente:

1. Ya posee una cuenta de AWS.
2. Ha creado un usuario de IAM con todos los permisos administrativos.

Para implementar instancias de NetScaler, lleve a cabo los siguientes pasos:

1. En **Crear perfil de acceso a la nube**, seleccione **AWS** como entorno de implementación. Especifique el **nombre del perfil de acceso** y **el ARN de rol** para crear un perfil de acceso a la nube.





La consola de NetScaler usa el perfil de acceso a la nube para acceder a una cuenta de AWS.

2. Especifique los siguientes detalles para preparar el entorno de AWS:

   a) En la sección **Detalles del centro de datos** , seleccione la **región** de **AWS y la VPC** de AWS en las que quiera implementar instancias de NetScaler.

      AWS VPC muestra las VPC presentes en la **región de AWS**seleccionada.

   b) En los **detalles del grupo NetScaler AutoScale** , especifique lo siguiente para las instancias de AutoScaler en la nube de AWS:

      - **Nombre de grupo de Autoscale**: nombre para identificar un grupo de Autoscale.
      - **Zonas de disponibilidad**: seleccione las zonas en las que quiere crear los grupos de Autoscale.

        Puede seleccionar varias zonas de la lista.
      - **Tipo de implementación**: seleccione **la opción Evaluación** o **Producción**.

        Si desea evaluar la solución Autoscale de NetScaler Console antes de comprar la licencia de producción, seleccione la opción **Evaluación**.

> **Importante**
>
> - La opción de evaluación solo admite una zona de disponibilidad.
> - Con la opción de evaluación, solo puede seleccionar NetScaler VPX Express. Además, la solución Autoscale de NetScaler Console puede escalar hasta tres instancias de NetScaler.

- **Producto**NetScaler VPX: seleccione licencias para aprovisionar instancias de NetScaler .

  Suscríbase a la licencia seleccionada en el mercado de AWS y vuelva a esta página.

  Revise y seleccione el mensaje de consentimiento del usuario.

- **Tipo de instancia**: seleccione el tipo de instancia requerido.

c) Haga clic en **Siguiente**.

Tras la validación correcta, haga clic en **Crear** para implementar instancias de NetScaler en AWS y crear un grupo de Autoscale.

3. Tras la implementación correcta de NetScaler, haga clic en **Implementar aplicación**.

   En **Configurar aplicación**, especifique los detalles necesarios y haga clic en **Enviar**.

   Para obtener más información, consulte Configurar una aplicación para el grupo de Autoscale.

Seleccione la implementación inteligente para Microsoft Azure

Esta opción de implementación crea la siguiente infraestructura en Azure:

- Una plantilla de Azure Resource Manager (ARM) para crear la infraestructura necesaria que incluye subredes, grupos de seguridad, puertas de enlace NAT, etc.
- Un agente en la VPC para administrar las instancias de NetScaler.
- Un grupo de NetScaler Autoscale. Puede personalizar este grupo más adelante en la página **Infraestructura > Nube pública > Grupos de Autoscale**.

Antes de implementar instancias de NetScaler, asegúrese de lo siguiente:

- Tiene una cuenta de Microsoft Azure que admite el modelo de implementación de Azure Resource Manager.
- Tiene un grupo de recursos en Microsoft Azure.

Para obtener más información sobre cómo crear una cuenta y otras tareas, consulte la documentación de Microsoft Azure.

Para implementar instancias de NetScaler, lleve a cabo los siguientes pasos:

1. En **Crear perfil de acceso a la nube**, seleccione **Microsoft Azure** como entorno de implementación. Especifique los detalles del perfil de acceso a la nube de NetScaler Console y NetScaler.

   La consola NetScaler usa el perfil de acceso a la nube de NetScaler Console para acceder a una cuenta de Microsoft Azure. Además, se utiliza un perfil de acceso a la nube de NetScaler para aprovisionar instancias de NetScaler VPX.

2. Especifique los siguientes detalles para preparar el entorno de Azure:

   a) En **Detalles del entorno de la aplicación**, especifique un nombre para la implementación. Además, asegúrese de seleccionar el perfil de acceso a la nube correcto.

   b) En **Detalles del centro de datos** , especifique la región, el grupo de recursos y los detalles de la red virtual en los que desea implementar las instancias de NetScaler.

   c) En **Detalles del grupo NetScaler AutoScale** , especifique lo siguiente:

      - **Disponibilidad**: seleccione la zona o el conjunto de disponibilidad en el que quiere crear los grupos de Autoscale. Según el perfil de acceso a la nube que haya seleccionado, las zonas de disponibilidad aparecen en la lista.
      - **Tipo de implementación**: seleccione **la opción Evaluación** o **Producción**.

        Si desea evaluar la solución Autoscale de NetScaler Console antes de comprar la licencia de producción, seleccione la opción **Evaluación**.

        > **Importante**
        >
        > - La opción de evaluación solo admite una zona o conjunto de disponibilidad.
        > - Con la opción de evaluación, solo puede seleccionar NetScaler VPX Express. Además, la solución Autoscale de NetScaler Console puede escalar hasta tres instancias de NetScaler.

      - **Seleccione el producto**NetScaler VPX: seleccione licencias para aprovisionar instancias de NetScaler .

        Suscríbase a esta licencia de Azure Marketplace y regrese a la página.

        Revise y seleccione el mensaje de consentimiento del usuario.

      - **Seleccione el tamaño de la máquina** virtual: seleccione el tamaño de máquina virtual requerido.

   d) Haga clic en **Siguiente**.

      Tras la validación correcta, haga clic en **Crear** para implementar instancias de NetScaler en Microsoft Azure y crear un grupo de Autoscale.

3. Tras la implementación correcta de NetScaler, haga clic en **Implementar aplicación**.

   En **Configurar aplicación**, especifique los detalles necesarios y haga clic en **Enviar**.

   Para obtener más información, consulte Configurar una aplicación para el grupo de Autoscale.

Selecciona una implementación inteligente para Google Cloud

Esta opción de implementación crea la siguiente infraestructura en Google Cloud:

- Un administrador de implementación de Google Cloud para crear la infraestructura necesaria, que incluye redes de VPC, subredes, NAT de la nube, puertas de enlace de Cloud Router y reglas de firewall.
- Un agente en la VPC para administrar las instancias de NetScaler.
- Un grupo de NetScaler Autoscale. Puede personalizar este grupo más adelante en la página **Infraestructura > Nube pública > Grupos de Autoscale**.

Antes de implementar instancias de NetScaler, asegúrese de que ya dispone de una cuenta de Google Cloud. Para obtener más información sobre cómo crear una cuenta, consulta la documentación de Google Cloud.

Para implementar instancias de NetScaler, lleve a cabo los siguientes pasos:

1. En **Crear perfil de acceso a la nube**, selecciona **Google Cloud** como entorno de implementación.

   Especifique el **nombre del perfil de acceso a la nubey la clave de cuenta**

   La consola de NetScaler usa el perfil de acceso a la nube para acceder a una cuenta de Google Cloud.

2. Especifica los siguientes detalles para preparar el entorno de Google Cloud:

   a) En **Detalles del entorno de la aplicación**, especifique un nombre para la implementación. Además, asegúrese de seleccionar el perfil de acceso a la nube correcto.

   b) En **Detalles del centro de datos** , selecciona la **región de Google Cloud** en la que deseas implementar instancias de NetScaler.

   c) En los **detalles del grupo NetScaler AutoScale** , especifique lo siguiente para Autoescalar las instancias de NetScaler en Google Cloud:

      - **CIDR de subred de la red de VPC**: especifique una red de VPC creada para el tráfico de administración, cliente y servidor. Sin embargo, puede seleccionar la red existente como servidor.

- **Zonas**: seleccione las zonas en las que quiere crear los grupos de Autoscale.

  Puede seleccionar varias zonas de la lista.

- **Tipo de implementación**: seleccione **la opción Evaluación** o **Producción**.

  Si desea evaluar la solución Autoscale de NetScaler Console antes de comprar la licencia de producción, seleccione la opción **Evaluación**.

  > **Importante**
  >
  > - La opción de evaluación solo admite una zona de disponibilidad.
  > - Con la opción de evaluación, solo puede seleccionar NetScaler VPX Express. Además, la solución Autoscale de NetScaler Console puede escalar hasta tres instancias de NetScaler.

- **Producto**NetScaler VPX: seleccione licencias para aprovisionar instancias de NetScaler .
- **Tipo de máquina**: seleccione el tipo de instancia requerido.

d) Haga clic en **Siguiente**.

Tras la validación correcta, haga clic en **Crear** para implementar instancias de NetScaler en Google Cloud y crear un grupo de Autoscale.

3. Tras la implementación correcta de NetScaler, haga clic en **Implementar aplicación**.

   En **Configurar aplicación**, especifique los detalles necesarios y haga clic en **Enviar**.

   Para obtener más información, consulte Configurar una aplicación para el grupo de Autoscale.

Seleccionar implementación personalizada

Esta opción proporciona una implementación en varias etapas. Seleccione esta opción para descubrir instancias de NetScaler de varios entornos. Con esta opción, también puede implementar nuevas instancias especificando opciones de entorno personalizadas.

Realice los siguientes pasos para implementar o descubrir instancias de NetScaler:

1. Seleccione cualquiera de los siguientes entornos:

   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**
   - **Local**

2. Instale el agente para permitir la comunicación entre la consola de NetScaler y las instancias administradas en su centro de datos o en la nube.

   El paso **Seleccionar tipo de agente** varía las opciones de instalación del agente en función del entorno seleccionado.

   - **Local**: si selecciona **Local,**puede instalar un agente en los siguientes hipervisores:
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Servidor KVM Linux
   - **Nubes públicas**: si selecciona **AWS**, **Microsoft Azure**o **Google Cloud Platform**, puede instalar un agente de forma externa en la nube seleccionada.

     A continuación se muestra una imagen de ejemplo para el entorno de AWS.
   - **Como microservicio** - Para implementar un agente como una aplicación Kubernetes.
   - **Agente integrado**: para descubrir los agentes integrados disponibles con NetScaler versión 12.0 o posterior.

3. Haga clic en **Siguiente**.

   Los pasos para instalar un agente varían según cada opción. Los siguientes vínculos le guiarán a los pasos específicos para instalar un agente:

   - Hipervisor
   - Agente externo
   - Como microservicio
   - Agente integrado

Instalar un agente en un Hypervisor

Realice los siguientes pasos para configurar un agente en un hipervisor:

1. Seleccione el hipervisor y haga clic en **Descargar imagen** para descargar la imagen del agente en su sistema local.

   Se generan una URL de servicio y un código de activación y se muestran en la GUI.

2. Copie la URL del servicio y un código de activación.
3. Especifique la URL del servicio copiada y el código de activación al instalar el agente en el hipervisor.

El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio. Para obtener instrucciones detalladas sobre la instalación de un agente en el hipervisor local, consulte Instalar un agente local.

4. Después de instalar correctamente el agente, vuelva a la página **Configurar agente** y haga clic en **Registrar Agente**.

Paso siguiente: Agregar instancias.

> **Nota**
>
> Si no desea añadir agentes durante la configuración inicial, haga clic en **Omitir** para comprobar las funciones que ofrece NetScaler Console. Puede agregar los agentes y las instancias más adelante. Para agregar agentes más adelante, vaya a **Configuración > Configurar agentes**. Para obtener instrucciones sobre cómo agregar instancias más adelante, consulte Agregar instancias.

Instalar un agente en una nube pública

No es necesario descargar la imagen del agente desde la página **Configurar agente**. La imagen del agente está disponible en el mercado en la nube correspondiente.

1. Copie y guarde la URL del servicio y el código de activación que se utilizarán durante la instalación del agente.

   Si quiere un nuevo código de activación, haga clic en **Crear nuevo código de activación**y, a continuación, copie y guarde el código que se va a utilizar durante la instalación del agente.

   - Para obtener instrucciones detalladas sobre la instalación de un agente en la nube de Microsoft Azure, consulte Instalar un agente en la nube de Microsoft Azure .
   - Para obtener instrucciones detalladas sobre la instalación de un agente en AWS, consulte Instalar un agente en AWS .
   - Para obtener instrucciones detalladas sobre cómo instalar un agente en Google Cloud, consulta Instalar un agente en GCP .

2. Después de instalar correctamente el agente, vuelva a la página **Configurar agente** y haga clic en **Registrar Agente**.

Paso siguiente: Agregar instancias.

Instalar un agente como microservicio

Puede implementar un agente como microservicio en el clúster de Kubernetes para ver el **gráfico de servicios** en NetScaler Console.

Para obtener más información sobre cómo empezar a usar el gráfico de servicio, consulte Configuración del gráfico de servicio.

1. 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**del agente : especifique una contraseña para que CPX la utilice para integrar CPX en la consola de NetScaler a través del agente.
    c) **Confirmar contraseña**: Especifique la misma contraseña para la confirmación.
    d) Haga clic en **Submit**.
2. Después de hacer clic en **Enviar**, puede descargar el gráfico YAML o Helm.
3. Haga clic en **Cerrar**.

    Para obtener más información, consulte Instalar un agente en un clúster de Kubernetes .

Usa el agente integrado

Las instancias de NetScaler de su entorno incluyen un agente integrado. Puede iniciar el agente integrado y usarlo para establecer la comunicación entre la instancia y NetScaler Console.

1. Copie la **URL del servicio** generada y el **código de activación**. Guárdelos para usarlos al iniciar el agente integrado en su instancia de NetScaler.

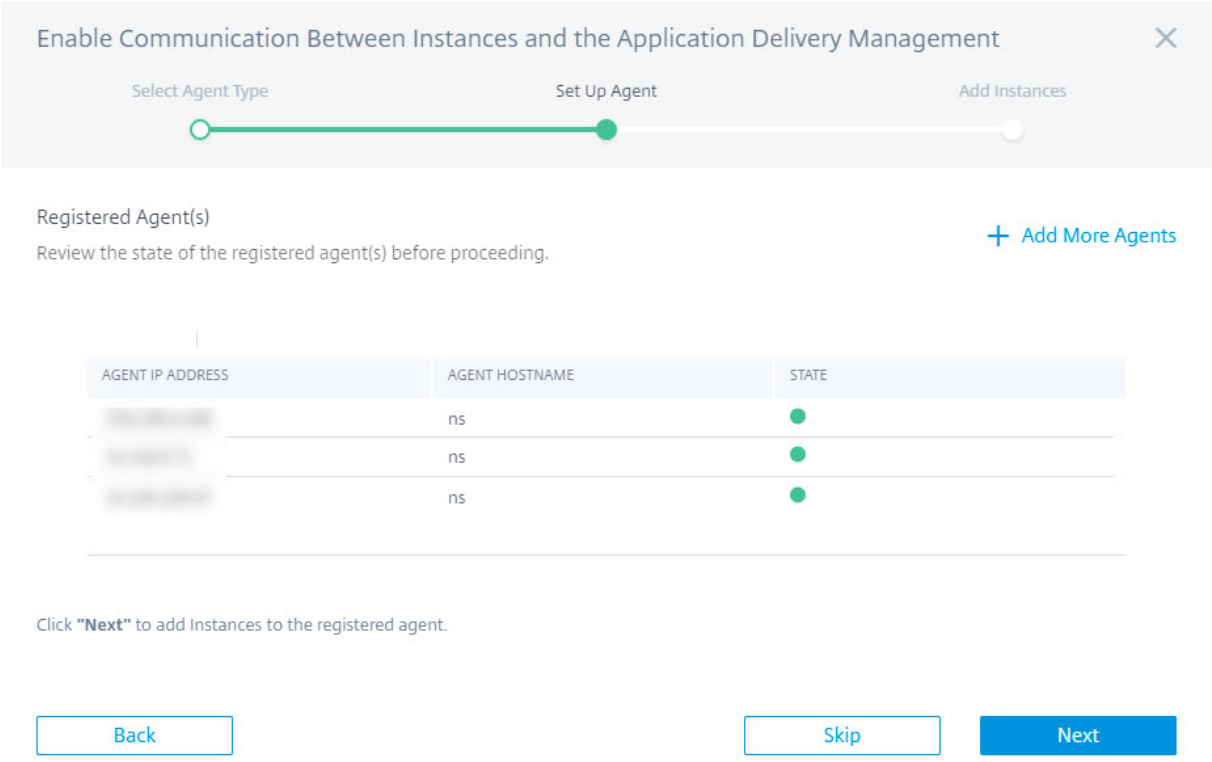
    Para obtener instrucciones detalladas sobre cómo iniciar el agente integrado en su instancia de NetScaler, consulte Iniciar el agente integrado en la instancia de NetScaler.
2. Una vez iniciado el agente integrado, vuelva a la página **Configurar agente** y haga clic en **Registrar instancia**.

Paso siguiente: Agregar instancias.

Agregar instancias

Las instancias son dispositivos de red o dispositivos virtuales que desea descubrir, administrar y monitorear desde NetScaler Console. Para administrar y supervisar estas instancias, debe agregarlas al servicio.

Después de la instalación y el registro correctos del agente, los agentes se muestran en la página **Configurar agente**. Cuando el estado del agente esté en el estado UP indicado por un punto verde junto a él, haga clic en **Siguiente** para comenzar a agregar instancias al servicio.



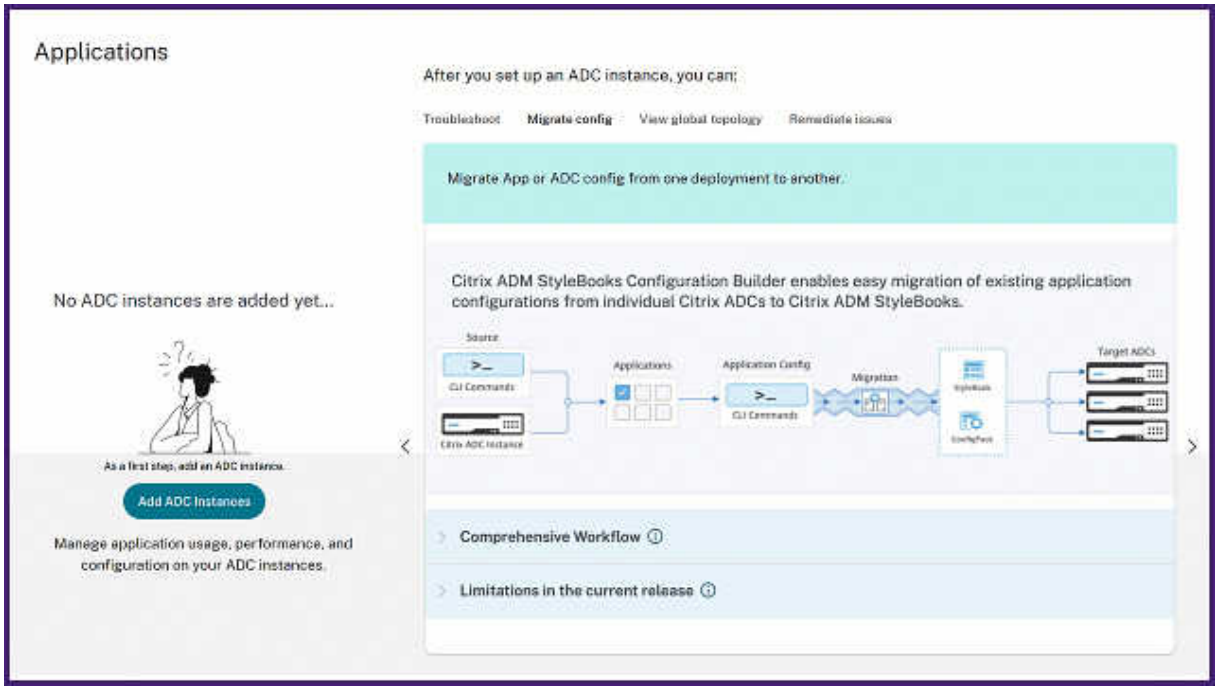
1. En la página **Agregar instancias** , consulte las instancias de NetScaler que están conectadas al agente registrado. Asegúrese de que la instancia esté en estado **Activo** y haga clic en **Siguiente**.
2. Haga clic en **Listo** para completar la configuración inicial y comenzar a administrar la implementación.

> **Nota**
>
> Si no quiere agregar instancias durante la configuración inicial, puede **hacer clic en Listo** para completar la configuración y agregar las instancias más adelante. Para obtener instrucciones sobre cómo agregar instancias más adelante a NetScaler Console, consulte Agregar instancias.

Instancias de NetScaler integradas mediante el panel de interfaz gráfica de usuario de NetScaler Console

Si omitió la incorporación de las instancias de NetScaler en el **flujo de**trabajo de introducción al configurar NetScaler Console por primera vez , puede incorporar las instancias desde el panel de interfaz gráfica de usuario de NetScaler Console. Si las instancias de NetScaler aún no se han agregado, la GUI le solicita que las agregue.

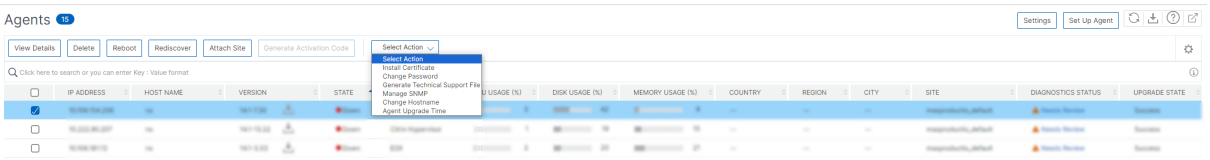
Al hacer clic en cualquier módulo de la barra de navegación de la izquierda, en el lado derecho aparece una vista previa tabular de las funciones y beneficios de ese módulo. Estas funciones y beneficios le ayudan a gestionar mejor las instancias de NetScaler mediante NetScaler Console.



Haga clic en **Agregar instancias de NetScaler** para incorporar las instancias. Se **reinicia** el flujo de trabajo de introducción. Siga los pasos del paso 3: seleccione un tipo de implementación de NetScaler en adelante, tal como se indica en este documento, para incorporar las instancias.
Si las instancias de NetScaler ya están incorporadas, después de iniciar sesión en NetScaler Console, solo verá la página de inicio de NetScaler Console con la barra de navegación a la izquierda.

Acciones del agente

Tras configurar la consola de NetScaler, puede aplicar varias acciones a un agente. Vaya a **Infraestructura > Instancias > Agentes**.



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

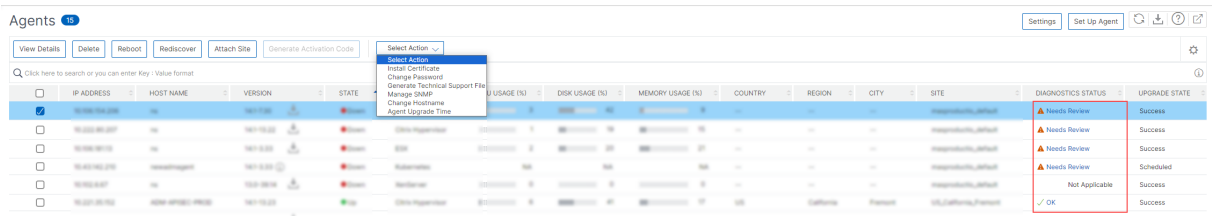
- **Instale un certificado nuevo**: si necesita un certificado de agente diferente para cumplir con sus requisitos de seguridad, puede agregar uno.
- **Cambie la contraseña del agente**: para garantizar la seguridad de su infraestructura, cambie la contraseña predeterminada de un agente.
- **Generar un archivo**de soporte técnico : genera un archivo de soporte técnico para un agente seleccionado. Puede descargar este archivo y enviarlo al soporte técnico de Citrix para su investigación y solución de problemas.

Vea los diagnósticos de los agentes y reciba alertas para la verificación de terminales

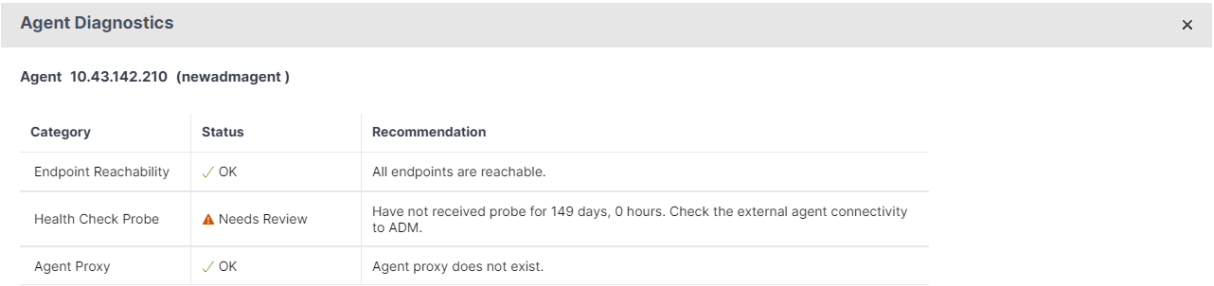
NetScaler Console realiza una comprobación de diagnóstico periódica (cada una hora) del agente y proporciona la siguiente información:

- **Accesibilidad de** los puntos finales: comprueba si se puede acceder a todos los puntos finales. El agente usa varios puntos finales para la comunicación entre NetScaler Console y las instancias de NetScaler. Para obtener más información, consulte Requisitos de software.
- **Sonda de control de estado**: proporciona la marca de tiempo del último chequeo de estado.
- **Proxy del agente**: comprueba si el proxy del agente existe.

Si el estado de accesibilidad del punto final del agente cambia (de **Aceptar** a **Necesita revisión**), el superadministrador recibe una notificación por correo electrónico con los detalles del problema. Vaya a **Infraestructura > Instancias > Agentes** para ver la opción **Estado de diagnóstico** recién agregada que proporciona el estado **Necesita revisión** o **Aceptar**.



Haga clic para ver la información de diagnóstico de un agente.

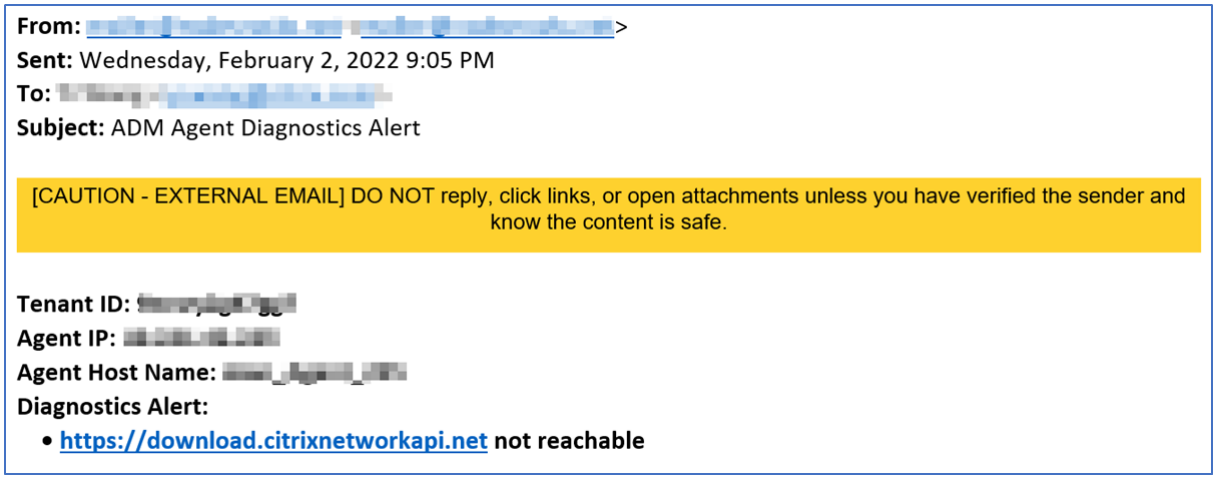


- **Categoría**. Proporciona la categoría del problema.
- **Status**. Indica el estado del problema, como **Necesita revisión** o **Aceptar**.
- **Recomendación**. Proporciona la recomendación necesaria para solucionar el problema.

Después de solucionar el problema y el estado de accesibilidad del punto final cambia de **Needs Review** a **OK**, el superadministrador recibe una notificación por correo electrónico en la que se indica que el problema se ha resuelto.

Notificación por correo

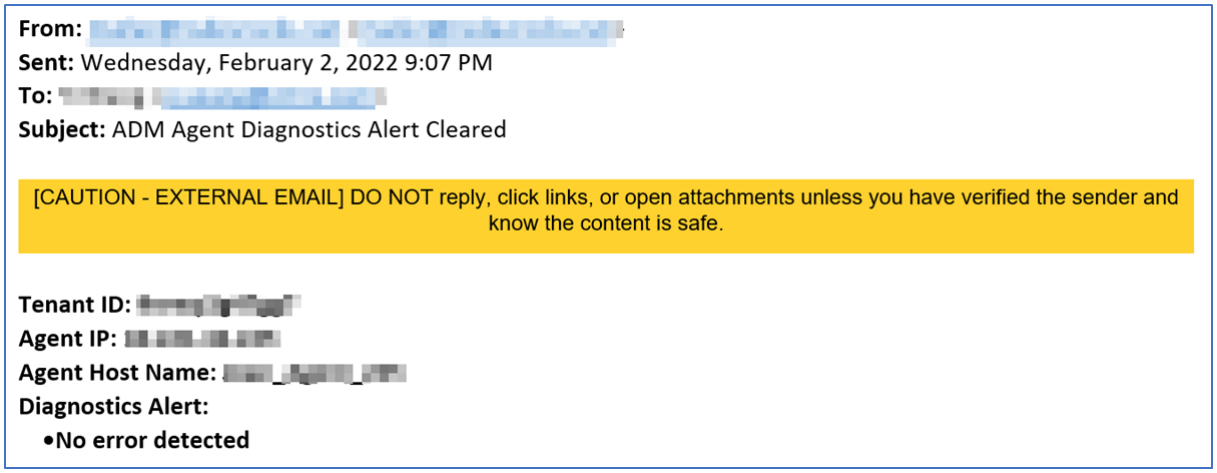
El siguiente ejemplo es una notificación por correo electrónico después de que el estado de accesibilidad del punto final haya cambiado de **OK** a **Needs Review**:


From: >
Sent: Wednesday, February 2, 2022 9:05 PM
To:
Subject: ADM Agent Diagnostics Alert

[CAUTION - EXTERNAL EMAIL] DO NOT reply, click links, or open attachments unless you have verified the sender and know the content is safe.

Tenant ID:
Agent IP:
Agent Host Name:
Diagnostics Alert:
- **https://download.citrixnetworkapi.net not reachable**

El siguiente ejemplo es una notificación por correo electrónico después de que el estado de accesibilidad del punto final haya cambiado de **Needs Review** a **OK**:


From:
Sent: Wednesday, February 2, 2022 9:07 PM
To:
Subject: ADM Agent Diagnostics Alert Cleared

[CAUTION - EXTERNAL EMAIL] DO NOT reply, click links, or open attachments unless you have verified the sender and know the content is safe.

Tenant ID:
Agent IP:
Agent Host Name:
Diagnostics Alert:
- **No error detected**

Configurar el agente integrado para gestionar las instancias

January 26, 2024

Hay un agente integrado disponible en las instancias de NetScaler MPX, VPX, Gateway que ejecutan la versión 12.1.48.13 y versiones posteriores, y en las instancias de NetScaler SDX que ejecutan la versión 13.0 61.x y posterior y 12.1 58.x y posteriores. Puede iniciar este agente en la instancia de NetScaler en lugar de instalar un agente dedicado en su centro de datos o nube pública. El agente integrado permite la comunicación entre la instancia y NetScaler Console.

> **Nota:**
>
> El agente integrado solo está disponible en los siguientes tipos de instancias de NetScaler:
>
> - NetScaler MPX
> - NetScaler VPX
> - NetScaler SDX
> - NetScaler Gateway

El agente integrado es ideal para las implementaciones más pequeñas de NetScaler independientes o de pares HA. Si tiene varias instancias de NetScaler, utilice un agente dedicado para las implementaciones. Este agente garantiza que tenga mejores capacidades de agregación de datos que el agente integrado. Para obtener más información, consulte Instalación de un agente local.

NetScaler Console admite la administración y la supervisión de las instancias de NetScaler mediante agentes integrados. Sin embargo, el agente integrado no admite las siguientes funciones:

- Panel de aplicaciones
- Información web
- SSL Insight
- HDX Insight
- Información sobre Gateway
- Security Insight
- Analítica avanzada
- Licencias agrupadas

Puede realizar la transición de un agente integrado a otro externo. Para obtener más información, consulte Transición de un agente integrado a un agente externo.

Requisitos previos

Antes de configurar un agente integrado en la instancia de NetScaler, asegúrese de lo siguiente:

- La instancia de NetScaler (MPX, VPX o Gateway) se ejecuta en la versión `12.1.48.13` o posterior. La instancia de SDX está ejecutando la versión `13.0.61.x` y posterior.
- Se agrega un servidor de nombres DNS a la instancia de NetScaler.

  Para obtener más información, consulte Agregar un servidor de nombres.
- Tener una cuenta de Citrix Cloud. Para obtener más información, consulte Inscribirse en Citrix Cloud.

> **Nota:**
>
> Para obtener toda la información relacionada con los puertos y otros requisitos del sistema, consulte Requisitos del sistema.

Configurar el agente integrado

Realice las siguientes tareas para configurar el agente integrado de NetScaler:

1. Seleccione la opción Agente integrado tal y como se indica en la sección Introducción.
2. Copie la **URL del servicio** y el **código de activación**.

   El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio. Omita el paso 7 si es cliente de MPX o Gateway.
3. Inicie el agente integrado mediante un cliente SSH. Los usuarios de la puerta de enlace deben omitir este paso.

   a) Inicie sesión en su instancia de NetScaler. Para obtener más información, consulte Acceder a un NetScaler.

   b) Desplácese hasta el `/var/mastools/scripts` directorio y escriba el siguiente comando:

   En la instancia de SDX

	Registro con el perfil de NetScaler	Registro sin perfil de NetScaler
Requisito previo	Antes de registrarse, cree un perfil de NetScaler. **Para obtener más información, consulte Cómo crear un perfil de NetScaler**	.
Ejecute este comando	**Credencial de./mastools_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile usuario./mastools_init.sh <user_name> <service-url> <activation-code> -sdx**	**Entrar.**`nsroot<device_profile_name>` Como alternativa, puede usar un nombre de usuario que tenga los mismos privilegios de acceso que nsroot.
Entrar `nsroot`. `<user_name>` Como alternativa, puede usar un nombre de usuario que tenga los mismos privilegios de acceso que nsroot.

   > **Nota:**
   >
   > NetScaler Console descubre todas las instancias VPX que se ejecutan en ese SDX y no es necesario registrar las instancias VPX de forma individual.

En las instancias VPX que no se ejecutan en un dispositivo SDX y en las instancias MPX y Gateway:

Si la versión de la imagen de NetScaler es inferior a 13.0 61.x o 12.1 57.x, debe comprobar la `mastools`versión escribiendo el comando `cat /var/mastools/version.txt`. Si la salida es `0.0-0.0`, es la primera vez.

Escriba uno de los siguientes comandos en función de la versión del software.

> **Nota:**
>
> Antes de registrarse con un perfil de NetScaler, debe crear el perfil. Para obtener más información, consulte Cómo crear un perfil de NetScaler.

Versión de imagen de NetScaler	¿Es mastools_version `0.0-0.0`?	Comando para el registro con perfil	Comando para el registro sin perfil
Menos de 13,0 61.xx y 12.1 57,xx	Sí	`./mastools_init.sh <device_profile_name> <service_url> "MAS;<activation_code>"-profile`	`./mastools_init.sh <user_name><pwd> <service_url> "MAS;<activation_code>"`
Menos de 13,0 61.xx y 12.1 57,xx	No	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name><pwd> <service_url> <activation_code>`
Más de 13,0 61.x y 12.1 57.xx	No aplicable	`./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name><pwd> <service_url> <activation_code>`

> **Nota:**
>
> - En <device_profile_name> o <user_name>, introduzca nsroot. Como alternativa, puede usar un nombre de usuario que tenga los mismos privilegios de acceso que nsroot.
> - En un par HA, complete el registro en el nodo principal. Si ejecuta los comandos de registro en el nodo secundario, aparecerá el siguiente mensaje: **Ejecute el comando de registro en el nodo principal**.

4. Vuelva a la página de la consola de NetScaler y haga clic en **Registrar instancia**.
5. En **Agregar instancias**, vea la instancia en la que inició el agente integrado. Asegúrese de que la instancia esté en estado **Activo** y haga clic en **Siguiente**.
6. Haga clic en **Listo**.

Tras configurar correctamente el agente integrado, puede acceder a las funciones de la consola de NetScaler, como:

- **Servidor virtual y análisis**: aplique licencias a su servidor virtual para administrar las instancias de NetScaler. Para obtener más información, consulte Administrar suscripciones.
- **Panel de aplicaciones**: para ver todas las aplicaciones de forma holística. Para obtener más información, consulte Administración de aplicaciones y panel de control.
- **Análisis de infraestructura**: esta función le ayuda a visualizar los factores que provocaron o podrían provocar un problema en las instancias. Para obtener más información, consulte Análisis de infraestructura.

> Nota: También
>
> puede configurar el agente integrado en la página **Infraestructura > Instancias > Agentes > Generar código de activación**. Copie y pegue la URL y el código de activación en una instancia de NetScaler y descubra esa instancia.

Una vez iniciado el agente integrado, vaya a **Infraestructura > Instancias > NetScaler**. Esta página muestra los detalles sobre la instancia administrada detectada mediante el agente integrado.

Solución de problemas

Puede comprobar los registros si el registro falla o si el registro se realiza correctamente, pero el agente integrado no aparece en la GUI de NetScaler Console.

- Si el registro falla, compruebe los registros en /var/mastools/logs/mastools_reg.py.log

- Si el registro se realiza correctamente, pero el agente integrado no aparece en la GUI de NetScaler Console, compruebe:
  - **MastOols_Upgrade** registra `/var/mastools/logs/mastools_upgrade.log`
  - **Inicia sesión binaria** `/var/log/mastoolsd.log`.

Instalación local de un agente de NetScaler

January 26, 2024

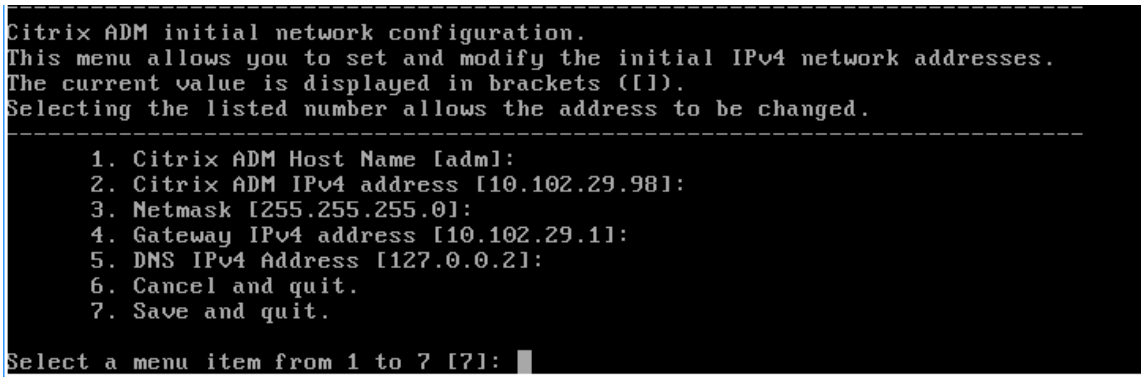
El agente actúa como intermediario entre la consola de NetScaler y las instancias descubiertas en el centro de datos.

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. Para obtener más información, consulte Requisitos de instalación del agente y Agente ligero para licencias agrupadas.

> **Nota**
>
> Para obtener toda la información relacionada con los puertos y otros requisitos, consulte Puertos compatibles.

Para instalar el agente de NetScaler:

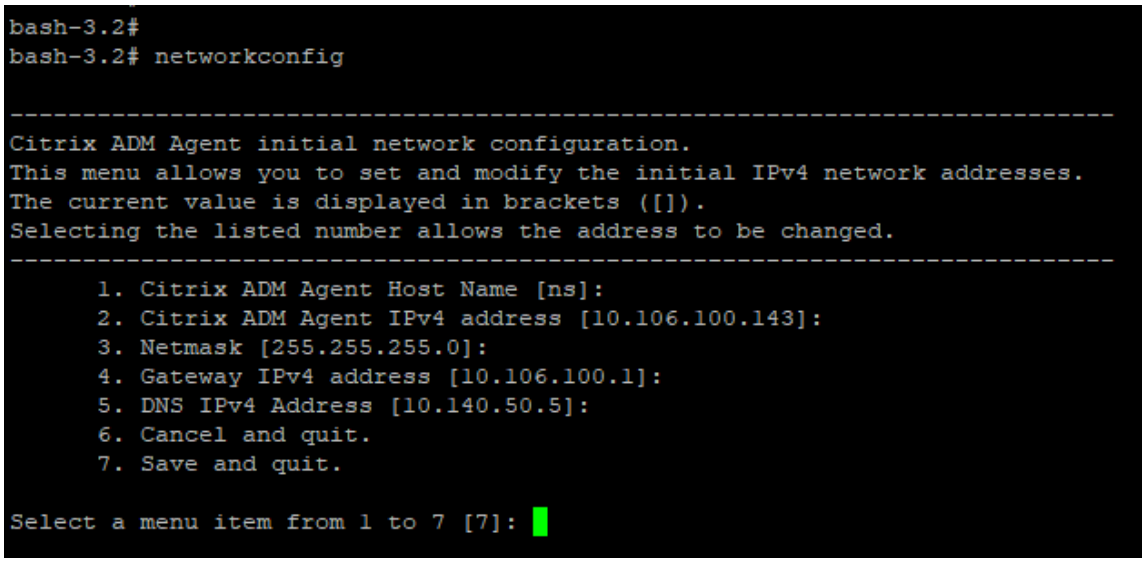
1. Descargue la imagen del agente como se indica en Introducción.
2. Importe el archivo de imagen del agente a su hipervisor.
3. En la ficha **Consola**, configure las opciones de configuración de red iniciales como se muestra en el siguiente ejemplo:



> **Nota**
>
> Asegúrese de configurar el DNS para permitir el acceso a Internet a su agente de NetScaler.

4. Después de completar la configuración de red inicial, guarde los valores de configuración. Cuando se le solicite, inicie sesión con las credenciales predeterminadas (`nsrecover`/`nsroot`).

   Si desea cambiar la configuración de red configurada en el agente, escriba el comando `networkconfig` y siga las instrucciones de la CLI.

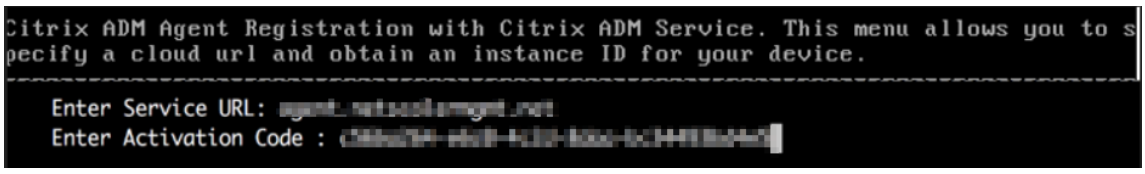


5. Si no aparece ninguna solicitud para introducir la URL del servicio, vaya a /mps en el agente de NetScaler y, a continuación, ejecute cualquiera de los siguientes scripts:

```
deployment_type.py
```

```
register_agent_cloud.py
```

6. Introduzca la **URL del servicio** y el **código de activación** que guardó al descargar la imagen del agente. El agente usa la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.

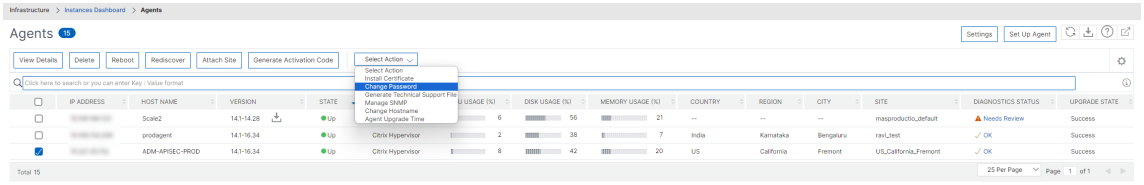


7. Una vez que el registro del agente se realiza correctamente, el agente se reinicia para completar el proceso de instalación.

Una vez reiniciado el agente, acceda a la GUI de NetScaler Console y vaya a **Infraestructura > Instancias > Agentes** para comprobar el estado del agente. Una vez configurado el agente, debe cambiar la contraseña.

1. Vaya a **Infraestructura > Instancias > Agentes**

2. Seleccione el agente y, en la lista **Seleccionar acción**, haga clic en **Cambiar contraseña**.



3. Introduzca la contraseña actual (`nsroot`), especifique una contraseña nueva y pulse **Aceptar** para cambiarla.

   La contraseña debe:

   - Tener al menos seis caracteres de longitud
   - Tener al menos un carácter especial
   - Tener al menos un carácter en mayúscula
   - Tener al menos un carácter en minúscula
   - Tener al menos un carácter numérico

Instalación de un agente de NetScaler en la nube de Microsoft Azure

January 26, 2024

El agente actúa como intermediario entre la consola de NetScaler y las instancias administradas en el centro de datos empresarial o en la nube.

Para instalar el agente de NetScaler en la nube de Microsoft Azure, debe crear una instancia del agente en la red virtual. Obtenga la imagen del agente de NetScaler en Azure Marketplace y, a continuación, utilice el portal Azure Resource Manager para crear el agente.

Antes de empezar a crear la instancia del agente de NetScaler, asegúrese de haber creado una red virtual con las subredes necesarias en las que reside la instancia. Puede crear redes virtuales durante el Provisioning de VM, pero sin la flexibilidad necesaria para crear subredes diferentes. Para obtener información sobre la creación de redes virtuales, consulte http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network.

Configure el servidor DNS y la conectividad VPN que permitan a una máquina virtual acceder a los recursos de Internet.

Requisitos previos

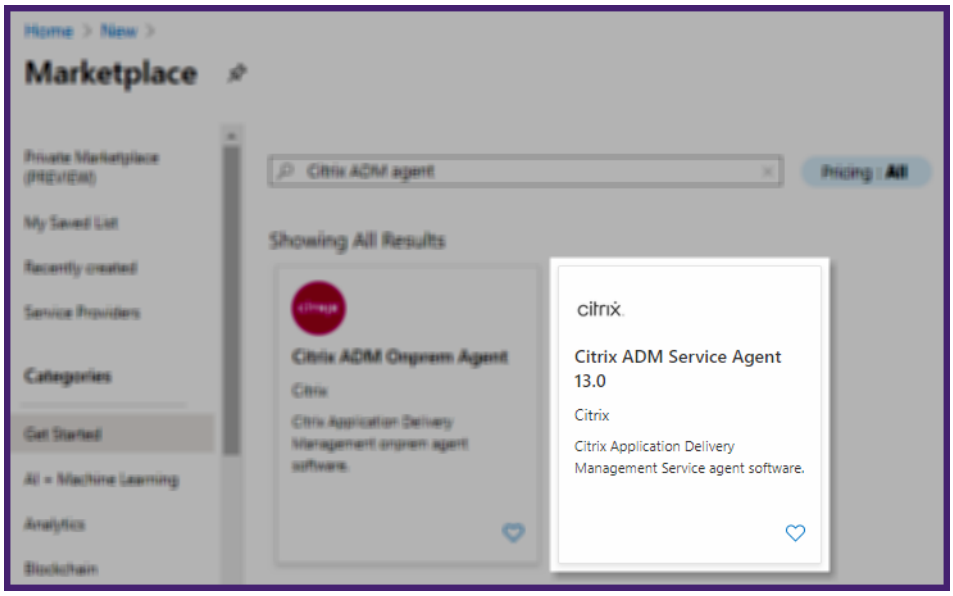
Asegúrese de que tiene lo siguiente:

- Una cuenta de usuario de Microsoft Azure
- Acceso al Administrador de recursos de Microsoft Azure

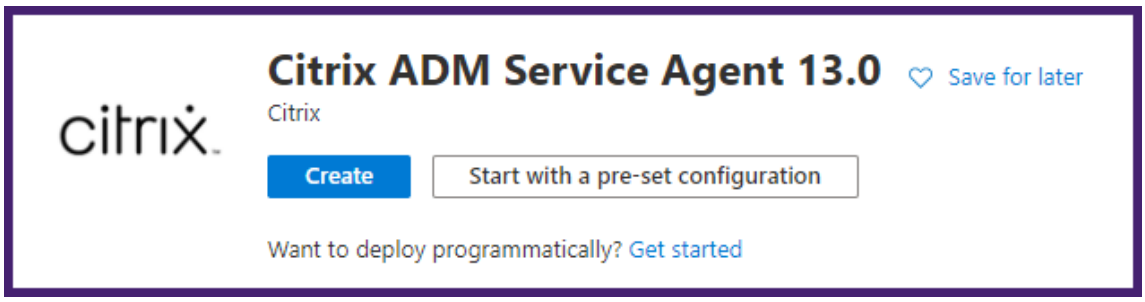
> **Nota**
>
> - Se recomienda crear un grupo de recursos, un grupo de seguridad de red, una red virtual y otras entidades antes de aprovisionar la máquina virtual del agente de NetScaler, de modo que la información de la red esté disponible durante el aprovisionamiento.
> - Para que el agente de NetScaler se comunique con NetScaler Console y las instancias de NetScaler, asegúrese de que los puertos recomendados estén abiertos. Para obtener información completa sobre los requisitos de puerto para el agente de NetScaler, consulte Puertos.

Para instalar el agente de NetScaler en Microsoft Azure Cloud:

1. Inicie sesión en el portal de Azure (https://portal.azure.com) con sus credenciales de Microsoft Azure.
2. Haga clic en **+Crear un recurso**.
3. Escriba `NetScaler agent`en la barra de búsqueda y seleccione el **agente NetScaler** .



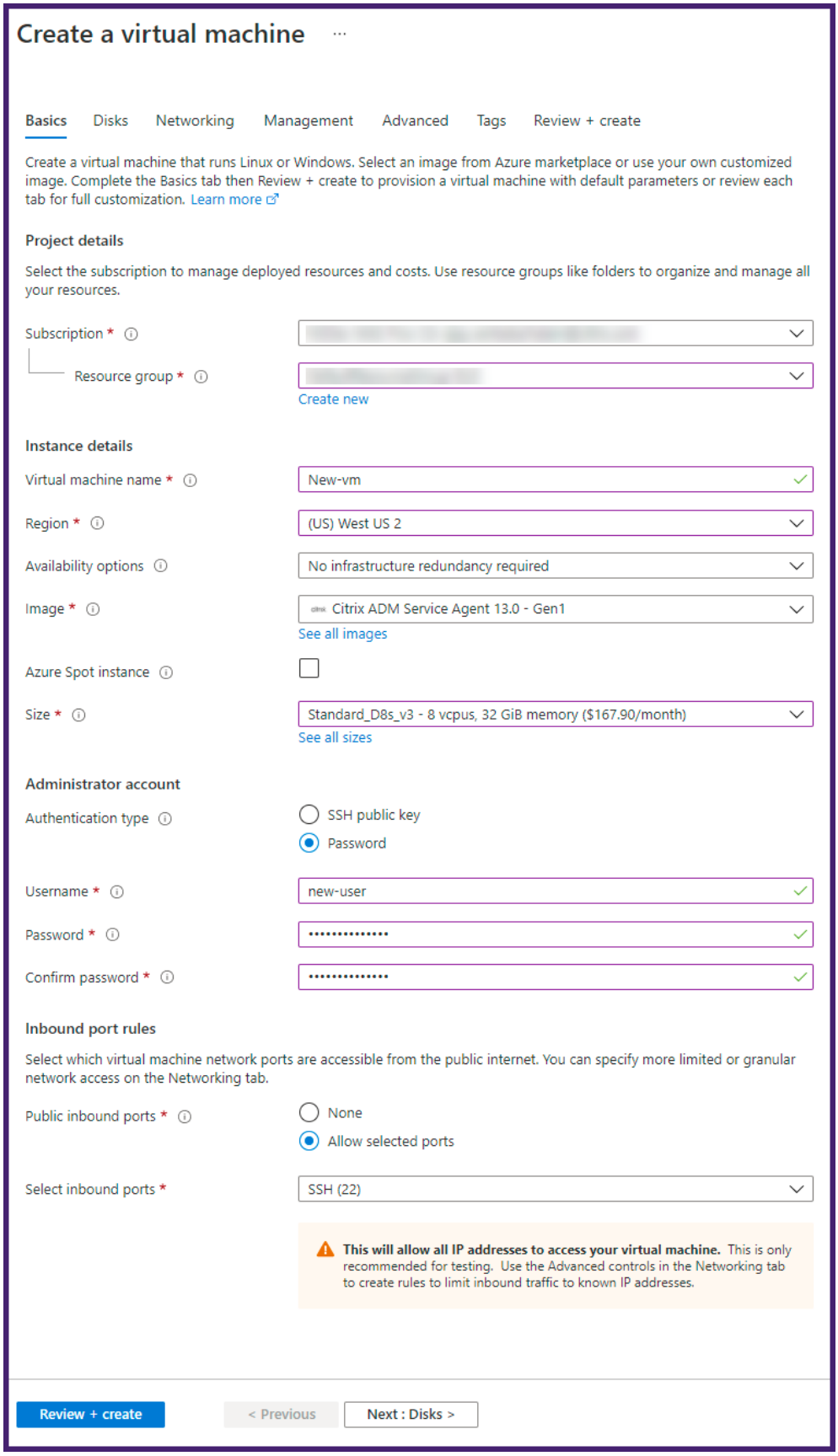
4. Haga clic en **Crear**.



5. En el panel **Crear máquina virtual**, especifique los valores necesarios en cada sección para crear una máquina virtual.

   Conceptos básicos:

   En esta ficha, especifique **detalles del proyecto**, **detalles de instancia**y **cuenta de administrador**.



- **Grupo**de recursos : seleccione el grupo de recursos que ha creado en la lista desplegable.

  > **Nota**
  >
  > Puede crear un grupo de recursos en este momento, pero le recomendamos que cree un grupo de recursos a partir de **los grupos de recursos** de Azure Resource Manager y, a continuación, seleccione el grupo en la lista desplegable.

- **Nombre**de la máquina virtual : especifique un nombre para la instancia del agente de NetScaler.
- **Región**: seleccione la región en la que quiere desplegar un agente.
- **Opciones de disponibilidad**: seleccione el conjunto de disponibilidad de la lista.
- **Imagen**: este campo muestra la imagen del agente ya seleccionada. Si quiere cambiar a una imagen de agente diferente, seleccione la imagen requerida en la lista.
- **Tamaño**: especifique el tipo y el tamaño del disco virtual para implementar el agente de NetScaler.

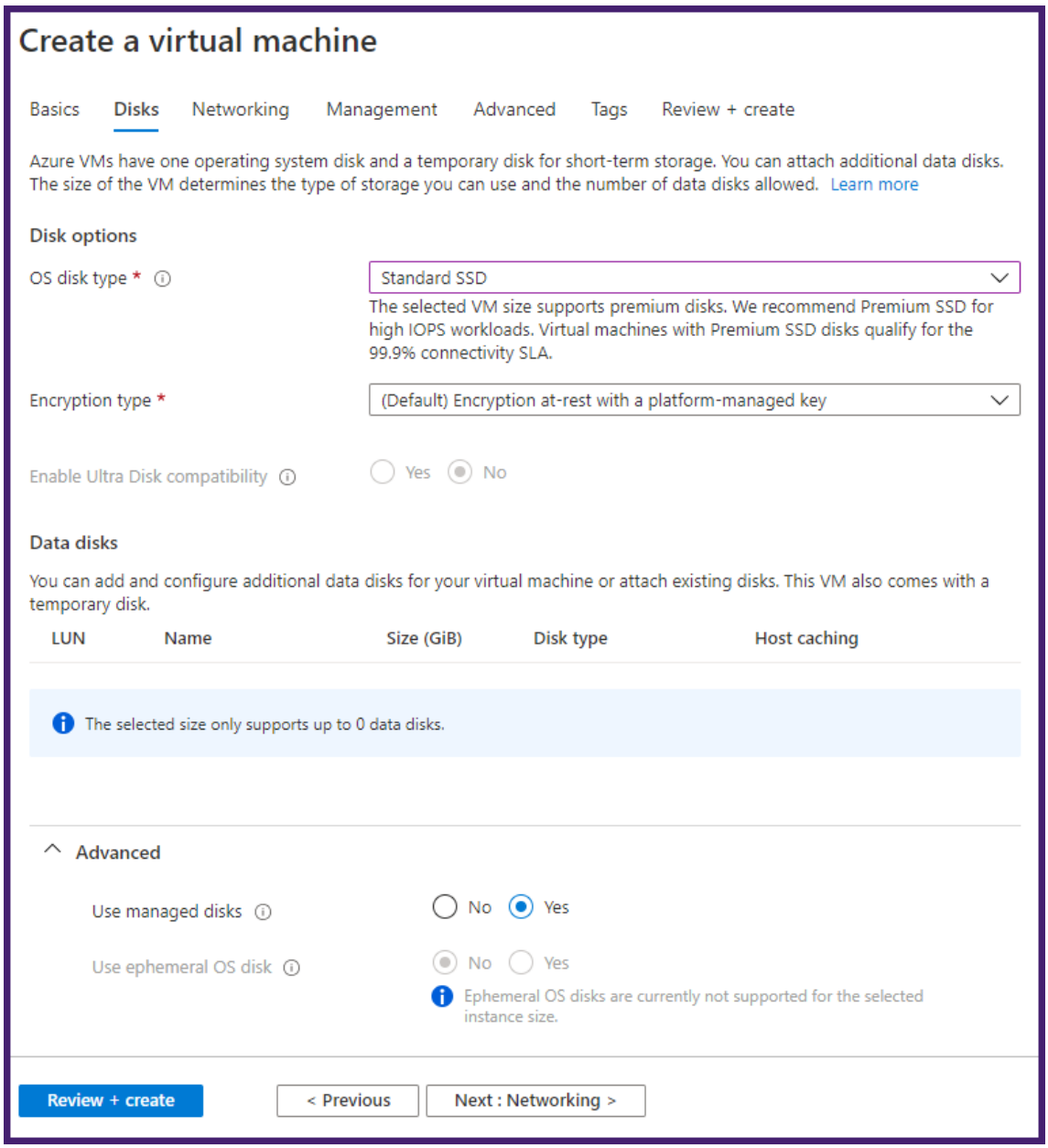
  Seleccione el tipo de disco virtual compatible (**HDD** o **SSD**) de la lista.

  Para obtener más información sobre los tamaños de discos virtuales admitidos, consulte Requisitos de instalación del agente y Agente ligero para licencias agrupadas.
- **Tipo de autenticación**: Seleccione Contraseña.
- **Nombre de usuario y contraseña**: Especifique un nombre de usuario y una contraseña para tener acceso a los recursos del grupo de recursos que ha creado.

  > **Importante**
  >
  > Le recomendamos que especifique su propio nombre de usuario y contraseña para su agente. No utilice `nsrecover` o `nsroot` como nombre de usuario porque están reservados para los usuarios del agente.

Discos:

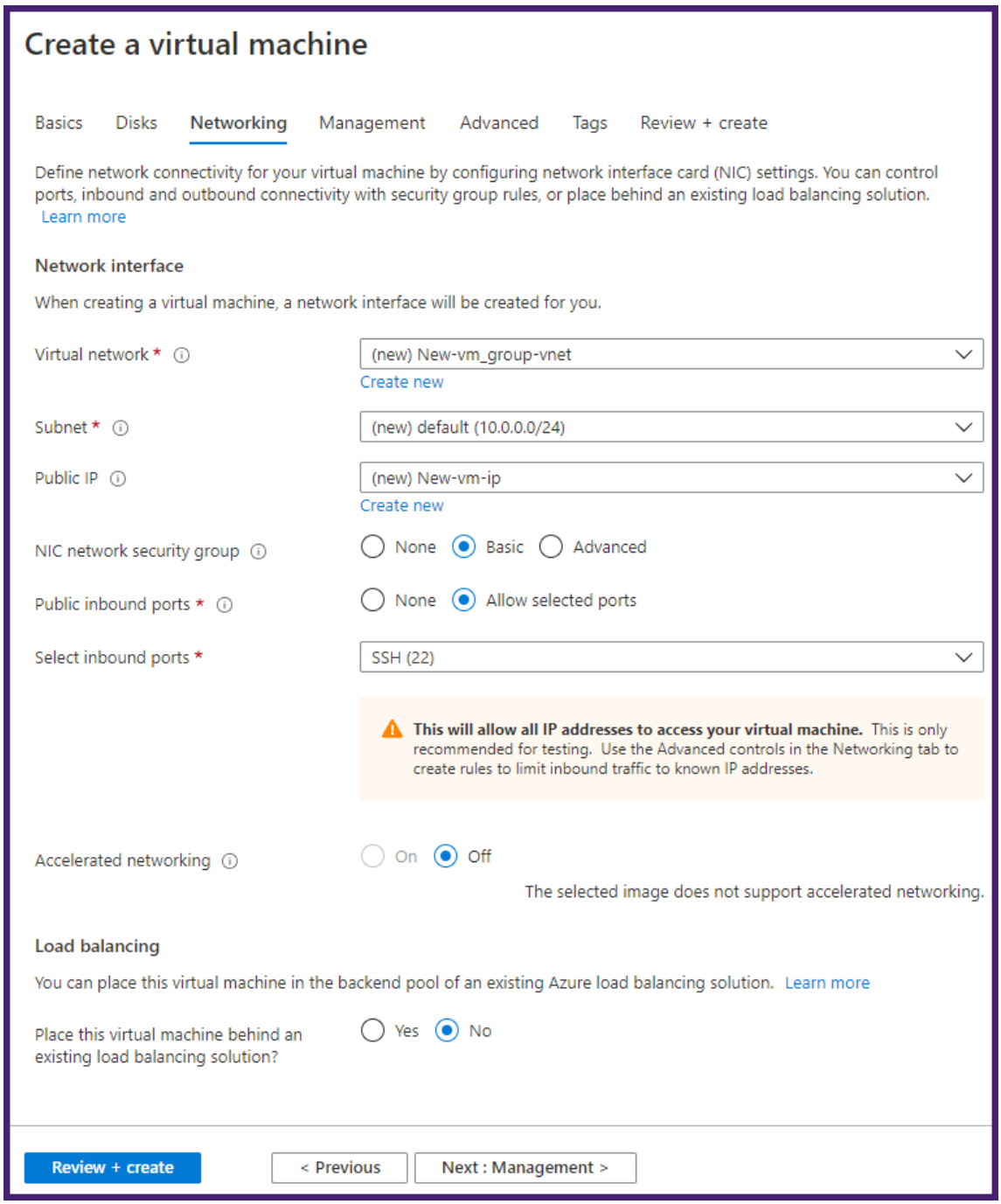
En esta ficha, especifique **las opciones de disco** y **Discos de datos**.



- **Tipo de disco de SO**: seleccione el tipo de disco virtual (HDD o SSD).

Redes:

Especifique los detalles de red requeridos:



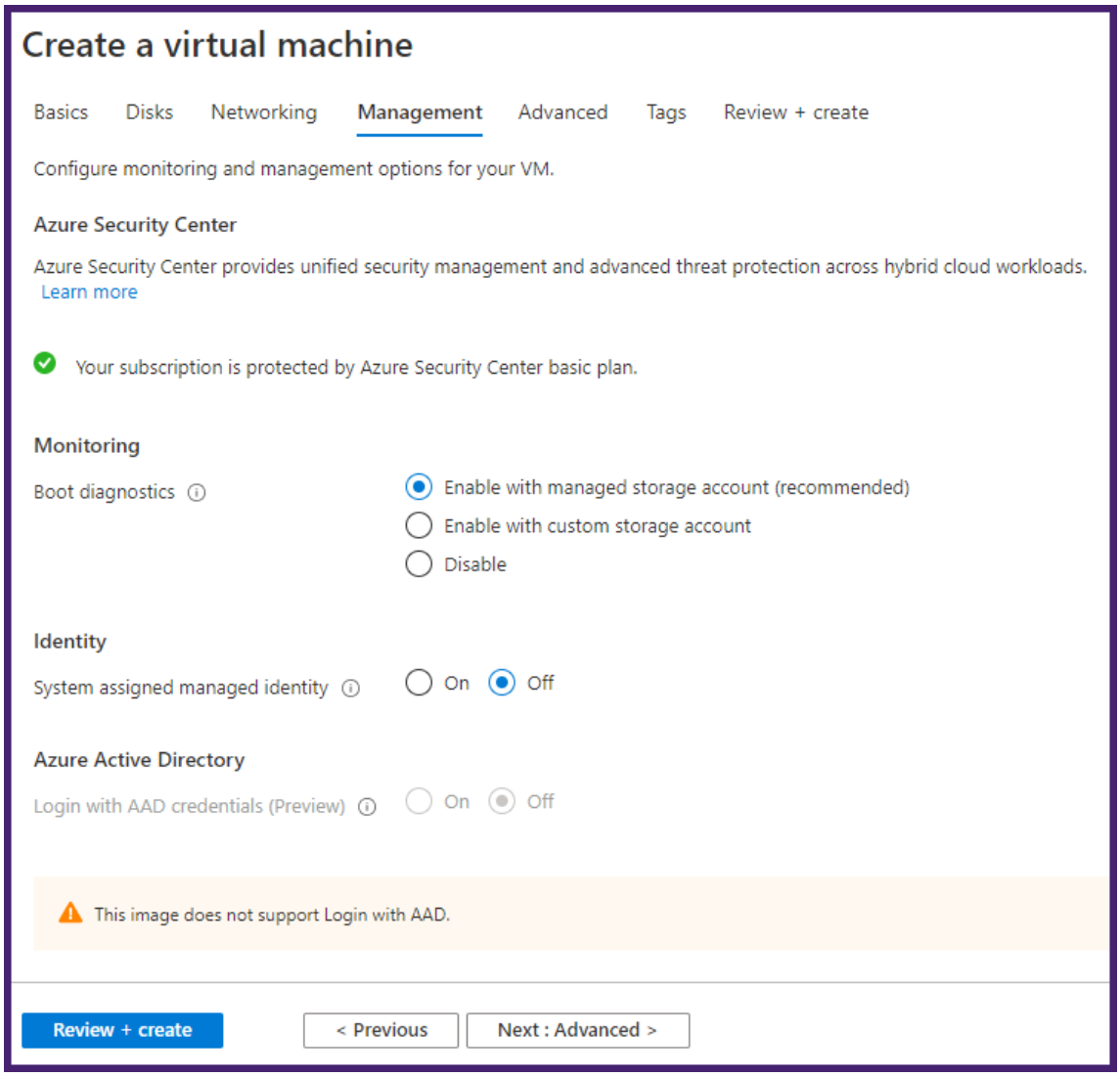
- **Red virtual**: Seleccione la red virtual.
- **Subred**: defina la dirección de la subred.
- **Dirección IP pública**: opcional, seleccione la dirección IP.
- **Grupo de seguridad de red**: si lo quiere, seleccione el grupo de seguridad que ha creado.
- **Seleccionar puertos entrantes**: si permite puertos entrantes públicos, asegúrese de que las reglas entrantes y salientes estén configuradas en el grupo de seguridad. A continuación, seleccione los puertos entrantes de la lista. Para obtener más información, con-

sulte Requisitos previos.

> **Nota**
>
> Asegúrese de que el agente tenga acceso a Internet.

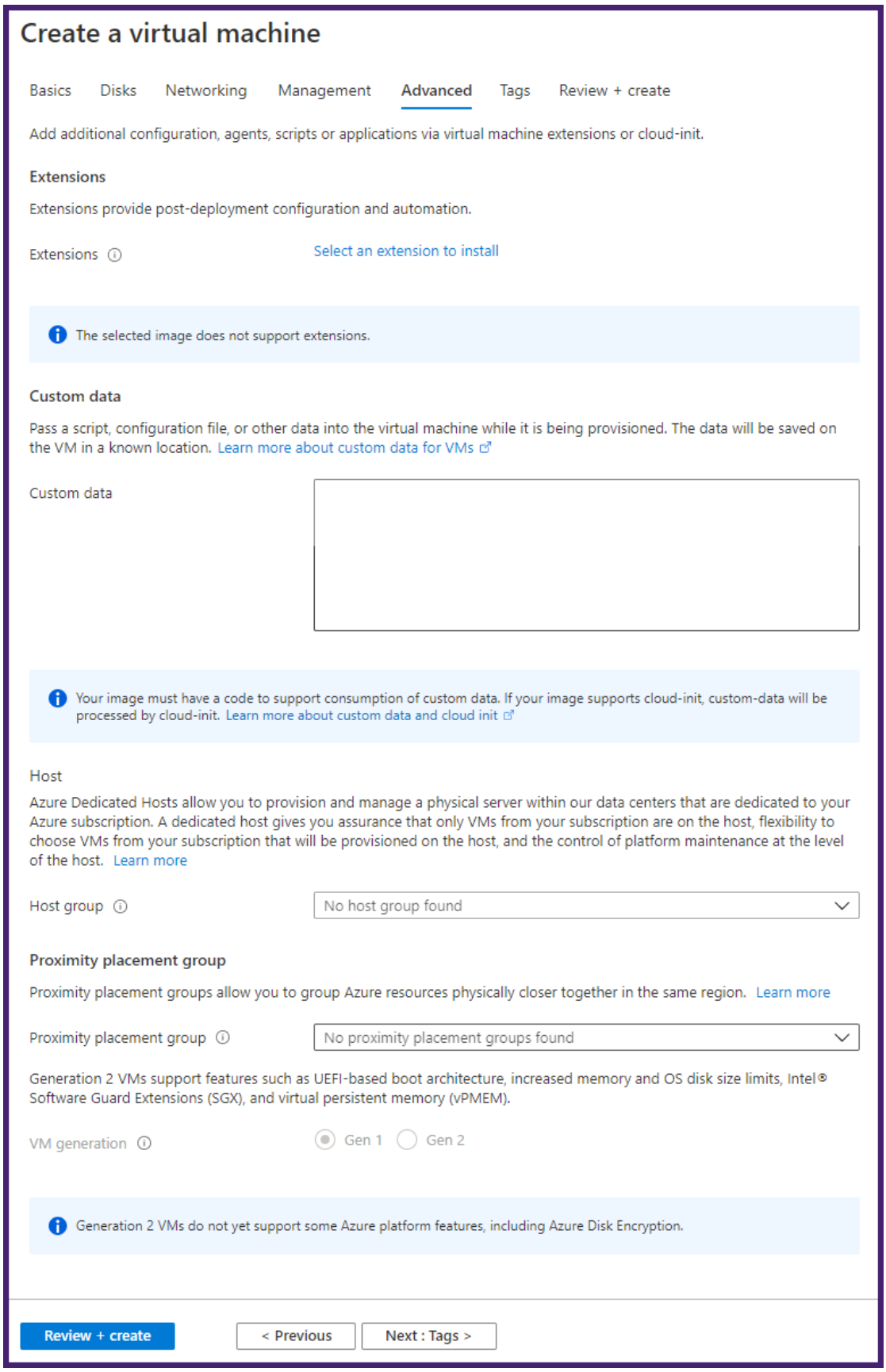
Gestión:

Especifique el **Centro de seguridad de Azure**, **la supervisión**y la **identidad**.



Avanzado:

Opcional, especifique el **grupo de ubicación**Extensiones**,**Datos personalizados**y Proximidad**.

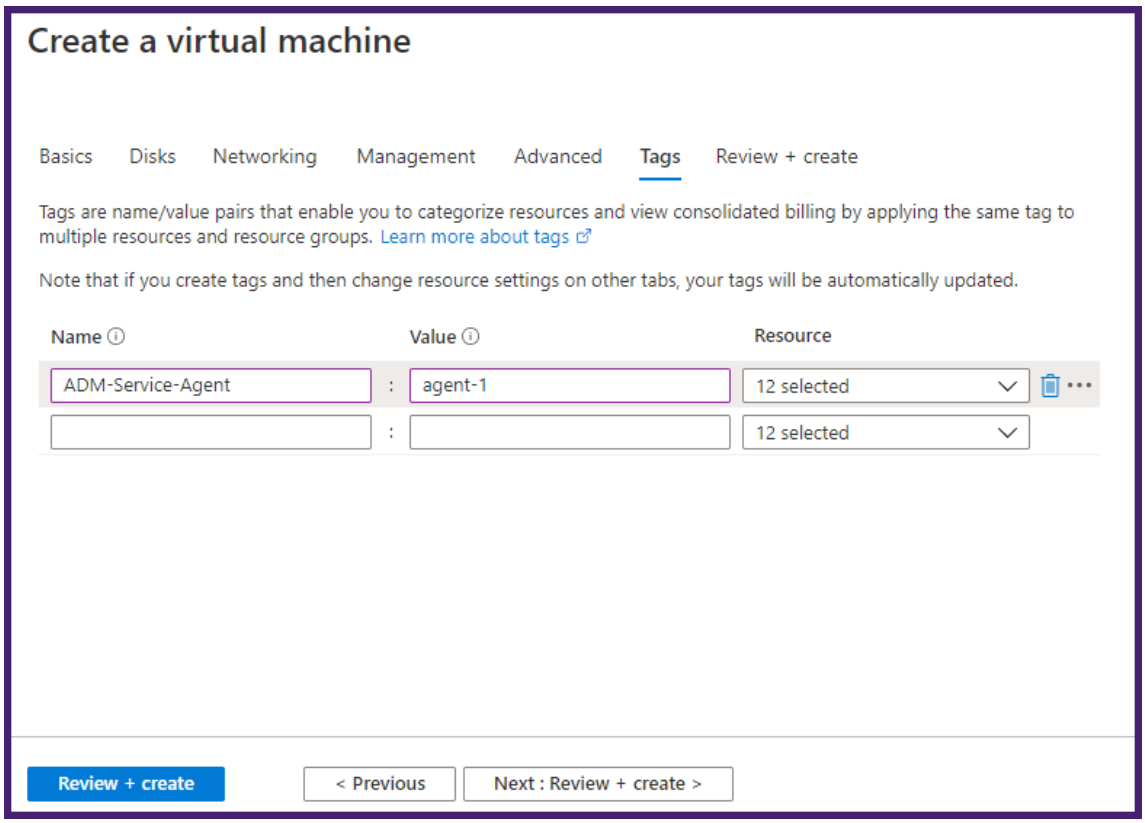


> **Nota** En **Datos personalizados** , especifique la **URL del servicio** y el **código de activación** que copió de la página **Configurar agentes** de NetScaler Console, tal y como se indica en Primeros pasos. Introduzca los detalles en el siguiente formato:
>
> ```
> registeragent -serviceurl <apigatewayurl> -activationcode <
>    activationcodevalue>
> ```
>
> El agente usa esta información para registrarse automáticamente en la consola de NetScaler durante el arranque.

Si especifica este script de registro automático, omita los pasos 7 y 8.

Etiquetas:

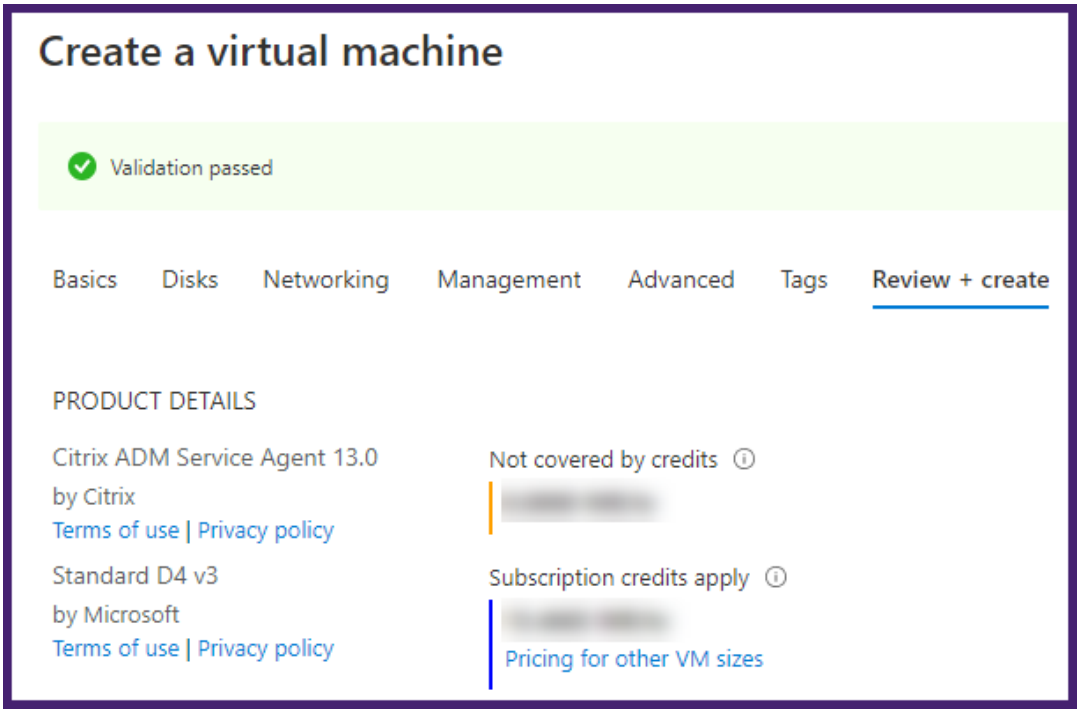
Escriba el par clave-valor para las etiquetas del agente de NetScaler. Una etiqueta consiste en un par clave-valor que distingue mayúsculas de minúsculas. Estas etiquetas le permiten organizar e identificar el agente fácilmente. Las etiquetas se aplican tanto a Azure como a NetScaler Console.



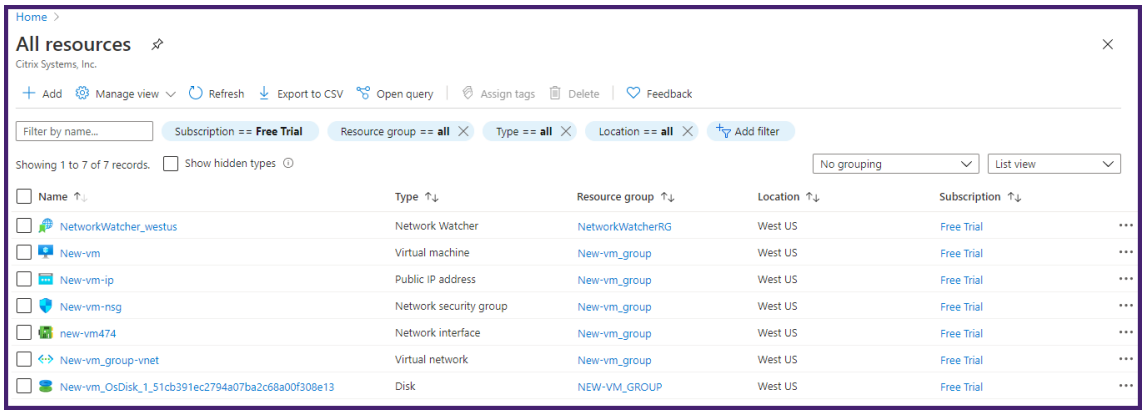
Los parámetros de configuración se validan y la ficha **Revisar y crear** muestra el resultado de la validación.

- Si la validación falla, esta ficha muestra el motivo del error. Vuelva a la sección en particular y realice los cambios necesarios.

- Si la validación pasa, haga clic en **Crear**. Comienza el proceso de implementación del agente.

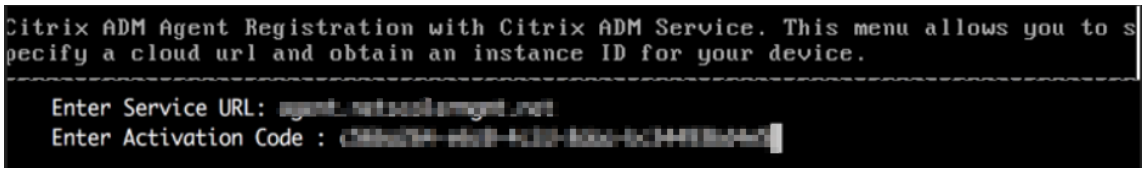


El proceso de implementación puede tardar entre 10 y 15 minutos aproximadamente. Una vez que la implementación se haya completado correctamente, podrá ver la máquina virtual del agente de NetScaler en su cuenta de Microsoft Azure.



6. Una vez que el agente esté en funcionamiento, utilice un cliente SSH para iniciar sesión en su agente de NetScaler. Utilice el nombre de usuario y la contraseña que se especificaron durante la creación de la máquina virtual.
7. Ejecute el script de implementación escribiendo el comando en la línea de comandos del shell: **deployment_type.py**.
8. Introduzca la **URL del servicio** y el **código de activación** que copió y guardó en la página **Configurar agentes** de NetScaler Console, tal y como se indica en Primeros pasos. El agente utiliza

la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.



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

Una vez reiniciado el agente, acceda **a NetScaler Console y, en la página Configurar** agente , en **Agentes descubiertos** , compruebe el estado del agente.

Instale un agente de NetScaler en Amazon Web Services (AWS)

January 26, 2024

El agente NetScaler funciona como intermediario entre la consola de NetScaler y las instancias descubiertas en el centro de datos o en la nube.

Requisitos previos

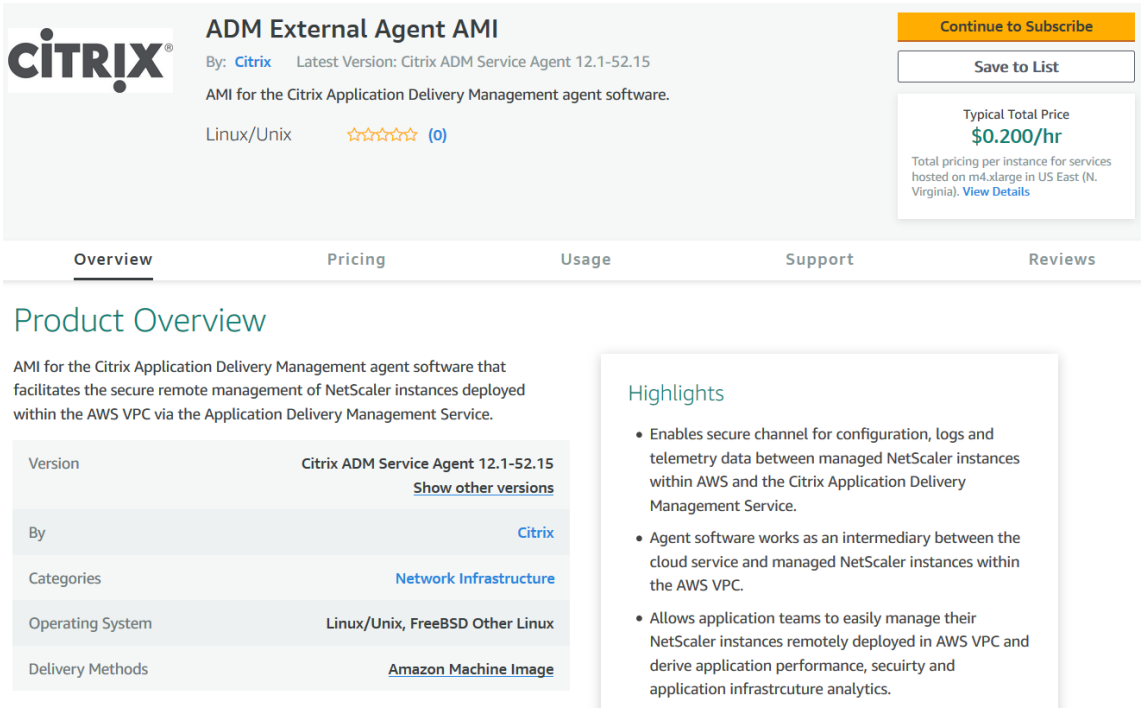
Para lanzar una AMI del agente de NetScaler en una nube privada virtual (VPC) de Amazon Web Services (AWS) mediante la GUI de Amazon, necesita:

- Una cuenta de AWS
- Una nube privada virtual (VPC) de AWS
- Una cuenta de IAM

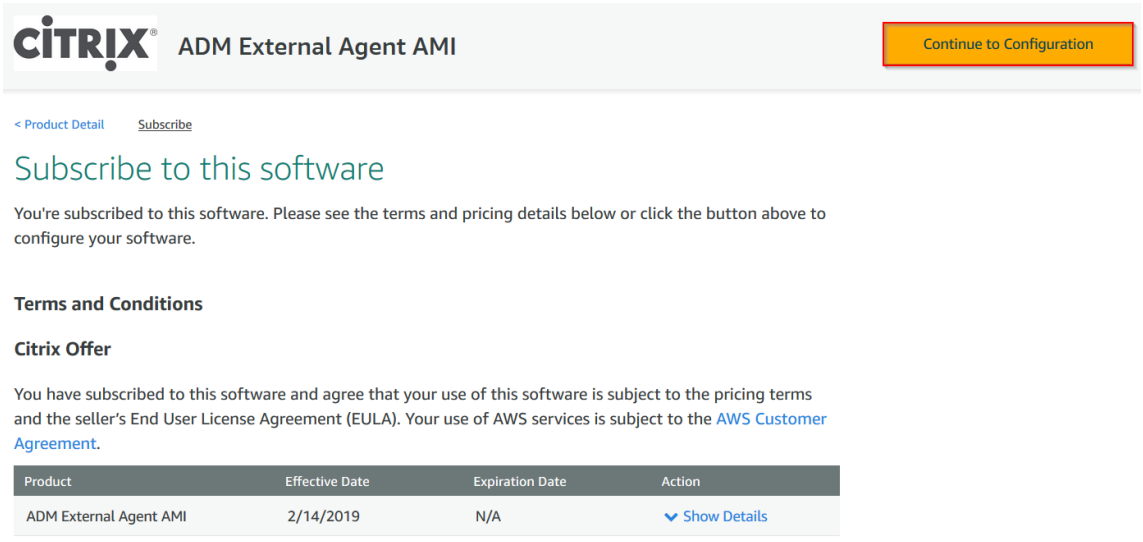
> **Nota**
>
> - Antes de aprovisionar una máquina virtual del agente de NetScaler, Citrix recomienda crear un grupo de seguridad, una red privada virtual, un par de claves, una subred y otras entidades. Por lo tanto, la información de red está disponible durante el aprovisionamiento.
> - Para que un agente de NetScaler se comunique con la consola de NetScaler y las instancias de NetScaler, asegúrese de que los puertos recomendados estén abiertos. Para obtener información completa sobre los requisitos de puerto para un agente de NetScaler, consulte Puertos.

Para instalar el agente de NetScaler en AWS:

1. Inicie sesión en el mercado de AWS mediante sus credenciales de AWS.
2. En el campo de búsqueda, escriba **NetScaler Agent** para buscar la AMI del agente NetScaler y haga clic en **Ir**.
3. En la página de resultados de la búsqueda, haga clic en la **AMI del agente externo de NetScaler Console** en la lista disponible.
4. En la página **AMI del agente externo de NetScaler Console** , haga clic en **Continuar con la suscripción**.



5. Cuando la suscripción se haya realizado correctamente, haga clic en **Continuar con la configuración**.



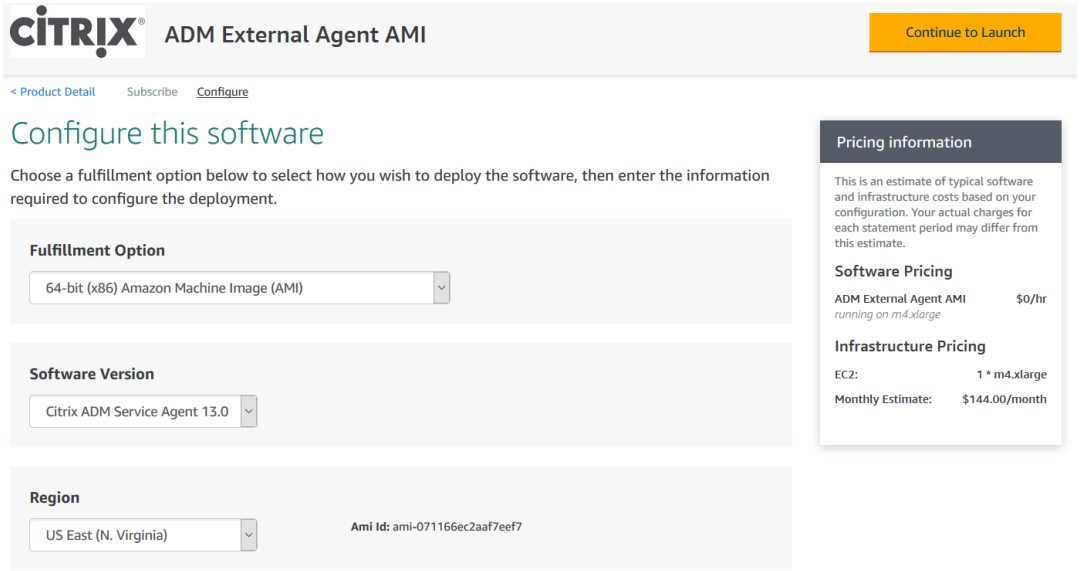
6. En la página **Configurar este software** :

   a) Seleccione la AMI de la lista de **opciones de cumplimiento**.

   b) Seleccione la versión más reciente del agente de NetScaler en la lista de versiones de **software**.

   c) Seleccione su región en la lista de **regiones**.

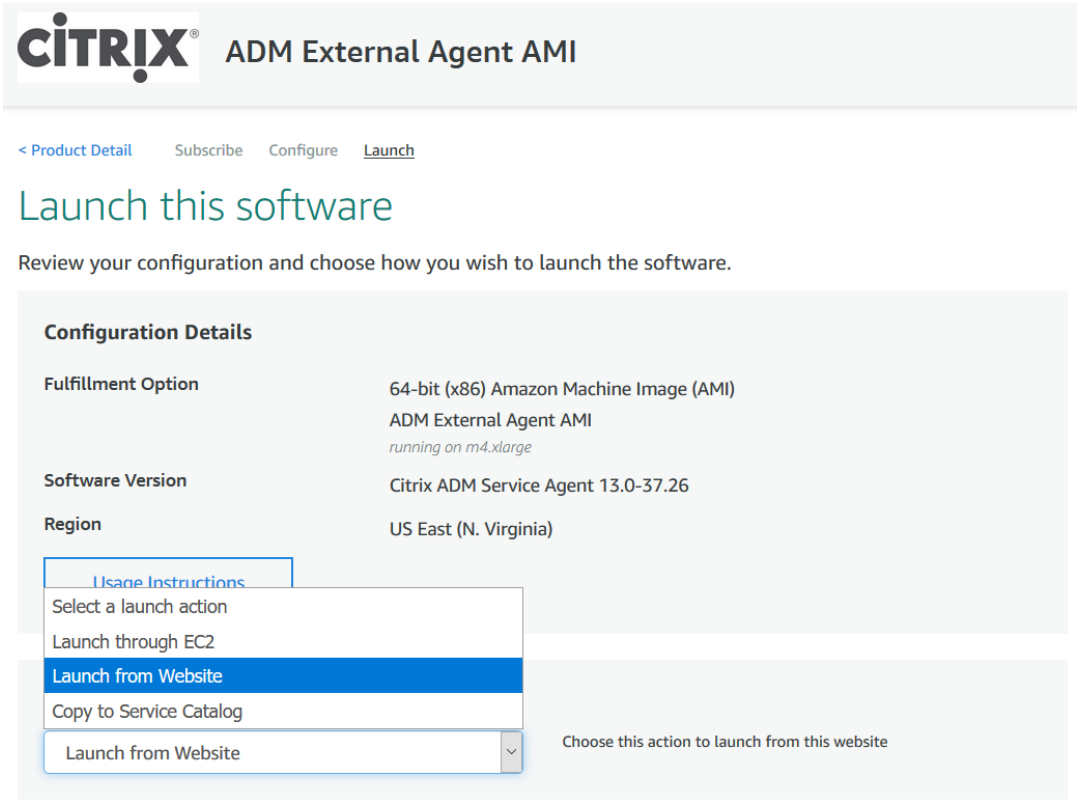
   d) Haga clic en **Continuar para iniciar**



7. En la página Iniciar **este software** , tiene dos opciones para registrar el agente de NetScaler:

   a) **Iniciar desde el sitio web**

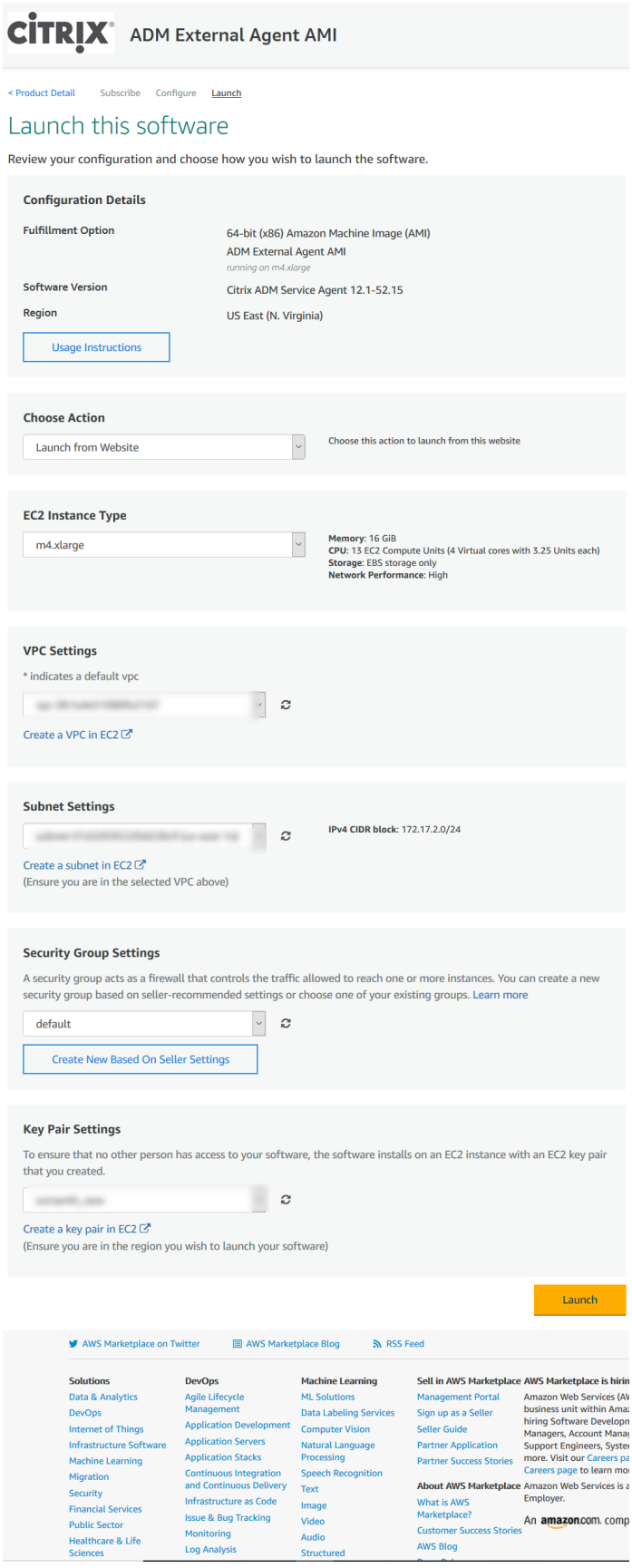
   b) **Lanzamiento con EC2**



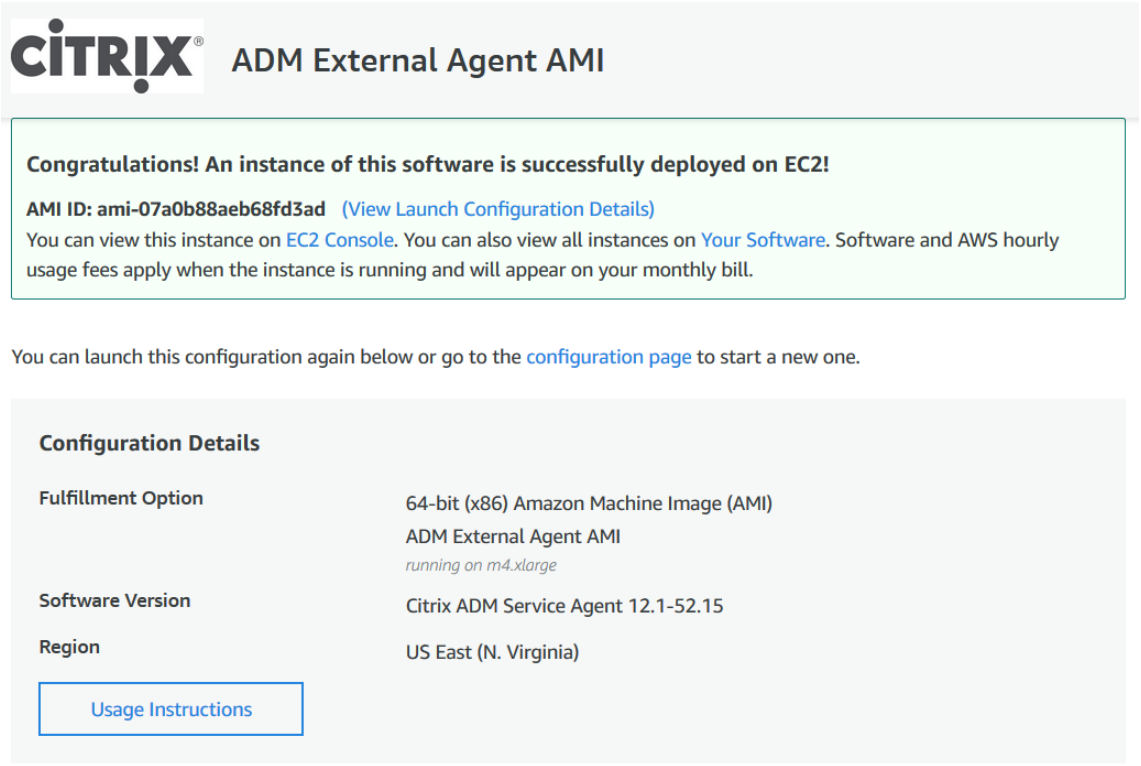
Lanzamiento desde un sitio web

Para iniciar desde un sitio web, selecciona:

1. Un tipo de instancia EC2 de la lista de **tipos de instancias EC2**
2. Una VPC de la lista de **ajustes de VPC**. Haga clic en **Crear una VPC en EC2** para crear una VPC para su software.
3. Una subred de la lista de **ajustes de subred**. Haga clic en **Crear una subred en EC2** para crear una subred después de seleccionar la VPC.
4. Un grupo de seguridad para el firewall de la lista de **configuración del grupo de seguridad**. Haga clic en **Crear nuevo según la configuración del vendedor** para crear un grupo de seguridad.
5. Un par de claves para garantizar la seguridad del acceso desde la lista de **ajustes de pares de claves**. Haga clic en **Crear un par de claves en EC2** para crear un par de claves para el software.
6. Haga clic en **Iniciar**



7. El lanzamiento desde un sitio web es un éxito.



> **Nota**
>
> El proceso de implementación puede tardar entre 10 y 15 minutos aproximadamente. Una vez completada correctamente la implementación, puede ver la máquina virtual del agente de NetScaler en su cuenta de AWS.

8. Una vez desplegado el agente, asigne un nombre al agente de NetScaler.
9. Una vez que el agente esté en funcionamiento, asigne una dirección IP elástica para su agente de NetScaler.

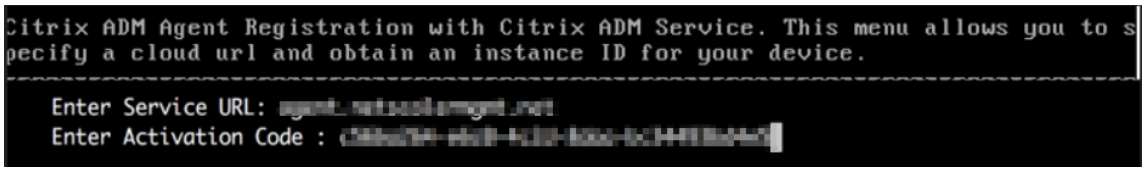
> **Nota**
>
> La dirección IP elástica permite al agente de NetScaler comunicarse con NetScaler Console. Sin embargo, es posible que no se necesite una dirección IP elástica si ha configurado NAT Gateway para dirigir el tráfico a Internet.

10. Con un cliente SSH, inicie sesión en su agente de NetScaler.

> **Nota**
>
> Puede iniciar sesión en el agente de NetScaler de una de las siguientes maneras:
>
> - Use `nsrecover` como nombre de usuario e ID de instancia de AWS como contraseña.

> • Use `nsroot` como nombre de usuario y un par de claves válido como contraseña.

11. Introduzca el siguiente comando para invocar la pantalla de implementación: **deployment_type.py**
12. Introduzca la **URL del servicio** y el **código de activación** que copió y guardó en la página **Configurar agentes** de NetScaler Console, tal y como se indica en Primeros pasos. El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.



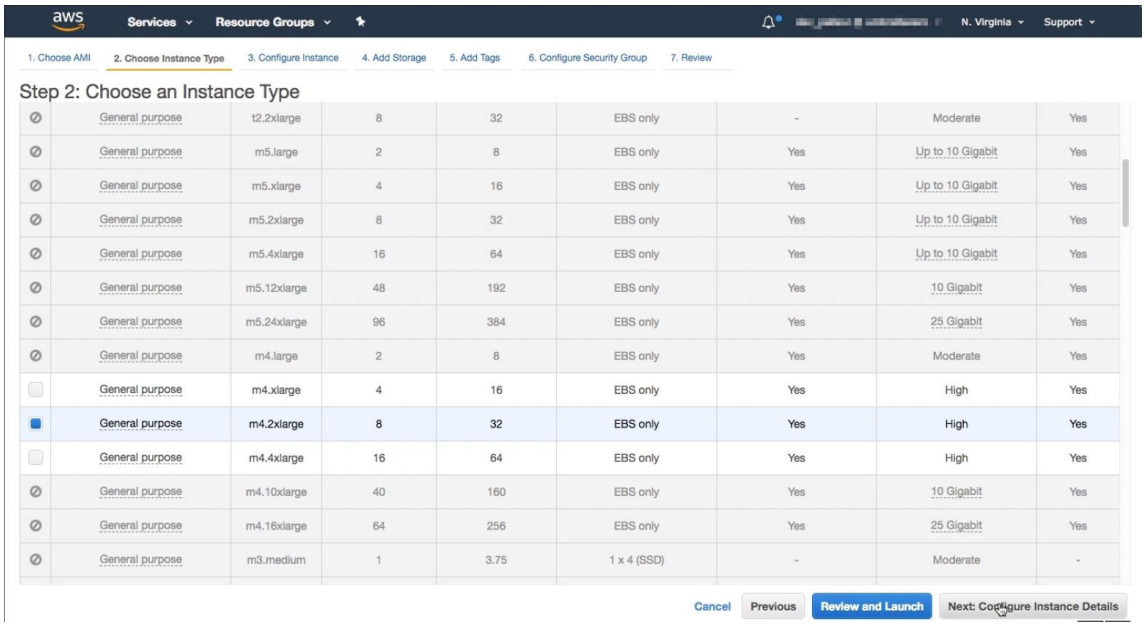
Una vez que el registro del agente se realiza correctamente, el agente se reinicia para completar el proceso de instalación.

Una vez reiniciado el agente, acceda **a NetScaler Console y, en la página Configurar** agente , en **Agentes descubiertos** , compruebe el estado del agente.

Lanzamiento con EC2

Para iniciar con EC2, seleccione **Iniciar a través de EC2** en la lista **Elegir acción** y, a continuación, haga clic en **Iniciar**.

1. En la página **Elegir un Tipo de Instancia**, seleccione la instancia y haga clic en **Siguiente: Configurar Detalles de Instancia**.



2. En la página **Configurar Detalles de Instancia**, especifique los parámetros necesarios.

   En la sección **Detalles avanzados**, puede habilitar un agente de contacto cero especificando detalles de autenticación o un script en el campo **Datos del usuario**.

   - **Detalles**de autenticación : especifique la **URL del servicio** y el **código de activación** que copió de la página **Configurar agentes** de NetScaler Console, tal y como se indica en Primeros pasos. Introduzca los detalles en el siguiente formato.

     ```
     registeragent -serviceurl <apigatewayurl> -activationcode <
         activationcodevalue>
     ```

     El agente usa esta información para registrarse automáticamente en la consola de NetScaler durante el arranque.

   - **Script**: especifique un script de registro automático del agente como datos de usuario. A continuación se muestra un script de ejemplo:

     ```
     #!/var/python/bin/python2.7
     import os
     import requests
     import json
     import time
     import re
     import logging
     import logging.handlers
     import boto3

     '''
     Overview of the Script:
     The script helps to register a NetScaler agent with NetScaler
          Console. Pass it in userdata to make NetScaler agent in
         AWS to autoregister on bootup. The workflow is as follows
     1)  Fetch the NetScaler Console API credentials (ID and
         secret) from AWS secret store (NOTE: you have to assign
         IAM role to the NetScaler agent that will give permission
         to fetch secrets from AWS secret store)
     2)  Login to NetScaler Console with credentials fetched in
         step 1
     3)  Call NetScaler Console to fetch credentials (serviceURL
         and token) for agent registration
     4)  Calls registration by using the credentials fetched in
         step 3
     '''

     '''
     These are the placeholders which you need to replace
         according to your setup configurations
     aws_secret_id: Id of the AWS secret where you have stored
         NetScaler Console Credentials
     The secrets value should be in the following json format
     {
     ```



```
 "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": "
    YOUR_SECRET" }

'''

aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Set up a specific logger with your desired output level and
    log file name
'''
log_file_name_local = os.path.basename(\_\_file\_\_)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50\*1024\*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(\_\_name\_\_)
logger.setLevel(logging.DEBUG)
logger_handler = logging.handlers.RotatingFileHandler(
    LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
    LOG_BACKUP_COUNT)
logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
    funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
    datefmt="%Y-%m-%d %H:%M:%S")
logger_handler.setFormatter(logger_fortmater)
logger.addHandler(logger_handler)

class APIHandlerException(Exception):
    def \_\_init\_\_(self, error_code, message):
        self.error_code = error_code
        self.message = message

    def \_\_str\_\_(self):
        return self.message + ". Error code '" + str(self.
            error_code) + "'"

def parse_response(response, url, print_response=True):
    if not response.ok:
        if "reboot" in url:
            logger.debug('No response for url: reboot')
            resp = {
"errorcode": "500", "message": "Error while reading response.
    " }

            return resp

        if print_response:
            logger.debug('Response text for %s is %s' % (url,
                response.text))

        response = json.loads(response.text)
        logger.debug("ErrorCode - " + str(response['errorcode
```



```
                '']) + ". Message -" + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
                response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                    str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
                headers=headers)
82          result = parse_response(response, url, print_response
                =print_response)
83          return result
84      except [requests.exceptions.ConnectionError, requests.
            exceptions.ConnectTimeout]:
85          if retry > 0:
86              return _request(method, url, data, headers, retry
                    -1, print_response=print_response)
87          else:
88              raise APIHandlerException(503, 'ConnectionError')
89      except requests.exceptions.RequestException as e:
90          logger.debug(str(e))
91          raise APIHandlerException(500, str(e))
92      except APIHandlerException as e:
93          logger.debug("URL: %s, Error: %s, Message: %s" % (url
                , e.error_code, e.message))
94          raise e
95      except Exception as e:
96          raise APIHandlerException(500, str(e))
97
98  try:
99      '''Get the AWS Region'''
100     client = boto3.client('s3')
101     my_region = client.meta.region_name
102     logger.debug("The rgion is %s" % (my_region))
103
104     '''Creating a Boto cleint session'''
105     session = boto3.session.Session()
106     client = session.client(
107         service_name='secretsmanager',
108         region_name=my_region
109     )
110
111     '''Getting the values stored in the secret with id: <
```

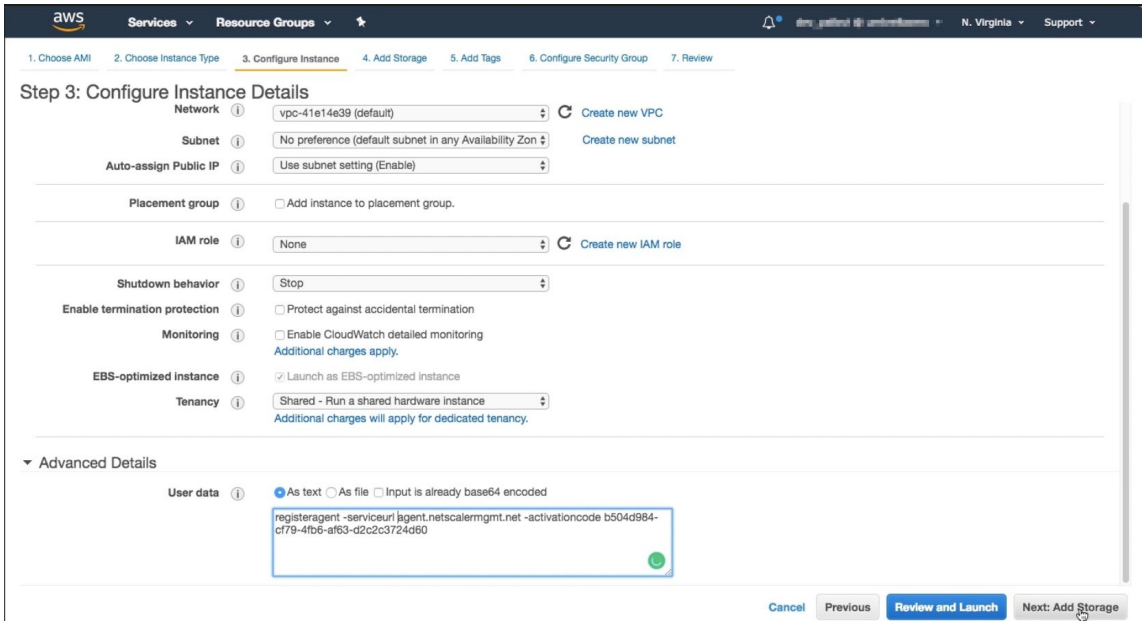


```
            aws_secret_id>'''
112         get_id_value_response = client.get_secret_value(
113             SecretId = aws_secret_id
114         )
115         adm_user_id = json.loads(get_id_value_response["
               SecretString"])["adm_user_id_key"]
116         adm_user_secret = json.loads(get_id_value_response["
               SecretString"])["adm_user_secret_key"]
117
118     except Exception as e:
119         logger.debug("Fetching of NetScaler Console credentials
               from AWS secret failed with error: %s" % (str(e)))
120         raise e
121
122     '''
123     Initializing common NetScaler Console API handlers
124     '''
125     mas_common_headers = {
126
127         'Content-Type': "application/json",
128         'Accept-type': "application/json",
129         'Connection': "keep-alive",
130         'isCloud': "true"
131      }
132
133
134     '''
135     API to login to the NetScaler Console and fetch the Session
           ID and Tenant ID
136     '''
137     url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
           config/login"
138     payload = 'object={
139     "login":{
140     "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"
            }
141      }
142     '
143     try:
144         response = _request("POST", url, data=payload, headers=
               mas_common_headers)
145         sessionid = response["login"][0]["sessionid"]
146         tenant_id = response["login"][0]["tenant_name"]
147     except Exception as e:
148         logger.debug("Login call to the NetScaler Console failed
               with error: %s" % (str(e)))
149         raise e
150
151     '''
152     API to fetch the service URL and Token to be used for
           registering the agent with the NetScaler Console
153     '''
154     mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
```



```
155   url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
          config/trust_preauthtoken/" + tenant_id +"?customer="+
          tenant_id
156   logger.debug("Fetching Service URL and Token.")
157   try:
158       response = _request("GET", url, data=None, headers=
              mas_common_headers)
159       service_name  = response["trust_preauthtoken"][0]["
              service_name"]
160       token = response["trust_preauthtoken"][0]["token"]
161       api_gateway_url = response["trust_preauthtoken"][0]["
              api_gateway_url"]
162   except Exception as e:
163       logger.debug("Fetching of the Service URL Passed with
              error. %s" % (str(e)))
164       raise e
165
166   '''
167   Running the register agent command using the values we
          retrieved earlier
168   '''
169   try:
170       registeragent_command = "registeragent -serviceurl "+
              api_gateway_url+" -activationcode "+service_name+";"+
              token
171       file_run_command = "/var/python/bin/python2.7 /mps/
              register_agent_cloud.py "+registeragent_command
172       logger.debug("Executing registeragent command: %s" % (
              file_run_command))
173       os.system(file_run_command)
174   except Exception as e:
175       logger.debug("Agent Registeration failed with error: %s"
              % (str(e)))
176           raise e
```

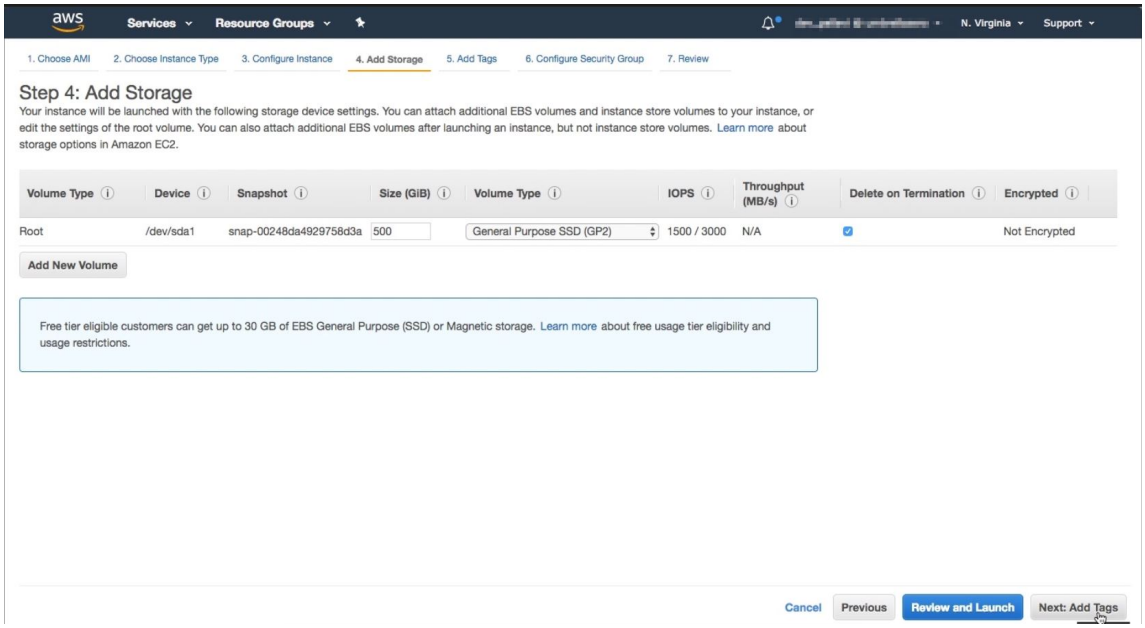
Este script obtiene los detalles de autenticación del administrador de secretos de AWS y lo ejecuta para `deployment.py`registrar el agente en la consola de NetScaler.



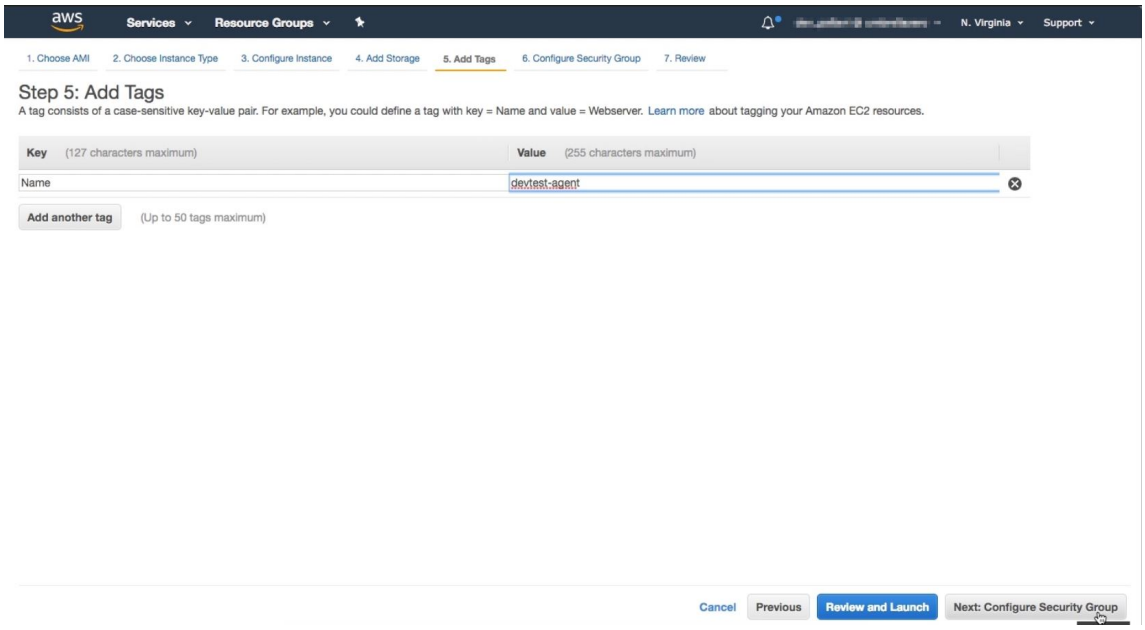
> **Nota**
>
> Si bien puede asignar automáticamente una dirección IP pública, también puede asignar una dirección IP elástica. La asignación de una dirección IP elástica es necesaria cuando la puerta de enlace NAT no está configurada.
>
> Si la dirección IP elástica no está configurada en este paso, aún puede hacerlo en la consola EC2. Puede crear una nueva dirección IP elástica y asociarla con el agente de NetScaler mediante el ID de instancia o el ENI-ID.

Haga clic en **Agregar almacenamiento**.

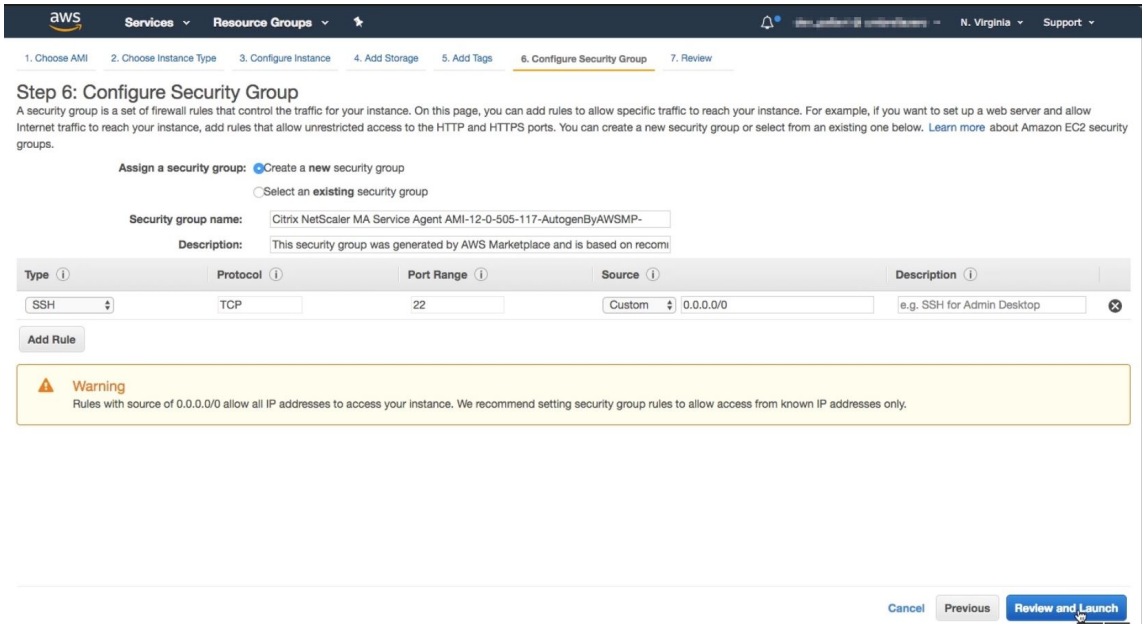
3. En la página **Agregar almacenamiento**, configure la configuración del dispositivo de almacenamiento para la instancia y haga clic en **Siguiente: Agregar etiquetas**.



4. En la página **Agregar etiquetas**, defina la etiqueta de la instancia y haga clic en **Siguiente: Configurar grupo de seguridad**.

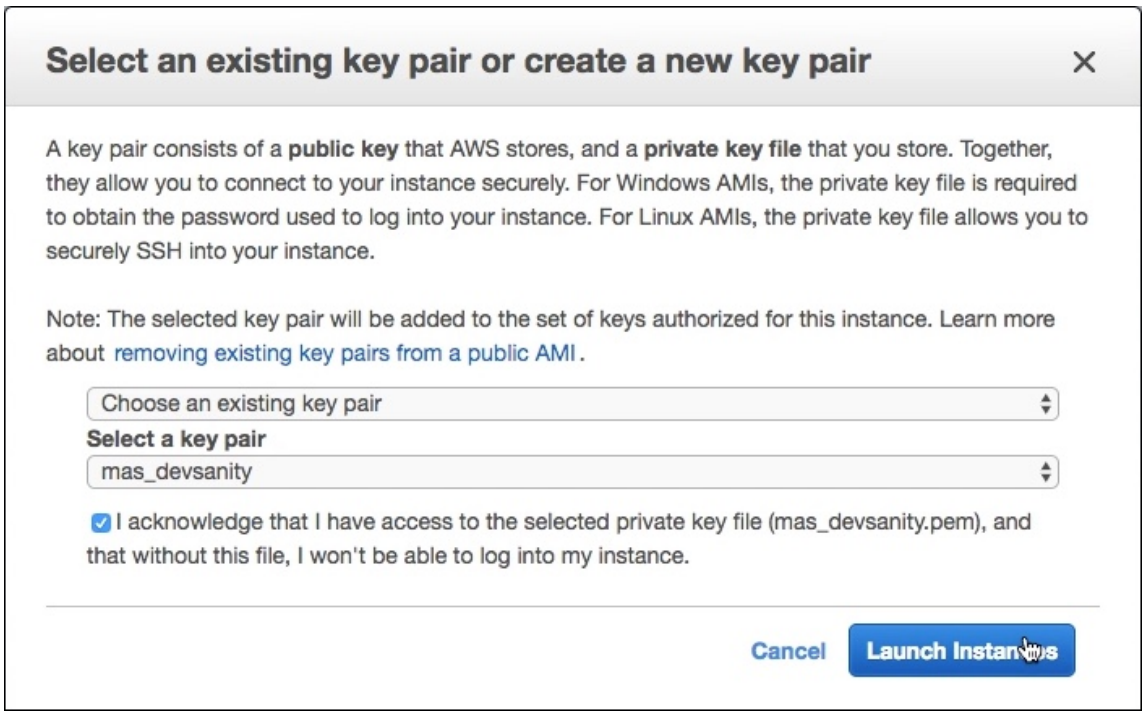


5. En la página **Configurar grupo de seguridad**, agregue reglas para permitir tráfico específico a la instancia y haga clic en **Revisar y lanzar**.



6. En la página **Revisar Inicio de Instancia**, revise la configuración de la instancia y haga clic en **Iniciar**.
7. En el cuadro de diálogo **Seleccionar un par de claves existente o crear un par de claves nuevo**, cree un par de claves. También puede seleccionar entre los pares de claves existentes.

   Acepte el acuse de recibo y haga clic en **Iniciar instancias**.



El proceso de implementación puede tardar entre 10 y 15 minutos aproximadamente. Una vez completada correctamente la implementación, puede ver la máquina virtual del agente de NetScaler en

su cuenta de AWS.

Instalar un agente de NetScaler en GCP

January 26, 2024

El agente NetScaler funciona como intermediario entre la consola de NetScaler y las instancias descubiertas en el centro de datos o en la nube. Puede implementar el agente en Google Cloud Platform (GCP) para facilitar la administración remota y segura de las instancias de NetScaler implementadas en la red virtual de Google Cloud a través de NetScaler Console. Para obtener más información, consulta Google Cloud Platform Marketplace.

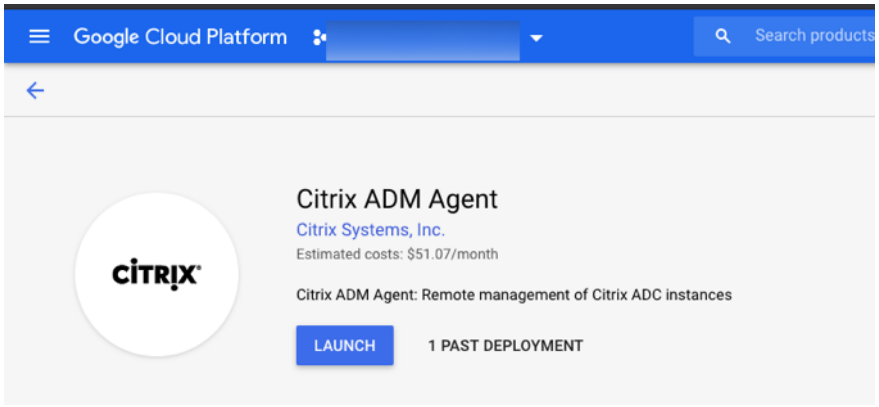
Requisitos previos

Para instalar un agente de NetScaler en GCP, necesitas una cuenta de GCP.

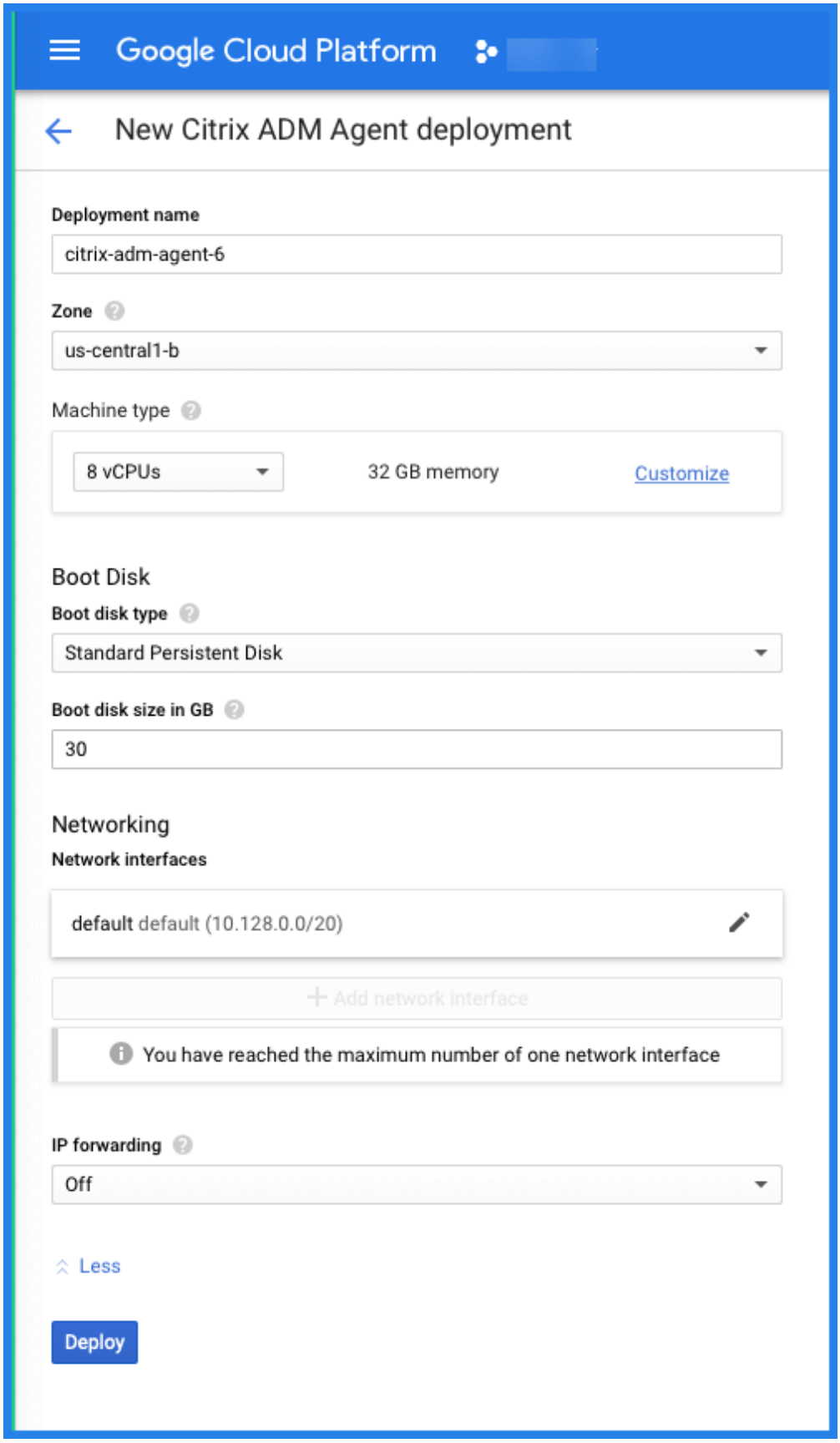
Instala el agente de NetScaler en GCP

Sigue estos pasos para instalar un agente de NetScaler en GCP.

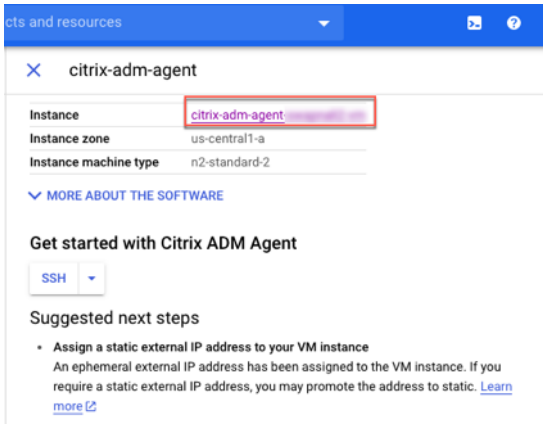
1. Inicie sesión en la consola de GCP (console.cloud.google.com) con sus credenciales y vaya al mercado.
2. En el campo de búsqueda, escriba **NetScaler agent** .
3. Haga clic en el **agente NetScaler** en el campo de resultados y, a continuación, haga clic en **Iniciar**.



4. En la página de **implementación del nuevo agente de NetScaler** , la mayoría de las opciones están configuradas de forma predeterminada. Puede cambiar las configuraciones predeterminadas según sea necesario y hacer clic en **Implementar**.



5. Una vez implementado el agente, haga clic en el vínculo de instancia y compruebe los detalles en la **página de detalles de la instancia de máquina virtual**.

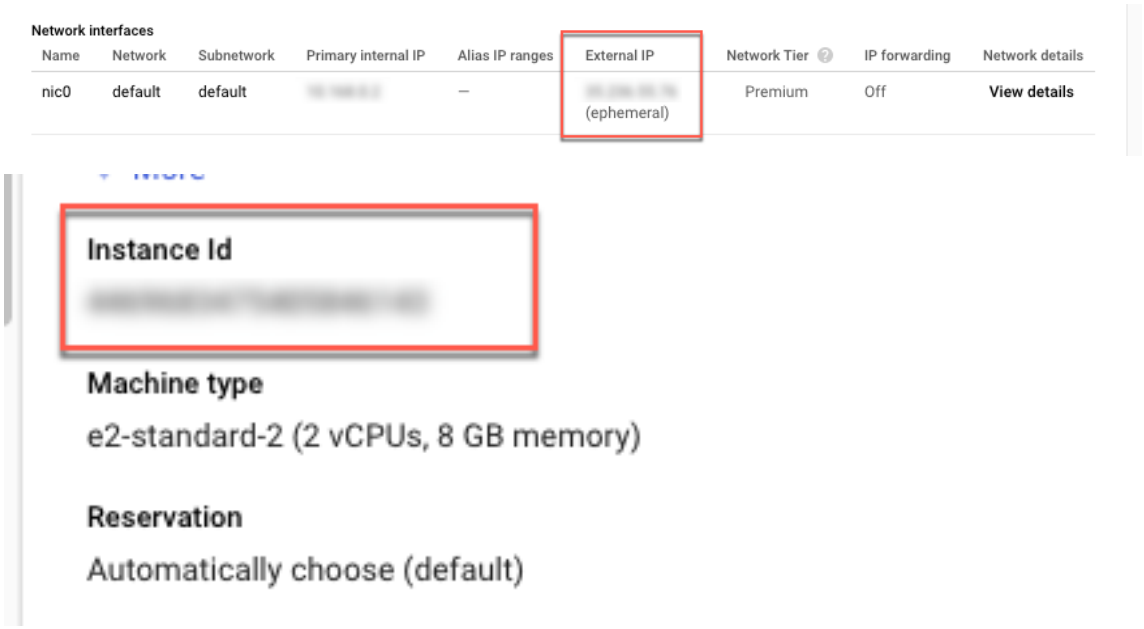


6. Inicie sesión en el agente a través de un cliente SSH utilizando la dirección IP externa del agente. Utilice los siguientes comandos:

   ```
   ssh nsrecover@<external IP address of the agent>
   ```

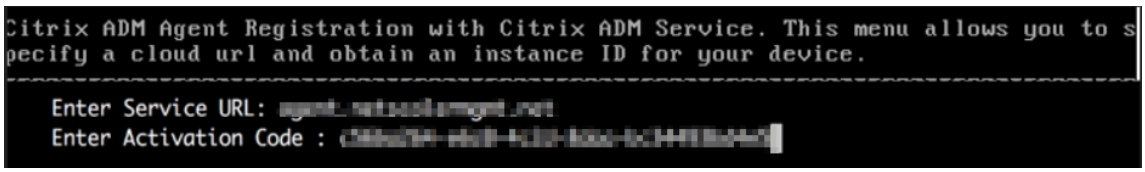
   Contraseña: ID de instancia

   ¿Puede encontrar la dirección IP externa y el identificador de instancia en la página de **detalles de la instancia de VM** ?



7. Introduzca el siguiente comando para invocar la pantalla de implementación: **deployment_type.py**
8. Introduzca la **URL del servicio** y el **código de activación** que copió y guardó en la página **Configurar agentes** de NetScaler Console, tal y como se indica en Primeros pasos. El agente utiliza

la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.



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

Una vez reiniciado el agente, acceda **a NetScaler Console y, en la página Configurar** agente , en **Agentes descubiertos** , compruebe el estado del agente.

Instale el agente NetScaler en un clúster de Kubernetes mediante YAML

January 26, 2024

> **Nota**
>
> El procedimiento para instalar un agente como microservicio está disponible en la sección Introducción.

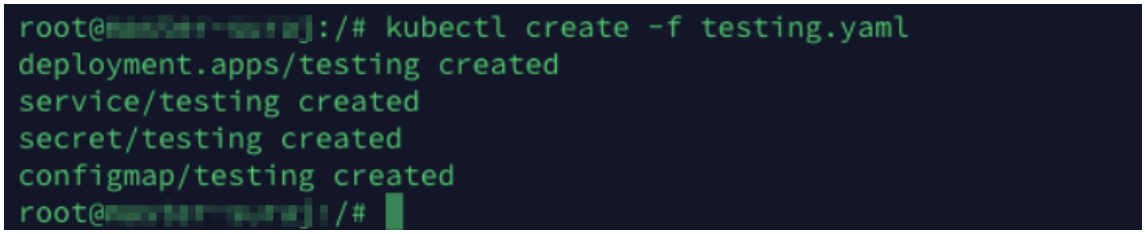
En el nodo principal de Kubernetes:

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

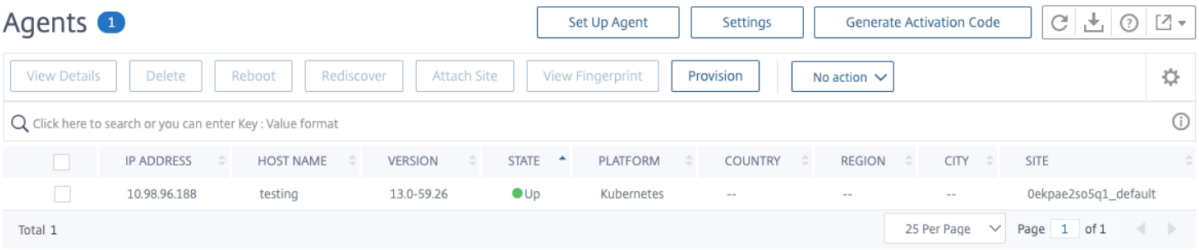
   `kubectl create -f <yaml file>`

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

   El agente se ha creado correctamente.



En NetScaler Console, vaya a **Infraestructura > Instancias Agentes** para ver el estado de los agentes.



> **Nota:**
>
> El agente de NetScaler configurado en un clúster de Kubernetes mediante YAML admite la actualización automática del agente (actualización permanente).

Instale un operador de agente de NetScaler mediante la consola de OpenShift

April 10, 2024

Un operador es un conjunto de herramientas de código abierto que permite implementar y administrar las aplicaciones de Kubernetes de forma eficaz, automatizada y escalable. Como administrador, puede implementar un agente en el clúster de OpenShift mediante el **operador de agentes ADM de NetScaler** .

> **Nota:**
>
> Un agente configurado en el clúster de OpenShift no se actualiza automáticamente de forma predeterminada.

Requisitos previos

Antes de realizar la implementación, asegúrese de que:

- Dispone de las restricciones de contexto de seguridad privilegiadas para controlar los permisos de los pods. Para el agente, ejecute el siguiente comando para obtener las restricciones del contexto de seguridad de privilegios para la cuenta de servicio:

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- Ejecute el siguiente comando para crear un secreto de inicio de sesión del agente:

  ```
  kubectl create secret generic admlogin --from-literal=username=
  nsroot --from-literal=password=<adm-agent-password> -n <namespace
  >
  ```


> **Nota:**
>
> - `<adm-agent-password>` es un ejemplo de contraseña. Debe establecer una contraseña para el agente y NetScaler CPX utilizará estas credenciales para registrarse en el agente.
> - Proporcione **admlogin** para `loginSecret` en el YAML del agente al crear la instancia.

Si va a implementar NetScaler CPX y el agente en diferentes espacios de nombres, asegúrese de:

- Etiquetar el espacio de nombres con `citrix-cpx=enabled` en el que se ha implementado NetScaler CPX.
- Establecer `helper.required` como true o false al instalar el operador del agente.

  > **Nota:**
  >
  > De forma predeterminada, `helper.required` se establece en **false**. Si este parámetro se establece en false, debe asegurarse de crear un secreto de **admlogin** en cada espacio de nombres si NetScaler CPX y el agente se encuentran en espacios de nombres diferentes.

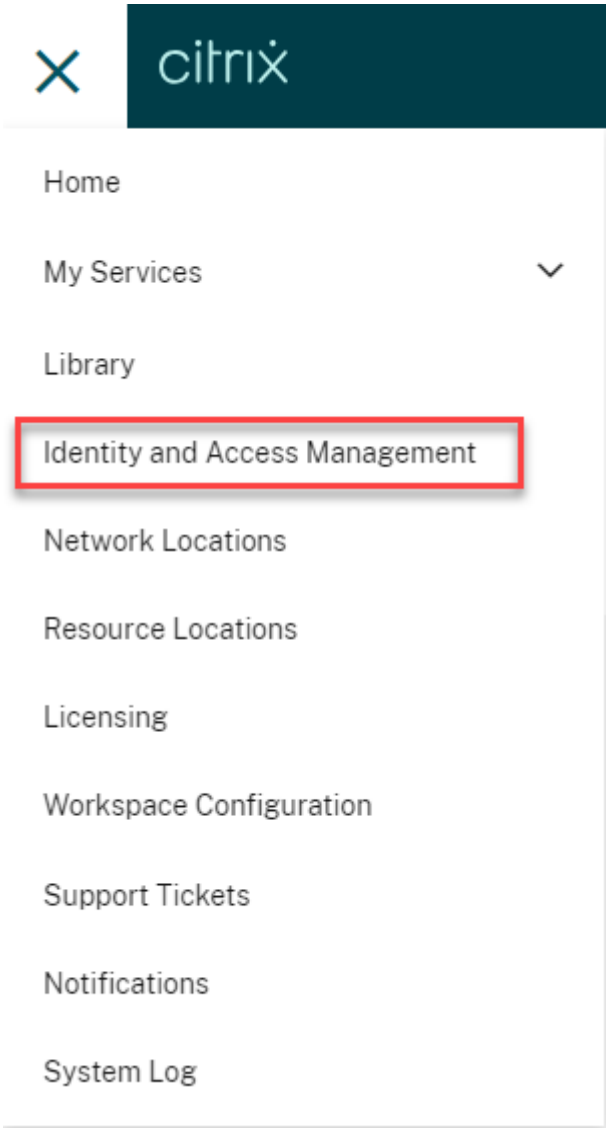
- Tienes lo `accessSecret`que se requiere en el YAML del agente. Estas credenciales son necesarias para que el agente se conecte al servicio NetScaler Console.

  ```
  kubectl create secret generic <secretname> --from-literal=accessid
  =<ID> --from-literal=accesssecret=<Secret> -n namespace
  ```

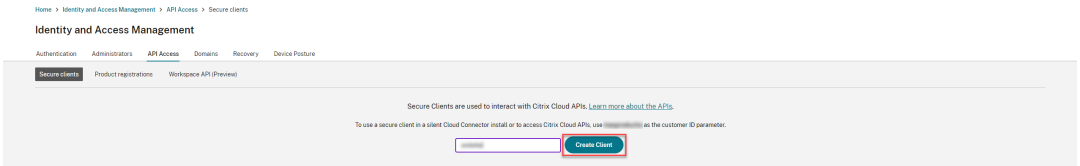
  > **Nota:**
  >
  > Proporcione un nombre secreto para AccessSecret en el agente YAML al crear la instancia.

  Puede obtener el ID de acceso y el secreto para acceder a la consola de NetScaler mediante el siguiente procedimiento:

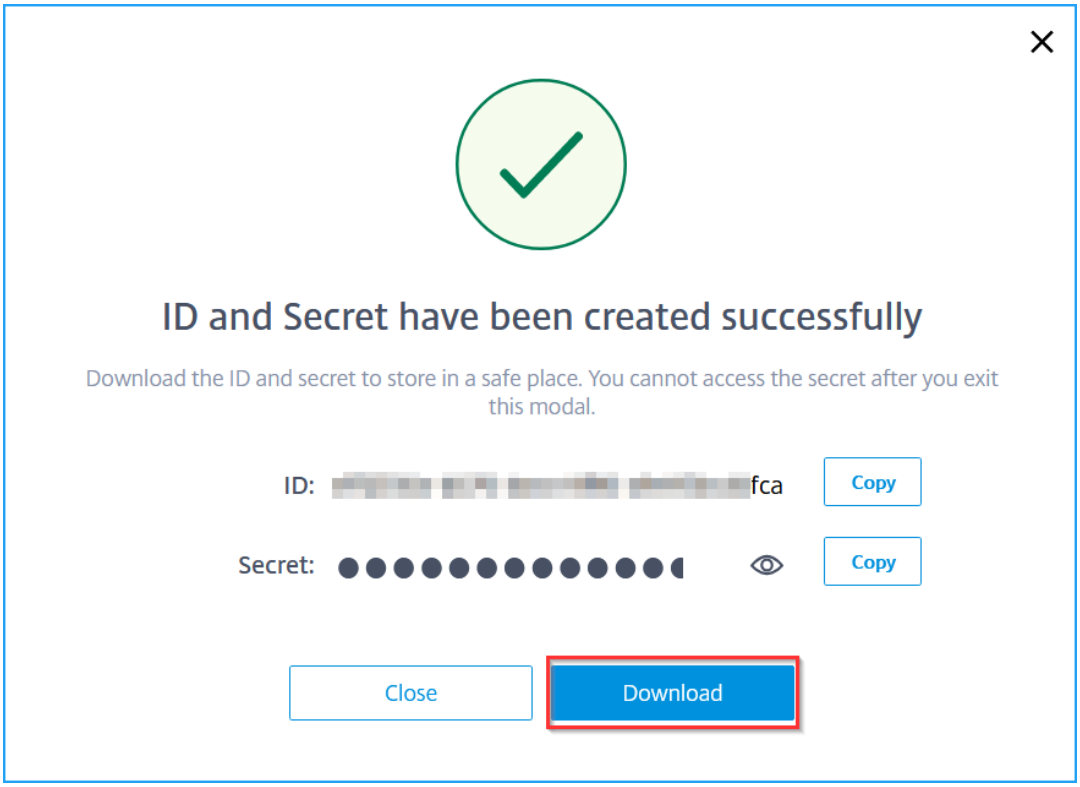
  1. Inicie sesión en la consola de administración de Citrix Cloud.
  2. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.



3. En la ficha **Acceso API**, introduzca un nombre de cliente seguro y haga clic en **Crear cliente**.

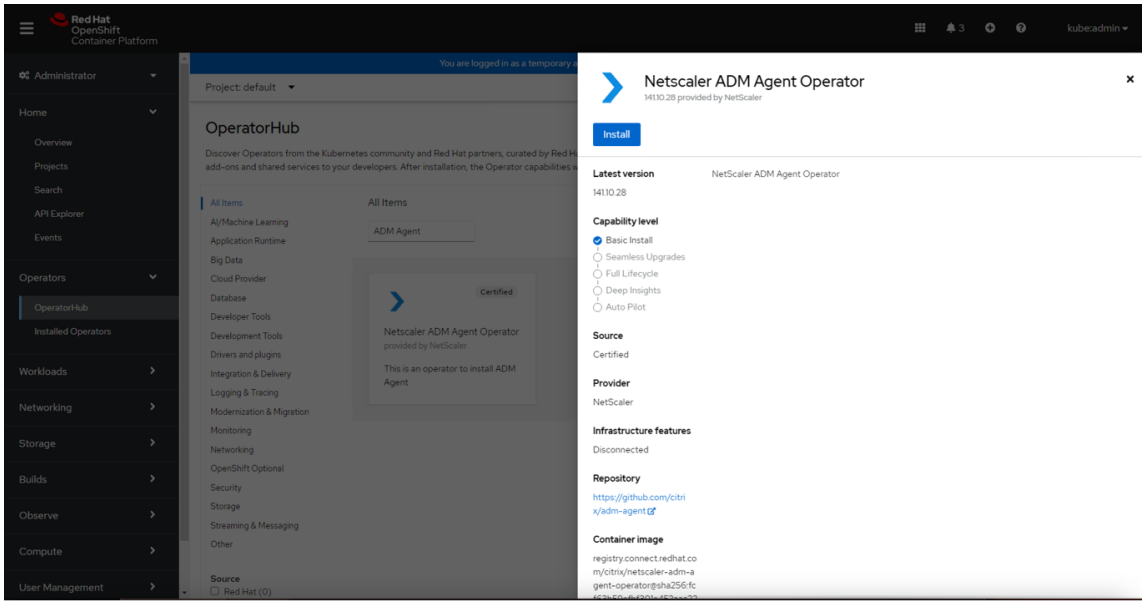


4. Se generan el ID y el secreto. Haga clic en **Descargar** y guarda el archivo CSV.



Instale el operador del agente

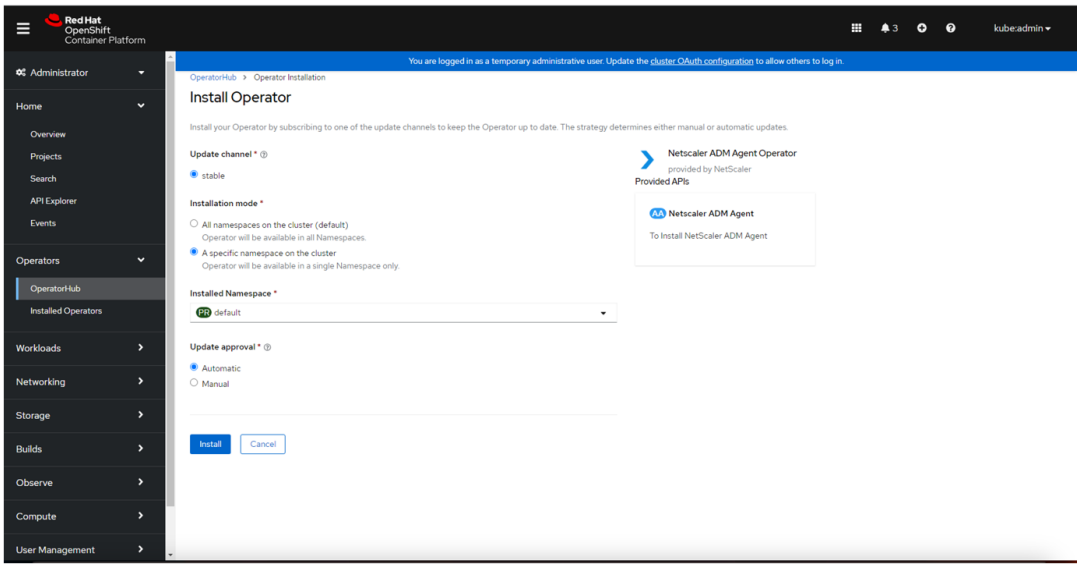
1. Inicie sesión en la consola de clústeres de OpenShift.
2. Navega hasta **Operadores > OperatorHub**.
3. En la barra de búsqueda, proporcione el nombre del agente, seleccione el **operador del agente de NetScaler ADM** y, a continuación, haga clic en **Instalar**.



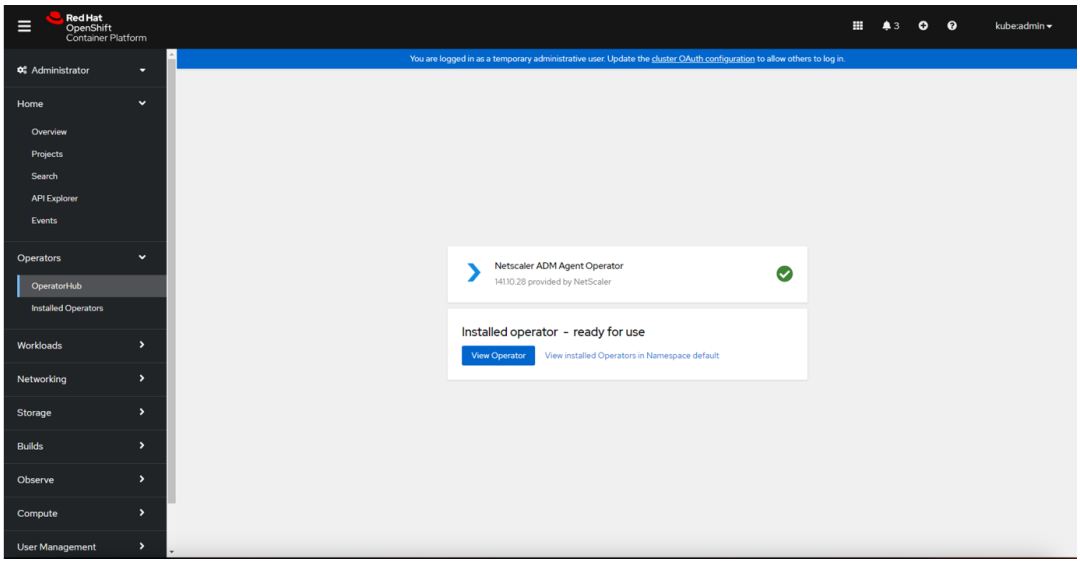
4. En la página **Install Operator**, tiene dos opciones:

   - **Todos los espacios de nombres del clúster (predeterminado)**: permite al operador del agente suscribirse a todos los espacios de nombres disponibles en el clúster y le permite iniciar la instancia del operador del agente desde cualquier espacio de nombres del clúster.
   - **Un espacio de nombres específico en el clúster**: permite al operador del agente suscribirse a un espacio de nombres seleccionado en el clúster y usted puede iniciar la instancia del operador del agente solo desde el espacio de nombres seleccionado.

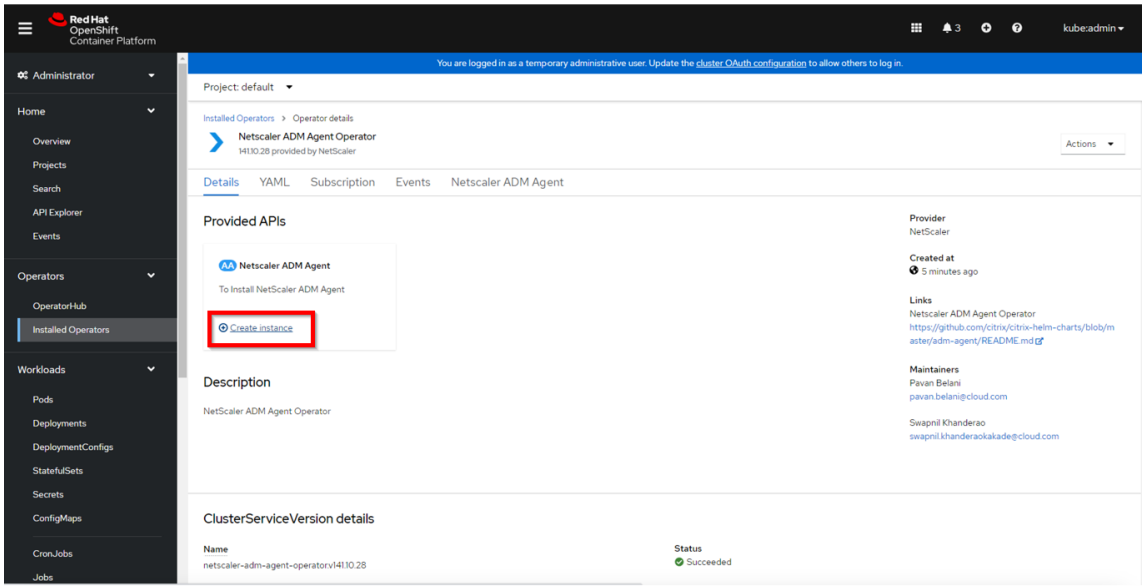
     En este ejemplo, el operador del agente se asigna a un espacio de nombres denominado **Predeterminado** . Seleccione **Automático** en **Aprobación de actualizaciones**y haga clic en **Instalar**.



Espere hasta que el operador del agente se haya suscrito correctamente.

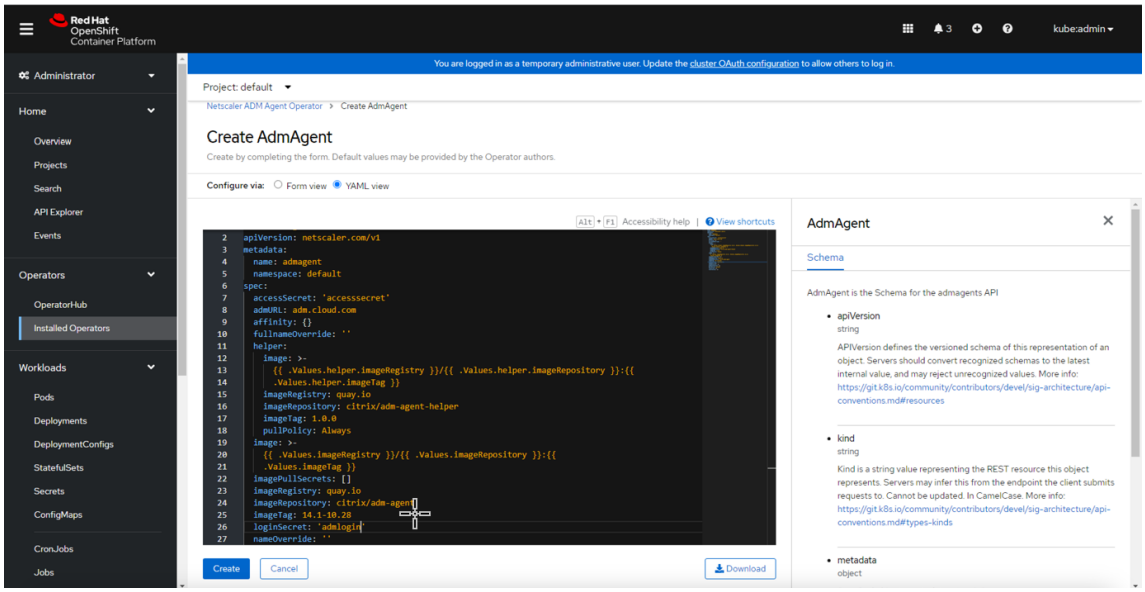


5. Vaya a **Cargas de trabajo > Pods** y compruebe que el pod `netscaler-adm-agent-operator-controller` esté en funcionamiento.
6. Una vez que el pod esté en funcionamiento, haga clic en **Crear instancia**.

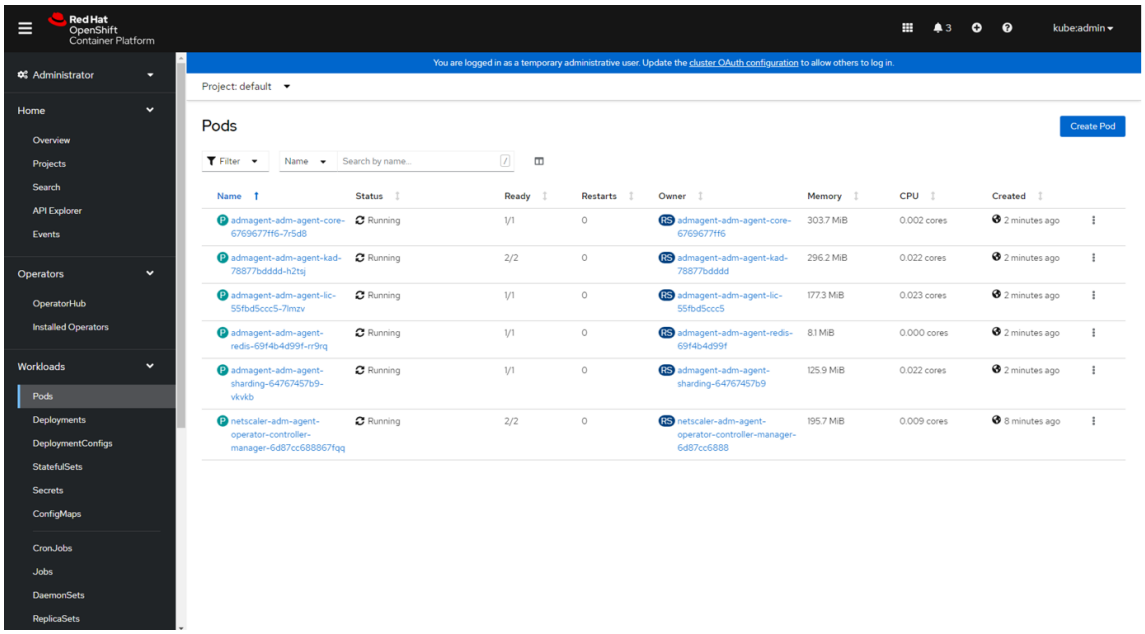


7. Seleccione la **vista YAML** para actualizar los parámetros y, a continuación, haga clic en **Crear**.

> **Nota:**
>
> Asegúrese de que solo haya una instancia de agente por clúster de OpenShift.

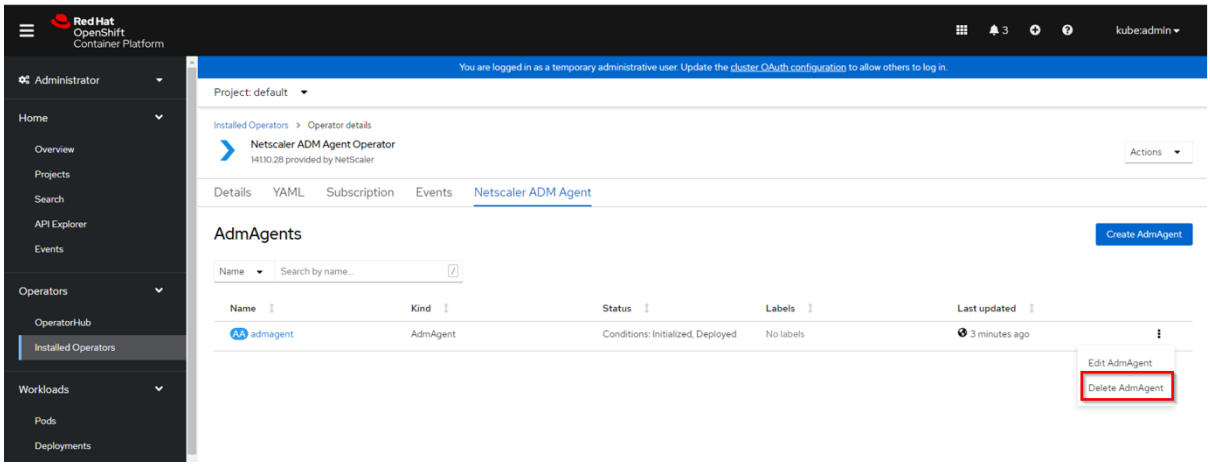


8. Vaya a Cargas de **trabajo > Pods** y asegúrese de que los pods del agente estén en funcionamiento.



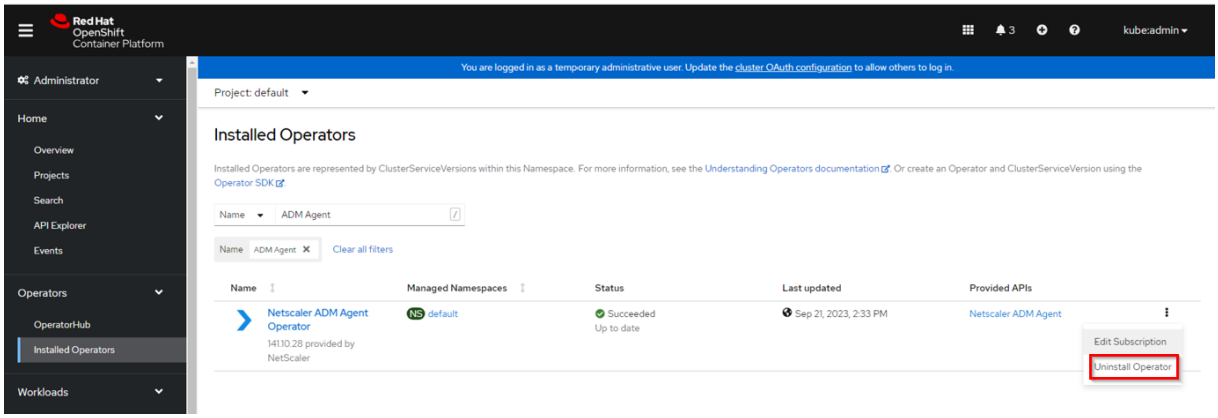
Eliminar una instancia de agente

Para eliminar la instancia del agente del clúster, vaya a **Operadores > Operadores instalados** . En la ficha **NetScaler ADM Agent** Operator, seleccione la instancia y **seleccione Eliminar** AdmAgent de la lista.



Desinstalar el operador del agente

Si desea desinstalar el pod de operadores del agente del clúster, vaya a Operadores **> Operadores instalados** y, a continuación, seleccione **Desinstalar operador** en la lista.



Instale un agente basado en contenedores mediante helm chart

January 26, 2024

Puede implementar un agente basado en contenedores para conectar NetScaler CPX con NetScaler Console para administrar y supervisar el NetScaler CPX. Para implementar un agente basado en contenedores, siga el procedimiento disponible en este documento.

> **Nota:**
>
> El agente basado en contenedores no se actualiza automáticamente (actualización permanente) de forma predeterminada.

Cómo obtener ayuda y asistencia técnica

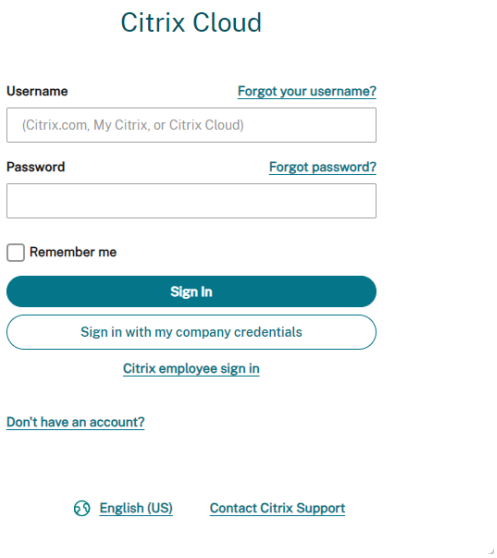
July 17, 2024

Como usuario de Citrix Cloud, a veces puede necesitar ayuda para garantizar un buen funcionamiento de nuestra infraestructura. En este tema se proporciona más información acerca de las diferentes opciones de ayuda y soporte y cómo acceder a ellas.

Crear una cuenta de Citrix Cloud

Si se produce un error al registrarse para obtener una cuenta de Citrix Cloud, póngase en contacto con el servicio de Asistencia al cliente de Citrix.

Inicie sesión en su cuenta



Si tiene problemas para iniciar sesión en su cuenta de Citrix Cloud:

- Compruebe que inicia sesión con la dirección de correo electrónico y la contraseña que suministró cuando se registró para obtener la cuenta.
- Citrix Cloud le solicita automáticamente que restablezca la contraseña antes de iniciar sesión si:
  - Hace tiempo que no inicia sesión en Citrix Cloud

  - Su contraseña no cumple los requisitos de Citrix Cloud

- Para obtener más información, consulte Cambiar la contraseña en este artículo.
- Si la empresa permite a los usuarios iniciar sesión en Citrix Cloud con sus credenciales de empresa en lugar de una cuenta de Citrix, haga clic en **Iniciar sesión** con mis credenciales de empresa e introduzca la URL de inicio de sesión de su empresa. Después, introduzca sus credenciales de empresa para acceder a la cuenta de Citrix Cloud de su empresa. Si no conoce la URL de inicio de sesión de su empresa, póngase en contacto con el administrador de su empresa para obtener ayuda.

Cambiar la contraseña

Si ha olvidado la contraseña de su cuenta de Citrix Cloud, haga clic en **¿Olvidó su nombre de usuario o contraseña?**y puede introducir la dirección de correo electrónico de su cuenta. Recibirá un correo electrónico para restablecer su contraseña. Si no recibe el correo electrónico de restablecimiento de contraseña o si necesita más ayuda, póngase en contacto con el servicio de atención al cliente de Citrix.

Para que la contraseña de su cuenta sea segura, puede que Citrix Cloud le pida que restablezca la contraseña cuando intente iniciar sesión. Este mensaje se produce si:

- Su contraseña no cumple los requisitos de complejidad de Citrix Cloud. Las contraseñas deben tener al menos 8 caracteres e incluir:
  - Al menos un número
  - Al menos una letra mayúscula
  - Al menos un símbolo: ! @ # $ % ^ * ? + = –
- Su contraseña incluye palabras del diccionario.
- Su contraseña aparece en una base de datos conocida de contraseñas desveladas.
- No ha iniciado sesión en Citrix Cloud en los últimos seis meses.

Cuando se le solicite, seleccione **Restablecer contraseña** para crear una nueva contraseña segura para su cuenta.

Foros de asistencia de Citrix Cloud

En los Foros de asistencia de Citrix Cloud puede obtener ayuda, publicar comentarios y sugerencias de mejoras, ver conversaciones de otros usuarios o iniciar nuevas conversaciones con sus propios temas.

Los miembros del personal de soporte de NetScaler realizan un seguimiento de estos foros y están listos para responder a sus preguntas. Otros miembros de la comunidad de Citrix Cloud también pueden ofrecer ayuda o unirse al debate.

No es necesario iniciar sesión para leer los temas del foro. Sin embargo, debe iniciar sesión para publicar un tema o responder en un tema. Para iniciar sesión, use sus credenciales existentes de cuenta de Citrix o use la dirección de correo electrónico y la contraseña que suministró al crear la cuenta de Citrix Cloud. Para crear una cuenta de Citrix, vaya a Crear o solicitar una cuenta.

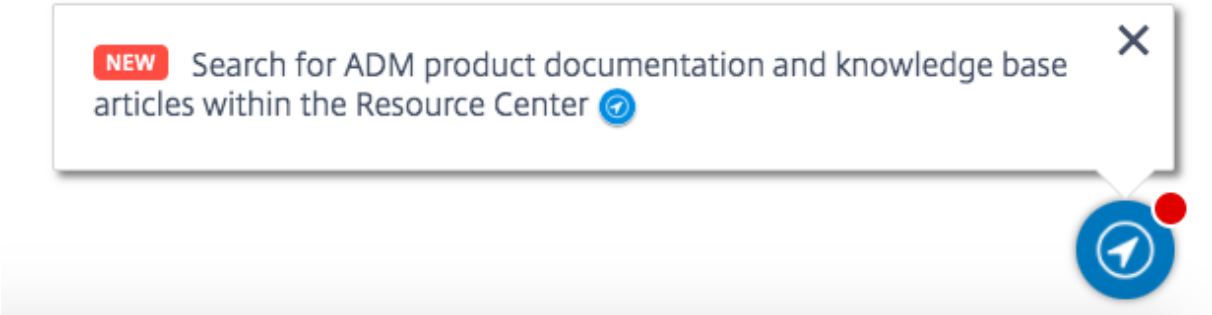
Artículos y documentación de asistencia

NetScaler proporciona una gran cantidad de contenido de productos y soporte para ayudarlo a aprovechar Citrix Cloud al máximo y resolver muchos problemas que pueda experimentar con los productos de NetScaler.

Centro de recursos de Citrix Cloud

El Centro de recursos de Citrix Cloud proporciona varios recursos para ayudarlo a comenzar a utilizar los servicios de Citrix Cloud, obtener más información sobre las funciones y resolver problemas. Los recursos que aparecen se aplican a la función o servicio de Citrix Cloud con el que está trabajando actualmente. Por ejemplo, si está en la consola de administración de servicios de Virtual Apps and Desktops, el Centro de recursos le muestra los siguientes recursos.

Acceda al Centro de recursos en cualquier momento haciendo clic en el icono de la brújula azul en la parte inferior derecha de la consola de Citrix Cloud.



- **Introducción**: Proporciona un breve tutorial guiado de las tareas clave específicas del servicio con el que está trabajando actualmente. También encontrará enlaces a recursos de formación e incorporación que le ayudarán a obtener más información sobre las capacidades del servicio y a preparar a sus usuarios finales para el éxito.

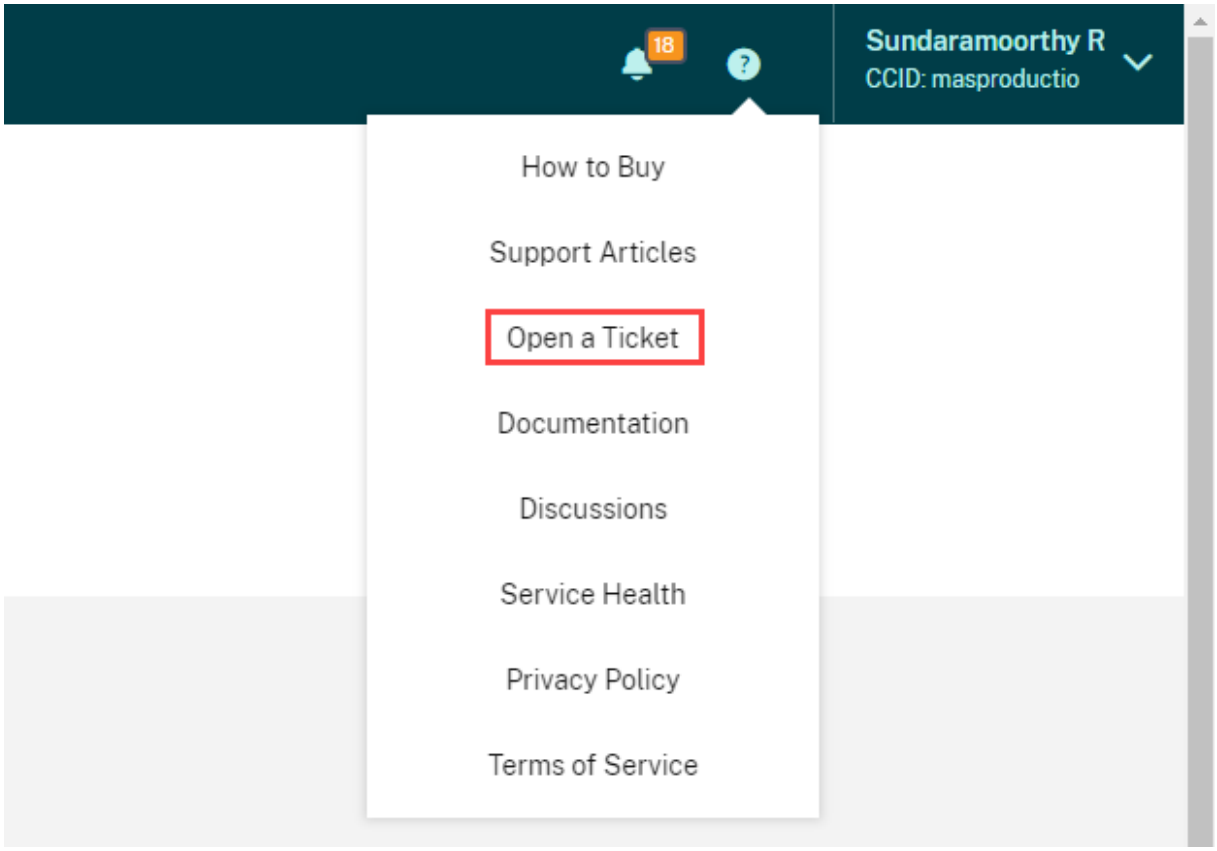
- **Anuncios**: Proporciona notificaciones de funciones recién publicadas y enlaces a comunicaciones esenciales de Citrix. Haga clic en una notificación de función para recibir un breve recorrido guiado de la función.
- **Búsqueda de artículos**: Proporciona una lista con artículos sobre documentación del producto y de Knowledge Center para tareas comunes, donde podrá encontrar otros artículos sin necesidad de salir de Citrix Cloud. Introduzca una consulta en el cuadro de **procedimientos** para obtener una lista filtrada de artículos basados en el servicio con el que está trabajando. En general, los artículos de asistencia aparecen en primer lugar en la lista, seguidos de los artículos de documentación del producto.

Citrix Tech Zone

Citrix Tech Zone contiene una gran cantidad de información para ayudarlo a obtener más información sobre Citrix Cloud y otros productos de NetScaler. Aquí encontrará arquitecturas de referencia, diagramas, vídeos y documentos técnicos que proporcionan información para diseñar, crear e implementar tecnologías de Citrix.

Asistencia técnica

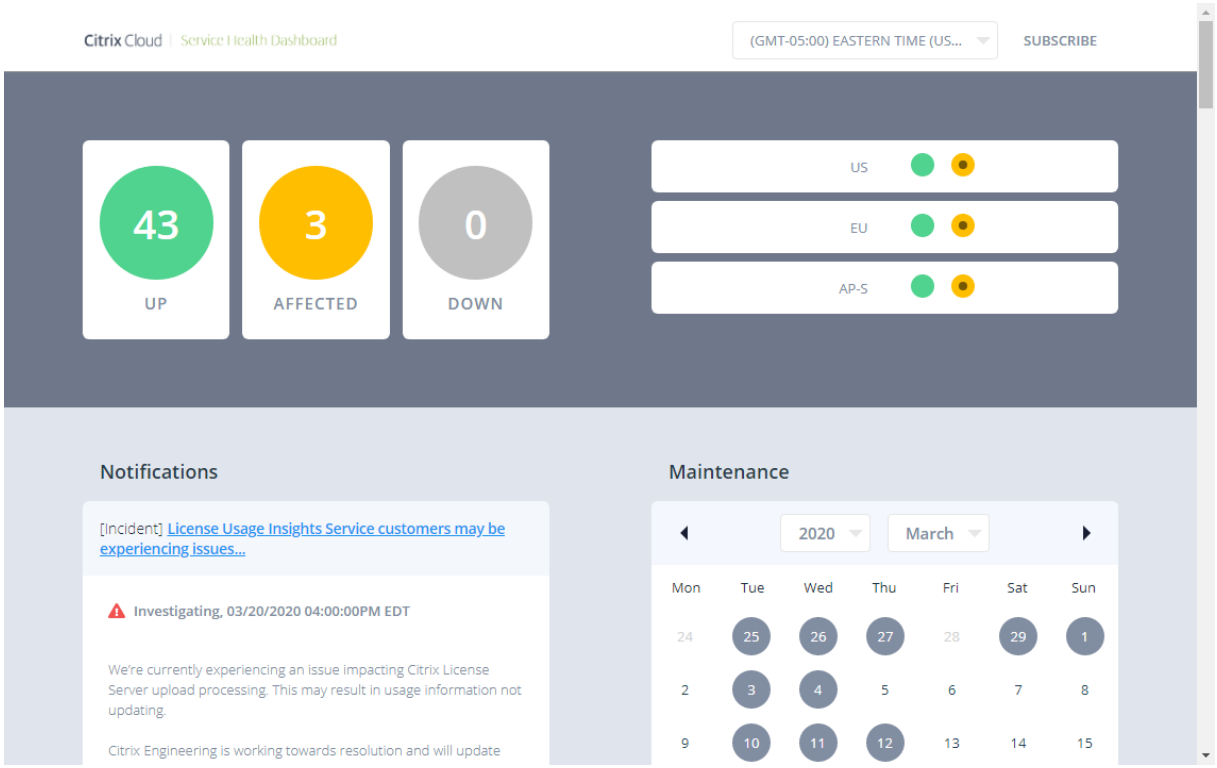
Si tiene un problema que requiere asistencia técnica, haga clic en el icono **Comentarios y asistencia** situado cerca de la parte superior derecha de la pantalla y, a continuación, seleccione **Abrir un tíquet**.



Haga clic en **Ir a My Support** y, a continuación, en **My Support** para abrir un tíquet a través del portal My Support. También puede utilizar el portal My Support para hacer un seguimiento de sus tíquets existentes y obtener información sobre sus suscripciones.

Panel de estado del servicio

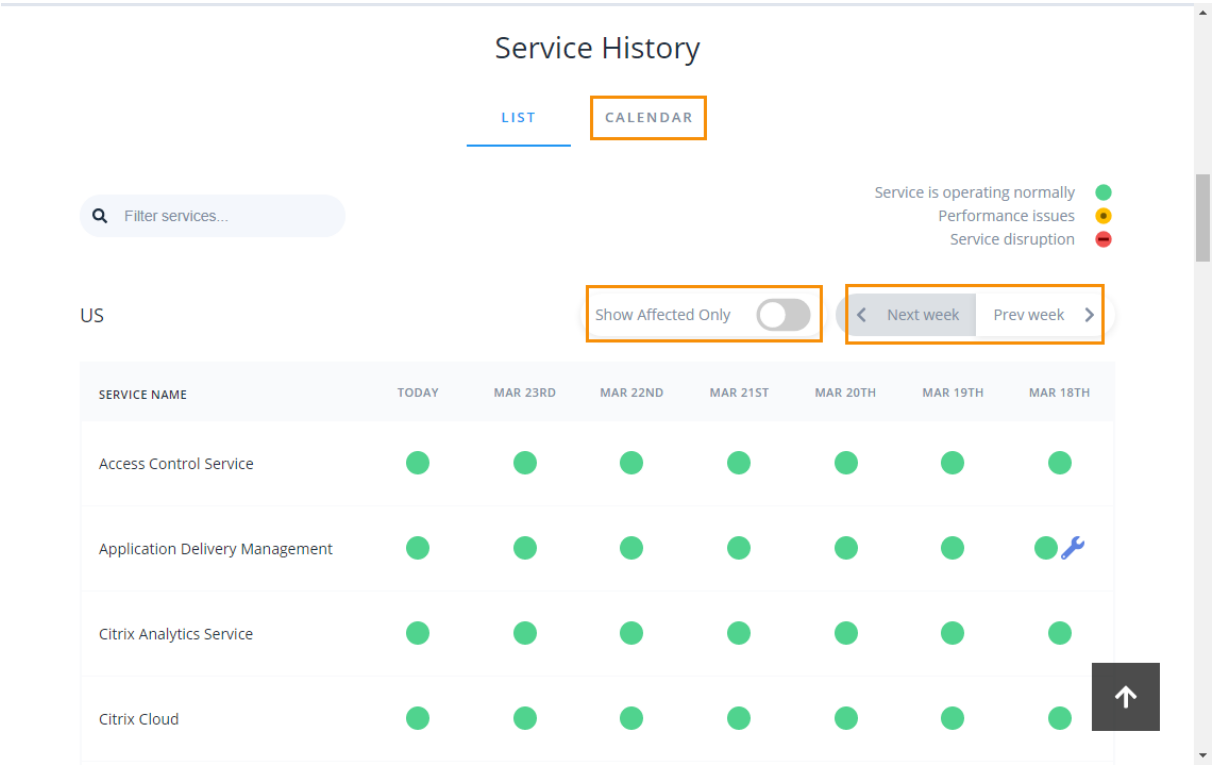
El panel de estado del servicio Citrix Cloud proporciona una descripción general de la disponibilidad en tiempo real de la plataforma y los servicios de Citrix Cloud en cada región geográfica. Si tiene algún problema con Citrix Cloud, consulte el panel de estado del servicio para comprobar que Citrix Cloud o algunos servicios específicos funcionan con normalidad.



Utilice el panel para obtener más información sobre las siguientes condiciones:

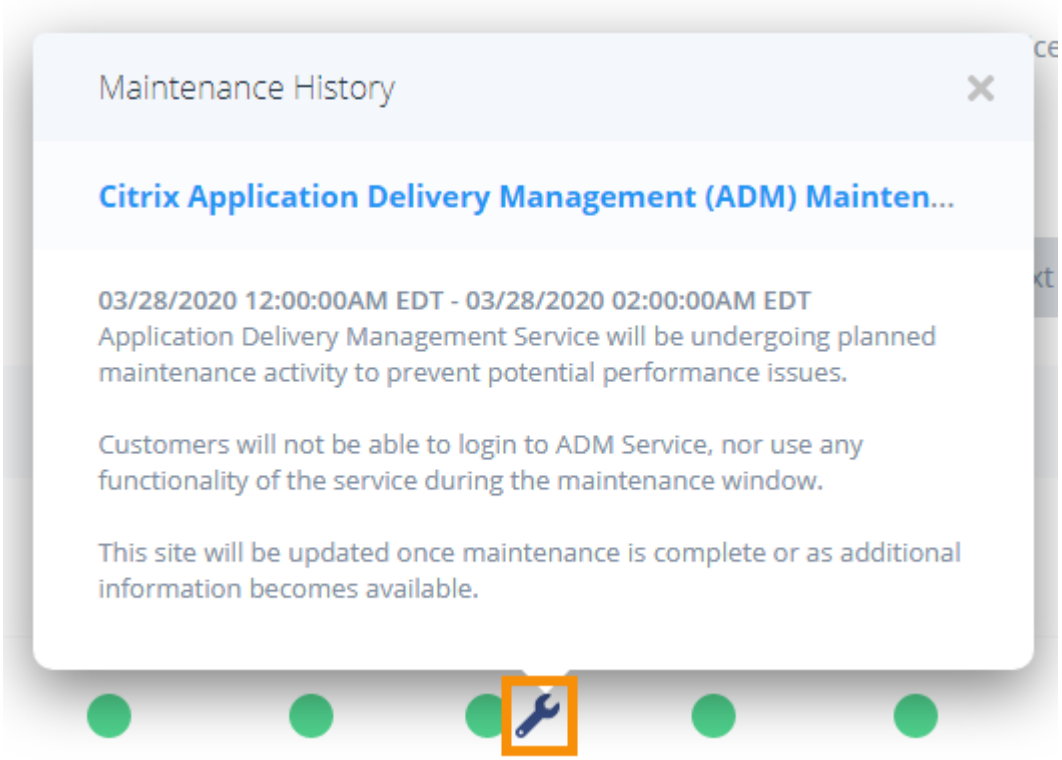
- El estado de disponibilidad actual de todos los servicios de Citrix Cloud, agrupados por región geográfica
- El historial de estado del servicio de cada servicio de los últimos siete días (predeterminado) o de los incrementos de siete días anteriores
- Períodos de mantenimiento para servicios específicos

De forma predeterminada, el estado del servicio se muestra como una lista, pero también puede mostrar el estado en una vista de calendario. Seleccione **Siguiente** o **Anterior** para recorrer el historial de estado del servicio en incrementos de siete días. También puede filtrar la lista para mostrar solo los servicios afectados.

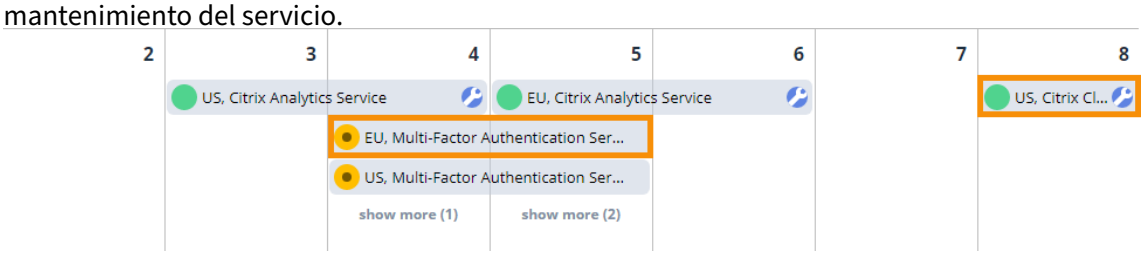


Para ver información más detallada sobre un incidente con relación a un servicio afectado:

- En la vista de lista, haga clic en el icono situado junto al indicador de servicio para ver información más detallada sobre el incidente de estado del servicio.

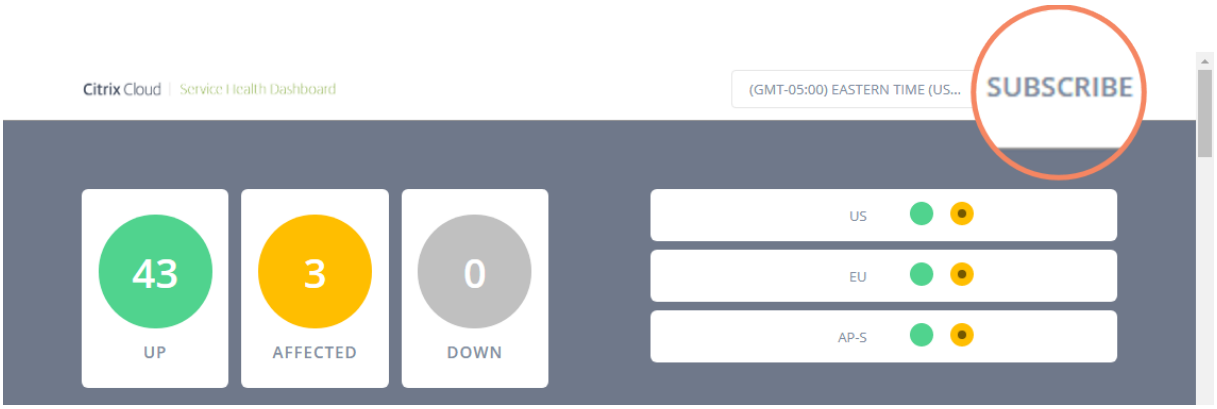


- En la vista de calendario, haga clic en la entrada de servicio para ver el estado del incidente de mantenimiento del servicio.

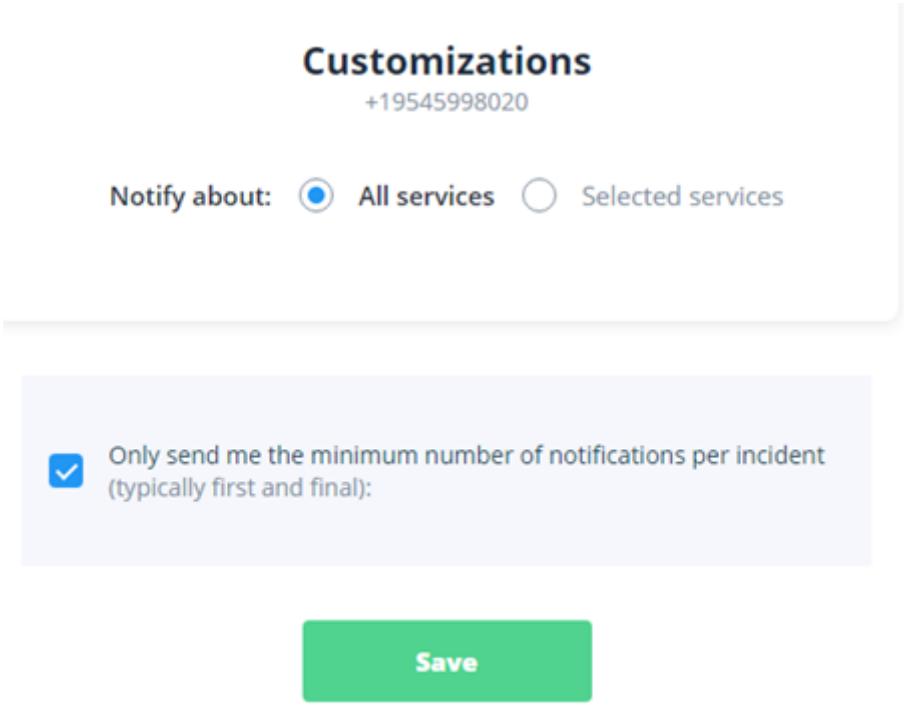


Suscripciones a servicios de salud

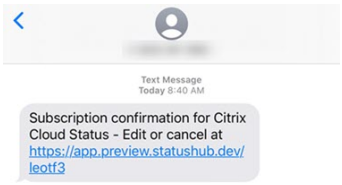
Para recibir notificaciones sobre el estado del servicio, haga clic en **Suscribirse** en la esquina superior derecha del panel y seleccione el método de notificación que desee utilizar.

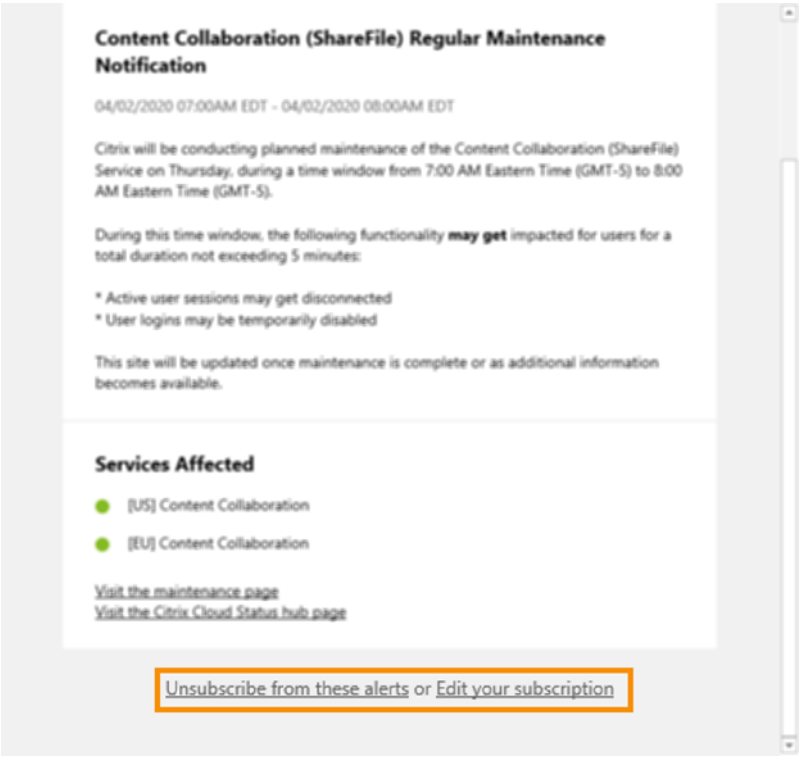


Puede suscribirse a las notificaciones de todos los servicios o solo de los servicios que seleccione. De forma predeterminada, recibes todas las notificaciones de un incidente de estado del servicio. Para limitar la frecuencia de las notificaciones durante un incidente, puede elegir recibir solo la primera y la última notificación.



Según el método de suscripción, se incluyen enlaces para cancelar la suscripción y cambiar sus preferencias en el mensaje de confirmación de la suscripción que recibes (por ejemplo, cuando se suscribe a las notificaciones telefónicas) o en cada mensaje de notificación (por ejemplo, cuando se suscribe a las notificaciones por correo electrónico).





Para cancelar la suscripción o cambiar sus preferencias de suscripción:

1. Busque una notificación existente y seleccione el enlace para cancelar la suscripción o cambiar sus preferencias de notificación.
2. Si cancelas la suscripción, selecciona **Cancelar suscripción** y, a continuación, selecciona el método de notificación que deseas cancelar. Para suscribirte desde todos los métodos de notificación, selecciona **Eliminar todas las suscripciones**.
3. Si cambia las preferencias, seleccione el método de notificación, realice los cambios apropiados en los servicios y notificaciones mínimas de incidentes y, a continuación, seleccione **Guardar**.

Incorporación sencilla de instancias de NetScaler mediante Console Advisory Connect

January 26, 2024

A medida que crece su infraestructura híbrida multinube (HMC), los desafíos para administrar, monitorear, analizar y solucionar problemas de las instancias de NetScaler se multiplican. Un controlador centralizado que proporciona visibilidad de toda su infraestructura y todas las aplicaciones que se ejecutan en ella se convierte en la necesidad de cada hora.

En el mundo actual, la incorporación de las instancias a un controlador central debe realizarse de

forma rápida, sencilla y sencilla. Teniendo en cuenta esta necesidad, NetScaler Console lanza un nuevo flujo de trabajo de incorporación, que le proporciona una forma más rápida de obtener una visibilidad completa de su implementación de HMC.

Descripción general: componentes del flujo de trabajo de incorporación de NetScaler Console

Los componentes básicos de este flujo de trabajo son dos componentes del lado del ADC: NetScaler service connect y Call Home.

- **Console Advisory Connect**: es una nueva función de NetScaler que ayuda a integrar sin problemas las instancias de NetScaler en NetScaler Console. Esta función permite que la instancia de NetScaler se conecte automáticamente con NetScaler Console y enviar datos del sistema, de uso y de telemetría a NetScaler Console. Basándose en estos datos, la consola de NetScaler le ofrece información y recomendaciones sobre su infraestructura de NetScaler. Como la identificación rápida de problemas de rendimiento, uso elevado de recursos y errores críticos.

  Console Advisory Connect está disponible en las siguientes versiones de NetScaler:

  - NetScaler MPX y VPX imagen versión 12.1 57.18 y posteriores y 13.0 61.48 y posteriores. Para obtener más información, consulte Introducción a NetScaler Console connect para dispositivos NetScaler .
  - Imagen de la versión 12.1 58.14 y posterior de NetScaler SDX y 13.0 61.48 y posteriores. Para obtener más información, consulte Introducción a NetScaler Console connect para dispositivos NetScaler SDX.

- **Call Home**: es una característica existente en ADC, que supervisa periódicamente las instancias y carga automáticamente los datos al servidor de soporte técnico de Citrix. Para obtener más información, consulta Call Home. Los datos recopilados por Call Home también se envían a NetScaler Console para permitir este nuevo flujo de trabajo.

Todas las instancias de NetScaler con conectividad a Internet o Call Home, o las instancias habilitadas con NetScaler Console connect, están conectadas a NetScaler Console. NetScaler Console comienza a recopilar métricas relevantes de estas instancias de NetScaler a través de la ruta Call Home, la ruta de conexión de NetScaler Console o ambas. Para obtener más información, consulte Gobernanza de datos para instancias MPX y VPX y Gobernanza de datos para instancias SDX.

Con estos datos, NetScaler Console crea un inventario de instancias de NetScaler para cada cliente (ID de organización único), que muestra una lista consolidada de sus instancias de NetScaler. NetScaler Console también usa estos datos para generar información sobre sus instancias de NetScaler y Gateway, lo que proporciona información significativa sobre sus implementaciones de HMC, identifica

problemas y recomienda acciones para mitigarlos. Antes de poder mitigar los problemas, debe incorporar las Instancias de NetScaler a NetScaler Console.

Puede marcar **Seleccionar instancias de NetScaler y Gateway para** incorporarlas y seleccionar las instancias de NetScaler que desea incorporar a NetScaler Console. Después de empezar, se le guiará al proceso de incorporación.

El proceso de incorporación automática utiliza Console Advisory Connect, lo que hace que la experiencia sea automática, fluida y rápida. Para las instancias de NetScaler en versiones que no admiten Console Advisory Connect ni la incorporación automática, NetScaler Console proporciona la incorporación basada en scripts, que es un proceso semiautomatizado.

> **Notas**
>
> - La incorporación automática y basada en scripts utiliza un agente integrado. Sin embargo, este flujo de trabajo también ofrece la flexibilidad de utilizar un agente externo para la incorporación. Puede utilizar la incorporación basada en agentes externos si desea utilizar las licencias agrupadas o la suite de análisis completa de NetScaler Console. O si quiere usar licencias agrupadas y el conjunto completo de análisis. El agente integrado solo admite administración y supervisión.
> - Las métricas recopiladas por Console Advisory Connect se envían directamente al punto final del servicio de NetScaler Console. Incluso si el NetScaler es un NetScaler administrado o descubierto en NetScaler Console y se ha configurado un agente externo para ese ADC, las métricas se envían directamente desde NetScaler al punto final del servicio de NetScaler Console y no se envían a través del agente externo.

Un recorrido rápido por la incorporación

Su primer punto de contacto en el viaje de incorporación es un correo electrónico iniciado por el producto. He aquí un recorrido rápido por el proceso de incorporación:

1. Un correo electrónico **iniciado por el producto NetScaler**: recibirá un correo electrónico de NetScaler Console en el que se muestran algunos datos clave sobre su infraestructura de NetScaler y se le invita a empezar a utilizar NetScaler Console. Haga clic en **Onboard to ADM Service** en el correo electrónico. Aparece la página **Citrix Cloud**.
2. En la página de inicio de sesión de **Citrix Cloud** :
    - Si ya es cliente de Citrix Cloud, inicie sesión en Citrix Cloud con sus credenciales de **Citrix.com**, **My Citrix**o **Citrix Cloud**.
    - Si aún no es cliente de Citrix Cloud, regístrese en Citrix Cloud. Para obtener más información, consulte Registrarse en Citrix Cloud.

> **Notas**
>
> - Si forma parte de varios identificadores de organización y uno de ellos está en Citrix Cloud, inicie sesión con las credenciales existentes. A continuación, complete el flujo de trabajo de incorporación para el nuevo ID de organización.
> - Puedes activar o desactivar las notificaciones por correo electrónico que recibes como parte del flujo de trabajo de incorporación sencillo basado en Console Advisory Connect. Para obtener más información, consulte Configuración del correo electrónico.

3. **Página**de bienvenida de NetScaler Console : obtendrá una descripción general de NetScaler Console y sus ventajas.
4. **Información sobre sus instancias**de NetScaler y Gateway : obtendrá información detallada sobre su infraestructura general de NetScaler, incluidos consejos de seguridad (consejos sobre los CVE actuales de NetScaler), consejos de actualización (consejos basados en los plazos de EOM/EOL), métricas clave, tendencias y aspectos destacados de los problemas que afectan al rendimiento y el estado de NetScaler, y recomienda formas de mitigar los problemas.
5. **Seleccione las instancias de NetScaler y Gateway para incorporarlas**: obtendrá una vista consolidada de su inventario de NetScaler. Puede seleccionar las instancias de NetScaler que desea incorporar a NetScaler Console.
6. **Instancias de NetScaler integradas en NetScaler Console**: Basándose en las Instancias de NetScaler seleccionadas para la incorporación, NetScaler Console lo guía durante el proceso de incorporación. De forma predeterminada, se selecciona el agente integrado para la incorporación automática.
7. **Panel**de interfaz gráfica de usuario de NetScaler Console : una vez finalizada la integración, se lo guiará al panel de instancias de NetScaler Console.

Para obtener más información sobre cada uno de estos métodos de incorporación, consulte Instancias de NetScaler integradas con NetScaler Console connect .

Instancias de NetScaler integradas mediante Console Advisory Connect

January 26, 2024

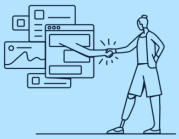
Este documento proporciona una guía paso a paso que le ayudará a empezar a usar NetScaler Console. Antes de empezar, lea cómo NetScaler Console lanza un nuevo flujo de trabajo de incorporación, que le proporciona una forma más rápida de obtener una visibilidad completa de su implementación de múltiples nubes híbridas (HMC). Vea la incorporación sencilla de instancias de NetScaler mediante NetScaler Console connect .

Paso 1: Empezar

Recibirá un correo electrónico de la consola de NetScaler en el que se muestran algunos datos clave sobre su infraestructura de NetScaler y se le invita a empezar a utilizar la consola de NetScaler.

citrix

Onboard to Citrix ADM Service for Security Advisory



Hello [redacted] Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs.

These new features can identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you onboard to Citrix ADM service. You can get started with Citrix ADM Service Express account at no additional cost.

Insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM Service Connect.

ADC instances by platforms

30	20	5	5
Total	VPX	SDX	MPX

Security Advisory

5 ADC instances are on versions with known common vulnerability exposures (CVEs).
This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc

Upgrade Advisory

2 ADC instances are on versions that have reached end of life in last 365 days or earlier.

1 ADC instance is on a version that will reach end of life in next 365 days.

3 ADC instances are on versions that have reached end of maintenance in last 365 days or earlier.

4 ADC instances are on versions that will reach end of maintenance in next 365 days.

2 ADC instances are on older builds and releases.

Recent events

4 ADC instances encountered SSL card failure.
2 ADC instances encountered hard disk failure.

Resource utilization

2 ADC instances CPU usage exceeded 50%
3 ADC instances memory usage exceeded 50%

ADC deployment

5 ADC instances are not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service, today.**

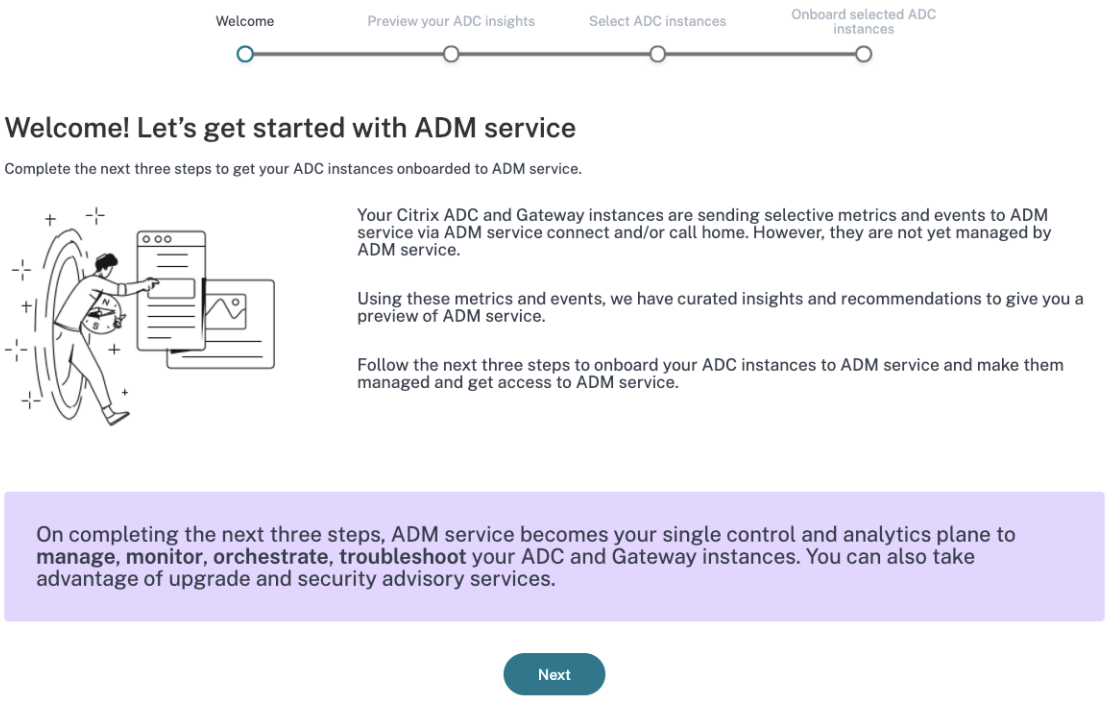
As a first step, you will need to create Citrix Cloud account by clicking on the button below.

Onboard to ADM Service

1. En el correo electrónico, haga clic en **Onboard to ADM Service**. Aparece la página **Citrix Cloud**.
2. En la página de inicio de sesión de **Citrix Cloud** :
   - Si ya es cliente de Citrix Cloud, inicie sesión en Citrix Cloud con sus credenciales de **Citrix.com**, **My Citrix**o **Citrix Cloud**.
   - Si aún no es cliente de Citrix Cloud, regístrese en Citrix Cloud. Para obtener más información, consulte Registrarse en Citrix Cloud.

   > **Notas**
   >
   > - Si forma parte de varios identificadores de organización y uno de ellos está en Citrix Cloud, inicie sesión con las credenciales existentes. A continuación, complete el flujo de trabajo de incorporación para el nuevo ID de organización.
   > - Puede habilitar o deshabilitar las notificaciones por correo electrónico que recibe como parte del flujo de trabajo de incorporación sencillo basado en Consolve Advisory Connect. Para obtener más información, consulte Configuración del correo electrónico.

3. En la página de inicio de NetScaler Console, dedique un momento a leer por qué está allí y las ventajas de usar NetScaler Console.



> **Nota**
>
> Las recomendaciones de seguridad incluidas en el correo electrónico se basan únicamente en el

> análisis de la versión compilada de NetScaler. Después de incorporar las instancias de NetScaler a NetScaler Console, podrá obtener información más concluyente y exhaustiva sobre los consejos de seguridad.

1. Haga clic en **Siguiente**. Se abre **la página Información sobre las instancias de NetScaler y Gateway** .

Los siguientes pasos actúan como un flujo de trabajo guiado para ofrecerle una vista previa de lo que NetScaler Console puede ofrecer y ayudarlo a integrar sus instancias de NetScaler en NetScaler Console sin problemas.

Paso 2: Información sobre sus instancias de NetScaler y Gateway

Esta página de información utiliza los datos recopilados a través de Call Home o NetScaler Console connect o de Call Home y NetScaler Console connect para proporcionar información sobre sus instancias de NetScaler. En esta página encontrará información sobre su infraestructura general de NetScaler, incluidos los consejos de seguridad (consejos sobre los CVE actuales de NetScaler), los consejos sobre actualizaciones (consejos basados en los plazos de EOM/EOL), las métricas clave y las tendencias, y destaca los problemas que afectan al rendimiento y el estado de NetScaler, y recomienda formas de mitigarlos. Estas ideas y recomendaciones son solo un pequeño adelanto de la gran cantidad de beneficios y valor agregado que ofrece NetScaler Console. Para obtener muchos más beneficios, información detallada y poder ejecutar las acciones recomendadas, debe incorporar las instancias de NetScaler a NetScaler Console.

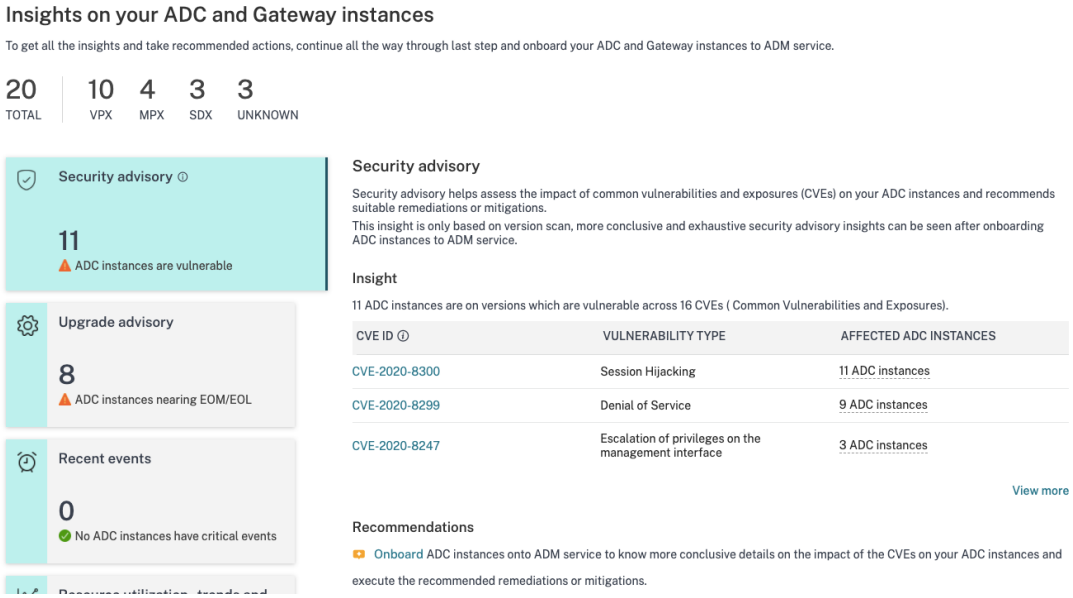
Los conocimientos y recomendaciones se clasifican en los siguientes tipos:

- **Asesoramiento**de seguridad : incorpore instancias de NetScaler para obtener los detalles del impacto del CVE en sus instancias de NetScaler y ejecutar las soluciones o mitigaciones recomendadas.
- **Asesoramiento**de actualización : incorpore instancias de NetScaler en NetScaler Console y actualice las instancias de NetScaler que hayan alcanzado o estén llegando a la EOM/EOL o que estén en versiones o compilaciones anteriores.
- **Eventos**recientes : incorpore instancias de NetScaler a NetScaler Console para supervisar más de 200 eventos con regularidad y crear reglas para recibir notificaciones por correo electrónico, PagerDuty, Slack y ServiceNow, y tome las medidas adecuadas.
- **Utilización de los recursos: tendencias y anomalías**: incorpore instancias de NetScaler en NetScaler Console para obtener una visión integral del estado de las instancias de NetScaler, los problemas de rendimiento y recomendaciones para mitigar esos problemas. También puede evaluar el uso previsto de CPU y memoria para sus instancias de NetScaler.
- **Guía**de implementación de NetScaler : incorpore instancias de NetScaler en NetScaler Console y configúrelas como un par de alta disponibilidad mediante trabajos de configuración en NetScaler Console.

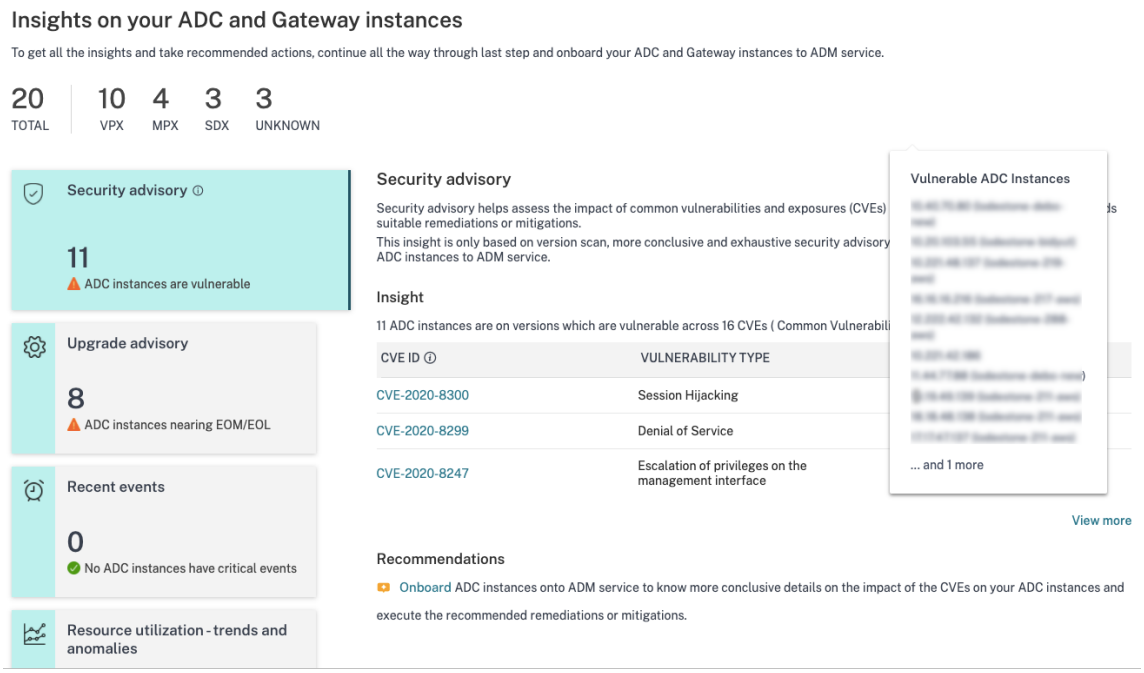
1. **Asesoramiento**de seguridad : el asesoramiento de seguridad de NetScaler Console lo alerta sobre las vulnerabilidades que ponen en riesgo sus instancias de NetScaler y recomienda mitigaciones y soluciones.

   > **Nota:**
   >
   > Las recomendaciones de seguridad incluidas en el correo electrónico de incorporación y el flujo de trabajo guiado se basan únicamente en el análisis de la versión compilada de NetScaler. Tras incorporar las instancias de NetScaler a NetScaler Console , podrá obtener información exhaustiva y concluyente sobre las recomendaciones de seguridad. **Ejemplo**: si un CVE necesita analizar tanto la versión como la configuración para evaluar la vulnerabilidad, el correo electrónico de incorporación y el flujo de trabajo guiado muestran los resultados en función del análisis de versiones. Por lo tanto, puede haber falsos positivos. Para obtener una evaluación más concluyente y precisa del impacto, incorpore NetScaler a NetScaler Console. Tras la incorporación, el aviso de seguridad de NetScaler Console muestra la evaluación de impacto, que es la evaluación de vulnerabilidad de NetScaler, basada en el escaneo de versiones y el escaneo de configuración.

   Puede comprobar el ID de CVE, el tipo de vulnerabilidad y las instancias de NetScaler afectadas. El vínculo CVE ID lleva al artículo del boletín de seguridad.

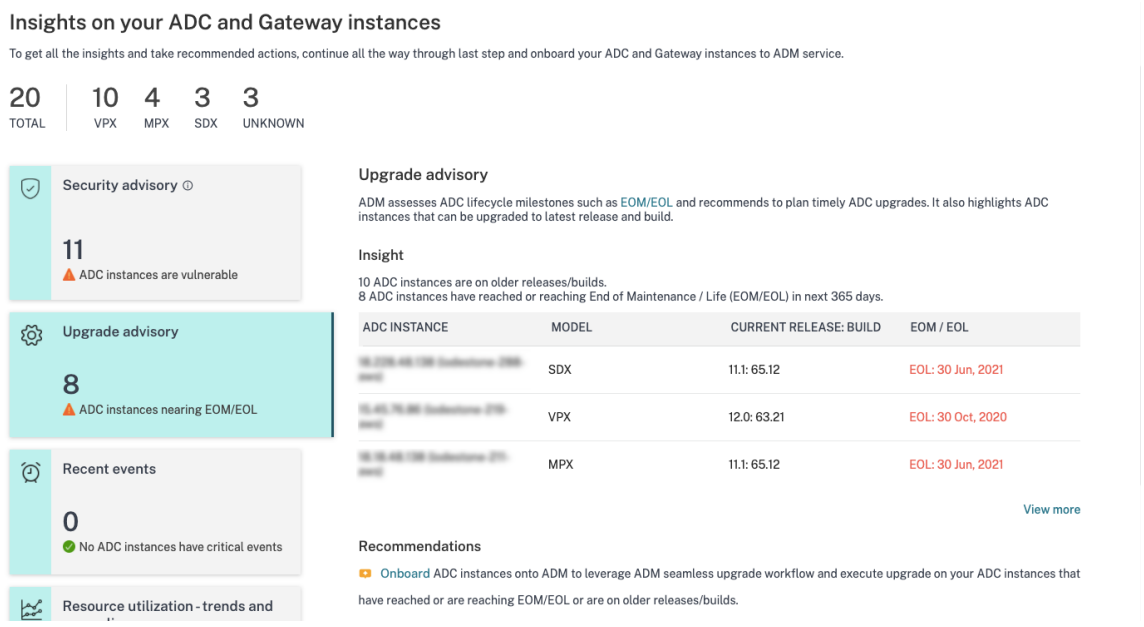
   La recomendación lo guía para que incorpore sus instancias de NetScaler a NetScaler Console para obtener más información sobre el impacto del CVE en sus instancias de NetScaler y ejecutar la mitigación o corrección recomendadas. Haga clic en las instancias de NetScaler afectadas para ver las direcciones IP de las instancias afectadas.



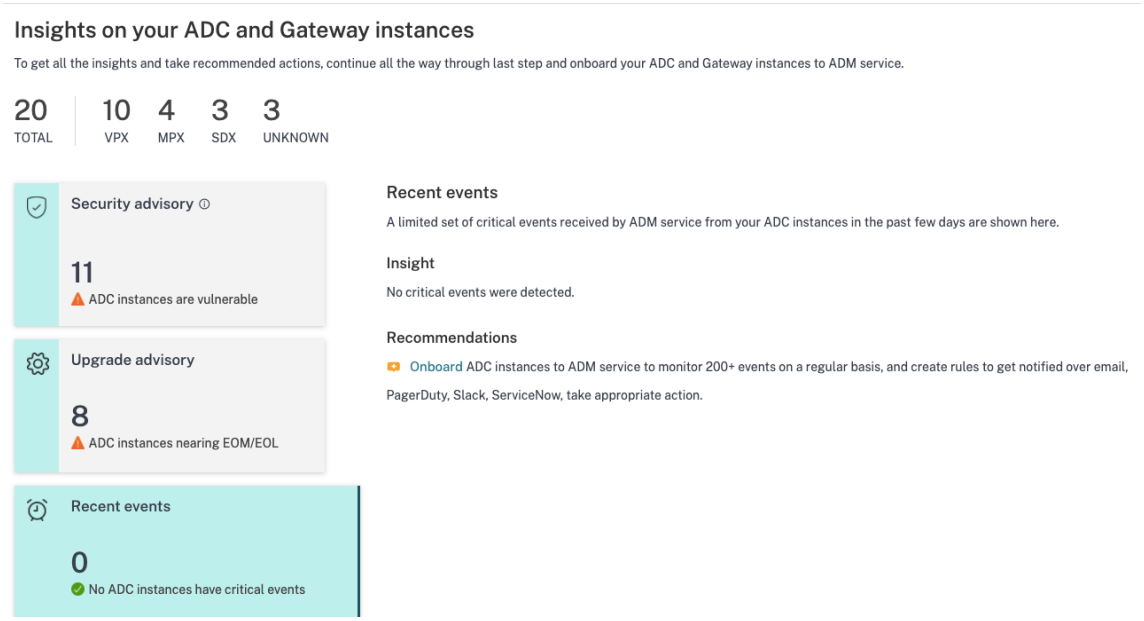
2. **Asesoramiento**de actualización : utilice este aviso para comprobar qué instancias de NetScaler se acercan al EOM/EOL o están en versiones anteriores.

   Basándose en esta información, NetScaler Console le recomienda planificar una actualización oportuna antes de la EOM/EOL o que se beneficie de las funciones y correcciones más recientes.

   Para realizar la actualización, debe incorporar las instancias de NetScaler a NetScaler Console.

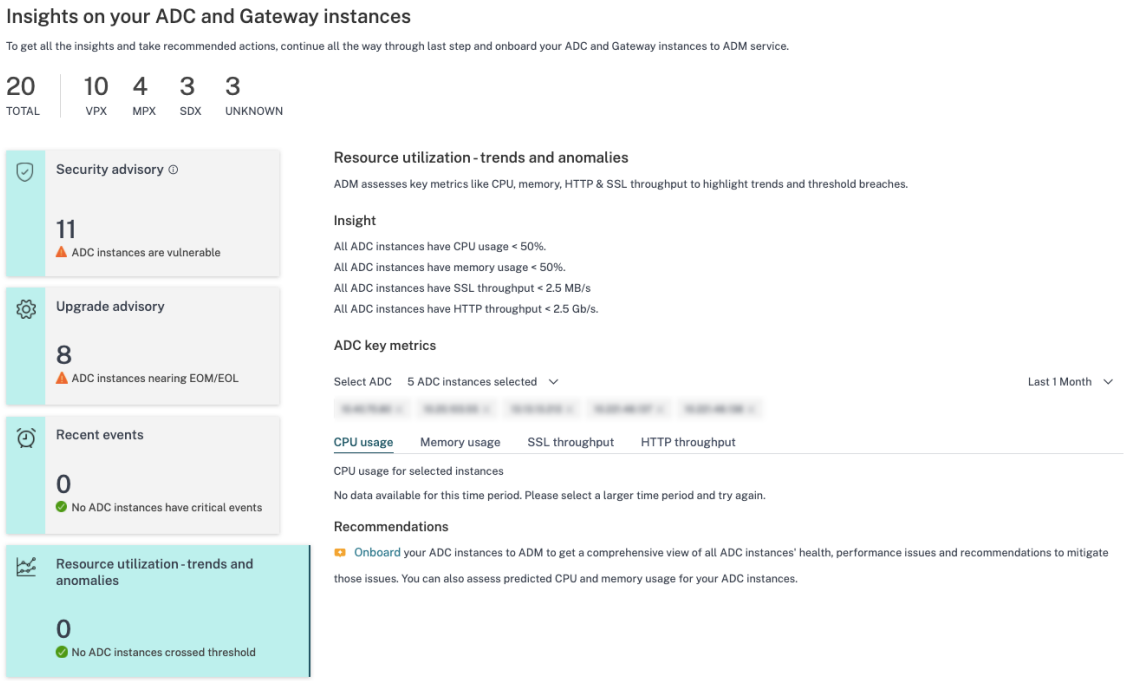


3. **Eventos**recientes : obtenga detalles de algunos errores críticos que se han producido en las instancias de NetScaler y una lista de las instancias de NetScaler en las que se han producido los errores.

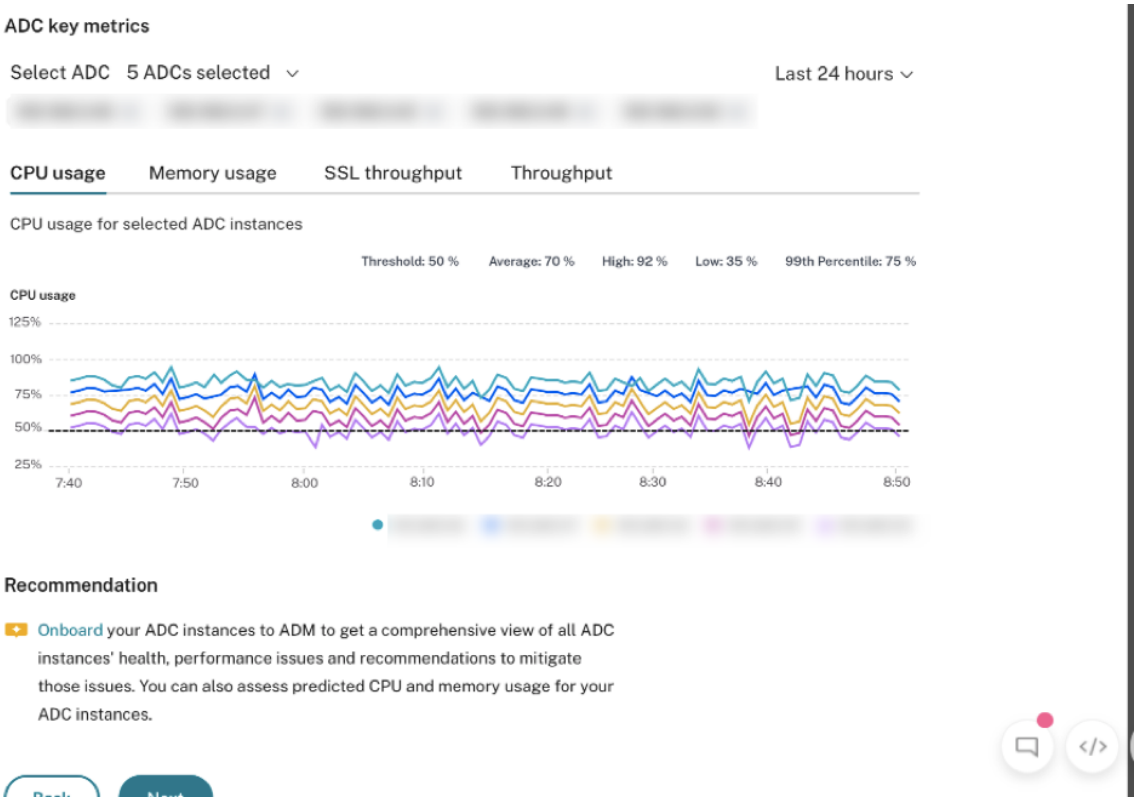


4. **Utilización de recursos: tendencias y anomalías**: Encuentre información sobre la alta utilización de recursos para CPU, memoria, rendimiento HTTP y rendimiento SSL. Para cada información, NetScaler Console sugiere una acción recomendada. Para tener más visibilidad de estas ideas y recomendaciones, debe incorporar sus instancias de NetScaler a NetScaler Console. Algunos beneficios después de la incorporación son:

    - CPU: prediga el uso de la CPU durante las próximas 24 horas en NetScaler Console.
    - Memoria: prediga el uso de la memoria durante las próximas 24 horas en NetScaler Console.
    - Rendimiento de SSL: vea la optimización de SSL en tiempo real con análisis de aplicaciones inteligentes en NetScaler Console.
    - Rendimiento HTTP: solucione los problemas de capacidad de rendimiento de NetScaler con Infrastructure Analytics.

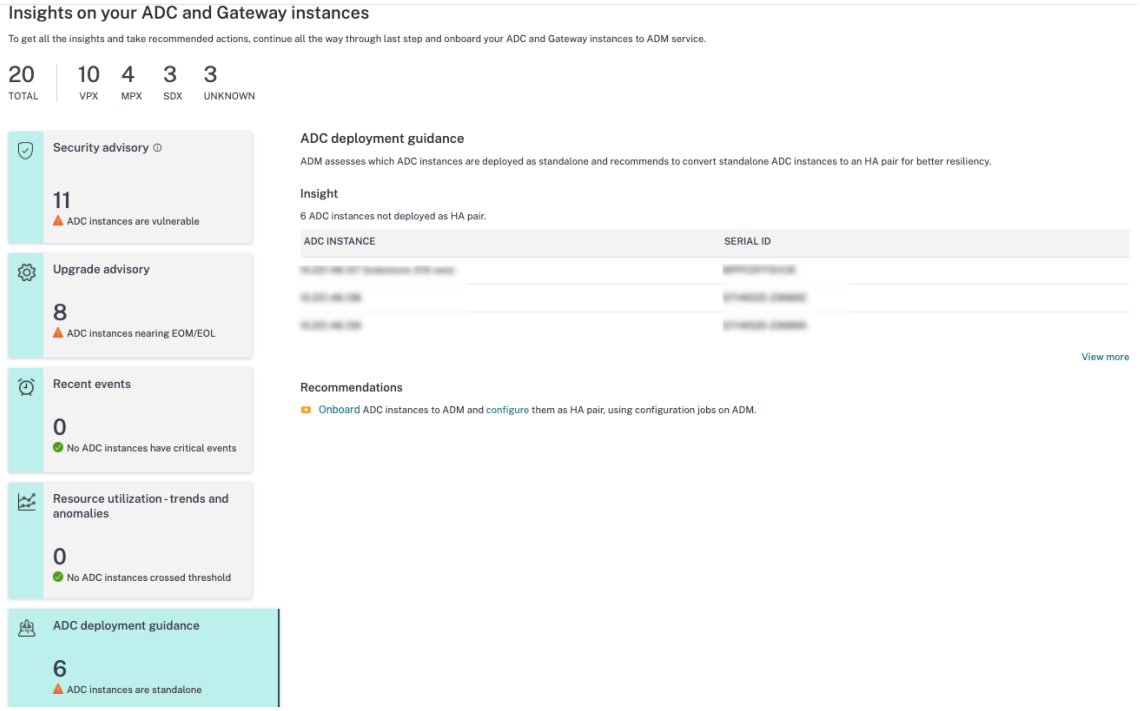


- **Métricas clave**: obtenga detalles de métricas clave relacionadas con la CPU, la memoria, el rendimiento HTTP, el rendimiento SSL y descubra tendencias anómalas en las métricas.



5. **Guía**de implementación : obtenga visibilidad de las instancias de NetScaler que se implementan como un NetScaler independiente. NetScaler Console recomienda configurar estas instan-

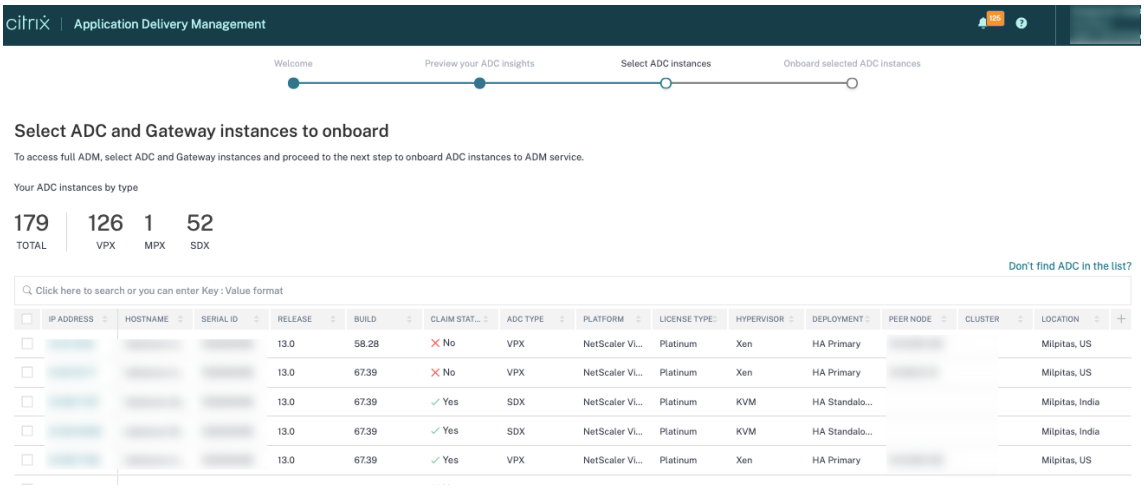
cias de NetScaler como un par de alta disponibilidad para mejorar la resiliencia. Esto requiere que incorpore las instancias de NetScaler a NetScaler Console y, a continuación, utilice los trabajos de mantenimiento para configurar las instancias como un par de alta disponibilidad.



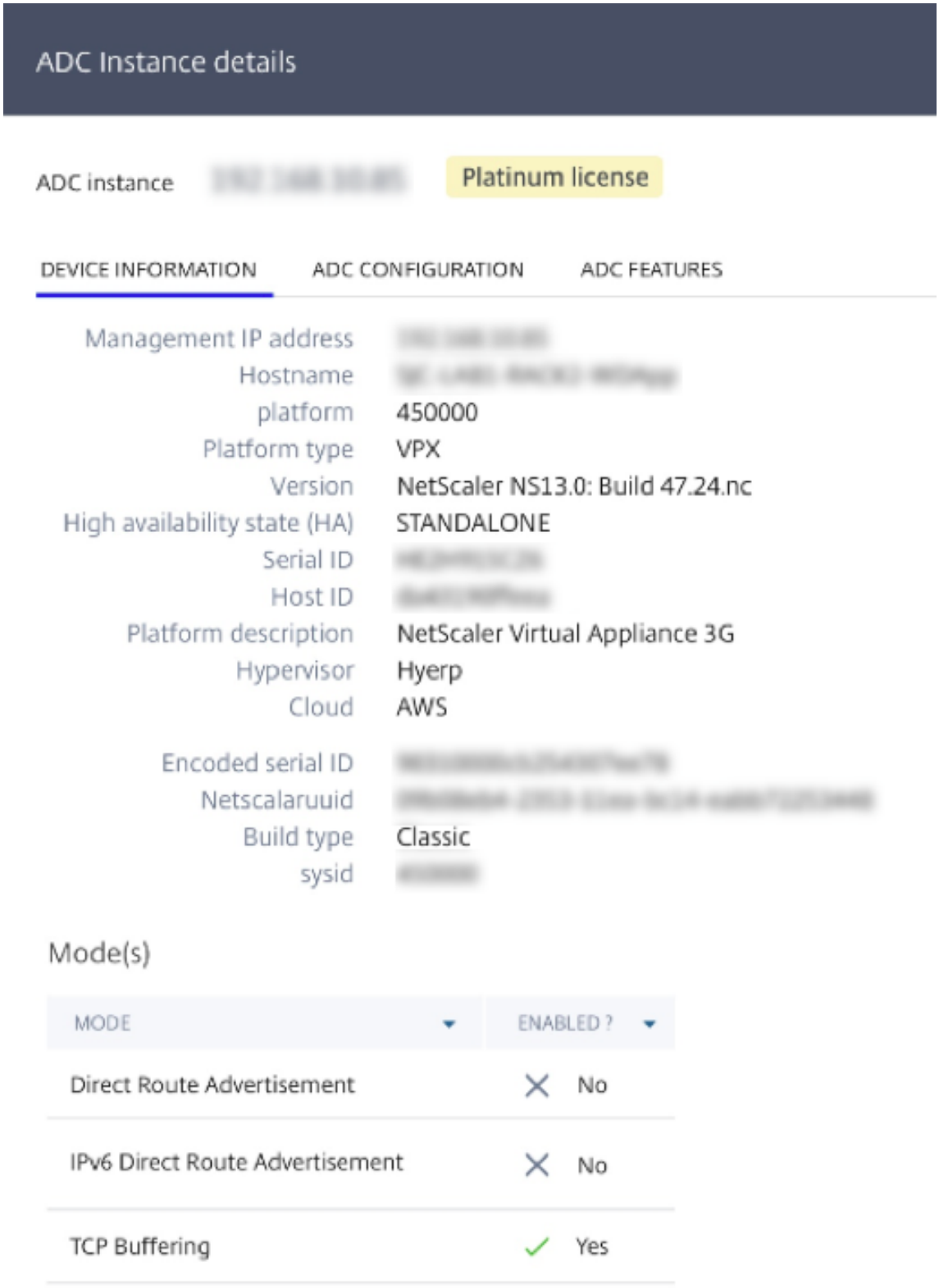
Paso 3: Seleccione las instancias de NetScaler y Gateway para incorporarlas

En esta página se muestran todas las instancias de NetScaler y Gateway de su entorno. Vea y seleccione las instancias de NetScaler y Gateway que desea incorporar a NetScaler Console y haga clic en **Siguiente**.

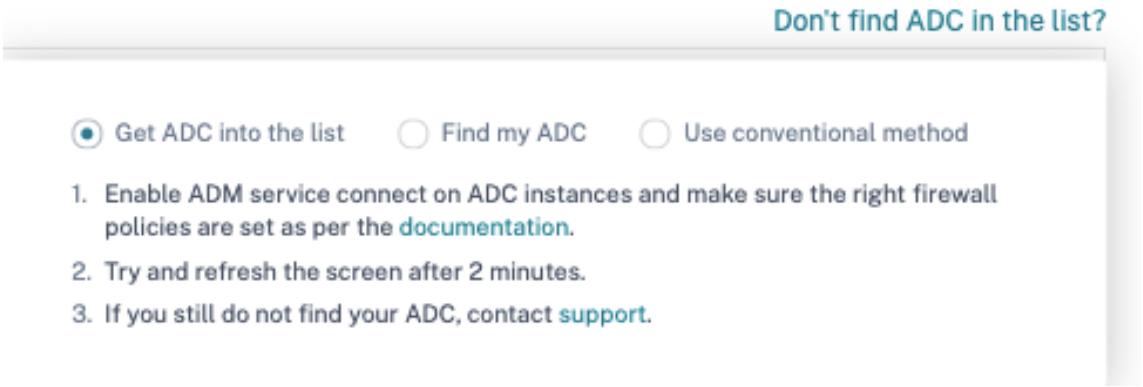
1. Vea y seleccione las instancias de NetScaler que desea incorporar a NetScaler Console.



Si necesita detalles sobre alguna instancia, como la información del dispositivo, la configuración de NetScaler, las funciones de NetScaler disponibles o la información de la licencia, haga clic en la dirección IP de la instancia de NetScaler.

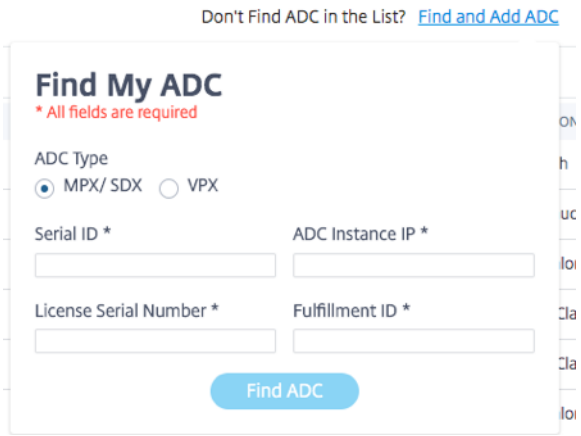


Si su instancia no aparece en la lista, utilice la opción No **encuentre NetScaler en la lista** de la esquina superior derecha.



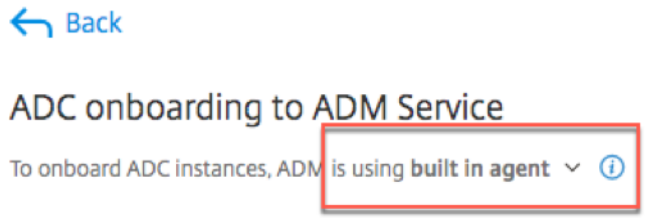
Puede proceder de tres maneras: siga los pasos que se indican en **Incluir NetScaler en la lista** o utilice la **opción Buscar mi NetScaler**. Si estos dos pasos no ayudan, haga clic en la opción **Usar método convencional** , que omite el flujo de trabajo y lo guía por la forma tradicional de incorporar instancias de NetScaler.

Para la **opción Find my NetScaler** , introduzca los detalles en los campos obligatorios (ID de serie, dirección IP de la instancia de NetScaler, número de serie de la licencia e ID de cumplimiento) y busque.



Paso 4: Incorporar instancias de NetScaler a NetScaler Console

Puede incorporarse a sus instancias utilizando el agente incorporado (opción predeterminada) o un agente externo.



Instancias de NetScaler integradas mediante un agente integrado

La incorporación automática y basada en scripts utiliza el agente integrado, que está configurado de forma predeterminada.

Incorporación automática : solose admite en las siguientes versiones de NetScaler:

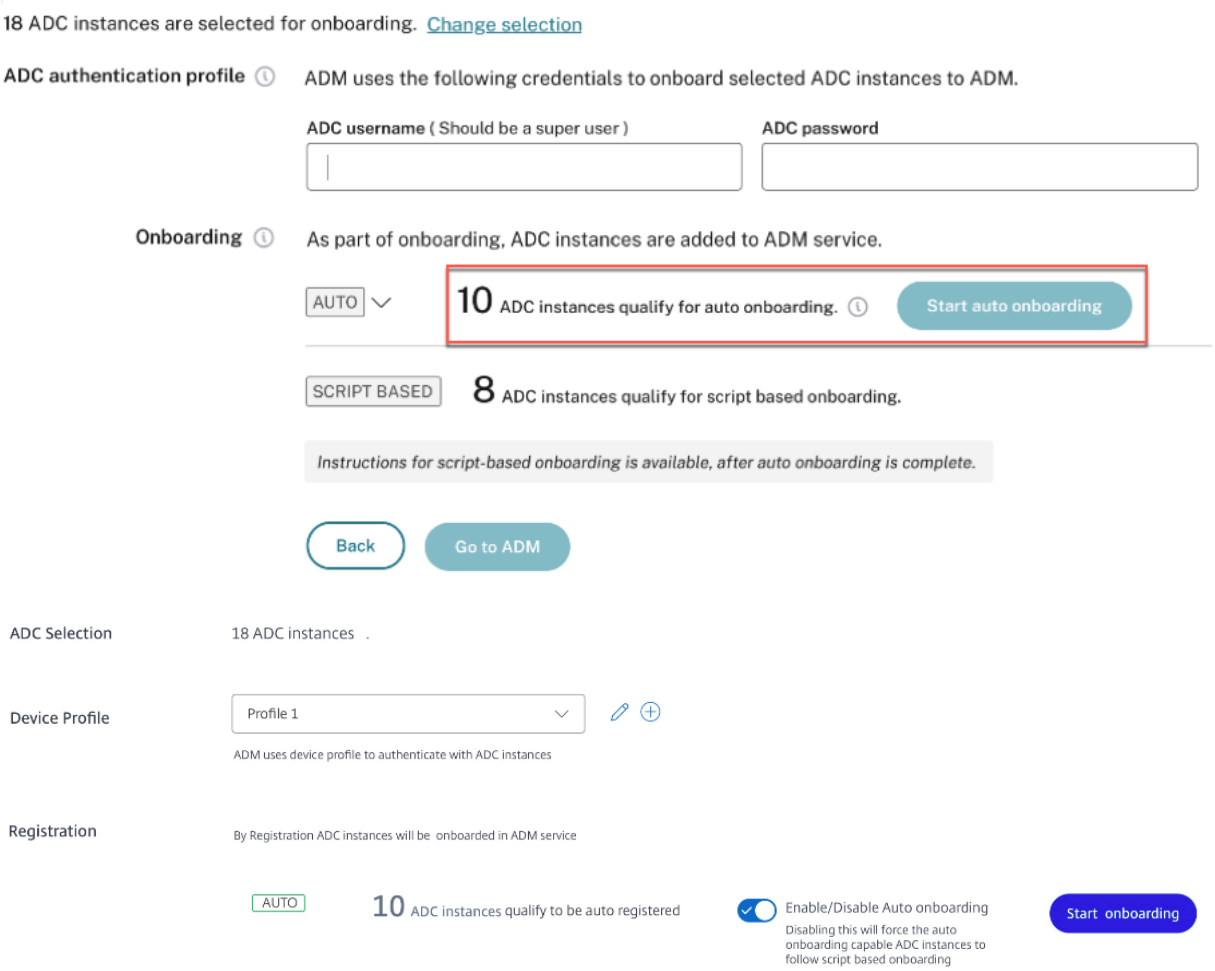
- NetScaler MPX y VPX imagen versión 12.1 57.18 y posteriores y 13.0 61.48 y posteriores
- Imagen de la versión de SDX 13.0 61.48 y posteriores y 12.1 58,14 y posteriores

Para seleccionar otra instancia de NetScaler, haga clic en **Cambiar selección**.

Del total de instancias de NetScaler seleccionadas, es posible que algunas cumplan los requisitos para la incorporación automática (según los criterios de versión mínimos). Puede ver las instancias que califican para la incorporación automática.

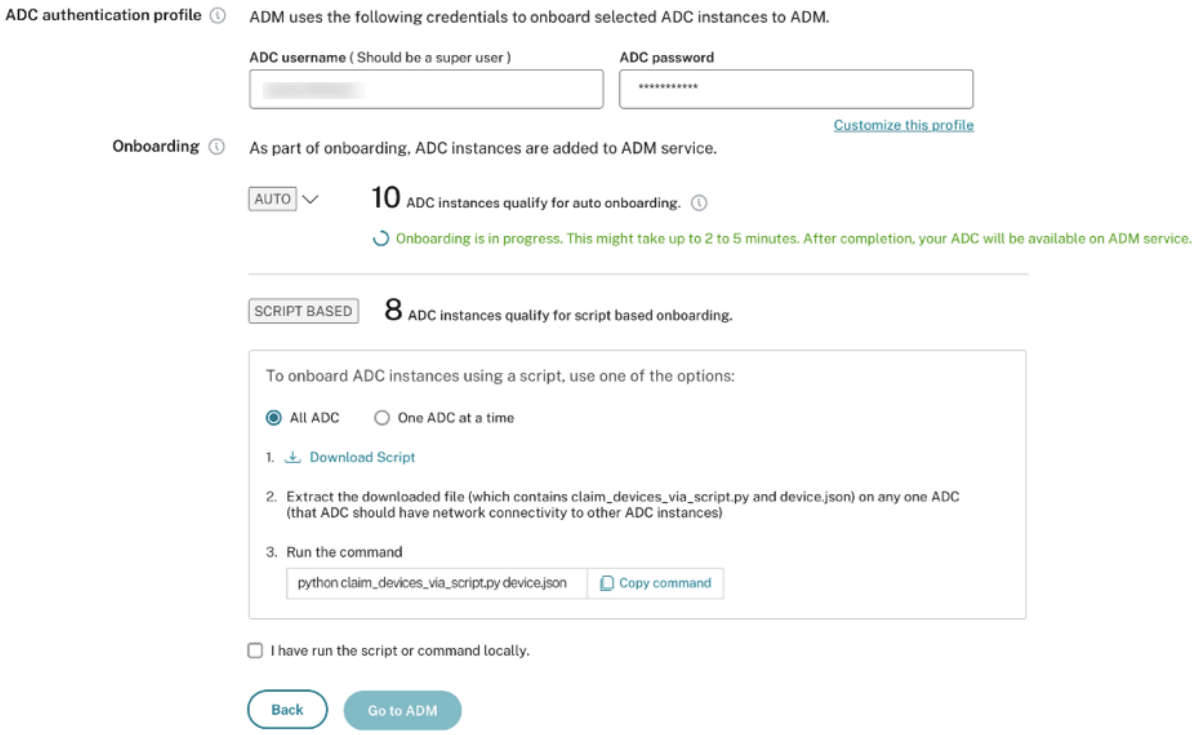
Puede realizar una prueba de incorporación para asegurarse de que la instancia de NetScaler esté lista para su incorporación. Haga clic en **Probar** para iniciar la prueba. Para obtener más información, consulte Probar la preparación para la incorporación de las instancias de NetScaler.

Si desea realizar la integración sin ejecutar la prueba, introduzca el nombre de usuario y la contraseña de NetScaler. Las credenciales deben ser credenciales de administrador de usuarios de NetScaler y NetScaler Console las usa para incorporar NetScaler. Haga clic en **Iniciar la incorporación automática** para incorporar las instancias de NetScaler en NetScaler Console.



> **Nota** después de especificar las credenciales de NetScaler y crear el perfil del dispositivo, la GUI de ADM no volverá a solicitar el nombre de usuario y la contraseña para cada instancia de NetScaler. Sin embargo, puede seleccionar el perfil en el menú desplegable **Perfil del dispositivo** para autenticar las instancias de NetScaler.

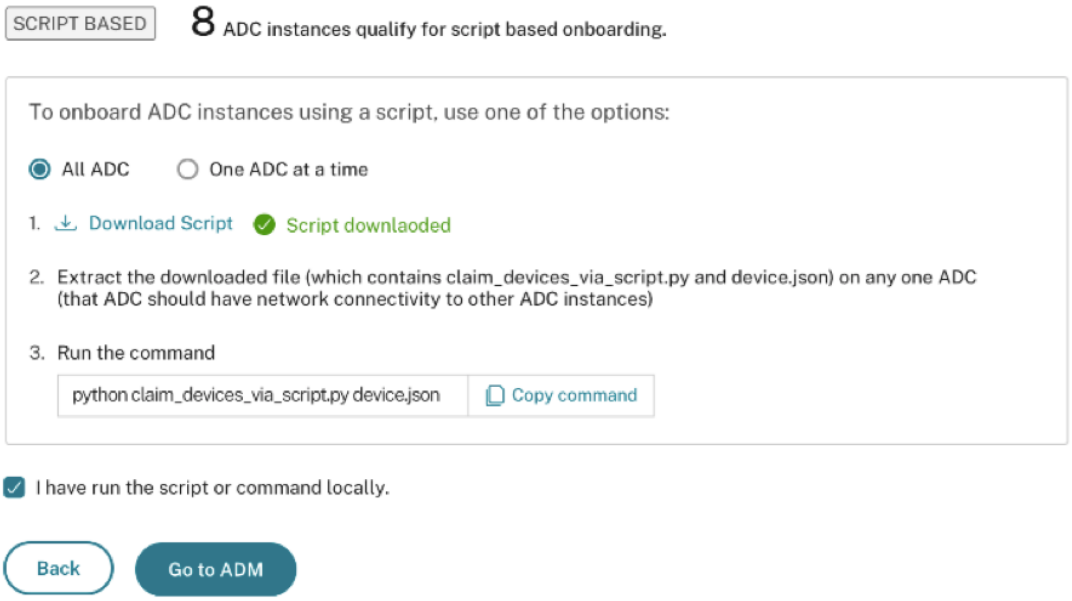
La incorporación automática puede tardar entre 2 y 5 minutos en completarse.



> **Nota:**
>
> Si no desea que las instancias de NetScaler se incorporen automáticamente a NetScaler Console, puede inhabilitar la incorporación automática y utilizar la opción basada en scripts para la incorporación.

Incorporación basada en secuenciasde comandos: una vez completada la incorporación automática, puede incorporar el resto de instancias mediante la incorporación basada en scripts. Use una de las siguientes opciones:

- **Opción 1**: descargue el script, extraiga el archivo tar y ejecútelo en cualquiera de las instancias de NetScaler mediante el comando que aparece en la interfaz de usuario. Asegúrese de que la instancia de NetScaler en la que ejecuta este script tenga conectividad de red con todas las demás instancias de NetScaler seleccionadas.
- **Opción 2**: inicie sesión en la consola CLI de cada instancia de NetScaler y ejecute los comandos que aparecen en la interfaz de usuario. Para obtener más información, consulte el paso 7 del documento Configurar el agente integrado de NetScaler para administrar las instancias. Asegúrese de generar un nuevo código de activación único para cada una de las instancias de NetScaler.

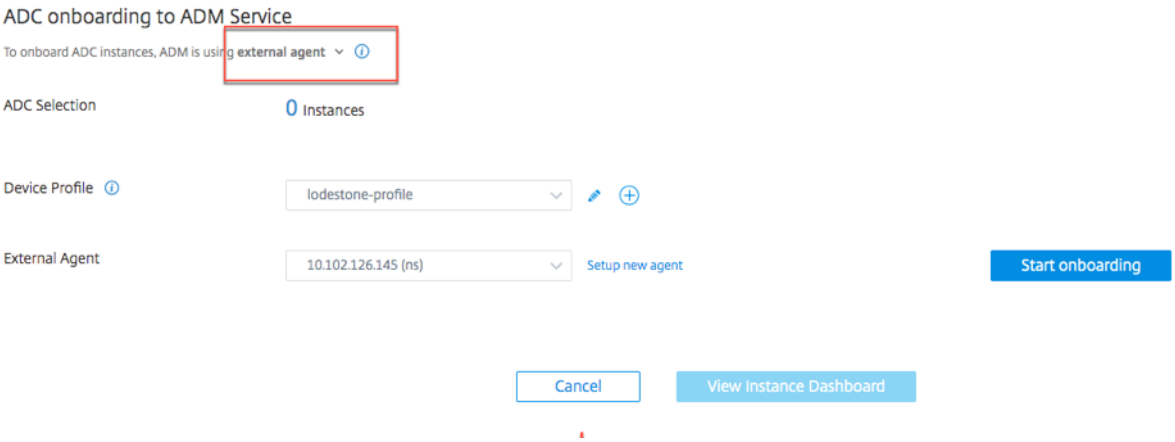


Después de incorporar todas las instancias, haga clic en **Ir a NetScaler Console** para ir al panel de la interfaz de usuario de administración de instancias de NetScaler Console y explorar las diferentes funciones.

> **Nota**
>
> Si es un cliente nuevo de NetScaler Console sin una licencia de NetScaler Console, su cuenta de servicio Citrix de forma predeterminada es una cuenta Express. Para obtener más información sobre los derechos de las cuentas de NetScaler Console, consulte Administrar los recursos de NetScaler Console mediante una cuenta Express.

Instancias de NetScaler integradas mediante un agente externo

Puede utilizar la incorporación externa basada en agentes si desea utilizar las licencias agrupadas o la suite de análisis completa de NetScaler Console, o ambas utilizar las licencias agrupadas y la suite de análisis completa.



Siga estos pasos:

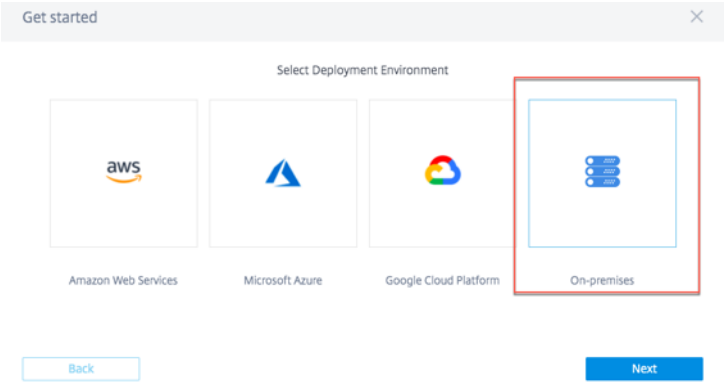
1. Seleccione un perfil de dispositivo.

   > **Nota**
   >
   > Por motivos de seguridad, no puede usar las credenciales predeterminadas de NetScaler (nsroot/nsroot) para la incorporación.

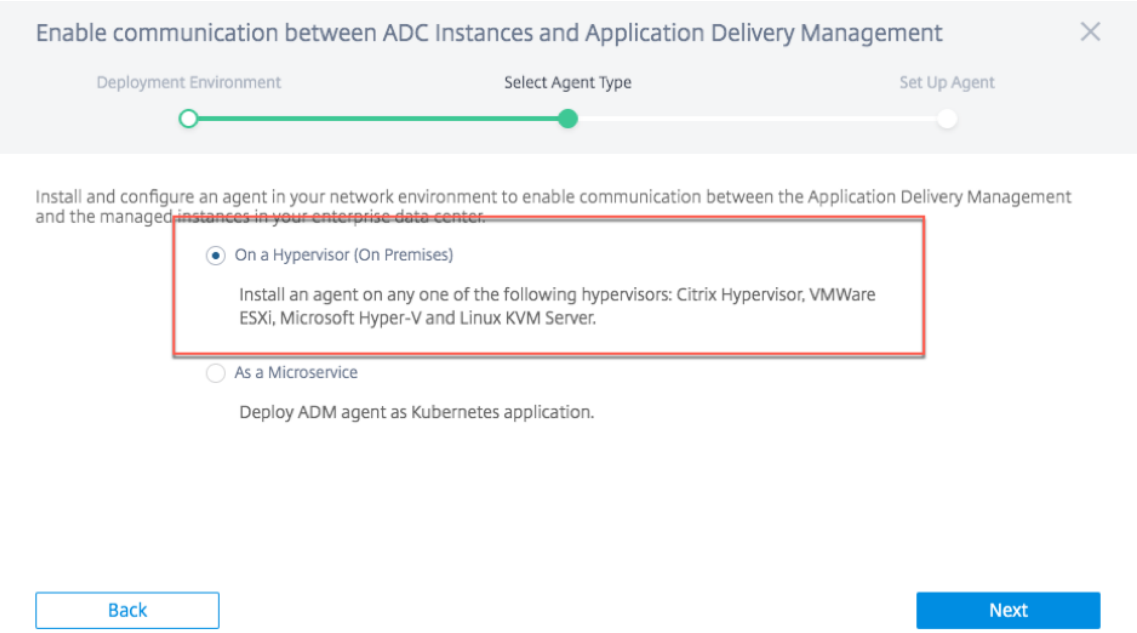
2. Seleccione un agente externo y haga clic en **Configurar nuevo agente**.
3. Seleccione cualquiera de los siguientes entornos:

   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - Local

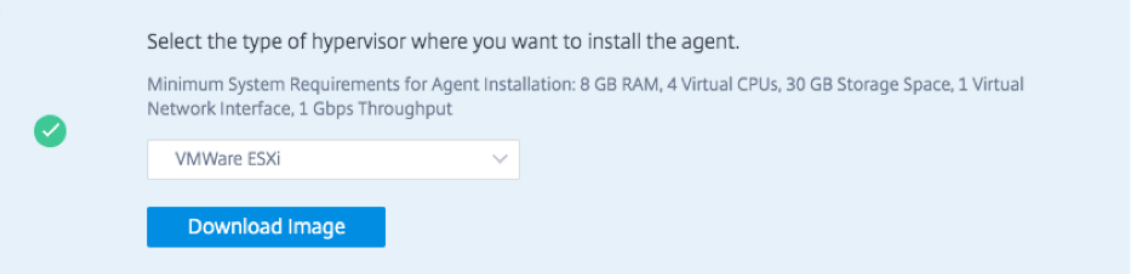
Instalar un agente en el hipervisor local Si selecciona **Local**, puede instalar el agente en los siguientes hipervisores: Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM Server.



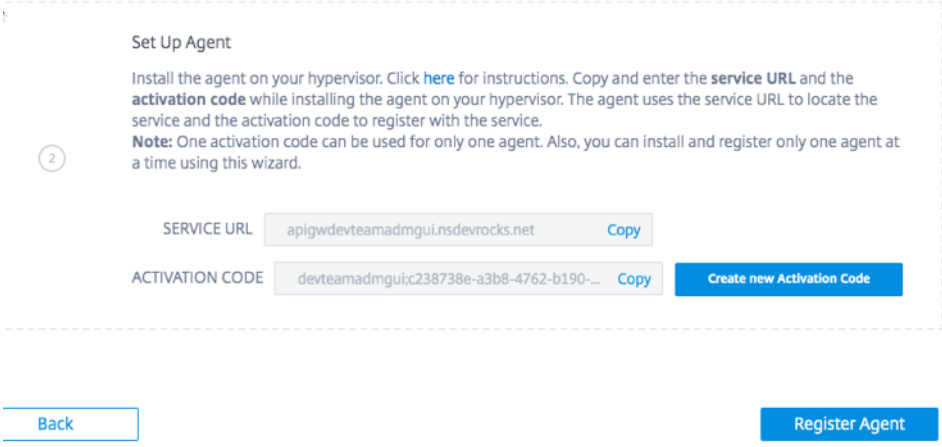
1. Seleccione **En un hipervisor (local)** y haga clic en **Siguiente**.



2. Seleccione el tipo de hipervisor y descargue la imagen, por ejemplo, VMware ESXi.

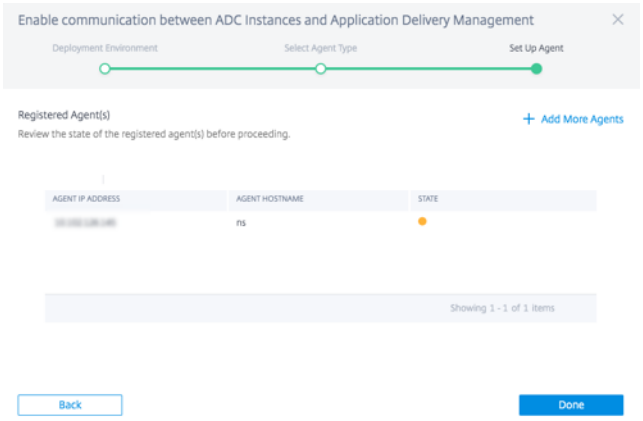


3. Utilice la URL del servicio y el código de activación para configurar el agente.

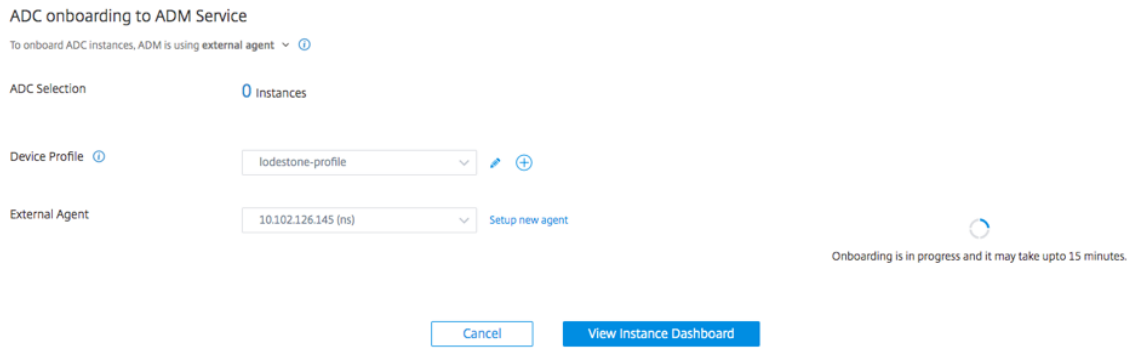


El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio. Para obtener instrucciones detalladas sobre la instalación de un agente en su hipervisor local, consulte Instalar un agente de NetScaler local

4. Haga clic en **Registrar agente**. Cuando haya terminado, haga clic **en**Listo para volver a la página de integración de NetScaler Console de NetScaler.



5. Haga clic en **Iniciar incorporación**. Después de incorporar todas las instancias, haga clic en Ver panel de instancias para ir al **panel** de la interfaz de usuario de administración de instancias de NetScaler Console y explorar las diferentes funciones.



Instalar un agente en una nube pública

Puede instalar el agente en uno de los siguientes entornos de nube:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

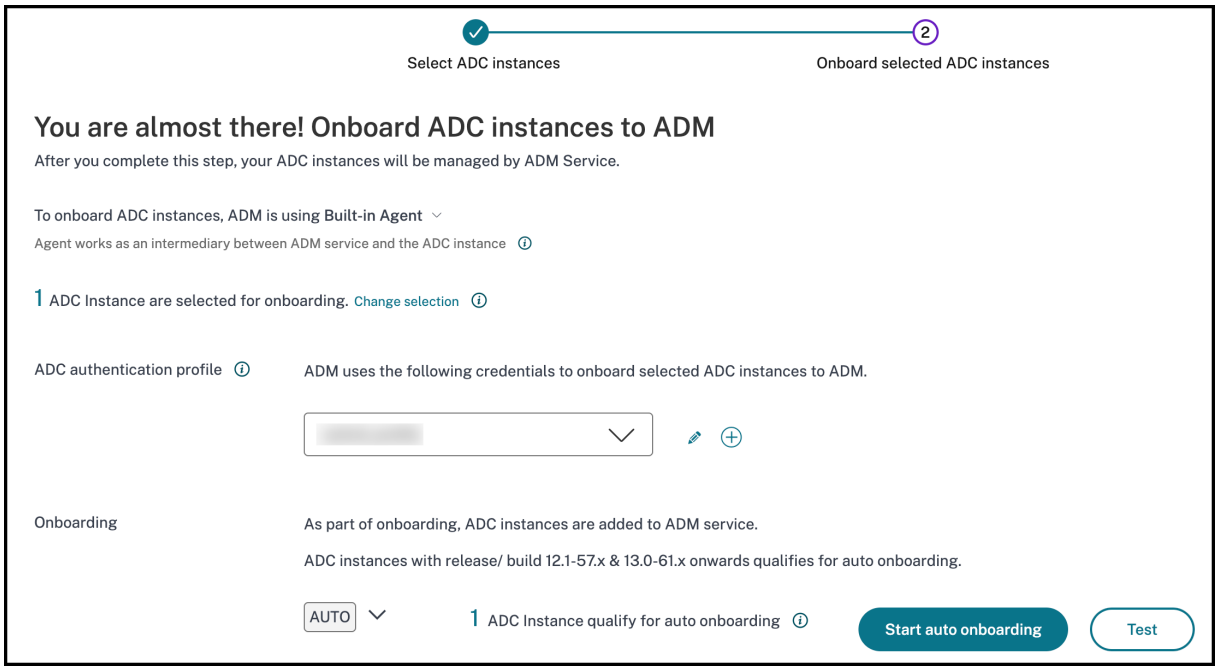
Para obtener más información, consulte los siguientes documentos:

- Instalación de un agente en la nube de Microsoft Azure
- Instalar un agente en AWS
- Instalar un agente en GCP

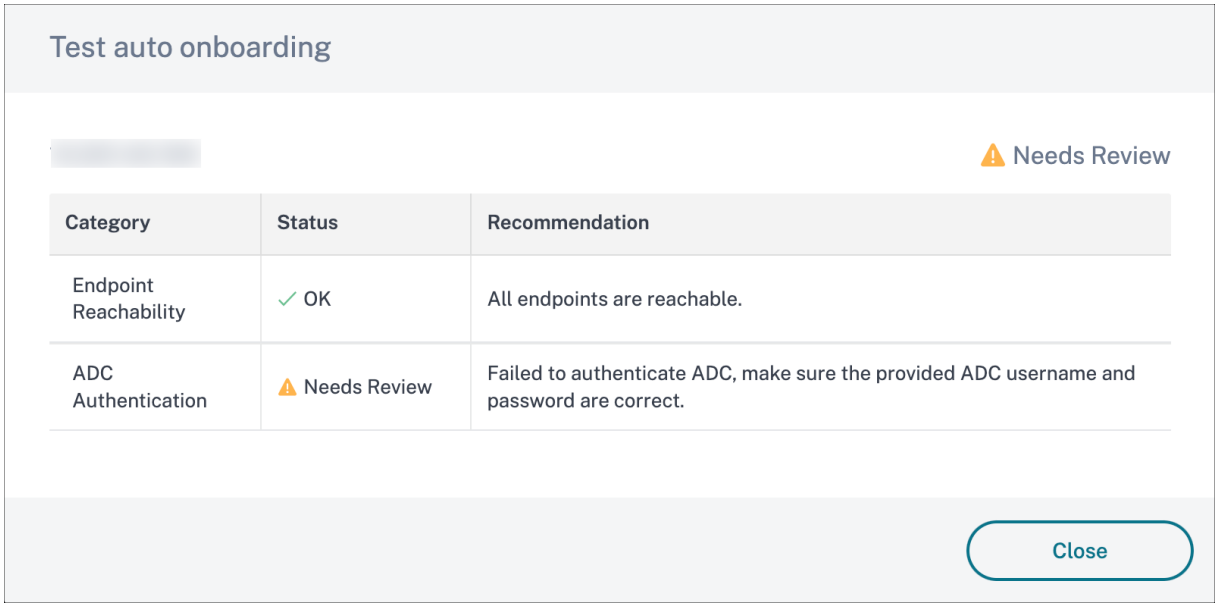
Pruebe la preparación para la incorporación de las instancias de NetScaler

September 2, 2024

Si desea incorporar una instancia de NetScaler a NetScaler Console, puede comprobar si las instancias están listas para la incorporación. El estado de ejecución de la prueba indica si las instancias están listas o necesitan ser revisadas.



Haga clic en **Probar** para iniciar el simulacro de diagnóstico. La página **Probar la incorporación automática** muestra la categoría del problema, el estado y la recomendación.



Para obtener más información, consulte Ver la información de diagnóstico de NetScaler en la GUI de NetScaler Console.

Si el estado de ejecución de la prueba de NetScaler está en el estado **Necesita revisión**, entonces:

- Revise las credenciales de inicio de sesión de NetScaler en el perfil del dispositivo.
- No se puede acceder a los siguientes puntos finales:
  - `adm.cloud.com`
  - `agent.adm.cloud.com`
  - `trust.citrixnetworkapi.net`
  - `download.citrixnetworkapi.net`

Si tiene algún problema al realizar la prueba de preparación para la incorporación, consulte Solución de problemas para obtener recomendaciones.

Parámetros de correo electrónico

January 26, 2024

El servicio NetScaler Console permite la incorporación de instancias de NetScaler mediante el flujo de trabajo de incorporación sencillo basado en Advisory Concole Connect. Como parte de este flujo de trabajo, los clientes reciben correos electrónicos iniciados por el producto desde el servicio NetScaler Console . Puedes activar o desactivar las notificaciones por correo electrónico que recibes como parte

del flujo de trabajo de incorporación sencillo basado en Advisory Console Connect. Puede configurar y administrar las notificaciones por correo electrónico de las siguientes maneras:

- **Habilite los correos electrónicos para todos los administradores**: podrá habilitar los correos electrónicos para todos los administradores de su organización. De forma predeterminada, los correos electrónicos están habilitados para todos los administradores de la organización.
- **Habilitar o inhabilitar los correos electrónicos para los administradores seleccionados**: puede personalizar la configuración del correo electrónico para que solo los administradores específicos de la organización reciban correos electrónicos y los demás administradores no.
- **Desactive los correos electrónicos para todos los administradores**: podrá inhabilitar y detener los correos electrónicos de todos los administradores de su organización.

Configurar ajustes de correo electrónico

Puedes configurar los ajustes de correo electrónico y activar o desactivar los correos electrónicos que recibes como parte del flujo de trabajo de incorporación sencillo basado en Console Advisory Connect. Para configurar los **ajustes de correo electrónico**:

1. Haga clic en **Incorporar al servicio ADM** en el correo electrónico de inicio del producto. Aparece la página **Citrix Cloud**.
2. En la página de inicio de sesión de **Citrix Cloud** :
   - Si ya es cliente de Citrix Cloud, inicie sesión en Citrix Cloud con sus credenciales de Citrix.com, My Citrixo Citrix Cloud.
   - Si aún no es cliente de Citrix Cloud, regístrese en Citrix Cloud. Para obtener más información, consulte Inscríbase en Citrix Cloud.

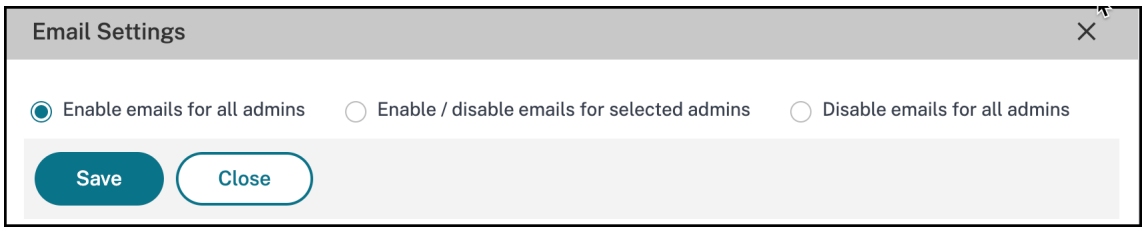
     > **Nota:**
     >
     > Si forma parte de varios ID de organización y uno de los ID de organización está en Citrix Cloud, inicie sesión con sus credenciales existentes.

   Aparece la página de inicio de NetScaler Console, que ofrece una descripción general de NetScaler Console y sus ventajas.
3. En la página de inicio de NetScaler Console, haga clic en **Siguiente**.

   Aparece la página **Información sobre las instancias de NetScaler y Gateway** , donde puede obtener información sobre su infraestructura general de NetScaler con recomendaciones.
4. En la página **Información sobre las instancias de NetScaler y Gateway** , haga clic en **Siguiente**.

Aparece la página **Seleccione las instancias de NetScaler y Gateway para** incorporar, donde puede ver una lista de las instancias de NetScaler que desea incorporar y opciones adicionales, como la **configuración del correo** electrónico.

5. Haga clic en **Configuración de correo electrónico** Aparece el panel **Configuración de correo electrónico**.



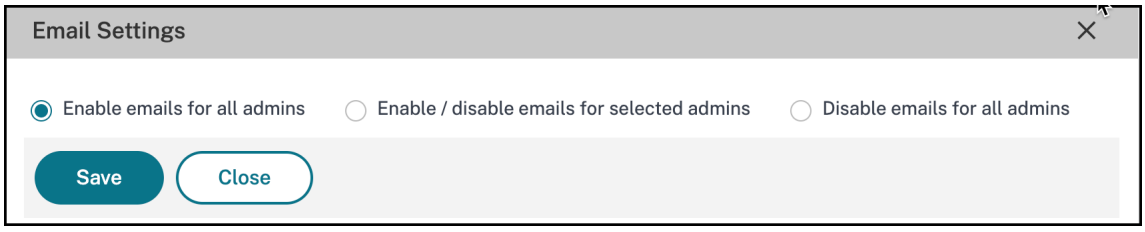
Ahora puede configurar los ajustes de correo electrónico para habilitar o inhabilitar los correos electrónicos.

> **Nota:**
>
> Si solo ha incorporado una instancia de NetScaler, no recibirá estos correos electrónicos.

Si ya utiliza la GUI de NetScaler Console y desea configurar los ajustes del correo electrónico:

1. En la GUI de NetScaler Console, vaya a **Infraestructura > Instancias** y, a continuación, haga clic en **NetScaler**. Aparece la página **NetScaler**.
2. En la página **NetScaler**, haga clic en **Inventario de activos**.

   Aparece la página **Seleccione las instancias de NetScaler y Gateway** para incorporarlas y muestra la lista de instancias de NetScaler que están incorporadas y opciones adicionales, como la **configuración de correo** electrónico.
3. Haga clic en **Configuración de correo electrónico** Aparece el panel **Configuración de correo electrónico**.



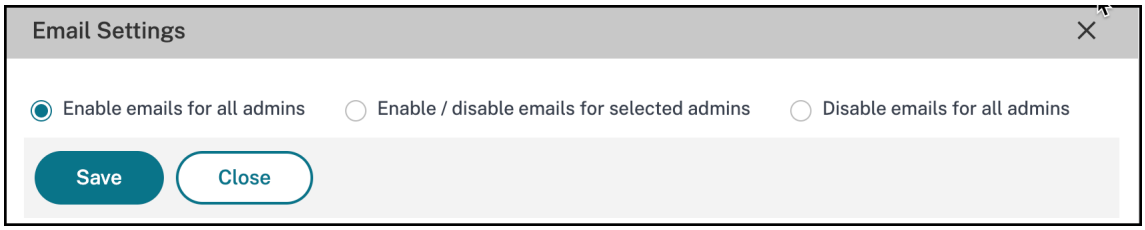
Ahora puede configurar los ajustes de correo electrónico para habilitar o inhabilitar los correos electrónicos.

Habilitar los correos electrónicos para todos los administradores

De forma predeterminada, los correos electrónicos están habilitados para todos los administradores de la organización.

Para habilitar o suscribirse a las notificaciones por correo electrónico como parte del flujo de trabajo basado en Console Advisory Connect:

1. En el panel **Configuración de correo electrónico**, selecciona **Habilitar correos electrónicos** para todos los administradores.



2. Haga clic en **Guardar** y **Cerrar**.

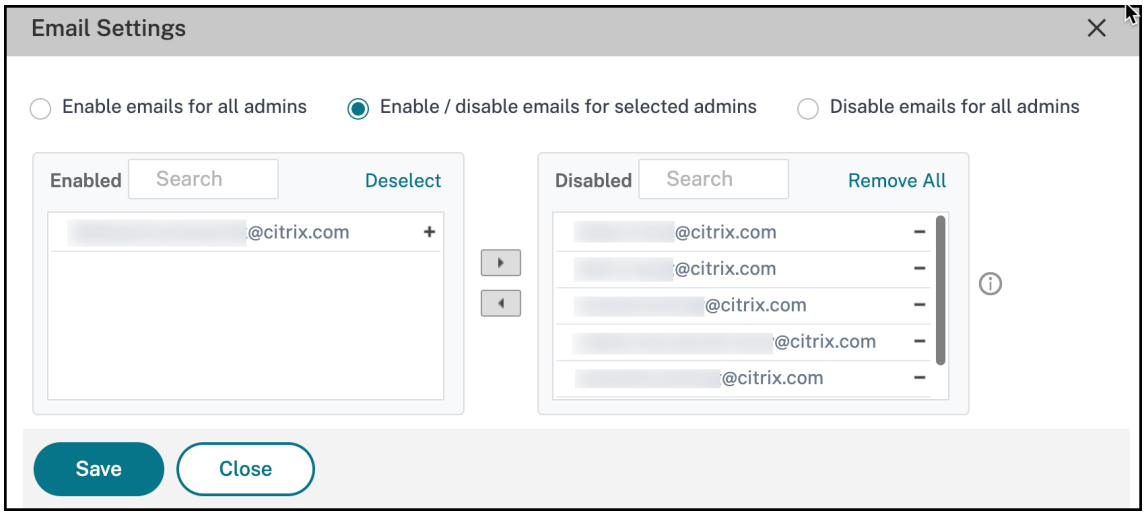
   Todos los administradores de la organización ya están suscritos y recibirán notificaciones por correo electrónico como parte del flujo de trabajo basado en Console Advisory Connect.

Activar o desactivar los correos electrónicos para administradores específicos de la organización

Puede personalizar la configuración del correo electrónico para que solo los administradores específicos de la organización reciban correos electrónicos. Verás la lista de administradores que tienen los correos electrónicos habilitados a la izquierda y la lista de administradores que tienen los correos electrónicos inhabilitados a la derecha.

Para inhabilitar los correos electrónicos para administradores específicos de la organización:

1. Busque la dirección de correo electrónico del administrador en la lista de **activados**.
2. Haga clic en el botón de agregar (**+**).



Verás que la dirección de correo electrónico del administrador se agregó a la lista de **inhabilitados**.

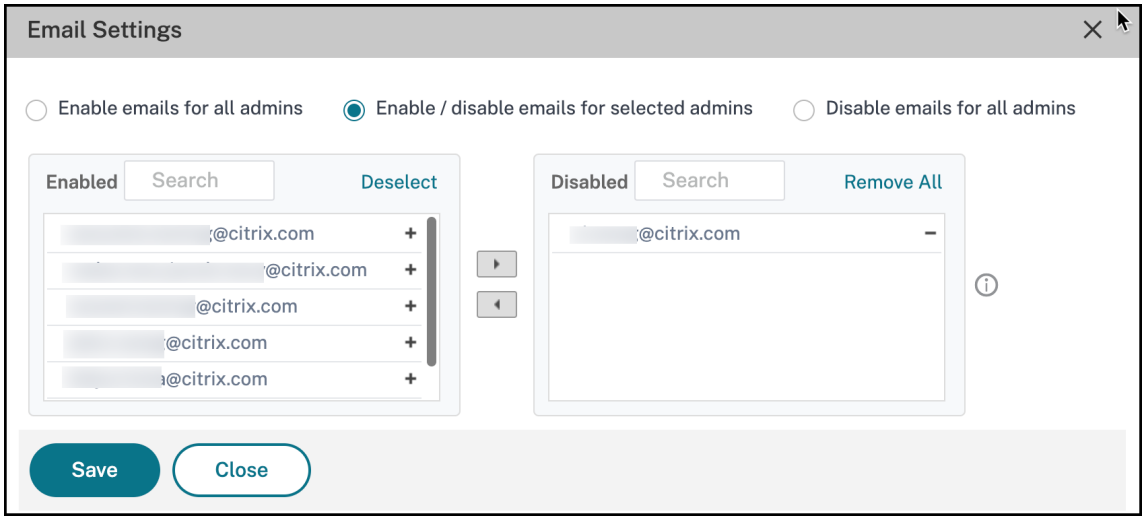
3. Haga clic en **Guardar** y **Cerrar**.

   El administrador ya no está suscrito para no recibir notificaciones por correo electrónico como parte del flujo de trabajo basado en Console Advisory Connect.

   > **Nota:**
   >
   > Si quieres inhabilitar los correos electrónicos de varios administradores, selecciona todos sus ID de correo electrónico en la lista de correos electrónicos **habilitados** y haz clic en el botón agregar (**+**) para agregar los ID de correo electrónico a la lista de **inhabilitados** . Haga clic en **Guardar** y **Cerrar**.

Si anteriormente ha inhabilitado los correos electrónicos para administradores específicos o para todos los administradores de su organización, podrá habilitar los correos electrónicos para todos los administradores. Para habilitar los correos electrónicos para administradores específicos de la organización:

1. Busque la dirección de correo electrónico del administrador en la lista de **inhabilitados**.
2. Haga clic en el botón de eliminación (-). Verás que la dirección de correo electrónico del administrador se elimina de la lista de **inhabilitados**.



3. Haga clic en **Guardar** y **Cerrar**.

   El administrador ahora comenzará a recibir correos electrónicos relacionados con la incorporación. El administrador ya está suscrito para recibir notificaciones por correo electrónico.

   > **Nota:**
   >
   > Si quieres habilitar los correos electrónicos para varios administradores, selecciona todos

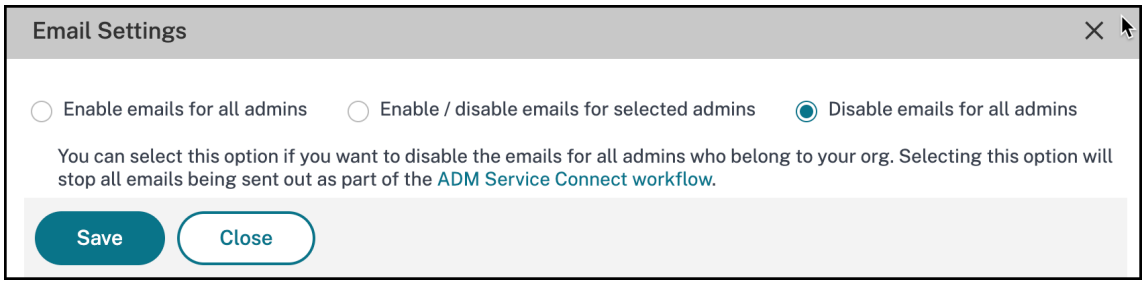
> sus ID de correo electrónico en la lista de correos electrónicos **deshabilitados** y haz clic en el botón de eliminar (**-**) para agregar los ID de correo electrónico a la lista **habilitados** . Haga clic en **Guardar** y **Cerrar**.

Desactivar los correos electrónicos para todos los administradores

Puede seleccionar esta opción si quiere inhabilitar o detener los correos electrónicos de todos los administradores que pertenecen a su organización.

Para inhabilitar o cancelar la suscripción a la recepción de correos electrónicos:

1. En el panel **Configuración del correo electrónico**, selecciona **Desactivar los correos electrónicos para todos los administradores**.



2. Haga clic en **Guardar** y **Cerrar**.

   Todos los administradores de la organización ya no están suscritos y no recibirán ninguna notificación por correo electrónico.

Solucione problemas con la herramienta de diagnóstico o la GUI de NetScaler Console

January 26, 2024

> Nota
>
> La herramienta de diagnóstico solo es aplicable a las instancias de NetScaler incorporadas o que se van a incorporar mediante la incorporación sencilla basada en Console Advisory Connect.
>
> Para obtener más información, consulte Incorporación discreta de instancias de NetScaler mediante NetScaler Console connect .

Al incorporar una instancia de NetScaler a NetScaler Console, es posible que experimente algunos problemas que impidan que la instancia de NetScaler se incorpore correctamente. Como admin-

istrador, debe saber el motivo del error de incorporación. Puede realizar comprobaciones de diagnóstico con la herramienta de diagnóstico cuando:

- Experimenta cualquier problema durante la incorporación automática o basada en guiones
- Quiere asegurarse de que la instancia de NetScaler está lista para su incorporación
- Quiere analizar los problemas de las instancias de NetScaler ya integradas que muestran el estado «Inactivo» en la GUI de NetScaler Console

Si Console Advisory Connect está habilitado en la instancia de NetScaler, los detalles del diagnóstico se envían automáticamente a Citrix y puede ver los detalles en la GUI de NetScaler Console. Si Console Advisory Connect no está habilitada, puede usar la herramienta de diagnóstico de forma manual .

Utilice manualmente la herramienta de diagnóstico

La herramienta de diagnóstico está disponible como parte de la actualización `mastools` (13.1-2.x o posterior) y se puede acceder a ella en `/var/mastools/scripts`. Puede verificar la `mastools`versión ejecutando el comando `cat /var/mastools/version.txt` en la instancia de NetScaler.

Para ejecutar la herramienta de diagnóstico:

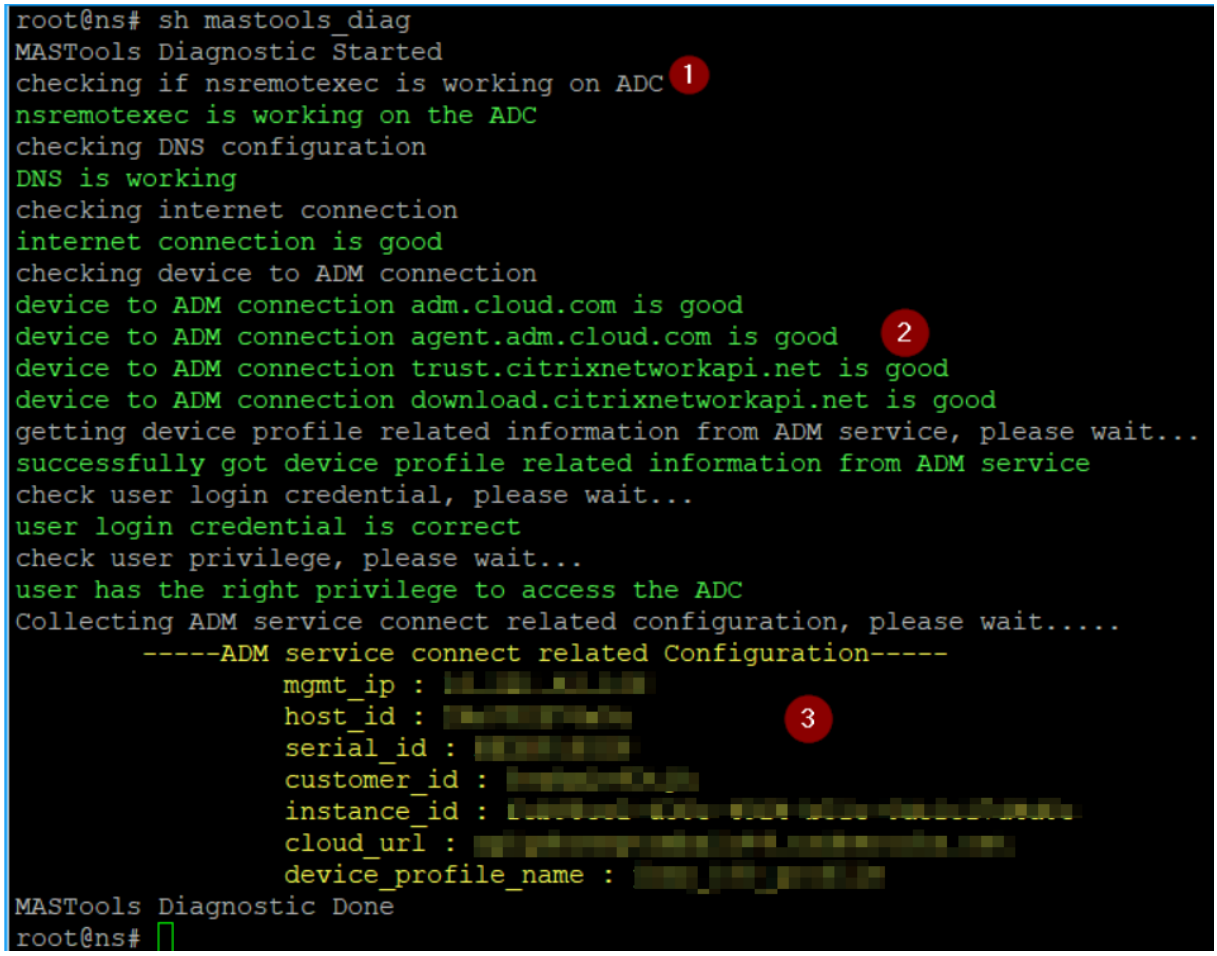
1. Con un cliente SSH, inicie sesión en la instancia de NetScaler.
2. Escribe shell y presiona Enter para cambiar al modo bash.
3. Escriba `cd /var/mastools/scripts`.
4. Escriba `sh mastools_diag`.

La herramienta se inicia y muestra los resultados de las siguientes comprobaciones de diagnóstico:

- **nscli**
- **Configuración de DNS**
- **Conexión a internet**
- **Conexión de instancia a ADM**
- **privilegio de usuario**

Si los problemas persisten incluso después de la solución de problemas, puedes ponerte en contacto con el servicio de asistencia. Cuando se ponga en contacto con el servicio de asistencia, debe proporcionar la información de configuración que se muestra después de ejecutar la herramienta de diagnóstico.

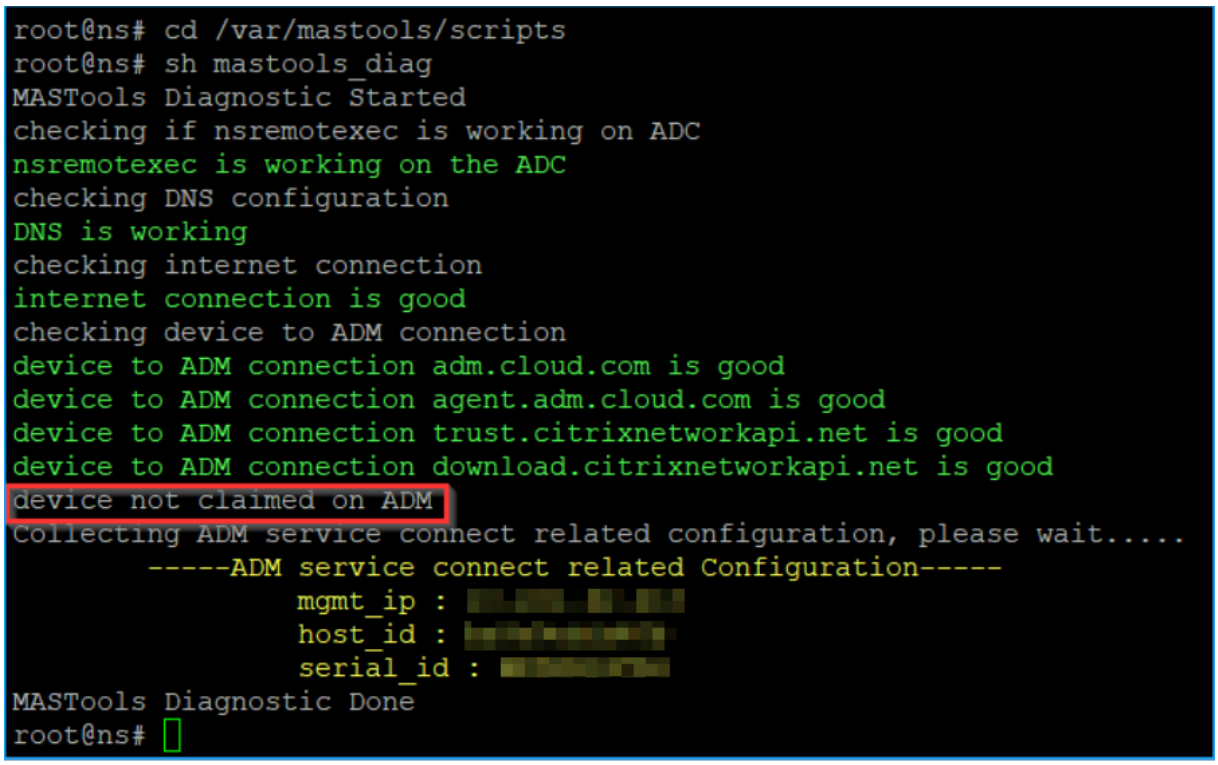
A continuación se muestra un ejemplo de los resultados de diagnóstico de una instancia de NetScaler que no presenta problemas:



- **1** —Muestra el tipo de comprobación de diagnóstico
- **2** —Muestra los resultados de la comprobación de diagnóstico en verde o rojo. El color verde indica que el resultado se ha realizado correctamente y el rojo indica que el resultado no es correcto.
- **3**—Muestra la información de configuración de la consola NetScaler en amarillo cada vez que ejecuta la herramienta de diagnóstico. Si desea ponerse en contacto con el soporte de NetScaler, debe proporcionar esta información.

Valide la preparación de la instancia de NetScaler para la incorporación mediante la herramienta de diagnóstico

Antes de incorporar la instancia de NetScaler a NetScaler Console, puede comprobar si la instancia de NetScaler está lista ejecutando la herramienta de diagnóstico en la instancia de NetScaler. Si la instancia de NetScaler no presenta problemas y está lista para su incorporación, la herramienta muestra el mensaje « el **dispositivo no reclamado en ADM**».



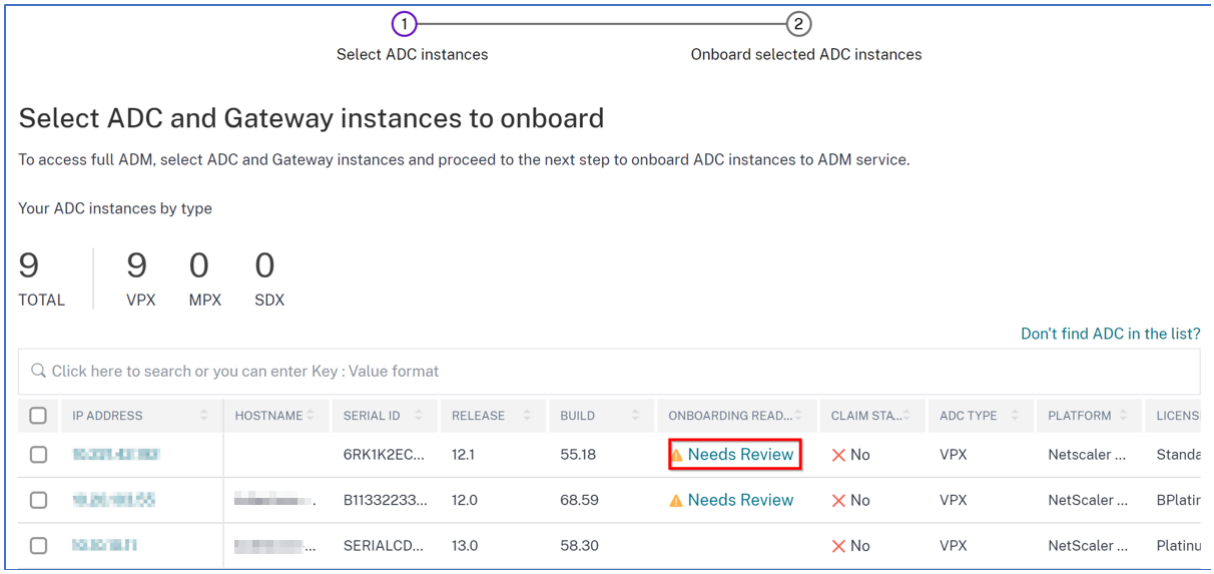
Ver la información de diagnóstico de NetScaler en la GUI de NetScaler Console

Vaya a **Infraestructura > Instancias > NetScaler** y haga clic en **Inventario de activos** para ver la nueva opción de **preparación** para la incorporación que indica el estado de preparación para la incorporación de la instancia de NetScaler, como **Needs Review** o **OK**.

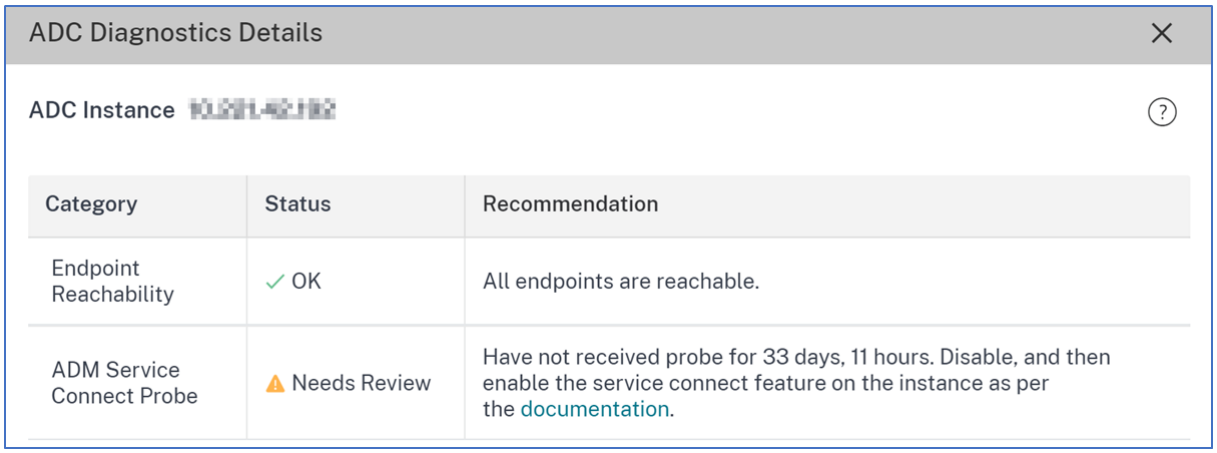
- **Necesita revisión**. La instancia de NetScaler tiene problemas que deben solucionarse.
- **OK**. La instancia de NetScaler está lista para su incorporación.

> **Nota:**
>
> Si la opción Listo para la **incorporación** aparece en blanco, significa que la instancia de NetScaler no se está ejecutando con la imagen más reciente compatible con el diagnóstico.

Si la instancia de NetScaler tiene algún problema, aparece la opción **Revisión** de necesidades y puede hacer clic para ver más detalles.



Tras hacer clic en **Necesita revisión** , la página **Detalles de diagnóstico de NetScaler** muestra los detalles del problema.



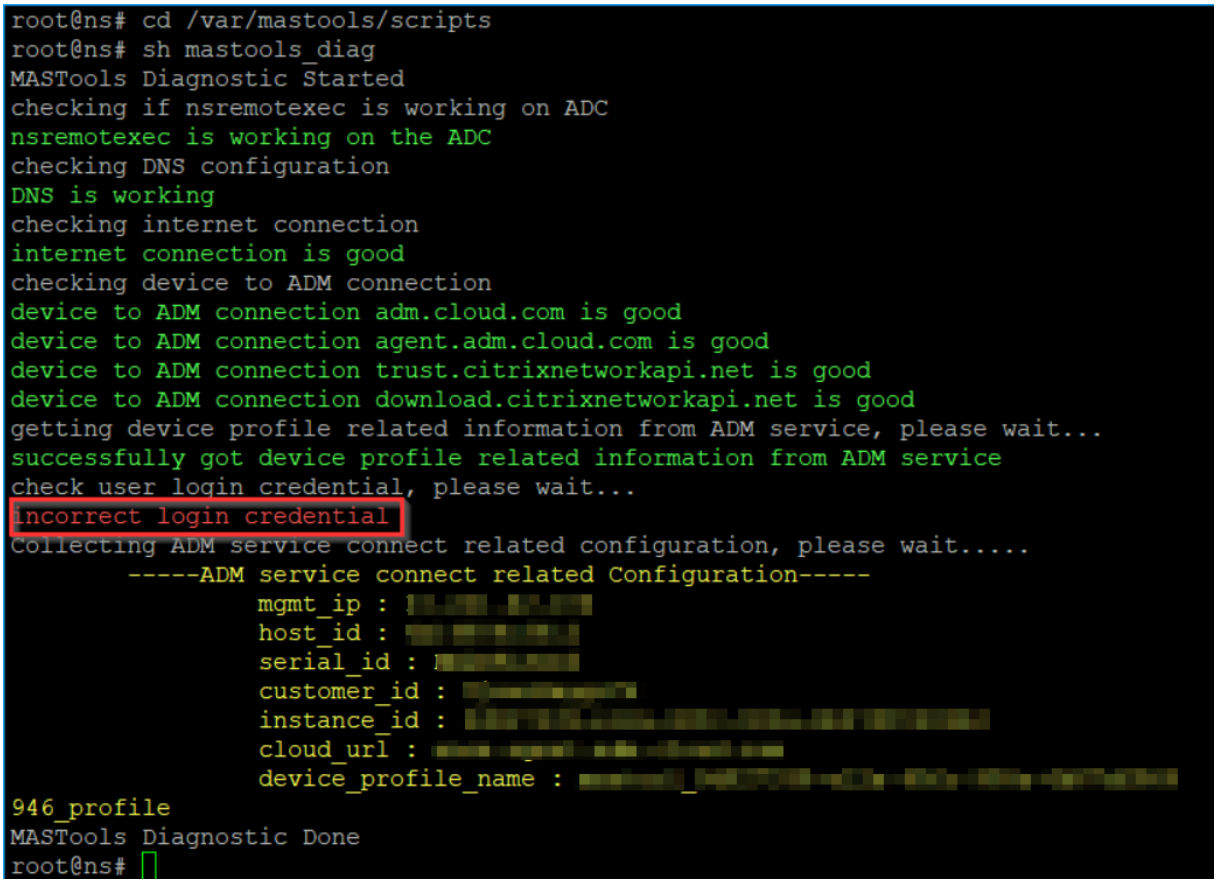
- **Categoría**. Proporciona la categoría del problema.
- **Status**. Indica el estado del problema, como **Necesita revisión**, **OK**o **No aplicable**.
- **Recomendación**. Proporciona la recomendación necesaria para solucionar el problema.

Tras solucionar el problema, el estado de preparación para la incorporación cambia a **Aceptar**.

Solución de problemas

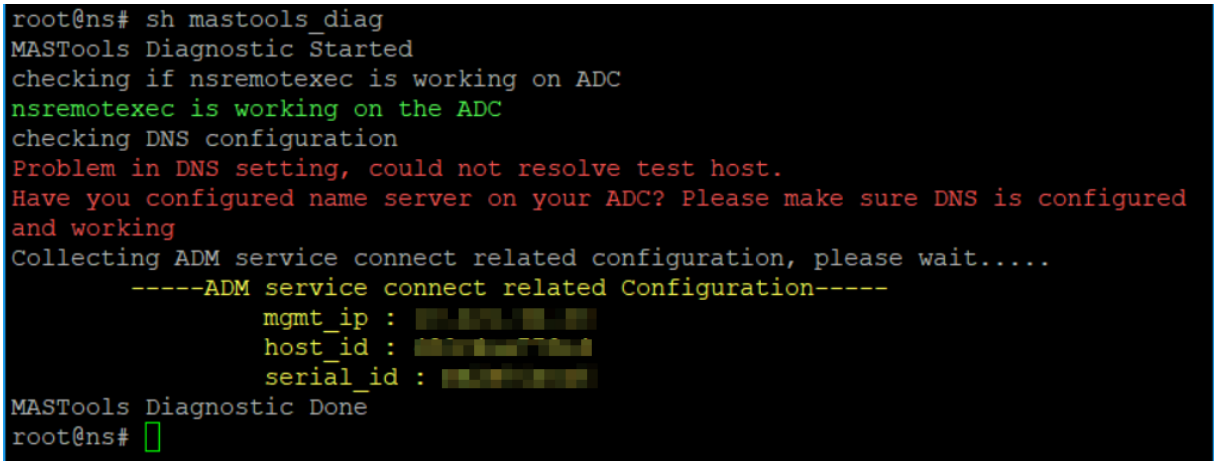
Los siguientes son algunos de los problemas de la instancia de NetScaler y sus pasos para solucionarlos:

Nombre de usuario o contraseña no válidos



Solución alternativa: Asegúrese de que el nombre de usuario y la contraseña proporcionados en el perfil de administrador son correctos. Si ha modificado la contraseña de la instancia de NetScaler, debe modificar los perfiles de administración de las instancias. Para obtener más información, consulte Modificar el perfil de administrador.

Error de configuración de DNS



Solución alternativa: Asegúrese de que el DNS esté configurado o que la dirección IP del DNS sea válida. Para obtener más información, consulte Configuración de DNS.

No hay conexión a internet

Solución alternativa: Asegúrese de que la configuración del firewall no esté bloqueando el acceso a Internet y de que el proxy requerido esté configurado.

No hay conexión con el punto final de NetScaler Console

Soluciónalternativa : asegúrese de comprobar la configuración del firewall y de que los siguientes puntos finales de la consola NetScaler no estén bloqueados en el firewall:

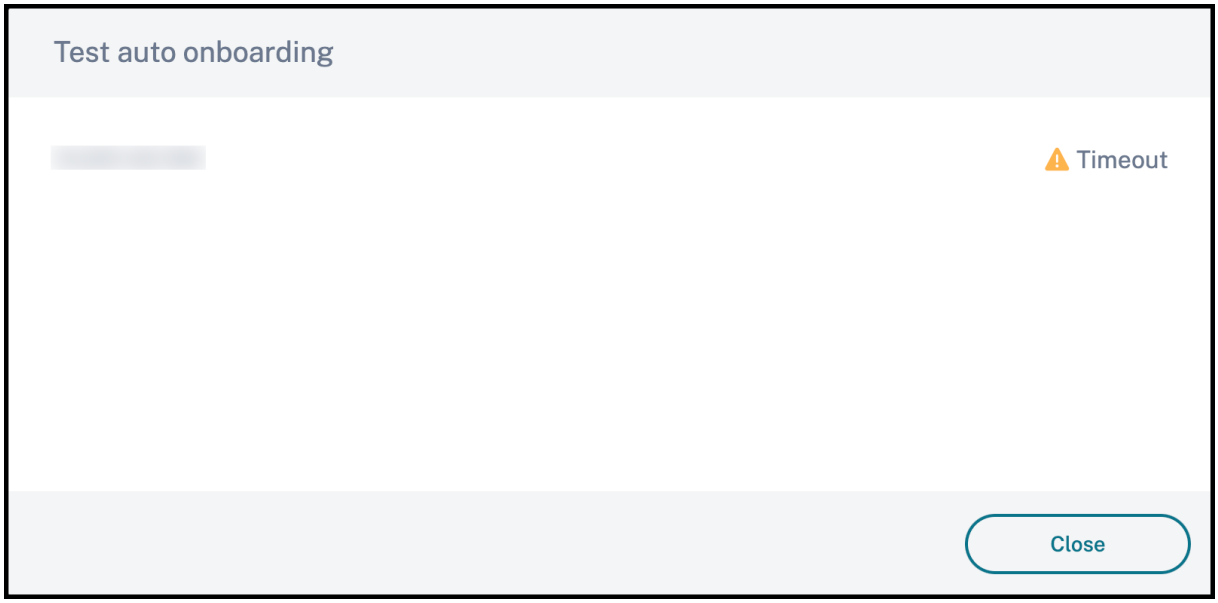
```
ADM_GRP_EP = "adm.cloud.com"

ADM_AGENT_EP = "agent.adm.cloud.com"

ADM_TRUST_EP = "trust.citrixnetworkapi.net"

ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
```

Si no se encuentra ningún problema en las comprobaciones de diagnóstico y el problema de falta de conexión persiste, anote la información de configuración de la consola de NetScaler (disponible en amarillo) y póngase en contacto con el servicio de asistencia de NetScaler.

Al realizar una ejecución de prueba para asegurarse de que la instancia de NetScaler está lista para su incorporación, es posible que se produzcan los siguientes problemas:

Tiempo de espera incorporado del agente en seco

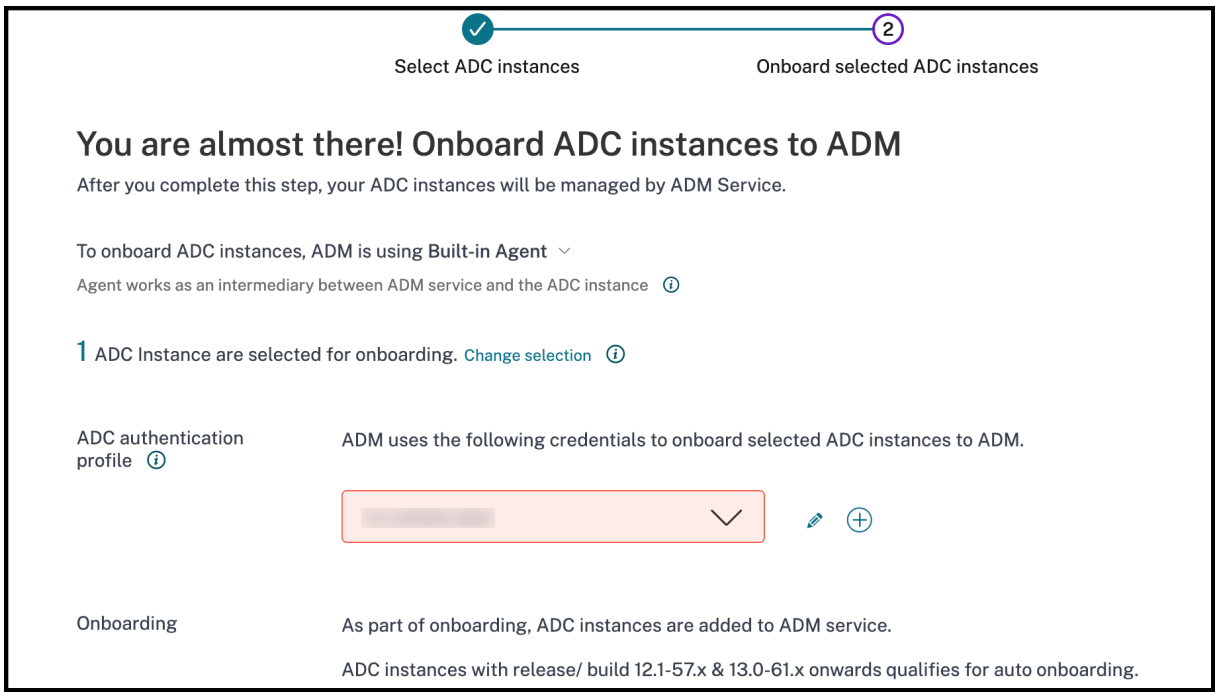
Si no se obtienen los resultados del simulacro transcurridos 5 minutos, aparece un mensaje de tiempo de espera.



Recomendación: Se recomienda comprobar si la instancia de NetScaler se está ejecutando con la imagen más reciente compatible con el diagnóstico. Además, en la tabla de selección de activos, la columna Preparación para la incorporación aparece en blanco.

Esquema rojo en el menú desplegable del perfil del dispositivo

La autenticación de NetScaler falla durante la ejecución en seco y aparece un contorno rojo en el menú desplegable del perfil del dispositivo.



Recomendación: Vuelva a introducir las credenciales de administrador del usuario de NetScaler, cree el perfil del dispositivo y haga clic en Probar para volver a ejecutar la prueba en seco.

Transición de un agente integrado a un agente externo

January 26, 2024

Es posible que haya empezado a utilizar NetScaler Console únicamente para la administración y la supervisión y, más adelante, puede que desee utilizar otras funciones, como las licencias agrupadas y los análisis. Para ello, debe pasar del agente integrado a un agente externo.

El agente integrado solo admite funciones de administración y supervisión. Para otras funciones de NetScaler Console, como las licencias agrupadas y los análisis, necesita un agente externo. Este documento describe los pasos para pasar de un agente integrado de NetScaler Console existente a un agente externo basado en un hipervisor.

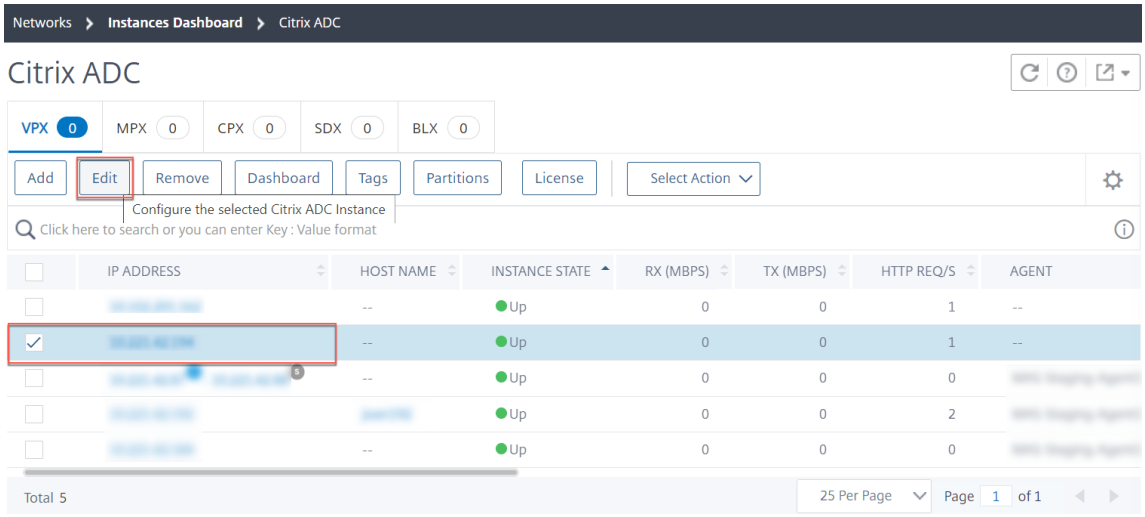
Antes de comenzar

Instale un agente externo antes de iniciar la transición. Siga el procedimiento que se indica en el tema Instalar un agente de NetScaler en las instalaciones.

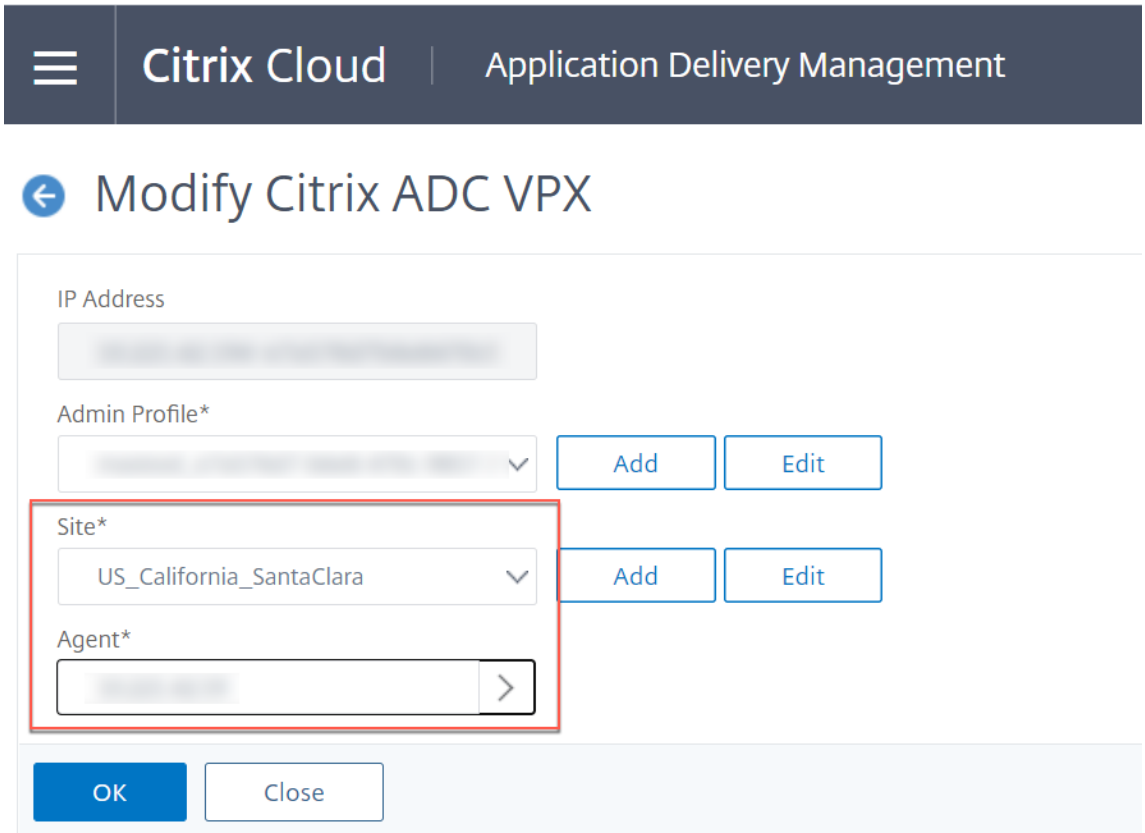
Transición de un agente integrado a un agente externo

Siga estos pasos para realizar la transición de un agente integrado a un agente externo:

1. En la GUI de NetScaler Console, en **Infraestructura > Panel de instancias > NetScaler**, seleccione la instancia de NetScaler y haga clic en **Editar**.



2. Seleccione el sitio y el agente y haga clic en **Aceptar**.



3. Seleccione la instancia de nuevo y haga clic en **Seleccionar acción > Redescubrir**.

Para obtener información sobre cómo crear un sitio en NetScaler Console y agregar el agente al sitio, consulte Agregar instancias

Conecte SAML como proveedor de identidades a NetScaler Console

January 26, 2024

NetScaler Console admite el uso de SAML (Security Assertion Markup Language) como proveedor de identidad para autenticar a los administradores y suscriptores que inician sesión en su consola NetScaler. Con su instancia de Active Directory (AD) local, puede usar el proveedor SAML 2.0 que prefiera.

Para la mayoría de los proveedores de SAML, use la información de este artículo para configurar la autenticación SAML. Si prefiere usar autenticación SAML con Azure AD, tiene la opción de usar la aplicación Citrix Cloud SAML SSO de la galería de aplicaciones de Azure AD.

Requisitos previos

La autenticación SAML con NetScaler Console tiene los siguientes requisitos:

- Proveedor SAML compatible con SAML 2.0
- Dominio de AD local
- Dos Cloud Connectors implementados en una ubicación de recursos y unidos al dominio de AD local. Los Cloud Connectors se utilizan para garantizar que Citrix Cloud pueda comunicarse con su ubicación de recursos.
- Integración de AD con su proveedor SAML.

Cloud Connectors

Debe tener al menos dos (2) servidores en los que instalar el software Citrix Cloud Connector. Se recomienda tener al menos dos servidores para la alta disponibilidad de Cloud Connector. Estos servidores deben cumplir los siguientes requisitos:

- Cumplir los requisitos del sistema descritos en los Detalles técnicos de Cloud Connector.
- No tener ningún otro componente de Citrix instalado, no ser un controlador de dominio de AD ni ser cualquier otra máquina de importancia crítica para la infraestructura de la ubicación de recursos.

- Estar unidos al dominio donde residen los recursos. Si los usuarios acceden a los recursos de varios dominios, debe instalar al menos dos Cloud Connectors en cada dominio.
- Estar conectados a una red que puede establecer contacto con los recursos a los que acceden los usuarios a través de Citrix Workspace.
- Conectado a internet.

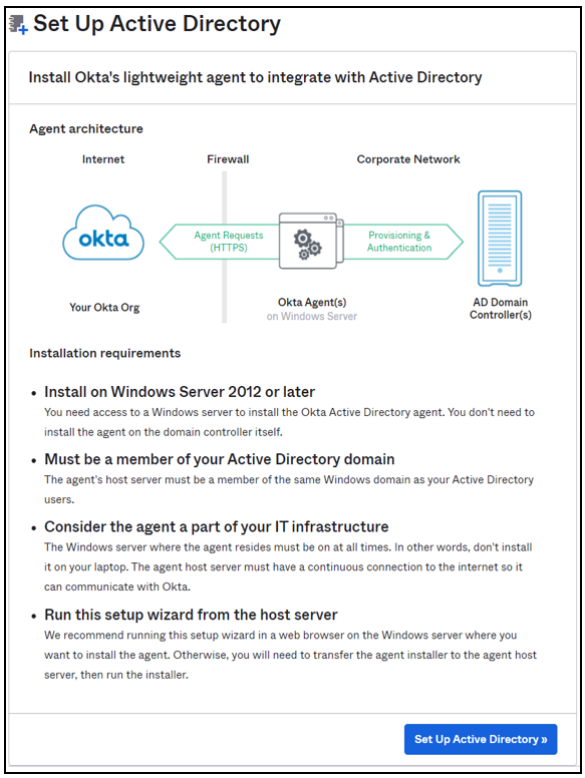
Active Directory

Antes de configurar la autenticación SAML, realice las siguientes tareas:

- Los campos Nombre, Apellidos y Correo electrónico son obligatorios para que los usuarios de Active Directory importen usuarios a la instancia de Okta.
- Compruebe que los suscriptores de Workspace tengan cuentas de usuario en Active Directory (AD). Los suscriptores sin cuentas de AD no pueden iniciar sesión correctamente en sus espacios de trabajo cuando la autenticación SAML está configurada.
- Asegúrate de que las propiedades de usuario de las cuentas de AD de tus suscriptores estén rellenadas. Citrix Cloud requiere estas propiedades para establecer el contexto de usuario cuando los suscriptores inician sesión en Citrix Workspace. Si estas propiedades no están rellenadas, los suscriptores no pueden iniciar sesión. Estas propiedades incluyen lo siguiente:
  - Dirección de correo electrónico
  - Nombre simplificado (opcional)
  - Nombre común
  - Nombre de cuenta SAM
  - Nombre principal del usuario
  - GUID de objeto
  - SID
- Implemente Cloud Connectors en su instancia de Active Directory (AD) local para conectar esta a su cuenta de Citrix Cloud.
- Sincronice los usuarios de AD con el proveedor SAML. Citrix Cloud necesita los atributos de usuario de AD para los suscriptores de espacios de trabajo para que puedan iniciar sesión correctamente.

Configuración de SSO de SAML

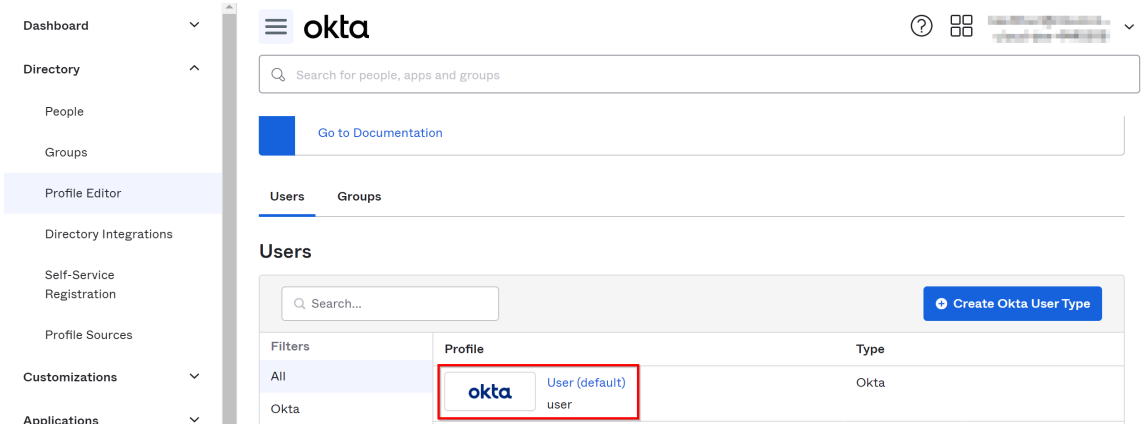
En una instancia de Okta, vaya a **Integraciones de directorios > Agregar Active Directory**.



Para una integración correcta, el proveedor de identidades SAML debe pasar a Citrix Cloud ciertos atributos de Active Directory del usuario en la aserción SAML. Concretamente,

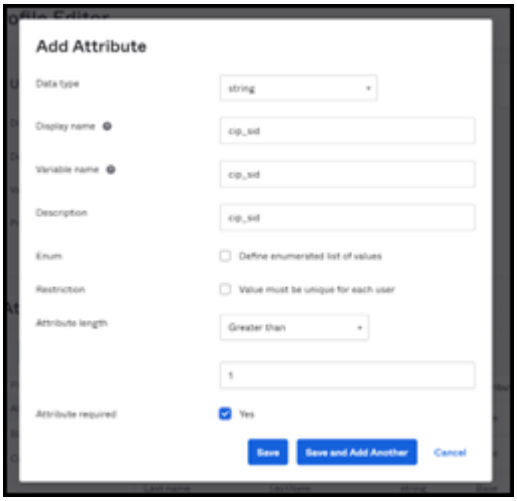
- Identificador de seguridad (SID)
- objectGUID (OID)
- Nombre principal del usuario (UPN)
- Correo (correo electrónico)

1. Inicie sesión en Okta con las credenciales de administrador.
2. Seleccione **Directorio > Editor de perfiles** y seleccione el perfil de **usuario de Okta (predeterminado)** . Okta muestra la página del perfil User.



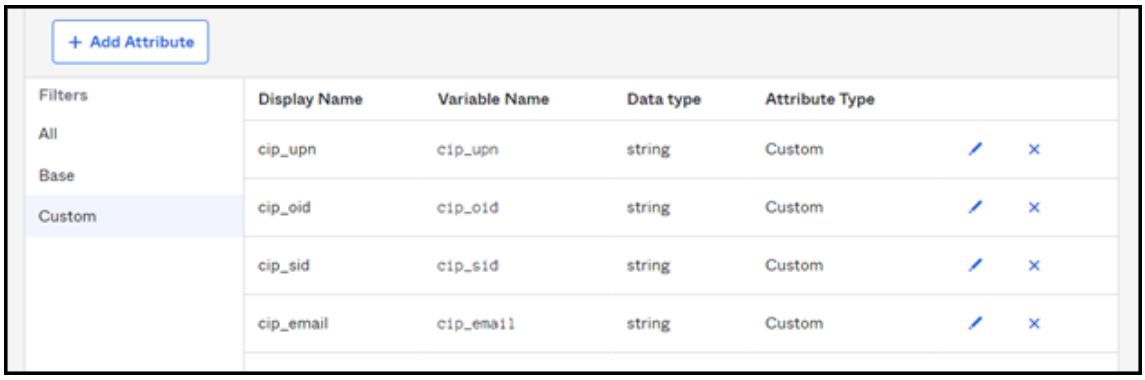
3. En **Atributos**, seleccione **Agregar atributos** y agregue los campos personalizados.

   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`

   Haga clic en **Guardar y agregar otro** y repita el proceso para crear 4 atributos personalizados.

   Puede ver los siguientes detalles después de crear 4 atributos personalizados:

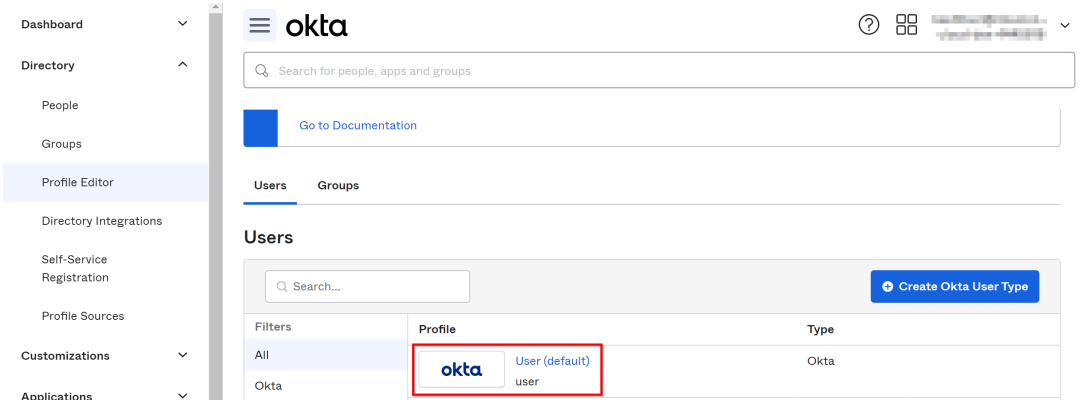
   

4. Asigne los atributos de Active Directory a los atributos personalizados. Seleccione el Active Directory que está utilizando en **Usuarios > Directorios**.
5. Edite las asignaciones de atributos:

   a) Desde la consola de Okta, vaya a **Directorio > Editor de perfiles**.

   b) Busca el `active_directory` perfil de tu AD. Este perfil puede etiquetarse con el formato MyDomain User, donde MyDomain es el nombre de tu dominio AD integrado.

   c) Seleccione **Mappings**. Aparece la página de **mapeos de perfil de usuario** de tu dominio de AD y se selecciona la pestaña para asignar tu AD a un usuario de Okta.



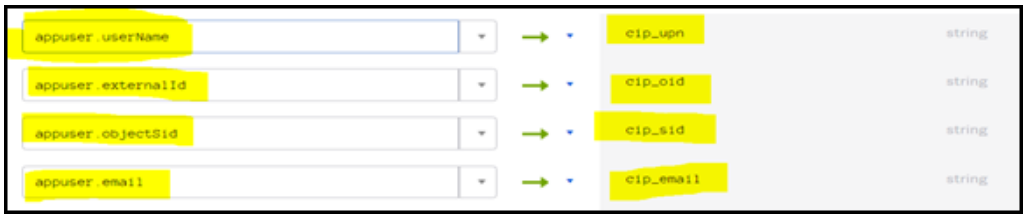
d) En la columna **Perfil de usuario de Okta** , asigne los atributos de Active Directory a los atributos personalizados que ha creado:

i. Para `cip_email`, selecciona el correo electrónico en la columna Perfil de usuario de tu dominio. Al seleccionarse, la asignación aparece como `appuser.email`.

ii. Para ello `cip_sid`, seleccione **ObjectSID** en la columna Perfil de usuario de su dominio. Al seleccionarse, la asignación aparece como `appuser.objectSid`.

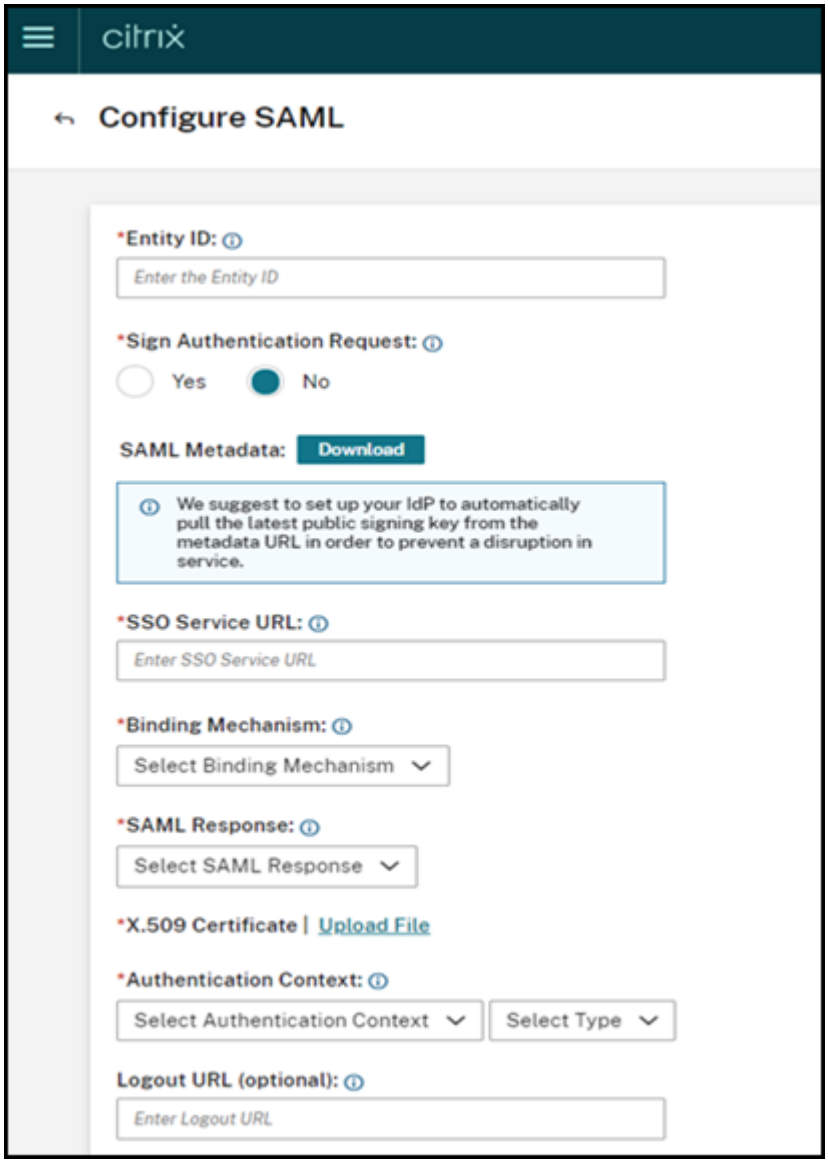
iii. Para `cip_upn`, selecciona `userName`tu dominio en la columna **Perfil de usuario** . Al seleccionarse, la asignación aparece como `appuser.userName`.

iv. Para `cip_oid`, selecciona `externalId`tu dominio en la columna **Perfil de usuario** . Al seleccionarse, la asignación aparece como `appuser.externalId`.



6. Inicie sesión en Citrix Cloud desde `https://citrix.cloud.com`.
7. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
8. Busca **SAML 2.0** y haz clic en **Conectar** .

   Aparece la página **Configurar SAML** .



Descargue el `xml` archivo y ábralo con cualquier editor de archivos. Debe volver a esta página después de completar la configuración adicional en Okta.

9. En Okta, dirígete a **Aplicación > Crear integración de aplicaciones**.
10. En la página **Agregar aplicación** , haga clic en **Crear nueva** aplicación .
11. En la página **Crear una nueva integración de aplicaciones** , seleccione **SAML 2.0** y haga clic en **Crear** .
12. Proporcione detalles como el nombre y el logotipo de la aplicación (opcional), configure la visibilidad de la aplicación y, a continuación, haga clic en **Siguiente**.
13. En la pestaña **SAML de configuración** , debes usar los detalles del archivo descargado`xml`:

    a) Proporcione los detalles de la URL para **la URL de inicio de sesión único** como `https` **:**

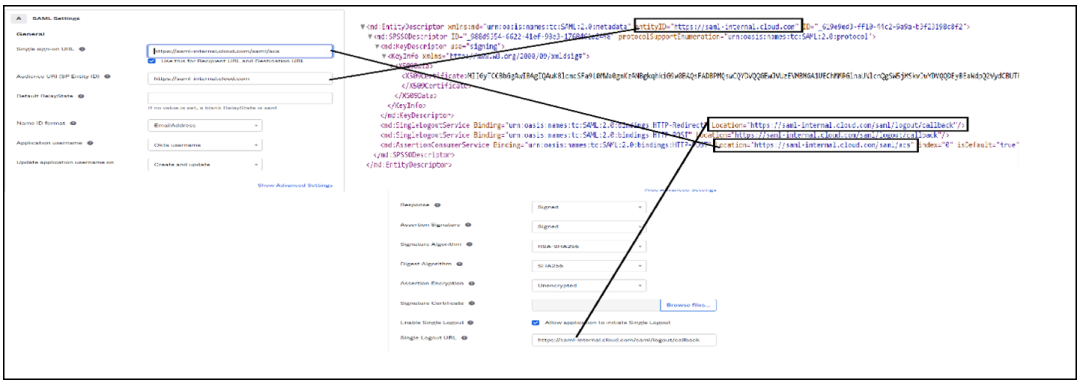
//saml-internal.cloud.com/saml/acsy la **URI de audiencia (ID de entidad de SP)** comohttps://saml-internal.cloud.com.

> **Nota:**
>
> Si es Citrix Cloud externo, la URL debe ser https://saml.cloud.com/saml/acsy https://saml.cloud.comen lugar de https://saml-internal.cloud.comdominio.

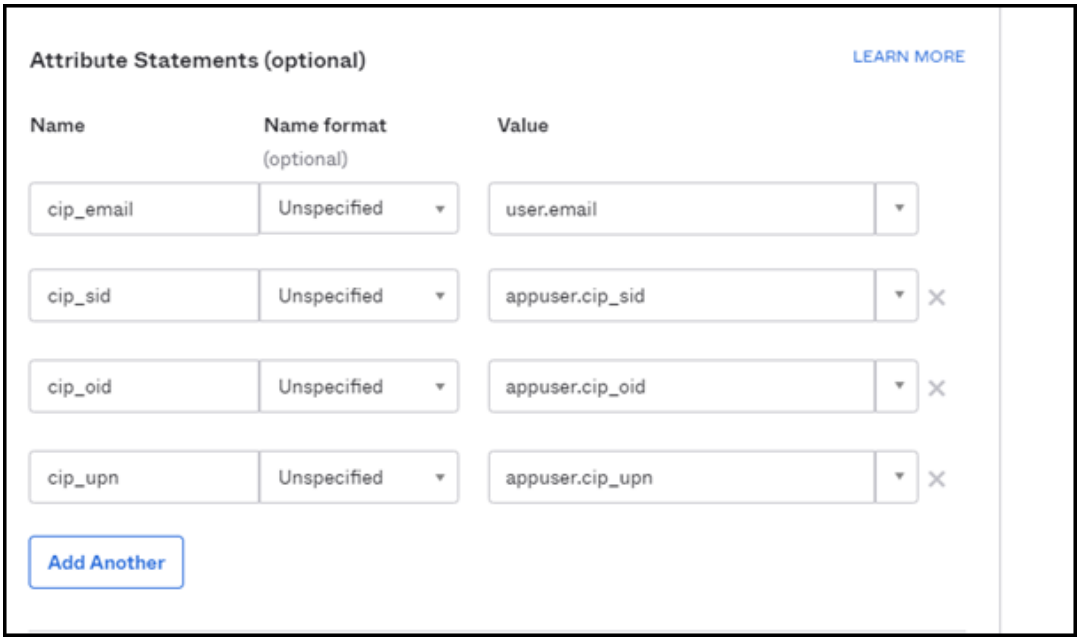
b) Seleccione Sin **especificar** para **Formato de identificador de nombre** .

c) Seleccione Nombre de usuario de **Okta para Nombre** de **usuario de la aplicación** .

d) Haga clic en **Mostrar configuración avanzada** y asegúrese de que la **respuesta** y la **afirmación** estén seleccionadas con **Firmado** .



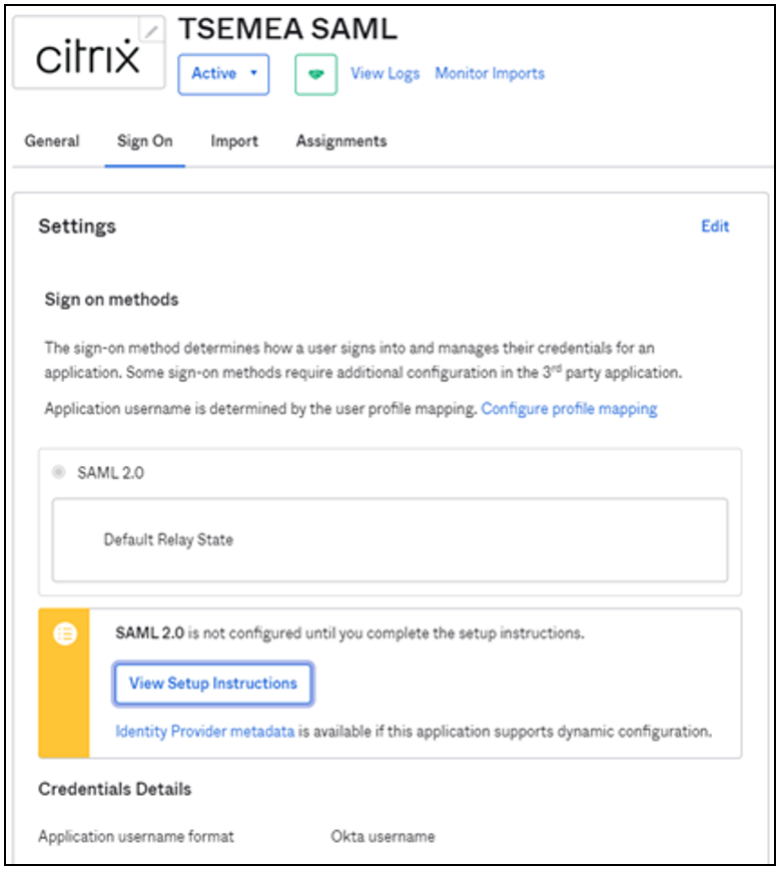
e) Agregue **declaraciones de atributos** como se muestra en la siguiente imagen.



f) Puede dejar todas las demás opciones por defecto y hacer clic en **Siguiente**.

g) Selecciona Soy **un cliente de Okta y añado una aplicación interna** y, a continuación, haz clic en **Finalizar**.

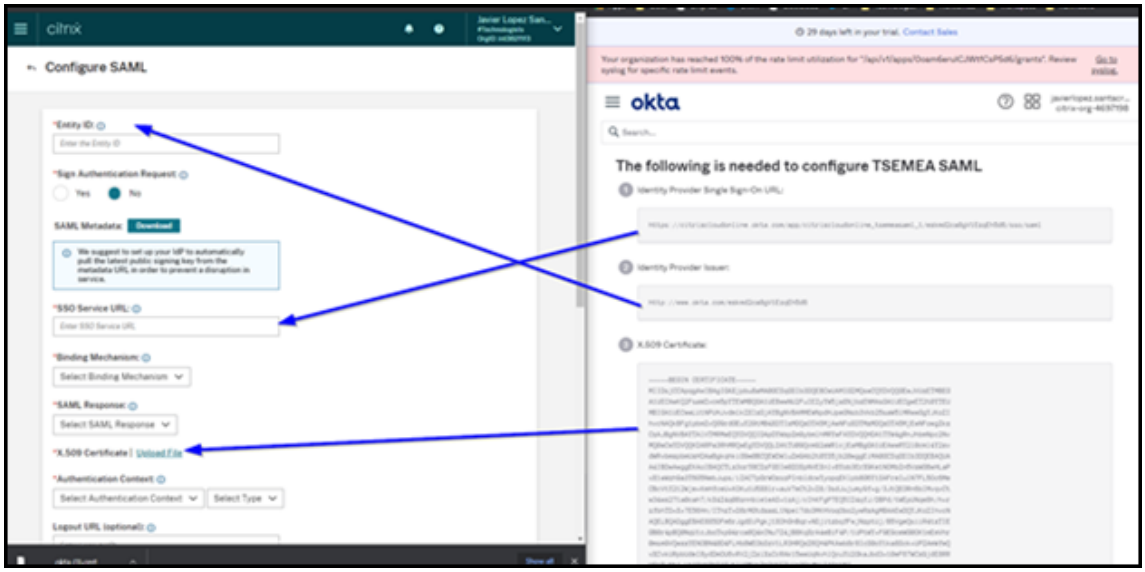
14. La aplicación Okta ya está creada y haga clic en **Ver instrucciones de configuración**.



Aparece la página **Cómo configurar SAML 2.0 para la aplicación de prueba** con detalles de que debe volver a agregarlo a Citrix Cloud.

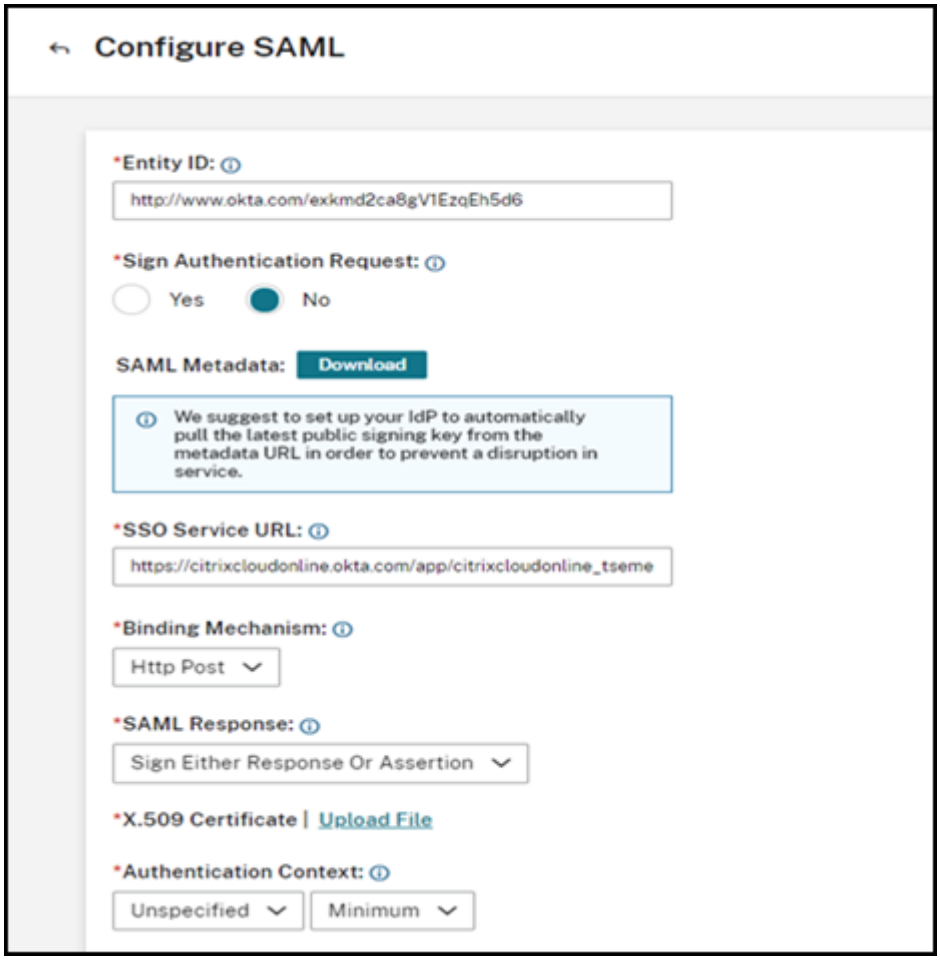
Descargue el certificado para cargarlo en Citrix Cloud.

15. Ahora debe volver a la página **Configurar SAML** en Citrix Cloud y completar el resto de la configuración tal y como se indica a continuación:

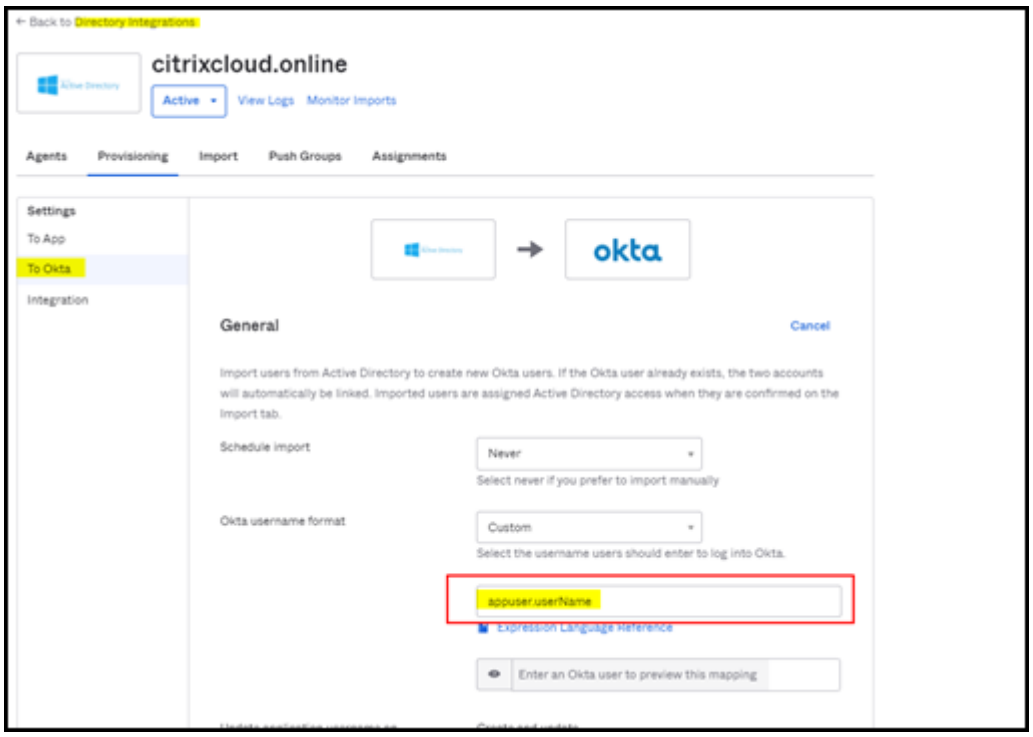


Utilice el certificado descargado y cambie el nombre de la extensión del `.cert`nombre `.crt`de archivo de a para cargarlo en Citrix Cloud.

16. Después de cargar el certificado, utilice todas las demás opciones predeterminadas:



17. A continuación, debe asegurarse de que `appuser.userName` esté definido en **Directory-Integrations > Active Directory -> Provisiong**> To okta.



> **Nota:**
>
> A veces, debes usar `user.cip_upn`, en `appuser.cip_upn`su lugar . Asegúrese de verificar la definición de su aplicación en la integración de OKTA, como se muestra en esta imagen.

18. Ahora debes intentar añadir usuarios de Okta a esta aplicación SAML. Puede asignar usuarios de varias formas.

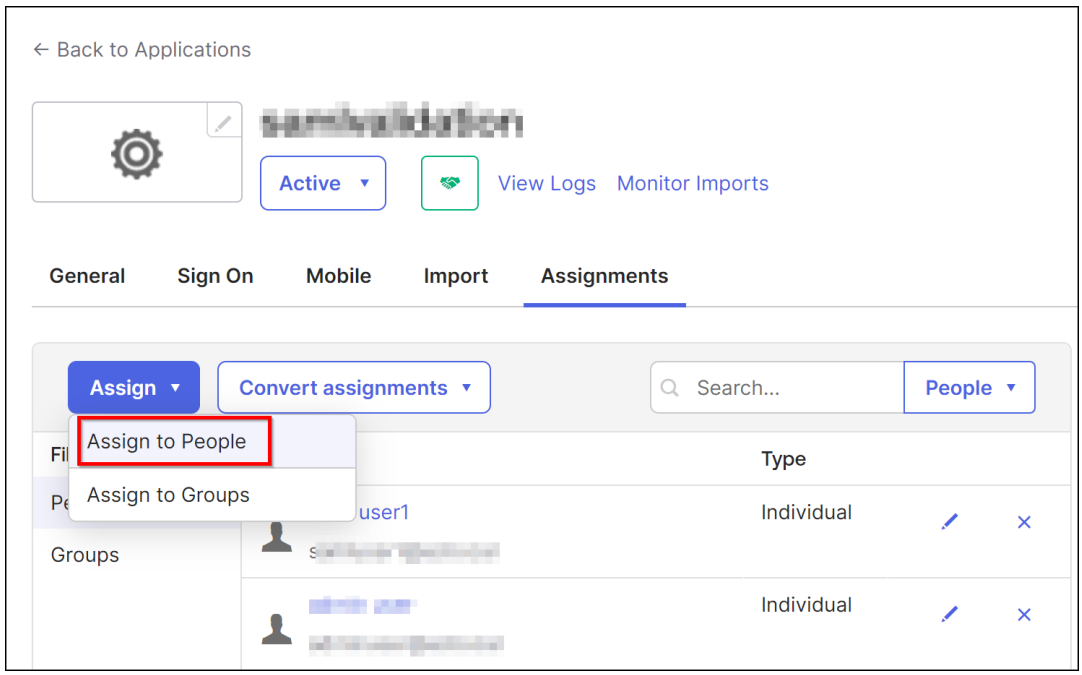
    Método 1:

    a) Inicie sesión en Okta con las credenciales de administrador

    b) Navegue hasta **Aplicaciones > Aplicaciones**

    c) Selecciona la aplicación SAML que creaste

    d) Haga clic en **Asignar > Asignar a personas**



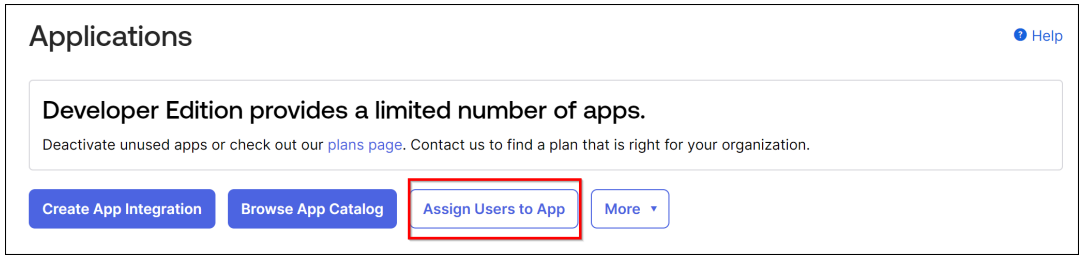
e) Haz clic en **Asignar** y, a continuación , selecciona **Guardar y volver** .

f) Haga clic en **Listo**.

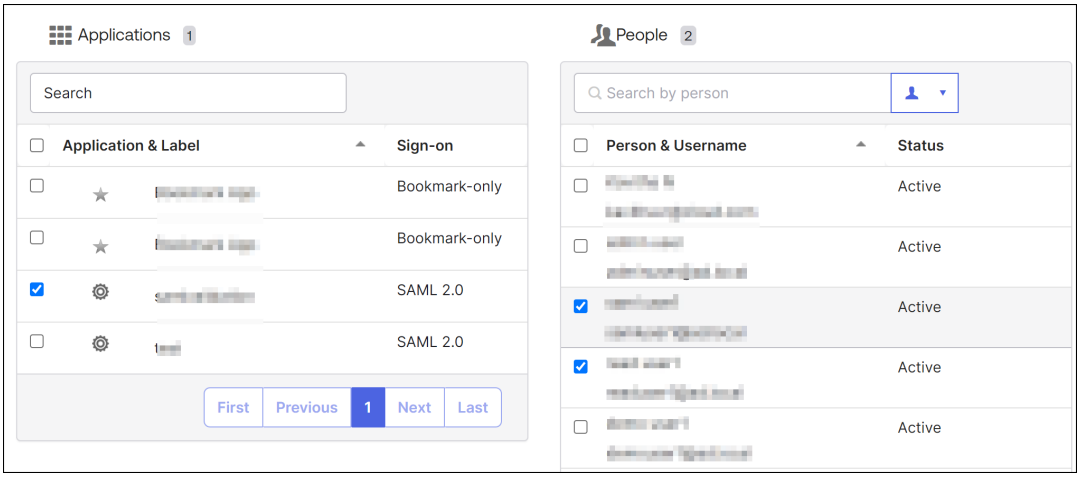
Método 2:

a) Navegue hasta **Aplicaciones > Aplicaciones**.

b) Haga clic en **Asignar usuarios a la aplicación**.



c) Seleccione la aplicación y los usuarios y, a continuación, haga clic en **Siguiente**.



d) Haz clic en **Confirmar asignaciones**.

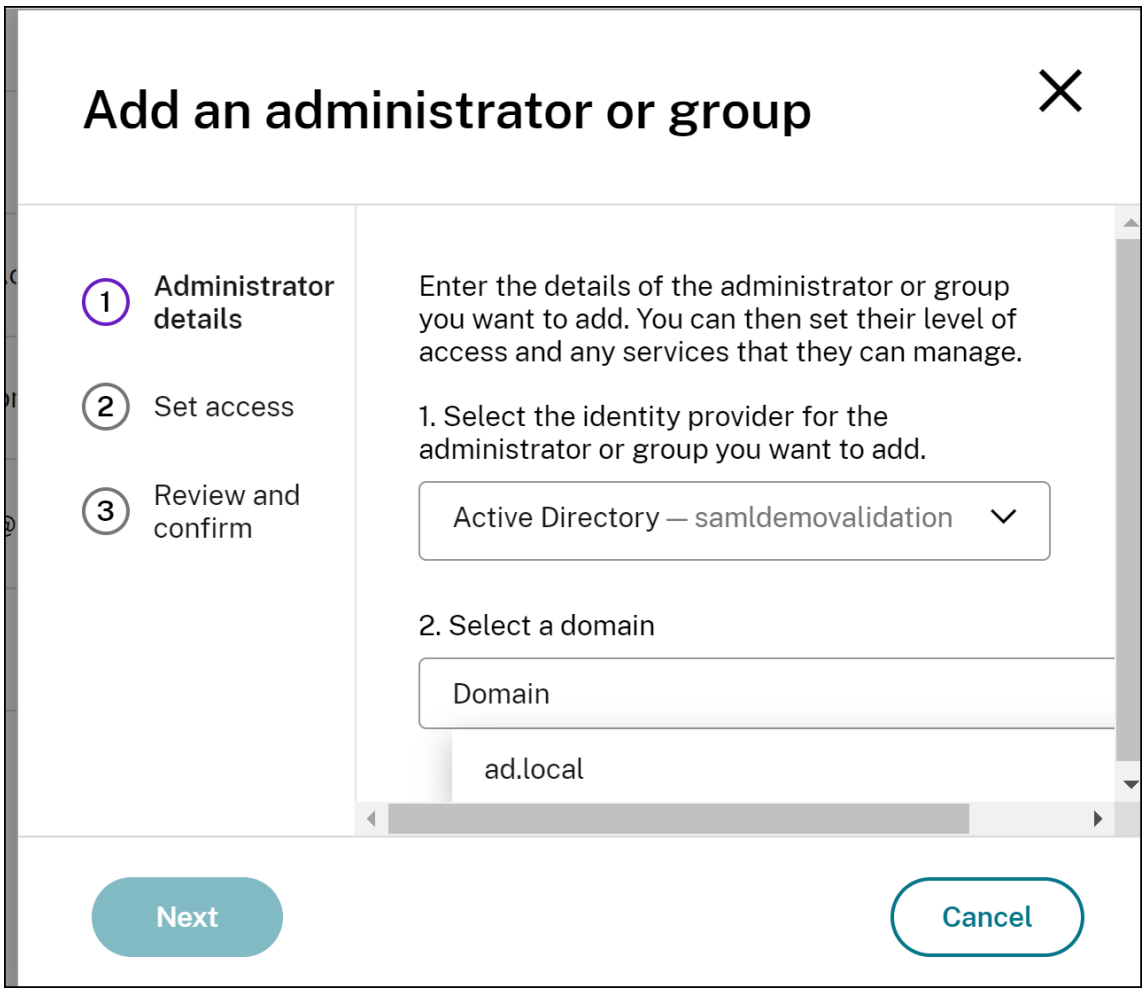
Método 3:

a) Navega hasta **Directorio > Personas**.

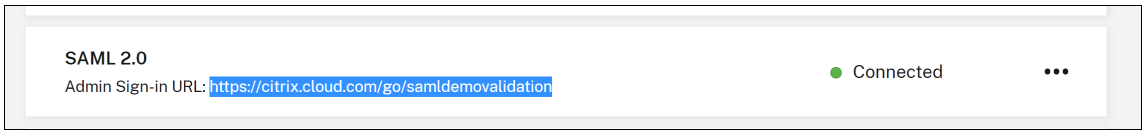
b) Selecciona cualquier usuario.

c) Haga clic en **Asignar aplicaciones** y asigne la aplicación SAML al usuario.

19. Después de asignar usuarios, inicie sesión en Citrix Cloud.
20. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
21. En la pestaña **Administradores** , haga clic en **Agregar administrador/grupo** .
22. Seleccione **Active Directory ([nombre de su aplicación SAML]**) de la lista, seleccione el dominio y, a continuación, haga clic en **Siguiente** .



23. Especifique los permisos de acceso.
24. Revisa si todo está correcto y haz clic en **Enviar invitación**.
25. En la pestaña **Autenticación** , puede ver la URL de inicio de sesión de SAML 2.0. A continuación, se muestra un ejemplo:



Requisitos del sistema

July 17, 2024

Antes de empezar a usar NetScaler Console, debe revisar los requisitos de software, los requisitos del navegador, la información de los puertos, la información de la licencia y las limitaciones.

Exploradores web compatibles

Para acceder a NetScaler Console, la estación de trabajo debe tener un navegador web compatible.

Se admiten los siguientes exploradores.

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

Requisitos de instalación del agente

Instale y configure un agente en su entorno de red para permitir la comunicación entre la consola de NetScaler y las instancias administradas de su centro de datos. En el centro de datos local, puede instalar un agente en el servidor Citrix XenServer, VMware ESXi, Microsoft Hyper-V y Linux KVM.

Los requisitos del agente son los recursos informáticos virtuales que el hipervisor debe proporcionar a cada agente. En la siguiente tabla se enumeran los requisitos del agente para aprovechar todas las funciones de NetScaler Console:

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

Los requisitos del agente para utilizar solo la función de licencias agrupadas, consulte Agente ligero para obtener licencias agrupadas.

También puede instalar un agente en Microsoft Azure o AWS o Google Cloud. Citrix recomienda usar los siguientes tipos de máquinas virtuales de los respectivos mercados de nube para aprovechar todas las funciones de NetScaler Console:

Cloud	Requisitos del agente	Tipo de máquina virtual preferido
AWS	8 CPU virtual, 32 GB de RAM y 30 GB de espacio de almacenamiento	`m4.2xlarge`
Microsoft Azure	8 CPU virtual, 32 GB de RAM y 30 GB de espacio de almacenamiento	`Standard_D8s_v3`
Google Cloud	8 CPU virtual, 32 GB de RAM y 30 GB de espacio de almacenamiento	`e2-standard-8`

> **Notas:**
>
> Azure ya no admitirá la escalabilidad horizontal para los agentes con las versiones 13.0 y 13.1 del instalador básico a partir del 23 de julio de 2024.
>
> Para los agentes de NetScaler:
>
> - Los agentes de NetScaler con 8 CPU virtuales, 32 GB de RAM y 30 GB de espacio de almacenamiento no se ven afectados. Estos agentes pueden someterse a actualizaciones sin interrupciones.
> - Las implementaciones iniciadas con la versión 14.1 tampoco se ven afectadas.
>
> Para agentes ligeros:
>
> - Los agentes ligeros con 4 CPU virtuales, 8 GB de RAM y 30 GB de espacio de almacenamiento que utilizan las versiones 13.0 o 13.1 del instalador básico no pueden escalar (aumentar la CPU o la RAM) después de la fecha de caducidad.
> - Para ampliar los agentes ligeros en el futuro, vuelva a aprovisionar un nuevo agente con la versión más reciente.

Para obtener instrucciones acerca de la instalación de un agente, consulte los siguientes vínculos:

- Instalar un agente en Microsoft Azure Cloud.
- Instalar un agente en AWS.
- Instalar un agente en Google Cloud.

Agente ligero para licencias agrupadas

Si planea usar la consola de NetScaler solo para licencias agrupadas, puede usar un agente con especificaciones más bajas, tal y como se indica en la tabla siguiente:

Componente	Requisito
RAM	8 GB
CPU virtual	4
Espacio de almacenamiento	30 GB

Estos agentes con especificaciones más bajas (ligeras) solo se admiten en NetScaler Console.

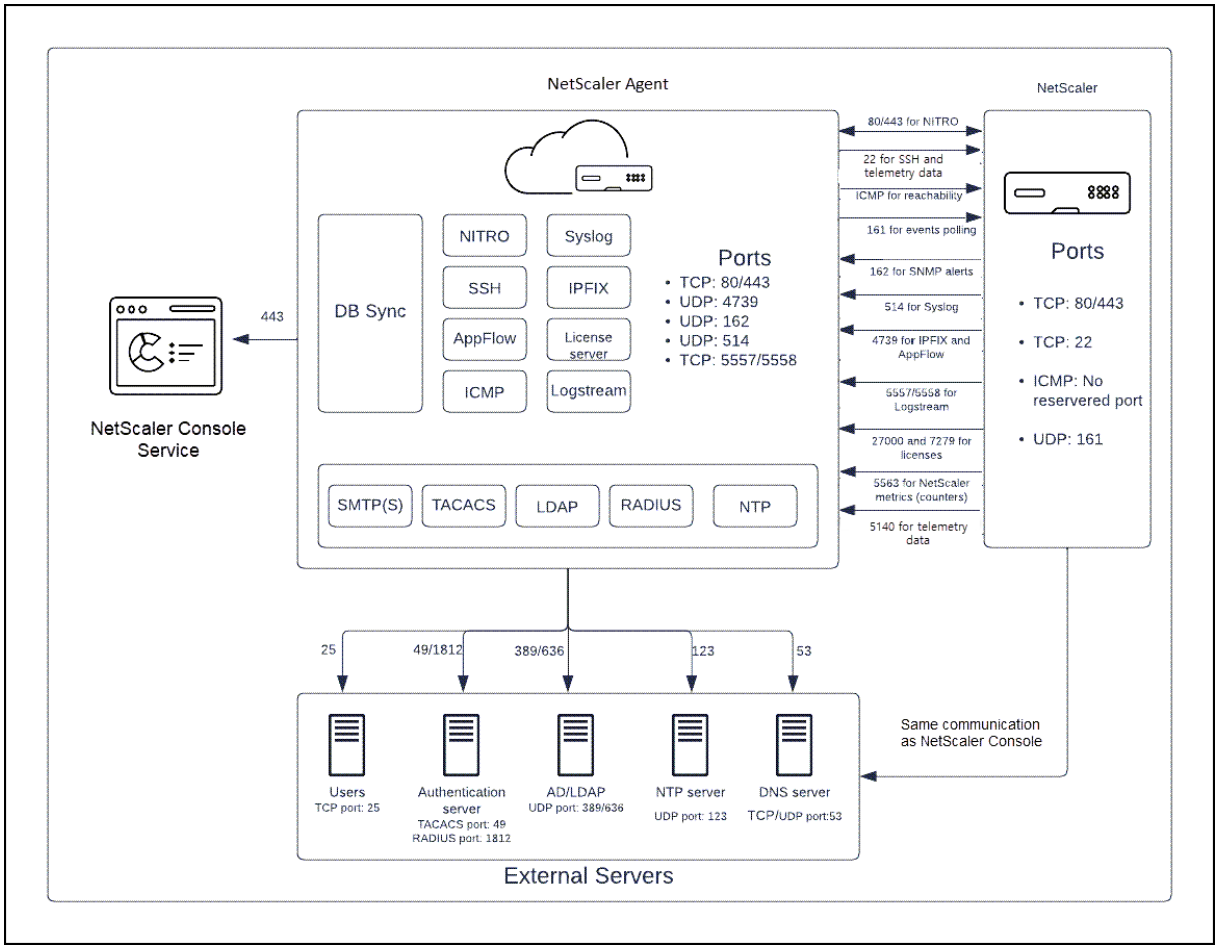
Citrix recomienda utilizar los siguientes tipos de máquinas virtuales de los respectivos mercados en la nube para utilizar únicamente la función de licencias agrupadas:

Cloud	Requisitos del agente	Tipo de máquina virtual preferido
AWS	4 CPU virtual, 8 GB de RAM y 30 GB de espacio de almacenamiento	`m4.xlarge`. Este tipo de instancia proporciona 4 CPU virtual, 16 GB de RAM y 30 GB de espacio de almacenamiento. Citrix recomienda este tipo de instancia, ya que coincide con la mayoría de los requisitos del agente entre los tipos de instancia existentes.
Microsoft Azure	4 CPU virtual, 8 GB de RAM y 30 GB de espacio de almacenamiento	`Standard_F4s_v2`
Google Cloud	4 CPU virtual, 8 GB de RAM y 30 GB de espacio de almacenamiento	`e2-standard-4`

> **Nota**
>
> Para inhabilitar la programación de tareas predeterminada, vaya a **Configuración > Configuración global > Funciones configurables**.

Puertos compatibles

Para las comunicaciones entre las instancias de NetScaler y el agente, abra los puertos necesarios.



Puertos para el agente de NetScaler

En esta tabla se explican los puertos necesarios que deben estar abiertos en el agente.

Puerto	Tipo	Detalles	Dirección de comunicación
80/443	TCP	Para la comunicación NITRO desde el servicio NetScaler Console a NetScaler.	Agente de NetScaler a NetScaler y de NetScaler a agente de NetScaler
4739	UDP	Para la comunicación de AppFlow entre NetScaler y el servicio NetScaler Console.	Agente de NetScaler a NetScaler

Puerto	Tipo	Detalles	Dirección de comunicación
162	UDP	Para recibir eventos SNMP de la instancia de NetScaler al servicio NetScaler Console.	Agente de NetScaler a NetScaler
514	UDP	Para recibir mensajes de syslog de la instancia de NetScaler al servicio NetScaler Console.	Agente de NetScaler a NetScaler
5563	TCP	Este puerto es necesario para que se ejecute el servicio NetScaler Console Collector. Para recibir las métricas (contadores) de NetScaler desde la instancia de NetScaler a la consola de NetScaler.	De NetScaler a NetScaler Console
5557/5558	TCP	Para la comunicación de logstream (para WAF Security Violations, Web Insight y HDX Insight) desde NetScaler al servicio NetScaler Console.	De NetScaler al agente de NetScaler
27000 y 7279	TCP	Puertos de licencia para la comunicación entre el agente de NetScaler y la instancia de NetScaler. Estos puertos también se utilizan para las licencias agrupadas de NetScaler.	Agente de NetScaler a NetScaler

Puerto	Tipo	Detalles	Dirección de comunicación
443	TCP	Puertos para la comunicación entre el agente NetScaler y el servicio NetScaler Console	Servicio del agente NetScaler a la consola NetScaler
5140	UDP	Puerto para recibir datos de telemetría de NetScaler Gateway	De NetScaler a NetScaler Console

Puertos para instancias de NetScaler

En esta tabla se explican los puertos obligatorios que deben estar abiertos en las instancias de NetScaler.

Puerto	Tipo	Detalles	Dirección de comunicación
80/443	TCP	Para la comunicación NITRO desde la consola de NetScaler a la instancia de NetScaler.	Agente de NetScaler a NetScaler y de NetScaler a agente de NetScaler
22	TCP	Para la comunicación SSH entre el agente y NetScaler. **Nota:** Este puerto también se usa para la telemetría de NetScaler.	Agente de NetScaler a NetScaler
Sin puerto reservado	ICMP	Para detectar la accesibilidad de la red entre el agente de NetScaler y las instancias de NetScaler.	Agente de NetScaler a NetScaler

Puerto	Tipo	Detalles	Dirección de comunicación
161	UDP	Para sondear los eventos de las instancias de NetScaler.	Agente de NetScaler a NetScaler

Puertos para el agente integrado de NetScaler

En esta tabla se explican los puertos necesarios que deben ser para el agente integrado de NetScaler.

Puerto	Tipo	Detalles	Dirección de comunicación
443	TCP	Para la comunicación NITRO desde la consola de NetScaler a la instancia de NetScaler.	Agente integrado de NetScaler Console a NetScaler y agente integrado de NetScaler a NetScaler Console

> **Nota**
>
> El punto final del servicio de NetScaler Console es el mismo que el de la «URL del servicio» que se generó al intentar registrar el agente. El agente usa la URL del servicio para localizar la consola de NetScaler.

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 servicio:

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
```

- Conectividad con Citrix Cloud:


```
citrix.cloud.com
accounts.cloud.com
```

FQDN obsoletos

Algunos FQDN están en desuso para el uso siguiente de la consola de NetScaler. Para ayudarle a cambiar a los nuevos FQDN sin ninguna interrupción, los FQDN obsoletos continúan funcionando durante algún tiempo y se eliminarán lentamente.

Terminales de consola NetScaler	FQDN antiguo	Nuevo FQDN
Acceso a la interfaz de usuario de la consola NetScaler	`netscalermas.cloud.com`	`adm.cloud.com`
URL de servicio	`agent.netscalermgmt.net`	`*.agent.adm.cloud.com` **Nota**: El valor de * dependerá del PoP (punto de presencia) que estén disponibles sus datos.
Interacciones de API	`netscalermas.cloud.com`	`api.adm.cloud.com`

Se requieren versiones mínimas de NetScaler

> Nota
>
> Las versiones 10.5, 11.0 y 12.0 de NetScaler ya han alcanzado el fin de vida (EOL). Para obtener más información, consulte la Tabla de productos. La versión recomendada de NetScaler es la 12.1.

Función de consola NetScaler	Versión del software NetScaler
StyleBooks	10.5 y versiones posteriores
Supervisión, generación de informes y configuración mediante trabajos Análisis	10.5 y versiones posteriores
HDX Insight	10.1 y versiones posteriores

Función de consola NetScaler	Versión del software NetScaler
Gateway Insight	11.0.65.31 y posteriores
Security Insight	11.0.65.31 y posteriores

Requisitos para la solución NetScaler Console Analytics

Se requieren versiones mínimas de Citrix Virtual Apps and Desktops

Función de consola NetScaler	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 Console no admite dispositivos Access Gateway Standard independientes.

La consola NetScaler puede generar informes para las aplicaciones que se publican en una aplicación o escritorio virtual de Citrix y a las que se accede a través de Citrix Workspace. Sin embargo, esta capacidad depende del sistema operativo en el que esté instalado Citrix 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 HDX Insight

NetScaler Console admite los siguientes clientes ligeros para supervisar las instancias de NetScaler que se ejecutan en la versión de software 11.0 Build 65.31 y versiones posteriores:

- 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

Se requiere una licencia de instancia NetScaler para HDX Insight

Los datos recopilados por NetScaler Console para HDX Insight dependen de la versión y las licencias instaladas de las instancias de NetScaler que se supervisen. Los informes de HDX Insight solo se mues-

tran para los dispositivos NetScaler Premium y Enterprise que se ejecutan en la versión 10.5 y posteriores del software.

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

Sistemas operativos compatibles y versiones de Citrix Workspace

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

Sistema operativo	Versión de Citrix 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

Licencias

March 6, 2024

A partir de la versión 14.1-21.x del servicio NetScaler Console, se elimina el concepto de VIP con licencia. Ahora hay un número ilimitado de VIP disponibles en el servicio NetScaler Console. Ya no tiene que comprar licencias de servidor virtual de NetScaler Console porque el SKU de la licencia VIP finalizará la venta (EOS) y la renovación (EOR) en breve.

Los cambios en el almacenamiento de servicios de NetScaler Console son los siguientes:

- La SKU de almacenamiento del servicio de NetScaler Console finalizará la venta (EOS) y la renovación (EOR) en breve.
- El derecho de almacenamiento predeterminado del servicio NetScaler Console ahora es de 5 GB.
- Todos los servicios de almacenamiento de NetScaler Console adquiridos en el pasado se respetarán hasta que finalice el plazo.
- Todas las licencias VIP de NetScaler Console adquiridas en el pasado que le dieran derecho a un derecho proporcional de almacenamiento de servicios de NetScaler Console se respetarán hasta que finalice el plazo.
- Si compra un paquete diferente que le da derecho a un derecho de almacenamiento de NetScaler Console superior, los 5 GB predeterminados se cambian para que coincidan con el derecho.

> **Nota:**
>
> Si ha adquirido un servidor virtual anteriormente, se aplican 500 MB de almacenamiento por servidor virtual hasta el final del período de suscripción.

Se requieren licencias de NetScaler para las funciones de NetScaler Console

En la siguiente tabla se enumeran las licencias de NetScaler que se requieren para utilizar algunas de las funciones de NetScaler Console.

Grupo de funciones de NetScaler Console	Características de la consola NetScaler	Requisito de licencia de NetScaler y Gateway
Análisis	HDX Insight	Avanzado (informes < 1 hora) Premium (informes = Ilimitado)
Análisis	Security Insight	Licencia Premium (o) Avanzada con App Firewall
Análisis	Gateway Insight	Avanzado (informes < 1 hora) Premium (informes = Ilimitado)
Aplicaciones	Estadísticas de aplicaciones (Panel de aplicaciones, Panel de seguridad de aplicaciones)	La información relacionada con NetScaler Web App Firewall en el panel de aplicaciones y el panel de seguridad de aplicaciones necesita una licencia Premium (o) Advanced con App Firewall
Aplicaciones	Puerta de enlace de la API	Licencia Premium (o) Avanzada
Aplicaciones	StyleBooks	N/D

Grupo de funciones de NetScaler Console	Características de la consola NetScaler	Requisito de licencia de NetScaler y Gateway
Aplicaciones	Administración de inventario: panel de infraestructura, grupos de instancias, paneles de instancias y sitios	N/D
Aplicaciones	Administración de eventos y Syslog	N/D
Aplicaciones	Trabajos de configuración, auditoría de configuración y consejos de configuración	N/D
Aplicaciones	Informes de red (a nivel de instancia)	N/D
Aplicaciones	Informes de red (a nivel de servidor virtual)	N/D
Aplicaciones	Funciones de red (visibilidad y administración sencillas de servidores virtuales, servicios, grupos de servicios y servidores)	N/D
Aplicaciones	Administración de certificados SSL (a nivel de instancia)	N/D
Aplicaciones	Administración de certificados SSL (a nivel de servidor virtual)	N/D
Sistema	RBAC y autenticación externa (nivel de instancia)	N/D
Sistema	RBAC y autenticación externa (nivel de servidor virtual)	N/D

Ver comprobaciones de caducidad de suscripciones a servidores virtuales

Puede ver el estado de las licencias instaladas con la fecha de caducidad y el límite de almacenamiento permitido para las licencias en NetScaler Console.

Para ver el estado de las licencias:

1. Ve a **Cuenta** > **Suscripciones**.
2. En la **sección Derechos**, puede ver los detalles de los servidores virtuales con licencia y los días de caducidad:

- **Servidores virtuales autorizados:** número de servidores virtuales disponibles para licenciar.
- **Servidores virtuales de terceros autorizados:** número de servidores virtuales de terceros que puede administrar con la licencia.
- **Almacenamiento autorizado:** límite de almacenamiento de la licencia.
- **Días hasta el vencimiento:** número de días restantes antes del vencimiento de la licencia.

Ver el tipo de análisis habilitado en los servidores virtuales

Después de habilitar AppFlow en los servidores virtuales seleccionados, puede ver el tipo de análisis habilitado en los servidores virtuales con licencia o en los servidores virtuales de terceros desde la página **Suscripciones**.

1. Vaya a **Cuenta > Suscripciones**.
2. En la sección **Resumen de análisis de servidores virtuales**, seleccione el tipo de servidores virtuales con licencia.
3. La página de servidores virtuales con licencia muestra la lista de servidores virtuales con licencia. En esta página, la columna **Estado del análisis** muestra el tipo de análisis habilitado en los servidores virtuales.

Asesoramiento de actualización

January 26, 2024

Como administrador de red, puede administrar muchas instancias de NetScaler que se ejecutan en diferentes versiones de NetScaler en NetScaler Console. Supervisar el ciclo de vida de cada instancia de NetScaler puede ser una tarea engorrosa. Debe visitar la matriz de productos de NetScaler e identificar las instancias de NetScaler que están llegando o están llegando al final del ciclo de vida (EOL) o al final del mantenimiento (EOM). Luego, planea su actualización.

Para facilitar este proceso, el asesoramiento de actualización de NetScaler Console le ayuda a supervisar el ciclo de vida de sus instancias de NetScaler de las siguientes maneras:

- Identifica las instancias que alcanzan o alcanzan la EOL o la MOE. Por lo tanto, puede planificar las actualizaciones de NetScaler antes de la fecha de EOL o EOM.
- Resalta las instancias que no están en la versión o compilación más recientes. Puede actualizar estas instancias a la versión más reciente o compilación. Con esta actualización, recibirá actualizaciones sobre nuevas características y problemas solucionados.

- Destaca las instancias que no están en las compilaciones preferidas de NetScaler. Es posible que algunas organizaciones tengan compilaciones de NetScaler preferidas para sus instancias. En NetScaler Console, puede establecer la versión preferida para su organización en función de la estabilidad de la construcción, las funciones y otras consideraciones. A continuación, revise y actualice las instancias que no están en compilaciones preferidas. Las instancias que ejecutan las compilaciones preferidas se indican con un icono de estrella.
- Resalta instancias que se ejecutan en las versiones o compilaciones más populares. Las instancias que ejecutan las compilaciones populares se indican con un icono de cinta de opciones.

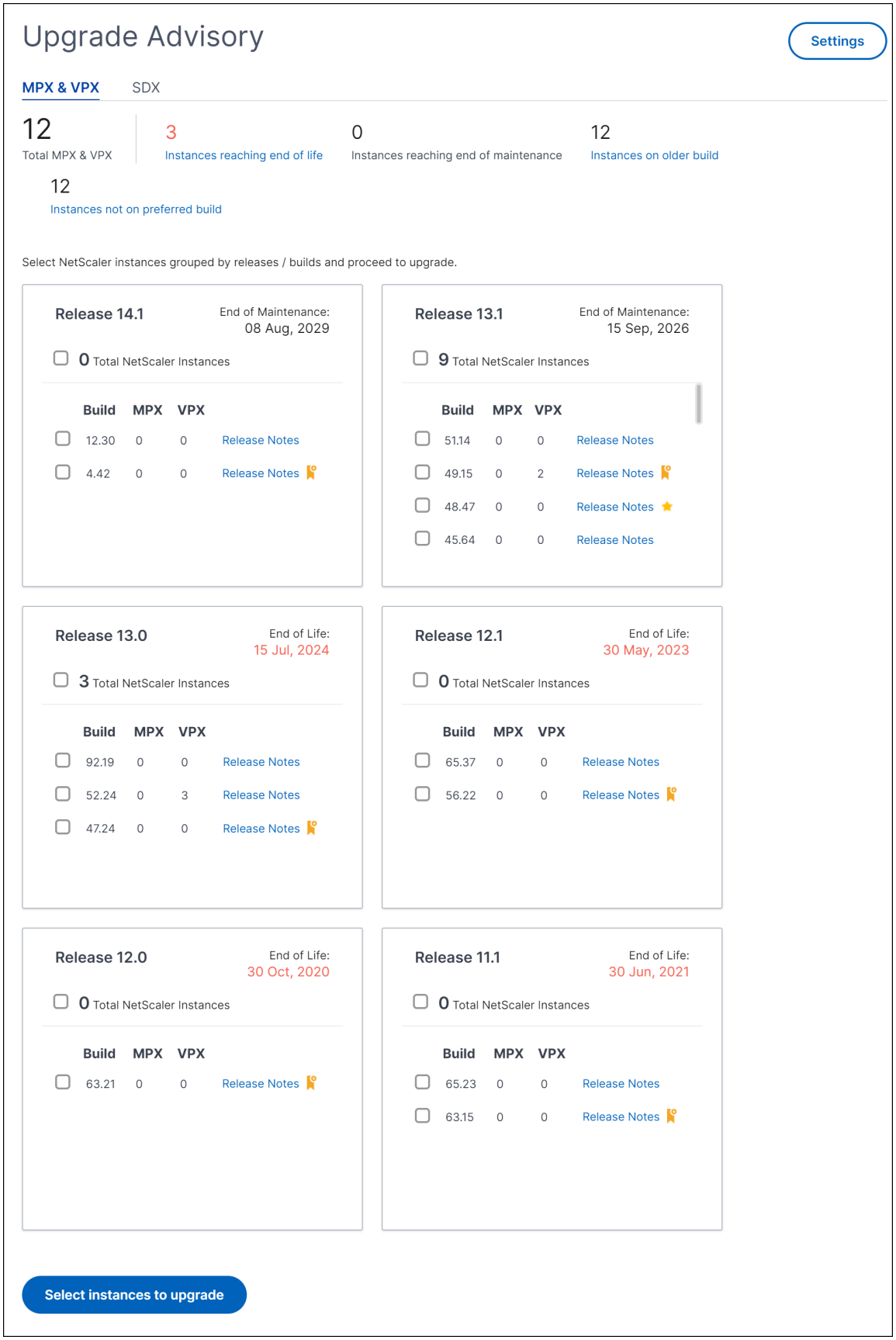
El aviso de actualización proporciona vínculos a las notas de la versión correspondientes. Con esta información, puede revisar y decidir qué versión de NetScaler necesita actualizarse. Puede continuar con la creación de un trabajo de mantenimiento para actualizar las instancias de NetScaler desde la página de asesoramiento sobre actualizaciones.

> **Importante** el aviso de actualización solo monitorea el EOL de las versiones del software NetScaler. No comprueba el EOL de los dispositivos NetScaler.

Consultar el aviso de actualización

Navegue por **Infraestructura > Asesoramiento de instancias > Asesoramiento de actualizaciones** y consulte la siguiente información:

- Recuento total de instancias de NetScaler.
- Instancias que llegan al final de la vida.
- Instancias que llegan al final del mantenimiento.
- Instancias en compilación anterior.
- Las instancias no están en la compilación preferida.
- Fechas de fin de ciclo y fin de mantenimiento de las distintas versiones de NetScaler.

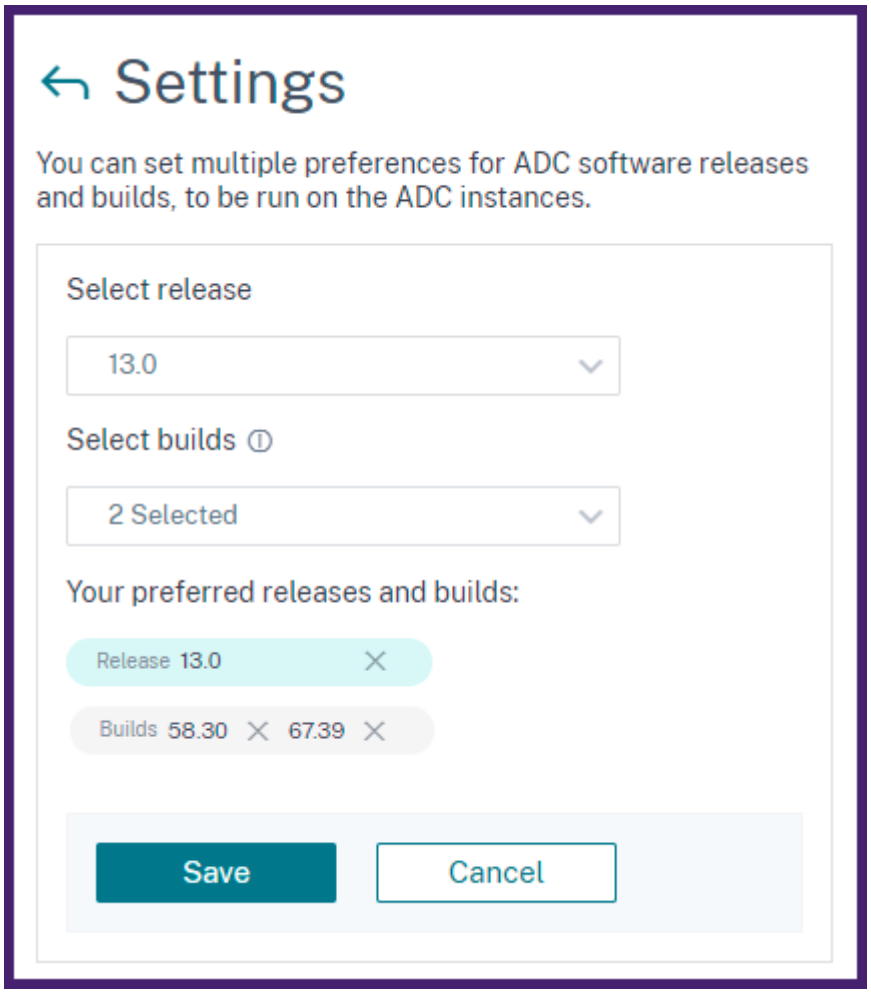


La página de **asesoramiento sobre actualizaciones** agrupa las instancias de NetScaler según sus versiones. El enlace **Notas de la versión** lo guía a las notas de la versión específicas de NetScaler. Revise las nuevas características, problemas solucionados y conocidos antes de decidir actualizar. Puede seleccionar varias instancias de NetScaler en diferentes versiones para actualizarlas a la vez. Cuando se continúa con una actualización, se crea un trabajo de actualización. Consulte Actualizar instancias de NetScaler .

Establecer las compilaciones preferidas

Como administrador, puede definir la versión de NetScaler que prefiera para la organización. Haga lo siguiente para establecer la compilación preferida:

1. En **Infraestructura > Asesoramiento de instancias > Asesoramiento de actualización**, haga clic en **Configuración**.
2. Seleccione la versión preferida y la compilación.



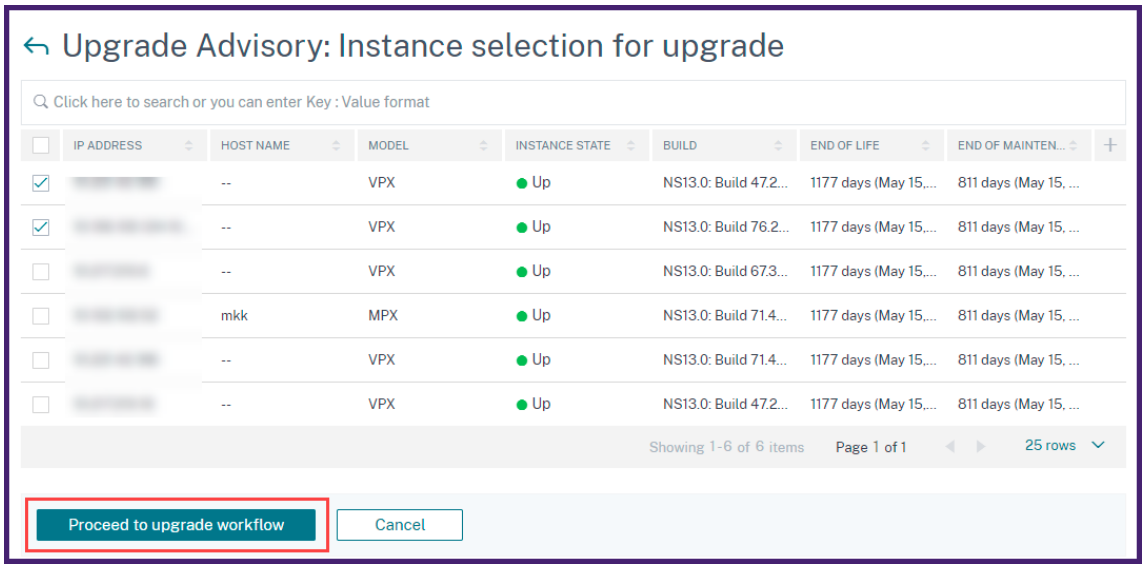
En este ejemplo, las compilaciones preferidas son `13.0-58.30` y `13.0-67.39`.

3. Haga clic en **Guardar**.

Actualizar instancias de NetScaler

En la página de **asesoramiento sobre actualizaciones** , tras su revisión, siga los pasos siguientes para actualizar las instancias de NetScaler necesarias:

1. Seleccione las compilaciones de instancias que quiere actualizar y haga clic en **Seleccionar instancias para actualizar**.
2. Seleccione la instancia de NetScaler que desea actualizar y haga clic en **Continuar para actualizar el flujo** de trabajo.



   Este flujo de trabajo crea un trabajo de actualización.

3. En la ficha **Seleccionar instancia**,

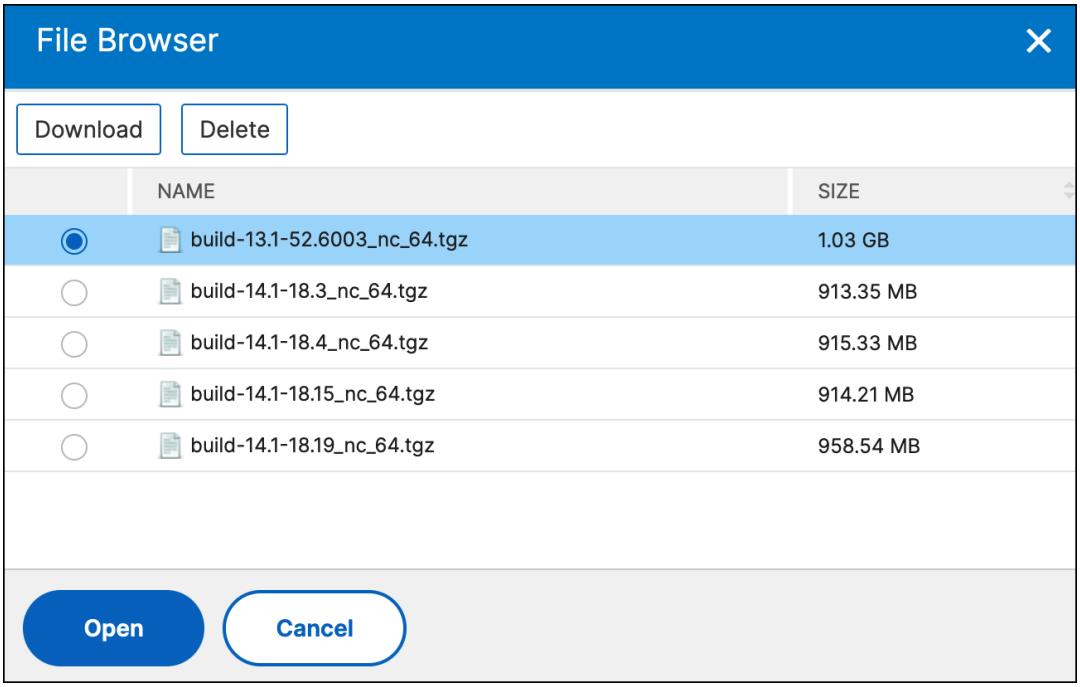
   a) Especifique un nombre para el trabajo de actualización.

   b) (Opcional) si quiere agregar otras instancias, haga clic en **Agregar instancias**.

   c) Haga clic en **Siguiente**.

4. En la pestaña **Seleccionar imagen** , seleccione una imagen de NetScaler de la biblioteca de imágenes, local o dispositivo.

   - **Seleccionar de la biblioteca**de imágenes: seleccione una imagen de NetScaler de la lista. Esta opción muestra todas las imágenes de NetScaler que están disponibles en el sitio web de descargas de NetScaler.



Las imágenes del software NetScaler muestran las compilaciones preferidas con el icono de estrella. Y, la mayoría de las compilaciones descargadas con el icono de marcador.

- **Seleccione entre local o dispositivo**: puede cargar la imagen desde su equipo local o desde el dispositivo NetScaler. Al seleccionar el dispositivo NetScaler, la GUI de NetScaler Console muestra los archivos de instancia que están presentes en `/var/mps/mps_images`. Seleccione la imagen en la GUI de NetScaler Console.
- **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.

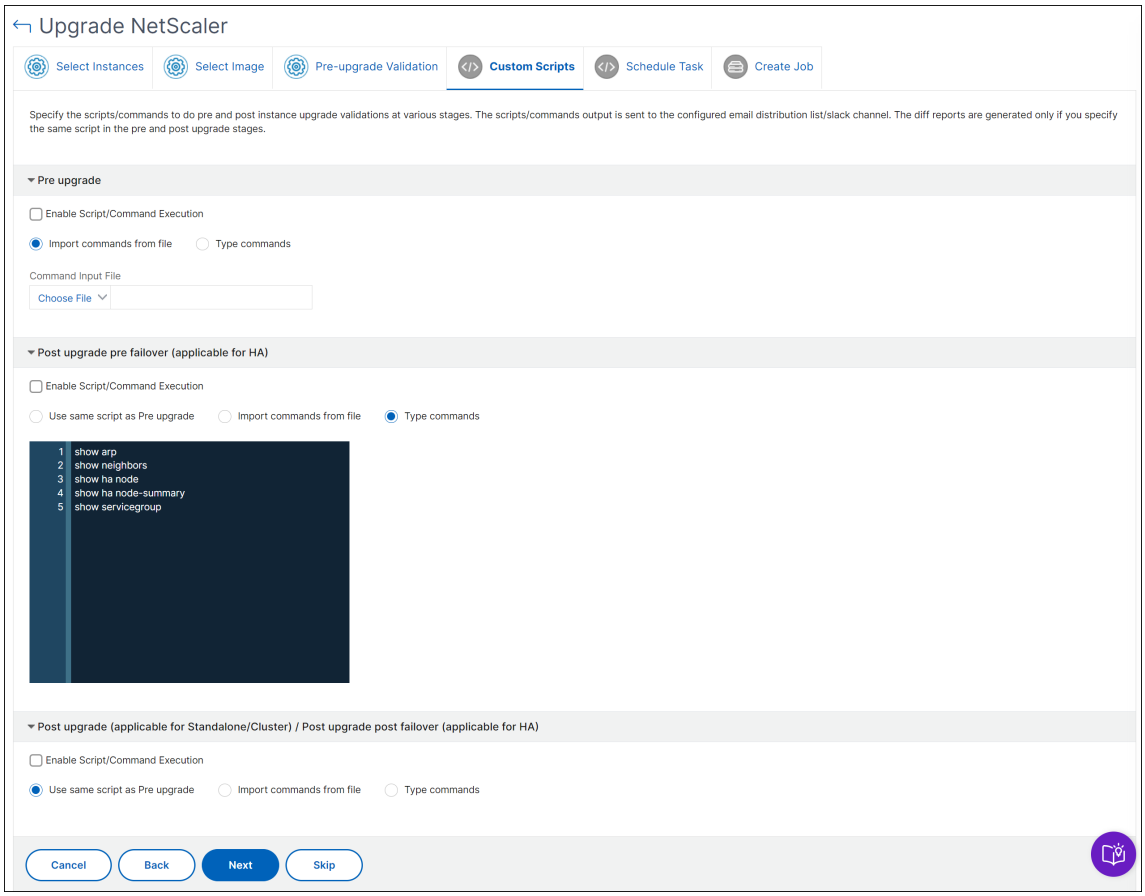
5. La ficha **Validación previa a la actualización** muestra las instancias fallidas. Puede quitar las instancias fallidas y hacer clic en **Siguiente**.

   - **Comprobación de espacio**en disco: 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 políticas : si NetScaler Console encuentra políticas clásicas no compatibles, puede eliminarlas para crear un trabajo de actualización.

> **Nota:**
>
> Si especifica la dirección IP del clúster, la consola de NetScaler realiza la validación previa a la actualización solo en la instancia especificada, no en los demás nodos del clúster.

6. Opcional, en la ficha **Scripts personalizados**, especifique los scripts que se ejecutarán antes y después de una actualización de instancia.

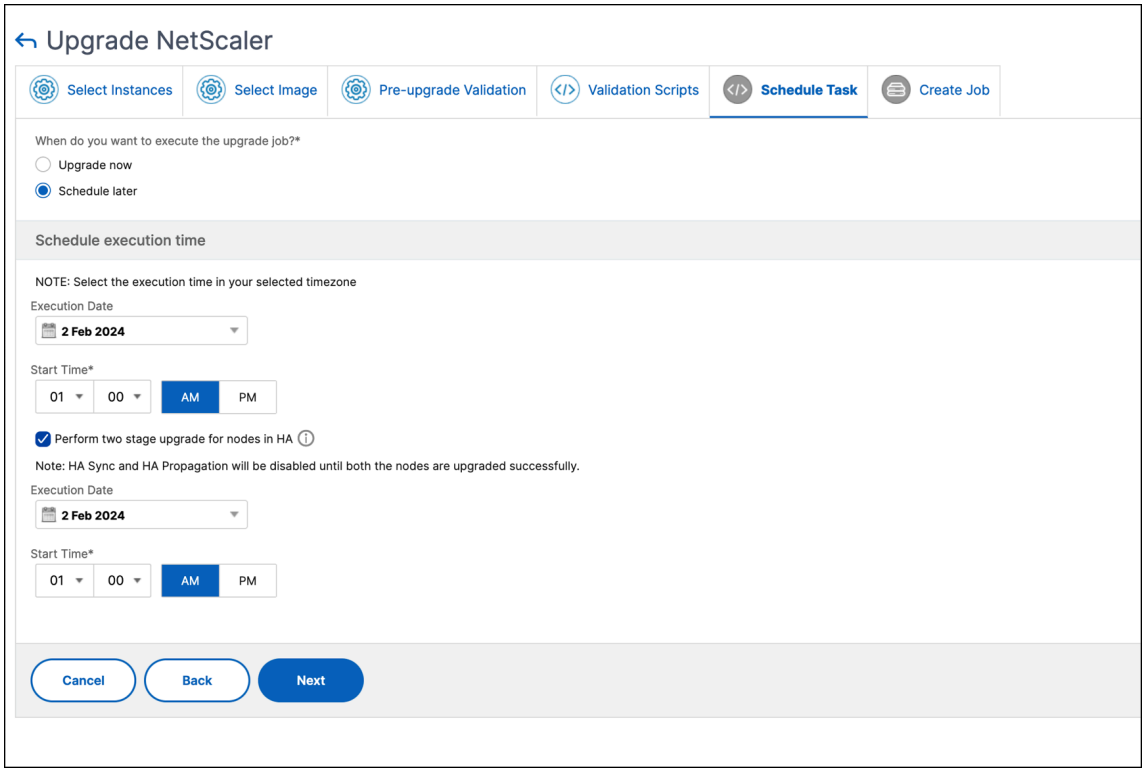


Para obtener más información, consulte Uso de scripts personalizados.

7. En **Programar 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 desea actualizar un par de alta disponibilidad de NetScaler en dos etapas, seleccione Realizar una actualización en dos etapas para los nodos de HA.



Para obtener más información, consulte Actualizar el par de alta disponibilidad de NetScaler .

8. En la ficha **Crear trabajo**, especifique los siguientes detalles:

   Si programa el trabajo de actualización, puede especificar cuándo quiere cargar la imagen en una instancia:

   - **Subir 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 obtener más información sobre las demás opciones, consulte Opciones de actualización de NetScaler .

Asesoramiento de seguridad

January 26, 2024

Una infraestructura segura, segura y resistente es la línea vital de cualquier organización. Aspectos destacados del asesoramiento de seguridad de NetScaler Console:

- **Detección y corrección de vulnerabilidades y exposiciones (CVE) comunes**: Le permite identificar las CVE que ponen en riesgo sus instancias de NetScaler y recomienda soluciones.
- **Supervisión de la integridad de los archivos**: Le permite identificar si se han realizado cambios o adiciones en los archivos de compilación de NetScaler.

Como administrador, debe asegurarse de:

- Realice un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE), evalúe el impacto de las CVE, comprenda la solución y resuelva las vulnerabilidades.
- Examine la integridad de los archivos de compilación de NetScaler.

Funciones de asesoramiento de seguridad

Las siguientes funciones de asesoramiento de seguridad le ayudan a proteger su infraestructura.

CVE:

Funciones	Descripción
Análisis del sistema	Analiza todas las instancias administradas de forma predeterminada una vez a la semana. NetScaler Console decide la fecha y la hora de los análisis del sistema y no puede cambiarlos.
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.
Informes CVE	Almacena copias de los últimos cinco escaneos. Puede descargar estos informes en formato CSV y analizarlos.

Funciones	Descripción
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.

Supervisión de la integridad de los archivos:

Funciones	Descripción
Escaneo bajo demanda	Debe ejecutar un análisis bajo demanda para obtener resultados sobre cualquier cambio de archivo detectado en los archivos de compilación de NetScaler.
Análisis de supervisión de integridad de archivos	Compara el valor de hash binario de los archivos de compilación actuales de NetScaler con el hash binario original y resalta si hay modificaciones o adiciones de archivos. Puede ver los resultados del análisis en la ficha **Control de integridad de archivos**.

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.
- Instancias compatibles con la supervisión de la integridad de los archivos: Instancias de MPX, VPX y Gateway.
- CVE compatibles: todos los CVE posteriores a diciembre de 2019.

> **Nota:**
>
> El aviso de seguridad de NetScaler Console no admite la detección y reparación de las vulnerabilidades que afectan al complemento 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 Console no tiene en cuenta ningún tipo de error de configuración de las funciones al identificar la vulnerabilidad.
- El aviso de seguridad de NetScaler Console solo admite la identificación y la corrección de 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 que NetScaler Console compare la versión de una instancia de NetScaler con las versiones y compilaciones en las que está disponible la solución. Esta comparación de versiones ayuda al asesoramiento de seguridad de NetScaler Console a identificar si el NetScaler es vulnerable al 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 Console haga coincidir 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 Console se conecte con la instancia de NetScaler gestionada, inserte un script en ella y ejecute el script. La salida del script ayuda a NetScaler Console a identificar si el 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.

- El siguiente análisis está disponible para la supervisión de la integridad de los archivos:
  - **Análisis de supervisión de**la integridad de los archivos : este análisis necesita que la consola de NetScaler se conecte con la instancia de NetScaler gestionada. NetScaler Console compara los valores hash ejecutando un script en NetScaler y recopilando los valores hash binarios actuales para los archivos de compilación de NetScaler. Tras la comparación, NetScaler Console proporciona el resultado con el número total de archivos existentes modificados y el número total de archivos recién agregados. Como administrador, puede ponerse en contacto con el departamento forense digital de su organización para investigar más a fondo los resultados del escaneo.

    Se escanean los siguientes archivos:

    * `/netscaler`
    * `/bin`, `/sbin`, `/usr/bin`, `/usr/sbin`, `/usr/local/bin`, `/usr/local/sbin`
    * `/lib`, `/libexec`, `/usr/lib`, `/usr/libexec`, `/usr/local/lib`, `/usr/lib32`, `/compat`
    * `/etc`
    * El resto de `/usr`
    * `/root`, `/home`, `/mnt`

- 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 Console no admite la mitigación de CVE. Si ha aplicado la mitigación (solución temporal) a la instancia de NetScaler, la consola de NetScaler seguirá identificando el NetScaler como un NetScaler vulnerable hasta que haya completado la corrección.
- Para las instancias de FIPS, no se admite el escaneo CVE, pero sí el escaneo de supervisión de integridad de archivos.
- Algunos cambios en los archivos pueden producirse como parte del funcionamiento normal del dispositivo, mientras que otros pueden requerir una investigación más profunda. Al revisar los cambios en los archivos, lo siguiente puede resultar útil:
  - Es posible que se produzcan cambios en el directorio `/netscaler` (en los **archivos.html** y **.js**) debido al uso de scripts o complementos.

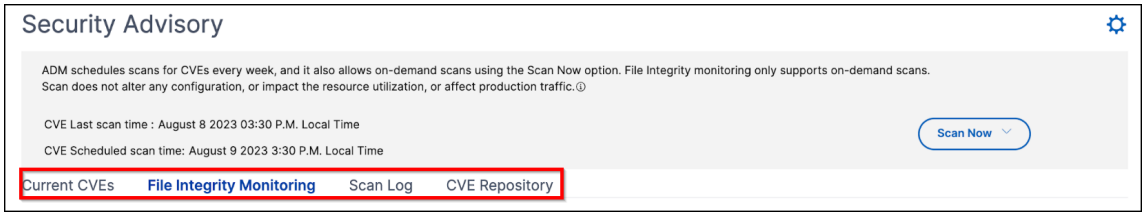
- El directorio /etc incluye archivos de configuración que pueden modificarse por una intervención inesperada después de arrancar el sistema.
- Sería inusual que hubiera:
  * Informes en los directorios /bin, /sbin o /lib
  * Nuevos archivos.php en el directorio /netscaler

Cómo utilizar el panel de asesoría de seguridad

Para acceder al panel de **asesoramiento de seguridad** , desde la GUI de NetScaler Console, vaya a **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**.

El panel de mandos incluye cuatro fichas:

- CVE actuales
- Supervisión de la integridad de los archivos
- 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 > Analizar CVE** 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.

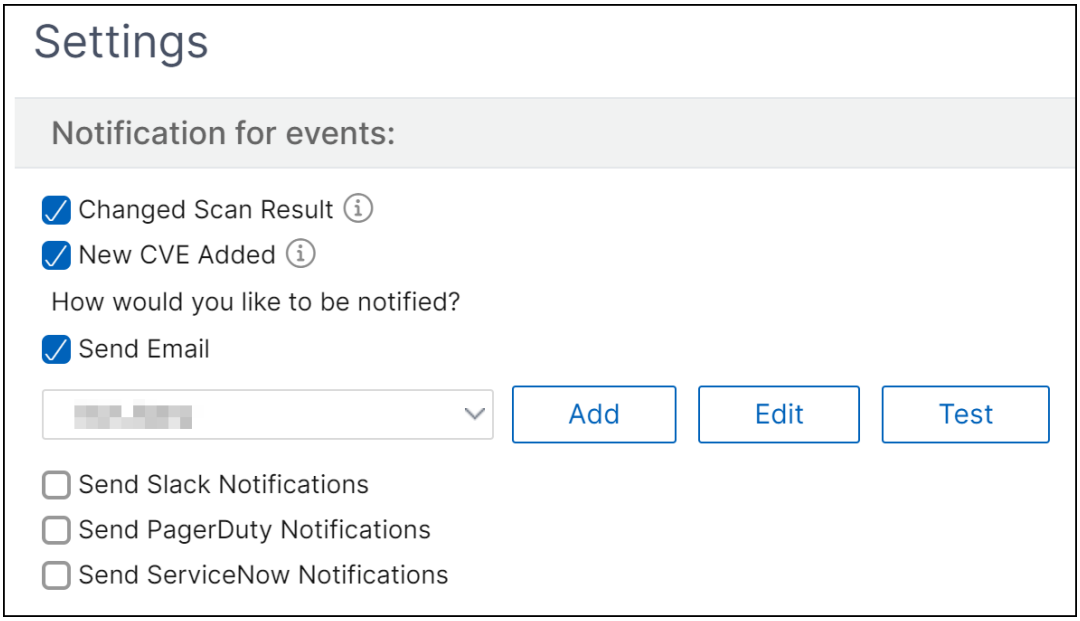
En la esquina superior derecha del panel de control se encuentra el icono de configuración, que le permite:

- Habilite e inhabilite las notificaciones (aplicable solo para la detección de CVE).

  Puede recibir las siguientes notificaciones sobre el impacto de las CVE.

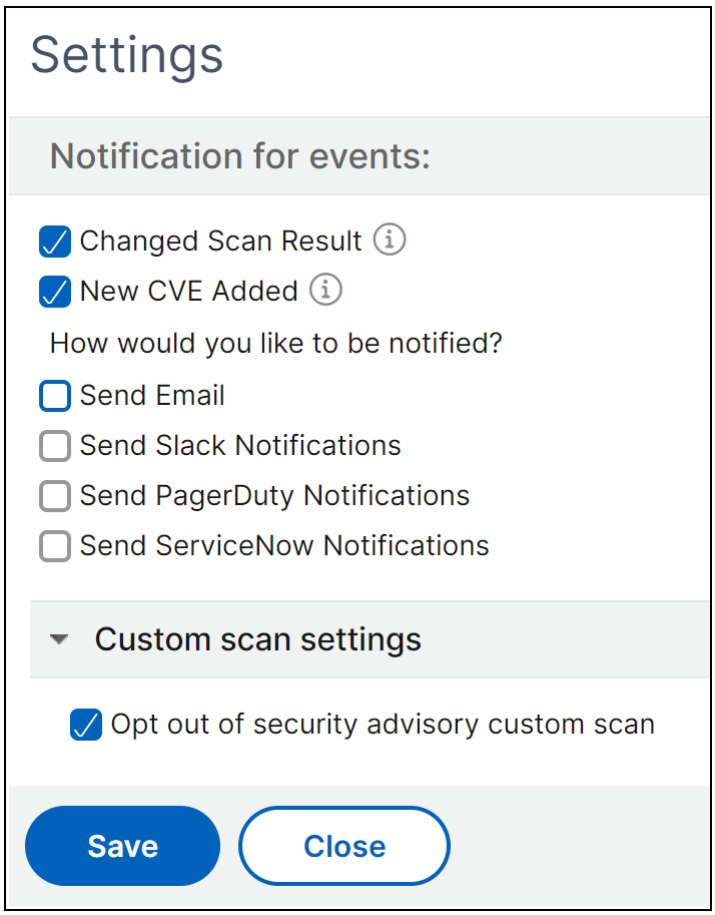
  - Notificaciones por correo electrónico, Slack, PagerDuty y ServiceNow sobre los cambios en los resultados del escaneo de CVE y los nuevos CVE que se agreguen al repositorio de CVE.

- Notificación en la nube para los cambios en los resultados del escaneo de impacto de CVE.



- Configurar los ajustes de escaneo personalizados (aplicable solo a los CVE)

  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.

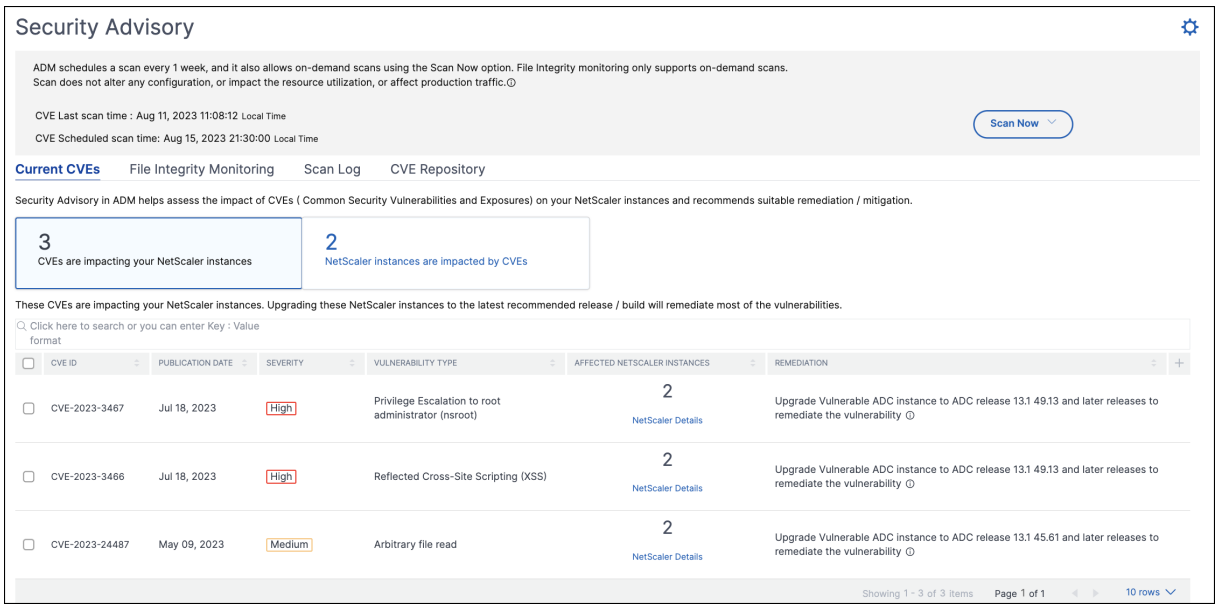
Tipo de vulnerabilidad: el tipo de vulnerabilidad de este CVE.

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.

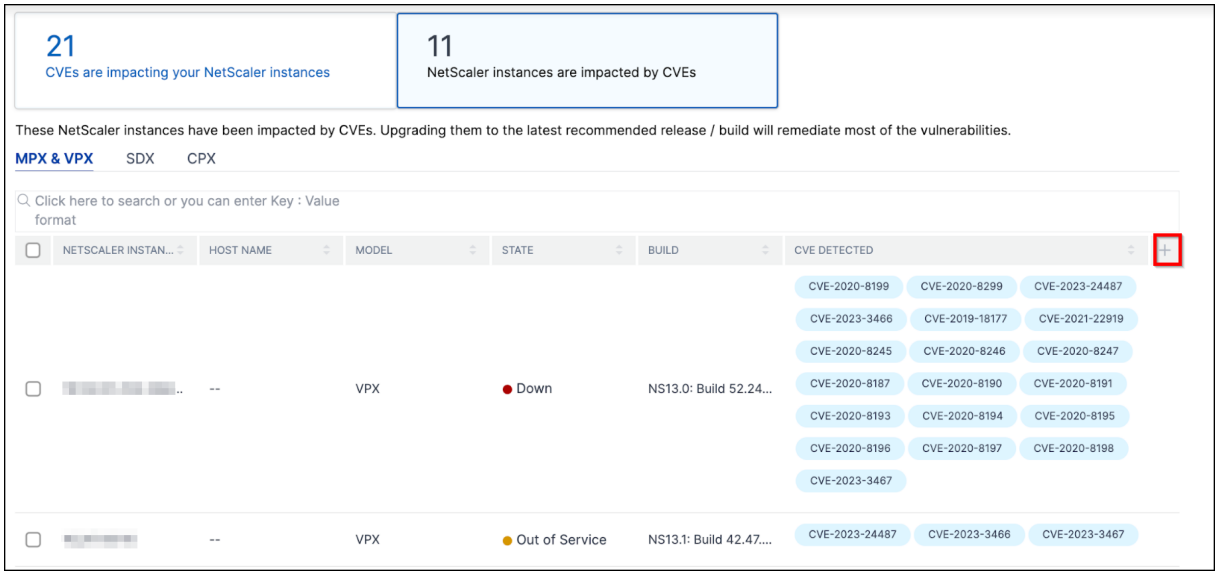
En esta pantalla, la cantidad de CVE que afectan a tus instancias es de 3 CVE y las instancias que se ven afectadas por estas CVE de dos.



Las **<number of>instancias de NetScaler se ven afectadas por** las CVE. La pestaña muestra todas las instancias de NetScaler Console 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.

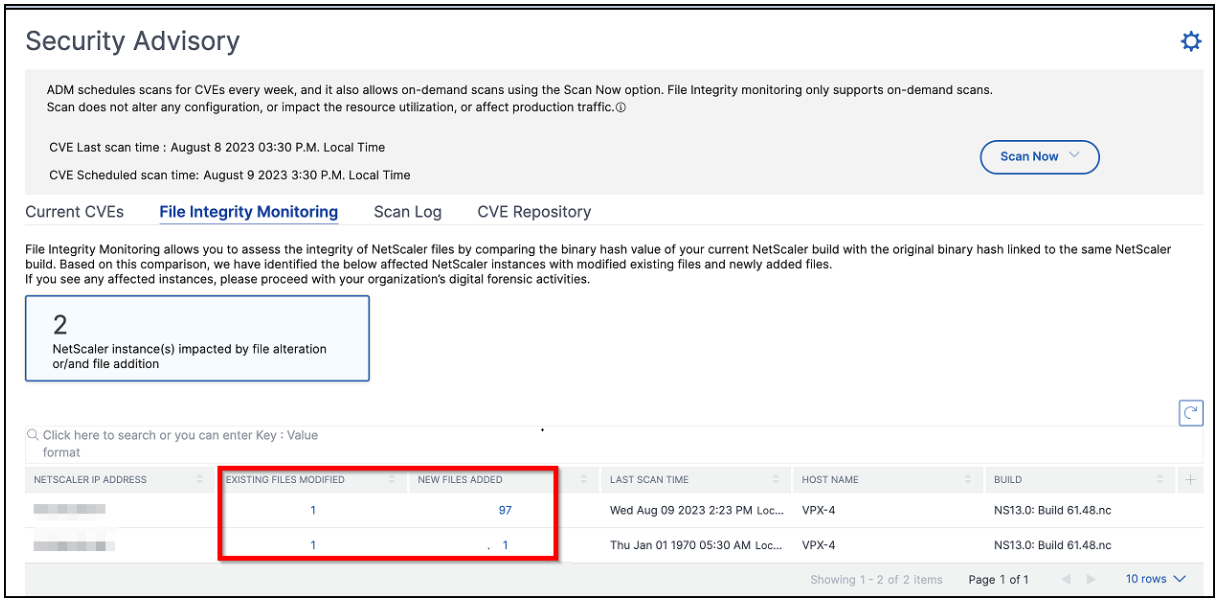
Se inicia el flujo de trabajo de actualización. Para obtener más información sobre cómo usar NetScaler Console para actualizar las instancias de NetScaler, consulte Usar trabajos para actualizar las instancias de NetScaler.

> **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.

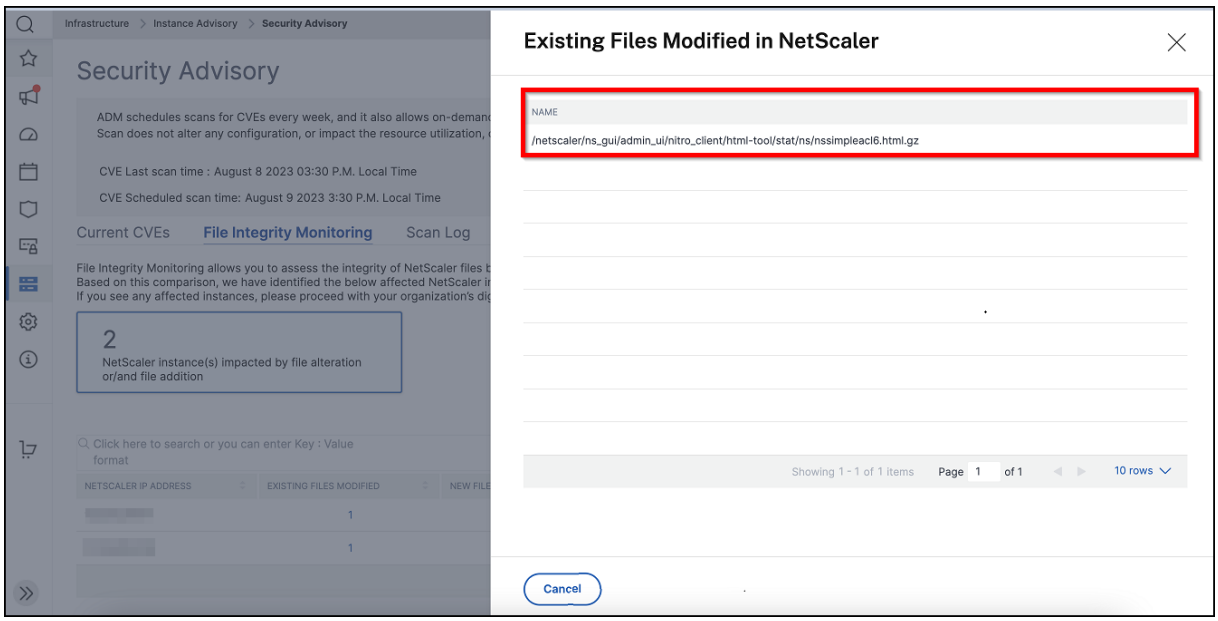
Supervisión de la integridad de los archivos

En esta ficha se muestra el resultado del análisis de la supervisión de la integridad de los archivos con instancias de NetScaler que presentan modificaciones o adiciones a los archivos de compilación originales de NetScaler.

El siguiente ejemplo muestra el resultado del análisis de dos instancias de NetScaler afectadas con archivos existentes modificados y archivos nuevos agregados a los archivos de compilación originales.

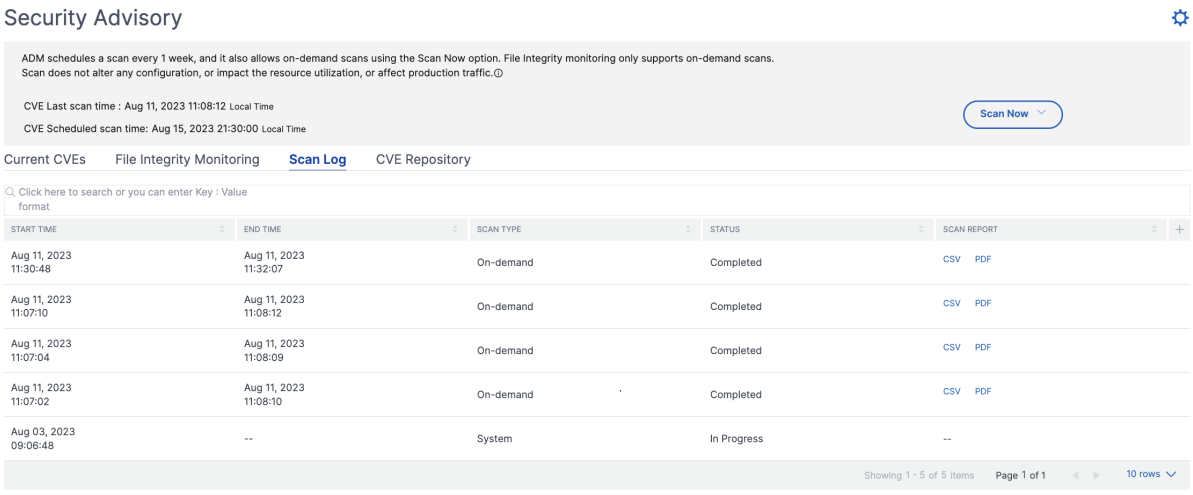


Haga clic en los números de **Archivos existentes modificados** y **Archivos nuevos agregados** para ver los detalles.



Registro de escaneo (aplicable solo para los CVE)

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. Si se está realizando un análisis bajo demanda, puede ver el estado de finalización aquí. Si se ha producido un error en el análisis, el estado indica eso.

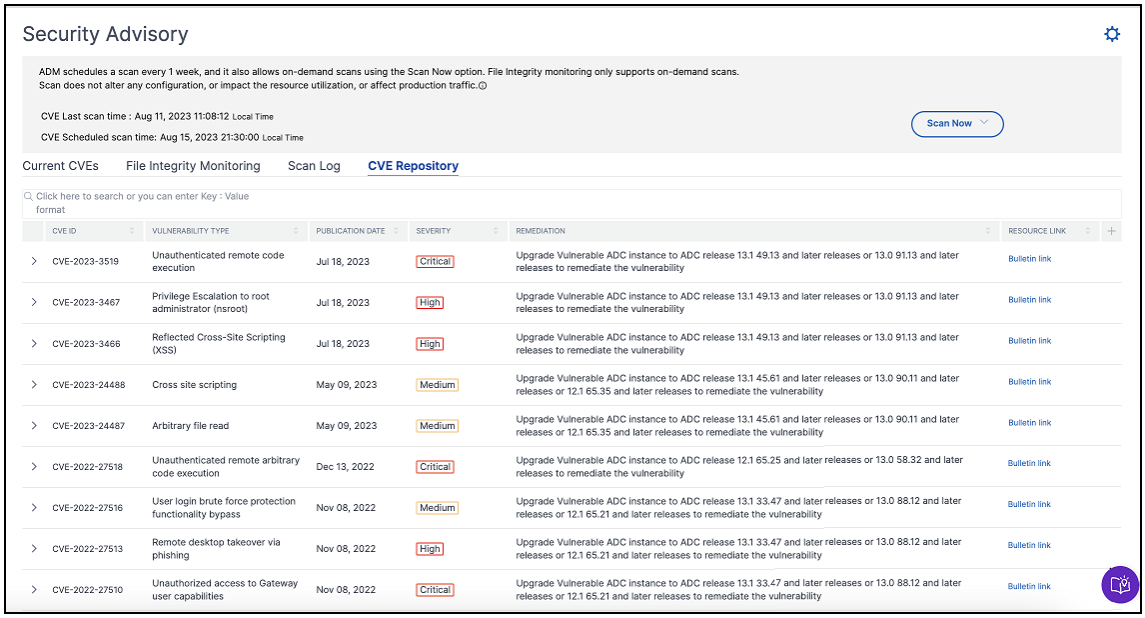


Repositorio CVE

Esta ficha incluye la información más reciente de todos los CVE de diciembre de 2019, junto con los siguientes detalles:

- Identificadores CVE

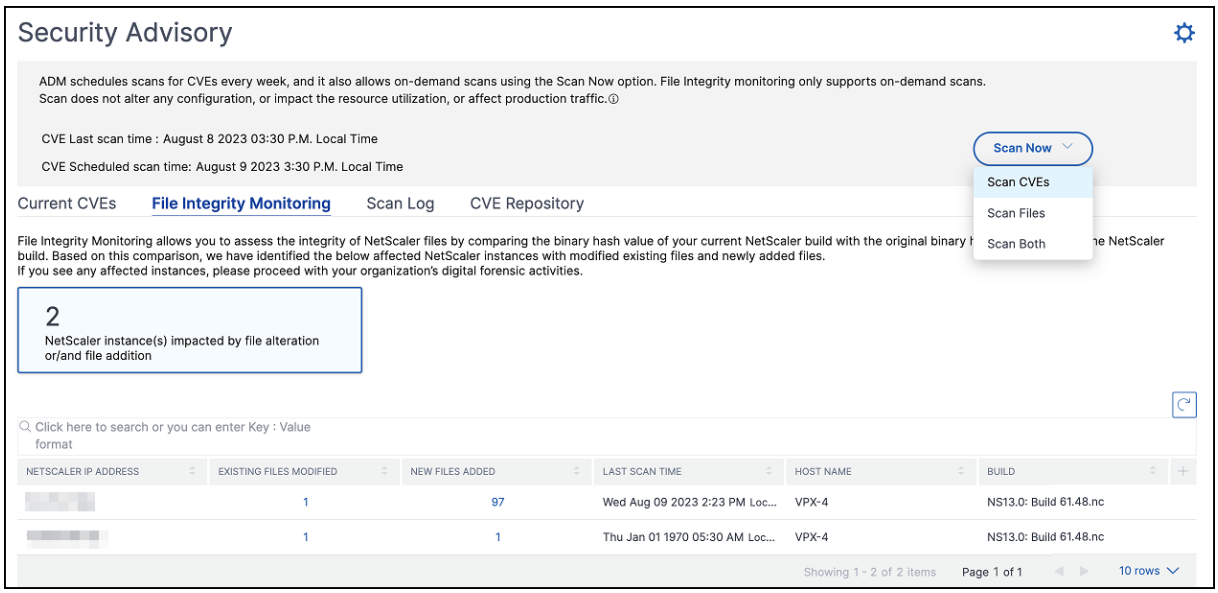
- Tipo de vulnerabilidad
- Fecha de publicación
- Nivel de gravedad
- Remediación
- Enlaces a boletines de seguridad



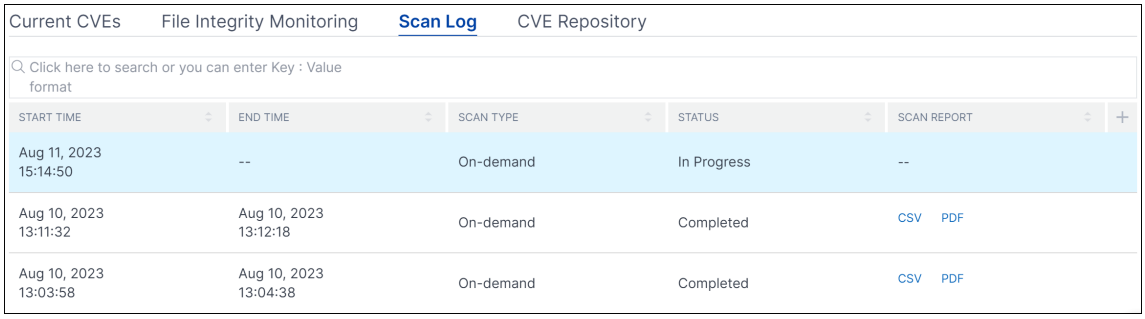
Escanear ahora

Puede escanear las instancias en cualquier momento, según sus necesidades.

Haga clic en **Analizar ahora** y seleccione **Analizar CVE**, **Escanear archivos** o **Analizar ambos** para obtener el informe de seguridad más reciente de sus instancias.



- **Escanear los CVE**: Escanea solo los CVE que están afectando a las instancias de NetScaler. Una vez finalizado el análisis, los detalles de seguridad revisados aparecen en la GUI de asesoramiento de seguridad. También puede encontrar el informe en el **registro de escaneo**, que también puede descargar.



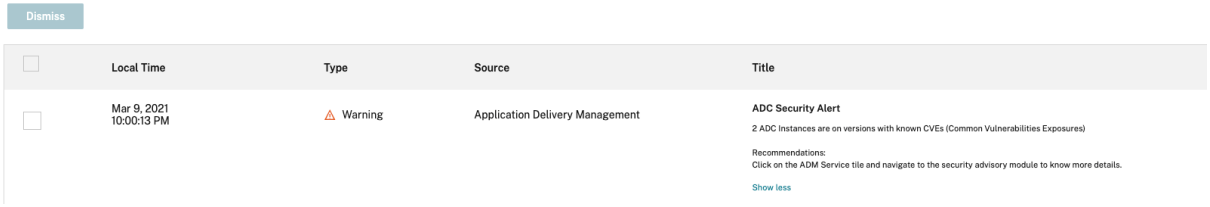
- **Escanear archivos**: Busca únicamente la supervisión de la integridad de los archivos y proporciona el resultado en la ficha **Supervisión de la integridad de los archivos**.
- **Escanear ambos**: Escanea tanto para detectar CVE como para supervisar la integridad de los archivos.

La consola NetScaler tarda unos minutos en completar el análisis.

> **Nota**
>
> El registro de escaneo muestra solo los registros de los últimos cinco escaneos de CVE, que pueden programarse o bajo demanda.

Notificación (aplicable solo a los CVE)

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 situado en la esquina superior derecha de la GUI de NetScaler Console.

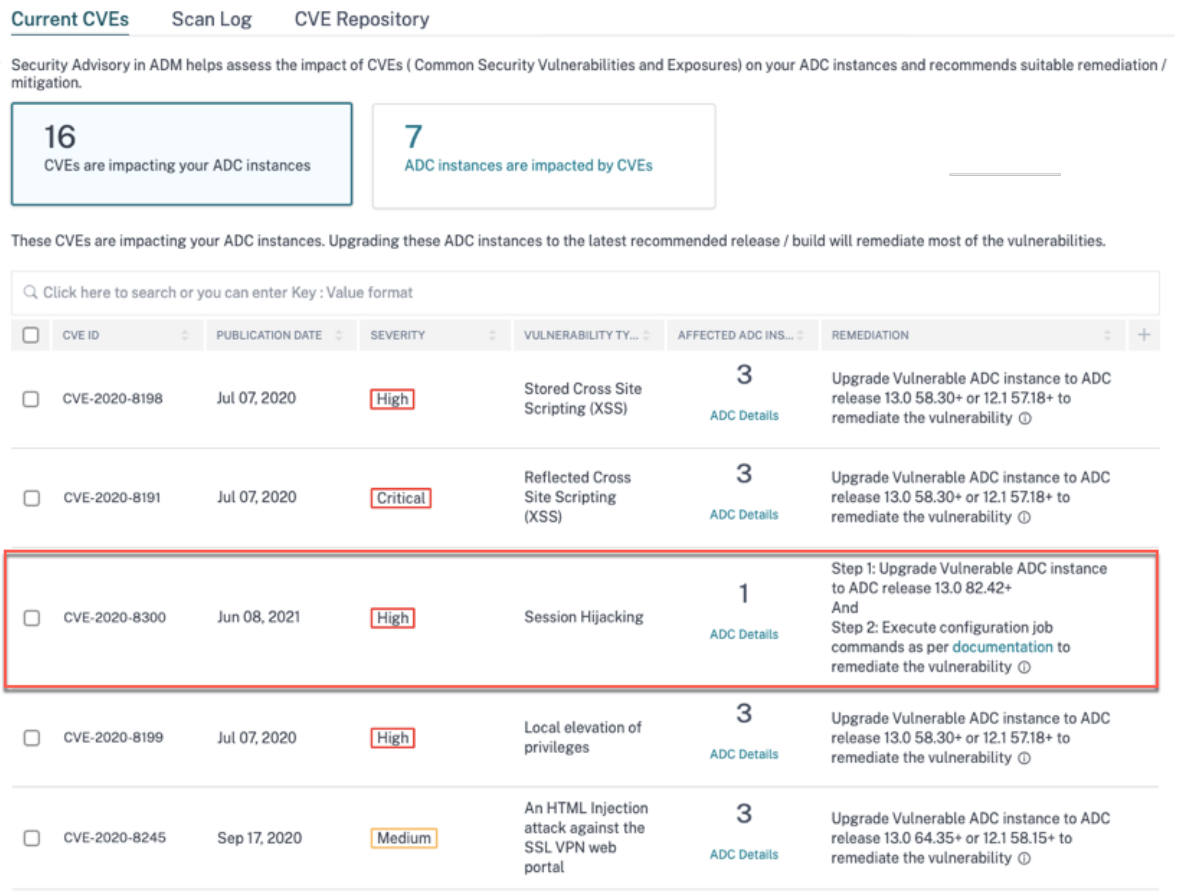


> **Renuncia de responsabilidades:**
>
> Tenga en cuenta que NetScaler File Integrity Monitoring ("la Función") no es capaz de detectar todas las técnicas, tácticas o procedimientos (TTP) que los actores de amenazas pueden utilizar cuando atacan los entornos pertinentes. Los actores de amenazas cambian los TTP y la infraestructura con frecuencia y, por lo tanto, la función puede tener un valor forense limitado o nulo en relación con ciertas amenazas. Le recomendamos encarecidamente que contrate los servicios de investigadores forenses con experiencia para evaluar su entorno en relación con cualquier posible amenaza.
>
> Este documento y la información que contiene se proporcionan tal cual. Cloud Software Group, Inc. no ofrece ninguna garantía ni representación, ya sea expresa o implícita, con respecto al documento o su contenido, incluyendo, sin limitación, que este documento o la información que contiene estén libres de errores o cumplan cualquier condición de comerciabilidad o idoneidad para un propósito particular.

Corrija las vulnerabilidades del CVE-2020-8300

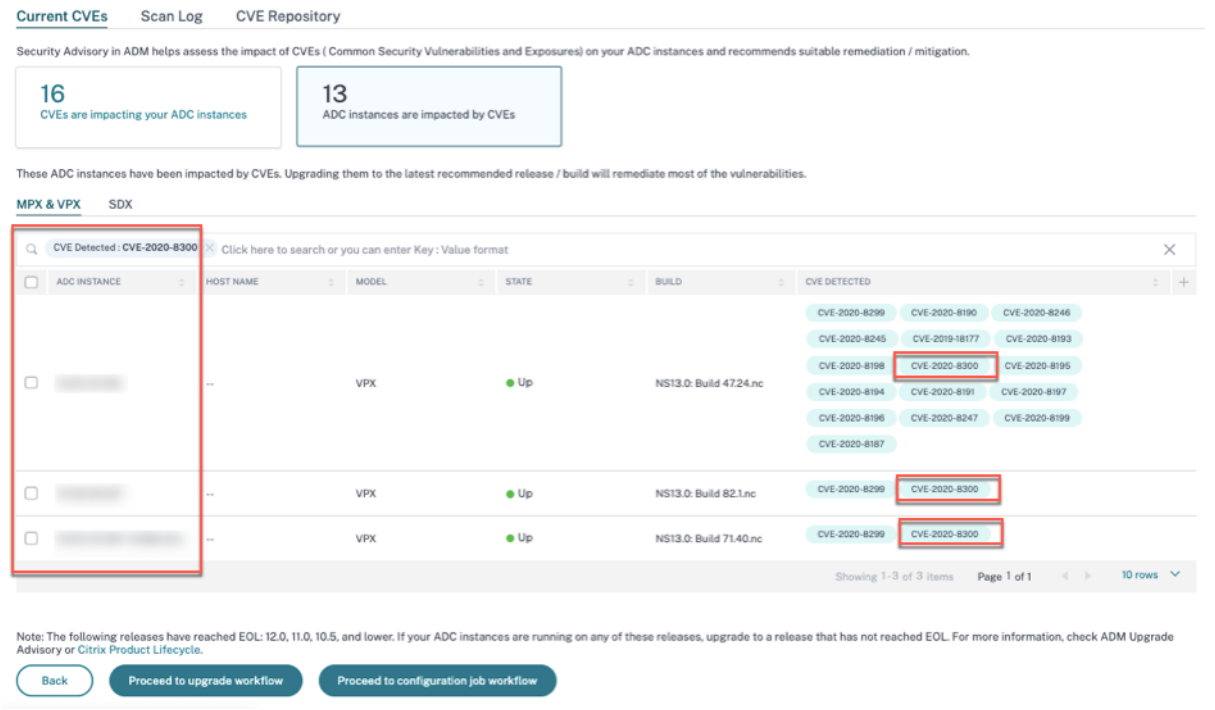
January 26, 2024

En el panel de asesoramiento de seguridad de NetScaler Console, en CVE **actuales > <number of> Las instancias de NetScaler 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**.



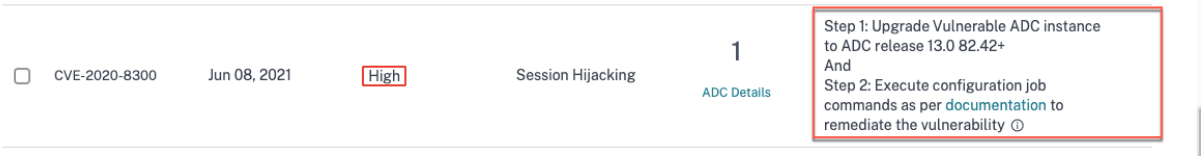
> **Nota**
>
> Para obtener más información sobre el panel de asesoramiento de seguridad, consulte Asesoramiento de seguridad .

Aparece la ventana **<number of>Instancias de NetScaler afectadas por** CVE . Aquí puede ver el recuento y los detalles de las instancias de NetScaler afectadas por el CVE-2020-8300.



Corrija el CVE-2020-8300

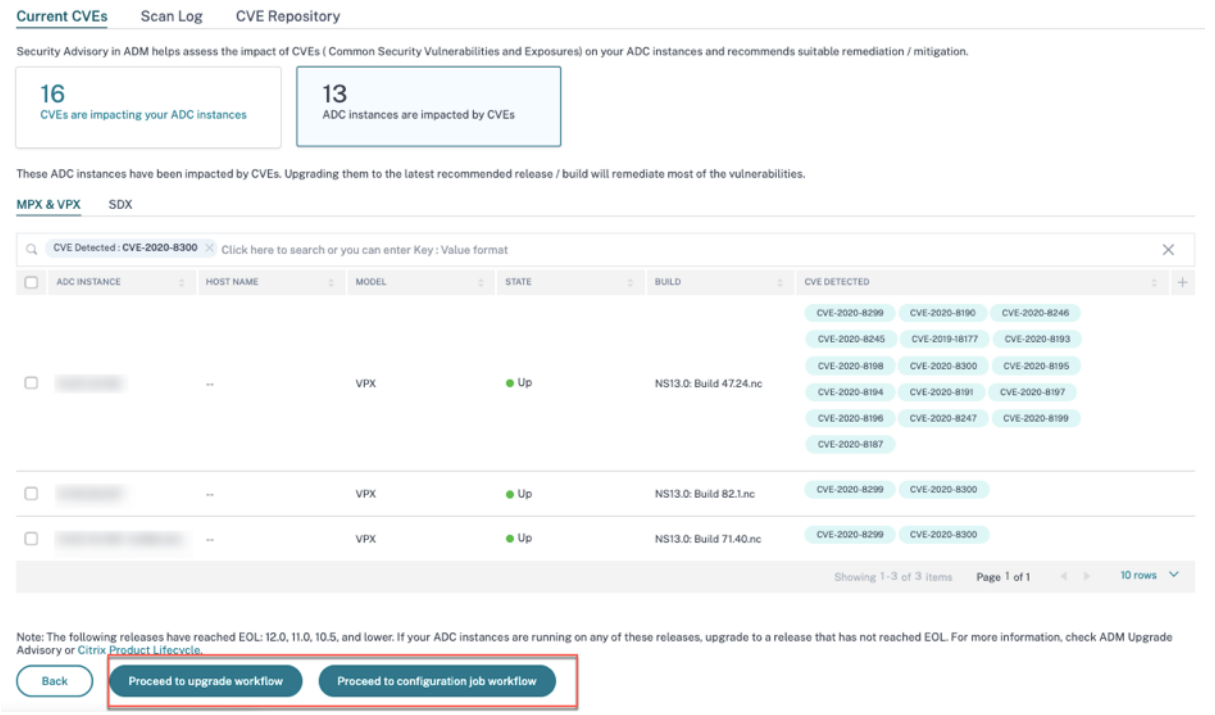
En el caso de las instancias de NetScaler afectadas por el CVE-2020-8300, la corrección es un proceso de dos pasos. En la GUI, en CVE **actuales > Las instancias de NetScaler se ven afectadas por** las CVE, puede ver los pasos 1 y 2.



Los dos pasos incluyen:

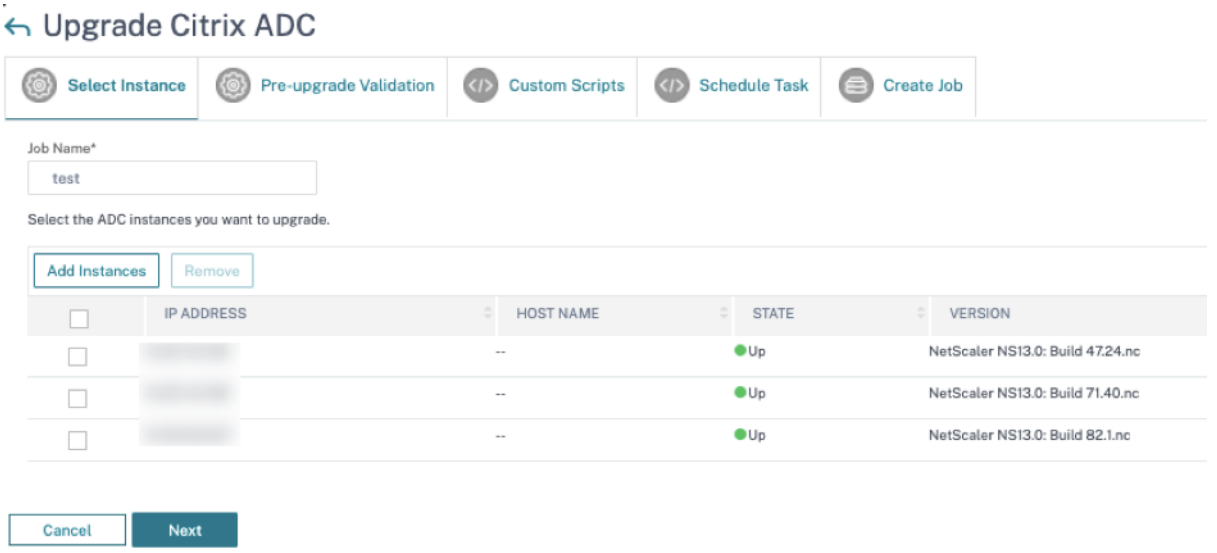
1. Actualización de las instancias vulnerables de NetScaler a una versión y compilación que tengan la solución.
2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración. Siga este paso para cada NetScaler vulnerable de uno en uno e incluya todas las acciones SAML y los perfiles SAML de ese NetScaler.

En CVE **actuales> Instancias de NetScaler afectadas por** las CVE , verá dos flujos de trabajo independientes para este proceso de corrección de dos pasos: continuar con el flujo de trabajo de **actualización** y continuar con el flujo de **trabajo de configuración**.



Paso 1: Actualizar las instancias vulnerables de NetScaler

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 vulnerables de NetScaler ya pobladas.



Para obtener más información sobre cómo usar NetScaler Console para actualizar las instancias de NetScaler, consulte Crear un trabajo de actualización de NetScaler.

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de NetScaler vulnerables.

Paso 2: Aplicar los comandos de configuración

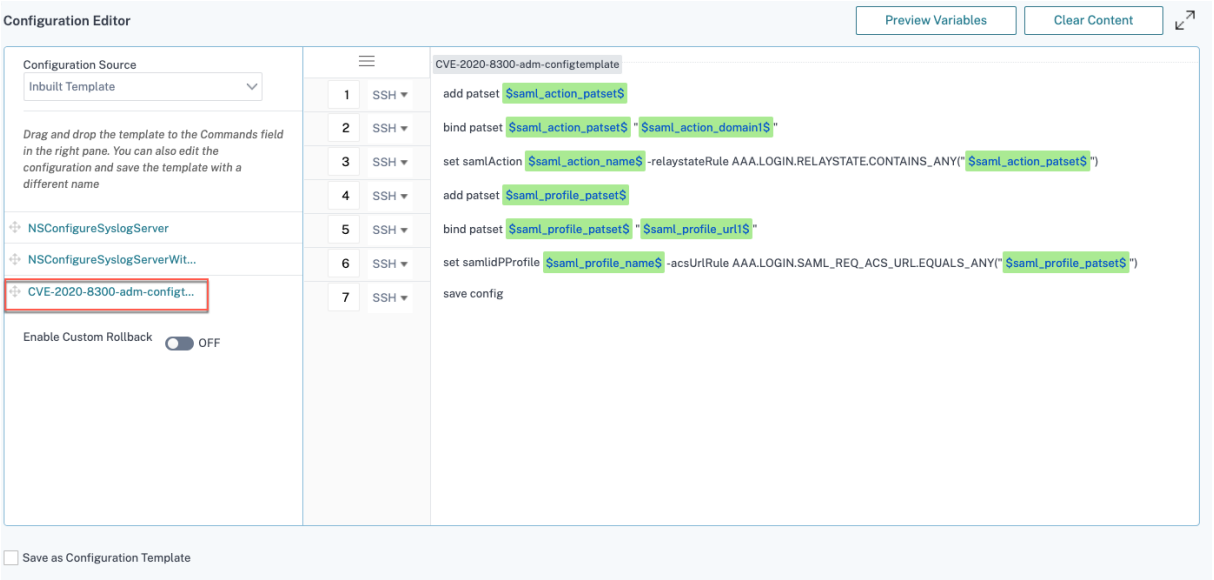
Después de actualizar las instancias afectadas, en la ventana **<number of> Instancias de NetScaler afectadas por** CVE, seleccione una instancia afectada por CVE-2020-8300 y haga clic en **Continuar con el flujo de trabajo del trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

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**:

- En el caso de una instancia de NetScaler 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 **Proceder al 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.
- Solo para varias instancias de NetScaler afectadas por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene NetScaler 1, NetScaler 2 y NetScaler 3, y todos ellos solo se ven afectados 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.
- En el caso de varias instancias de NetScaler afectadas por el CVE-2021-22956 y uno o varios otros CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren la aplicación de correcciones a cada NetScaler a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo del trabajo de configuración**, aparece un mensaje de error que le indica que debe ejecutar el trabajo de configuración en cada NetScaler a la vez NetScaler 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**.



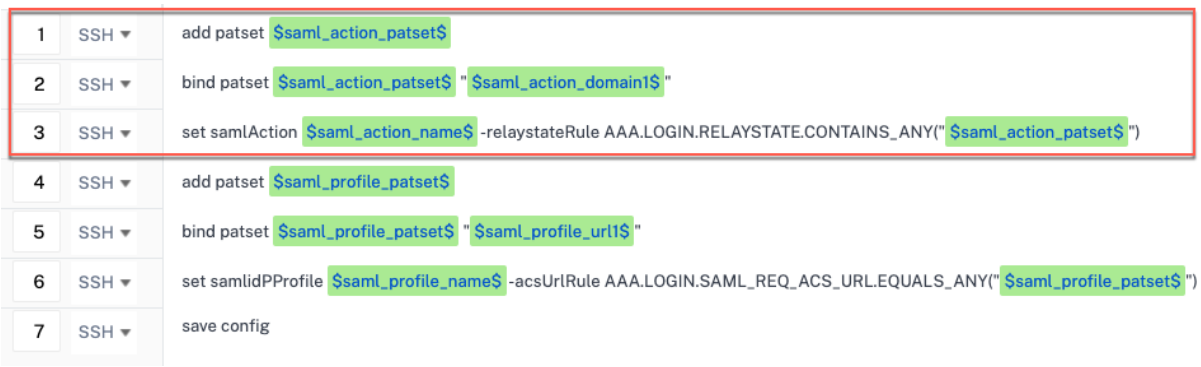
Ejecute un trabajo de configuración independiente para cada instancia de NetScaler afectada, una por una, e incluya todas las acciones de SAML y los perfiles de SAML de ese NetScaler. Por ejemplo, si tiene dos instancias de NetScaler vulnerables, cada una con dos acciones SAML y dos perfiles SAML, debe ejecutar este trabajo de configuración dos veces. Una vez por NetScaler que cubra todas sus acciones de SAML y perfiles de SAML.

NetScaler 1	NetScaler 2
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.

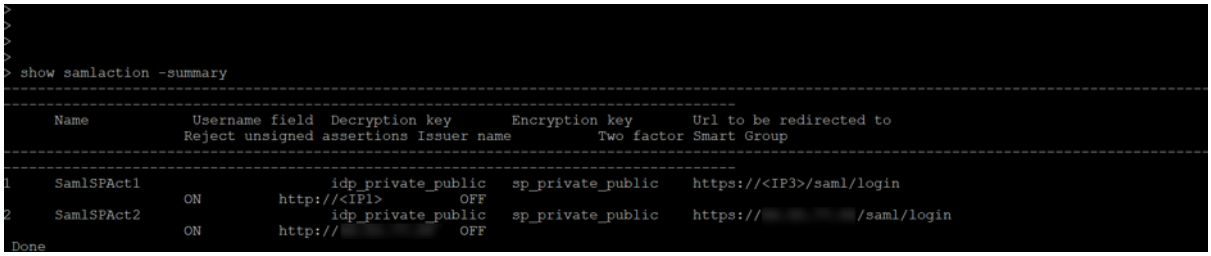


Por ejemplo, si tiene dos acciones de SAML, repita las líneas 1 a 3 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

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:

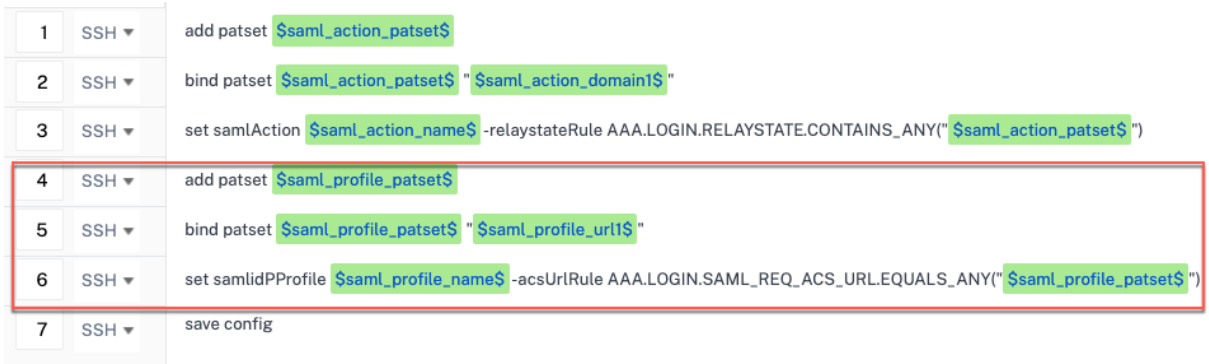
- `saml_action_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) de la acción SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables 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.

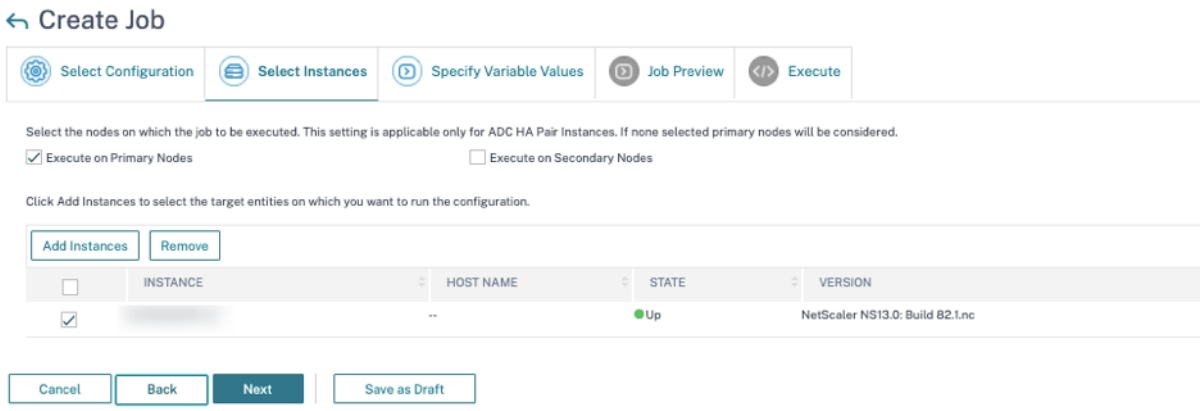
Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_profile_patset "$saml_profile_url1$"` manualmente varias veces para asegurarse de que la línea aparezca N veces para ese perfil de SAML. Y cambie los siguientes nombres de definición de variables:

- `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**.

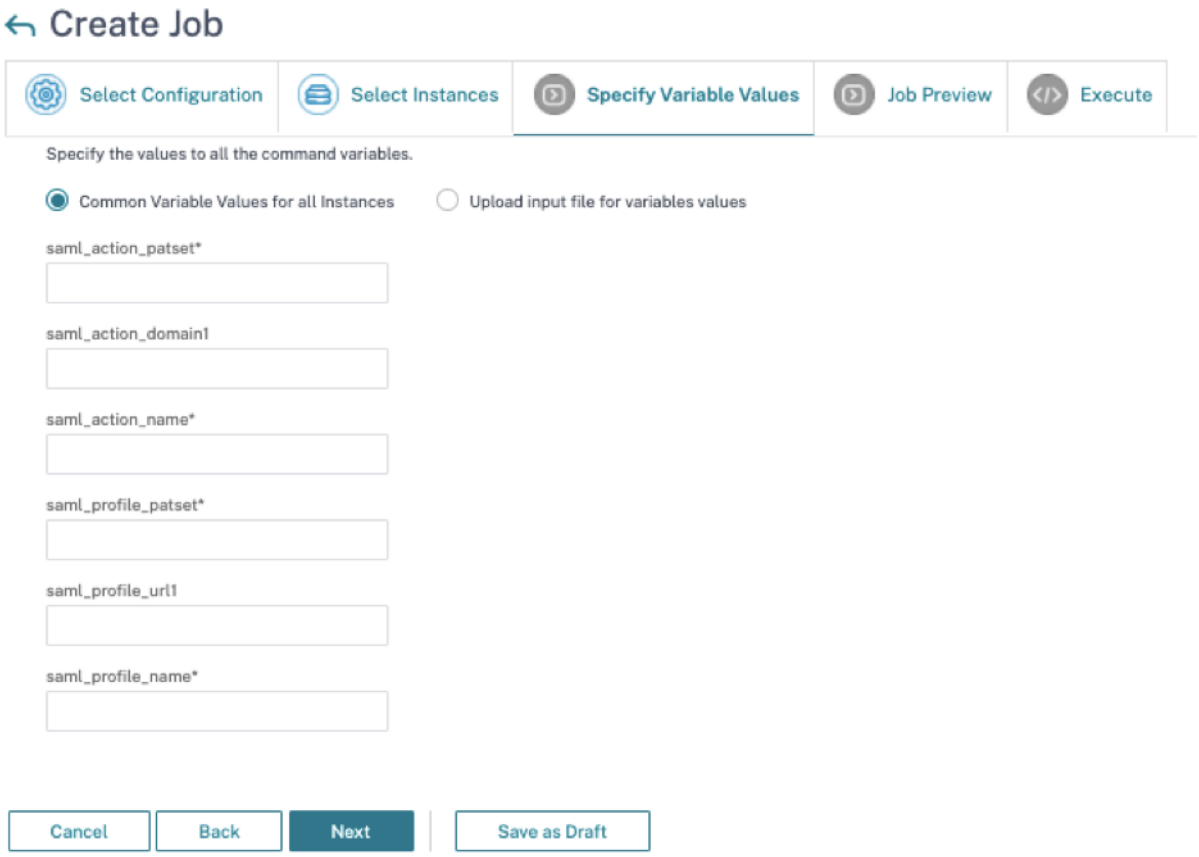


Paso 3: especificar los valores de las variables Introduzca los valores de las variables.

- `saml_action_patset`: agregar un nombre para la acción SAML

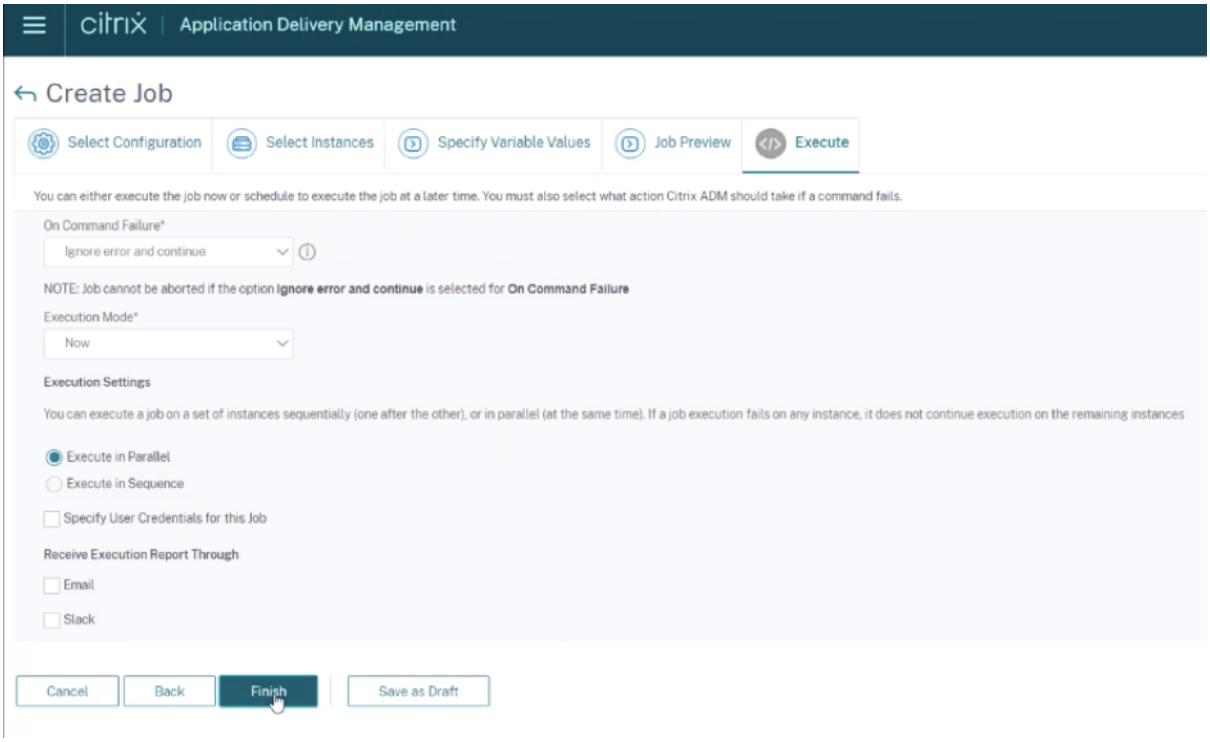
- `saml_action_domain1`: introduzca un dominio con el formato `https://<example1.com>/`
- `saml_action_name`: introduzca lo mismo de la acción SAML para la que está configurando el trabajo
- `saml_profile_patset`: agregue un nombre para el perfil SAML
- `saml_profile_url1`: introduzca la URL en este 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 todas las instancias vulnerables de NetScaler, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Puntos a tener en cuenta para la cuenta NetScaler Console Express

La cuenta NetScaler Console Express tiene funciones limitadas, que incluyen la limitación de solo dos trabajos de configuración. Para obtener más información sobre la cuenta NetScaler Console Express, consulte Administrar los recursos de NetScaler Console mediante la cuenta Express.
Para solucionar el problema del CVE-2020-8300, debe ejecutar tantos trabajos de configuración como el número de instancias de NetScaler vulnerables. Por lo tanto, si tiene una cuenta Express y necesita ejecutar más de dos trabajos de configuración, siga esta solución alternativa.

Soluciónalternativa : ejecute dos trabajos de configuración para dos instancias de NetScaler vulnerables y, a continuación, elimine ambos trabajos para seguir ejecutando los dos trabajos siguientes para las dos instancias de NetScaler vulnerables siguientes. 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 NetScaler vulnerables, ejecute dos trabajos de configuración en dos instancias vulnerables respectivamente y, a continuación, elimine ambos trabajos de configu-

ración. Repite este paso otras dos veces. Al final, habría ejecutado seis trabajos de configuración para seis instancias de NetScaler, respectivamente. En la interfaz de usuario de NetScaler Console, en **Infraestructura Trabajos**, solo verá los dos últimos trabajos de configuración.

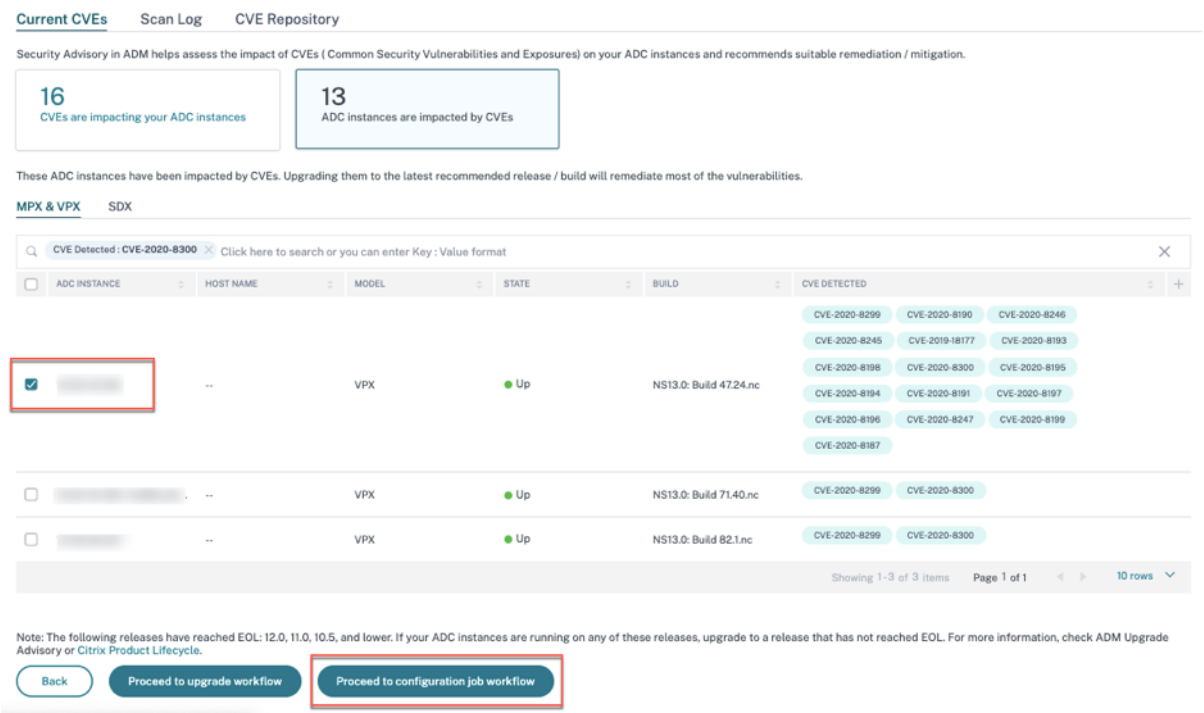
Escenario

En este escenario, tres instancias de NetScaler son vulnerables al CVE-2020-8300 y es necesario corregir todas las instancias. Siga estos pasos:

1. Actualice las tres instancias de NetScaler siguiendo los pasos que se indican en la sección **Actualizar una instancia** de este documento.
2. Aplique el parche de configuración a un NetScaler 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 NetScaler 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 NetScaler 1 y haga clic en **Continuar con el flujo de trabajo del 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 de NetScaler	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 de NetScaler	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 NetScaler 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.

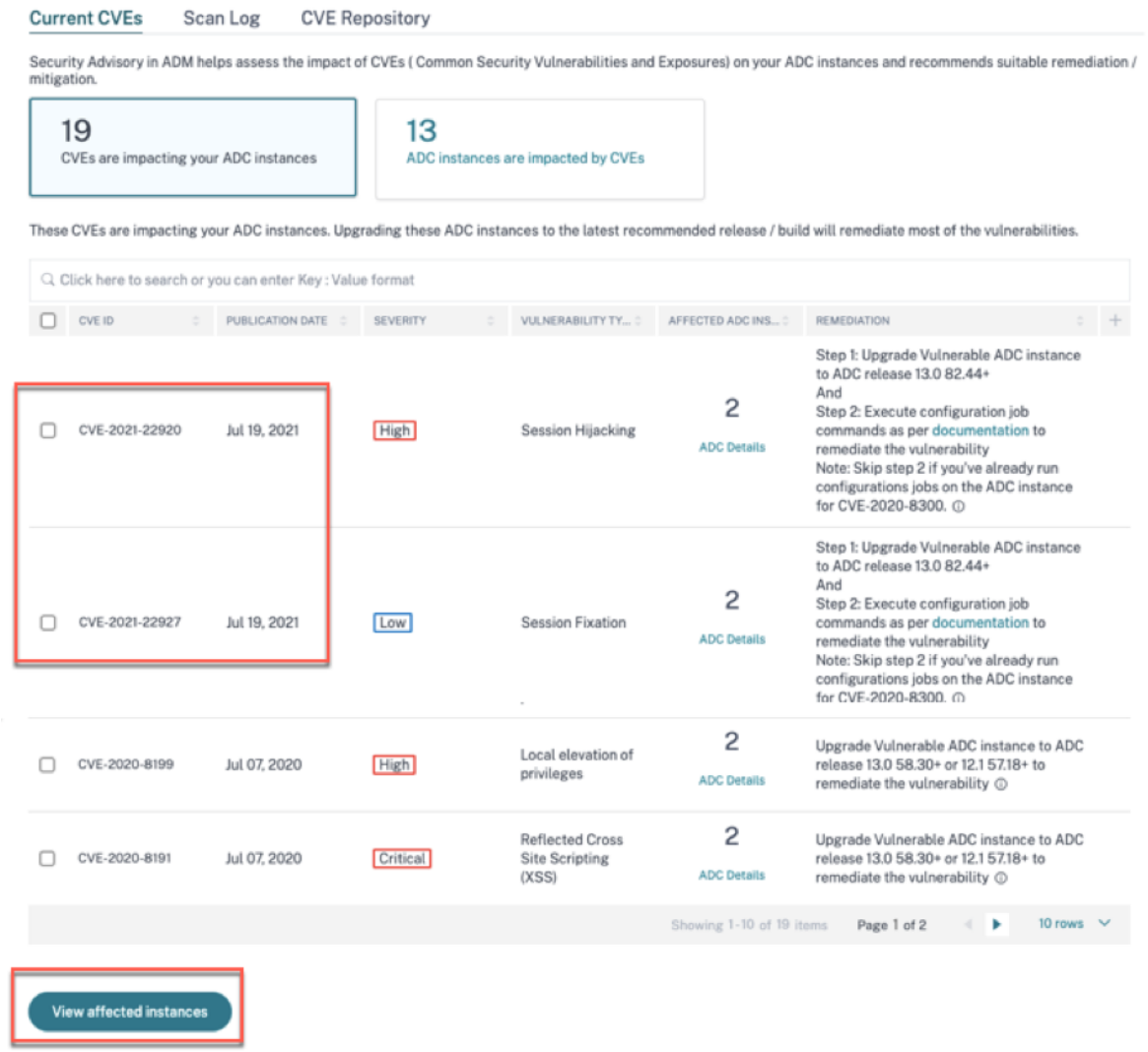
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para NetScaler 1, siga los mismos pasos para corregir NetScaler 2 y NetScaler 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 26, 2024

En el panel de asesoramiento de seguridad de NetScaler Console, en CVE **actuales > <number of >Las instancias de NetScaler 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**.

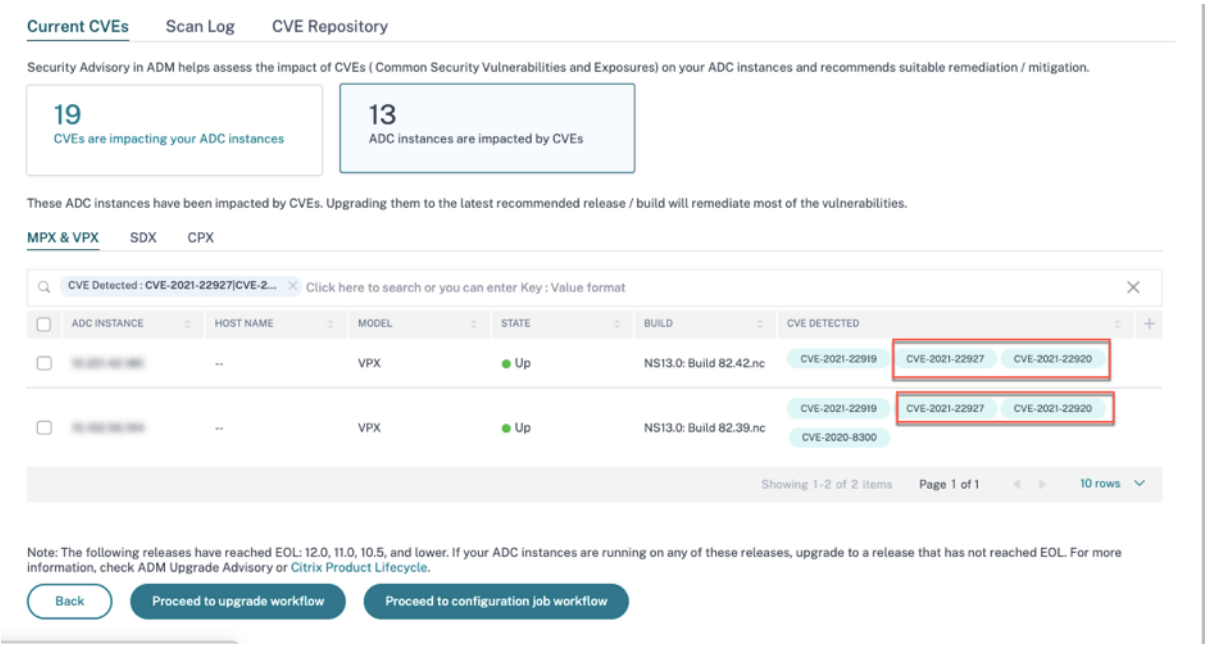


Nota

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**.

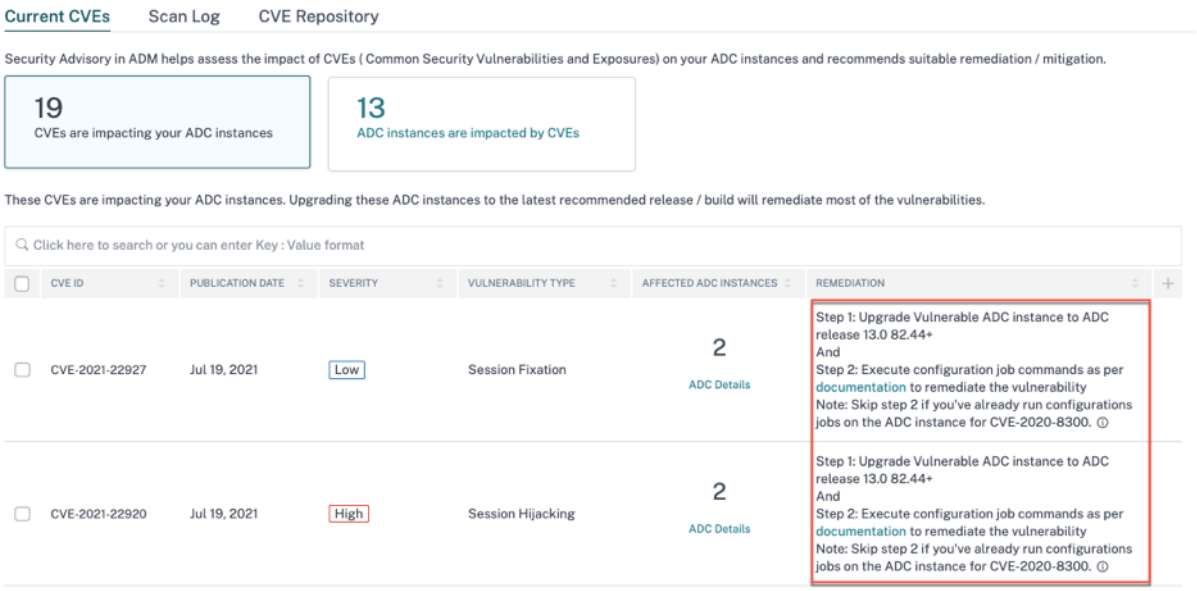
Para obtener más información sobre el panel de asesoramiento de seguridad, consulte Asesoramiento de seguridad .

Aparece la ventana **<number of>Instancias de NetScaler afectadas por** CVE . En la siguiente captura de pantalla, puede ver el recuento y los detalles de las instancias de NetScaler afectadas por CVE-2021-22927 y CVE-2021-22920.



Corrija los CVE-2021-22927 y CVE-2021-22920

Para las instancias de NetScaler afectadas por CVE-2021-22927 y CVE-2021-22920, la corrección es un proceso de dos pasos. En la GUI, en CVE **actuales > Las instancias de NetScaler se ven afectadas por** las CVE, puede ver los pasos 1 y 2.



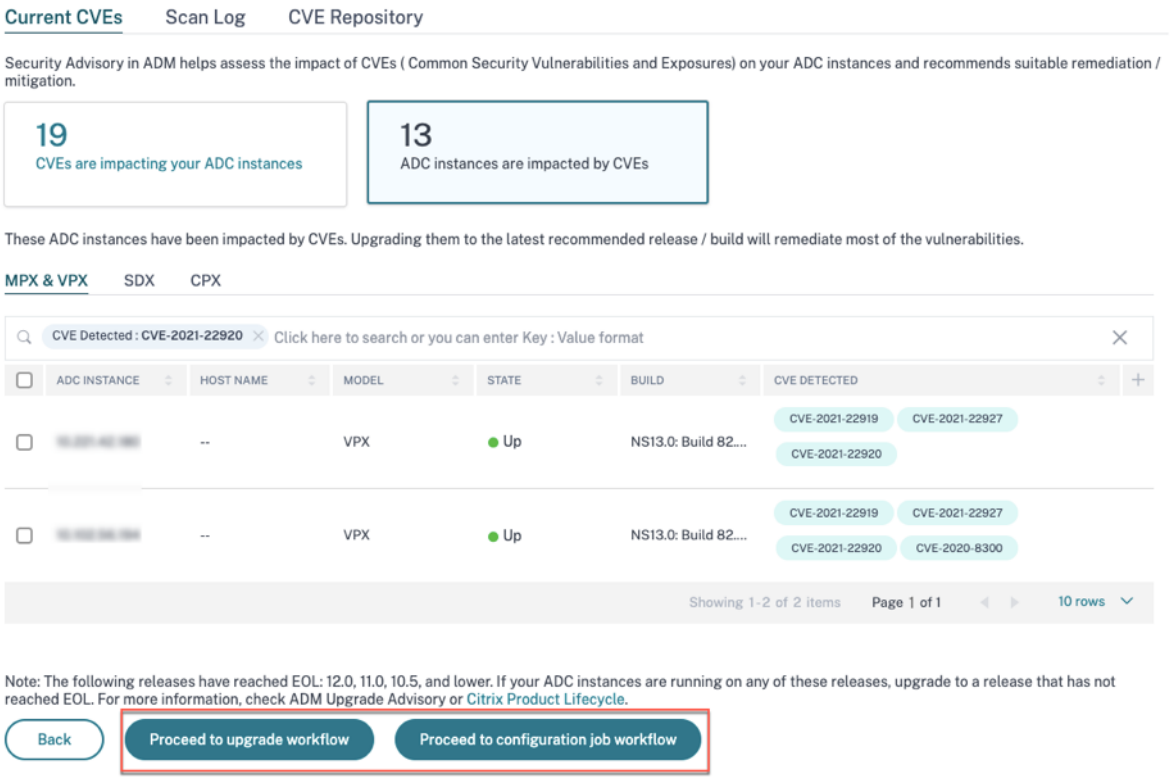
Los dos pasos incluyen:

1. Actualización de las instancias vulnerables de NetScaler a una versión y 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 NetScaler vulnerable de uno en uno e incluya todas las acciones de SAML para ese NetScaler.

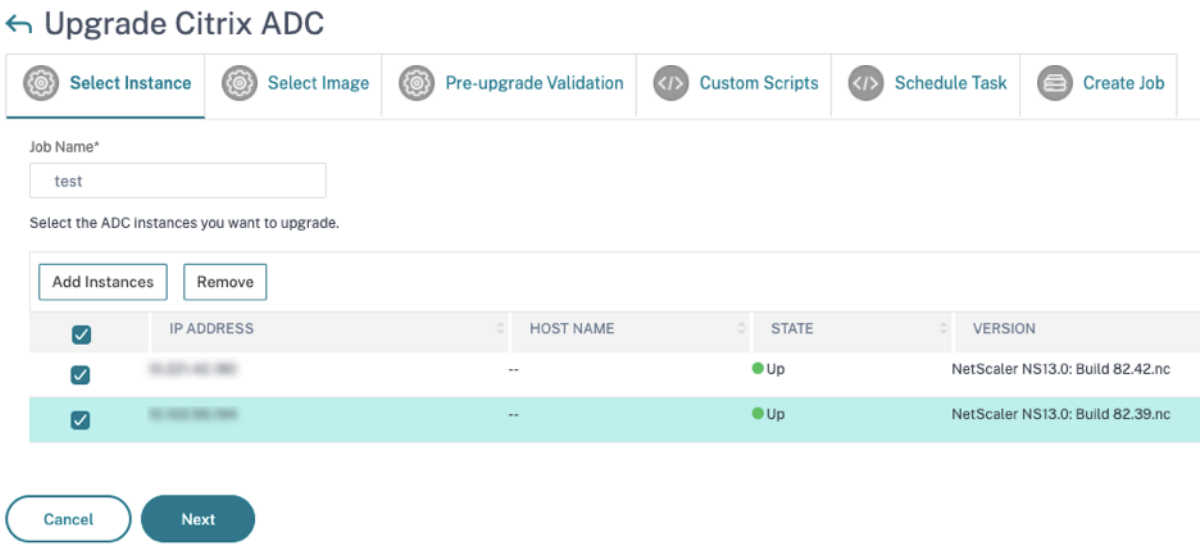
> **Nota**
>
> Omita el paso 2 si ya ha ejecutado trabajos de configuración en la instancia de NetScaler para CVE-2020-8300.

En CVE **actuales> Instancias de NetScaler afectadas por** las CVE , verá dos flujos de trabajo independientes para este proceso de corrección de dos pasos: continuar con el flujo de trabajo de **actualización** y continuar con el flujo de **trabajo de configuración**.



Paso 1: Actualizar las instancias vulnerables de NetScaler

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 vulnerables de NetScaler ya pobladas.



Para obtener más información sobre cómo usar NetScaler Console para actualizar las instancias de NetScaler, consulte Crear un trabajo de actualización de NetScaler.

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de NetScaler vulnerables.
>
> **Nota**
>
> Cuando haya completado el paso 1 para todas las instancias de NetScaler vulnerables a CVE-2021-22920 y CVE-2021-22927, realice un análisis bajo demanda. La postura de seguridad actualizada en las CVE **actuales** le ayuda a comprender si las instancias de NetScaler siguen siendo vulnerables a alguna de estas 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 NetScaler para CVE-2020-8300 y ahora ha actualizado la instancia de NetScaler, tras realizar el análisis bajo demanda, la instancia ya no se muestra como vulnerable a CVE-2020-8300, CVE-2021-22920 y CVE-2021-22927.

Paso 2: Aplicar los comandos de configuración

Después de actualizar las instancias afectadas, en la ventana **<number of> Instancias de NetScaler afectadas por** CVE, seleccione una instancia afectada por CVE-2021-22927 y CVE-2021-22920 y haga clic en **Continuar con el flujo de trabajo del trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

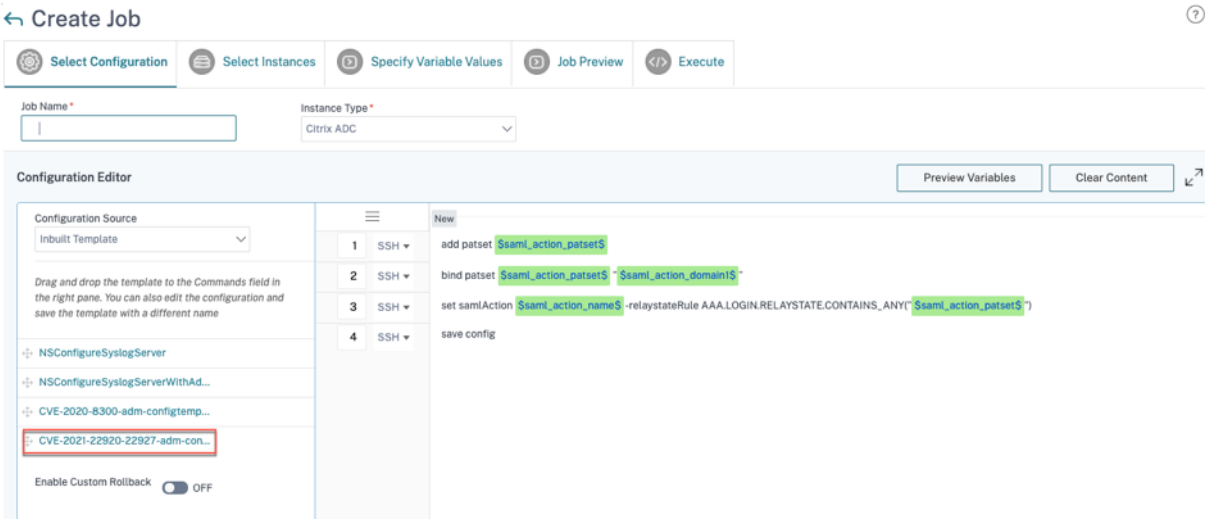
1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.

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**:

- En el caso de una instancia de NetScaler 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 **Proceder al 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.
- Solo para varias instancias de NetScaler afectadas por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene NetScaler 1, NetScaler 2 y NetScaler 3, y todos ellos solo se ven afectados 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.
- En el caso de varias instancias de NetScaler afectadas por el CVE-2021-22956 y uno o varios otros CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren la aplicación de correcciones a cada NetScaler a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo del trabajo de configuración**, aparece un mensaje de error que le indica que debe ejecutar el trabajo de configuración en cada NetScaler a la vez NetScaler 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 NetScaler 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 para CVE-2020–8300 se rellena automáticamente. La plantilla CVE-2020-8300 es un supercon-junto 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 NetScaler.

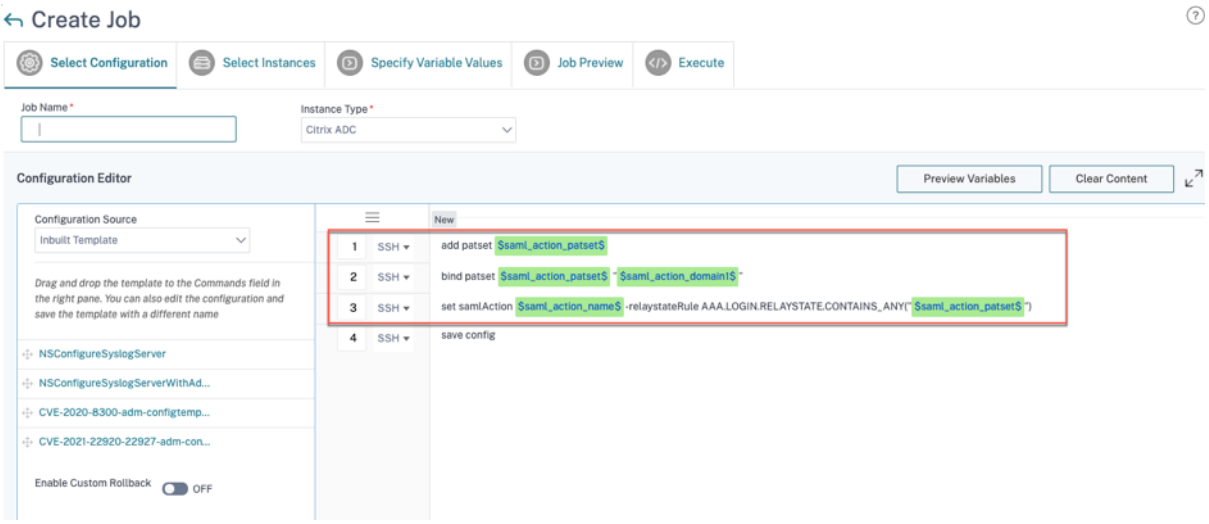
Debe ejecutar un trabajo de configuración independiente para cada instancia de NetScaler afectada, una por una, e incluir todas las acciones de SAML para ese NetScaler. Por ejemplo, si tiene dos in-stancias de NetScaler vulnerables, cada una con dos acciones de SAML, debe ejecutar este trabajo de configuración dos veces. Una vez por NetScaler para cubrir todas sus acciones de SAML.

NetScaler 1	NetScaler 2
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.



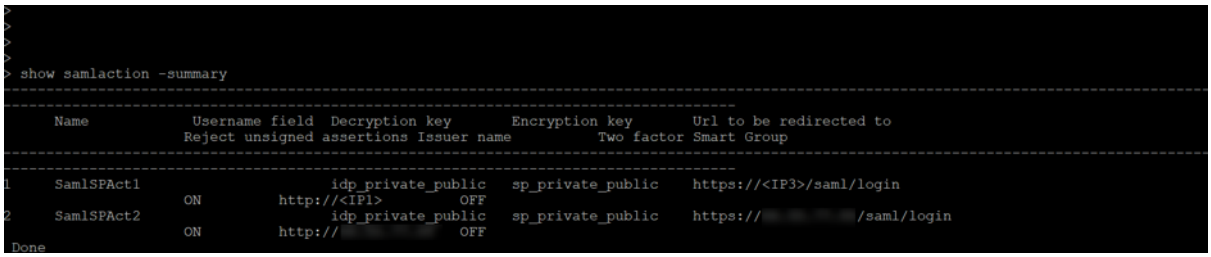
Por ejemplo, si tiene dos acciones de SAML, repita las líneas 1 a 3 dos veces y, en consecuencia, per-sonalice las definiciones de variables para cada acción de SAML.

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:

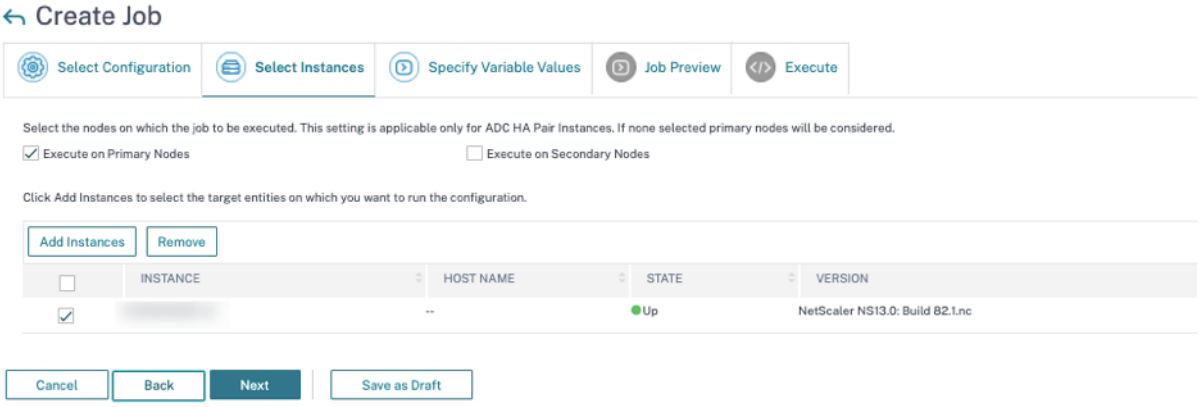
- `saml_action_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) de la acción SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables 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` .



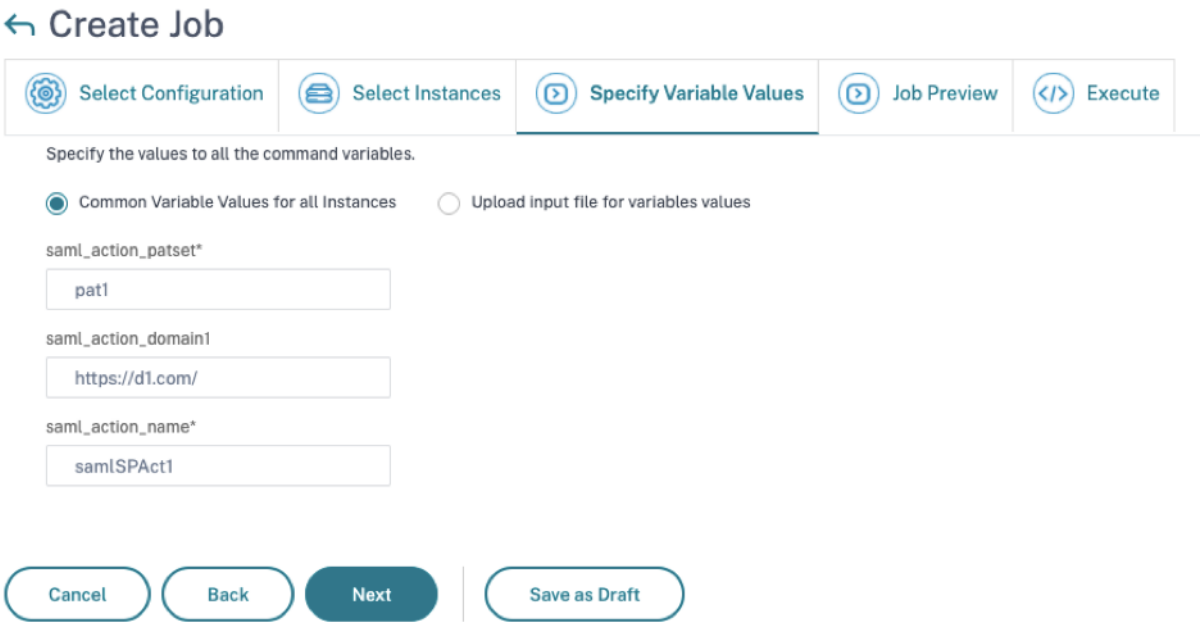
Paso 2: selecciona la instancia

La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia y haga clic en **Siguiente**.

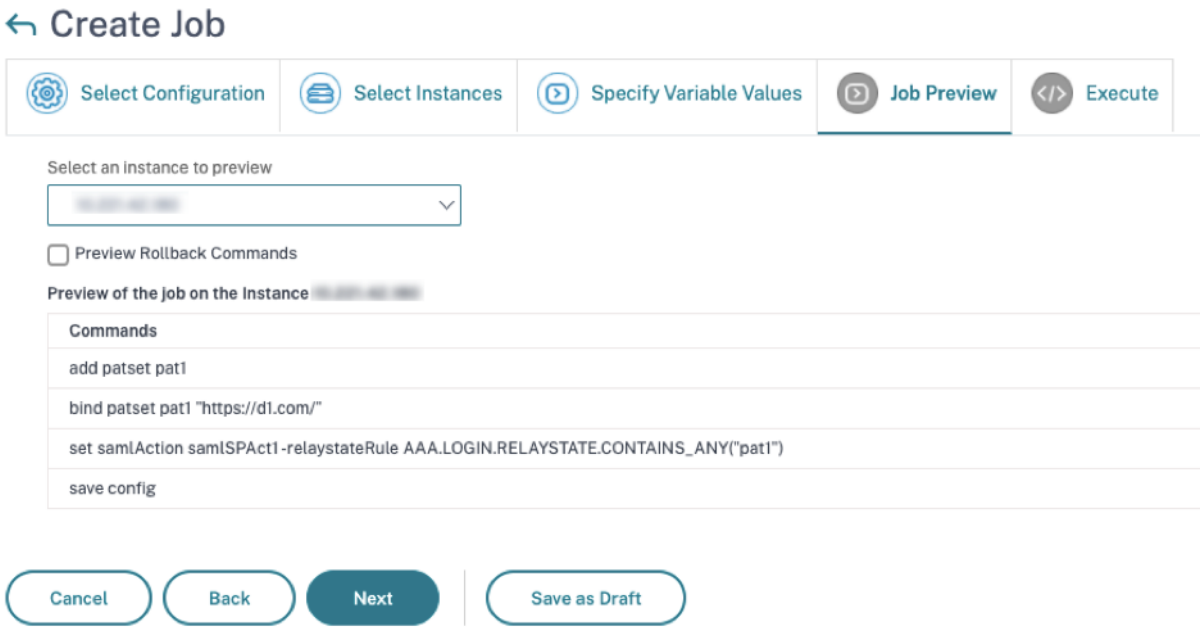


Paso 3: especificar los valores de las variables Introduzca los valores de las variables.

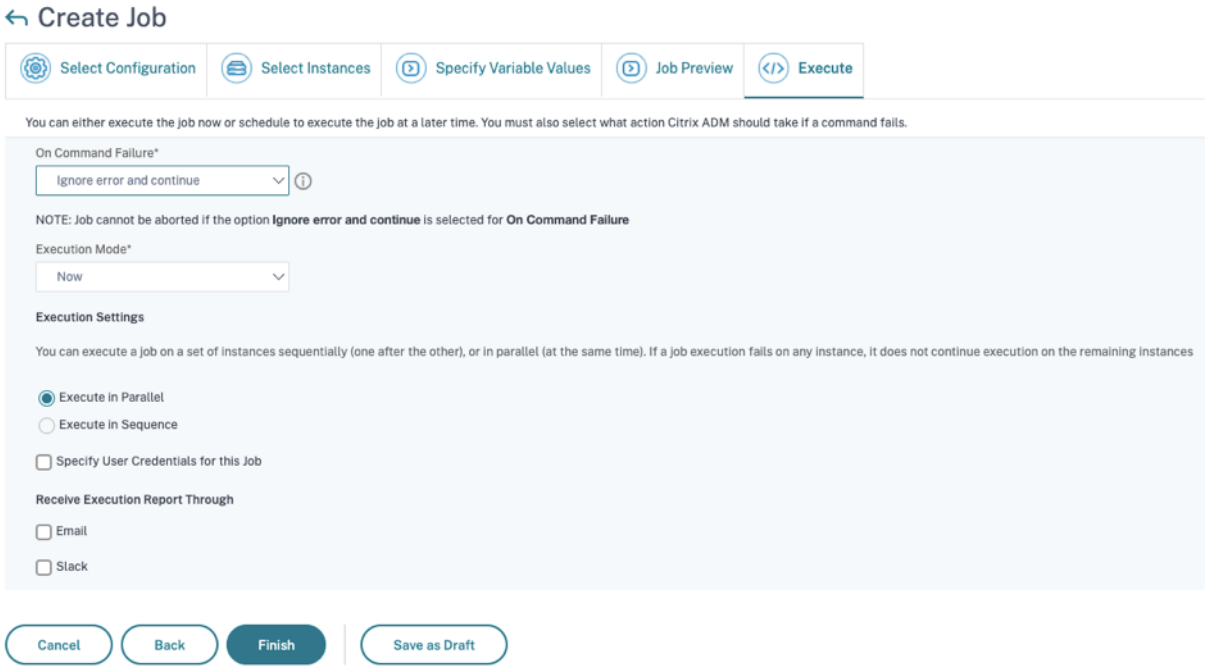
- saml_action_patset: agregar un nombre para la acción SAML
- saml_action_domain1: introduzca un dominio con el formato https://<example1.com>/
- saml_action_name: introduzca lo mismo de la acción SAML para la que está configurando el trabajo



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 todas las instancias vulnerables de NetScaler, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

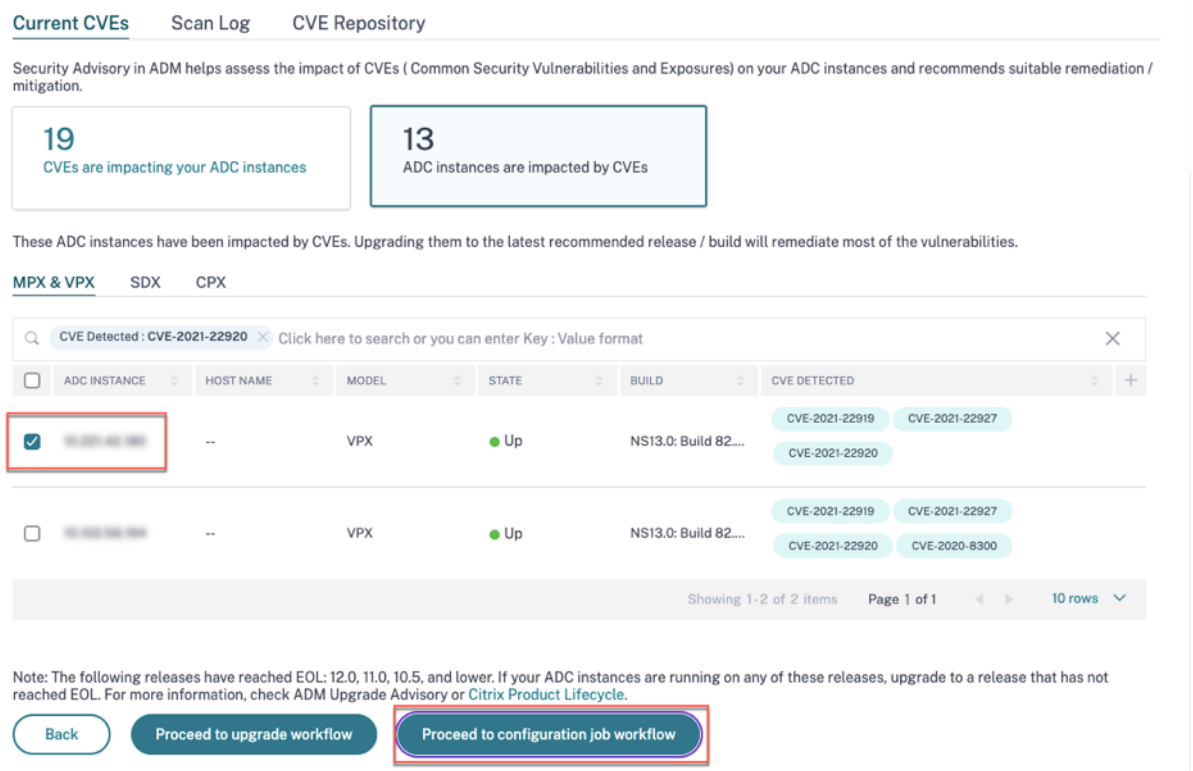
Escenario

En este escenario, dos instancias de NetScaler son vulnerables al CVE-2021-22920 y es necesario corregir todas las instancias. Siga estos pasos:

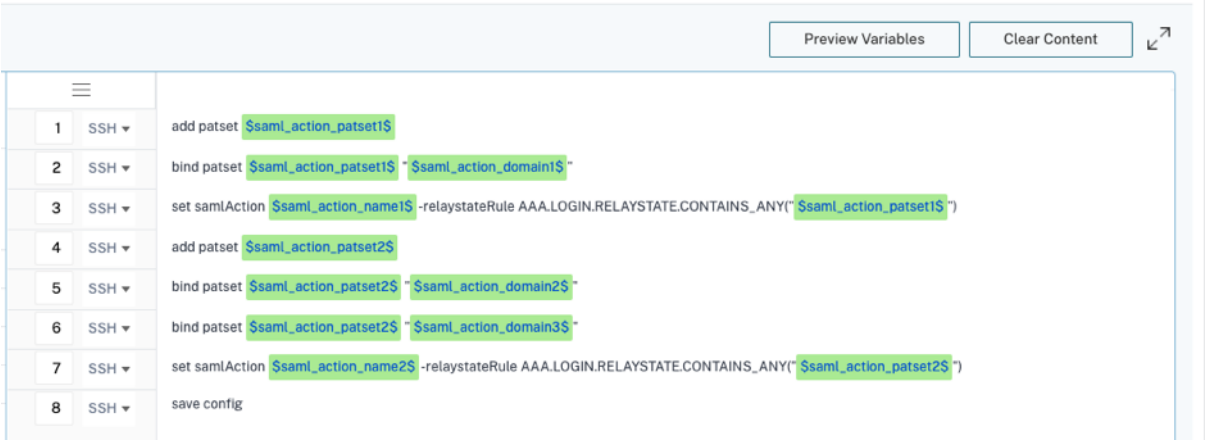
1. Actualice las tres instancias de NetScaler siguiendo los pasos que se indican en la sección «Actualizar una instancia» de este documento.
2. Aplique el parche de configuración a un NetScaler a la vez, mediante el flujo de trabajo de configuración. Consulte los pasos que se indican en la sección "Aplicar comandos de configuración" de este documento.

El NetScaler 1 vulnerable tiene dos acciones de SAML:

- La acción 1 de SAML tiene un dominio
- La acción 2 de SAML tiene dos dominios



Seleccione NetScaler 1 y haga clic en **Continuar con el flujo de trabajo del 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.

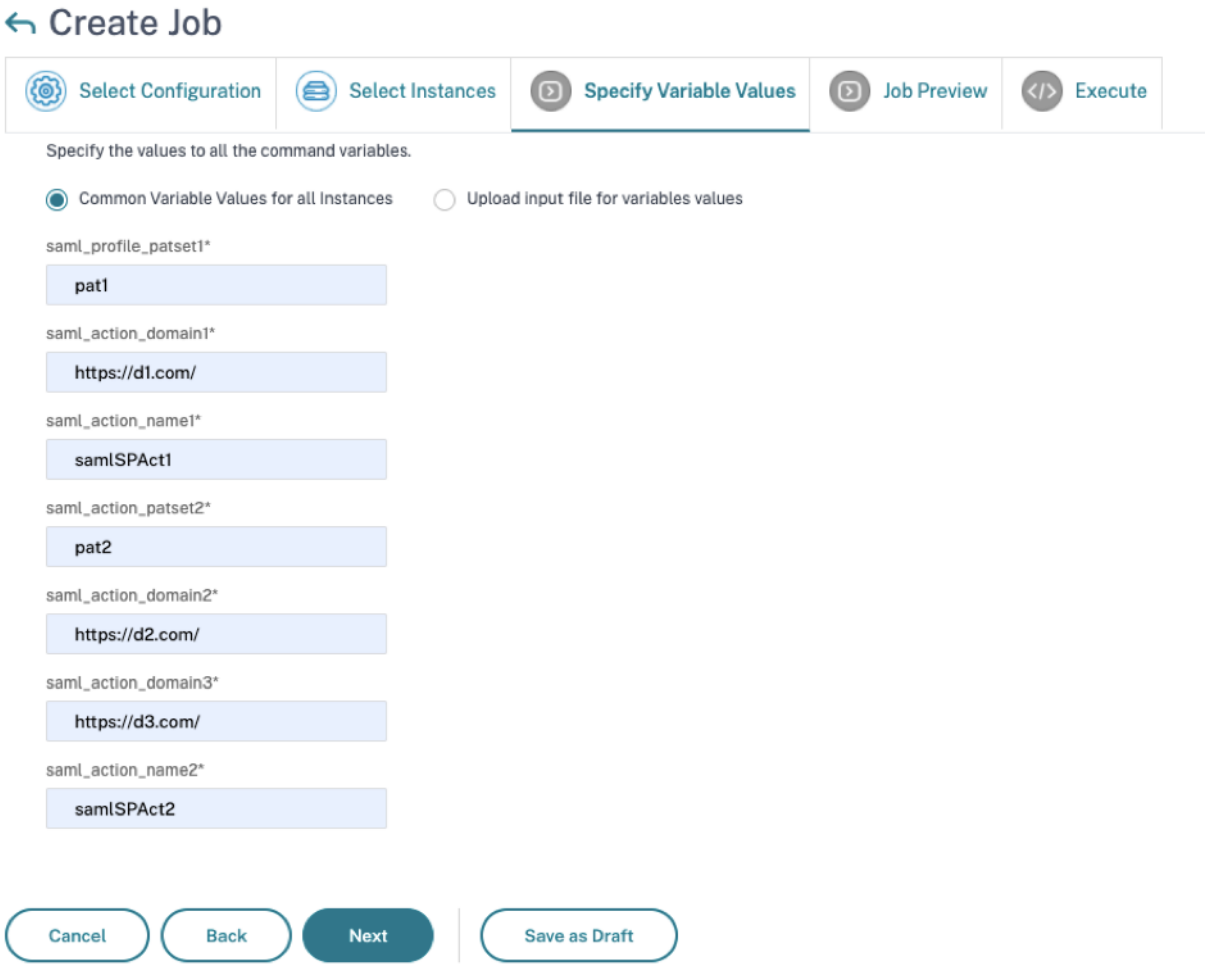


En la tabla siguiente se enumeran las definiciones de variables para los parámetros personalizados.

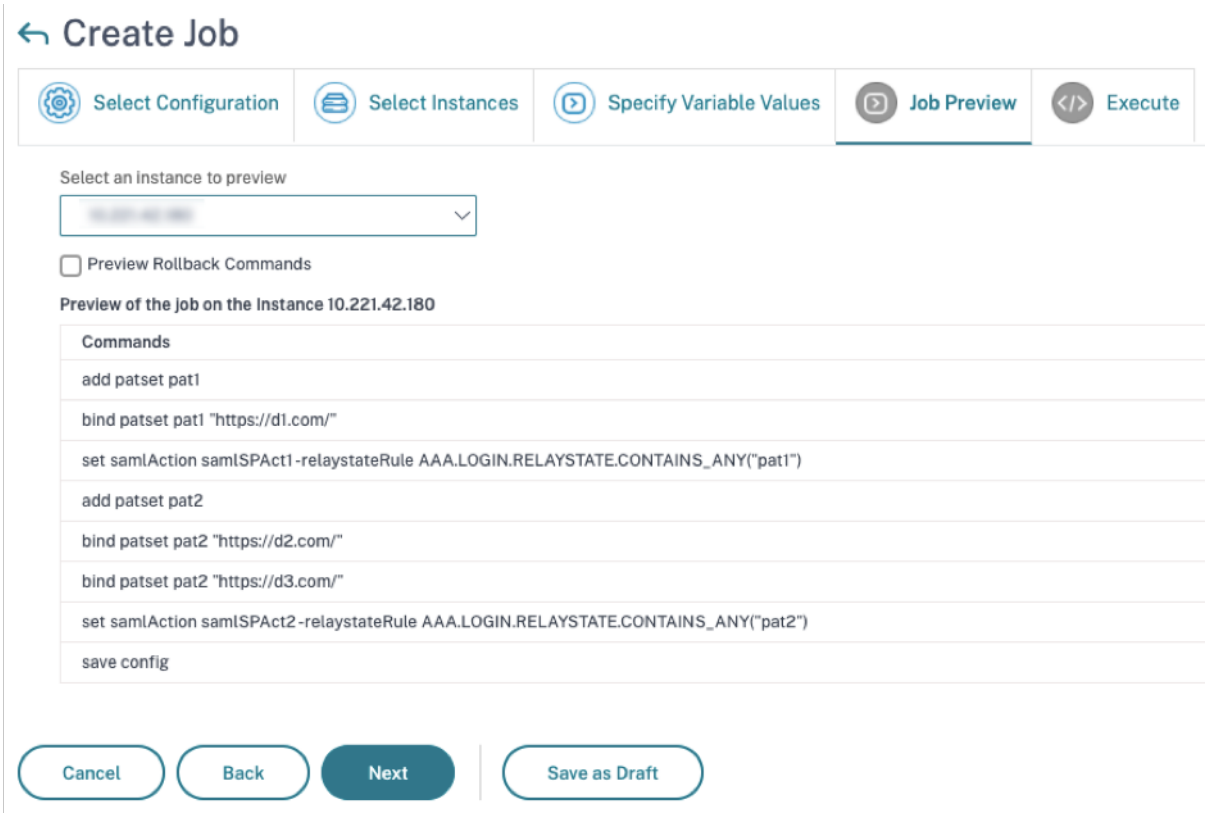
Tabla. Definiciones de variables para la acción SAML

Configuración de NetScaler	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 NetScaler 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.

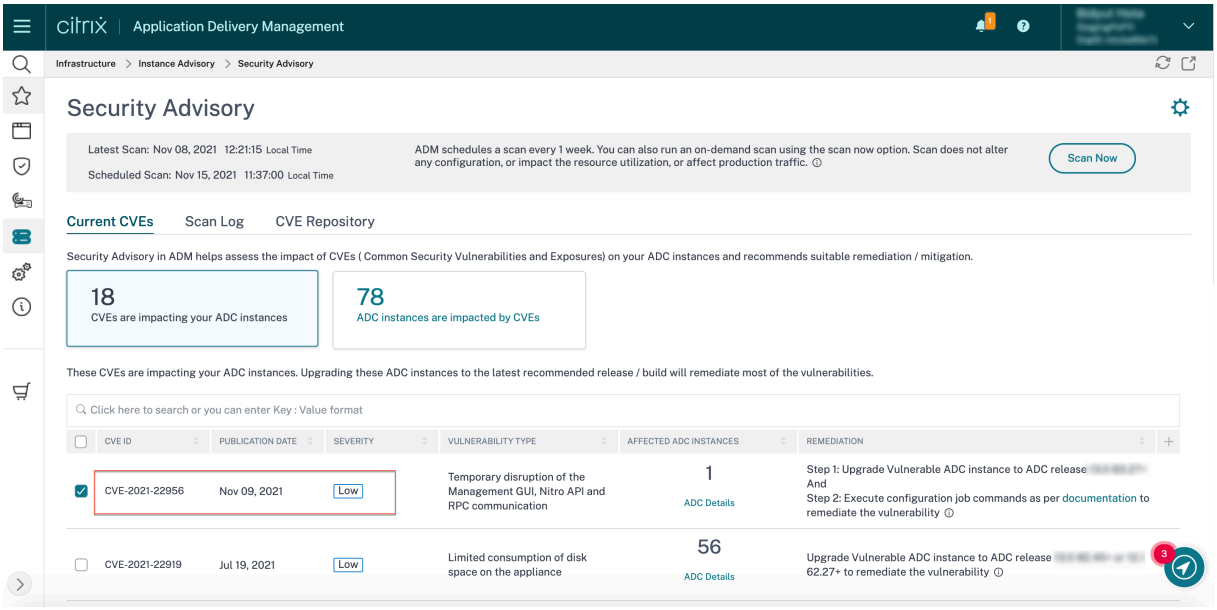
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para NetScaler 1, siga los mismos pasos para corregir NetScaler 2 y NetScaler 3. Una vez finalizada la corrección, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

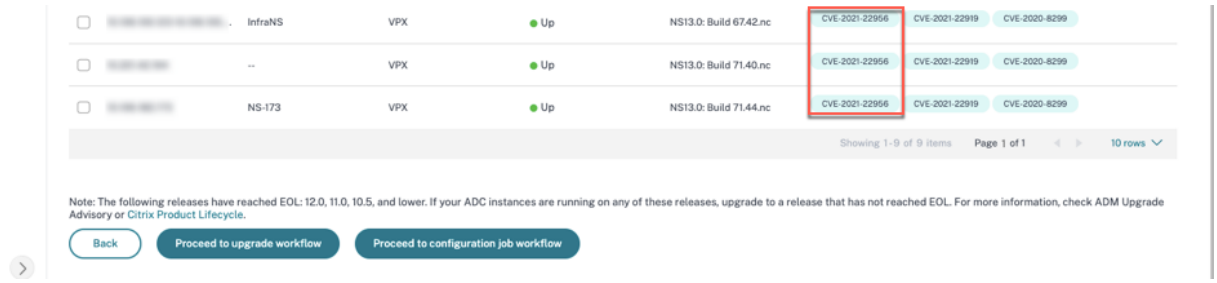
Identificar y corregir las vulnerabilidades del CVE-2021-22956

January 26, 2024

En el panel de asesoramiento de seguridad de NetScaler Console, en **CVE actuales > Las <number of>**instancias de NetScaler se ven afectadas por vulnerabilidades y exposiciones comunes (CVE), 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**.



Aparece <number of>la ventana de instancias de NetScaler afectadas por CVE. Aquí puede ver el recuento y los detalles de las instancias de NetScaler 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

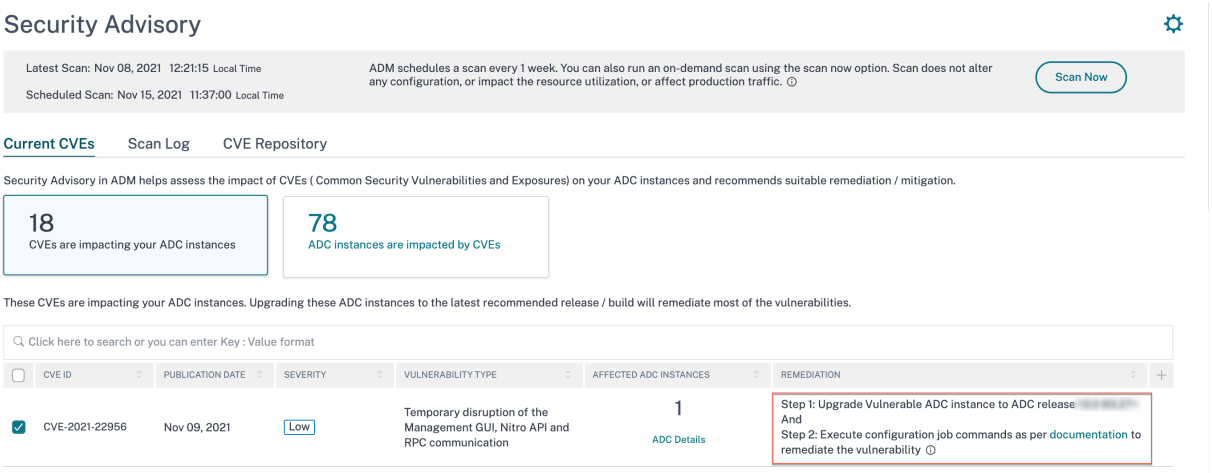
El CVE-2021-22956 requiere un análisis personalizado, en el que la consola de NetScaler se conecta con la instancia de NetScaler administrada y envía un script a la instancia. El script se ejecuta en la instancia de NetScaler y comprueba los parámetros del archivo de configuración de Apache (`httpd.conf 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 NetScaler Console es el estado de la vulnerabilidad en booleano (verdadero o falso). El script también devuelve a NetScaler Console

una lista de recuentos de max_clients para diferentes interfaces de red, por ejemplo, host local, NSIP y SNIP con acceso de administración. Puede ver un informe detallado de esta lista en el archivo CSV que puede descargar de la ficha **Registros de escaneo** de la página de **consejos de seguridad**.

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 NetScaler.

Remediar CVE-2021-22956

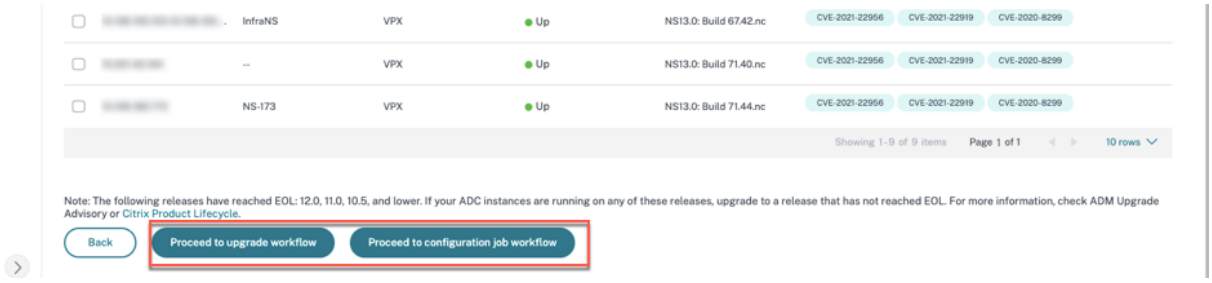
En el caso de las instancias de NetScaler afectadas por el CVE-2021-22956, la corrección es un proceso de dos pasos. En la GUI, en CVE **actuales > Las instancias de NetScaler se ven afectadas por** las CVE, puede ver los pasos 1 y 2.



Los dos pasos incluyen:

1. Actualización de las instancias vulnerables de NetScaler a una versión y 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 NetScaler afectadas por las CVE, verá dos flujos de trabajo independientes para este proceso de corrección de dos pasos: continuar con el flujo de trabajo de actualización y continuar con el flujo de trabajo de configuración.



Paso 1: Actualizar las instancias vulnerables de NetScaler

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 vulnerables de NetScaler ya pobladas.

Para obtener más información sobre cómo usar NetScaler Console para actualizar las instancias de NetScaler, consulte Crear un trabajo de actualización de NetScaler.

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de NetScaler vulnerables.

Paso 2: Aplicar los comandos de configuración

Después de actualizar las instancias afectadas, en la ventana **<number of> Instancias de NetScaler afectadas por** CVE, seleccione la instancia afectada por el CVE-2021-22956 y haga clic en **Continuar con el flujo de trabajo del trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

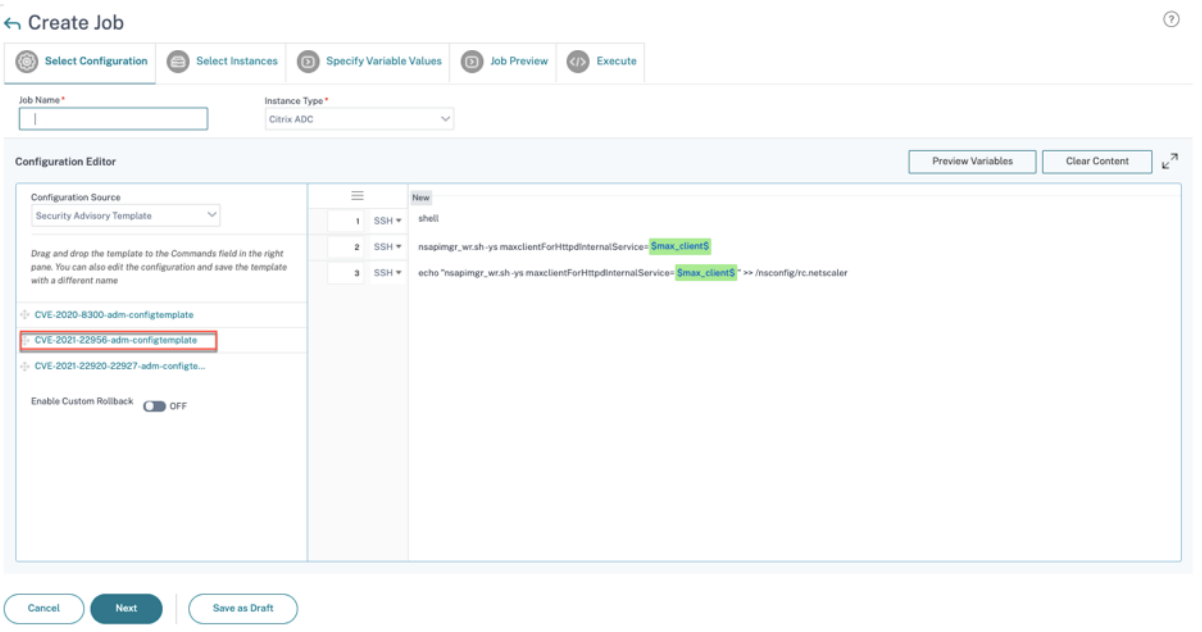
1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.
5. Ejecutar el trabajo.

Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**:

- En el caso de una instancia de NetScaler 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 **Proceder al 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.
- Solo para varias instancias de NetScaler afectadas por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene NetScaler 1, NetScaler 2 y NetScaler 3, y todos ellos solo se ven afectados 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.

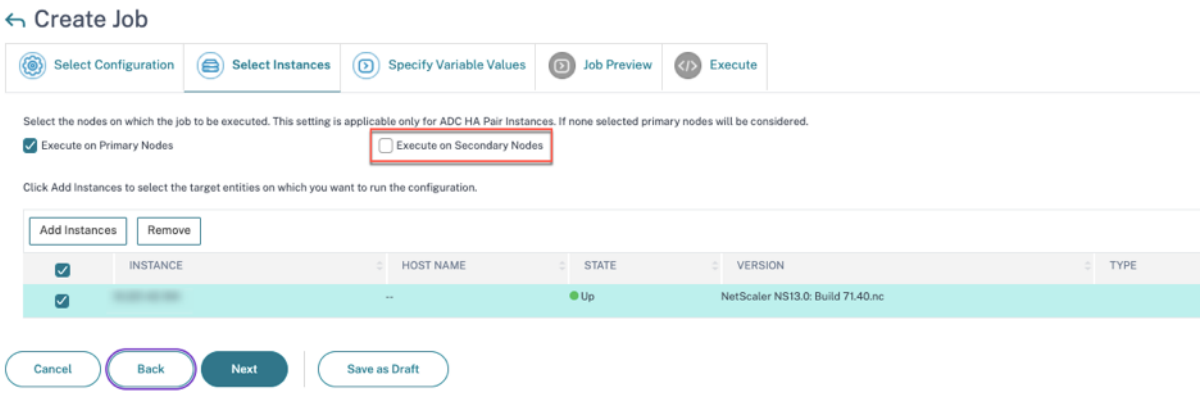
- En el caso de varias instancias de NetScaler afectadas por el CVE-2021-22956 y uno o varios otros CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren la aplicación de correcciones a cada NetScaler a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo del trabajo de configuración**, aparece un mensaje de error que le indica que debe ejecutar el trabajo de configuración en cada NetScaler a la vez NetScaler 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

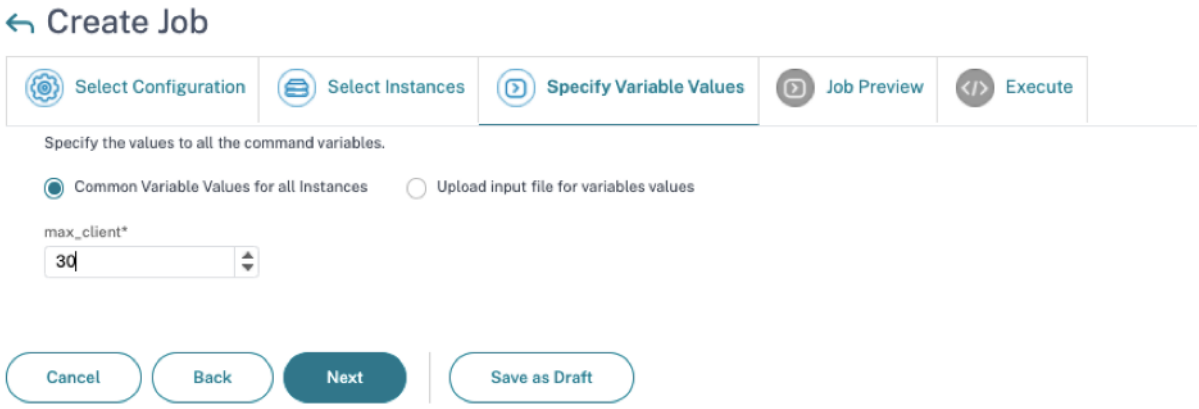
La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia. Si esta instancia forma parte de un par de HA, seleccione **Ejecutar en nodos secundarios**. Haz clic en **Siguiente** .



> **Nota**
>
> Para las instancias de NetScaler en modo clúster, mediante el asesoramiento de seguridad, la consola de NetScaler permite ejecutar el trabajo de configuración solo en el nodo del coordinador de configuración de clústeres (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.



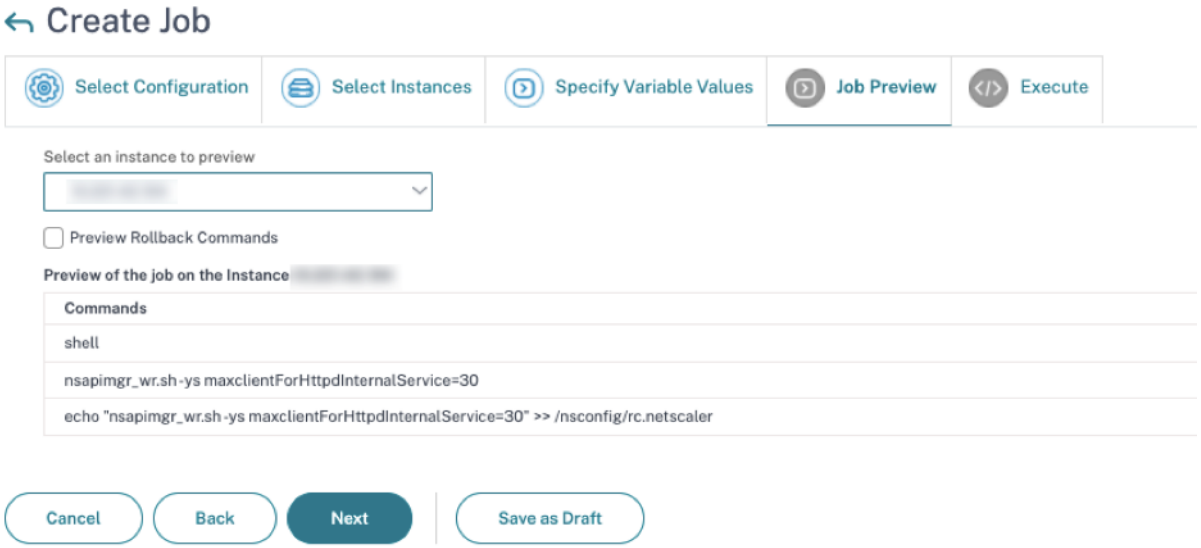
Seleccione una de las siguientes opciones para especificar las variables de sus instancias:

Valores de variables comunes para todas las instancias: introduzca un valor común para la variable `max_client`.

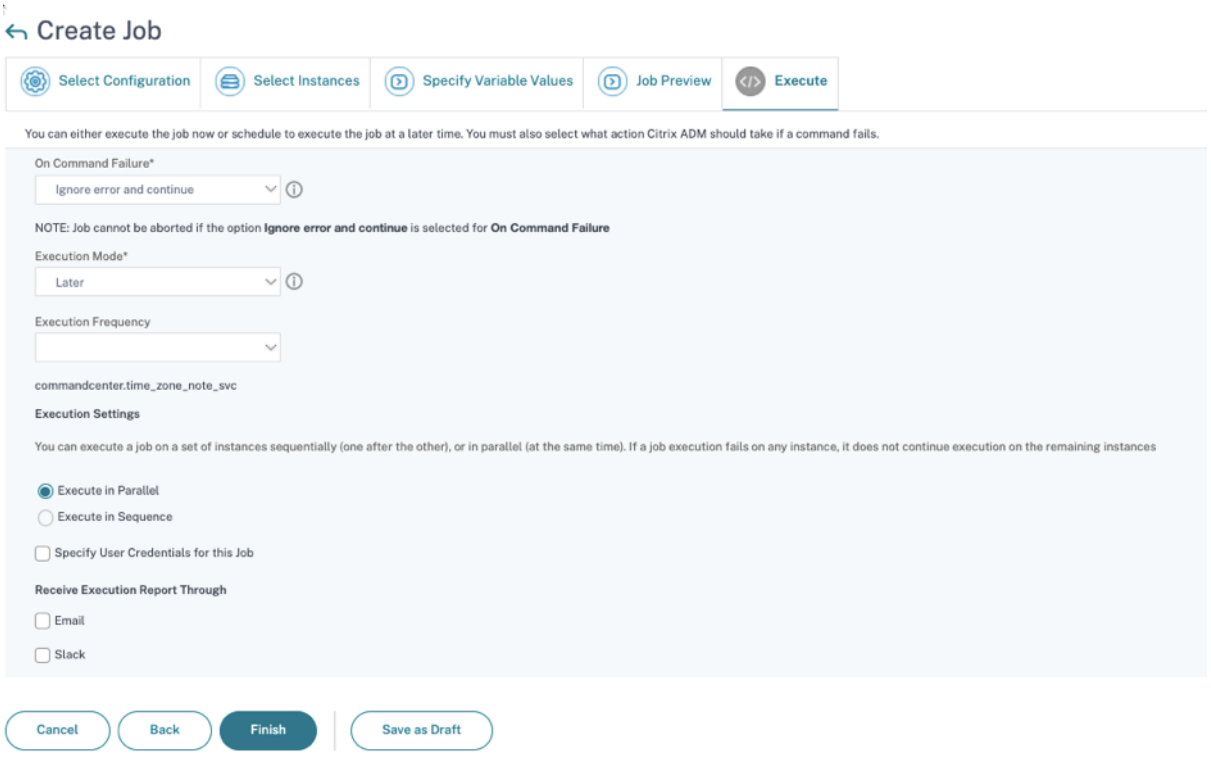
Cargar archivo de entrada para valoresde variables : haga clic en **Descargar archivo de claves** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca los valores de la variable `max_client`y, a continuación, cargue el archivo en el servidor de NetScaler Console. Consulte 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 valor actual establecido en el archivo `/etc/httpd.conf`de configuración del servidor HTTP Apache buscando la cadena `MaxClients`en la instancia de NetScaler

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.



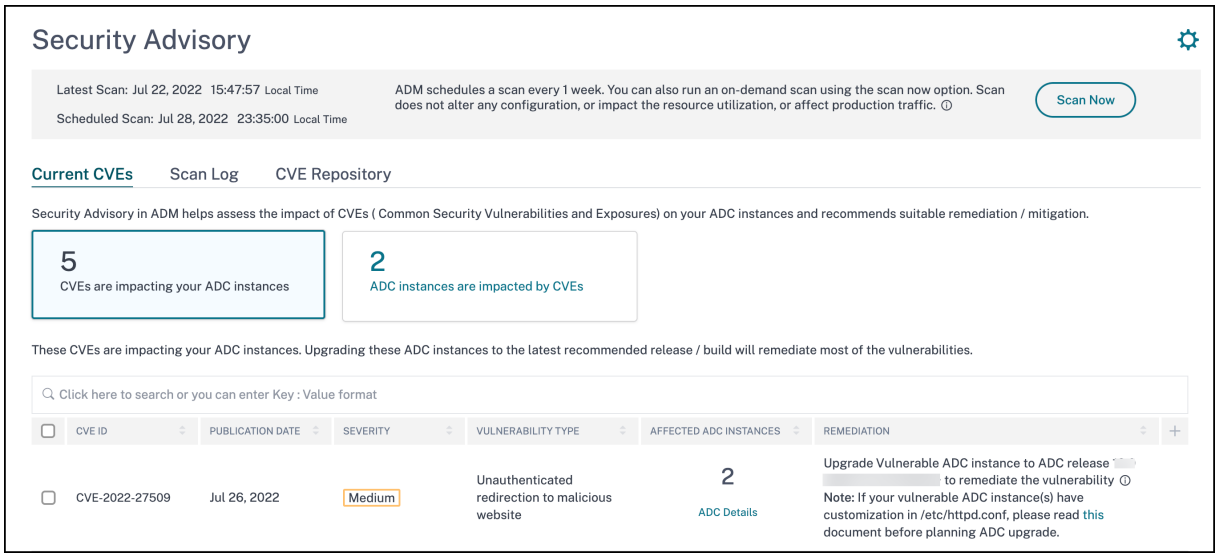
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para todas las instancias vulnerables de NetScaler, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Identificar y corregir las vulnerabilidades del CVE-2022-27509

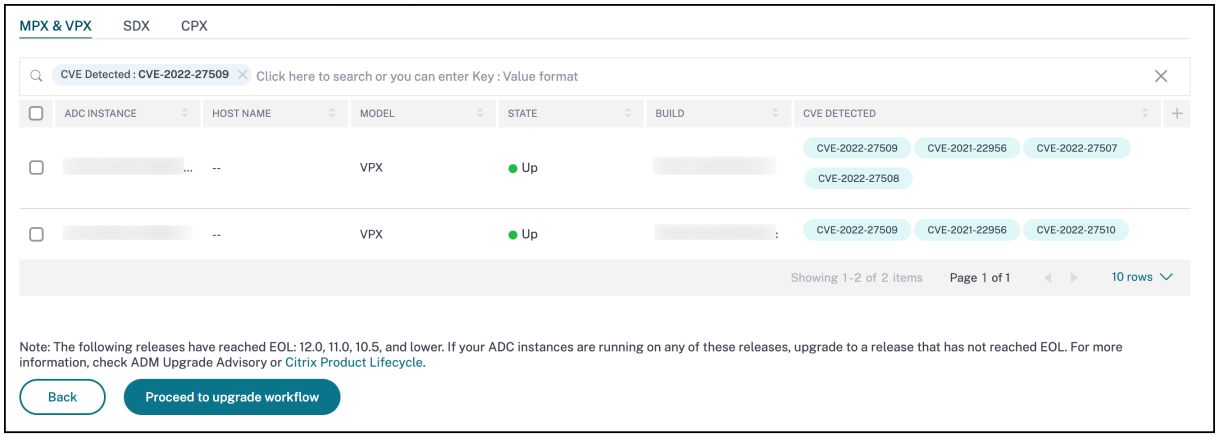
January 26, 2024

En el panel de asesoramiento de seguridad de **NetScaler Console, en CVE actuales, <number of> las instancias de NetScaler se ven afectadas por** las CVE, puede ver todas las instancias vulnerables debido al CVE-777727509. 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 NetScaler, descargue el informe CSV en la pestaña Registros de escaneo de Security Advisory.

Aparece la ventana **<number of>Instancias de NetScaler afectadas por** CVE . En la siguiente captura de pantalla, puede ver el recuento y los detalles de las instancias de NetScaler afectadas por el CVE-777727509.



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 análisis personalizado, la consola de NetScaler se conecta con la instancia de NetScaler gestionada y envía un script a la instancia. El script se ejecuta en la instancia de NetScaler 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 NetScaler.

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

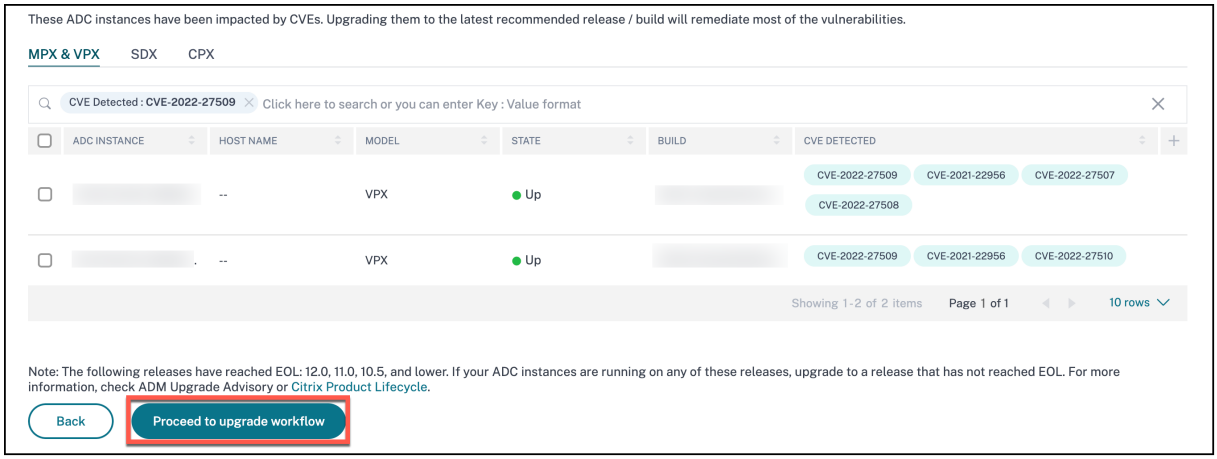
En el caso de las instancias de NetScaler afectadas por el CVE-777727509, la corrección es un proceso de un solo paso y es necesario actualizar las instancias de NetScaler vulnerables a una versión y compilación que tenga la solución. En la GUI, en CVE **actuales > Las instancias de NetScaler se ven afectadas por** las CVE, puede ver el paso a seguir para solucionarlo.

En CVE **actuales > Instancias de NetScaler afectadas por** las CVE , verá el siguiente flujo de trabajo para este proceso de corrección de un solo paso, que es el flujo de trabajo Continuar con la **actualización**.

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 vulnerables de NetScaler ya pobladas.

> **IMPORTANTE**
>
> Si sus instancias vulnerables de NetScaler tienen el archivo /etc/httpd.conf copiado en el directorio /nsconfig, consulte Consideraciones de actualización para configuraciones de NetScaler personalizadas antes de planificar la actualización de NetScaler.

Para obtener más información sobre cómo usar NetScaler Console para actualizar las instancias de NetScaler, consulte Crear un trabajo de actualización de NetScaler.



CVE no compatibles en el asesoramiento de seguridad

January 26, 2024

El asesoramiento de seguridad de NetScaler Console rastrea 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 corrección de las vulnerabilidades están fuera del alcance del asesoramiento de seguridad de NetScaler Console.

- **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.

La consola de NetScaler no admite la detección y reparación de las vulnerabilidades que afectan al complemento NetScaler Gateway para Windows. Además, las vulnerabilidades de los complementos de NetScaler Gateway no se pueden evaluar realizando ninguna comprobación por parte de NetScaler, verificando la versión de NetScaler o comprobando la configuración de NetScaler. 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 solución de esta vulnerabilidad están fuera del alcance del asesoramiento de seguridad de NetScaler Console.

Configuración

January 26, 2024

Una vez finalizada la configuración inicial, debe configurar ciertos ajustes para empezar a administrar la implementación por completo.

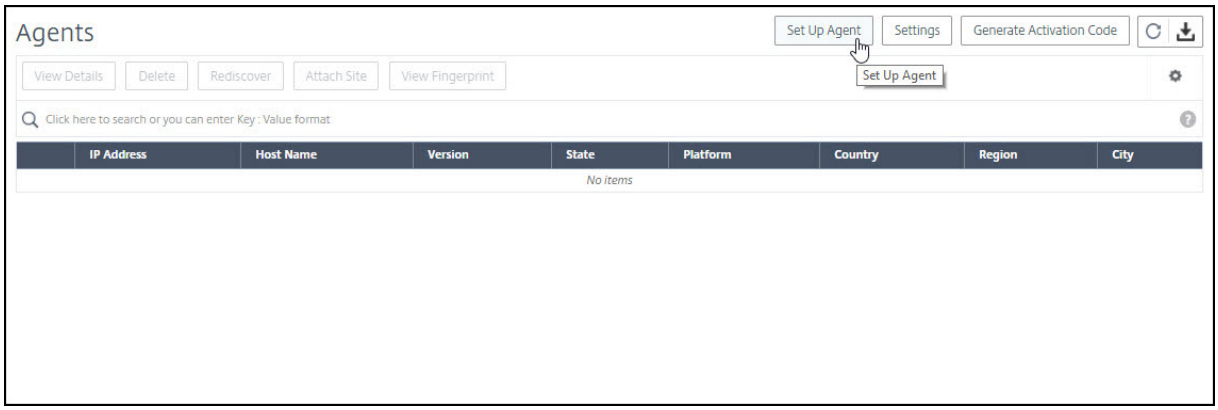
- Agregar varios agentes. La cantidad de agentes que se instalarán depende de la cantidad de instancias administradas en un centro de datos o en la nube y del rendimiento total. Citrix recomienda instalar al menos un agente por cada centro de datos.
- Agregar instancias. Puede agregar instancias al configurar la consola de NetScaler por primera vez o más adelante. Tienes que agregar instancias al servicio para empezar a gestionarlas y supervisarlas. Tras instalar varios agentes, debe agregar instancias y asociarlas a los agentes.
- Habilitar la analítica. 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.
- Configurar syslog en las instancias. Puede supervisar los eventos de syslog generados en las instancias de NetScaler si ha configurado el dispositivo para redirigir todos los mensajes de syslog a NetScaler Console. Para supervisar los eventos de syslog, primero debe configurar NetScaler Console como el servidor de syslog de la instancia de NetScaler.
- Configuración del control de acceso basado en roles. NetScaler Console proporciona un control de acceso (RBAC) detallado y basado en funciones con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales de su empresa.
- Configuración de los ajustes de Analytics. Puede configurar ciertos ajustes para garantizar una experiencia óptima con la función de análisis. Por ejemplo, puede especificar la duración durante la que quiere almacenar los datos de análisis históricos y también puede establecer umbrales y alertas para supervisar las métricas de análisis deseadas.

Agregar varios agentes

January 26, 2024

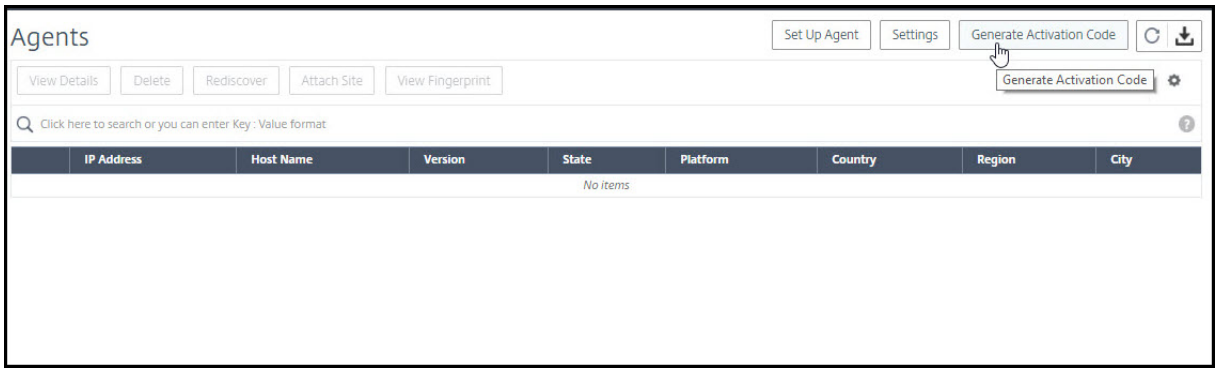
La cantidad de agentes que se instalarán depende de la cantidad de instancias administradas en un centro de datos y del rendimiento total. Citrix recomienda instalar al menos un agente por cada centro de datos.

Solo puede instalar un agente al iniciar sesión en el servicio por primera vez. Para agregar varios agentes, primero complete la configuración inicial y, a continuación, vaya a **Infraestructura > Instancias > Agentes** y haga clic en **Configurar agente.**



Descargue la imagen del hipervisor necesario e instale el agente siguiendo las instrucciones de Getting Started. Asegúrese de copiar la URL del servicio y el código de activación que aparecen en la pantalla, ya que debe introducir la URL del servicio y el código de activación al instalar el agente en el hipervisor. El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.

Puede usar la misma imagen para instalar varios agentes en el hipervisor. Sin embargo, no puede usar el mismo código de activación en varios agentes. Tras instalar un agente, vuelva a generar el código de activación para el siguiente agente. Para generar un nuevo código de activación, vaya a **Infraestructura > Instancias > Agentes**y haga clic en **Generar código de activación**.



Una vez que el agente se haya instalado y registrado correctamente, verifique el estado del agente en la GUI del servicio y agregue instancias a él.

> **Nota**
>
> También puede instalar un agente en la nube de Microsoft Azure o en la nube de AWS. La imagen del agente está disponible en el mercado en la nube correspondiente.
>
> - Para obtener instrucciones sobre la instalación de un agente en la nube de Microsoft Azure, consulte Instalar un agente de NetScaler en la nube de Microsoft Azure.
> - Para obtener instrucciones sobre la instalación de un agente en AWS, consulte Instalar un agente de NetScaler en AWS.

Configurar agentes para la implementación en varios sitios

January 26, 2024

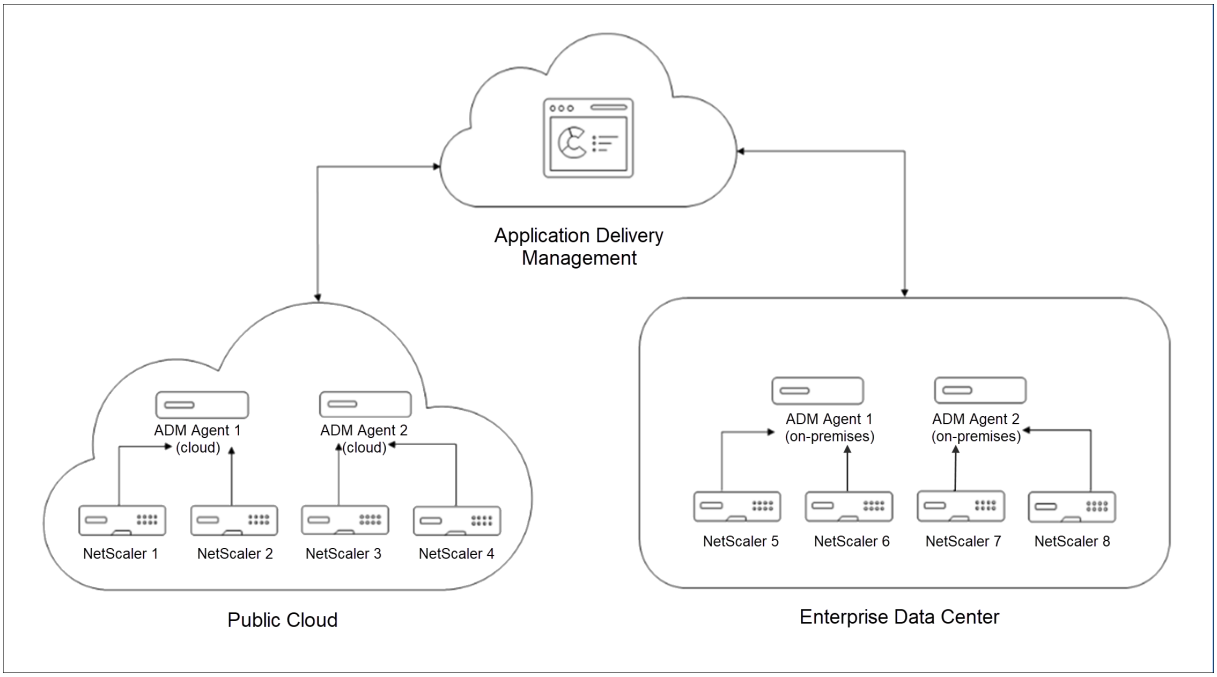
Los agentes actúan como intermediarios entre la consola de NetScaler y las instancias descubiertas en diferentes centros de datos y nubes públicas. NetScaler Console admite la conmutación por error de los agentes en un centro de datos o en una nube pública.

Las ventajas de instalar agentes son las siguientes:

- Las instancias configuradas para un agente envían los datos sin procesar directamente al agente en lugar de a NetScaler Console. El agente realiza el primer nivel de procesamiento de datos y envía los datos procesados en formato comprimido a la consola de NetScaler para su almacenamiento.
- Los agentes y las instancias se encuentran en el mismo centro de datos o nube 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 cambia a otro agente disponible en el mismo sitio.

Arquitectura

La siguiente figura ilustra las instancias de NetScaler configuradas en varios agentes en un centro de datos y una nube pública para lograr la conmutación por error de los agentes:



La nube pública tiene cuatro instancias de NetScaler y dos agentes. El centro de datos empresarial también tiene cuatro instancias de NetScaler y dos agentes. Cada agente está configurado con dos instancias de NetScaler.

Los agentes reciben datos directamente de las instancias configuradas. Una vez que el agente recibe los datos, los procesa y los envía a la consola de NetScaler en un formato comprimido. Los agentes se comunican con el servidor de NetScaler Console a través de un canal seguro.

En la nube pública, cuando el **agente 1** pasa a estar inactivo (estado INACTIVO), se produce una conmutación por error del agente. NetScaler Console redistribuye las instancias de NetScaler del **Agente 1** con el **Agente 2**. La redistribución de instancias se produce en un centro de datos corporativo si uno de los agentes falla en el centro de datos.

Para instalar un agente, consulte Instalar un agente de NetScaler .

Conmutación por error del agente

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, la consola de NetScaler redistribuye las instancias de NetScaler del agente inactivo con otros agentes activos.

> **Importante**
>
> - La conmutación por error del agente no tiene en cuenta las instancias CPX.
> - Asegúrese de que la función de conmutación por error del agente esté habilitada en su

> cuenta. Para habilitar esta función, consulte Habilitar o deshabilitar las funciones de la consola NetScaler .
>
> - 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 NetScaler Console:

1. Vaya a **Infraestructura > Instancias > Agentes**.
2. Seleccione el agente que quiera adjuntar a un sitio.
3. Especifique el sitio de la lista. Si quiere agregar un nuevo sitio, haga clic en **Agregar**.
4. Haga clic en **Guardar**.

Para lograr una conmutación por error de los agentes, seleccione los agentes uno por uno y adjúntelos al mismo sitio.

Por ejemplo, dos agentes 10.106.1xx.2x y 10.106.1xx.7x están conectados y operativos en el sitio de Bangalore. Si un agente queda inactivo, NetScaler Console lo detecta y muestra su estado como inactivo.

Cuando un agente pasa a estar inactivo (estado inactivo) en un sitio, NetScaler Console espera unos minutos hasta que el agente se active (estado activo). Si el agente permanece inactivo, NetScaler Console redistribuye automáticamente las instancias entre los agentes disponibles en el mismo sitio. Esta redistribución puede tardar aproximadamente 10-15 minutos.

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

Las instancias conectadas y reconfiguradas automáticamente a los agentes del mismo sitio para destino de captura, servidor syslog y análisis.

Configuración de las opciones de actualización del agente

January 26, 2024

En NetScaler Console, los agentes que se ejecutan en la versión de software 12.0 build 507.110 y posteriores se actualizan automáticamente a las versiones más recientes y recomendadas por NetScaler Console. El agente se actualiza cuando hay una nueva versión disponible o en el momento que usted especifique.

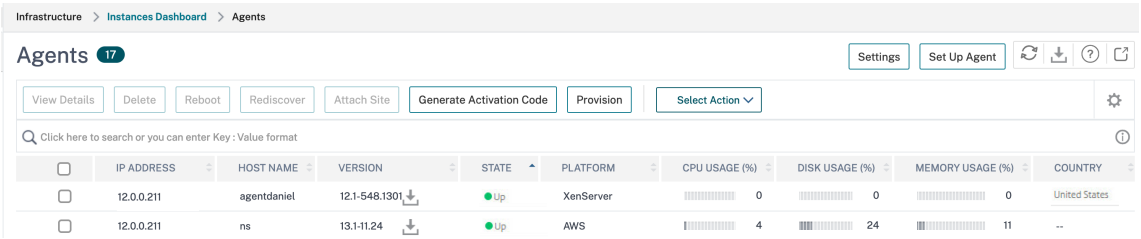
Para ver la versión actual y la versión recomendada de sus agentes, vaya a **Infraestructura > Instancias > Agentes**.

De forma predeterminada, un agente se actualiza automáticamente cuando hay una versión más reciente disponible. Sin embargo, puede programar una actualización para cada uno de los agentes.

Durante la actualización, puede haber un tiempo de inactividad de aproximadamente cinco minutos.

Para configurar los ajustes de actualización del agente:

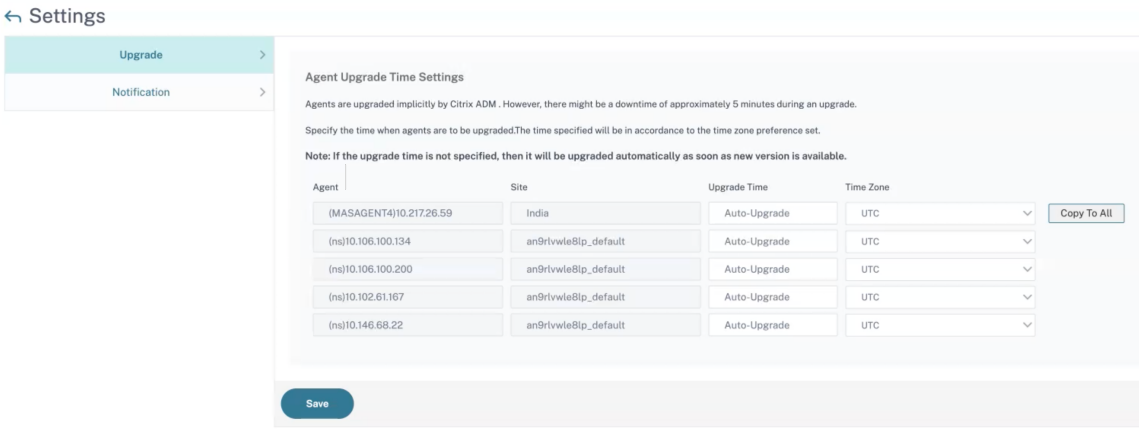
1. Vaya a **Infraestructura > Instancias > Agentes**y haga clic en **Configuración**.



2. Especifique cuándo quiere que se inicie la actualización para cada uno de los agentes.

   Puede utilizar una de las siguientes opciones para actualizar el agente:

   - Actualización automática: Seleccione **Actualización automática** para que el agente se actualice cuando haya una nueva imagen del agente disponible. Si no introduce ningún valor, la **opción Actualización automática** está seleccionada de forma predeterminada.
   - Establezca una hora específica: introduzca la hora (en formato hh:mm) y seleccione la zona horaria en la que desea que NetScaler Console actualice automáticamente el agente.



   Puede hacer clic en **Copiar a todos** para aplicar el mismo tiempo de actualización a todos los agentes.

3. Haga clic en **Guardar**.

   Esta configuración persiste para futuras actualizaciones del agente hasta que cambie la configuración.

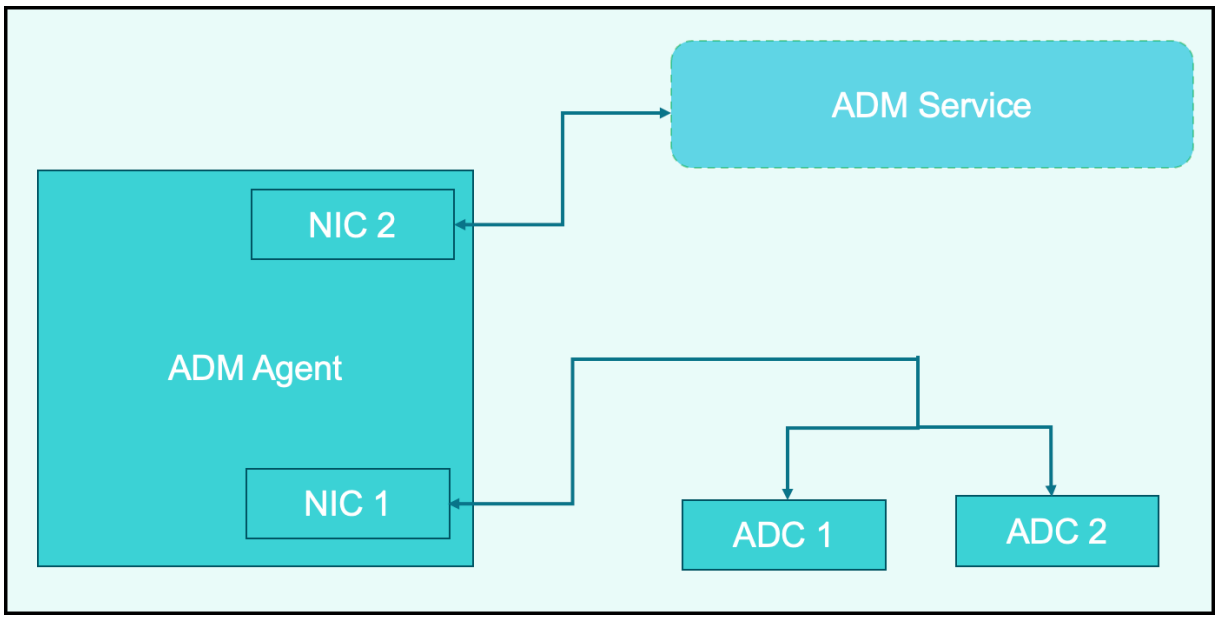
Soporte de doble NIC en la consola NetScaler

January 26, 2024

Puede configurar dos NICs en un agente. Con la arquitectura de doble NIC, el agente podrá:

- Establezca la comunicación entre el agente y las instancias de NetScaler: puede usar la primera NIC para aislar el tráfico que se recibe y envía a través de la consola de NetScaler y también para comunicarse entre NetScaler Console y sus instancias de NetScaler administradas en otra red.
- Establezca la comunicación entre el agente y la consola de NetScaler: puede usar la segunda NIC para administrar la consola de NetScaler que está en una red y realizar tareas administrativas.

> **Nota**
>
> No puede intercambiar la funcionalidad y la configuración de ambas NICS.



En este caso, como administrador, puede:

- Configure la dirección IP para el tráfico entre NetScaler Console y sus instancias de NetScaler administradas.
- Configure la dirección IP para administrar el software NetScaler Console para realizar todas las tareas administrativas del software.

> **Nota**
>
> No es obligatorio configurar NIC duales para un agente. Es opcional y solo se requiere cuando es necesario separar el tráfico entre el agente, el servicio de NetScaler Console y las instancias de NetScaler.

Requisitos previos

- Asegúrese de haber implementado y configurado el agente NetScaler 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.

Modificar las direcciones de red de la NIC IPV4

1. Abra una conexión SSH a la consola del agente de NetScaler 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 y la comunicación de NetScaler
    - NIC 2: para la comunicación entre el agente y la consola NetScaler


```
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.

Agregar instancias

January 26, 2024

Puede agregar instancias al configurar la consola de NetScaler por primera vez o más adelante .

Las instancias son dispositivos NetScaler o dispositivos virtuales que desea descubrir, administrar y monitorear desde NetScaler Console. Puede agregar los siguientes dispositivos NetScaler y dispositivos virtuales a NetScaler Console:

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway
- Citrix Secure Web Gateway

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

Especifique un perfil de instancia que NetScaler Console pueda usar para acceder a la instancia. Este perfil de instancia contiene el nombre de usuario y la contraseña de las instancias que quiere agregar al servicio. Para cada tipo de instancia, está disponible un perfil predeterminado. Por ejemplo, ns-root-profile es el perfil predeterminado para las instancias de NetScaler. Las credenciales predeterminadas de administrador de NetScaler definen este perfil. 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 acceder a las GUI de las instancias de NetScaler desde la consola de NetScaler después de agregar las instancias a la consola de NetScaler. Para acceder a las instancias de NetScaler desde la consola de NetScaler, debe estar conectado a la red Citrix.

> **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 Console, la dirección IP del clúster representa el clúster.
> - Para las instancias de NetScaler configuradas como un par HA, al agregar una instancia, la otra instancia del par se agrega automáticamente.

> - Para asegurarse de que el usuario de NetScaler tiene todos los privilegios, asigne permisos de superusuario al usuario en NetScaler. Para obtener más información, consulte Directivas de usuario, grupos de usuarios y comandos

Cómo crear un perfil NetScaler

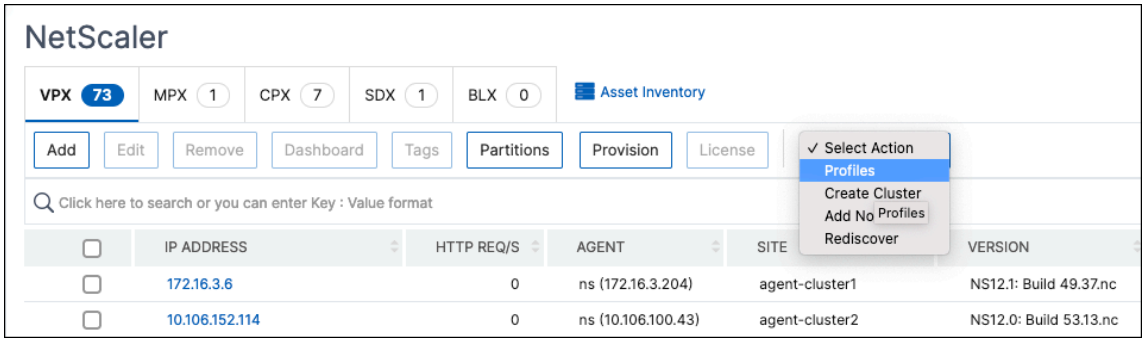
El perfil de NetScaler contiene el nombre de usuario, la contraseña, los puertos de comunicación y los tipos de autenticación de las instancias que desea agregar a NetScaler Console. Para cada tipo de instancia, está disponible un perfil predeterminado. Por ejemplo, `nsroot` es el perfil predeterminado 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.

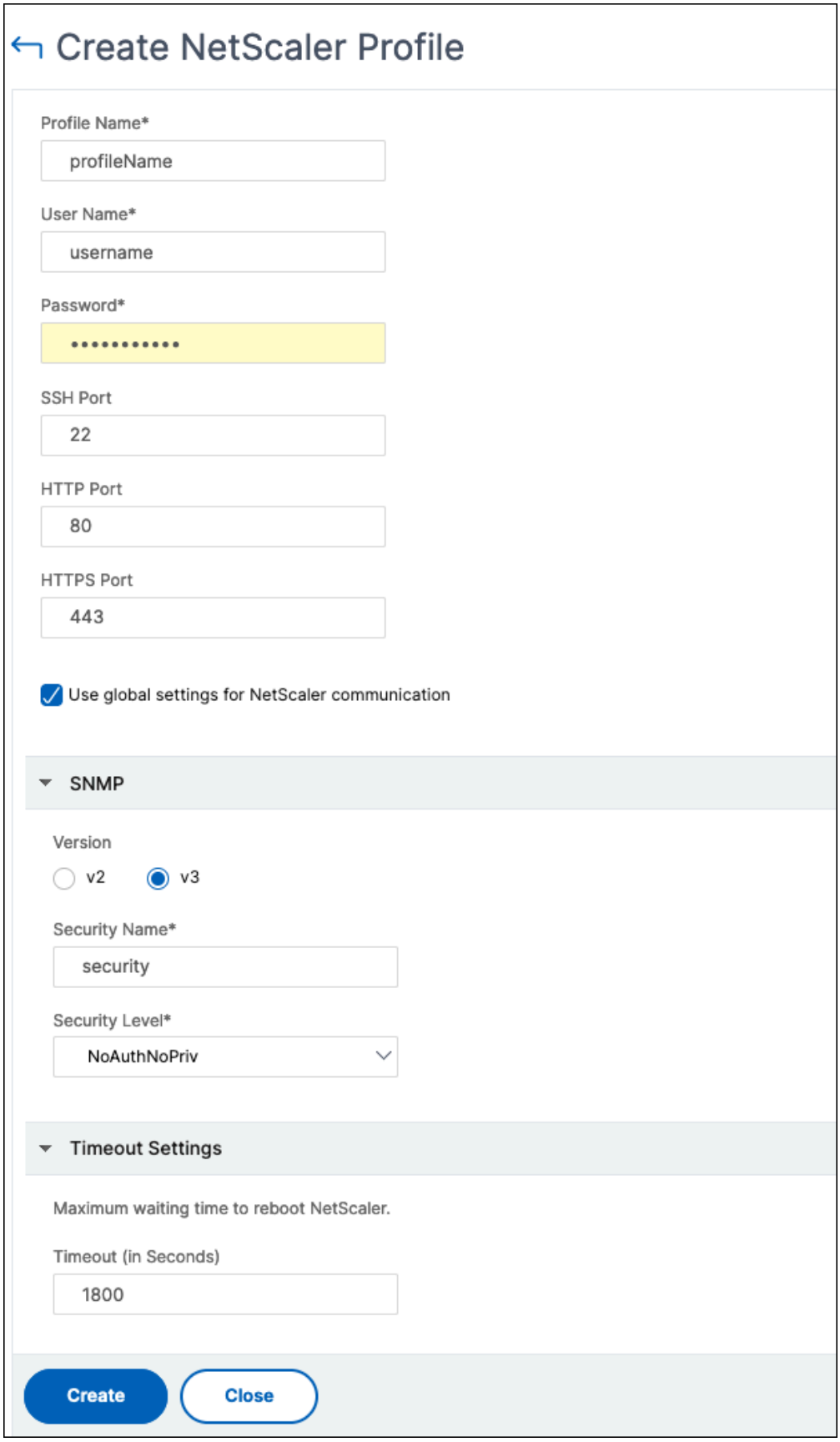
> **Nota:**
>
> Asegúrate de usar la cuenta de superadministrador para crear un perfil de instancia.

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 Console y la instancia de NetScaler.

e) **Puerto**HTTP: especifique el puerto para la comunicación HTTP entre NetScaler Console 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 usar para la comunicación entre NetScaler Console y NetScaler CPX.

f) **Puerto**HTTPS: especifique el puerto para la comunicación HTTPS entre NetScaler Console 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 usar para la comunicación entre NetScaler Console y NetScaler CPX.

g) **Usar la configuración global para la comunicación**de NetScaler : seleccione esta opción si quiere usar la configuración del sistema para la comunicación entre la consola de NetScaler 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**del tiempo de espera : especifique el tiempo que debe esperar NetScaler Console antes de enviar una solicitud de conexión a la instancia de NetScaler tras un reinicio.

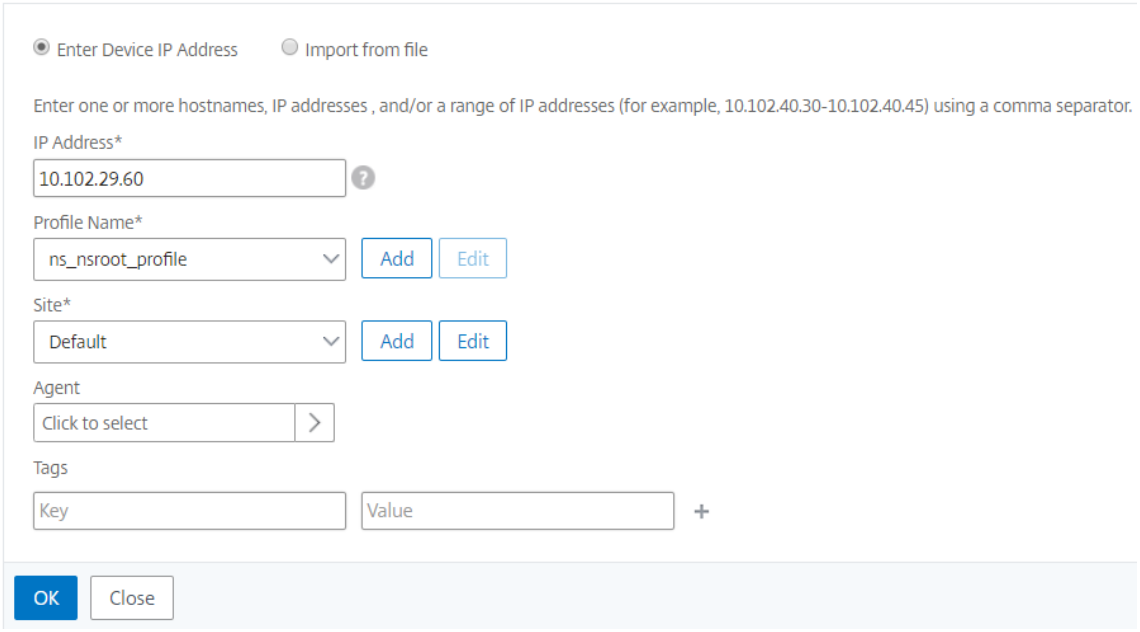
j) Seleccione **Crear**.

Para añadir una instancia de NetScaler a NetScaler Console

> **Nota**
>
> Realice esta tarea para agregar todas las demás instancias de NetScaler excepto la instancia de NetScaler CPX.

1. Vaya a **Infraestructura > Instancias > NetScaler**. En Instancias, seleccione el tipo de instancia que quiere agregar (por ejemplo, NetScaler VPX) y haga clic en **Agregar**.
2. Seleccione una de estas opciones:
   - **Introduzca la dirección IP del dispositivo**: para las instancias de NetScaler, especifique el nombre de host o la dirección IP de cada instancia, o un rango de direcciones IP.
   - **Importar desde un archivo**: Desde el sistema local, sube un archivo de texto que contenga las direcciones IP de todas las instancias que quieras agregar.
3. (Opcional) Seleccione **Activar adición de dispositivo en caso de fallo de inicio de sesión por primera vez**. Con esta opción, puede agregar la instancia incluso sin credenciales válidas.
4. En Nombre del **perfil**, seleccione el perfil de instancia adecuado o cree un perfil haciendo clic en el icono **+**.
5. En **Sitio**, seleccione el sitio en el que quiere agregar la instancia.
6. En **Agente**, seleccione el agente al que quiere asociar las instancias y, a continuación, haga clic en **Aceptar**.

   Si solo hay un agente configurado en la consola de NetScaler, ese agente se selecciona de forma predeterminada.



Para agregar una instancia de NetScaler CPX en NetScaler Console

1. Vaya a **Infraestructura > Instancias**. En **Instancias**, seleccione **NetScaler** y seleccione la ficha CPX.
2. Haga clic en **Agregar**.
3. Seleccione una de estas opciones:
   - **Introduzca la dirección IP del dispositivo**. Especifique el nombre de host o la dirección IP de cada instancia, o un rango de direcciones IP.
   - **Importar desde un archivo**. Desde el sistema local, cargue un archivo de texto que contenga las direcciones IP de todas las instancias que quiera agregar.
4. (Opcional) Seleccione **Activar adición de dispositivo en caso de fallo de inicio de sesión por primera vez**. Con esta opción, puede agregar la instancia incluso sin credenciales válidas.
5. En el campo **IP redirigible o IP de Docker**, introduzca la dirección IP. La dirección IP puede ser la instancia CPX de NetScaler (si se puede acceder a ella) o el host de Docker.
6. En el campo **Nombre de perfil**, seleccione el perfil de instancia correspondiente o cree un perfil haciendo clic en el icono +.

   > **Nota**
   >
   > Al crear un perfil, asegúrese de especificar los detalles de los puertos HTTP, HTTPS, SSH y SNMP del host. También puede especificar el rango de puertos que publica el host en el campo Puerto de inicio y Número de puertos.

7. Como opción, seleccione el sitio en el que quiere implementar la instancia de CPX. También puede crear un sitio haciendo clic en **Agregar**.
8. Si está disponible, seleccione el agente de la lista de agentes.
9. Haga clic **en**Aceptar para iniciar el proceso de agregar instancias a NetScaler Console.

   > **Nota**
   >
   > Si quiere volver a descubrir una instancia, lleve a cabo los siguientes pasos:
   >
   > a) Vaya a **Infraestructura > Instancias > NetScaler** > **CPX**.
   > b) Selecciona la instancia que quieres volver a descubrir.
   > c) En la lista **Seleccionar acción**, haga clic en **Redescubrir**.

Para agregar una instancia de NetScaler BLX independiente en NetScaler Console

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. (Opcional) Seleccione **Activar adición de dispositivo en caso de fallo de inicio de sesión por primera vez**. Con esta opción, puede agregar la instancia incluso sin credenciales válidas.
4. Seleccione la opción **Independiente** de la lista **Tipo de Instancia**.
5. En el campo **Dirección IP**, especifique la dirección IP de la instancia de BLX.
6. En el campo **Dirección IP del host**, especifique la dirección IP del servidor Linux en el que está alojada la instancia de BLX.
7. En la lista **de nombres de perfil**, seleccione el perfil adecuado para una instancia de BLX o cree un perfil.

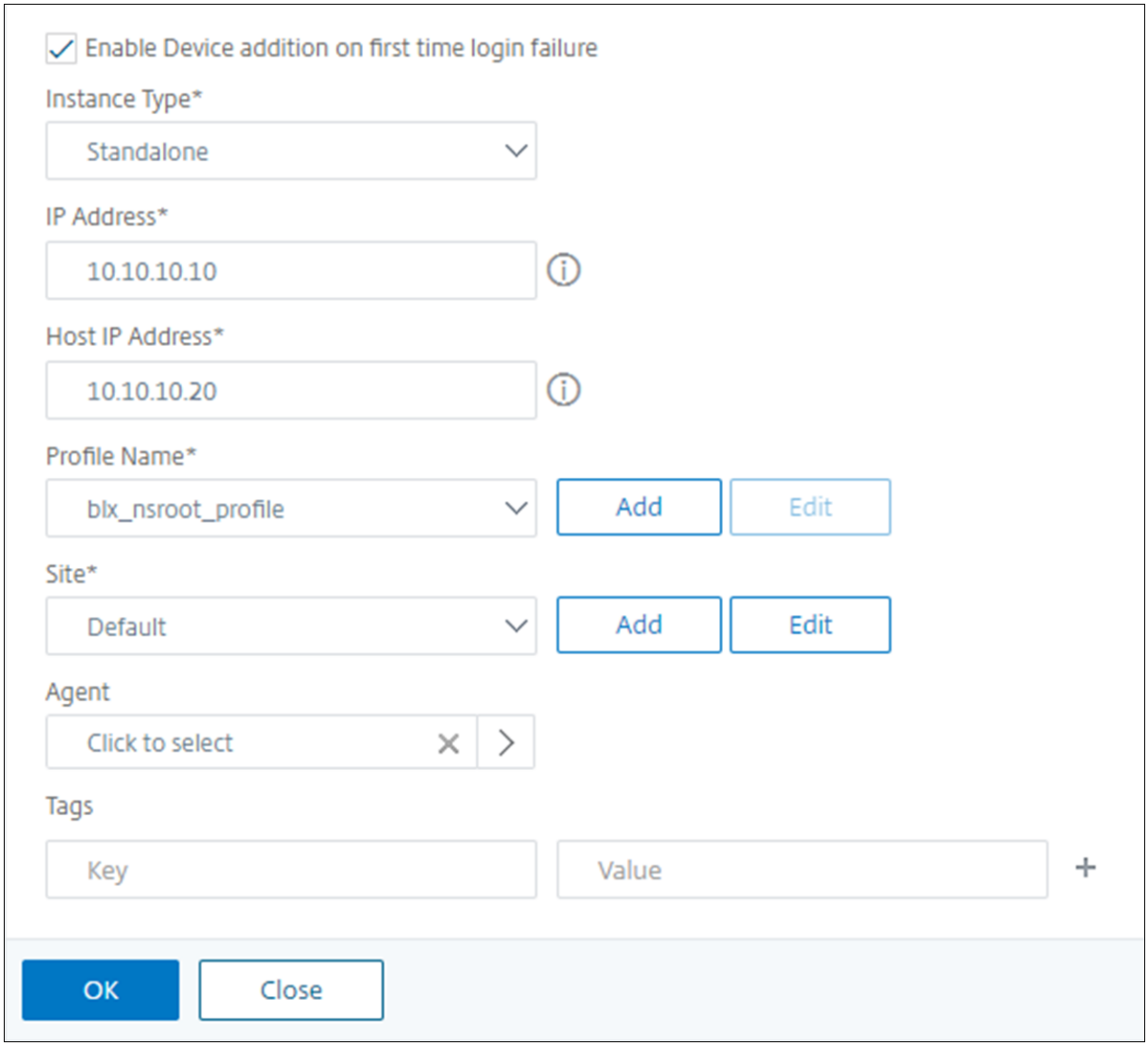
   Para crear un perfil, haga clic en **Agregar**.

   > **Importante**
   >
   > Asegúrese de haber especificado el nombre de usuario 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 al que quiere asociar la instancia.

   Si solo hay un agente configurado en la consola de NetScaler, ese agente se selecciona de forma predeterminada.
10. Haga clic en **Aceptar**.



Para agregar instancias de NetScaler BLX de alta disponibilidad en NetScaler Console

Las instancias de NetScaler BLX de alta disponibilidad que se ejecutan en diferentes servidores host Linux. Un servidor Linux no puede alojar más de una instancia de BLX.

1. En la ficha **BLX**, haga clic en **Agregar**.
2. (Opcional) Seleccione **Activar adición de dispositivo en caso de fallo de inicio de sesión por primera vez**. Con esta opción, puede agregar la instancia incluso sin credenciales válidas.
3. Seleccione la opción **Alta disponibilidad** en 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 el campo **Dirección IP del mismo** nivel, especifique la dirección IP de la instancia BLX homóloga.
7. 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.
8. En la lista **de nombres de perfil**, seleccione el perfil adecuado para una instancia de BLX o cree un perfil.

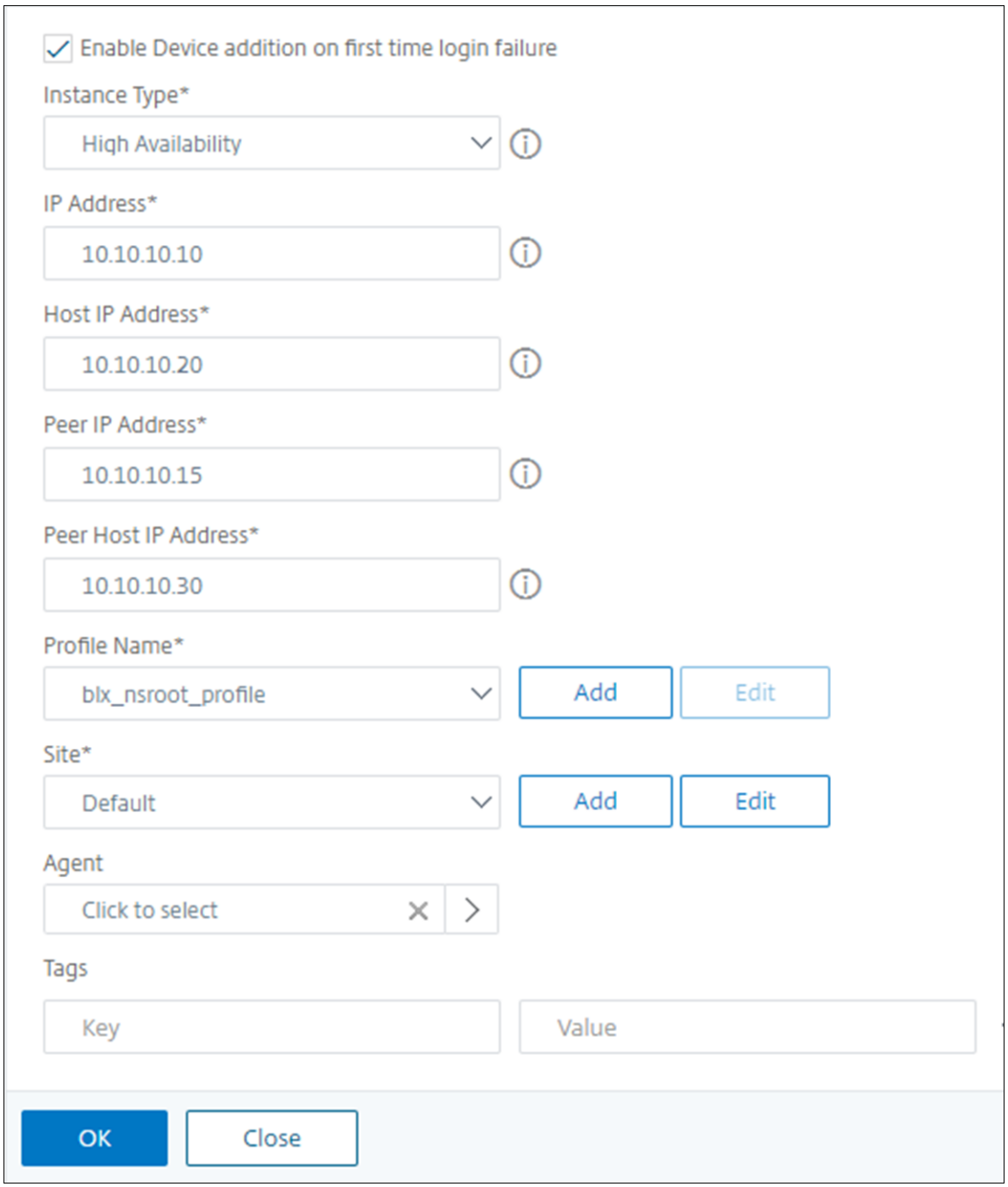
   Para crear un perfil, haga clic en **Agregar**.

   > **Importante**
   >
   > Asegúrese de haber especificado el nombre de usuario host y la contraseña correctos del servidor Linux en el perfil.

9. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

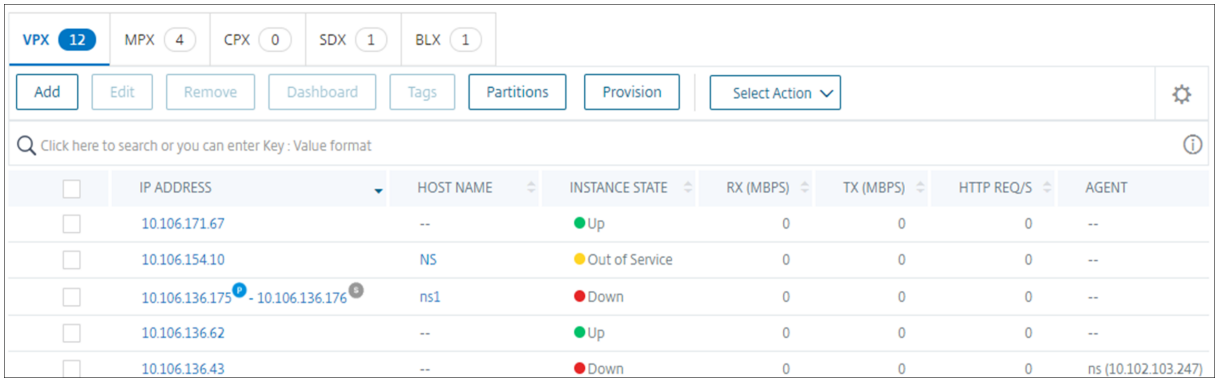
   Si quieres agregar un sitio, haga clic en **Agregar**.
10. En la **lista**de agentes , seleccione el agente al que quiere asociar la instancia.

    Si solo hay un agente configurado en la consola de NetScaler, ese agente se selecciona de forma predeterminada.
11. Haga clic en **Aceptar**.



Para acceder a la GUI de una instancia desde la consola de NetScaler

1. Vaya a **Infraestructura > InstanciasNetScaler**.
2. Seleccione el tipo de instancia a la que quiere 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.



Las direcciones IP de la instancia indican el tipo de implementación con las siguientes anotaciones:

- En el par de alta disponibilidad, **P**: servidor principal y **S**: servidor secundario.
- Clúster**C**
- **A**- Grupo Autoscale

Si una instancia no tiene ninguna anotación, indica la implementación independiente.

La GUI de la instancia seleccionada aparece en una ventana emergente.

Resolver advertencias de instancia

Aparece un signo de advertencia en la instancia por los siguientes motivos:

- **Error de inicio** de sesión: cuando agrega una instancia sin credenciales válidas, aparece en estado DOWN, con una advertencia de error de inicio de sesión. Especifique las credenciales correctas para administrar la instancia en NetScaler Console.

  Si la instancia no tiene licencia, aparece la opción **Licencia** al seleccionar la instancia. Haga clic en **Licencia** para aplicar la licencia a una instancia del grupo de licencias.
- **Instancia sin licencia con perfil**HTTPS : si una instancia sin licencia solo usa una conexión HTTPS, aplique la licencia a la instancia desde la GUI de NetScaler.

Configuración de syslog en instancias

July 17, 2024

El protocolo syslog proporciona un transporte que permite a las instancias de NetScaler enviar mensajes de notificación de eventos a NetScaler Console, que está configurada como recopilador o servidor syslog para estos mensajes.

Puede supervisar los eventos de syslog generados en las instancias de NetScaler si ha configurado el dispositivo para redirigir todos los mensajes de syslog a NetScaler Console. Para supervisar los eventos de syslog, primero debe configurar NetScaler Console como el servidor de syslog de la instancia de NetScaler. Una vez configurada la instancia, todos los mensajes de syslog se redirigen a NetScaler Console para que estos registros se puedan mostrar al usuario de forma estructurada.

Syslog utiliza el Protocolo de datagramas de usuario (UDP), puerto 514, para la comunicación y, dado que UDP es un protocolo sin conexión, no proporciona ningún acuse de recibo a las instancias. El tamaño del paquete syslog está limitado a 1024 bytes e incluye la siguiente información:

- Instalación
- Gravedad
- Nombre de host
- Timestamp
- Mensaje

En NetScaler Console, debe configurar los niveles de gravedad de las instalaciones y los registros de las instancias.

- **Facilidad** : los mensajes de Syslog se clasifican en términos generales en función de las fuentes que los generan. Estas fuentes pueden ser el sistema operativo, el proceso o una aplicación. Estas categorías se denominan instalaciones y se representan mediante números enteros. Por ejemplo, los mensajes del núcleo utilizan 0, los mensajes a nivel de usuario, el sistema de correo usa 1, el sistema de correo, etc. Las instalaciones de uso local (de local0 a local7) no están reservadas y están disponibles para uso general. Por lo tanto, los procesos y las aplicaciones que no tienen valores de instalación preasignados se pueden dirigir a cualquiera de las ocho instalaciones de uso local.
- **Gravedad** : la fuente o la instalación que genera el mensaje de syslog también especifica la gravedad del mensaje mediante un entero de un solo dígito, como se muestra a continuación:

```
1 - Emergency: System is unusable.

2 - Alert: Action must be taken immediately.

3 - Critical: Critical conditions.

4 - Error: Error conditions.

5 - Warning: Warning conditions.

6 - Notice: Normal but significant condition.

7 - Informational: Informational messages.

8 - Debug: Debug-level messages.
```


Para configurar syslog en instancias de NetScaler:

1. En NetScaler Console, vaya a **Infraestructura > Instancias**.
2. Seleccione la instancia de NetScaler desde la que desea recopilar los mensajes de syslog y mostrarlos en NetScaler Console.
3. En la lista desplegable **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 **OK**.

Esto configura todos los comandos de syslog de la instancia de NetScaler y NetScaler Console comienza a recibir los mensajes de syslog. Para ver los mensajes, vaya a **Infraestructura > Eventos > Mensajes de Syslog**.

Visión general de Logstream

March 6, 2024

Las instancias NetScaler generan registros de AppFlow y son un punto central de control para todo el tráfico de aplicaciones en el centro de datos. **IPFIX**y **Logstream** son los protocolos que transportan estos registros de AppFlow desde las instancias de NetScaler a NetScaler Console. Para obtener más información, consulte AppFlow.

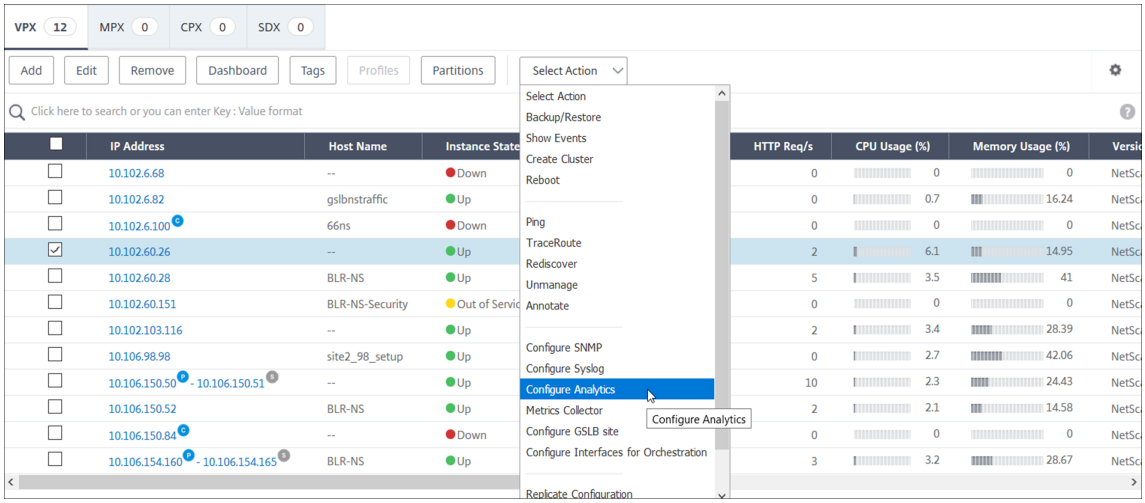
- **IPFIX** es un estándar abierto del Grupo de Trabajo de Ingeniería de Internet (IETF) definido en el RFC 5101. **IPFIX** utiliza el protocolo UDP que es un protocolo de transporte poco confiable utilizado para el flujo de datos en una dirección. Como IPFIX usa el protocolo UDP, la adhesión al estándar IPFIX implica procesar más recursos en NetScaler Console.
- **Logstream**es un protocolo propiedad de Citrix que se usa como uno de los modos de transporte para transferir de manera eficiente los datos de registro de análisis de las instancias de NetScaler a NetScaler Console. **Logstream** usa un protocolo TCP confiable y requiere menos recursos para procesar los datos.

Para NetScaler entre **la versión 11.1, compilación 47.14, y la versión 11.1, compilación 62.8**, **Logstream** es el modo de transporte predeterminado para habilitar Web Insight (HTTP) e IPFIX es el único modo de transporte para habilitar otros conocimientos. Para la versión NetScaler desde la **12.0 hasta la versión más reciente**, puede seleccionar **Logstream** o **IPFIX** como modo de transporte.

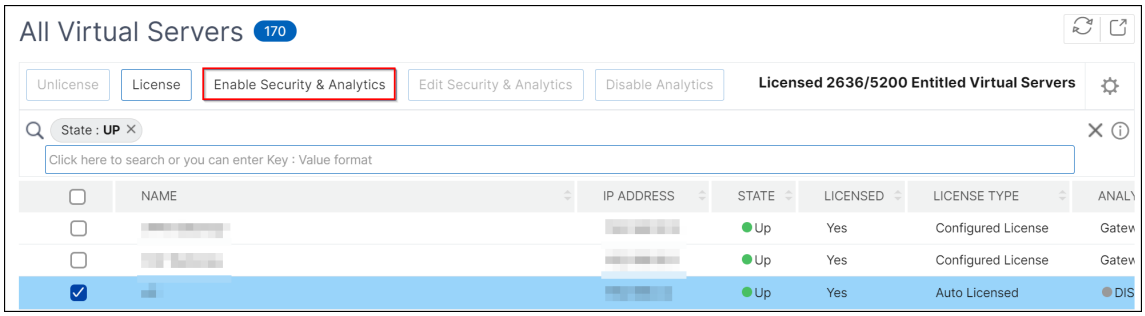
> **Nota**
>
> La versión y la compilación de NetScaler Console deben ser **iguales o superiores a** las de la versión y compilación de NetScaler. Por ejemplo, si ha instalado NetScaler 12.1 Build 50.28/50.31, asegúrese de haber instalado NetScaler Console 12.1 Build 50.39 o posterior.

Habilitar Logstream como modo de transporte

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 los servidores virtuales y, a continuación, haga clic en **Habilitar seguridad y análisis**.

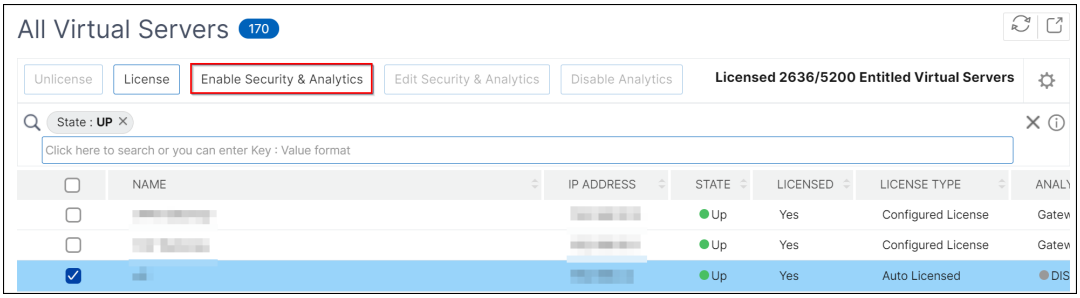


4. En la ventana **Habilitar seguridad y análisis** :
   a) Seleccione los tipos de información (violaciones de seguridad de Web Insight o WAF o infracciones de seguridad de bots)
   b) Seleccione **Logstream** como modo de transporte

> **Nota**
>
> Para NetScaler entre **la versión 11.1, compilación 47.14, y la versión 11.1, compilación 62.8**, **Logstream** es el modo de transporte predeterminado para habilitar Web Insight (HTTP) e IPFIX es el único modo de transporte para habilitar otros conocimientos. Para la versión NetScaler desde la **12.0 hasta la versión más reciente**, puede seleccionar **Logstream** o **IPFIX** como modo de transporte.

c) La expresión es verdadera por defecto

d) Haga clic en **Guardar análisis**



> **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.

En la siguiente tabla se describen las funciones de NetScaler Console que admiten **Logstream** como modo de transporte:

Función	**IPFIX**	**Flujo de registro**
Información web	•	•
Infracciones a la seguridad	No compatible	•
Infracciones de seguridad de WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
Insight SSL	No compatible	•
CR Insight	•	•
Reputación IP	•	•

Función	**IPFIX**	**Flujo de registro**
AppFirewall	•	•
Medición del lado del	•	•
Syslog/Auditlog	•	•

Cómo asignar más permisos a usuarios administradores delegados

January 26, 2024

Cuando el primer usuario de su organización se registre e inicie sesión en NetScaler Console, se le asignarán los privilegios de superadministrador. A cada usuario subsiguiente que inicie sesión se le asigna un rol de administrador delegado de forma predeterminada. Un administrador delegado no tiene permiso para ver y realizar ninguna tarea relacionada con la administración de usuarios o la configuración de RBAC.

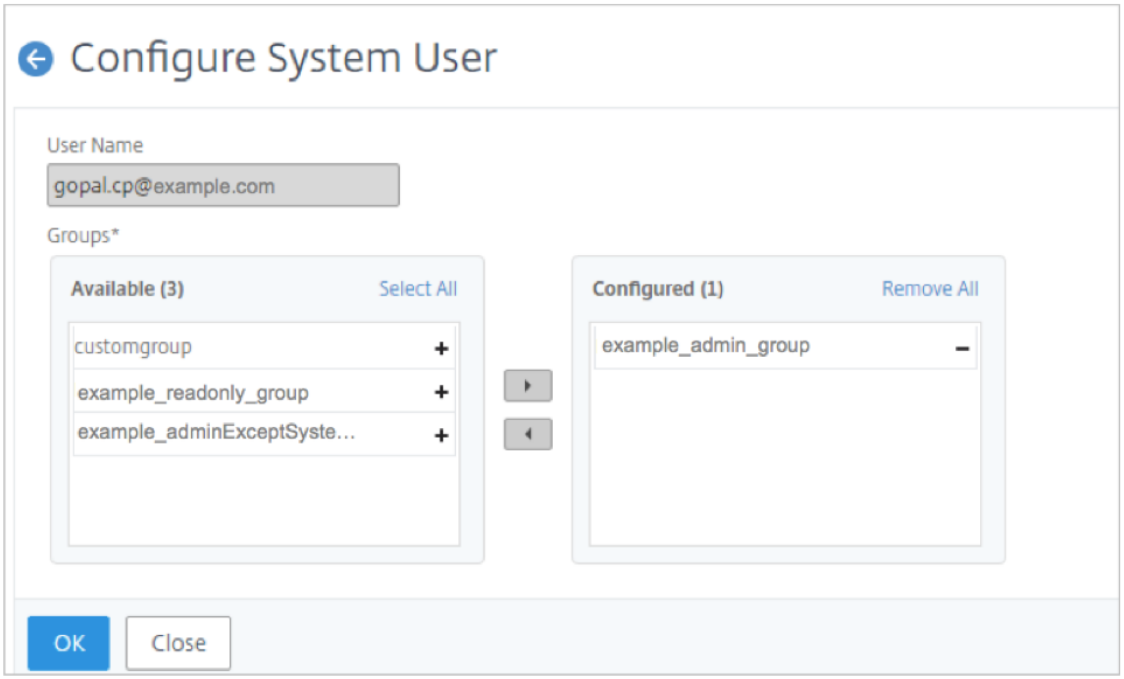
Sin embargo, puede asignar privilegios de superadministrador o roles específicos no superadministradores a un administrador delegado para que el administrador pueda realizar tareas relacionadas con la administración de usuarios.

Para obtener información detallada sobre el control de acceso basado en roles, consulte Configuración del control de acceso basado en roles.

Asignación de permisos de superadministrador a un administrador delegado

Para asignar permisos de superadministrador a un administrador delegado, este debe asignar el grupo de administradores predeterminado a un usuario administrador delegado. Realice las siguientes tareas:

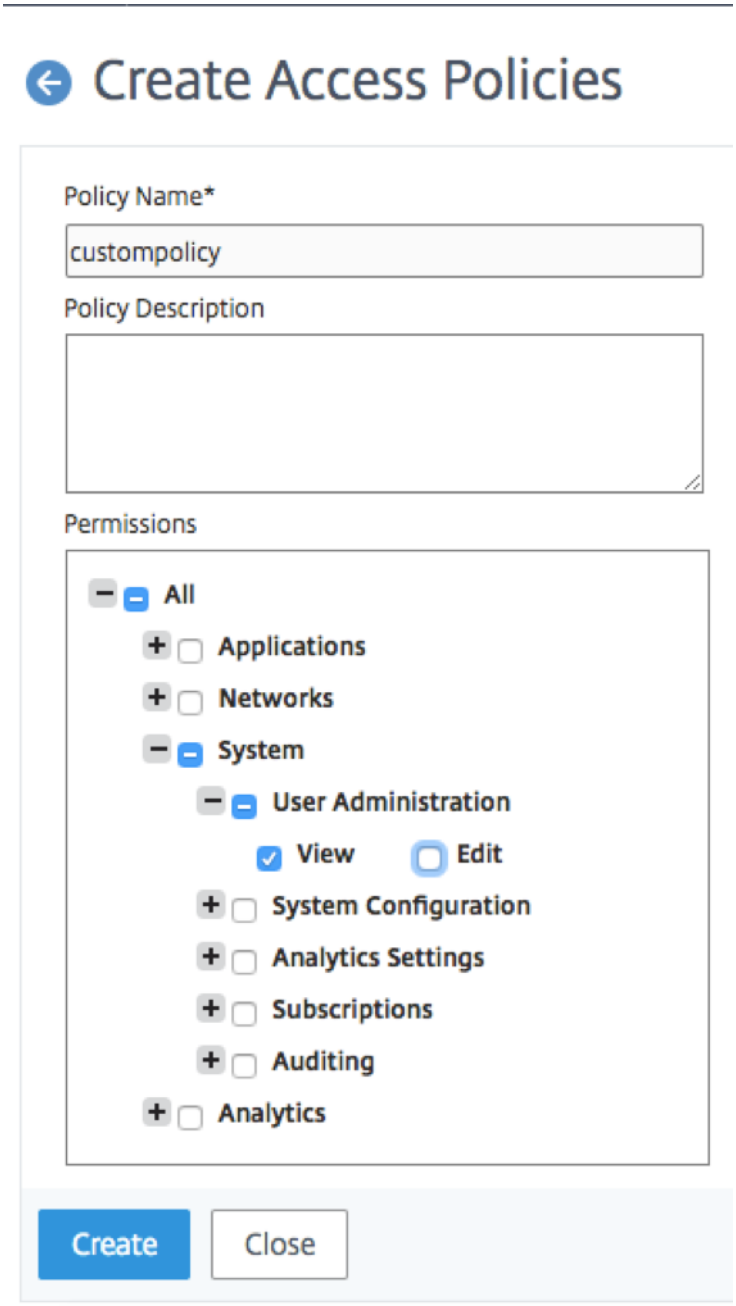
1. Inicie sesión en NetScaler Console como superadministrador.
2. Vaya a **Cuenta** > **Administración** de **usuarios > Usuarios**.
3. Seleccione el nombre de usuario del administrador delegado y haga clic en **Modificar**.
4. Asigne el grupo **<*arrendatario_name*>_admin_group** al administrador delegado y haga clic en **Aceptar**. Por ejemplo, en la siguiente imagen, “example_admin_group”se asigna a un usuario administrador delegado.



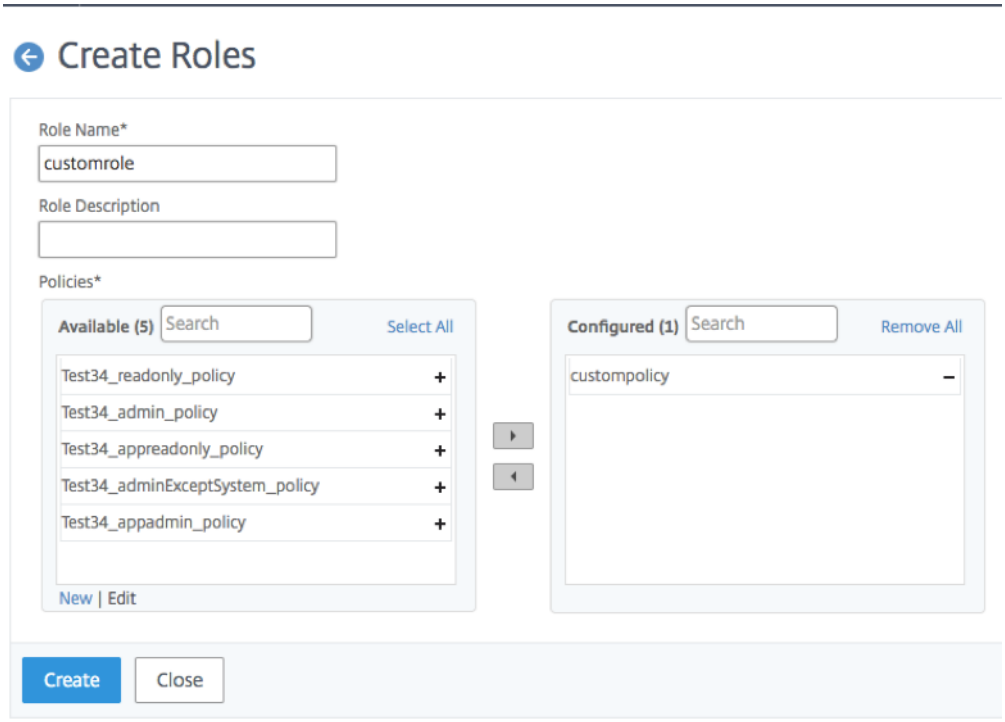
Asignación de rol personalizado a un administrador delegado

Para asignar cualquier rol personalizado a un administrador delegado, el superadministrador tiene que crear un grupo, rol y directiva y asignarlo al usuario administrador delegado. Esto garantiza que el administrador delegado solo tenga los permisos necesarios. Realice las siguientes tareas:

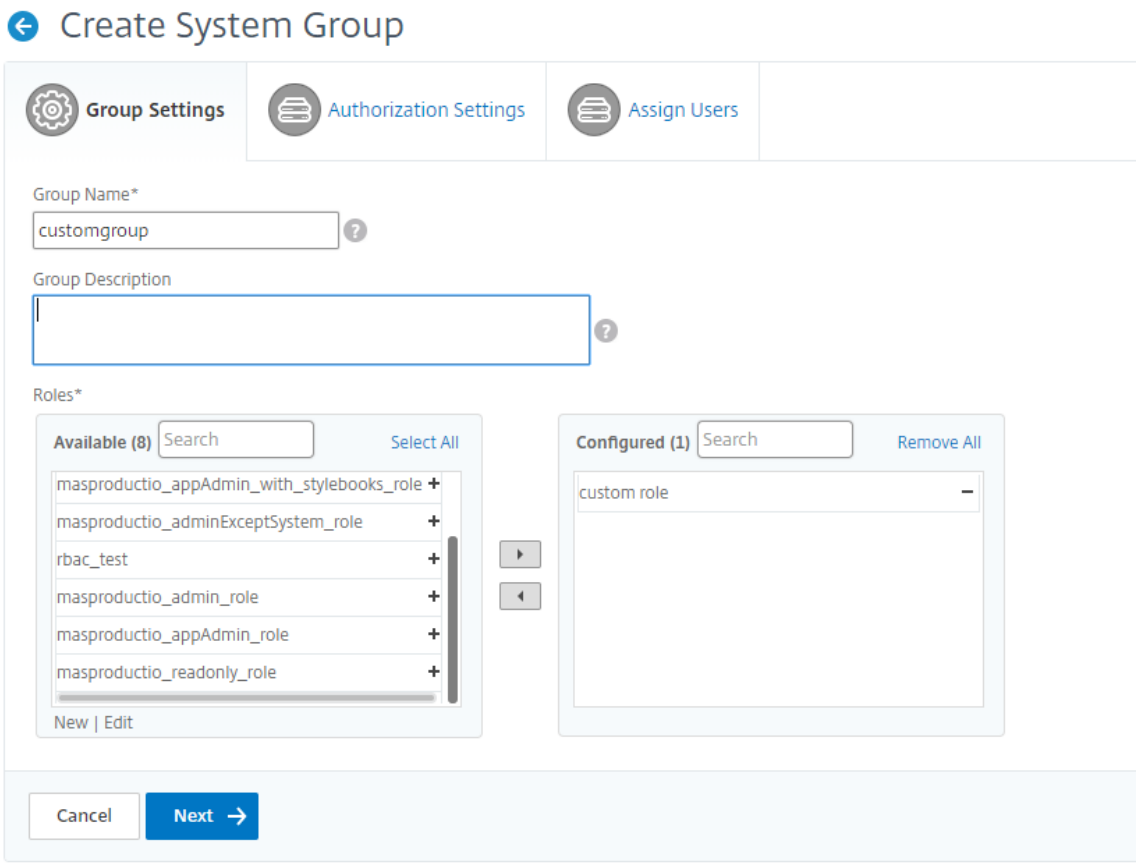
1. Inicie sesión en NetScaler Console como superadministrador.
2. Vaya a **Cuenta** > **Administración de usuarios** > **Directivas de acceso**. Seleccione **Agregar** para crear una directiva de acceso con los permisos necesarios para el administrador delegado. En este ejemplo, `custompolicy` se crea una directiva de acceso que permite el acceso de vista a la configuración de Administración de usuarios.



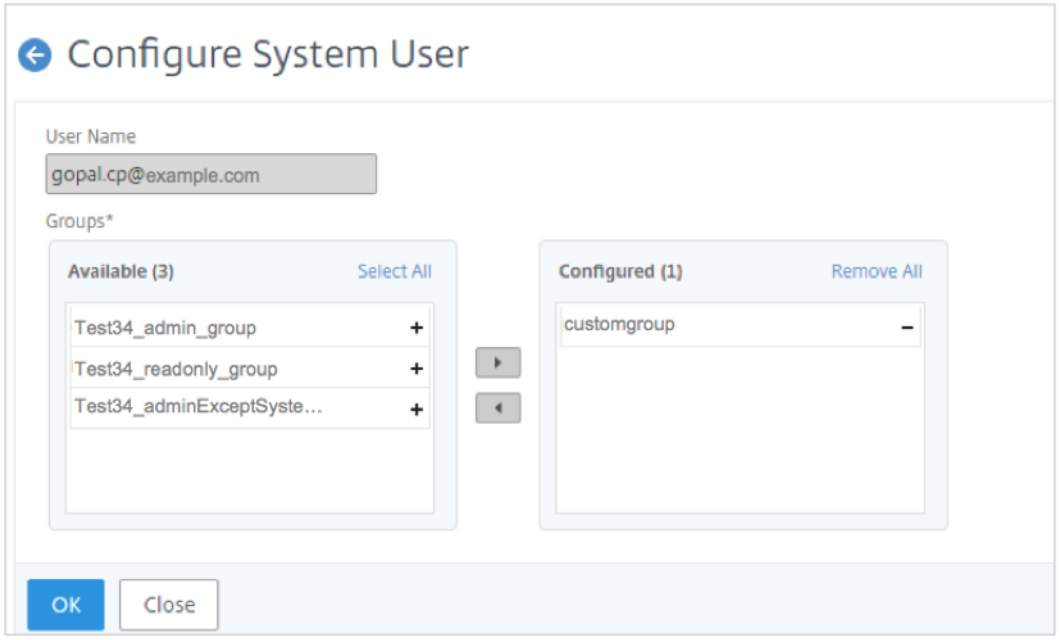
3. Acceda a **Cuenta** > **Administración de usuarios** > **Roles**. Seleccione **Agregar** para crear un rol y enlazar este rol a la directiva de acceso que creó en el paso anterior. En este ejemplo, `customrole` se crea un rol y se enlazado a la directiva de `custompolicy` acceso.



4. Vaya a **Cuenta** > **Administración de usuarios** > **Grupos**. Seleccione **Agregar** para crear un grupo y enlazar este grupo al rol que creó en el paso anterior. En este ejemplo, el grupo “grupo personalizado”se crea y enlazado al rol “rol personalizado”. “



5. Vaya a **Cuenta** > **Administración de usuarios** > **Usuarios**
6. Seleccione el nombre de usuario del administrador delegado y haga clic en **Modificar**.
7. Asigne el grupo que creó en el paso anterior al usuario administrador delegado. En este ejemplo, el usuario administrador delegado tiene asignado el grupo `customgroup`.



Integración con la instancia de ServiceNow

January 26, 2024

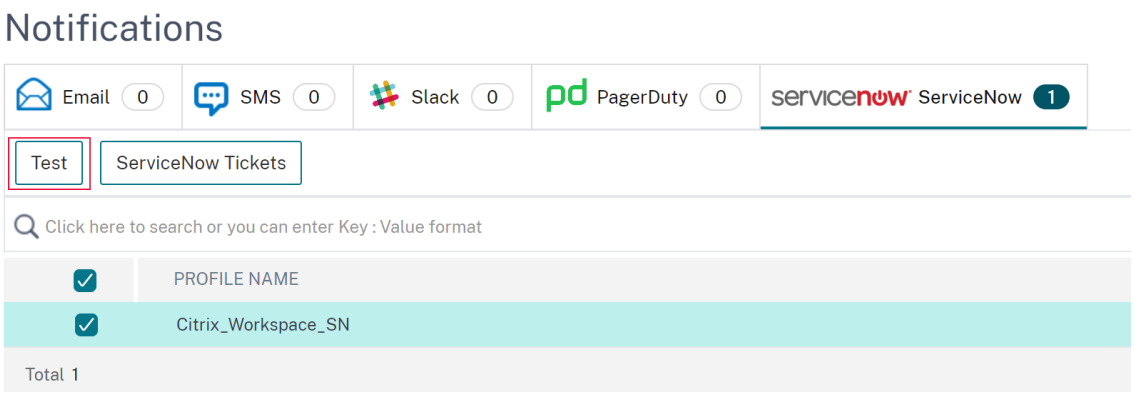
Como administrador de NetScaler, puede utilizar ServiceNow como el principal sistema de soporte y solicitudes de TI. Debe generar tickets o incidentes para que los eventos críticos de NetScaler los investiguen, rastreen y solucionen los problemas.

Puede automatizar la creación de tickets en ServiceNow mediante NetScaler Console y el conector Citrix ITSM para ServiceNow. Para iniciar esta automatización, incorpore el servicio de adaptadores ITSM de Citrix para recibir eventos y crear incidentes relevantes en ServiceNow. Para obtener más información sobre los pasos de preparación e integración, consulte Introducción al servicio de adaptadores ITSM de Citrix.

Tras la integración satisfactoria, configure la generación automática de incidentes de ServiceNow en NetScaler Console. Siga los pasos para verificar si los tickets de ServiceNow se generan automáticamente.

1. Inicie sesión en NetScaler Console.
2. Vaya a **Configuración > 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 desea ver los tickets de ServiceNow en la GUI de NetScaler Console, seleccione **ServiceNow Tickets**.



Al integrar NetScaler Console con ServiceNow, puede automatizar la generación de incidentes de ServiceNow para lo siguiente:

- Cualquier evento de NetScaler
- Certificados SSL que están a punto de caducar
- Eventos de caducidad de la licencia de NetScaler Console

Además, también puede personalizar las políticas de eventos de NetScaler Console.

Genere incidentes de ServiceNow para cualquier evento de NetScaler

En NetScaler Console, puede configurar reglas para generar automáticamente un ticket en ServiceNow para eventos específicos. NetScaler Console genera automáticamente un ticket de ServiceNow para eventos como:

- Los servidores virtuales se quedan fuera de servicio o están fuera de servicio.
- El consumo de recursos supera el valor umbral.
- La licencia caduca en una instancia de NetScaler.

El ticket generado automáticamente en ServiceNow tiene los detalles necesarios para rastrear y solucionar el problema. Puede administrar las notificaciones en uno o más dispositivos de red desde una única consola de ServiceNow. A continuación, asigne al administrador para un análisis más detallado.

Para crear una regla de eventos en la consola de NetScaler, vaya a **Infraestructura > Eventos > Reglas** . Para obtener más información, consulte Enviar notificaciones de ServiceNow.

Genere incidentes de ServiceNow para los certificados SSL que están a punto de caducar

Cuando un certificado SSL en las instancias de NetScaler está a punto de caducar, NetScaler Console genera automáticamente un ticket de ServiceNow. De esta forma, puede comprobar los próximos tickets de caducidad de los certificados SSL con antelación en su panel de ServiceNow.

Para enviar notificaciones de ServiceNow sobre la caducidad de un certificado SSL, consulte Vencimiento del certificado SSL.

Genere incidentes de ServiceNow para el vencimiento de la licencia de NetScaler Console

En NetScaler Console, puede configurar las reglas para generar automáticamente un ticket en ServiceNow para eventos específicos de caducidad de licencias de NetScaler Console.

Para enviar notificaciones de ServiceNow sobre la caducidad de la licencia de NetScaler Console, consulte Caducidad de la licencia de NetScaler Console.

Personalice las políticas de eventos de NetScaler Console

Puede definir políticas para controlar la forma en que ServiceNow procesa los eventos de NetScaler Console en función de los atributos de los eventos. Configure las políticas de eventos de NetScaler Console en el conector ITSM de Citrix. Puede decidir cómo se debe generar, procesar y reportar un incidente en ADM. A continuación, realice las siguientes acciones a través de ITSM:

- Ignorar incidentes
- Mostrar las incidencias en el panel
- Crear incidencias

Para obtener más información, consulte Personalizar las políticas de eventos de NetScaler Console.

Tareas y recomendaciones prácticas

June 7, 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.

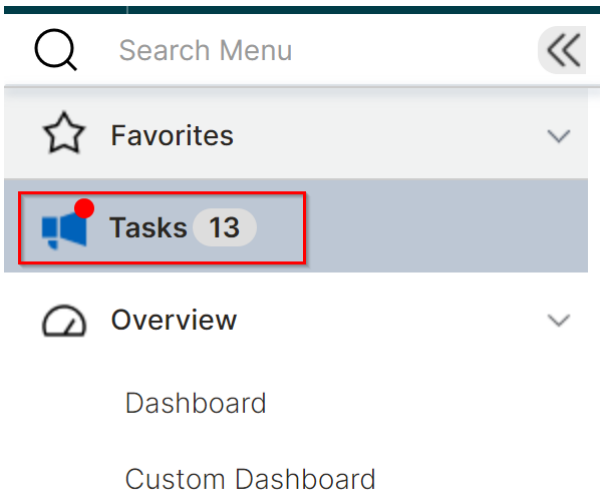
Es posible que haya descubierto cientos de instancias de NetScaler y que haya configurado varios servidores virtuales (aplicaciones) desde cada instancia. Como administrador, debe asegurarse de que todas las instancias de NetScaler y sus aplicaciones se administren de manera eficiente para obtener información 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 la consola NetScaler sea eficiente, segura y compatible. En función de su uso y suscripción actuales, la función **Tareas** de NetScaler Console le permite ver tanto las **tareas** procesables que debe tomar de inmediato como las **recomendaciones** para garantizar una implementación eficiente .

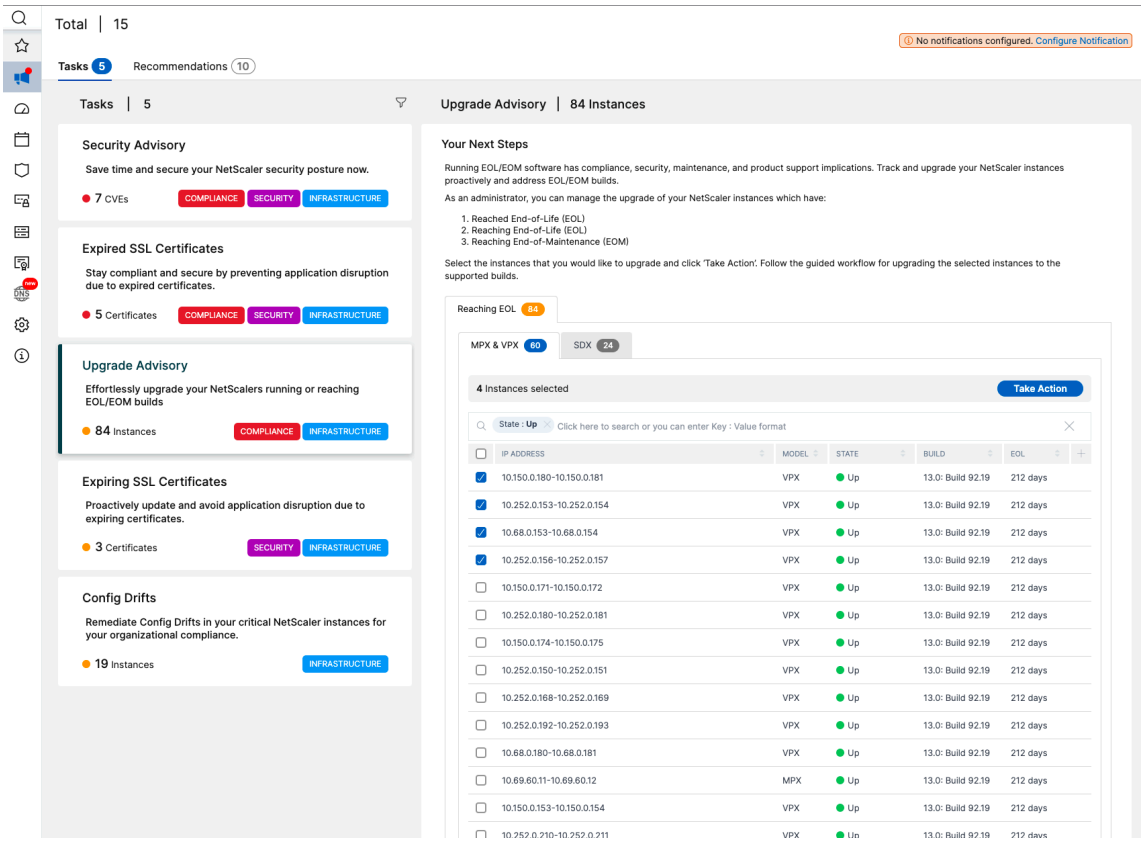
Como administrador, al hacer uso de estas **recomendaciones** y **tareas**prácticas, puede:

- Obtenga visibilidad instantánea de cualquier observación o problema que requiera su acción inmediata.
- Configure las notificaciones para recibir notificaciones cada vez que NetScaler Console detecte alguna tarea y tome medidas de forma proactiva.
- Logre una implementación eficiente de las instancias de NetScaler Console y NetScaler.
- Reduzca el tiempo y el esfuerzo cruciales para identificar los problemas críticos.
- Asegúrese de utilizar todas las capacidades de NetScaler Console, habilite el descubrimiento de productos y las funcionalidades recomendadas por el producto para una administración eficiente de la implementación.

En la GUI de NetScaler Console, haga clic en **Tareas** para ver tanto las **tareas** como las **recomendaciones**.

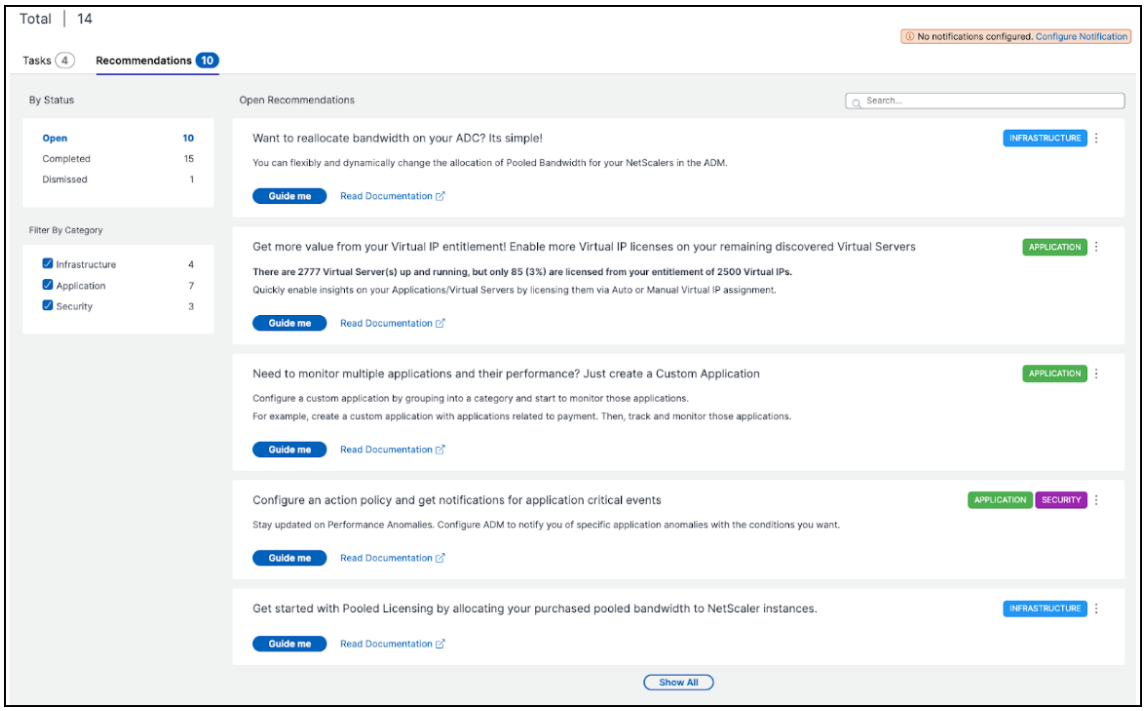


- **Tareas**: Le permite ver una lista de tareas que requieren su atención y acción inmediatas. A medida que amplíe su infraestructura, es posible que algunos problemas críticos pasen desapercibidos y provoquen brechas de seguridad. Por ejemplo, las instancias de NetScaler con CVE requieren atención 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 5 tareas. Las tareas se muestran en función de la gravedad (crítica y media).



- **Recomendaciones**: ofrece algunas recomendaciones basadas en su uso actual para mejorar la implementación de la consola NetScaler. 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 4 tareas siguientes en función de la implementación actual de NetScaler Console.

- **Certificados**SSL caducados : proporciona información sobre los certificados SSL caducados instalados en NetScaler Console. 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:

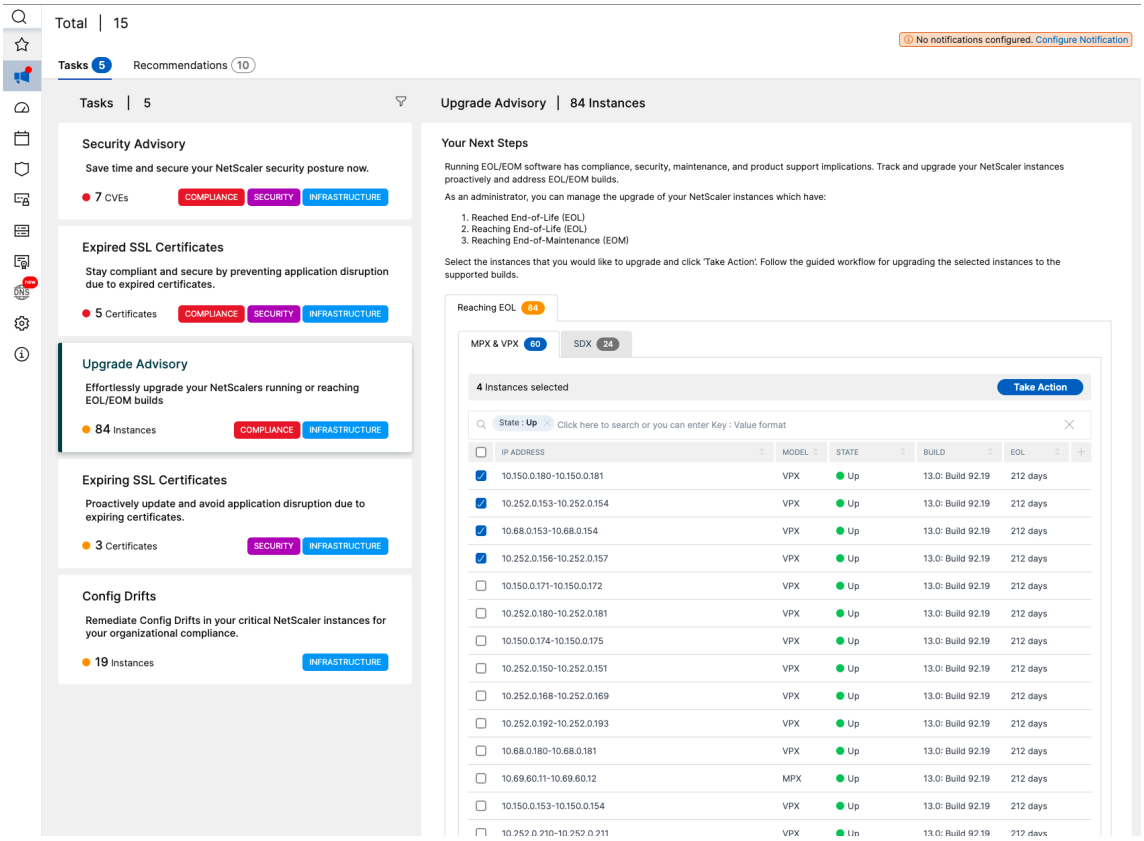
  - **CVE detectados**: muestra los CVE detectados y las instancias de NetScaler que afectan a los CVE. Para completar esta tarea, seleccione una CVE y haga clic en **Ver y corregir**.

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.**

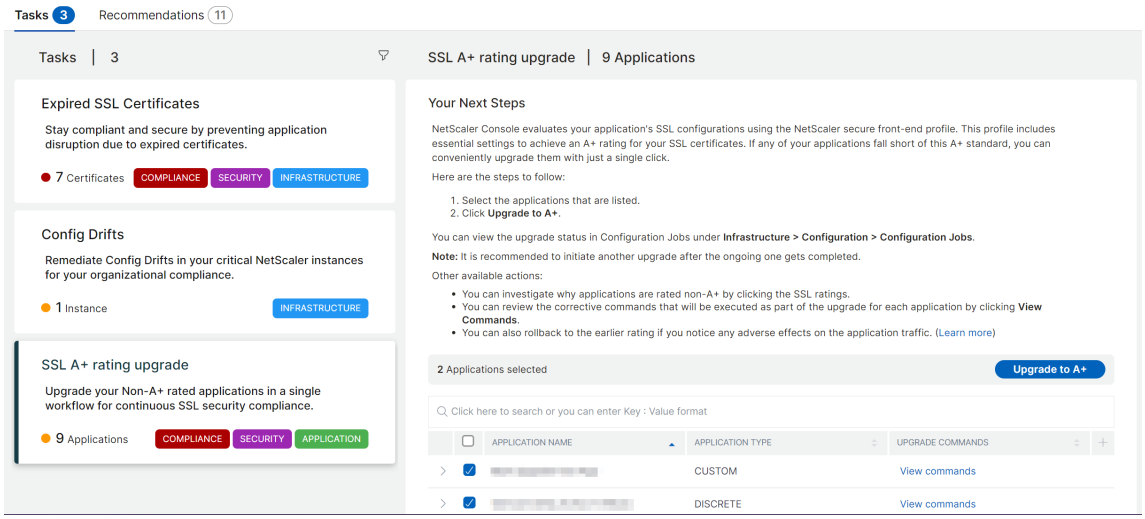
  Acción recomendada: se le redirigirá a la página de **consejos de seguridad** en **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**. Siga la documentación para completar la tarea.

- **Aviso**de actualización : proporciona información sobre las instancias de NetScaler que ya han alcanzado o están a punto de llegar al final del ciclo de vida (EOL) o al final del mantenimiento (EOM) en un plazo de 90 días.



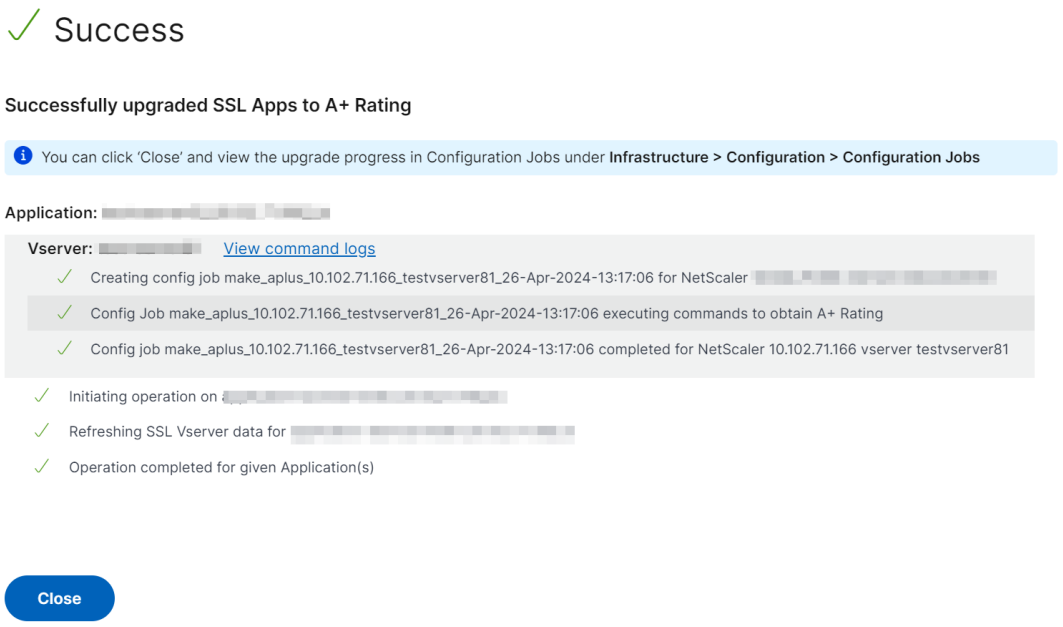
Acción recomendada: haga clic en **Tomar medidas** y actualice las instancias a una compilación recomendada.

- **Actualización de la clasificación SSL A+**: proporciona información sobre las aplicaciones que no cumplen con la calificación A+.



Acción recomendada: Seleccione las aplicaciones de la lista y haga clic en **Actualizar a A+**.

Cuando la actualización se haya realizado correctamente, puede ver el siguiente mensaje de éxito:



Una vez completada la actualización, los detalles de la aplicación se quitan de la tarea.

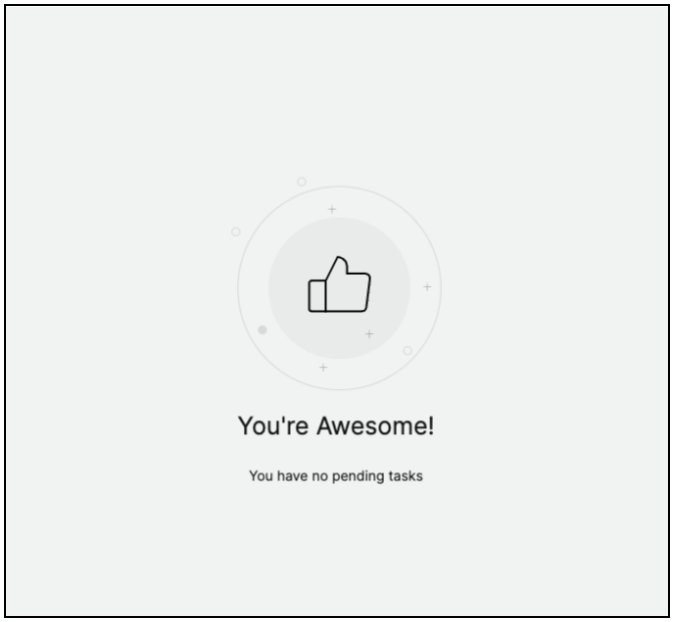
Puntos a tener en cuenta:

- Según la cantidad de aplicaciones seleccionadas, la duración del proceso de finalización de la actualización puede variar.
- Tras iniciar un proceso de actualización, se recomienda iniciar otro proceso de actualización una vez que se haya completado el proceso en curso.

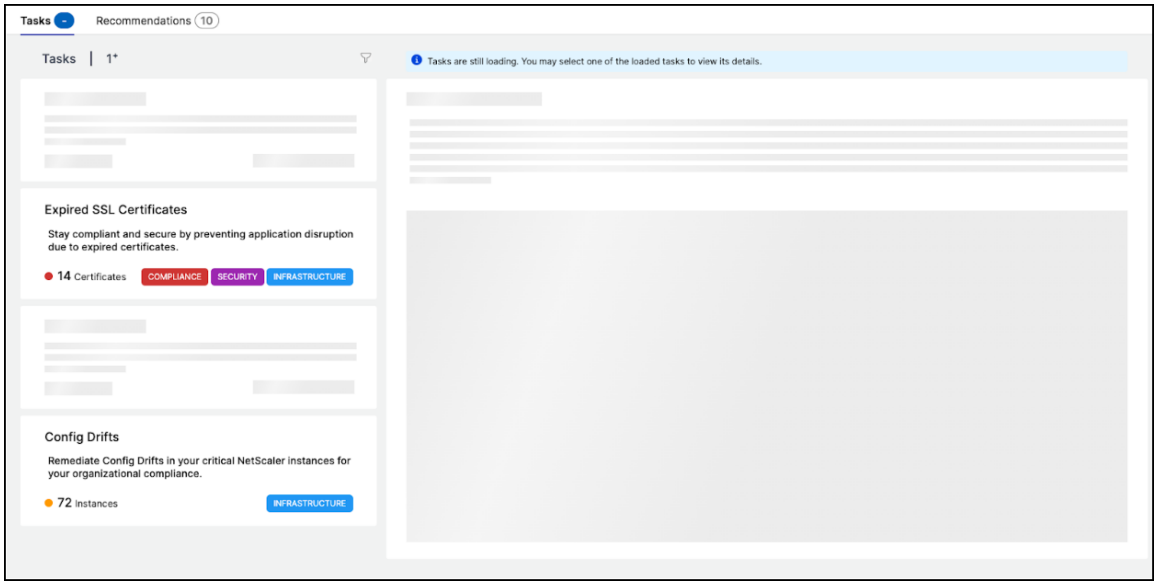
- También puede ver el estado del proceso de actualización en **Infraestructura > Configuración > Trabajos de configuración**.
- Si el proceso de actualización no se realiza correctamente, puede ver el estado en **Infraestructura > Configuración > Trabajos de configuración**. Puede volver a iniciar el proceso de actualización desde la tarea.
- Si realiza una actualización masiva y una o más aplicaciones no se actualizan, podrá ver solo los detalles de las aplicaciones fallidas en la tarea. Puede volver a iniciar el proceso de actualización para completarlo.

Nota:

- Puede ver la página siguiente si la consola NetScaler 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 Console:

> **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 una instancia de NetScaler	Después de la incorporación a NetScaler Console y si no se descubre ninguna instancia de NetScaler.
Agregue un agente externo para aprovechar al máximo las funciones de NetScaler Console	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.

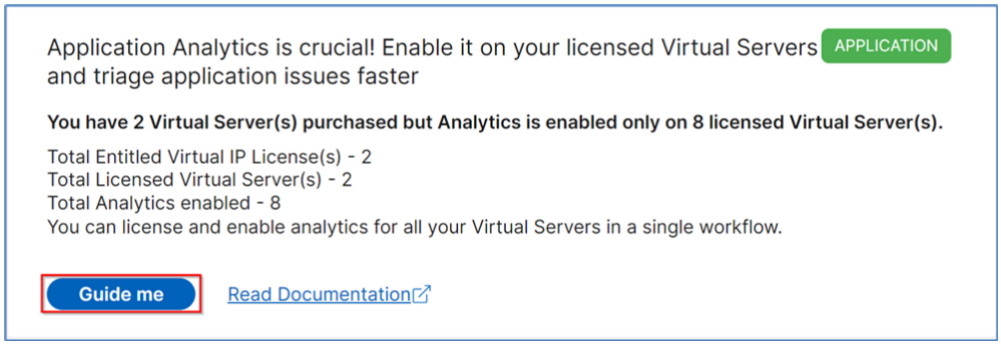
Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
Registrar un NetScaler desde un agente integrado a un agente externo	Tras la incorporación a NetScaler Console mediante el flujo de trabajo de Service Connect, las instancias de NetScaler se incorporan mediante el agente integrado. Puede registrar esas instancias de NetScaler en un agente externo para usar todas las funciones, como el análisis, las licencias agrupadas, etc.
¡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 el ancho de banda de su NetScaler? ¡Es sencillo!	Si las licencias agrupadas se asignan en la GUI de NetScaler y esas instancias de NetScaler se descubren en NetScaler Console, puede realizar la reasignación mediante NetScaler Console.
¡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 Console.
Configure las reglas y no se pierda ningún evento crítico en sus instancias de NetScaler	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 instancias de NetScaler actualizadas con CVE y mitigaciones	Si las instancias de NetScaler tienen algún impacto en el CVE.

Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
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 varias instancias de NetScaler	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.
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 Console 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 Console aún no está configurada.
Automatice la administración de certificados SSL con Venafi y ADM	Si el servidor Venafi aún no está configurado en NetScaler Console.
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.

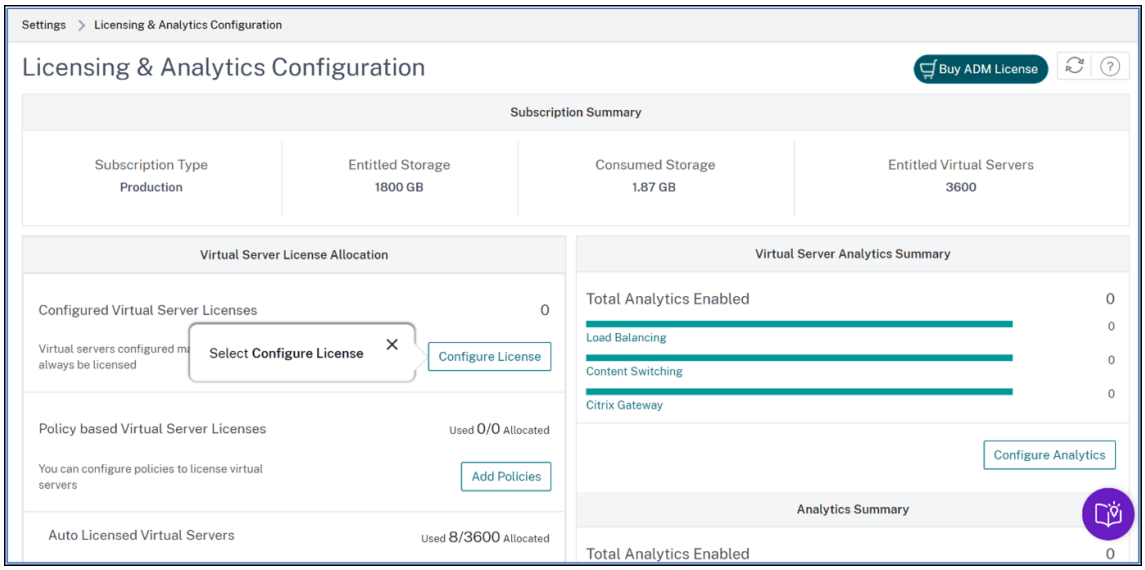
Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
Considere la posibilidad de adquirir más capacidad de ancho de banda agrupada. Su permiso de ancho de banda agrupado actual está infrautilizado. Revisa y considera la posibilidad de asignar más	Si ha utilizado el 90% o más de sus derechos de ancho de banda agrupados. Si el uso de la asignación de licencias agrupadas es inferior al 70%.

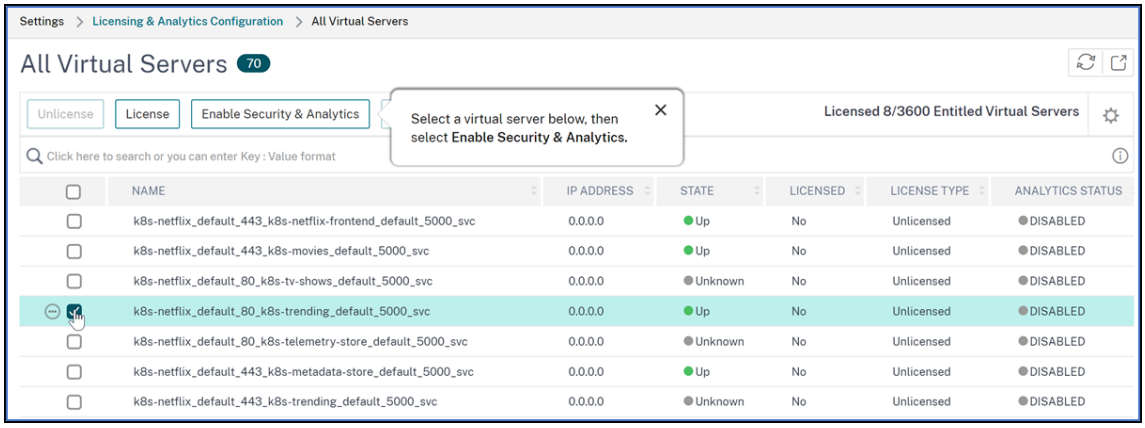
¿Cómo utilizar el flujo de trabajo de Guide me y completar la recomendación?

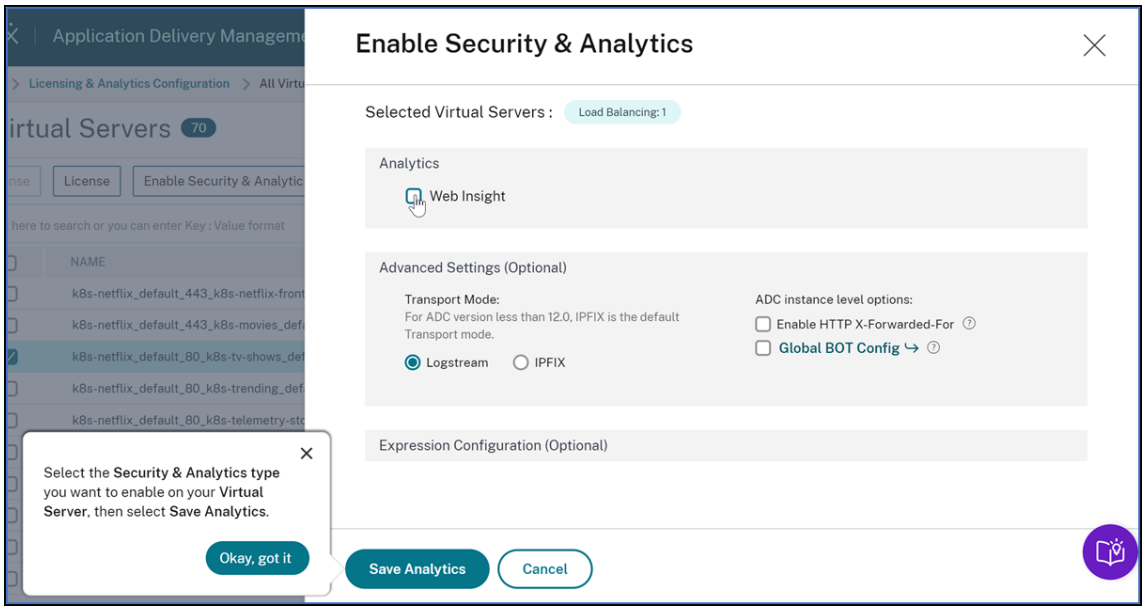
Tenga en cuenta que quiere habilitar el análisis para todos los servidores virtuales. Haga clic en **Guiarme** para realizar la siguiente tarea:



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:

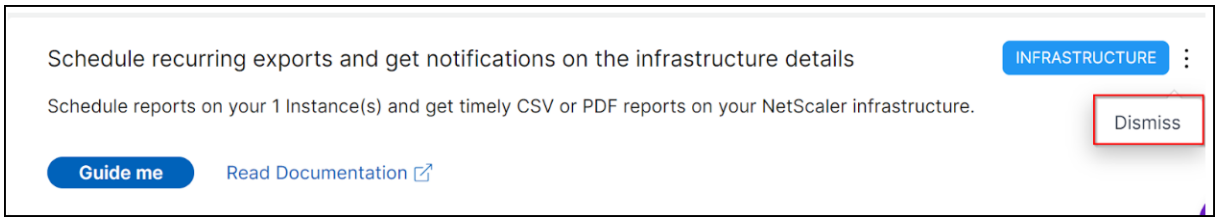
1. 

2. 

3. 

Tras seleccionar el tipo de análisis y hacer clic en **Guardar análisis**, la recomendación estará completa y pasará a Completado.

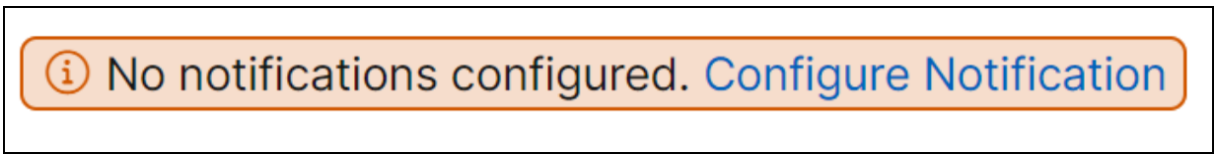
Del mismo modo, si quiere completar alguna recomendación más adelante, puede seleccionar **Descartar** en la lista y se moverá a **Descartada**.



Configurar notificaciones

Puede configurar y recibir notificaciones siempre que NetScaler Console identifique cualquier tarea abierta que requiera una 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 Console muestra la lista o el perfil de distribución configurados. NetScaler Console envía notificaciones a la lista de distribución o perfil seleccionados.

Preguntas frecuentes

1. ¿**Guide me** no muestra la descripción de herramientas y solo muestra la redirección de la interfaz de usuario? ¿Qué debo hacer para solucionar este problema?

   Este problema puede ocurrir si el firewall bloquea el FQDN de Pendo. Consulte Habilitar Pendo para su empresa y asegúrese de que el FQDN esté permitido en el firewall. Al habilitar el FQDN de Pendo, **la Guía** puede mostrar sugerencias sobre herramientas. Puede disfrutar al máximo del flujo de trabajo de **Guide me** solo cuando Pendo esté disponible.

2. ¿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 tener conocimientos previos ni saber si la función existe en NetScaler Console o no.

3. ¿Qué ocurre si rechazo alguna recomendación?

   Las recomendaciones que desestime se trasladan a **Rechazadas**. Puede completar estas recomendaciones más adelante.

4. ¿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.

5. ¿Puedo realizar búsquedas o filtros?

   ¡Sí! Puede utilizar la barra de búsqueda o limitarse a tareas específicas seleccionando la categoría de la lista.

6. ¿Recibiré tareas para realizar acciones en eventos dinámicos?

   ¡Sí! Actualmente puede ver un total de 4 tareas procesables. Para obtener más información, consulte Tareas.

7. ¿Aparecerán todas las tareas procesables y las más de 20 recomendaciones aunque no haya agregado instancias de NetScaler a NetScaler Console?

   No. Debe tener la instancia de NetScaler y los servidores virtuales disponibles en NetScaler Console para mostrar todas las tareas y recomendaciones.

8. ¿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 26, 2024

En NetScaler Console, puede ver varios datos sobre el uso y el rendimiento de las aplicaciones, la infraestructura de NetScaler, las infracciones de seguridad (Bot y WAF), etc. Como administrador, es posible que tenga que navegar hasta varias opciones de la GUI de NetScaler Console para ver varios datos. Por ejemplo, para comprobar la información sobre los servidores virtuales (aplicaciones) y las instancias de NetScaler:

- 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 NetScaler.

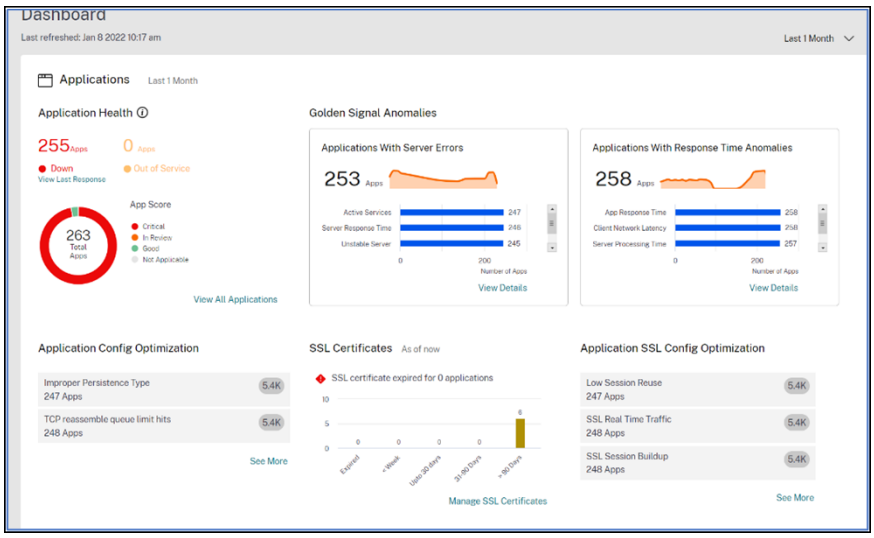
Para una mejor experiencia de supervisión, es necesario que tenga un privilegio que contenga una descripción general de todos los datos requeridos. Vaya a **Descripción general > Panel de control** para visualizar un panel de control de un solo panel con una descripción general de los detalles de las métricas clave en función de las siguientes categorías:

- Aplicaciones
- Infraestructura de NetScaler
- Seguridad de las aplicaciones
- Gateway
- Análisis de API

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 de NetScaler

En **NetScaler Infrastructure**, puede ver las siguientes métricas clave relacionadas con las instancias de NetScaler:

- **Estado**de las instancias de NetScaler: proporciona una descripción general del total de instancias de NetScaler en función de la puntuación de las instancias.
- **Instancias de NetScaler afectadas por las**CVE: proporciona una descripción general del total

de instancias de NetScaler que se ven afectadas por vulnerabilidades y exposiciones comunes (CVE). Para obtener más información, consulte Aviso de seguridad.

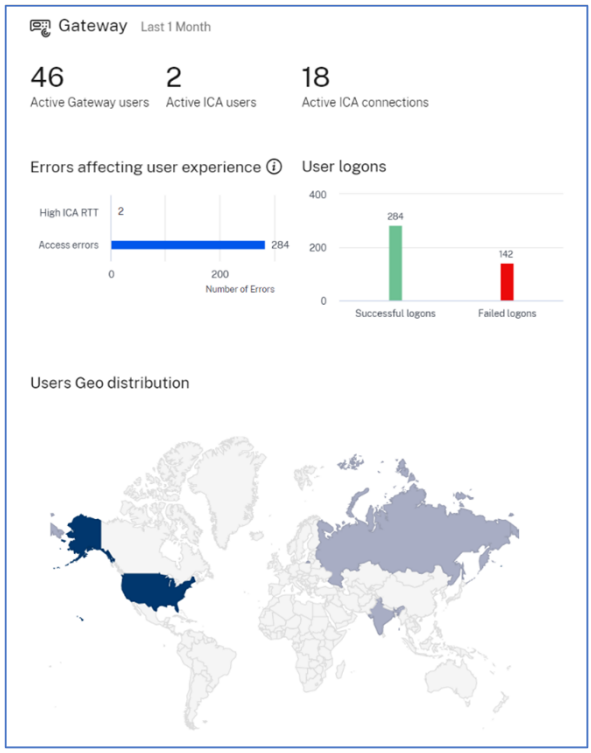
- **Problemas**con las instancias de NetScaler : proporciona una descripción general de los problemas de las instancias de NetScaler en función de la categoría del problema. Para obtener más información, consulte Análisis de infraestructura.
- **Resumen**de la actualización de instancias de NetScaler : proporciona una descripción general del total de instancias de NetScaler que no están en la versión más reciente. Haga clic en **Ver panel de instancias de NetScaler** 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

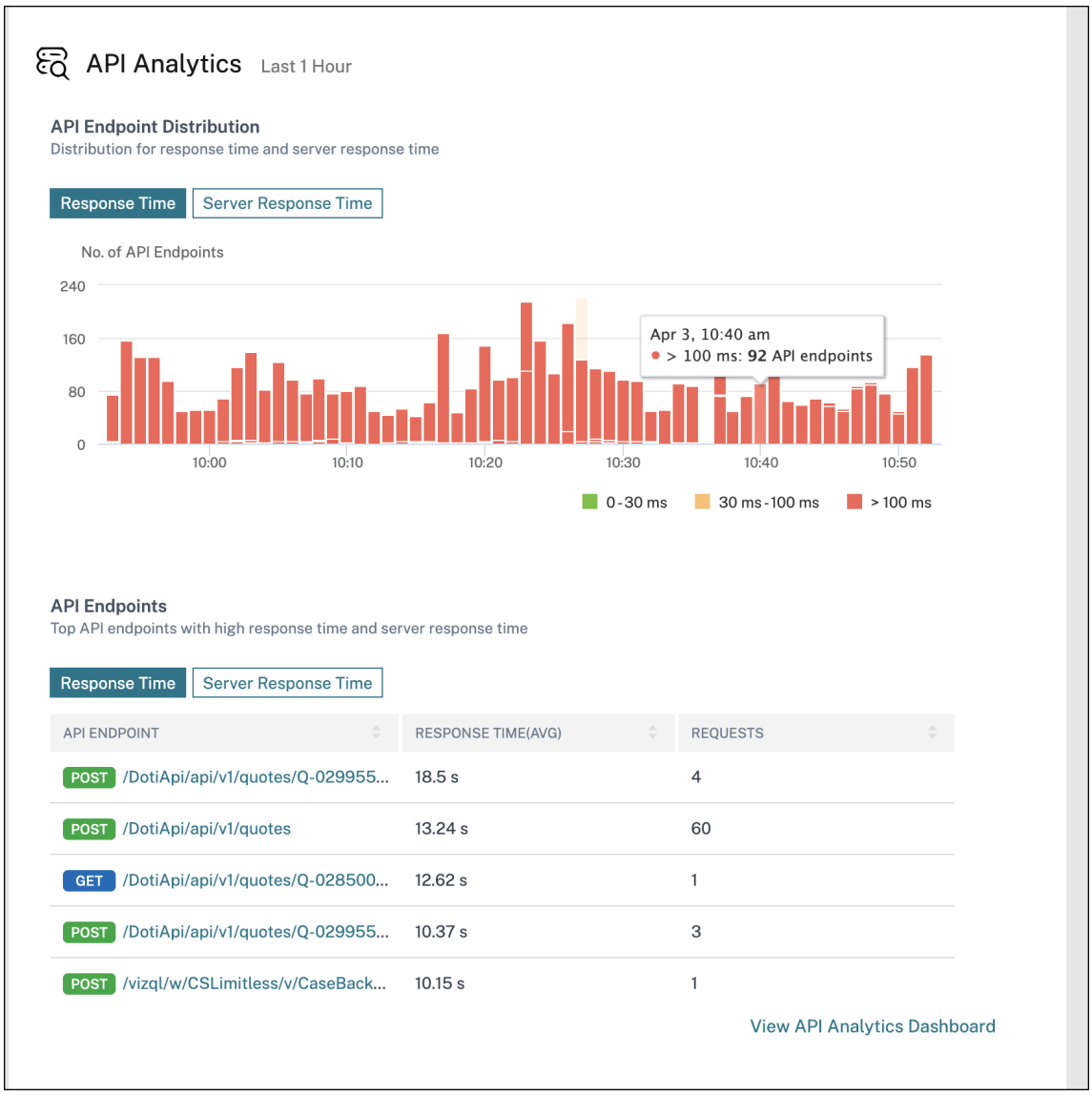
Proporciona una descripción general del total de usuarios de gateway activos, el total de usuarios de ICA activos y el total de conexiones ICA activas. También puede ver los errores, los detalles de inicio de sesión de los usuarios y un mapa geográfico que proporciona detalles sobre las ubicaciones de los usuarios.



Análisis de API

Proporciona una descripción general del rendimiento y el uso de los puntos finales de la API configurados mediante NetScaler Console. Puede ver:

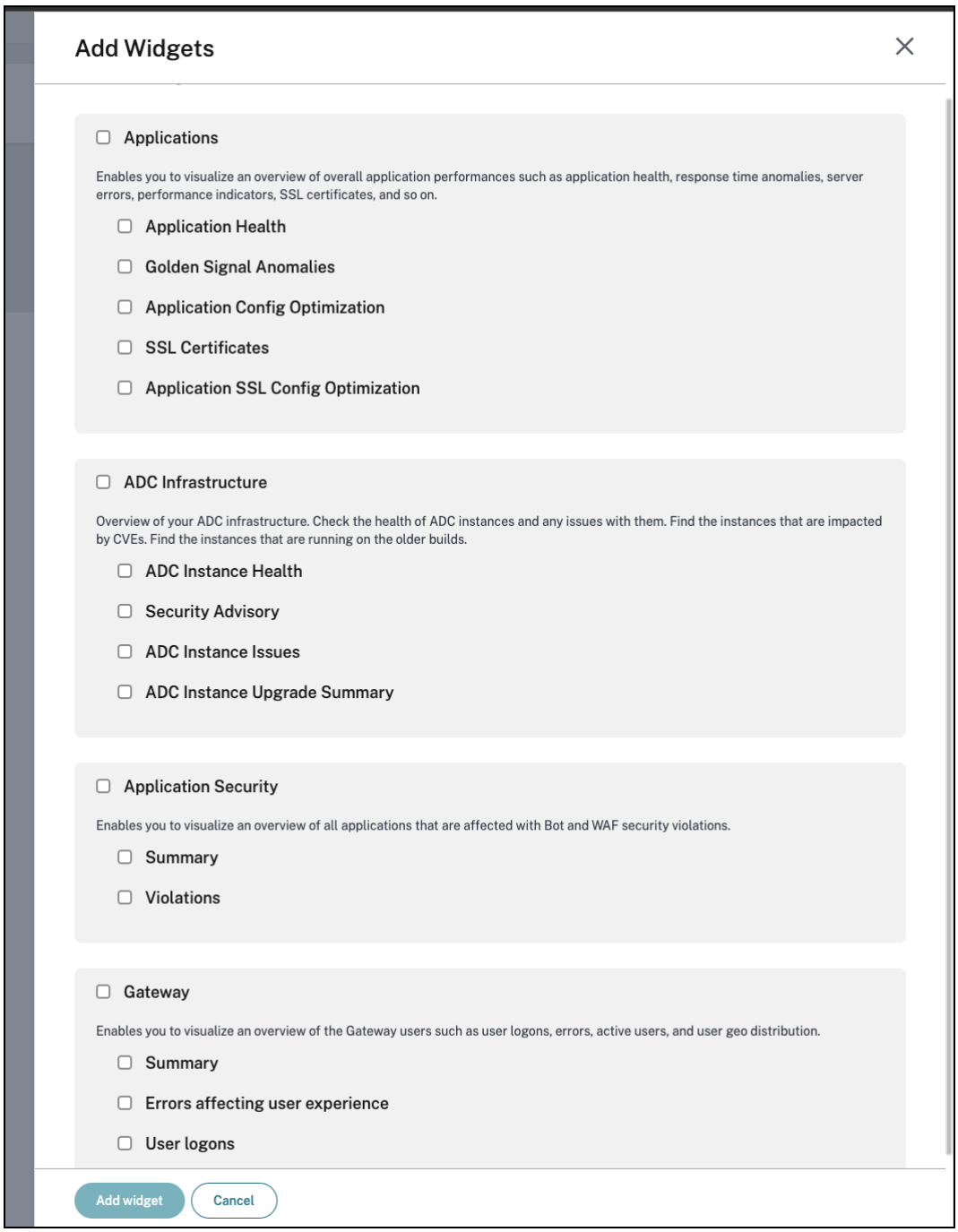
- Distribución del tiempo de respuesta de las aplicaciones y los servidores para los puntos finales de la API.
- Terminales con un alto tiempo de respuesta de aplicaciones y servidores.



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 de NetScaler, 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**.

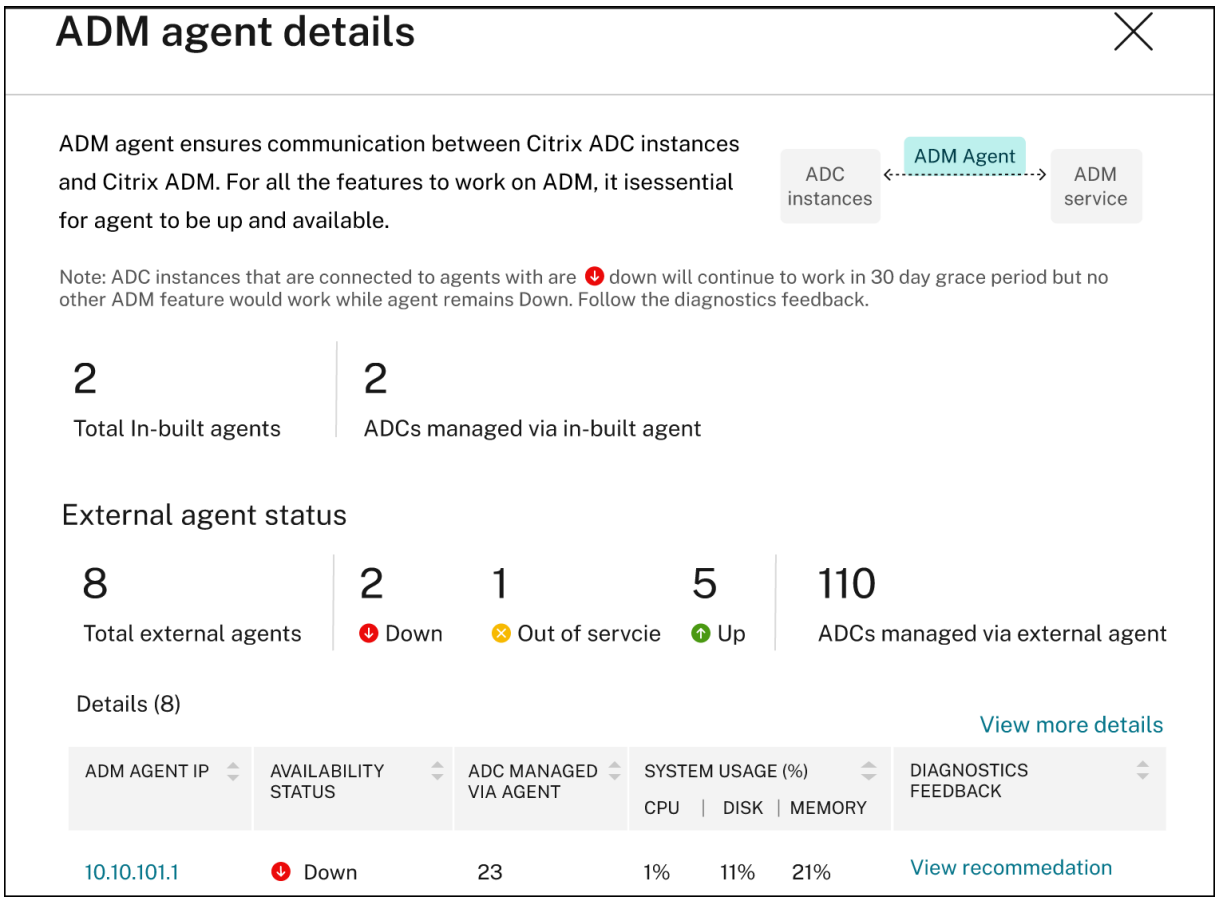
> **Nota**
>
> - De forma predeterminada, se muestran todos los widgets. Si personaliza el panel, guarde los cambios y utilice de nuevo la opción **Restablecer los valores predeterminados**, todos los widgets se agregarán al panel.
> - La opción **Restablecer la última vez guardada** carga la configuración guardada anteriormente.

Ver detalles del agente

En el panel unificado, puede visualizar una descripción general de los detalles de los agentes. En **Descripción general > Panel** de control , junto al estado del **agente** , 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 de los agentes, como el total de agentes incorporados, el total de agentes externos, la IP del agente, el estado, el uso del sistema, las comprobaciones de diagnóstico, etc.



Crear y aplicar filtros

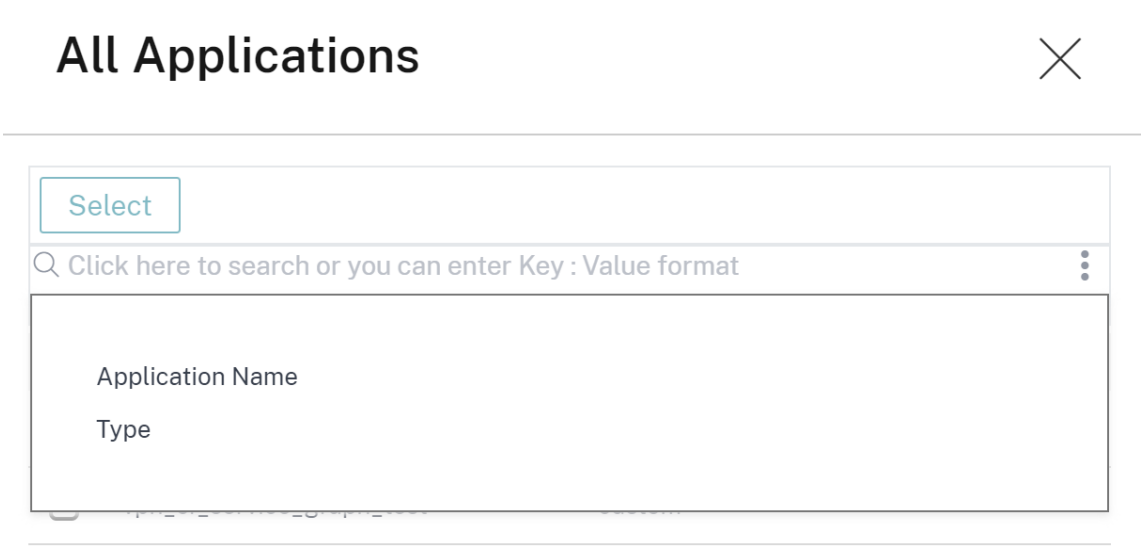
Puede aplicar filtros y ver la información solo para las instancias o aplicaciones seleccionadas de la siguiente manera:

- Aplicaciones
- Infraestructura de NetScaler
- Seguridad de las aplicaciones

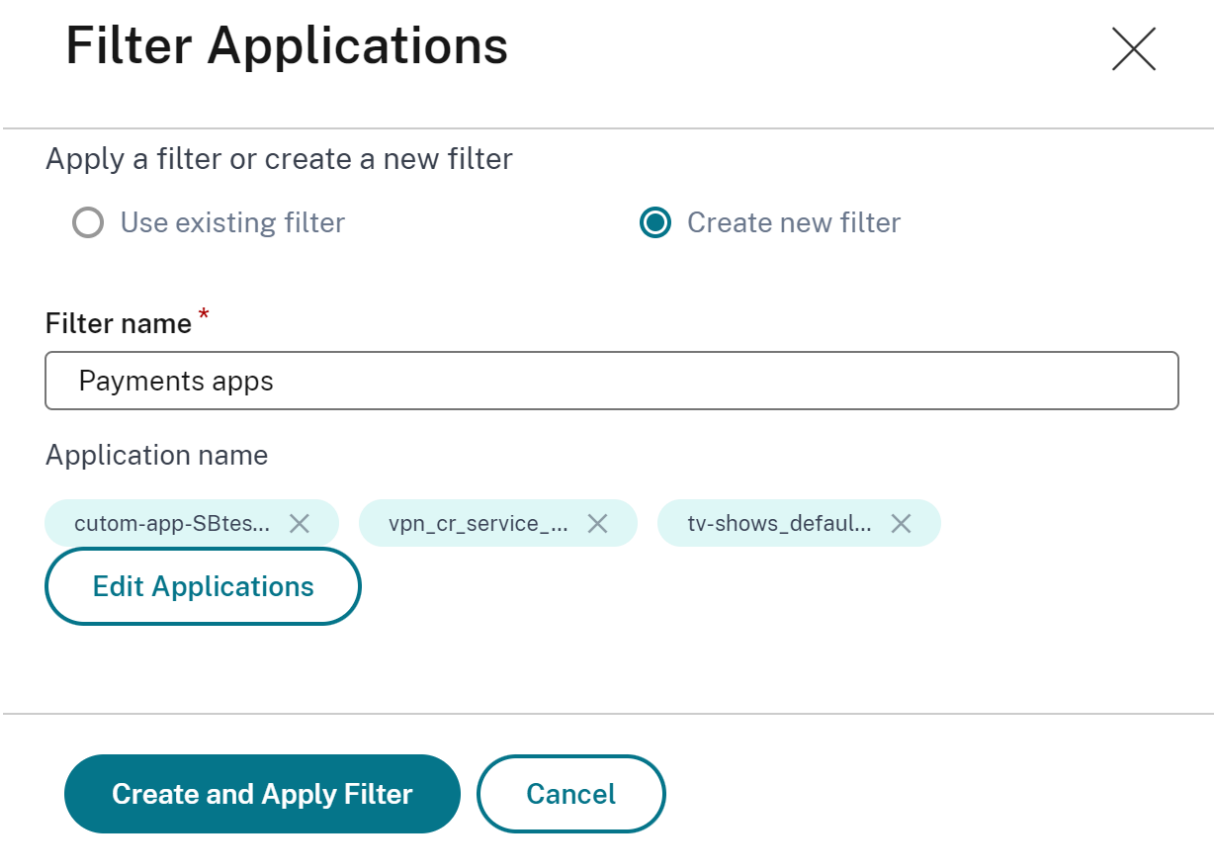
De forma predeterminada, se seleccionan todas las aplicaciones. Puede crear un archivador personalizado desde el panel de control haciendo clic en el icono de filtros disponible en el mosaico.

En la ventana **Filtrar aplicaciones**:

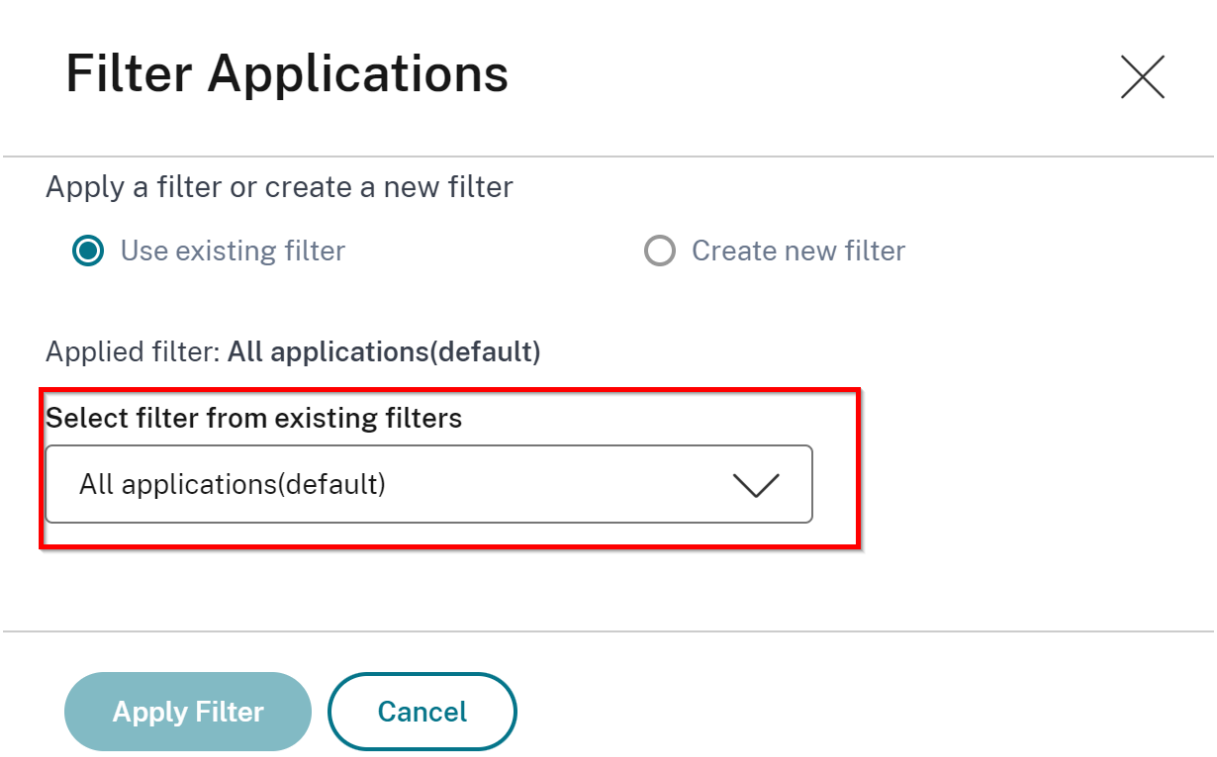
1. Seleccione **Crear filtro nuevo**.
2. Proporcione un nombre de filtro según su elección.
3. Haga clic en **Seleccionar aplicaciones** y agregue todas las aplicaciones necesarias para el filtro. Al seleccionar aplicaciones, también puede utilizar los filtros (**nombre** y **tipo de aplicación**) y, a continuación, seleccionar las aplicaciones.



4. Haga clic en **Crear y aplicar filtro**.

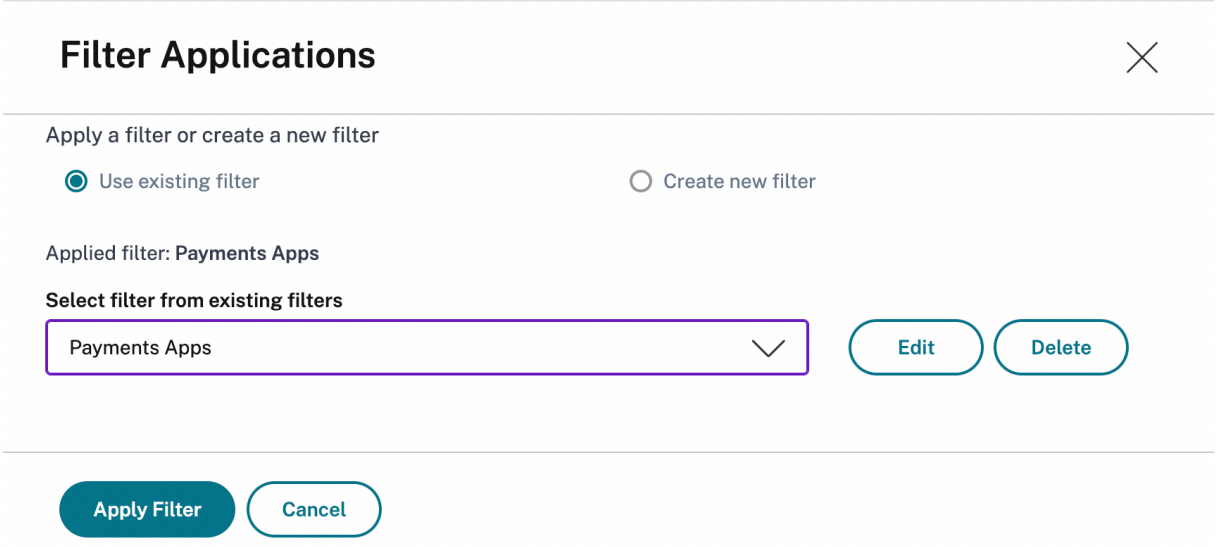


El filtro ya está creado y aplicado. Puede crear más filtros siguiendo el mismo procedimiento. Después de crear filtros, puede seleccionar y aplicar filtros a través de la lista **Seleccionar un filtro de entre los filtros existentes**.



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.

Crea paneles personalizados para ver los detalles de las métricas clave de la instancia

January 26, 2024

Al igual que en el panel unificado (**Descripción general > Panel de control**), puedes ver los detalles de las métricas de la instancia en función de tu elección mediante la creación de paneles personalizados. Puede crear hasta 20 paneles con un nombre único para cada panel. Como administrador, esta mejora le permite crear varios paneles y supervisar solo la información necesaria sobre las instancias.

Para empezar, tenga en cuenta que desea supervisar las métricas clave de las **aplicaciones** y la **seguridad de las aplicaciones**:

1. Navega hasta **Descripción general > Panel de control personalizado**.
2. Haga clic en **+** para crear un panel nuevo.

   En la página **Crear panel personalizado** :

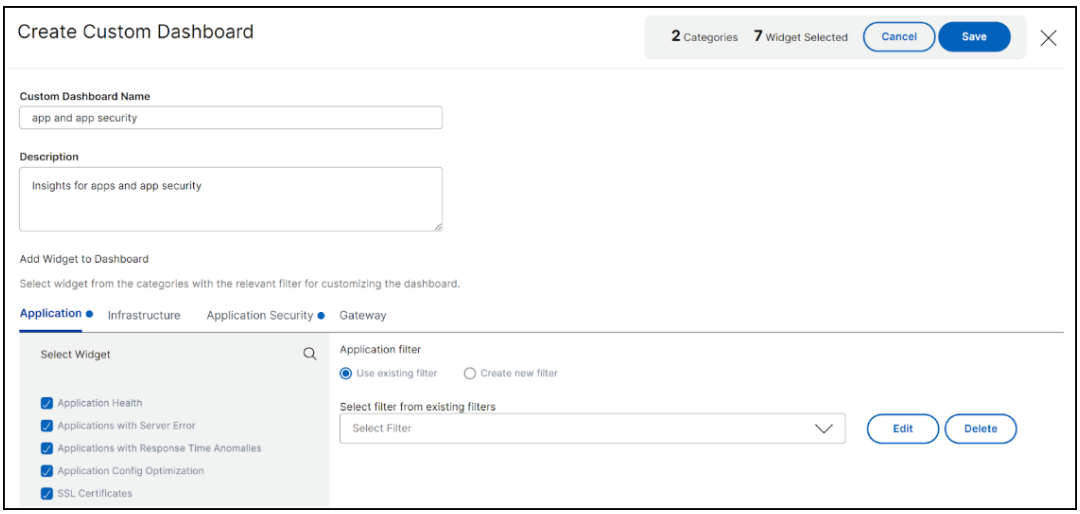
   a) **Nombre de panel personalizado**: Especifique un nombre único para el panel.

   b) **Descripción**: Proporcione una descripción breve para obtener detalles adicionales.

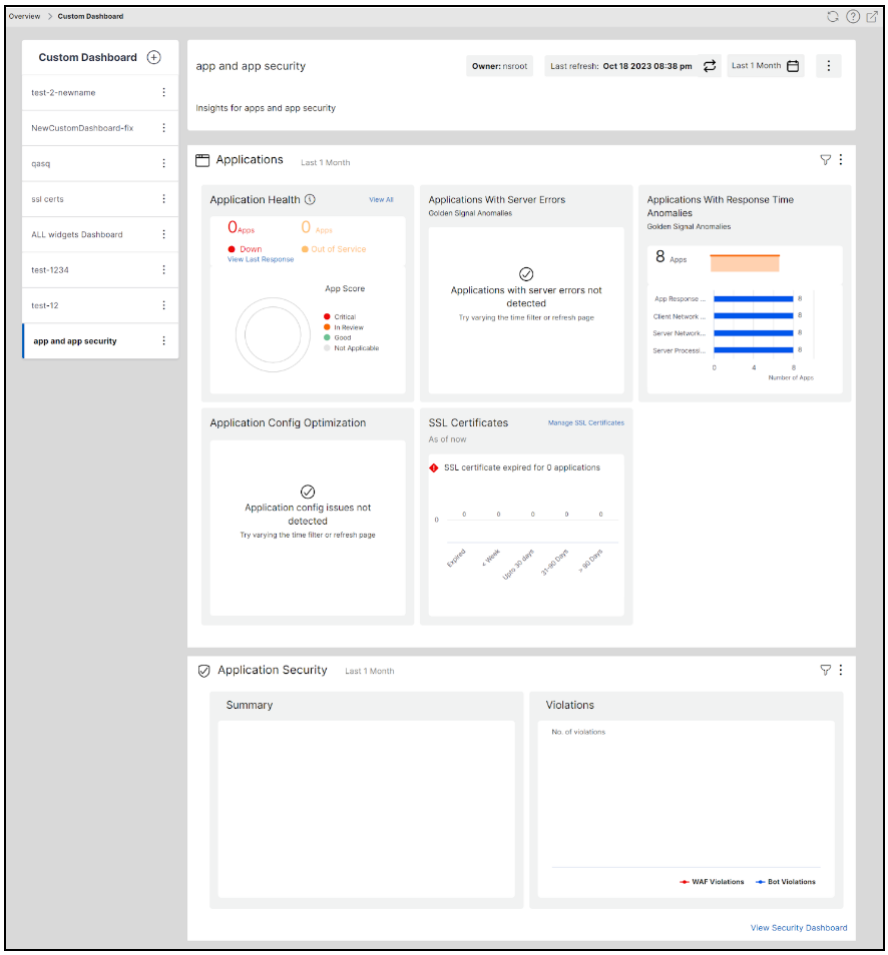
   c) **Agregar widget al panel**: En este ejemplo, el requisito es agregar widgets para las aplicaciones y la seguridad de las aplicaciones. Seleccione los widgets que desea supervisar de las categorías **Aplicacióny Seguridad de aplicaciones** .

   d) **Filtro de aplicaciones**: De forma predeterminada, el filtro se aplica a todas las aplicaciones. También puede crear un filtro y seleccionar solo aplicaciones específicas. Para obtener más información, consulte Crear y aplicar filtros.

   e) Haga clic en **Guardar**.



El panel se creó correctamente. Del mismo modo, puede crear hasta 20 paneles y seleccionar categorías en función de su elección especificando un nombre único para cada panel.

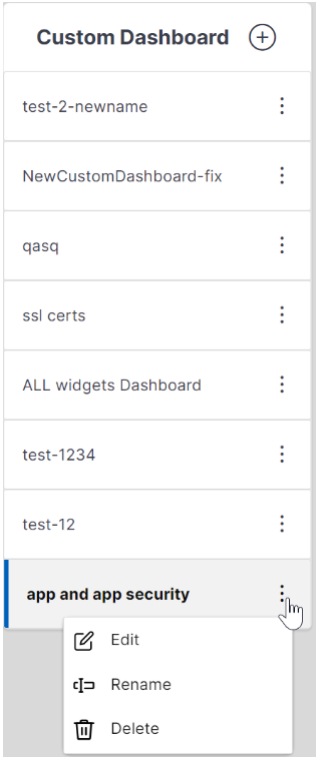


Puede utilizar las siguientes opciones después de crear un panel personalizado:

- **Modificar**: puede modificar el panel añadiendo más widgets o eliminándolos, aplicando filtros,

etc.

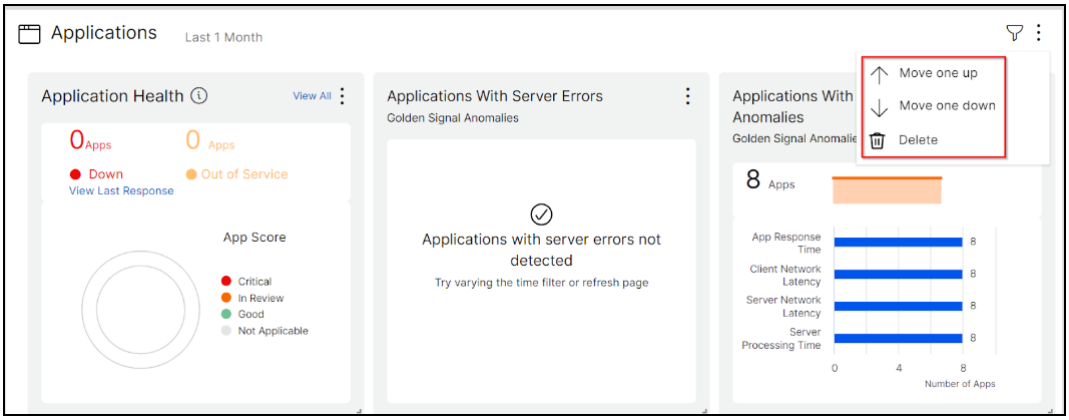
- **Cambiar nombre**: puede cambiar el nombre del panel.
- **Eliminar**: puede eliminar el panel de control.



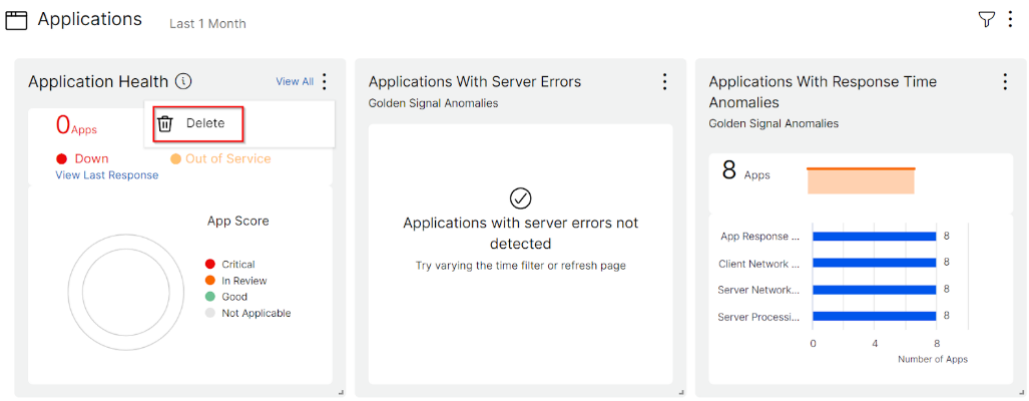
Más opciones en el panel

En el panel personalizado que ha creado, puede usar las siguientes opciones:

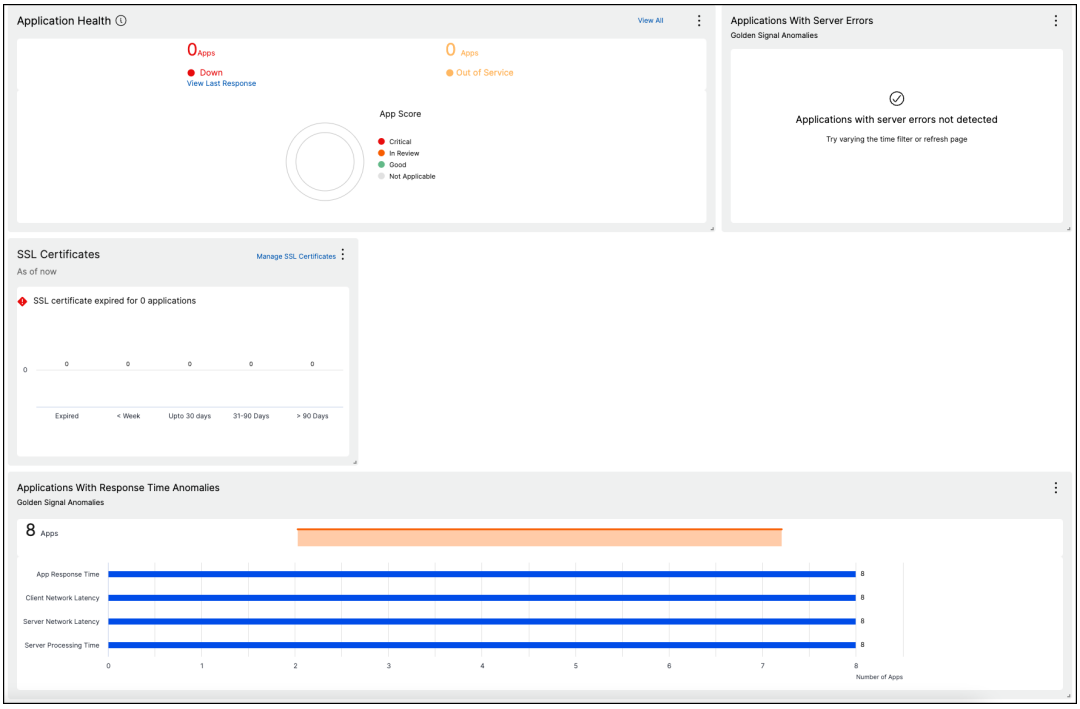
- **Modificar configuración**: también puede utilizar esta opción para modificar el panel añadiendo más widgets o eliminándolos, aplicando filtros, etc.
- **Modificar diseño**: puede usar esta opción para personalizar aún más el panel.
  - Puede seleccionar moverse hacia arriba, hacia abajo o eliminar.



- En los widgets, puede eliminar cualquier widget seleccionando la opción Eliminar.



- Arrastra y suelta para colocar los widgets donde quieras.
- Aumente o disminuya el tamaño del widget para tener una mejor visibilidad de ciertos datos.



Después de realizar los cambios, haga clic en **Guardar** para ver el panel actualizado.

Compartir el panel con otros usuarios

Puede compartir el panel con otros usuarios. Selecciona un panel existente y haz clic en **Compartir** . Escriba el nombre de usuario y haga clic en **Invitar** para compartir el panel. El usuario asignado puede ver el panel en modo de solo lectura.

Seguridad de API

January 26, 2024

Las API, o interfaces de programación de aplicaciones, son conjuntos de reglas, protocolos y herramientas que permiten que diferentes aplicaciones o sistemas de software se comuniquen entre sí. Las API desempeñan un papel importante en la protección de los datos confidenciales al hacer cumplir los controles de acceso, la autenticación y el cifrado, lo que garantiza que solo las entidades autorizadas puedan acceder a la información confidencial y transmitirla de forma segura.

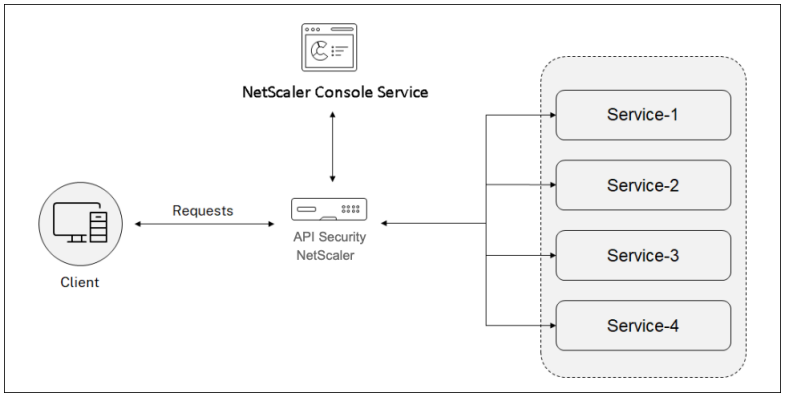
Las API funcionan como marco de backend para aplicaciones web y móviles. Por lo tanto, es fundamental proteger los datos confidenciales que transfieren. La seguridad de las API se refiere a la práctica de prevenir o mitigar los ataques a las API.

En la seguridad de las API, una puerta de enlace actúa como punto de entrada para todas las solicitudes a los puntos finales de la API. Además, garantiza un acceso seguro y confiable a todos los endpoints y microservicios de API en su sistema.

Para proteger tus API, sigue estos pasos:

- Crear o cargar una definición de API
- Implementar una instancia de API
- Agregar directivas a una implementación de API

La siguiente imagen describe cómo la seguridad de la API de NetScaler Console recibe la solicitud del cliente y envía la respuesta desde los servicios de API de fondo:



> **Nota:**
>
> En NetScaler Console, esta función está disponible para los usuarios que tienen licencias Premium o Advanced.

Ventajas de la seguridad de las API

La seguridad de la API le ofrece las siguientes ventajas:

- **Protege los puntos finales de la API**: la seguridad de la API añade una capa de seguridad y protege los puntos finales de la API y los servidores API de fondo de ataques como los siguientes:
  - Desbordamiento de búfer
  - Inyección SQL
  - Scripts entre sitios
  - Denegación de servicio (Dos)
- **Supervisa y mejora el rendimiento de la API**: la seguridad de la API proporciona servicios como la descarga de SSL, la autenticación, la autorización, la limitación de velocidad y más. Estos servicios aumentan el rendimiento de la API y su disponibilidad.

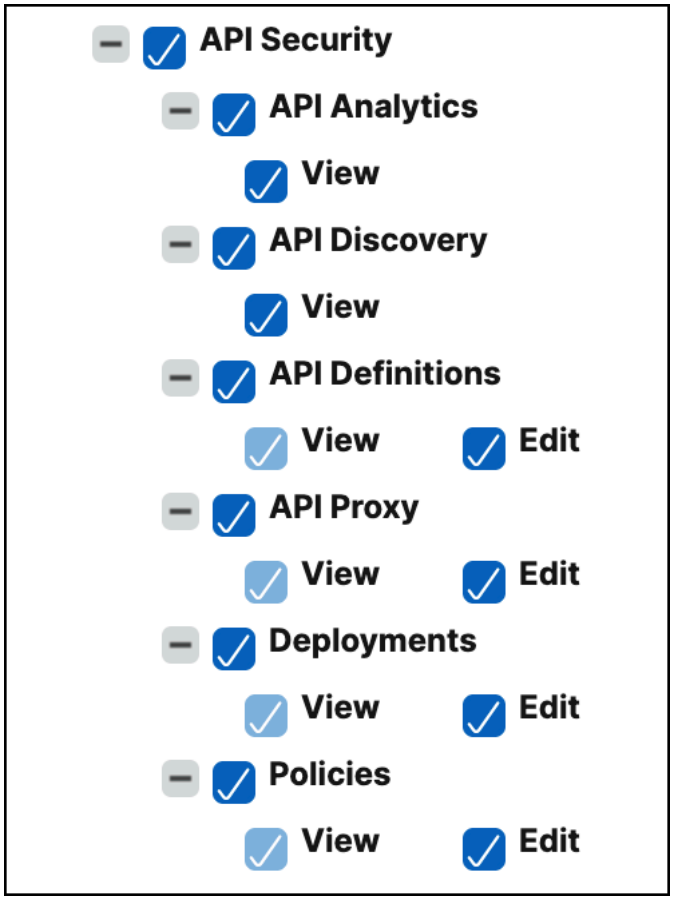
  Los análisis de API le proporcionan la visibilidad de las métricas de rendimiento de la API y las amenazas a sus endpoints de API. Para obtener más información, consulte Ver análisis de la API.

- **Administra el tráfico de la API**: la seguridad de la API abstrae la complejidad de su infraestructura de API de back-end.
- **Descubre los puntos finales de la API**: la seguridad de la API descubre los puntos finales de la API que se encuentran en su organización y los agrega a la página de **detección de la API** .

Otorgue permisos de configuración y administración de API Security

Como administrador, puede crear una directiva de acceso para conceder permisos a los usuarios para la configuración y administración de API Security. Los permisos de usuario pueden ser ver, agregar, modificar y eliminar. Haga lo siguiente para conceder permisos:

1. Vaya a **Configuración > Usuario y funciones > Directivas de acceso**.
2. Haga clic en **Agregar**.
3. En **Crear directivas de acceso**, especifique un nombre de directiva y la descripción.
4. En el campo **Permisos**, expanda **Aplicaciones** y, a continuación, **Seguridad de API**.
5. Selecciona las páginas de **seguridad de la API** necesarias. A continuación, seleccione los permisos que quiere conceder.



> **Importante:**
>
> Asegúrese de conceder permisos para las funciones necesarias para utilizar una seguridad de API. Por ejemplo, si concede acceso de usuario a la página **Implementaciones**, las siguientes características también requieren acceso de usuario:
>
> - StyleBooks
> - IPAM
> - Equilibrio de carga (en **Funciones de red**)
> - Conmutación de contenido (en **Funciones de red**)
> - Proxy API de dispositivo (en **API**)

Para obtener más información sobre las políticas de acceso, consulte Configurar las políticas de acceso en NetScaler Console.

Crear o cargar una definición de API

January 26, 2024

Una definición de API es un documento que describe una API utilizando estándares de especificación OpenAPI (Swagger 2.0, OpenAPI 3.0.x). Esta definición puede contener rutas de recursos API y métodos para operarlas. Puede añadir definiciones de API a NetScaler Console e implementarlas en una puerta de enlace de API (NetScaler).

Puede crear definiciones de API de una de las siguientes maneras:

- Cargar archivo de especificación de Swagger OAS
- Cree su propia definición de API

> **Nota:**
>
> Actualmente, NetScaler Console admite el análisis de archivos de especificaciones de OAS que utilizan **Swagger 2.0** u **openapi 3.0.1**.

Cargar la especificación de la OEA

Puede cargar la especificación OAS en la GUI de NetScaler Console.

1. Vaya a **Seguridad > API Security > Definiciones de API**.
2. Haga clic en **Agregar**.
3. Seleccione **Cargar Especificación OAS**.

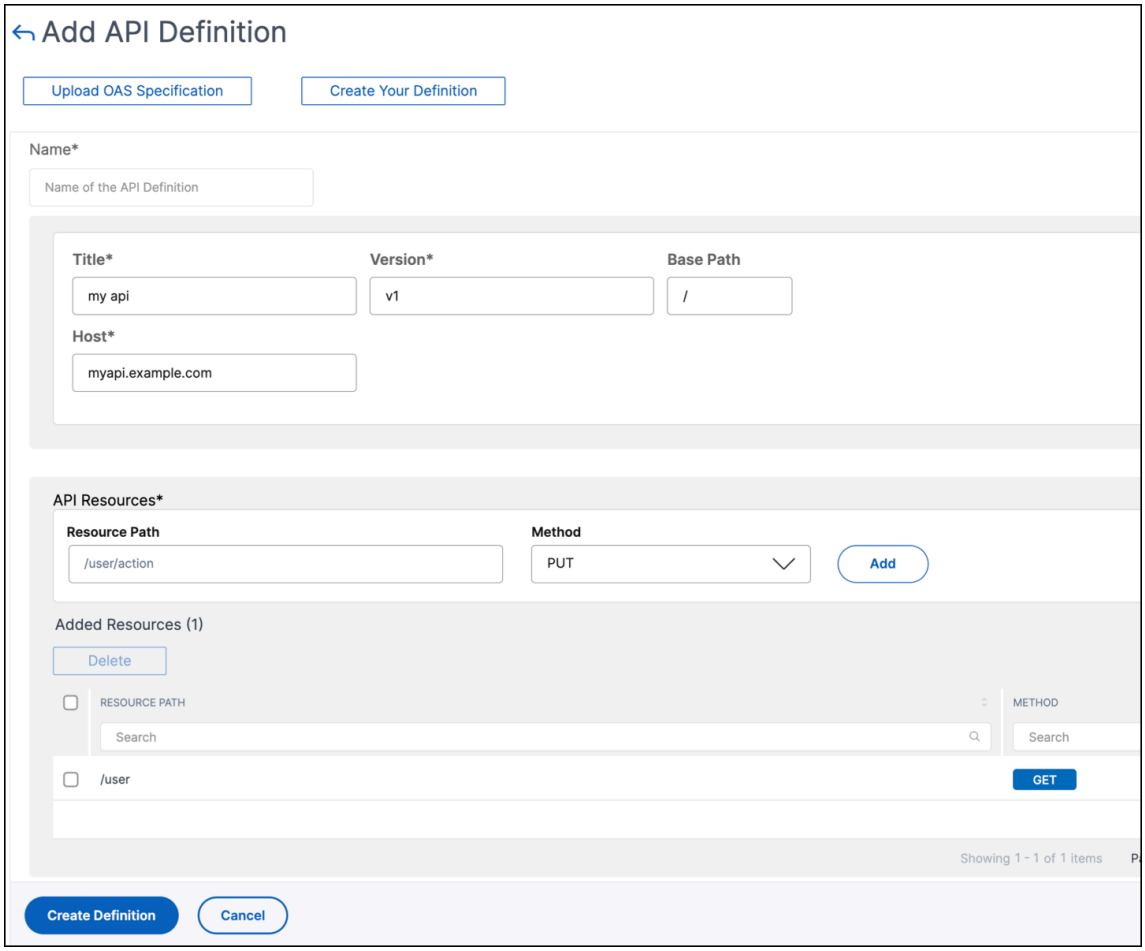
> **Nota:**
>
> Asegúrese de que el archivo de especificación OAS esté en formato YAML o JSON. Además, este archivo no debe contener referencias externas. Actualmente, NetScaler Console es compatible con la versión 2.0 de Swagger.

4. Busque una especificación de OAS en su equipo local y cárguela en NetScaler Console.

Crear una definición de API

Puede crear su propia definición de API en la GUI de NetScaler Console.

1. Vaya a **Seguridad > API Security > Definiciones de API**.
2. Haga clic en **Agregar**.
3. Seleccione **Crear su definición** y especifique lo siguiente:
   - **Nombre**: Nombre para la definición de API.
   - **Definición de API**: Una definición debe incluir título, versión, ruta base y host. Puede especificar un nombre de dominio o una dirección IP en el campo **Host**.
   - **Recursos de API**: Agregue varios recursos API a su definición. Cada recurso tiene una ruta de acceso y un método soportado. Haga clic en **Agregar**. El recurso se agrega a la tabla **Recursos agregados** . Haga clic en **Eliminar** para eliminar un recurso de API.



4. Haga clic en **Crear**.

Ver definiciones de API

La página **Definiciones de API** muestra la definición cargada. Haga clic en **Ver** para ver los siguientes detalles de la definición de API:

- **Nombre**: Muestra el nombre de una definición de API.
- **Definición de API**: Muestra el título, la versión, la ruta base y el host de una definición.
- **Recursos de API**: Enumera los recursos de API en una definición de API y sus métodos para operarlos.

Implementar una instancia de API

January 26, 2024

Para implementar una instancia de API, necesitas un proxy de API. Un proxy de API es un servidor virtual de cliente en el que API Security (instancia de NetScaler) recibe el tráfico de API de los clientes de API. Los clientes de la API pueden ser navegadores, aplicaciones móviles, etc.

Puede compartir un proxy de API con diferentes implementaciones de API. En una organización en la que tiene muchos servicios de API, puede crear un proxy de API independiente para cada servicio de API. O bien, puede crear y compartir un proxy de API con instancias de API para diferentes servicios de API.

Por ejemplo, los dos servicios de API `app1` y `app2` se implementan en la misma seguridad de API y utilizan el mismo servidor virtual front-end. Desea proporcionar la misma dirección IP virtual e información de certificado SSL a ambos servicios de API. En este caso, puede agregar un proxy de API con la información requerida y compartirlo con distintas implementaciones. Por lo tanto, los servicios de API en diferentes implementaciones pueden recibir solicitudes mediante el proxy de API compartido.

Como administrador, haga lo siguiente para implementar una instancia de API:

1. Agregue un proxy de API.
2. Implemente una instancia de API mediante el proxy de la API.

Agregar un proxy de API

Siga los pasos para agregar un proxy de API:

1. Vaya a **Seguridad > Seguridad de API > Proxy de API > Agregar**.
2. Especifique lo siguiente:
    - **Nombre de proxy**: Nombre de un proxy de API.
    - Instancia de**NetScaler de destino**: Seleccione una instancia de NetScaler que actúe como puerta de enlace de API.
    - **Dirección IP: dirección** IP del servidor virtual que aloja los servicios de API.
    - **Puerto**: número de puerto del servidor virtual que aloja los servicios de API.
    - **Protocolo**: Establezca un protocolo en función del tipo de tráfico que desee recibir en el proxy de la API (HTTP o HTTPS).
    - **Perfil de seguridad TLS**: seleccione Alto o Medio en la lista. Si selecciona Alto, se asigna al perfil SSL con calificación A+ en una instancia de NetScaler.
    - **Almacén de certificados**: Seleccione el certificado SSL para la seguridad de la API. El almacén de certificados del agente de NetScaler le ayuda a almacenar y administrar sus certificados SSL en un solo lugar.

En el almacén de certificados del agente de NetScaler, puede almacenar los certificados SSL en el agente de NetScaler y reutilizarlos durante la configuración de NetScaler.

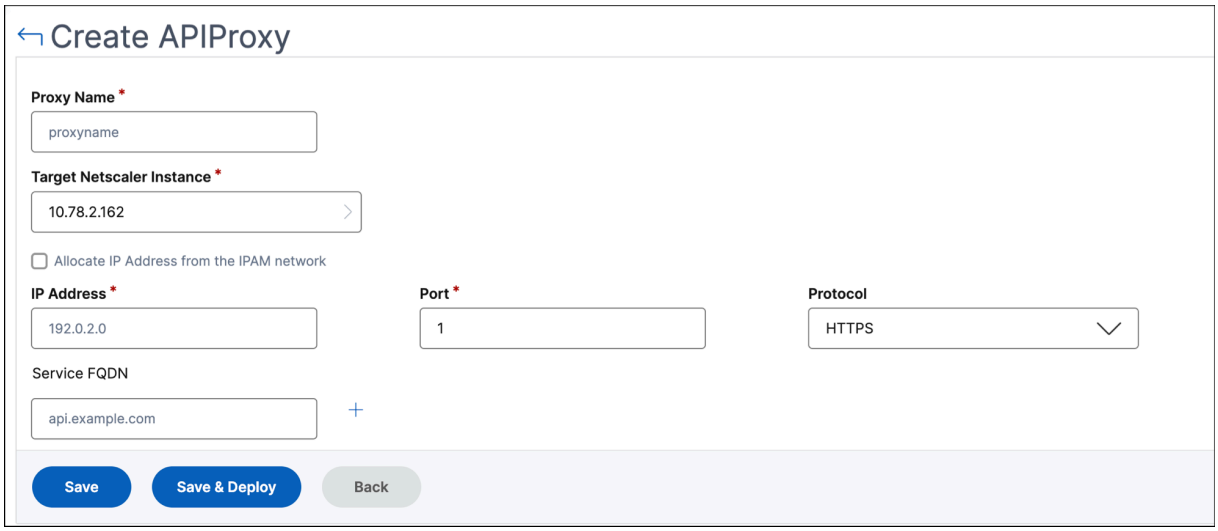
> **Nota:**
>
> Si sus implementaciones actuales utilizan el certificado o la clave SSL que no se encuentran en el almacén de certificados del agente de NetScaler, debe agregar el certificado y la clave al almacén con el mismo nombre.

- **FQDN del servicio**: un nombre de dominio completo en el que se alojan los servicios de la API. Por ejemplo: `api.example.com`

Alternativamente, puede seleccionar una red IPAM para asignar la dirección IP. Para ver la dirección IP asignada desde la red de IPAM, vaya a **Configuración > IPAM**. Para obtener más información sobre IPAM, consulte Configurar IPAM.

3. Haga clic en **Guardar** para guardar la configuración de implementación.

   Si desea implementar este proxy de API en la seguridad de la API, haga clic en **Guardar e implementar**.



Tras agregar un proxy de API, implemente una instancia de API.

Implemente una instancia de API mediante el proxy de API

Siga los pasos para implementar una instancia de API:

1. Vaya a **Seguridad > API Security > Implementaciones**.
2. Haga clic en **Agregar**.
3. En Información **básica de implementación** ,

a) Especifique el **nombre de la implementación**.

b) En **Definiciones de API**, seleccione la definición de API requerida.

c) Seleccione el **proxy de la API** que quiere usar con esta implementación.

4. En **Upstream Services**, haga clic en **Agregar** para agregar los servidores de API de fondo (origen) de los que quiera eliminar el tráfico de la API. Puede configurar un servicio ascendente con su nombre de dominio o dirección IP.

   Puede especificar los detalles de la dirección SNIP y la máscara de red al implementar una instancia de API. La instancia de NetScaler usa la dirección SNIP especificada para comunicarse con los servicios ascendentes (backend). La dirección SNIP especificada se convierte en la dirección IP de origen del tráfico de salida enviado a los servicios ascendentes. También puede usar IPAM para configurar la dirección SNIP y la máscara de red. Si no configura la dirección SNIP, la dirección SNIP predeterminada de la instancia de NetScaler se convierte en la dirección IP de origen de los servicios ascendentes.

   > **Nota:**
   >
   > De forma predeterminada, las opciones de dirección SNIP y máscara de red son opcionales. Sin embargo, si especifica una de estas opciones, también debe especificar otra opción.

   a) Especifique un nombre para un servicio ascendente.

   b) Especifique el dominio.

   c) En **Servicios**, especifique una dirección IP y un valor de puerto. Para agregar más direcciones IP, haga clic en **Agregar una nueva fila**.

   d) Haga clic en **Agregar**.

5. En **Enrutamiento**, especifique los siguientes detalles para enrutar el tráfico de API entrante según el prefijo de la ruta del recurso:

   a) Especifique el nombre de la ruta.

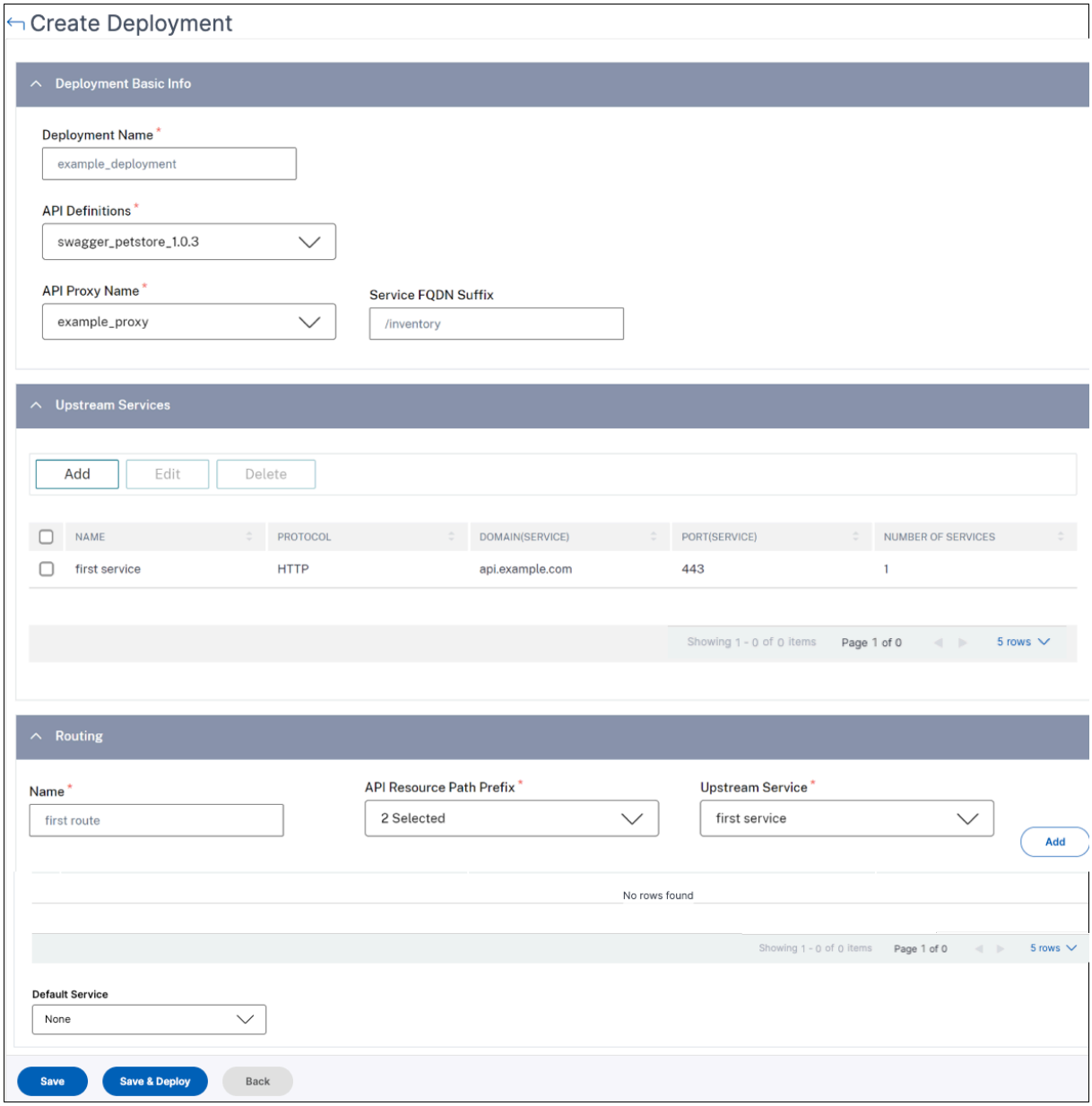
   b) Seleccione un **recurso de API** para recibir una solicitud de API.

   > **Nota:**
   >
   > También puede especificar la ruta personalizada o el prefijo de ruta.

   c) Seleccione un **servicio ascendente** de la lista al que quiera transferir el tráfico de la API.

6. Haga clic en **Guardar** para guardar la configuración de implementación.

   Si desea implementar la configuración en la seguridad de la API, haga clic en **Guardar e implementar**.



Habilitar el análisis de API

Los siguientes son los requisitos previos para habilitar el análisis para una implementación:

- 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**

Para habilitar el análisis de API para una implementación, haga lo siguiente:

1. En **Seguridad > Seguridad de la API > Implementaciones**, seleccione la implementación en la que desea habilitar el análisis de la API.
2. Haga clic en **Habilitar análisis**.
3. En la página **Configurar Analytics para implementación**, seleccione el servidor virtual y haga clic en **Habilitar Analytics**.
4. En la ventana **Habilitar análisis**:
   a) Seleccione el tipo de información (Web Insight, Security Insight, Bot Insight)
   b) Seleccione **Logstream** o **IPFIX** como modo de transporte.

      Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

      La expresión es true de forma predeterminada.
   c) Haga clic en **Aceptar**.

NetScaler Console permite realizar análisis en los servidores virtuales seleccionados.

Agregar directivas a una implementación de API

January 26, 2024

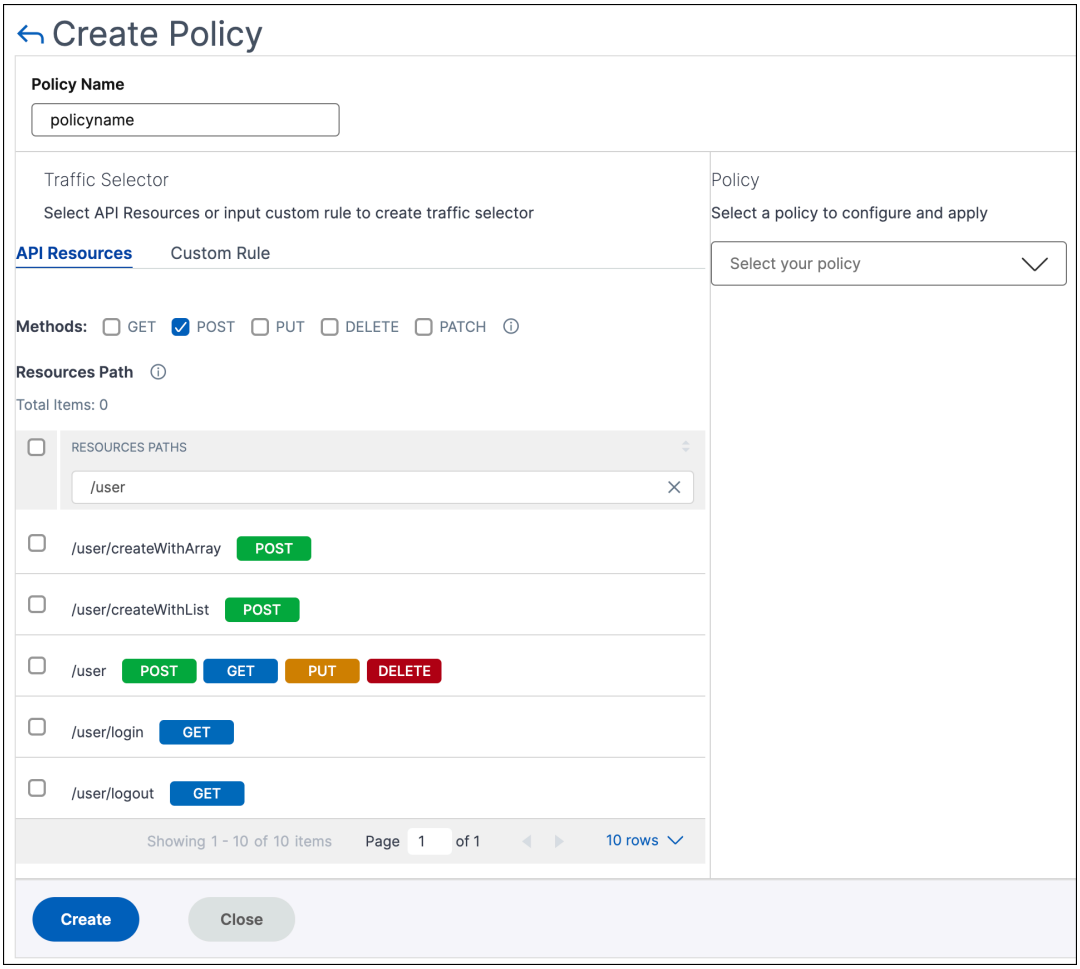
Puede configurar varias directivas de seguridad para el tráfico de la API. Esta configuración requiere que especifique los criterios de selección de tráfico y los parámetros necesarios para una directiva. Realice los siguientes pasos para agregar una directiva a una definición de API:

1. Vaya a **Seguridad > Seguridad de API > Directivas**.
2. Haga clic en **Agregar**.
3. Especifique el nombre de un grupo de directivas.
4. Seleccione una **implementación** de la lista.
5. Seleccione un **servicio ascendente** de la lista para el que quiera configurar directivas.
6. Haga clic en **Agregar** para seleccionar selectores de tráfico y un tipo de directiva.

   Selector de tráfico: los criterios de selección de tráfico incluyen rutas de recursos de API o prefijos de ruta, métodos y directivas.

   Puede utilizar cualquiera de las siguientes opciones para especificar criterios de selección de tráfico:

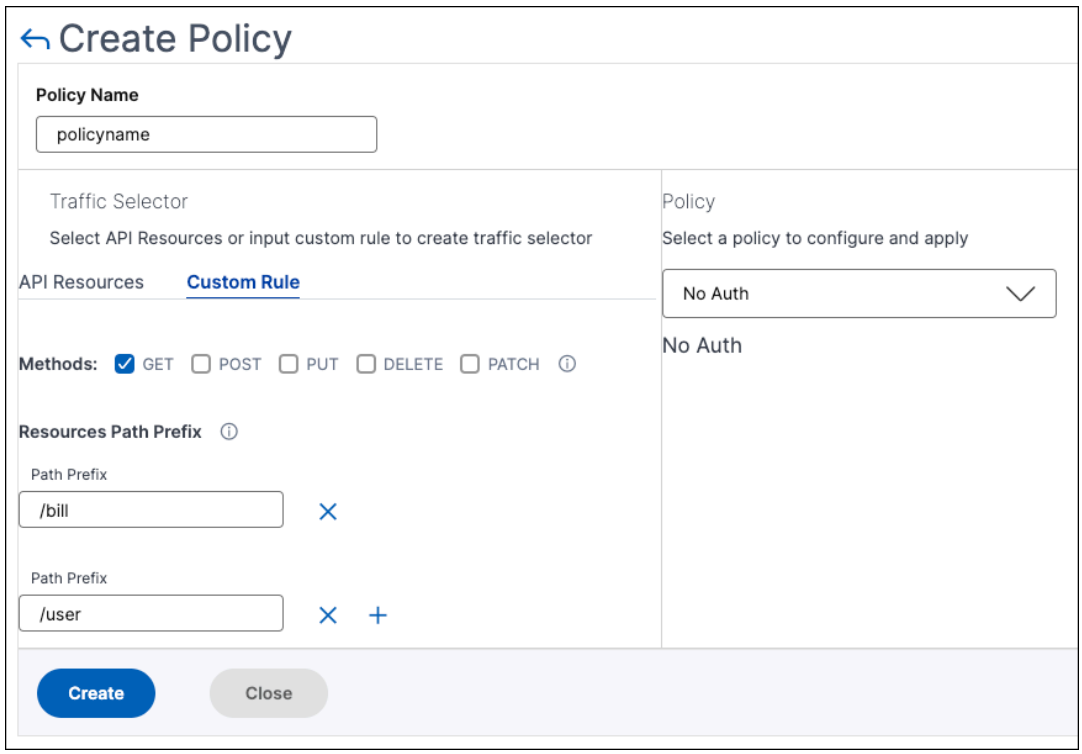
- **Recursos de API**: Seleccione un recurso de API y sus métodos para los que quiere aplicar una directiva. Puede buscar recursos y métodos de la API con una palabra clave.



En este ejemplo, se enumeran los recursos de API con `/user` que tienen el método `POST`.

- **Regla personalizada**: en esta ficha, puede especificar prefijos de ruta personalizados y varios métodos.

  La directiva configurada se aplica a una solicitud de API entrante que coincide con la regla personalizada para la selección del tráfico de API.



En este ejemplo, la directiva **Sin autenticación** se aplica a los recursos de API que tienen el prefijo `/bill` y el método `GET`.

En **Directiva**, seleccione una directiva de la lista que quiera aplicar al recurso y método de API seleccionados. Para obtener más información sobre cada directiva, consulte Tipos de directivas.

7. Opcional, puede mover tipos de directivas para establecer una prioridad. Los tipos de directivas con mayor prioridad se aplican primero.
8. Haga clic en **Guardar** para agregar una directiva. Si quiere aplicar la directiva inmediatamente, haga clic en **Guardar y aplicar**.

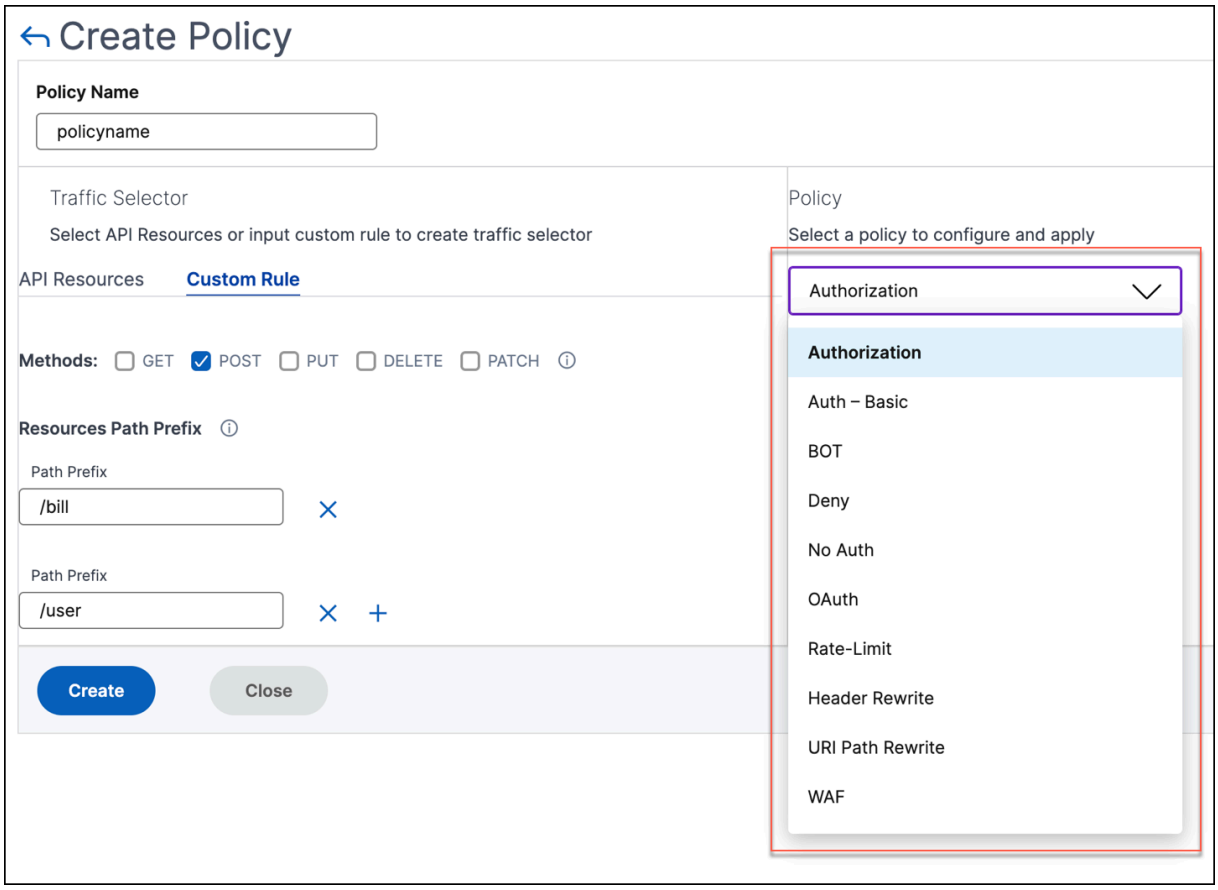
Tipos de directivas

Al configurar una directiva de API, puede seleccionar las siguientes directivas que quiere aplicar al recurso y método de la API:

- **Autenticación y autorización**
- **Límite de tarifa**
- **WAF**
- **BOT**

- **Reescritura de encabezado**
- **Reescritura de ruta de URI**
- **Negar**

> **Nota:**
>
> Para gestionar la seguridad de las API mediante las API, consulta Utilizar las API para gestionar la seguridad de las API.



Autenticación y autorización

Los recursos de API están alojados en una aplicación o servidor API. Cuando quiera aplicar restricciones de acceso a dichos recursos de API, puede usar las directivas de autenticación y autorización. Estas directivas verifican si la solicitud de API entrante tiene un permiso necesario para acceder al recurso.

Utilice las siguientes directivas para definir la autenticación y autorización para los recursos de API seleccionados:

No-Auth Utilice esta directiva para omitir la autenticación en el tráfico seleccionado.

Auth-Basic Esta directiva especifica la autenticación local que se utilizará con el esquema de autenticación básica HTTP. Para utilizar la autenticación local, debe crear cuentas de usuario en NetScaler.

OAuth OAuth requiere un proveedor de identidades externo para autenticar un cliente mediante OAuth2 y emitir un token de acceso. Cuando el cliente proporciona este token como credencial de acceso a una puerta de enlace de API, el token se valida en función de los valores configurados.

- **URI de JWK**: La URL de un extremo que tiene JWK (JSON Web Key) para la verificación JWT (JSON Web Token)
- **Emisor**: la identidad (normalmente una URL) del servidor de autenticación.
- **Audiencia**: La identidad del servicio o aplicación para la que se aplica el token.
- **Reclamaciones para guardar**: los permisos de acceso se representan como un conjunto de notificaciones y valores esperados. Especifique los valores de notificación en el formato CSV.
- **URI de introspección**: URL de extremo de introspección del servidor de autenticación. Esta URL se utiliza para verificar tokens de acceso opacos. Para obtener más información sobre estos tokens, consulte Configuración de OAuth para tokens de acceso opacos.

  Después de especificar el **URI de introspect**, especifique el **Id. de cliente** y el **secreto de cliente** para tener acceso al servidor de autenticación.
- **Algoritmos permitidos**: esta opción le permite restringir ciertos algoritmos en los tokens entrantes. De forma predeterminada, todos los métodos admitidos están permitidos. Sin embargo, puede verificar los algoritmos necesarios para el tráfico seleccionado.

Si la validación se realiza correctamente, API Security otorga acceso al cliente.

> **Importante:**
>
> Al configurar una directiva de OAuth o **Auth-Basic** para los recursos de API seleccionados, configure la directiva de **no autenticación** para los recursos de API restantes. Esta configuración indica explícitamente que quiere omitir la autenticación para los recursos restantes.

Autorización Esta directiva verifica los permisos necesarios para acceder a un recurso API. Los permisos de acceso se representan como un conjunto de notificaciones y valores esperados. Para configurar esta directiva, seleccione **Agregar una nueva notificación** y especifique lo siguiente:

- Nombre del reclamo
- Valores de reclamación

> **Importante:**
>
> La seguridad de la API requiere directivas de autenticación y autorización para el tráfico de la API. Por lo tanto, debe configurar una directiva de autorización con una directiva de autenticación. La directiva de autenticación puede ser OAuth o. `Auth-Basic`
>
> Incluso si no tiene ninguna comprobación de autorización, debe crear una directiva de autorización con solicitudes vacías. De lo contrario, la solicitud se deniega con un error 403.

Límite de tarifa

Especifique la carga máxima dada al recurso API seleccionado. Con esta directiva, puede supervisar la tasa de tráfico de la API y tomar medidas preventivas. Para configurar esta directiva, especifique lo siguiente:

- **Nombre de encabezado HTTP**: es una clave de selector de tráfico que filtra el tráfico para identificar las solicitudes de API. Además, la directiva Límite de tarifas se aplica y supervisa solo a dichas solicitudes de API.
- **Valores de encabezado**: estos valores de encabezado están separados por comas para el nombre del encabezado mencionado.
- **Umbral**: el número máximo de solicitudes que se pueden permitir en el intervalo especificado. Si ha especificado **valores de encabezado**, este umbral se aplica a cada valor de encabezado.

  Ejemplo 1:

  Al especificar los valores de encabezado (`"key1","key2","key3"`) para el nombre del encabezado `x-api-key` y establecer el umbral en `80`, el umbral establecido se aplica a cada valor de encabezado.

  Ejemplo-2:

  Si quiere especificar umbrales diferentes para cada valor de encabezado, cree directivas de límite de velocidad independientes con el mismo nombre de encabezado HTTP.

  - **Directiva 1**: especifique los valores de encabezado (`"key1","key2"`) para el nombre del encabezado `x-api-key` y establezca el umbral en `80`.
  - **Directiva 2**: especifique los valores de encabezado (`"key3"`) para el nombre del encabezado `x-api-key` y establezca el umbral en `30`.

  Si no especificas un valor de encabezado, el umbral se aplica al nombre de encabezado HTTP especificado.
- **Time Slice** - El intervalo especificado en microsegundos. Durante este intervalo, las solicitudes se supervisan en función de los límites configurados. De forma predeterminada, se establece en 1000 microsegundos (1 milisegundo).

- **Tipo de límite**: el modo en el que quiere aplicar la directiva de límite de tasa. Puede seleccionar el tipo de límite de **ráfaga** o **Suavizar**.
- **Acción**: define una acción que quiere realizar sobre el tráfico que infringe el umbral. Puede especificar una de las siguientes acciones:
  - **DROP**: elimina las solicitudes por encima de los límites de tráfico configurados.
  - **RESET: restablece**la conexión de las solicitudes.
  - **REDIRECT**: Redirige el tráfico al redirect_url configurado.
  - **RESPOND**: Responde con la respuesta estándar (`429 Too many requests`).

WAF

Esta directiva evita infracciones de seguridad, pérdida de datos y posibles modificaciones no autorizadas en sitios web que acceden a información confidencial de negocios o clientes.

Antes de configurar una política WAF, cree un perfil WAF en NetScaler Console con StyleBooks.

En **Nombre de perfil WAF**, seleccione o especifique el perfil WAF que ha creado.

Bot

Esta directiva identifica los robots defectuosos y protege el dispositivo de ataques de seguridad avanzados.

Antes de configurar una política de BOT, cree un perfil de BOT en NetScaler Console con StyleBooks.

En **Nombre de perfil de bot**, especifique el perfil BOT que ha creado.

Reescritura de encabezado

Esta directiva le ayuda a modificar el encabezado de las solicitudes y respuestas de API. Si quiere reemplazar el valor en el encabezado HTTP, especifique lo siguiente:

- **Nombre de encabezado HTTP**: nombre archivado que quiere modificar en el encabezado de solicitud.

  Ejemplo:`Host`
- **Valor de encabezado**: opcional, la cadena de valor que quiere modificar en el nombre de encabezado especificado.

  Ejemplo:`sample.com`

- **Nuevo valor de encabezado**: El nuevo valor para reemplazar el valor de encabezado especificado.

  Si no se especifica ningún **valor de encabezado**, sustituye cualquier valor recibido por el valor especificado al **Nombre de encabezado HTTP**.

  Ejemplo:`example.com`

En este ejemplo, la directiva de reescritura de encabezado reemplaza `sample.com` a `example.com` en el `Host` campo de una solicitud de API.

Reescritura de ruta de URI

Esta directiva le ayuda a modificar la ruta de URI de las solicitudes y respuestas de la API. Si quiere reemplazar un segmento en la ruta de la URI, agregue una regla para realizar una de las siguientes acciones:

- **Reemplazar un segmento de ruta**: al seleccionar este tipo de acción, especifique lo siguiente:
  - Segmento de**ruta actual: segmento** de ruta que quiere reemplazar.
  - **Nuevo segmento de ruta**: nuevo segmento de ruta que reemplaza solo al segmento de ruta actual.

  Por ejemplo, para cambiar una configuración regional en la ruta de la URI de inglés a chino, especifíquela `/en-us/` en **Segmento de ruta actual**. Y especifique `/zh-zh` en **Nuevo segmento de ruta**. Reemplaza solo el segmento de ruta y conserva la ruta URI restante.
- **Reemplazar la ruta completa**: este tipo de acción reemplaza por completo la ruta de URI de las solicitudes y respuestas de la API por la ruta especificada. Si especifica `/example.html` en **Nuevo segmento de ruta**, la ruta de URI de una solicitud o respuesta de la API se cambia a la ruta especificada.
- **Eliminar el segmento de ruta**: esta acción elimina el segmento especificado del URI. Por ejemplo, para eliminar la configuración regional en inglés de la ruta URI, especifíquela `/en-us/` en **Segmento de ruta actual**.
- **Insertar un segmento de ruta**: esta acción inserta el segmento especificado en la ruta URI. Para aplicar esta regla, especifique la posición en la que quiere insertar el segmento. Y qué segmento quiere insertar.

  Por ejemplo, si quiere insertar un segmento justo después de un texto, haga lo siguiente:

  1. Especifique la posición en la que quiere insertar un segmento nuevo.
  2. En **Segmento de ruta actual**, especifique el texto tras el cual se agregará un segmento nuevo.
  3. En **Nuevo segmento de ruta**, especifique el segmento que quiere agregar.

Negar

Esta directiva le ayuda a impedir que las solicitudes de API lleguen a sus recursos de API.

Ver análisis de API

January 26, 2024

El análisis de API permite la visibilidad del tráfico de API. Este análisis permite a los administradores de TI supervisar las instancias de API y los puntos finales servidos por una puerta de enlace API. Proporciona supervisión periódica integrada de las solicitudes de API.

Antes de supervisar los análisis de la API, asegúrese de completar lo siguiente:

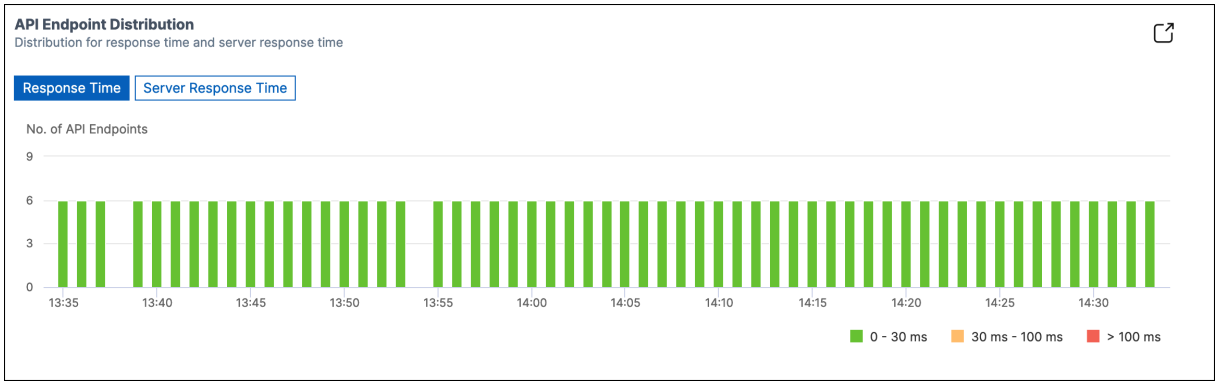
1. Agregar una definición de API
2. Implemente una definición de API
3. Agregar una directiva a una definición de API
4. Aplicar la licencia a las instancias de API
5. Habilitar Web Insight en instancias de API

En **API Analytics**, puede supervisar el tiempo de respuesta de las instancias y puntos de enlace de la API que se agregan como parte de las definiciones de la API. También muestra el ancho de banda que consumen las instancias y puntos finales de la API.

De forma predeterminada, el panel muestra los análisis de la API de la última hora. Puede seleccionar una duración para ver el análisis de API para ese intervalo. Haga clic en **Ver más** en cada icono para ver toda la lista. En esta vista, puede buscar instancias de API y puntos finales por sus nombres parciales, excepto el mosaico **Ubicaciones geográficas**.

Distribución de punto final de API

Este gráfico muestra la distribución del tiempo de respuesta de las aplicaciones y los servidores para los puntos de enlace de la API. Puede identificar un punto final de API que tenga un tiempo de respuesta enorme y tomar las medidas necesarias.

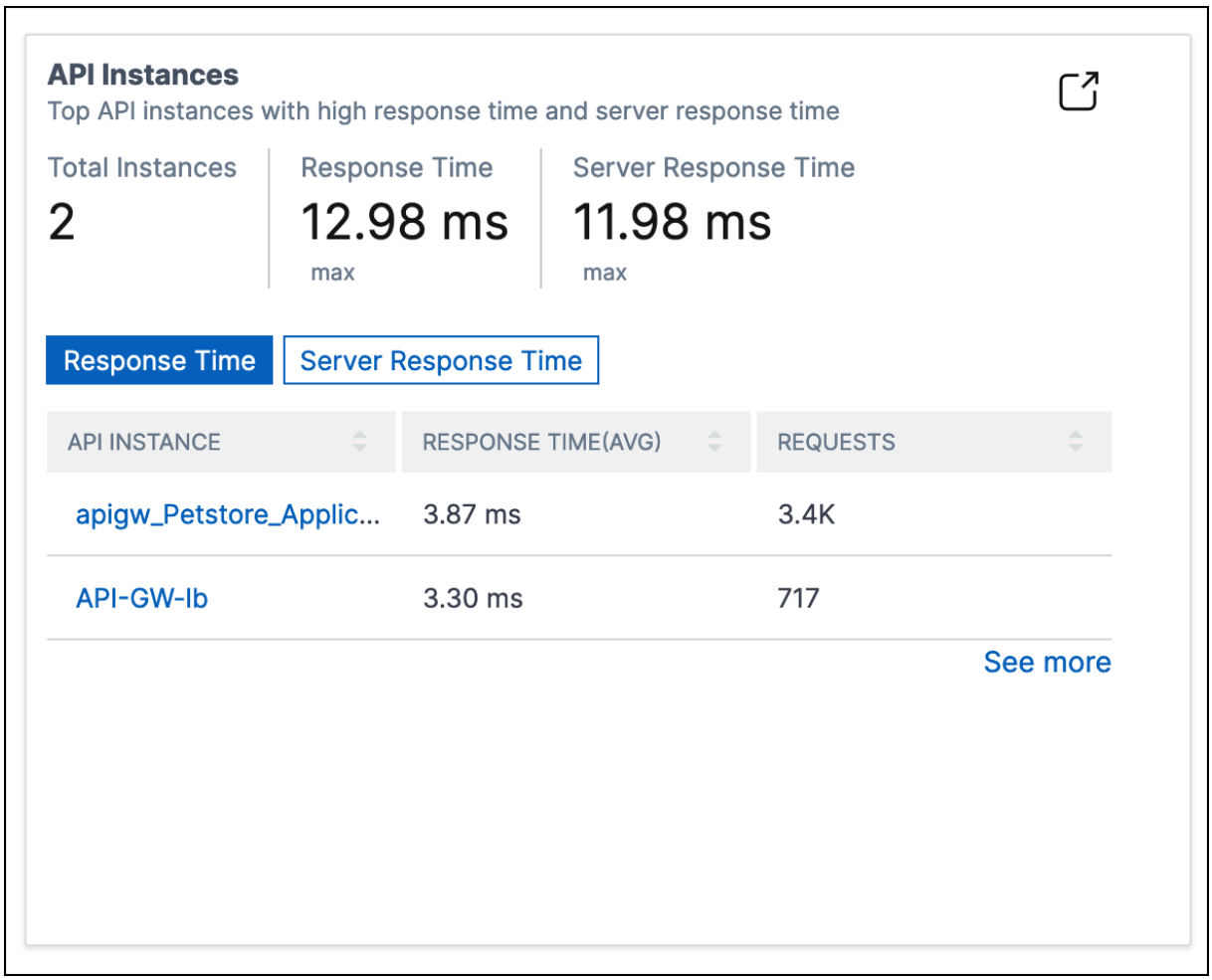


Los puntos de enlace de la API aparecen en uno de los siguientes colores en función de sus límites de tiempo de respuesta:

- **Verde**: Si el tiempo de respuesta es inferior a 30 milisegundos.
- **Naranja**: si el tiempo de respuesta está entre 30 y 100 milisegundos.
- **Rojo**: si el tiempo de respuesta es superior a 100 milisegundos.

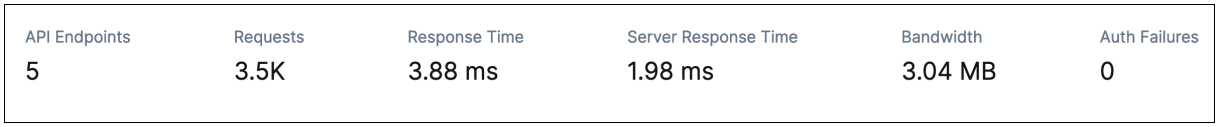
instancias de API

El mosaico de **instancias de API** muestra las principales instancias de API con un tiempo de respuesta elevado de aplicaciones y servidores.



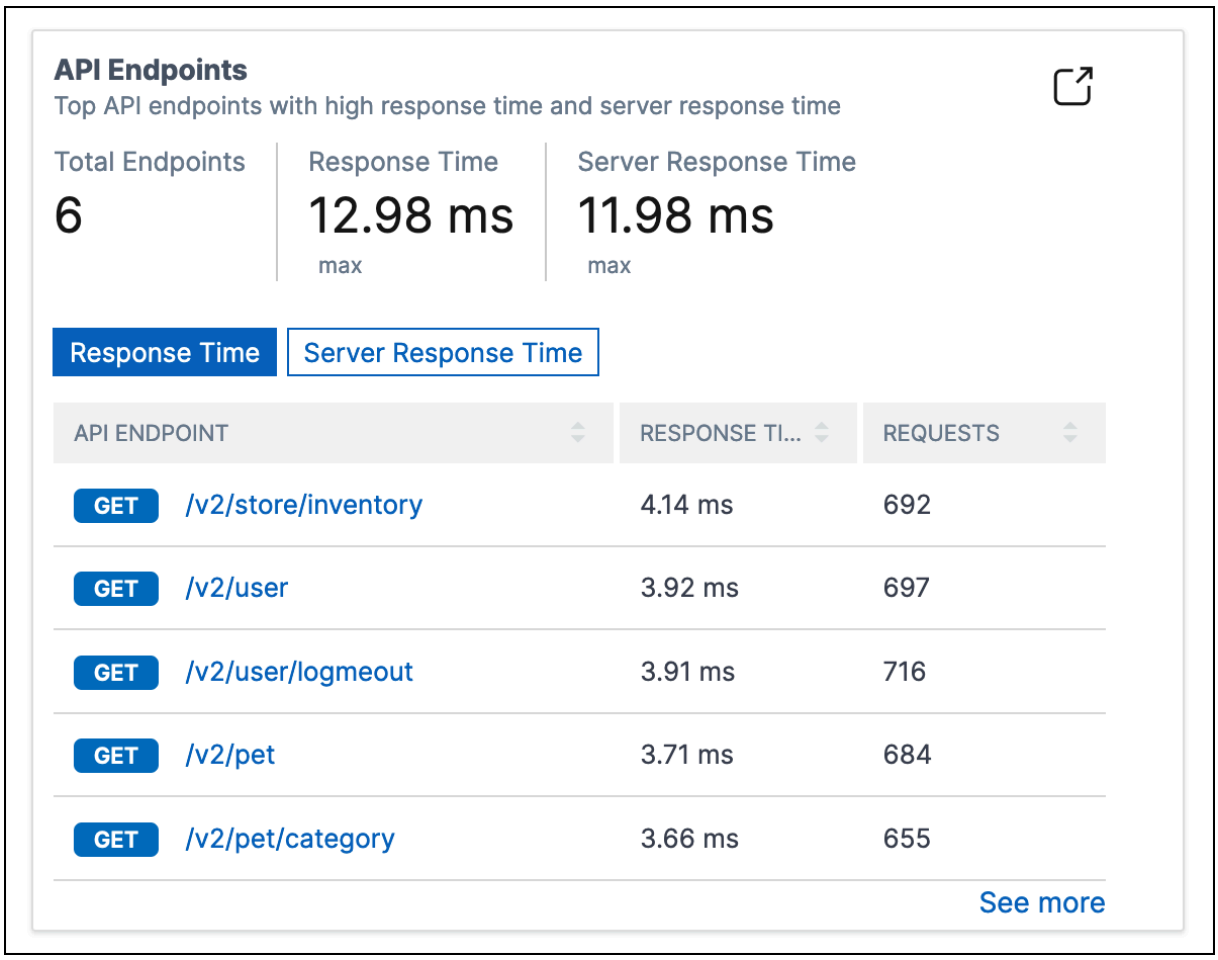
Seleccione una instancia de API para ver sus detalles de rendimiento, uso y seguridad. La instancia de API seleccionada muestra la siguiente información:

- Recuento de puntos finales de API
- Recuento de solicitudes
- Tiempo de respuesta de aplicaciones y servidores
- Ancho de banda utilizado
- Fallos de autenticación



Dispositivos de punto final de API

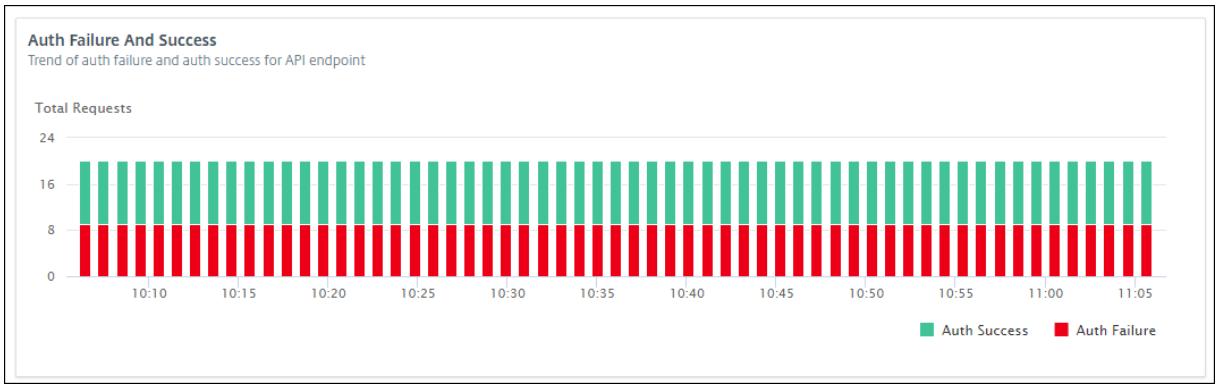
El mosaico **de puntos de enlace de la API** muestra los puntos de enlace principales con un tiempo de respuesta elevado de aplicaciones y servidores.



Seleccione un punto de enlace de la API para ver los detalles de rendimiento, uso y seguridad.

Fallos de autenticación

El cuadro **Fallos de autenticación muestra los** principales puntos de enlace de la API que tienen más errores de autenticación. El error o el éxito de la autenticación se producen en función de la directiva agregada a una definición de API.



Si quiere ver los errores y la tasa de éxito de la autenticación en un punto final de la API, haga lo siguiente:

1. Seleccione un punto final de los **extremos de la API**.
2. Seleccione la ficha **Seguridad**. Esta ficha muestra los errores y éxitos de autenticación en el punto final seleccionado.

Si quieres ver los errores y el porcentaje de éxito de la autenticación en los puntos de enlace de la API de una instancia, haga lo siguiente:

1. Seleccione una instancia de la **instancia de API**.
2. Seleccione la ficha **Seguridad**. En esta ficha se muestran los errores y éxitos de autenticación en los puntos finales de la instancia seleccionada.

Vea diferentes perspectivas de la API

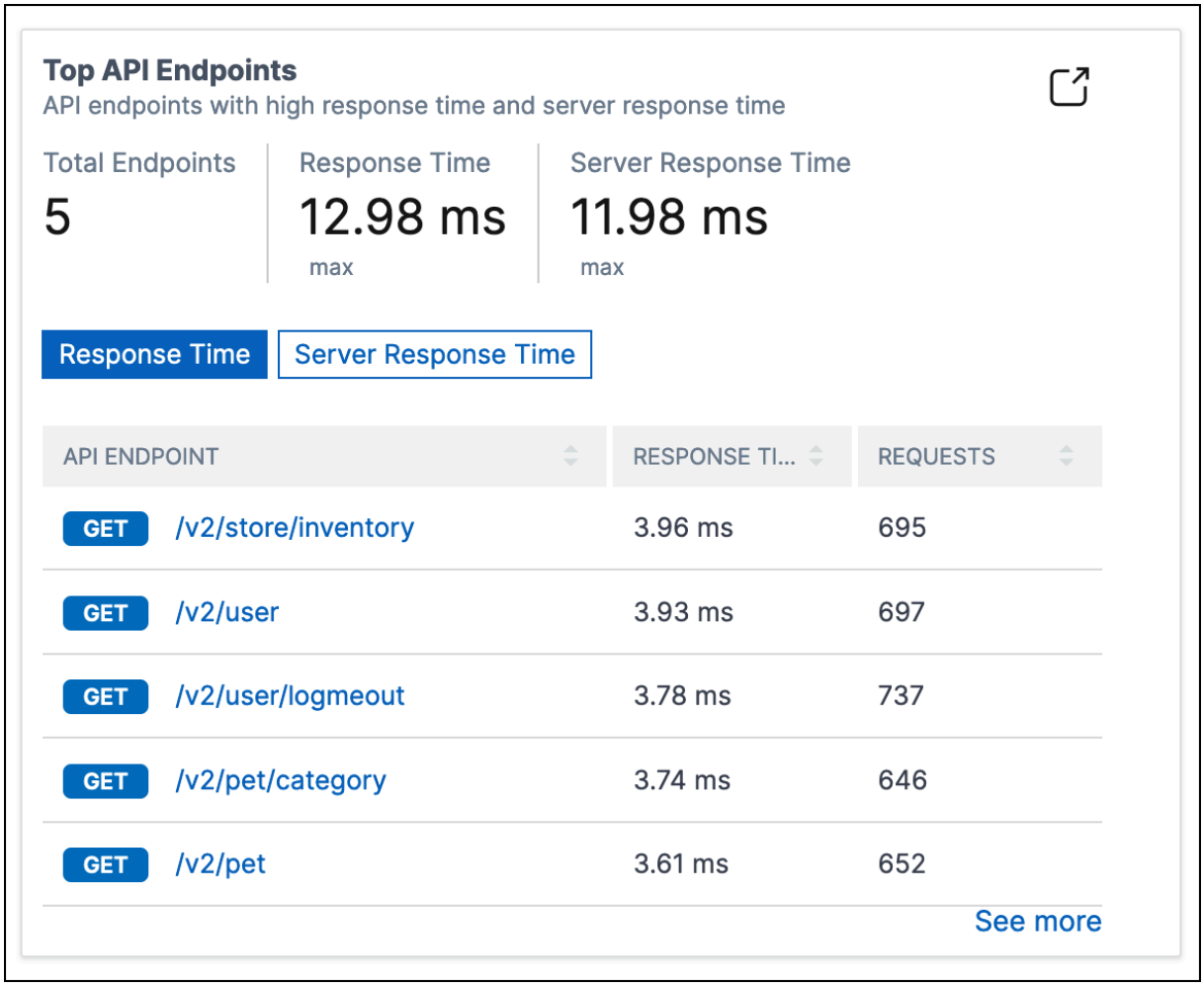
Navegue por API Analytics para ver información específica sobre lo siguiente:

- Principales puntos de enlace de API en una instancia
- APIs más accedidas
- Geolocalización de un punto final
- Estado de respuesta HTTPS
- Tendencia de solicitudes API
- Consumo de ancho de banda de un terminal
- Errores y uso de SSL

Ver los principales puntos de enlace de la API en una instancia

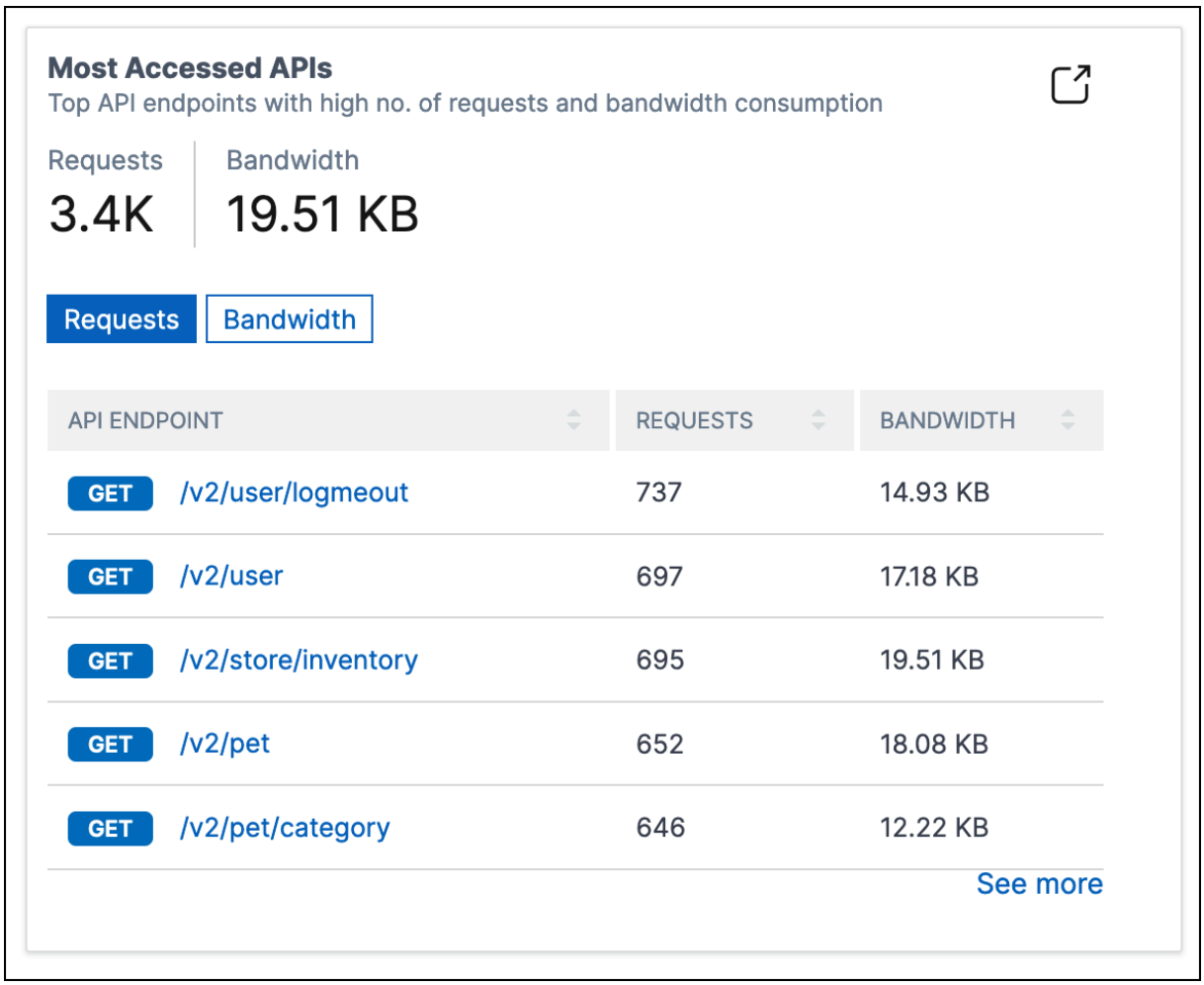
La página **de análisis de la API** muestra los principales puntos de enlace que tienen un tiempo de respuesta alto. Si quieres ver puntos de enlace similares de una instancia, selecciona una instancia de **las instancias de API**.

El **recuadro Principales puntos de conexión de la API** muestra los puntos de enlace que tienen un tiempo de respuesta elevado de aplicaciones y servidores.



Ver las API más accedidas

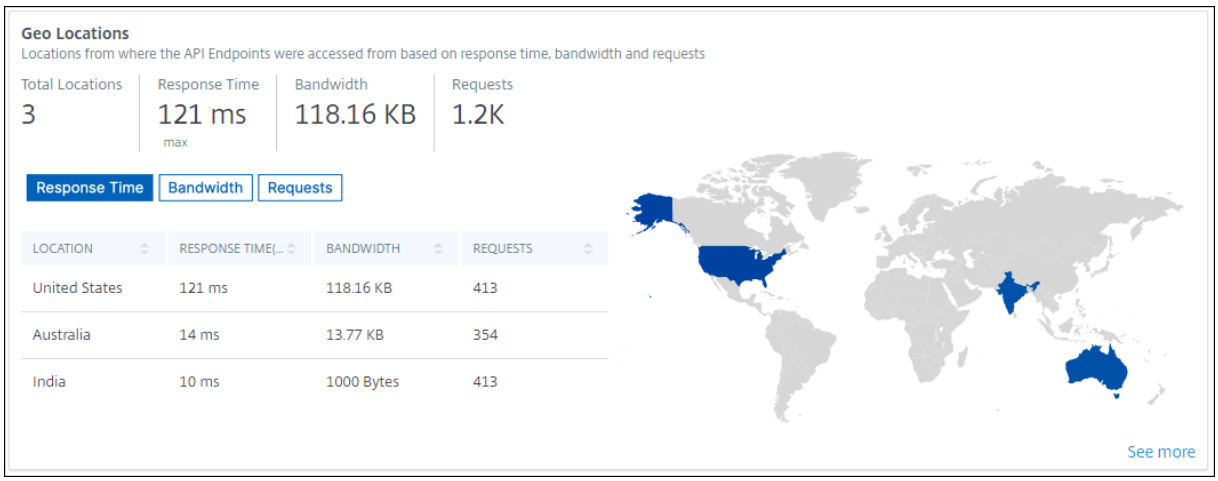
En **API Analytics**, selecciona una instancia de API de entre las instancias de API. El mosaico de **las API más accedidas** muestra los puntos de enlace principales que tienen más solicitudes y ancho de banda.



Ver la geolocalización de un punto final

1. En **API Analytics**, selecciona cualquiera de las siguientes opciones:
   - Seleccione una instancia de **las instancias de API** para ver las ubicaciones desde las que los puntos finales de la instancia seleccionada recibieron las solicitudes.
   - Seleccione un punto final de los **puntos de conexión de la API** para ver las ubicaciones desde las que el terminal recibió las solicitudes.
2. En **Rendimiento y uso**, aparece el **icono de ubicaciones geográficas**.

   Puede ordenar las ubicaciones según el tiempo de respuesta, el ancho de banda y las solicitudes.

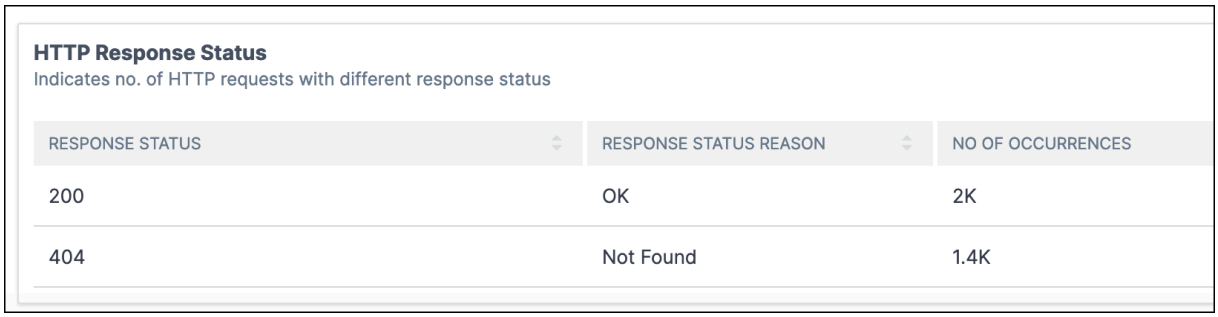


Ver el estado de la respuesta HTTPS

El mosaico **Estado de respuesta HTTPS** muestra el estado de la respuesta con sus motivos y ocurrencias. Puede ver el estado de la respuesta de HTTPS de una de las siguientes maneras:

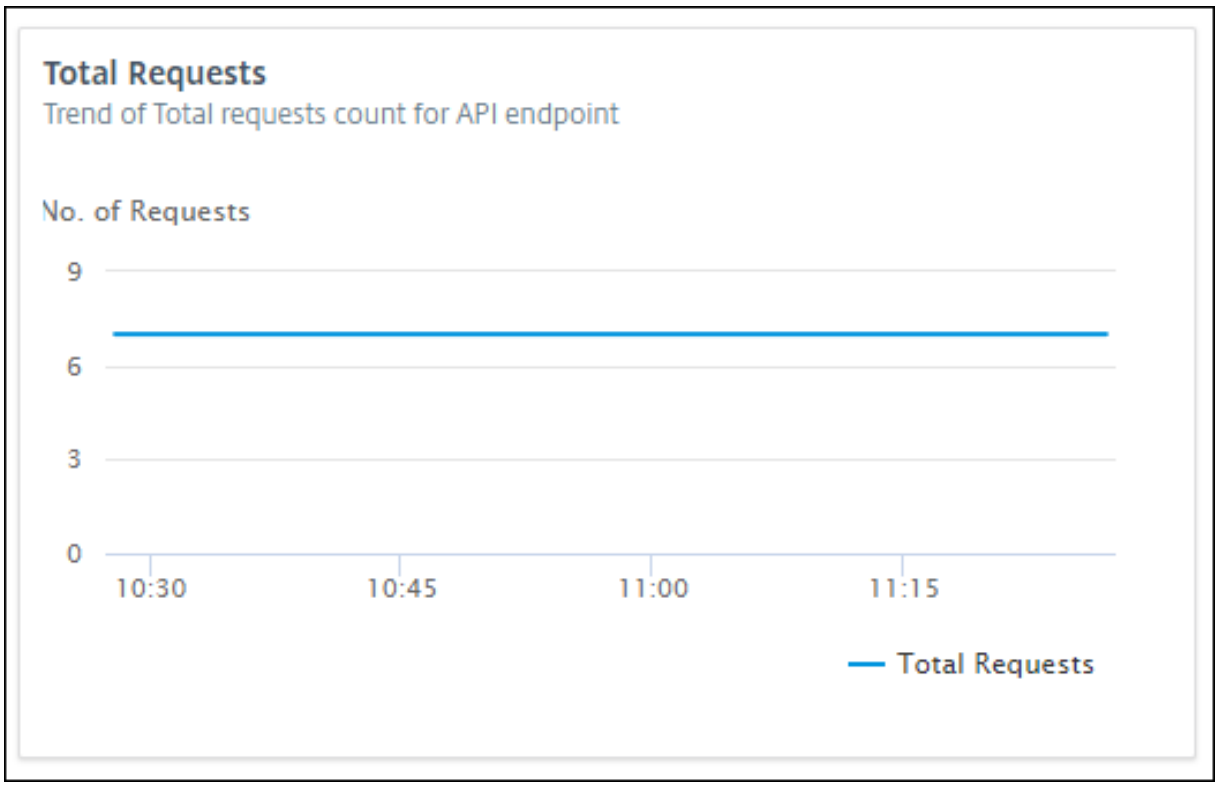
- Seleccione una instancia de las **instancias de API**.
- Seleccione un punto final de los **extremos de la API**.

Este mosaico aparece en la ficha **Rendimiento y uso**.

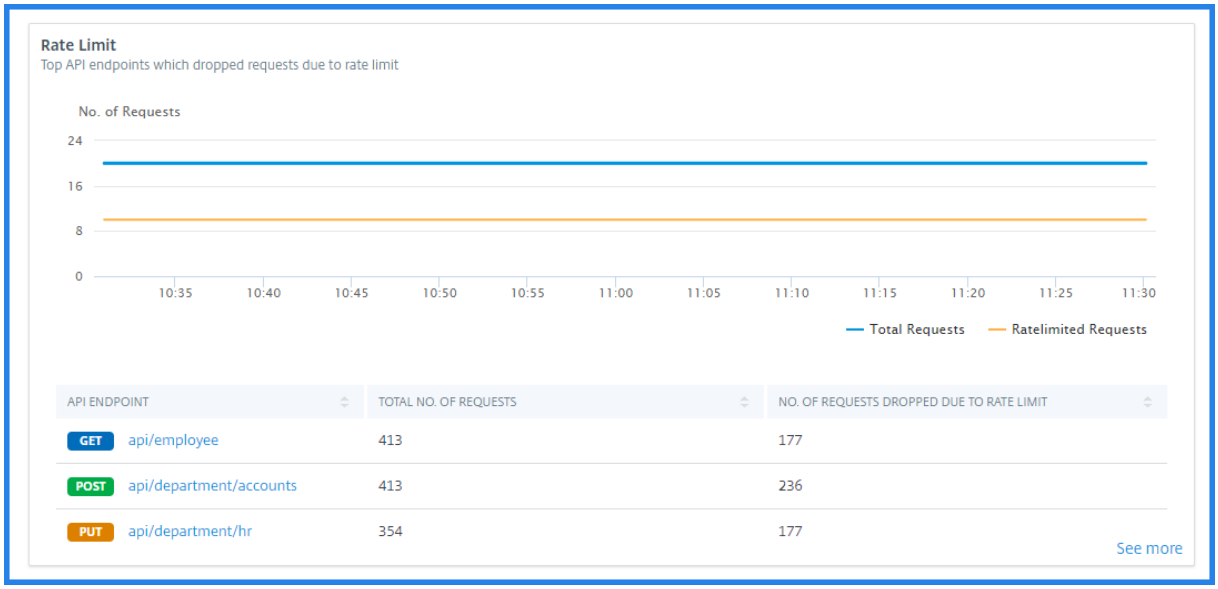


Ver tendencia de las solicitudes de API

Seleccione un punto final de los **extremos de la API**. En **Rendimiento y uso**, el **recuadro Total de solicitudes** muestra la tendencia del recuento total de solicitudes recibidas por un punto final.



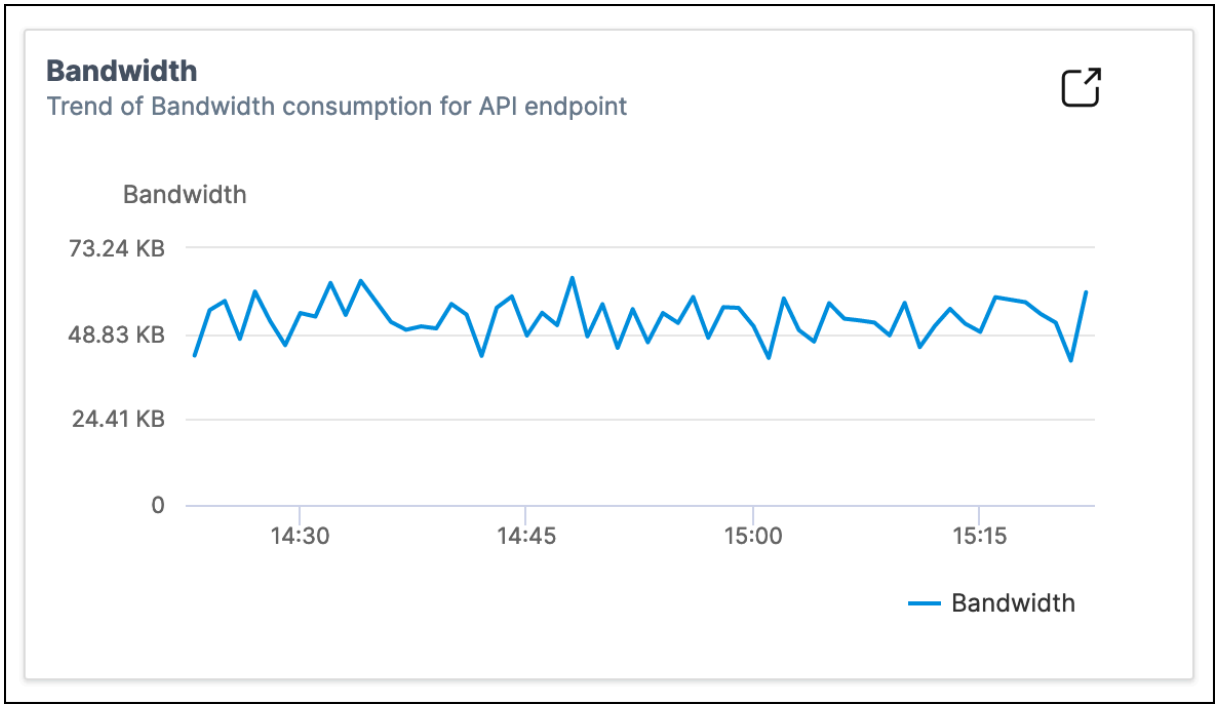
Si quieres ver la tendencia de las solicitudes rechazadas debido a un límite de velocidad, selecciona una instancia de **las instancias de API**. En **Seguridad**, el recuadro **Límite de velocidad** muestra la tendencia de las solicitudes descartadas. También muestra la tendencia del total de solicitudes recibidas por un punto final.



Con esta comparación, puede determinar cuántas solicitudes se descartan debido a un límite de velocidad entre el total de solicitudes.

Ver el consumo de ancho de banda de un

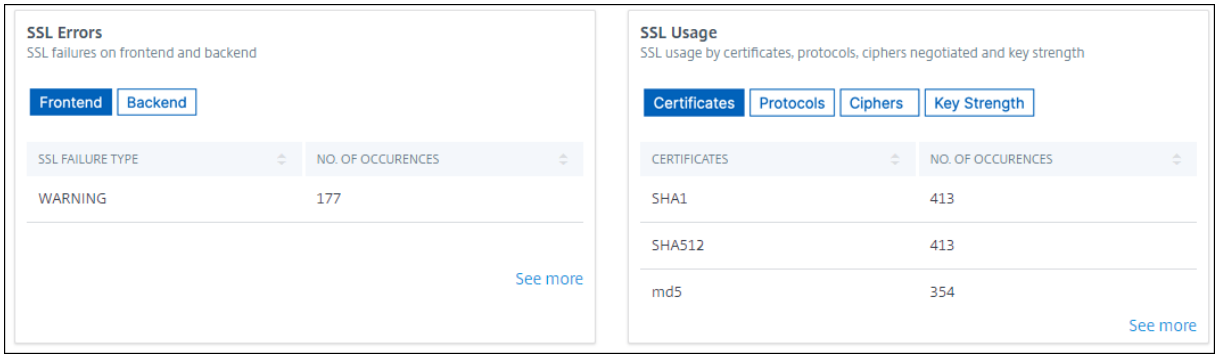
Para ver la tendencia del consumo de ancho de banda de un punto final, seleccione un punto final de los puntos de enlace de la API. El mosaico **Ancho de banda** muestra un gráfico de consumo de ancho de banda



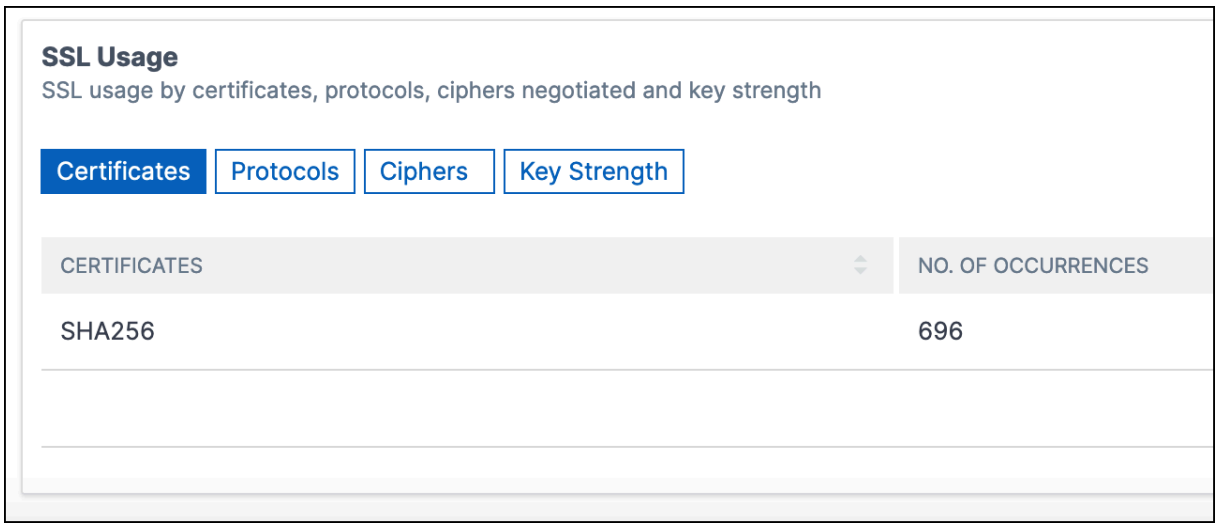
Ver los errores y el uso de SSL

Seleccione una instancia de las **instancias de API**. En **Seguridad**, aparecen los siguientes mosaicos:

- **Errores de SSL**: muestra los errores de SSL que se produjeron en los servidores de clientes y aplicaciones
- **Uso de SSL**: muestra los certificados SSL, los protocolos, el cifrado y las fortalezas clave con sus ocurrencias.



Para ver el uso de SSL en un punto final, seleccione un punto final de los puntos de enlace de la API. El icono **Uso de SSL** aparece en la ficha **Seguridad**.



Descubra los puntos finales de API

July 17, 2024

Puede ver los dispositivos de punto final de API detectados que se encuentran en su organización mediante API Security. NetScaler Console descubre los puntos finales de la API en función del tráfico de API recibido en las instancias y despliegues de API de NetScaler.

En NetScaler Console, la página **Seguridad > Seguridad de API > Detección de API** muestra los puntos finales de API descubiertos.

- **Servidores**virtuales : la pestaña **vServer** muestra los servidores virtuales de las instancias de NetScaler. Los servidores virtuales aparecen en esta ficha cuando reciben las solicitudes de API durante el período especificado.
- **Implementaciones**de API : en esta pestaña se muestran las implementaciones de API que se implementan desde NetScaler Console mediante una definición de API. Esta ficha descubre los extremos de la API cuando las implementaciones de API reciben las solicitudes de API durante el período especificado. Para agregar e implementar una definición de API, consulte Agregar una definición de API e Implementar definiciones de API.

> **Nota:**
>
> - Asegúrese de configurar el análisis y habilitar Web Insights en servidores virtuales. Consulte Habilitar Web Insight en las instancias de API.

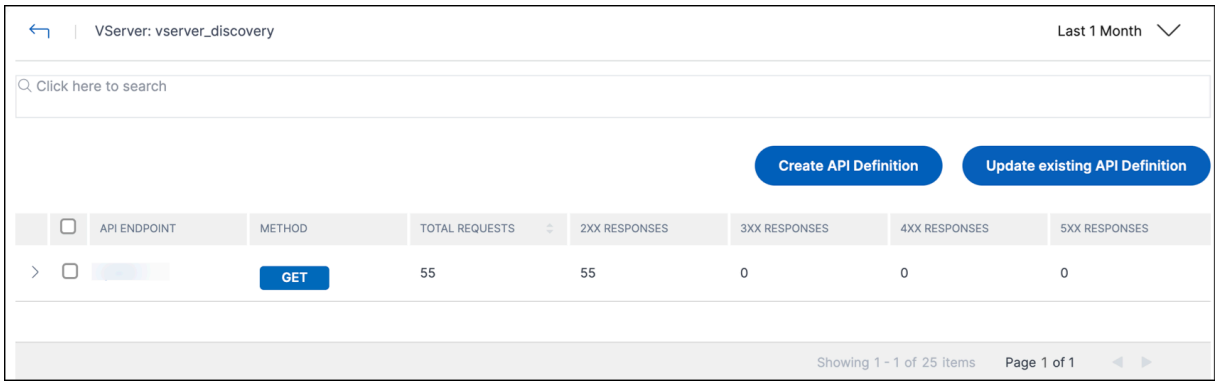
> - Solo puede agregar directivas a los extremos de API que se descubren en la ficha **Implementaciones de API**.

Ver puntos finales de API

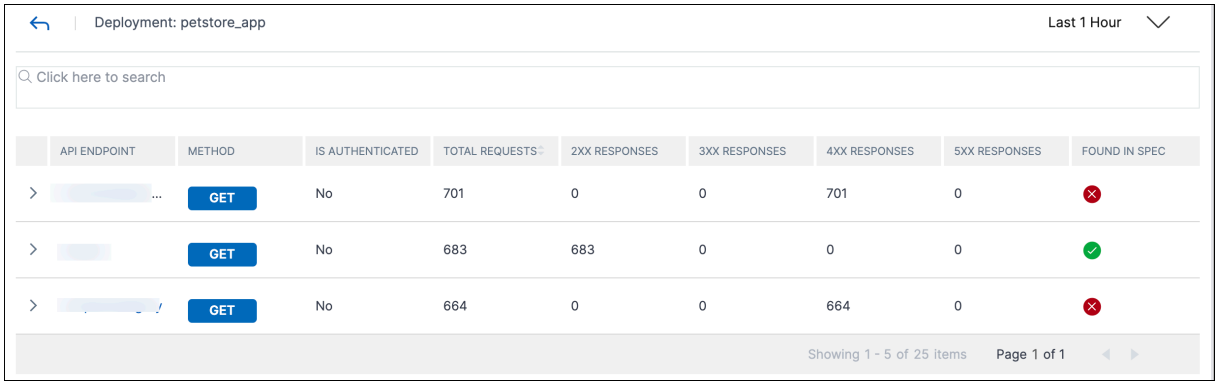
En **API Discovery** , al seleccionar un servidor virtual o una implementación de API, la GUI de NetScaler Console muestra los puntos finales de la API y sus detalles, como:

- **Método** - Muestra el método utilizado en un extremo API. Por ejemplo, los métodos GET y POST.
- **Total de solicitudes** - Muestra el recuento de solicitudes API en el extremo de la API.
- **Estados de respuesta**: muestra el recuento de cada estado de respuesta. Por ejemplo, 2xx, 3xx, 4xx, y 5xx.
- **Encontrado en la especificación**: esta columna aparece solo para implementaciones de API. A veces, las API internas que no forman parte de la definición de la API pueden recibir tráfico del exterior. Esta columna le ayuda a identificar si el extremo de API y el método observado forman parte de la definición de API.

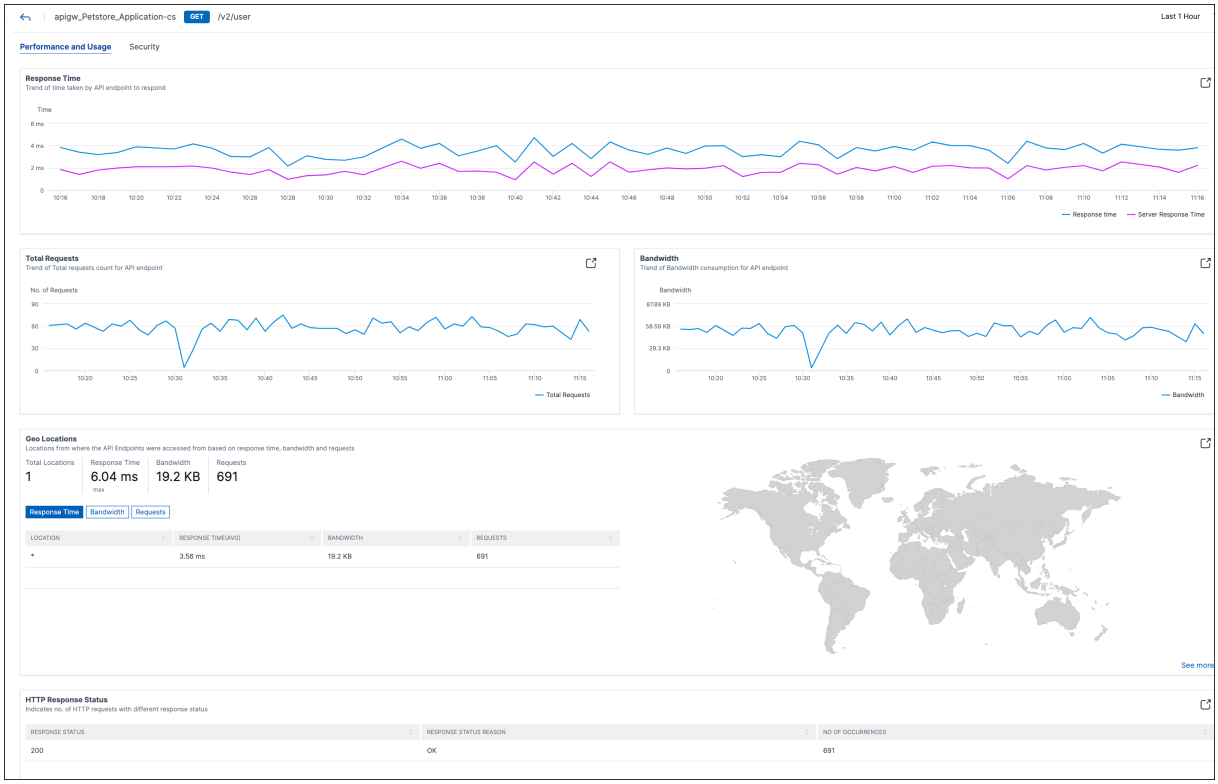
Los puntos finales de la API de un servidor virtual están disponibles de la siguiente manera:



Los puntos finales de API en las implementaciones de API están disponibles de la siguiente manera:



También puede seleccionar el punto final de API requerido para ver su informe de análisis detallado.

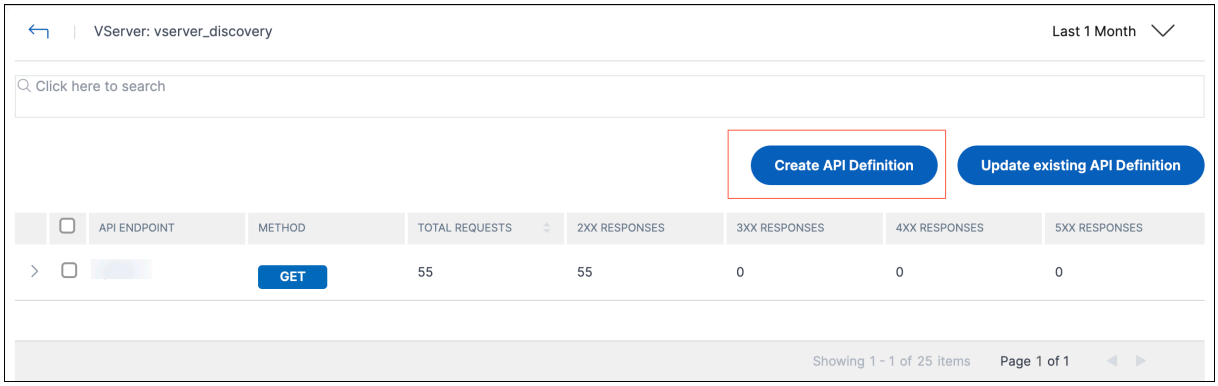


Para obtener más información sobre cada sección, consulte Ver análisis de la API.

Cree definiciones de API a partir de puntos de enlace de API descubiertos

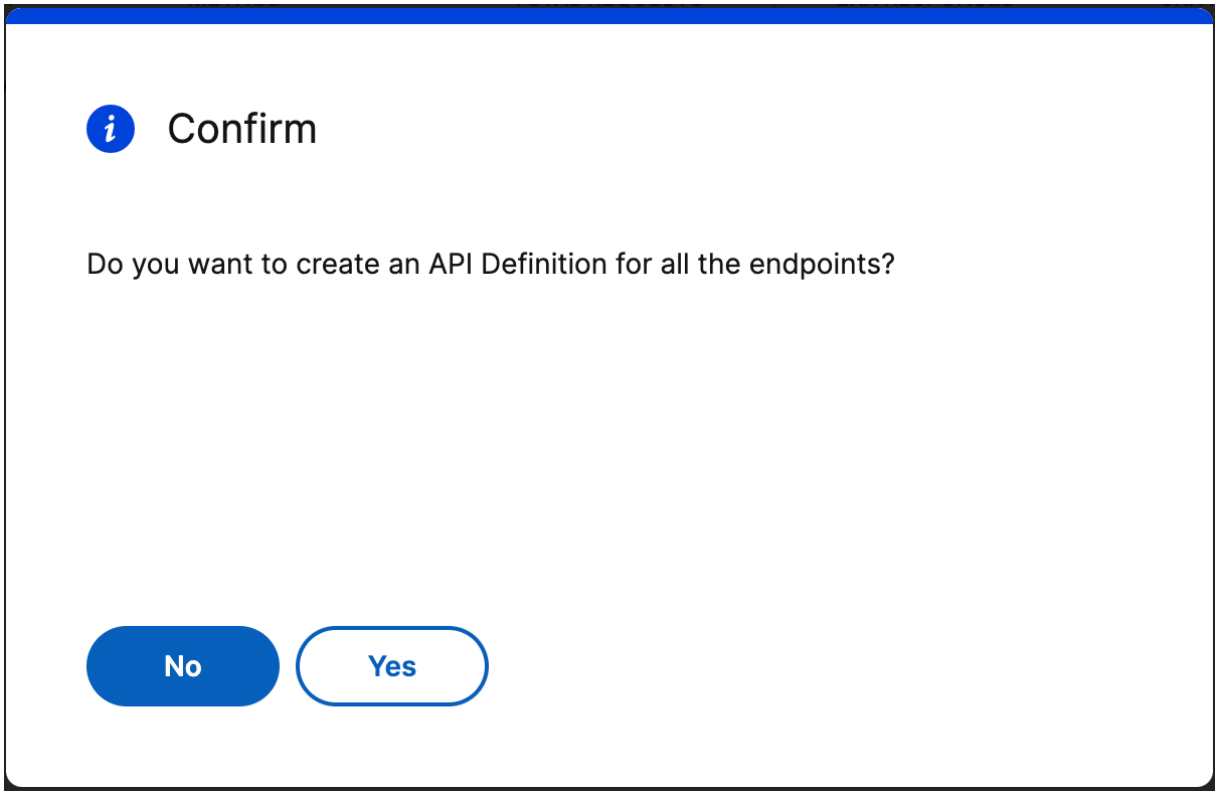
Para crear definiciones de API a partir de puntos finales de API descubiertos (recursos y métodos de la API):

1. Vaya a **Seguridad > API Security > Descubrimiento de API** para ver la lista de servidores virtuales e implementaciones de API.
2. Haga clic en cualquier servidor virtual de la ficha **vServers**.
3. La página del servidor virtual muestra la lista de puntos finales detectados. Seleccione cualquier punto final y haga clic en **Crear definición de API**.



Nota:

Si no selecciona ningún punto final y hace clic en **Crear definición de API**, aparecerá una ventana emergente para confirmar si quiere crear una definición de API para todos los puntos de conexión. Haga clic en **Sí** para crear la definición de API con todos los puntos finales; de lo contrario, haga clic en **No**.

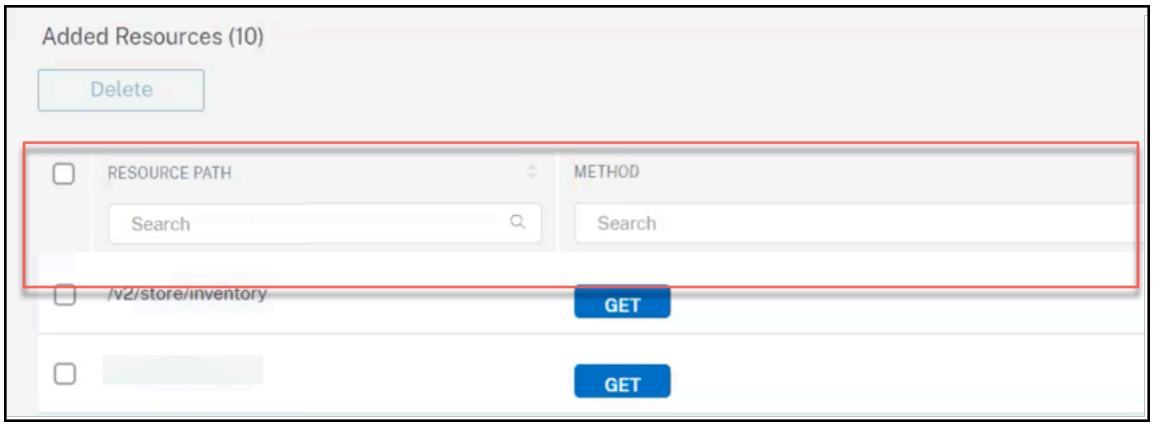


1. En **Crear definición de API**, especifique lo siguiente:
   - **Nombre**: Nombre para la definición de API.
   - **Definición de API**: Una definición debe incluir título, versión, ruta base y host. Puede especificar un nombre de dominio o una dirección IP en el campo **Host**.

- **Recursos de API**: Agregue varios recursos API a su definición. Cada recurso tiene una ruta de acceso y un método soportado.

2. Haga clic en **Crear definición** para crear la definición de API.

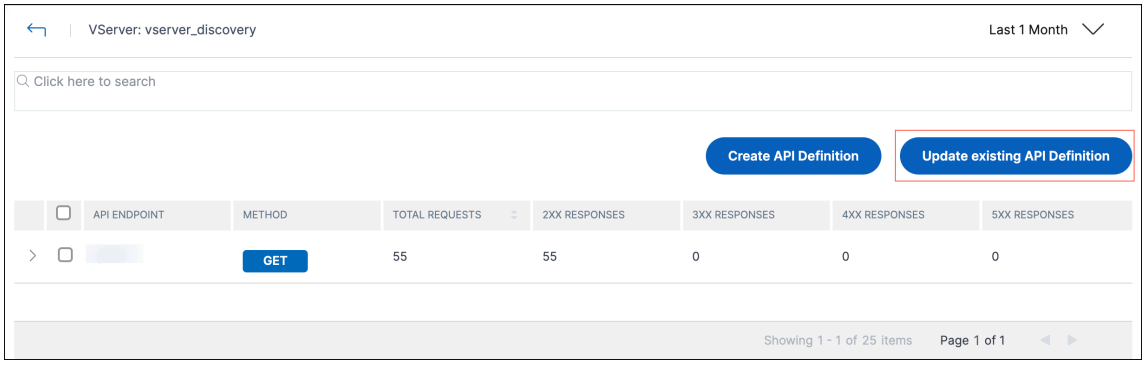
> **Nota:**
>
> Si quieres modificar una ruta de recursos de API antes de agregarla a la definición de API, usa la función de clasificación o búsqueda de los recursos de API en la pantalla de definición de API.
>
> Por ejemplo, considere un recurso de API denominado "/api/products/123-3243-2344334/reviews" donde el segmento de ruta "123-3243-2344334"es un identificador de producto variable. Ahora puede ordenar los recursos de la API, agregar la ruta del recurso como "/api/products/{id}/reviews"y eliminar todos los extremos de la API con identificadores como "/api/products/123-3243-2344334/reviews".



Actualizar una definición de API existente con puntos finales de API descubiertos

Para actualizar una definición de API existente con puntos finales de API (recursos y métodos de API):

1. Vaya a **Seguridad > API Security > Descubrimiento de API** para ver la lista de servidores virtuales e implementaciones de API.
2. Haga clic en cualquier servidor virtual de la ficha **vServers**.
3. La página del servidor virtual muestra la lista de puntos finales detectados. Seleccione el punto final que quiere agregar a una definición de API existente. Haga clic en **Actualizar la definición de API existente**.



4. En la lista desplegable **Seleccione una definición de API existente**, seleccione la definición de API que quiere actualizar. Haga clic en **Actualizar definición**.
5. Aparece la página **Actualizar la definición de la API existente**. La sección **Recursos de la API** muestra las siguientes tablas:
   - **Recursos adicionales**: Los puntos finales de la API que seleccionó.
   - **Recursos existentes**: Los puntos finales de la API ya están disponibles en la definición de la API.

   > **Nota:**
   >
   > Si el mismo punto final de la API está disponible en **Recursos agregados** y **Recursos existentes**, el punto final se agrega solo una vez a la definición de la API.

6. Haga clic en **Actualizar definición**.

Anular una instancia de API

January 26, 2024

Puede usar la opción Undeploy cuando quiera eliminar la configuración de la instancia de API de una instancia de NetScaler, pero mantener los objetos de la instancia de API en NetScaler Console como borradores. Esta acción establece el estado de implementación en En borrador. Además, solo se puede aplicar a las configuraciones de instancias de API implementadas.

> **Importante:**
>
> - Antes de anular la implementación de una API, asegúrese de que todas las directivas de API asociadas no estén implementadas o eliminadas. Consulte Anular la implementación de una directiva de API.
> - Antes de anular la implementación de un proxy de API, asegúrese de que todas las imple-

> mentaciones de API asociadas no estén implementadas o eliminadas. Consulte Anular la implementación de una API.

Anular una directiva de API

Siga los pasos para anular la implementación de una directiva de API:

1. En **Seguridad > Seguridad de API > Directivas**, seleccione la directiva cuya implementación quiere anular.
2. Haga clic en **Anular implementación**.

Esta acción establece el **estado de la directiva** como En borrador.

Anular la implementación de una API

Siga los pasos para anular la implementación de una API:

1. En **Seguridad > Seguridad de API > Implementaciones de API**, seleccione la implementación de API cuya implementación quiere anular.

   > **Nota:**
   >
   > Asegúrese de anular la implementación o eliminación de todas las directivas asociadas a la implementación seleccionada.

2. Haga clic en **Anular implementación**.

Esta acción establece el **estado de implementación** como En borrador.

Anular la implementación de un proxy API

Siga los pasos para anular la implementación de un proxy de API:

1. En **Seguridad > Seguridad de API > Proxies de API**, seleccione el proxy de API cuya implementación quiere anular.

   > **Nota:**
   >
   > Puedes compartir un proxy de API con diferentes implementaciones de API. Por lo tanto, asegúrese de que todas las implementaciones asociadas al proxy seleccionado no estén implementadas o eliminadas.

2. Haga clic en **Anular implementación**.

Esta acción establece el **estado del proxy** como En borrador.

Utilice las API para gestionar la seguridad de las API

January 26, 2024

Puede acceder a las API para crear, configurar e implementar una seguridad de API.

> **Nota:**
>
> Para saber cómo usar las API de seguridad de las API para configurar la función, consulta la documentación de la API de Nitro.

	Pasos	URL del recurso
1	Crear una definición de API	`https://adm.cloud.com/{ customerid } /apisec/nitro/v1/config/apidefs`
2	Agregar un proxy de API	`https://adm.cloud.com/apiproxies`
3	Implementar una instancia de API mediante el proxy de la API	`https://adm.cloud.com/apiproxies/{ customerid } /deployments`
4	Agregar directivas de API	`https://adm.cloud.com/{ customerid } /apisec/nitro/v1/config/policies/{ id }`

Cada directiva de API tiene un objeto `config_spec` diferente. Es un objeto opaco que contiene un diccionario JSON para configurar un `policytype` con valores específicos.

En este objeto, puede seleccionar un recurso de API y sus métodos mediante las siguientes opciones:

- `api-resource-paths` - Especifique las rutas y los métodos de los recursos de la API que se definen en una definición de API.

  Ejemplo:

  ```
  {

  "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
      "get": true,
      "post": false,
      "put": false,
      "delete": false
   }
  ```

- `custom-rules` - Especifique las rutas y los métodos de los recursos de la API personalizados que pueden no existir en una definición de API.

  Ejemplo:

  ```
  {

  "endpoints": ["/pet/categories", "/pet/findByName"],
      "get": true,
      "post": false,
      "put": false,
      "delete": false
   }
  ```

Con esta configuración, la directiva filtra las solicitudes de tráfico entrantes que coinciden con las rutas de recursos de API especificadas.

Para obtener información sobre cada tipo de directiva `config_spec`, consulte los ejemplos de API para los tipos de directivas.

Ejemplos de API para tipos de directivas

En esta sección se describen los tipos de directivas de API compatibles y su configuración:

- Límite de tarifa
- OAuth
- Autenticación
- Sin autenticación
- Bot
- WAF
- Reescritura de encabezado
- Reescritura de ruta de URI
- Autorización
- Negar

Límite de tarifa

A continuación se muestra un ejemplo de configuración para el tipo de directiva `Ratelimit`. Especifique la siguiente configuración en el objeto `config_spec`:

```
{

    "policytype": "Ratelimit",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "threshold": "10",
        "timeslice": "20000",
        "limittype": "BURSTY",
        "api-respondertype": "DROP",
        "header_name": "x-api-key",
        "per_client_ip": true
     }
 ,
    "order_index": 1,
    "policy_name": "ratelimit_policy"
 }
```

Para obtener más información sobre cada atributo, consulte Directiva de límites de tarifas.

OAuth

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva `JWT Auth validation`. Especifique la siguiente configuración en el objeto `config_spec`:

```
{

    "policytype": "JWT Auth Validation",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
```



```
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
,
        "custom-rules": {
 }
,
        "jwks-uri": "https://uri.petstore.com",
        "issuer": "https://issuer.petstore.com",
        "audience": "petstore",
        "introspect-uri": "https://introspect.uri.com",
        "clientid": "client",
        "clientsecret": "clientsecret",
        "claims-to-save": ["scope", "scope2"],
        "allowed-algorithms": {

            "hs256": true,
            "rs256": true,
            "rs512": true
         }

     }
,
   "order_index": 2,
   "policy_name": "Jwt_auth_policy"
}
```

Para obtener más información sobre cada atributo, consulta la directiva de OAuth

Autenticación

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva `BasicAuth` :

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
               "],
            "get": true,
            "post": true,
            "put": false
         }
,
        "custom-rules": {
```



```
15    }
16
17        }
18   ,
19       "order_index": 3,
20       "policy_name": "Auth_BaSIC",
21       "policytype": "BasicAuth"
22   }
```

Para obtener más información sobre cada atributo, consulte Directiva de autenticación básica.

Sin autenticación

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva `NoAuth`:

```
1  {
2
3      "config_spec": {
4
5          "api-resource-paths": {
6
7              "delete": false,
8              "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                   "],
9              "get": true,
10             "post": false,
11             "put": false
12          }
13   ,
14         "custom-rules": {
15    }
16
17       }
18   ,
19      "order_index": 4,
20      "policy_name": "no_auth_policy",
21      "policytype": "NoAuth"
22   }
```

Bot

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva `Bot`:

```
1  {
2
3      "config_spec": {
4
5          "api-resource-paths": {
6
7              "delete": false,
```



```
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": false,
            "post": false,
            "put": false
         }
,
        "bot-prof-name": "apisec_test_profile",
        "custom-rules": {
 }

    }
,
   "order_index": 5,
   "policy_name": "bot_policy",
   "policytype": "Bot"
}
```

Para obtener más información sobre cada atributo, consulte Directiva de bots.

WAF

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva WAF:

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": false,
            "post": false,
            "put": false
         }
,
        "waf-prof-name": "apisec_waf_profile",
        "custom-rules": {
 }

    }
,
   "order_index": 6,
   "policy_name": "waf_policy",
   "policytype": "WAF"
}
```

Para obtener más información sobre cada atributo, consulte la directiva de WAF.

Reescritura de encabezado

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva de reescritura de encabezados. Especifique esta configuración en el objeto `config_spec`:

```
{

    "policytype": "Header Rewrite",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "rewrite-policy-header-field-name": "org",
        "rewrite-policy-header-field-val": "Citrix",
        "rewrite-policy-header-field-new-val": "Citrite"
     }
 ,
    "order_index": 7,
    "policy_name": "header_rewrite_pol"
 }
```

Para obtener más información sobre cada atributo, consulte Directiva de reescritura de encabezados.

Reescritura de ruta de URI

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva de reescritura de rutas de URI:

```
{

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/store/order", "/store/inventory"],
            "delete": false,
            "get": true,
            "post": true,
```



```
            "patch": false,
            "put": false
         }
,
        "custom-rules": {

            "delete": false,
            "endpoints": [],
            "get": false,
            "post": false,
            "patch": false,
            "put": true
         }
,
        "path-rewrite-params": [
        {

            "insert-segment-position": "beginning",
            "new-path-value": "v3",
            "old-path-value": "v2",
            "action-type": "replace path segment"
         }
,
        {

            "insert-segment-position": "beginning",
            "new-path-value": "begin",
            "action-type": "insert path segment"
         }
,
        {

            "insert-segment-position": "end",
            "new-path-value": "end",
            "action-type": "insert path segment"
         }
,
        {

            "insert-segment-position": "before",
            "new-path-value": "before",
            "old-path-value": "store",
            "action-type": "insert path segment"
         }
,
        {

            "insert-segment-position": "after",
            "new-path-value": "after",
            "old-path-value": "store",
            "action-type": "insert path segment"
         }

```



```
        ]
    }
,
        "order_index": 24,
        "policy_name": "eats_uripathrewrite",
        "policytype": "URI Path Rewrite "
}
```

Para obtener más información sobre cada atributo, consulte la directiva de reescritura de rutas de URI.

Autorización

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva `Authorization`. Especifique la siguiente configuración en el objeto `config_spec`:

```
{

    "policytype": "Authorization",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
,
        "custom-rules": {
 }
,
        "claims": [{

            "name": "scope",
            "values": ["value1", "value2"]
         }
]
    }
,
    "order_index": 8,
    "policy_name": "authorization"
}
```

Para obtener más información sobre cada atributo, consulte Directiva de autorización.

Negar

A continuación se muestra un ejemplo de configuración de API para el tipo de directiva `Deny`. Especifique la siguiente configuración en el objeto `config_spec`:

```
{

    "policytype": "Deny",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "api-denytype": "RESPONDWITH"
     }
 ,
    "order_index": 9,
    "policy_name": "deny_policy"
 }
```

En `api-denytype`, puede especificar uno de los siguientes valores:

- RESPONDWITH
- RESET

Para obtener más información sobre cada atributo, consulte Regla de denegación.

Cree perfiles WAF y BOT con StyleBooks

January 26, 2024

Cuando puede seleccionar una directiva para un recurso API en **API Gateway**, permite definir los criterios de selección de tráfico para autenticar una solicitud de API. Además, le permite configurar las directivas de seguridad de la API para el tráfico de la API. Para obtener más información, consulte Seguridad de API .

Puede configurar directivas WAF y BOT en un recurso API. Antes de configurar una política, asegúrese

de crear su perfil en NetScaler Console. Utilice los siguientes StyleBooks predeterminados para crear un perfil:

- API WAF Detection StyleBook
- API BOT Detection StyleBook

Cree un perfil WAF con StyleBooks

Realice lo siguiente para crear un perfil WAF:

1. En NetScaler Console, vaya a **Aplicaciones** > **ConfiguracionesStyleBooks**. Busque el StyleBook escribiendo el nombre como `api-waf-profile`. Haga clic en**Crear configuración**.

   El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.

2. Especifique los valores para los siguientes parámetros:

   - **API WAF nombre de perfil**: un nombre para identificar un perfil WAF.
   - **Tipo de aplicación**: agregue tipos de aplicación al perfil. El perfil WAF admite tipos de aplicaciones JSON y XML.

3. Opcional, habilite **Configuración de seguridad** para especificar comprobaciones de protección HTTP, JSON o XML. También puede especificar una dirección URL de error para NetScaler Web App Firewall. Para obtener más información, consulte Creación de un perfil de Web App Firewall.

4. Seleccione la instancia o grupo de instancias de NetScaler de destino en el que quiere implementar esta configuración.

5. Haga clic en **Crear**.

Para configurar una directiva WAF, consulte Agregar directivas a una implementación de API.

Crear un perfil BOT con StyleBook

Realice lo siguiente para crear un perfil BOT:

1. En NetScaler Console, vaya a **Aplicaciones** > **ConfiguracionesStyleBooks**. Busque el StyleBook escribiendo el nombre como `api-bot-profile`. Haga clic en**Crear configuración**.

   El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.

2. En **Nombre de perfil BOT**, especifique un nombre para identificar un perfil BOT.

3. Opcional, habilite las siguientes opciones según sus requisitos:
    - **Habilitar comprobación de reputación IP**: esta opción identifica la dirección IP que envía solicitudes no deseadas. Puede utilizar la lista de reputación IP para rechazar de forma preventiva las solicitudes que provienen de la IP con mala reputación.
    - **Habilitar firmas BOT**: especifique el nombre de la firma BOT. Bloquea las solicitudes de la firma especificada.
    - **Lista de permitidos**: especifique dirección IPv4 o subred (CIDR). Esta opción permite que el perfil BOT omita las solicitudes de la dirección IPv4 o subred especificada.
    - **Denegar lista**: especifique la dirección IPv4 o subred (CIDR). Esta opción permite que el perfil BOT bloquee solicitudes desde la dirección IPv4 o subred especificada.
4. Seleccione la instancia o grupo de instancias de NetScaler de destino en el que quiere implementar esta configuración.
5. Haga clic en **Crear**.

Para configurar una directiva de BOT, consulte Agregar directivas a una implementación de API.

Aplicaciones

April 10, 2024

La función de análisis y administración de aplicaciones de NetScaler Console le permite supervisar las aplicaciones mediante un enfoque centrado en las aplicaciones. Este enfoque le ayuda a:

- Comprobar la puntuación y analizar el rendimiento general de las aplicaciones
- Comprobar si hay algún problema que persista con el servidor o el cliente
- Detectar anomalías en los flujos de tráfico de la aplicación y tomar 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 Console.
- Asegúrese de tener una licencia válida para las instancias de NetScaler. Para obtener más información, consulte Licencias.

Descripción general de la aplicación

Las aplicaciones pueden ser:

- Aplicaciones discretas
- Aplicaciones personalizadas
- Aplicaciones de microservicios (k8s_discrete)

Aplicaciones discretas

Todos los servidores virtuales que se descubren en NetScaler Console 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 NetScaler. 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"**.

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

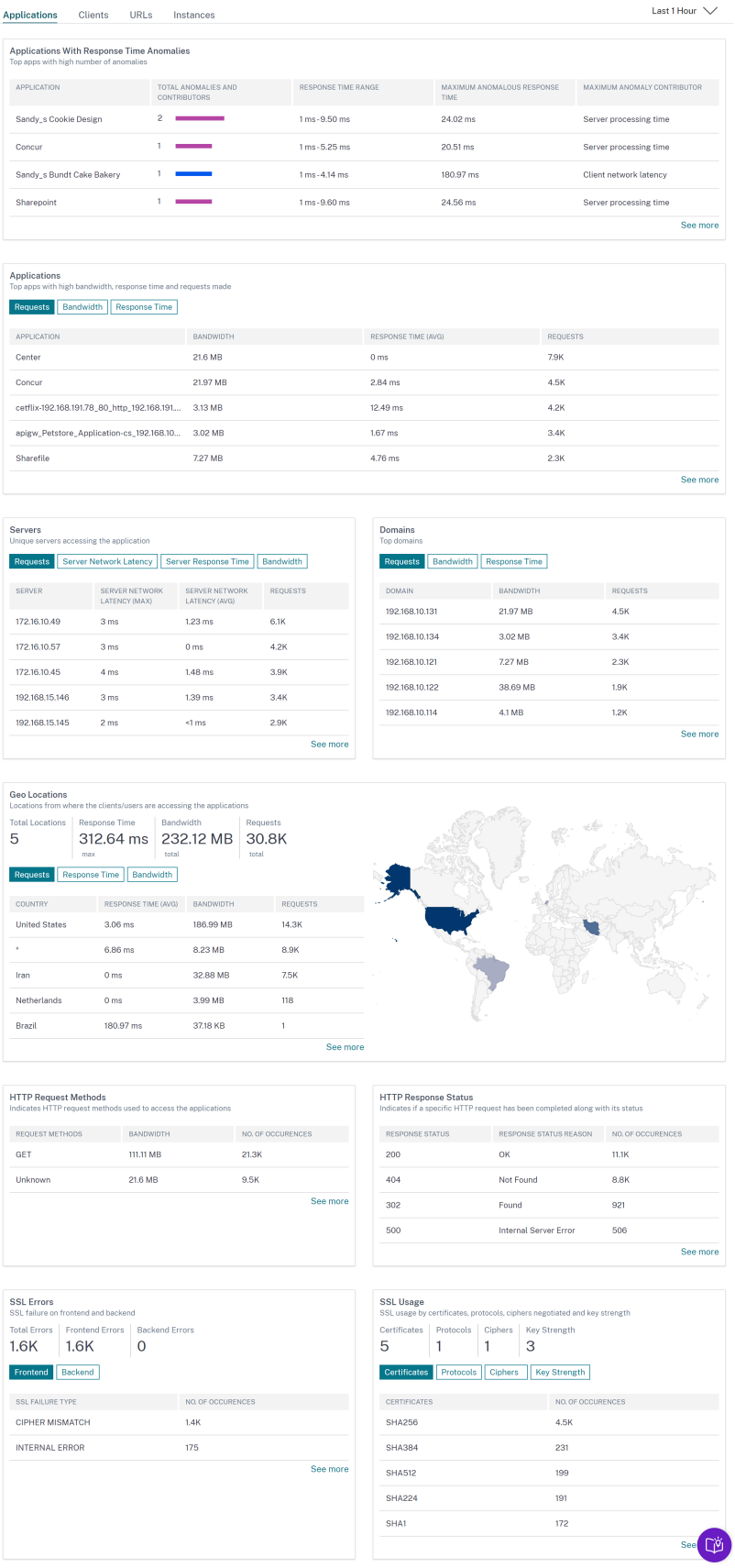
January 26, 2024

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	URLs	Instancias
Aplicación con anomalías de tiempo de respuesta	Clientes	URLs	Métricas de Instancia
Aplicaciones	Ubicaciones geográficas		Aplicaciones
Servidores	Métodos de solicitud HTTP		Dominios
Dominios	Estado de respuesta HTTP		URLs
Ubicaciones geográficas	URLs		Métodos de solicitud HTTP
URLs	Sistema operativo		Estado de respuesta HTTP
Métodos de solicitud HTTP	Exploradores web		Clientes

Aplicaciones	Clientes	URLs	Instancias
Estado de respuesta HTTP	Errores SSL		Servidores
Errores SSL	Uso SSL		Sistema operativo
Uso SSL			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.

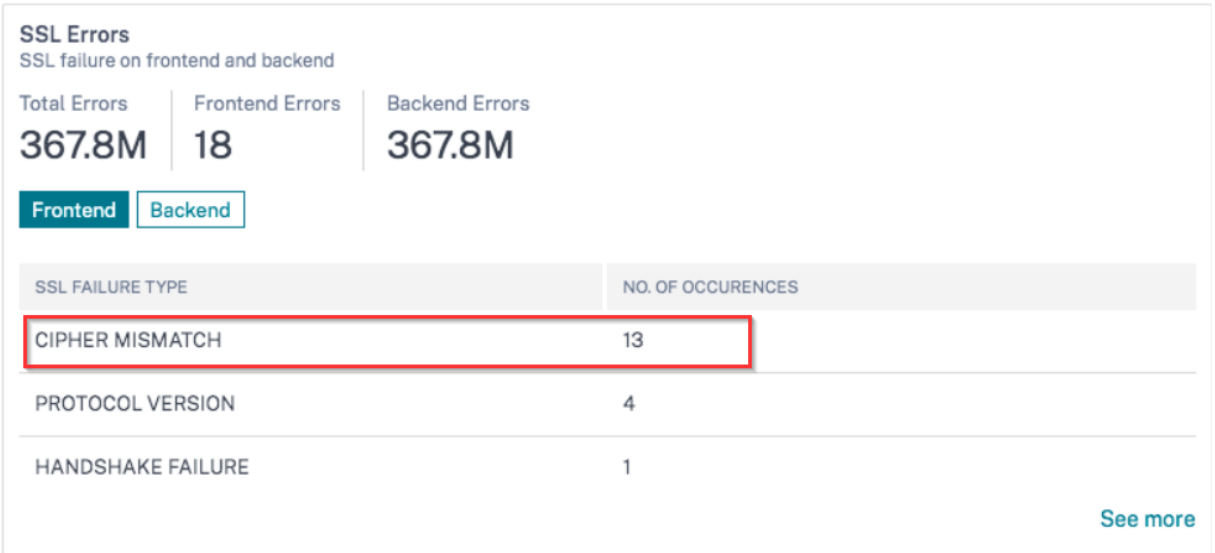
> **Nota**
>
> - A partir de la versión **14.1 a la 1.16** o posterior, al analizar una métrica, la vista de análisis del gráfico de series temporales muestra valores nulos (por ejemplo, 0 ms y 0 solicitudes) durante la duración seleccionada. Antes, si no se recibía tráfico ni transacción durante el 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 estas transacciones, NetScaler Console muestra los valores de RTT como:
>
> - **NA**: aparece cuando la instancia de NetScaler no puede calcular el RTT.
> - **< 1 ms**: aparece cuando la instancia de NetScaler calcula el RTT en decimales entre 0 ms y 1 ms. Por ejemplo, 0,22 ms.

Ver detalles de problemas relacionados con el cifrado

En **Errores de SSL**, puede ver los detalles de los siguientes parámetros de SSL:

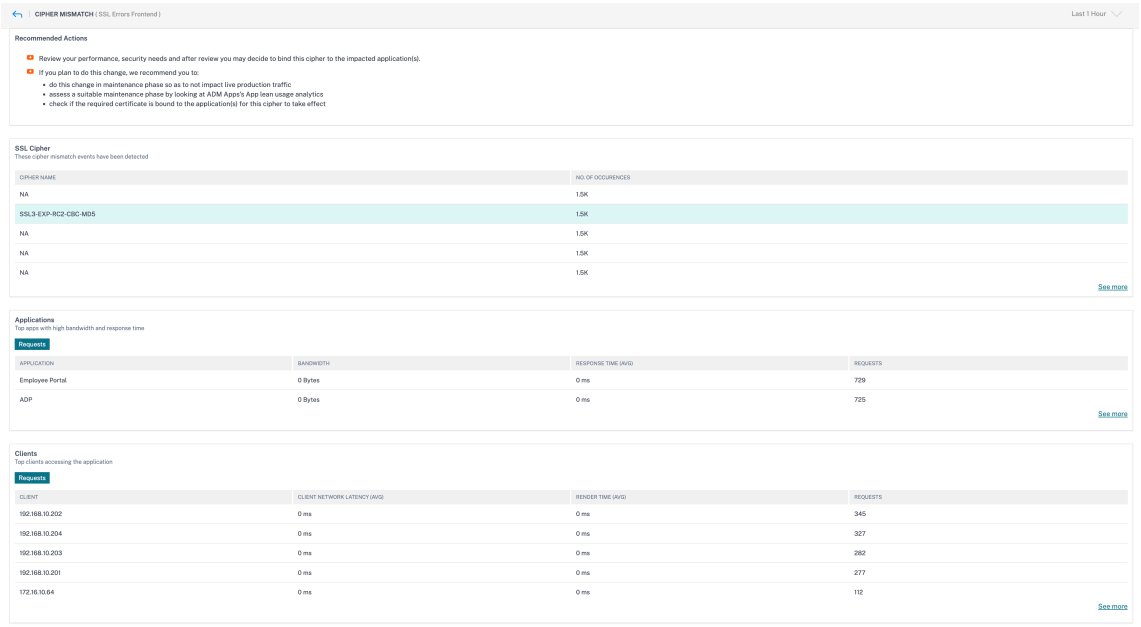
- Desajuste de cifrado
- Cifrados no compatibles

En **Errores de SSL**, haga clic en un parámetro de SSL (códigos que no coinciden o cifrados no compatibles) para ver detalles como el nombre del cifrado SSL, las acciones recomendadas y los detalles de las aplicaciones y los clientes afectados.

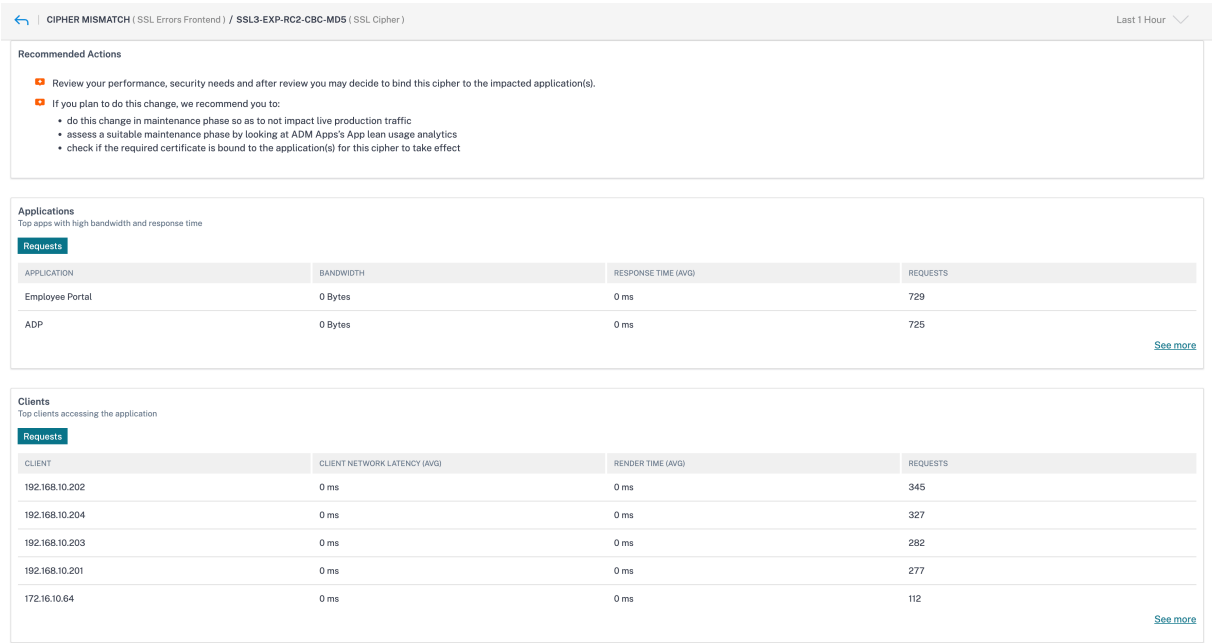


Aparece la página de detalles del parámetro SSL seleccionado. Puede hacer lo siguiente:

- Revise las sugerencias que se proporcionan en las **Acciones recomendadas**.
- Vea los nombres de los cifrados y el número de ocurrencias en el **cifrado SSL**.
- Vea el total de aplicaciones y clientes afectados.



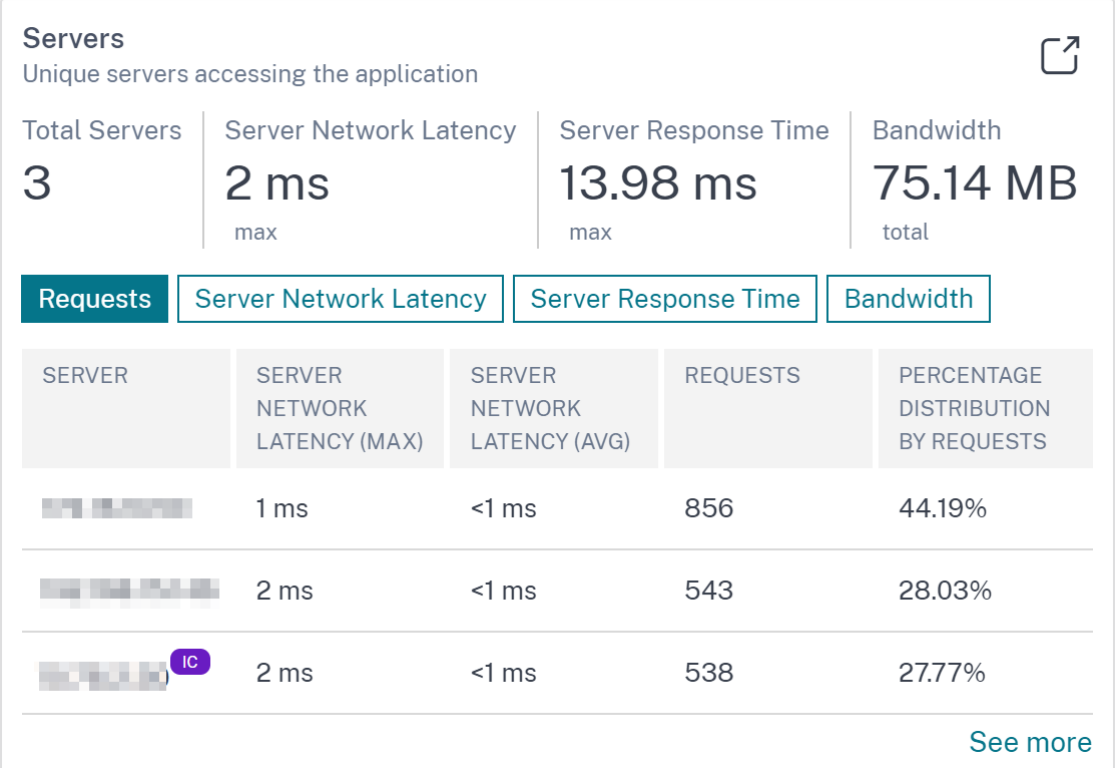
Haga clic en el **nombre del cifrado SSL** para ver las aplicaciones y los clientes afectados por el cifrado SSL seleccionado.



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.

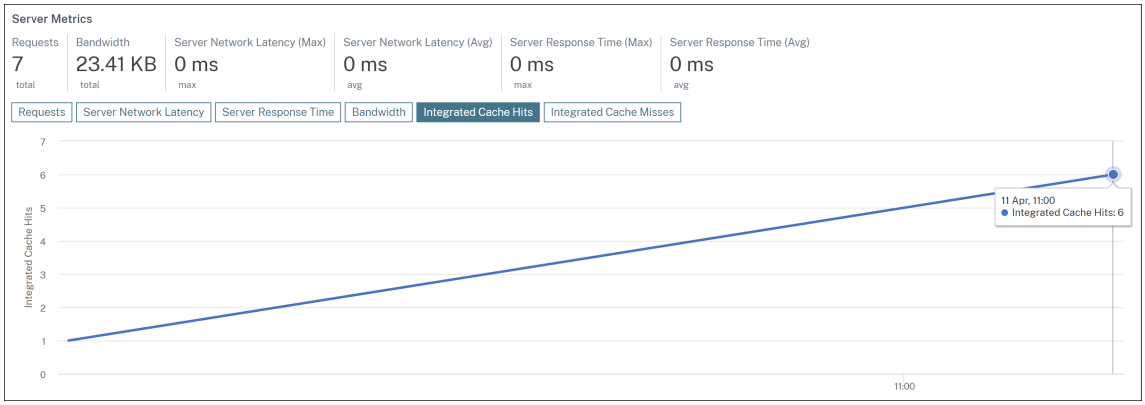
Las solicitudes de caché de integración están visibles actualmente en **Servidores** con una notificación IC junto a la dirección IP del servidor virtual de NetScaler. Todas las demás solicitudes están visibles con la dirección IP del servidor de origen.



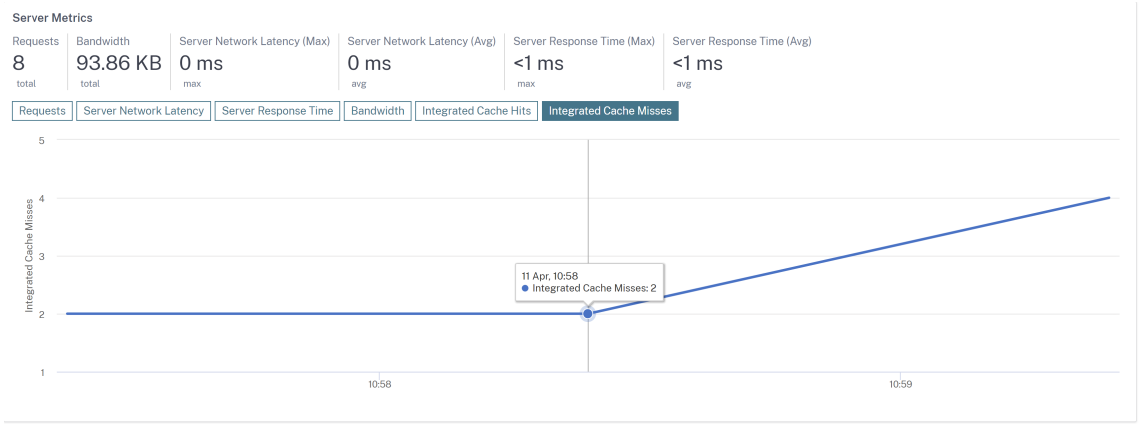
Al analizar un servidor para ver más detalles, **las métricas del servidor muestran las** fichas integradas de aciertos y errores de la memoria caché.

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.



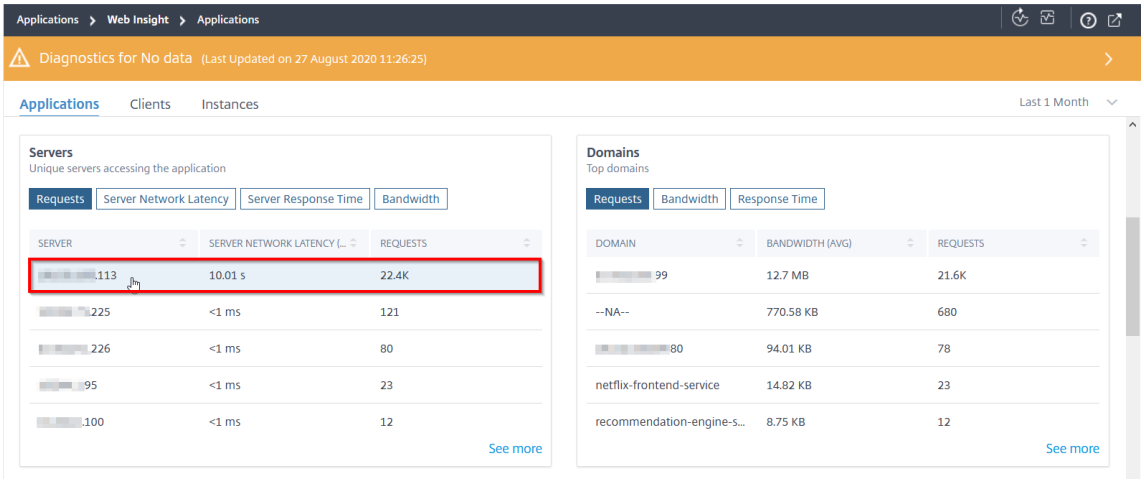
- La ficha **Errores de la memoria caché integrada** le permite ver el total de respuestas que el dispositivo NetScaler proporciona desde el servidor de origen.



Otro caso de uso

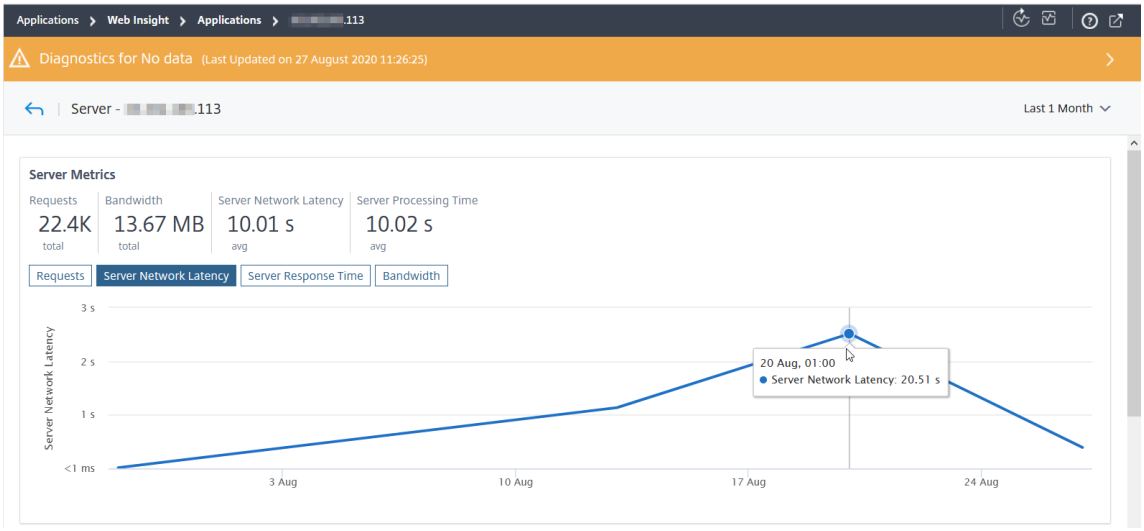
Tenga en cuenta que quiere analizar la latencia de la red del servidor durante un mes y decidir si quiere ampliar o reducir el entorno de producción. Para analizar esto:

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 ampliar el entorno de producción.

Analizar la causa raíz de la lentitud de las aplicaciones

January 26, 2024

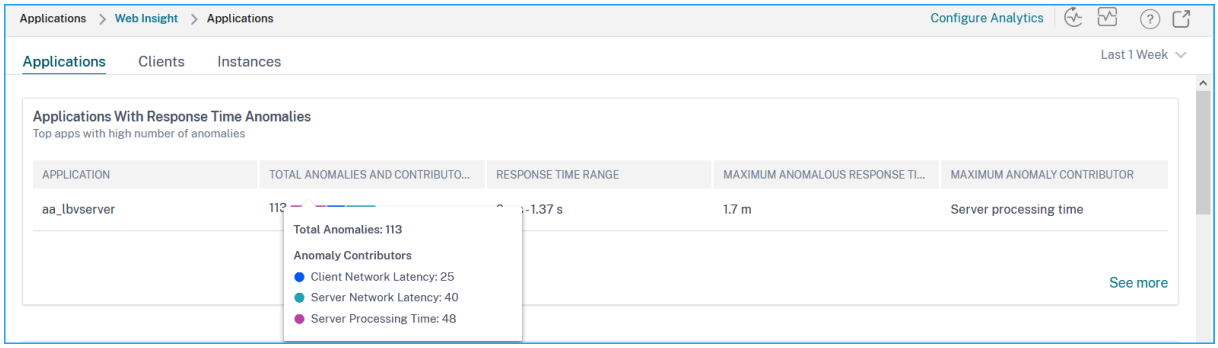
La lentitud de las aplicaciones es una preocupación importante para cualquier organización, ya que tiene como resultado un impacto en el negocio o productividad. Como administrador, debe asegurarse de que todas las aplicaciones funcionen de manera óptima para evitar cualquier impacto en el

negocio. Cuando los usuarios experimentan una lentitud en el acceso a la aplicación, debe asegurarse de que el problema es con:

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

NetScaler Console realiza comprobaciones de anomalías cada hora e informa de las anomalías del tráfico de la última hora, en función de ciertos 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.

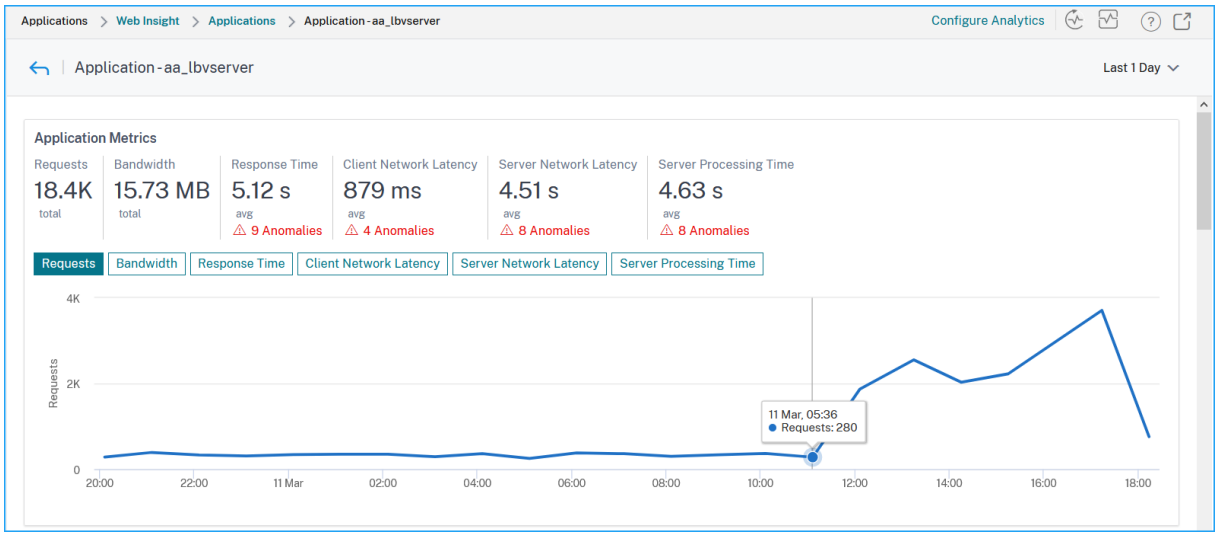
La página **Aplicaciones > Web Insight** permite ver las aplicaciones con anomalías de tiempo de respuesta durante la duración seleccionada. La métrica **Aplicaciones con anomalías de tiempo de respuesta** muestra las cinco aplicaciones principales en función de las anomalías totales. Haga clic en **Ver 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.



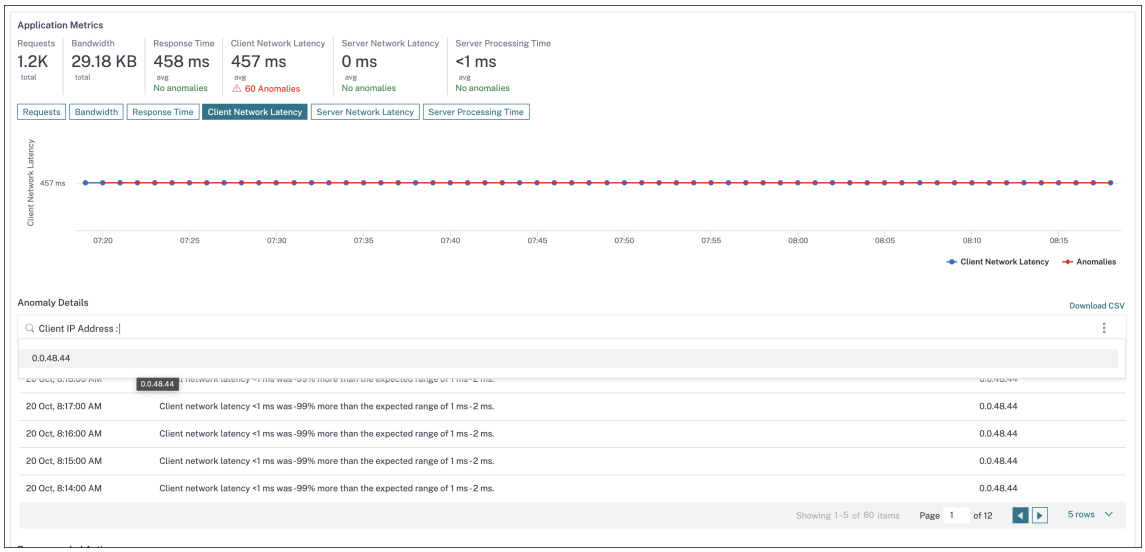
Las **Métricas de la Aplicación** le permiten ver:

- **Resumen**: 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: la latencia media de la red del cliente (del cliente a NetScaler)
- **Latencia**de red de servidores: latencia media de red de servidores (de NetScaler a servidor)
- **Tiempo**de procesamiento del servidor: el tiempo medio de procesamiento del servidor (del servidor a NetScaler)

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.

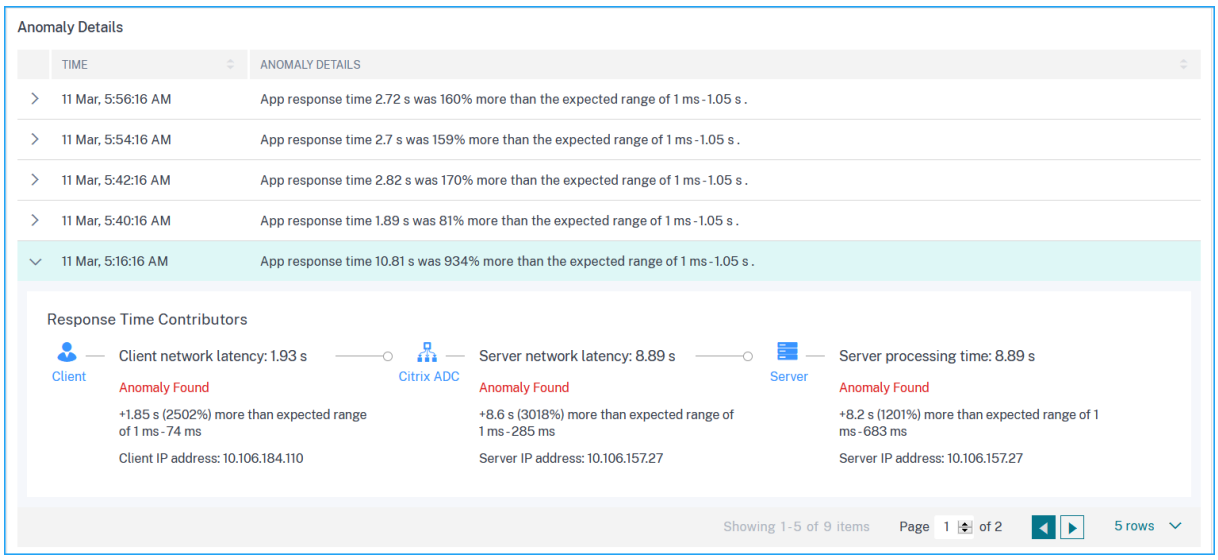
En las fichas **Latencia de la red del cliente** y **Latencia de la red del servidor**, puede ver:

- **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.

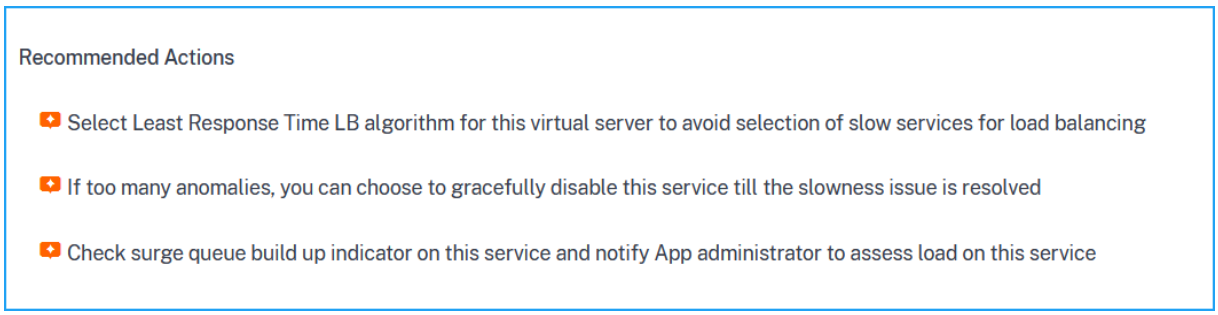


Tiempo de respuesta

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.

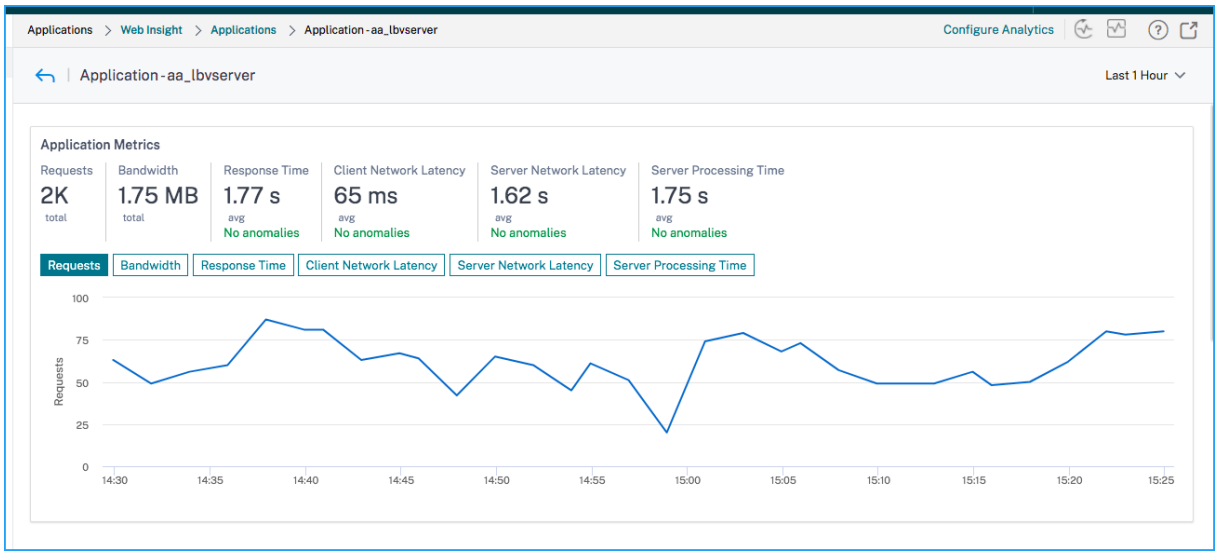


Gráfico de servicio

March 6, 2024

La función de gráfico de servicios de NetScaler Console le permite supervisar todos los servicios de Kubernetes en una representación gráfica. Esta función también le permite ver un análisis detallado y métricas accionables de los servicios. Vaya a **Aplicaciones > Gráfico de servicio** para 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 > Service Graph** y haga clic en la ficha **Microservicios** para:

- 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
- Ver métricas de cliente y detalles de resumen de transacciones de cliente

Al visualizar estas métricas en NetScaler Console, puede analizar la causa raíz de los problemas y tomar las medidas de solución de problemas necesarias con mayor rapidez. 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 NetScaler, 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 Console 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 Console muestra el estado del cliente según 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 Console 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 26, 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.

Con un StyleBook, puede:

- Configure una función específica de NetScaler.
- Cree 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 en las instrucciones paso a paso sobre cómo lograrlo en una instancia de NetScaler en particular. NetScaler Console calcula la diferencia entre el estado existente en un NetScaler y el estado deseado que especificó, y realiza las modificaciones necesarias en la infraestructura. Como los StyleBooks utilizan una sintaxis declarativa, escrita en YAML, los componentes de un StyleBook se pueden especificar en cualquier orden y NetScaler Console 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 sola configuración en una o varias instancias de NetScaler y también se puede mover entre instancias.
- **Interfaz de usuario generada automáticamente**: NetScaler Console genera automáticamente los formularios de interfaz de usuario que se utilizan para rellenar los parámetros del StyleBook cuando la configuración se realiza mediante la GUI de NetScaler Console. 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 Console 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 utilizar el mismo StyleBook para crear otra configuración con valores diferentes y ejecutarla en la misma instancia o en una instancia diferente. Se crea un nuevo paquete de configuración para esta configuración. El paquete de configuración se guarda tanto en NetScaler Console como en la instancia de NetScaler en la que se ejecuta la configuración.

Puede usar los StyleBooks predeterminados, que vienen con NetScaler Console, para crear configuraciones para su implementación, o diseñar sus propios StyleBooks e importarlos a NetScaler Console. Puede usar los StyleBooks para crear configuraciones mediante la GUI de NetScaler Console o mediante las API.

Este documento incluye las siguientes secciones:

- 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

March 6, 2024

El panel **de seguridad de las aplicaciones** le proporciona una descripción general de las métricas de seguridad de las aplicaciones descubiertas. Este panel muestra la información sobre los ataques de seguridad de las aplicaciones descubiertas, como los ataques de sincronización, los ataques de ventanas pequeñas y los ataques de inundación de DNS.

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 sobre infracciones se envía a NetScaler Console solo cuando se produce una infracción o un ataque. Muchas infracciones y vulnerabilidades conducen a un alto valor del índice de amenazas.

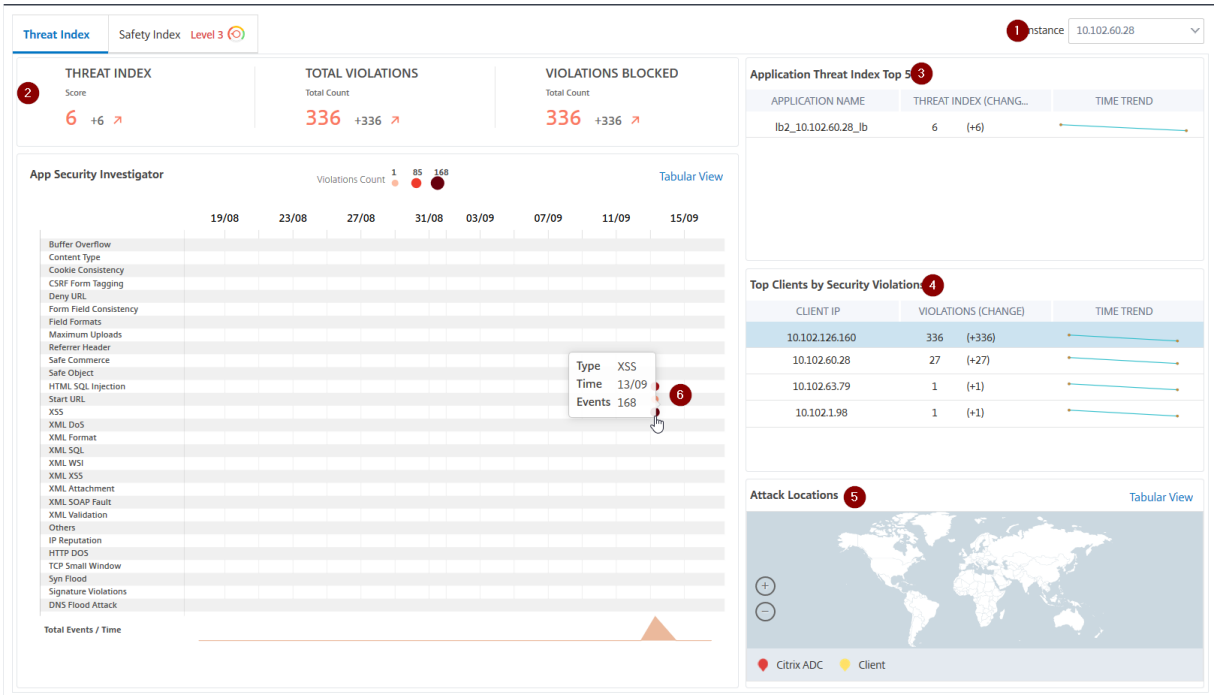
   - **Índice de seguridad**. Sistema de clasificación de un solo dígito que indica con qué seguridad ha configurado las instancias NetScaler para proteger las aplicaciones de amenazas y vulnerabilidades externas. Cuanto menores sean los riesgos de seguridad de una aplicación, mayor será el índice de seguridad. 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 las aplicaciones, pero no se proporcionan medidas de

seguridad del sistema NetScaler, como una contraseña segura para el usuario de nsroot, a las aplicaciones se les asigna un valor de índice de seguridad bajo.

Puede ver las discrepancias notificadas 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.

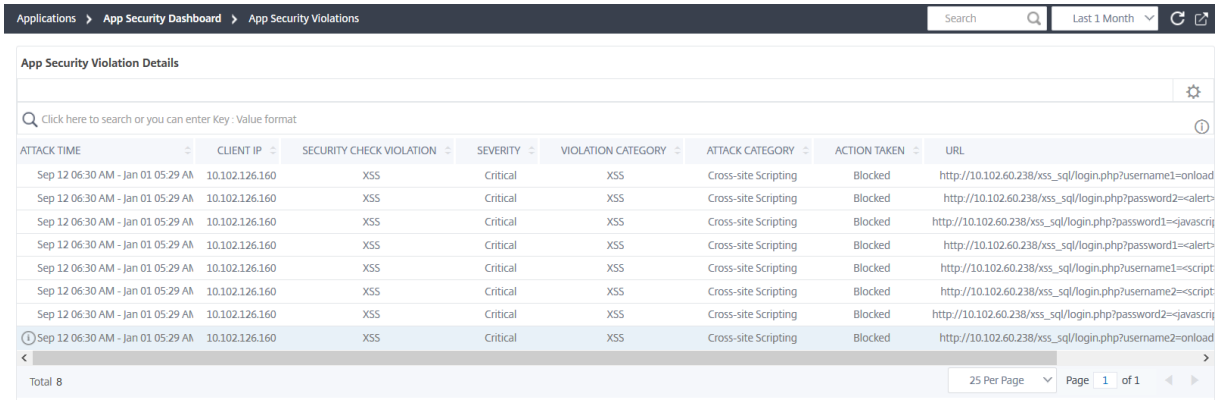
4: muestra las violaciones de seguridad según los clientes. Se muestra el gráfico App Security Investigator para cada cliente. Puede hacer clic en cada IP de cliente para ver los resultados.

5: Muestra las infracciones en la vista de mapa y en la vista tabular.

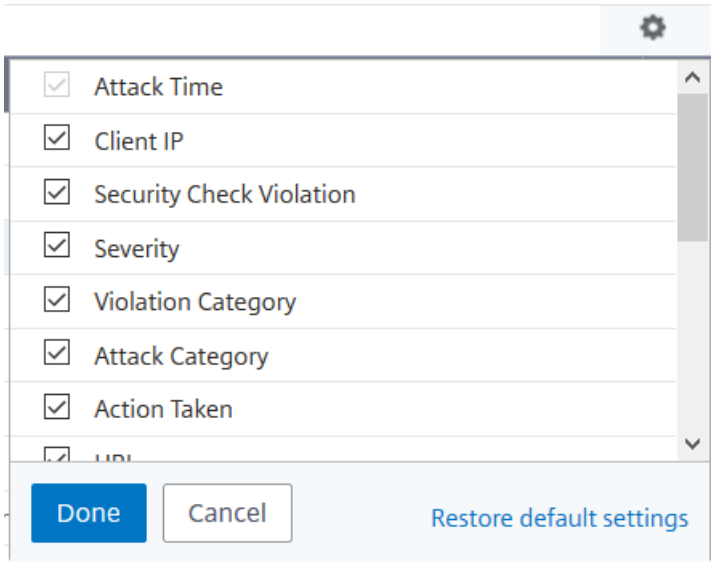
6: muestra los detalles de la infracción. Al situar el puntero del mouse sobre el gráfico, se muestran los detalles como el tipo de infracción, la hora del ataque y el total de eventos.

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 sobre la infracción de secuencias de comandos 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.



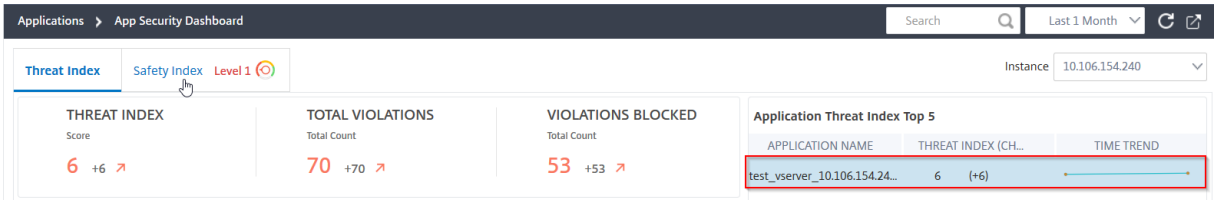
Detalles del índice de seguridad

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.

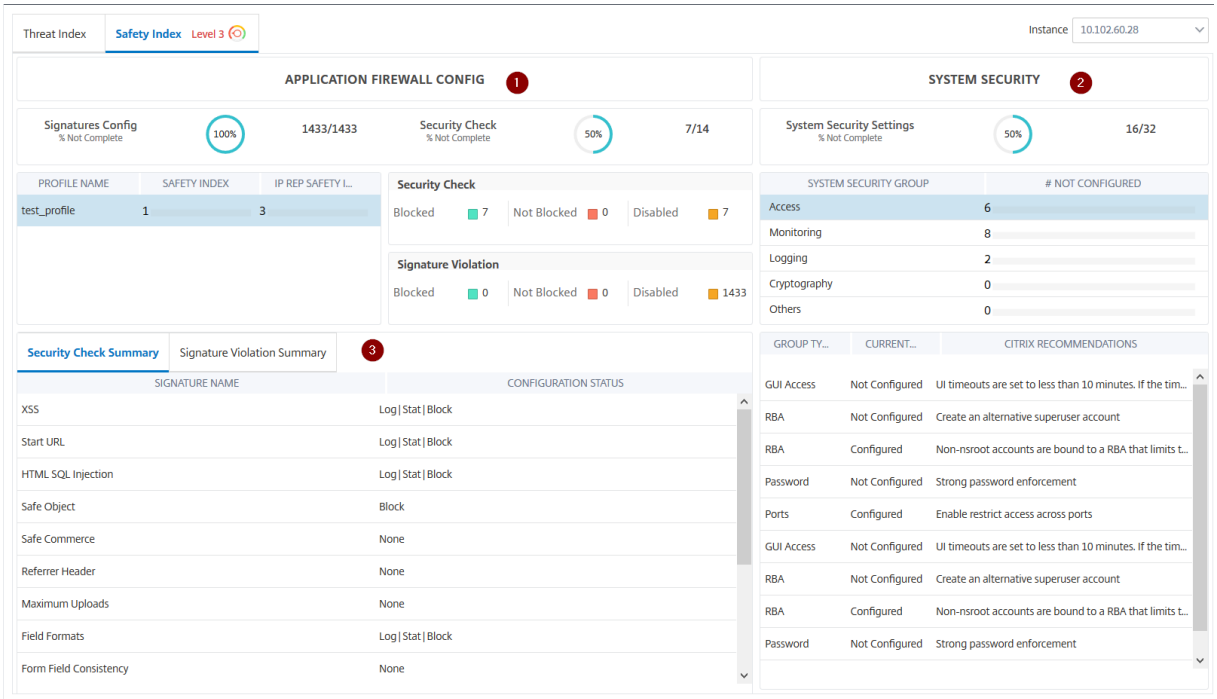
El resumen del índice de seguridad proporciona información sobre la eficacia de las siguientes configuraciones de seguridad:

- **Configuración del firewall de aplicaciones**. Muestra cuántas entidades de firma y seguridad no están configuradas.
- **Seguridad del sistema de consola de NetScaler**. 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 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 habilitando la información de seguridad para los servidores virtuales y, a continuación, yendo a **Seguridad > Violaciones de seguridad**. Para obtener más información sobre el caso de uso del índice de seguridad, consulte Security Insight.

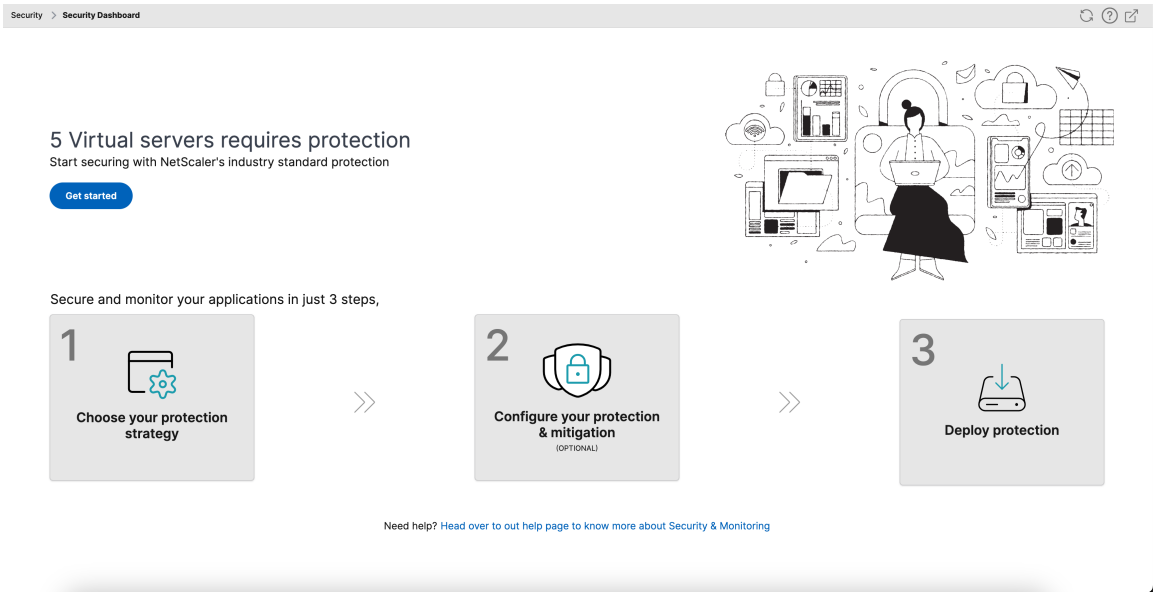
Panel de seguridad unificada

March 6, 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.

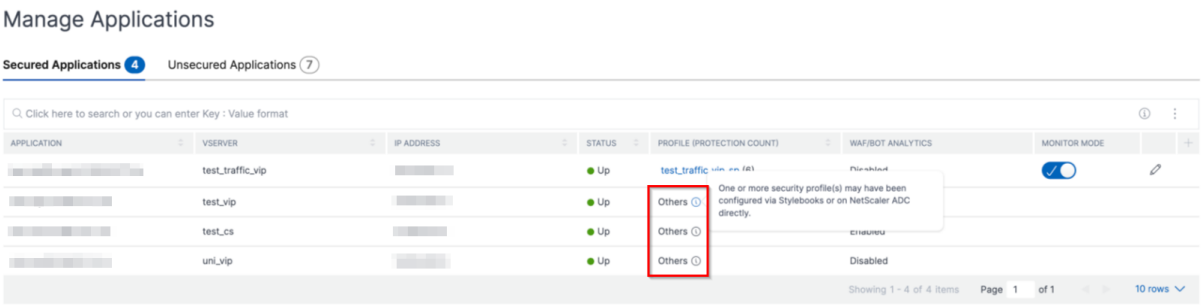


- Puede ver la cantidad total de servidores virtuales que requieren protección. Haga clic en **Comenzar** para ver los detalles en **Aplicaciones no seguras.**
- Los tipos de servidores virtuales aptos para configurar las protecciones son el equilibrio de carga y la conmutación de contenido.

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.

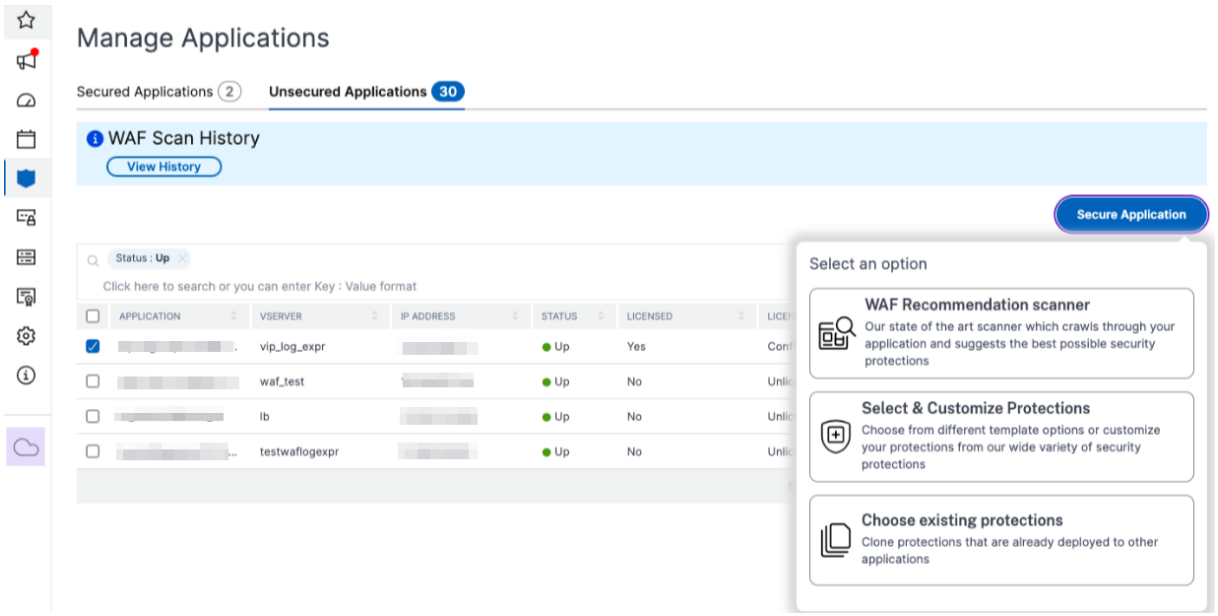
Si ya ha configurado las protecciones directamente en las instancias de NetScaler o mediante StyleBooks, puede ver las aplicaciones en la ficha **Aplicaciones seguras** marcada como **Otras** en **Perfil**.



Configurar protecciones para aplicaciones no seguras

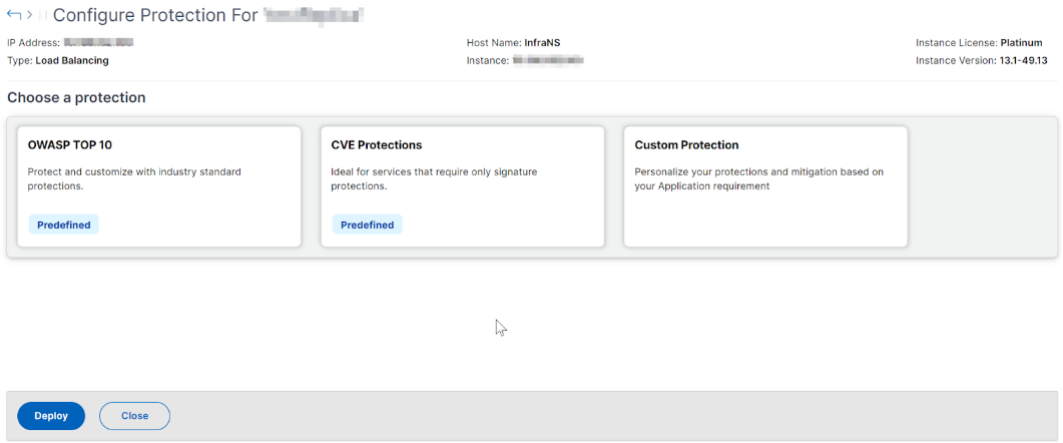
> **Nota:**
>
> El número máximo de entidades de configuración (reglas) admitidas en la lista de bloques es 32.

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 Console.
    - **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**

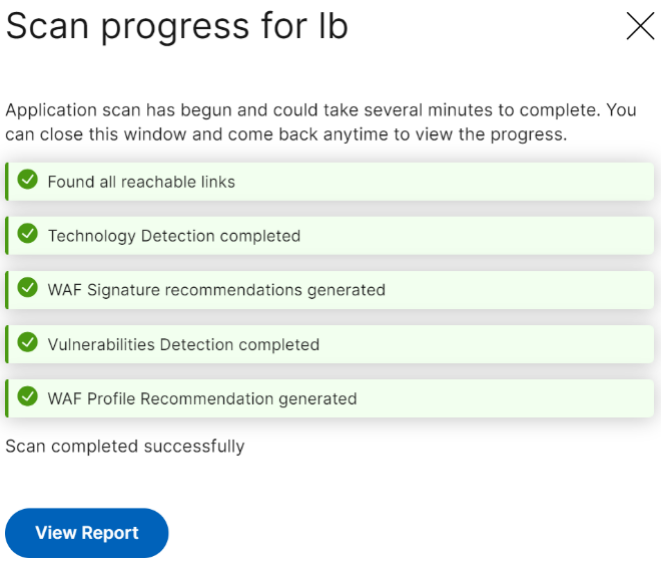
del campo es la clave y el valor del **campo es el valor**. Asegúrese de que todos los campos del formulario necesarios para iniciar sesión se agreguen correctamente, incluidas las contraseñas. Los valores se cifran antes de almacenarlos en la base de datos. Puede hacer clic en **Agregar** para agregar 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`.

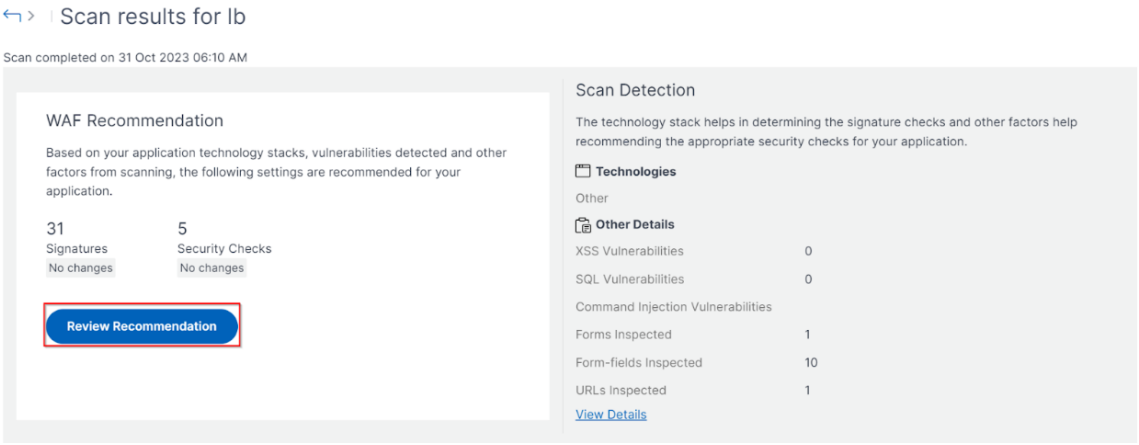
2. En **Configuraciones de escaneo**:

   - **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.

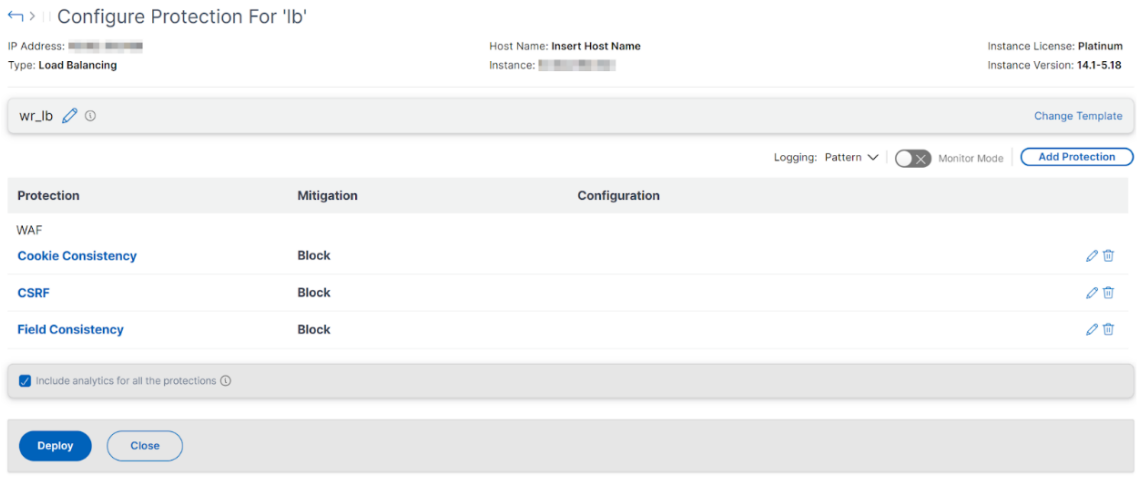
3. La configuración de los ajustes de escaneo del WAF está completa. Puede hacer clic en **Iniciar escaneo** para comenzar el proceso de escaneo y esperar a que finalice el progreso. Una vez finalizado el escaneo, haga clic en **Ver informe**.



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**.

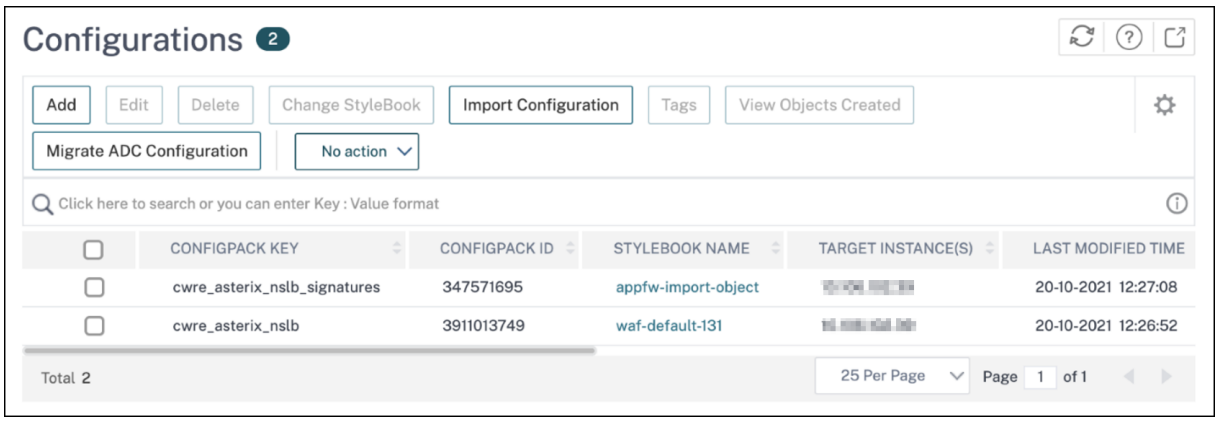


Si aplica correctamente las comprobaciones de seguridad:

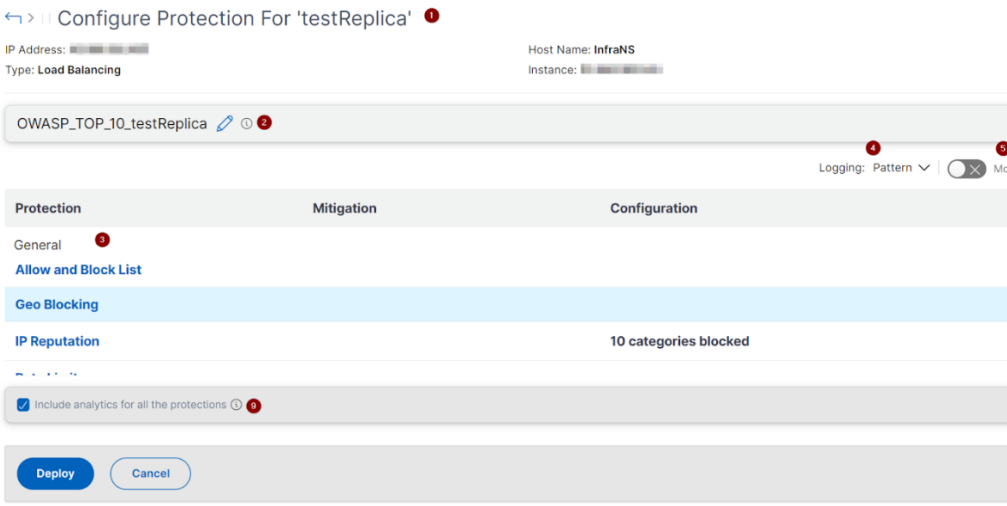
- La configuración se aplica a la instancia de NetScaler a través de StyleBooks, según la versión.
  - Para NetScaler 13.0 `unified-appsec-protection-130`, se usa StyleBook.
  - Para NetScaler 13.1 `unified-appsec-protection-131`, se usa StyleBook.
  - Para NetScaler 14.1 `unified-appsec-protection-141`, 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.

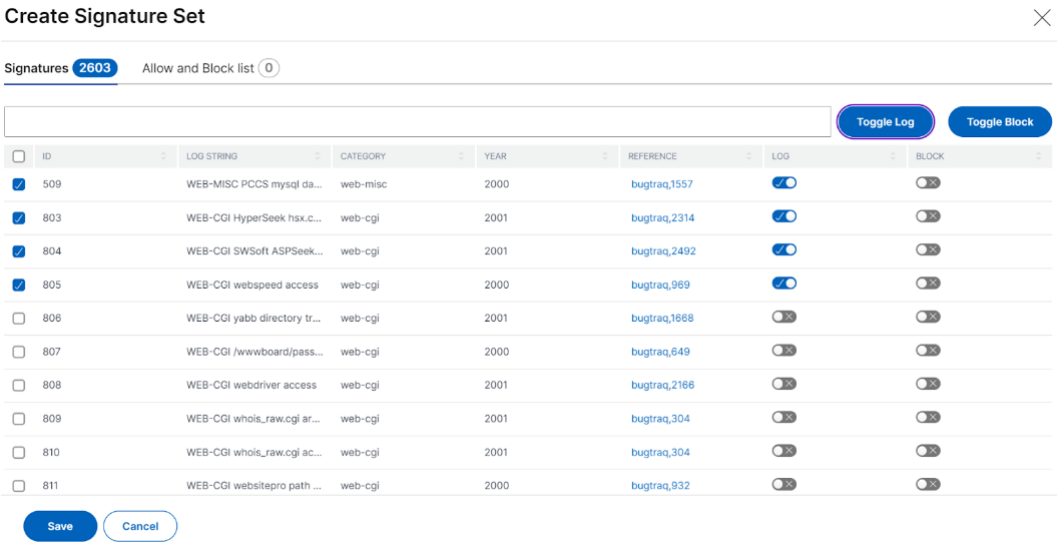
7 - Le permite elegir una nueva plantilla mediante la opción Cambiar plantilla.

8: Permite modificar o eliminar la protección.

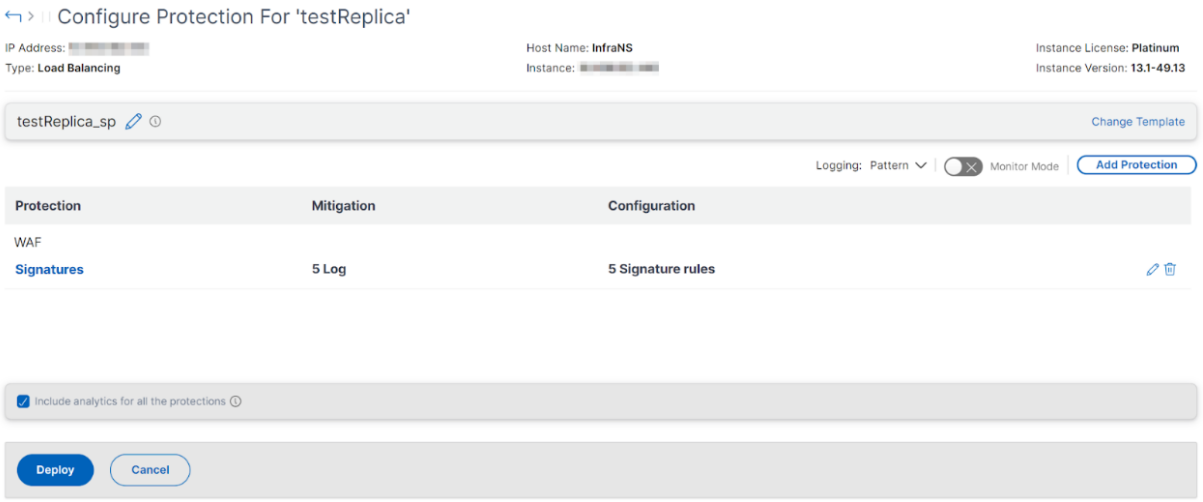
9: Habilita el análisis para las protecciones que seleccione. Esta opción está seleccionada de forma predeterminada. Puede ver los análisis de las protecciones configuradas en **Seguridad > Violaciones de seguridad**.

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**.

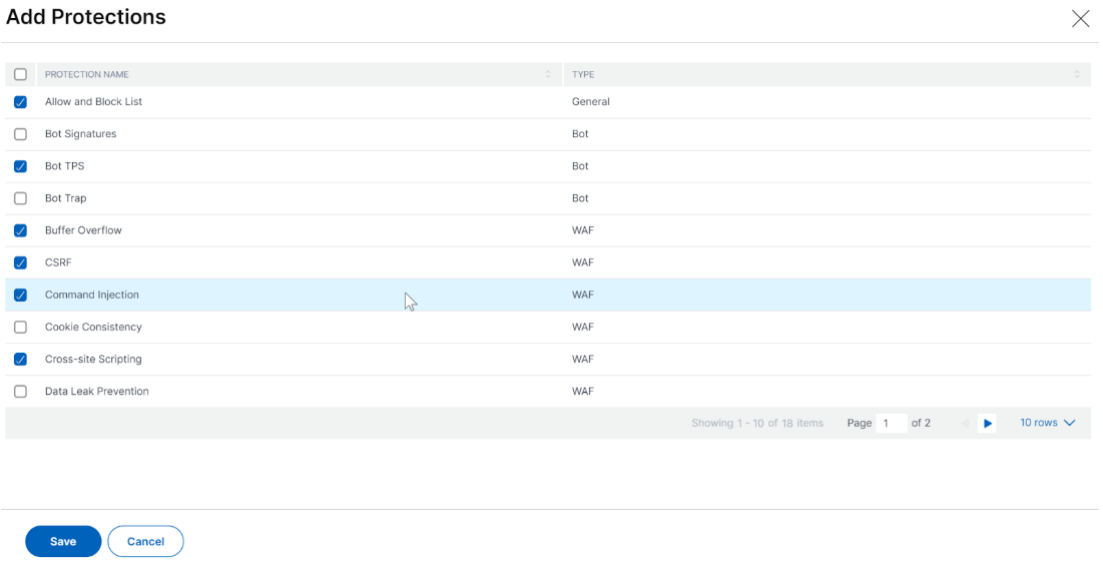


Después de hacer clic en **Guardar**, puede ver las firmas agregadas a la página de configuración.



También puede hacer clic en **Agregar protección** para agregar más protecciones a la aplicación. Después de configurar todas las protecciones, haga clic en **Implementar**.

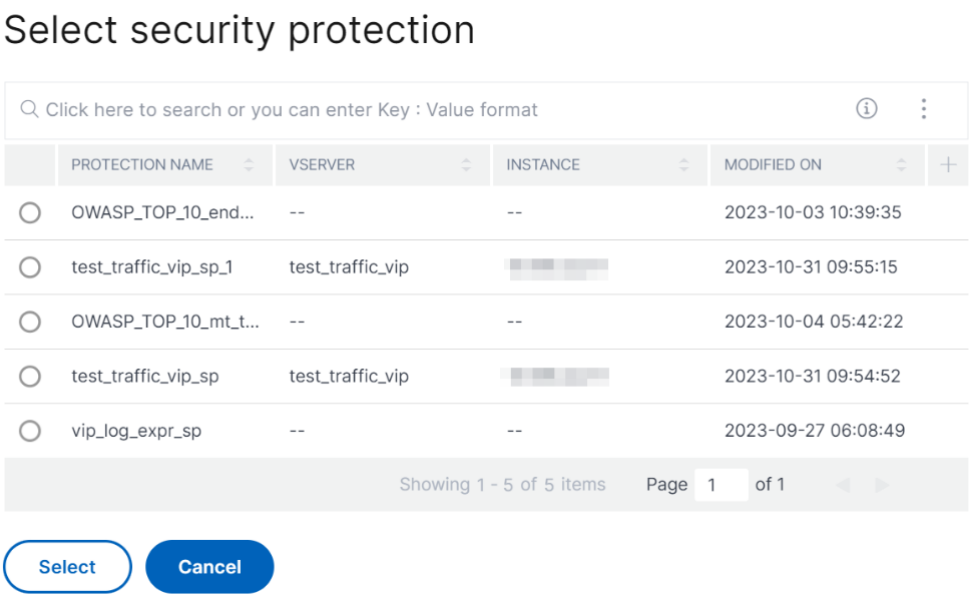
Protección personalizada Para realizar la implementación con protecciones según sus necesidades, haga clic en **Crear nueva protección**. En la página **Agregar protecciones**, seleccione las protecciones que quiere implementar y haga clic en **Guardar**.



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

March 6, 2024

Las aplicaciones web que están expuestas a Internet se han vuelto vulnerables a los ataques drásticamente. NetScaler Console le permite visualizar los detalles de las infracciones procesables para proteger las aplicaciones de los ataques. Navegue hasta **Seguridad** > **Violaciones de seguridad** para obtener una solución de panel único para:

- Visualice las aplicaciones con una visibilidad total de los detalles de las amenazas asociados tanto a la información de WAF como a la de los bots. Para obtener más información, consulte Panel de seguridad unificada.
- Acceda a las infracciones de seguridad de la aplicación en función de sus categorías, como **Red**, **Bot**y **WAF**.
- Tome 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.

Configuración

Para ver las infracciones, debes asegurarte de:

- Para empezar a configurar las protecciones y habilitar el análisis en sus aplicaciones. Para obtener más información, consulte Panel de seguridad unificada.

  Si ha configurado las protecciones mediante StyleBook o directamente en la instancia de NetScaler, puede seguir el procedimiento parahabilitar las infracciones de seguridad de WAF y las infracciones de seguridad**de bots:**

  1. Vaya a **Infraestructura > Instancias > NetScaler** y seleccione el tipo de instancia. Por ejemplo, VPX.
  2. Seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Configurar análisis**.
  3. Seleccione los servidores virtuales y haga clic en **Activar seguridad y análisis**.
  4. En la ventana **Habilitar análisis**, seleccione **Infracciones seguridad de WAF** e **Infracciones de seguridad de bots** y, a continuación, haga clic en **Aceptar**.

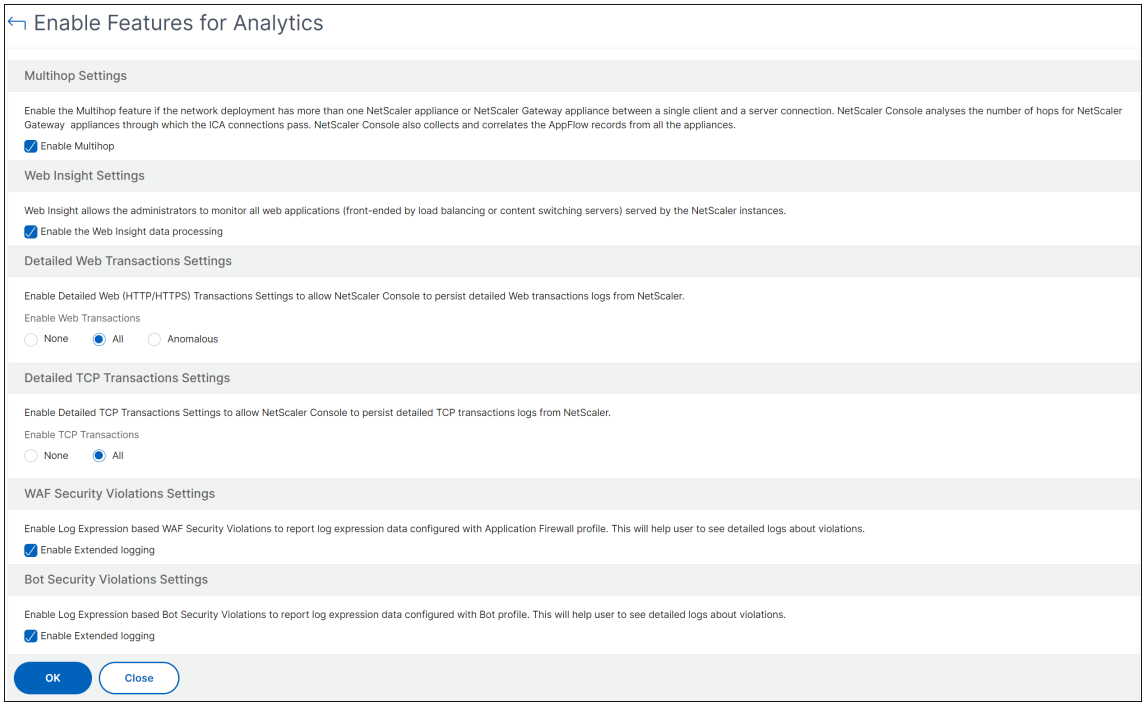
- Para configurar los ajustes detallados de las transacciones web.
- Si el **recopilador de métricas** está activado. Para obtener más información, consulte Configurar el análisis inteligente de aplicaciones.

Habilitar la configuración de transacciones web

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

   Se muestra la página **Configuración de análisis**.

2. Haga clic en **Habilitar funciones para Analytics**.
3. En **Configuración detallada de transacciones web**, selecciona **Todo**.

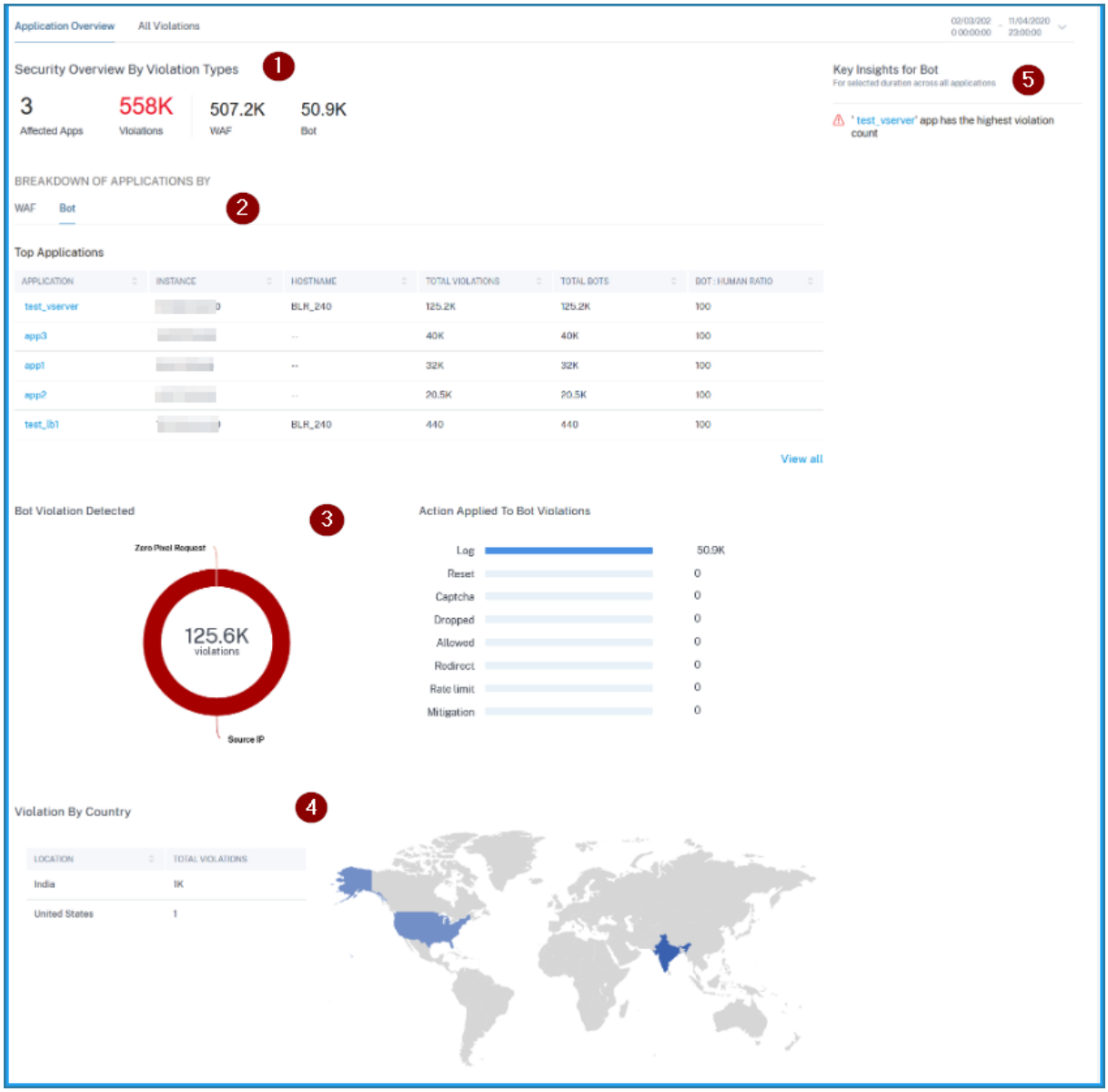


4. Haga clic en **OK**.

Descripción general de la aplicación

March 6, 2024

La página **Visión General** de las Aplicaciones muestra las aplicaciones con visibilidad completa de los detalles de amenazas asociados tanto a la información de seguridad como a los robots. También puede ver información como infracciones totales, infracciones totales de WAF y bot, infracciones por país, etc.



1 —Muestra el total de aplicaciones afectadas, el total de infracciones, el total de infracciones WAF y el total de infracciones de Bot durante la duración seleccionada.

2 —Muestra los detalles de las infracciones de WAF y Bot. Haga clic en la ficha **WAF** y **Bot** para ver las 5 principales aplicaciones personalizadas o discretas según el total de infracciones ocurridas. Haga clic en **Ver todo** para ver todos los detalles de la aplicación.

3 —Muestra las infracciones superiores basadas en las incidencias y las acciones aplicadas.

4 —Muestra una vista de mapa geográfico que proporciona visibilidad desde qué ubicaciones se han producido las infracciones.

5 —Proporciona información basada en las infracciones.

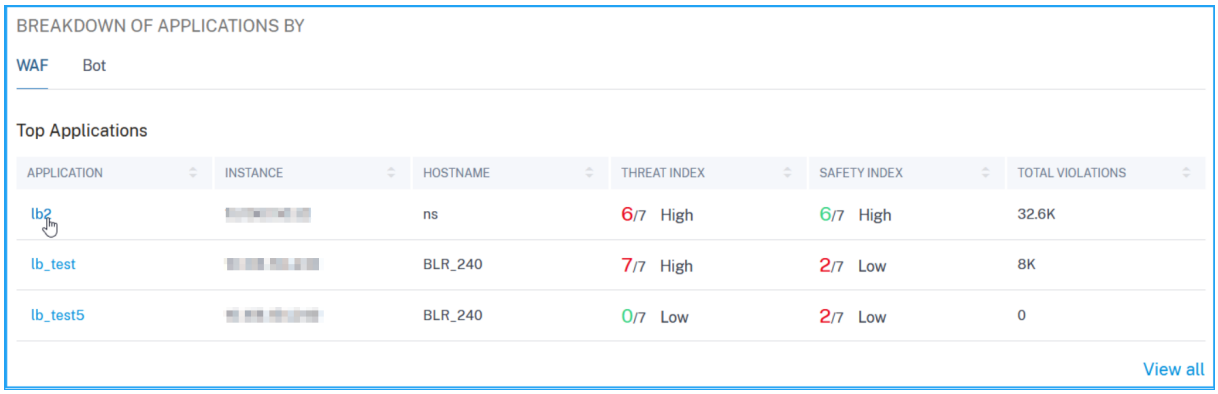
Categorías de infracción

WAF	Bot
Secuestro de cookies	raspador
Inducir XML de tipo de contenido	Creador de captura de pantalla
Desbordamiento de búfer	Buscador
Tipo de contenido	Agente de servicio
Consistencia de cookies	Monitor de sitio
Etiquetado de formularios CSRF	Probador de velocidad
Denegar URL	Sin categoría
Consistencia de campos de formulario	Analizador de virus
Formato de campo	Analizador de vulnerabilidades
Máximo de cargas	Se ha superado la espera de DeviceFP
Encabezado de referencia	DeviceFP no válido
Comercio seguro	Respuesta Captcha no válida
Objeto seguro	Herramienta
Inyección HTML SQL	Se han superado los intentos de Captcha
URL de inicio	Respuesta Captcha válida
Scripts entre sitios	Cliente Captcha Silenciado
XML DoS	Tiempo de espera de Captcha superado
Formato XML	Excedido el límite de tamaño de solicitud
XML WSI	Límite de tasa superado
XML SSL	Lista de bloqueos (IP, subred, expresión de directiva)
Datos adjuntos XML	Lista de permitidos (IP, subred, expresión de directiva)
Error SOAP de XML	Solicitud de cero píxeles
Validación XML	IP de origen
Otros	Host
Reputación IP	Crawler
HTTP DOS	Buscador de alimentación

WAF	Bot
Ventana pequeña TCP	Comprobador de vínculos
Infracción de firma	Márketing
Tipo de carga de archivo	Ubicación geográfica
Scripting entre sitios JSON	URL
JSON SQL	
JSON DOS	
Inyección de	
Bloquear palabra clave	
Palabra clave de bloqueo de JSON	
Gramática de la inyección	

Ver detalles de infracción de WAF

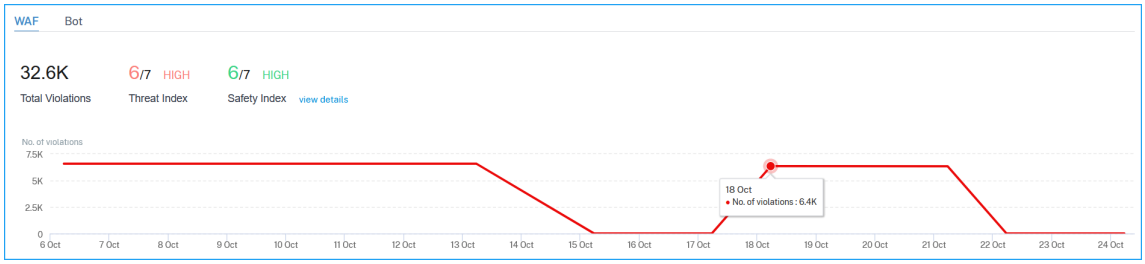
Haga clic en una aplicación en la opción **Aplicaciones principales** o en la opción **Ver todo** para ver los detalles de WAF.



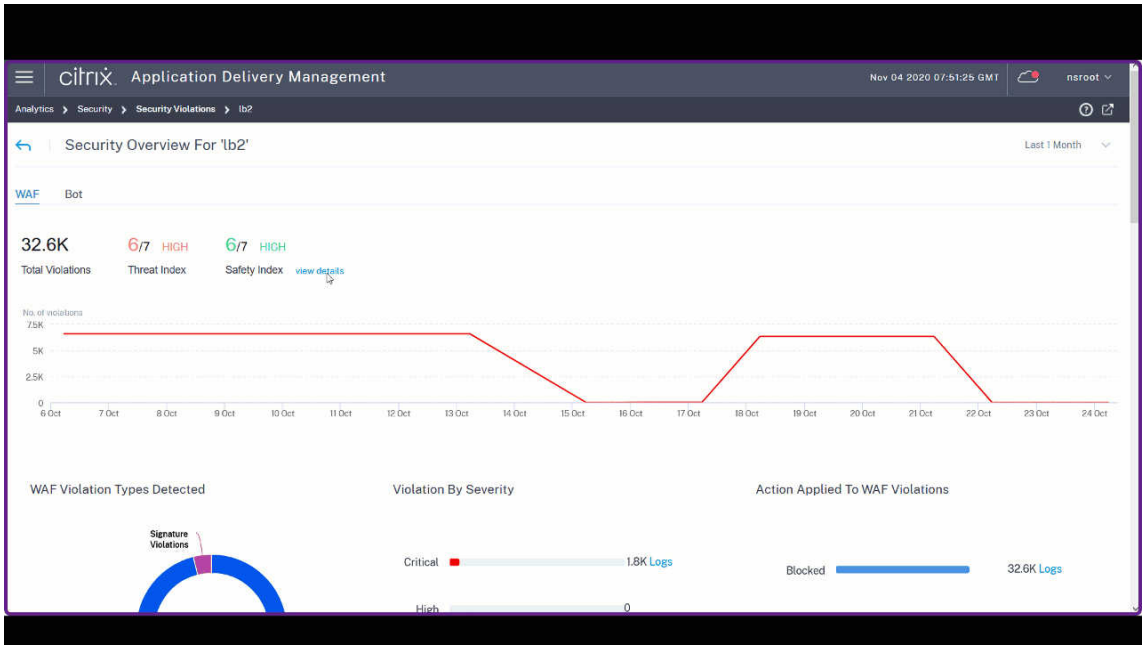
> **Nota:**
>
> Si selecciona una aplicación personalizada, puede ver los detalles de las aplicaciones consolidadas en la página de información **general de seguridad**. En la lista, seleccione una aplicación para ver los detalles de la aplicación seleccionada.

Aparecerá la página **Visión General de Seguridad** de la aplicación seleccionada. En **WAF**, puede ver:

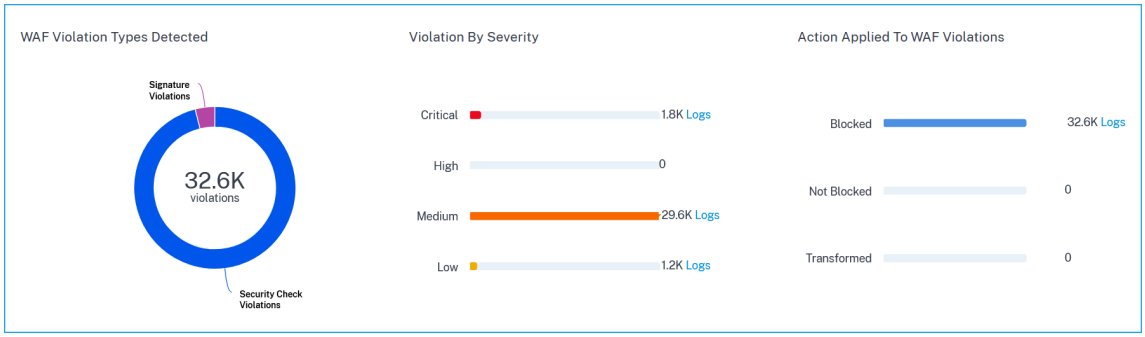
- Una vista gráfica que indica el total de infracciones, la puntuación del índice de amenaza y la puntuación del índice de seguridad de la aplicación.



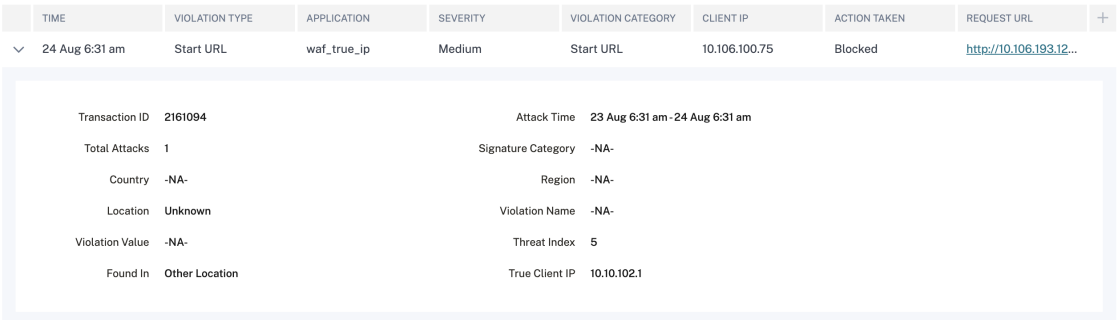
Haga clic en **Ver detalles** para ver los detalles de configuración de Application Firewall y NetScaler System Security.



- Las infracciones basadas en los tipos, la gravedad y las acciones aplicadas.



Haga clic en **Registros** para ver los detalles en función de la gravedad o la acción realizada. También puede ver la dirección IP del cliente.



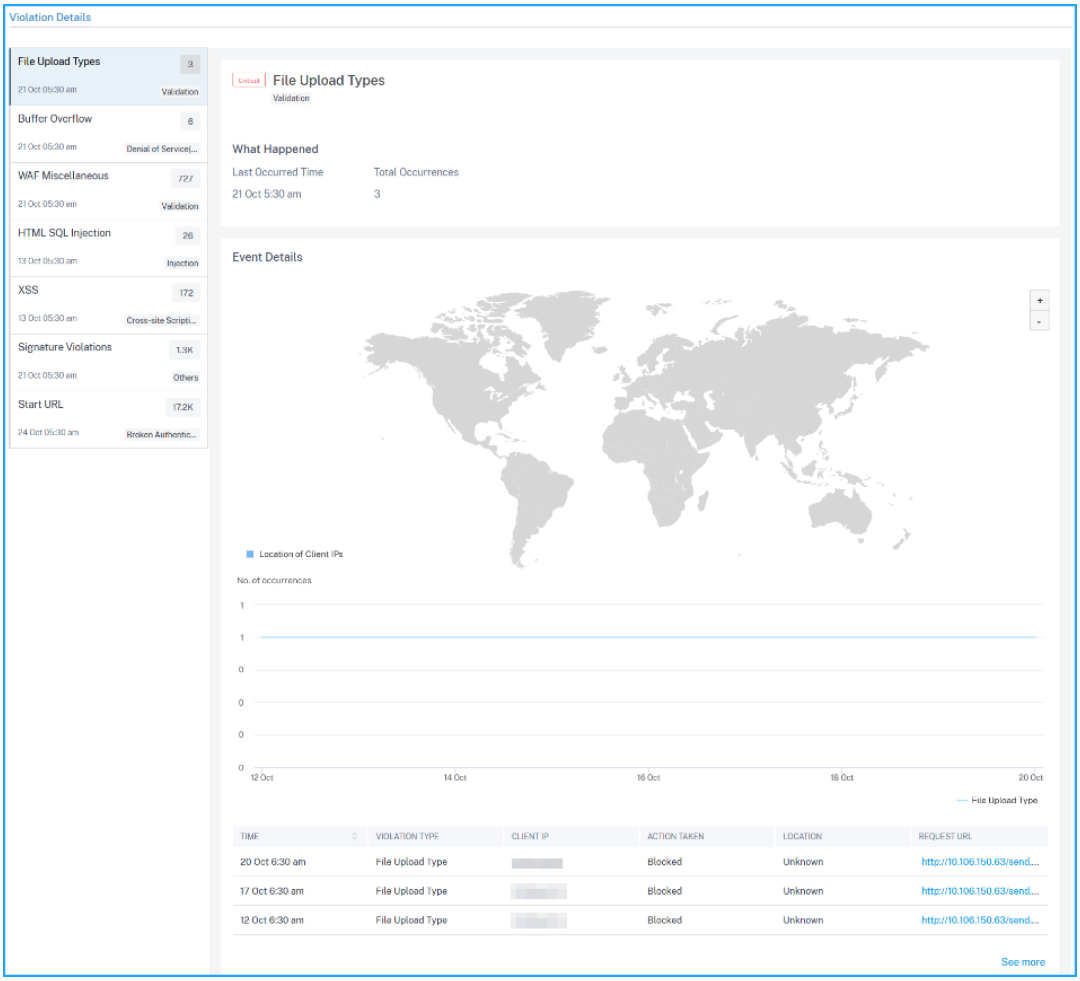
También puede utilizar el cuadro de texto de búsqueda donde puede ver los detalles según sus necesidades. Al hacer clic en el cuadro de búsqueda, el cuadro de búsqueda muestra la lista de sugerencias de búsqueda.

- Las infracciones afectadas en la aplicación. En **Detalles de la infracción**, puede ver los detalles de la infracción afectada.

  > **Nota**
  >
  > En el caso de una aplicación personalizada, se muestran las infracciones aplicables a todas las aplicaciones. Puede hacer clic en una aplicación de la lista para ver las infracciones afectadas en la aplicación seleccionada.

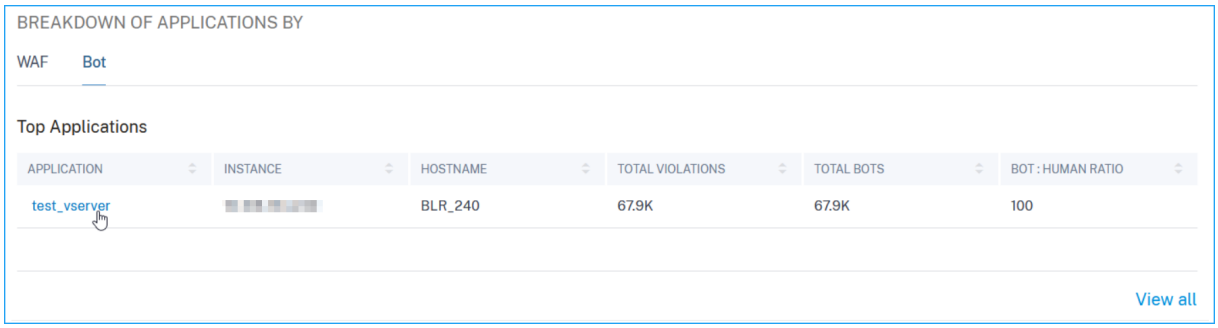
  Haga clic en cada infracción para ver detalles como:

  - **Lo que ocurrió**: indica el total de ocurrencias y la última fecha y hora ocurridas.
  - **Detalles del evento**: muestra un mapa geográfico que indica la IP del cliente y otros detalles de infracción, como el tipo de infracción, la IP del cliente, la ubicación, etc.



Ver detalles de infracción de bot

En la ficha **Bot**, haga clic en una aplicación de **Aplicaciones principales** o en la opción **Ver todas** para ver los detalles del bot.

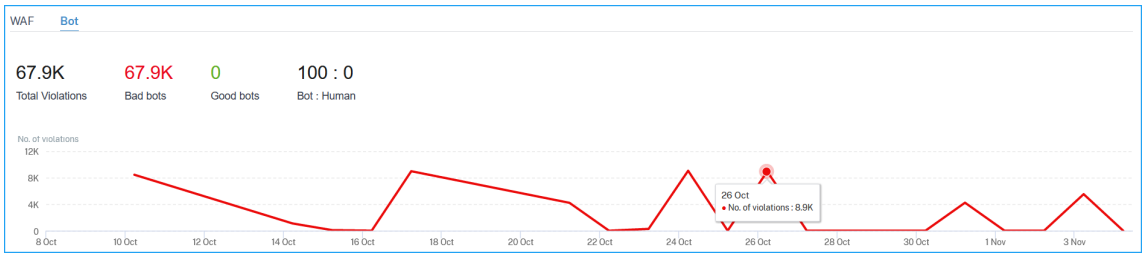


> **Nota**
>
> Si selecciona una aplicación personalizada, puede ver los detalles de las aplicaciones consolidadas en la página de información **general de seguridad**. En la lista, seleccione una aplicación

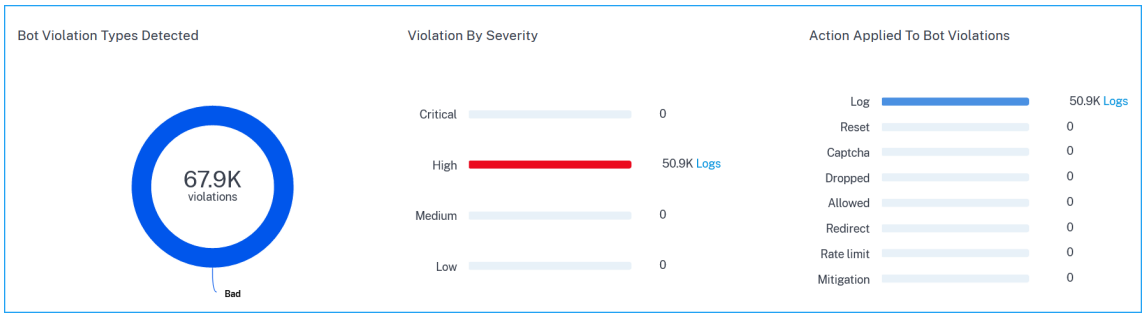
> para ver los detalles de la aplicación seleccionada.

Aparecerá la página **Visión General de Seguridad** de la aplicación seleccionada. En **Bot**, puede ver:

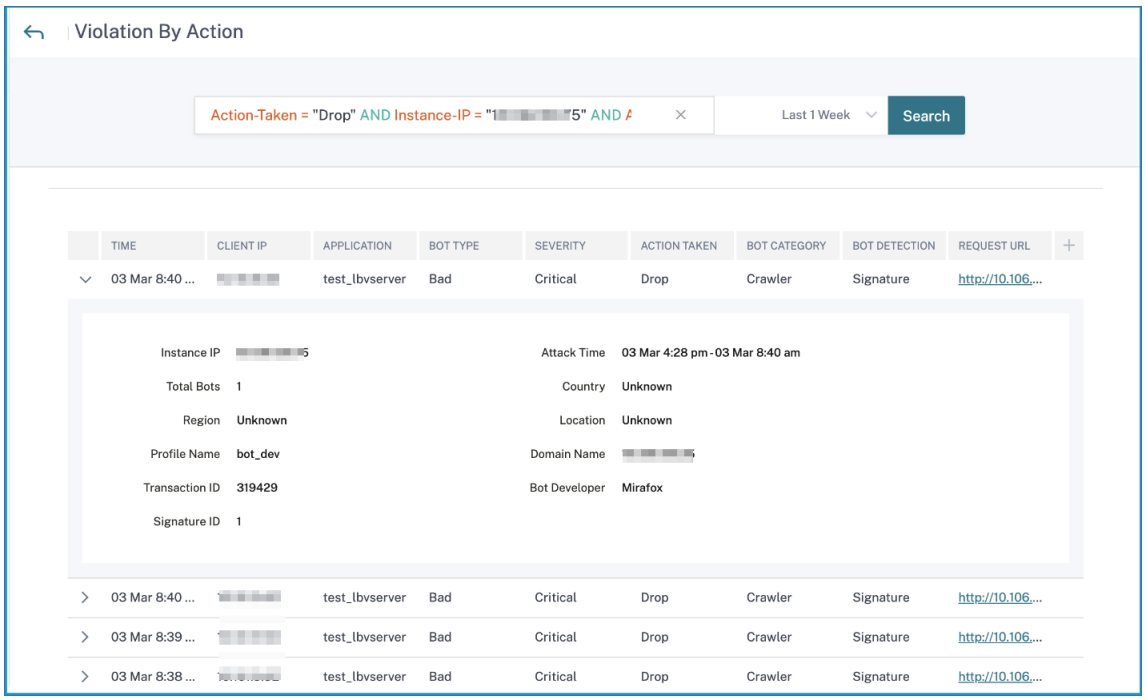
- Gráfico que indica bots totales, bots incorrectos totales, bots buenos totales y relación total entre usuarios humanos y bots que acceden a la aplicación.



- Las infracciones basadas en los tipos de bot, la gravedad y las acciones aplicadas.

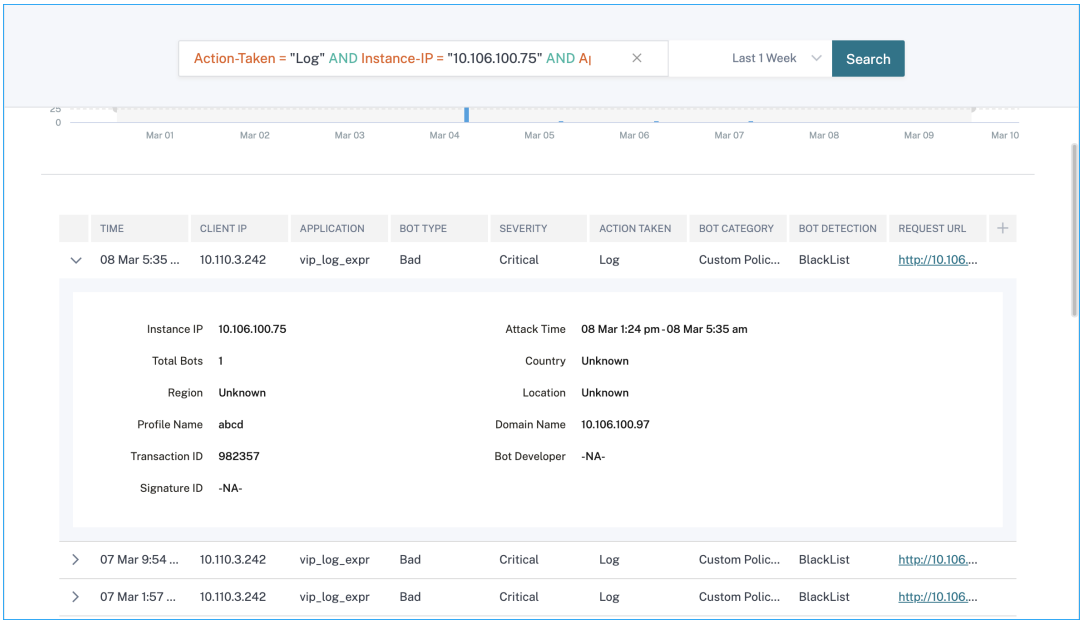


  Haga clic en **Registros** para ver los detalles en función de la gravedad o las acciones realizadas. Si un bot detectado es un bot de tipo Firma, puede ver más detalles como desarrollador de bot e ID de firma. El identificador de firma le permite identificar si el bot detectado es un bot bueno o un bot malo.



Nota:

Si un bot detectado es cualquier otro tipo de bot aparte del bot de firma, el identificador de firma y el desarrollador de bot se muestran como N/A.



También puede utilizar el cuadro de texto de búsqueda donde puede ver los detalles del bot según sus necesidades. Al hacer clic en el cuadro de búsqueda, el cuadro de búsqueda muestra la lista de sugerencias de búsqueda.

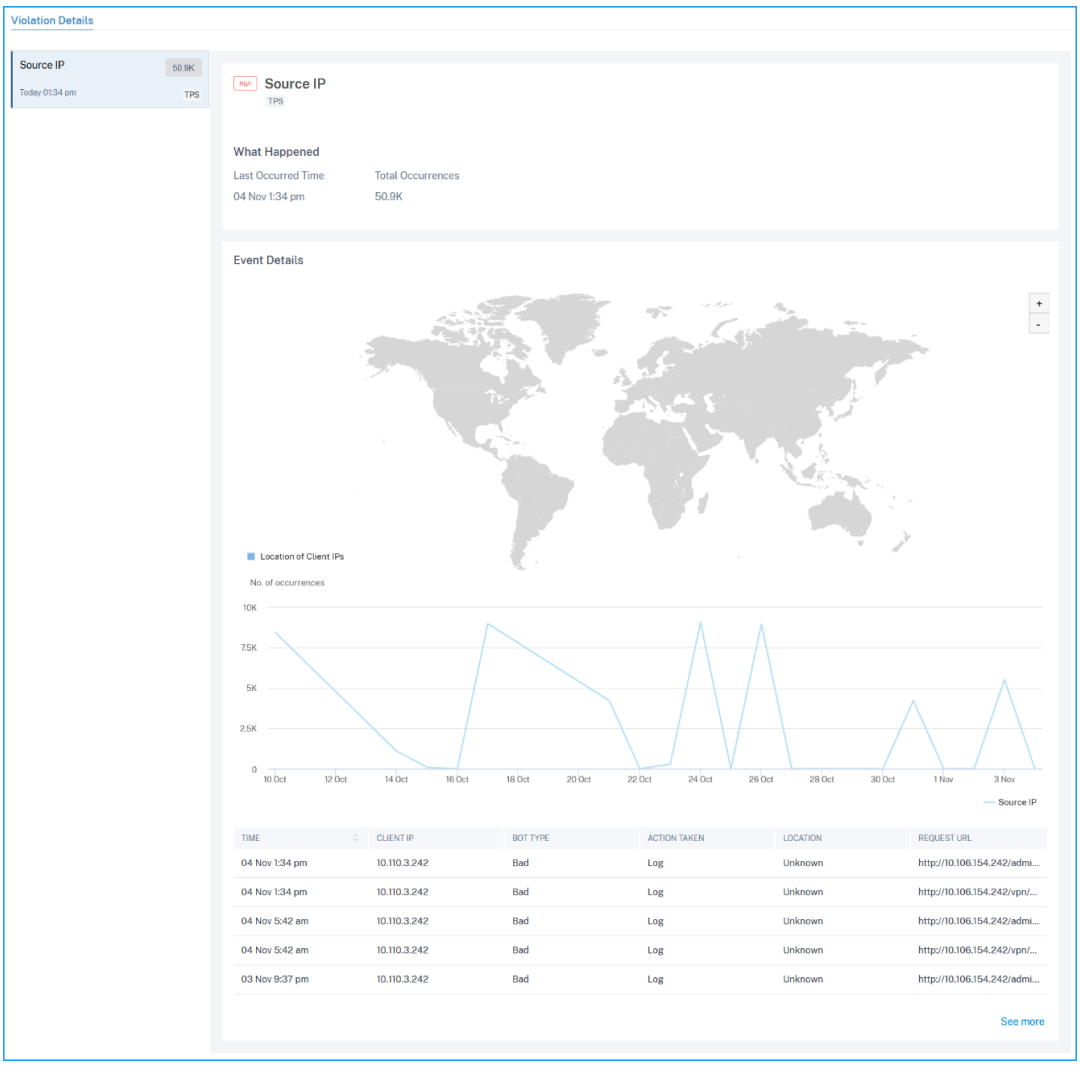
- Las infracciones afectadas en la aplicación. En **Detalles de la infracción**, puede ver los detalles

de la infracción afectada.

> **Nota:**
>
> En el caso de una aplicación personalizada, se muestran las infracciones aplicables a todas las aplicaciones. Puede hacer clic en una aplicación de la lista para ver las infracciones afectadas en la aplicación seleccionada.

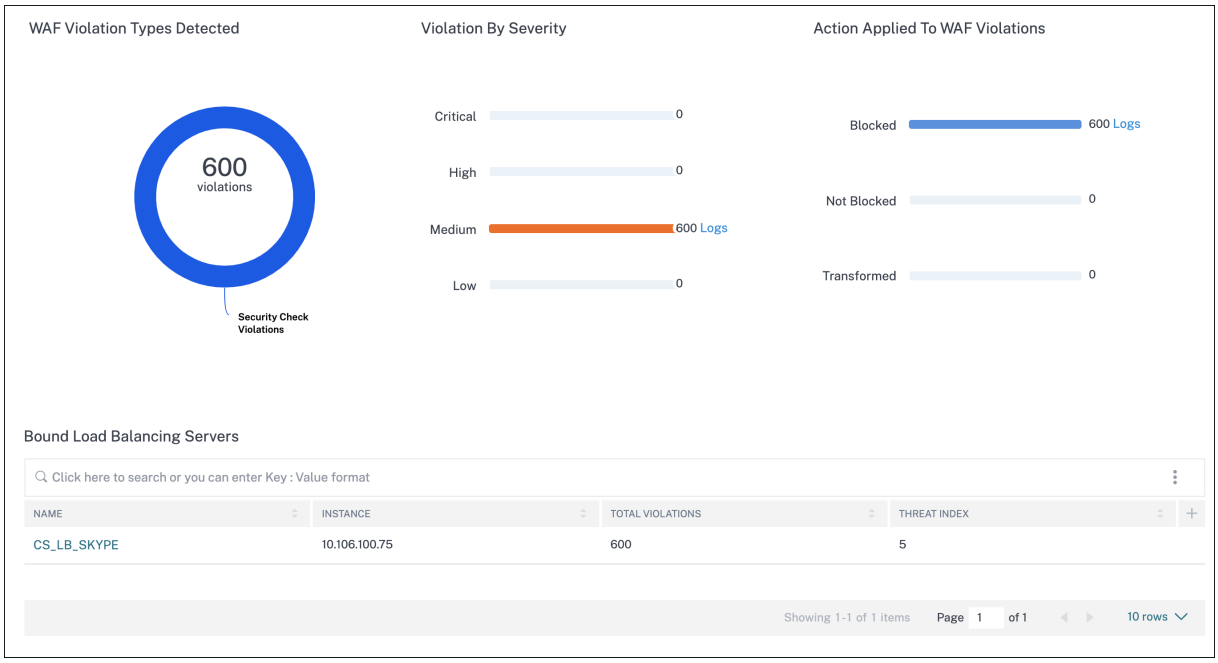
Haga clic en cada infracción para ver detalles como:

- **Lo que ocurrió**: indica el total de ocurrencias y la última fecha y hora ocurridas.
- **Detalles del evento**: muestra un mapa geográfico que indica la IP del cliente y otros detalles de infracción, como el tipo de infracción, la IP del cliente, la ubicación, etc.



> **Nota:**
>
> En **WAF** y **Bot**, puede ver los análisis para el servidor virtual de conmutación de contenido que

> está vinculado a los servidores virtuales de equilibrio de carga. Haga clic en el servidor virtual de conmutación de contenido y, en **Servidor de equilibrio de carga enlazado**, puede ver la lista de servidores de equilibrio de carga enlazados al servidor virtual de conmutación de contenido.



Ver historial de eventos

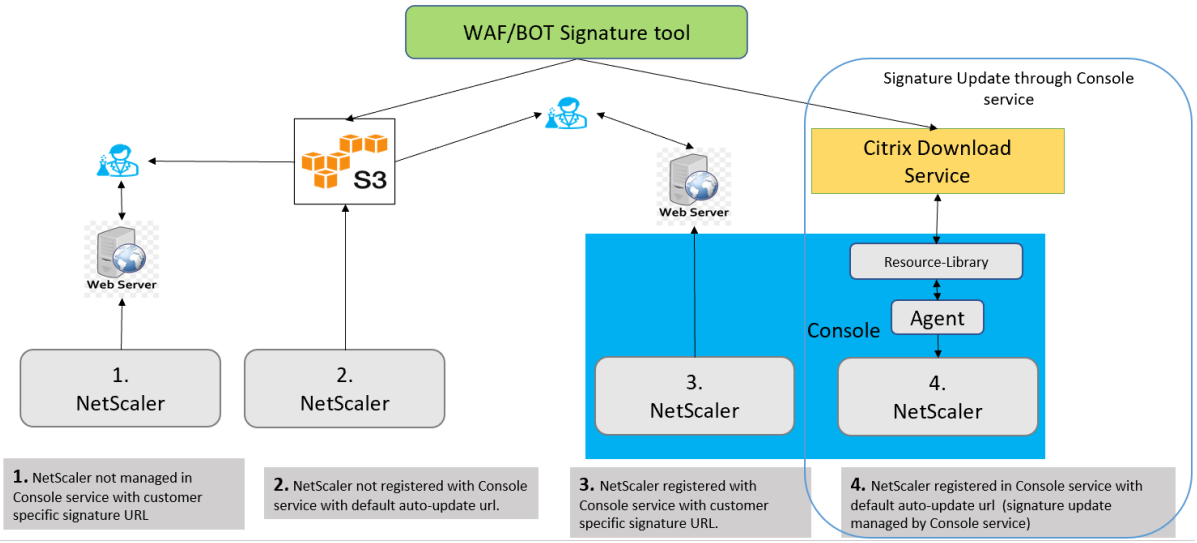
Puedes ver las actualizaciones de firmas en **Eventos**cuando:

- Se agregan nuevas firmas en las instancias de NetScaler.
- Las firmas existentes se actualizan en las instancias de NetScaler.

Actualización automática de firmas

NetScaler Console comprueba automáticamente si hay nuevas actualizaciones de firmas y las aplica a las instancias de NetScaler administradas.

El siguiente diagrama muestra cómo se recuperan las firmas de la nube de AWS, se actualizan en NetScaler y se ve el resumen de las actualizaciones de firmas en NetScaler Console.



Todas las infracciones

March 6, 2024

La página **Todas las infracciones** muestra los detalles de infracciones de seguridad de la aplicación en función de las categorías **Red**, **WAF**y **Bot**. Para ver las infracciones de seguridad en NetScaler Console, asegúrese de haber habilitado todos los ajustes necesarios. Para obtener más información, consulte el procedimiento disponible en Configuración.

Categorías de infracción

NetScaler Console le permite ver las siguientes infracciones. En **Detalles de infracción**, puede hacer clic en cada ficha de infracción para ver los detalles de la infracción.

Red	WAF	Bot
HTTP Lento Loris	Inducir XML de tipo de contenido	raspador
Loris lentos DNS	Desbordamiento de búfer	Creador de captura de pantalla
Entrada lenta HTTP	Tipo de contenido	Buscador
Ataque de inundación de NXDomain	Consistencia de cookies	Agente de servicio

Red	WAF	Bot
Ataque de desincronización HTTP	Etiquetado de formularios CSRF	Monitor de sitio
Ataque Bleichenbacher	Denegar URL	Probador de velocidad
Ataque SegmentSmack	Consistencia de campos de formulario	Herramienta
SYN Ataque de inundación	Formato de campo	Sin categoría
Ataque de ventana pequeña	Encabezado de referencia	Analizador de virus
		Scripts entre sitios
		XML DoS
		Formato XML
		XML WSI
		XML SSL
		Datos adjuntos XML
		Error SOAP de XML
		Validación XML
		Otros
		Reputación IP
		HTTP DOS
		Ventana pequeña TCP
		Infracción de firma
		Tipo de carga de archivo
		Scripting entre sitios JSON
		JSON SQL
		JSON DOS
		Inyección de
	Secuestro de cookies	Buscador de alimentación
	Bloquear palabra clave	Comprobador de vínculos
	Palabra clave de bloqueo de JSON	Márketing
		Comercio seguro

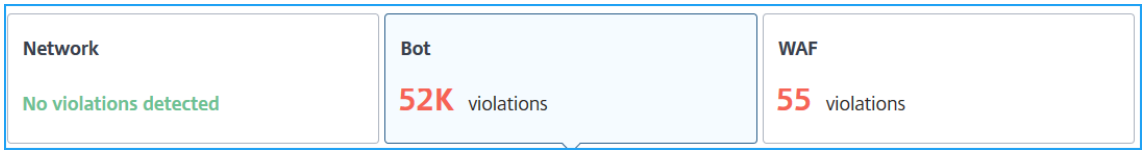
Red	WAF	Bot
		Objeto seguro
		Inyección HTML SQL
		URL de inicio
	Gramática de la inyección	
	Gramática de inyección JSON	
	SQL	

Panel de infracciones de seguridad

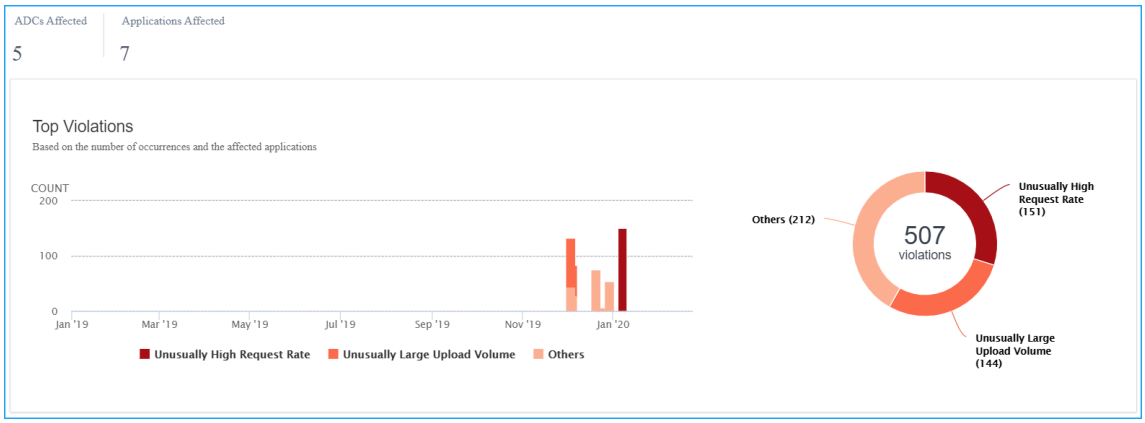
En el panel de control de infracciones de seguridad, puede ver:

- Se produjeron infracciones totales en todas las instancias y aplicaciones de NetScaler. Las infracciones totales se muestran en función de la duración de tiempo seleccionada.

- Total de infracciones en cada categoría.



- Total de instancias de NetScaler afectadas, total de aplicaciones afectadas y principales infracciones según el total de incidencias y las aplicaciones afectadas.



Detalles de infracción

Para cada infracción, NetScaler Console monitorea el comportamiento durante un período de tiempo específico y detecta infracciones para detectar comportamientos inusuales. Haga clic en cada ficha para ver los detalles de la infracción. Puede ver detalles como:

- El total de incidencias, último ocurrido y el total de aplicaciones afectadas
- En Detalles del evento, puede ver:
  - La aplicación afectada. También puede seleccionar la aplicación de la lista si dos o más aplicaciones se ven afectadas por infracciones.
  - El gráfico que indica infracciones.
  - **Acciones recomendadas** que sugieren solucionar el problema.
  - Otros detalles de infracción, como el tiempo de ocurrencia de violencia y el mensaje de detección.

Seguridad de API

January 26, 2024

Las API, o interfaces de programación de aplicaciones, son conjuntos de reglas, protocolos y herramientas que permiten que diferentes aplicaciones o sistemas de software se comuniquen entre sí. Las API desempeñan un papel importante en la protección de los datos confidenciales al hacer cumplir los controles de acceso, la autenticación y el cifrado, lo que garantiza que solo las entidades autorizadas puedan acceder a la información confidencial y transmitirla de forma segura.

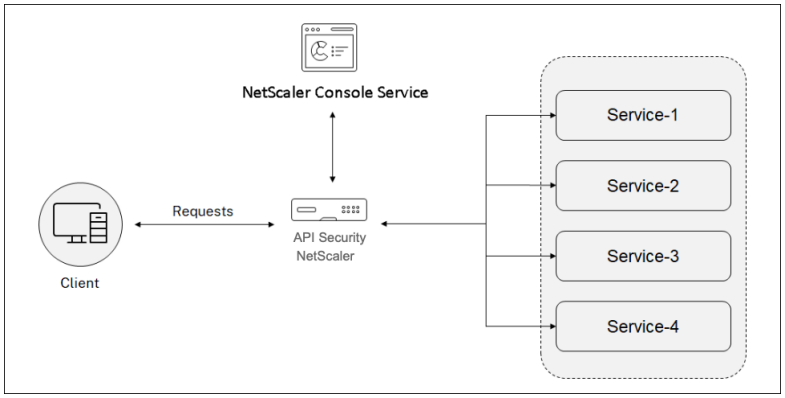
Las API funcionan como marco de backend para aplicaciones web y móviles. Por lo tanto, es fundamental proteger los datos confidenciales que transfieren. La seguridad de las API se refiere a la práctica de prevenir o mitigar los ataques a las API.

En la seguridad de las API, una puerta de enlace actúa como punto de entrada para todas las solicitudes a los puntos finales de la API. Además, garantiza un acceso seguro y confiable a todos los endpoints y microservicios de API en su sistema.

Para proteger tus API, sigue estos pasos:

- Crear o cargar una definición de API
- Implementar una instancia de API
- Agregar directivas a una implementación de API

La siguiente imagen describe cómo la seguridad de la API de NetScaler Console recibe la solicitud del cliente y envía la respuesta desde los servicios de API de fondo:



> **Nota:**
>
> En NetScaler Console, esta función está disponible para los usuarios que tienen licencias Premium o Advanced.

Ventajas de la seguridad de las API

La seguridad de la API le ofrece las siguientes ventajas:

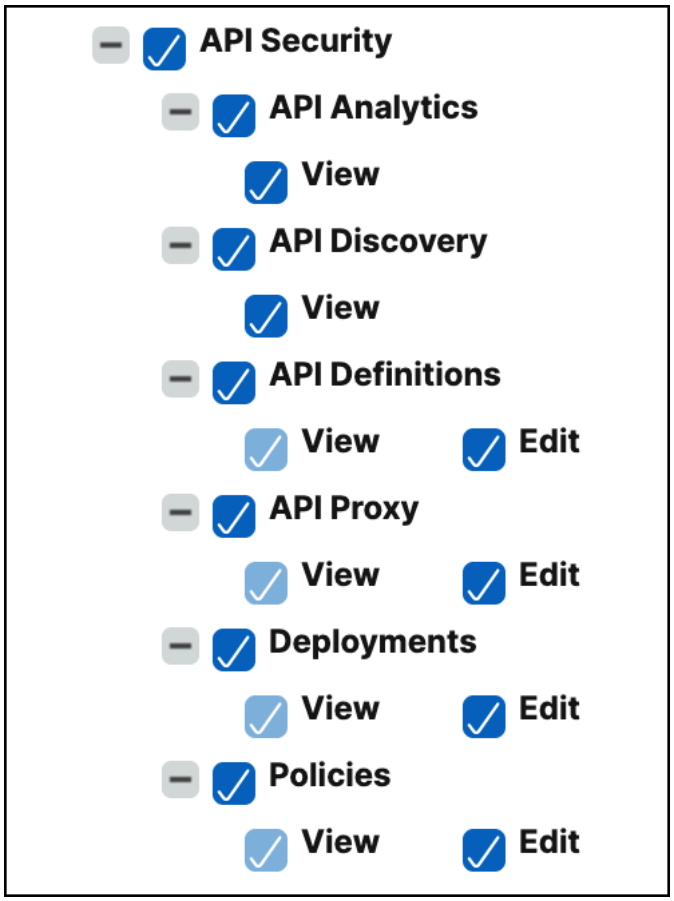
- **Protege los puntos finales de la API**: la seguridad de la API añade una capa de seguridad y protege los puntos finales de la API y los servidores API de fondo de ataques como los siguientes:
  - Desbordamiento de búfer
  - Inyección SQL
  - Scripts entre sitios
  - Denegación de servicio (Dos)
- **Supervisa y mejora el rendimiento de la API**: la seguridad de la API proporciona servicios como la descarga de SSL, la autenticación, la autorización, la limitación de velocidad y más. Estos servicios aumentan el rendimiento de la API y su disponibilidad.

  Los análisis de API le proporcionan la visibilidad de las métricas de rendimiento de la API y las amenazas a sus endpoints de API. Para obtener más información, consulte Ver análisis de la API.
- **Administra el tráfico de la API**: la seguridad de la API abstrae la complejidad de su infraestructura de API de back-end.
- **Descubre los puntos finales de la API**: la seguridad de la API descubre los puntos finales de la API que se encuentran en su organización y los agrega a la página de **detección de la API** .

Otorgue permisos de configuración y administración de API Security

Como administrador, puede crear una directiva de acceso para conceder permisos a los usuarios para la configuración y administración de API Security. Los permisos de usuario pueden ser ver, agregar, modificar y eliminar. Haga lo siguiente para conceder permisos:

1. Vaya a **Configuración > Usuario y funciones > Directivas de acceso**.
2. Haga clic en **Agregar**.
3. En **Crear directivas de acceso**, especifique un nombre de directiva y la descripción.
4. En el campo **Permisos**, expanda **Aplicaciones** y, a continuación, **Seguridad de API**.
5. Selecciona las páginas de **seguridad de la API** necesarias. A continuación, seleccione los permisos que quiere conceder.



> **Importante:**
>
> Asegúrese de conceder permisos para las funciones necesarias para utilizar una seguridad de API. Por ejemplo, si concede acceso de usuario a la página **Implementaciones**, las siguientes características también requieren acceso de usuario:

> - StyleBooks
> - IPAM
> - Equilibrio de carga (en **Funciones de red**)
> - Conmutación de contenido (en **Funciones de red**)
> - Proxy API de dispositivo (en **API**)

Para obtener más información sobre las políticas de acceso, consulte Configurar las políticas de acceso en NetScaler Console.

Aprendizaje WAF

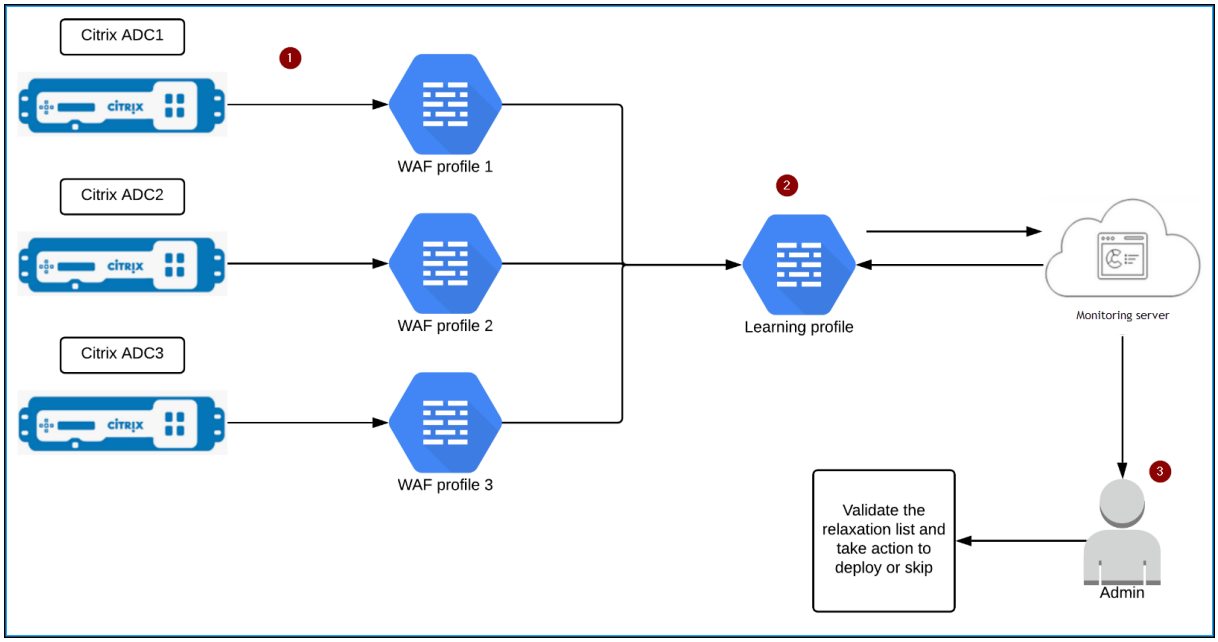
January 26, 2024

NetScaler Web App Firewall (WAF) protege sus aplicaciones web de ataques malintencionados, como la inyección SQL y las secuencias de comandos entre sitios. Para evitar infracciones de datos y proporcionar la protección de seguridad adecuada, debe supervisar su tráfico en busca de amenazas y datos accionables en tiempo real en caso de ataques. A veces, los ataques denunciados pueden ser falsos positivos y es necesario proporcionarlos como excepción.

El motor de aprendizaje de NetScaler Console es un filtro de patrones repetitivos que permite a WAF aprender el comportamiento (las actividades normales) de sus aplicaciones web. En función de la supervisión, el motor genera una lista de reglas o excepciones sugeridas para cada comprobación de seguridad aplicada al tráfico HTTP.

Es mucho más fácil implementar reglas de relajación con el motor de aprendizaje que implementarlas manualmente según las relajaciones necesarias.

La siguiente imagen explica la información de alto nivel sobre cómo funciona el aprendizaje de WAF en NetScaler Console:



1 —Instancias de NetScaler con sus perfiles WAF

2—Configure un perfil de aprendizaje en NetScaler Console, añada los perfiles WAF y seleccione la implementación automática o manual de las reglas de relajación

3—El administrador puede validar las reglas de relajación en NetScaler Console y decidir si implementarlas o omitirlas

Introducción

Para implementar la función de aprendizaje, debe:

- Habilite el aprendizaje centralizado en la instancia de NetScaler. Ejecute el siguiente comando en la instancia de NetScaler:

  ```
  set appfw settings -centralizedLearning ON
  ```

- Asegúrese de que la versión de la instancia de NetScaler sea **13.0-76.6** o posterior.
- Configure un perfil de Web App Firewall (conjunto de ajustes de seguridad) en su dispositivo NetScaler. Para obtener más información, consulte Creación de perfiles de Web App Firewall.

Tras habilitar el aprendizaje centralizado y configurar el perfil WAF, NetScaler Console genera una lista de excepciones (relajaciones) para la comprobación de seguridad configurada. Como administrador, puede revisar la lista de excepciones en NetScaler Console y decidir si implementarla o omitirla.

Con la función de aprendizaje WAF de NetScaler Console, puede:

- Configure un perfil de aprendizaje con las siguientes comprobaciones de seguridad:

- URL de inicio
- Consistencia de cookies
- Tarjeta de crédito

  > **Nota**
  >
  > Para la comprobación de seguridad de la tarjeta de crédito, debe configurar `doSecureCreditCardLogging` en la instancia de NetScaler y asegurarse de que la configuración esté **DESACTIVADA**.

- Tipo de contenido
- Consistencia de campos de formulario
- Formato de campo
- Etiquetado de formularios CSRF
- Scripts HTML entre sitios
- Inyección HTML SQL

  > **Nota**
  >
  > Para la comprobación de la inyección de HTML SQL, debe configurar `set -sqlinjectionTransformSpecialChars ON` y `set -sqlinjectiontype sqlspclcharorkeywords` en la instancia de NetScaler.

- Inyección de comandos

  > **Nota**
  >
  > Solo se admite en la instancia 13.0-72.12 de NetScaler o posterior.

- JSON SQL

  > **Nota**
  >
  > Solo se admite en la instancia 13.1-14.10 de NetScaler o en una versión posterior.

- inyección de comandos JSON

  > **Nota**
  >
  > Solo se admite en la instancia 13.1-14.10 de NetScaler o en una versión posterior.

- JSON XSS

> **Nota**
>
> Solo se admite en la instancia 13.1-14.10 de NetScaler o en una versión posterior.

- Compruebe las reglas de relajación en NetScaler Console y decida tomar las medidas necesarias (implementar o omitir)
- Recibe las notificaciones por correo electrónico, slack y ServiceNow
- Utilice la página **Resumen de Acción** para ver los detalles de relajación

Para usar el aprendizaje de WAF en NetScaler Console:

1. Configurar el perfil de aprendizaje
2. Gestiona las reglas de relajación
3. Utilizar la página Resumen de Acción de Aprendizaje WAF

Recomendaciones del WAF

January 26, 2024

El perfil de NetScaler Web App Firewall (WAF) y las firmas WAF protegen sus aplicaciones web de los ataques maliciosos. Las firmas WAF proporcionan reglas específicas y configurables para simplificar la tarea de proteger sus sitios web contra los ataques conocidos. Una firma representa un patrón que es un componente de un ataque conocido en un sistema operativo, servidor web, sitio web, servicio web basado en XML u otro recurso. Para proteger su aplicación mediante firmas, debe revisar las reglas, habilitar y configurar las que quiera aplicar.

Del mismo modo, para evitar filtraciones de datos y proporcionar la protección de seguridad adecuada en la aplicación, debe crear un perfil WAF con controles de seguridad. Al crear un perfil WAF en la instancia de NetScaler, el tráfico puede:

- Genérese con las comprobaciones de seguridad mencionadas
- No se genera con las comprobaciones de seguridad mencionadas

Es posible que la instancia esté recibiendo otros ataques, pero es posible que no hayas activado esa comprobación de seguridad en los perfiles de WAF.

Como administrador, debe comprender cómo habilitar las firmas correctas y crear los perfiles WAF correctos para proteger la aplicación web. Identificar las firmas y los perfiles WAF correctos puede ser una tarea difícil en algunos escenarios.

La recomendación WAF de NetScaler Console analiza la aplicación en busca de vulnerabilidades y genera las siguientes recomendaciones:

- Perfil WAF
- Firma WAF

Para obtener más información, consulte Perfil WAF y Firmas WAF.

La base de datos de recomendaciones de WAF se actualiza con frecuencia para incluir cualquier vulnerabilidad nueva. Puede escanear y, a continuación, seleccionar para habilitar las recomendaciones necesarias. Puede habilitar todas las firmas y comprobaciones de seguridad, pero esto podría generar falsos positivos y afectar al rendimiento de la instancia de NetScaler. Por lo tanto, se recomienda seleccionar solo las comprobaciones de seguridad y firmas necesarias. El motor de recomendaciones de WAF también detecta automáticamente qué firmas y comprobaciones de seguridad deben habilitarse para la aplicación.

> **Nota**
>
> 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).

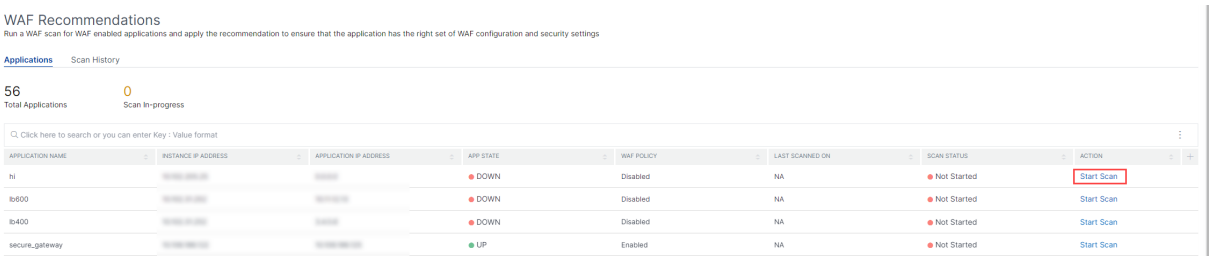
Requisitos previos

Las aplicaciones:

- Debe tener la licencia premium.
- Debe ser el servidor virtual de equilibrio de carga.

Configure los ajustes de escaneo de WAF

En NetScaler Console, vaya a **Seguridad > Recomendación de WAF** y, en **Aplicaciones**, haga clic en **Iniciar escaneo** para configurar los ajustes de escaneo de WAF para una aplicación.

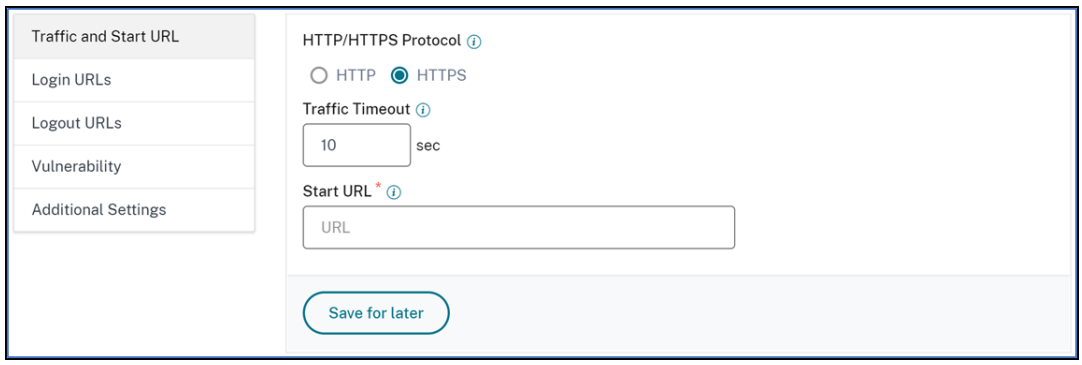


En la página de recomendaciones de la WAF:

- **Nombre de dominio**: Especifique el nombre de dominio de acceso público/acceso público que está asociado a la aplicación VIP. Por ejemplo: `www.example.com`.

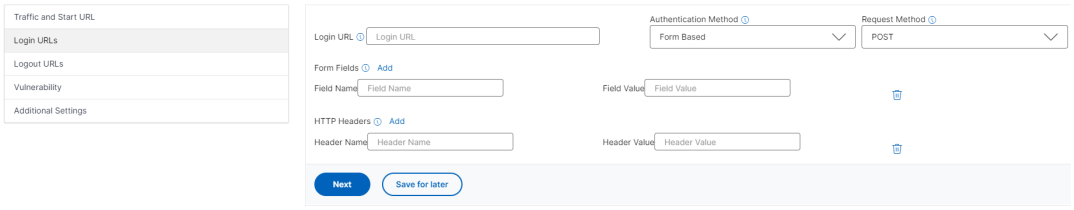
> Nota
>
> La URL inicial, la URL de inicio y la URL de cierre de sesión deben coincidir con el dominio especificado.

- **Tráfico y URL de inicio**: Proporcione los detalles de la URL de la aplicación (servidor).
  - **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 de inicio**: 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 Console.

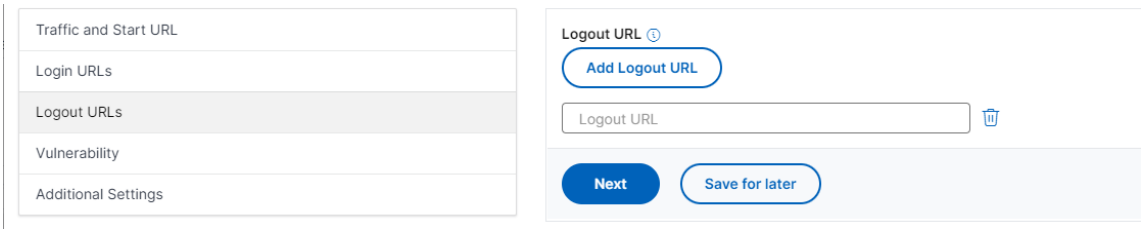


- **URL de inicio** de sesión: especifique las credenciales de inicio de sesión y las URL, si las hay, para acceder a la aplicación.
  - **URL de inicio** de sesión: URL a la que se envían los datos de inicio de sesión para la autenticación. En HTML, esta URL se conoce comúnmente como URL de acción.
  - **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.

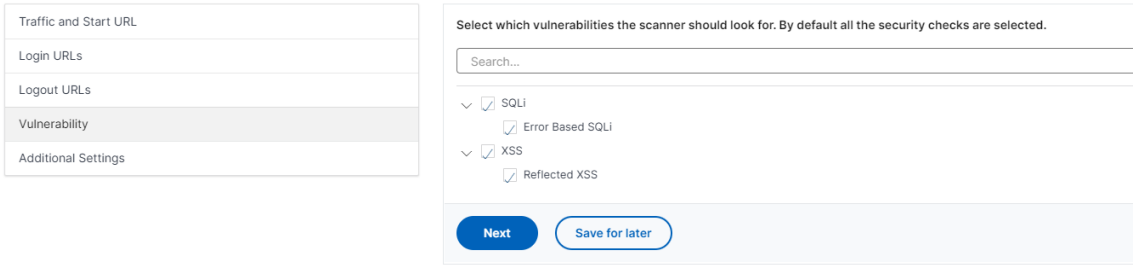
- **Método de solicitud**: Seleccione el método HTTP utilizado al enviar los datos del formulario a la URL de inicio de sesión. Los métodos de solicitud permitidos son POST, GETy PUT.
- **Campos de formulario**: Especifique los datos del formulario que se enviarán a la URL de inicio de sesión. Los campos 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 el botón Agregar para agregar varios campos de formulario. Por ejemplo, Nombre de campo (nombre de usuario) y Valor de campo (admin).
- **Encabezados HTTP: los** encabezados HTTP pueden ser necesarios para que el inicio de sesión se realice correctamente. Debe especificarlo en los pares clave-valor, donde el nombre del encabezado es la clave y el valor del encabezado es el valor. Puede hacer clic en el botón Agregar para agregar varios encabezados HTTP. Uno de los encabezados HTTP obligatorios más comunes es el encabezado Content-Type.



- **URL de cierre de sesión**: Especifique la URL que termina la sesión después de acceder a ella. Por ejemplo: `https://www.example.com/customer/logout`.

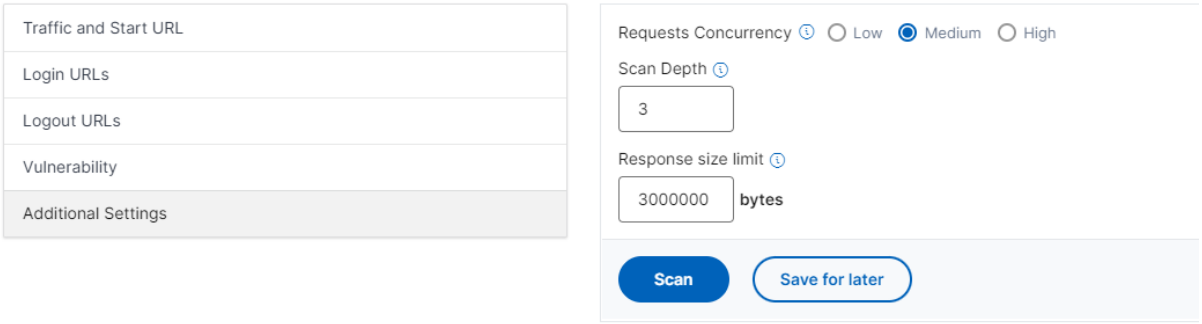


- **Vulnerabilidad**: Seleccione las vulnerabilidades para que el analizador las detecte. Actualmente, esto se hace por la inyección de SQL y las infracciones de scripts entre sitios. De forma predeterminada, se seleccionan todas las infracciones. Tras seleccionar las vulnerabilidades, simula estos ataques 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.



- **Parámetros adicionales**
  - **Simultaneidad** de solicitudes: el total de solicitudes enviadas a la aplicación web en paralelo.
  - **Profundidad de escaneo**: Profundidad de la aplicación web hasta la que debe continuar el escaneo. Por ejemplo, para una profundidad de escaneo de valor 2, se escanean la URL de inicio y todos los enlaces que se encuentran en esta URL. Debe especificar un valor igual o superior a 1.
  - **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 3 MB (300000 bytes).

La configuración de los ajustes de escaneo del WAF está completa. Puede hacer clic en **Escanear** para iniciar el proceso de escaneo o puede hacer clic en **Guardar para más adelante para** guardar las configuraciones y escanear más adelante.



Proceso de recomendación de escaneo WAF

Al iniciar el escaneo, el motor de recomendaciones del WAF:

- Escanea la aplicación web proporcionada a través de la URL proporcionada.
- Inspecciona la aplicación web para descubrir las tecnologías utilizadas por la aplicación web.
- Simula los ataques de seguridad a la aplicación web para detectar posibles vulnerabilidades.
- Recomienda firmas basadas en las tecnologías web detectadas.

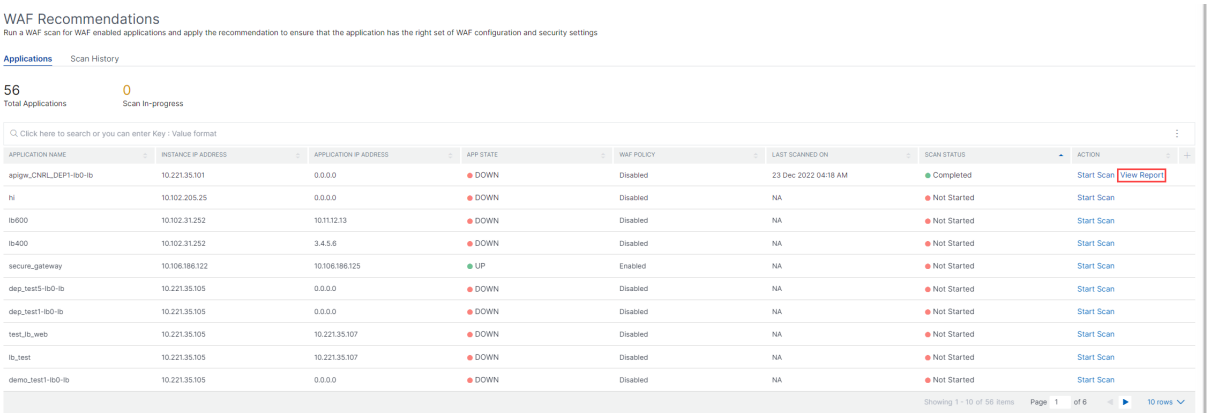
- Recomienda realizar comprobaciones de seguridad basadas en las vulnerabilidades encontradas y en el análisis del tráfico.
- Analiza las respuestas de las aplicaciones web para generar configuraciones más detalladas.

Se admiten las siguientes comprobaciones de seguridad:

- Desbordamiento de búfer
- Formato de campo
- Tarjeta de crédito
- Consistencia de cookies
- Inyección HTML SQL
- Secuencias de comandos HTML entre sitios
- Consistencia de campos de formulario
- Etiquetado de formularios CSRF

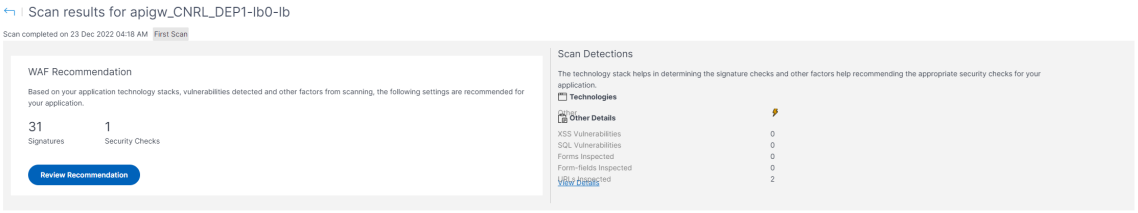
Ver informe de escaneo

Una vez finalizado el escaneo, haga clic en **Ver informe** para ver los resultados.



El resultado del análisis proporciona:

- **Recomendación de WAF**: Le permite ver el resumen del total de firmas y comprobaciones de seguridad recomendadas para la aplicación.
- **Detecciones de escaneo**: Le permite ver la recopilación de información, como las tecnologías y los detalles de las infracciones realizadas en la aplicación. Haga clic en **Ver detalles** para ver la información sobre las detecciones y otros detalles del análisis.



En **Recomendación de WAF**, haga clic en **Revisar recomendación** para ver los detalles de las **comprobaciones de seguridad** y **las firmas**.

La configuración de seguridad recomendada sugiere las comprobaciones de seguridad y las firmas recomendadas para la aplicación. Puede modificar las recomendaciones de la lista y hacer clic en **Ver o modificar** para ver los detalles o modificar los cambios según los requisitos. La opción Restablecer la configuración predeterminada restablece todos los cambios realizados y vuelve a las recomendaciones originales.

Tras revisar los detalles, haga clic en **Aplicar recomendación**. Las recomendaciones se configuran mediante los StyleBooks. Debe asegurarse de aplicar la recomendación en las fichas **Comprobaciones de seguridad** y **Firma** por separado.

Se recomienda aplicar primero las firmas y, a continuación, las comprobaciones de seguridad. Esto vincula las firmas al perfil automáticamente.

Cuando apliques las firmas correctamente:

- La configuración se aplica en la instancia de NetScaler a través del `appfw-import-object` StyleBook.
- El archivo de firmas con las recomendaciones configuradas se importa en la instancia de NetScaler.

> **Nota**
>
> Las firmas se admiten en NetScaler 13.0 o en una versión posterior.

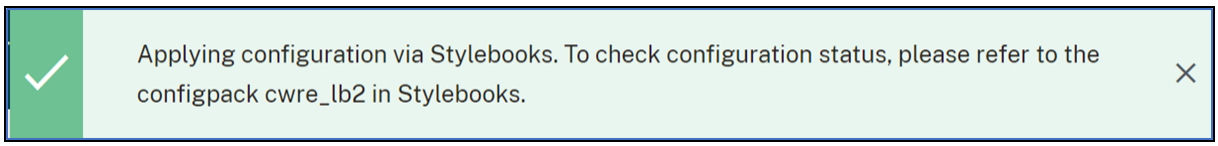
Antes de proceder a aplicar las recomendaciones de la **comprobación de seguridad**, vaya a **Aplicaciones > Configuración > Paquetes de configuración** y asegúrese de que el paquete de configuración de firmas se haya creado correctamente.

Si aplica correctamente las comprobaciones de seguridad:

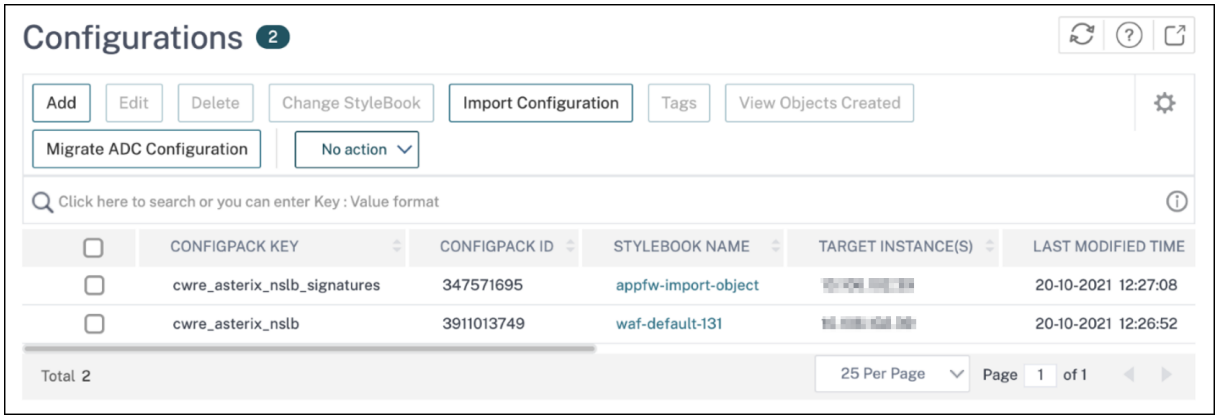
- La configuración se aplica en la instancia de NetScaler a través de StyleBooks, según la versión de NetScaler. Para NetScaler 13.0 , `waf-default-130`se usa StyleBook y para NetScaler 13.1, `waf-default-131`se usa Stylebook.
- El perfil `Appfw` se crea en NetScaler y se enlaza a la aplicación mediante `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.

Tras aplicar la recomendación (comprobaciones de seguridad y firmas), puede ver el siguiente mensaje de confirmación:



Para comprobar que los perfiles y las firmas WAF se aplican a través de los StyleBooks predeterminados, vaya a **Aplicaciones > Configuración > Paquetes de configuración**.



Gateway Insight

March 6, 2024

En una implementación de NetScaler Gateway, la visibilidad de un detalle de acceso de 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 quiere conocer la actividad del usuario y los motivos del error de inicio de sesión, pero esa información normalmente no está disponible a menos que el usuario envíe una solicitud de resolución.

Gateway Insight proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, en el momento de iniciar sesión en 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 el número de aplicaciones iniciadas, el número de sesiones totales y activas, el número de bytes totales y el ancho de banda consumidos por las aplicaciones. Puede ver los detalles de los usuarios, las sesiones, el ancho de banda y los errores de inicio de una aplicación.

Puede ver 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 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 de NetScaler Console, por lo que puede ver los detalles de los errores en 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 a tener en cuenta:

- Gateway Insight se admite en las siguientes implementaciones:
  - Access Gateway
  - Unified Gateway

- La versión y la compilación de NetScaler Console 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. Se requiere una licencia Premium 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.
- 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).
- No se incluyen los registros de Gateway Insight para la autenticación SAML.
- 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
  - OAuth

Habilitar Gateway Insight

Para habilitar Gateway Insight para su dispositivo NetScaler Gateway, primero debe agregar el dispositivo NetScaler Gateway a NetScaler Console. A continuación, debe habilitar AppFlow para el servidor virtual que representa la aplicación VPN. Para obtener información sobre cómo agregar un dispositivo a NetScaler Console, consulte Agregar instancias.

> **Nota**
>
> Para ver los errores del análisis de punto final (EPA) en NetScaler Console, debe habilitar el registro de nombres de usuario de autenticación, autorización y control de acceso de AppFlow en el dispositivo NetScaler Gateway.

Habilite AppFlow para un servidor virtual en NetScaler Console

1. Vaya a **Configuración > Configuración de licencias y análisis**.
2. En **Resumen de análisis de servidores virtuales**, haga clic en **Configurar análisis**.
3. En la página **Todos los servidores virtuales**, seleccione el servidor virtual NetScaler Gateway y haga clic en **Habilitar seguridad y análisis**.
4. Seleccione **Gateway Insight**.
5. Haga clic en **Guardar**.

Habilite el registro de nombres de usuario de AppFlow 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 informes de Gateway Insight

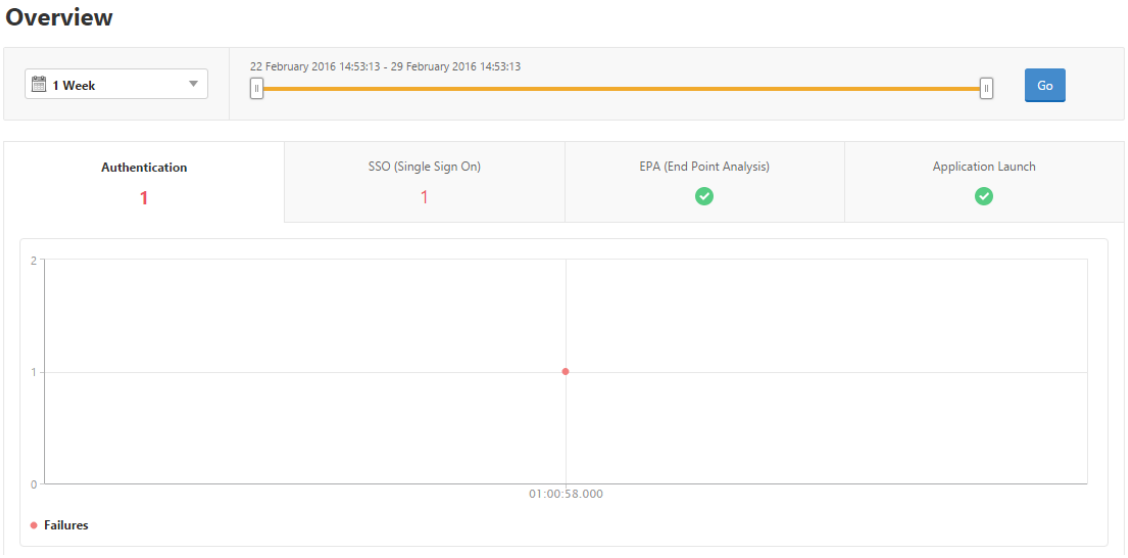
En NetScaler Console, puede ver los informes de todos los usuarios, aplicaciones y puertas de enlace asociados a los dispositivos NetScaler Gateway, y puede ver los detalles de un usuario, una aplicación o una puerta de enlace en particular. En la sección **Descripción general**, puede ver los errores 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. Los análisis de NetScaler Console ahora admiten 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 en NetScaler Console.

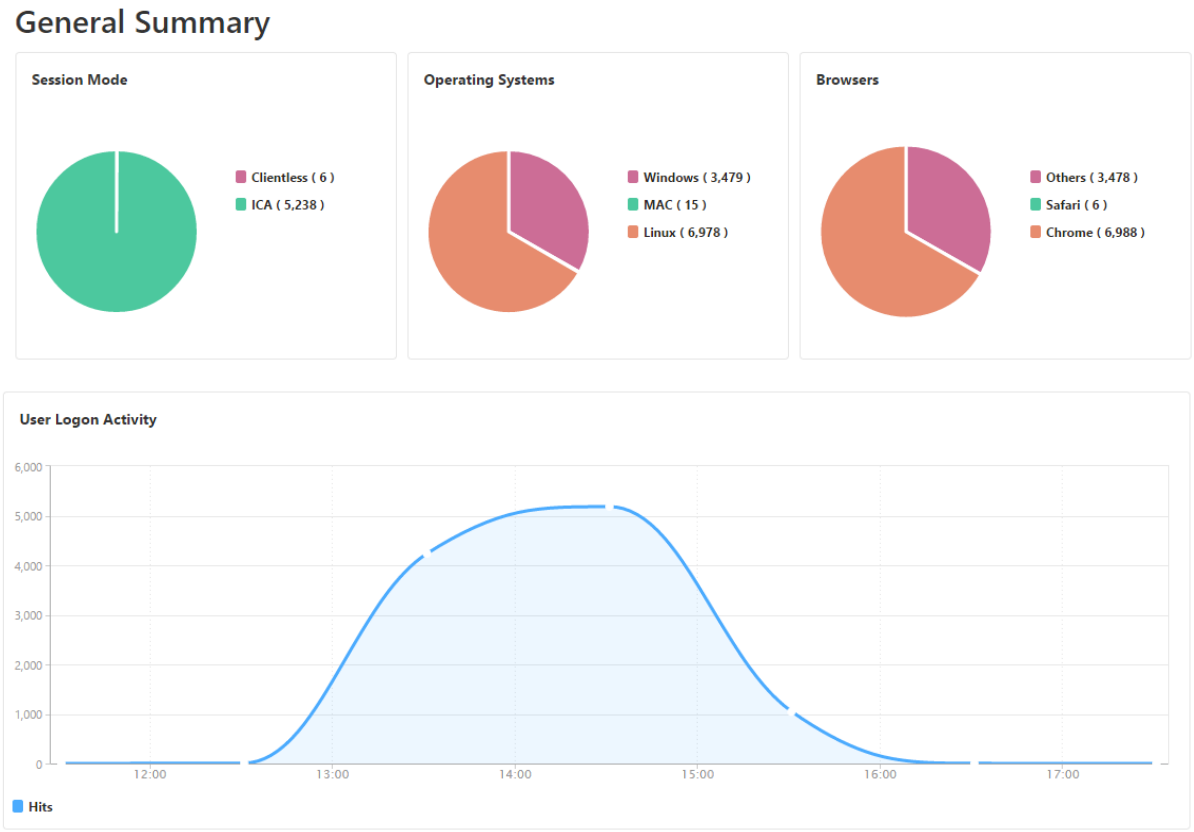
Ver errores de EPA, inicio de sesión único, autenticación, autorización y inicio de aplicaciones

1. En NetScaler Console, 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.



Ver resumen de los modos de sesión, los clientes y el número de usuarios

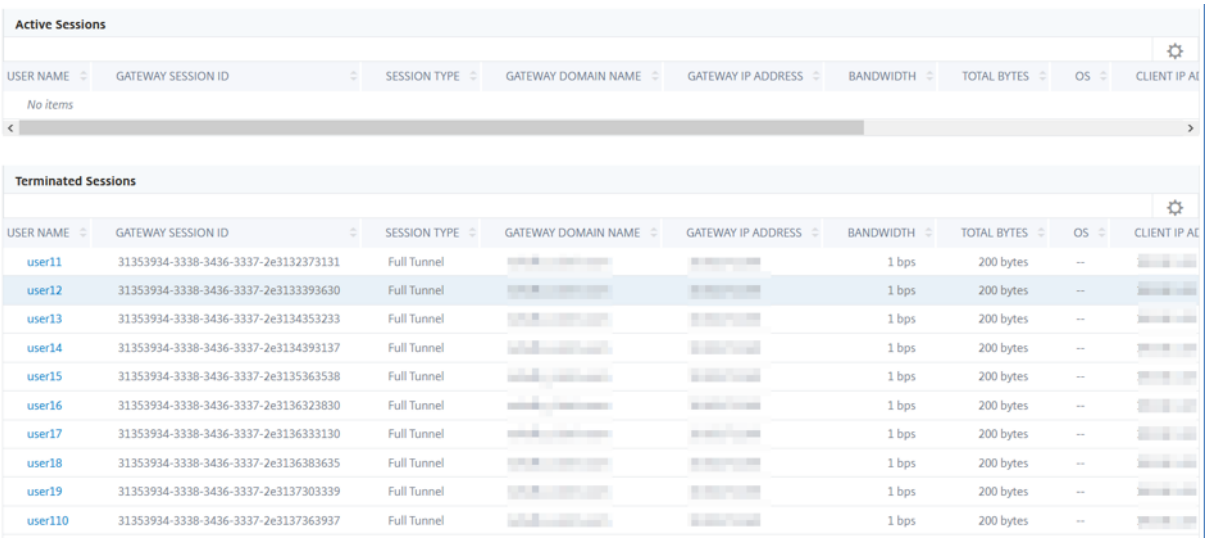
En NetScaler Console, vaya a **Gateway > Gateway Insight** y desplácese hacia abajo para ver los informes.



Usuarios

Puede ver un informe completo de los usuarios asociados a los dispositivos NetScaler Gateway. Puede ver la EPA, la autenticación, el inicio de sesión único, los errores de inicio de la aplicación, etc. de un usuario.

También puede visualizar una vista consolidada de todas las sesiones activas y terminadas de los usuarios.

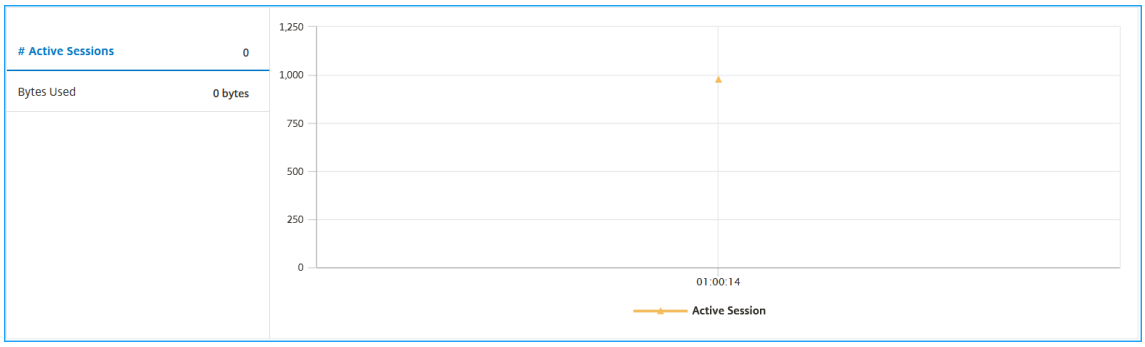


Como administrador, esta vista le permite:

- Ver todos los detalles de los usuarios en una visualización de un solo panel
- Elimine la complejidad de seleccionar cada usuario y ver las sesiones activas y terminadas

Ver detalles del usuario

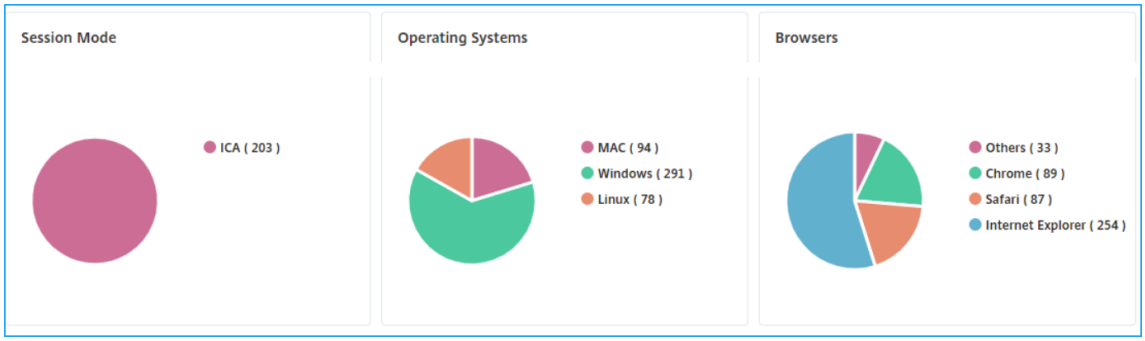
1. En NetScaler Console, vaya a **Gateway > Gateway Insight > Users** .
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Puede ver el número de usuarios activos, el número de sesiones activas y bytes de todos los usuarios durante el período de tiempo.



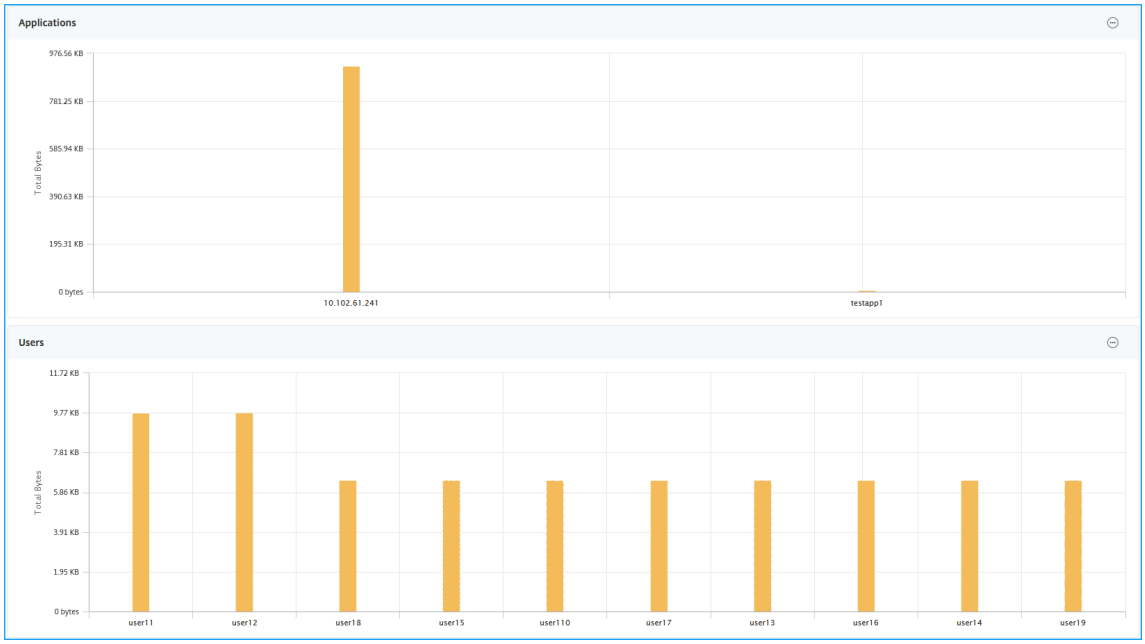
Desplácese hacia abajo para ver una lista de usuarios disponibles y usuarios activos.

En la ficha **Usuarios** o **Usuarios activos**, haga clic en un usuario para ver los siguientes detalles de usuario:

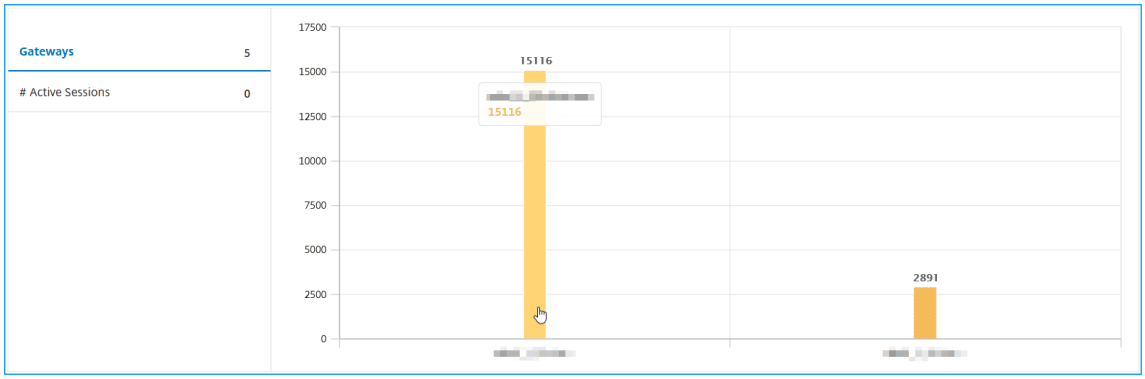
- **Detalles**del usuario : puede ver la información de cada usuario asociado a los dispositivos NetScaler Gateway. Vaya a **Gateway** > **Gateway Insight** > **Usuarios** y haga clic en un usuario para ver las perspectivas del usuario seleccionado, como el modo de sesión, el sistema operativo y los exploradores.



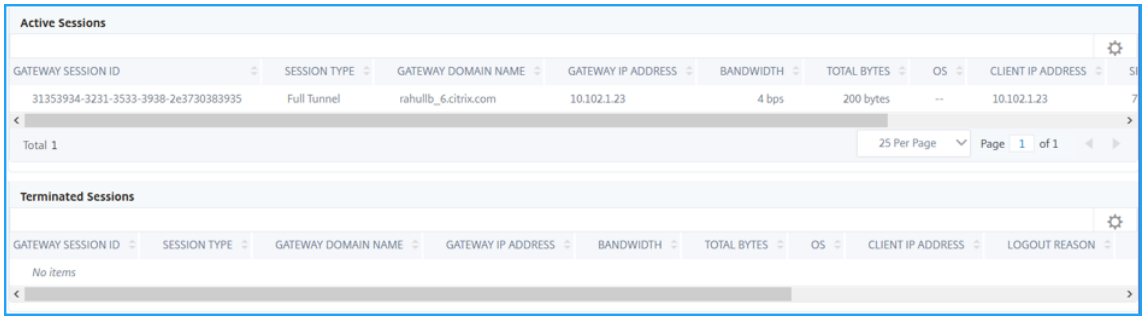
- **Usuarios y aplicaciones para la puerta de enlace seleccionada**: vaya a Puerta de **enlace > GatewayInsight**>**Puerta de enlace** y haga clic en el nombre de dominio de una puerta de enlace para ver las 10 aplicaciones principales y los 10 usuarios principales que están asociados a la puerta de enlace seleccionada.



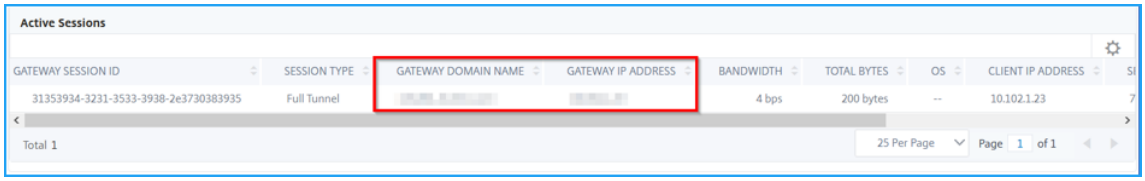
- **Ver más opción para aplicaciones y usuarios**: para más de 10 aplicaciones y usuarios, puede hacer clic en el icono más en Aplicaciones y Usuarios para ver todos los detalles de usuarios y aplicaciones asociados a la puerta de enlace seleccionada.
- **Ver detalles haciendo clic en el gráfico de barras**: 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



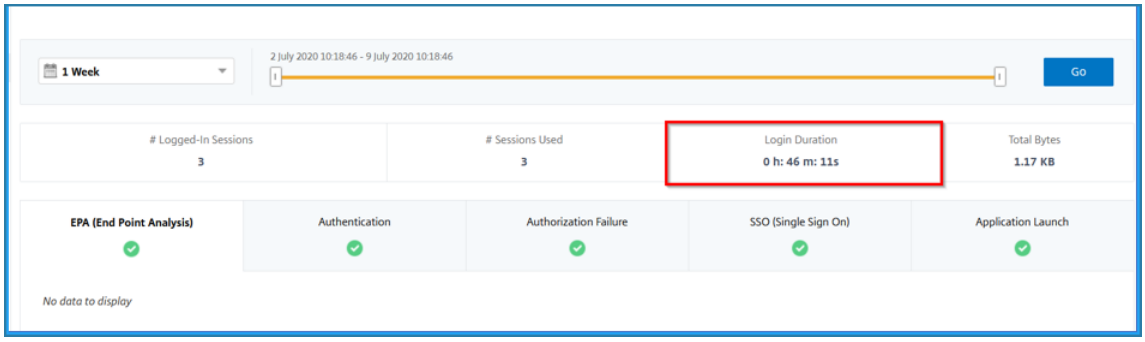
- El usuario **Sesiones Activas y SesionesTerminadas**.



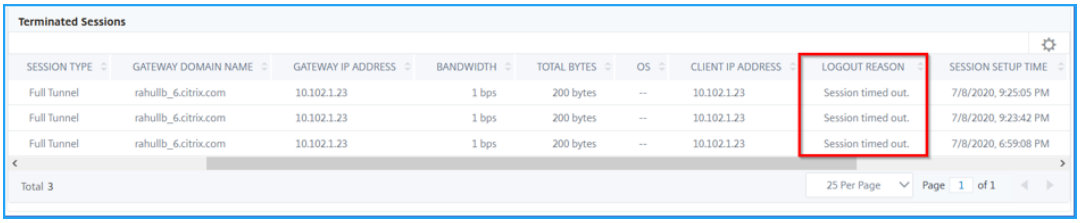
- El nombre del dominio de puerta de enlace y la dirección IP de la puerta de **enlace en Sesiones**



- 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



Barra de búsqueda y vista de mapa geográfico

Podrá ver lo siguiente:

- Barra de búsqueda que permite filtrar los resultados en función del nombre de usuario. Vaya a **Gateway > Gateway Insight > Usuarios** para ver la barra de búsqueda de **usuarios** y **usuarios activos**. Coloque el puntero del mouse en la barra de búsqueda, seleccione **Nombre de usuario**y escriba un nombre de usuario para filtrar los resultados.

- Mapa geográfico que muestra la información de los usuarios en función de la ubicación geográfica de los usuarios. Como administrador, este mapa geográfico le permite ver el resumen del total de usuarios, el total de aplicaciones y el total de sesiones de una ubicación específica.

  1. Vaya a **Gateway > Gateway Insight** para ver el mapa geográfico
  2. Haga clic en un país. Por ejemplo, Estados Unidos

     El mapa geográfico muestra los detalles como la lista de usuarios, las sesiones activas, las sesiones terminadas y las aplicaciones para el país seleccionado.

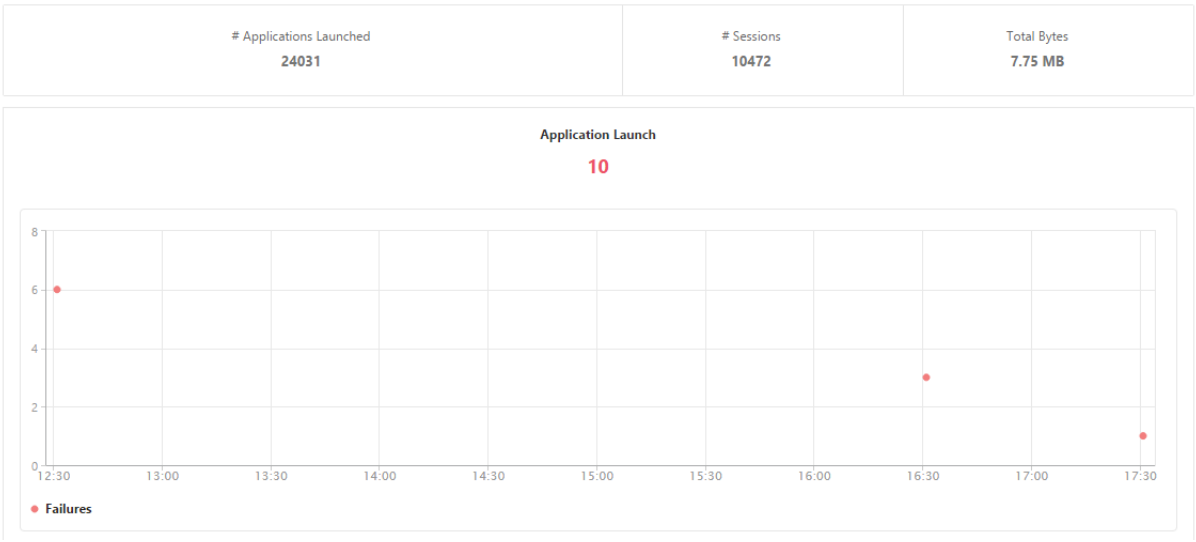
Aplicaciones

Puede ver el número de aplicaciones iniciadas, el número de sesiones totales y activas, el número de bytes totales 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.

Ver detalles de la aplicación

1. En NetScaler Console, vaya a **Gateway > Gateway Insight > Applications** .
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 iniciadas, el número de sesiones totales y activas, el número de bytes totales 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.

Puertas de enlace

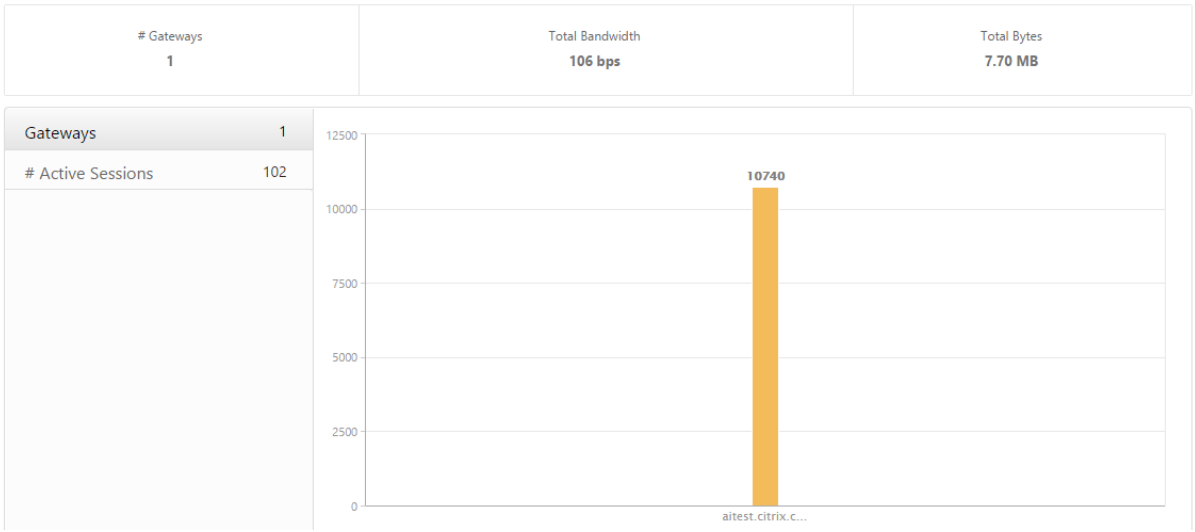
Puede ver la cantidad de puertas de enlace, la cantidad de sesiones activas, el total de bytes y el ancho de banda utilizados por todas las puertas de enlace asociadas a un dispositivo NetScaler Gateway en un momento dado. Puede ver los errores de EPA, autenticación, inicio de sesión único y lanzamiento 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.

Ver detalles de la puerta de enlace

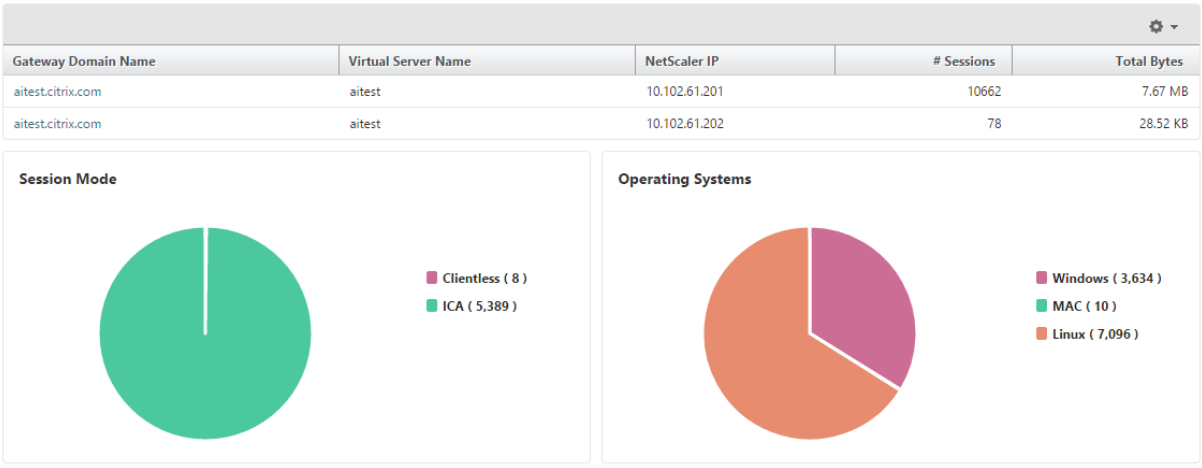
1. En NetScaler Console, vaya a **Gateway > Gateway Insight > Gateways** .

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 a 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.

También puede ver un mapa geográfico para puertas de enlace que le permite filtrar usuarios en función de una ubicación determinada.

1. Vaya a **Gateway > Gateway Insight > Gateways**
2. Seleccione un nombre de dominio de puerta de enlace para ver el mapa geográfico
3. Haga clic en un país. Por ejemplo, Estados Unidos

   El mapa geográfico muestra los detalles como la lista de usuarios, las sesiones activas, las sesiones terminadas y las aplicaciones para el país seleccionado.

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 solo se exportan si la consola de NetScaler tiene conectividad a Internet.

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 modificar el programa de exportación:

1. En la ficha Configuración, vaya a **Configuración** > **NetScaler Insight Center** > **Exportar programas**.
2. Seleccione un informe de la lista disponible y, a continuación, haga clic en **Modificar**.
3. Tras la edición, haga clic en **Guardar**.

> **Nota**
>
> Configure los ajustes del servidor de correo electrónico antes de programar el informe. Para ello, vaya a **Sistema** > **Notificaciones** > **Correo electrónico** y haga clic en **Agregar**.

Para agregar un servidor de correo electrónico o una lista de distribución de correo electrónico:

1. En la ficha **Configuración**, vaya a **Sistema** > **Notificaciones** > **Correo electrónico**.
2. En el panel derecho, seleccione Servidor de **correo electrónico para agregar un servidor**de correo electrónico o seleccione Lista de **distribución de correo electrónico para crear una lista** de distribución de correo electrónico.
3. Especifique los detalles y haga clic en **Crear**.

Para exportar todo el panel de Gateway Insight:

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Exportar ahora**, seleccione Formato **PDF** y, a continuación, haga clic en **Exportar**.

Casos de uso de Gateway Insight

Los siguientes casos de uso muestran cómo puede usar Gateway Insight para obtener visibilidad de los detalles de acceso, las aplicaciones y las puertas de enlace de los usuarios en los dispositivos NetScaler Gateway.

1. El usuario no puede iniciar sesión en el dispositivo NetScaler Gateway ni en los servidores web internos

Es un administrador de NetScaler Gateway que supervisa los dispositivos NetScaler Gateway a través de NetScaler Console y desea saber por qué un usuario no puede iniciar sesión o en qué fase del proceso de inicio de sesión se ha producido el error.

NetScaler Console 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 Console, puede buscar un usuario concreto y, a continuación, ver todos los detalles de ese usuario.

Para buscar un usuario:

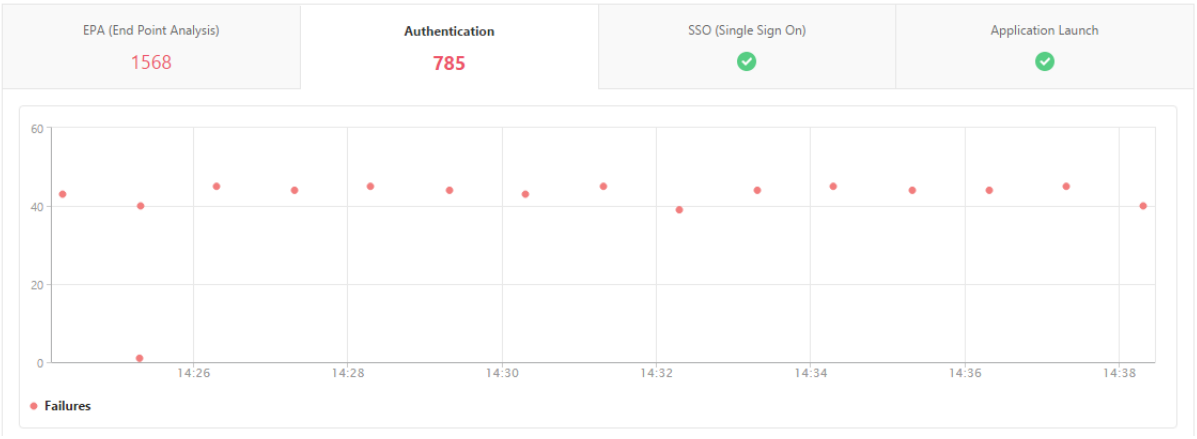
En NetScaler Console, vaya a **Gateway > Gateway Insight** y, en el cuadro de texto **Buscar usuarios**, especifique el usuario que desea buscar.

Fallos de autenticación

Puede ver errores de autenticación, como credenciales incorrectas o ninguna respuesta del servidor de autenticación. Si ha configurado la autenticación en dos etapas, puede ver si han fallado las etapas principal, secundaria o ambas de la autenticación.

Ver los detalles del error de autenticación

1. En NetScaler Console, 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 en qué etapa de una autenticación en dos etapas se produjo el error.

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de autenticación y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas mediante la opción de configuración.

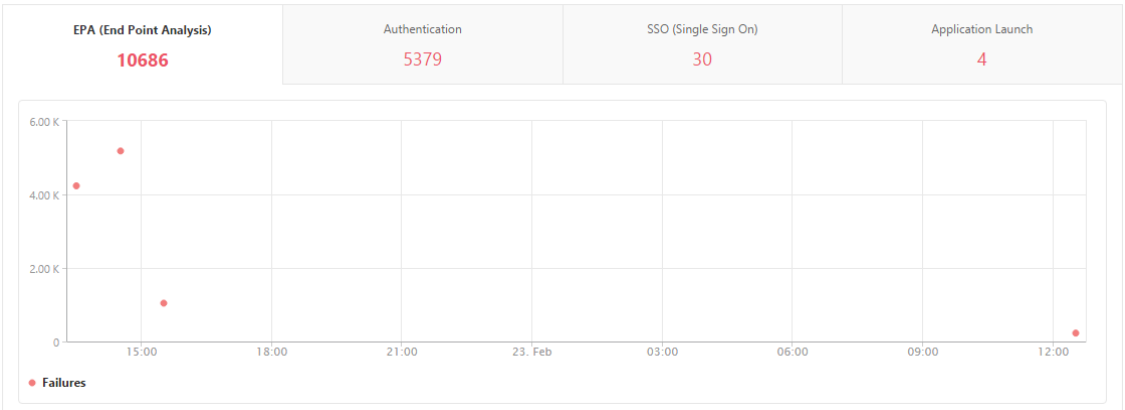
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

Fallas de EPA

Puede ver las fallas de la EPA antes o después de la autenticación.

Ver detalles de fallas de la EPA

1. En NetScaler Console, 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**.

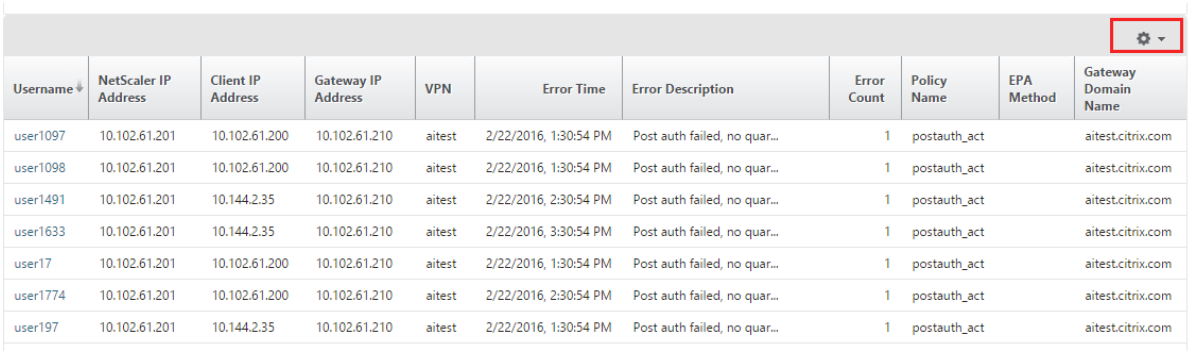


Desplázate hacia abajo para ver los detalles de cada error de la EPA, como el nombre de **usuario, la dirección IP de NetScaler, la dirección IP de Gateway, la VPN, el tiempo de error, el nombre de la**

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 error EPA y la columna **Nombre de la directiva** muestra la directiva que dio lugar al error.

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 opción de configuración.



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

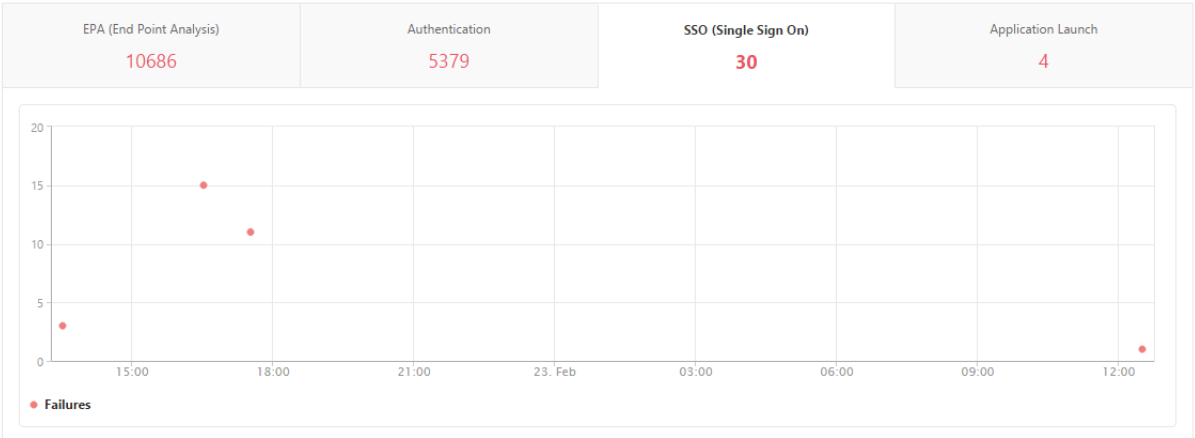
> **Nota**
>
> NetScaler Gateway no informa de los errores de la EPA cuando la expresión «ClientSecurity» está configurada como una regla de directiva de sesión de VPN.

Fallos 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.

Ver detalles de los errores de SSO

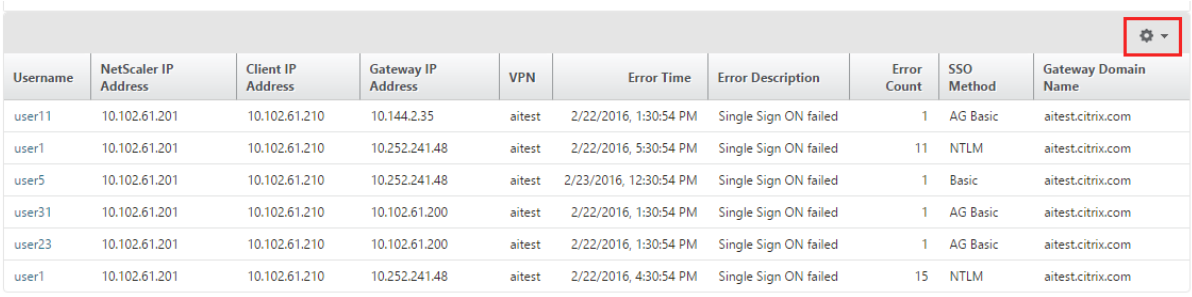
1. En NetScaler Console, vaya a **Gateway Gateway Insight**.
2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.
3. 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.

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 opción de configuración.



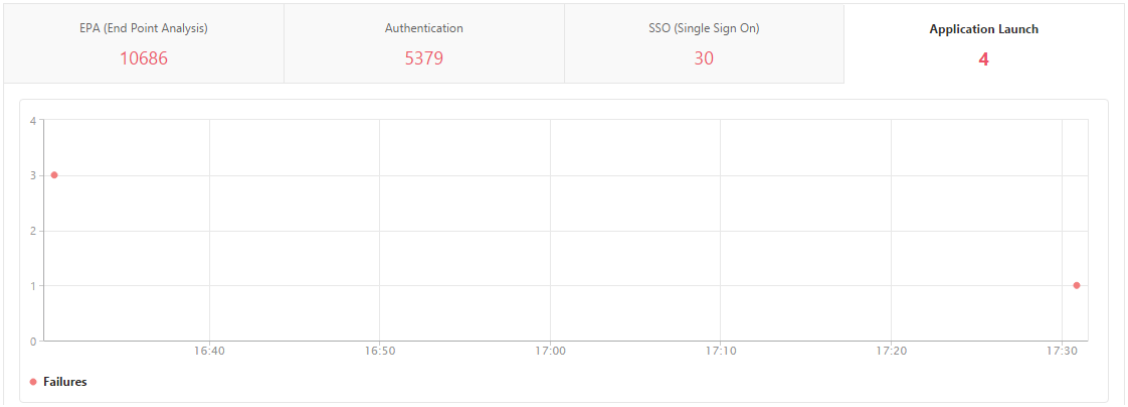
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	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

2. 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.

Ver detalles del error al iniciar la aplicación

1. En NetScaler Console, 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**.

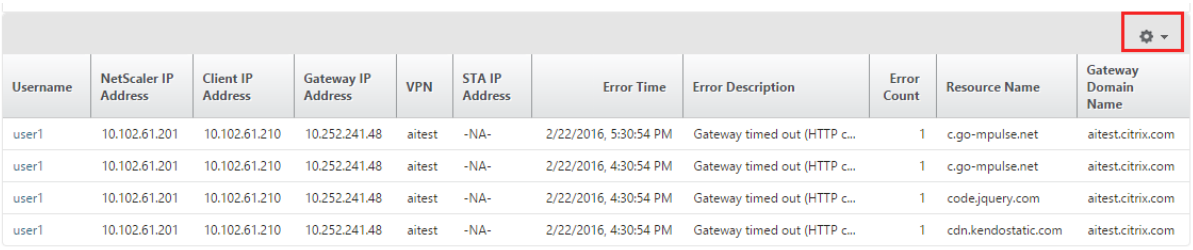
3. Haga clic en la ficha **Inicio de la aplicación**. Puede ver el número de errores de inicio de la aplicación en un momento dado en el gráfico **Fallos**.



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.

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 opción de configuración.



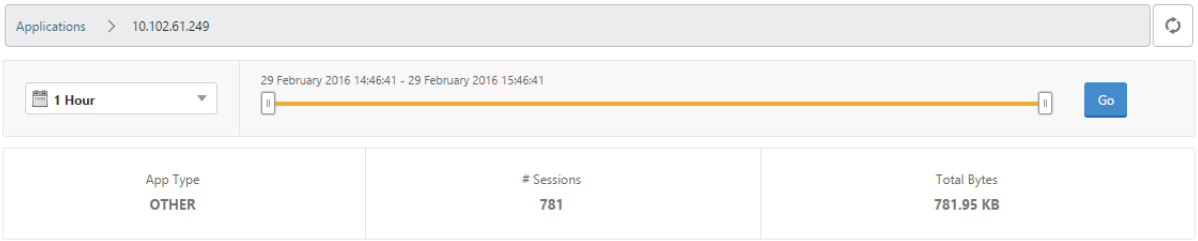
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
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

3. Después de iniciar correctamente una nueva aplicación, un usuario quiere ver el total de bytes y ancho de banda consumidos por esa aplicación Una vez que haya lanzado correctamente una nueva aplicación, en NetScaler Console, podrá ver el total de bytes y ancho de banda consumidos por esa aplicación.

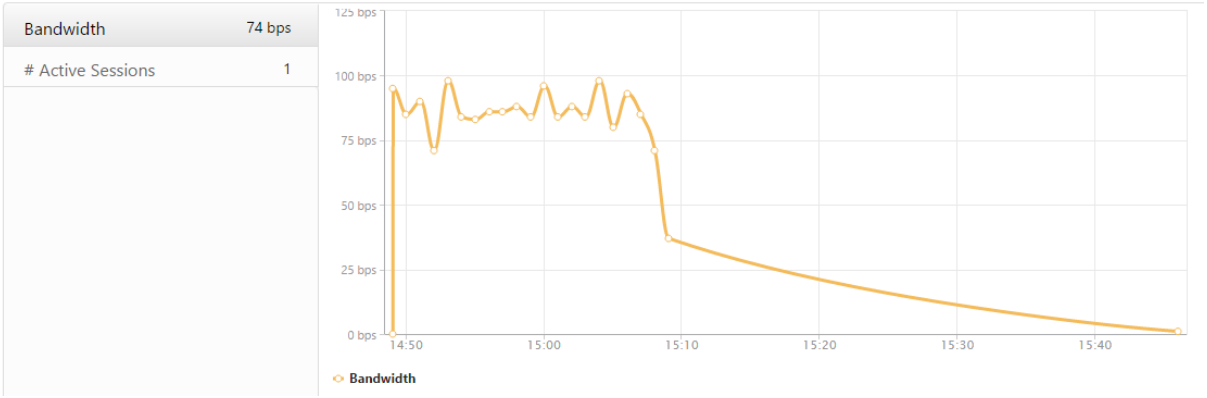
Ver el total de bytes y ancho de banda consumidos por una aplicación

En NetScaler Console, vaya a **Gateway > Gateway Insight Aplicaciones**, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, haga clic en la aplicación de la que desea ver los detalles.

Puede ver el número de sesiones y el número total de bytes consumidos por esa aplicación.



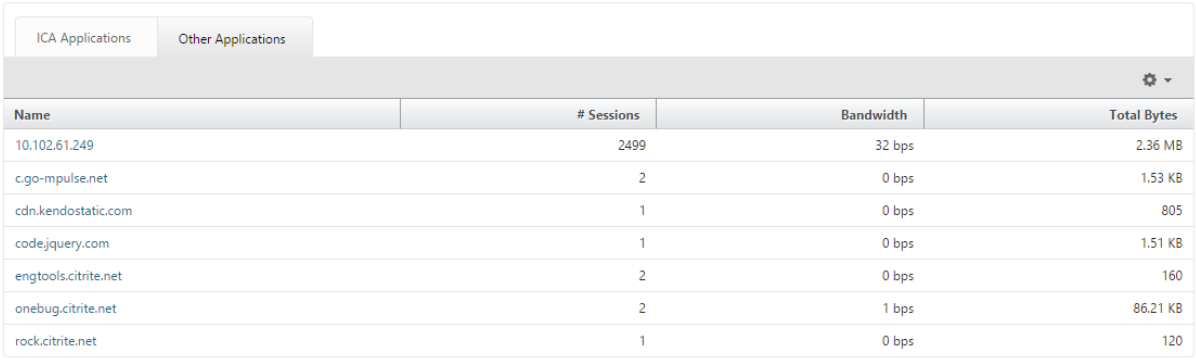
También puede ver el ancho de banda consumido por esa aplicación.



4. 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.

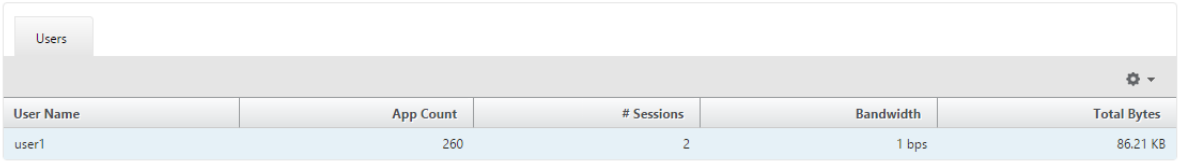
Ver el acceso de los usuarios a los recursos

1. En NetScaler Console, 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

En la pantalla que aparece, desplácese hacia abajo y, en la tabla **Usuarios**, se muestran todos los usuarios que tienen acceso a esa aplicación.

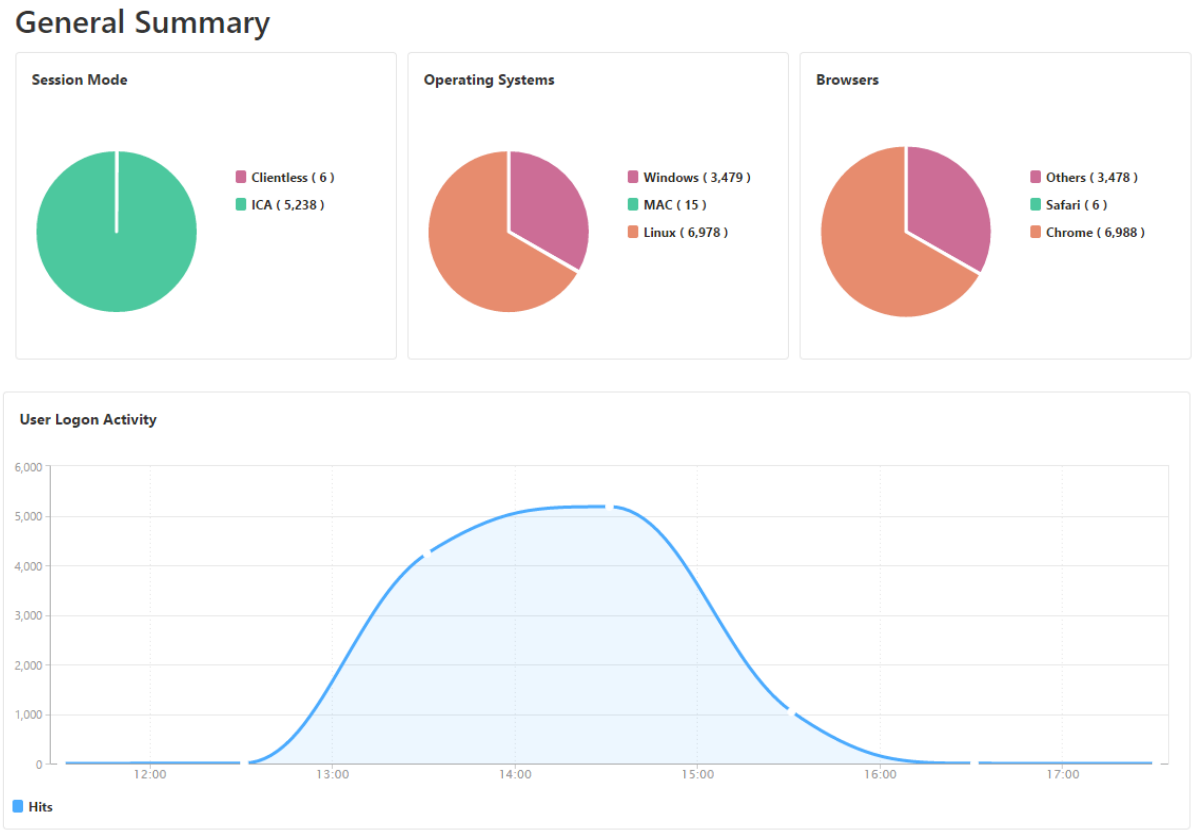


User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. 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.

Ver un resumen de los modos de sesión, el tipo de clientes y el número de usuarios que han iniciado sesión

1. En NetScaler Console, 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.



HDX Insight

January 26, 2024

HDX Insight proporciona una visibilidad integral del tráfico de HDX a Citrix Virtual Apps and Desktops 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 que NetScaler Console sea compatible con una amplia variedad de casos de uso.

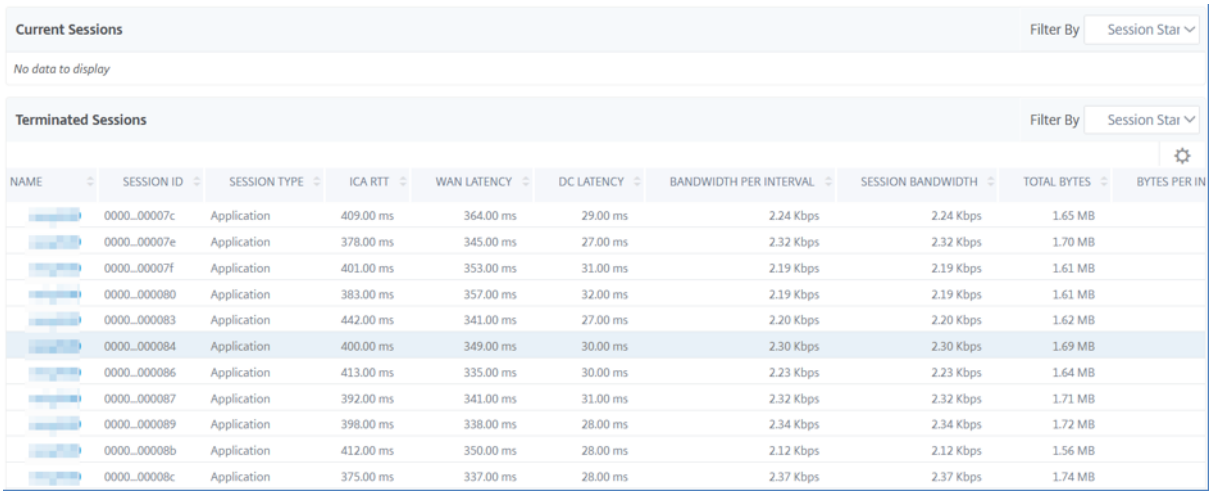
Para que aparezca cualquier dato, debe habilitar AppFlow en sus servidores virtuales de NetScaler Gateway. AppFlow se puede entregar mediante el protocolo **IPFIX** o el método **Logstream**.

> **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 de ancho de banda de canales virtuales individuales, como el audio, la asignación de impresoras y la asignación de unidades de cliente.

También puede visualizar una vista consolidada de todas las sesiones activas y terminadas de los usuarios.



Como administrador, esta vista le permite:

- Ver todos los detalles de los usuarios en una visualización de un solo panel
- Elimine la complejidad de seleccionar cada usuario y ver las sesiones activas y terminadas

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso de nivel de aplicación al grupo y asignar usuarios al grupo. Los análisis de NetScaler Console ahora admiten 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 Configuración de grupos en NetScaler Console.

También puede ir a **HDX Insight** > **Aplicaciones** y hacer clic en **Duración del lanzamiento** para ver el tiempo que tarda en iniciarse la aplicación. También puede ver el agente de usuario de todos los usuarios conectados navegando a **HDX Insight > Usuarios**.

> **Nota** HDX insight admite particiones de administración configuradas en instancias de NetScaler que se ejecutan en la versión de software 12.0.

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

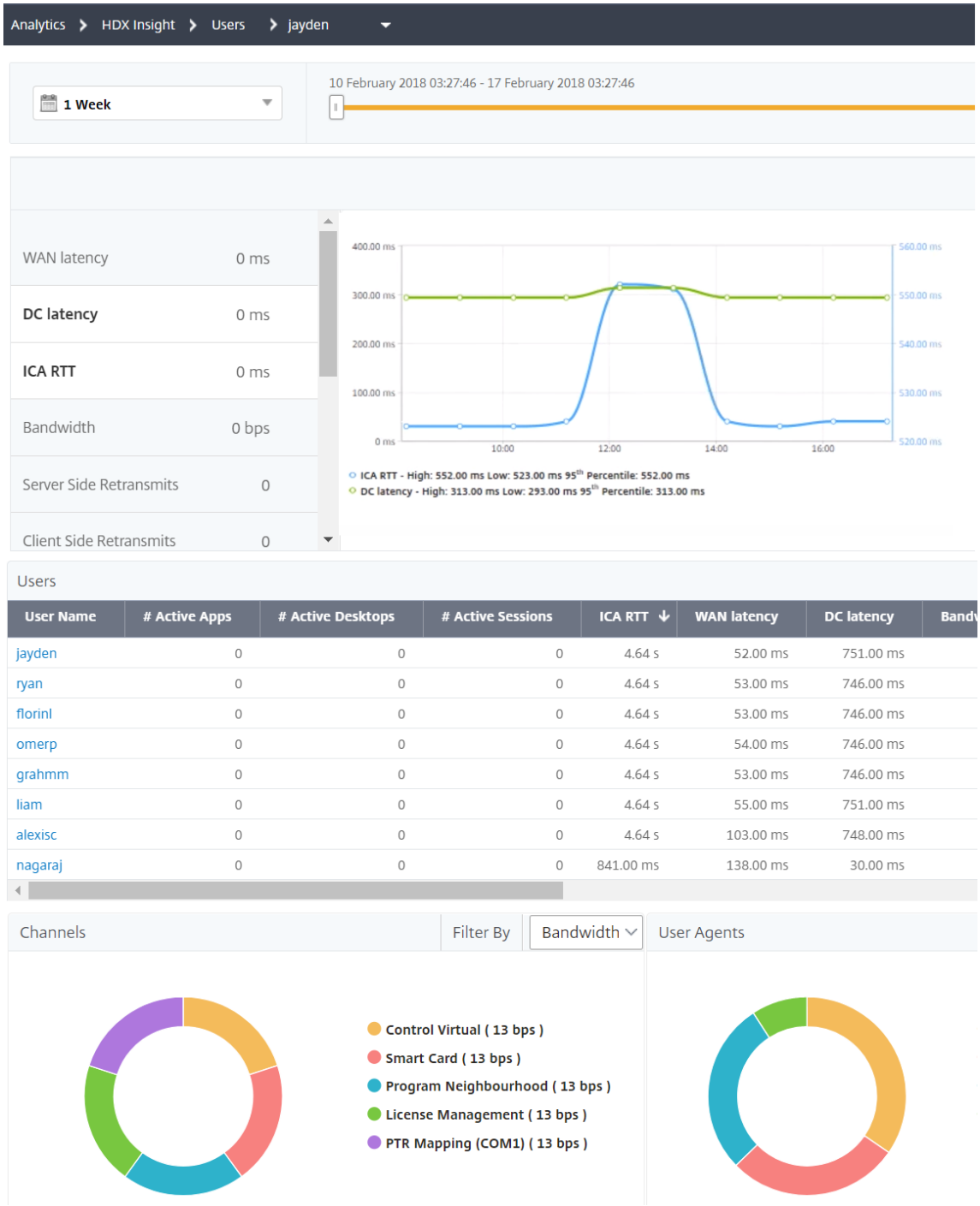
El usuario experimenta retrasos al acceder a Citrix Virtual Apps and Desktops Los retrasos pueden deberse a la latencia en la red del servidor, retrasos en el tráfico ICA causados por la red del servidor o latencia en la red del cliente.

Para identificar la causa principal del problema, analice las siguientes métricas:

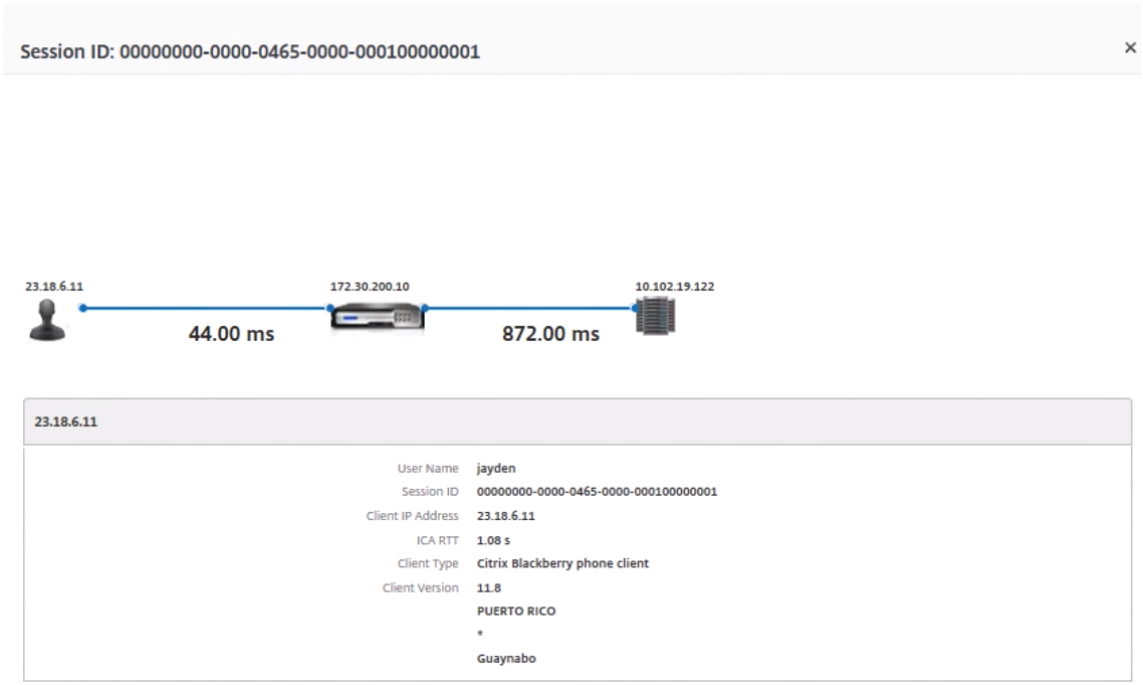
- Latencia de WAN
- Latencia de DC
- Demora de host

Para ver las métricas del cliente:

1. En la ficha **Analytics**, vaya a **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 de aplicación actuales**, coloque el mouse sobre el valor **RTT** y anote los valores de retardo del host, latencia de CC y latencia de WAN.
5. En la tabla **Sesiones de aplicación actuales**, haga clic en el símbolo de diagrama de saltos para mostrar información sobre la conexión entre el cliente y el servidor, incluidos los valores de latencia.



Resumen:

En este ejemplo, la **latencia de DC** es de 751 milisegundos, la **latencia de la WAN** es de 52 milisegundos y **los retrasos de host** son de 6 segundos. Esto indica que el usuario está experimentando un retraso debido a la latencia promedio causada por la red del servidor.

Caso 2

El usuario experimenta un retraso al iniciar una aplicación en Citrix Virtual Apps or Desktops
El retraso puede deberse a la latencia en la red del servidor, retrasos de tráfico ICA causados por la red del servidor, latencia en la red del cliente o tiempo tardado en iniciar una aplicación.

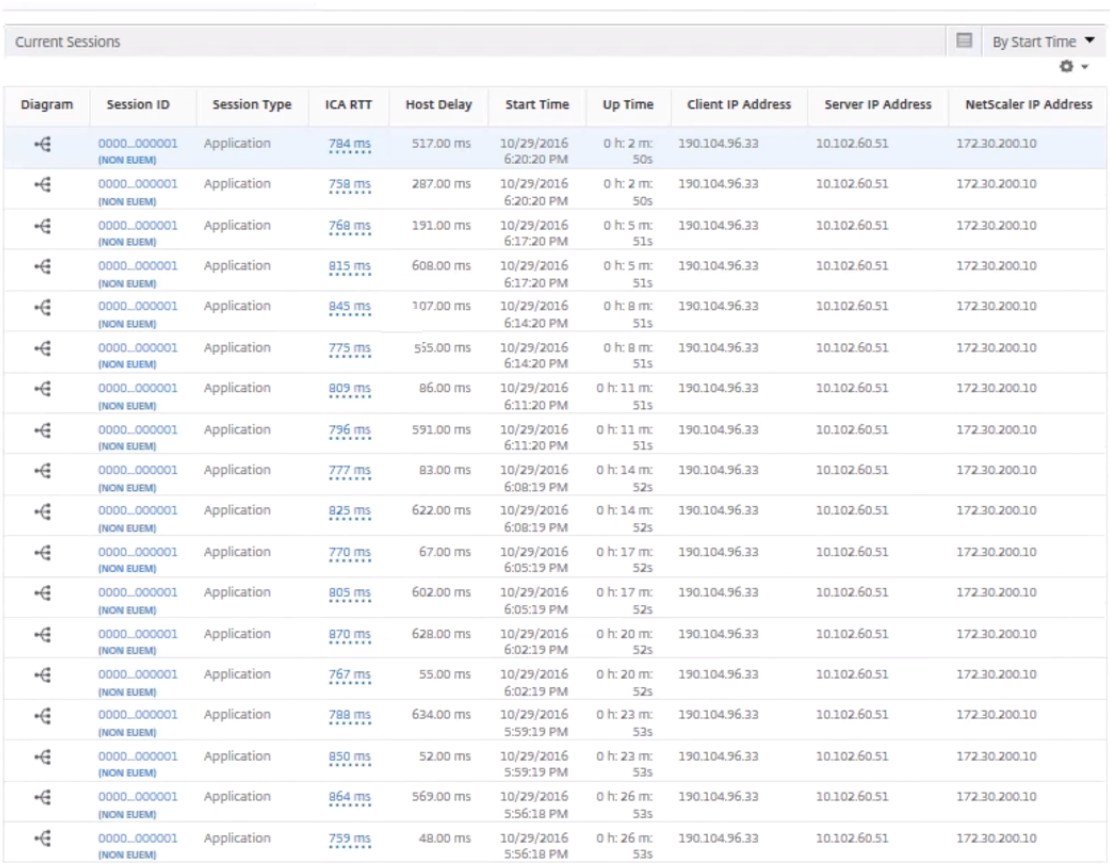
Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia de WAN
- Latencia de DC
- Demora del host

Para ver las métricas de usuario:

1. Vaya a **Gateway** > **HDX** Insight **Usuarios.
2. Desplácese hacia abajo y haga clic en el nombre de usuario.
3. En la representación gráfica, observe los valores de Latencia de WAN, Latencia de DC y RTT para la sesión en particular.

4. En la tabla **Sesiones de aplicación 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 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 la WAN y las retransmisiones del lado del servidor si utiliza NetScaler Console con 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.

Mapa geográfico de HDX Insight

La función de mapa geográfico de NetScaler Console muestra el uso de aplicaciones web en diferentes ubicaciones geográficas en un mapa. Como administrador, puede utilizar esta información para comprender las tendencias en el uso de aplicaciones y en la planificación de la capacidad.

El mapa geográfico proporciona información sobre las siguientes métricas específicas de un país, estado y ciudad:

- Número total de visitas: Número total de veces que se accede a una aplicación.
- Ancho de banda: ancho de banda total consumido al atender las solicitudes
- Tiempo de respuesta: Tiempo medio necesario para enviar respuestas a las solicitudes de los clientes.

El mapa geográfico proporciona información que se puede utilizar para abordar varios casos de uso, como los siguientes:

- Región que tiene el número máximo de clientes que acceden a una aplicación
- Región que tiene el tiempo de respuesta más alto
- Región que consume más ancho de banda

NetScaler Console **habilita automáticamente** los mapas geográficos para direcciones IP privadas o públicas cuando habilita **Web Insight**.

Crear un bloque de IP privado

NetScaler Console puede reconocer la ubicación de un cliente cuando la dirección IP privada del cliente se agrega al servidor de NetScaler Console. Por ejemplo, si la dirección IP de un cliente se

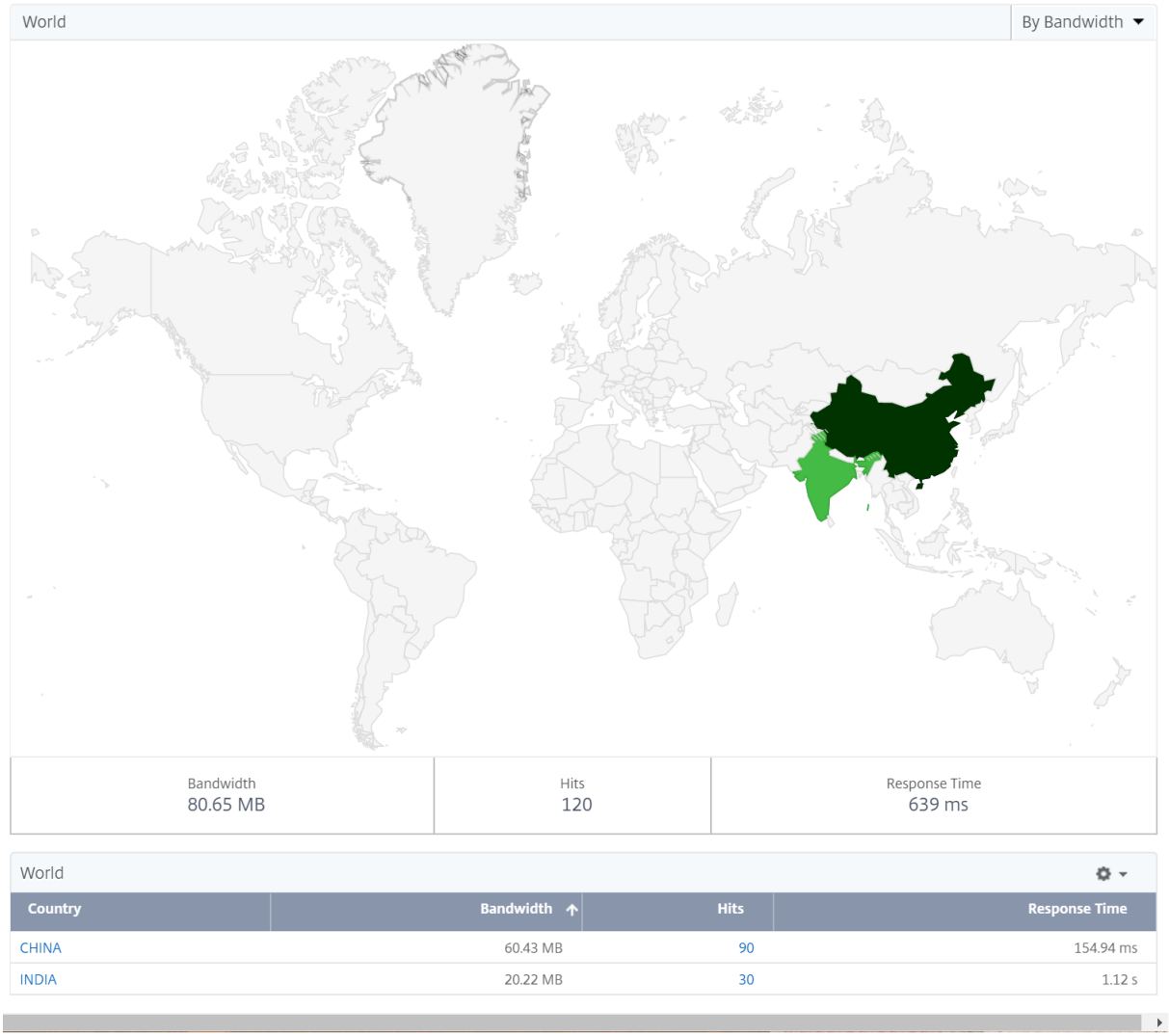
encuentra dentro del rango de un bloque de direcciones IP privadas asociado a la ciudad A, NetScaler Console reconoce que el tráfico proviene de la ciudad A para este cliente.

Para crear un bloque IP:

1. En NetScaler Console, vaya a Configuración > **Configuración de análisis > Bloques de IP** y, a continuación , haga clic en **Agregar**.
2. En la página **Crear Bloques de IP**, especifique los siguientes parámetros:
    - **Nombre**. Especifique un nombre para el bloque de IP privado
    - **Dirección IP inicial**. Especifique el rango de direcciones IP más bajo para el bloque de IP.
    - **Dirección IP final**. Especifique el rango de direcciones IP más alto para el bloque de IP.
    - **País**. Selecciona el país de la lista.
    - **Región**. Según el país, la región se rellena automáticamente, pero puede seleccionarla.
    - **Ciudad**. Según la región, la ciudad se rellena automáticamente, pero puede seleccionar la ciudad.
    - **Latitud** y **longitud de la ciudad**. Según la ciudad que selecciones, la latitud y la longitud se rellenan automáticamente.
3. Haga clic en **Crear** para finalizar.

Bloques IP públicos NetScaler Console también puede reconocer la ubicación del cliente si este utiliza una dirección IP pública. NetScaler Console tiene un archivo CSV de ubicación integrado que coincide con la ubicación según el rango de direcciones IP del cliente. Para usar un bloque de IP público, el único requisito es **habilitar la recopilación de datos geográficos** desde la página Configure Insight.

> Nota
>
> NetScaler Console requiere una conexión a Internet para mostrar los mapas geográficos de una ubicación geográfica concreta. También se requiere conexión a Internet para exportar el GeoMap en formatos.pdf,.png o.jpg.



Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Programar el informe a diario, semanal o mensual y enviarlo por correo electrónico o mensaje de Slack.

> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere pro-

> gramar el informe separados por comas.

Para configurar una geomapa para centros de datos:

En la ficha **Infraestructura**, vaya a **Sitios** > **Bloques de IP privados** para configurar mapas geográficos para una ubicación en particular.

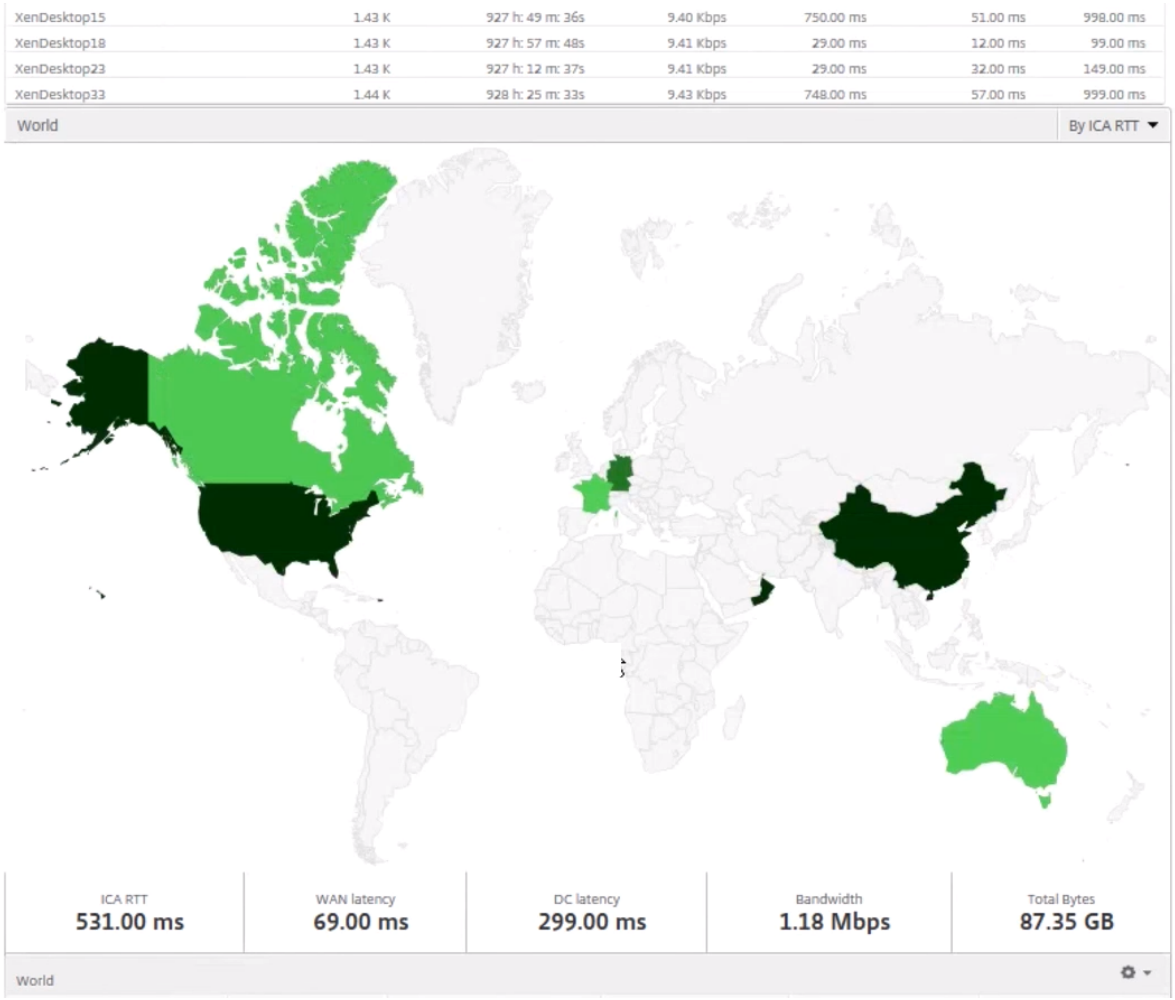
Caso de uso

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 de NetScaler tienen una licencia avanzada, no se activarán los umbrales establecidos en NetScaler Console para HDX Insight, ya que los datos analíticos solo se recopilan durante 1 hora.

Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Programar el informe a diario, semanal o mensual y enviarlo por correo electrónico o mensaje de Slack.

Nota

- Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
- Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

Habilitar la recopilación de datos de HDX Insight

January 26, 2024

HDX Insight permite al administrador ofrecer una experiencia de usuario excepcional al proporcionar una visibilidad integral del tráfico ICA que pasa por el dispositivo NetScaler.

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 permitir la recopilación de datos en las instancias de NetScaler difiere según la posición del dispositivo en la topología de implementación. En este tema se incluyen los siguientes detalles:

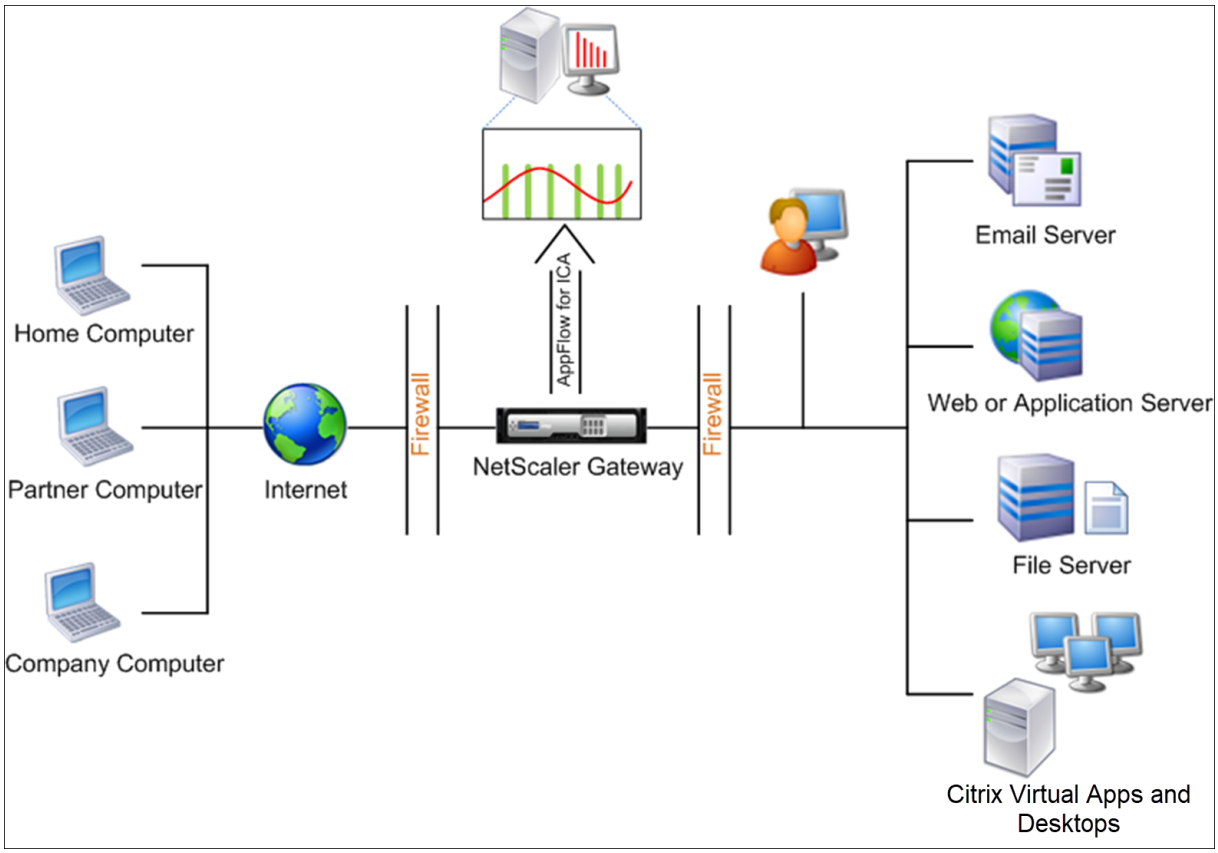
- Permitir la recopilación de datos para supervisar las instancias de NetScaler implementadas en modo transparente
- Habilitar la recopilación de datos para los dispositivos NetScaler Gateway implementados en modo de salto único
- Habilitar la recopilación de datos para los dispositivos NetScaler Gateway implementados en modo de doble salto
- Habilitar la recopilación de datos para supervisar los NetScalers implementados en modo de usuario de LAN

Habilitar la recopilación de datos para dispositivos NetScaler Gateway implementados en modo de salto único

January 26, 2024

Cuando NetScaler Gateway se implementa en modo de salto único, el NetScaler Gateway se encuentra en el borde de la red y redirige las conexiones ICA a la infraestructura de entrega de escritorios. Esta implementación es la implementación más simple y común. Este modo 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 Console y habilitar AppFlow en NetScaler Console. La siguiente imagen muestra una consola de NetScaler implementada en modo de salto único.



Habilite la función AppFlow desde NetScaler Console

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 los servidores virtuales VPN y haga clic en **Habilitar análisis**.
4. Selecciona **Web Insight** .
5. Haga clic en **Aceptar**.

Nota

Los siguientes comandos comienzan a ejecutarse en segundo plano cuando habilita AppFlow en modo de salto único. Estos comandos se especifican explícitamente aquí para solucionar problemas.

- `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

Habilite la recopilación de datos para supervisar los NetScalers implementados en modo transparente

January 26, 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 dispositivo NetScaler se implementa en modo transparente en un entorno de Citrix Virtual Apps and Desktops, el tráfico ICA no se transmite a través de una VPN.

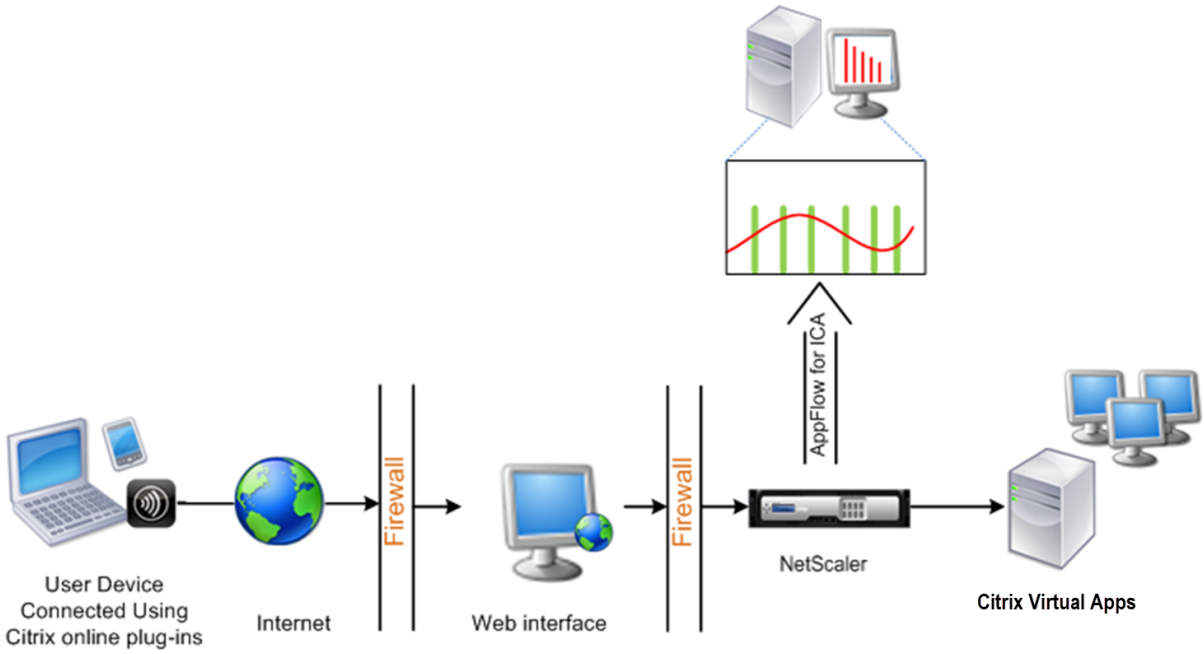
Después de añadir el NetScaler al inventario de la consola de NetScaler, debe habilitar AppFlow para la recopilación de datos. Habilitar la recopilación de datos depende del dispositivo y del modo. En ese caso, debe agregar NetScaler Console como recopilador de AppFlow en cada dispositivo NetScaler y debe configurar una política 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 Console.
- 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 .

La siguiente imagen muestra la implementación en red de una consola de NetScaler cuando se implementa un NetScaler 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:

```
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 del **tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarse al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
```

8. Guarde la configuración.

```
save ns config
```


Habilitar la recopilación de datos para dispositivos NetScaler Gateway implementados en modo de salto doble

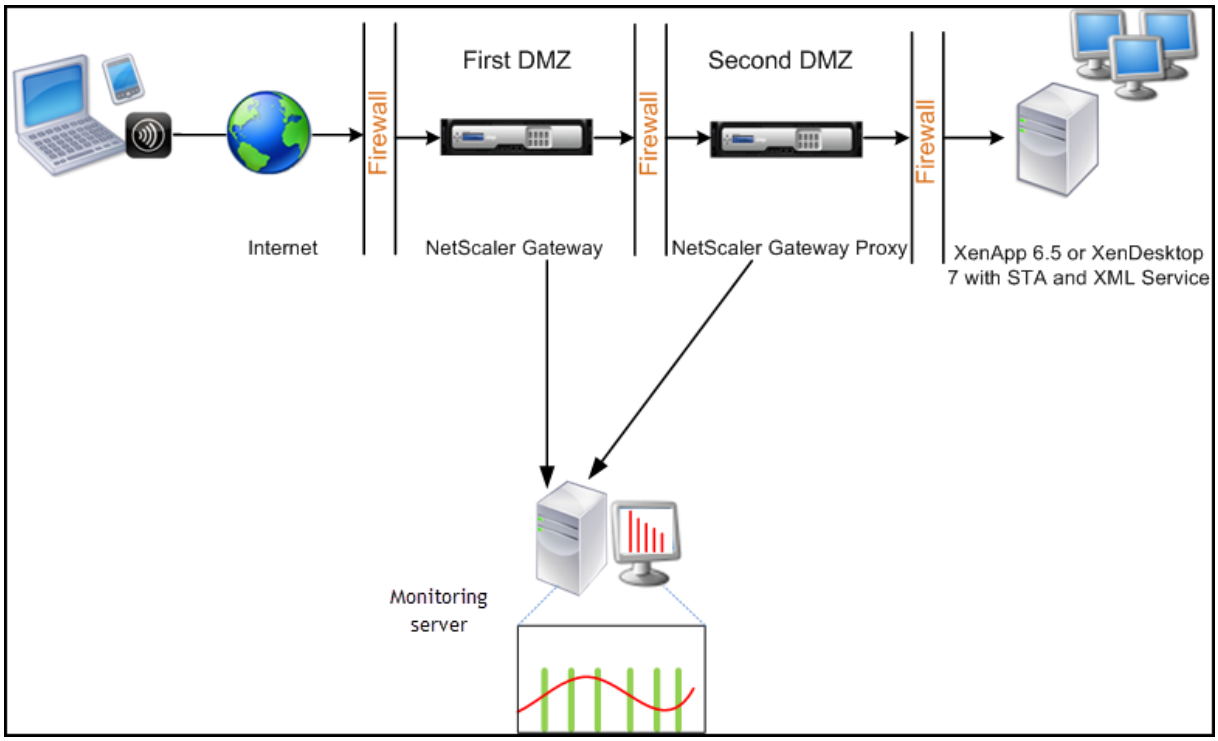
March 6, 2024

El modo de doble salto de NetScaler Gateway proporciona protección adicional a una red interna de la 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.

Como administrador, con NetScaler Console, puede analizar:

- El número de saltos (dispositivos NetScaler Gateway) a través de los cuales pasan las conexiones ICA
- Los detalles sobre la latencia en cada conexión TCP y cómo se ferias frente a la latencia ICA total percibida por el cliente

La siguiente imagen indica que NetScaler Console y NetScaler Gateway de la primera DMZ están implementados en la misma subred.



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.

La consola NetScaler 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 el modo de doble salto, NetScaler Console 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 Console y habilitar la recopilación de datos, cada dispositivo exporta los informes realizando un seguimiento del recuento de saltos y el ID de la cadena de conexión.

Para que NetScaler Console identifique qué dispositivo está exportando registros, cada dispositivo se especifica con un recuento de saltos y cada conexión se especifica con un identificador 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 Console utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dos 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 Console, habilitar AppFlow en NetScaler Console y, a continuación, ver los informes en el panel de control de NetScaler Console.

Habilitar la recopilación de datos en NetScaler Console

Si habilita NetScaler Console para empezar a recopilar los detalles ICA de ambos dispositivos, los detalles recopilados son redundantes. Para superar esta situación, debe habilitar AppFlow para TCP en el primer dispositivo 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 Console:

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 los servidores virtuales y haga clic en **Habilitar seguridad y análisis**.
4. Seleccione Web **Insight**
5. Haga clic en **Aceptar**.

Configurar los dispositivos de NetScaler Gateway para exportar datos

Tras instalar los dispositivos NetScaler Gateway, debe configurar los siguientes ajustes en los dispositivos NetScaler Gateway para exportar los informes a NetScaler Console:

- 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**] …

```
1 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:

   vincular vservervpn\ **-NextHopServer** <name\ >\ <name\ >

```
1 bind vpn vserver vs1 -nextHopServer nh1
```

3. Habilite el salto doble y AppFlow en NetScaler Gateway en la segunda DMZ.

---

configurar vpn vserver\ DISABLED)] [**- appflowLog** (DISABLED)] <name\ >\ [**- DoubleHop** ENABLED (HABILITADO)

```
1 set vpn vserver vpnhop2 – doubleHop ENABLED – appFlowLog ENABLED
```


4. Inhabilite la autenticación en el servidor virtual de NetScaler Gateway en la segunda DMZ.

configurar vpn vserver\ <name\ >\ [OFF)]
-autentificación (ACTIVADA)

```
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:

establecer el parámetro AppFlow [DISABLED)]
-ConnectionChaining (ENABLED)

```
set appflow param -connectionChaining ENABLED
```

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 salto** siguiente y enlace un servidor de salto siguiente 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 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** y desactive **Habilitar autenticación** .

4. Habilite uno de los dispositivos NetScaler Gateway para exportar registros TCP.

a) En la ficha **Configuración**, expanda **NetScaler Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda Directivas.

c) Haga clic en el icono + y, en la lista **Elegir directiva**, seleccione **AppFlow** y, en la lista **Elegir tipo**, seleccione **Otra solicitud TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar** .

5. Habilite el otro dispositivo NetScaler Gateway para exportar registros ICA:

a) En la ficha **Configuración**, expanda **NetScaler Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo **Avanzado**, expanda **Directivas**.

c) Haga clic en el icono + y, en la lista **Elegir directiva**, seleccione **AppFlow** y, en la lista **Elegir tipo**, seleccione **Otra solicitud TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar** .

6. Habilite el encadenamiento de conexiones en ambos dispositivos NetScaler Gateway.

a) En la ficha **Configuración**, vaya a **Sistema** > **Appflow**.

b) En el panel derecho, en el grupo **Configuración**, haga clic en **Cambiar la configuración de Appflow**.

c) Seleccione **Conexión encadenamiento** y haga clic en **Aceptar**.

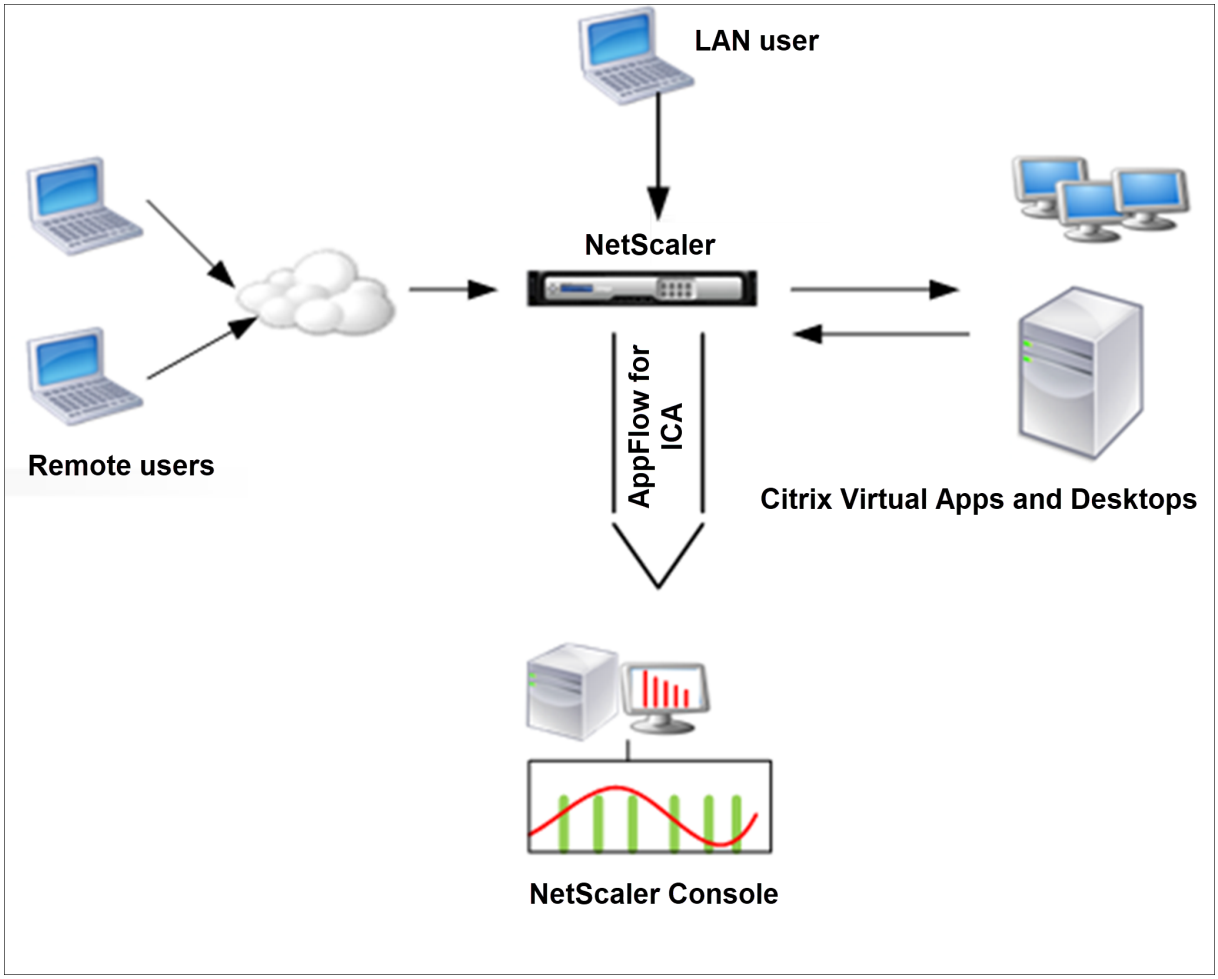
Habilite la recopilación de datos para supervisar los NetScalers implementados en modo de usuario de LAN

January 26, 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 las aplicaciones Citrix Virtual Apps and Desktops, puede implementar el dispositivo NetScaler en modo de usuario de LAN configurando un servidor virtual de redirección de caché. El servidor virtual de redirección de caché actúa como un proxy SOCKS en el dispositivo NetScaler Gateway.

La siguiente imagen muestra la consola NetScaler implementada en **modo de usuario LAN**.



> **Nota**
>
> El dispositivo NetScaler Gateway debe poder comunicarse con el agente.

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 Console, 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 Console.
> - 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 el dispositivo NetScaler.
2. Agregue un servidor virtual de redirección de caché de proxy de reenvío con la IP y el puerto proxy, y especifique el tipo de servicio como HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
    cacheType <cachetype>] [ - cltTimeout <secs>]
```

Ejemplo:

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD –
    cltTimeout 180
```

> **Nota:**
>
> Si accede a la red LAN mediante un dispositivo NetScaler Gateway, agregue una acción para aplicar una directiva que coincida con el tráfico de VPN.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

Ejemplo:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Añada NetScaler Console como recopilador de AppFlow en el dispositivo NetScaler.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
    \\>
```

Ejemplo:

```
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 del tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarse al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
```

Ejemplo:

```
set appflow param -flowRecordInterval 60
```

8. Guarde la configuración.

```
save ns config
```

Crear umbrales y configurar alertas para HDX Insight

January 26, 2024

HDX Insight en NetScaler Console le permite supervisar el tráfico HDX que pasa por las instancias de NetScaler. NetScaler Console le permite establecer umbrales en varios contadores que se utilizan para supervisar el tráfico de Insight. También puede configurar reglas y crear alertas en NetScaler Console.

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 para HDX Insight en NetScaler Console le permitió crear reglas y configurar alertas de forma proactiva cada vez que se superaran 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 la entidad de usuarios, el grupo de umbrales también se puede asociar con una geolocalización.

Solo se genera una alerta en NetScaler Console si se infringen 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 Console 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 Console o recibirla como correo electrónico o ambos, o como SMS en su dispositivo móvil. Para las dos últimas acciones, debe configurar el servidor de correo electrónico o el servidor de SMS en NetScaler Console.

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 Citrix Virtual Apps and Desktops en todo el mundo mediante la redirección basada en NetScaler Gateway y 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.

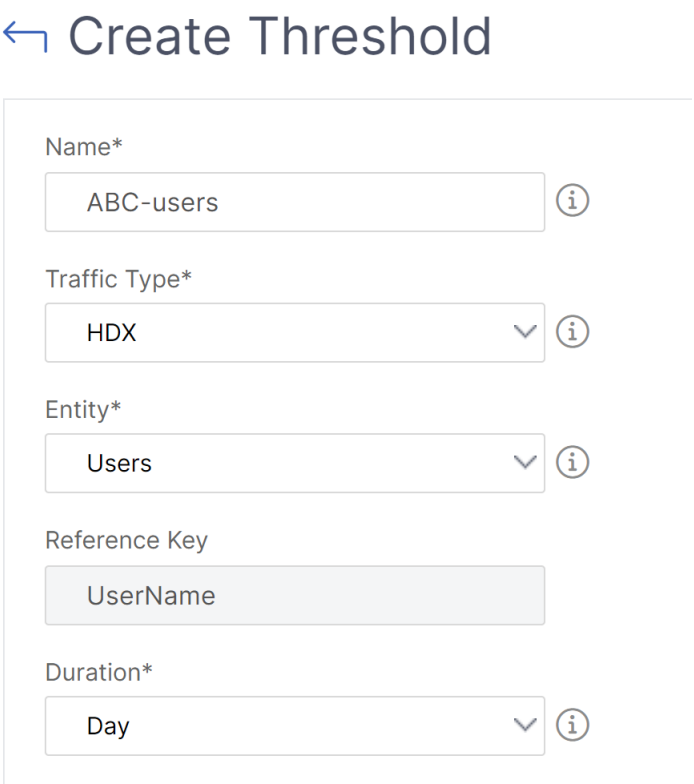
Con la administración de grupos de reglas de umbral para HDX Insight, Eric puede establecer grupos de reglas de umbral geoespecíficos para cada ubicación y recibir alertas por correo electrónico o SMS sobre las infracciones por área. Eric también puede combinar el seguimiento de más de una métrica dentro 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 revisar manualmente todas las métricas de la cartera de Citrix Virtual Apps and Desktops para ver HDX Insight.

Cree un grupo de reglas de umbral y configure alertas para HDX Insight mediante NetScaler Console

1. En NetScaler Console, vaya a **Configuración > Configuración de análisis > 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 Console genere una alerta.
    b) **Tipo de tráfico**. En la lista, selecciona **HDX**.
    c) **Entidad**. En la lista, seleccione la categoría o el tipo de recurso. Las entidades difieren para cada tipo de tráfico seleccionado anteriormente.

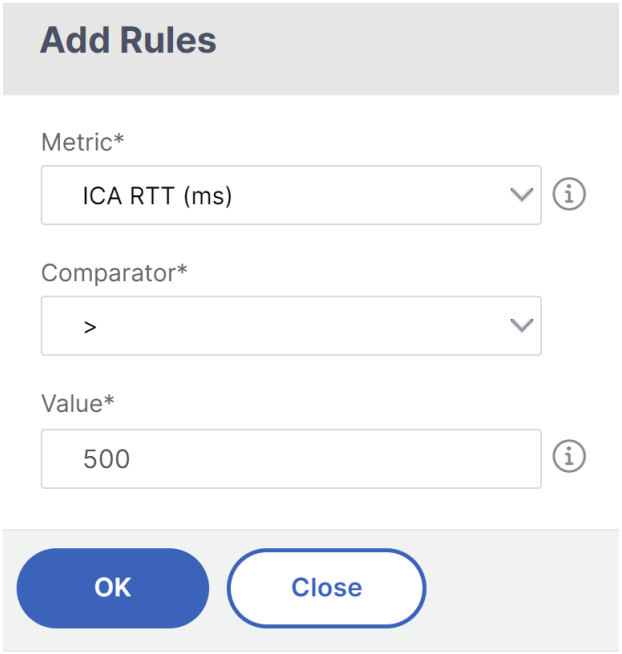
d) **Clave de referencia**. Se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.

e) **Duración**. En la 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.

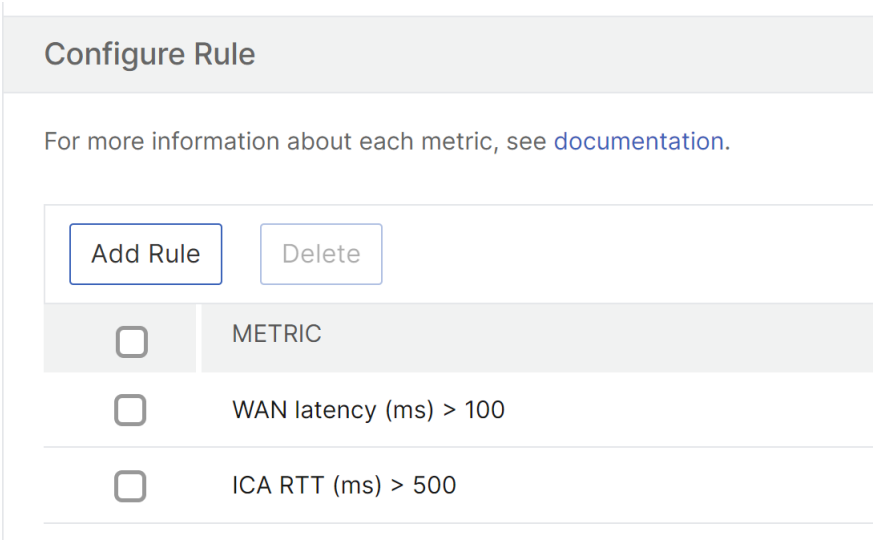


3. **Creación de grupo de reglas de umbral para todas las entidades:**

   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.

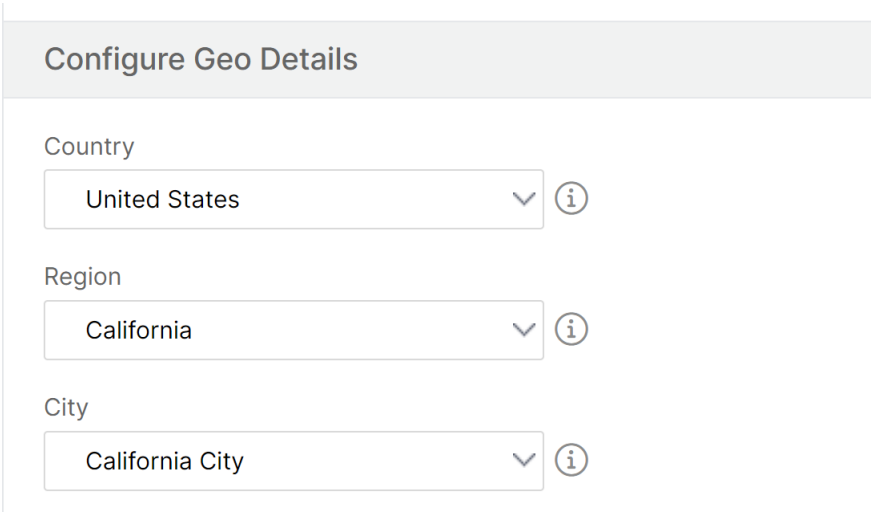


Puede crear varias reglas para supervisar cada entidad. La creación de varias reglas en un solo grupo le permite supervisar las entidades como un grupo de reglas de umbral en lugar de reglas individuales. Haga clic en **Aceptar** para cerrar la ventana.



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 Console comience a supervisar las entidades.
6. Opcionalmente, configure acciones como correo electrónico y notificaciones de Slack.
7. Haga clic en **Crear** para crear un grupo de reglas de umbral.

Ver informes y métricas de HDX Insight

January 26, 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 Apps and Desktops dentro del intervalo de tiempo seleccionado.
- **Aplicaciones:**muestra los informes del número total de aplicaciones y toda la información relevante relacionada, como el número total de veces que se lanzaron las aplicaciones 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.

Este documento incluye lo siguiente:

- Informes y métricas de visualización de usuarios
- Informes y métricas de vista de aplicaciones
- Informes y métricas de Desktop View
- Informes y métricas de vista de instancias
- Informes y métricas de vista de licencias

Solucionar problemas de HDX Insight

January 26, 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 Console.
- Generación de registros para el tráfico HDX/ICA en NetScaler.
- Población de registros en NetScaler Console.

Lista de comprobación de configuración de HDX Insight

- Asegúrese de que la función AppFlow está 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 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 la conectividad entre NetScaler y NetScaler Console

- 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 ir a **Sistema > AppFlow > Directivas** en la GUI para comprobar los aciertos de las directivas de AppFlow.
- Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

Generación de registros para el tráfico HDX/ICA en la lista de comprobación de NetScaler

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 la aplicación Citrix Workspace

Solución: Actualice la aplicación Citrix Workspace a una versión compatible. Para obtener más información, consulte la aplicación Citrix Workspace.

- Log: **Error de Expand Packet: Omitir todo el procesamiento hdx para este flujo**

  Causa: problema al descomprimir el tráfico ICA

  Solución: no hay informes disponibles para esta sesión de ICA hasta que se establezca una nueva sesión.

- Registro: **Transición no válida: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  Causa: problema al analizar el protocolo de enlace ICA

  Solución: No hay informes disponibles para esta sesión de ICA en particular hasta que se establezca una nueva sesión.

- Registro: **Falta EUEM ICA RTT**

  Causa: No se pueden analizar los datos del canal de End-User Experience Monitoring

  Solución: asegúrese de que el servicio de supervisión de la experiencia del usuario final esté iniciado en los servidores Citrix Virtual Apps and Desktops. Asegúrese de usar las versiones compatibles de la aplicación Citrix Workspace.

- Registro: **encabezado de canal no válido**

  Causa: no se puede identificar el encabezado del canal

  Solución: No hay informes disponibles para esta sesión de ICA en particular hasta que se establezca una nueva sesión.

- Registro: **omitir código**

  Si ves alguno de los siguientes valores para el código de omisión, se omiten los detalles de Insight.

  > El código de omisión 0 indica que el registro se ha exportado correctamente desde NetScaler.

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

Omitir código	Mensaje de error	Causa del error
102	NS_ICA_ERR_REDUC_PARAM_CNT	Parámetro no válido especificado para la inicialización del expansor V3
103	NS_ICA_ERR_REDUC_INIT	No se puede inicializar correctamente el expansor V3
104	NS_ICA_ERR_REDUC_PARAM_BYTES	Bytes insuficientes para asignar un codificador a un canal
105	NS_ICA_ERR_INVALID_CHANNEL	Número de canal ICA no válido
106	NS_ICA_ERR_INVALID_DECODER	Decodificador no válido especificado para un canal
107	NS_ICA_ERR_INVALID_TW_PARAM	Recuento de parámetros no válido especificado en el canal Thinwire
108	NS_ICA_ERR_INVALID_TW_DECODER	Decodificador no válido para el canal Thinwire
109	NS_ICA_ERR_REDUC_NO_DECODER	No hay decodificador definido para el canal
110	NS_ICA_ERR_REDUC_V3_EXPANDER	No se pudieron expandir los datos del canal
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	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

Omitir código	Mensaje de error	Causa del error
118	NS_ICA_ERR_PIR_MANY_FRAG	La solicitud Packet Init está fragmentada, no se puede procesar
119	NS_ICA_ERR_INIT_ICA_CAPS	Error de inicialización de la capacidad ICA
120	NS_ICA_ERR_NO_MSI_SUPPORT	El host no admite la función MSI. Indica para la versión de XenApp inferior a 6.5 o para las versiones de XenDesktop inferiores a 5.0
121	NS_ICA_ERR_CGP_INVALID_CMD	Se encontró un comando CGP no válido
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	Bytes insuficientes en el canal
123	NS_ICA_ERR_CHANNEL_DATA	Datos incorrectos en el canal EUEM, CONTROL o SEAMLESS
124	NS_ICA_ERR_INVALID_PURE_CMD	Se recibió un comando no válido al procesar datos de canal ICA puros
125	NS_ICA_ERR_INVALID_PURE_LEN	Se encontró una longitud no válida al procesar datos de canal ICA puros
126	NS_ICA_ERR_INVALID_PURE_LEN	Se encontró una longitud no válida al procesar los datos del canal ICA PURO
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_NS_6_0_CONNECT	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

Omitir código	Mensaje de error	Causa del error
134	NS_ICA_ERR_IDENT_PROTO	No se puede identificar el protocolo ICA o CGP, visto con receptores incorrectos
135	NS_ICA_ERR_INVALID_SIGNATURE	Firma ICA o cadena mágica incorrectas
136	NS_ICA_ERR_PARSE_RAW	Error al analizar el paquete de enlace ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquete incompleto recibido en el protocolo de enlace
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	La trama ICA es demasiado grande, supera los 1.460 bytes
139	NS_ICA_ERR_FORWARD	Error al reenviar los datos ICA
140	NS_ICA_ERR_MAX_HOLES	No se puede procesar el comando CGP porque se divide más allá del límite admitido
141	NS_ICA_ERR_ASSEMBLE_FRAME	No se puede volver a montar el marco ICA correctamente
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	Se 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

Omitir código	Mensaje de error	Causa del error
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	Se encontraron bytes insuficientes para un comando transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTE	Se encontraron bytes insuficientes para el comando EUEM
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	Evento no válido para el análisis continuo de canales
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Evento no válido para el análisis del canal CTRL
154	NS_ICA_ERR_EUEM_INVALID_EVENT	Evento no válido para el análisis del canal de EUEM
155	NS_ICA_ERR_USB_INVALID_EVENT	Evento no válido para el análisis de canales USB
156	NS_ICA_ERR_PURE_INVALID_EVENT	Evento no válido para el análisis de canal puro
157	NS_ICA_ERR_VCP_INVALID_EVENT	Evento no válido para el análisis de canales virtuales
158	NS_ICA_ERR_ICAP_INVALID_EVENT	Evento no válido para el análisis de datos ICA
159	NS_ICA_ERR_CGPP_INVALID_EVENT	Evento no válido para el análisis de datos CGP
160	NS_ICA_ERR_BASICCRYPT_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

Omitir código	Mensaje de error	Causa del error
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	VDA_xp 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
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

Omitir código	Mensaje de error	Causa del error
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONSAP	Error al habilitar 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 una PCB cliente.	Estadísticas
hdx_tot_cgp_conn	Indica el número total de conexiones CGP detectadas por NS (Session Reliability ON). Se incrementa cada vez que se detecta una conexión CGP basada en la firma CGP en una PCB cliente.	Estadísticas
hdx_dbg_tot_udt_conn	Indica el número total de conexiones UDP ICA detectadas por NS	Estadísticas
hdx_dbg_tot_nsap_conn	Indica el número total de conexiones compatibles con NSAP detectadas por NS	Estadísticas
hdx_tot_skip_conn	Indica cuántas conexiones ICA omitió el analizador debido a una firma ICA o CGP no válida.	Estadísticas
hdx_dbg_active_conn	Total de conexiones EDT/CGP/ICA activas en ese instante.	Estadísticas
hdx_dbg_active_nsap_conn	Número total de conexiones EDT/CGP/ICA NSAP activas en ese instante.	Estadísticas
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

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
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 reconecta solicitudes por cliente	Estados/Diagnósticos
hdx_euem_available	Indica el número de conexiones que tienen disponible el canal de supervisión de la experiencia del usuario final. El canal de supervisión de la experiencia del usuario final es necesario para recopilar estadísticas como ICA RTT.	Estados/Diagnósticos
hdx_err_disabled_sr	La fiabilidad de la sesión se inhabilita mediante el `nsapimgr`mando.La sesión no funciona para esta sesión.	Error
hdx_err_skip_no_msi	Al servidor XA/XD le falta la capacidad MSI. Esto indica una versión de servidor anterior, HDX Insight omite esta conexión.	Error
hdx_err_skip_old_server	Versión de servidor antigua no compatible	Error
hdx_err_clnt_not_whitelist	El receptor del cliente no está en la lista de permitidos, HDX Insight omite esta conexión	Error

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_sm_ica_cam_channel_disabled	Número total de NS_ICA_CAM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_usb_channel_disabled	Número total de NS_ICA_USB_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_clip_channel_disabled	Número total de NS_ICA_CLIP_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_ccm_channel_disabled	Número total de NS_ICA_CCM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_cdm_channel_disabled	Número total de NS_ICA_CDM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_com1_channel_disabled	Número total de NS_ICA_COM1_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_com2_channel_disabled	Número total de NS_ICA_COM2_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_cpm_channel_disabled	Número total de NS_ICA_CPM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_lpt1_channel_disabled	Número total de NS_ICA_LPT1_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/diagnóstico)
hdx_sm_ica_lpt2_channel_disabled	Número total de NS_ICA_LPT2_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
dx_dbg_sm_ica_msi_disabled	Número total de casos en los que MSI está inhabilitado mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_file_channel_disabled	El número total de NS_ICA_FILE_CHANNEL está inhabilitado mediante la directiva SmartAccess	Diagnóstico
hdx_dbg_usb_accept_device	Número total de dispositivos USB aceptados	Diagnóstico
hdx_dbg_usb_reject_device	Número total de dispositivos USB rechazados	Diagnóstico
hdx_dbg_usb_reset_endpoint	Número total de puntos finales USB restablecidos	Diagnóstico
hdx_dbg_usb_reset_device	Número total de dispositivos USB restablecidos	Diagnóstico
hdx_dbg_usb_stop_device	Número total de dispositivos USB detenidos	Diagnóstico
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.

Lista de comprobación de la población de registros de NetScaler Console

- Ejecute el comando `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` y compruebe los registros para confirmar que NetScaler Console

recibe los registros de AppFlow.

- Confirme que la instancia de NetScaler esté agregada a NetScaler Console.
- Compruebe que el servidor virtual NetScaler Gateway/VPN tiene licencia en NetScaler Console.
- 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 Console.
- Versiones del servidor Citrix Virtual Apps and Desktops.
- Versiones del espacio de trabajo del cliente.
- 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 Console.
- 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 NetScaler para conocer los problemas conocidos en HDX Insight.

Información de métricas para umbrales

January 26, 2024

Puede crear umbrales y recibir una notificación cada vez que se supere el valor del umbral. En una implementación típica, puede establecer umbrales para:

- Realice un seguimiento de las diferentes métricas
- Facilitar la planificación
- Reciba notificaciones cuando el valor de la métrica de la aplicación supere el umbral establecido

Para configurar el umbral:

1. Vaya a **Configuración > Configuración de análisis > Umbrales** .
2. En la página **Umbrales**, haga clic en **Agregar**.

Web

Métricas	Entidad	Descripción
Aplicaciones	Resultados	Número total de visitas recibidas por un servidor virtual (aplicación)
	Ancho de banda (MB)	Ancho de banda total consumido por el servidor virtual (aplicación)
	Tiempo de respuesta (ms)	El tiempo que tarda el servidor virtual en responder
Clientes	Solicitudes	El total de solicitudes recibidas por un cliente
	Tiempo de procesamiento (ms)	El tiempo necesario para procesar la respuesta del servidor por parte del cliente
	Latencia de red del cliente	El tiempo necesario para las solicitudes de la red del cliente
Dispositivos	Resultados	Número total de visitas recibidas por un dispositivo. Por ejemplo: equipo portátil, teléfono móvil
	Ancho de banda (MB)	Ancho de banda total consumido por un dispositivo

Métricas	Entidad	Descripción
Dominios	Resultados	Número total de visitas recibidas por un dominio de red
	Ancho de banda (MB)	Ancho de banda total consumido por un dominio de red
	Tiempo de respuesta (ms)	El tiempo que tarda un dominio de red en responder a las solicitudes
Sistema operativo	Resultados	Número total de visitas recibidas por un sistema operativo
	Ancho de banda (MB)	Ancho de banda total consumido por un sistema operativo
	Tiempo de procesamiento (ms)	El tiempo que tarda un sistema operativo en procesar la respuesta del servidor
Métodos de solicitud	Resultados	Número total de solicitudes recibidas por un método de solicitud. Por ejemplo: GET, POST
	Ancho de banda (MB)	Ancho de banda total consumido por un método de solicitud
Estado de respuesta	Resultados	Número total de visitas recibidas con códigos de respuesta
	Ancho de banda (MB)	Ancho de banda total consumido por el código
Servidores	Resultados	Número total de solicitudes/visitas recibidas por un servidor
	Ancho de banda (MB)	Ancho de banda total consumido por un servidor
	Latencia de red del servidor (ms)	El tiempo necesario para las solicitudes de la red de servidores

Métricas	Entidad	Descripción
	Tiempo de procesamiento del servidor (ms)	El tiempo que tarda un servidor en responder a las solicitudes
URLs	Resultados	Número total de visitas recibidas por una URL. Por ejemplo: www.Citrix.com
	Tiempo de carga (ms)	El tiempo que tarda una URL en cargarse desde el servidor
	Tiempo de procesamiento (ms)	El tiempo que tarda la URL en renderizarse y mostrarse
Agentes de usuario	Resultados	Número total de solicitudes recibidas por un agente de usuario. Por ejemplo: navegador web Chrome
	Ancho de banda (MB)	Ancho de banda total consumido por el agente de usuario
	Tiempo de procesamiento (ms)	El tiempo necesario para representar la respuesta del servidor por el agente de usuario

Seguridad

Métrica	Entidad	Descripción
Aplicaciones	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.

Métrica	Entidad	Descripción
	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.

ANÁLISIS DE APLICACIONES

Métrica	Entidad	Descripción
Aplicaciones	AppScore	App Score define el rendimiento de una aplicación y muestra si la aplicación funciona bien en términos de capacidad de respuesta. Los valores oscilan entre 0 y 80.

HDX

Para obtener información sobre los umbrales de HDX, consulte Crear umbrales y configurar alertas para HDX Insight

Análisis de infraestructura

March 6, 2024

Un objetivo clave para los administradores de red es supervisar las instancias de NetScaler. Las instancias de NetScaler ofrecen información interesante sobre el uso y el rendimiento de las aplicaciones y los escritorios a los que se accede a través de él. Los administradores deben supervisar la instancia

de NetScaler y analizar los flujos de aplicaciones procesados por cada instancia de NetScaler. Los administradores también deben poder solucionar cualquier problema probable en la configuración, la configuración, la conectividad, los certificados y otros impactos en 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 de 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 cuantificarlos con una puntuación medible que define el estado de una instancia. Con esta función, los administradores tienen un único punto de contacto para comprender el problema, su origen y las posibles soluciones que pueden realizar.

Análisis de infraestructura en NetScaler Console

La función Infrastructure Analytics 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 instancia indica el estado de una instancia de NetScaler. 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 explicados

- Indicadores de recursos del sistema

  Los siguientes son los problemas críticos de recursos del sistema que pueden producirse en las instancias de NetScaler y que son supervisados por NetScaler Console.

  - 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 NetScaler.
  - **Fallo de alimentación**. La fuente de alimentación falló o se desconectó de la instancia de NetScaler.
  - **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 los eventos incluidos en la función de administración de eventos de NetScaler Console, que están configurados con una gravedad crítica.

- **Fallo de sincronización de HA**. La sincronización de la configuración entre las instancias de NetScaler en alta disponibilidad falló en el servidor secundario.
- **No tiene latidos**. El servidor principal de un par de instancias de NetScaler en alta disponibilidad no recibe los latidos del servidor secundario.
- **Tiene un mal estado secundario**. El servidor secundario de un par de instancias de NetScaler en alta disponibilidad se encuentra en estado secundario Inactivo, Desconocido o Permanecido secundario.
- **La versión HA no coincide**. La versión de las imágenes del software NetScaler instaladas en un par de instancias de NetScaler en alta disponibilidad no coincide.
- **Fallo de sincronización del clúster**. No se pudo sincronizar la configuración entre las instancias de NetScaler en modo clúster.
- **La versión del clúster no coincide**. La versión de las imágenes del software NetScaler instaladas en las instancias de NetScaler en modo 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 su 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 Console, consulte [Eventos.] (/en-us/netscaler-console-service/networks/events.html)

- 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 de NetScaler ha caducado.
  - **Los certificados SSL están vencidos**. El certificado SSL instalado en la instancia de NetScaler 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 NetScaler 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.

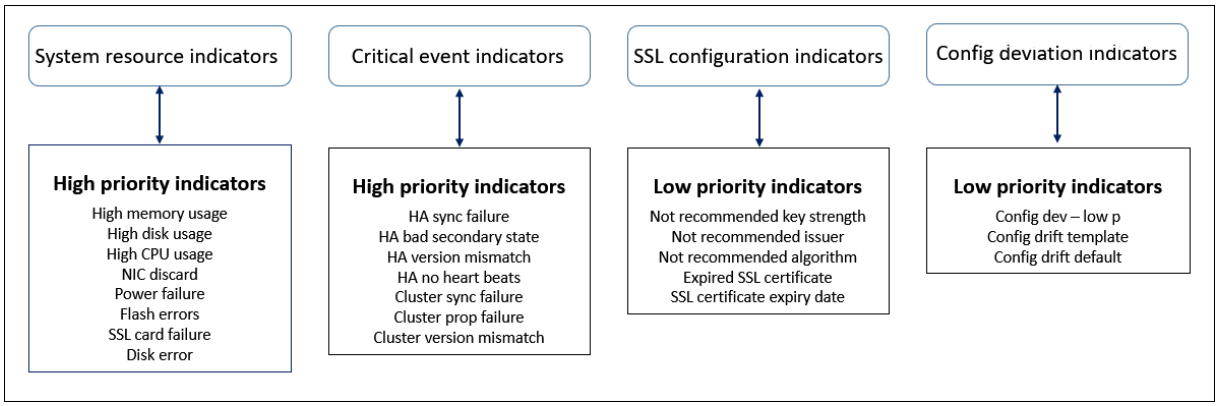
Para obtener más información sobre las desviaciones de configuración y sobre cómo ejecutar informes de auditoría para comprobar las desviaciones de configuración, consulte Ver informes de auditoría..

Ver los problemas de capacidad de NetScaler

Cuando una instancia de NetScaler ha consumido la mayor parte de su capacidad disponible, es posible que se descarten paquetes mientras se procesa el tráfico del cliente. Al comprender estos problemas de capacidad de NetScaler, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento de NetScaler. Para obtener más información, consulte Ver los problemas de capacidad en una instancia de NetScaler .

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:

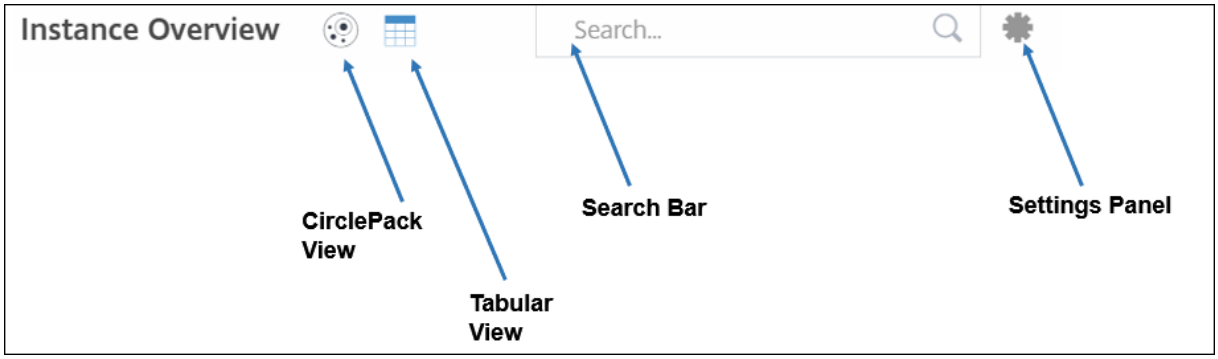
1. **Basado en una actividad**. Por ejemplo, un indicador de recursos del sistema se activa cada vez que se produce un corte de energía en la instancia y este indicador reduce el valor de la puntuación de la instancia. Cuando se borra el indicador, se elimina la penalización y la puntuación de la instancia 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.

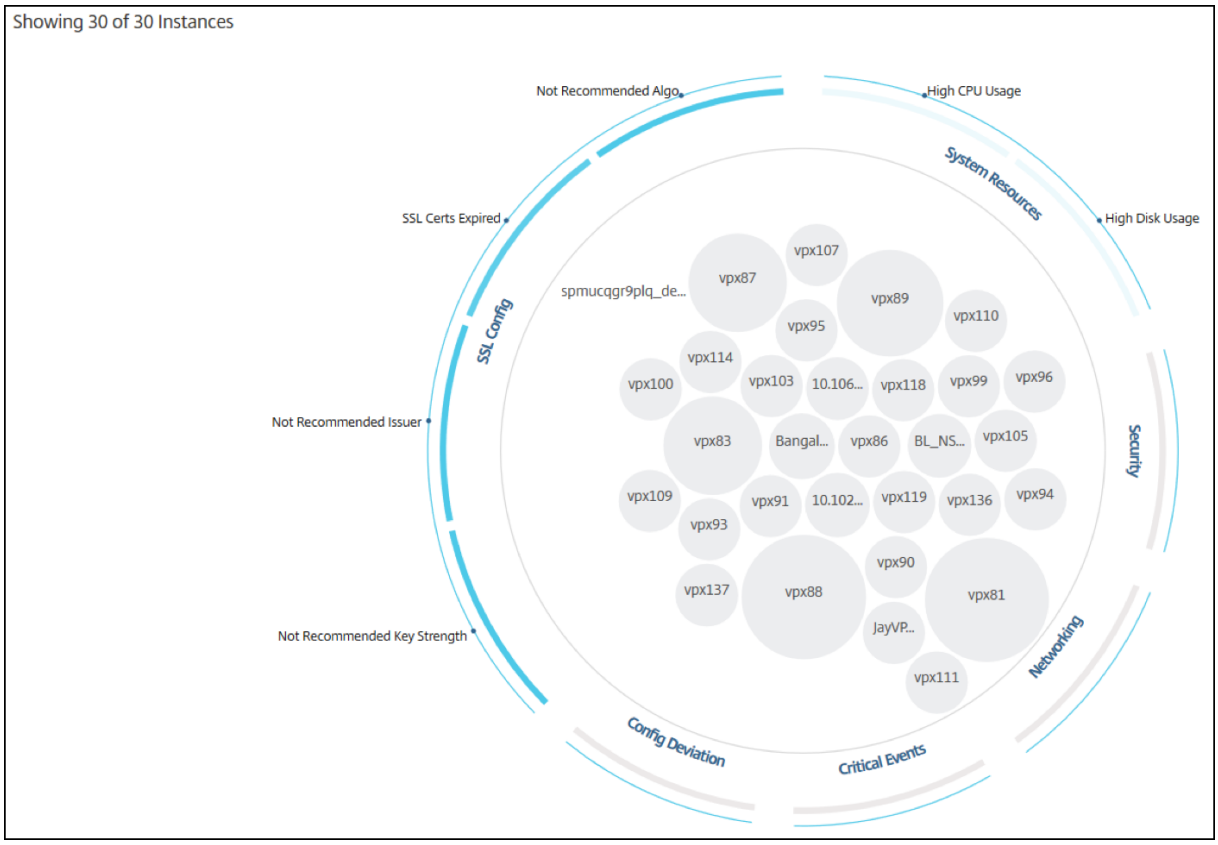


- En la vista Tabular, puede buscar una instancia escribiendo el nombre de host o la dirección IP en la barra de búsqueda.

- 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

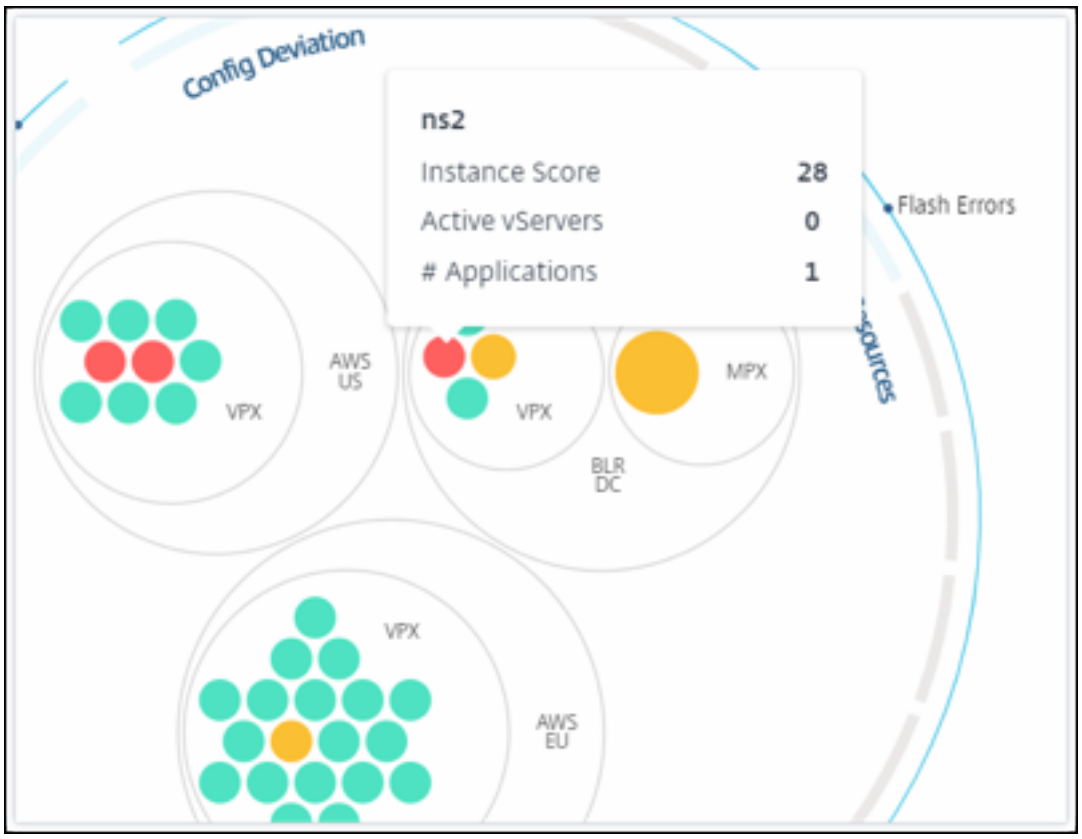
Color. Cada instancia se representa en Circle Pack como un círculo coloreado. El color del círculo indica el estado de la instancia.

- **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 observado algunos problemas y es necesario revisarlos.
- **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.

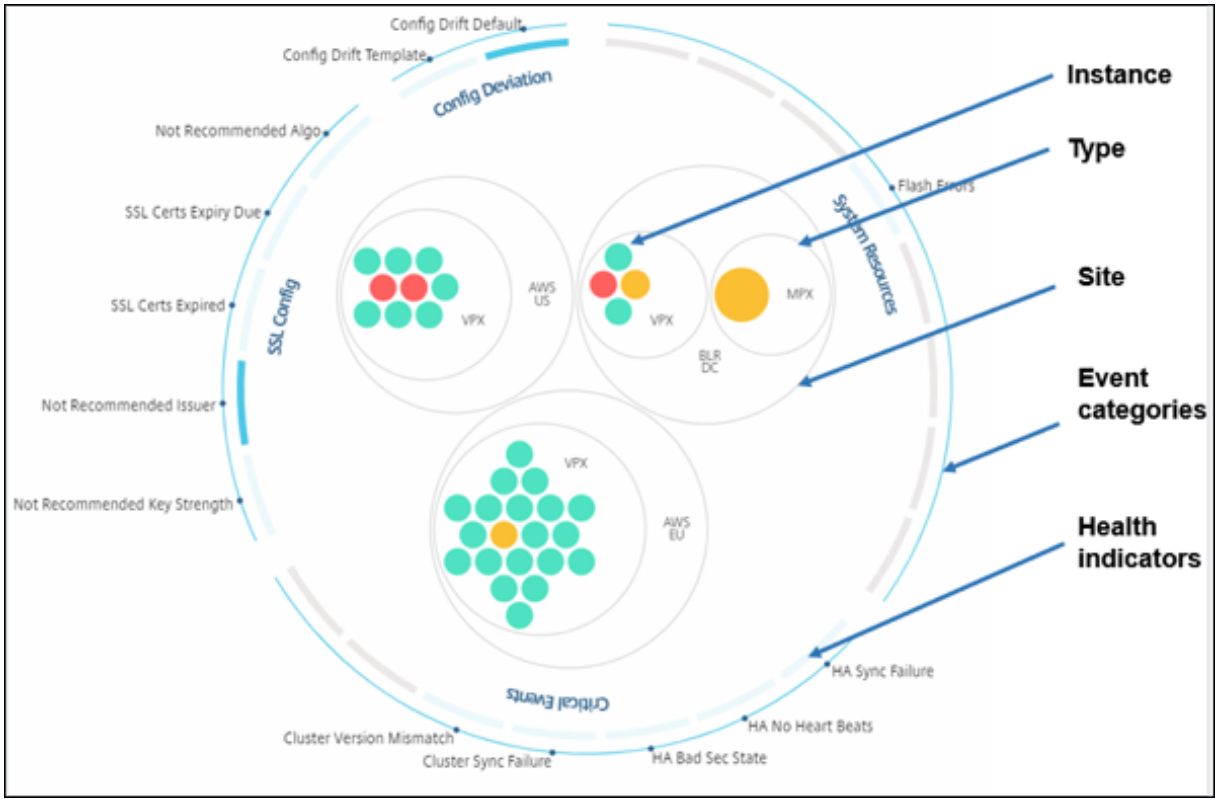


Círculos de instancia agrupados

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 NetScaler
- la versión de imagen de NetScaler 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.

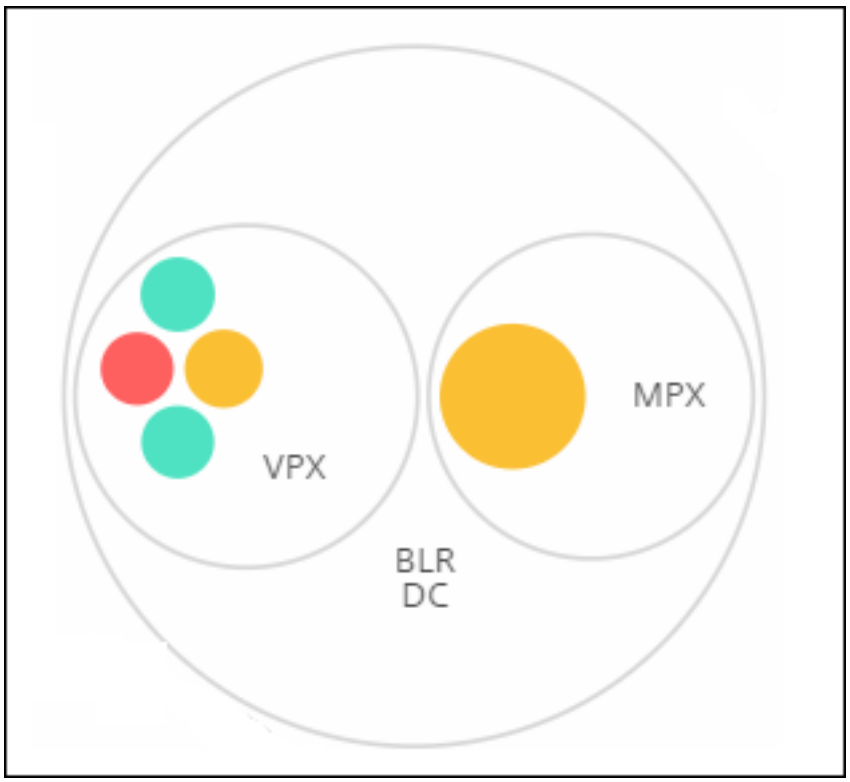


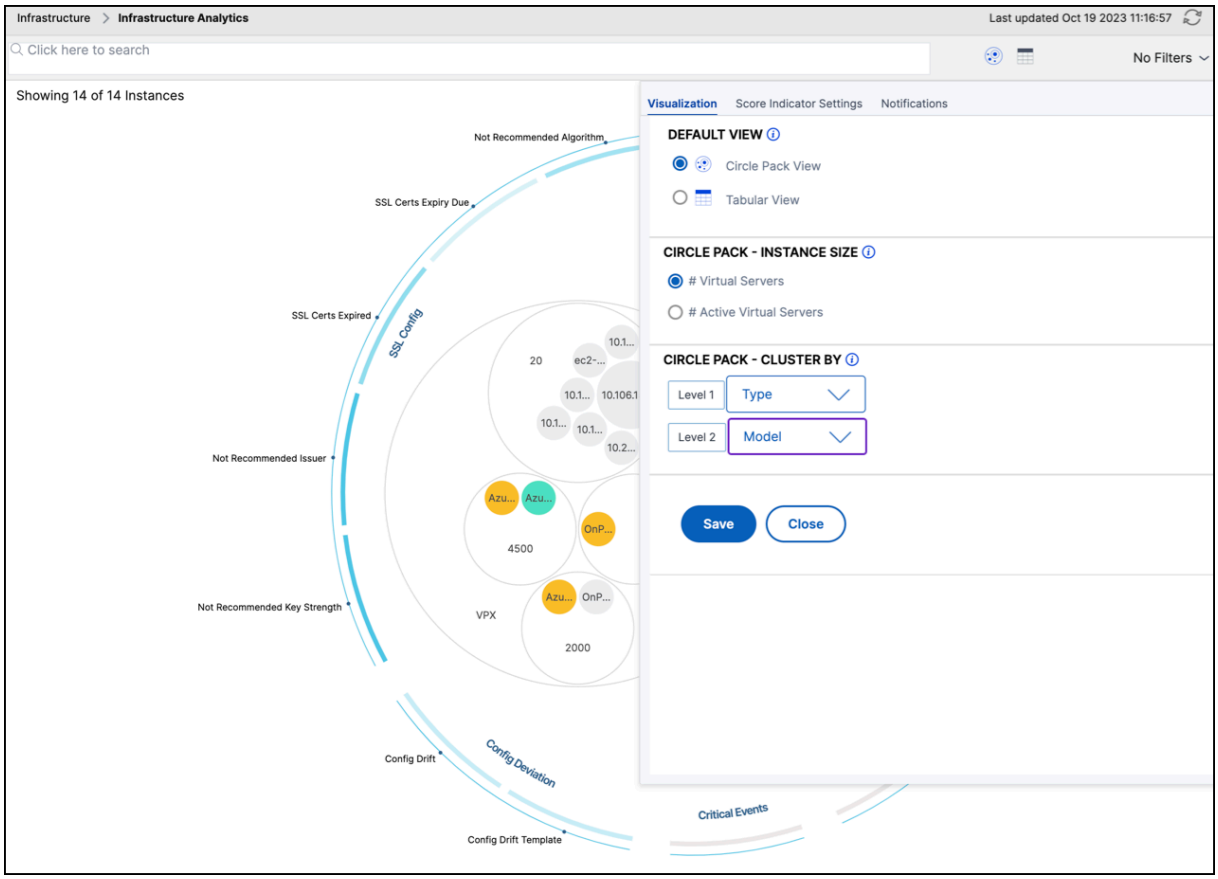
Todos estos círculos anidados están delimitados por dos círculos exteriores. Los dos círculos exteriores representan las cuatro categorías de eventos supervisados por la consola de NetScaler (recursos del sistema, eventos críticos, configuración de SSL y desviación de la configuración) y los indicadores de estado que contribuyen a ello.

Círculos de instancia agrupados

NetScaler Console 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 implementadas dos tipos de instancias de NetScaler: VPX y MPX. En primer lugar, puede agrupar las instancias de NetScaler por 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.

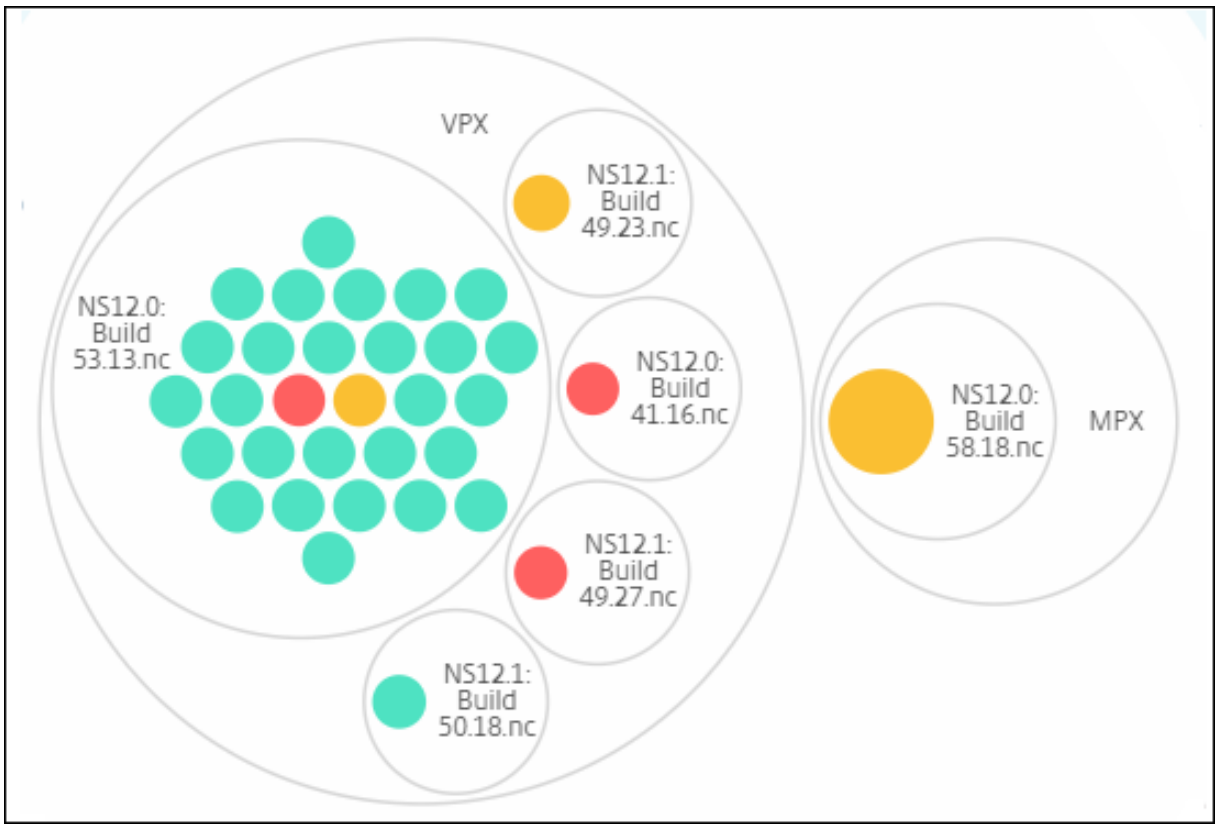




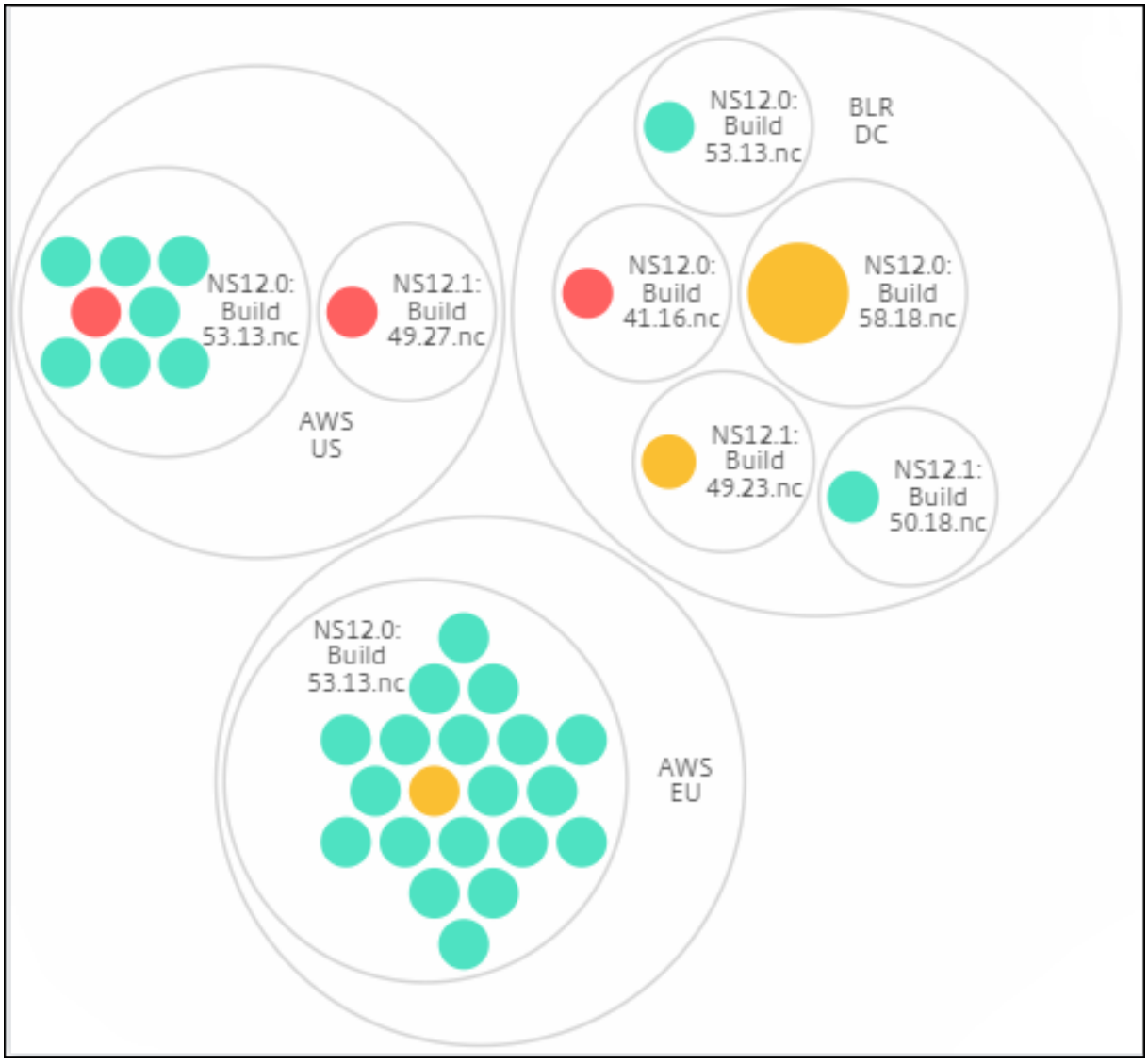
Algunos ejemplos más de clustering de dos niveles son los siguientes:

Sitio y modelo:

Tipo y versión:

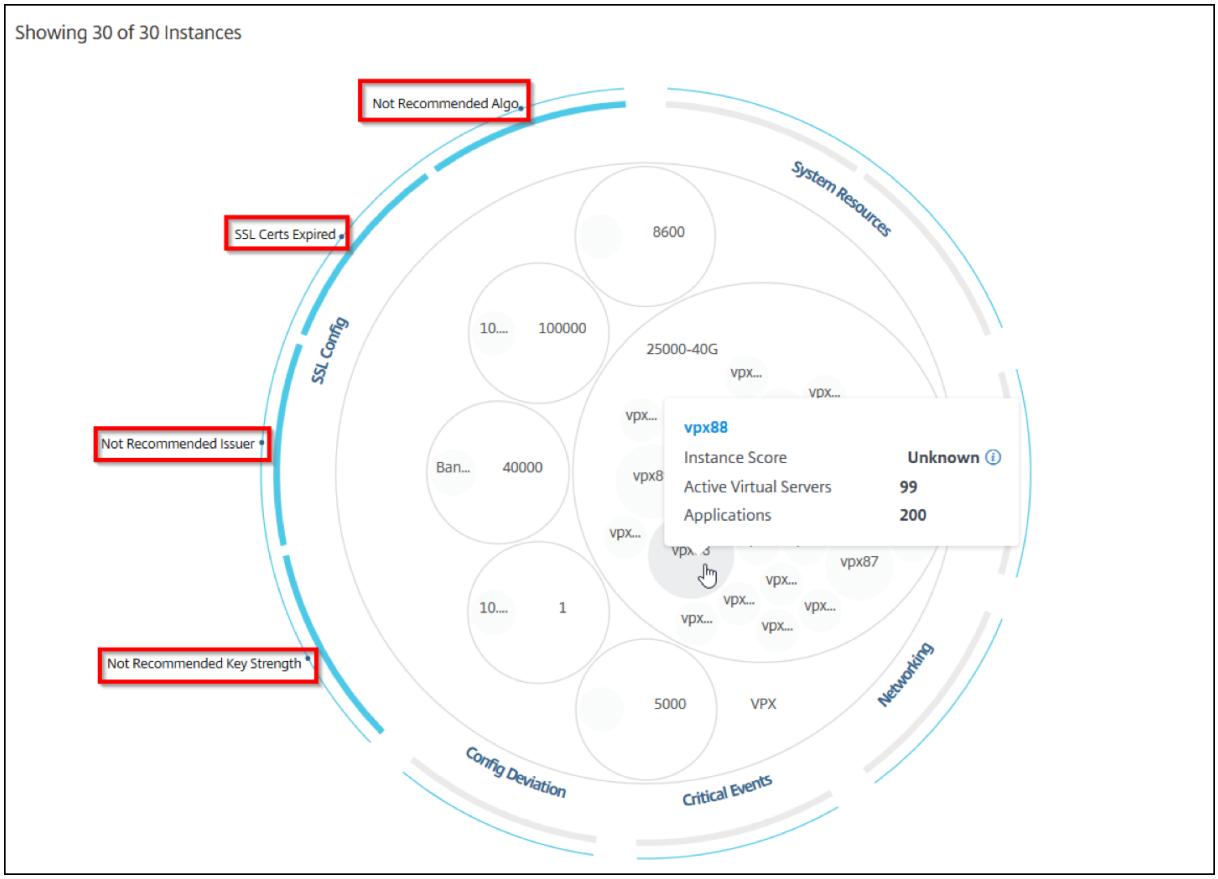


Sitio y versión:

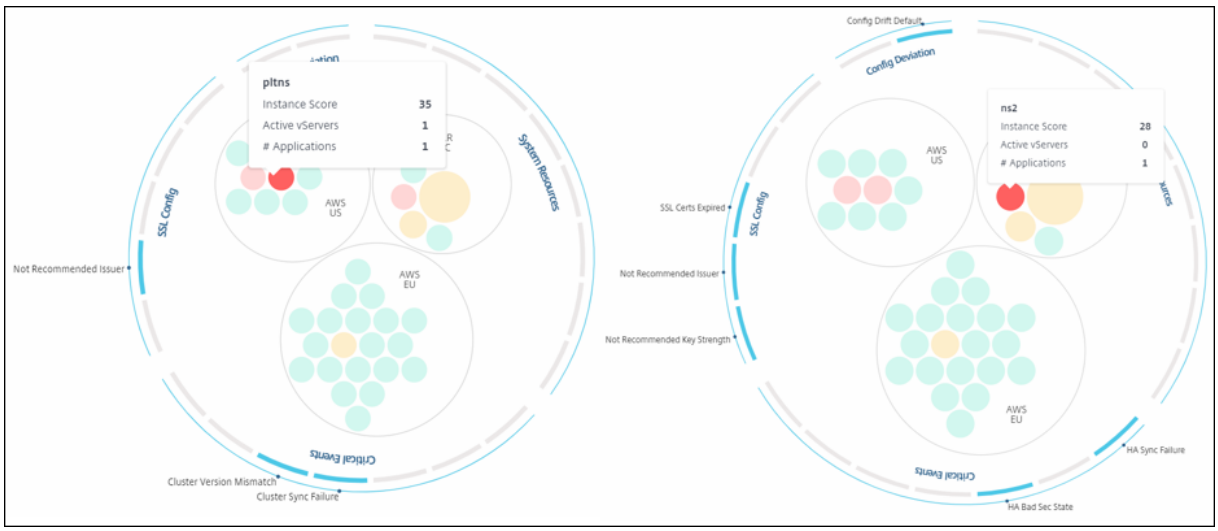


Cómo usar Circle Pack

Haga clic en cada uno de los círculos coloreados para resaltar esa instancia.

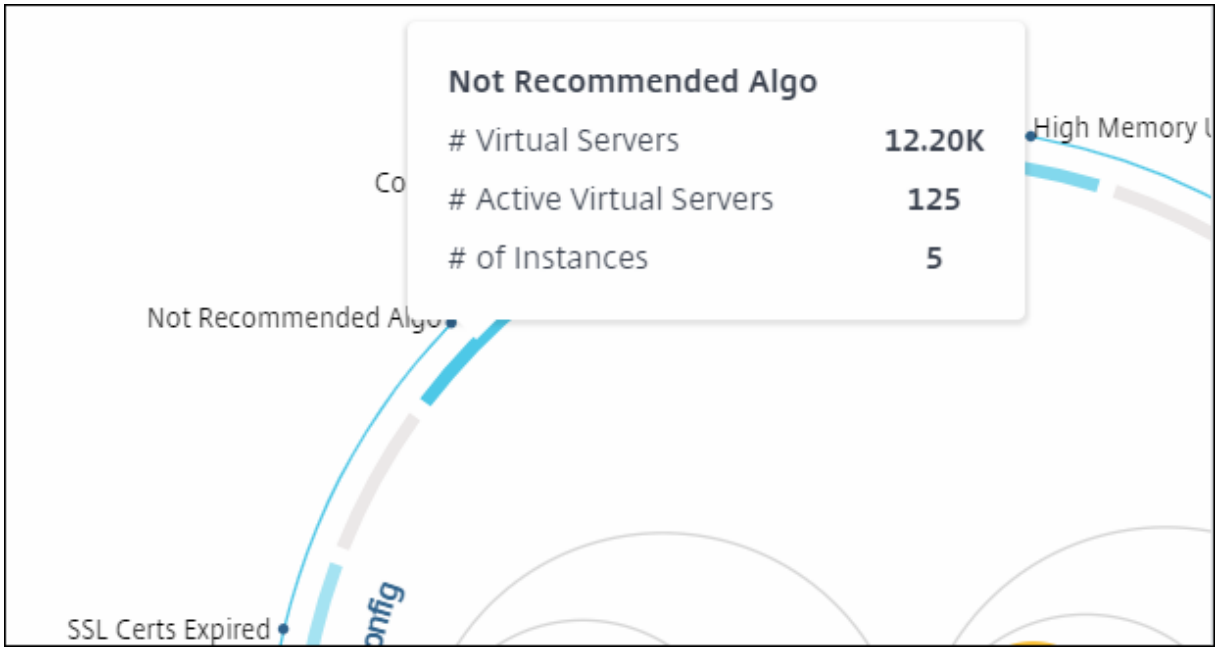


Dependiendo de los eventos que se hayan producido en ese caso, solo los indicadores de salud aparecen resaltados en los círculos exteriores. Por ejemplo, las dos imágenes siguientes de Circle Pack muestran diferentes conjuntos de indicadores de riesgo, aunque ambas instancias se encuentran en un estado 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 clic`Not recommended`

Algo para ver el informe resumido de ese indicador de riesgo.



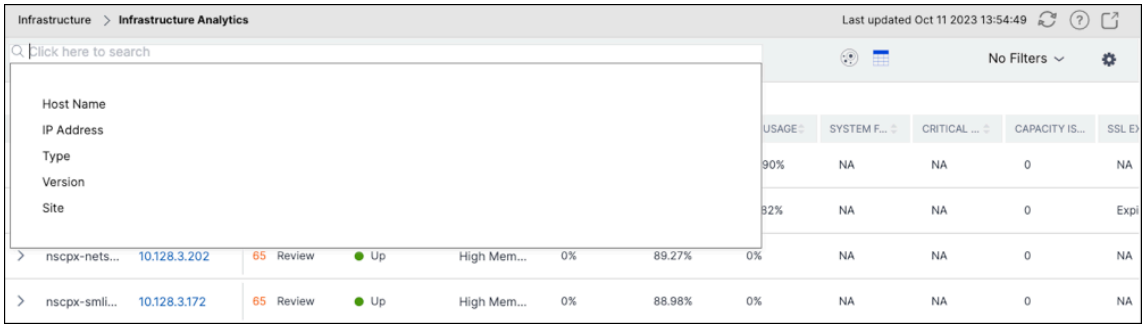
Vista tabular

La vista tabular muestra las instancias y los detalles de esas instancias en un formato tabular. Para obtener más información, consulte Detalles de la instancia

Barra de búsqueda

Coloque el cursor del ratón en la barra de búsqueda y seleccione los siguientes atributos de búsqueda para filtrar los resultados:

- Nombre de host
- Dirección IP
- Tipo
- Versión
- Sitio



Los resultados de búsqueda funcionan tanto para la vista de círculo como para la vista de tabla.

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

Para obtener más información sobre estos indicadores, consulte *Indicadores de estado en las instancias de NetScaler*.

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.

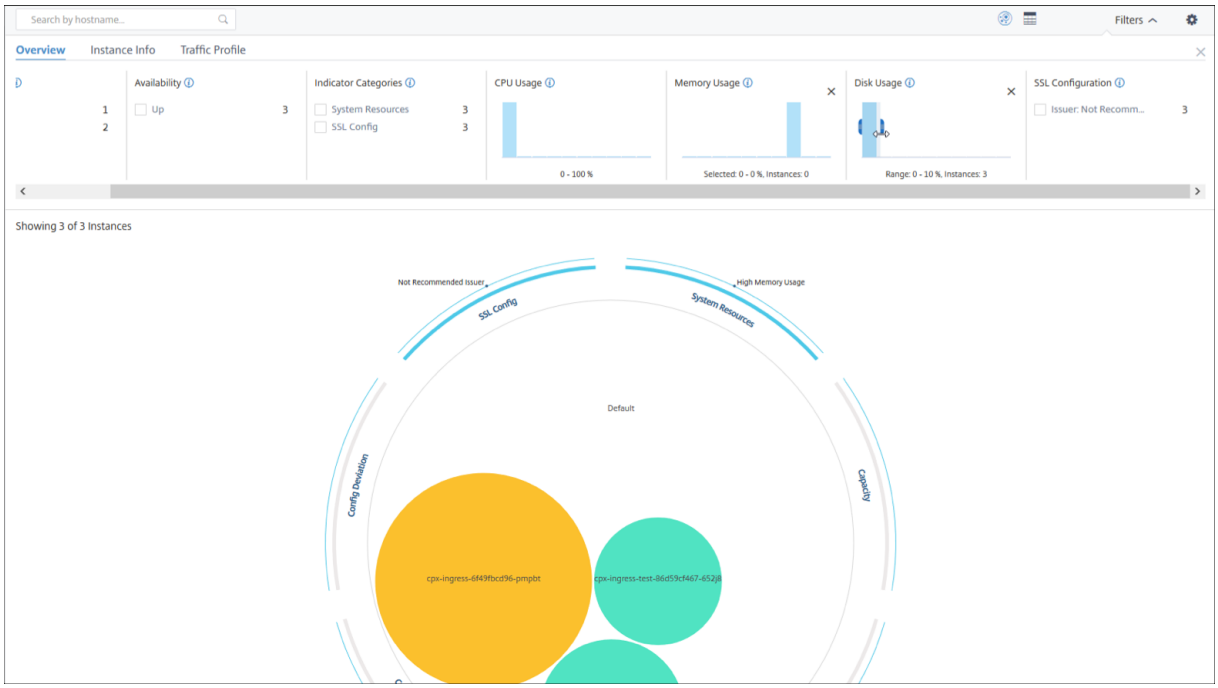
Ejemplo 2: Vea las instancias que consumen entre el 10 y el 20% de la memoria asignada:

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 espacio en disco en varios rangos:

Para ver las instancias que han consumido memoria entre el 0% y el 10% de espacio en disco, arrastre el puntero del ratón sobre los dos rangos, tal y como se muestra en la siguiente imagen.



> **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:

En la sección **Caducidad de los certificados SSL**, selecciona la casilla de verificación **Vencidos** para ver las tres instancias.

1: Haga clic en la lista **Filtro**.

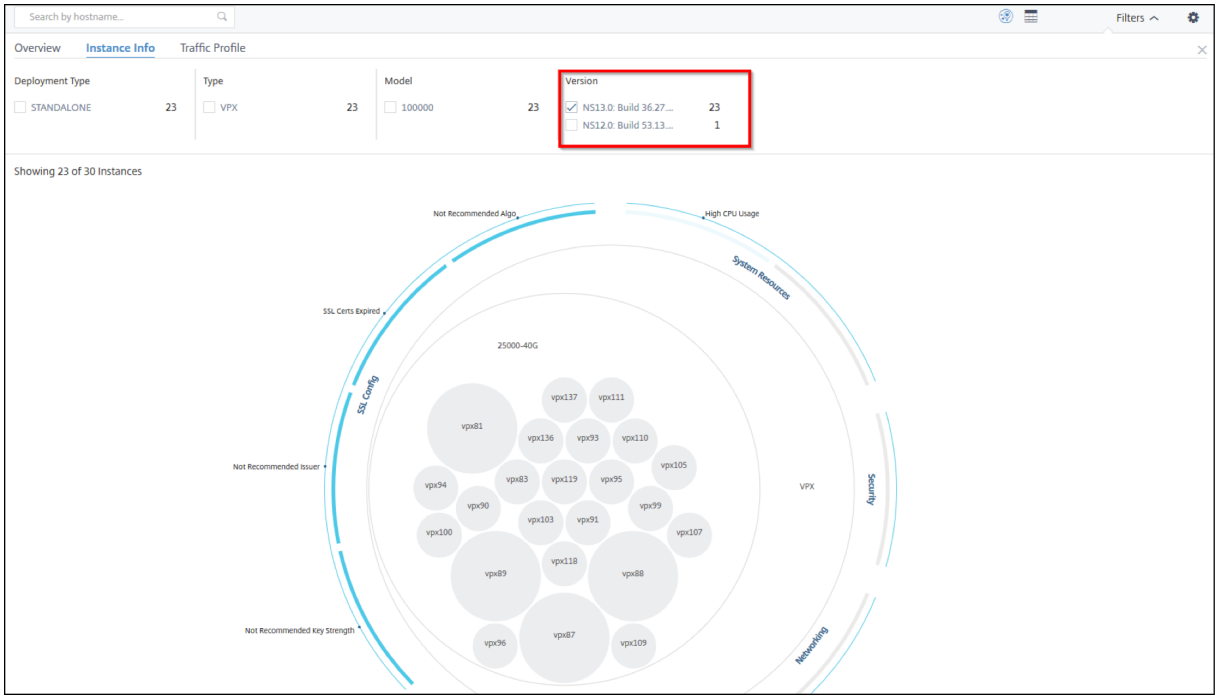
2 - En la sección **Caducidad de los certificados SSL**, seleccione la casilla de verificación **Vencidos** para ver las instancias.

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.

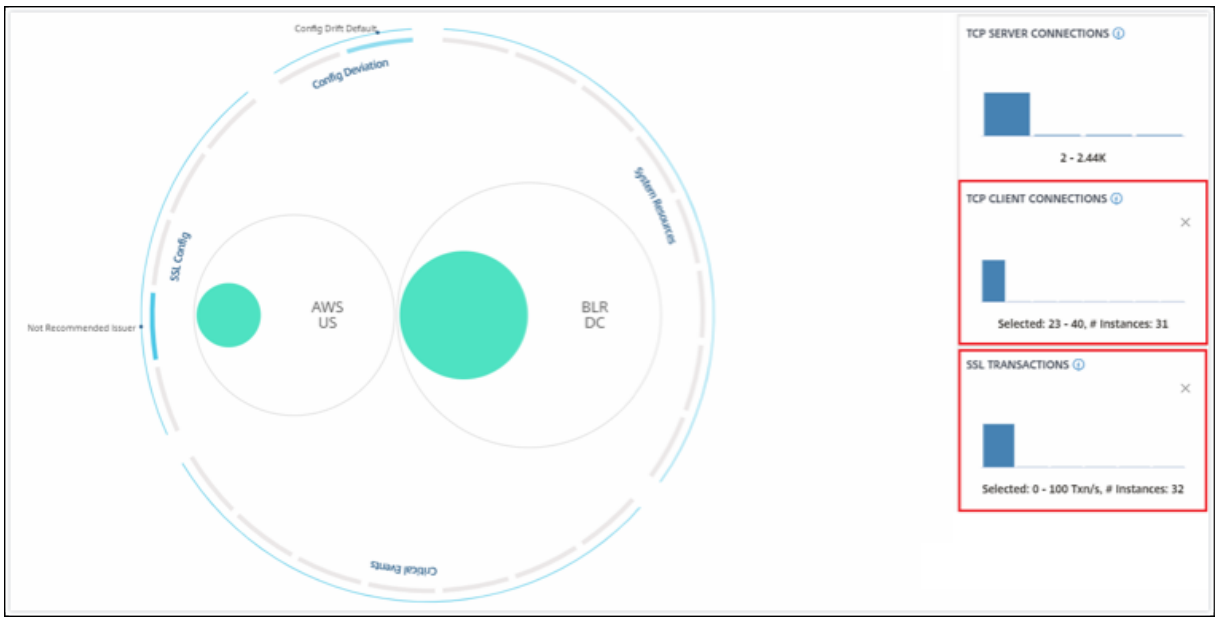


Perfil de tráfico

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 entre 23 y 40, y que también procesan hasta 100 transacciones SSL por segundo.



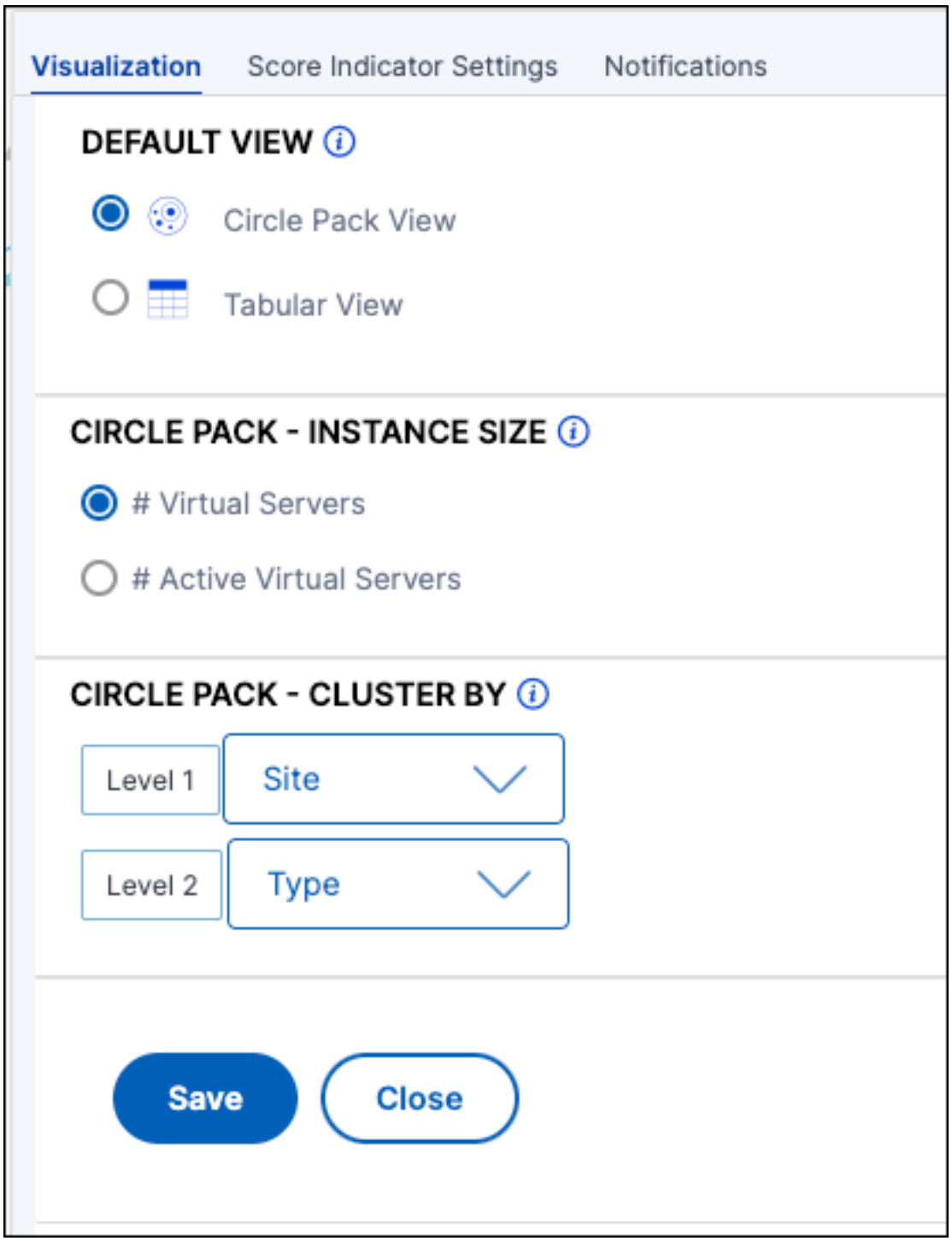
Cómo usar el panel de configuración

El panel de **ajustes** le permite:

- Configure la vista predeterminada de Infrastructure Analytics.
- Establezca los valores de umbral bajo y alto para un uso elevado de la CPU, un uso elevado del disco y un uso elevado de la memoria.
- Seleccione las métricas de la instancia, configure los umbrales y asigne una ponderación a esas métricas para calcular la puntuación de la instancia
- Seleccione los problemas requeridos, active las notificaciones para los problemas que infrinjan los umbrales configurados y reciba notificaciones solo para los problemas seleccionados.

Ver

- **Vista predeterminada**. Seleccione el formato **Circle Pack** o Tabular como vista predeterminada en la página de análisis. El formato que seleccione es el que verá cada vez que acceda a la página en NetScaler Console.
- **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.



Seleccione las métricas y personalice la ponderación, por ejemplo, el cálculo

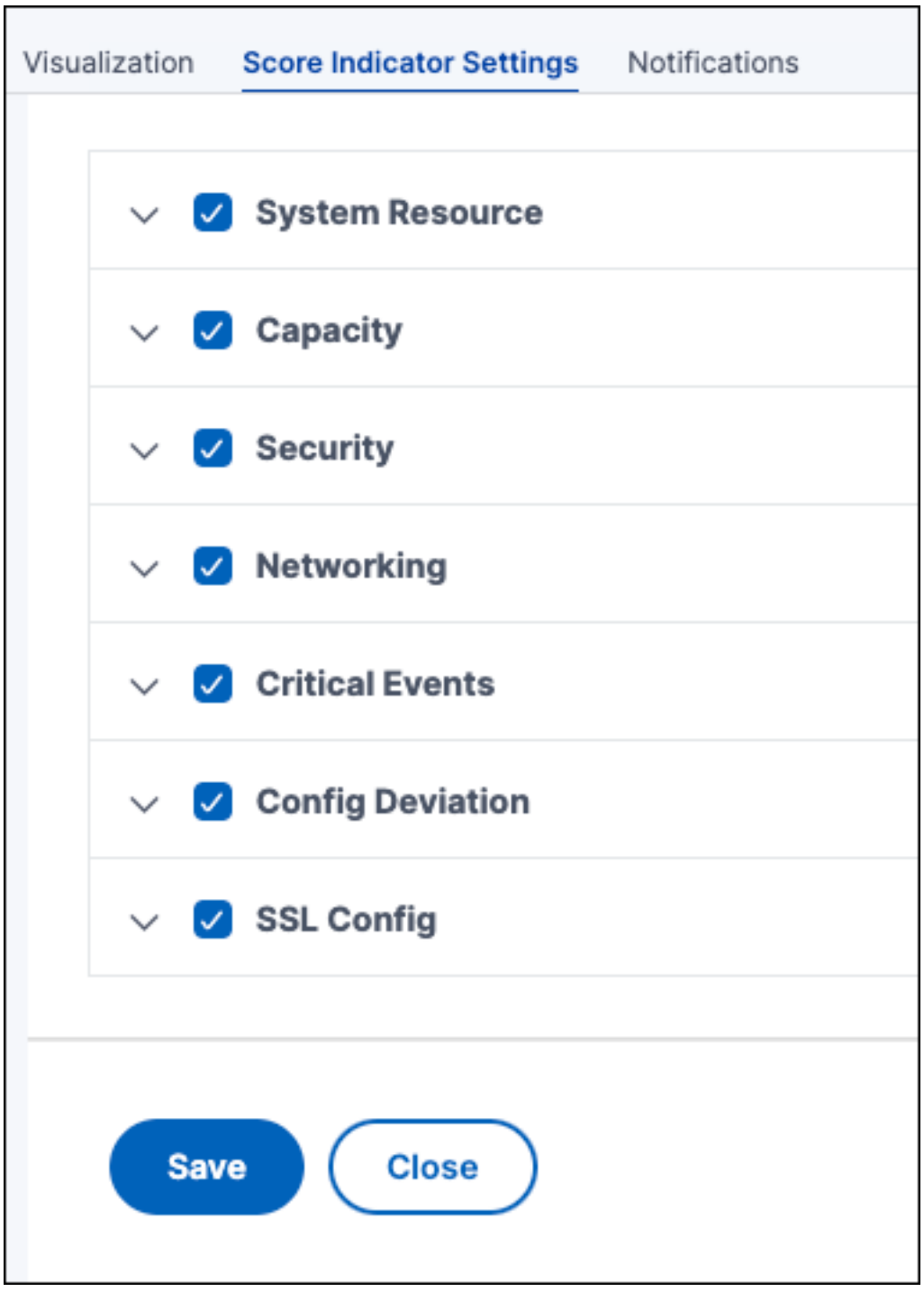
Puede seleccionar las métricas de la instancia, configurar los umbrales y asignar una ponderación a esas métricas para calcular la puntuación de la instancia. De forma predeterminada, se seleccionan todas las métricas y se asigna una ponderación predeterminada a cada métrica. Puede seleccionar

las métricas en función de sus necesidades y asignar una ponderación adecuada para determinar el cálculo de la puntuación de la instancia.

Haga clic en el icono de **Configuración** y seleccione la ficha **Configuración del indicador de puntuación** para:

- Seleccione las métricas necesarias y agregue umbrales
- Asigne la ponderación de las métricas.

Después de configurar los umbrales y asignar el peso, haga clic en **Guardar**. La puntuación de la instancia solo se actualiza en función de las métricas seleccionadas y su ponderación.



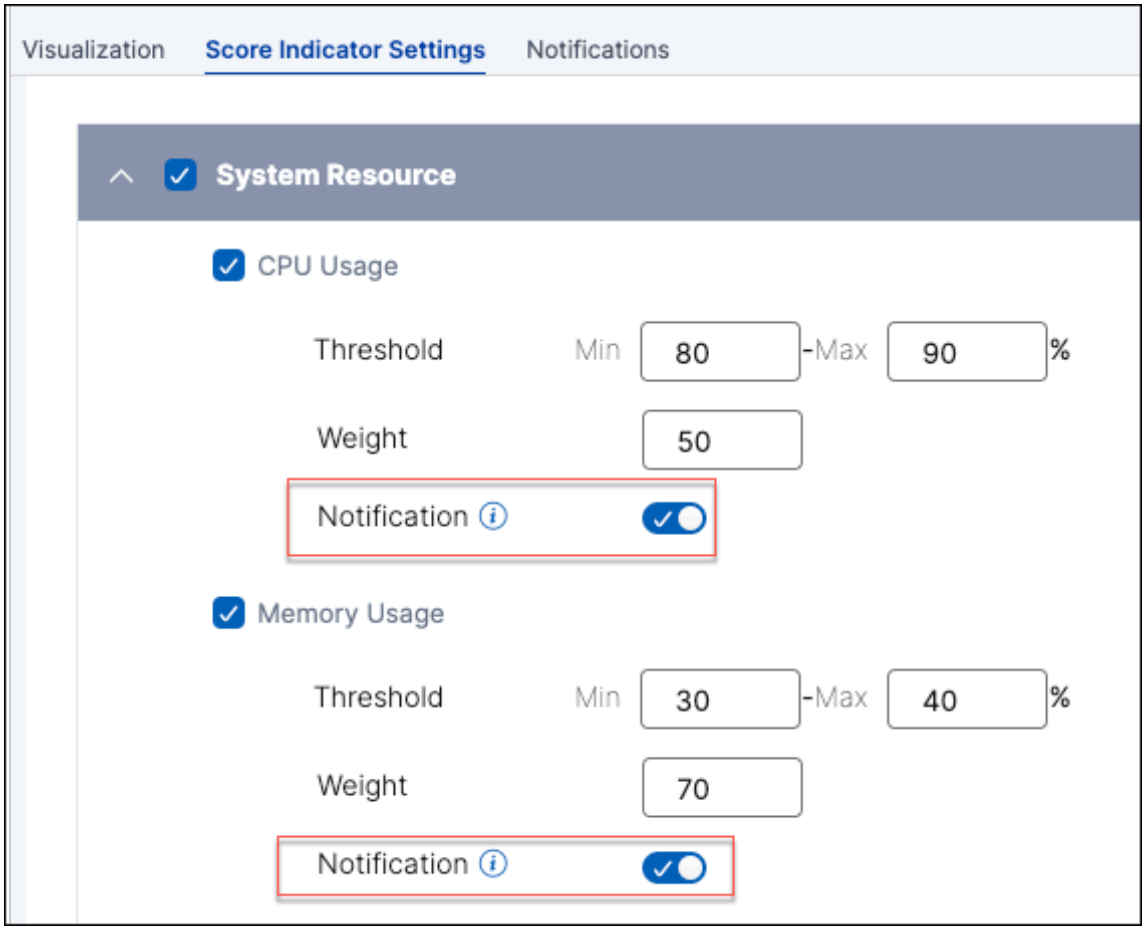
Configurar notificaciones

Puede seleccionar los problemas requeridos, habilitar las notificaciones para los problemas que infrinjan los umbrales configurados y recibir notificaciones solo para los problemas seleccionados. Esta mejora le permite recibir notificaciones solo para los problemas seleccionados que quiera

supervisar.

> **Nota:**
>
> De forma predeterminada, se seleccionan los números de todas las categorías. Puede habilitar la notificación solo para los problemas en los que puede configurar los umbrales.

1. Haga clic en el icono de **Configuración** y seleccione la ficha **Configuración del indicador de puntuación**.
2. Selecciona los problemas sobre los que quieres recibir notificaciones.
3. Para los problemas de las categorías **Recursos y**Capacidad**del sistema**, habilite la **Notificación**.



4. Haga clic en **Guardar**.

> **Nota:**
>
> Debe asegurarse de configurar al menos un perfil en la ficha **Notificaciones**.

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 esto con más detalle, consideremos el caso de Chris, un administrador de red de ExampleCompany.

Chris mantiene muchas instancias de NetScaler en su organización. Algunas de las instancias procesan mucho tráfico y él necesita monitorearlas de cerca. Observa que algunas instancias de alto tráfico ya no procesan todo el tráfico que pasa por ellas. Para analizar esta reducción, anteriormente tuvo que leer varios informes de datos provenientes de varias fuentes. Chris tuvo que dedicar más tiempo a intentar correlacionar los datos de forma manual y averiguar qué instancias no se encuentran en un estado óptimo y requieren atención. Utiliza la función Infrastructure Analytics 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". Hace clic en la 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, por lo tanto, esa 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.

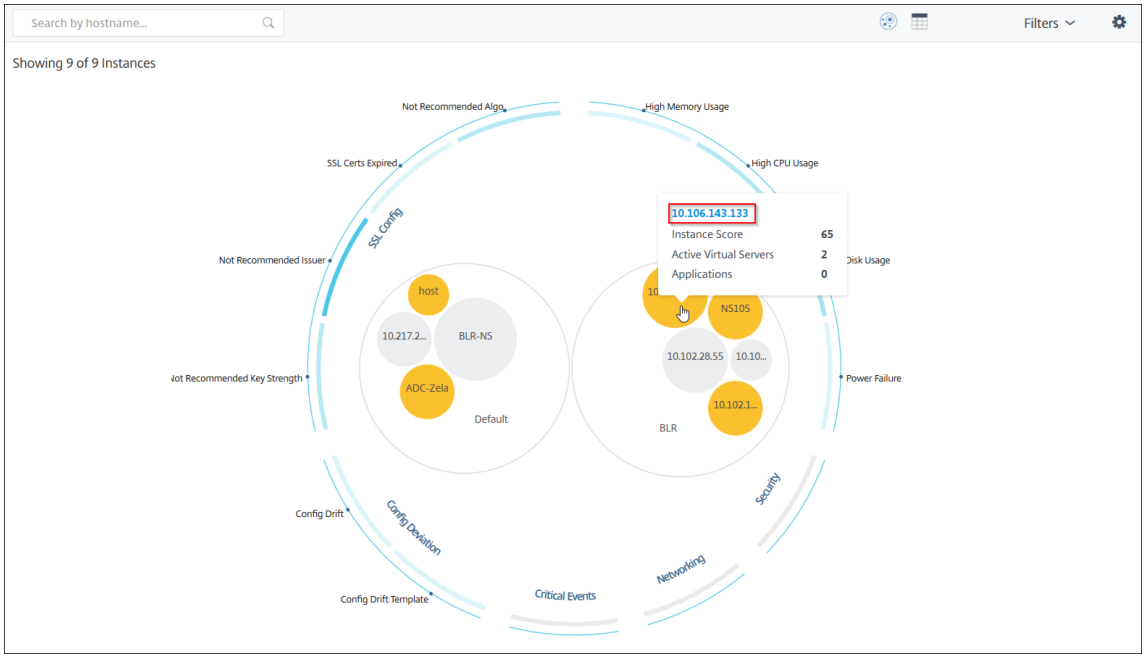
Ejemplo 2: Para supervisar los cambios de configuración:

Chris también observa que otra instancia está en estado "Revisar"y que recientemente se ha producido una desviación de configuración. Al hacer clic en el indicador de riesgo de desviación de la configuración, observa 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. También observa que el perfil de tráfico de transacciones SSL de esta instancia ha caído. Exporta este informe y lo envía al administrador para obtener más información.

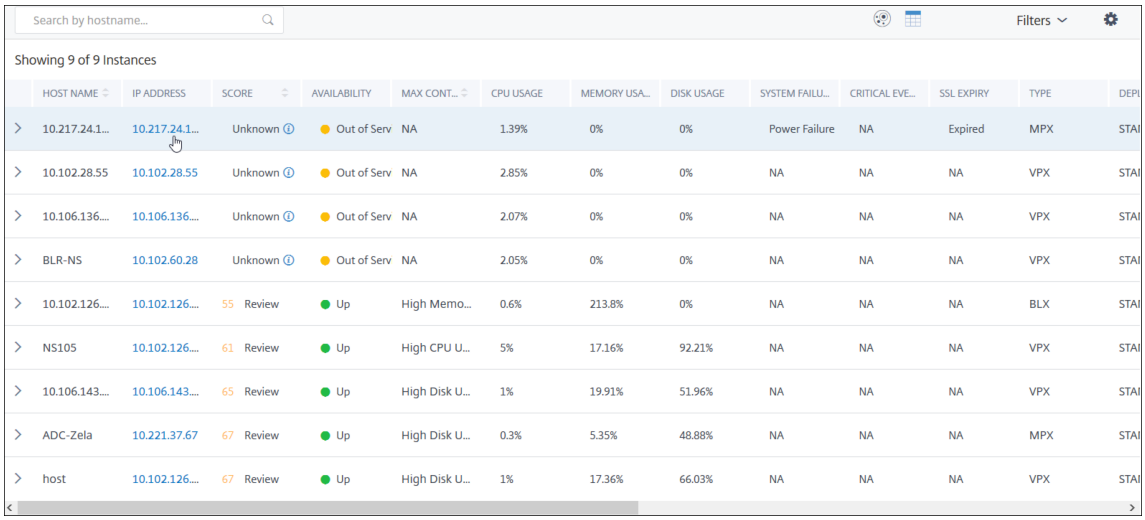
Ver detalles de instancia en Infrastructure Analytics

January 26, 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 NetScaler
- **Dirección**IP : indica la dirección IP de la instancia de NetScaler
- **Puntuación**: indica la puntuación de la instancia de NetScaler y el estado, como Crítico, Bueno y Justo
- **Disponibilidad**: indica el estado actual de la instancia de NetScaler, como **Activa**, **Inactiva**o **Fuera de servicio**.
- **Contribución**máxima : indica la categoría de problema en la que la instancia de NetScaler tiene el máximo número de errores.
- **Uso de la CPU**: indica el% de CPU actual que utiliza la instancia

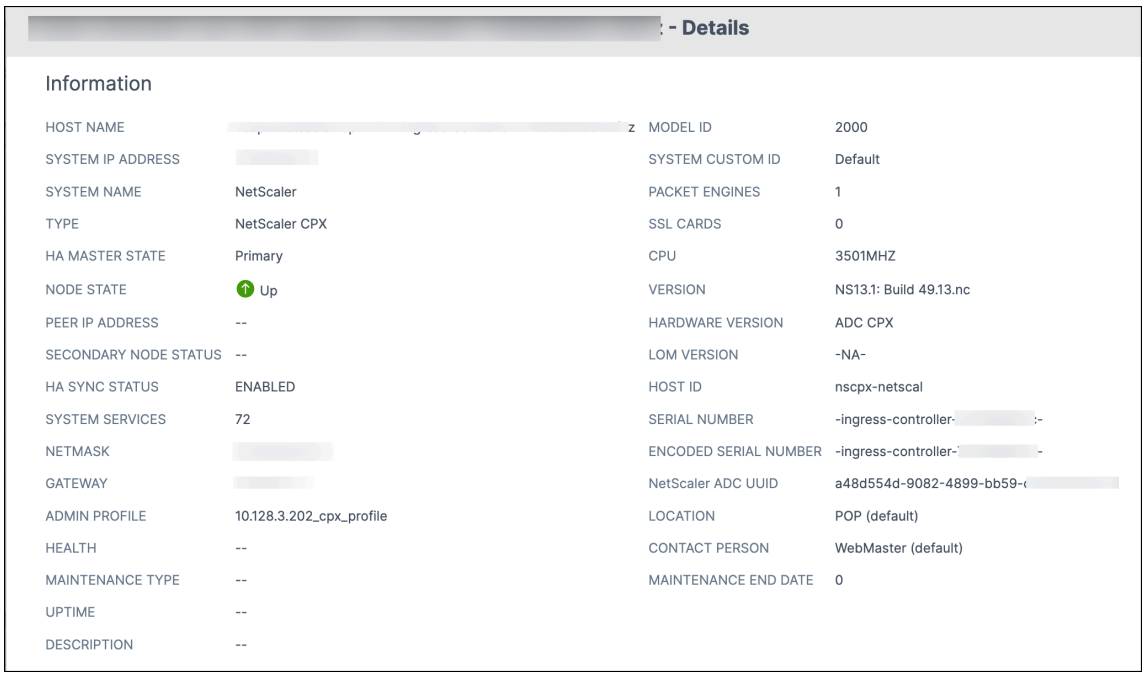
- **Uso de memoria**: indica el% de memoria actual que utiliza la instancia
- **Uso del disco**: indica el% de disco actual utilizado por la instancia
- **Fallo del sistema**: indica el número total de errores del sistema de instancias
- **Eventos críticos**: Indica la categoría de eventos en la que la instancia NetScaler tiene el máximo de eventos
- **Caducidad**de SSL : indica el estado actual del certificado SSL instalado en la instancia de NetScaler
- **Tipo**: indica el tipo de instancia de NetScaler, como VPX, SDX, MPX o CPX
- **Implementación**: indica si la instancia de NetScaler se implementa como una instancia independiente o un par de alta disponibilidad
- **Modelo**: indica el número de modelo de la instancia de NetScaler
- **Versión**: indica la versión y el número de compilación de la instancia de NetScaler
- **Rendimiento**: indica el rendimiento actual de la red desde la instancia de NetScaler
- **Solicitud HTTPS por**segundo: indica las solicitudes HTTPS actuales por segundo recibidas por la instancia de NetScaler
- **Conexión TCP**: indica las conexiones TCP actuales establecidas
- **Transacción**SSL : indica las transacciones SSL actuales procesadas por la instancia de NetScaler
- **Sitio**: indica el nombre del sitio en el que está implementada la instancia de NetScaler.

> **Nota:**
>
> Cada 5 minutos, se actualizan los valores actuales de uso de la CPU, de memoria, de disco, de rendimiento, etc.

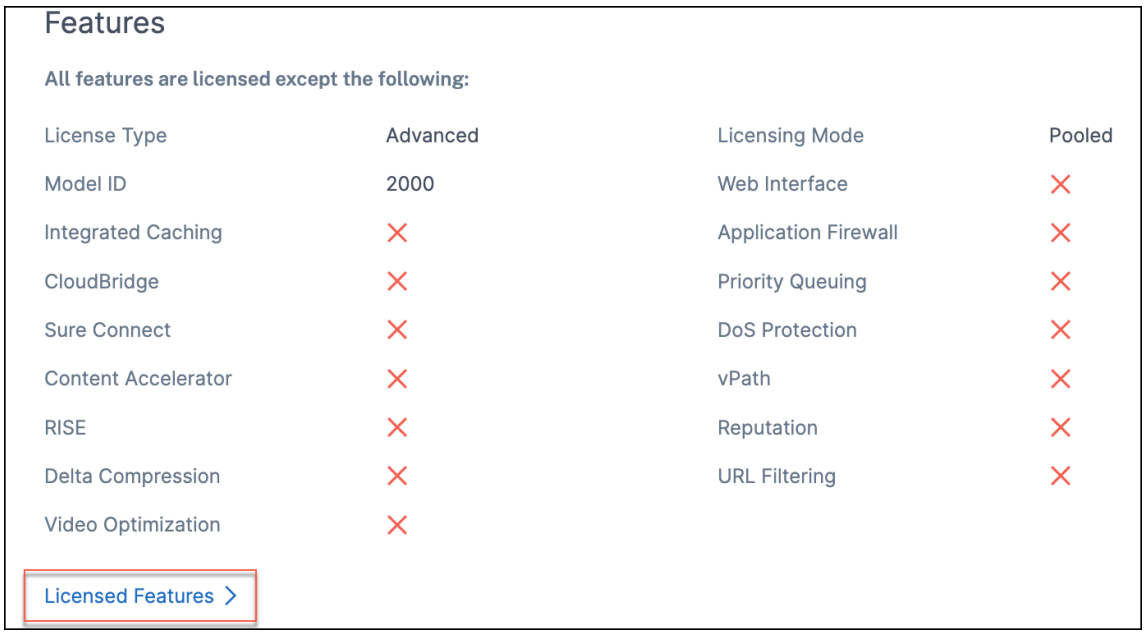
Haga clic en una dirección IP y, en la página que aparece, haga clic en **Detalles de la instancia** para ver los detalles de la instancia.

Se muestran los siguientes detalles:

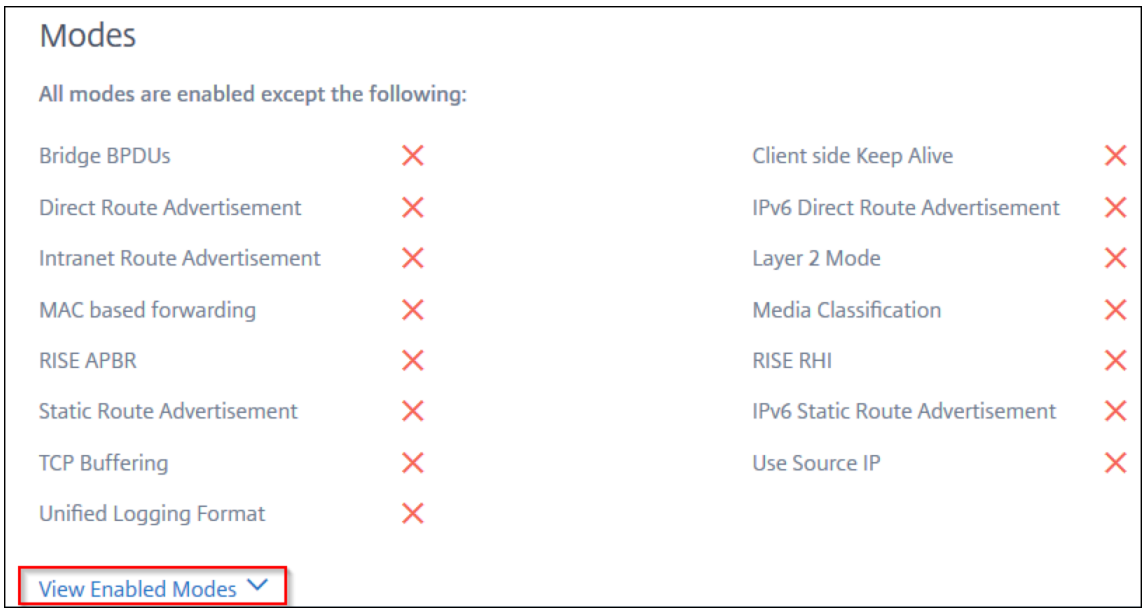
- **Información**: detalles de la instancia, como el tipo de instancia, el tipo de implementación, la versión, el modelo, etc.



- **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.

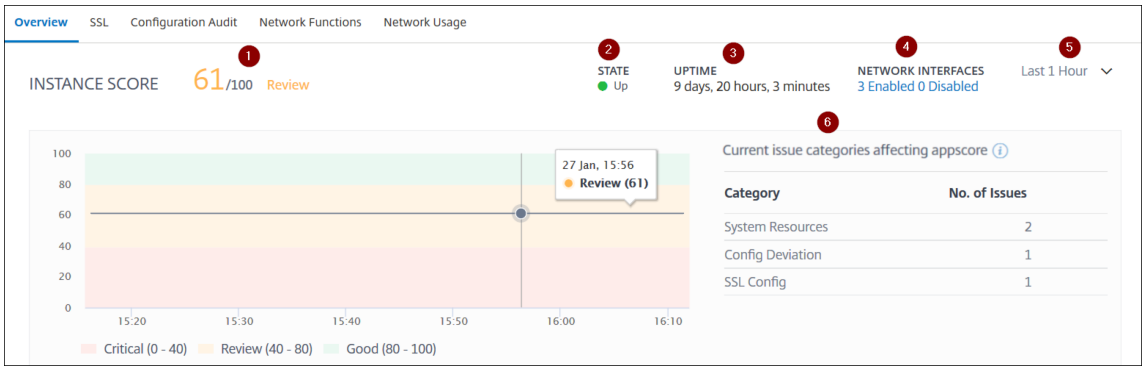


- **Modos**: de forma predeterminada, se muestran todos los modos que están inhabilitados en la instancia. Haga clic en **Ver modos habilitados** para ver los modos habilitados en la instancia.



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 actual 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 en **Activadoo Desactivado** para ver los detalles, como el nombre de la interfaz de red y el estado (activado o desactivado).

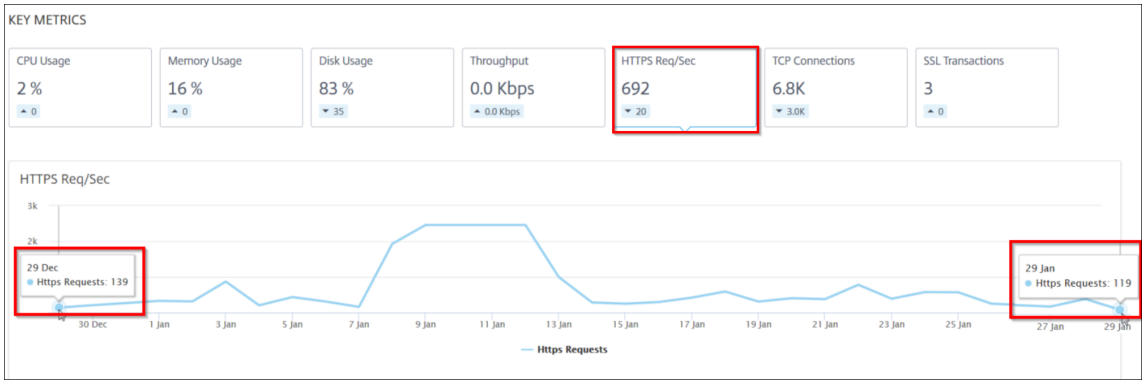
5 —Seleccione la duración del tiempo de la lista para ver los detalles de la instancia.

6: Muestra el total de problemas y la categoría de problemas de la instancia de NetScaler.

- **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.

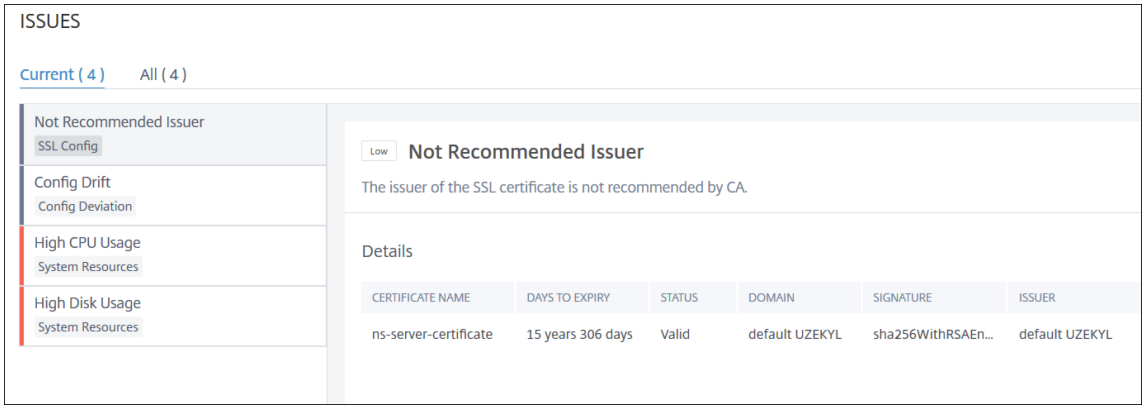
- **Problemas**

  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 el recurso del sistema NetScaler, como CPU, memoria, uso del disco, etc.	– 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 – Algo 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 – Estado de mala seguridad

Categoría de problema	Descripción	Problemas
Cuestiones de capacidad	Muestra los problemas de capacidad de NetScaler. La consola de NetScaler sondea estos eventos cada cinco minutos desde la instancia de NetScaler y muestra las caídas de paquetes o los incrementos del contador de límite de velocidad, si existen. Los problemas se clasifican en los siguientes parámetros de capacidad.	– HA No Heat Beats – Fallo de sincronización de HA – No coincide la versión de HA – Se alcanzó el límite de rendimiento
Redes	Muestra los problemas operativos que se producen en las instancias.	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 NetScaler

January 26, 2024

Cuando una instancia de NetScaler ha consumido la mayor parte de su capacidad disponible, es posible que se descarten paquetes mientras se procesa el tráfico del cliente. Este problema provoca un bajo rendimiento en una instancia de NetScaler. Al comprender estos problemas de capacidad de NetScaler, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento de NetScaler.

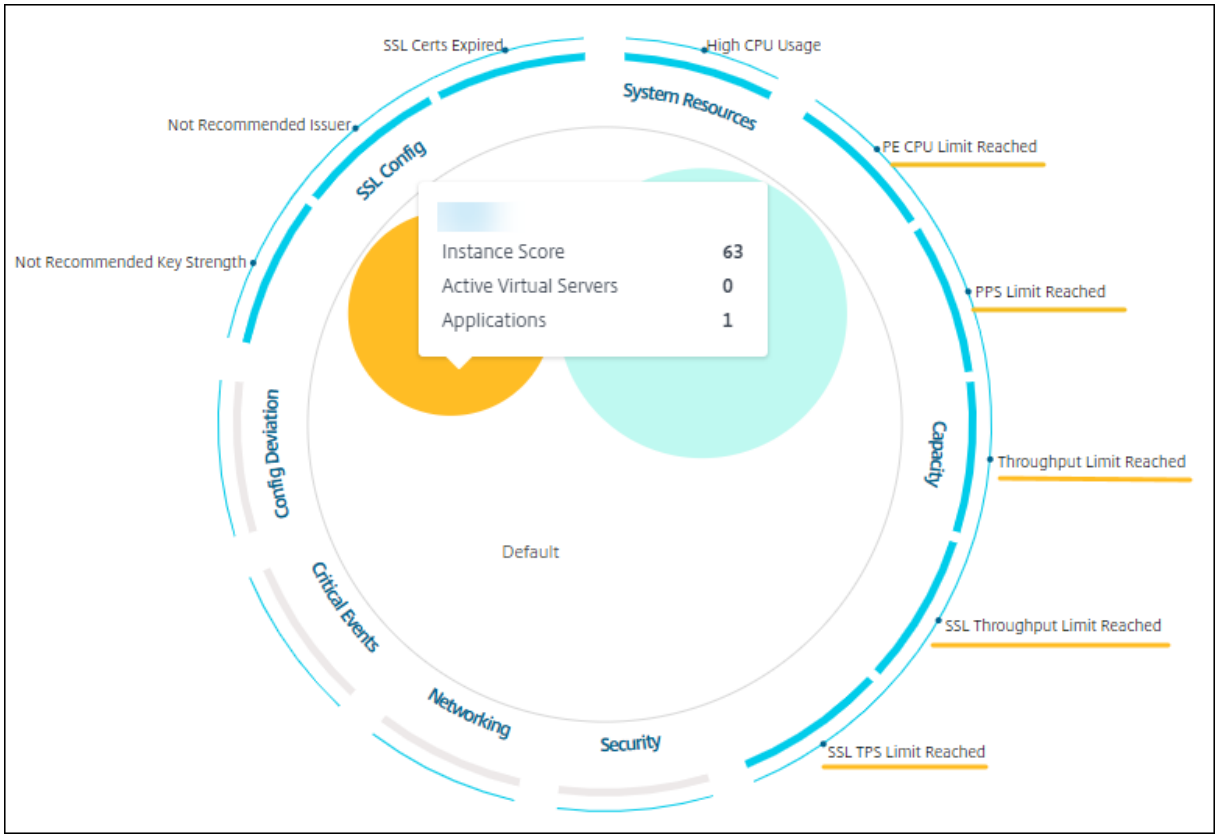
En **Circle Pack View** , puede ver los problemas de capacidad de las instancias de NetScaler, si los hay.

Para ver los problemas de capacidad de NetScaler,

1. Vaya a **Infraestructura > Análisis de infraestructura**.
2. Seleccione la vista de paquete de círculos.

> **Nota:**
>
> En **Infrastructure Analytics**, las vistas tabulares y de paquete circular muestran los eventos y problemas que se han producido en la última hora.

La siguiente ilustración sugiere los problemas de capacidad existentes en la instancia seleccionada:



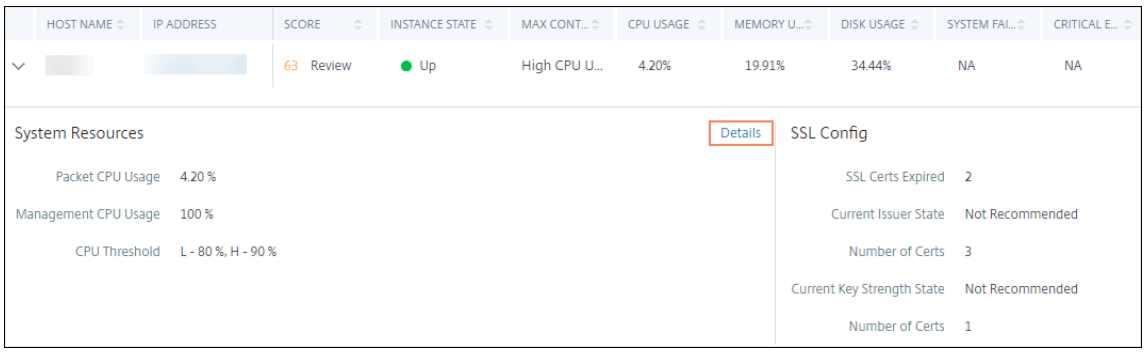
Los problemas se clasifican según los siguientes parámetros de capacidad:

- **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.
- **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.

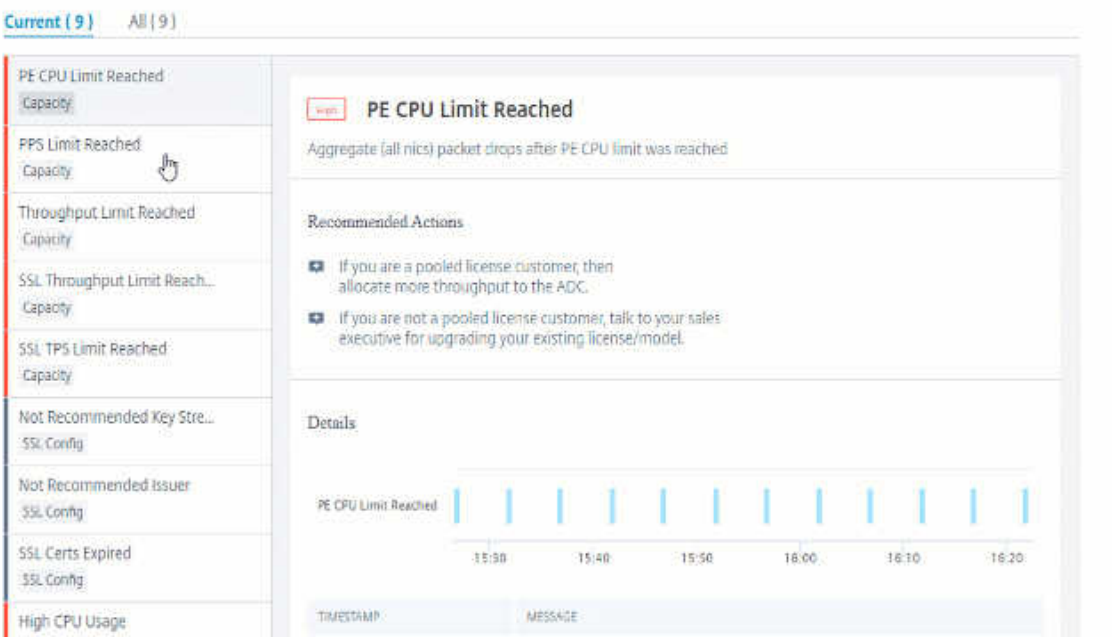
Vea las acciones recomendadas para resolver problemas de capacidad

La consola de NetScaler recomienda acciones que pueden resolver los 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.



La consola de NetScaler sondea estos eventos cada cinco minutos desde la instancia de NetScaler y muestra las caídas de paquetes o los incrementos del contador de límite de velocidad, si existen.

La consola de NetScaler calcula la puntuación de la instancia según 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 NetScaler 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 **Configuración > Eventos del**

sistema.

Análisis de infraestructura mejorado con nuevos indicadores

January 26, 2024

Con el **análisis de infraestructura** de NetScaler Console , 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.

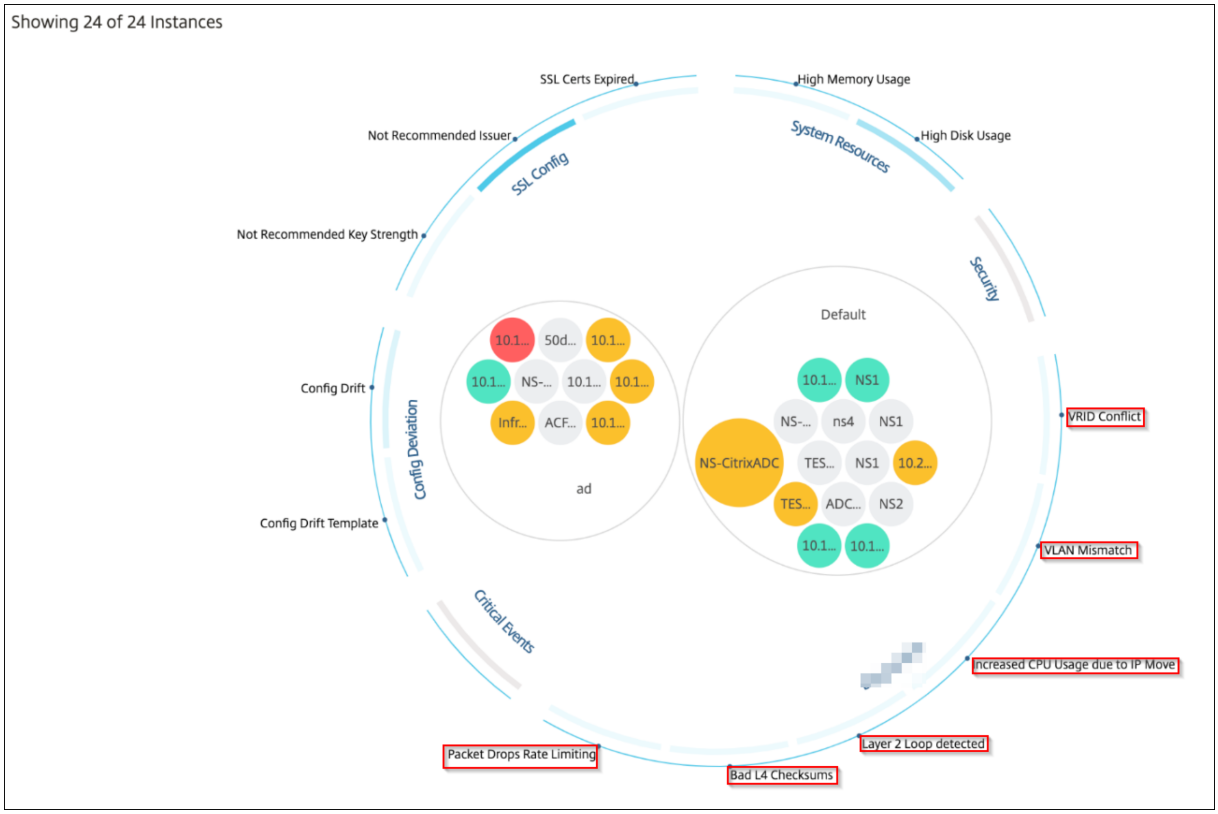
Como administrador, puede identificar rápidamente la causa principal del análisis de los problemas.

> **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 Console, vaya a **Infrastructure > Infrastructure Analytics** para ver los indicadores de:

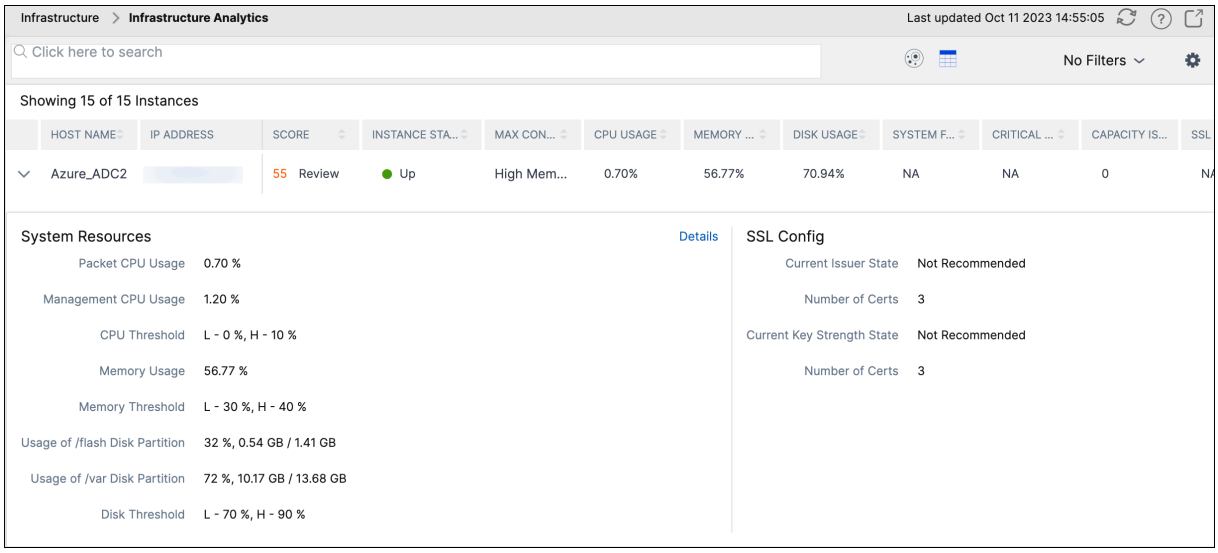
Nombre del indicador en Infrastructure Analytics	Descripción
Error de asignación de puertos	Detecta cuándo NetScaler usa SNIP para comunicarse con una nueva conexión de servidor y el total de puertos disponibles en ese SNIP está agotado. La acción recomendada es agregar otro SNIP en la misma subred.
Acumulación de sesiones	Detecta cuándo las sesiones SSL retienen la memoria de NetScaler.
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.

Nombre del indicador en Infrastructure Analytics	Descripción
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 informativa, porque NetScaler 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.



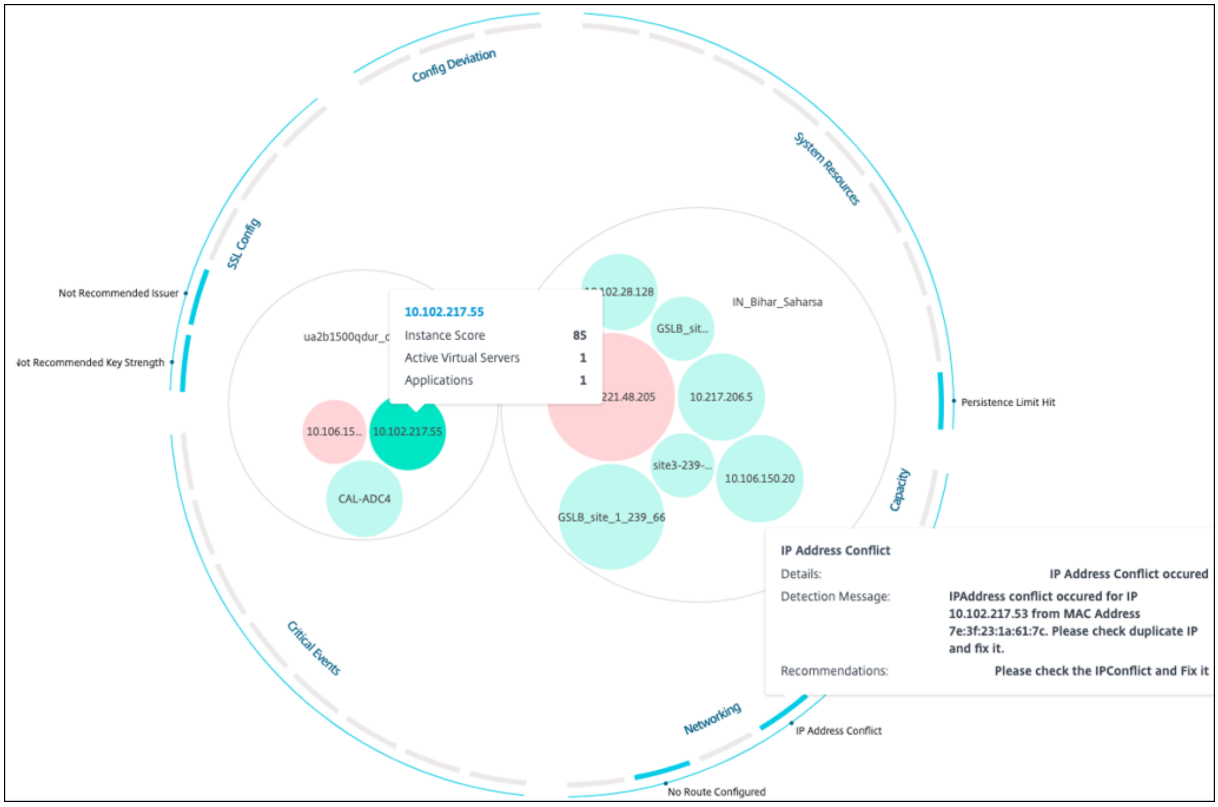
Vista tabular

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 quiere ver los detalles del **conflicto de direcciones IP** en la red, haga clic en la anomalía que aparece para el conflicto de direcciones IP.



- **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 procedimiento de solución de problemas para resolver este conflicto de direcciones IP

Administración de instancias

September 2, 2024

Las instancias son dispositivos Citrix Application Delivery Controller (ADC) que se pueden administrar, supervisar y solucionar problemas mediante NetScaler Console. Añada instancias a NetScaler Console para supervisarlas. Las instancias también se pueden agregar al configurar NetScaler Console o más adelante. Después de añadir instancias a NetScaler Console, se consultan continuamente

para recopilar información que luego se puede utilizar para resolver problemas o como datos de generación de informes.

Las instancias se pueden agrupar como un grupo estático o como un bloque IP privado. Un grupo estático de instancias puede ser útil cuando se quiere ejecutar tareas específicas, como trabajos de configuración y otras. Un bloque IP privado agrupa sus instancias en función de sus ubicaciones geográficas.

Agregar una instancia

Puede agregar instancias al configurar el servidor de NetScaler Console por primera vez o más adelante. 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 Console, consulte Agregar instancias a NetScaler Console.

Cuando agrega una instancia al servidor de NetScaler Console, el servidor se agrega implícitamente como destino de captura para la instancia y recopila un inventario de la instancia. Para obtener más información, consulte [Cómo NetScaler Console descubre instancias.] (http://docs.citrix.com/en-us/netscaler-mas/12-1/overview/how-mas-discovers-instances.html)

Después de agregar una instancia, puede eliminarla yendo a **Infraestructura > Instancias y seleccionando la categoría de instancias**. A continuación, selecciona la instancia que deseas eliminar y haga clic en **Eliminar**.

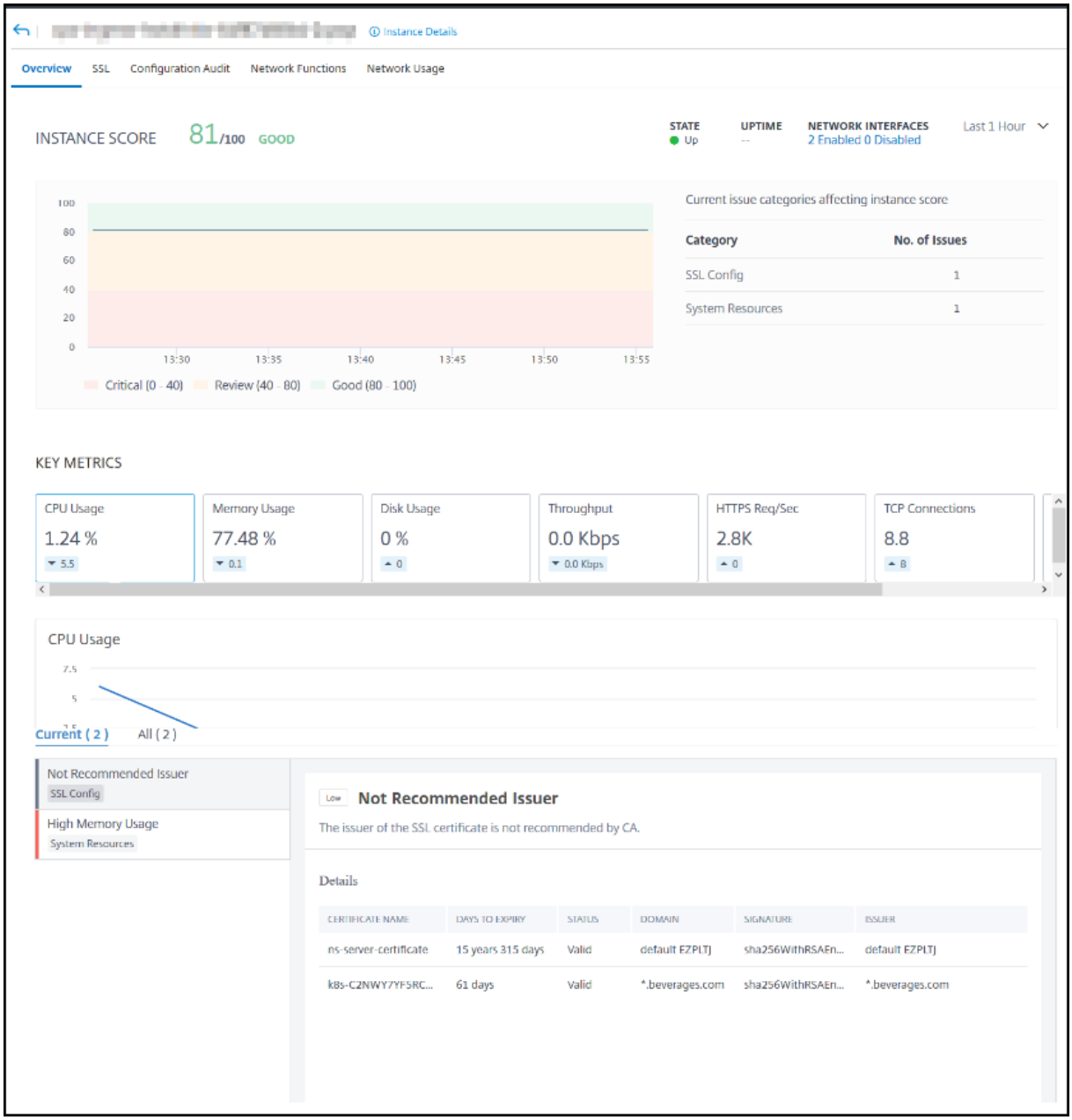
Cómo usar el panel de instancias

El panel de control por instancia de NetScaler Console 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 > NetScaler**. En la página NetScaler, 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 y otros. 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. El estado **guardado** de la configuración de **NetScaler y los gráficos de deriva** de la configuración de NetScaler del panel muestran detalles de alto nivel sobre los cambios de configuración guardados en comparación con las configuraciones 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"en la esquina inferior derecha de la pantalla para agregar otro informe de rendimiento.

Cómo supervisar sitios distribuidos globalmente

June 7, 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 Console le proporciona una representación gráfica de sus sitios y desglosa su experiencia de monitoreo de redes por ubicación geográfica. Con las geometrías, puede visualizar la distribución de instancias de red por ubicación y supervisar los problemas de red.

En las siguientes secciones se explica cómo puede supervisar los centros de datos en NetScaler Console.

Supervisión de sitios distribuidos por todo el mundo en NetScaler Console

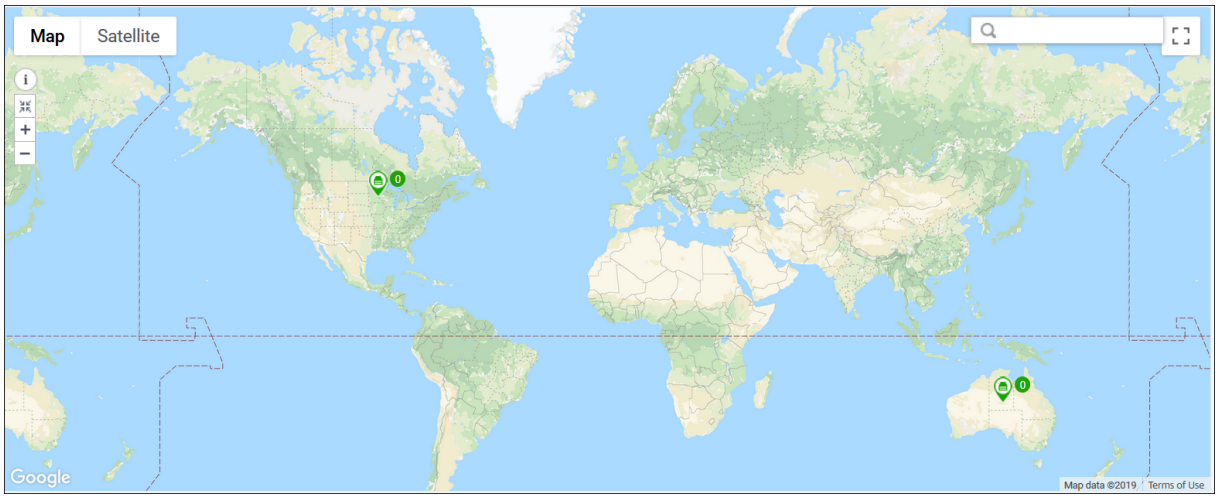
El sitio de NetScaler Console es una agrupación lógica de instancias de Citrix Application Delivery Controller (NetScaler) en una ubicación geográfica específica. Por ejemplo, mientras que un sitio está asignado a Amazon Web Services (AWS) y otro sitio puede estar asignado a Azure™. Otro sitio más está alojado en las instalaciones del arrendatario. NetScaler Console administra y monitorea

todas las instancias de NetScaler conectadas a todos los sitios. Puede usar NetScaler Console para supervisar y recopilar syslog, AppFlow, SNMP y cualquier dato similar que se origine en las instancias administradas.

Geomaps de NetScaler Console 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 hacer clic en **Infraestructura** en el menú y aparecerá el **panel de instancias** para obtener una representación visual de los sitios creados en el mapa mundial.

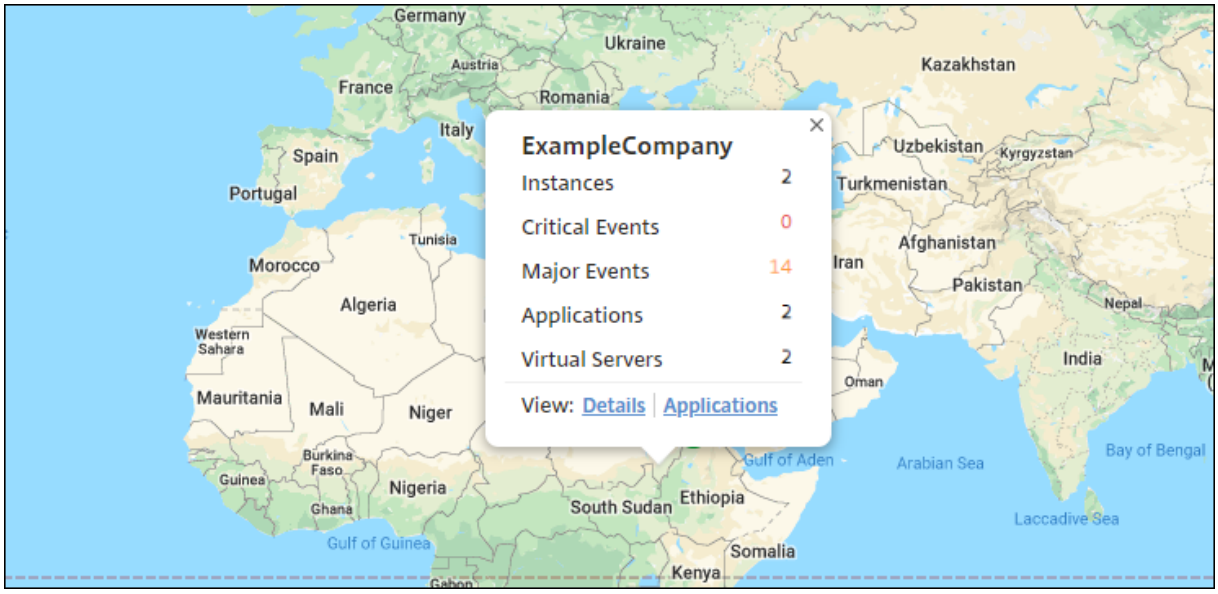
Caso de uso

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 el recuento de los siguientes componentes en el sitio:

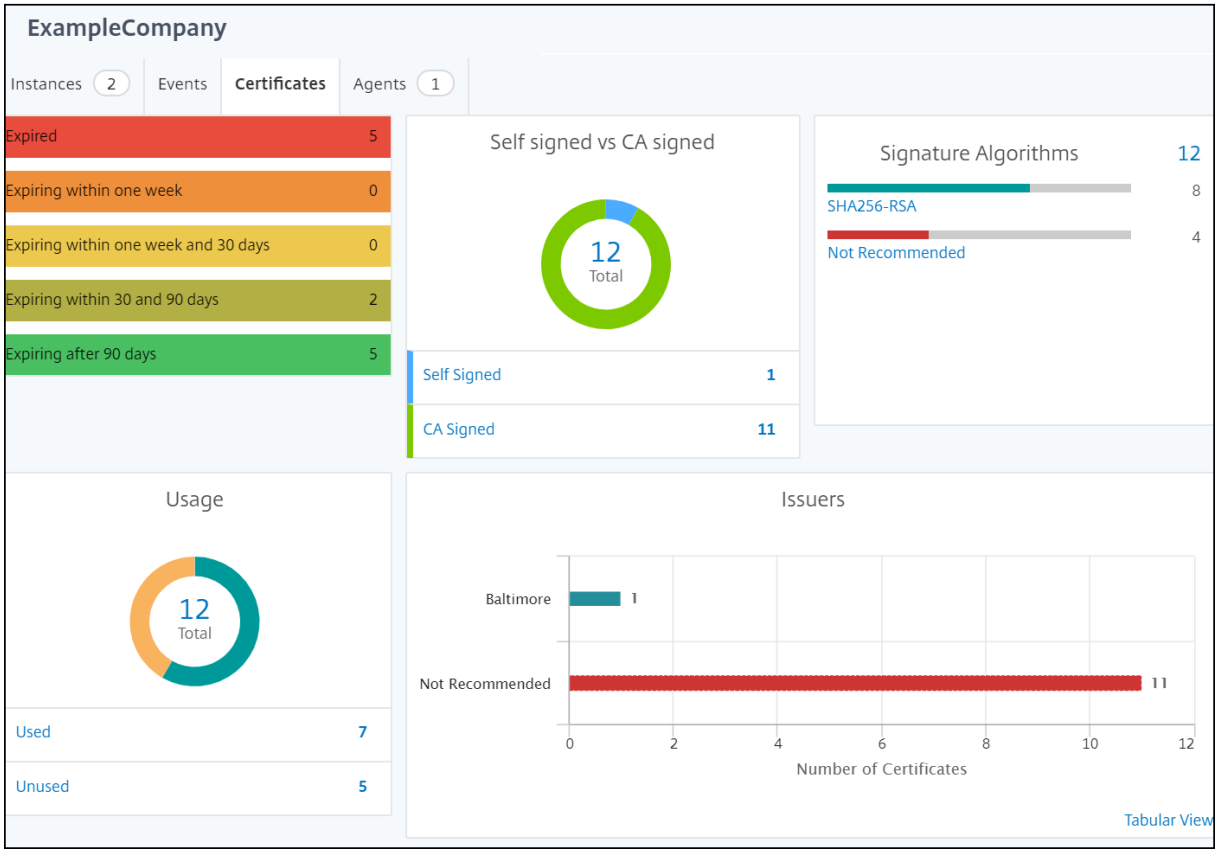
- **Instancias**: indica el número de instancias disponibles.
- **Aplicaciones**: indica el número de aplicaciones alojadas.
- **Servidores virtuales**: Indica el número de servidores virtuales disponibles.
- **Eventos Críticos**: Indica el recuento de eventos críticos ocurridos en las instancias.
- **Eventos**principales : indica que el recuento de eventos importantes se produjo en las instancias.



Haga clic en **Aplicaciones** para ver todas las aplicaciones personalizadas creadas en cada sitio.

Haga clic en **Detalles** para ver una lista de las instancias de NetScaler agregadas en 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 de NetScaler
  - Número de eventos críticos
  - 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 Console. También debe agregar la instancia al sitio, agregar un agente y vincular el agente al sitio. A continuación, NetScaler Console reconoce el sitio al que pertenecen la instancia de NetScaler y el agente.

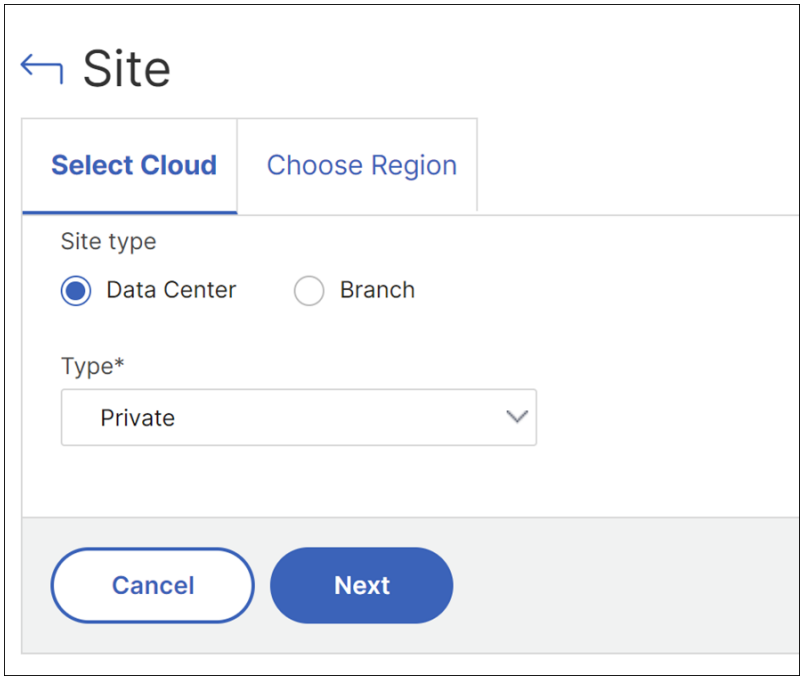
Para obtener más información sobre cómo agregar instancias de NetScaler, consulteAgregar instancias.

Crear un sitio

Cree sitios antes de añadir instancias en NetScaler Console. Proporcionar información de ubicación le permite localizar el sitio con precisión.

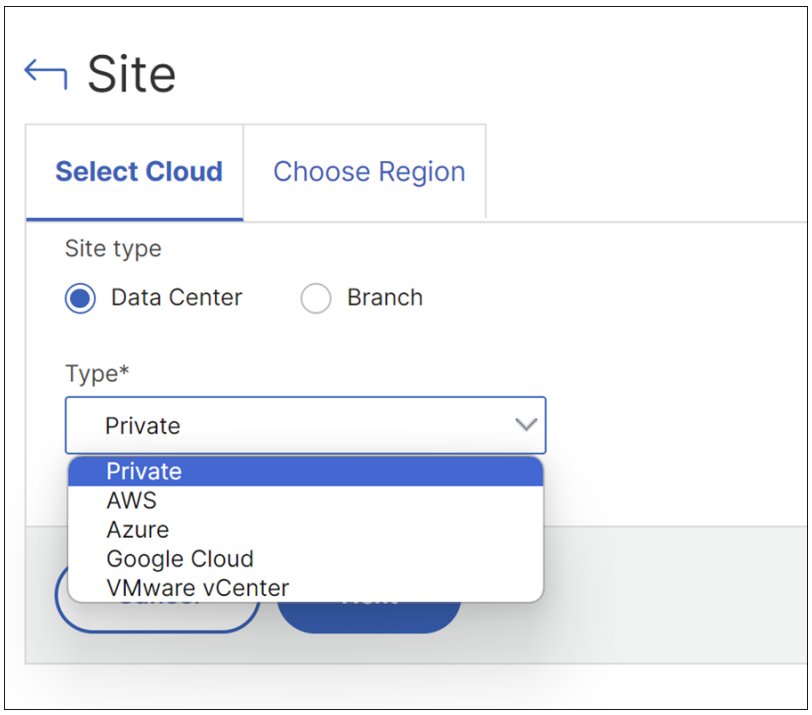
Para crear un sitio:

1. Vaya a **Infraestructura > Instancias > Sitio** . Haga clic en **Agregar**.
2. En la ficha **Seleccionar nube**, elija el **tipo de sitio** . Puede crear un sitio del tipo **Centro de datos** o **Sucursal**.



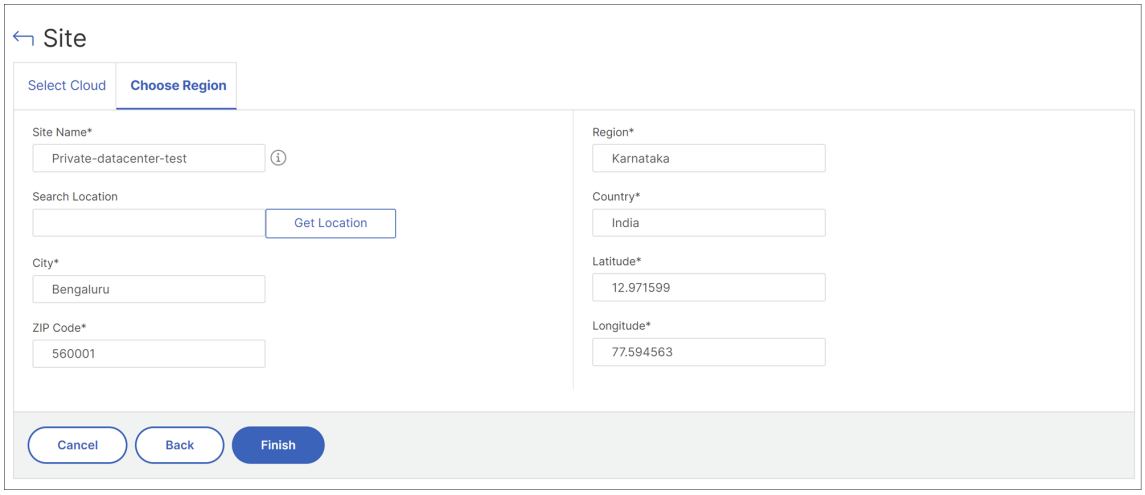
Para el tipo de sitio del centro de datos, seleccione el **Tipo** en la lista:

- Privada
- AWS
- Azure
- Google Cloud
- VMware vCenter



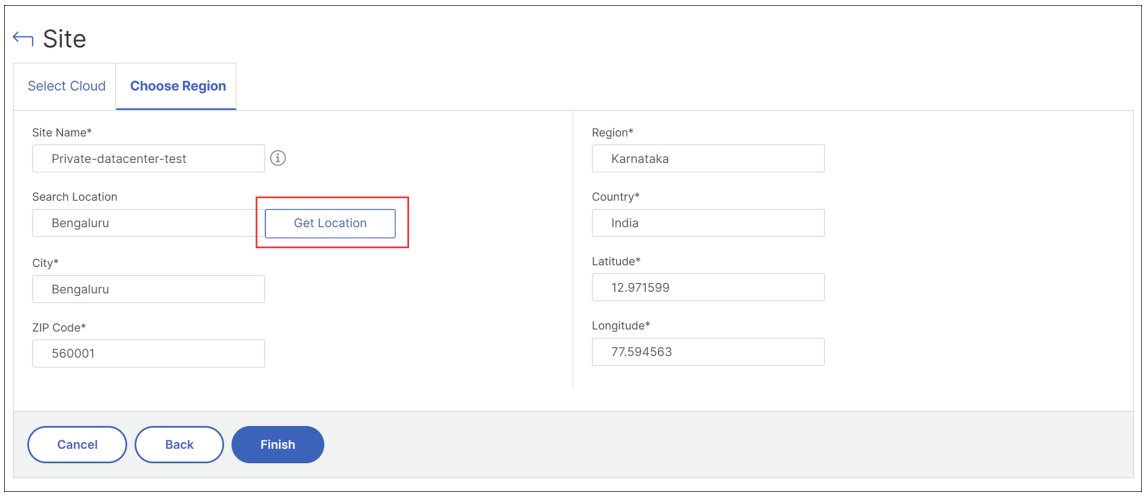
3. Haga clic en **Siguiente**.
4. En la ficha **Elegir región**, introduzca los siguientes detalles:

    - Nombre del sitio
    - City
    - Código postal
    - Region
    - País
    - Latitud
    - Longitud



También puede introducir la ubicación en **Buscar** ubicación y hacer clic en **Obtener ubicación**

para localizar el sitio con precisión. Los campos Ciudad, Código postal, Región, País, Latitud y Longitud se rellenan automáticamente.



5. Haga clic en **Finalizar**.

> **Notas:**
>
> Los pasos descritos son aplicables a:
>
> - Tipo de sucursal.
> - Tipo de sitio de centro de datos con el tipo privado.
> - Cuando la opción de búsqueda no está seleccionada para los tipos de proveedores de nube.

Cree un sitio para los tipos de proveedores de la nube

Puede crear un sitio con un tipo de proveedor de nube y elegir si quiere habilitar o deshabilitar la opción **Fetch** . De forma predeterminada, la opción **Recuperar** no está seleccionada.

La opción **Fetch** (Obtener) solo está disponible para las plataformas AWS, Azure y Google Cloud.

Para obtener instrucciones detalladas sobre cómo crear un sitio para proveedores de nube específicos, consulte las siguientes secciones:

1. Crear un sitio en AWS
2. Crear un sitio en Azure
3. Crear un sitio en Google Cloud
4. Crear un sitio en VMware vCenter

Editar un sitio

Para modificar un sitio existente:

1. Seleccione el sitio y haz clic en **Editar** .
2. En la página **Configurar sitio**, puede actualizar el **tipo de sitio** . Por ejemplo, si seleccionó **Branch** anteriormente, puede actualizar a **Data Center** .
3. Según el tipo de sitio, puede modificar el **tipo** . Por ejemplo, puede cambiar el tipo de un centro de datos privado a una nube pública de la lista.

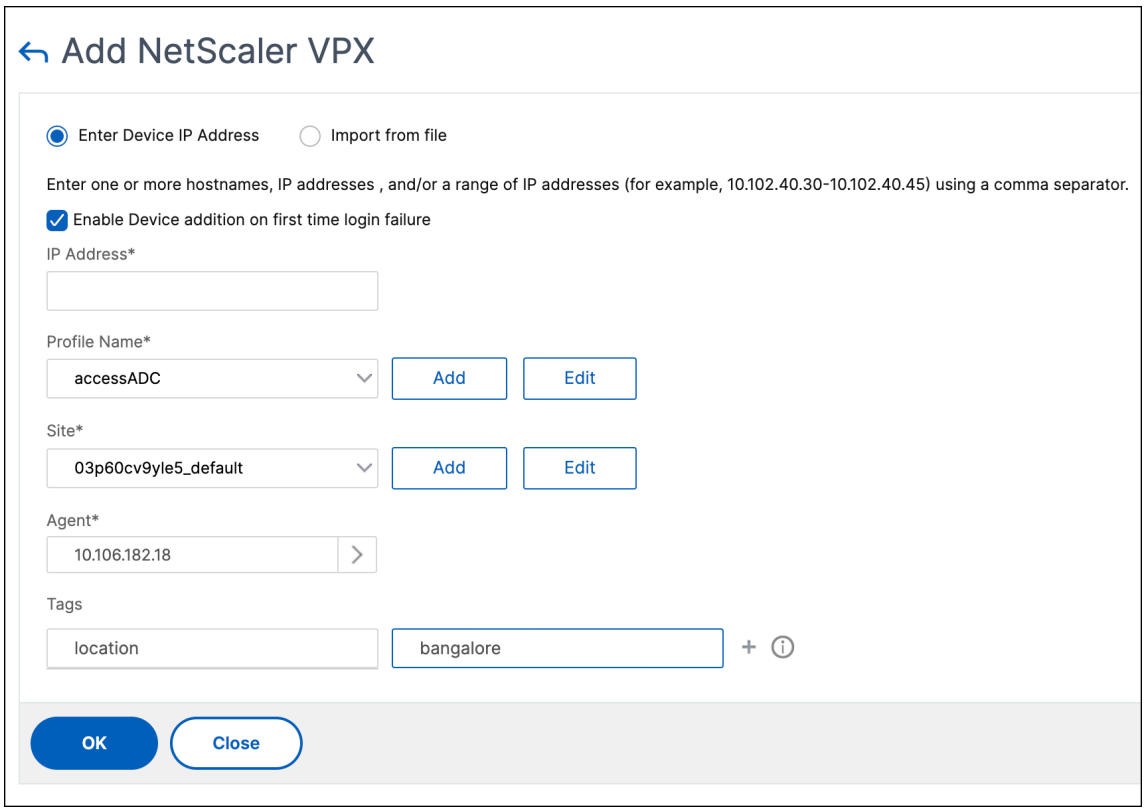
Eliminar un sitio

1. Para eliminar un sitio, selecciónelo y haga clic en **Eliminar** .
2. En la página de confirmación, haz clic en **Sí**.

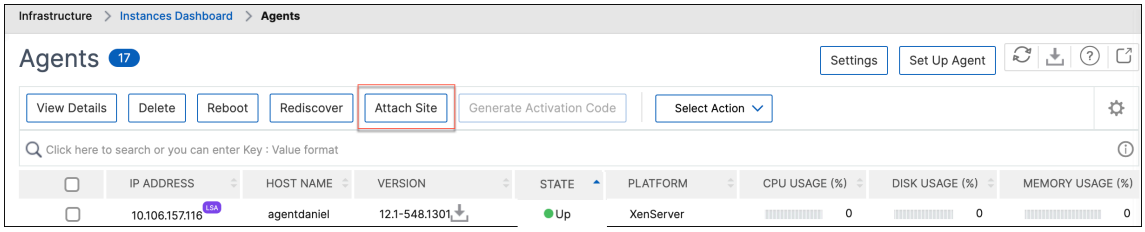
Para agregar instancias y seleccionar sitios:

Tras crear los sitios, debe añadir instancias en NetScaler Console. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

1. En NetScaler Console, vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione el **VPX**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 botón **Agregar** situado junto al campo **Sitio** para crear un sitio o hacer clic en el botón **Modificar** 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**.



   a) Seleccione el sitio de la lista y haga clic en **Guardar**.

7. Opcionalmente, puede introducir campos clave y valor para **Etiquetas**.
8. Haga clic en **Aceptar**.

También puede adjuntar un agente a un sitio navegando a **Infraestructura > Instancias > Agentes**.

Para asociar un agente al sitio:

1. En NetScaler Console, vaya a **Infraestructura > Instancias > Agentes** .
2. Seleccione el agente y haga clic en **Adjuntar sitio**.
3. Puede asociar el sitio y hacer clic en **Guardar**.

NetScaler Console comienza a supervisar las instancias de NetScaler agregadas al sitio de Bangalore, junto con las instancias de los otros dos sitios.

Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** situado en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

> **Nota:**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona **Periodicidad mensual**, asegúrese de introducir todos los días en los que quiere que se programe el informe separados por comas.

Cómo crear etiquetas y asignar a instancias

January 26, 2024

NetScaler Console ahora le permite asociar sus instancias de NetScaler con etiquetas. Una etiqueta es una palabra clave o un término de una palabra que puede asignar a una instancia. Las etiquetas agregan información adicional sobre la instancia. Las etiquetas pueden considerarse metadatos que ayudan a describir una instancia. Las etiquetas le permiten clasificar y buscar instancias basadas en estas palabras clave específicas. También puede asignar varias etiquetas a una sola instancia.

Los siguientes casos de uso le ayudan a entender cómo el etiquetado de las instancias le ayudará a supervisarlas mejor.

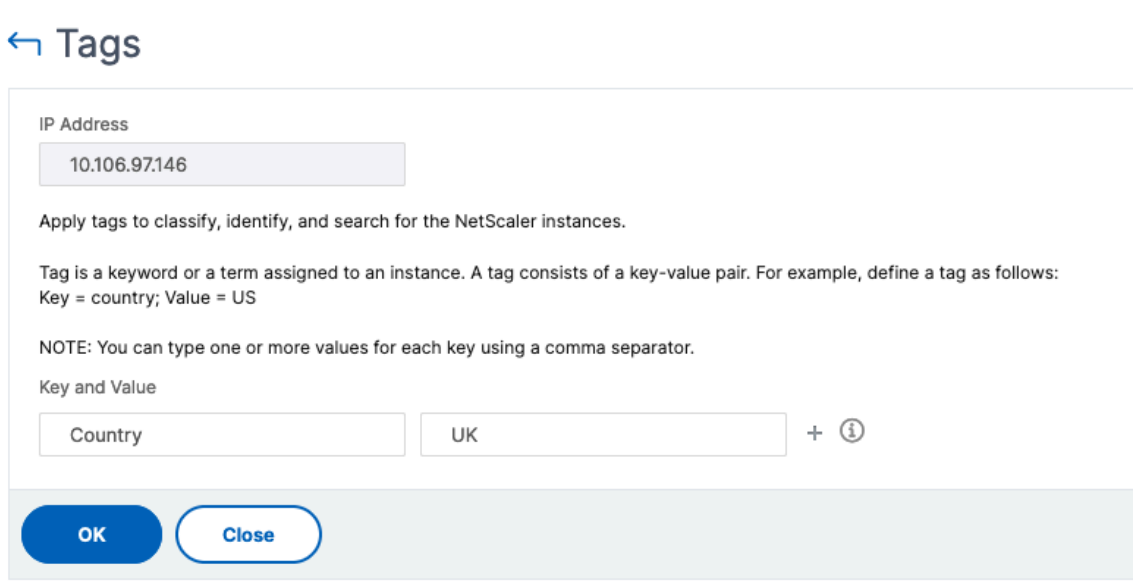
- **Caso de uso 1**: Puede crear una etiqueta para identificar todas las instancias que se encuentran en el Reino Unido. Aquí, puede crear una etiqueta con la clave como "País"y el valor como "Reino Unido". Esta etiqueta le ayuda a buscar y supervisar todas las instancias que se encuentran en el Reino Unido.
- **Caso de uso 2**: Quiere buscar instancias que se encuentran en el entorno provisional. Aquí, puede crear una etiqueta con la clave como "Propósito"y un 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.

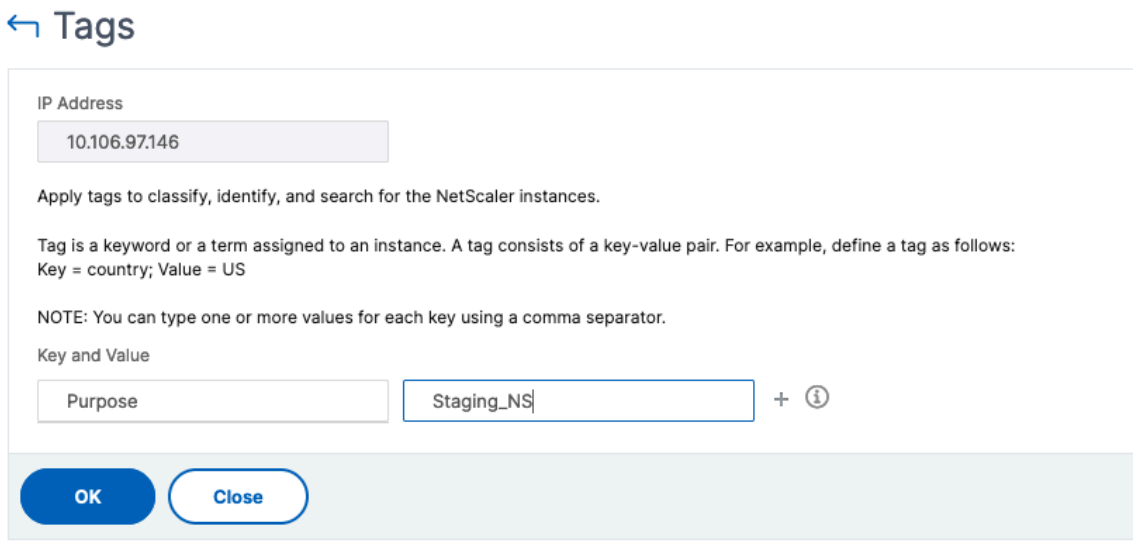
- **Caso de uso 3**: considere una situación en la que quiera conocer la lista de instancias de NetScaler que se encuentran en el área de Swindon en el Reino Unido y que son propiedad de usted, David T. Puede crear etiquetas para todos estos requisitos y asignarlas a todas las instancias que cumplan estas condiciones.

Para asignar etiquetas a la instancia de NetScaler VPX:

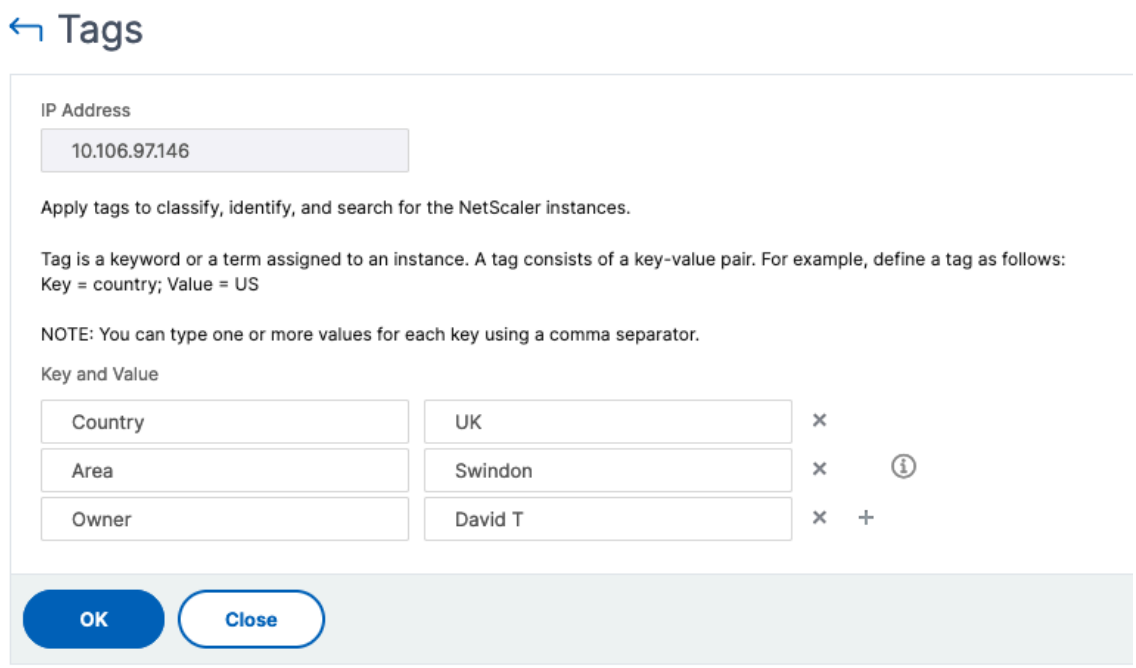
1. En NetScaler Console, vaya a **Infraestructura > Instancias > NetScaler**.
2. Selecciona la ficha **VPX**.
3. Seleccione la instancia VPX requerida.
4. Haga clic en **Etiquetas**. La ventana de **etiquetas** que aparece le permite crear sus propios pares de "clave-valor"asignando valores a cada palabra 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.



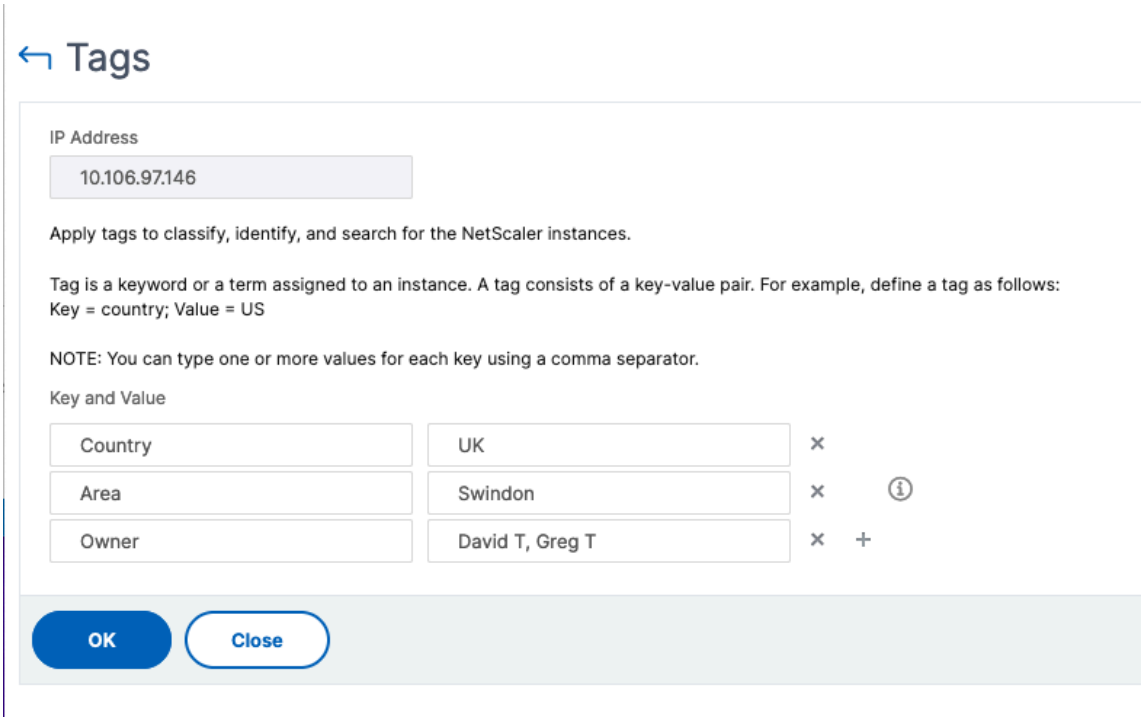


También puede agregar varias etiquetas haciendo clic en "+". La adición de etiquetas múltiples y significativas le permite buscar de manera eficiente las instancias.



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 Console 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.

5. Haga clic en **Aceptar**.

> **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 26, 2024

Puede darse una situación en la que NetScaler Console 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 Console 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 una 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 que se agrega a NetScaler Console 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.

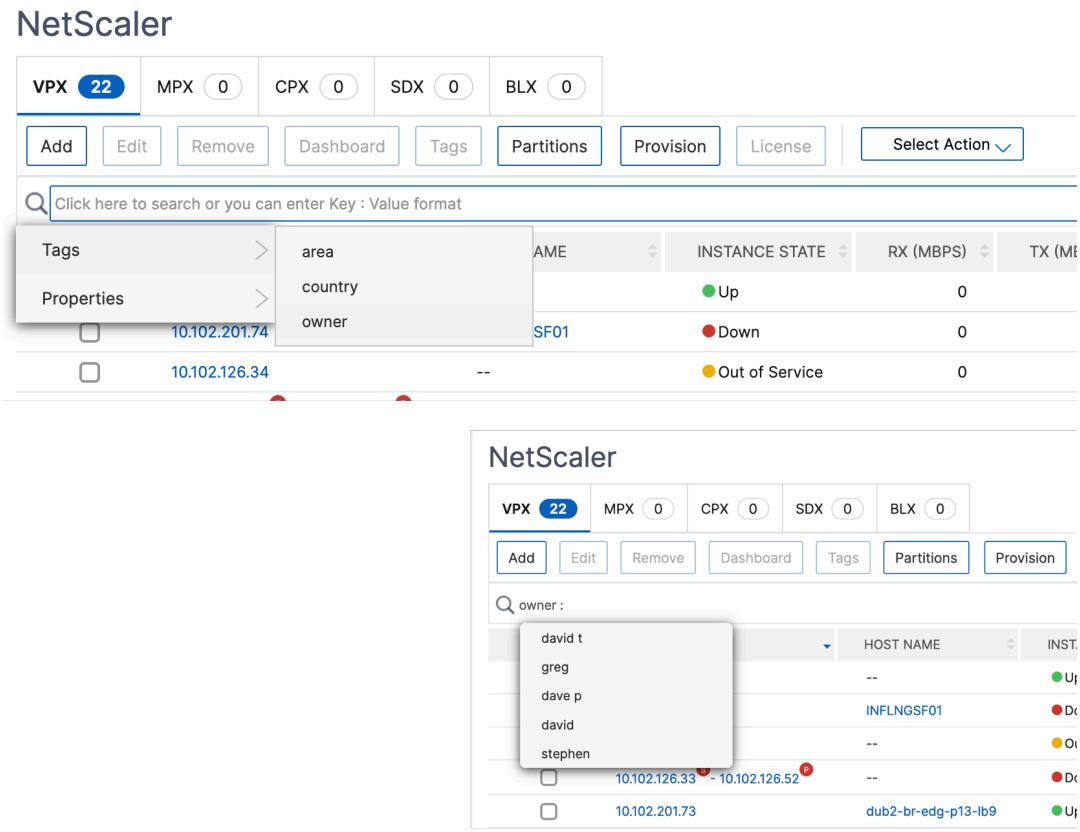
Puede utilizar una combinación de etiquetas y propiedades para crear sus propios criterios de búsqueda.

Para buscar instancias de NetScaler VPX

1. En NetScaler Console, vaya a **Infraestructura > Instancias > NetScaler**.
2. Selecciona la ficha **VPX**.
3. Haga clic en el campo de búsqueda. Puede crear una expresión de búsqueda mediante etiquetas o propiedades o combinando ambas.

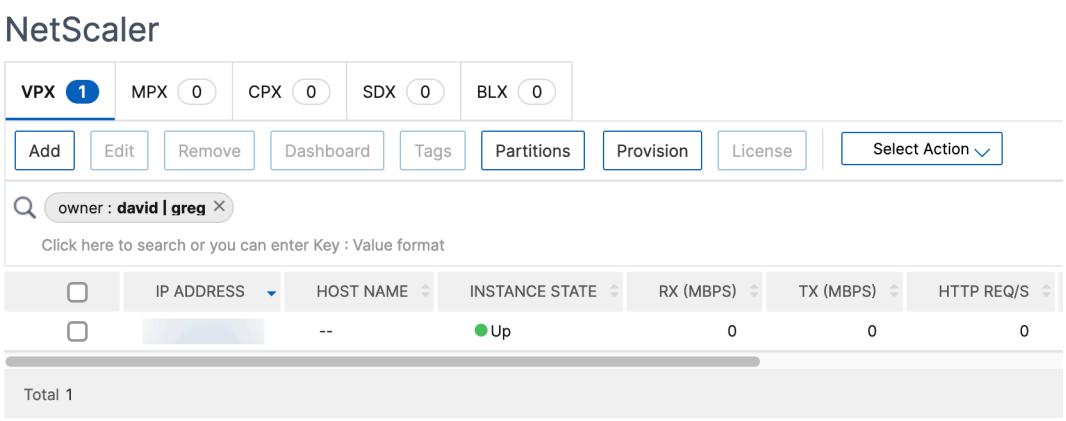
   Los siguientes ejemplos muestran cómo puede utilizar la expresión de búsqueda de manera eficiente para buscar la instancia.

   a) Seleccione la opción **Etiquetas** y seleccione **Propietario**. Seleccione "David T".

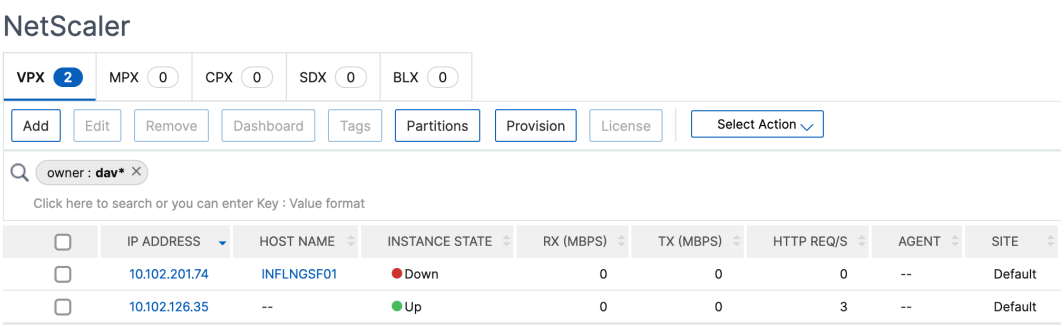


NetScaler Console admite expresiones regulares y caracteres comodín en las expresiones de búsqueda.

a) 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 "|".



b) 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» y «Dave P».



> **Nota:**
>
> Para obtener más información sobre las expresiones regulares y los caracteres comodín y sobre cómo usarlos, haga clic en el icono de «información» de la barra de búsqueda.

Administrar particiones de administración de instancias NetScaler

January 26, 2024

Puede configurar particiones de administración en sus instancias de Citrix Application Delivery Controller (NetScaler) para que a los diferentes grupos de su organización se les asignen diferentes particiones en la misma instancia de NetScaler. Puede asignar un administrador de red para administrar varias particiones en varias instancias de NetScaler.

NetScaler Console ofrece una forma perfecta de administrar todas las particiones que pertenecen a un administrador desde una única consola. Puede administrar estas particiones sin interrumpir otras configuraciones de particiones.

Para permitir que varios usuarios administren diferentes particiones de administración, debe crear grupos y, a continuación, asignar usuarios y particiones a esos grupos. Para obtener más información sobre la creación de un grupo o un usuario, consulte [Crear un usuario] (/en-us/netscaler-console-service/setting-up/configuring-role-based-access-control.html #configure -Users-on-NetScaler Console) y [Crear un grupo] (/en-us/netscaler-console-service/setting-up/configuring-role-based-access-control.html #configure -Groups-on-NetScaler Console).

Un usuario solo puede ver y administrar las particiones del grupo al que pertenece el usuario. Cuando detecta una instancia de NetScaler, las particiones de administración configuradas en esa instancia de NetScaler se agregan al sistema automáticamente. Cada partición de administración se considera una instancia en NetScaler Console.

Ver particiones de administración

Tenga en cuenta que tiene dos instancias de NetScaler VPX y que hay dos particiones de administración configuradas en cada instancia. Por ejemplo, la instancia 10.xx.xx.100 de NetScaler tiene la partición-1 y la partición-2, y la instancia 10.xx.xx.101 tiene la primera y la segunda partición.

Realice los siguientes pasos para ver las particiones de administración:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. En la ficha **VPX**, haga clic en **Particiones**.

Por ejemplo, si crea un grupo con las siguientes condiciones:

- En **Configuración > Usuarios y funciones > Crear grupo > Configuración de autorización > Seleccionar instancias**, selecciona las instancias «10.xx.xx.100-partition-1”y «10.xx.xx.101-first-partition».
- Tú asignas «Usuario1”al grupo.

El usuario 1 solo puede ver y administrar las particiones que se agregan al grupo. Sin embargo, las particiones que no se agregan al grupo están restringidas al usuario aunque pertenezcan a las mismas instancias.

En este ejemplo, 10.xx.xx.100-partition-2 y 10.xx.xx.101-second-partition están restringidas porque las instancias no se agregan al grupo al que está asignado el usuario.

Si desea que otro usuario administre las particiones de administración 10.xx.xx.100-partition-2 y 10.xx.xx.101-second-partition, cree un grupo con las siguientes condiciones:

- En la pestaña **Configuración de autorización** , seleccione las instancias de 10.xx.xx.100-partition-2 y 10.xx.xx.101 de segunda partición.
- Asigne el usuario requerido al grupo.

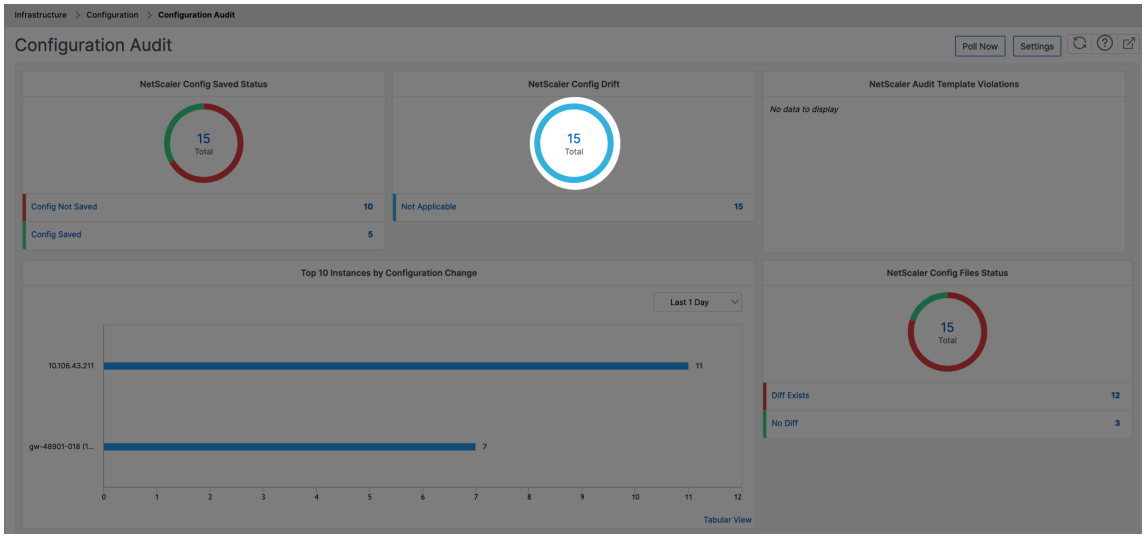
Este grupo permite al usuario asignado ver y administrar las particiones de administración seleccionadas.

Ver la diferencia en el historial de revisiones

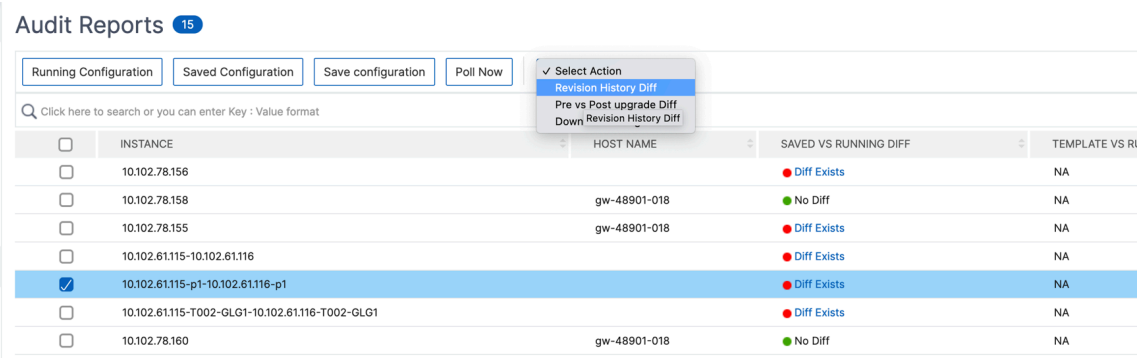
La diferencia del historial de revisiones para una partición de administrador le permite ver la diferencia entre los cinco archivos de configuración más recientes para una instancia de NetScaler particionada. Puede comparar los archivos de configuración entre sí (por ejemplo, Revisión de configuración: 1 con Revisión de configuración -2) o con la configuración actual en ejecución/guardada con 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**. El panel de auditoría de configuración muestra varios informes. Haga clic en el número que se muestra en el centro del gráfico de donut.

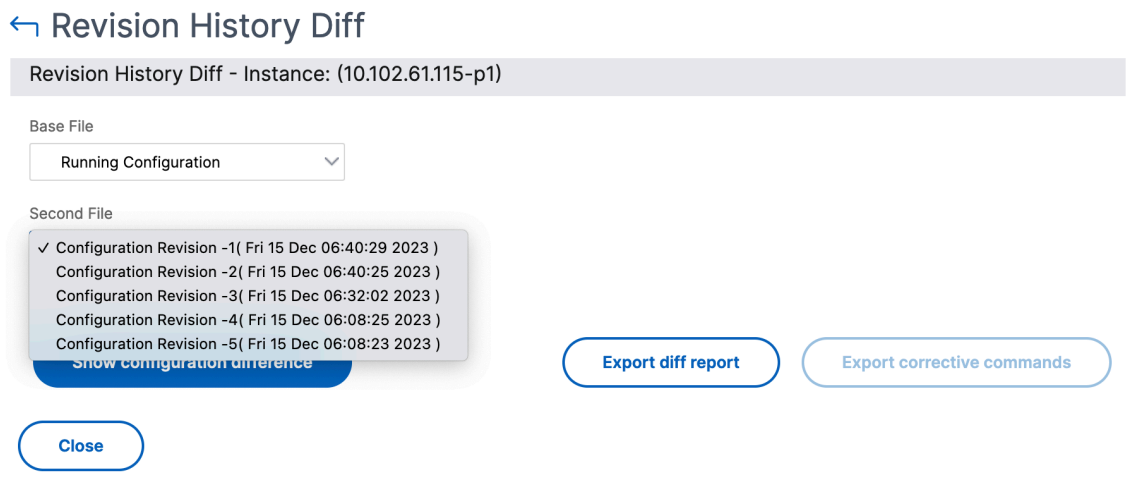


2. Seleccione la instancia de NetScaler particionada.
3. En el cuadro Acción, haga clic en **Diff del historial de revisiones**.

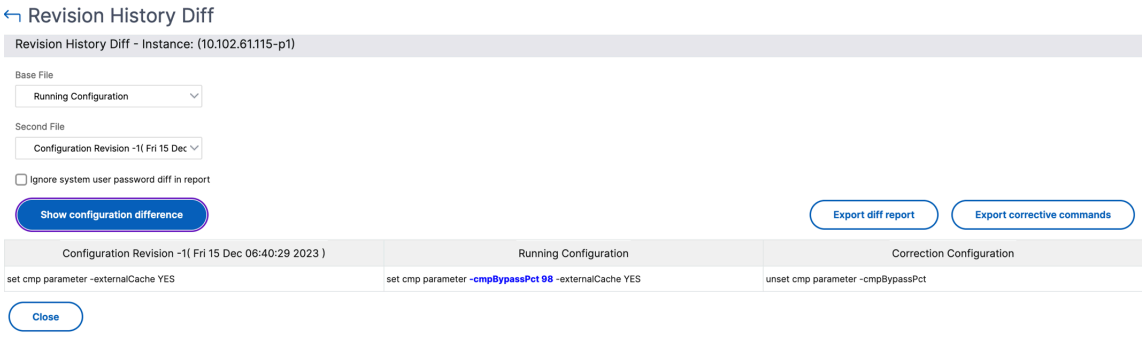


4. En la página **Diferencia del historial de revisiones**, seleccione los archivos que quiere comparar. Por ejemplo, compare la configuración guardada con la revisión de configuración 2 y, a continuación, haga clic en **Mostrar diferencia de configuración**.

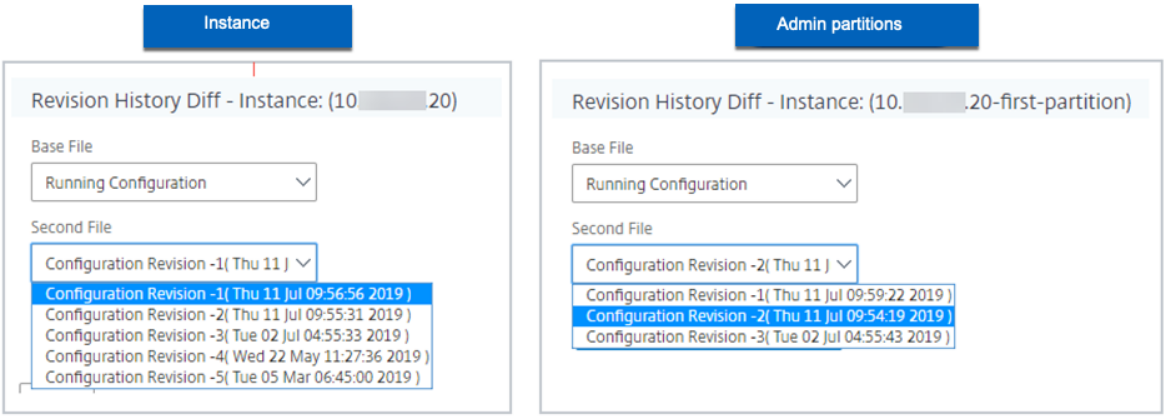
   A continuación, puede ver las diferencias entre los cinco archivos de configuración más recientes para la instancia de NetScaler particionada seleccionada. A continuación se muestra un ejemplo de partición de administración que tiene cinco configuraciones guardadas:



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).



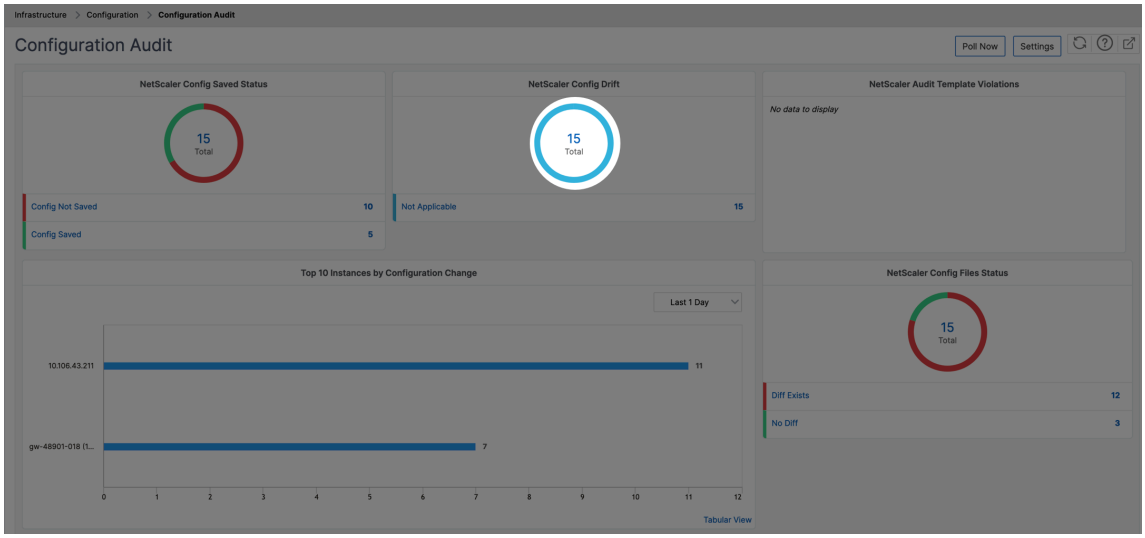
Las configuraciones guardadas en una partición de administración y la instancia son diferentes. En el ejemplo siguiente, la instancia 10.xx.xx.20 tiene cinco configuraciones guardadas en las que la partición admin de esta instancia tiene tres configuraciones guardadas diferentes:



Ver la plantilla frente a la diferencia de ejecución

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 "**Plantilla frente a Ejecutar diff**" 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.

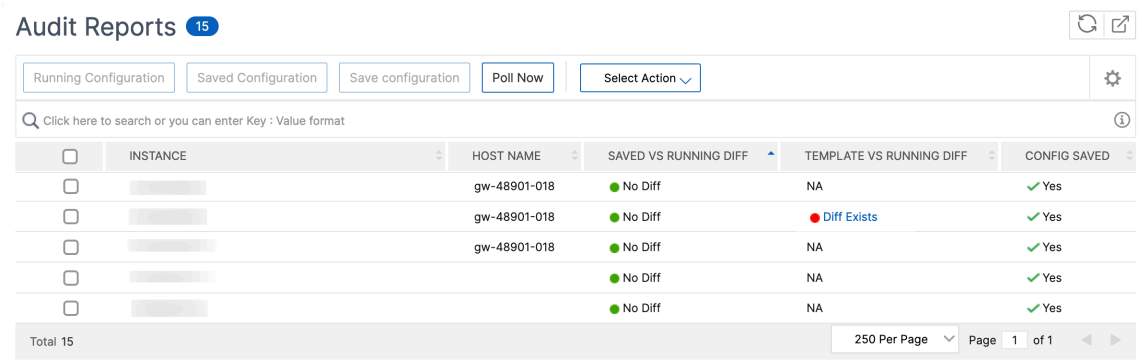
1. Vaya a **Infraestructura > Auditoría de configuración**. El panel de auditoría de configuración muestra varios informes. Haga clic en el número que se muestra en el centro del gráfico de donut.



2. En la página **Informes de auditoría**, haga clic en el hipervínculo **Diff existe** en la columna Plantilla frente a Diff en ejecución.

   Si hay alguna diferencia entre la plantilla de auditoría y la configuración en ejecución, la difer-

encia 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 exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

> **Nota:**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

Realizar copias de seguridad y restaurar instancias de NetScaler

January 26, 2024

Puede realizar una copia de seguridad del estado actual de una instancia de Citrix Application Delivery Controller (NetScaler) y posteriormente utilizar los archivos de copia de seguridad para restaurar la instancia de NetScaler al mismo estado. Siempre debe realizar una copia de seguridad de una instancia antes de actualizarla o por motivos de precaución. Una copia de seguridad de un sistema

estable le permite restaurarlo a un punto estable si se vuelve inestable. Existen varias formas de realizar copias de seguridad y restauraciones en una instancia de NetScaler. Puede realizar copias de seguridad y restaurar manualmente las configuraciones de NetScaler mediante la GUI o la CLI, o puede usar NetScaler Console para realizar copias de seguridad automáticas y restauraciones manuales. NetScaler Console realiza copias 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 Console crea una copia de seguridad completa y restaura los siguientes tipos de instancias de NetScaler:

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

Para obtener más información, consulte Realizar copias de seguridad y restaurar una instancia de NetScaler .

> **Nota:**
>
> - Desde NetScaler Console, no puede realizar la operación de respaldo 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/tenants/<specify-the-tenant-name>/device_backup/
```

Para evitar problemas debido a la falta de disponibilidad de espacio en disco, puede guardar un máximo de tres archivos de respaldo en este directorio.

Para realizar copias de seguridad y restaurar instancias de NetScaler, primero debe configurar los ajustes de respaldo en NetScaler Console. 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 utilizando estos archivos de copia de seguridad.

Crear una copia de seguridad para una instancia de NetScaler seleccionada mediante NetScaler Console

Realice esta tarea si quiere realizar una copia de seguridad de una instancia de NetScaler seleccionada o de varias instancias:

1. En NetScaler Console, vaya a **Infraestructura > Instancias**. En **Instancias**, seleccione el tipo de instancias (por ejemplo, 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 **Hacer copia de seguridad**.
4. Especifique si quiere cifrar el archivo de copia de seguridad para mayor seguridad. Puede introducir su contraseña o utilizar la contraseña global especificada anteriormente en la página Configuración de Copia de Seguridad de Instancia.
5. Haga clic en **Continuar**.

Transferir un archivo de reserva a un sistema externo

Puede transferir una copia del archivo de reserva a otro sistema como medida de precaución. Si desea restaurar la configuración, primero tiene que cargar el archivo de respaldo en el servidor de NetScaler Console y, a continuación, realizar la operación de restauración.

Para transferir un archivode respaldo de NetScaler Console :

1. Vaya a **Infraestructura > Instances > NetScaler** y, a continuación, seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Respaldar/Restaurar**.
3. Seleccione el archivo de copia de seguridad y haga clic en **Transferir**.

   Aparecerá la página **Transferir Archivo de Copia** de Seguridad. Especifique los siguientes parámetros:

   a) **Servidor**: dirección IP del sistema al que quiere transferir el archivo de reserva.

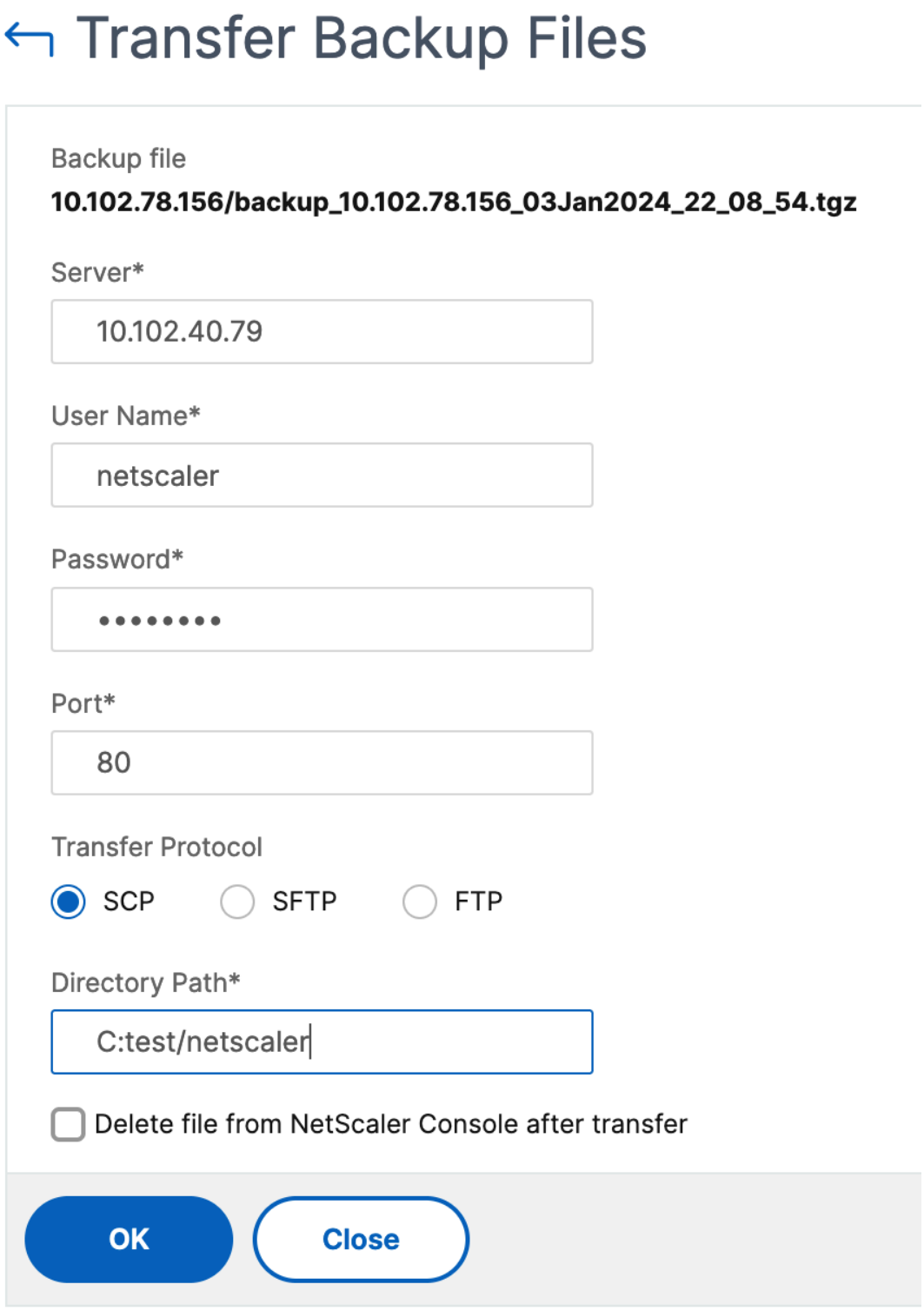
   b) **Nombre de usuario** y **contraseña**: credenciales de usuario del nuevo sistema, en el que se copian los archivos de la copia de seguridad.

   c) **Puerto**: número de puerto del sistema al que se transfieren los archivos.

d) **Protocolo de transferencia**: protocolo que se utiliza para realizar la transferencia del archivo de reserva. Puede seleccionar los protocolos SCP, SFTP o FTP para transferir el archivo de reserva.

e) **Ruta del directorio**: la ubicación a la que se transfiere el archivo de la copia de seguridad en el nuevo sistema.

f) Haga clic en **Aceptar**.



Nota:

Los archivos de respaldo del servicio NetScaler Console se envían al servidor externo a través

de un agente. Si hay muchos agentes, se envía un archivo de respaldo de NetScaler a través del mismo agente que se usó para agregar esa instancia de NetScaler. Para obtener más información sobre las instancias asociadas a un agente, vaya a **Infraestructura > NetScaler > Agentes**.

Restaure una instancia de NetScaler mediante NetScaler Console

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 principal de NetScaler, no puede acceder a la instancia principal y la instancia secundaria se cambia a **STAYSECONDARY**. Una vez completado el proceso de restauración en la instancia principal, la instancia secundaria de NetScaler cambia del modo **STAYSECONDARY** al 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 **Ver copia de seguridad**.
2. En la página **Archivos de copia** de seguridad, seleccione el archivo de copia de seguridad que contiene la configuración que desea restaurar y, a continuación, haga clic en **Restaurar**.

Restaure un dispositivo NetScaler SDX mediante NetScaler Console

En NetScaler Console, la copia de seguridad de un 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)

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

Si está restaurando el dispositivo NetScaler 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 dispositivo para que coincida con la del archivo de copia de seguridad antes de iniciar el proceso de restauración.

Asegúrese de que se tomó la variante de la plataforma NetScaler SDX de la que se realizó una copia de seguridad es la misma en la que intenta restaurar. No se puede restaurar desde una variante de plataforma diferente.

> **Nota:**
>
> Antes de restaurar el 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 Console, vaya a **Infraestructura > Instancias > NetScaler**.
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**.

Exportar el informe de este panel

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

Forzar una conmutación por error a la instancia secundaria de NetScaler

January 26, 2024

Es posible que quiera forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar la instancia principal de Citrix Application Delivery Controller (NetScaler). 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 Console:

1. En NetScaler Console, vaya a **Infraestructura > Instancias**. Vaya a la ficha **VPX** y selecciona una instancia.
2. Seleccione instancias en una configuración de alta disponibilidad de las instancias enumeradas en el tipo de instancia seleccionado.
3. En el cuadro **Acción**, seleccione **Forzar 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 26, 2024

En una configuración de alta disponibilidad (HA), el nodo secundario puede ser forzado 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 tome el control y quiere 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 en segundo plano mediante NetScaler Console:

1. En NetScaler Console, vaya a **Infraestructura > Instancias** y, a continuación, seleccione una instancia en un tipo de instancia (VPX).
2. Seleccione instancias en una configuración de alta disponibilidad de las instancias enumeradas en el tipo de instancia seleccionado.
3. En el cuadro **Acción**, selecciona **Permanecer en segundo plano**.
4. Haga clic en **Sí** para confirmar la ejecución de la acción "Permanecer secundario".

Crear grupos de instancias

January 26, 2024

Para crear un grupo de instancias, primero debe agregar todas las instancias de NetScaler a NetScaler Console. 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 Console

1. En NetScaler Console, vaya a **Infraestructura > Instancias > 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. En **Categoría**, seleccione la opción **Predeterminada**.
4. 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** .
5. Haga clic en **Crear**.

Grupos de sitios de equilibrio de carga de servidores

January 26, 2024

Si quiere garantizar la disponibilidad continua y la recuperación ante desastres de sus instancias de ADC, puede configurar un grupo de sitios GSLB. Equilibra la carga entre los sitios al dirigir las solicitudes de los clientes al sitio más cercano o con mejor rendimiento, o a los sitios supervivientes si se produce una interrupción.

A veces, en un grupo de sitios GSLB, los objetos de configuración de las instancias de ADC intentan sobrescribirse entre sí. Conduce a una condición de raza. Para solucionar estos problemas, debe controlar la selección del nodo principal en el grupo de sitios GSLB. La configuración del nodo principal se aplicará a las instancias de ADC restantes. En NetScaler Console, puede crear un grupo de sitios GSLB y hacer lo siguiente:

- Elija un nodo principal entre las instancias de ADC seleccionadas.
- Establezca el orden de prioridad para la selección del nodo principal si el nodo principal seleccionado deja de funcionar.

Puede ver sus grupos de sitios GSLB en **Infraestructura > Instancias > Grupo de sitios GSLB**.

Crear un grupo de sitios GSLB

Realice los siguientes pasos para crear un grupo de sitios GSLB con instancias de ADC:

1. Vaya a **Infraestructura > Instancias > Grupo de sitios GSLB**.
2. Haga clic en **Agregar**.
3. Especifique un nombre para el grupo de sitios GSLB.
4. Seleccione las instancias que quiera agregar al grupo de sitios GSLB. Estas instancias actúan como sitios del grupo.
5. Seleccione al menos un sitio y **haga clic en Crear sitio activo**.

   La instancia que tiene prioridad 1 se convierte en el nodo principal. Puede cambiar el orden de prioridad de los sitios activos. Seleccione la instancia de menor prioridad y haga clic en **Subir prioridad**.
6. Haga clic en **Crear**.

En **Infraestructura > Funciones de red > GSLB**, la GUI muestra las entidades solo del nodo ADC principal del grupo de sitios GSLB.

Cree administradores y usuarios de SNMP para el agente NetScaler

January 26, 2024

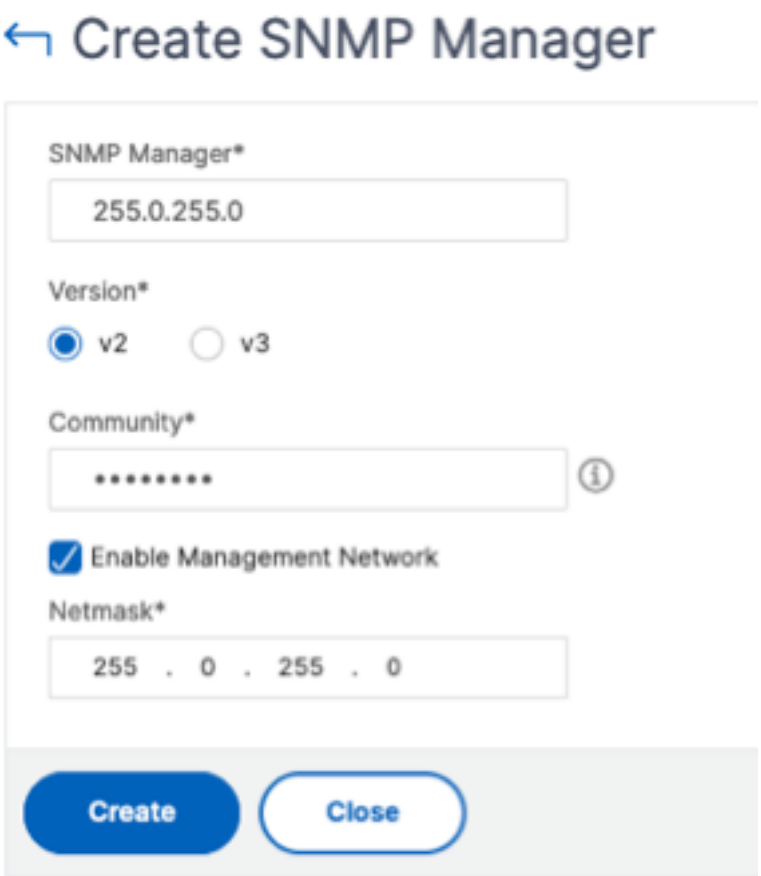
Puede consultar al agente SNMP para obtener información específica del sistema desde un dispositivo remoto denominado administrador SNMP. A continuación, el agente busca en la base de información de administración (MIB) los datos solicitados y los envía al administrador SNMP.

Puede agregar un administrador de SNMP para consultar un agente de NetScaler. El administrador cumple con SNMP V2 y V3. Si especifica uno o más administradores de SNMP, el agente de NetScaler no acepta consultas de SNMP de ningún host, excepto de los administradores de SNMP especificados.

Agregar un administrador SNMP v2

Para agregar un administrador de SNMP v2 para el agente de NetScaler:

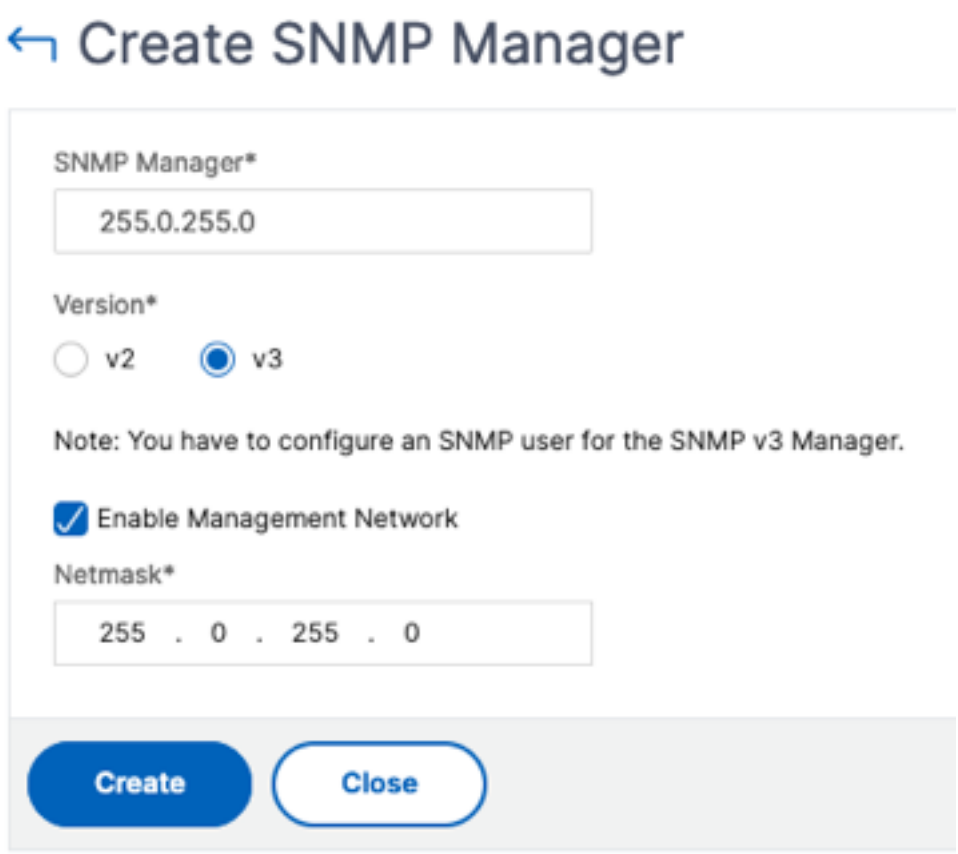
1. Vaya a **Infraestructura > Instancias > Agentes** , seleccione un agente de NetScaler y haga clic en **Seleccionar acción > Administrar SNMP**.
2. En la ficha **SNMP > Administrador de SNMP**, haga clic en **Agregar**.
3. En la página **Crear un administrador de SNMP**, especifique los siguientes 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**: Marque esta casilla 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**.



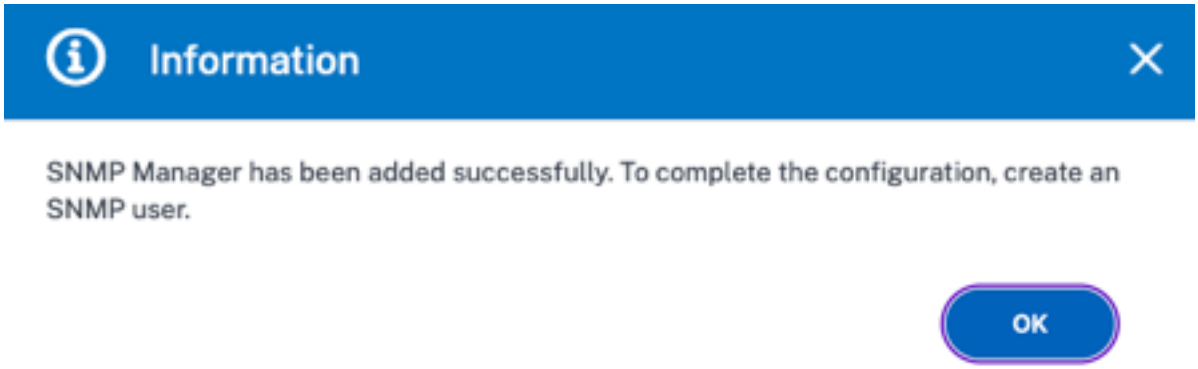
Agregar un administrador SNMP v3

Para agregar un administrador SNMP v3 para el agente de NetScaler:

1. Vaya a **Infraestructura > Instancias > Agentes** , seleccione un agente de NetScaler y haga clic en **Seleccionar acción> Administrar SNMP**.
2. En la ficha **SNMP > Administrador de SNMP**, 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**: Marque esta casilla 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**.

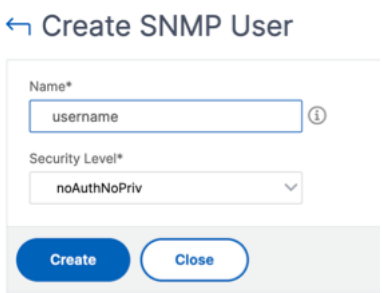
Agregar un usuario SNMP

Agregue un usuario SNMP para responder a las consultas SNMP v3 de un administrador de SNMP.

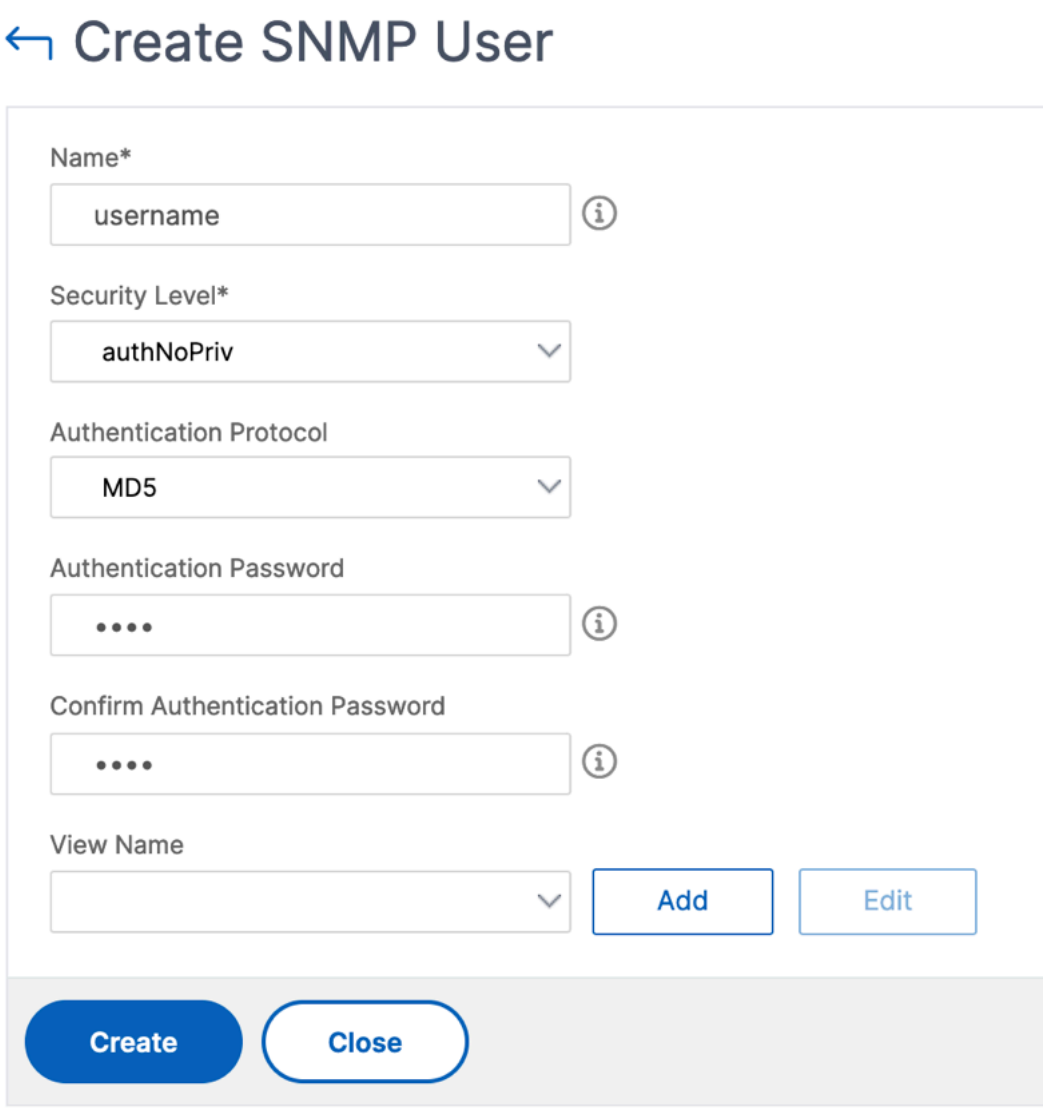
Para agregar un usuario de SNMP para el agente de NetScaler:

1. Vaya a **Infraestructura > Instancias > Agentes** , seleccione un agente 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 de NetScaler y el administrador de SNMP.

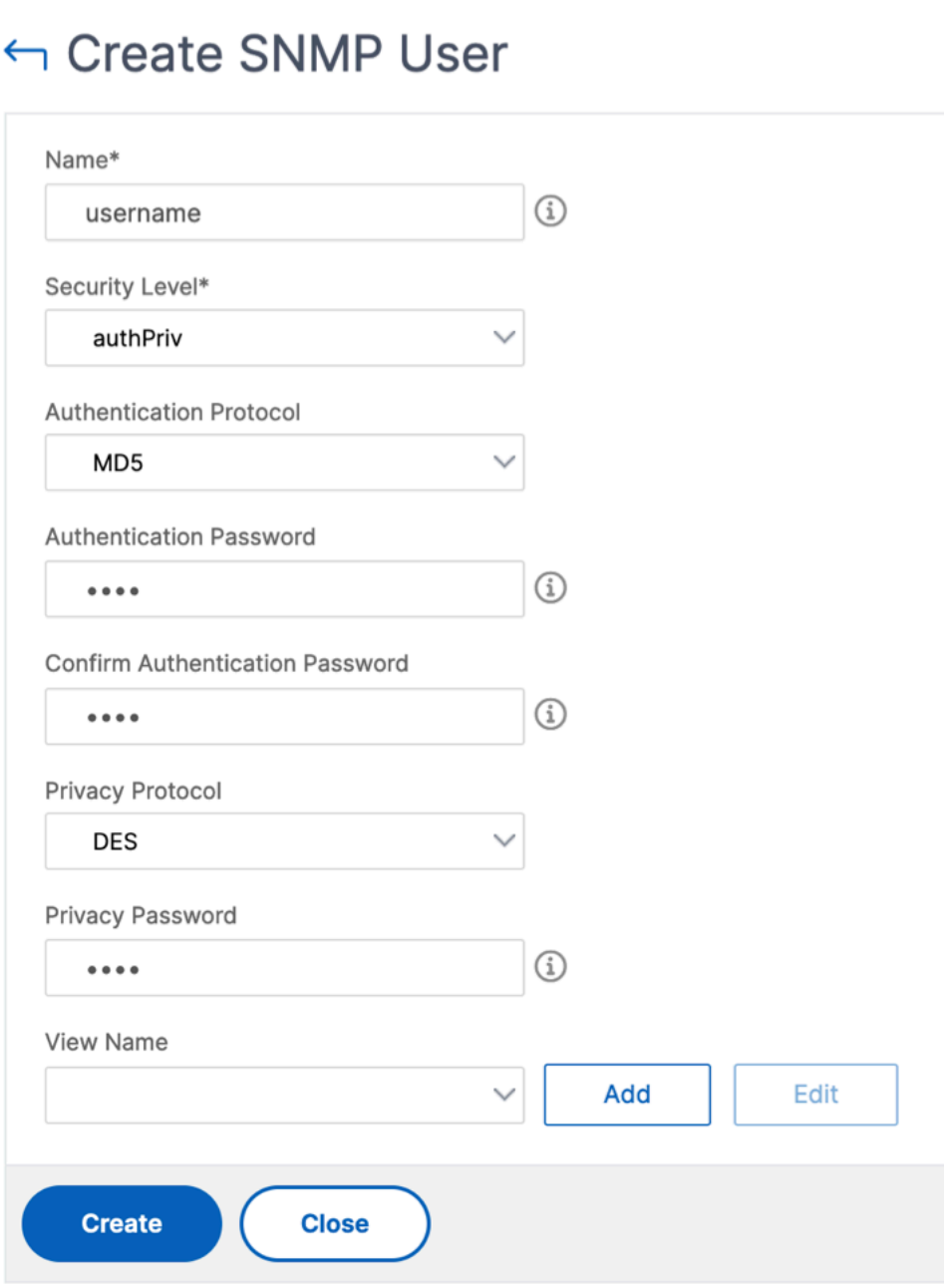
     Seleccione uno de los siguientes niveles de seguridad:
   - **NoAuthNoPriv**. No requieren autenticación ni cifrado.



   - **AuthNoPriv**. Requiere autenticación pero no cifrado.



- **AuthPriv**. Exigen autenticación y cifrado.



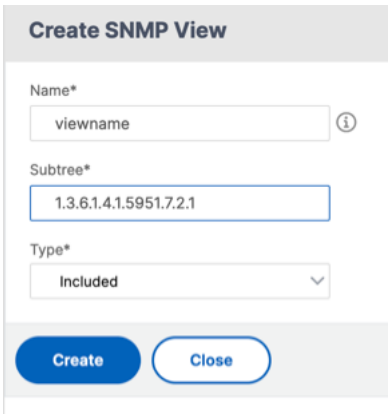
En función del nivel de seguridad asignado al usuario, proporcione protocolos de autenticación adicionales, como protocolos de autenticación, contraseñas de privacidad y asigne vistas SNMP.

Administración de vistas SNMP

Las vistas SNMP se utilizan para implementar el control de acceso para un usuario de SNMP. Las vistas de SNMP restringen el acceso del usuario a partes específicas de la MIB.

Para permitir o restringir un OID de SNMP para el agente de NetScaler:

1. Vaya a **Infraestructura > Instancias > Agentes** , seleccione un agente de NetScaler y haga clic en **Seleccionar acción> Administrar SNMP**.
2. En la ficha **SNMP > Usuario SNMP**, haga clic en **Agregar**.
3. 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 subárbol.
   - **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.
4. Haga clic en **Crear**.



Aprovisione instancias de NetScaler VPX en SDX

January 26, 2024

Puede aprovisionar una o más instancias de NetScaler VPX en el dispositivo SDX mediante NetScaler Console. El número de instancias que puede implementar depende de la licencia que haya adquirido. Si la cantidad de instancias agregadas es igual a la cantidad especificada en la licencia, la consola de NetScaler no le permite aprovisionar más instancias de NetScaler.

Antes de empezar, asegúrese de añadir una instancia SDX en NetScaler Console donde desee aprovisionar instancias VPX.

Para aprovisionar una instancia VPX, haga lo siguiente:

1. Vaya a **Infraestructura > Instancias > NetScaler**.

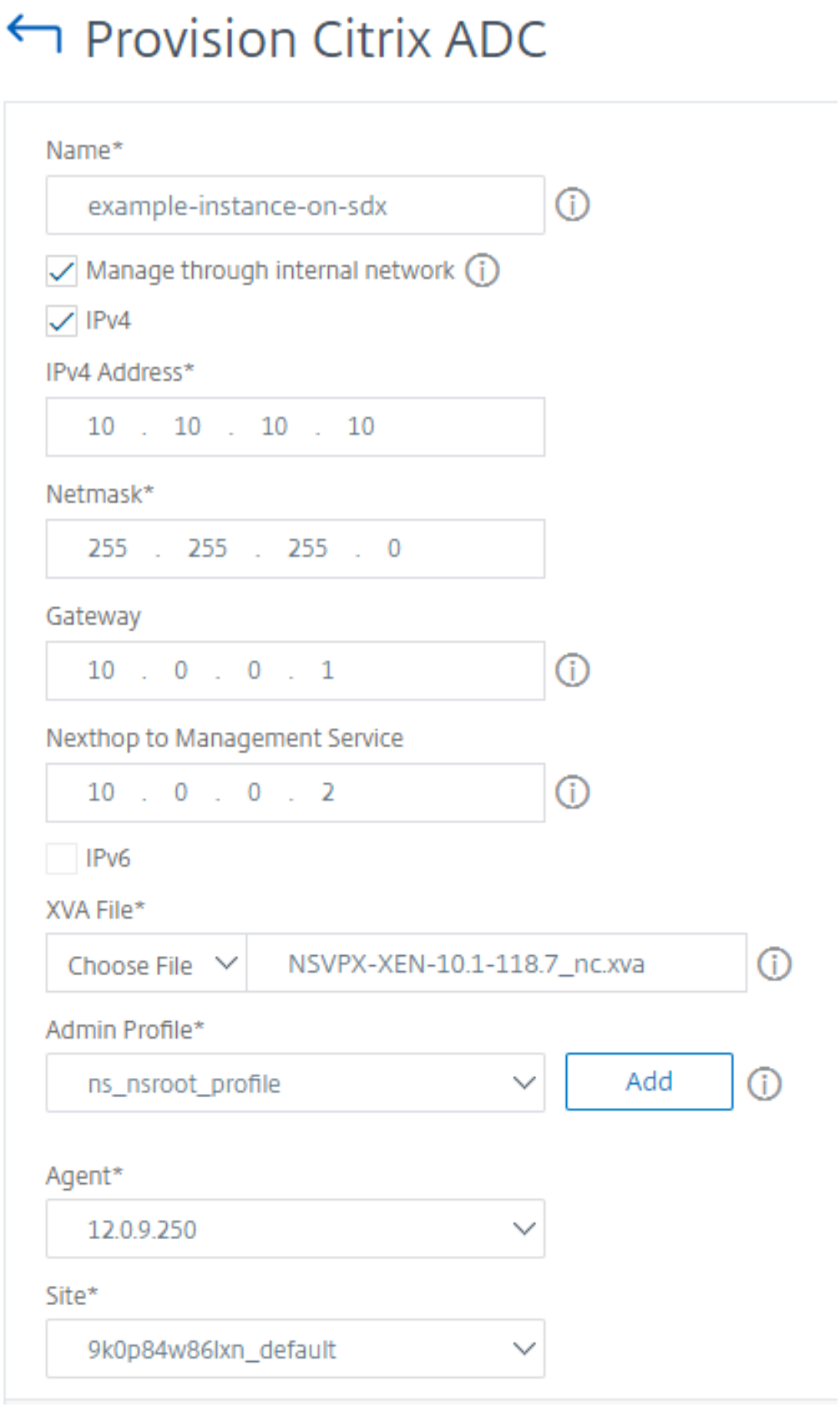
2. En la ficha **SDX**, seleccione una instancia SDX en la que quiera aprovisionar una instancia VPX.
3. En **Seleccionar acción**, seleccione **Aprovisionar VPX**.

Paso 1: Agregar una instancia VPX

La consola de NetScaler utiliza la siguiente información para configurar las instancias VPX en un dispositivo SDX:

- **Nombre**: especifique un nombre para una instancia de NetScaler.
- 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 la consola de NetScaler 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, a continuación, vaya a la consola de NetScaler para obtener 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 de NetScaler Console.
- **Perfil de administrador**: este perfil proporciona acceso para aprovisionar instancias VPX. Con este perfil, NetScaler Console 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

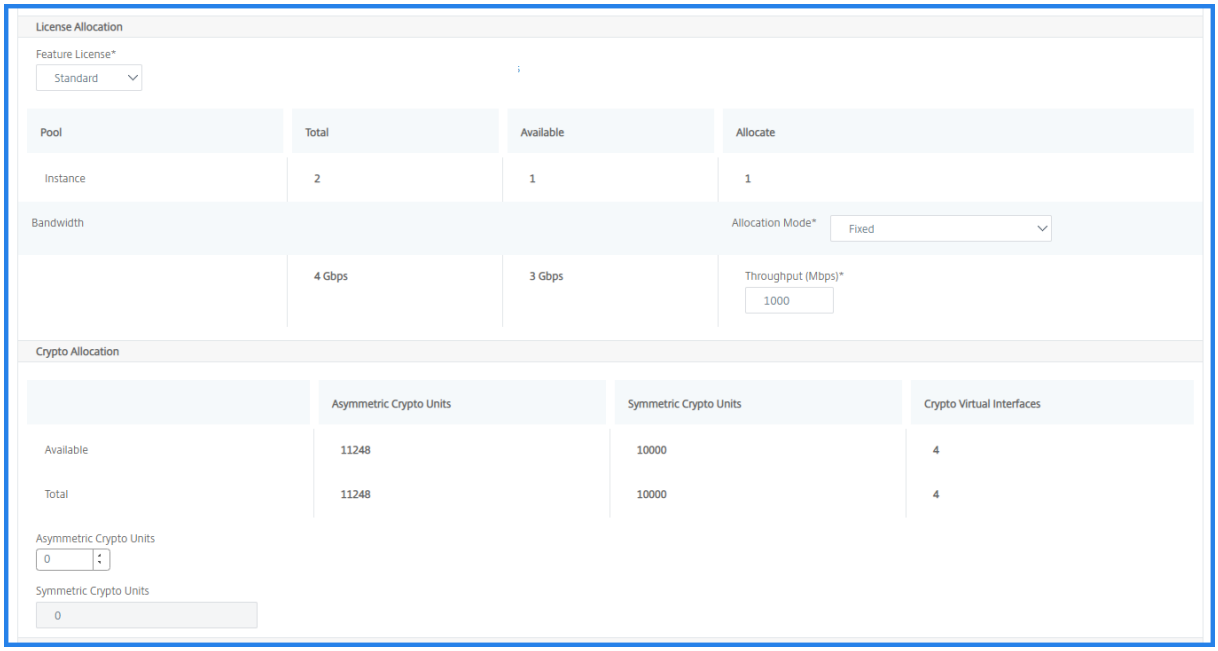
En la sección **Asignación de licencias**, especifique la licencia VPX. Puede utilizar las licencias Standard, Advanced y Premium.

- **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.

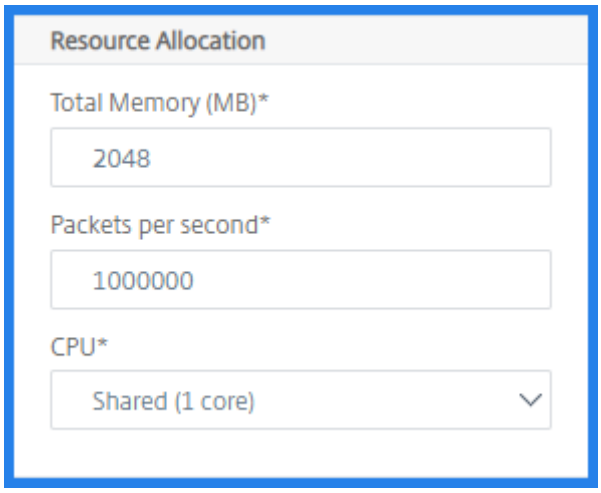
- **Memoria total (MB)**: asigna la memoria total a una instancia. El valor mínimo es 2048 MB.
- **Paquetes por segundo**: especifique la cantidad de paquetes que se van a transmitir por segundo.
- **CPU**: especifique el número de núcleos de CPU de una instancia. Puede utilizar núcleos de CPU compartidos 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.



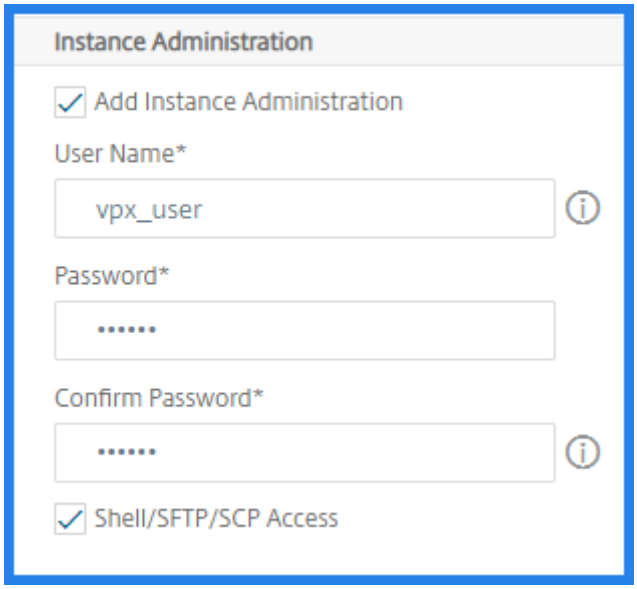
Consulte la tabla de Aprovisionar instancias de NetScaler que muestra el VPX compatible, la versión de imagen de un solo paquete y la cantidad de núcleos que puede asignar a una instancia.

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

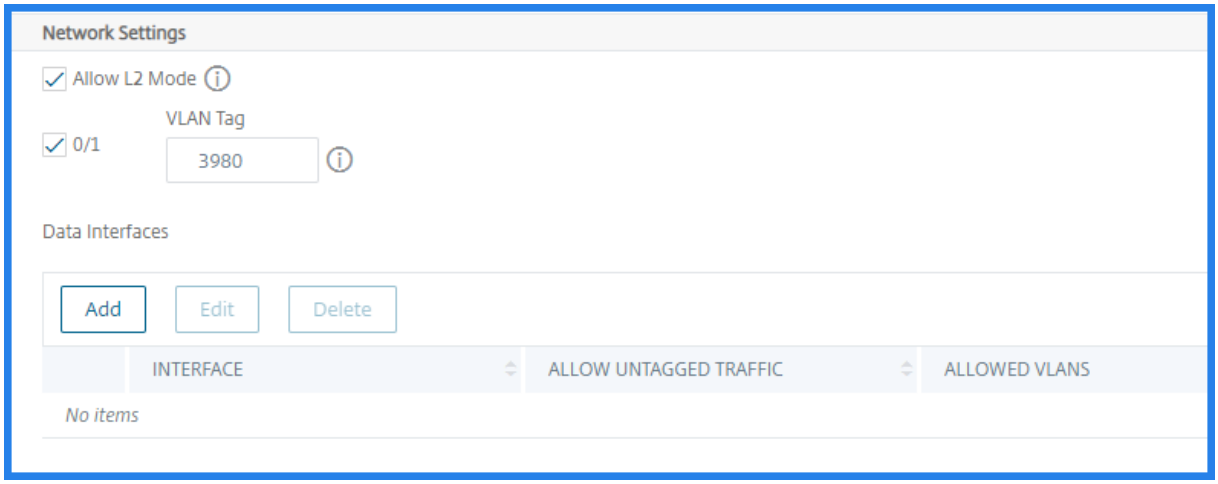
Seleccione la configuración de red requerida para una instancia:

- **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**.



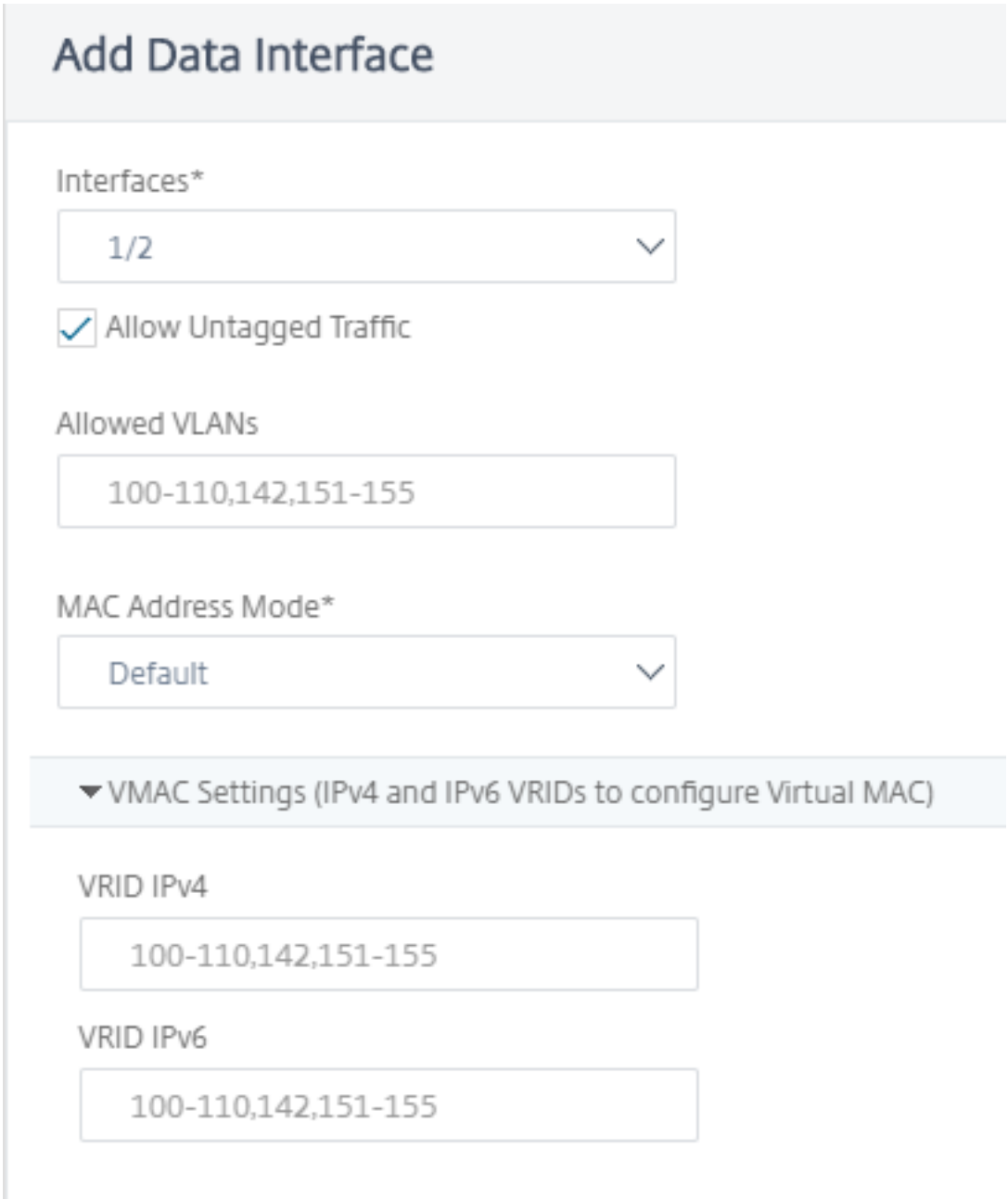
En **Interfaces de datos**, haga clic en **Agregar** para agregar interfaces de datos y especifique lo siguiente:

- **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

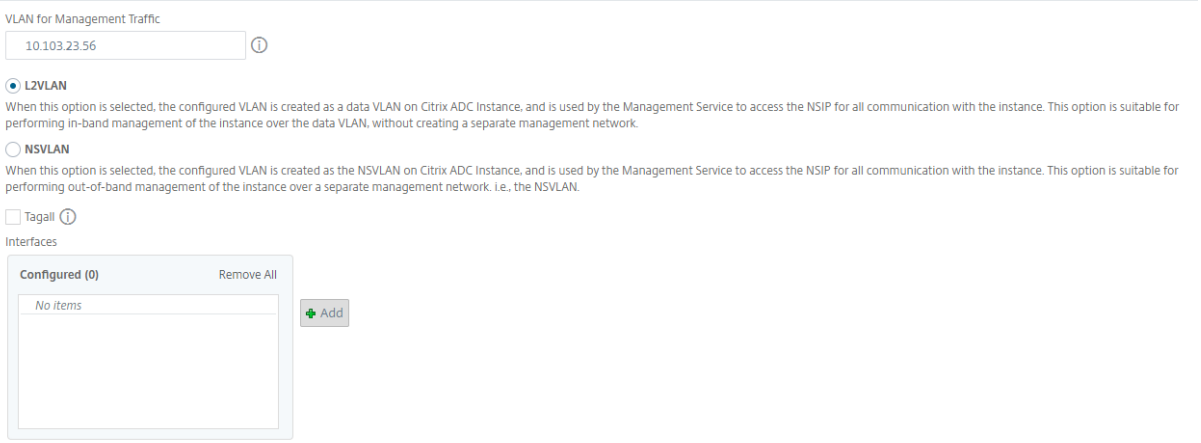
El Servicio de administración y la dirección de administración (NSIP) de la instancia VPX se encuentran en la misma subred y la comunicación se realiza a través de una interfaz de administración.

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**.

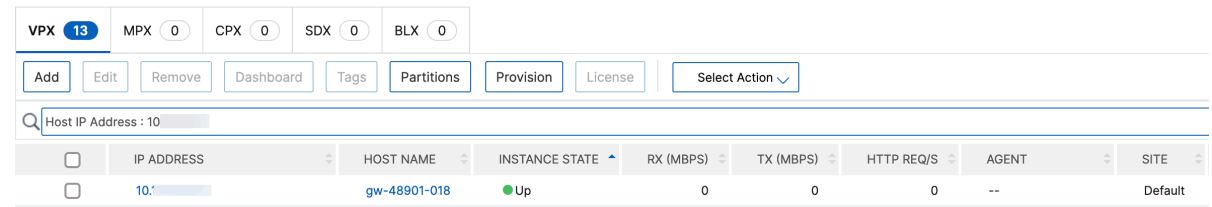


Haga clic en **Listo** para aprovisionar una instancia VPX.

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.



Redescubra varias instancias de NetScaler

January 26, 2024

Puede volver a descubrir varias instancias de Citrix Application Delivery Controller (NetScaler) (VPX, MPX, SDX, BLX y CPX) en la configuración de NetScaler Console. Tras volver a descubrir las instancias, podrá ver los estados y configuraciones más recientes de esas instancias. El servidor de NetScaler Console redescubre todas las instancias de ADC y comprueba si se puede acceder a ellas.

Para volver a descubrir varias instancias de NetScaler VPX:

1. Vaya a **Infraestructura > Instancias > NetScaler**. Selecciona la ficha de instancias (VPX, MPX, SDX, BLX y CPX) y selecciona las instancias que deseas redescubrir.
2. En el cuadro **Acción**, haga clic en **Redescubrir**. También puedes redescubrir varias instancias VPX.
3. 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.

Visión general de sondeo

January 26, 2024

El sondeo es un proceso en el que NetScaler Console 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 monitorear sus instancias a través de NetScaler Console, NetScaler Console debe recopilar cierta información, como el uso de la CPU, el uso de la memoria, los certificados SSL, las funciones con licencia y los tipos de licencia de todas las instancias de NetScaler administradas. Los siguientes son los diferentes tipos de sondeos que se producen entre NetScaler Console 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 Console utiliza protocolos como NITRO call, Secure Shell (SSH) y Secure Copy (SCP) para sondear la información de las instancias de NetScaler.

Cómo sondea NetScaler Console las instancias y entidades administradas

De forma predeterminada, NetScaler Console sondea automáticamente a intervalos regulares. NetScaler Console también le permite configurar los intervalos de sondeo para algunos tipos de sondeo y permite sondear manualmente cuando sea necesario.

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

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

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Encuesta de inventario	Cada 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)	El archivo de respaldo del estado actual de las instancias de NetScaler 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 NetScaler (por ejemplo, configuración en ejecución frente a configuración guardada)	Llamada SSH, SCP y NITRO	Sí. Vaya a **Infraestructura > Configuración > 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 añadir todas las auditorías de configuración de las instancias inmediatamente a NetScaler Console. Para hacerlo, vaya a **Infraestructura > Configuración > Auditoría de configuración** y haga clic en **Sondear ahora**. La página **Sondear 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 añadir todos los certificados de las instancias inmediatamente a NetScaler Console. Para hacerlo, vaya a **Infraestructura > Panel de control SSL** y haga clic en **Sondear ahora**. La página **Sondear ahora** le permite sondear todas las instancias o seleccionadas de la red.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Sondeo de entidades	Cada 60 minutos (de forma predeterminada)	Todas las entidades configuradas en las instancias. Una entidad es una política, un servidor virtual, un servicio o una acción adjunta a una instancia de NetScaler. Para habilitar el sondeo de entidades, consulte Habilitar o deshabilitar las funciones de la consola NetScaler .	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 las entidades manualmente y añadir todas las entidades de las instancias inmediatamente a NetScaler Console. Para hacerlo, vaya a **Infraestructura > Funciones de red** y haga clic en **Sondear ahora**. La página **Sondear ahora** le permite sondear todas las instancias o seleccionadas de la red

> **Nota** Además del sondeo, NetScaler Console recibe los eventos generados por las instancias de NetScaler administradas a través de trampas de SNMP que se envían 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, los archivos SSL, los archivos de certificados de CA, las plantillas de NetScaler, la información de la base de datos, etc., se descargan a NetScaler Console. 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

Las siguientes son las diferentes formas de sondeo que NetScaler Console realiza en las instancias administradas:

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

Sondeo global de instancias

NetScaler Console sondea automáticamente todas las instancias administradas de la red en función del intervalo que haya configurado. Aunque el intervalo de sondeo predeterminado es de 60 minutos, puede configurar el intervalo en función de sus requisitos yendo a **Infraestructura > Funciones de red > Configuración**.

Sondeo manual de instancias

Cuando NetScaler Console administra muchas entidades, el ciclo de sondeo tarda más en generar el informe, lo que puede provocar que la pantalla quede en blanco o que el sistema siga mostrando datos anteriores.

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

NetScaler Console sondea automáticamente las instancias administradas para recopilar información en momentos determinados del día. El sondeo seleccionado reduce el tiempo de actualización que necesita NetScaler Console para mostrar el estado más reciente de las entidades enlazadas a estas instancias seleccionadas.

Para sondear instancias específicas en NetScaler Console:

1. En NetScaler Console, 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 Console inicia el sondeo manual y agrega todas las entidades.

Encuesta manual de entidades

NetScaler Console también le permite sondear solo algunas entidades seleccionadas que están enlazadas a una instancia. Por ejemplo, puede utilizar esta opción para conocer el estado más reciente de una entidad concreta en una instancia. En este caso, no es necesario sondear la instancia en su conjunto para conocer el estado de una entidad actualizada. Al seleccionar y sondear una entidad, NetScaler Console sondea solo esa entidad y actualiza el estado en la GUI de NetScaler Console.

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**produzca el siguiente sondeo automático. Para ver el estado modificado del servidor virtual, es posible que quiera sondear solo ese servidor virtual, de modo que el estado correcto se muestre inmediatamente en la GUI.

Ahora puede sondear las siguientes entidades para obtener 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 Console:

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 Console, vaya a **Infraestructura > Funciones de red > Equilibrio de carga > Servidores virtuales** .
2. Seleccione el servidor virtual que muestre el estado como INACTIVO y, **a**continuación, haga clic en **Sondear ahora**. El estado del servidor virtual ahora cambia a **ACTIVO**.

Desadministrar una instancia

January 26, 2024

Si desea detener el intercambio de información entre NetScaler Console y las instancias de su red, puede desadministrar las instancias.

Para anular la gestión de una instancia:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione la pestaña Instancia de NetScaler (por ejemplo, VPX).
3. En la lista de instancias, haga clic con el botón derecho en una instancia y, a continuación, seleccione **Desadministrar**, o seleccione instancia y, en la lista **Acción**, seleccione **Desadministrar**.

   El estado de la instancia seleccionada cambia a **Fuera de servicio**.

   NetScaler Console ya no administra la instancia y ya no intercambia datos con NetScaler Console.

Rastrear la ruta a una instancia

January 26, 2024

Al rastrear la ruta de un paquete desde la consola de NetScaler hasta una instancia, puede encontrar información como la cantidad de saltos necesarios para llegar a la instancia. El traceroute rastrea 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, el traceroute muestra dónde existe el problema.

Para rastrear la ruta de una instancia:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione la pestaña Instancia de NetScaler (por ejemplo, VPX).
3. 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 la lista **Acción**, haga clic en **TraceRoute**.

   El cuadro de mensaje TraceRoute muestra la ruta a la instancia y la cantidad de tiempo, en milisegundos, consumida por cada salto.

Ver las direcciones IP propiedad de NetScaler

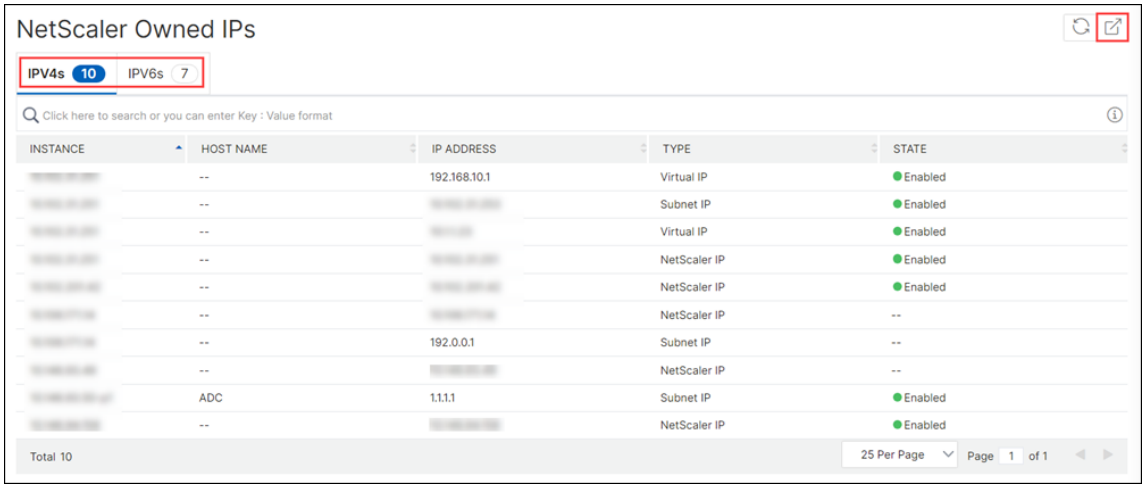
July 17, 2024

Puede ver las direcciones IP configuradas en las instancias de NetScaler directamente desde la GUI de NetScaler Console. Tenga en cuenta que los cambios de configuración y otras operaciones solo se pueden realizar en instancias de NetScaler.

Para ver las direcciones IP propiedad de NetScaler, vaya a **Infraestructura > Instancias > IP propiedad de NetScaler**.

Esta función muestra las direcciones IPv4 e IPv6 configuradas en las instancias de NetScaler. Los tipos de direcciones IP incluyen:

- Dirección IP de NetScaler
- Dirección IP de subred
- Dirección IP virtual
- Dirección IP del servicio ADNS
- Dirección IP GSLB
- Dirección IP del clúster
- Dirección IP asignada



Exportar direcciones IP propiedad de NetScaler

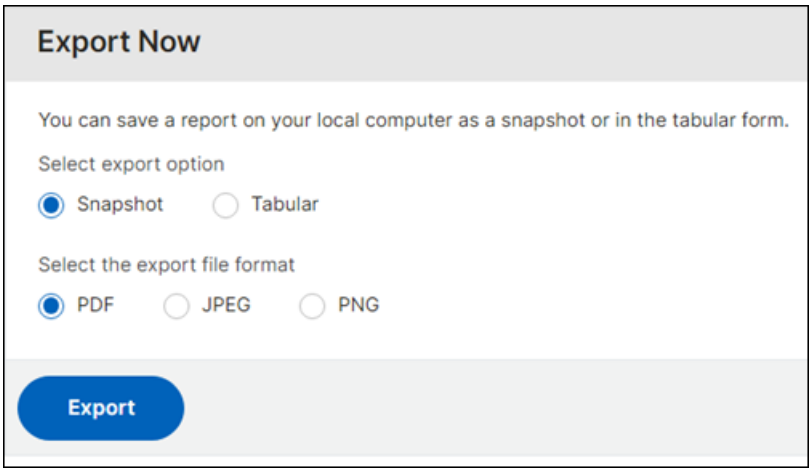
Para exportar direcciones IP propiedad de NetScaler, siga estos pasos:

1. Vaya a **Infraestructura > Instancias > IP propiedad de NetScaler**.

2. En la página **IP propiedad de NetScaler**, haga clic en el icono de exportación situado en la esquina superior derecha.
3. En la página **Exportar informes**, haga clic en **Exportar ahora**.
4. En la página **Exportar ahora**, seleccione la opción de exportación:

   Para la exportación de **instantáneas**:

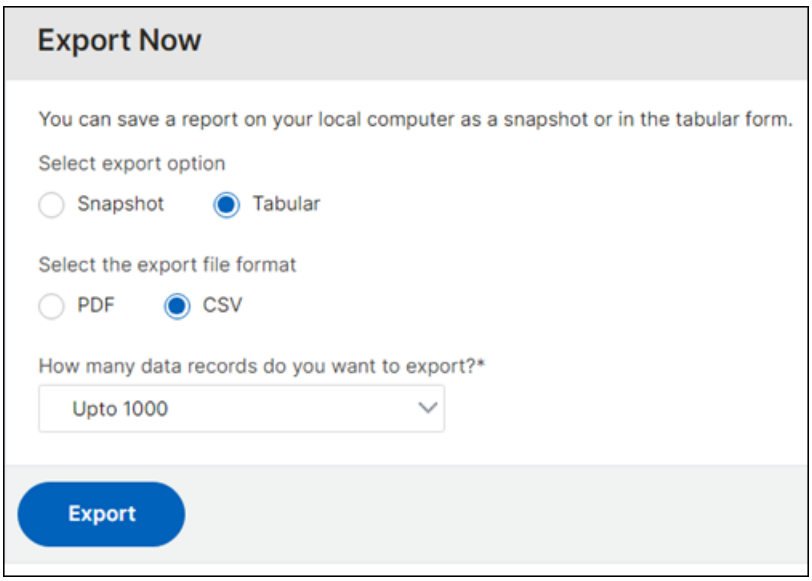
   a) Seleccione el formato del archivo de exportación: PDF, JPG o PNG.



   Para la exportación **tabular**:

   a) Seleccione el formato del archivo de exportación: PDF o CSV.

   b) Seleccione la cantidad de registros de datos que desea exportar de la lista.



5. Haga clic en **Exportar**.

Programar la exportación de direcciones IP propiedad de NetScaler

Para programar la exportación de direcciones IP propiedad de NetScaler, siga estos pasos:

1. Vaya a **Infraestructura > Instancias > IP propiedad de NetScaler**.
2. En la página **IP propiedad de NetScaler**, haga clic en el icono de exportación situado en la esquina superior derecha.
3. En la página **Exportar informes**, haga clic en **Programar exportación**.
4. En la página **Programar exportación**, introduzca los siguientes detalles:
   a) Introduzca el asunto y la descripción.
   b) Seleccione el tipo de exportación.

      Para el tipo de exportación de **instantáneas**:

      - Seleccione el formato del archivo de exportación: PDF, JPG o PNG.

      Para el tipo de exportación **tabular**:

      - Seleccione el formato del archivo de exportación: PDF o CSV.
      - Seleccione la cantidad de registros de datos que desea exportar de la lista.

   c) Seleccione la periodicidad: diaria, semanal o mensual.
   d) Seleccione la hora de exportación.
   e) Seleccione cómo enviar las direcciones IP exportadas: correo electrónico, Slack o ambos.

      Para correo electrónico:

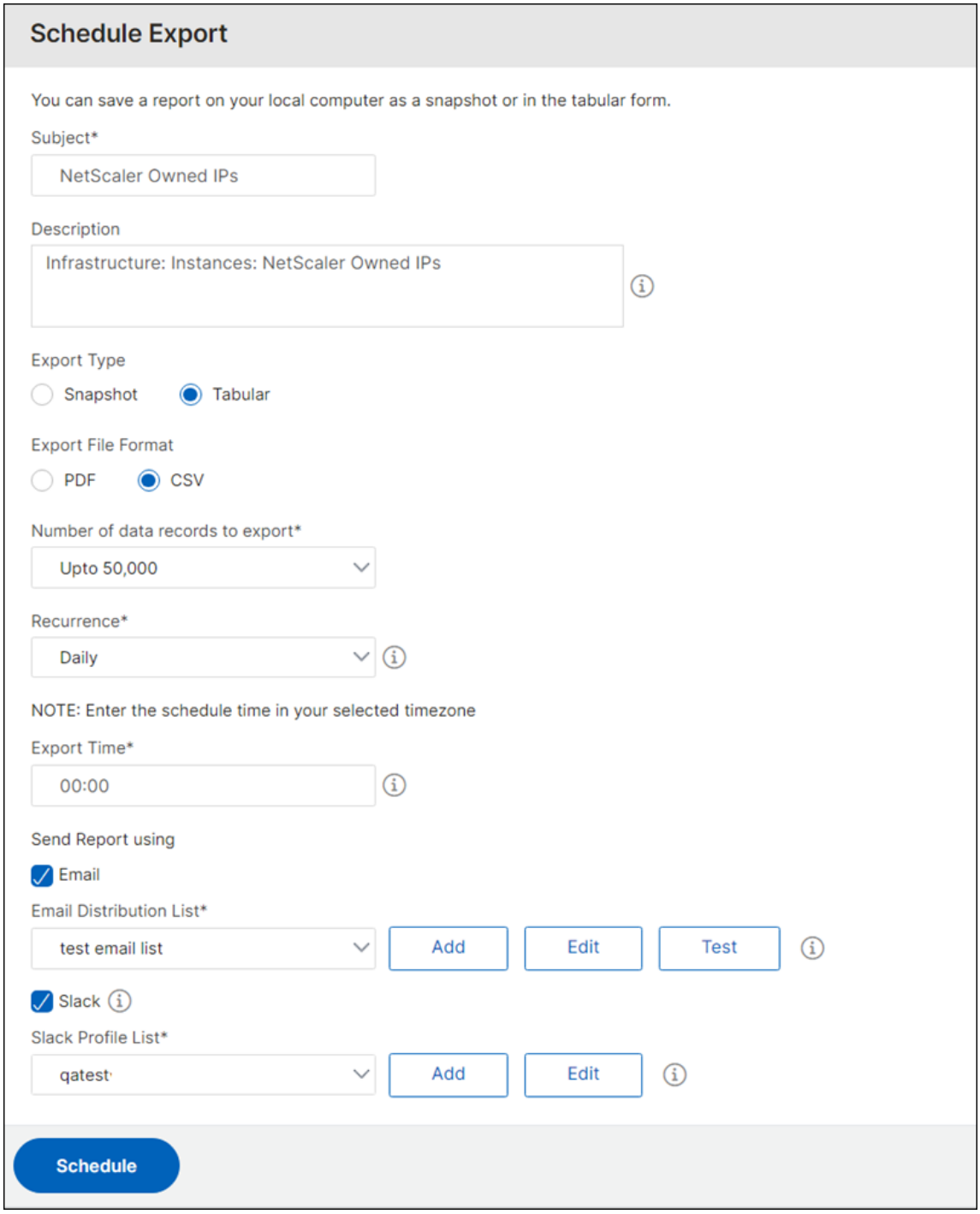
      - Seleccione **Correo electrónico** y elija la lista de distribución de correo electrónico para enviar la lista de direcciones IP propiedad de NetScaler.
        - Para agregar una lista de distribución de correo electrónico, haga clic en **Agregar** y especifique los detalles del servidor de correo electrónico.
        - Para editar una lista de distribución de correo electrónico, haga clic en **Editar**.
        - Para comprobar que la lista de distribución de correo electrónico funciona, haz clic en **Probar**. Esto enviará un correo electrónico de prueba a la lista de distribución de correo electrónico seleccionada.

      Para Slack:

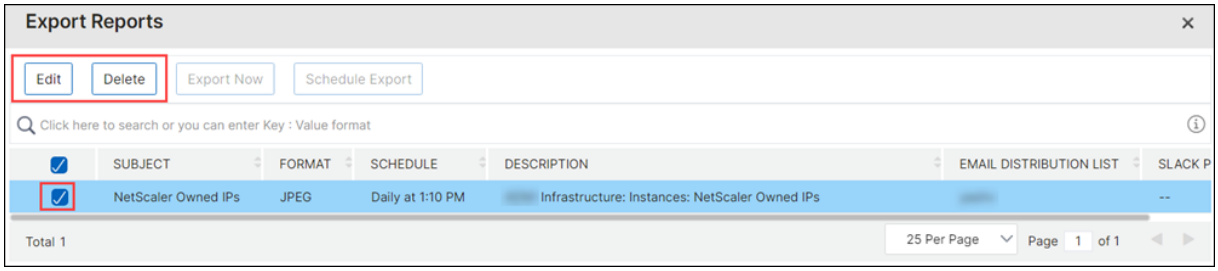
      - Seleccione **Slack** y elija la lista de perfiles de Slack para enviar la lista de direcciones IP propiedad de NetScaler.
        - Para agregar un perfil de Slack, haga clic en **Agregar** y especifique el **nombre del perfil**, el **nombre del canal** y el **token** del canal de Slack.

- Para editar un canal de Slack existente, haga clic en **Editar**.

5. Haga clic en **Programar** para programar la exportación.



Una vez programada, su programación de exportación aparece en la página **Exportar informes** y puede seleccionar la programación para realizar la operación de edición o eliminación.



Cómo cambiar la contraseña raíz de NetScaler MPX o VPX

January 26, 2024

Ocasionalmente, debe cambiar la contraseña raíz del dispositivo NetScaler por razones de seguridad o de conformidad con la directiva de rotación de contraseñas.

Este documento describe los pasos necesarios para cambiar la contraseña raíz de los dispositivos NetScaler MPX y VPX gestionados a través de la nube de NetScaler Console.

Si cambia la contraseña de NetScaler, debe modificar el perfil de administrador de NetScaler Console que está asociado al NetScaler. Un perfil de administrador de NetScaler Console mantiene las credenciales de NetScaler para la comunicación basada en REST API, SSH, SCP o SNMP con el dispositivo NetScaler. A través de los perfiles de administración, NetScaler Console administra los dispositivos NetScaler MPX y VPX.

Cambiar la contraseña mediante la función Trabajos de configuración

Al utilizar la función de trabajos de configuración de la consola de NetScaler, puede simplificar el proceso repetitivo de cambio de contraseñas y aplicar los cambios a los dispositivos NetScaler, sin acceder a las instancias individuales.

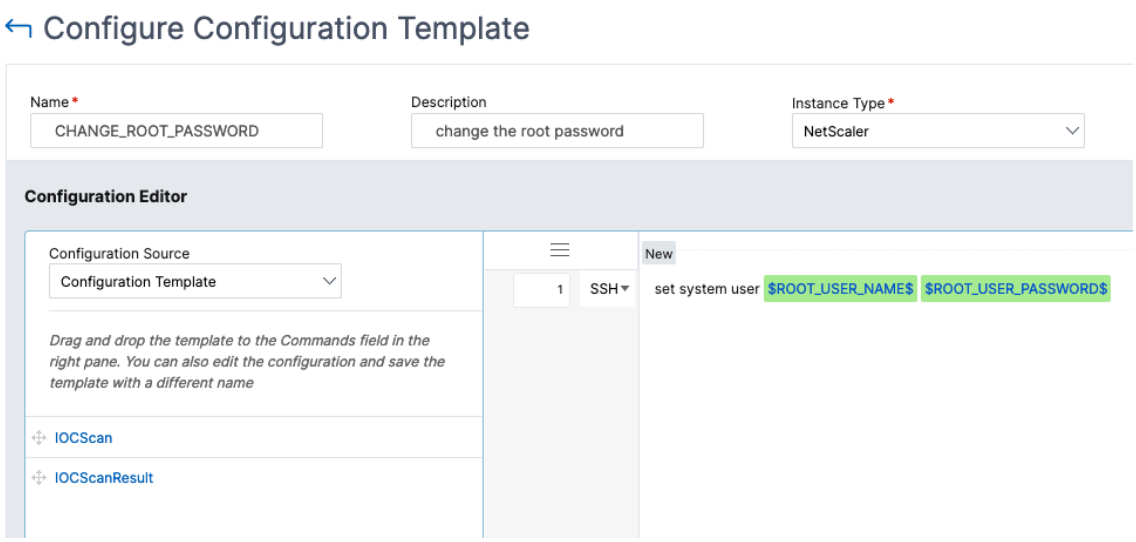
Siga estos pasos para cambiar la contraseña:

- Paso 1. Cree una plantilla de configuración.
- Paso 2. Cree un trabajo de configuración.
- Paso 3. Crea un perfil de administrador y modifícalo.

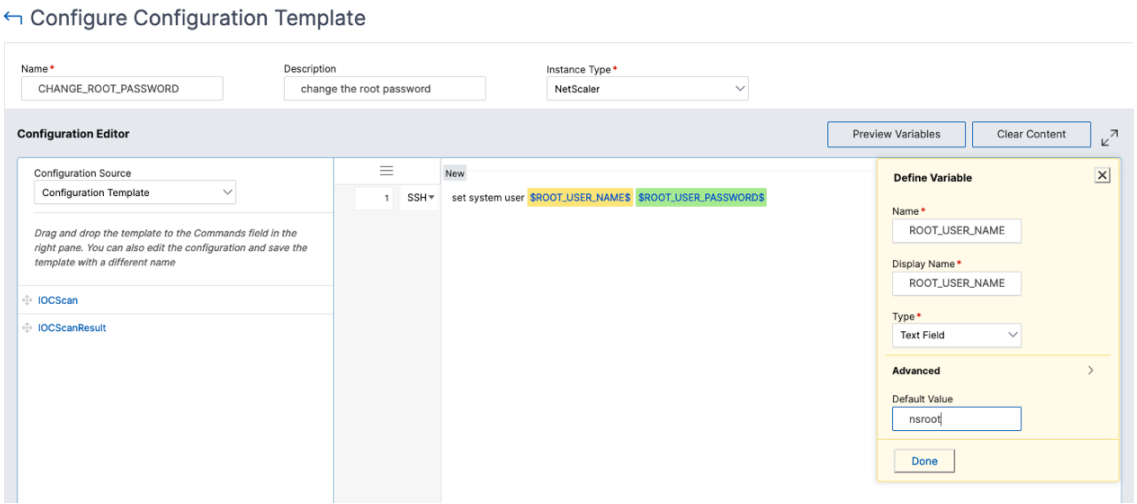
> Nota:
>
> Si los dispositivos NetScaler también se administran con otras herramientas, también debe cambiar las credenciales de esas herramientas.

Crear una plantilla de configuración

1. Desde la GUI de NetScaler Console, vaya a **Infraestructura > Trabajos de configuración > Plantillas de configuración** .
2. Seleccione **Add**. Cree una plantilla de configuración con escribiendo el comando SSH `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



3. Seleccione la variable $ROOT_USER_NAME$ y seleccione **Campo de texto como Tipo**.
4. Si lo quiere, proporcione el valor predeterminado para el nombre de usuario raíz. Seleccione **Listo** para guardar la configuración de la variable.

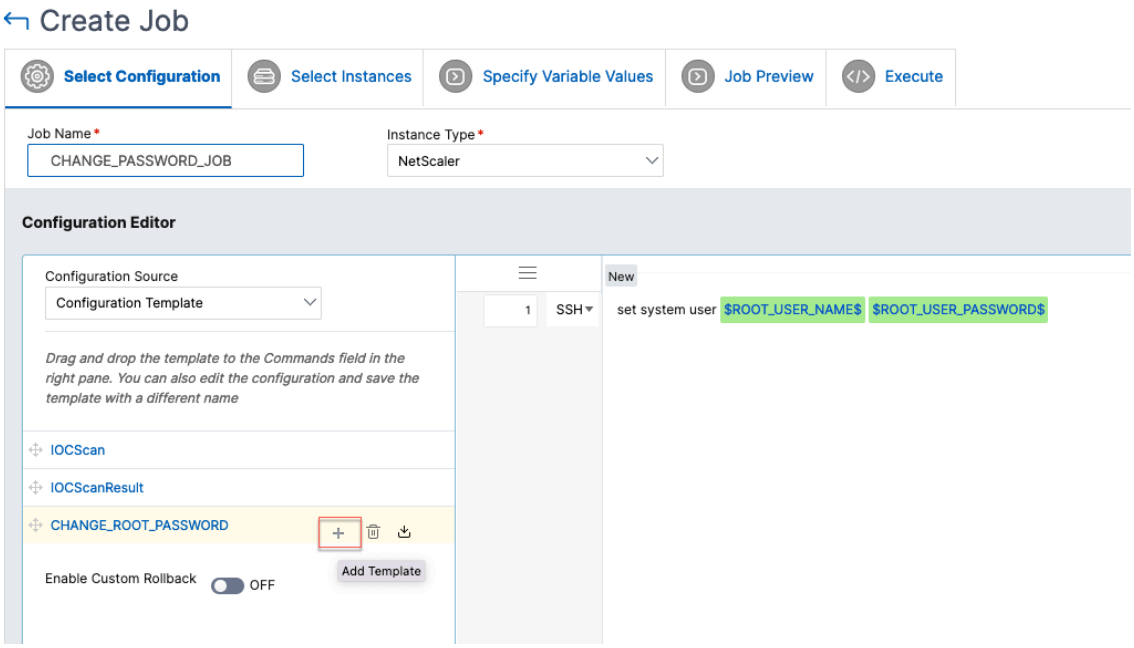


5. Seleccione la variable $ROOT_USER_PASSWORD$ y seleccione **Campo de contraseña como Tipo**. Seleccione **Listo** para guardar la configuración de la variable.
6. Seleccione **Aceptar** para guardar la plantilla de configuración.

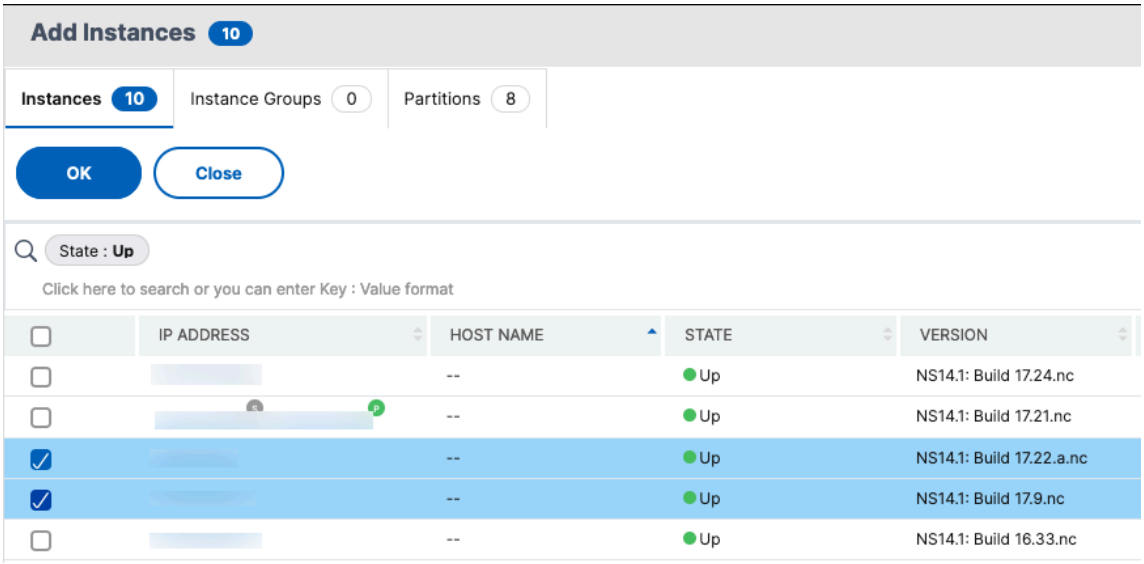
7. La nueva plantilla de configuración aparece en **Plantillas de configuración**.

Crear un trabajo de configuración

1. Desde la GUI de NetScaler Console, vaya a **Infraestructura > Trabajos de configuración**.
2. Seleccione **Crear trabajo** y haga clic en el icono "+"de la nueva plantilla de configuración. Seleccione **Siguiente**.

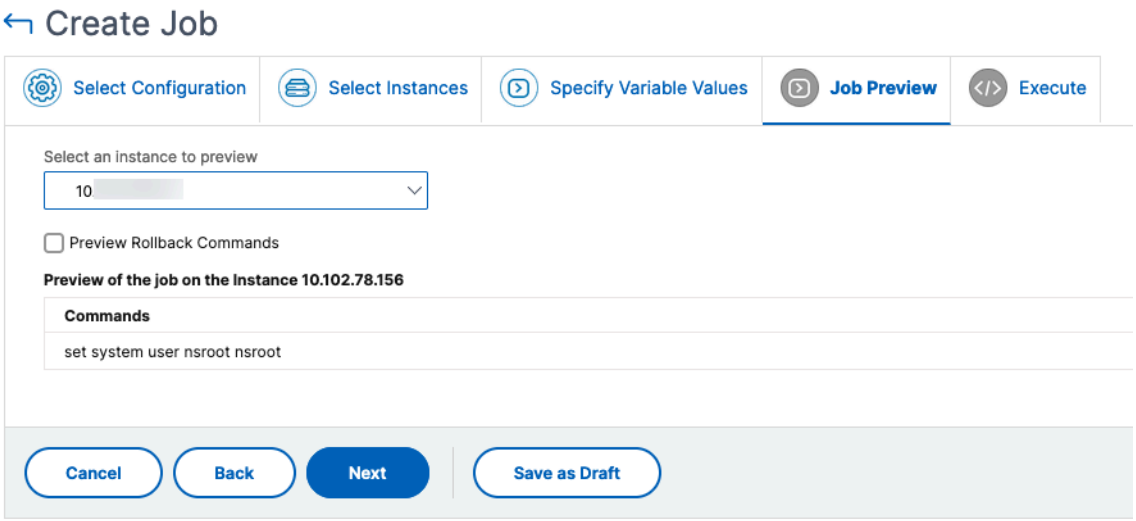


3. Seleccione la instancia o instancias de NetScaler para las que se debe modificar la contraseña.



4. En el panel **Seleccionar instancias**, seleccione las instancias y haga clic en **Siguiente**.

5. En el panel **Especificar valores variables**, especifique los valores para el nombre de usuario y la contraseña y haga clic en **Siguiente**.
6. En Vista **previa del trabajo** , compruebe los comandos de la CLI reales que la consola de NetScaler ejecutará en las instancias de NetScaler. Si la vista previa se ve bien, haga clic en **Siguiente**.

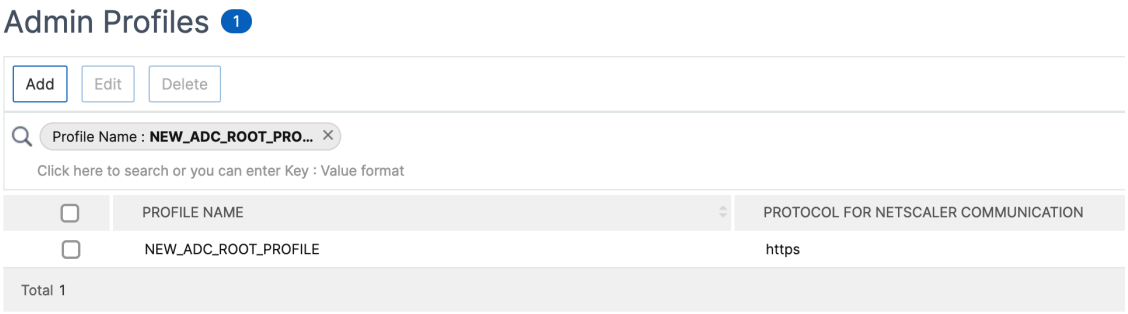


7. En el panel **Ejecutar**, puede ejecutar el trabajo inmediatamente o programarlo para más adelante. También puede optar por ejecutar el trabajo en paralelo en todas las instancias seleccionadas o hacerlo de forma secuencial. Seleccione Finalizar después de proporcionar los detalles de la ejecución.
8. El trabajo de configuración muestra si la ejecución se realizó correctamente o falló.
9. Seleccione el **trabajo** y haga clic en **Detalles**. Los detalles de ejecución muestran el estado a nivel de instancia individual.

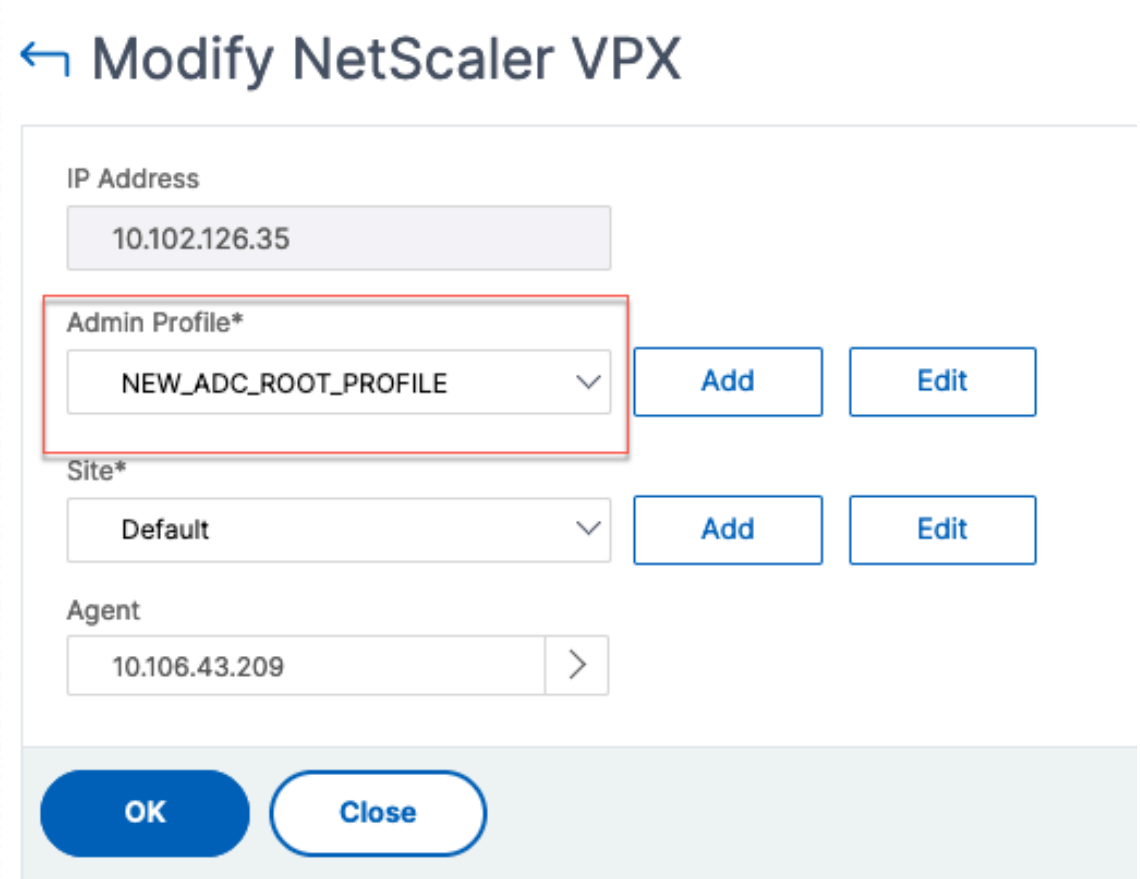
Modificar el perfil de administrador

Después de modificar las contraseñas de NetScaler, debe agregar y modificar los perfiles de administración de las instancias. Siga estos pasos:

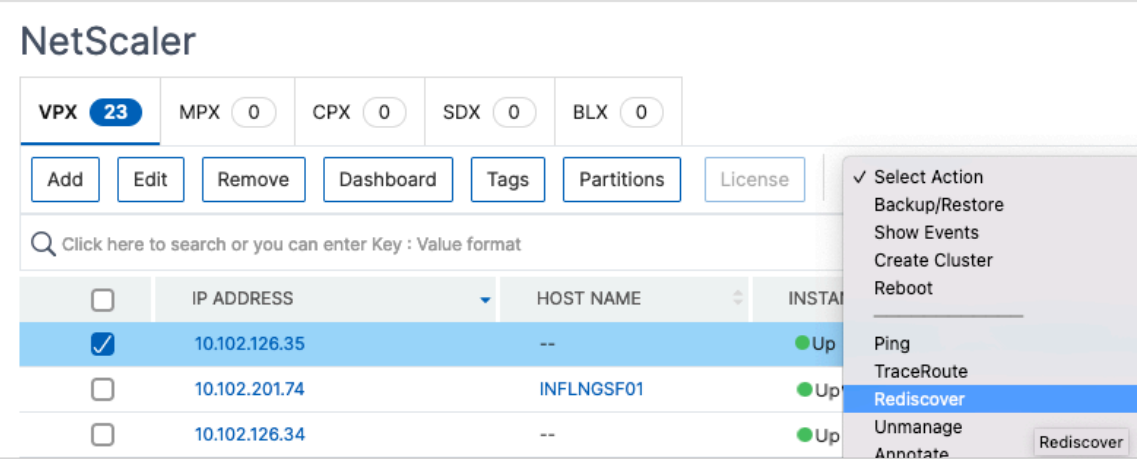
1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. Haga clic en **Perfiles** para ver todos los perfiles de administración.
3. Seleccione **Agregar** para crear un perfil de administrador y proporcionar nuevas credenciales de NetScaler.



4. El perfil recién creado aparece en **Perfiles de administración**.
5. Vaya a **Red > Instancias > NetScaler**. Seleccione la instancia de NetScaler para la que se modificó la contraseña y, a continuación, seleccione **Modificar**.
6. Seleccione el nombre de perfil recién creado y haga clic en **Aceptar**.



7. Vuelva a seleccionar la instancia, pulse con el botón derecho y seleccione **Redescubrir**.



Ha cambiado correctamente la contraseña.

Para obtener información sobre cómo cambiar la contraseña de un dispositivo SDX, consulte Cómo cambiar una contraseña raíz SDX de NetScaler.

Cómo cambiar una contraseña nsroot de NetScaler SDX

January 26, 2024

Ocasionalmente, debe cambiar la contraseña nsroot del dispositivo NetScaler por motivos de seguridad o por cumplir con la directiva de rotación de contraseñas.

Este documento describe los pasos necesarios para cambiar la contraseña nsroot de un dispositivo NetScaler SDX administrado a través de la nube de NetScaler Console.

Si cambia la contraseña de NetScaler, debe modificar el perfil de administrador de NetScaler Console que está asociado al NetScaler. Un perfil de administrador de NetScaler Console mantiene las credenciales de NetScaler para la comunicación basada en REST API, SSH, SCP o SNMP con el dispositivo NetScaler. A través de los perfiles de administración, NetScaler Console administra los dispositivos NetScaler SDX.

Cambiar contraseña

Siga estos pasos para cambiar la contraseña:

- Paso 1. Cambie la contraseña de SDX desde la GUI del servicio de administración de SDX.
- Paso 2. Modifique el perfil de administrador de NetScaler Console asociado al SDX.

> Nota:
>
> Si el dispositivo SDX también lo administran otras herramientas, también debe cambiar las credenciales de esas herramientas.

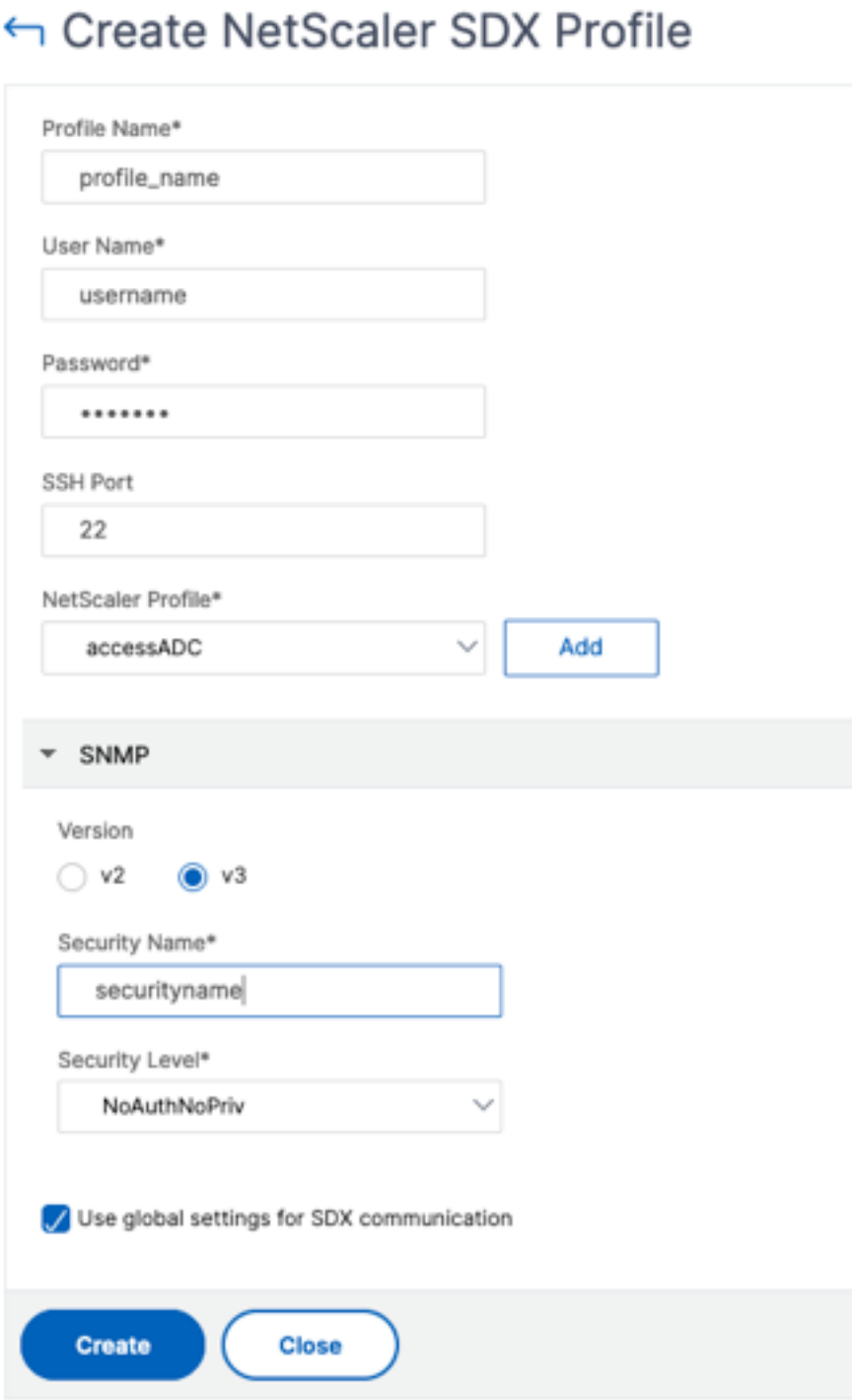
Cambie la contraseña de SDX desde la GUI del servicio de administración de SDX

1. Desde SDX Management Service, vaya a **Sistema > Administración de usuarios > Usuarios**.
2. Seleccione el nombre de usuario para el que quiere cambiar la contraseña y haga clic en **Modificar**.
3. Selecciona **Cambiar contraseña**.
4. Introduzca una contraseña nueva y haga clic en **Aceptar**.
5. Se ha cambiado la contraseña de SDX

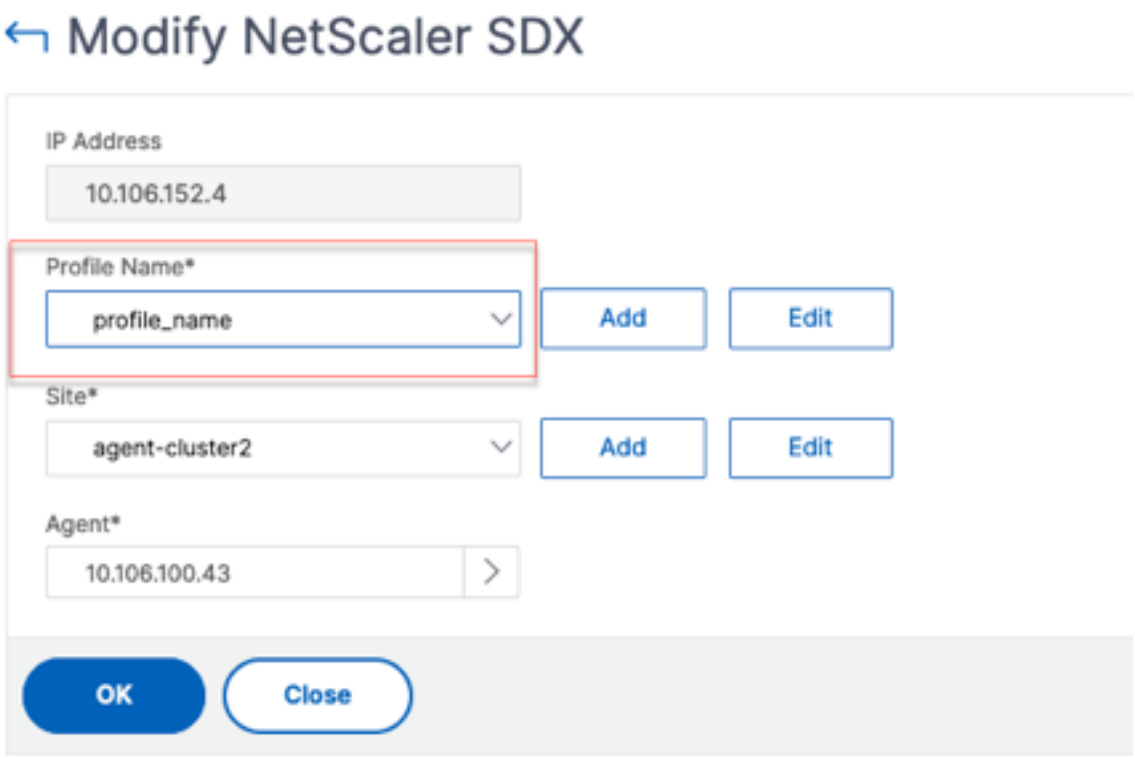
Modificar el perfil de administrador de NetScaler Console

Después de modificar las contraseñas de SDX, debes modificar los perfiles de administrador de las instancias. Siga estos pasos:

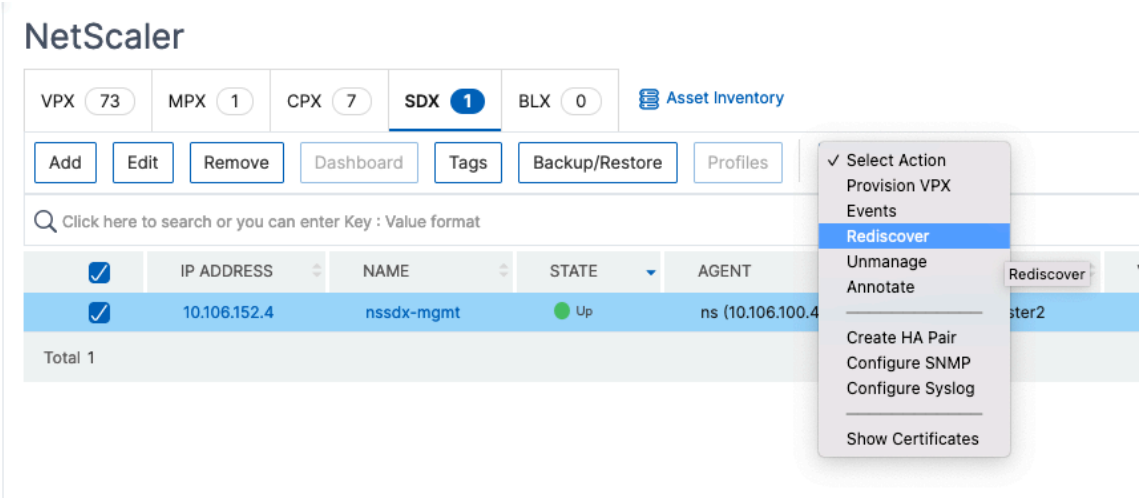
1. Vaya a **Infraestructura > Panel de instancias > NetScaler > SDX**.
2. Selecciona **Perfiles** para ver todos los perfiles de administración.
3. Selecciona **Agregar** para crear un perfil de administrador.
4. Proporcione las nuevas credenciales de NetScaler y haga clic en **Crear**.



5. El perfil recién creado aparece en **Perfiles de administración**.
6. Vaya a **Red > Instancias > NetScaler > SDX**. Seleccione la instancia para la que se modificó la contraseña y, a continuación, seleccione **Modificar**.
7. Seleccione el nombre del perfil recién creado y haga clic en **Aceptar**.



8. Vuelva a seleccionar la instancia, pulse con el botón derecho y elija **Redescubrir**



Ha cambiado correctamente la contraseña.

Para obtener información sobre cómo cambiar la contraseña de un dispositivo SDX, consulte Cómo cambiar una contraseña raíz de NetScaler MPX o VPX.

Cómo generar un paquete de soporte técnico para una instancia de NetScaler

January 26, 2024

Para obtener ayuda para analizar y resolver cualquier problema con una instancia de NetScaler, puede generar un paquete de soporte técnico en la instancia y enviarlo al soporte técnico de Citrix. El paquete de soporte técnico es un archivo tar comprimido con datos y estadísticas de configuración del sistema. El paquete de soporte técnico recopila los siguientes datos de la instancia de NetScaler en la que se genera el paquete:

- Archivos de configuración. Todos los archivos del directorio /flash/nsconfig.
- `newnslog` archivos. Los archivos que se están ejecutando actualmente `newnslog` y algunos archivos anteriores. Para minimizar el tamaño del archivo de almacenamiento, la colección `newnslog` está restringida a 500 MB, 6 archivos o 7 días, lo que ocurra primero. Si se necesitan datos antiguos, es posible que requiera la recopilación manual.
- Archivos de registro. Archivos en /var/log/messages, /var/log/ns.log y otros archivos en /var/log y /var/nslog.
- Archivos principales de la aplicación. Archivos creados en el directorio /var/core durante la última semana, si los hubiera.
- Salida de algunos comandos show de CLI.
- Salida de algunos comandos stat de CLI.
- Salida de los comandos de shell de BSD.

También puede cargar de forma segura el paquete de soporte técnico en el servidor de soporte técnico de Citrix. A partir de la versión 8.x de NetScaler 14.1, debe generar un token de autenticación antes de cargar el paquete de soporte técnico. En las versiones anteriores, puede cargar el paquete de soporte técnico con el nombre de usuario y la contraseña de Citrix.

Para generar el token de autenticación:

1. Inicie un navegador e introduzca la siguiente URL: https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600.
2. Inicie sesión con la autenticación multifactor.

   > **Nota:**
   >
   > Para obtener información sobre cómo inscribirse para la autenticación multifactor, consulte Cómo inscribirse en la autenticación multifactor (MFA).

3. Haga clic en **Copiar** para copiar el token de autenticación que aparece en la pantalla. El token es válido durante 3600 segundos (1 hora). La longitud máxima permitida para el token es de 1023 caracteres.

Después de copiar el token de autenticación, utilice la GUI para cargar el archivo.

Para cargar el paquete de soporte técnico mediante la GUI:

1. Vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione una instancia de NetScaler.
3. Seleccione **Generar archivo de soporte técnico** en **Seleccionar acciones**.
4. Haga clic en **Generar archivo de soporte técnico**.
5. Use la opción **Alcance** para especificar si desea recopilar datos en el nodo actual, en todos los nodos del clúster o para las particiones especificadas.
6. Seleccione **Cargar el archivo recopilador**.
7. En la sección **Mi cuenta de Citrix**, introduzca el token de autenticación en el campo **Token de autenticación de Citrix**.
8. Haga clic en **Crear soporte técnico**.

Eventos

January 26, 2024

Cuando la dirección IP de una instancia de Citrix Application Delivery Controller (NetScaler) se agrega a NetScaler Console, NetScaler Console envía una llamada 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 se produce un error del sistema o un cambio en la configuración, se genera un evento y se graba en el servidor de NetScaler Console. Los eventos recibidos en NetScaler Console se muestran en la página Resumen de eventos (**Infraestructura Eventos**) y todos los eventos activos se muestran en la página Mensajes de eventos (**Infraestructura > Eventos > Mensajes** de eventos).

NetScaler Console también comprueba los eventos generados en las instancias para crear alarmas de diferentes niveles de gravedad y las muestra 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 se puede solucionar inmediatamente.

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de varios eventos generados en 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 intervalo de tiempo específico para un evento hasta que se borre el evento. Como medida adicional, es posible que quiera personalizar su correo electrónico con una línea de asunto específica, un mensaje de usuario y cargar un archivo adjunto.

Usar panel de eventos

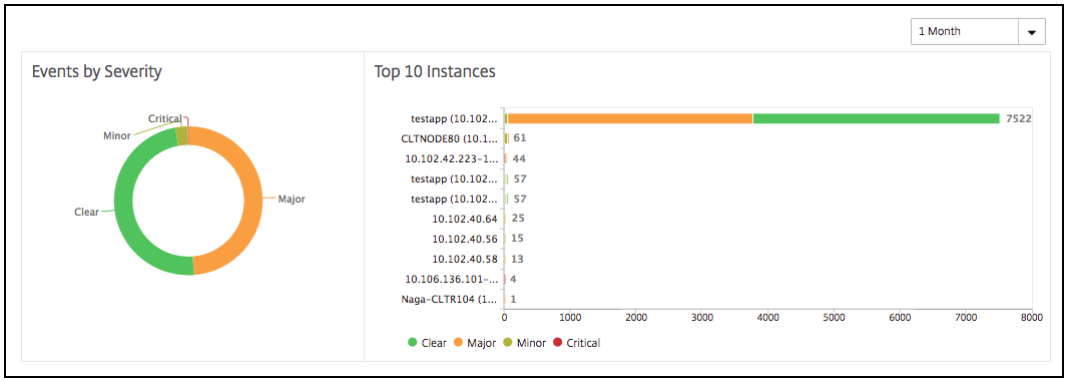
March 6, 2024

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 (NetScaler), junto con los eventos y su gravedad en instancias específicas. Puede usar el panel de eventos de NetScaler Console para ver los informes generados para obtener detalles sobre la gravedad de los eventos críticos en todas sus instancias de NetScaler.

Para ver los detalles en el panel de eventos:

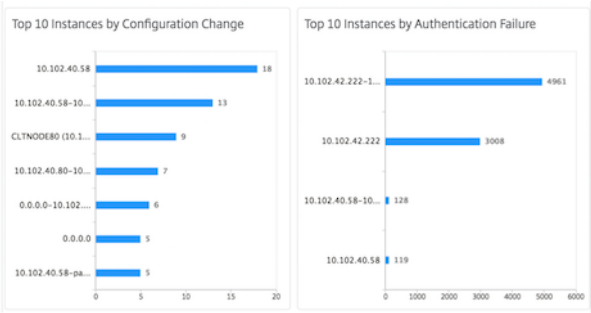
Vaya a **Infraestructura > Eventos > Informes**.

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.

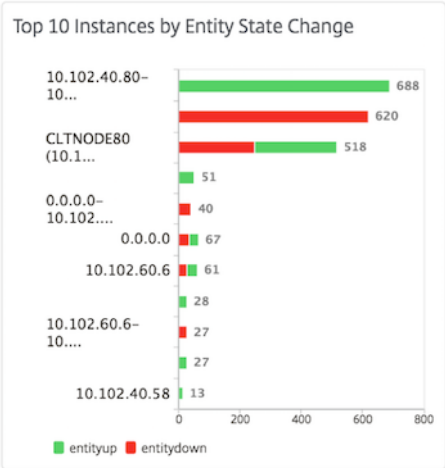


Para ver más detalles, vaya al tipo de instancia de NetScaler (**Infraestructura > Eventos > Informes > NetScaler/ NetScaler SDX/ NetScaler**) para ver lo siguiente:

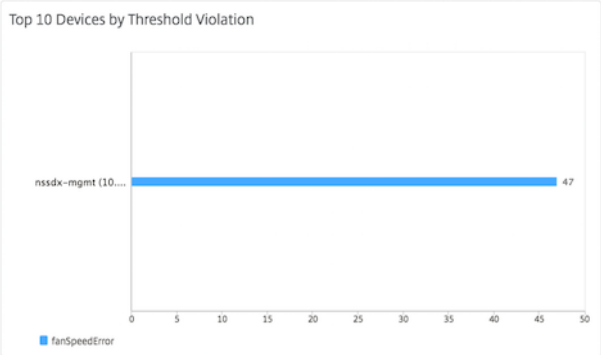
- Los 10 dispositivos principales por fallo de hardware
- Los 10 dispositivos principales por cambio de configuración
- Los 10 dispositivos principales por error de autenticación



- Los 10 principales dispositivos por cambios de estado de entidad



- Los 10 dispositivos principales por infracción de umbral



Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de

demora.

> **Nota:**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona **Periodicidad mensual**, asegúrese de introducir todos los días en los que quiere que se programe el informe separados por comas.

Crear reglas de eventos

May 9, 2024

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan el filtrado de los eventos generados en 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.

Puede crear filtros para las siguientes condiciones:

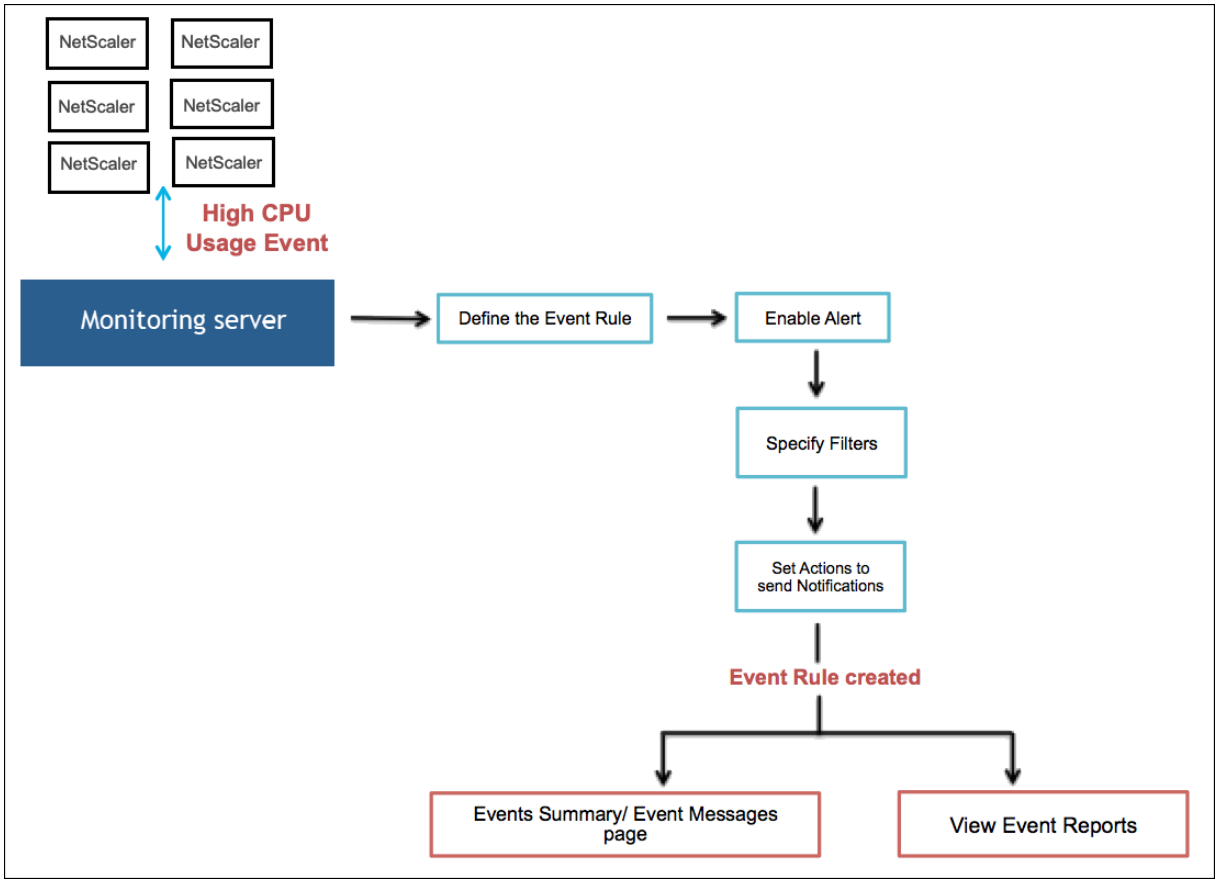
- Gravedad
- Instancias de Citrix Application Delivery Controller (NetScaler)
- Categoría
- Objetos de error
- Comandos de configuración
- Mensajes

Después de crear eventos, puede asignar acciones a los eventos. Para obtener más información, consulte Agregar acciones de reglas de eventos.

Por ejemplo, como administrador, es posible que desee supervisar los eventos de «uso elevado de la CPU» en las instancias de NetScaler que podrían provocar una interrupción. Puede realizar cualquiera de las siguientes acciones para recibir notificaciones:

- Cree una regla para supervisar las instancias y agregue una acción a la regla para recibir notificaciones cuando se produzcan dichos eventos.
- Programa una regla para supervisar las instancias en un intervalo específico. Por lo tanto, recibirá notificaciones cuando dichos eventos ocurran dentro de ese intervalo.

La siguiente imagen explica el flujo de trabajo de cómo funcionan las reglas de eventos.



Configurar una regla de eventos

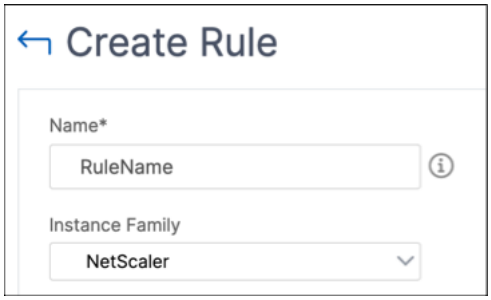
Para configurar una regla de eventos, vaya a **Infraestructura > Eventos > Reglas** y haga clic en **Agregar**. En la página **Crear regla** , realice las siguientes tareas:

1. Especifique el nombre y la familia de instancias
2. Configurar la antigüedad del evento
3. Elija la gravedad del evento que detecta la regla
4. Especifique la categoría del evento
5. Especificar instancias NetScaler a las que se aplica la regla
6. Seleccionar objetos de error
7. Especificar filtros avanzados
8. Especificar las acciones que se deben realizar cuando la regla detecta un evento

Paso 1: Especificar el nombre y la familia de instancias

1. **Nombre**. Introduzca un nombre para la regla del evento.
2. **Familia**de instancias . Seleccione una familia de instancias en la lista desplegable **Familia de instancias**.

   Puede filtrar las reglas de eventos por **familia** de instancias para rastrear la instancia de NetScaler desde la que NetScaler Console recibe un evento.



Paso 2: Configurar la edad del evento

1. **Edad del evento**. Especifique el intervalo de tiempo (en segundos) tras el cual NetScaler Console actualiza una regla de evento.

   Por ejemplo, quiere que se envíe un correo electrónico cada vez que la instancia de NetScaler tenga un evento de «uso elevado de la CPU» durante 60 segundos o más. Puede establecer la edad del evento en 60 segundos. Ahora, cada vez que su instancia de NetScaler tenga un evento de "uso elevado de CPU"durante 60 segundos o más, recibirá una notificación por correo electrónico.

   > **Nota:**
   >
   > La**edad del evento** es un campo obligatorio. El valor mínimo para la antigüedad del evento es de 60 segundos. Si deja el campo **Antigüedad del evento** en blanco, la regla del evento se aplica inmediatamente después de que se produzca el evento.

2. Elige una de las siguientes opciones para hacer seguimiento de los eventos:

   - **Omitir el registro de eventos hasta que se alcance la antigüedad del evento**. Los eventos que se producen antes de la antigüedad especificada no se registran en la base de datos del servidor de NetScaler Console. Cuando se alcanza la antigüedad del evento, los eventos se registran en la base de datos y se activan las acciones de eventos configuradas.
   - **Registrar los eventos al instante, independientemente de la antigüedad y duración del evento**. Todos los eventos se registran en la base de datos del servidor de NetScaler

Console, independientemente de la antigüedad de los eventos especificada. Una vez alcanzada la antigüedad del evento, se activan las acciones del evento configuradas.

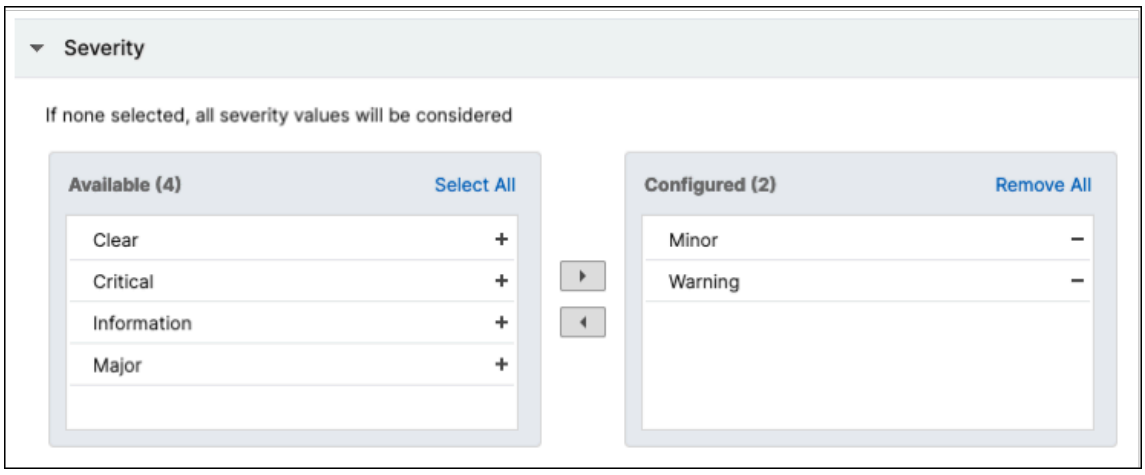
3. **Habilitar el filtro avanzado con coincidencia de expresiones regulares**. Seleccione esta opción para incluir una expresión regular distinta de la coincidencia con patrón de asterisco (*). Esta opción es aplicable a los objetos de error, los comandos de configuración y los mensajes.

Paso 3: Elegir la gravedad del evento

- En la sección **Gravedad**, seleccione una gravedad para la regla de evento.

  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 Console, 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**.

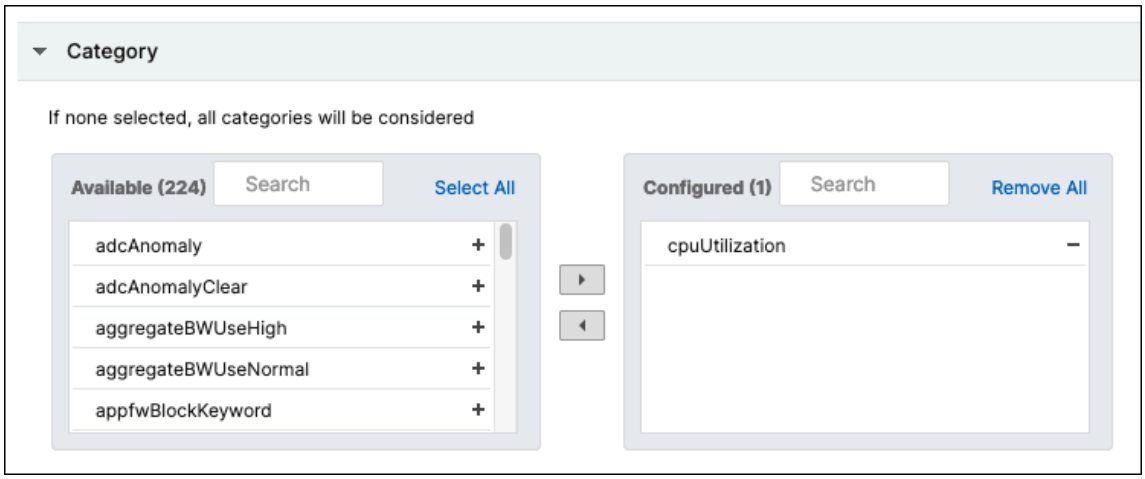


Paso 4: Especificar la categoría del evento

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 asignan con la consola de NetScaler, que se puede utilizar para definir las reglas de eventos.

- Seleccione la categoría que quiera considerar y muévala de la tabla **Disponible** a la tabla **Configurada**.

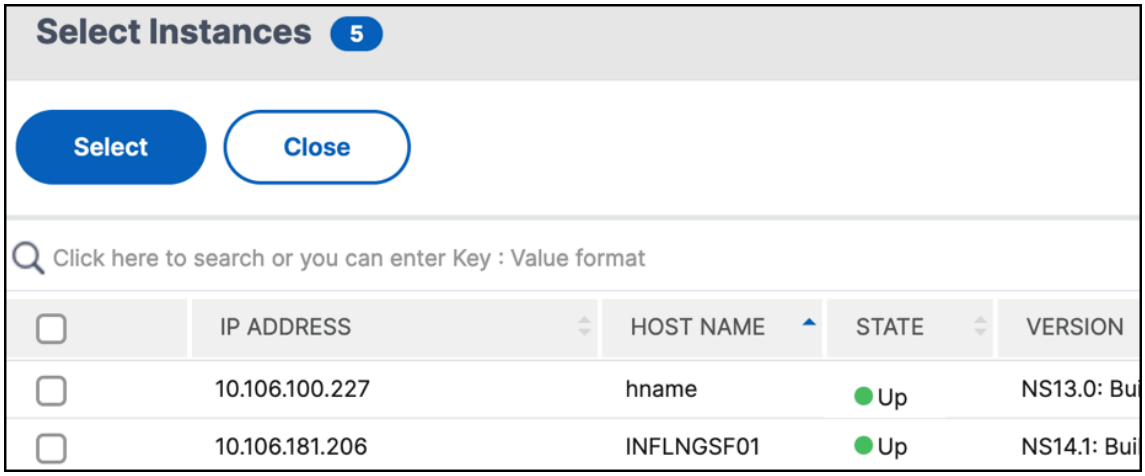
  En el ejemplo, debe elegir "cpuUtilization"como categoría de eventos en la tabla que se muestra.



Paso 5: Especificar instancias de NetScaler

En la sección **Instancias**, haga lo siguiente:

1. Haga clic en **Seleccionar instancias**. En la página **Seleccionar instancias**, seleccione las direcciones IP de las instancias de NetScaler para las que quiere definir la regla de eventos.
2. Haga clic en **Seleccionar**.



Paso 6: Seleccione objetos de error

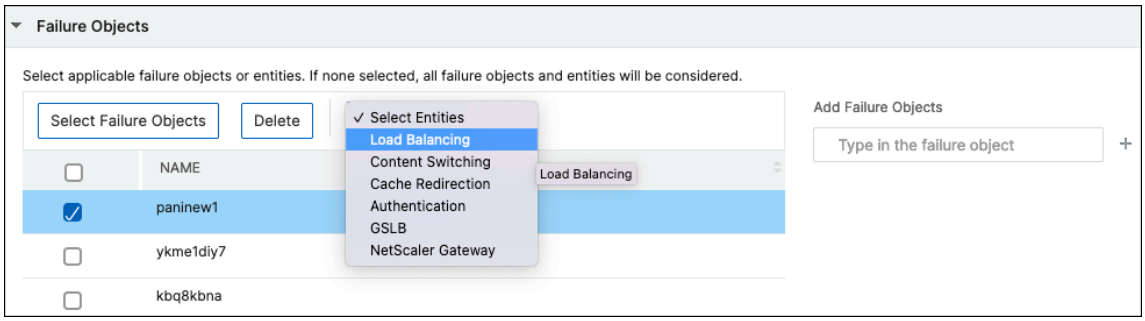
Los objetos de error son instancias de entidad o contadores para los que se ha generado un evento.

1. Haga clic en **Seleccionar objetos de error**.
2. En la página **Objetos de error**, seleccione un objeto de error de la lista. Haga clic en **Seleccionar**.
3. Para agregar un objeto de error, introduzca una expresión regular en **Agregar objetos de error**. Según la expresión regular especificada, los objetos de error se agregan automáticamente a la lista.

   > **Importante:**
   >
   > Para enumerar los objetos fallidos mediante expresiones regulares, seleccione **Habilitar filtro avanzado con coincidencia de expresiones** regulares en el paso1.

   El filtro avanzado le permite realizar un seguimiento rápido de los problemas en los objetos de error e identificar la causa de un problema. Por ejemplo, si un usuario tiene problemas para iniciar sesión, el objeto de error es el nombre de usuario o la contraseña, como `nsroot`.
4. Para agregar entidades, elija una entidad de **Seleccionar entidades**.

   Esta lista puede incluir nombres de contador para todos los eventos relacionados con los umbrales, nombres de entidades para todos los eventos relacionados con la entidad, nombres de certificados para los eventos relacionados con los certificados, etc.

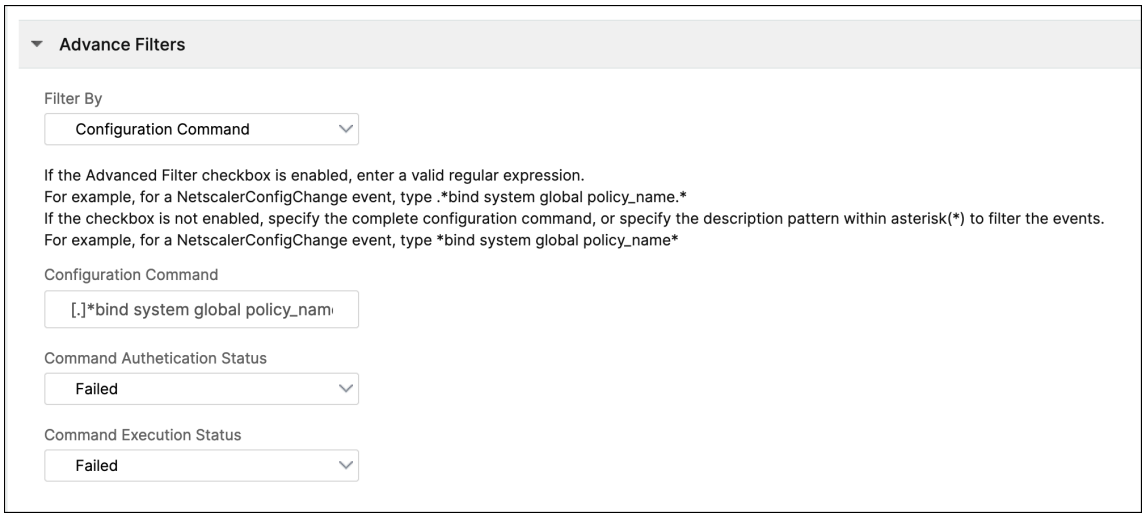


Paso 7: Especificar filtros avanzados

Puede filtrar aún más una regla de evento con filtros avanzados. Seleccione uno de los siguientes filtros:

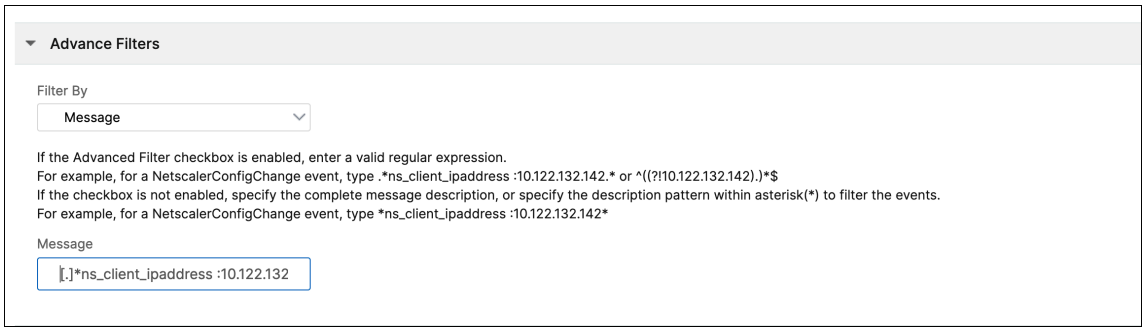
- **Comandos de configuración**: Especifique el comando de configuración completo o especifique una expresión regular para filtrar los eventos.

También puede filtrar las reglas de eventos según el estado de autenticación del comando y su estado de ejecución. Por ejemplo, para a `NetscalerConfigChange event`, escriba `[.]* bind system global policy_name[.]*`.



- **Mensajes**: Especifique la descripción completa del mensaje o especifique 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[.]*)` .



> **Importante:**
>
> Para filtrar los comandos y mensajes de configuración mediante expresiones regulares distintas de la coincidencia de patrones con asterisco (*), seleccione **Habilitar filtro avanzado con coincidencia de expresiones regulares en el paso 1**.

Paso 8: 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 se realizan cuando un evento cumple los criterios de filtro definidos que estableciste en el paso 7.

1. Haga clic en **Agregar acción**.
2. En la página **Agregar acción de evento**, puede agregar las siguientes acciones de evento:

- Acción de envío de correo electrónico
- 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

Acción de envío de correo electrónico

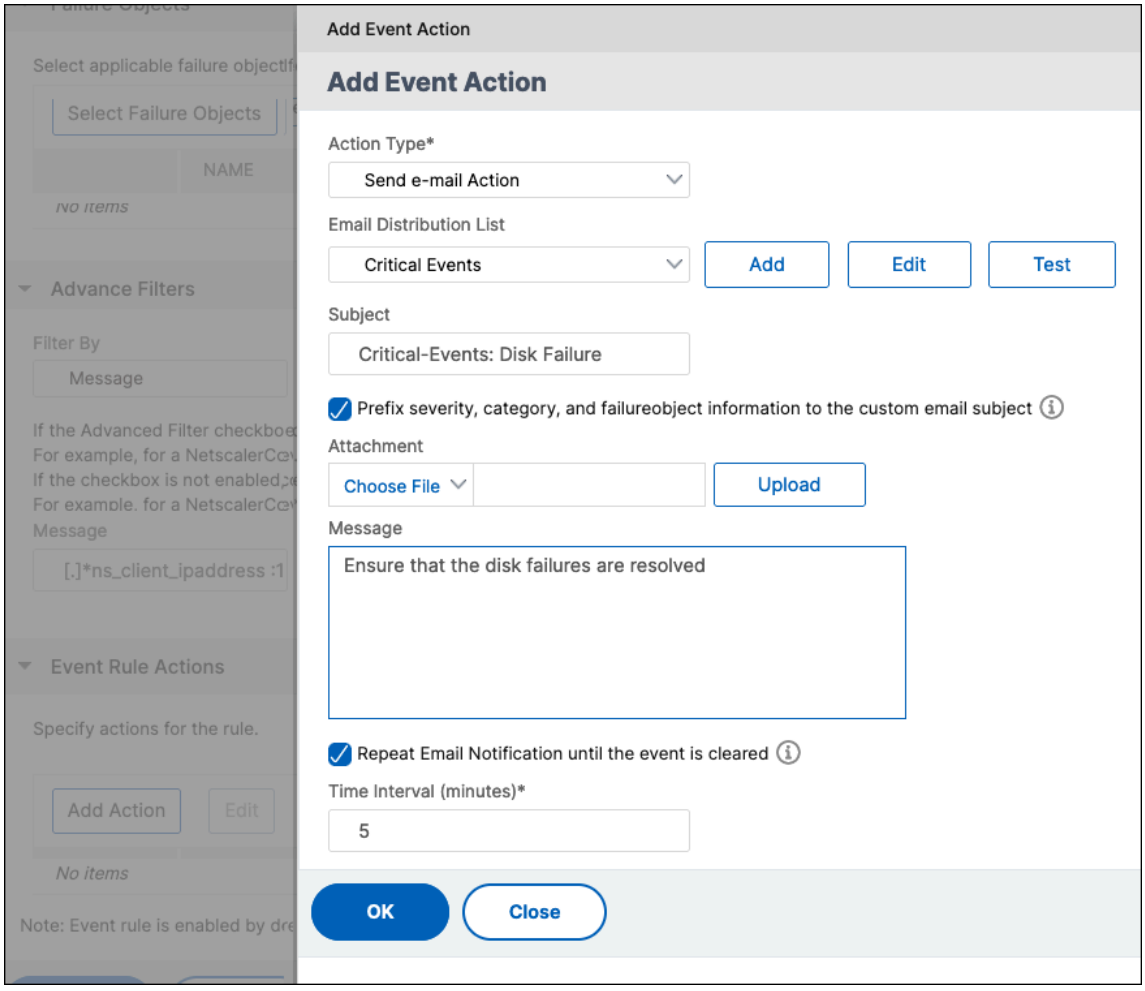
Al elegir **Enviar acción de correo electrónico**, se activa un correo electrónico cuando los eventos cumplen los criterios de filtro definidos.

1. **Lista de distribución de correo electrónico**. Seleccione una lista de distribución de correo electrónico. Para agregar una lista de distribución, haga clic en Agregar.
    a) En la página **Crear lista de distribución de correo electrónico**, haga lo siguiente:
        i. **Nombre**. Agregue un nombre para la lista de distribución.
        ii. **Servidores de correo electrónico**. Seleccione un servidor de correo electrónico. También puede agregar un servidor o modificar uno existente.
        iii. **De**. Agregue la dirección de correo electrónico del remitente.
        iv. **Para**. Agregue las direcciones de correo electrónico de los destinatarios. También puede especificar las direcciones de correo electrónico que se incluirán en la lista CC y Bcc.
        v. Haga clic en **Crear**.
2. **Asunto**. Agregue una línea de asunto para sus correos electrónicos, como el nombre de la entidad afectada, es decir, el nombre del objeto de error. Esta línea de asunto proporciona información sobre el servidor virtual en el que se producen estos eventos.

> **Nota:**
>
> Si no agrega una línea de asunto, se muestra una línea de asunto predeterminada. La línea de asunto predeterminada solo proporciona información sobre la gravedad del evento, la

> categoría del evento y el objeto de error. El nombre del servidor virtual en el que se produjo el evento no está disponible.

3. **Adjunto**. Cargue un adjunto al correo electrónico. Este adjunto se envía cuando un evento entrante coincide con la regla configurada.
4. **Prueba**. Haga clic en este botón para enviar un correo electrónico de prueba después de configurar un servidor de correo electrónico, las listas distribuidas asociadas y otros parámetros. Esta opción le permite probar los parámetros configurados
5. **Repita la notificación por correo electrónico hasta que se borre el evento**. Seleccione esta opción para asegurarse de que no se pierdan las notificaciones por correo electrónico en caso de eventos críticos. Esta opción envía correos electrónicos repetidos para las reglas de evento que cumplen los criterios seleccionados. Por ejemplo, ha creado una regla de evento para las instancias que implican errores de disco. Si quiere recibir una notificación hasta que se resuelva el problema, opte por recibir notificaciones repetidas por correo electrónico sobre esos eventos.



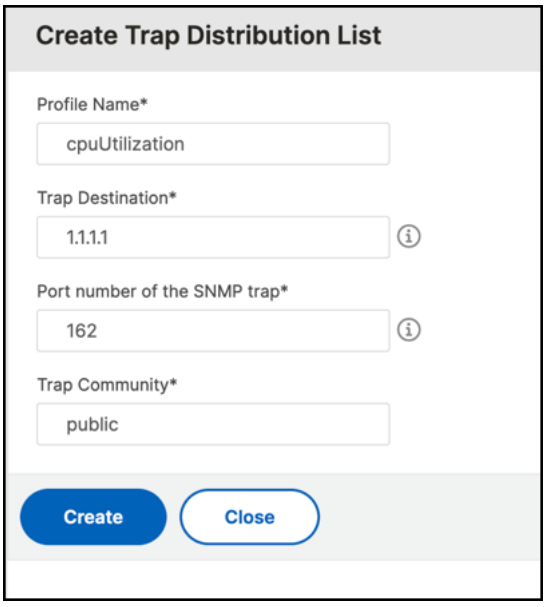
6. Haga clic en **Aceptar**.

> **Nota:**
>
> También puede agregar listas de distribución de correo electrónico si va a **Parámetros** > **Notificaciones** > **Correo electrónico**. Haga clic en **Agregar** y cree la lista.

Acción de captura de envío

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. Los mensajes de captura se envían a la escucha de capturas específica cuando los eventos cumplen los criterios de filtro definidos.

1. **Lista de distribución de captura**. Seleccione una lista de distribución de captura (o el destino de captura y los detalles del perfil de captura). Para crear una lista de distribución de captura, haga clic en **Agregar**.
2. En la página **Crear lista de distribución de captura**, haga lo siguiente:
   a) **Nombre del perfil**. Introduzca el nombre del perfil.
   b) **Destino de la captura**. Introduzca el nombre o la dirección IP de la instancia que debe recibir los mensajes de captura.
   c) **Número de puerto de la captura SNMP**. Introduzca el número de puerto.
   d) **Comunidad de captura**. Introduzca el grupo al que pertenece la instancia.



   e) Haga clic en **Crear**.
3. Haga clic en **Aceptar**.

Ejecutar acción de comando

Al elegir la acción de evento **Run Command Action**, puede crear un comando o un script que se pueda ejecutar en NetScaler Console para los 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 definidas 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 muestre 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 que quiera ofrecer una solución rápida agregando otro servidor virtual. En NetScaler Console, 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
```

- Guarde el archivo.sh en cualquier ubicación persistente del agente. Por ejemplo, /var.
- Proporcione la ubicación del archivo.sh en NetScaler Console para que se ejecute cuando se cumplan los criterios de la regla.

1. En **Lista de ejecución de comandos**, haga clic en **Agregar**.

   Aparece la página Crear lista de distribución de comandos.

   a) **Nombre del perfil**. Especifique un nombre de su elección

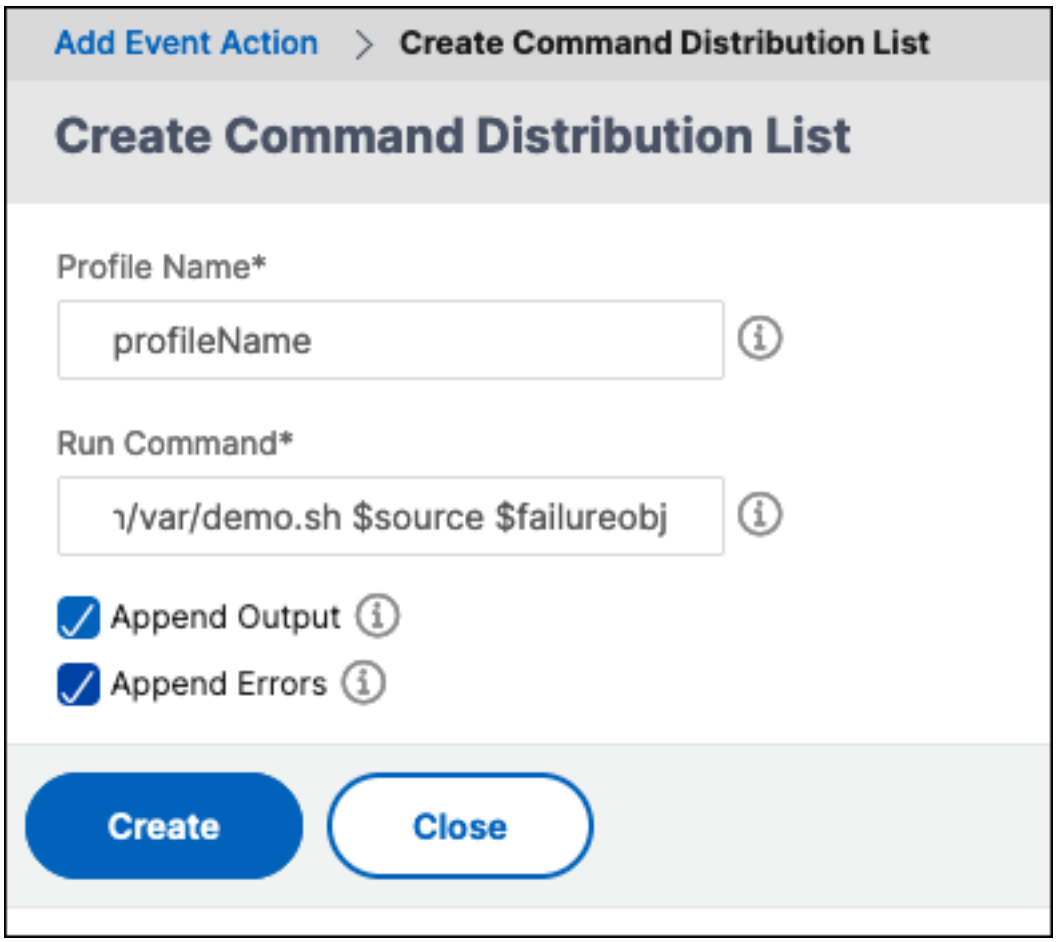
   b) **Ejecute el comando**. Especifique la ubicación del agente en la que debe ejecutarse el script. Por ejemplo: sh/var/demo.sh $source $failureobj.

   c) Seleccione **Anexar salida** y **Anexar errores**

   > **Nota:**
   >
   > Puede habilitar las opciones **Anexar salida** y **Anexar errores** si desea almacenar la salida y los errores generados (si los hay) al ejecutar un script de comandos en los archivos de registro del servidor de NetScaler Console. Si no habilita estas opciones, NetScaler Console descarta todos los resultados y errores generados al ejecutar el script de comandos.

   d) Haga clic en **Crear**.

2. En la página **Agregar acción de evento**, haga clic en **Aceptar**.



> **Nota:**
>
> Puede habilitar las opciones **Anexar salida** y **Anexar errores** si desea almacenar la salida y los errores generados (si los hay) al ejecutar un script de comandos en los archivos de registro del servidor de NetScaler Console. Si no habilita estas opciones, NetScaler Console descarta todos los resultados y errores generados al ejecutar el script de comandos.

Ejecutar acción de trabajo

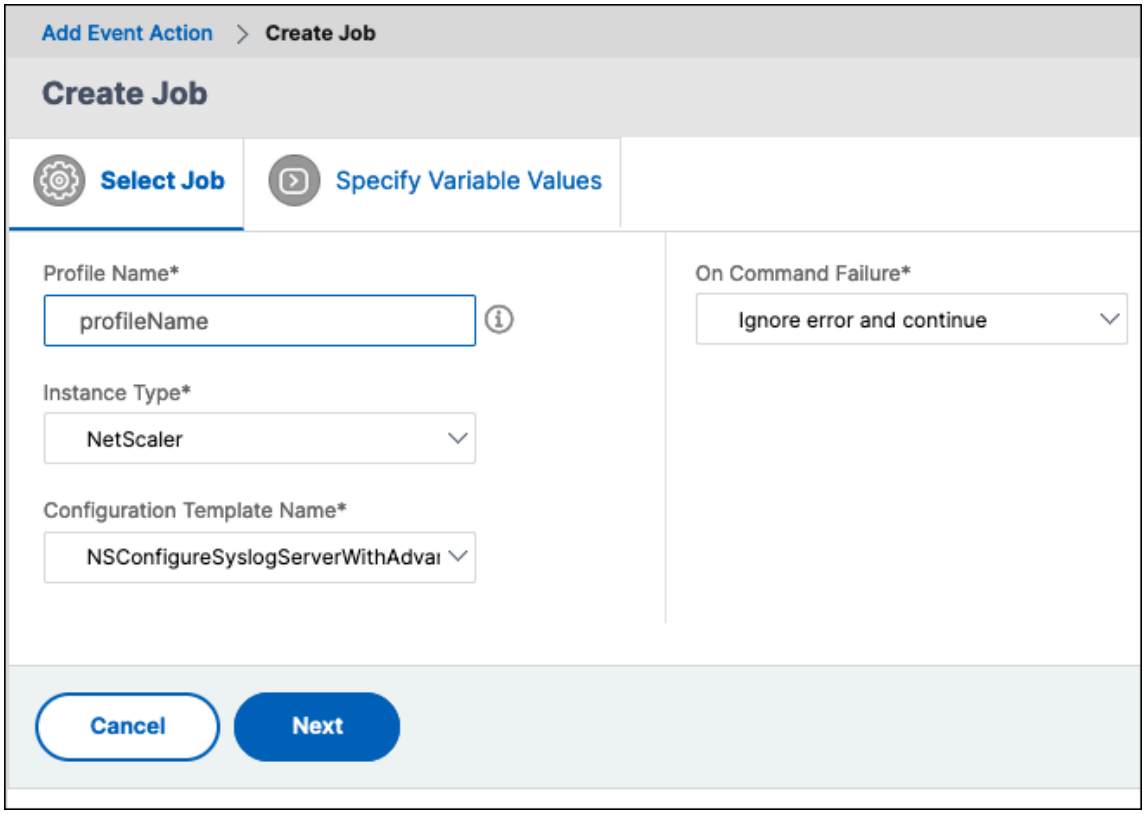
Al crear un perfil con trabajos de configuración, un trabajo se ejecuta como un trabajo integrado o personalizado para NetScaler, y las instancias SDX de NetScaler para eventos y alarmas que coinciden con los criterios de filtro que ha especificado.

1. En **Lista de perfiles de trabajo**, seleccione un perfil de trabajo. Para agregar una lista, haga clic en **Agregar**.
2. En la página **Crear trabajo**, haga lo siguiente:
    a) **Seleccione Trabajo**. Cree un perfil con un trabajo que quiera ejecutar cuando los eventos cumplan con los criterios de filtro definidos. 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.

b) **Especifique los valores de las variables**. En función del tipo de instancia seleccionado y de la plantilla de configuración elegida, especifique los valores de las variables.

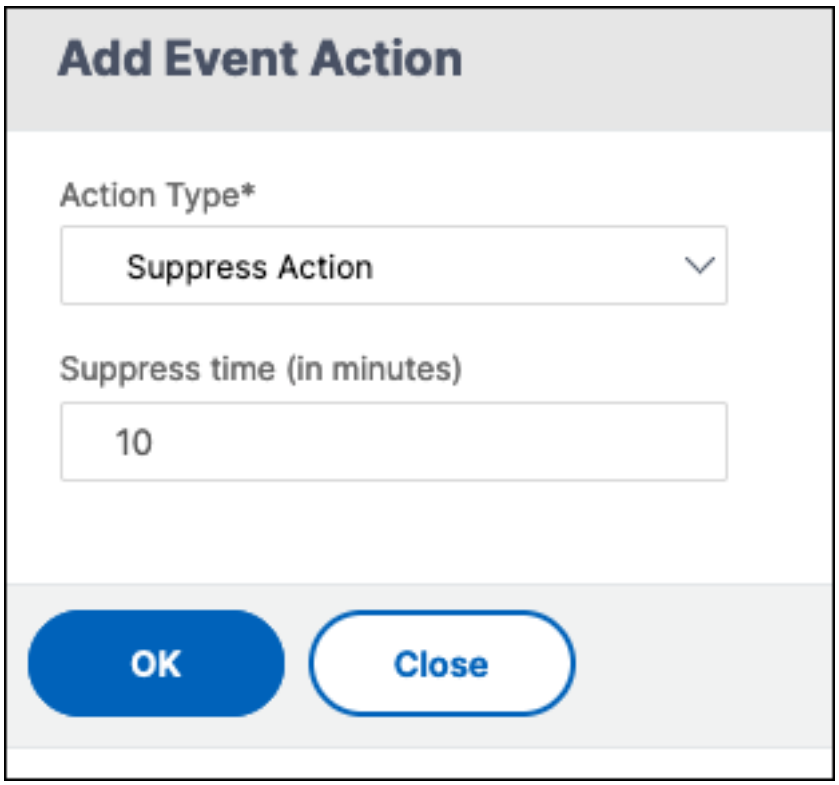
c) Haga clic en **Finalizar** para crear el trabajo.



3. Haga clic en **Aceptar**.

Acción de supresión

- En **Tiempo de supresión**, introduzca un período de tiempo, en minutos, para el que 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, NetScaler Console considera que el tiempo de supresión es cero y nunca caduca.

Enviar notificaciones de Slack

Cuando configura un canal de Slack, las notificaciones del evento se envían a este canal. Puede configurar muchos canales de Slack para recibir estas notificaciones

1. En la **Lista de perfiles de Slack**, seleccione un perfil de Slack. Para agregar un perfil de Slack, haga clic en **Agregar**.
2. En la página **Crear perfil de Slack** , haga lo siguiente:
    a) **Nombre del perfil**. Escriba un nombre para la lista de perfiles que se configurará en NetScaler Console.
    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**. Escriba la URL del webhook del canal que ha introducido. 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 se envían a esta URL y, a continuación, se publican en el canal de Slack elegido. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK

d) Haga clic en **Crear**.

3. Haga clic en **Aceptar**.

> **Nota:**
>
> También puede agregar los perfiles de Slack desde **Parámetros** > **Notificaciones** > **Perfiles de Slack**. Haga clic en **Agregar** y cree el perfil.

Enviar notificaciones de PagerDuty

Puede añadir un perfil de PagerDuty como opción en NetScaler Console para supervisar las notificaciones de incidentes en función de sus configuraciones de PagerDuty. PagerDuty le permite configurar notificaciones a través de correo electrónico, SMS, notificaciones push y llamadas telefónicas en un número registrado.

1. En la **lista de perfiles de PagerDuty**, seleccione un perfil de PagerDuty. Para agregar un perfil, haga clic en **Agregar**.
2. En la **página Crear perfil de PagerDuty**:
   a) **Nombre del perfil**. Introduzca un nombre de perfil de su elección.
   b) **Clave de integración**. Introduzca la clave de integración.

      Puede obtener la clave de integración en su portal de PagerDuty.
   c) Haga clic en **Crear**.

Antes de agregar un perfil de PagerDuty en NetScaler Console, 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.

Caso de uso:

Considere un escenario en el que quiera:

- Enviar notificaciones a su perfil de PagerDuty.
- Configurar una llamada telefónica como una opción en PagerDuty para recibir notificaciones.
- Recibir alertas de llamadas telefónicas para eventos de NetScaler.

Cree la configuración de PagerDuty. Una vez finalizada 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

Enviar notificaciones de ServiceNow

Puede generar automáticamente incidentes de ServiceNow para los eventos de NetScaler Console seleccionando el perfil de ServiceNow en la GUI de NetScaler Console. Debe elegir el perfil de **ServiceNow** en NetScaler Console para configurar una regla de eventos.

Antes de configurar una regla de eventos para generar automáticamente los incidentes de ServiceNow, integre la consola de NetScaler con la instancia de ServiceNow. Para obtener más información, consulte Configurar el adaptador ITSM para ServiceNow.

1. En el **perfil de ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.
2. Haga clic en **Aceptar**.

Programar un filtro de eventos

March 6, 2024

Después de crear un filtro para la regla, si no desea que la consola de NetScaler envíe una notificación cada vez que el evento generado cumpla los criterios de filtro, puede programar el filtro para que se active solo en intervalos de tiempo específicos, 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 muchas notificaciones por correo electrónico cuando NetScaler

Console 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 Console:

1. En la consola de NetScaler, 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.
    - **Intervalo de tiempo programado (horas)** : horas en las que programar la regla (utilice el formato de 24 horas).
4. Haga clic en **Programar**.

Modificar la gravedad reportada de los eventos que se producen en instancias de NetScaler

January 26, 2024

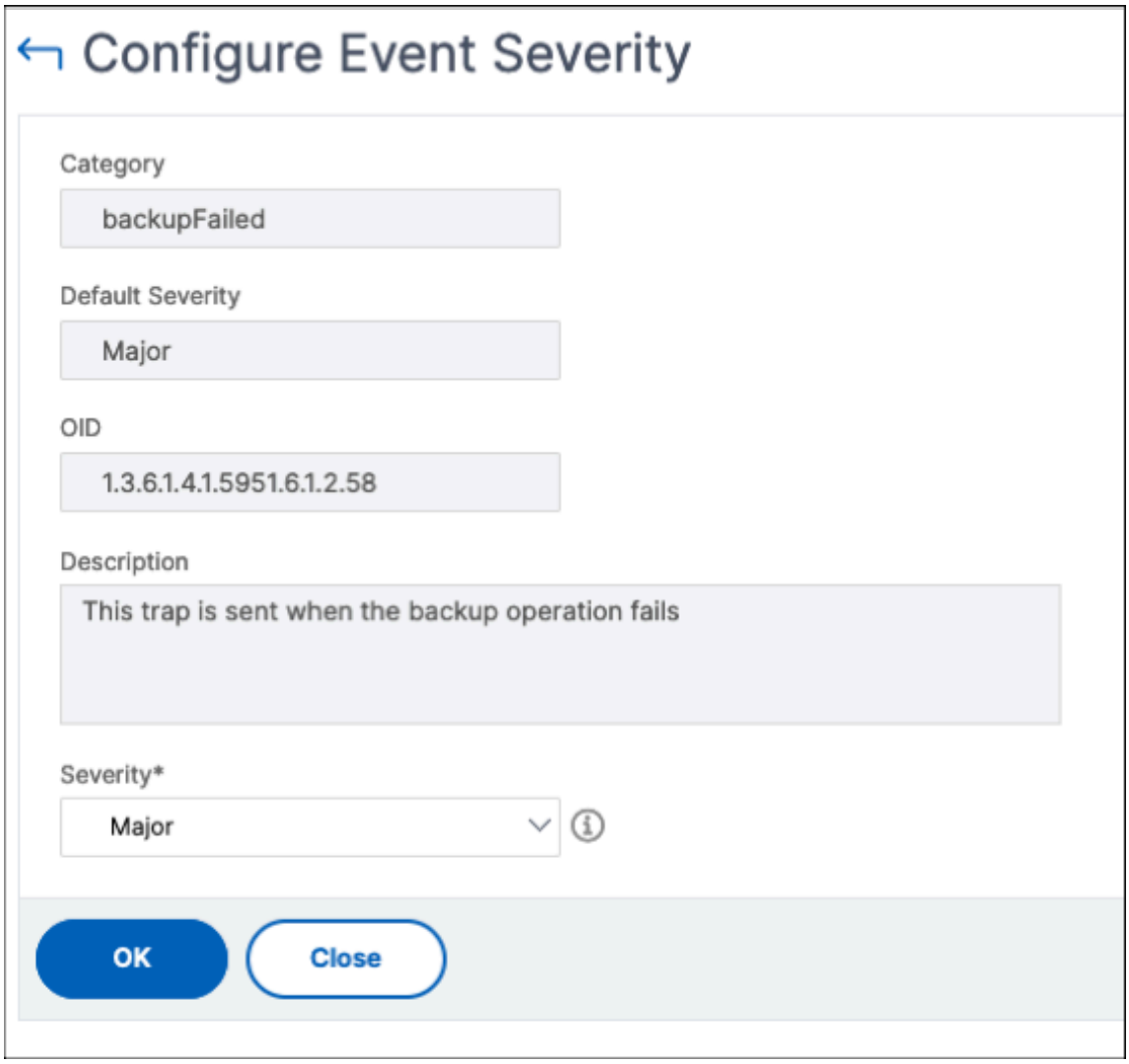
Puede administrar la generación de informes de eventos generados en todos los dispositivos, de modo que pueda ver los detalles de un evento concreto en una instancia y ver los informes en función de la gravedad del evento. Además, puede crear reglas de eventos que utilicen la configuración de gravedad 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 NetScaler que quiera 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**.



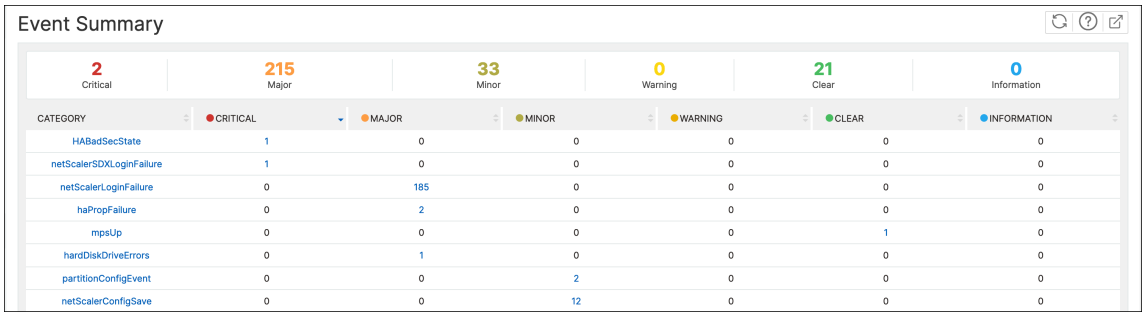
Ver resumen de eventos

March 6, 2024

Ahora puede ver una página de resumen de eventos para supervisar los eventos y las trampas recibidos en la consola de NetScaler. Vaya a **Infraestructura > Eventos** . La página Resumen de Eventos muestra la siguiente información en formato de tabla:

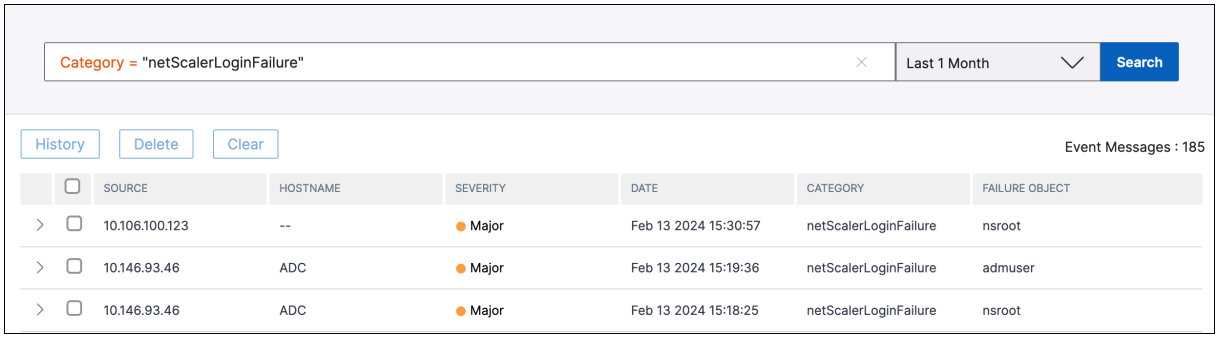
- **Resumen de todos los eventos recibidos por NetScaler Console**. Los eventos se enumeran por categoría y los diferentes niveles de gravedad se muestran en diferentes columnas: Crítico, Mayor, Menor, Advertencia, Claro e Información. Por ejemplo, se produce un evento crítico

cuando una instancia de Citrix Application Delivery Controller (NetScaler) deja de funcionar y deja de enviar información a la consola de NetScaler. 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 que estuvo inactiva, etc. A continuación, el evento se registra en la página Resumen de eventos, en la que puede ver el 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 las instancias de NetScaler a NetScaler Console tiene una gravedad asignada, pero como administrador de red, puede especificar su gravedad en la GUI de NetScaler Console.

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 de host de una 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.



Puede configurar el número de días entre 1 y 40 para los que desea ver los eventos en NetScaler Console. Por ejemplo, si selecciona 30 días, NetScaler Console muestra los eventos de 30 días y, después de 30 días, los eventos se borran. Para configurar este ajuste de eventos, vaya a **Configuración > Configuración global > Directiva de retención de datos**. Para obtener más información, consulte Directiva de retención de datos.

Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

> **Nota:**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona **Periodicidad mensual**, asegúrese de introducir todos los días en los que quiere que se programe el informe separados por comas.

Mostrar severidades de eventos y detalles de capturas SNMP

March 6, 2024

Al crear un evento y su configuración en NetScaler Console, puede ver el evento inmediatamente en la página Resumen del evento. Del mismo modo, puede ver y supervisar el estado, el tiempo de actividad, los modelos y las versiones de todas las instancias de Citrix Application Delivery Controller (NetScaler) agregadas al servidor de NetScaler Console con todo detalle en Infrastructure Dashboard.

En el panel Infraestructura, ahora puede enmascarar valores irrelevantes para que pueda ver y supervisar con más facilidad información como eventos por severidades, estado, tiempo de actividad, modelos y versión de instancias de NetScaler 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. 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 *de fuera de servicio* ya está aplicado, y verá detalles como el nombre del

host, el número de solicitudes HTTP que recibió por segundo, el uso de CPU y otros. También puede seleccionar la instancia y ver el panel de la instancia para obtener más detalles.

Para seleccionar eventos específicos por gravedad en NetScaler Console:

1. Inicie sesión en NetScaler Console con sus credenciales de administrador.
2. Vaya a **Infraestructura > Instancias**.

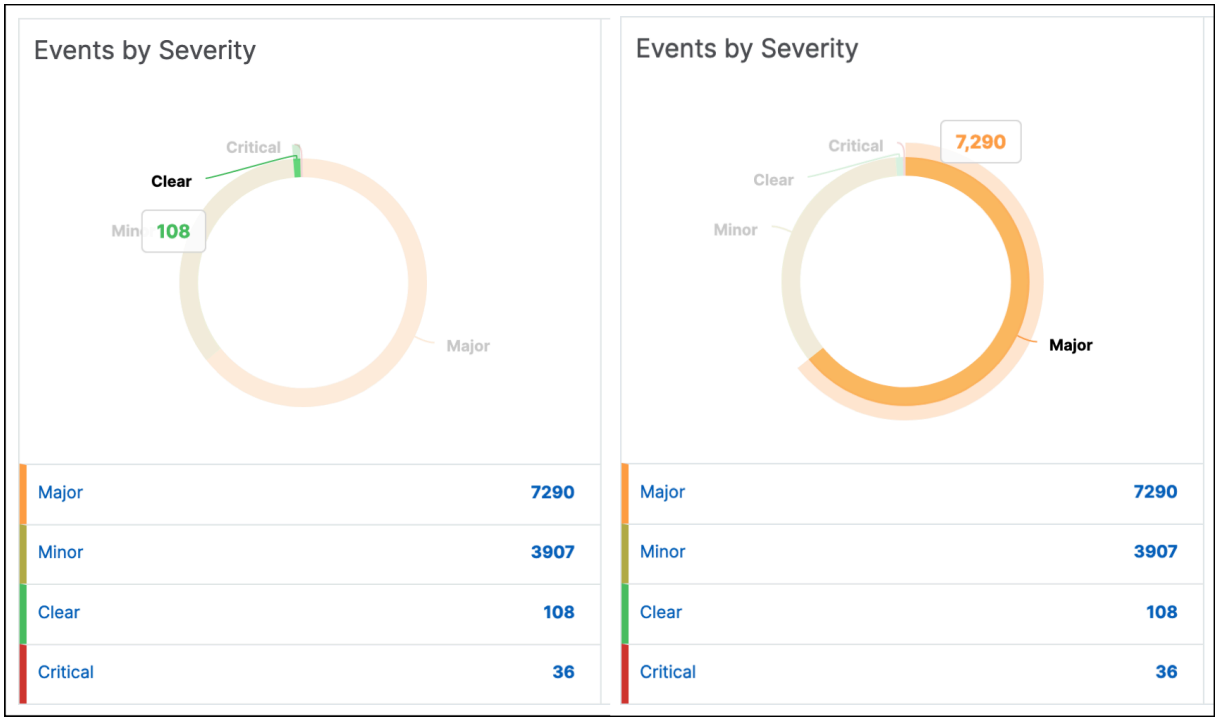
   O bien:

   Vaya a **Infraestructura > Eventos > Informes**.
3. En la lista desplegable de la esquina superior derecha de la página, seleccione la duración para la que quiere ver los eventos por gravedad.

4. El gráfico de anillos de **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 anillos, puede ver una lista de los niveles de gravedad 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. Pase el ratón sobre los tipos de gravedad para ver y supervisar la gravedad elegida con mayor facilidad.

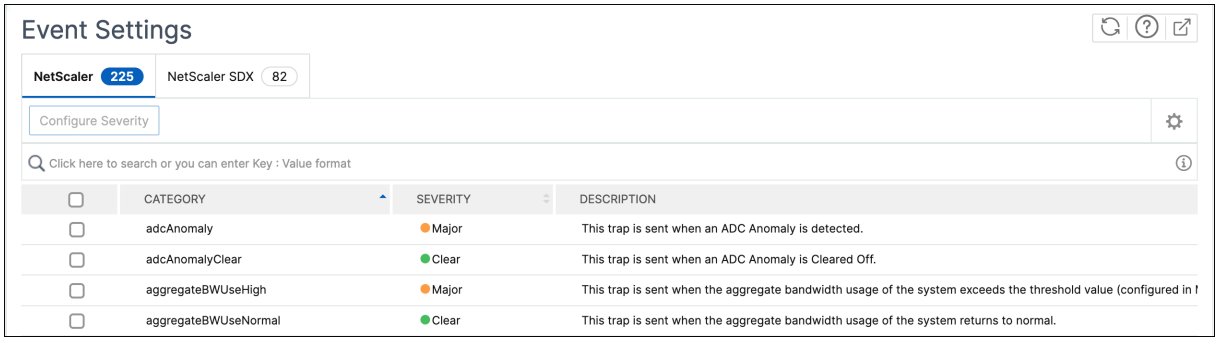


Para ver los detalles de la captura SNMP de NetScaler en NetScaler Console:

Ahora puede ver los detalles de cada captura de SNMP recibida de sus instancias de NetScaler administradas en la consola de NetScaler, en la página de **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 **AggregateBWUseNormal**, la descripción de la captura se muestra como "Esta trampa se envía cuando el uso total del ancho de banda del sistema vuelve a la normalidad".



Ver y exportar mensajes de syslog

July 17, 2024

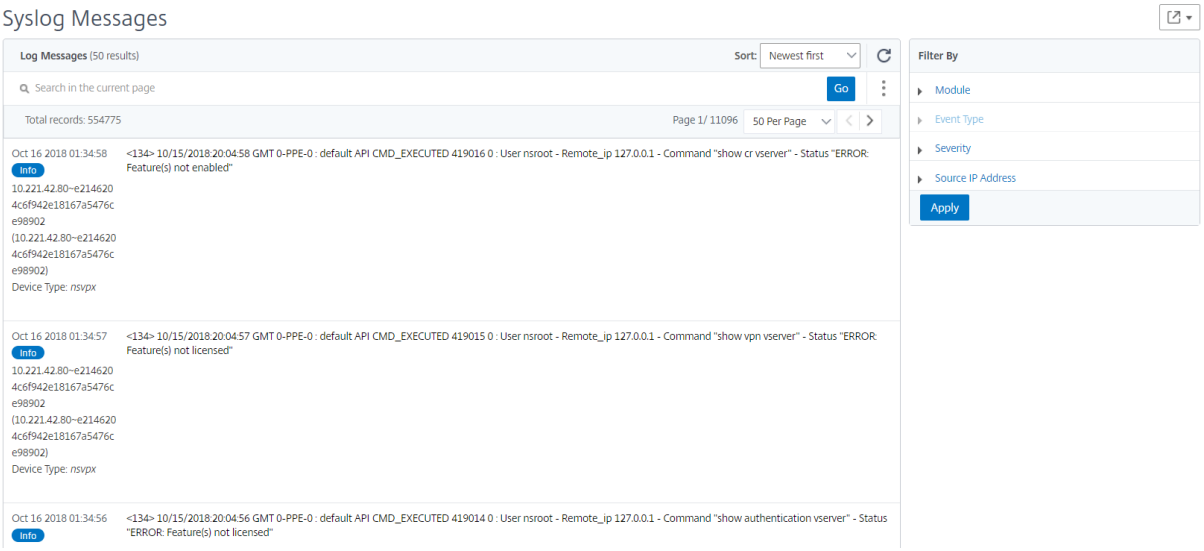
Puede ver los mensajes de syslog sin iniciar sesión en NetScaler Console programando la exportación de todos los mensajes de syslog recibidos en el servidor. Puede exportar los mensajes de syslog que se generan en las instancias de Citrix Application Delivery Controller (NetScaler) en formatos PDF, CSV, PNG y JPEG. Además, puede programar la exportación de estos informes a direcciones de correo electrónico específicas en distintos intervalos.

Ver mensajes de syslog

Puede ver todos los mensajes de syslog generados en las instancias administradas de NetScaler. Para ver los mensajes, debe configurar las instancias para redirigir los mensajes de syslog al servidor de NetScaler Console. Los mensajes de syslog se almacenan en la base de datos de forma centralizada y están disponibles en el visor de syslog con fines de auditoría. Puede combinar esta información de registro y derivar informes para análisis a partir de los datos recopilados.

También puede configurar syslog para registrar diferentes tipos de eventos.

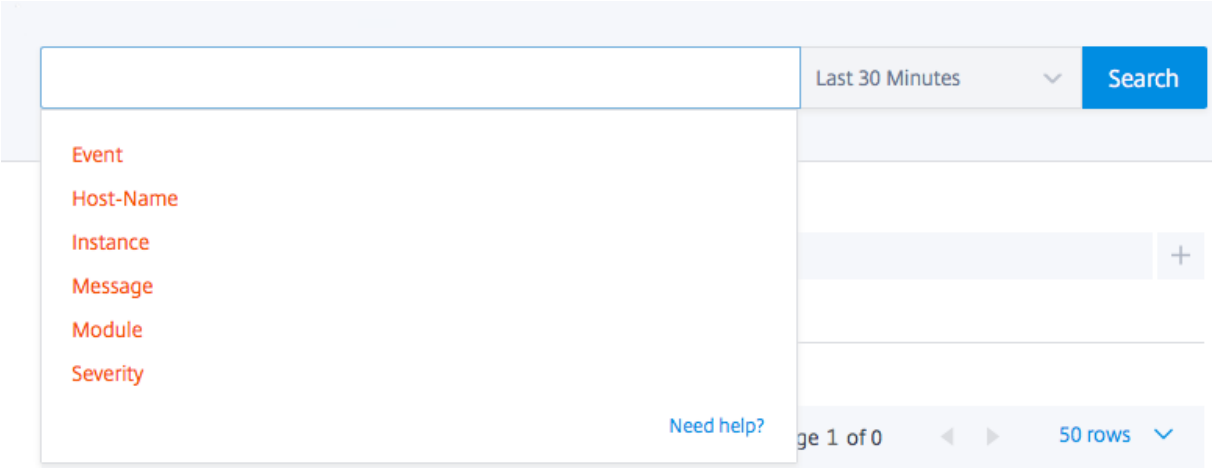
Para ver el visor de Syslog, vaya a **Infraestructura > Eventos > Mensajes de Syslog**. Elija los filtros adecuados para ver los mensajes de registro del sistema.



Buscar mensajes syslog

Puede utilizar filtros para buscar los mensajes de syslog y los mensajes del registro de auditoría a fin de acotar los resultados y encontrar exactamente lo que busca en tiempo real.

Para buscar mensajes de syslog para todas las instancias de NetScaler presentes en el software NetScaler Console, desde la GUI de NetScaler Console, vaya a **Infraestructura > Eventos > Mensajes de Syslog**. Las nuevas categorías de filtros son instancia, módulo, evento, gravedad y mensaje.



Para buscar todos los mensajes de registro de auditoría del sistema de NetScaler Console presentes en el software NetScaler Console, desde la GUI de NetScaler Console, vaya a **Configuración > Mensajes de registro de auditoría**. Las nuevas categorías de filtros son instancia, módulo, evento, gravedad y mensaje.

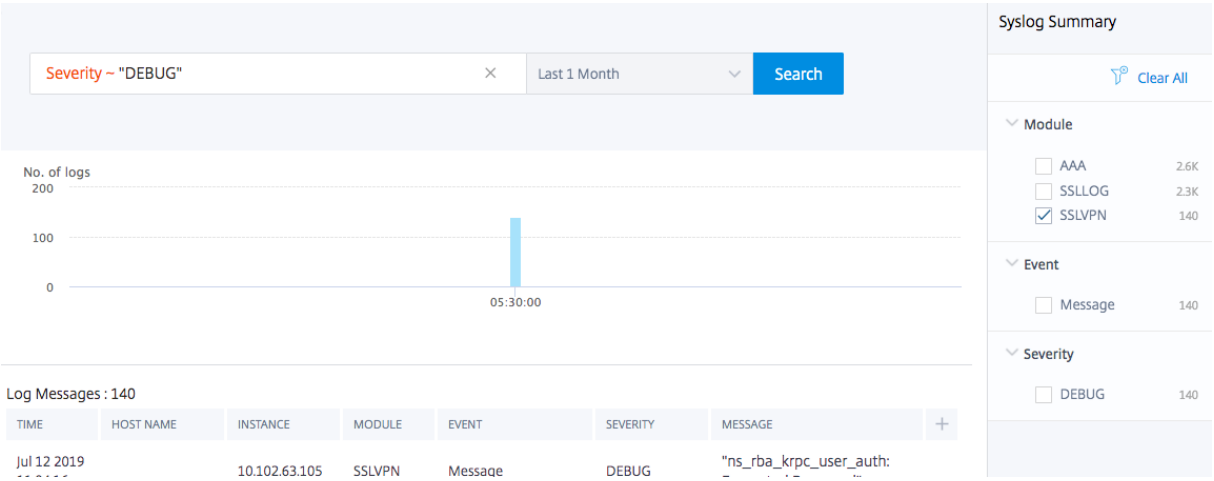
Para buscar los mensajes de registro de auditoría de todas las aplicaciones presentes en NetScaler Console, desde la GUI de NetScaler Console, vaya a **Infraestructura > Funciones de red > Audi-**

toría.

Para buscar los mensajes del registro de auditoría de una aplicación específica en la consola de NetScaler, desde la GUI de NetScaler Console, vaya a **Aplicación > Panel de control** y seleccione el servidor virtual en el que desea buscar los mensajes del registro de auditoría. A continuación, haga clic en la ficha **Registro de auditoría**.

Tras seleccionar una categoría de filtro, especifique si es igual o contiene el término de búsqueda.

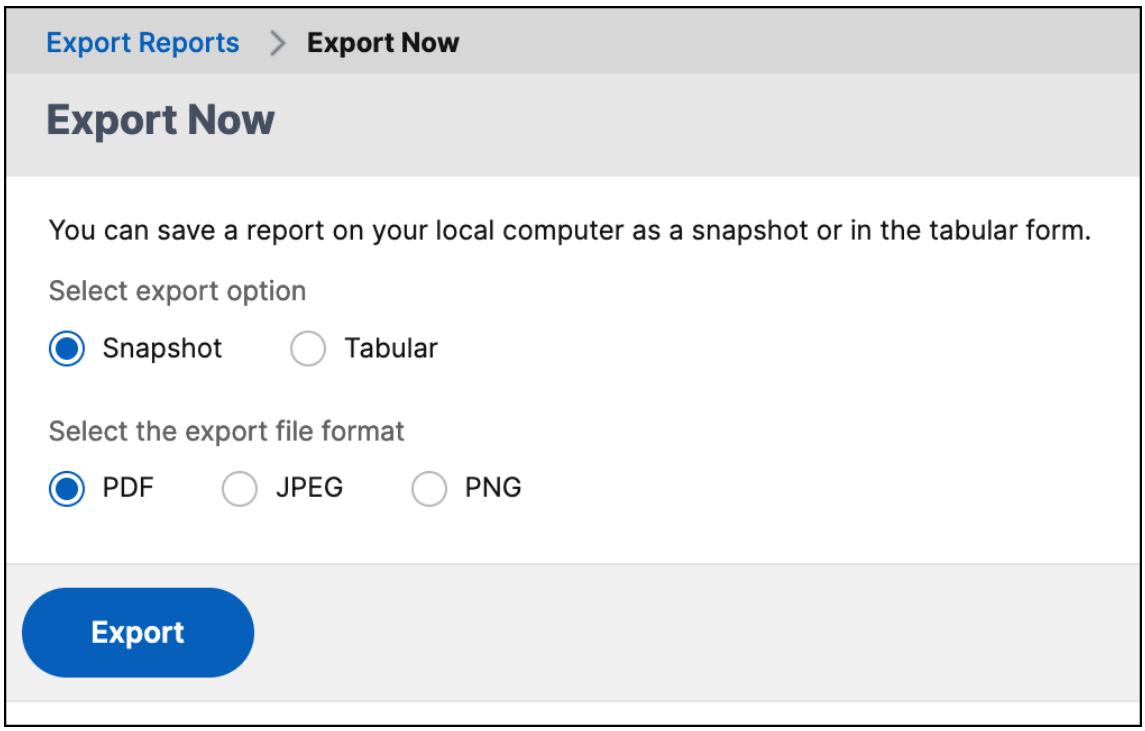
A continuación, agregue el término de búsqueda. Para algunas categorías, se muestra una lista precompletada de términos de búsqueda. De forma predeterminada, el tiempo de búsqueda es de 1 día. Puede cambiar la hora y el intervalo de fechas haciendo clic en la flecha hacia abajo. Puede reducir aún más la búsqueda seleccionando las opciones del panel Resumen de **Syslog o Resumen** del **registro de auditoría**.



Exportar mensajes syslog

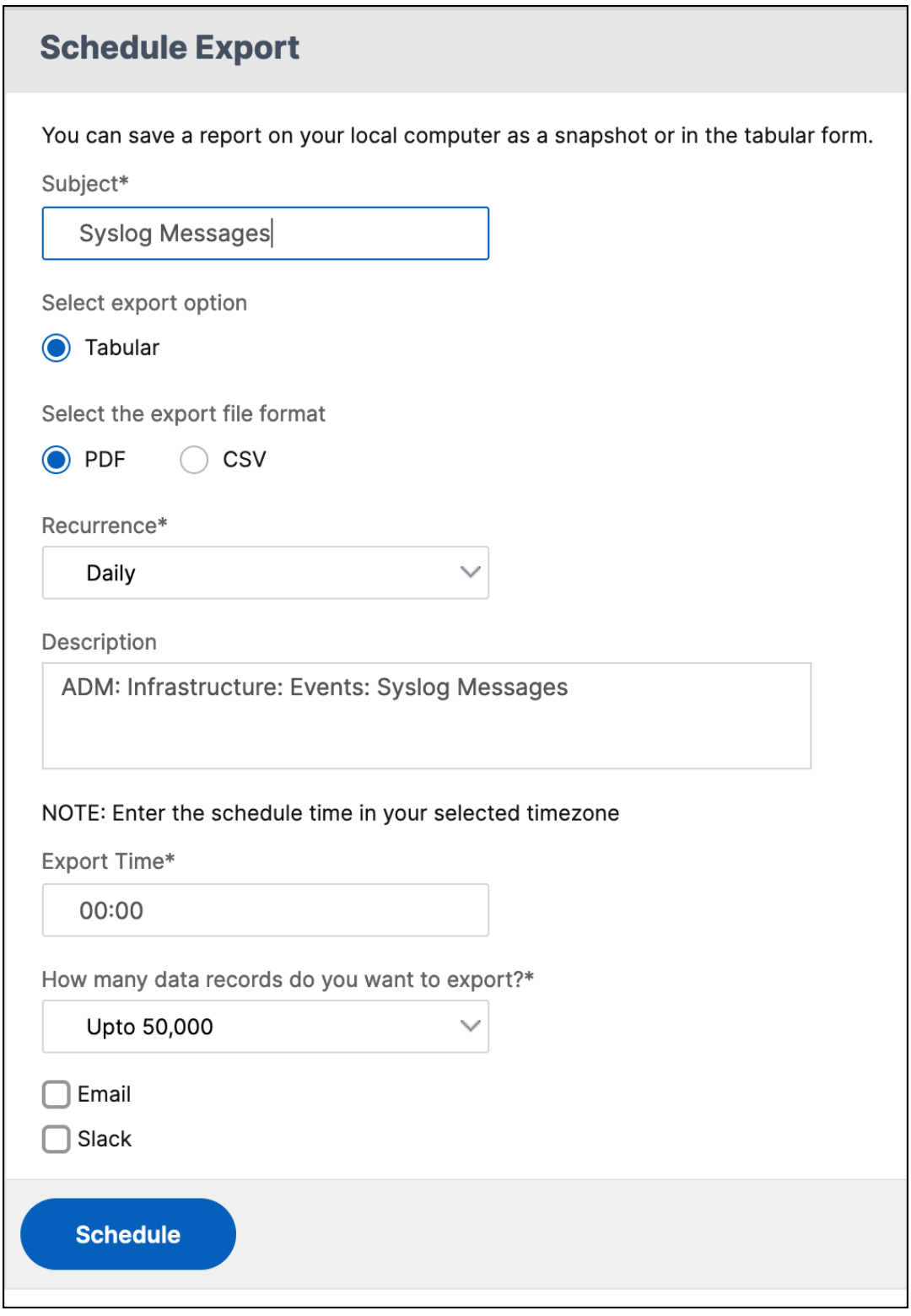
Para exportar un informe de mensajes de syslog mediante NetScaler Console:

1. Vaya a **Infraestructura > Eventos > Mensajes de Syslog**.
2. En el panel derecho, haga clic en el botón Exportar situado en la esquina superior derecha de la página Mensajes de Syslog.
3. En **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.



Para programar la exportación del informe de mensajes de syslog mediante NetScaler Console:

1. Vaya a **Infraestructura > Eventos > Mensajes de Syslog**.
2. En la página **Mensajes de Syslog**, en el panel derecho, haga clic en **Exportar**.
3. En la ficha **Informe de planificación**, defina los siguientes parámetros:
    - **Descripción**: Mensaje que describe el motivo para exportar el informe.
    - **Formato**: formato en el que se va a exportar el informe.
    - **Periodicidad**: intervalo en el que se exporta el informe.
    - **Hora de exportación**: Hora a la que se exporta el informe. Introduzca la hora en un formato de 24 horas para su zona horaria local.
    - **Lista de distribución de correo electrónico**: Lista de destinatarios para recibir el informe por correo electrónico. Elija una lista de distribución de correo electrónico de la lista proporcionada. Un correo electrónico se activa cuando se genera el informe y cumple los criterios de tiempo programados. Si quiere crear una lista de distribución de correo electrónico, haga clic en **+** y proporcione los detalles del servidor de correo y del perfil de correo.



Suprimir mensajes de syslog

July 17, 2024

Cuando se configura como un servidor syslog, NetScaler Console recibe todos los mensajes syslog de las instancias configuradas de Citrix Application Delivery Controller (NetScaler). Es posible que haya muchos mensajes que no quiera ver. Por ejemplo, es posible 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 la consola de NetScaler configurando algunos filtros. NetScaler Console elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de NetScaler Console y tampoco se almacenan en la base de datos de NetScaler Console del cliente.

Puede suprimir algunos de los mensajes de syslog registrados que llegan a NetScaler Console 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 Console busque y suprima los mensajes. NetScaler Console elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de NetScaler Console y tampoco se almacenan en la base de datos de clientes. 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 Console, vaya a **Infraestructura > Eventos Mensajes de Syslog**.
2. Haga clic en el icono de engranaje para abrir la página **Suprimir filtros**.

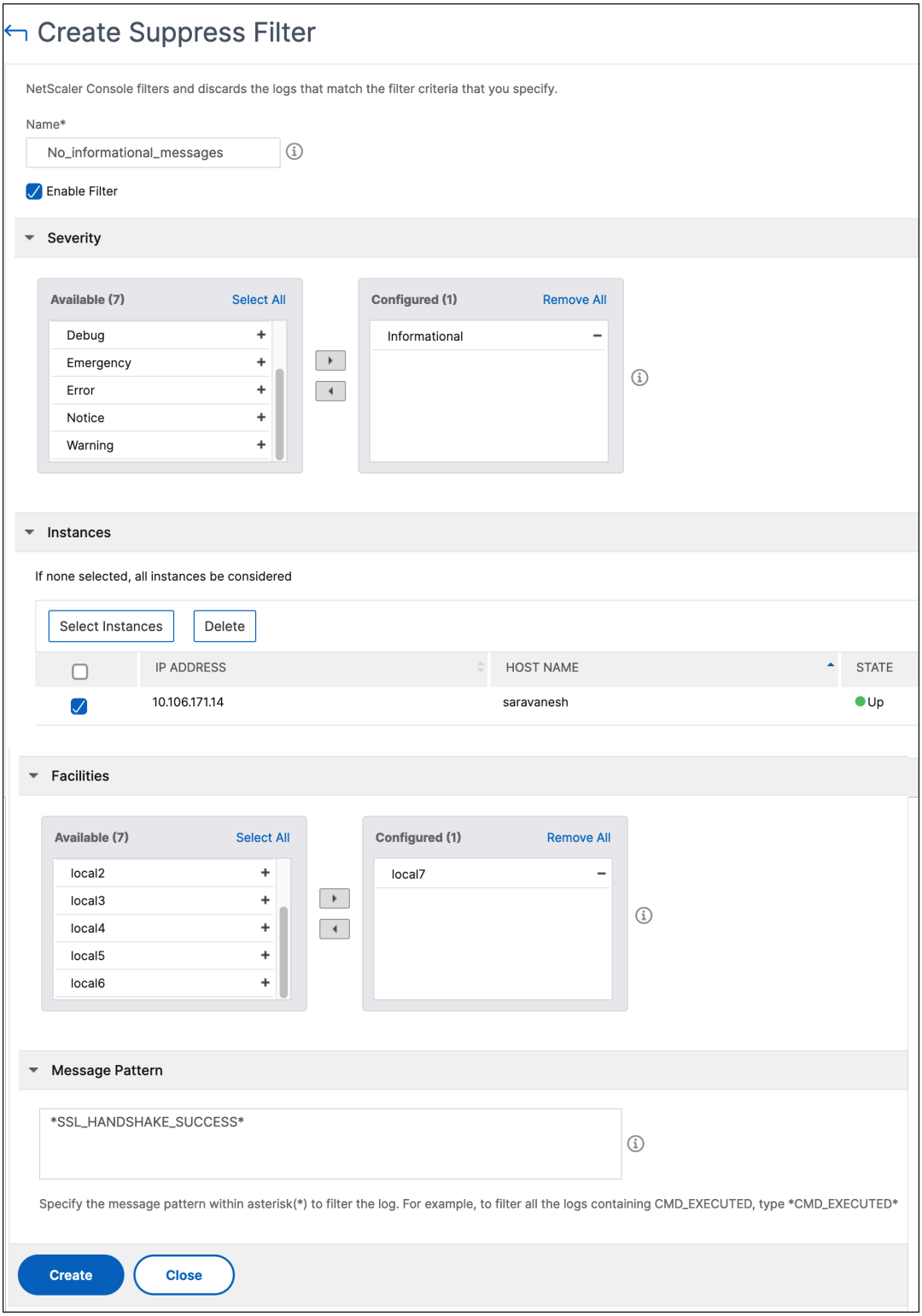
3. En la página **Suprimir filtros**, haga clic en **Agregar**.
4. En **Crear filtro de supresión**, actualice la siguiente información:

    a) **Nombre**: Escriba un nombre para el filtro.

> **Nota:**
>
> Si distintos usuarios tienen un acceso diferente a varias instancias de NetScaler, se deben crear filtros diferentes para las distintas 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 instalación para suprimir los mensajes en función del origen que los genera.

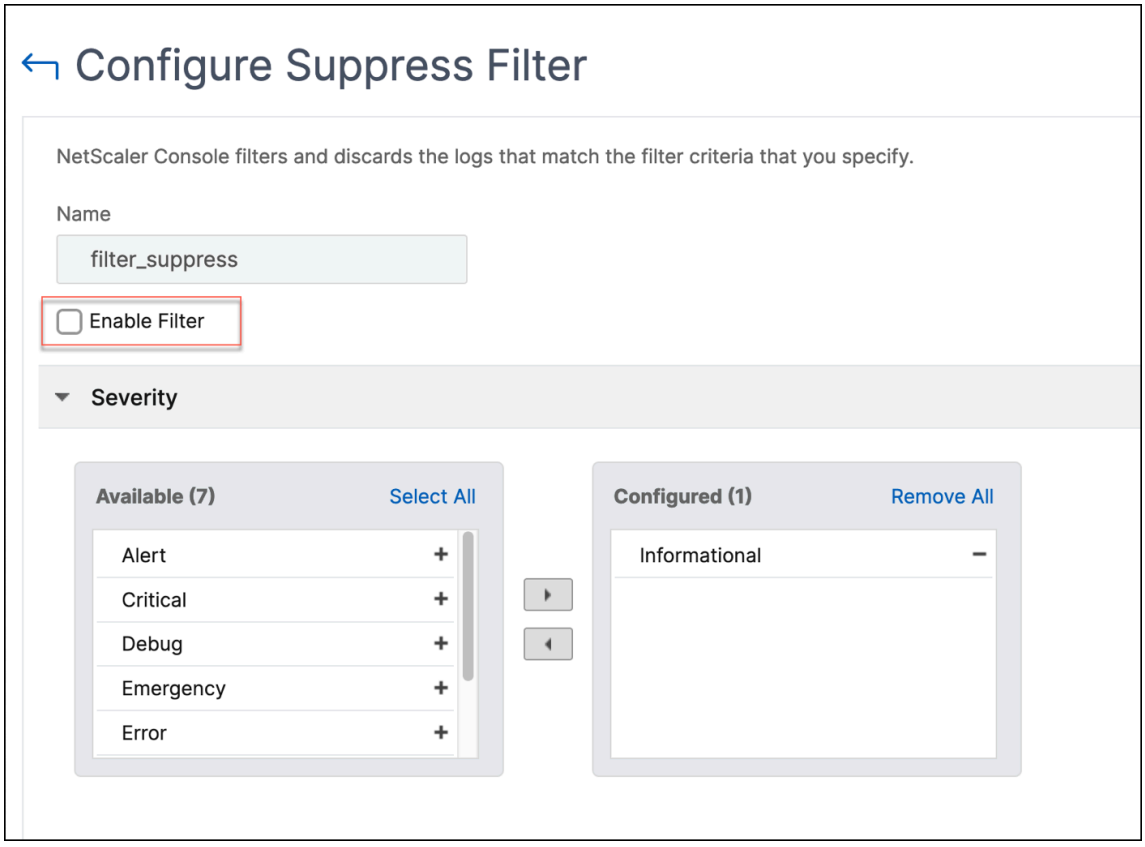
e) **Patrón de mensajes** : también puede escribir un patrón de texto rodeado de asteriscos

(*) 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 Console, debe deshabilitar el filtro.

1. Vaya a **Infraestructura > Eventos > Mensajes de Syslog**.
2. Haga clic en el icono de engranaje para abrir la página **Suprimir filtros**.
3. En la página **Suprimir filtros**, seleccione el filtro y haga clic en **Modificar**.
4. En la página **Configurar suprimir filtro**, desactive la casilla **Activar filtro** para inhabilitar el filtro.



Tablero SSL

May 9, 2024

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

Un certificado Secure Socket Layer (SSL), que forma parte de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. El certificado tiene un componente de clave pública visible para cualquier cliente que quiera iniciar una transacción segura con el servidor. La clave privada correspondiente, que reside de forma segura en el dispositivo NetScaler, se utiliza para completar el cifrado y descifrado de clave asimétrica (o clave pública).

Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

- De una autoridad de certificación autorizada (CA)
- Al generar un nuevo certificado SSL y una clave en el dispositivo NetScaler

NetScaler Console proporciona una vista centralizada de los certificados SSL instalados en todas las instancias de NetScaler administradas. En el panel de control de SSL, puede ver gráficos que le ayudan a rastrear los emisores de certificados, los puntos fuertes clave, los algoritmos de firma, los certificados caducados o no utilizados, etc. También puede ver la distribución de los protocolos SSL que se ejecutan en sus servidores virtuales y las claves que están habilitadas en ellos.

También puede configurar notificaciones para informarle cuando los certificados están a punto de caducar e incluir información sobre las instancias NetScaler que utilizan dichos certificados.

Puede vincular un certificado de instancia de NetScaler a un certificado de CA. Sin embargo, asegúrese de que los certificados que vincula al mismo certificado de CA tengan la misma fuente y el mismo emisor. Después de vincular uno o más certificados a un certificado de CA, puede desvincularlos.

> **Nota:**
>
> También puede usar un servidor Venafi Trust Protection Platform con NetScaler Console para automatizar la administración de todo el ciclo de vida de los certificados SSL. Para obtener más información, consulte Automatizar la administración de certificados SSL.

Usar el panel de mandos de SSL

May 9, 2024

Puede usar el panel de certificados SSL de NetScaler Console 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:

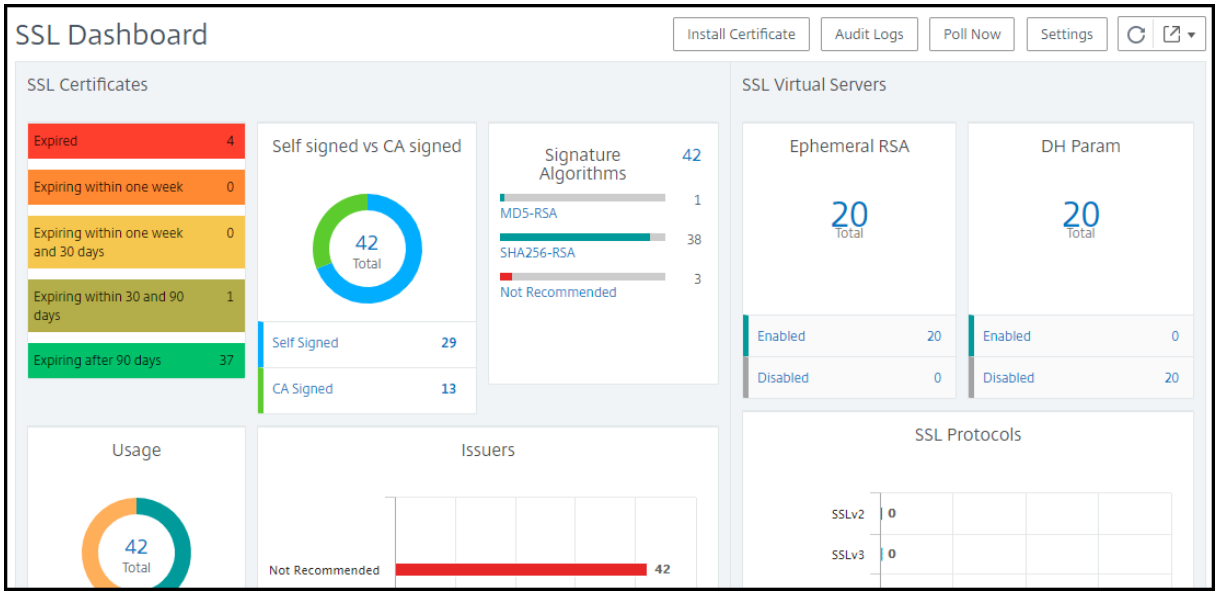
- Número de días después de los cuales caducan los certificados
- Número de certificados usados y no utilizados
- Número de certificados autofirmados y firmados por una CA
- Número de emisores
- algoritmos de firma
- Protocolos SSL
- Las 10 instancias principales por número de certificados en uso

Supervisar certificados SSL

Utilice el panel de control SSL de NetScaler Console para supervisar sus certificados si su empresa tiene una política de SSL en la que ha definido ciertos requisitos para los certificados SSL, como que todos los certificados deben tener un nivel mínimo de claves de 2048 bits y una autoridad de CA de confianza debe autorizarlos.

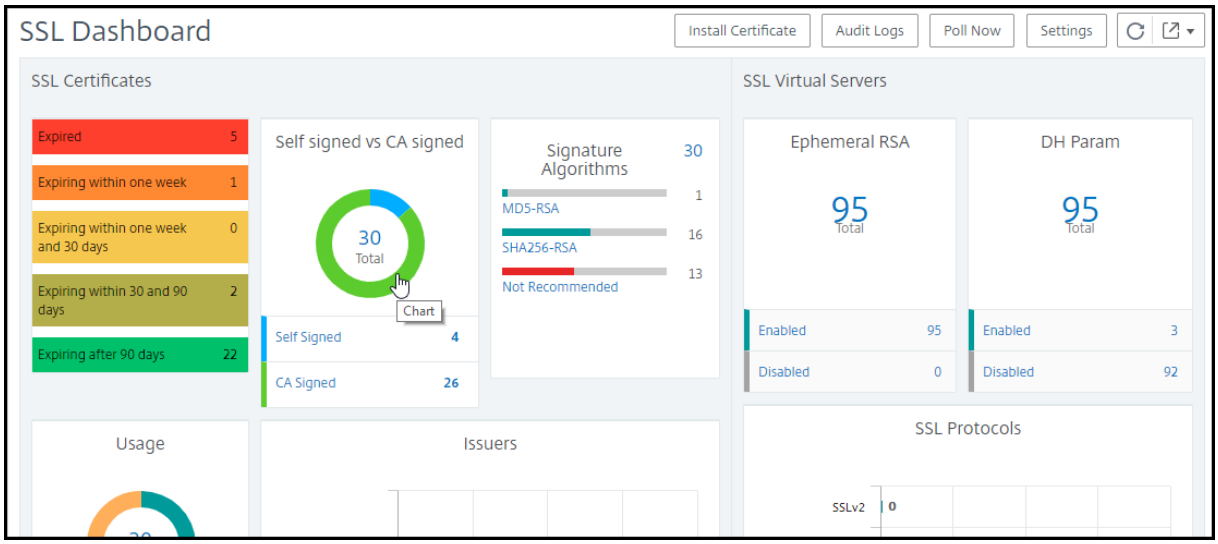
En otro ejemplo, es posible que haya subido un certificado nuevo pero haya olvidado vincularlo a un servidor virtual. El panel de control SSL resalta los certificados SSL que se están utilizando o no. En la sección **Uso**, puede ver el número de certificados que se han instalado y el número de certificados que se están utilizando. También 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 Console, vaya a **Infraestructura > Panel de control SSL**.

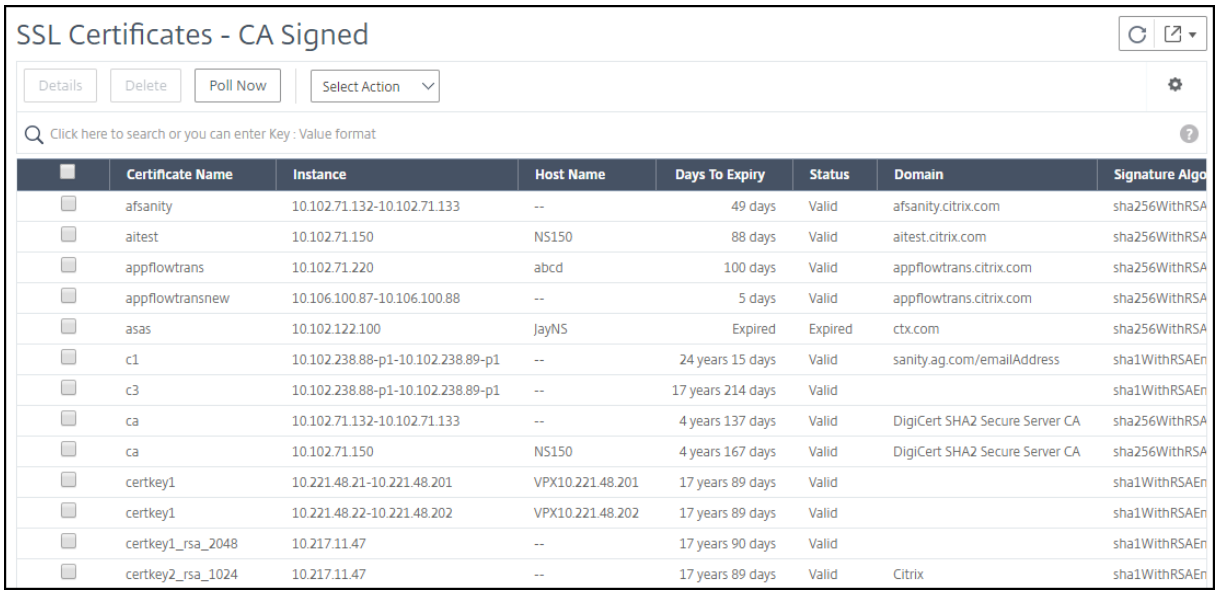


NetScaler Console le permite sondear los certificados SSL y añadir todos los certificados SSL de las instancias inmediatamente a NetScaler Console. Para hacerlo, vaya a **Infraestructura > Panel de control SSL** y haga clic en **Sondear ahora**. Aparece la página **Encuesta ahora**, que presenta la opción de sondear todas las instancias de NetScaler en la red o sondear las instancias seleccionadas.

Puede usar el panel SSL de NetScaler Console para ver o supervisar los detalles de los certificados SSL, los servidores virtuales SSL y los protocolos SSL. Los números son hipervínculos en los que puede hacer clic para mostrar detalles relacionados con los certificados SSL, los servidores virtuales SSL o los protocolos SSL.



Por ejemplo, cuando un usuario hace clic en el número 30 en **Autofirmado frente a CA inició**sesión en la figura anterior y aparece una nueva ventana que muestra los detalles de los 30 certificados SSL de las instancias de NetScaler.

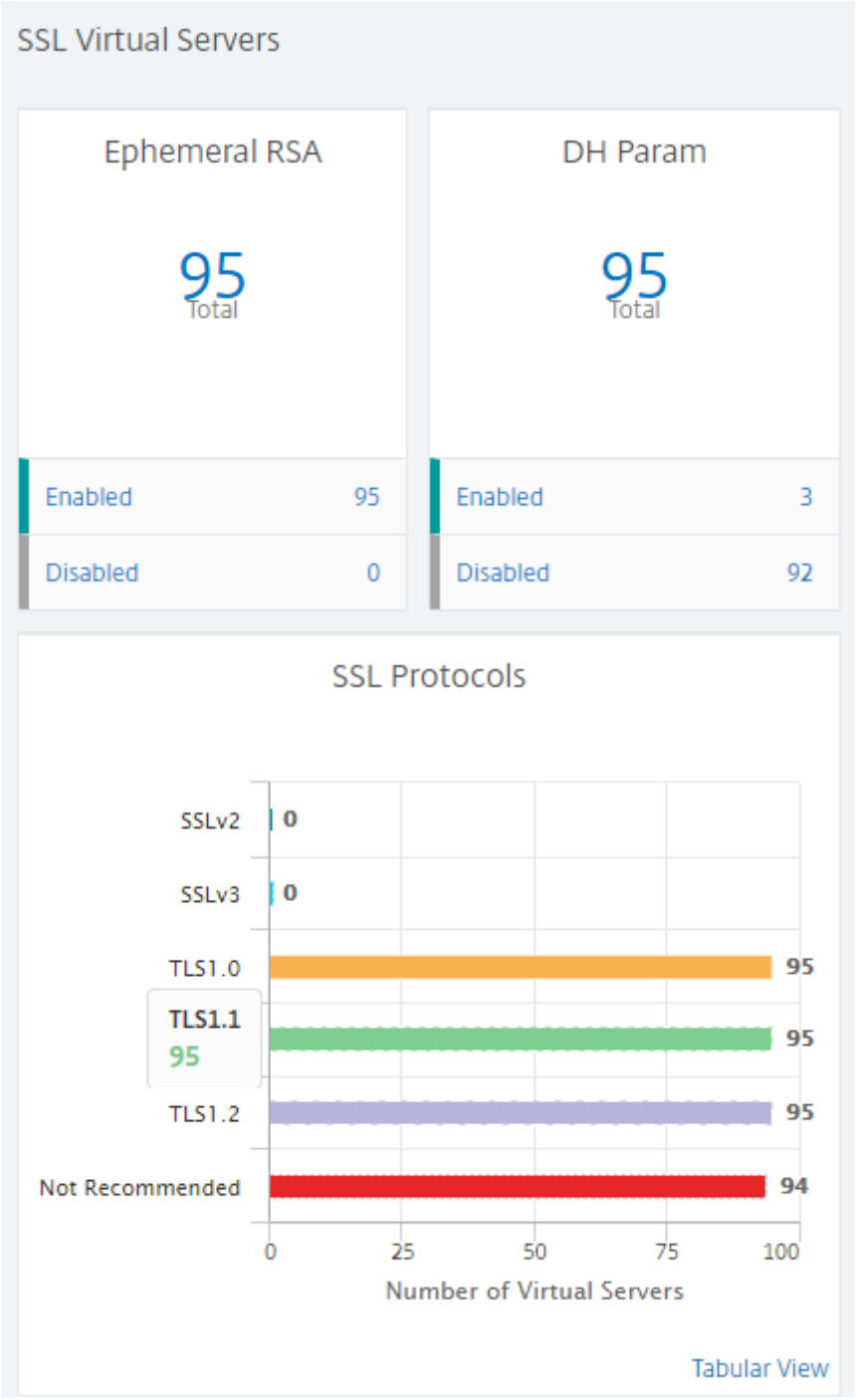


Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

El panel SSL de NetScaler Console también muestra la distribución de los protocolos SSL que se eje-

cutan en sus 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 compatibles son SSLv2, SSLv3, TLS1.0, TLS1.1 y TLS1.2. Los protocolos SSL utilizados en servidores virtuales aparecen en formato de gráfico de barras. Al hacer clic en un protocolo específico, se muestra una lista de servidores virtuales que utilizan ese protocolo.

Aparece un gráfico de anillos después de habilitar o 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.



Ver registros de auditoría de certificados SSL

Ahora puede ver los detalles de registro de los certificados SSL en NetScaler Console. Los detalles del registro muestran las operaciones realizadas con certificados SSL en NetScaler Console, como instalar certificados SSL, vincular y desvincular certificados SSL, actualizar certificados SSL y eliminar certificados SSL. La información del registro de auditoría es útil para supervisar los cambios en los

certificados SSL realizados en una aplicación con varios propietarios.

Para ver un registro de auditoría de una operación concreta realizada en NetScaler Console con certificados SSL, vaya a **Infraestructura > Panel de control SSL** y seleccione Registros de **auditoría**.

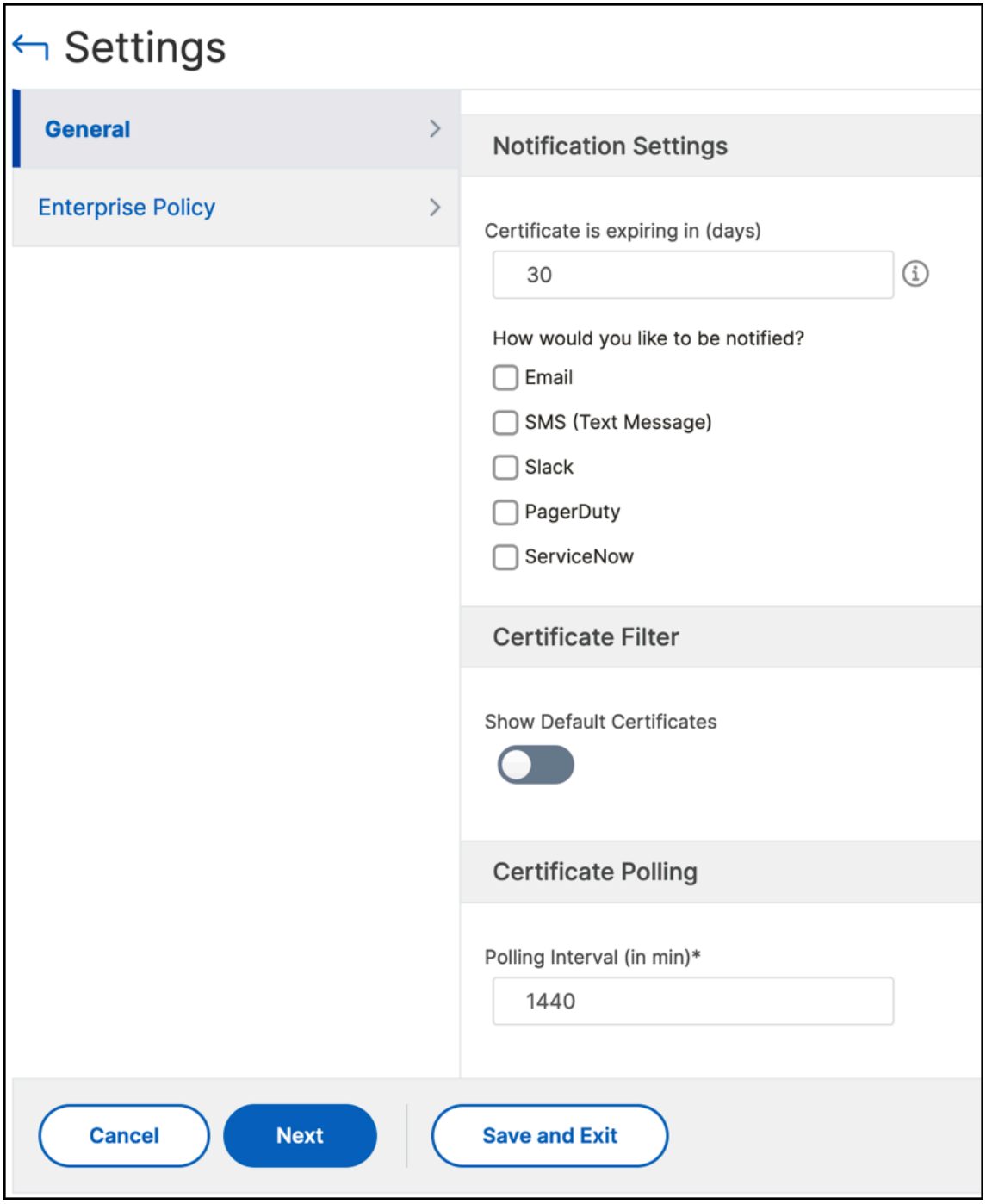
Para una operación concreta realizada con el certificado SSL, puede ver su estado, hora de inicio y hora de finalización. Además, puede ver la instancia en la que se realizó la operación y los comandos ejecutados en esa instancia.

Excluir certificados NetScaler predeterminados en el panel SSL

NetScaler Console le permite mostrar u ocultar los certificados predeterminados que aparecen en los gráficos del panel de control SSL 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 de control SSL** en la GUI de NetScaler Console.
2. En la página **Tablero de SSL**, haga clic en **Configuración**.
3. En la página **Configuración**, seleccione **General**.
4. En la sección **Filtro de certificados**, inhabilite **Mostrar certificados predeterminados** y seleccione **Guardar y salir**.



Descargar certificados SSL

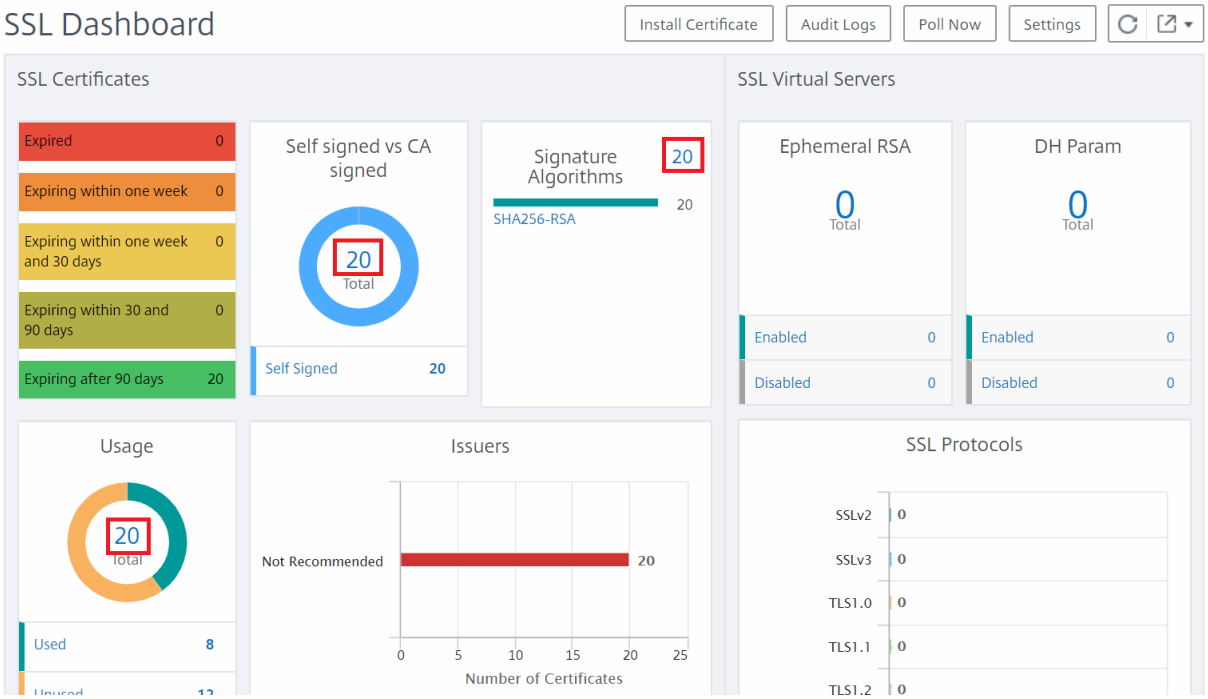
Los certificados SSL se deben administrar de forma individual por instancia. NetScaler Console proporciona visibilidad de todos los certificados implementados en varias instancias.

- Puede seleccionar los certificados que caducan y automatizar las renovaciones de certificados.

- Las directivas se pueden establecer y aplicar en torno a los tipos de certificados y autoridades de firma permitidos.
- También puede descargar los certificados SSL para su renovación y cargarlos más tarde.

Para descargar certificados SSL:

1. Vaya a **Infraestructura > Panel de control SSL** en la GUI de NetScaler Console.
2. En la página **Panel de SSL**, haga clic en el número total de certificados SSL en cualquiera de los gráficos.



1. En la página **Certificados SSL** , haz clic en el certificado que deseas descargar. Por ejemplo, quieres descargar el que caduca en la próxima semana.
2. En el cuadro de lista **Seleccionar acción**, selecciona **Descargar**.
   El certificado se descarga en su sistema.

Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

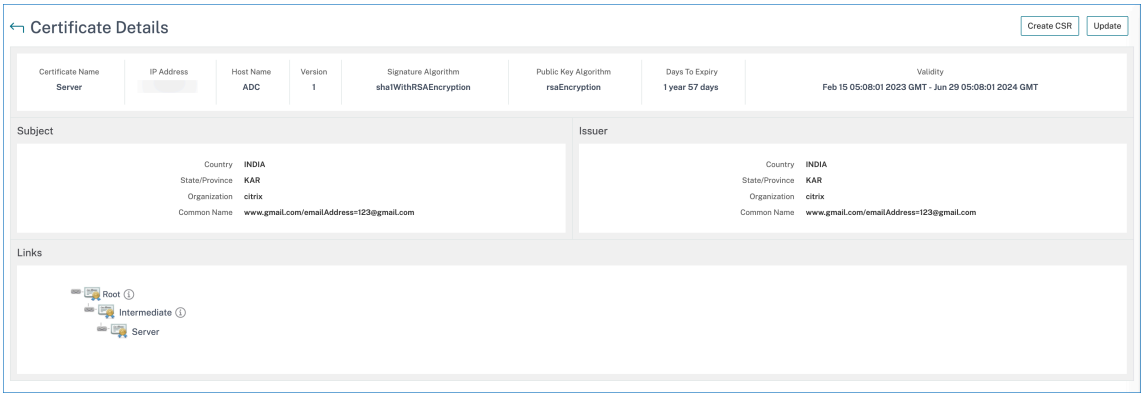
> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona **Periodicidad mensual**, asegúrese de introducir todos los días en los que quiere que se programe el informe separados por comas.

Ver cadena de certificados SSL

Puede ver la cadena completa de enlaces de un certificado, incluidos los certificados intermedios hasta el certificado de 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

May 9, 2024

Como administrador de seguridad, puede configurar las notificaciones cuando los certificados estén a punto de caducar e incluir información sobre qué instancias de NetScaler 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 las notificaciones desde NetScaler Console:

1. En NetScaler Console, vaya a **Infraestructura > Panel de control SSL**.
2. En la página **Tablero de SSL**, haga clic en **Configuración**.
3. En la página **Configuración**, haga clic en **General**.
4. En la sección **Configuración de notificaciones**, especifique cuándo 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. 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.
   - **Slack**: especifica un perfil de Slack. Se envía una notificación cuando los certificados están a punto de caducar.
   - **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 el adaptador ITSM de Citrix Cloud esté configurado para ServiceNow y esté integrado con NetScaler Console. Para obtener más información, consulte Integrar la consola de NetScaler con la instancia de ServiceNow.
6. Haga clic en **Guardar y salir**.

Actualizar un certificado instalado

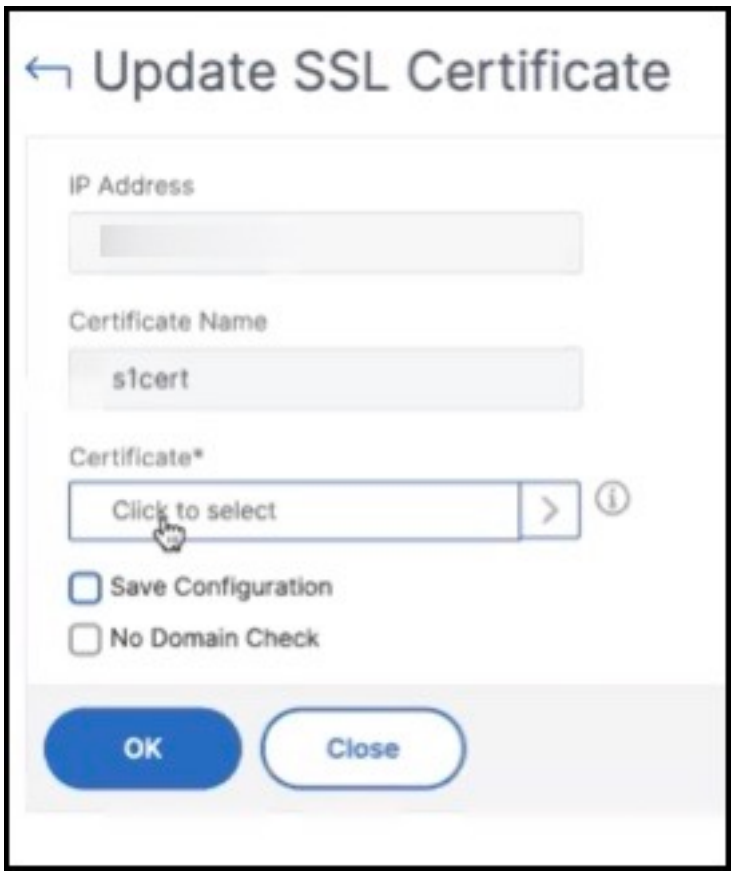
January 26, 2024

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 Console con los certificados del almacén de certificados.

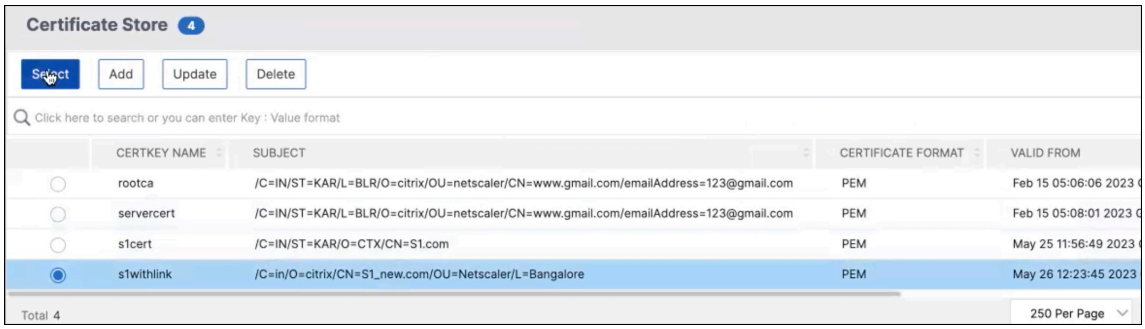
Para actualizar un certificado SSL desde NetScaler Console:

1. En NetScaler Console, vaya a **Infraestructura > Panel de control SSL**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.

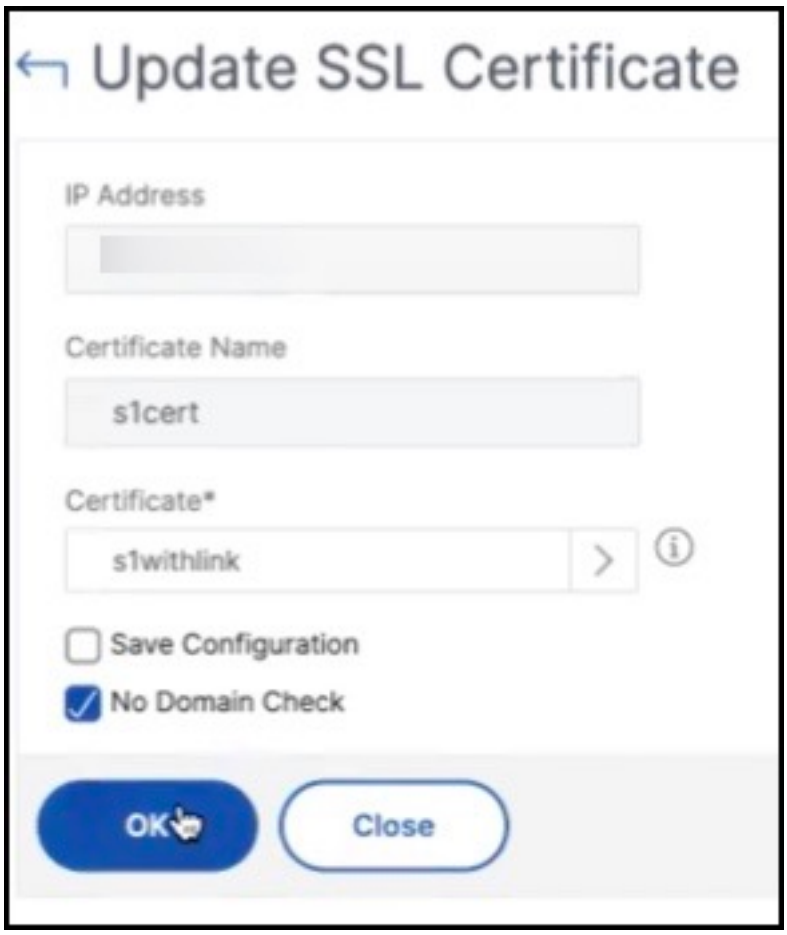
3. En la página **Certificados SSL**, seleccione un certificado y haga clic en **Actualizar**. También puede hacer clic en el certificado SSL para ver sus detalles y, a continuación, haga clic en **Actualizar** en la esquina superior derecha de la página **Certificado SSL**.
4. En la página **Actualizar certificado SSL**, seleccione **Certificado** para mostrar la página **Almacén** de certificados.



5. En la página **Almacén de certificados**, seleccione el archivo de certificado que desee agregar. Haga clic en **Seleccionar**.

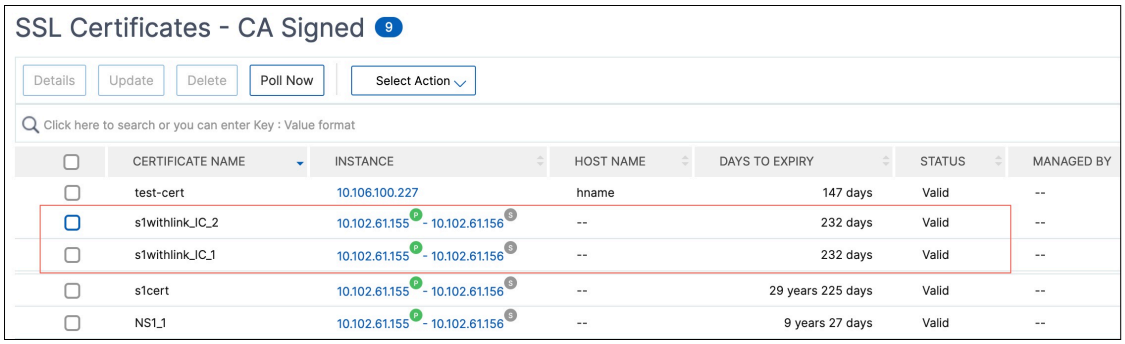


6. Si el nombre de dominio del nuevo certificado no coincide con el certificado anterior y desea que el servidor aloje el nuevo dominio, seleccione **Sin comprobación de dominio**.

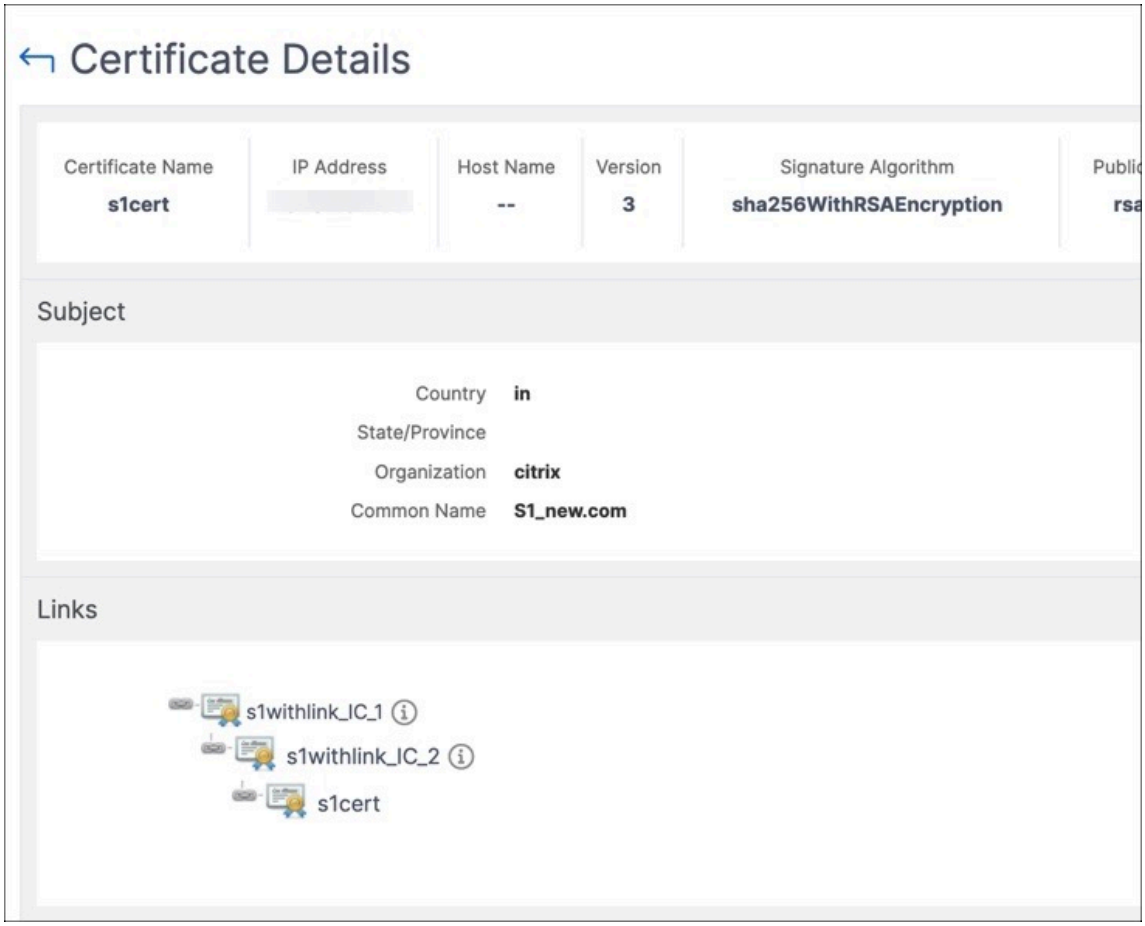


Haga clic en **Aceptar**. Todos los servidores virtuales SSL a los que está vinculado este certificado se actualizan automáticamente.

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

May 9, 2024

Antes de instalar certificados SSL en instancias NetScaler, asegúrese de que los certificados sean emitidos por CA de confianza. Además, asegúrese de que la intensidad de clave de las claves de certificado sea 2.048 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 elegida y aplicarlo a otras instancias de NetScaler específicas desde la GUI de NetScaler Console.

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 del certificado

Seleccione la opción **Importar desde una 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.

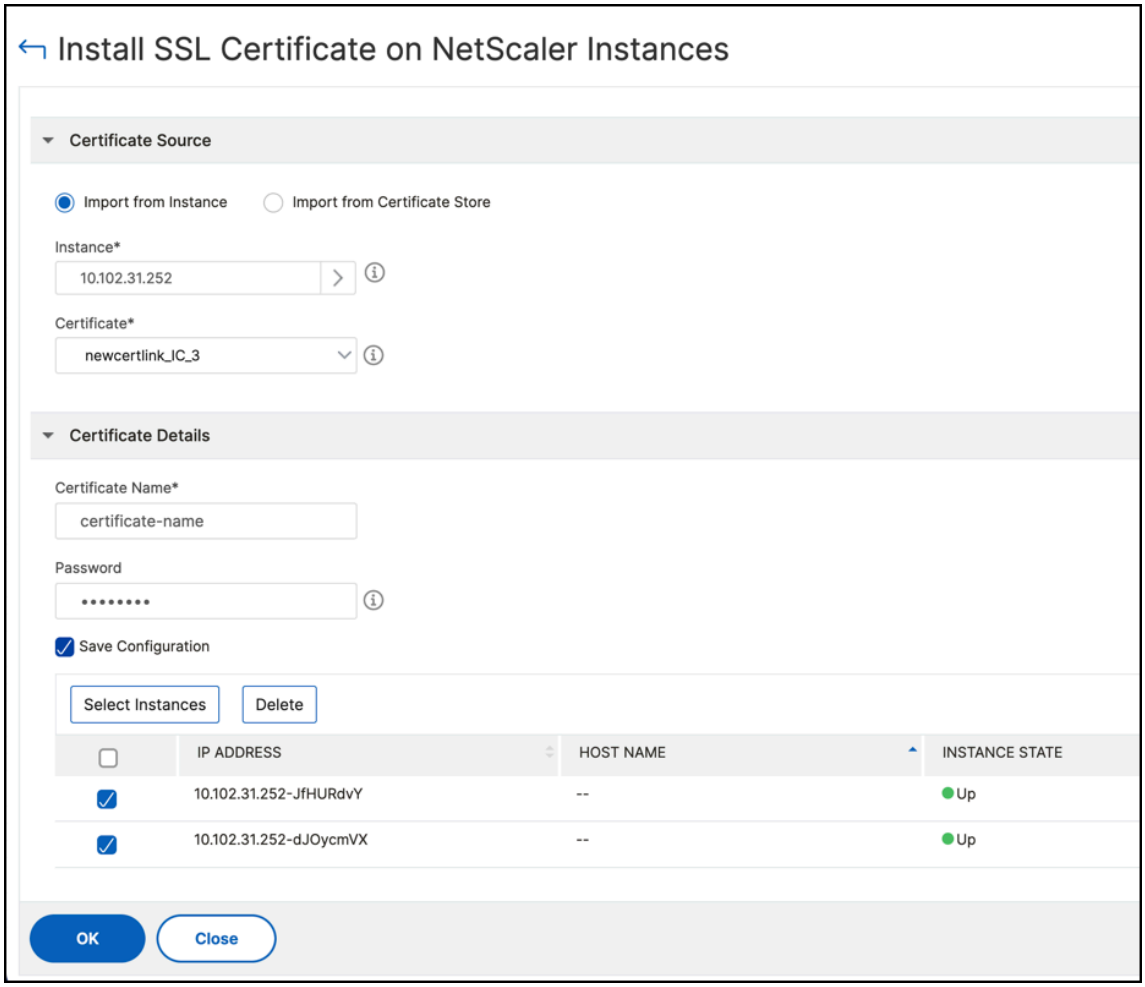
4. Haga clic en **Seleccionar instancias** para seleccionar las instancias de NetScaler en las que quiere instalar sus certificados.
5. Haga clic en Aceptar.

Para instalar un certificado SSL desde NetScaler Console:

1. Vaya a **Infraestructura > Panel de control SSL**.
2. En la esquina superior derecha del panel de control, haga clic en **Instalar certificado**.
3. En la página **Instalar certificado SSL en NetScaler Instance**, especifique los siguientes parámetros:

   - **Archivo de certificado** : cargue un archivo de certificado SSL seleccionando **Local** (su máquina local) o **Dispositivo** (el archivo de certificado debe estar presente en la instancia de NetScaler).
   - **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 en las que quiere instalar sus 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)

May 9, 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 incluida en el certificado, como el nombre de la organización, el nombre común (nombre de dominio), la localidad y el país.

Para crear una CSR con NetScaler Console:

1. En NetScaler Console, vaya a **Infraestructura > Panel de control SSL**.
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 desplegable **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 **Dispositivo**(el archivo de claves debe estar presente en la instancia virtual de NetScaler Console).
   - **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 selecciona este algoritmo, debe proporcionar una frase de contraseña PEM.
Contraseña PEM	Si ha elegido el algoritmo de codificación PEM, introduzca una contraseña.
Confirmar contraseña PEM	Confirme su 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>
```

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 26, 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 quiere 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 Console:

1. En NetScaler Console, vaya a **Infraestructura > Panel de control SSL**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Seleccione el certificado que quiere vincular y, a continuación, seleccione **Vincular** en la lista desplegable **Seleccionar 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 Console:

1. En NetScaler Console, vaya a **Infraestructura > Panel de control SSL**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Elija uno de los certificados vinculados que están vinculados y, a continuación, seleccione **Desvincular** en la lista desplegable **Seleccionar 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

August 8, 2024

Puede configurar una política empresarial y agregar todas las CA de confianza, algoritmos de firma seguros y seleccionar la fortaleza de clave recomendada para sus claves de certificado en NetScaler Console. Si alguno de los certificados instalados en su instancia de NetScaler no se ha agregado a la directiva empresarial, 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 política empresarial en NetScaler Console:

1. En NetScaler Console, vaya a **Infraestructura > Panel de control SSL** y, a continuación, haga clic en **Configuración**.
2. En la página **Configuración**, haga clic en el icono **Directiva de empresa** para agregar todas las CA de confianza, algoritmos de firma seguros y seleccione la intensidad de clave recomendada para sus certificados y claves. Los niveles de clave admitidos son 512, 1024, 2048, 3072 y 4096 bits.
    - **Fortalezas de clave recomendadas** : denota la seguridad del algoritmo y el número de bits en una clave.
    - **Algoritmos de firma recomendados** : denota los problemas de tokens firmados para las aplicaciones.
    - **CA de confianza recomendada** : indica la entidad de confianza que emite los certificados digitales. Haga clic en el icono **+** para agregar más entidades.
    - **Protocolos SSL recomendados** : denota las versiones TLS/SSL.
3. Haga clic en **Finalizar** o **Guardar y salir** 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

May 9, 2024

NetScaler Console sondea automáticamente los certificados SSL una vez cada 24 horas mediante llamadas NITRO y el protocolo Secure Copy (SCP). También puede sondear manualmente los certificados SSL para descubrir los certificados SSL recién agregados en las instancias de NetScaler. 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. Vaya a **Infraestructura > Panel de control 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 SLL de todas las instancias de NetScaler, seleccione la ficha **Todas las instancias** y haga clic en **Iniciar sondeo**.
4. Para sondear instancias específicas, seleccione la ficha **Seleccionar instancias**, seleccione las instancias de la lista y haga clic en **Sondear ahora**.

Usar el almacén de certificados de NetScaler Console para administrar los certificados SSL

June 7, 2024

El almacén de certificados de NetScaler Console le ayuda a almacenar y administrar sus certificados SSL en un solo lugar. 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 **Eliminar**.
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 de NetScaler**.

2. En la página **Importar certificados de NetScaler**, puede seleccionar una de las siguientes fichas:

    - **Importar certificados de NetScaler**: 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 de NetScaler** 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.

Trabajos de configuración

January 26, 2024

El proceso de administración de la configuración de NetScaler Console garantiza la replicación adecuada de los cambios de configuración, las actualizaciones del sistema y otras actividades de mantenimiento en varias instancias de NetScaler de la red.

NetScaler Console le permite crear trabajos de configuración que le ayudan 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 y las convierte en una sola tarea en NetScaler Console. 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 Console. 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. Para obtener más información, consulte Cómo usar la plantilla de configuración maestra en NetScaler Console .

> **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.

Para obtener más información, consulte Cómo utilizar plantillas de configuración para crear plantillas de auditoría

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 Console. 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. Esta actualización 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. Al ejecutar el trabajo, los cambios en el ns.conf de la instancia seleccionada se registran y se copian en NetScaler Console. Consulte Cómo utilizar la función de grabación y reproducción para crear trabajos de configuración.

Exportar el informe de este panel

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

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

Crear un trabajo de configuración

January 26, 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. Puede replicar las configuraciones en varias instancias de la red y grabar y reproducir las tareas de configuración mediante la GUI de NetScaler Console y convertirla en comandos de la CLI.

Puede usar la función Trabajos de configuración de NetScaler Console 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 Console:

1. Vaya a **Infraestructura > Configuración > 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 plantilla Deploy Master Configuration Job por primera vez, agrega una plantilla

> de diferente tipo y, entonces, toda la plantilla de trabajo pasa a ser un tipo de configuración maestra.

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 **Vista** previa de 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.

   b) Haga clic en **Agregar instancias** y seleccione las instancias de la lista. Haga clic en **Aceptar**.

   c) Haga clic en **Siguiente**.

6. 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 y, a continuación, cargue el archivo en el servidor de NetScaler Console.

b) Introduzca valores comunes para las variables que ha definido para todas las instancias.

c) Haga clic en **Siguiente**.

7. Evalúe y verifique los comandos que se ejecutarán en cada instancia en la ficha **Vista previa del trabajo**. Esta ficha también muestra los comandos de reversión si se especifica en la ficha **Seleccionar configuración**.

8. En la ficha **Ejecutar**, elija ejecutar el trabajo ahora o programar para ejecutar el trabajo más tarde.

   Además, seleccione una de las siguientes acciones de la lista Al **fallar un comando** que NetScaler Console debe realizar si se produce un error en el comando:

   - **Ignorar el error y continuar**: NetScaler Console ignora el comando fallido y ejecuta los comandos restantes de la instancia seleccionada.

     > **Nota**
     >
     > Esta acción no permite anular un trabajo de configuración en curso.

   - **Detener la ejecución**posterior : NetScaler Console detiene los comandos restantes si algún comando falla durante la ejecución.
   - **Revertir comandos**correctos : NetScaler Console restaura los comandos ejecutados correctamente si algún comando falla durante la ejecución.

     Si la reversión personalizada está habilitada, la consola de NetScaler ejecuta los comandos de reversión correspondientes a los comandos fallidos.

9. 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.

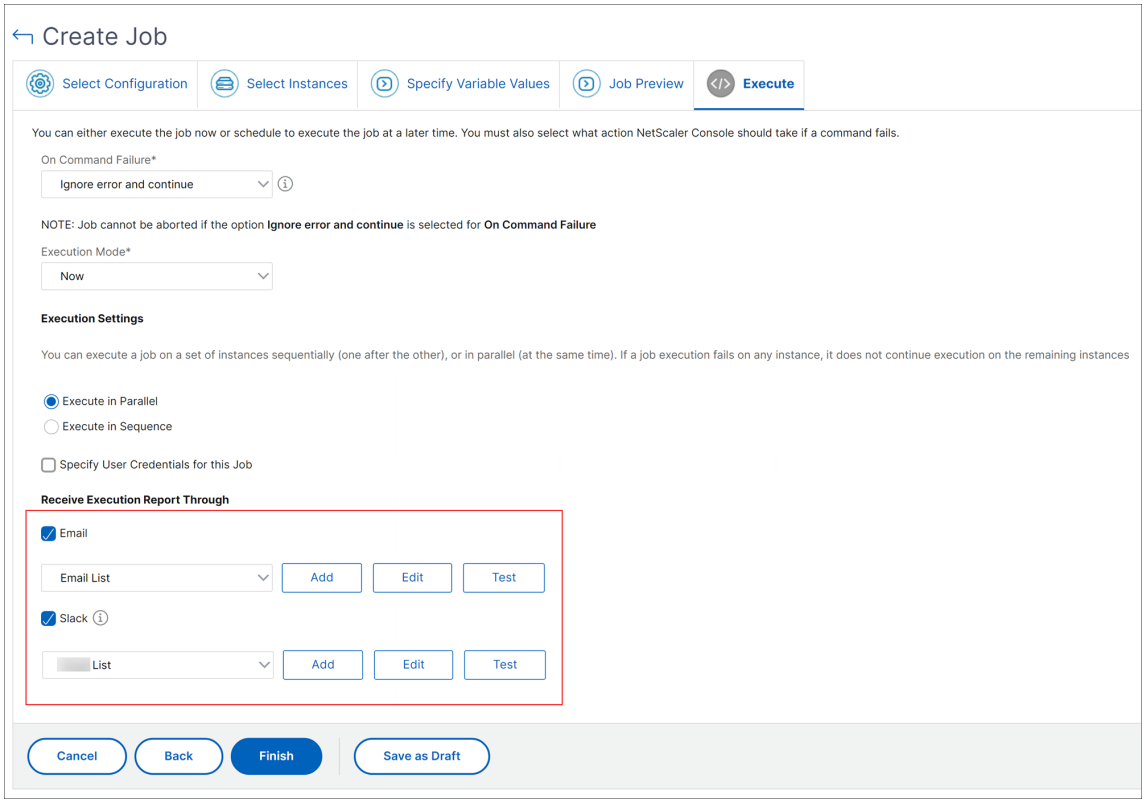
1. Vaya a **Infraestructura > Configuración > Trabajos de configuración**.
2. Seleccione el trabajo que quiere habilitar la notificación de correo electrónico y Slack y haga clic en **Modificar**.
3. En la ficha **Ejecutar**, vaya al panel **Recibir informe de ejecución mediante** :

   - 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.

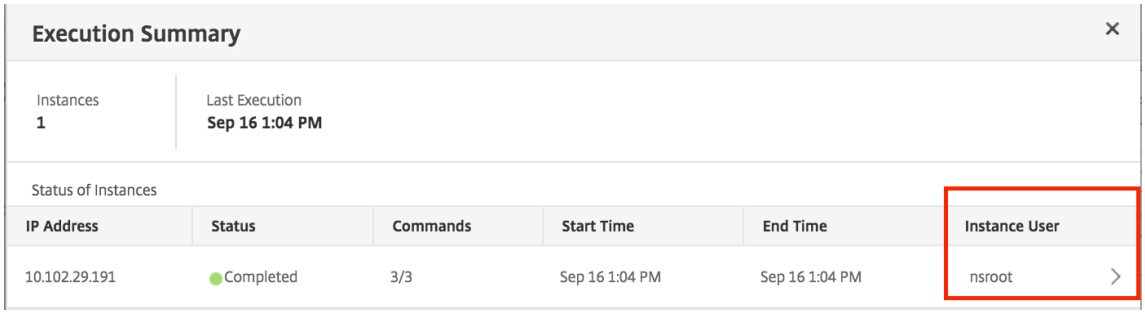


4. Haga clic en **Finalizar**.

Para ver los detalles del resumen de ejecución:

1. Vaya a **Infraestructura > Configuración > 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 el trabajo que se ejecutó
   - Los comandos se ejecutan en el trabajo
   - La hora de inicio y finalización del trabajo, y
   - Nombre del usuario de la instancia



Auditoría de configuración

January 26, 2024

Este documento incluye:

- Creación de plantillas de auditoría
- Ver los informes de auditoría
- Auditar los cambios de configuración en todas las instancias
- Obtener consejos de configuración sobre la configuración de la red
- Cómo sondear la auditoría de configuración de las instancias de NetScaler Console
- Genere una diferencia de auditoría de configuración para las trampas SNMP de ConfigChange

Trabajos de actualización de versiones

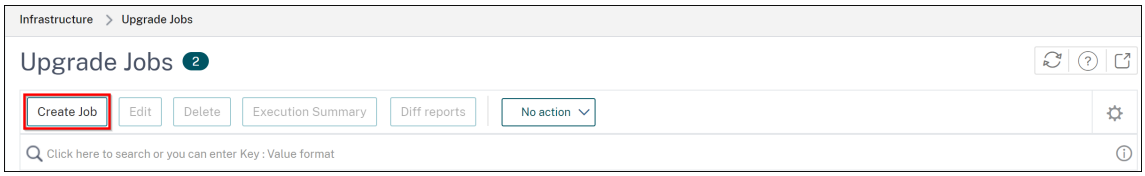
January 26, 2024

Puede crear las siguientes tareas de mantenimiento con NetScaler Console. A continuación, puede programar las tareas de mantenimiento en una fecha y hora específicas.

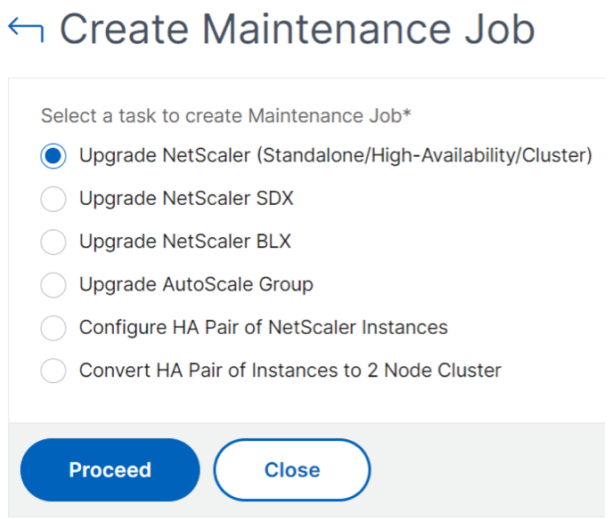
- Actualizar instancias de NetScaler
- Actualizar instancias SDX de NetScaler
- Actualización de instancias NetScaler BLX
- Actualización de instancias de NetScaler en el grupo de Autoscale
- Configurar el par HA de instancias NetScaler
- Convertir un par de instancias de HA en clúster

Programar la actualización de instancias NetScaler

1. En NetScaler Console, 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 las instancias de NetScaler que desee 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 la instancia en un explorador de archivos de NetScaler Console. La GUI de NetScaler Console muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.
     - **Omitir la carga de imágenes a NetScaler si la imagen seleccionada ya está disponible**: seleccione esta opción si la imagen ya está presente en la instancia de

NetScaler.

- **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.

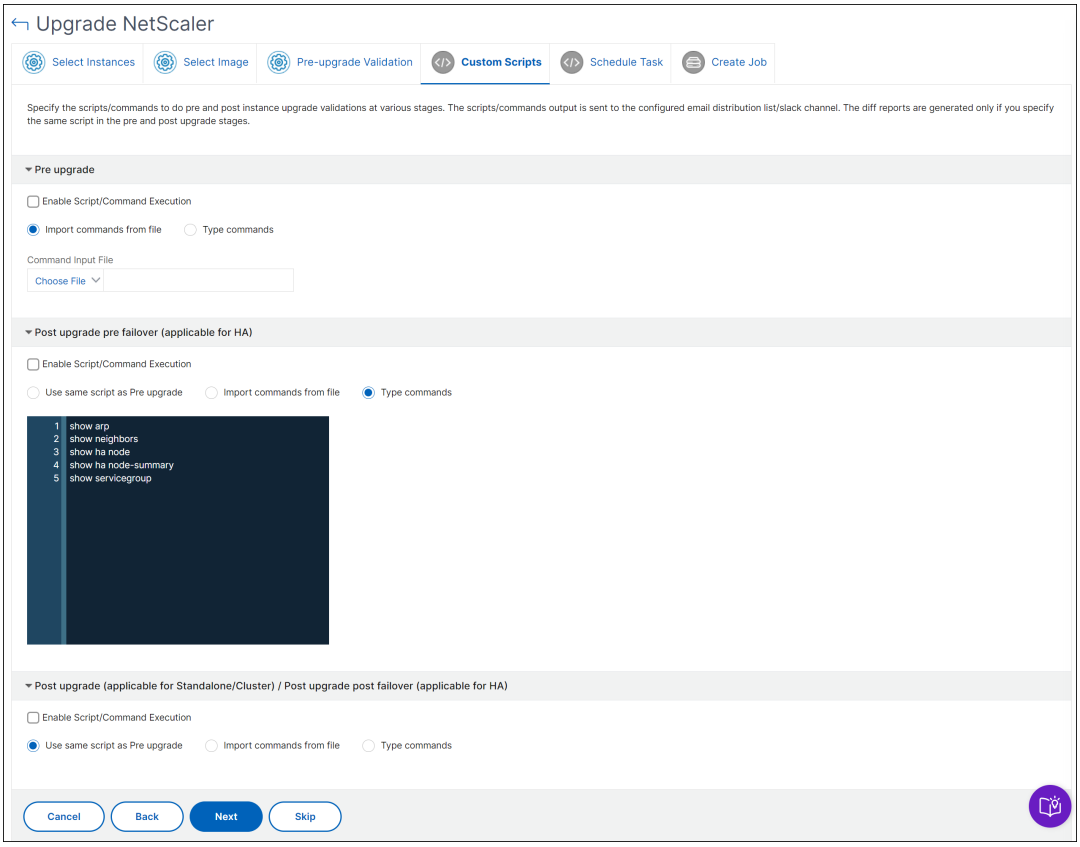
6. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   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, la consola de NetScaler realiza la validación previa a la actualización solo en la instancia especificada, no en los demás 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:

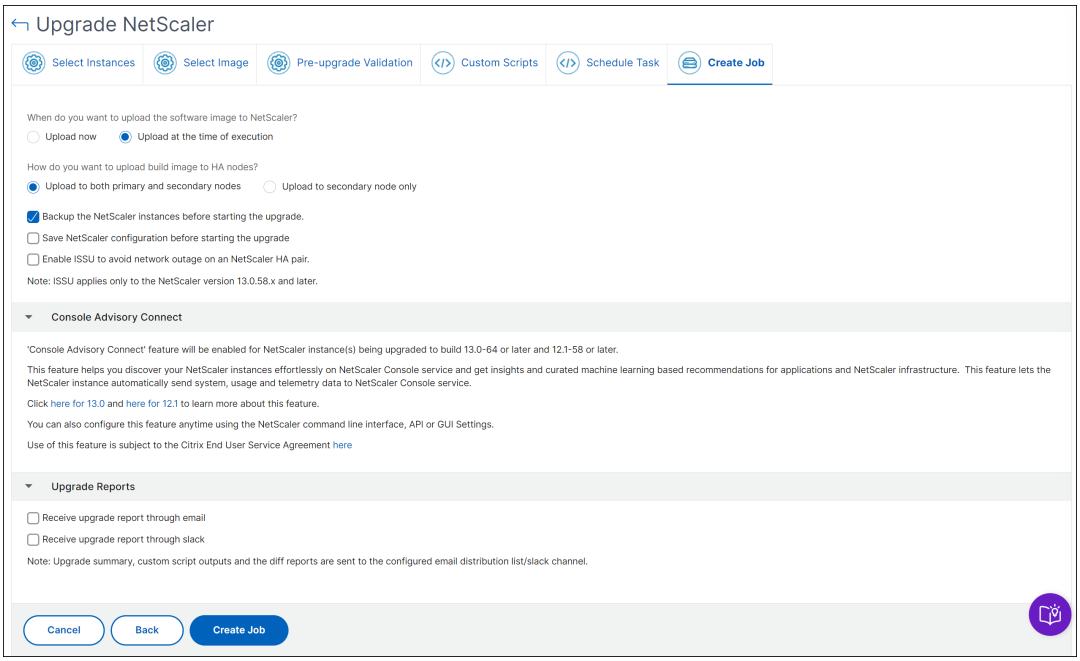
- La versión de la instancia antes y después de la actualización.
- El estado de las interfaces, los nodos de alta disponibilidad, los servidores virtuales y los servicios antes y después de la actualización.
- Las estadísticas de los servicios y servidores virtuales.
- Las rutas dinámicas.

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 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. 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 de NetScaler antes de iniciar la actualización.** - Crea una copia de seguridad de las instancias de NetScaler seleccionadas.
      - **Guardar la configuración de NetScaler antes de iniciar la actualización**: guarda los trabajos de configuración configurados en la instancia antes de la actualización.
      - **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.

- **Console Advisory Connect**: si vas a actualizar a la versión **13.0-64 o posterior** y a la **12.1-58 o posterior** , Console Advisory Connect se habilita automáticamente. Para obtener más información, consulte Incorporación discreta de instancias de NetScaler mediante NetScaler Console 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. En NetScaler Console, 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 de **imágenes de software** , seleccione **Local** (su máquina local) o **Dispositivo**(el archivo de compilación debe estar presente en el dispositivo virtual de NetScaler Console).

   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. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar 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. En NetScaler Console, 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 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 la instancia en un explorador de archivos de NetScaler Console. La GUI de NetScaler Console muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.

- **Omitir la carga de imágenes a NetScaler si la imagen seleccionada ya está disponible**: seleccione esta opción si la imagen ya está presente en la instancia de NetScaler.
- **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.

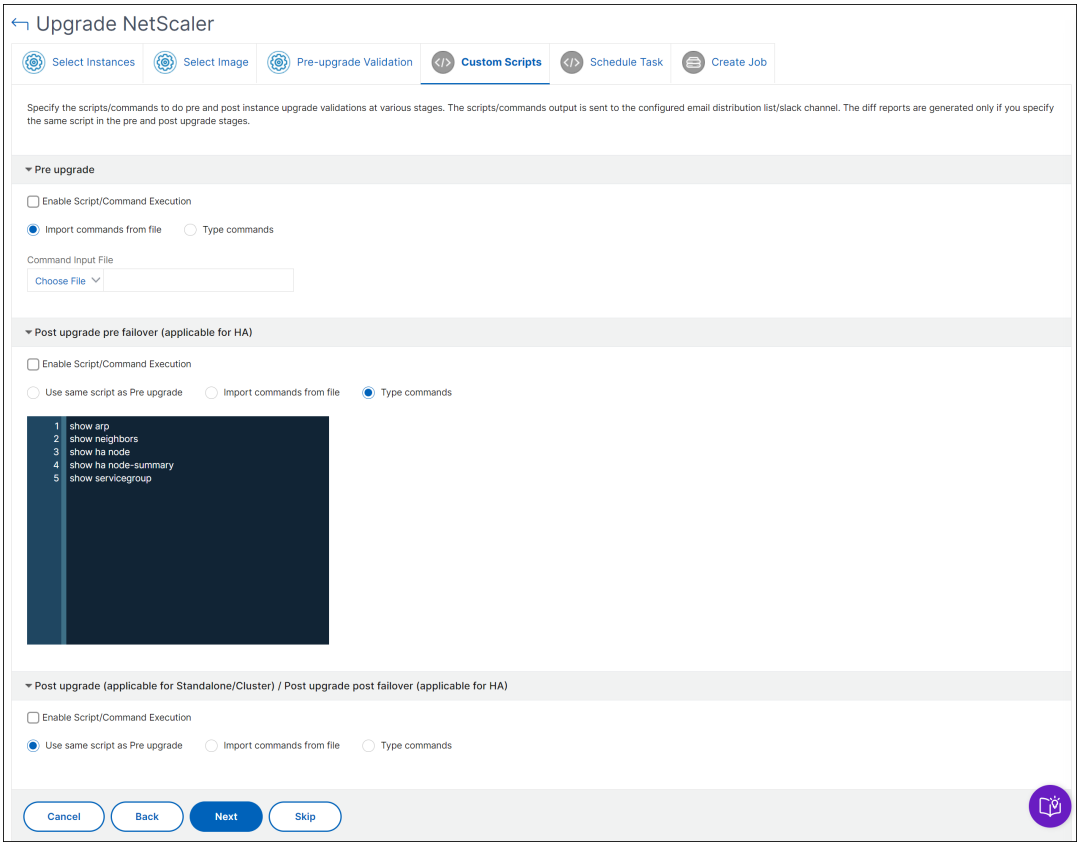
6. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   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, la consola de NetScaler realiza la validación previa a la actualización solo en la instancia especificada, no en los demás 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.
    - **Haga 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.
    - **Guarda la configuración de NetScaler antes de iniciar la actualización**: guarda los trabajos de configuración configurados en la instancia antes de la actualización.
    - **Habilite la ISSU para evitar la interrupción de la red en el par**NetScaler HA: ISSU garantiza la actualización sin tiempo de inactividad en un par de NetScaler de alta disponibilidad. 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.

    - **Console Advisory Connect**: si vas a actualizar a la versión **13.0-64 o posterior** y a la **12.1-58 o posterior** , Console Advisory Connect se habilita automáticamente. Para obtener más información, consulte Incorporación discreta de instancias de NetScaler mediante Console Advisory 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. En NetScaler Console, 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. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar las notificaciones.
5. Haga clic en **Finalizar**.

Programar la configuración del par de instancias de NetScaler de HA

1. En NetScaler Console, 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) Introduzca la dirección IP principal.
    c) Introduzca la dirección IP secundaria.
    d) Haga clic en **Siguiente**.

e) Haga clic para **activar el modo Activar INC (Configuración de red independiente)** si tiene las instancias de par HA en dos subredes.

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 por correo electrónico y Slack para recibir el informe de ejecución de la creación del par NetScaler HA. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar 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.

Programar la conversión del par de instancias de HA en clúster

1. En NetScaler Console, 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. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar 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

September 2, 2024

En NetScaler Console, puede actualizar una o más instancias de NetScaler. Debe conocer el marco de licencias y los tipos de licencias antes de actualizar una instancia.

NOTA: Si quiere actualizar una instancia que tiene directivas clásicas, le recomendamos que convierta las directivas clásicas en avanzadas antes de actualizar la instancia mediante la herramienta NSPEPI. Esto es aplicable a las funciones compatibles con la herramienta NSPEPI. Para obtener más información, consulte Consideraciones de actualización para configuraciones con directivas clásicas.

Requisitos previos

NetScaler Console realiza las siguientes comprobaciones previas a la validación en la instancia que desea actualizar:

1. **Comprueba el espacio en disco**: Limpia el espacio en disco para tener una capacidad de disco suficiente para actualizar una instancia. Resuelva los problemas de disco, si
2. **Compruebe si hay problemas de hardware de disco**: Resuelva los problemas de hardware si los hay.
3. **Comprobar si hay personalizaciones**: Haga una copia de seguridad de sus personalizaciones y elimínelas de las instancias. Puedes volver a aplicar la personalización de la copia de seguridad después de la actualización de la instancia.
4. **Problemas con las directivas**: NetScaler no admite las directivas clásicas de la versión `13.1`. Antes de actualizar una instancia a esta versión, migre las directivas clásicas a las directivas avanzadas.

   Para obtener más información, consulte Directivas clásicas y avanzadas.

Consideraciones sobre la actualización de las configuraciones personalizadas de NetScaler

Es importante que tanto los cambios de actualización como las personalizaciones se apliquen a un dispositivo NetScaler actualizado. Por lo tanto, si tiene archivos de configuración personalizados en el directorio /etc, consulte Consideraciones sobre la actualización de los archivos de configuración personalizados antes de continuar con la actualización del dispositivo NetScaler. Estos son los pasos generales que debe realizar:

1. Pasos previos a la actualización en NetScaler

    - Realice una copia de seguridad del archivo personalizado antes
    - Elimine el enlace simbólico del archivo personalizado antes de la actualización

2. Actualice NetScaler mediante ADM. Para actualizar, siga las instrucciones disponibles al principio de la página.
3. Pasos posteriores a la actualización en NetScaler

    - Restaurar las personalizaciones después de la actualización

Los pasos previos y posteriores a la actualización deben realizarse en cada instancia de NetScaler. Sin embargo, en el paso 2, para actualizar NetScaler mediante ADM, todas las instancias vulnerables de NetScaler se pueden seleccionar y actualizar juntas.

Par de alta disponibilidad NetScaler

Cuando actualice un par de alta disponibilidad de NetScaler, 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.
- Después de la actualización correcta del par de alta disponibilidad, aparece un mensaje de error en el historial de ejecución. Este mensaje aparece si los nodos del par de alta disponibilidad están en versiones o versiones diferentes. Indica que la sincronización entre los nodos principal y secundario está deshabilitada.

Puede actualizar un par de alta disponibilidad de NetScaler 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.

Clústeres NetScaler

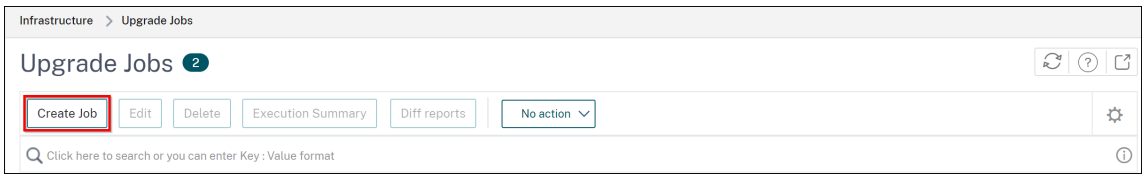
Al actualizar un clúster de NetScaler, en la etapa de validación previa a la actualización, la consola de NetScaler solo valida la instancia especificada. Por lo tanto, compruebe y resuelva los siguientes problemas en los nodos del clúster:

- Personalización
- Uso del disco
- problemas de hardware

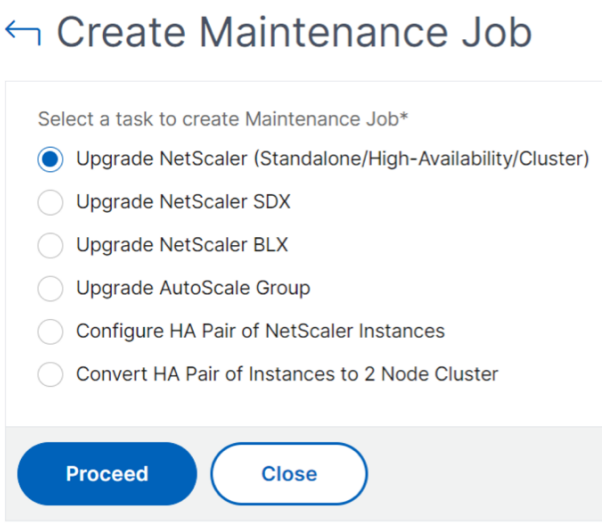
Crear un trabajo de actualización de NetScaler

Para crear un trabajo de actualización de NetScaler, haga lo siguiente:

1. Vaya a **Infraestructura > Trabajos de actualización**.



2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar NetScaler (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.



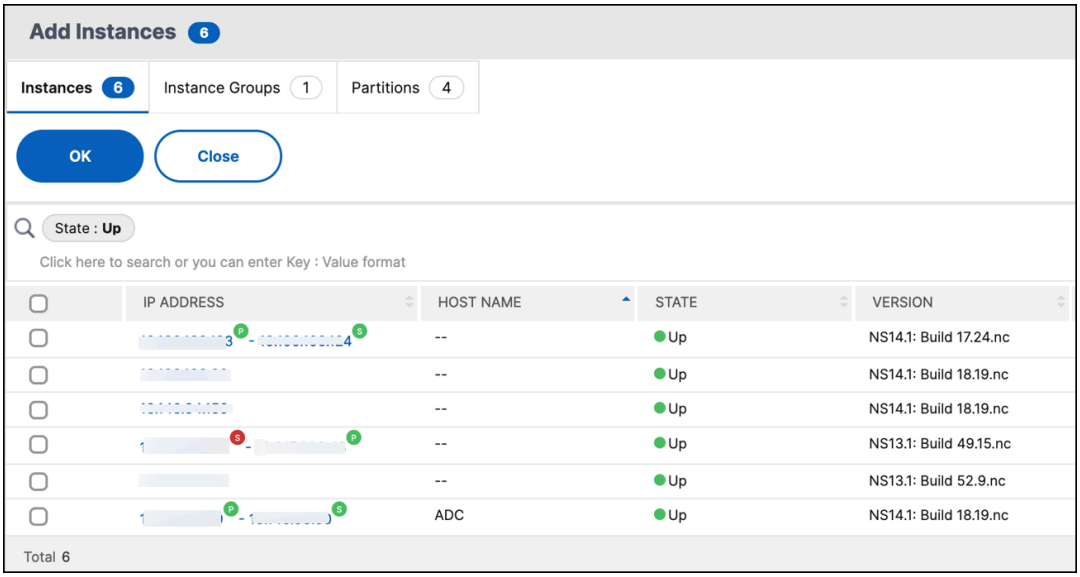
> **Nota:**
>
> Para actualizar los grupos de Autoscale, consulte Actualizar un grupo de Autoscale.

3. En la ficha **Seleccionar instancias**,

   a) Especifique el nombre de su elección para el **nombre del trabajo**.

   b) Haga clic en **Agregar instancias** para agregar las instancias de NetScaler que desee actualizar.

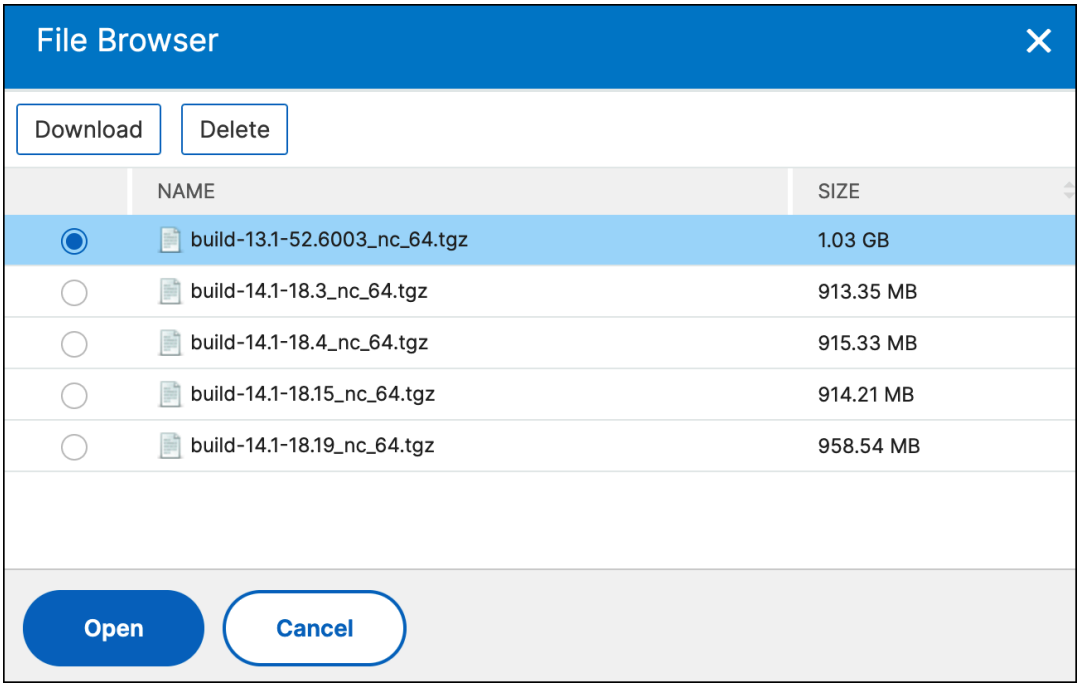
      - Para actualizar un par de alta disponibilidad de NetScaler, seleccione las direcciones IP del par de alta disponibilidad (indicadas por los superíndices “S”y “P”).
      - Para actualizar un clúster, seleccione la dirección IP del clúster (indicada con el superíndice “C”).



c) Haga clic en **Aceptar**.

4. En la ficha **Seleccionar imagen** , seleccione una imagen de NetScaler de la biblioteca de imágenes, local o dispositivo.

   - **Seleccionar de la biblioteca**de imágenes: seleccione una imagen de NetScaler de la lista. Esta opción muestra todas las imágenes de NetScaler que están disponibles en el sitio web de descargas de NetScaler.



Las imágenes del software NetScaler muestran las compilaciones preferidas con el icono de estrella. Y, la mayoría de las compilaciones descargadas con el icono de marcador.

- **Seleccione entre local o dispositivo**: puede cargar la imagen desde su equipo local o desde el dispositivo NetScaler. Al seleccionar el dispositivo NetScaler, la GUI de NetScaler Console muestra los archivos de instancia que están presentes en `/var/mps/ns_images`. Seleccione la imagen en la GUI de NetScaler Console.
- **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.

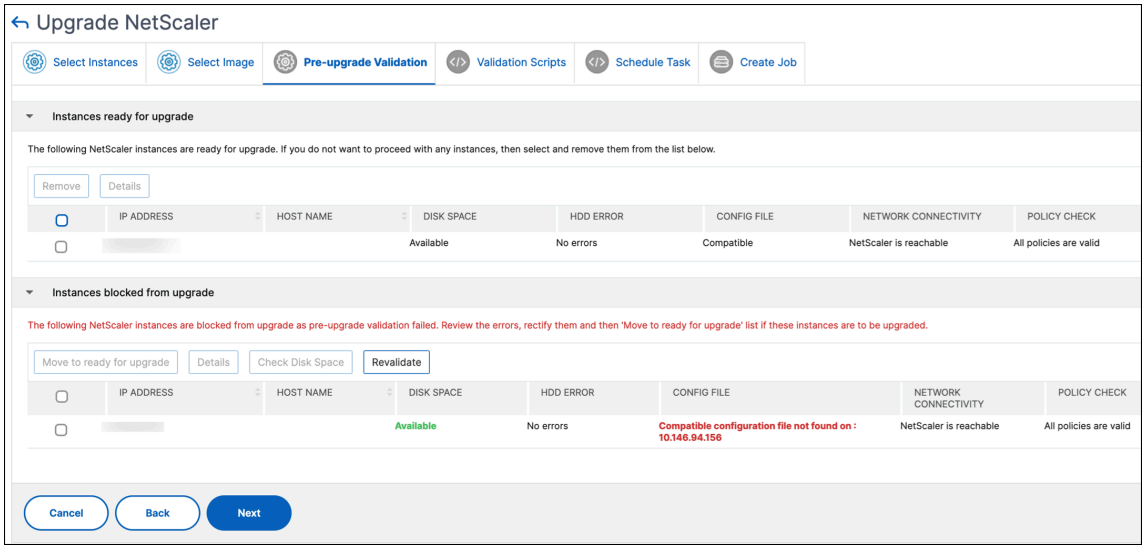
Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

> **Nota:**
>
> - Las imágenes de NetScaler descargadas se almacenan en el agente 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 Console borra las imágenes de NetScaler almacenadas en caché cada tres días en función de la hora de la última modificación de las imágenes. Solo los dos archivos de imagen más recientes se almacenan en caché en el agente a la vez.

5. 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.

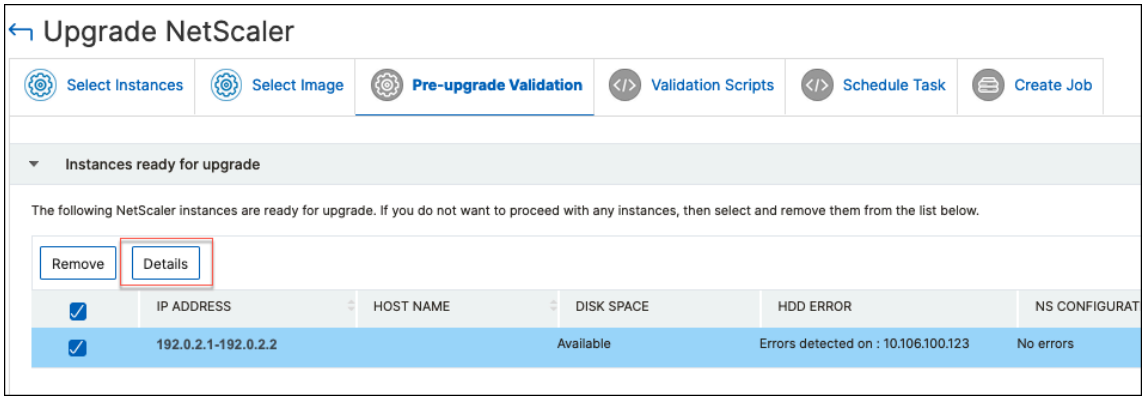
     Puede revisar, corregir los errores y, a continuación, hacer clic en **Mover a listo para la actualización** para actualizarlos. Si no tiene suficiente espacio en disco en una instancia, puede comprobar y limpiar el espacio en disco. Consulte Limpiar espacio en disco de NetScaler.

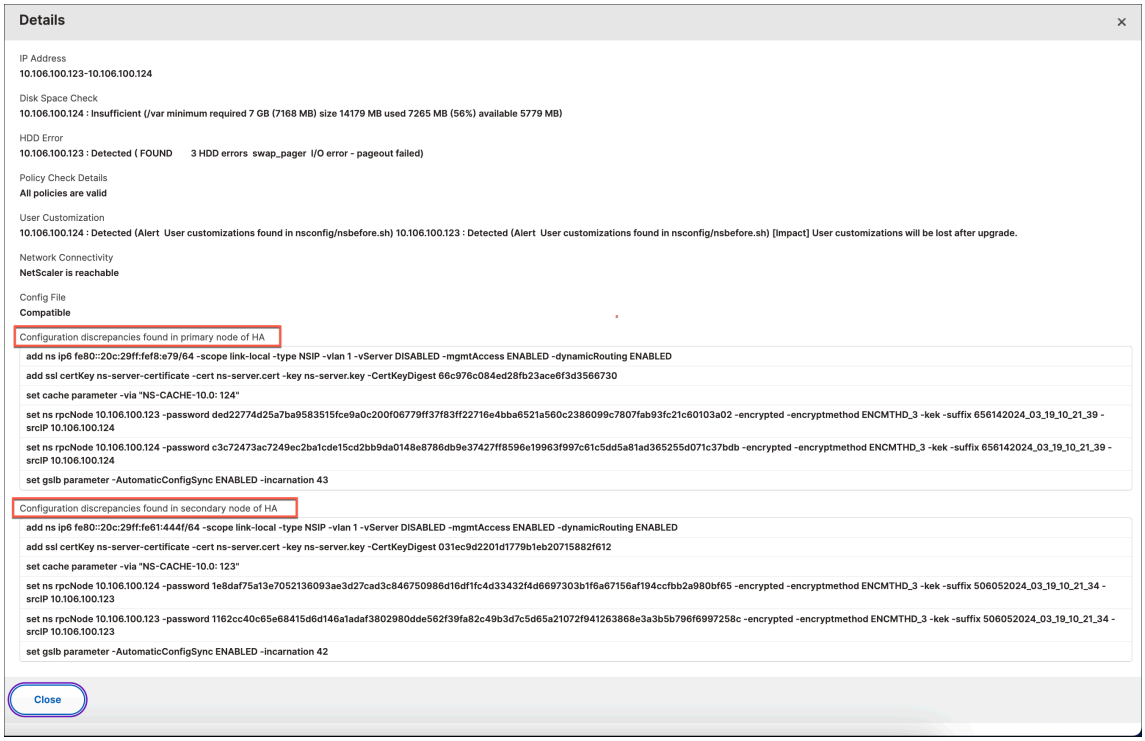


- **Verificación de directivas**: si NetScaler Console encuentra directivas clásicas no compatibles, puede eliminarlas para crear un trabajo de actualización.

> **Importante:**
>
> Si especifica una dirección IP de clúster, NetScaler Console realiza la validación previa a la actualización solo en la instancia especificada y no en los demás nodos del clúster.

Para ver las discrepancias entre los nodos principales y secundarios durante una actualización, seleccione el nodo de alta disponibilidad y haga clic en **Detalles**.





- **Discrepancias de configuración encontradas en el nodo principal de alta disponibilidad**: Muestra todas las configuraciones encontradas en el nodo secundario del par de alta disponibilidad de NetScaler que faltan en el nodo principal.
- **Discrepancias de configuración encontradas en el nodo secundario de alta disponibilidad**: Muestra todas las configuraciones encontradas en el nodo principal del par de alta disponibilidad de NetScaler que faltan en el nodo secundario.

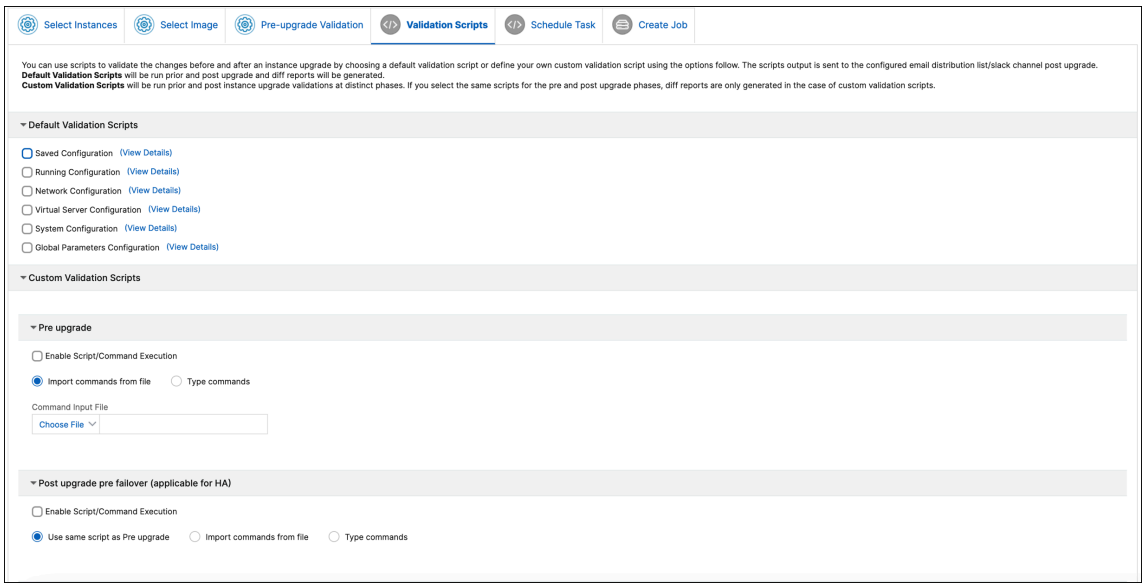
> **Nota:**
>
> Puede ignorar las siguientes discrepancias que pueden aparecer en las secciones de discrepancias de configuración:
>
> - Configuraciones específicas del dispositivo, como las direcciones IP.
> - Contraseñas o certificados cifrados, que pueden diferir entre los nodos, incluso si la contraseña es la misma.
>
> Puede revisar las discrepancias y optar por ignorarlas si no son relevantes.

6. En **Scripts de validación**, especifique los scripts que se ejecutarán antes y después de la actualización de una instancia. Puede realizar una de las siguientes acciones:

   - **Scripts de validación predefinidos**: Elija esta opción para ejecutar los scripts de validación predefinidos. Estos scripts se ejecutan antes y después del trabajo de actualización, lo que genera un informe de diferencias para el script de validación.

> **Nota:**
>
> No puede cambiar ni editar este conjunto predefinido de comandos.

- **Scripts de validación personalizados**: Elija esta opción para ejecutar su propio script de validación. Puede especificar si desea que los scripts se ejecuten antes o después de la actualización. Solo se genera un informe de diferencias si se seleccionan los mismos scripts antes y después de la actualización.



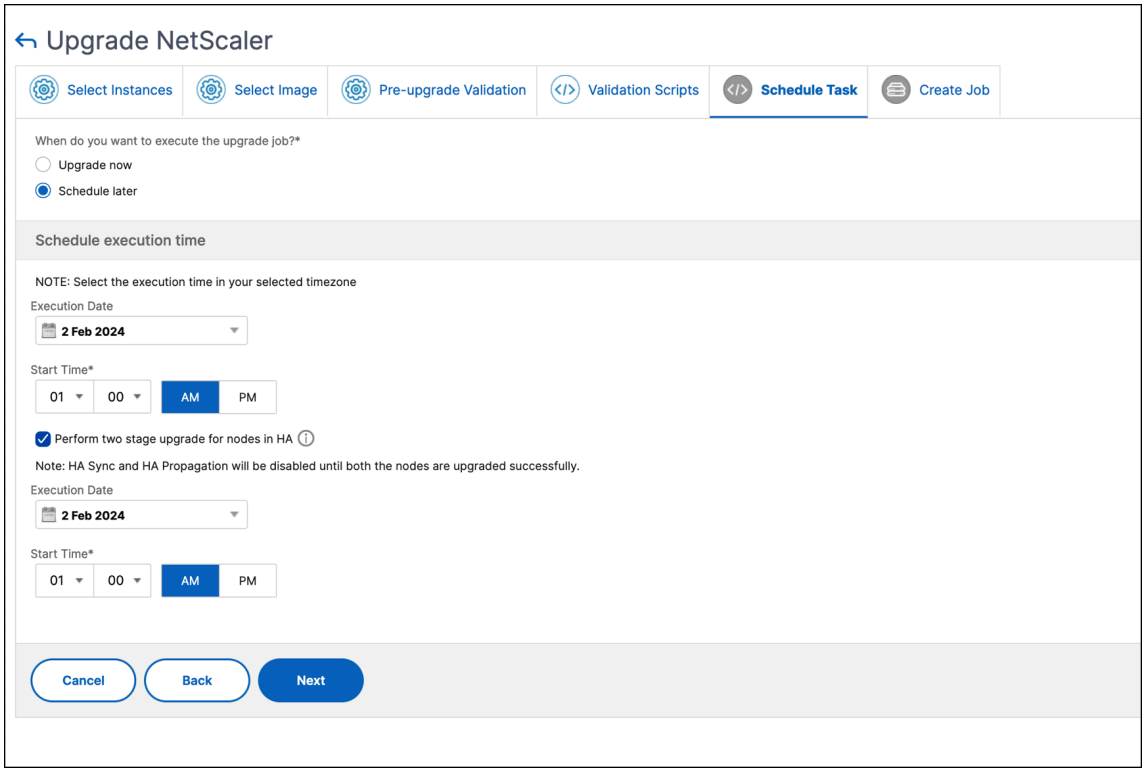
Para conocer el conjunto de comandos de cada configuración, haga clic en **Ver detalles**. Para obtener más información, consulte Usar scripts personalizados.

7. 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 desea actualizar un par de alta disponibilidad de NetScaler en dos etapas, seleccione **Realizar una actualización en dos etapas para los nodos con alta disponibilidad**.

   Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia del par de alta disponibilidad.



Para obtener más información, consulte Par de alta disponibilidad de NetScaler.

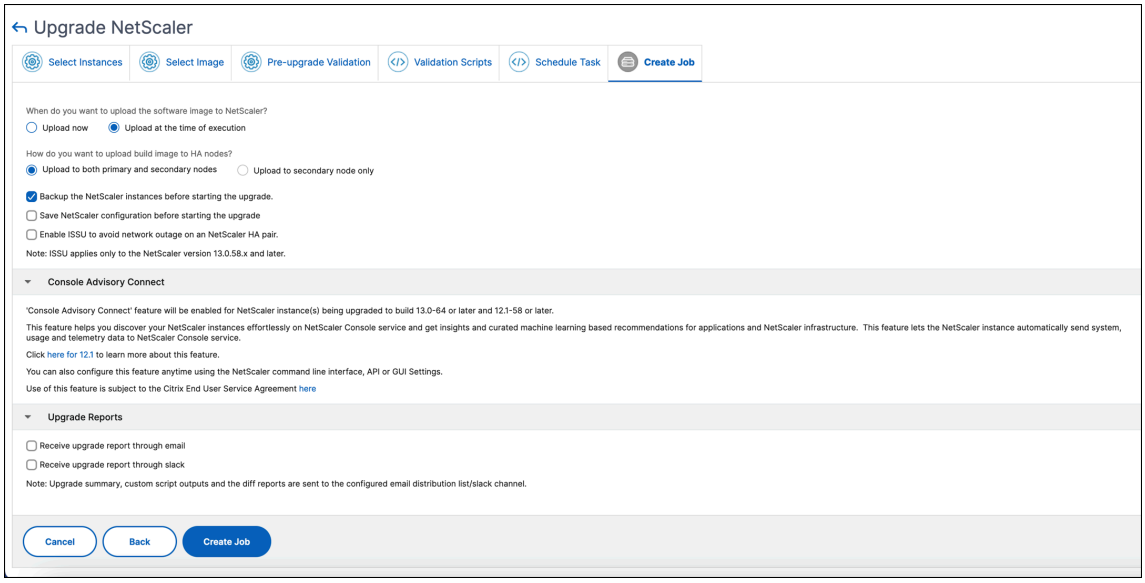
8. En **Crear trabajo**, especifique los siguientes detalles:

   Si programa el trabajo de actualización, puede especificar cuándo quiere cargar la imagen en una instancia:

   - **Subir 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 los pares de alta disponibilidad, puede especificar los nodos en los que desea 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 escenarios de programación disponibles para el par de alta disponibilidad, consulte Programación de trabajos de actualización para el par de alta disponibilidad de NetScaler.

Para obtener más información sobre otras opciones de actualización, consulte Opciones de actualización de NetScaler.

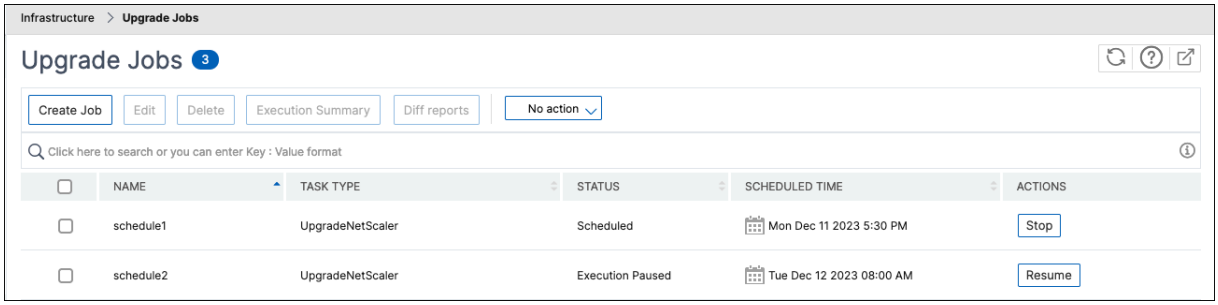
9. Haga clic en **Crear trabajo**.

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**.

Pausar o reanudar un trabajo de actualización programado

También puede pausar el trabajo de actualización programado.

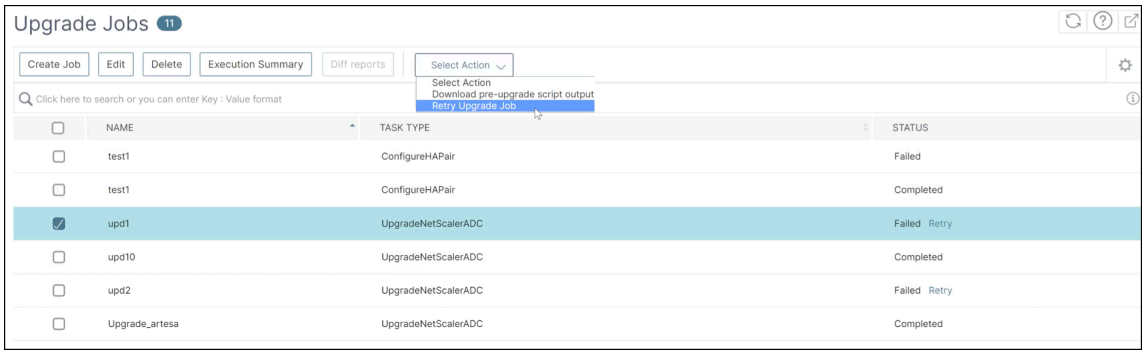
Para usar esta función, vaya a **Infraestructura > Trabajos de actualización, seleccione un trabajo** de actualización programado existente y haga clic en **Detener** para pausar el trabajo. Para reanudar el trabajo de actualización programado, haga clic en **Reanudar** .



> **Nota:**
>
> Si el tiempo programado para el trabajo de actualización ha pasado después de haber decidido reanudarlo, debe volver a crear el trabajo de actualización.

Reintentar trabajos de actualización fallidos

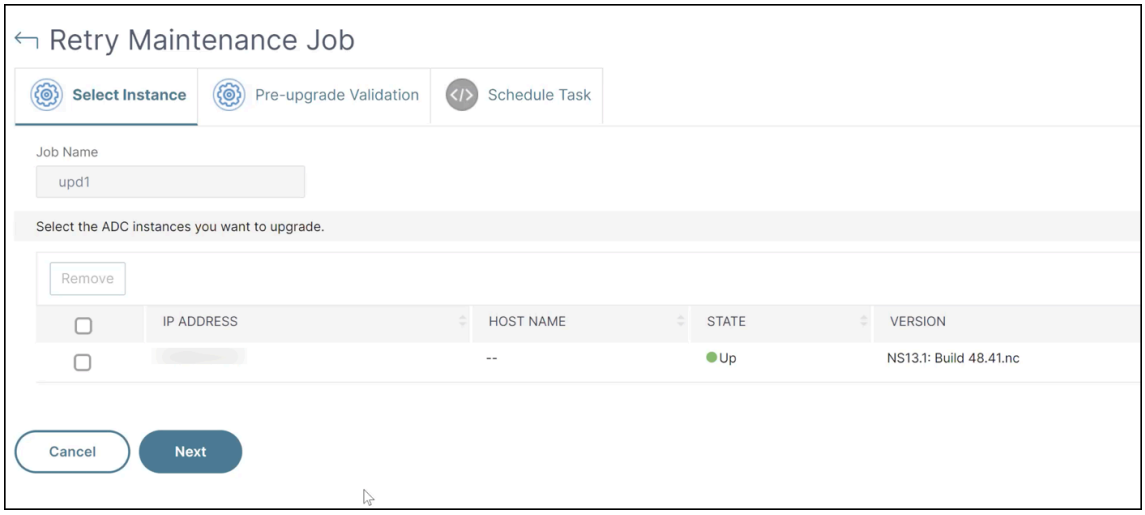
1. En **Infraestructura > Trabajos de actualización**, seleccione el trabajo de actualización fallido y haga clic en **Reintentar**. Como alternativa, también puede ir a **Seleccionar acción > Reintentar un trabajo de actualización** para volver a intentar un trabajo fallido.



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**.

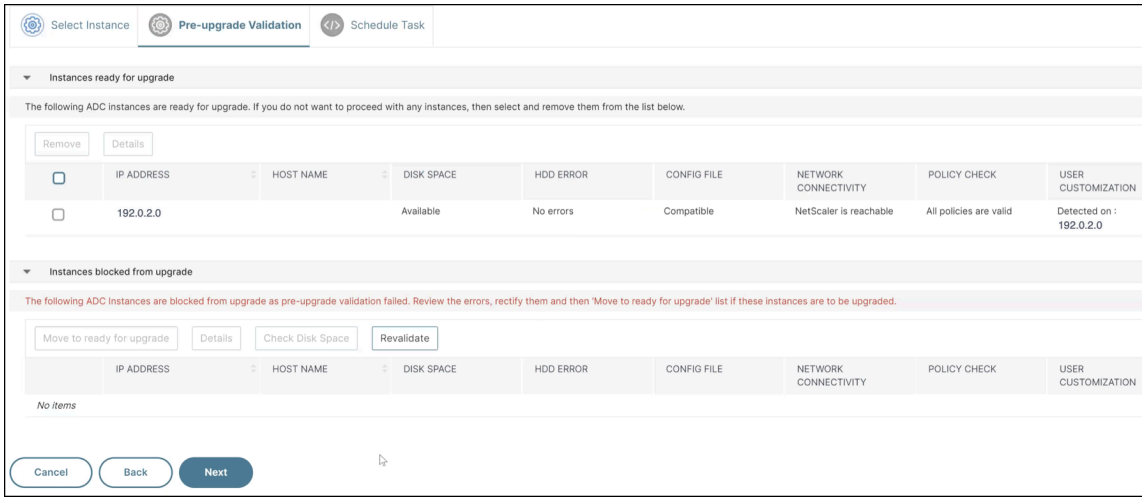
   Haga clic en **Siguiente** para iniciar el proceso de validación.



3. La ficha **Validación previa a la actualización** muestra las siguientes secciones:

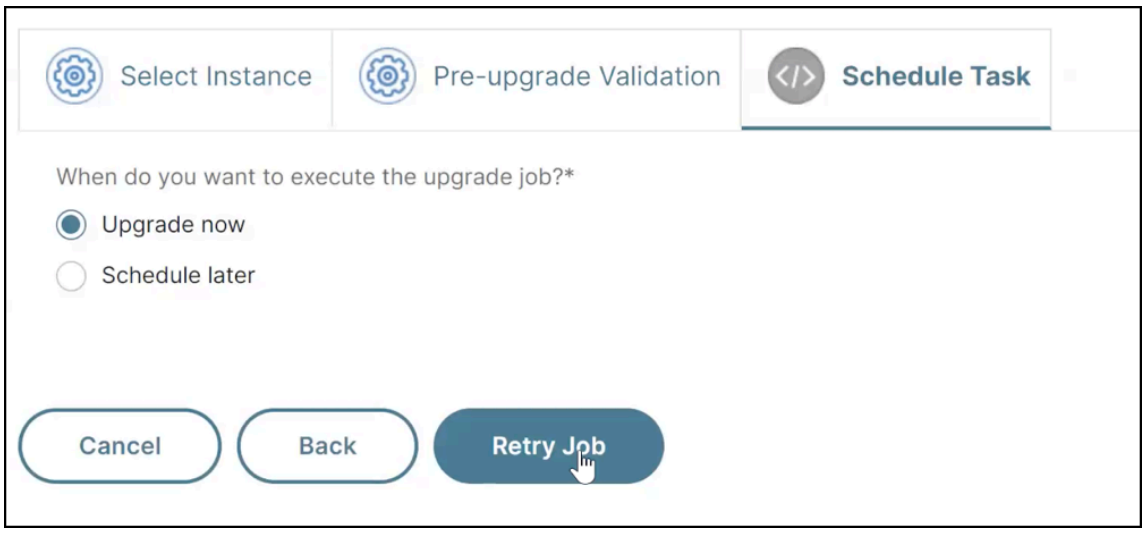
- **Instancias listas para la actualización**. Puede continuar con la actualización de estas instancias.
- **Instancias bloqueadas para la actualización**. Se ha bloqueado la actualización de estas instancias de NetScaler debido a errores de validación previos a la actualización.

  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 espacio en disco de NetScaler.
- **Verificación de directivas**: si NetScaler Console 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.



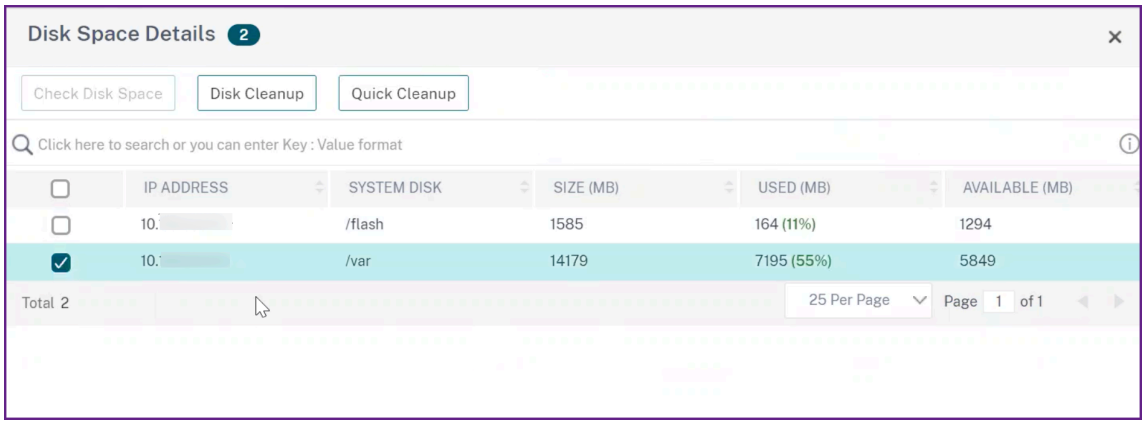
Haga clic en **Reintentar**.

Limpie el espacio en disco de NetScaler

Si se enfrenta a un problema de espacio insuficiente en disco al actualizar una instancia de NetScaler, limpie el espacio en disco de la propia GUI de NetScaler Console.

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**.

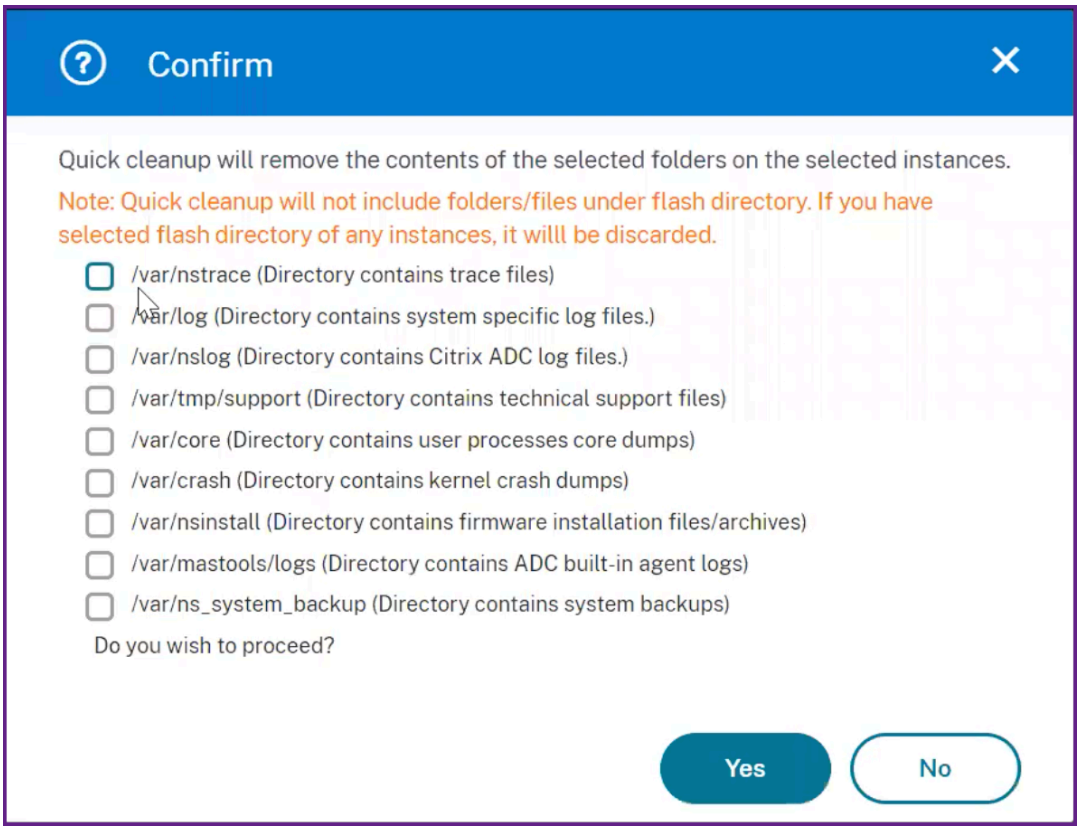
   Aparece el panel **Detalles del espacio en disco**. Este panel muestra las instancias, la memoria utilizada y la memoria disponible.



3. En el panel **Detalles del espacio en disco**, seleccione la instancia que deba limpiarse y realice una de las siguientes acciones:

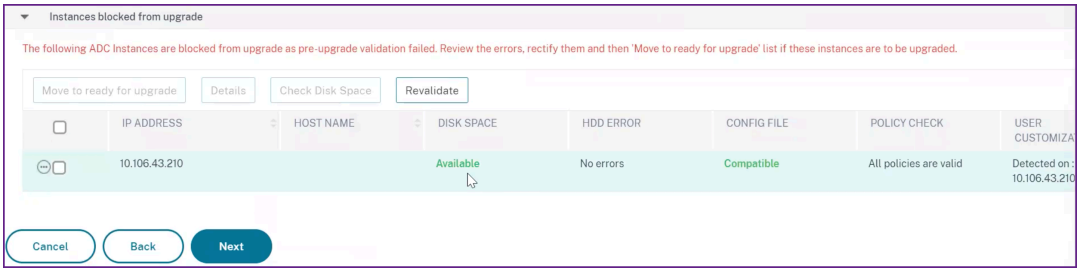
a) **Liberador de espacio en disco**: Vaya hasta las carpetas o directorios necesarios y elimínelos para liberar espacio en disco.

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.



Usar scripts personalizados

Puede especificar scripts personalizados mientras crea un trabajo de actualización de NetScaler. 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.

Especifique los scripts personalizados que se van a ejecutar en las siguientes etapas:

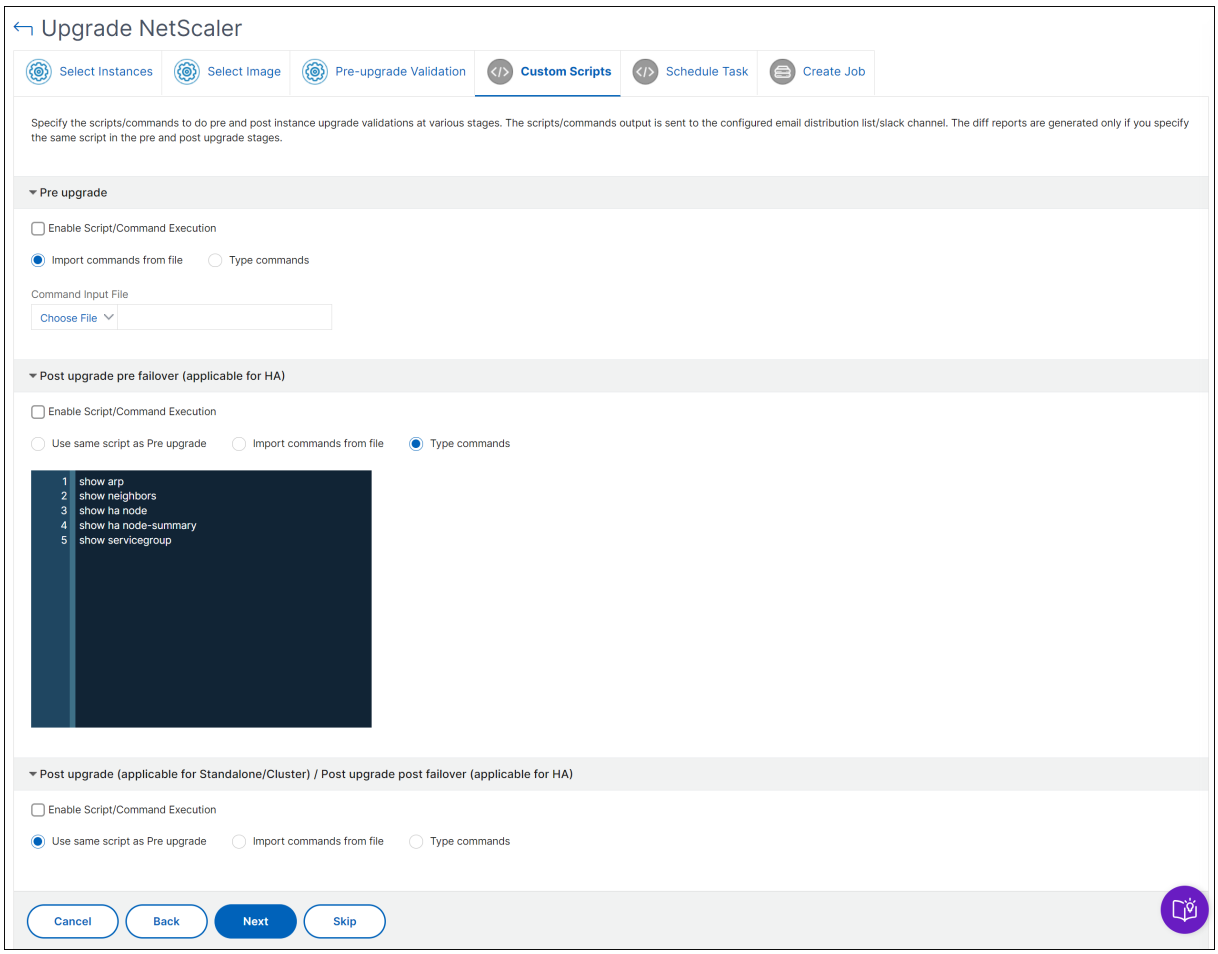
- **Preactualización**: el script especificado se ejecuta antes de actualizar una instancia.
- **Después de la actualización previa a la conmutación por error (aplicable para HA)**: esta etapa solo se aplica a la implementación de alta disponibilidad. El script especificado se ejecuta después de actualizar 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 de scripts o comandos en las etapas requeridas. De lo contrario, los scripts especificados no se ejecutan.
> - El informe diff solo se genera si especifica el mismo script en las fases previa a la actualización y posterior a la actualización. Por lo tanto, asegúrese de seleccionar **Usar el mismo script que antes de la actualización** en las etapas posteriores a la actualización. Consulte Descargar un informe de diferencias consolidado de un trabajo de actualización de NetScaler.

Puede importar un archivo de script o escribir comandos directamente en la GUI de NetScaler Console.

- **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 la fase posterior a la actualización, puede utilizar el mismo script especificado en la fase previa a la actualización.

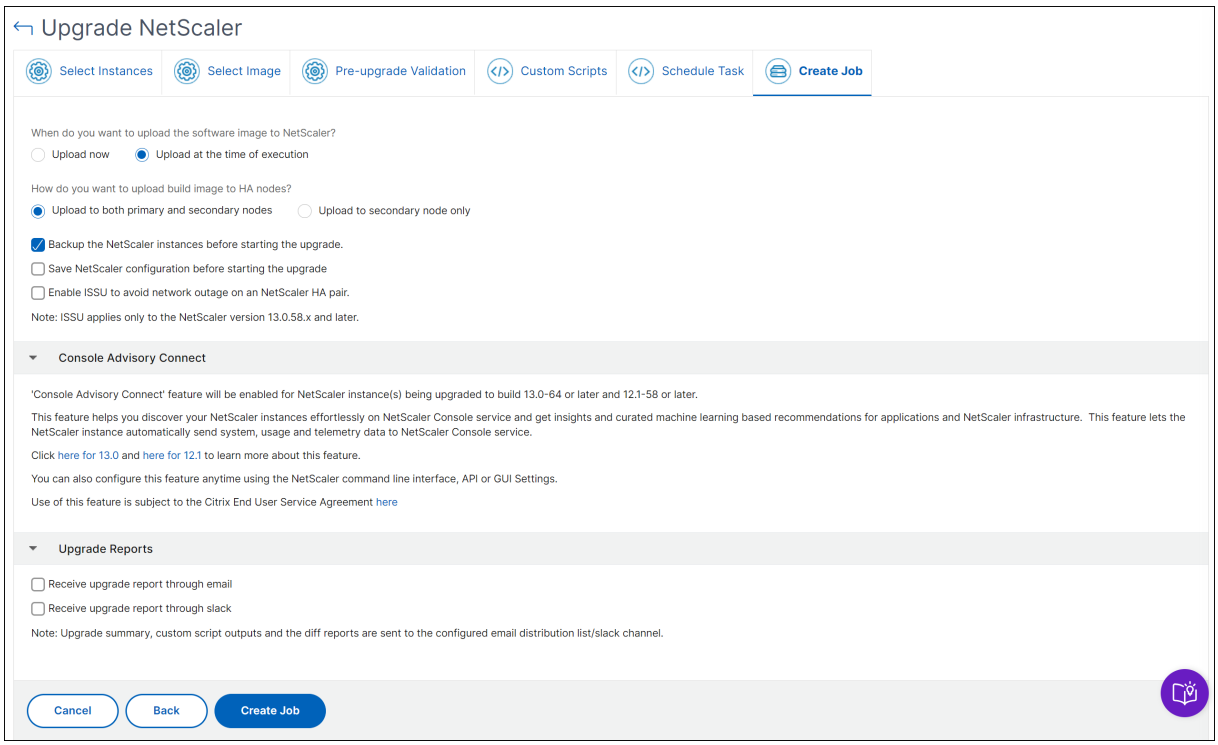


Opciones de actualización de NetScaler

Al crear un trabajo de actualización de NetScaler , puede seleccionar las siguientes opciones en la ficha **Crear trabajo**:

- **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.
- **Mantener 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 la ISSU para evitar la interrupción de la red en el par**NetScaler HA: ISSU garantiza la actualización sin tiempo de inactividad en un par de NetScaler de alta disponibilidad. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par de alta disponibilidad de NetScaler 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.



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**

Descargue un informe de diferencias consolidado de un trabajo de actualización de NetScaler

En NetScaler Console, puede descargar un informe de diferencias de un trabajo de actualización de NetScaler. Para ello, el trabajo de actualización debe tener 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 de diferencias solo se genera si especificas el mismo script en las etapas previas y posteriores a la actualización.

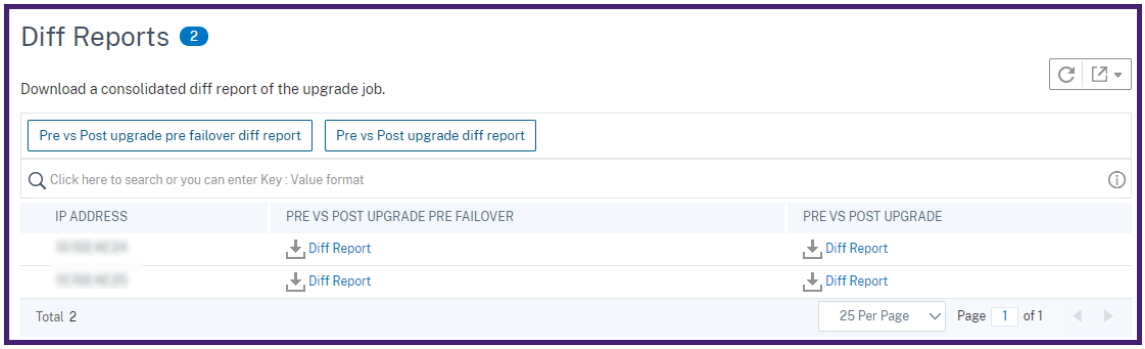
Para descargar un informe diff de un trabajo de actualización, haga lo siguiente:

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**



Funciones de red

January 26, 2024

Con la función Funciones de red, puede supervisar el estado de las entidades configuradas en las instancias administradas de Citrix Application Delivery Controller (NetScaler). 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
- Método de equilibrio de carga
- Persistencia de equilibrio de carga

Generar informes para entidades de equilibrio de carga

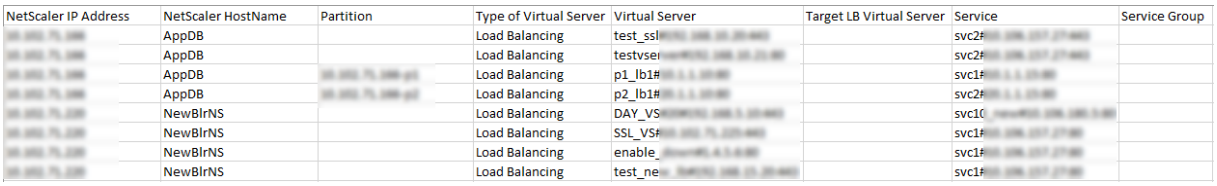
January 26, 2024

La consola NetScaler le permite ver los informes de las entidades de instancia de Citrix Application Delivery Controller (NetScaler) en todos los niveles. Hay dos tipos de informes que puede descargar en **NetScaler Console > 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
	AppDB		Load Balancing	test_ssl		svc2#	
	AppDB		Load Balancing	testvser		svc2#	
	AppDB		Load Balancing	p1_lb1#		svc1#	
	AppDB		Load Balancing	p2_lb1#		svc2#	
	NewBlrNS		Load Balancing	DAY_VS		svc1	
	NewBlrNS		Load Balancing	SSL_VS#		svc1#	
	NewBlrNS		Load Balancing	enable_		svc1#	
	NewBlrNS		Load Balancing	test_ne		svc1#	

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 Console 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 Console, vaya a **Infraestructura > Funciones de red**.
2. Haga clic en **Generar informe**.
3. En la página **Generar informe** que se abre, tiene dos opciones para ver el informe:
   a) En la ficha **Exportar ahora**, seleccione **Equilibrio de carga** y haga clic en **Aceptar**.

      El informe consolidado se descarga en su sistema.

   b) Seleccione **Programar Informe** para crear un programa para generar y exportar informes 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. Seleccione **Activar programación**.

      ii. **Periodicidad**: Seleccione **Diaria**, **Semanal**o **Mensual** en la lista.

      > **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 días del mes, con valores comprendidos entre 1 y 31.

iii. **Tiempo de exportación** - Introduzca la hora en el formato Hora: Minuto en formato de 24 horas.

iv. **Correo electrónico**: Marque la casilla de verificación y, a continuación, seleccione un perfil de la lista, o haga clic en **Agregar** para crear un perfil de correo electrónico.

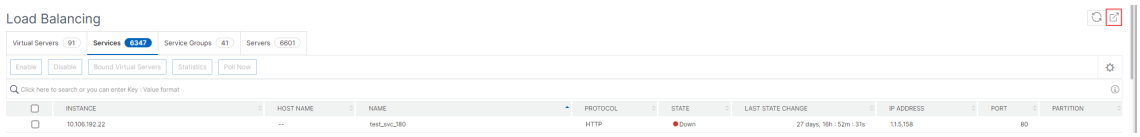
v. **Progreso**: Active la casilla de verificación Slack y, a continuación, seleccione un perfil en el cuadro de lista, o haga clic en **Agregar** para crear un perfil de demora.

vi. Haga clic en **Programar** para completar el proceso.

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 Console, 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.



Seleccione la ficha **Exportar ahora** si quiere generar y ver el informe en este instante.

> **Nota**
>
> Solo puede descargar los informes o exportarlos como archivos adjuntos de correo. No puede ver los informes en la GUI de NetScaler Console.

Exportar o programar la exportación de informes de funciones de red

January 26, 2024

Puede generar un informe completo para funciones de red seleccionadas, como el equilibrio de carga, la conmutación de contenido, la redirección de caché, el equilibrio de carga global de servidores

(GSLB), la autenticación y NetScaler Gateway en NetScaler Console. Este informe permite tener una vista de alto nivel de la asignación entre las instancias, 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 LB de destino enumera todos los servidores LB, es decir, tanto los servidores predeterminados como los 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. Para obtener información sobre cómo configurar las notificaciones por correo electrónico, consulte Crear reglas de eventos.

> **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 no se mantiene una lista separada de servidores virtuales SSL en NetScaler Console.
> - Cuando se genera un nuevo informe, los informes antiguos se depuran automáticamente de su cuenta.

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]	AppDB		Load Balancing	test_ssl[redacted]		svc2#[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2#[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1#[redacted]		svc1#[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1#[redacted]		svc2#[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1C[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS#[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1#[redacted]	

   b) Seleccione **Programar informe** para crear una programación que genere y exporte informes 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 **Diario**, **Semanal** o **Mensual** en el cuadro de lista desplegable.

      ii. **Tiempo de recurrencia**: introduzca la hora en Hora: Minuto en formato de 24 horas.

      iii. **Correo electrónico**: Active la casilla de verificación y, a continuación, seleccione el perfil en el cuadro de lista desplegable, o haga clic en **Agregar** para crear un perfil de correo electrónico.

      iv. **Slack**: selecciona la casilla de verificación y, a continuación, selecciona el perfil en el cuadro de lista desplegable o haga clic en **Agregar** 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 26, 2024

Puede optimizar el uso de los recursos supervisando los informes de red en NetScaler Console. 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 seguir manteniendo el rendimiento de sus aplicaciones, debe supervisar periódicamente el rendimiento de la red y asegurarse de que todos los recursos se utilizan de manera óptima.

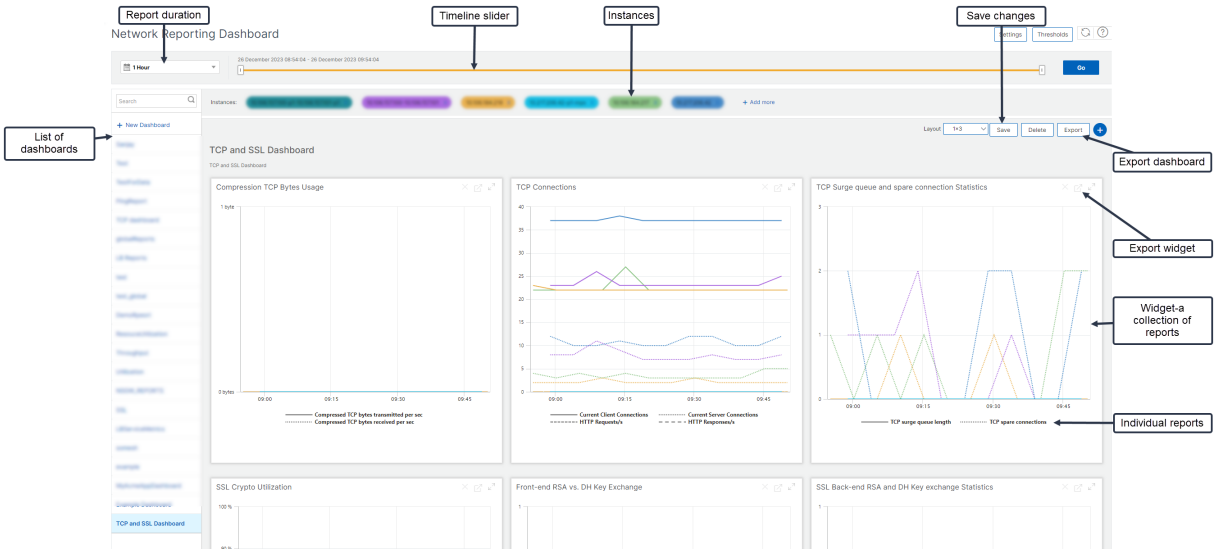
NetScaler Console le permite generar informes para instancias a nivel global y entidades como los servidores virtuales y las interfaces de red. Los servidores virtuales para los que puede generar informes son los siguientes:

- 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

Puede crear varios paneles para varias instancias, servidores virtuales y otras entidades en NetScaler Console.

Panel de informes de red

La siguiente imagen muestra las distintas funciones del panel de control:



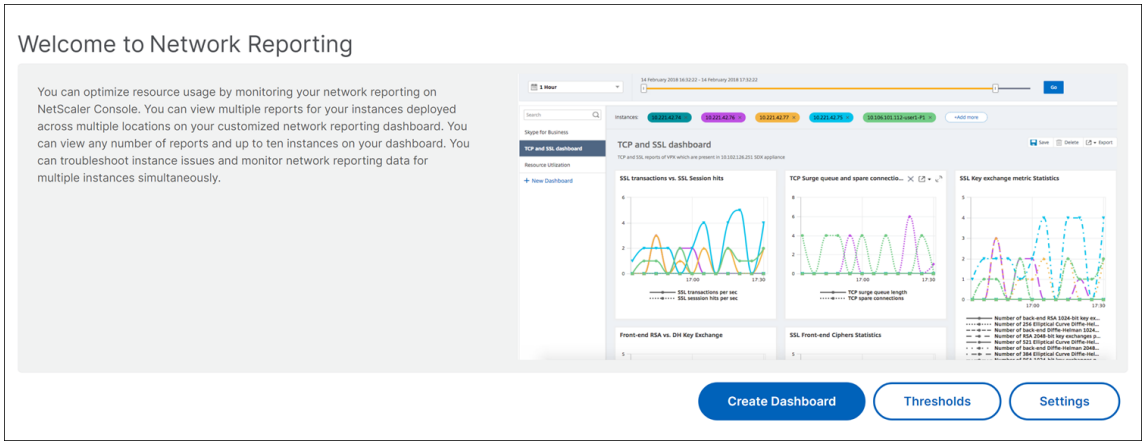
- El panel lateral izquierdo muestra todos los paneles personalizados que se crean en NetScaler Console. Puede hacer clic en uno de ellos para ver los diversos informes de los que está compuesto el panel. Por ejemplo, un panel TCP y SSL contiene varios informes relacionados con protocolos TCP y SSL.

- 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. Puede usar la opción de control deslizante de cronograma para personalizar la duración de los informes que se generan en la consola de NetScaler.
- 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 generar el informe. También puede configurar una lista de distribución de correo electrónico a la que quiere 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 Console permite ver los 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.

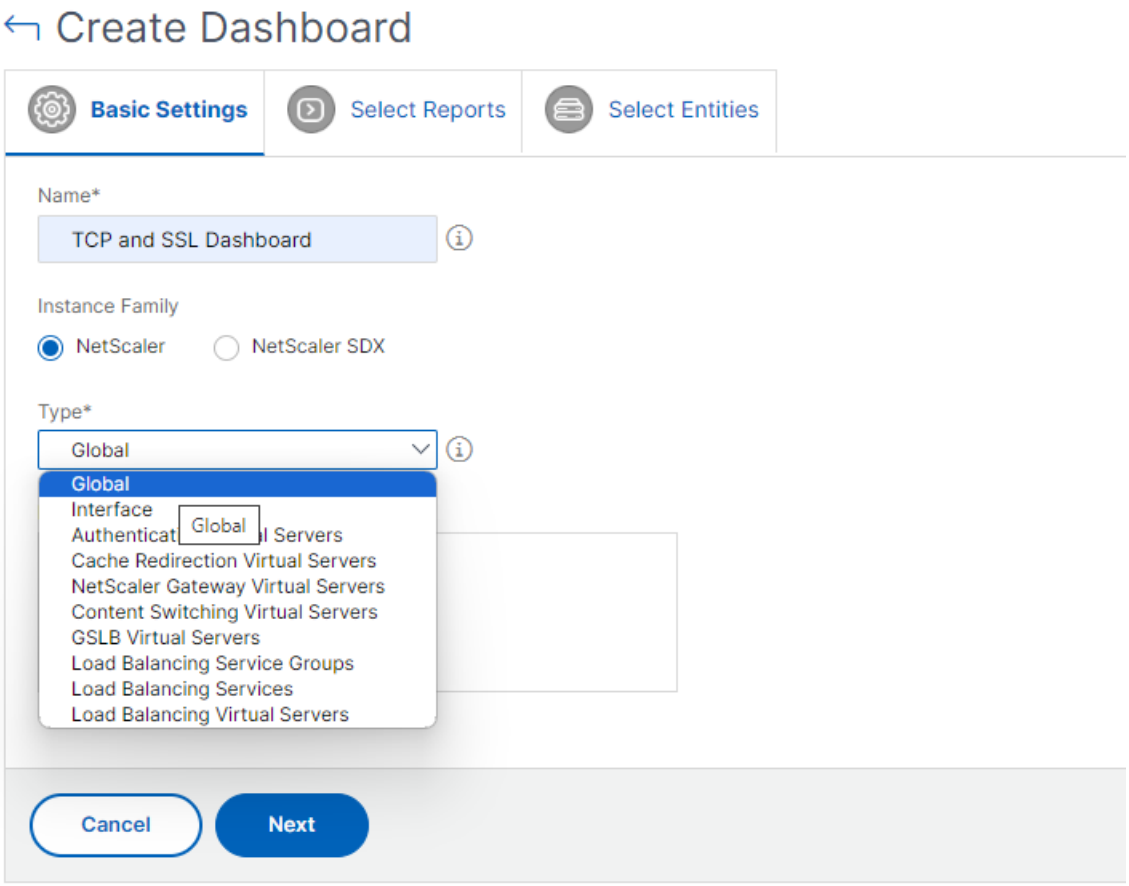
Para ver o crear un tablero de mandos:

1. En NetScaler Console, 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 **Crear 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.

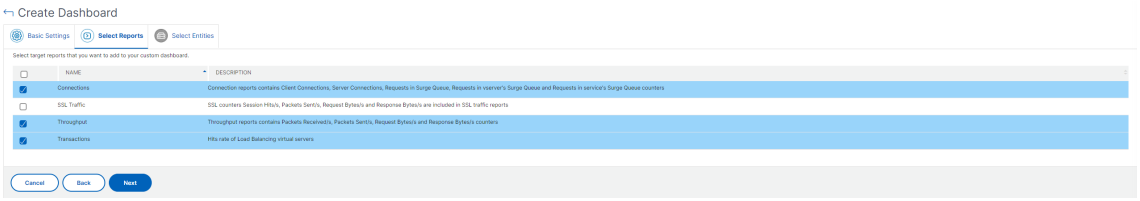
   <!–1. **Familia**de instancias . Seleccione el tipo de instancia: NetScaler, Citrix SD-WAN o NetScaler SDX. —>

   a) **Escriba**. Seleccione el tipo de entidad para el que quiere generar informes. En este ejemplo, seleccione servidores virtuales de equilibrio de carga.

   b) **Descripción**. Escriba una descripción significativa para el panel de control.

5. Haga clic en **Siguiente**.

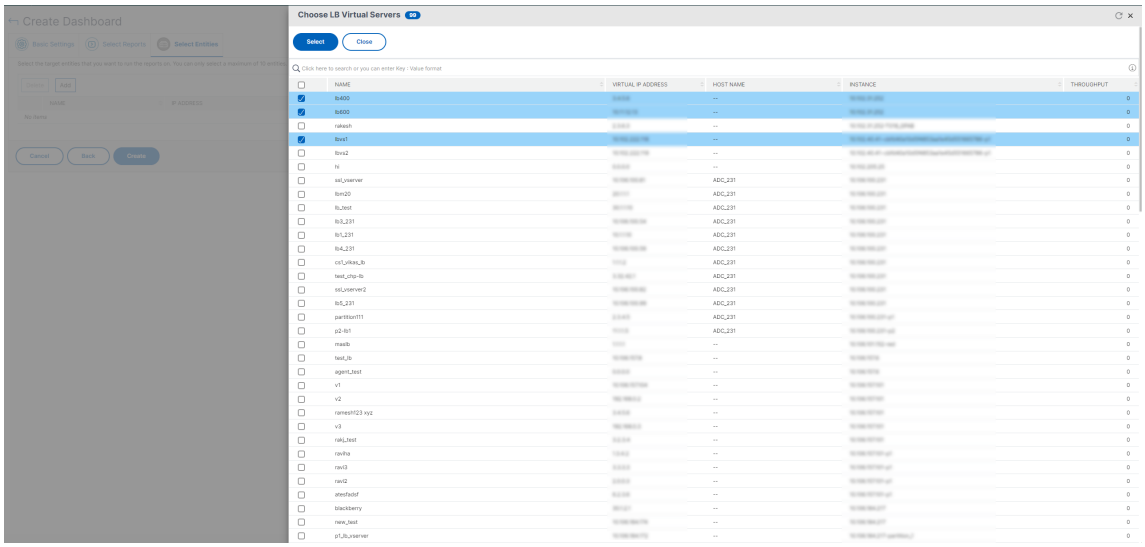
6. En la ficha **Seleccionar informes**, seleccione los informes necesarios. En este ejemplo, puede seleccionar las transacciones, las conexiones y el rendimiento. Haga clic en **Siguiente**.



7. 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 **Elegir servidores virtuales LB**.

8. Seleccione las entidades que quiere supervisar.



9. Haga clic en **Crear**.

Se crea el panel de control y muestra todos los informes que ha seleccionado.

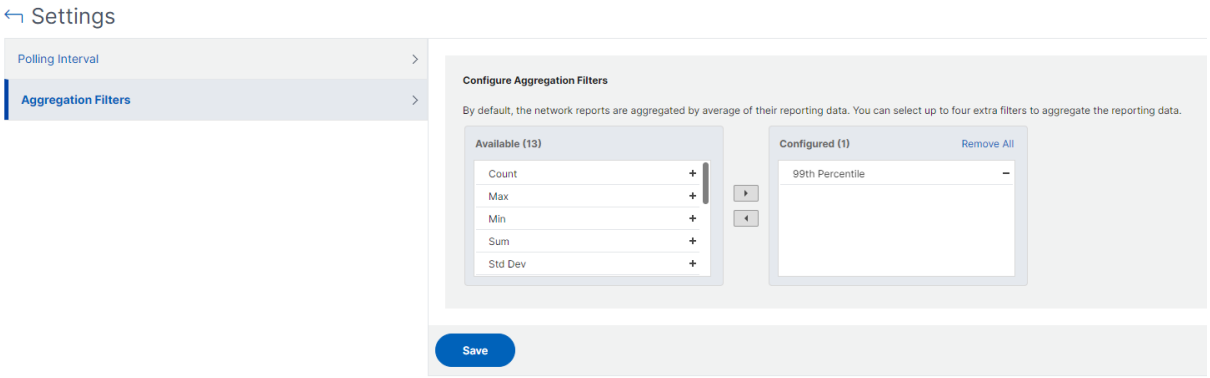
> **Nota**
>
> Actualmente, los cambios que realice en leyendas o filtros no se pueden guardar.

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. Con estas agregaciones aplicadas a los datos, puede analizar y comprobar si 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. Tras añadir las opciones de agregación, NetScaler Console tarda aproximadamente 1 hora en generar informes para las opciones de agregación seleccionadas.

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 Console si tiene permisos de solo lectura. Necesita un permiso de edición para crear un archivo en NetScaler Console y 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 **Panel de informes de red** de forma periódica. 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, seleccione los días de la semana en los que quiera programar el informe.
> - Si selecciona Periodicidad mensual, introduzca todos los días en los que quiera programar el informe separados por comas.

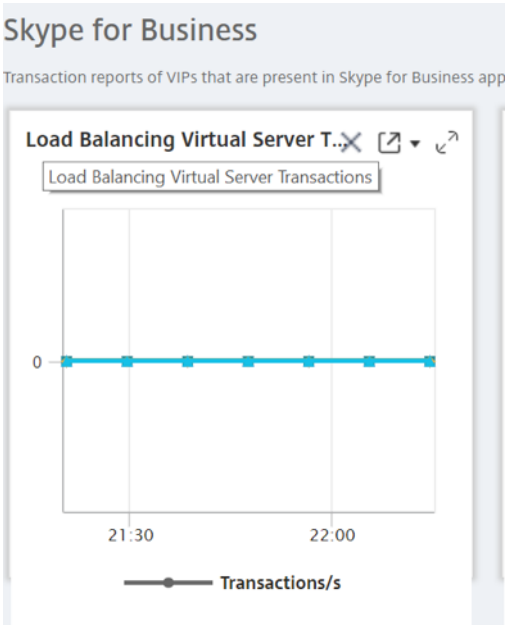
Al programar informes de red, puede personalizar el encabezado del informe escribiendo una cadena de texto en el campo **Asunto**. El informe creado a la hora programada tiene esta cadena como nombre.

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.

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 gestionar los umbrales de los informes de red en NetScaler Console

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 Console, puede configurar los umbrales y verlos, editarlos 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:

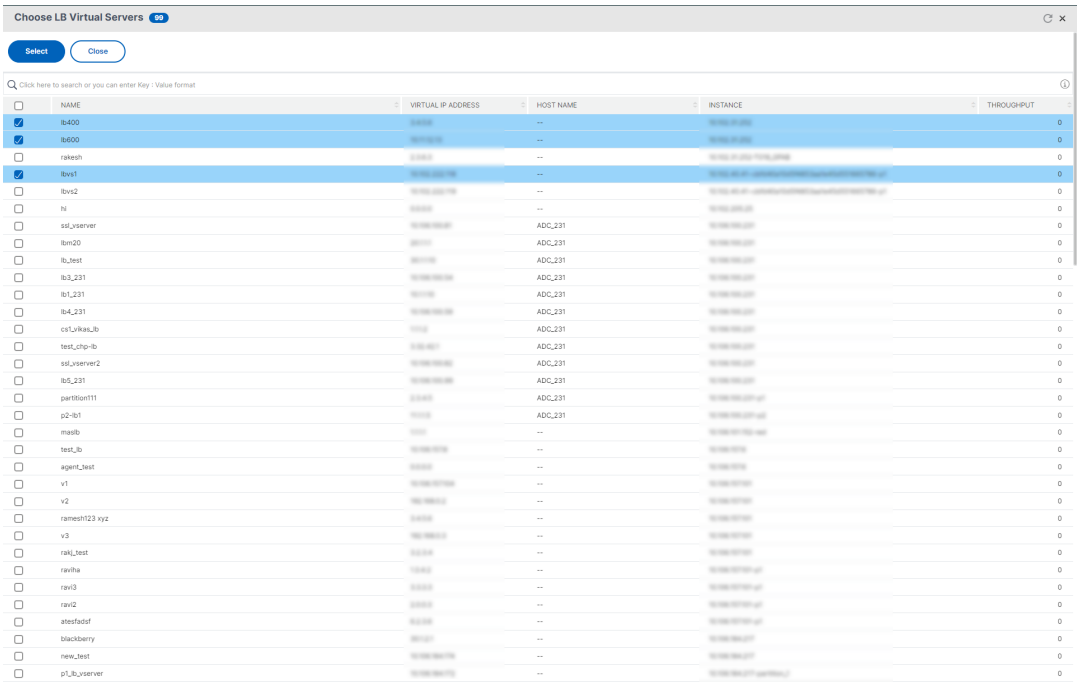
1. En NetScaler Console, vaya a **Infraestructura > Informes de red > Umbrales** . En **Umbrales**, haga clic en **Agregar**.
2. En la página **Crear umbral**, especifique los siguientes detalles:
    - **Nombre**. Nombre del umbral.
    - **Tipo de instancia**. Una instancia de NetScaler.
    - **Nombre 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. Para ver los eventos de "gravedad crítica", 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.
    - **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**.

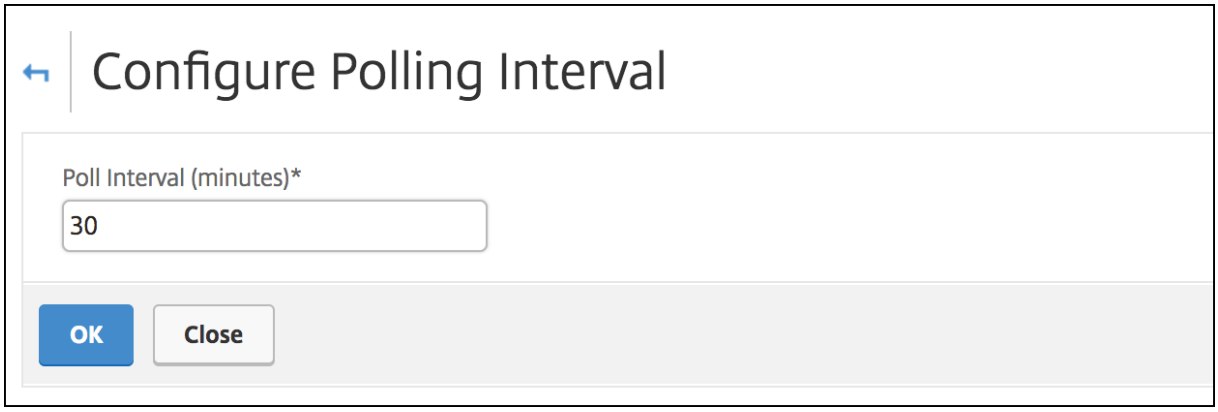
5. Puede elegir que aparezca un mensaje cuando se alcance el umbral. En la sección **Mensaje de evento**, escriba el mensaje en el cuadro de mensajes. NetScaler Console añade el valor supervisado y el valor de umbral a este mensaje.
6. En la sección **Configuración de notificaciones**, seleccione **Habilitar umbral** para habilitar el umbral para generar alarmas. Si quiere, puede seleccionar **Notificar por correo electrónico** para recibir notificaciones a través de varios canales, como correo electrónico, Slack, ServiceNow o PageDuty, cuando se alcance el umbral.

7. Haga clic en **Crear**.

Establecer el intervalo de sondeo de rendimiento para los informes

De forma predeterminada, cada 5 minutos, las llamadas NITRO recopilan datos de rendimiento para la generación de informes de red. La consola de NetScaler recupera las estadísticas de las instancias, como la información de los contadores, y las agrega por minuto, hora, día o semana. Puede ver estos datos agregados en informes predefinidos.

Para configurar 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 purga de los datos de los informes de red en NetScaler Console. Este intervalo limita la cantidad de datos de informes de red que se almacenan en la base de datos del servidor de NetScaler Console. De forma predeterminada, la poda ocurre cada 24 horas (a las 01.00 horas) para la red que informa de datos históricos.

> **Nota**
>
> El valor que puede especificar no puede superar los 90 días ni ser inferior a 1 día.

Provisioning de instancias VPX de NetScaler en AWS

January 26, 2024

Cuando traslada sus aplicaciones a la nube, los componentes que forman parte de la aplicación aumentan, se distribuyen más y deben gestionarse de forma dinámica.

Con las instancias VPX de NetScaler en AWS, puede ampliar sin problemas su pila de red L4-L7 a AWS. Con NetScaler VPX, AWS se convierte en una extensión natural de su infraestructura de TI local. Puede usar NetScaler VPX en AWS para combinar la elasticidad y la flexibilidad de la nube, con las mismas funciones de optimización, seguridad y control que admiten los sitios web y las aplicaciones más exigentes del mundo.

Con la consola NetScaler que monitorea sus instancias de NetScaler, obtiene visibilidad del estado, el rendimiento y la seguridad de sus aplicaciones. Puede automatizar la configuración, la implementación y la administración de su infraestructura de entrega de aplicaciones en entornos híbridos de múltiples nubes.

Terminología de AWS

La siguiente sección proporciona una breve descripción de los términos de AWS utilizados en este documento:

Término	Definición
Imagen de máquina de Amazon (AMI)	Una imagen de máquina, que proporciona la información necesaria para lanzar una instancia, que es un servidor virtual en la nube.
Nube de computación elástica (EC2)	Un servicio web que proporciona una capacidad informática segura y de tamaño variable en la nube. Está diseñado para que la informática en la nube a escala web sea más fácil para los desarrolladores.
Interfaz de red elástica (ENI)	Una interfaz de red virtual que se puede adjuntar a una instancia de una VPC.
Tipo de instancia	Amazon EC2 ofrece una amplia selección de tipos de instancias optimizados para adaptarse a diferentes casos de uso. Los tipos de instancias comprenden distintas combinaciones de capacidad de CPU, memoria, almacenamiento y red, y le ofrecen la flexibilidad de elegir la combinación de recursos adecuada para sus aplicaciones.

Término	Definición
Función de gestión de identidades y accesos (IAM)	Una identidad de AWS con directivas de permisos que determinan lo que la identidad puede y no puede hacer en AWS. Puede utilizar un rol de IAM para permitir que las aplicaciones que se ejecutan en una instancia de EC2 accedan de forma segura a los recursos de AWS.
Grupos de seguridad	Conjunto con nombre de conexiones de red entrantes permitidas para una instancia.
Subredes	Un segmento del rango de direcciones IP de una VPC al que se pueden conectar las instancias de EC2. Puede crear subredes para agrupar las instancias según las necesidades operativas y de seguridad.
Nube privada virtual (VPC)	Un servicio web para Provisioning una sección aislada lógicamente de la nube de AWS donde puede lanzar recursos de AWS en una red virtual que defina.

Requisitos previos

Este documento asume lo siguiente:

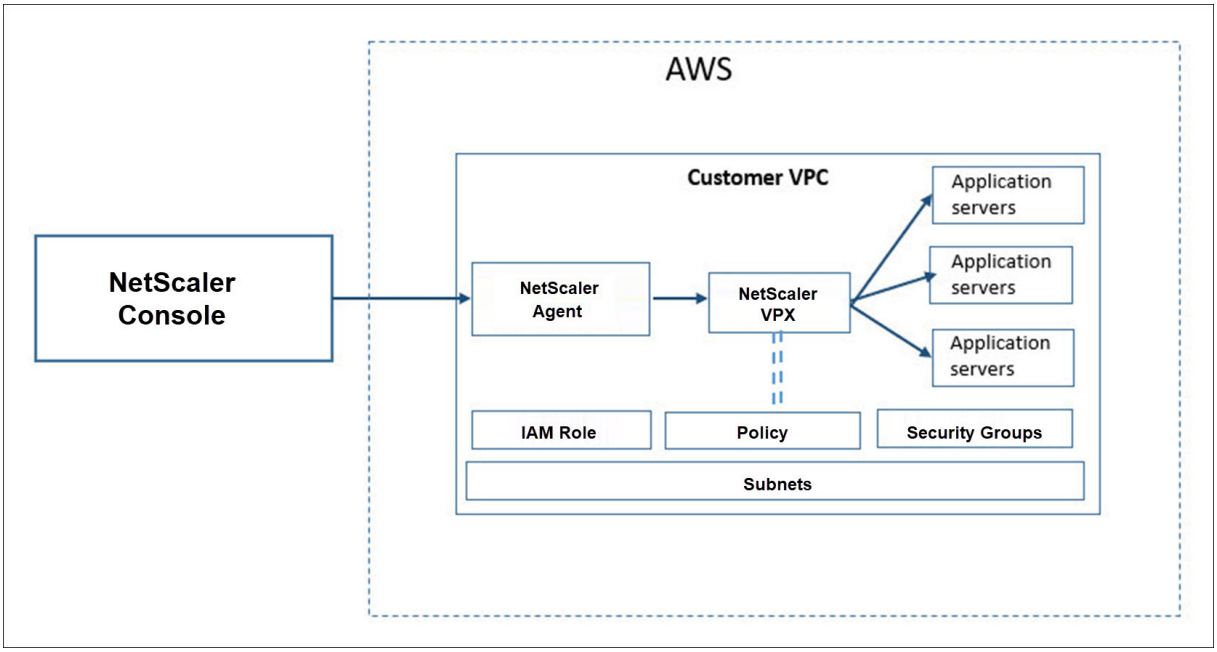
- Posee una cuenta de AWS.
- Ha creado la VPC necesaria y ha seleccionado las zonas de disponibilidad.
- Ha agregado el agente en AWS.

Para obtener más información sobre cómo crear una cuenta y otras tareas, consulte la documentación de AWS.

Para obtener más información sobre cómo instalar un agente en AWS, consulte Instalar un agente de NetScaler en AWS.

Diagrama de arquitectura

La siguiente imagen ofrece una descripción general de cómo NetScaler Console se conecta con AWS para aprovisionar instancias de NetScaler VPX en AWS.



Tareas de configuración

Realice las siguientes tareas en AWS antes de aprovisionar instancias de NetScaler VPX en NetScaler Console:

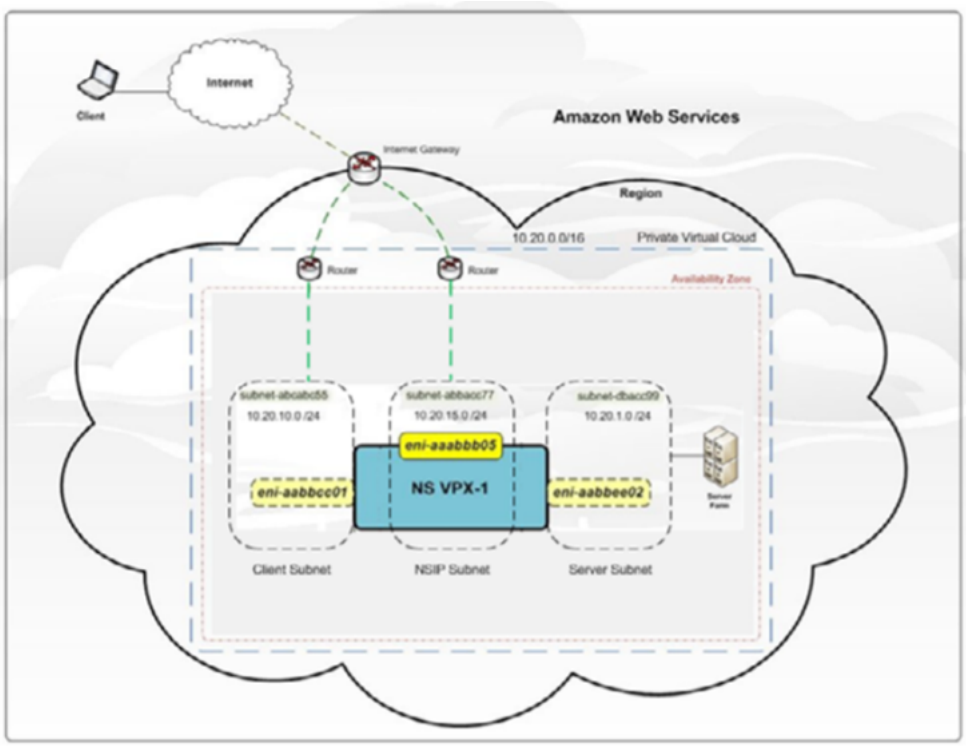
- Crear subredes
- Crear grupos de seguridad
- Crear un rol de IAM y definir una directiva

Realice las siguientes tareas en la consola de NetScaler para aprovisionar las instancias en AWS:

- Crear sitio
- Aprovisione la instancia NetScaler VPX en AWS

Para crear subredes

Cree tres subredes en su VPC. Las tres subredes que se requieren para aprovisionar instancias de NetScaler VPX en su VPC son la administración, el cliente y el servidor. Especifique un bloque CIDR IPv4 del rango definido en la VPC para cada una de las subredes. Especifique la zona de disponibilidad en la que quiere que resida la subred. Cree las tres subredes en la misma zona de disponibilidad. La imagen siguiente ilustra las tres subredes creadas en su región y su conectividad con el sistema cliente.



Para obtener más información sobre VPC y subredes, consulte VPC y subredes.

Para crear grupos de seguridad

Cree un grupo de seguridad para controlar el tráfico entrante y saliente en la instancia de NetScaler VPX. Un grupo de seguridad actúa como un firewall virtual para su instancia. Cree grupos de seguridad en el nivel de instancia y no en el nivel de subred. Es posible asignar cada instancia de una subred de la VPC a un conjunto diferente de grupos de seguridad. Agregue reglas para cada grupo de seguridad para controlar el tráfico entrante que pasa a través de la subred del cliente a las instancias. También puede agregar un conjunto independiente de reglas que controlen el tráfico saliente que pasa a través de la subred del servidor a los servidores de aplicaciones. Aunque puede usar el grupo de seguridad predeterminado para sus instancias, es posible que quiera crear sus grupos. Cree tres grupos de seguridad: Uno para cada subred. Crea reglas para el tráfico entrante y saliente que quieras controlar. Puede agregar cuantas reglas quiera.

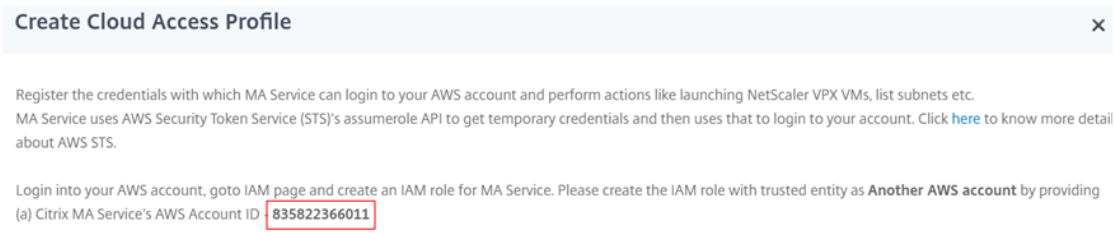
Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad para su VPC.

Para crear un rol de IAM y definir una directiva

Cree un rol de IAM para que pueda establecer una relación de confianza entre sus usuarios y la cuenta de AWS de confianza de Citrix y cree una directiva con permisos de Citrix.

1. En AWS, haga clic en **Servicios** . En el panel de navegación del lado izquierdo, seleccione **IAM > Roles**y haga clic en **Crear rol**.
2. Va a conectar su cuenta de AWS con la cuenta de AWS en NetScaler Console. Por lo tanto, seleccione **Otra cuenta de AWS** para permitir que NetScaler Console realice acciones en su cuenta de AWS.

   Escriba el identificador de cuenta AWS de 12 dígitos de NetScaler Console. El ID de Citrix es 835822366011. También puede encontrar el ID de Citrix en NetScaler Console al crear el perfil de acceso a la nube.



3. Habilite **Requerir ID externo** para conectarse a una cuenta de terceros. Puede aumentar la seguridad de su función solicitando un identificador externo opcional. Escriba un ID que puede ser una combinación de caracteres.
4. Haga clic en **Permisos**.
5. En la página **Adjuntar directivas de permisos**, haga clic en **Crear directiva**.
6. Puede crear y modificar una directiva en el editor visual o mediante JSON.

   La lista de permisos de Citrix se proporciona en el cuadro siguiente:

```
{

"Version": "2012-10-17",
"Statement":
[
    {

          "Effect": "Allow",
         "Action": [
             "ec2:DescribeInstances",
             "ec2:DescribeImageAttribute",
             "ec2:DescribeInstanceAttribute",
             "ec2:DescribeRegions",
             "ec2:DescribeDhcpOptions",
             "ec2:DescribeSecurityGroups",
             "ec2:DescribeHosts",
             "ec2:DescribeImages",
             "ec2:DescribeVpcs",
             "ec2:DescribeSubnets",
             "ec2:DescribeNetworkInterfaces",
             "ec2:DescribeAvailabilityZones",
```



```
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeInstanceStatus",
                "ec2:DescribeAddresses",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeTags",
                "ec2:DescribeVolumeStatus",
                "ec2:DescribeVolumes",
                "ec2:DescribeVolumeAttribute",
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:CreateKeyPair",
                "ec2:DeleteKeyPair",
                "ec2:ResetInstanceAttribute",
                "ec2:RunScheduledInstances",
                "ec2:ReportInstanceStatus",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:UnmonitorInstances",
                "ec2:MonitorInstances",
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:CreateNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:DetachNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ResetNetworkInterfaceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:AssociateAddress",
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:DisassociateAddress",
                "ec2:GetConsoleOutput"
            ],
                "Resource": "*"
        }

    ]
     }
```

7. Copie y pegue la lista de permisos en la ficha JSON y haga clic en **Revisar directiva**.
8. En la página **Revisar directiva**, escriba un nombre para la directiva, introduzca una descripción y haga clic en **Crear directiva**.

Para crear un sitio en NetScaler Console

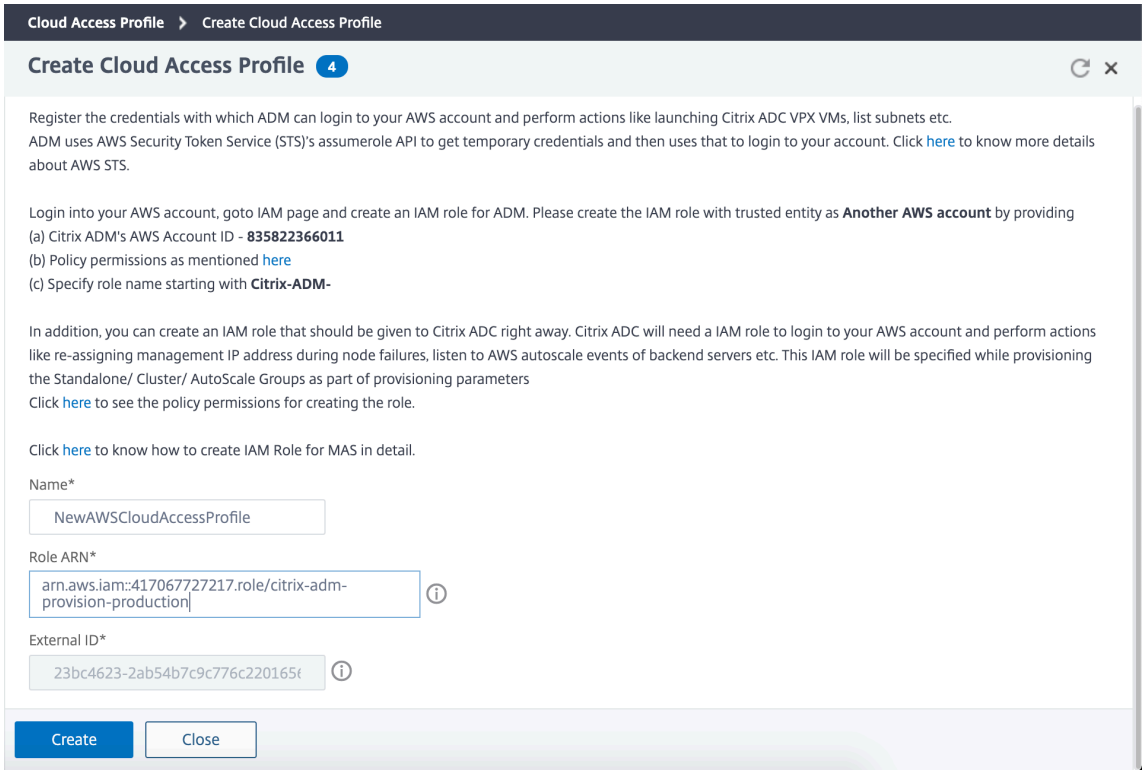
Cree un sitio en NetScaler Console y añada los detalles de la VPC asociada a su rol de AWS.

1. En NetScaler Console, vaya a **Infraestructura > Sitios**.
2. Haga clic en **Agregar**.
3. Seleccione el tipo de servicio como AWS y habilite **Usar la VPC existente como sitio**.
4. Seleccione el perfil de acceso a la nube.
5. Si el perfil de acceso a la nube no existe en el campo, haga clic en **Agregar** para crear un perfil.

   a) En la página **Crear perfil de acceso a la nube**, escriba el nombre del perfil con el que quiere acceder a AWS.

   b) Escriba el ARN asociado al rol que ha creado en AWS.

   c) Escriba el ID externo que proporcionó al crear un rol de administración de identidades y acceso (IAM) en AWS. Consulte el paso 4 en Para crear un rol de IAM y definir una tarea de directiva. Asegúrese de que el nombre de rol de IAM especificado en AWS comience por "Citrix-ADM-"y aparezca correctamente en el ARN de rol.



   Los detalles de la VPC, como la región, el ID de VPC, el nombre y el bloque de CIDR, asociados a su rol de IAM en AWS se importan en NetScaler Console.

6. Escriba un nombre para el sitio.
7. Haga clic en **Crear**.

Para aprovisionar NetScaler VPX en AWS

Utilice el sitio que creó anteriormente para aprovisionar las instancias VPX de NetScaler en AWS. Proporcione los detalles del agente para aprovisionar las instancias vinculadas a ese agente.

1. En NetScaler Console, vaya a **Infraestructura > Instancias > NetScaler**.
2. En la ficha **VPX**, haga clic en **Aprovisionar**.

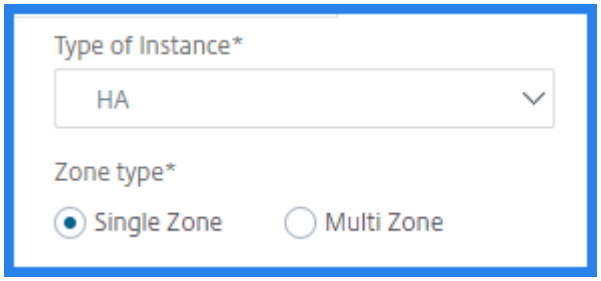
   Esta opción muestra la página **Provisionar NetScaler VPX on Cloud**.
3. Seleccione **Amazon Web Services (AWS)** y haga clic en **Siguiente**.
4. En la ficha **Parámetros básicos**,

   a) Seleccione el **tipo de instancia** de la lista.

   - **Independiente:** esta opción proporciona una instancia de NetScaler VPX independiente en AWS.
   - **HA:** Esta opción aprovisiona las instancias de NetScaler VPX de alta disponibilidad en AWS.

     Para aprovisionar las instancias VPX de NetScaler en la misma zona, seleccione la opción **Zona única** en **Tipo de zona**.

     Para aprovisionar las instancias de NetScaler VPX en varias zonas, seleccione la opción Multizona en Tipo de zona**.** En la ficha **Parámetros de provisión**, asegúrese de especificar los detalles de red para cada zona creada en AWS.



   b) Especifique el nombre de una instancia de NetScaler VPX.

   c) En **Sitio**, seleccione el sitio que creó anteriormente.

   d) En **Agente**, seleccione el agente que se creó para administrar la instancia de NetScaler VPX.

   e) En **Perfil de acceso a la nube**, seleccione el perfil de acceso a la nube creado durante la creación del sitio.

   f) En **Perfil del dispositivo**, seleccione el perfil para proporcionar la autenticación.

   NetScaler Console usa el perfil del dispositivo cuando es necesario iniciar sesión en la instancia de NetScaler VPX.

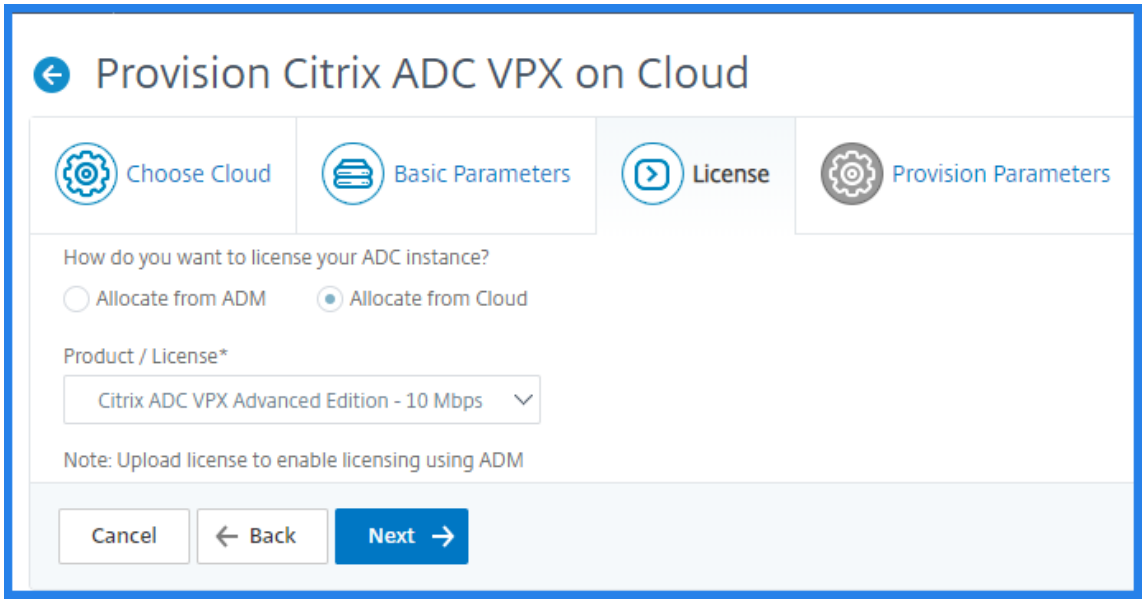
g) Haga clic en **Siguiente**.

5. En la pestaña **Licencia** , seleccione uno de los siguientes modos para aplicar la licencia a una instancia de NetScaler:

   - **Uso de NetScaler Console**: la instancia que desea aprovisionar comprueba las licencias de NetScaler Console.
   - **Uso de la nube de AWS**: la opción **Asignar desde la nube** utiliza las licencias de productos de NetScaler disponibles en el mercado de AWS. La instancia que quiere aprovisionar utiliza las licencias del mercado.

     Si decide utilizar licencias del mercado de AWS, especifique el producto o licencia en la ficha **Parámetros de aprovisionamiento**.

   Para obtener más información, consulte Requisitos de licencia.



6. En la pestaña **Licencia** , si selecciona **Asignar desde la consola de NetScaler** , especifique lo siguiente:

   - Tipo de licencia: seleccione licencias de ancho de banda o CPU virtual:

     Licencias de ancho de banda: puede seleccionar una de las siguientes opciones de la lista **Tipos de licencia de ancho de banda** :

     - **Capacidad agrupada:** especifique la capacidad que se asignará a una instancia.

       Desde el grupo común, la instancia de NetScaler extrae una licencia de instancia y solo se especifica la cantidad de ancho de banda.

     - **Licencias VPX:**cuando se aprovisiona una instancia de NetScaler VPX, la instancia extrae la licencia de la consola de NetScaler.

Licencias de CPU virtuales: la instancia de NetScaler VPX aprovisionada comprueba las licencias en función del número de CPU que se ejecutan en la instancia.

> **Nota** Cuando las instancias aprovisionadas se eliminan o destruyen, las licencias aplicadas vuelven al grupo de licencias de NetScaler Console. Estas licencias se pueden reutilizar para aprovisionar nuevas instancias.

a) En **Edición de licencia**, seleccione la edición de licencia. La consola de NetScaler usa la edición especificada para aprovisionar las instancias.

7. Haga clic en **Siguiente**.
8. En la ficha **Parámetros de aprovisionamiento**,

   a) Seleccione el **rol de Citrix IAM** creado en AWS. Un rol de IAM es una identidad de AWS con directivas de permisos que determinan lo que la identidad puede y no puede hacer en AWS.

   b) En el campo **Producto**, seleccione la versión del producto NetScaler que quiere aprovisionar.

   c) Seleccione el tipo de instancia EC2 de la lista de **tipos de instancia**.

      Esta lista muestra los tipos de instancias de AMI compatibles para la instancia de NetScaler seleccionada.

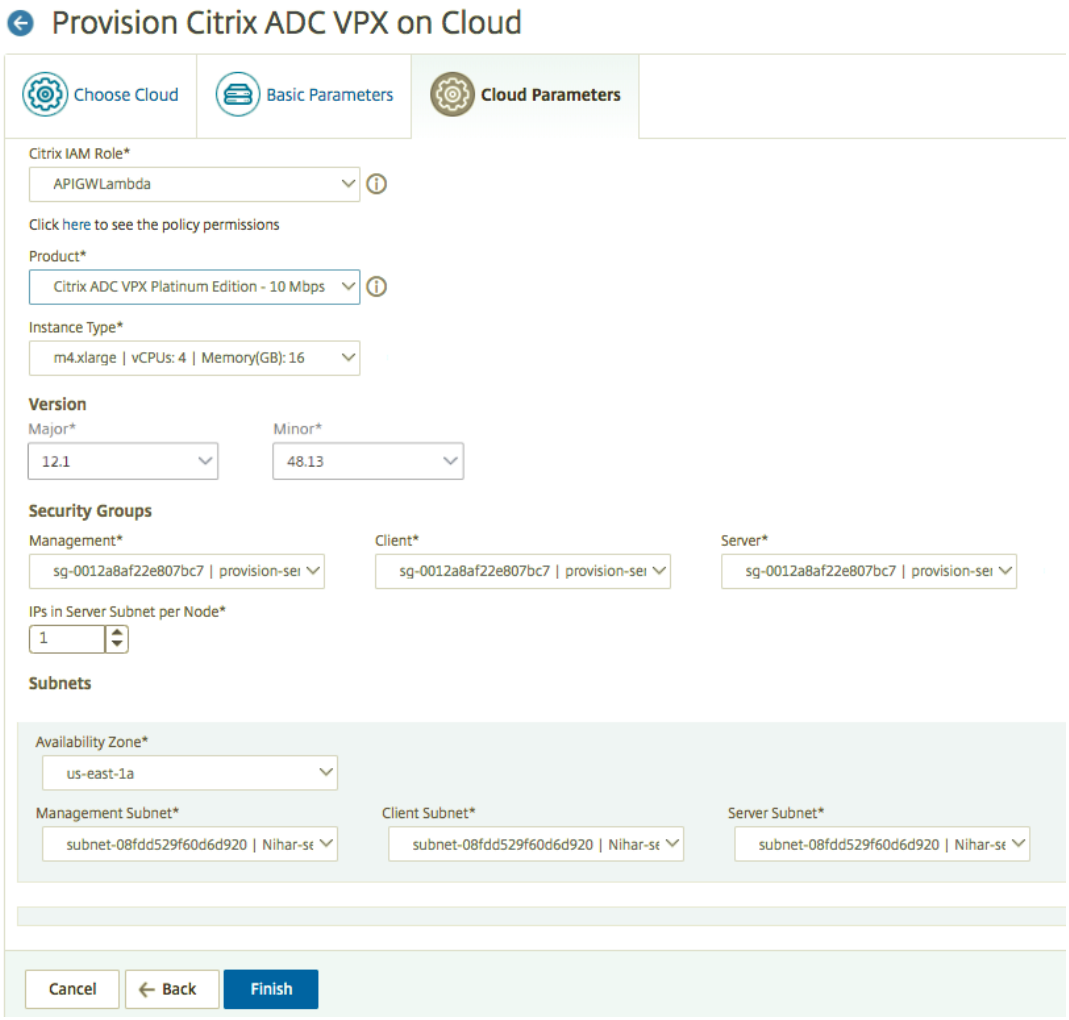
   d) Seleccione la **versión** de NetScaler que quiere aprovisionar. Seleccione la versión **principal** y la **secundaria** de NetScaler.

   e) En **Grupos de seguridad**, seleccione los grupos de seguridad de administración, cliente y servidor que ha creado en la red virtual.

   f) En **IPs en la subred del servidor por nodo**, seleccione el número de direcciones IP en la subred del servidor por nodo para el grupo de seguridad.

   g) En **Subredes**, seleccione las subredes de administración, cliente y servidor para cada zona que se cree en AWS. También puede seleccionar la región en la lista de **zonas de disponibilidad**.

   h) Haga clic en **Finalizar**.



La instancia de NetScaler VPX se aprovisiona ahora en AWS.

> **Nota**
>
> Actualmente, NetScaler Console no admite el desaprovisionamiento de instancias de NetScaler de AWS.

Para ver NetScaler VPX aprovisionado en AWS

1. En la página principal de AWS, vaya a **Servicios** y haga clic en **EC2**.
2. En la página **Recursos**, haga clic en **Instancias en ejecución**.
3. Puede ver NetScaler VPX aprovisionado en AWS.

El nombre de la instancia de NetScaler VPX es el mismo que proporcionó al aprovisionar una instancia en la consola de NetScaler.

Para ver el NetScaler VPX aprovisionado en NetScaler Console

1. En NetScaler Console, vaya a **Infraestructura > Instancias > NetScaler**.
2. Seleccione la ficha **NetScaler VPX**.
3. La instancia de NetScaler VPX aprovisionada en AWS se muestra aquí.

Autorizaciones autogestionadas del servicio App Delivery and Security de NetScaler

January 26, 2024

El servicio autogestionado de App Delivery and Security de NetScaler es la nueva forma de consumir licencias agrupadas, con un alto grado de automatización en la gestión de licencias y capacidades. Los clientes no necesitan gestionar las licencias de forma manual y obtener flexibilidad a la hora de gestionar sus necesidades de capacidad en múltiples nubes híbridas.

> **Requisitos previos**
>
> Asegúrese de que se cumplen los siguientes requisitos previos:
>
> - Asegúrese de tener el agente NetScaler registrado en el servicio NetScaler Console
> - Las versiones de NetScaler compatibles son:
>   - Versión 13.0: Utilice la versión 13.0 - 88.12 o posterior
>   - Versión 13.1: Utilice la versión 13.1 - 30.x o posterior
> - Está utilizando un agente de NetScaler 13.1 a 32.x o posterior

Como parte de la función autogestionada del servicio NetScaler App Delivery and Security, la información de la licencia se carga automáticamente al servicio NetScaler Console una vez que el cliente realiza una compra y crea un agente de NetScaler en el servicio NetScaler Console. Las licencias se descargan directamente al License Server Agent (LSA) o al agente de su VPC o centro de datos, como parte de la infraestructura de NetScaler Console.

> **Nota**
>
> El servicio autogestionado de NetScaler App Delivery and Security solo está disponible en el servicio NetScaler Console.

NetScaler Console puede alojar los derechos autogestionados existentes de Pooled y NetScaler App Delivery and Security Service. Para usar la licencia requerida, configure un servidor de licencias en el dispositivo NetScaler y extraiga o asigne la capacidad del grupo correspondiente.

El servicio de App Delivery and Security de NetScaler Self Managed incluye las siguientes funciones:

- Disponible en las ediciones Standard, Advanced y Premium
- NetScaler App Delivery and Security Citrix gestionó un derecho premium de 100 TB más de 8 millones de consultas DNS por cada grupo inicial autogestionado durante el primer año
- Los grupos de inicio incluyen 1 VIP por 1 Gbps o 1 VIP por cada vCPU comprada. Se pueden comprar VIP adicionales como complementos

Para obtener más información sobre las autorizaciones autogestionadas de NetScaler App Delivery and Security Service disponibles, vaya a **Infraestructura**> Autogestionada.

Puede configurar la dirección IP de un servidor de licencias en NetScaler de la siguiente manera:

- Uso de la CLI. Para obtener más información, consulte Configurar la licencia de grupo autogestionado mediante la CLI
- Uso de la GUI. Para obtener más información, consulte Configurar la licencia de grupo autogestionado mediante la GUI

Los clientes también pueden realizar un seguimiento de información como la caducidad de la licencia y el uso en el servicio NetScaler Console .

Asigne la capacidad autogestionada del servicio de entrega de aplicaciones y seguridad de NetScaler a las instancias de NetScaler

January 26, 2024

Puede asignar los derechos y la capacidad autogestionados del servicio App Delivery and Security de NetScaler de dos maneras:

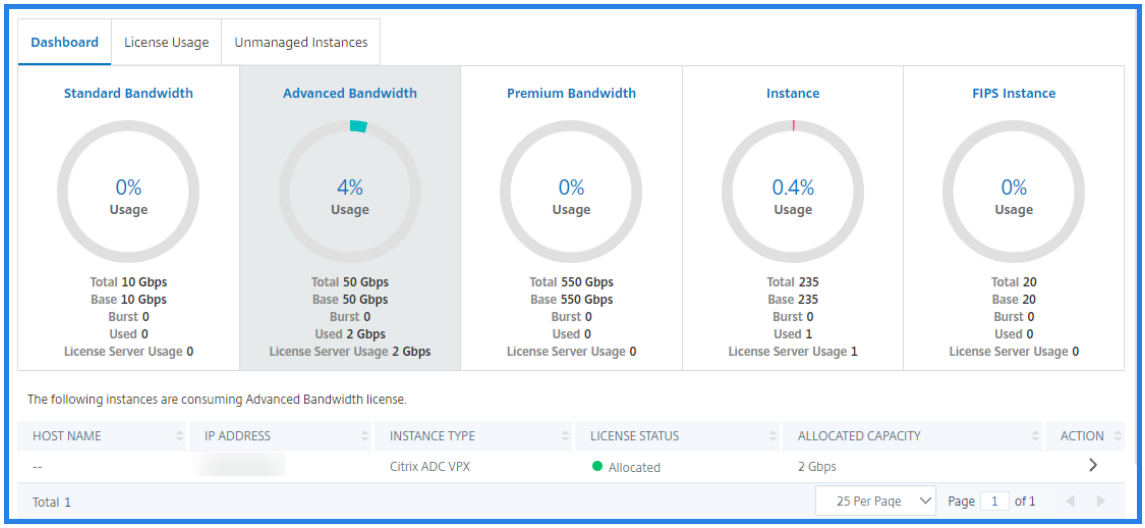
- Uso de la instancia de NetScaler
- Uso de ADM, si NetScaler está administrado por ADM.

Para asignar la capacidad autogestionada de NetScaler App Delivery and Security Service desde la GUI de NetScaler Console:

1. Inicie sesión en NetScaler Console.
2. Vaya a **Infraestructura > Autogestionado > Licencias de ancho de banda > Grupo autogestionado**.
3. Haga clic en el grupo de licencias que quiera administrar: Estándar, Avanzado o Premium.

> **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.

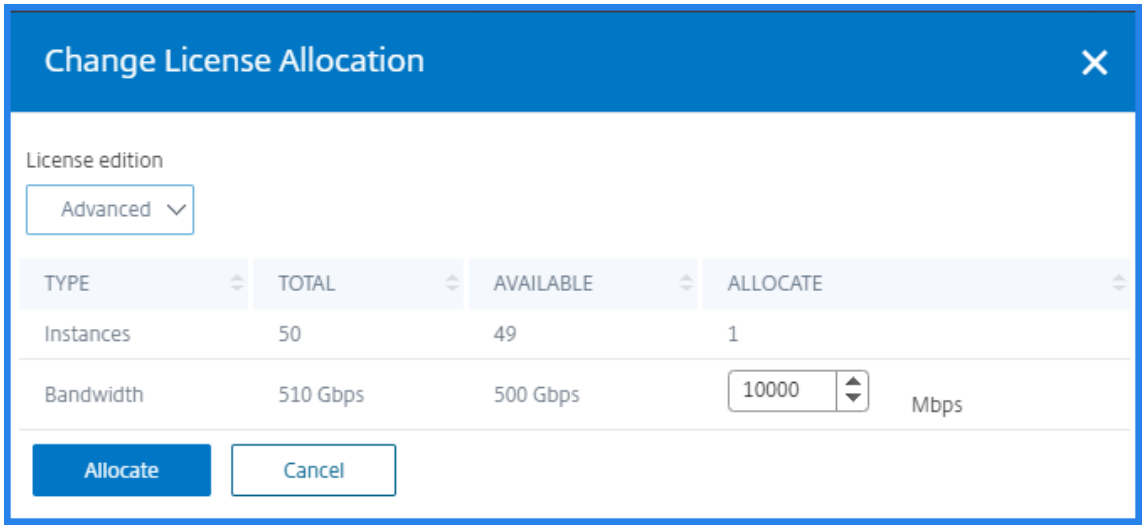
4. Seleccione una instancia de NetScaler de la lista de instancias disponibles haciendo clic en el botón **>**.



La columna Estado de la licencia muestra los mensajes de estado de asignación de derechos correspondientes.

> **Nota**
>
> La pestaña **Instancias** no administradas muestra las instancias que se descubren pero no se administran en NetScaler Console.

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. Elija el ancho de banda o la asignación de instancias a la instancia configurando las opciones de la lista de asignaciones. 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**.



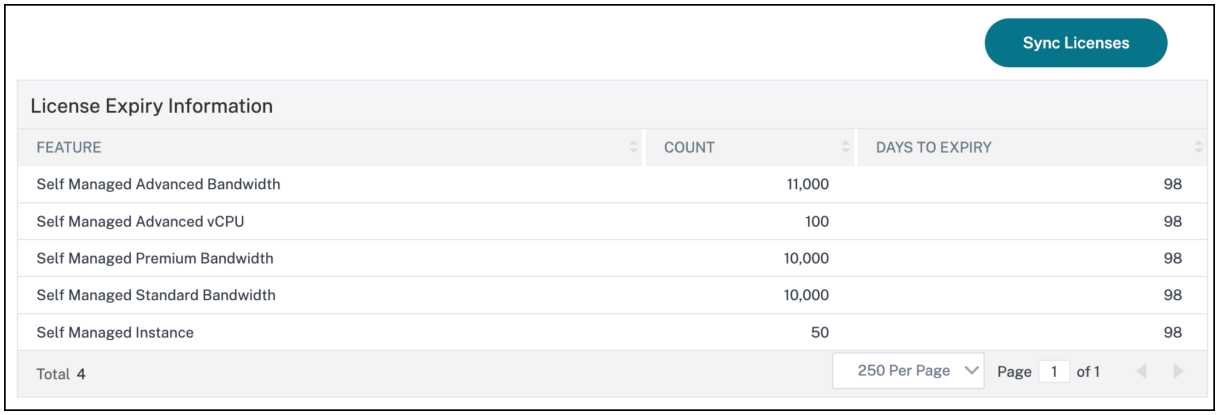
Nota

Reinicie en caliente una instancia si cambia la edición de la licencia.

Consulte la información sobre las autorizaciones autogestionadas de NetScaler App Delivery and Security Service

January 26, 2024

Para comprobar los derechos autogestionados del servicio NetScaler App Delivery and Security, disponibles en NetScaler Console, vaya a **Infraestructura > Autogestionado**.



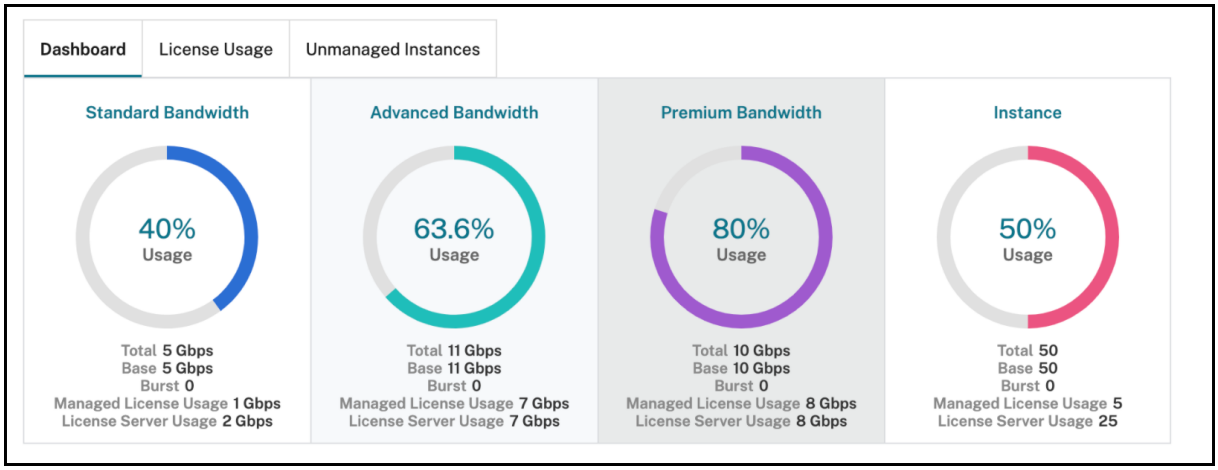
El panel muestra la información sobre las autorizaciones de autogestión de NetScaler App Delivery and Security Service. Si la información de derechos no aparece en el panel de control o hay un retraso en la adición de la información de derechos, haga clic en el botón **Sincronizar licencias** y aparecerá la información sobre los grupos de ancho de banda, el recuento y la caducidad disponibles.

Para obtener más información sobre cómo configurar las comprobaciones de caducidad de las licencias, consulte Configurar las comprobaciones

En la sección **Información sobre la caducidad de las licencias**, puede ver los detalles de las licencias que van a caducar

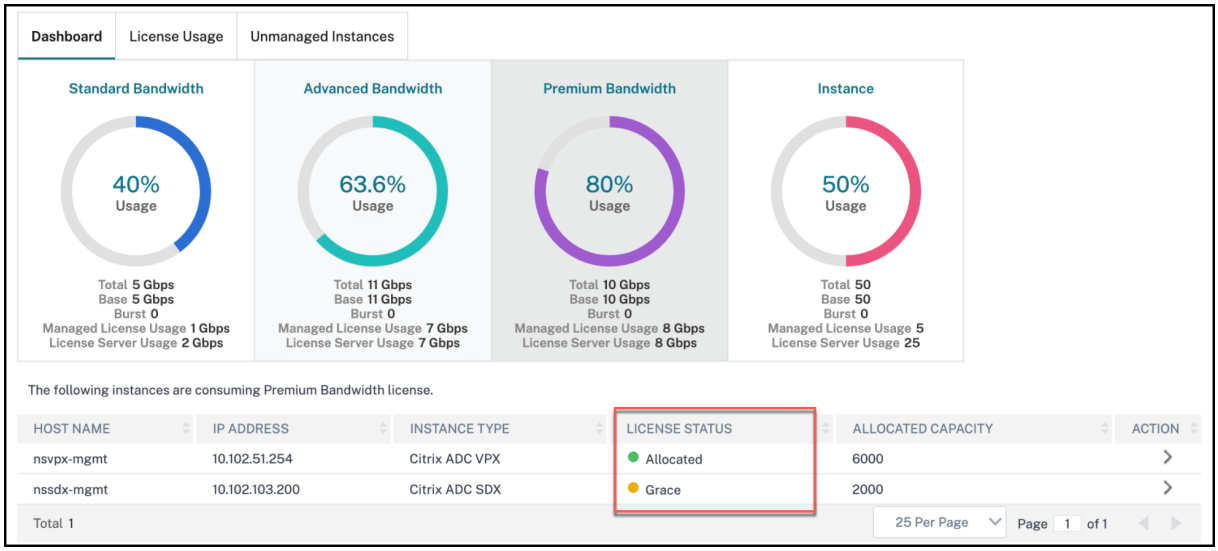
- **Función**: tipo de licencia que va a caducar.
- **Recuento**: número de servidores o instancias virtuales que se verán afectados.
- **Días hasta el vencimiento**: número de días antes del vencimiento de la licencia.

Para comprobar los grupos disponibles para las diferentes ediciones de licencias, vaya a **Infraestructura > Autogestionado > Licencias de ancho de banda > Grupo autogestionado**



Compruebe el uso de licencias

Si ha configurado NetScaler Console como servidor de licencias para la licencia de capacidad agrupada de NetScaler, puede usar la GUI de NetScaler Console para comprobar el estado de la licencia. Vaya a **Infraestructura > Autogestión > Capacidad agrupada > Uso de licencias**.



Para obtener más información sobre el tipo de estado de la licencia y su significado, consulte Comprobar el estado de la licencia.

Administre el clúster de Kubernetes para Service Graph

January 26, 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.

> **Nota**
>
> - NetScaler Console admite la visibilidad de los clústeres para Service Graph con las versiones 1.14—1.23 de Kubernetes.

Puede especificar los siguientes aspectos de la integración de Kubernetes en NetScaler Console:

- **Clúster**: puede registrar o anular el registro de clústeres de Kubernetes para los que NetScaler Console supervisa todos los microservicios y rellena el gráfico de servicios. Al registrar un clúster en NetScaler Console, especifique la información del servidor de la API de Kubernetes. A continuación, seleccione un agente que pueda llegar al clúster de Kubernetes.

Antes de comenzar

Para monitorear y visualizar sus microservicios en los clústeres de Kubernetes y comenzar a usar Service Graph, asegúrese de:

- Kubernetes agrupamiento en su lugar.
- El agente se instaló y configuró para permitir la comunicación entre NetScaler Console y el clúster de Kubernetes o las instancias administradas. Puede usar las instancias administradas que están presentes en su centro de datos o en la nube.
- Clúster de Kubernetes registrado en NetScaler Console.

Configurar el agente de NetScaler para que se registre en el clúster de Kubernetes

Para habilitar la comunicación entre el clúster de Kubernetes y NetScaler Console, debe instalar y configurar un agente. Puede desplegar un agente en las siguientes plataformas:

- Hipervisor (ESX, XenServer, KVM, Hyper-V)
- Servicios de nube pública (como Microsoft Azure, AWS)

Siga el procedimiento para configurar un agente.

> **Nota**
>
> También puede usar un agente existente si ya hay uno implementado.

Configure la consola de NetScaler con un token secreto para administrar un clúster de Kubernetes

Para que NetScaler Console pueda recibir eventos de Kubernetes, debe crear una cuenta de servicio en Kubernetes for NetScaler Console. Además, configure la cuenta de servicio con los permisos RBAC necesarios en el clúster.

1. Cree una cuenta de servicio para NetScaler Console. Por ejemplo, el nombre de la cuenta de servicio puede sercitrixadm-sa. Para crear una cuenta de servicio, consulte Usar varias cuentas de servicio.
2. Utilice la cluster-adminfunción para vincular la cuenta de NetScaler Console. 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
   ```

   Tras vincular la cuenta de NetScaler Console al rolcluster-admin, la cuenta de servicio tiene acceso a 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`:

   ```
   1 kubectl describe sa citrixadm-sa
   ```

4. Ejecute el siguiente comando para obtener la cadena secreta del token:

   ```
   1 kubectl describe secret <token-name>
   ```

Agregue el clúster de Kubernetes en NetScaler Console

Tras configurar un agente y configurar las rutas estáticas, debe registrar el clúster de Kubernetes en NetScaler Console.

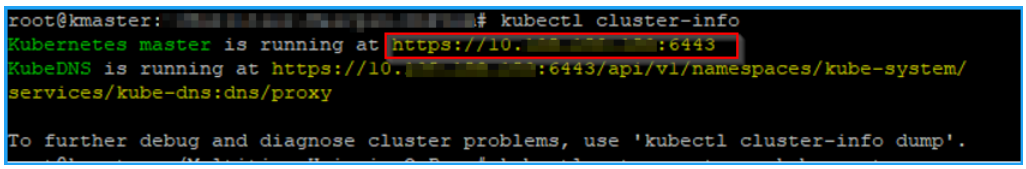
Para registrar el clúster de Kubernetes:

1. Inicie sesión en NetScaler Console con las 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 de API**: puede obtener los detalles de la URL del servidor de API en el nodo maestro de Kubernetes.

      i. En el nodo principal de Kubernetes, ejecuta 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 obtenida al configurar NetScaler Console 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 Console. Para generar un token de autenticación:

      i. En el nodo principal de Kubernetes, ejecuta los siguientes comandos:

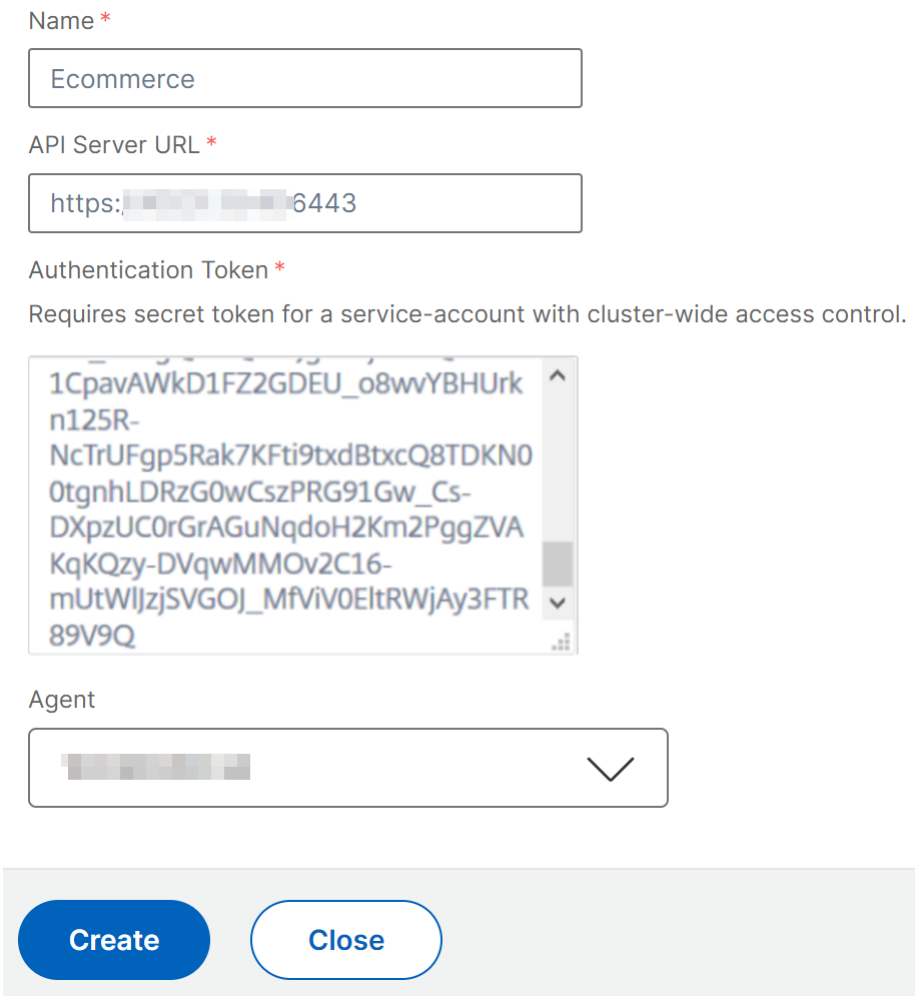

```
kubectl describe secret <token-name>
```

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**.



Administración de licencias para licencias Flexed y Pooled

September 2, 2024

> **Nota:**
>
> Al comprar una licencia Universal Hybrid Multicloud (UHMC) o Citrix Platform License (CPL), las licencias de NetScaler que se entregan se denominan licencias Flexed.

Archivos de licencias

La licencia Flexed de NetScaler incluye los siguientes archivos que debe descargar del portal MyCitrix. Para obtener más información sobre la transición del tipo actual de licencias de NetScaler a las licencias Flexed, consulte Transición al licenciamiento Flexed.

Los archivos de licencia presentes en su NetScaler se enumeran en esta sección.

El nombre del archivo contiene	Descripción	Descargar información	Dónde cargar/aplicar la licencia
Instancia de software NetScaler Flexed VPX	Le da derecho a disponer de instancias de software VPX/CPX/BLX	Descargue este archivo con su ID de host de NetScaler Console	En NetScaler Console
Instancia de software NetScaler MPX Flexed	Le da derecho a disponer de instancias de software MPX	Descargue este archivo con su ID de host de NetScaler Console	En NetScaler Console
Instancia de software NetScaler SDX Flexed	Le da derecho a utilizar instancias de software SDX	Descargue este archivo con su ID de host de NetScaler Console	En NetScaler Console
NetScaler Flexed Platinum BW	Le da derecho a la capacidad de procesamiento Flexed Platinum	Descargue este archivo con su ID de host de NetScaler Console	En NetScaler Console
Instancia de software NetScaler Flexed VPX FIPS	Le da derecho a instancias de software VPX FIPS	Descargue este archivo con su ID de host de NetScaler Console	En NetScaler Console
Licencia de plataforma MPX-Z de capacidad cero	Le permite hacer que su hardware NetScaler MPX participe en las licencias Flexed	Descargue este archivo	En NetScaler MPX
Licencia de plataforma SDX-Z de capacidad cero	Le permite hacer que su hardware NetScaler SDX participe en las licencias Flexed	Descargue este archivo	En NetScaler SDX

Puntos importantes que tener en cuenta

1. Si es un cliente de licencias Pooled que está haciendo la transición a las licencias Flexed y su hardware MPX y SDX ya tiene licencias perpetuas de Z-Cap, no necesita aplicar las licencias de Z-Cap recibidas con Flexed. Sin embargo, si las licencias Z-Cap actuales que se aplican a NetScaler MPX/NetScaler SDX son válidas durante un período específico, debe aplicar las licencias Z-Cap recibidas con la licencia Flexed. La licencia de software Flexed incluye la instancia de software NetScaler Flexed MPX/SDX/VPX/VPX FIPS y las licencias de ancho de banda NetScaler Flexed Platinum.
2. Debe aplicar las licencias Flexed en NetScaler Console para el formato de NetScaler que está utilizando en la implementación. Por ejemplo:

   Aplique las siguientes licencias si utiliza el formato NetScaler SDX:

Archivo de licencias	Se aplica a
Instancia de software NetScaler SDX Flexed	NetScaler Console
Instancia de software NetScaler Flexed VPX	NetScaler Console
NetScaler Flexed Platinum BW	NetScaler Console
Plataforma ADC SDX-Z de capacidad cero	NetScaler SDX

   Aplique las siguientes licencias si utiliza el formato NetScaler MPX:

Archivo de licencias	Se aplica a
Instancia de software NetScaler MPX Flexed	NetScaler Console
NetScaler Flexed Platinum BW	NetScaler Console
Plataforma MPX-Z ADC de capacidad cero	NetScaler MPX

   Aplique las siguientes licencias si utiliza el formato NetScaler VPX, NetScaler BLX o NetScaler CPX:

Archivo de licencias	Se aplica a
Instancia de software NetScaler Flexed VPX	NetScaler Console
NetScaler Flexed Platinum BW	NetScaler Console

   Aplique las siguientes licencias si utiliza el formato NetScaler VPX FIPS

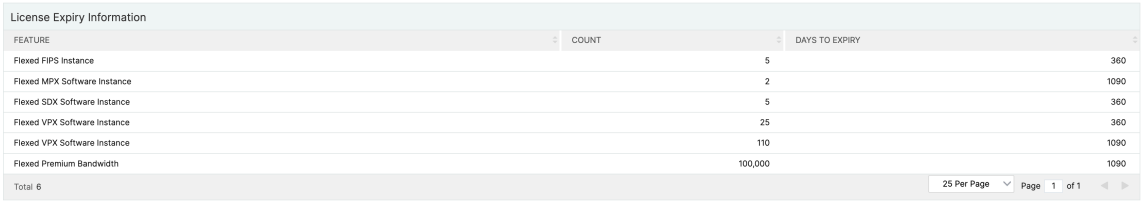
Archivo de licencias	Se aplica a
Instancia de software NetScaler Flexed VPX FIPS	NetScaler Console
NetScaler Flexed Platinum BW	NetScaler Console

Aplicar un archivo de licencia

Puede añadir, eliminar y descargar licencias. Debe aplicar las licencias antes de poder utilizarlas.

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 la consola de NetScaler.
   - **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 añaden a NetScaler Console.
   En la sección **Información de caducidad** de licencias se enumeran las licencias presentes en NetScaler Console, el recuento y los días que faltan para caducar.

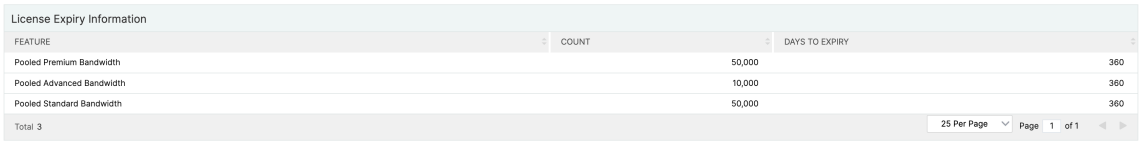
   La siguiente captura de pantalla muestra el número de licencias de instancias de software FIPS de Flexed NetScaler VPX, NetScaler MPX, NetScaler SDX y NetScaler VPX, la capacidad de ancho de banda premium de Flexed actual y los días que faltan para su vencimiento.

   
   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.

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Pooled Premium Bandwidth	50,000	360
Pooled Advanced Bandwidth	10,000	360
Pooled Standard Bandwidth	50,000	360

   Total 3 — 25 Per Page — Page 1 of 1
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.

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.

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 Console envía notificaciones por correo electrónico cuando una licencia está a punto de caducar. También se envían una captura SNMP y una notificación cuando la licencia ha caducado en NetScaler Console.

Se genera un evento cuando se envía una notificación de caducidad de licencia y este evento se puede ver en NetScaler Console 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:
    - **Función**: tipo de licencia que va a caducar.
    - **Recuento**: número de instancias o servidores virtuales que se verán 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 la asignación 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 como un porcentaje de la capacidad de licencias Flexed o Pooled que se asignará para enviar una notificación.
2. Seleccione el tipo de notificación que desea enviar cuando las licencias alcancen el umbral o estén a punto de caducar; para ello, seleccione la casilla correspondiente. Los tipos de notificación son los siguientes.

   - **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.
   - **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 actualmente es la única opción disponible.
     Para obtener más información sobre la creación de estos perfiles, consulte Configurar notificaciones

   Select a notification type and click **Add** to add details. You can also test each notification system before saving your settings.
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 la 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 Console envía el mensaje.
- **Para**: especifique las direcciones de correo electrónico a las que la consola NetScaler envía el mensaje.
- **Cc**: especifique las direcciones de correo electrónico en las que la consola de NetScaler copia el mensaje.
- **Bcc**: especifique las direcciones de correo electrónico en las que la consola NetScaler copia el mensaje a ciegas (no muestra la dirección de correo electrónico).

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 la consola 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, notificaciones push y llamadas telefónicas en un número registrado. Antes de añadir un perfil de PagerDuty en NetScaler Console, 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, debe integrar NetScaler Console con ServiceNow mediante el conector ITSM. Para obtener más información, consulte Integrar NetScaler Console 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.

> **Nota:**
>
> Para obtener información sobre los diferentes tipos de licencias de NetScaler, consulte Descripción general de las licencias.

Capacidad mínima y máxima para licencias Flexed y Pooled

April 10, 2024

Las licencias Flexed de NetScaler utilizan NetScaler Console configurada como un 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 mínima de ancho de banda para cada desprotección 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 en múltiplos de la unidad de ancho de banda mínima.

En las tablas 1 a 5 se resumen el ancho de banda máximo y las instancias, el ancho de banda mínimo y la unidad de ancho de banda mínima para todas las instancias de NetScaler compatibles. En la tabla 6 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 1. 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

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Unidad mínima de ancho de banda
MPX 15000Z	20	120	1 Gbps
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 2A. 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

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 25000Z-40G	100	200	20	115	1 Gbps
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 2B. 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

Línea de productos	Ancho de banda mínimo (Gbps)	Ancho de banda máximo (Gbps)	Instancias mínimas	Instancias máximas	Unidad mínima de ancho de banda
SDX 25000Z-40G	50	200	10	115	1 Gbps
SDX 26000Z	50	200	10	115	1 Gbps
SDX 2600Z-50S	50	200	10	115	1 Gbps
SDX 2600Z-100G	50	200	10	115	1 Gbps

Tabla 2C. 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

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	50	200	1	115	1 Gbps
SDX 2600Z-50S	50	200	1	115	1 Gbps
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 3. 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 4. 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
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 5. 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 6. 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	-

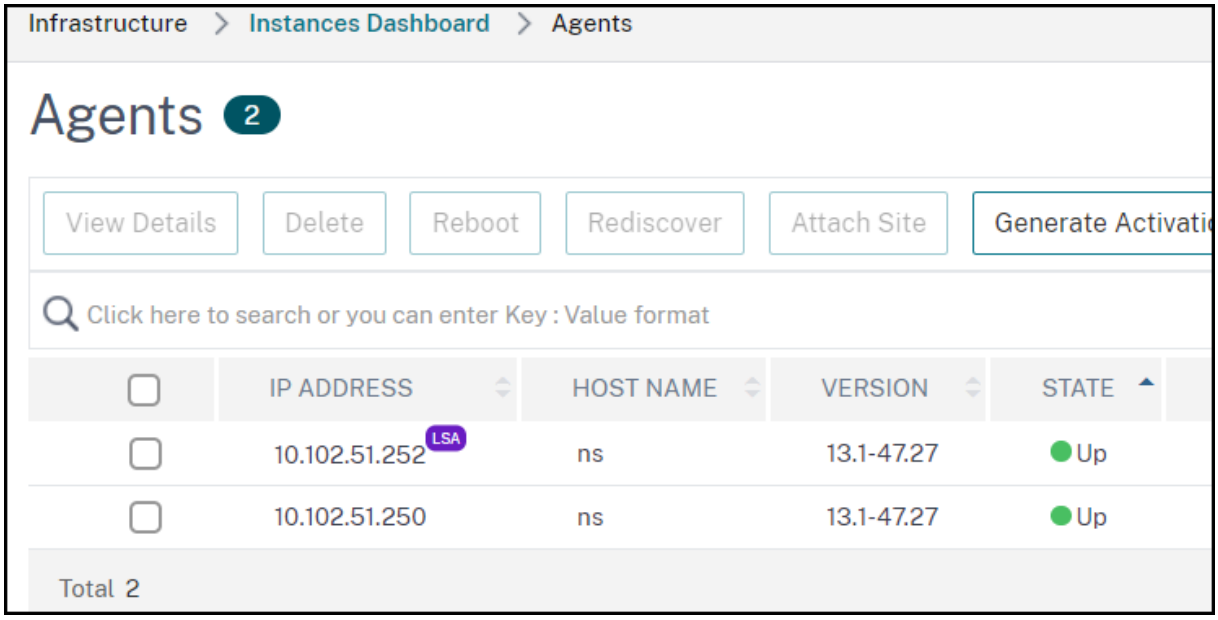
Línea de productos	Hardware de capacidad cero
CPX	-
BLX	-

Comportamiento de los agentes de NetScaler para licencias Flexed o Pooled

April 10, 2024

El agente NetScaler funciona como intermediario entre NetScaler Console y las instancias descubiertas en diferentes centros de datos y nubes públicas. El servicio NetScaler Console requiere un mínimo de un agente por inquilino para que funcionen las licencias Flexed o Pooled. Se pueden implementar varios agentes de NetScaler por sitio o en varios sitios, pero solo un agente puede tener el rol de agente del servidor de licencias (LSA) en todo el entorno del arrendatario.

El siguiente ejemplo muestra dos agentes desplegados y uno de ellos tiene el rol LSA:



Un LSA es un agente que funciona como servidor de licencias en la implementación de licencias agrupadas basada en el servicio NetScaler Console. Si el LSA deja de funcionar, el servicio espera 24 horas para elegir un nuevo LSA.

Hasta entonces, las instancias de NetScaler que utilizan licencias agrupadas o flexibles pasarán por un período de gracia. Como administrador, también puede elegir manualmente un LSA.

Seleccionar manualmente un agente de NetScaler Console como LSA

Los administradores pueden seleccionar manualmente un agente de NetScaler Console como LSA para las licencias NetScaler Pooled o NetScaler Flexed. Cuando el LSA está inactivo, el servicio NetScaler Console espera 24 horas antes de seleccionar automáticamente el siguiente LSA. El administrador puede elegir manualmente un nuevo LSA mientras tanto mediante esta función. Sin embargo, el administrador debe asegurarse de que el estado del nuevo LSA elegido sea ACTIVO y que su estado de diagnóstico sea correcto.

Cuando el administrador selecciona manualmente un nuevo LSA, la funcionalidad de licencias puede tardar hasta 5 minutos en funcionar correctamente. Durante este tiempo, las instancias de NetScaler están en un período y se produce un error al intentar reservar una nueva licencia.

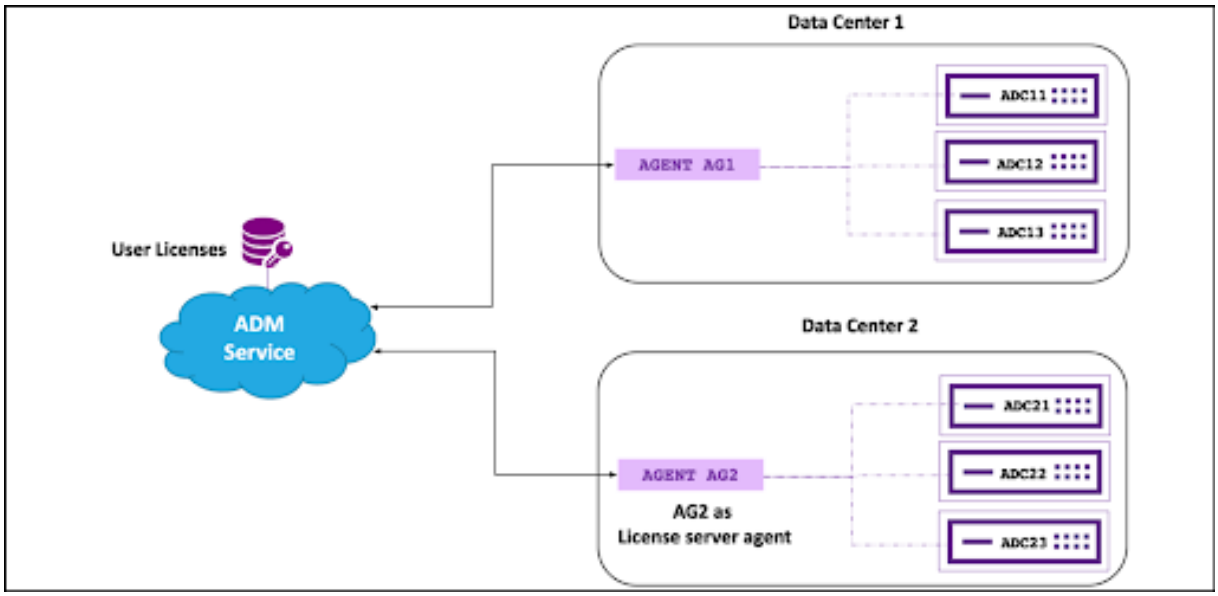
Para seleccionar un LSA:

1. Vaya a **Infrastructure > Instances Dashboard > Agents** y seleccione un agente.
2. En la lista **Select Action**, seleccione **Set as LSA**.
3. Haga clic en **Yes** para confirmar. El agente seleccionado asume el rol de LSA.

Comportamiento de varios agentes de NetScaler

En una implementación con una combinación de varios agentes y varios sitios, los agentes de NetScaler siguen la arquitectura cliente/servidor.

Al primer agente o al más antiguo registrado en un estado UP se le asigna la función LSA. Los demás agentes que se añadan posteriormente actúan como proxy y se comunican con el agente que desempeña el rol principal de LSA para la asignación de licencias. Cada agente que aloja el rol de proxy se comunica con el agente con el rol de LSA actual a través del servicio NetScaler Console.



> **Nota**
>
> No hay comunicación directa entre el agente que desempeña el rol de LSA y los demás agentes (que no son LSA). Todas las conexiones pasan únicamente por el servicio NetScaler Console.

Comportamiento de conmutación por error del agente de NetScaler

La conmutación por error del agente funciona en una implementación de varios agentes de la siguiente manera.

Supongamos que hay dos agentes, AG1 y AG2, en el mismo centro de datos.

- El AG1 está configurado para usar ADC11, ADC12 y ADC13 como host de licencias remotas o LSA.
- El AG2 está configurado para usar ADC21, ADC22 y ADC23 como host de licencias remotas o LSA.
- AG2 actúa como servidor de licencias.
  - Si AG1 falla, ADC11, ADC12 y ADC13 se conectan automáticamente a través de AG2 para la conciliación de licencias.
    - Es posible que el ADC11, el ADC12 y el ADC13 aún experimenten un pequeño período de gracia si se pierden algunos latidos mientras se produce esta reconexión.
  - Si el AG2 falla, todos los ADC permanecerán en estado de gracia hasta que:
    - O AG2 vuelve a activarse o AG1 se selecciona como el nuevo LSA de forma automática después de 24 horas mediante el servicio NetScaler Console o manualmente por el administrador.
    - O bien, AG2 se elimina del servicio NetScaler Console. Una vez cancelado el registro, el servicio NetScaler Console designa a AG1 como el agente con la función LSA.
    - Una vez finalizada la elección, AG1 comienza a asignar y conciliar recursos a las instancias configuradas.

Si tiene preguntas relacionadas con el LSA, consulte las preguntas frecuentes sobre License Server Agent.

Licencia flexible

April 10, 2024

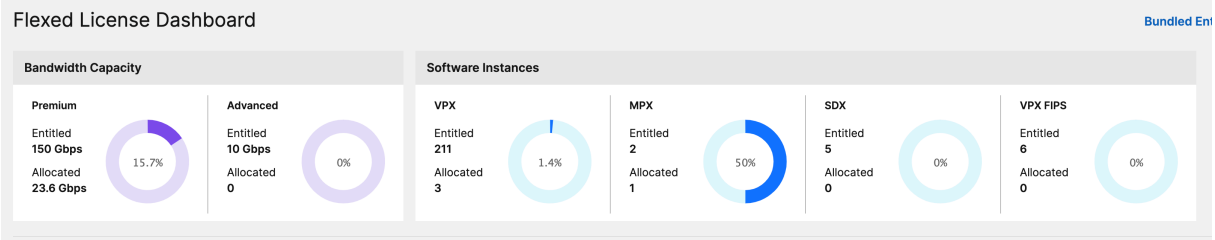
El licenciamiento Flexed de NetScaler es el nuevo marco de licenciamiento destinado a simplificar el proceso de administración de licencias. Su licencia Flexed incluye licencias de instancias de software (VPX/CPX/BLX, SDX, MPX y VPX FIPS) y licencias de capacidad de ancho de banda. Debe aplicar

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 anteriormente tenía licencias agrupadas y compró 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.

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 las tablas 1 y 2 de la sección Capacidad mínima y máxima para las licencias flexibles y agrupadas.

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 compilación 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

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.

Configurar las licencias Flexed

January 26, 2024

> **Nota:**
>
> Si ha agrupado licencias y ya ha comprado y aplicado licencias Flexed, el derecho combinado ahora aparece en el panel de licencias Flexed.

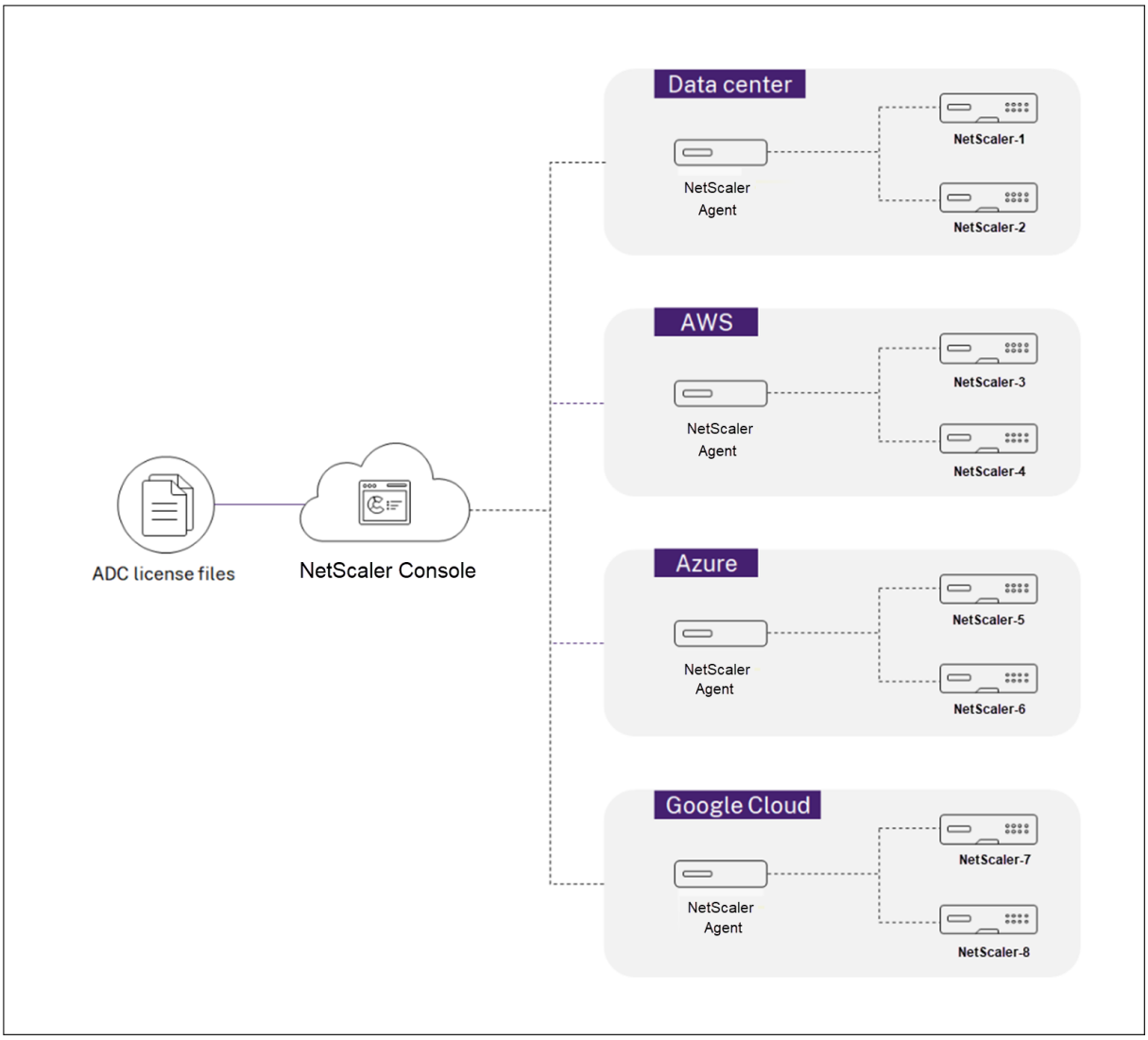
La licencia Flexed de NetScaler le permite compartir licencias de instancia o de ancho de banda en diferentes formatos de NetScaler. Utilice esta capacidad flexible para las instancias que se encuentran en el centro de datos o en las nubes públicas. Cuando una instancia ya no requiere los recursos, comprueba 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.

Para usar las licencias de NetScaler Flexed, debe adjuntar un agente de NetScaler Console a una instancia de NetScaler. Las instancias de NetScaler registran y retiran licencias de NetScaler Console a través de un agente.

Puede realizar las siguientes tareas en NetScaler Console:

1. Cargue los archivos de licencia Flexed (grupo de ancho de banda o grupo de instancias de software) al servidor de licencias.
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 entre NetScaler Console y la instancia no funciona.

Antes de comenzar

Asegúrese de que se cumplen los siguientes requisitos previos antes de configurar las licencias Flexed:

- Instale y registre un agente en NetScaler Console. Para instalar y registrar un agente, consulte Introducción.
- Asegúrese de que todos los agentes registrados estén en el estado de UP para que las licencias flexibles funcionen correctamente. Si los agentes se encuentran en estado DOWN pero aún no han sido retirados del servicio o despedidos, llévelos al estado UP Si los agentes DOWN se retiran o se cancelan o ya no se utilizan, elimínelos de NetScaler Console.
- Los `27000`puertos `7279`y están disponibles para transferir las licencias de NetScaler Console a una instancia. Consulte Requisitos del sistema.

Paso 1: Aplicar licencias en NetScaler Console

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 cargarlo en NetScaler Console.
   - **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 añadir más licencias a NetScaler Console desde la **configuración** de licencias.

3. Haga clic en **Finalizar**.

   Los archivos de licencia se añaden a NetScaler Console. En la sección **Información de caducidad** de licencias se enumeran las licencias presentes en la consola de NetScaler 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.

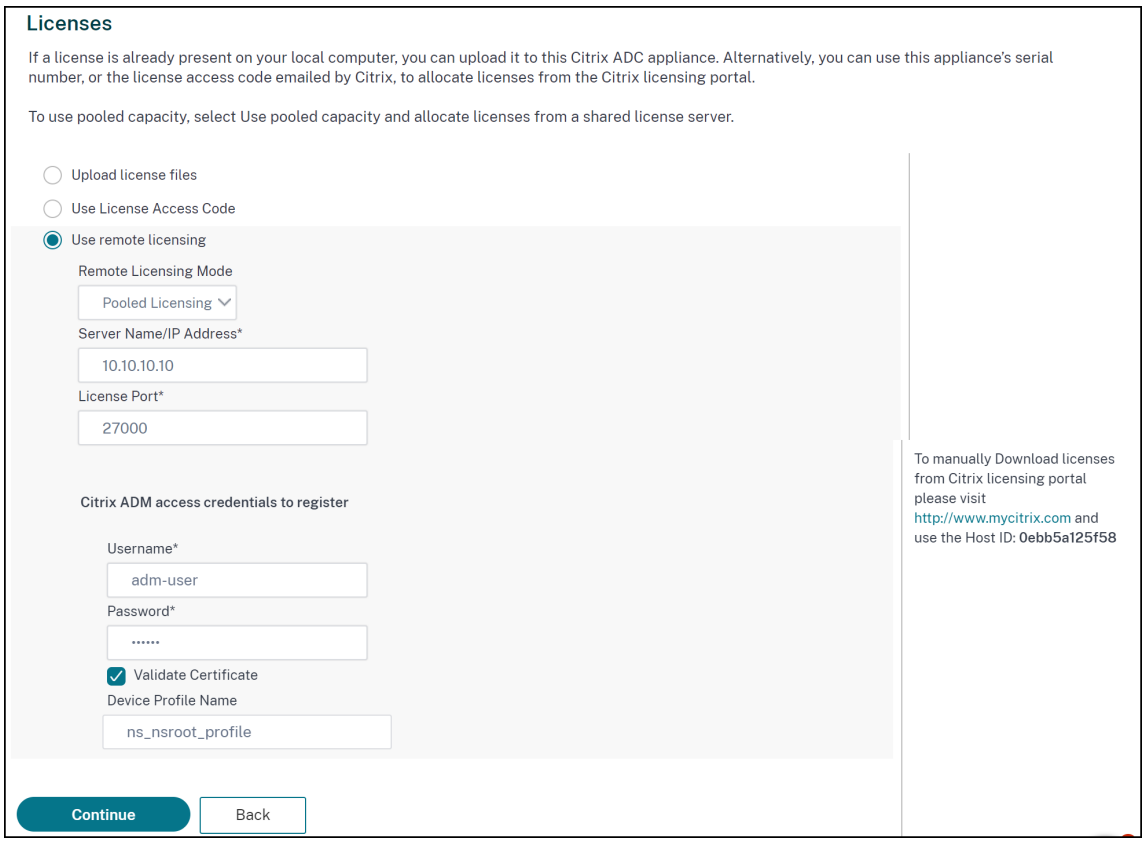
Paso 2: Registrar NetScaler Console como servidor de licencias y asignar licencias

Puede registrar NetScaler Console como servidor de licencias en una instancia de NetScaler mediante un agente.

Registrar un agente de NetScaler Console mediante la GUI

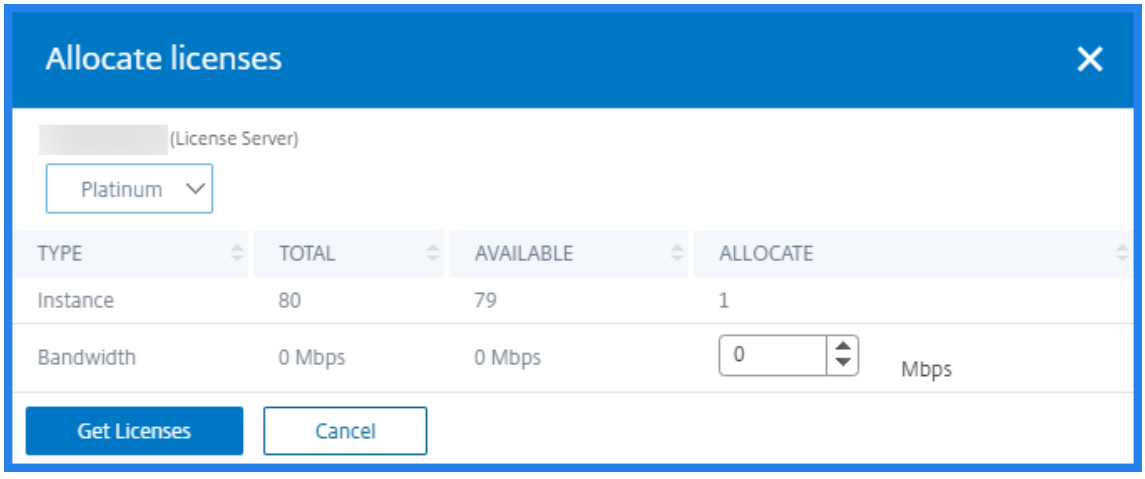
En la GUI de NetScaler Console, registre el agente de NetScaler Console asociado a una instancia de NetScaler.

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 agente de NetScaler Console asociado que está registrada en la consola de NetScaler.
6. Seleccione **Registrarse en NetScaler Console** .
7. Introduzca sus credenciales de agente de NetScaler Console para registrar una instancia en NetScaler Console y haga clic en **Continuar**. En NetScaler Console, uno de los agentes 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 Console.



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 agente de NetScaler Console mediante la CLI

Si una instancia de NetScaler no tiene ninguna GUI, utilice los siguientes comandos de la CLI para agregar un agente de NetScaler Console asociado a una instancia:

1. Inicie sesión en la consola de NetScaler.
2. Agregue la dirección IP del agente de NetScaler Console asociada que está registrada en NetScaler Console:

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. Ver el ancho de banda de licencia disponible en el servidor de licencias:

```
> sh ns licenseserverpool
```

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>
```

> **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 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 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 de instancia se entregan al servidor de licencias.

Puede modificar dinámicamente el ancho de banda de una instancia SDX-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.

Par de alta disponibilidad NetScaler

Antes de empezar, asegúrese de que el servidor de NetScaler Console esté configurado como servidor de licencias. Para obtener más información, consulte Configurar NetScaler Console como servidor de licencias

Al asignar el ancho de banda a un par de NetScaler HA, la consola 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.

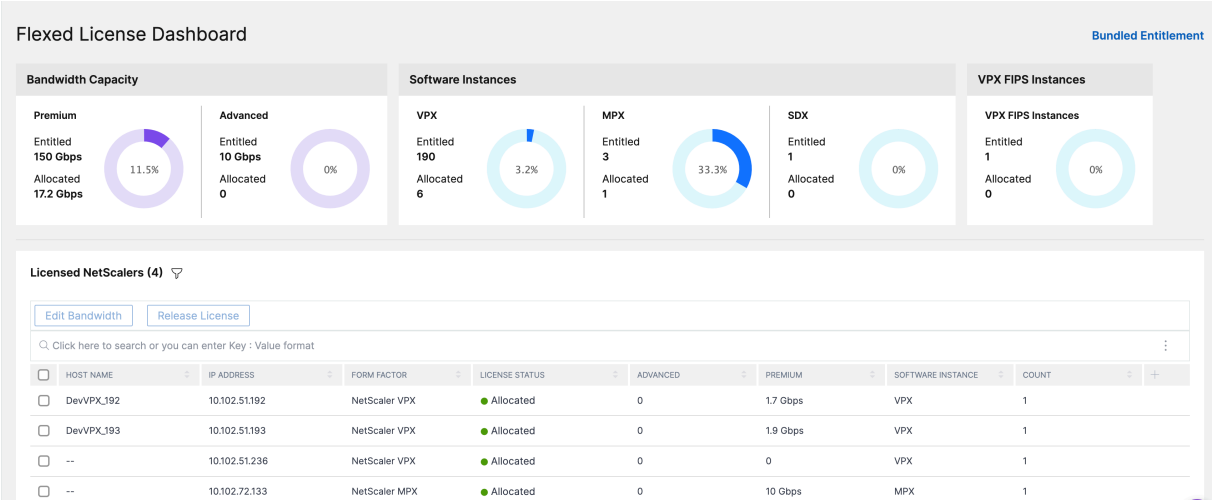
Panel de licencias flexible

April 10, 2024

> **Nota:**
>
> Si anteriormente tenía licencias agrupadas y ahora ha comprado y aplicado licencias Flexed, el derecho combinado ahora aparece en el panel de licencias Flexed.

El panel de licencias flexible 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. MPX y MPX FIPS tienen el mismo archivo de licencia. Del mismo modo, SDX y SDX FIPS tienen el mismo archivo de licencia. Sin embargo, VPX FIPS tiene un archivo diferente al de VPX y se muestra por separado. Además, VPX (incluido VPX en SDX), BLX y CPX requieren licencias VPX y forman parte de los derechos y la asignación de VPX. Una licencia flexible solo admite la edición premium. Sin embargo, si ha adquirido licencias flexibles y anteriormente había agrupado la capacidad de ancho de banda estándar o avanzada, los detalles relacionados con la capacidad de ancho de banda (estándar o avanzada) también aparecen en el panel de licencias flexibles.



Los formatos VPX (incluido VPX en SDX), BLX y CPX requieren el archivo de licencia de instancia de software Flexed VPX de NetScaler. Es decir, estos factores de forma forman parte de los derechos y la asignación de las licencias de instancia de software Flexed VPX.

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

June 7, 2024

En este panel, puede ver detalles sobre:

- Derechos y asignación de instancias de software (VPX, MPX, SDX y VPX FIP)
- Derechos, asignación y uso real del ancho de banda o rendimiento de la capacidad
- Asignación máxima y media en todas las instancias administradas o seleccionadas
- Uso máximo y promedio en todas las instancias administradas o seleccionadas

Funciones (para instancias de NetScaler)	Descripción
Derecho	Los derechos totales de instancia para los tipos de instancias de software (VPX, SDX, MPX).
Asignación	La asignación total de instancias para los tipos de instancias de software (VPX, SDX, MPX).

Funciones (para ancho de banda y capacidad de rendimiento)	Descripción
Derecho	Los derechos totales de ancho de banda y capacidad de rendimiento en todas las instancias de NetScaler administradas. Los derechos totales se calculan a partir de las licencias aplicadas en la administración de licencias (**NetScaler Licensing > License Management**).
Asignación	El ancho de banda y la capacidad de rendimiento que se asignan a los **NetScalers con licencia** en Panel de licencias flexible (**NetScaler Licensing > Flexed Licensing > Flexed License Dashboard**).
Uso	El rendimiento total consumido por las instancias de NetScaler.

> **Nota:**
>
> Una licencia flexible solo admite la edición premium. Sin embargo, si ha comprado y aplicado licencias flexibles y anteriormente había agrupado la capacidad de ancho de banda estándar o avanzada, también se muestran los detalles relacionados con el ancho de banda y la capacidad de rendimiento (estándar o avanzada). Por ejemplo, si ha solicitado una licencia Flexed de 1000 Gbps (que es premium) y también tiene una licencia agrupada activa de 100 Gbps de ancho de banda avanzado, entonces el panel de informes muestra tanto el ancho de banda Premium de 1000 Gbps como el de 100 Gbps avanzado.

El siguiente ejemplo le ayuda a comprender cómo el panel muestra el uso máximo y el uso promedio:

Tenga en cuenta que hay 3 instancias administradas de NetScaler (NetScaler A, NetScaler B y NetScaler C) con licencia Flexed (ancho de banda premium) y la duración seleccionada es de 1 día. Para los cálculos, NetScaler Console considera los puntos de datos (en Mbps) de cada hora por instancia de NetScaler. Durante 1 día, hay 24 puntos de datos para cada instancia de NetScaler. Por lo tanto, para 3 instancias de NetScaler, hay (24 * 3) puntos de datos.

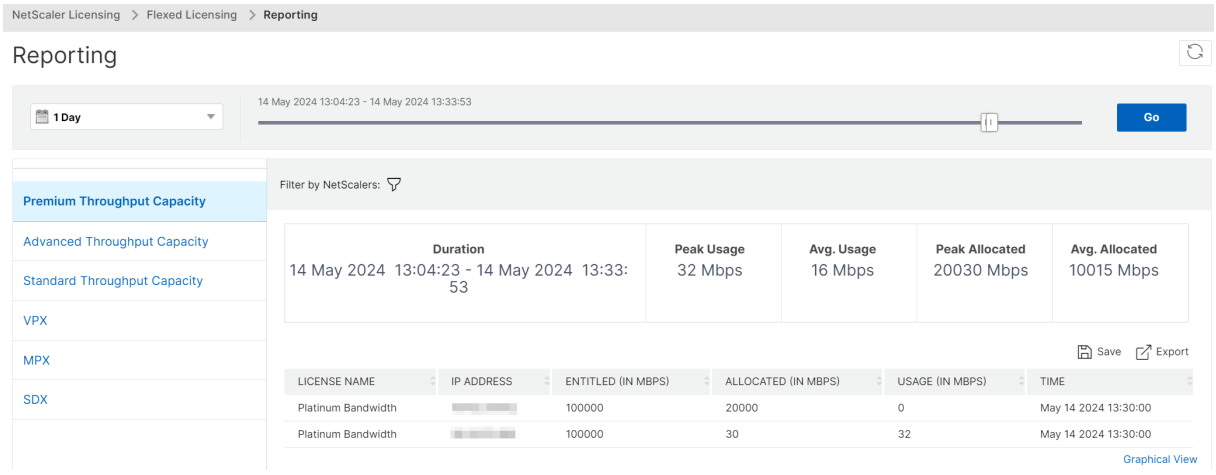
- **Uso máximo** = La suma del punto de datos más alto (Mbps) de las 24 horas de todas las instancias de NetScaler. Por ejemplo, si el punto de datos más alto de las 24 horas de duración de NetScaler A es de 30 Mbps, NetScaler B tiene 45 Mbps y NetScaler C es de 120 Mbps, el uso máximo se muestra como 195 Mbps (30 + 45 + 120).

- **Uso promedio** = La suma de todos los puntos de datos de 24 horas dividida por 24 para cada instancia de NetScaler. Por lo tanto, para 3 instancias de NetScaler, el promedio total de las 3 instancias de NetScaler se dividió por 3. Por ejemplo, si el promedio de NetScaler A es de 25 Mbps, el promedio de NetScaler B es de 20 Mbps y el promedio de NetScaler C es de 45 Mbps, el uso promedio se muestra como 30 Mbps (25 + 20 + 35 dividido por 3).

Del mismo modo, los detalles de asignación de picos y promedios se muestran con la misma lógica.

Puede seleccionar la duración de la lista, desde una hora hasta un año, y ver los detalles tanto en la vista tabular como en la vista gráfica.

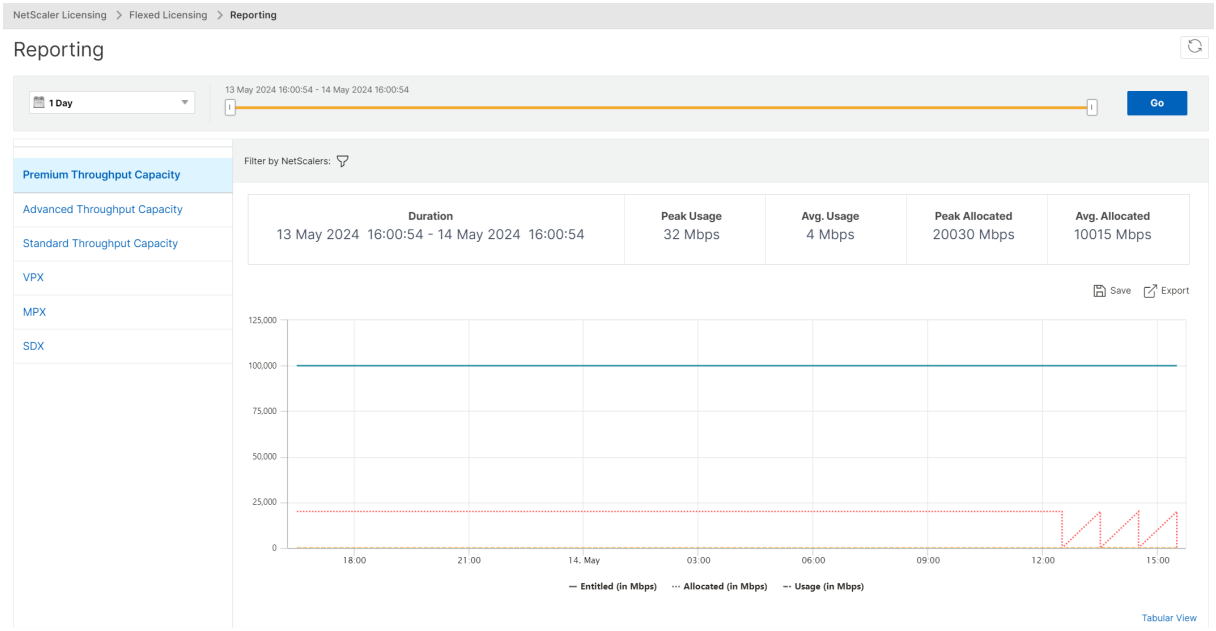
El siguiente ejemplo muestra la vista tabular de las instancias que utilizan la licencia Flexed (ancho de banda Premium):



En el panel de control aparecen los siguientes detalles:

- **Uso máximo**: el uso máximo (en Mbps) durante la duración seleccionada.
- **Uso promedio**: el uso promedio (en Mbps) durante la duración seleccionada.
- **Pico asignado**: la asignación más alta para la duración seleccionada.
- **Asignación promedio**: la asignación promedio para la duración seleccionada.
- **Filtro**: puede seleccionar una o más instancias para ver los detalles de uso y asignación de las instancias específicas.
- **Exportar**: puede exportar detalles en formato PDF, JPEG y PNG.

El siguiente ejemplo muestra la vista gráfica de las instancias que utilizan la licencia Flexed (ancho de banda Premium):



Transición a licencias Flexed

April 10, 2024

> **Nota:**
>
> Debe cambiar al licenciamiento Flexed antes de que caduque su licencia actual. Al planificar la transición, tenga en cuenta los siguientes pasos y planifique un período de mantenimiento si los pasos implican la reconfiguración de la licencia o el reinicio de NetScaler.

De la licencia de ancho de banda Pooled a las licencias Flexed

Algunos pasos son comunes a MPX, SDX y VPX. Estos pasos se enumeran primero, seguidos de los pasos específicos de MPX, SDX o VPX.

Pasos comunes para VPX/MPX/SDX

1. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
2. Si tiene una licencia de software de Z-Cap válida durante un período específico, aplíquela en el hardware de NetScaler (MPX/SDX).

Para VPX/MPX

Se requieren los siguientes pasos adicionales:

1. Si tiene una licencia de ancho de banda Pooled Premium (Platinum), la licencia cambia automáticamente a Flexed cuando caduca la licencia anterior.
2. Si tiene una licencia de ancho de banda Pooled Standard o Pooled Advanced, compruebe manualmente el ancho de banda Premium y reinicie NetScaler en caliente.

Para SDX

> **Nota:**
>
> Asegúrese de cambiar al licenciamiento Flexed antes de que caduque su licencia actual.

Se requieren los siguientes pasos adicionales:

1. Desproteja la licencia de instancia y ancho de banda requerida de licenciamiento Flexed a SDX. No es necesario reiniciar SDX.
2. Si todos los VPX en SDX tienen una edición Premium, la licencia cambia automáticamente a Flexed tras la caducidad de la licencia anterior.
3. Cambie la edición de todos los VPX (en SDX) con Standard o Advanced a Premium. Estas instancias VPX se reinician automáticamente.
4. Reduzca a cero la capacidad de ancho de banda Standard y Advanced en SDX.

Licencias de vCPU agrupada a Flexed

Para VPX

1. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
2. Quite el servidor de licencias existente mediante la GUI de NetScaler. NetScaler no tiene licencia hasta que se completen todos los pasos.
3. Agregue el servidor de licencias con la opción Flexed/Pooled.
4. Desproteja las licencias de instancia y ancho de banda necesarias para NetScaler.
5. Reinicie en caliente NetScaler.

Suscripción fija o licencia perpetua para las licencias Flexed

Algunos pasos son comunes a MPX, SDX y VPX. Estos pasos se enumeran primero, seguidos de los pasos específicos de MPX, SDX o VPX.

Pasos comunes para VPX/MPX/SDX

1. Procese la incorporación a NetScaler Console.
2. Implemente el agente NetScaler.
3. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
4. Aplique la licencia de software Z-Cap en el hardware de NetScaler (MPX/SDX).

Para VPX/MPX

Se requieren los siguientes pasos adicionales:

1. Desproteja las licencias de instancia y ancho de banda necesarias para NetScaler.
2. Reinicie en caliente NetScaler.
3. Elimine la licencia de suscripción fija después de que NetScaler se reinicie.

Para SDX

Se requieren los siguientes pasos adicionales:

1. Desproteja la licencia de instancia y ancho de banda requerida de licenciamiento Flexed en SDX.
2. Si todos los VPX en SDX tienen la edición Premium, no es necesario reiniciar SDX.
3. Si algún VPX tiene la edición Advanced o Standard, ese VPX debe cambiarse a la edición Premium. VPX se reinicia automáticamente.
4. Aplique la licencia de software Z-Cap en NetScaler SDX.
5. Desproteja la licencia de instancia y ancho de banda requerida de licenciamiento Flexed en SDX.
6. Elimine la licencia de suscripción fija después de que NetScaler se reinicie.

Licencias de vCPU fija a Flexed

Para VPX

1. Procese la incorporación a NetScaler Console.
2. Implemente el agente NetScaler.
3. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
4. Configure el servidor de licencias en NetScaler en modo Flexed/Pooled.
5. Desproteja las licencias de instancia y ancho de banda necesarias para NetScaler.
6. Reinicie en caliente NetScaler.
7. Elimine la licencia fija después de que NetScaler se reinicie.

Licencias de CICO a Flexed

Para VPX

1. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
2. Quite el servidor de licencias existente mediante la GUI de NetScaler. NetScaler no tiene licencia hasta que se completen todos los pasos.
3. Agregue el servidor de licencias con la opción Flexed/Pooled.
4. Desproteja las licencias de instancia y ancho de banda necesarias para NetScaler.
5. Reinicie en caliente NetScaler.

De la licencia de ancho de banda aujtoadministrada a las licencias Flexed

Algunos pasos son comunes a MPX, SDX y VPX. Estos pasos se enumeran primero, seguidos de los pasos específicos de MPX, SDX o VPX.

Pasos comunes para VPX/MPX/SDX

1. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
2. Si tiene una licencia de software de Z-Cap válida durante un período específico, aplíquela en el hardware de NetScaler (MPX/SDX).

Para VPX/MPX

1. Si tiene una licencia Premium autoadministrada, cambie el modo de licencia mediante la GUI de NetScaler de Self Managed Pool a Flexed/Pooled.
2. No es necesario reiniciar NetScaler.
3. Si tiene una licencia autoadministrada Standard o Advanced, quite el servidor de licencias existente mediante la GUI de NetScaler.
4. Agregue el servidor de licencias con la opción Flexed/Pooled.
5. Compruebe la capacidad de ancho de banda Flexed Premium para VPX/MPX.
6. Reinicie en caliente NetScaler.

Para SDX

1. Si todas las VPX en SDX tienen una licencia autoadministrada Premium, cambie el modo de licencia mediante la GUI de NetScaler de Self Managed Pool a Flexed/Pooled.
2. No es necesario reiniciar NetScaler.

3. Si algunos VPX en SDX tienen una licencia autoadministrada Standard o Advanced, contacte con Citrix Support.

Licencias de vCPU autoadministrada a Flexed

Para VPX

1. Cargue y aplique licencias Flexed en NetScaler Console. Consulte Archivos de licencia.
2. Quite el servidor de licencias existente mediante la GUI de NetScaler. NetScaler no tiene licencia hasta que se completen todos los pasos.
3. Agregue el servidor de licencias con la opción Flexed/Pooled.
4. Desproteja las licencias de instancia y ancho de banda necesarias para NetScaler.
5. Reinicie en caliente NetScaler.

Capacidad agrupada

January 26, 2024

La capacidad agrupada de NetScaler es un marco de licenciamiento que incluye un ancho de banda común y un grupo de instancias que se hospeda y sirve en NetScaler Console. De este grupo común, cada instancia de NetScaler de su centro de datos, independientemente de la plataforma o el formato, obtiene una licencia de instancia y solo el ancho de banda que necesita. El archivo de licencia y el ancho de banda no están enlazados a la instancia. Cuando la instancia ya no requiere estos recursos, vuelve a registrarlos en el grupo común, haciendo que los recursos estén disponibles para otras instancias que los necesiten.

> **Nota**
>
> En NetScaler Console, uno de los agentes es el servidor de licencias.

Este marco de licencias maximiza la utilización del ancho de banda al garantizar que las instancias no tengan un ancho de banda superior al requerido. La capacidad de las instancias de NetScaler para comprobar las licencias y el ancho de banda dentro y fuera de un grupo común también le permite automatizar el aprovisionamiento de instancias.

Puedes aumentar o disminuir el ancho de banda asignado a una instancia en tiempo de ejecución sin afectar al tráfico. También puede transferir las licencias del grupo de una instancia a otra.

Configurar la capacidad agrupada

January 26, 2024

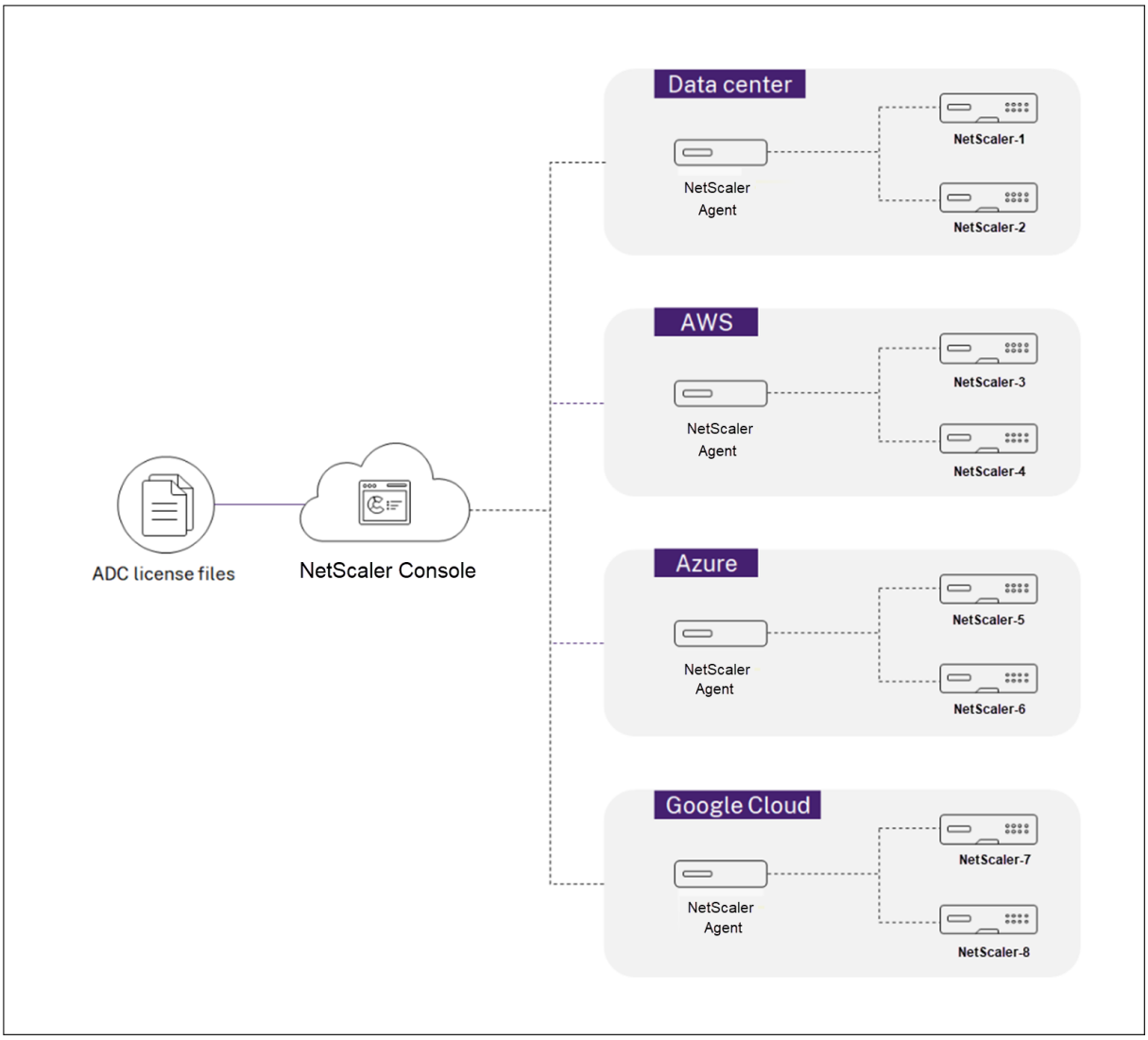
La capacidad agrupada de NetScaler le permite compartir ancho de banda o licencias de instancia en diferentes formatos de NetScaler. Para las instancias basadas en suscripciones de CPU virtuales, puede compartir la licencia de CPU virtual en todas las instancias. Utilice esta capacidad agrupada para 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.

Para usar la capacidad agrupada de NetScaler, debe conectar un agente de NetScaler Console a una instancia de NetScaler. Las instancias de NetScaler registran y retiran licencias de NetScaler Console a través de un agente.

También puede usar licencias de capacidad agrupada para instancias FIPS de NetScaler. Puede realizar las siguientes tareas en NetScaler Console:

1. Cargue los archivos de licencia de capacidad agrupados (grupo de ancho de banda o grupo de instancias) al servidor de licencias.
2. 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.



Puede descargar las licencias agrupadas, 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.

Problemas 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 Console para su administración o la comunicación NITRO desde NetScaler Console a las instancias no funciona.
- **No asignada**: la licencia no está asignada en la instancia.

Antes de comenzar

Asegúrese de lo siguiente antes de configurar la capacidad agrupada:

- Instale y registre un agente en NetScaler Console. Para instalar y registrar un agente, consulte Introducción.
- Asegúrese de que todos los agentes registrados estén en el estado de UP para que las licencias agrupadas funcionen correctamente. Si los agentes se encuentran en estado DOWN pero aún no han sido retirados del servicio o despedidos, llévelos al estado UP Si los agentes DOWN se retiran o se cancelan o ya no se utilizan, elimínelos de NetScaler Console.
- Los `27000`puertos `7279`y están disponibles para transferir las licencias de NetScaler Console a una instancia. Consulte Requisitos del sistema.

Paso 1: Aplicar licencias en NetScaler Console

1. En NetScaler Console, vaya a **Infraestructura > Licencias agrupadas**.
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 cargarlo en NetScaler Console.
   - **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 añadir más licencias a NetScaler Console desde la **configuración** de licencias.

3. Haga clic en **Finalizar**.

   Los archivos de licencia se añaden a NetScaler Console. La pestaña **Información de caducidad** de licencias muestra las licencias presentes en la consola de NetScaler 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.

Paso 2: Registrar la consola de NetScaler como servidor de licencias

Puede registrar NetScaler Console como servidor de licencias en una instancia de NetScaler mediante un agente.

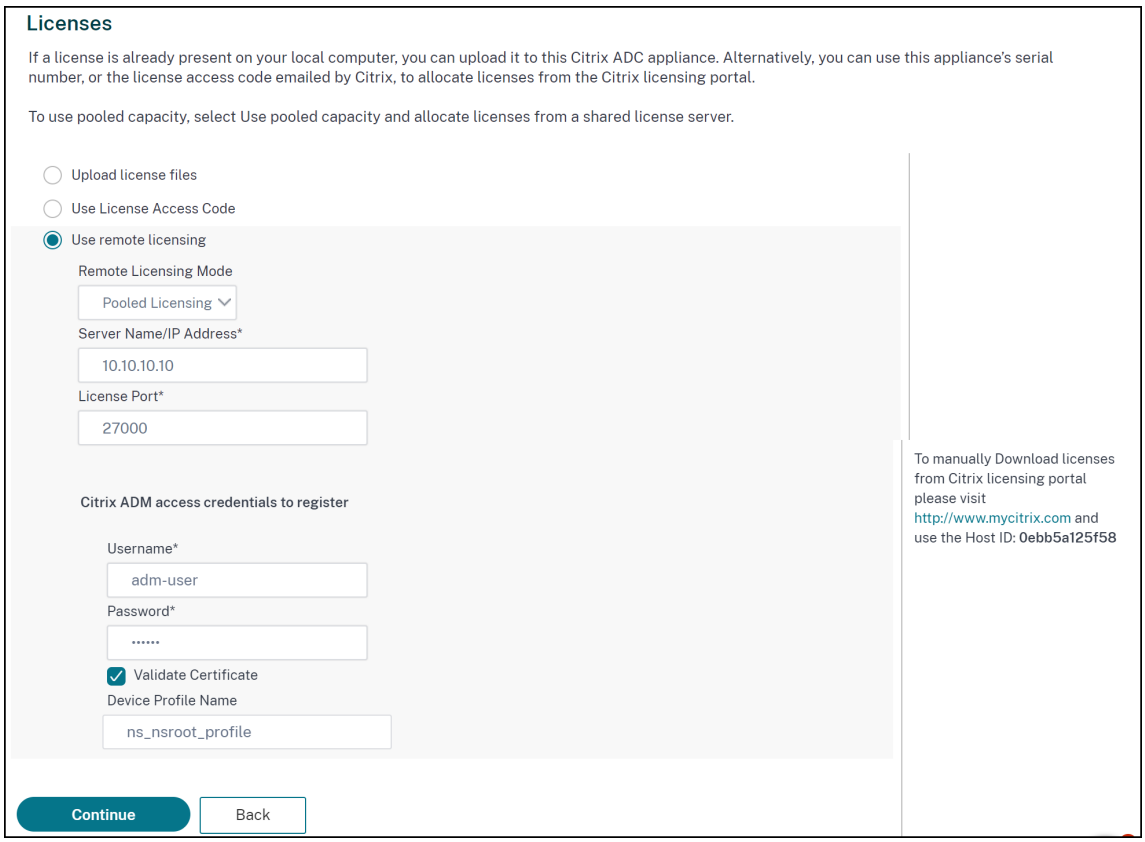
Utilice uno de los procedimientos siguientes para registrar la consola de NetScaler como servidor de licencias:

- Usar GUI

Use la GUI para registrar un agente

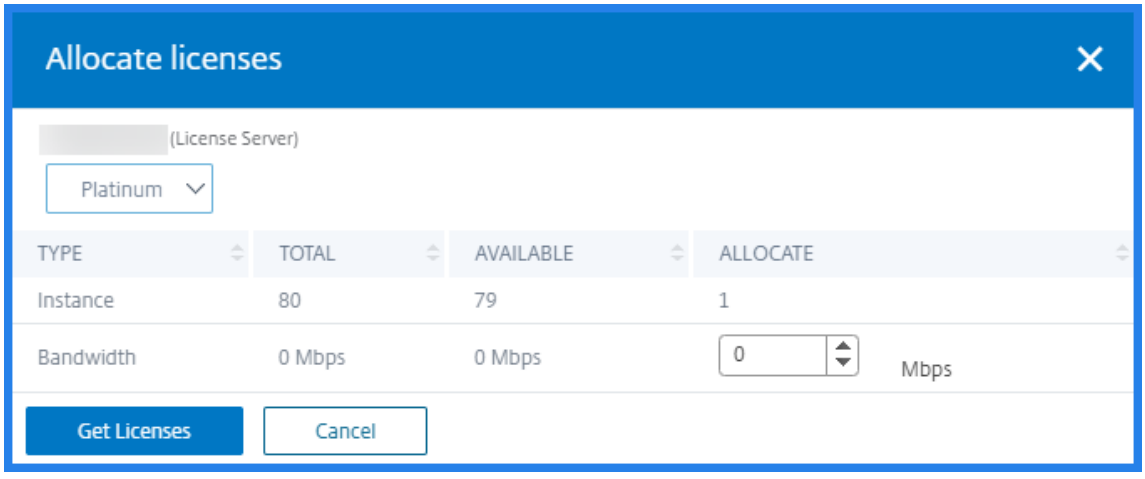
En la GUI de NetScaler Console, registre el agente asociado a una instancia de NetScaler.

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 agente asociado que está registrada en la consola de NetScaler.
6. Seleccione **Registrarse en NetScaler Console** .
7. Introduzca las credenciales de su agente para registrar una instancia en NetScaler Console y haga clic en **Continuar**. En NetScaler Console, uno de los agentes 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 Console.



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.

Use la CLI para agregar un agente

Si una instancia de NetScaler no tiene ninguna GUI, utilice los siguientes comandos de la CLI para agregar un agente asociado a una instancia:

1. Inicie sesión en la consola de NetScaler.
2. Agregue la dirección IP del agente asociado que está registrada en la consola de NetScaler:

```
> add ns licenseserver <adm-agent-IP-address> -port <adm-agent-license-port-number>
```

3. Ver el ancho de banda de licencia disponible en el servidor de licencias:

```
> sh ns licenseserverpool
```

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>
```

   La edición de licencia puede ser **Standard** o **Advanced** o **Premium**.

   > **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

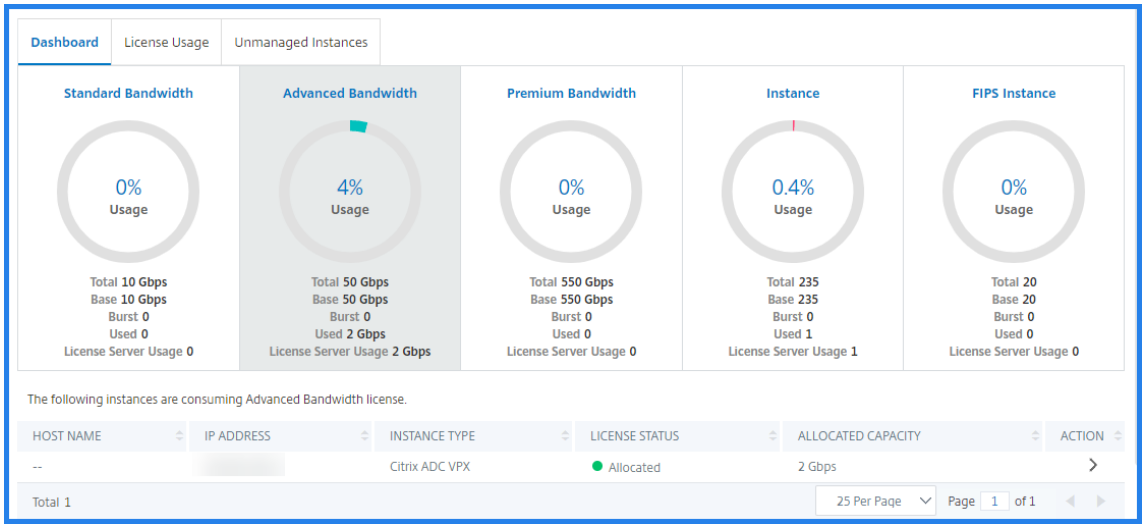
Para asignar licencias de capacidad agrupada desde la GUI de NetScaler Console:

1. Inicie sesión en NetScaler Console.
2. Vaya a **Infraestructura > Licencias agrupadas > Licencias de ancho de banda > Capacidad agrupada**.

   La capacidad de la instancia FIPS solo aparece si carga las licencias de instancia FIPS en NetScaler Console.
3. Haga clic en el grupo de licencias que quiere administrar.

> **Nota:**
>
> El campo **Capacidad asignada** no refleja inmediatamente el ancho de banda modificado. 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.

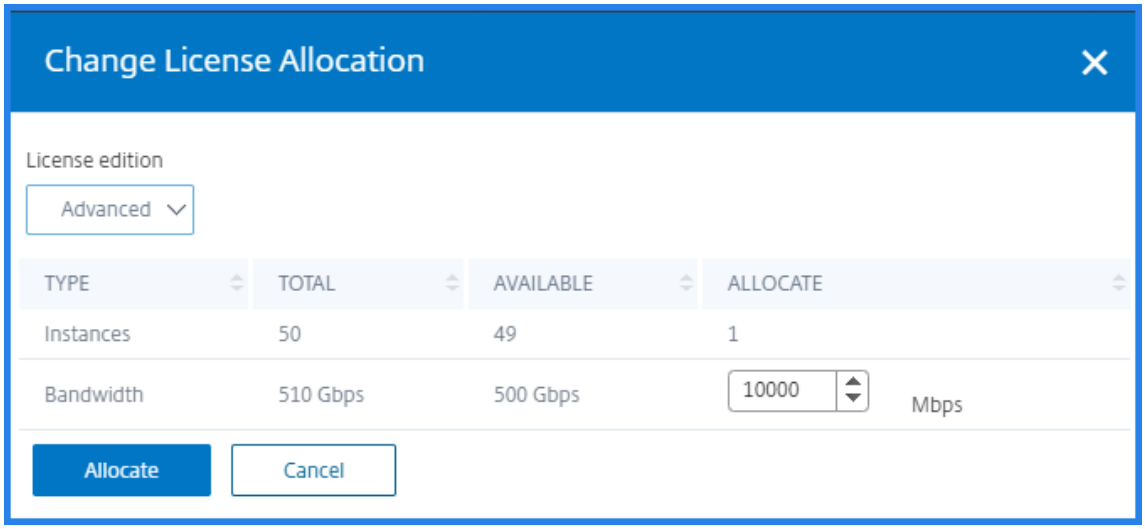
4. Seleccione una instancia de NetScaler de la lista de instancias disponibles haciendo clic en el botón **>**.



La columna Estado de la licencia muestra los mensajes de estado de asignación de licencias correspondientes.

> **Nota:**
>
> La pestaña **Instancias** no administradas muestra las instancias que se descubren pero no se administran en NetScaler Console.

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:**
>
> Reinicie en caliente una instancia si cambia la edición de la licencia.

Configurar la capacidad agrupada en instancias de NetScaler

Puede configurar licencias de capacidad agrupada en las siguientes instancias de NetScaler:

- Instancias de NetScaler MPX-Z
- Instancias de NetScaler SDX-Z
- Instancias de NetScaler VPX
- Par de alta disponibilidad NetScaler

Instancias de NetScaler MPX-Z

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.

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, se deshabilita la función de capacidad agrupada. 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 SDX-Z

SDX-Z es el dispositivo NetScaler SDX con capacidad agrupada. SDX-Z admite la agrupación de instancias y ancho de banda para las licencias de las ediciones Premium, Advanced o Standard.

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 quita la licencia SDX-Z, la función de capacidad agrupada se deshabilita. Las licencias de instancia se entregan al servidor de licencias.

Puede modificar dinámicamente el ancho de banda de una instancia SDX-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

Una instancia de NetScaler VPX con capacidad agrupada puede extraer las 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 de NetScaler Console.

Par de alta disponibilidad NetScaler

Antes de empezar, asegúrese de que el servidor de NetScaler Console esté configurado como servidor de licencias. Para obtener más información, consulte Configurar NetScaler Console como servidor de licencias

Al asignar el ancho de banda a un par de NetScaler HA, la consola de NetScaler comprueba el mismo ancho de banda para las instancias principales y secundarias. Si asigna un ancho de banda de 10 Mbps a un par de NetScaler HA, NetScaler Console hace lo siguiente:

1. Comprueba el ancho de banda de 20 Mbps para el par HA.
2. Asigna 10 Mbps a cada instancia del par HA.

Para asignar una licencia de grupo a un par de NetScaler HA, consulte Asignar licencias agrupadas a instancias de NetScaler.

La página **Capacidad AGRUPADA** muestra las instancias y su capacidad asignada por separado. Si cambias o liberas el ancho de banda de la instancia principal, el ancho de banda de la instancia secundaria se sincroniza automáticamente con la instancia principal. Sin embargo, la sincronización no se produce si cambia o libera el ancho de banda de la instancia secundaria.

Actualice una licencia perpetua en NetScaler MPX a la capacidad agrupada de NetScaler

El dispositivo NetScaler MPX con licencia perpetua se puede actualizar a la licencia de capacidad agrupada de NetScaler. La actualización a la licencia de capacidad agrupada de NetScaler le permite asignar licencias del grupo de licencias a los dispositivos NetScaler a pedido. NetScaler puede usar una licencia a la vez, es decir, una licencia perpetua o una licencia agrupada. Un cliente puede cambiar de una licencia agrupada a una licencia perpetua. Mientras la licencia perpetua sea válida, puede volver a configurar NetScaler y eliminar la configuración de licencias agrupadas. Cuando un cliente cambia de una licencia perpetua a una licencia agrupada o de una licencia agrupada a una licencia perpetua, se reinician todas las instancias de NetScaler.

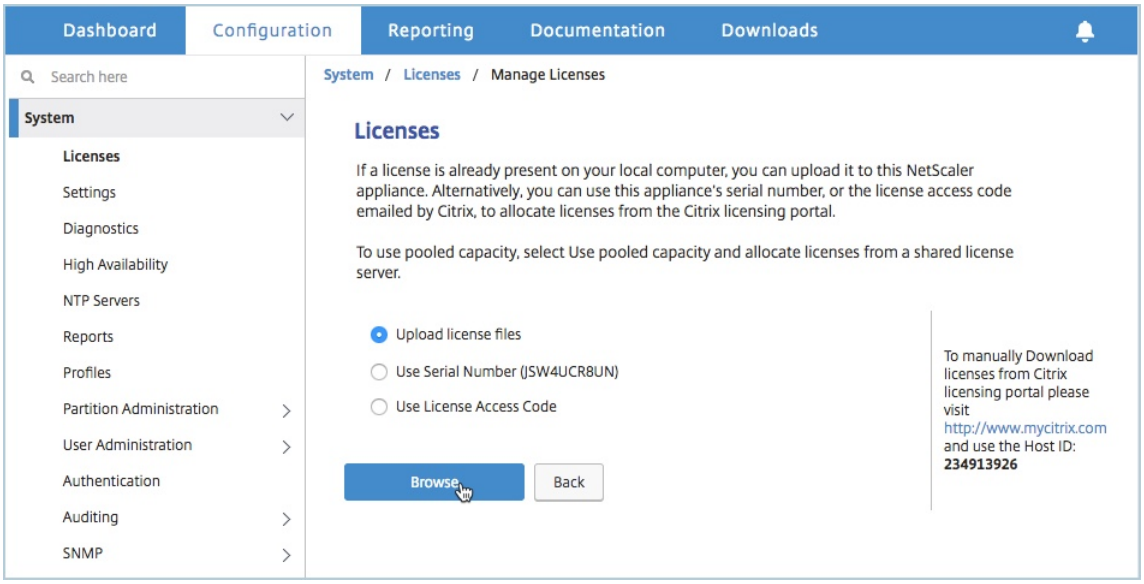
También puede configurar la licencia de capacidad agrupada de NetScaler para las instancias de NetScaler configuradas en modo de alta disponibilidad. Para configurar la licencia de capacidad agrupada de NetScaler para instancias MPX de NetScaler en modo de alta disponibilidad, consulte Actualización de la licencia perpetua del par de alta disponibilidad de NetScaler MPX a NetScaler Pooled capacity.

> **Nota**
>
> Para actualizar el dispositivo NetScaler MPX a la licencia de capacidad agrupada de NetScaler,

> debe cargar la licencia MPX-Z en el dispositivo.

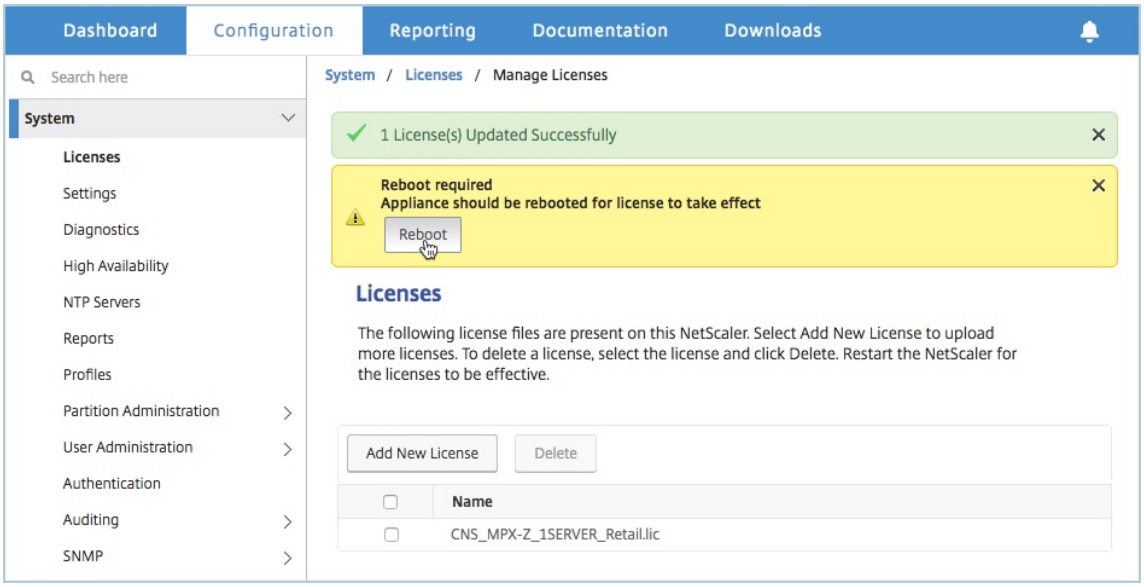
Para actualizar a la capacidad agrupada de NetScaler:

1. En un explorador web, escriba la dirección IP del dispositivo NetScaler, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha Configuración, vaya a **Sistema** > **Licencias**.
5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en Agregar **nueva licencia** .
6. En la página **Licencias** , seleccione Cargar **archivos de licencia** y haga clic **en**Examinar para seleccionar la licencia de capacidad cero de su máquina local.

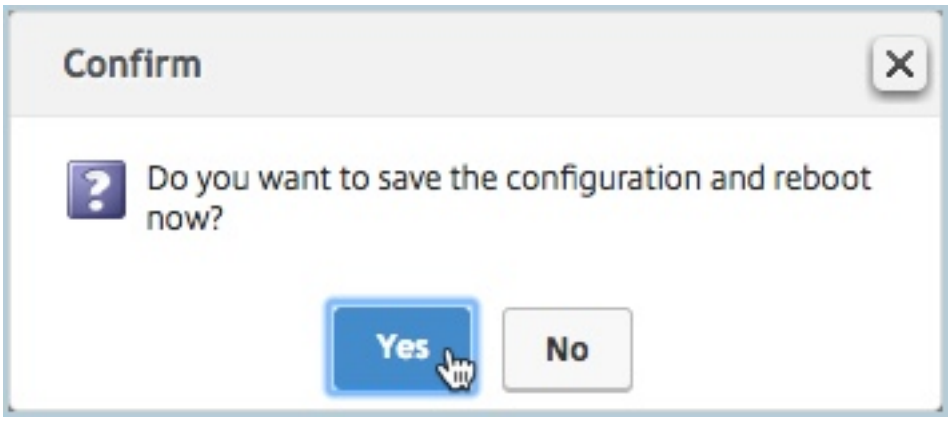


7. Después de cargar la licencia, haga clic en **Reiniciar** para reiniciar el dispositivo.

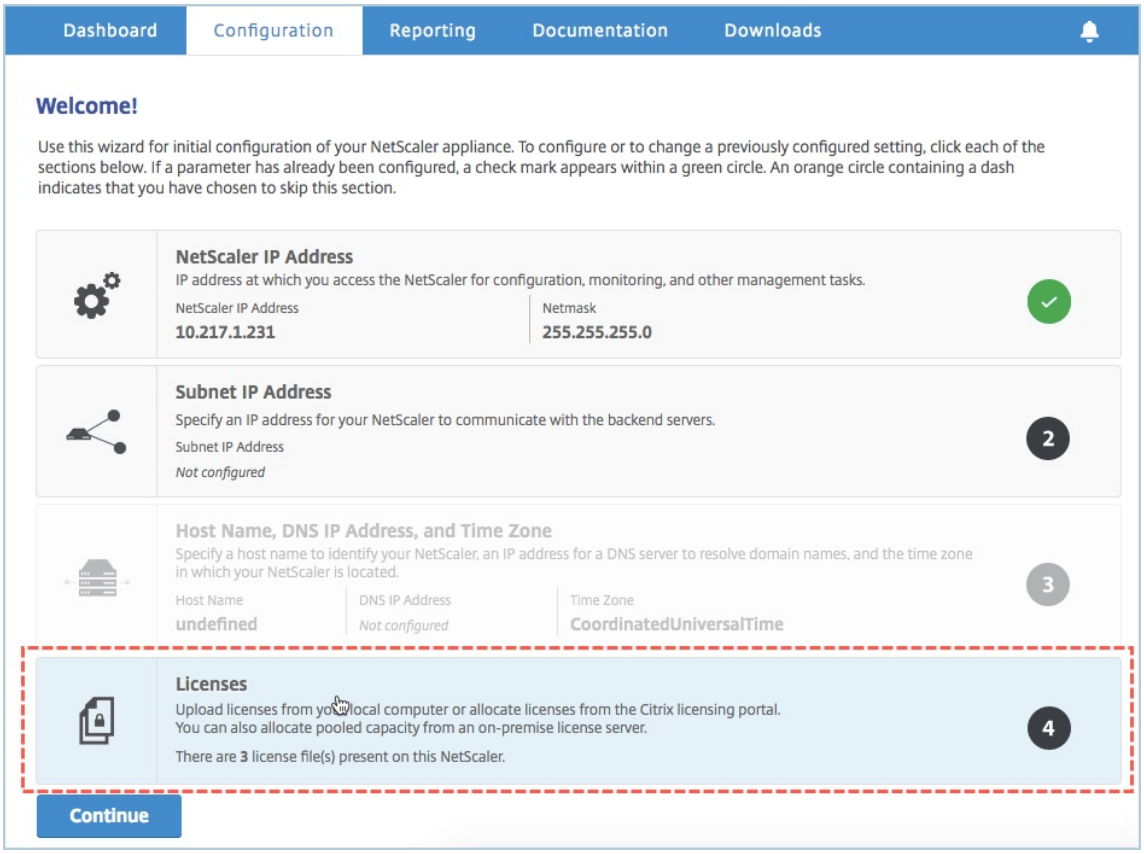
> **Advertencia**
>
> Después de aplicar la licencia MPX-Z, las funciones, incluida la descarga de SSL en el dispositivo, quedan sin licencia. El dispositivo deja de procesar solicitudes HTTPS.
>
> Si la opción **Solo acceso seguro** está habilitada en el dispositivo antes de la actualización, no podrá conectarse al dispositivo a través de la GUI de NetScaler Console mediante HTTPS.



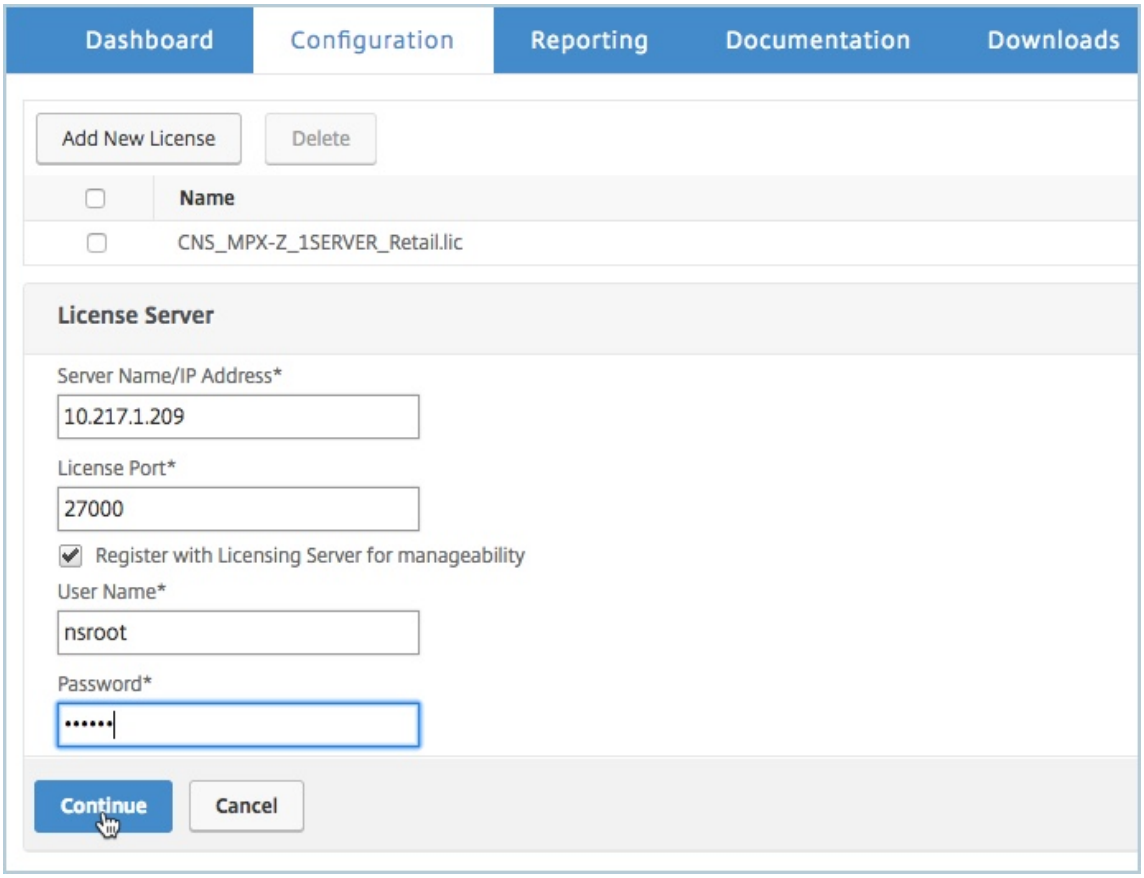
8. En la página **Confirmar**, haga clic en **Sí**.



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.

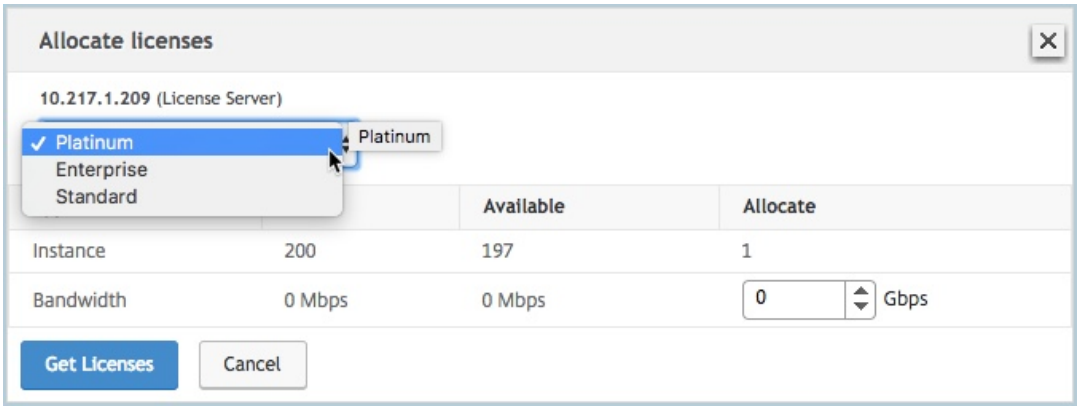
b) En el campo **Puerto de licencias**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Si desea administrar las licencias del grupo de instancias a través de NetScaler Console, seleccione la casilla **Registrarse en el servidor de licencias para obtener capacidad de administración** e introduzca las credenciales de NetScaler Console.

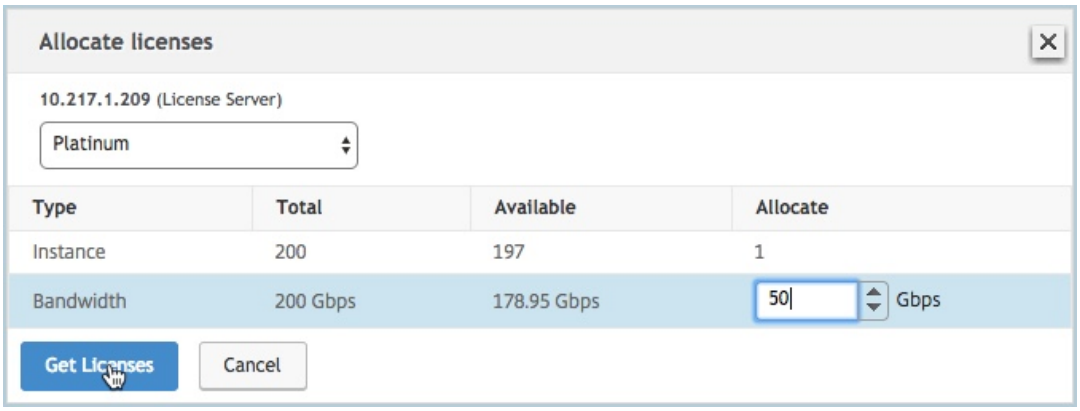
d) Haga clic en **Continuar**.

12. En la ventana Asignar licencias, haga lo siguiente:

a) Seleccione la edición de licencia en la lista desplegable.

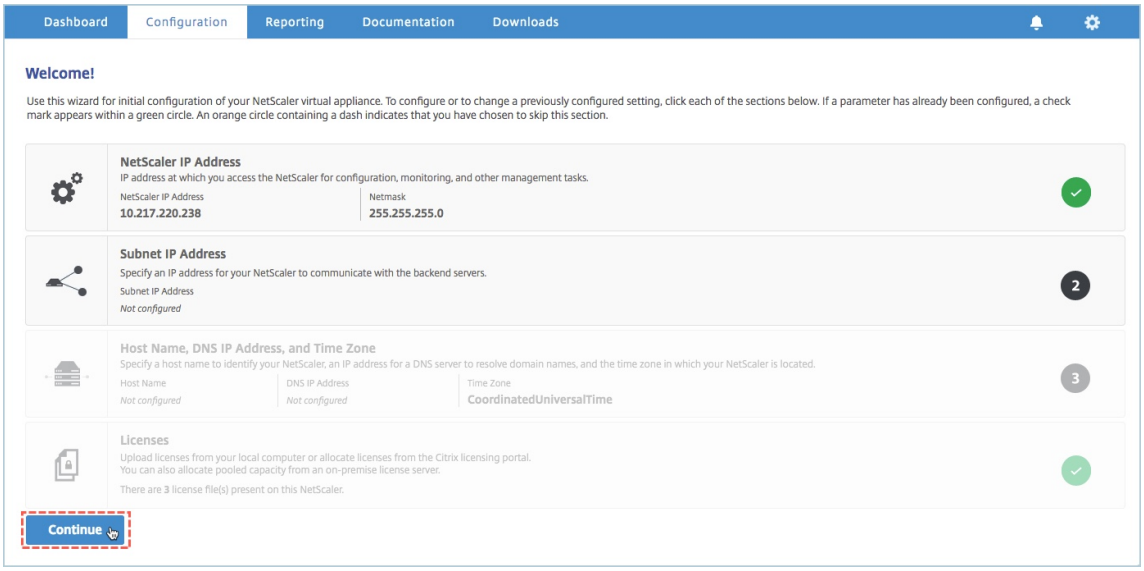


b) Asigne el ancho de banda al dispositivo NetScaler desde el menú **Asignar** y haga clic en **Obtener licencias**.

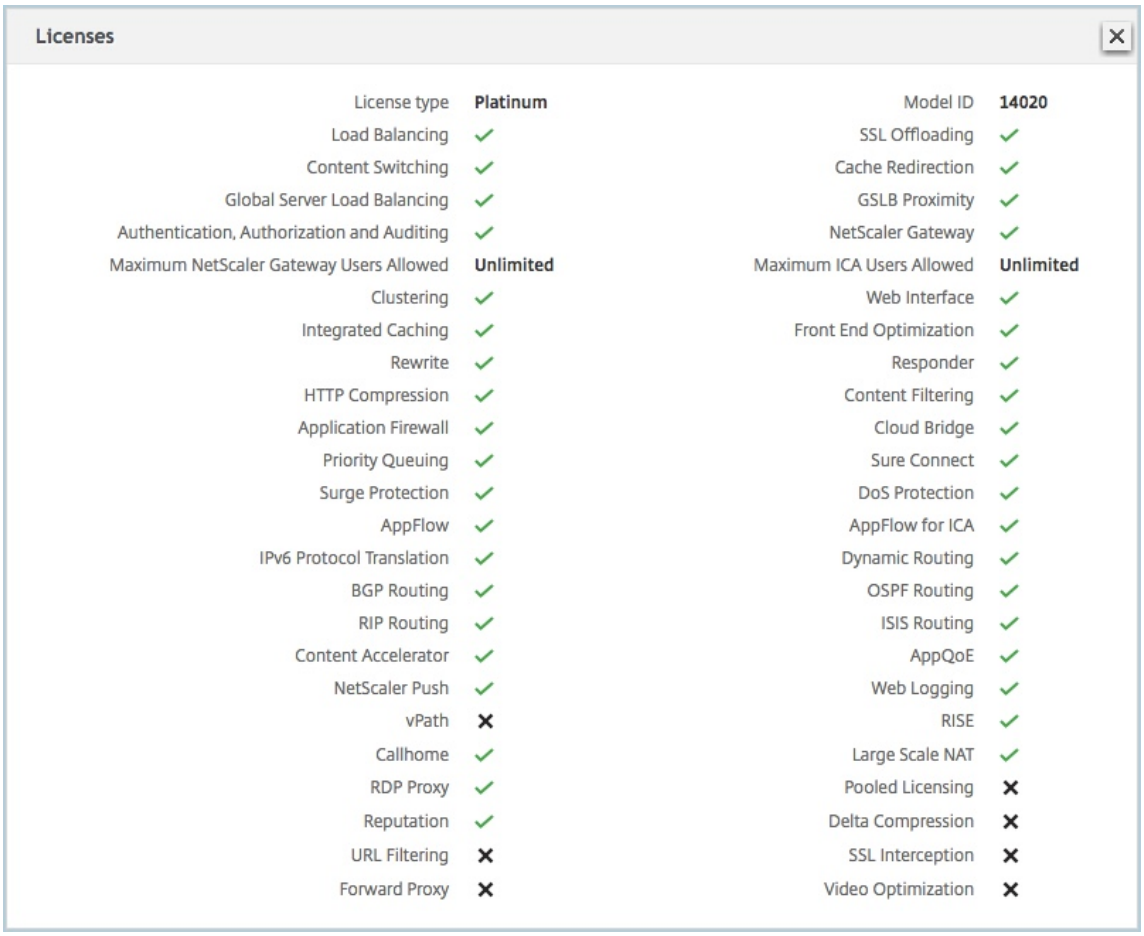


c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.

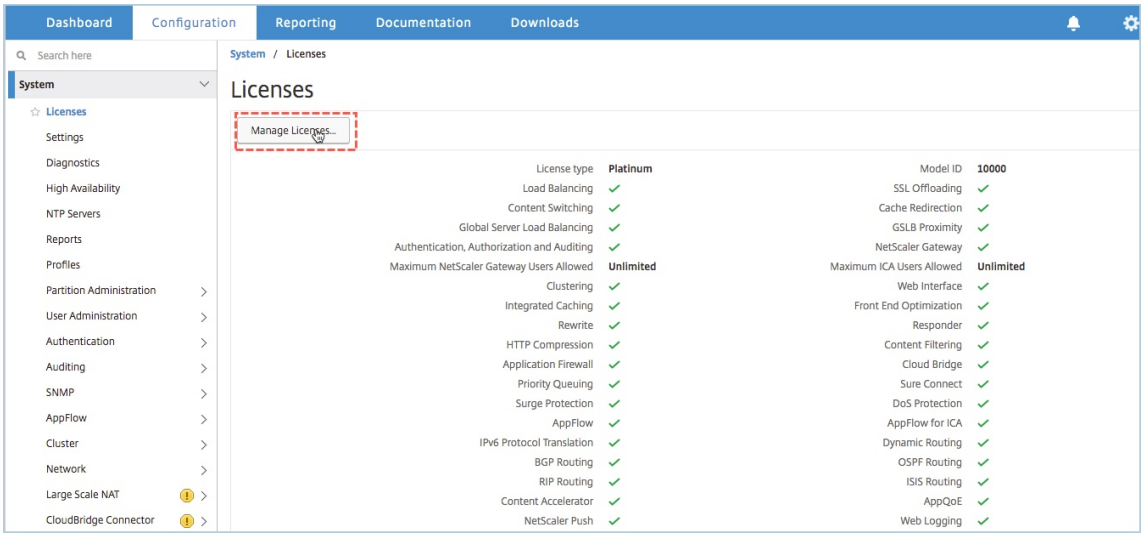
13. Una vez que se reinicie el dispositivo NetScaler MPX, inicie sesión en el dispositivo NetScaler MPX. En la página de **bienvenida**, haga clic en **Continuar**.



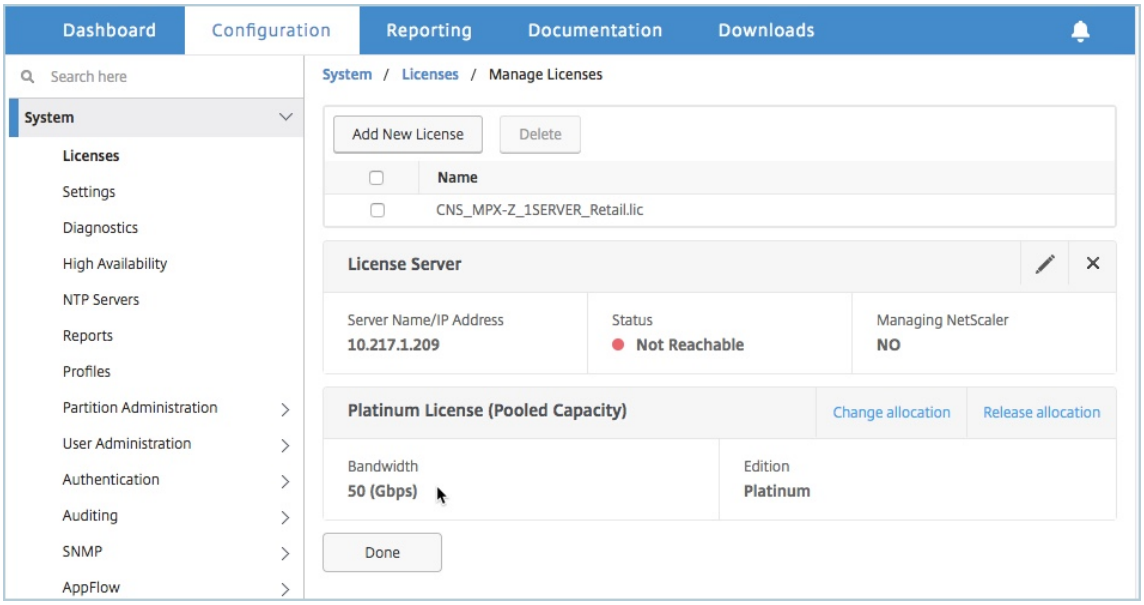
La página **Licencias** muestra todas las funciones con licencia.



14. Vaya a **Sistema > Licencias agrupadas** 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 NetScaler MPX configurados en modo de alta disponibilidad, debe configurar la capacidad agrupada de NetScaler en las instancias de NetScaler principales y secundarias del par HA. Debe asignar licencias de la misma capacidad a las instancias primarias y secundarias de NetScaler en el par HA. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia del par HA, debe asignar una capacidad de 2 Gbps del grupo común para poder asignar una capacidad de 1 Gbps a cada una de las instancias de NetScaler principales y secundarias del par HA.

> **Importante**
>
> Para actualizar el dispositivo NetScaler MPX para que utilice la licencia de capacidad agrupada de NetScaler, debe cargar el MPX-Z en el dispositivo.

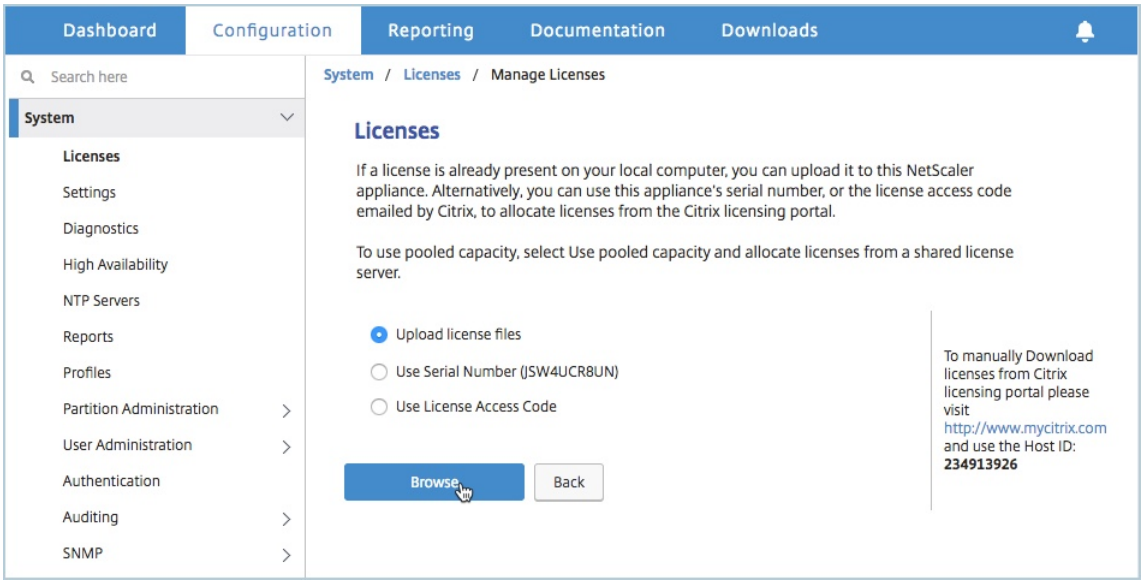
Requisitos previos

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:

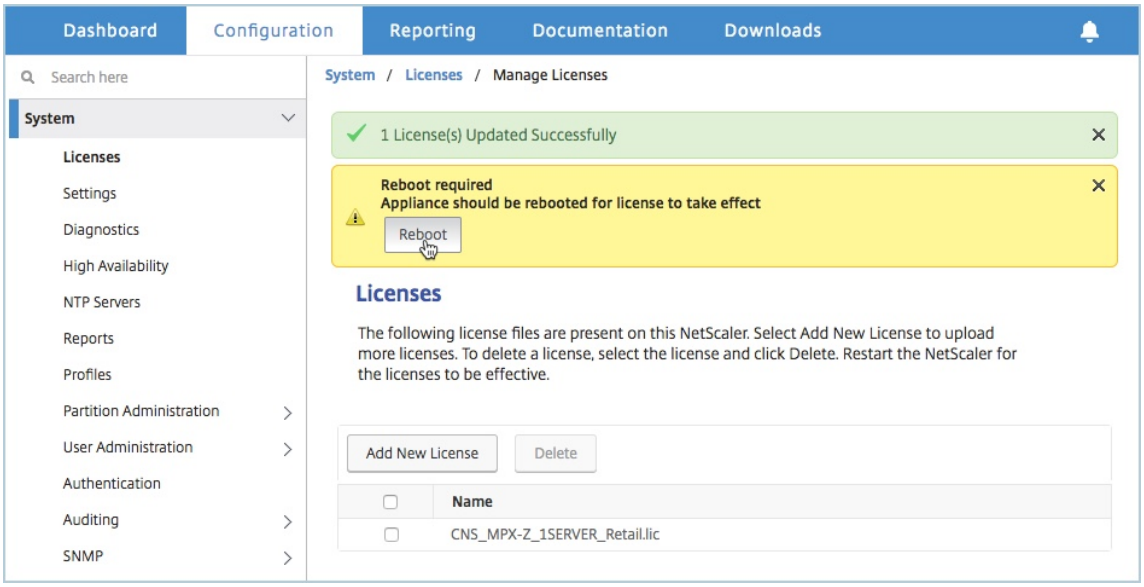
1. En un explorador web, escriba la dirección IP del dispositivo. Por ejemplo: http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha **Configuración**, vaya a **Sistema > Licencias**.

5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en **Agregar nueva licencia** .
6. En la página **Licencias** , seleccione Cargar **archivos de licencia** y haga clic **en**Examinar para seleccionar la licencia de capacidad cero de su máquina local.

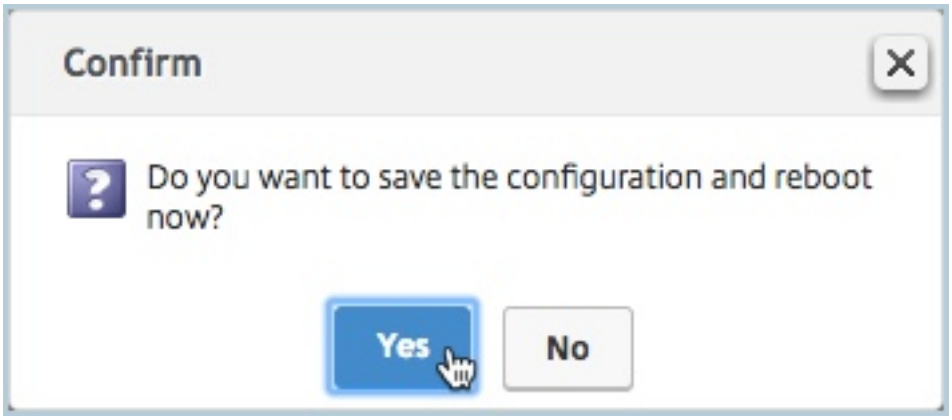


Una vez cargada la licencia, se le pedirá que reinicie el dispositivo.

7. Haga clic en **Reiniciar** para reiniciar el dispositivo.

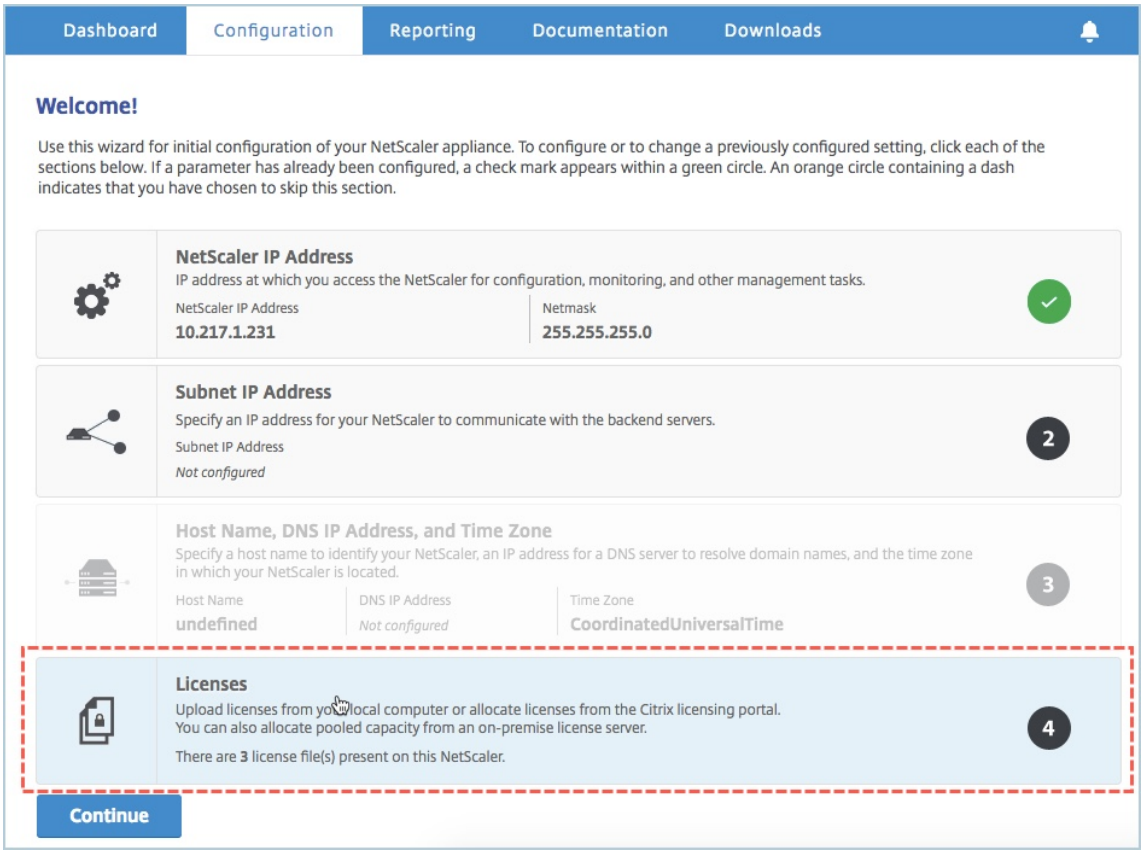


8. En la página **Confirmar**, haga clic en **Sí**.

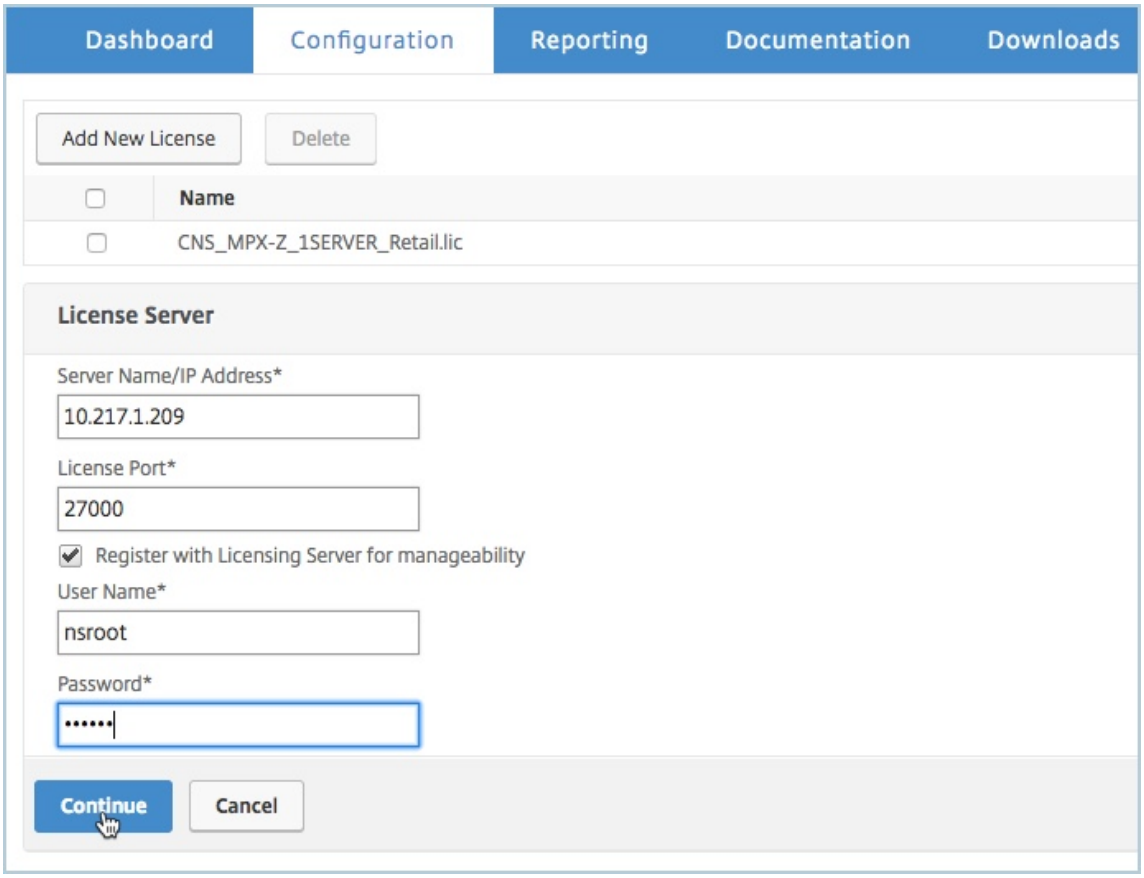


Para actualizar una configuración de alta disponibilidad existente a la capacidad agrupada de NetScaler:

1. Inicie sesión en la instancia de NetScaler MPX secundaria. En un explorador web, escriba la dirección IP del dispositivo NetScaler, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida** , haga clic en la sección **Licencias** .



4. En la sección **Servidor de licencias**, haga lo siguiente:



a) En el campo **Nombre del servidor/Dirección IP**, introduzca los detalles del servidor de licencias.

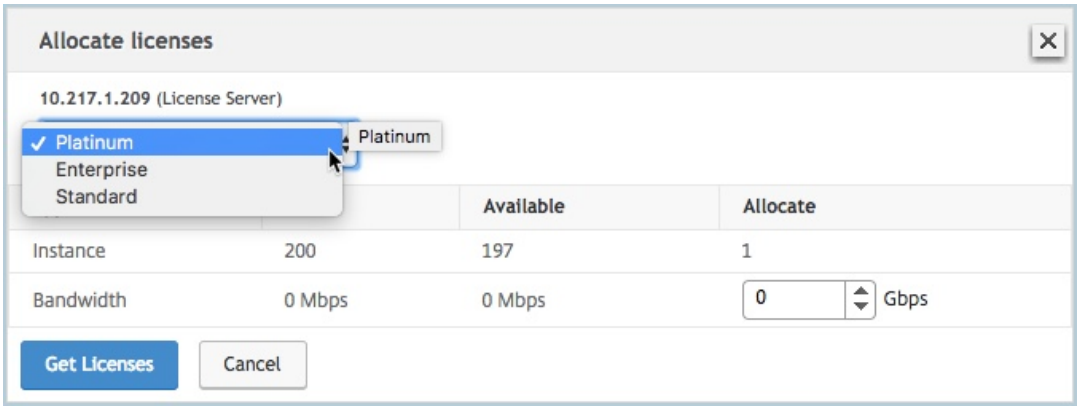
b) En el campo **Puerto de licencias**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Si desea administrar las licencias del grupo de instancias a través de NetScaler Console, seleccione la casilla **Registrarse en el servidor de licencias para obtener capacidad de administración** e introduzca las credenciales de NetScaler Console.

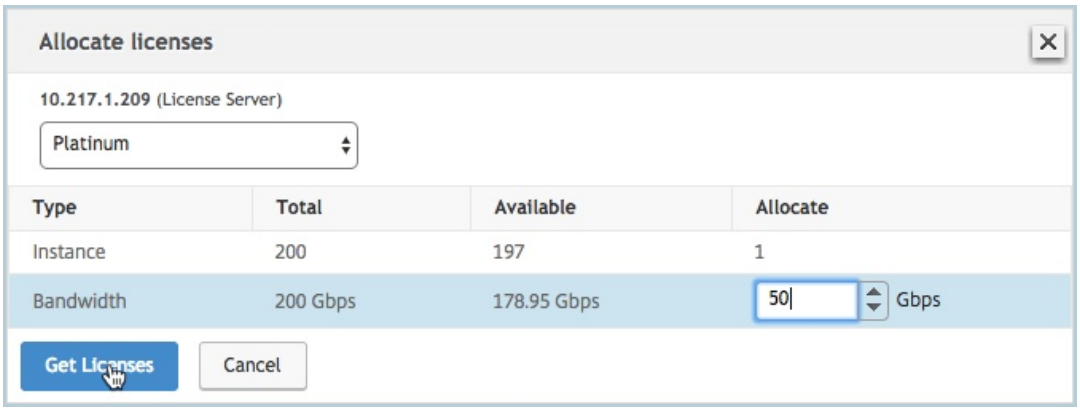
d) Haga clic en **Continuar**.

5. En la ventana **Asignar licencias**, haga lo siguiente:

a) Seleccione la edición de licencia en la lista desplegable.



b) Asigne el ancho de banda al dispositivo NetScaler desde el menú **Asignar** y haga clic en **Obtener licencias**.



c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.

Después de que se reinicie el dispositivo NetScaler MPX secundario, se convierte en el dispositivo NetScaler MPX principal en el par HA.

6. Inicie sesión en el dispositivo NetScaler MPX principal existente y reinicie el dispositivo. Lleve a cabo lo siguiente:

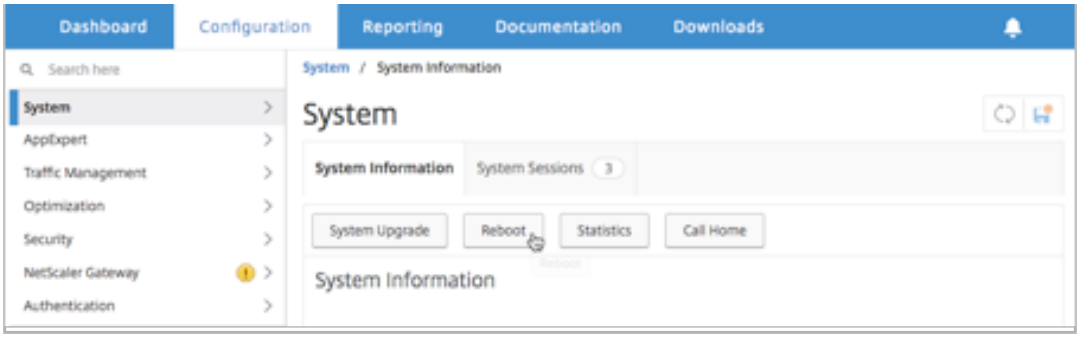
a) En un explorador web, escriba la dirección IP del dispositivo NetScaler, como http://192.168.100.1.

b) En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.

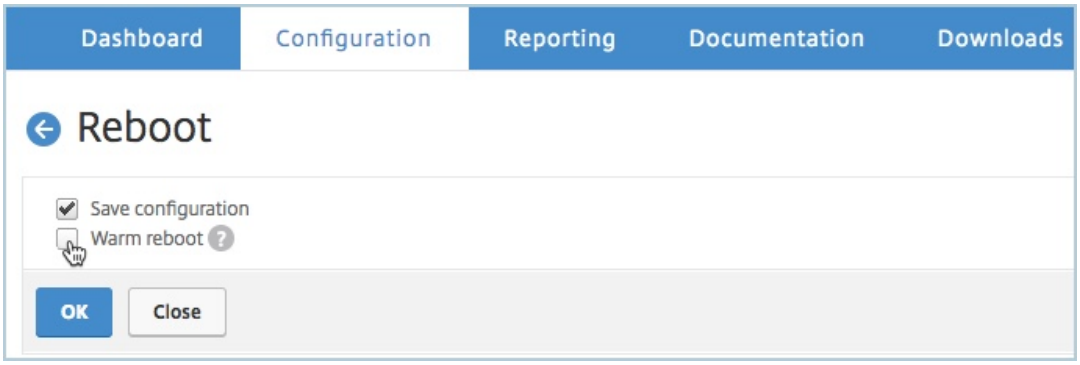
c) En la página de **bienvenida**, haga clic en **Continuar**.

d) En la ficha **Configuración**, haga clic en **Sistema**.

e) En la página **Sistema**, haga clic en **Reiniciar**.



f) En la página **Reiniciar**, seleccione **Reiniciar en caliente** y haga clic en **Aceptar**.



Una vez que se reinicie el dispositivo NetScaler MPX principal, se convierte en el dispositivo NetScaler MPX secundario en el par HA. Si es necesario, puede cambiar las instancias principales y secundarias del par de alta disponibilidad a su configuración original de pares de alta disponibilidad mediante el siguiente comando en cualquier instancia del par de alta disponibilidad:

```
> force ha failover
```

Actualice una licencia perpetua en un NetScaler SDX a la capacidad agrupada de NetScaler

January 26, 2024

Un NetScaler SDX con licencia perpetua se puede actualizar a una licencia de capacidad agrupada de NetScaler. La actualización a la licencia de capacidad agrupada de NetScaler le permite asignar licencias del grupo de licencias a los dispositivos NetScaler a pedido. NetScaler puede usar una licencia a la vez, es decir, una licencia perpetua o una licencia agrupada. Un cliente puede cambiar de una licencia agrupada a una licencia perpetua. Mientras la licencia perpetua sea válida, el cliente puede reconfigurar NetScaler y eliminar la configuración de licencias agrupadas. Cuando un cliente cambia

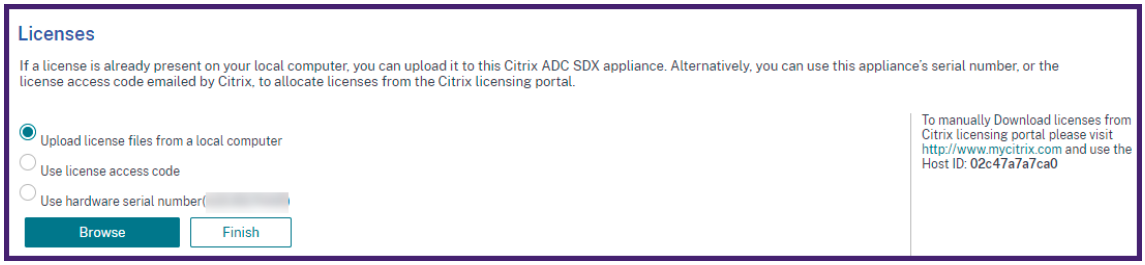
de una licencia perpetua a una licencia agrupada o a una licencia agrupada a una licencia perpetua, se reinician todas las instancias de NetScaler.

También puede configurar la licencia de capacidad agrupada de NetScaler para las instancias de NetScaler configuradas en modo de alta disponibilidad.

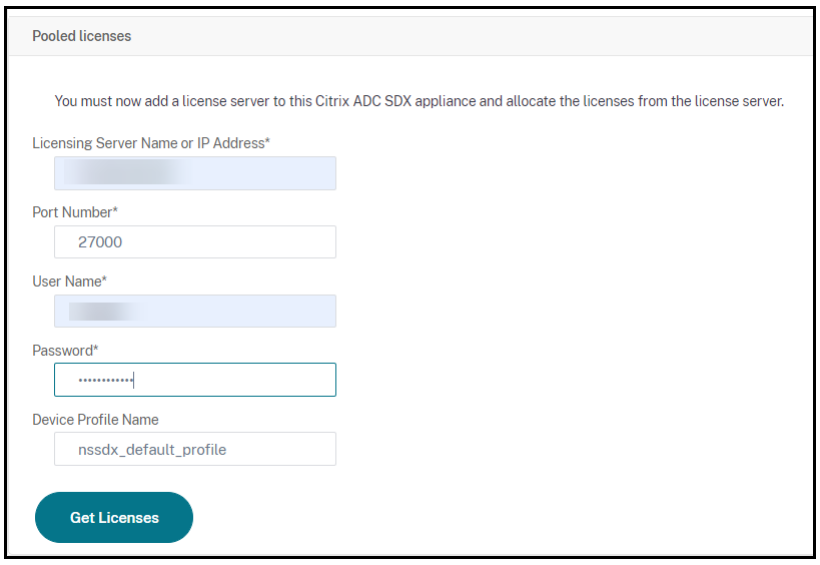
> **Nota**
>
> Para actualizar el dispositivo SDX a la licencia de capacidad agrupada de NetScaler, debe cargar la licencia SDX-Z en el dispositivo.
>
> Asegúrese de tener permiso para agregar instancias de NetScaler en NetScaler Console.

Para actualizar a la capacidad agrupada de NetScaler:

1. En un explorador web, escriba la dirección IP del dispositivo SDX. Por ejemplo: http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero. 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, aparecerá una sección de **licencias** agrupadas en la página **Licencias**.
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.

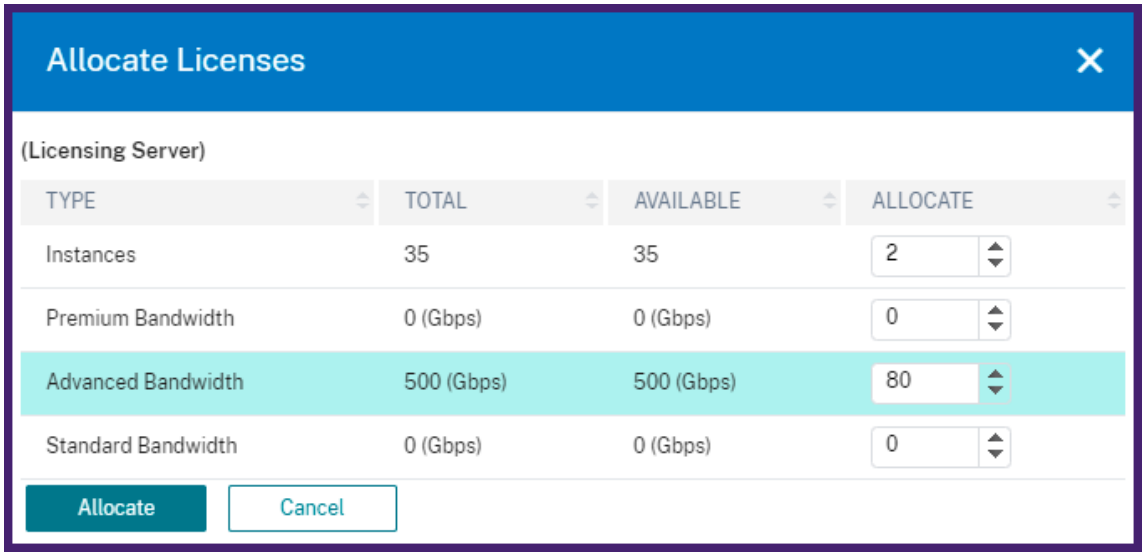
   Si desea configurar el servidor de NetScaler Console como un servidor de licencias, especifique la dirección IP del servidor de NetScaler Console.

   Si utiliza un agente para comunicarse con el servidor de NetScaler Console, especifique la dirección IP del agente.

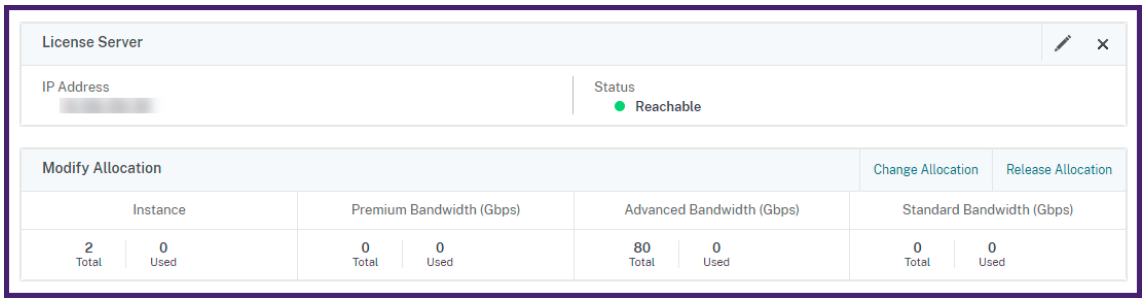
b) En el campo **Número de puerto**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) 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.

Escenarios de caducidad de licencias flexibles o agrupadas y comportamiento de problemas de conectividad

January 26, 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 licencia nueva en NetScaler Console 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 licencia nueva en NetScaler Console 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 licencia nueva en NetScaler Console 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 licencia nueva en NetScaler Console:

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 agente, o entre el agente y el servicio NetScaler Console, 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 NetScaler Console solo como servidor de licencias Flexed o Pooled

January 26, 2024

Como administrador, puede configurar la consola de NetScaler solo para la función de licencias agrupadas. Con esta configuración, la consola de NetScaler 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 estas situaciones, puede implementar una instancia local de un servidor de NetScaler Console en su zona reguladora para utilizar las

capacidades de administración, supervisión y análisis. Si utiliza la función de licencias agrupadas del mismo modo, tiene que dividir las licencias agrupadas en varios servidores de licencias de NetScaler Console. Este enfoque no le brinda la flexibilidad necesaria para asignar licencias agrupadas entre las instancias de NetScaler implementadas en todo el mundo.

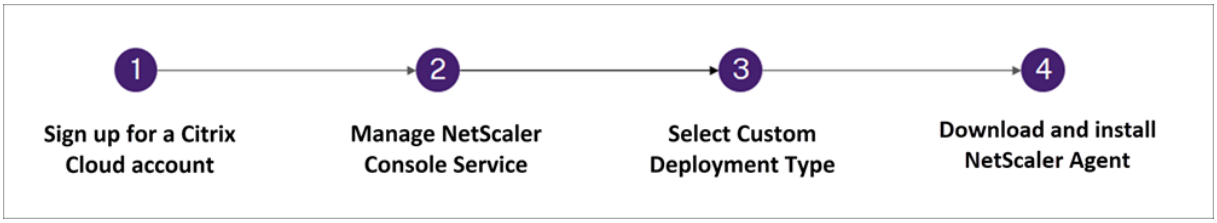
Por lo tanto, configure la consola de NetScaler solo para la función de licencias agrupadas. La consola de NetScaler solo recibe datos de licencias de todas las instancias de NetScaler. Por lo tanto, puede cumplir con el mandato reglamentario y asignar de forma dinámica las licencias de capacidad agrupada entre las instancias de NetScaler implementadas en todo el mundo.

En este documento se explica cómo configurar la consola de NetScaler únicamente para la función de licencias agrupadas.

Requisitos previos

Antes de configurar la consola de NetScaler solo para la función de licencias agrupadas, complete la primera vez que incorpore y configure la consola de NetScaler. Asegúrese de revisar las especificaciones del agente en los requisitos del sistema.

> **Importante**
>
> La primera vez que incorpore o configure la consola NetScaler, asegúrese de lo siguiente:
>
> - Se selecciona la opción Implementación personalizada.
> - Las instancias de NetScaler se agregarán después de completar el paso 4 de este procedimiento de configuración



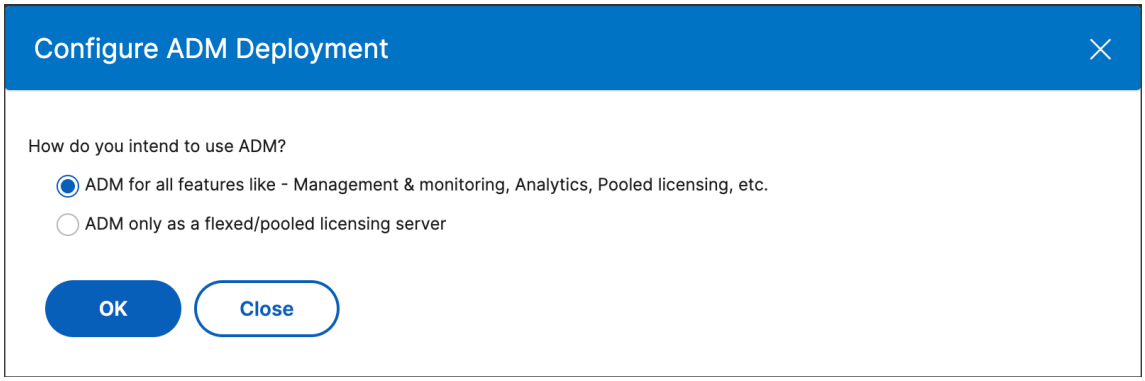
Para obtener más información sobre la incorporación y la configuración de NetScaler Console, consulte Cómo empezar.

Tras completar los pasos de incorporación, configure la consola de NetScaler solo para la función de licencias agrupadas.

Cómo configurar NetScaler Console solo como servidor de licencias Flexed o Pooled

Haga lo siguiente para configurar la consola de NetScaler solo para la función de licencias:

1. Vaya a **Configuración > Configuración global > Configuraciones del sistema > Implementación del sistema**.
2. En **NetScaler Console Deployment**, seleccione **NetScaler Console solo como servidor de licencias flexible/agrupado**.



3. Haga clic en **Aceptar**.

   Esta acción conserva únicamente la función de licencias agrupadas y desactiva las siguientes funciones de NetScaler Console:

   - Respaldo de NetScaler Console
   - 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 Console está deshabilitada. Asegúrese de inhabilitar esta función si la ha habilitado.

   En el cuadro de confirmación, haga clic en **Sí**.

   La GUI de NetScaler Console ahora solo muestra la función de licencias agrupadas. Y las funciones restantes no aparecen.

4. Después de configurar NetScaler Console solo para la función de licencias, añada instancias de NetScaler en la página **Infraestructura > Instancias**.

> **Nota**
>
> - También puede agregar una instancia de NetScaler a NetScaler Console y a otros servidores de NetScaler Console. Al cambiar la contraseña de dichas instancias de NetScaler, asegúrese de actualizar la contraseña en todos los servidores de NetScaler Console en los

> que se descubra la instancia. Esta nota se aplica cuando la consola de NetScaler está configurada únicamente para usar la función de licencias agrupadas.
>
> - Un usuario aún puede realizar algunas operaciones con las funciones deshabilitadas en la GUI de NetScaler Console. Por ejemplo, el sondeo de eventos y el backup de NetScaler. Como superadministrador, Si quiere restringir tales operaciones, inhabilite los accesos de usuario para otros administradores mediante una directiva de acceso adecuada. Para obtener más información, consulte Configurar políticas de acceso en NetScaler Console.

Licencias de registro y salida de NetScaler VPX

January 26, 2024

Puede asignar licencias de NetScaler VPX a instancias de NetScaler VPX a petición desde NetScaler Console. Las licencias se almacenan y administran mediante NetScaler Console, que cuenta con un marco de licencias que proporciona un aprovisionamiento de licencias escalable y automatizado. Una instancia de NetScaler VPX, una vez aprovisionada, puede extraer la licencia de NetScaler Console o volver a consultar su licencia en NetScaler Console cuando se elimina o destruye una instancia.

Instalar licencias en NetScaler Console

Para instalar los archivos de licencia en la consola de NetScaler:

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 subirlo a la consola.
   - **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 añaden a NetScaler Console.

   > **Nota**
   >
   > Asegúrese de estar conectado a Internet antes de usar el código de acceso de la licencia para instalarlas.

Asigne la licencia de NetScaler VPX a una instancia de NetScaler VPX mediante la GUI de NetScaler

1. Inicie sesión en la instancia de NetScaler VPX y vaya a **Sistema > Licencias > Administrar licencias**, haga clic en **Agregar nueva licencia**y seleccione **Usar licencias remotas**.
2. Introduzca los detalles del servidor de licencias en el campo **Nombre del servidor/dirección IP**.

   > Nota
   >
   > Si desea administrar las licencias de NetScaler VPX de su instancia a través de NetScaler Console, seleccione la casilla **Registrarse en NetScaler MA Service** e introduzca las credenciales de NetScaler Console .

3. Haga clic en **Continuar**.
4. 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**.
5. 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.

6. Para cambiar o liberar la asignación de licencias, vaya a **Sistema > Licencias > Administrar licencias** y seleccione **Cambiar asignación o Asignación** de **versiones** .
7. 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 una licencia de NetScaler VPX a una instancia de NetScaler VPX 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:

```
1 add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
      port number >]
```



```
> 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
```

```
> 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 a una instancia de NetScaler VPX, introduzca el siguiente comando:

```
set capacity  –platform V[S/E/P][Bandwidth]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

Configurar comprobaciones de caducidad para las licencias de registro y salida de NetScaler VPX

Ahora puede configurar el umbral de caducidad de las licencias de NetScaler VPX. Al establecer los umbrales, NetScaler Console 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 Console.

Se genera un evento cuando se envía una notificación de caducidad de licencia y este evento se puede ver en NetScaler Console.

Para obtener más información, consulte Administración de licencias .

Licencias de CPU virtual NetScaler

January 26, 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

Tal 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 casos, el requisito de ancho de banda puede ser menor, pero el requisito es más para otro rendimiento de L7, como SSL TPS, rendimiento de compresión, etc. Es posible que la actualización de la licencia NetScaler 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 Console 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 la capacidad de licencias agrupadas y las funcionalidades de licencias de CICO, el servidor de licencias de NetScaler Console 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**
   >
   > Registre siempre la instancia de NetScaler VPX con NetScaler Console. Si aún no lo ha hecho, habilite Registrar en NetScaler Console y escriba las credenciales de inicio de sesión de NetScaler Console.

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**.

   > **Nota** Para un par de NetScaler HA, asigne licencias de CPU virtuales a cada nodo por separado.

8. Haga clic en **Reiniciar** en la página siguiente para solicitar las licencias.

   > **Nota**También
   >
   > puede liberar la licencia actual y salir de una edición diferente. Por ejemplo, ya está ejecutando la licencia Standard Edition en su instancia. Puede liberar esa licencia y luego retirarse de la edición Advanced.

Preguntas frecuentes y otros recursos

April 10, 2024

En esta sección se enumeran los documentos de referencia sobre la configuración y el funcionamiento de las licencias agrupadas. Puede consultar estos documentos para obtener ayuda relacionada con problemas de configuración y operación.

Configuración

1. ¿Dónde puedo encontrar información sobre la descripción general y las características de la capacidad agrupada?

   Respuesta: Consulte Configurar la capacidad agrupada .

2. ¿Cómo puedo convertir o migrar licencias perpetuas a licencias agrupadas y viceversa?

   Respuesta: 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.

3. ¿Cómo se implementa el servidor de NetScaler Console?

   Respuesta: Siga el documento de introducción.

4. ¿Cómo puedo añadir una licencia a una licencia agrupada existente y asignarla?

   Respuesta: Siga el documento de administración de licencias .

5. ¿Cómo asigno/aumento de la capacidad y el ancho de banda en las instancias?

   Respuesta: Siga el documento de administración de licencias .

Agente de servidor de licencias

1. ¿Cómo asigno el rol LSA a un agente específico?

   Respuesta: Al primer agente desplegado se le asigna la función LSA. Si el agente de LSA deja de funcionar, todas las instancias de NetScaler conectadas a NetScaler Console para obtener licencias agrupadas entran en un período de gracia de un día. Al día siguiente, NetScaler Console selecciona un nuevo agente como LSA. Este comportamiento está activado de forma predeterminada.

   Los administradores pueden seleccionar manualmente un agente de NetScaler como LSA en un plazo de 24 horas, en lugar de esperar a que el servicio NetScaler Console seleccione automáticamente un agente después de 24 horas de inactividad del LSA.

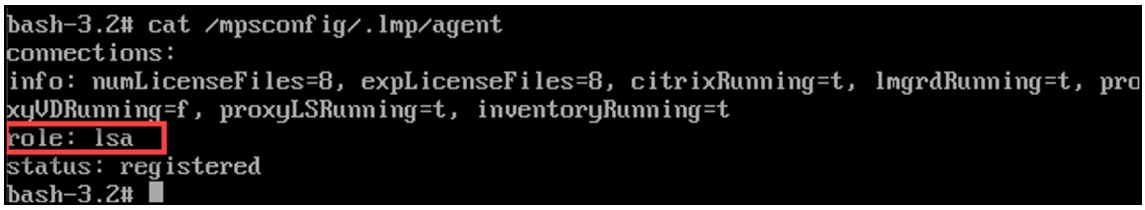
   > **Nota:**
   >
   > Durante esta transición, la funcionalidad de NetScaler no se ve afectada.

2. ¿Cómo podemos determinar qué agente aloja la función del servidor de licencias?

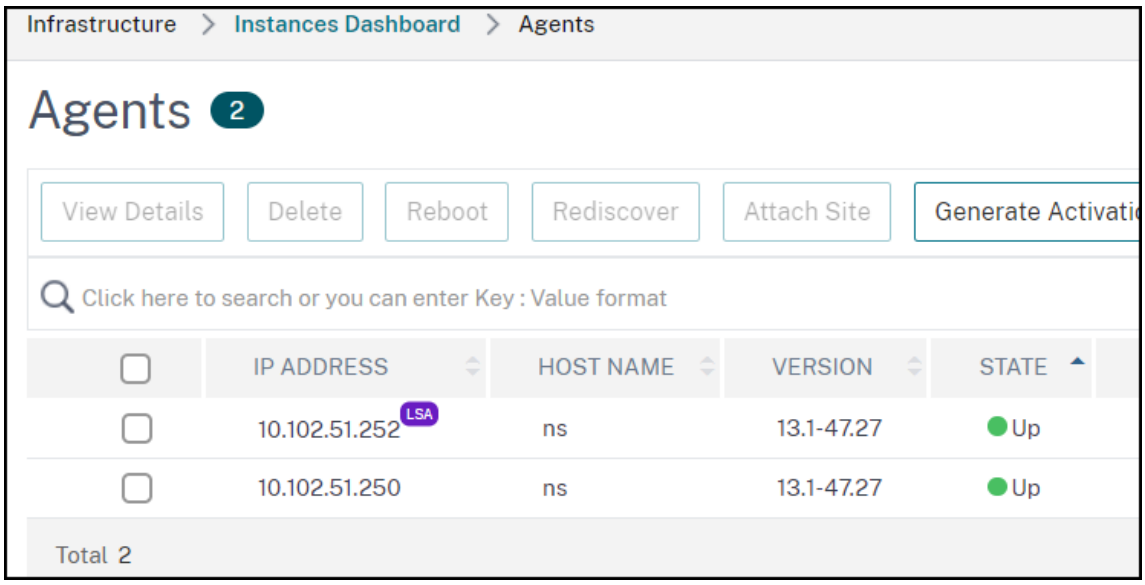
   Respuesta: Para saber qué agente aloja la función LSA, puede ejecutar el siguiente comando en el shell:

   ```
   cat /mpsconfig/.lmp/agent
   ```


Si el valor de salida de "rol"es **lsa**, entonces ese agente aloja el rol de servidor de licencias.



En la GUI de NetScaler Console, verá el LSA escrito junto a la dirección IP del agente designado.



3. ¿Qué ocurre cuando el agente que aloja la función de LSA deja de funcionar?

   Respuesta: Si el agente que aloja la función de LSA está desconectado, todos los dispositivos NetScaler implementados configurados para la concesión de licencias de capacidad agrupada entran en período de gracia. El período de gracia dura 30 días y los recursos asignados a los dispositivos NetScaler persisten durante este período. Las instancias de NetScaler en este estado no pueden asignar ni modificar la asignación de licencias hasta que el agente que aloja la función LSA vuelva a estar en línea o se designe un nuevo agente con la función LSA.

4. Si el agente que aloja el puesto de LSA se desconecta durante un período prolongado, ¿habrá una reelección?

   Respuesta: Si el administrador no selecciona un nuevo LSA en un plazo de 24 horas, el servicio NetScaler Console selecciona automáticamente el siguiente agente que esté ACTIVO como nuevo LSA transcurridas 24 horas desde que el agente LSA esté inactivo. El período de gracia de los dispositivos NetScaler finaliza una vez que se elige la nueva LSA.

Problemas comunes

1. Instancias que se ejecutan en modo de gracia debido a un error de conectividad, una actualización, una división del cerebro, etc.

   Respuesta: Consulte el comportamiento del servidor de licencias de NetScaler Console documentado en Configuración de la capacidad agrupada de NetScaler .

2. Licencias que no se aplican ni reflejan en instancias.

   Respuesta: Consulte Solucionar problemas de licencias de capacidad agrupada .

3. La asignación de licencias se bloquea en "sincronización en curso".

   Respuesta: Consulte Solucionar problemas de licencias de capacidad agrupada .

4. Error debido a un ID de host incorrecto en el archivo de licencia.

   Respuesta: Para identificar un servidor de NetScaler Console, puede asignarle un nombre de host. El nombre del host aparece en la licencia universal de NetScaler Console. Para obtener más información, consulte Asignar un nombre de host a un servidor de NetScaler Console .

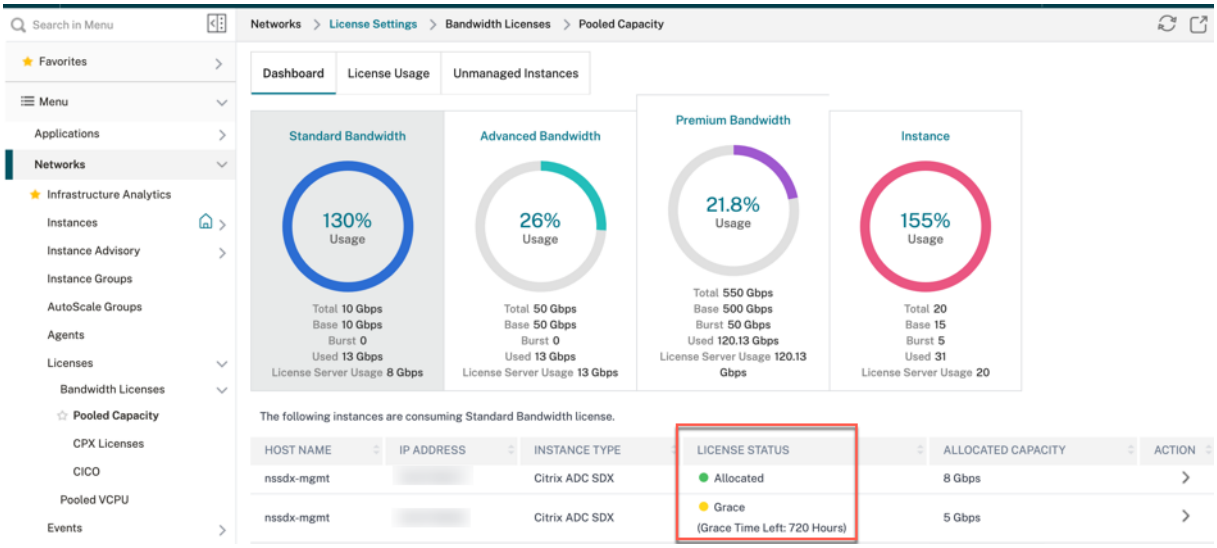
Solución de problemas de licencias de capacidad agrupada

January 26, 2024

En esta sección se describe cómo analizar y solucionar problemas comunes de capacidad agrupada.

Comprobar el estado de licencia

La consola NetScaler actúa como un servidor de licencias para su licencia de capacidad agrupada de NetScaler. Puede usar la GUI de NetScaler Console para comprobar el estado de la licencia. Vaya a **Infraestructura > Licencias agrupadas > Capacidad agrupada > Uso de licencias**.



En la tabla siguiente se enumeran los tipos de estado de licencia y lo que significan

Estado	Lo que significa
Asignado	El estado de la licencia está bien.
Asignado: no se aplica en NetScaler	Es posible que NetScaler necesite reiniciarse si la licencia se retiró o se registró desde NetScaler, pero NetScaler aún no se ha reiniciado.
No asignado	La licencia no está asignada en la instancia de NetScaler.
¡Grace	La instancia de NetScaler se encuentra en el período de gracia de la licencia durante 30 días
Sincronización en curso	NetScaler Console obtiene información de NetScaler en intervalos de 2 minutos. La sincronización de las licencias entre NetScaler Console y NetScaler puede tardar hasta 15 minutos. Es posible que NetScaler Console se haya reiniciado o que se haya activado la conmutación por error de NetScaler Console HAS.

Estado	Lo que significa
Parcialmente asignado	NetScaler no puede aceptar la capacidad asignada porque podría estar ejecutándose en su asignación máxima. Por ejemplo, NetScaler se ejecuta con una capacidad de grupo de licencias de 10 Gbps. Cuando NetScaler se reinicia, los 10 Gbps se vuelven a registrar en el servidor de licencias de NetScaler Console. Cuando NetScaler vuelve a estar en línea, intenta comprobar automáticamente los 10 Gbps asignados anteriormente. Mientras tanto, es posible que otras instancias de NetScaler hayan comprobado ese ancho de banda. La opción Asignado parcialmente aparece si el grupo de licencias no tiene suficiente capacidad para asignar 10 Gbps completos o incluso una capacidad parcial a este NetScaler.
No administrado	NetScaler no se agrega a NetScaler Console para facilitar la administración. Esto no afecta a las licencias de NetScaler, pero puede afectar a la supervisión de las licencias desde NetScaler Console.
No administrado	NetScaler no se agrega a NetScaler Console para facilitar la administración. Esto no afecta a las licencias de NetScaler, pero puede afectar a la supervisión de las licencias desde NetScaler Console.
Conexión perdida	No se puede acceder a NetScaler desde NetScaler Console para facilitar la administración. Por ejemplo, hay problemas de conectividad de red, NITRO no funciona o no coincide con las contraseñas de NetScaler. Si NITRO no funciona o no coincide con las contraseñas de NetScaler, esto no afecta a las licencias de NetScaler. Sin embargo, puede afectar a la supervisión de licencias desde NetScaler Console.

Comprobar el estado del servidor

En esta sección se describen los problemas comunes de estado del servidor y las posibles razones y correcciones.

Problema: NetScaler muestra el servidor de licencias como inaccesible y el estado de la licencia cambia a correcto.

- La conexión al servidor de licencias (NetScaler Console o agente) se interrumpió durante más de 15 minutos. Compruebe si el servidor de licencias está activo y accesible.
- NetScaler está en modo de gracia.

Problema: NetScaler muestra el estado del servidor de licencias como accesible, pero el intento del usuario de cambiar la asignación no tiene ningún efecto. Al hacer clic en **Cambiar asignación**, se devuelve 0 0. Este valor puede hacer que parezca que la capacidad configurada se ha perdido.

- La conexión al servidor de licencias se interrumpió recientemente, pero el NetScaler aún no ha perdido ni un segundo latido. Por lo tanto, no está en gracia (todavía). Compruebe si el servidor de licencias está activo y accesible.

Problema: NetScaler muestra la capacidad y el recuento de instancias, pero se puede acceder o no se puede **acceder** al servidor de licencias. Al hacer clic en **Cambiar asignación** se devuelven algunos números, pero no se tiene en cuenta la capacidad configurada.

- Se restableció la conexión con el servidor de licencias, pero el NetScaler aún no ha captado el segundo latido ni ha enviado la sonda de reconexión.

Problema: NetScaler indica que no se puede conectar al servidor de licencias al configurar las licencias agrupadas con NetScaler Console

- Compruebe las reglas del firewall para asegurarse de que los puertos 27000 y 7279 estén abiertos.
- El agente no está registrado. Para obtener más información, consulte Introducción.
- La consola de NetScaler no tiene archivos de licencia cargados. Para obtener más información, consulte Configurar la capacidad agrupada de NetScaler
- NetScaler Console tiene un archivo de licencia incorrecto.

Comprobar el informe de uso de la licencia

En **NetScaler Licensing > Licencias agrupadas > Licencias de ancho de banda > Capacidad agrupada > Uso** de licencias en la GUI de NetScaler Console, puede ver el pico mensual de uso de licencias. Puede usar este informe para aumentar el uso de la licencia o planificar la compra de una licencia adicional.

Los siguientes son algunos detalles de cómo se genera el informe y se puede utilizar.

Sondeo: los datos de licencia de las instancias de NetScaler se consultan cada 15 minutos.

Mantenimiento de picos por hora: NetScaler Console solo mantiene el uso máximo de licencias en una hora, por dispositivo.

Informes: puede generar un informe de GUI para cada instancia, para un intervalo de tiempo específico.

Exportación: puede exportar informes como en formato CSV o XLS.

Depuración: NetScaler Console purga los datos el primer día de cada mes a las 12:10 a.m. El período de purga es configurable (el período predeterminado es de dos meses).

Contadores y estadísticas para las licencias de capacidad agrupadas

Los siguientes contadores, registros y comandos muestran las métricas de licencias agrupadas de NetScaler que indican el comportamiento de las instancias de NetScaler Console y NetScaler en el modo de licencias agrupadas.

- **Capturas**SNMP: disponibles a partir de la versión 13.xx de NetScaler.
- **Contadores NSCONMSG para limitar**la velocidad: disponibles en la versión 12.1 57.xx de NetScaler.
- **Contadores**de consola de NetScaler Las acciones de comando de la consola de NetScaler están disponibles en el servicio NetScaler Cloud.

Trampas SNMP

Puede configurar las siguientes alarmas agrupadas de licencias agrupadas contra trampas SNMP v.13

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

Para obtener más información sobre estas alarmas, consulte la referencia de OID SNMP de NetScaler.

Contador NSCONMSG

Compruebe los siguientes `NCCONMSG` contadores y lo que significan:

- `allnic_err_rl_cpu_pkt_drops`: desaparece el paquete agregado (todas las NIC) después de alcanzar el límite de CPU
- `allnic_err_rl_pps_pkt_drops`: paquete agregado cae en todo el sistema después del límite de pps
- `allnic_err_rl_rate_pkt_drops`: la tasa agregada disminuye en todo el sistema
- `allnic_err_rl_pkt_drops`: caídas de limitación de velocidad acumulada debido a la tasa, pps y CPU
- `rl_tot_ssl_rl_enforced`: número de veces que se aplicó SSL RL (en nuevas conexiones SSL)
- `rl_tot_ssl_rl_data_limited`: número de veces que se alcanzó el límite de rendimiento de SSL
- `rl_tot_ssl_rl_sess_limited`: número de veces que se alcanzó el límite de SSL TPS

Contadores de consola NetScaler

Al elegir la acción de evento **Run Command Action**, puede crear un comando o un script que se pueda ejecutar en NetScaler Console para los 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 definidas 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.

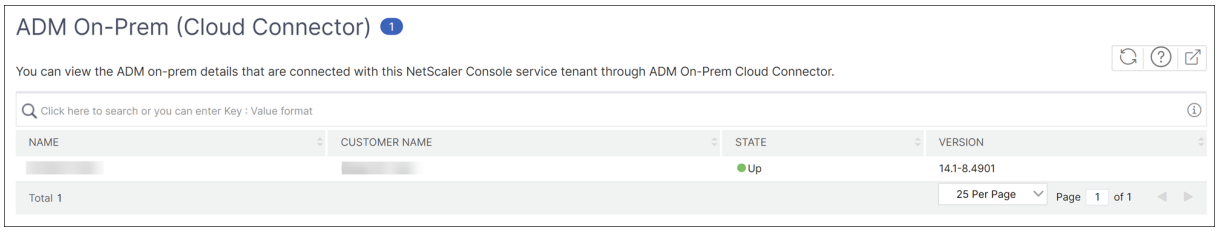
Parámetro	Descripción
$failure.obj	El objeto de error afecta a la forma en que se procesa un evento y garantiza que el objeto de error refleje el problema exacto tal como se notificó. Este parámetro se puede usar para rastrear los problemas rápidamente e identificar el motivo del error, en lugar de simplemente informar de los eventos sin procesar.

> **Nota**
>
> Durante la ejecución del comando, estos parámetros se reemplazan con valores reales.

Instancias locales de consola conectadas con el servicio de consola mediante Cloud Connect

March 6, 2024

En **Configuración > NetScaler Console**On-Prem, puede ver los detalles de las instancias locales de la consola que están conectadas con el arrendatario del servicio de la consola a través de Cloud Connect.



- **Nombre** : la dirección IP de la consola local de NetScaler
- **Nombre**del cliente : el nombre del arrendatario del servicio de NetScaler Console
- **Estado** : el estado de conectividad entre la instancia local de NetScaler Console y el servicio de NetScaler Console
- **Versión** : la versión de creación de instancias locales de NetScaler Console

Carga local en Console

July 17, 2024

Esta página solo es aplicable a los usuarios locales de NetScaler que han optado por el modo manual para cargar sus datos de telemetría en el servicio NetScaler Console. Asegúrese de haber descargado los datos de telemetría de la consola NetScaler local (haga clic en **Descargar telemetría** en la página principal de **NetScaler Telemetry** para descargar el archivo de paquete (.tgz) que contiene los datos de telemetría necesarios).

Para cargar la telemetría de datos en el servicio NetScaler Console:

1. En la página de **carga local de NetScaler Console**, haga clic en **Cargar telemetría** y seleccione el archivo descargado (.tgz) para completar el proceso de carga.
2. Complete la primera carga en un plazo de 30 días a partir de la selección del modo manual. Repita el mismo procedimiento y suba el archivo de telemetría cada 90 días a partir de entonces.

> **Notas:**
>
> - La carga falla si el archivo no está en un formato válido (.tgz) o si el archivo no pasa las comprobaciones de integridad. La recomendación es volver a descargarlo y volver a intentar subirlo. Si el problema persiste, ponte en contacto con el servicio de atención al cliente.
> - Puede inhabilitar los datos de telemetría opcionales. Para inhabilitar, en NetScaler Console local, primero debe inhabilitar el **aviso de seguridad** en la página de **telemetría de NetScaler** y, a continuación, ir a **Configuración > Administración > Habilitar o inhabilitar el uso compartido de datos de las funciones de la consola** y desactivar la casilla **Acepto compartir los datos de uso de las funciones de la consola**.

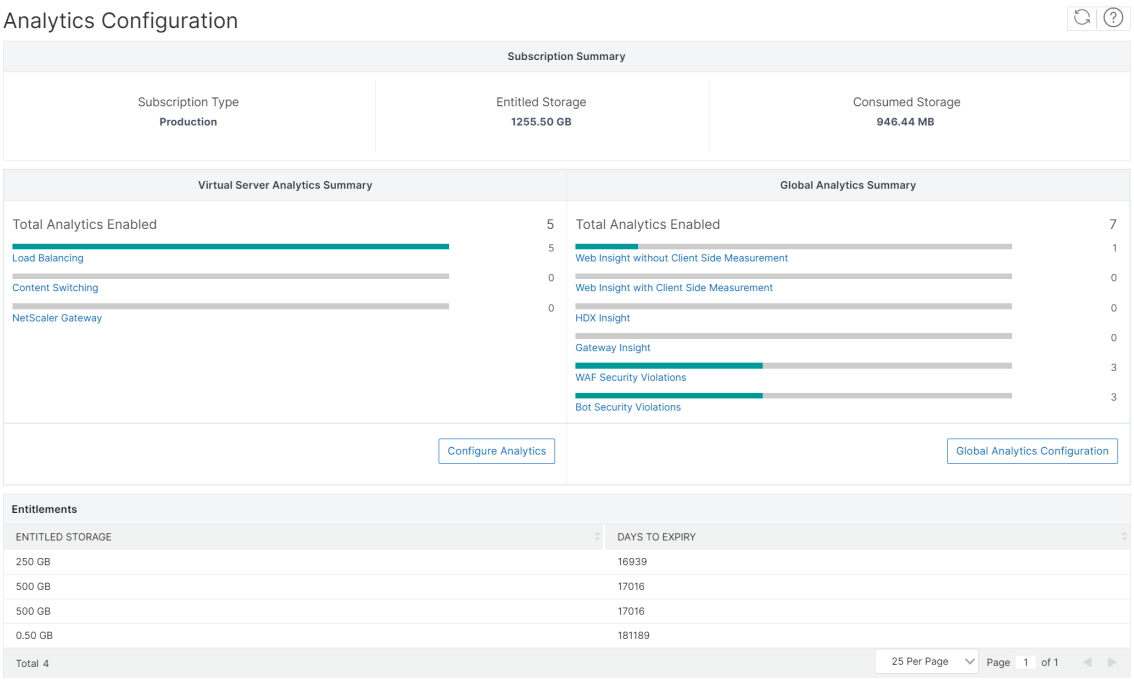
Configurar el análisis en servidores virtuales

March 6, 2024

A partir de la compilación 14.1-21.x, todos los servidores virtuales descubiertos 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 descubiertos.
- **Resumen de análisis global**: Le permite configurar los análisis en los servidores virtuales descubiertos y posteriores.



Configurar los análisis en los servidores virtuales descubiertos

> **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 seguridad y 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.
> 2
> 3 1. Seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Configurar análisis** .
> 4 1. En la página **Configurar análisis en servidores virtuales**, seleccione el servidor virtual y haga clic en **Habilitar seguridad y análisis**.
> ```

3. En la ventana **Habilitar seguridad y 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.

Tras hacer clic **en**Aceptar , NetScaler Console realiza los procesos para habilitar el análisis en los servidores virtuales seleccionados.

> **Nota**
>
> NetScaler Console usa NetScaler SNIP para Logstream y NSIP para IPFIX. Si hay un firewall habilitado entre el agente de NetScaler y la instancia de NetScaler, asegúrese de abrir el siguiente puerto para permitir que NetScaler Console 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 **Editar seguridad y análisis**.
   > ```

2. Haga clic en **Modificar seguridad y 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. Haga clic en **Desactivar análisis** .

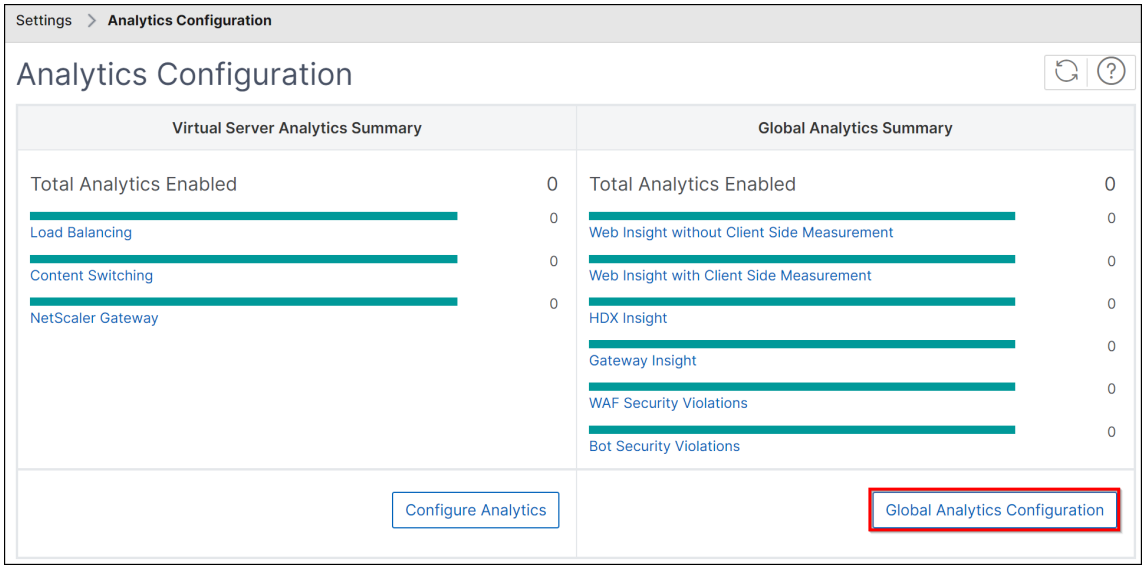
NetScaler Console desactiva los análisis en los servidores virtuales seleccionados.

En la tabla siguiente se describen las funciones de NetScaler Console 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 tanto en los servidores virtuales descubiertos como en los subsiguientes.

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 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 y que ha desactivado 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.

Configurar el control de acceso basado en roles

March 6, 2024

NetScaler Console proporciona un control de acceso detallado y basado en funciones (RBAC) con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales de su empresa.

En NetScaler Console, todos los usuarios se agregan a Citrix Cloud. Como primer usuario de su organización, primero debe crear una cuenta en Citrix Cloud y, a continuación, iniciar sesión en la GUI de NetScaler Console con las credenciales de Citrix Cloud. Se le otorga la función de superadministrador y, de forma predeterminada, tiene todos los permisos de acceso en NetScaler Console. Más adelante, puede crear otros usuarios en su organización en Citrix Cloud.

Los usuarios que se crean más adelante y que inician sesión en NetScaler Console como usuarios habituales se denominan administradores delegados. Estos usuarios, de forma predeterminada, tienen todos los permisos excepto los permisos de administración de usuarios. Sin embargo, puede conceder permisos de administración de usuarios específicos creando las directivas adecuadas y asignándolas a estos usuarios delegados. Los permisos de administración de usuarios se encuentran en **Configuración** > **Usuarios y roles**.

Para obtener más información sobre cómo asignar permisos específicos, consulte Cómo asignar permisos adicionales a usuarios administradores delegados.

En las siguientes secciones se proporciona más información sobre cómo crear directivas, roles, grupos y cómo vincular a los usuarios a los grupos.

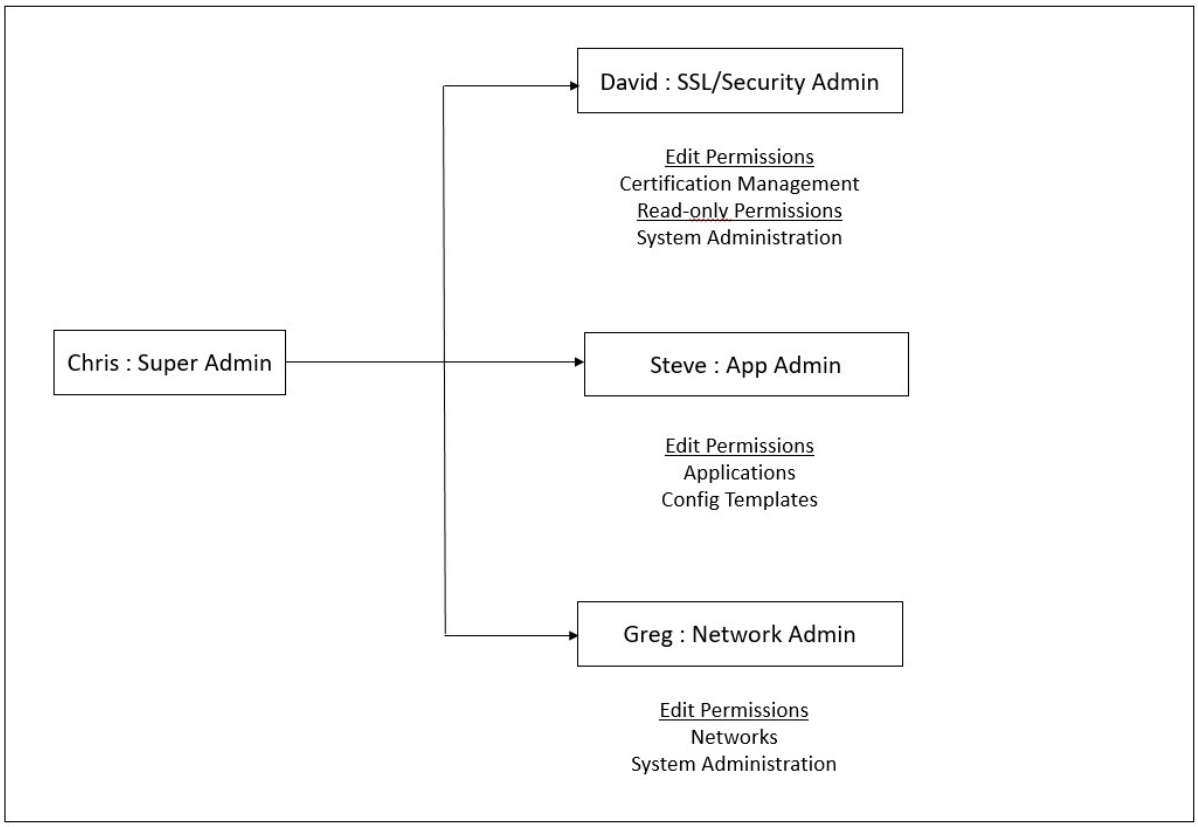
Ejemplo:

El siguiente ejemplo ilustra cómo se puede lograr el RBAC en NetScaler Console.

Chris, el jefe del grupo NetScaler, es el superadministrador de NetScaler Console en su organización. Crea tres funciones de administrador: Administrador de seguridad, administrador de aplicaciones y administrador de red.

- David, el administrador de seguridad, debe tener acceso completo para la administración y supervisión de certificados SSL, pero debe tener acceso de solo lectura para las operaciones de administración del sistema.
- Steve, un administrador de aplicaciones, necesita acceso solo a aplicaciones específicas y a plantillas de configuración específicas.
- Greg, un administrador de red, necesita acceso a la administración de sistemas y redes.
- Chris también debe proporcionar RBAC para todos los usuarios, independientemente del hecho de que sean locales o externos.

La imagen siguiente muestra los permisos que tienen los administradores y otros usuarios y sus roles en la organización.



Para ofrecer un control de acceso basado en roles a sus usuarios, Chris primero debe añadir usuarios en Citrix Cloud y solo después podrá ver a los usuarios en NetScaler Console. Chris debe crear directivas de acceso para cada uno de los usuarios en función de su función. Las directivas de acceso están estrechamente vinculadas a los roles. Por lo tanto, Chris también debe crear roles y, luego, debe crear grupos, ya que los roles se pueden asignar solo a grupos y no a usuarios individuales.

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 la 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 usuario puede observar el flujo de tráfico en las aplicaciones y ayudar a crear plantillas de configuración.

Las directivas determinan las funciones de los usuarios. Tras crear las directivas, puede crear funciones, vincular cada función a una o más directivas y asignar 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 al agregarlos a grupos específicos en función de condiciones específicas. En NetScaler Console, la creación de funciones y políticas es específica de la función RBAC de 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. Los administradores de aplicaciones solo pueden acceder a los recursos dentro de su ámbito.

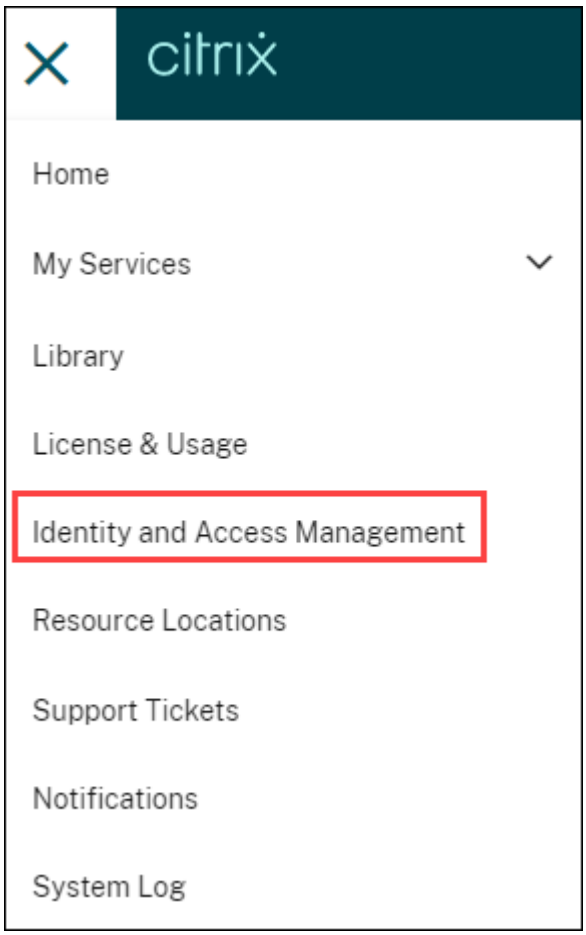
Por lo tanto, en su papel de Chris, el superadministrador, lleve a cabo las siguientes tareas de ejemplo en NetScaler Console para configurar las políticas de acceso, las funciones y los grupos de usuarios para David, que es el administrador de seguridad de su organización.

Configurar usuarios en la consola de NetScaler

Como superadministrador, puede crear más usuarios configurando cuentas para ellos en Citrix Cloud y no en NetScaler Console. Cuando los nuevos usuarios se agregan a NetScaler Console, solo puede definir sus permisos asignando los grupos apropiados al usuario.

Para agregar nuevos usuarios en Citrix Cloud:

1. En la GUI de NetScaler Console, haga clic en el icono de hamburguesa situado en la parte superior izquierda y seleccione **Administración de identidades y accesos**.

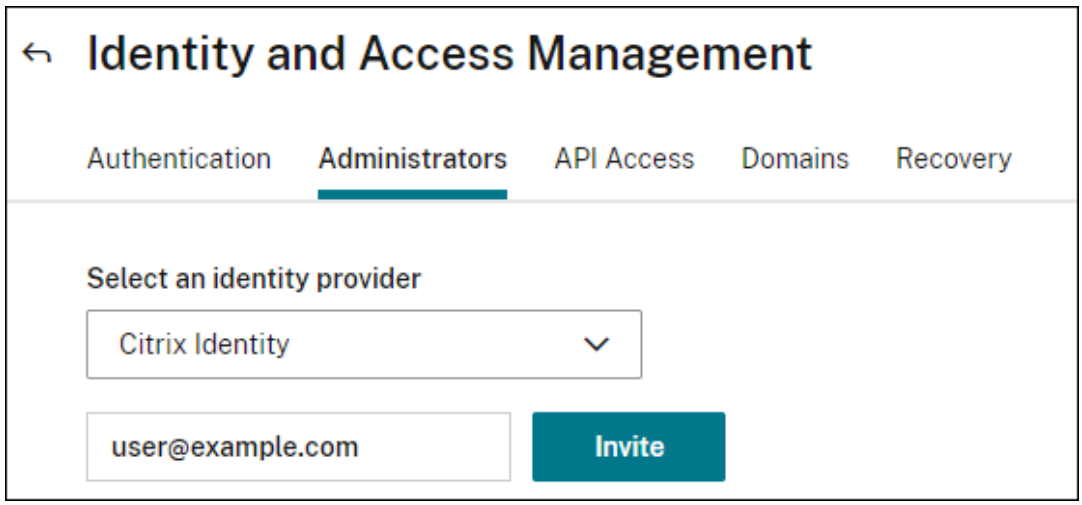


2. En la página Administración de identidades y accesos, seleccione la ficha **Administradores** .

   Esta ficha muestra los usuarios creados en Citrix Cloud.

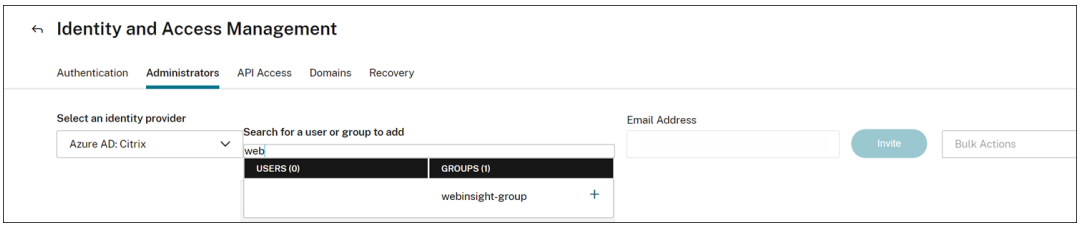
3. Seleccione el proveedor de identidad de la lista.

   - **Identidad**de Citrix : escriba la dirección de correo electrónico del usuario que quiere agregar en NetScaler Console y haga clic en **Invitar**.



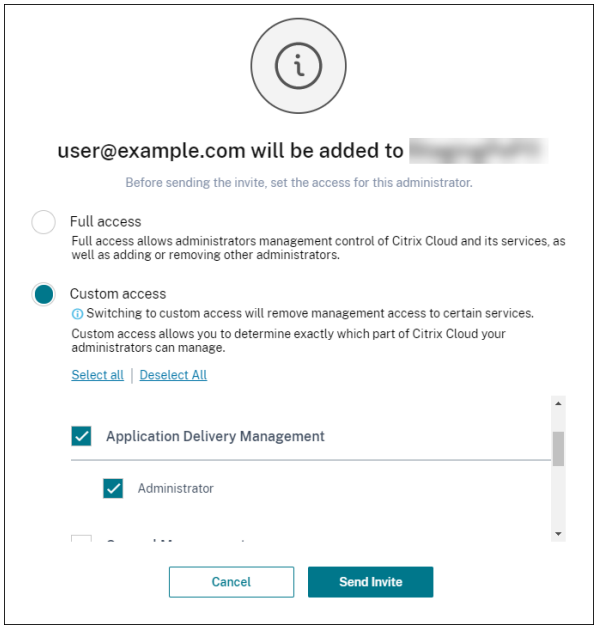
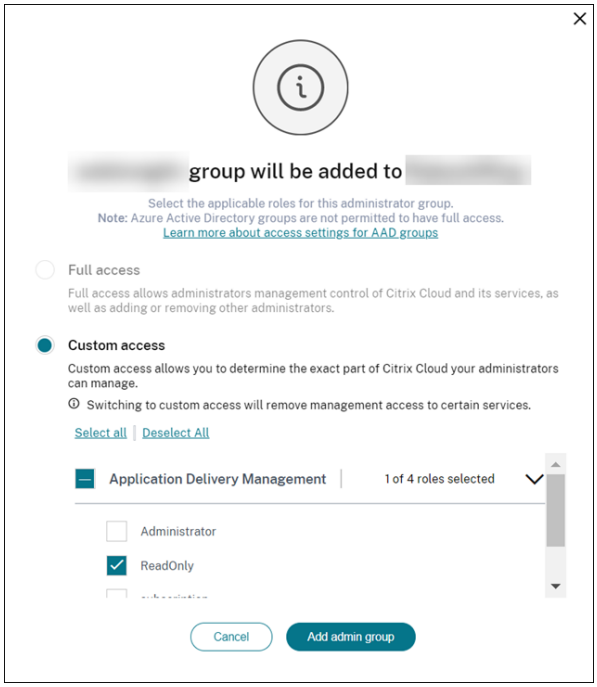
> **Nota:**
>
> El usuario recibe una invitación por correo electrónico de Citrix Cloud. El usuario debe hacer clic en el enlace incluido en el correo electrónico para completar el proceso de registro con su nombre completo y contraseña y, más adelante, iniciar sesión en NetScaler Console con sus credenciales.

- **Azure Active Directory (AD)**: esta opción solo aparece si su Azure AD está conectado a Citrix Cloud; consulte Conectar Azure Active Directory a Citrix Cloud. Al seleccionar esta opción para invitar a usuarios o grupos, solo puede especificar el **acceso personalizado** para el usuario o grupo seleccionado. Los usuarios pueden iniciar sesión en NetScaler Console con sus credenciales de Azure AD. Además, no es necesario crear una identidad de Citrix para los usuarios que forman parte del Azure AD seleccionado. Si se agrega un usuario al grupo invitado, no es necesario que envíes una invitación para el usuario recién agregado. Este usuario puede acceder a NetScaler Console con las credenciales de Azure AD.



4. Seleccione **Acceso personalizado** para el usuario o grupo especificado.
5. Seleccione **Administración de entrega de aplicaciones**.

   Esta opción muestra los grupos de usuarios creados en NetScaler Console. Seleccione el grupo al que quiere agregar el usuario.

Identidad de Citrix	Azure AD
	
Haga clic en **Enviar invitación**.	Haga clic en **Agregar grupo de administradores**.

Como administrador, verá al nuevo usuario en la lista de usuarios de NetScaler Console solo después de que el usuario inicie sesión en NetScaler Console.

Para configurar los usuarios en NetScaler Console:

1. En la GUI de NetScaler Console, vaya a **Configuración** > **Usuarios y funciones** > **Usuarios** .
2. El usuario se muestra en la página **Usuarios**.
3. Puede modificar los privilegios proporcionados al usuario seleccionándolo y haciendo clic en **Modificar**. También puede modificar los permisos de grupo en la página **Grupos** del nodo **Configuración**.

   > **Nota:**
   >
   > - Los usuarios se agregan a NetScaler Console únicamente desde Citrix Cloud. Por lo tanto, aunque tenga permisos de administrador, no puede agregar ni eliminar usuarios en la GUI de NetScaler Console. Solo puede modificar los permisos de grupo. Se pueden agregar o eliminar usuarios de Citrix Cloud.
   > - Los detalles del usuario aparecen en la GUI del servicio solo después de que el usuario haya iniciado sesión en la consola de NetScaler al menos una vez.

Configurar las políticas de acceso en la consola de NetScaler

Las directivas de acceso definen los permisos. Se puede aplicar una directiva a un grupo de usuarios o a varios grupos mediante la creación de roles. Las directivas determinan las funciones de los usuarios. Después de crear directivas, debe crear roles, enlazar cada rol a una o varias directivas y asignar roles a grupos de usuarios. NetScaler Console proporciona cinco políticas de acceso predefinidas:

- **admin_policy**. Otorga acceso a todos los nodos de NetScaler Console. El usuario tiene permisos de visualización y edición, puede ver todo el contenido de NetScaler Console y realizar todas las operaciones de edición. Es decir, el usuario puede agregar, modificar y eliminar operaciones en los recursos.
- **adminExceptSystem_Policy**. Concede acceso a los usuarios a todos los nodos de la GUI de NetScaler Console, excepto el acceso al nodo Configuración.
- **readonly_policy**. Otorga permisos de solo lectura. El usuario puede ver todo el contenido en NetScaler Console, pero no está autorizado a realizar ninguna operación.
- **appadmin_policy**. Otorga permisos administrativos para acceder a las funciones de la aplicación en NetScaler Console. Un usuario vinculado a esta directiva puede:
  - Agregar, modificar y eliminar aplicaciones personalizadas
  - Habilitar o inhabilitar los servicios, los grupos de servicios y los distintos servidores virtuales, como la conmutación de contenido y la redirección de la memoria caché
- **appreadonly_policy**. 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.

Aunque no puede modificar estas directivas predefinidas, puede crear sus propias directivas (definidas por el usuario).

Anteriormente, al asignar políticas a los roles y vincular los roles a los grupos de usuarios, podía proporcionar permisos para los grupos de usuarios a nivel de nodo en la GUI de NetScaler Console. Por ejemplo, solo puede proporcionar permisos de acceso a todo el nodo de **equilibrio de carga** . Sus usuarios tenían permiso para acceder a todos los subnodos específicos de la entidad en **Equilibrio de carga** (por ejemplo, servidor virtual, servicios y otros) o no tenían permiso para acceder a ningún nodo en **Equilibrio de carga**.

En la compilación 507.x de NetScaler Console y en las versiones posteriores, la administración de políticas de acceso se amplía para proporcionar también permisos para los subnodos. La configuración de directiva de acceso se puede configurar para todos los subnodos, como servidores virtuales, servicios, grupos de servicios y servidores.

Actualmente, puede proporcionar un permiso de acceso de nivel tan granular solo para los subnodos de un nodo de **equilibrio de carga** y también para los subnodos del nodo **GSLB** .

Por ejemplo, como administrador, es posible que desee conceder al usuario un permiso de acceso solo para ver los servidores virtuales, pero no los servicios de back-end, los grupos de servicios y los servidores de aplicaciones del nodo de **equilibrio de carga** . Los usuarios a los que se les haya asignado una directiva de este tipo solo pueden acceder a los servidores virtuales.

Para crear directivas de acceso definidas por el usuario:

1. En la GUI de NetScaler Console, vaya a **Configuración** > **Usuarios y funciones** > **Políticas de acceso**.
2. Haga clic en **Agregar**.
3. En la página **Crear directivas de acceso**, en el campo **Nombre de la directiva**, introduzca el nombre de la directiva e introduzca la descripción en el campo **Descripción de la directiva**.

   En la sección **Permisos** se enumeran todas las funciones de NetScaler Console, con opciones para especificar el acceso de solo lectura, habilitar-deshabilitar o editar.

   a) Haga clic en el icono (+) para expandir cada grupo de funciones en muchas funciones.

   b) Seleccione la casilla de permisos situada junto al nombre de la función para conceder permiso a los usuarios.

   - **Ver:**esta opción permite al usuario ver la función en NetScaler Console.
   - **Activar y desactivar:**esta opción solo está disponible para las **funciones de red** que permiten activar o desactivar la acción en la consola de NetScaler. El usuario puede activar o desactivar la función. El usuario también puede realizar la acción **Sondear ahora** .

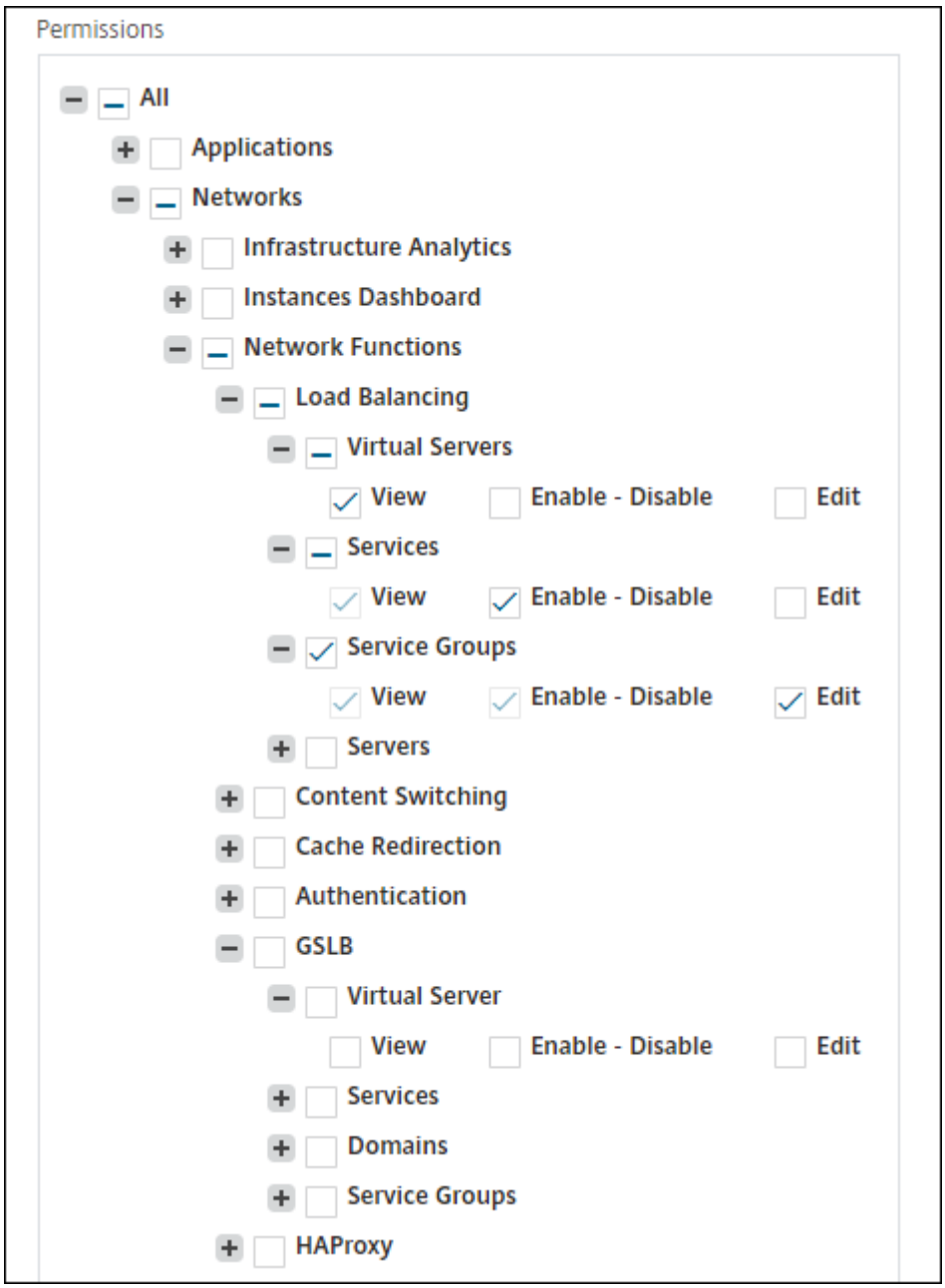
     Cuando se concede el permiso **Habilitar-Inhabilitar** a un usuario, también se concede el permiso **Ver**. No puede anular la selección de esta opción.
   - **Modificar:** esta opción otorga el acceso total al usuario. El usuario puede modificar la función y sus funciones.

     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 **Load Balancing** 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 Console. 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 Sondear 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**.

4. Haga clic en **Crear**.

> **Nota:**
>
> Al seleccionar **Modificar**, es posible que se asignen internamente permisos dependientes que no se muestran como habilitados en la sección Permisos. Por ejemplo, al habilitar los permisos de edición para la administración de errores, NetScaler Console proporciona internamente permisos para configurar un perfil de correo o para crear configuraciones de servidores SMTP, de modo que el usuario pueda enviar el informe como correo.

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 funciones en la consola de NetScaler

En NetScaler Console, cada rol está vinculado a una o más políticas 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 política puede conceder permiso para agregar instancias de NetScaler en NetScaler Console y la otra política puede conceder permiso para crear e implementar un StyleBook y configurar instancias de NetScaler.

Cuando varias directivas definen los permisos de edición y de solo lectura para una única entidad, los permisos de edición tienen prioridad sobre los permisos de solo lectura.

NetScaler Console proporciona cinco funciones predefinidas:

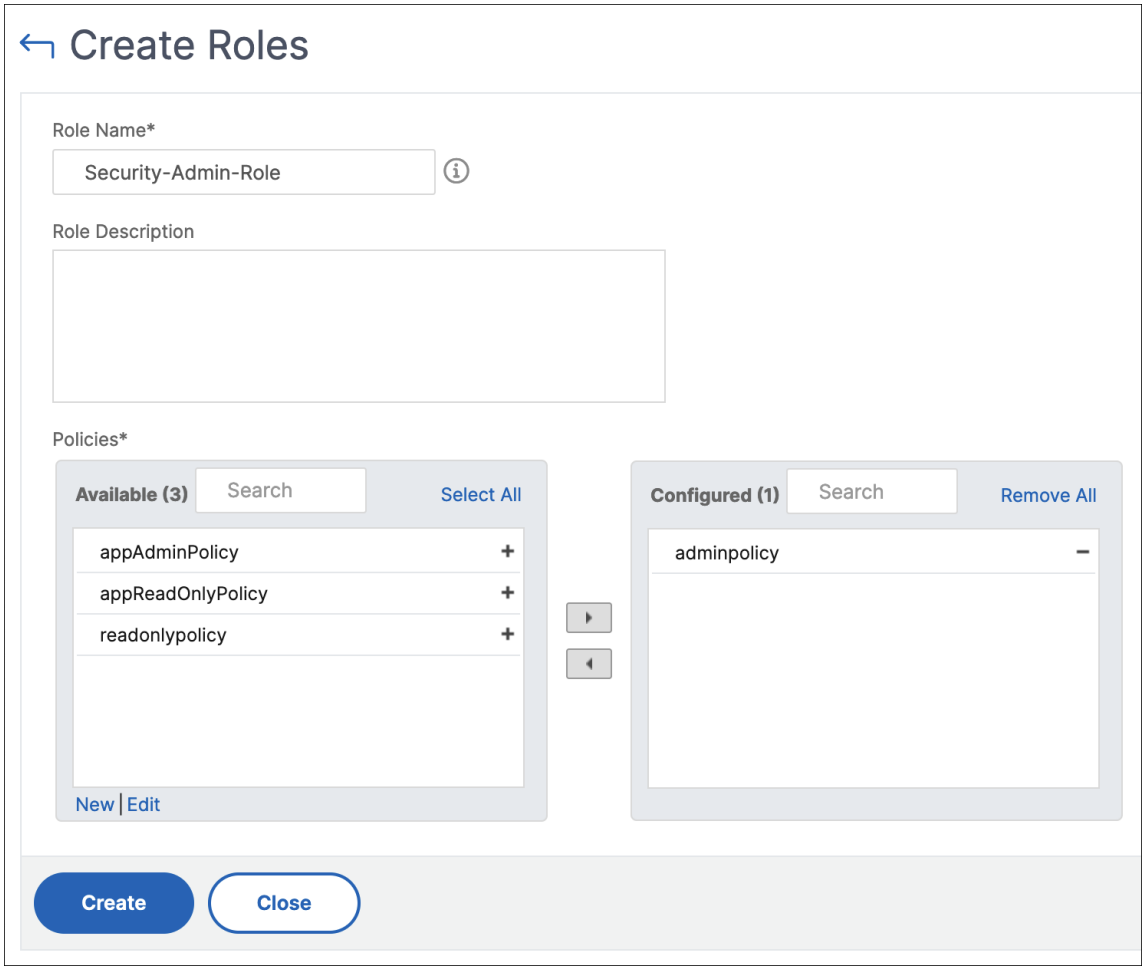
- **admin_role**. Tiene acceso a todas las funciones de NetScaler Console. (Esta función está vinculada a`adminpolicy`.)
- **adminExceptSystem_role**. Tiene acceso a la GUI de NetScaler Console, excepto a los permisos de configuración. (Este rol está vinculado a adminExceptSystem_Policy)
- **readonly_role**. Tiene acceso de solo lectura. (Esta función está vinculada a`readonlypolicy` .)
- **appAdmin_role**. Tiene acceso administrativo solo a las funciones de la aplicación en NetScaler Console. (Este rol está vinculado a appAdminPolicy).
- **appReadonly_role**. Tiene acceso de solo lectura a las funciones de la aplicación. (Este rol está vinculado a appReadOnlyPolicy).

Aunque no puede modificar las funciones predefinidas, puede crear las suyas propias (definidas por el usuario).

Para crear roles y asignarles directivas:

1. En la GUI de NetScaler Console, vaya a **Configuración** > **Usuarios y funciones** > **Funciones** .
2. Haga clic en **Agregar**.
3. En la página **Crear funciones**, en el campo **Nombre de función**, introduzca el nombre de la función y proporcione la descripción en el campo **Descripción de la función** (opcional).
4. En la sección **Directivas**, agregue y mueva una o más directivas a la lista de **configuraciones**.

   > **Nota:**
   >
   > Las directivas llevan como prefijo un identificador de arrendatario (por ejemplo, `maasdocfour`) que es único para todos los arrendatarios.



> **Nota:**
>
> Puede crear una política de acceso haciendo clic en **Nueva** o puede ir a **Configuración** > **Usuarios y funciones** > **Políticas de acceso** y crear políticas.

5. Haga clic en **Crear**.

Configurar grupos en la consola de NetScaler

En NetScaler Console, un grupo puede tener acceso tanto a nivel de funciones 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 Console.

Puede administrar el acceso de un usuario en NetScaler Console en el nivel individual de las entidades de funciones de red. Puede asignar dinámicamente permisos específicos al usuario o al grupo a nivel

de entidad.

NetScaler Console trata los servidores, los servicios, los grupos de servicios y los servidores virtuales como entidades de funciones de red.

- **Servidor virtual (Aplicaciones)**: Equilibrio de carga (`lb`), GSLB, conmutación de contexto (`CS`), redirección de caché (`CR`), autenticación (`Auth`) y NetScaler Gateway (`vpn`)
- **Servicios**: Equilibrio de carga y servicios GSLB
- **Grupo de servicios**: Equilibrio de carga y grupos de servicios GSLB
- **Servidores: servidores** de equilibrio de carga

Para crear un grupo:

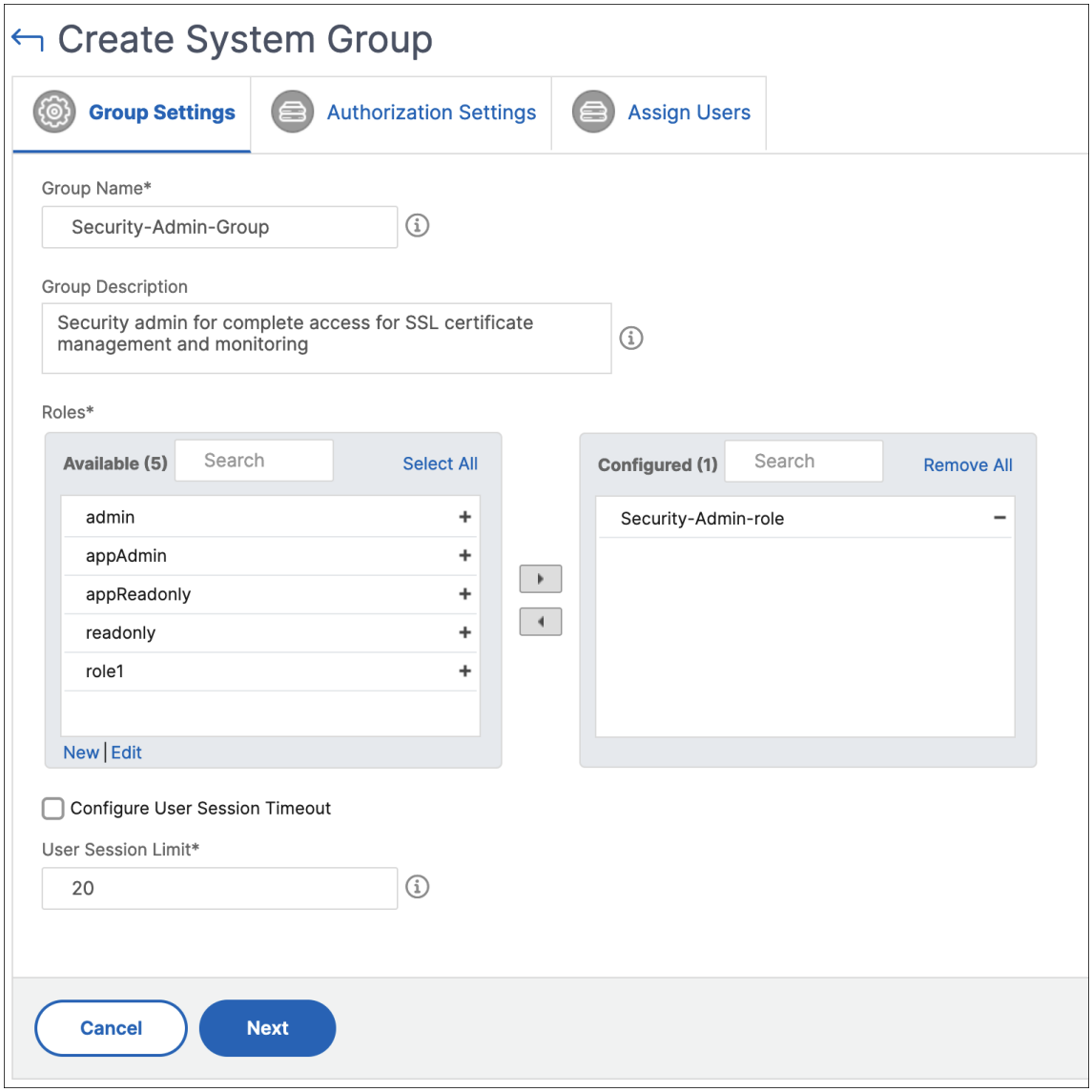
1. En NetScaler Console, vaya a **Configuración** > **Usuarios y funciones** > **Grupos** .
2. Haga clic en **Agregar**.

   Aparece la página **Crear grupo de sistemas**.
3. En el campo **Nombre de grupo**, escriba el nombre del grupo.
4. En el campo **Descripción del grupo**, escribe una descripción de tu grupo. Proporcionar una buena descripción le ayuda a entender el rol y la función del grupo.
5. En la sección **Funciones**, mueva una o más funciones a la lista de funciones **configuradas**.

   > **Nota:**
   >
   > Los roles llevan como prefijo un identificador de arrendatario (por ejemplo, `maasdocfour`) que es único para todos los arrendatarios.

6. En la lista **Disponible**, puede hacer clic en **Nuevo** o **Modificar** y crear o modificar funciones.

   Como alternativa, puede ir a **Configuración > Usuarios y roles > Usuarios**y crear o modificar usuarios.



7. Haga clic en **Siguiente**.
8. En la ficha **Configuración de autorización**, puede elegir recursos de las siguientes categorías:

   - **Grupos de Autoscale**
   - **Instancias**
   - **Aplicaciones**
   - **Plantillas de configuración**
   - **Proveedores y redes de IPAM**
   - **StyleBooks**
   - **Paquetes de configuración**
   - **Nombres de dominio**

   Seleccione recursos específicos de las categorías a las que los usuarios pueden tener acceso.

Grupos de Autoscale:

Para seleccionar los grupos de Autoscale específicos que un usuario puede ver o administrar:

a) Desactive la casilla de verificación **Todos los grupos de AutoScale** y haga clic en **Agregar grupos de AutoScale**.

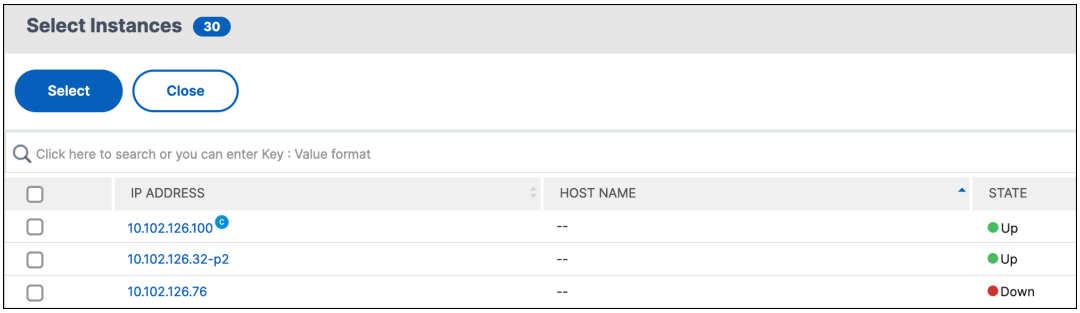
b) Seleccione los grupos de Autoscale necesarios de la lista y haga clic en **Aceptar**.

Instancias:

Para seleccionar las instancias específicas que un usuario puede ver o administrar:

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**.

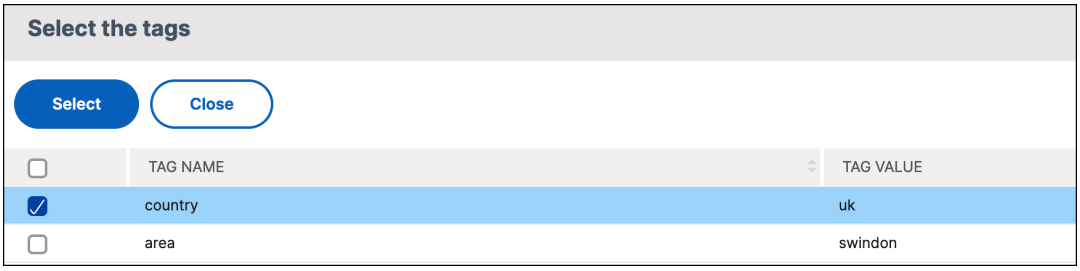


Etiquetas:

Para autorizar a los usuarios a ver o gestionar instancias específicas en función de las etiquetas asociadas:

a) Desactive la casilla de verificación **Todas las instancias** y haga clic en **Seleccionar etiquetas**.

b) Seleccione las etiquetas necesarias de la lista y haga clic en **Aceptar**.



Más adelante, a medida que asocies más instancias a las etiquetas seleccionadas, los usuarios autorizados accederán automáticamente a las nuevas instancias.

Para obtener más información sobre las etiquetas y la asociación de etiquetas a las instancias, consulta Cómo crear etiquetas y asignarlas a instancias.

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. Porque las aplicaciones son independientes de sus instancias para conceder el acceso a los usuarios.

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.

Esta lista le ofrece las siguientes opciones:

- **Todas las aplicaciones:** Esta opción está seleccionada por defecto. Agrega todas las aplicaciones que están presentes en la consola de NetScaler.
- **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.
- **Seleccionar Tipo de Entidad Individual:** Esta opción le permite seleccionar el 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 a las entidades enlazadas también** autoriza las entidades que están enlazadas al tipo de entidad seleccionado. Por ejemplo, si selecciona una aplicación y selecciona **Aplicar también a las entidades enlazadas** , NetScaler Console autoriza todas las entidades que están enlazadas a la aplicación seleccionada.

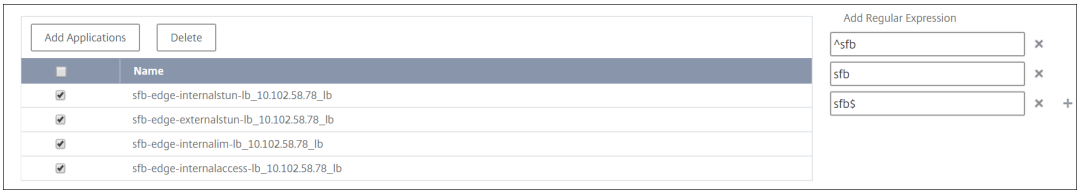
  > **Nota:**
  >
  > Asegúrese de haber seleccionado solo un tipo de entidad si quiere autorizar entidades enlazadas.

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 regular especificada se conserva en NetScaler Console. Para agregar una expresión regular, lleve a cabo los siguientes pasos:

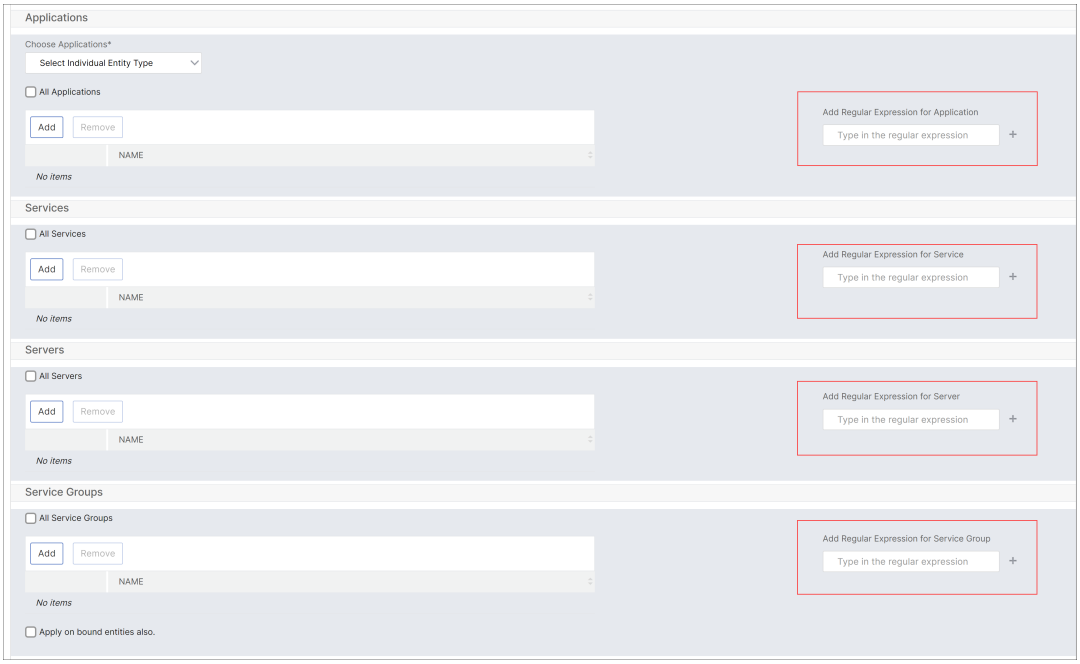
a) Haga clic en **Agregar expresión regular**.

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 una expresión regular para agregar entidades de funciones de red cuando se elige 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.

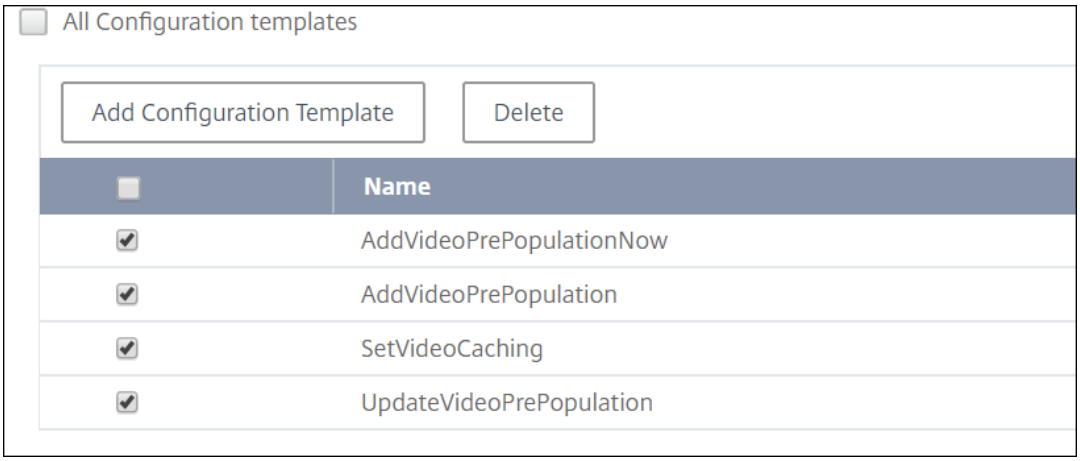
La expresión regular se almacena en el sistema para actualizar el alcance de la autorización. Cuando las nuevas entidades coinciden con la expresión regular de su tipo de entidad, NetScaler Console actualiza el alcance de autorización de las nuevas entidades.

Plantillas de configuración:

Si desea seleccionar la plantilla de configuración específica que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Borre **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**.



Proveedores y redes de IPAM:

Si quiere agregar los proveedores y redes de IPAM específicos que un usuario puede ver o administrar, realice lo siguiente:

- **Agregar proveedores**: Borra **todos los proveedores** y haz clic en **Agregar proveedores**. Puede seleccionar los proveedores necesarios y hacer clic en **Aceptar**.
- **Agregar redes**: Borre **todas las redes** y haga clic en **Agregar redes**. Puede seleccionar las redes necesarias y hacer clic en **Aceptar**.

StyleBooks:

Si desea seleccionar el StyleBook específico que un usuario puede ver o administrar, siga estos 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 de 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
```

Esta consulta enumera los StyleBooks que cumplen las condiciones siguientes:

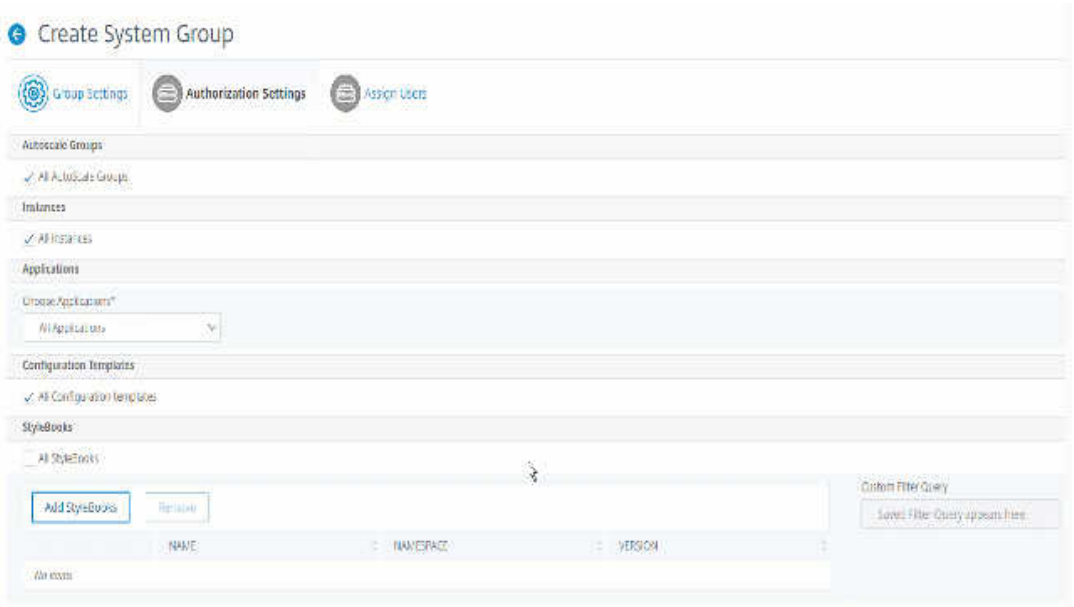
- El nombre de StyleBook es `lb-mon` o `lb`.
- El espacio de nombres StyleBook es `com.citrix.adc.stylebooks`.
- La versión de StyleBook es `1.0`.

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**. Según la consulta guardada, la consola de NetScaler proporciona a los usuarios acceso 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, seleccione una de las siguientes opciones:

- **Todas las configuraciones**: Esta opción está seleccionada de forma predeterminada. Permite a los usuarios administrar todas las configuraciones 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 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:

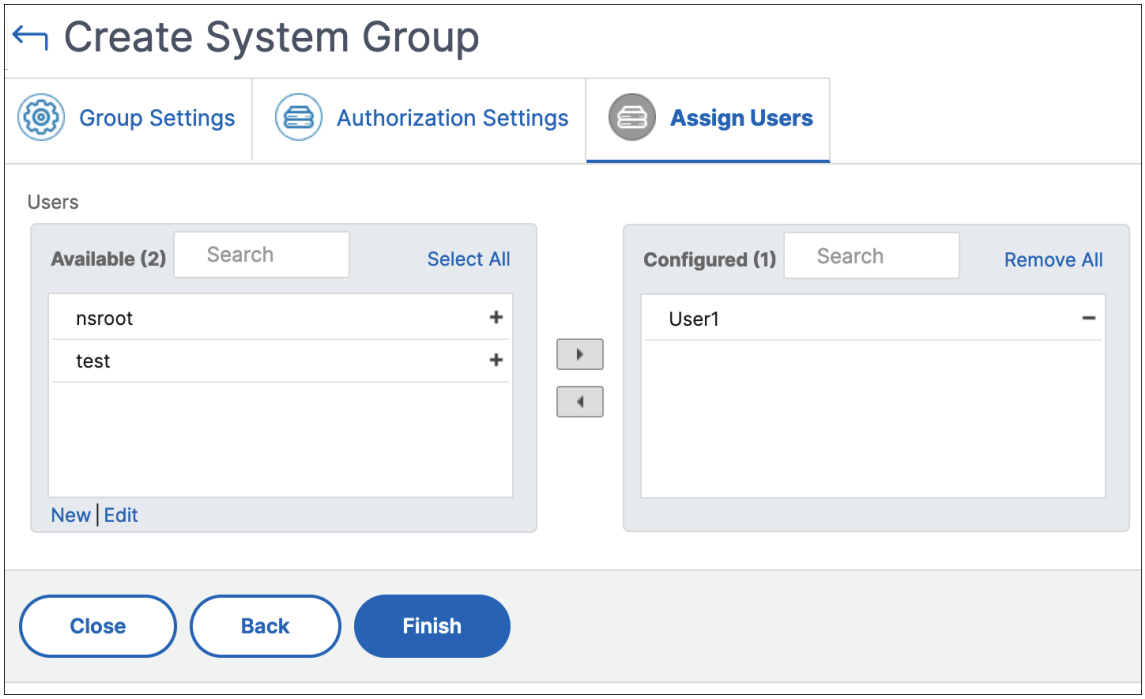
a) Desactive la casilla **Todos los nombres de dominio** y haga clic en **Agregar nombre de dominio**.

b) Seleccione los nombres de dominio necesarios de la lista y haga clic en **Aceptar**.

c) Haga clic en **Crear grupo**.

d) En la sección **Asignar usuarios**, seleccione el usuario en la lista **Disponible** y agréguelo a la lista **Configurada**.

> **Nota:**
>
> También puede agregar nuevos usuarios haciendo clic en **Nuevo**.



a) Haga clic en **Finalizar**.

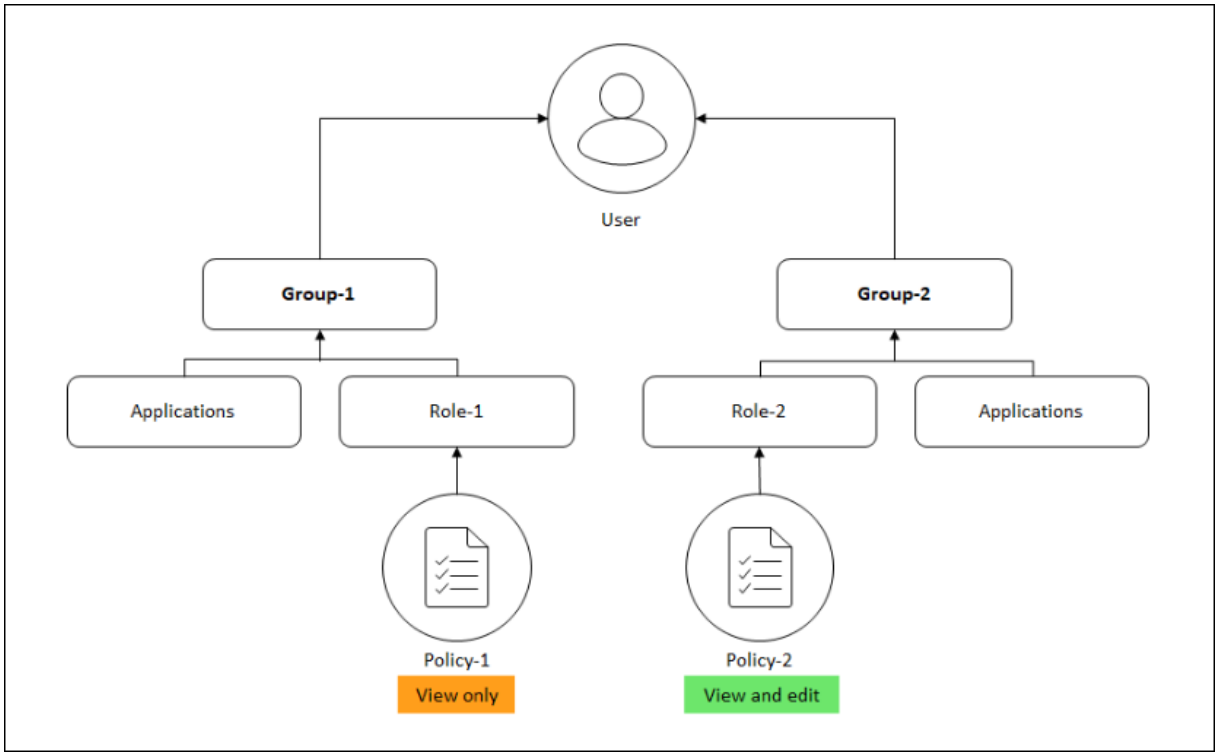
Cómo cambia el acceso de usuario en función del ámbito de autorización

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, la consola de NetScaler otorga al usuario acceso a las aplicaciones en función del 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.

Limitaciones

Las siguientes funciones de NetScaler Console no son totalmente compatibles con el RBAC:

- **Análisis**: L os módulos de análisis no son totalmente compatibles con RBAC. La compatibilidad con RBAC se limita a un nivel de instancia y no se aplica a nivel de aplicación en los módulos de análisis de Gateway Insight, HDX Insight y Security Insight.
  - Ejemplo 1: RBAC basado en instancias (compatible). Un administrador al que se le hayan asignado algunas instancias solo puede ver esas instancias en **HDX Insight** > **Dispositivos**y solo los servidores virtuales correspondientes en **HDX Insight** > **Aplicaciones**, ya que el RBAC se admite 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 **HDX Insight** > **Aplicaciones**, pero no puede acceder a ellos, ya que el RBAC no es compatible a nivel de aplicaciones.
- **StyleBooks**: RBAC no es totalmente compatible con StyleBooks.

- Imagine una situación en la que muchos usuarios tienen acceso a un único StyleBook, pero tienen permisos de acceso para diferentes instancias de NetScaler. Los usuarios pueden crear y actualizar paquetes de configuración en sus propias instancias, ya que no tienen acceso a otras instancias que no sean las suyas. Pero todavía pueden ver los paquetes de configuración y los objetos creados en instancias de NetScaler que no sean las suyas.

Asignar un perfil de red para la instancia de NetScaler gestionada

July 17, 2024

Al habilitar el recopilador de métricas o análisis para los servidores virtuales en NetScaler Console, los datos de AppFlow o métricas del NetScaler se exportan a NetScaler Console a través de la dirección IP de subred (SNIP) de NetScaler. 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. 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 a través de NetScaler Console para exportar los datos de AppFlow de NetScaler a NetScaler Console.

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 Console:

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 AppFlow.
   - Haga clic en **Configurar perfiles de red para el recopilador de métricas** para asignar un perfil de red al recopilador de métricas.
3. Seleccione un perfil de red de la lista y haga clic en **Aplicar**.

> **Nota:**
>
> - Para AppFlow, asegúrese de inhabilitar los análisis de todos los servidores virtuales antes de asignar un perfil de red a la instancia.
> - Para Metrics Collector, asegúrese de inhabilitar las métricas de todos los servidores virtuales antes de asignar un perfil de red a la instancia.

Gestión del almacenamiento de datos

January 26, 2024

Es importante saber qué funciones se utilizan en NetScaler Console y el uso de datos de cada una de estas funciones. El panel de **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 de la consola 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**:

- Vea 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 Console durante los últimos 30 días. Estas tendencias están disponibles en forma gráfica o tabular. Estas tendencias muestran la cantidad de datos ingresados y la cantidad de datos almacenados después de los ciclos de eliminación programados en NetScaler Console.
- 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:

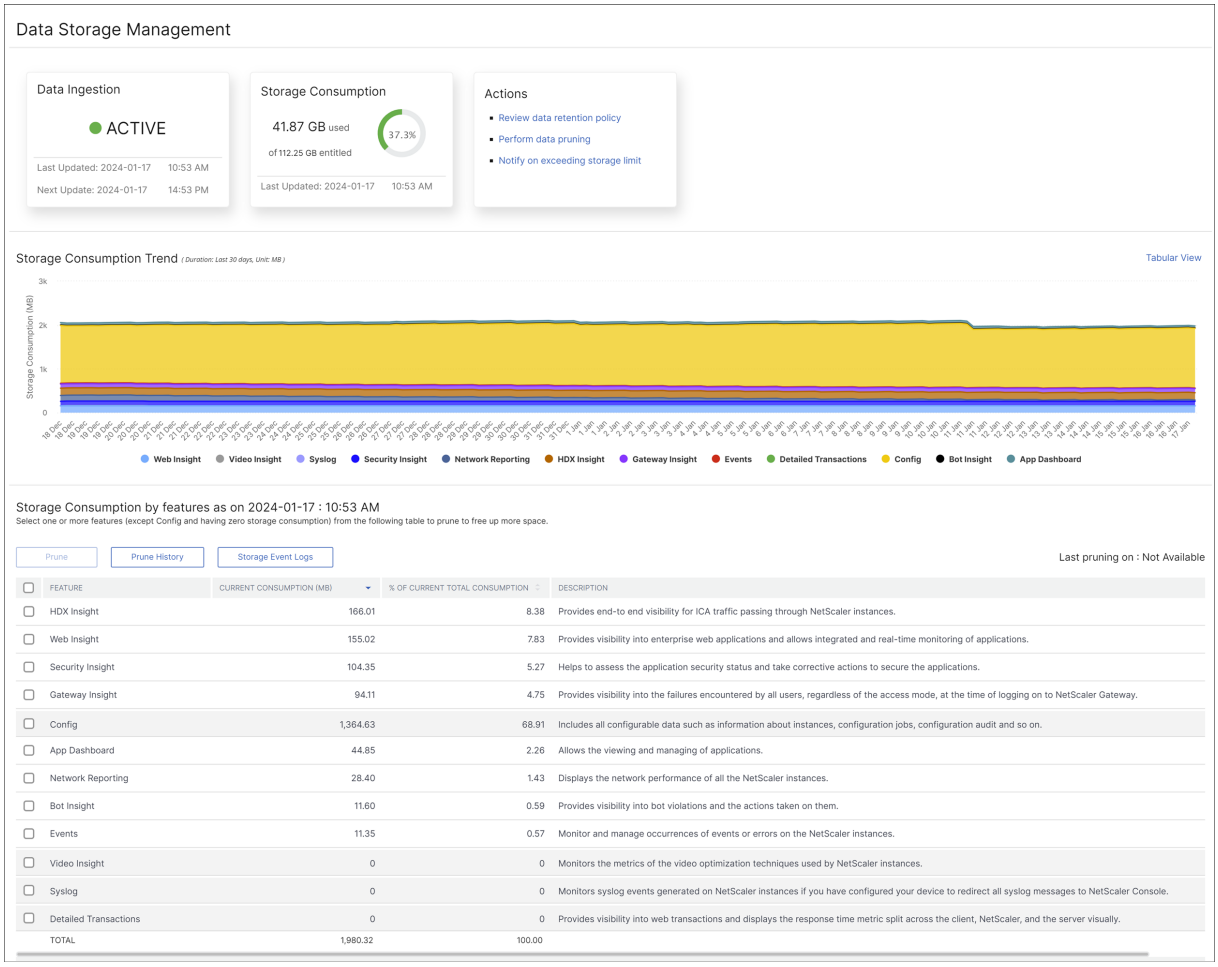
- Comprender su almacenamiento de datos: Esta sección le ayuda a entender cómo puede usar el panel para ver información sobre su almacenamiento de datos.
- Administrar el almacenamiento de datos: En esta sección se proporciona información sobre las acciones que puede realizar en el panel de control para administrar el almacenamiento de datos.

Comprenda su almacenamiento de datos

May 9, 2024

Puede usar el panel de **administración del almacenamiento de datos** de NetScaler Console para ver los datos y los 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
- Estado de depuración de datos
- Tendencias de consumo de almacenamiento
- Consumo de almacenamiento por funciones

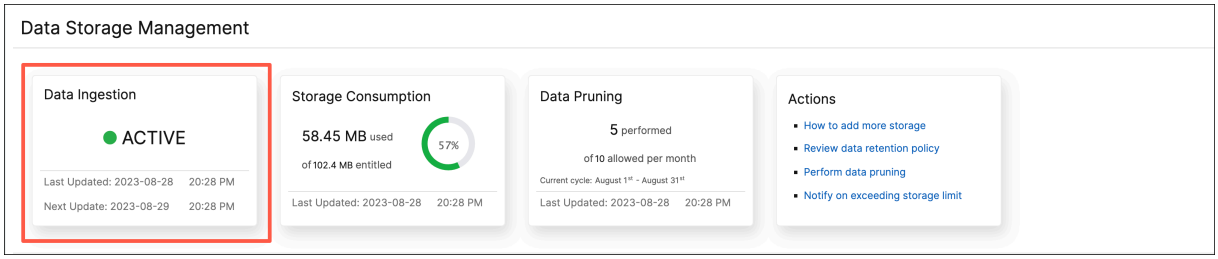
Estado de su actividad de ingestión de datos

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 de NetScaler Console.

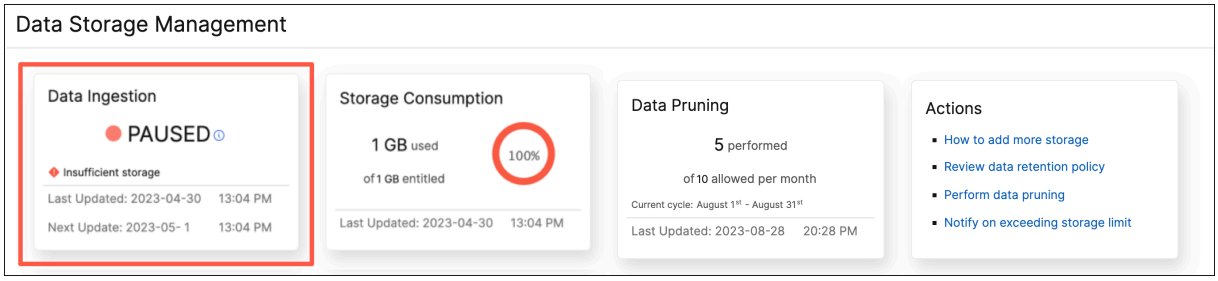
El estado de ingesta de datos indica si NetScaler Console recopila estadísticas de las instancias de NetScaler. La actividad de ingesta de datos continúa mientras el almacenamiento consumido esté dentro del almacenamiento autorizado. Cuando el consumo es mayor al almacenamiento autorizado, la ingesta 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.



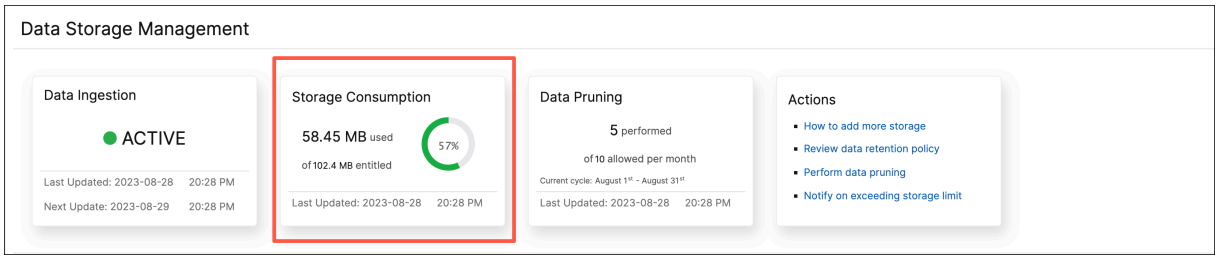
Cómo reanudar la ingesta de datos pausada

Para reanudar la actividad de ingesta de datos, puede realizar una de las siguientes acciones:

- Agregue más almacenamiento de datos.
- Realice una 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.

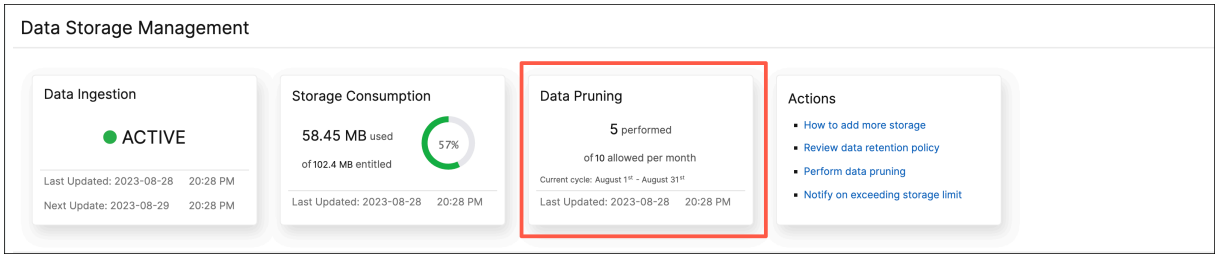
Almacenamiento consumido

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.

Estado de depuración de datos

La depuración es el proceso de eliminar datos manualmente y liberar espacio de almacenamiento. Se le permiten 10 podas de datos en cada mes natural. Por ejemplo, puede eliminar sus datos 10 veces entre el 1 y el 31 de julio.



Para saber cuántas podas de datos ha usado y cuántas le quedan, consulte el mosaico de **Poda de datos**.

> **Nota:**
>
> Cada actividad de poda se cuenta como una poda de datos, independientemente del número de funciones seleccionadas.

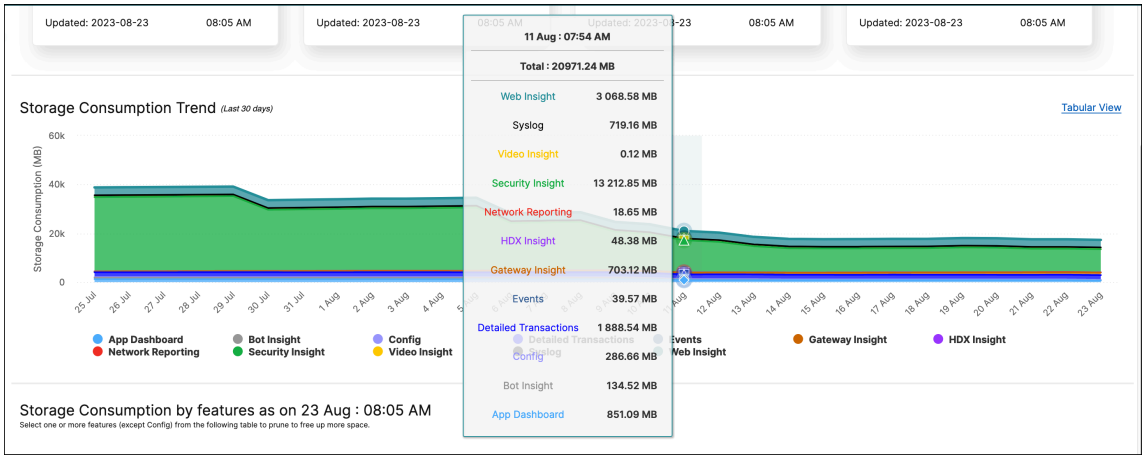
Tendencias de consumo de almacenamiento

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 entre las diferentes funciones de NetScaler Console. 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.

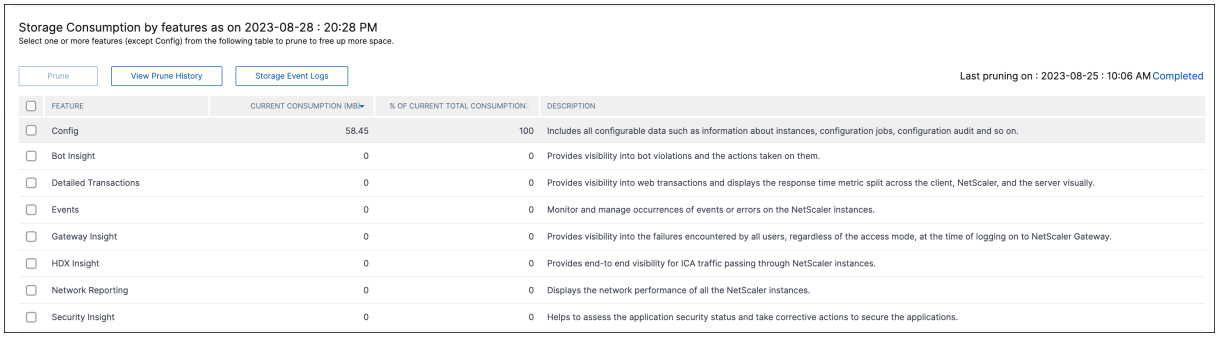
FUNCIÓN	DESCRIPCIÓN
Eventos	Supervise y administre la aparición de eventos o errores en las instancias de NetScaler.
Panel de aplicaciones	Permite la visualización y administración de aplicaciones.
Insight del bot	Proporciona visibilidad sobre las infracciones de los bots y las acciones que se han tomado al respecto.
Syslog	Supervisa los eventos de syslog generados en las instancias de NetScaler si ha configurado el dispositivo para redirigir todos los mensajes de syslog a NetScaler Console.
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 las diferentes funciones de NetScaler Console
- 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 Console ordena

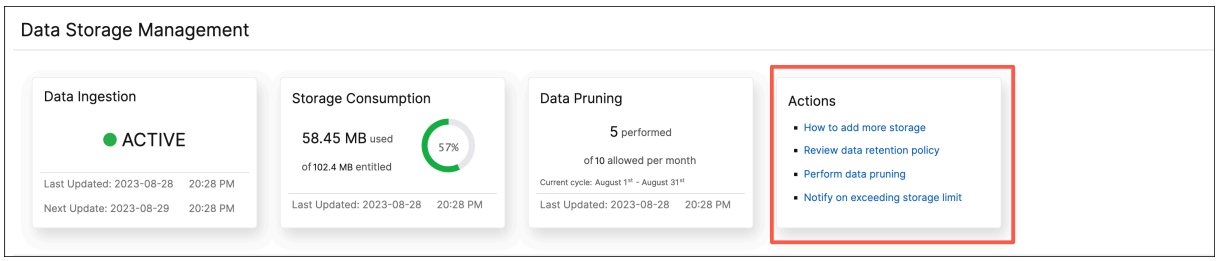
alfanuméricamente la tabla de arriba a abajo en función de los datos de la columna elegida. Para ordenar la tabla en orden inverso, vuelva a hacer clic en el encabezado de la columna.

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.

Administrar el espacio de almacenamiento

July 17, 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

Cuando el almacenamiento consumido alcanza el 100% del almacenamiento con licencia, la actividad de ingesta de datos se detiene y los datos dejan de almacenarse en NetScaler Console.

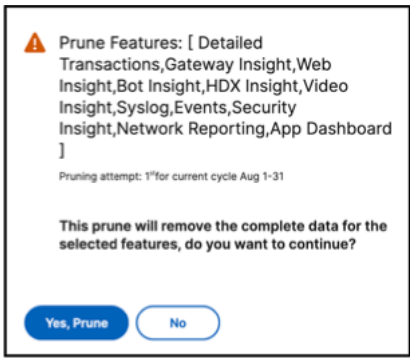
Realizar una depuración de datos

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 los recursos se utilicen con prudencia y que NetScaler Console sea ágil y responsiva.

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.

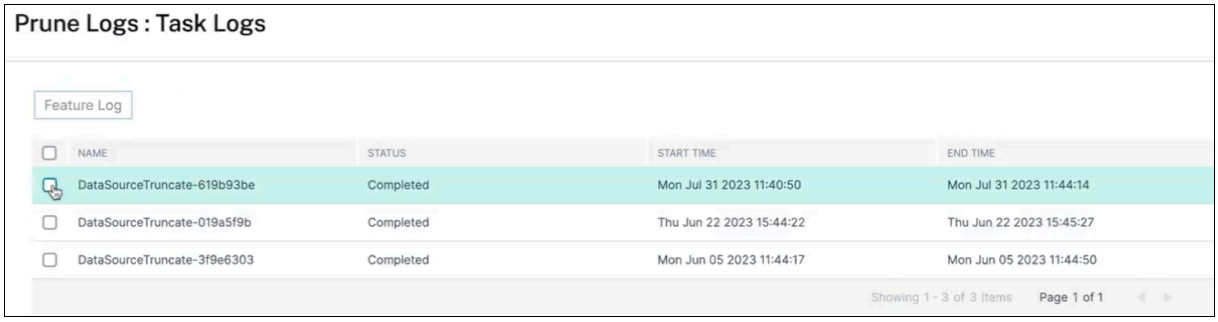
   Una ventana emergente le pide que confirme si quiere eliminar todos los datos de las funciones seleccionadas. Haga clic en **Sí, podar**.



> **Nota:**
>
> La ventana emergente también muestra información sobre su intento de poda actual.

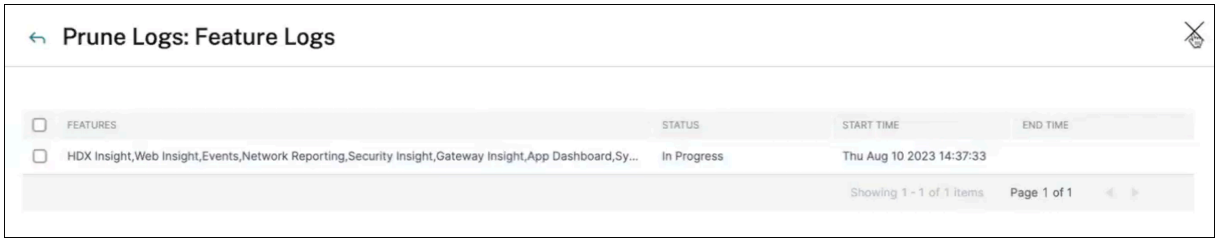
Ver el historial de podas

Haga clic en **Ver historial de poda** para obtener detalles sobre todas las actividades de poda que realizó en NetScaler Console.



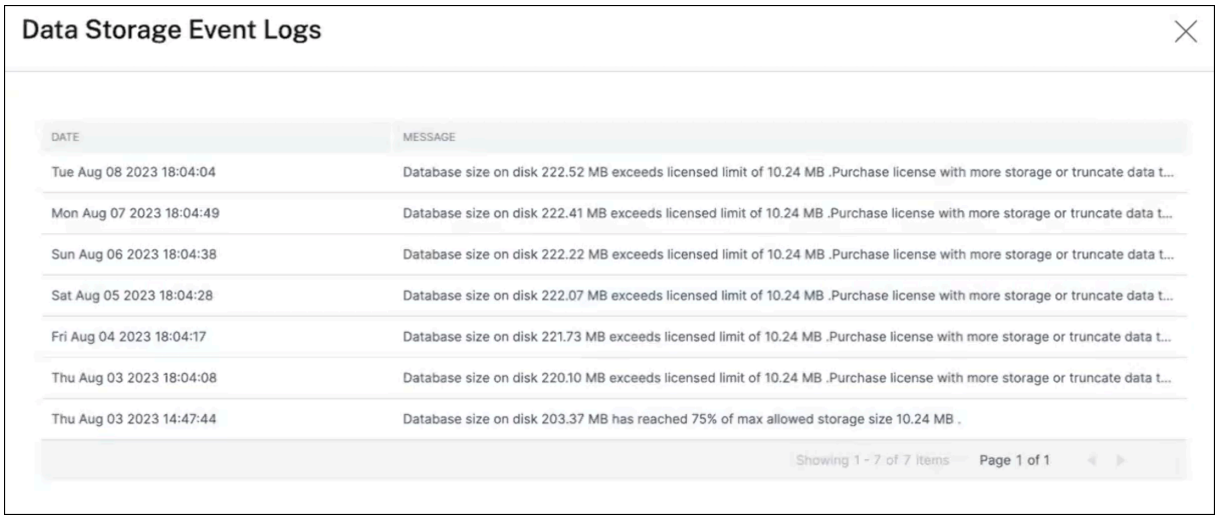
La página **Registros de poda: registros de tareas** muestra la lista de todas las tareas de eliminación, incluidos sus respectivos estados, hora de inicio y hora de finalización.

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 política de retención de datos hace referencia a un conjunto de reglas y configuraciones que determinan cómo NetScaler Console 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 desea reducir el espacio de almacenamiento que utilizan las distintas funciones, puede cambiar el tiempo que se guardan los datos en NetScaler Console.

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 Console le envíen 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.

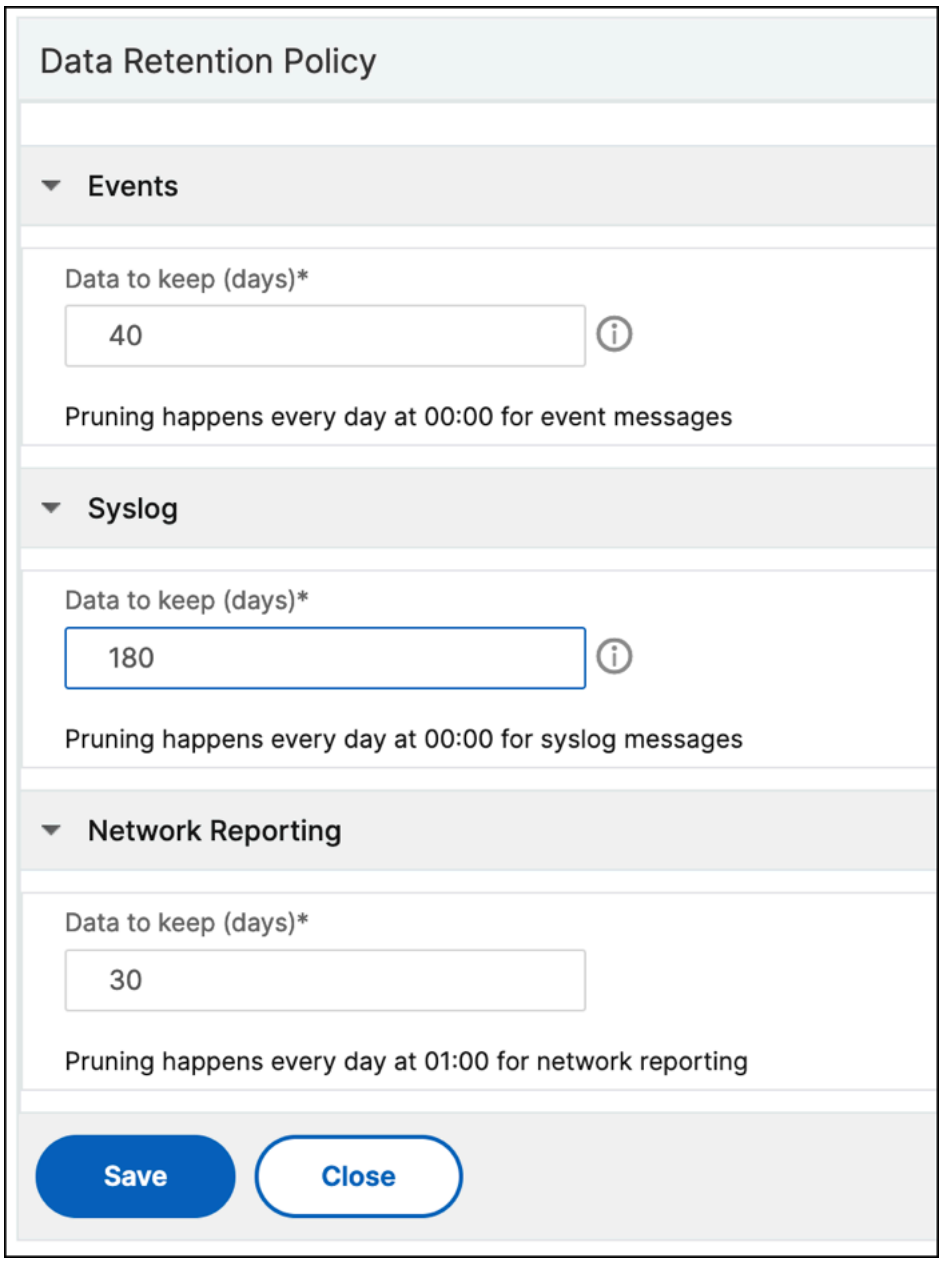
Directiva de retención de datos

January 26, 2024

Puede acceder a los eventos del sistema, los mensajes de syslog y los datos de informes de red durante un período específico en NetScaler Console.

1. Vaya a **Configuración > Administración del almacenamiento de datos > Directiva de retención de datos** para configurar la retención de datos.
2. Haga clic en el botón de edición.
3. Introduzca el número de días que desea que se conserven los datos en NetScaler Console para cada una de las siguientes opciones:

Opciones	Descripción
Eventos	Le permite limitar los mensajes de eventos almacenados en NetScaler Console a un máximo de 40 días. Los eventos se eliminan de NetScaler Console una vez caducada la política de retención. Los eventos borrados se eliminan después de un día.
Syslog	Le permite limitar la cantidad de datos de syslog almacenados en la base de datos hasta 180 días.
Informes de red	Le permite limitar los datos de informes de red almacenados en NetScaler Console a un máximo de 30 días.



Importante:

No puede modificar la directiva de retención de datos con una cuenta Express.

Cuando su cuenta se convierte en una cuenta Express, la consola de NetScaler conserva los datos de almacenamiento de hasta 500 MB o los datos de un día, lo que sea menor. Para obtener más información, consulte Administrar los recursos de NetScaler Console mediante una cuenta Express.

Configurar y ver alarmas del sistema

May 9, 2024

Puede activar y configurar un conjunto de alarmas para supervisar el estado de los servidores de NetScaler Console. 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.

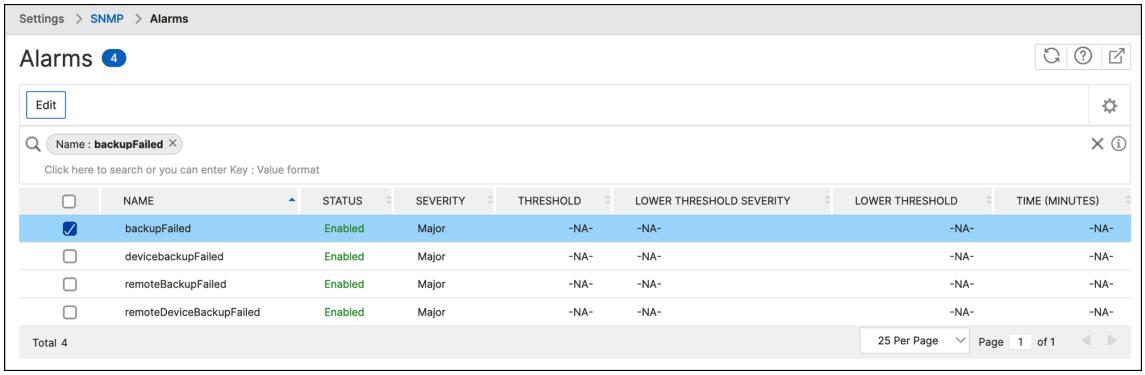
Configurar una alarma

Considere un caso en el que quiere supervisar un intento fallido de copia de seguridad. Puede habilitar la alarma BackupFailed y asignarle una gravedad, como Major, a ella. Cada vez que NetScaler Console intenta hacer una copia de seguridad de los archivos del sistema y el intento falla, se activa una alarma. Puede ver el mensaje en la página de mensajes de registro de NetScaler Console o recibir notificaciones por correo electrónico o SMS.

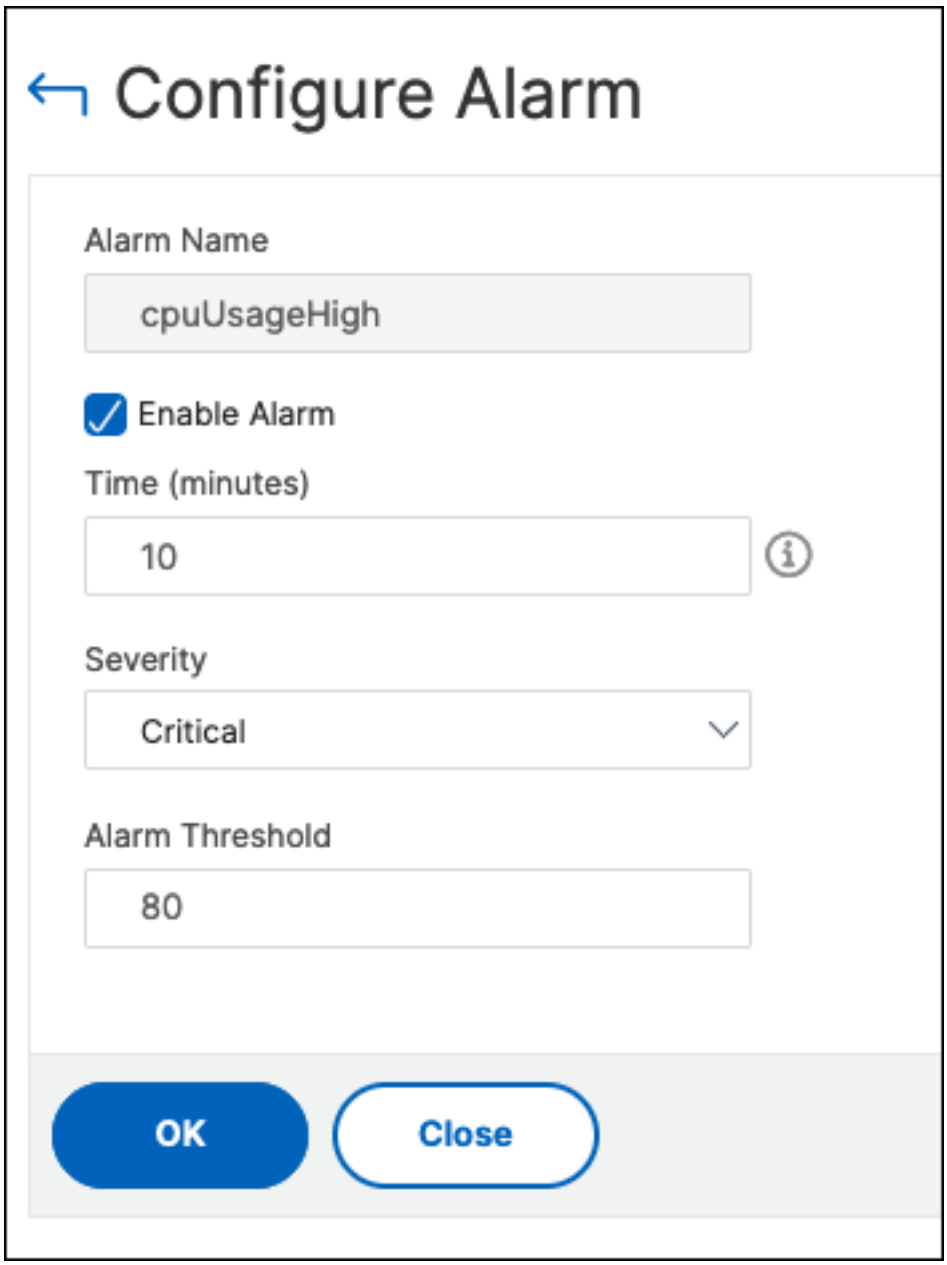
Para configurar la alarma, debe seleccionar la alarma BackupFailed y especificar el nivel de gravedad como Principal. La alarma está activada de forma predeterminada.

Para configurar y ver una alarma del sistema mediante NetScaler Console:

1. Vaya a **Parámetros > SNMP**. Haga clic en **Alarmas** en la esquina superior derecha.



2. Seleccione la alarma que quiere configurar (por ejemplo, cpuUsageHigh) y haga clic en **Modificar** para modificar sus parámetros.



3. En la página **Configurar alarma**, seleccione **Activar alarma** para crear alertas y, a continuación, especifique lo siguiente:

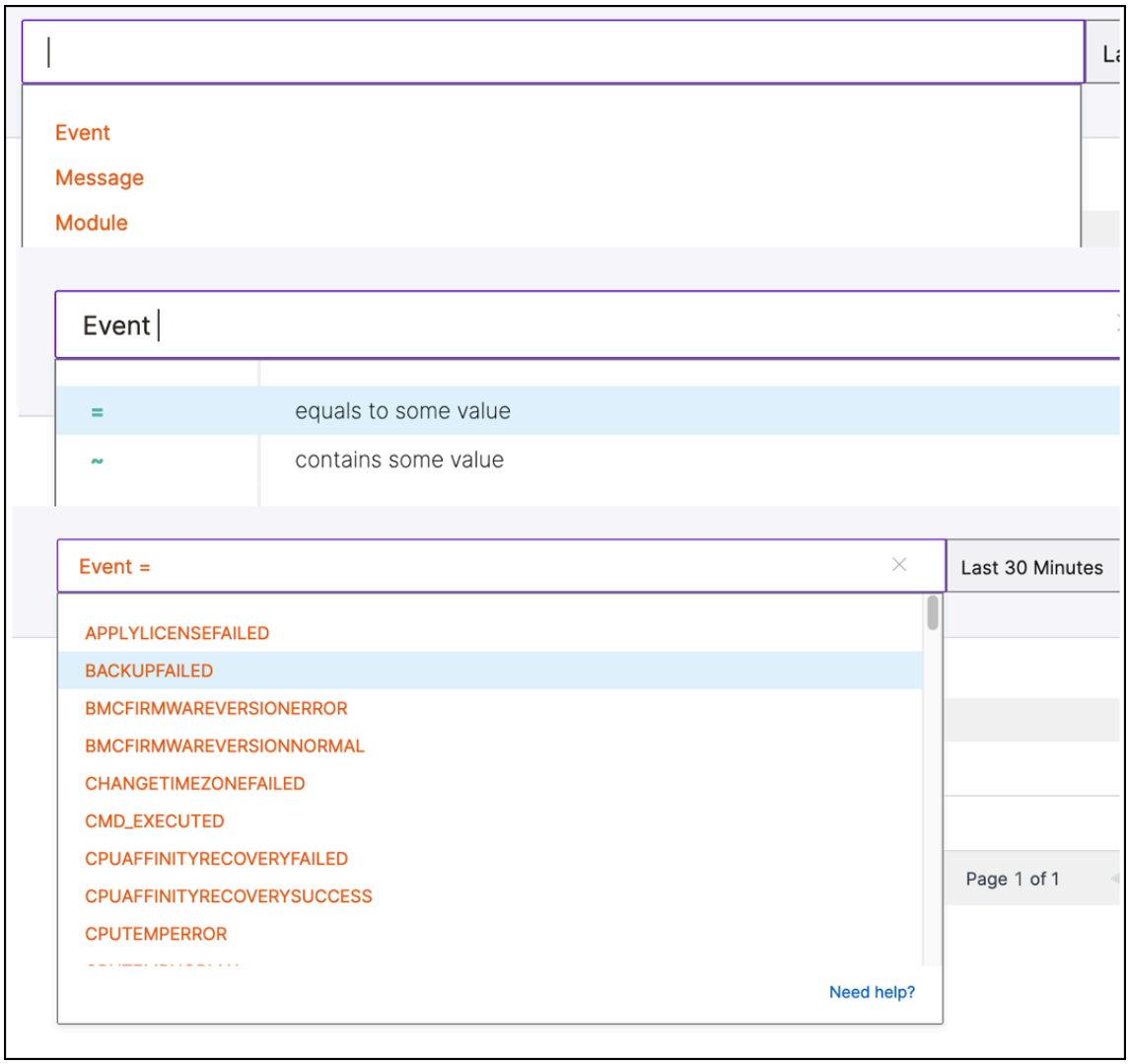
   - **Hora**. Escriba el tiempo (en minutos) tras el cual desea desencadenar la alarma.
   - **Gravedad**. Seleccione el nivel de gravedad.
   - **Umbral de alarma**. Introduzca el valor para el que debe desencadenarse la alarma y enviarse las alertas.

   Haga clic en **Aceptar**.

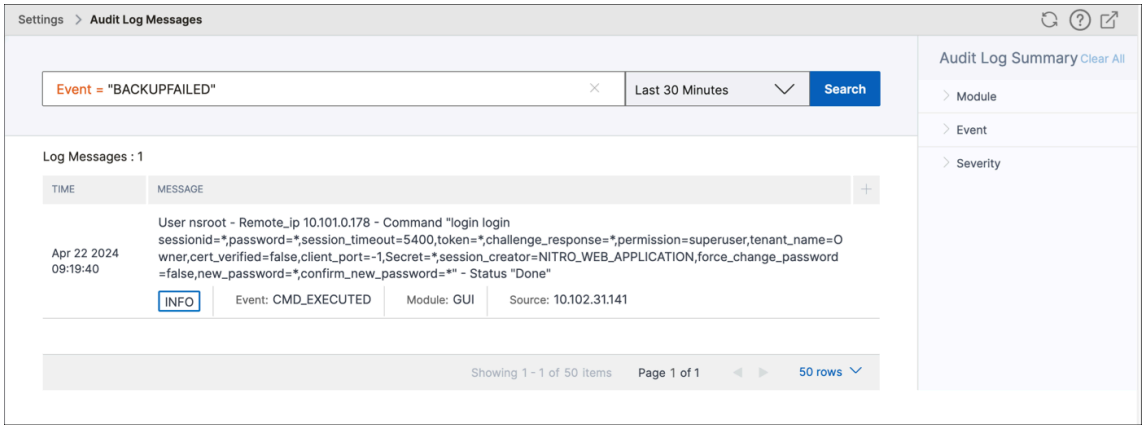
> **Nota:**
>
> No puede establecer el umbral para algunas alarmas, por ejemplo, backupFailed. Cuando se desencadena la alarma, puede ver el evento generado como un mensaje de syslog.

Para ver el evento generado por la alarma (por ejemplo, backupFailed):

1. Vaya a **Parámetros** > **Mensajes del registro de auditoría**.
2. En el campo de búsqueda, seleccione el tipo de alarma. En este ejemplo, seleccione **Event**, **=** (igual a algún valor) y, a continuación, **BACKUPHAILED**.



Se muestra el evento generado para una copia de seguridad fallida.



También puede configurar las notificaciones para recibir un correo electrónico o un mensaje de texto SMS (servicio de mensajes breves) cuando se active una alarma.

Agregar límites de umbral a las alarmas de utilización de disco

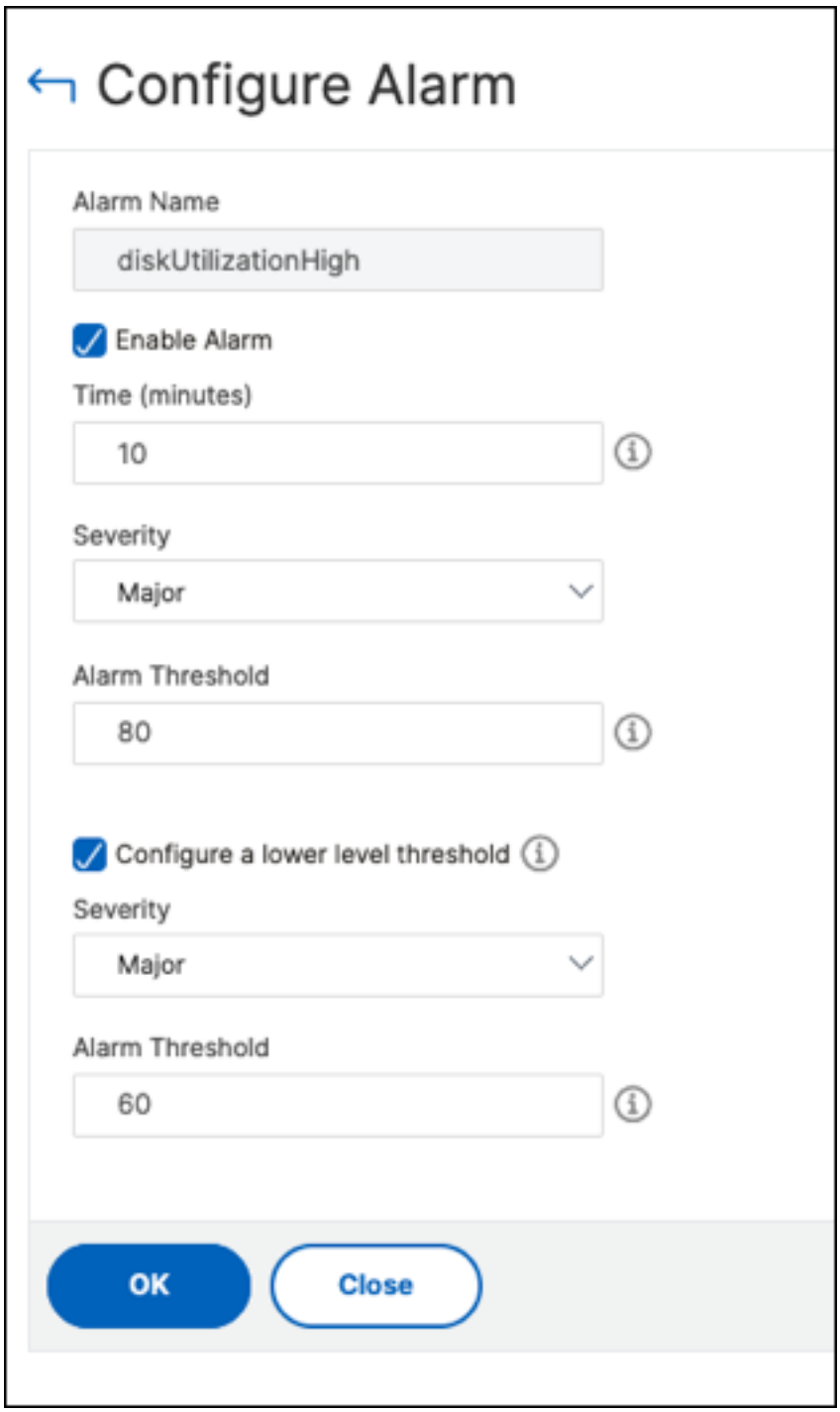
Las alarmas de utilización del disco se activan cuando la cantidad de espacio en disco utilizada en el servidor de NetScaler Console supera un umbral predefinido.

Como administrador, cuando recibe alertas, puede optar por eliminar los datos innecesarios o asignar recursos de almacenamiento adicionales para evitar interrupciones del servicio o la degradación del rendimiento.

A partir de la versión 14.1, compilación 25x, también puede agregar un umbral de nivel inferior para las alarmas de utilización del disco. Con este valor de umbral, puede establecer un límite de nivel inferior para recibir alertas antes de que se supere un límite de umbral superior.

Para configurar un umbral de nivel inferior:

1. Vaya a **Parámetros > SNMP > Alarmas** y, en el campo de búsqueda, escriba diskUtilizationHigh para ver las alarmas de utilización del disco.
2. Seleccione la alarma y haga clic en **Modificar**.
3. En la página **Configurar alarma**, seleccione **Configurar un umbral de nivel inferior**. Introduzca el límite de umbral inferior.



Por ejemplo, si establece un umbral inferior de utilización del disco de 60 y un umbral superior de 80, recibirá una alerta cuando el uso del disco supere el 60% de la capacidad del disco. Este parámetro le permite adoptar medidas correctivas antes de que la utilización del disco alcance el 80%.

Integración de observabilidad

July 17, 2024

Debido a la creciente complejidad de las aplicaciones modernas, los administradores se enfrentan a desafíos en lo siguiente:

- Aplicaciones de supervisión y solución de problemas.
- Obtener visibilidad del comportamiento de la infraestructura y las aplicaciones.

La observabilidad cierra esta brecha al proporcionar esta información sobre toda la infraestructura. Con la función de integración de observabilidad de NetScaler Console, puede:

- Integre NetScaler Console con Splunk.
- Integre NetScaler Console con New Relic.
- Integrar NetScaler Console con Microsoft Sentinel
- Configure las instancias de NetScaler para exportar información a Prometheus mediante el esquema predeterminado.

Integración con Splunk

July 17, 2024

Ahora puede integrar NetScaler Console con Splunk para ver los análisis de:

- Violaciones de WAF
- Infracciones de bots
- Información sobre certificados SSL
- Información sobre Gateway

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 Console 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 Console
- Configurar NetScaler Console para exportar datos a Splunk
- Ver paneles en Splunk

Configurar Splunk para recibir datos de NetScaler Console

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

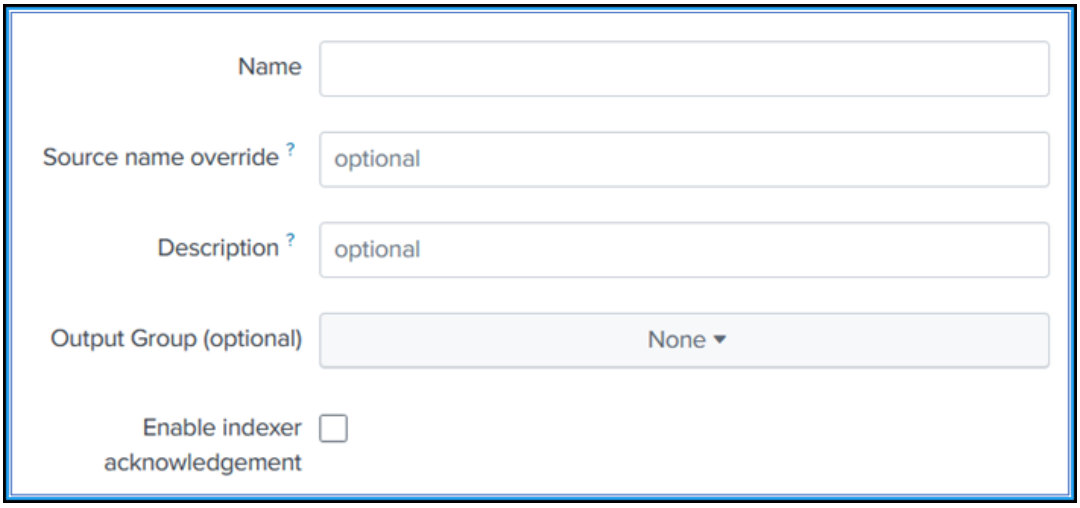
Configure el extremo del recopilador de eventos HTTP de Splunk y genere un token

Primero debes configurar el recopilador de eventos HTTP en Splunk. Esta configuración permite la integración entre la consola de NetScaler y Splunk para enviar los datos del WAF o del bot. A continuación, debes generar un token en Splunk para:

- Habilite la autenticación entre NetScaler Console y Splunk.
- Reciba datos a través del extremo del recopilador de eventos.

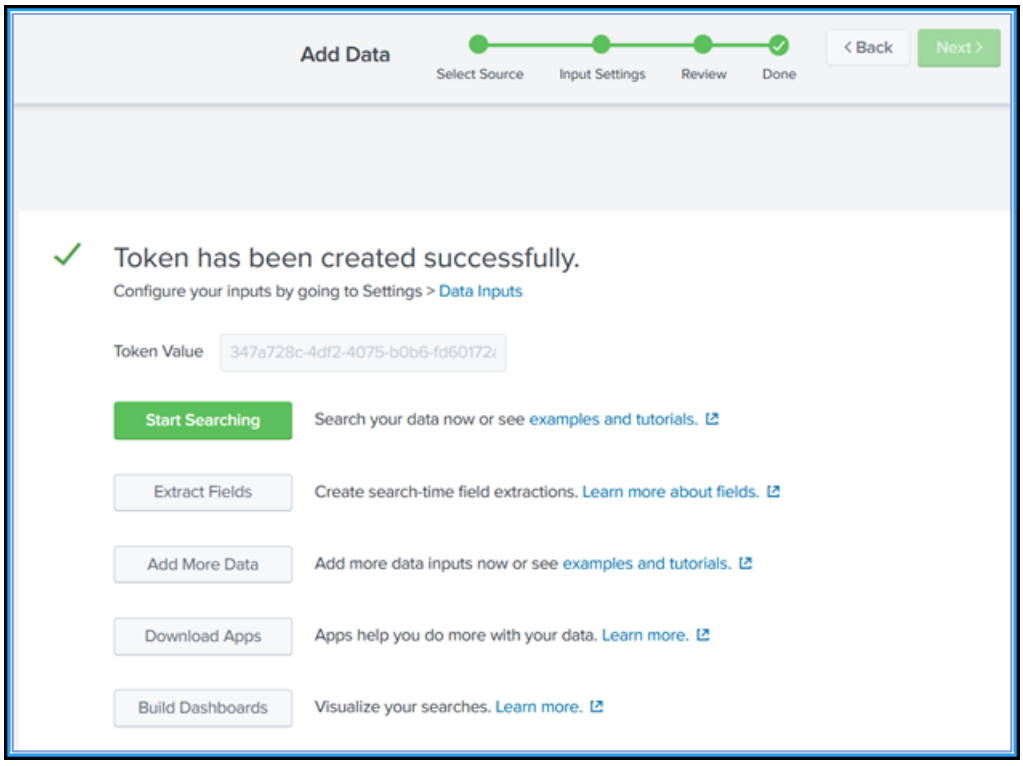
1. Inicie sesión en Splunk.
2. Vaya a **Configuración > Entradas de datos > Recopilador de eventos HTTP** y haga clic en **Agregar nuevo**.
3. Especifique los siguientes parámetros:
    a) **Nombre**: especifique un nombre de su elección.
    b) **Anulación del nombre de origen (opcional)**: si establece 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**: NetScaler Console no admite esta opción. Se recomienda no seleccionar esta opción.



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 añada detalles en NetScaler Console.

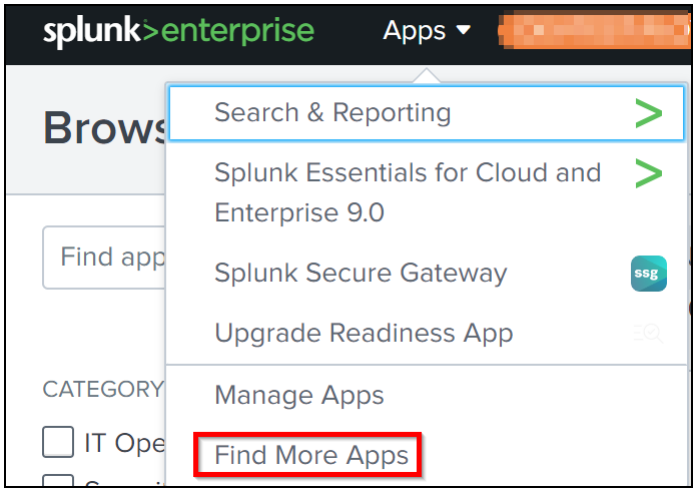


Instale el modelo de información común de Splunk

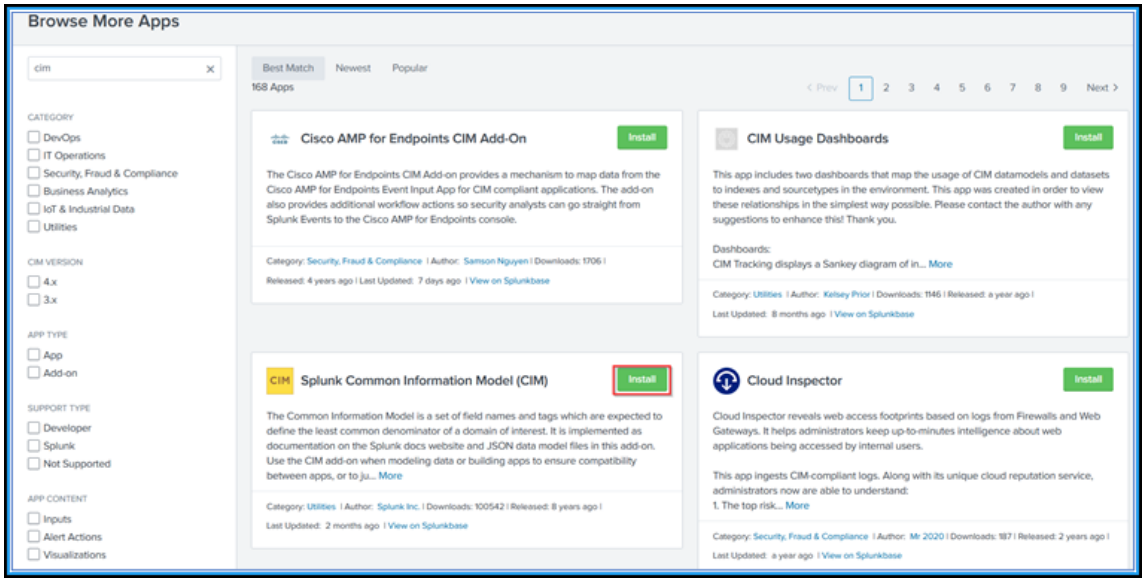
En Splunk, debes instalar el complemento CIM de Splunk. Este complemento garantiza que los datos recibidos de NetScaler Console normalicen los datos ingeridos y coincidan con un estándar común utilizando los mismos nombres de campo y etiquetas de eventos para eventos equivalentes.

> **Nota**
>
> Puede omitir este paso si ya ha instalado el complemento Splunk CIM.

1. Inicie sesión en Splunk.
2. Vaya a **Aplicaciones > Buscar más aplicaciones**.



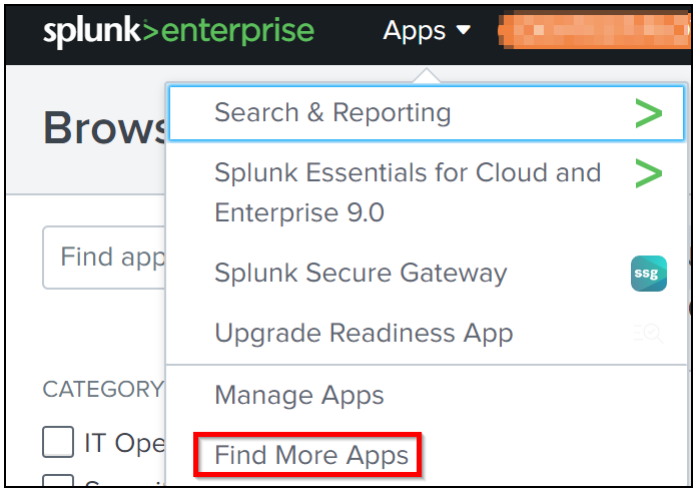
3. Escriba **CIM** en la barra de búsqueda y pulse **Entrar** para obtener el complemento del **modelo de información común (CIM) de Splunk** y haga clic en **Instalar**.



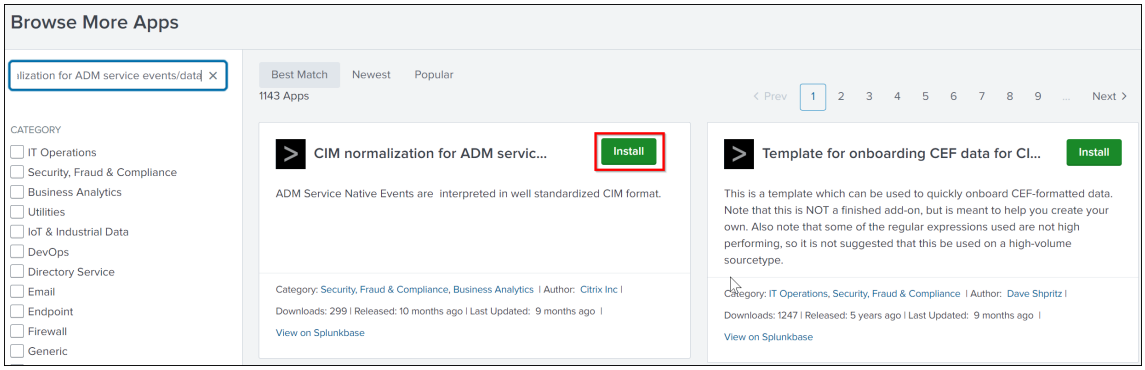
Instale el normalizador CIM

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

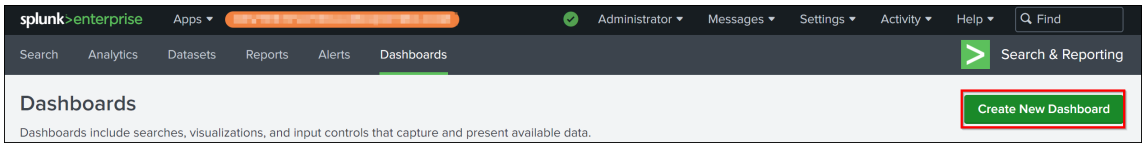
Tras instalar el CIM de Splunk, debe preparar un panel de ejemplo con una plantilla para WAF y Bot y SSL Certificate Insights. Puede descargar el archivo de plantilla del panel (`.tgz`), usar cualquier editor (por ejemplo, el bloc de notas) para copiar su contenido y crear un panel pegando los datos en Splunk.

> **Nota:**
>
> El siguiente procedimiento para crear un panel de ejemplo se aplica tanto a WAF como a Bot, y a SSL Certificate Insights. Debe utilizar el archivo `json` requerido.

1. Inicie sesión en la página de descargas de Citrix y descargue el panel de ejemplo disponible en Observability Integration.
2. Extraiga el archivo, abra el archivo `json` con cualquier editor y copie los datos del archivo.

   > **Nota:**
   >
   > Después de extraer, obtendrá dos archivos `json`. Use `adm_splunk_security_violations.json` para crear el panel de ejemplo de WAF y Bot, y use `adm_splunk_ssl_certificate.json` para crear el panel de muestra de información sobre certificados SSL.

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:

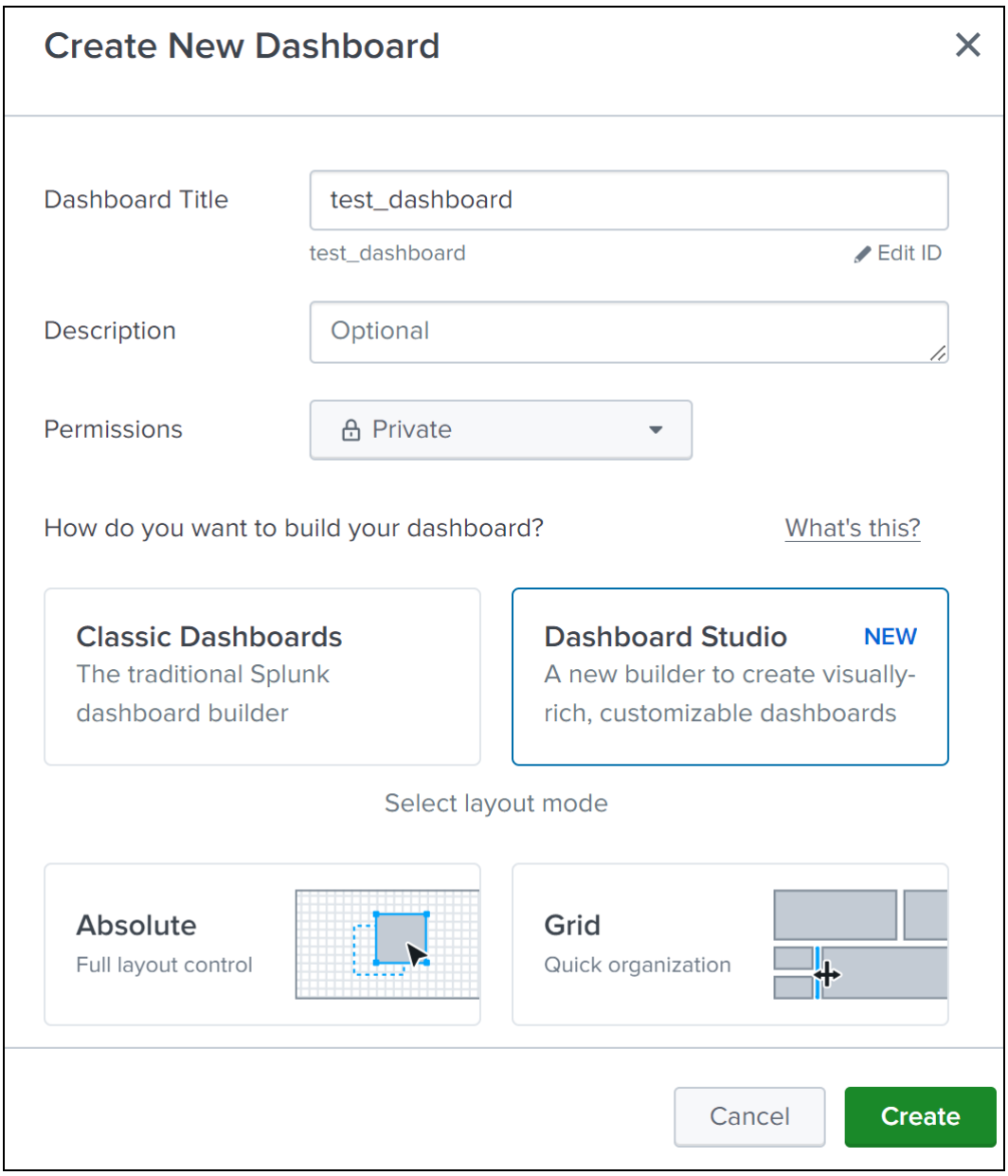
   a) **Título del panel**: Proporcione un título.

   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**.

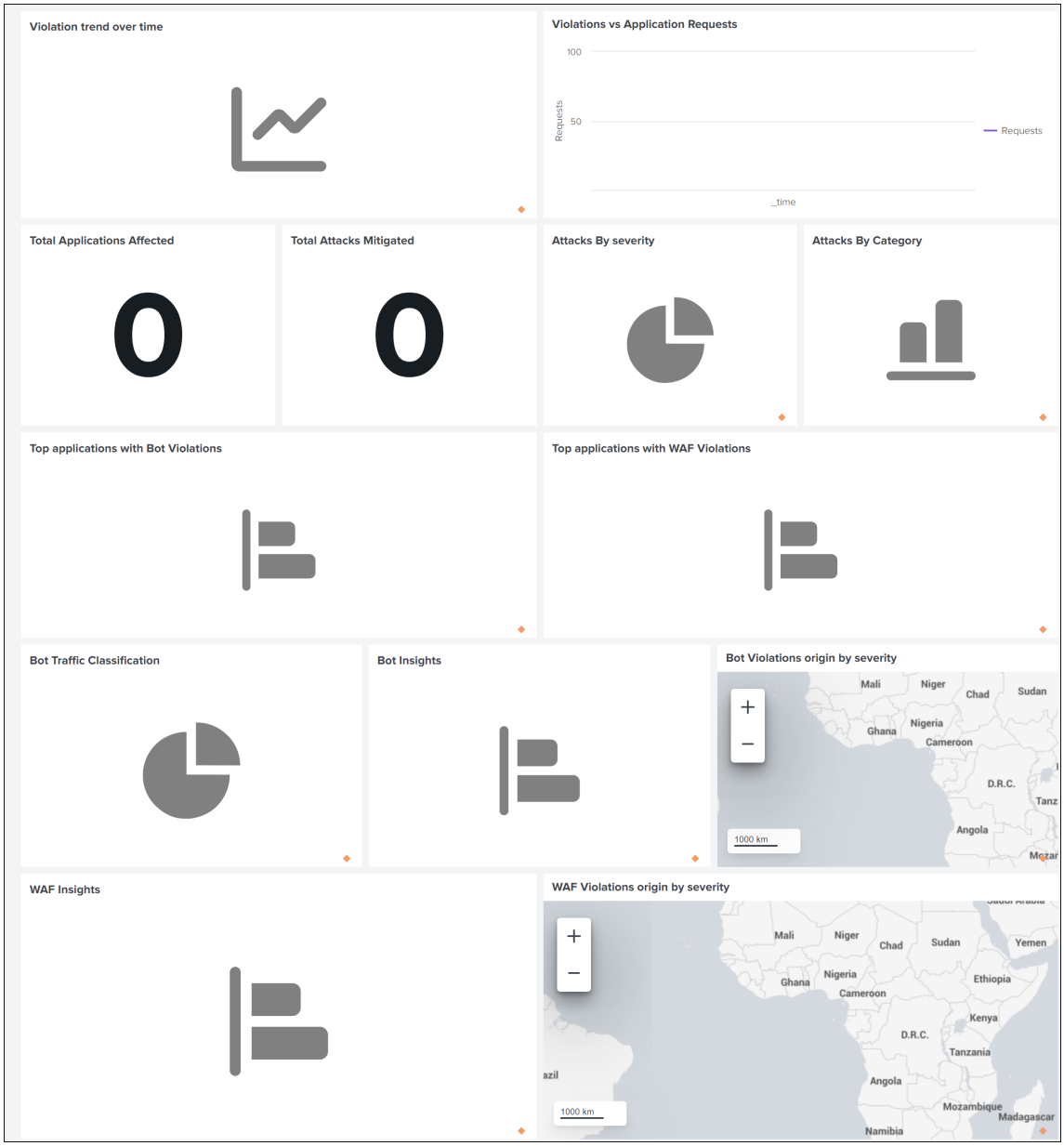
   e) Seleccione cualquier diseño (**Absoluto** o **Cuadrícula**) y, a continuación, haga clic en **Crear**.



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 siguiente panel de ejemplo en su instancia de Splunk.



Configurar NetScaler Console para exportar datos a Splunk

Ya lo tienes todo preparado en Splunk. El último paso consiste en configurar NetScaler Console creando una suscripción y añadiendo el token.

Al completar el siguiente procedimiento, puede ver el panel actualizado en Splunk que está disponible actualmente en su consola de NetScaler:

1. Inicie sesión en NetScaler Console.
2. Vaya a **Configuración > Integración de observabilidad**.

3. En la página **Integraciones**, haga clic en **Agregar**.
4. En la página **Crear suscripción**, especifique los siguientes detalles:
    a) Especifique un nombre de su elección en el campo **Nombre de la suscripción**.
    b) Seleccione **Consola de NetScaler** como **Origen** y haga clic en **Siguiente**.
    c) Seleccione **Splunk** y haga clic en **Configurar**. En la página **Configurar punto final**:
        i. **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.

        ii. **Token de autenticación** : copia y pega el token de autenticación de Splunk.
        iii. Haga clic en **Enviar**.
    d) Haga clic en **Siguiente**.
    e) Haga clic en **Agregar información** y, en la ficha **Seleccionar función**, puede seleccionar las funciones que quiere exportar y hacer clic en **Agregar selección**.
    f) Haga clic en **Siguiente**.
    g) 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.
    h) Haga clic en **Enviar**.

        > **Nota:**

> Los datos de las estadísticas seleccionadas se envían a Splunk inmediatamente después de que se detecten las infracciones en NetScaler Console.

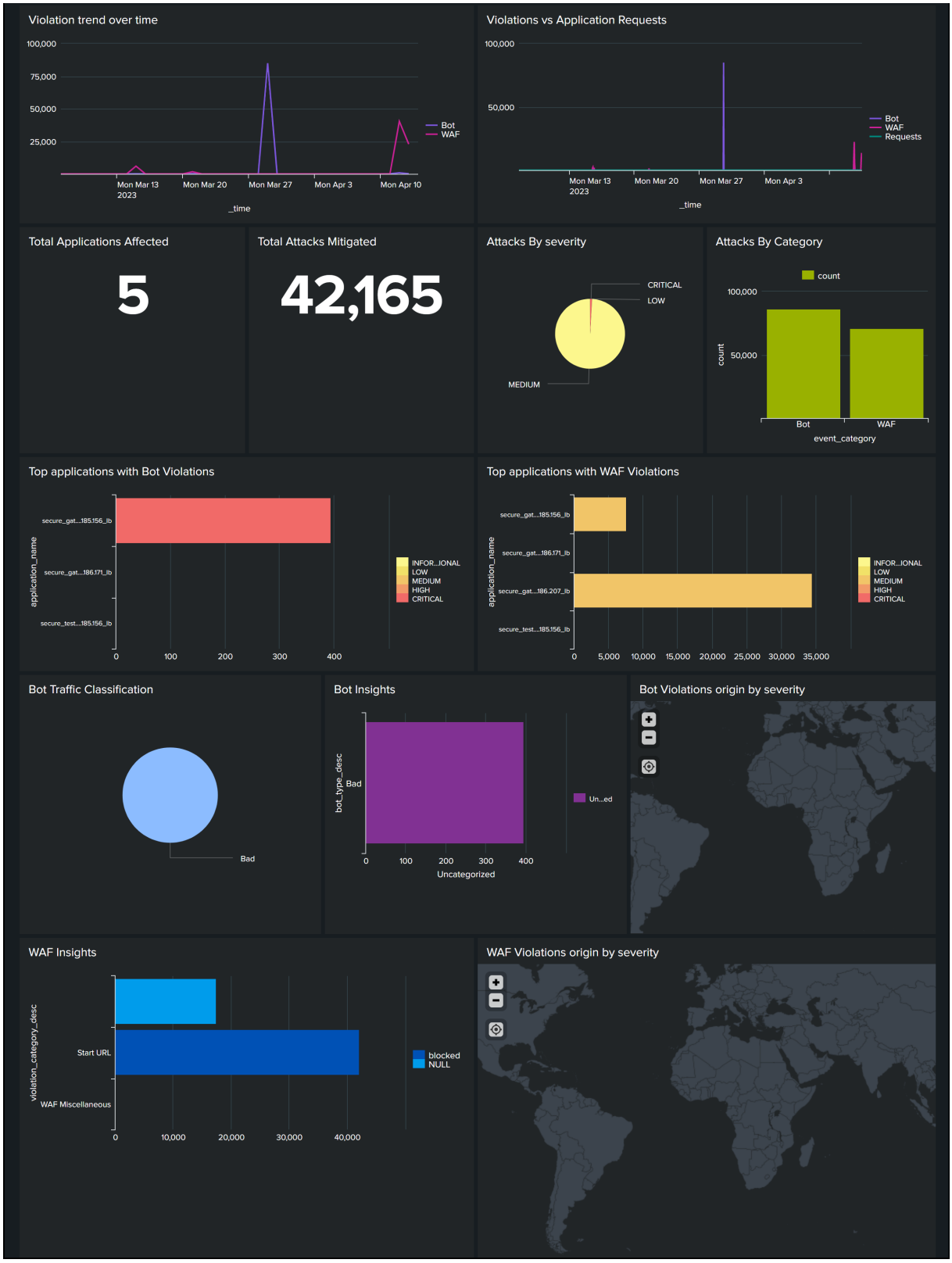
Ver paneles en Splunk

Tras completar la configuración en NetScaler Console, los eventos aparecen en Splunk.

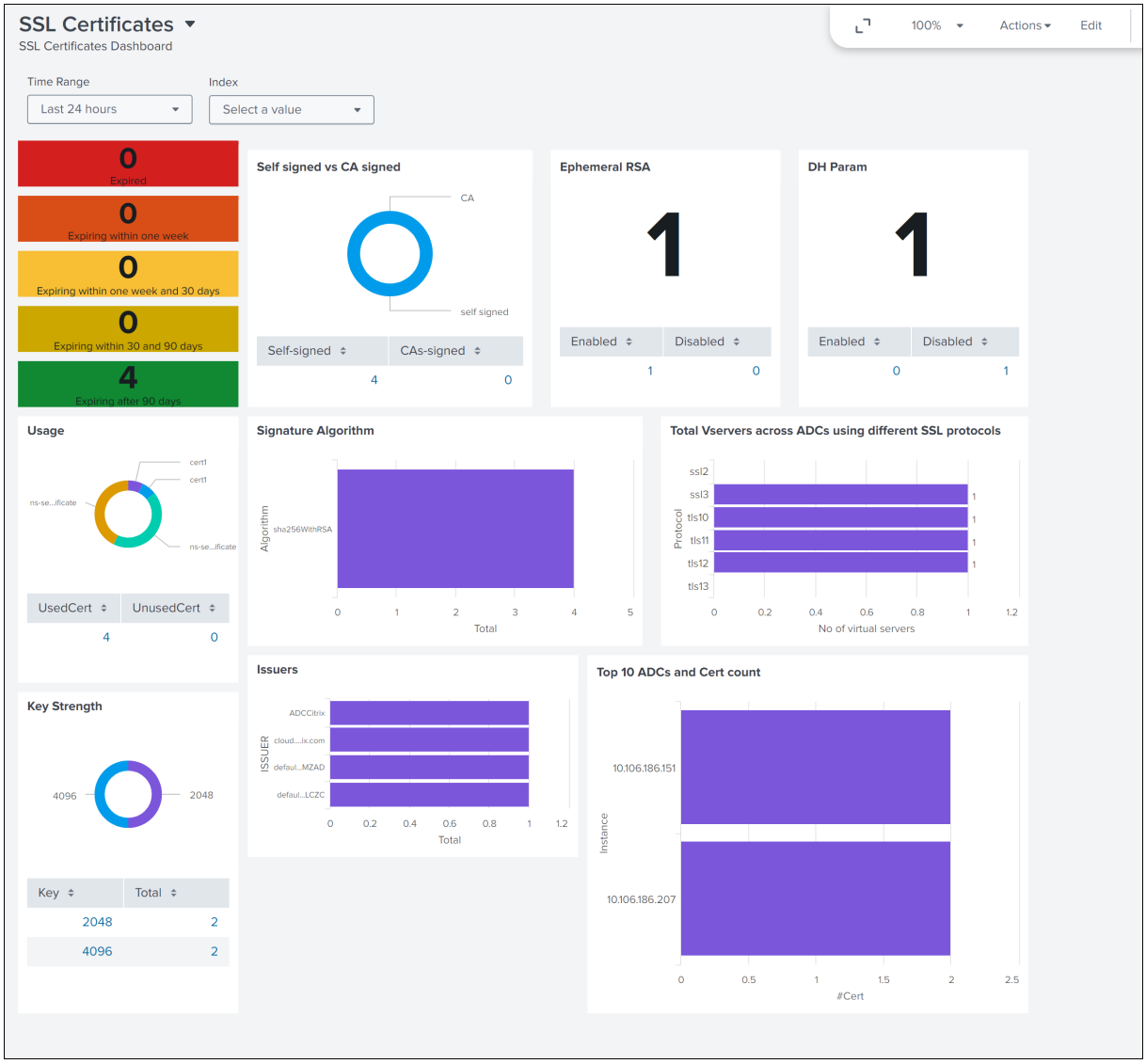
Ya está todo listo para ver el panel actualizado en Splunk sin ningún paso adicional.

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 SSL Certificate Insights actualizado.



Además del panel de control, también puedes 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="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.
   - Escriba `sourcetype="gateway_insights"` y seleccione la duración en la lista para ver los datos de Gateway Insights.

Integración de New Relic

July 17, 2024

Ahora puede integrar NetScaler Console 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 Console 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.
- Agregue los detalles clave en NetScaler Console

Agregue los detalles clave en NetScaler Console

Después de generar un token, debe agregar detalles en NetScaler Console para integrarlo con New Relic.

1. Inicie sesión en NetScaler Console.
2. Vaya a **Configuración > Integración de observabilidad**.
3. En la página **Integraciones**, haga clic en **Agregar**.

4. En la página **Crear suscripción**, especifique los siguientes detalles:

   a) Especifique un nombre de su elección en el campo **Nombre de la suscripción**.

   b) Seleccione **Consola de NetScaler** como **Origen** y haga clic en **Siguiente**.

   c) Seleccione **New Relic** y haz clic en **Configurar**. En la página **Configurar punto final**:

      i. **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.

   d) **Token de autenticación** : copia y pega el token de autenticación de New Relic.

      i. Haga clic en **Enviar**.

   e) Haga clic en **Siguiente**.

   f) Haga clic en **Agregar información** y, en la ficha **Seleccionar función**, puede seleccionar las funciones que quiere exportar y hacer clic en **Agregar selección**.

   g) Haga clic en **Siguiente**.

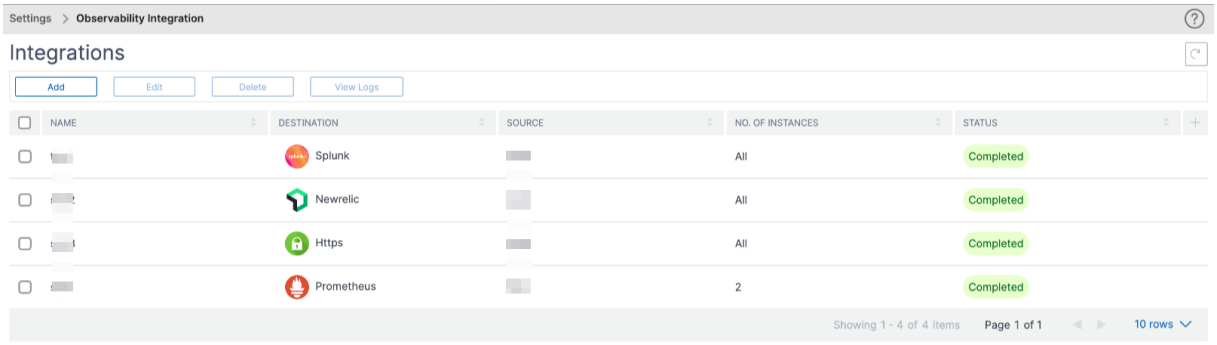
   h) En la ficha **Seleccionar instancia**, puede elegir **Seleccionar todas las instancias** o Selección **personalizada**y, a continuación, hacer clic en **Siguiente**.

      - **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.

   i) Haga clic en **Enviar**.

      > **Nota:**
      >
      > - Los datos de la información seleccionada se envían a New Relic inmediatamente después de que se detecten las infracciones en NetScaler Console.

La configuración está completa. Puede ver los detalles en la página **Suscripciones**.

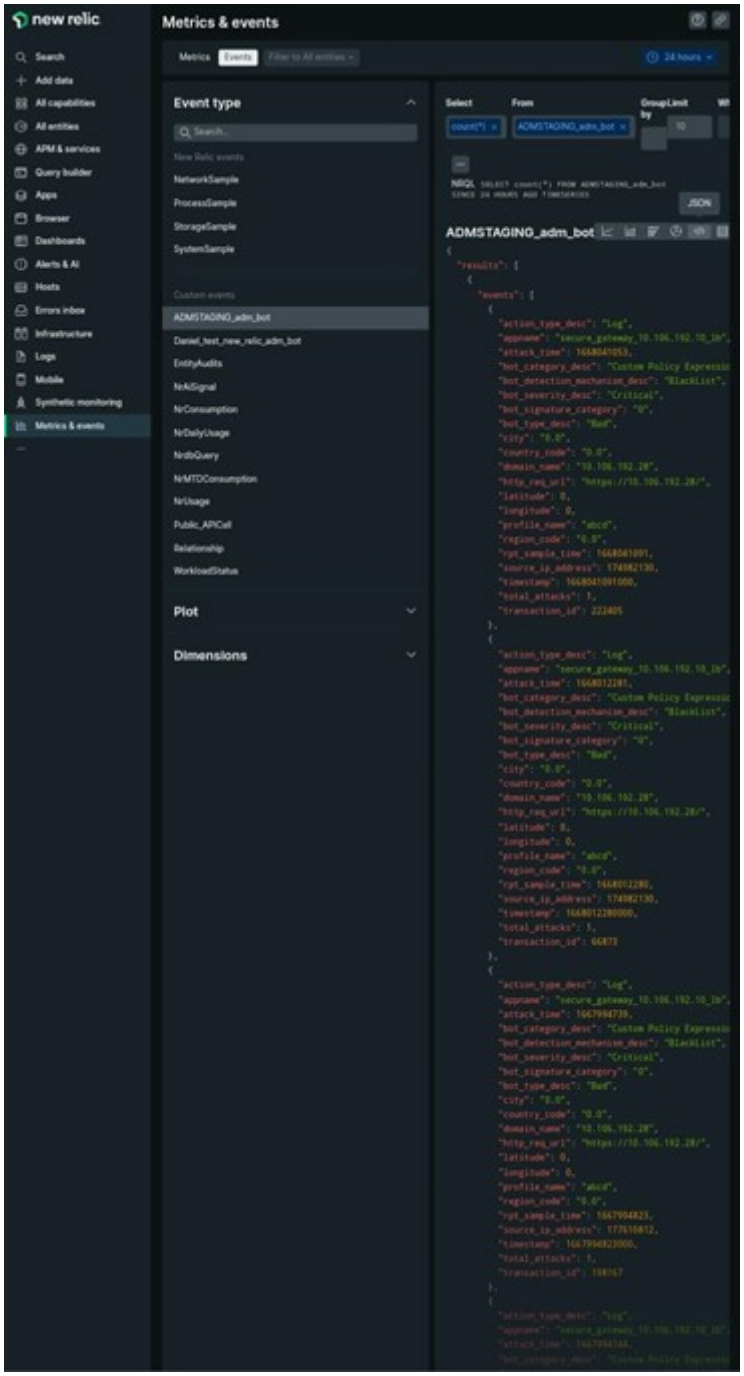


Panel de mandos de New Relic

Cuando los eventos se exportan a New Relic, puede ver los detalles de los eventos en **Métricas y eventos** en el siguiente formato JSON:

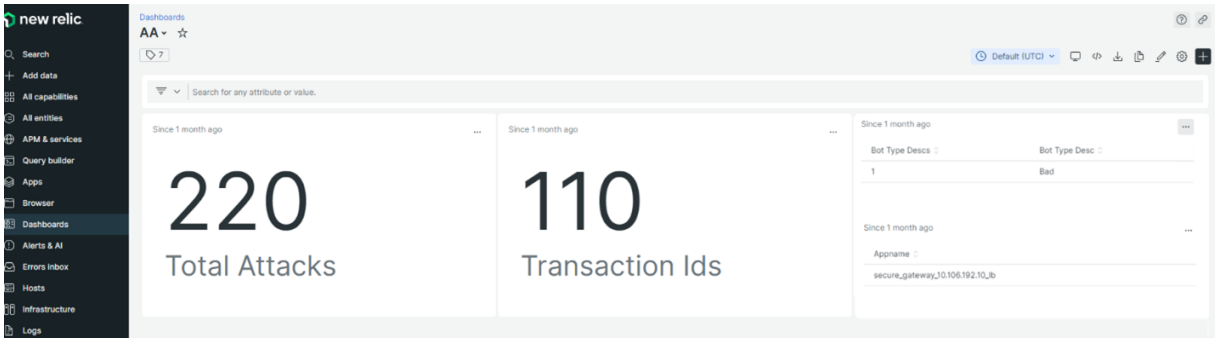
<subsription_name>_adm_<event name> donde el nombre del evento puede ser Bot, WAF, etc.

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
  ```

Integración con Microsoft Sentinel

September 2, 2024

Puede integrar NetScaler Console con Microsoft Sentinel para exportar los siguientes análisis de NetScaler Console a Microsoft Sentinel:

- Violaciones de WAF
- Infracciones de bots
- Información sobre certificados SSL
- Información sobre Gateway

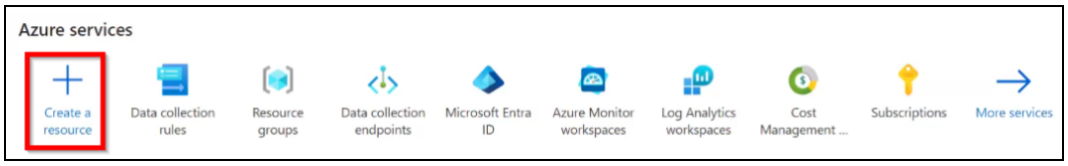
Microsoft Sentinel proporciona una recopilación de datos centralizada que reúne datos de diversas fuentes, como aplicaciones, servidores, etc. Como administrador, puede ver los datos y tomar decisiones después de que se notifiquen las ideas o las infracciones en Microsoft Sentinel.

Para que la integración se realice correctamente, asegúrese de tener una suscripción de Azure activa y, a continuación, siga el procedimiento que se indica en cada sección:

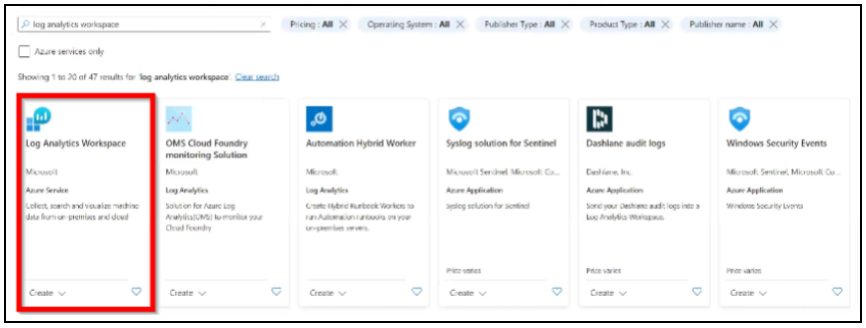
Configurar el espacio de trabajo de análisis de registros

Se requiere un espacio de trabajo de análisis de registros para almacenar y analizar los datos recopilados.

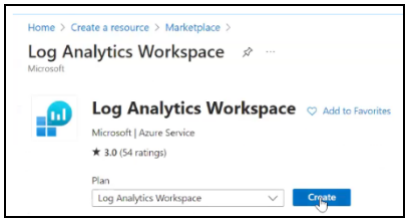
1. Inicie sesión en Azure.
2. Haga clic en **Crear un recurso**.



3. En la barra de búsqueda, escriba Log Analytics Workspace y haga clic en **Crear** en **Log Analytics Workspace**.



4. En la página principal de **Log Analytics Workspace**, haga clic en **Crear**.



5. En el **espacio de trabajo Crear análisis de registros**:

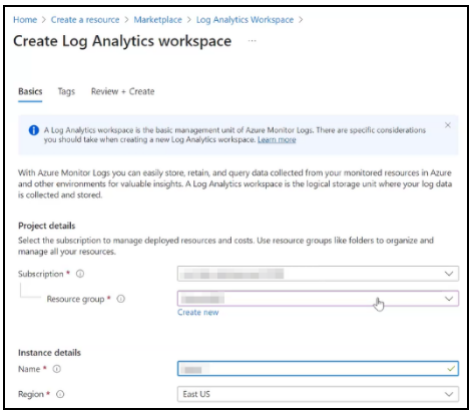
   a) Seleccione la suscripción activa y el grupo de recursos.

   > **Nota:**
   >
   > También puede hacer clic en **Crear nuevo** para agregar un grupo de recursos si tiene el privilegio.

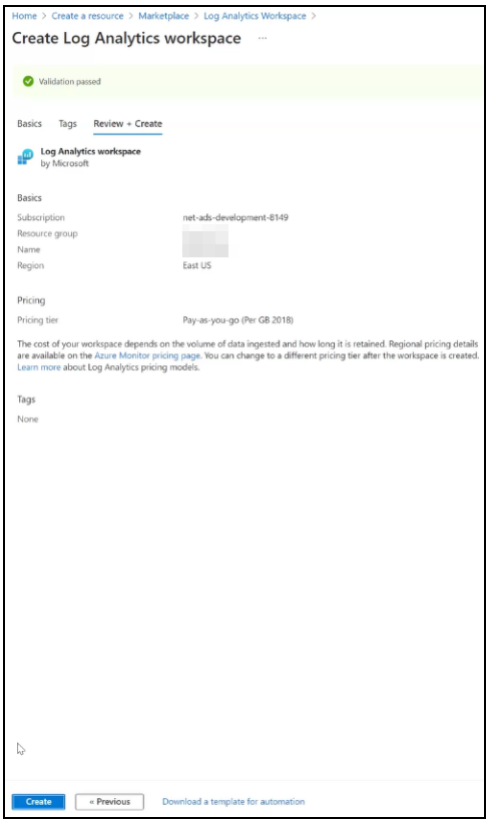
   b) Especifique un nombre de su elección.

c) Seleccione su región de la lista.

d) Haga clic en **Revisar + Crear**.



e) Aparece un mensaje de validación aprobada. Haga clic en **Crear** para implementar el espacio de trabajo.



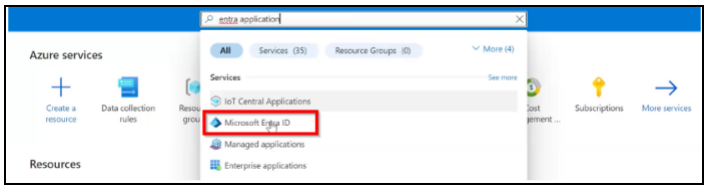
f) Puede ver el mensaje de implementación en curso. Cuando vea el mensaje de finalización de la implementación, haga clic en **Ir al recurso**.

El espacio de trabajo se creó correctamente.

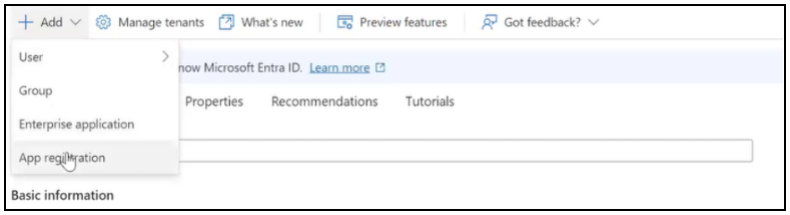
Crear una aplicación de Microsoft Entra

Debe crear una aplicación Entra asociada a su suscripción de Azure para comunicarse en nombre de Log Analytics Workspace. Tras crear la aplicación, también debe conceder el permiso con la función de **colaborador de Microsoft Sentinel**. La aplicación también proporciona detalles como el **ID de cliente**, el **ID de arrendatario** y el **secreto del cliente**. Le recomendamos que tome nota de estos detalles. Estos detalles son necesarios al crear una suscripción en NetScaler Console para completar el proceso de integración.

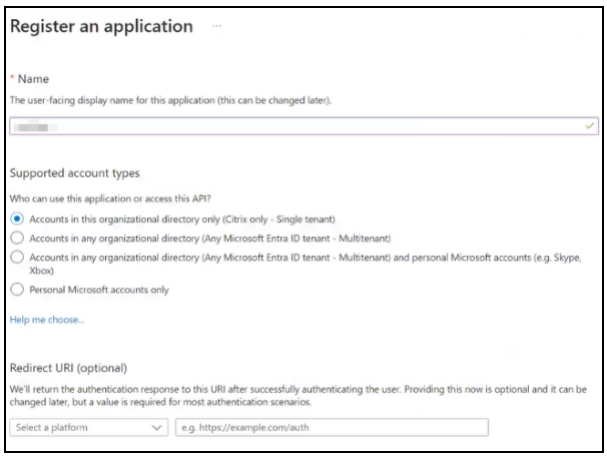
1. En su portal de Azure, escriba la palabra clave en la barra de búsqueda.
2. Haga clic en **Microsoft Entra ID**.



3. Haga clic en **Agregar** y seleccione **Registro de aplicaciones**.

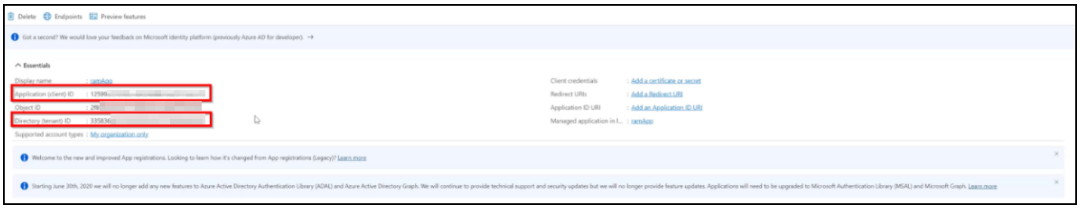


4. Especifique un nombre para la aplicación, seleccione la opción predeterminada en **Tipos de cuentas compatibles** y, a continuación, haga clic en **Registrar**.



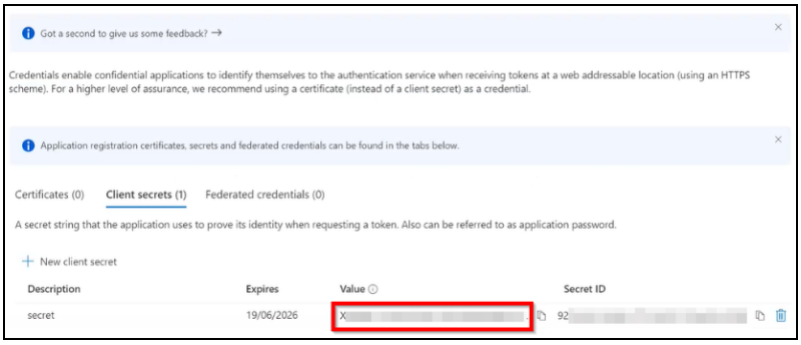
5. Después de registrar la solicitud:

   a) Anote el **ID de cliente** y el **ID de arrendatario**.



   b) Cree un identificador secreto para su aplicación. Haga clic en **Certificados y secretos** y, en **Secretos de cliente**, haga clic en **Nuevo secreto de cliente**. Proporcione una descripción, la validez y, a continuación, haga clic en **Agregar** para crear un ID secreto para su aplicación.

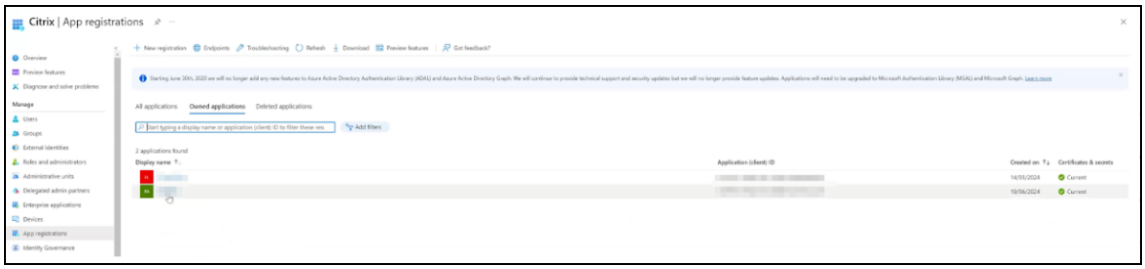
   c) Se muestran los detalles de su solicitud. Asegúrese de anotar el ID que aparece en **Valor** inmediatamente después de crear el secreto. Este valor se oculta si navega a cualquier otra opción de la GUI.



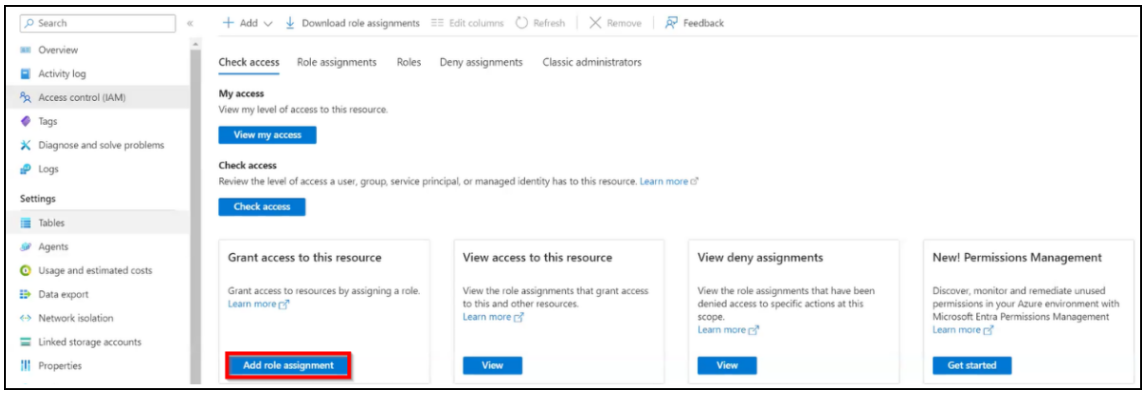
Asignar permiso para la aplicación Entra

Debe asignar a la aplicación la función de colaborador de Microsoft Sentinel. Para conceder el permiso:

1. Navegue hasta Microsoft Entra ID en su portal de Azure.
2. Haga clic en **Registros de aplicaciones** y, a continuación, seleccione su aplicación.



3. Haga clic en **Control de acceso (IAM)** y, a continuación, en **Agregar asignación de funciones**.

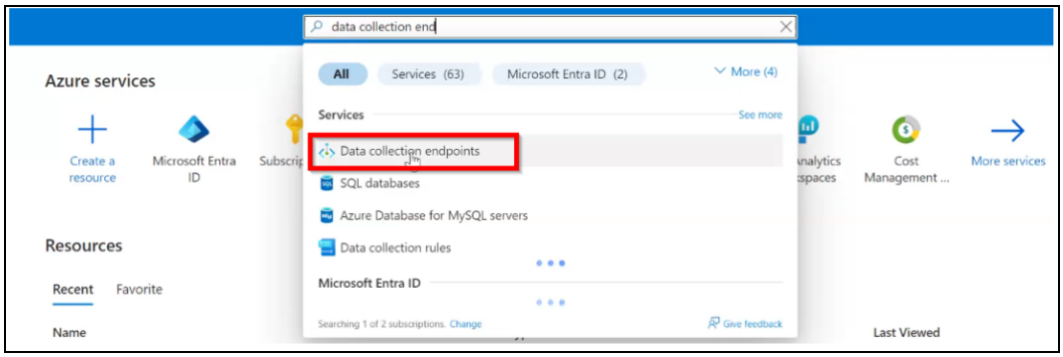


4. En la barra de búsqueda, escriba la palabra clave sentinel, seleccione **Microsoft Sentinel Contributor** y haga clic en **Siguiente**.
5. En la pestaña **Miembros**, haga clic en **Seleccionar miembros** y seleccione la aplicación Entra que creó.
6. Haga clic en **Revisar + asignar**.

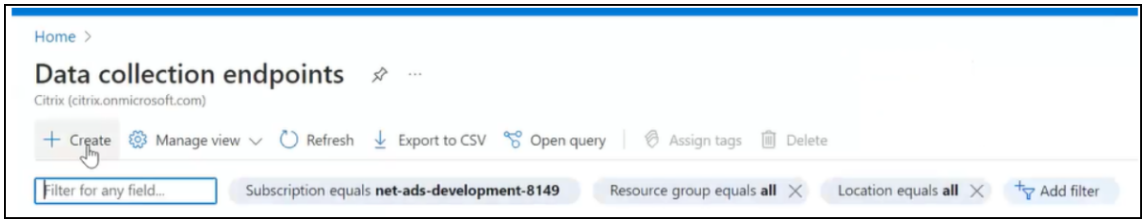
Configurar el punto final de recopilación de datos

Debe crear un punto final de recopilación de datos para obtener la URL del punto final. Esto es obligatorio al crear una suscripción en NetScaler Console.

1. En el portal de Azure, en **Servicios de Azure**, seleccione **Terminales de recopilación de datos** o escriba la palabra clave en la barra de búsqueda.



2. Haga clic en **Crear** en la página de **puntos finales de recopilación de datos** .



3. En **Crear punto final de recopilación de datos**:

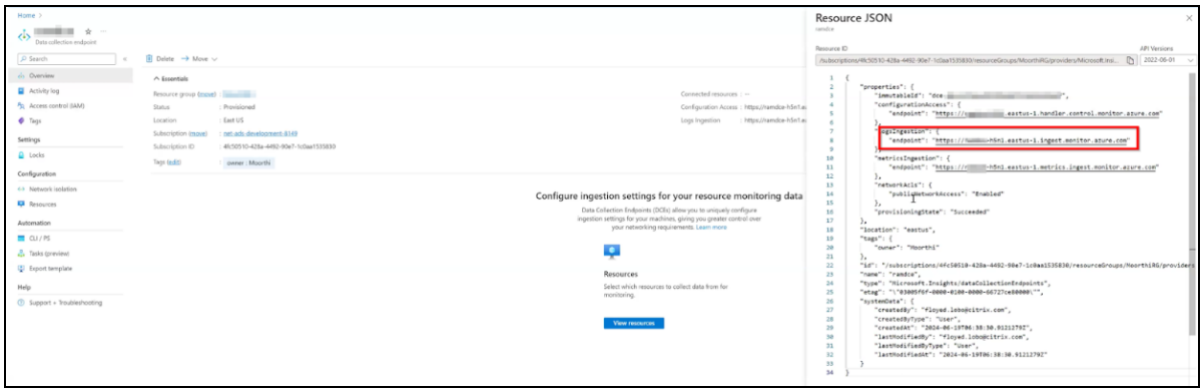
   a) Especifique un nombre de punto final de su elección

   b) Seleccione la **suscripción, grupo de recursos** y **región**.

   c) Haga clic en **Revisar + Crear**.

   d) Cuando vea el mensaje de validación aprobada, haga clic en **Crear**.

Debe tomar nota de la URL del punto final. En la página principal del **punto final de recopilación de datos**, seleccione el punto final creado, haga clic en la **vista JSON** y anote el ID del punto final.



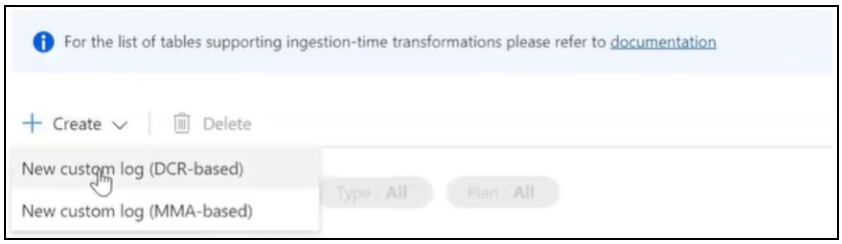
Crear tablas para exportar datos

Debe crear una tabla y proporcionar la información de JSON para cada información que quiera exportar de NetScaler Console a Microsoft Sentinel. Puede consultar los siguientes detalles en la tabla de requisitos para cada información:

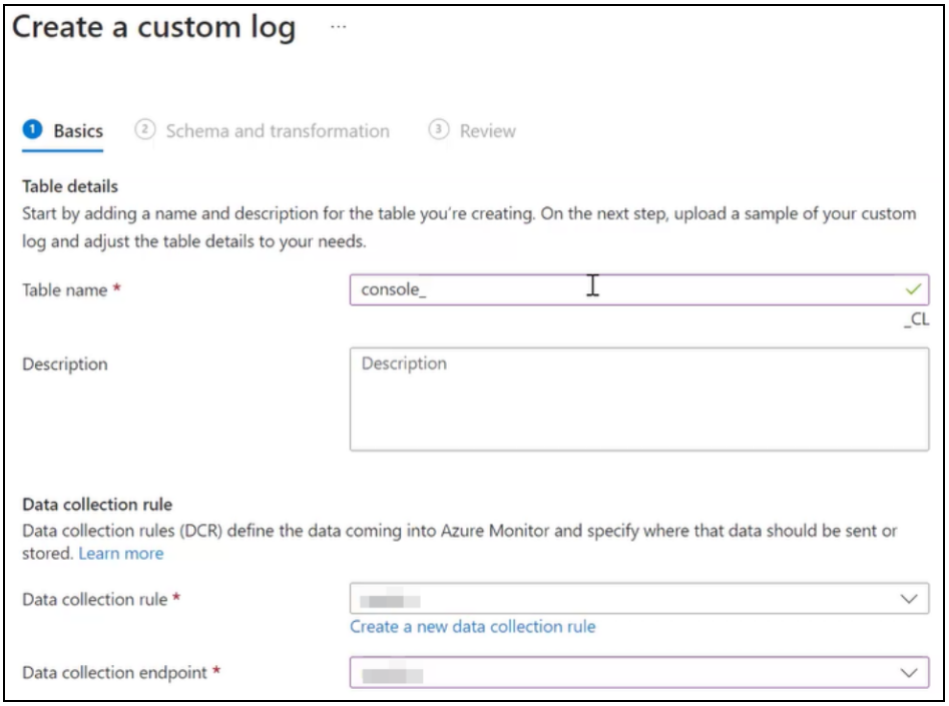
Ideas	Número total de tablas requeridas
Información sobre SSL	3
WAF	1
Bot	1
Información sobre Gateway	5

Para cada espacio de trabajo, puede crear un máximo de 10 tablas. Más allá de 10 tablas, debe crear otro espacio de trabajo.

1. Navegue hasta su espacio de trabajo en el portal de Azure y haga clic en **Tablas** en **Configuración**.
2. Haga clic en **Crear** y seleccione **Nuevo registro personalizado (basado en DCR)**



3. En **Crear un registro personalizado**:
    a) Especifique un nombre de tabla. El nombre de la tabla debe tener el formato **console_insightname**. Por ejemplo: **console_ns_sslvserver**, **console_ns_ssl_certkey**. Puede consultar el paso 4 para obtener los nombres de las tablas aplicables a cada información.
    b) Proporcione una descripción para agregar más información sobre el nombre de la tabla. Este paso es opcional.
    c) Cree una nueva regla de recopilación de datos y agréguela.
    d) Seleccione el punto final de recopilación de datos de la lista.



e) Haga clic en **Siguiente**.

4. En la pestaña **Esquema y transformación**, debe cargar los registros de muestra de JSON para obtener la información que desea exportar. Puedes usar el siguiente ejemplo de JSON para cada información y crear un archivo JSON para subirlo:

Ideas	JSON	Nombre de la tabla que se utilizará

Ideas	JSON	Nombre de la tabla que se utilizará
SSL (1)	{ "id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite":	console_ns_sslvserver

Ideas	JSON	Nombre de la tabla que se utilizará
SSL (2)	{ "id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size":	console_ns_ssl_certkey

Ideas	JSON	Nombre de la tabla que se utilizará
SSL (3)	{ "id": "2baffd1a-7ed6-4035-91e8-ad3a3125bff4", "certkeypair_name": "cert1", "ns_ip_address": "10.106.186.127", "poll_time": 1715671567, "partition_name": "", "display_name": "10.106.186.127", "hostname": "", "entity_name": "secure_gateway", "entity_type": "sslvserver", "table_name": "ns_sslcertkey_binding"}	console_ns_sslcertkey_binding

Ideas	JSON	Nombre de la tabla que se utilizará
WAF	[{ "ip_address": " 10.106.185.156", " ctnsappname": " vserver_1", "severity ": 2, "violation_type ": 19, " violation_type_desc": "Start URL", " block_flags": 1, " transformed_flags": 0, "not_blocked_flags ": 0, "country_code": "-NA-", "region_code ": "-NA-", "city": "- NA-", "latitude": 200.0, "longitude": 200.0, " signature_category": "", "attack_category" : 2, " attack_category_desc" : "Broken Authentication and Session Management", "total_attacks": 1, " rpt_sample_time": 1704783773, " source_ip_address": 174766492, " attack_time": 1704783538, " profile_name": " appfw_cs_lb_prof", " session_id": "", " http_req_url": "https ://10.106.192.54/ csrf_ffc/ffc.html? field10=asfasd", " violation_name": "-NA ", "violation_value" : "-NA-", " violation_location": 4, "	console_af_threat_exporter_data_l2

Ideas	JSON	Nombre de la tabla que se utilizará
Bot	{ "ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	console_af_bot_attack_details_l2

Ideas	JSON	Nombre de la tabla que se utilizará
Gateway Insight (1)	{ "adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}	console_af_vpn_error_details
Gateway Insight (2)	{ "adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}	console_ns_vpnvserver

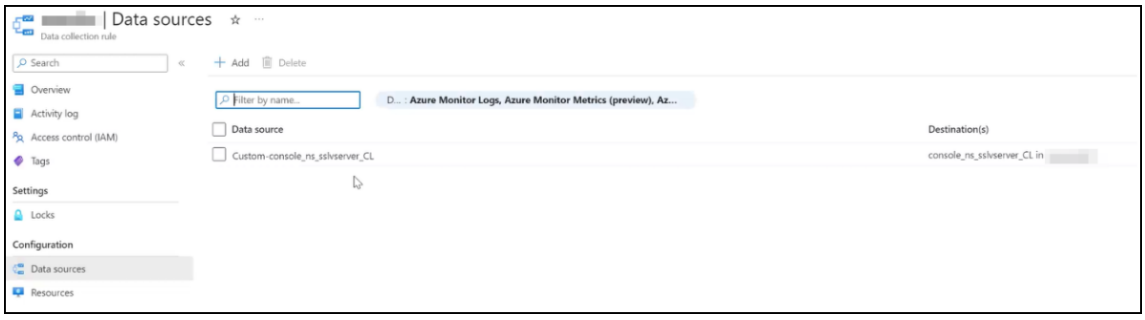
Ideas	JSON	Nombre de la tabla que se utilizará
Gateway Insight (3)	{ "adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1 }	console_af_vpn_session_details
Gateway Insight (4)	{ "active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}	console_af_vpn_active_session_1
Gateway Insight (5)	{ "adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports" }	console_af_vpn_error_reports

Tras cargar el JSON, puede ver los siguientes detalles:

Haga clic en el **editor de transformaciones**, introduzca la siguiente consulta que sea aplicable para obtener la información adecuada y haga clic en **Ejecutar** para aceptar los datos a partir del momento del sondeo en NetScaler Console.

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time)| project-rename sslvserver_id = id`
- **WAF** y **Bot** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

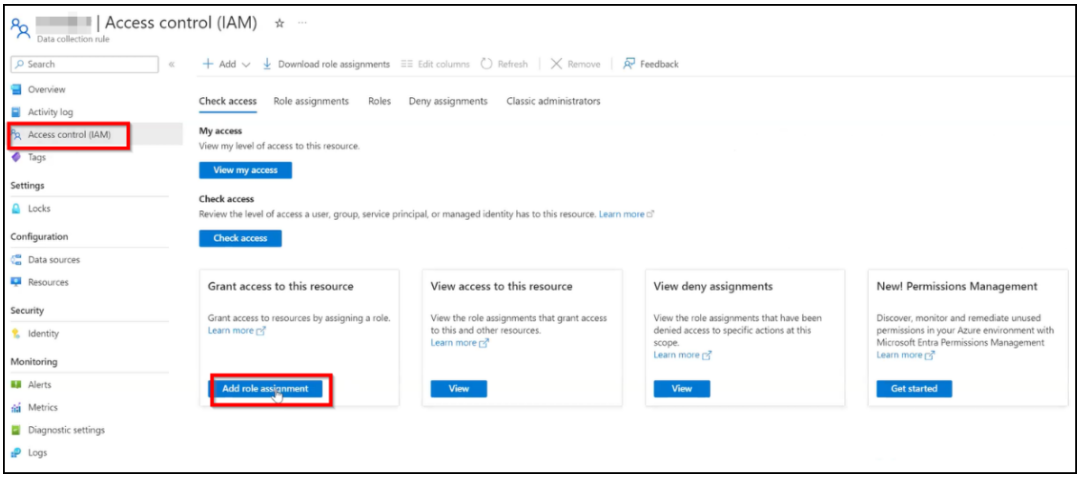
5. Haga clic en **Siguiente** y, a continuación, en **Crear** para completar.
6. Navegue hasta **Reglas de recopilación de datos** y haga clic en el DCR que ha creado.
7. En **Configuración**, haga clic en **Fuentes de datos** para ver la tabla creada.



La DCR (regla de recopilación de datos) requiere acceso a la función de **publicador de métricas de monitoreo**.

a) Navegue hasta su DCR, al que puede acceder desde su portal de Azure, en **Recientes**.

b) Haga clic en **Control de acceso (IAM)** en la página de DCR y, a continuación, haga clic en **Agregar asignación de funciones**.



c) En la barra de búsqueda, escriba la palabra clave monitor para seleccionar **Monitoring Metrics Publisher** y haga clic en **Siguiente**.

d) En la pestaña **Miembros**, haga clic en **Seleccionar miembros** y seleccione la aplicación Entra que creó.

e) Haga clic en **Revisar + asignar**.

Debe anotar el ID de las reglas de recopilación de datos. Vaya a la página de reglas de recopilación de datos, seleccione su DCR y haga clic en la vista JSON para tomar nota del ID.

Crear una suscripción en NetScaler Console

Ya tiene todo listo. El último paso consiste en configurar NetScaler Console mediante la creación de una suscripción y la adición de los detalles necesarios. Para crear una suscripción en NetScaler Console, necesita los siguientes detalles que ha anotado:

- URL de punto final
- ID de reglas de recopilación de datos

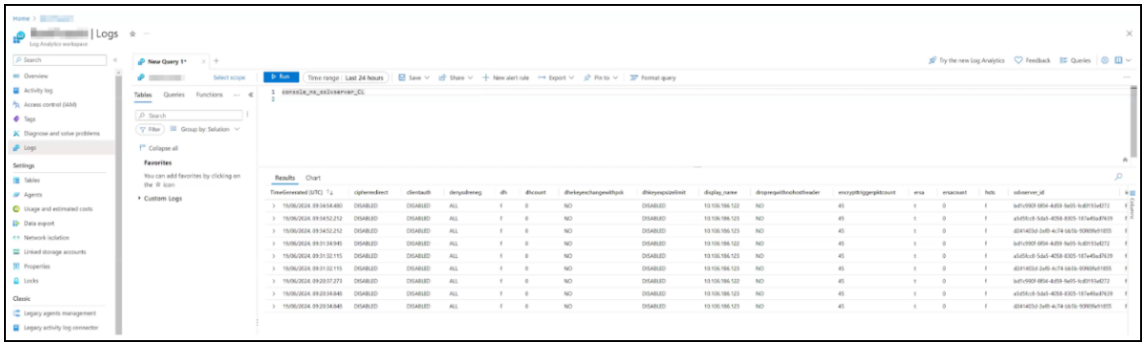
- ID de arrendatario
- ID de cliente
- Secreto del cliente

1. Inicie sesión en NetScaler Console.
2. Vaya a **Configuración > Integración de observabilidad**.
3. En la página **Integraciones**, haga clic en **Agregar**.
4. En la página **Crear suscripción**, especifique los siguientes detalles:
    a) Especifique un nombre de su elección en el campo Nombre de la suscripción.
    b) Seleccione **Consola de NetScaler** como **Origen** y haga clic en **Siguiente**.
    c) Seleccione **Microsoft Sentinel** y haga clic en **Configurar**. En la página **Configurar punto final**, introduzca todos los detalles y haga clic en **Enviar**.
    d) Haga clic en **Siguiente**.
5. Haga clic en **Agregar información** y, en la pestaña **Seleccionar función**, según las tablas que haya agregado en Microsoft Azure, seleccione las funciones que desea exportar, haga clic en **Agregar selección** y, a continuación, haga clic en **Siguiente**.
6. En la ficha **Seleccionar instancia**, puede elegir **Seleccionar todas las instancias** o **Selección personalizada** y, a continuación, hacer clic en **Siguiente**.
    - **Seleccionar todas las instancias**: exporta datos a Microsoft Sentinel 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 exportan a Microsoft Sentinel solo desde las instancias de NetScaler seleccionadas.
7. Haga clic en **Enviar**.

Ver registros en Microsoft Azure

Después de configurar todo, le recomendamos que espere hasta 30 minutos para ver los detalles en Microsoft Azure.

1. En su portal de Azure, navegue hasta su **espacio de trabajo de Log Analytics**.
2. Haga clic en **Registros**, introduzca el nombre de la tabla y haga clic en **Ejecutar** para ver los resultados.



Configure las instancias de NetScaler para la exportación de información a Prometheus mediante el esquema predeterminado

September 2, 2024

NetScaler admite la exportación directa de métricas a Prometheus. Puede utilizar el amplio conjunto de métricas que proporciona la instancia de NetScaler para supervisar el estado de NetScaler y el estado de las aplicaciones. Por ejemplo, puede recopilar métricas sobre el uso de la CPU y la memoria para conocer el estado de NetScaler. Del mismo modo, puede utilizar métricas como la cantidad de solicitudes HTTP recibidas por segundo o la cantidad de clientes activos para supervisar el estado de la aplicación.

Para exportar las métricas a Prometheus, debes configurar un perfil de análisis con el tipo de serie temporal. Para obtener más información, consulte Supervisar NetScaler, las aplicaciones y la seguridad de las aplicaciones con Prometheus.

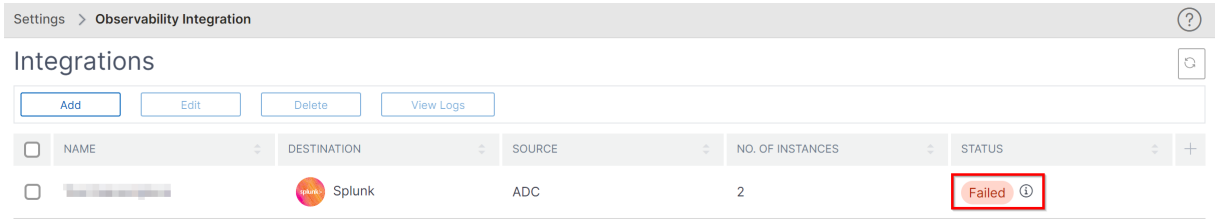
Con la función de integración de observabilidad de NetScaler Console, puede configurar la exportación de información a Prometheus mediante el esquema predeterminado.

1. Vaya a **Configuración > Integración de observabilidad**.
2. En la página **Integraciones**, haga clic en **Agregar**.
3. En la página **Crear suscripción**, especifique los siguientes detalles:
    a) Especifique un nombre de su elección en el campo **Nombre de la suscripción**.
    b) Seleccione **NetScaler** como **Origen** y haga clic en **Siguiente**.
    c) Seleccione **Prometheus** como destino.
    d) Seleccione **Predeterminado** para ver la información predeterminada de los exportados.
    e) Haga clic en **Agregar instancias** y selecciona las instancias para las que deseas exportar información a Prometheus.

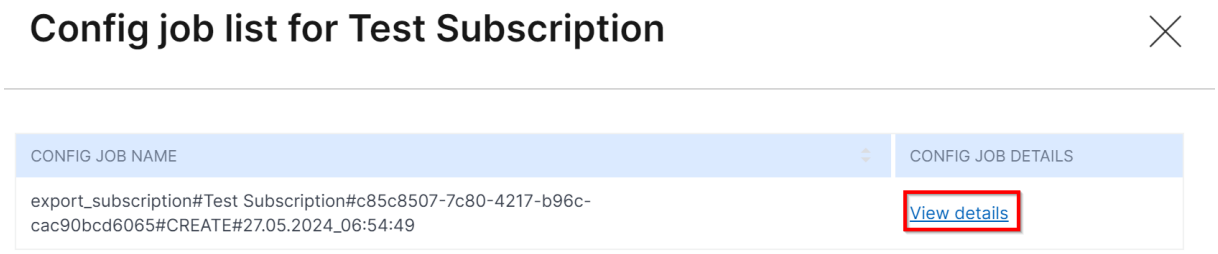
f) Haga clic en **Enviar**.

Ver los registros de configuraciones fallidas

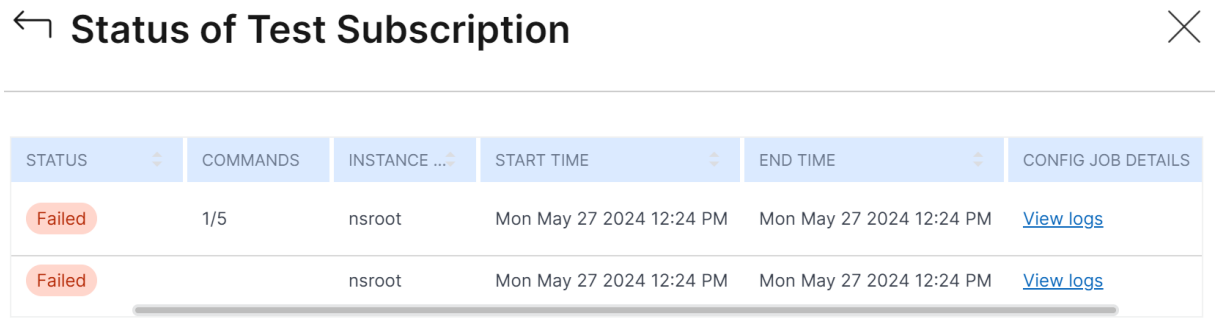
Después de crear una suscripción, puede ver su estado en **Parámetros > Integración de observabilidad**. Si el estado muestra **Fallido**, haga clic para ver los detalles.



Haga clic en **Ver detalles** en la sección **Detalles del trabajo de configuración**.



Haga clic en **Ver registros** para ver los detalles del problema.



Configurar la exportación de las métricas y los registros de auditoría de NetScaler a Splunk

September 2, 2024

NetScaler admite la exportación directa de métricas a Splunk en formato JSON. NetScaler proporciona métricas detalladas para supervisar el estado de las aplicaciones y el estado de la seguridad de

las aplicaciones. Al exportar las métricas proporcionadas por NetScaler a Splunk, puede visualizar las métricas y obtener información significativa.

El registro de auditoría le permite registrar los estados de NetScaler y la información de estado recopilada por varios módulos de NetScaler. Al revisar los registros, puede solucionar problemas o errores y corregirlos.

Para obtener más información, consulte:

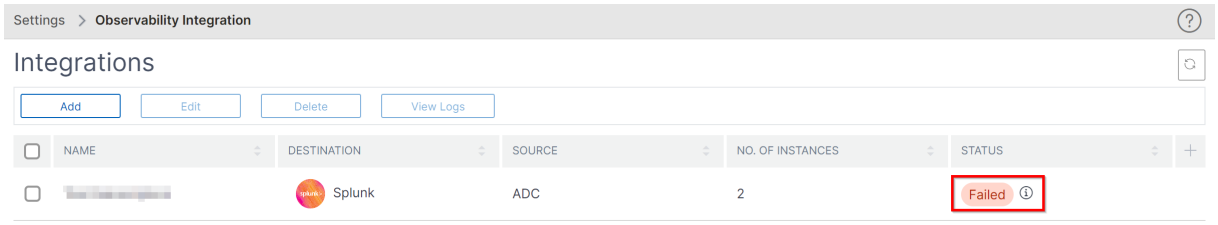
- Exportar los registros de auditoría directamente desde NetScaler a Splunk
- Exportar las métricas directamente de NetScaler a Splunk

Para configurar la exportación de métricas y registros de auditoría a Splunk a través de NetScaler Console:

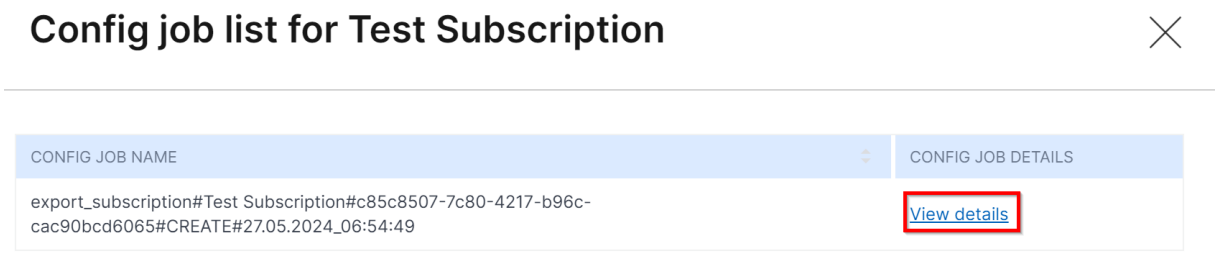
1. Vaya a **Configuración > Integración de observabilidad**.
2. En la página **Integraciones**, haga clic en **Agregar**.
3. En la página **Crear suscripción**, especifique los siguientes detalles:
    a) Especifique un nombre de su elección en el campo **Nombre de la suscripción**.
    b) Seleccione **NetScaler** como **Origen** y haga clic en **Siguiente**.
    c) Seleccione **Splunk** como **destino** y haga clic en **Configurar**. En Configurar dispositivo de punto final:
        - **URL del dispositivo de punto final**: Especifique los detalles del dispositivo de punto final de Splunk. El punto final debe estar en el formato <https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event> ‘.
        - **Token de autenticación**: Copie y pegue el token de autenticación de Splunk.
        - Haga clic en **Enviar**.
    d) Haga clic en **Siguiente**.
    e) Haga clic en **Agregar información** y seleccione **Métricas de NetScaler** y **Registros de audoltoría de NetScaler** y, a continuación, haga clic en **Agregar seleccionados**.
    f) Haga clic en **Siguiente**.
    g) Haga clic en **Agregar instancias** y seleccione las instancias.
    h) Haga clic en **Enviar**.

Ver los registros de configuraciones fallidas

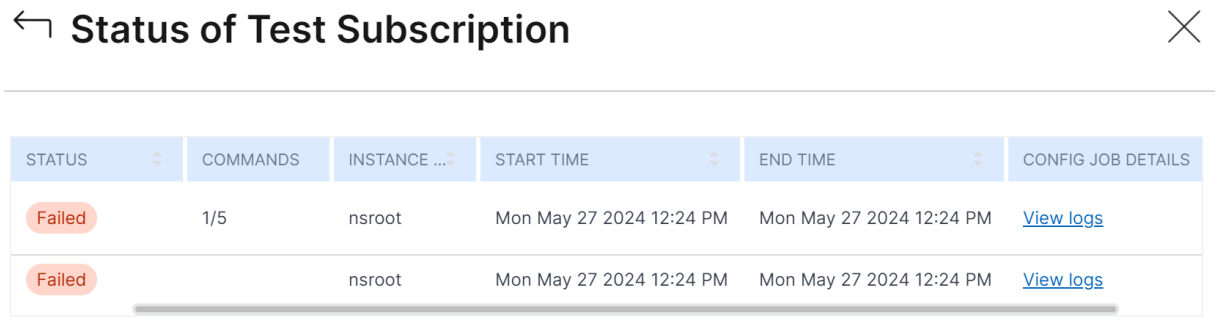
Después de crear una suscripción, puede ver su estado en **Parámetros > Integración de observabilidad**. Si el estado muestra **Fallido**, haga clic para ver los detalles.



Haga clic en **Ver detalles** en la sección **Detalles del trabajo de configuración**.



Haga clic en **Ver registros** para ver los detalles del problema.



Configurar los ajustes de Analytics

January 26, 2024

Antes de empezar a utilizar la función Analytics de NetScaler Console para obtener visibilidad de los datos de las instancias y las aplicaciones, se recomienda configurar algunos ajustes de análisis para garantizar una experiencia óptima con esta función.

Creación de umbrales y alertas para Analytics

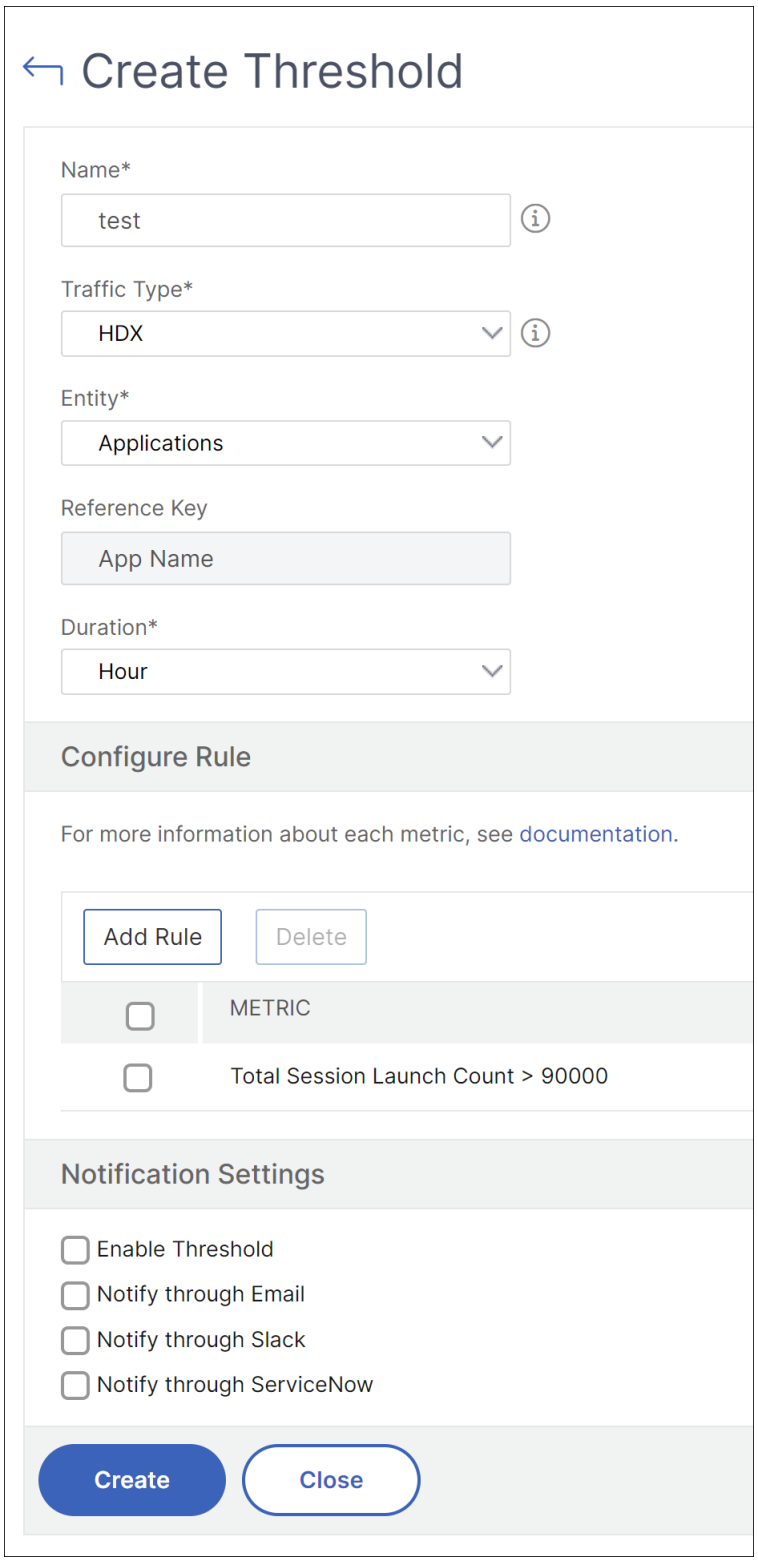
Puede establecer umbrales y alertas para supervisar las métricas analíticas de los servidores virtuales administrados configurados en las instancias detectadas. Cuando el valor de una métrica supera el umbral, NetScaler Console genera un evento que indica una infracción del umbral.

También puede asociar acciones con los umbrales establecidos. Las acciones incluyen mostrar una alerta en la GUI y enviar el correo electrónico tal como está configurado.

Por ejemplo, puede establecer un umbral para generar un evento para HDX Insight si el valor ICA RTT de algún usuario supera 1 segundo. También puede habilitar las alertas para el evento generado y enviar la información sobre el incumplimiento del umbral a una lista de correo electrónico configurada.

Para crear umbrales y alertas para análisis:

1. Vaya a **Configuración** > **Configuración de Analytics** > **Umbrales**.
2. En la pantalla **Umbrales**, haga clic en **Agregar** para agregar un nuevo umbral y configurar alertas para los umbrales establecidos.
3. En la página **Crear umbrales y alertas**, especifique los siguientes detalles:
    - **Nombre**: Nombre para configurar el umbral.
    - **Tipo de tráfico** : tipo de tráfico de análisis para el que quiere configurar el umbral. Por ejemplo: HDX Insight, Security Insight.
    - **Entidad**: Categoría o tipo de recurso para el que quiere configurar el umbral.
    - **Clave de referencia**: Valor generado automáticamente según el tipo de tráfico y la entidad seleccionados.
    - **Duración**: Intervalo para el que quiere configurar el umbral.
4. Para configurar las notificaciones por correo electrónico, seleccione la casilla de verificación de los umbrales establecidos.
5. En la sección **Reglas**, especifique lo siguiente:
    - **Métrica** : métrica del tipo de tráfico seleccionado para configurar el umbral.
    - **Comparador** : comparador con la métrica seleccionada (por ejemplo: <, > =).
    - **Valor** : valor de la métrica para establecer el umbral e invocar alertas.
6. Haga clic en **Crear**.



Configurar notificaciones

January 26, 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 Console.
- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias NetScaler. Para obtener más información, consulte Caducidad del certificado SSL

NetScaler Console admite los siguientes tipos de notificaciones:

- Correo electrónico
- SMS
- Slack
- PagerDuty
- ServiceNow

Para cada tipo de notificación, la GUI de NetScaler Console muestra la lista o el perfil de distribución configurados. La consola de NetScaler envía notificaciones a la lista de distribución o perfil seleccionados.

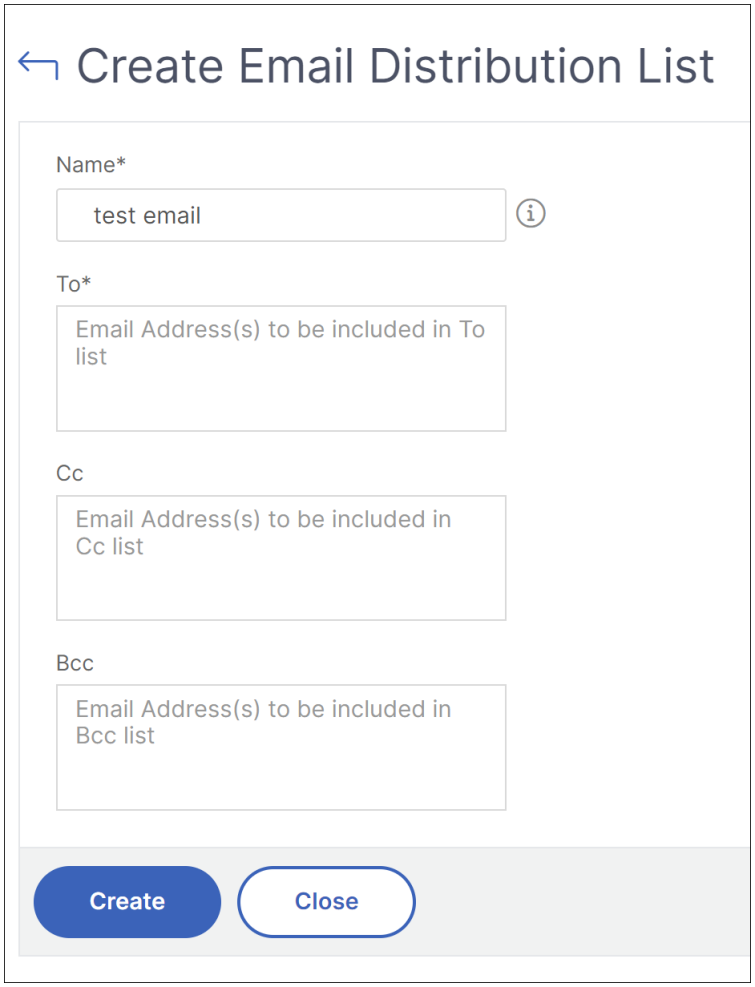
Crea una lista de distribución de correo electrónico

Para recibir notificaciones por correo electrónico para las funciones de NetScaler Console, 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.
    - **Para**: especifique las direcciones de correo electrónico a las que NetScaler Console debe enviar mensajes.
    - **Cc**: especifique las direcciones de correo electrónico a las que NetScaler Console debe enviar copias de los mensajes.

- **Bcc**: especifique las direcciones de correo electrónico a las que NetScaler Console 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 pestaña **Correo** electrónico muestra todas las listas de distribución de correo electrónico presentes en NetScaler Console.

Crea una lista de distribución de SMS

Para recibir notificaciones por SMS para las funciones de NetScaler Console, debe añadir un servidor de 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 NetScaler Console debe enviar los mensajes.
4. Haga clic en **Crear**.

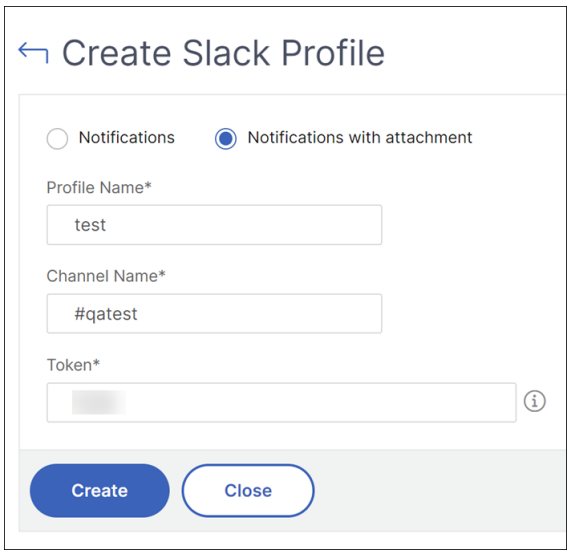
Repita este procedimiento para crear varias listas de distribución de SMS. La pestaña **SMS** muestra todas las listas de distribución de SMS presentes en NetScaler Console.

Crear un perfil de Slack

Para recibir notificaciones de Slack sobre las funciones de la consola NetScaler, 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 : especifique el nombre del canal de Slack al que NetScaler Console 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 pestaña **Slack** muestra todos los perfiles de Slack presentes en NetScaler Console.

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 añadir un perfil de PagerDuty en NetScaler Console, 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 pestaña **PagerDuty** muestra todos los perfiles de PagerDuty presentes en NetScaler Console.

Ver el perfil de ServiceNow

Si desea habilitar las notificaciones de ServiceNow para los eventos de NetScaler y los eventos de NetScaler Console, debe integrar NetScaler Console con ServiceNow mediante el conector ITSM. Para obtener más información, consulte Integrar NetScaler Console 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 desea ver los tickets de ServiceNow en la GUI de NetScaler Console, seleccione los **tickets de ServiceNow**.

Exportar o programar informes de exportación

January 26, 2024

En NetScaler Console, puede exportar un informe completo para la función de NetScaler Console seleccionada. Este informe proporciona una visión general de la asignación entre las instancias, las particiones y los detalles correspondientes.

NetScaler Console muestra informes de exportación programados específicos de cada función en las funciones individuales de NetScaler Console, que puede ver, editar o eliminar. Por ejemplo, para ver los informes de exportación de las instancias de NetScaler, vaya a **Infraestructura > Instancias > NetScaler** y haga clic en el icono de exportación. Puede exportar estos informes en formato PDF, JPEG, PNG y CSV.

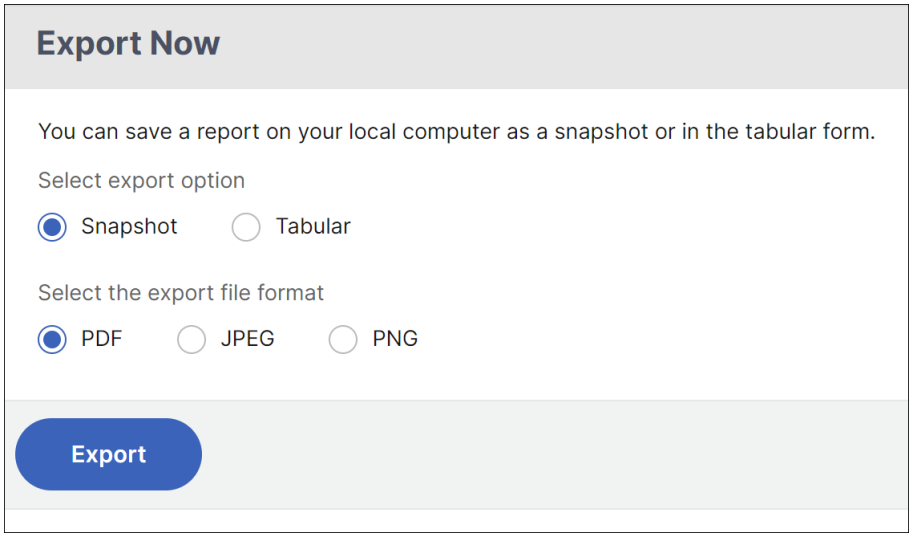
En **Exportar informes**, puede realizar las siguientes acciones:

- 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 de la consola de NetScaler al equipo local, lleve a cabo 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 los informes de NetScaler Console como una instantánea.
    - **Tabular**: esta opción exporta los informes de NetScaler Console 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**.

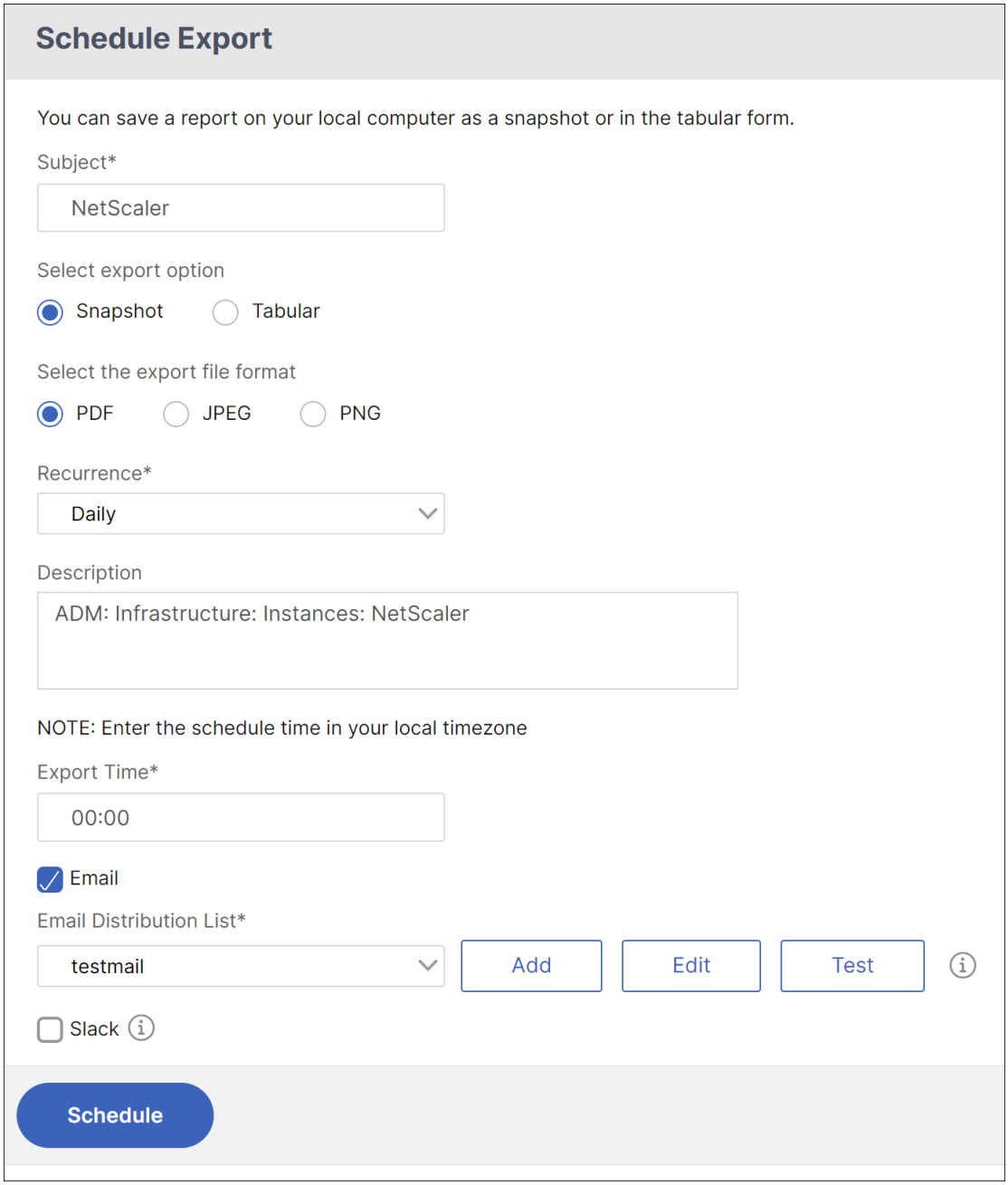
Programar informe de exportación

Para programar el informe de exportación a intervalos regulares, especifique el intervalo de recurrencia. NetScaler Console 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**de exportación : exporte los informes de NetScaler Console en formato de instantánea o 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**.

Configuración de instancia

January 26, 2024

Puede administrar las instancias descubiertas en NetScaler Console y configurar los ajustes de respaldo de las instancias.

Gestiona la configuración de la instancia

En **Configuración > Configuración global > Configuración de instancias > Administración de instancias**, puedes modificar las siguientes configuraciones de instancias:

- **Comunicación con las instancias : puede**elegir un canal de comunicación HTTP o HTTPS entre NetScaler Console y las instancias descubiertas.
- **Habilitar la descarga de certificados**: le permite descargar los certificados SSL de una instancia detectada.
- **Credenciales rápidas para iniciar sesión en la instancia :**al acceder a la instancia a través de la GUI de NetScaler Console, aparece la página de inicio de sesión de la instancia. Especifica sus credenciales de inicio de sesión para acceder a una instancia.

Configurar las opciones de copia de seguridad de instancia

En **Configuración > Configuración global > Configuración de instancia > Copia de seguridad** de instancias , puede configurar los ajustes de respaldo de las instancias de NetScaler descubiertas en NetScaler Console.

En **Configurar los ajustes de copia de seguridad**de la **instancia, seleccione Habilitar las copias**

- **Cantidad de archivos de copia de seguridad que se van a conservar**: especifique la cantidad de archivos de copia de seguridad que se van a conservar en la consola de NetScaler. Puede conservar hasta 3 archivos de backup por instancia de NetScaler. El valor predeterminado es 1 archivo de respaldo.
- **Configuración de programación de copias**de seguridad: puede programar una copia de seguridad de una instancia de dos maneras:
  - **Basado**en intervalos : se crea un archivo de respaldo en NetScaler Console una vez transcurrido el intervalo especificado. El intervalo de copia de seguridad predeterminado es de 12 horas.

- **Basado**en el tiempo : especifique la hora en `hours:minutes`el formato a la que desea que NetScaler Console realice la copia de seguridad de la instancia.

- Configuración de**NetScaler**: Con esta opción, puede iniciar una copia de seguridad en función de la captura e incluir archivos de GeoDB en la copia de seguridad. Esta configuración se aplica a las instancias MPX, VPX, CPX y BLX.

  - **Realice una copia de seguridad de la instancia cuando reciba**la captura de NetScaler-ConfigSave : de forma predeterminada, NetScaler Console no crea un archivo de copia de seguridad cuando recibe la captura «NetScalerConfigSave». Sin embargo, puede habilitar la opción de crear un archivo de respaldo siempre que una instancia de NetScaler envíe una `NetScalerConfigSave`trampa a NetScaler Console.

    Se envía una instancia de NetScaler `NetScalerConfigSave` cada vez que se guarda la configuración de la instancia.

    Especifique el **retraso de Backup on trap** en minutos. Si la captura recibida `NetScalerConfigSave`persiste durante los minutos especificados en NetScaler Console, NetScaler Console realiza una copia de seguridad de la instancia.

  - **Incluir archivos**de GeoDB : de forma predeterminada, NetScaler Console no hace copias de seguridad de los archivos de GeoDatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.

- **Configuración de NetScaler SDX**: para hacer copias de seguridad de las instancias SDX, especifique el **tiempo de espera de la copia de seguridad** en minutos. Durante la copia de seguridad de una instancia SDX, la conexión entre NetScaler Console y SDX se mantiene durante el período especificado.

  Para archivos de respaldo SDX de gran tamaño, mantenga la conexión entre NetScaler Console y la instancia SDX durante un período más largo para garantizar la finalización del respaldo.

  > **Importante:**
  >
  > La copia de seguridad falla si se agota el tiempo de espera de la conexión.

- **Transferencia externa :**NetScaler Console le permite transferir los archivos de respaldo de la instancia de NetScaler a una ubicación externa:

  1. Especifique la dirección IP de la ubicación.
  2. Especifique el nombre de usuario y la contraseña del servidor externo al que quiere transferir los archivos de copia de seguridad.
  3. Especifique el protocolo de transferencia y el número de puerto.
  4. Especifique la ruta del directorio en la que debe almacenarse el archivo.

5. Si quiere eliminar el archivo de copia de seguridad después de transferir el archivo a un servidor externo, seleccione **Eliminar archivo de Administración de entrega de aplicaciones después de la transferencia**.

Configuración de instancia

January 26, 2024

Puede administrar las instancias descubiertas en NetScaler Console y configurar los ajustes de respaldo de las instancias.

Gestiona la configuración de la instancia

En **Configuración > Configuración global > Configuración de instancias > Administración de instancias**, puedes modificar las siguientes configuraciones de instancias:

- **Comunicación con las instancias : puede**elegir un canal de comunicación HTTP o HTTPS entre NetScaler Console y las instancias descubiertas.
- **Habilitar la descarga de certificados**: le permite descargar los certificados SSL de una instancia detectada.
- **Credenciales rápidas para iniciar sesión en la instancia :**al acceder a la instancia a través de la GUI de NetScaler Console, aparece la página de inicio de sesión de la instancia. Especifica sus credenciales de inicio de sesión para acceder a una instancia.

Configurar las opciones de copia de seguridad de instancia

En **Configuración > Configuración global > Configuración de instancia > Copia de seguridad** de instancias , puede configurar los ajustes de respaldo de las instancias de NetScaler descubiertas en NetScaler Console.

En **Configurar los ajustes de copia de seguridad**de la **instancia, seleccione Habilitar las copias**

- **Cantidad de archivos de copia de seguridad que se van a conservar**: especifique la cantidad de archivos de copia de seguridad que se van a conservar en la consola de NetScaler. Puede conservar hasta 3 archivos de backup por instancia de NetScaler. El valor predeterminado es 1 archivo de respaldo.
- **Configuración de programación de copias**de seguridad: puede programar una copia de seguridad de una instancia de dos maneras:

  - **Basado**en intervalos : se crea un archivo de respaldo en NetScaler Console una vez transcurrido el intervalo especificado. El intervalo de copia de seguridad predeterminado es de 12 horas.
  - **Basado**en el tiempo : especifique la hora en `hours:minutes`el formato a la que desea que NetScaler Console realice la copia de seguridad de la instancia.

- Configuración de**NetScaler**: Con esta opción, puede iniciar una copia de seguridad en función de la captura e incluir archivos de GeoDB en la copia de seguridad. Esta configuración se aplica a las instancias MPX, VPX, CPX y BLX.
  - **Realice una copia de seguridad de la instancia cuando reciba**la captura de NetScalerConfigSave : de forma predeterminada, NetScaler Console no crea un archivo de copia de seguridad cuando recibe la captura «NetScalerConfigSave». Sin embargo, puede habilitar la opción de crear un archivo de respaldo siempre que una instancia de NetScaler envíe una `NetScalerConfigSave`trampa a NetScaler Console.

    Se envía una instancia de NetScaler `NetScalerConfigSave` cada vez que se guarda la configuración de la instancia.

    Especifique el **retraso de Backup on trap** en minutos. Si la captura recibida `NetScalerConfigSave`persiste durante los minutos especificados en NetScaler Console, NetScaler Console realiza una copia de seguridad de la instancia.
  - **Incluir archivos**de GeoDB : de forma predeterminada, NetScaler Console no hace copias de seguridad de los archivos de GeoDatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.

- **Configuración de NetScaler SDX**: para hacer copias de seguridad de las instancias SDX, especifique el **tiempo de espera de la copia de seguridad** en minutos. Durante la copia de seguridad de una instancia SDX, la conexión entre NetScaler Console y SDX se mantiene durante el período especificado.

  Para archivos de respaldo SDX de gran tamaño, mantenga la conexión entre NetScaler Console y la instancia SDX durante un período más largo para garantizar la finalización del respaldo.

  > **Importante:**
  >
  > La copia de seguridad falla si se agota el tiempo de espera de la conexión.

- **Transferencia externa :**NetScaler Console le permite transferir los archivos de respaldo de la instancia de NetScaler a una ubicación externa:

  1. Especifique la dirección IP de la ubicación.
  2. Especifique el nombre de usuario y la contraseña del servidor externo al que quiere transferir los archivos de copia de seguridad.

3. Especifique el protocolo de transferencia y el número de puerto.
4. Especifique la ruta del directorio en la que debe almacenarse el archivo.
5. Si quiere eliminar el archivo de copia de seguridad después de transferir el archivo a un servidor externo, seleccione **Eliminar archivo de Administración de entrega de aplicaciones después de la transferencia**.

Configuraciones del sistema

January 26, 2024

Puede modificar el intervalo de mantenimiento del agente de NetScaler Console y la zona horaria del servidor de NetScaler Console.

Establecer el intervalo de mantenimiento-vivo del agente

El servidor y el agente de NetScaler Console mantienen la misma conexión TCP durante el intervalo de mantenimiento con vida especificado. Un agente usa esta conexión para enviar los datos de las instancias administradas al servidor de NetScaler Console.

1. Vaya a **Configuración > Configuración global**.
2. Seleccione **Agente y zona horaria** en **Configuraciones del sistema**.
3. En **Agente**, especifique el intervalo de mantenimiento activo entre 30 y 120 segundos.
4. Haga clic en **Guardar**.

Configurar la zona horaria de la consola NetScaler

Puede elegir la zona horaria en la que desea mostrar la hora en la página web, las notificaciones y los informes de NetScaler Console.

1. Vaya a **Configuración > Configuración global**.
2. Seleccione **Agente y zona horaria** en **Configuraciones del sistema**.
3. En **Zona** horaria , seleccione la zona horaria local o GMT para mostrar la hora en NetScaler Console.
4. Haga clic en **Guardar**.

suscripciones por correo electrónico

January 26, 2024

NetScaler Console envía notificaciones por correo electrónico a todos los usuarios inactivos y nuevos.

Los clientes inactivos reciben una notificación por correo electrónico si:

- Las instancias de NetScaler no están configuradas
- La licencia de arrendatario vence en menos de 30 días

> **Nota:**
>
> De forma predeterminada, todos los clientes inactivos reciben una notificación por correo electrónico.

Los nuevos clientes reciben un correo electrónico de NetScaler Console en el que se les invita a incorporar las instancias de NetScaler al servicio NetScaler Console, donde pueden gestionar y supervisar los eventos críticos en las instancias de NetScaler, solucionar problemas y automatizar tareas como la configuración de NetScaler.

citrix

Manage, monitor, troubleshoot, automate with Citrix ADM Service

Hello [redacted] Org ID - [redacted] Customer name - [redacted]

Congratulations on getting started with ADM service successfully! You can now onboard your ADC instances to ADM service to :

- Monitor critical events on your ADC instances through alerts.
- Automate mundane tasks like ADC configuration.
- Get rich analytics pertaining to ADC and Applications health, performance, and security.

All this is easy to set up and we have resources below to get you started.

Onboard ADC instances on ADM service in 3 quick steps

Start with this brief video to know the exact steps to onboard ADC instances to ADM service quickly. Learn more

Onboard ADC Instances

Sign in using Citrix Cloud/ My Citrix credentials

Your free ADM use cases resources

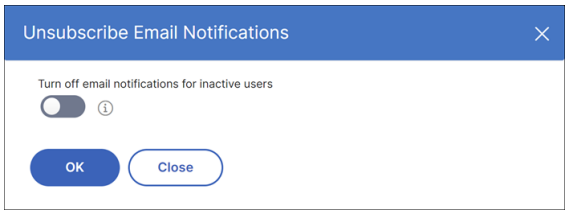
- Get bird's eye visibility into entire ADC infra and debug critical issues on your ADC instances.
- Manage the complete SSL cert lifecyle using Citrix ADM.
- Always stay on top of critical events with Citrix ADM ServiceNow integration.

Join ADM community

Notificaciones por correo electrónico de cancelación

Puede suscribirse o cancelar la suscripción a las notificaciones por correo electrónico que recibe del servicio NetScaler Console. Para cancelar la **suscripción a las notificaciones por correo** electrónico :

1. En NetScaler Console, vaya a Configuración > Configuración **global > Configuraciones del sistema** y, a continuación, haga clic en **Suscripciones de correo** electrónico. Aparece la ventana **Notificaciones de cancelación de suscripción por correo electrónico**.



> **Nota:**
>
> De forma predeterminada, el botón para desactivar las notificaciones por correo electrónico está desactivado y las notificaciones por correo electrónico están habilitadas para todos los usuarios inactivos.

2. En la ventana **Notificaciones de cancelación de suscripción por correo electrónico**, active el botón de conmutación. Haga clic en **Aceptar**.

Ya ha cancelado la suscripción a las notificaciones por correo electrónico y no recibirá ningún correo electrónico en las instancias de NetScaler integradas.

Habilite o inhabilite las funciones

July 17, 2024

Como administrador, puede habilitar o inhabilitar las siguientes funciones en la página **Configuración > Configuración global > 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 pasa a estar inactivo (estado INACTIVO) en el sitio, la consola de NetScaler redistribuye las instancias de NetScaler del agente inactivo con otros agentes activos. Para obtener más información, consulte Configurar los agentes del agente de NetScaler para la implementación en varios sitios.
- **Función de red de sondeo de entidades**: Una entidad es una directiva, un servidor virtual, un servicio o una acción adjunta a una instancia de NetScaler. De forma predeterminada,

NetScaler Console sondea automáticamente las entidades de funciones de red configuradas cada 60 minutos. Para obtener más información, consulte Descripción general de sondeos.

- **Copia de seguridad**de instancias: haga una copia de seguridad del estado actual de una instancia de NetScaler y, más adelante, utilice los archivos de la copia de seguridad para restaurar la instancia de NetScaler 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 Console se muestran en la página **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 Console proporciona una vista centralizada de los certificados SSL instalados en todas las instancias de NetScaler administradas. Para obtener más información, consulte Panel de control SSL.
- **Syslog**de instancias : puede supervisar los eventos de syslog generados en las instancias de NetScaler si ha configurado el dispositivo para redirigir todos los mensajes de syslog a NetScaler Console. Para obtener más información, consulta Configurar syslog en las instancias.

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 deshabilitada, el usuario no puede realizar las operaciones asociadas a esa función.

Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación

March 6, 2024

Además de la vista analítica existente de los eventos de la aplicación, puede configurar una directiva de acción para recibir notificaciones de eventos de la aplicación a través de Slack, Email, PagerDuty o ServiceNow. Los eventos de la aplicación incluyen problemas de rendimiento, infracciones de bots y WAF e infracciones de gráficos de servicio. Como administrador, mediante la directiva de acción, puede recibir notificaciones de eventos en tiempo real.

Con la directiva de acción, puede:

- Predefina ciertas condiciones para los eventos de la aplicación.
- Recibe notificaciones de los siguientes eventos a través de Slack, Email, PagerDuty y ServiceNow:

Categorías de eventos	Subcategorías de eventos	Eventos
Infracciones de seguridad	Todas las infracciones de seguridad	Todas las infracciones de bots (para obtener más información sobre la lista de infracciones de bots, consulta las categorías de infracciones). Todas las infracciones de WAF (infracciones de WAF SQL, infracciones de WAF XSS e infracciones de WAF inferir de XML)
	Todas las infracciones de seguridad por cliente	Infracciones de bots por cliente Infracciones de WAF por cliente

Categorías de eventos	Subcategorías de eventos	Eventos
		Nota: Para recibir la notificación de infracción del WAF, las transacciones de infracción mínimas deben ser del 20%. Por ejemplo, de cada 100 transacciones, un mínimo de 20 deben ser transacciones de infracción.
Rendimiento de las aplicaciones		Infracción de la puntuación
		Latencia de red del cliente
		Latencia de red del servidor
		Tiempo de procesamiento del servidor
		Tiempo de respuesta
		Solicitudes
		Ancho de banda
		Infracción del gráfico de
Uso de aplicaciones		Solicitudes por segundo
		Rendimiento
		Volumen de datos

Configurar una directiva de acción

1. Diríjase a **Configuración > Acción > Directivas de acción**.
2. Haga clic en **Agregar**.
3. En la página **Crear directiva de acción** :
    a) **Nombre de la directiva**: Proporcione el nombre de la directiva de su elección.
    b) **Activada**: Esta opción está seleccionada de forma predeterminada.
    c) Si **se produce el siguiente evento**, seleccione un evento de la lista.
    d) **Y se cumple la siguiente condición**: En la lista, seleccione para definir una condición para la que quiere recibir una notificación. Puedes hacer clic en **+** para agregar más condiciones.

Para eliminar una condición, haga clic en —.

Puede configurar la directiva de acciones mediante los siguientes operadores. Los operadores aparecen en función de las condiciones que seleccione.

Operador	Descripción
Igual a	Es igual a un valor definido
No igual a	No es igual a un valor definido
Mayor que	Mayor que un valor definido
Mayor o igual a	Mayor o igual a un valor definido
Menos de	Menor que un valor definido
Menor o igual a	Menor o igual a un valor definido
Contiene	Contiene el término o valor definido
Empieza con	Empieza con un término o valor definido
Termina con	Termina con un término o valor definido
IN	Permite seleccionar varios valores

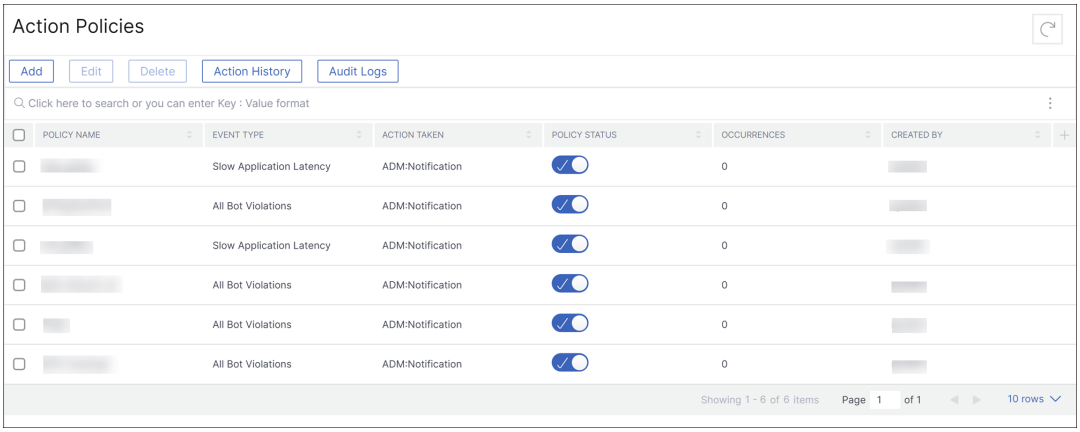
e) **A continuación, haga lo siguiente**: Seleccione **Notificar**. Tras seleccionar **Notificar**, aparece la opción Tipo de notificación.

f) **Tipo de notificación**: Seleccione el tipo de notificación Correo electrónico, Slack, PagerDuty o ServiceNow. Según el tipo de notificación que selecciones, aparecerá la opción correspondiente (lista de distribución, perfil de Slack, perfil de PagerDuty o perfil de ServiceNow). Seleccione un perfil de la lista.

   Si quiere crear un perfil nuevo, haga clic en **Agregar**.

g) Haga clic en **Crear directiva**.

   La directiva está configurada. Puede ver los detalles de la directiva configurada.



Después de configurar la directiva, puede seleccionarla y hacer clic en:

- **Modifique** para actualizar o cambiar la directiva de acción. Tras la actualización, haga clic en Actualizar directiva.
- **Eliminar** para eliminar la directiva de acción. Puede seleccionar varias directivas y hacer clic en **Eliminar** para eliminarlas.
- **Historial de acciones** para ver detalles como la hora, la acción realizada, el nombre de la directiva, el tipo de alerta y el mensaje de alerta.

La siguiente tabla describe los detalles de la configuración de la directiva de acción.

Nombre de la infracción	Condición	Descripción
Todas las infracciones de seguridad	IP de instancia	Dirección IP de la instancia de NetScaler. Seleccione la dirección IP de la lista.
	Recuento de infracciones	El recuento de infracciones por el que quiere recibir una notificación. Por ejemplo, si configuras el recuento de infracciones como inferior o igual a 10, recibirás una notificación si se reciben 10 o menos transacciones de infracción de bots.

Nombre de la infracción	Condición	Descripción
	Coeficiente de infracciones	Este valor indica las infracciones totales de transacciones específicas y el valor debe estar comprendido entre 0 y 1. Por ejemplo, de cada 100 transacciones, 20 son infracciones y, si quiere recibir una notificación de este tipo, debe introducir 0.2.
Todas las infracciones de bots	Perfil de bot	El nombre del perfil de bot que se usa para configurar la administración de bots en la instancia de NetScaler.
	IP de instancia	Dirección IP de la instancia de NetScaler. Seleccione la dirección IP de la lista.
	Recuento de infracciones	El recuento de infracciones por el que quiere recibir una notificación. Por ejemplo, si configuras el recuento de infracciones como inferior o igual a 10, recibirás una notificación si se reciben 10 o menos transacciones de infracción de bots.
	Coeficiente de infracciones	Este valor indica las infracciones totales de transacciones específicas y el valor debe estar comprendido entre 0 y 1. Por ejemplo, de cada 100 transacciones, 20 son infracciones y, si quiere recibir una notificación de este tipo, debe introducir 0.2.
Todas las infracciones de WAF, infracción de SQL de WAF, infracción de WAF XSS, infracción de WAF Infer XML	Perfil WAF	El nombre del perfil WAF que se usa para configurar los ajustes de seguridad de WAF en la instancia de NetScaler.

Nombre de la infracción	Condición	Descripción
	IP de instancia	Dirección IP de la instancia de NetScaler. Seleccione la dirección IP de la lista.
	Recuento de infracciones	El recuento de infracciones por el que quiere recibir una notificación. El requisito mínimo para que se notifiquen las infracciones de la WAF es del 20%.
	Coeficiente de infracciones	Este valor indica las infracciones totales de transacciones específicas y el valor debe estar comprendido entre 0 y 1. Por ejemplo, de cada 100 transacciones, 20 son transacciones de infracción de SQL de WAF y, si quiere recibir una notificación de este tipo, debe introducir 0.2.
Todas las infracciones de seguridad por cliente	Nombre de la aplicación	El nombre de la aplicación personalizada. Seleccione la aplicación de la lista. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia de NetScaler.
	IP de instancia	Dirección IP de la instancia de NetScaler. Seleccione la dirección IP de la lista.
	Client IP	La fuente de donde se origina el Bot. Especifique la dirección IP.
	Ataques totales	El total de ataques de los que quiere recibir una notificación.
	Request URL	La URL que quiere configurar para bloquear. Especifique la URL.

Nombre de la infracción	Condición	Descripción
	Nombre de vserver	Las aplicaciones asociadas configuradas para aplicaciones personalizadas. Seleccione la aplicación de la lista. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia de NetScaler.
Infracciones de bots por cliente	Nombre de la aplicación	El nombre de la aplicación personalizada. Seleccione la aplicación de la lista. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia de NetScaler.
	IP de instancia	Dirección IP de la instancia de NetScaler. Seleccione la dirección IP de la lista.
	Client IP	La fuente de donde se origina el Bot. Especifique la dirección IP.
	Ataques totales	El total de ataques de los que quiere recibir una notificación.
	Tipo de infracción	Seleccione la infracción del bot de la lista.
	Request URL	La URL que quiere configurar para bloquear. Especifique la URL.
	Nombre de vserver	Las aplicaciones asociadas configuradas para aplicaciones personalizadas. Seleccione la aplicación de la lista. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia de NetScaler.

Nombre de la infracción	Condición	Descripción
Infracciones de WAF por cliente	Nombre de la aplicación	El nombre de la aplicación personalizada. Seleccione la aplicación de la lista. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia de NetScaler.
	IP de instancia	Dirección IP de la instancia de NetScaler. Seleccione la dirección IP de la lista.
	Client IP	La fuente de donde se origina el Bot. Especifique la dirección IP.
	Ataques totales	El total de ataques de los que quiere recibir una notificación.
	Tipo de infracción	Seleccione la infracción del WAF de la lista.
	Request URL	La URL que quiere configurar para bloquear. Especifique la URL.
	Nombre de vserver	Las aplicaciones asociadas configuradas para aplicaciones personalizadas. Seleccione la aplicación de la lista. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia de NetScaler.
Infracción de la puntuación	Indicador de rendimiento	La aplicación puntúa los componentes y sus valores de umbral. Seleccione el componente de puntuación de la aplicación en la lista. Para obtener más información, consulte Seleccionar los componentes de App Score y establecer umbrales.

Nombre de la infracción	Condición	Descripción
	Recuento de infracciones	El recuento de infracciones por el que quiere recibir una notificación. Por ejemplo, si configuras un recuento de infracciones igual a 5 para el tiempo de respuesta, recibirás una notificación cuando se supere el umbral de tiempo de respuesta 5 veces.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Latencia de red del cliente	Latencia promedio de la red del cliente	Especifique el valor de latencia del cliente (del cliente a NetScaler) en milisegundos para el que desea recibir la notificación.
	Anomalías de latencia de la red del cliente	Especifique el recuento de anomalías de la latencia de red que desea recibir.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Latencia de red del servidor	Latencia promedio de la red de servidores	Especifique el valor de latencia del servidor (del servidor a NetScaler) en milisegundos para el que desea recibir la notificación.
	Anomalías de latencia de la red de servidores	Especifique el recuento de anomalías de la latencia de red que desea recibir.

Nombre de la infracción	Condición	Descripción
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Tiempo de respuesta	Tiempo promedio de respuesta	Especifique el valor (en milisegundos) para el que desea recibir la notificación.
	Anomalías en el tiempo promedio de respuesta	Especifique los recuentos de anomalías para los que desea recibir notificaciones.
	Nombre de la aplicación	Haga clic en Seleccionar **aplicaciones** para seleccionar las aplicaciones que desea recibir notificaciones. Si no selecciona ninguna aplicación, se aplicará en todas las aplicaciones.
Solicitudes	Total de solicitudes	Especifique el total de solicitudes para las que desea recibir notificaciones.
	Nombre de la aplicación	Haga clic en Seleccionar **aplicaciones** para seleccionar las aplicaciones que desea recibir notificaciones. Si no selecciona ninguna aplicación, se aplicará en todas las aplicaciones.
Ancho de banda	Ancho de banda total	Especifique el ancho de banda (MB) para el que desea recibir la notificación.
	Nombre de la aplicación	Haga clic en Seleccionar **aplicaciones** para seleccionar las aplicaciones que desea recibir notificaciones. Si no selecciona ninguna aplicación, se aplicará en todas las aplicaciones.

Nombre de la infracción	Condición	Descripción
Tiempo de procesamiento del servidor	Tiempo promedio de procesamiento del servidor	Especifique el valor de procesamiento del servidor (del servidor a NetScaler) en milisegundos para el que desea recibir la notificación.
	Anomalías del tiempo de procesamiento del servidor	Especifique el recuento de anomalías para el tiempo de procesamiento del servidor que desea recibir.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Infracción del gráfico de		Microservicios que infringen los umbrales configurados. Para obtener más información, consulte Configurar umbrales en el gráfico de servicios.
Solicitudes por segundo	Promedio de solicitudes por segundo	El número de solicitudes recibidas por segundo por la aplicación. Especifique el valor promedio para recibir la notificación.
	Anomalías promedio de solicitudes por segundo	Especifique el recuento promedio de anomalías para el que desea recibir una notificación. **Nota:** Si utiliza la condición AND para este evento, puede configurar el promedio de solicitudes por segundo y el nombre de la aplicación o el promedio de anomalías de solicitudes por segundo y el nombre de la aplicación.

Nombre de la infracción	Condición	Descripción
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Rendimiento	Promedio de rendimiento	El total de datos transmitidos durante un período específico. Especifique el valor promedio (en MB) para recibir la notificación.
	Anomalías promedio de rendimiento	Especifique el recuento promedio de anomalías para el que desea recibir una notificación. **Nota:** Si utiliza la condición AND para este evento, puede configurar el promedio de rendimiento y el nombre de la aplicación o la anomalía del promedio de rendimiento y el nombre de la aplicación.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Volumen de datos	Volumen total de datos	El total de datos que se van a transferir durante un período específico. Especifique el valor (en MB) para recibir la notificación.
	Anomalías en el volumen de datos	Especifique el recuento de anomalías para el que desea recibir una notificación.

Nombre de la infracción	Condición	Descripción
		Nota: Si utiliza la condición AND para este evento, puede configurar el volumen total de datos y el nombre de la aplicación o las anomalías del volumen de datos y el nombre de la aplicación.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.

Usa la barra de búsqueda

La barra de búsqueda permite filtrar los resultados. Al hacer clic en la barra de búsqueda, aparece una lista de sugerencias de búsqueda. Puede seleccionar el componente y filtrar los resultados en función de sus requisitos.

Utilice la opción de registros de auditoría

Haga clic en Registros de **auditoría** y seleccione la duración de la lista para ver las directivas de acción que se crean, modifican y eliminan durante el período seleccionado y, a continuación, haga clic en **Buscar** .

> **Nota**
>
> Se espera que las directivas de almacenamiento de datos cambien en las próximas versiones. Con estos cambios, no puede almacenar datos históricos después de que superen el límite de almacenamiento. Por ahora, se recomienda agregar más espacio de almacenamiento o mantener

> el almacenamiento dentro de los límites de derechos de licencia.

Utilice los registros de auditoría para administrar y monitorear su infraestructura

March 6, 2024

Puede usar NetScaler Console para realizar un seguimiento de todos los eventos de NetScaler Console y de los eventos de syslog generados en las instancias de NetScaler. 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 revisa, y NetScaler Console simplifica la forma de revisar los mensajes de registro.

Puede usar filtros para buscar mensajes de registro de auditoría y syslog de NetScaler Console. 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 NetScaler Console:

- Registros de auditoría relacionados con las instancias de NetScaler
- Registros de auditoría relacionados con NetScaler Console
- Registros de auditoría de aplicaciones

Registros de auditoría relacionados con las instancias de NetScaler

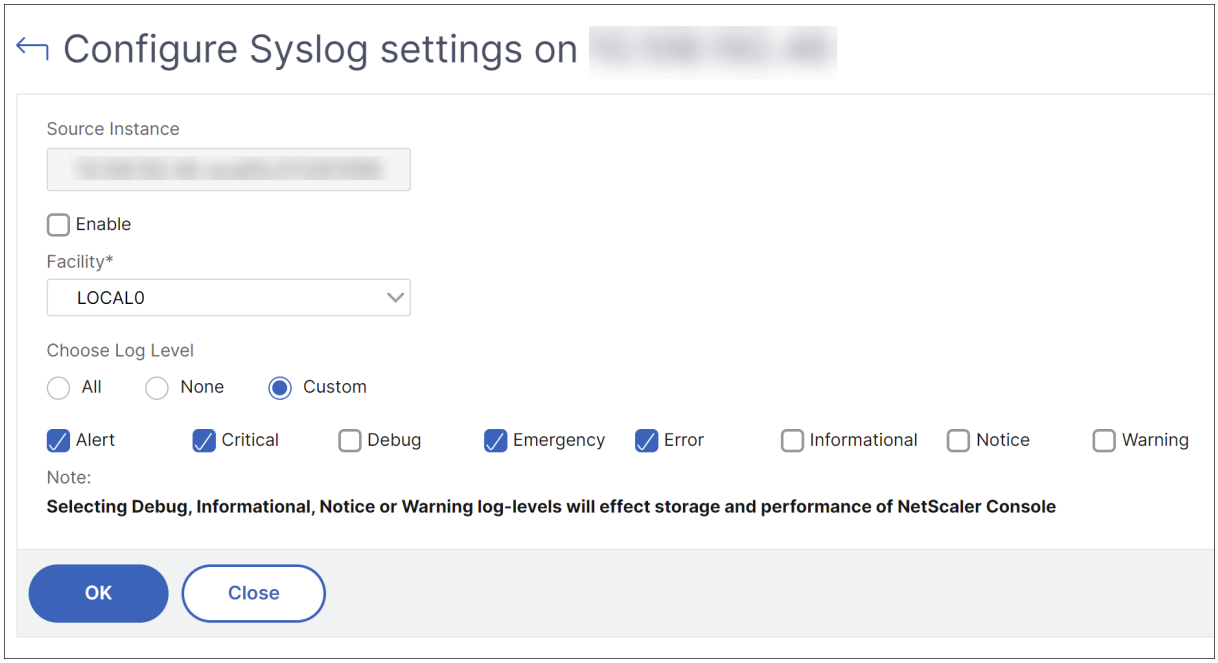
Antes de poder ver los mensajes de syslog relacionados con la instancia de NetScaler desde NetScaler Console, configure la consola de NetScaler como el servidor de syslog de la instancia de NetScaler. Una vez finalizada la configuración, todos los mensajes de syslog se redirigen de la instancia a NetScaler Console.

Configurar NetScaler Console como servidor syslog

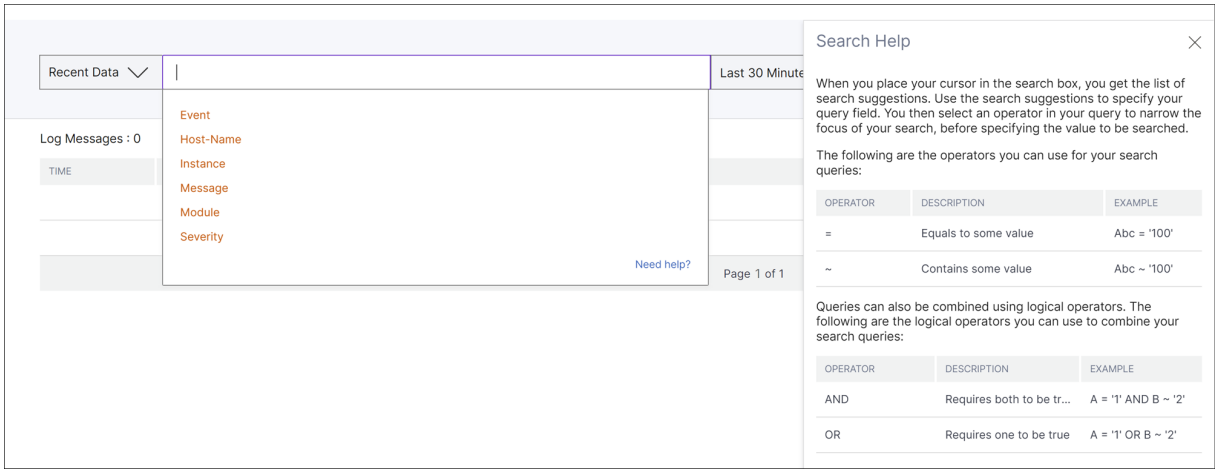
Siga estos pasos para configurar NetScaler Console como servidor syslog:

1. Desde la GUI de NetScaler Console, vaya a **Infraestructura > Instancias**.
2. Seleccione la instancia de NetScaler desde la que desea recopilar los mensajes de syslog y mostrarlos en NetScaler Console.

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 de syslog de la instancia de NetScaler y NetScaler Console comienza a recibir los mensajes de 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 informa-

ción, consulte Exportar mensajes de syslog.

Registros de auditoría relacionados con NetScaler Console

Basándose en reglas preconfiguradas, NetScaler Console genera mensajes de registro de auditoría para todos los eventos en curso, lo que le ayuda a supervisar el estado de su infraestructura. Para ver todos los mensajes del registro de auditoría presentes en la consola de NetScaler, vaya a **Configuración > Mensajes del registro de auditoría**.

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 de todas las aplicaciones de NetScaler Console o de una aplicación específica.

- Para ver todos los mensajes de registro de auditoría de todas las aplicaciones presentes en la consola de NetScaler, vaya a **Infraestructura > Funciones de red Auditoría**.
- Para ver los mensajes del registro de auditoría de cualquier aplicación específica en la consola de NetScaler, vaya a **Aplicaciones > Panel de control > Haga doble clic en el servidor virtual Registro de auditoría**.

> **Nota** Puede reenviar los mensajes de registro de auditoría de NetScaler Console a un servidor externo. Para obtener más información, consulte Ver información de auditoría.

Configurar la administración de direcciones IP (IPAM)

January 26, 2024

El IPAM de NetScaler Console le permite asignar y liberar automáticamente direcciones IP en las configuraciones gestionadas de NetScaler Console. Puede asignar direcciones IP desde redes o rangos de IP definidos mediante los siguientes proveedores de IP:

- Proveedor de IPAM integrado en NetScaler Console.
- Solución IPAM de Infoblox.

Puede usar el IPAM de NetScaler Console 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 rango de IP gestionado por NetScaler Console.

Agregar un proveedor de direcciones IP externo

NetScaler Console tiene un proveedor de IPAM integrado para administrar las IP y los rangos de IP. También puede usar un proveedor de direcciones IP externo para NetScaler Console.

> **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 Console:

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 va a usar en NetScaler Console.
   - **Proveedor**: Seleccione un proveedor IPAM de la lista.
   - **URL**: especifique la URL de la solución de IPAM que asigna direcciones IP en un entorno de consola de NetScaler. Asegúrese de especificar la dirección URL en el siguiente formato:

     ```
     1  https://<host name>
     ```

     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 Console admite Infoblox DDI como proveedor externo.

Puede usar el IPAM de NetScaler Console 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 IPAM de NetScaler Console con el proveedor de Infoblox, debe existir una red con el mismo rango de IP de CIDR en Infoblox.

Cuando crea una red de IPAM en la consola de NetScaler, solo registra el uso de la red de Infoblox en la consola de NetScaler. A continuación, la consola de NetScaler trabaja junto con Infoblox para administrar las direcciones IP asignadas desde la red. La red InfoBlox puede seguir utilizándose fuera de la consola de NetScaler.

Del mismo modo, si elimina la red IPAM de NetScaler Console, NetScaler Console anula el registro de la red de Infoblox. Esto significa que la consola de NetScaler ya no interactúa con Infoblox para la administración de direcciones IP en esa red.

API de Infoblox DDI El IPAM de NetScaler Console utiliza las siguientes API de Infoblox para realizar las acciones correspondientes:

- (/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

> **Nota:**
>
> - La IP y el puerto del servidor DNS, DHCP y administración de direcciones IP (DDI) de Infoblox deben estar accesibles desde la red pública para que el servicio de consola de NetScaler pueda llegar al servidor de Infoblox y conectarse al mismo.
> - La cuenta de usuario de Infoblox configurada en NetScaler Console debe tener los permisos necesarios para usar las API de 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 Console.

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 identificarla en NetScaler Console.
   - **Proveedor**: Seleccione el proveedor de la lista.

     Esta lista muestra los proveedores agregados a NetScaler Console.
   - **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:**
     >
     > El IPAM de NetScaler Console solo admite direcciones IPv4.

     Para el **intervalo de IP**, especifique el valor de red en el siguiente formato:

     ```
     <first-IP-address>-<last-IP-address>
     ```

     Ejemplo:

     ```
     10.0.0.20-10.0.0.100
     ```

     Para **CIDR**, especifique el valor de la red en el siguiente formato:

     ```
     <IP-address>/<subnet-mask>
     ```

     Ejemplo:

     ```
     10.70.124.0/24
     ```
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 de NetScaler Console 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.
   - **Identificador de recurso**: muestra el identificador de recurso exacto con un vínculo. 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 identificador de recurso.

> **Nota:**
>
> Si quiere liberar la dirección IP, seleccione la dirección IP que quiera liberar y haga clic en Liberar **direcciones IP asignadas**.

Artículos de procedimientos

August 8, 2024

Los «artículos prácticos» de NetScaler Console son artículos sencillos, relevantes y fáciles de implementar sobre las funciones disponibles con el servicio. Estos artículos contienen información sobre algunas de las funciones populares de NetScaler Console, como la administración de instancias, la administración de configuraciones, la administración de eventos, la administración de aplicaciones, StyleBooks y la administración de certificados.

Haga clic en un nombre de elemento de la tabla siguiente para ver la lista de artículos de procedimientos para esa característica.

TEMAS		
Administración de instancias	Administración de la configuración	Administración de certificados
StyleBooks	Gestión de eventos	

Administración de instancias

Cómo supervisar sitios distribuidos globalmente

Cómo administrar las particiones de administración de las instancias de NetScaler

Cómo añadir instancias a NetScaler Console

Cómo crear grupos de instancias en NetScaler Console

Cómo sondear instancias y entidades de NetScaler en NetScaler Console

Cómo configurar sitios para Geomaps en NetScaler Console

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

Cómo forzar que una instancia secundaria de NetScaler permanezca secundaria

Cómo cambiar una contraseña raíz de NetScaler MPX o VPX

Cómo cambiar una contraseña raíz de NetScaler SDX

Administración de la configuración

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

Cómo actualizar las instancias SDX de NetScaler mediante NetScaler Console

Cómo programar los trabajos creados mediante el uso de plantillas integradas en NetScaler Console

Cómo reprogramar los trabajos que se configuraron mediante plantillas integradas en NetScaler Console

Reutilizar trabajos de configuración de ejecución

Cómo actualizar las instancias de NetScaler mediante NetScaler Console

Cómo crear un trabajo de configuración en NetScaler Console

Cómo usar variables en los trabajos de configuración en NetScaler Console

Cómo usar las plantillas de configuración para crear plantillas de auditoría en NetScaler Console

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

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

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

Cómo usar la plantilla de configuración maestra en NetScaler Console

Administración de certificados

Cómo configurar una política empresarial en NetScaler Console

Cómo instalar certificados SSL en una instancia de NetScaler desde NetScaler Console

Cómo actualizar un certificado instalado desde NetScaler Console

Cómo vincular y desvincular certificados SSL mediante NetScaler Console

Cómo crear una solicitud de firma de certificado (CSR) mediante NetScaler Console

Cómo configurar las notificaciones de caducidad de los certificados SSL desde NetScaler Console

Cómo usar el panel de control SSL en NetScaler Console

StyleBooks

Cómo usar los StyleBooks predeterminados en NetScaler Console

Cómo crear sus propios StyleBooks

Cómo usar StyleBooks definidos por el usuario en NetScaler Console

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 cargar el certificado SSL y los archivos de claves de certificado en NetScaler Console

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

Cómo usar Microsoft ADFS Proxy StyleBook

Cómo utilizar Oracle e-Business StyleBook

Cómo usar el SSO Office 365 StyleBook

Cómo usar el SSO Google Apps StyleBook

Gestión de eventos

Cómo establecer la antigüedad de los eventos en NetScaler Console

Cómo programar un filtro de eventos mediante NetScaler Console

Cómo configurar notificaciones de correo electrónico repetidas para eventos desde NetScaler Console

Cómo suprimir eventos mediante NetScaler Console

Cómo utilizar el panel de eventos para supervisar eventos

Cómo crear reglas de eventos en NetScaler Console

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

Cómo ver el resumen de eventos en NetScaler Console

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

Cómo exportar mensajes de syslog con NetScaler Console

Cómo suprimir los mensajes de Syslog en NetScaler Console

Preguntas frecuentes

June 7, 2024

¿Cuántos agentes debo instalar?

La cantidad de agentes depende de la cantidad de instancias administradas en un centro de datos y del rendimiento total. Citrix recomienda instalar al menos un agente por cada centro de datos.

¿Cómo puedo instalar varios agentes?

Solo puede instalar un agente al iniciar sesión en el servicio por primera vez. Para agregar varios agentes, primero complete la configuración inicial y, a continuación, vaya a **Configuración> Agentes de instalación**.

¿El agente NetScaler es compatible con los procesadores AMD?

Sí.

¿Puedo realizar la transición de un agente integrado a un agente externo?

Sí, puede. Para obtener más información, consulte Transición de un agente integrado a un agente externo.

¿Cómo obtengo un nuevo código de activación si lo pierdo?

Si se está incorporando por primera vez, acceda a la GUI del servicio, vaya a la pantalla **Configurar agente** y haga clic en **Generar código de activación**.

Al intentar instalar un segundo agente, para generar un nuevo código de activación, vaya a **Infraestructura > Instancias > Agentes > Generar código de activación.**

¿Cómo inicio sesión en la máquina virtual del agente? ¿Cuáles son las credenciales predeterminadas?

Si el agente está instalado en un hipervisor o en una nube de Microsoft Azure, las credenciales de inicio de sesión predeterminadas para el agente son `nsrecover`/`nsroot`, lo que abre la línea de comandos del intérprete de comandos del agente.

Si su agente está instalado en AWS, las credenciales predeterminadas para iniciar sesión en el agente son `nsrecover`/`instance id`.

¿Cuáles son los requisitos de recursos para instalar un agente en un hipervisor local?

32 GB de RAM, 8 CPU virtual, 500 GB de almacenamiento, 1 interfaz de red virtual, rendimiento de 1 Gbps

¿Es necesario asignar un disco adicional al agente durante el aprovisionamiento?

No, no tiene que agregar un disco adicional. El agente solo se usa como intermediario entre NetScaler Console y las instancias del centro de datos empresarial o de la nube. No almacena datos de inventario o análisis que necesitarían un disco adicional.

¿Puedo reutilizar mi código de activación con varios agentes?

No, no puede.

¿Cómo puedo volver a ejecutar la configuración de red si he introducido un valor incorrecto?

Acceda a la consola del agente en el hipervisor, inicie sesión en el símbolo del shell utilizando las credenciales nsrecover/nsroot y, a continuación, ejecute el comando `networkconfig`.

¿Qué hago si falla el registro de mi agente?

Compruebe que:

- Su agente tiene acceso a Internet (configure DNS).
- Ha copiado correctamente el código de activación.
- Ha introducido la URL del servicio correctamente.
- Tiene abiertos los puertos necesarios.

El registro se ha realizado correctamente, pero ¿cómo puedo saber si el agente funciona correctamente?

Una vez que el agente se haya registrado correctamente, acceda a NetScaler Console y navegue hasta la pantalla **Configurar agente**. Puede ver el agente descubierto en la pantalla. Si el agente está funcionando bien, aparece un icono verde. Si no se está ejecutando, aparece un icono rojo.

¿Cómo puedo conectar los agentes a NetScaler Console mediante un servidor proxy?

Puede conectar los agentes a NetScaler Console mediante un servidor proxy. El script está disponible en la carpeta `/mps` del agente. Los agentes reenvían todos sus datos al servidor proxy, que luego los envía a NetScaler Console a través de Internet.

Para reenviar datos mediante el servidor proxy, escriba los detalles del servidor proxy en el agente mediante el siguiente script: `proxy_input.py`y siga las instrucciones proporcionadas por el script para introducir más información. El agente obtiene esta información mientras se conecta a NetScaler Console mediante el servidor proxy.

Puede autenticar su servidor proxy proporcionando su nombre de usuario y contraseña. Cuando el agente envía los datos, el servidor proxy autentica las credenciales de usuario antes de reenviarlas a NetScaler Console.

Para obtener más información, consulte NetScaler Console como servidor proxy de API .

> **Nota** NetScaler Console admite servidores proxy con la autenticación básica habilitada. NetScaler Console también admite servidores proxy en los que la autenticación está deshabilitada.

No veo mis informes de Analytics

Obtenga información sobre sus servidores virtuales para ver los informes de análisis. Para obtener más información, consulte Enabling Analytics.

¿Qué versiones de las instancias de NetScaler se admiten en NetScaler Console?

Para las funciones de administración y supervisión, se admiten las instancias de NetScaler que ejecutan la versión 10.5 y versiones posteriores. Algunas funciones solo son compatibles con determinadas versiones de NetScaler. Para obtener más información, consulte Requisitos del sistema.

¿Cómo puedo exportar los informes del panel en NetScaler Console?

Para exportar el informe de cualquier panel de NetScaler Console, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
   El informe se descarga en su sistema.
2. Seleccione **Programar Informe** para configurar programas para generar y exportar informes 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.

   a) **Periodicidad**: Seleccione **Diario**, **Semanal** o **Mensual** en el cuadro de lista desplegable.

   > **Nota**
   >
   > - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
   > - Si selecciona **Periodicidad mensual**, asegúrese de introducir todos los días en los que quiere que se programe el informe separados por comas.

   b) **Tiempo de periodicidad** : introduzca la hora como `Hour : Minute` en formato de 24 horas.

   c) **Correo electrónico**: Active la casilla de verificación y, a continuación, seleccione el perfil en el cuadro de lista desplegable, o haga clic en **Agregar** para crear un perfil de correo electrónico.

   d) **Slack**: selecciona la casilla de verificación y, a continuación, selecciona el perfil en el cuadro de lista desplegable o haga clic en **Agregar** 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.

¿Qué hace la habilitación de mediciones del lado del cliente?

Con las mediciones del lado del cliente habilitadas, NetScaler Console captura las métricas del tiempo de carga y renderizado de las páginas HTML mediante la inyección de HTML. Mediante estas métricas, los administradores pueden identificar problemas de latencia L7.

¿El tráfico SSL del agente al servicio de NetScaler Console pasa por una inspección SSL?

Le recomendamos que omita la inspección SSL para el tráfico SSL del servicio del agente a NetScaler Console.