Citrix Application Delivery Management

Machine translated content

Disclaimer

Contents

Información general

November 16, 2022

Citrix Application Delivery and Management (Citrix ADM) es una solución basada en la web para administrar todas las implementaciones de Citrix, que incluyen Citrix ADC MPX, Citrix ADC VPX, Citrix ADC SDX, Citrix ADC CPX, Citrix ADC BLX, Citrix Gateway y Citrix Secure Web Gateway, que se implementan localmente 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. Citrix ADM proporciona todas las capacidades necesarias para configurar, implementar y administrar rápidamente la entrega de aplicaciones en las implementaciones de Citrix ADC y con análisis detallados del estado, el rendimiento y la seguridad de las aplicaciones.

Citrix ADM ofrece las siguientes ventajas:

- **Ágil**: Fácil de operar, actualizar y consumir. El modelo de servicio de Citrix ADM está disponible en la nube, lo que facilita el funcionamiento, la actualización y el uso de las funciones que proporciona Citrix ADM. La frecuencia de las actualizaciones, combinada con la función de actualización automatizada, mejora rápidamente la implementación de Citrix ADC.
- **Tiempo de obtención de valor** más rápido: Logro de objetivos empresariales más rápido. A diferencia de la implementación local tradicional, puede usar su Citrix ADM 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 Citrix ADM, puede administrar y supervisar los ADC de Citrix que se encuentran en varios tipos de implementaciones. Tiene una administración integral para los ADC de Citrix implementados en las instalaciones y en la nube.
- **Eficiencia operativa**: Forma optimizada y automatizada de lograr una mayor productividad operativa. Con Citrix ADM, sus costos operativos se reducen al ahorrar tiempo, dinero y recursos en el mantenimiento y la actualización de las implementaciones de hardware tradicionales.

Cómo funciona Citrix ADM

Citrix ADM 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 el Citrix ADM y las instancias administradas de su centro de datos. El agente recopila datos de las instancias administradas de la red y los envía al Citrix ADM.

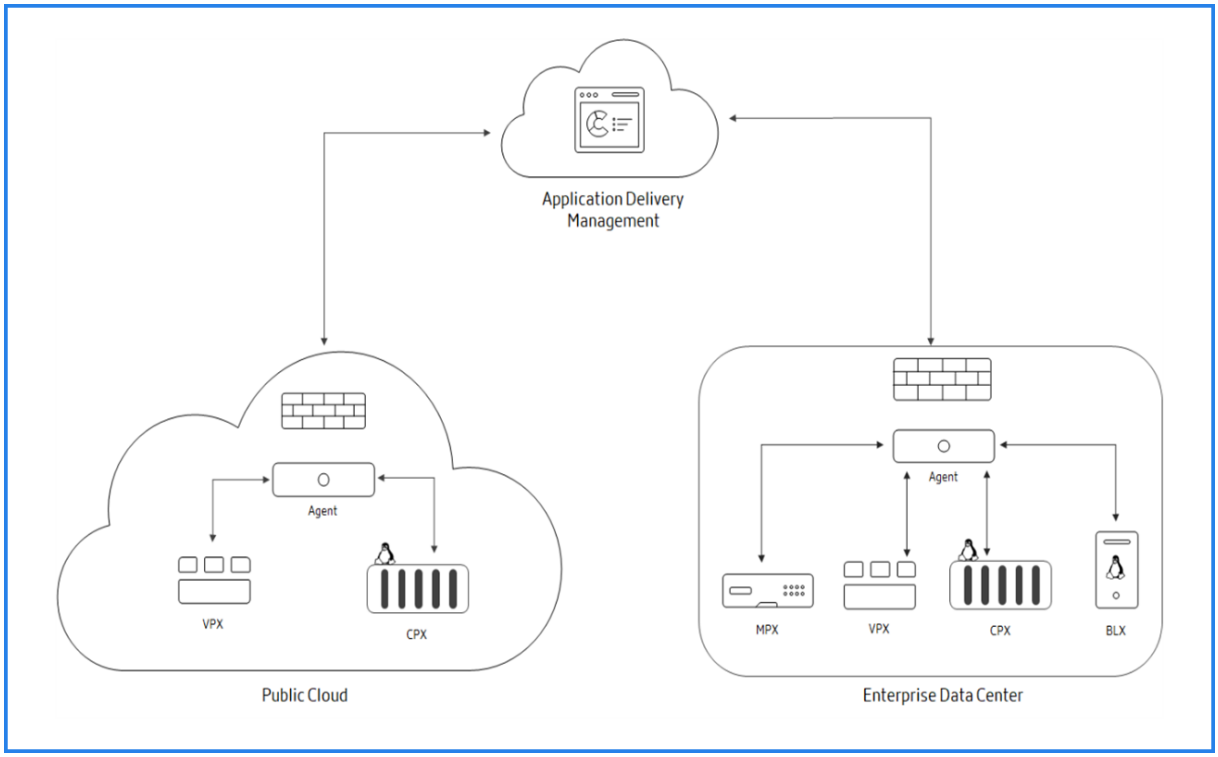
Cuando agrega una instancia a Citrix ADM, se agrega implícitamente como destino de captura y recopila el inventario de la instancia.

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.

Citrix ADM sondea periódicamente las instancias administradas para recopilar información. Para obtener más información, consulte el documento de gobernanza de datos .

La siguiente imagen ilustra la comunicación entre el servicio, los agentes y las instancias:



Funciones y soluciones

December 2, 2022

Este documento describe las funciones que admite el Citrix ADM.

Análisis y administración de aplicaciones

La función de análisis y administración de aplicaciones de Citrix ADM 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 seguridad clave, como infracciones de seguridad, infracciones de firmas, índices de amenazas. El panel de seguridad de aplicaciones también muestra información relacionada con los ataques, como ataques SYN, ataques de ventanas pequeñas y ataques de inundación DNS para las instancias detectadas de Citrix ADC.
- 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 Citrix ADC. 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 Citrix ADC para sus aplicaciones. Un StyleBook es una plantilla que puede utilizar para crear y administrar configuraciones de Citrix ADC. Puede crear un StyleBook para configurar una función específica de Citrix ADC, 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 Citrix ADC, Citrix Gateway y Citrix Secure Web Gateway.

Gestión de eventos

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

- Creación de reglas de eventos

- Uso de Citrix ADM para exportar mensajes de syslog

Administración de certificados

Citrix ADM 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

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

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: le permite supervisar los cambios en una configuración específica.

Gestión de licencias

Le permite administrar las licencias de Citrix ADC mediante la configuración de Citrix ADM como administrador de licencias.

- Capacidad agrupada de Citrix ADC: un grupo de licencias común desde el que la instancia de Citrix ADC 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 de Citrix ADC VPX: Citrix ADM asigna licencias a las instancias de Citrix ADC VPX a pedido. Una instancia de Citrix ADC VPX puede retirar la licencia del Citrix ADM cuando se aprovisiona una instancia de Citrix ADC VPX, o volver a registrar su licencia en Citrix ADM cuando se quita o destruye una instancia.

Informes de red

Puede optimizar el uso de los recursos mediante la supervisión de los informes de red en Citrix ADM.

Análisis

Proporciona una forma fácil y escalable de analizar los diversos conocimientos de los datos de las instancias de Citrix ADC 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 Citrix ADC. 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 Citrix ADC al proporcionar una supervisión integrada y en tiempo real de las aplicaciones. Web Insight procesa los datos de Citrix ADC 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 Citrix ADC al proporcionar una supervisión histórica, en tiempo real e integrada de las transacciones web. SSL Insight procesa los datos de Citrix ADC mediante un algoritmo de aproximación. Proporciona los 1000 registros principales de las métricas relacionadas con las transacciones web de su empresa.

Control de acceso basado en 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.

Suscripciones

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 recursos limitados de Citrix ADM. Para obtener más información, consulte Administrar los recursos de Citrix ADM mediante una cuenta Express.

Las siguientes funciones de Citrix ADM no están disponibles actualmente:

- Implementación

  - Migración de Citrix Insight Center a Citrix ADM
  - Integración de Citrix ADM con Citrix Virtual Desktop Director
- Análisis: TCP Insight y Video Insight
- Configuración limitada del sistema
- Orchestration
  - Integración con OpenStack y VMware NSX Manager
  - Automatización de Citrix ADC en el modo híbrido de Cisco ACI
  - Container Orchestration: Integración con Mesos/Marathon y Kubernetes

Notas de la versión

January 18, 2023

Las notas de la versión de Citrix Application Delivery Management (Citrix ADM) describen las nuevas funciones, las mejoras de las funciones existentes, los problemas solucionados y los problemas conocidos disponibles en una versión de servicio.

Para obtener más información, consulte:

- Novedades
- Versiones anteriores

De forma predeterminada, los agentes de Citrix Application Delivery Manager (ADM) se actualizan automáticamente a la versión más reciente de Citrix ADM. 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

February 27, 2023

07 de febrero de 2023

Análisis

Las violaciones de seguridad muestran las etiquetas OWASP

En la GUI de Citrix ADM, las infracciones de seguridad ahora muestran las 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.

Selecciona 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 puedes utilizarlos para obtener más información sobre la infracción en el sitio web de OWASP.

[NSADM-92999]

Gestión 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** > **Configuración global** > **Configuraciones del sistema** > **Agente y zona horaria > Agente** y marque la casilla **Quitar 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 mostrar de nuevo el campo **Contraseña actual**, desmarque la casilla **Quitar 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 Citrix ADM 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

Los siguientes 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 Citrix ADM.

[NSHELP-33264]

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 Citrix ADC SDX desde la GUI de Citrix ADM. Para ello, vaya a **Infraestructura > Instancias > Citrix ADC > SDX > Seleccione Acción > Configurar SNMP**.

[NSHELP-33852]

10 de enero de 2023

Gestión 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 Citrix ADM, se presenta una nueva opción **Tarea**, donde ahora puede ver las recomendaciones basadas en su suscripción y su 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
- Ve a **Tareas archivadas** y utiliza las herramientas guiadas (consejos para necesidades recurrentes)

Estas recomendaciones garantizan que utilice todas las capacidades de Citrix ADM y permiten el descubrimiento del producto 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`type: ipnetwork` atributo, la GUI de configuración de StyleBook ahora muestra el botón **Netmask** Length junto al campo de 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

Gestión y supervisión

Función para la identificación y la corrección de CVE-2021-27518

El aviso de seguridad de Citrix ADM ahora permite identificar y corregir CVE-2021-27518.

La identificación de CVE-22/27518 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-2021-27518, 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-2021-27518 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

Citrix ADM ya no ofrecerá **Advanced Security Analytics** para las instancias de ADC con licencia Premium. Con esta actualización, en la GUI de Citrix ADM:

- 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.

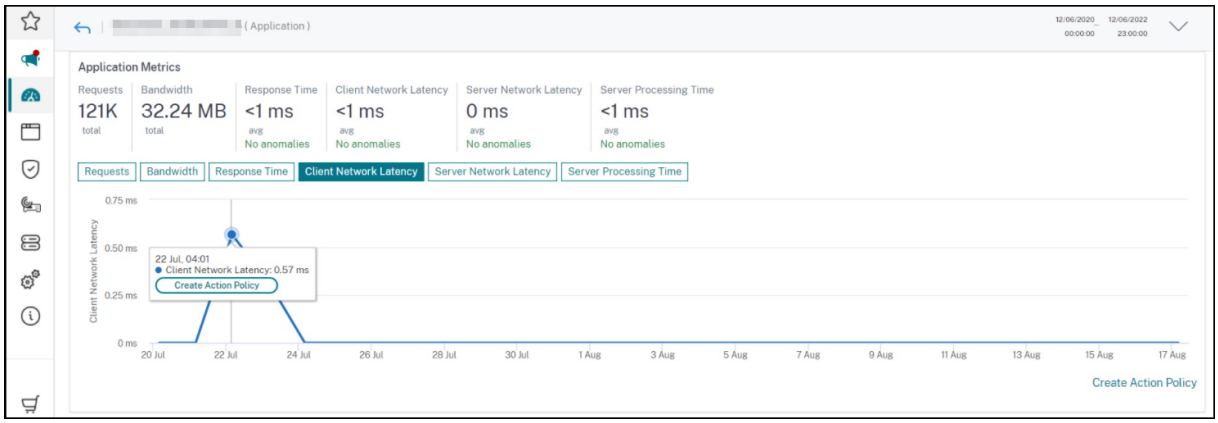
[NSADM-92342]

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 cliente**
- **Latencia de la red**
- **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 Citrix ADM

Ahora puede ver la información de caducidad de las licencias Z de las instancias MPX y SDX en Citrix ADM. Para ello, vaya a **Infraestructura > Licencias agrupadas > Capacidad agrupada > Licencias Z.**

[NSADM-80202]

Gestión y supervisión

Funciones descontinuadas de SD-WAN y HAProxy en Citrix ADM

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

[NSADM-90549]

Mejoras en la actualización de SDX: Función para seleccionar imágenes SDX de la biblioteca de recursos

Cuando programa un trabajo de mantenimiento para actualizar una instancia SDX en Citrix ADM, ahora tiene la opción de seleccionar una de las bibliotecas de imágenes necesarias para la actualización. Vaya a **Infraestructura > Actualizar trabajos > Crear trabajo**, seleccione **Actualizar Citrix ADC SDX**y haga clic en **Continuar** para actualizar una instancia de SDX.

[NSADM-88832]

Problemas resueltos

Los problemas que se abordan en Build el 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 Citrix antes de 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 Citrix ADM con New Relic para ver los análisis de las infracciones relacionadas con el WAF, los bots y 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

Citrix ADM 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 puedes ver el bot, el WAF y otros eventos basados en el comportamiento en tu 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. Citrix ADM realiza las comprobaciones necesarias y actualiza el grupo Autoscale.

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

[NSADM-84955]

Gestión 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 **unidades criptográficas asimétricas** y las **unidades criptográficas simétricas** ahora son campos modificables en la GUI de Citrix ADM. Puede introducir el número de ASUS y SCU al aprovisionar una instancia de Citrix ADC VPX en el dispositivo Citrix ADC SDX con chips Intel Coleto (COL).

Vaya a **Infraestructura** > **Instancias** > **Citrix ADC** y, en la ficha **SDX**, seleccione una instancia SDX en la que quiera aprovisionar una instancia de Citrix ADC 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

Gestión y supervisión

Identificación y corrección de los CVE-2022-27510, CVE-2022-27513 y CVE-2022-27516

El aviso de seguridad de Citrix ADM ahora permite identificar y corregir 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 Citrix ADM solo permite identificar y corregir 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 Configurar la zona horaria de Citrix ADM.

[NSADM-88417]

Problemas resueltos

Los problemas que se abordan en Build el 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
- State
- Tipo

[NSHELP-32807]

Al configurar una segunda NIC para aislar el acceso de administración a Citrix ADM, a la segunda dirección IP de la 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 Autoscale que se conecta a AWS necesita permisos de IAM adicionales. Actualmente, el servicio Citrix ADM invalida 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 Citrix ADM, 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 Citrix ADM.

[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]

Citrix ADM reprograma los trabajos cuando se producen imprevistos

A veces, al ejecutar un trabajo de configuración o actualización, es posible que te enfrentes a eventos como los siguientes:

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

En tales casos, Citrix ADM reprograma los trabajos para la hora siguiente.

Anteriormente, Citrix ADM 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]

Gestión 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 Citrix ADC BLX

Al crear un paquete de configuración, ahora puede elegir instancias de Citrix ADC BLX como instancias de destino. Anteriormente, StyleBooks admitía instancias Citrix ADC 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 Citrix ADM con sus versiones mejoradas:

Nombre	Versión
libra	2.0
lb-mon	2.0

[NSADM-80663]

Problemas resueltos

Los problemas que se abordan en Build el 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 Citrix antes de ADM.

  [NSHELP-32556]

29 de agosto de 2022

Habilitar automáticamente Gateway Insight y Account Takeover para Citrix Gateway

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

- Ataques de apropiación de cuentas para Citrix Gateway en **Seguridad > Infracciones de seguridad**. La disponibilidad de la página de inicio de sesión de Citrix 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 Citrix Gateway. Para obtener más información, consulte Adquisición de cuentas para Citrix Gateway.
- Problemas relacionados con los servidores virtuales Citrix 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 Citrix Gateway se lanzará a los clientes por fases.
>
> - Su Citrix ADM debe tener uno o más agentes Citrix ADM externos configurados y tener uno o más dispositivos Premium o Advanced Gateway.
> - Una vez que se publique esta funcionalidad en su Citrix ADM, todos los servidores virtuales

de Citrix Gateway con licencia existentes y los siguientes servidores virtuales de Citrix Gateway con licencia se habilitarán automáticamente con Gateway Insight y Account Takeover para Citrix Gateway.

- Para todos los servidores virtuales de Citrix 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 Citrix Gateway y haga clic en **Modificar análisis**.
  4. Deseleccione la opción **Gateway Insight** y haga clic en **Guardar**.
- La **adquisición de cuentas para Citrix 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 añadiendo o eliminando los widgets necesarios en cada categoría.

[NSADM-86337]

Elige un país de la región seleccionada

Cuando inicie sesión en el servicio Citrix ADM por primera vez, ahora puede elegir un país que 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 Citrix ADC SDX desde la GUI de ADM. Vaya a la ficha **Infraestructura > Instancias > Citrix ADC > 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 Citrix ADC.

[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 Citrix ADM. 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 Citrix ADM.

[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]

Gestión 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 Citrix 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

Gestión y supervisión

Soporte para la identificación y corrección del CVE-2022-27509

El asesoramiento de seguridad de Citrix ADM 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/Modificar) para los trabajos de actualización y aplicar la directiva a los usuarios de Citrix ADM. 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 las directivas de acceso en Citrix ADM.

[NSADM-82494]

Soporte para la auditoría de configuración en instancias de Citrix ADC 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 Citrix ADC 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 Citrix ADM Service, 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 **Application Dashboard**, 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]

Gestión y supervisión

Navegadores compatibles para acceder a la GUI Citrix ADM

Ahora solo se puede acceder a la GUI de Citrix ADM desde las siguientes versiones de navegador 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 Citrix ADM y solucione los problemas mediante el demonio de autorreparación

El agente Citrix ADM ahora supervisa los recursos del sistema (CPU, memoria y disco) ejecutando automáticamente el demonio de autorreparación 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]

Gestión 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 Citrix ADC

En **Infraestructura > Trabajos de actualización**, ahora puede crear un trabajo para actualizar las instancias BLX de Citrix ADC. 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 Citrix ADM 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 Citrix ADM se envían a Splunk inmediatamente.

Para obtener más información, consulte Integración con Splunk.

[NSADM-84529]

Mejoras en el motor de aprendizaje WAF

En Citrix ADM, 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 Citrix ADC 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

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 asesoramiento de seguridad de Citrix ADM ahora permite identificar y corregir dos nuevos 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 > Citrix ADC**, 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

Gestión 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**
- **La función de persistencia**

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]

Soporte de infracción del navegador Headless en caso de infracción

En **Seguridad > Infracciones de seguridad > Descripción general de la aplicación**, en **Bot**, ahora puede ver los detalles de las **infracciones de Headless Brow**. 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]

Gestión y supervisión

El CVE-2022-21827 no está incluido en el ámbito del aviso de seguridad de Citrix ADM

El CVE-2022-21827 afecta al complemento de Citrix Gateway para las versiones compatibles con Windows anteriores a la 21.9.1.2.

Citrix ADM no admite la detección y la corrección de las vulnerabilidades que afectan al complemento de Citrix Gateway para Windows. Además, las vulnerabilidades de los complementos de Citrix 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 Citrix Gateway para Windows implementada en el cliente.

Como resultado, la detección y la corrección de esta vulnerabilidad están fuera del alcance del asesoramiento de seguridad de Citrix ADM.

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 Citrix ADM. 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 paquetes de configuración

Cuando se actualiza un certificado SSL en el almacén de certificados Citrix ADM, 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/aplicación/puerta de enlace de ADC 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]

Gestión 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

Citrix ADM 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

Cuando quiera incorporar una instancia de ADC en Citrix ADM mediante la opción de agente integrado predeterminada, puede realizar una ejecución de prueba para asegurarse de que la instancia de ADC esté lista para integrarse. Para obtener más información, consulte Probar la preparación para la incorporación de las instancias de ADC.

[NSADM-80502]

01 de marzo de 2022

Gestión y supervisión

Invitar usuarios o grupos a ADM desde Azure AD

Como superadministrador, ahora puede invitar usuarios o grupos a Citrix ADM desde el Azure AD conectado a Citrix ADM. 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 Citrix ADM 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 Citrix ADM 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]

Deshabilitar los escaneos personalizados de Security Advisory

La interfaz de usuario de Citrix 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`
display-name: `Example App StyleBook`
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,` />'
<!--NeedCopy-->
```

[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

Gestión 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 Citrix ADC.

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**

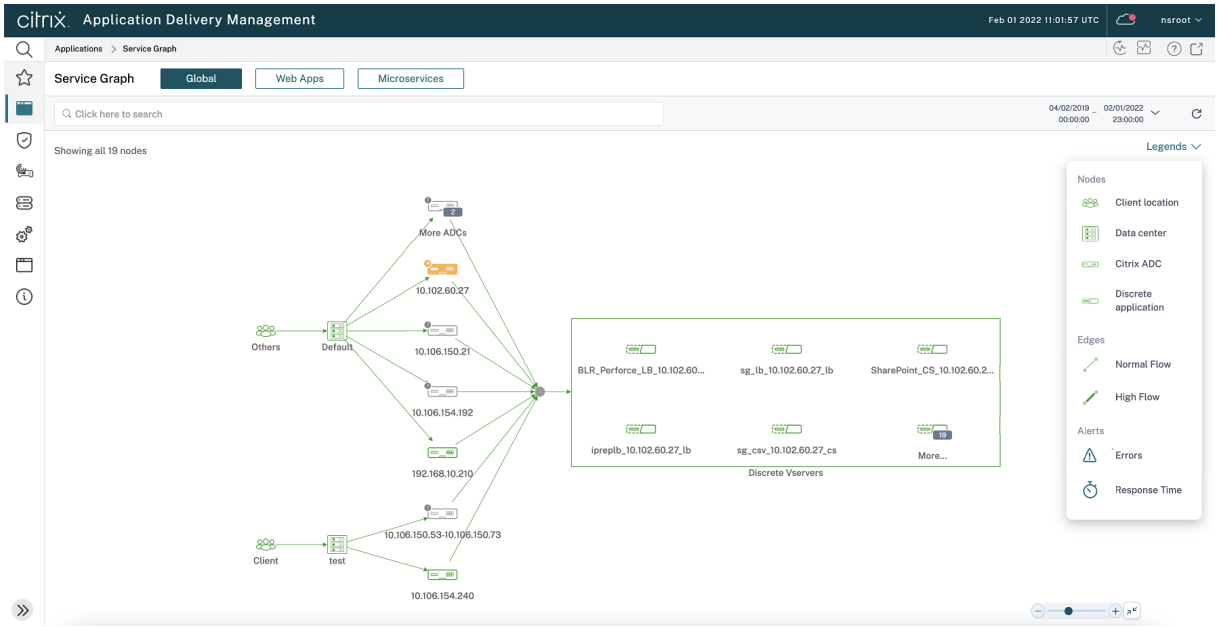
Para obtener más información, consulte Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación.

[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 de bajo nivel basado en ADM Service Connect, recibirá correos electrónicos iniciados por el producto del servicio Citrix ADM. 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 Citrix ADM y reciba alertas para la verificación de terminales

Citrix ADM ahora realiza una verificación de diagnóstico periódica (cada una hora) para el agente Citrix ADM 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 desplegado en una instancia de ADC puede tener diferencias con respecto a su estado desplegado. 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 Citrix ADM le ayuda a utilizar 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 Citrix ADM, puede utilizar cualquier instancia de ADC administrada como fuente de datos para la entrada de una configuración de StyleBook. En Citrix ADM, puede usar las instancias de 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
<!--NeedCopy-->
```

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

[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 > Citrix ADC** 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 Citrix ADC 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 Citrix ADM que les guiará hasta el servicio **Onboard to 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 Citrix ADC 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 monitoreo 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 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:

```
"and", "false", "in", "not", "true", "or"
<!--NeedCopy-->
```


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
<!--NeedCopy-->
```

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

January 31, 2023

Citrix Application Delivery Management (Citrix ADM) tiene los siguientes problemas conocidos:

Infraestructura

Al aprovisionar una instancia de Citrix ADC VPX en un Citrix ADC SDX con el nombre de una instancia VPX eliminada anteriormente, aparece un mensaje de error.

[NSADM-92705]

Gestión y supervisión

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

[NSADM-88273]

Introducción

December 2, 2022

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

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

Paso 1: Inscríbase en Citrix Cloud

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

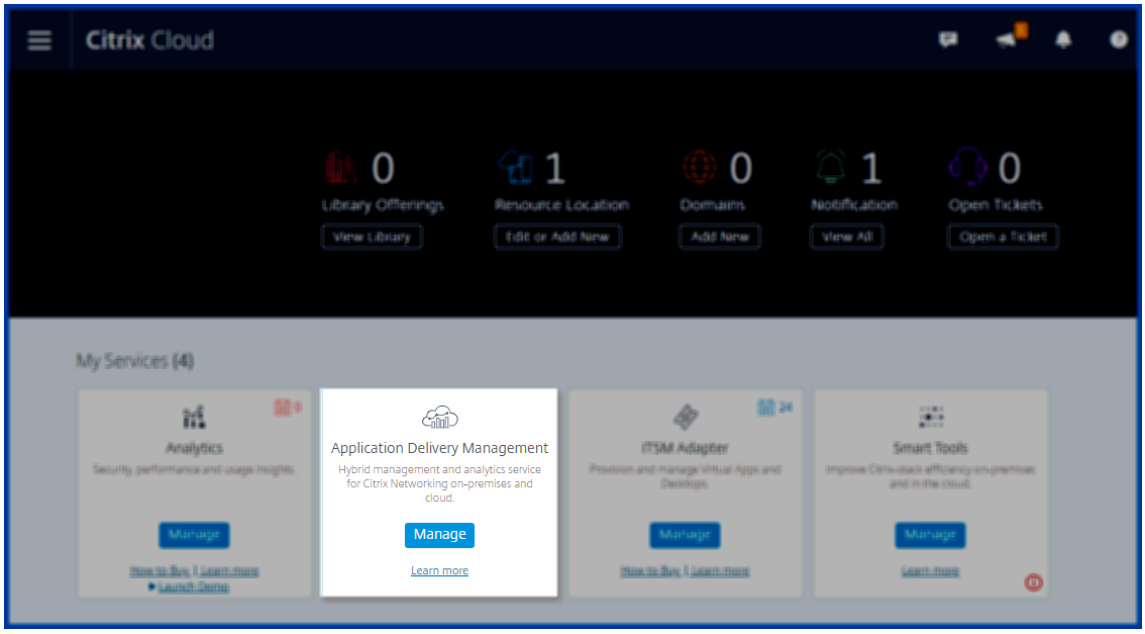
Paso 2: Administre Citrix ADM con una cuenta Express

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

1. Vaya a la sección **Servicios disponibles** .

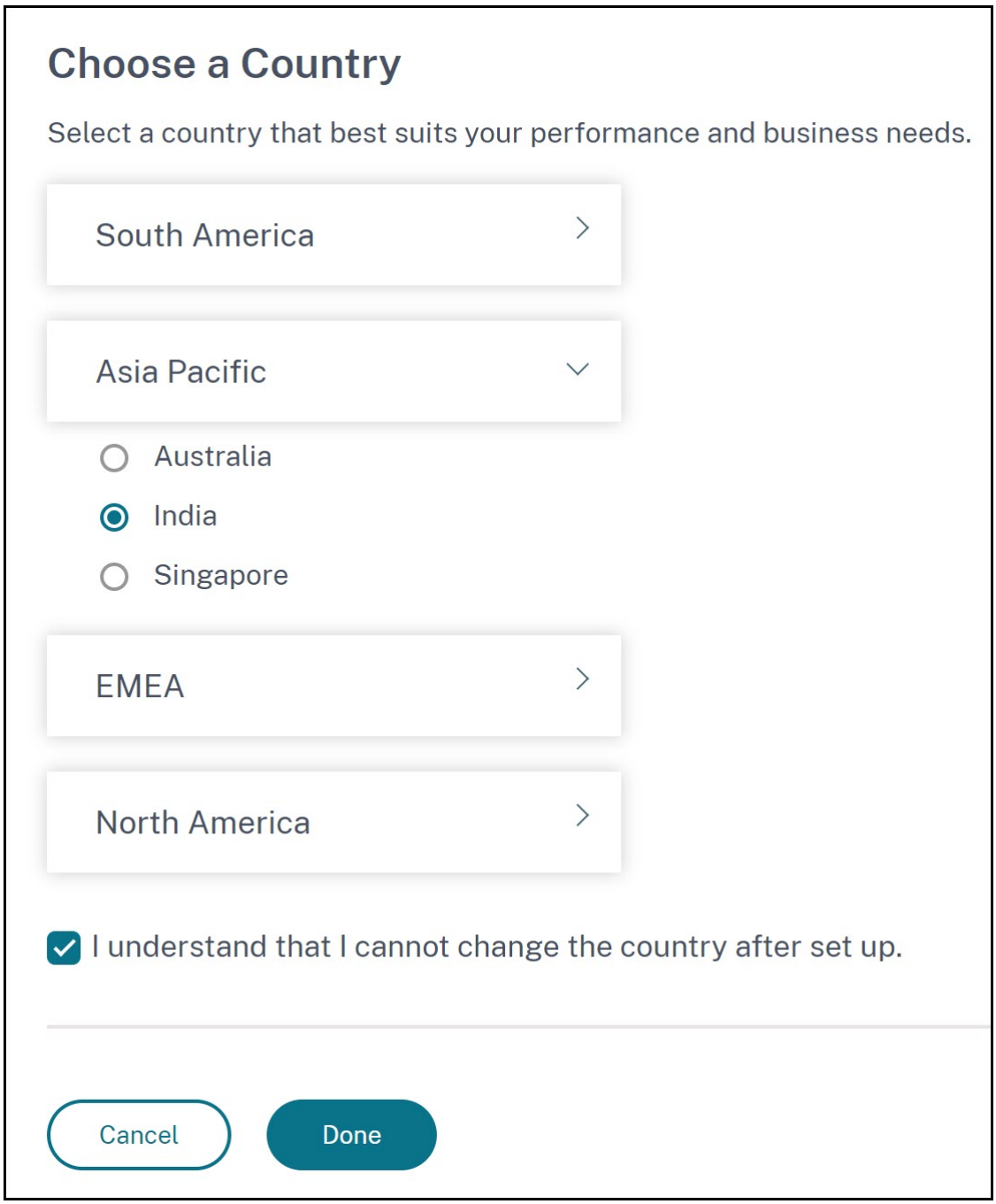
2. En el icono **Administración de entrega de aplicaciones**, haga clic en **Administrar**.

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



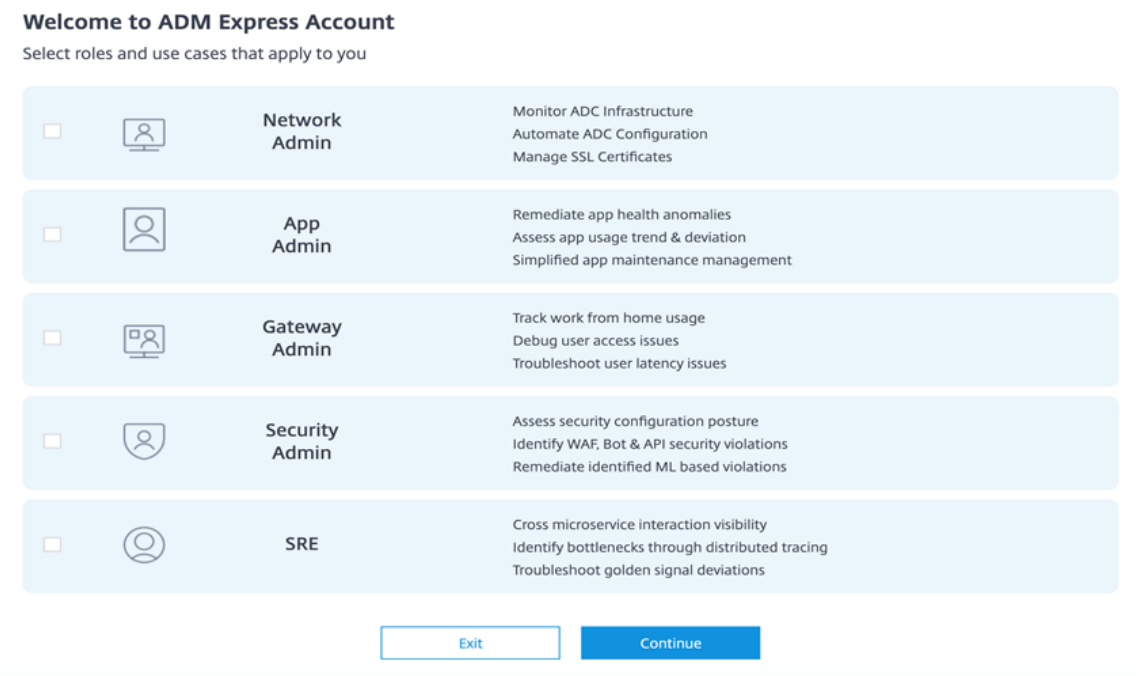
3. Seleccione el país que mejor se adapte a las necesidades de su empresa. Los países aparecen en función de las regiones seleccionadas.

Regiones	Sudamérica	Asia-Pacífico	Europa-Oriente Medio-África	Norteamérica
Países	Brasil	Australia, India y Singapur	Francia, Alemania y Reino Unido	Estados Unidos

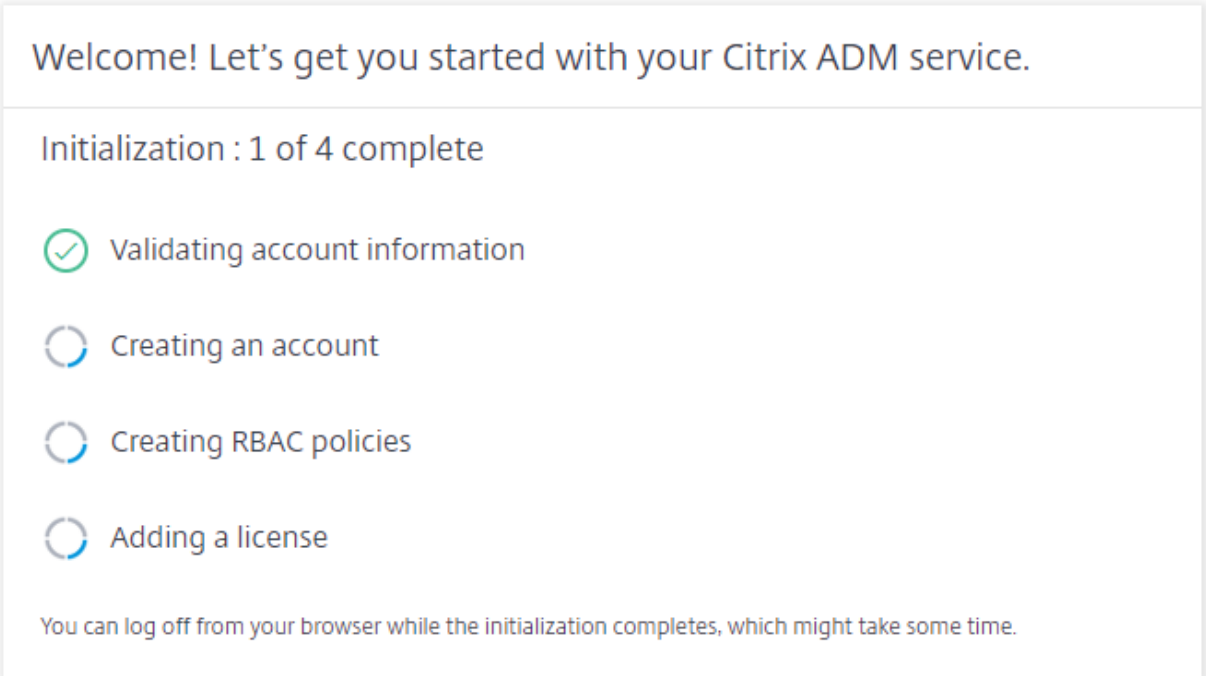


> **Importante**No
>
> puede cambiar la región más tarde.

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

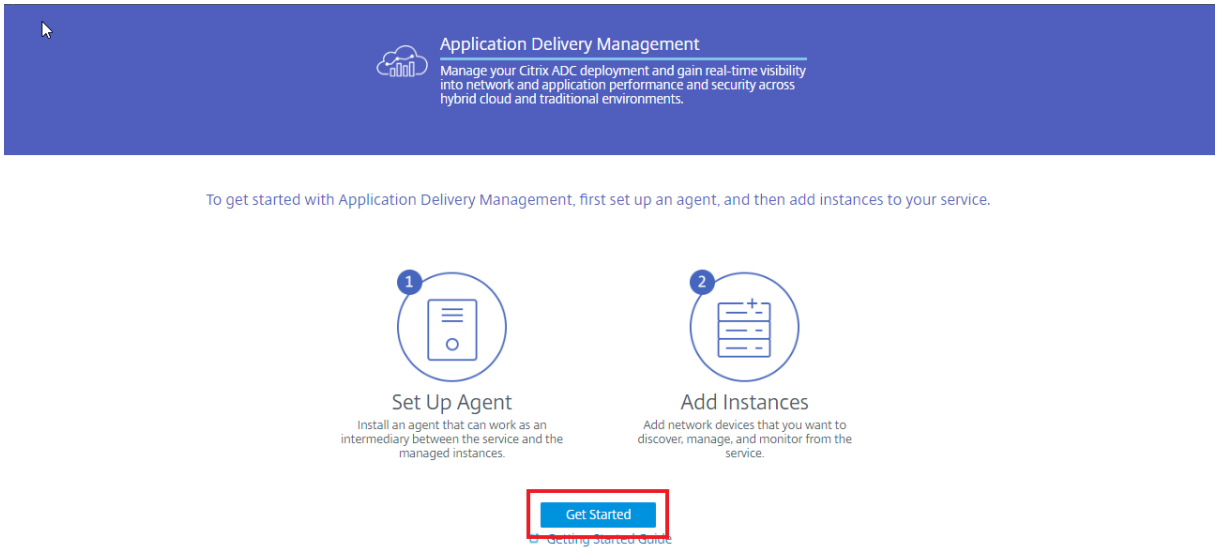


Puede cerrar la sesión en el explorador mientras la inicialización se completa en segundo plano, lo que puede tardar algún tiempo.



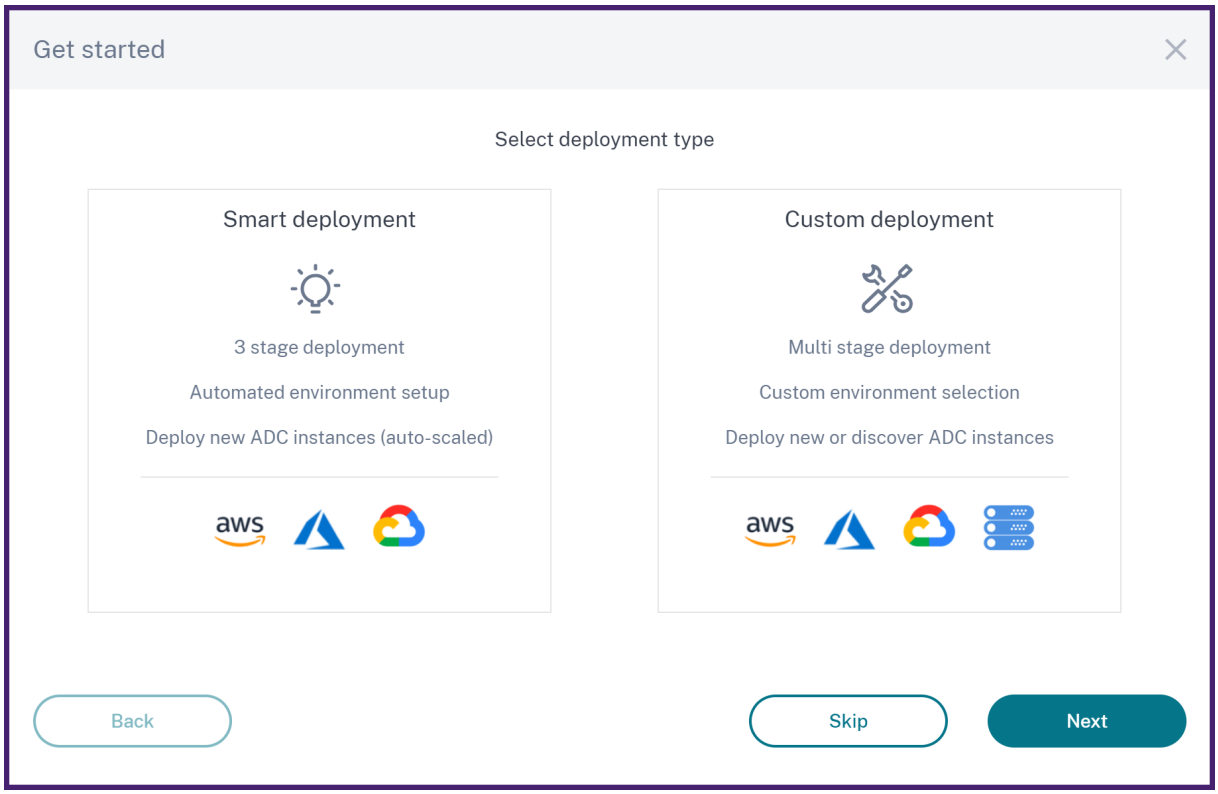
> **Nota**
>
> Citrix asigna una cuenta Express para administrar los recursos de Citrix ADM. Si su cuenta de Citrix ADM Express permanece inactiva durante 90 días, la cuenta se elimina. Para obtener más información, consulte Administrar Citrix ADM mediante una cuenta Express.

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



Paso 3: Seleccione un tipo de implementación ADC

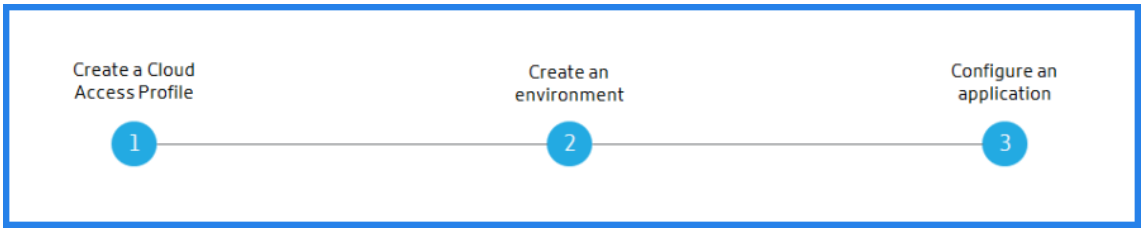
Seleccione una de las siguientes opciones de implementación que se adapte a sus requisitos empresariales:



- **Implementación inteligente** : esta opción es una configuración de entorno automatizada para

implementar nuevas instancias de ADC. Instala automáticamente un agente para habilitar la comunicación entre Citrix ADM 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 ADC.



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

Seleccione una implementación inteligente para AWS

Esta opción de implementación crea la siguiente infraestructura en AWS:

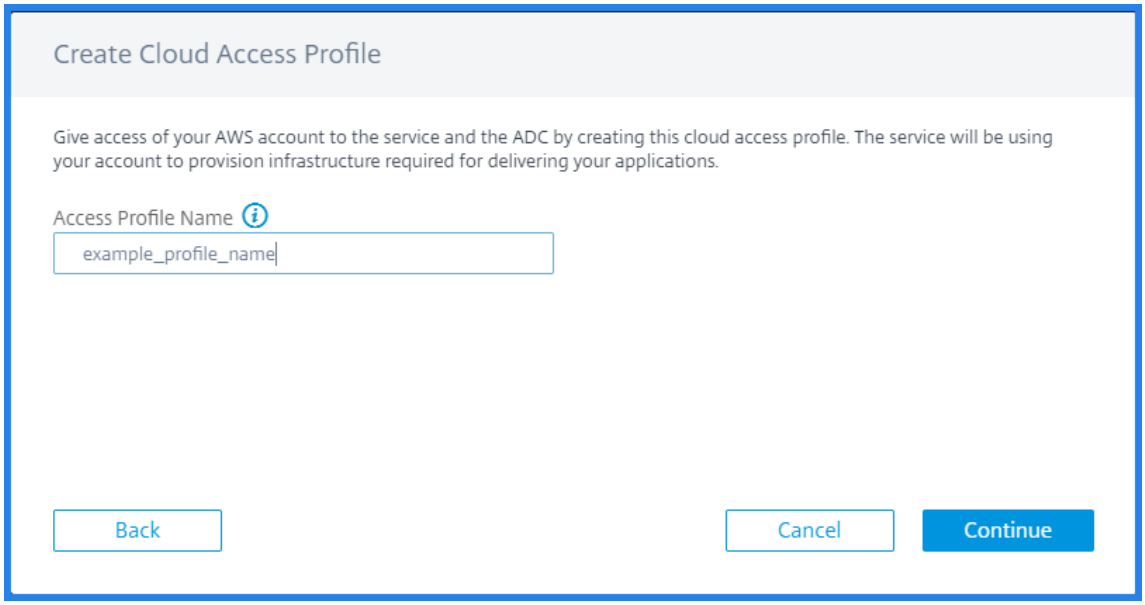
- Una pila de CloudFormation en AWS para crear la infraestructura necesaria que incluye subredes, grupos de seguridad, puertas de enlace NAT, etc.
- Un agente Citrix ADM en la VPC para administrar las instancias de ADC.
- Un grupo de ADC Autoscale. Puede personalizar este grupo más adelante en la página **Infraestructura > Nube pública > Grupos de Autoscale** .

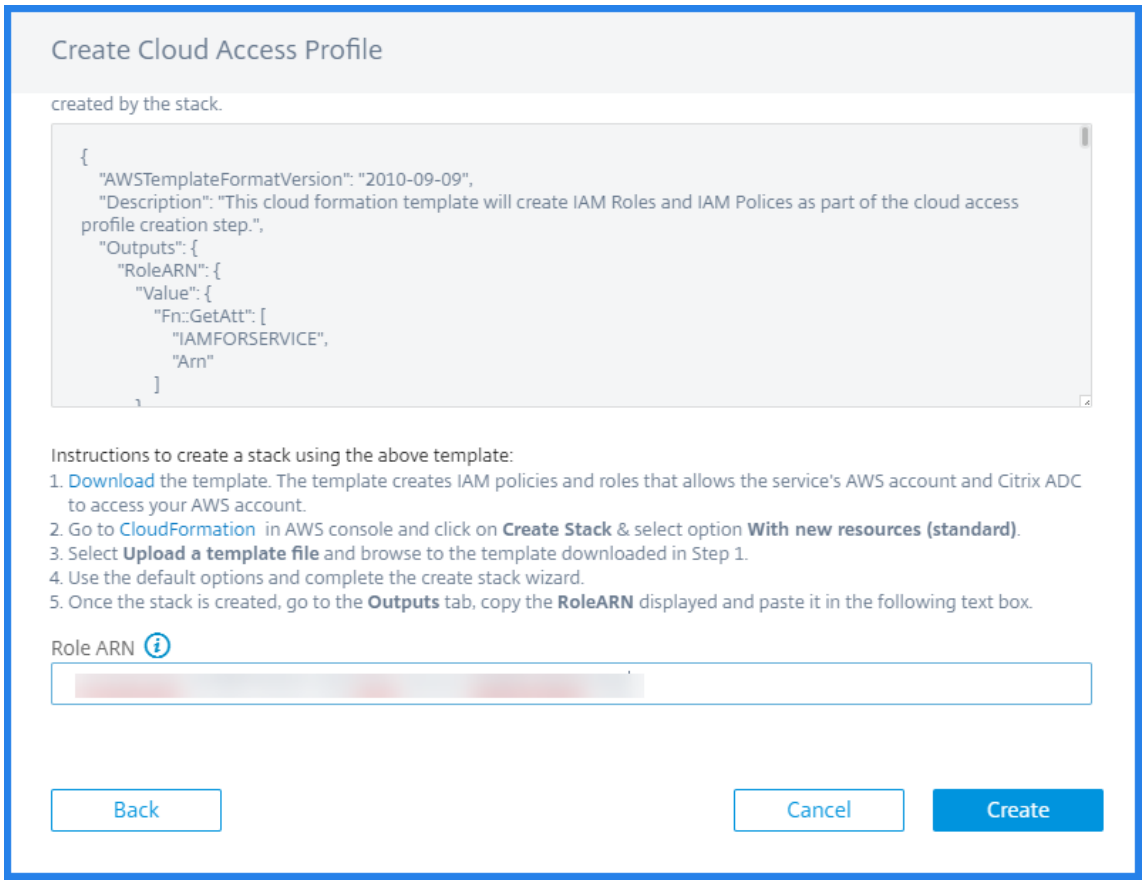
Antes de implementar instancias de ADC, asegúrese de lo siguiente:

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

Para implementar instancias de ADC, 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.



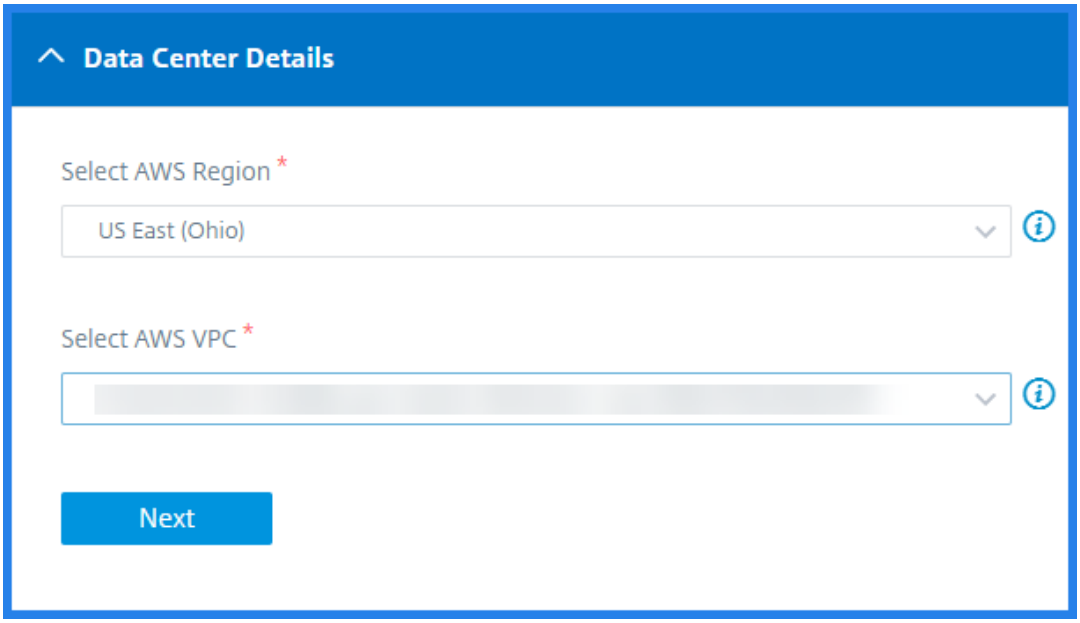


El Citrix ADM usa el perfil de acceso a la nube para acceder a una cuenta de AWS.

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

   a) En **Detalles del centro de datos**, seleccione **Región** de **AWS y AWS VPC** donde quiera implementar instancias de ADC.

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



b) En **Detalles del grupo de escalado automático de ADC**, especifique lo siguiente para escalar automáticamente las instancias de ADC en la nube de AWS:

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

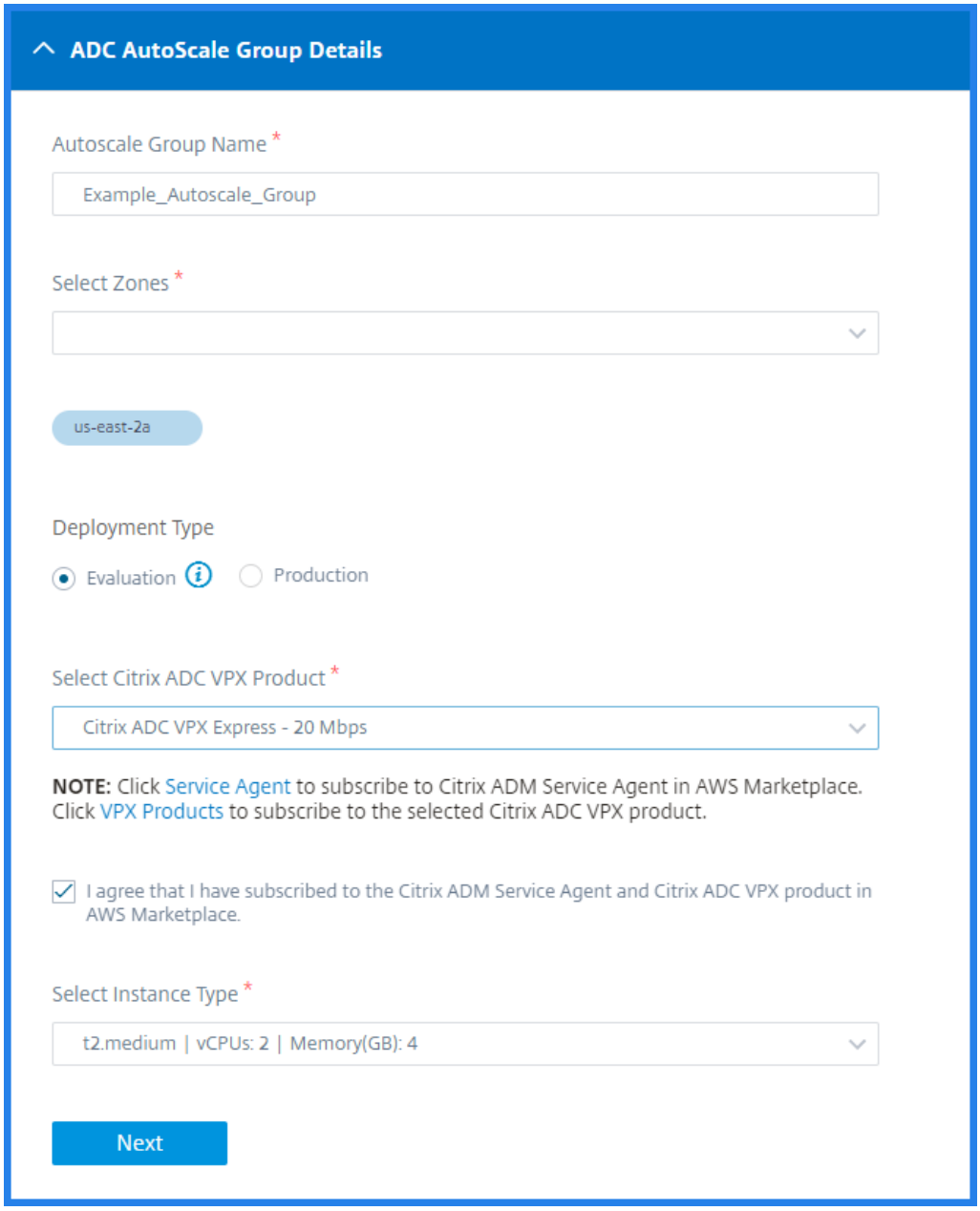
  Puede seleccionar varias zonas de la lista.
- **Tipo de implementación** : seleccione **la opción Evaluación** o **Producción**.

  Si quiere evaluar la solución Citrix ADM Autoscale 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, sólo puede seleccionar Citrix ADC VPX Express. Además, la solución Citrix ADM Autoscale puede escalar hasta tres instancias de ADC.
- **Producto Citrix ADC VPX** : seleccione licencias para aprovisionar instancias de ADC.

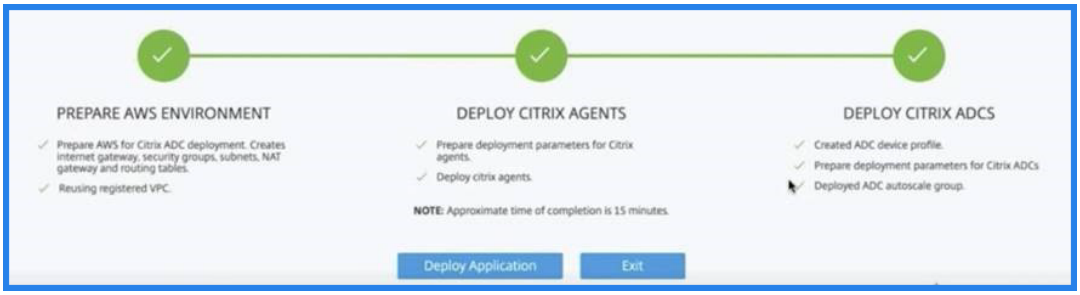
  Suscríbase a la licencia seleccionada en el mercado de AWS y vuelva a esta página.

  Revise y seleccione el mensaje de consentimiento del usuario.
- **Tipo de instancia** : seleccione el tipo de instancia requerido.



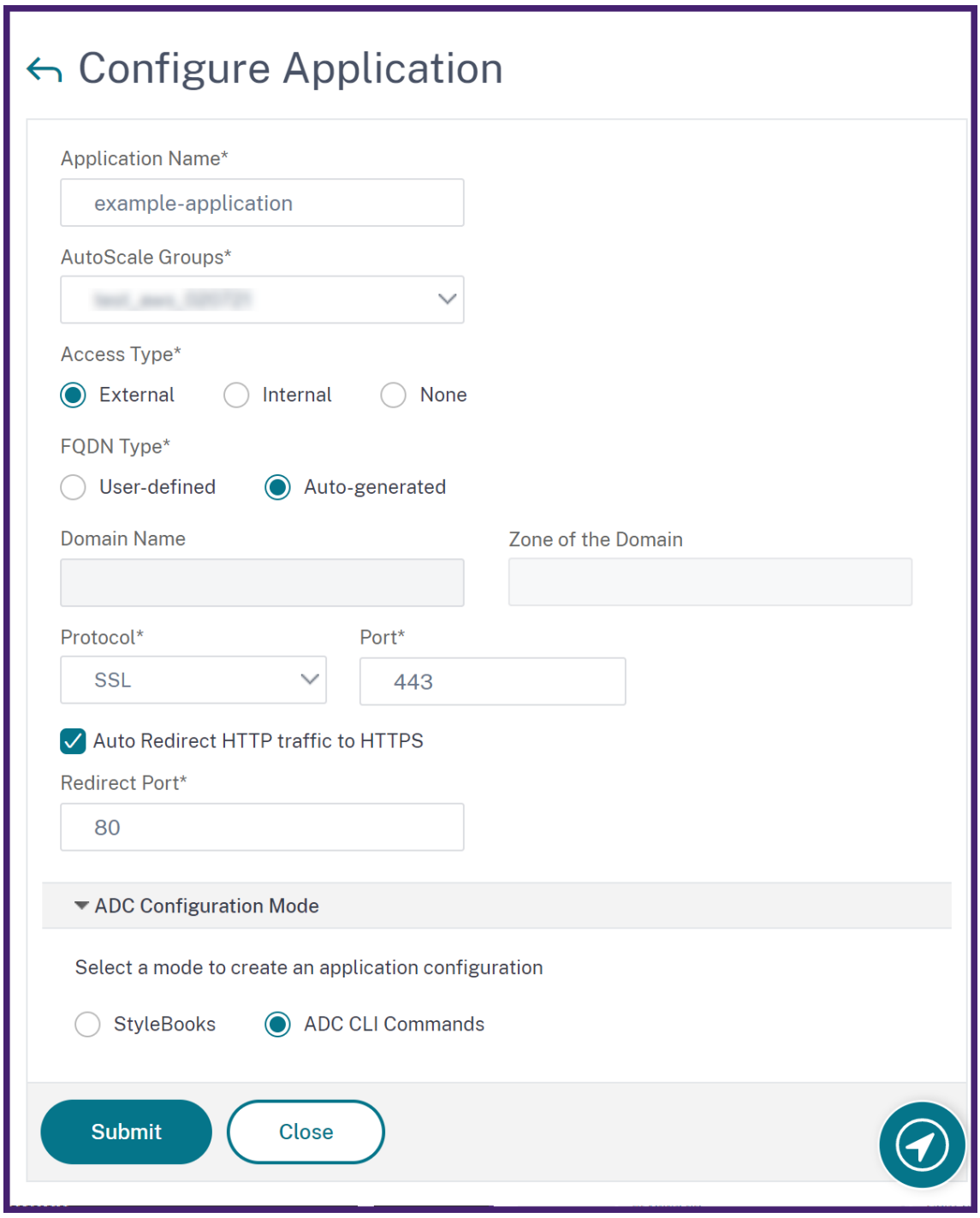
c) Haga clic en **Siguiente**.

Después de la validación correcta, haga clic en **Crear** para implementar instancias ADC en AWS y crear un grupo de AutoScale.



3. Después de la implementación correcta de ADC, 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 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 in-

cluye subredes, grupos de seguridad, pasarelas NAT, etc.

- Un agente Citrix ADM en la VPC para administrar las instancias de ADC.
- Un grupo de ADC Autoscale. Puede personalizar este grupo más adelante en la página **Infraestructura > Nube pública > Grupos de Autoscale** .

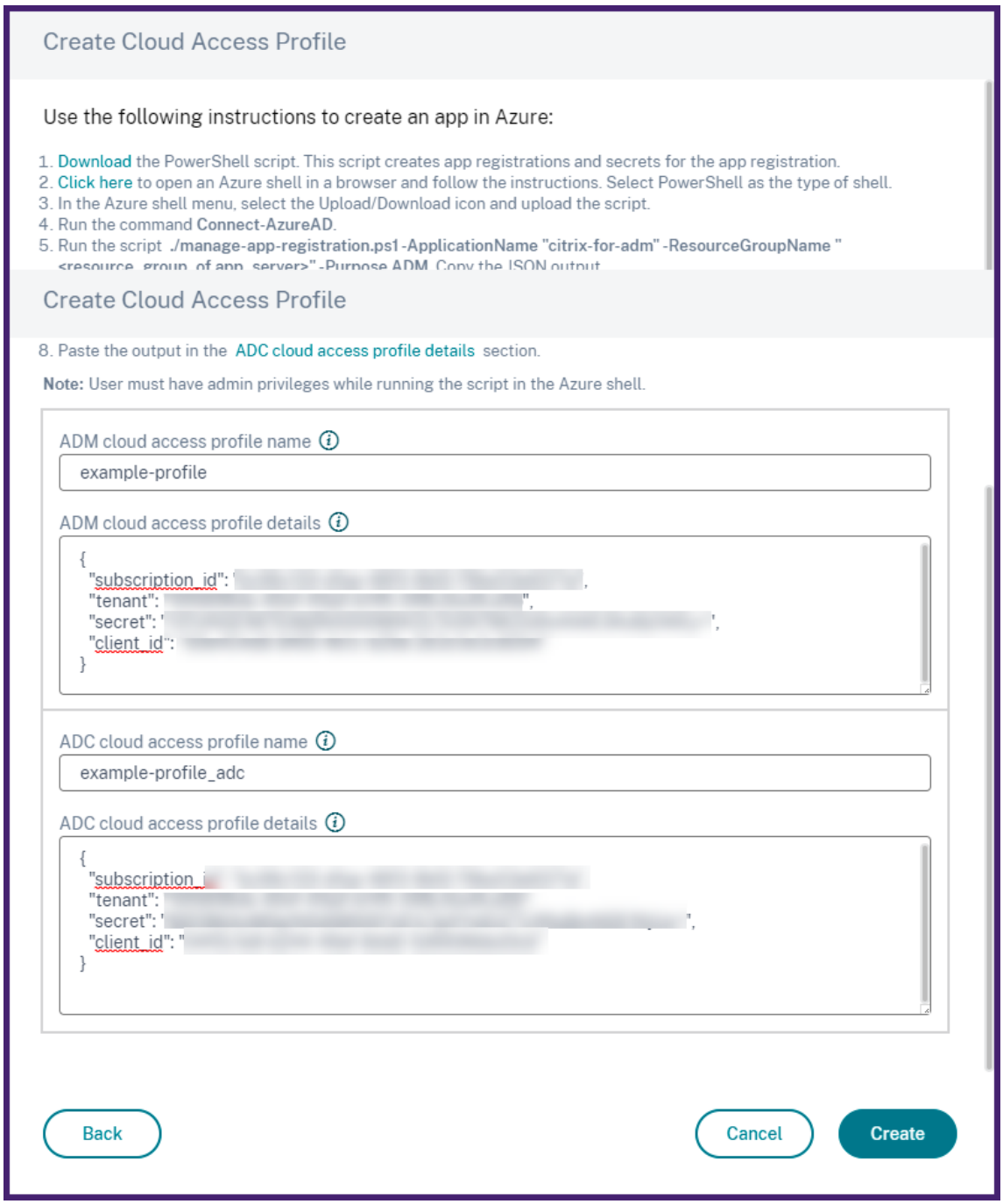
Antes de implementar instancias de ADC, asegúrese de lo siguiente:

- 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 ADC, lleve a cabo los siguientes pasos:

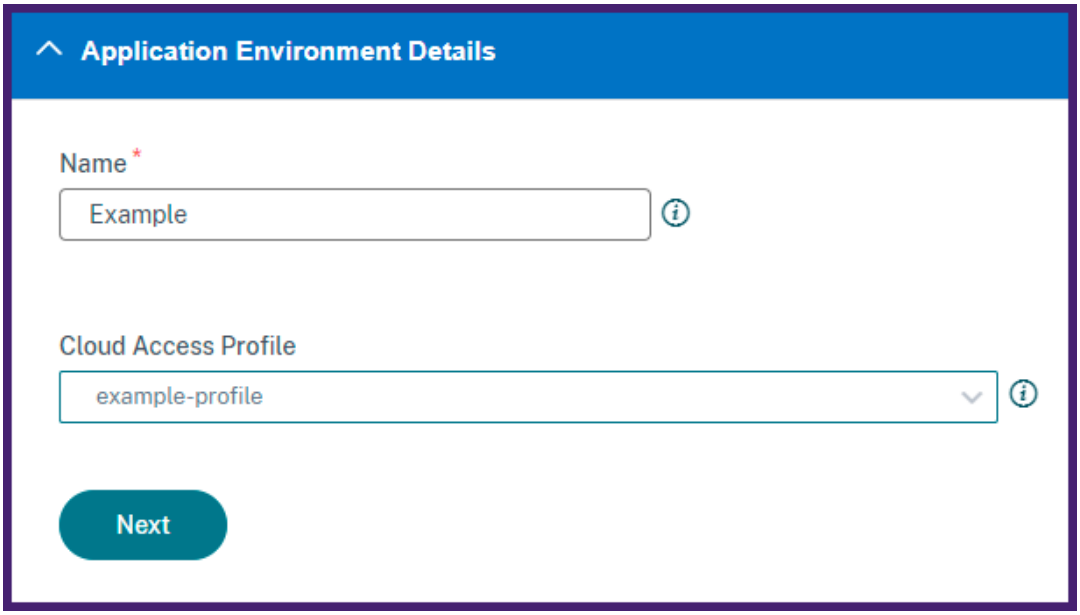
1. En **Crear perfil de acceso a la nube**, seleccione **Microsoft Azure** como entorno de implementación. Especifique los detalles del perfil de acceso a la nube de Citrix ADM y ADC.



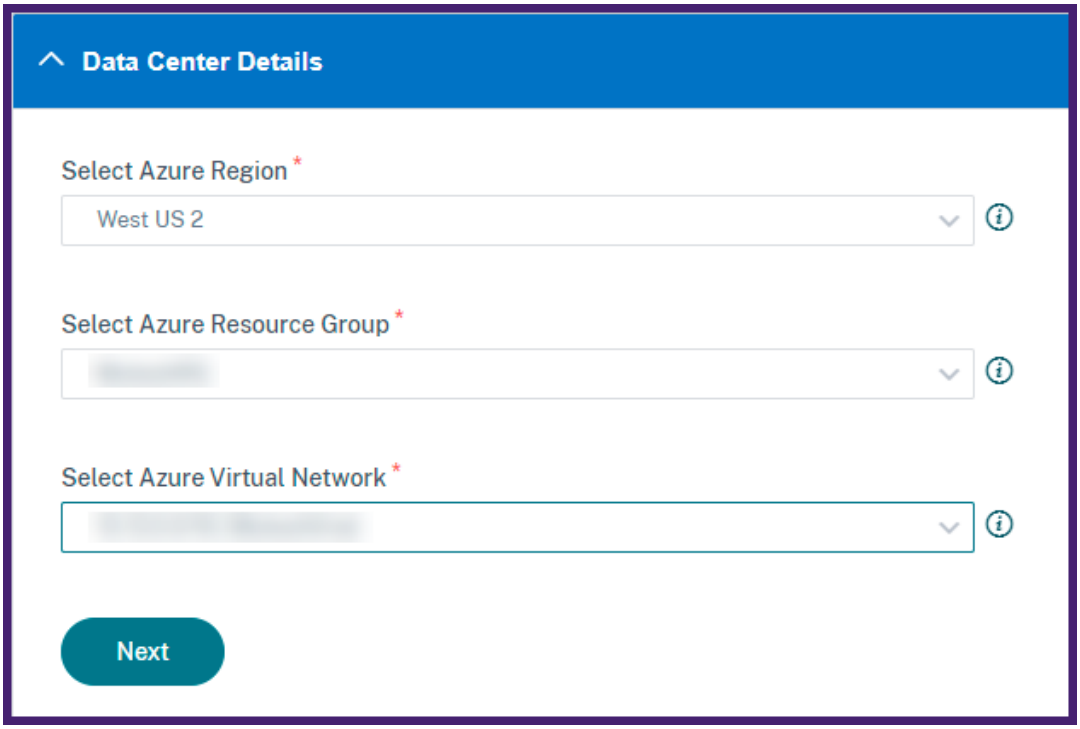
El ADM de Citrix utiliza el perfil de acceso a la nube de Citrix ADM para acceder a una cuenta de Microsoft Azure. Además, se utiliza un perfil de acceso a la nube de ADC para aprovisionar las instancias VPX de ADC.

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 quiere implementar las instancias de ADC.



c) En **Detalles del grupo de ADC 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 quiere evaluar la solución Citrix ADM Autoscale antes de comprar la licencia de producción, seleccione la opción **Evaluación** .

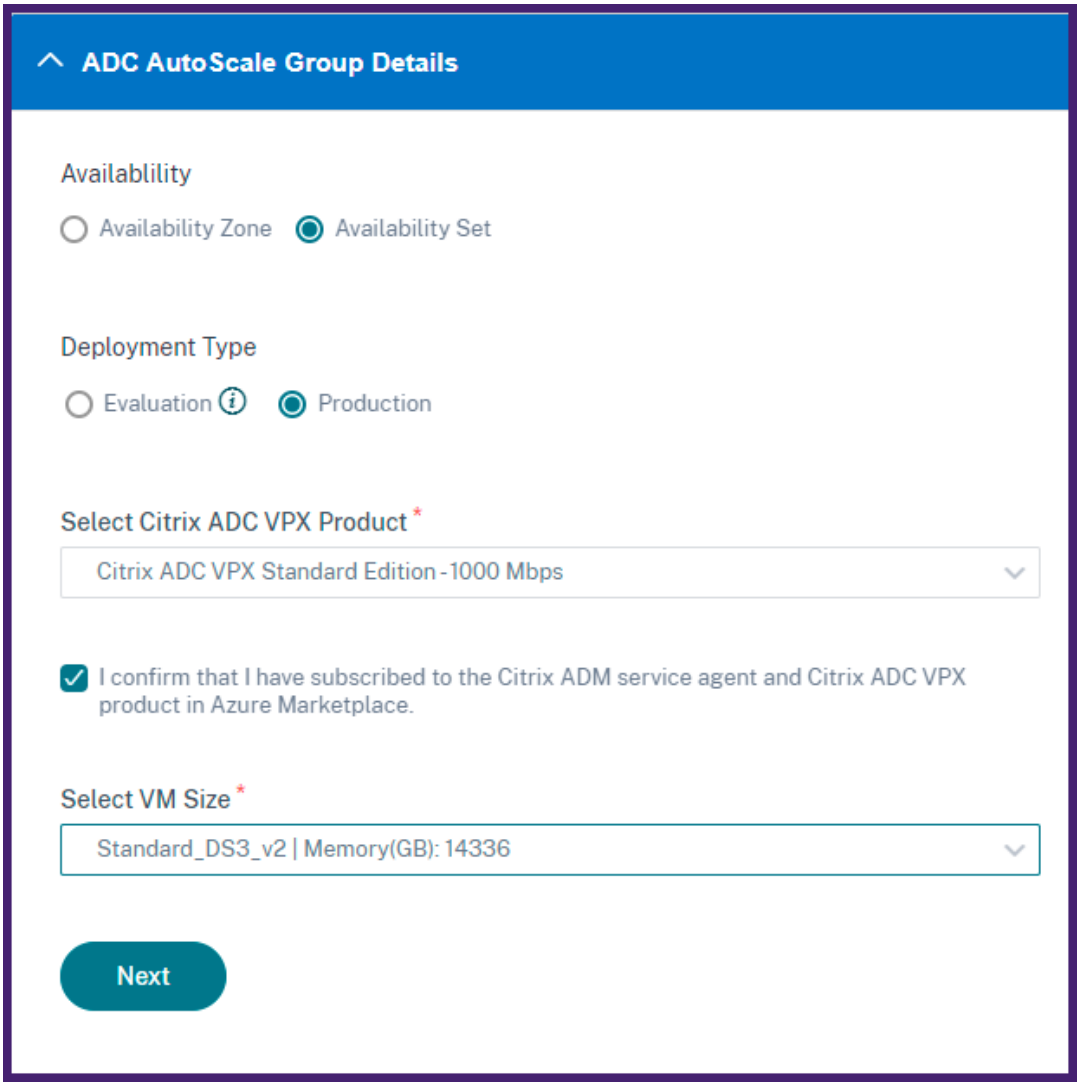
> **Importante**
>
> – La opción de evaluación solo admite una zona o conjunto de disponibilidad.
> - Con la opción de evaluación, sólo puede seleccionar Citrix ADC VPX Express. Además, la solución Citrix ADM Autoscale puede escalar hasta tres instancias de ADC.

- **Seleccione el producto Citrix ADC VPX** : seleccione las licencias para aprovisionar las instancias de ADC.

  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.

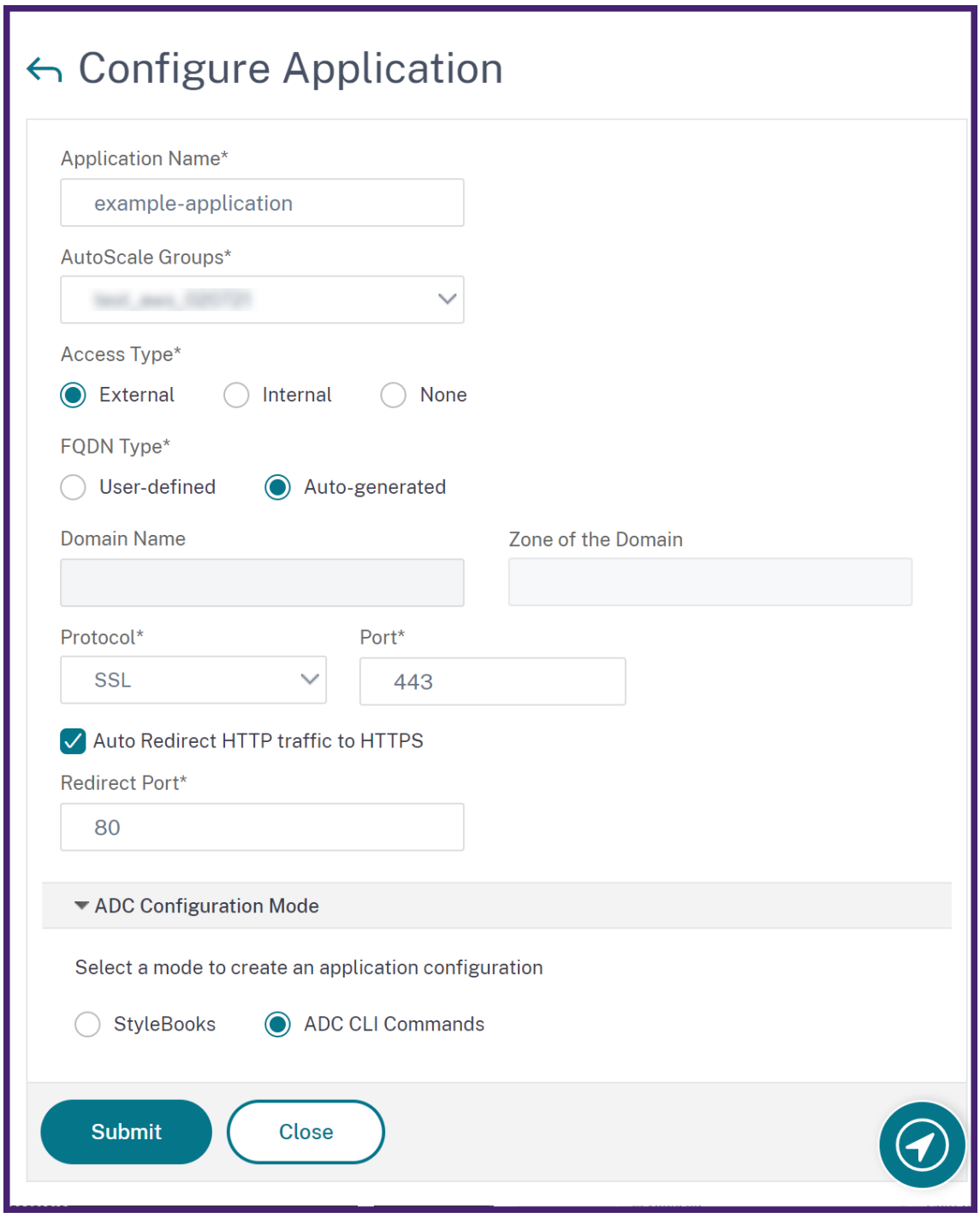


d) Haga clic en **Siguiente**.

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

3. Después de la implementación correcta de ADC, 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 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, Cloud NAT, pasarelas de Cloud Router y reglas de firewall.

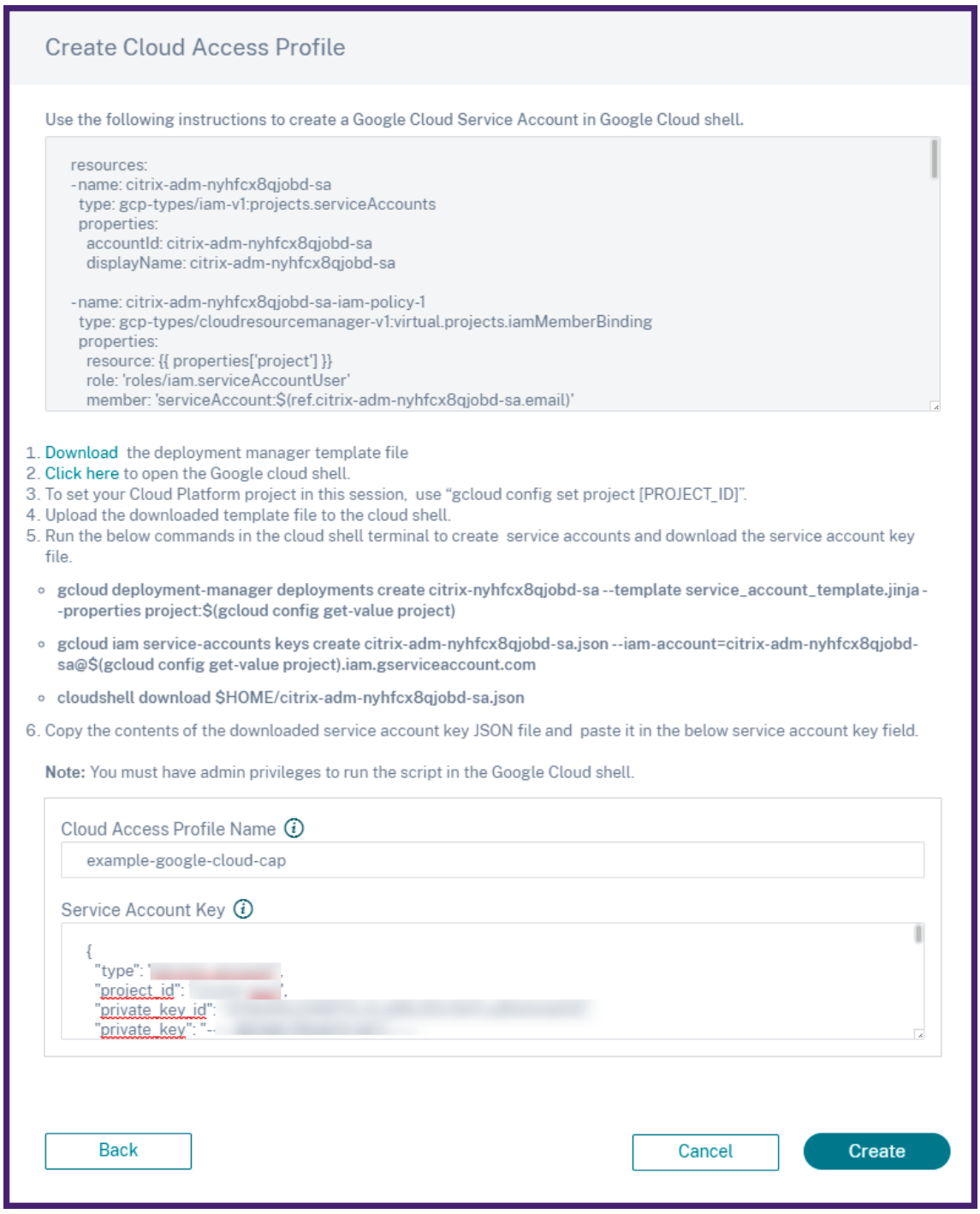
- Un agente Citrix ADM en la VPC para administrar las instancias de ADC.
- Un grupo de ADC Autoscale. Puede personalizar este grupo más adelante en la página **Infraestructura > Nube pública > Grupos de Autoscale** .

Antes de implementar instancias de ADC, asegúrate de que ya tiene una cuenta de Google Cloud. Para obtener más información sobre cómo crear una cuenta, consulta la documentación de Google Cloud.

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

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

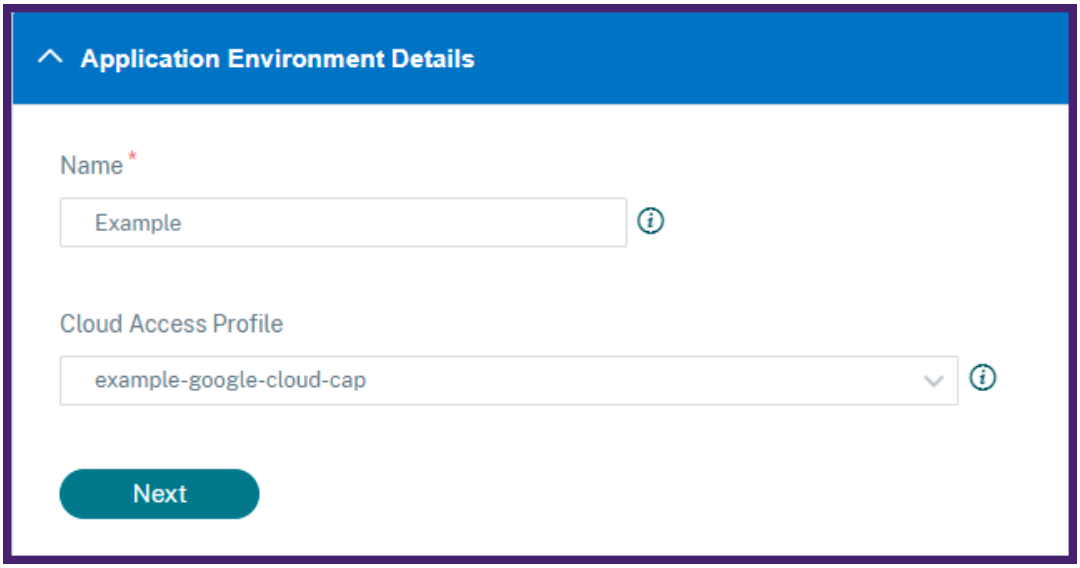
   Especifique el **nombre del perfil de acceso a la nubey la clave de cuenta**



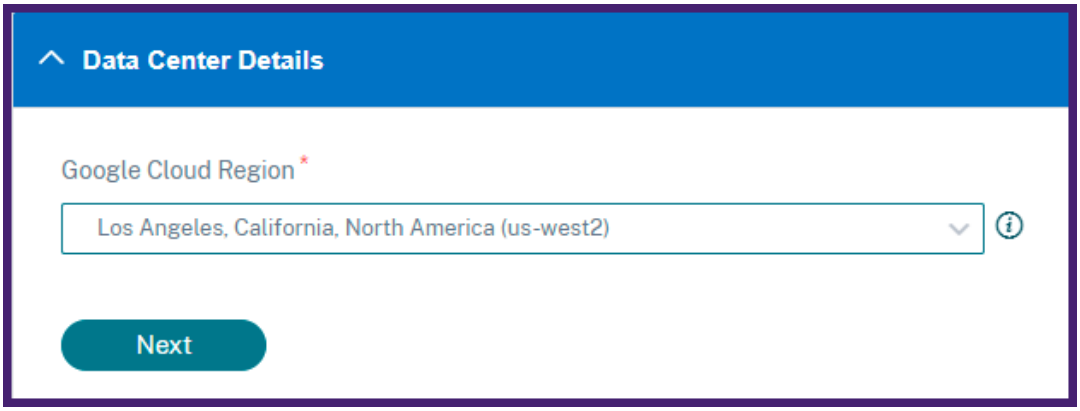
El Citrix ADM usa el perfil de acceso a la nube para acceder a una cuenta de Google Cloud.

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 las instancias de ADC.



c) En **Detalles del grupo de ADC AutoScale**, especifique lo siguiente para las instancias de ADC de Autoscale en Google Cloud:

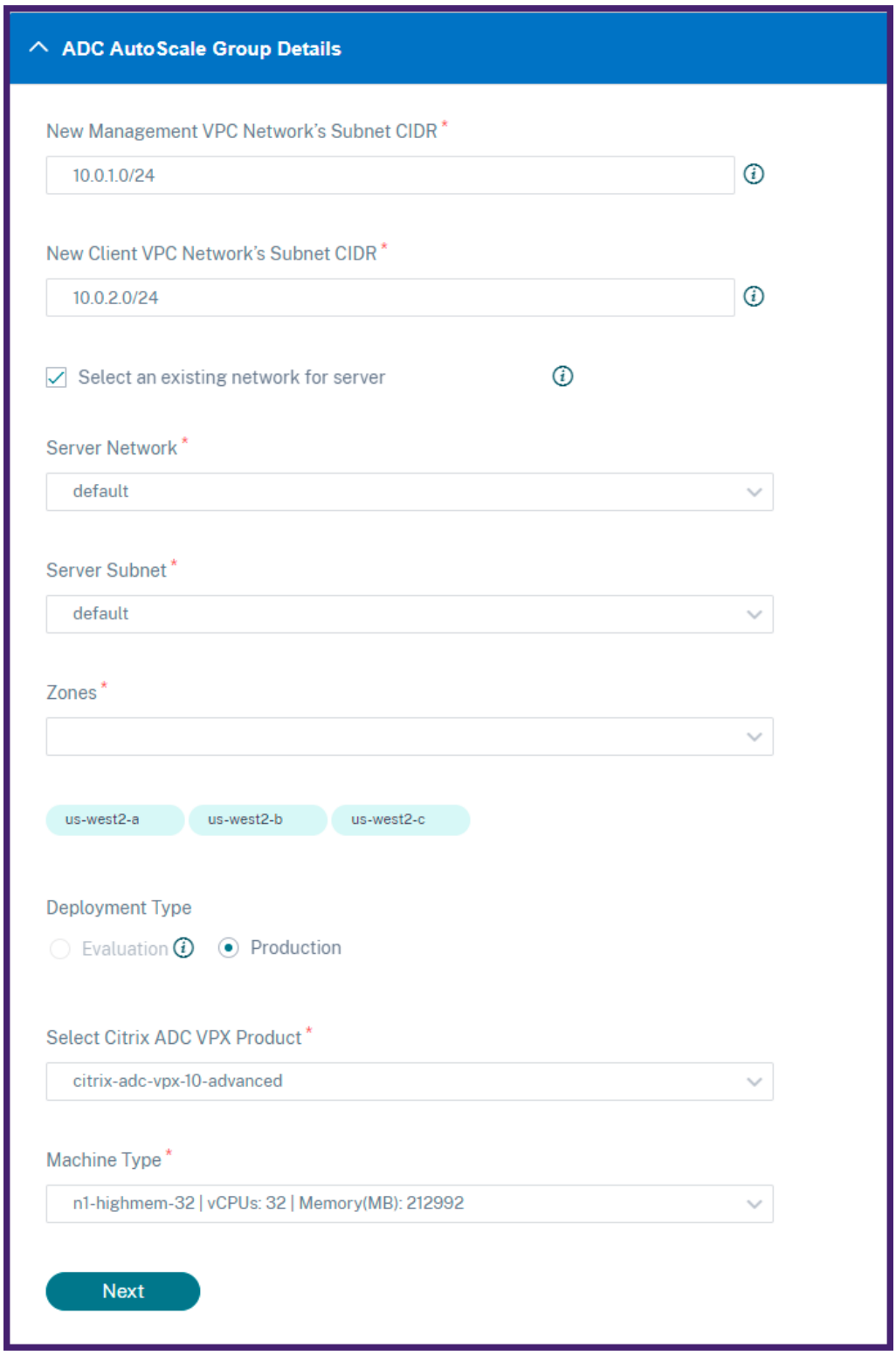
- **CIDR de subred de la red de VPC** : especifique una red de VPC creada para el tráfico de administración, cliente y servidor. Sin embargo, puede seleccionar la red existente como servidor.
- **Zonas** : seleccione las zonas en las que quiere crear los grupos de Autoscale.

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

  Si quiere evaluar la solución Citrix ADM Autoscale 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, sólo puede seleccionar Citrix ADC VPX Express. Además, la solución Citrix ADM Autoscale puede escalar hasta tres instancias de ADC.

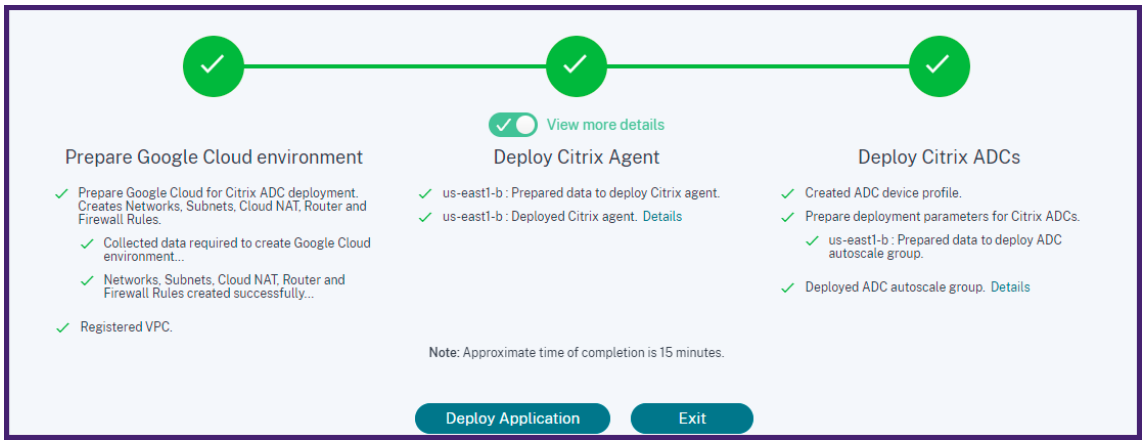
- **Producto Citrix ADC VPX** : seleccione licencias para aprovisionar instancias de ADC.
- **Tipo de máquina** : seleccione el tipo de instancia requerido.



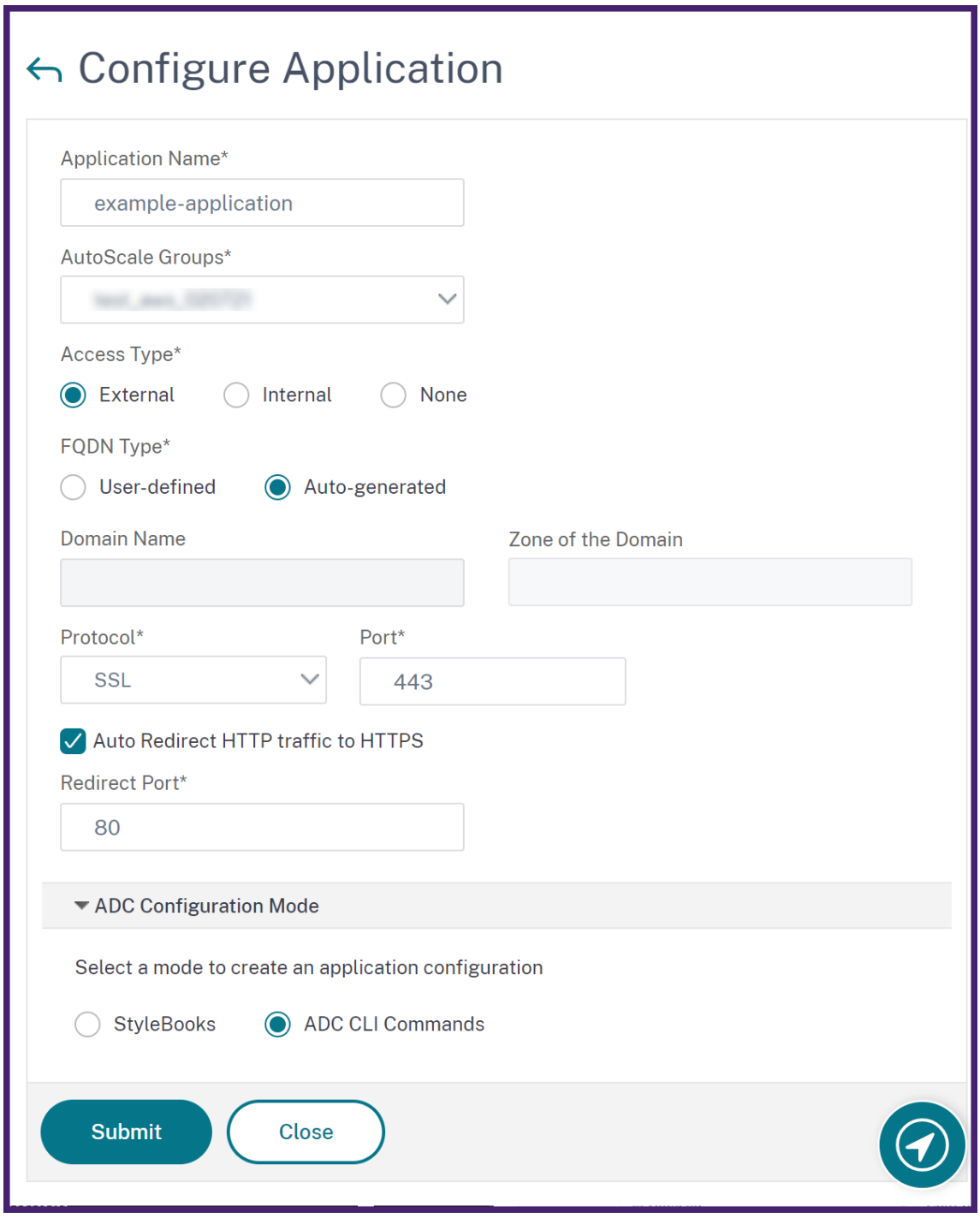
d) Haga clic en **Siguiente**.

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

3. Después de la implementación correcta de ADC, 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 Autoscale.

Seleccionar implementación personalizada

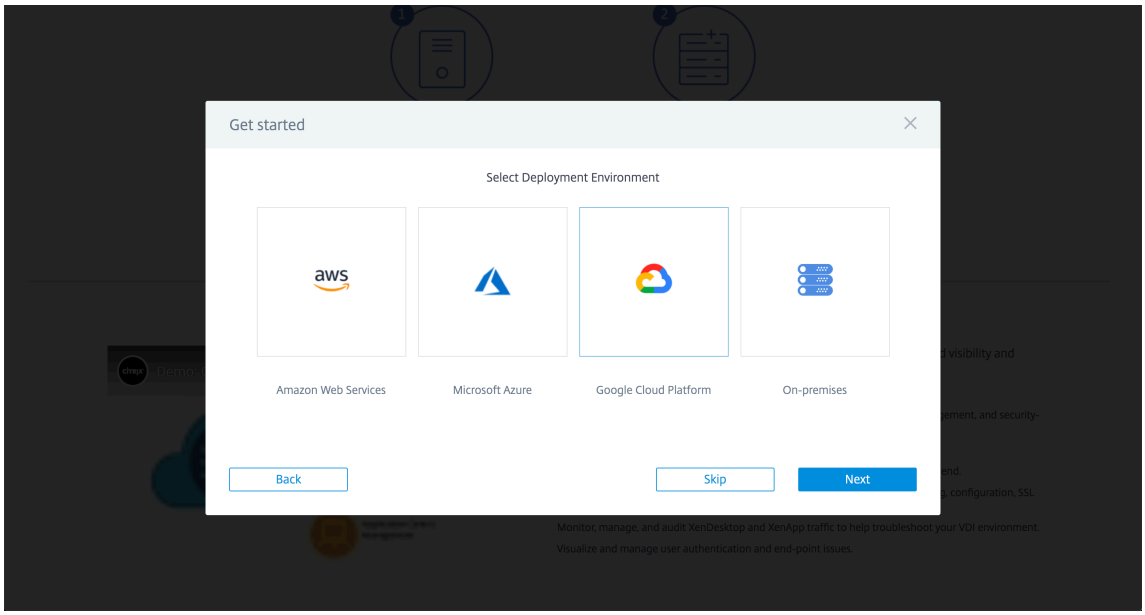
Esta opción proporciona una implementación en varias etapas. Seleccione esta opción para descubrir instancias de ADC de varios entornos. Con esta opción, también puede implementar nuevas instan-

cias especificando opciones de entorno personalizadas.

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

1. Seleccione cualquiera de los siguientes entornos:

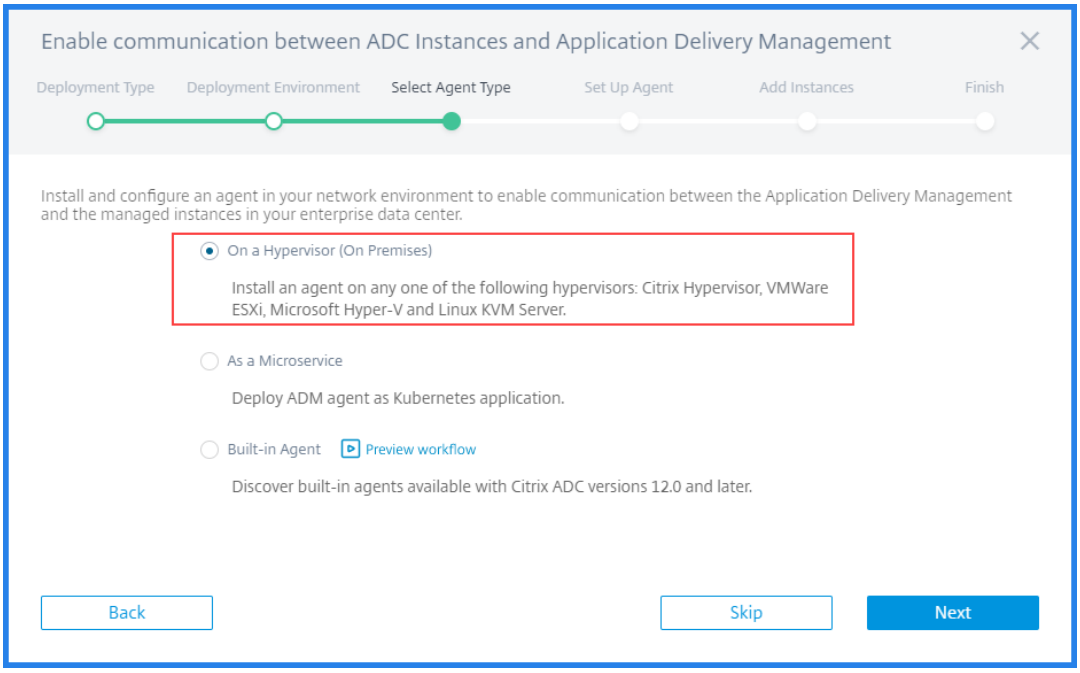
   - **AWS**
   - **Microsoft Azure**
   - **Google Cloud Platform**
   - **Local**



2. Instale Citrix ADM Agent para habilitar la comunicación entre Citrix ADM y las instancias administradas en el centro de datos o la nube.

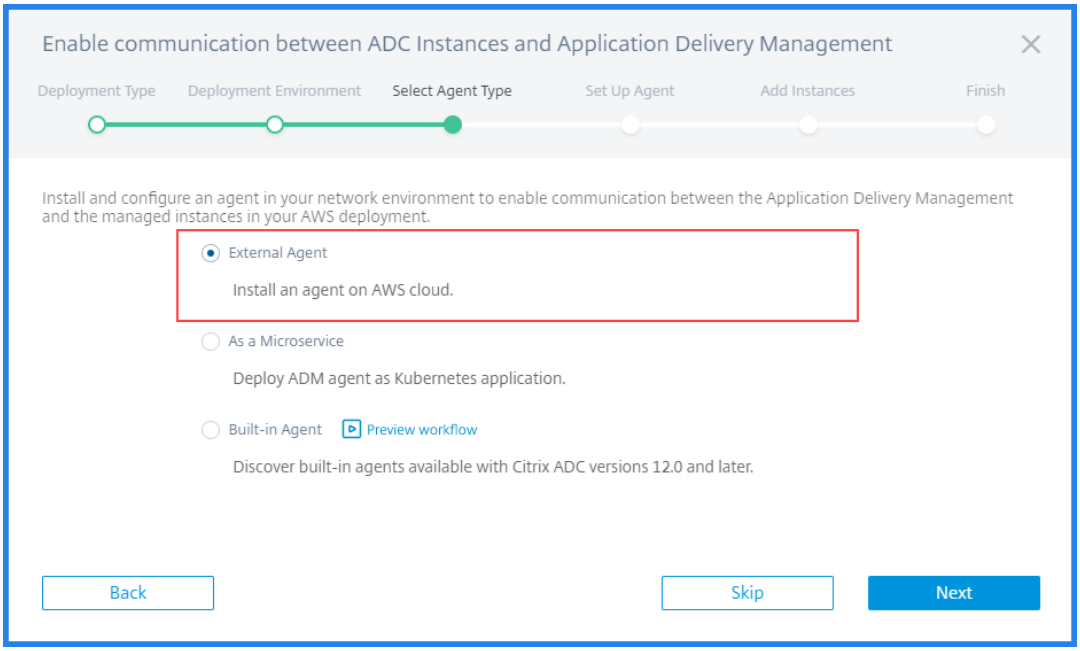
   El paso **Seleccionar tipo de agente** varía las opciones de instalación del agente en función del entorno seleccionado.

   - **Local** : si selecciona **Local,**puede instalar un agente en los siguientes hipervisores:
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Servidor KVM Linux

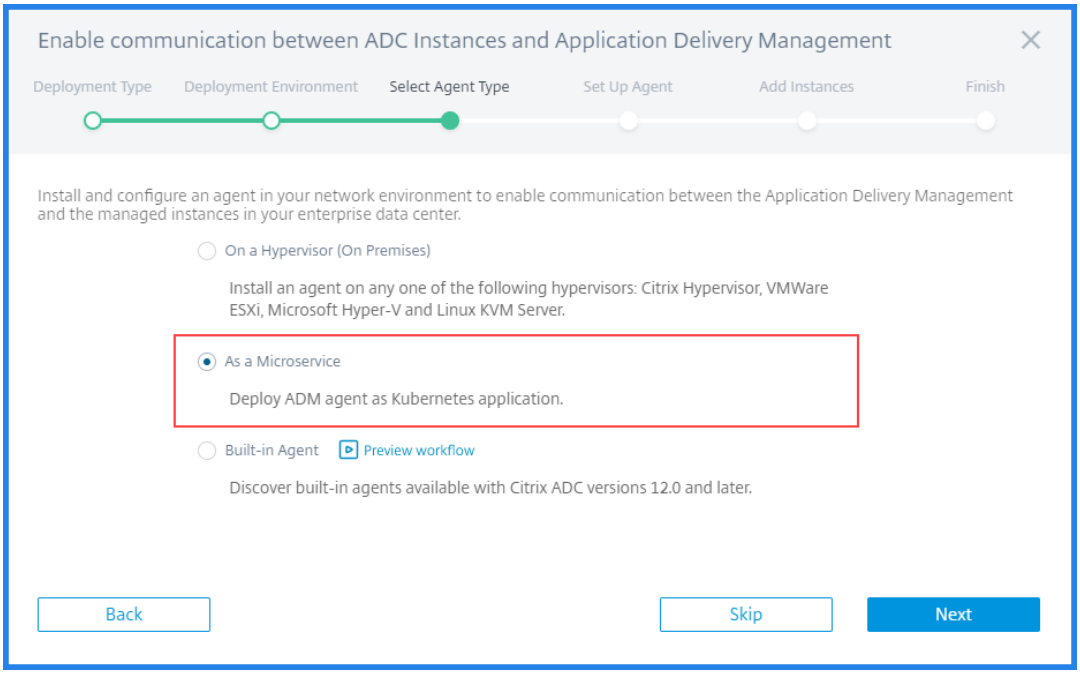


- **Nubes públicas** : si selecciona **AWS**, **Microsoft Azure**o **Google Cloud Platform**, puede instalar un agente de forma externa en la nube seleccionada.

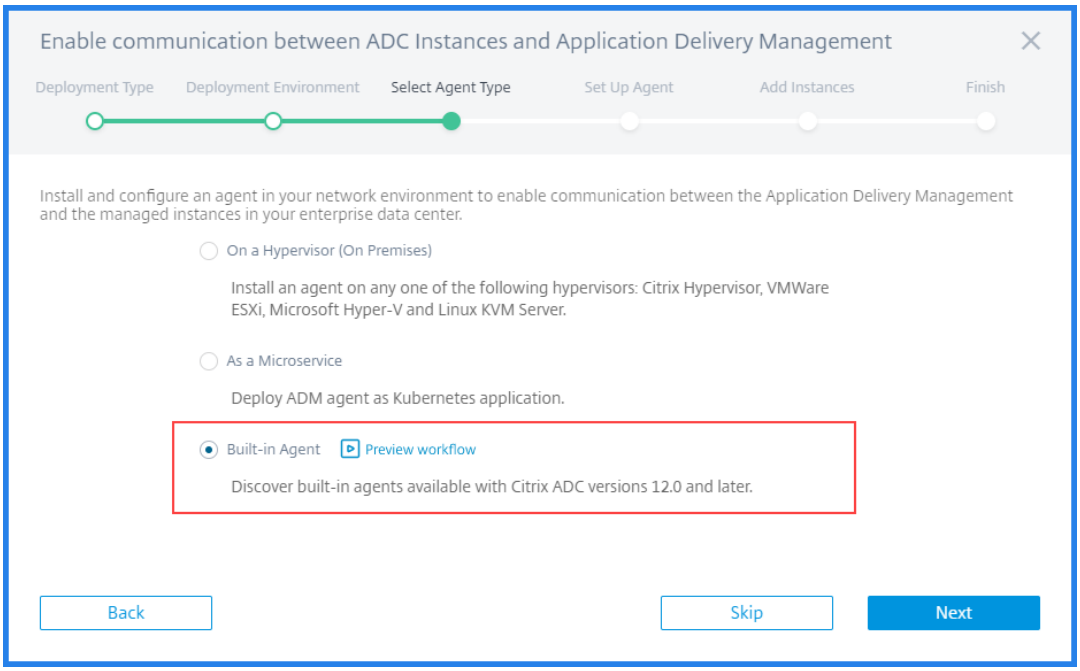
  A continuación se muestra una imagen de ejemplo para el entorno de AWS.



- **Como microservicio** - Para implementar un agente como una aplicación Kubernetes.



- **Agente integrado** : para descubrir los agentes integrados disponibles con Citrix ADC 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:

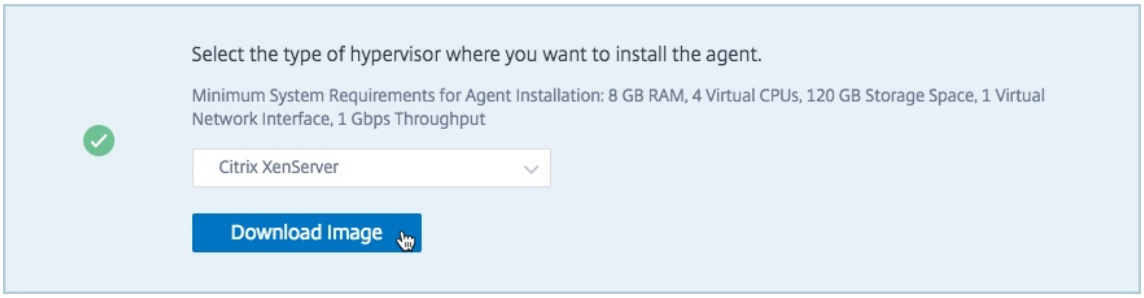
   - Hipervisor
   - Agente externo

- Como microservicio
- Agente integrado

Instalar un agente en un Hypervisor

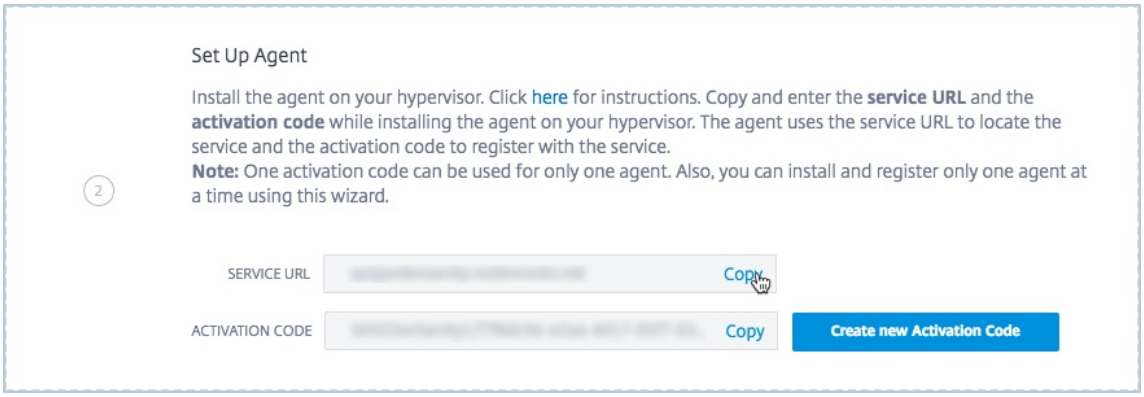
Realice los siguientes pasos para configurar un agente Citrix ADM en un hipervisor:

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 su hipervisor local, consulte Instalar el agente Citrix ADM de forma local.

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

Paso siguiente: Agregar instancias.

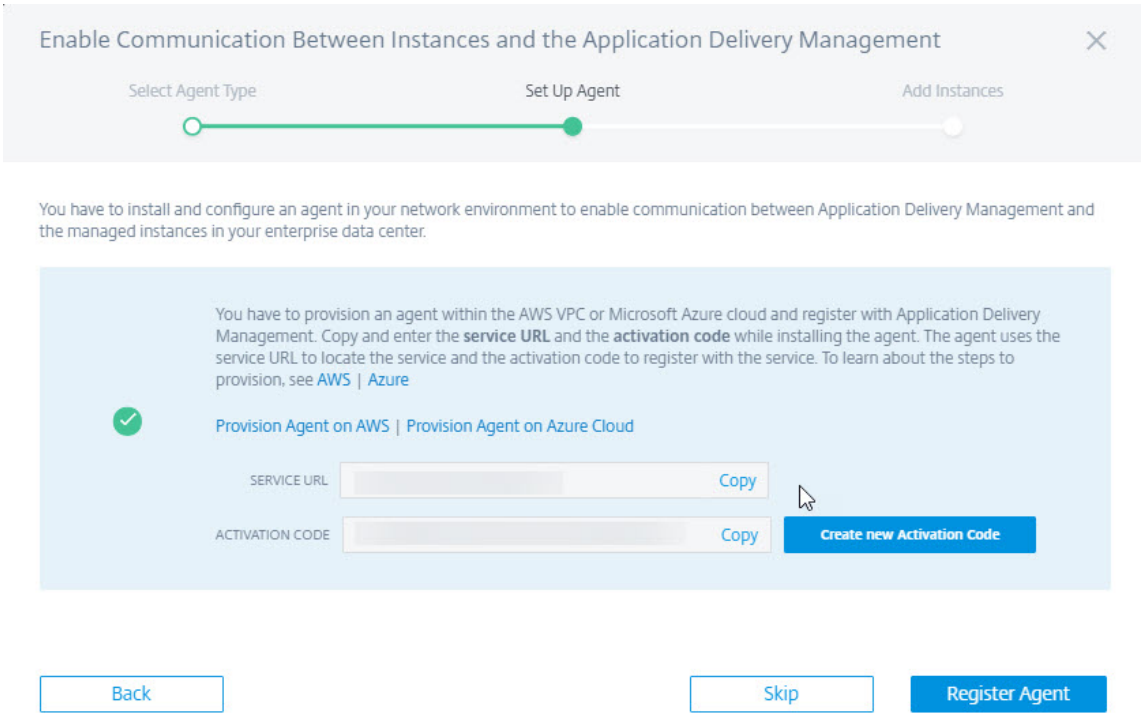
> **Nota**
>
> Si no quiere agregar agentes durante la configuración inicial, haga clic en **Omitir** para comprobar las funciones que proporciona Citrix ADM. Puede agregar los agentes y las instancias más adelante. Para agregar agentes más adelante, vaya a **Configuración > Configurar agentes**. Para 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 Instalación del agente Citrix ADM en Microsoft Azure Cloud.
   - Para obtener instrucciones detalladas sobre la instalación de un agente en AWS, consulte Instalación del agente Citrix ADM en AWS.
   - Para obtener instrucciones detalladas sobre la instalación de un agente en Google Cloud, consulte Instalar el agente Citrix ADM en GCP.

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

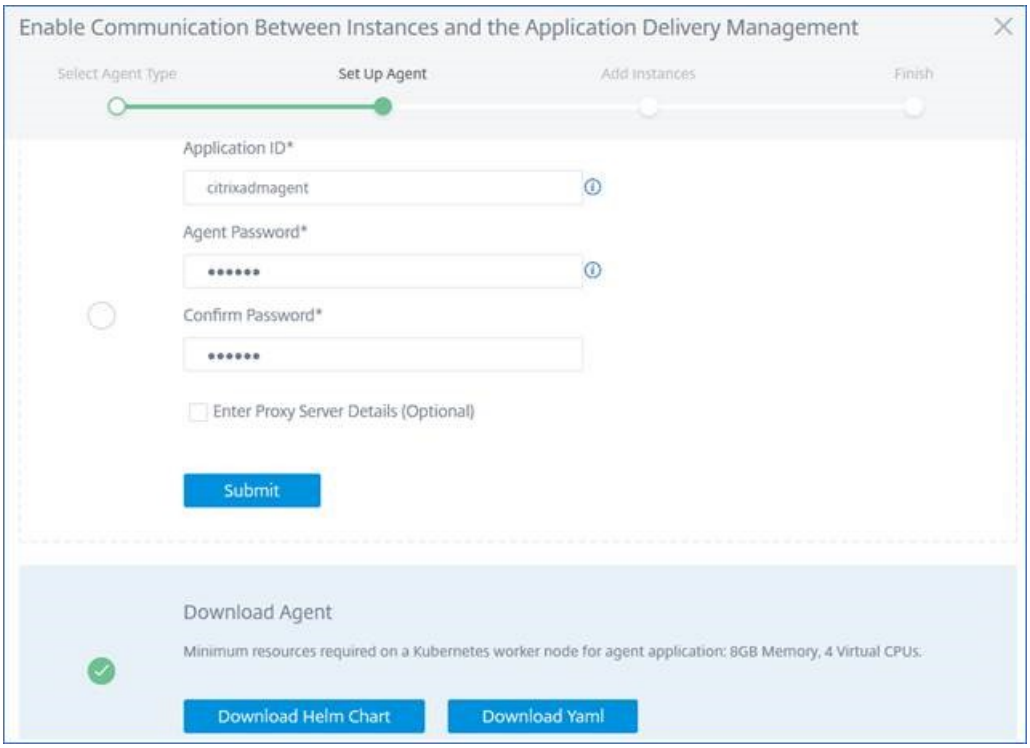
Paso siguiente: Agregar instancias.

Instalar un agente como microservicio

Puede implementar un agente de Citrix ADM como un microservicio en el clúster de Kubernetes para ver el **gráfico de servicio** en Citrix ADM.

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 use para incorporar CPX a Citrix ADM a través del agente.
   c) **Confirmar contraseña**: Especifique la misma contraseña para la confirmación.



   d) Haga clic en **Submit**.

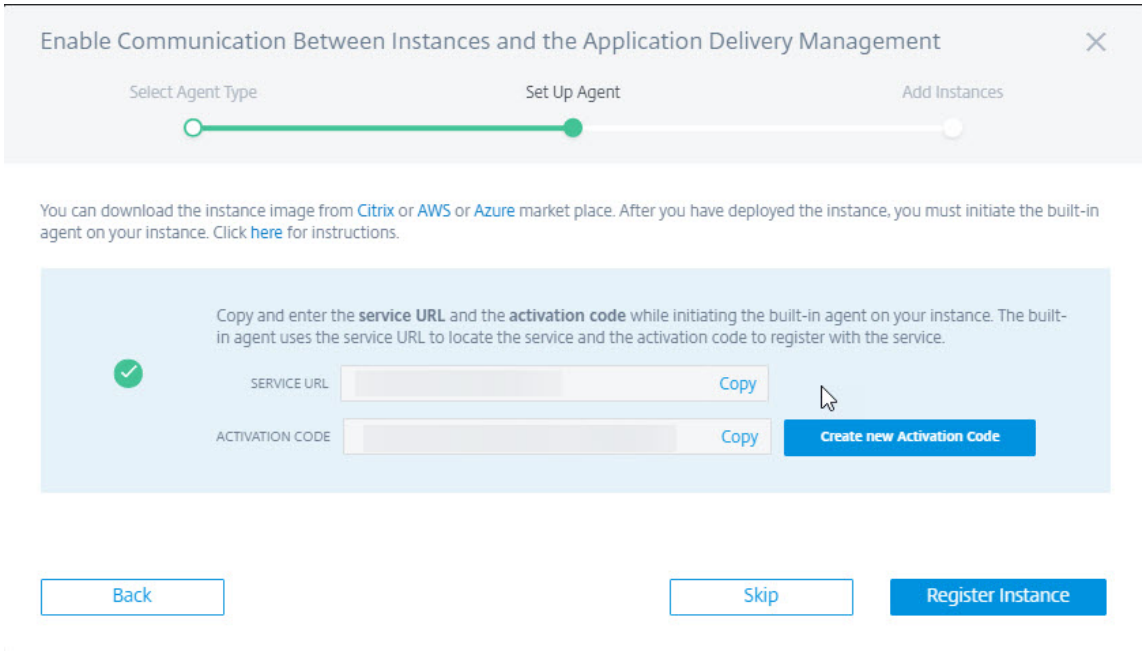
2. Después de hacer clic en **Enviar**, puede descargar el gráfico YAML o Helm.
3. Haga clic en **Cerrar**.

Para obtener más información, consulte Instalar el agente Citrix ADM en el clúster de Kubernetes.

Utilice el agente integrado en la instancia de Citrix ADC

Las instancias de Citrix ADC de su entorno incluyen un agente integrado. Puede iniciar el agente integrado y utilizarlo para establecer la comunicación entre la instancia y Citrix ADM.

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



   Para obtener instrucciones detalladas sobre cómo iniciar el agente integrado en su instancia de Citrix ADC, consulte Iniciar el agente integrado en la instancia de Citrix ADC.

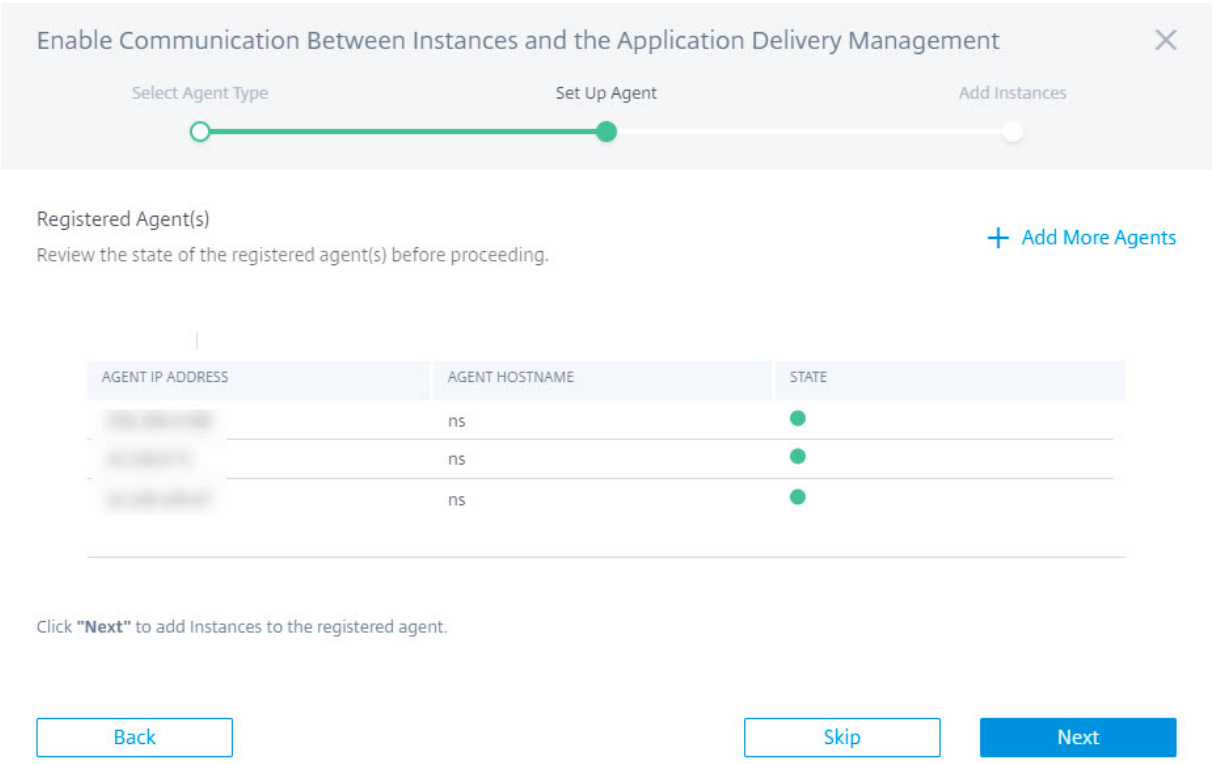
2. Una vez iniciado el agente integrado, vuelva a la página **Configurar agente** y haga clic en **Registrar instancia**.

Paso siguiente: Agregar instancias.

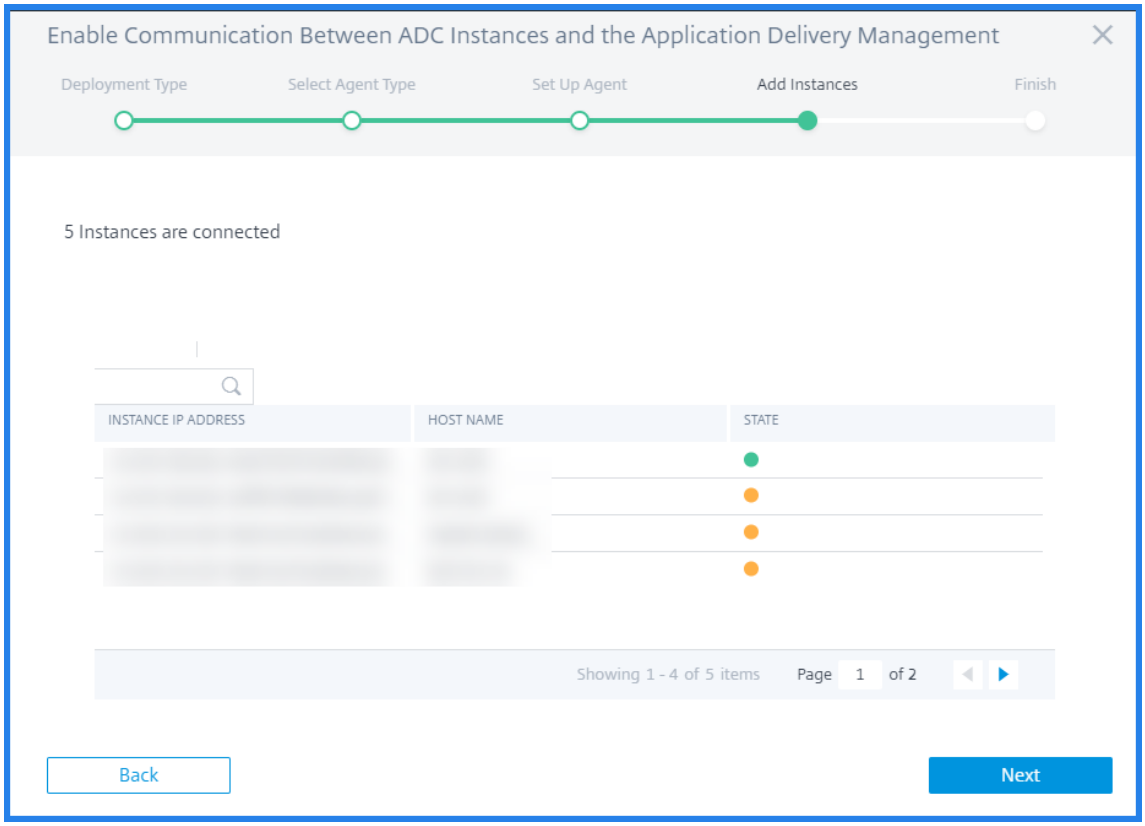
Agregar instancias a Citrix ADM

Las instancias son dispositivos de red o dispositivos virtuales que quiere detectar, administrar y supervisar desde Citrix ADM. 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**, vea las instancias de ADC conectadas al agente registrado. Asegúrese de que la instancia esté en estado **Activo** y haga clic en **Siguiente**.



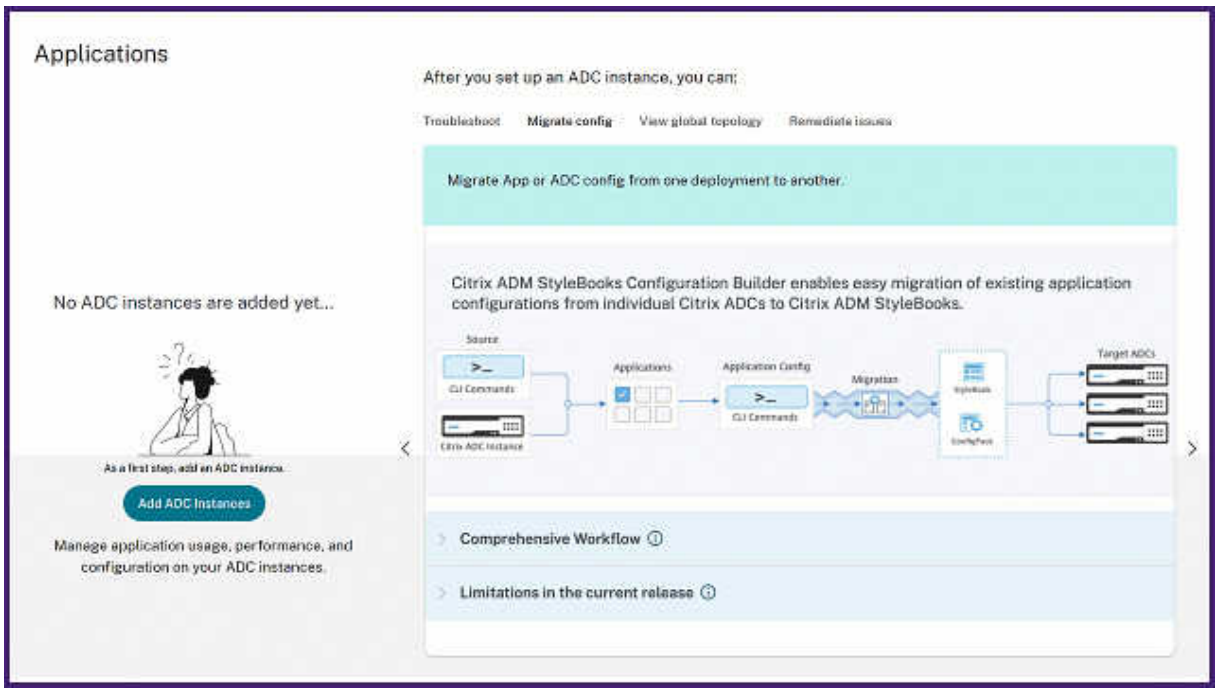
2. Haga clic en **Listo** para completar la configuración inicial y comenzar a administrar la implementación.

> **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 Citrix ADM, consulte Agregar instancias.

Instancias ADC integradas mediante el panel de interfaz gráfica de usuario de Citrix ADM

Si omitió la incorporación de las instancias de ADC en el flujo de trabajo de introducción al configurar Citrix ADM por primera vez, puede incorporar las instancias desde el panel de la GUI de Citrix ADM. Si las instancias de ADC aún no se han agregado, la GUI le pedirá 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 administrar mejor las instancias de ADC mediante Citrix ADM.

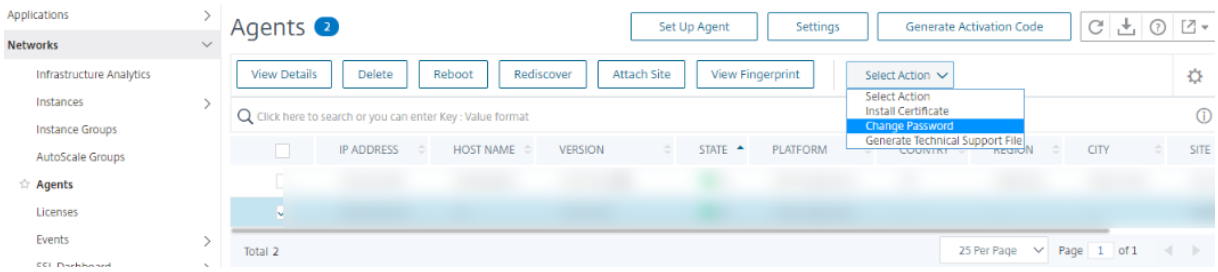


Haga clic en **Agregar instancias de ADC** para incorporar las instancias. Se **reinicia** el flujo de trabajo de introducción. Siga los pasos del paso 3: Seleccione un tipo de implementación de ADC en adelante, que se indican en este documento, para incorporar las instancias.

Si las instancias de ADC ya están incorporadas, después de iniciar sesión en Citrix ADM, solo verá la página de inicio de Citrix ADM con la barra de navegación a la izquierda.

Acciones del agente

Después de configurar su Citrix ADM, 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.

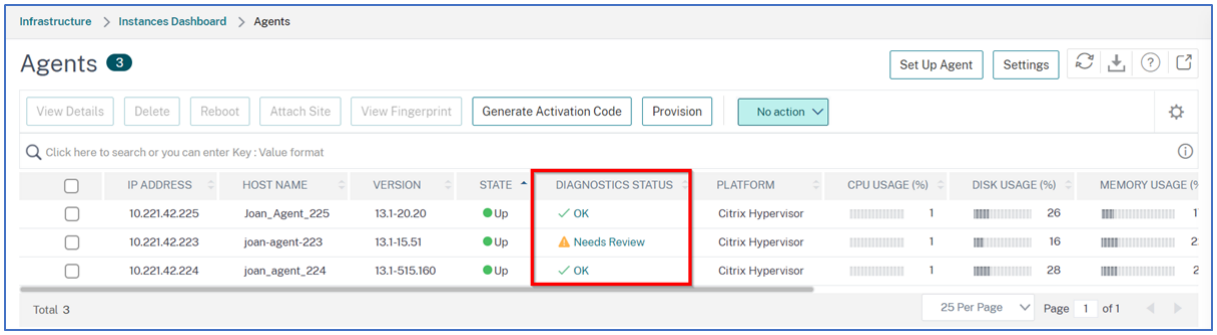
- **Generar un archivo de soporte técnico**: genere un archivo de soporte técnico para un agente de Citrix ADM seleccionado. Puede descargar este archivo y enviarlo al soporte técnico de Citrix para su investigación y solución de problemas.

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

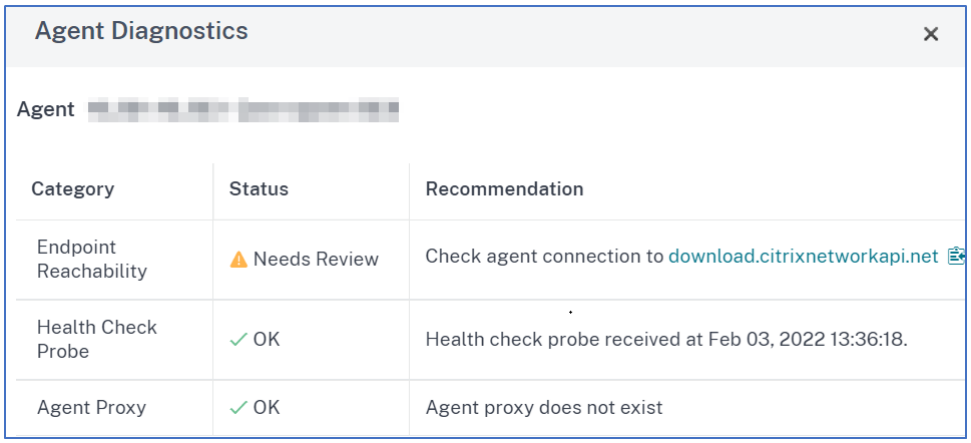
Citrix ADM realiza una comprobación de diagnóstico periódica (cada una hora) para el agente y proporciona la siguiente información:

- **Accesibilidad de** los puntos finales: comprueba si se puede acceder a todos los puntos finales. El agente ADM usa varios puntos finales para la comunicación entre las instancias de ADM y ADC. 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.



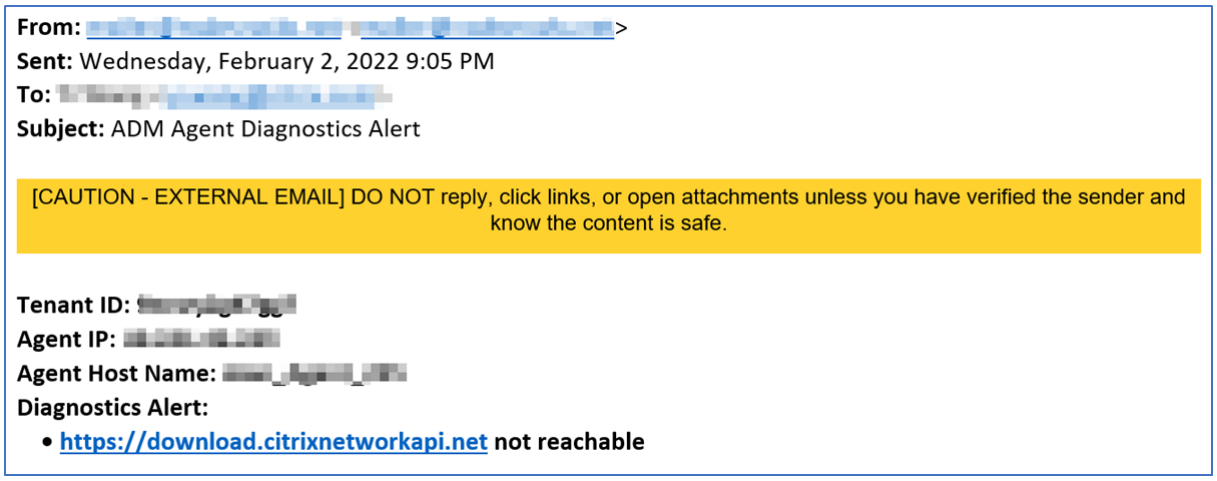
- **Categoría**. Proporciona la categoría del problema.

- **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

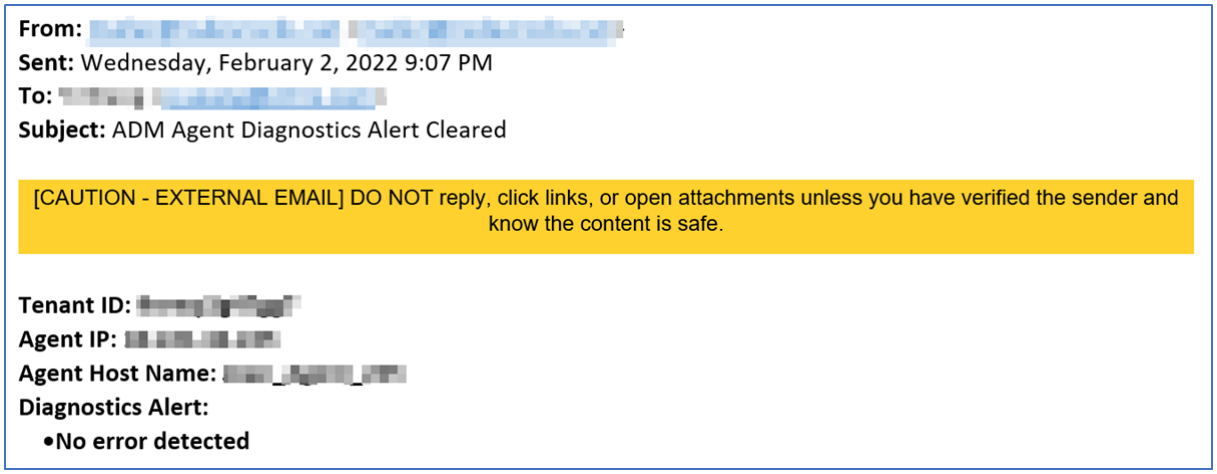
El siguiente ejemplo es una notificación por correo electrónico después de que el estado de accesibilidad del punto final haya cambiado de **OK** a **Needs Review**:


From: [redacted]>
Sent: Wednesday, February 2, 2022 9:05 PM
To: [redacted]
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: [redacted]
Agent IP: [redacted]
Agent Host Name: [redacted]
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: [redacted]
Sent: Wednesday, February 2, 2022 9:07 PM
To: [redacted]
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: [redacted]
Agent IP: [redacted]
Agent Host Name: [redacted]
Diagnostics Alert:
- **No error detected**

Configurar el agente integrado ADC para administrar instancias

November 17, 2022

Hay un agente integrado disponible en las instancias de Citrix ADC MPX, VPX, Gateway que ejecutan la versión `12.1.48.13` y versiones posteriores, y en las instancias de Citrix ADC 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 ADC 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 Citrix ADM.

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

El agente integrado es ideal para implementaciones de pares de alta disponibilidad o independientes ADC más pequeños. Si tiene varias instancias ADC, 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.

Citrix ADM admite la administración y la supervisión de las instancias de Citrix ADC 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 Citrix ADC, asegúrese de lo siguiente:

- La instancia de Citrix ADC (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 Citrix ADC.

  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.

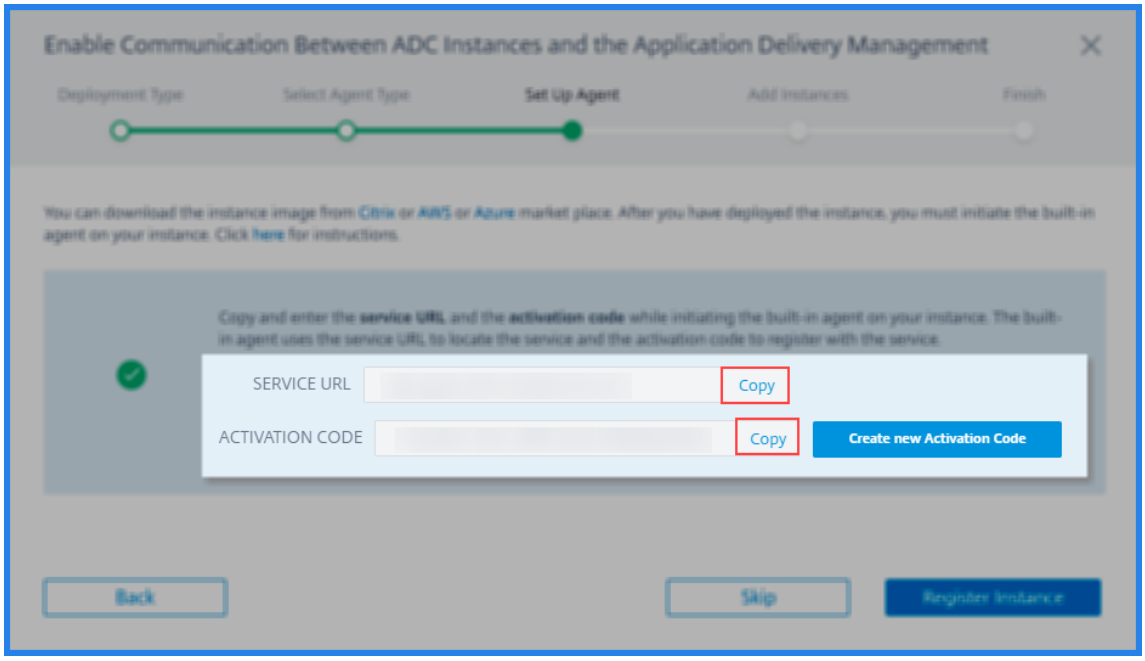
> **Nota**
>
> Para obtener toda la información relacionada con los puertos y otros requisitos del sistema, consulte Requisitos del sistema.

Configurar el agente integrado

Realice las siguientes tareas para configurar el agente integrado de ADC:

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 Citrix ADC. Para obtener más información, consulte Acceder a un Citrix ADC.

   b) Desplácese hasta el `/var/mastools/scripts` directorio y escriba el siguiente comando:

   En la instancia de SDX


```
./mastools_init.sh <user_name> <service-url> <activation-code>
    -sdx
<!--NeedCopy-->
```

- En<user_name>, introduzca el nombre de usuario de Citrix ADC.

```
./mastools_init.sh <device-profile-name> <service-url> <
   activation-code> -sdx -profile

<!--NeedCopy-->
```

> Nota:
>
> Citrix ADM descubre todas las instancias VPX que se ejecutan en ese SDX y usted no tiene que 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 ADC es inferior a 13.0 61.x o 12.1 57.x, debe comprobar la versión `mastools` 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 que se indican a continuación, dependiendo de la versión del software.

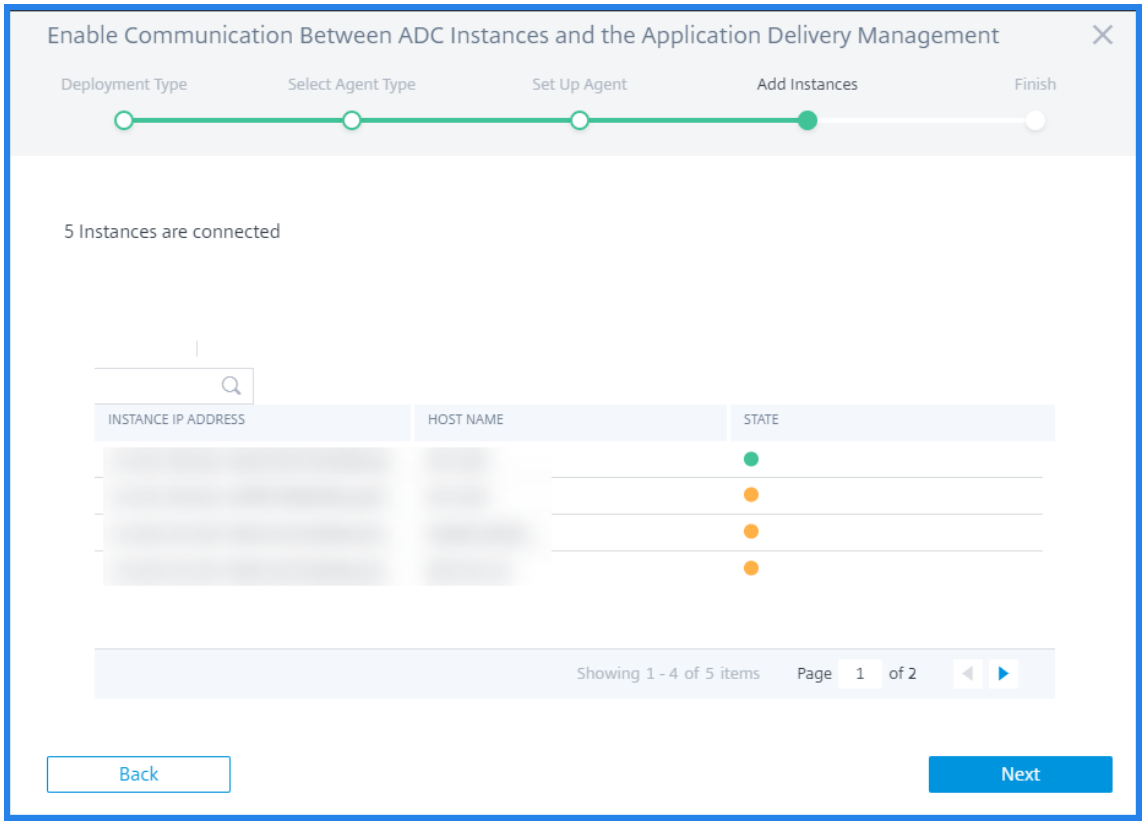
Versión de imagen ADC	¿Es mastools_version `0.0-0.0`?	Comando para el registro con perfil	Comando para el registro sin perfil
Menos de 13,0 61.xx y 12.1 57,xx	Sí	`./mastools_init.sh < device_profile_nam > <service_url> "MAS;< activation_code> "-profile`	`./mastools_init.sh <user_name> < pwd> < service_url> " 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>`

Versión de imagen ADC	¿Es mastools_version 0.0-0.0?	Comando para el registro con perfil	Comando para el registro sin perfil
Más de 13,0 61.x y 12.1 57.xx	No aplicable	`./mastools_init.sh <device_profile_nam> <service_url> <activation_code> -profile`	`./mastools_init.sh <user_name> <pwd> <service_url> <activation_code>`

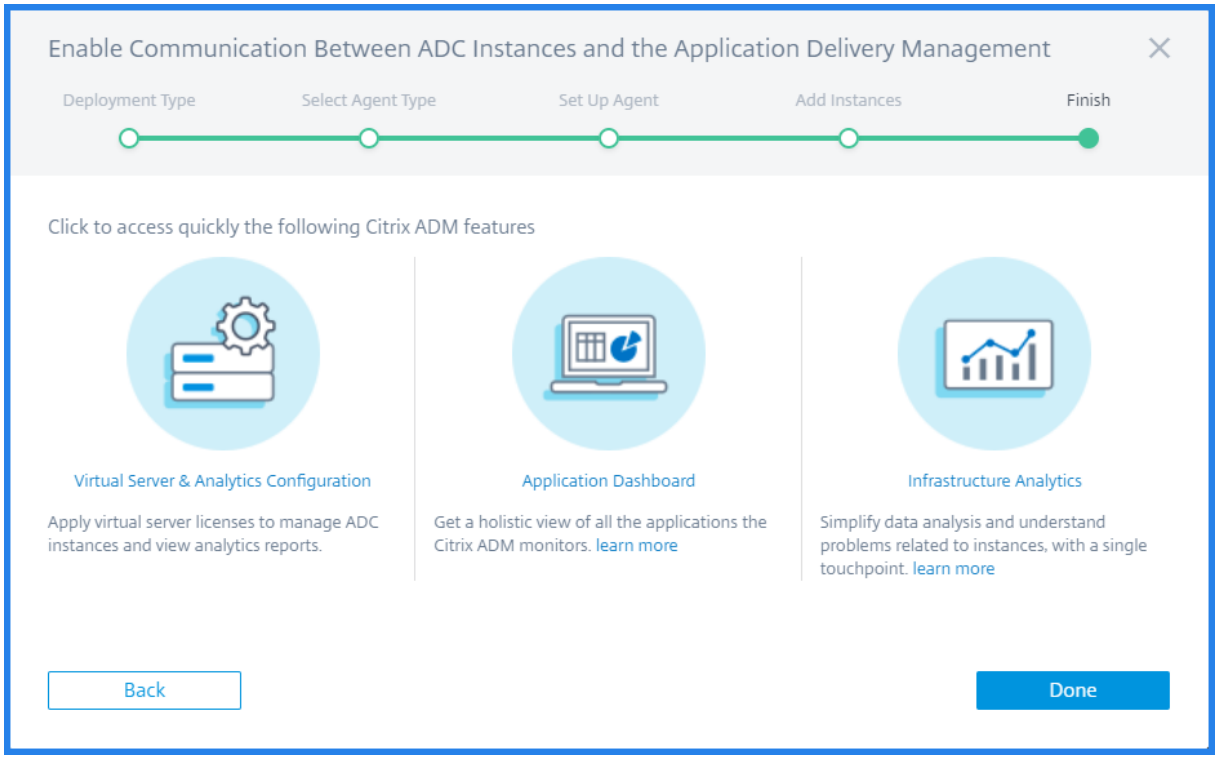
- En`<user_name>`, introduzca el nombre de usuario de Citrix ADC.

> **Nota**
>
> En un par HA, complete el registro en el nodo principal. Si ejecuta el registro en el nodo secundario, aparece el siguiente mensaje:
>
> **Ejecute el comando de registro en el nodo principal.**

4. Vuelva a la página Citrix ADM 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 está en el estado **Arriba** y haga clic en **Siguiente**.



6. Haga clic en **Listo**.



Tras configurar correctamente el agente integrado, puede acceder a las funciones de Citrix ADM, como:

- **Servidor virtual y análisis** : aplique licencias a su servidor virtual para administrar las instancias de ADC. 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** . Copia y pega la URL y el código de activación en una instancia de ADC y descubre esa instancia.

Una vez iniciado el agente integrado, vaya a **Infraestructura > Instancias > Citrix ADC**. 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 Citrix ADM.

- 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 Citrix ADM, compruebe:
  - **MastOols_Upgrade** registra `/var/mastools/logs/mastools_upgrade.log`
  - **Inicia sesión binaria**`/var/log/mastoolsd.log`.

Instalación de un agente local

November 16, 2022

El agente funciona como intermediario entre el Citrix ADM 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.

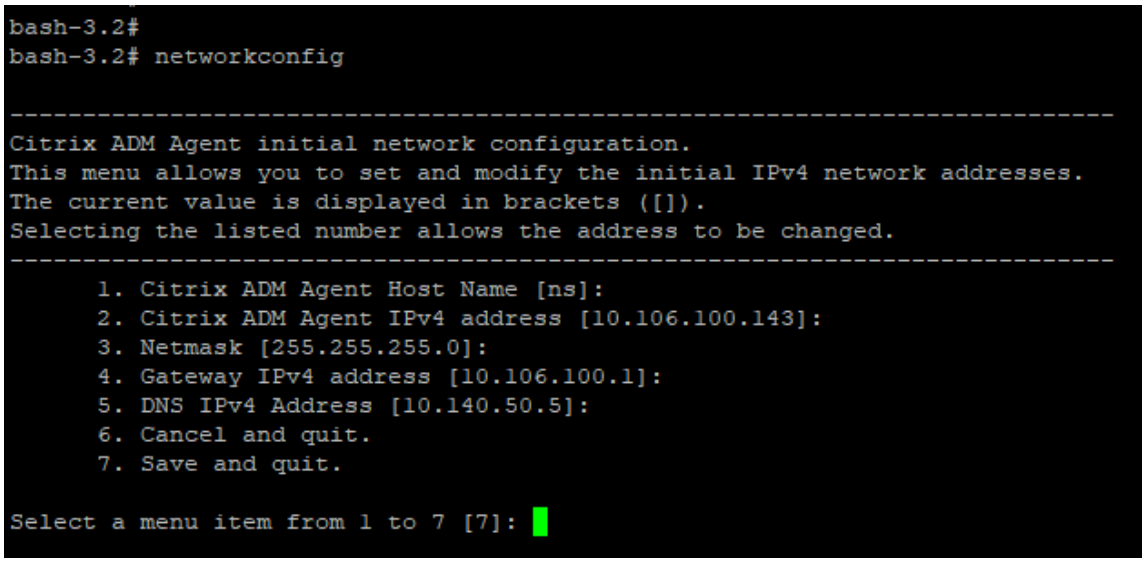
Para instalar el agente Citrix ADM:

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 su DNS para permitir el acceso a Internet a su agente Citrix ADM.

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 quiere cambiar la configuración de red configurada en el agente, escriba el comando `networkconfig` y siga las instrucciones de la CLI.

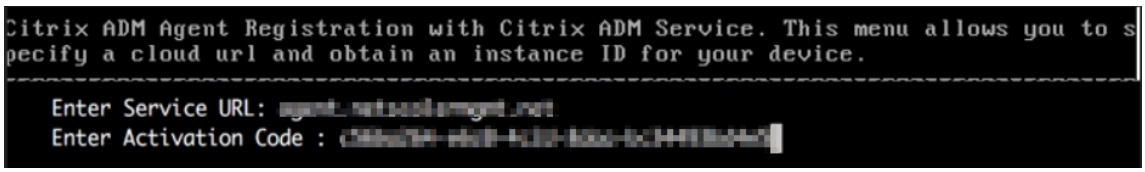


5. Si no se le pide que introduzca la URL del servicio, desplácese hasta /mps en el agente Citrix ADM y, a continuación, ejecute cualquiera de los siguientes scripts:

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

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

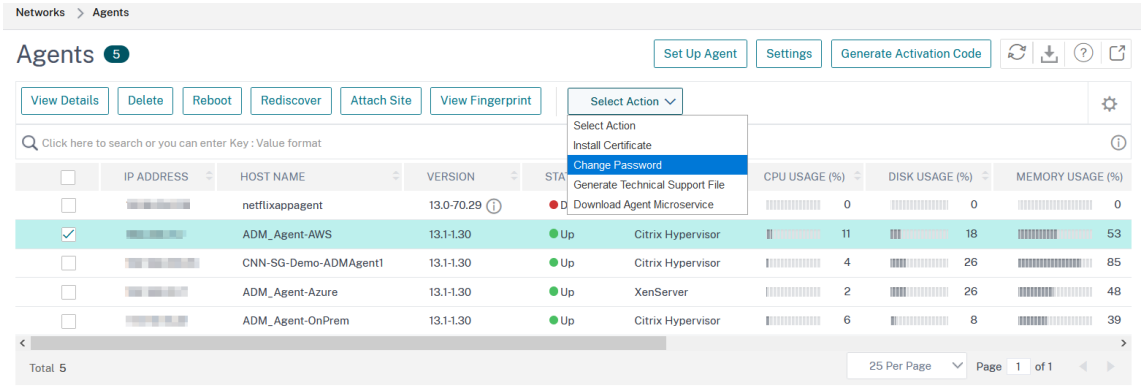
6. Introduzca la **URL del servicio** y el **código de activación** que guardó al descargar la imagen del agente. El agente usa la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.



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 Citrix ADM 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 en la nube de Microsoft Azure

November 16, 2022

El agente funciona como intermediario entre el Citrix ADM y las instancias administradas en el centro de datos empresarial o en la nube.

Para instalar el agente de Citrix ADM en la nube de Microsoft Azure, debe crear una instancia del agente en la red virtual. Obtenga la imagen del agente de Citrix ADM de Azure Marketplace y, a continuación, use el portal de Azure Resource Manager para crear el agente.

Antes de comenzar a crear la instancia del agente de Citrix ADM, asegúrese de haber creado una red virtual con las subredes necesarias en las que residirá 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

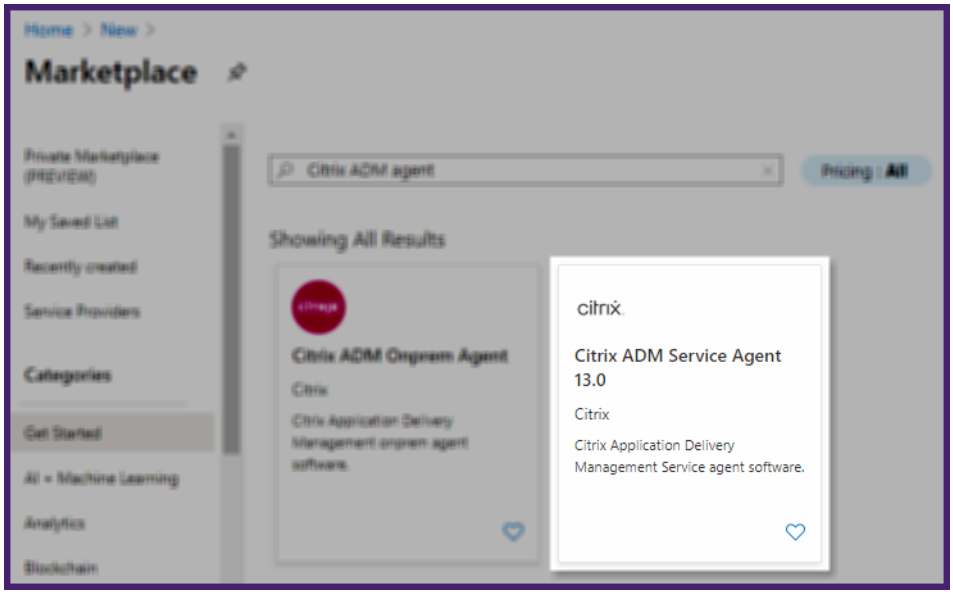
Asegúrese de que tiene lo siguiente:

- Una cuenta de usuario de Microsoft Azure
- Acceso al Administrador de recursos de Microsoft Azure

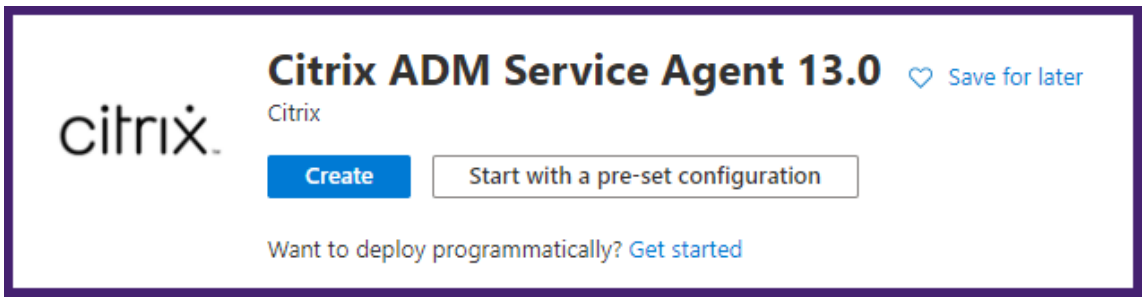
> **Nota**
>
> - Citrix recomienda crear grupos de recursos, grupos de seguridad de red, redes virtuales y otras entidades antes de aprovisionar la máquina virtual del agente Citrix ADM, de modo que la información de red esté disponible durante el Provisioning.
> - Para que el agente de Citrix ADM se comunique con Citrix ADM y las instancias de Citrix ADC, asegúrese de que los puertos recomendados estén abiertos. Para obtener información completa sobre los requisitos de puertos para el agente Citrix ADM, consulte Puertos.

Para instalar el agente Citrix ADM 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 `Citrix ADM agent` en la barra de búsqueda y seleccione el **agente Citrix ADM**.



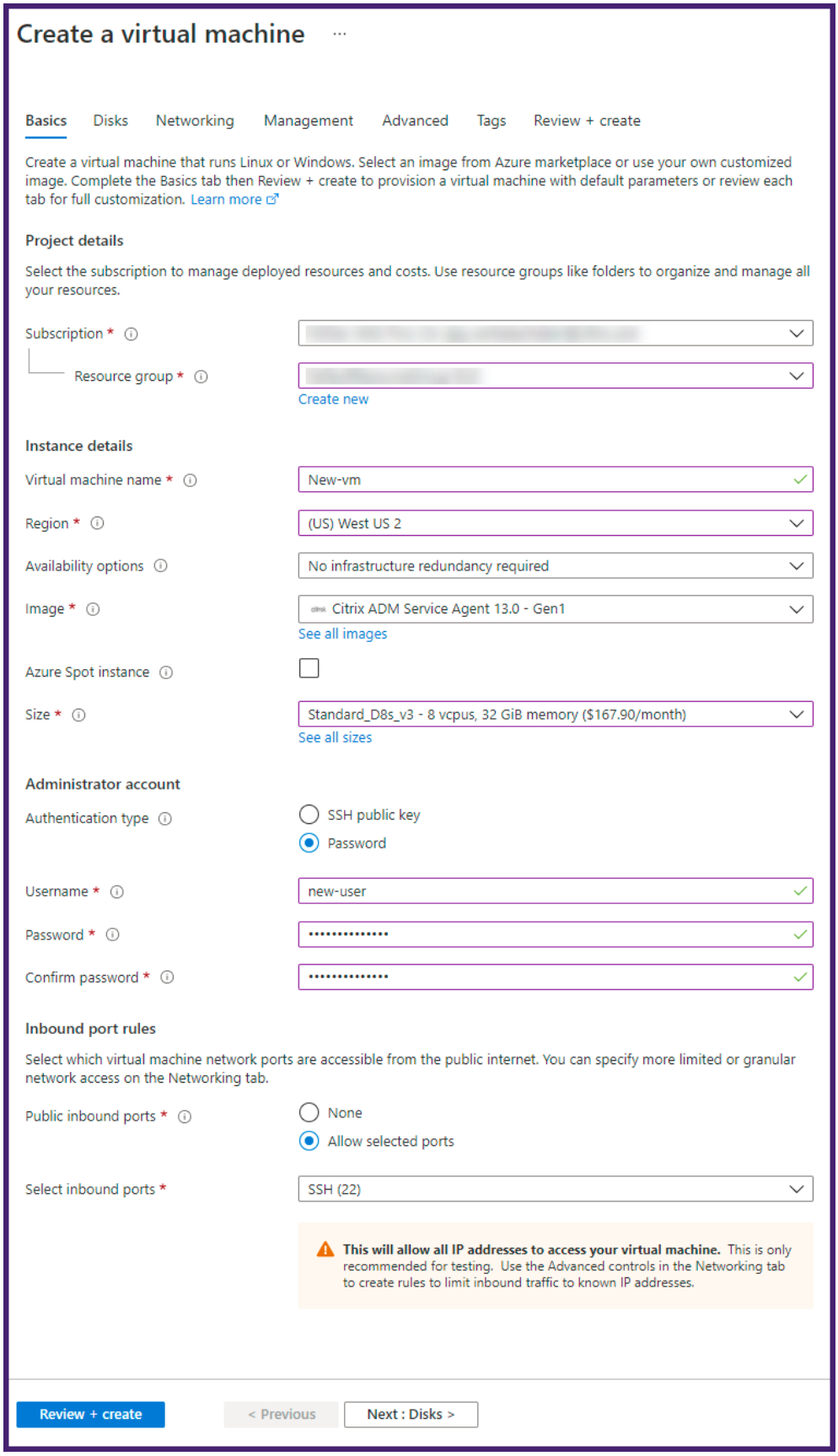
4. Haga clic en **Crear**.



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 punto, pero Citrix recomienda que cree un grupo de recursos a partir de Grupos de recursos en el Azure Resource Manager y, a continuación, seleccione el grupo en la lista desplegable.

- **Nombre de máquina virtual** : especifique un nombre para la instancia del agente de Citrix ADM.
- **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 Citrix ADM.

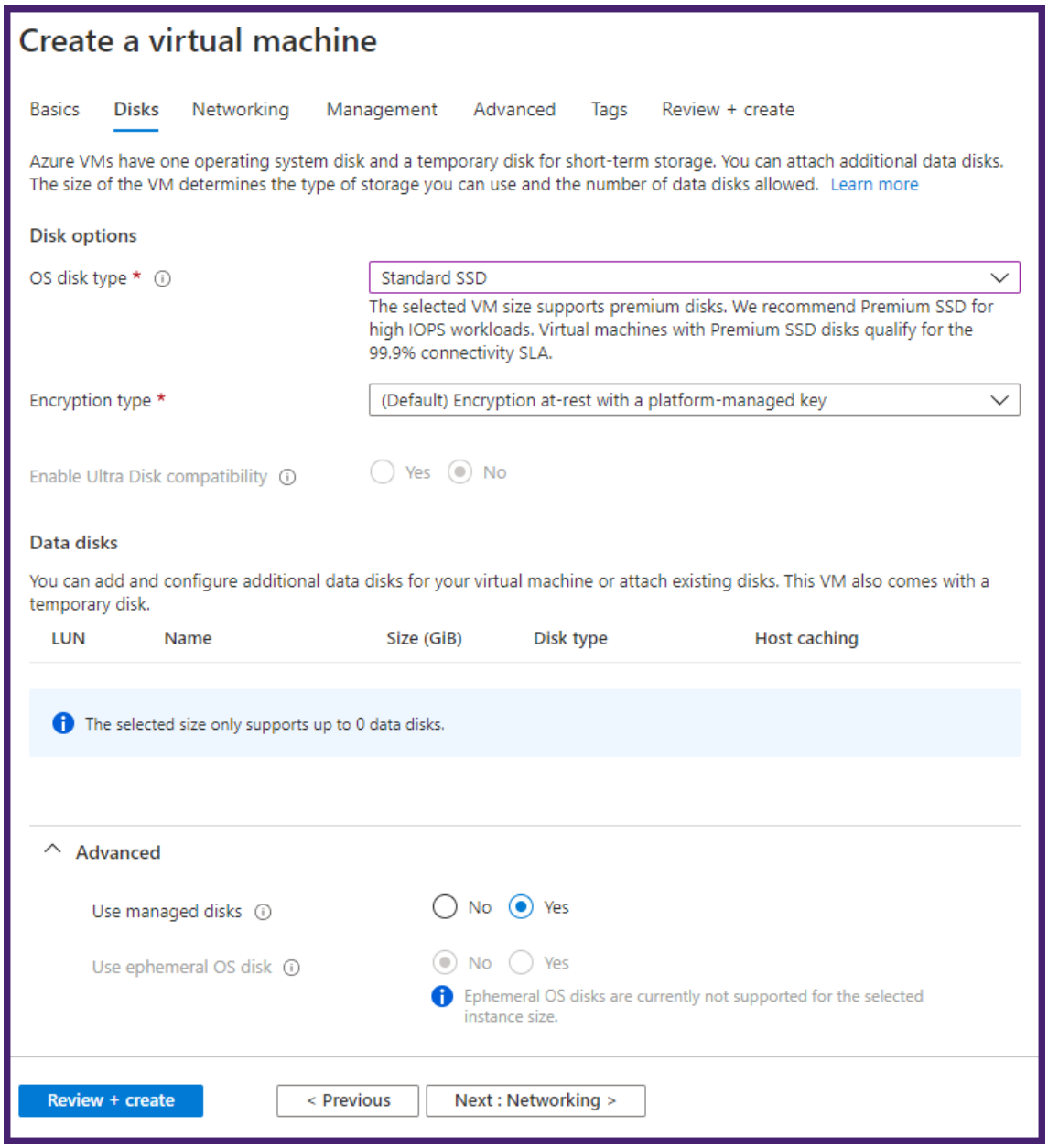
  Seleccione el tipo de disco virtual compatible (**HDD** o **SSD**) de la lista.

  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** Citrix recomienda 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:

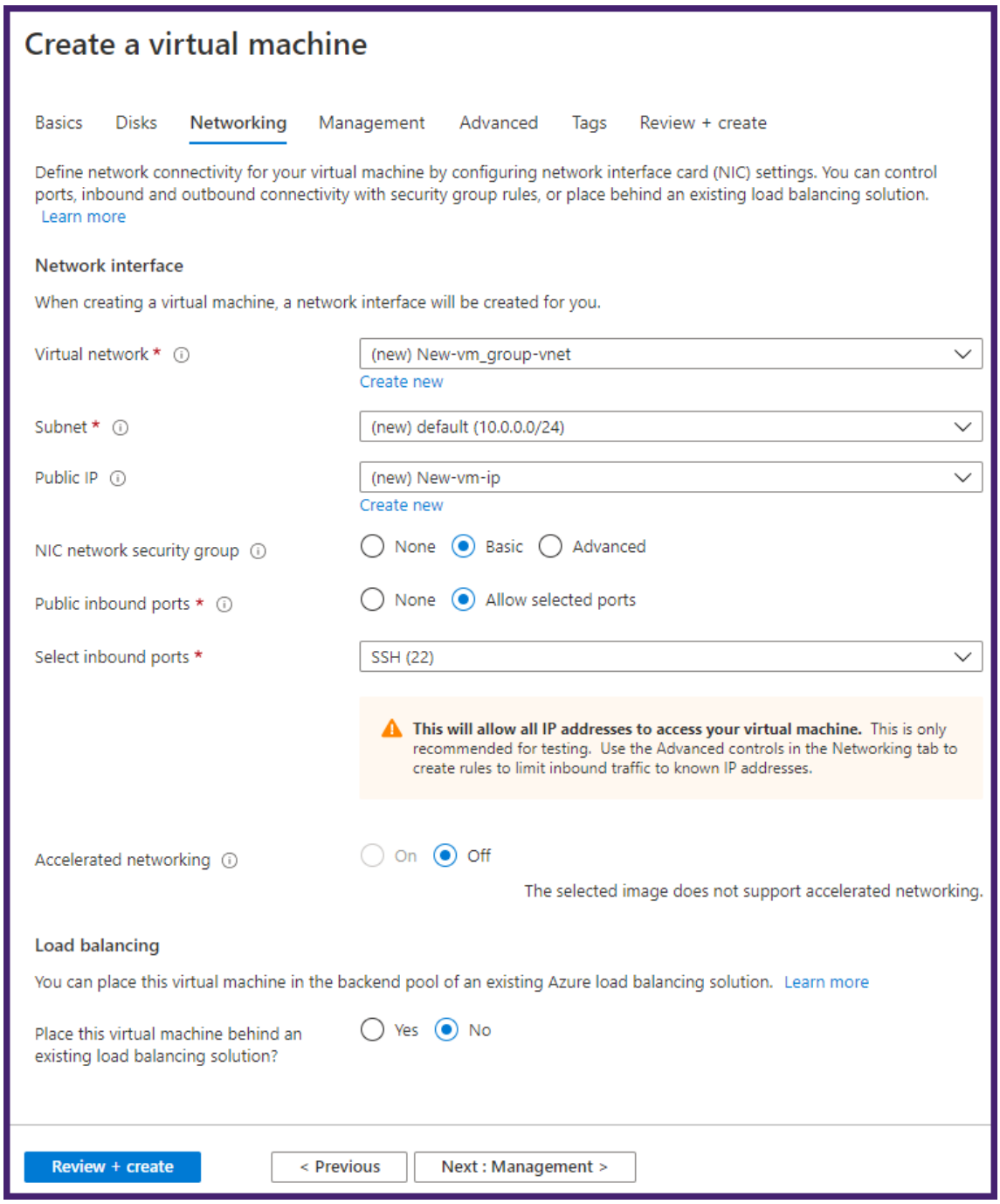
En esta ficha, especifique **las opciones de disco** y **Discos de datos**.



- **Tipo de disco de SO** : seleccione el tipo de disco virtual (HDD o SSD).

Redes:

Especifique los detalles de red requeridos:



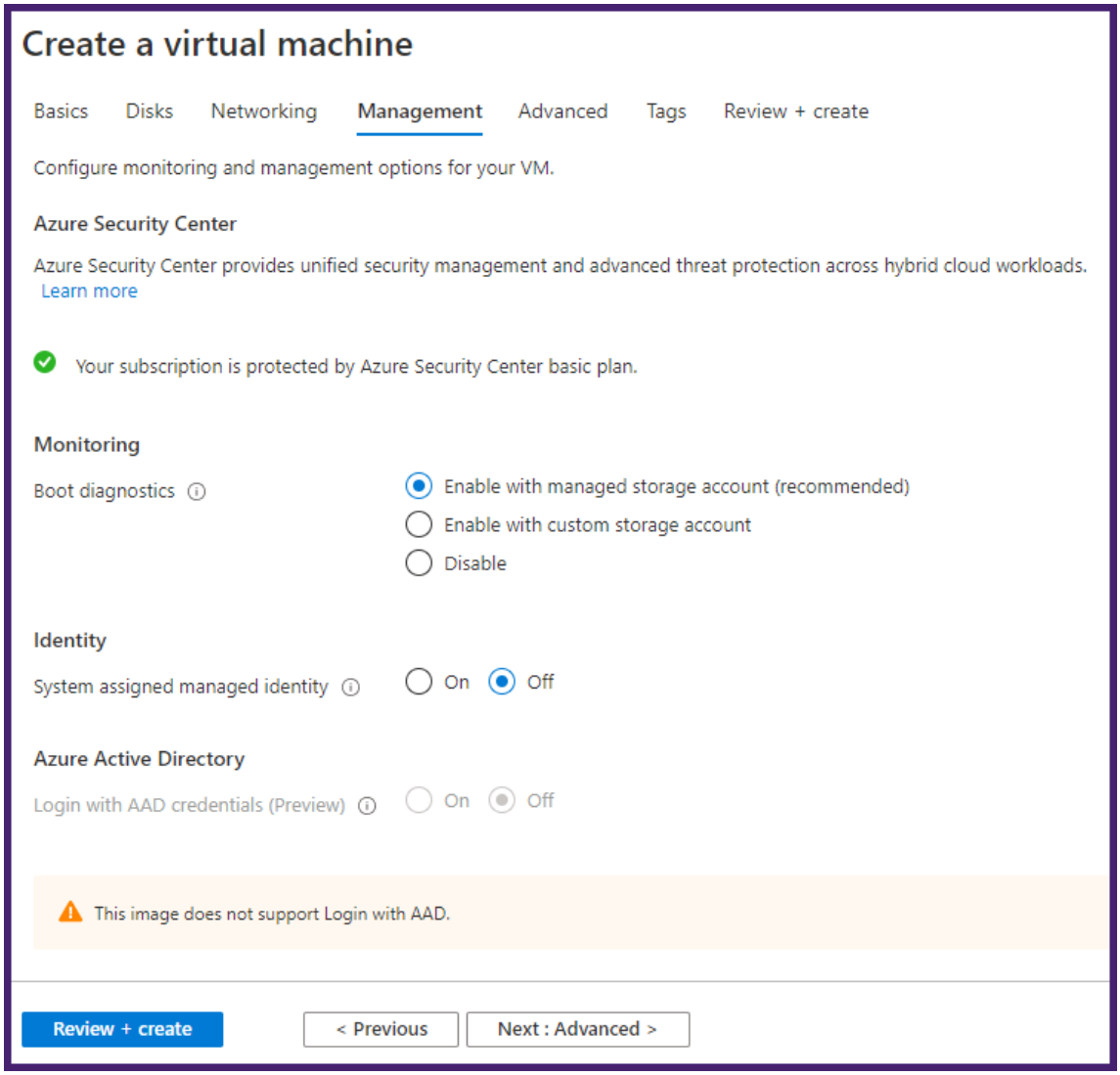
- **Red virtual**: Seleccione la red virtual.
- **Subred** : defina la dirección de la subred.
- **Dirección IP pública** : opcional, seleccione la dirección IP.
- **Grupo de seguridad de red** : si lo quiere, seleccione el grupo de seguridad que ha creado.
- **Seleccionar puertos entrantes** : si permite 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.

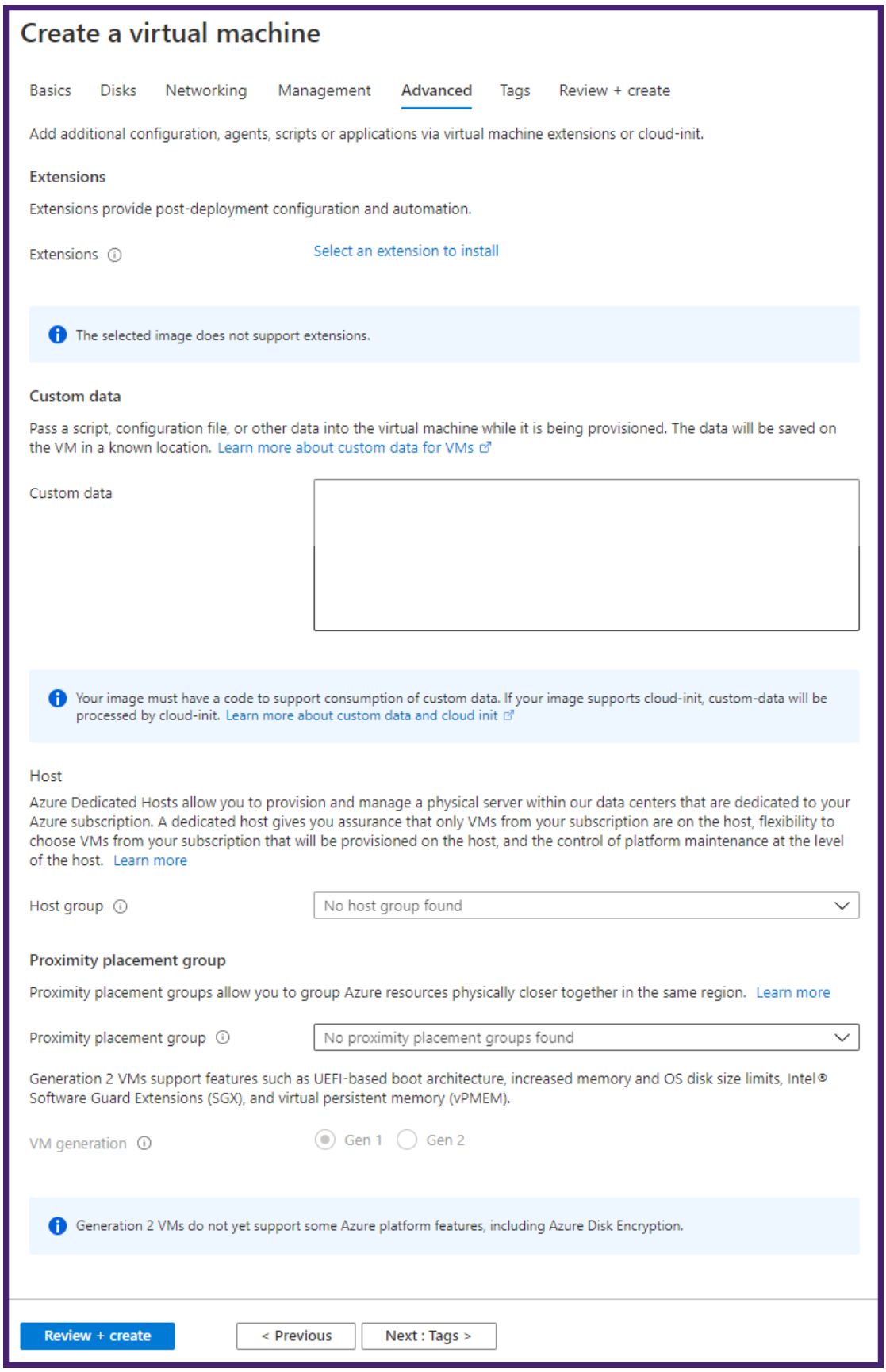
Gestión:

Especifique el **Centro de seguridad de Azure**, **la supervisión**y la **identidad**.



Avanzado:

Opcional, especifique el **grupo de ubicación**Extensiones**,**Datos personalizados**y Proximidad**.

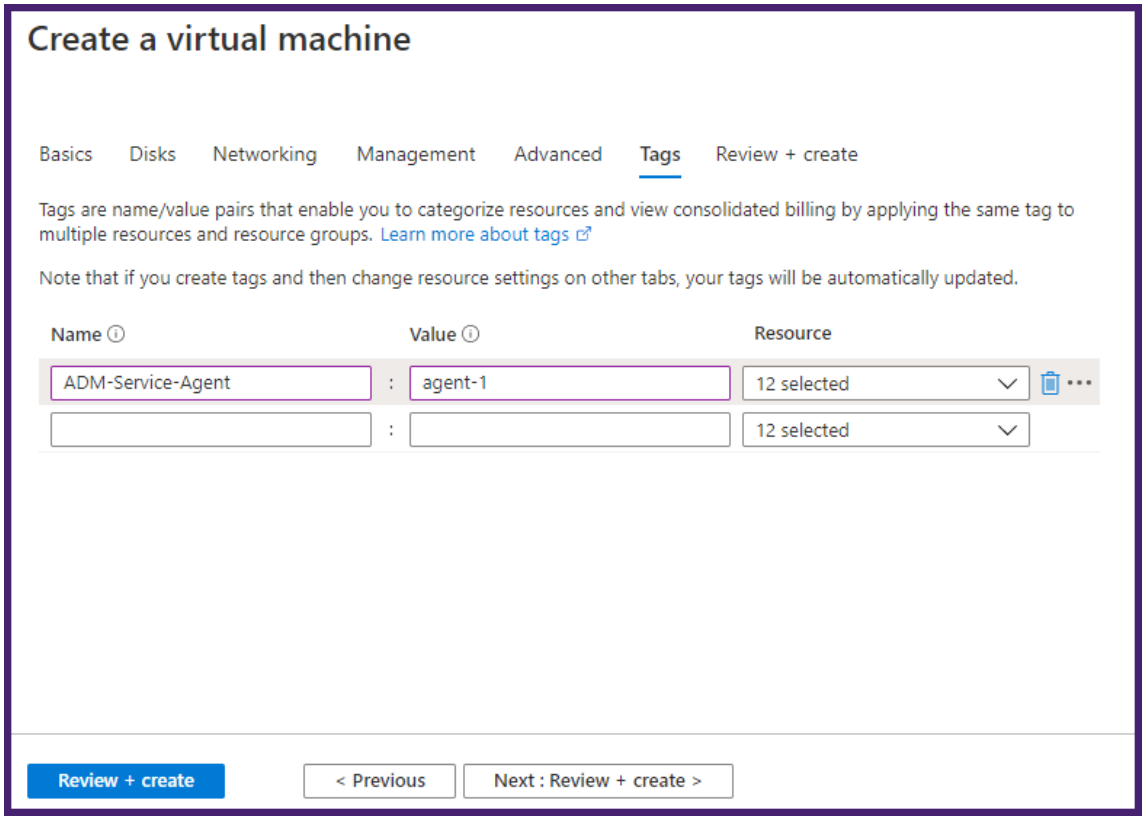


> **Nota:**
>
> En **Datos personalizados**, especifique la **URL del servicio** y el **código de activación** que copió de la página **Configurar agentes** de Citrix ADM, tal como se indica en la sección Introducción. Introduzca los detalles en el siguiente formato:
>
> ```
> registeragent -serviceurl <apigatewayurl> -activationcode <
>    activationcodevalue>
> <!--NeedCopy-->
> ```
>
> El agente usa esta información para registrarse automáticamente en Citrix ADM durante el arranque.

Si especifica este script de registro automático, omita los pasos 7 y 8.

Etiquetas:

Escriba el par clave-valor de las etiquetas del agente Citrix ADM. 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 Citrix ADM.

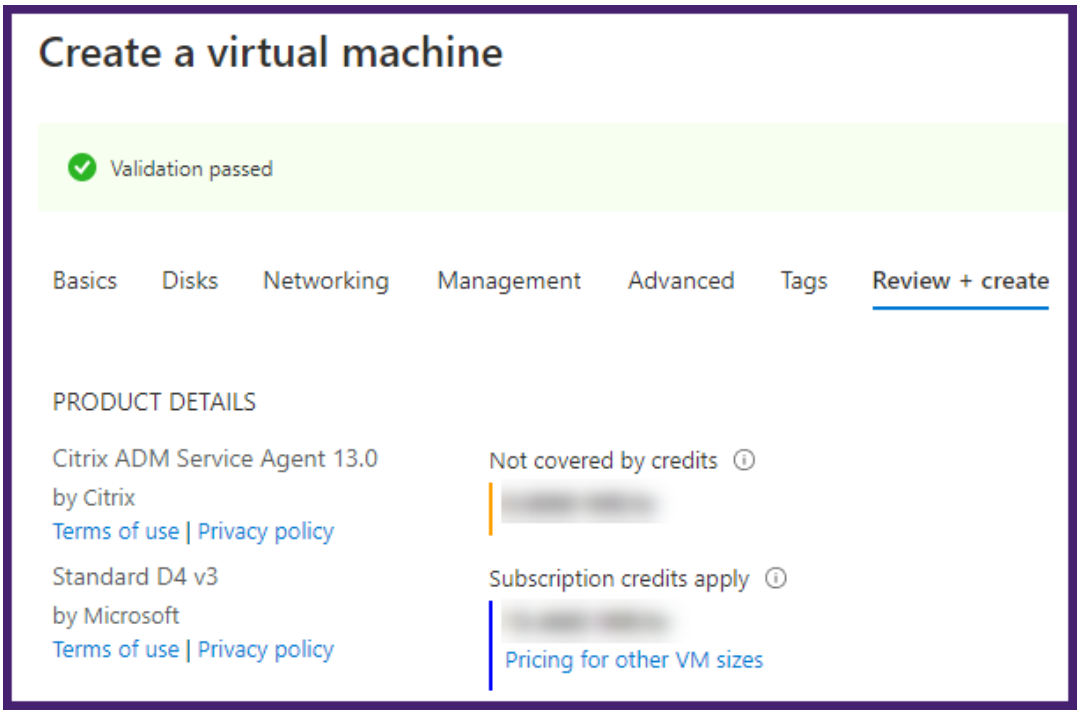


Los parámetros de configuración se validan y la ficha **Revisar y crear** muestra el resultado de la validación.

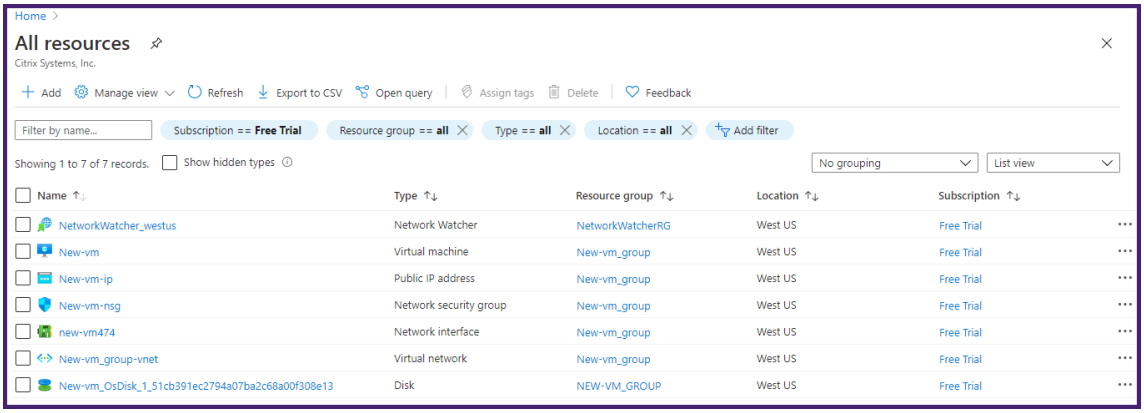
- Si la validación falla, esta ficha muestra el motivo del error. Vuelva a la sección en particular

y realice los cambios necesarios.

- Si la validación pasa, haga clic en **Crear**. Comienza el proceso de despliegue del agente.



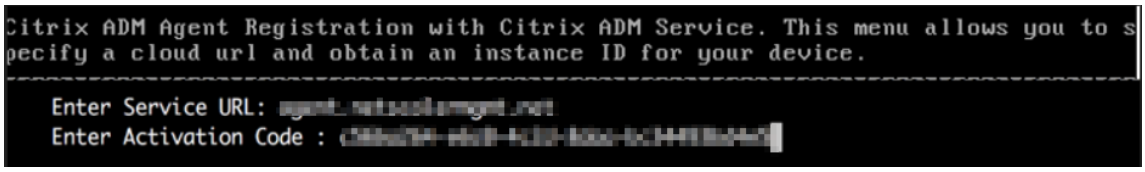
El proceso de implementación puede tardar entre 10 y 15 minutos aproximadamente. Una vez que la implementación se haya completado correctamente, puede ver la máquina virtual del agente Citrix ADM en su cuenta de Microsoft Azure.



6. Una vez que el agente esté en funcionamiento, mediante un cliente SSH, inicie sesión en su agente Citrix ADM con el nombre de usuario y la contraseña especificados. Desde el cliente SSH, también puede iniciar sesión con los siguientes nombres de usuario:

   - `nsrecover` - la contraseña por defecto es `nsroot`.
   - `nsroot` - utilice la clave pública SSH. Asegúrese de haber especificado la clave pública durante la creación de la máquina virtual.

7. Introduzca el siguiente comando para invocar la pantalla de despliegue: **deployment_type.py**.
8. Introduzca la **URL del servicio** y el **código de activación** que copió y guardó en la página **Configurar agentes** de Citrix ADM, tal como se indica en la sección Introducción. 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 Citrix ADM y, en la página **Configurar agente**, en **Agentes detectados**, compruebe el estado del agente.

Instalación de un agente en Amazon Web Services (AWS)

November 16, 2022

El agente Citrix ADM funciona como intermediario entre Citrix ADM y las instancias detectadas en el centro de datos o en la nube.

Requisitos previos

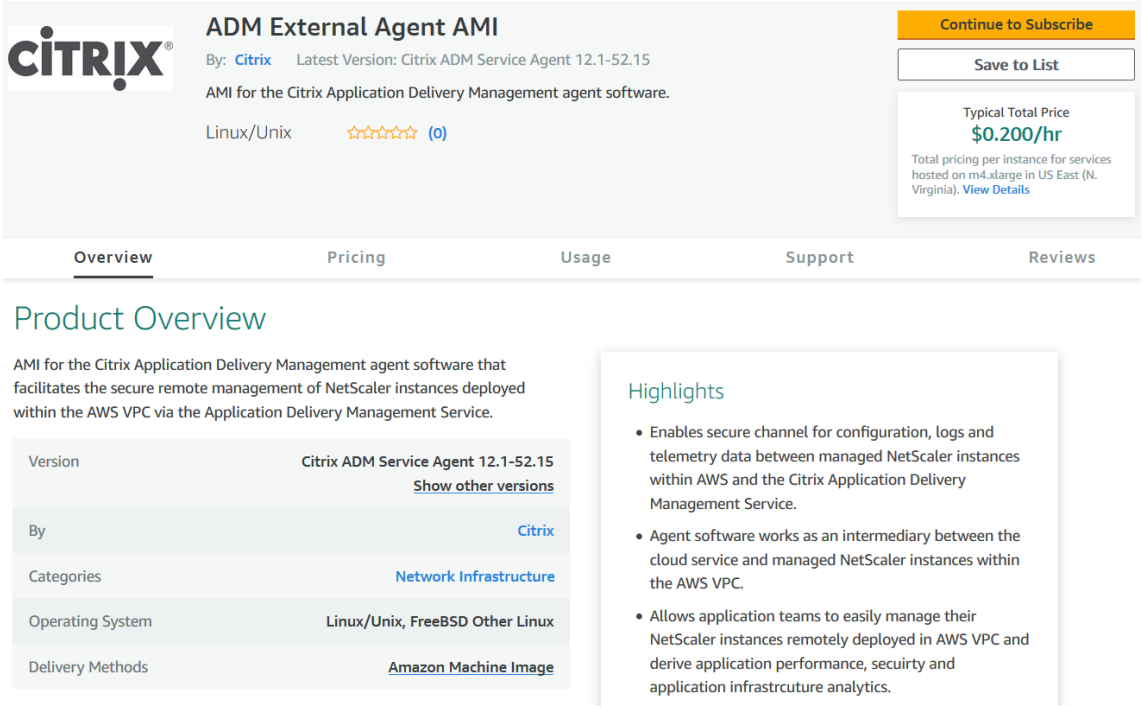
Para lanzar una AMI de agente de Citrix ADM dentro de una nube privada virtual (VPC) de Amazon Web Services (AWS) mediante la GUI de Amazon, necesita:

- Una cuenta de AWS
- Una nube privada virtual (VPC) de AWS
- Una cuenta de IAM

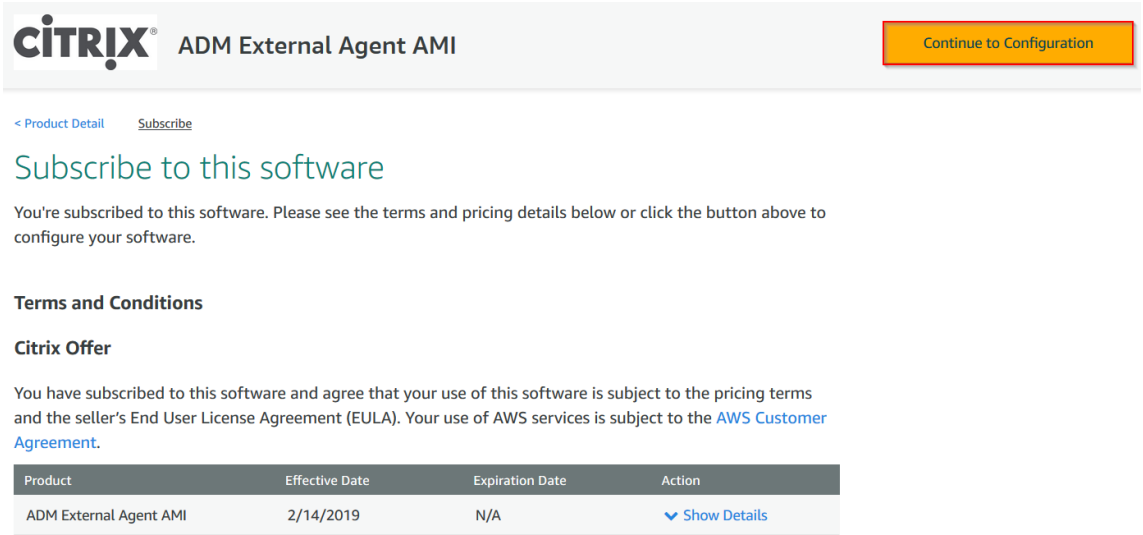
> **Nota**
>
> - Antes de aprovisionar una máquina virtual con un agente Citrix ADM, Citrix recomienda crear un grupo de seguridad, una red privada virtual, un par de claves, una subred y otras entidades. Por lo tanto, la información de red está disponible durante el aprovisionamiento.
> - Para que un agente Citrix ADM se comunique con Citrix ADM y las instancias de Citrix ADC, asegúrese de que los puertos recomendados estén abiertos. Para obtener más información sobre los requisitos de puertos para un agente Citrix ADM, consulte Puertos.

Para instalar el agente Citrix ADM en AWS:

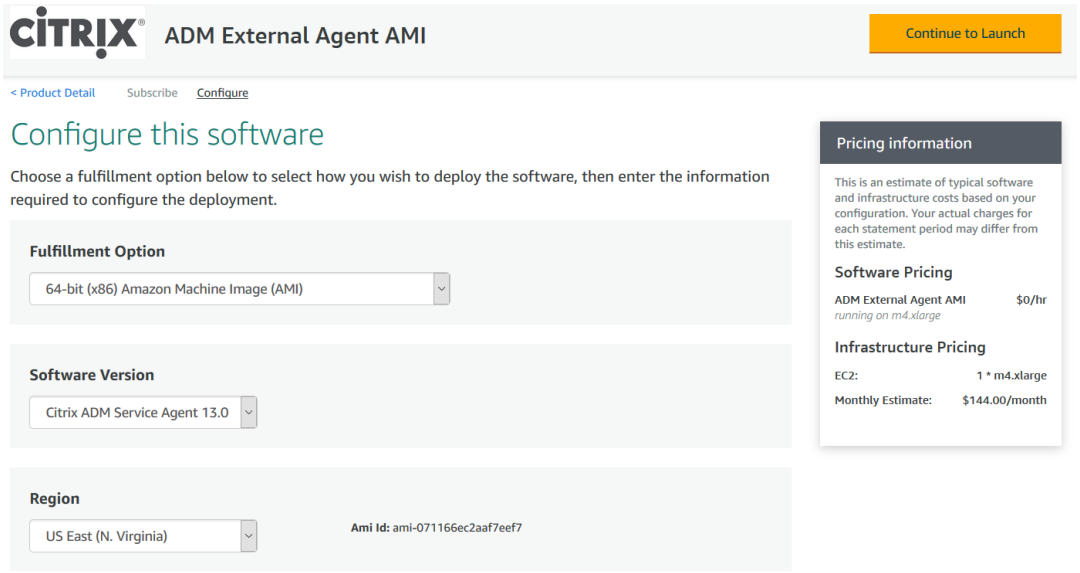
1. Inicie sesión en el mercado de AWS mediante sus credenciales de AWS.
2. En el campo de búsqueda, escriba el **agente Citrix ADM** para buscar la AMI del agente Citrix ADM y haga clic en **Ir**.
3. En la página de resultados de la búsqueda, haga clic en la **AMI del agente externo de Citrix ADM** de la lista disponible.
4. En la página **AMI del agente externo de Citrix ADM**, haga clic en **Continuar para suscribirse**.



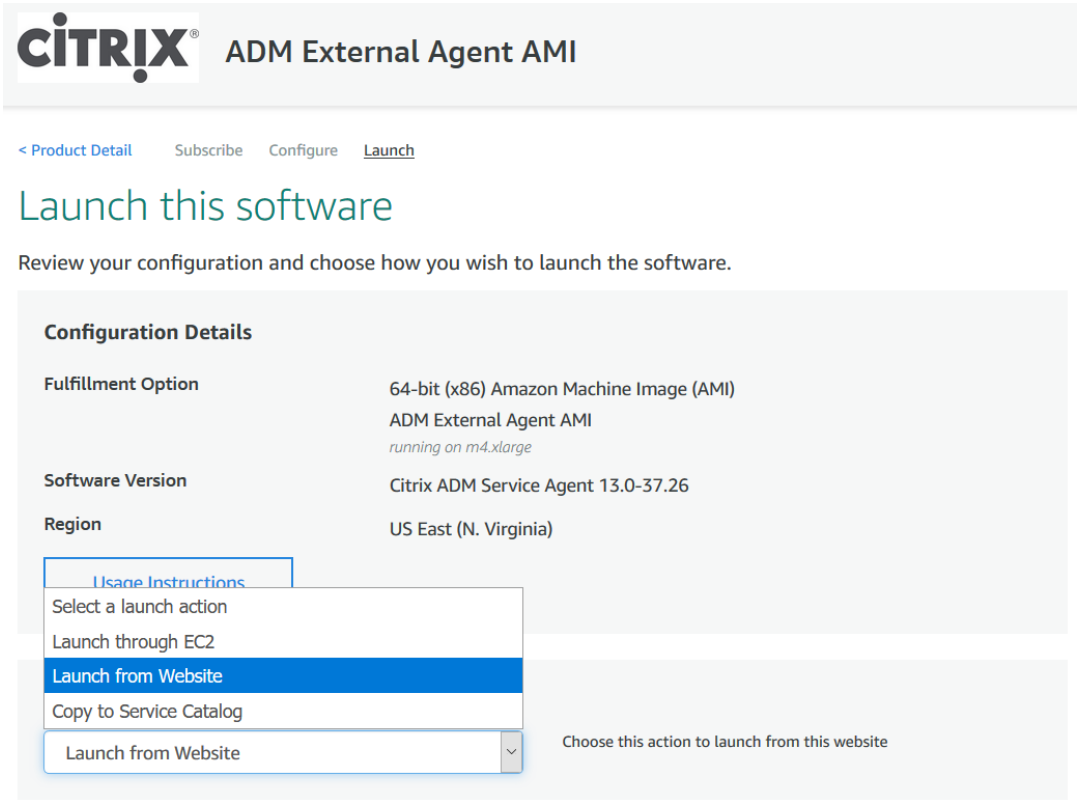
5. Cuando la suscripción se haya realizado correctamente, haga clic en **Continuar con la configuración**.



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 Citrix ADM en la lista de **versiones de software** .
   c) Selecciona tu región en la lista de **regiones** .
   d) Haga clic en **Continuar para iniciar**



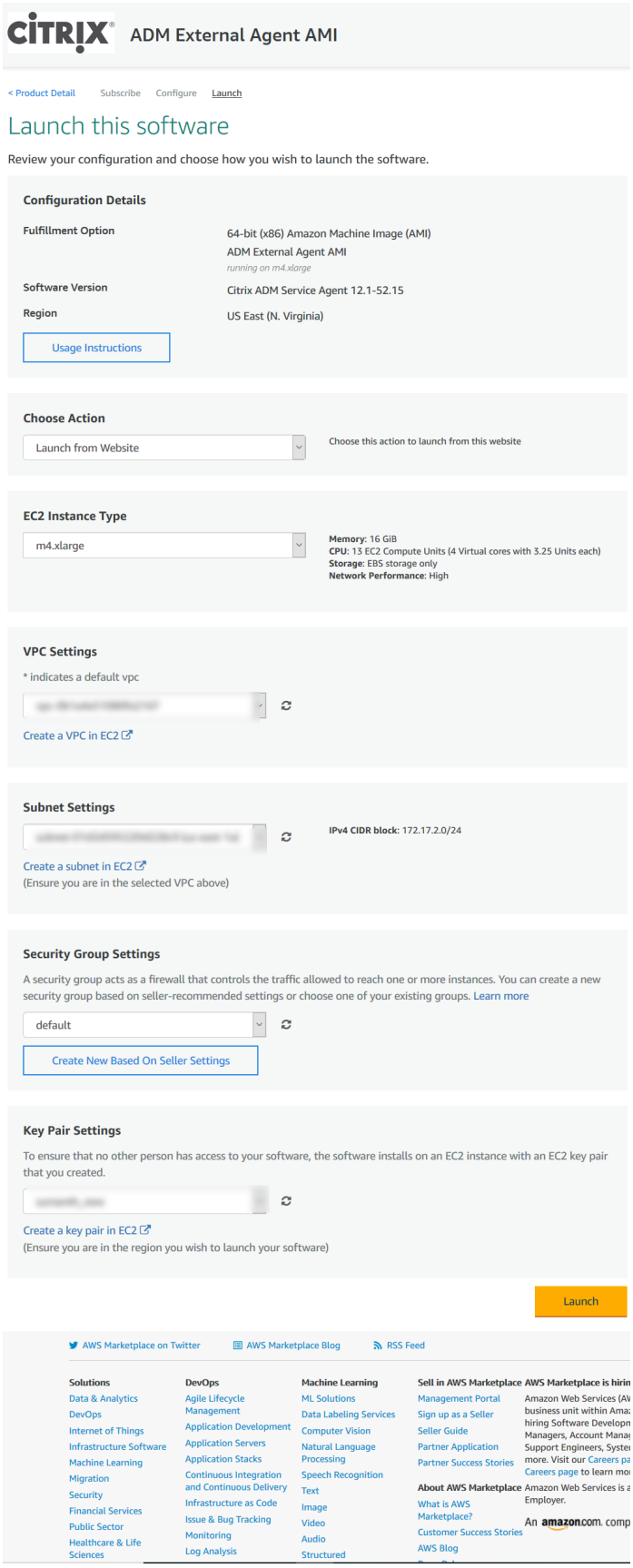
7. En la página **Iniciar este software**, tiene dos opciones para registrar el agente Citrix ADM:
   a) **Iniciar desde el sitio web**
   b) **Lanzamiento con EC2**



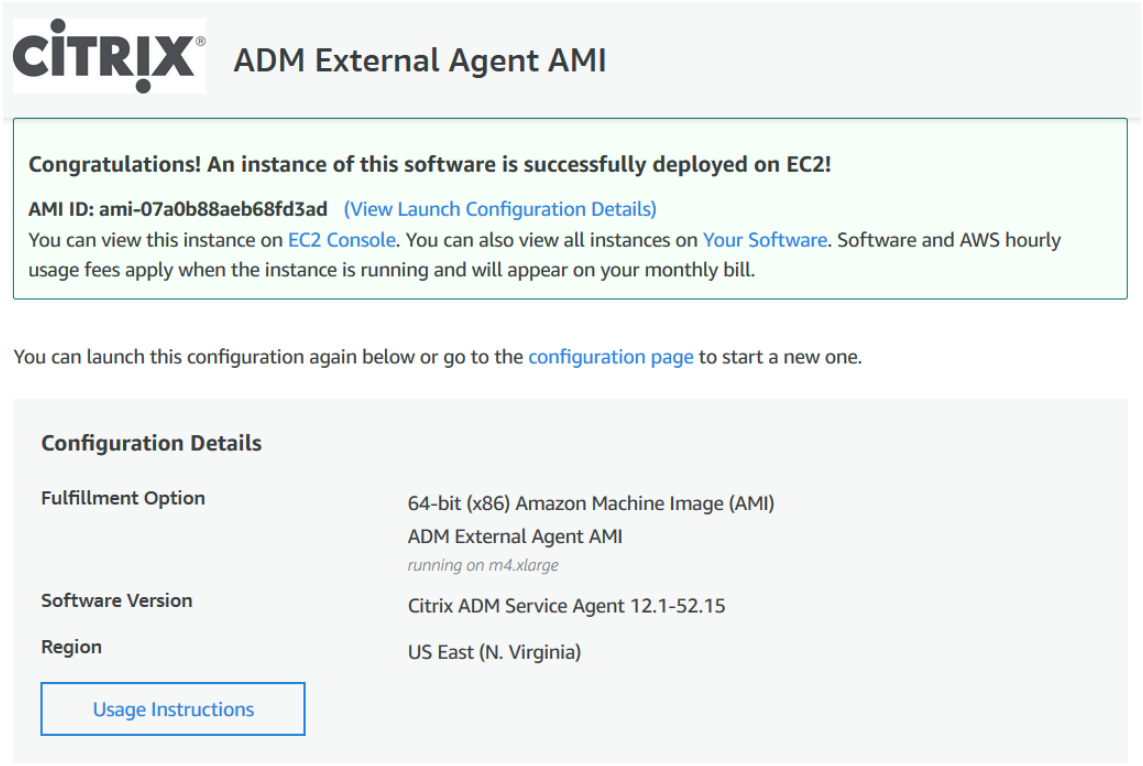
Lanzamiento desde un sitio web

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 Citrix ADM en su cuenta de AWS.

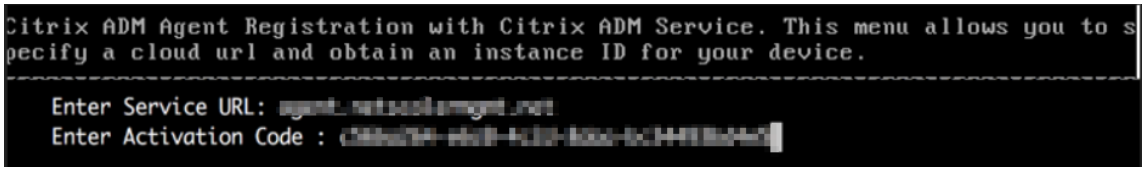
8. Una vez desplegado el agente, asigne un nombre a su agente de Citrix ADM.
9. Una vez que el agente esté en funcionamiento, asigne una dirección IP elástica a su agente Citrix ADM.

> **Nota**
>
> La dirección IP elástica permite que el agente Citrix ADM se comunique con Citrix ADM. 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 Citrix ADM.

> **Nota:**
>
> Puede iniciar sesión en el agente Citrix ADM 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 Citrix ADM, tal como se indica en la sección Introducción. El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio.



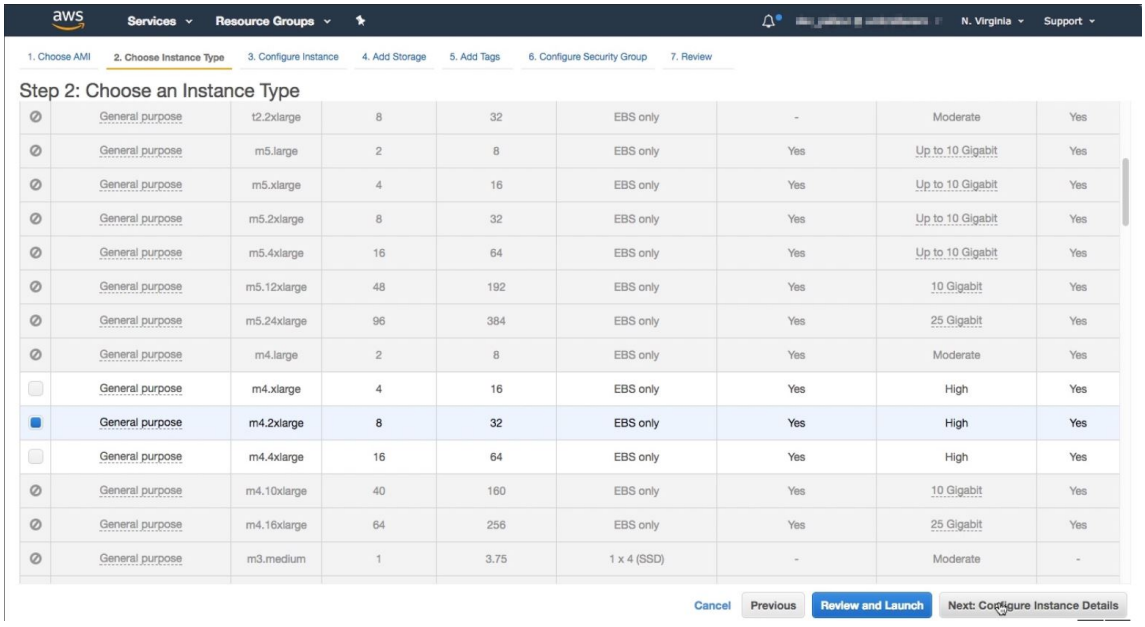
Una vez que el registro del agente se realiza correctamente, el agente se reinicia para completar el proceso de instalación.

Una vez reiniciado el agente, acceda a Citrix ADM y, en la página **Configurar agente**, en **Agentes detectados**, 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 una secuencia de comandos 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 Citrix ADM, tal como se indica en la sección Introducción. Introduzca los detalles en el siguiente formato.

```
registeragent -serviceurl <apigatewayurl> -activationcode <
    activationcodevalue>
<!--NeedCopy-->
```

El agente usa esta información para registrarse automáticamente en Citrix ADM durante el arranque.

- **Script** : especifique un script de registro automático del agente como datos de usuario. A continuación se muestra una secuencia de comandos 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 Citrix ADM agent with Citrix
    ADM. Pass it in userdata to make Citrix ADM agent in AWS
    to autoregister on bootup. The workflow is as follows
1)  Fetch the Citrix ADM API credentials (ID and secret) from
     AWS secret store (NOTE: you have to assign IAM role to
    the Citrix ADM agent that will give permission to fetch
    secrets from AWS secret store)
2)  Login to Citrix ADM with credentials fetched in step 1
3)  Call Citrix ADM 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
    Citrix ADM 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.
```



```
        " }
61
62              return resp
63
64          if print_response:
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          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 Citrix ADM credentials from AWS
                secret failed with error: %s" % (str(e)))
120         raise e
121
122     '''
123     Initializing common Citrix ADM 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     '''
```

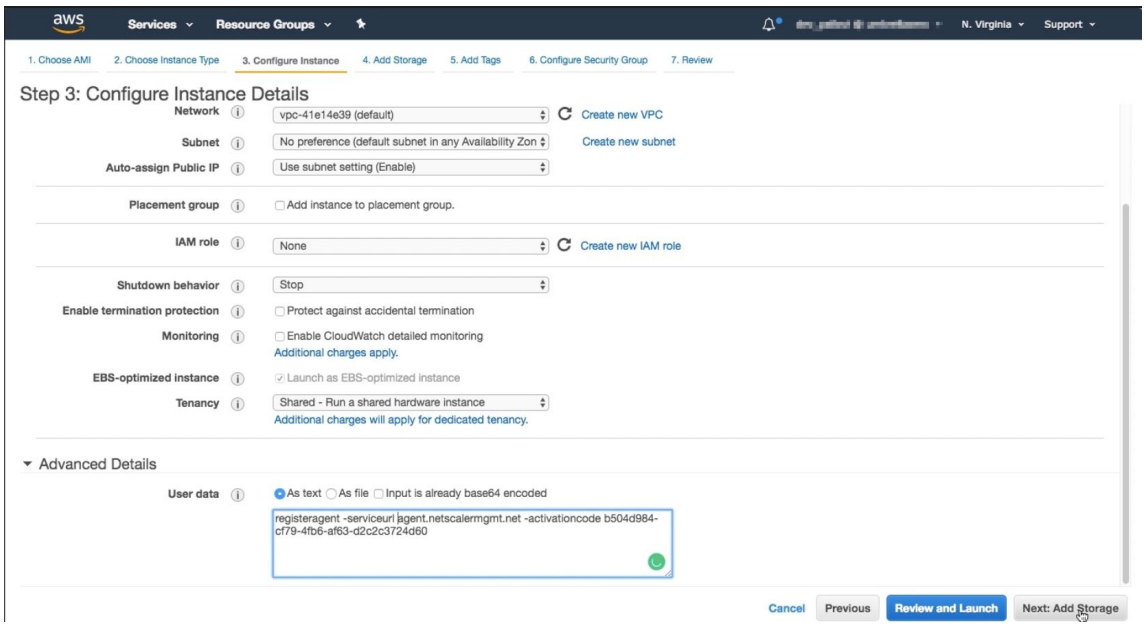


```
API to login to the Citrix ADM and fetch the Session ID and Tenant ID
'''
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/login"
payload = 'object={
"login":{
"ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"}
 }
'
try:
    response = _request("POST", url, data=payload, headers=mas_common_headers)
    sessionid = response["login"][0]["sessionid"]
    tenant_id = response["login"][0]["tenant_name"]
except Exception as e:
    logger.debug("Login call to the Citrix ADM failed with error: %s" % (str(e)))
    raise e

'''
API to fetch the service URL and Token to be used for registering the agent with the Citrix ADM
'''
mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/config/trust_preauthtoken/" + tenant_id +"?customer="+ tenant_id
logger.debug("Fetching Service URL and Token.")
try:
    response = _request("GET", url, data=None, headers=mas_common_headers)
    service_name  = response["trust_preauthtoken"][0]["service_name"]
    token = response["trust_preauthtoken"][0]["token"]
    api_gateway_url = response["trust_preauthtoken"][0]["api_gateway_url"]
except Exception as e:
    logger.debug("Fetching of the Service URL Passed with error. %s" % (str(e)))
    raise e

'''
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
177     <!--NeedCopy-->
```

Este script obtiene los detalles de autenticación del administrador de secretos de AWS y ejecuta el script `deployment.py` para registrar el agente en el Citrix ADM.



Nota

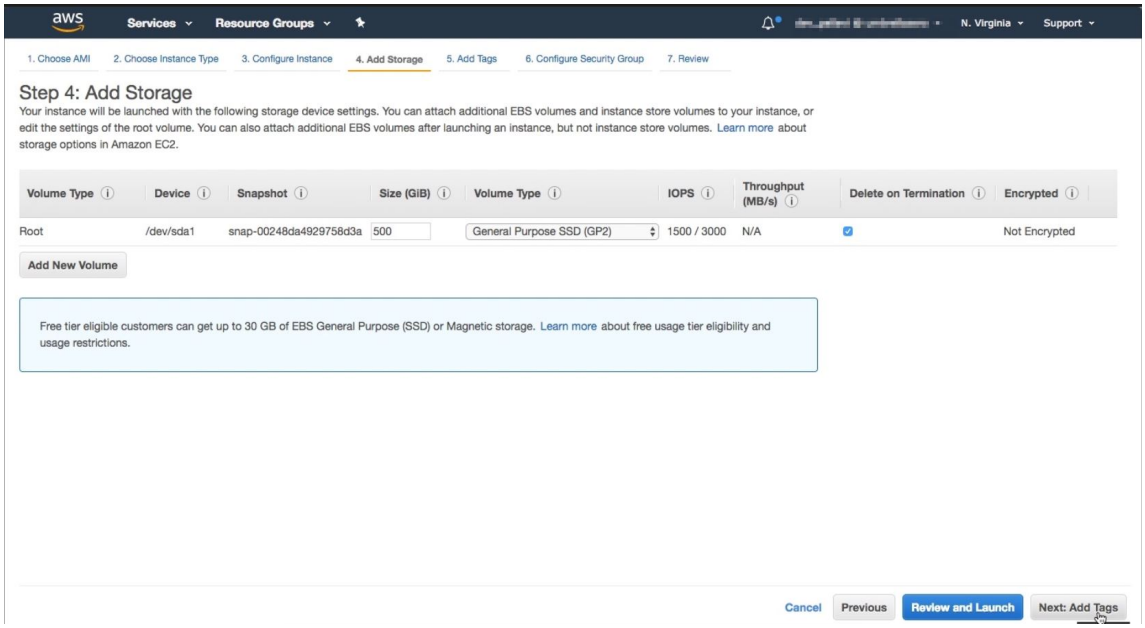
Si bien puede asignar automáticamente una dirección IP pública, también puede asignar una dirección IP elástica. La asignación de una dirección IP elástica es necesaria cuando la puerta de enlace NAT no está configurada.

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 al agente Citrix ADM mediante

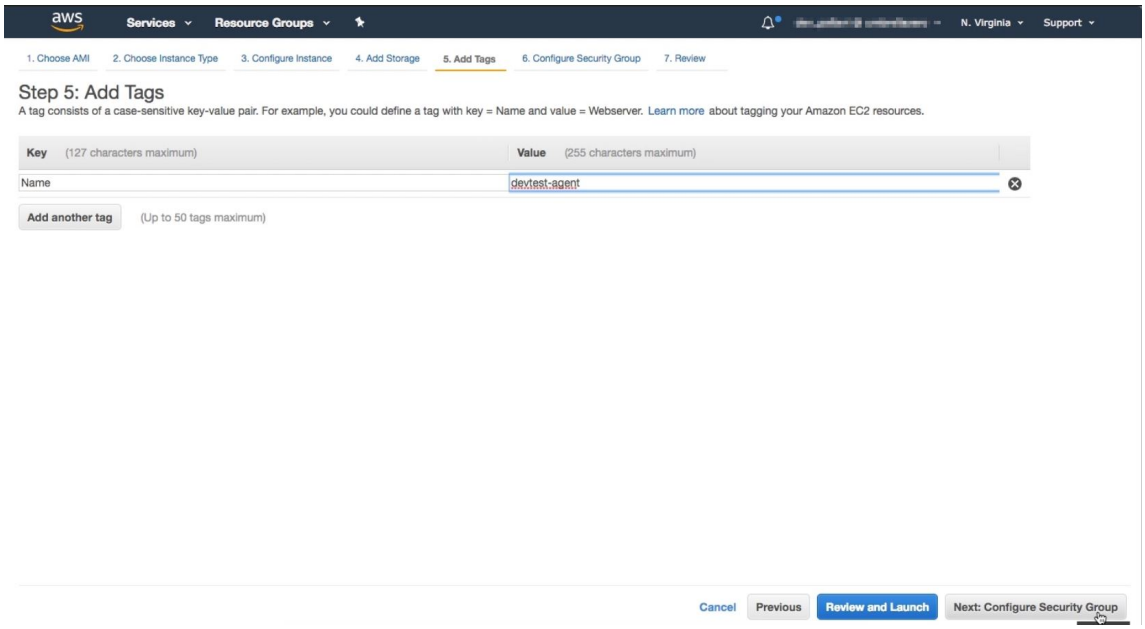
> el ID de instancia o el ENI-ID.

Haga clic en **Agregar almacenamiento**.

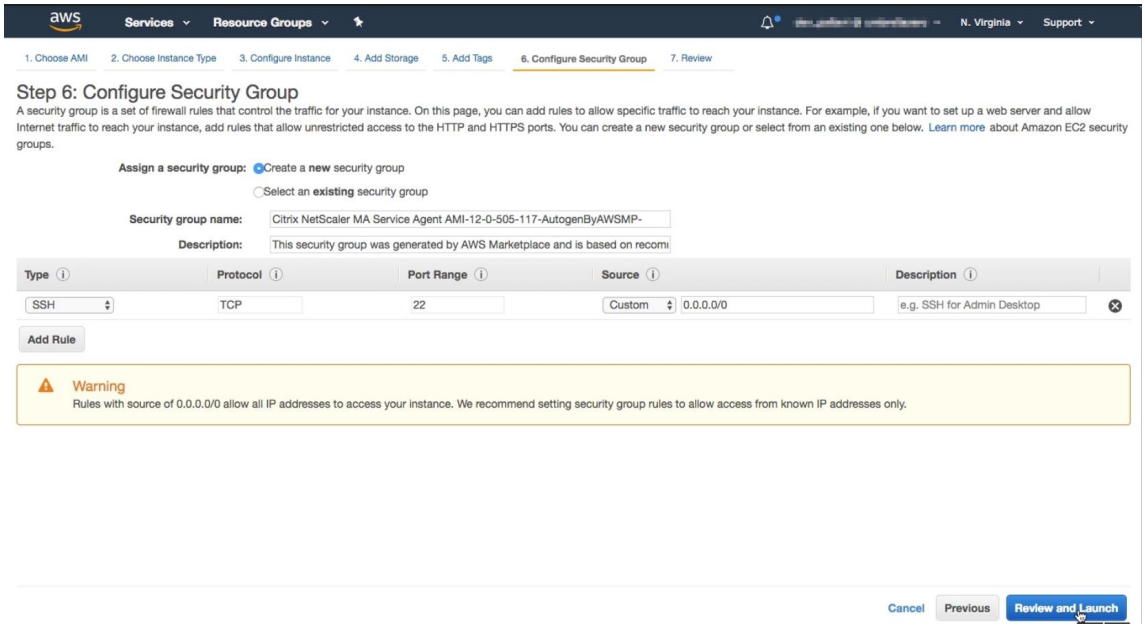
3. En la página **Agregar almacenamiento**, configure la configuración del dispositivo de almacenamiento para la instancia y haga clic en **Siguiente: Agregar etiquetas**.



4. En la página **Agregar etiquetas**, defina la etiqueta de la instancia y haga clic en **Siguiente: Configurar grupo de seguridad**.

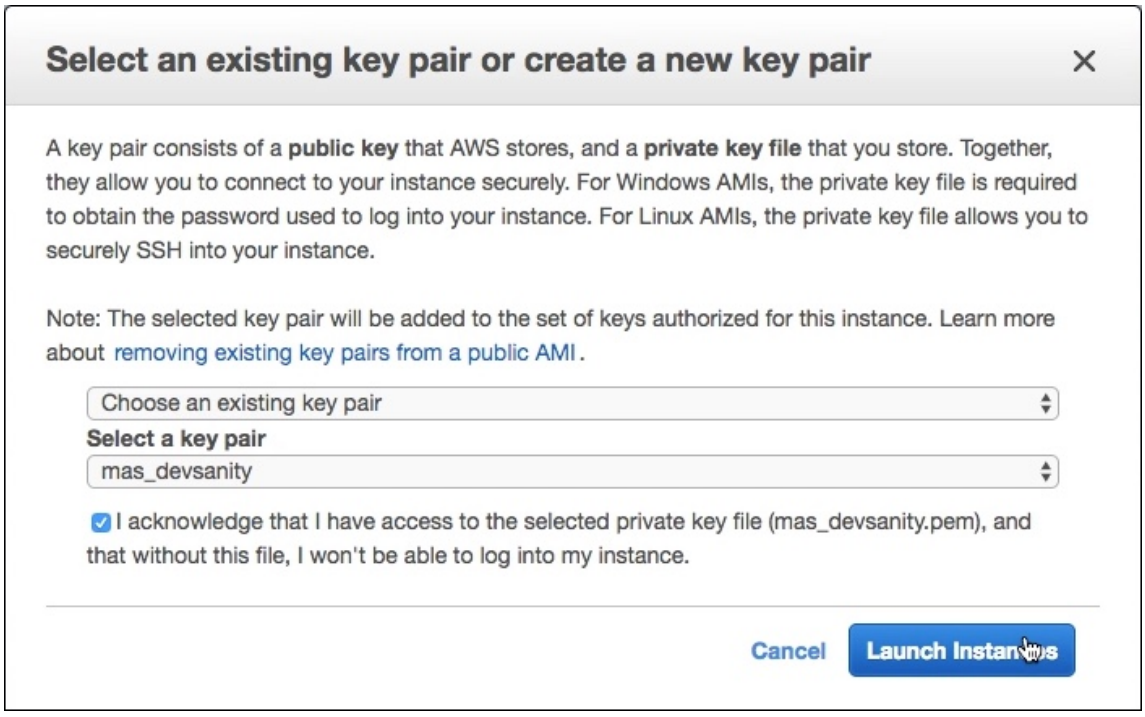


5. En la página **Configurar grupo de seguridad**, agregue reglas para permitir tráfico específico a la instancia y haga clic en **Revisar y lanzar**.



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 Citrix ADM en su

cuenta de AWS.

Instalar un agente en GCP

November 16, 2022

El agente Citrix ADM funciona como intermediario entre Citrix ADM y las instancias detectadas en el centro de datos o en la nube. Puede implementar el agente en Google Cloud Platform (GCP) para facilitar la administración remota segura de las instancias de Citrix ADC implementadas dentro de la red virtual de la nube de Google a través de Citrix ADM. Para obtener más información sobre cómo funciona el agente Citrix ADM en GCP para los administradores de TI, lea el blog El agente Citrix ADM ya está disponible en Google Cloud Platform Marketplace.

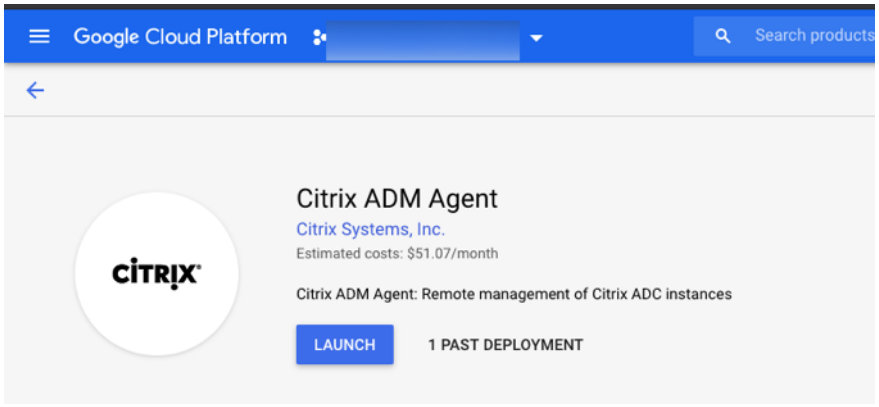
Requisitos previos

Para instalar un agente Citrix ADM en GCP, necesita una cuenta de GCP.

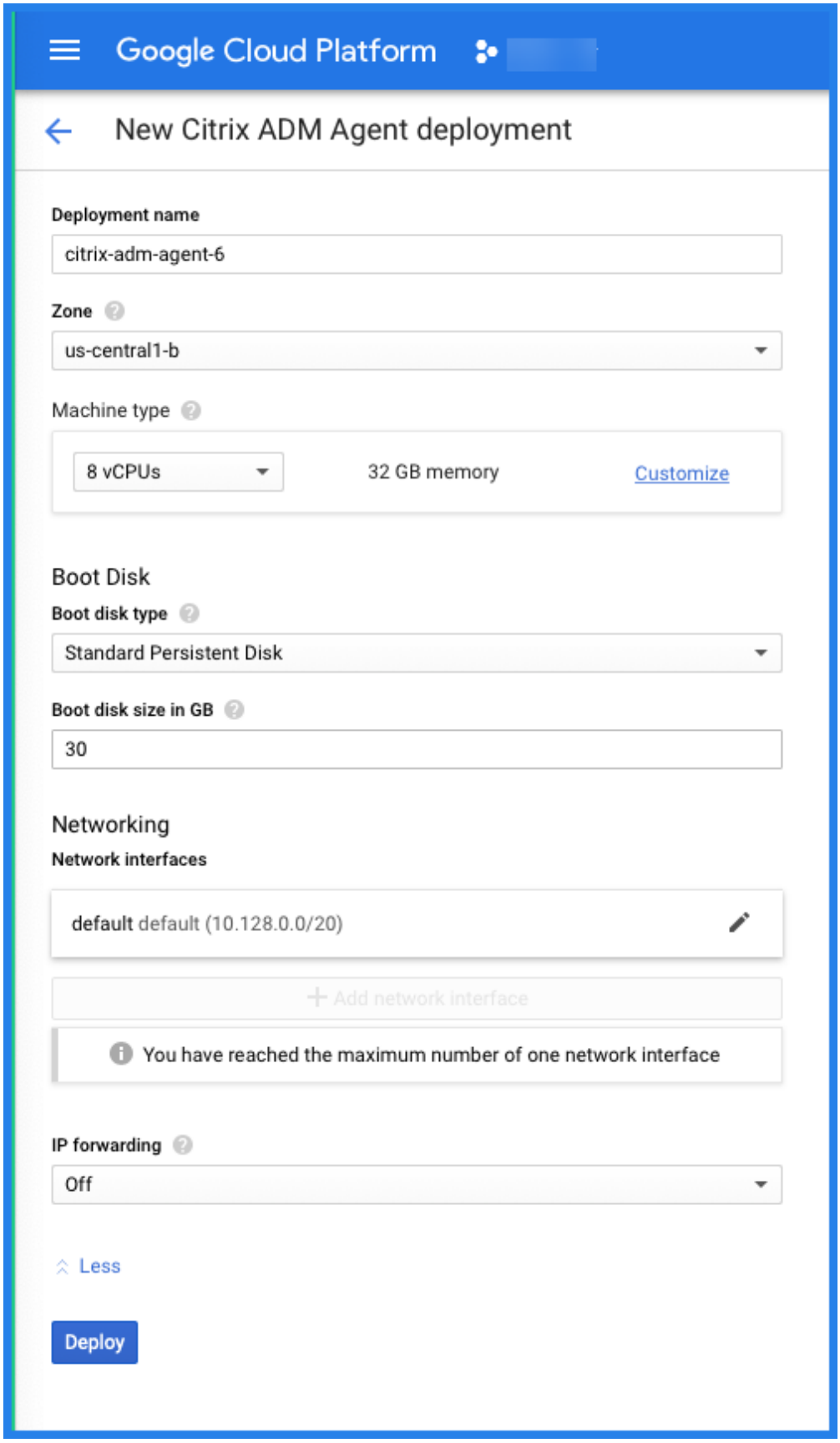
Instalar el agente Citrix ADM en GCP

Siga estos pasos para instalar un agente Citrix ADM en GCP.

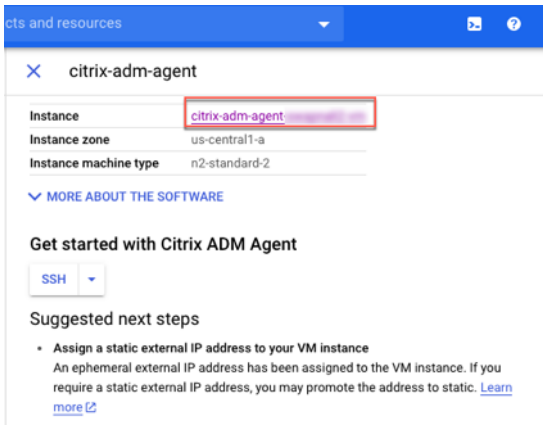
1. Inicie sesión en la consola GCP (console.cloud.google.com) con sus credenciales y vaya al mercado.
2. En el campo de búsqueda, escriba el **agente Citrix ADM**.
3. Haga clic en el **agente Citrix ADM** en el campo de resultados y, a continuación, en **Iniciar**.



4. En la página de **implementación del nuevo agente Citrix ADM**, 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**.

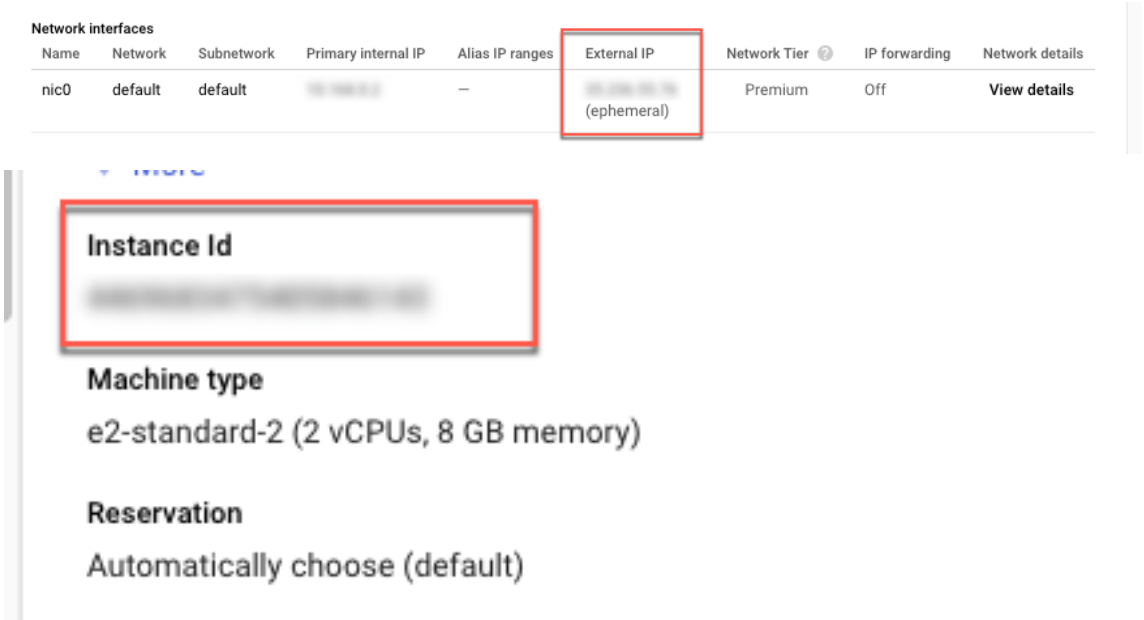


6. Inicie sesión en el agente a través de un cliente SSH utilizando la dirección IP externa del agente. Utilice los siguientes comandos:

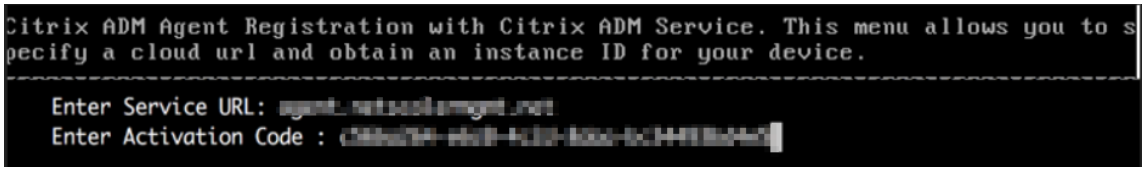
   ```
   ssh nsrecover@<external IP address of the agent>
   ```

   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 Citrix ADM, tal como se indica en la sección Introducción. 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 Citrix ADM y, en la página **Configurar agente**, en **Agentes detectados**, compruebe el estado del agente.

Instalar un agente en el clúster de Kubernetes

November 16, 2022

> **Nota**
>
> El procedimiento para instalar un agente como microservicio está disponible en la sección Introducción .

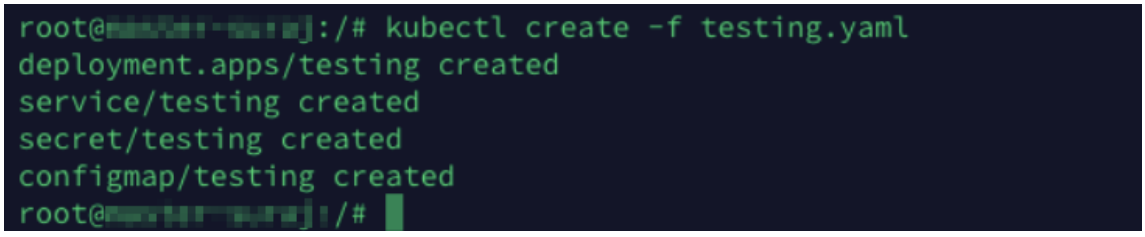
En el nodo principal de Kubernetes:

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

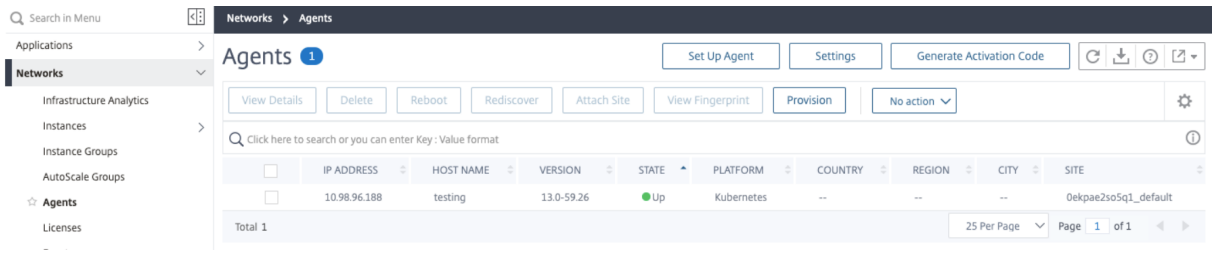
   `kubectl create -f <yaml file>`

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

   El agente se ha creado correctamente.



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



Cómo obtener ayuda y asistencia técnica

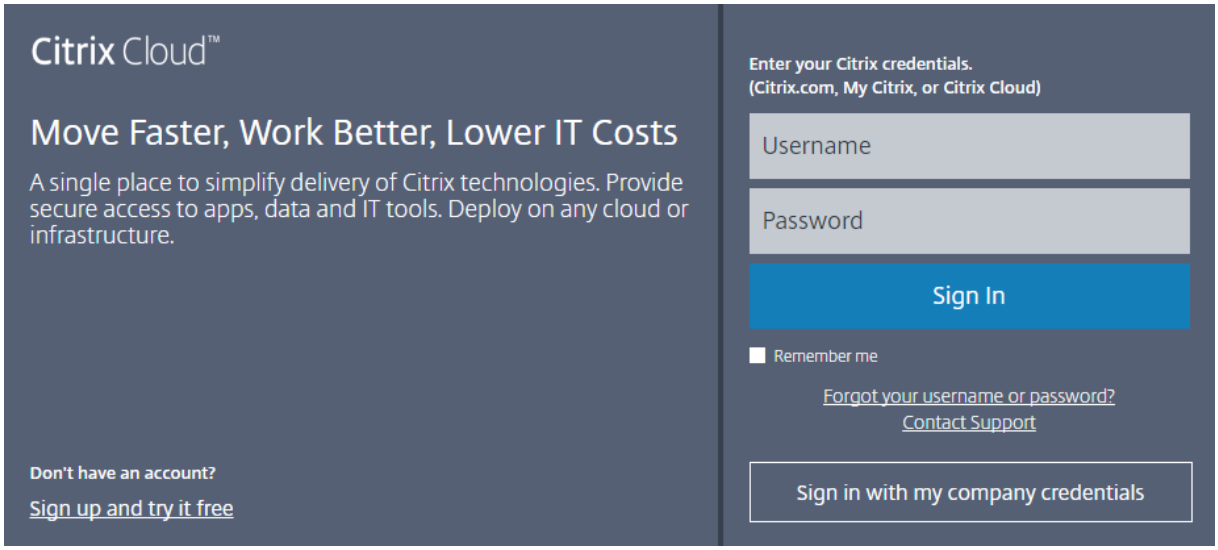
April 30, 2021

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 atención 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 ha iniciado sesión en Citrix Cloud
  - Su contraseña no cumple con 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 em-

presa 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 para restablecer la contraseña, o necesita más ayuda, póngase en contacto conservicio 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 asistencia de Citrix realizan un seguimiento de estos foros y pueden responder a sus preguntas. Otros miembros de la comunidad de Citrix Cloud también pueden ofrecer ayuda o unirse a la discusión.

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 aCrear o solicitar una cuenta.

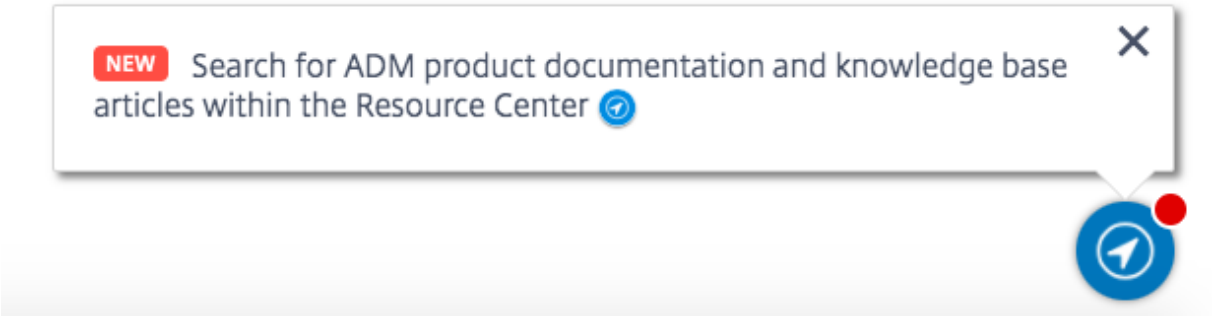
Artículos y documentación de asistencia

Citrix ofrece una gran variedad de contenido sobre productos y de asistencia para ayudarle a sacar el máximo partido de Citrix Cloud y resolver problemas que pueda encontrar al usar los productos Citrix.

Centro de recursos de Citrix Cloud

Citrix Cloud Resource Center proporciona varios recursos para ayudarle a comenzar con los servicios de Citrix Cloud, obtener más información sobre las funciones y resolver problemas. Los recursos que aparecen son aplicables a la función o servicio de Citrix Cloud con la que está trabajando actualmente. Por ejemplo, si se encuentra en la consola de administración del servicio Virtual Apps y escritorios, el Centro de recursos le mostrará los siguientes recursos.

Acceda al Centro de recursos en cualquier momento haciendo clic en el icono de brújula azul situado en la parte inferior derecha de la consola de Citrix Cloud.



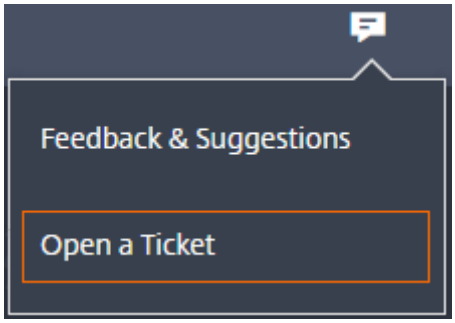
- **Introducción**: Proporciona un breve tutorial guiado de las tareas clave específicas del servicio con el que está trabajando actualmente. También encontrará enlaces a recursos de capacitación e incorporación que le ayudarán a obtener más información sobre las capacidades de servicio y a configurar a sus usuarios finales para el éxito.
- **Anuncios**: Proporciona notificaciones de funciones recientemente publicadas y vínculos a comunicaciones esenciales de Citrix. Haga clic en una notificación de entidad para recibir un breve recorrido guiado de la entidad.
- **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 conocer más sobre Citrix Cloud y otros productos Citrix. Aquí encontrará arquitecturas de referencia, diagramas, vídeos y documentos técnicos que proporcionan información para diseñar, crear e implementar tecnologías Citrix.

Asistencia técnica

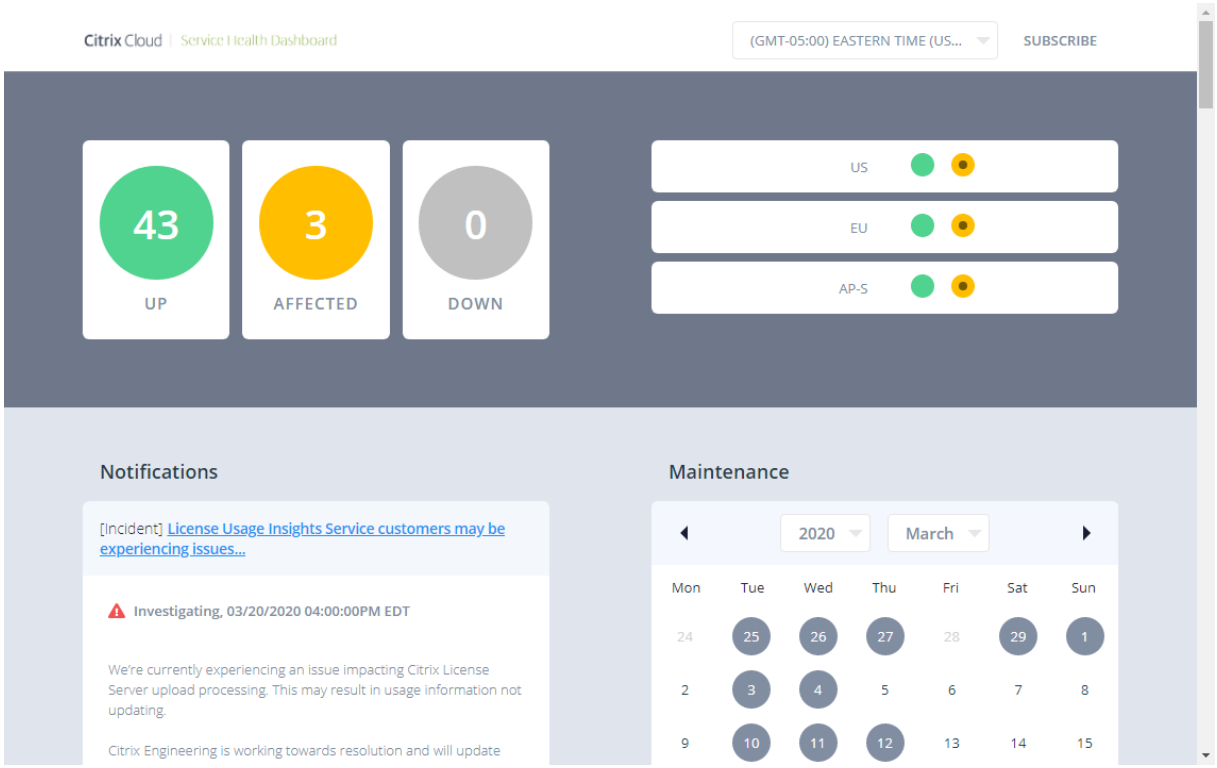
Si tiene un problema que requiere asistencia técnica, haga clic en el icono **Comentarios y asistencia** situado cerca de la parte superior derecha de la pantalla y, a continuación, seleccione **Abrir un tíquet**.



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

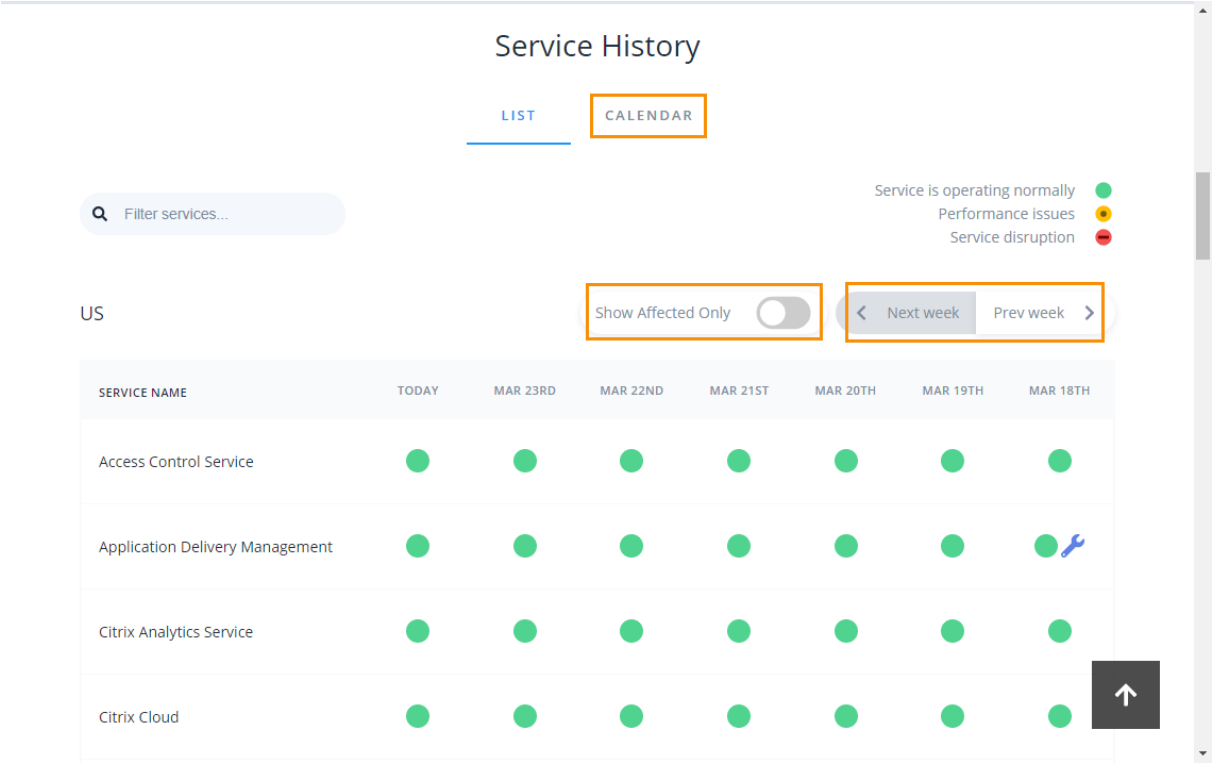
ElPanel de estado de Citrix Cloud Service proporciona una visión general de la disponibilidad en tiempo real de la plataforma y los servicios de Citrix Cloud en cada región geográfica. Si experimenta algún problema con Citrix Cloud, consulte el Panel de estado del servicio para comprobar que Citrix Cloud o servicios específicos funcionan normalmente.



Utilice el panel para obtener más información sobre las siguientes condiciones:

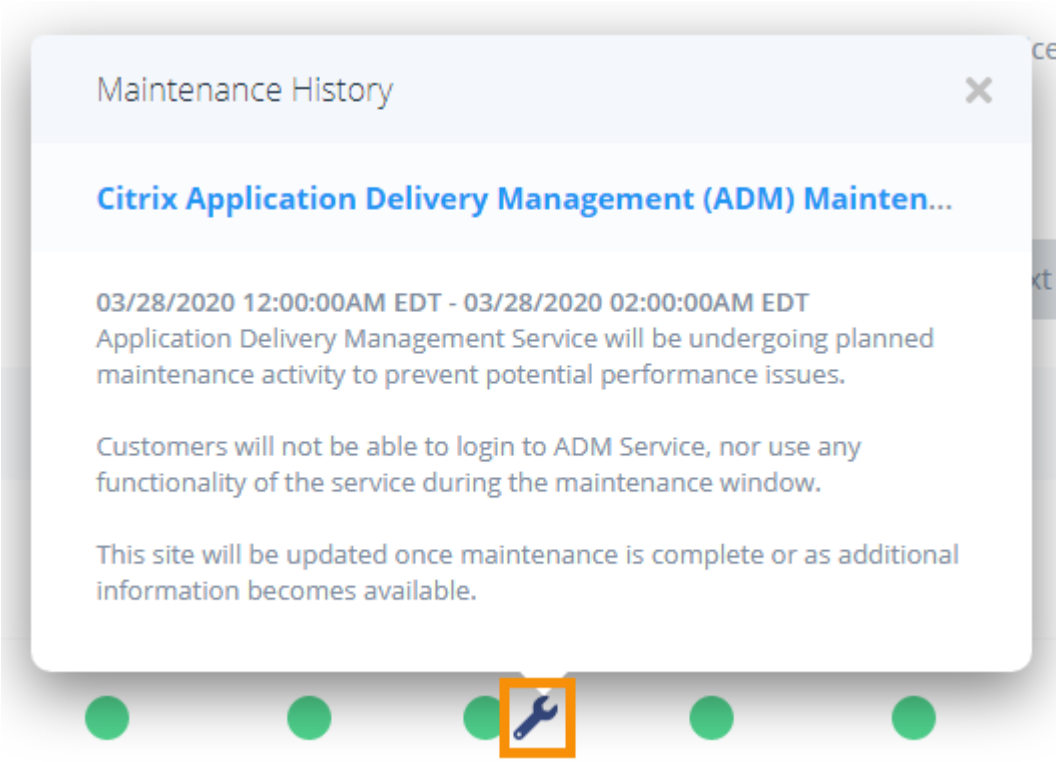
- El estado actual de disponibilidad de todos los servicios de Citrix Cloud, agrupados por región geográfica
- Historial de mantenimiento del servicio de cada servicio durante los últimos siete días (predeterminado) o para incrementos de siete días anteriores
- Ventanas de mantenimiento para servicios específicos

De forma predeterminada, el estado de mantenimiento del servicio se muestra como una lista, pero también se puede mostrar en una vista de calendario. Seleccione **Siguiente** o **Anterior** para desplazarse por el historial de mantenimiento del servicio en incrementos de siete días. También puede filtrar la lista para mostrar solo los servicios afectados.

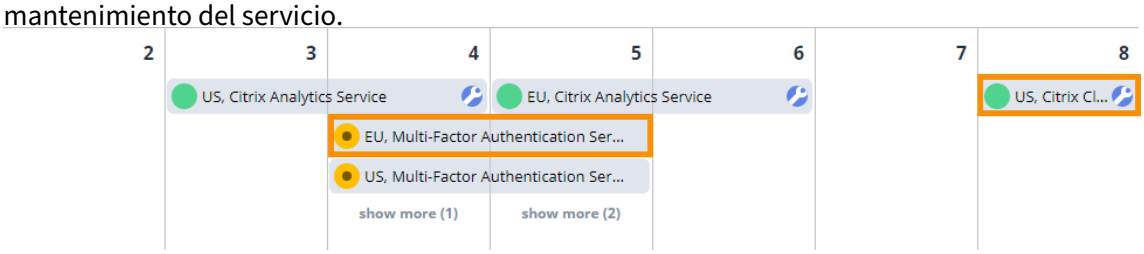


Para ver información más detallada sobre el incidente de mantenimiento del servicio de un servicio afectado:

- 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 mantenimiento del servicio.

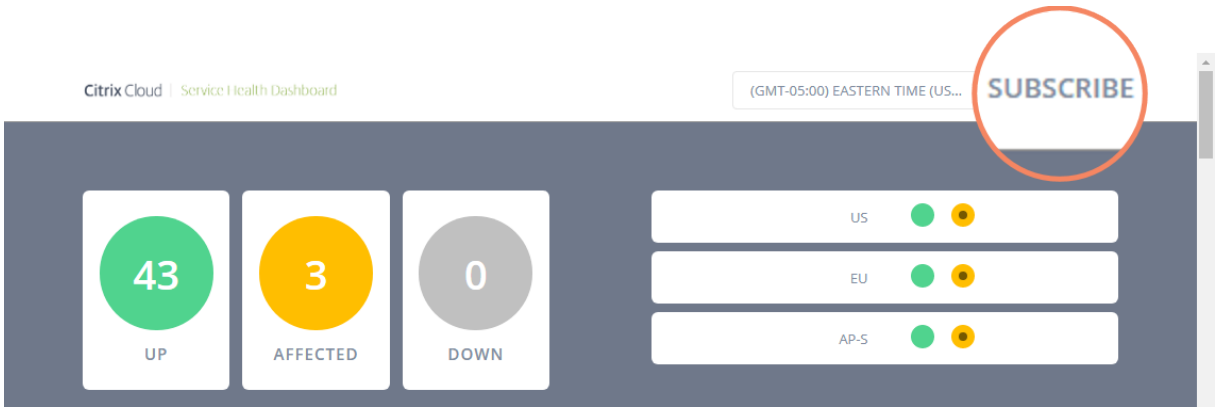


- En la vista de calendario, haga clic en la entrada de servicio para ver el estado del incidente de mantenimiento del servicio.

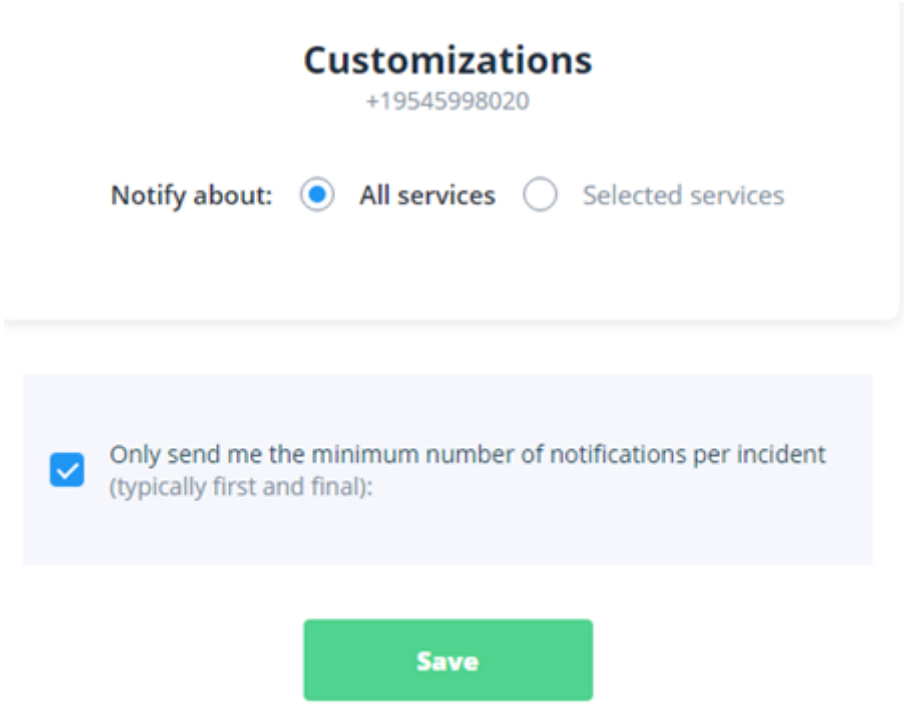


Suscripciones de mantenimiento del servicio

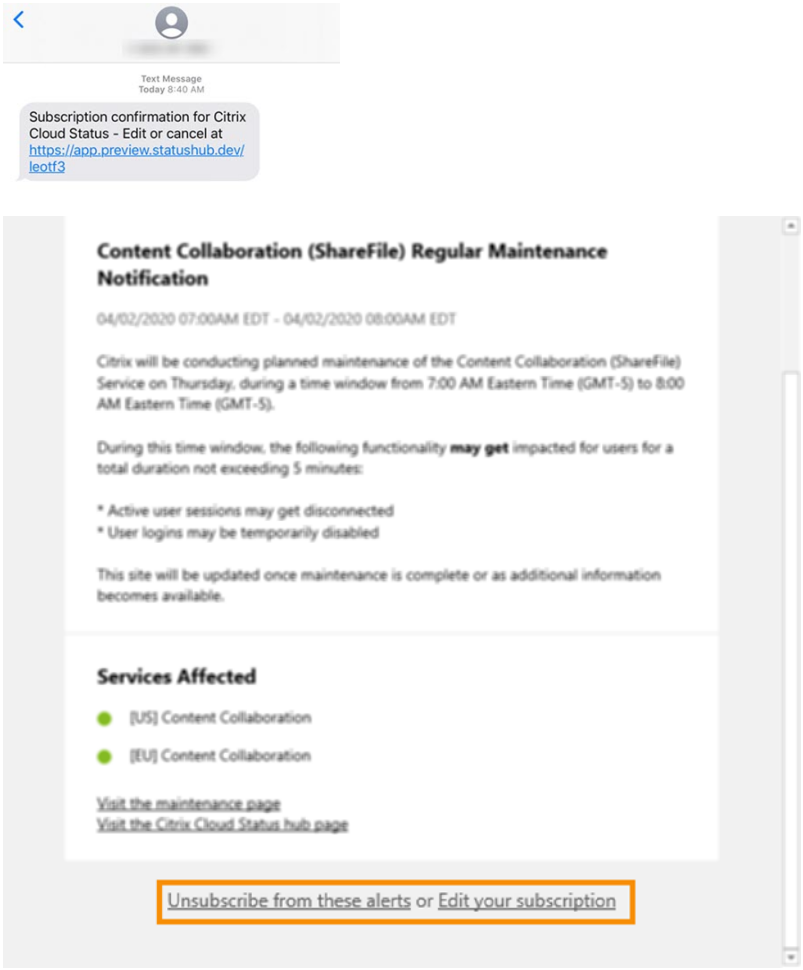
Para recibir notificaciones de estado del servicio, haga clic en **Suscribirse** en la parte superior derecha del panel y seleccione el método de notificación que desea utilizar.



Puede suscribirse a notificaciones de todos los servicios o solo de los servicios que seleccione. De forma predeterminada, recibirá todas las notificaciones de un incidente de mantenimiento del servicio. Para limitar la frecuencia de las notificaciones durante un incidente, puede optar por recibir solo la primera y última notificación.



Dependiendo del método de suscripción, los enlaces para cancelar la suscripción y cambiar sus preferencias se incluyen en el mensaje de confirmación de suscripción que recibe (por ejemplo, al suscribirse a notificaciones telefónicas) o en cada mensaje de notificación (por ejemplo, cuando se suscribe a notificaciones por correo electrónico).



Para cancelar la suscripción o cambiar sus preferencias de suscripción:

1. Localice una notificación existente y seleccione el enlace para cancelar la suscripción o cambiar sus preferencias de notificación.
2. Si cancela la suscripción, seleccione Cancelar **suscripción** y, a continuación, seleccione el método de notificación que desea cancelar. Para suscribirse a todos los métodos de notificación, seleccione **Quitar 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 de instancias de Citrix ADC de bajo contacto mediante Citrix ADM Service connect

November 16, 2022

A medida que crece su infraestructura híbrida multinube (HMC), los desafíos para administrar, super-

visar, analizar y solucionar problemas de las instancias de ADC 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, Citrix ADM 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 Citrix ADM

Los componentes básicos de este flujo de trabajo son dos componentes del lado ADC: conexión de servicio ADC y Call Home.

- **Citrix ADM connect**: es una nueva función de ADC que ayuda a permitir la incorporación perfecta de las instancias de Citrix ADC en Citrix ADM. Esta función permite que la instancia de Citrix ADC se conecte automáticamente con Citrix ADM y envíe datos del sistema, de uso y de telemetría a Citrix ADM. Basándose en estos datos, el Citrix ADM le ofrece información y recomendaciones sobre su infraestructura Citrix ADC. Como la identificación rápida de problemas de rendimiento, uso elevado de recursos y errores críticos.

  Citrix ADM connect está disponible en las siguientes versiones de ADC:

  - Citrix ADC 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 Citrix ADM connect para dispositivos Citrix ADC.
  - Imagen de la versión 12.1 58.14 y posterior de Citrix ADC SDX y 13.0 61.48 y posteriores. Para obtener más información, consulte Introducción a Citrix ADM connect para dispositivos Citrix ADC 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 Citrix ADM para habilitar este nuevo flujo de trabajo.

Todas las instancias de ADC con conectividad a Internet o Call Home, o las instancias habilitadas con Citrix ADM Connect, están conectadas a Citrix ADM. Citrix ADM comienza a recopilar las métricas relevantes de estas instancias de ADC a través de la ruta Call Home, la ruta de conexión de Citrix ADM 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, Citrix ADM crea un inventario de instancias de ADC para cada cliente (ID de organización único), que le muestra una lista consolidada de sus instancias de ADC. Citrix ADM también utiliza estos datos para generar información sobre sus instancias de ADC 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 ADC a Citrix ADM.
Puede marcar **Seleccionar instancias de ADC y Gateway para incorporarlas** y seleccionar las instancias de ADC que quiere incorporar a Citrix ADM. Después de empezar, se le guiará al proceso de incorporación.

El proceso de incorporación automática utiliza Citrix ADM connect, lo que hace que la experiencia sea automatizada, fluida y rápida. Para las instancias de ADC en versiones que no admiten la conexión y la incorporación automática de Citrix ADM, Citrix ADM proporciona el uso de 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 quiere utilizar licencias agrupadas o el conjunto de análisis completo de Citrix ADM. O si quiere usar licencias agrupadas y el conjunto completo de análisis. El agente integrado solo admite administración y supervisión.
> - Las métricas recopiladas por ADM Service Connect se envían directamente al punto final del servicio ADM. Incluso si el ADC es un ADC gestionado o descubierto en el servicio ADM y se ha configurado un agente externo para ese ADC, las métricas se envían directamente desde el ADC al punto final del servicio ADM 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 un producto de Citrix**: recibe un correo electrónico de Citrix ADM que muestra algunos datos clave de su infraestructura de ADC y lo invita a comenzar con Citrix ADM. 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.
> - Puede habilitar o deshabilitar las notificaciones por correo electrónico que recibe como parte del flujo de trabajo de incorporación sencillo basado en ADM Service Connect. Para obtener más información, consulte Configuración del correo electrónico.

3. **Página de bienvenida de Citrix ADM**: obtendrá una descripción general de Citrix ADM y sus beneficios.
4. **Información sobre sus instancias de ADC y Gateway**: obtendrá información detallada sobre su infraestructura general de ADC, que incluye consejos de seguridad (consejos sobre los CVE actuales de Citrix), consejos de actualización (consejos basados en los plazos de EOM/EOL), métricas clave, tendencias y destaca los problemas que afectan al rendimiento de ADC y salud y recomienda una forma de mitigar los problemas.
5. **Seleccione las instancias de ADC y Gateway para incorporarlas**: obtendrá una vista consolidada de su inventario de ADC. Puede seleccionar qué instancias de ADC quiere incorporar a Citrix ADM.
6. **Instancias ADC integradas en Citrix ADM**: en función de las instancias de ADC seleccionadas para la incorporación, Citrix ADM lo guía en el proceso de incorporación. De forma predeterminada, se selecciona el agente integrado para la incorporación automática.
7. **Panel de interfaz gráfica de usuario de Citrix ADM**: una vez finalizada la incorporación, se le dirigirá al panel de instancias de Citrix ADM.

Para obtener más información sobre cada uno de estos métodos de incorporación, consulte Instancias integradas de Citrix ADC que utilizan Citrix ADM connect.

Instancias de Citrix ADC incorporadas con Citrix ADM Service connect

November 16, 2022

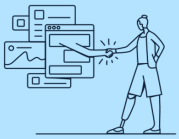
A continuación, se incluye una guía paso a paso que le ayudará a comenzar a utilizar Citrix ADM. Antes de empezar, lea cómo Citrix ADM lanza un nuevo flujo de trabajo de incorporación, que le proporciona una forma más rápida de obtener una visibilidad completa de su implementación multinube híbrida (HMC). Consulte Incorporación discreta de instancias de Citrix ADC mediante Citrix ADM Connect.

Paso 1: Empezar

Recibirá un correo electrónico de Citrix ADM en el que se muestran algunos datos clave de su infraestructura de ADC y se le invita a comenzar con Citrix ADM.

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.**

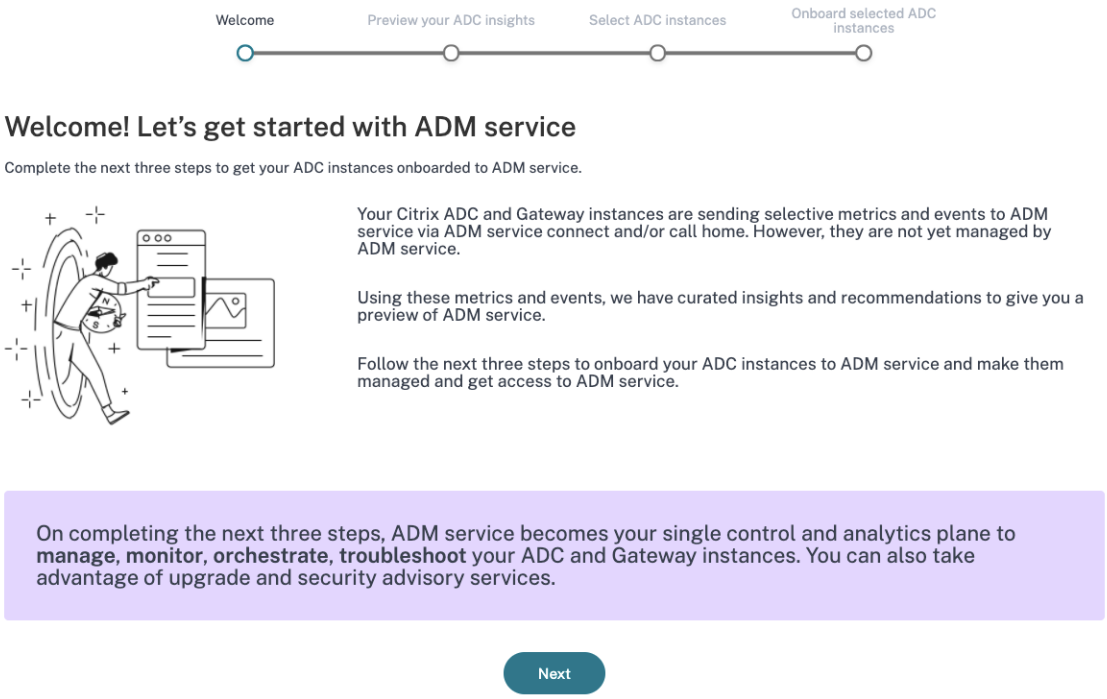
As a first step, you will need to create Citrix Cloud account by clicking on the button below.

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 ADM Service Connect. Para obtener más información, consulte Configuración del correo electrónico.

3. En la página de inicio de Citrix ADM, dedique un momento a leer por qué está allí y las ventajas de usar Citrix ADM.



> **Nota**
>
> Los consejos de seguridad incluidos en el correo electrónico se basan únicamente en el escaneo

> de la versión de compilación de ADC. Puede obtener información de asesoramiento de seguridad más concluyente y exhaustiva después de incorporar sus instancias de ADC a Citrix ADM.

1. Haga clic en **Siguiente**. Se abrirá la página **Insights on your ADC y Gateway Instancias**.

Los siguientes pasos actúan como un flujo de trabajo guiado para ofrecerle una vista previa de lo que Citrix ADM puede ofrecer y ayudarlo a integrar sus instancias de ADC en Citrix ADM sin problemas.

Paso 2: Información sobre sus instancias de ADC y Gateway

Esta página de información utiliza los datos recopilados a través de Call Home o Citrix ADM connect o tanto Call Home como Citrix ADM Connect para proporcionar información sobre sus instancias de ADC. Esta página le brinda información sobre su infraestructura general de ADC, incluidos consejos de seguridad (consejos sobre los CVE actuales de Citrix), consejos de actualización (consejos basados en los plazos de EOM/EOL), métricas clave y tendencias, y destaca los problemas que afectan al rendimiento y el estado de los ADC, y recomienda formas de mitigar los problemas. Estas ideas y recomendaciones son solo una pequeña vista previa de la gran cantidad de beneficios y valor agregado que ofrece Citrix ADM. Para obtener muchos más beneficios, información detallada y poder ejecutar las acciones recomendadas, debe incorporar las instancias de ADC en Citrix ADM.

Los conocimientos y recomendaciones se clasifican en los siguientes tipos:

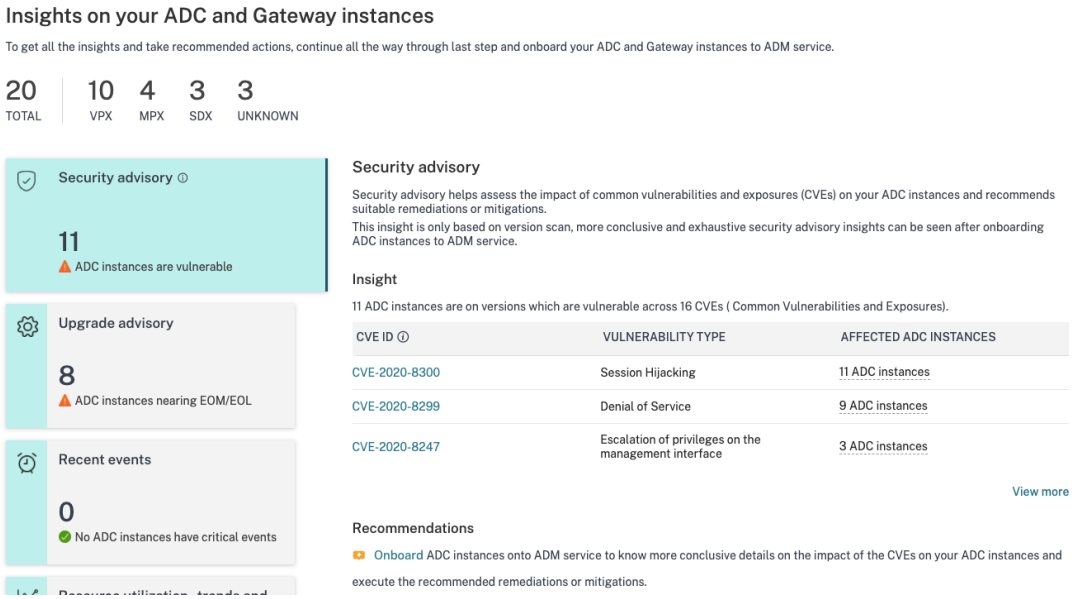
- **Asesoramiento de seguridad**: instancias ADC incorporadas para obtener los detalles del impacto de CVE en sus instancias de ADC y ejecutar las correcciones o mitigaciones recomendadas.
- **Aviso de actualización**: incorpore instancias de ADC en Citrix ADM y actualice las instancias de ADC que hayan alcanzado o estén llegando a la EOM/EOL o que se encuentren en versiones o compilaciones anteriores.
- **Eventos recientes**: incorpore instancias de ADC a Citrix ADM para monitorear más de 200 eventos con regularidad y cree reglas para recibir notificaciones por correo electrónico, PagerDuty, Slack o ServiceNow, tome las medidas adecuadas.
- **Utilización de recursos: tendencias y anomalías**: incorpore instancias de ADC a Citrix ADM para obtener una visión completa del estado de las instancias de ADC, los problemas de rendimiento y las recomendaciones para mitigarlos. También puede evaluar el uso predicho de CPU y memoria para las instancias de ADC.
- **Guía de implementación de ADC**: incorpore instancias de ADC en Citrix ADM y configúrelas como un par HA, mediante trabajos de configuración en Citrix ADM.

1. **Asesoramiento de seguridad**: Citrix ADM Security Advisory le alerta sobre vulnerabilidades que ponen en riesgo sus instancias de ADC y recomienda mitigaciones y correcciones.

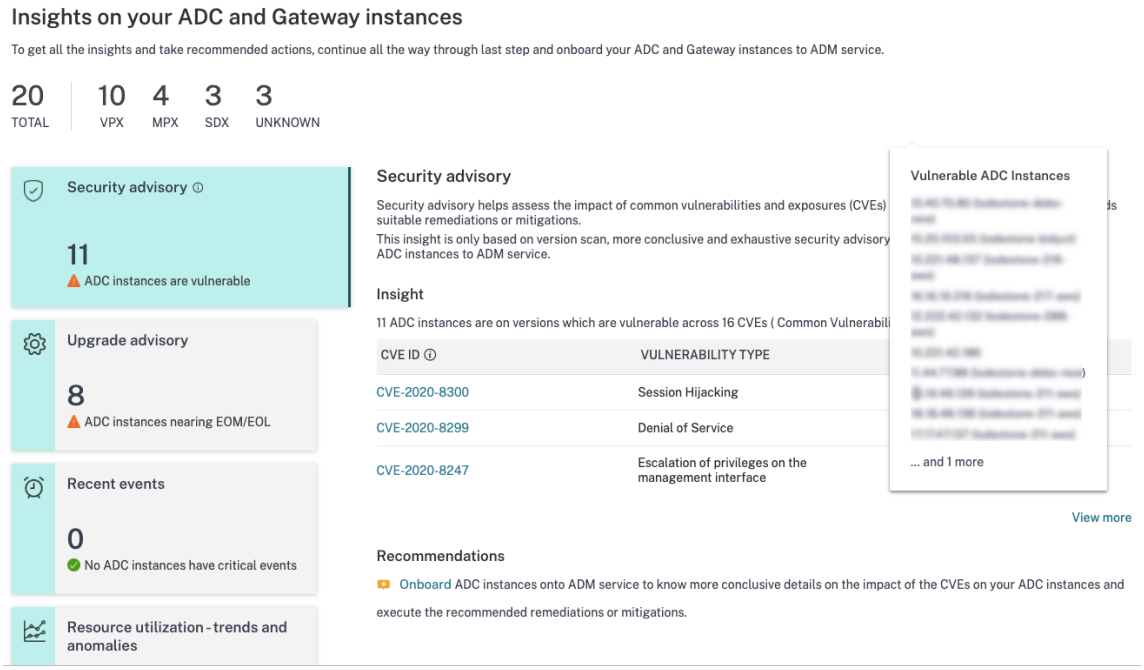
   > **Nota:**
   >
   > Los consejos de seguridad incluidos en el correo electrónico de incorporación y el flujo de trabajo guiado se basan únicamente en el escaneo de versiones de ADC. Puede obtener

> información de asesoramiento de seguridad concluyente y exhaustiva después de incorporar sus instancias de ADC a Citrix ADM **Ejemplo**: si un CVE necesita tanto un escaneo de versiones como un escaneo de configuración para evaluar las vulnerabilidades, el correo electrónico de incorporación y el flujo de trabajo guiado muestran los resultados según el escaneo de versiones. Por lo tanto, puede haber falsos positivos. Para obtener una evaluación más concluyente y precisa del impacto, incorpore ADC a Citrix ADM. Tras la incorporación, el aviso de seguridad de Citrix ADM muestra la evaluación de impacto, qué evaluación de ADC vulnerable, basada en el escaneo de versiones y el escaneo de configuración.

Puede comprobar el ID de CVE, el tipo de vulnerabilidad y las instancias ADC afectadas. El vínculo CVE ID lleva al artículo del boletín de seguridad.



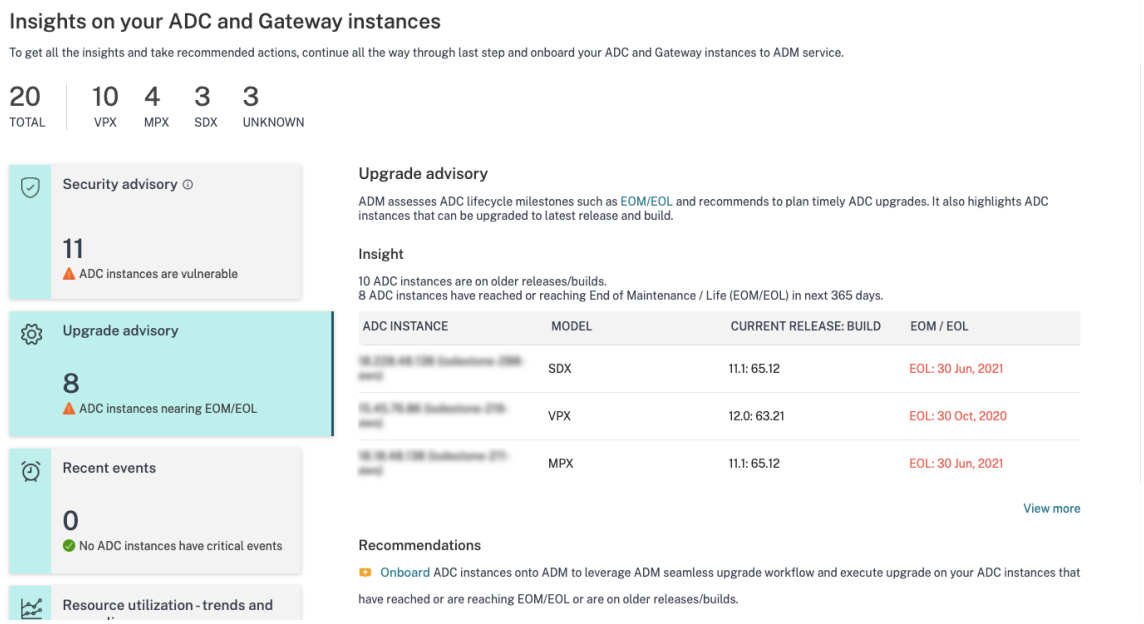
La recomendación lo guía para incorporar sus instancias de ADC en Citrix ADM para obtener más detalles sobre el impacto de la CVE en sus instancias de ADC y ejecutar la mitigación o solución recomendada. Haga clic en las instancias ADC afectadas para ver las direcciones IP de las instancias afectadas.



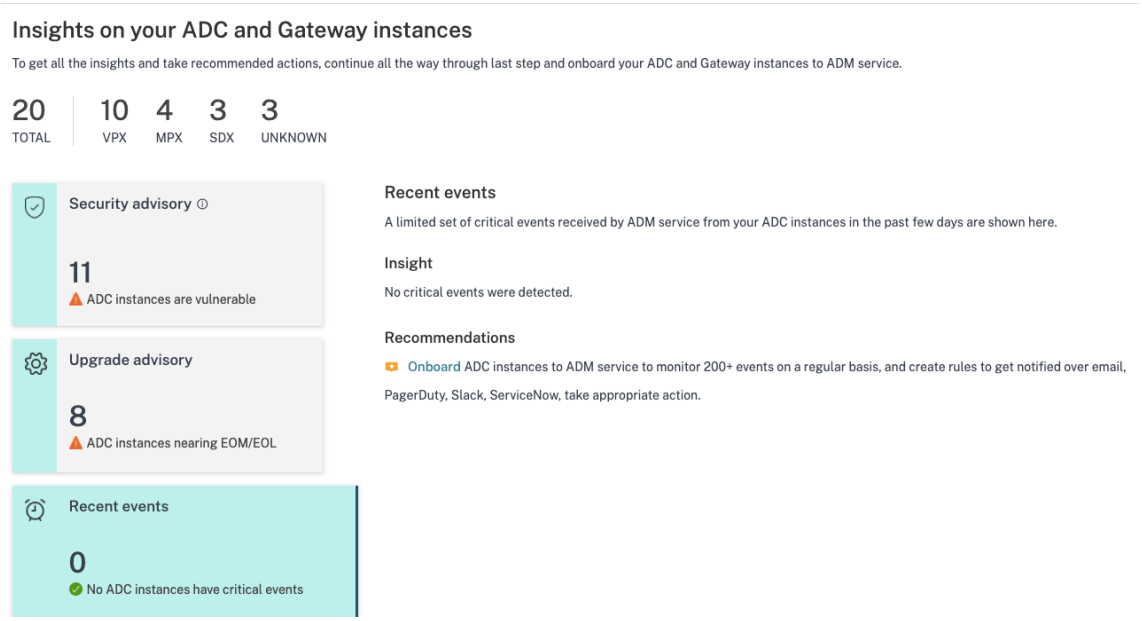
2. **Aviso de actualización**: utilice este aviso para comprobar qué instancias de ADC están cerca de EOM/EOL o están en compilaciones más antiguas.

   Basándose en estos conocimientos, Citrix ADM 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 ADC en Citrix ADM.

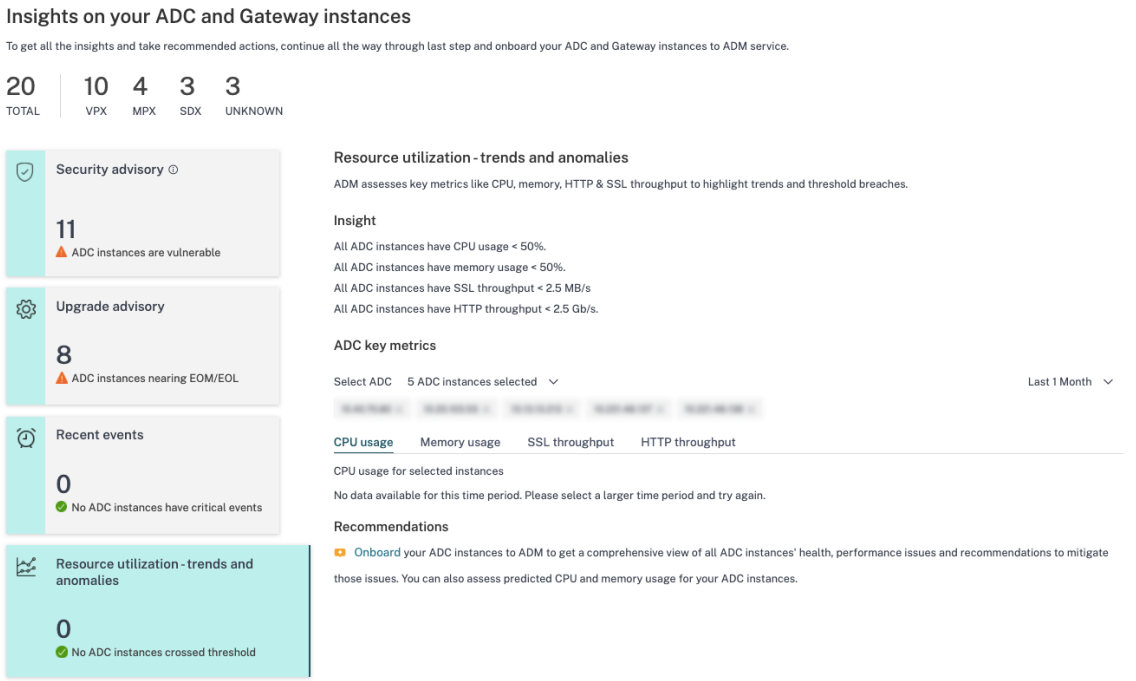


3. **Eventos recientes**: obtenga detalles de algunos errores críticos que han ocurrido en las instancias de ADC y una lista de instancias de ADC en las que se han producido los errores.

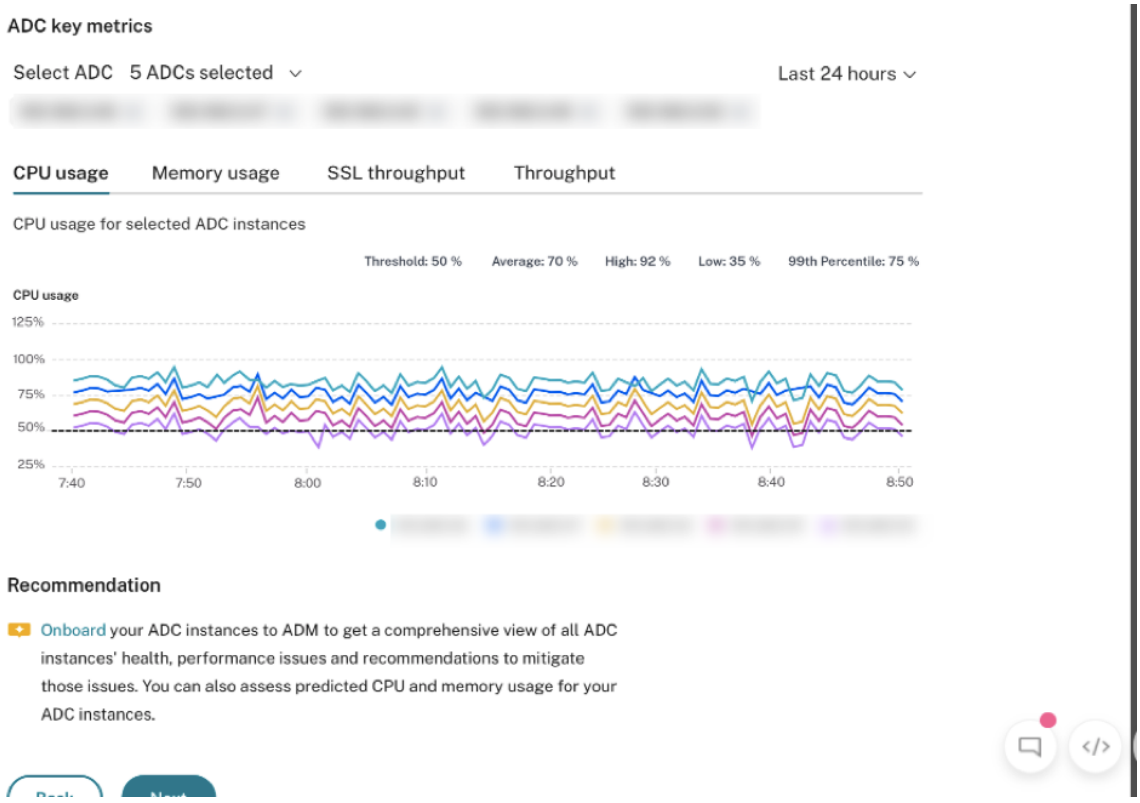


4. **Utilización de recursos: tendencias y anomalías**: Encuentre información sobre la alta utilización de recursos para CPU, memoria, rendimiento HTTP y rendimiento SSL. Para cada información, Citrix ADM sugiere la acción recomendada. Para tener más visibilidad de estos conocimientos y recomendaciones, debe incorporar sus instancias de ADC en Citrix ADM. Algunos beneficios después de la incorporación son:

    - CPU: prediga el uso de la CPU para las próximas 24 horas en Citrix ADM.
    - Memoria: prediga el uso de la memoria para las próximas 24 horas en Citrix ADM.
    - Rendimiento de SSL: vea la optimización de SSL en tiempo real con App Analytics inteligente en Citrix ADM.
    - Rendimiento HTTP: solucione problemas de capacidad de rendimiento de ADC con Infrastructure Analytics.

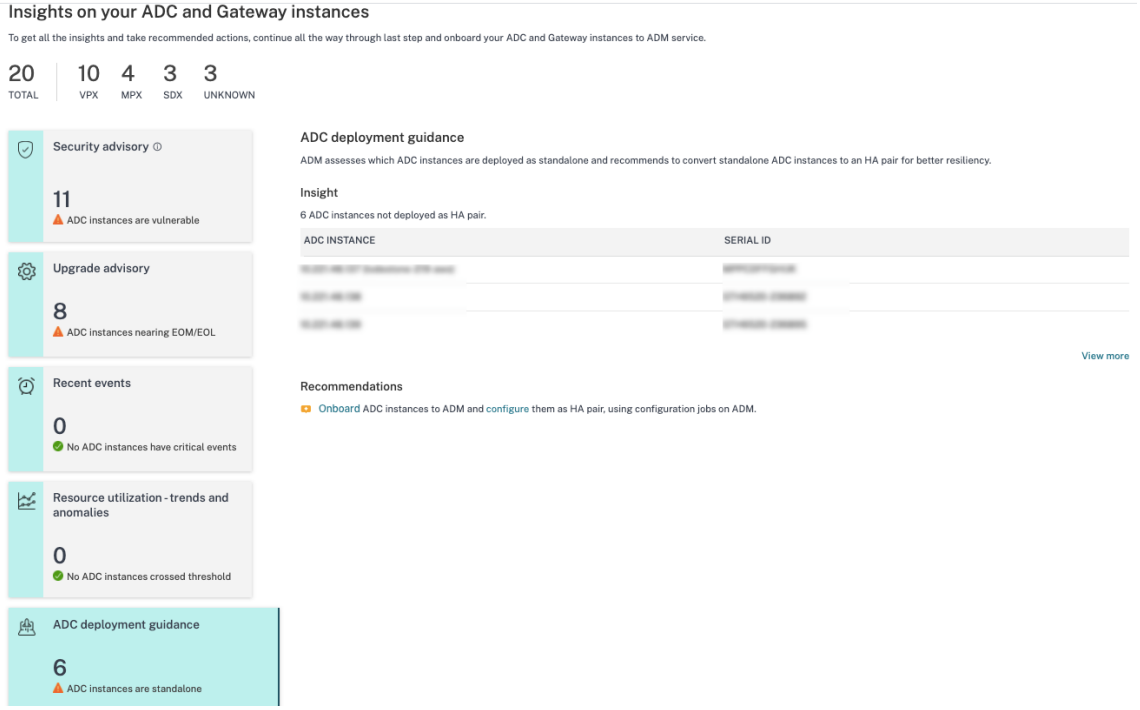


- **Métricas clave**: obtenga detalles de métricas clave relacionadas con la CPU, la memoria, el rendimiento HTTP, el rendimiento SSL y descubra tendencias anómalas en las métricas.



5. **Guía de implementación**: tenga visibilidad de las instancias de ADC que se implementan como un ADC independiente. Citrix ADM recomienda configurar estas instancias de ADC como un par

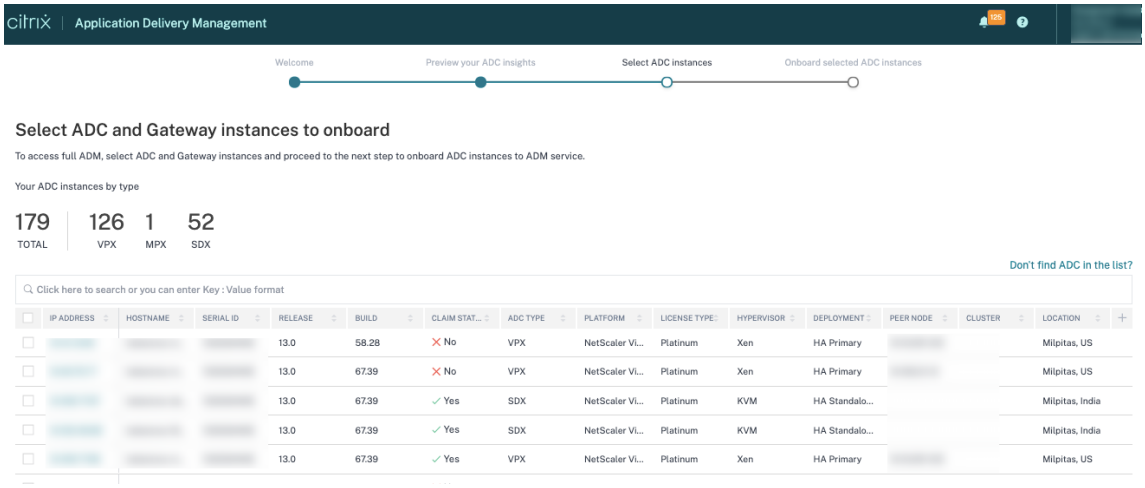
de HA para una mejor resiliencia. Esto requiere que incorpore sus instancias de ADC en Citrix ADM y, a continuación, utilice trabajos de mantenimiento para configurar las instancias como un par de HA.



Paso 3: Seleccione las instancias de ADC y Gateway para incorporarlas

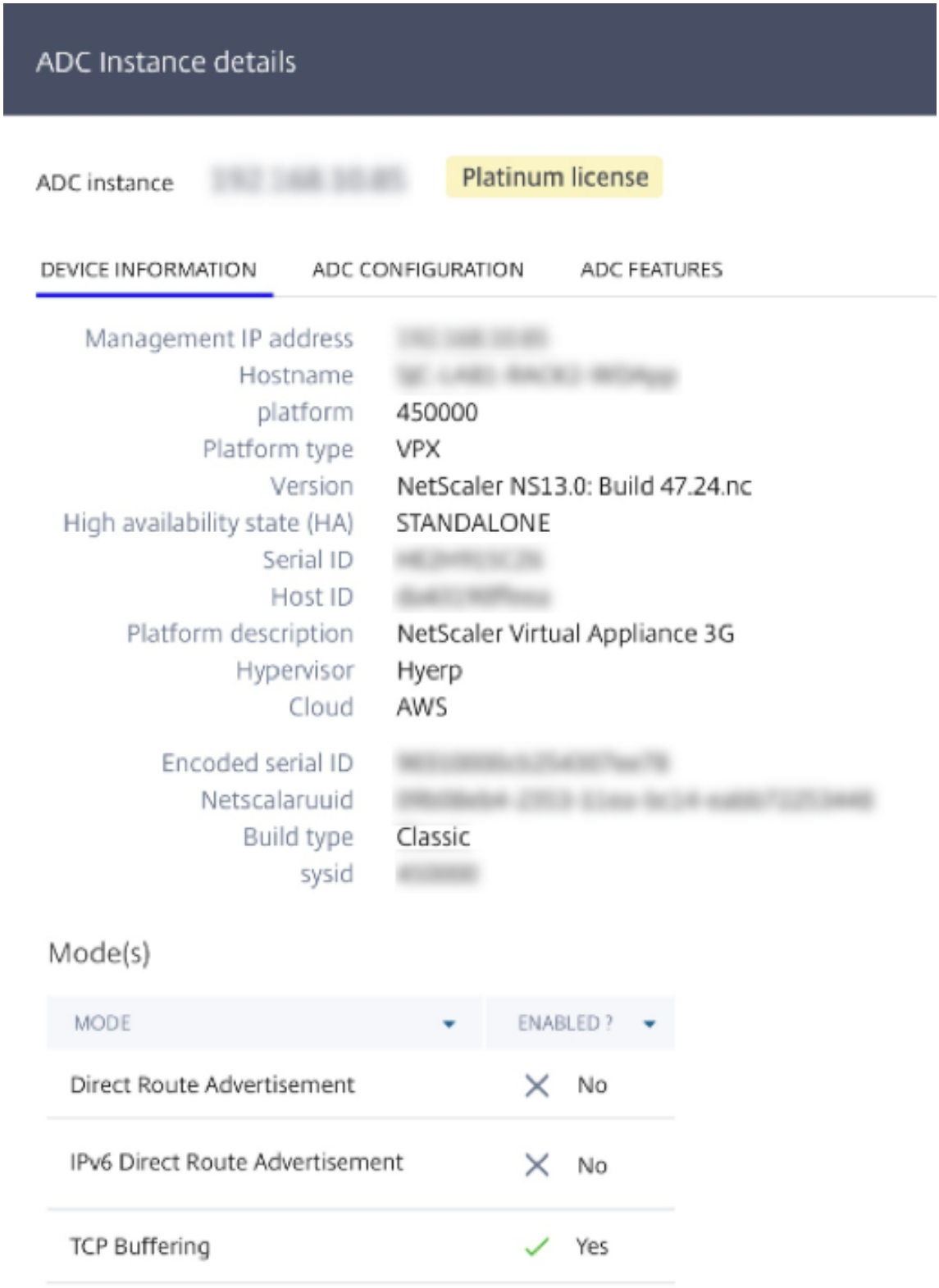
Esta página muestra todas las instancias de ADC y Gateway en su entorno. Consulte y seleccione las instancias de ADC y Gateway que quiere incorporar a Citrix ADM y haga clic en **Siguiente**.

1. Vea y seleccione las instancias de ADC que quiere incorporar a Citrix ADM.

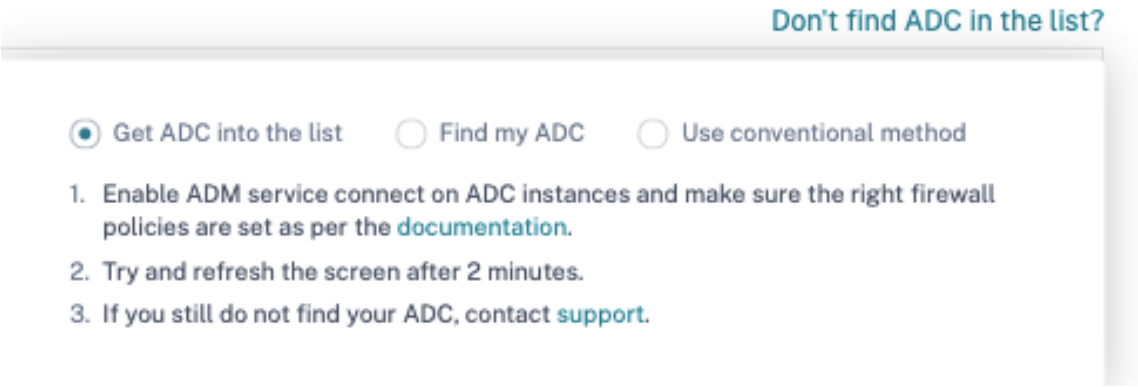


Si necesita detalles sobre cualquier instancia, como información del dispositivo, configuración de ADC, características de ADC disponibles o información de licencia, haga clic en la dirección

IP de la instancia situada debajo de la instancia de ADC.

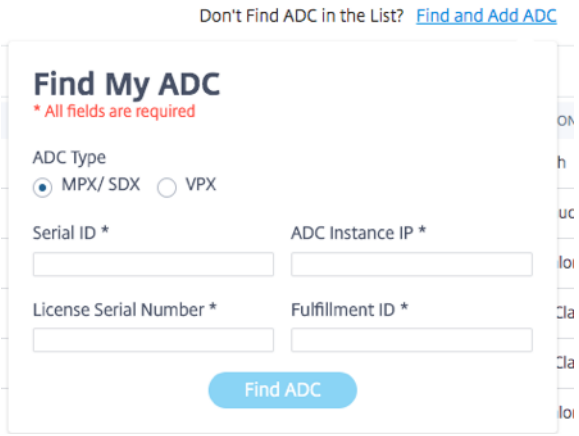


Si la instancia no aparece en la lista, utilice la **opción No encontrar ADC en la lista** de la esquina superior derecha.



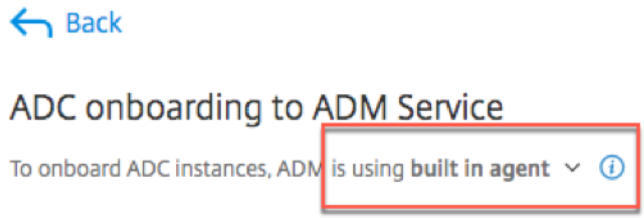
Puede proceder de tres maneras: siga los pasos que se indican en **Incluir ADC en la lista** o utilice la **opción Buscar mi ADC**. Si estos dos pasos no ayudan, haga clic en la opción **Usar método convencional**, que omite el flujo de trabajo y le llevará a través de la forma tradicional de incorporar instancias ADC.

Para la **opción Buscar mi ADC**, introduzca los detalles en los campos obligatorios (ID de serie, dirección IP de instancia de ADC, número de serie de licencia e ID de cumplimiento) y busque.



Paso 4: Incorporar instancias de ADC a Citrix ADM

Puede incorporarse a sus instancias utilizando el agente incorporado (opción predeterminada) o un agente externo.



Instancias de ADC integradas que utilizan un agente integrado

La incorporación automática y basada en scripts utiliza el agente integrado, que está configurado de forma predeterminada.

Incorporación automática: solo se admite en las siguientes versiones de ADC:

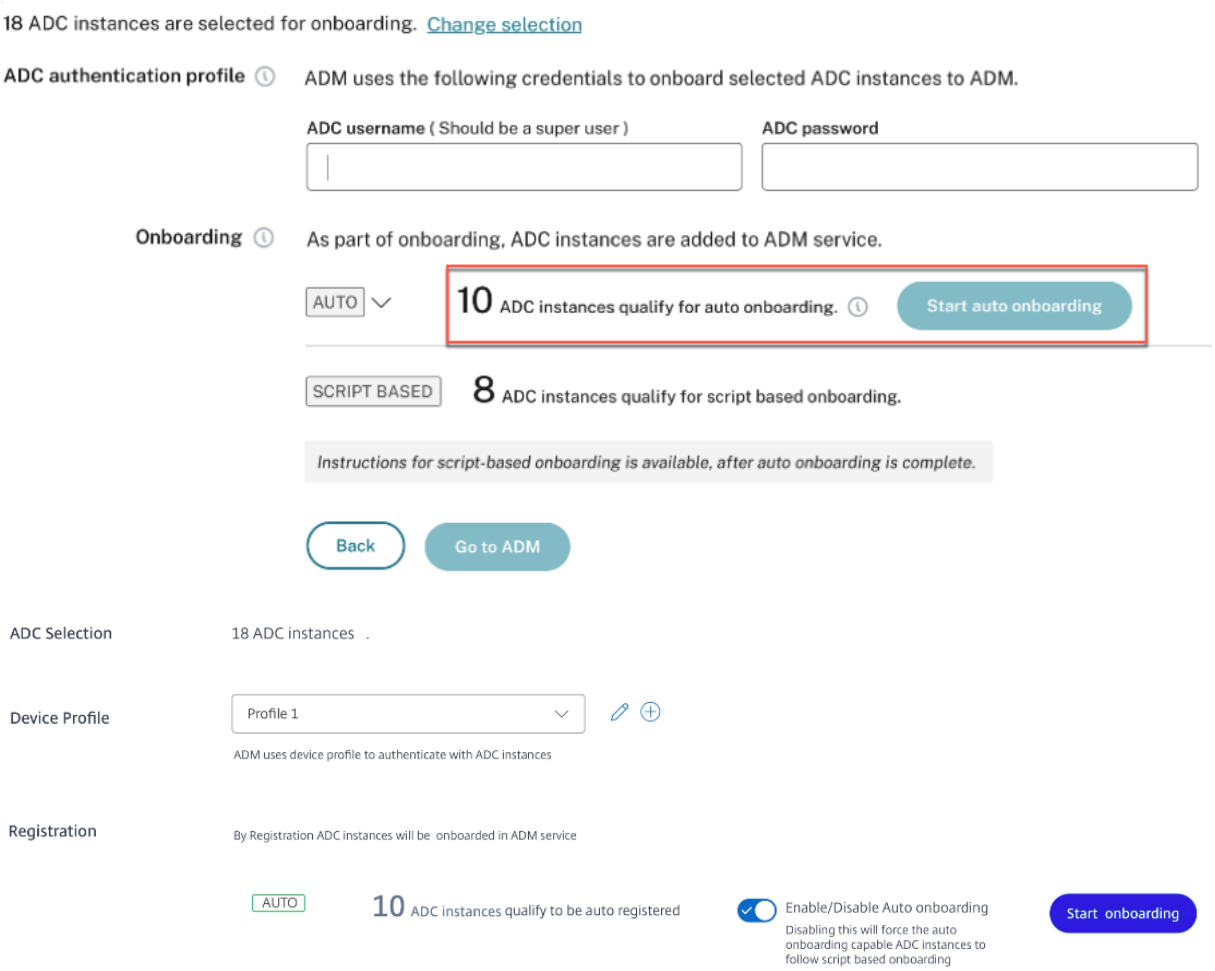
- Citrix ADC MPX y VPX imagen versión 12.1 57.18 y posteriores y 13.0 61.48 y posteriores
- Imagen de la versión de SDX 13.0 61.48 y posteriores y 12.1 58,14 y posteriores

Para seleccionar una instancia de ADC diferente, haga clic en **Cambiar selección**.

Del total de instancias ADC seleccionadas, algunas instancias pueden calificar para la incorporación automática (según criterios de versión mínima). Puede ver las instancias que califican para la incorporación automática.

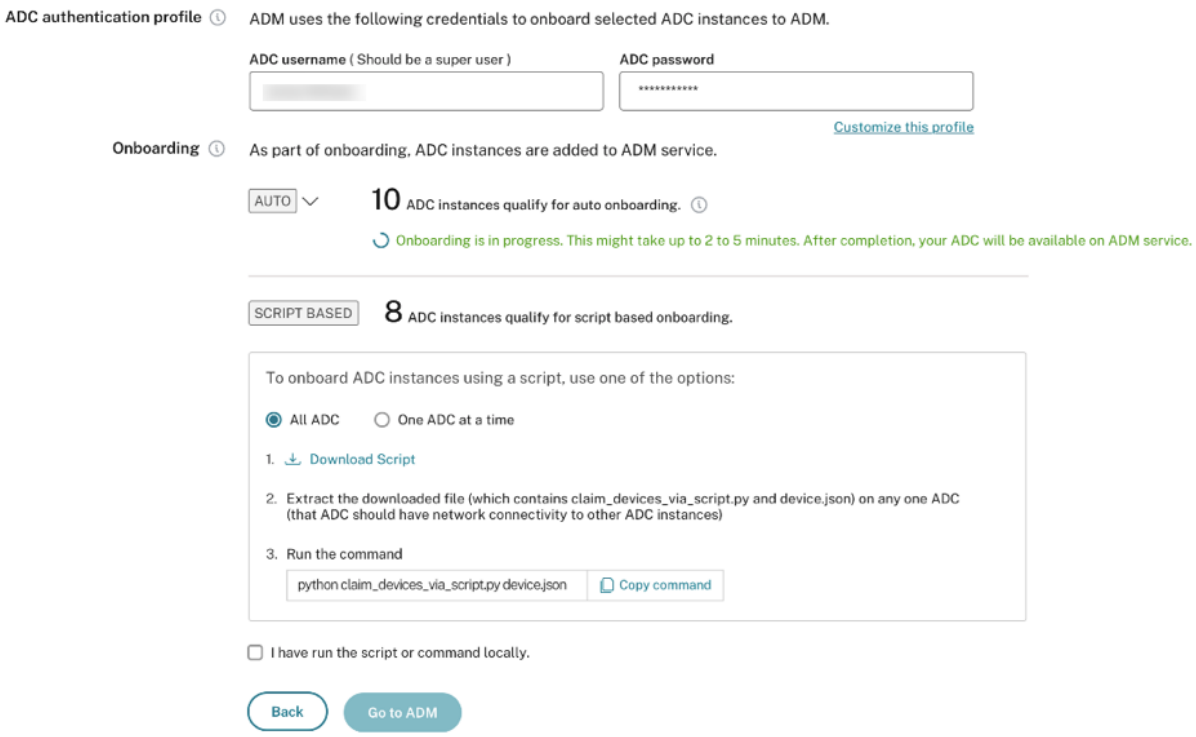
Puede realizar una prueba de incorporación para asegurarse de que la instancia de ADC esté lista para su incorporación. Haga clic en **Probar** para iniciar la prueba. Para obtener más información, consulte Probar la preparación para la incorporación de las instancias de ADC.

Si quiere embarcarse sin realizar la prueba, introduzca el nombre de usuario y la contraseña del ADC. Las credenciales deben ser credenciales de administrador de usuarios de ADC y Citrix ADM las usa para incorporar ADC. Haga clic en **Iniciar la incorporación automática** para incorporar sus instancias de ADC en Citrix ADM.



> **Nota:**
>
> Después de especificar las credenciales del ADC 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 ADC. Sin embargo, puede seleccionar el perfil en el menú desplegable **Perfil del dispositivo** para autenticar las instancias de ADC.

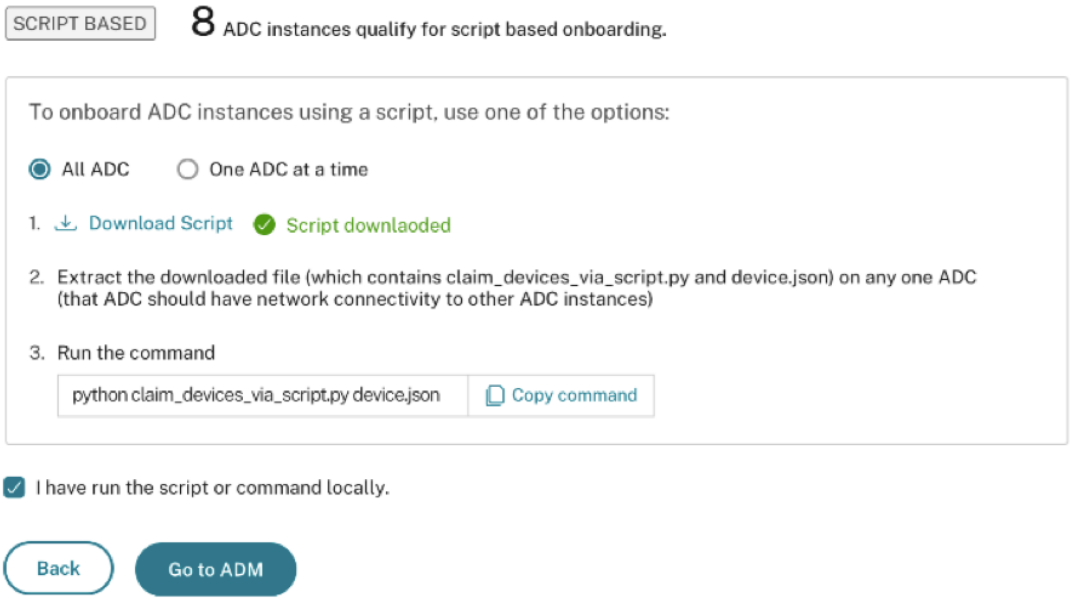
La incorporación automática puede tardar entre 2 y 5 minutos en completarse.



> **Nota:**
>
> Si no quiere que las instancias de ADC se incorporen automáticamente a Citrix ADM, puede deshabilitar 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 ejecutarlo en cualquiera de las instancias de ADC, utilizando el comando dado en la interfaz de usuario. Asegúrese de que la instancia de ADC en la que ejecuta este script tenga conectividad de red con todas las demás instancias de ADC seleccionadas.
- **Opción 2**: Inicie sesión en la consola CLI de cada instancia de ADC y ejecute los comandos dados en la interfaz de usuario. Para obtener más información, consulte el paso 7 del documento Configurar el agente integrado de ADC para administrar las instancias. Asegúrese de generar un nuevo código de activación único para cada una de las instancias de ADC.

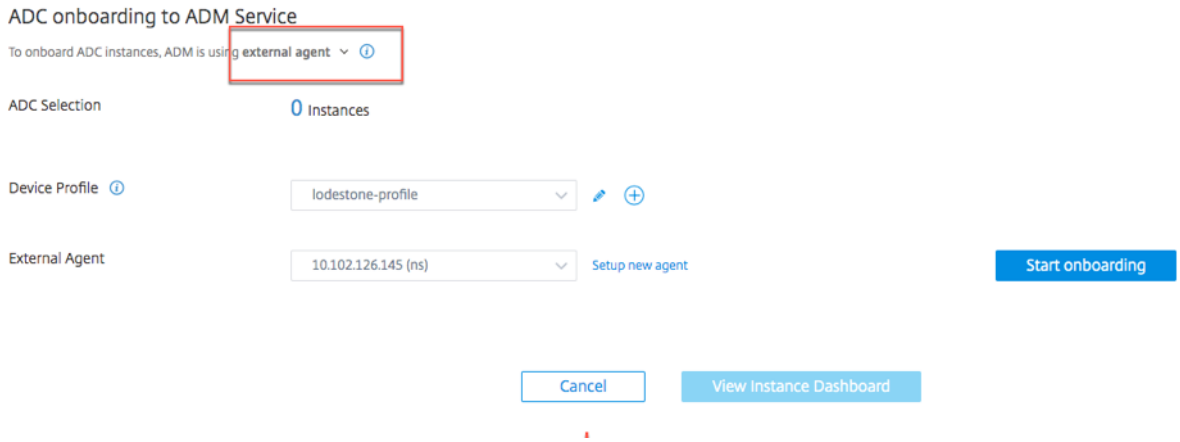


Una vez que haya incorporado todas las instancias, haga clic en **Ir a Citrix ADM** para ir al panel de la interfaz de usuario de administración de instancias de Citrix ADM y explorar las diferentes funciones.

> **Nota:**
>
> Si es un cliente nuevo de Citrix ADM sin una licencia de Citrix ADM, su cuenta de servicio de Citrix de forma predeterminada es una cuenta Express. Para obtener más información sobre los derechos de la cuenta Citrix ADM, consulte Administrar los recursos de Citrix ADM mediante una cuenta Express.

Instancias de ADC incorporadas mediante un agente externo

Puede utilizar la incorporación basada en agentes externos si quiere utilizar licencias agrupadas o la suite de análisis completa de Citrix ADM, o ambas utilizar las licencias agrupadas y la suite de análisis completa.



Siga estos pasos:

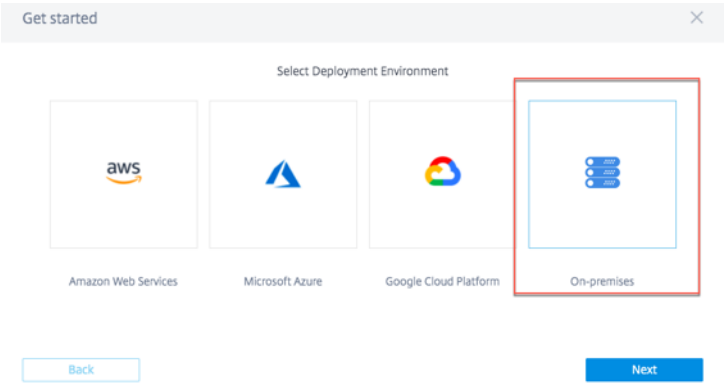
1. Seleccione un perfil de dispositivo.

   > **Nota**
   >
   > Por motivos de seguridad, no puede usar las credenciales ADC predeterminadas (nsroot/nsroot) para la incorporación.

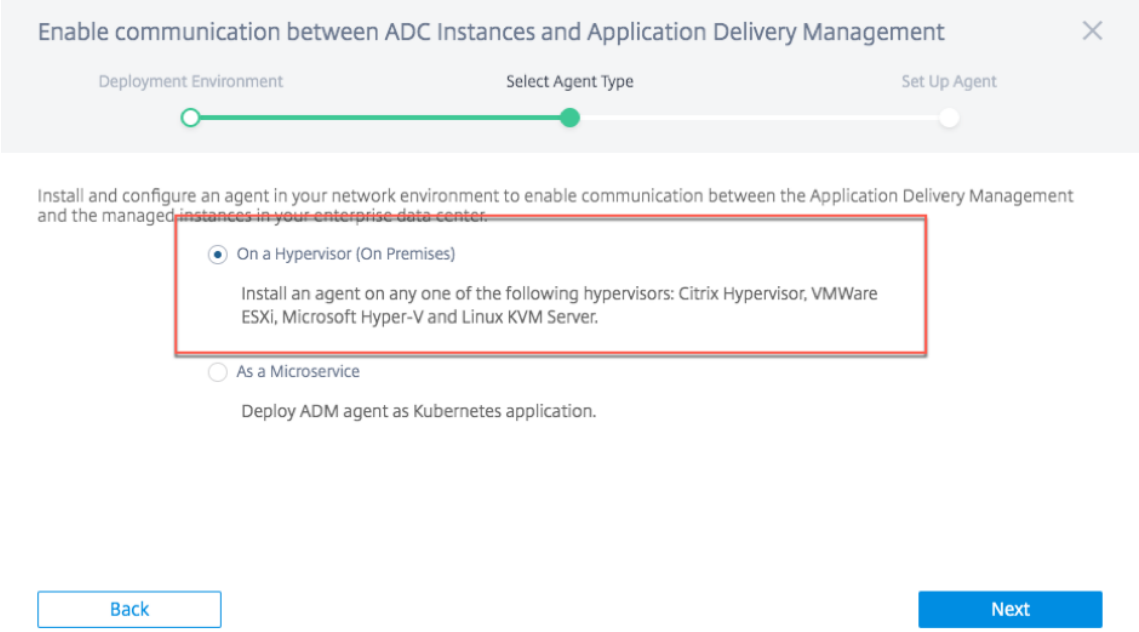
2. Seleccione un agente externo y haga clic en **Configurar nuevo agente**.
3. Seleccione cualquiera de los siguientes entornos:
   - Amazon Web Services
   - Microsoft Azure
   - Google Cloud Platform
   - Local

Instalar un agente en el hipervisor local

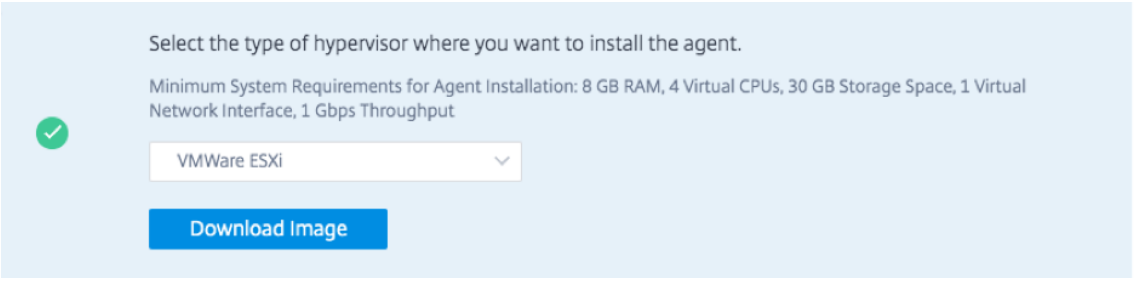
Si selecciona **Local**, puede instalar el agente en los siguientes hipervisores: Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM Server.



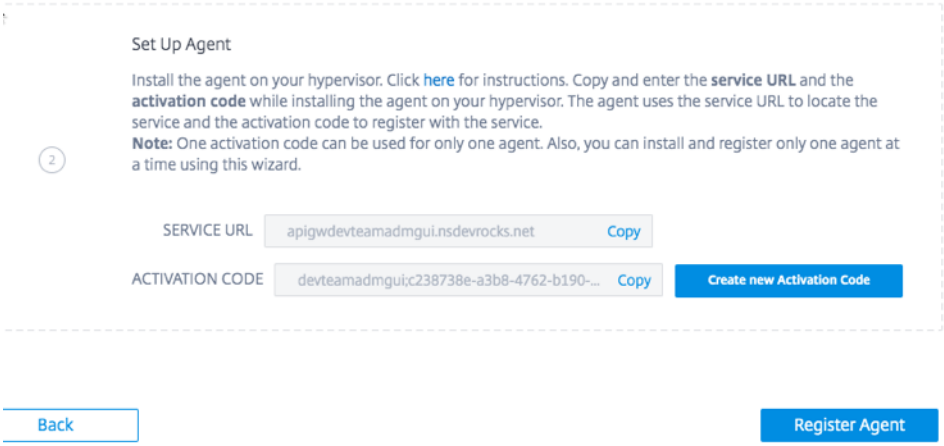
1. Seleccione **En un hipervisor (local)** y haga clic en **Siguiente**.



2. Seleccione el tipo de hipervisor y descargue la imagen, por ejemplo, VMware ESXi.



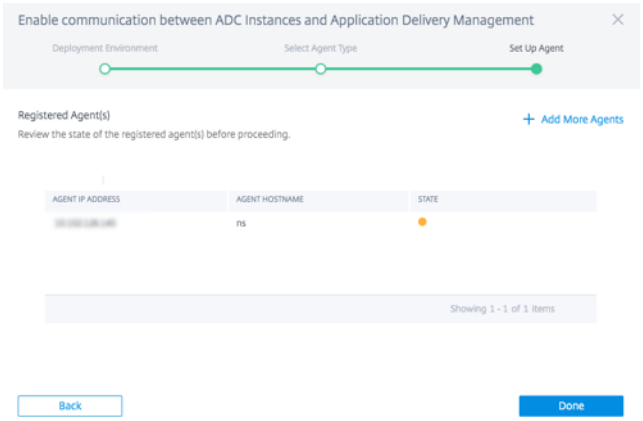
3. Utilice la URL del servicio y el código de activación para configurar el agente.



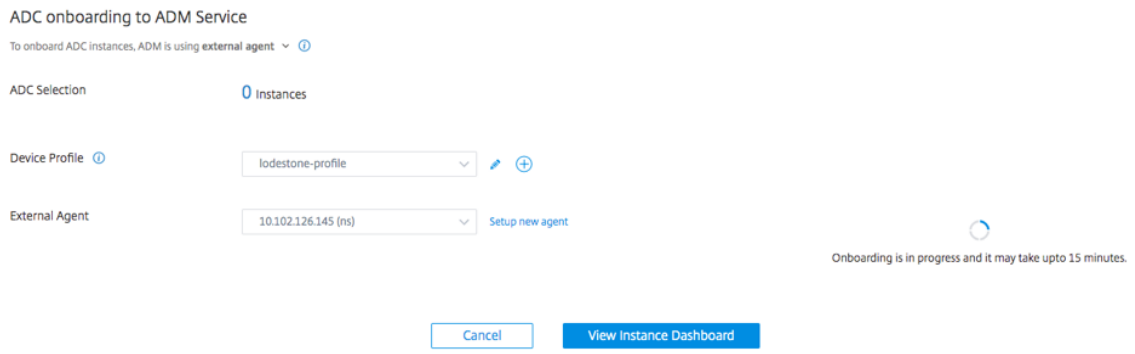
El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio. Para obtener instrucciones detalladas sobre la instalación de un agente

en su hipervisor local, consulte Instalar el agente Citrix ADM de forma local.

4. Haga clic en **Registrar agente**. Cuando haya terminado, haga clic en **Listo** para volver a la página de incorporación de Citrix ADM a ADC.



5. Haga clic en **Iniciar incorporación**. Una vez que haya incorporado todas sus instancias, haga clic en **Ver panel de instancias para ir al panel** de la interfaz de usuario de administración de instancias de Citrix ADM 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

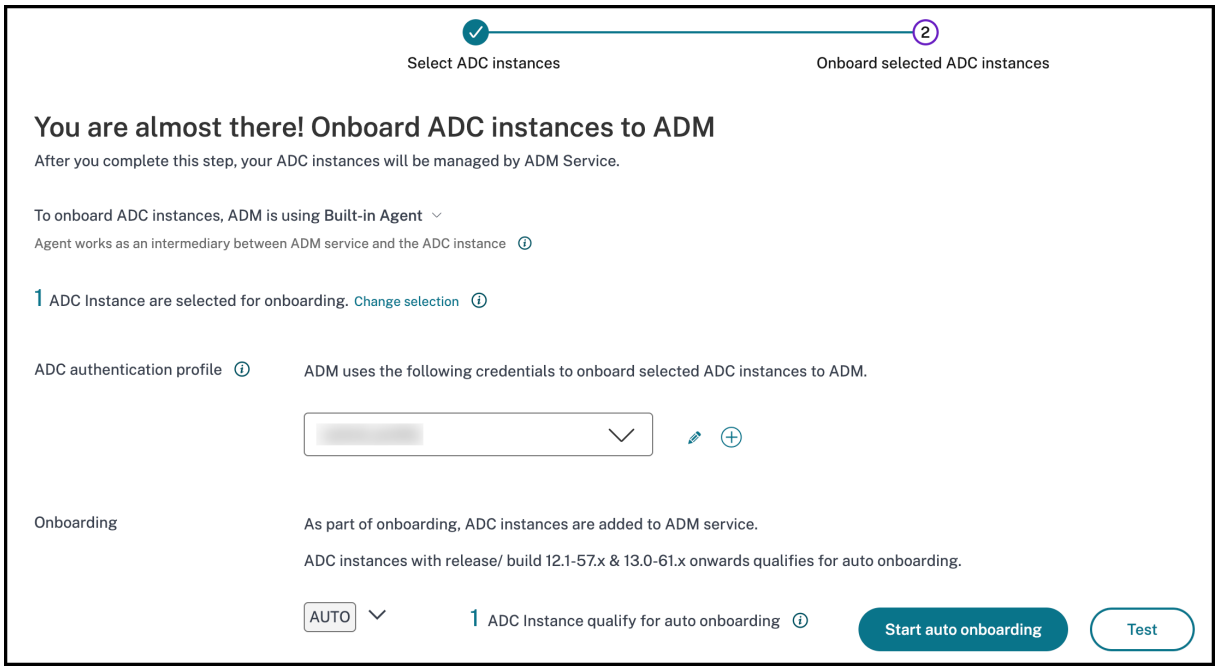
Para obtener más información, consulte los siguientes documentos:

- Instalar el agente Citrix ADM en la nube de Microsoft Azure
- Instalar el agente Citrix ADM en AWS
- Instalar el agente Citrix ADM en GCP

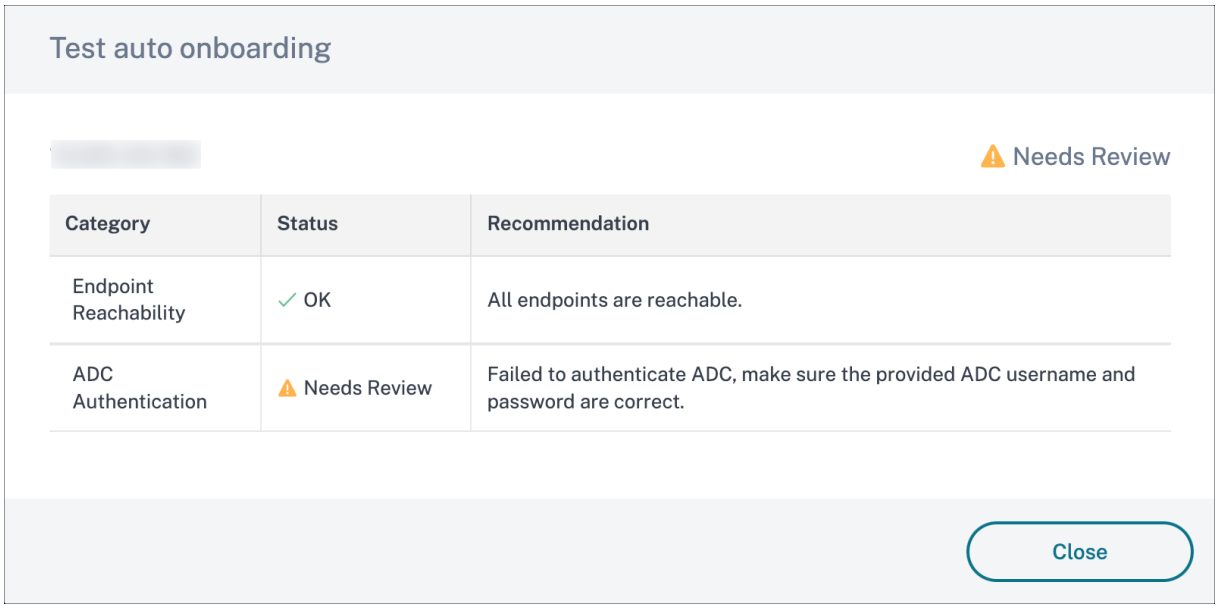
Pruebe la preparación para la incorporación de las instancias de ADC

November 16, 2022

Cuando quiera incorporar una instancia de ADC en Citrix ADM, 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 de detalles del diagnóstico de ADC muestra la categoría, el estado y la recomendación del problema.



Para obtener más información, consulte Ver la información de diagnóstico del ADC en la GUI de ADM.

Si el estado de ejecución de la prueba de ADC está **en estado de revisión**, entonces:

- Revise las credenciales de inicio de sesión de ADC en el perfil del dispositivo.
- No se puede acceder a los siguientes puntos finales:
  - `adm.cloud.com`
  - `agent.adm.cloud.com`
  - `trust.citrixworkapi.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 18, 2023

El servicio Citrix ADM permite la incorporación de instancias de Citrix ADC mediante el flujo de trabajo de incorporación sencillo basado en ADM Service Connect. Como parte de este flujo de trabajo, los clientes reciben correos electrónicos iniciados por el producto desde el servicio Citrix ADM. Puede habilitar o deshabilitar las notificaciones por correo electrónico que recibe como parte del flujo de trabajo de incorporación discreto basado en ADM Service 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 deshabilitar 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 deshabilitar y detener los correos electrónicos de todos los administradores de su organización.

Configurar ajustes de correo electrónico

Puede configurar los ajustes de correo electrónico y habilitar o deshabilitar los correos electrónicos que recibe como parte del flujo de trabajo de incorporación discreto basado en ADM Service Connect. Para configurar los **ajustes de correo electrónico**:

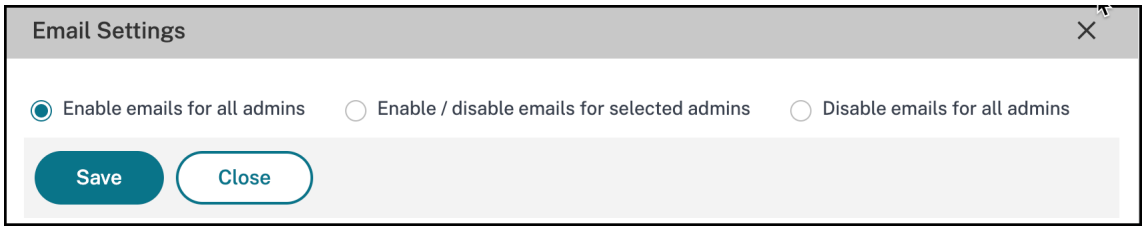
1. Haga clic en **Incorporar al servicio ADM** en el correo electrónico de inicio del producto. Aparece la página **Citrix Cloud** .
2. En la página de inicio de sesión de **Citrix Cloud** :
   - Si ya es cliente de Citrix Cloud, inicie sesión en Citrix Cloud con sus credenciales de Citrix.com, My Citrixo 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 ellos está en Citrix Cloud, inicie sesión con las credenciales existentes.

   Aparece la página de inicio de **entrega y administración de aplicaciones de Citrix**, que ofrece una descripción general de la entrega y administración de aplicaciones de Citrix y sus beneficios.
3. En la página de inicio de **entrega y administración de aplicaciones de Citrix**, haga clic en **Siguiente**.

   Aparece la página **Información sobre sus instancias de ADC y Gateway**, donde puede obtener información sobre su infraestructura general de ADC con recomendaciones.
4. En la página **Información sobre tus instancias de ADC y Gateway**, haga clic en **Siguiente**.

   Aparece la página **Seleccione las instancias de ADC y Gateway para incorporar**, donde puede ver una lista de instancias de ADC para 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** .

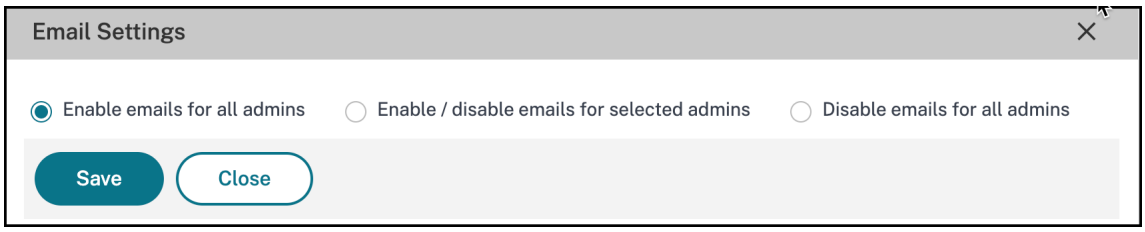
   Ahora puede configurar los ajustes de correo electrónico para habilitar o deshabilitar los correos electrónicos.

> **Nota:**
>
> Si ha incorporado solo una instancia de ADC, no recibirá estos correos electrónicos.

Si ya está en la GUI del servicio ADM y quiere configurar los ajustes del correo electrónico:

1. En Citrix Application Delivery and Management, vaya a **Infraestructura > Instances**y, a continuación, haga clic en **Citrix ADC**. Aparece la página **Citrix ADC** .
2. En la página **Citrix ADC**, haga clic en **Inventario de activos**.

   La página **Seleccione las instancias de ADC y Gateway para incorporar** aparece para mostrar la lista de instancias de ADC que están incorporadas y opciones adicionales, como la **configuración del correo electrónico**.
3. Haga clic en **Configuración de correo electrónico** Aparece el panel **Configuración de correo electrónico** .



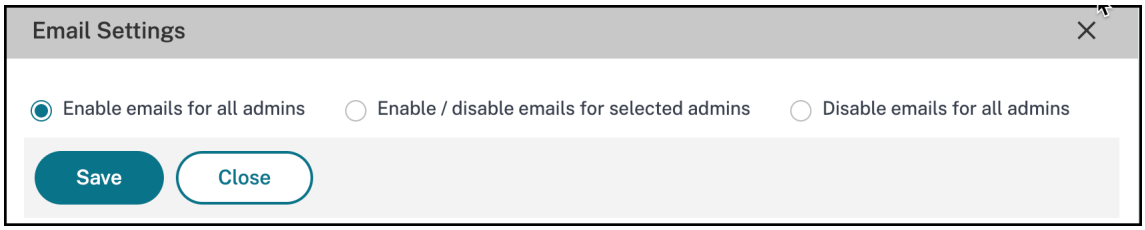
   Ahora puede configurar los ajustes de correo electrónico para habilitar o deshabilitar los correos electrónicos.

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 ADM Service Connect:

1. En el panel **Configuración de correo electrónico**, selecciona **Habilitar correos electrónicos** para todos los administradores.



2. Haga clic en **Guardar** y **Cerrar**.

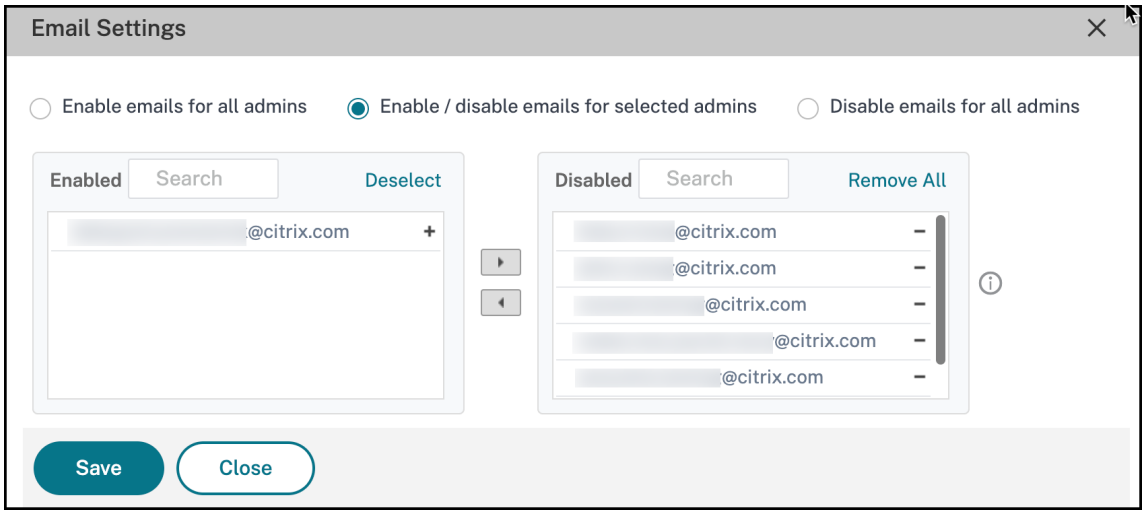
   Todos los administradores de la organización ya están suscritos y recibirán notificaciones por correo electrónico como parte del flujo de trabajo basado en ADM Service Connect.

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 deshabilitados a la derecha.

Para deshabilitar 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 **deshabilitados** .

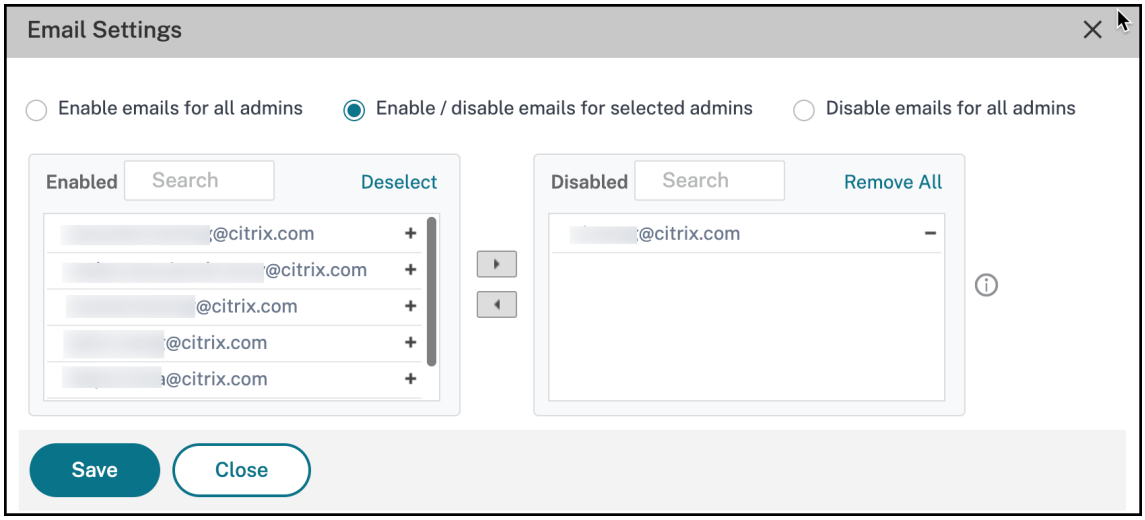
3. Haga clic en **Guardar** y **Cerrar**.

   El administrador ya no está suscrito para no recibir notificaciones por correo electrónico como parte del flujo de trabajo basado en ADM Service Connect.

   > **Nota**
   >
   > Si quiere deshabilitar los correos electrónicos para varios administradores, seleccione todos sus ID de correo electrónico en la lista de correos electrónicos **habilitados** y haga clic en el botón Agregar (**+**) para agregar los ID de correo electrónico a la lista de **deshabilitados** . Haga clic en **Guardar** y **Cerrar**.

Si anteriormente ha deshabilitado 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 **deshabilitados** .
2. Haga clic en el botón de eliminación (-). Verás que la dirección de correo electrónico del administrador se elimina de la lista de **deshabilitados** .



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.

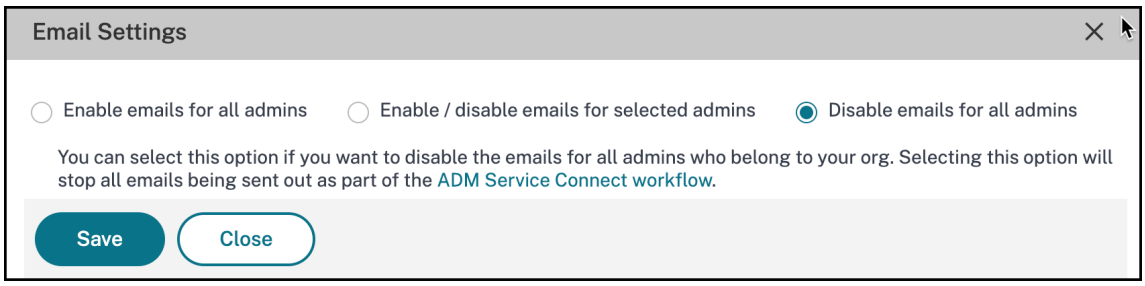
   > **Nota**
   >
   > Si quiere habilitar los correos electrónicos para varios administradores, seleccione todos sus ID de correo electrónico en la lista de correos electrónicos **deshabilitados** y haga clic en el botón de eliminación (-) para agregar los ID de correo electrónico a la lista de **activados** . Haga clic en **Guardar** y **Cerrar**.

Desactivar los correos electrónicos para todos los administradores

Puede seleccionar esta opción si quiere deshabilitar o detener los correos electrónicos de todos los administradores que pertenecen a su organización.

Para deshabilitar 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.

Solucionar problemas mediante la herramienta de diagnóstico o la GUI de ADM

November 16, 2022

> Nota
>
> La herramienta de diagnóstico solo se aplica a las instancias de ADC incorporadas o que se van a incorporar mediante la incorporación discreta basada en Citrix ADM Connect.
>
> Para obtener más información, consulte Incorporación discreta de instancias de Citrix ADC mediante Citrix ADM connect.

Cuando incorpora una instancia de ADC en Citrix ADM, es posible que experimente algunos problemas que impidan que la instancia de ADC se incorpore correctamente. Como administrador, 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 ADC está lista para su incorporación?
- Quiere analizar los problemas de las instancias de ADC ya integradas que muestran el estado «Inactivo» en la GUI de Citrix ADM

Si la conexión al servicio ADM está habilitada en la instancia de ADC, los detalles del diagnóstico se envían automáticamente a Citrix y puede verlos en la GUI de ADM. Si la conexión al servicio ADM no está habilitada, puede utilizar la herramienta de diagnóstico manualmente.

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 comprobar la versión `mastools` ejecutando el comando `cat /var/mastools/version.txt` en la instancia de ADC.

Para ejecutar la herramienta de diagnóstico:

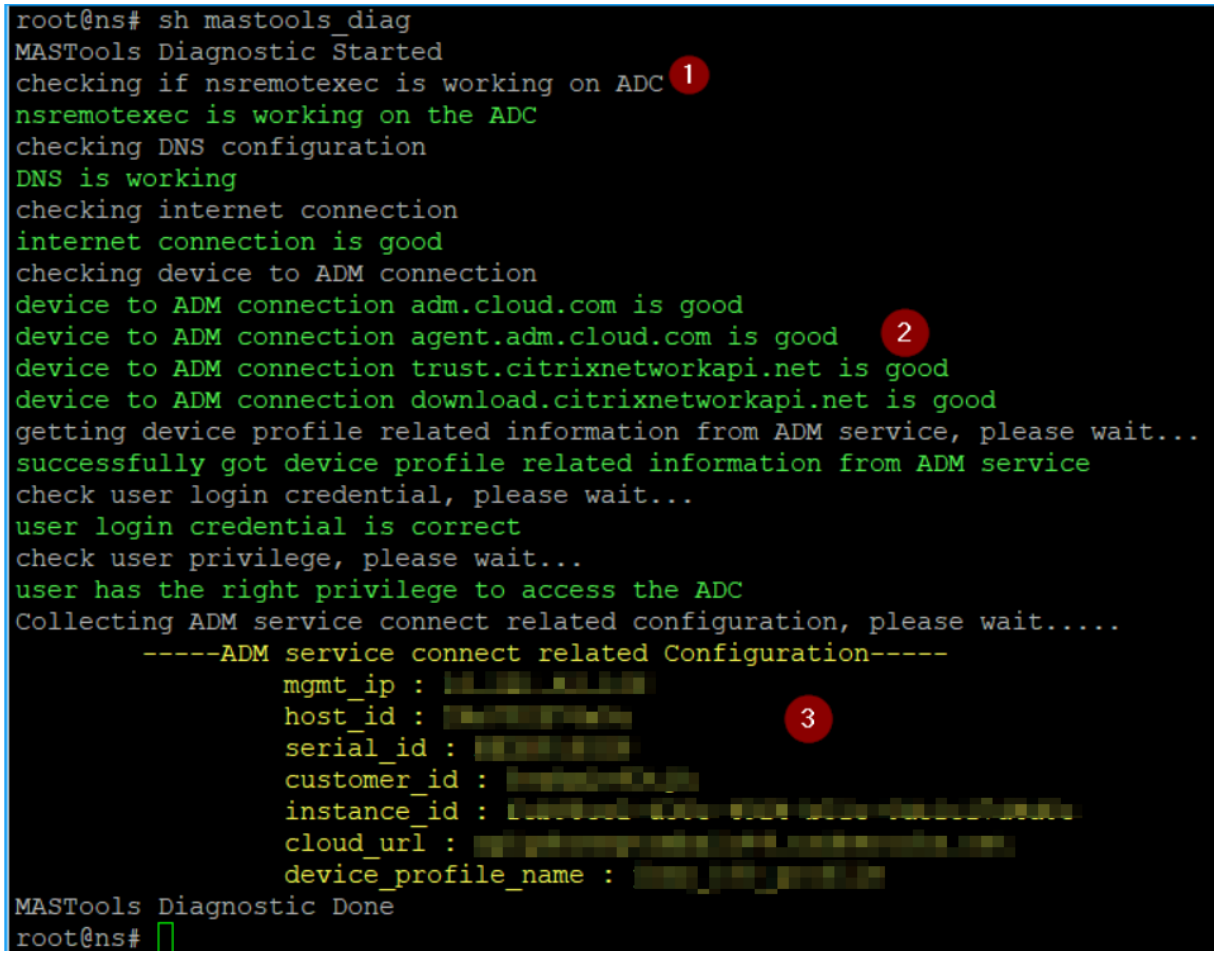
1. Con un cliente SSH, inicie sesión en la instancia ADC.
2. Escribe shell y presiona Entrar para cambiar al modo bash.
3. Escriba `cd /var/mastools/scripts`.
4. Escriba `sh mastools_diag`.

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 resolución de problemas, puede ponerse en contacto con el soporte de Citrix Al ponerse en contacto con el soporte de Citrix, debe proporcionar la información de configuración de ADM Connect que se muestra después de ejecutar la herramienta de diagnóstico.

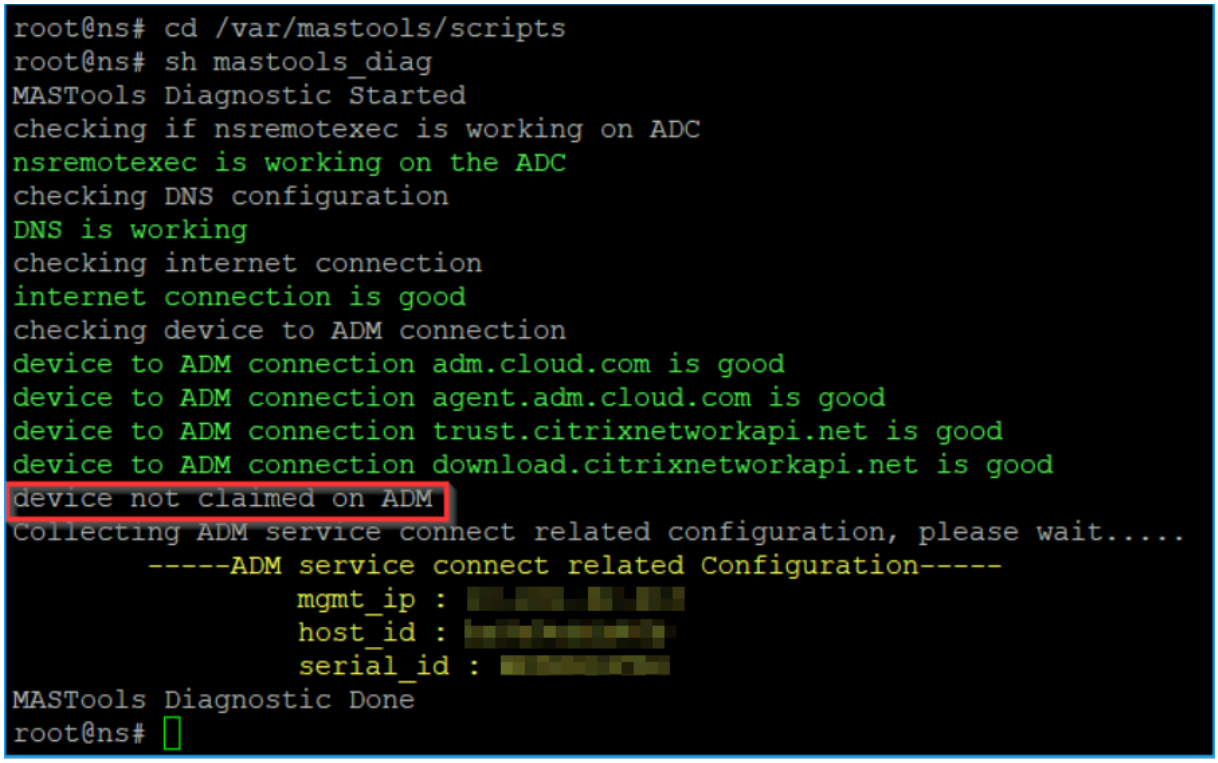
A continuación, se muestra un ejemplo de los resultados de diagnóstico de una instancia de ADC que no presenta problemas:



- **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 Citrix ADM en amarillo cada vez que ejecuta la herramienta de diagnóstico. Si quiere ponerse en contacto con el servicio de asistencia de Citrix, debe proporcionar esta información.

Valide la preparación de la instancia de ADC para la incorporación mediante la herramienta de diagnóstico

Antes de incorporar la instancia de ADC en Citrix ADM, puede comprobar si la instancia de ADC está lista ejecutando la herramienta de diagnóstico en la instancia de ADC. Si la instancia de ADC no tiene problemas y está lista para integrarse, la herramienta muestra el **dispositivo no reclamado en el mensaje de ADM** .



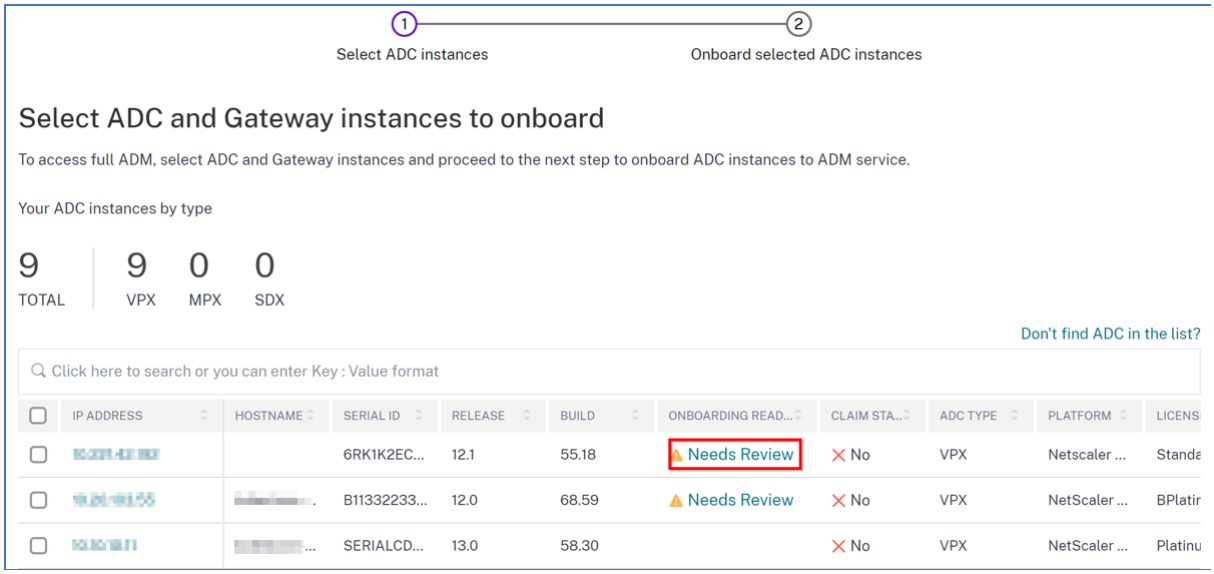
Ver información de diagnóstico del ADC en la GUI de ADM

Vaya a **Infraestructura > Instancias > Citrix ADC** y haga clic en **Inventario de activos** para 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**.

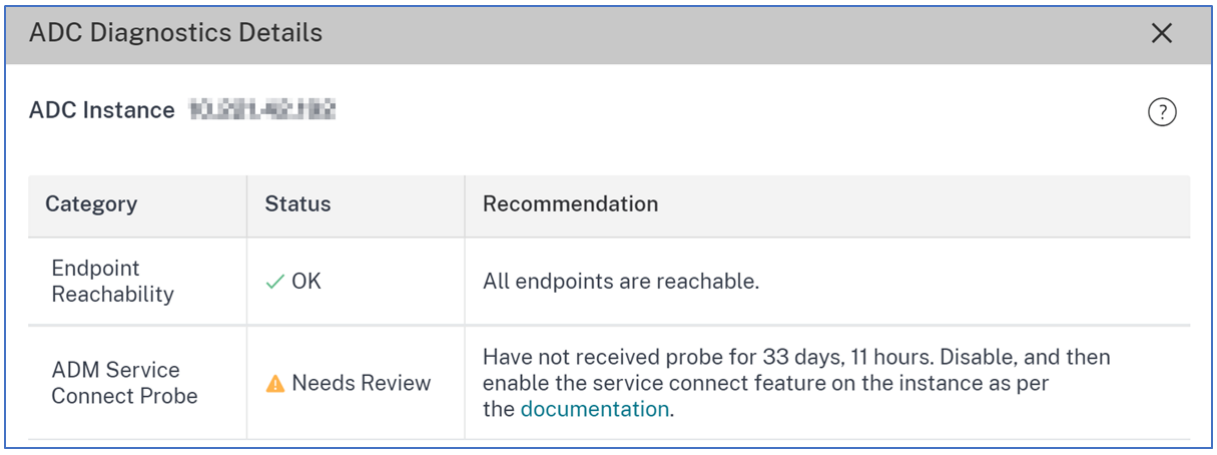
- **Necesita revisión**. La instancia ADC tiene problemas que deben solucionarse.
- **OK**. La instancia ADC está lista para su incorporación.

> Nota
>
> Si la opción **Preparación para la incorporación** aparece en blanco, significa que la instancia de ADC no se está ejecutando con la imagen más reciente compatible con el diagnóstico.

Si la instancia de ADC tiene algún problema, aparece la opción **Necesita revisión** y puede hacer clic para ver más detalles.



Tras hacer clic en **Necesita revisión**, la página **Detalles de diagnóstico del ADC** muestra los detalles del problema.



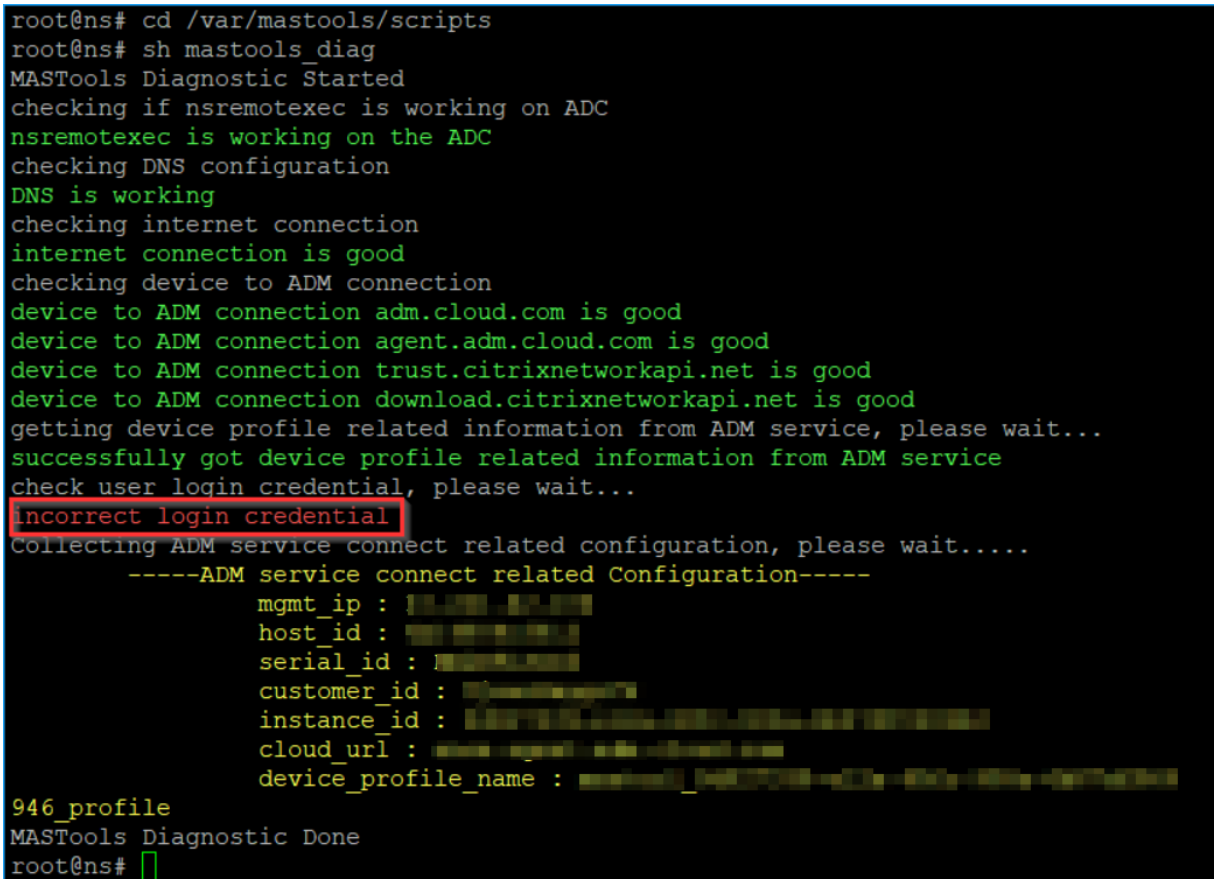
- **Categoría**. Proporciona la categoría del problema.
- **Status**. Indica el estado del problema, como **Necesita revisión**, **OK**o **No aplicable**.
- **Recomendación**. Proporciona la recomendación necesaria para solucionar el problema.

Tras solucionar el problema, el estado de preparación para la incorporación cambia a **Aceptar**.

Solución de problemas

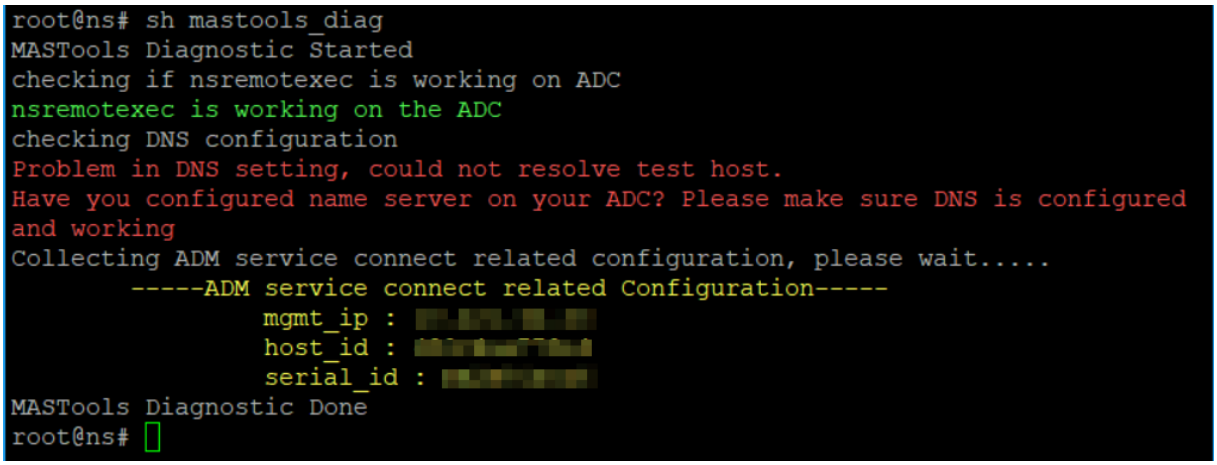
A continuación, se muestran algunos de los problemas de la instancia ADC y sus pasos para solucionarlos:

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 ADC, 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 endpoint de Citrix ADM

Solución alternativa: Asegúrese de comprobar la configuración del firewall y de que los siguientes puntos de enlace de Citrix ADM no estén bloqueados en el firewall:

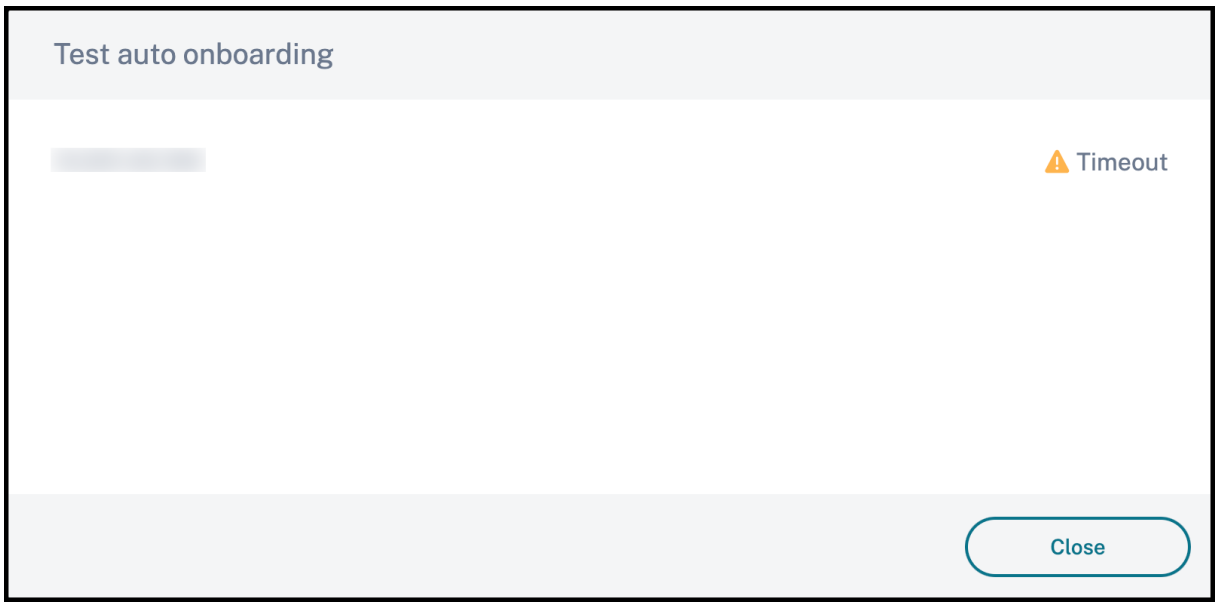
```
ADM_GRP_EP = "adm.cloud.com"

ADM_AGENT_EP = "agent.adm.cloud.com"

ADM_TRUST_EP = "trust.citrixnetworkapi.net"

ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
<!--NeedCopy-->
```

Si no se encontró ningún problema en las comprobaciones de diagnóstico y el problema de falta de conexión persiste, tome nota de la información de configuración de Citrix ADM (disponible en amarillo) y póngase en contacto con el soporte de Citrix.

Al realizar una ejecución de prueba para garantizar que la instancia de ADC esté lista para su incorporación, pueden aparecer los siguientes problemas:

Tiempo de espera incorporado del agente en seco

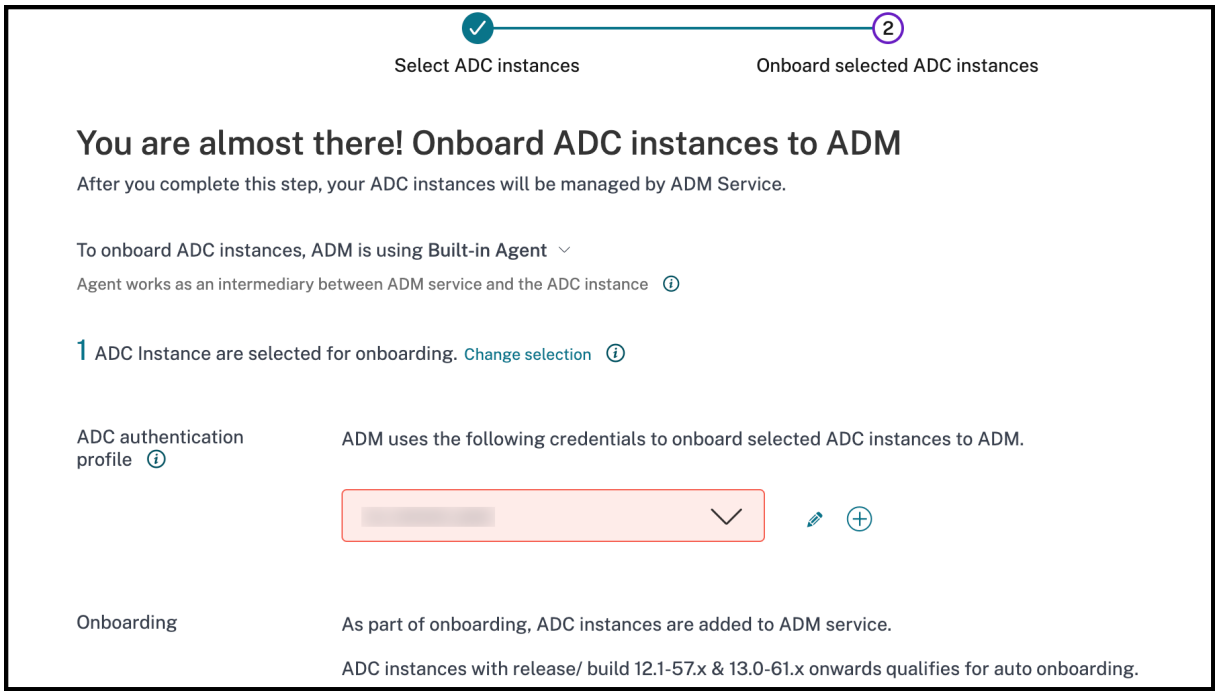
Si no se obtienen los resultados del simulacro transcurridos 5 minutos, aparece un mensaje de tiempo de espera.



Recomendación: Se recomienda que compruebe si la instancia de ADC se ejecuta 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 ADC falla durante la ejecución y aparece un contorno rojo en el menú desplegable del perfil del dispositivo.



Recomendación: Vuelva a introducir las credenciales de administrador del usuario de ADC, cree el

perfil del dispositivo y haga clic en Probar para volver a ejecutar el simulacro.

Transición de un agente integrado a un agente externo

November 16, 2022

Es posible que haya empezado a utilizar Citrix ADM únicamente para la administración y la supervisión y, más adelante, puede que quiera utilizar otras funciones, como el análisis y las licencias agrupadas. Para ello, debe pasar del agente Citrix ADM integrado a un agente externo.

El agente integrado solo admite funciones de administración y supervisión. Para otras funciones de Citrix ADM, como el análisis y las licencias agrupadas, necesita un agente externo. Este documento describe los pasos para la transición de un agente integrado de Citrix ADM existente a un agente externo basado en hipervisor.

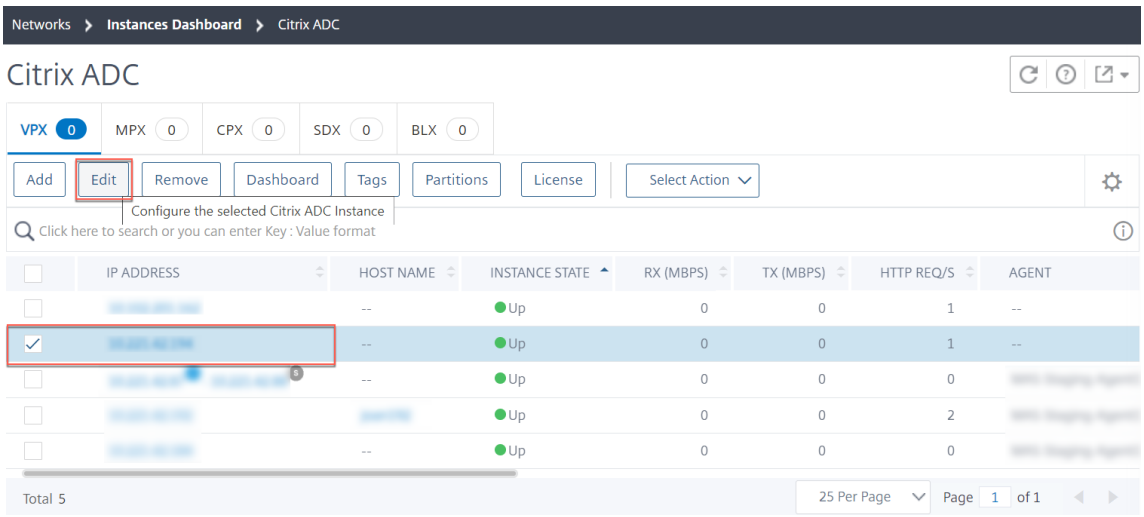
Antes de comenzar

Instale un agente externo antes de iniciar la transición. Siga el procedimiento que se indica en el tema Instalación del agente Citrix ADM de forma local.

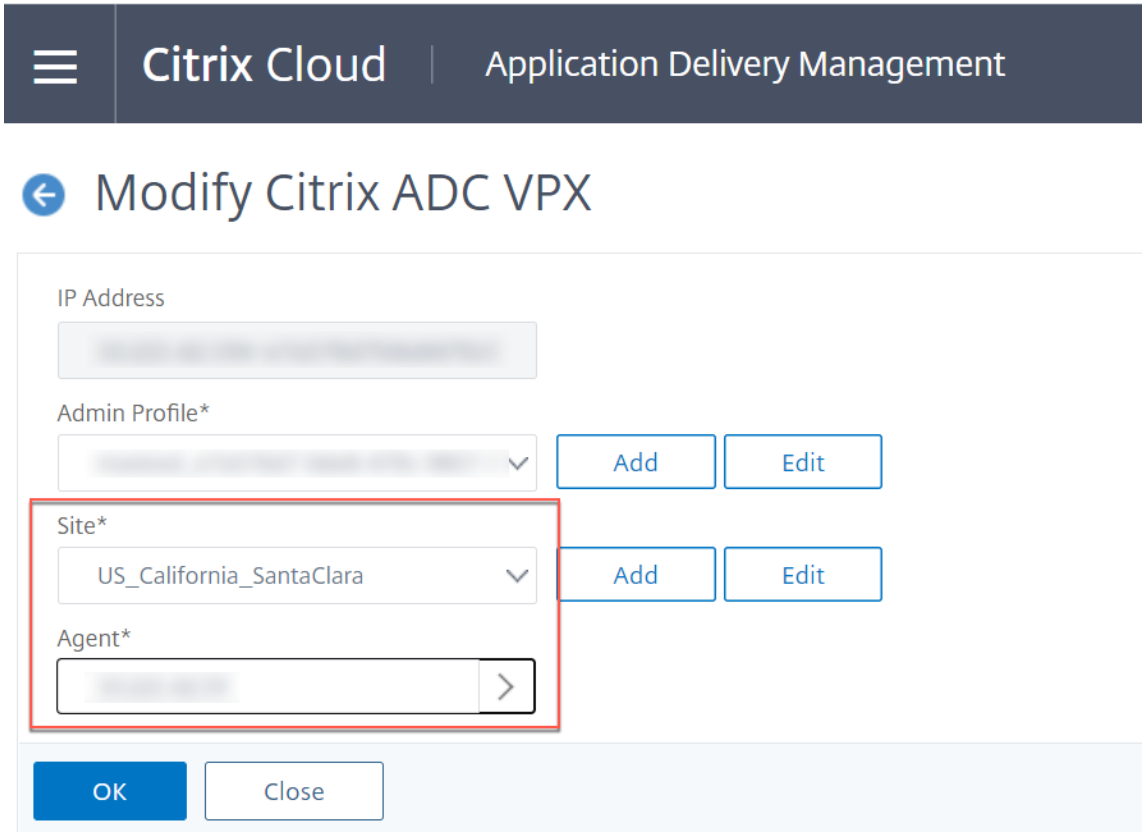
Transición de un agente integrado a un agente externo

Siga estos pasos para realizar la transición de un agente integrado a un agente externo:

1. En la GUI de Citrix ADM, en **Infraestructura > Panel de instancias > Citrix ADC**, seleccione la instancia de Citrix ADC y haga clic en **Modificar**.



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 el servicio ADM y agregar el agente al sitio, consulte Agregar instancias

Requisitos del sistema

February 27, 2023

Antes de empezar a utilizar Citrix ADM, debe revisar los requisitos de software, los requisitos del navegador, la información de puertos, la información de licencias y las limitaciones.

Exploradores web compatibles

Para acceder a Citrix ADM, su 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 el Citrix ADM 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 para cada agente de Citrix ADM. En la siguiente tabla se enumeran los requisitos del agente para aprovechar todas las funciones de Citrix ADM:

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 utilizar los siguientes tipos de máquinas virtuales de los respectivos mercados en la nube para aprovechar todas las funciones de Citrix ADM:

Nube	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`

Nube	Requisitos del agente	Tipo de máquina virtual preferido
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`

Para obtener instrucciones acerca de la instalación de un agente, consulte los siguientes vínculos:

- Instalación del agente Citrix ADM en Microsoft Azure Cloud.
- Instalación del agente Citrix ADM en AWS.
- Instalación del agente Citrix ADM en Google Cloud.

Agente ligero para licencias agrupadas

Si planea usar Citrix ADM solo para licencias agrupadas, puede usar un agente con especificaciones más bajas, como se indica en la siguiente tabla:

Componente	Requisito
RAM	8 GB
CPU virtual	4
Espacio de almacenamiento	30 GB

Estos agentes con especificaciones más bajas (ligeros) solo son compatibles con Citrix ADM.

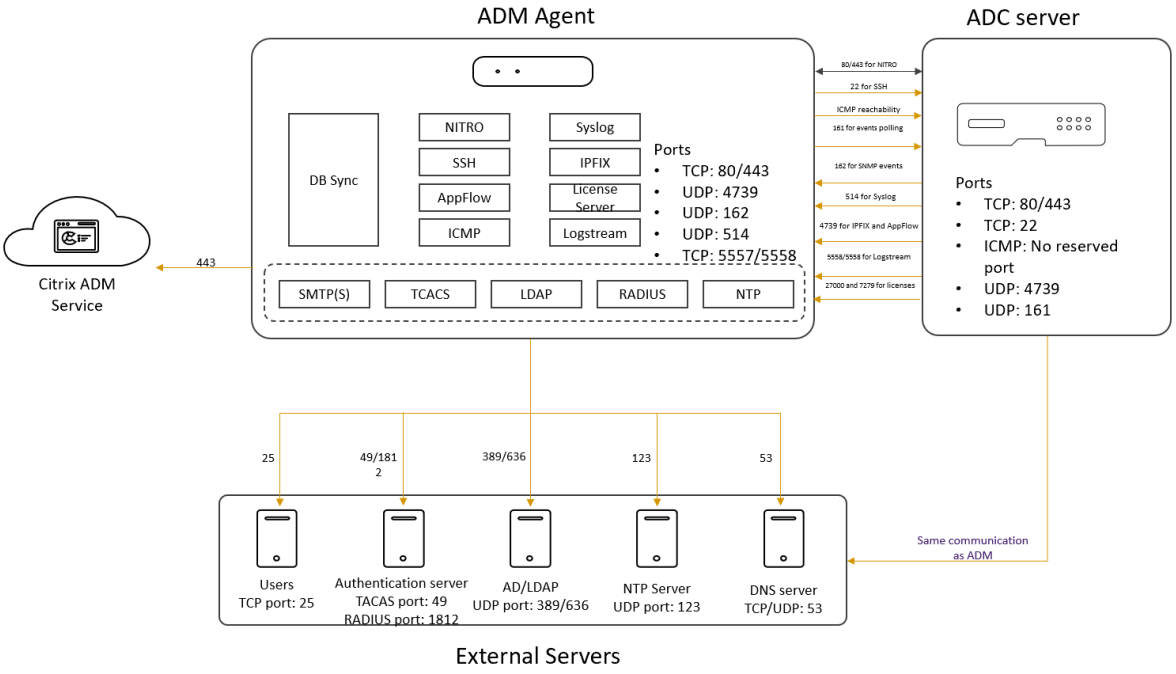
Citrix recomienda utilizar los siguientes tipos de máquinas virtuales de los respectivos mercados en la nube para utilizar únicamente la función de licencias agrupadas:

Nube	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 deshabilitar la programación de tareas predeterminada, vaya a **Configuración > Configuración global > Funciones configurables**.

Puertos compatibles

Para las comunicaciones entre las instancias de Citrix ADC y el agente Citrix ADM y el agente Citrix ADM, abra los puertos necesarios.



Puertos para el agente Citrix ADM

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

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

Puerto	Tipo	Detalles	Dirección de comunicación
514	UDP	Para recibir mensajes de syslog desde la instancia de Citrix ADC al servicio Citrix ADM.	Citrix ADC a agente Citrix ADM
5557/5558	TCP	Para la comunicación de flujo de registro (para violaciones de seguridad de WAF, Web Insight y HDX Insight) desde Citrix ADC al servicio Citrix ADM.	De Citrix ADC al agente Citrix ADM
27000 y 7279	TCP	Puertos de licencia para la comunicación entre el agente Citrix ADM y la instancia ADC. Estos puertos también se utilizan para licencias agrupadas de ADC.	Citrix ADC a agente Citrix ADM
443	TCP	Puertos para la comunicación entre el agente Citrix ADM y el servicio Citrix ADM	Del agente Citrix ADM al servicio Citrix ADM

Puertos para instancias de ADC

En esta tabla se explican los puertos obligatorios que deben estar abiertos en las instancias de Citrix ADC.

Puerto	Tipo	Detalles	Dirección de comunicación
80/443	TCP	Para la comunicación NITRO desde Citrix ADM a la instancia de Citrix ADC.	Agente de Citrix ADM a Citrix ADC y Citrix ADC a Citrix ADM agente
22	TCP	Para la comunicación SSH desde Citrix ADM a la instancia de Citrix ADC. Además, este puerto es necesario para la comunicación SSH entre el agente ADM y Citrix ADC.	Agente de Citrix ADM a Citrix ADC
Sin puerto reservado	ICMP	Para detectar la accesibilidad a la red entre el agente Citrix ADM y las instancias de Citrix ADC.	Agente de Citrix ADM a Citrix ADC
161	UDP	Para sondear eventos de instancias de ADC.	Agente de Citrix ADM a Citrix ADC

Puertos para el agente integrado de Citrix ADC

En esta tabla se explican los puertos necesarios que deben ser para el agente integrado de Citrix ADC.

Puerto	Tipo	Detalles	Dirección de comunicación
443	TCP	Para la comunicación NITRO desde Citrix ADM a la instancia de Citrix ADC.	De Citrix ADM al agente integrado de Citrix ADC y del agente integrado de Citrix ADC a Citrix ADM

Puertos para servicios

En esta tabla se explican los puertos necesarios que deben estar abiertos para que se ejecuten los servicios:

Puerto	Tipo	Detalles	Dirección de comunicación
5563	TCP	Este puerto es necesario para que se ejecute el servicio Citrix ADM Collector. Para recibir métricas de ADC (contadores) de la instancia de Citrix ADC a Citrix ADM.	Citrix ADC a Citrix ADM

Puertos para servidores externos

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

Puerto	Tipo	Detalles	Dirección de comunicación
25	TCP	Para enviar notificaciones SMTP desde el servicio Citrix ADM a los usuarios.	Agente Citrix ADM para los usuarios.
389/636	TCP	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre el servicio Citrix ADM y el servidor de autenticación externo LDAP.	Agente Citrix ADM al servidor de autenticación externo LDAP

Puerto	Tipo	Detalles	Dirección de comunicación
5563	TCP	Para recibir métricas ADC (contadores), eventos del sistema y mensajes de registro de auditoría desde la instancia Citrix ADC a Citrix ADM.	Citrix ADC a Citrix ADM
123	UDP	Puerto de servidor NTP predeterminado para, sincronización con varias fuentes de tiempo.	Agente Citrix ADM al servidor NTP
1812	RADIUS	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre el servicio Citrix ADM y el servidor de autenticación externo RADIUS.	Agente Citrix ADM al servidor de autenticación externo RADIUS
49	TACACS	Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre el servicio Citrix ADM y el servidor de autenticación externo TACACS.	Agente Citrix ADM al servidor de autenticación externo TACACS

> **Nota**
>
> El punto final del servicio Citrix ADM es el mismo que la «URL del servicio» generada al intentar registrar el agente. El agente usa la URL del servicio para localizar el Citrix ADM.

Asegúrese de que se permita el acceso a las siguientes URL de puntos de conexión:

- Servicio de descarga:

```
https://download.citrixnetworkapi.net
<!--NeedCopy-->
```

- Servicio de confianza:

```
*.citrixnetworkapi.net
<!--NeedCopy-->
```

- URL de servicio:

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
<!--NeedCopy-->
```

- Servicio de copia de seguridad de ADC:

```
adm-prod-backup-.*.s3..*amazonaws.com
<!--NeedCopy-->
```

- Conectividad con Citrix Cloud:

```
citrix.cloud.com
accounts.cloud.com
<!--NeedCopy-->
```

Para la comunicación entre el agente Citrix ADM y Citrix Analytics Service, asegúrese de que se permita el acceso a las siguientes URL de punto de conexión:

Dispositivo de punto final	Región de Estados Unidos	Región de la UE	Región APS
Centro de eventos	https://cas-eh-ns-alias.servicebus.windows.net	https://cas-eh-ns-eu-alias.servicebus.windows.net	https://cas-eh-ns-aps-alias.servicebus.windows.net
	https://cas-eh-ns2-alias.servicebus.windows.net	https://cas-eh-ns2-eu-alias.servicebus.windows.net	https://cas-eh-ns2-aps-alias.servicebus.windows.net

Dispositivo de punto final	Región de Estados Unidos	Región de la UE	Región APS
	`https://cas-eh-ns3-alias.servicebus.windows.net`		
	`https://cas-eh-ns4-alias.servicebus.windows.net`		

FQDN obsoletos

Algunos FQDN están en desuso para el siguiente uso del Citrix ADM. Para ayudarle a cambiar a los nuevos FQDN sin ninguna interrupción, los FQDN obsoletos continúan funcionando durante algún tiempo y se eliminarán lentamente.

Terminales Citrix ADM	FQDN antiguo	Nuevo FQDN
Acceso a Citrix ADM UI	`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 tus datos.
Interacciones de API	`netscalermas.cloud.com`	`api.adm.cloud.com`

Se requieren versiones mínimas de Citrix ADC

> Nota
>
> Las versiones 10.5, 11.0 y 12.0 de Citrix ADC ya han alcanzado el fin de vida (EOL). Para obtener más información, consulte la matriz de productos. La versión ADC recomendada es 12.1.

Función Citrix ADM	Versión del software Citrix ADC
StyleBooks	10.5 y versiones posteriores

Función Citrix ADM	Versión del software Citrix ADC
Supervisión, generación de informes y configuración mediante trabajos	10.5 y versiones posteriores
Análisis	
HDX Insight	10.1 y versiones posteriores
Gateway Insight	11.0.65.31 y posteriores
Security Insight	11.0.65.31 y posteriores

Requisitos de la solución Citrix ADM Analytics

Se requieren versiones mínimas de Citrix Virtual Apps and Desktops

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

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

Citrix ADM puede generar informes para aplicaciones que se publican en 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 Citrix ADC 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

Citrix ADM admite los siguientes clientes ligeros para supervisar las instancias de Citrix ADC que se ejecutan en la versión 11.0 del software, compilación 65.31 y versiones posteriores:

- Clientes ligeros basados en Dell Wyse Windows
- Clientes ligeros basados en Dell Wyse Linux
- Clientes ligeros basados en Dell Wyse ThinOS
- Clientes ligeros basados en Ubuntu 10ZiG

Se requiere una licencia de instancia Citrix ADC para HDX Insight

Los datos recopilados por Citrix ADM para HDX Insight dependen de la versión y las licencias instaladas de las instancias de Citrix ADC que se supervisan. Los informes de HDX Insight solo se muestran para los dispositivos Citrix ADC Premium y Enterprise que se ejecutan en la versión 10.5 y posteriores del software.

Licencia y duración de Citrix ADC	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 Citrix ADM 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

November 16, 2022

Citrix ADM requiere una licencia Citrix ADM verificada para administrar y supervisar las instancias de Citrix ADC.

Los siguientes son los tipos de licencia compatibles con Citrix ADM for Service:

Tipo de licencia	Con derecho a
Servidor virtual	500 MB de almacenamiento por servidor virtual
Almacenamiento	5 GB por licencia
Licencia Express	La cuenta Citrix ADM Express es una cuenta predeterminada para administrar los recursos de Citrix ADM.

Con una cuenta Express, puede administrar recursos limitados de Citrix ADM. Para obtener más información, consulte Administrar los recursos de Citrix ADM mediante una cuenta Express.

Después de que la licencia adquirida haya expirado, tendrá 60 días de período de gracia. Durante el período de gracia, puede elegir los recursos de Citrix ADM que se pueden administrar mediante una cuenta Express.

Para obtener más información sobre cómo empezar a utilizar una cuenta Express, consulte Introducción y para administrar las suscripciones, consulte Administración de suscripciones.

> Nota:
>
> Las licencias ADM son licencias híbridas. Puede usar estas licencias para el servicio ADM o ADM local.

Agregar una licencia

> Nota:
>
> Solo puede agregar una licencia agrupada para las instancias de Citrix ADC.

Puede agregar una licencia agrupada para las instancias de Citrix ADC en Citrix ADM. Después de agregar la licencia, puede comprobar la información de la licencia en **Configuración > Configuración de licencias y análisis**.

Para agregar una licencia agrupada:

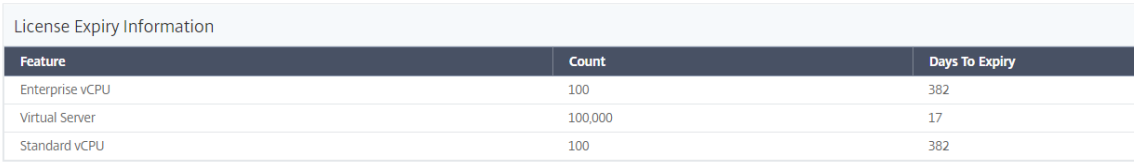
1. Vaya a**Infraestructura > Licencias agrupadas**.
2. Haga clic en **Examinar** para seleccionar el archivo de licencia de su equipo local.
3. Seleccione el archivo de licencia (.lic) y haga clic en **Aceptar**.

Comprobaciones de caducidad de las licencias

Ahora puede ver el estado de la caducidad de la licencia y configurar alertas al respecto en Citrix ADM.

Para ver el estado de las licencias:

1. Vaya a**Infraestructura > Licencias agrupadas**.
2. En la sección **Información de caducidad de licencia**, puede encontrar los detalles de las licencias que van a caducar:



License Expiry Information

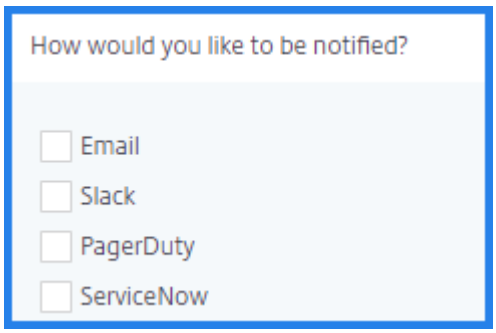
Feature	Count	Days To Expiry
Enterprise vCPU	100	382
Virtual Server	100,000	17
Standard vCPU	100	382

   - **Función**: Tipo de licencia que va a caducar.
   - **Recuento**: Número de instancias afectadas.
   - **Días hasta el vencimiento**: número de días restantes antes del vencimiento.

Para configurar los valores de notificación de las licencias:

1. Vaya a**Infraestructura > Licencias agrupadas**.
2. En la sección **Configuración de notificaciones**, haga clic en el icono del lápiz y modifique los parámetros.
   a) **¿Sobre qué le gustaría recibir notificaciones?** - Especifique el porcentaje de la capacidad.
   b) **¿Cómo le gustaría recibir una notificación?** - Selecciona las siguientes opciones de notificación:
      - **Correo electrónico** : especifique un servidor de correo y los detalles del perfil. Se activa un correo electrónico cuando las licencias están a punto de caducar.
      - **Slack** : especifica un perfil de Slack. Se envía una notificación cuando las licencias están a punto de caducar.
      - **PagerDuty** : especifique un perfil de PagerDuty. Según la configuración de notificación configurada en su portal de PagerDuty, se envía una notificación cuando las licencias están a punto de caducar.
      - **ServiceNow** : se envía una notificación al perfil predeterminado de ServiceNow cuando las licencias están a punto de caducar.

        > **Importante**
        >
        > Asegúrese de que Citrix Cloud ITSM Adapter esté configurado para ServiceNow e integrado con Citrix ADM. Para obtener más información, consulte Integrar Citrix ADM con la instancia de ServiceNow.



c) **Caducidad de licencias** : especifique los días antes de que caduque la licencia, cuando quiera que se le notifique.

Gestione los recursos con la cuenta Express

November 16, 2022

La cuenta Citrix ADM Express es una cuenta predeterminada para administrar los recursos de Citrix ADM. Esta cuenta está disponible fácilmente en Citrix Cloud.

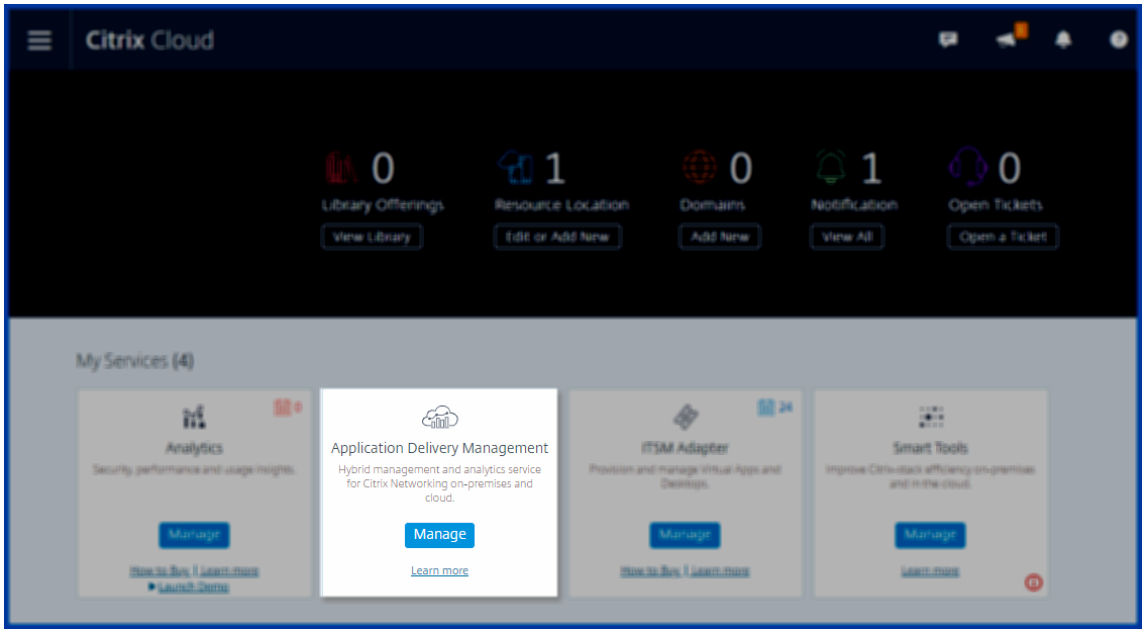
Con esta cuenta, puede administrar hasta dos servidores virtuales en Citrix ADM. Sin embargo, puede supervisar todos los servidores virtuales detectados en **Network Reporting** y **Network Functions**.

Para administrar los servidores virtuales específicos con una cuenta Express, debe seleccionar los servidores virtuales necesarios durante el período de gracia. De lo contrario, Citrix ADM selecciona automáticamente los servidores virtuales que puede administrar con la cuenta Express.

> **Importante**
>
> - Cuando su cuenta se convierte en una cuenta Express, Citrix ADM conserva los datos de almacenamiento de hasta 500 MB o datos de un día, lo que sea menor.
> - Si su cuenta de Citrix ADM Express permanece inactiva durante 90 días, se eliminará la cuenta. Citrix envía un recordatorio después de 60 días de inactividad.

Para administrar los recursos de Citrix ADM:

1. Inicie sesión en Citrix Cloud con sus credenciales.
2. Haga clic en **Administrar** en el archivo **Citrix ADM** .



Una vez finalizada la licencia de suscripción a Citrix ADM y el período de gracia, su cuenta se convertirá en una cuenta Express a menos que renueve la licencia. La cuenta Express le ayuda a continuar con su negocio con Citrix ADM. Para renovar su licencia, puede realizar una de las siguientes acciones:

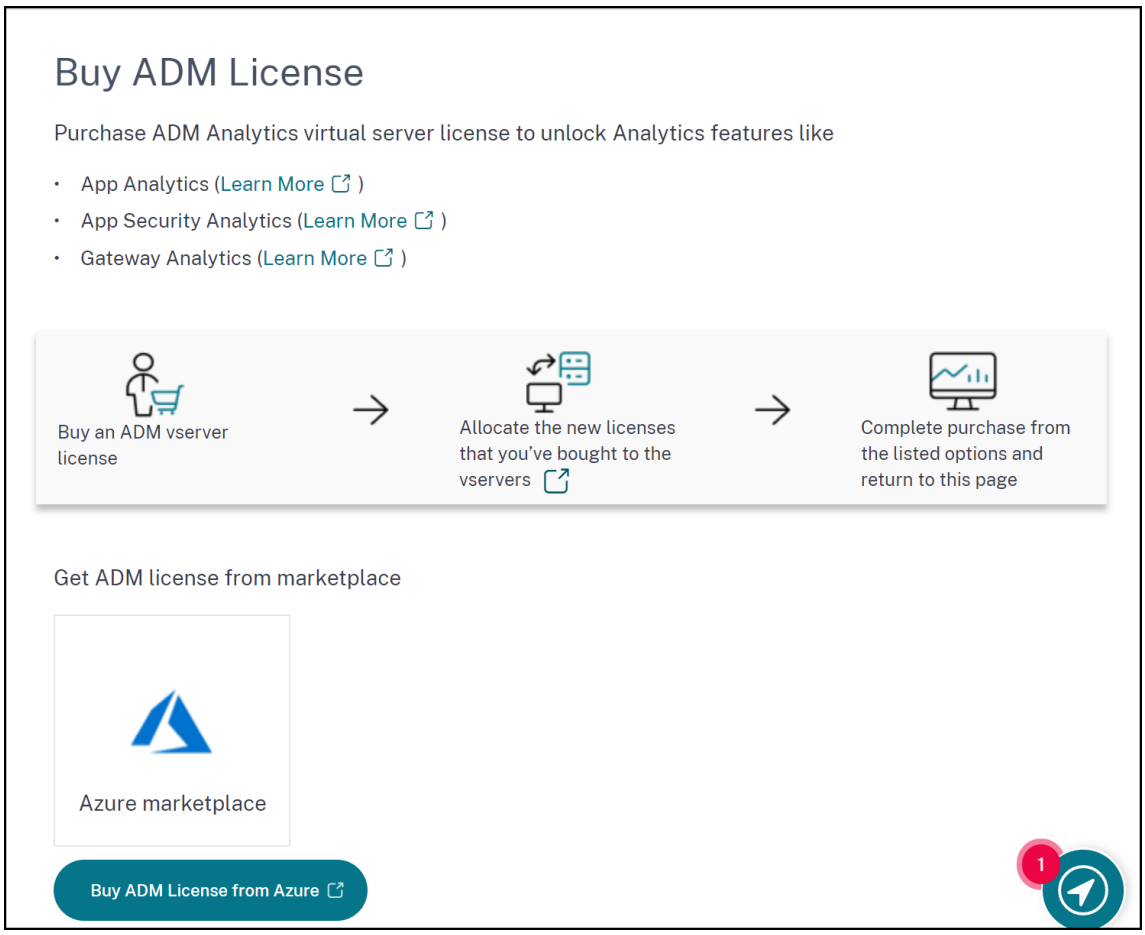
- Compre la licencia Citrix ADM desde la GUI.
- Visite Citrix Cloud.
- Póngase en contacto con el soporte técnico

Al renovar la licencia, las configuraciones se conservan de su cuenta Express. Además, recibirá servidores virtuales adicionales en función de su licencia. Para obtener más información, consulte Diferencias entre los derechos Express y Advance.

Comprar licencias ADM

Puede usar la GUI de ADM para comprar licencias de servidores virtuales de ADM desde la nube de Microsoft Azure. Seleccione **Comprar licencia ADM** en el menú de navegación. Como alternativa, puede ir a **Configuración > Licencias y análisis**.

1. Selecciona **Comprar licencia ADM**.
2. Seleccione **Microsoft Azure** para comprar licencias en Azure Marketplace.



La imagen de la licencia ADM se abre en Azure Marketplace.

3. Revise las opciones y seleccione la licencia de servidor virtual del servicio ADM adecuada.
4. Asigne las licencias a sus servidores virtuales en ADM.
5. Complete la compra en Azure Marketplace y vuelva a la GUI de ADM.

Actualice a una cuenta Citrix ADM Advance

November 16, 2022

Al iniciar sesión en Citrix ADM por primera vez, Citrix asigna una cuenta Express para administrar los recursos de ADM. Esta cuenta tiene opciones de ADM limitadas. Sin embargo, puede actualizar a la cuenta ADM Advance para obtener opciones ilimitadas. Estas opciones le ayudan a administrar, supervisar, analizar, organizar, automatizar y solucionar problemas de las instancias de ADC.

Compre una licencia Citrix ADM para convertir su cuenta express en la cuenta Citrix ADM Advance. Esta cuenta ofrece un límite de almacenamiento superior al de la cuenta express. También puede

usar SKU adicionales para aumentar el límite de almacenamiento. Para comprar una licencia, visite Citrix Cloud o póngase en contacto con el soporte técnico.

> Nota
>
> Después de actualizar a una cuenta avanzada, todas las configuraciones continúan como antes en el mismo inquilino.

Para obtener más información, consulte Diferencias entre los derechos Express y Advance.

Diferencias entre los derechos Express y Advance

November 16, 2022

En la siguiente tabla se explican las diferencias entre los derechos Express y Advance:

Funciones	Opciones	Derecho expreso	Derecho anticipado
Límite de almacenamiento	NA	500 MB o datos de un día, lo que sea menor.	De forma predeterminada, 500 MB de datos por licencia de servidor virtual. Por ejemplo, si tiene dos servidores virtuales, el límite de almacenamiento pasa a ser de 1 GB.
Aplicaciones	Panel de aplicaciones	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
	Información web	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
	Gráfico de servicio	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.

Funciones	Opciones	Derecho expreso	Derecho anticipado
	Configuración > StyleBooks	Sin límite	Sin límite
Seguridad	Panel de seguridad	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
	Infracciones de seguridad	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
	Puerta de enlace API	Sin límite	Sin límite
	Recomendaciones de la WAF	Sin límite	Sin límite
	Aprendizaje WAF	Sin límite	Sin límite
	Usuarios y puntos finales	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
Gateway	HDX Insight	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
	Gateway Insight	Hasta dos servidores virtuales.	Autorizado para todas las licencias de servidor virtual adquiridas.
Infraestructura	Análisis de infraestructura	Sin límite	Sin límite
	Instancias	Sin límite	Sin límite
	(Asesoramiento de instancias) Asesoramiento de actualización y asesoramiento de seguridad	Sin límite	Sin límite

Funciones	Opciones	Derecho expreso	Derecho anticipado
	Tablero SSL	Sin límite	Sin límite
	Eventos	Sin límite	Sin límite
	Funciones de red	Sin límite	Sin límite
	Informes de red	Sin límite	Sin límite
	Nube pública	Sin límite	Sin límite
	Licencias agrupadas	Sin límite	Sin límite
	Configuración > Trabajos de configuración, plantillas de configuración y consejos de configuración	Sin límite	Sin límite
	Trabajos de actualización	Sin límite	Sin límite
	Orchestration	Sin límite	Sin límite
	WAN Insight	Sin límite	Sin límite

Gestión de suscripciones

December 2, 2022

Citrix ADM requiere una licencia verificada para administrar y supervisar las instancias de Citrix ADC, las instancias de Citrix Gateway y los balanceadores de carga de terceros.

Puede administrar y supervisar cualquier número de instancias cuando utilice una cuenta Express o cuando se haya suscrito a una licencia válida. Sin embargo, puede administrar las aplicaciones detectadas en el panel de control de aplicaciones, ver los datos de análisis y supervisar las funciones de la red y los informes de red solo para la cantidad de servidores virtuales para los que ha adquirido licencias. Para obtener más información sobre los recursos de Citrix ADM que puede administrar con la cuenta Express, consulte Administrar recursos mediante la cuenta Express.

Con cada licencia instalada, recibirá una cantidad limitada de datos y capacidad para administrar ciertos servidores virtuales. Sin embargo, también puede comprar y aplicar licencias de solo datos para recargar su almacenamiento de datos.

Para obtener información e instrucciones sobre la compra y actualización de sus licencias de Citrix ADM, consulte Diferencias entre las autorizaciones Express y Advance y Citrix ADM.

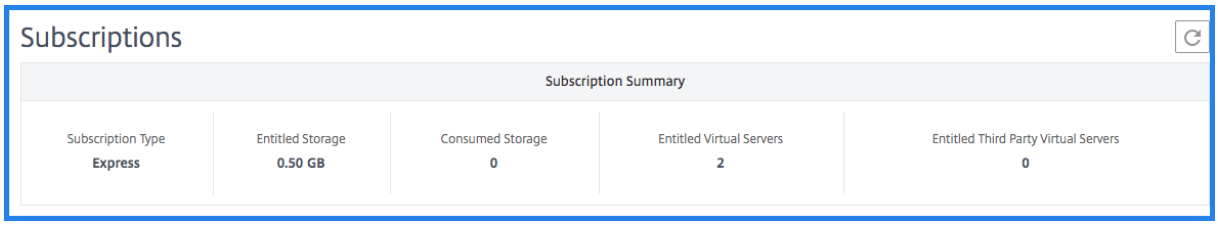
En la siguiente tabla se enumeran las licencias de Citrix necesarias para utilizar algunas de las funciones de Citrix ADM.

Grupo de funciones de Citrix ADM	Funciones de Citrix ADM	Requisito de licencia de Citrix ADC 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 Citrix 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	Pasarela de API	Licencia Premium (o) Avanzada
Aplicaciones	StyleBooks	N/D
Aplicaciones	Gestión de inventario: panel de infraestructura, grupos de instancias, paneles de instancias y sitios	N/D
Aplicaciones	Gestión 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

Grupo de funciones de Citrix ADM	Funciones de Citrix ADM	Requisito de licencia de Citrix ADC y Gateway
Aplicaciones	Funciones de red (visibilidad y administración sencillas de servidores virtuales, servicios, grupos de servicios, 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 (a nivel de servidor virtual)	N/D

Ver los detalles de la suscripción

Para ver las licencias instaladas en su Citrix ADM, vaya a **Cuenta** > **Suscripciones**. También puede ver el resumen de la licencia, como el tipo de licencia a la que se ha suscrito, la suscripción de datos autorizada y la suscripción de datos consumidos, así como los servidores virtuales permitidos y gestionados y los servidores virtuales de terceros en la sección **Resumen de la suscripción** .



Administrar servidores virtuales

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

Puntos a tener en cuenta:

- De forma predeterminada, Citrix ADM licencia automáticamente los servidores virtuales aleatoriamente después de cada ciclo de sondeo de servidores virtuales.

- Si el número total de servidores virtuales descubiertos en su Citrix ADM es inferior al número de licencias de servidor virtual instaladas, Citrix ADM, de forma predeterminada, otorga licencias a todos los servidores virtuales.

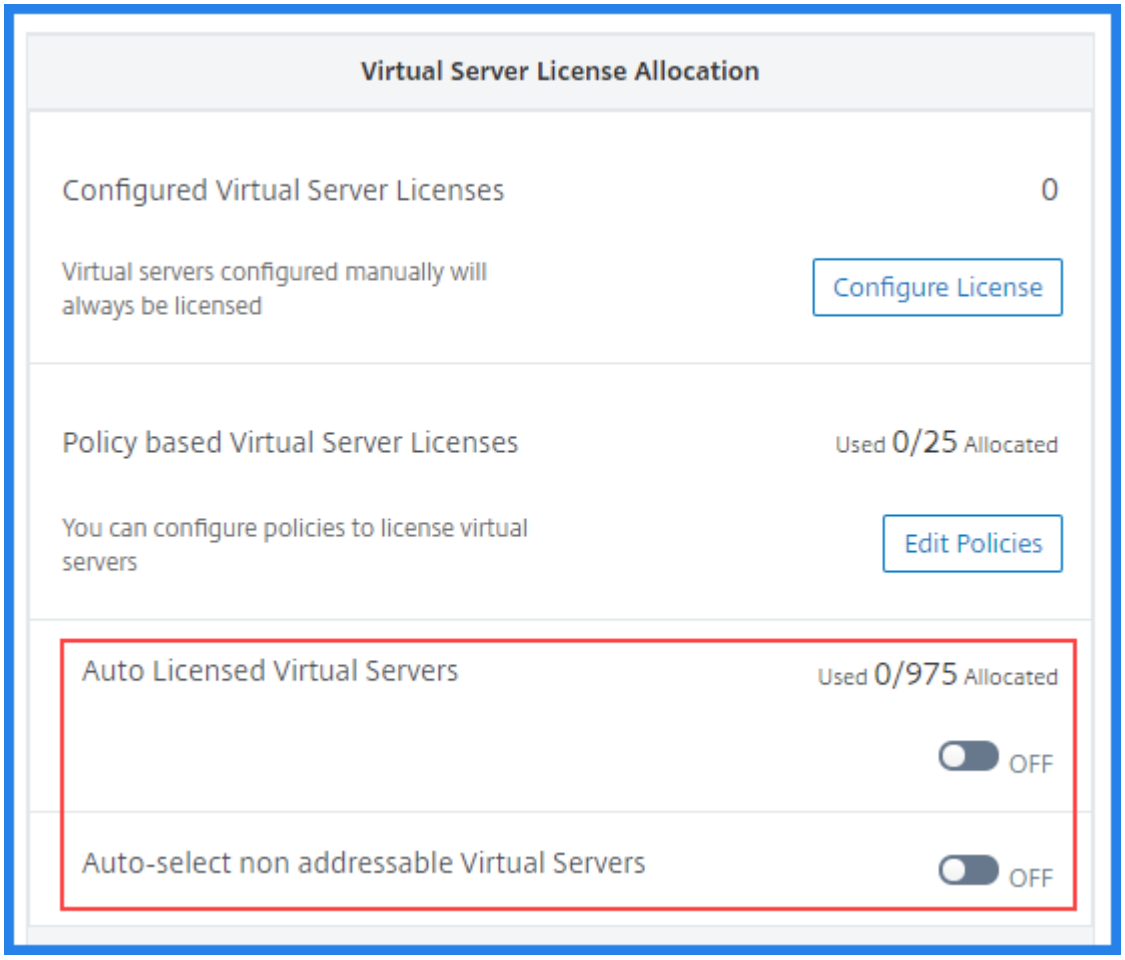
Para seleccionar manualmente los servidores virtuales o para restringir las licencias a los servidores virtuales limitados, primero debe inhabilitar la concesión automática de licencias de los servidores virtuales y, a continuación, seleccionar los servidores virtuales que quiere administrar.

Para deshabilitar los servidores virtuales de licencias automáticas:

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

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

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

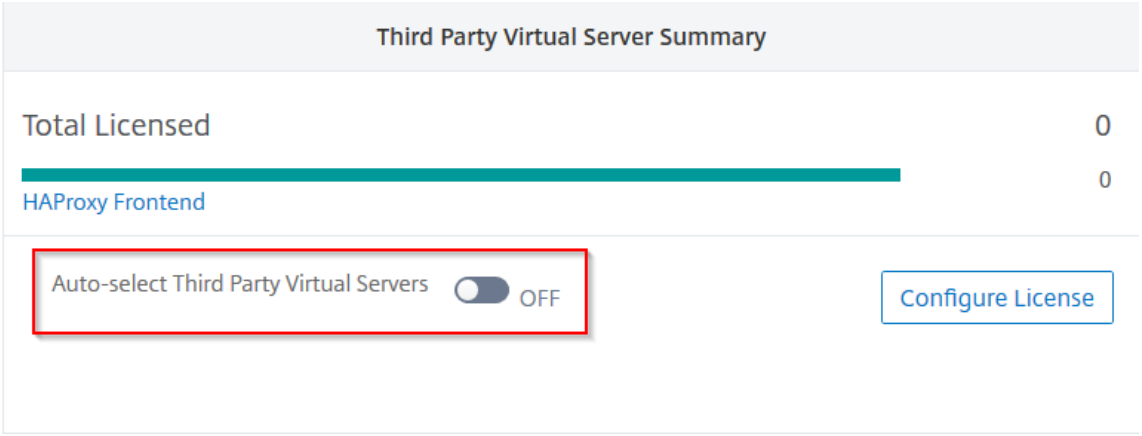


Para seleccionar servidores virtuales de terceros para la concesión de licencias:

1. Vaya a **Cuenta** > **Suscripciones**.

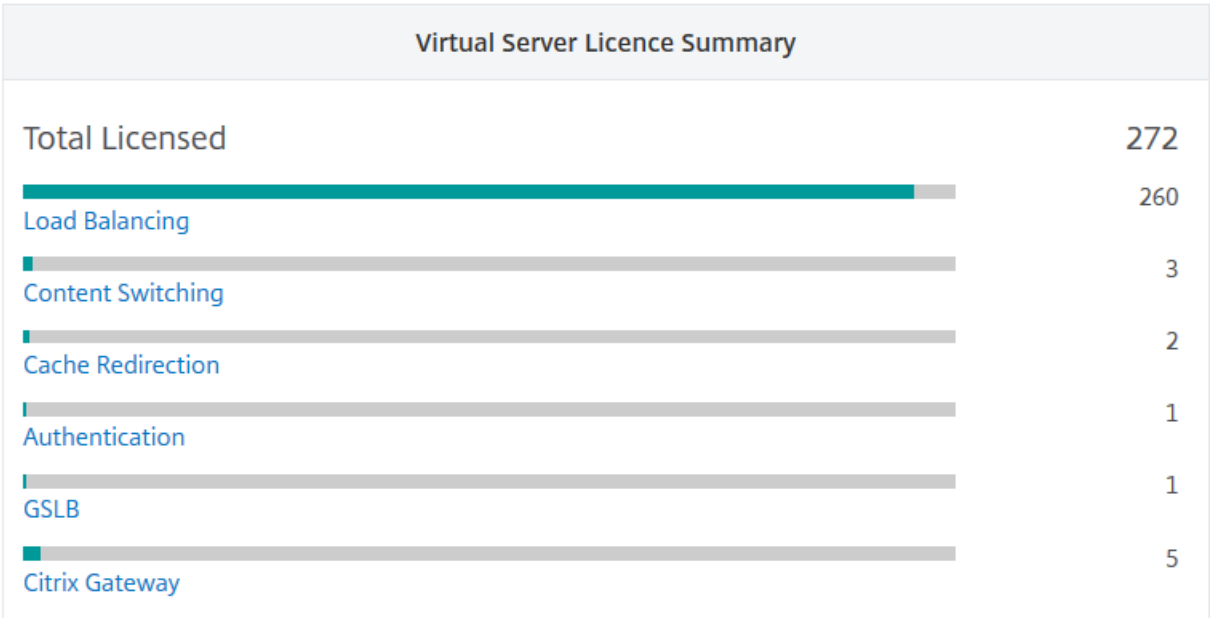
El panel muestra las licencias de servidor virtual disponibles, los servidores virtuales administrados junto con el tipo de servidor virtual e información sobre la caducidad de la licencia.

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



Ver los servidores virtuales con licencia

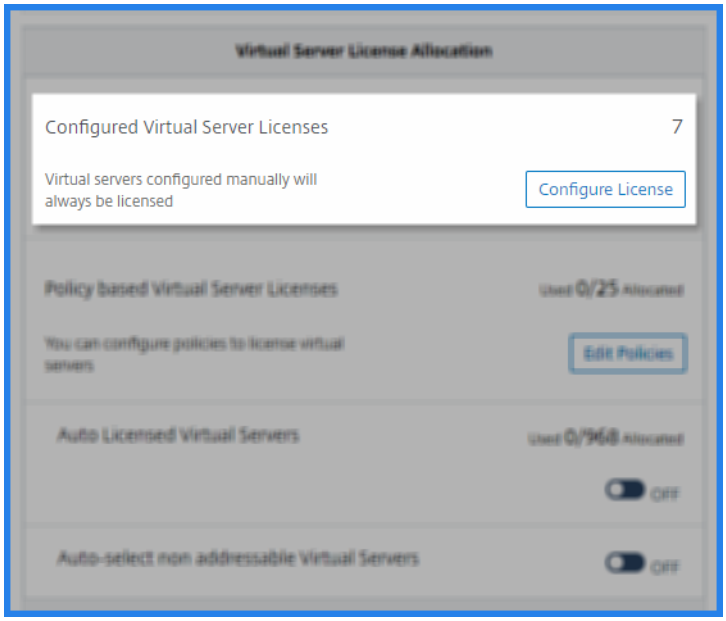
Después de aplicar las licencias a los servidores virtuales, puede ver los servidores virtuales con licencia o los servidores virtuales de terceros en la página **Suscripciones** . Para ver los servidores virtuales con licencia, vaya a **Configuración > Configuración de licencias y análisis de Citrix ADM** y haga clic en el tipo de servidor virtual en la sección **Total de licencias** del **Resumen de licencias de servidores virtuales**.



Aplicar licencias de servidor virtual manualmente

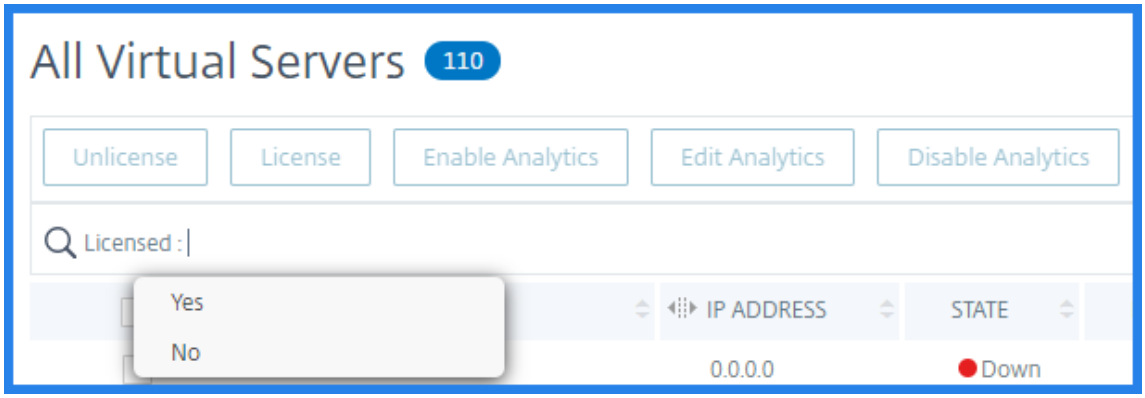
Puede aplicar licencias manualmente a un servidor virtual individual.

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



   Aparece la página **Todos los Servidores Virtuales**.

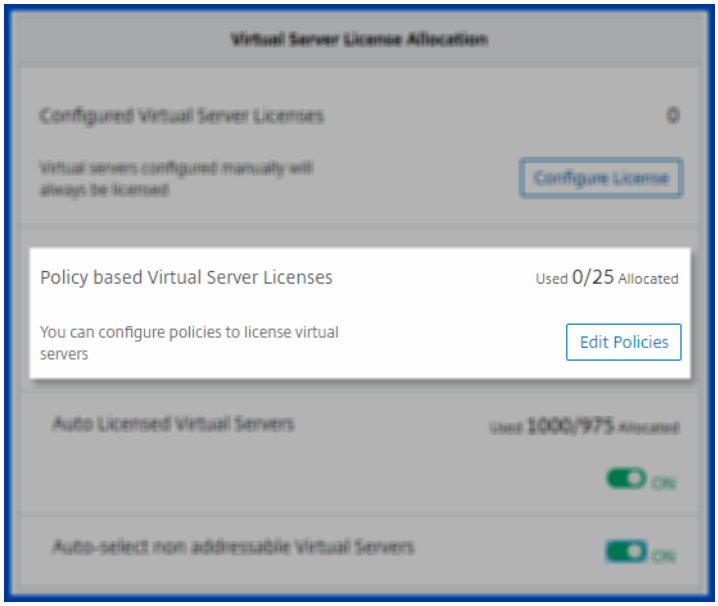
2. Filtrar servidores virtuales sin licencia mediante la propiedad:`Licensed: No`.



3. Seleccione el servidor virtual que quiere licenciar.
4. Haga clic en **Licencia**.

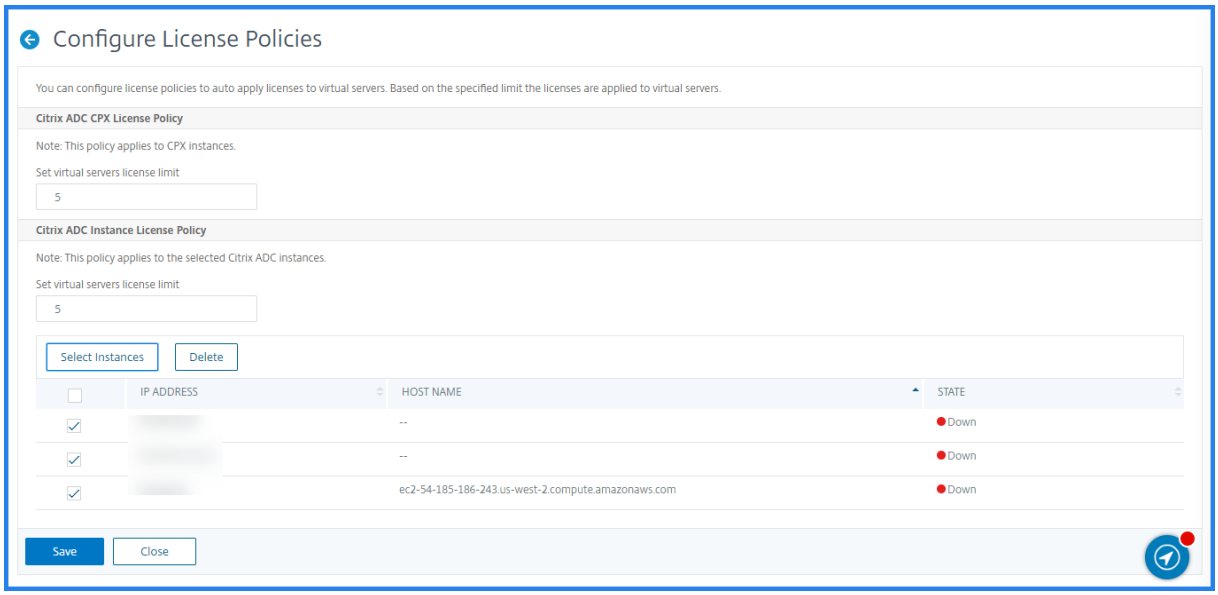
Configurar licencias de servidor virtual basadas en directivas

Puede configurar una directiva para aplicar la licencia a los servidores virtuales. Esta directiva controla el número de servidores virtuales que quiere conceder licencias automáticas. También aplica licencias solo a los servidores virtuales de las instancias seleccionadas.



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

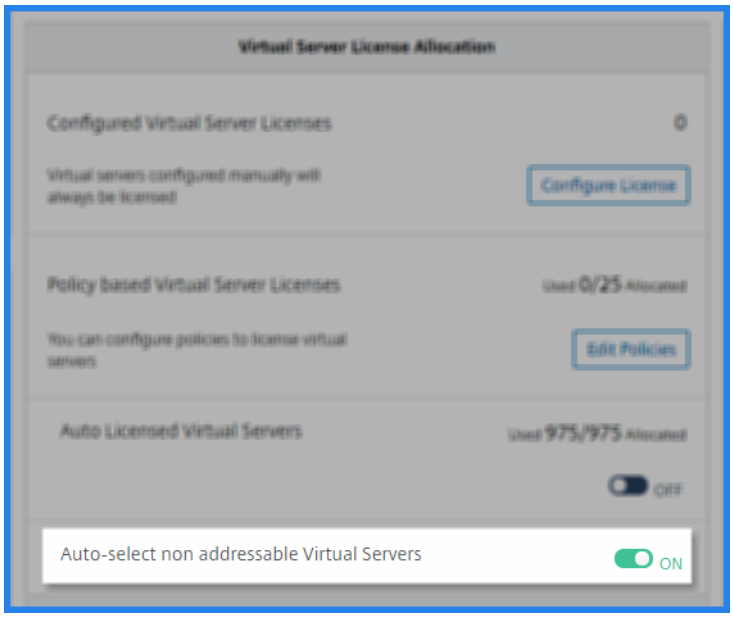
- Establezca el límite de servidores virtuales en instancias CPX por separado para aplicar licencias. El Citrix ADM aplica la licencia a los servidores virtuales en las instancias de CPX hasta un límite especificado.
- Establezca el límite de servidores virtuales en instancias ADC seleccionadas (MPX/VPX/BLX)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



Configurar la compatibilidad con licencias automáticas para servidores virtuales no direccionables

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

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



Nota

- De forma predeterminada, Citrix ADM sigue sin seleccionar automáticamente los servidores virtuales no direccionables para la concesión de licencias.
- Application Analytics (App Dashboard) es la única analítica admitida actualmente en servidores virtuales con licencia no direccionables.

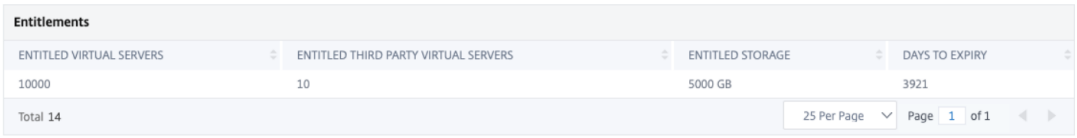
Ver comprobaciones de caducidad de suscripciones a servidores virtuales

Puede ver el estado de las licencias instaladas con la caducidad y el límite de almacenamiento permitido para las licencias en Citrix ADM.

Para ver el estado de las licencias:

1. Vaya a **Cuenta** > **Suscripciones**.

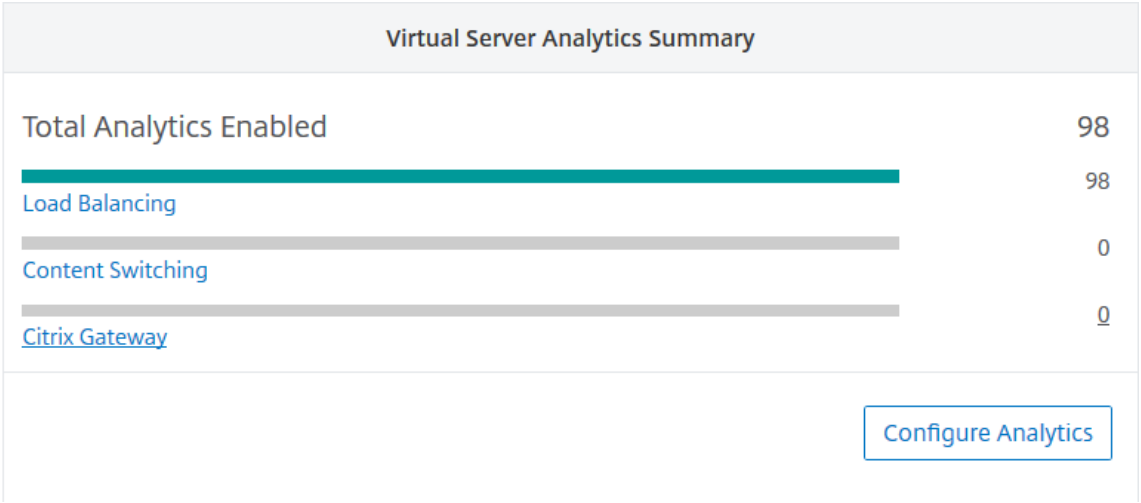
2. En la **sección Derechos**, puede ver los detalles de los servidores virtuales con licencia y los días de caducidad:
    - **Servidores virtuales autorizados:** número de servidores virtuales disponibles para licenciar.
    - **Servidores virtuales de terceros autorizados:** número de servidores virtuales 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.



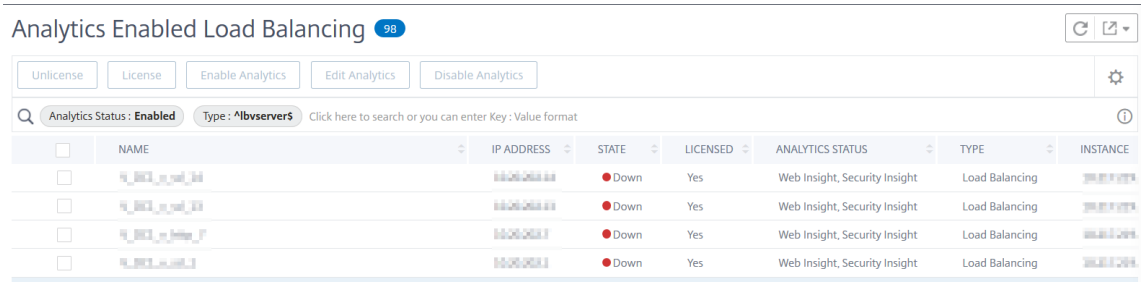
Ver el tipo de análisis habilitado en los servidores virtuales

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

November 16, 2022

Como administrador de red, puede administrar muchas instancias de ADC que se ejecutan en diferentes versiones de ADC en Citrix ADM. Supervisar el ciclo de vida de cada instancia de ADC puede ser una tarea engorrosa. Debe visitar la matriz de productos de Citrixe identificar las instancias de ADC que están llegando al final de su vida útil (EOL) o al final del mantenimiento (EOM). Luego, planea su actualización.

Para facilitar este proceso, el asesor de actualización de Citrix ADM le ayuda a supervisar el ciclo de vida de sus instancias de ADC de las siguientes maneras:

- Identifica las instancias que alcanzan o alcanzan la EOL o la MOE. Por lo tanto, puede planificar actualizaciones de ADC 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.
- Resalta las instancias que no están en las compilaciones ADC preferidas. Algunas organizaciones pueden tener un ADC preferido compilaciones para sus instancias. En Citrix ADM, puede configurar la compilación preferida para su organización en función de la estabilidad de la compilación, las características 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.

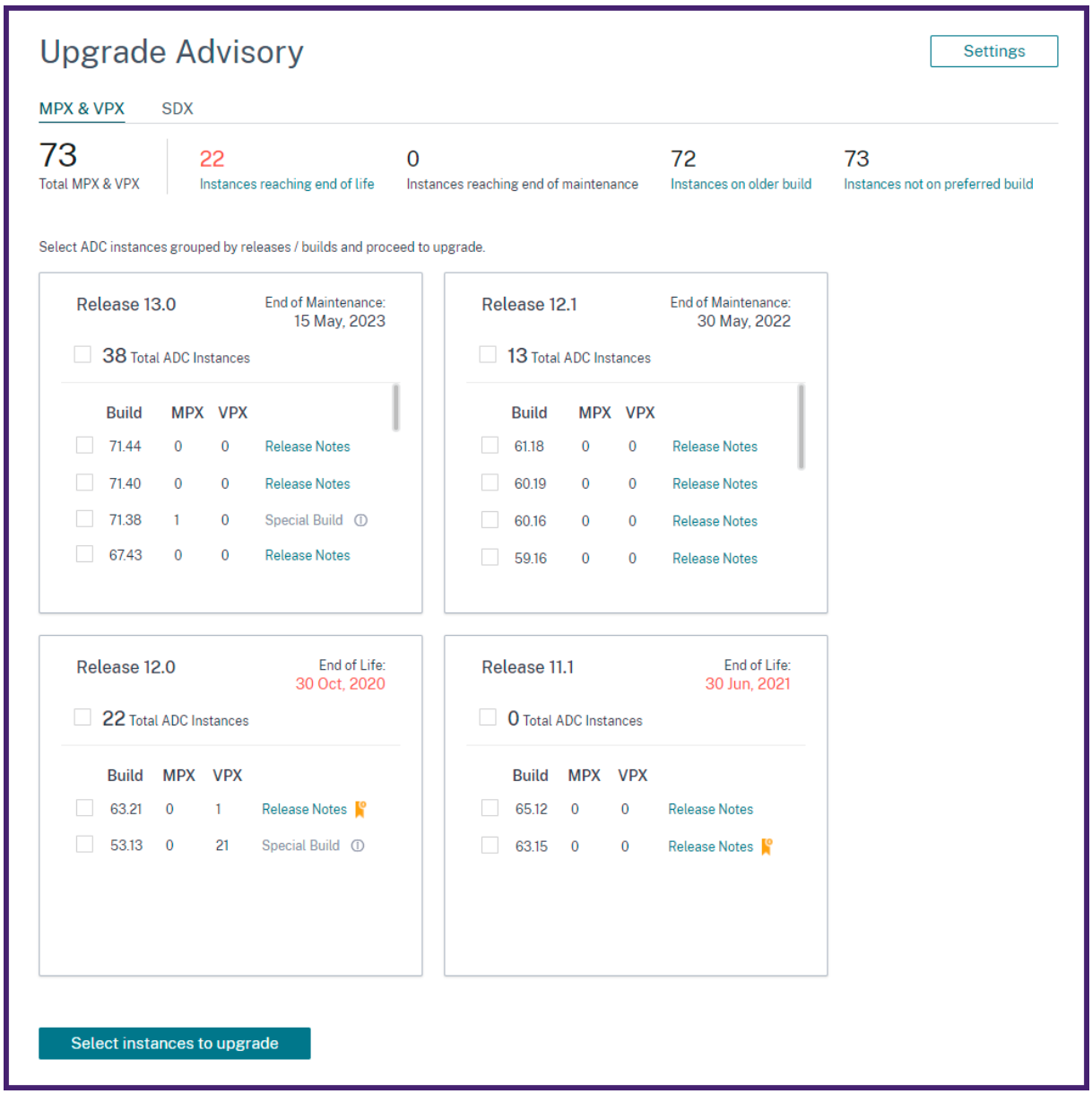
El aviso de actualización proporciona vínculos a las notas de la versión correspondientes. Con esta información, puede revisar y decidir una compilación de ADC para la actualización. Puede proceder a crear un trabajo de mantenimiento para actualizar instancias de ADC desde la página Asesor de Actualización.

> **Importante**
>
> Asesoramiento de actualización solo supervisa la EOL de las versiones de software ADC. No comprueba la EOL de los dispositivos ADC.

Consultar el aviso de actualización

Navegue por **Infraestructura > Asesoramiento de instancias > Asesoramiento de actualizaciones** y consulte la siguiente información:

- Recuento total de instancias de ADC.
- Instancias que llegan al final de la vida.
- Instancias que llegan al final del mantenimiento.
- Instancias en compilación anterior.
- Las instancias no están en la compilación preferida.
- Fechas de fin de vida útil y fin de mantenimiento para las diversas versiones de ADC.



La página **Asesor de Actualización** agrupa las instancias de ADC por sus versiones. El vínculo **Notas de la versión** le guía a las notas de la versión de ADC específicas. Revise las nuevas características, problemas solucionados y conocidos antes de decidir actualizar. Puede seleccionar varias instancias de ADC en diferentes versiones para actualizar a la vez. Cuando se continúa con una actualización, se crea un trabajo de actualización. Consulte Actualizar las instancias de ADC.

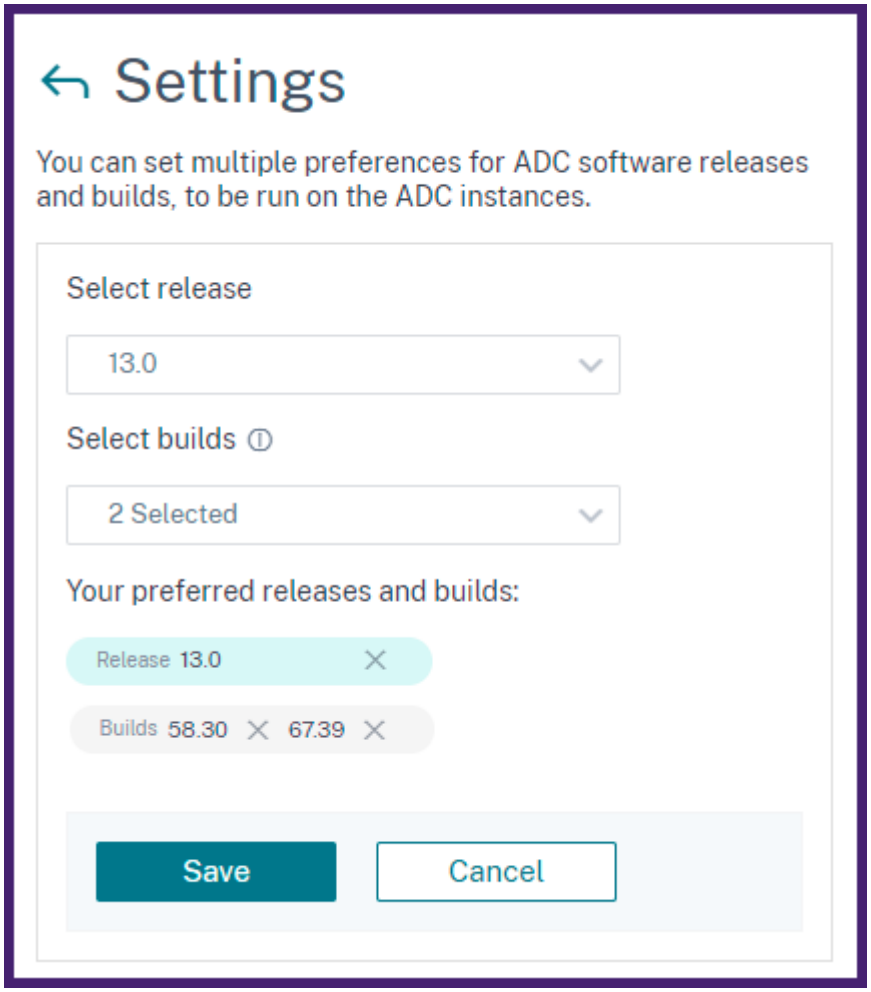
Establecer las compilaciones preferidas

Como administrador, puede definir una compilación de ADC preferida 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.



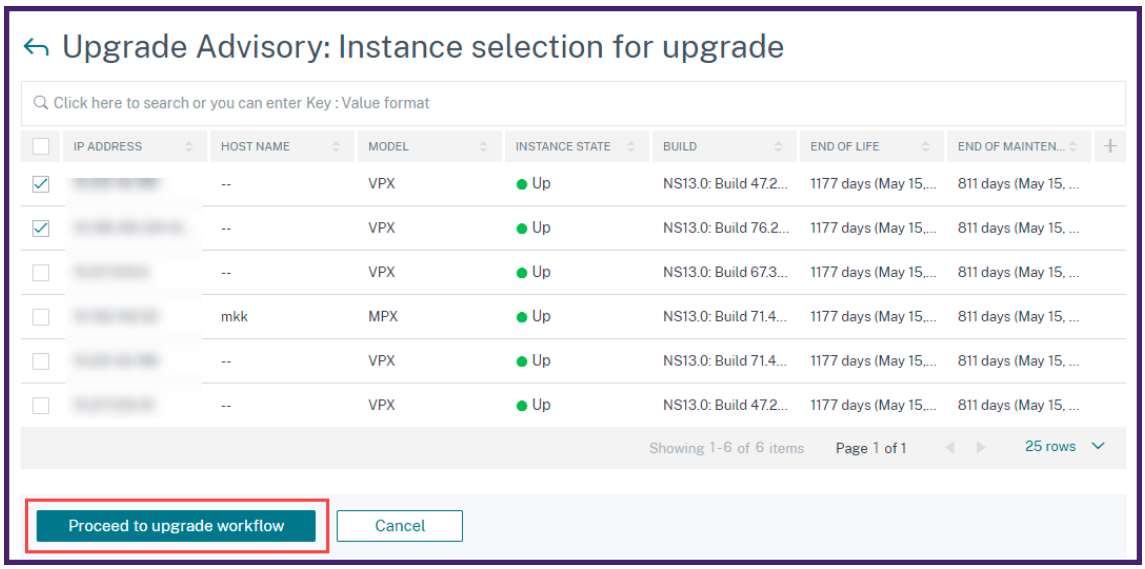
En este ejemplo, las compilaciones preferidas son `13.0-58.30` y `13.0-67.39`.

3. Haga clic en **Guardar**.

Actualizar instancias de ADC

En la página **Asesor de Actualización**, después de la revisión, realice los siguientes pasos para actualizar las instancias de ADC requeridas:

1. Seleccione las compilaciones de instancias que quiere actualizar y haga clic en **Seleccionar instancias para actualizar**.
2. Seleccione la instancia de ADC que quiere actualizar y haga clic en **Continuar para actualizar el flujo de trabajo**.

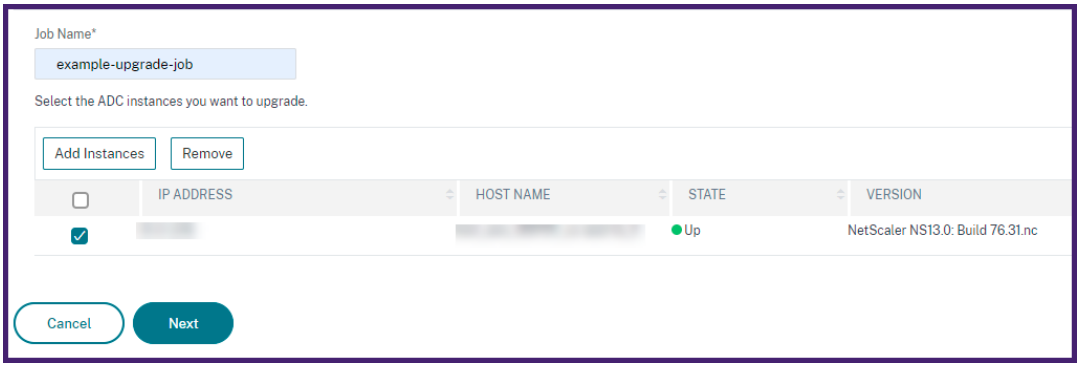


Este flujo de trabajo crea un trabajo de actualización.

3. En la ficha **Seleccionar instancia**,

   a) Especifique un nombre para el trabajo de actualización.

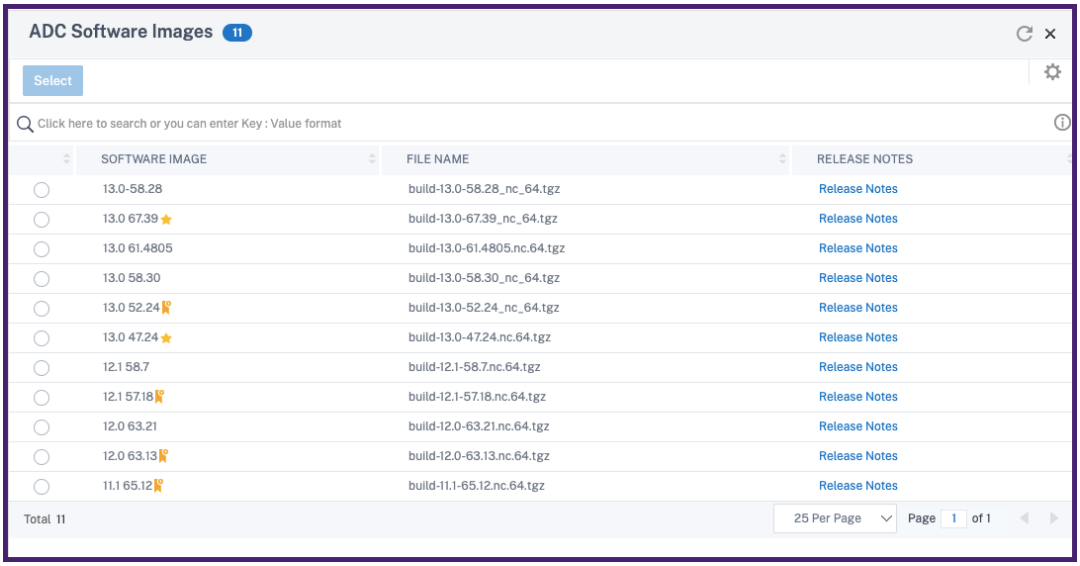
   b) (Opcional) si quiere agregar otras instancias, haga clic en **Agregar instancias**.



   c) Haga clic en **Siguiente**.

4. En la ficha **Seleccionar imagen**, seleccione una imagen ADC de la biblioteca de imágenes o local o del dispositivo.

   - **Seleccione de la biblioteca de imágenes**: seleccione una imagen ADC de la lista. Esta opción muestra todas las imágenes ADC que están disponibles en el sitio web de descargas de Citrix.

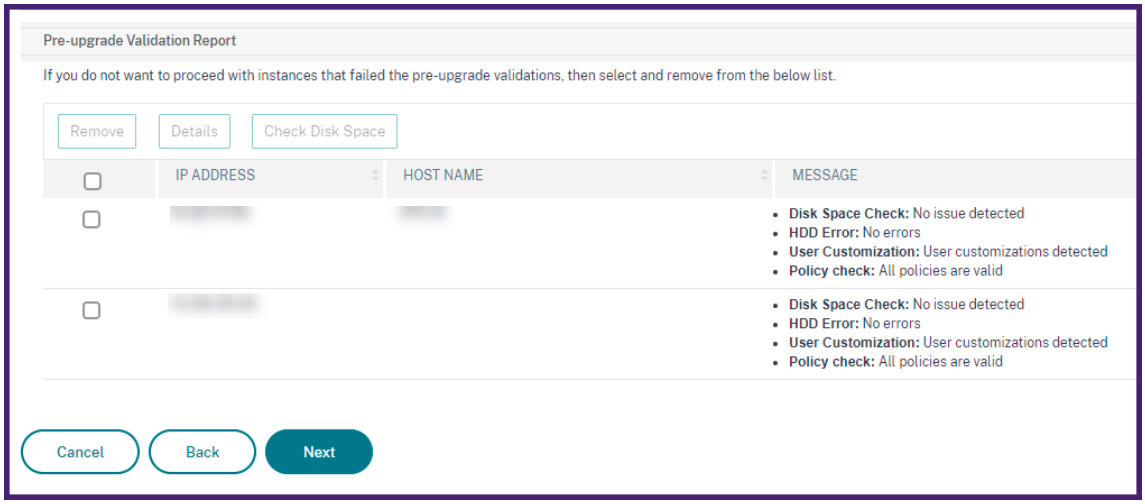


Las imágenes del software ADC muestran las compilaciones preferidas con el icono de estrella. Y, la mayoría de las compilaciones descargadas con el icono de marcador.

- **Seleccione entre local o dispositivo**: puede cargar la imagen desde su ordenador local o desde el dispositivo ADC. Al seleccionar el dispositivo ADC, la GUI de Citrix ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`. Seleccione la imagen de la GUI de Citrix ADM.
- **Omitir la carga de imágenes a ADC si la imagen seleccionada ya está disponible** : esta opción comprueba si la imagen seleccionada está disponible en ADC. El trabajo de actualización omite la carga de una imagen nueva y utiliza la imagen disponible en ADC.
- **Limpiar la imagen de software de Citrix ADC tras la actualización correcta** : esta opción borra la imagen cargada en la instancia de ADC después de la actualización de la instancia.

Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

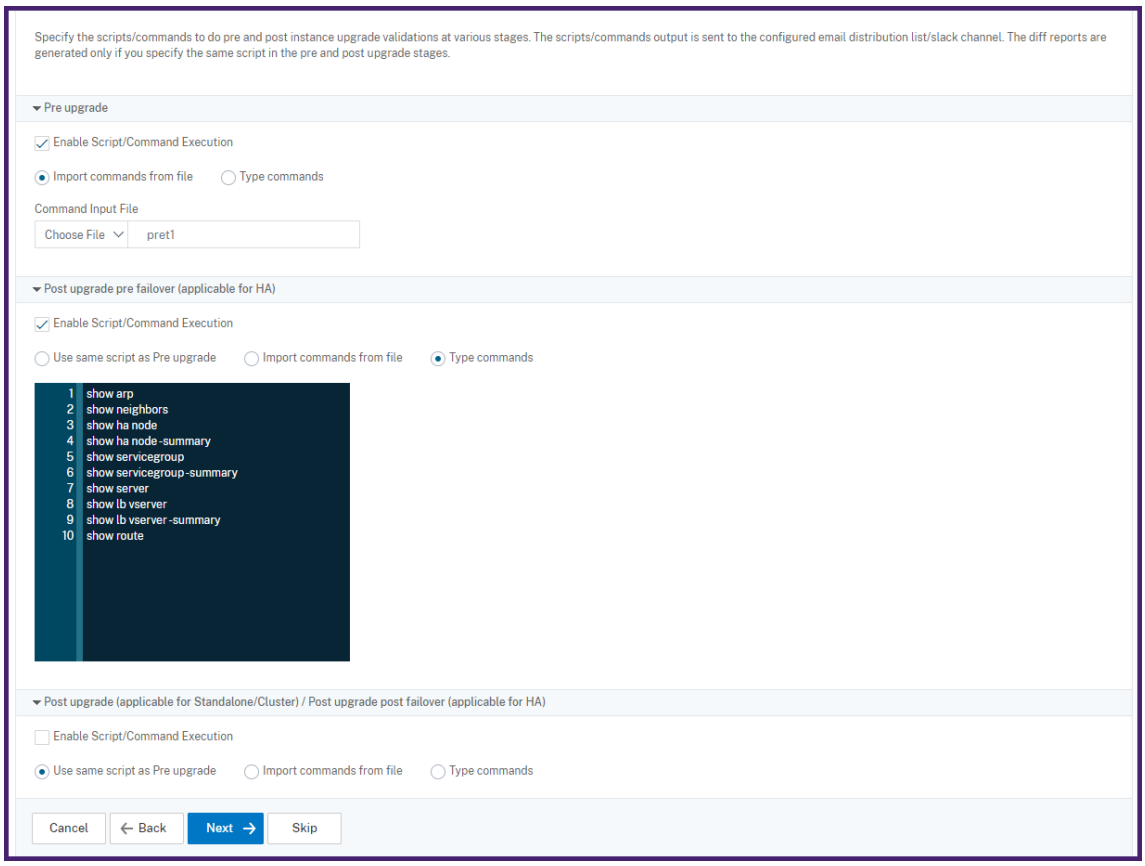
5. La ficha **Validación previa a la actualización** muestra las instancias fallidas. Puede quitar las instancias fallidas y hacer clic en **Siguiente**.



- **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 ADC.
- **Verificación de directivas**: si Citrix ADM encuentra directivas clásicas no compatibles, puede eliminarlas para crear un trabajo de actualización.

> **Nota:**
>
> Si especifica la dirección IP del clúster, Citrix ADM 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.

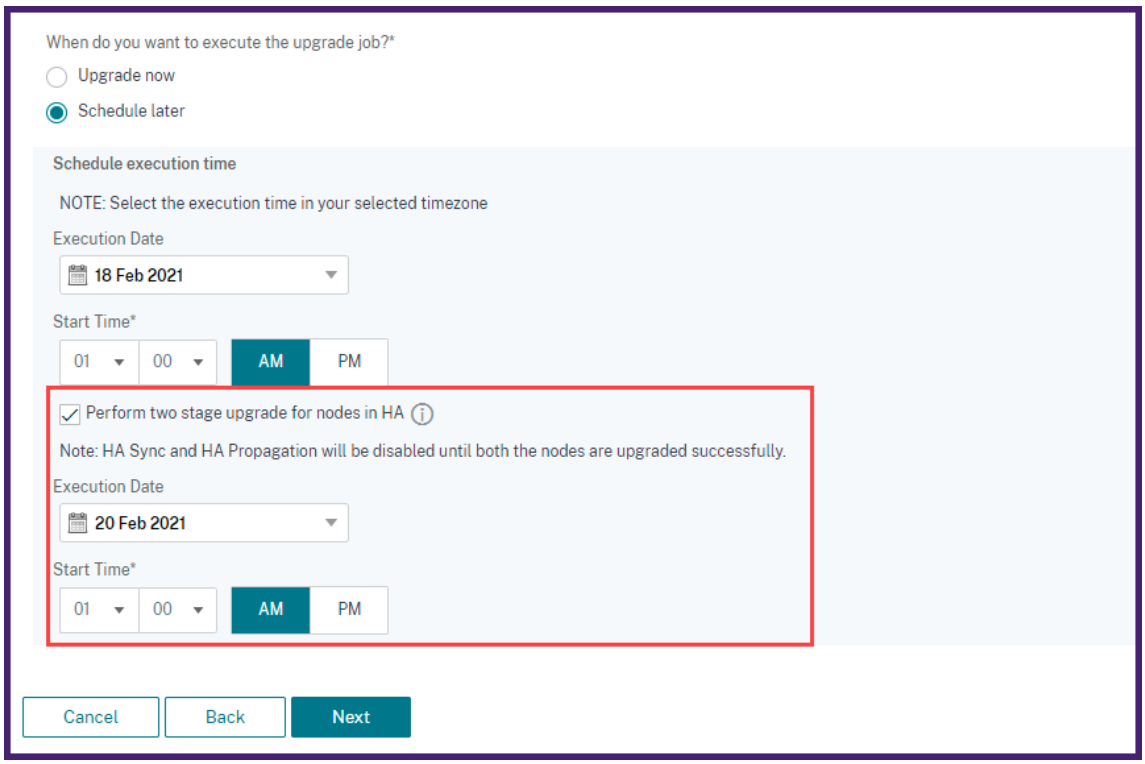


Para obtener más información, consulte Uso de scripts personalizados.

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 quiere actualizar un par de alta disponibilidad de ADC en dos etapas, seleccione Realizar actualización de dos etapas para nodos en HA.



Para obtener más información, consulte Actualizar el par de alta disponibilidad de ADC.

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 ADC.

Asesoramiento de seguridad

December 2, 2022

Una infraestructura segura, segura y resistente es la línea vital de cualquier organización. Por lo tanto, la organización debe hacer un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE) y evaluar el impacto de las CVE en su infraestructura. Comprenda la mitigación y la remediación. Además, la organización debe planificar la mitigación y la corrección para resolver las vulnerabilidades.

El asesor de seguridad de Citrix ADM destaca que Citrix CVes pone en riesgo sus instancias de ADC y recomienda mitigaciones y correcciones. Puede revisar las recomendaciones y tomar las medidas adecuadas mediante Citrix ADM para aplicar las mitigaciones y las soluciones.

Funciones de asesoramiento de seguridad

Las siguientes funciones de asesoramiento de seguridad le ayudan a proteger su infraestructura.

- Análisis: incluye análisis predeterminados del sistema y análisis bajo demanda.
  - Análisis del sistema: analiza todas las instancias administradas de forma predeterminada una vez a la semana. Citrix ADM decide la fecha y la hora de los escaneos del sistema y no puede cambiarlos.
  - Análisis bajo demanda: permite 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 escanear después de aplicar una corrección o mitigación, para evaluar la postura revisada.
- Análisis de impacto de CVE: muestra los resultados de todos los CVE que afectan a su infraestructura y todas las instancias de ADC que se ven afectadas, y sugiere soluciones y mitigación. Utilice esta información para aplicar mitigación y corrección 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.
- Repositorio de CVE: ofrece una vista detallada de todos los CVE relacionados con ADC que Citrix ha anunciado desde diciembre de 2019 y que podrían afectar a su infraestructura de ADC. Puede utilizar esta vista para comprender los CVE en el ámbito del asesoramiento de seguridad y para obtener más información sobre los CVE. Para obtener información sobre los CVE no compatibles, consulte los CVE no compatibles en el Aviso de seguridad.

Puntos que tener en cuenta

Tenga en cuenta los siguientes puntos al utilizar el asesoramiento de seguridad:

- Instancias compatibles con la detección de CVE: todas las ADC (SDX, MPX, VPX) y Gateway.
- CVE compatibles: todos los CVE posteriores a diciembre de 2019.

> **Nota**
>
> El aviso de seguridad de Citrix ADM no admite la detección y la corrección de las vulnerabilidades que afectan al complemento de Citrix 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 Citrix ADM no tiene en cuenta ningún tipo de configuración incorrecta de la función al identificar la vulnerabilidad.
- El aviso de seguridad de Citrix ADM solo permite identificar y corregir los CVE. No permite la identificación y la solución de los problemas de seguridad que se destacan en el artículo sobre seguridad.
- Alcance de las versiones de ADC y Gateway: la función se limita a las versiones principales. El aviso de seguridad no incluye ninguna versión especial en su alcance.
  - El asesoramiento de seguridad se admite en instancias ADC que ejecutan versiones superiores a 10.5 y no en instancias con versiones 10.5 y versiones inferiores.
  - La partición de administración no admite el asesoramiento de seguridad.
- Tipos de escaneo:
  - **Análisis de versiones**: este análisis necesita Citrix ADM para comparar la versión de una instancia de ADC con las versiones y compilaciones en las que está disponible la corrección. Esta comparación de versiones ayuda a los consejos de seguridad de Citrix ADM a identificar si el ADC es vulnerable al CVE. Por ejemplo, si se corrige un CVE en las versiones de ADC y xx.yy, el aviso de seguridad considera que todas las instancias de ADC de las compilaciones inferiores a xx.yy son vulnerables. El análisis de versiones se admite actualmente en el asesoramiento de seguridad.
  - **Análisis de configuración**: este escaneo necesita que Citrix ADM coincida con un patrón específico del escaneo CVE con el archivo de configuración ADC (nsconf). Si el patrón de configuración específico está presente en el archivo ns.conf de ADC, 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 Citrix ADM se conecte a la instancia de ADC administrada, le envíe un script y lo ejecute. El resultado del script ayuda a Citrix ADM a identificar si el ADC 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 realizar escaneos personalizados específicos en la documentación de asesoramiento de seguridad de ese CVE.
- Los análisis no afectan al tráfico de producción en ADC y no alteran ninguna configuración de ADC en ADC.

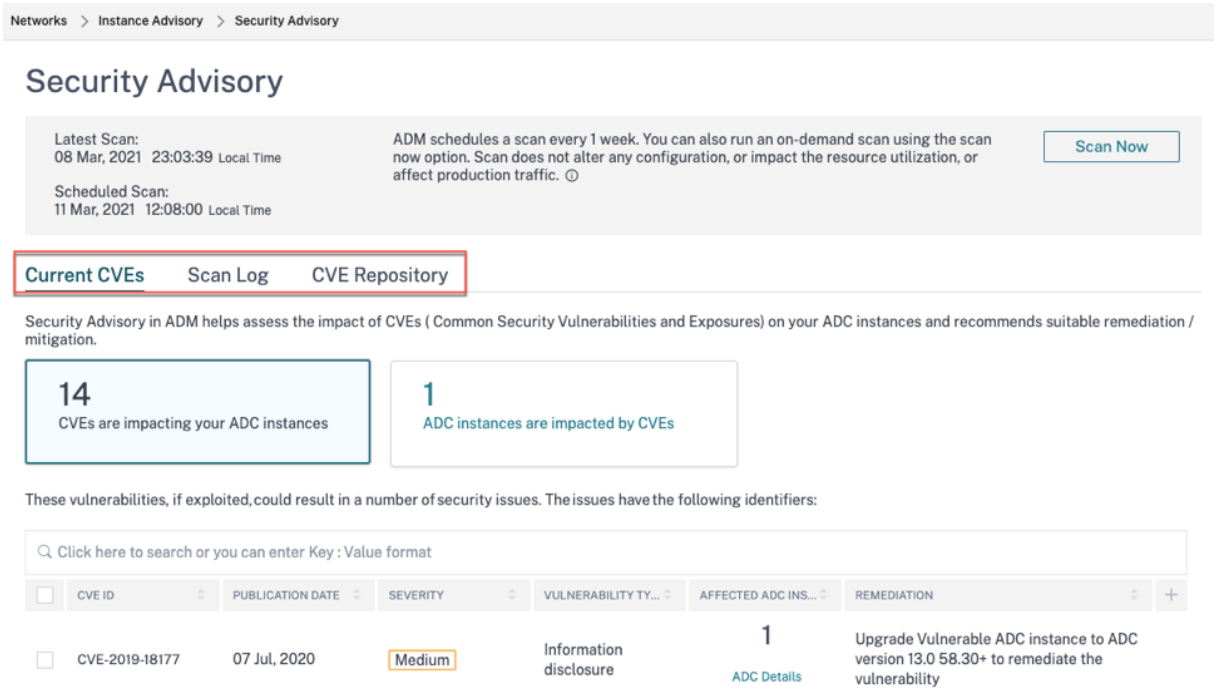
- El aviso de seguridad de ADM no admite la mitigación. Si ha aplicado la mitigación (solución temporal) a la instancia de ADC, ADM seguirá identificando el ADC como un ADC vulnerable hasta que haya completado la corrección.

Cómo utilizar el panel de asesoría de seguridad

Para acceder al panel **de asesoramiento de seguridad**, desde la GUI de Citrix ADM, vaya a **Infraestructura > Asesoramiento de instancias > Asesoramiento de seguridad**. El panel muestra el estado de vulnerabilidad de todas las instancias de ADC que administra a través de Citrix ADM. Las instancias se escanean una vez a la semana; sin embargo, puede escanearlas en cualquier momento haciendo clic en **Escanear ahora**.

El tablero incluye tres fichas:

- CVE actuales
- Registro de exploración
- Repositorio CVE



> **Importante**
>
> En la GUI o en el informe del **asesor de seguridad**, es posible que no aparezcan todas las CVE y es posible que solo vea un CVE. Como solución alternativa, haga clic en **Analizar ahora** para ejecutar un análisis bajo demanda. Una vez finalizado el análisis, todas las CVE del ámbito (aproximadamente 15) aparecen en la interfaz de usuario o informe.

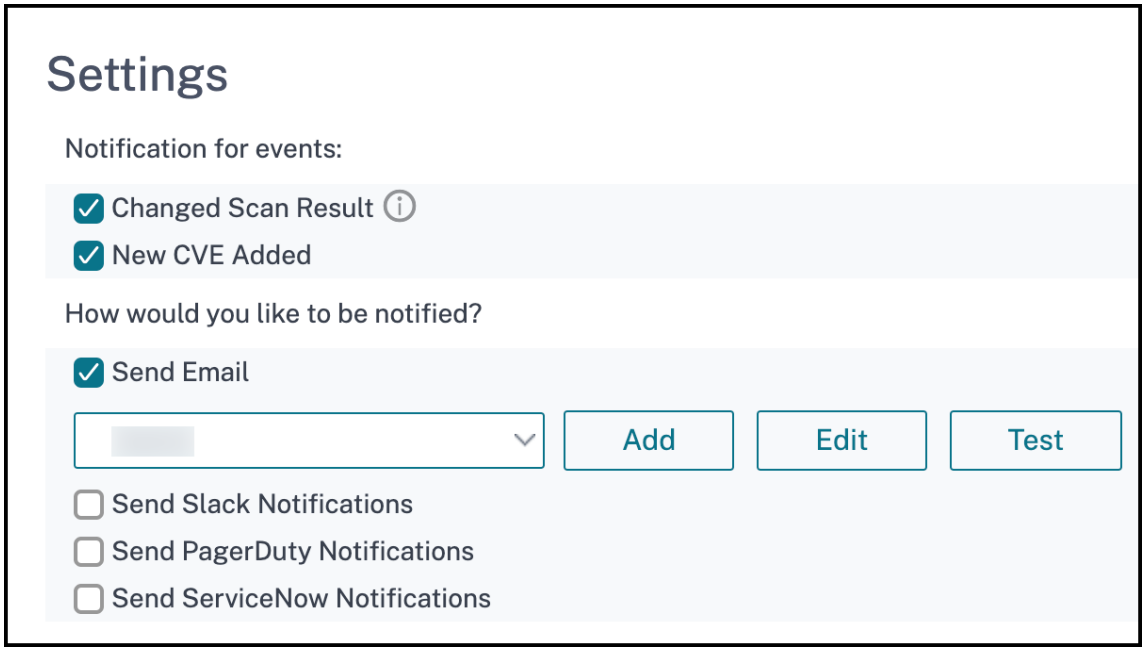
En la esquina superior derecha del panel de control se encuentra el icono de configuración, que le

permite:

- Activar y desactivar las notificaciones

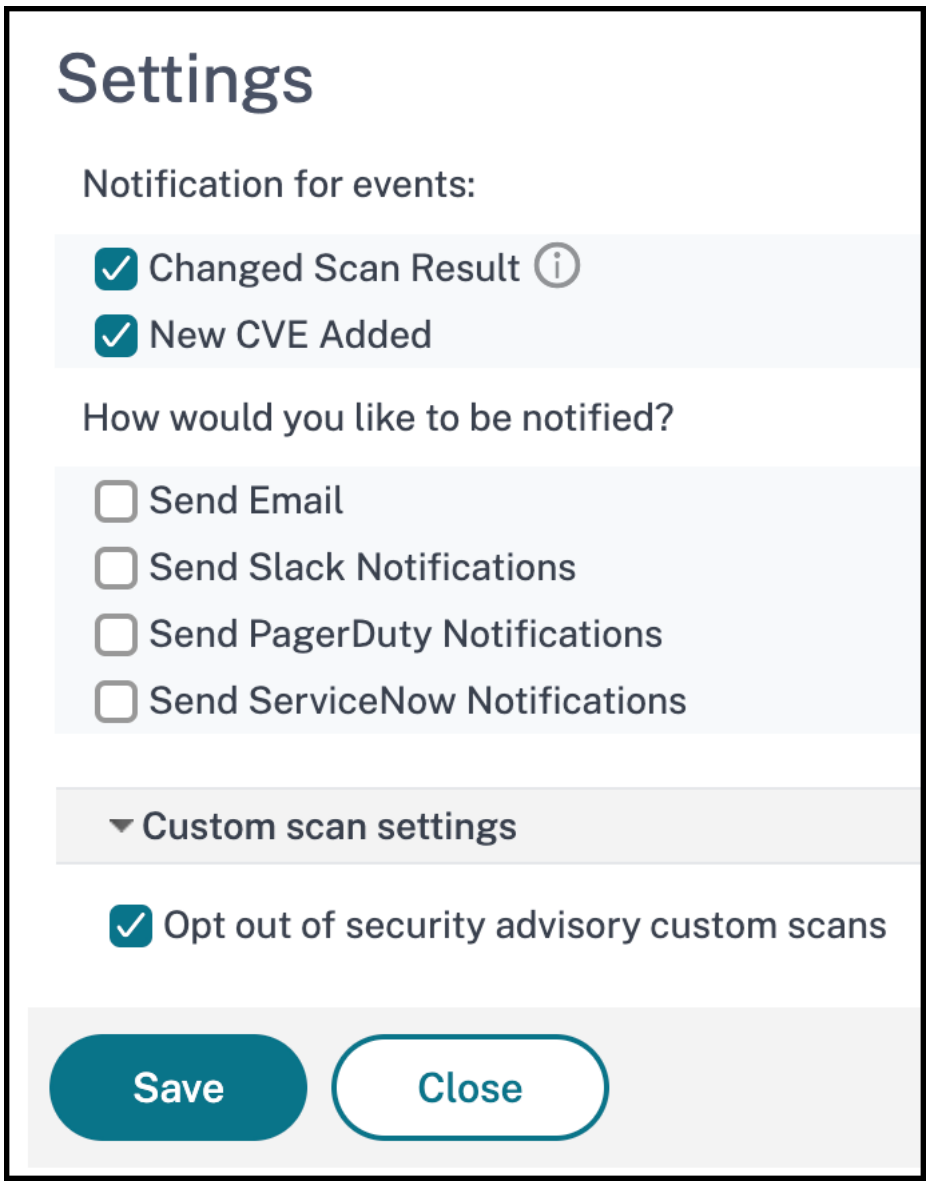
  Puede recibir las siguientes notificaciones sobre las actividades de asesoramiento de seguridad de Citrix ADM:

  - Notificaciones por correo electrónico, Slack, PagerDuty y ServiceNow sobre los cambios en los resultados del escaneo y los nuevos CVE que se agregan al repositorio de consejos de seguridad
  - Notificación en la nube para cambiar los resultados



- Configurar los ajustes de escaneo personalizados

  Puede hacer clic en el menú desplegable **Configuración de escaneo 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 asesoramiento de seguridad. El impacto de los CVE que requieren un análisis personalizado no se evaluará para sus instancias de ADC 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 tu caso de uso.

La tabla que muestra el número de CVE que afectan a las instancias de ADC tiene 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 pun-

tuación, pase el cursor sobre el tipo de gravedad.

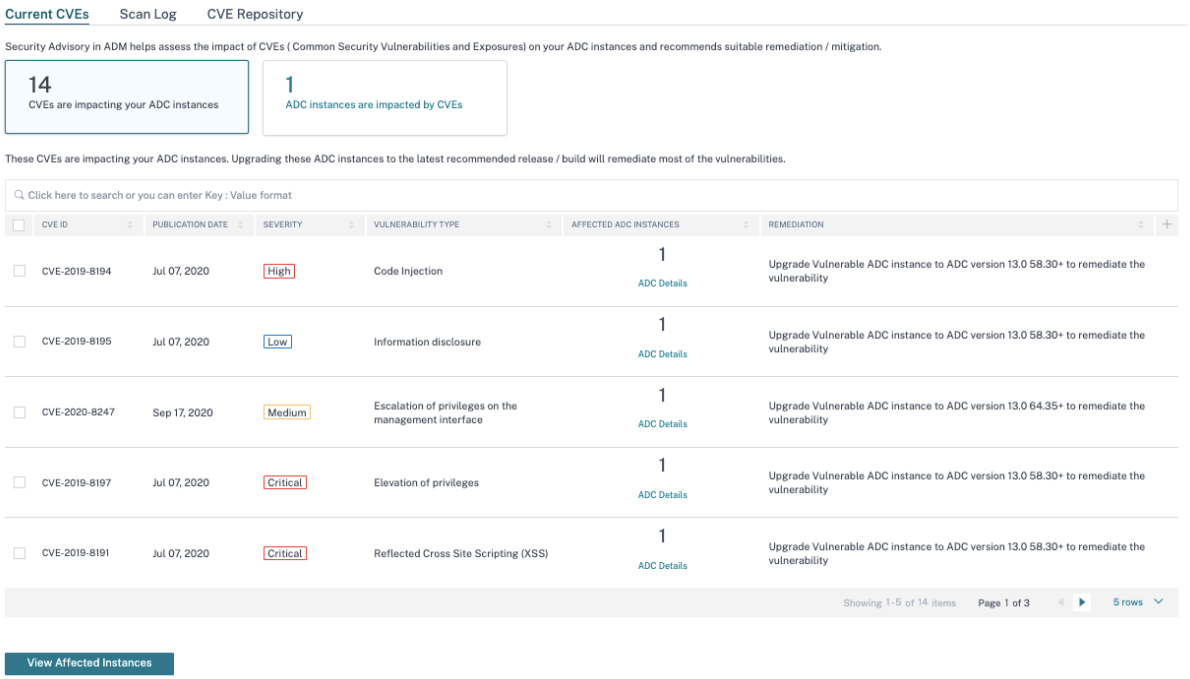
Tipo de vulnerabilidad: el tipo de vulnerabilidad de este CVE.

Instancias de**ADC afectadas: el recuento de instancias**a las que afecta el ID de CVE. Al pasar el cursor sobre, aparece la lista de instancias de ADC.

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, pase el cursor sobre Detalles de ADC en **Instancias ADC afectadas**. Para comprobar los detalles de la instancia afectada, haga clic en **Ver instancias afectadas** en la parte inferior de la tabla.
También puede agregar o quitar columnas de la tabla haciendo clic en el signo más.

En esta pantalla, el número de CVE que afectan a tus instancias es de 14 CVE y las instancias que se ven afectadas por estos CVE son una.

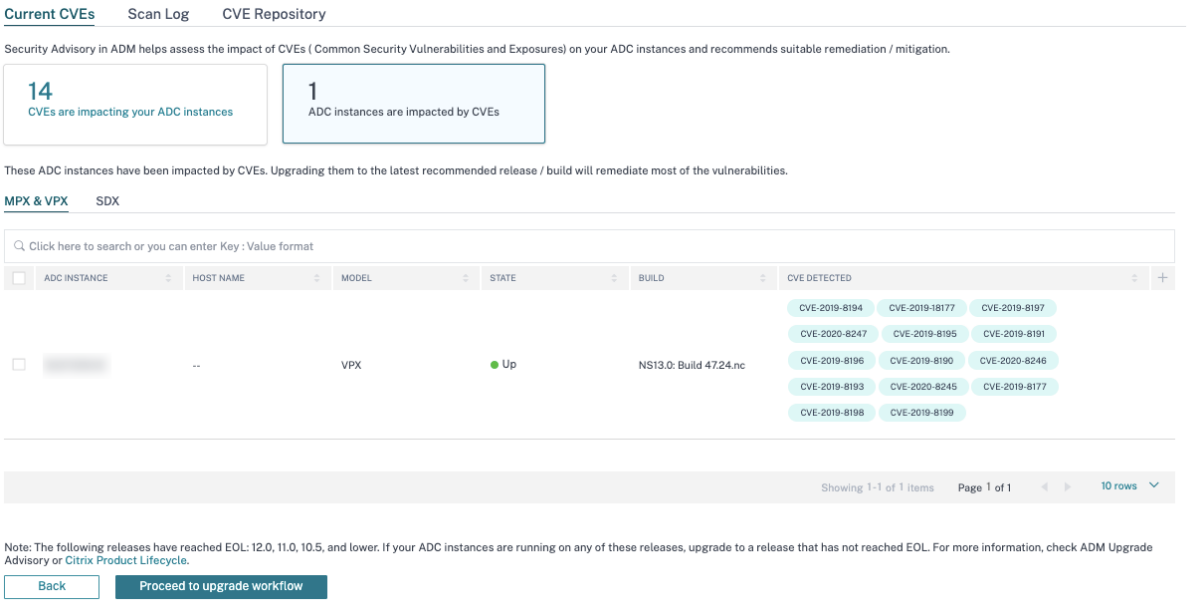


La **<number of> instancias de ADC se ven afectadas por la ficha CVE** que muestra todas las instancias ADC de Citrix ADM afectadas. La tabla muestra los siguientes detalles:

- Dirección IP ADC
- Nombre de host
- Número de modelo ADC
- Estado de la ADC
- Versión y compilación del software

- Lista de CVE que afectan al ADC.

En la siguiente captura de pantalla, se ve afectada una instancia de ADC. Agregue o elimine cualquiera de estas columnas de acuerdo a su necesidad, haciendo clic en el signo +.



Para corregir el problema de vulnerabilidad, seleccione la instancia ADC 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

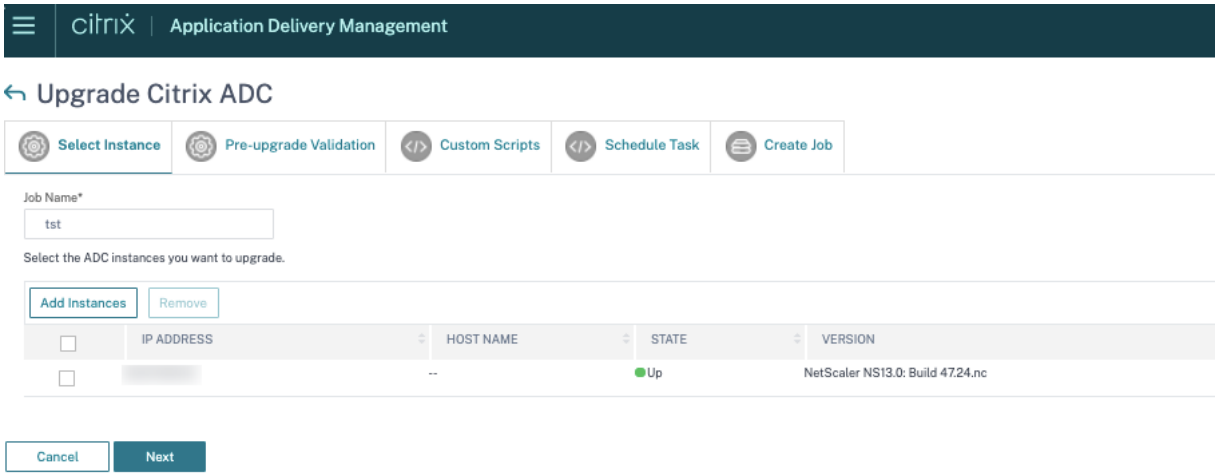
> **Nota**
>
> Si las instancias de ADC tienen personalizaciones, consulte Consideraciones de actualización para las configuraciones de ADC personalizadas antes de planificar la actualización de ADC.

Actualización: puede actualizar las instancias ADC vulnerables 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 ADC vulnerable se rellena automáticamente como ADC de destino.

> **Nota**
>
> Las versiones 12.0, 11,0, 10.5 e inferiores ya están al final de la vida (EOL). Si las instancias de ADC se están ejecutando en cualquiera de estas versiones, actualice a una versión compatible.

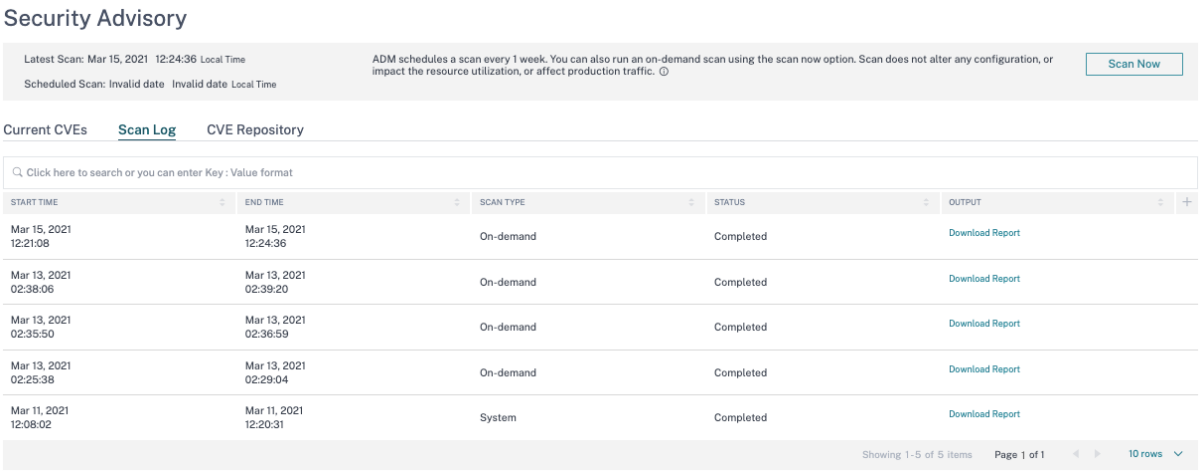
Se inicia el flujo de trabajo de actualización. Para obtener más información sobre cómo usar Citrix ADM para actualizar las instancias de ADC, consulte Crear un trabajo de actualización de ADC.

> **Nota**
>
> La versión y compilación a la que quiere actualizar está a su discreción. Consulta los consejos de la columna de corrección para saber qué versión y qué compilaciones tienen la corrección de seguridad. Y, en consecuencia, seleccione una versión y una compilación compatibles que aún no hayan llegado al final de su vida útil.



Registro de exploración

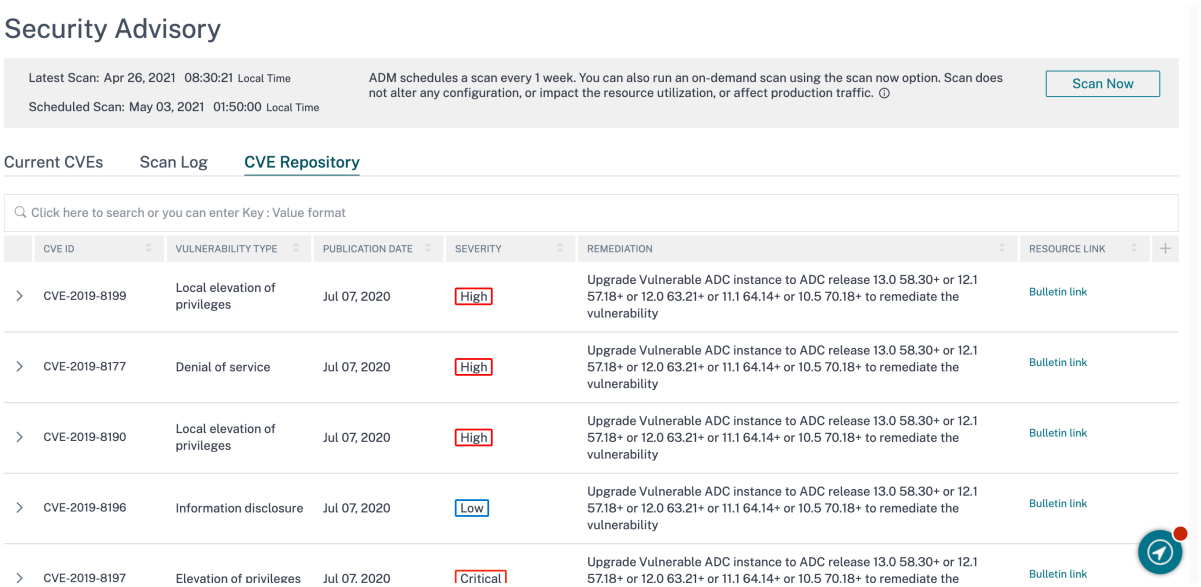
La ficha muestra informes de los últimos cinco análisis, que incluyen tanto los análisis predeterminados del sistema como los análisis bajo demanda iniciados por el usuario. Puede descargar el informe de cada escaneo en formato CSV. Si se está realizando un análisis bajo demanda, puede ver el estado de finalización aquí. Si se ha producido un error en el análisis, el estado indica eso.



Repositorio CVE

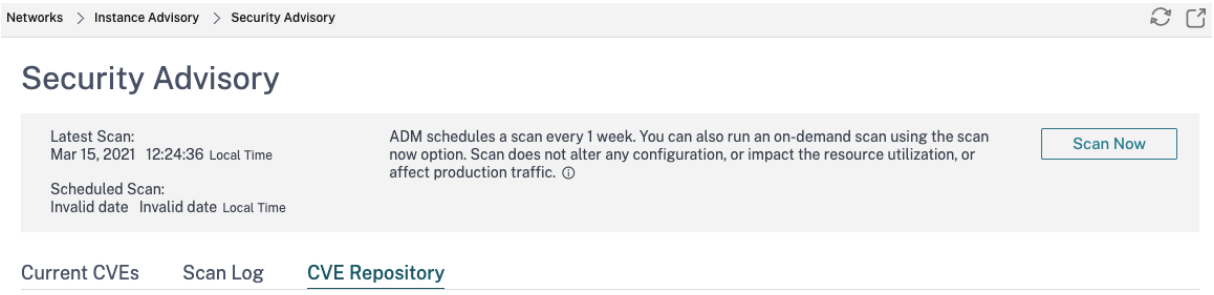
Esta ficha incluye la información más reciente de todos los CVE de diciembre de 2019, junto con los siguientes detalles:

- Identificadores CVE
- Tipo de vulnerabilidad
- Fecha de publicación
- Nivel de gravedad
- Remediación
- Enlaces a boletines de seguridad

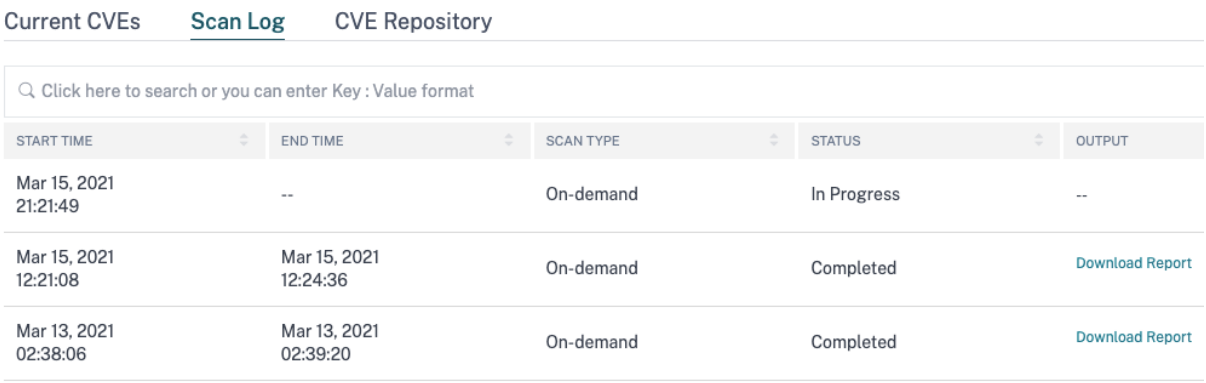


Escanear ahora

El aviso de seguridad muestra cuándo se analizaron las instancias por última vez y cuándo vence el siguiente programa. También puede escanear las instancias en cualquier momento, de acuerdo con sus necesidades. Haga clic en **Escanear ahora** para obtener el informe de seguridad más reciente de su instancia. Citrix ADM tarda unos minutos en completar el escaneo.



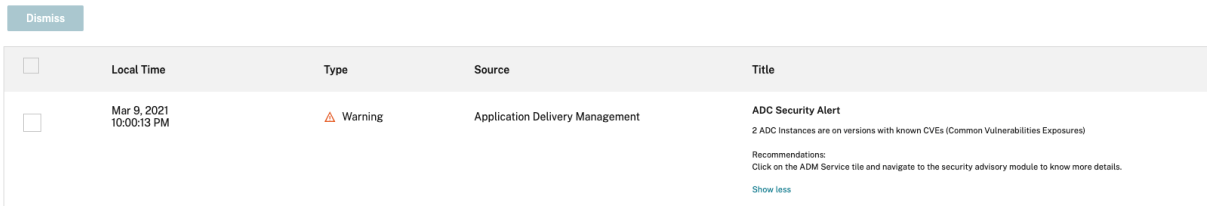
Una vez finalizado el escaneo, los detalles de seguridad revisados aparecen en la GUI del aviso de seguridad. También puede encontrar el informe en el **registro de escaneo**, que también puede descargar.



> **Nota**
>
> El registro de análisis muestra los registros de sólo los últimos cinco análisis, que pueden ser programados o bajo demanda.

Notificación

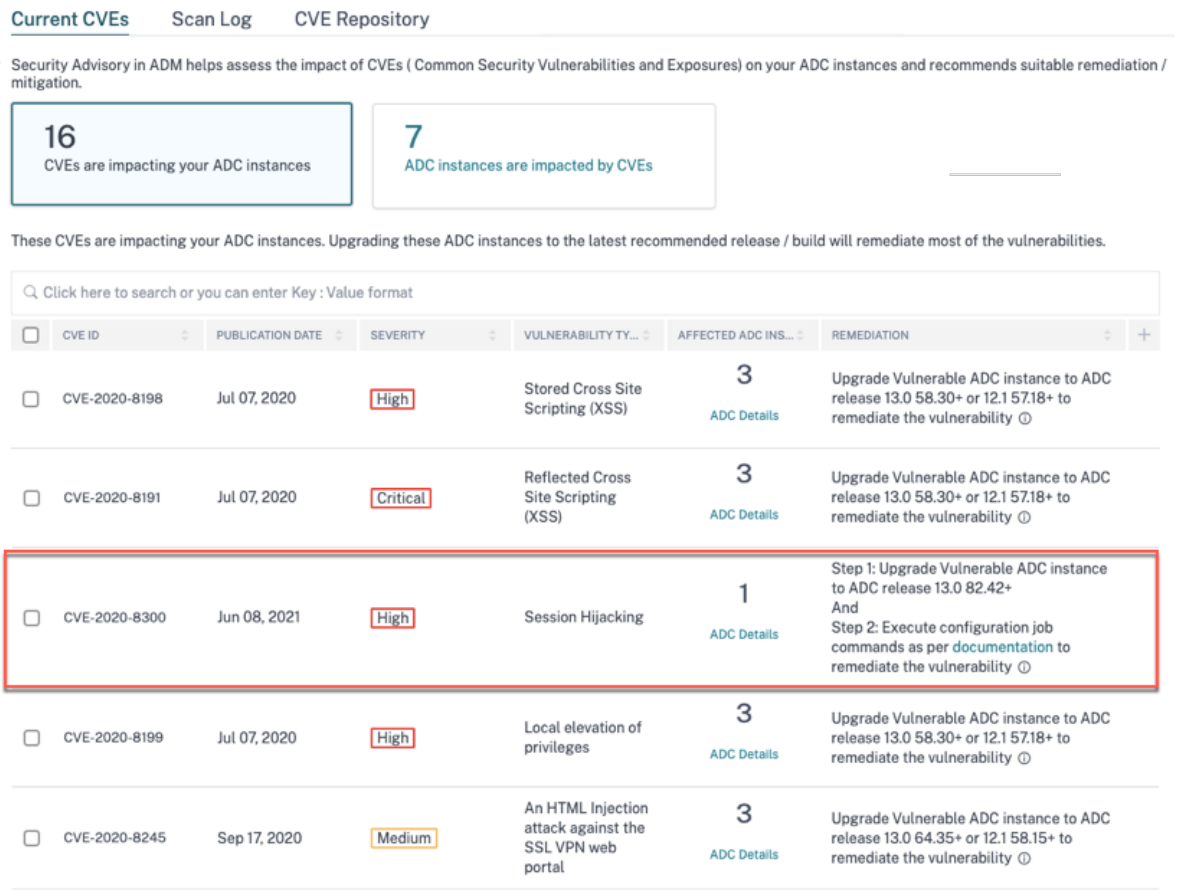
Como administrador, recibe notificaciones de Citrix Cloud, que indican cuántas instancias ADC son vulnerables. Para ver las notificaciones, haga clic en el icono de campana en la esquina superior derecha de la GUI de Citrix ADM.



Corrija las vulnerabilidades del CVE-2020-8300

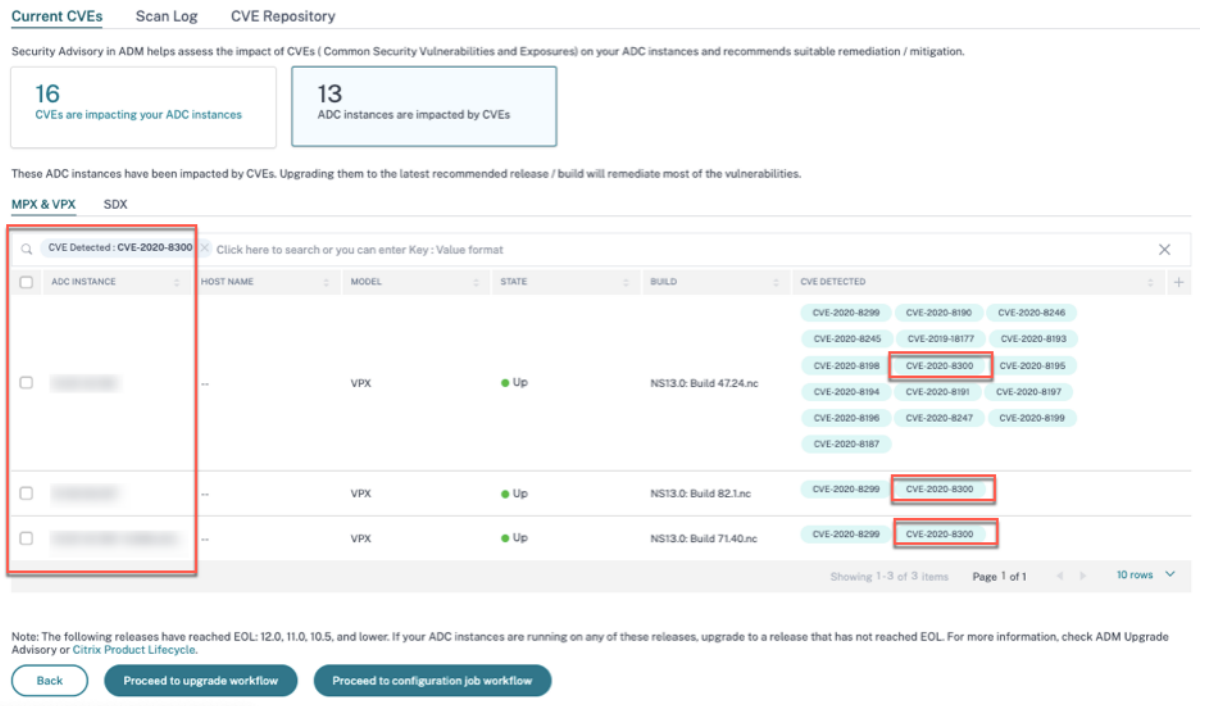
November 18, 2022

En el panel de consejos de seguridad de Citrix ADM, en **CVE actuales > Las instancias de <number of> ADC se ven afectadas por las CVE**, puede ver todas las instancias vulnerables debido a este CVE específico. Para comprobar los detalles de las instancias afectadas por el CVE-2020-8300, seleccione **CVE-2020-8300** y haga clic en **Ver instancias afectadas**.



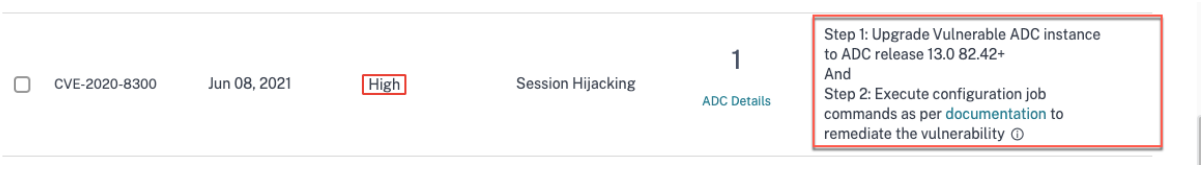
> **Nota**
>
> Para obtener más información sobre el panel de consejos de seguridad, consulte Aviso de seguridad.

Aparece la ventana **<number of>Instancias de ADC afectadas por los CVE**. Aquí puede ver el recuento y los detalles de las instancias de ADC afectadas por el CVE-2020-8300.



Corrija el CVE-2020-8300

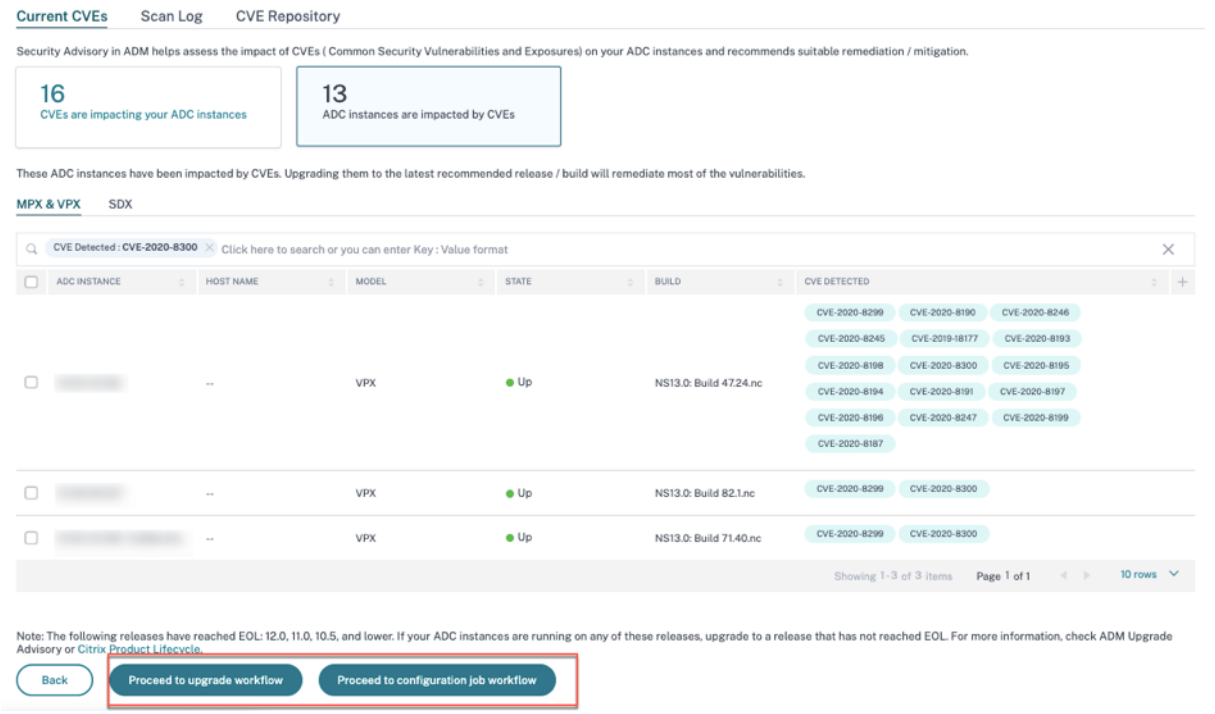
Para las instancias de ADC afectadas por el CVE-2020-8300, la corrección consiste en un proceso de dos pasos. En la GUI, en los **CVE actuales > Las instancias de ADC se ven afectadas por los CVE**, puede ver los pasos 1 y 2.



Los dos pasos incluyen:

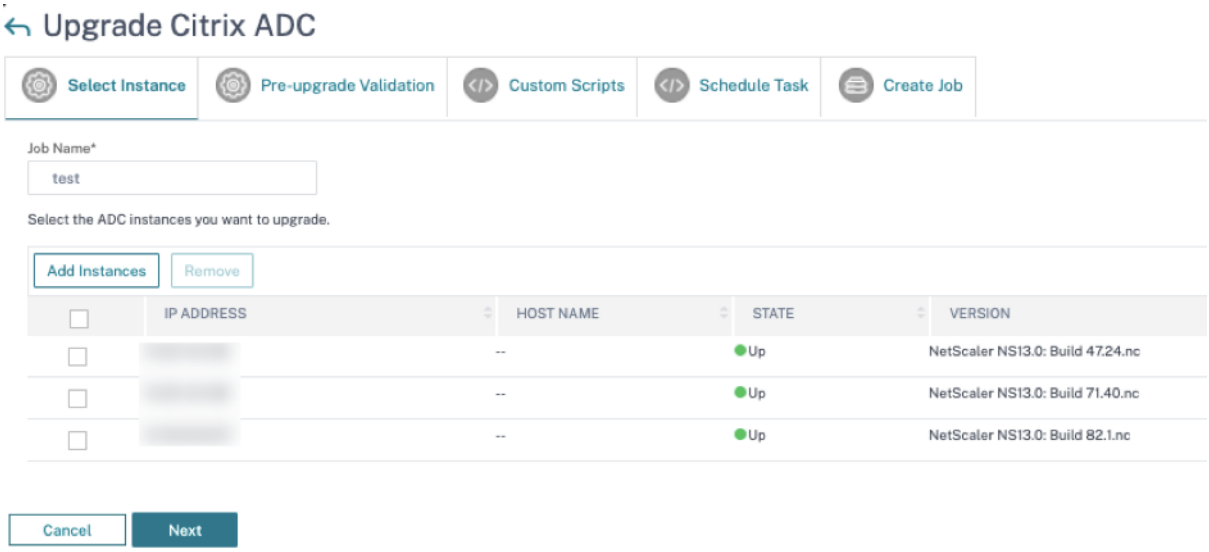
1. Actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.
2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración. Siga este paso para cada ADC vulnerable de uno en uno e incluya todas las acciones de SAML y los perfiles de SAML para ese ADC.

En **CVE actuales > Instancias de ADC afectadas por las CVE**, verá dos flujos de trabajo independientes para este proceso de corrección de 2 pasos: **Proceder a actualizar el flujo de trabajo** y **Proceder al flujo de trabajo de configuración**.



Paso 1: Actualizar las instancias de ADC vulnerables

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.



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

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de ADC vulnerables.

Paso 2: Aplicar los comandos de configuración

Tras actualizar las instancias afectadas, en la ventana **<number of> Instancias de ADC afectadas por los CVE**, seleccione una instancia afectada por el CVE-2020-8300 y haga clic en **Continuar con el flujo de trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

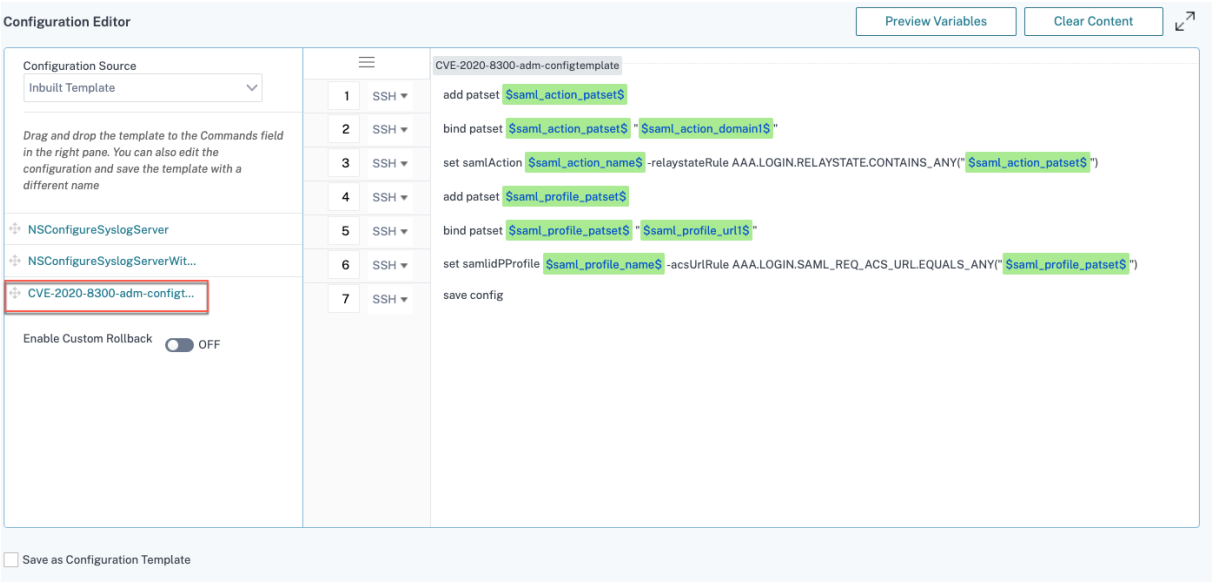
1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.
5. Ejecutar el trabajo.

Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**:

- Para una instancia de ADC afectada por varios CVE (como CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 y CVE-2021-22956): al seleccionar la instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**, la plantilla de configuración integrada no se rellena automáticamente en Seleccionar configuración. Arrastre y suelte la plantilla de trabajo de configuración correspondiente en la sección **Plantilla de asesoramiento de seguridad** manualmente en el panel de tareas de configuración del lado derecho.
- Para varias instancias de ADC que se ven afectadas únicamente por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene ADC 1, ADC 2 y ADC 3, y todos ellos se ven afectados únicamente por el CVE-2021-22956. Seleccione todas estas instancias y haga clic en **Continuar con el flujo de trabajo de configuración**, y la plantilla de configuración integrada se rellenará automáticamente en **Seleccionar configuración**. Consulte el problema conocido NSADM-80913 en las notas de la versión.
- Para varias instancias de ADC afectadas por CVE-2021-22956 y uno o más CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren una corrección para aplicarla a cada ADC a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo de configuración**, se produce un error aparece un mensaje que le indica que ejecute el trabajo de configuración en cada ADC a la vez.

Paso 1: Seleccione la configuración

En el flujo de trabajo de configuración, la plantilla de configuración integrada se rellena automáticamente en **Seleccionar configuración**.



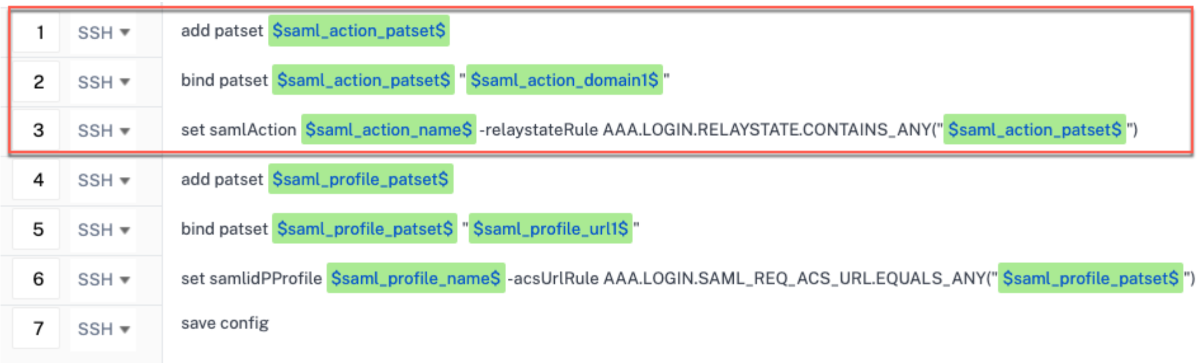
Ejecute un trabajo de configuración independiente para cada instancia de ADC afectada, de una en una, e incluya todas las acciones de SAML y los perfiles de SAML para ese ADC. Por ejemplo, si tiene dos instancias de ADC vulnerables, cada una con dos acciones de SAML y dos perfiles de SAML, debe ejecutar este trabajo de configuración dos veces. Una vez por ADC, cubriendo todas sus acciones de SAML y perfiles de SAML.

ADC 1	ADC2
Trabajo 1: dos acciones SAML+dos perfiles SAML	Trabajo 2: dos acciones SAML+dos perfiles SAML

Asigne un nombre al trabajo y personalice la plantilla para las siguientes especificaciones. La plantilla de configuración integrada es solo un esquema o una plantilla base. Personalice la plantilla en función de su implementación para cumplir con los siguientes requisitos:

a. **Acciones de SAML y sus dominios asociados**

Según la cantidad de acciones de SAML que tenga en su implementación, debe replicar las líneas 1 a 3 y personalizar los dominios para cada acción de SAML.



Por ejemplo, si tiene dos acciones de SAML, repita las líneas 1 a 3 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

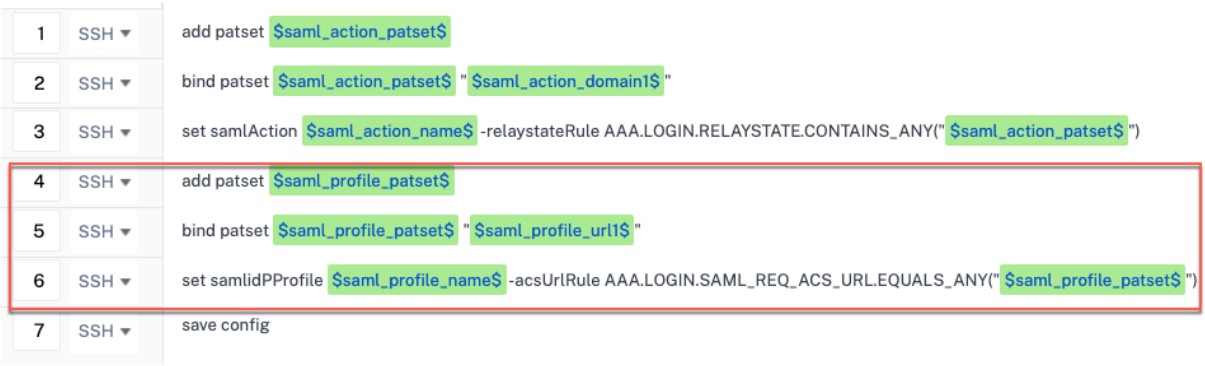
Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_action_patset$ “$saml_action_domain1$”` manualmente varias veces para asegurarse de que la línea aparezca N veces para esa acción de SAML. Y cambie los siguientes nombres de definición de variables:

- `saml_action_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) de la acción SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.
- `saml_action_domain1`: es la variable de plantilla de configuración y representa el nombre de dominio de esa acción SAML específica. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

Para buscar todas las acciones de SAML de un dispositivo, ejecute el comando `show samlaction`.

b. **Perfiles SAML y sus URL asociadas**

Según la cantidad de perfiles SAML que tenga en su implementación, replique las líneas de 4 a 6. Personalice las URL de cada perfil de SAML.



Por ejemplo, si tiene dos perfiles SAML, introduzca manualmente las líneas 4 a 6 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

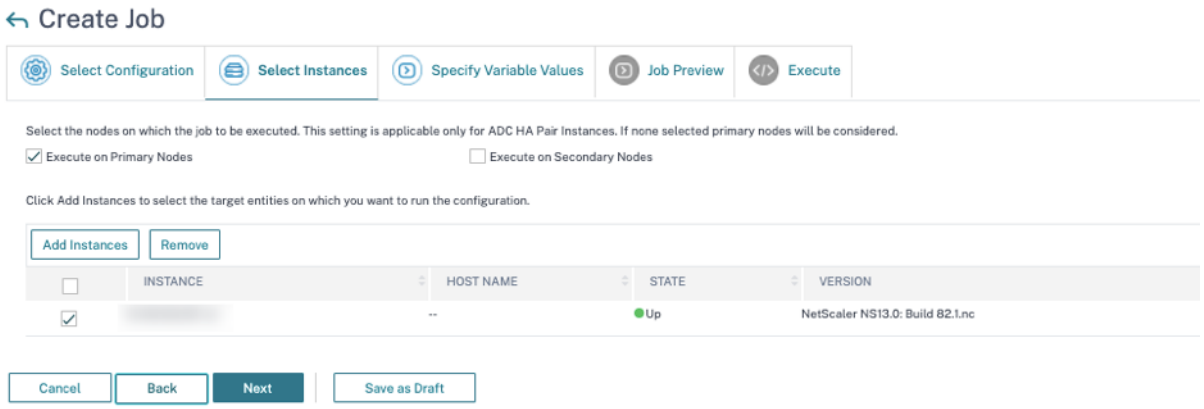
Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_profile_patset$ “$saml_profile_url1$”` manualmente varias veces para asegurarse de que la línea aparezca N veces para ese perfil de SAML. Y cambie los siguientes nombres de definición de variables:

- `saml_profile_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) del perfil SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.
- `saml_profile_url1`: es la variable de plantilla de configuración y representa el nombre de dominio de ese perfil SAML específico. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

Para buscar todos los perfiles SAM de un dispositivo, ejecute el comando `show samlidpProfile`.

Paso 2: selecciona la instancia

La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia y haga clic en **Siguiente**.

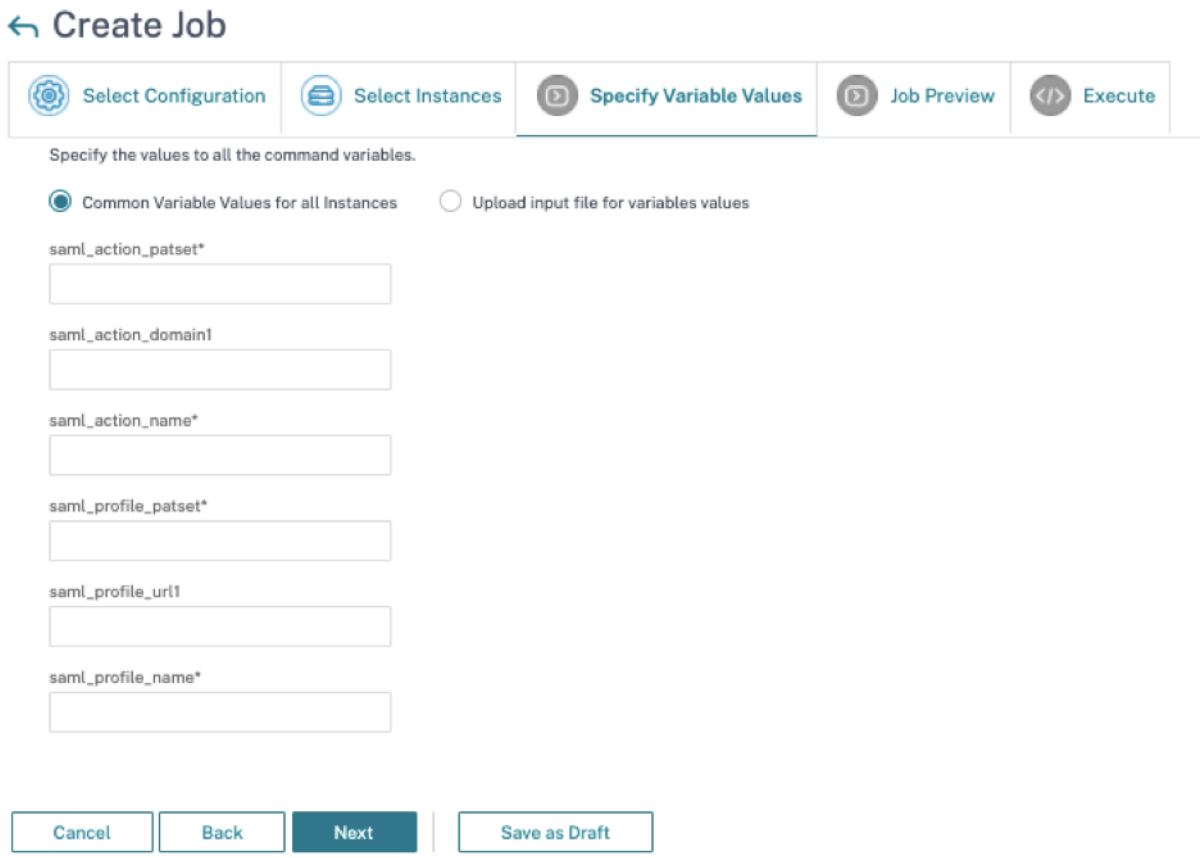


Paso 3: especificar los valores de las variables

Introduzca los valores de las variables.

- `saml_action_patset`: agregar un nombre para la acción SAML
- `saml_action_domain1`: introduzca un dominio con el formato `https://<example1.com>/`
- `saml_action_name`: introduzca lo mismo de la acción SAML para la que está configurando el trabajo
- `saml_profile_patset`: agregue un nombre para el perfil SAML
- `saml_profile_url1`: introduzca la URL en este formato `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`: introduzca el mismo perfil SAML para el que está configurando el trabajo

> **Nota**
>
> En el caso de las URL, la extensión no siempre es así `cgi/samlauth`. Depende de la autorización de terceros que tenga y, en consecuencia, debe colocar la extensión.

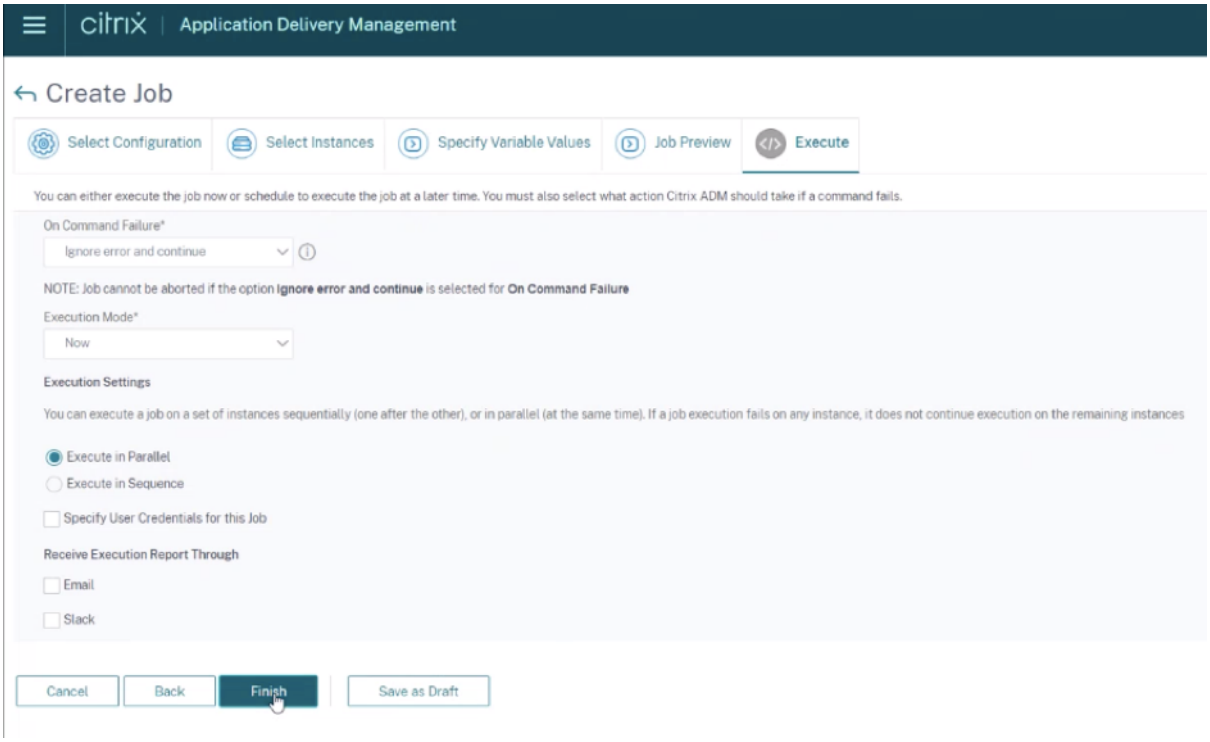


Paso 4: Vista previa de la configuración

Previsualiza los valores de las variables que se han insertado en la configuración y haga clic en **Siguiente**.

Paso 5: Ejecute el trabajo

Haga clic en **Finalizar** para ejecutar el trabajo de configuración.



Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para todos los ADC vulnerables, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Puntos a tener en cuenta sobre la cuenta Citrix ADM Express

La cuenta Citrix ADM Express tiene funciones limitadas, que incluyen la limitación de dos trabajos de configuración únicamente. Para obtener más información sobre la cuenta Citrix ADM Express, consulte Administrar los recursos de Citrix ADM mediante la cuenta Express.
Para corregir el CVE-2020-8300, debe ejecutar tantos trabajos de configuración como el número de instancias de ADC vulnerables. Por lo tanto, si tiene una cuenta Express y necesita ejecutar más de dos trabajos de configuración, siga esta solución alternativa.

Solución alternativa: ejecute dos trabajos de configuración para dos instancias de ADC vulnerables y, a continuación, elimine ambos trabajos para seguir ejecutando los dos trabajos siguientes para las dos siguientes instancias de ADC vulnerables. Continúe con esto hasta que haya cubierto todos los casos vulnerables. Antes de eliminar los trabajos, puede descargar el informe para consultarlo en el futuro. Para descargar el informe, en **Red > Trabajos**, seleccione los trabajos y haga clic en **Descargar** en **Acciones**.

Ejemplo: Si tiene seis instancias de ADC vulnerables, ejecute dos trabajos de configuración en dos instancias vulnerables respectivamente y, a continuación, elimine ambos trabajos de configuración.

Repite este paso otras dos veces. Al final, habría ejecutado seis trabajos de configuración para seis instancias de ADC, respectivamente. En la interfaz de usuario de Citrix ADM, **en Infraestructura > Trabajos**, solo verá los dos últimos trabajos de configuración.

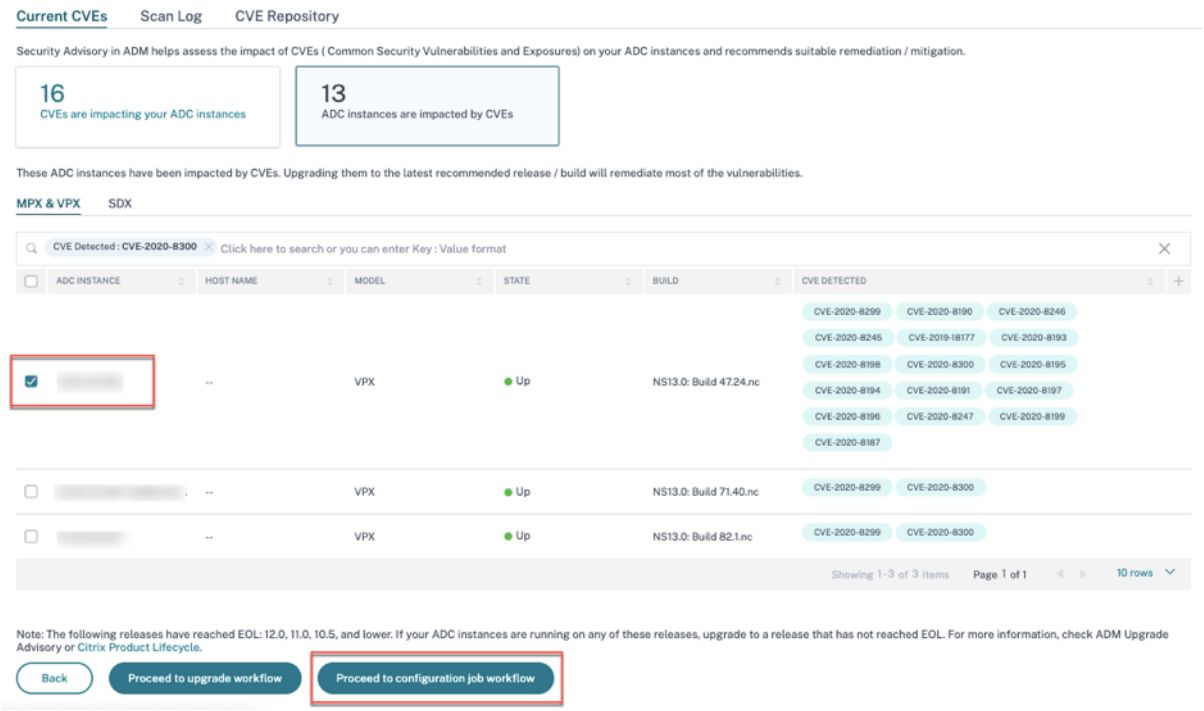
Caso

En este escenario, tres instancias de ADC son vulnerables a CVE-2020-8300 y debe corregir todas las instancias. Siga estos pasos:

1. Actualice las tres instancias de ADC siguiendo los pasos que se indican en la sección **Actualizar una instancia** de este documento.
2. Aplique el parche de configuración a un ADC a la vez, mediante el flujo de trabajo de configuración. Consulte los pasos que se indican en la sección **Aplicar comandos de configuración** de este documento.

El ADC 1 vulnerable tiene la siguiente configuración:

Dos acciones SAML	Dos perfiles SAML
La acción 1 de SAML tiene un dominio y la acción 2 de SAML tiene dos dominios	El perfil SAML 1 tiene una URL y el perfil SAML 2 tiene dos URL



Seleccione ADC 1 y haga clic en **Continuar con el flujo de trabajo de configuración**. La plantilla integrada se rellena automáticamente. A continuación, asigne un nombre a la tarea y personalice la

plantilla de acuerdo con la configuración dada.

En las tablas siguientes se enumeran las definiciones de variables para los parámetros personalizados.

Tabla 1. Definiciones de variables para la acción SAML

Configuración ADC	Definición de variable para patset	Definición de variable para el nombre de la acción SAML	Definición de variable para dominio
La acción 1 de SAML tiene un dominio	saml_action_patset1	saml_action_name1	saml_action_domain1
La acción 2 de SAML tiene dos dominios	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

Tabla 2. Definiciones de variables para el perfil SAML

Configuración ADC	Definición de variable para patset	Definición de variable para el nombre de perfil SAML	Definición de variable para URL
El perfil SAML 1 tiene una URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
El perfil SAML 2 tiene dos URL	saml_profile_patset2	saml_profile_name2	saml_profile_url2, saml_profile_url3

En **Seleccionar instancias**, seleccione ADC 1 y haga clic en **Siguiente**. Aparece la ventana **Especificar valores variables** . En este paso, debe proporcionar valores para todas las variables definidas en el paso anterior.

A continuación, revise las variables.

Haga clic en **Siguiente** y, después, en **Finalizar** para ejecutar el trabajo.

Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para ADC1, siga los mismos pasos para corregir el ADC 2 y el ADC 3. Una vez finalizada la corrección, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Vídeo de formación

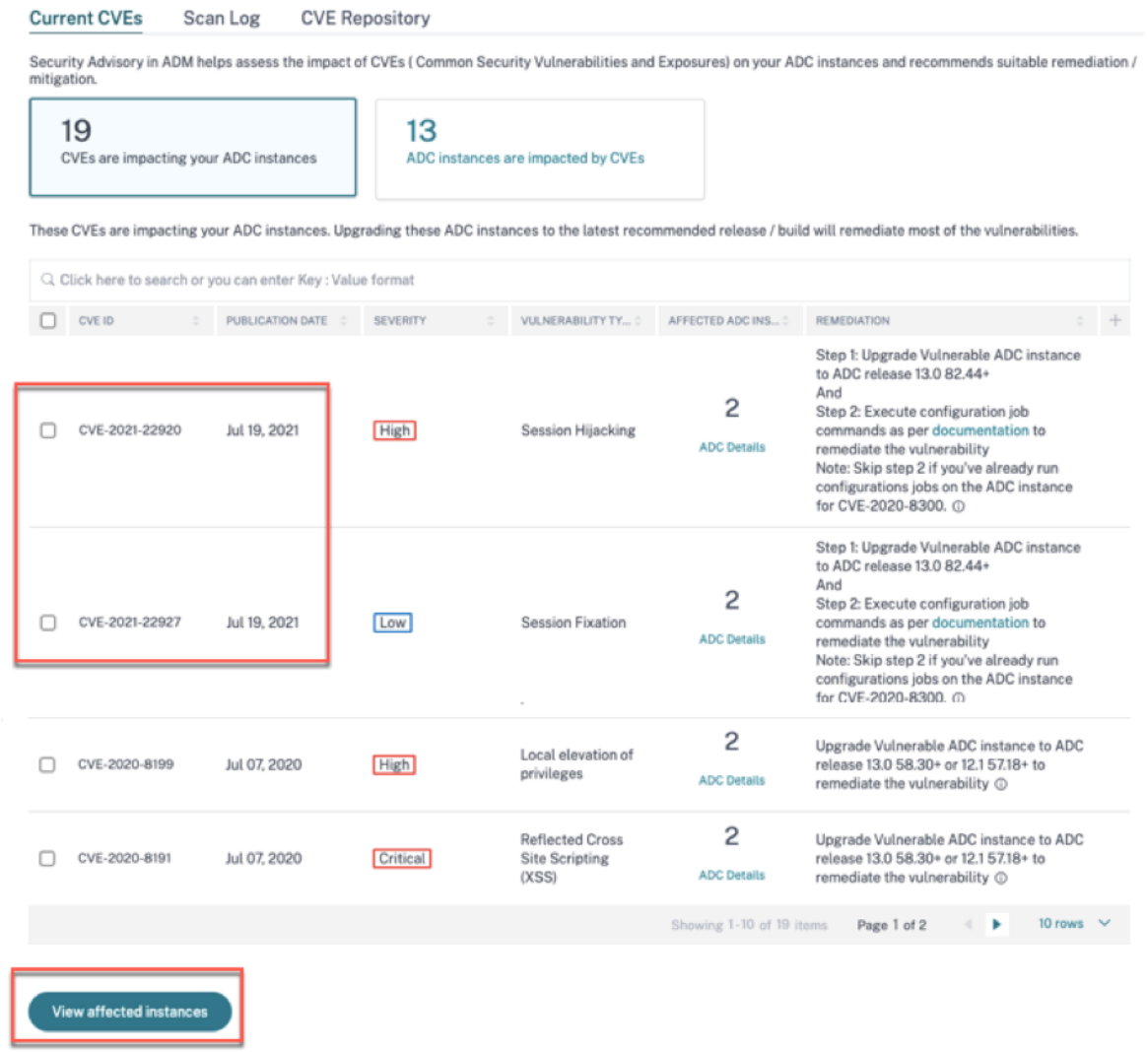
Consulte el siguiente vídeo de formación para obtener más información.

Elasesoramiento de seguridad de Citrix ADM puede ayudarlo a identificar y corregir el CVE-2020-8300.

Corrija las vulnerabilidades de los CVE-2021-22927 y CVE-2021-22920

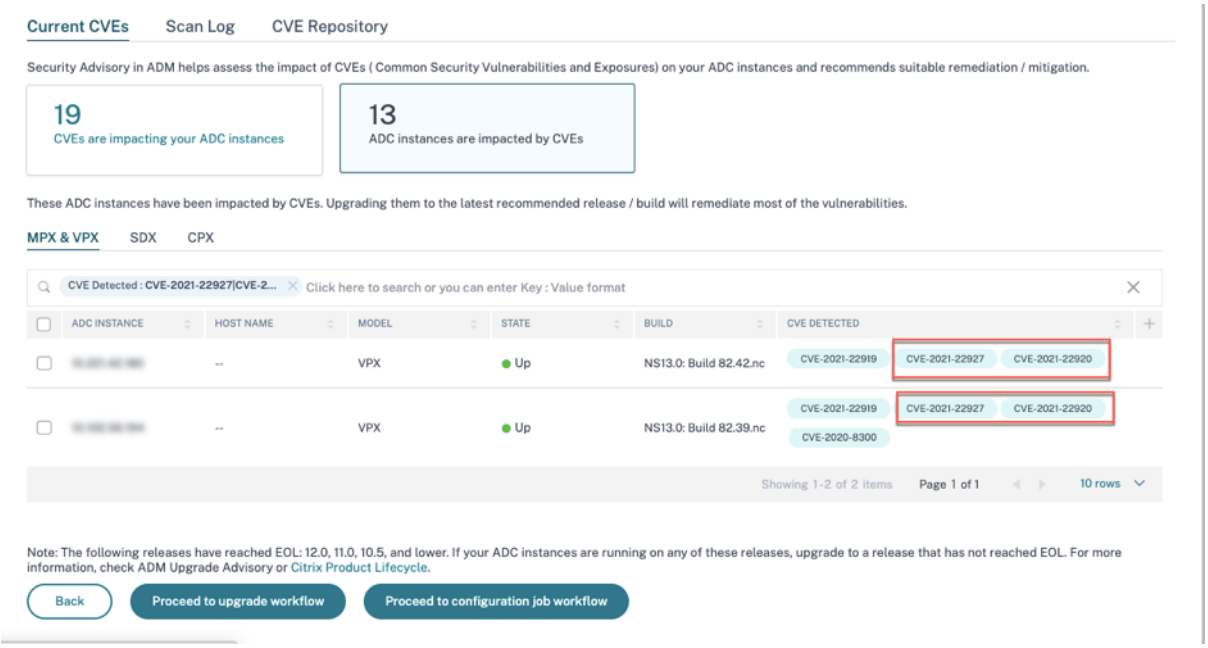
November 18, 2022

En el panel de consejos de seguridad de Citrix ADM, en **CVE actuales > Las instancias de <number of> ADC se ven afectadas por las CVE**, puede ver todas las instancias vulnerables debido a los CVE-2021-22927 y CVE-2021-22920. Para comprobar los detalles de las instancias afectadas por estos dos CVE, seleccione uno o más CVE y haga clic en **Ver instancias afectadas**.



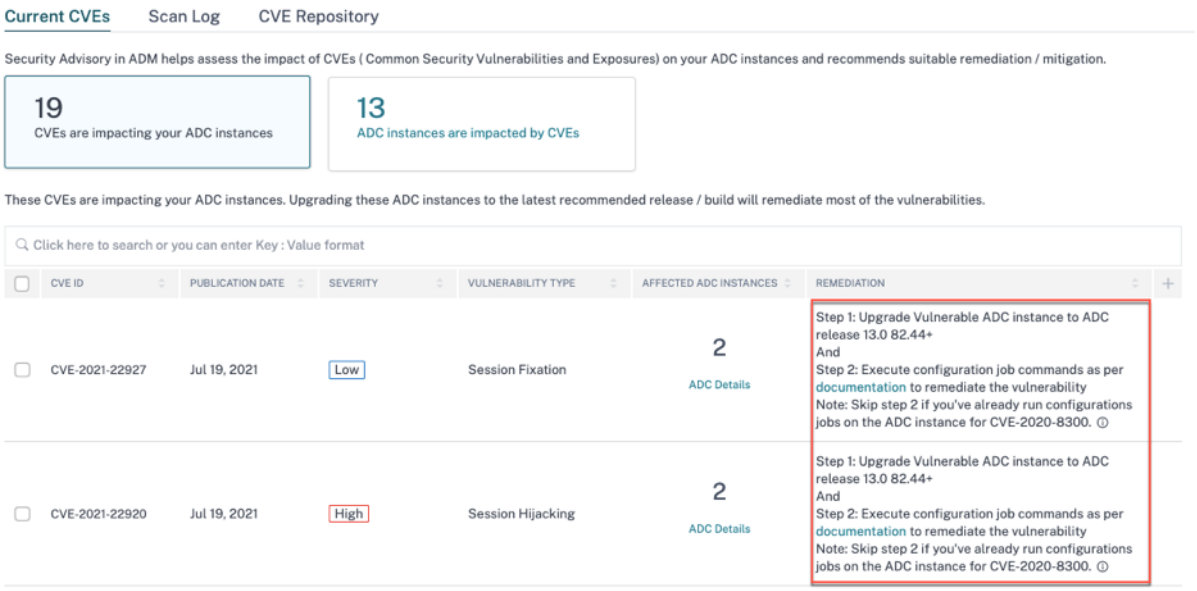
> **Nota**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde un par de horas en concluir y reflejar el impacto de los CVE-2021-22927 y CVE-2021-22920 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, inicie un análisis bajo demanda haciendo clic en **Escanear ahora**.
>
> Para obtener más información sobre el panel de consejos de seguridad, consulte Aviso de seguridad.

Aparece la ventana **<number of>Instancias de ADC afectadas por los CVE**. En la siguiente captura de pantalla, puede ver el recuento y los detalles de las instancias de ADC afectadas por los CVE-2021-22927 y CVE-2021-22920.



Corrija los CVE-2021-22927 y CVE-2021-22920

Para las instancias de ADC afectadas por los CVE-2021-22927 y CVE-2021-22920, la corrección consiste en un proceso de dos pasos. En la GUI, en los **CVE actuales > Las instancias de ADC se ven afectadas por los CVE**, puede ver los pasos 1 y 2.



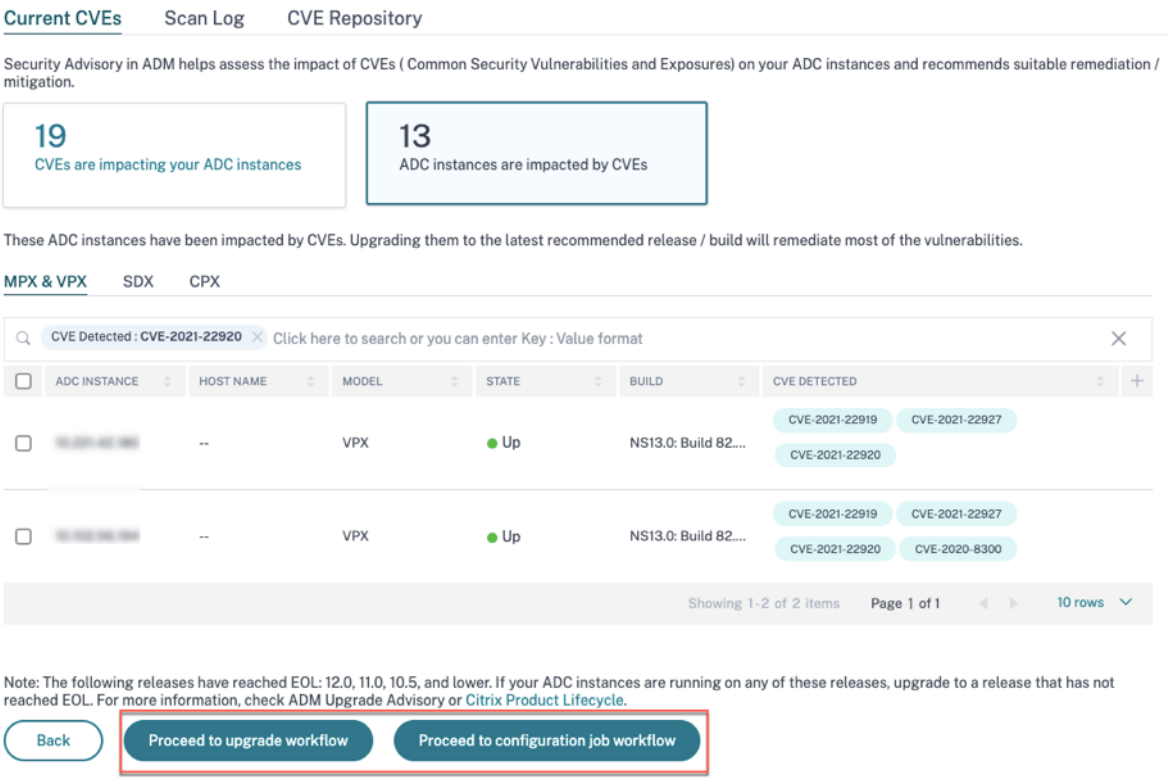
Los dos pasos incluyen:

1. Actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.

2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración. Siga este paso para cada ADC vulnerable, uno a la vez, e incluya todas las acciones de SAML para ese ADC.

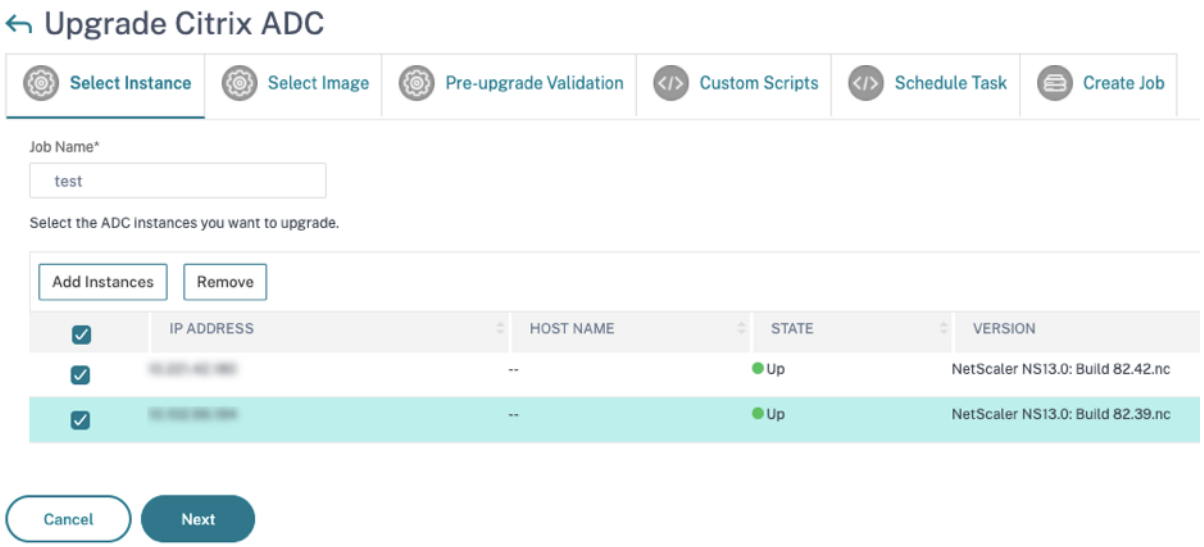
> **Nota**
>
> Omita el paso 2 si ya ha ejecutado trabajos de configuración en la instancia ADC para el CVE-2020-8300.

En **CVE actuales > Instancias de ADC afectadas por las CVE**, verá dos flujos de trabajo independientes para este proceso de corrección de 2 pasos: **Proceder a actualizar el flujo de trabajo** y **Proceder al flujo de trabajo de configuración**.



Paso 1: Actualizar las instancias de ADC vulnerables

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.



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

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de ADC vulnerables.
>
> **Nota**
>
> Tras completar el paso 1 para todas las instancias de ADC vulnerables a los CVE-2021-22920 y CVE-2021-22927, realice un análisis a petición. La postura de seguridad actualizada en los **CVE actuales** le ayuda a comprender si las instancias de ADC siguen siendo vulnerables a alguno de estos CVE. Desde la nueva postura, también puede comprobar si necesita ejecutar trabajos de configuración.
>
> Si ya ha aplicado los trabajos de configuración adecuados a la instancia de ADC para CVE-2020-8300 y ahora ha actualizado la instancia de ADC, después de realizar el análisis bajo demanda, la instancia ya no se muestra como vulnerable para CVE-2020-8300, CVE-2021-22920 y CVE-2021-22927.

Paso 2: Aplicar los comandos de configuración

Tras actualizar las instancias afectadas, en la ventana **<number of> Instancias de ADC afectadas por los CVE**, seleccione una instancia afectada por los CVE-2021-22927 y CVE-2021-22920 y haga clic en **Continuar con el flujo de trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.

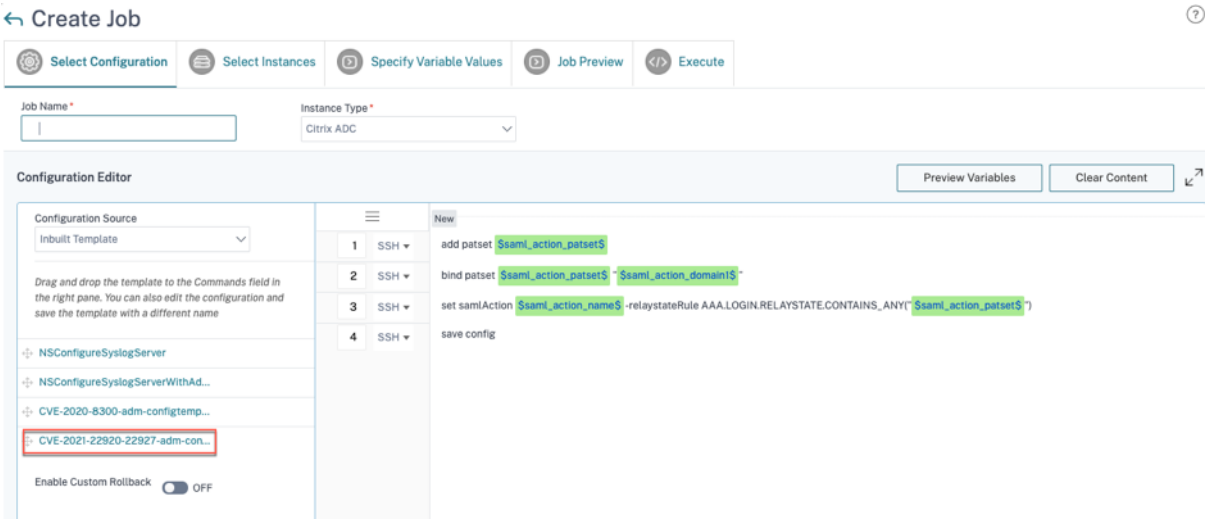
5. Ejecutar el trabajo.

Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**:

- Para una instancia de ADC afectada por varios CVE (como CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 y CVE-2021-22956): al seleccionar la instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**, la plantilla de configuración integrada no se rellena automáticamente en Seleccionar configuración. Arrastre y suelte la plantilla de trabajo de configuración correspondiente en la sección **Plantilla de asesoramiento de seguridad** manualmente en el panel de tareas de configuración del lado derecho.
- Para varias instancias de ADC que se ven afectadas únicamente por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene ADC 1, ADC 2 y ADC 3, y todos ellos se ven afectados únicamente por el CVE-2021-22956. Seleccione todas estas instancias y haga clic en **Continuar con el flujo de trabajo de configuración**, y la plantilla de configuración integrada se rellenará automáticamente en **Seleccionar configuración**. Consulte el problema conocido NSADM-80913 en las notas de la versión.
- Para varias instancias de ADC afectadas por CVE-2021-22956 y uno o más CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren una corrección para aplicarla a cada ADC a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo de configuración**, se produce un error aparece un mensaje que le indica que ejecute el trabajo de configuración en cada ADC a la vez.

Paso 1: Seleccione la configuración

En el flujo de trabajo de configuración, la plantilla base de configuración integrada se rellena automáticamente en **Seleccionar configuración**.



> **Nota**
>
> Si la instancia de ADC seleccionada en el paso 2 para aplicar los comandos de configuración es vulnerable a CVE-2021-22927, CVE-2021-22920 y también a CVE-2020-8300, la plantilla base de CVE-2020-8300 se rellena automáticamente. La plantilla CVE-2020-8300 es un superconjunto de comandos de configuración necesarios para los tres CVE. Personalice esta plantilla base de acuerdo con la implementación y los requisitos de su instancia de ADC.

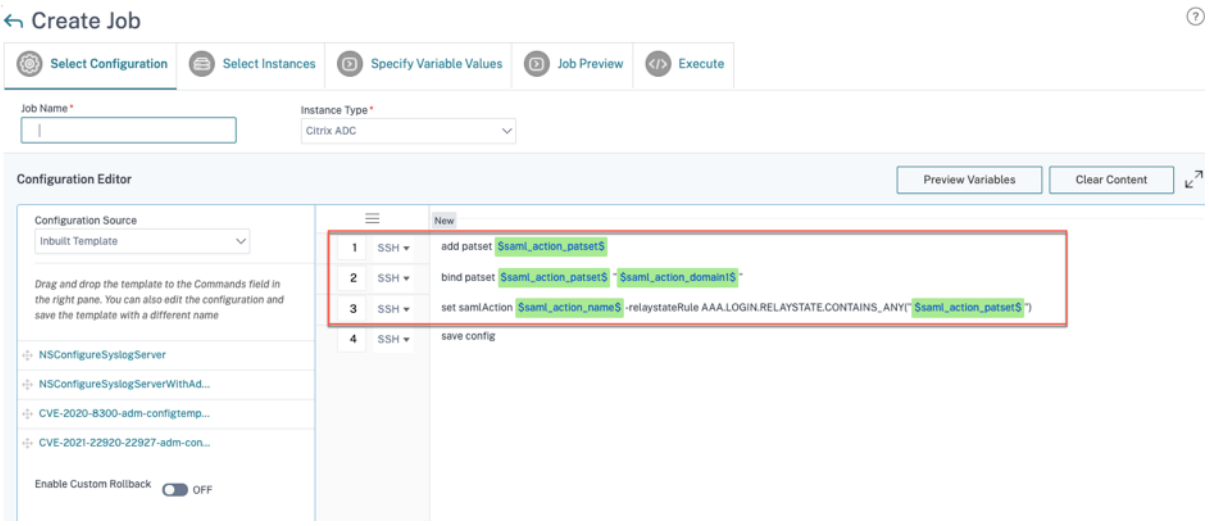
Debe ejecutar un trabajo de configuración independiente para cada instancia de ADC afectada, una a la vez, e incluir todas las acciones de SAML para ese ADC. Por ejemplo, si tiene dos instancias de ADC vulnerables, cada una con dos acciones de SAML, debe ejecutar este trabajo de configuración dos veces. Una vez por ADC cubriendo todas sus acciones de SAML.

ADC 1	ADC2
Trabajo 1: dos acciones de SAML	Trabajo 2: dos acciones de SAML

Asigne un nombre al trabajo y personalice la plantilla para las siguientes especificaciones. La plantilla de configuración integrada es solo un esquema o una plantilla base. Personalice la plantilla en función de su implementación para cumplir con los siguientes requisitos:

a. **Acciones de SAML y sus dominios asociados**

Según la cantidad de acciones de SAML que tenga en su implementación, debe replicar las líneas 1 a 3 y personalizar los dominios para cada acción de SAML.



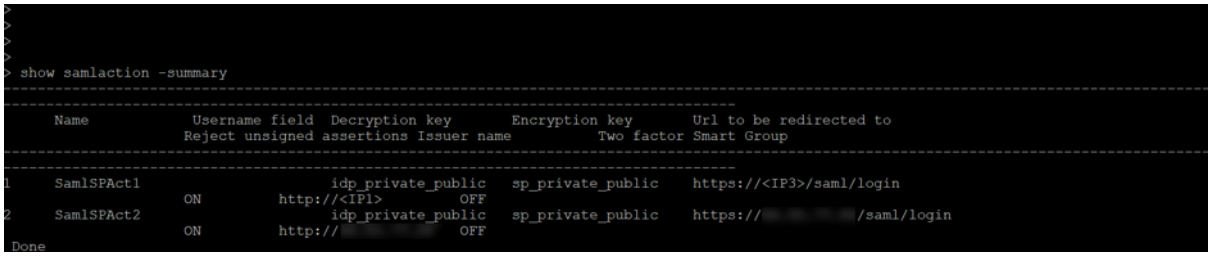
Por ejemplo, si tiene dos acciones de SAML, repita las líneas 1 a 3 dos veces y, en consecuencia, personalice las definiciones de variables para cada acción de SAML.

Y si tiene N dominios para una acción de SAML, debe escribir la línea `bind patset $saml_action_patset$ “$saml_action_domain1$”` manualmente varias veces para asegurarse de que la línea aparezca

N veces para esa acción de SAML. Y cambie los siguientes nombres de definición de variables:

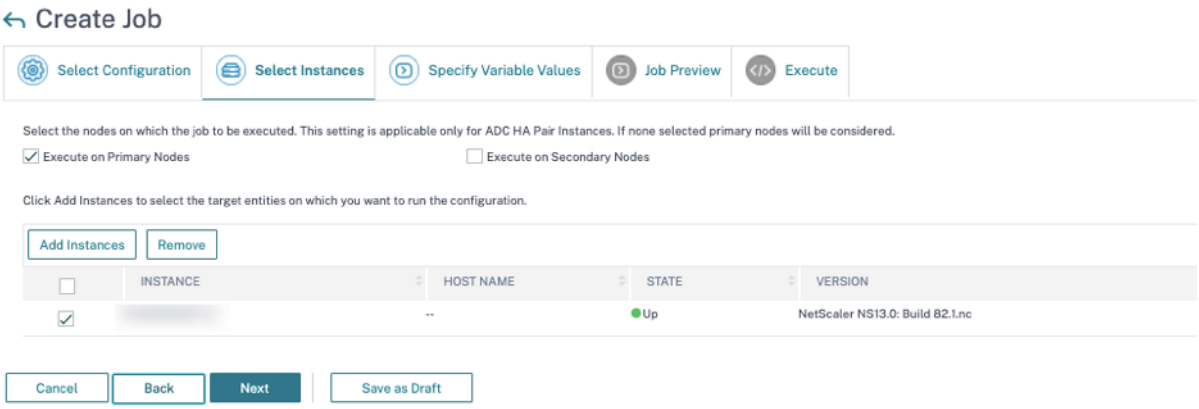
- `saml_action_patset`: es la variable de plantilla de configuración y representa el valor del nombre del conjunto de patrones (patset) de la acción SAML. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.
- `saml_action_domain1`: es la variable de plantilla de configuración y representa el nombre de dominio de esa acción SAML específica. Puede especificar el valor real en el paso 3 del flujo de trabajo de configuración. Consulte la sección Paso 3: Especificar los valores de las variables en este documento.

Para buscar todas las acciones de SAML de un dispositivo, ejecute el comando `show samlaction`.



Paso 2: selecciona la instancia

La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia y haga clic en **Siguiente**.

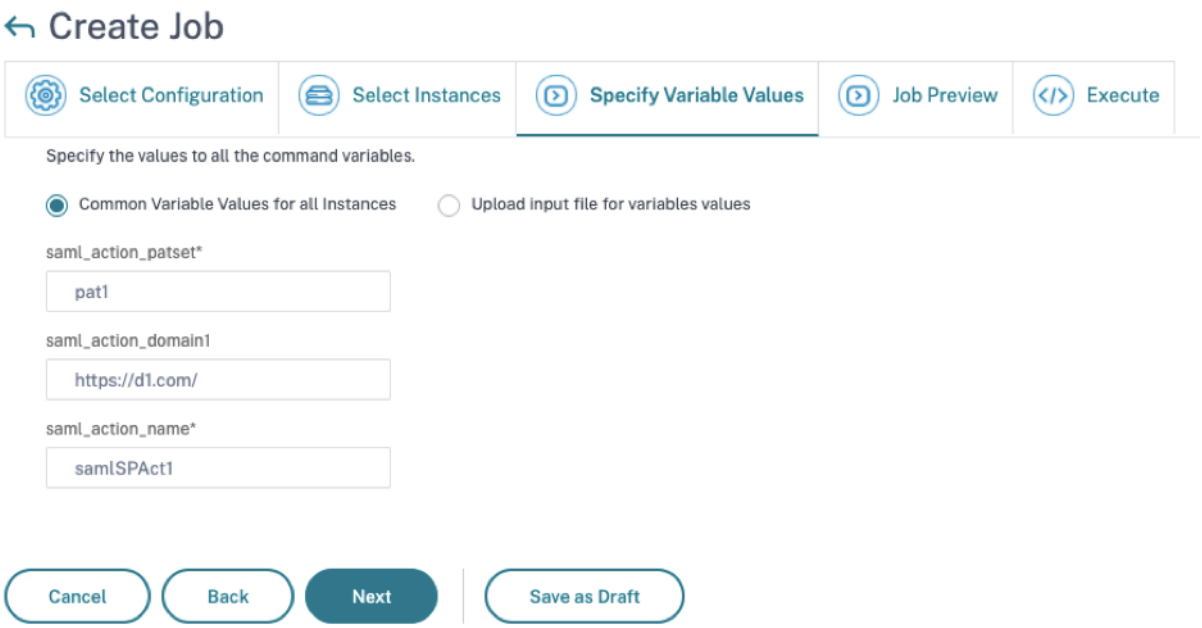


Paso 3: especificar los valores de las variables

Introduzca los valores de las variables.

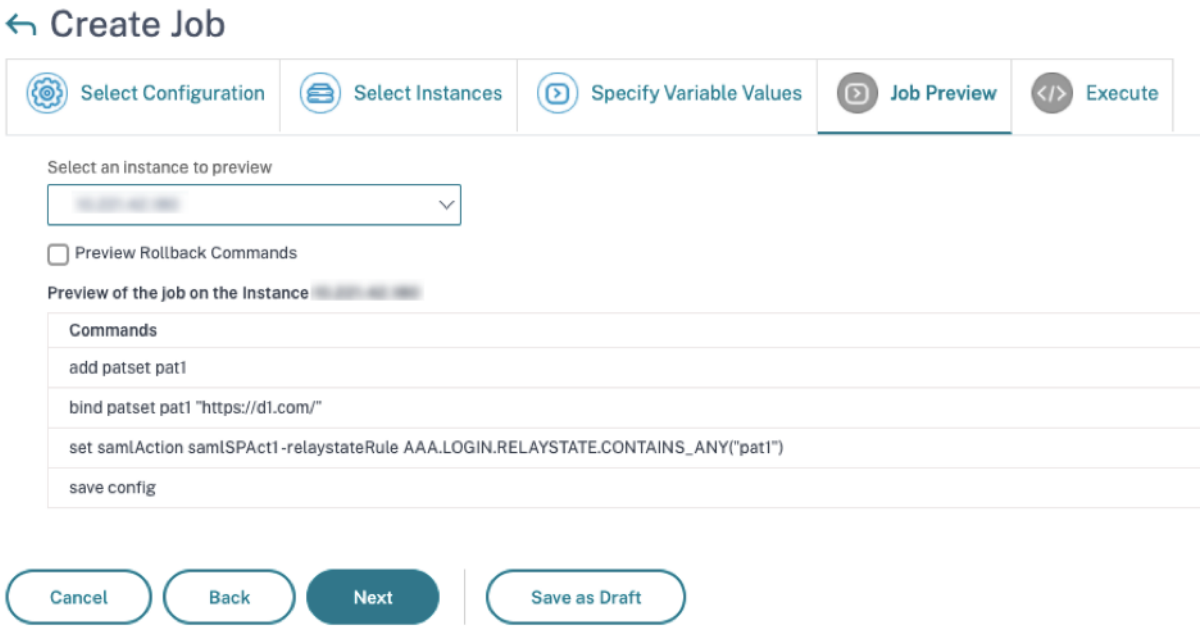
- `saml_action_patset`: agregar un nombre para la acción SAML

- `saml_action_domain1`: introduzca un dominio con el formato `https://<example1.com>/`
- `saml_action_name`: introduzca lo mismo de la acción SAML para la que está configurando el trabajo



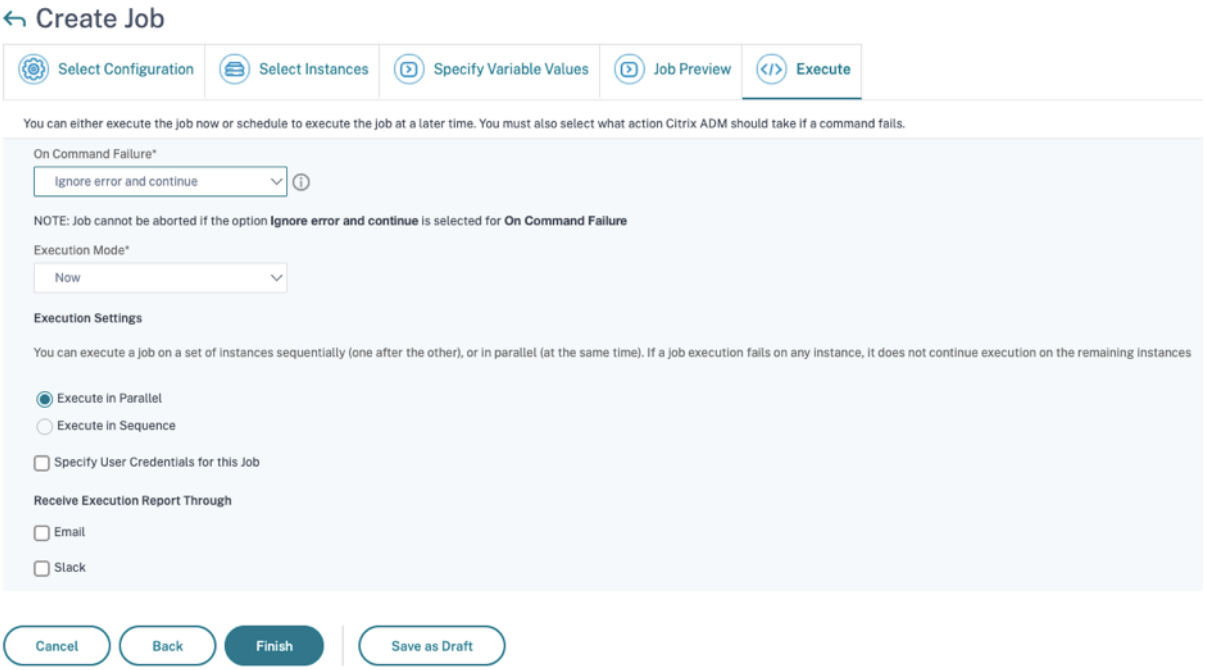
Paso 4: Vista previa de la configuración

Previsualiza los valores de las variables que se han insertado en la configuración y haga clic en **Siguiente**.



Paso 5: Ejecute el trabajo

Haga clic en **Finalizar** para ejecutar el trabajo de configuración.



Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para todos los ADC vulnerables, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

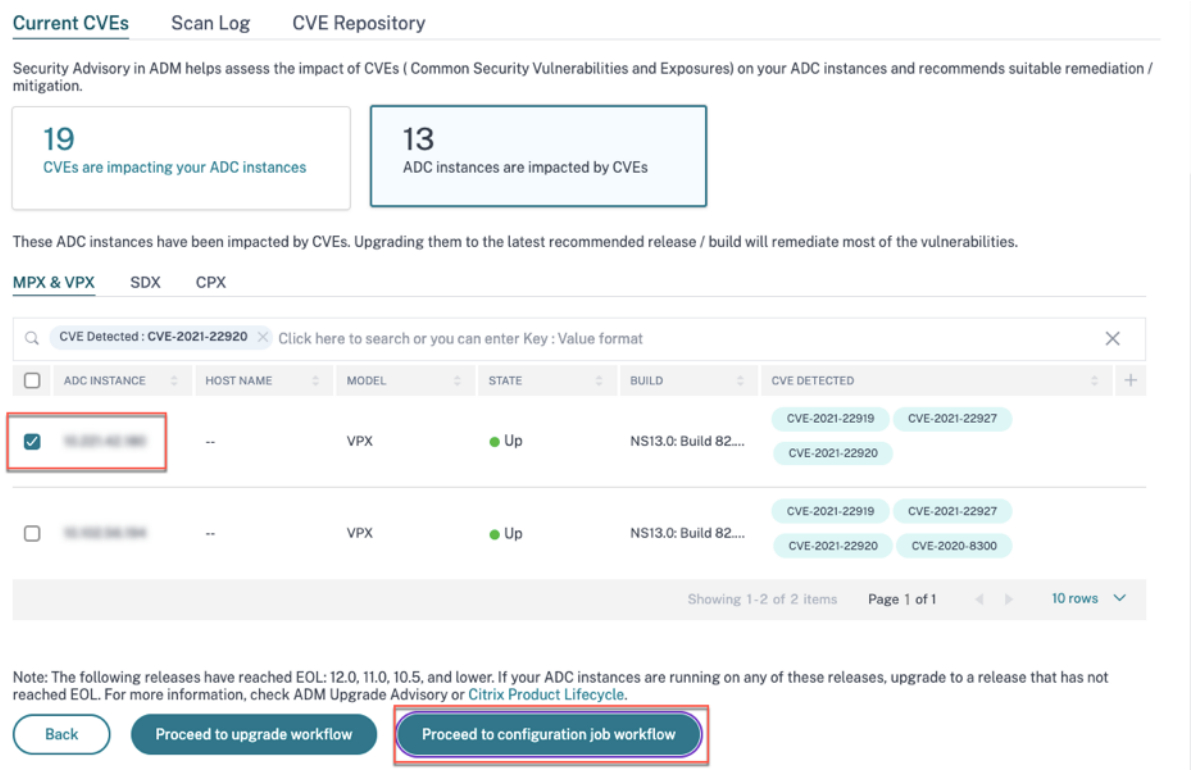
Caso

En este escenario, dos instancias de ADC son vulnerables a CVE-2021-22920 y debe corregir todas las instancias. Siga estos pasos:

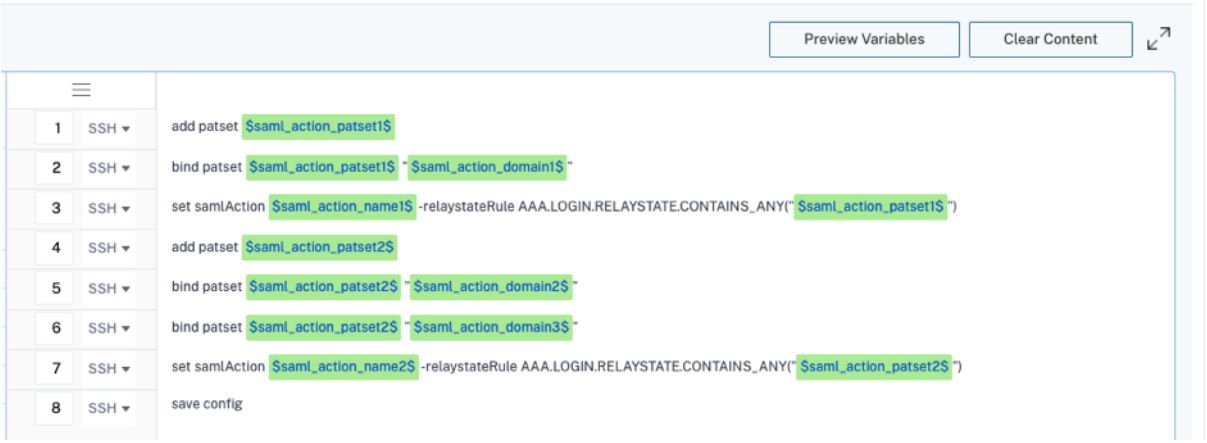
1. Actualice las tres instancias de ADC siguiendo los pasos que se indican en la sección «Actualizar una instancia» de este documento.
2. Aplique el parche de configuración a un ADC a la vez, mediante el flujo de trabajo de configuración. Consulte los pasos que se indican en la sección «Aplicar comandos de configuración» de este documento.

El ADC 1 vulnerable tiene dos acciones de SAML:

- La acción 1 de SAML tiene un dominio
- La acción 2 de SAML tiene dos dominios



Seleccione ADC 1 y haga clic en **Continuar con el flujo de trabajo de configuración**. La plantilla base integrada se rellena automáticamente. A continuación, asigne un nombre a la tarea y personalice la plantilla de acuerdo con la configuración dada.

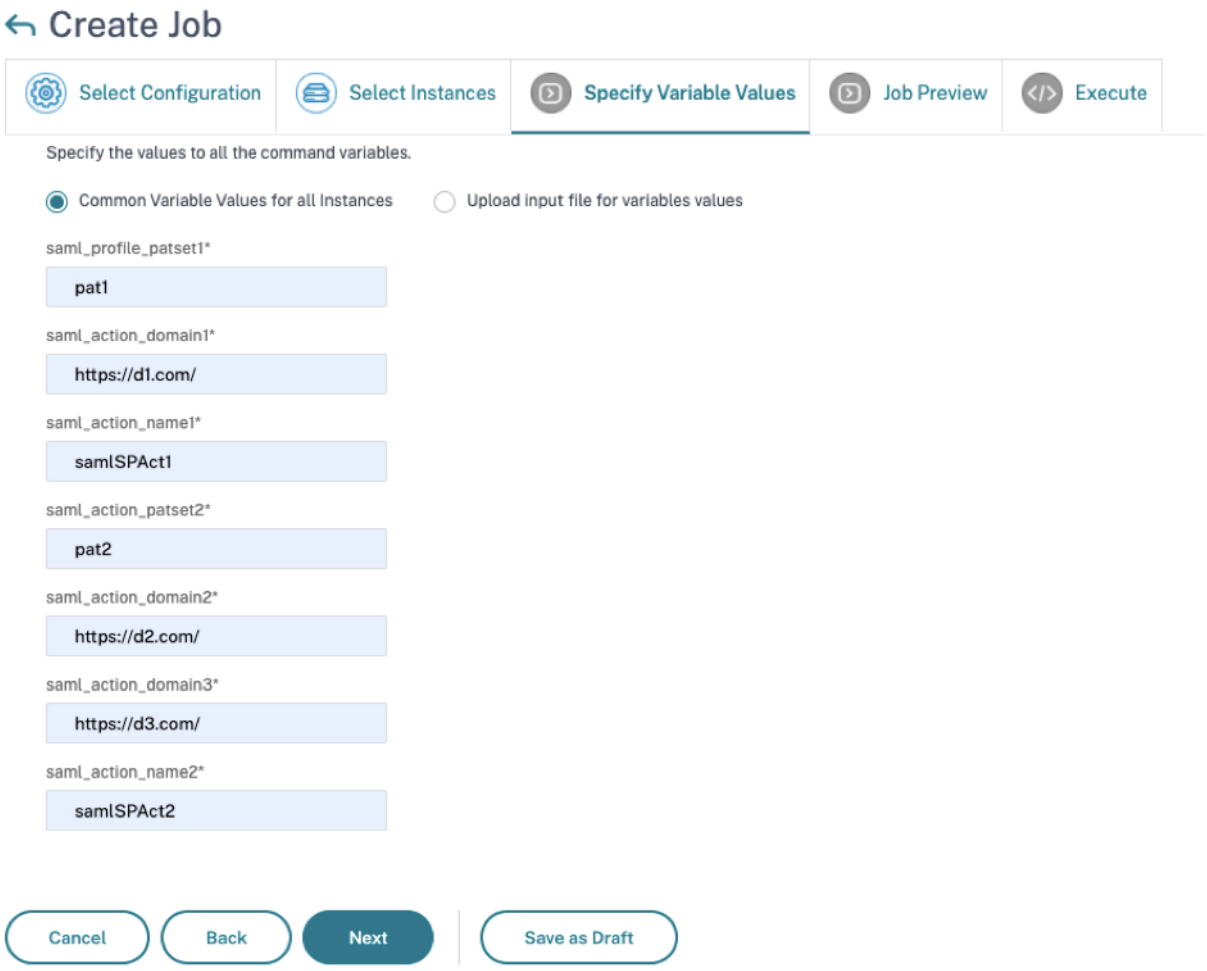


En la tabla siguiente se enumeran las definiciones de variables para los parámetros personalizados.

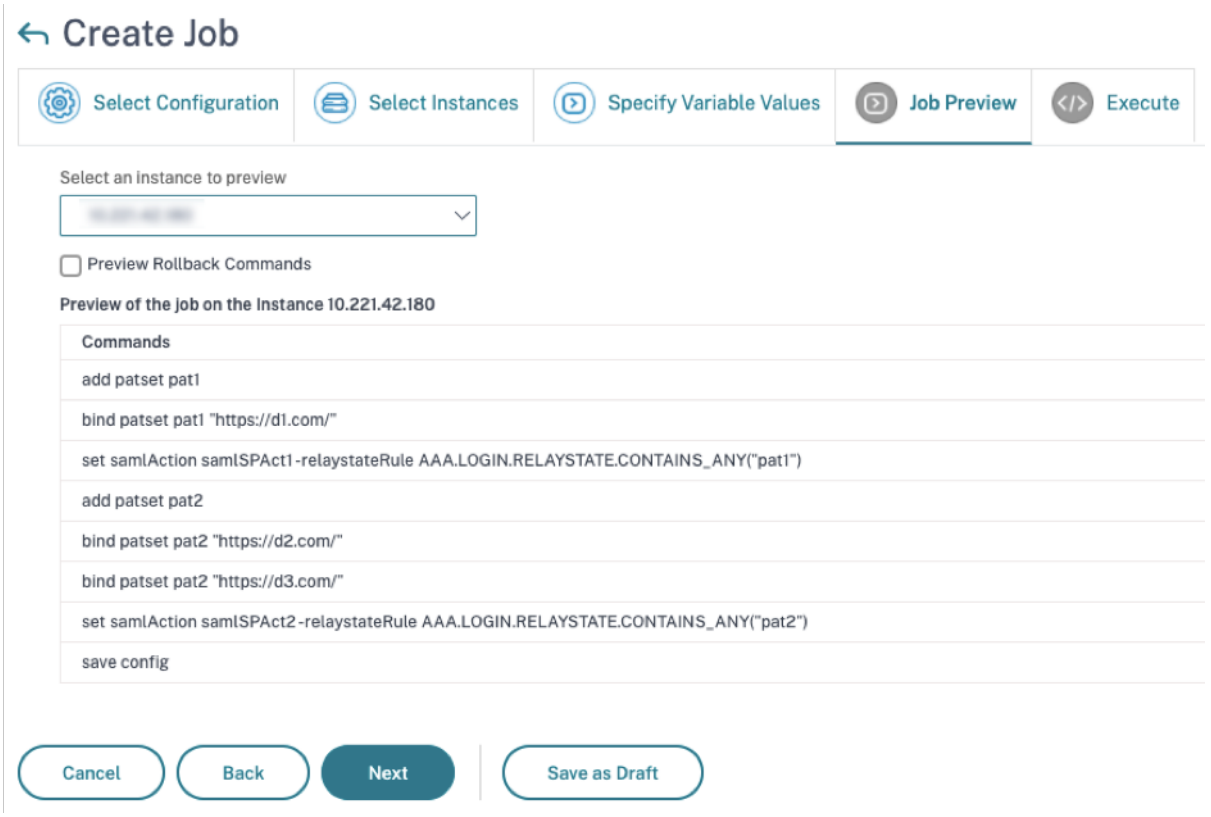
Mesa. Definiciones de variables para la acción SAML

Configuración ADC	Definición de variable para patset	Definición de variable para el nombre de la acción SAML	Definición de variable para dominio
La acción 1 de SAML tiene un dominio	saml_action_patset1	saml_action_name1	saml_action_domain1
La acción 2 de SAML tiene dos dominios	saml_action_patset2	saml_action_name2	saml_action_domain2, saml_action_domain3

En **Seleccionar instancias**, seleccione ADC 1 y haga clic en **Siguiente**. Aparece la ventana **Especificar valores variables** . En este paso, debe proporcionar valores para todas las variables definidas en el paso anterior.



A continuación, revise las variables.



Haga clic en **Siguiente** y, después, en **Finalizar** para ejecutar el trabajo.

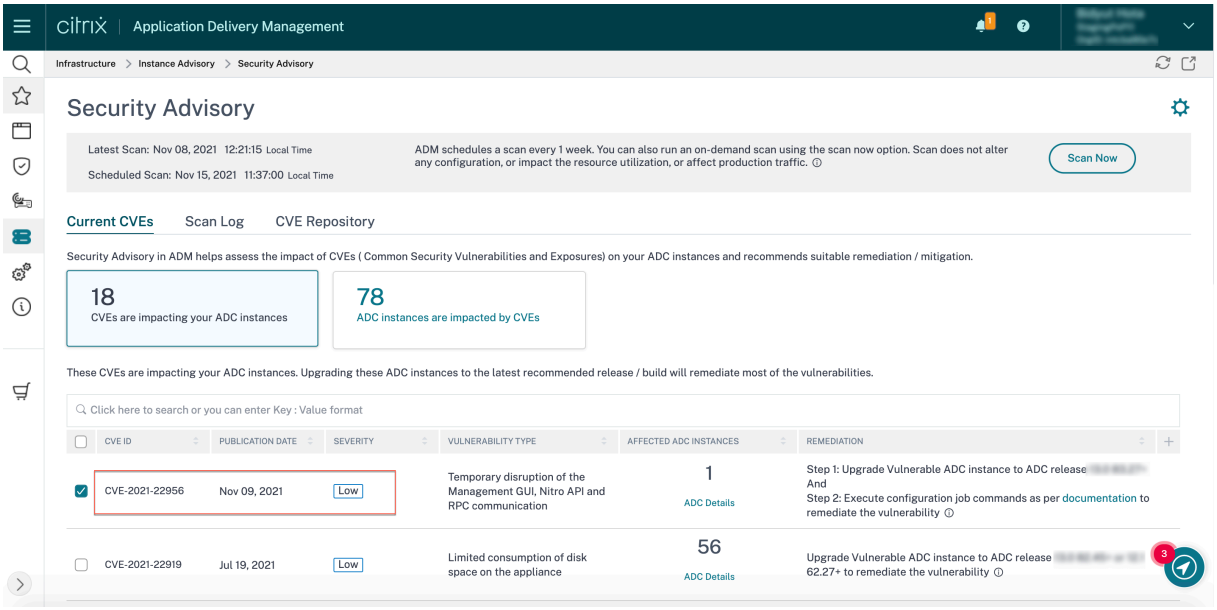
Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configuración**.

Tras completar los dos pasos de corrección para ADC1, siga los mismos pasos para corregir el ADC 2 y el ADC 3. Una vez finalizada la corrección, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

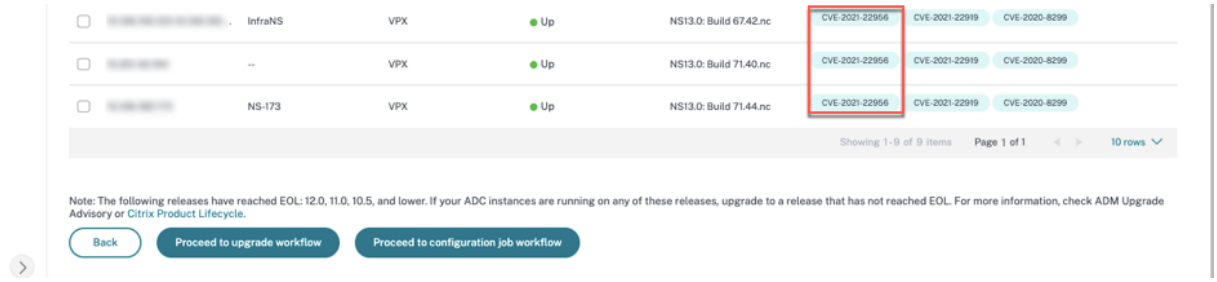
Identificar y corregir las vulnerabilidades del CVE-2021-22956

November 18, 2022

En el panel de asesoramiento de seguridad de Citrix ADM, en CVE**actuales > Las instancias de<** `number of`**>**ADC se ven afectadas por vulnerabilidades y exposiciones (CVE) comunes, puede ver todas las instancias vulnerables debido a este CVE específico. Para comprobar los detalles de las instancias afectadas por el CVE-2021-22956, seleccione CVE-2021-22956 y haga clic en **Ver instancias afectadas**.



Aparecen las instancias de<number of>ADC afectadas por la ventana CVE. Aquí puede ver el recuento y los detalles de las instancias de ADC afectadas por el CVE-2021-22956.



Para obtener más información sobre el panel de consejos de seguridad, consulte Aviso de seguridad.

> **Nota**
>
> Es posible que el escaneo del sistema de asesoramiento de seguridad tarde algún tiempo en concluir y reflejar el impacto del CVE-2021-22956 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, inicie un análisis bajo demanda haciendo clic en **Escanear ahora**.

Identifique las instancias afectadas por el CVE-2021-22956

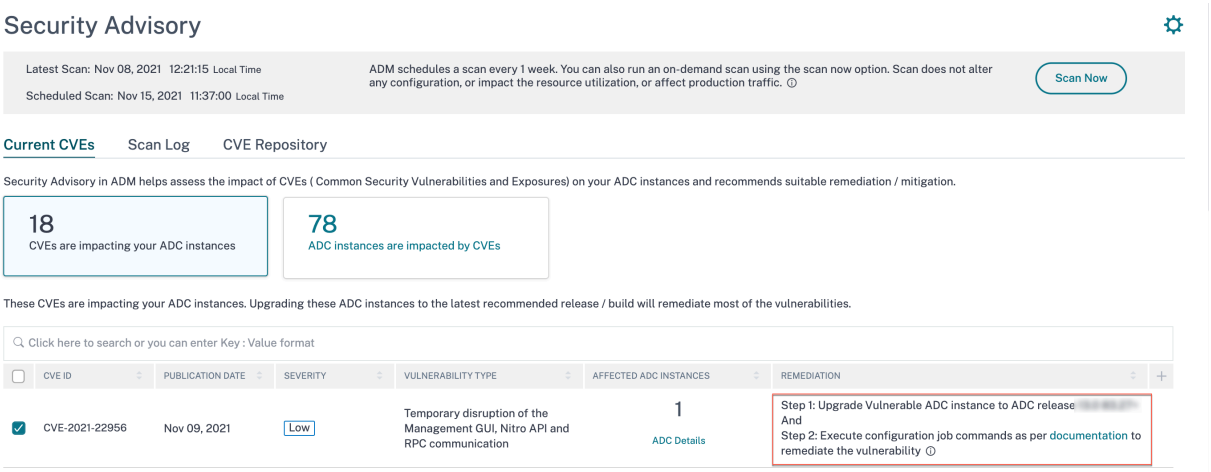
El CVE-2021-22956 requiere un escaneo personalizado, en el que el servicio ADM se conecta con la instancia ADC administrada y envía un script a la instancia. El script se ejecuta en la instancia ADC y comprueba los parámetros del archivo de configuración de Apache (`httpd.conf file`) y del número máximo de conexiones de cliente (`maxclient`) para determinar si una instancia es vulnerable o no. La información que el script comparte con el servicio ADM es el estado de la vulnerabilidad en formato booleano (verdadero o falso). El script también devuelve al servicio ADM una lista de recuentos de max_clients para diferentes interfaces de red, por ejemplo, host local, NSIP y SNIP con acceso de

administración. 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 ADC.

Remediar CVE-2021-22956

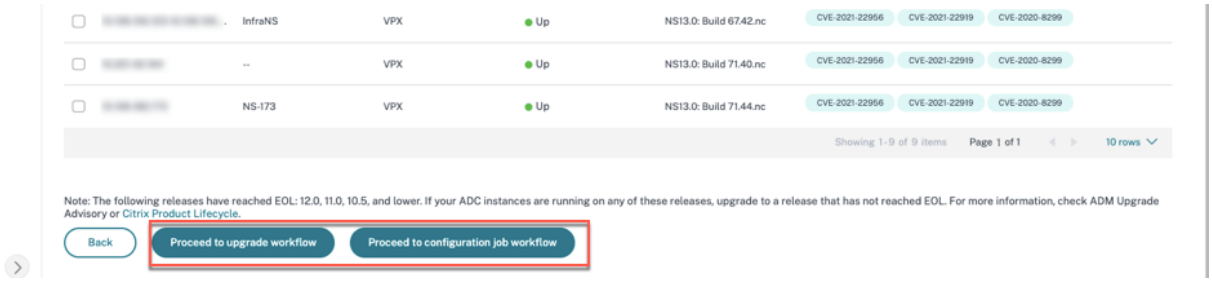
Para las instancias de ADC afectadas por el CVE-2021-22956, la corrección consiste en un proceso de dos pasos. En la GUI, en los**CVE actuales > Las instancias de ADC se ven afectadas por los CVE**, puede ver los pasos 1 y 2.



Los dos pasos incluyen:

1. Actualización de las instancias de ADC vulnerables a una versión y una compilación que tengan la solución.
2. Aplicar los comandos de configuración necesarios mediante la plantilla de configuración integrada personalizable en los trabajos de configuración.

En CVE actuales > Instancias de ADC afectadas por las CVE, verá dos flujos de trabajo independientes para este proceso de corrección de 2 pasos: Proceder a actualizar el flujo de trabajo y Proceder al flujo de trabajo de configuración.



Paso 1: Actualizar las instancias de ADC vulnerables

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.

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

> **Nota**
>
> Este paso se puede realizar de una vez para todas las instancias de ADC vulnerables.

Paso 2: Aplicar los comandos de configuración

Tras actualizar las instancias afectadas, en la ventana **<number of> Instancias de ADC afectadas por los CVE**, seleccione la instancia afectada por el CVE-2021-2295 y haga clic en **Continuar con el flujo de trabajo de configuración**. El flujo de trabajo incluye los siguientes pasos.

1. Personalización de la configuración.
2. Revisar las instancias afectadas que se rellenan automáticamente.
3. Especificar entradas para las variables del trabajo.
4. Revisar la configuración final con las entradas variables rellenadas.
5. Ejecutar el trabajo.

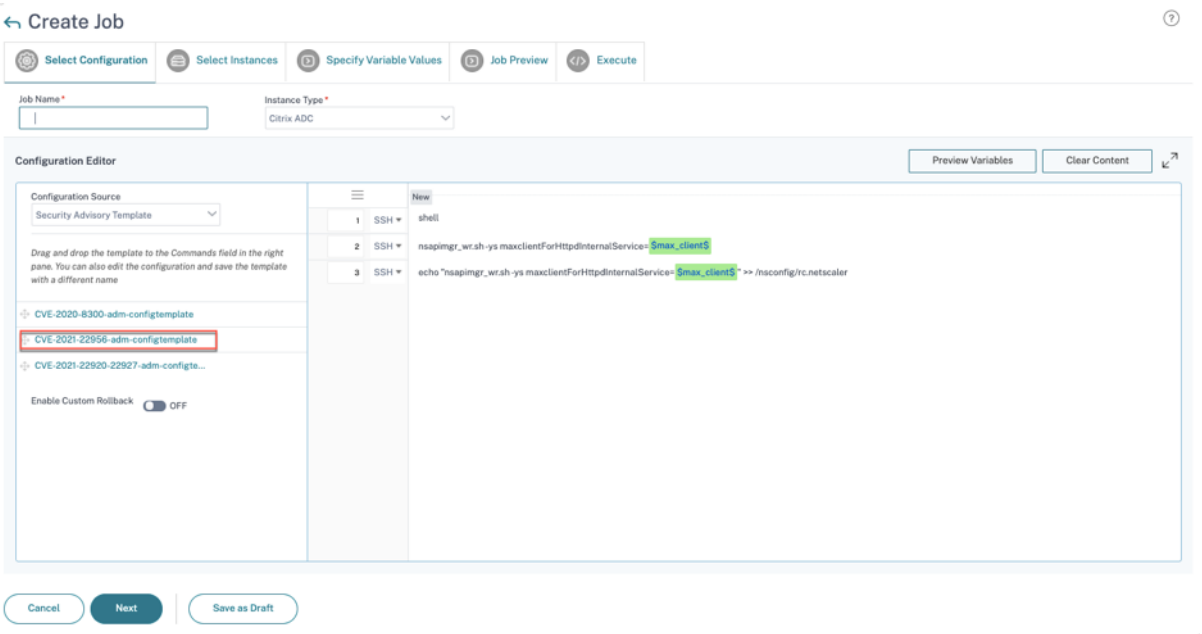
Tenga en cuenta los siguientes puntos antes de seleccionar una instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**:

- Para una instancia de ADC afectada por varios CVE (como CVE-2020-8300, CVE-2021-22927, CVE-2021-22920 y CVE-2021-22956): al seleccionar la instancia y hacer clic en **Continuar con el flujo de trabajo de configuración**, la plantilla de configuración integrada no se rellena automáticamente en Seleccionar configuración. Arrastre y suelte la plantilla de trabajo de configuración correspondiente en la sección **Plantilla de asesoramiento de seguridad** manualmente en el panel de tareas de configuración del lado derecho.
- Para varias instancias de ADC que se ven afectadas únicamente por el CVE-2021-22956: puede ejecutar trabajos de configuración en todas las instancias a la vez. Por ejemplo, tiene ADC 1, ADC 2 y ADC 3, y todos ellos se ven afectados únicamente por el CVE-2021-22956. Seleccione todas estas instancias y haga clic en **Continuar con el flujo de trabajo de configuración**, y la plantilla de configuración integrada se rellenará automáticamente en **Seleccionar configuración**. Consulte el problema conocido NSADM-80913 en las notas de la versión.
- Para varias instancias de ADC afectadas por CVE-2021-22956 y uno o más CVE (como CVE-2020-8300, CVE-2021-22927 y CVE-2021-22920), que requieren una corrección para aplicarla a cada ADC a la vez: al seleccionar estas instancias y hacer clic en **Continuar con el flujo de trabajo**

de configuración, se produce un error aparece un mensaje que le indica que ejecute el trabajo de configuración en cada ADC a la vez.

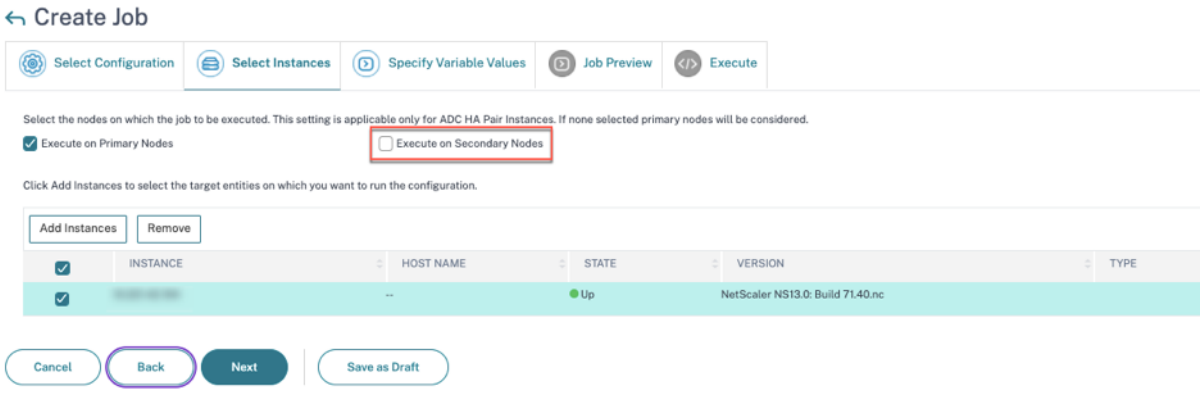
Paso 1: Seleccione la configuración

En el flujo de trabajo de configuración, la plantilla base de configuración integrada se rellena automáticamente en **Seleccionar configuración**.



Paso 2: selecciona la instancia

La instancia afectada se rellena automáticamente en **Seleccionar instancias**. Seleccione la instancia. Si esta instancia forma parte de un par de HA, seleccione **Ejecutar en nodos secundarios**. Haga clic en**Siguiente**.

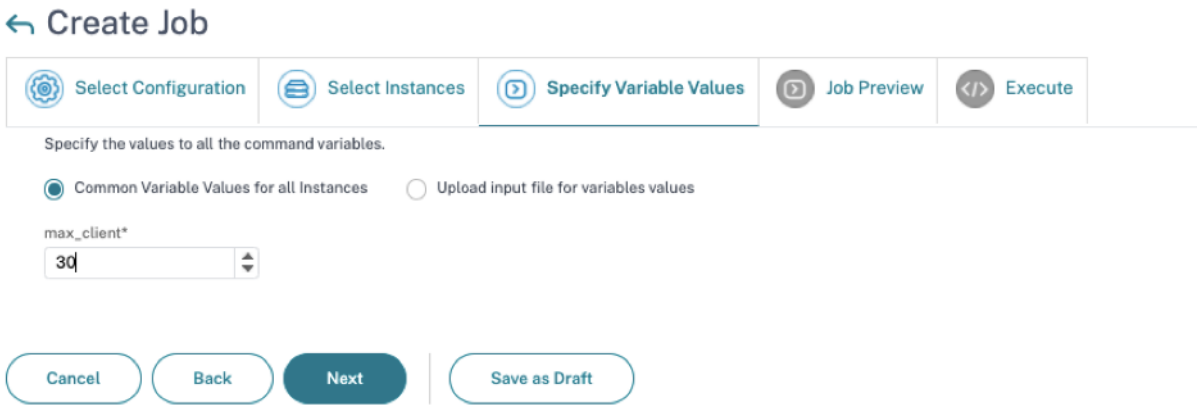


> **Nota**
>
> Para las instancias de ADC en modo clúster, mediante el asesoramiento de seguridad de ADM, ADM permite ejecutar el trabajo de configuración solo en el nodo del coordinador de configuración del clúster (CCO). Ejecute los comandos en nodos que no sean de CCO por separado.

`rc.netscaler` se sincroniza en todos los nodos de alta disponibilidad y del clúster, lo que hace que la corrección sea persistente después de cada reinicio.

Paso 3: especificar los valores de las variables

Introduzca los valores de las variables.



Selecciona una de las siguientes opciones para especificar las variables de tus instancias:

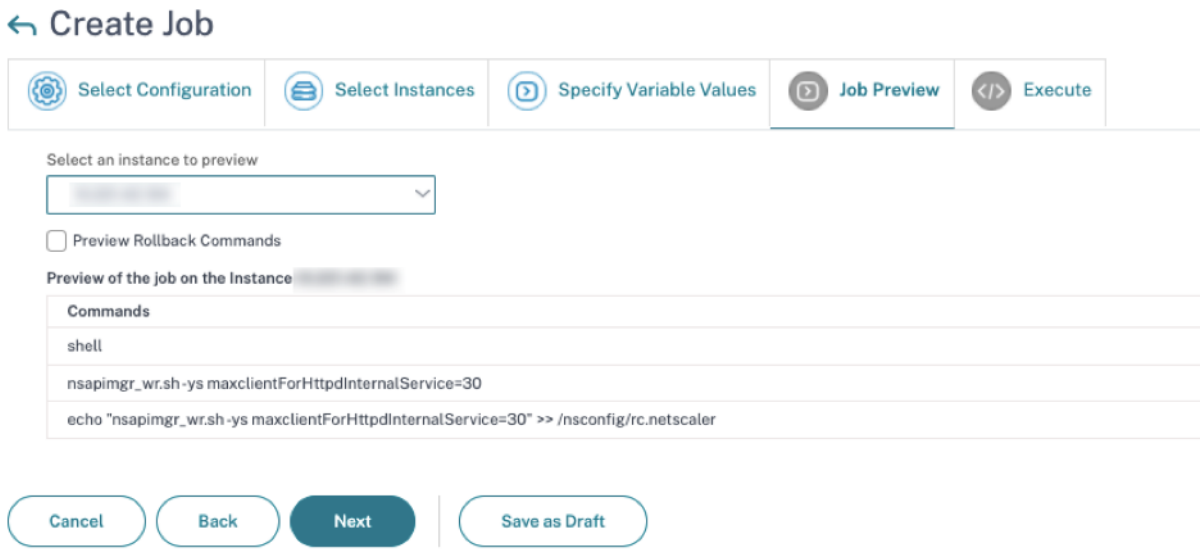
Valores de variables comunes para todas las instancias: introduzca un valor común para la variable `max_client`.

Cargar archivo de entrada para valores de variables: haga clic en **Descargar archivo de clave** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca los valores de la variable `max_client` y, a continuación, suba el archivo al servidor ADM. Consulte el problema conocido NSADM-80913 en las notas de la versión, notas sobre un problema relacionado con esta opción.

> **Nota**
>
> Para las dos opciones mencionadas anteriormente, el valor `max_client` recomendado es 30. Puede establecer el valor de acuerdo con su valor actual. Sin embargo, no debe ser cero y debe ser inferior o igual al conjunto max_client del archivo `/etc/httpd.conf`. Puede comprobar el conjunto de valores actuales en el archivo de configuración `/etc/httpd.conf` del servidor HTTP Apache buscando la cadena `MaxClients`, en la instancia de ADC.

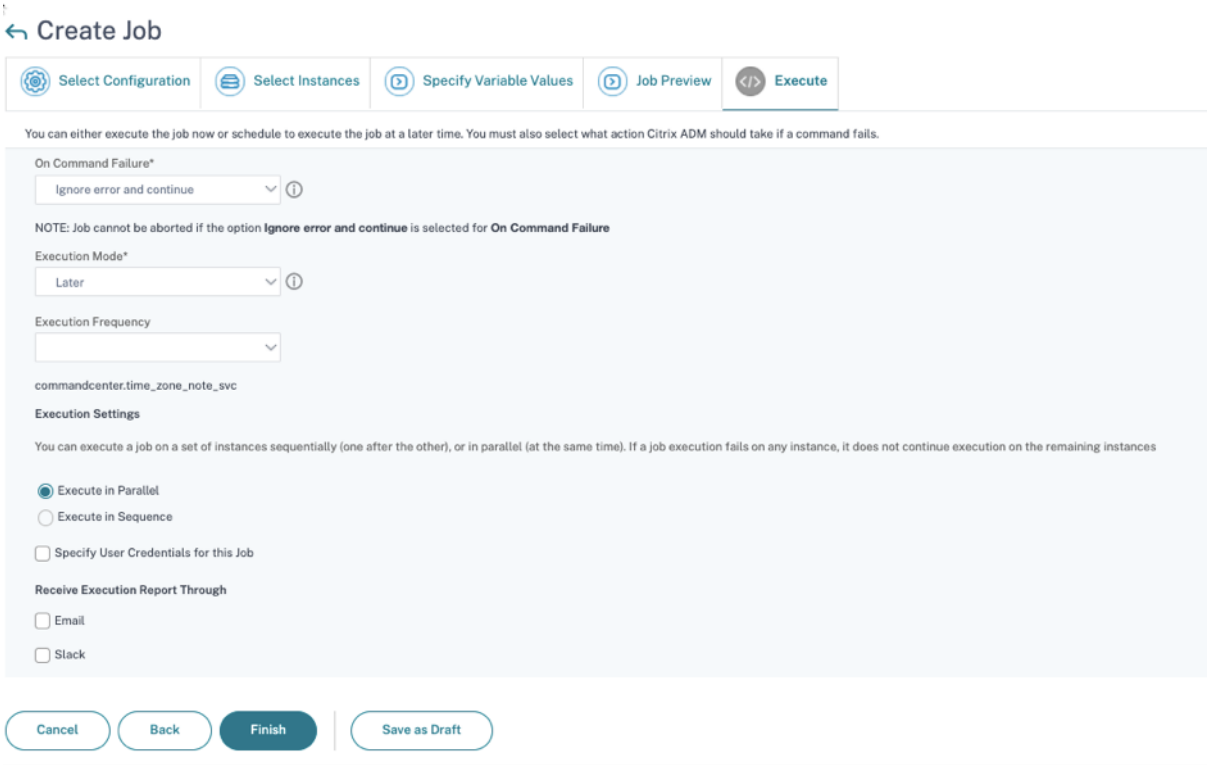
Paso 4: Vista previa de la configuración

Previsualiza los valores de las variables que se han insertado en la configuración y haga clic en **Siguiente**.



Paso 5: Ejecute el trabajo

Haga clic en **Finalizar** para ejecutar el trabajo de configuración.



Una vez ejecutado el trabajo, aparece en **Infraestructura > Configuración > Trabajos de configu-**

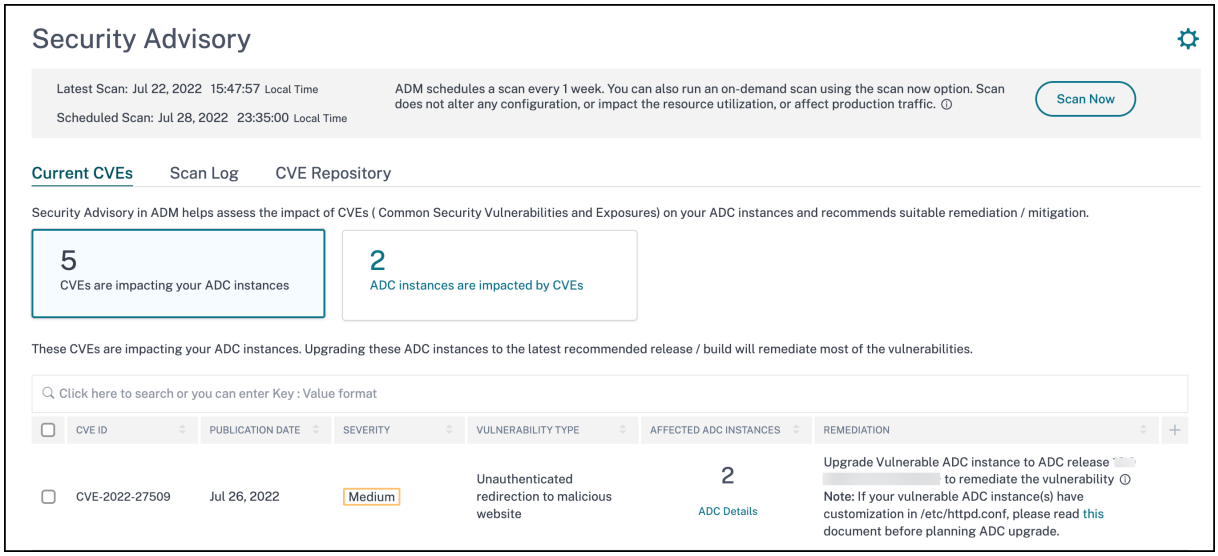
ración.

Tras completar los dos pasos de corrección para todos los ADC vulnerables, puede ejecutar un análisis bajo demanda para ver la postura de seguridad revisada.

Identificar y corregir las vulnerabilidades del CVE-2022-27509

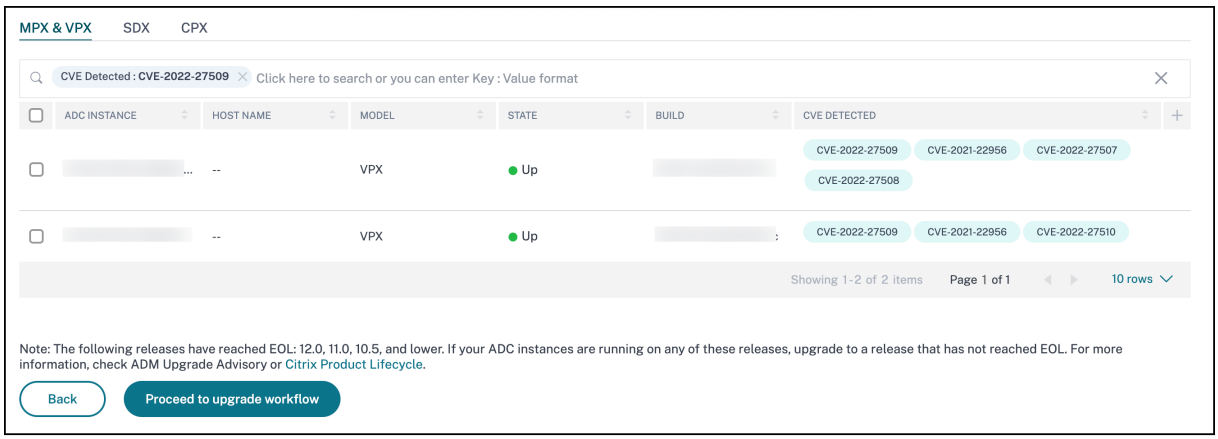
November 16, 2022

En el panel de consejos de seguridad de Citrix ADM, en **CVE actuales Las instancias de <number of> ADC se ven afectadas por las CVE**, puede ver todas las instancias vulnerables debido a CVE-2022-27509. Para comprobar los detalles de las instancias afectadas por los CVE, seleccione CVE-2022-27509 y haga clic en **Ver instancias afectadas**.



> **Nota**
>
> Para entender el motivo de la vulnerabilidad de ADC, descargue el informe CSV en la ficha Registros de escaneo del Aviso de seguridad.

Aparece la ventana **<number of>Instancias de ADC afectadas por los CVE**. En la siguiente captura de pantalla, puede ver el recuento y los detalles de las instancias de ADC afectadas por el CVE-2022-27509.



Para obtener más información sobre el panel de consejos de seguridad, consulte 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 del CVE-2022-27509 en el módulo de asesoramiento de seguridad. Para ver el impacto antes, inicie un análisis bajo demanda haciendo clic en **Escanear ahora**.

Identifique las instancias afectadas por el CVE-2022-27509

El CVE-2022-27509 requiere una combinación de escaneo personalizado y escaneo de versiones. Como parte del escaneo personalizado, el servicio ADM se conecta con la instancia de ADC administrada y envía un script a la instancia. El script se ejecuta en la instancia de ADC y determina si la instancia es vulnerable. Este script se ejecuta cada vez que se ejecuta el análisis programado o bajo demanda.

Una vez finalizado el escaneo, el script se elimina de la instancia de ADC.

También puede optar por no recibir estos escaneos personalizados de asesoramiento de seguridad. Para obtener más información sobre la configuración de escaneo personalizado y la inhabilitación de los escaneos personalizados, consulte la sección **Configurar la configuración del escaneo personalizado** en la página de **consejos de seguridad** .

Remediar CVE-2022-27509

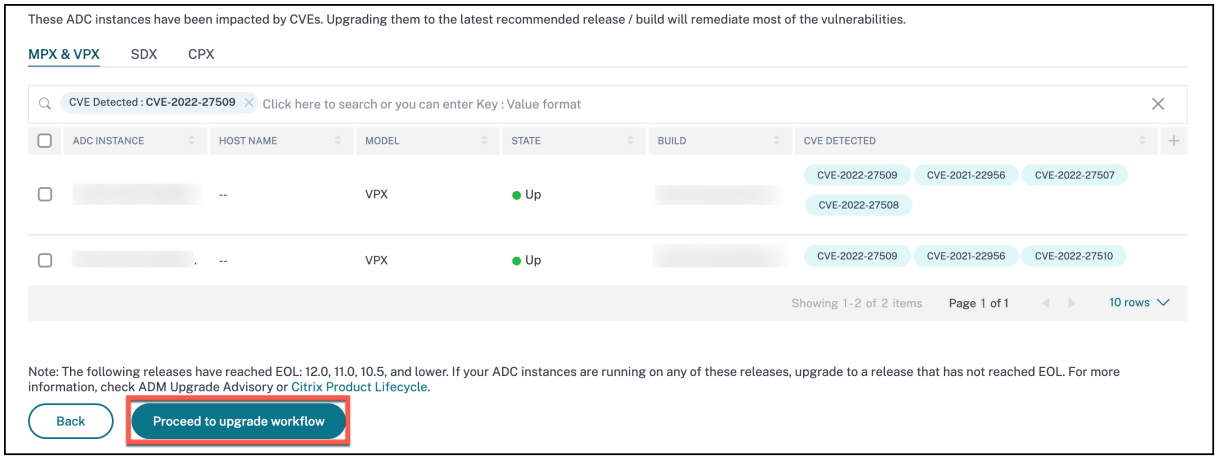
Para las instancias de ADC afectadas por el CVE-2022-27509, la corrección es un proceso de un solo paso y es necesario actualizar las instancias de ADC vulnerables a una versión y una compilación que tengan la solución. En la GUI, en los **CVE actuales > Las instancias de ADC se ven afectadas por las CVE**, puede ver el paso a seguir para solucionarlo.

En **CVE actuales > Instancias de ADC afectadas por las CVE**, verá el siguiente flujo de trabajo para este proceso de corrección de un solo paso, que es **Proceder a actualizar el flujo de trabajo**.

Para actualizar las instancias vulnerables, seleccione las instancias y haga clic en **Continuar para actualizar el flujo de trabajo**. El flujo de trabajo de actualización se abre con las instancias de ADC vulnerables ya ocupadas.

> **IMPORTANTE**
>
> Si sus instancias de ADC vulnerables tienen el archivo /etc/httpd.conf copiado al directorio /nsconfig, consulte Consideraciones de actualización para configuraciones de ADC personalizadas antes de planificar la actualización del ADC.

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



CVE no compatibles en el asesoramiento de seguridad

November 16, 2022

El asesoramiento de seguridad de Citrix ADM hace un seguimiento de todas las nuevas vulnerabilidades y exposiciones comunes (CVE) y evalúa el impacto de las CVE en la infraestructura. Puede revisar las recomendaciones y tomar las medidas adecuadas. Sin embargo, hay algunos CVE que no son compatibles y la detección y la corrección de las vulnerabilidades están fuera del alcance del asesoramiento de seguridad de Citrix ADM.

- **CVE-2022-21827**:

  El CVE-2022-21827 afecta al complemento de Citrix Gateway para las versiones compatibles con Windows anteriores a la 21.9.1.2.

  Citrix ADM no admite la detección y la corrección de las vulnerabilidades que afectan al complemento de Citrix Gateway para Windows. Además, las vulnerabilidades de los complementos de Citrix 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 Citrix Gateway para Windows implementada en el cliente.

Como resultado, la detección y la corrección de esta vulnerabilidad están fuera del alcance del asesoramiento de seguridad de Citrix ADM.

Configuración

November 16, 2022

Una vez finalizada la configuración inicial, debe configurar ciertos ajustes para empezar a administrar la implementación por completo.

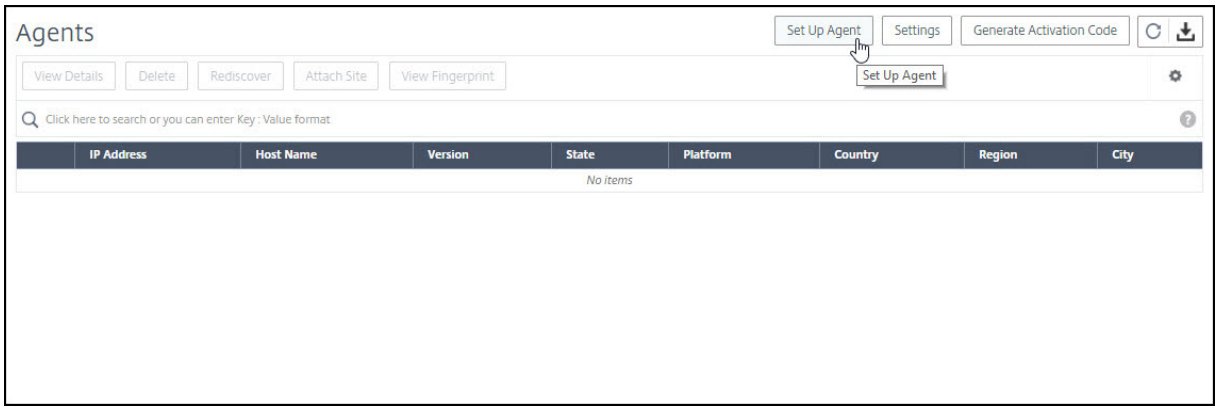
- Agregar varios agentes. La cantidad de agentes que se instalarán depende de la cantidad de instancias administradas en un centro de datos o en la nube y del rendimiento total. Citrix recomienda instalar al menos un agente por cada centro de datos.
- Agregar instancias. Puede agregar instancias al configurar Citrix ADM 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 aplicaciones, debe habilitar la función Analytics en los servidores virtuales que reciben tráfico para las aplicaciones específicas.
- Configurar syslog en las instancias. Puede supervisar los eventos de syslog generados en sus instancias de Citrix ADC si ha configurado su dispositivo para redirigir todos los mensajes de syslog a Citrix ADM. Para supervisar los eventos de syslog, primero debe configurar Citrix ADM como el servidor syslog de su instancia de Citrix ADC.
- Configuración del control de acceso basado en roles. Citrix ADM proporciona un control de acceso detallado y basado en roles (RBAC) con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales dentro 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

November 16, 2022

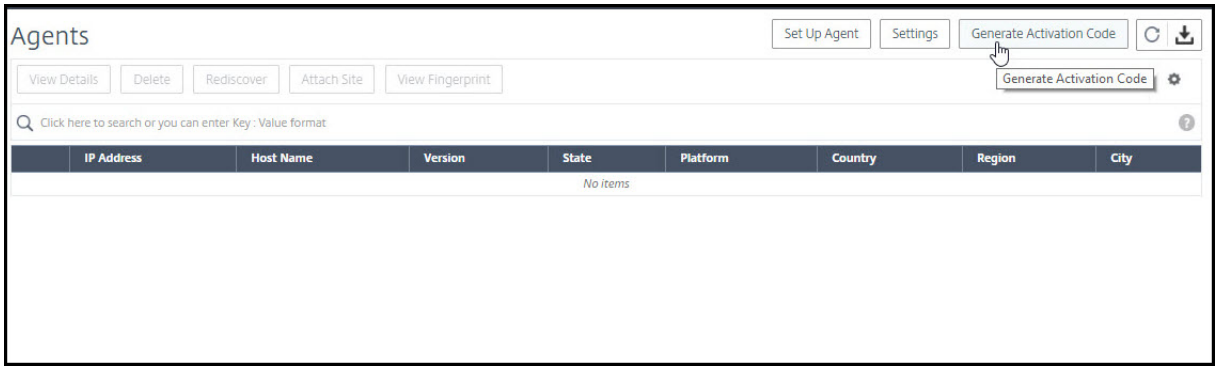
La cantidad de agentes que se instalarán depende de la cantidad de instancias administradas en un centro de datos y del rendimiento total. Citrix recomienda instalar al menos un agente por cada centro de datos.

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 de Citrix ADM 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 Instalación del agente Citrix ADM en Microsoft Azure Cloud.
> - Para obtener instrucciones sobre la instalación de un agente en AWS, consulte Instalación del agente Citrix ADM en AWS.

Configurar agentes para la implementación en varios sitios

November 16, 2022

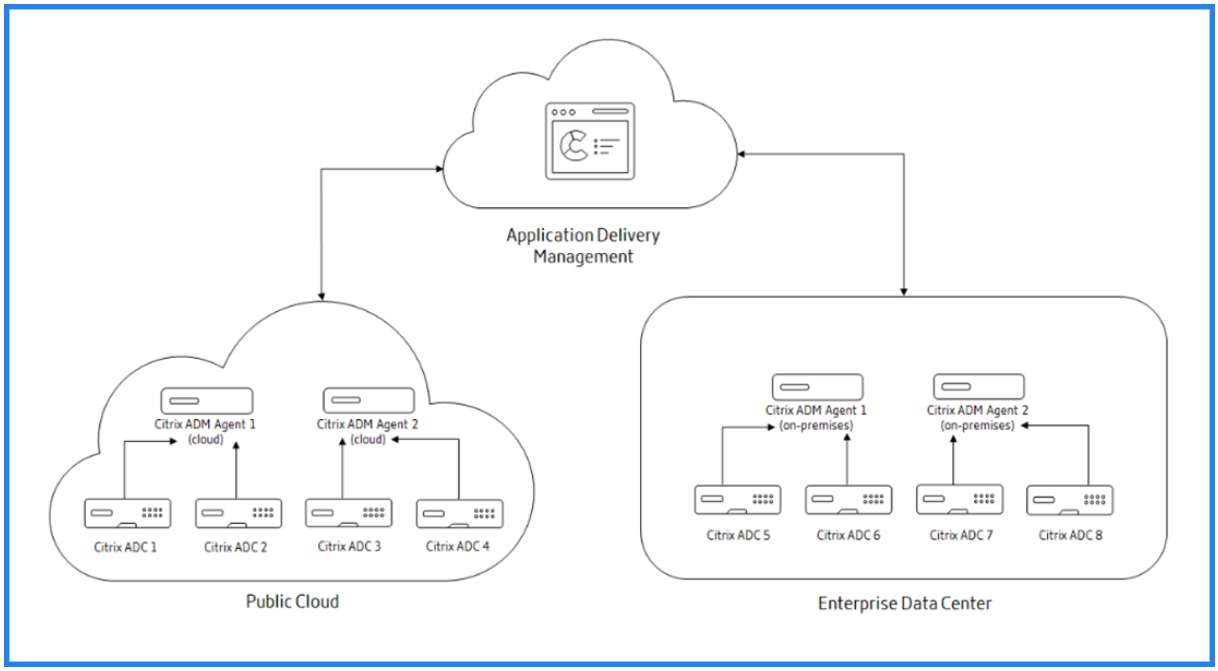
Los agentes trabajan como intermediarios entre el Citrix ADM y las instancias descubiertas en diferentes centros de datos y nubes públicas. Citrix ADM admite la conmutación por error de agentes dentro de un centro de datos o una nube pública.

Las ventajas de instalar agentes son las siguientes:

- Las instancias configuradas a un agente envían los datos sin procesar directamente al agente en lugar de a Citrix ADM. El agente realiza el primer nivel de procesamiento de datos y envía los datos procesados en formato comprimido a Citrix ADM 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 Citrix ADC en caso de conmutación por error del agente. Cuando un agente de un sitio falla, el tráfico de las instancias de Citrix ADC cambia a otro agente disponible en el mismo sitio.

Arquitectura

La siguiente figura ilustra las instancias de Citrix ADC 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 ADC y dos agentes Citrix ADM. El centro de datos empresarial también tiene cuatro instancias de ADC y dos agentes Citrix ADM. Cada agente está configurado con dos instancias de ADC.

Los agentes reciben datos directamente de las instancias configuradas. Una vez que el agente recibe los datos, los procesa y los envía al Citrix ADM en formato comprimido. Los agentes se comunican con el servidor Citrix ADM a través de un canal seguro.

En la nube pública, cuando el **agente Citrix ADM 1** pasa a estar inactivo (estado INACTIVO), se produce la conmutación por error del agente. Citrix ADM redistribuye las instancias de ADC del **agente 1 de Citrix ADM con el agente2 de Citrix ADM**. 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 Citrix ADM, consulte Instalar el agente Citrix ADM.

Failover de Citrix ADM Agent

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, Citrix ADM redistribuye las instancias de ADC del agente inactivo con otros agentes activos.

> **Importante**
>
> - La conmutación por error del agente de Citrix ADM no tiene en cuenta las instancias de 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 Cit-

> rix ADM.
>
> - Si un agente está ejecutando un script, asegúrese de que el script está presente en todos los agentes del sitio. Por lo tanto, el agente modificado puede ejecutar el script después de la conmutación por error del agente.

Para adjuntar un sitio a un agente en la GUI de Citrix ADM:

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 del agente, seleccione agentes Citrix ADM uno por uno y adjunte 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, Citrix ADM lo detecta y muestra el estado como inactivo.

Cuando un agente de Citrix ADM se vuelve inactivo (estado inactivo) en un sitio, Citrix ADM espera unos minutos a que el agente se active (estado Arriba). Si el agente permanece inactivo, Citrix ADM redistribuye automáticamente las instancias entre los agentes disponibles en el mismo sitio. Esta redistribución puede tardar aproximadamente 10-15 minutos.

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

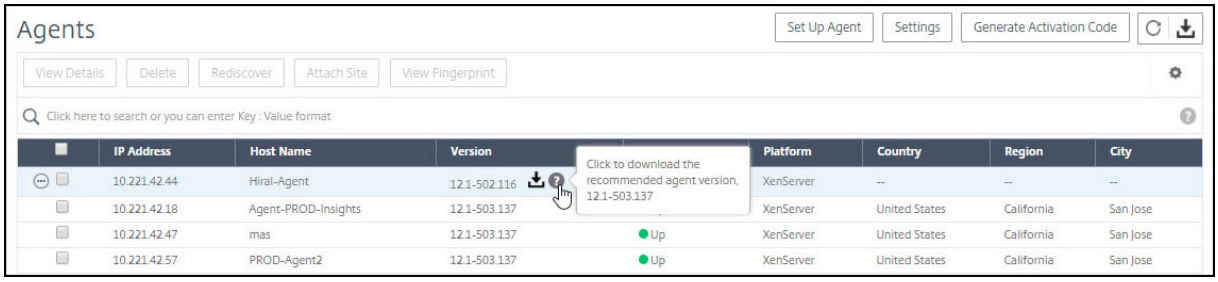
Las instancias conectadas y reconfiguradas automáticamente a los agentes del mismo sitio para destino de captura, servidor syslog y análisis.

Configuración de las opciones de actualización del agente

February 27, 2023

En Citrix ADM, Citrix ADM actualiza automáticamente los agentes que se ejecutan en la versión 12.0 del software, compilación 507.110 y posteriores, a las versiones más nuevas y recomendadas. 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**.



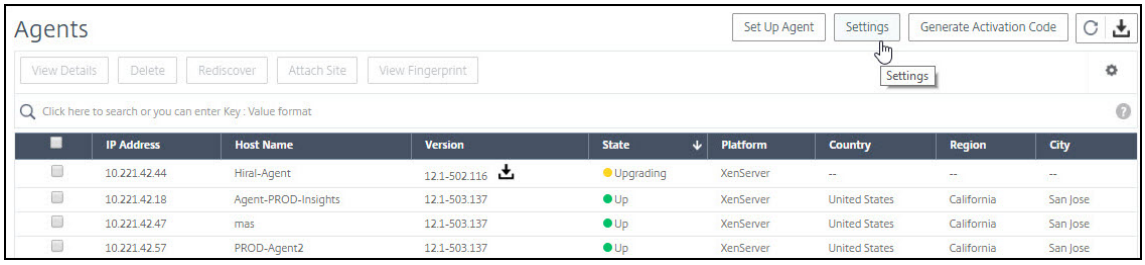
De forma predeterminada, un agente se actualiza automáticamente cuando hay una versión más reciente disponible. Sin embargo, puede especificar la hora a la que quiere que se realice la actualización del agente.

Si selecciona una hora específica, los agentes se actualizan a esa hora especificada, pero en la zona horaria en la que están desplegados sus 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 del agente.

   Puede optar por actualizar cuando haya una nueva imagen del agente disponible o puede establecer una hora específica en la que quiere que Citrix ADM actualice automáticamente el agente.

   > **Nota:**
   >
   > La hora que establezca utilizará la zona horaria que seleccionó en **Configuración global > Configuración del sistema**. Para obtener más información sobre la configuración de una zona horaria, consulte Configurar la zona horaria de Citrix ADM.

3. Haga clic en **Guardar** para guardar la configuración.

   Esta configuración persiste para futuras actualizaciones del agente hasta que cambie la configuración.

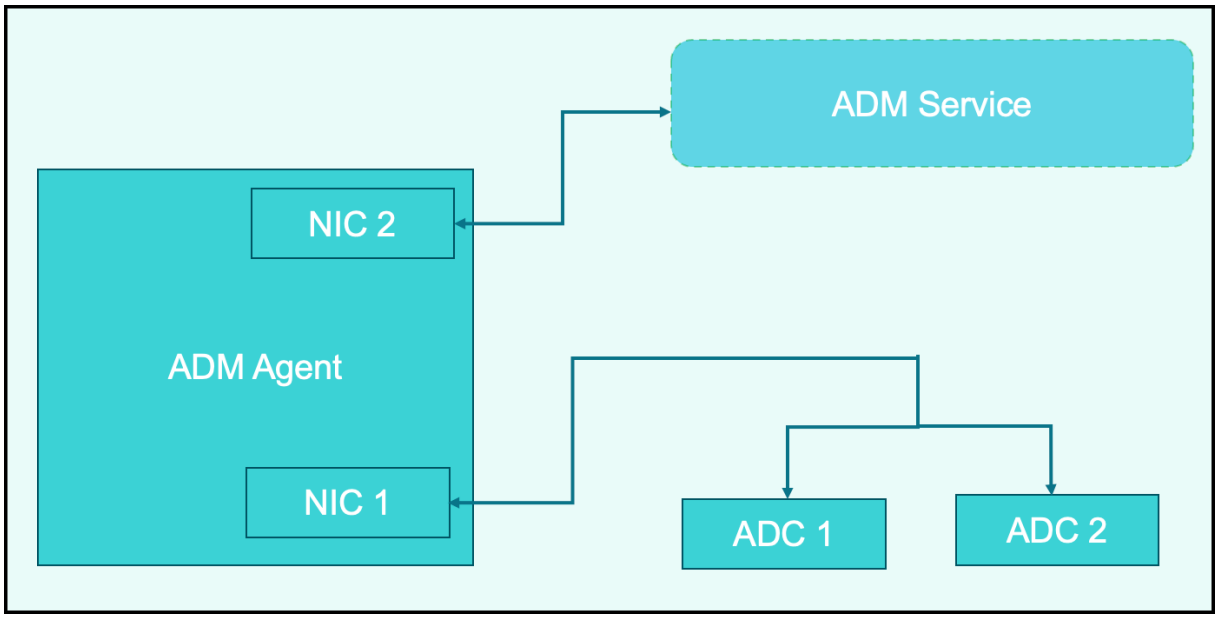
Soporte de NIC dual en Citrix ADM

November 16, 2022

Puede configurar dos NIC en un agente de ADM. Mediante la arquitectura de NIC dual, el agente ADM podrá:

- Establezca la comunicación entre el agente de ADM y las instancias de ADC: puede usar la primera NIC para aislar el tráfico que se recibe y envía a través del ADM de Citrix y también para comunicarse entre Citrix ADM y sus instancias de Citrix ADC administradas en otra red.
- Establecer la comunicación entre el agente de ADM y el servicio de ADM: puede usar la segunda NIC para administrar el servicio de ADM que se encuentra en una red y realizar tareas administrativas.

> **Nota**
>
> No puede intercambiar la funcionalidad y la configuración de ambas NICS.



En este escenario, como administrador, puede:

- Configure la dirección IP para el tráfico entre Citrix ADM y sus instancias de Citrix ADC administradas.
- Configure la dirección IP para administrar el software Citrix ADM para realizar todas las tareas administrativas del software.

> **Nota**
>
> No es obligatorio configurar dos NIC para un agente de ADM. Es opcional y solo se requiere

> cuando es necesario separar el tráfico entre el agente ADM, el servicio ADM y los ADC.

Requisitos previos

- Asegúrese de haber implementado y configurado el agente Citrix ADM 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).

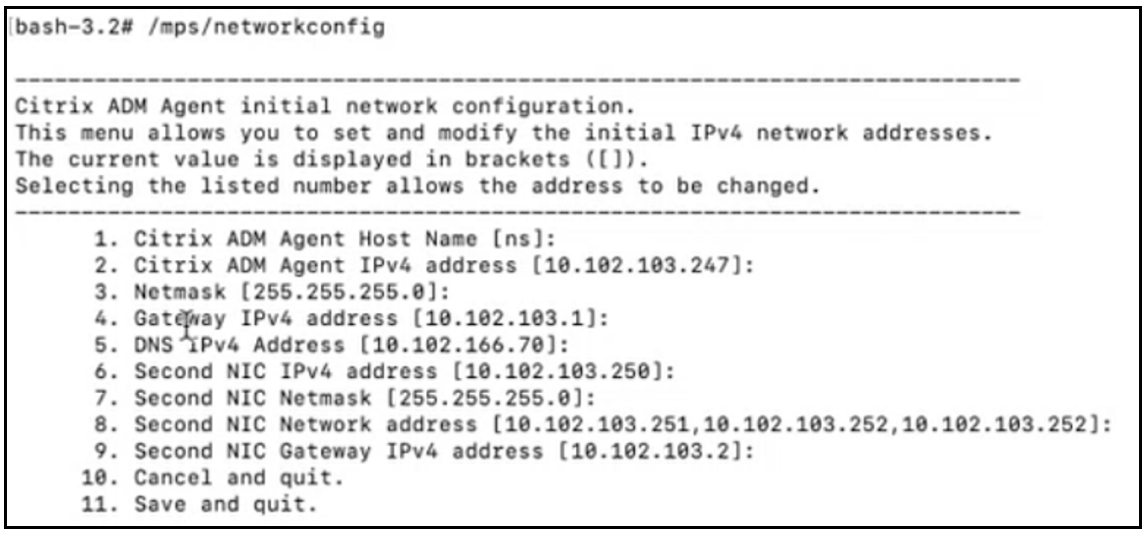
Para asignar una dirección IP a una NIC en un hipervisor de Citrix y crear una interfaz secundaria, consulte Asignar una dirección IP a una NIC.

Modificar las direcciones de red de la NIC IPV4

1. Abra una conexión SSH a la consola del agente Citrix ADM mediante un cliente SSH, como PuTTY.
2. Inicie sesión con las credenciales de **nsrecover/nsroot** y cambie a la línea de comandos de la consola.
3. Ejecute el comando **ifconfig**. Puede ver los detalles de las dos NIC que ha configurado:
   - NIC 1: para la comunicación entre el agente de ADM y la comunicación de ADC
   - NIC 2: para la comunicación entre el agente ADM y el servicio ADM

```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. Ejecute el comando **networkconfig**. Aparece un menú que le permite configurar o modificar las direcciones de red IPV4.



> **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

December 2, 2022

Puede agregar instancias al configurar Citrix ADM por primera vez o más adelante.

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

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix Secure Web Gateway

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

Especifique un perfil de instancia que Citrix ADM pueda utilizar 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 Citrix ADC. Las credenciales predeterminadas de administrador de Citrix ADC 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 Citrix ADC desde Citrix ADM después de agregar las instancias en Citrix ADM. Para acceder a las instancias de Citrix ADC desde Citrix ADM, debe estar conectado a la red Citrix.

> **Nota**
>
> - Para agregar instancias de Citrix ADC 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 Citrix ADM, la dirección IP del clúster representa el clúster.
> - Para las instancias de Citrix ADC configuradas como un par HA, al agregar una instancia, la otra instancia del par se agrega automáticamente.
> - Para asegurarse de que el usuario de Citrix ADC tiene todos los privilegios, asigne permisos de superusuario al usuario en Citrix ADC. Para obtener más información, consulte Usuarios, grupos de usuarios y políticas de comandos

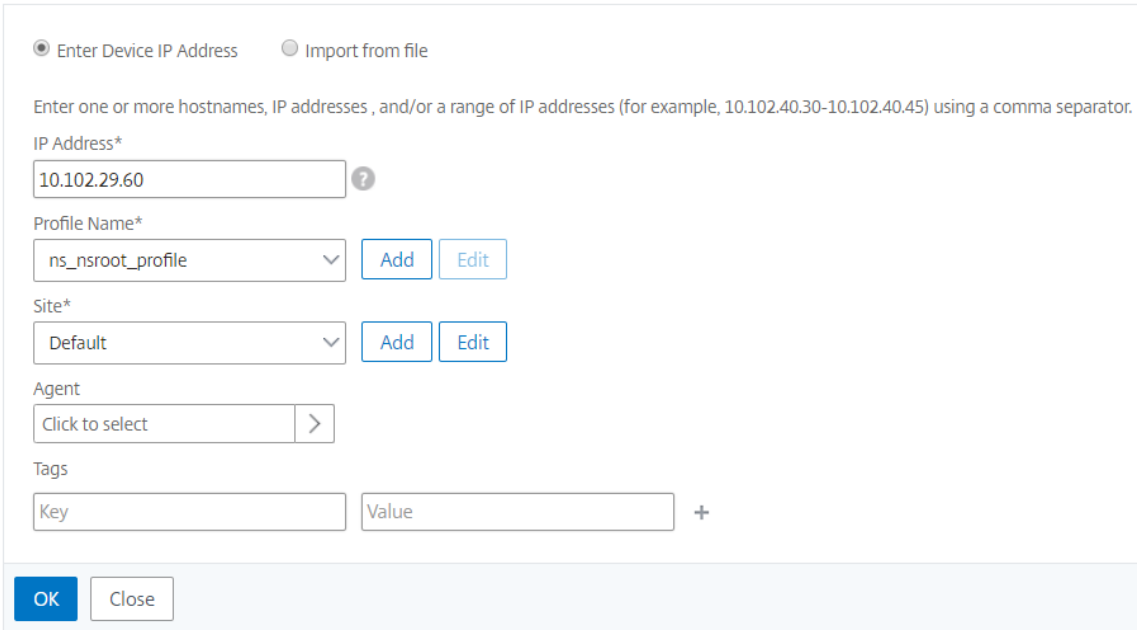
Para agregar una instancia de Citrix ADC a Citrix ADM

> **Nota**
>
> Realice esta tarea para agregar todas las demás instancias de ADC, excepto la instancia CPX de ADC.

1. Vaya a **Infraestructura > Instancias > Citrix ADC**. En Instancias, seleccione el tipo de instancia que quiere agregar (por ejemplo, Citrix ADC VPX) y haga clic en **Agregar**.
2. Seleccione una de estas opciones:
   - **Introduzca la dirección IP del dispositivo** : para las instancias de Citrix ADC, especifique el nombre de host o la dirección IP de cada instancia, o un rango de direcciones IP.
   - **Importar desde archivo**: Desde su sistema local, cargue un archivo de texto que contenga las direcciones IP de todas las instancias que quiera 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 su Citrix ADM, ese agente se selecciona de forma predeterminada.



Para agregar una instancia de Citrix ADC CPX en Citrix ADM

1. Vaya a **Infraestructura > Instancias**. En **Instancias**, seleccione **Citrix ADC** 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 Citrix ADC (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 Citrix ADM de la lista de agentes.
9. Haga clic en **Aceptar** para iniciar el proceso de agregar instancias a Citrix ADM.

> **Nota**
>
> Si quiere volver a descubrir una instancia, lleve a cabo los siguientes pasos:
>
> a) Vaya a **Infraestructura > Instancias > Citrix ADC** > **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 Citrix ADC BLX independiente en Citrix ADM

Una instancia independiente de Citrix ADC BLX es una instancia única que se ejecuta en el servidor host Linux dedicado.

1. Vaya a **Infraestructura > Instancias > Citrix ADC**.
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.

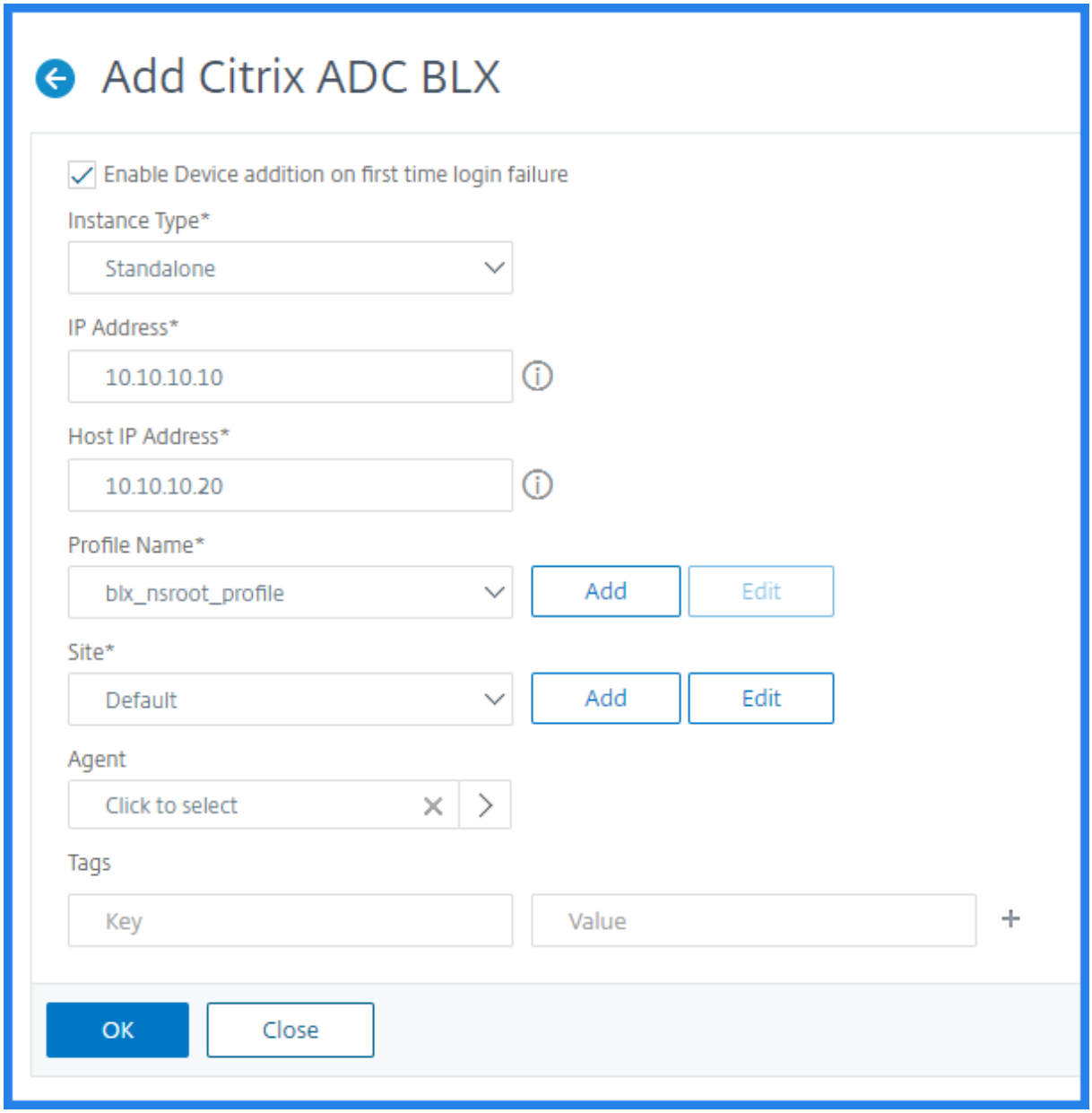
8. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

   Si quieres agregar un sitio, haga clic en **Agregar**.

9. En la lista de **agentes**, seleccione el agente Citrix ADM al que quiere asociar la instancia.

   Si solo hay un agente configurado en su Citrix ADM, ese agente se selecciona de forma predeterminada.

10. Haga clic en **Aceptar**.



Para agregar instancias de Citrix ADC BLX de alta disponibilidad en Citrix ADM

Las instancias de Citrix ADC 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.

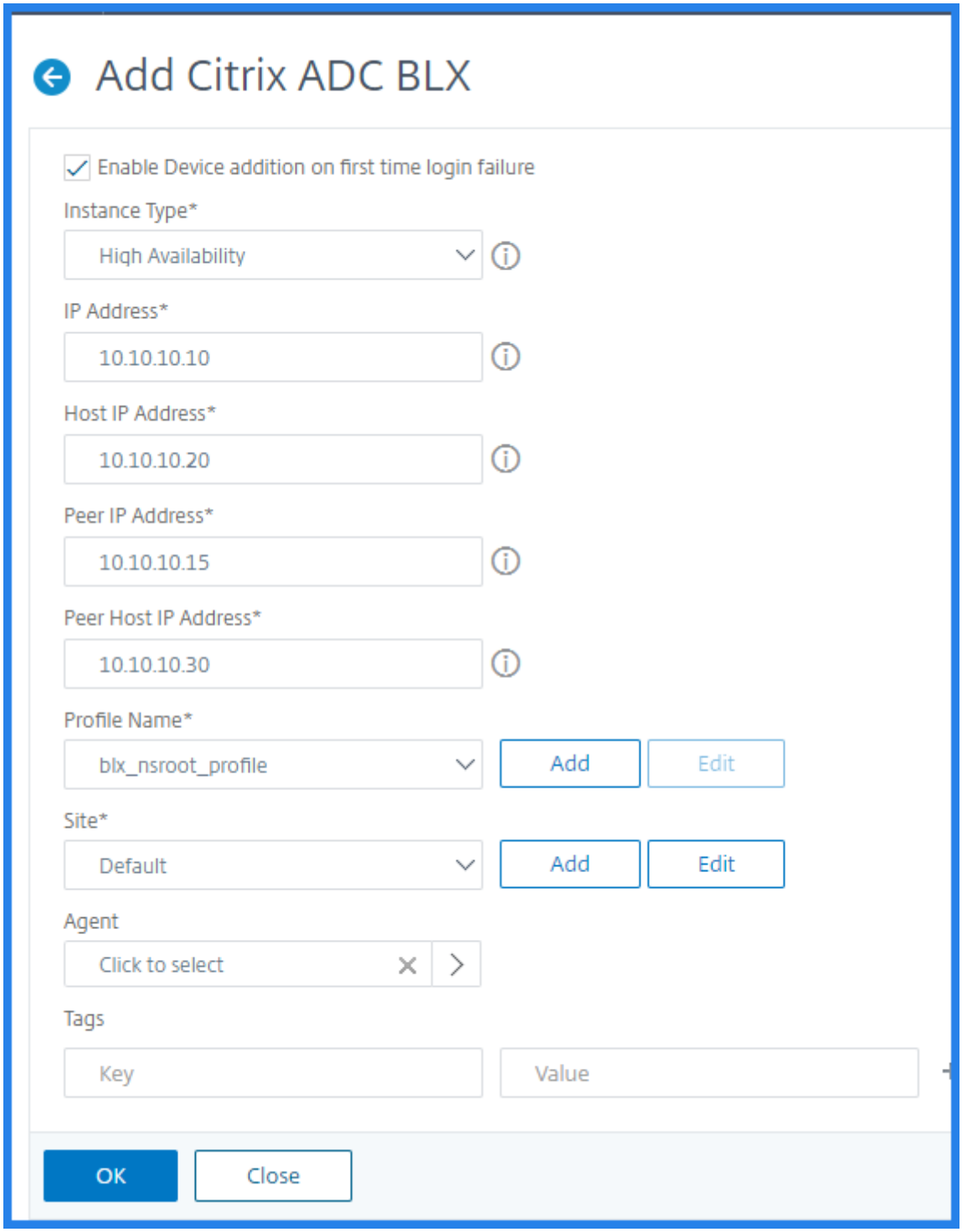
9. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

   Si quieres agregar un sitio, haga clic en **Agregar**.

10. En la lista de **agentes**, seleccione el agente Citrix ADM al que quiere asociar la instancia.

    Si solo hay un agente configurado en su Citrix ADM, ese agente se selecciona de forma predeterminada.

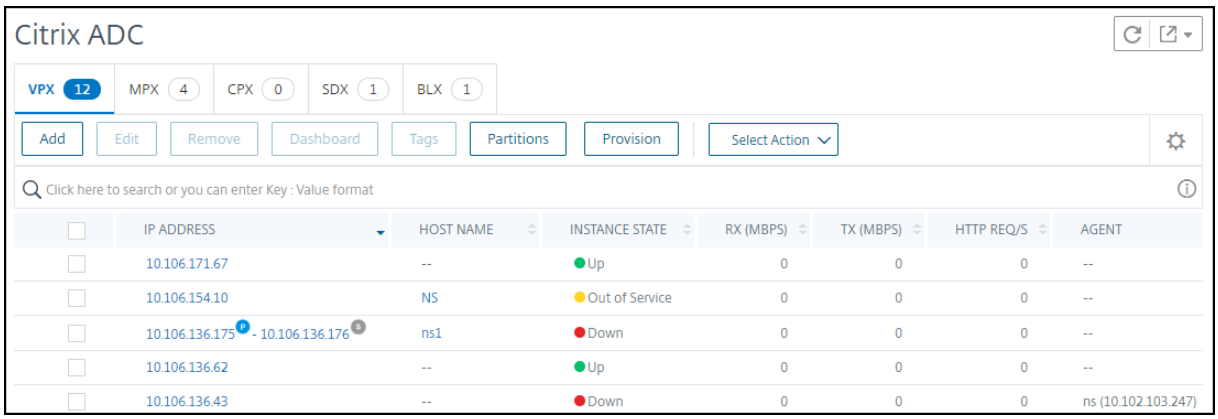
11. Haga clic en **Aceptar**.



Para acceder a la GUI de una instancia desde Citrix ADM

1. Vaya a **Infraestructura > Instancias** > **Citrix ADC**.
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 Citrix ADC 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 Citrix ADM.

  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 utiliza sólo una conexión HTTPS, aplique licencia a una instancia desde la GUI de ADC.

Configuración de syslog en instancias

November 16, 2022

El protocolo syslog proporciona un transporte que permite a las instancias de Citrix ADC enviar mensajes de notificación de eventos a Citrix ADM, que está configurado como recopilador o servidor syslog para estos mensajes.

Puede supervisar los eventos de syslog generados en sus instancias de Citrix ADC si ha configurado su dispositivo para redirigir todos los mensajes de syslog a Citrix ADM. Para supervisar los eventos de syslog, primero debe configurar Citrix ADM como el servidor syslog de su instancia de Citrix ADC. Una vez configurada la instancia, todos los mensajes de syslog se redirigen a Citrix ADM, de modo 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 Citrix ADM, debe configurar los niveles de gravedad de las instalaciones y los registros en 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.

```



```
15   8 - Debug: Debug-level messages.
```

Para configurar syslog en instancias de Citrix ADC:

1. En Citrix ADM, vaya a **Infraestructura > Instancias**.
2. Seleccione la instancia de Citrix ADC desde la que quiere que se recopilen y muestren los mensajes syslog en Citrix ADM.
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 **Aceptar**.

Esto configura todos los comandos de syslog en la instancia de Citrix ADC y Citrix ADM comienza a recibir los mensajes de syslog. Para ver los mensajes, vaya a **Infraestructura > Eventos > Mensajes de Syslog**.

Visión general de Logstream

November 16, 2022

Las instancias Citrix ADC generan registros de AppFlow y son un punto central de control para todo el tráfico de aplicaciones en el centro de datos. **IPFIX** y **Logstream** son los protocolos que transportan estos registros de AppFlow desde las instancias de Citrix ADC a Citrix ADM. Para obtener más información, consulte AppFlow.

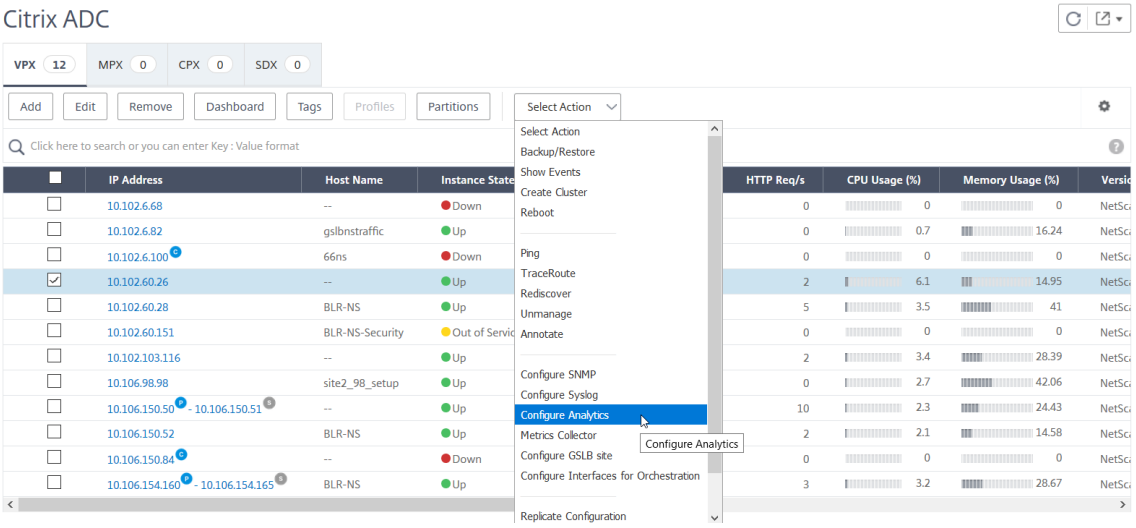
- **IPFIX** es un estándar abierto del Grupo de Trabajo de Ingeniería de Internet (IETF) definido en el RFC 5101. **IPFIX** utiliza el protocolo UDP que es un protocolo de transporte poco confiable utilizado para el flujo de datos en una dirección. Dado que IPFIX utiliza el protocolo UDP, la adhesión al estándar IPFIX permite procesar más recursos en Citrix ADM.
- **Logstream** es un protocolo propiedad de Citrix que se utiliza como uno de los modos de transporte para transferir eficientemente los datos de registro de análisis de las instancias de Citrix ADC a Citrix ADM. **Logstream** utiliza un protocolo TCP confiable y requiere menos recursos para procesar los datos.

Para Citrix ADC entre la versión **11.1 de la compilación 47.14 y la 11.1 de la 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 datos. Para la versión Citrix ADC desde la **12.0 hasta la versión más reciente**, puede seleccionar **Logstream** o **IPFIX** como modo de transporte.

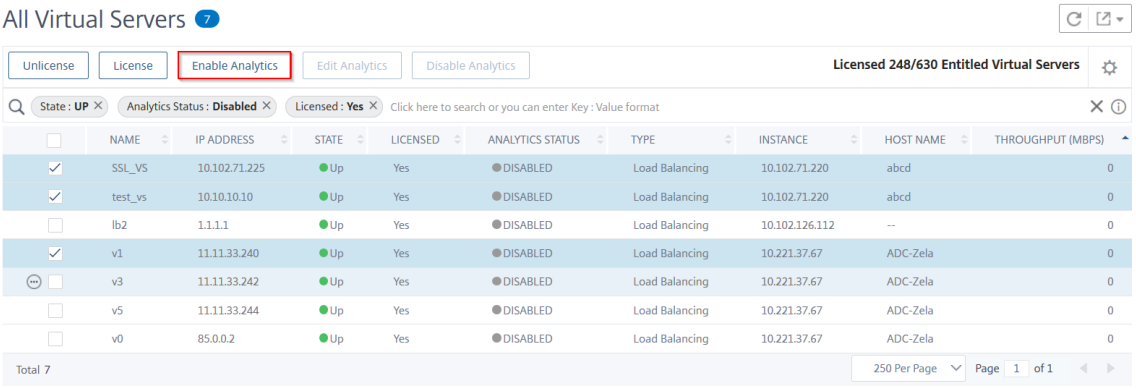
> **Nota**
>
> La versión y compilación de Citrix ADM deben ser **iguales o superiores a** la versión y compilación de Citrix ADC. Por ejemplo, si ha instalado Citrix ADC 12.1 Build 50.28/50.31, asegúrese de haber instalado Citrix ADM 12.1 Build 50.39 o posterior.

Habilitar Logstream como modo de transporte

1. Vaya a **Infraestructura > Instancias**y seleccione la instancia de ADC en la que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.



3. Seleccione los servidores virtuales y, a continuación, haga clic en **Habilitar análisis**.

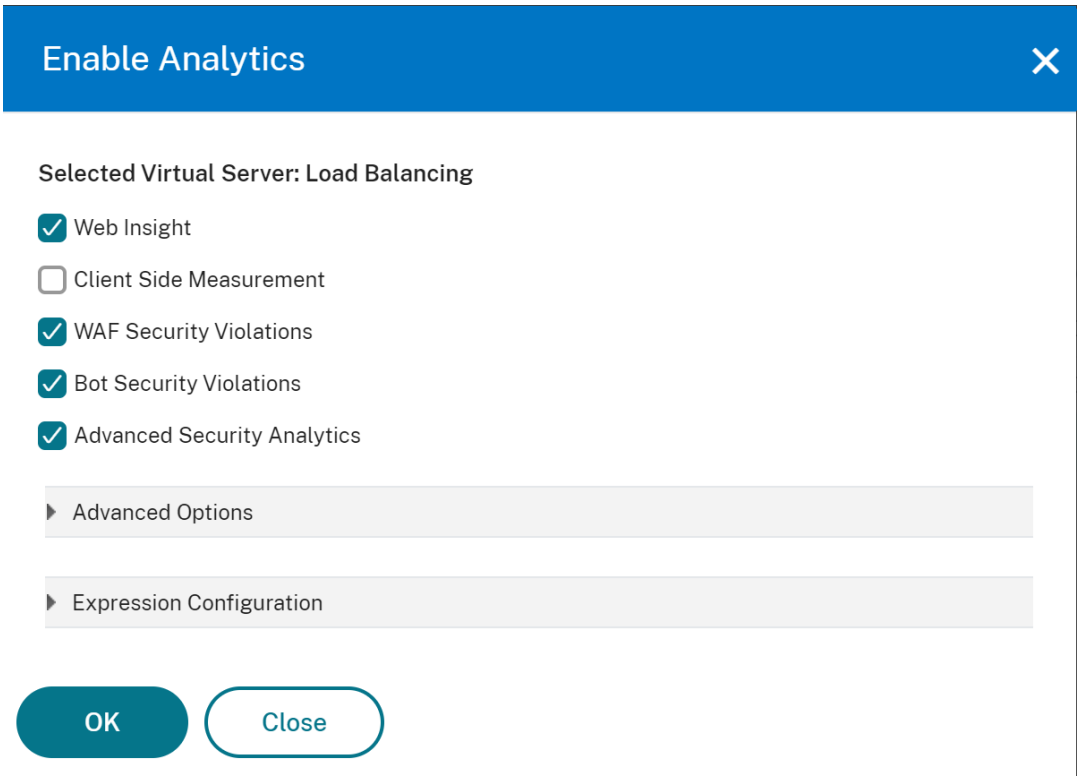


4. En la ventana **Habilitar análisis**:
   a) Seleccione los tipos de información (violaciones de seguridad de Web Insight o WAF o infracciones de seguridad de bots)
   b) Seleccionar **flujo logstream** como modo de transporte

> **Nota**
>
> Para Citrix ADC entre la versión **11.1 de la compilación 47.14 y la 11.1 de la 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 datos. Para la versión Citrix ADC 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 **OK**.



> **Nota**
>
> - Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
> - Para particiones de administración, solo se admite **Web Insight**
> - Para servidores virtuales como Redirección de caché, Autenticación y GSLB, no puede habilitar el análisis. Aparece un mensaje de error.

En la siguiente tabla se describen las funciones de Citrix ADM que admiten **Logstream** como modo de transporte:

Función	**IPFIX**	**Flujo de registro**
Información web	•	•
Infracciones a la seguridad	No se admite	•
Infracciones de seguridad de WAF	•	•
Gateway Insight	•	•
HDX Insight	•	•
Insight SSL	No se admite	•
CR Insight	•	•
Reputación IP	•	•
AppFirewall	•	•
Medición del lado del	•	•
Syslog/Auditlog	•	•

Cómo asignar más permisos a usuarios administradores delegados

November 16, 2022

Cuando el primer usuario de la organización se registra e inicia sesión en Citrix ADM, a este usuario se le asignan 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.

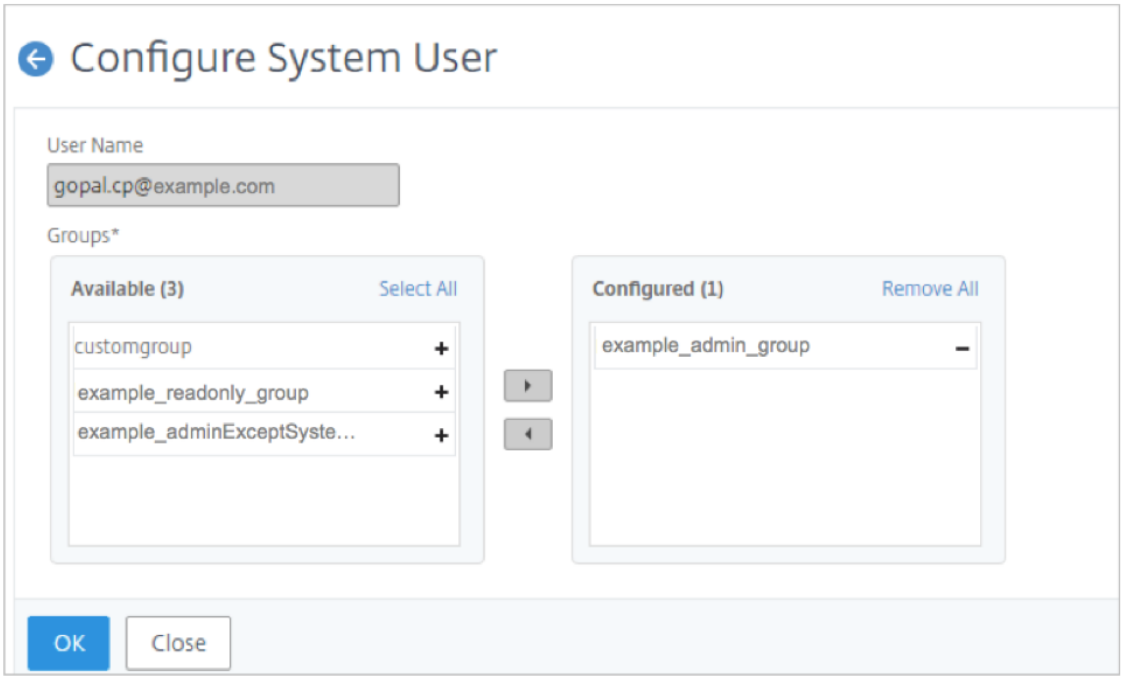
Sin embargo, puede asignar privilegios de superadministrador o roles específicos no superadministradores a un administrador delegado para que el administrador pueda realizar tareas relacionadas con la administración de usuarios.

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:

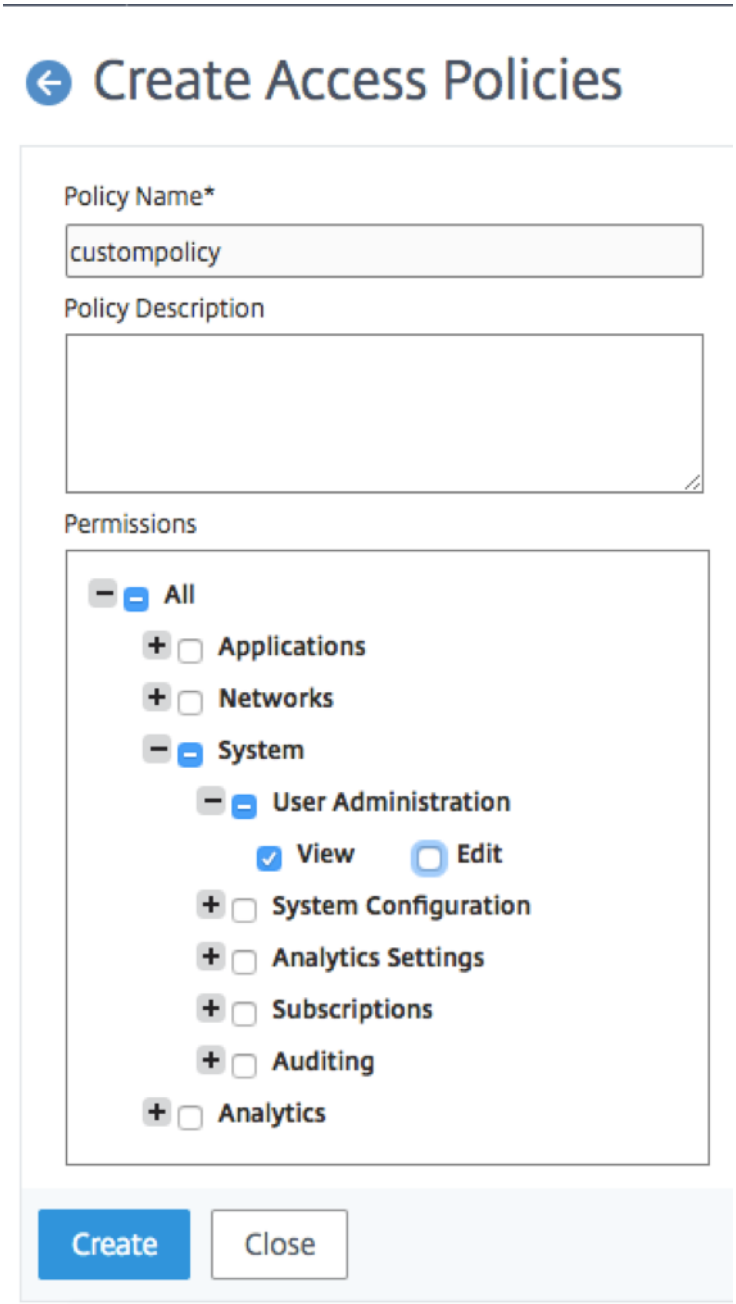
1. Inicie sesión en Citrix ADM como superadministrador.
2. Vaya a **Cuenta** > **Administración** de **usuarios > Usuarios**.
3. Seleccione el nombre de usuario del administrador delegado y haga clic en **Modificar**.
4. Asigne el grupo ***<arrendatario_name>*_admin_group** al administrador delegado y haga clic en **Aceptar**. Por ejemplo, en la siguiente imagen, «example_admin_group» se asigna a un usuario administrador delegado.



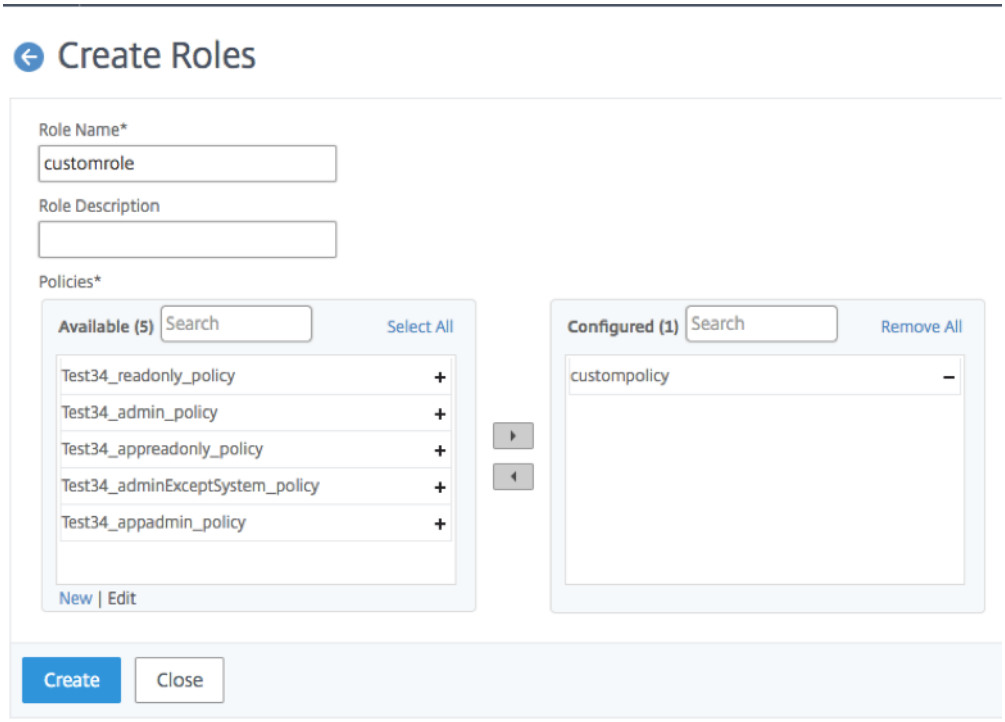
Asignación de rol personalizado a un administrador delegado

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:

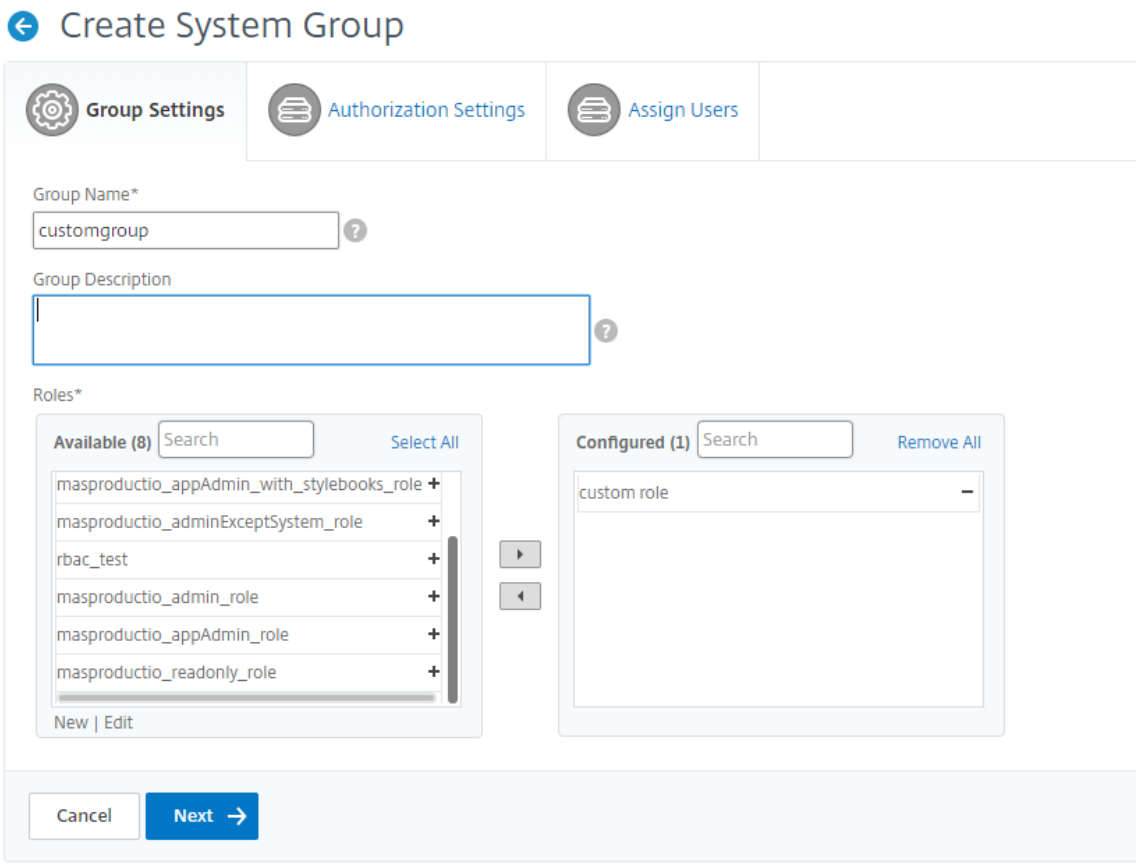
1. Inicie sesión en Citrix ADM como superadministrador.
2. Vaya a **Cuenta** > **Administración de usuarios** > **Directivas de acceso**. Seleccione **Agregar** para crear una directiva de acceso con los permisos necesarios para el administrador delegado. En este ejemplo, `custompolicy` se crea una directiva de acceso que permite el acceso de vista a la configuración de Administración de usuarios.



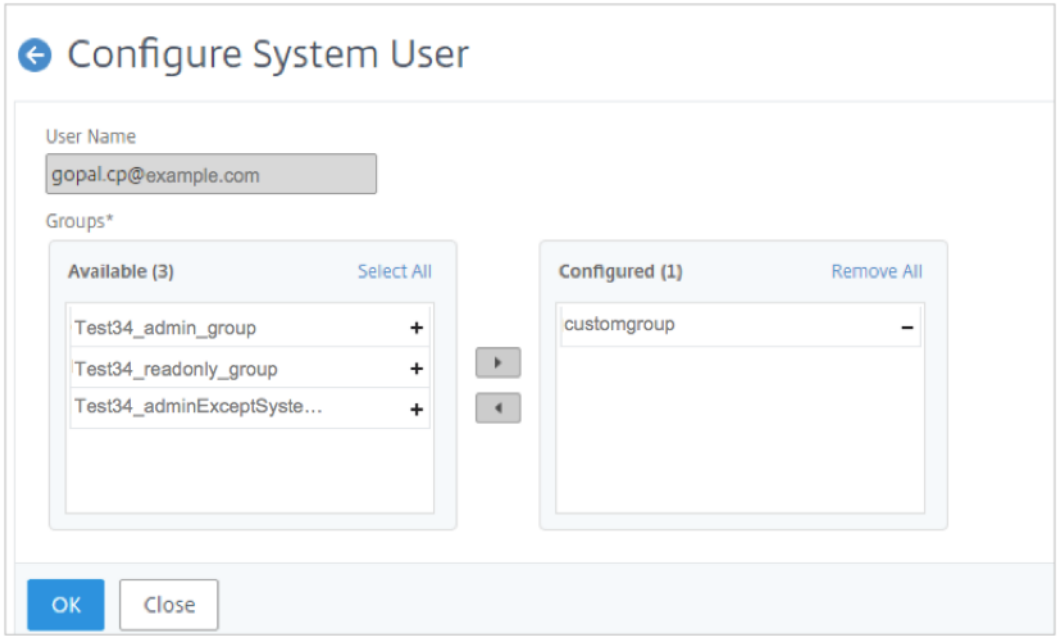
3. Acceda a **Cuenta** > **Administración de usuarios** > **Roles**. Seleccione **Agregar** para crear un rol y enlazar este rol a la directiva de acceso que creó en el paso anterior. En este ejemplo, `customrole` se crea un rol y se enlazado a la directiva de `custompolicy` acceso.



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

November 16, 2022

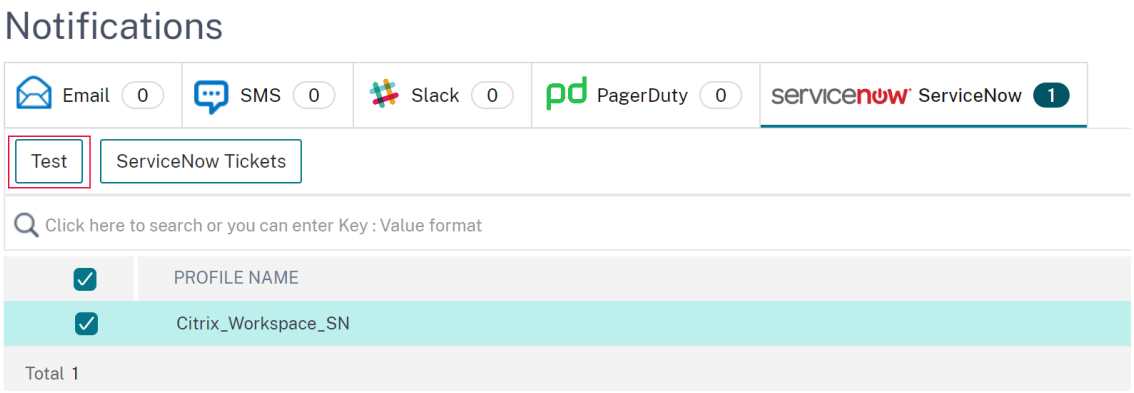
Como administrador de Citrix ADC, puede utilizar ServiceNow como el principal sistema de soporte y solicitudes de TI. Debe generar tickets o incidentes para los eventos críticos del ADC para investigarlos, rastrearlos y solucionarlos.

Puede automatizar la creación de tickets en ServiceNow mediante Citrix ADM y el conector Citrix ITSM para ServiceNow. Para iniciar esta automatización, incorpore el servicio de adaptador ITSM de Citrix para recibir eventos de ADM 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 correcta, configure los incidentes de ServiceNow generados automáticamente en Citrix ADM. Siga los pasos para verificar si los tickets de ServiceNow se generan automáticamente.

1. Inicie sesión en Citrix ADM.
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 quiere ver los tickets de ServiceNow en la GUI de Citrix ADM, seleccione **ServiceNow Tickets**.



Al integrar Citrix ADM con ServiceNow, puede automatizar la generación de incidentes de ServiceNow para lo siguiente:

- Cualquier evento de Citrix ADC
- Certificados SSL que están a punto de caducar
- Eventos de caducidad de la licencia ADM

Además, también puede personalizar las directivas de eventos de ADM.

Genere incidentes de ServiceNow para cualquier evento de Citrix ADC

En Citrix ADM, puede configurar reglas para generar automáticamente un ticket en ServiceNow para eventos específicos. Citrix ADM 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 ADC.

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.

Puede crear una regla de eventos en Citrix ADM yendo 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 ADC está a punto de caducar, Citrix ADM 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 por caducidad de la licencia ADM

En Citrix ADM, puede configurar las reglas para que generen automáticamente un ticket en ServiceNow para eventos específicos de caducidad de licencias de ADM.

Para enviar notificaciones de ServiceNow sobre el vencimiento de una licencia ADM, consulte Vencimiento de la licencia ADM.

Personalizar directivas de eventos de ADM

Puede definir directivas para controlar la forma en que ServiceNow procesa los eventos de ADM en función de los atributos de los eventos. Configure las directivas de eventos de ADM 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 directivas de eventos de ADM.

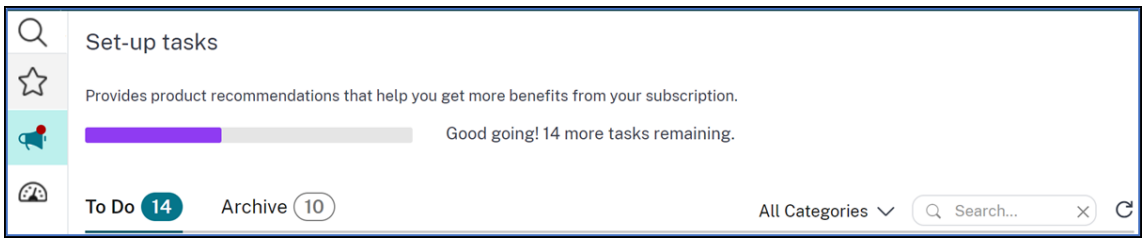
Vea las recomendaciones y administre sus ADC y aplicaciones de manera eficiente

February 27, 2023

Es posible que haya descubierto cientos de instancias de Citrix ADC y haya configurado varios servidores virtuales (aplicaciones) desde cada instancia de ADC. Como administrador, debe asegurarse de que todas las instancias de Citrix ADC y sus aplicaciones se administren de manera eficiente para obtener información que permita priorizar mejor y solucionar problemas.

A medida que amplíe más su infraestructura, es posible que también deba centrarse en las instancias y aplicaciones que requieren atención inmediata. La función Tareas de Citrix ADM proporciona recomendaciones basadas en la suscripción y el uso actual que:

- Ayude a los administradores a saber cómo Citrix ADM puede proporcionar una implementación eficiente mediante los flujos de trabajo prácticos de Guide me.
- Reduzca el tiempo y el esfuerzo cruciales de los administradores completando las tareas o reconociéndolas para que las completen más adelante.
- Asegúrese de que los administradores utilicen todas las capacidades de Citrix ADM y permitan el descubrimiento del producto y las funcionalidades recomendadas por el producto para una administración eficiente de la implementación.



En la página **Configurar tareas**, puede ver las siguientes fichas:

- **Por hacer**: Le permite ver una lista de recomendaciones. Puede revisar y hacer clic en **Guiarme** para completar la tarea o hacer clic en **Confirmar** para omitir esta tarea.
- **Archivar**: Le permite ver la lista de todas las tareas completadas o confirmadas. También puede usar la opción Guiarme para completar los requisitos periódicos.

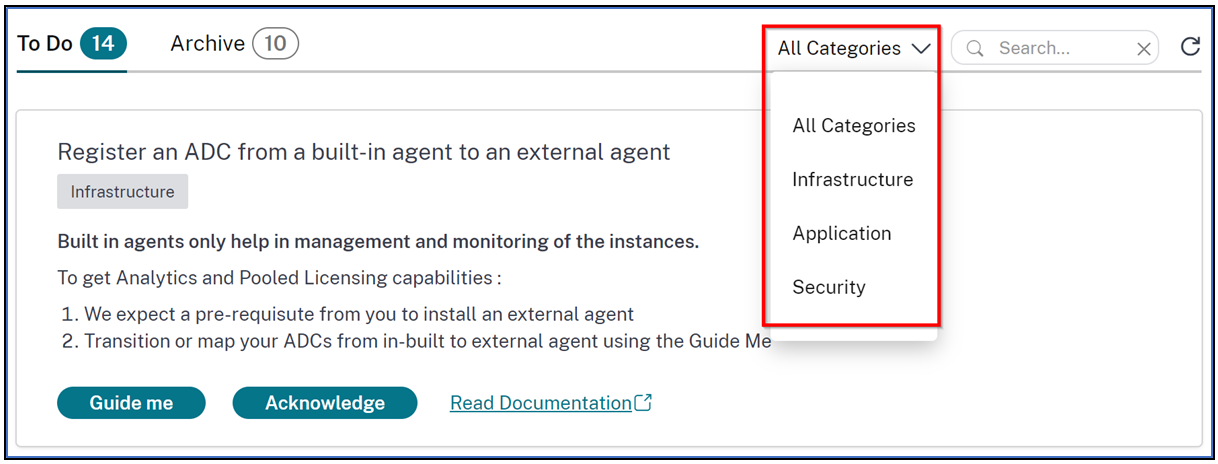
En la siguiente tabla se describen las tareas o recomendaciones que puede ver en la GUI de Citrix ADM:

Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
Agregar un ADC	Después de la integración en Citrix ADM y si no se detecta ninguna instancia de ADC.
Agregue un agente de ADM externo para utilizar al máximo las funciones de Citrix ADM	Si el agente externo no está configurado. Puede empezar con un agente integrado. Sin embargo, se requiere un agente externo para utilizar todas las funciones, como los análisis, las licencias agrupadas, etc.
Registrar un ADC de un agente integrado a un agente externo	Tras la integración en Citrix ADM mediante el flujo de trabajo de Service Connect, las instancias de ADC se incorporan mediante el agente integrado. Puede registrar esas instancias de ADC en un agente externo para utilizar todas las funciones, como el análisis, las licencias agrupadas, etc.
¡El análisis de aplicaciones es crucial! Habilitelo en sus servidores virtuales con licencia y solucione los problemas de las aplicaciones más rápidamente	Si tiene varios servidores virtuales con licencia pero no tiene habilitados los análisis.
¿Quiere reasignar ancho de banda en su ADC? ¡Es sencillo!	Si las licencias agrupadas se asignan en la GUI de ADC y esas instancias de ADC se descubren en Citrix ADM, puede realizar la reasignación mediante Citrix ADM.

Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
¡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 Citrix ADM.
Configure reglas y no se pierda ningún evento crítico en sus instancias de ADC	Si aún no se ha configurado una regla de eventos personalizada.
¿Necesita supervisar varias aplicaciones y su rendimiento? Simplemente cree una aplicación personalizada	Si la aplicación personalizada aún no está configurada.
Notifique y nunca se pierda eventos críticos en sus aplicaciones	Si la directiva de acción no está configurada para la desviación de la puntuación de la aplicación, el tiempo de procesamiento del servidor, la latencia de la red del cliente, la latencia de la red del servidor o el tiempo de respuesta.
Evite las interrupciones de uso de las aplicaciones y nunca se pierda los certificados SSL que caducan en una aplicación	Si no hay alertas o notificaciones configuradas para los certificados SSL que van a caducar
Asesoramiento de seguridad: Mantenga sus ADC actualizados con los CVEs y las mitigaciones	Si las instancias de ADC tienen algún impacto en el CVE.
Configurar una directiva empresarial y supervisar desviaciones	Si la configuración empresarial de SSL no ha cambiado o sigue siendo la predeterminada.
¿Repite tareas manuales? Cree trabajos de configuración y aplíquelos a varios ADC	Si la tarea **Config Job** aún no está configurada.
Administre y supervise la puntuación de su 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.

Nombre de la recomendación	¿Cuándo la tarea está visible en la GUI?
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 Citrix ADM aún no está configurada.
Personalice el umbral predeterminado o crea uno para sus servicios de Kubernetes	Si solo se utilizan los umbrales predeterminados en el gráfico de servicios y no se aplica ningún umbral simple o doble a los servicios.
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 Citrix ADM aún no está configurada.
Automatice la administración de certificados SSL con Venafi y ADM	Si el servidor Venafi aún no está configurado en Citrix ADM.

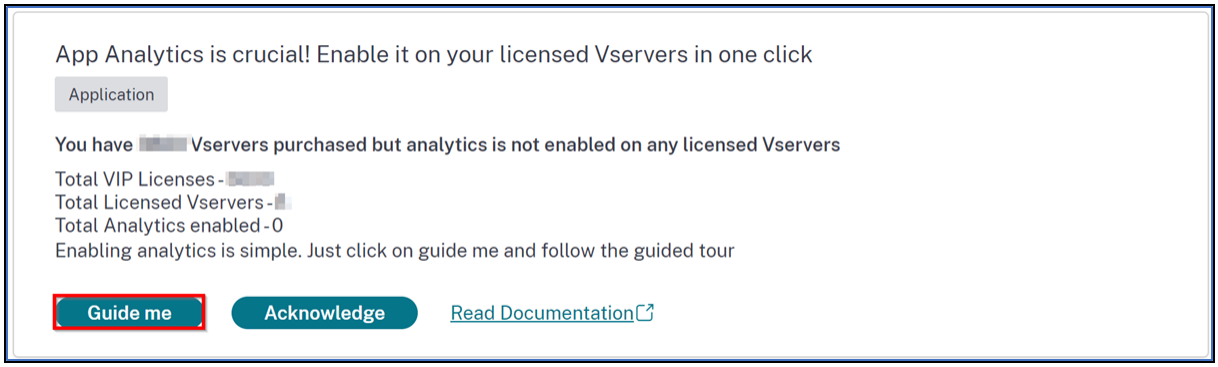
De forma predeterminada, puede ver las 5 recomendaciones principales. Haga clic en **Mostrar todo** para ver todas las recomendaciones. Puede utilizar la lista de categorías y seleccionar una categoría para filtrar recomendaciones específicas en función de la selección.



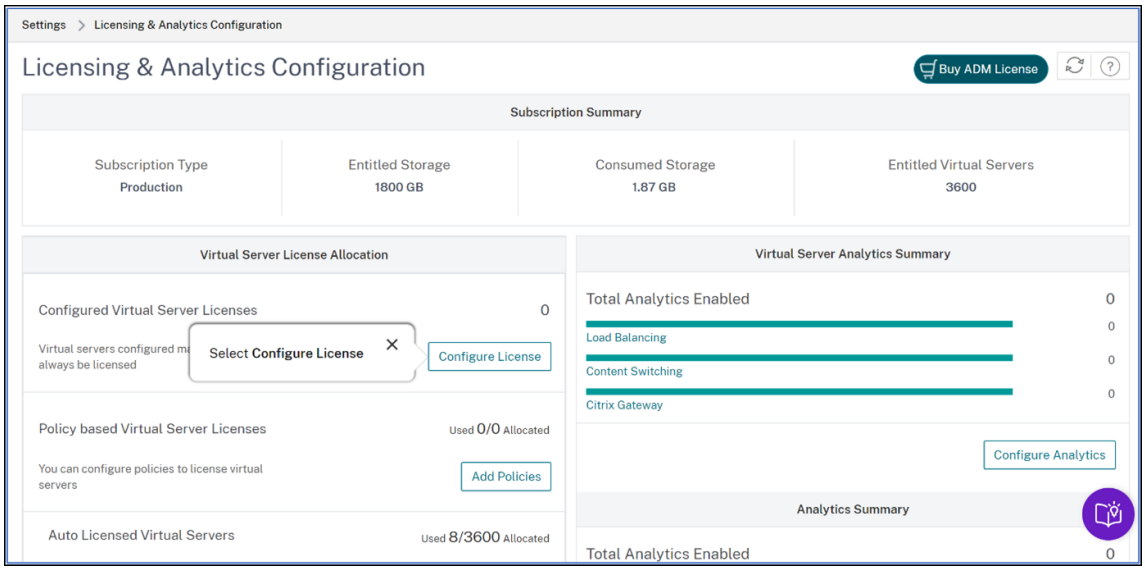
Como alternativa, también puede usar la barra de búsqueda y escribir los primeros caracteres para desglosar la tarea.

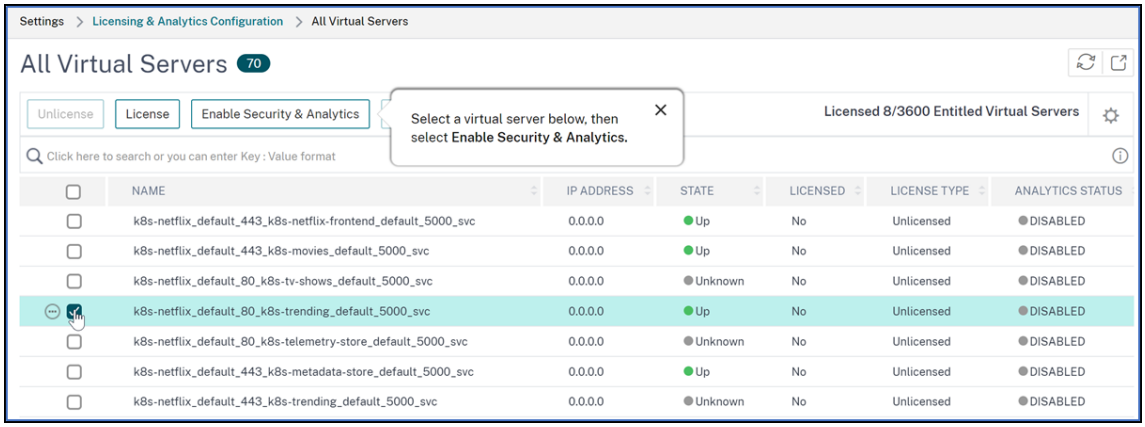
¿Cómo utilizar el flujo de trabajo de Guide me y completar la tarea?

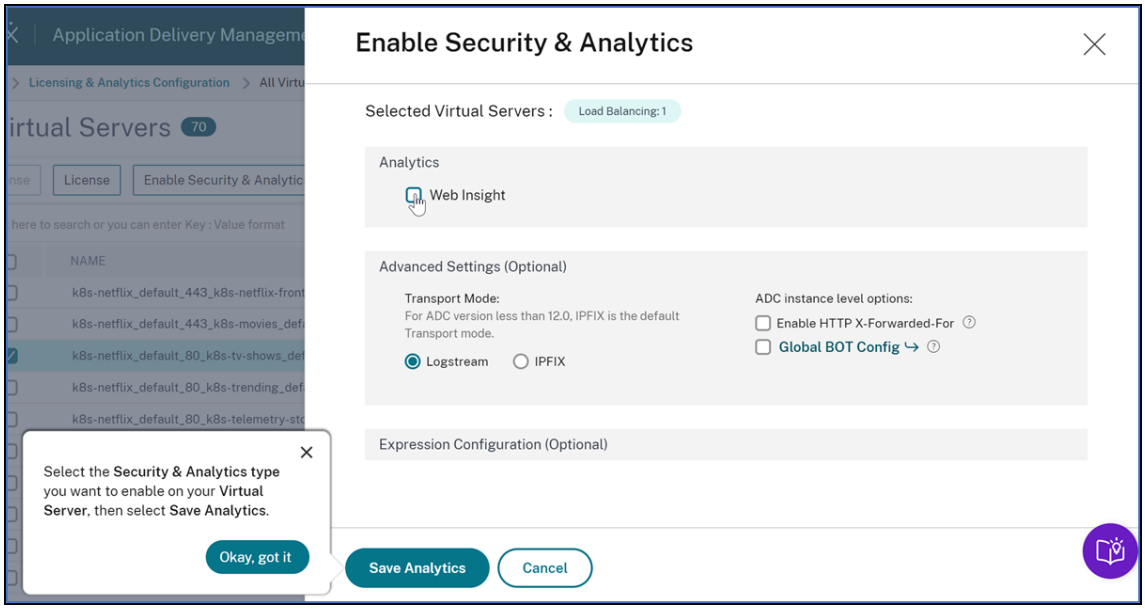
Pongamos que quiere habilitar el análisis para todos los servidores virtuales con licencia. Haga clic en **Guiarme** para realizar la siguiente tarea:



El flujo de trabajo proporciona las sugerencias necesarias para completar la tarea. En este ejemplo, después de hacer clic en **Guiarme**, siga las sugerencias de información sobre herramientas que se proporcionan:

1. 

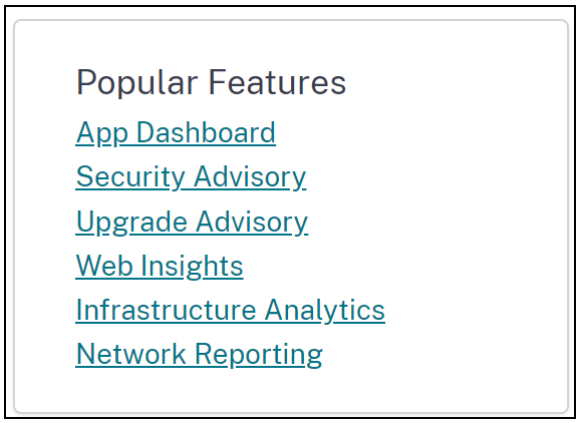
2. 

3. 

Tras seleccionar el tipo de análisis y hacer clic en **Guardar análisis**, la tarea habrá finalizado. Esta tarea se mueve a la ficha **Archivado**.

Del mismo modo, también puede utilizar el mismo flujo de trabajo para los requisitos periódicos en la ficha **Archivar**.

En **Funciones populares**, puede ver las funciones importantes de Citrix ADM y le permite explorarlas haciendo clic en una función.



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. Puedes disfrutar al máximo

del flujo de trabajo de **Guide me** solo cuando Pendo esté disponible.

2. ¿Por qué tipo de tareas están presentes los administradores?

   Actualmente, las recomendaciones son específicas para las implementaciones y ayudan a los administradores a realizar más configuraciones y tareas de configuración para que la implementación sea eficiente. También permite descubrir mejor los productos y los administradores pueden saber qué hace una tarea y cómo puede ayudar sin ningún conocimiento previo ni saber si la función existe en ADM o no.

3. ¿Puedo devolver una tarea de **Archivar** a **Por hacer**?

   Cualquier tarea archivada vuelve **a la categoría de tareas pendientes** únicamente en función de condiciones específicas. Por ejemplo, si se eliminan todas las reglas del evento o se eliminan todos los ADC, una tarea archivada vuelve a pasar a Tareas pendientes para los administradores, a fin de llamar su atención.

4. ¿Se completa la barra de progreso si confirmo?

   ¡Sí! Sin embargo, se recomienda completar estas tareas. Sin embargo, si quieres hacerlo más adelante, puedes confirmar que conoces la recomendación del producto y volver a Archivar para completarla más tarde.

5. ¿La tarea va a Archivar si inicio una guía para mí y la dejo en el medio?

   No, la tarea sigue estando disponible en Tareas pendientes a menos que la acción se guarde o se complete.

6. ¿Puedo realizar búsquedas o filtros?

   ¡Sí! Puede utilizar la barra de búsqueda o limitarse a tareas específicas seleccionando la categoría de la lista.

7. ¿Conseguiré que las tareas tomen medidas en caso de eventos dinámicos, como el pico de memoria de ADC, la caída de la aplicación, la caída del servidor virtual de LB, etc.?

   Todo esto forma parte de las mejoras y está previsto que estén disponibles en las próximas versiones.

8. ¿Estará disponible para el ADM local?

   Actualmente, esta función solo está disponible en el servicio ADM.

9. ¿Aparecerán todas mis más de 20 tareas incluso si no tengo un ADC agregado en Citrix ADM?

   No. Debe tener tanto la instancia de ADC como los servidores virtuales disponibles en Citrix ADM para mostrar todas estas tareas.

10. ¿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. Se obtienen y actualizan los detalles de cada tarea. Las tareas se actualizan automáticamente cada 24 horas. Para un mejor control administrativo, también puede actualizar manualmente las tareas para obtener el estado más reciente.

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

November 17, 2022

En Citrix ADM, puede ver varios datos sobre el uso y el rendimiento de las aplicaciones, la infraestructura de ADC, las infracciones de seguridad (bots y WAF), etc. Como administrador, es posible que tenga que navegar hasta varias opciones de la GUI de ADM para ver varios datos. Por ejemplo, para comprobar la información sobre los servidores virtuales (aplicaciones) y las instancias de ADC:

- Primero debe ir a **Aplicaciones > Panel de control** para ver información sobre las aplicaciones.
- A continuación, debe ir a **Infraestructura > Análisis de infraestructura** para ver información sobre las instancias de ADC.

Para una mejor experiencia de monitoreo, es necesario que tenga un privilegio que contenga una descripción general de todos los datos requeridos. Vaya a **Descripción general > Panel de control** para visualizar un panel de control de un solo panel con una descripción general de los detalles de las métricas clave en función de las siguientes categorías:

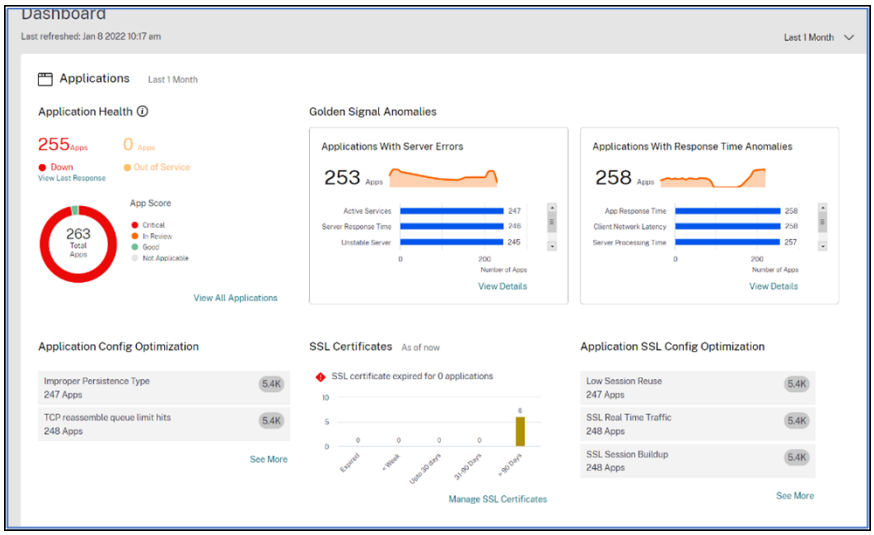
- Aplicaciones
- Infraestructura ADC
- Seguridad de las aplicaciones
- Gateway

Aplicaciones

En **Aplicaciones**, puede ver:

- Estado de**la aplicación** : proporciona una descripción general de las aplicaciones que están **inactivas** o **fuera de servicio**y en función de su estado, como **Crítico**, **En revisión**, En **buen**estado y **No aplicable**. Haga clic en **Ver todas las aplicaciones** para ver los detalles en el panel de aplicaciones
- **Anomalías de Golden Signal** : proporciona una descripción general de las aplicaciones que tienen errores de servidor y anomalías en el tiempo de respuesta. Haga clic en **Ver detalles** para obtener más información.

- **Optimización de la configuración de aplicaciones** : proporciona una descripción general del total de aplicaciones que tienen problemas de rendimiento. Haga clic en **Ver más** para ver los detalles del problema en el panel de control
- **Certificados SSL** : proporciona una descripción general de los certificados SSL junto con su validez. Haga clic en **Administrar certificados SSL** para ver más información en el panel de control SSL.
- **Optimización de la configuración SSL** de aplicaciones: proporciona una descripción general del total de aplicaciones que tienen problemas relacionados con SSL. Haga clic en **Ver más** para ver los detalles del problema.



Infraestructura ADC

En **ADC Infrastructure**, puede ver las siguientes métricas clave relacionadas con la instancia de ADC:

- Estado de**la instancia de ADC** : proporciona una descripción general del total de instancias de ADC en función de la puntuación de la instancia.
- **Instancias de ADC afectadas por los CVE** : proporciona una descripción general del total de instancias de ADC que se ven afectadas por vulnerabilidades y exposiciones comunes (CVE). Para obtener más información, consulte Aviso de seguridad.
- **Problemas de instancias de ADC** : proporciona una descripción general de los problemas de las instancias de ADC en función de la categoría de problema. Para obtener más información, consulte Análisis de infraestructura.
- **Resumen de actualización de instancias de ADC** : proporciona una descripción general del total de instancias de ADC que no están en la versión más reciente. Haga clic en Ver panel de instancias de ADC para obtener más información.

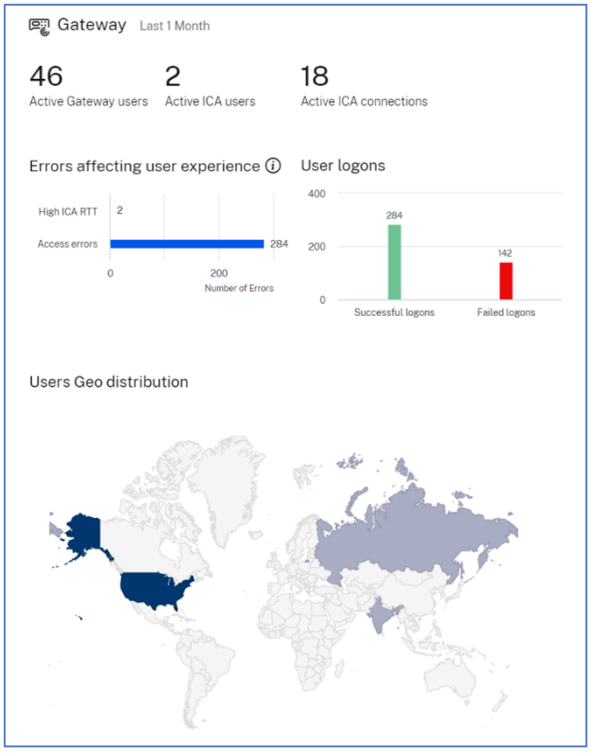
Seguridad de las aplicaciones

Proporciona una descripción general del total de aplicaciones afectadas y del total de infracciones (bots y WAF) notificadas durante el período seleccionado. Haga clic en **Ver panel de seguridad** para ver los detalles de las infracciones de seguridad y de bots

Gateway

Proporciona una descripción general del total de usuarios de gateway activos, el total de usuarios de ICA activos y el total de conexiones ICA activas. También puede ver los errores, los detalles de inicio

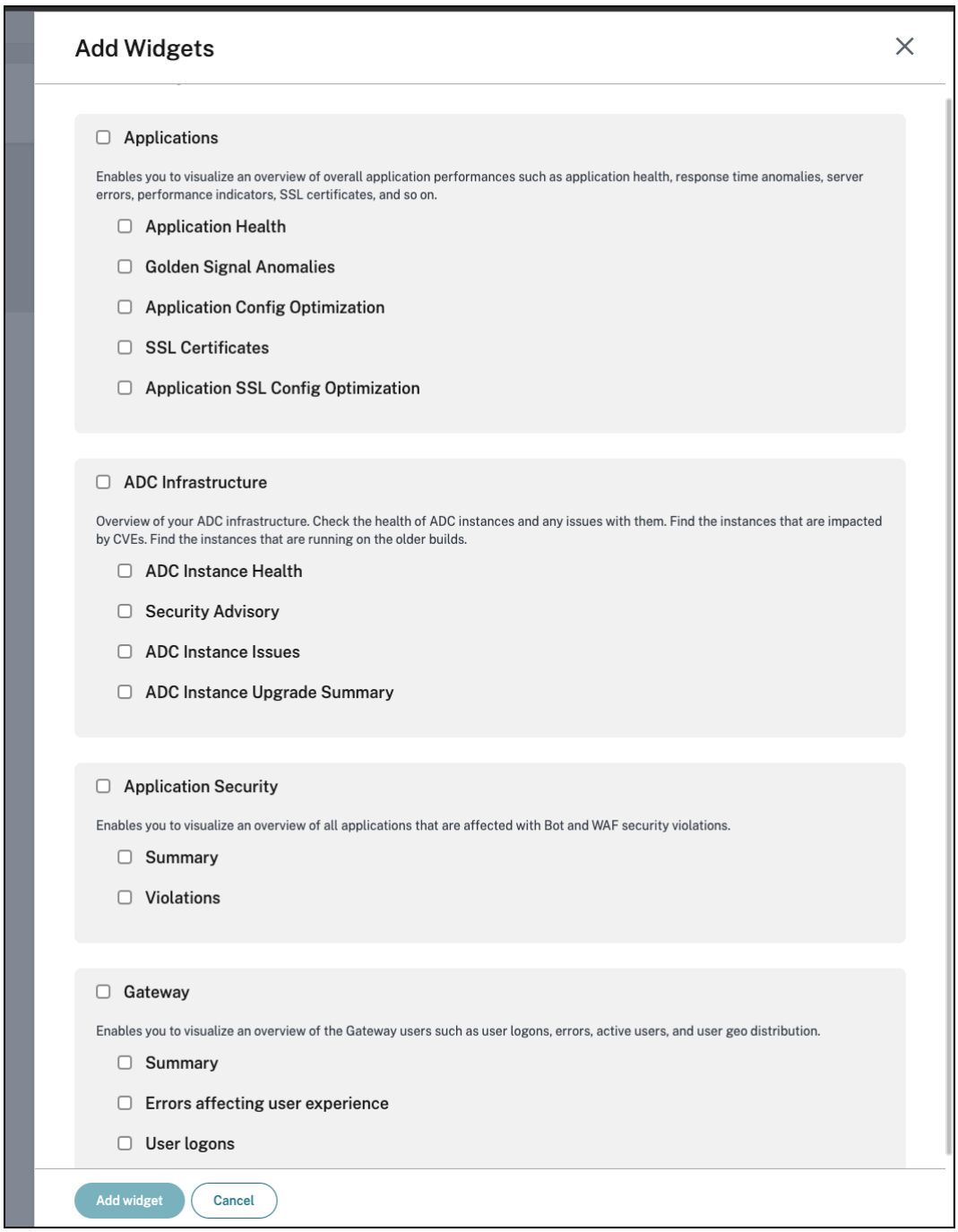
de sesión de los usuarios y un mapa geográfico que proporciona detalles sobre las ubicaciones de los usuarios.



Personaliza el panel

Puede usar la opción **Modificar panel** y personalizar la vista del panel según su elección. Con la opción **Modificar panel** de control, puede:

- Arrastrar widgets
- Elimine todo el widget (aplicaciones, infraestructura ADC, gateway o seguridad de aplicaciones).
- Elimine los widgets más pequeños presentes debajo de cada widget.
- Haga clic en **Agregar widget** y seleccione las métricas clave necesarias que quiere ver en cada widget.



- Restablecer los valores predeterminados
- Restablecer la última vez que se guardó

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

> **Nota**
>
> - De forma predeterminada, se muestran todos los widgets. Si personaliza el panel, guarde

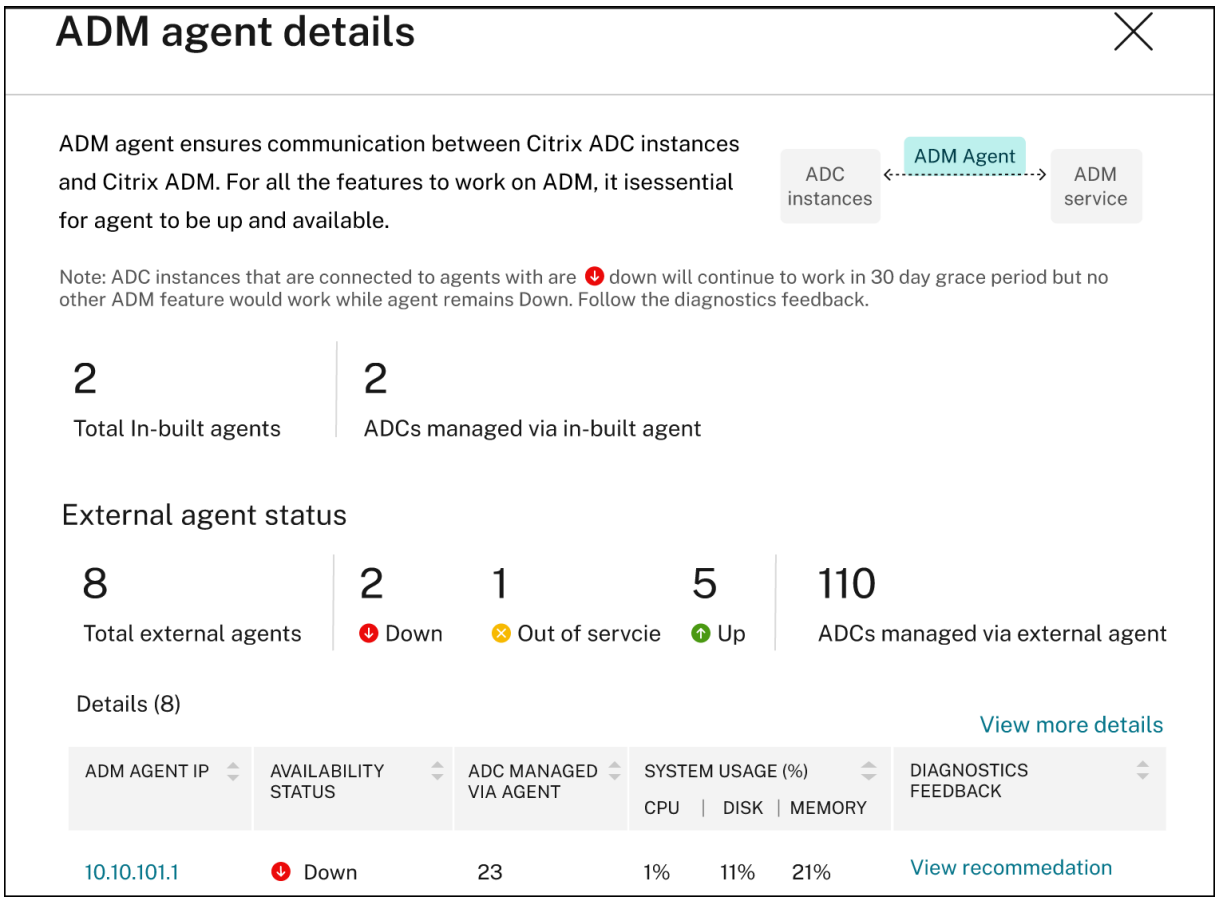
> los cambios y utilice de nuevo la opción **Restablecer los valores predeterminados**, todos los widgets se agregarán al panel.
>
> - La opción **Restablecer la última vez guardada** carga la configuración guardada anteriormente.

Ver detalles del agente

En el panel unificado, puede visualizar una descripción general de los detalles del agente de ADM. En **Descripción general > Panel de control**, junto al **estado del agente de ADM**, puede ver el siguiente estado que le permite analizar la disponibilidad general de los agentes:

- **Todos disponibles**. Indica que todos los agentes están en funcionamiento.
- **Todo no está disponible**. Indica que todos los agentes están fuera de servicio y no están disponibles.
- **[número de agentes] no disponible**. Indica que algunos agentes están inactivos y no se puede acceder a ellos.
- **Todo fuera de servicio**. Indica que todos los agentes están fuera de servicio.
- **[número de agentes] fuera de servicio**. Indica que algunos agentes están fuera de servicio.
- **No se ha encontrado el agente externo**. Indica que no hay ningún agente configurado (a través de ningún hipervisor).

Haga clic en **Ver detalles** para ver una descripción general de los detalles del agente de ADM, como el total de agentes integrados, el total de agentes externos, la IP del agente, el estado, el uso del sistema, las comprobaciones de diagnóstico, etc.



Aplicaciones

December 2, 2022

La función de análisis y administración de aplicaciones de Citrix ADM le permite supervisar las aplicaciones mediante un enfoque centrado en las aplicaciones. Este enfoque le ayuda a:

- Compruebe la puntuación y analice el rendimiento general de las aplicaciones
- Compruebe si hay algún problema que persista con el servidor o el cliente
- Detecte anomalías en los flujos de tráfico de la aplicación y tome medidas correctivas

> **Nota**
>
> Las aplicaciones hacen referencia a uno o más servidores virtuales que están configurados en las instancias (Citrix ADC).

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 Citrix ADC en Citrix ADM
- Asegúrese de tener una licencia válida para sus instancias Citrix ADC. Para obtener más información, consulte Licencias
- Asegúrese de haber aplicado una licencia para servidores virtuales. Para obtener más información, consulte Administrar licencias en servidores virtuales

Descripción general de la aplicación

Las aplicaciones pueden ser:

- Aplicaciones discretas
- Aplicaciones personalizadas
- Aplicaciones de microservicios (k8s_discrete)

Aplicaciones discretas

Todos los servidores virtuales con licencia se denominan aplicaciones discretas.

Aplicaciones personalizadas

Los servidores virtuales de una categoría se denominan aplicaciones personalizadas. Como administrador, debe agregar aplicaciones personalizadas basadas en una categoría. A continuación, puede gestionar y supervisar las aplicaciones a través del panel de control. Obtiene la facilidad de monitorear aplicaciones específicas que se agrupan en una categoría.

Por ejemplo, puede crear una categoría para su centro de datos1 y agregar sus instancias de ADC. Tras definir una categoría y agregar la instancia para el centro de datos1, el panel de la aplicación se muestra con una categoría independiente, que incluye todas las aplicaciones relacionadas con el centro de datos1.

Puntos que tener en cuenta

- Las aplicaciones discretas que se agregan a las aplicaciones personalizadas se eliminan de las aplicaciones discretas.
- Todas las aplicaciones que no se añaden a ninguna categoría están disponibles como **«otras»**.
- De forma predeterminada, Citrix ADM le permite agregar licencias para hasta 2 aplicaciones. Dependiendo de su licencia, puede seleccionar y aplicar licencias para las aplicaciones que quiere supervisar.

Aplicaciones de microservicios

En un clúster de Kubernetes, Citrix proporciona un Ingress Controller para Citrix ADC MPX (hardware), Citrix ADC VPX (virtualizado) y Citrix ADC CPX (contenedor). Para obtener más información, consulte Citrix Ingress Controller.

Las aplicaciones discretas que se configuran mediante las instancias de Citrix ADC CPX se denominan aplicaciones de microservicios.

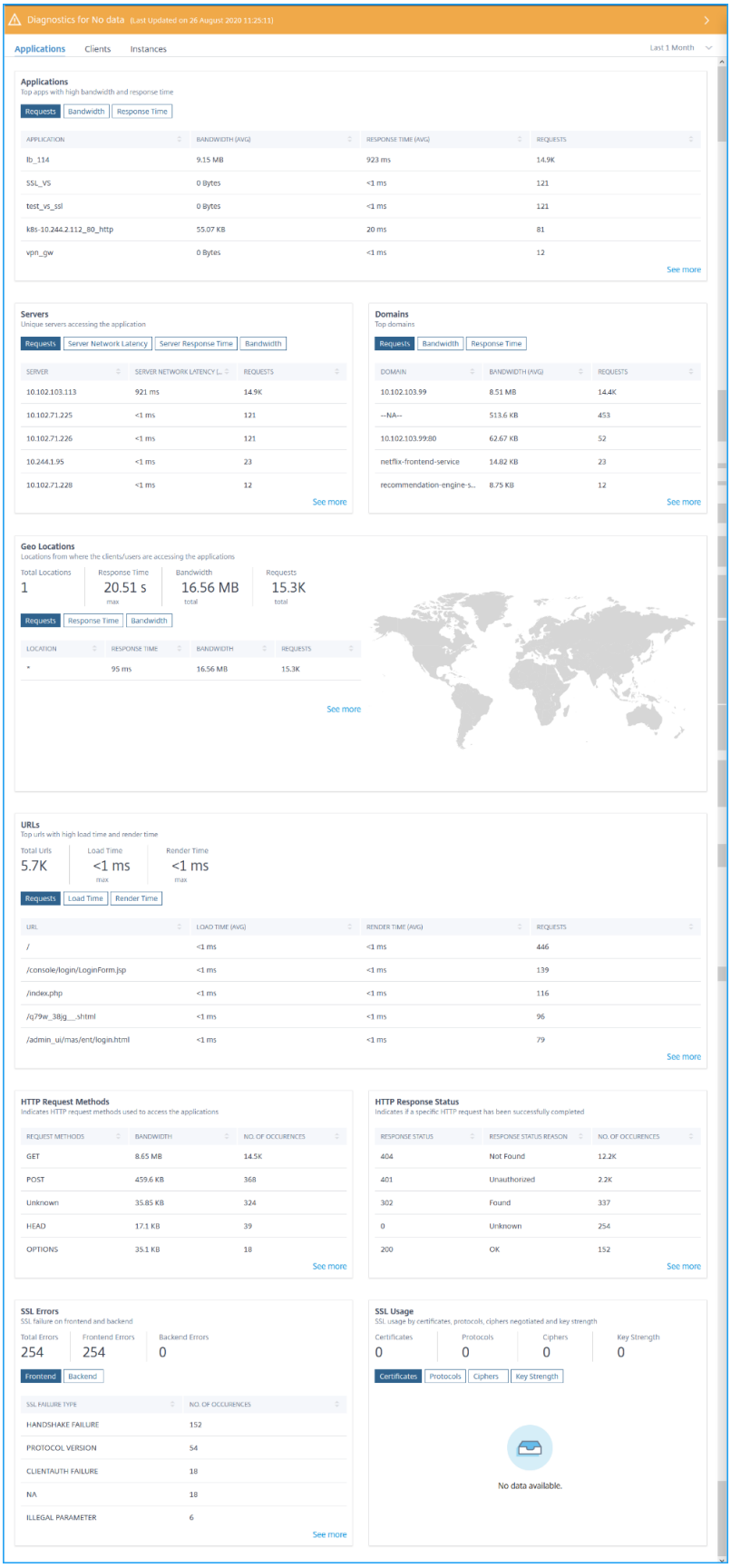
Panel de control Web Insight

November 16, 2022

La función de Web Insight mejorada se incrementa y proporciona visibilidad de métricas detalladas para aplicaciones web, clientes e instancias de Citrix ADC. Esta Web Insight mejorada le permite evaluar y visualizar la aplicación completa desde las perspectivas de rendimiento y uso juntos. Como administrador, puede ver Web Insight para:

- Una aplicación. Vaya a **Aplicaciones > Panel**, haga clic en una aplicación y seleccione la ficha **Web Insight** para ver las métricas detalladas. Para obtener más información, consulte Análisis de uso de aplicaciones.
- Todas las aplicaciones. Vaya a **Aplicaciones > Web Insight** y haga clic en cada ficha (Aplicaciones, Clientes, Instancias) para ver las siguientes métricas:

Aplicaciones	Clientes	Instancias
Aplicación con anomalías de tiempo de respuesta	Clientes	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
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.

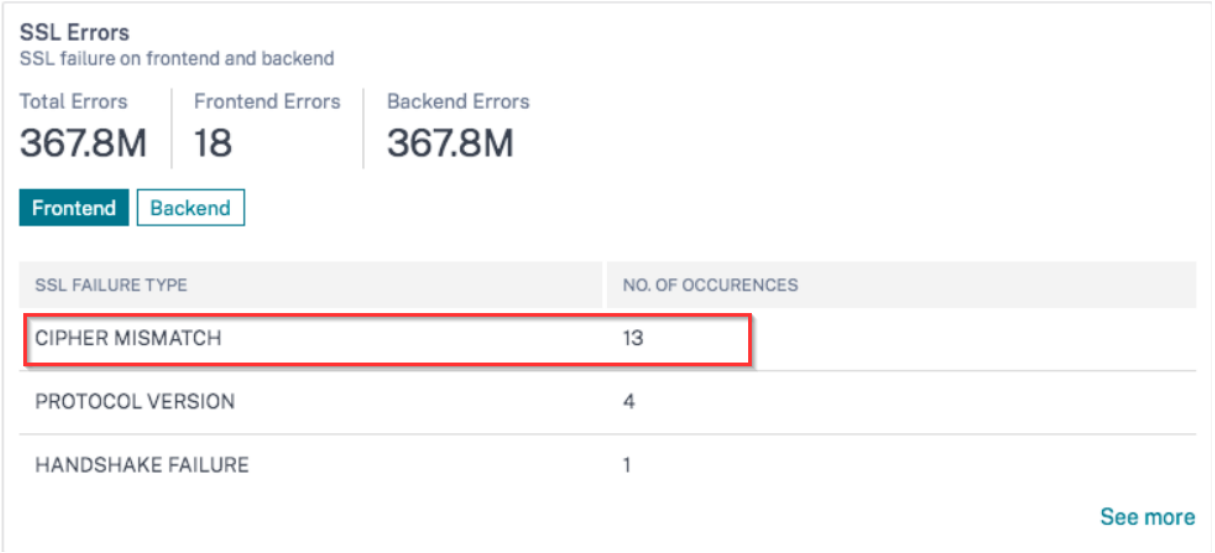
> Nota
>
> En algunos casos, es posible que Citrix ADC no pueda calcular los valores de RTT para algunas transacciones. Para este tipo de transacciones, Citrix ADM muestra los valores de RTT como
>
> - **NA**: Se muestra cuando la instancia de ADC no puede calcular el RTT.
> - **< 1 ms**: Se muestra cuando la instancia de ADC calcula el RTT en decimales entre 0 ms y 1 ms. Por ejemplo, 0,22 ms.

Ver detalles de problemas relacionados con el cifrado

En **Errores de SSL**, puede ver los detalles de los siguientes parámetros de SSL:

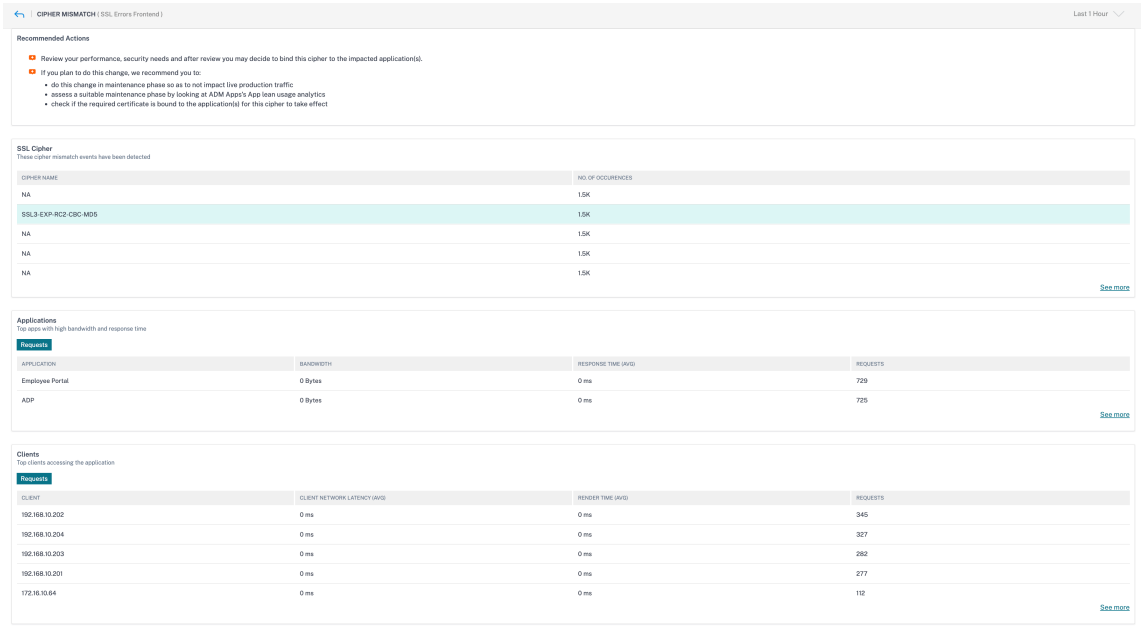
- Desajuste de cifrado
- Cifrados no compatibles

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.

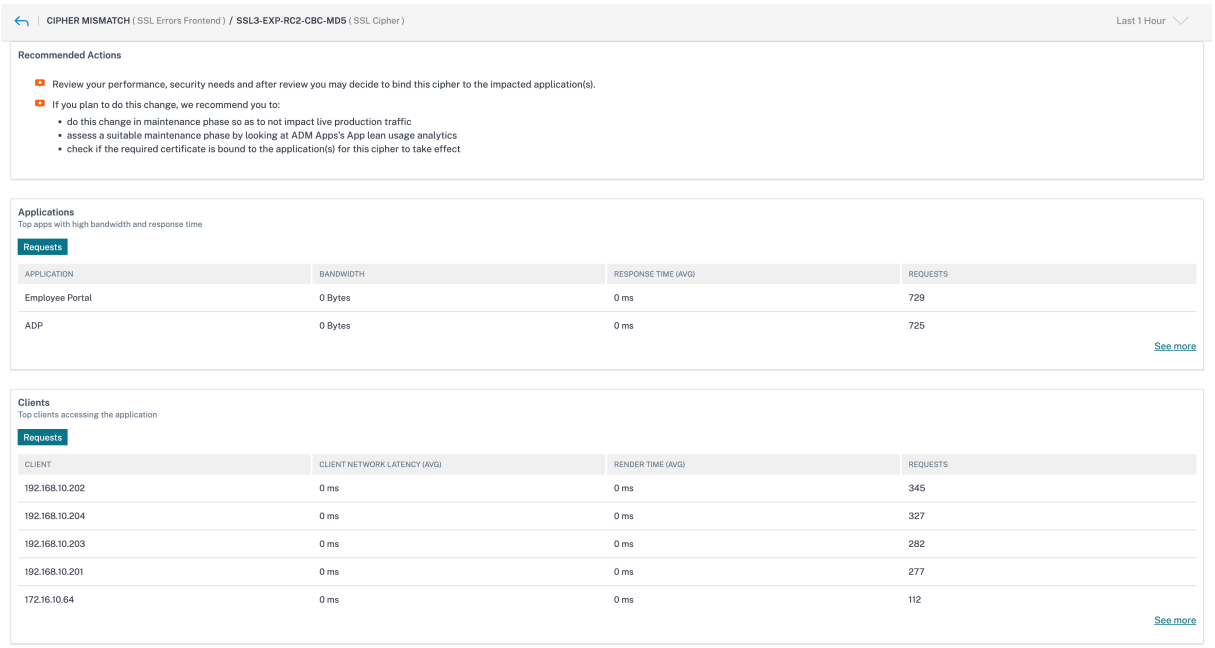


Aparece la página de detalles del parámetro SSL seleccionado. Puede hacer lo siguiente:

- 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.



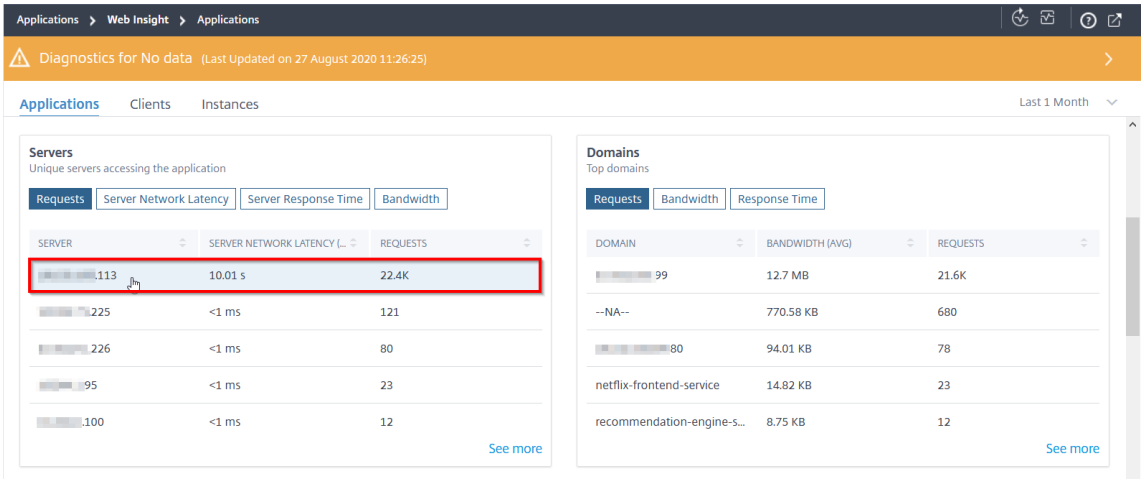
Haga clic en el **nombre del cifrado SSL** para ver las aplicaciones y los clientes afectados por el cifrado SSL seleccionado.



Otro caso de uso

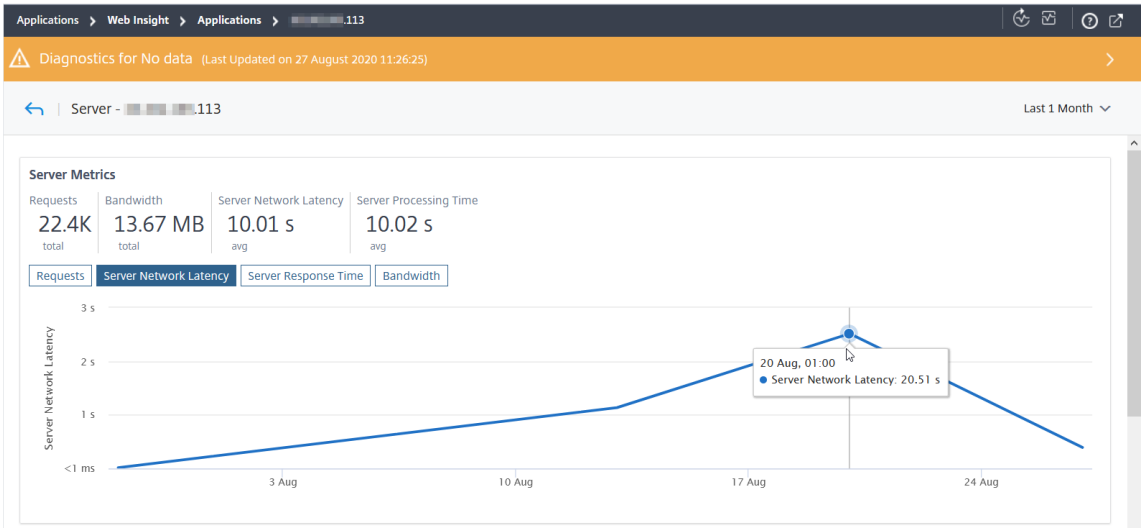
Tenga en cuenta que quiere analizar la latencia de la red del servidor durante un mes y decidir si quiere ampliar o reducir el entorno de producción. Para analizar esto:

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 10.01s y, a partir del gráfico, puede analizar que la latencia de red del servidor durante el último 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

November 16, 2022

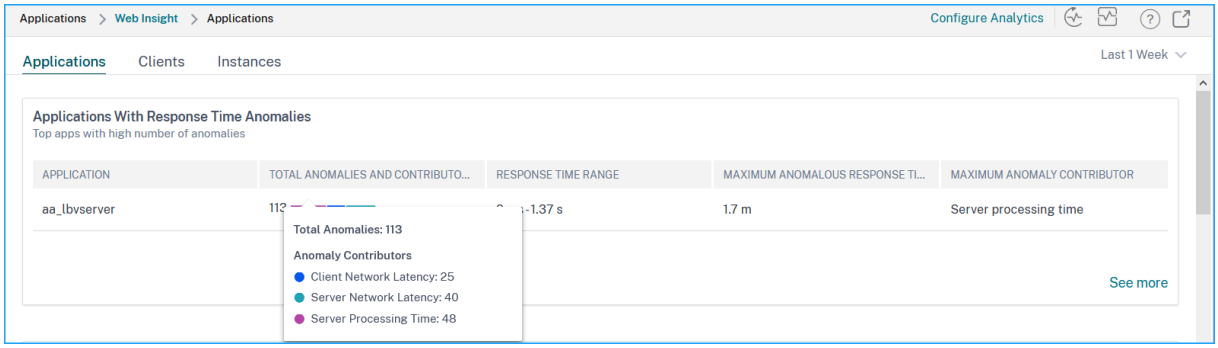
La lentitud de las aplicaciones es una preocupación importante para cualquier organización, ya que tiene como resultado un impacto en el negocio o productividad. Como administrador, debe asegurarse de que todas las aplicaciones funcionen de manera óptima para evitar cualquier impacto en el

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

Citrix ADM realiza comprobaciones de anomalías cada hora e informa de 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.

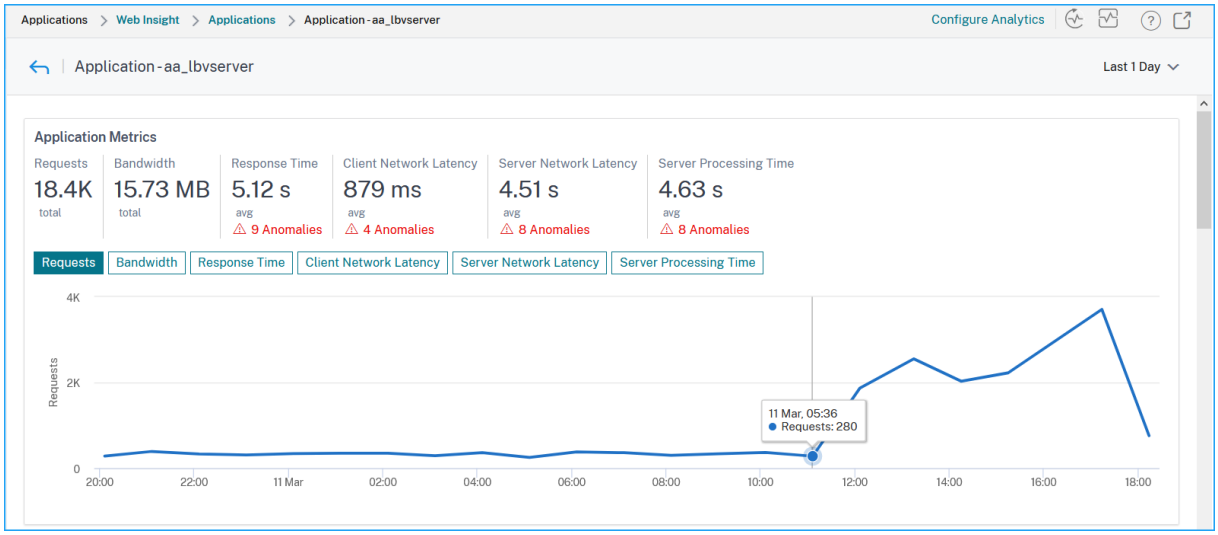
La página **Aplicaciones > Web Insight** permite ver las aplicaciones con anomalías de tiempo de respuesta durante la duración seleccionada. La métrica **Aplicaciones con anomalías de tiempo de respuesta** muestra las cinco aplicaciones principales en función de las anomalías totales. Haga clic en **Ver 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.



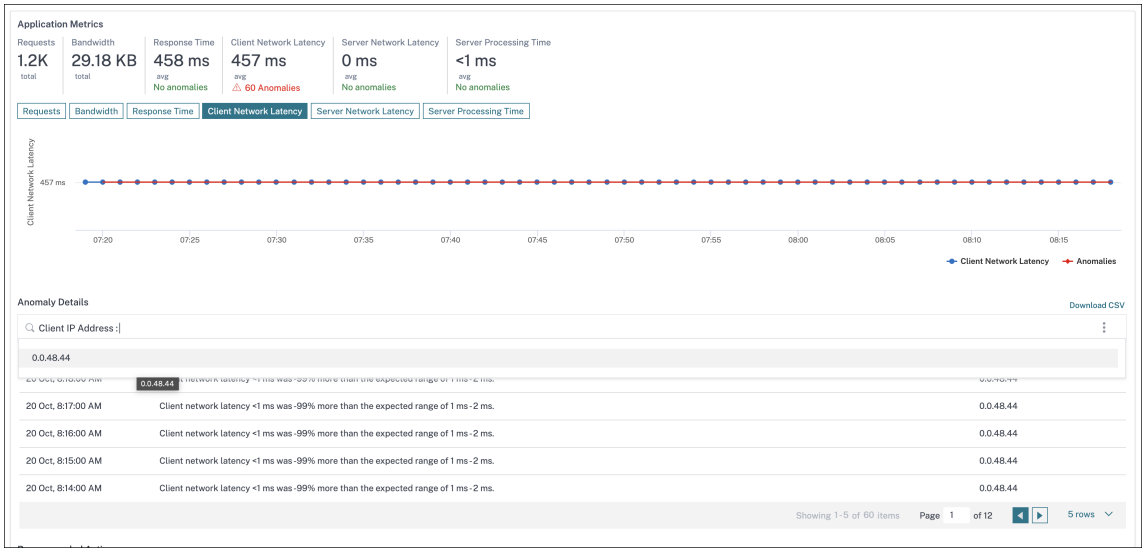
Las **Métricas de la Aplicación** le permiten ver:

- **Solicitudes** — El total de solicitudes recibidas por la solicitud
- Ancho de**banda** : ancho de banda total procesado por la aplicación
- **Tiempo de respuesta** : el tiempo medio de respuesta de la aplicación
- **Latencia de red** del cliente: latencia media de la red del cliente (del cliente al ADC)
- **Latencia de red** del servidor: latencia media de la red del servidor (de ADC a servidor)
- **Tiempo de procesamiento del servidor** : el tiempo medio de procesamiento del servidor (del servidor al ADC)

Si la aplicación tiene anomalías, puede ver si las anomalías provienen de latencia de red cliente, latencia de red del servidor o tiempo de procesamiento del servidor. Haga clic en cada ficha para ver los detalles.

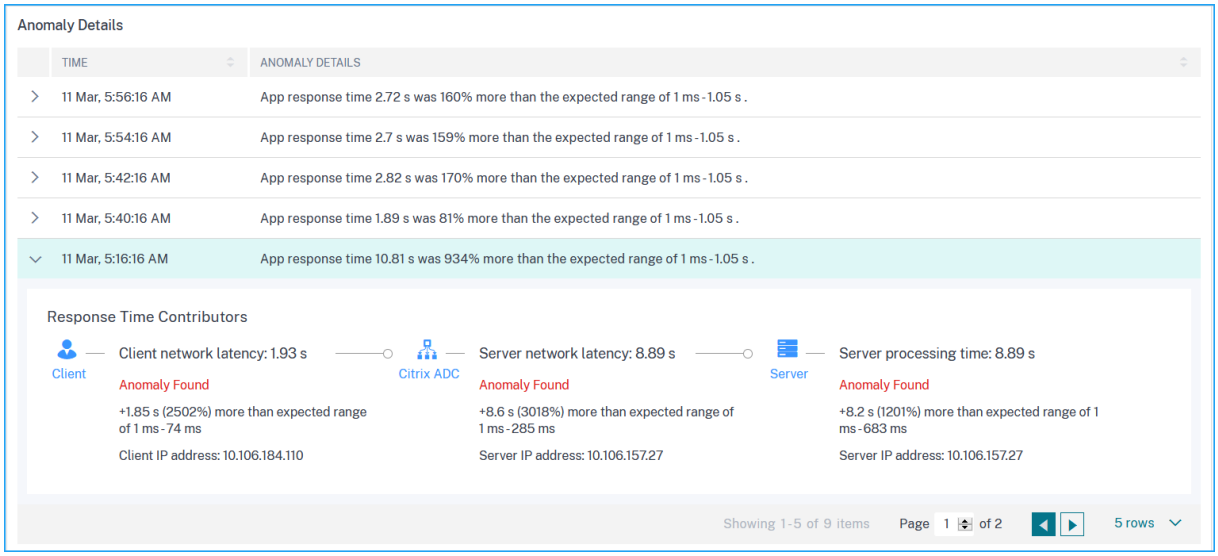
En las fichas **Latencia de la red del cliente** y **Latencia de la red del servidor**, puede ver:

- **Una barra de búsqueda** : haga clic en la barra de búsqueda para ver la dirección IP de todos los clientes (en Latencia de red de clientes) y servidores (en Latencia de red de servidores). Puede seleccionar la dirección IP para filtrar los resultados.
- **Una opción de exportación** : haga clic en **Descargar CSV** para exportar los detalles en formato CSV.

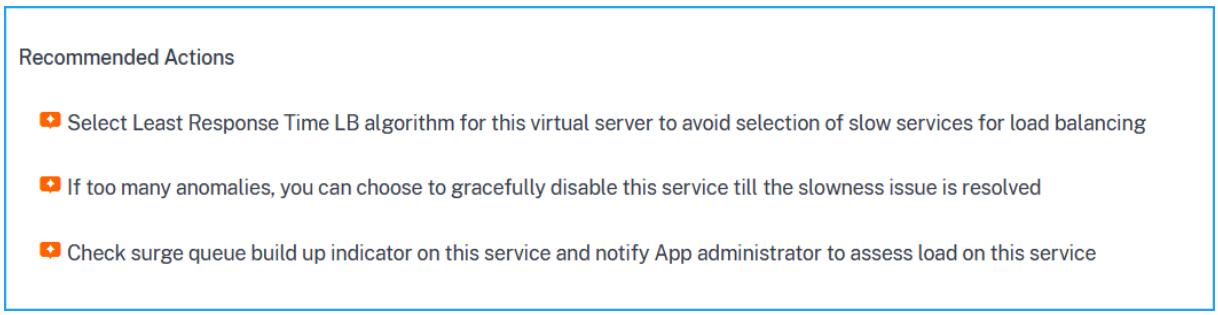


Tiempo de respuesta

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.

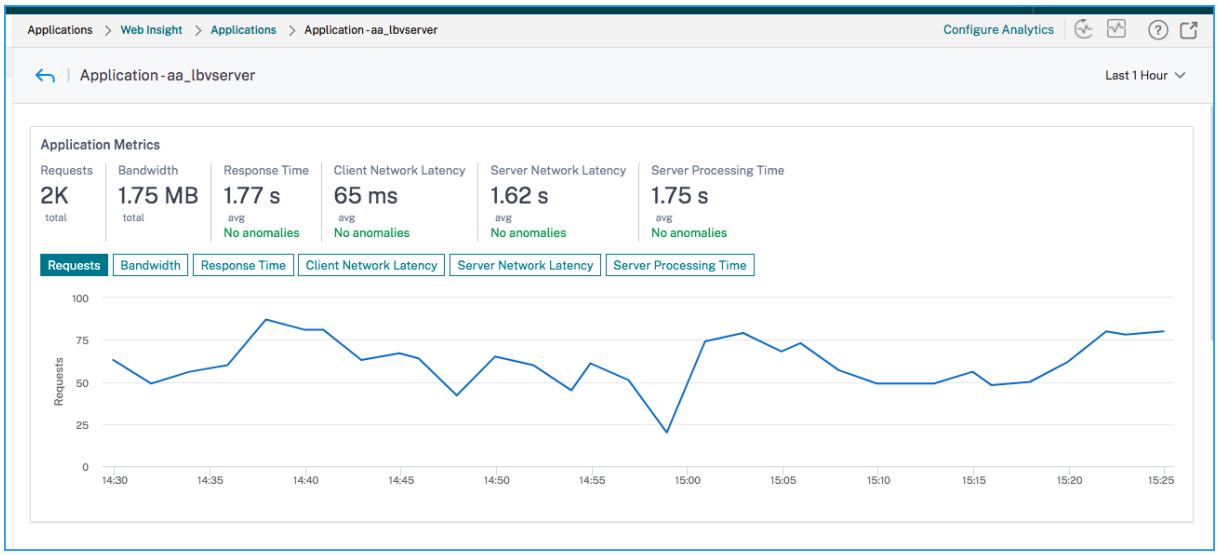


Gráfico de servicio

November 16, 2022

La función de gráfico de servicio de Citrix ADM permite supervisar todos los servicios de una representación gráfica. Esta función también le permite ver un análisis detallado y métricas accionables de los servicios. Vaya a **Aplicaciones > Gráfico de servicio** para ver el gráfico de servicio para:

- Aplicaciones configuradas en todas las instancias de Citrix ADC
- Aplicaciones de Kubernetes

- Aplicaciones web de 3 niveles

Gráfico de servicio para aplicaciones en todas las instancias de Citrix ADC

La función de gráfico de servicio global le permite obtener una visualización holística de la vista `clients to infrastructure to application`. 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 Citrix ADC) 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 Citrix ADC 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 Citrix ADC
- Todas las instancias de Citrix ADC que tienen aplicaciones discretas, aplicaciones personalizadas y aplicaciones de microservicio discretas
- Las 4 principales aplicaciones de puntuación baja que pertenecen a aplicaciones personalizadas, aplicaciones discretas y aplicaciones de microservicios
- Información de métricas para los 4 principales servidores virtuales de puntuación baja
- El estado de las aplicaciones (aplicaciones discretas, aplicaciones personalizadas y aplicaciones de microservicios) como **Crítica**, **Revisión**, **Buena** y **No Aplicable**.

Para obtener más información, consulte Vista holística de las aplicaciones en el gráfico de servicio.

Gráfico de servicio para aplicaciones Kubernetes

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Microservicios** para ver:

- Garantice el performance general de las aplicaciones end-to-end

- Identifique los cuellos de botella creados por la interdependencia de los diferentes componentes de sus aplicaciones
- Reúna información sobre las dependencias de los diferentes componentes de sus aplicaciones
- Supervise los servicios dentro del clúster de Kubernetes
- Supervisa qué servicio tiene problemas
- Compruebe los factores que contribuyen a los problemas de rendimiento
- Ver la visibilidad detallada de las transacciones HTTP del servicio
- Analizar las métricas HTTP, TCP y SSL
- Ver métricas de cliente y detalles de resumen de transacciones de cliente

Al visualizar estas métricas en Citrix ADM, puede analizar la causa raíz de los problemas y realizar las acciones necesarias para solucionar problemas más rápidamente. El gráfico de servicio muestra sus aplicaciones en varios servicios de componentes. Estos servicios que se ejecutan dentro del clúster de Kubernetes pueden comunicarse con varios componentes dentro y fuera de la aplicación. Para empezar, consulta Configurar el gráfico de servicios.

Gráfico de servicios para aplicaciones web de 3 niveles

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Aplicaciones Web** para ver:

- Detalles sobre cómo se configura la aplicación (con el servidor virtual de conmutación de contenido y el servidor virtual de equilibrio de carga)

  Para las aplicaciones GSLB, puede ver los servidores virtuales de centros de datos, instancias de ADC, CS y LB.
- Transacciones de extremo a extremo desde el cliente hasta el servicio
- La ubicación desde la que el cliente accede a la aplicación
- El nombre del centro de datos donde se procesan las solicitudes de cliente y las métricas Citrix ADC 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**. Citrix ADM muestra el estado del servicio según el tiempo de respuesta del servicio y el recuento de errores.
  - **Crítico (rojo)** : indica cuándo el tiempo promedio de respuesta del servicio es superior a 200 ms Y el recuento de errores es > 0
  - **Revisión (naranja)** : indica si el tiempo promedio de respuesta del servicio es > 200 ms O el recuento de errores es > 0

  - **Bueno (verde)** : indica que no hay errores y que el tiempo medio de respuesta del servicio es inferior a 200 ms

- El estado del cliente, como **Crítico**, **Revisado**y **Bueno**. Citrix ADM muestra el estado del cliente en función de la latencia de la red del cliente y el recuento de errores.
  - **Crítico (rojo)**: indica si la latencia promedio de la red del cliente es > 200 ms Y el recuento de errores es > 0
  - **Revisión (naranja)** : indica si la latencia promedio de la red del cliente es > 200 ms O el recuento de errores es > 0
  - **Bueno (verde)** : indica que no hay ningún error y que la latencia media de la red del cliente es inferior a
- El estado del servidor virtual, como **Crítico**, **Revisado**y **Correcto**. Citrix ADM muestra el estado del servidor virtual en función de la puntuación de la aplicación.
  - **Crítico (rojo)** : indica si la puntuación de la aplicación es inferior a
  - **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

November 16, 2022

Los StyleBooks simplifican la tarea de administrar configuraciones complejas de Citrix ADC para sus aplicaciones. Un StyleBook es una plantilla que puede utilizar para crear y administrar configuraciones de Citrix ADC. Puede crear un StyleBook para configurar una función específica de Citrix ADC, o puede diseñar un StyleBook para crear configuraciones para la implementación de una aplicación empresarial, como Microsoft Exchange o Lync.

Los StyleBooks se ajustan perfectamente a los principios de la infraestructura como código que practican los equipos de DevOps, donde las configuraciones son declarativas y se controlan por versiones. Las configuraciones también se repiten y se implementan como un todo. Los StyleBooks ofrecen las siguientes ventajas:

- **Declarativo**: Los StyleBooks se escriben en una sintaxis declarativa en lugar de imperativa. StyleBooks le permite centrarse en describir el resultado o el «estado deseado» de la configuración en lugar de las instrucciones paso a paso sobre cómo lograrlo en una instancia ADC particular. Citrix ADM calcula la diferencia entre el estado existente en un ADC y el estado deseado especificado, y realiza las modificaciones necesarias en la infraestructura. Dado que los StyleBooks utilizan una sintaxis declarativa, escrita en YAML, los componentes de un StyleBook se pueden especificar en cualquier orden, y Citrix ADM determina el orden correcto en función de sus dependencias calculadas.
- **Atomic**: cuando usas StyleBooks para implementar configuraciones, se despliega la configuración completa o no se despliega 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 Citrix ADC de una aplicación completa. La configuración de la aplicación se puede abstraer mediante el uso de parámetros. Por lo tanto, los usuarios que crean configuraciones a partir de un StyleBook pueden interactuar con una interfaz sencilla que consiste en rellenar algunos parámetros para crear lo que puede ser una configuración ADC compleja. Las configuraciones creadas a partir de StyleBooks no están vinculadas a la infraestructura. De este modo, se puede implementar una única configuración en una o varias instancias de ADC y también se puede mover de una instancia a otra.
- **Interfaz de usuario generada automáticamente**: Citrix ADM genera automáticamente formu-

larios de interfaz de usuario utilizados para rellenar los parámetros del StyleBook cuando se realiza la configuración mediante la interfaz gráfica de usuario de Citrix ADM. Los autores de StyleBook no necesitan aprender un nuevo lenguaje de interfaz gráfica de usuario ni crear páginas y formularios de interfaz de usuario por separado.

- Basado en**API:**todas las operaciones de configuración se admiten mediante la GUI de Citrix ADM o mediante las API REST. Las API se pueden usar en modo sincrónico o asíncrono. Además de las tareas de configuración, las API de StyleBooks también permiten descubrir el esquema (descripción de los parámetros) de cualquier StyleBook en tiempo de ejecución.

Puede utilizar un StyleBook para crear varias configuraciones. Cada configuración se guarda como un paquete de configuración. Por ejemplo, considere que tiene un StyleBook que define una configuración típica de la aplicación de equilibrio de carga HTTP. Puede crear una configuración con valores para las entidades de equilibrio de carga y ejecutarla en una instancia de Citrix ADC. Esta configuración se guarda como un paquete de configuración. Puede 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. Se guarda un paquete de configuración tanto en Citrix ADM como en la instancia de ADC en la que se ejecuta la configuración.

Puede utilizar StyleBooks predeterminados, incluidos con Citrix ADM, para crear configuraciones para su implementación, o diseñar sus propios StyleBooks e importarlos a Citrix ADM. Puede usar los StyleBooks para crear configuraciones mediante la GUI de Citrix ADM o mediante las API.

Este documento incluye la siguiente información:

- Cómo ver StyleBooks
- StyleBooks predeterminados
- StyleBooks desarrollados para aplicaciones empresariales
- StyleBooks personalizados
- APIs en StyleBooks
- Gramática de StyleBooks

Panel de seguridad de aplicaciones

November 16, 2022

El panel **de seguridad de aplicaciones** proporciona información general sobre las métricas de seguridad para las aplicaciones detectadas/con licencia. Este panel muestra la información de ataques de seguridad para las aplicaciones detectadas o con licencia, como ataques de sincronización, ataques de ventanas pequeñas o ataques de inundación DNS.

Para ver las métricas de seguridad en el panel de seguridad de la aplicación:

1. Diríjase a **Seguridad > Panel de seguridad**.

2. Seleccione la dirección IP de la instancia en la lista Instancia.

   Los informes incluyen la siguiente información para cada aplicación:

   - **Índice de amenazas**. Sistema de clasificación de un solo dígito que indica la importancia de los ataques a la aplicación. Cuanto más críticos sean los ataques a una aplicación, mayor será el índice de amenazas para esa aplicación. Los valores oscilan entre 1 y 7.

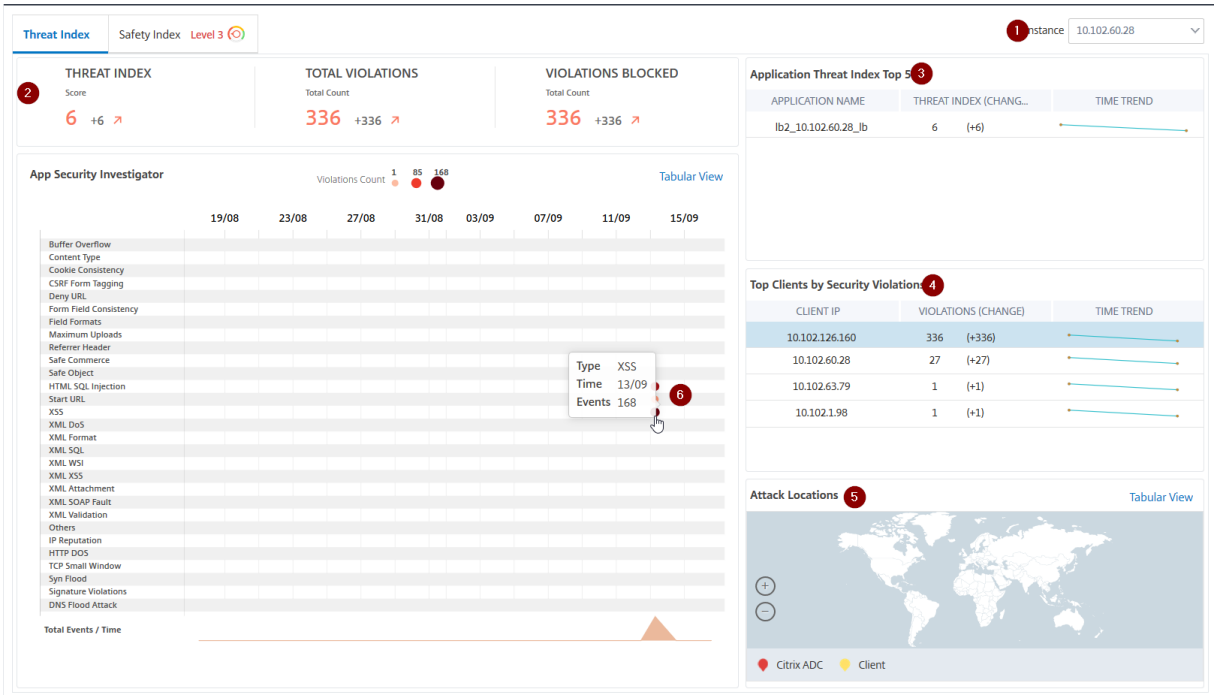
     El índice de amenazas se basa en la información de ataque. La información relacionada con el ataque, como el tipo de infracción, la categoría del ataque, la ubicación y los detalles del cliente, proporciona una visión de los ataques a la aplicación. La información de infracción se envía a Citrix ADM 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 Citrix ADC para proteger las aplicaciones de amenazas y vulnerabilidades externas. Cuanto menores sean los riesgos de seguridad de una aplicación, mayor será el índice de seguridad. Los valores oscilan entre 1 y 7.

     El índice de seguridad considera tanto la configuración del firewall de aplicaciones como la configuración de seguridad del sistema Citrix ADC. Para un valor de índice de seguridad elevado, ambas configuraciones deben ser fuertes. Por ejemplo, si se realizan comprobaciones rigurosas del firewall de las aplicaciones, pero no se proporcionan medidas de seguridad del sistema Citrix ADC, 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 Citrix ADC 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.

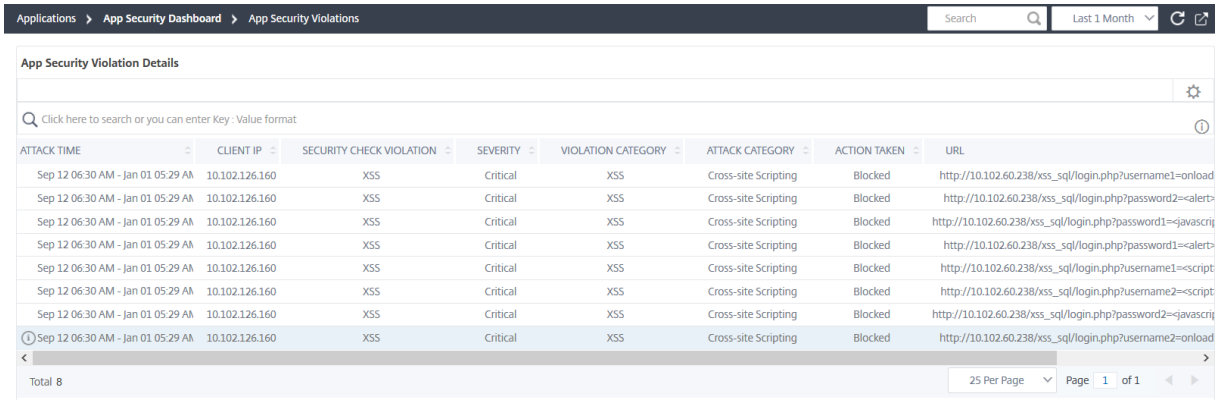
4 : muestra las violaciones de seguridad según los clientes. Se muestra el gráfico App Security Investigator para cada cliente. Puede hacer clic en cada IP de cliente para ver los resultados.

5: Muestra las infracciones en la vista de mapa y en la vista tabular.

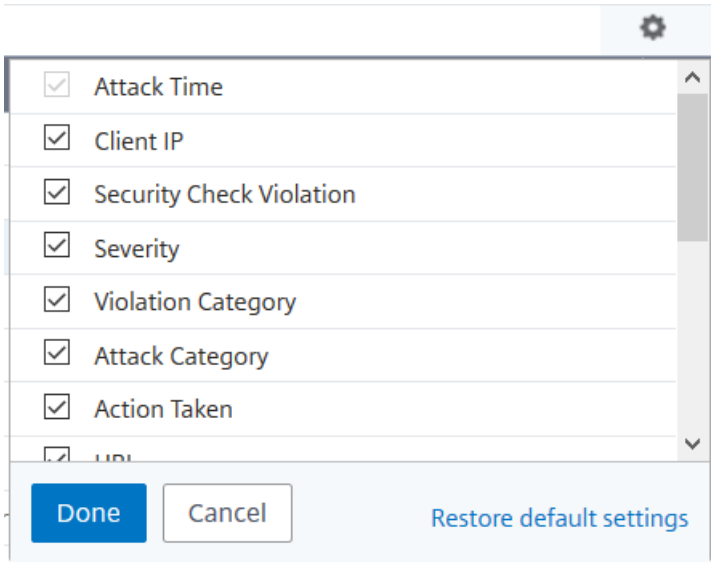
6 : muestra los detalles de la infracción. Al situar el puntero del ratón sobre el gráfico, se muestran los detalles como el tipo de infracción, la hora del ataque y el total de eventos.

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.



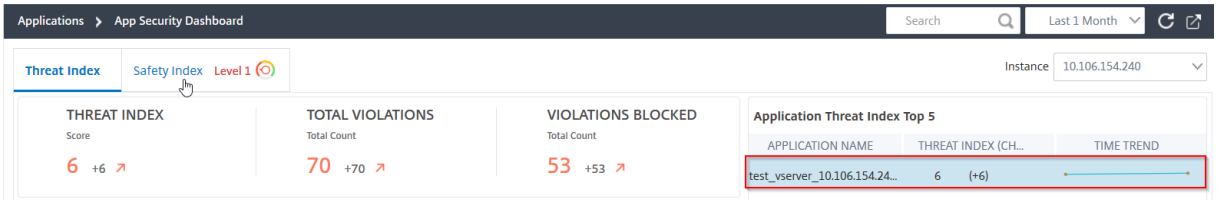
Detalles del índice de seguridad

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.

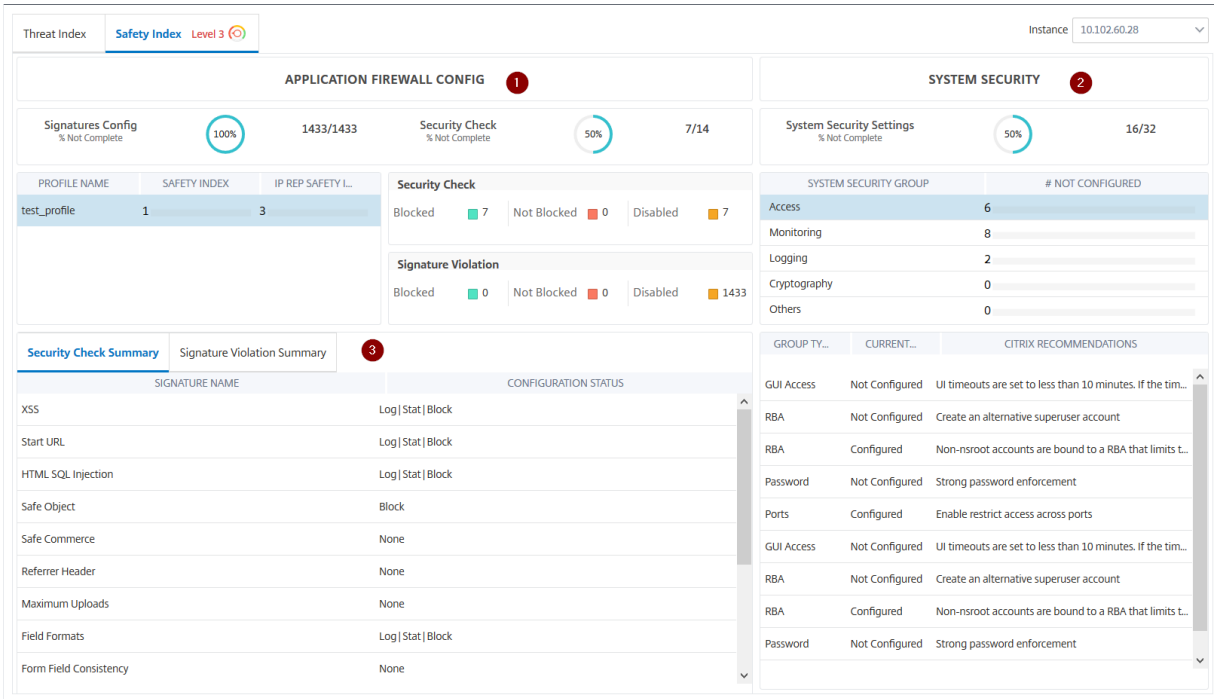
El resumen del índice de seguridad proporciona información sobre la eficacia de las siguientes configuraciones de seguridad:

- **Configuración del firewall de aplicaciones**. Muestra cuántas entidades de firma y seguridad no están configuradas.
- **Seguridad del sistema Citrix ADM**. Muestra cuántas opciones de seguridad del sistema no están configuradas.

Para ver los detalles del **índice de seguridad**, seleccione un servidor/aplicación virtual y haga clic en la ficha **Índice de seguridad**.



Se muestran los detalles.



1: Muestra la información detallada de las configuraciones de Application Firewall.

2: Muestra la información detallada de Seguridad del sistema. Haga clic en cada grupo de seguridad para obtener detalles sobre el estado 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.

Ver detalles de infracciones de seguridad de la aplicación

December 12, 2022

Las aplicaciones web que están expuestas a Internet se han vuelto vulnerables a los ataques drásticamente. Citrix ADM le permite visualizar detalles de infracciones accionables para proteger las aplicaciones contra ataques. Vaya a **Seguridad** > **Infracciones de seguridad** para una solución de un solo panel para:

- Visualice las aplicaciones con visibilidad completa de los detalles de amenazas asociados tanto a la información de seguridad como a la información sobre robots
- Acceda a las infracciones de seguridad de la aplicación en función de sus categorías como **Network**, **Bot** y **WAF**
- Tomar medidas correctivas para proteger las aplicaciones

La página **Infracciones de Seguridad** tiene las siguientes opciones:

- **Descripción general de la aplicación** : muestra una descripción general de las aplicaciones que tienen infracciones totales, infracciones de WAF y bot totales, infracciones por país, etc. Para obtener más información, consulte Descripción general de la aplicación.
- **Todas las infracciones** : muestra los detalles de infracción de seguridad de la aplicación. Para obtener más información, consulte Todas las infracciones.

Configuración

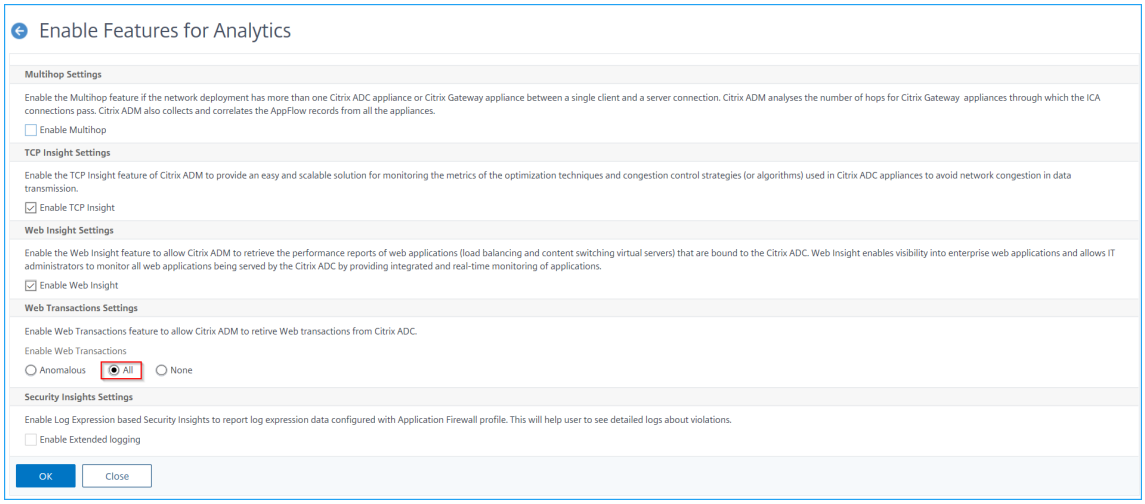
Para ver las infracciones, debe:

- Seleccione **Configuración de transacciones web** para **todos**
- Asegúrese de que el **recopilador de métricas** esté habilitado. De forma predeterminada, **Metrics Collector** está habilitado en la instancia de Citrix ADC. 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 de transacciones web**, selecciona **Todas**.

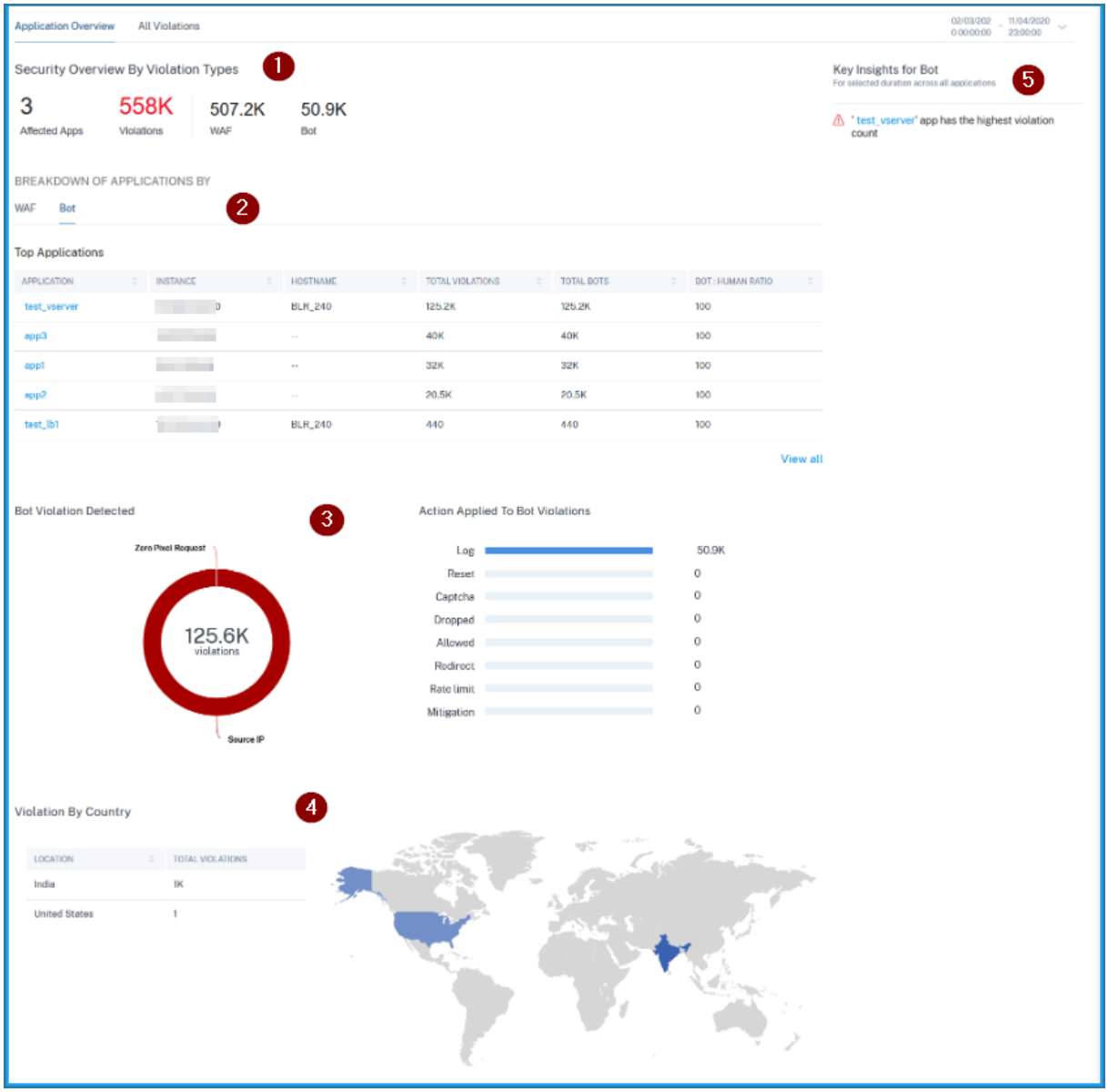


4. Haga clic en **OK**.

Descripción general de la aplicación

December 12, 2022

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.

Para obtener más información sobre los robots y los conocimientos de seguridad, consulte:

- Bot Insight
- Security Insight

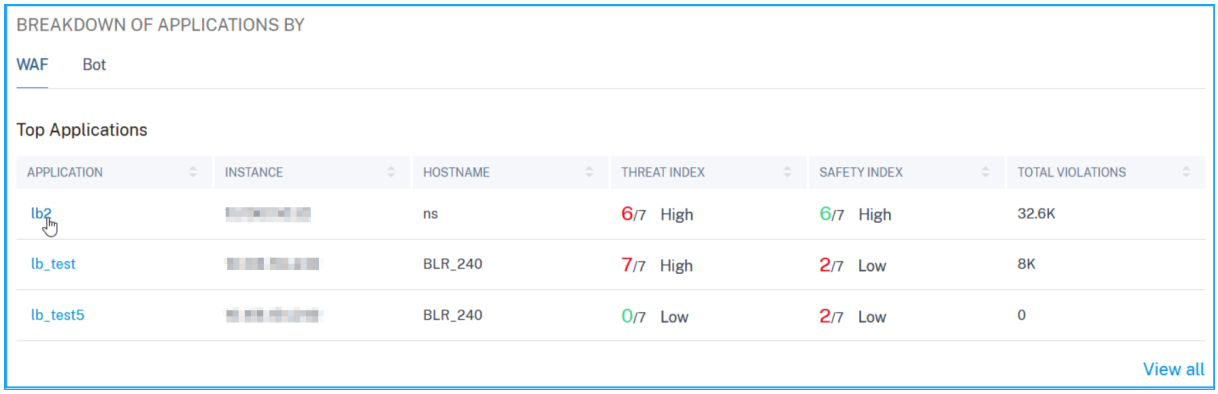
Categorías de infracción

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

WAF	Bot
Otros	Host
Reputación IP	Crawler
HTTP DOS	Buscador de alimentación
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

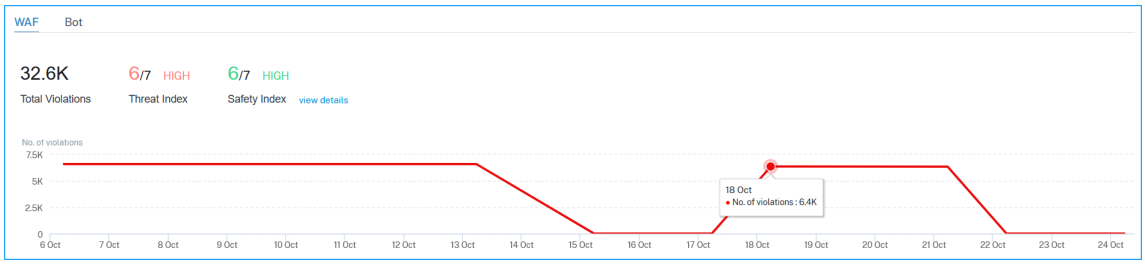
Haga clic en una aplicación en la opción **Aplicaciones principales** o en la opción **Ver todo** para ver los detalles de WAF.



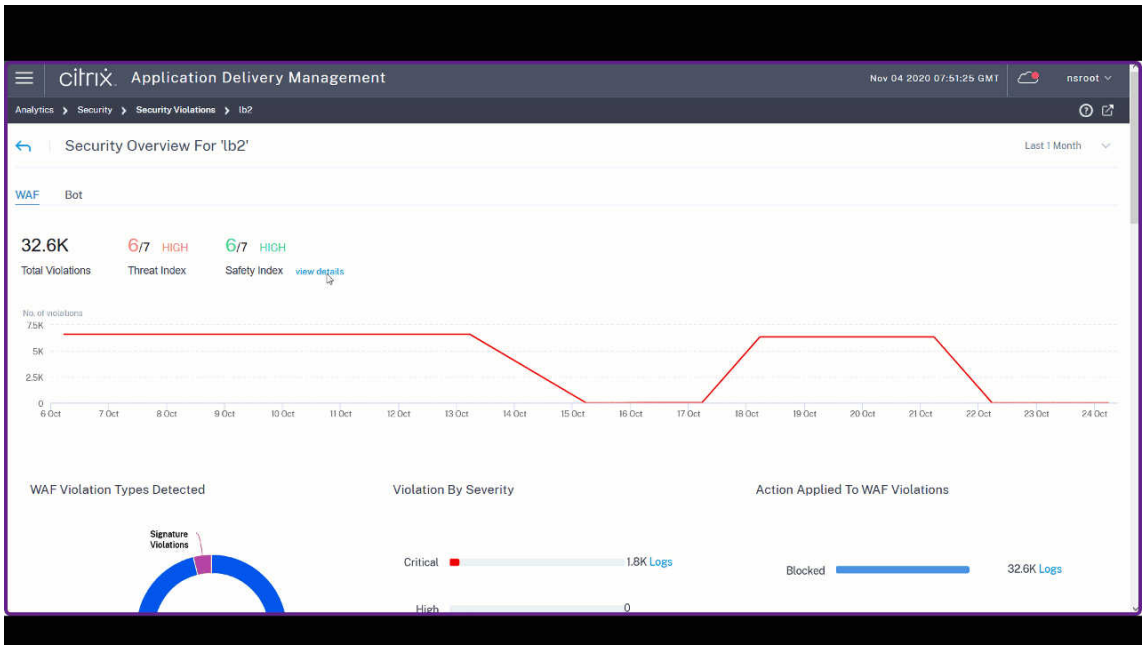
> **Nota**
>
> Si selecciona una aplicación personalizada, puede ver los detalles de las aplicaciones consolidadas en la página de información **general de seguridad** . En la lista, seleccione una aplicación para ver los detalles de la aplicación seleccionada.

Aparecerá la página **Visión General de Seguridad** de la aplicación seleccionada. En **WAF**, puede ver:

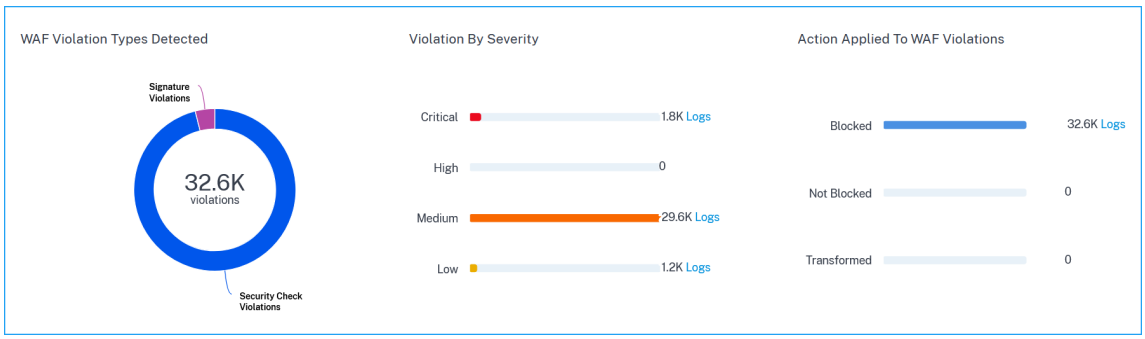
- Una vista gráfica que indica el total de infracciones, la puntuación del índice de amenaza y la puntuación del índice de seguridad de la aplicación.



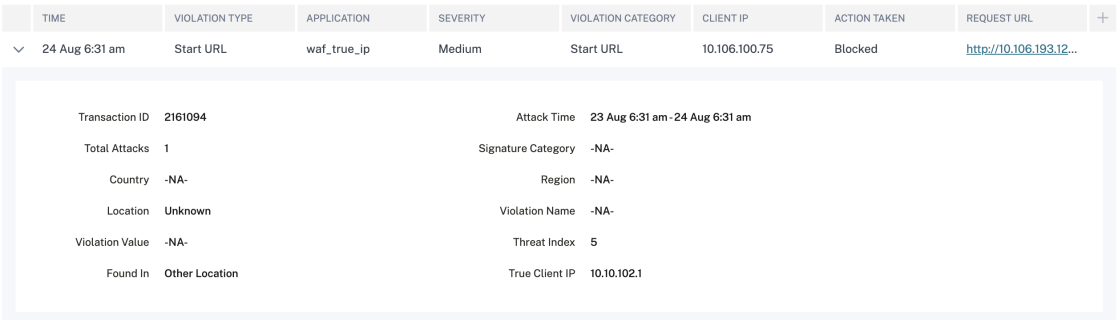
Haga clic en **Ver detalles** para ver los detalles de configuración de Application Firewall y Citrix ADC System Security.



- 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.

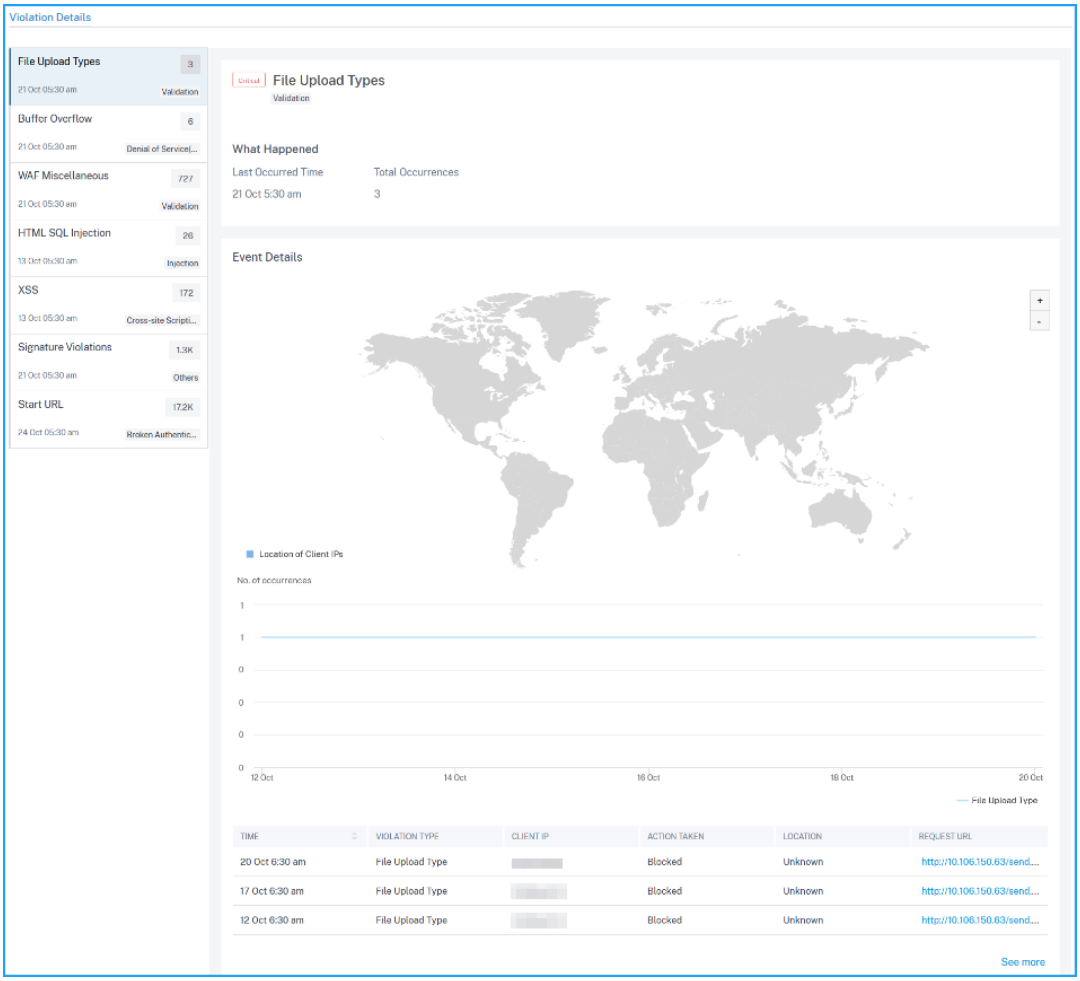


- Las infracciones afectadas en la aplicación. En **Detalles de la infracción**, puede ver los detalles de la infracción afectada.

  > **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.

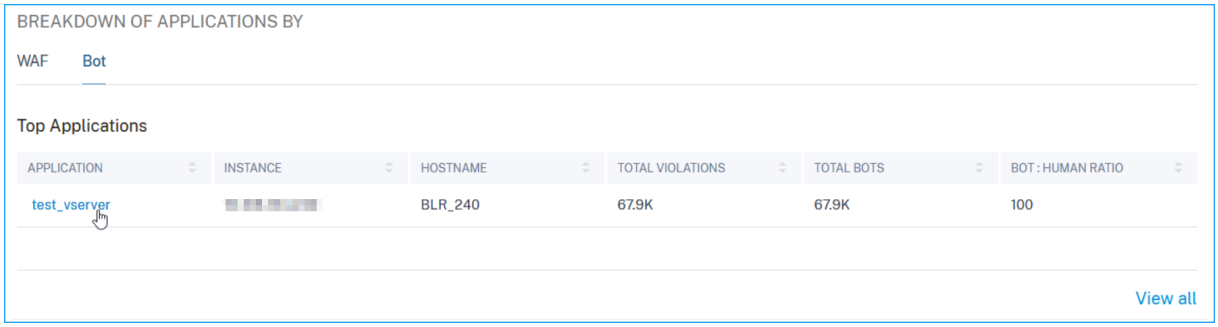
  Haga clic en cada infracción para ver detalles como:

  - **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 las **principales aplicaciones** o de la opción **Ver todas** para ver los detalles del bot.

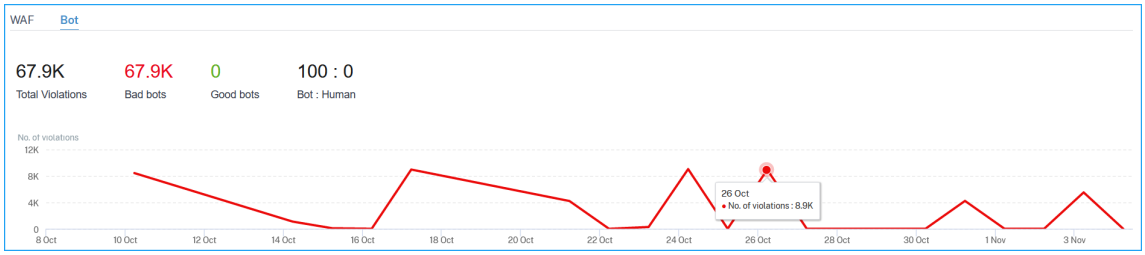


> **Nota**
>
> Si selecciona una aplicación personalizada, puede ver los detalles de las aplicaciones consolidadas en la página de información **general de seguridad** . En la lista, seleccione una aplicación

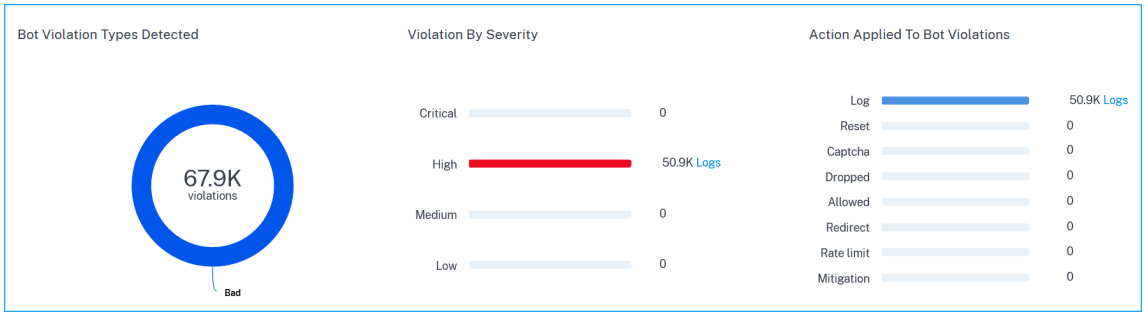
> para ver los detalles de la aplicación seleccionada.

Aparecerá la página **Visión General de Seguridad** de la aplicación seleccionada. En **Bot**, puede ver:

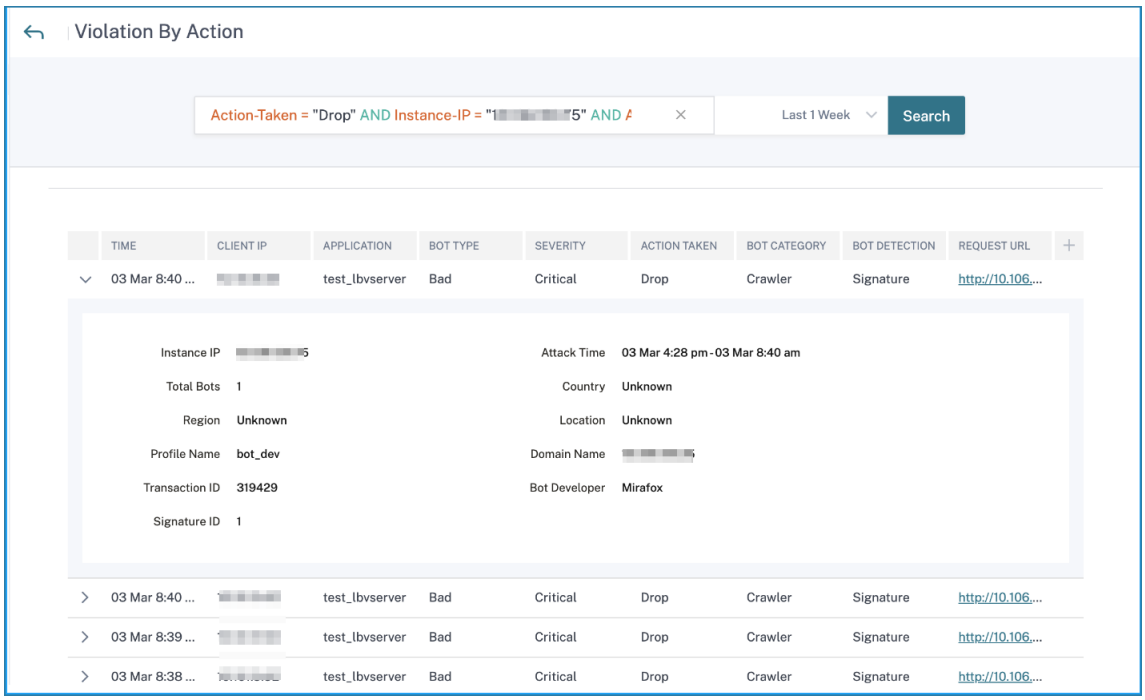
- Gráfico que indica bots totales, bots incorrectos totales, bots buenos totales y relación total entre usuarios humanos y bots que acceden a la aplicación.



- Las infracciones basadas en los tipos de bot, la gravedad y las acciones aplicadas.

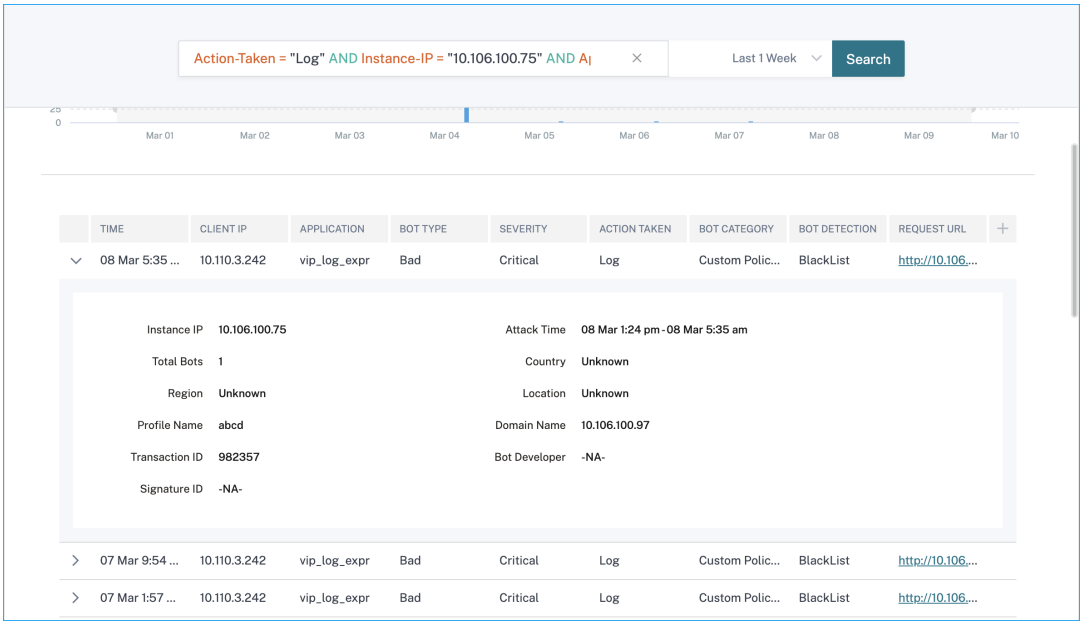


  Haga clic en **Registros** para ver los detalles en función de la gravedad o las acciones realizadas. Si un bot detectado es un bot de tipo Firma, puede ver más detalles como desarrollador de bot e ID de firma. El identificador de firma le permite identificar si el bot detectado es un bot bueno o un 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.



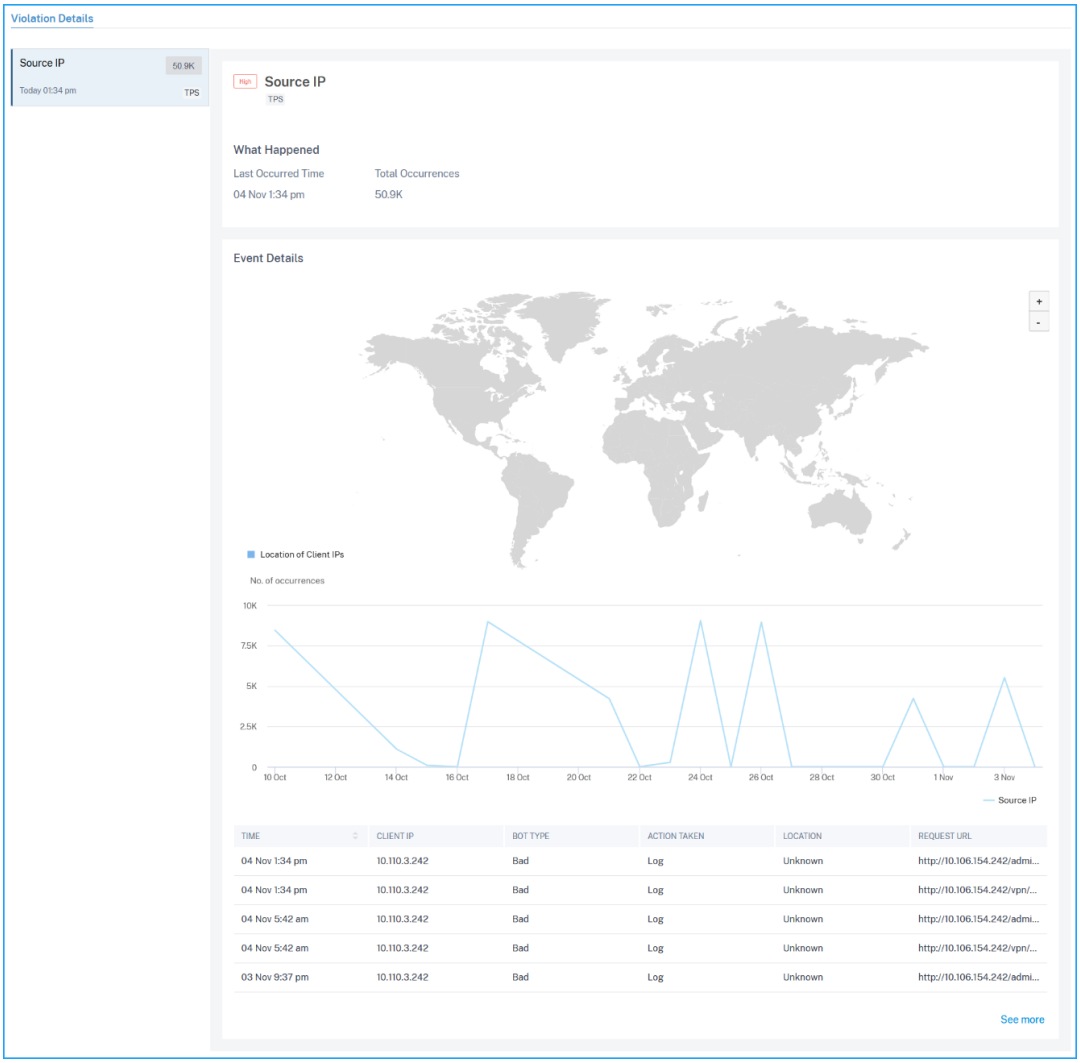
- Las infracciones afectadas en la aplicación. En **Detalles de la infracción**, puede ver los detalles de la infracción afectada.

  Nota

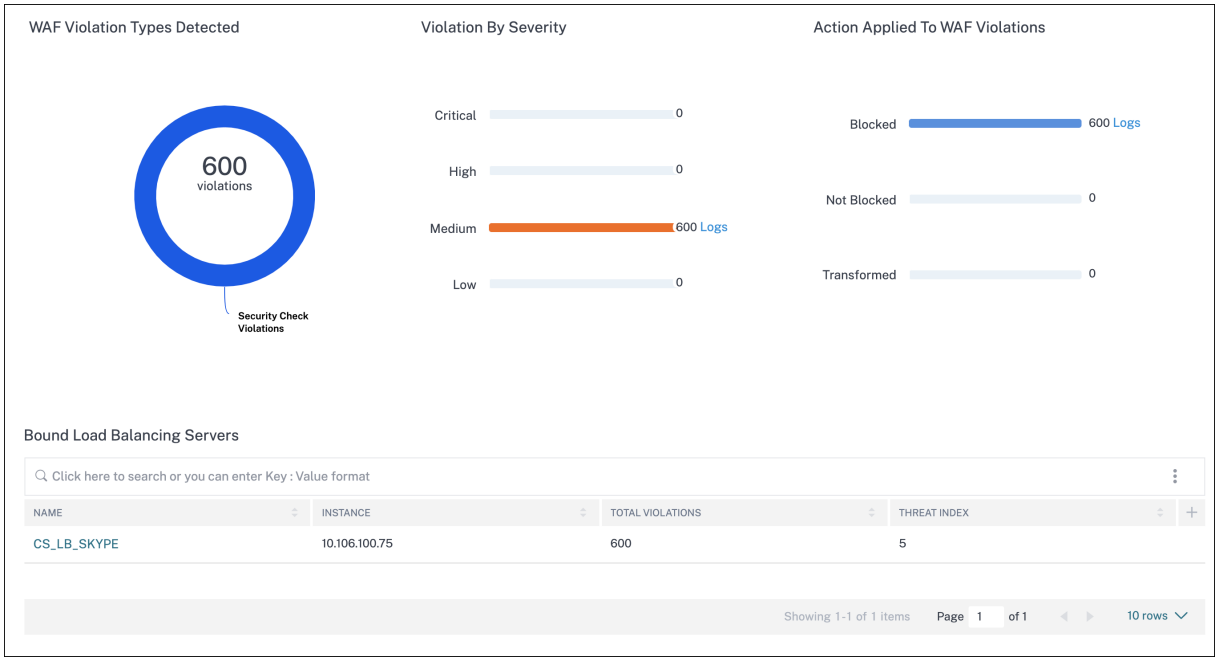
> En el caso de una aplicación personalizada, se muestran las infracciones aplicables a todas las aplicaciones. Puede hacer clic en una aplicación de la lista para ver las infracciones afectadas en la aplicación seleccionada.

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**, podrá ver la lista de servidores de equilibrio de carga enlazados al servidor virtual de conmutación de contenido.



Ver historial de eventos

Haga clic en la ficha **Eventos** para ver los eventos bot y WAF.

Todas las infracciones

December 12, 2022

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 Citrix ADM, asegúrese de:

- Tiene una licencia premium para la instancia Citrix ADC (para infracciones de WAF y BOT).
- Ha aplicado la licencia a los servidores virtuales de equilibrio de carga o conmutación de contenido (para WAF y BOT). Para obtener más información, consulte Administrar licencias en servidores virtuales.
- Habilita más configuraciones. Para obtener más información, consulte el procedimiento disponible en Configuración.

Categorías de infracción

Citrix ADM 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
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	Analizador de vulnerabilidades
	XML DoS	Se ha superado la espera de DeviceFP
	Formato XML	DeviceFP no válido
	XML WSI	Respuesta Captcha no válida
	XML SSL	Se han superado los intentos de Captcha
	Datos adjuntos XML	Respuesta Captcha válida
	Error SOAP de XML	Cliente Captcha Silenciado
	Validación XML	Tiempo de espera de Captcha superado
	Otros	Excedido el límite de tamaño de solicitud
	Reputación IP	Límite de tasa superado
	HTTP DOS	Lista de bloqueos (IP, subred, expresión de directiva)

Red	WAF	Bot
	Ventana pequeña TCP	Lista de permitidos (IP, subred, expresión de directiva)
	Infracción de firma	Solicitud de cero píxeles
	Tipo de carga de archivo	IP de origen
	Scripting entre sitios JSON	Host
	JSON SQL	Ubicación geográfica
	JSON DOS	URL
	Inyección de	Crawler
	Secuestro de cookies	Buscador de alimentación
	Bloquear palabra clave	Comprobador de vínculos
	Palabra clave de bloqueo de JSON	Márketing
	Comercio seguro	
	Objeto seguro	
	Inyección HTML SQL	
	URL de inicio	
	Gramática de la inyección	
	Gramática de inyección JSON SQL	

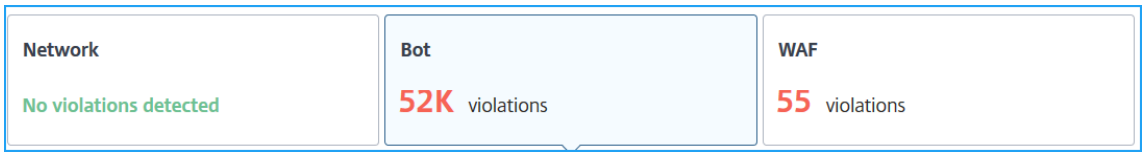
> Nota
>
> Para ver las infracciones de **adquisición de cuentas**, **analizadores de sitios web**y **Scrapers de contenido**, debe configurar las opciones en Citrix ADM. Consulte el requisito previo mencionado en la página de detalles de infracción.

Panel de infracciones de seguridad

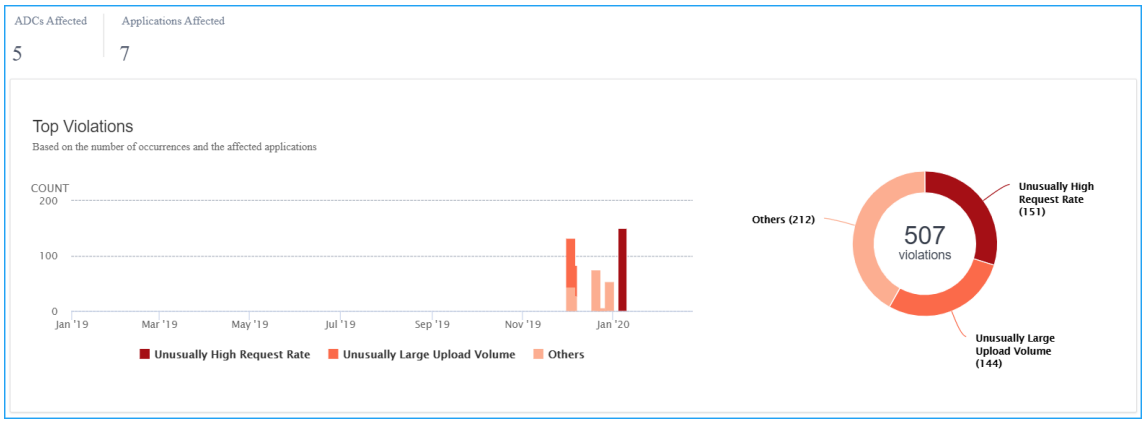
En el panel de control de infracciones de seguridad, puede ver:

- Se han producido infracciones totales en todas las instancias y aplicaciones de ADC. Las infracciones totales se muestran en función de la duración de tiempo seleccionada.

- Total de infracciones en cada categoría.



- Total de ADC afectados, total de aplicaciones afectadas e infracciones superiores en función del total de incidencias y de las aplicaciones afectadas.



Detalles de infracción

Para cada infracción, Citrix ADM supervisa el comportamiento durante un período de tiempo específico y detecta las infracciones por 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.

Gateway API

November 16, 2022

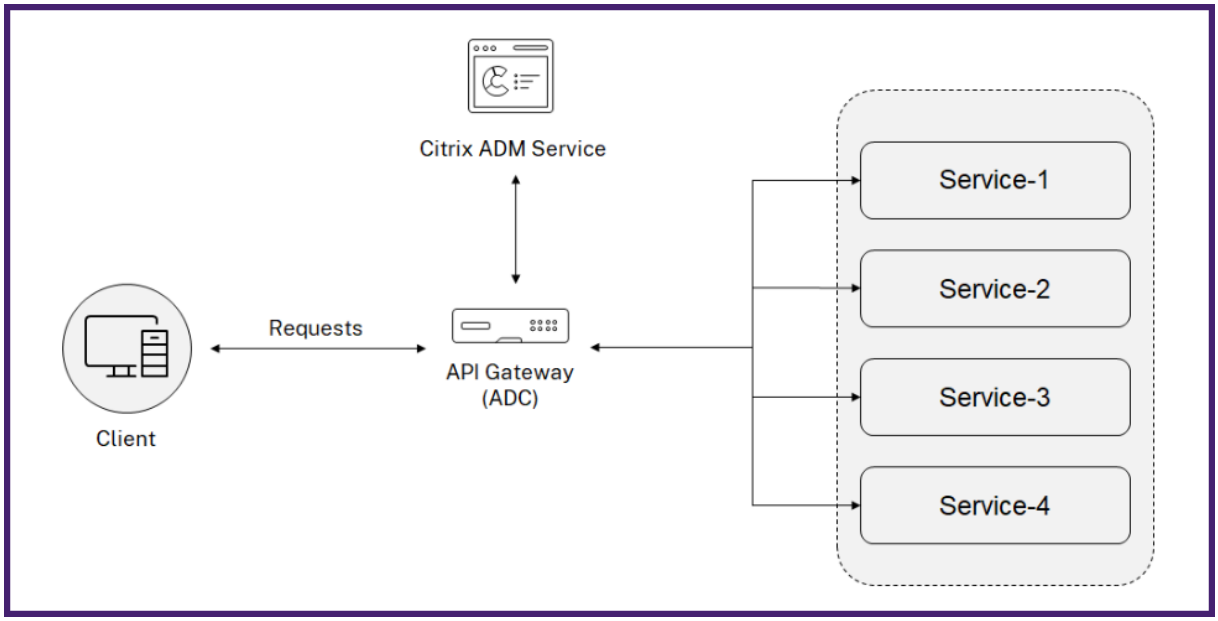
Una puerta de enlace API actúa como punto de entrada para todas las solicitudes a los extremos de la API. Además, garantiza un acceso seguro y confiable a todos los endpoints y microservicios de API en su sistema.

Una puerta de enlace API ofrece proxy de todas las solicitudes y respuestas entre sus clientes/aplicaciones API y los servicios de API back-end. Le ayuda a configurar, administrar y proteger los puntos finales de API. También puede crear y administrar definiciones de API de una de las siguientes maneras:

- Cargar archivo de especificación de Swagger OAS
- Cree su propia definición de API

Para obtener más información, consulte Crear o cargar una definición de API.

La siguiente imagen describe cómo la puerta de enlace API recibe la solicitud del cliente y envía la respuesta desde los servicios API back-end:



> **Nota:**
>
> En Citrix ADM, esta función está disponible para los usuarios que tienen licencias Premium o Advanced.

Ventajas de la puerta de enlace API

La puerta de enlace API le ofrece las siguientes ventajas:

- **Protege los extremos**de la API: la puerta de enlace de API agrega una capa de seguridad y protege sus endpoints API y servidores API back-end de ataques como:
  - Desbordamiento de búfer
  - Inyección SQL
  - Scripts entre sitios
  - Denegación de servicio (Dos)
- **Supervisa y mejora el rendimiento**de la API: la puerta de enlace API proporciona servicios como descarga SSL, Autenticación, Autorización, Limitación de velocidad y mucho 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 API**: la puerta de enlace API abstrae la complejidad de su infraestructura API back-end.
- **Detección de puntos finales de API**: la puerta de enlace API descubre los extremos de API que se encuentran en su organización y se agrega a la página **Descubrimiento de API** .

Administrar puerta de enlace API

Como administrador, puede crear definiciones de API e implementar las instancias de API en una puerta de enlace de API (ADC) en Citrix ADM. Para obtener más información, consulte:

- Agregar una definición de API
- Implementar una instancia de API

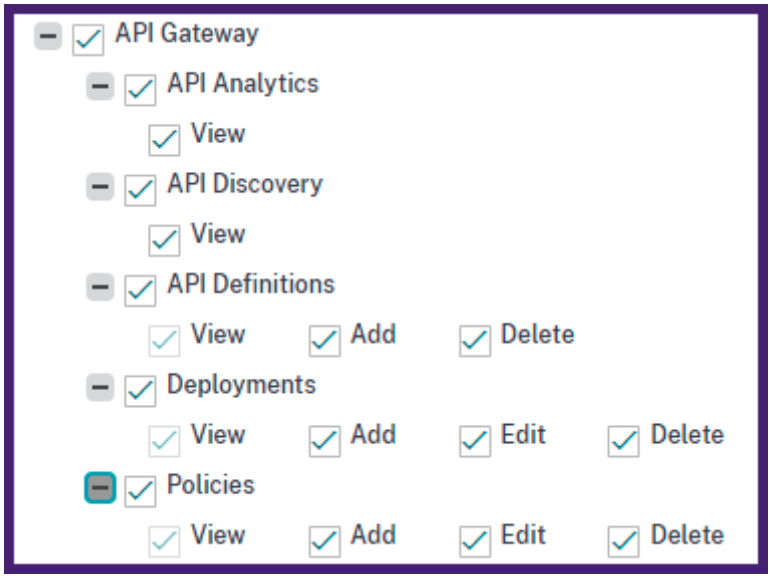
En una puerta de enlace API, puede aplicar directivas de seguridad. Para saber cómo crear una directiva de API, consulte Agregar directivas a una implementación de API.

Conceder permisos de administración y configuración de gateway de API

Como administrador, puede crear una directiva de acceso para otorgar permisos a los usuarios para la configuración y administración de la puerta de enlace API. 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, **API Gateway**.

5. Seleccione las páginas de **API Gateway** necesarias. A continuación, seleccione los permisos que quiere conceder.



> **Importante**
>
> Asegúrese de conceder permisos para las características necesarias para utilizar una puerta de enlace 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 directivas de acceso, consulte Configurar las directivas de acceso en Citrix ADM.

Integración con Splunk

February 13, 2023

Ahora puede integrar Citrix ADM con Splunk para ver los análisis de las infracciones de WAF y Bot en su panel de control de Splunk. El complemento Splunk le permite:

- Combine todas las demás fuentes de datos externas.
- Proporcione una mayor visibilidad de los análisis en un lugar centralizado.

Citrix ADM recopila eventos de Bot y WAF 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 las infracciones de WAF y Bot en el panel de control de Splunk.

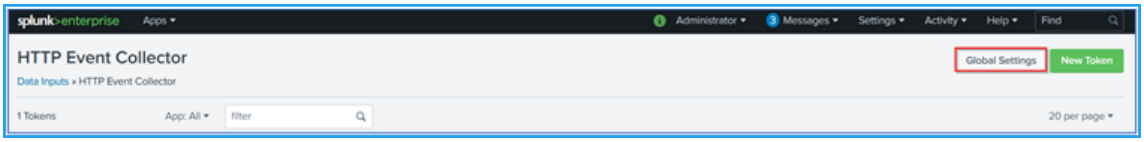
Requisitos previos

Para la integración con Splunk, debe:

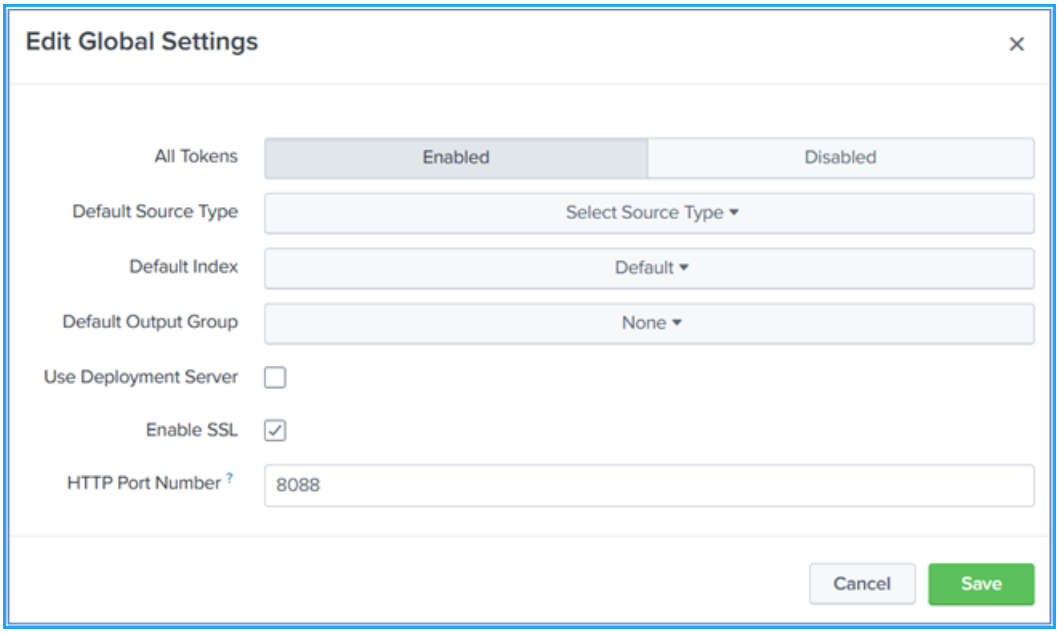
- Configurar la configuración global
- Configure el punto final del recopilador de eventos HTTP en Splunk
- Instale el complemento del modelo de información común (CIM) de Splunk
- Instale el normalizador CIM de Citrix
- Agregue los detalles del recopilador HTTP y del token de Splunk

Configurar la configuración global

1. Inicia sesión en Splunk.
2. Vaya a **Configuración > Entradas de datos > Recopilador de eventos HTTP**.
   Aparece la página **del recopilador de eventos HTTP** .
3. Haga clic en **Configuración global**.



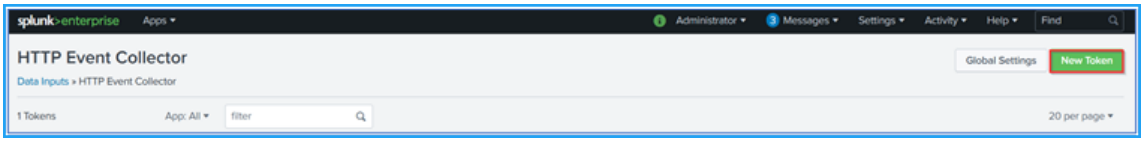
4. Especifique los siguientes parámetros y haga clic en **Guardar**.



> **Nota**
>
> De forma predeterminada, el número de puerto HTTP indica el puerto predeterminado. Si tiene cualquier otro número de puerto preferido, puede especificar el número de puerto requerido.

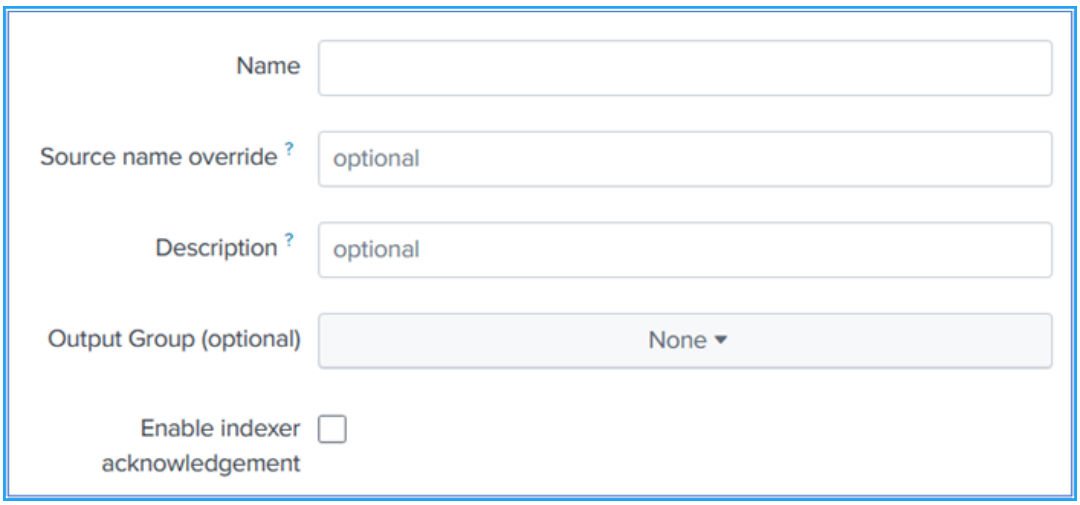
Configure el punto final del recopilador de eventos HTTP en Splunk

1. Inicia sesión en Splunk.
2. Vaya a **Configuración > Entradas de datos > Recopilador de eventos HTTP**.
   Aparece la página **del recopilador de eventos HTTP** .
3. Haga clic en **Nuevo token**.



4. Especifique lo siguiente:
   a) **Nombre**: especifique un nombre de su elección.
   b) **Anulación del nombre de origen (opcional)**: si establece un valor, anula el valor de origen del recopilador de eventos HTTP.
   c) **Descripción (opcional)**: especifique una descripción.
   d) **Grupo de salida (opcional)**: de forma predeterminada, esta opción aparece seleccionada como Ninguna.

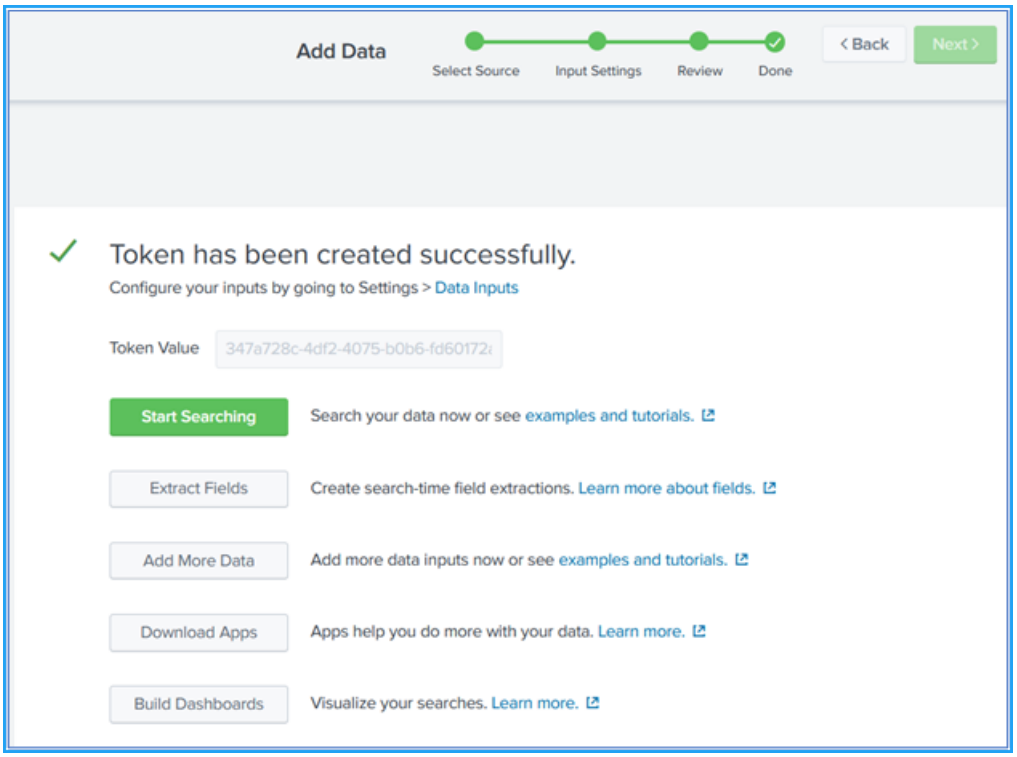
e) **Habilitar el reconocimiento del indexador**: de forma predeterminada, esta opción no está seleccionada.



f) Haga clic en **Siguiente**

g) En la página **Configuración de entrada**, especifique el **tipo de fuente**, el **contexto de la aplicación, elíndice**y, después, haga clic en**Revisar**.

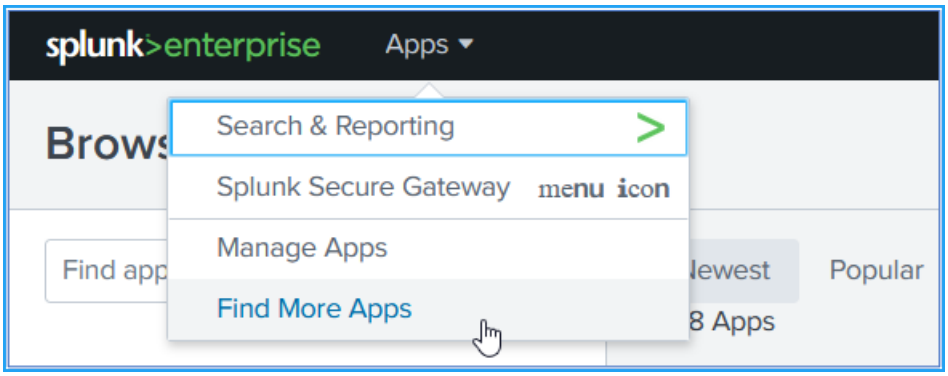
h) Compruebe si todo lo que ha especificado es correcto y, a continuación, haga clic en **Enviar**.
Se genera un token. Debe usar este token cuando agregue detalles en Citrix ADM.



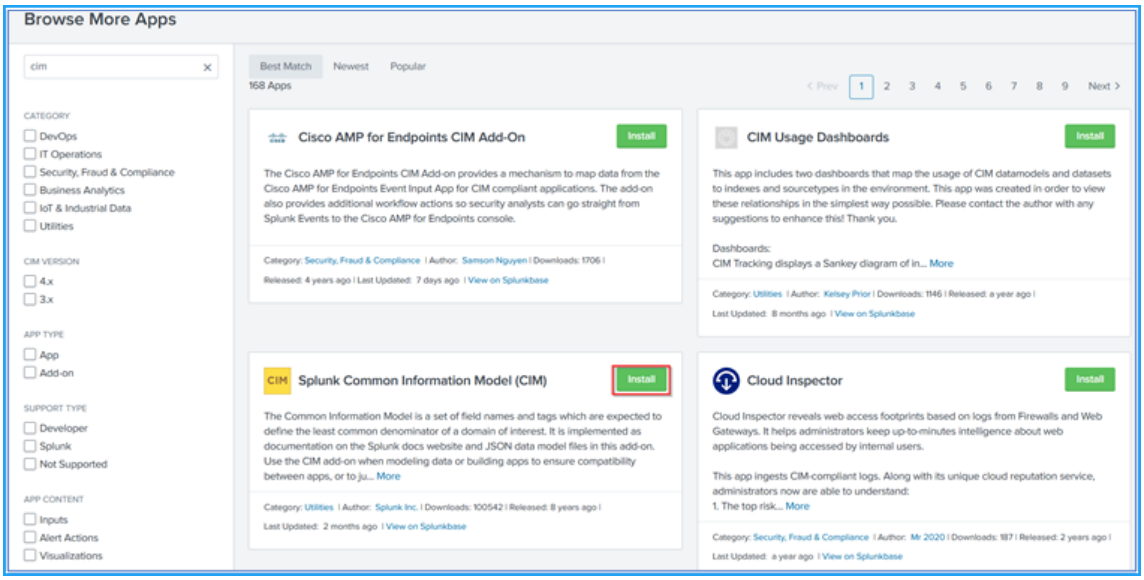
Instale el modelo de información común de Splunk

En Splunk, debe instalar el CIM de Splunk para asegurarse de que los datos se rellenen en el panel de control.

1. Inicia sesión en Splunk.
2. Vaya a **Aplicaciones > Buscar más aplicaciones**.



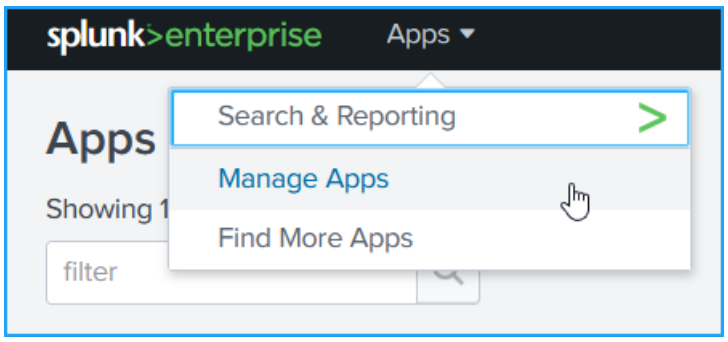
3. Escriba **CIM** en la barra de búsqueda y pulse **Entrar** para obtener el complemento del **modelo de información común (CIM) de Splunk** y haga clic en **Instalar**.



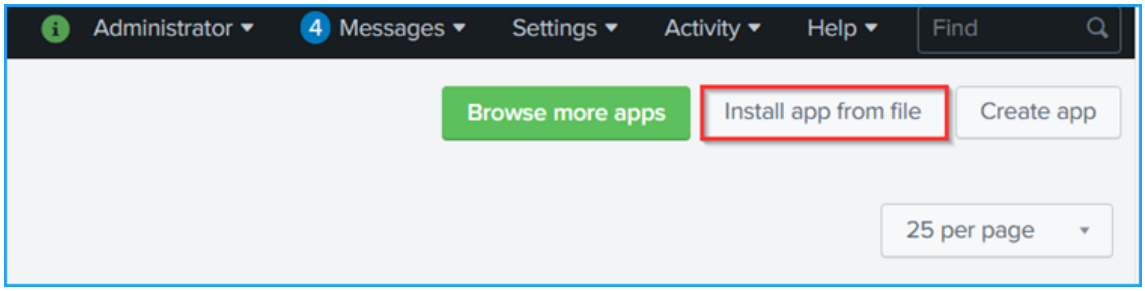
Instale el normalizador CIM de Citrix

Después de instalar el CIM de Splunk, debe instalar el normalizador CIM de Citrix para transformar los eventos en el CIM de Splunk.

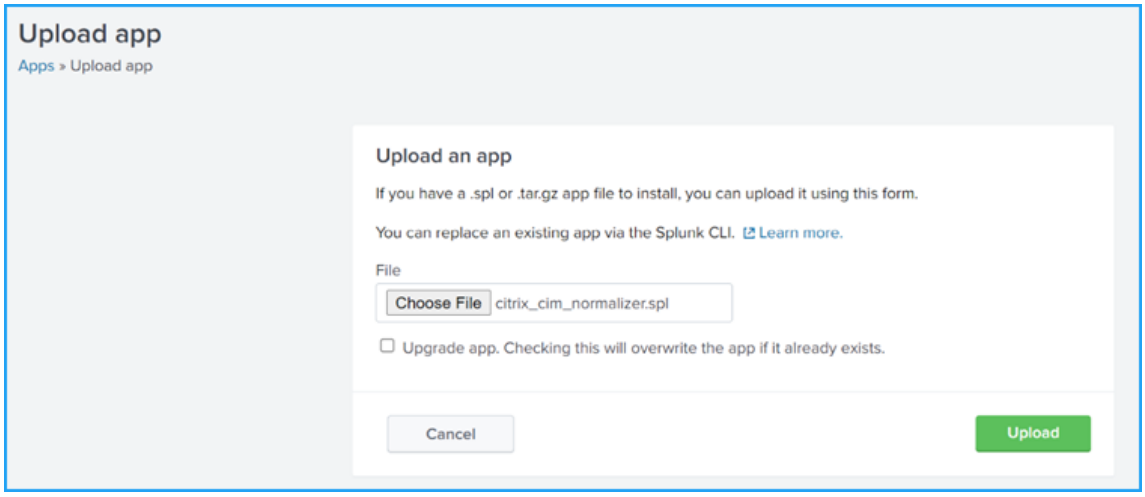
1. Inicie sesión en la página de descargas de Citrix y descargue el complemento CIM de Citrix para Splunk.
2. En el portal de Splunk, vaya a **Aplicaciones > Administrar aplicaciones**.



3. Haga clic en **Instalar aplicación desde un archivo**.



4. Cargue el archivo **.spl** o **.tgz** y haga clic en **Cargar**.



Recibirá un mensaje de notificación en la página **Aplicaciones** que indica que el complemento está instalado.

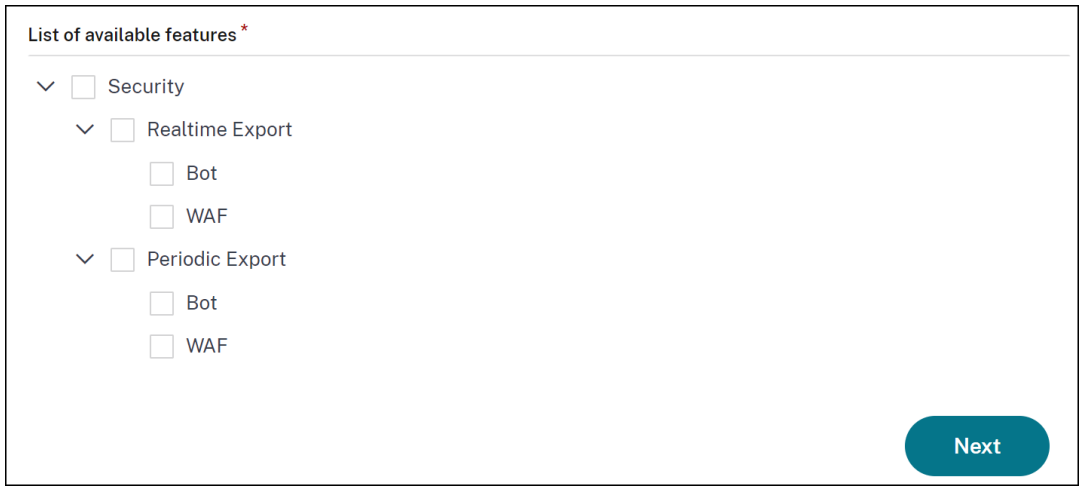
Agregue los detalles del recopilador HTTP y del token de Splunk

Después de generar un token, debe agregar detalles en Citrix ADM para integrarlo con Splunk.

1. Inicie sesión en Citrix ADM.
2. Vaya a **Configuración > Integración de ecosistemas**.
3. En la página **Suscripciones**, haga clic en **Agregar**.

4. En la ficha **Seleccionar funciones para suscribirse**, puede seleccionar las funciones que quiere exportar y hacer clic en **Siguiente**.

   - **Exportación en tiempo real** : las infracciones seleccionadas se exportan inmediatamente a Splunk.
   - **Exportación periódica** : las infracciones seleccionadas se exportan a Splunk en función de la duración que seleccione.



5. En la ficha **Especificar la configuración de exportación** :

   a) **Tipo de punto final** : seleccione **Splunk** en la lista.

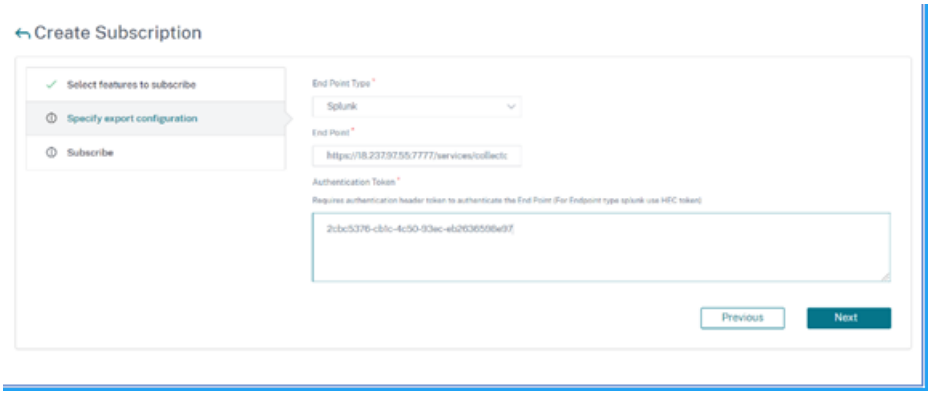
   b) **Punto final** : especifique los detalles del punto final de Splunk. El punto final debe estar en el formato https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event.

   > **Nota**
   >
   > Se recomienda utilizar HTTPS por motivos de seguridad.

   - **SPLUNK_PUBLIC_IP** : una dirección IP válida configurada para Splunk.
   - **SPLUNK_HEC_PORT** : indica el número de puerto que especificó durante la configuración del punto final del evento HTTP. El número de puerto predeterminado es 8088.
   - **Servicios/coleccionador/evento** : indica la ruta de la aplicación HEC.

   c) **Token de autenticación** : copie y pegue el token de autenticación de la página de Splunk.

   d) Haga clic en **Siguiente**.



6. En la página de **suscripción** :

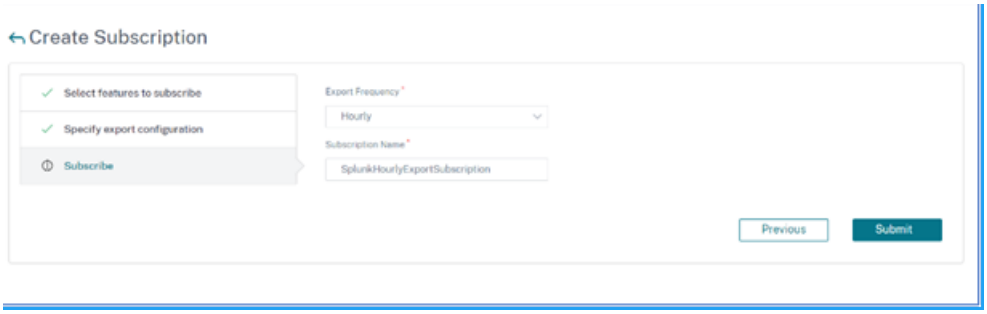
   a) **Frecuencia de exportación** : seleccione Diaria o Cada hora de la lista. Según la selección, Citrix ADM exporta los detalles a Splunk.

   > **Nota**
   >
   > Aplicable solo si ha seleccionado infracciones en la **exportación periódica**.

   b) **Nombre de la suscripción** : especifique un nombre de su elección.

   c) Seleccione la casilla **Activar notificaciones**.

   d) Haga clic en **Submit**.

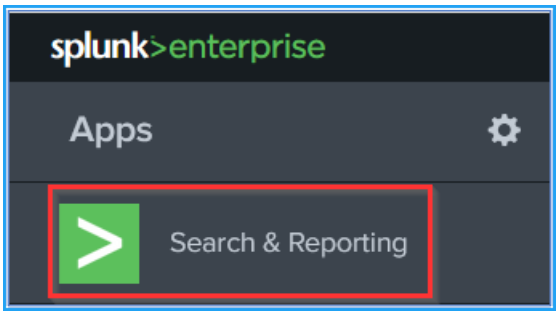


> **Nota**
>
> - Cuando se configura con la opción de **exportación periódica** por primera vez, los datos de las funciones seleccionadas se envían a Splunk inmediatamente. La siguiente frecuencia de exportación se realizará en función de su selección (diaria u horaria).
> - Cuando se configura con la opción **Realtime Export** por primera vez, los datos de las funciones seleccionadas se envían a Splunk inmediatamente tan pronto como se detectan las infracciones en Citrix ADM.

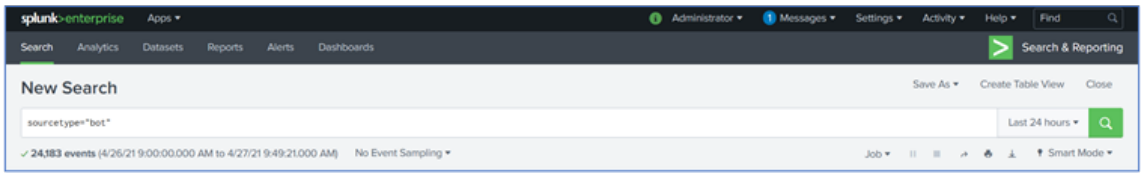
Verifique los detalles en Splunk

Después de agregar detalles en Citrix ADM, puede verificar si Splunk recibe los eventos.

1. En la página de inicio de Splunk, haga clic en **Buscar e informes**.

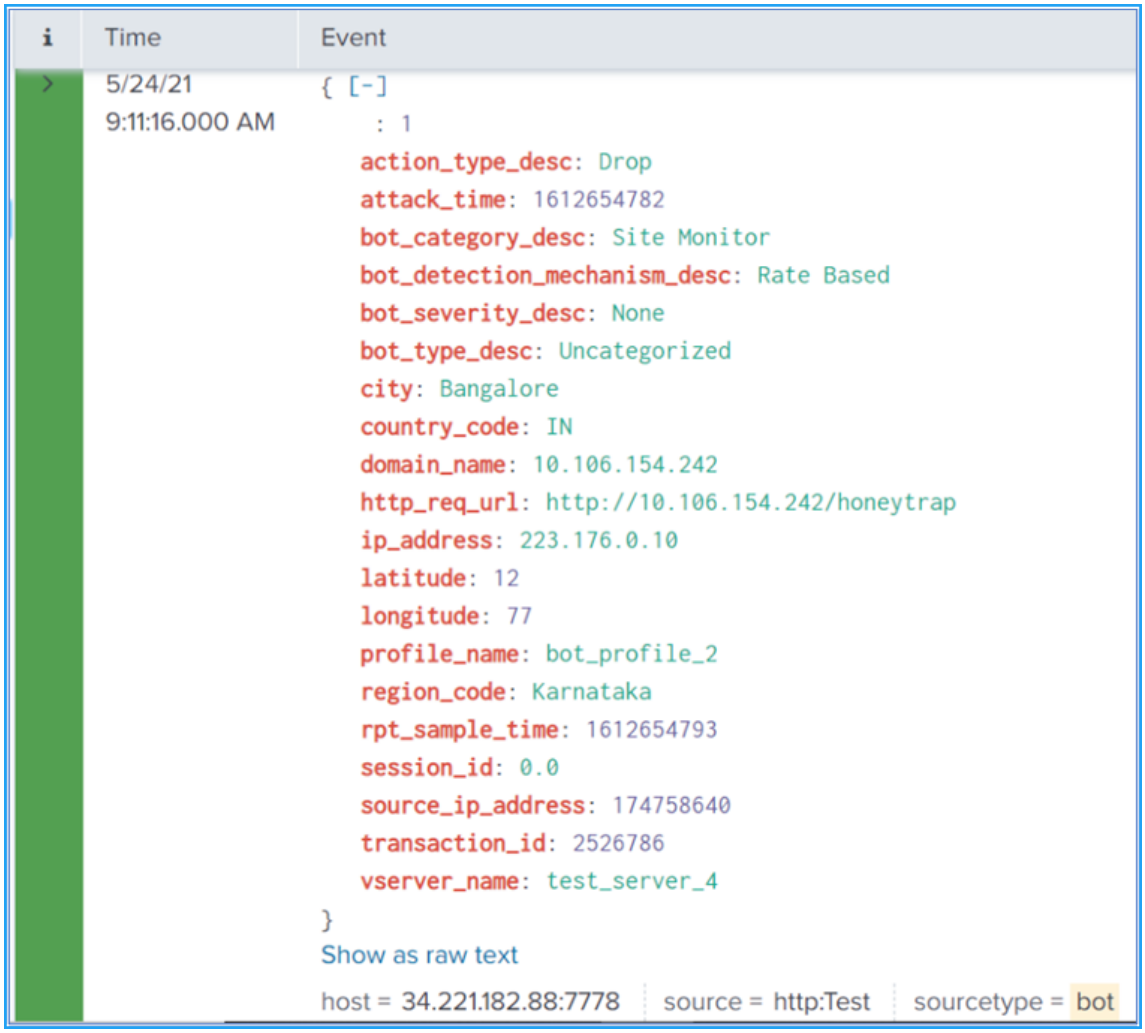


2. En la barra de búsqueda, escriba los detalles en la barra de búsqueda, seleccione la duración de la lista y haga clic en el icono de búsqueda o pulse Entrar. Por ejemplo, puede escribir `sourcetype=" bot"` o `sourcetype=" waf"` o `sourcetype="ml"` para comprobar los detalles.



El siguiente resultado de búsqueda es un ejemplo de infracción del WAF:

El siguiente resultado de búsqueda es un ejemplo de infracción de un bot:

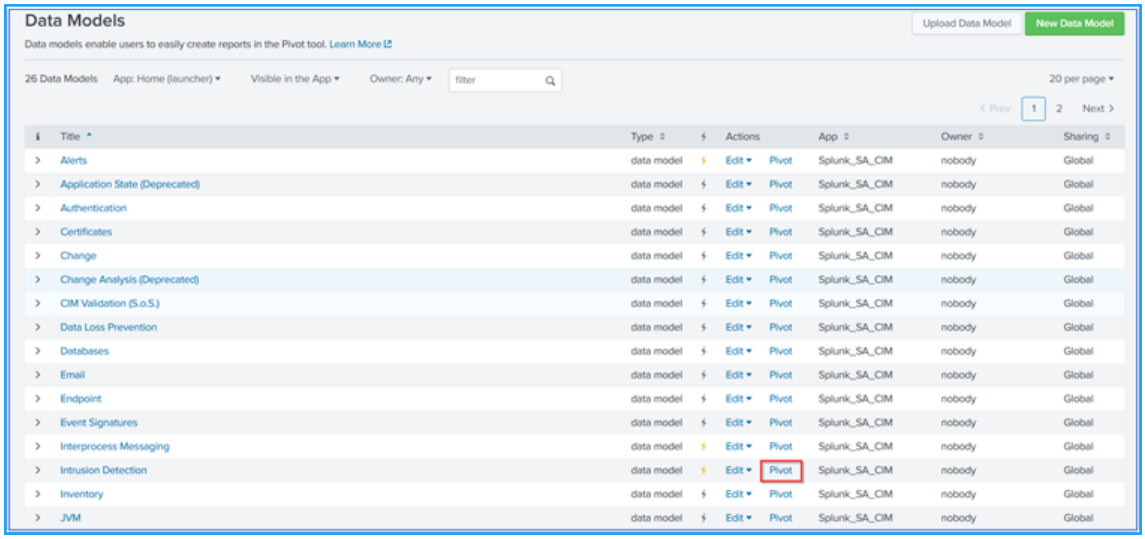


Accede a los detalles

Debe identificar el tipo de modelo de datos para ver los detalles de la tabla dinámica. Por ejemplo, el complemento Splunk convierte los eventos WAF y Bot en formato CIM, con el tipo de modelo de datos más parecido, como la detección de alertas e intrusiones.

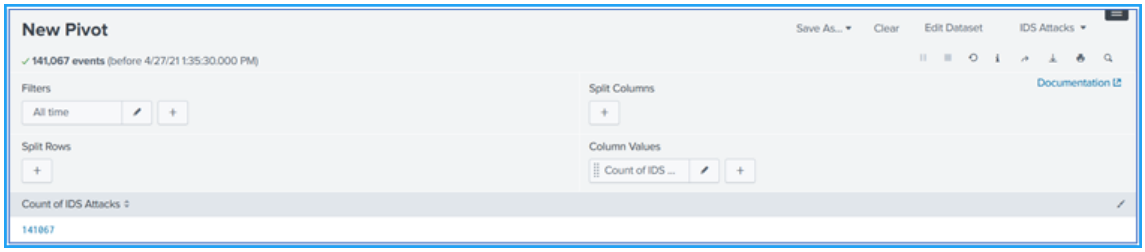
Para acceder a los eventos en Splunk:

1. Vaya a **Configuración > Modelos de datos**.
2. Identifique el modelo **de datos de detección de intrusiones** y haga clic **en**Cambiar

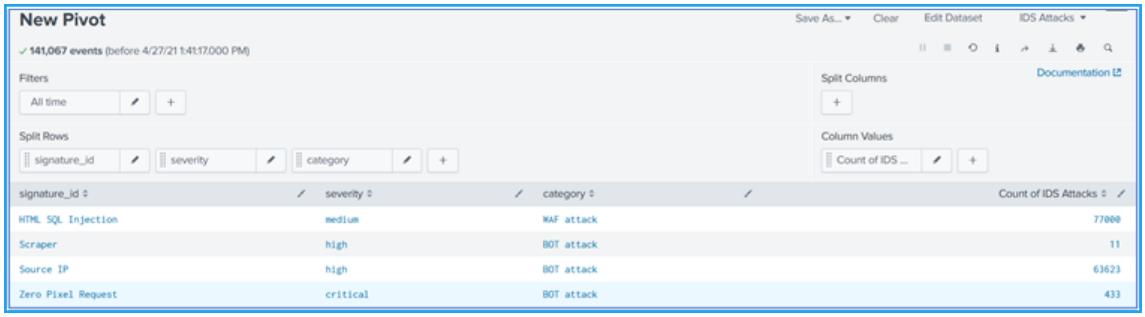


3. Seleccione un conjunto de datos. En el siguiente ejemplo, se selecciona la opción **Ataques de IDS** .

Se muestra el recuento total de **ataques de IDS** .



También puede hacer clic en el botón **+** para agregar más detalles a la tabla. El siguiente ejemplo muestra los detalles según la gravedad, la categoría y el identificador de firma:



Panel de Splunk

Mediante un panel de control, puede ver los detalles de los análisis de infracciones de WAF y Bot con paneles como gráficos, tablas, listas, etc. Puede configurar:

- Panel de control con aplicaciones que utilizan datos compatibles con el CIM.
- Panel de control personalizado que extrae datos de los modelos de datos CIM.

Dependiendo de su elección, puede crear el panel de control. Para obtener más información, consulta la sección Acerca del panel de control en la **documentación de Splunk**.

Integración de New Relic

February 13, 2023

Ahora puede integrar Citrix ADM con New Relic para ver los análisis de las infracciones de WAF y Bot en su panel de control de New Relic. Con esta integración, puede:

- Combine todas las demás fuentes de datos externas en su panel de control de New Relic.
- Obtenga visibilidad de los análisis en un lugar centralizado.

Citrix ADM recopila los eventos de Bot y WAF y los envía a New Relic en tiempo real o de forma periódica, según su elección. Como administrador, también puedes ver los eventos de Bot y WAF en tu panel de control de New Relic.

Requisitos previos

Para que la integración tenga éxito, debe:

- Obtén un punto final del evento New Relic con el siguiente formato:

  ```
  https://insights-collector.newrelic.com/v1/accounts/<account_id>/events
  ```

  Para obtener más información sobre la configuración de un punto final de eventos, consulte la documentación de New Relic.

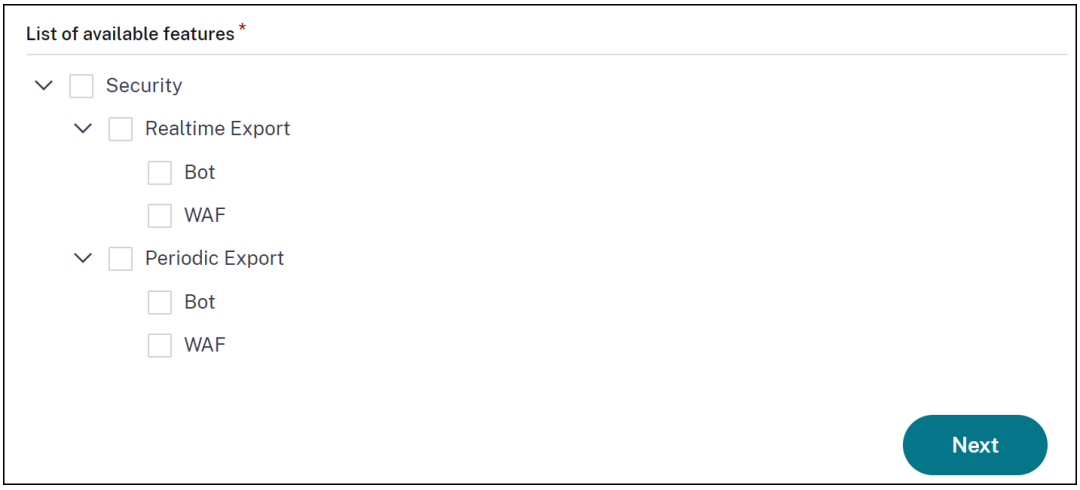
  Para obtener más información sobre cómo obtener un ID de cuenta, consulte la documentación de New Relic.

- Obtenga una nueva clave de reliquia. Para obtener más información, consulte la documentación de New Relic.
- Agregar los detalles clave en Citrix ADM

Agregar los detalles clave en Citrix ADM

Después de generar un token, debe agregar detalles en Citrix ADM para integrarlo con New Relic.

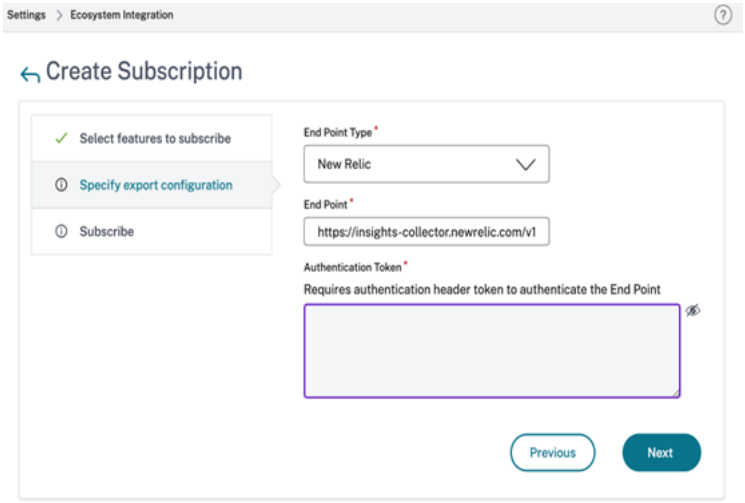
1. Inicie sesión en Citrix ADM.
2. Vaya a **Configuración > Integración de ecosistemas**.
3. En la página **Suscripciones**, haga clic en **Agregar**.
4. En la ficha **Seleccionar funciones para suscribirse**, seleccione las funciones que desee exportar y haga clic en **Siguiente**.
    - **Exportación en tiempo real**: Las infracciones seleccionadas se exportan inmediatamente a New Relic.
    - **Exportación periódica**: Las infracciones seleccionadas se exportan a New Relic en función de la duración que seleccione.



5. En la ficha **Especificar la configuración de exportación** :
    a) **Tipo de dispositivo de punto final**: Seleccione **New Relic** en la lista.
    b) **Dispositivo de punto final**: Especifique los detalles del dispositivo de punto final de New Relic. El punto final debe estar en el formato `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events`.

    > **Nota**
    >
    > Se recomienda utilizar HTTPS por motivos de seguridad.

    c) **Token de autenticación**: Copie y pegue el token de autenticación de la página New Relic.
    d) Haga clic en **Siguiente**.



6. En la página de **suscripción** :

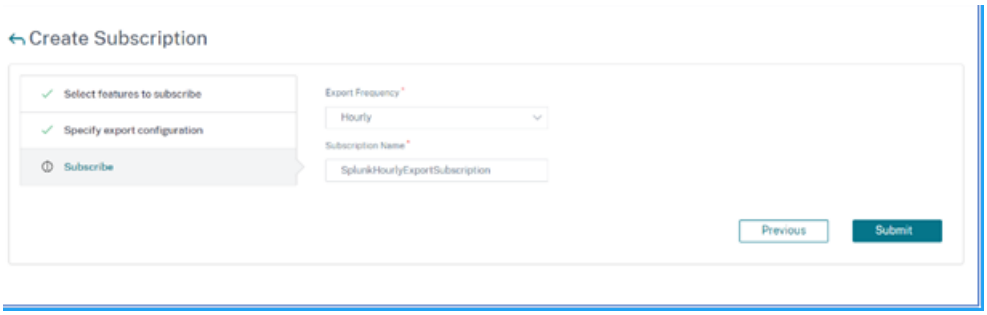
   a) **Frecuencia de exportación** : seleccione Diaria o Cada hora de la lista. Según la selección, Citrix ADM exporta los detalles a New Relic.

   > **Nota**
   >
   > Aplicable solo si ha seleccionado infracciones en la **exportación periódica**.

   b) **Nombre de la suscripción** : especifique un nombre de su elección.

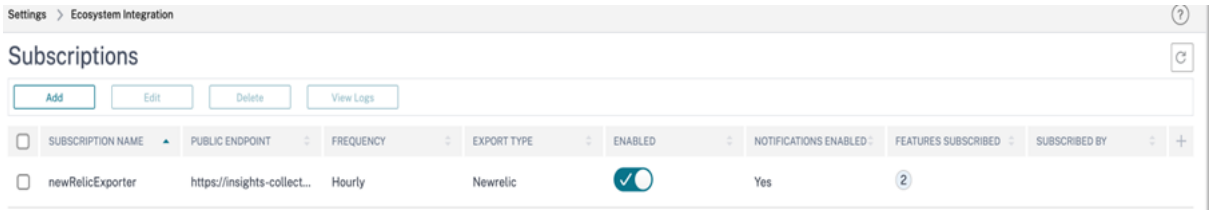
   c) Seleccione la casilla **Activar notificaciones**.

   d) Haga clic en **Submit**.



> **Nota**
>
> - Cuando se configura con la opción **Exportación periódica** por primera vez, los datos de las funciones seleccionadas se envían inmediatamente a New Relic. La siguiente frecuencia de exportación se realizará en función de su selección (diaria u horaria).
> - Al configurar con la opción **Exportación en tiempo real** por primera vez, los datos de las funciones seleccionadas se envían a New Relic inmediatamente en cuanto se detectan las infracciones en Citrix ADM.

La configuración está completa. Puede ver los detalles en la página **Suscripciones**.

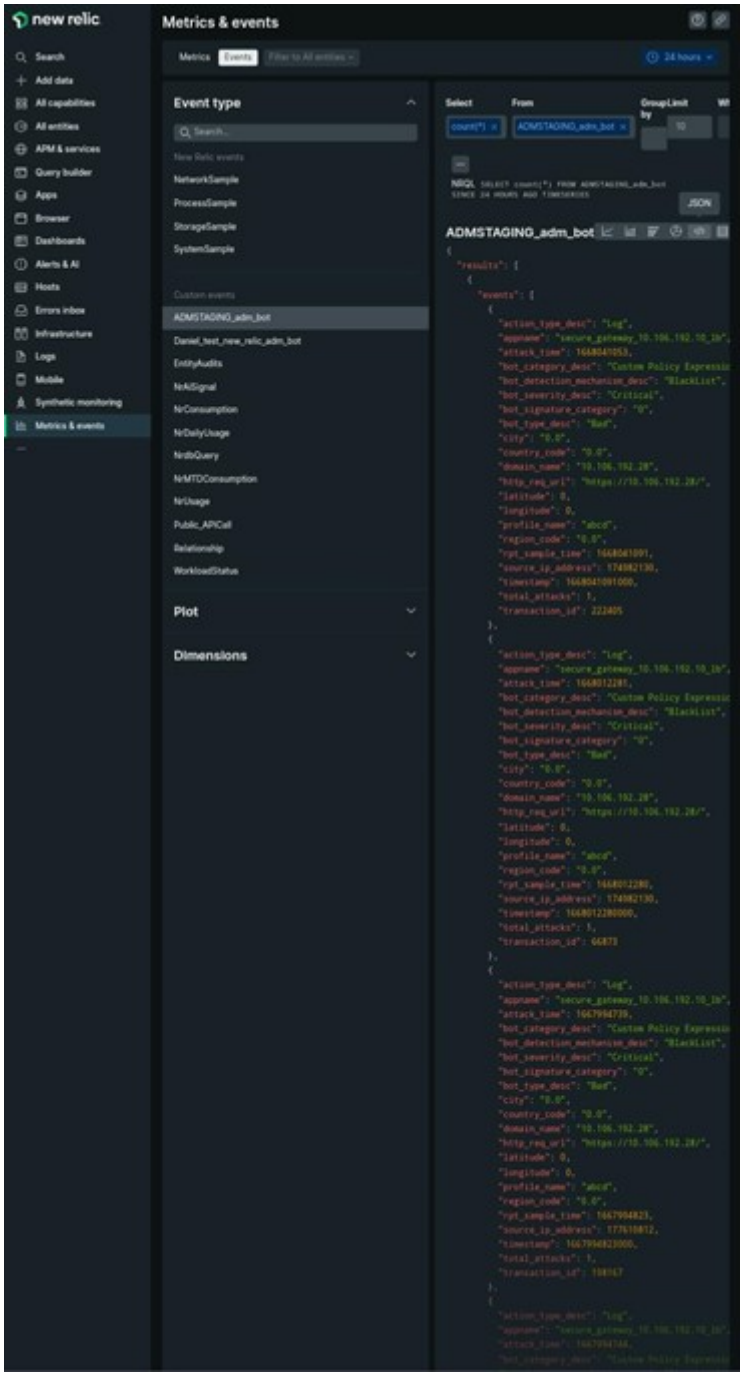


Panel de mandos de New Relic

Cuando los eventos se exportan a New Relic, puedes ver los detalles de los eventos en **Métricas y eventos** en el siguiente formato JSON:

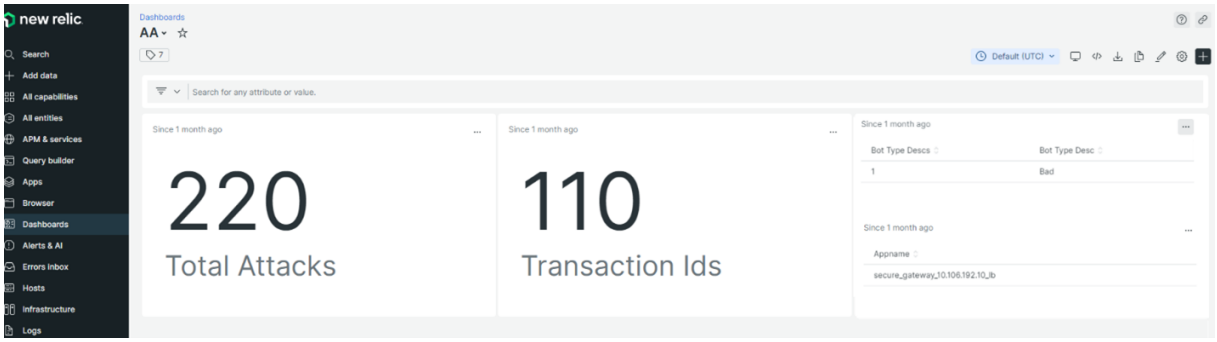
<subsription_name>_adm_<event name> donde el nombre del evento puede ser Bot, WAF, etc.

En el siguiente ejemplo, ADMSTAGING es <subscription_name> y bot es <event_name>.



Una vez que hayas incorporado los datos JSON a tu panel de control de New Relic, como administrador, puedes usar el NRQL (lenguaje de consulta de New Relic) y crear un panel personalizado con facetas y widgets según tu 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
  ```

Motor de aprendizaje WAF

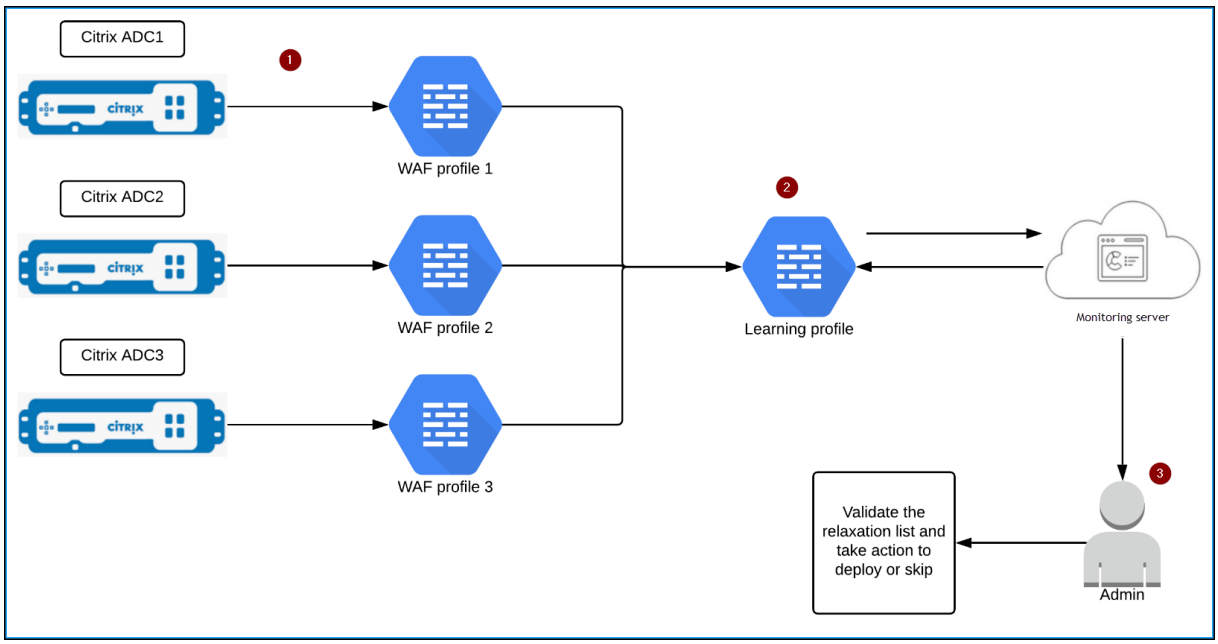
November 16, 2022

Citrix 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 Citrix ADM 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 Citrix ADM:



1 — Instancias de Citrix ADC con sus perfiles WAF

2 — Configure un perfil de aprendizaje en Citrix ADM, agregue los perfiles WAF y seleccione implementar automáticamente o implementar manualmente las reglas de relajación

3 — El administrador puede validar las reglas de relajación en Citrix ADM y decidir implementarlas u omitirlas

Introducción

Para implementar la función de aprendizaje, debe:

- Habilite el aprendizaje centralizado en la instancia de ADC. Ejecute el siguiente comando en la instancia de ADC:

  ```
  set appfw settings -centralizedLearning ON
  ```

- Asegúrese de que la versión de la instancia ADC sea **13.0-76.6** o posterior.
- Configure un perfil de Web App Firewall (conjunto de ajustes de seguridad) en su dispositivo Citrix ADC. Para obtener más información, consulte Creación de perfiles de Web App Firewall.

Tras habilitar el aprendizaje centralizado y configurar el perfil WAF, Citrix ADM genera una lista de excepciones (relajaciones) para la comprobación de seguridad configurada. Como administrador, puede revisar la lista de excepciones en Citrix ADM y decidir si implementarlas u omitirlas.

Con la función de aprendizaje WAF de Citrix ADM, 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 Citrix ADC 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 Citrix ADC.

  - Inyección de comandos

    > **Nota**
    >
    > Solo se admite en la instancia de ADC 13.0-72.12 o posterior.

  - JSON SQL

    > **Nota**
    >
    > Solo se admite en la instancia de ADC 13.1-14.10 o posterior.

  - inyección de comandos JSON

    > **Nota**
    >
    > Solo se admite en la instancia de ADC 13.1-14.10 o posterior.

  - JSON XSS

> **Nota**
>
> Solo se admite en la instancia de ADC 13.1-14.10 o posterior.

- Compruebe las reglas de relajación en Citrix ADM y decida tomar las medidas necesarias (implementar u omitir)
- Recibe las notificaciones por correo electrónico, slack y ServiceNow
- Utilice la página **Resumen de Acción** para ver los detalles de relajación

Para utilizar el aprendizaje WAF en Citrix ADM:

1. Configurar el perfil de aprendizaje
2. Ver las reglas de relajación
3. Utilizar la página Resumen de Acción de Aprendizaje WAF

Recomendaciones de la WAF

November 16, 2022

El perfil de Citrix 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 ADC, 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 de Citrix ADM WAF 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 ADC. 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 ADC debe ser **13.0 41.28 o posterior** (para las comprobaciones de seguridad) y **13.0 o posterior** (para las firmas).

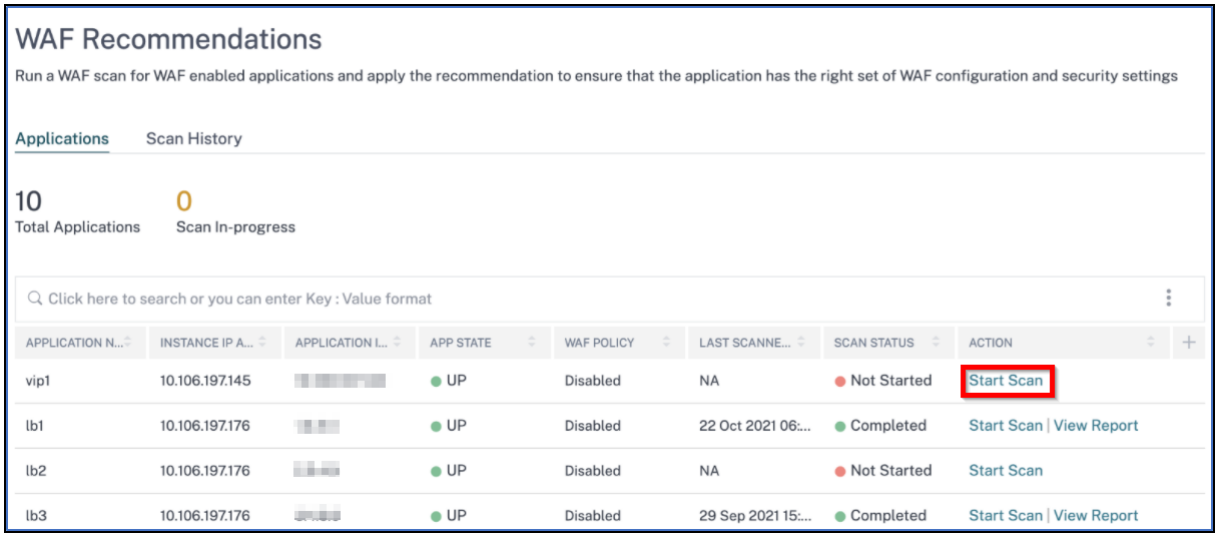
Requisitos previos

Las aplicaciones:

- Debe tener la licencia premium.
- Debe ser el servidor virtual de equilibrio de carga.

Configure los ajustes de escaneo de WAF

En Citrix ADM, 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.

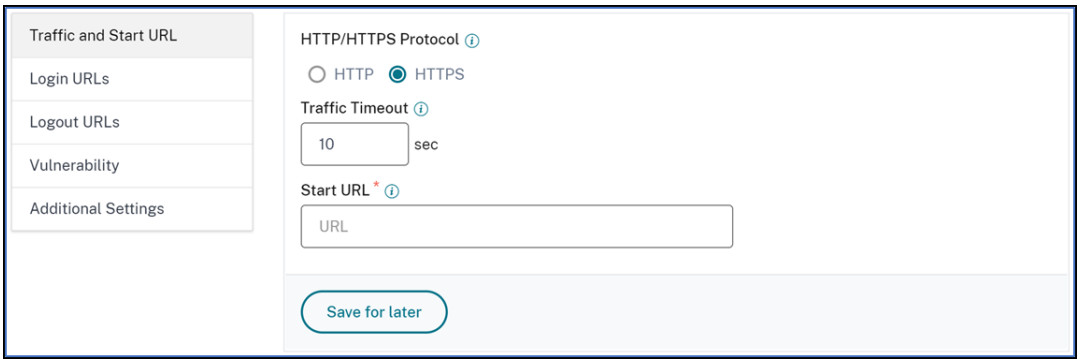


En la página de recomendaciones de la WAF:

- **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`.

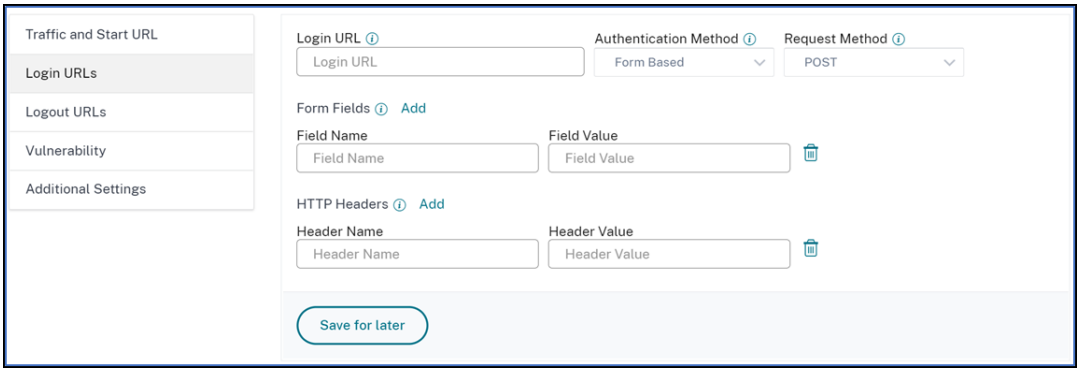
  > Nota
  >
  > La URL inicial, la URL de inicio y la URL de cierre de sesión deben coincidir con el dominio especificado.

- **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. No se permiten direcciones IP internas en el rango 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

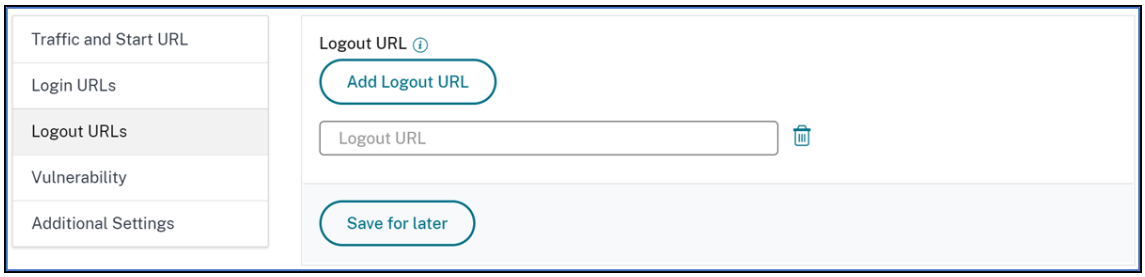


- **URL de inicio** de sesión: especifique las credenciales de inicio de sesión y las URL, si las hay, para acceder a la aplicación.
  - **URL de inicio** de sesión: URL a la que se envían los datos de inicio de sesión para la autenticación. En HTML, esta URL se conoce comúnmente como URL de acción.
  - **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, 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 especificarlo 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.

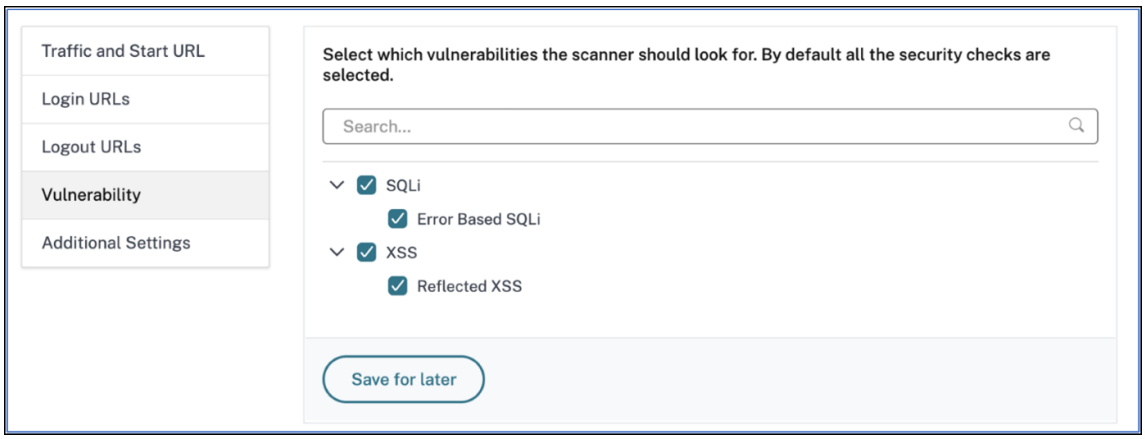


- **URL de cierre de sesión** : especifique la URL que termina la sesión después de acceder a ella. Por ejemplo: `https://www.example.com/customer/logout`.



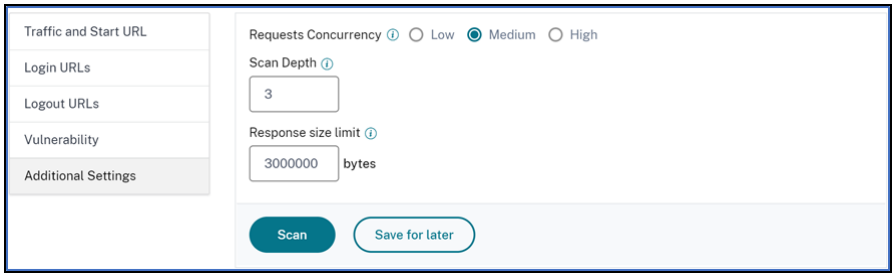
- **Vulnerabilidad** : seleccione las vulnerabilidades para que el analizador las detecte. Actualmente, esto se hace por la inyección de SQL y las infracciones de scripts entre sitios. De forma predeterminada, se seleccionan todas las infracciones. Tras seleccionar las vulnerabilidades, simula estos 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.

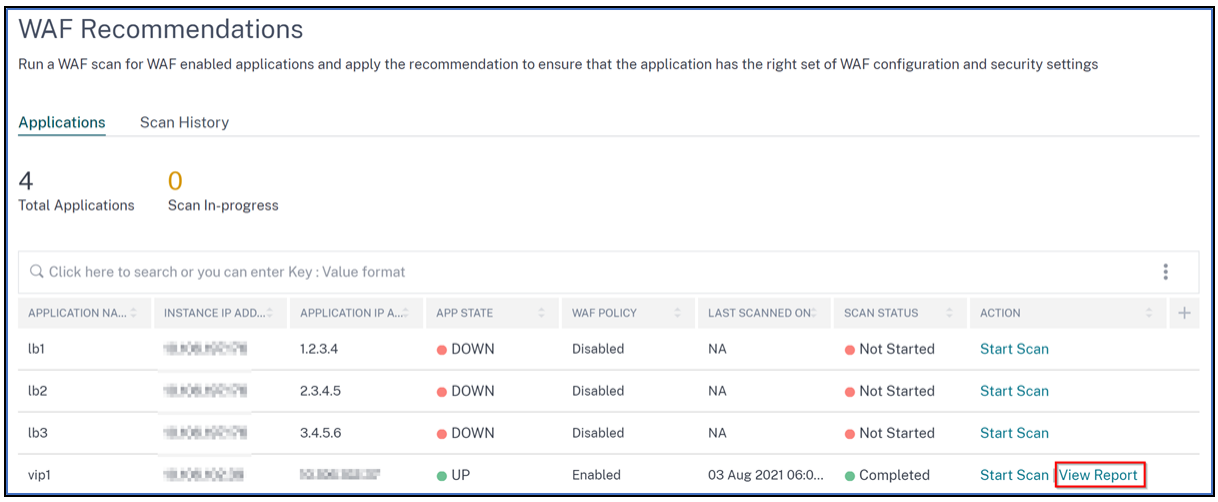
- Inspecciona la aplicación web para descubrir las tecnologías utilizadas por la aplicación web.
- Simula los ataques de seguridad a la aplicación web para detectar posibles vulnerabilidades.
- Recomienda firmas basadas en las tecnologías web detectadas.
- Recomienda realizar comprobaciones de seguridad 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

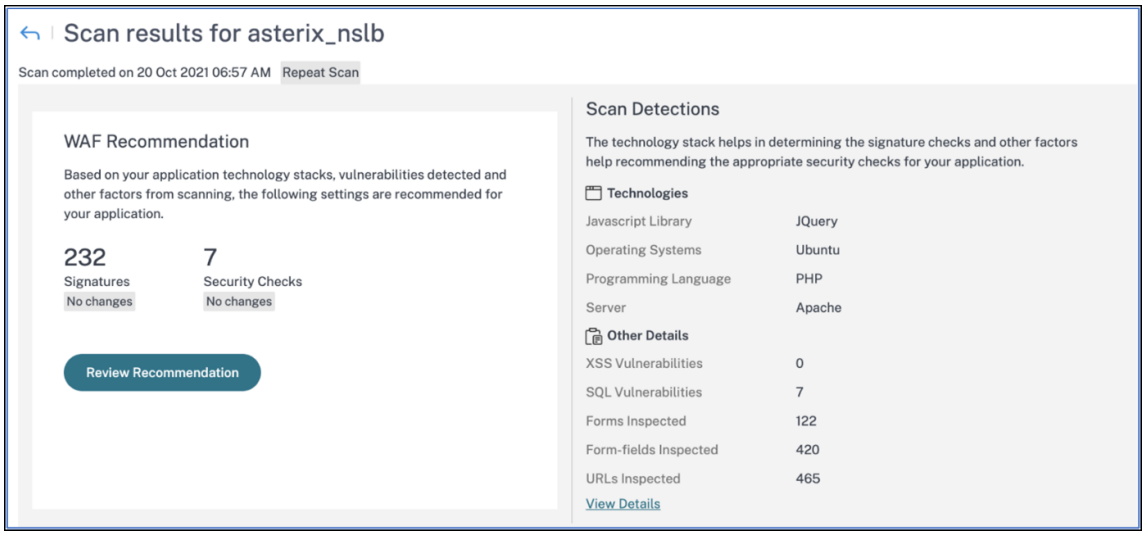
Una vez finalizado el escaneo, haga clic en **Ver informe** para ver los resultados.



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.

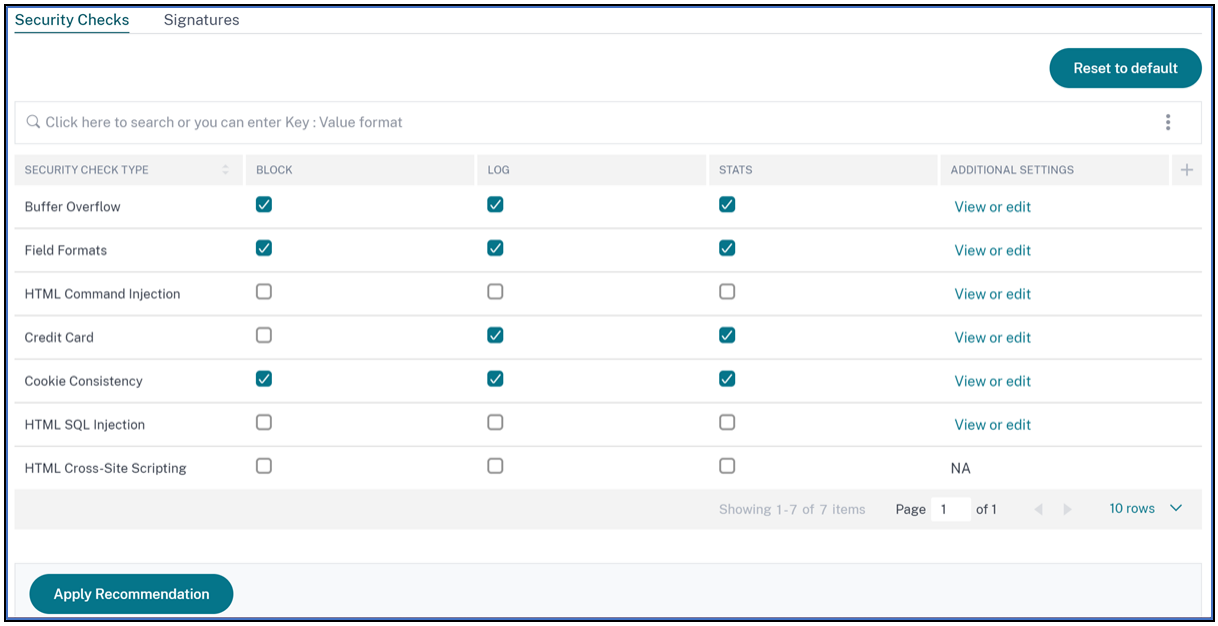
- **Detecciones de escaneo** : le permite ver la recopilación de información, como las tecnologías y los detalles de las infracciones realizadas en la aplicación. Haga clic en **Ver detalles** para ver la información sobre las detecciones y otros detalles del análisis.



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 a la instancia de ADC a través del StyleBook `appfw-import-object`.
- El archivo de firmas con las recomendaciones configuradas se importa a la instancia de ADC.

> **Nota**
>
> Las firmas se admiten en ADC 13.0 o en una versión posterior.

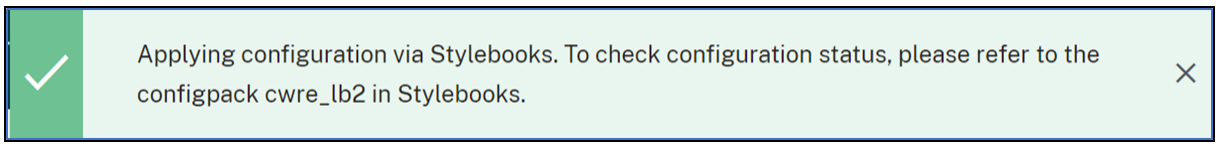
Antes de proceder a aplicar las recomendaciones de la **comprobación de seguridad**, vaya a **Aplicaciones > Configuración > Paquetes de configuración** y asegúrese de que el paquete de configuración de firmas se haya creado correctamente.

Si aplica correctamente las comprobaciones de seguridad:

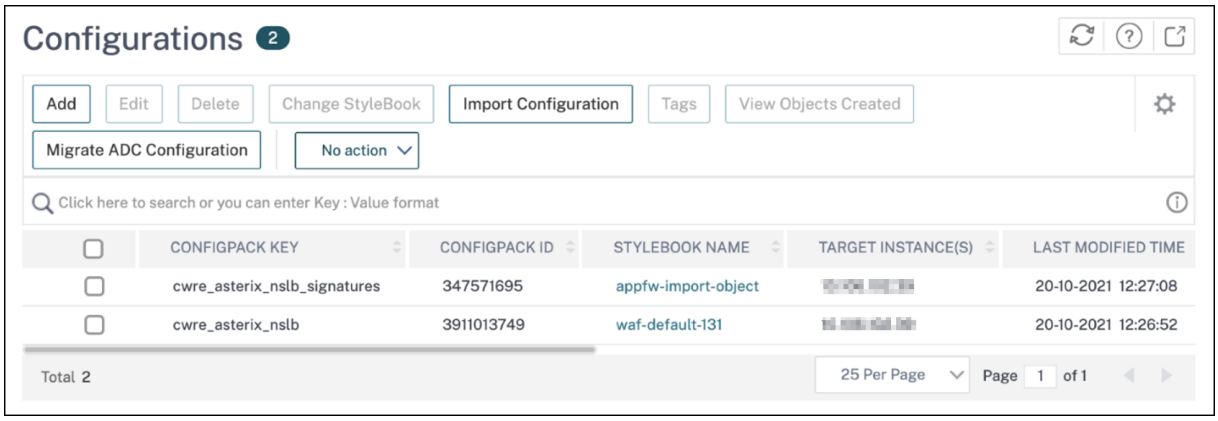
- La configuración se aplica a la instancia de ADC a través de StyleBooks, según la versión de ADC. Para ADC 13.0, se usa el StyleBook `waf-default-130` y para ADC 13.1, se usa el StyleBook `waf-default-131`.
- El perfil `Appfw` se crea en su ADC y se vincula a la aplicación mediante `policylabel`.
- Las firmas están enlazadas al perfil appfw, si las firmas recomendadas ya están aplicadas.

> **Nota**
>
> Las comprobaciones de seguridad son compatibles con ADC 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

November 16, 2022

En una implementación de Citrix 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 Citrix Gateway y quiere conocer la actividad del usuario y los motivos del error de inicio de sesión, pero esa información normalmente no está disponible a menos que el usuario envíe una solicitud de resolución.

Gateway Insight proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, en el momento de iniciar sesión en Citrix Gateway. Puede ver una lista de todos los usuarios disponibles, el número de usuarios activos, el número de sesiones activas y los bytes y licencias utilizados por todos los usuarios en un momento dado. Puede ver los errores del análisis de puntos finales (EPA), la autenticación, el inicio de sesión único (SSO) y el inicio de aplicaciones de un usuario. También puede ver los detalles de las sesiones activas y finalizadas de un usuario.

Gateway Insight también proporciona visibilidad de los motivos del error de inicio de aplicaciones para aplicaciones virtuales. Esto mejora su capacidad para solucionar cualquier tipo de problemas de inicio de sesión o inicio de aplicaciones. Puede ver el número de aplicaciones 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 utilizados por todas las puertas de enlace asociadas con un dispositivo de puerta de enlace de ADC en un momento dado. Puede ver los errores de EPA, autenticación, inicio de sesión único y lanzamiento de aplicaciones para una Gateway. También puede ver los detalles de todos los usuarios asociados a una Gateway y su actividad de inicio de sesión.

Todos los mensajes de registro se almacenan en la base de datos Citrix ADM, por lo que puede ver los detalles de los errores de cualquier período de tiempo. También puede ver un resumen de los errores de inicio de sesión y determinar en qué etapa del proceso de inicio de sesión se ha producido un error.

Puntos a tener en cuenta:

- Gateway Insight se admite en las siguientes implementaciones:
  - Access Gateway
  - Unified Gateway
- La versión y la compilación de Citrix ADM deben ser iguales o posteriores a las del dispositivo Citrix Gateway.
- Se puede ver una hora de informes de Gateway Insight para instancias ADC con licencia Advanced. Se requiere una licencia Premium para ver los informes de Gateway Insight más allá de una hora.

Limitaciones:

- Citrix Gateway no admite Gateway Insight cuando el método de autenticación está configurado como autenticación basada en certificados.
- 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 ADC 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

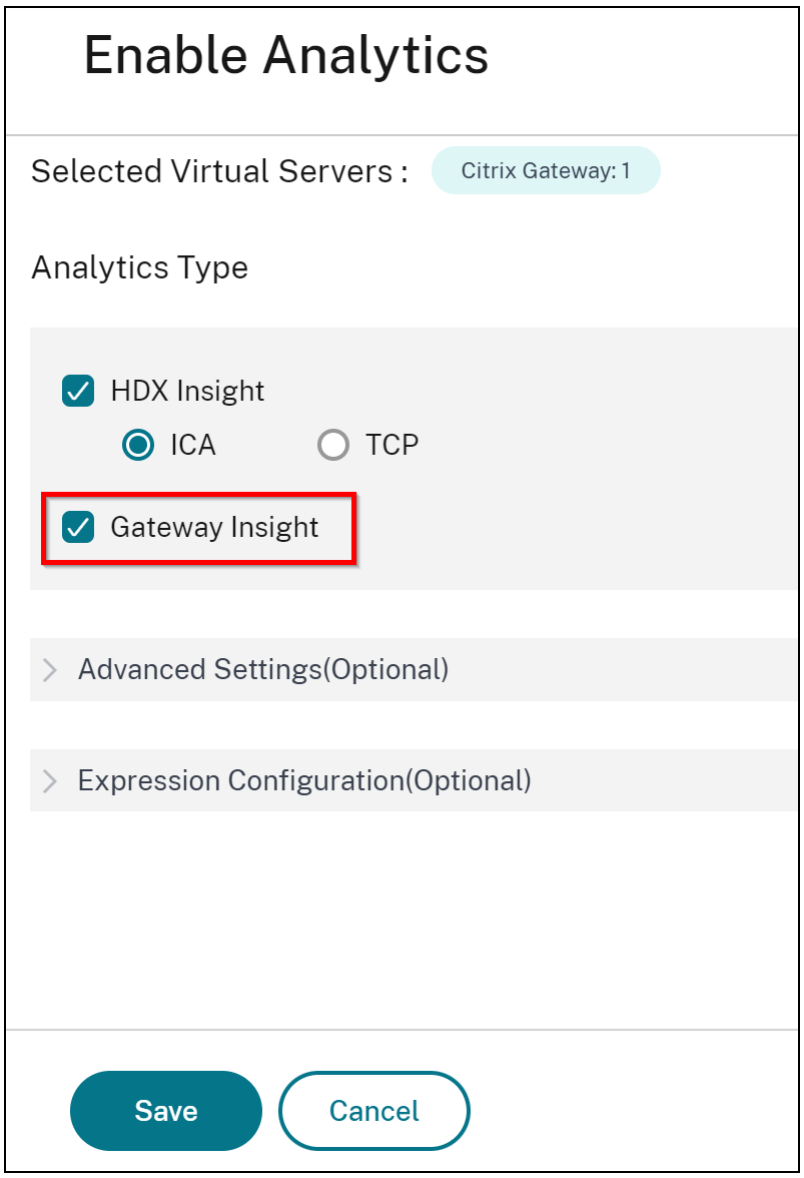
Habilitar Gateway Insight

Para habilitar Gateway Insight para su dispositivo Citrix Gateway, primero debe agregar el dispositivo ADC Gateway a Citrix ADM. A continuación, debe habilitar AppFlow para el servidor virtual que representa la aplicación VPN. Para obtener información sobre cómo agregar un dispositivo a Citrix ADM, consulte Agregar instancias.

> **Nota**
>
> Para ver los errores del análisis de puntos finales (EPA) en Citrix ADM, debe habilitar el registro de nombres de usuario de autenticación, autorización y control de acceso de AppFlow en el dispositivo ADC Gateway.

Habilite AppFlow para un servidor virtual en Citrix ADM

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 Citrix Gateway y haga clic en **Habilitar análisis**.
4. Selecciona **Gateway Insight**.
5. Haga clic en **Guardar**.



Habilitar el registro de nombres de usuario de AppFlow en un dispositivo de puerta de enlace de ADC 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**

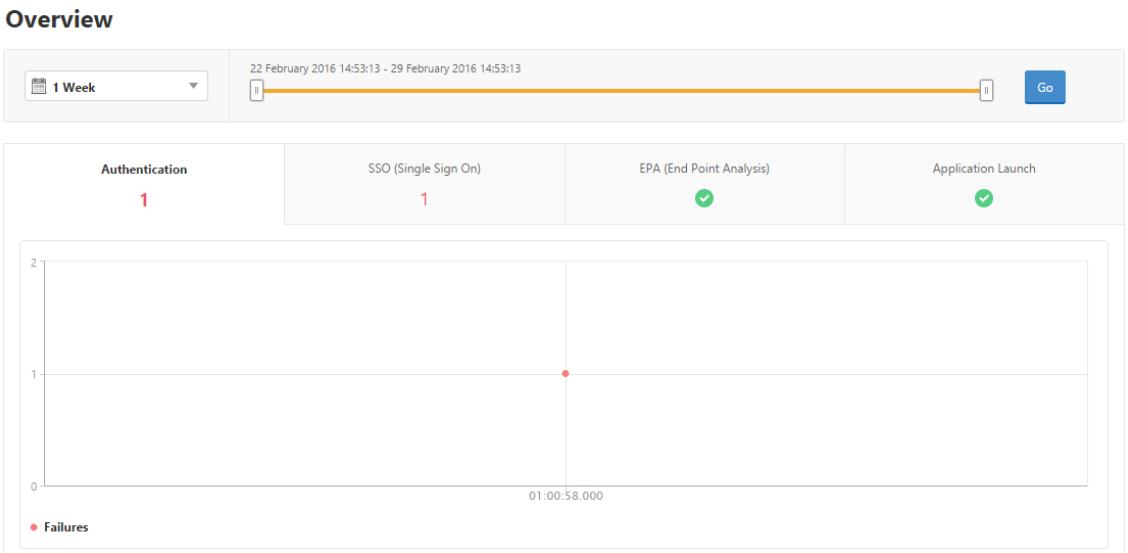
Ver informes de Gateway Insight

En Citrix ADM, puede ver informes de todos los usuarios, aplicaciones y puertas de enlace asociados a los dispositivos de ADC Gateway, y puede ver los detalles de un usuario, aplicación o puerta de enlace en particular. En la sección **Descripción general**, puede ver los errores de EPA, SSO, Autenticación y Lanzamiento de aplicaciones. También puede ver un resumen de los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora.

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso de nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de Citrix ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos en Citrix ADM.

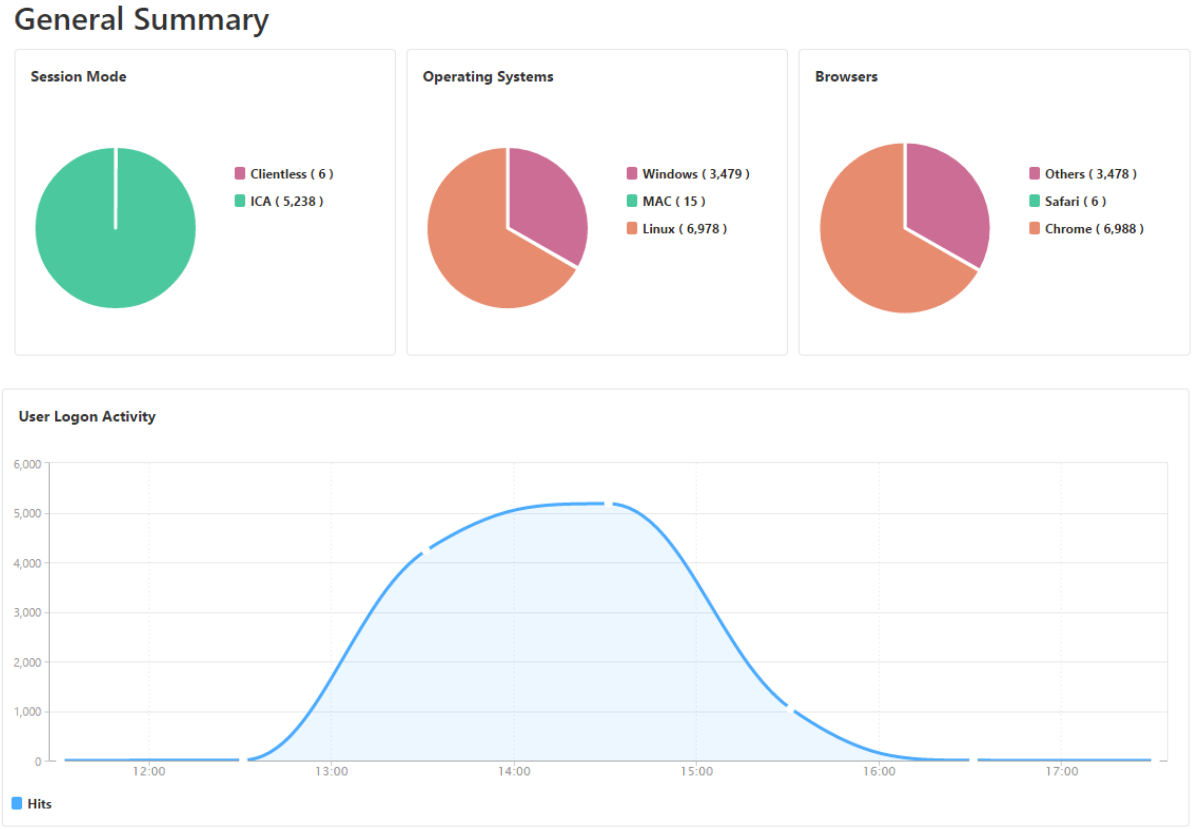
Ver errores de EPA, inicio de sesión único, autenticación, autorización y inicio de aplicaciones

1. En Citrix ADM, vaya a **Gateway > Gateway Insight**.
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Haga clic en las fichas EPA (Análisis de punto final), Autenticación, Autorización, SSO (Inicio de sesión único) o Inicio de aplicación para mostrar los detalles del error.



Ver resumen de los modos de sesión, los clientes y el número de usuarios

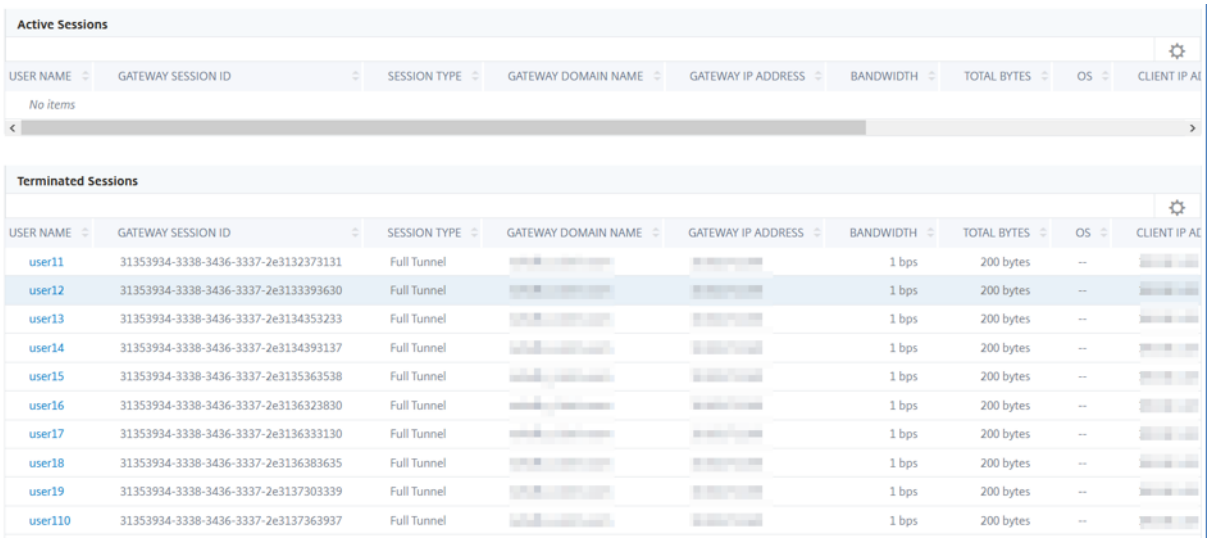
En Citrix ADM, vaya a **Gateway > Gateway Insight**, desplácese hacia abajo para ver los informes.



Usuarios

Puede ver un informe completo de los usuarios asociados a los dispositivos de puerta de enlace de ADC. 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.

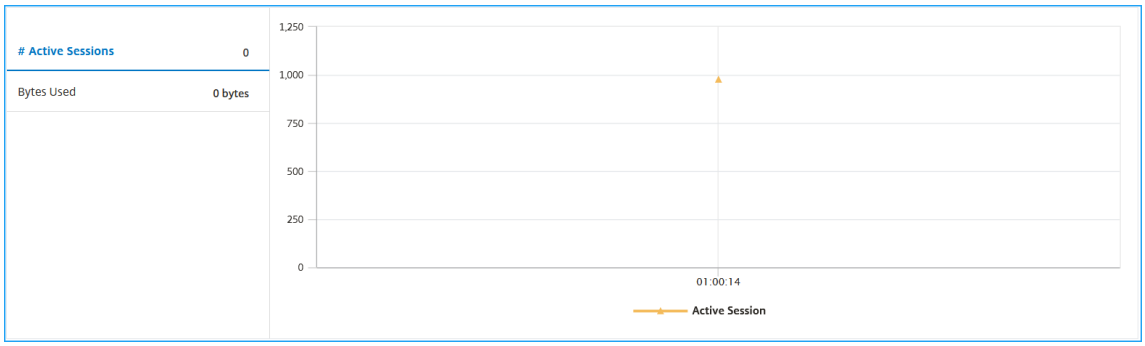


Como administrador, esta vista le permite:

- 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 Citrix ADM, vaya a **Gateway > Gateway Insight > Usuarios**.
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Puede ver el número de usuarios activos, el número de sesiones activas y bytes de todos los usuarios durante el período de tiempo.

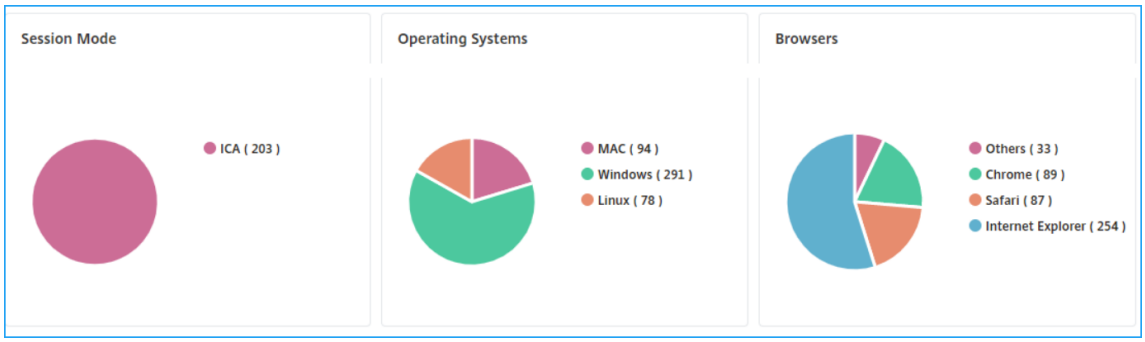


Desplácese hacia abajo para ver una lista de usuarios disponibles y usuarios activos.

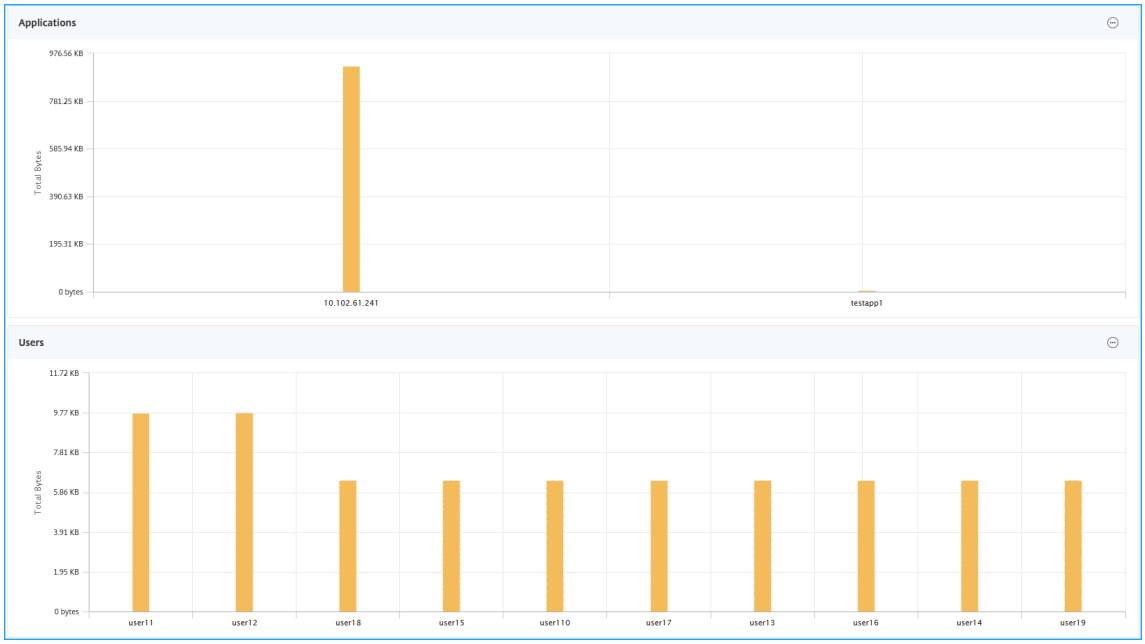
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

En la ficha **Usuarios** o **Usuarios activos**, haga clic en un usuario para ver los siguientes detalles de usuario:

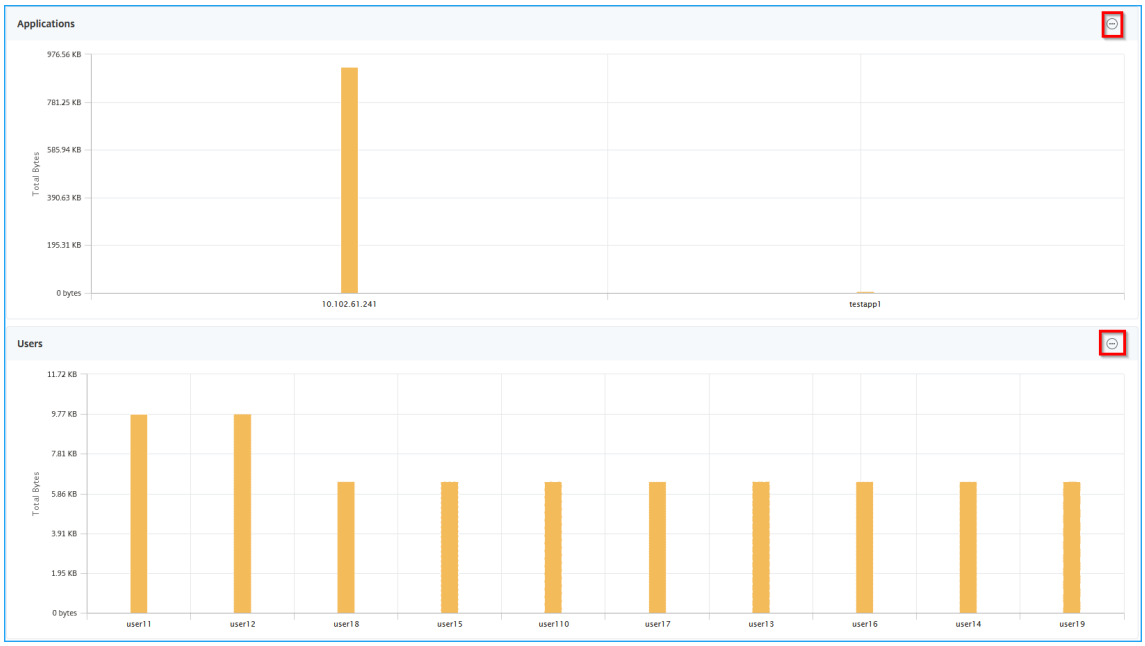
- **Detalles del usuario** : puede ver información sobre cada usuario asociado con los dispositivos de puerta de enlace de ADC. Vaya a **Gateway** > **Gateway Insight** > **Usuarios** y haga clic en un usuario para ver las perspectivas del usuario seleccionado, como el modo de sesión, el sistema operativo y los exploradores.



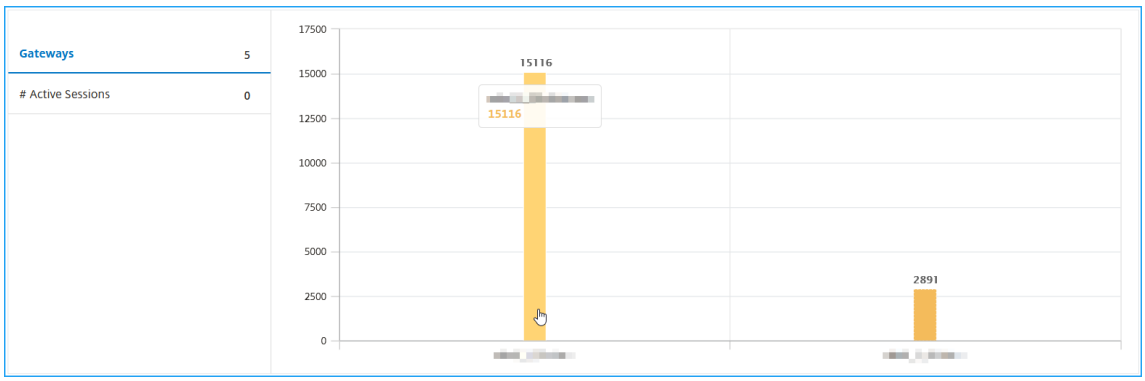
- **Usuarios y aplicaciones para la puerta de enlace seleccionada** : vaya a Puerta de **enlace > GatewayInsight**>**Puerta de enlace** y haga clic en el nombre de dominio de una puerta de enlace para ver las 10 aplicaciones principales y los 10 usuarios principales que están asociados a la puerta de enlace seleccionada.



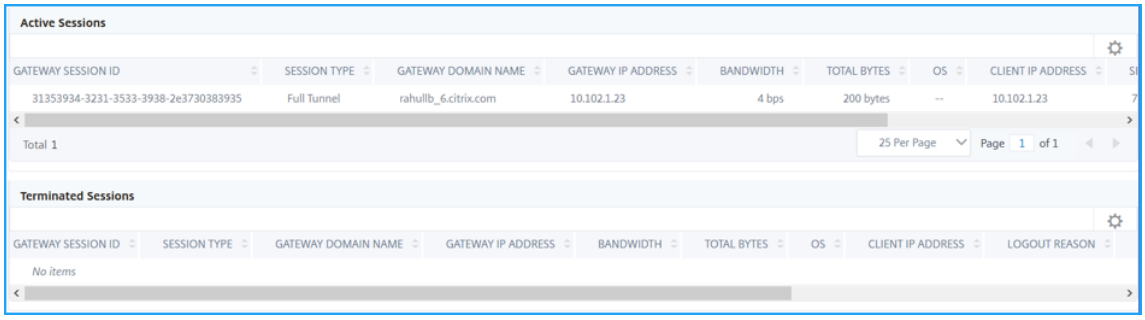
- **Ver más opción para aplicaciones y usuarios** : para más de 10 aplicaciones y usuarios, puede hacer clic en el icono más en Aplicaciones y Usuarios para ver todos los detalles de usuarios y aplicaciones asociados a la puerta de enlace seleccionada.



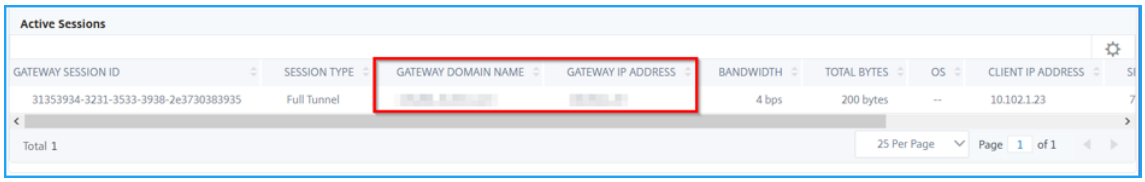
- **Ver detalles haciendo clic en el gráfico de barras** : al hacer clic en un gráfico de barras, puede ver los detalles relevantes. Por ejemplo, vaya a **Gateway > Gateway Insight > Gateway** y haga clic en el gráfico de barras de gateway para ver los detalles de la puerta de enlace



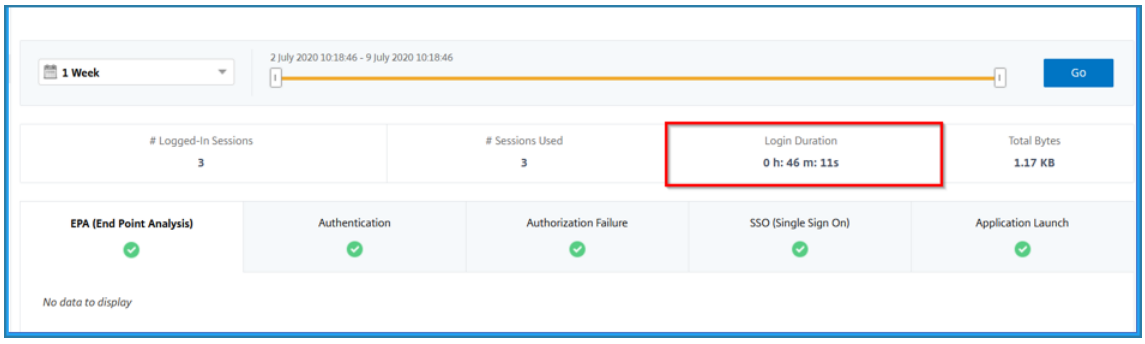
- El usuario **Sesiones Activas y SesionesTerminadas**.



- El nombre del dominio de puerta de enlace y la dirección IP de la puerta de **enlace en Sesiones**

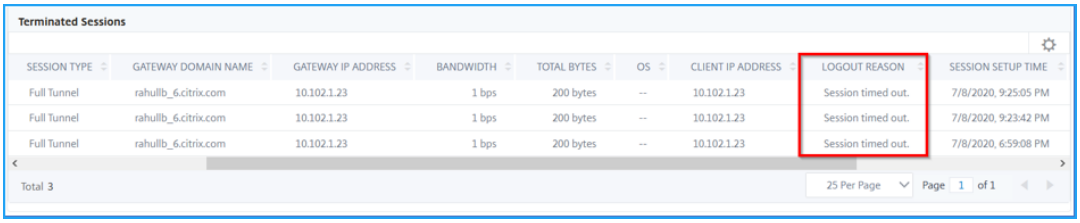


- Duración del inicio de sesión del usuario.



- El motivo de la sesión de cierre de sesión del usuario. Los motivos de cierre de sesión pueden ser:
  - Tiempo de espera excedido
  - Se cerró la sesión debido a un error interno
  - Se ha cerrado la sesión debido al tiempo de espera de la sesión inactiva

- El usuario ha cerrado sesión
- El administrador ha detenido la sesión



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

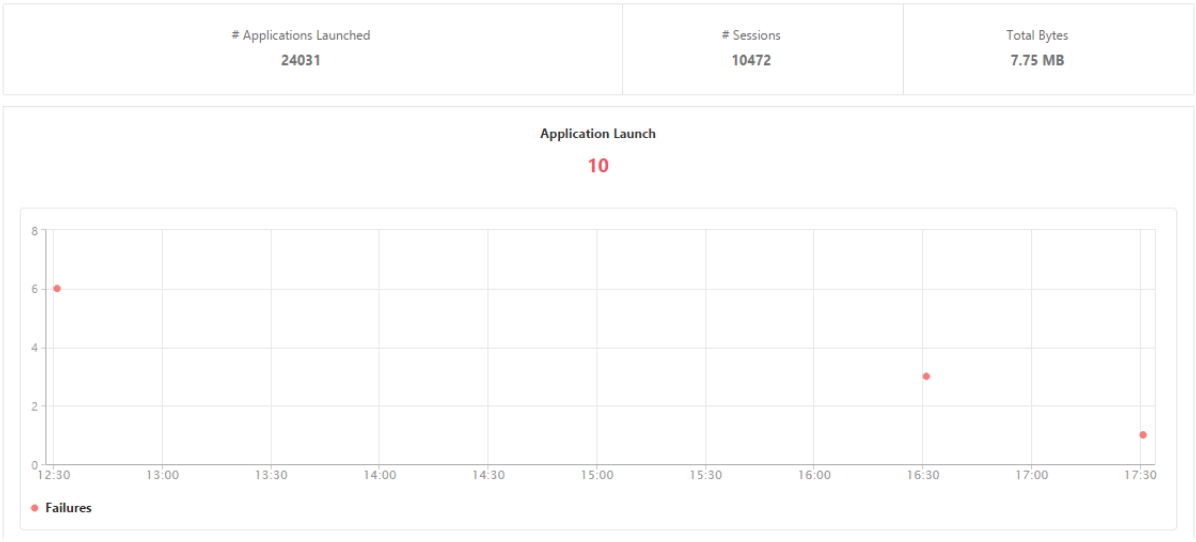
Puede ver el número de aplicaciones iniciadas, el número de sesiones totales y activas, el número de bytes totales y el ancho de banda consumidos por las aplicaciones. Puede ver los detalles de los

usuarios, las sesiones, el ancho de banda y los errores de inicio de una aplicación.

Ver detalles de la aplicación

1. En Citrix ADM, vaya a **Gateway > Gateway Insight > Aplicaciones**.
2. Seleccione el período de tiempo para el que quiere ver los detalles de la aplicación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

Ahora puede ver el número de aplicaciones 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.

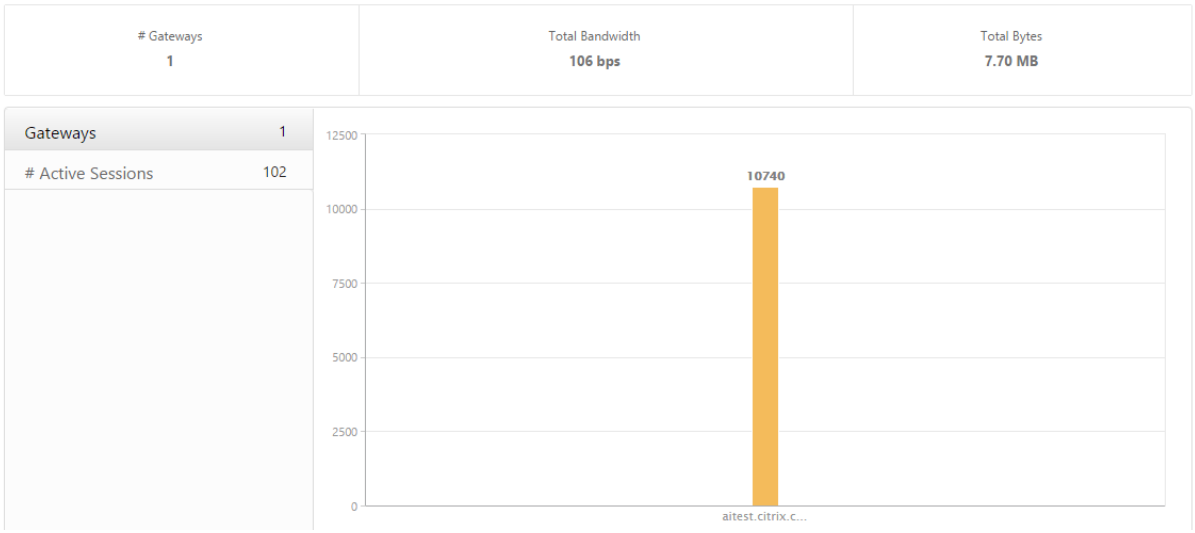
Puertas de enlace

Puede ver el número de puertas de enlace, el número de sesiones activas, el total de bytes y el ancho de banda utilizados por todas las puertas de enlace asociadas con un dispositivo de puerta de enlace de ADC 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.

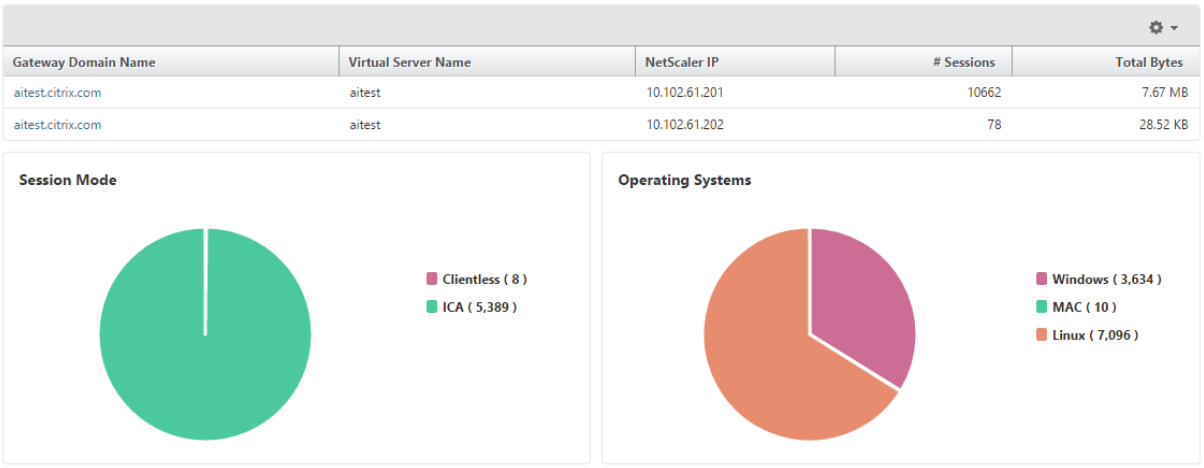
Ver detalles de la pasarela

1. En Citrix ADM, vaya a **Gateway > Gateway Insight > Gateways**.
2. Seleccione el período de tiempo para el que quiere ver los detalles de la Gateway. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

Ahora puede ver el número de puertas de enlace, el número de sesiones activas, el total de bytes y el ancho de banda utilizados por todas las puertas de enlace asociadas con un dispositivo de puerta de enlace de ADC 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 ADC, 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 se exportan solo si el Citrix ADM 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 utilizar Gateway Insight para obtener visibilidad de los detalles de acceso, las aplicaciones y las puertas de enlace de los usuarios en los dispositivos ADC Gateway.

1. El usuario no puede iniciar sesión en el dispositivo de puerta de enlace de ADC ni en los servidores web internos

Usted es un administrador de ADC Gateway que supervisa los dispositivos ADC Gateway a través de Citrix ADM y quiere saber por qué un usuario no puede iniciar sesión o en qué etapa del proceso de inicio de sesión se produjo el error.

Citrix ADM le permite ver los detalles del error de inicio de sesión del usuario en las siguientes etapas del proceso de inicio de sesión:

- Autenticación
- Análisis de puntos finales (EPA)
- Single Sign-On

En Citrix ADM, puede buscar un usuario en particular y, a continuación, ver todos los detalles de ese usuario.

Para buscar un usuario:

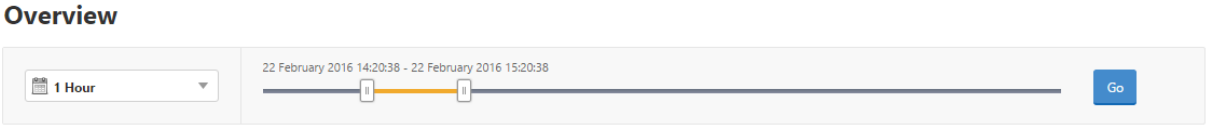
En Citrix ADM, vaya a **Gateway > Gateway Insight** y, en el cuadro de texto **Buscar usuarios**, especifique el usuario en el que quiere buscar.

Fallos de autenticación

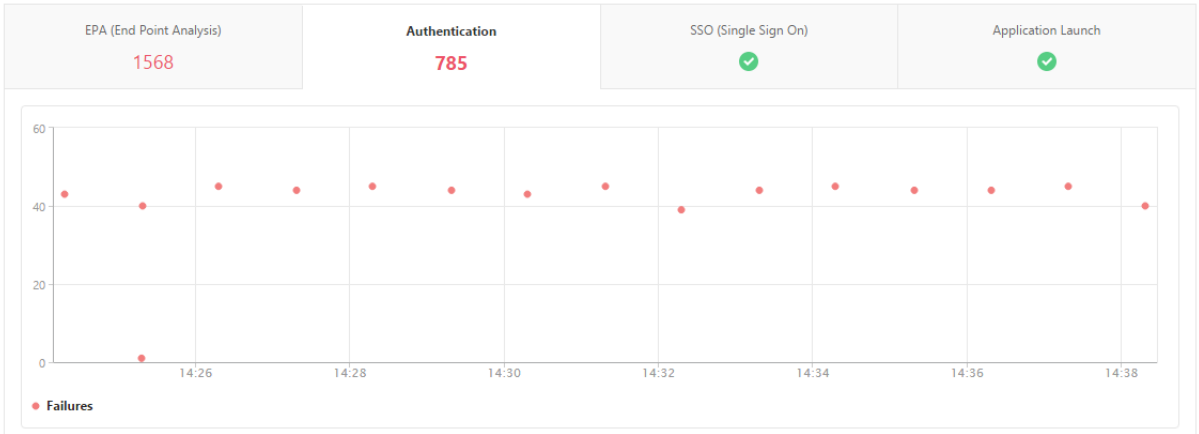
Puede ver errores de autenticación, como credenciales incorrectas o ninguna respuesta del servidor de autenticación. Si ha configurado la autenticación en dos etapas, puede ver si han fallado las etapas principal, secundaria o ambas de la autenticación.

Ver los detalles del error de autenticación

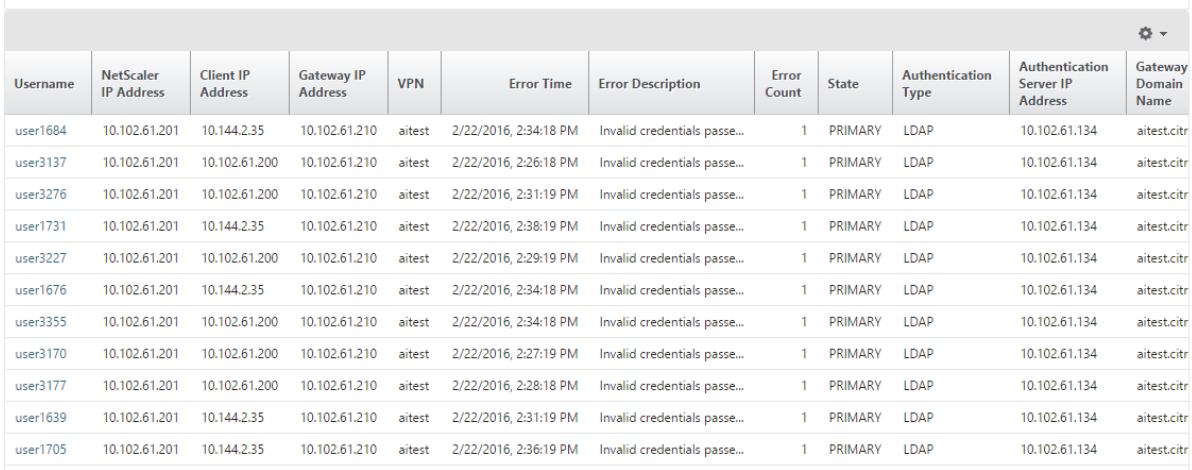
1. En Citrix ADM, vaya a **Gateway > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de autenticación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



1. Haga clic en la ficha **Autenticación**. Puede ver el número de errores de autenticación en un momento dado en el gráfico de **errores** .



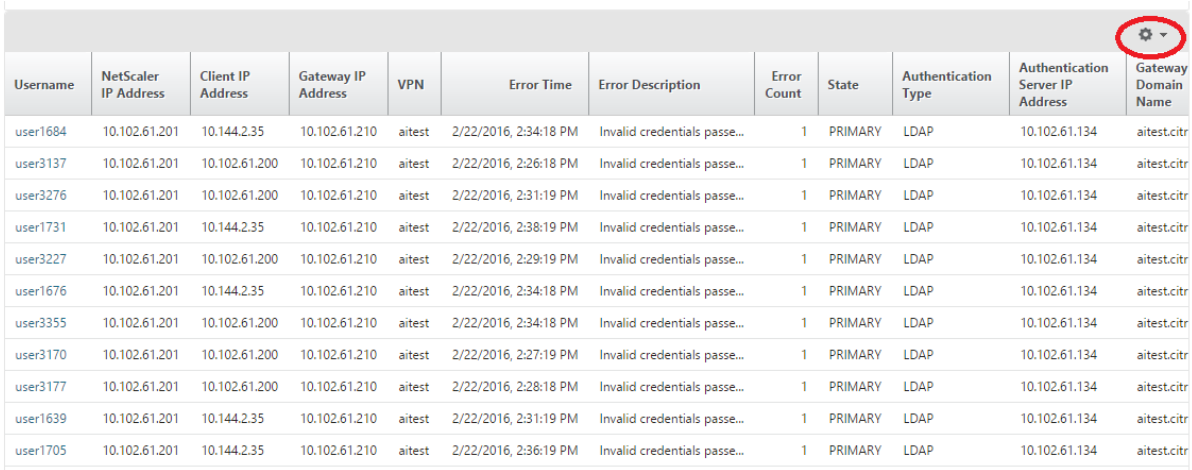
Desplácese hacia abajo para ver los detalles de cada error de autenticación, como **Nombre de usuario, Dirección IP del cliente, Tiempo de error, Tipo de autenticación, Dirección IP del servidor de autenticación**, etc. en la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra el motivo del error de inicio de sesión y la columna **Estado** muestra en qué etapa de una autenticación en dos etapas se produjo el error.



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de autenticación y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas utilizando la flecha de lista como se indica en la imagen siguiente.



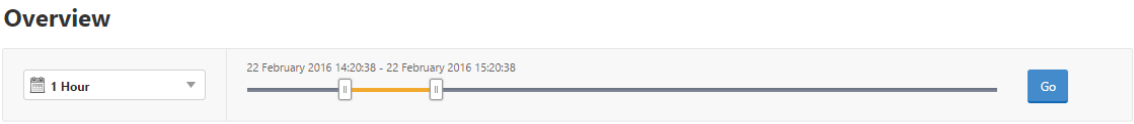
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	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

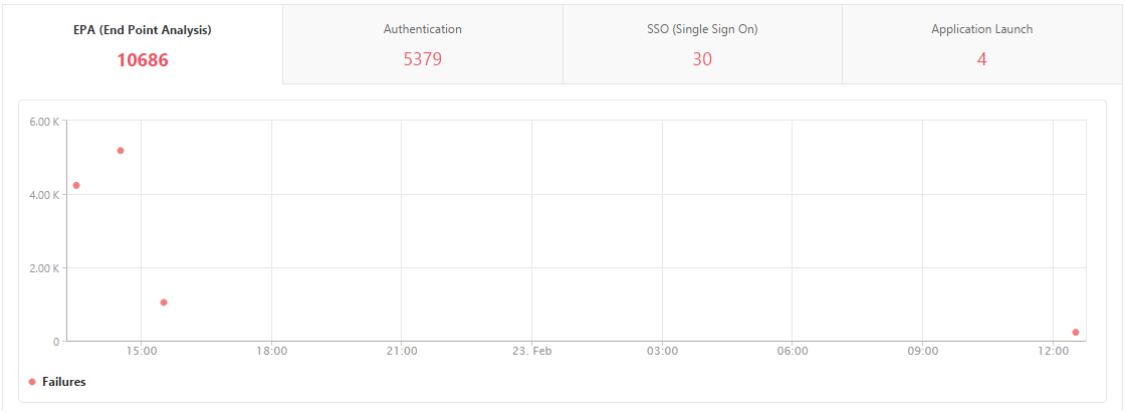
Puede ver las fallas de la EPA antes o después de la autenticación.

Ver detalles de fallas de la EPA

1. En Citrix ADM, vaya a **Gateway > Gateway Insight**.
2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de EPA. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **EPA (Análisis de punto final)**. Puede ver el número de errores de EPA en un momento dado en el gráfico de **errores**.



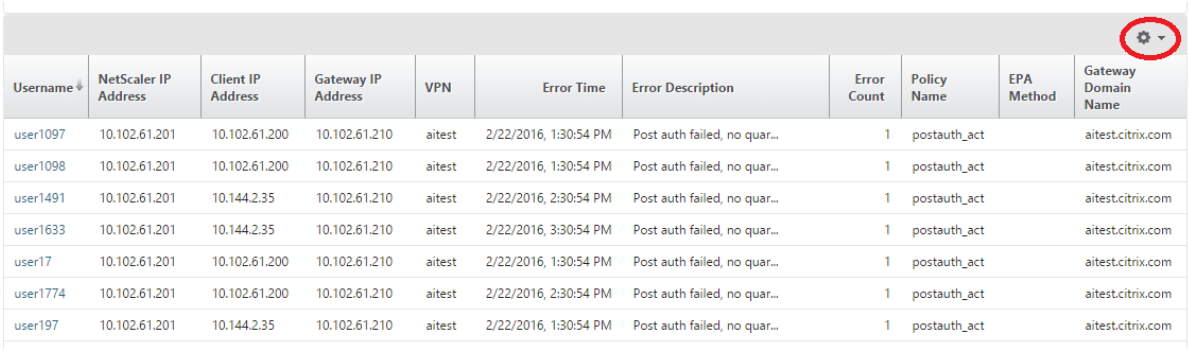
Desplácese hacia abajo para ver los detalles de cada error de EPA, como **Nombre de usuario, Dirección IP de ADC, Dirección IP de puerta de enlace, VPN, Tiempo de error, Nombre de directiva, Nombre de dominio de puerta de enlace** y más en la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra el motivo del error EPA y la columna **Nombre de la directiva** muestra la directiva que dio lugar al error.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de EPA y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas utilizando la flecha de lista como se

indica en la imagen siguiente.



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

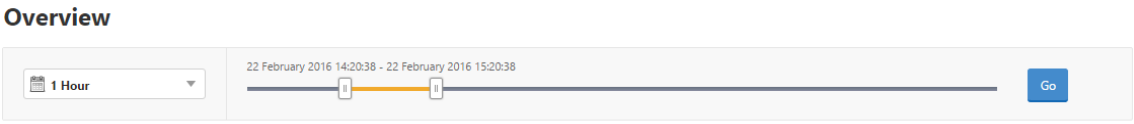
> **Nota**
>
> ADC Gateway no informa de los errores de la EPA cuando la expresión «ClientSecurity» se configura como una regla de directiva de sesión de VPN.

Fallos de SSO

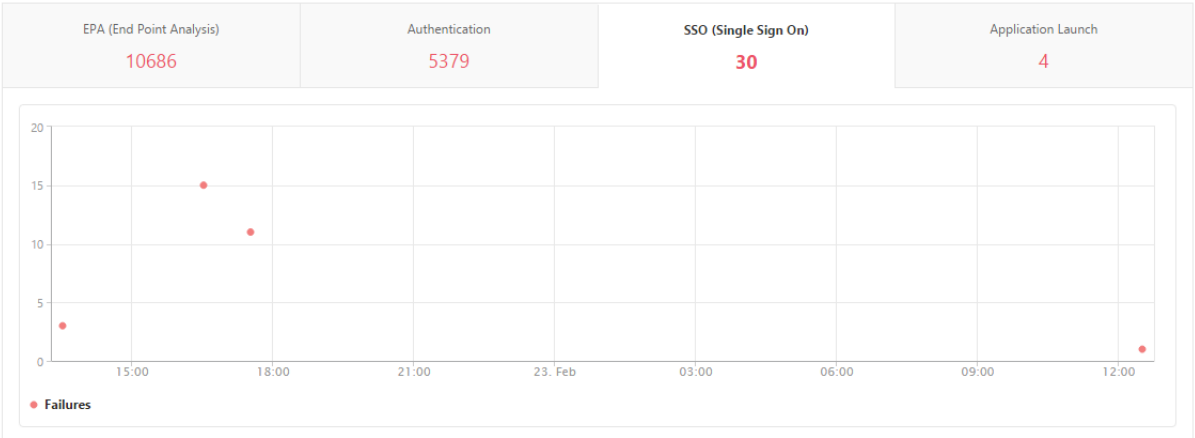
Puede ver todos los errores de SSO en cualquier momento para que un usuario acceda a cualquier aplicación a través del dispositivo ADC Gateway.

Ver detalles de los errores de SSO

1. En Citrix ADM, vaya a **Gateway > Gateway Insight**.
2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **SSO (Inicio de sesión único)**. Puede ver el número de errores de SSO en cualquier momento dado en el gráfico de errores.



Deplácese hacia abajo para ver los detalles de cada error de SSO, como **Nombre de usuario, Dirección IP de ADC, Tiempo de error, Descripción del error, Nombre del recurso** y más desde la tabla de la misma ficha.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de SSO y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas utilizando la flecha de lista como se indica en la imagen siguiente.

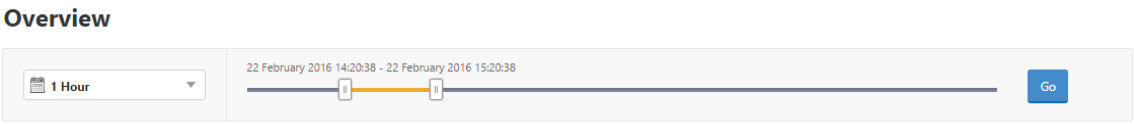
Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	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. Tras iniciar sesión correctamente en ADC Gateway, el usuario no puede iniciar ninguna aplicación virtual

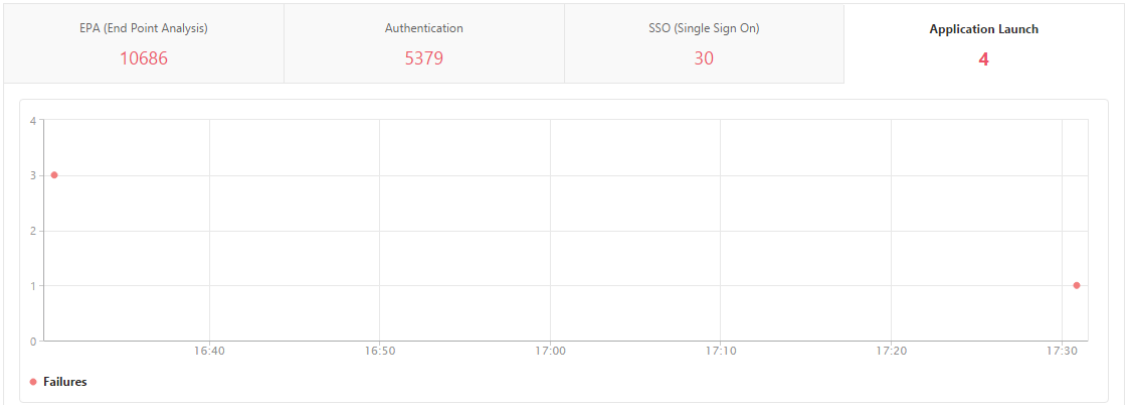
Si se produce un error en el inicio de la aplicación, puede obtener visibilidad de los motivos, como Secure Tíquet Authority (STA) o Citrix Virtual App Server, o un tíquet STA no válido. Puede ver la hora en que se produjo el error, los detalles del error y el recurso para el que falló la validación STA.

Ver detalles del error al iniciar la aplicación

1. En Citrix ADM, vaya a **Gateway > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.



3. Haga clic en la ficha **Inicio de la aplicación**. Puede ver el número de errores de inicio de la aplicación en un momento dado en el gráfico **Fallos**.

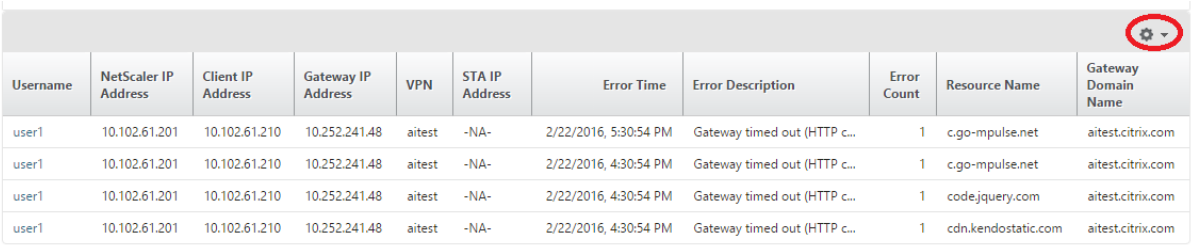


Desplácese hacia abajo para ver los detalles de cada error de inicio de aplicación, como **Dirección IP de ADC, Tiempo de error, Descripción de error, Nombre de recurso, Nombre de dominio de puerta**de enlace, etc., desde la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra la dirección IP del servidor STA y la columna **Nombre del recurso** muestra los detalles del recurso para el que ha fallado la validación STA.

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de inicio de la aplicación y otros detalles de ese usuario.

Puede personalizar la tabla para agregar o eliminar columnas utilizando la flecha de lista como se indica en la imagen siguiente.



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

Después de haber iniciado correctamente una nueva aplicación, en Citrix ADM, puede ver el total de bytes y ancho de banda consumidos por esa aplicación.

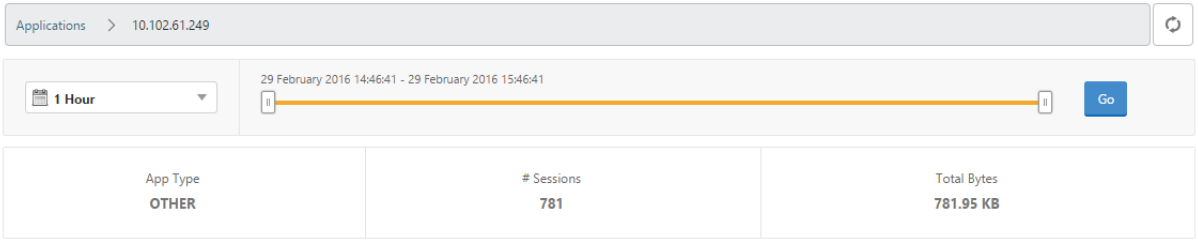
Ver el total de bytes y ancho de banda consumidos por una aplicación

En Citrix ADM, vaya a **Gateway > Gateway Insight > Aplicaciones**, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, haga clic en la aplicación de la que quiere ver los detalles.

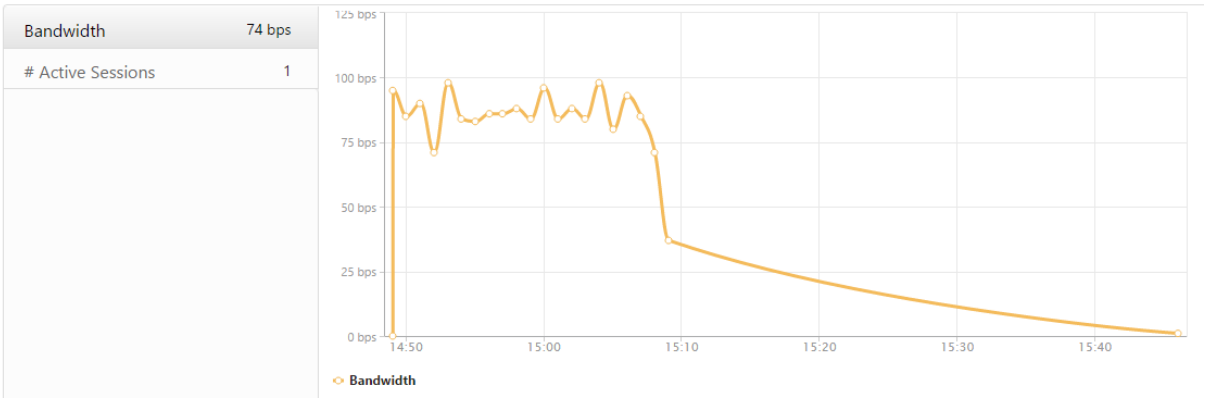
ICA Applications | Other Applications

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

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.

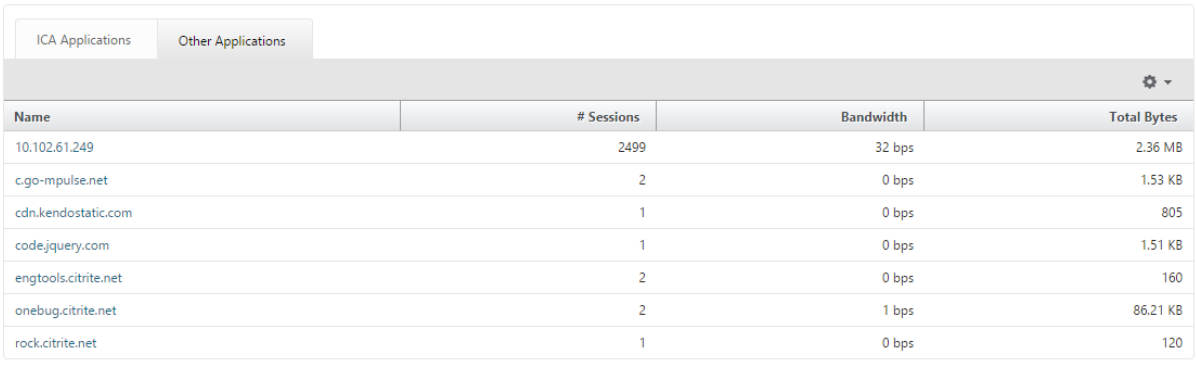


4. Un usuario ha iniciado sesión correctamente en ADC Gateway, pero no puede acceder a ciertos recursos de la red interna

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.

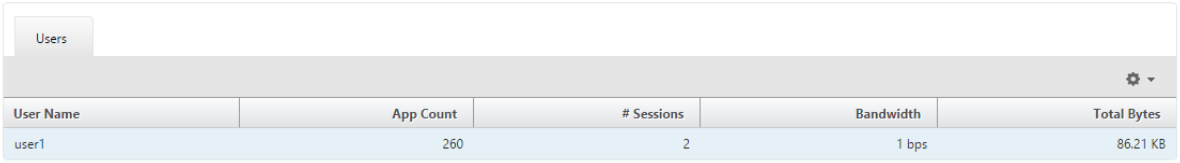
Ver el acceso de usuario para los recursos

1. En Citrix ADM, vaya a **Gateway > Gateway Insight > Aplicaciones**.
2. En la pantalla que aparece, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, seleccione la aplicación en la que el usuario no pudo iniciar sesión.



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

En la pantalla que aparece, desplácese hacia abajo y, en la tabla **Usuarios**, se muestran todos los usuarios que tienen acceso a esa aplicación.



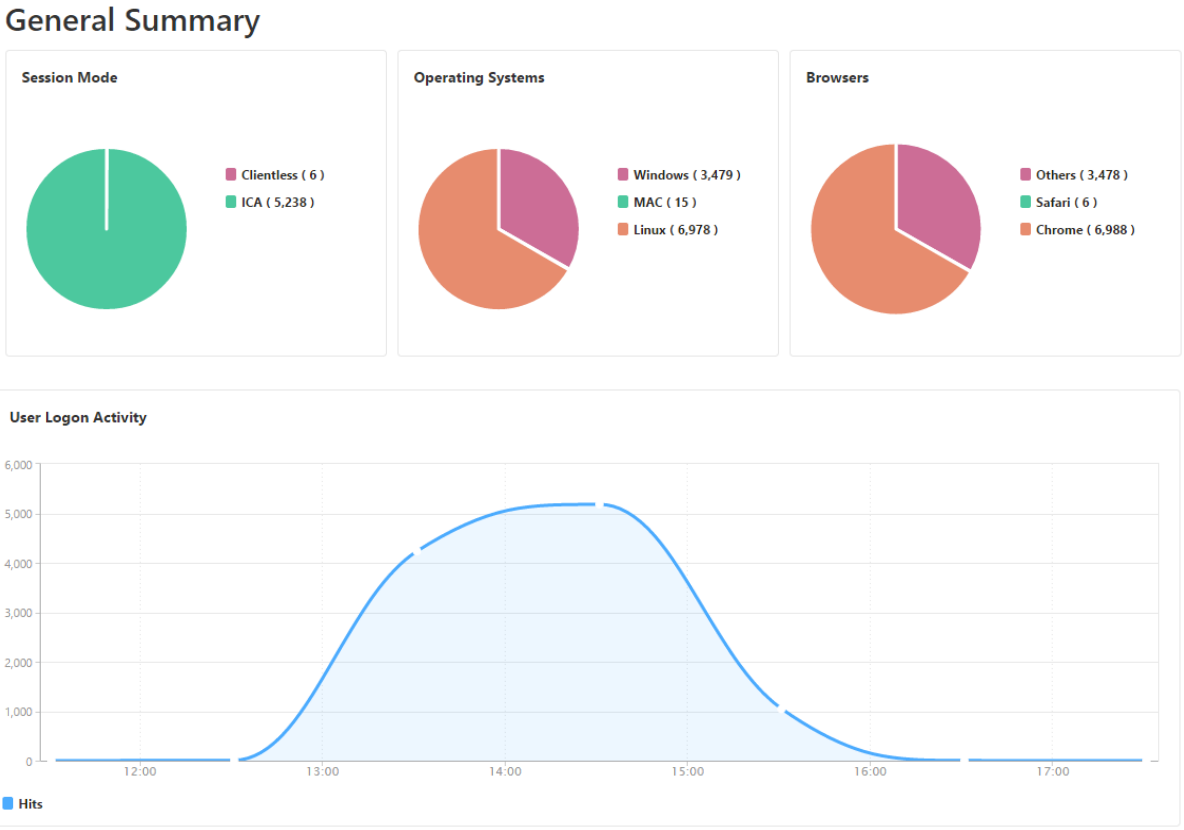
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

5. Es posible que diferentes usuarios usen distintas implementaciones de ADC Gateway o que inicien sesión en ADC 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 pasarela unificada o una implementación clásica de ADC 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 Citrix ADM, vaya a **Gateway > Gateway Insight**.
2. En la sección **Descripción general**, desplácese hacia abajo para ver los gráficos **Modo de sesión, Sistemas operativos, Exploradores** y **Actividad de inicio de sesión del usuario** que muestran los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora.



HDX Insight

November 16, 2022

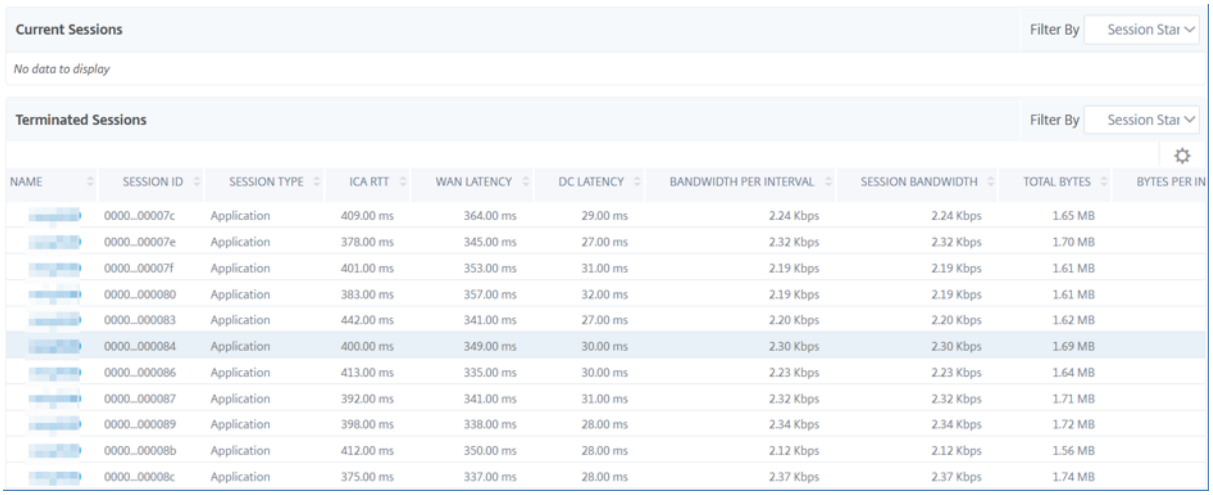
HDX Insight proporciona una visibilidad integral del tráfico de HDX a Citrix Virtual Apps and Desktops que pasa por Citrix ADC. También permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento. La disponibilidad de datos de visibilidad histórica y en tiempo real permite a Citrix ADM admitir una amplia variedad de casos de uso.

Para que aparezcan los datos, debe habilitar AppFlow en los servidores virtuales de la puerta de enlace ADC. 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. El análisis de Citrix ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configuración de grupos en Citrix ADM.

También puede ir a **HDX Insight** > **Aplicaciones** y hacer clic en **Duración del lanzamiento** para ver el tiempo que tarda la aplicación en lanzarse. 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 ADC que se ejecutan en la versión 12.0 del software.

Los siguientes clientes ligeros admiten HDX Insight:

- Thin Clients WYSE basados en Windows
- Clientes ligeros basados en Linux de WYSE
- Thin Clients de WYSE basados en Thinos
- Clientes ligeros basados en Ubuntu de 10 Zig

Identificación de la causa raíz de los problemas de rendimiento lento

Caso 1

El usuario experimenta retrasos al acceder a Citrix Virtual Apps and Desktops

Los retrasos pueden deberse a la latencia en la red del servidor, retrasos en el tráfico ICA causados por la red del servidor o latencia en la red del cliente.

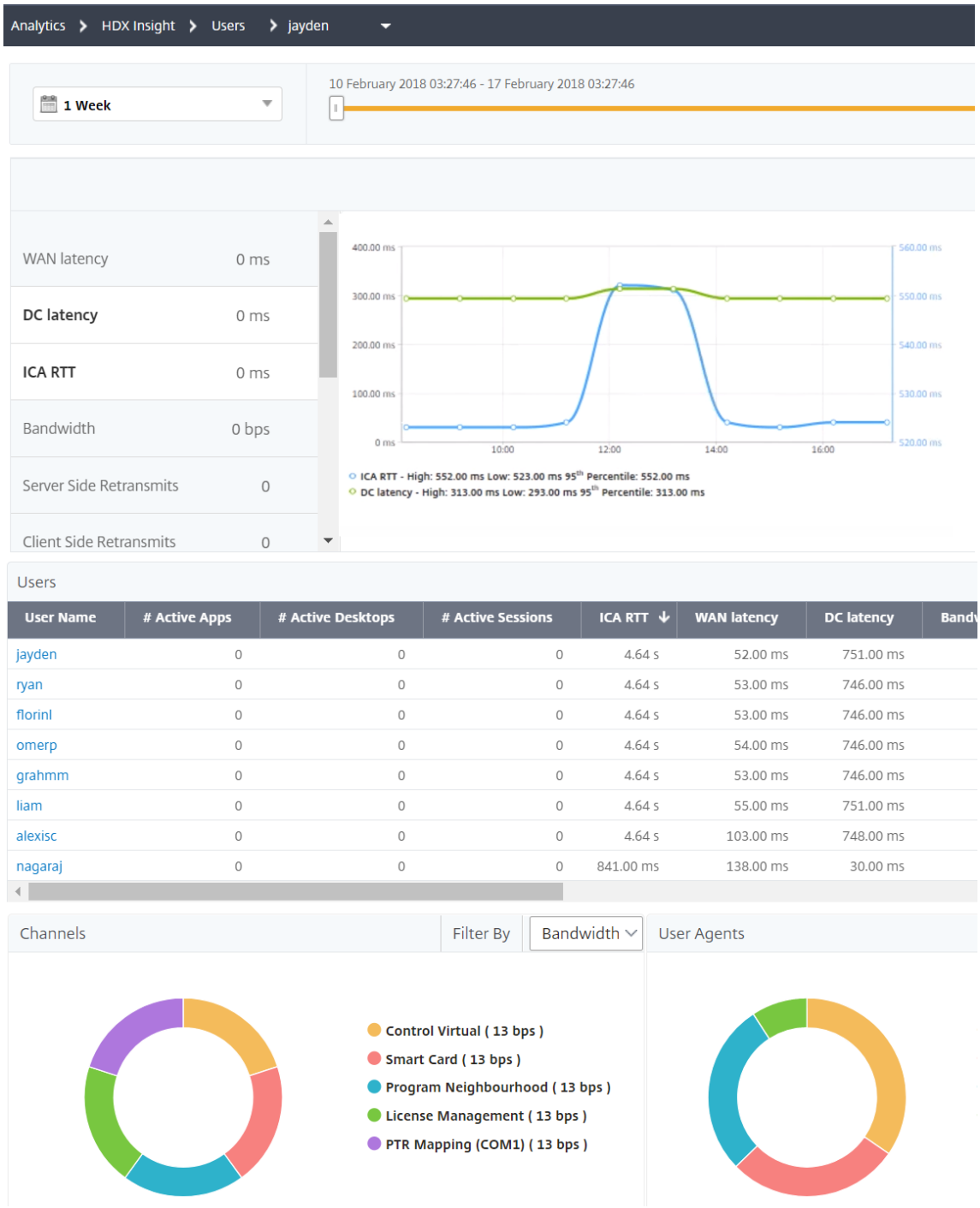
Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia WAN
- Latencia DC
- Demora de host

Para ver las métricas del cliente:

1. En la ficha **Analytics**, vaya a **HDX Insight** > **Usuarios**.

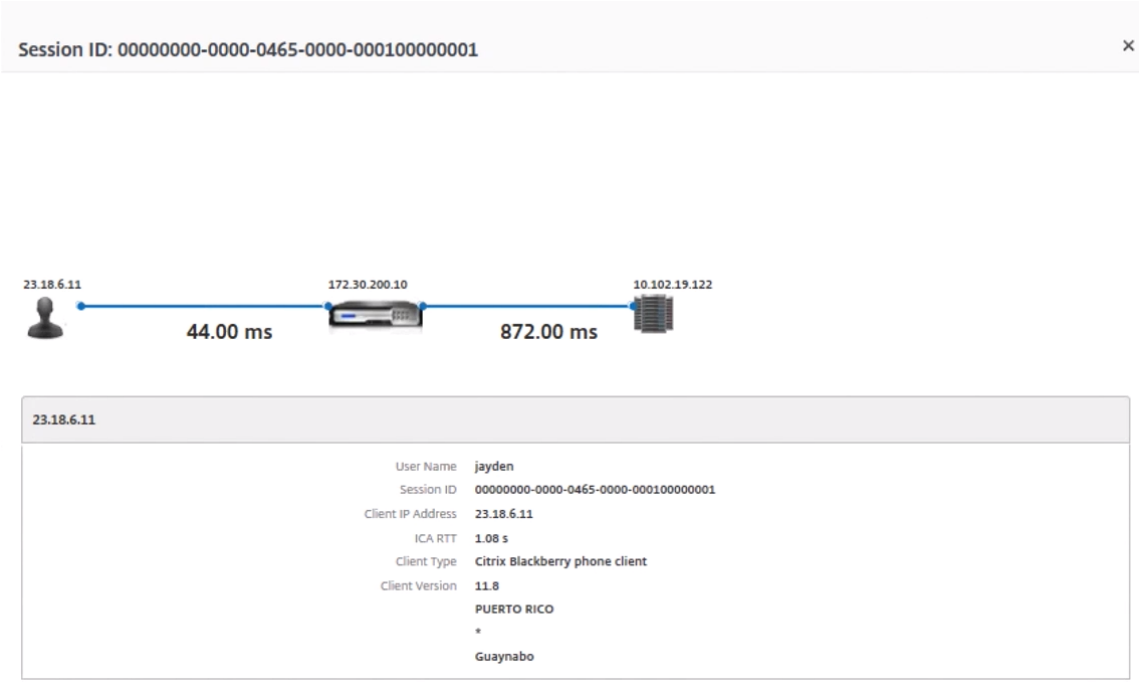
2. Desplácese hacia abajo y seleccione el nombre de usuario y seleccione el período de la lista. El período puede ser de un día, una semana, un mes o incluso puede personalizar el período del que quiere ver los datos.
3. El gráfico muestra los valores de latencia ICA RTT y DC del usuario para el período 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.

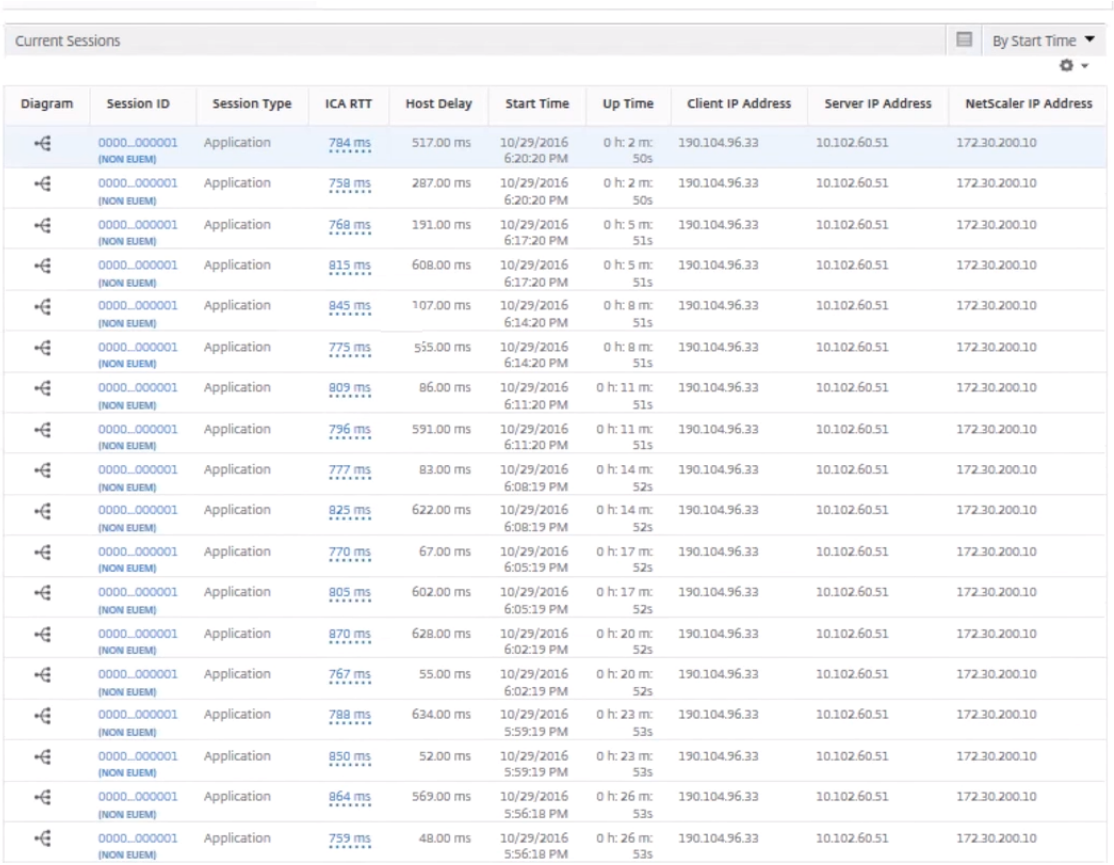
Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia de WAN
- Latencia de DC
- Demora del anfitrión

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	535.00 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 WAN** es de 12 milisegundos, pero el **retraso del host** es de 517 milisegundos. RTT alto con latencias de DC y WAN bajas indica un error de aplicación en el servidor host.

> **Nota**
>
> HDX Insight también muestra más métricas de usuario, como la fluctuación de WAN y las retransmisiones del lado del servidor si utiliza Citrix ADM ejecutando el software 11.1 compilación 51.21 o posterior. Para ver estas métricas, vaya a **Gateway** > **HDX Insight** > **Usuarios**y seleccione un nombre de usuario. Las métricas de usuario aparecen en la tabla junto al gráfico.

Mapa geográfico de HDX Insight

La función de mapa geográfico de Citrix ADM muestra el uso de aplicaciones web en diferentes ubicaciones geográficas de 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

Citrix ADM **habilita automáticamente** los geomaps para direcciones IP privadas o públicas, al habilitar **Web Insight**.

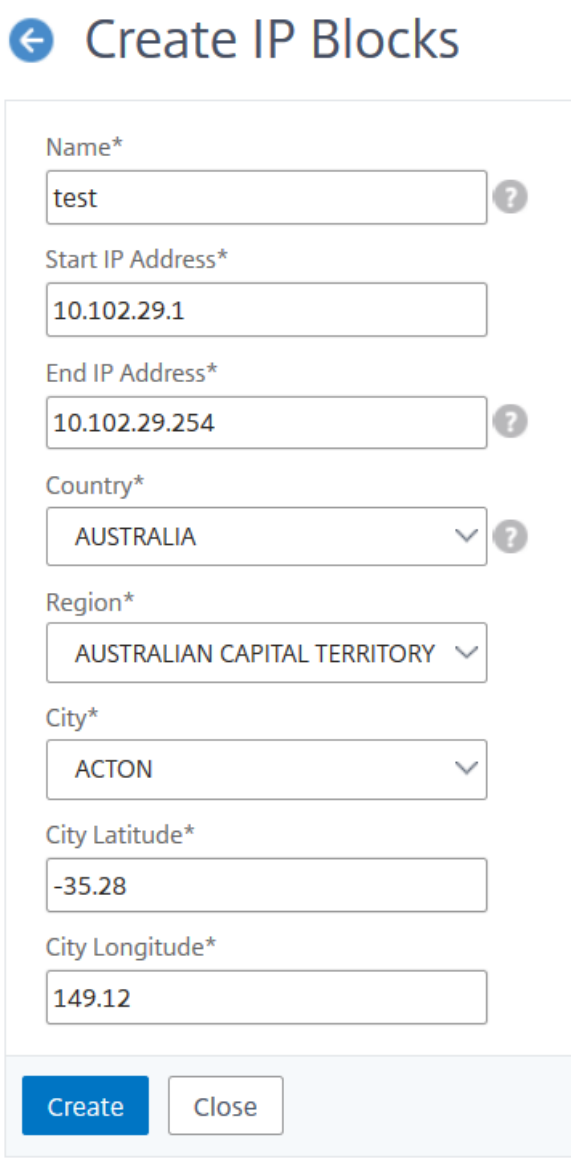
Crear un bloque de IP privado

Citrix ADM puede reconocer la ubicación de un cliente cuando la dirección IP privada del cliente se agrega al servidor Citrix ADM. Por ejemplo, si la dirección IP de un cliente se encuentra dentro del

intervalo de un bloque de direcciones IP privado asociado con Ciudad A, Citrix ADM reconoce que el tráfico se origina desde Ciudad A para este cliente.

Para crear un bloque IP:

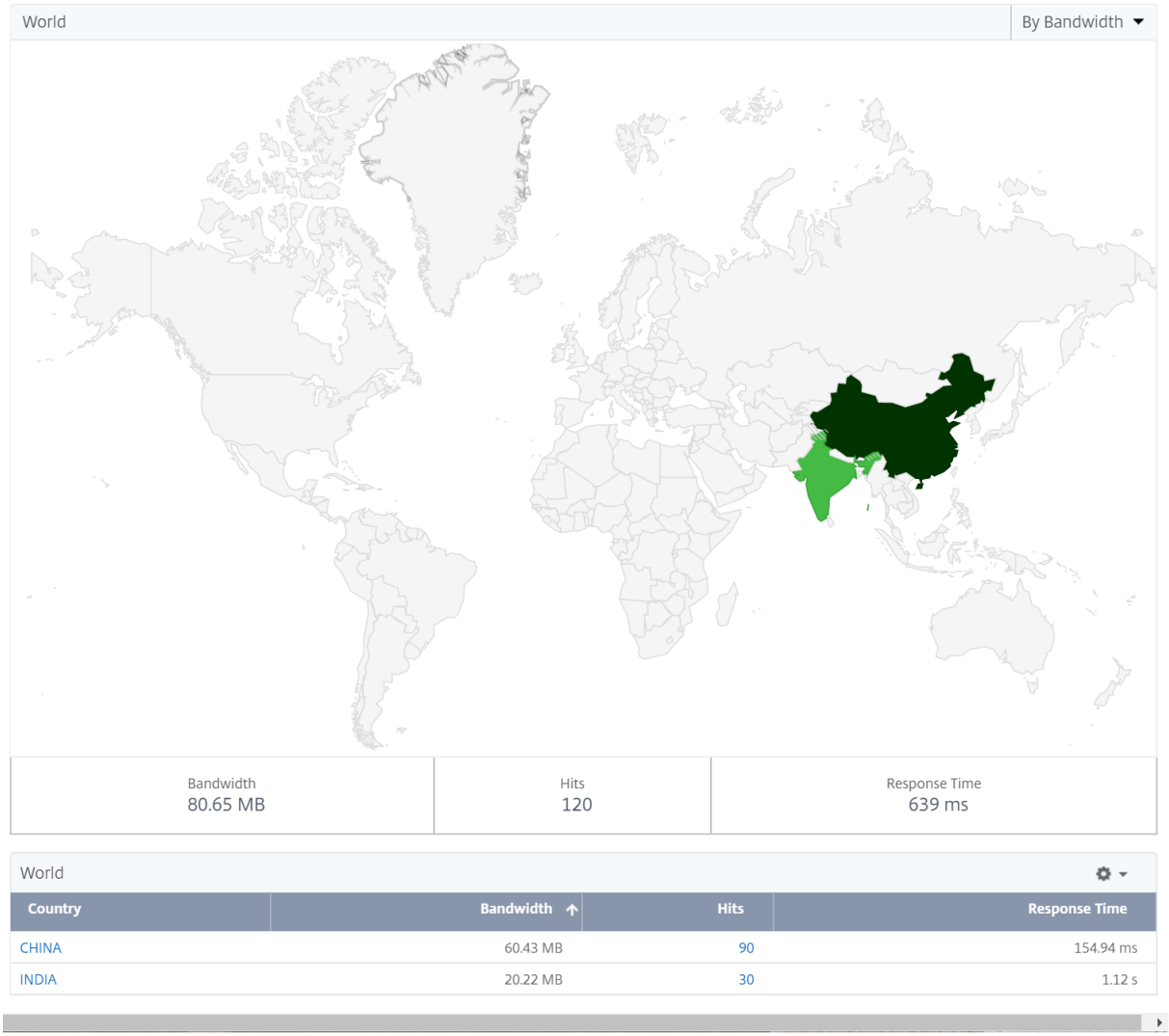
1. En Citrix ADM, vaya a **Configuración > Configuración de análisis > Bloques de IP**y, a continuación, haga clic en **Agregar**.
2. En la página **Crear Bloques de IP**, especifique los siguientes parámetros:
   - **Nombre**. Especifique un nombre para el bloque de IP privado
   - **Dirección IP inicial**. 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

Citrix ADM también puede reconocer la ubicación del cliente si el cliente utiliza una dirección IP pública. Citrix ADM tiene su archivo CSV de ubicación integrado que coincide con la ubicación según el intervalo de direcciones IP del cliente. Para usar un bloque de IP público, el único requisito es **habilitar la recopilación de datos geográficos** desde la página Configurar Insight.

> Nota
>
> Citrix ADM requiere una conexión a Internet para mostrar los mapas geográficos de una ubicación geográfica determinada. También se requiere conexión a Internet para exportar el GeoMap en formatos.pdf,.png o.jpg.



Para exportar el informe de este panel:

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

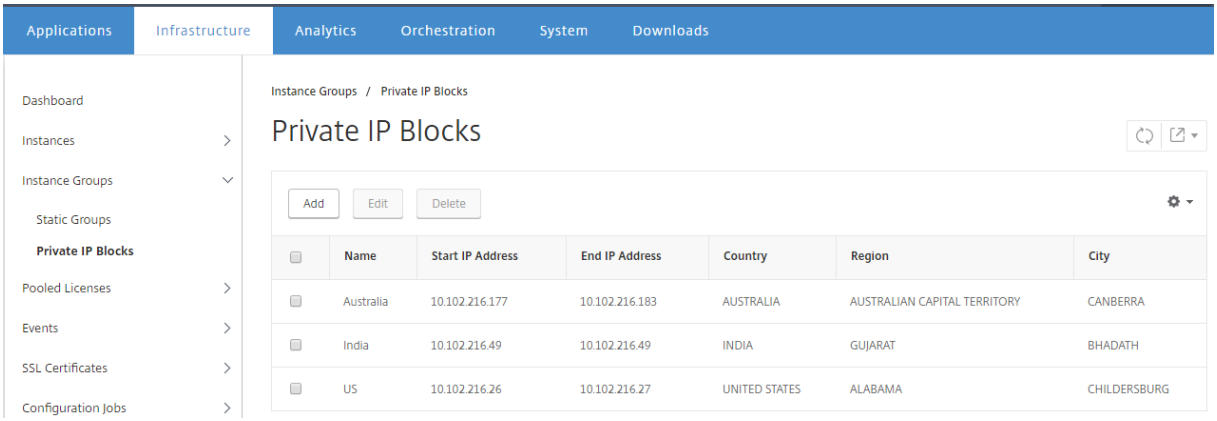
1. Seleccione la ficha **Exportar ahora** . Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Programar el informe a diario, semanal o mensual y enviarlo por correo electrónico o mensaje de Slack.

> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.

- Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

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.



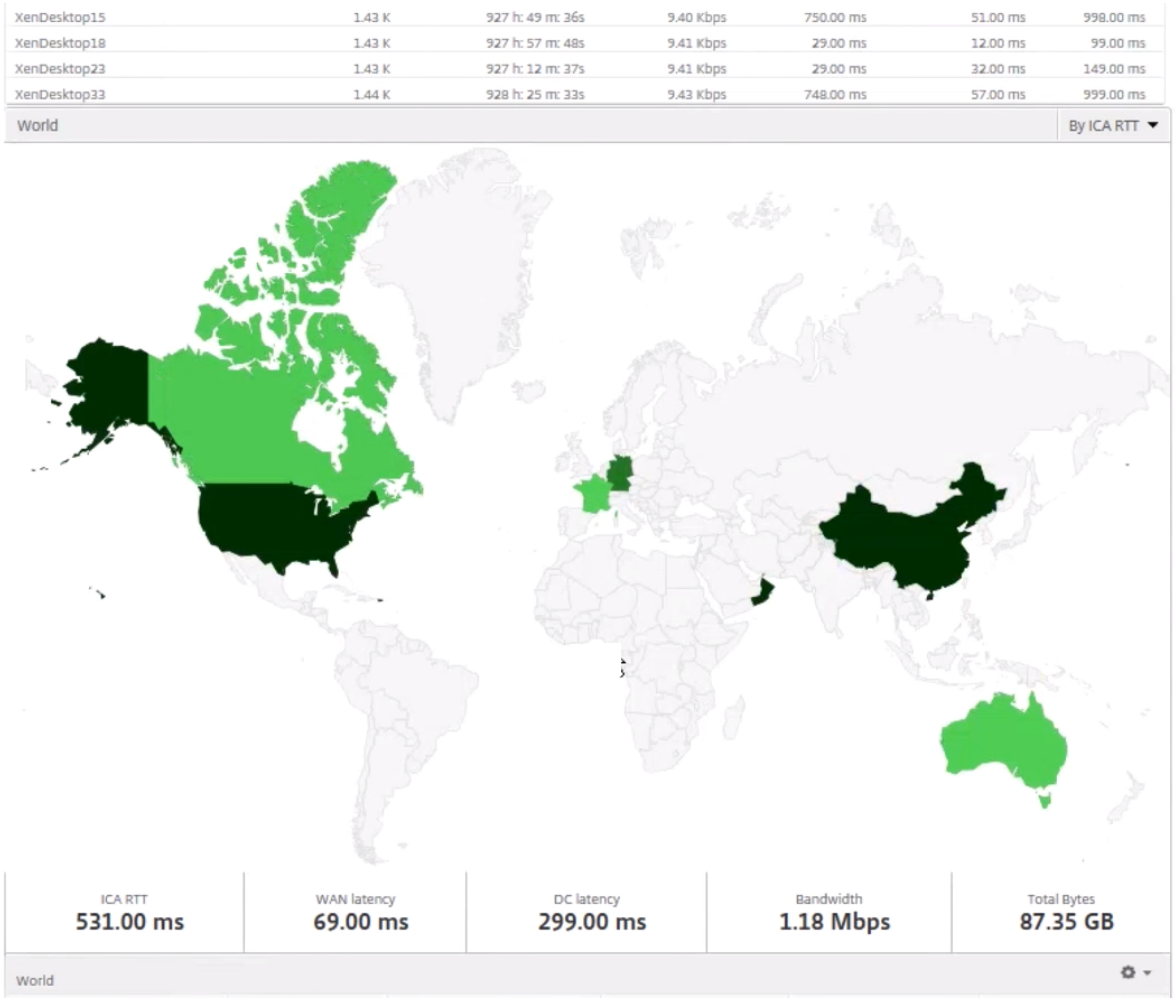
Caso de uso

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 ADC Gateway en Sclara.x.com para acceder al tráfico de VPN. Los usuarios indios utilizan el dispositivo ADC 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 enlace ADC, causando un retraso en la conexión a la VPN, por lo que algunos usuarios se conectan a India.x.com en lugar de SClara.x.com.

Un administrador de ADC que analice el tráfico puede usar 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, ya que la oficina de Santa Clara sólo tiene un dispositivo de puerta de enlace ADC a través del cual los usuarios pueden acceder al tráfico VPN. Por lo tanto, el administrador puede decidir instalar otra puerta de enlace de ADC, de modo que los usuarios tengan dos dispositivos de puerta de enlace de ADC locales a través de los cuales acceder a la VPN.



Limitaciones

Si las instancias de ADC tienen una licencia avanzada, los umbrales establecidos en Citrix ADM para HDX Insight no se activarán, ya que los datos analíticos se recopilan solo 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

December 2, 2022

HDX Insight permite al administrador ofrecer una experiencia de usuario excepcional al proporcionar una visibilidad integral del tráfico ICA que pasa por el dispositivo Citrix ADC.

HDX Insight ofrece capacidades de análisis de fallos y de inteligencia empresarial atractivas y potentes para la red, los escritorios virtuales, las aplicaciones y la estructura de aplicaciones. HDX Insight puede analizar al instante los problemas de los usuarios, recopilar datos sobre las conexiones de escritorio virtual y generar registros de AppFlow y presentarlos como informes visuales.

La configuración para habilitar la recopilación de datos en las instancias de ADC varía según la posición del dispositivo en la topología de despliegue. En este tema se incluyen los siguientes detalles:

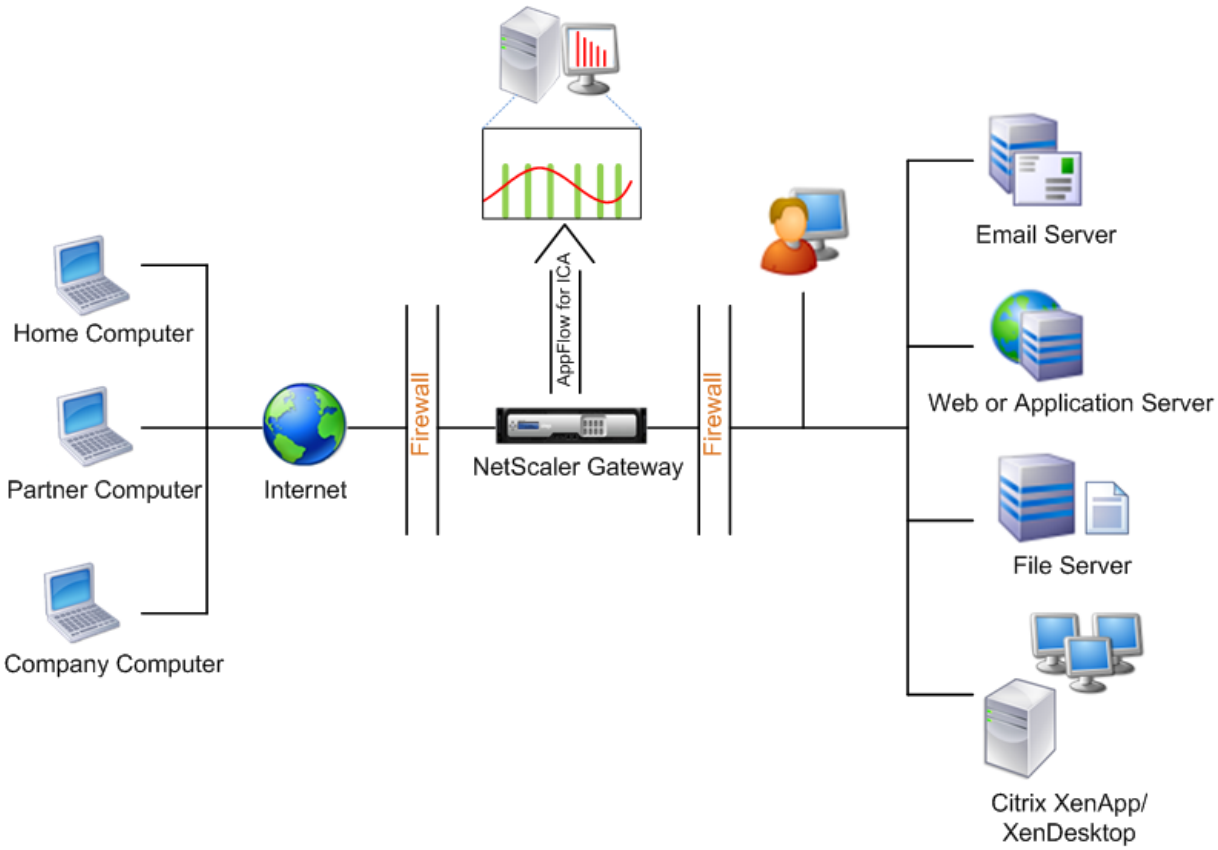
- Habilitar la recopilación de datos para supervisar los ADC de Citrix implementados en modo transparente
- Habilitar la recopilación de datos para los dispositivos Citrix ADC Gateway implementados en modo de salto único
- Habilitar la recopilación de datos para los dispositivos Citrix ADC Gateway implementados en modo de doble salto
- Habilitar la recopilación de datos para monitorear los ADC de Citrix implementados en modo de usuario LAN

Habilitar la recopilación de datos para dispositivos Citrix ADC Gateway implementados en modo de salto único

November 16, 2022

Cuando Citrix ADC Gateway se implementa en modo de salto único, la puerta de enlace ADC se encuentra en el borde de la red y proporciona conexiones ICA a la infraestructura de entrega de escritorio. 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 ADC a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo ADC Gateway al inventario de Citrix ADM y habilitar AppFlow en Citrix ADM. La siguiente imagen ilustra un Citrix ADM implementado en modo de salto único



Habilitar la función AppFlow desde Citrix ADM

1. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia ADC que quiere 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
```

Habilitar la recopilación de datos para supervisar los ADC de Citrix implementados en modo transparente

November 16, 2022

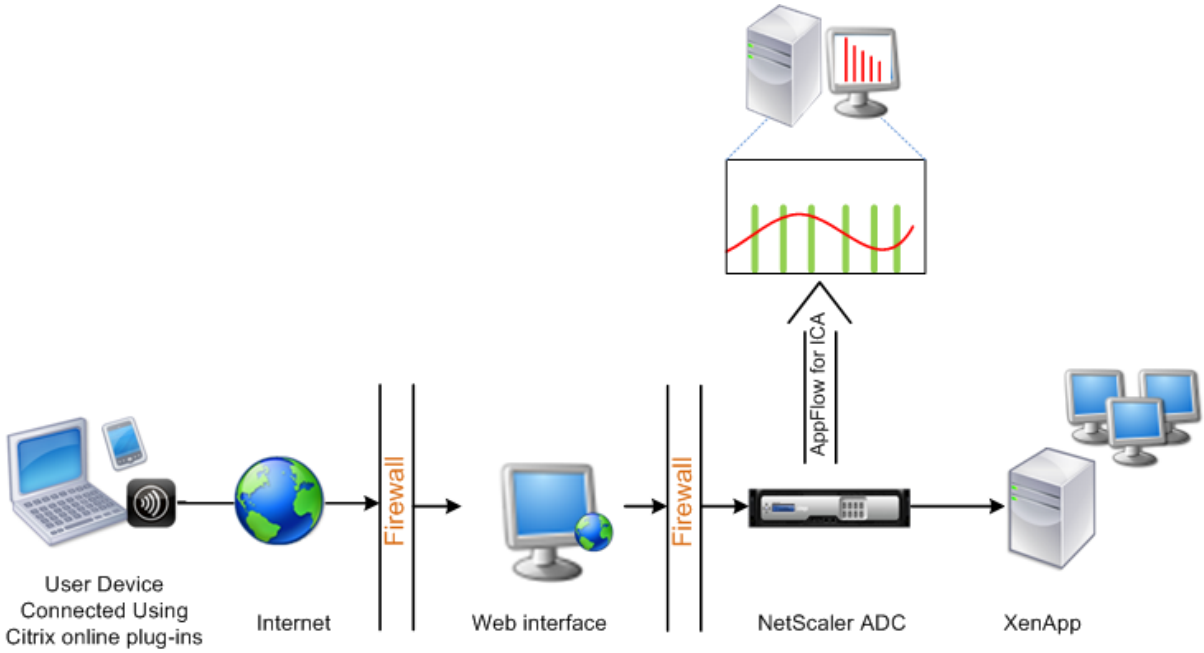
Cuando un Citrix ADC se implementa en modo transparente, los clientes pueden acceder a los servidores directamente, sin que intervenga ningún servidor virtual. Si un dispositivo Citrix ADC se implementa en modo transparente en un entorno de Citrix Virtual Apps and Desktops, el tráfico ICA no se transmite a través de una VPN.

Después de agregar Citrix ADC al inventario Citrix ADM, debe habilitar AppFlow para la recopilación de datos. Habilitar la recopilación de datos depende del dispositivo y del modo. En ese caso, debe agregar Citrix ADM como un recopilador de AppFlow en cada dispositivo Citrix ADC y debe configurar una directiva de AppFlow para recopilar todo o el tráfico ICA específico que fluye a través del dispositivo.

Nota

- No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo transparente mediante la utilidad de configuración de Citrix ADM.
- Para obtener información detallada sobre los comandos y su uso, consulte la Referencia de comandos.
- Para obtener información sobre las expresiones de directivas, consulte Directivas y expresiones.

La siguiente imagen muestra la implementación en red de un Citrix ADM cuando se implementa un Citrix ADC en modo transparente:



Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Especifique los puertos ICA en los que el dispositivo Citrix ADC escucha el tráfico.

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

Ejemplo:

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> **Nota**
>
> - Puede especificar hasta 10 puertos con este comando.
> - El número de puerto predeterminado es 2598. Puede modificar el número de puerto según sea necesario.

3. Agregue NetScaler Insight Center como un recopilador AppFlow en el dispositivo Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Ejemplo:


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> **Nota**
>
> Para ver los recopiladores AppFlow configurados en el dispositivo Citrix ADC, utilice el comando **show appflow collector** .

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

Ejemplo:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

Ejemplo:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Nota**
>
> El valor de **tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarlo al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```


8. Guarde la configuración.

```
save ns config
<!--NeedCopy-->
```

Habilitar la recopilación de datos para dispositivos Citrix ADC Gateway implementados en modo de salto doble

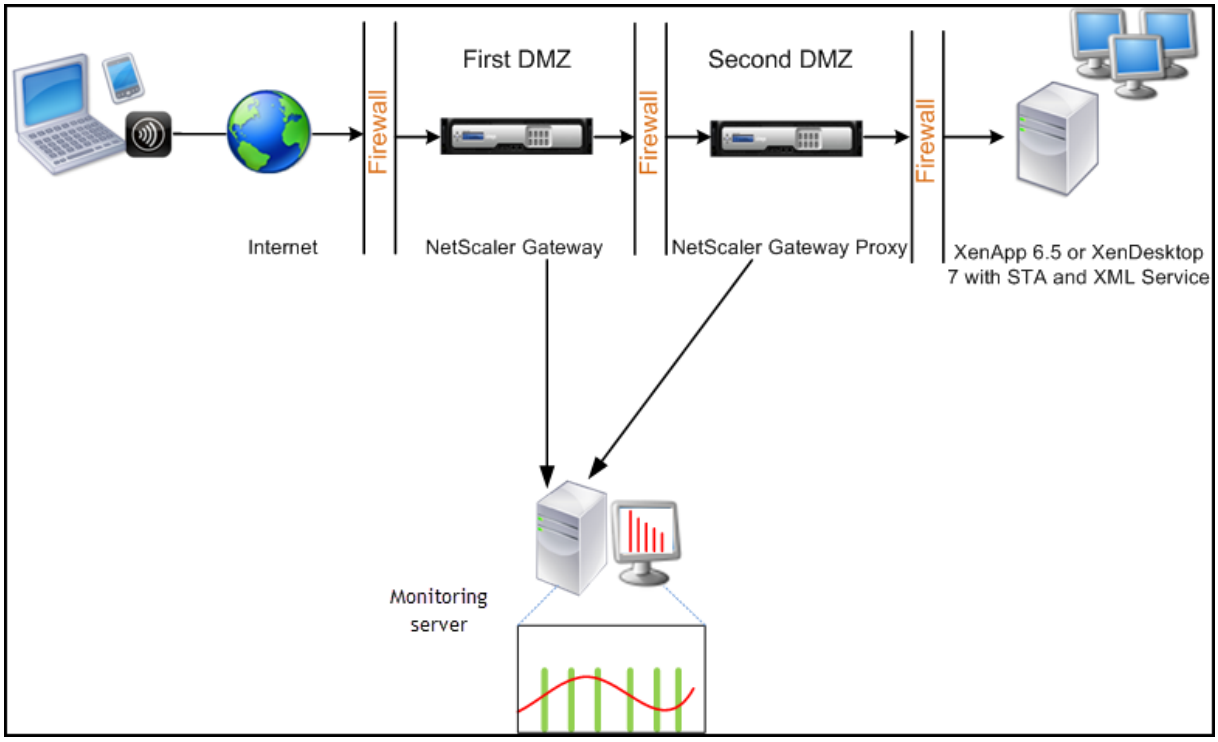
November 17, 2022

El modo de doble salto de Citrix ADC 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, mediante Citrix ADM, puede analizar:

- El número de saltos (dispositivos Citrix ADC 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 imagen siguiente indica que Citrix ADM y Citrix ADC Gateway en la primera DMZ se implementan en la misma subred.



Citrix ADC Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Este Citrix ADC Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

El Citrix ADC Gateway de la segunda DMZ sirve como dispositivo proxy de Citrix ADC Gateway. Este Citrix ADC Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de los usuarios a la granja de servidores.

Citrix ADM se puede implementar en la subred que pertenece al dispositivo Citrix ADC Gateway en la primera DMZ o en la subred que pertenece al dispositivo Citrix ADC Gateway segunda DMZ.

En modo de salto doble, Citrix ADM recopila los registros TCP de un dispositivo y los registros ICA del otro dispositivo. Después de agregar los dispositivos de Citrix ADC Gateway al inventario de Citrix ADM y habilitar la recopilación de datos, cada dispositivo exporta los informes haciendo un seguimiento del recuento de saltos y el ID de la cadena de conexión.

Para que Citrix ADM identifique qué dispositivo está exportando registros, cada dispositivo se especifica con un recuento de saltos y cada conexión se especifica con un ID de cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos Citrix ADC Gateway a través de los cuales el tráfico fluye de un cliente a los servidores. El ID de cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexión para relacionar los datos de los dispositivos Citrix ADC Gateway y generar los informes.

Para supervisar los dispositivos Citrix ADC Gateway implementados en este modo, primero debe agregar Citrix ADC Gateway al inventario de Citrix ADM, habilitar AppFlow en Citrix ADM y, a continuación, ver los informes en el panel de control de Citrix ADM.

Habilitar la recopilación de datos en Citrix ADM

Si habilita Citrix ADM para comenzar a recopilar los detalles de ICA de ambos dispositivos, los detalles recopilados serán redundantes. Para superar esta situación, debe habilitar AppFlow para TCP en el primer dispositivo Citrix ADC Gateway y, a continuación, habilitar AppFlow para ICA en el segundo dispositivo. Al hacerlo, uno de los dispositivos exporta registros ICA AppFlow y el otro dispositivo exporta registros TCP AppFlow. Esto también ahorra tiempo de procesamiento al analizar el tráfico ICA.

Para habilitar la función AppFlow desde Citrix ADM:

1. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia de Citrix ADC que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione los servidores virtuales y haga clic en **Habilitar análisis**.

4. Seleccione Web **Insight**
5. Haga clic en **Aceptar**.

Configurar los dispositivos de Citrix ADC Gateway para exportar datos

Después de instalar los dispositivos Citrix ADC Gateway, debe configurar las siguientes opciones en los dispositivos Citrix ADC Gateway para exportar los informes a Citrix ADM:

- Configure los servidores virtuales de los dispositivos Citrix ADC Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlace el servidor virtual Citrix ADC Gateway de la segunda DMZ al servidor virtual Citrix ADC Gateway de la primera DMZ.
- Habilite el doble salto en el Citrix ADC Gateway en la segunda DMZ.
- Inhabilite la autenticación en el servidor virtual de Citrix ADC Gateway en la segunda DMZ.
- Habilite uno de los dispositivos Citrix ADC Gateway para exportar registros ICA
- Permita que el otro dispositivo Citrix ADC Gateway exporte registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos Citrix ADC Gateway.

Configure Citrix ADC Gateway mediante la interfaz de línea de comandos:

1. Configure el servidor virtual de Citrix ADC Gateway en la primera DMZ para comunicarse con el servidor virtual de Citrix ADC Gateway en la segunda DMZ.

add vpn nextHopServer \\\ <name\ > OFF)] [**-imgGifToPng**] … <nextHopIP\ > <nextHopPort\ >\ [**-secure** **(ACTIVADO**)

```
add vpn nextHopServer nh1 10.102.2.33 8443  - secure ON
<!--NeedCopy-->
```

2. Enlace el servidor virtual Citrix ADC Gateway de la segunda DMZ al servidor virtual Citrix ADC Gateway de la primera DMZ. Ejecute el siguiente comando en Citrix ADC Gateway en la primera DMZ:

   vincular vpn vserver \ <name\ > **-NextHopServer** \ <name\ >

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. Habilite el doble salto y AppFlow en Citrix ADC Gateway en la segunda DMZ.

set vpn vserver \ <name\ >\ [- **DoubleHop** (ACTIVADO)	DESACTIVADO) [- **AppFlowLog** (ACTIVADO	DISABLED)]

```
set vpn vserver vpnhop2  - doubleHop ENABLED  - appFlowLog ENABLED
<!--NeedCopy-->
```

4. Inhabilite la autenticación en el servidor virtual de Citrix ADC Gateway en la segunda DMZ.

set vpn vserver\ <name\ >\ [**-authentication** **(ACTIVADO**)	OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. Habilite uno de los dispositivos Citrix ADC Gateway para exportar registros TCP.

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  - type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. Habilite el otro dispositivo Citrix ADC Gateway para exportar registros ICA:

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. Habilite el encadenamiento de conexiones en los dispositivos Citrix ADC Gateway:

establecer el parámetro AppFlow [**-ConnectionChaining** (ACTIVADO)	DESHABILITADO)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

Configuración de Citrix ADC Gateway mediante la utilidad de configuración:

1. Configure Citrix ADC Gateway en la primera DMZ para comunicarse con Citrix ADC Gateway en la segunda DMZ y vincular Citrix ADC Gateway en la segunda DMZ con Citrix ADC Gateway en la primera DMZ.
    a) En la ficha **Configuración**, expanda **Citrix ADC Gateway** y haga clic en **Servidores virtuales**.
    b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzadas, expanda **Aplicaciones publicadas**.
    c) Haga clic en **Servidor de salto siguiente** y vincule un servidor de salto siguiente al segundo dispositivo Citrix ADC Gateway.
2. Habilite el doble salto en el Citrix ADC Gateway en la segunda DMZ.
    a) En la ficha **Configuración**, expanda **Citrix ADC 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. Deshabilite la autenticación en el servidor virtual de Citrix ADC Gateway en la segunda DMZ.
    a) En la ficha **Configuración**, expanda **Citrix ADC Gateway** y haga clic en **Servidores virtuales**.
    b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo **Configuración básica**, haga clic en el icono de edición.
    c) Expanda **Más**y desactive **Habilitar autenticación**.
4. Habilite uno de los dispositivos Citrix ADC Gateway para exportar registros TCP.
    a) En la ficha **Configuración**, expanda **Citrix ADC Gateway** y haga clic en **Servidores virtuales**.
    b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzadas, expanda Directivas.
    c) Haga clic en el icono + y, en la lista **Elegir directiva**, seleccione **AppFlow** y, en la lista **Elegir tipo**, seleccione **Otra solicitud TCP**.
    d) Haga clic en **Continue**.
    e) Agregue un enlace de directivas y haga clic en **Cerrar**.
5. Habilite el otro dispositivo Citrix ADC Gateway para exportar registros ICA:
    a) En la ficha **Configuración**, expanda **Citrix ADC Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo **Avanzadas**, expanda **Directivas**.

c) Haga clic en el icono + y, en la lista **Elegir directiva**, seleccione **AppFlow** y, en la lista **Elegir tipo**, seleccione **Otra solicitud TCP**.

d) Haga clic en **Continue**.

e) Agregue un enlace de directivas y haga clic en **Cerrar**.

6. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix ADC 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**.

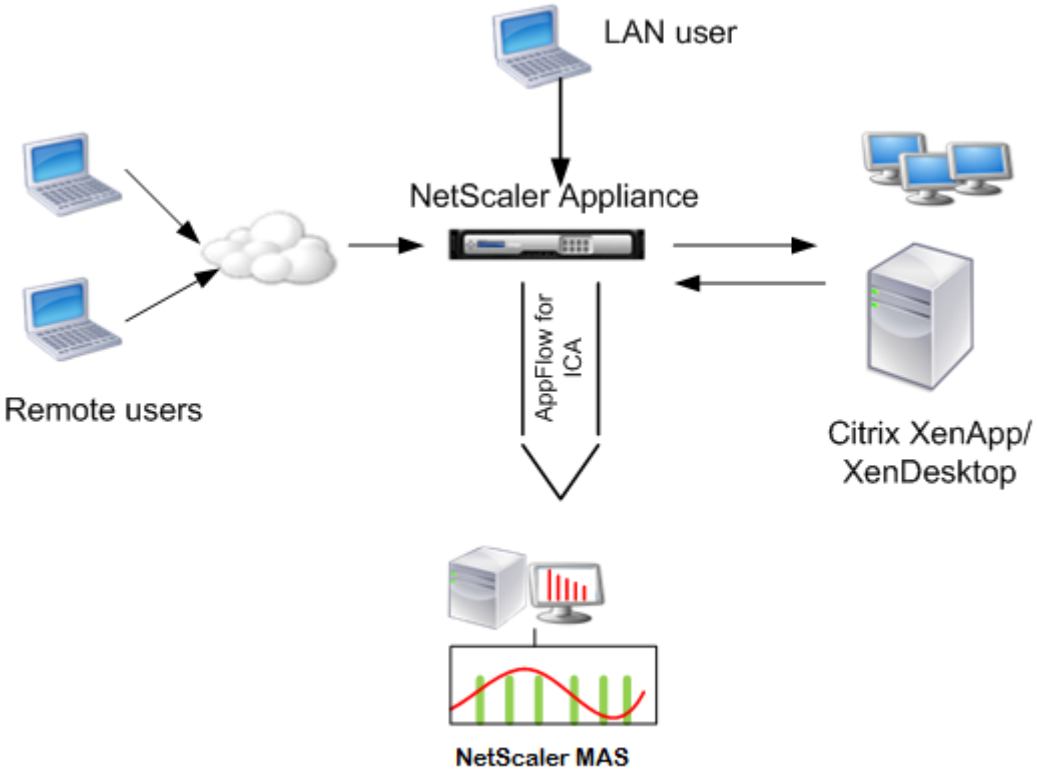
Habilitar la recopilación de datos para supervisar los ADC de Citrix implementados en modo de usuario LAN

November 16, 2022

Los usuarios externos que acceden a las aplicaciones de Citrix Virtual App o Desktop deben autenticarse en Citrix ADC Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a ADC Gateway. Además, en una implementación de modo transparente, el administrador debe aplicar manualmente las directivas de redirección para que las solicitudes se redirijan al dispositivo Citrix ADC.

Para superar estos desafíos y para que los usuarios de LAN se conecten directamente a las aplicaciones de Citrix Virtual Apps and Desktops, puede implementar el dispositivo ADC en un modo de usuario de LAN mediante la configuración de un servidor virtual de redirección de caché. El servidor virtual de redirección de caché actúa como un proxy SOCKS en el dispositivo ADC Gateway.

La siguiente imagen muestra Citrix ADM implementado en **modo de usuario LAN**.



> **Nota**
>
> El dispositivo Citrix ADC Gateway debe poder comunicarse con el agente Citrix ADM.

Para supervisar los dispositivos Citrix ADC implementados en este modo, primero agregue el dispositivo Citrix ADC al inventario de Citrix ADC Insight, habilite AppFlow y, a continuación, vea los informes en el panel de control.

Después de agregar el dispositivo Citrix ADC al inventario de Citrix ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo de usuario de LAN mediante la utilidad de configuración de Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte Referencia de comandos.
> - Para obtener información sobre las expresiones de directiva, vea Directivas y expresiones.

Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en el dispositivo Citrix ADC.

2. Agregue un servidor virtual de redirección de caché de proxy de reenvío con la IP y el puerto proxy, y especifique el tipo de servicio como HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
    cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

Ejemplo:

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
    cltTimeout 180
<!--NeedCopy-->
```

> **Nota:**
>
> Si accede a la red LAN mediante un dispositivo Citrix ADC 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\>
<!--NeedCopy-->
```

Ejemplo:

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. Agregue Citrix ADM como un recopilador AppFlow en el dispositivo Citrix ADC.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
    \\>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```


Ejemplo:

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

Ejemplo:

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
   type\>
<!--NeedCopy-->
```

Ejemplo:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> **Nota**
>
> El valor 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
<!--NeedCopy-->
```

Ejemplo:

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. Guarde la configuración.

```
save ns config
<!--NeedCopy-->
```


Crear umbrales y configurar alertas para HDX Insight

November 16, 2022

HDX Insight en Citrix ADM le permite supervisar el tráfico de HDX que pasa a través de las instancias de Citrix ADC. Citrix ADM le permite establecer umbrales en varios contadores utilizados para supervisar el tráfico de Insight. También puede configurar reglas y crear alertas en Citrix ADM.

El tipo de tráfico HDX está asociado con varias entidades, como aplicaciones, escritorios, puertas de enlace, licencias y usuarios. Cada entidad puede contener diferentes métricas asociadas a ellas. Por ejemplo, la entidad de aplicación está asociada con varios accesos, ancho de banda consumido por la aplicación y tiempo de respuesta del servidor. Una entidad de usuario puede asociarse con latencia de WAN, latencia DC, RTT ICA y ancho de banda consumido por un usuario.

La administración de umbrales de HDX Insight en Citrix ADM le permitió crear reglas y configurar alertas de forma proactiva cada vez que se superaban los umbrales establecidos. Ahora, esta administración de umbrales se amplía para configurar un grupo de reglas de umbrales. Ahora puede supervisar el grupo en lugar de las reglas individuales. Un grupo de reglas de umbral comprende una o más reglas de umbral definidas por el usuario para las métricas elegidas de entidades como usuarios, aplicaciones y escritorios. Cada regla se controla con un valor esperado que se introduce al crear la regla. En la entidad de usuarios, el grupo de umbrales también se puede asociar con una geolocalización.

Una alerta se genera en Citrix ADM solo si se incumplen todas las reglas del grupo de umbrales configurado. Por ejemplo, puede supervisar una aplicación según el recuento total de inicios de sesión y también el recuento de lanzamientos de aplicaciones como un grupo umbral. Solo se genera una alerta si se infringen ambas reglas. Esto le permite establecer umbrales más realistas en una entidad.

A continuación se enumeran algunos ejemplos:

- Regla de umbral 1: 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, Citrix ADM genera un evento que indica una violación del umbral y se crea una alerta para cada evento.

Debe configurar cómo recibe la alerta. Puede habilitar la alerta para que se muestre en Citrix ADM o recibir la alerta como un correo electrónico o ambos, o como un SMS en su dispositivo móvil. Para las dos últimas acciones, debe configurar el servidor de correo electrónico o el servidor de SMS en Citrix ADM.

Los grupos de umbral también se pueden vincular a las geolocalizaciones para el supervisión 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 Citrix ADC 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.

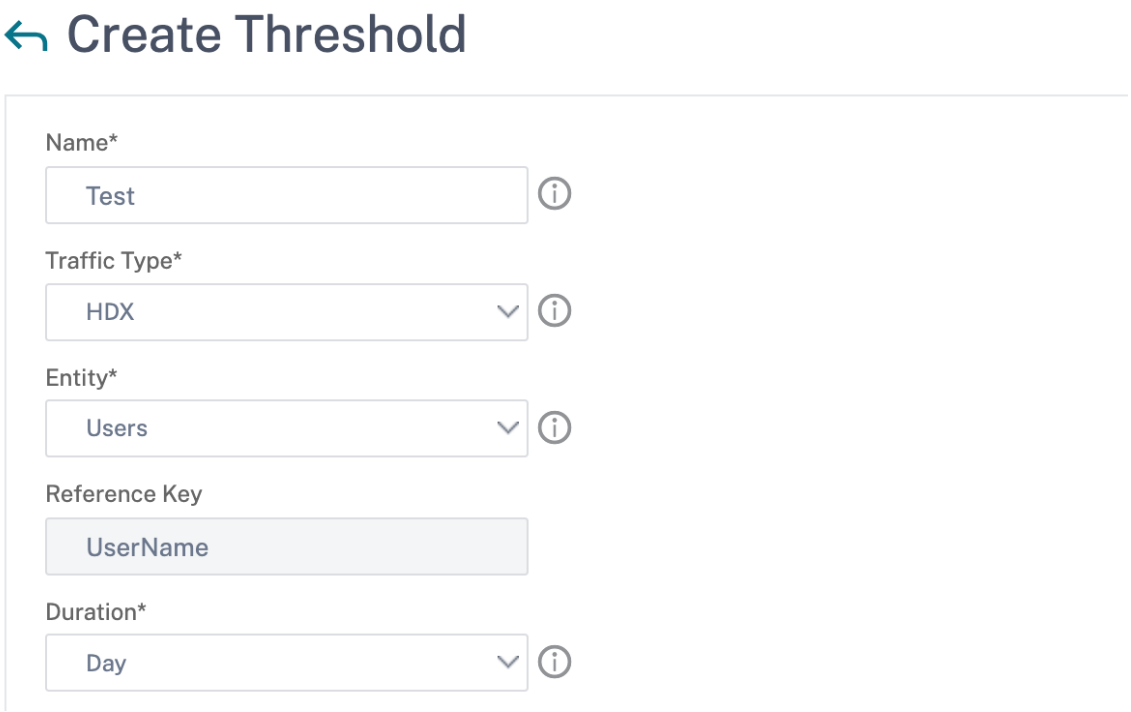
Los usuarios de ABC Inc. tienen una presencia distribuida. Algunos usuarios se encuentran cerca del centro de datos, mientras que algunos se encuentran en más lejos del centro de datos. Como la base de usuarios se distribuye ampliamente, las métricas y los umbrales correspondientes también varían entre 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 Citrix ADM

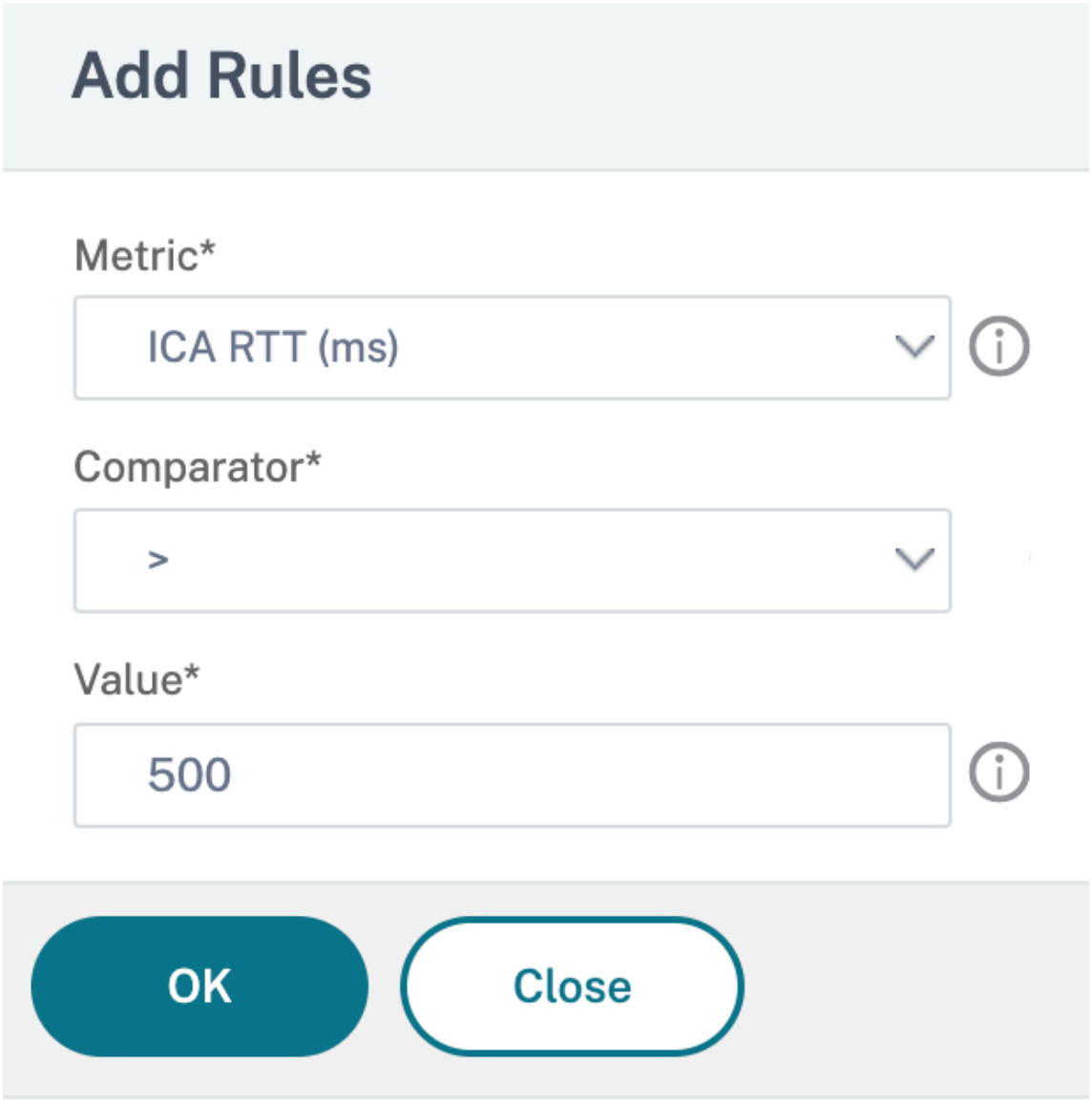
1. En Citrix ADM, vaya a **Configuración > Configuración de análisis > Umbrales**. En la página **Umbrales** que se abre, haga clic en **Agregar**.
2. En la página **Crear umbrales y alertas**, especifique los siguientes detalles:
    a) **Nombre**. Escriba un nombre para crear un evento para el que Citrix ADM 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.

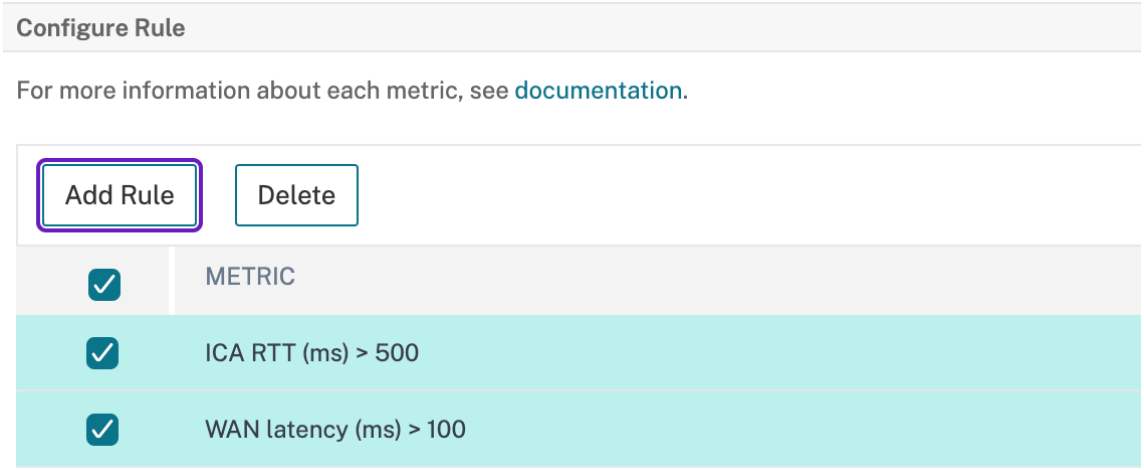


3. **Creación de grupo de reglas de umbral para todas las entidades:**

   Para el tráfico de HDX, debe crear una regla haciendo clic en **Agregar regla**. Introduzca los valores en la ventana emergente **Agregar reglas** que se abre.

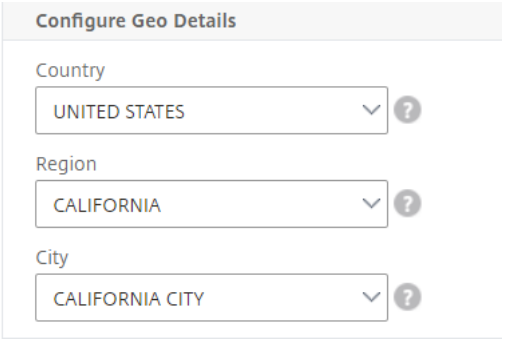


Puede crear varias reglas para supervisar cada entidad. La creación de varias reglas en un solo grupo le permite supervisar las entidades como un grupo de reglas de umbral en lugar de reglas individuales. Haga clic en **Aceptar** para cerrar la ventana.

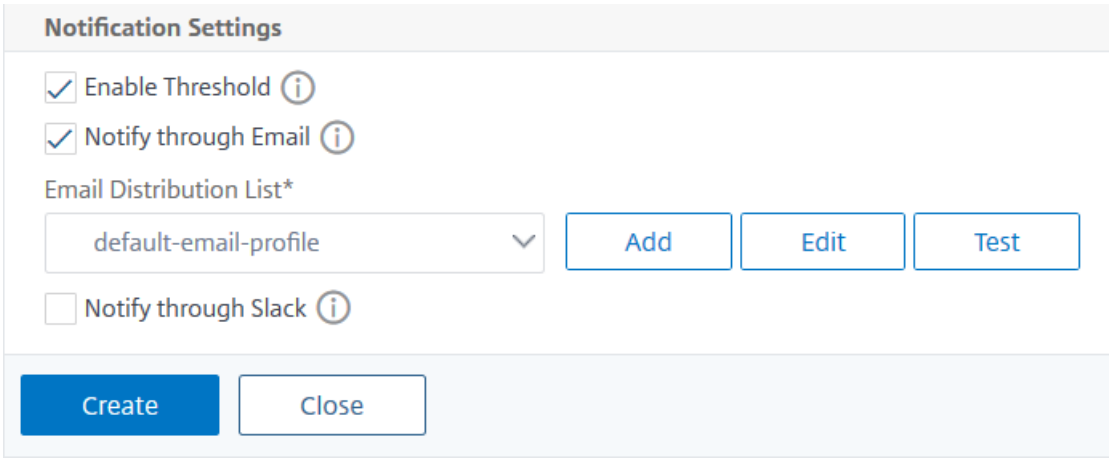


4. **Configuración del etiquetado de geolocalización para la entidad Usuarios:**

   Si lo quiere, puede crear una alerta basada en la ubicación para la entidad de usuario en la sección **Configurar detalles geográficos** . La siguiente imagen muestra un ejemplo de creación de un etiquetado basado en geolocalización para supervisar el rendimiento de latencia de WAN para los usuarios de la costa oeste de los Estados Unidos.



5. Haga clic en **Habilitar umbrales** para permitir que Citrix ADM comience a supervisar las entidades.
6. Opcionalmente, configure acciones como 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

December 2, 2022

HDX insight proporciona una visibilidad completa de los informes y las métricas relacionados con el tráfico HDX en sus instancias de Citrix ADC.

Puede ver las métricas de HDX de cualquier entidad seleccionada. Las vistas incluyen las siguientes categorías de entidades:

- **Usuarios**: Muestra los informes de todos los usuarios que acceden a Citrix Virtual Apps and Desktops dentro del intervalo de tiempo seleccionado.
- **Aplicaciones:** muestra los informes del número total de aplicaciones y toda la información relevante relacionada, como el número total de veces que se lanzaron las aplicaciones dentro del intervalo de tiempo especificado.
- **Instancias**: Muestra los informes de las instancias ADC que actúan como puertas de enlace para el tráfico entrante.
- **Escritorios**: muestra los informes de los escritorios utilizados en el período de tiempo seleccionado.
- **Licencias**: muestra los informes del total de licencias de VPN con SSL utilizadas dentro del intervalo de tiempo especificado.

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

November 17, 2022

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 Citrix ADC y Citrix ADM.
- Generación de registros para el tráfico HDX/ICA en Citrix ADC.
- Población de registros en Citrix ADM.

Lista de comprobación de configuración de HDX Insight

- Asegúrese de que la función AppFlow está habilitada en Citrix ADC. Para obtener más información, consulte Habilitar AppFlow.
- Compruebe la configuración de HDX Insight en la configuración de Citrix ADC en ejecución.

  Ejecute el comando `show running | grep -i <appflow_policy>` para comprobar la configuración de HDX Insight. Asegúrese de que el tipo de enlace es ICA REQUEST. Por ejemplo;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Para el modo transparente, el tipo de enlace debe ser ICA_REQ_DEFAULT. Por ejemplo;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Para la implementación de Access Gateway o de un solo salto, asegúrese de que la directiva de HDX Insight AppFlow esté enlazada al servidor virtual VPN, por donde fluye el tráfico HDX/ICA.
- Para el modo transparente o el modo de usuario LAN, asegúrese de que los puertos ICA 1494 y 2598 están configurados.
- Compruebe que el parámetro `appflowlog` en Citrix Gateway o el servidor virtual VPN esté habilitado para Access Gateway o implementación de doble salto. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.
- Compruebe que "Conexión encadenamiento" está activado en Citrix ADC de doble salto. Para obtener más información, consulte Configuración de dispositivos Citrix 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 Citrix ADC.

Lista de comprobación de conectividad entre Citrix ADC y Citrix ADM

- Compruebe el estado del recopilador AppFlow en Citrix ADC. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre Citrix ADC y AppFlow Collector.
- Compruebe los resultados de las directivas de HDX Insight AppFlow.

  Ejecute el comando `show appflow policy <policy_name>` para comprobar los aciertos de la directiva 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 Citrix ADC

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 Citrix ADC.

Omitir código	Mensaje de error	Causa del error
100	NS_ICA_ERR_NULL_FRAG	Error en el manejo de fragmentos ICA, probablemente debido a condiciones de memoria
101	NS_ICA_ERR_INVALID_HS_CMD	Se recibió un comando de enlace no válido
102	NS_ICA_ERR_REDUC_PARAM_C	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_B	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_DECODE	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_DEC	Decodificador no válido para el canal Thinwire
109	NS_ICA_ERR_REDUC_NO_DECODER	No hay decodificador definido para el canal

Omitir código	Mensaje de error	Causa del error
110	NS_ICA_ERR_REDUC_V3_EXPAN	No se pudieron expandir los datos del canal
111	NS_ICA_ERR_REDUC_BYTES_V3_ERR	Error de expansión: los bytes consumieron más de los bytes disponibles
112	NS_ICA_ERR_REDUC_BYTES_O	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	Error de asignación de memoria para el contexto del expansor
117	NS_ICA_ERR_ICA_OLD_SERVER	Servidor antiguo, bloques de capacidad no admitidos
118	NS_ICA_ERR_PIR_MANY_FRAG	La solicitud Packet Init está fragmentada, no se puede procesar
119	NS_ICA_ERR_INIT_ICA_CAPS	Error de inicialización de la capacidad ICA
120	NS_ICA_ERR_NO_MSI_SUPPOR	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_CH	Bytes insuficientes en el canal
123	NS_ICA_ERR_CHANNEL_DATA	Datos incorrectos en el canal EUEM, CONTROL o SEAMLESS

Omitir código	Mensaje de error	Causa del error
124	NS_ICA_ERR_INVALID_PURE_C	Se recibió un comando no válido al procesar datos de canal ICA puros
125	NS_ICA_ERR_INVALID_PURE_LENG	Se encontró una longitud no válida al procesar datos de canal ICA puros
126	NS_ICA_ERR_INVALID_PURE_LI	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_REC	Error en la recuperación de la sesión reconectada
131	NS_ICA_ERR_DISABLE_SR_NON_RECONNECT	Error al inhabilitar SR
132	NS_ICA_ERR_REDUC_NOT_V3	Versión ICA Reducer no compatible
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	Compresión desactivada, no respetada por el host
134	NS_ICA_ERR_IDENT_PROTO	No se puede identificar el protocolo ICA o CGP, visto con receptores incorrectos
135	NS_ICA_ERR_INVALID_SIGNATURE	Firma ICA o cadena mágica incorrectas
136	NS_ICA_ERR_PARSE_RAW	Error al analizar el paquete de enlace ICA
137	NS_ICA_ERR_INCOMPLETE_PKT	Paquete incompleto recibido en el protocolo de enlace
138	NS_ICA_ERR_ICAFRAME_TOO_I	La trama ICA es demasiado grande, supera los 1.460 bytes
139	NS_ICA_ERR_FORWARD	Error al reenviar los datos ICA

Omitir código	Mensaje de error	Causa del error
140	NS_ICA_ERR_MAX_HOLES	No se puede procesar el comando CGP porque se divide más allá del límite admitido
141	NS_ICA_ERR_ASSEMBLE_FRAME	No se puede volver a montar el marco ICA correctamente
142	NS_ICA_ERR_UNSUPPORTED_F	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_RECONN	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_	Cadena de versión de espacio de trabajo no válida recibida del cliente
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	ID de producto no válido recibido del cliente
148	NS_ICA_ERR_V3_HDR_CORRUP	Longitud de canal no válida tras la expansión
149	NS_ICA_ERR_SPECIAL_THINWIRE	Error de descompresión
150	NS_ICA_ERR_SEAMLESS_INSUF	Se encontraron bytes insuficientes para un comando transparente
151	NS_ICA_ERR_EUEM_INSUFFBYTES	Se encontraron bytes insuficientes para el comando EUEM
152	NS_ICA_ERR_SEAMLESS_INVAL	Evento no válido para el análisis continuo de canales

Omitir código	Mensaje de error	Causa del error
153	NS_ICA_ERR_CTRL_INVALID_EVENT	Evento no válido para el análisis del canal CTRL
154	NS_ICA_ERR_EUEM_INVALID_E	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_E'	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_EV	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_INV/	Estado no válido para un comando crypt en el cifrado básico
161	NS_ICA_ERR_BASICCRYPT_INVALID_CRYPTCMD	Comando crypt no válido en el cifrado básico
162	NS_ICA_ERR_ADVCRYPT_INVAL	Estado no válido para un comando crypt en el cifrado RC5
163	NS_ICA_ERR_ADVCRYPT_INVALID_CRYPTCMD	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_RE	El VDA no admite la versión 3 de Reducer
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace no admite la versión 3 de Reducer
168	NS_ICA_ERR_ICAP_INSUFFBYTI	Número inesperado de bytes en el protocolo de enlace ICA

Omitir código	Mensaje de error	Causa del error
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_ABS	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_E	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_CLIEI	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_REC(	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 inhabilitar HDX Insight para conexiones que no son NSAP

Registros de ejemplo:

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223
 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session
GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314],
 Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12
-215], Ctx Flags [0x8820220228], 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 [0x8820220008], 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 del cliente.	Estadísticas
hdx_tot_cgp_conn	Indica el número total de conexiones CGP detectadas por NS (la confiabilidad de la sesión está activada). 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	Total de conexiones NSAP activas de EDT/CGP/ICA en ese instante.	Estadísticas

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/-diagnóstico)
hdx_dbg_skip_appflow_disabled	Número total de instancias en las que AppFlow se desconectó de una sesión debido a la desactivación de AppFlow	Estados/Diagnósticos
hdx_dbg_transparent_user	Número total de accesos de usuarios transparentes	Estados/Diagnósticos
hdx_dbg_ag_user	Número total de accesos de usuarios de Access Gateway	Estados/Diagnósticos
hdx_dbg_lan_user	Número total de accesos en modo de usuario de LAN	Estados/Diagnósticos
hdx_basic_enc	Indica el número de conexiones ICA que utilizan cifrado básico	Estados/Diagnósticos
hdx_advanced_enc	Indica el número de conexiones ICA que utilizan un cifrado avanzado basado en RC5	Estados/Diagnósticos
hdx_dbg_reconnected_session	Número total de solicitudes de reconexión del cliente sin ningún error de Citrix ADC	Estados/Diagnósticos
hdx_dbg_host_rejected_ns_rec	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 monitoreo de la experiencia del usuario final es necesario para recopilar estadísticas como ICA RTT.	Estados/Diagnósticos

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/-diagnóstico)
hdx_err_disabled_sr	La fiabilidad de la sesión se inhabilita mediante el `nsapimgr`mando.La sesión no funciona para esta sesión.	Error
hdx_err_skip_no_msi	Falta la capacidad de MSI en el servidor XA/XD. 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
hdx_sm_ica_cam_channel_disa	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_disa	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_disa	Número total de NS_ICA_CDM_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/-diagnóstico)
hdx_sm_ica_com1_channel_disabled	Número total de NS_ICA_COM1_CHANNEL inhabilitados mediante la directiva de SmartAccess	Diagnóstico
hdx_sm_ica_com2_channel_di	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_disa	Número total de NS_ICA_LPT1_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_lpt2_channel_disabled	Número total de NS_ICA_LPT2_CHANNEL inhabilitados mediante la directiva SmartAccess	Diagnóstico
dx_dbg_sm_ica_msi_disabled	Número total de casos en los que MSI está inhabilitado mediante la directiva SmartAccess	Diagnóstico
hdx_sm_ica_file_channel_disabled	El número total de NS_ICA_FILE_CHANNEL está inhabilitado mediante la directiva SmartAccess	Diagnóstico
hdx_dbg_usb_accept_device	Número total de dispositivos USB aceptados	Diagnóstico
hdx_dbg_usb_reject_device	Número total de dispositivos USB rechazados	Diagnóstico
hdx_dbg_usb_reset_endpoint	Número total de puntos finales USB restablecidos	Diagnóstico

Nombre del contador HDX	Propósito	Categoría (Estadísticas/error/-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 Citrix ADC.

Población de registros en la lista de comprobación de Citrix ADM

- Ejecute el comando `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`y compruebe los registros para confirmar que Citrix ADM está recibiendo registros de AppFlow.
- Confirme que la instancia de Citrix ADC se haya agregado a Citrix ADM.
- Validar que el servidor virtual de Citrix Gateway/VPN tiene licencia en Citrix ADM.
- Asegúrese de que la configuración de parámetros de salto múltiple esté habilitada para el doble salto.
- Asegúrese de que Citrix 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 Citrix ADC y Citrix ADM.

- 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 Citrix ADC.
- Paquete de soporte técnico capturado para Citrix ADM.
- Rastreos de paquetes capturados en todos los Citrix ADC.
  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 Citrix ADC para conocer los problemas conocidos en HDX Insight.

Información de métricas para umbrales

November 16, 2022

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 cliente	El tiempo necesario para las solicitudes de la red del cliente
Dispositivos	Resultados	Número total de visitas recibidas por un dispositivo. Por ejemplo: ordenador portátil, teléfono móvil
	Ancho de banda (MB)	Ancho de banda total consumido por un dispositivo
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

Métricas	Entidad	Descripción
	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
	Tiempo de procesamiento del servidor (ms)	El tiempo que tarda un servidor en responder a las solicitudes
URL	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

Métricas	Entidad	Descripción
	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 Citrix ADC para proteger las aplicaciones de amenazas y vulnerabilidades externas. Cuanto menores sean los riesgos de seguridad de una aplicación, mayor será el índice de seguridad. Los valores oscilan entre 1 y 7.

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

November 16, 2022

Un objetivo clave para los administradores de red es supervisar las instancias de Citrix ADC. Las instancias de ADC ofrecen información interesante sobre el uso y el rendimiento de las aplicaciones y escritorios a los que se accede mediante ellas. Los administradores deben supervisar la instancia de

ADC y analizar los flujos de aplicación procesados por cada instancia de ADC. 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 Citrix ADM

La función Infrastructure Analytics recopila todos los datos recopilados de las instancias de Citrix ADC y los cuantifica en una **puntuación de instancias** que define el estado de las instancias. La puntuación de la instancia se resume en una vista tabular o como visualización de paquetes circulares. La función Análisis de infraestructura le ayuda a visualizar los factores que provocaron o podrían provocar un problema en las instancias. Esta visualización también le ayuda a determinar las acciones que deben realizarse para evitar que el problema se repita.

Puntuación de instancia

La puntuación de la instancia indica el estado de una instancia de ADC. Una puntuación de 100 significa una instancia perfectamente sana sin problemas. La puntuación de la instancia captura diferentes niveles de posibles problemas en la instancia. Es una medida cuantificable de la salud de las instancias y múltiples «indicadores de salud» contribuyen a la puntuación.

Los**indicadores de salud son los** componentes básicos de la puntuación de la instancia, donde la puntuación se calcula periódicamente para un «período de monitoreo» 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 ocurrir en las instancias de Citrix ADC y que Citrix ADM puede supervisar.

  - Uso**elevado de la CPU**. El uso de la CPU ha superado el valor de umbral más alto en la instancia de Citrix ADC.
  - **Alto uso de memoria**. El uso de memoria ha superado el valor de umbral superior en la instancia de Citrix ADC.
  - **Uso elevado del disco**. El uso del disco ha superado el valor umbral superior en la instancia de Citrix ADC.
  - **Errores de disco**. Hay errores en el disco duro 0 o en el disco duro 1 del hipervisor en el que está instalada la instancia de ADC.
  - **Fallo de alimentación**. La fuente de alimentación ha fallado o se ha desconectado de la instancia de ADC.
  - **Fallo en la tarjeta SSL**. La tarjeta SSL instalada en la instancia ha fallado.
  - **Errores de flash**. Se observan errores de Compact Flash en la instancia de Citrix ADC.
  - La**NIC descarta**. Los paquetes descartados por la tarjeta NIC han cruzado el valor de umbral más alto en la instancia de Citrix ADC.

Para obtener más información sobre estos errores de recursos del sistema, consulta el panel de instancias.

- Indicadores de eventos críticos

  Los siguientes eventos críticos se identifican mediante la función de administración de eventos de Citrix ADM que están configurados con una gravedad crítica.

  - **Fallo de sincronización de HA**. La sincronización de la configuración entre las instancias de ADC en alta disponibilidad falló en el servidor secundario.
  - **No tiene latidos**. El servidor principal de un par de instancias de ADC con alta disponibilidad no recibe los latidos del servidor secundario.

- **Tiene un mal estado secundario**. El servidor secundario de un par de instancias de ADC con alta disponibilidad se encuentra en estado secundario Inactivo, Desconocido o Permanecer.
- **La versión HA no coincide**. La versión de las imágenes del software ADC instaladas en un par de instancias de ADC en alta disponibilidad no coincide.
- **Fallo de sincronización del clúster**. La sincronización de la configuración entre las instancias de ADC en el modo de clúster ha fallado.
- **La versión del clúster no coincide**. La versión de las imágenes del software ADC instaladas en las instancias de ADC en modo de clúster no coincide.
- **Fallo de propagación del clúster**. Se produjo un error al propagar las configuraciones a todas las instancias de un clúster.

> **Nota**
>
> Puede tener la lista de eventos SNMP críticos cambiando los niveles de gravedad de los eventos. Para obtener más información sobre cómo cambiar los niveles de gravedad, consulte Modificar la gravedad informada de los eventos que se producen en las instancias de Citrix ADC.

Para obtener más información sobre los eventos en Citrix ADM, consulte Eventos.

- Indicadores de configuración SSL
  - **No se recomienda la fuerza clave**. La fortaleza clave de los certificados SSL no se ajusta a los estándares de Citrix
  - **Emisor no recomendado**. Citrix no recomienda el emisor del certificado SSL.
  - **Los certificados SSL han caducado**. El certificado SSL instalado en la instancia ADC ha caducado.
  - **Los certificados SSL están vencidos**. El certificado SSL instalado en la instancia ADC está a punto de caducar en la próxima semana.
  - **Algoritmos no recomendados**. Los algoritmos de firma de certificados SSL instalados en la instancia ADC no se ajustan a los estándares de Citrix.

Para obtener más información sobre los certificados SSL, consulte Panel de control SSL.

- Indicadores de desviación de configuración
  - **Plantilla Config Drift**. Hay una desviación (cambios sin guardar) en la configuración con respecto a las plantillas de auditoría que ha creado con configuraciones específicas que quiere auditar en determinadas instancias.
  - **Desviación de configuración predeterminada**. Hay una desviación (cambios no guardados) en la configuración de los archivos de configuración predeterminados.

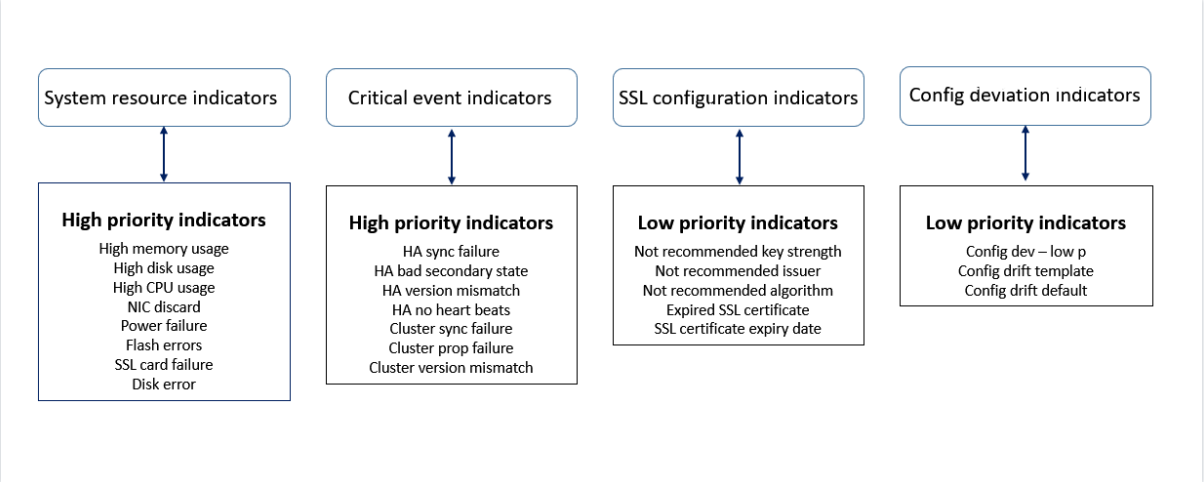
Para obtener más información sobre las desviaciones de la configuración y cómo ejecutar informes de auditoría para comprobar la desviación de la configuración, consulte Ver informes de auditoría..

Ver problemas de capacidad ADC

Cuando una instancia de ADC ha consumido la mayor parte de su capacidad disponible, es posible que se descarten paquetes al procesar el tráfico del cliente. Al comprender estos problemas de capacidad del ADC, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento del ADC. Para obtener más información, consulte Ver los problemas de capacidad en una instancia de ADC.

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.

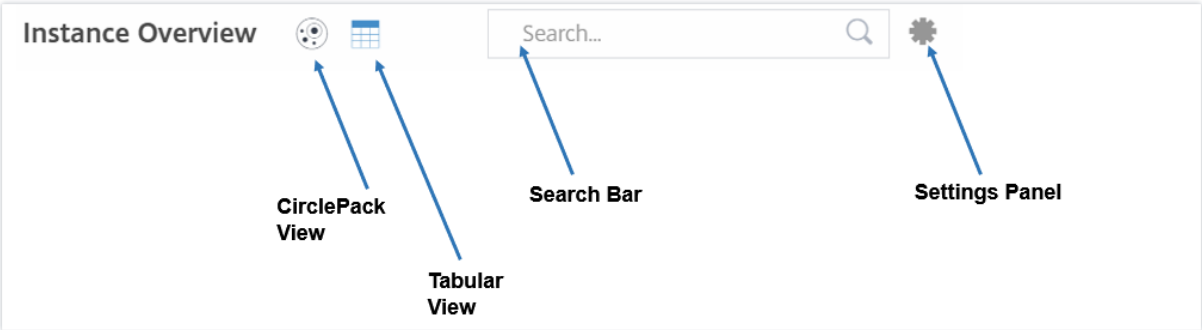
2. **Basado en la violación del valor umbral**. Por ejemplo, se activa un indicador de recursos del sistema cuando la tarjeta NIC descarta paquetes y se infringe el nivel de umbral.
3. **Basado en la brecha de valor de umbral bajo y alto**. En este caso, un indicador se puede activar de dos maneras:
    - 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.

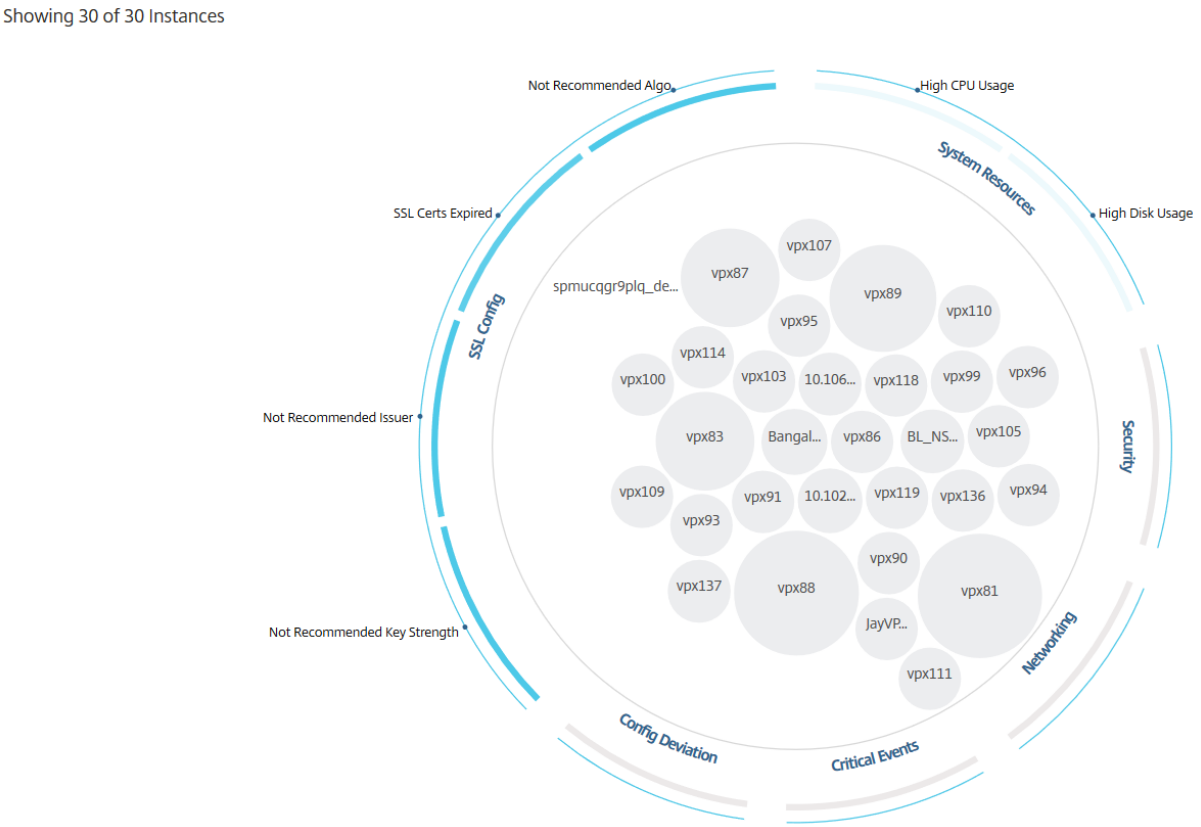


- En la vista Tabular, puede buscar una instancia escribiendo el nombre de host o la dirección IP en la barra de búsqueda.
- De forma predeterminada, la página Infrastructure Analytics muestra el panel de resumen en la parte derecha de la página.
- Haga clic en el icono de **configuración** para mostrar 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

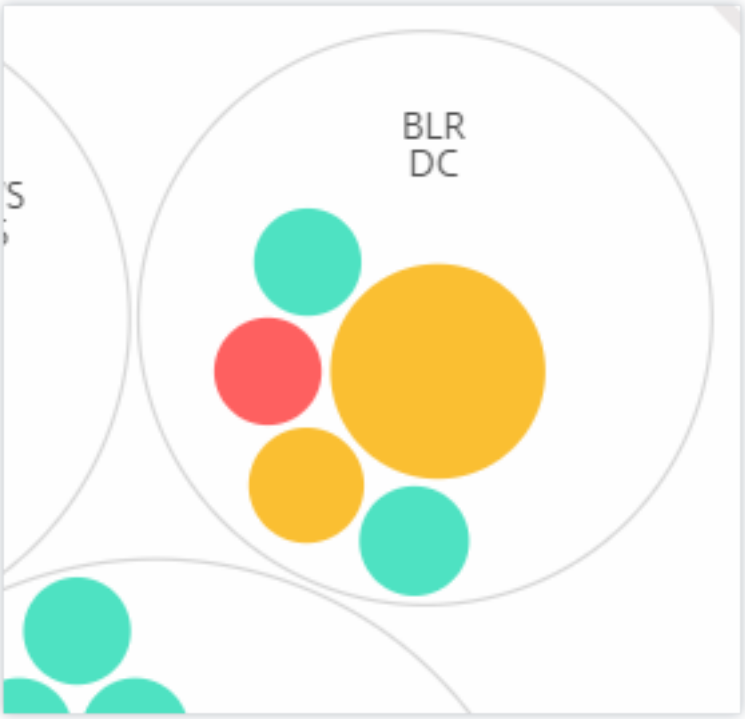
similar al de otros grupos de la misma categoría o están anidados dentro de grupos más grandes. Los paquetes de círculo representan conjuntos de datos jerárquicos y muestran diferentes niveles en la jerarquía y cómo interactúan entre sí.



Círculos de instancia

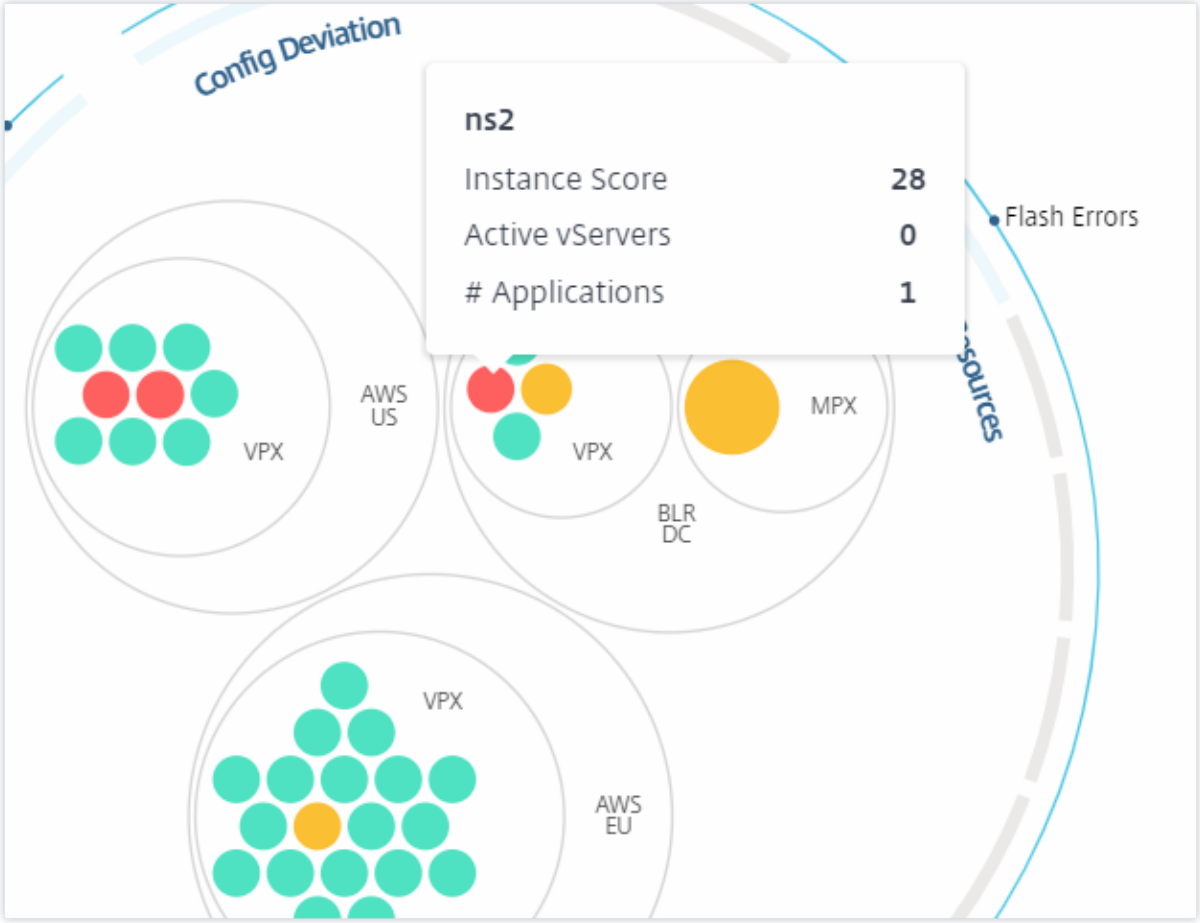
Color. Cada instancia se representa en Circle Pack como un círculo coloreado. El color del círculo indica el estado de la instancia.

- **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.

Puedes pasar el puntero del ratón sobre cada uno de los círculos de la instancia (círculos de colores) para ver un resumen. La sugerencia de la herramienta al pasar el ratón muestra el nombre de host de la instancia, el número de servidores virtuales activos y el número de aplicaciones configuradas en esa instancia.

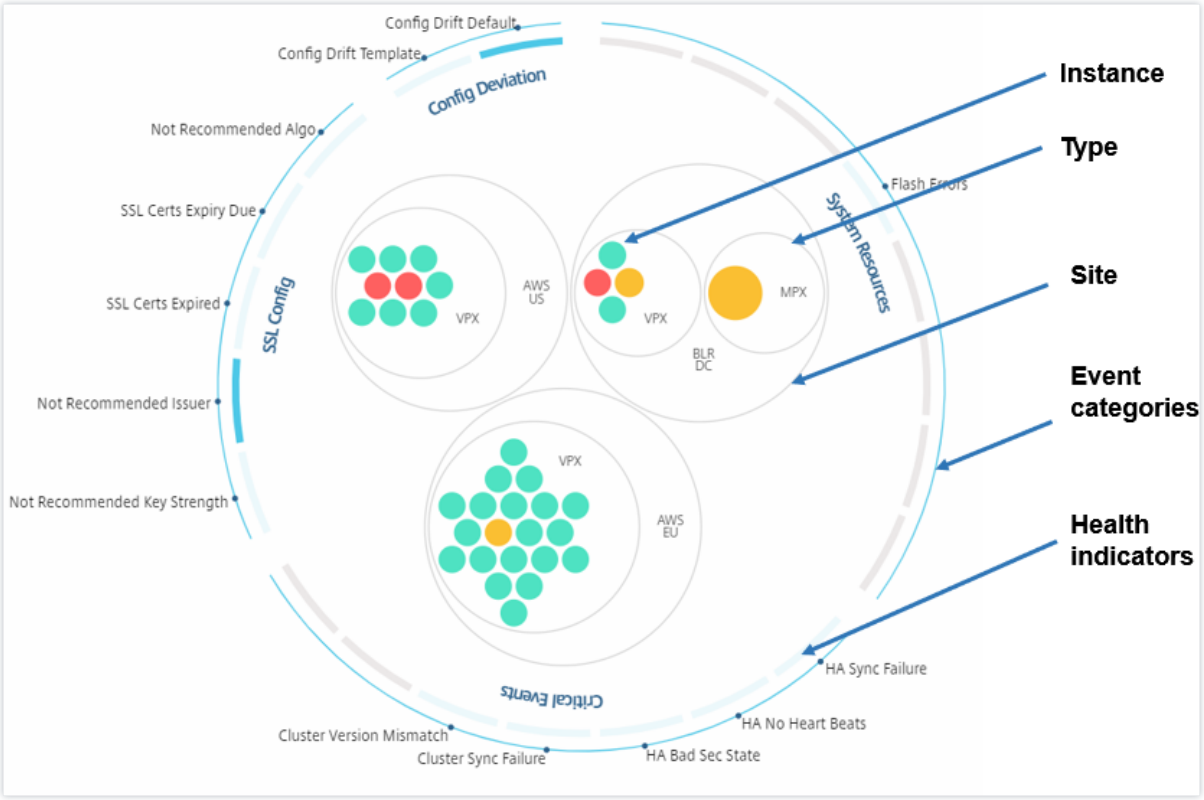


Círculos de instancia agrupados

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 están desplegados
- el tipo de instancias implementadas: VPX, MPX, SDX y CPX
- el modelo virtual o físico de la instancia de ADC
- la versión de la imagen ADC instalada en las instancias

La siguiente imagen muestra un paquete de círculo donde las instancias se agrupan primero por el sitio o centro de datos donde se implementan y, a continuación, se agrupan en función de su tipo, VPX y MPX.

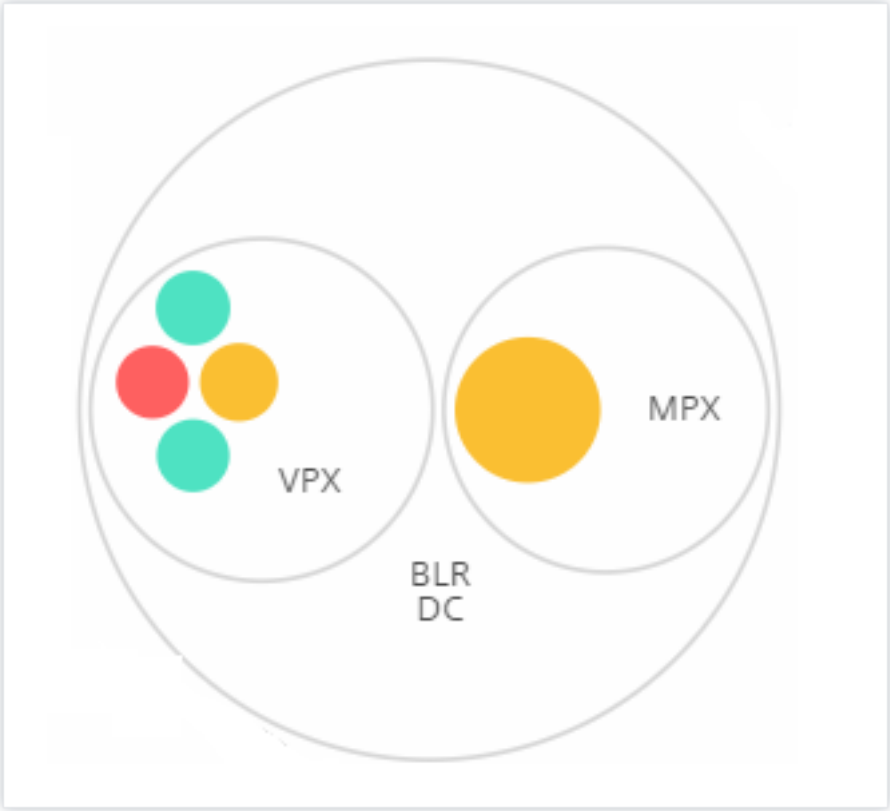


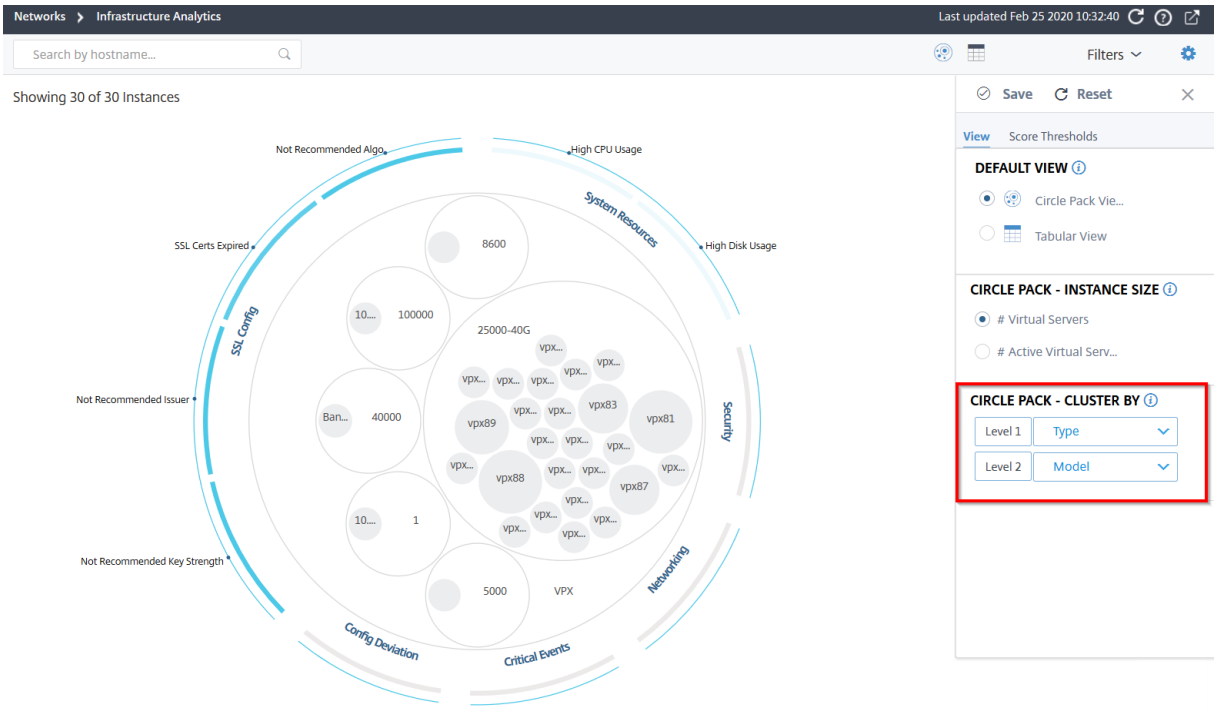
Todos estos círculos anidados están delimitados por dos círculos exteriores. Los dos círculos exteriores representan las cuatro categorías de eventos supervisados por el Citrix ADM (recursos del sistema, eventos críticos, configuración de SSL y desviación de configuración) y los indicadores de estado que contribuyen.

Círculos de instancia agrupados

Citrix ADM supervisa muchas instancias. Para facilitar la supervisión y el mantenimiento de estas instancias, Infrastructure Analytics permite agruparlas en dos niveles. Es decir, las agrupaciones de instancias se pueden anidar dentro de otra agrupación.

Por ejemplo, el centro de datos de BLR tiene dos tipos de instancias de ADC: VPX y MPX, implementadas en él. Primero puede agrupar las instancias de ADC por su tipo y, a continuación, agrupar todas las instancias por el sitio en el que están agrupadas. Ahora puede identificar fácilmente cuántos tipos de instancias se implementan en los sitios que está administrando.

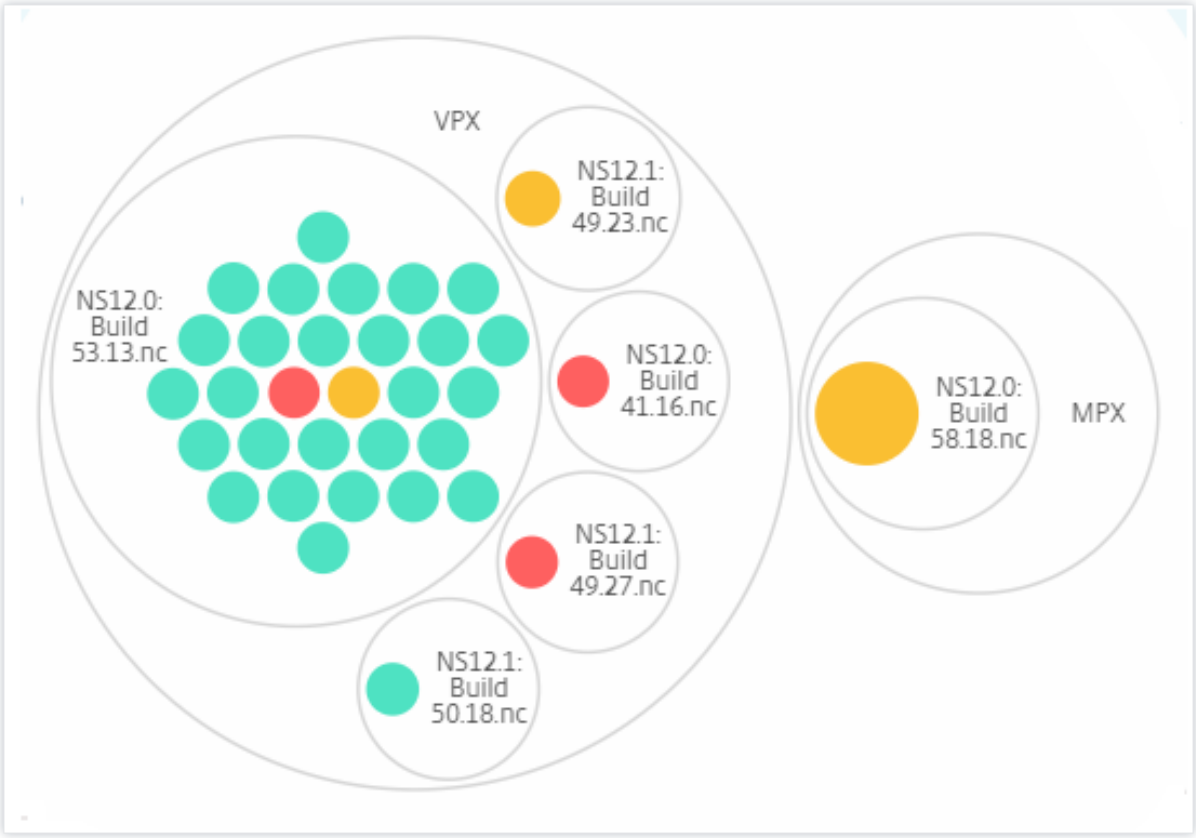




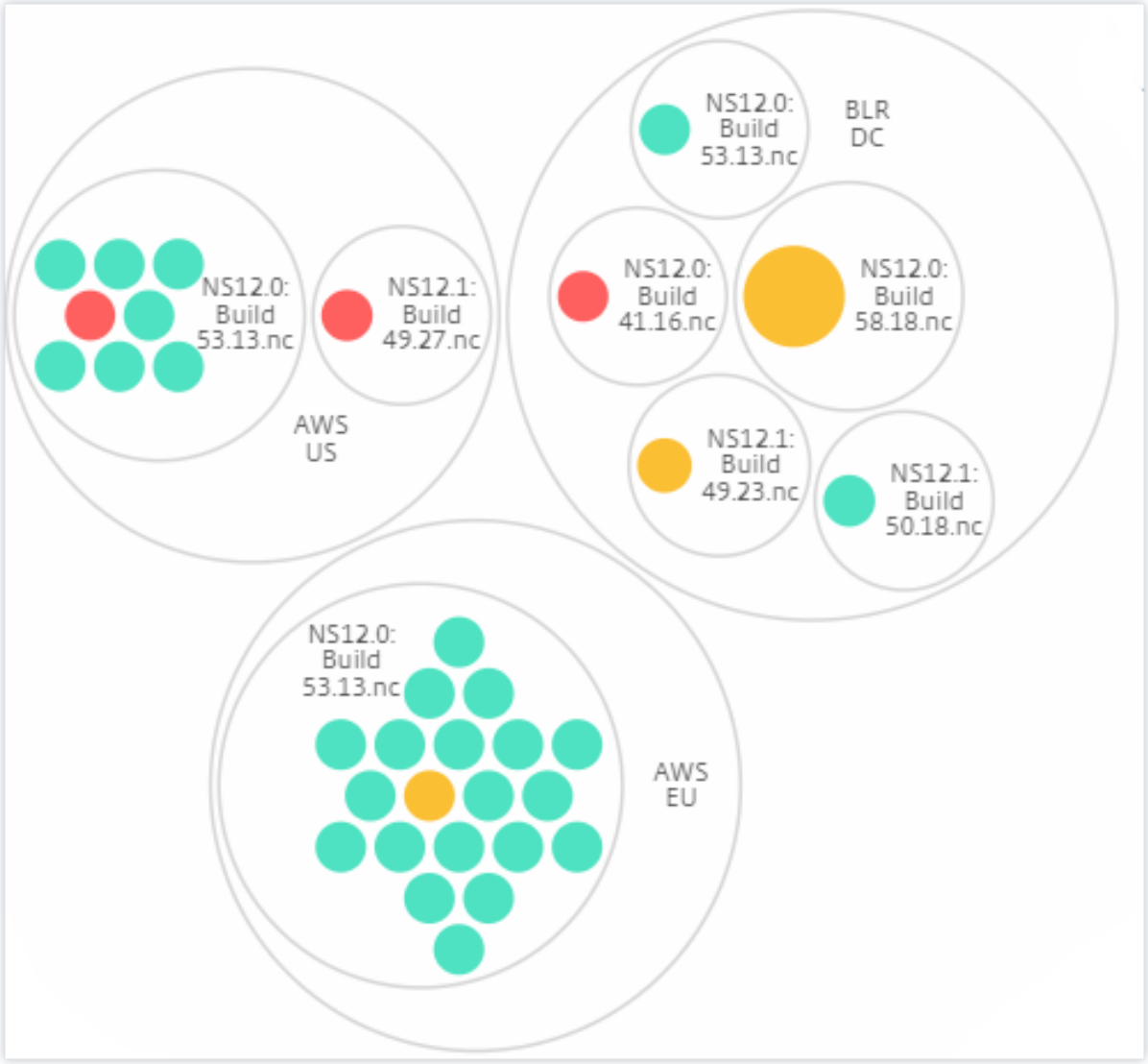
Algunos ejemplos más de clustering de dos niveles son los siguientes:

Sitio y modelo:

Tipo y versión:

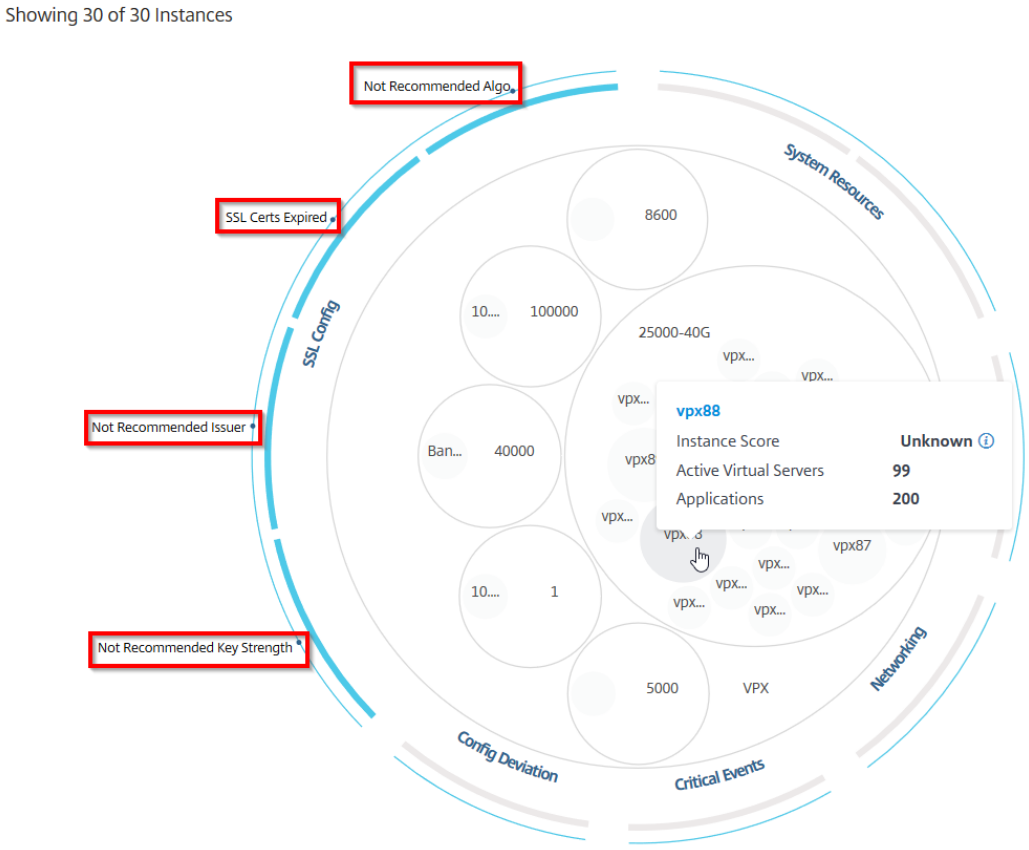


Sitio y versión:

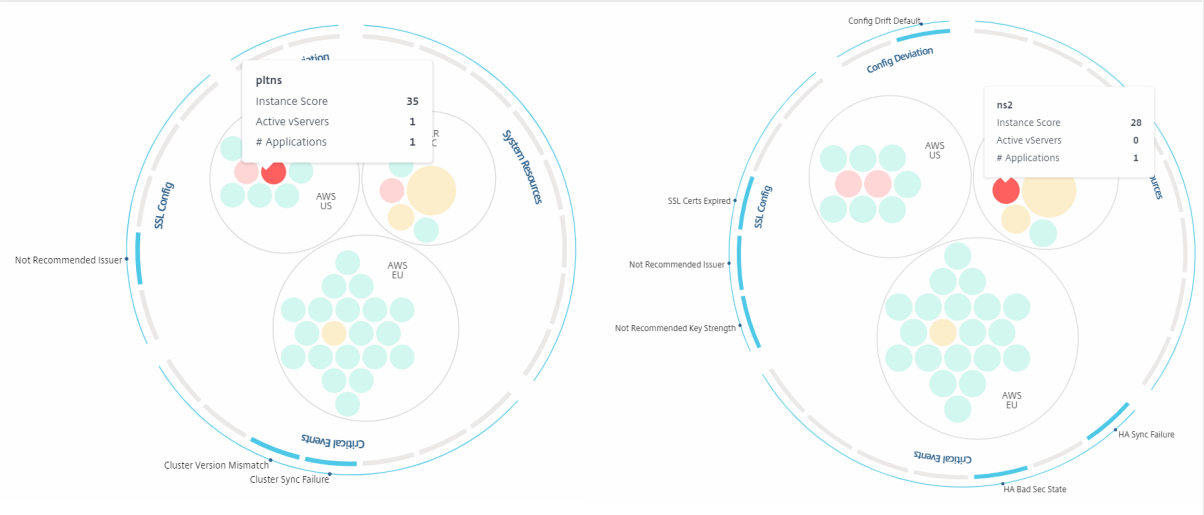


Cómo usar Circle Pack

Haga clic en cada uno de los círculos coloreados para resaltar esa instancia.

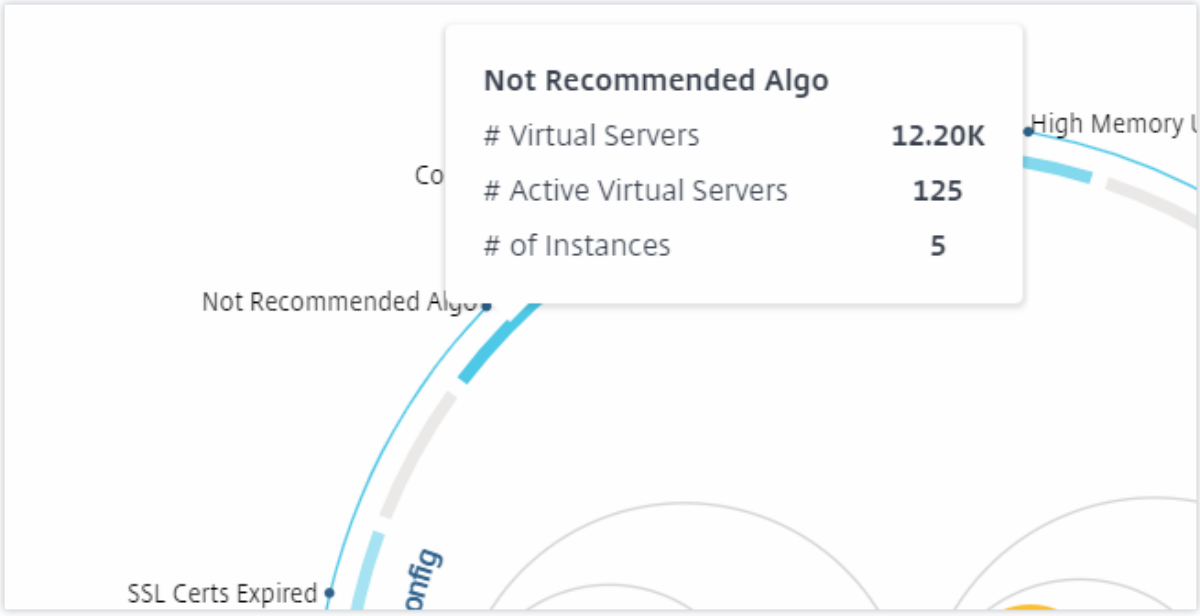


Dependiendo de los eventos que se hayan producido en ese caso, solo los indicadores de salud aparecen resaltados en los círculos exteriores. Por ejemplo, las dos imágenes siguientes de Circle Pack muestran diferentes conjuntos de indicadores de riesgo, aunque ambas instancias se encuentran en un estado crítico.



También puede hacer clic en los indicadores de estado para obtener más detalles sobre el número de instancias que han informado de ese indicador de riesgo. Por ejemplo, haga clicNot recommended

`Algo` para ver el informe resumido de ese indicador de riesgo.



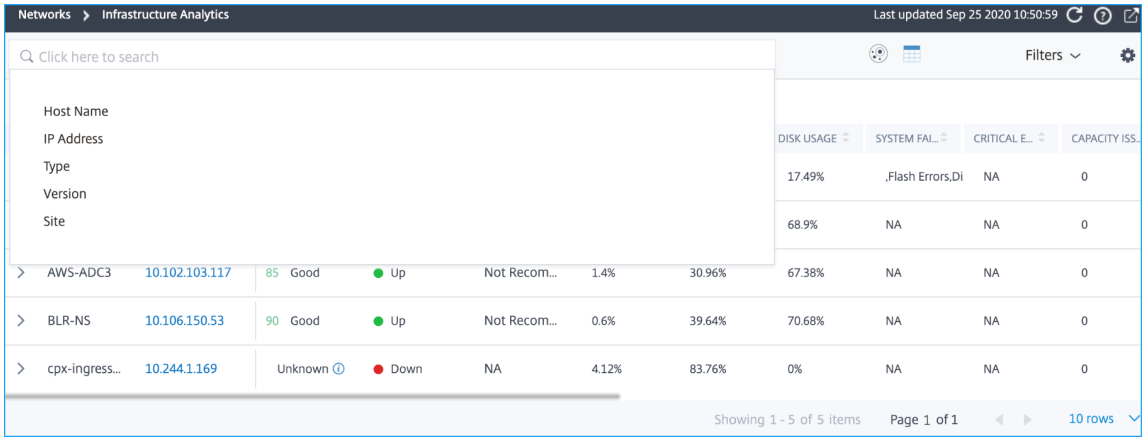
Vista tabular

La vista tabular muestra las instancias y los detalles de esas instancias en un formato tabular. 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 monitorear 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 Citrix ADC*.

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 ratón 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:

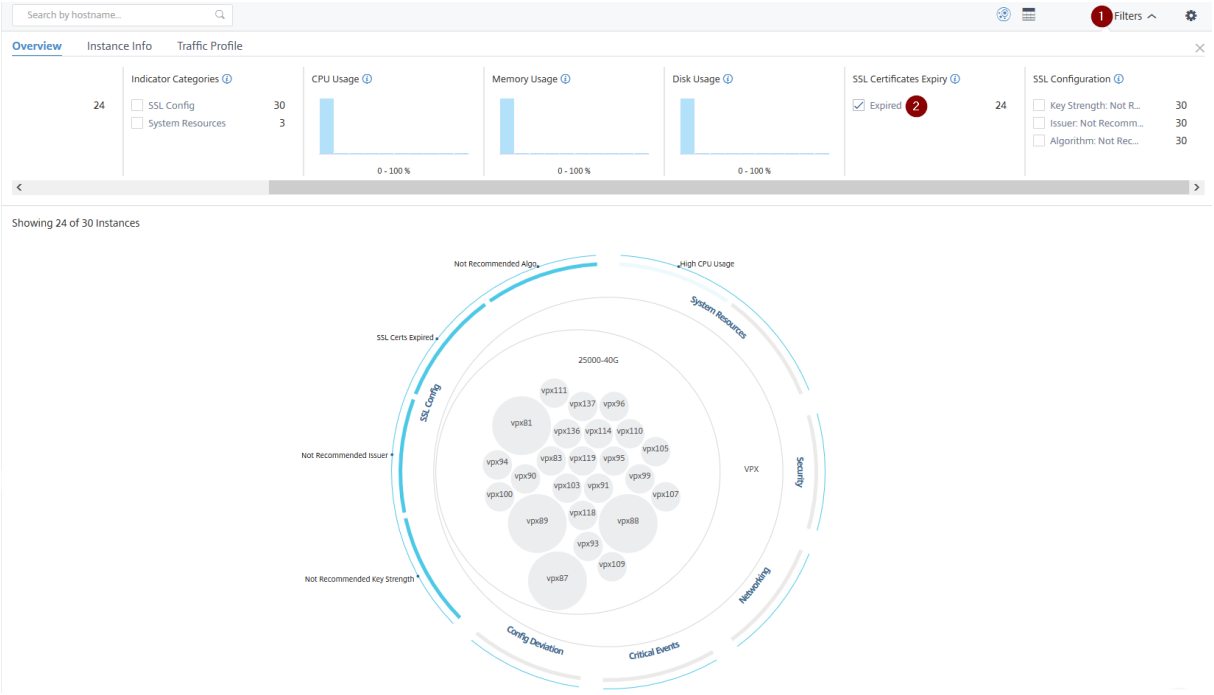
Para ver las instancias que han consumido memoria entre el 0% y el 10% de espacio en disco, arrastre el puntero del ratón sobre los dos rangos, tal y como se muestra en la siguiente imagen.

> **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**.

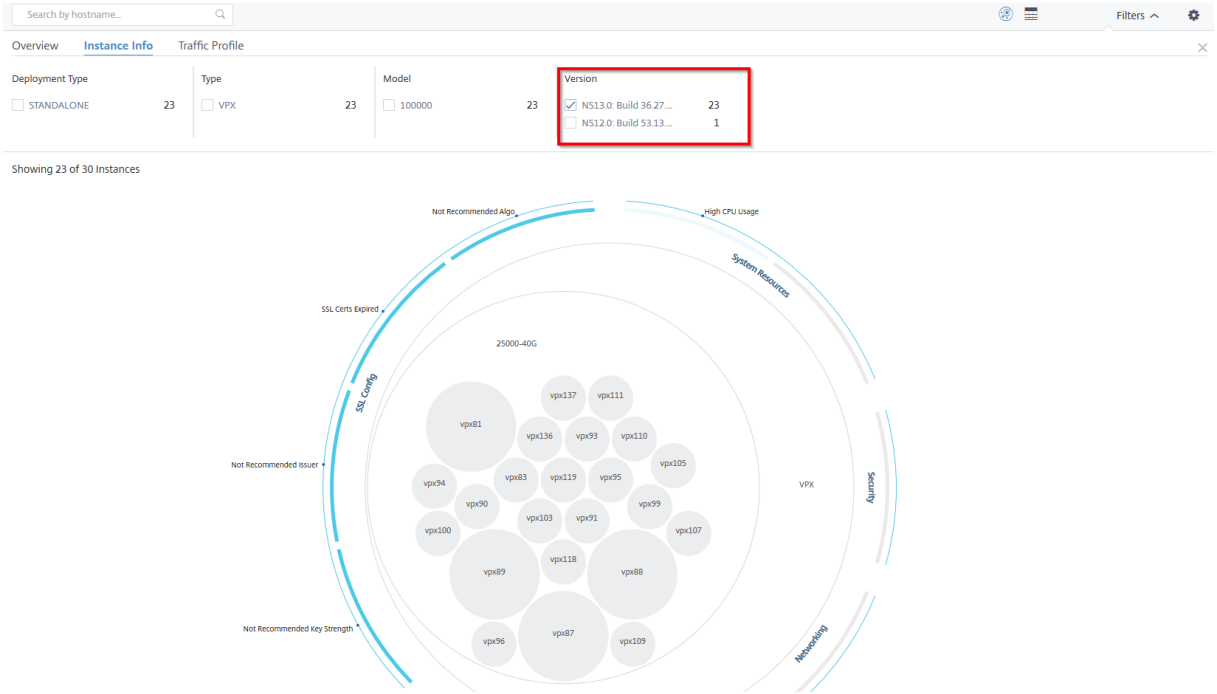
2 - En la sección **Caducidad de los certificados SSL**, seleccione la casilla de verificación **Vencidos** para ver las instancias.

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 las instancias VPX de ADC con un número de compilación específico:

Seleccione la versión que quiere ver.

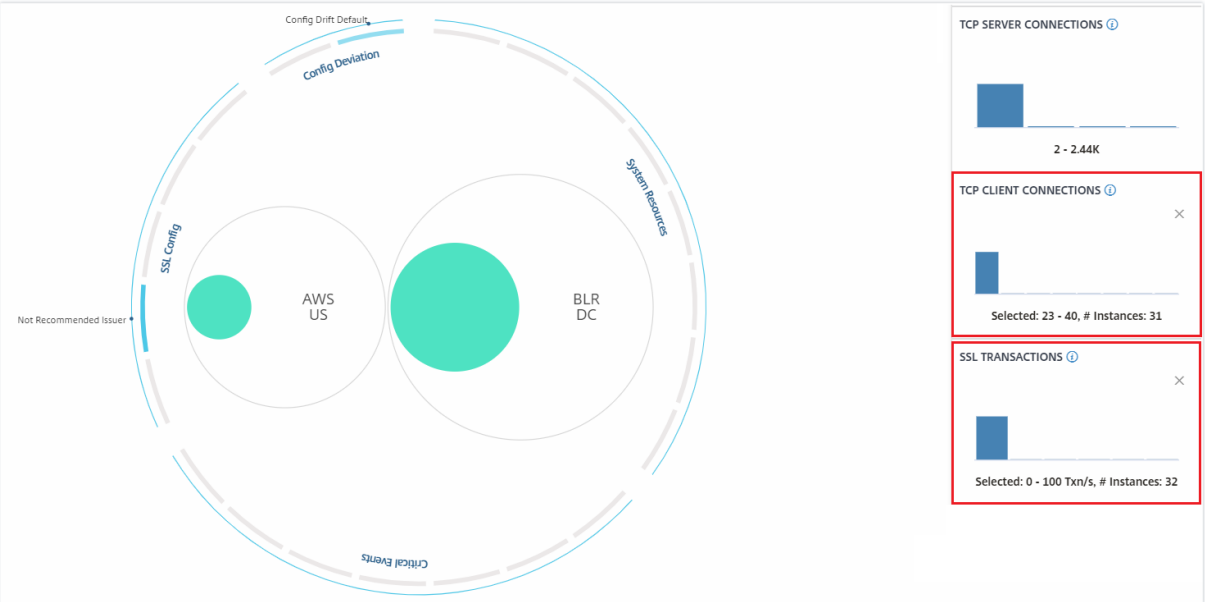


Perfil de tráfico

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.



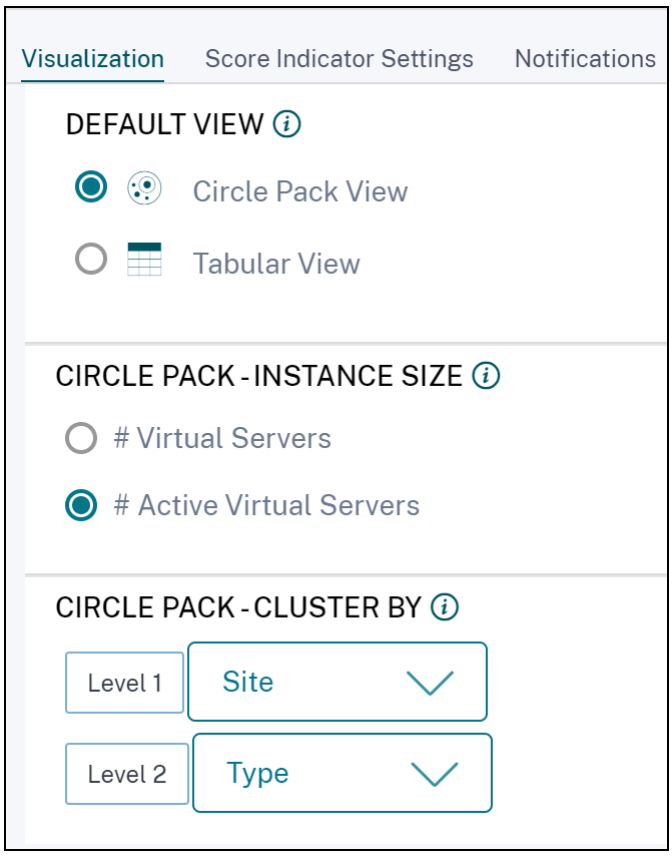
Cómo usar el panel de configuración

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 selecciona es el que aparece cada vez que accede a la página en Citrix ADM.
- **Paquete circular: tamaño de instancia**. Permita que el tamaño del círculo de instancias sea igual al número de servidores virtuales o al número de servidores virtuales activos.
- **Paquete Circle, Cluster By**. Decida el agrupamiento de dos niveles de los círculos de instancia. Para obtener más información sobre la agrupación en clústeres de instancias, consulta Círculos de instancias agrupados



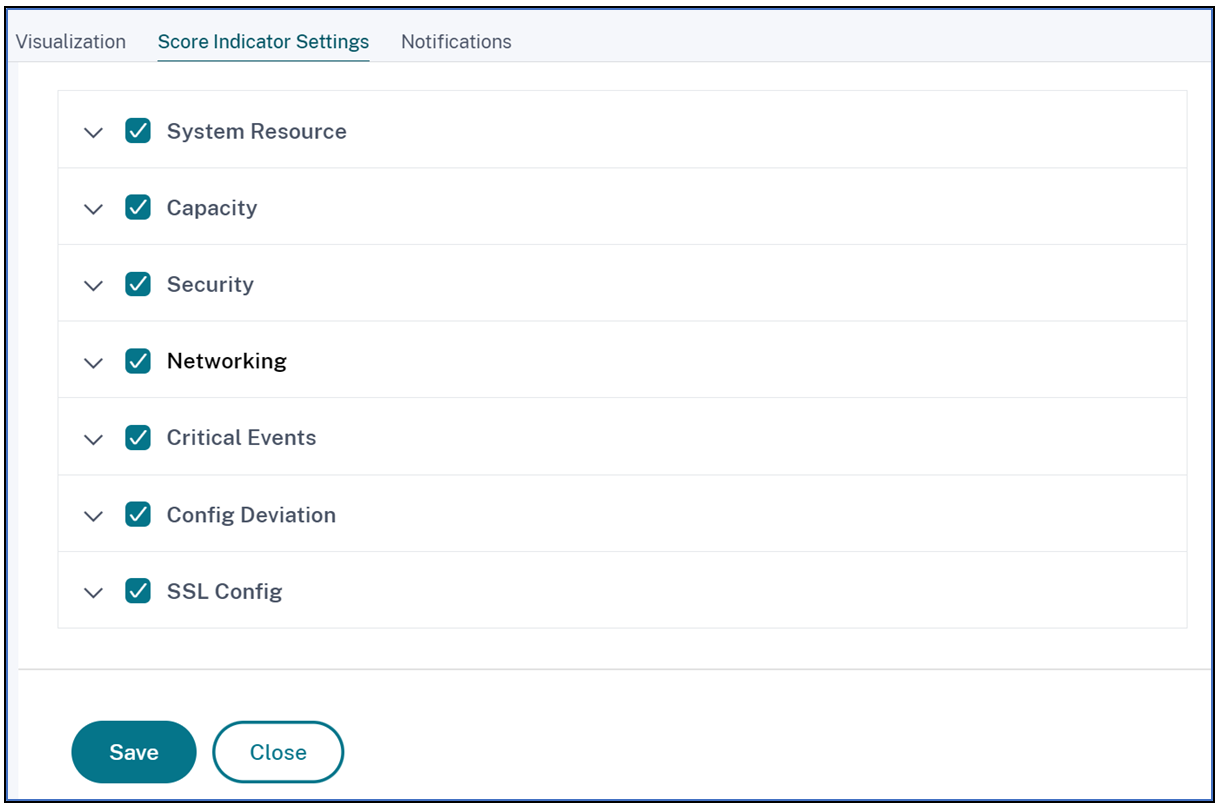
Seleccione las métricas y personalice la ponderación, por ejemplo, el cálculo

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.

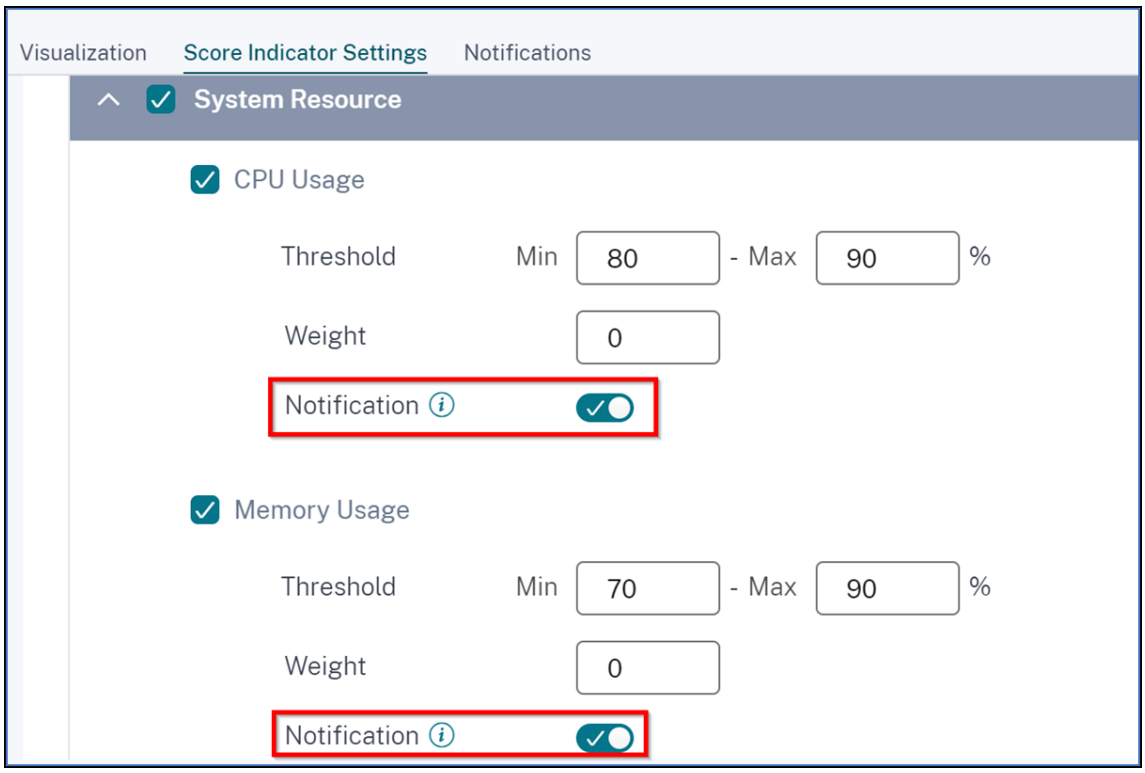


Configurar notificaciones

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 Citrix ADC 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:

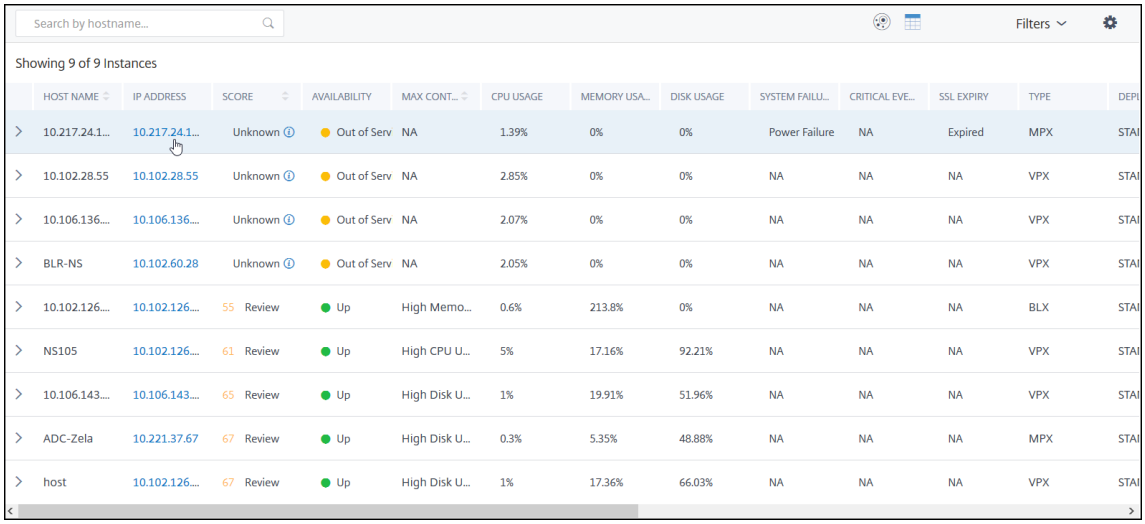
Chris también observa que otra instancia está en estado «Revisar» y que recientemente se ha producido una desviación de configuración. Al hacer clic en el indicador de riesgo de desviación de la configuración, observa que se han realizado cambios de configuración relacionados con RC4 Cipher, SSL v3, 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

November 16, 2022

1. Vaya a **Infraestructura > Análisis de infraestructura**.
2. Haga clic en la vista de paquete de círculo y seleccione la dirección IP.

También puede hacer clic en una dirección IP en la vista de tabla.

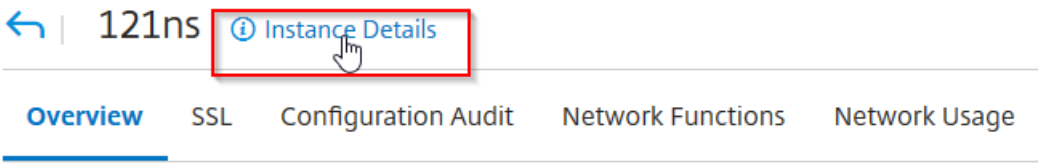


- **Nombre de host** : indica el nombre de host asignado a la instancia de ADC
- **Dirección IP** : indica la dirección IP de la instancia de ADC
- **Puntuación**: Denota la puntuación de instancia ADC y el estado como Crítico, Bueno y Justo
- **Disponibilidad: indica el estado actual de la instancia de ADC, como Activa **, Inactiva**o **Fuera de servicio**.**
- **Contribución máxima**: Indica la categoría de problema en la que la instancia de ADC tiene el número máximo de errores.
- **Uso de la CPU** : indica el% de CPU actual que utiliza la instancia
- **Uso de memoria** : indica el% de memoria actual que utiliza la instancia
- **Uso del disco** : indica el% de disco actual utilizado por la instancia
- **Fallo del sistema** : indica el número total de errores del sistema de instancias
- **Eventos críticos**: Indica la categoría de eventos en la que la instancia Citrix ADC tiene el máximo de eventos
- **Caducidad de SSL** : indica el estado actual del certificado SSL instalado en la instancia de ADC
- **Tipo**: Indica el tipo de instancia ADC como VPX, SDX, MPX o CPX
- **Implementación** : indica si la instancia de ADC se implementa como una instancia independiente o un par de HA
- **Modelo** : indica el número de modelo de la instancia de ADC
- **Versión** : indica la versión y el número de compilación de la instancia ADC
- **Rendimiento** : indica el rendimiento de la red actual desde la instancia de ADC.
- **Solicitud de HTTPS por segundo** : indica las solicitudes HTTPS actuales por segundo recibidas por la instancia de ADC

- **Conexión TCP** : indica las conexiones TCP actuales establecidas
- **Transacción SSL** : indica las transacciones SSL actuales procesadas por la instancia de ADC
- **Sitio** : indica el nombre del sitio en el que está implementada la instancia de ADC.

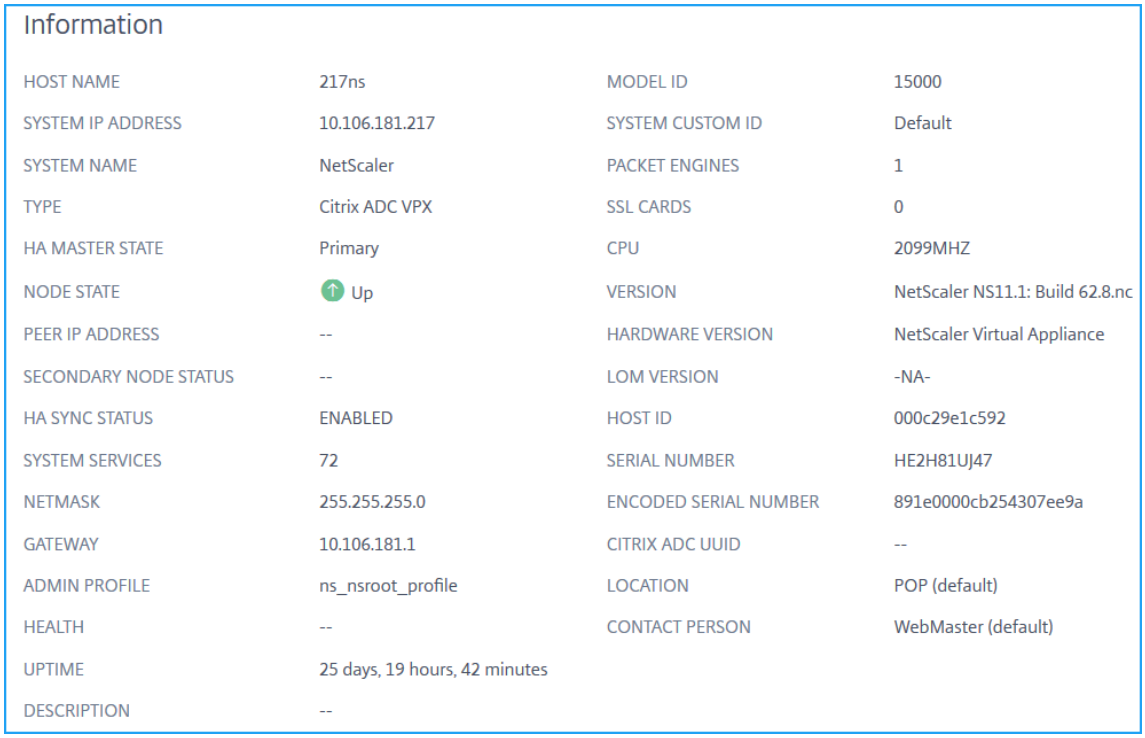
> **Nota**
>
> Cada 5 minutos, se actualizan los valores actuales de uso de la CPU, de memoria, de disco, de rendimiento, etc.

Haga clic en **Detalles de ejemplar** para ver los detalles.

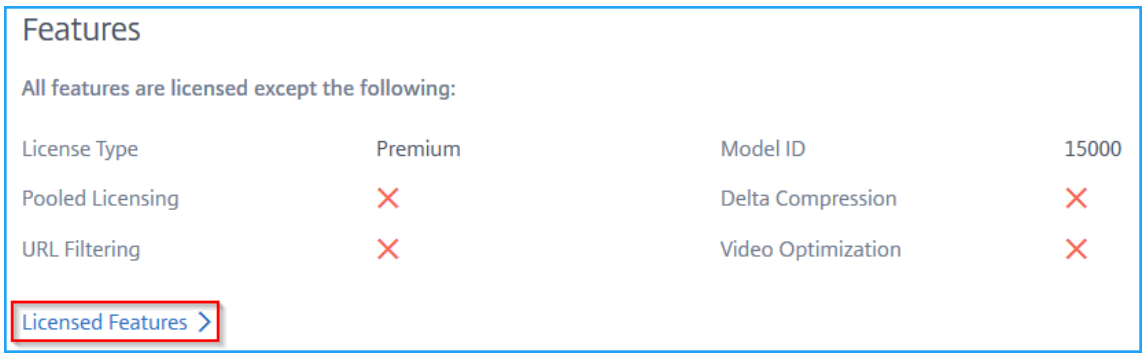


Se muestran los siguientes detalles:

- **Información** : detalles de la instancia, como el tipo de instancia, el tipo de implementación, la versión, el modelo, etc.



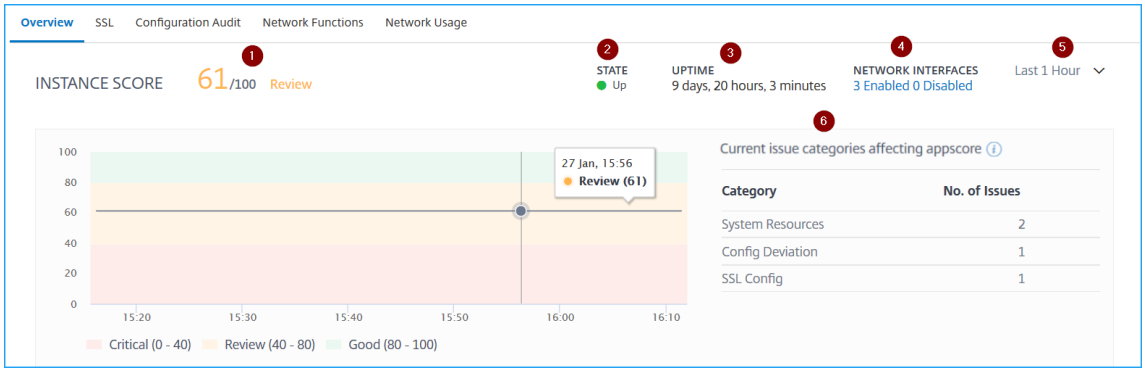
- **Funciones** : de forma predeterminada, se muestran las funciones que no tienen licencia. Haga clic en **Funciones con licencia** para ver las funciones que tienen licencia.



- **Modos** : de forma predeterminada, se muestran todos los modos que están deshabilitados 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**



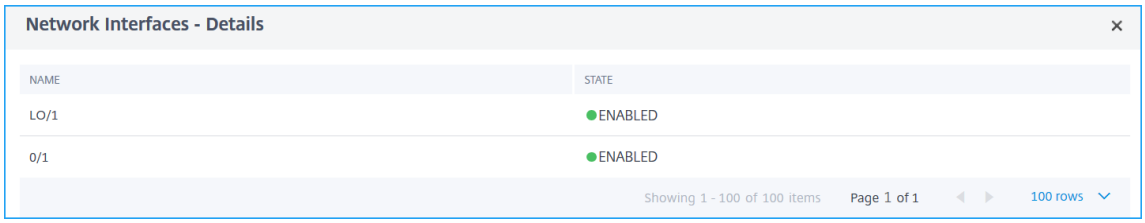
1 : indica la puntuación actual de la instancia de Citrix ADC durante el tiempo seleccionado. La puntuación final se calcula en **100 menos el total de penaltis**. El gráfico muestra los rangos de

puntuación para la duración de tiempo seleccionada.

2: Indica el estado actual de la instancia de Citrix ADC, como **Activo**, **Inactivo** y **Fuera de servicio**.

3 : indica el tiempo que la instancia de Citrix ADC está activa y en ejecución.

4 : indica el total de interfaces de red habilitadas y deshabilitadas para la instancia. Haga clic para ver los detalles, como el nombre de la interfaz de red y el estado (habilitada o deshabilitada).



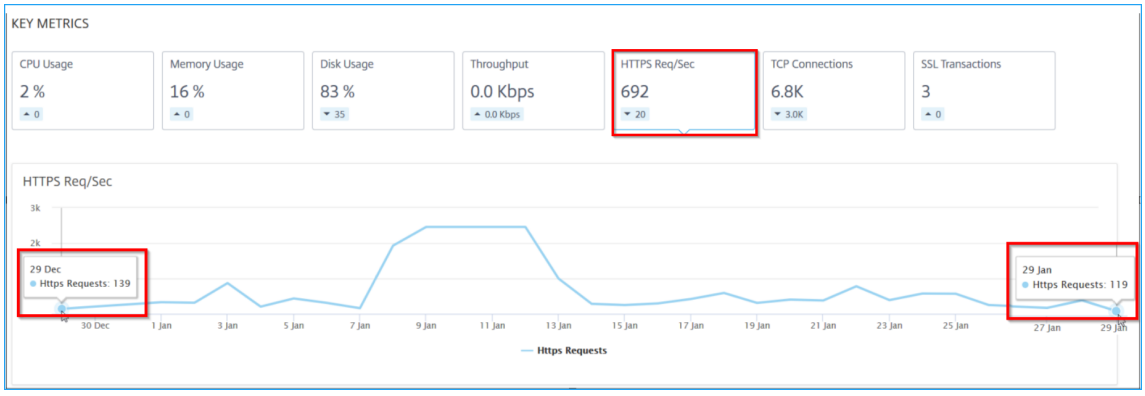
5 — Seleccione la duración del tiempo de la lista para ver los detalles de la instancia.

6 : muestra el total de problemas y la categoría de problemas de la instancia de ADC.

- **Métricas clave**

  Haga clic en cada ficha para ver los detalles. En cada métrica, puede ver el valor medio y el valor de diferencia para el tiempo seleccionado.

  La siguiente imagen es un ejemplo de HTTPS Req/Sec y la duración seleccionada es de 1 hora. El valor **692** es la media de las Req/Sec de HTTPS para el mes de duración y el valor **20** es el valor de la diferencia. En el gráfico, el primer valor es **139** y el último valor es **119**. El valor de la diferencia es **139 — 119 = 20**.



  Puede ver las siguientes métricas de instancia en un formato de gráfico para la duración de tiempo seleccionada:

  - **Uso de CPU** : el% de CPU promedio de la instancia durante el tiempo seleccionado (se muestra tanto para la CPU de paquetes como para la CPU de administración).

- **Uso de memoria** : el% promedio de uso de memoria de la instancia durante el tiempo seleccionado.
- **Uso del disco** : el% medio de espacio en disco de la instancia durante el tiempo seleccionado.
- **Rendimiento** : el rendimiento de red promedio procesado por la instancia durante el tiempo seleccionado.
- **Solicitud de HTTPS por segundo** : el promedio de solicitudes HTTPs recibidas por la instancia durante el tiempo seleccionado.
- **Conexiones TCP** : el promedio de conexiones TCP establecidas por el cliente y el servidor durante el tiempo seleccionado.
- **Transacciones SSL** : el promedio de transacciones SSL procesadas por la instancia durante el tiempo seleccionado.

- **Problemas**

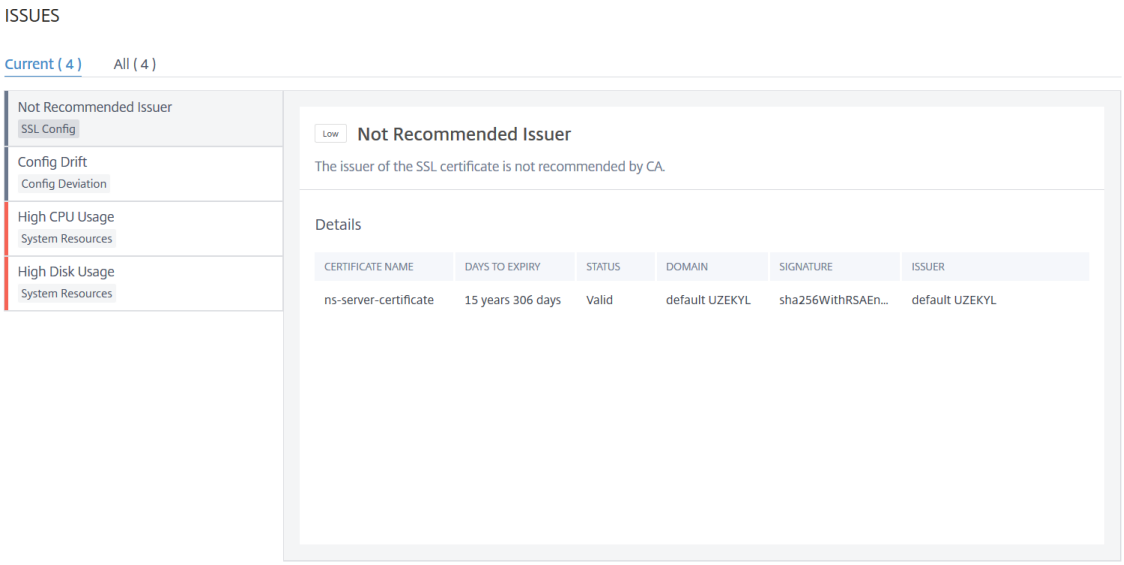
  Puede ver los siguientes problemas que se producen en la instancia de Citrix ADC:

Categoría de problema	Descripción	Problemas
Recursos del sistema	Muestra todos los problemas relacionados con el recurso del sistema Citrix ADC, 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 Citrix ADC.	- Los certificados SSL han caducado
		- Emisor no recomendado
		- Algo no recomendado

Categoría de problema	Descripción	Problemas
		- 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 Citrix ADC.	- Deriva de configuración
		- Ejecución vs plantilla
Eventos críticos	Muestra todos los eventos críticos relacionados con las instancias de Citrix ADC 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
		- HA No Heat Beats
		- Fallo de sincronización de HA
		- No coincide la versión de HA
Cuestiones de capacidad	Muestra problemas de capacidad de ADC. El Citrix ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra los paquetes descartados o los incrementos del contador de límites de velocidad, si existen. Los problemas se clasifican en los siguientes parámetros de capacidad.	- Se alcanzó el límite de rendimiento
		- Se ha alcanzado el límite de CPU PE
		- Límite PPS alcanzado

Categoría de problema	Descripción	Problemas
		- Límite de velocidad de rendimiento SSL
		- Límite de velocidad SSL TPS
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 ADC

November 16, 2022

Cuando una instancia ADC ha consumido la mayor parte de su capacidad disponible, puede producirse la caída de paquetes al procesar el tráfico del cliente. Este problema provoca un bajo

rendimiento en una instancia de ADC. Al comprender estos problemas de capacidad del ADC, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento del ADC.

En la **vista Circle Pack**, puede ver los problemas de capacidad de la instancia de ADC si existe.

Para ver las cuestiones relativas a la capacidad de los CCA,

1. Vaya a **Infraestructura > Análisis de infraestructura**.
2. Seleccione la vista de paquete de círculos.

> **Nota**
>
> En **Infrastructure Analytics**, el paquete circular y las vistas tabulares muestran los eventos y problemas que ocurrieron en la última hora.

La siguiente ilustración sugiere los problemas de capacidad existentes en la instancia seleccionada:

Los problemas se clasifican según los siguientes parámetros de capacidad:

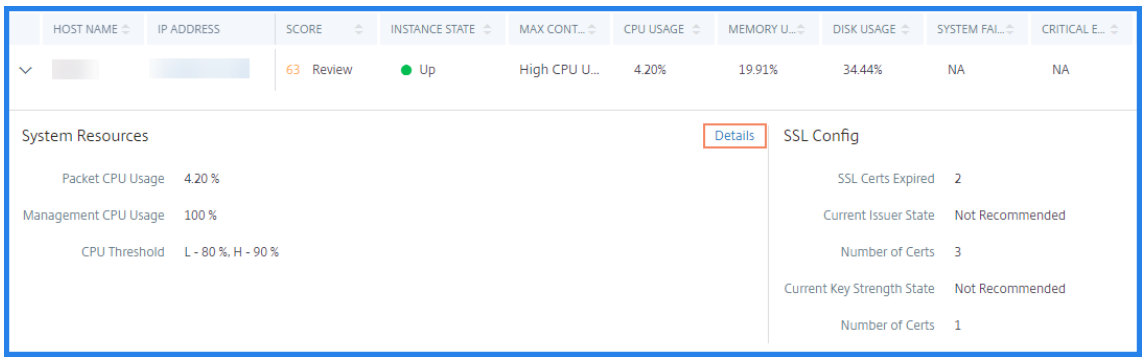
- **Límite de rendimiento alcanzado** : el número de paquetes descartados en la instancia una vez alcanzado el límite de rendimiento.
- **Se alcanzó el límite de CPU PE** : la cantidad de paquetes descartados en todas las NIC una vez alcanzado el límite de CPU PE.
- **Se alcanzó el límite de PPS** : 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.

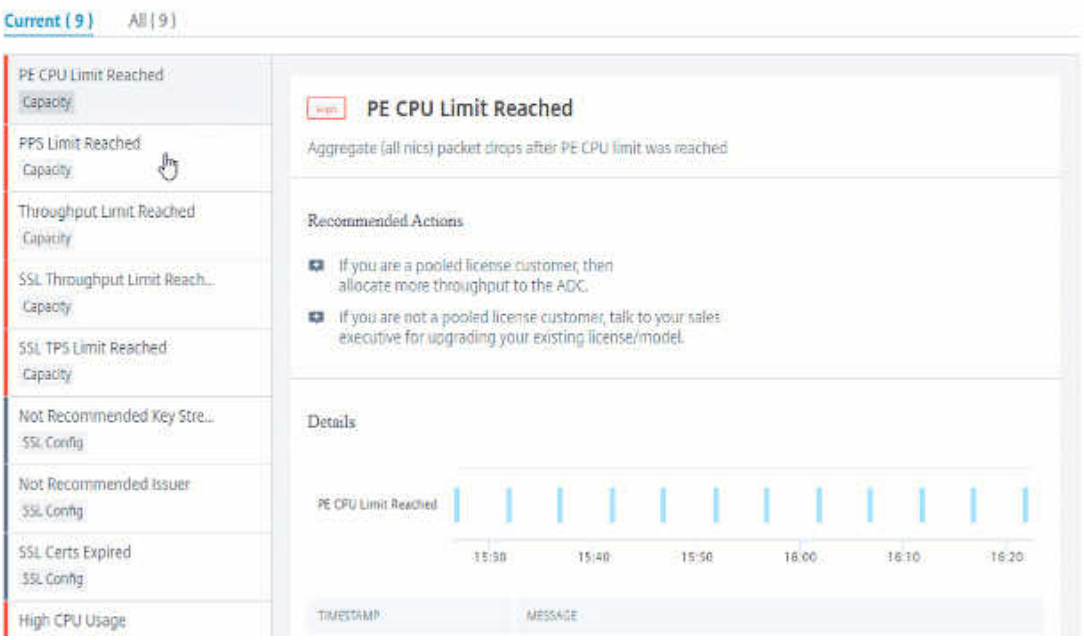
Vea las acciones recomendadas para resolver problemas de capacidad

El Citrix ADM 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.



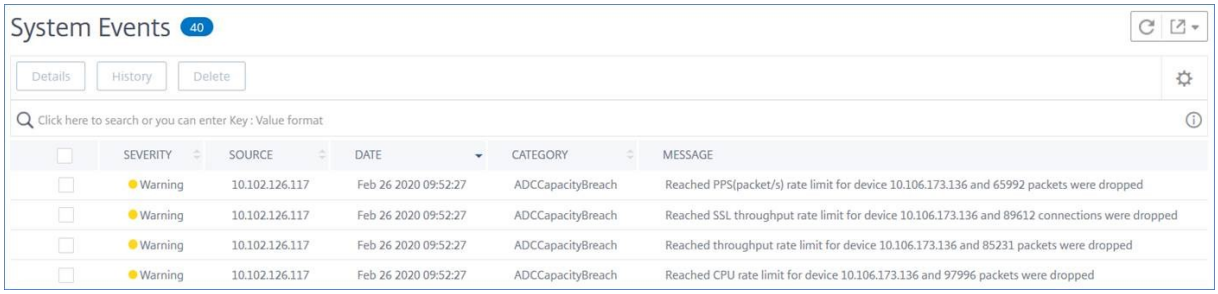
El Citrix ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra los paquetes descartados o los incrementos del contador de límites de velocidad, si existen.

El Citrix ADM calcula la puntuación de la instancia en el umbral de capacidad definido.

- **Umbral bajo** : 1 caída de paquete o incremento de contador de límite de tasa
- **Umbral alto**: Incremento del contador de límite de velocidad o caída de 10000 paquetes

Por lo tanto, cuando una instancia de ADC infringe el umbral de capacidad, la puntuación de la instancia se ve afectada.

Cuando los paquetes caen o el contador de límite de velocidad aumenta, se genera un evento bajo la categoría `ADCCapacityBreach`. Para ver estos eventos, vaya a **Configuración > Eventos del sistema Citrix ADM**.



Análisis de infraestructura mejorado con nuevos indicadores

November 16, 2022

Con Citrix ADM **Infrastructure Analytics**, puede:

- Vea un nuevo conjunto de problemas operativos que se producen en las instancias de Citrix ADC.
- Consulta los mensajes de error y consulta las recomendaciones para solucionar los problemas.

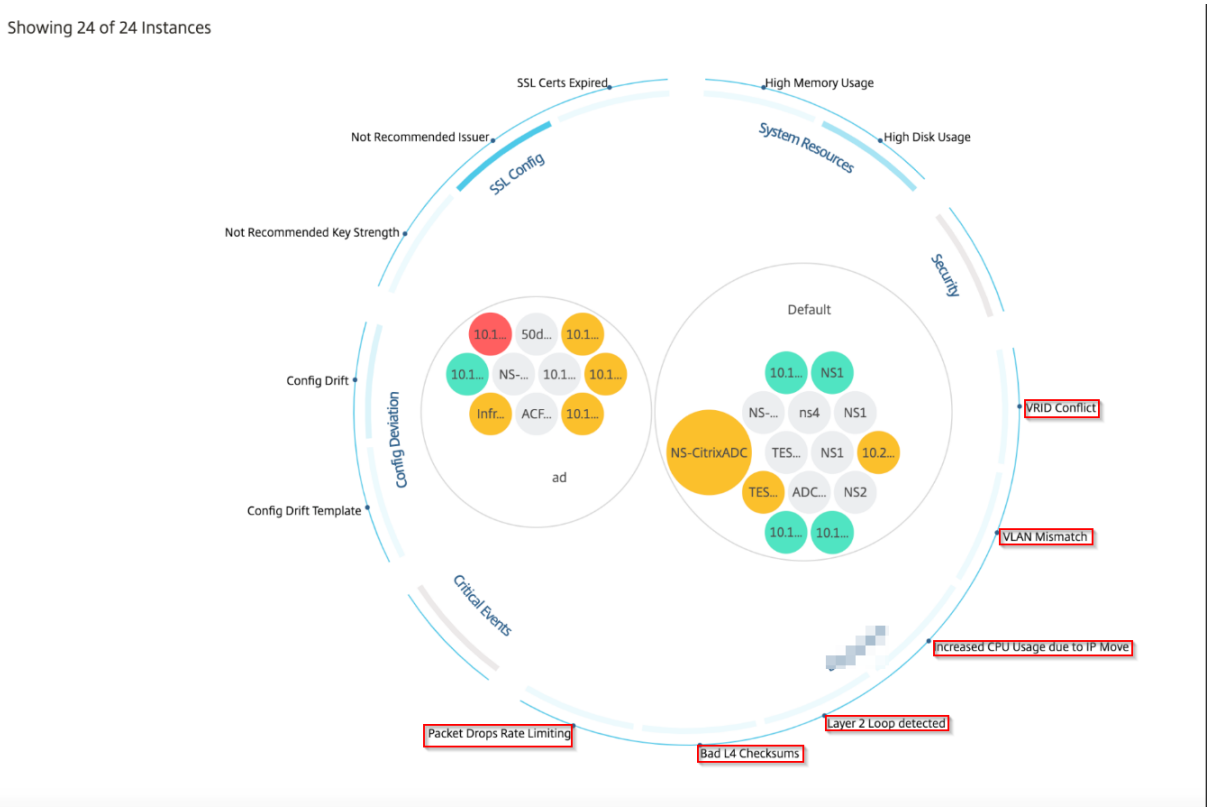
Como administrador, puede identificar rápidamente la causa principal del análisis de los problemas.

> **Nota**
>
> Los indicadores de reglas no son compatibles con:
>
> - Instancias de Citrix ADC configuradas en modo de clúster.
> - Instancias Citrix ADC configuradas con particiones de administración.

En Citrix ADM, vaya a **Infraestructura > Análisis de infraestructura** para ver los indicadores de:

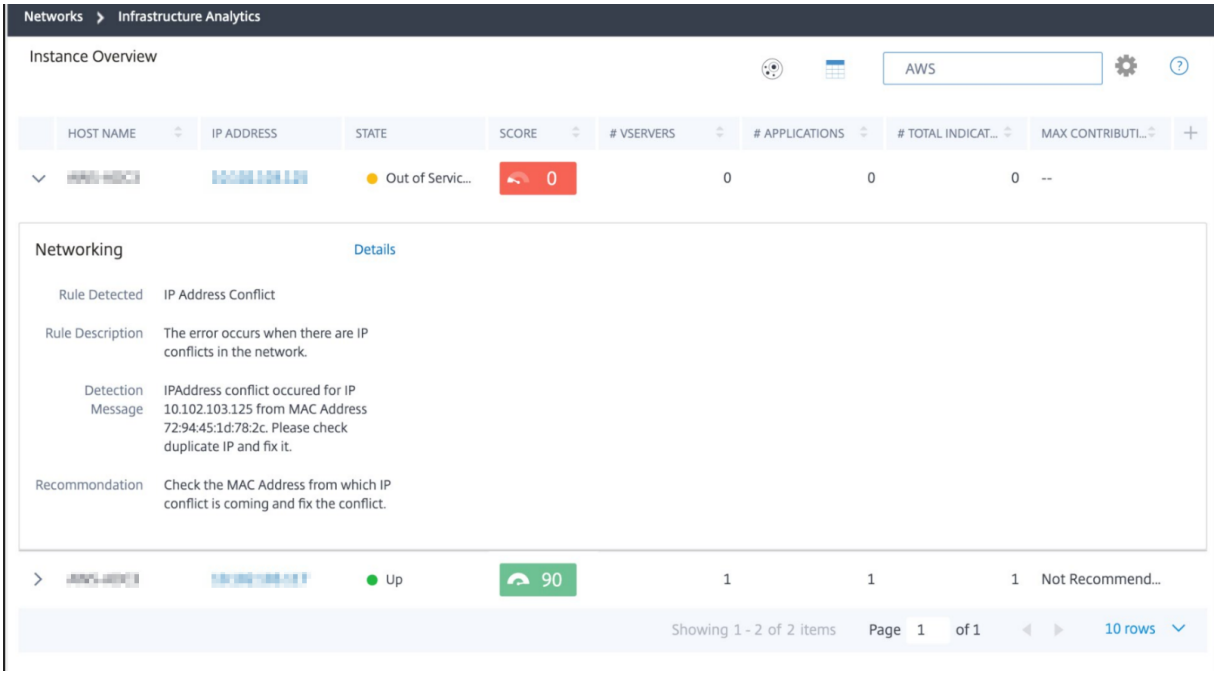
Nombre del indicador en Infrastructure Analytics	Descripción
Error de asignación de puertos	Detecta cuándo Citrix ADC usa SNIP para comunicarse con una nueva conexión de servidor y el total de puertos disponibles en ese SNIP está agotado. La acción recomendada es agregar otro SNIP en la misma subred.
Acumulación de sesiones	Detecta cuándo las sesiones SSL retienen la memoria de Citrix ADC.
No hay configuración de ruta predeterminada	Detecta cuándo se interrumpe el tráfico debido a la falta de disponibilidad de rutas.
Conflicto de IP	Detecta si se configura o se aplica una misma dirección IP en dos o más instancias de una red.
Conflicto de VRID	Detecta cuando se producen problemas de acceso intermitentes para el VRID especificado.
Discordancia de VLAN	Detecta si se produce algún error durante la configuración de la VLAN enlazada a las subredes IP.
Ataque de ventana pequeña TCP	Detecta si hay un posible ataque a una ventana pequeña en curso. Esta alerta es solo a título informativo, porque ADC ya mitiga este ataque.
umbral de control de velocidad	Detecta cuándo se descartan paquetes según el umbral de control de velocidad configurado.
Límite de persistencia	Detecta cuándo se impone el máximo de visitas a la memoria Citrix ADC.
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.

Nombre del indicador en Infrastructure Analytics	Descripción
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.



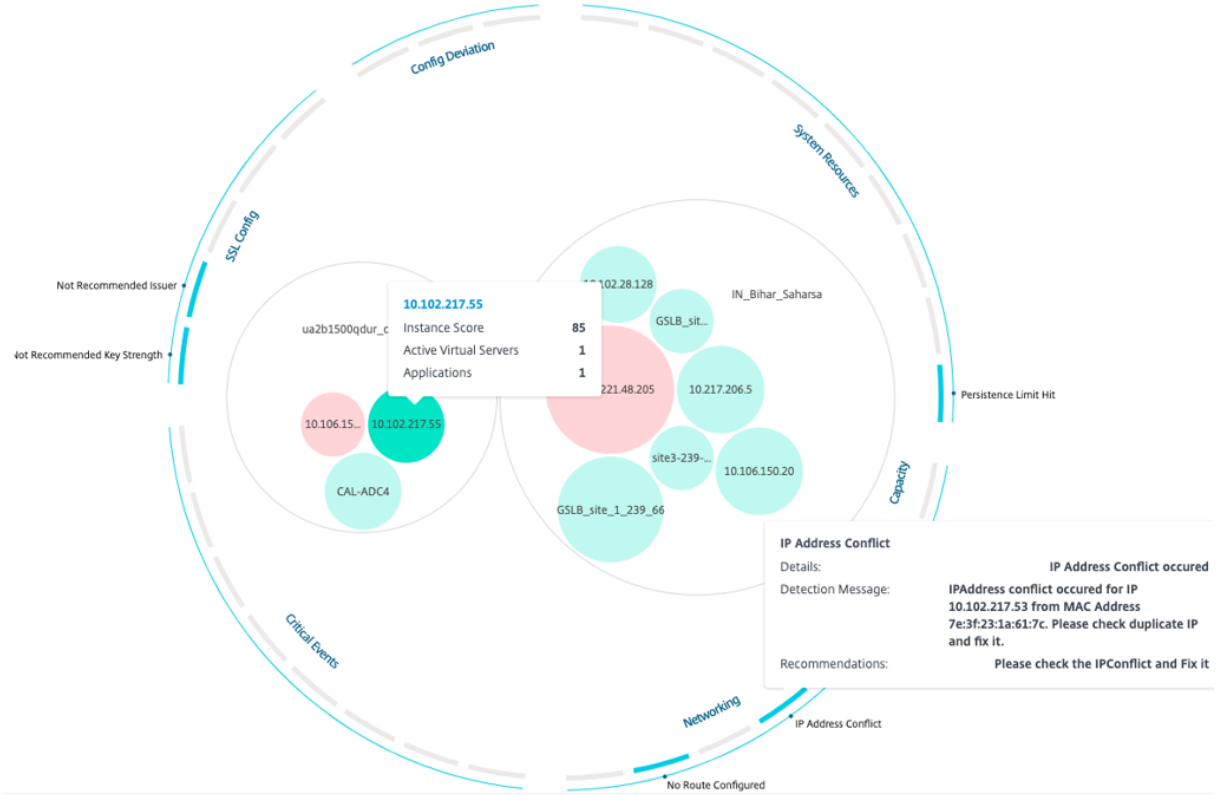
Vista tabular

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

November 16, 2022

Las instancias son dispositivos Citrix Application Delivery Controller (ADC) que se pueden administrar, supervisar y solucionar problemas mediante Citrix ADM. Agregue instancias a Citrix ADM para supervisarlas. Se pueden agregar instancias al configurar Citrix ADM o posterior también. Después de agregar instancias a Citrix ADM, se sondean continuamente para recopilar información que posteriormente se puede utilizar para resolver problemas o como datos de informes.

Las instancias se pueden agrupar como un grupo estático o como un bloque IP privado. Un grupo estático de instancias puede 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 mientras configura el servidor Citrix ADM por primera vez o más tarde. Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de Citrix ADC, o un intervalo de direcciones IP.

Para obtener información sobre cómo agregar una instancia a Citrix ADM, consulte Agregar instancias a Citrix ADM.

Cuando agrega una instancia al servidor Citrix ADM, 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 Citrix ADM descubre instancias.

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**.

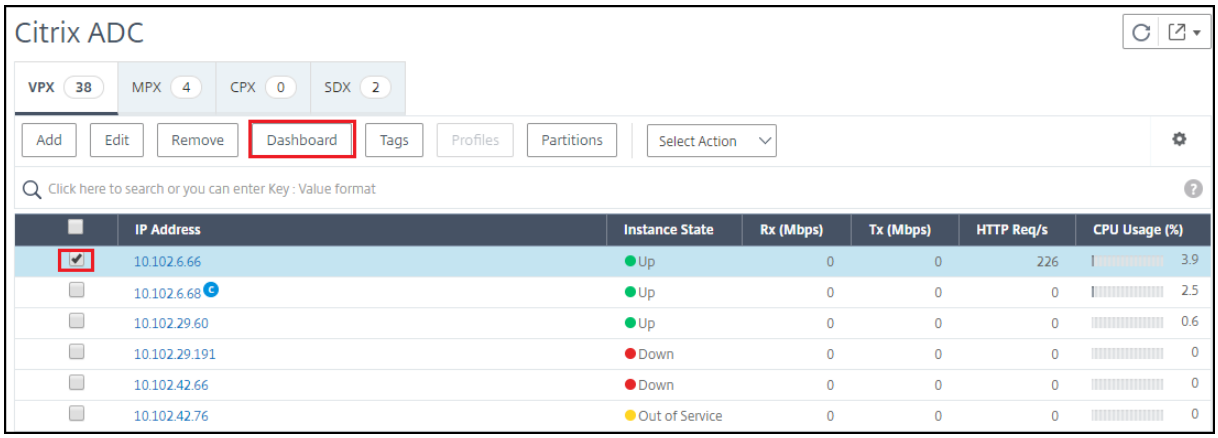
Cómo usar el panel de instancias

El panel de control por instancia de Citrix ADM muestra los datos en formato tabular y gráfico de la instancia seleccionada. Los datos recopilados de tu instancia durante el proceso de sondeo se mues-

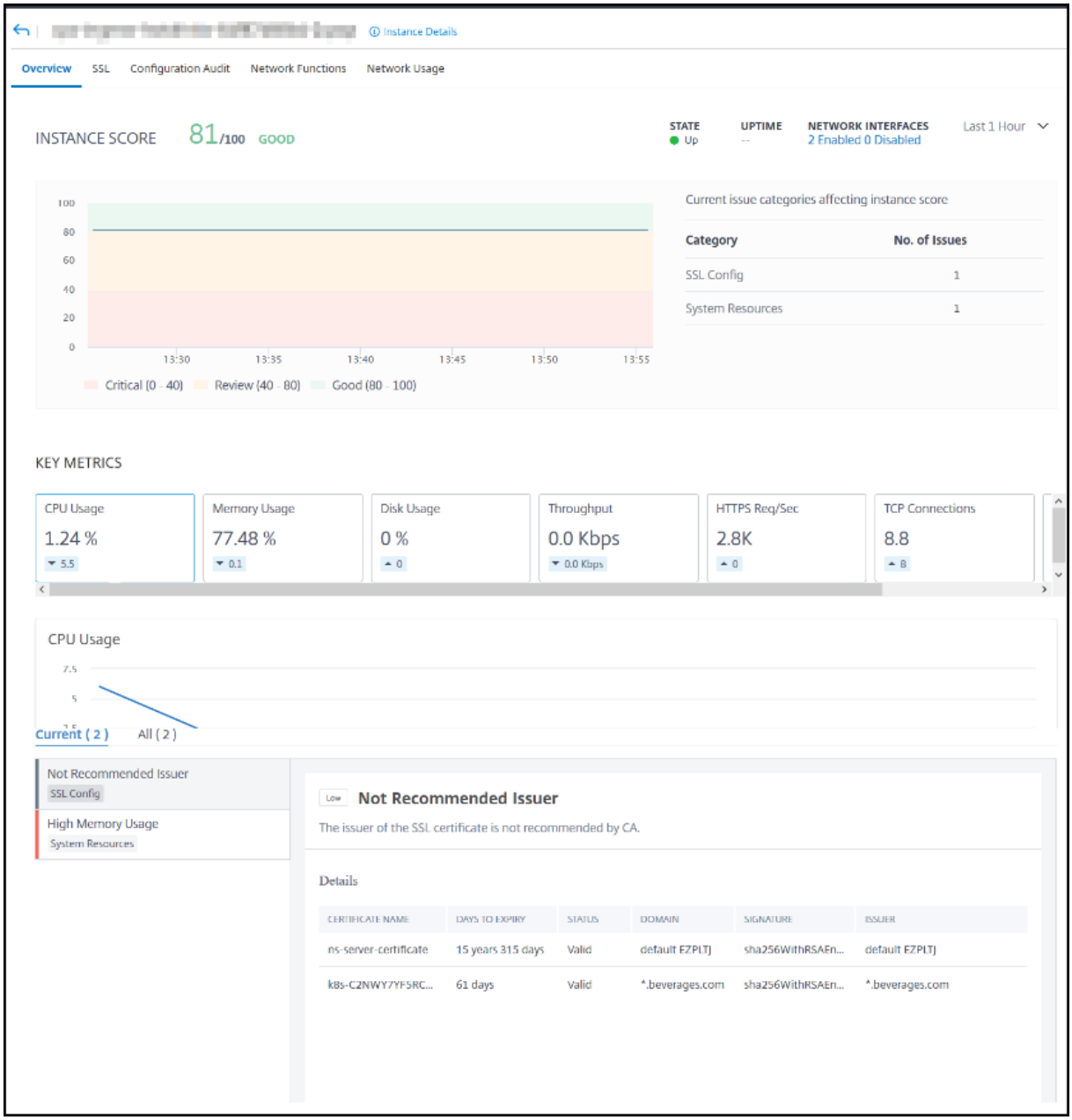
tran en el panel de control.

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 > Citrix ADC**. En la página Citrix ADC, 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**. Puedes 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 Citrix ADCy los gráficos de deriva de la configuración** de Citrix ADC del panel muestran detalles de alto nivel sobre los cambios de configuración en las configuraciones guardadas frente a las no guardadas
- **Funciones de red**. Mediante el panel de funciones de red, puede supervisar el estado de las entidades configuradas en la instancia de Citrix ADC seleccionada. Puede ver gráficos de sus servidores virtuales que muestran datos como las conexiones de los clientes, el rendimiento y las conexiones de los servidores.
- **Uso de red**. Puedes 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

November 16, 2022

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 en Citrix ADM le proporciona una representación gráfica de sus sitios y desglosa su experiencia de monitoreo de redes por geografía. 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 Citrix ADM.

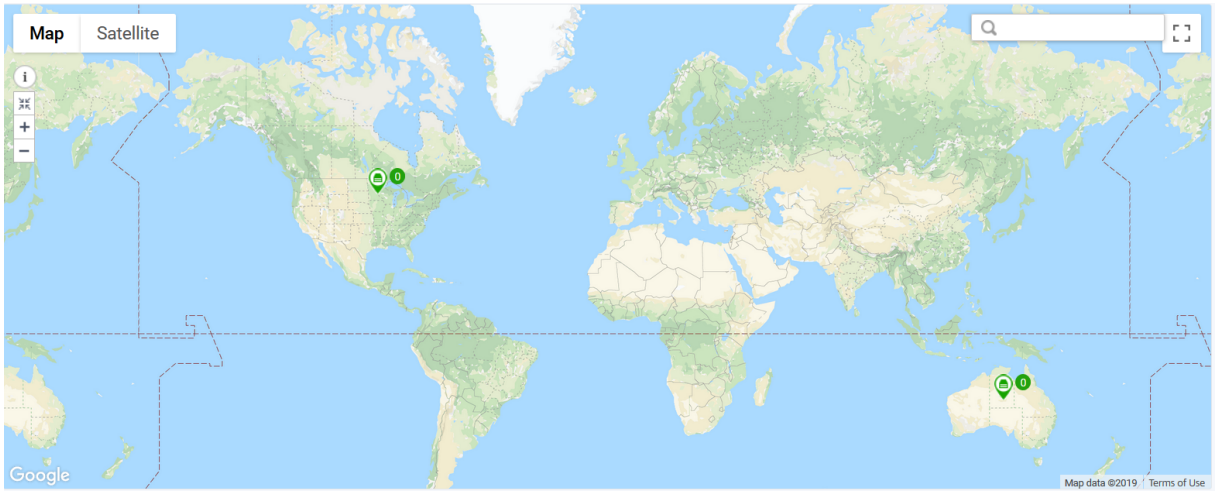
Supervisión de sitios distribuidos globalmente en Citrix ADM

El sitio Citrix ADM es una agrupación lógica de instancias de Citrix Application Delivery Controller (Citrix ADC) en una ubicación geográfica específica. Por ejemplo, mientras que un sitio está asignado a Amazon Web Services (AWS) y otro sitio puede estar asignado a Azure™. Otro sitio más está alojado en las instalaciones del inquilino. Citrix ADM administra y supervisa todas las instancias de Citrix ADC conectadas a todos los sitios. Puede usar Citrix ADM para supervisar y recopilar syslog, AppFlow, SNMP y cualquier dato de este tipo que se origine en las instancias administradas.

Geomaps en Citrix ADM le proporciona una representación gráfica de sus sitios. Geomaps también desglosa su experiencia de monitoreo 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.

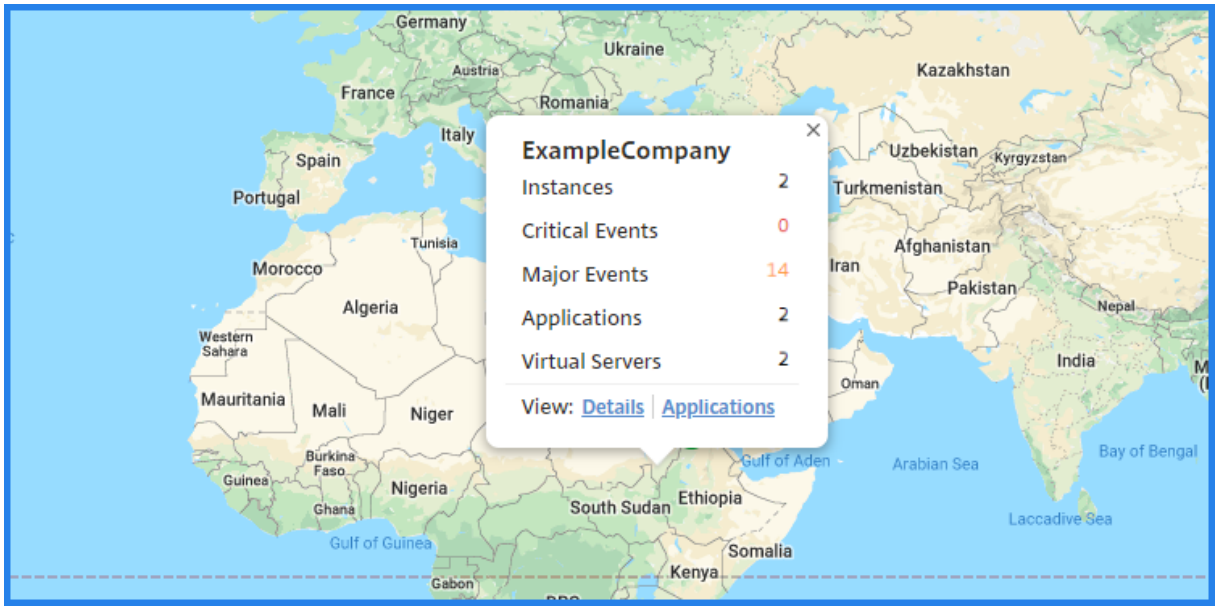
Caso de uso

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:

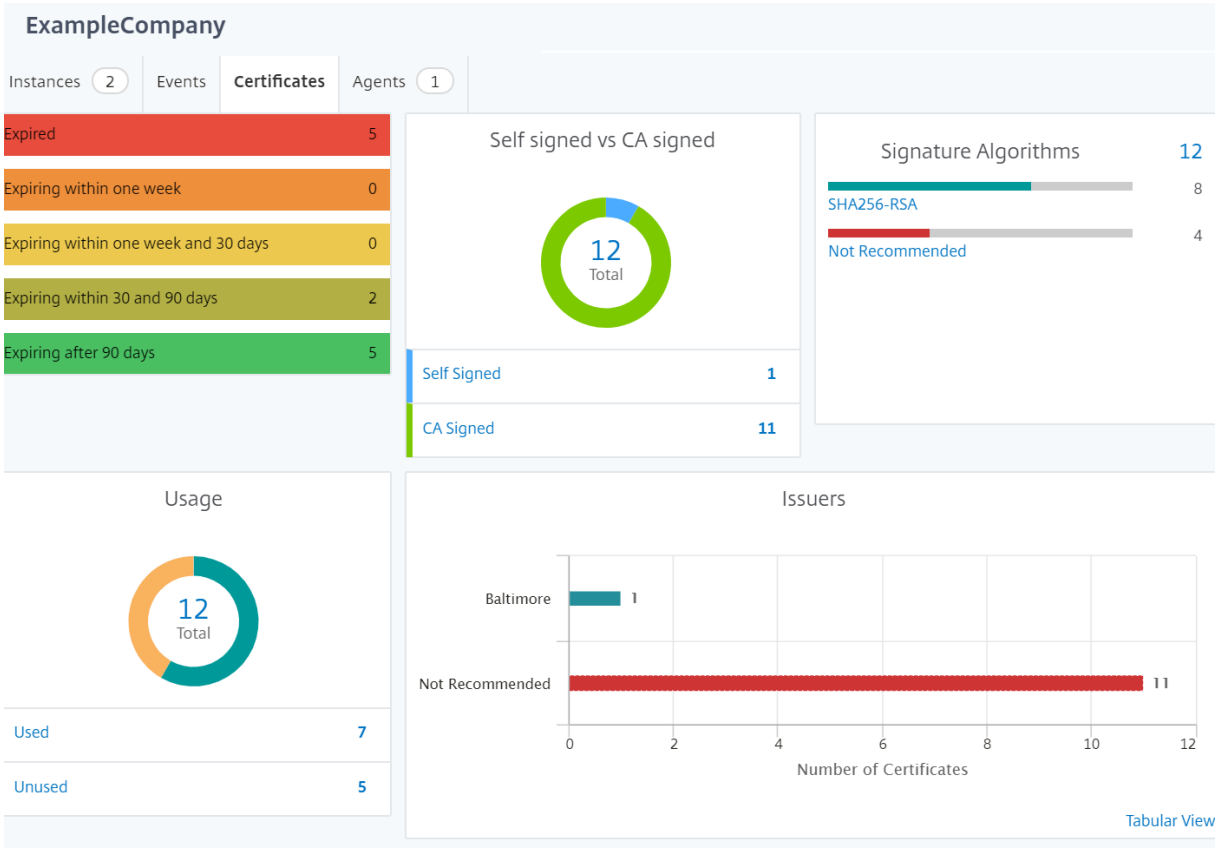
- **Instancias**: indica el número de instancias disponibles.
- **Aplicaciones**: indica el número de aplicaciones alojadas.
- **Servidores virtuales**: Indica el número de servidores virtuales disponibles.
- **Eventos Críticos**: Indica el recuento de eventos críticos ocurridos en las instancias.
- **Eventos principales**: Indica el recuento de eventos principales ocurridos 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 Citrix ADC 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 Citrix ADC
  - Número de eventos críticos
  - Eventos significativos y todos los eventos generados en una instancia de Citrix ADC.
- Ficha**Eventos** : consulta una lista de los eventos importantes y críticos que se producen en las instancias.
- Ficha**Certificados** : vea lo siguiente en esta ficha:
  - Lista de certificados de todas las instancias
  - Estado de caducidad
  - Información vital y las 10 instancias principales según muchos certificados en uso.
- Ficha**Agentes**: Permite ver una lista de agentes a los que están enlazadas las instancias.



Configuración de Geomaps

ExampleCompany decidió crear un tercer sitio en Bangalore, India. La empresa quería probar la nube descargando algunas de sus aplicaciones de TI internas menos críticas a la oficina de Bangalore. La empresa decidió utilizar los servicios de computación en la nube de AWS.

Como administrador, primero debe crear un sitio y, a continuación, agregar las instancias de Citrix ADC en Citrix ADM. También debe agregar la instancia al sitio, agregar un agente y vincular el agente al sitio. A continuación, Citrix ADM reconoce el sitio al que pertenecen la instancia de Citrix ADC y el agente.

Para obtener más información sobre cómo agregar instancias de Citrix ADC, consulte Agregar instancias.

Para crear sitios:

Cree sitios antes de agregar instancias en Citrix ADM. Proporcionar información de ubicación le permite localizar el sitio con precisión.

1. En Citrix ADM, vaya a **Infraestructura > Instancias > Sitios** y haga clic en **Agregar**.
2. En la página **Crear sitio**, actualice la siguiente información y haga clic en **Crear**.
    a) **Tipo de sitio**. Selecciona **Centro de datos**.

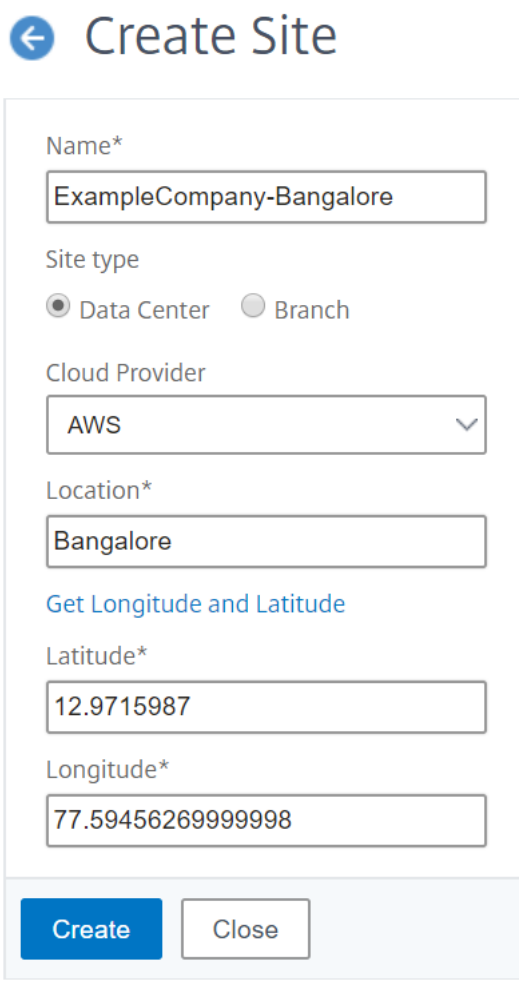
> **Nota**
>
> El sitio puede funcionar como centro de datos principal o como sucursal. Elija según corresponda.

a) **Tipo**. Seleccione AWS como proveedor de nube de la lista.

> **Nota**
>
> Active la casilla **Usar VPC existente como sitio** en consecuencia.

b) **Nombre del sitio**. Escriba el nombre del sitio.

c) **Ubicación de búsqueda**. Escriba el nombre de la ciudad. Haga clic en **Obtener ubicación** para colocar el sitio exactamente en la ubicación.
Los campos Ciudad, Código postal, Región, País, Latitud y Longitud se rellenan automáticamente.

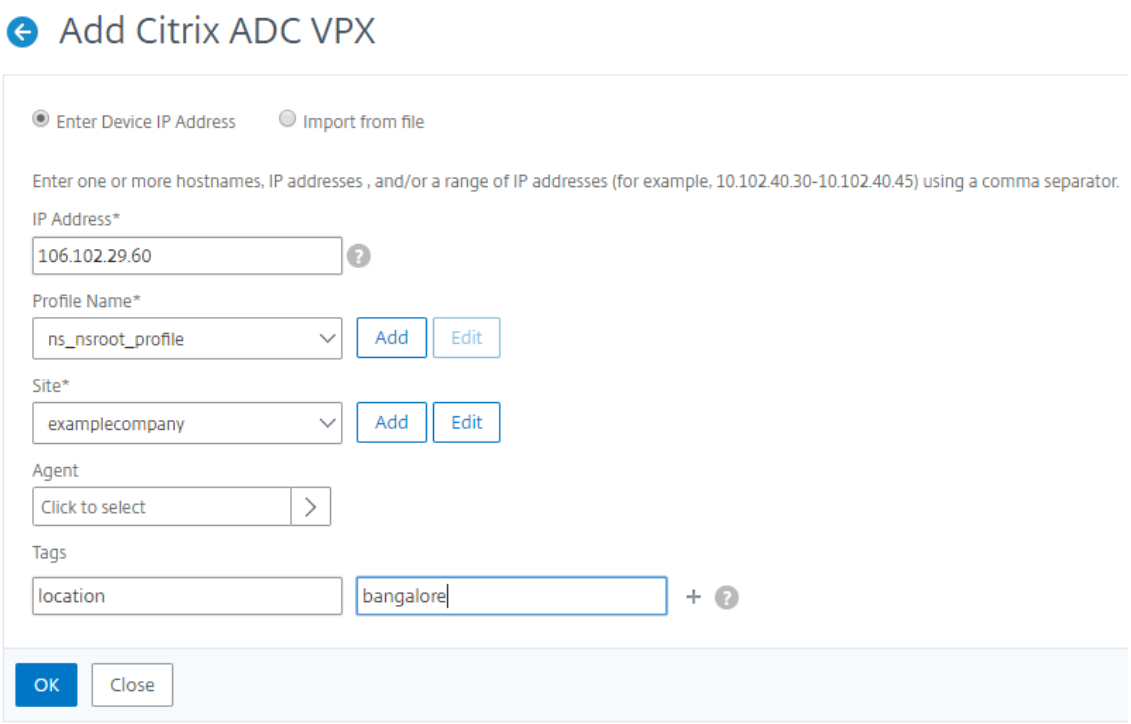


d) Haga clic en **Crear** para crear un sitio en Bangalore.

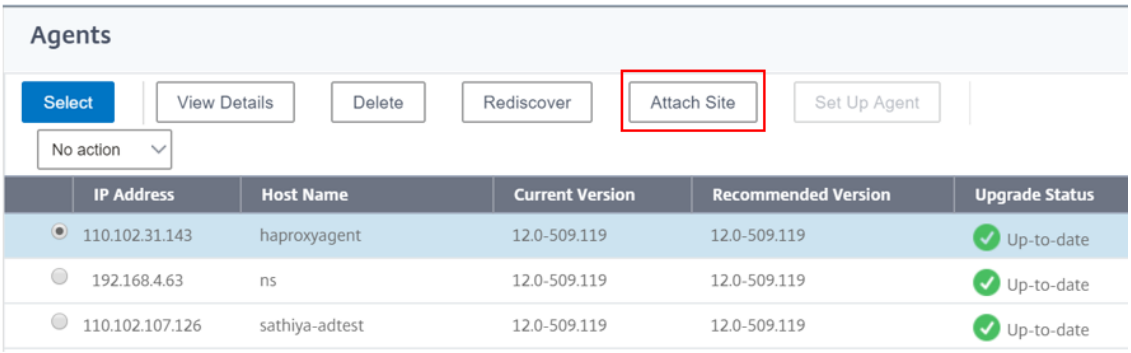
Para agregar instancias y seleccionar sitios:

Tras crear los sitios, debe agregar instancias en Citrix ADM. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

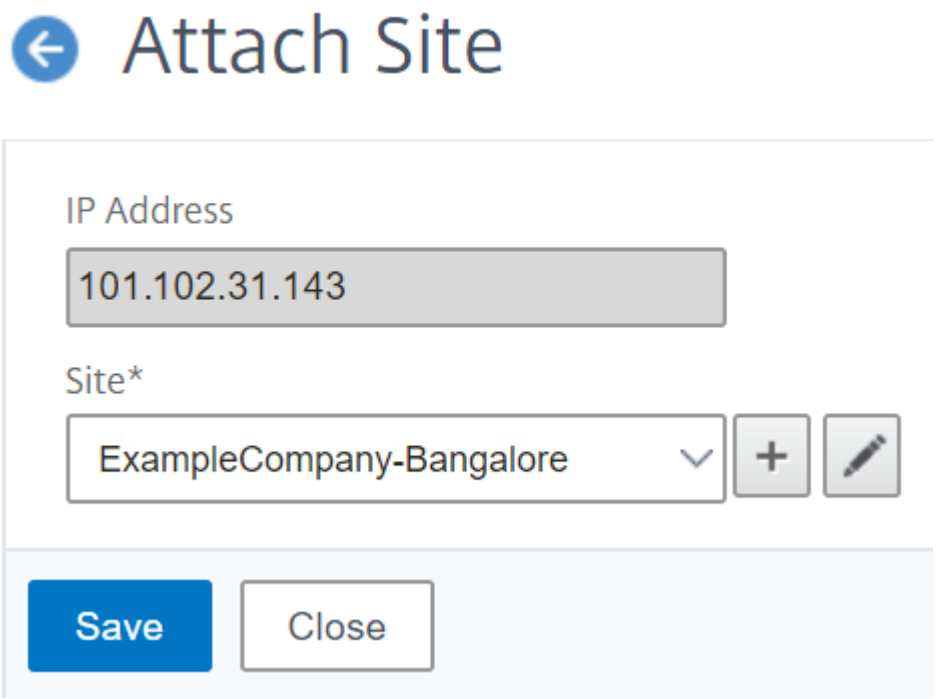
1. En Citrix ADM, vaya a **Infraestructura > Instancias > Citrix ADC**.
2. Seleccione el **VPX**y haga clic en **Agregar**.
3. En la página **Agregar Citrix ADC VPX**, escriba la dirección IP y seleccione el perfil de la lista.
4. Seleccione el sitio de la lista. Puede hacer clic en el botón **Agregar** 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 Citrix ADM al sitio:

1. En Citrix ADM, 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**.

Citrix ADM comienza a supervisar las instancias de Citrix ADC agregadas en el sitio de Bangalore junto con las instancias de los otros dos sitios también.

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 especificar todos los días que quiere programar el informe separados por comas.

Cómo crear etiquetas y asignar a instancias

November 16, 2022

Citrix ADM ahora le permite asociar sus instancias de Citrix ADC con etiquetas. Una etiqueta es una palabra clave o un término de una palabra que puede asignar a una instancia. Las etiquetas agregan información adicional sobre la instancia. Las etiquetas se pueden considerar como 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.

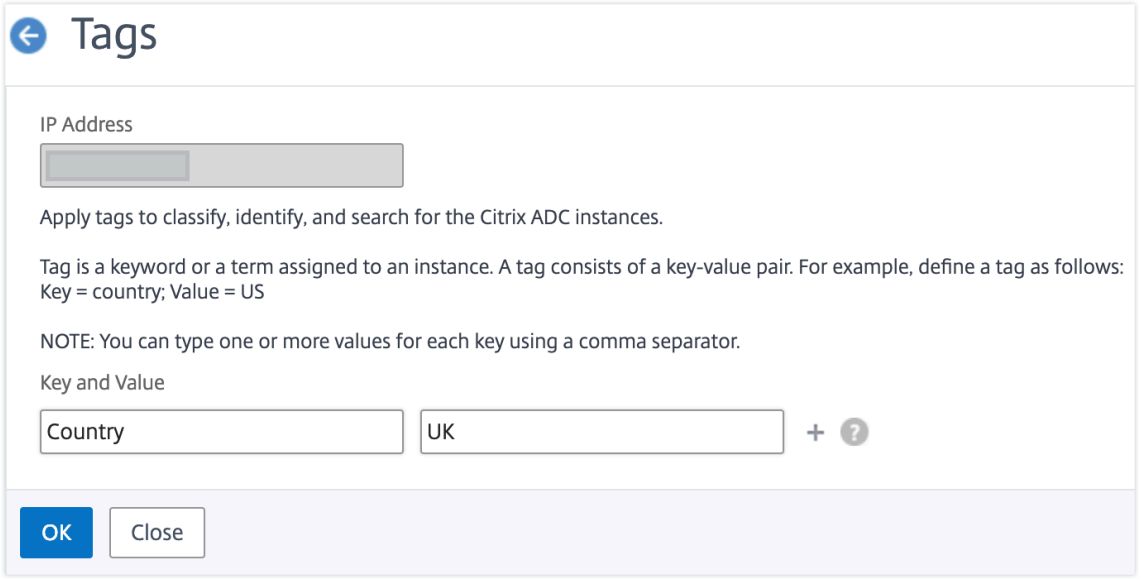
Los siguientes casos de uso le ayudan a entender cómo el etiquetado de las instancias le ayudará a supervisarlas mejor.

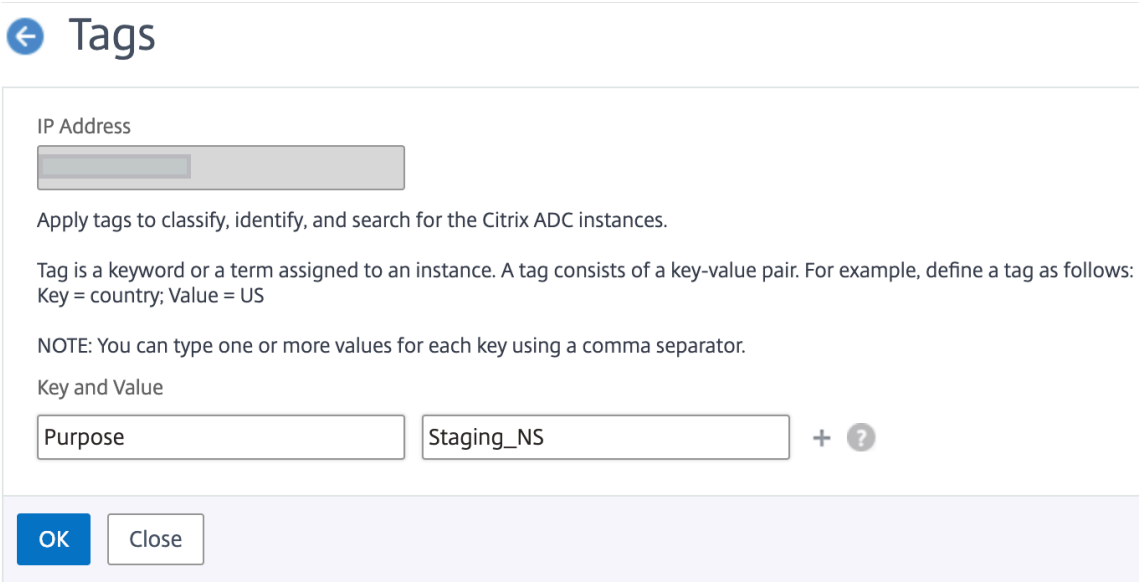
- **Caso de uso 1**: Puede crear una etiqueta para identificar todas las instancias que se encuentran en el Reino Unido. Aquí, puede crear una etiqueta con la clave como “País” y el valor como “Reino Unido”. “ Esta etiqueta le ayuda a buscar y supervisar todas las instancias que se encuentran en el Reino 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 Citrix ADC 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 Citrix ADC VPX:

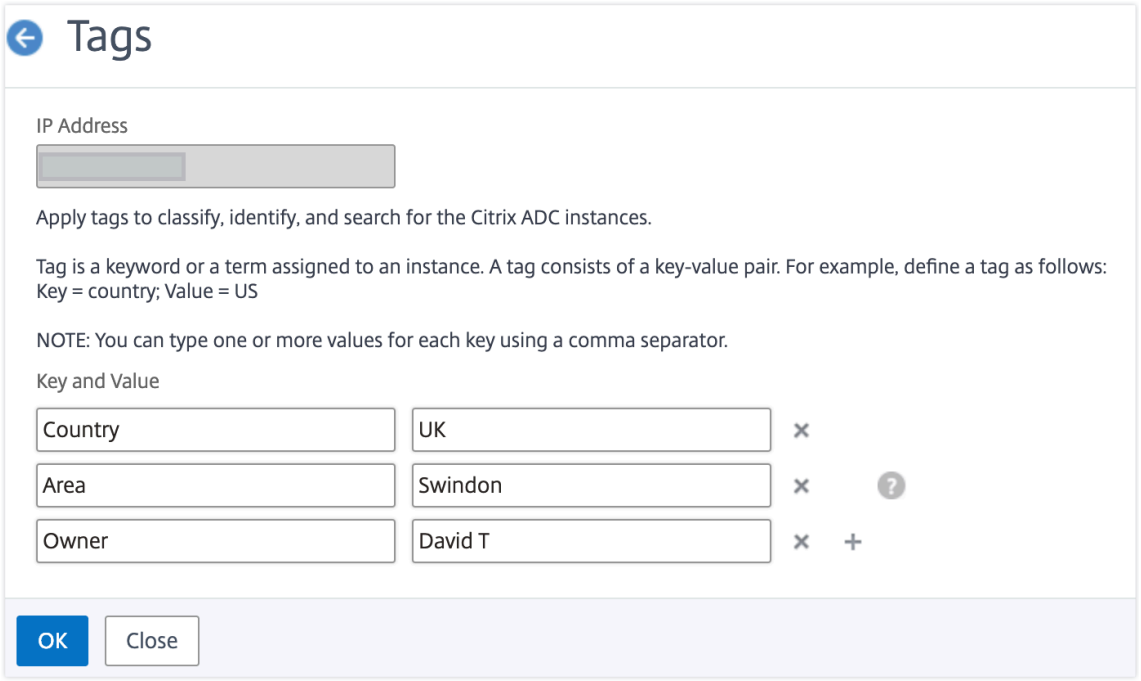
1. En Citrix ADM, vaya a **Infraestructura > Instancias > Citrix ADC**.
2. Selecciona la ficha **VPX** .
3. Seleccione la instancia VPX requerida.
4. Haga clic en **Etiquetas**. La ventana de **etiquetas** que aparece le permite crear sus propios pares de «clave-valor» asignando valores a cada palabra 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.



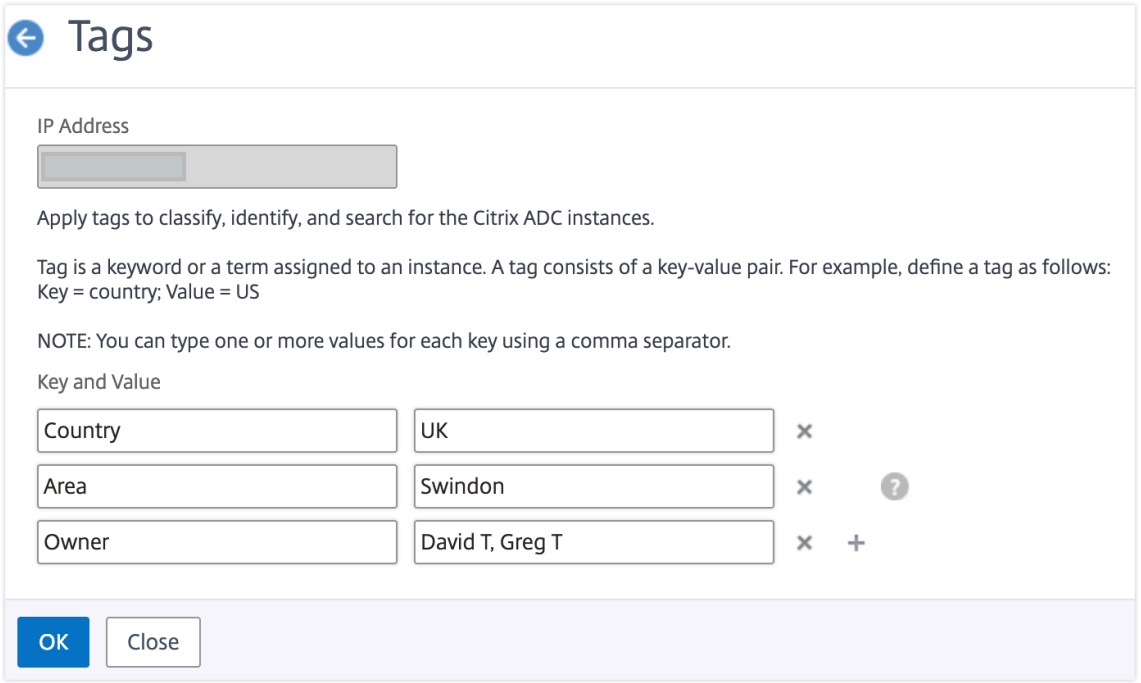


También puede agregar varias etiquetas haciendo clic en “+”. La adición de etiquetas múltiples y significativas le permite buscar de manera eficiente las instancias.



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. Citrix ADM reconoce los valores separados por comas en dos valores diferentes.



Para obtener más información sobre cómo buscar instancias en función de etiquetas, consulte

Cómo buscar instancias mediante valores de etiquetas y propiedades.

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

November 16, 2022

Puede darse una situación en la que Citrix ADM administre muchas instancias de Citrix ADC. Como administrador, es posible que desees tener la flexibilidad de buscar en el inventario de instancias en función de ciertos parámetros. Citrix ADM ahora ofrece una capacidad de búsqueda mejorada para buscar en un subconjunto de instancias de Citrix ADC en función de los parámetros que defina en el campo de búsqueda. Puede buscar las instancias en función de dos criterios: etiquetas y propiedades.

- **Etiquetas**. Las etiquetas son términos o palabras clave que puede asignar a una instancia de Citrix ADC para agregar una descripción adicional sobre la instancia de Citrix ADC. Ahora puede asociar sus instancias de Citrix ADC con etiquetas. Estas etiquetas se pueden usar para identificar y buscar mejor las instancias de Citrix ADC.
- **Propiedades**. Cada instancia de Citrix ADC agregada en Citrix ADM tiene algunos parámetros o propiedades predeterminados asociados a esa instancia. Por ejemplo, cada instancia tiene su propio nombre de host, dirección IP, versión, ID de host, ID de modelo de hardware, etc. Puede buscar instancias especificando valores para cualquiera de estas propiedades.

Por ejemplo, considere una situación en la que quiere obtener la lista de instancias de Citrix ADC que están en la versión 12.0 y están en estado ACTIVO. Aquí, la versión y el estado de la instancia se definen mediante las propiedades predeterminadas.

Además de la versión 12.0 y el estado de funcionamiento de las instancias, también puede buscar aquellas instancias que te pertenezcan. Puedes 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.

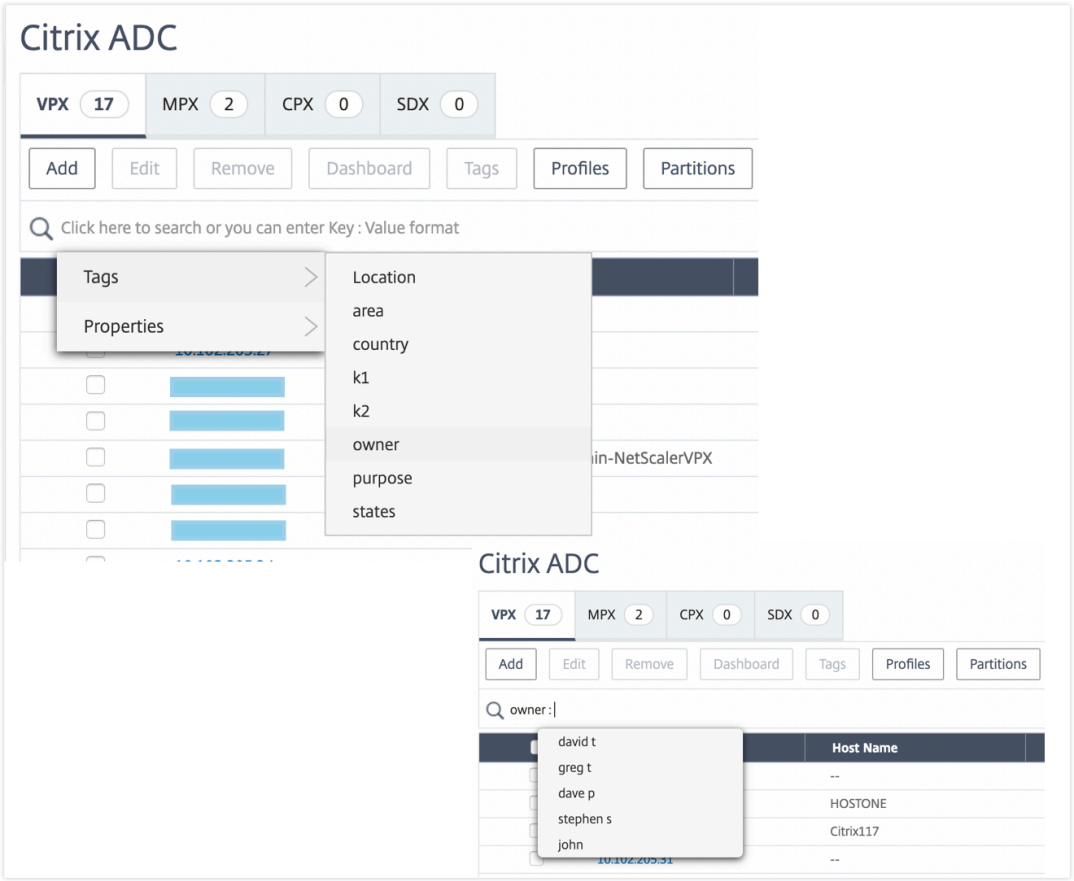
Para buscar instancias de Citrix ADC VPX

1. En Citrix ADM, vaya a **Infraestructura > Instancias > Citrix ADC**.

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.

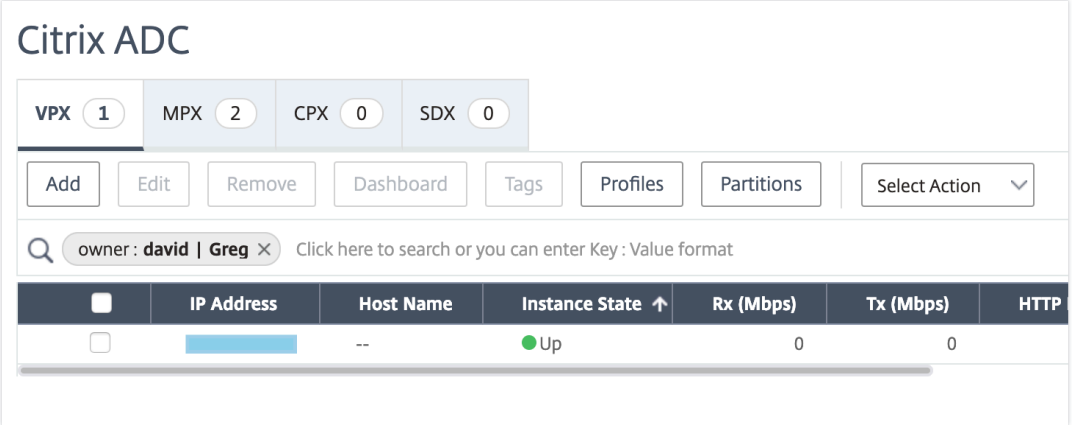
   Los siguientes ejemplos muestran cómo puede utilizar la expresión de búsqueda de manera eficiente para buscar la instancia.

   a) Seleccione la opción **Etiquetas** y seleccione **Propietario**. Seleccione “David T”.

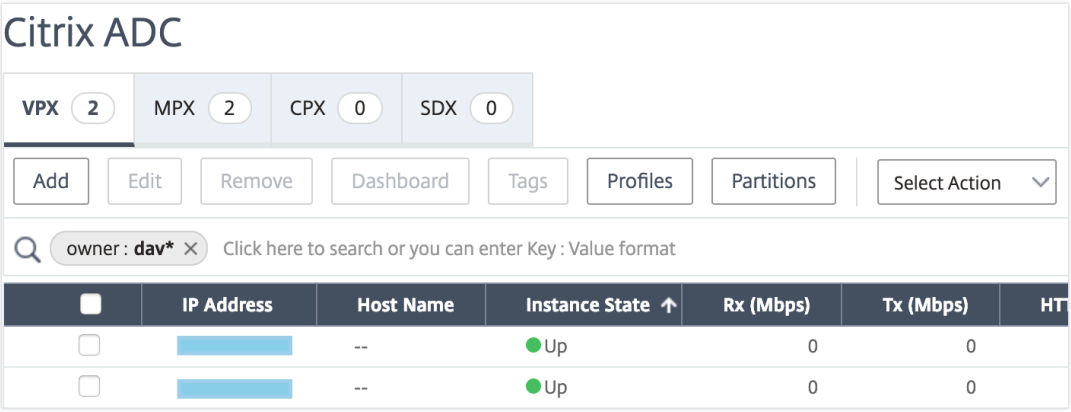


Citrix ADM admite expresiones regulares y caracteres comodín en las expresiones de búsqueda.

   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 expresiones regulares y caracteres comodín y cómo usarlos, haga clic en el icono “información” de la barra de búsqueda.

Administrar particiones de administración de instancias Citrix ADC

November 16, 2022

Puede configurar particiones de administración en sus instancias de Citrix Application Delivery Controller (Citrix ADC) para que a los diferentes grupos de su organización se les asignen diferentes particiones en la misma instancia de Citrix ADC. Puede asignar un administrador de red para administrar varias particiones en varias instancias de Citrix ADC.

Citrix ADM proporciona una forma sencilla de administrar todas las particiones que pertenecen a un administrador desde una única consola. Puede administrar estas particiones sin interrumpir otras configuraciones de particiones.

Para permitir que varios usuarios administren diferentes particiones de administración, debe crear grupos y, a continuación, asignar usuarios y particiones a esos grupos. Para obtener más información sobre la creación de un grupo o un usuario, consulte [Crear un usuario] (/en-us/citrix-application-delivery-management-service/setting-up/configuring-role-based-access-control.html #configure -Users-on-Citrix ADM) y [Crear un grupo] (/en-us/citrix-application-delivery-management-service/setting-up/configuring-role -based-access-control.html #configure -Grupos en Citrix ADM).

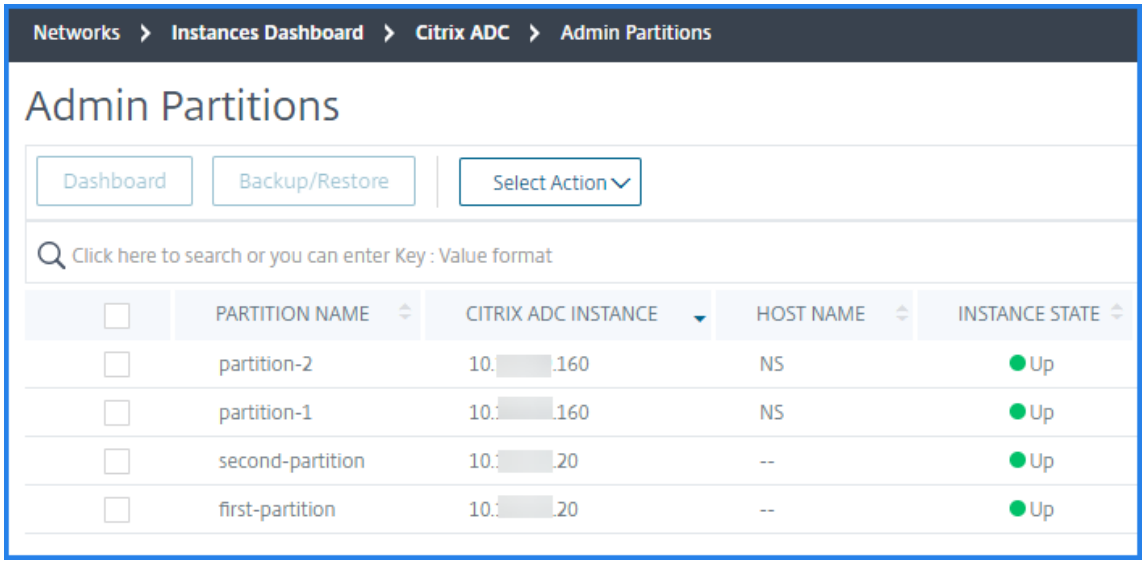
Un usuario solo puede ver y administrar las particiones del grupo al que pertenece el usuario. Cuando detecta una instancia de Citrix ADC, las particiones de administración configuradas en esa instancia de Citrix ADC se agregan al sistema automáticamente. Cada partición de administración se considera como una instancia en Citrix ADM.

Ver particiones de administración

Tenga en cuenta que tiene dos instancias de Citrix ADC VPX y que hay dos particiones de administración configuradas en cada instancia. Por ejemplo, la instancia 10.xx.xx.160 de Citrix ADC tiene la partición 1 y la partición 2, y la instancia 10.xx.xx.20 tiene la primera y la segunda partición.

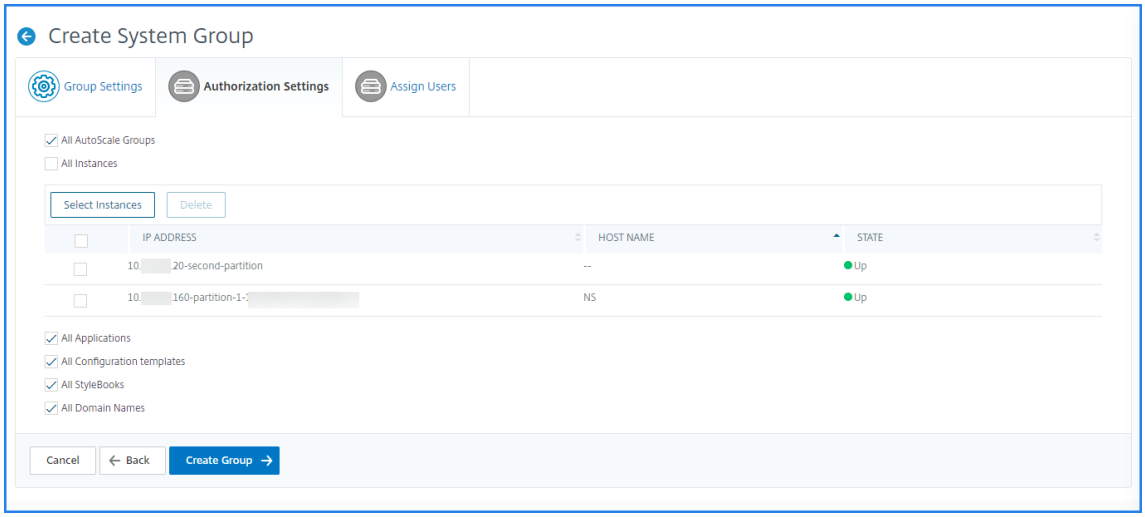
Realice los siguientes pasos para ver las particiones de administración:

1. Vaya a**Infraestructura > Instancias > Citrix ADC**.
2. En la ficha **VPX**, haga clic en **Particiones**.

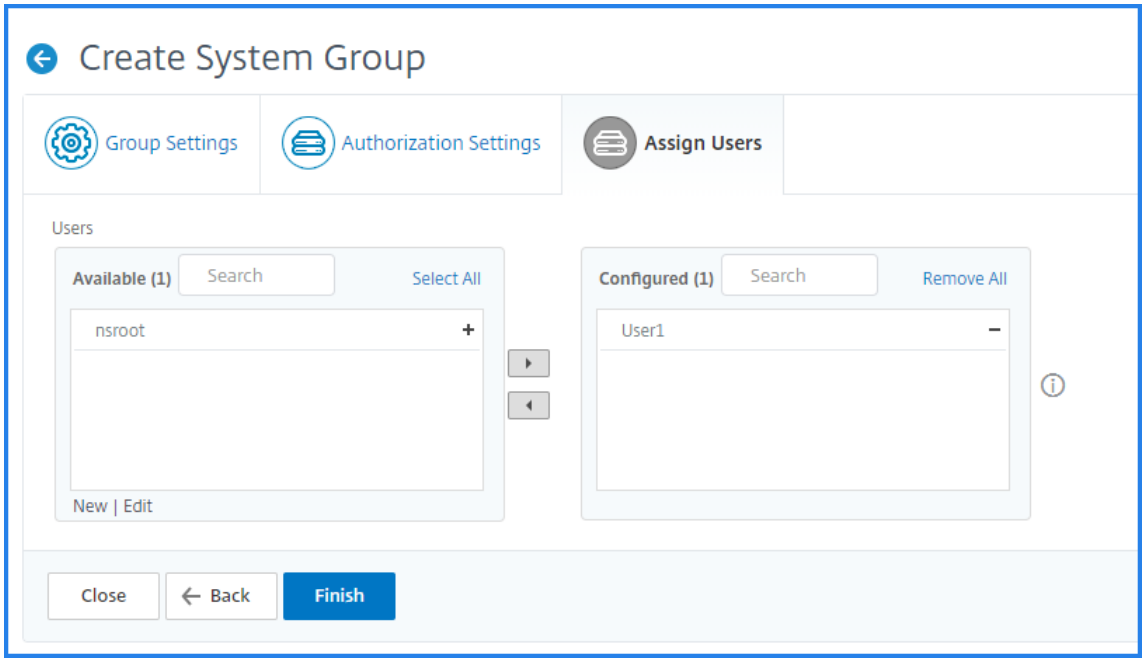


Por ejemplo, al crear un grupo con las siguientes condiciones:

- En la ficha **Configuración de autorización**, se seleccionan las instancias «10.xx.xx.20-second-partition» y «10.xx.xx.160-partition-1”.



- El «usuario 1” está asignado 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.20-first-partition y 10.xx.xx.160-partition-2 están restringidas. Porque las instancias no se agregan al grupo donde se asigna el usuario.

Si quiere que un usuario diferente administre las particiones admin 10.xx.xx.20-first partition y 10.xx.xx.160-partition-2, cree un grupo con las siguientes condiciones:

- En la ficha **Configuración de autorización**, seleccione las instancias 10.xx.xx.20-first-partition y 10.xx.xx.160-partition-2.
- Asigne el usuario requerido al grupo.

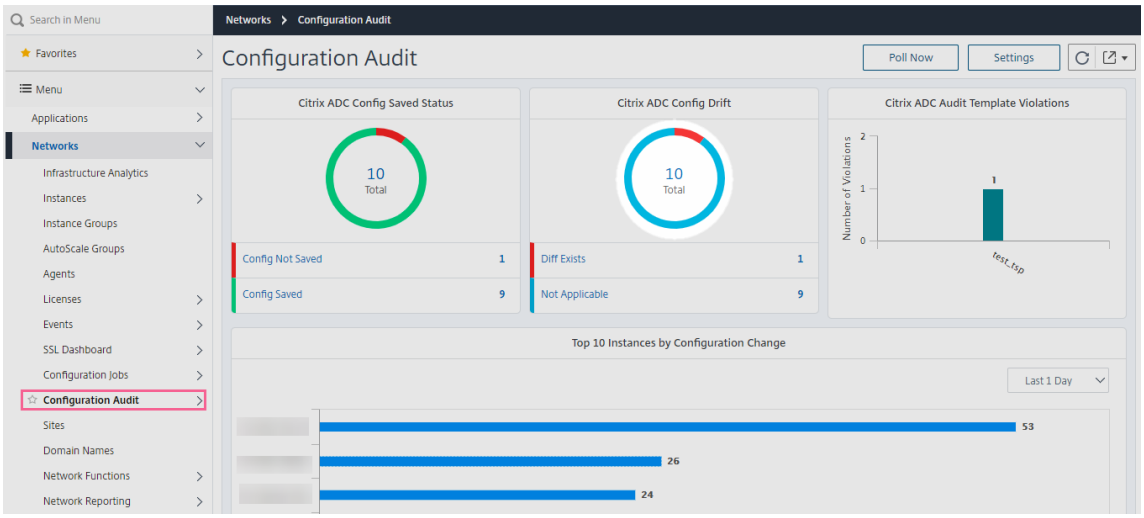
Este grupo permite al usuario asignado ver y administrar las particiones de administración seleccionadas.

Ver la diferencia en el historial de revisiones

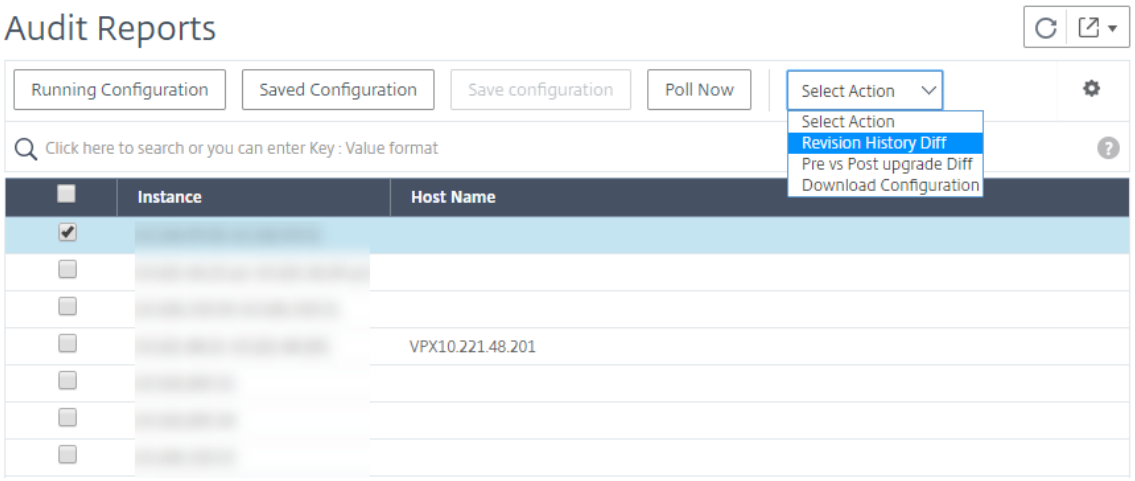
La diferencia del historial de revisiones para una partición de administrador le permite ver la diferencia entre los cinco archivos de configuración más recientes para una instancia de Citrix ADC particionada. Puede comparar los archivos de configuración entre sí (por ejemplo, Revisión de configuración: 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.

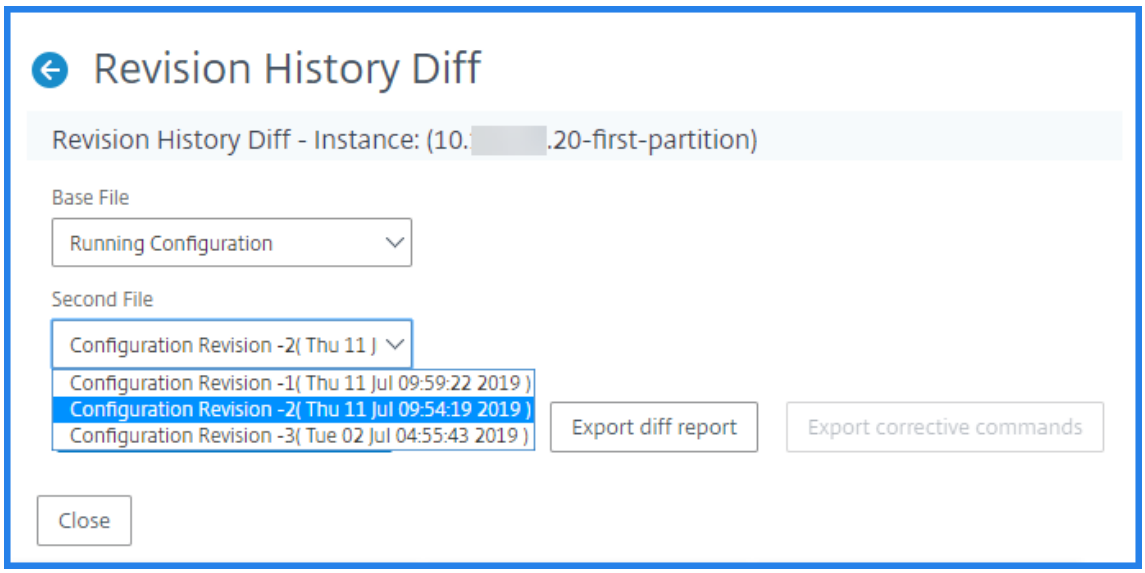


2. Seleccione la instancia de Citrix ADC particionada.
3. En el cuadro Acción, haga clic en **Diff del historial de revisiones**.

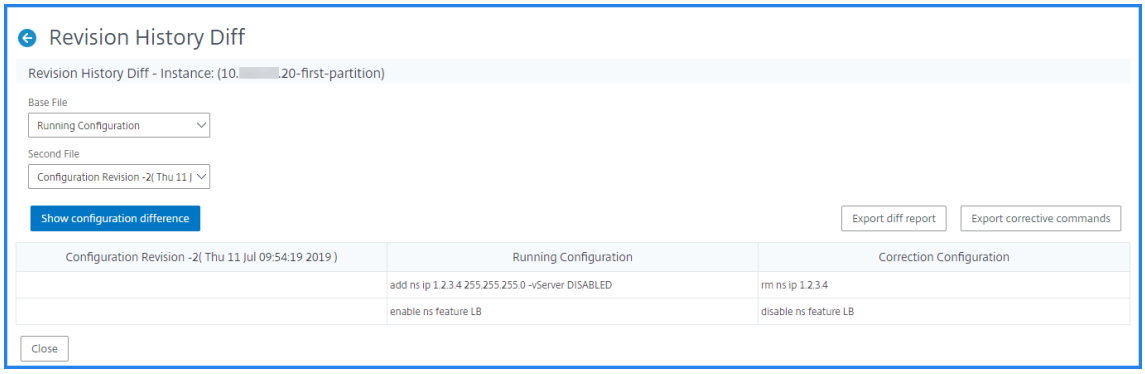


4. En la página **Diferencia del historial de revisiones**, seleccione los archivos que quiere comparar. Por ejemplo, compare la configuración guardada con la revisión de configuración 2 y, a continuación, haga clic en **Mostrar diferencia de configuración**.

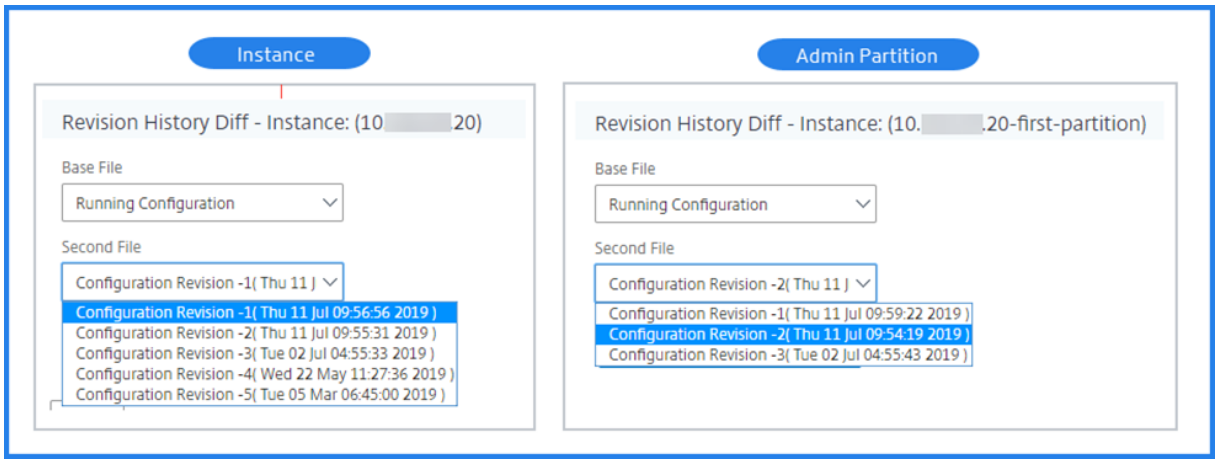
   A continuación, puede ver las diferencias entre los cinco archivos de configuración más recientes para la instancia de Citrix ADC particionada seleccionada. La siguiente es una partición de administrador de ejemplo que tiene tres configuraciones guardadas:



   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).



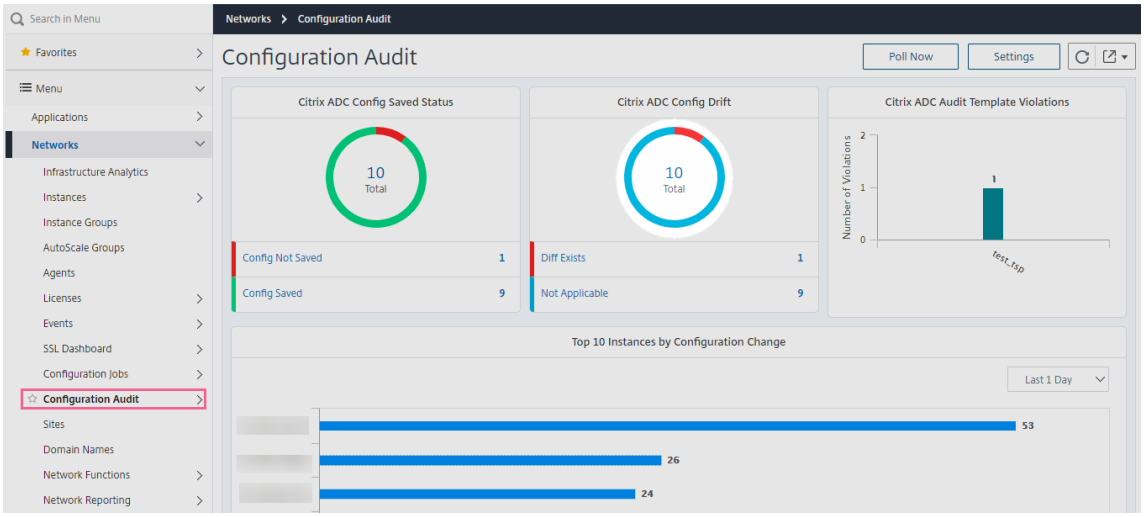
Las configuraciones guardadas en una partición de administración y la instancia son diferentes. En el ejemplo siguiente, la instancia 10.xx.xx.20 tiene cinco configuraciones guardadas en las que la partición admin de esta instancia tiene tres configuraciones guardadas diferentes:



Ver la plantilla frente a la diferencia de ejecución

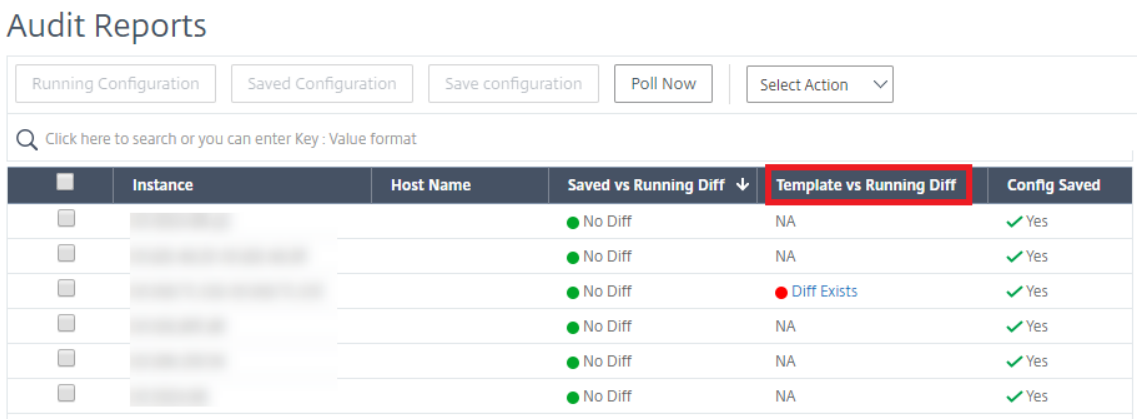
Las plantillas de auditoría para partición le permiten crear una plantilla de configuración personalizada y asociarla a una instancia de partición. Cualquier variación en la configuración en ejecución de la instancia con la plantilla de auditoría se muestra en la columna "**Plantilla frente a Ejecutar 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 diferencia se muestra como un hipervínculo. Haga clic en el hipervínculo para ver las diferencias si las hay. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. También puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.



Para 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 Citrix ADC

November 16, 2022

Puede realizar una copia de seguridad del estado actual de una instancia de Citrix Application Delivery Controller (Citrix ADC) y posteriormente utilizar los archivos de copia de seguridad para restaurar la instancia de Citrix ADC 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 Citrix ADC. Puede realizar copias de seguridad y restaurar manualmente las configuraciones de Citrix ADC mediante la GUI o la CLI, o puede usar Citrix ADM para realizar copias de seguridad automáticas y restauraciones manuales. Citrix ADM realiza una copia de seguridad del estado actual de las instancias de Citrix ADC administradas mediante llamadas NITRO y los protocolos Secure Shell (SSH) y Secure Copy (SCP).

Citrix ADM crea una copia de seguridad completa y restaura los siguientes tipos de instancias de Citrix ADC:

- Citrix ADC SDX
- Citrix ADC VPX
- Citrix ADC MPX
- Citrix ADC BLX

Para obtener más información, consulte Realizar copias de seguridad y restaurar una instancia de ADC.

> **Nota**
>
> - Desde Citrix ADM, no puede realizar la operación de copia de seguridad y restauración en un clúster de Citrix ADC.
> - No puede usar el archivo de copia de seguridad tomado de una instancia para restaurar una instancia diferente.

Los archivos de copia de seguridad se almacenan como un archivo TAR comprimido en el siguiente directorio:


```
/var/mps/tenants/root/tenants/<specify-the-tenant-name>/device_backup/

<!--NeedCopy-->
```

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 Citrix ADC, primero debe configurar las opciones de copia de seguridad en Citrix ADM. Después de configurar los parámetros, puede seleccionar una sola instancia de Citrix ADC o varias instancias y crear una copia de seguridad de los archivos de configuración en estas instancias. Si es necesario, también puede restaurar las instancias de Citrix ADC utilizando estos archivos de copia de seguridad.

Crear una copia de seguridad para una instancia de Citrix ADC seleccionada mediante Citrix ADM

Realice esta tarea si quiere realizar una copia de seguridad de una instancia de Citrix ADC seleccionada o de varias instancias:

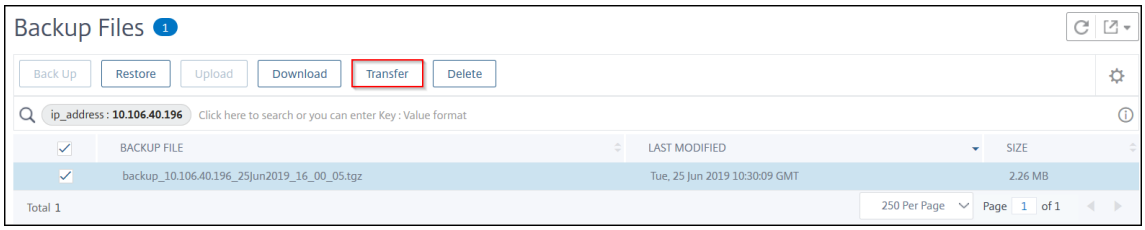
1. En Citrix ADM, vaya a **Infraestructura > Instancias**. En **Instancias**, seleccione el tipo de instancias (por ejemplo, VPX) que se mostrarán en la pantalla.
2. Seleccione la instancia de la que quiere realizar una copia de seguridad.
   - Para las instancias de MPX, VPX y BLX, seleccione **Respaldar/Restaurar** en la lista **Seleccionar acción** .
   - Para una instancia SDX, haga clic en **Copia de seguridad/restauración**.
3. En la página **Archivos de respaldo**, 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 **Continue**.

Transferir un archivo de respaldo a un sistema externo

Puede transferir una copia del archivo de respaldo a otro sistema como medida de precaución. Cuando quiera restaurar la configuración, primero debe cargar el archivo de copia de seguridad en el servidor Citrix ADM y, a continuación, realizar la operación de restauración.

Para transferir un archivo de respaldo de Citrix ADM:

1. Vaya a **Infraestructura > Instances > Citrix ADC** 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 respaldo.

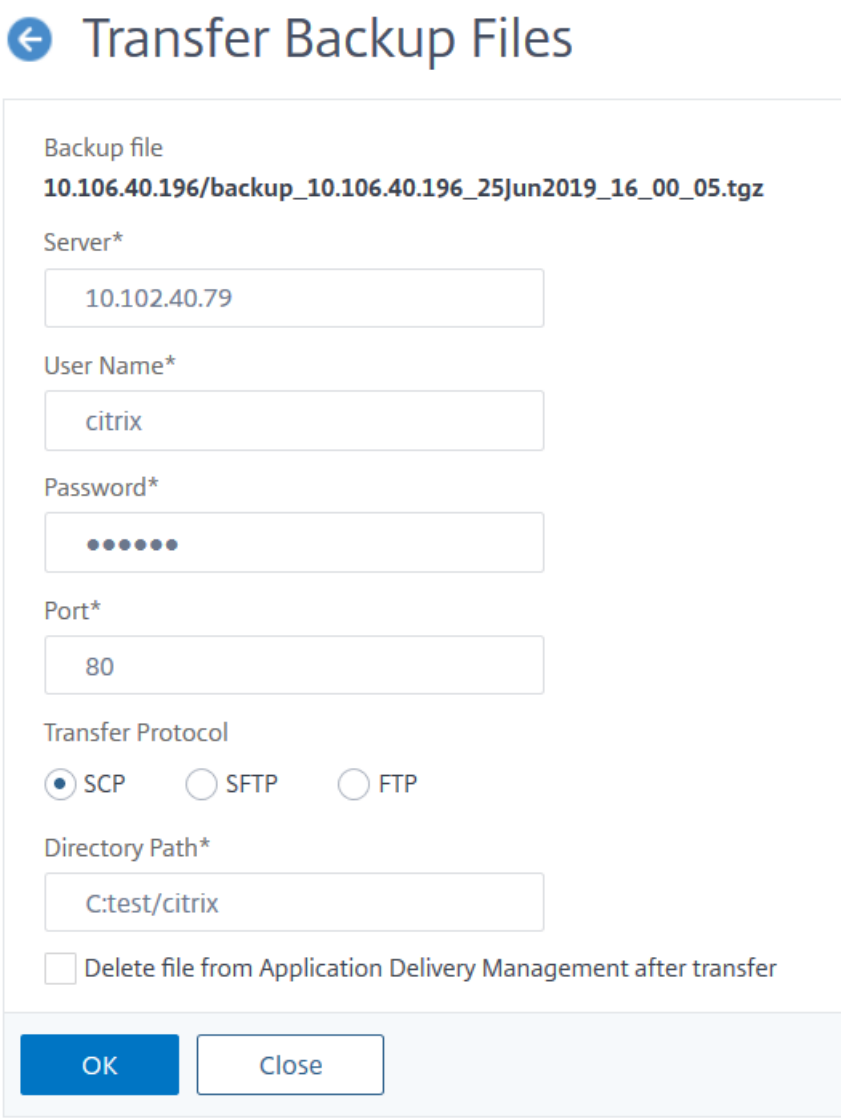
b) **Nombre de usuario** y **contraseña** : credenciales de usuario del nuevo sistema, en el que se copian los archivos de la copia de seguridad.

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 respaldo. Puede seleccionar los protocolos SCP, SFTP o FTP para transferir el archivo de respaldo.

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**.



Restaurar una instancia de Citrix ADC con Citrix ADM

Nota:

Si tiene instancias de Citrix ADC en un par HA, debe tener en cuenta lo siguiente:

- Restaure la misma instancia desde la que se creó el archivo de copia de seguridad. Por ejemplo, consideremos un caso en el que se tomó una copia de seguridad de la instancia principal del par HA. Durante el proceso de restauración, asegúrese de restaurar la misma instancia, aunque ya no sea la instancia principal.
- Al iniciar el proceso de restauración en la instancia de ADC principal, no puede acceder a la instancia principal y la instancia secundaria se cambia a **STAYSECONDARY**. Una vez que se completa el proceso de restauración en la instancia principal, la instancia de ADC

> secundaria pasa del modo **STAYSECONDARYal** modo ENABLED y vuelve a formar parte del par HA. Puede esperar un posible tiempo de inactividad en la instancia principal hasta que se complete el proceso de restauración.

Realice esta tarea para restaurar una instancia de Citrix ADC mediante el archivo de copia de seguridad que había creado 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 contenga la configuración que quiere restaurar y, a continuación, haga clic en **Restaurar**.

Restaurar un dispositivo Citrix ADC SDX con Citrix ADM

En Citrix ADM, la copia de seguridad de un dispositivo Citrix ADC SDX incluye lo siguiente:

- Instancias de Citrix ADC alojadas en el dispositivo
- Certificados y claves SSL SVM
- Configuración de poda de instancias (en formato XML)
- Configuración de copia de seguridad de instancias (en formato XML)
- Configuración del sondeo de certificados SSL (en formato XML)
- Archivo SVM db
- Archivos de configuración Citrix ADC de los dispositivos presentes en SDX
- Imágenes de creación de Citrix ADC
- Imágenes de Citrix ADC XVA, estas imágenes se almacenan en la siguiente ubicación: `/var/mps/sdx_images/`
- Imagen de paquete único de SDX (SVM+XS)
- Imágenes de instancias de terceros (si se aprovisionan)

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

Si está restaurando el dispositivo Citrix ADC SDX mediante una copia de seguridad de otro dispositivo Citrix ADC SDX, asegúrese de agregar las licencias y configurar la configuración de red del servicio de administración del dispositivo para que coincida con la del archivo de copia de seguridad antes de iniciar el proceso de restauración.

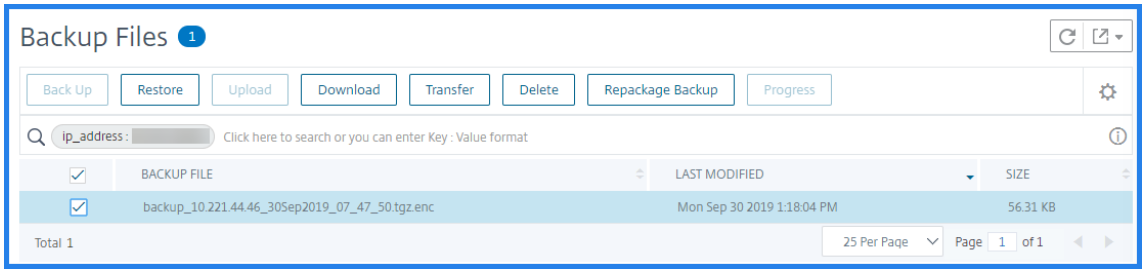
Asegúrese de que se tomó la variante de la plataforma Citrix ADC SDX de la que se realizó una copia de seguridad es la misma en la que intenta restaurar. No se puede restaurar desde una variante de plataforma diferente.

> **Nota**
>
> Antes de restaurar el dispositivo SDX RMA, asegúrese de que la versión de copia de seguridad es

> la misma o superior a la versión de RMA.

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

1. En la GUI de Citrix ADM, vaya a **Infraestructura > Instancias > Citrix ADC**.
2. Haga clic en **Copia de seguridad/restauración**.
3. Selecciona el archivo de copia de seguridad de la misma instancia que deseas restaurar.
4. Haga clic en **Reempaquetar respaldo**.



   Cuando se realiza una copia de seguridad del dispositivo SDX, los archivos e imágenes XVA se almacenan por separado para ahorrar el ancho de banda de la red y el espacio en disco. Por lo tanto, debe volver a empaquetar el archivo de la copia de seguridad antes de restaurar el dispositivo SDX.

   Al volver a empaquetar el archivo de copia de seguridad, incluye todos los archivos de la copia de seguridad juntos para restaurar el dispositivo SDX. El archivo de copia de seguridad reempaquetado garantiza la restauración correcta del dispositivo SDX.

5. Seleccione el archivo de copia de seguridad que se ha reempaquetado y haga clic en **Restaurar**.

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 Citrix ADC

November 16, 2022

Es posible que quiera forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar la instancia principal de Citrix Application Delivery Controller (Citrix ADC). Puede forzar la conmutación por error desde la instancia principal o la instancia secundaria. Cuando se fuerza una conmutación por error en la instancia principal, la instancia principal se convierte en la secundaria y la secundaria en la principal. La conmutación por error forzada solo es posible cuando la instancia principal puede determinar que la instancia secundaria está activa.

Una conmutación por error forzada no se propaga ni sincroniza. Para ver el estado de la sincronización tras una conmutación por error forzada, puede ver el estado de la instancia.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

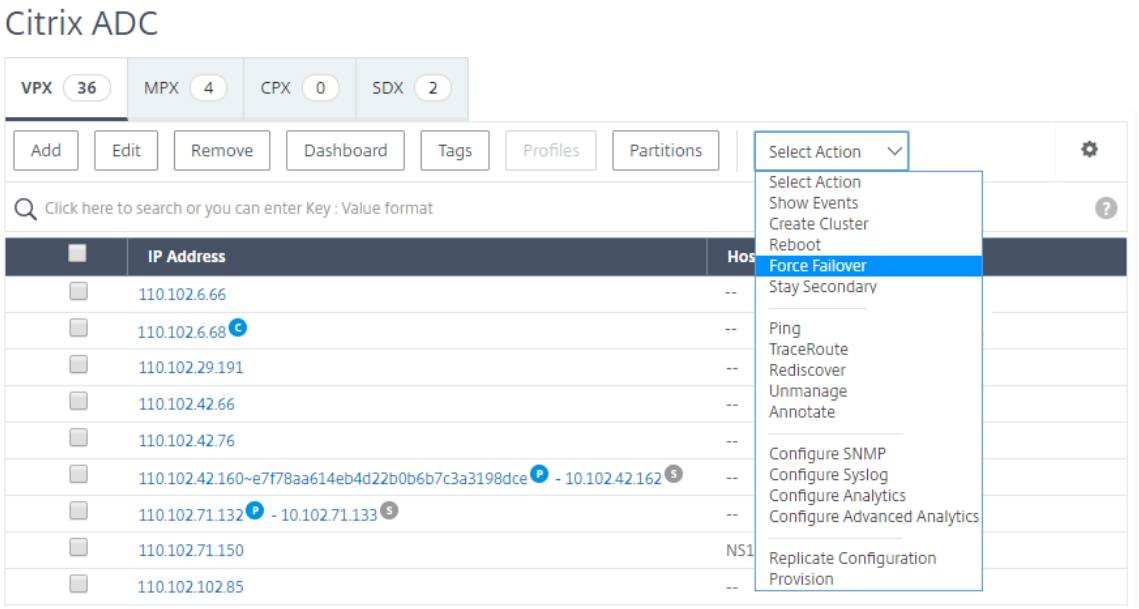
- Se fuerza la conmutación por error en un sistema independiente.
- La instancia secundaria está deshabilitada o inactiva. Si la instancia secundaria se encuentra en un estado inactivo, debe esperar a que su estado sea ACTIVO para forzar una conmutación por error.
- La instancia secundaria está configurada para permanecer secundaria.

La instancia de Citrix ADC muestra un mensaje de advertencia si detecta un posible problema al ejecutar el comando force failover. El mensaje incluye la información que activó la advertencia y solicita confirmación antes de continuar.

Puede forzar una conmutación por error en una instancia principal o secundaria.

Para forzar una conmutación por error a la instancia secundaria de Citrix ADC mediante Citrix ADM:

1. En Citrix ADM, 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 Citrix ADC para que permanezca secundaria

November 16, 2022

En una configuración de alta disponibilidad (HA), el nodo secundario puede ser forzado a permanecer secundario independientemente del estado del nodo principal.

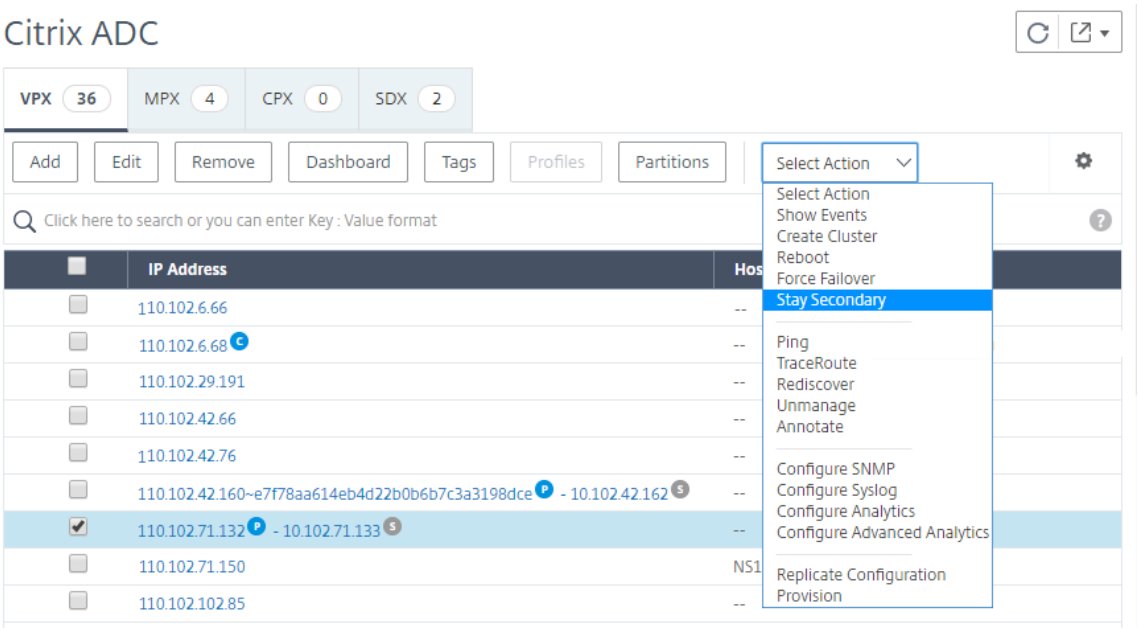
Por ejemplo, supongamos que el nodo principal necesita ser actualizado y el proceso tarda unos segundos. Durante la actualización, es posible que el nodo principal desaparezca durante unos segundos, pero no quiere que el nodo secundario tome el control y quiere que siga siendo el nodo secundario incluso 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 Citrix ADC para que permanezca secundaria mediante Citrix ADM:

1. En Citrix ADM, 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

November 16, 2022

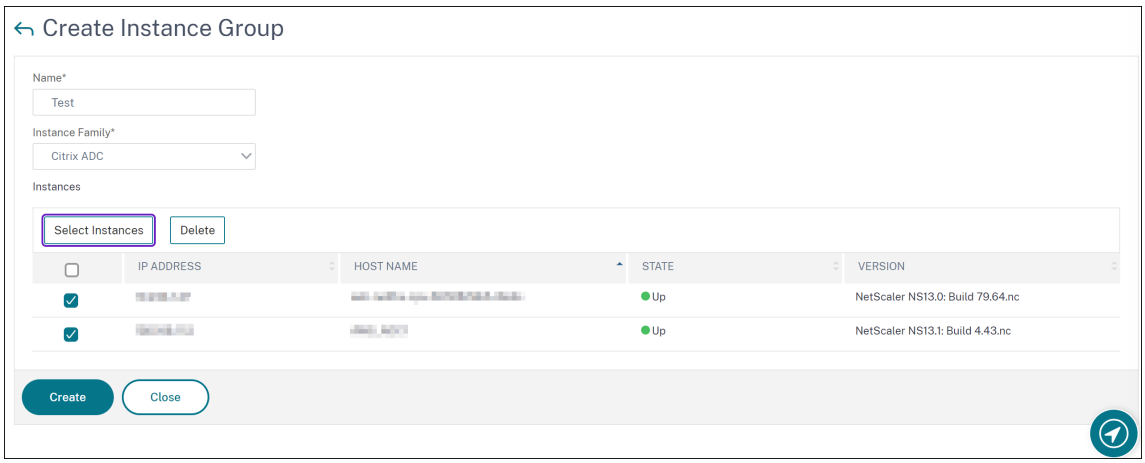
Para crear un grupo de instancias, primero debe agregar todas las instancias de Citrix ADC a Citrix ADM. Una vez que hayas agregado las instancias correctamente, crea grupos de instancias según su familia de instancias. La creación de un grupo de instancias le ayuda a actualizar, hacer copias de seguridad o restaurar las instancias agrupadas al mismo tiempo.

Para crear un grupo de instancias con Citrix ADM

1. En Citrix ADM, 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 **Citrix ADC** 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 quiere eliminar cualquier instancia del grupo, selecciónela en la tabla y haga clic en **Eliminar**.
5. Haga clic en **Crear**.



Grupos de sitios de equilibrio de carga de servidores

November 16, 2022

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 Citrix ADM, 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.

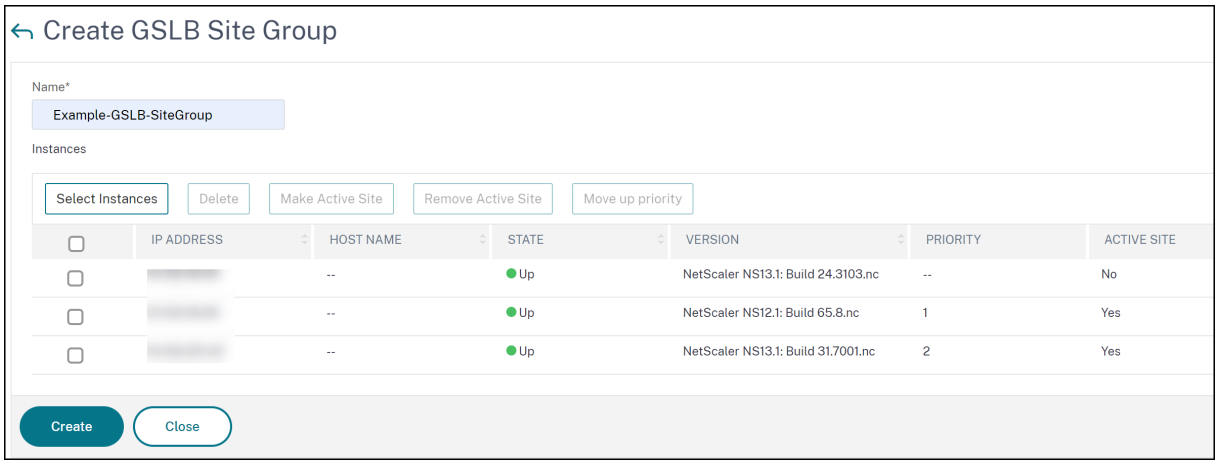
Puede ver sus grupos de sitios GSLB en **Infraestructura > Instancias > Grupo de sitios GSLB**.

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.

Aprovisiona instancias de ADC VPX en SDX

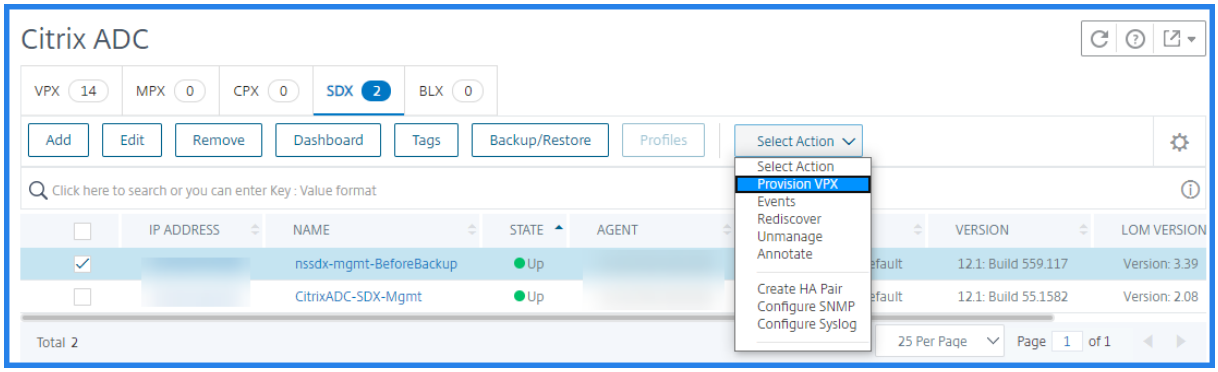
November 16, 2022

Puede aprovisionar una o más instancias de ADC VPX en el dispositivo SDX mediante Citrix ADM. El número de instancias que puede implementar depende de la licencia que haya adquirido. Si el número de instancias agregadas es igual al número especificado en la licencia, el Citrix ADM no le permite aprovisionar más instancias de Citrix ADC.

Antes de empezar, asegúrese de agregar una instancia SDX en Citrix ADM donde quiera aprovisionar las instancias VPX.

Para aprovisionar una instancia VPX, haga lo siguiente:

1. Vaya a**Infraestructura > Instancias > Citrix ADC**.
2. En la ficha **SDX**, seleccione una instancia SDX en la que quiera aprovisionar una instancia VPX.
3. En **Seleccionar acción**, seleccione **Aprovisionar VPX**.



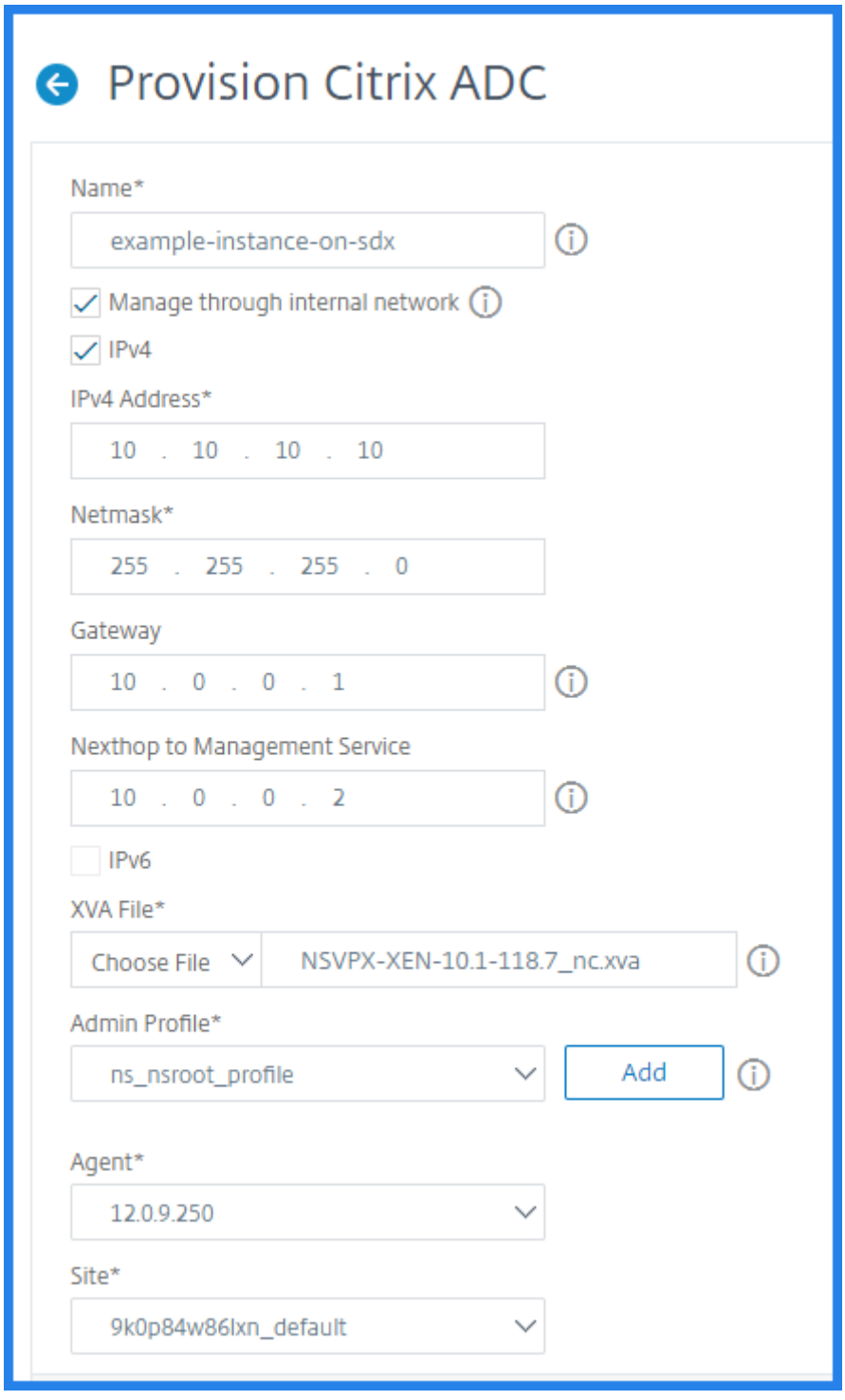
Paso 1: Agregar una instancia VPX

El Citrix ADM utiliza la siguiente información para configurar las instancias VPX en un dispositivo SDX:

- **Nombre** : especifique un nombre para una instancia de ADC.
- Establezca una red de comunicación entre SDX y VPX. Para ello, seleccione las opciones necesarias de la lista:
  - **Administrar a través de la red interna** : esta opción establece una red interna para la comunicación entre el Citrix ADM y una instancia VPX.
  - **Dirección IP** : puede seleccionar una dirección **IPv4** o **IPv6** o ambas para administrar la instancia de Citrix VPX. Una instancia VPX solo puede tener una IP de administración (también denominada IP de Citrix ADC). No puede quitar la dirección IP de Citrix ADC.

    Para la opción seleccionada, asigne una máscara de red, una puerta de enlace predeterminada y el siguiente salto al Citrix ADM para la dirección IP.
- **Archivo XVA**: Seleccione el archivo XVA desde el que quiere aprovisionar una instancia VPX. Utilice una de las siguientes opciones para seleccionar el archivo XVA.
  - **Local** : seleccione el archivo XVA de su equipo local.
  - **Dispositivo** : seleccione el archivo XVA en un explorador de archivos Citrix ADM.
- **Perfil de administrador** : este perfil proporciona acceso para aprovisionar instancias VPX. Con este perfil, Citrix ADM recupera los datos de configuración de una instancia. Si tiene que agregar un perfil, haga clic en **Agregar**.

- **Agente**: Seleccione el agente al que quiere asociar las instancias
- **Sitio**: Seleccione el sitio donde quiere agregar la instancia.



Paso 2: Asignar licencias

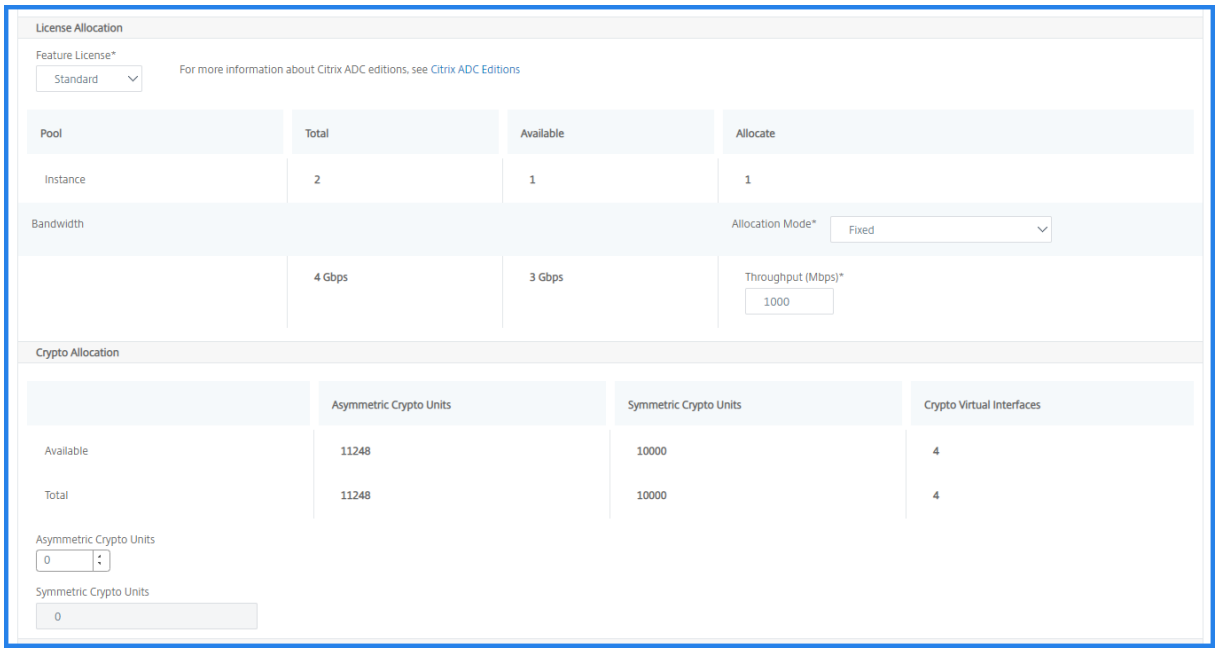
En la sección **Asignación de licencias**, especifique la licencia VPX. Puede utilizar las licencias Standard, Advanced y Premium.

- **Modo de asignación** : puede elegir los modos **fijo** o de **ráfaga** para el conjunto de ancho de banda.

  Si elige el modo **Burstable**, puede usar ancho de banda adicional cuando se alcanza el ancho de banda fijo.

- **Rendimiento** : asigne el rendimiento total (en Mbps) a una instancia.

> **Nota**
>
> Compre una licencia independiente (SDX 2-Instance Add-On Pack para Secure Web Gateway) para instancias de Citrix Secure Web Gateway (SWG) en dispositivos SDX. Este paquete de instancias es diferente de la licencia de plataforma SDX o del paquete de instancias SDX.
>
> Para obtener más información, consulte Implementación de una instancia de Citrix Secure Web Gateway en un dispositivo SDX.



A partir de la versión 12.0 57.19 de SDX, la interfaz para administrar la capacidad de cifrado ha cambiado. Para obtener más información, consulte Administrar la capacidad de cifrado.

Paso 3: Asignar recursos

En la sección **Asignación de recursos**, asigne recursos a una instancia VPX para mantener el tráfico.

- **Memoria total (MB)** : asigna la memoria total a una instancia. El valor mínimo es `2048` MB.

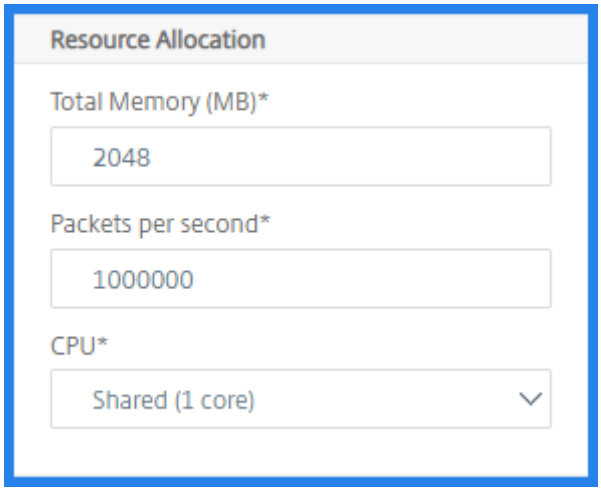
- **Paquetes por segundo** : especifique la cantidad de paquetes que se van a transmitir por segundo.
- **CPU** : especifique el número de núcleos de CPU de una instancia. Puede utilizar núcleos de CPU compartidos o dedicados.

  Cuando selecciona un núcleo compartido para una instancia, las demás instancias pueden utilizar el núcleo compartido en el momento de escasez de recursos.

  Reinicie instancias en las que se reasignan núcleos de CPU para evitar cualquier degradación del rendimiento.

  Si utiliza la plataforma SDX 25000xx, puede asignar un máximo de 16 núcleos a una instancia. Además, si utiliza la plataforma SDX 2500xxx, puede asignar un máximo de 11 núcleos a una instancia.

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



Consulte la tabla de Aprovisionar instancias de Citrix ADC que muestra el VPX compatible, la versión de imagen de un solo paquete y la cantidad de núcleos que puede asignar a una instancia.

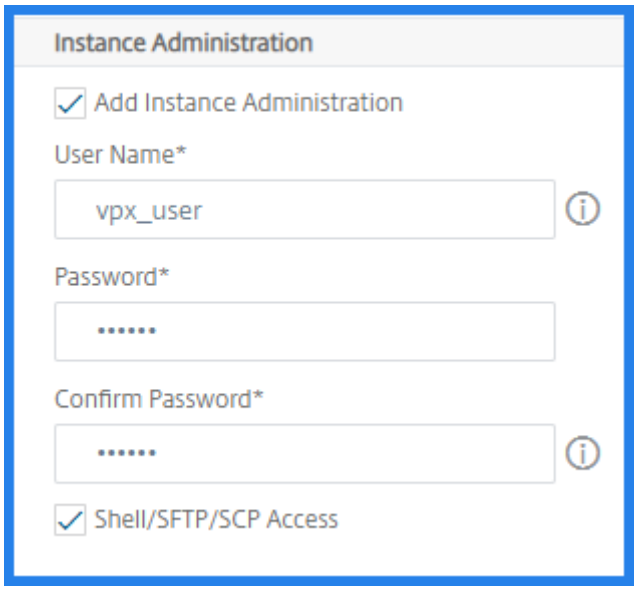
Paso 4: Agregar la administración de instancias

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 Citrix ADC. 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 Citrix ADC. Esta opción está seleccionada de forma predeterminada.



Paso 5: Especificar la configuración de red

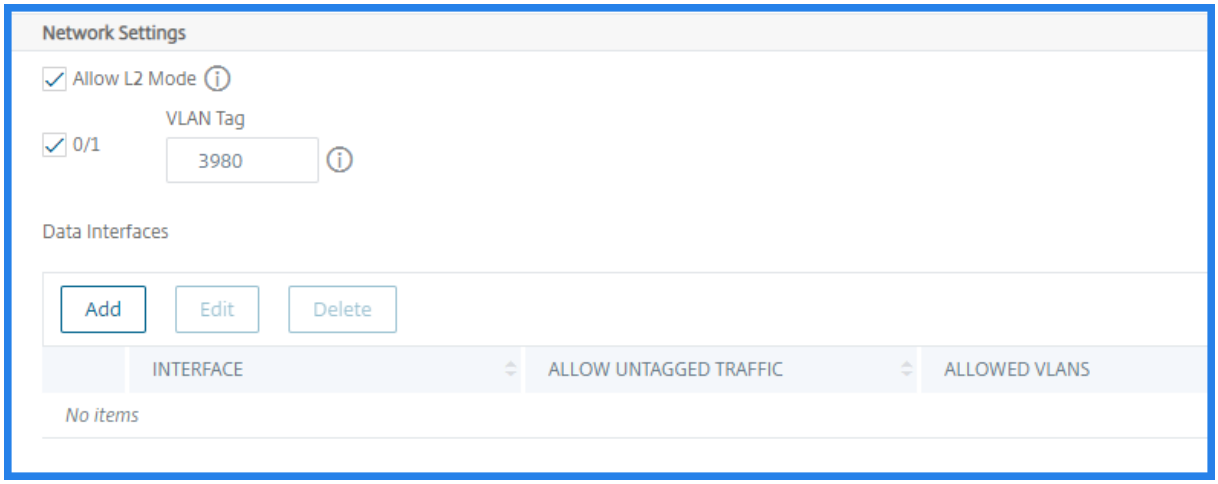
Seleccione la configuración de red requerida para una instancia:

- **Permitir el modo L2 en la configuración de red** : puede permitir el modo L2 en la instancia de Citrix ADC. Seleccione Permitir modo L2 en Configuración de red. Antes de iniciar sesión en la instancia y habilitar el modo L2. Para obtener más información, consulte Permitir el modo L2 en una instancia de Citrix ADC.

  > **Nota**
  >
  > Si inhabilita el modo L2 para una instancia, 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 Citrix ADC 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 **0/1y 0/2** .

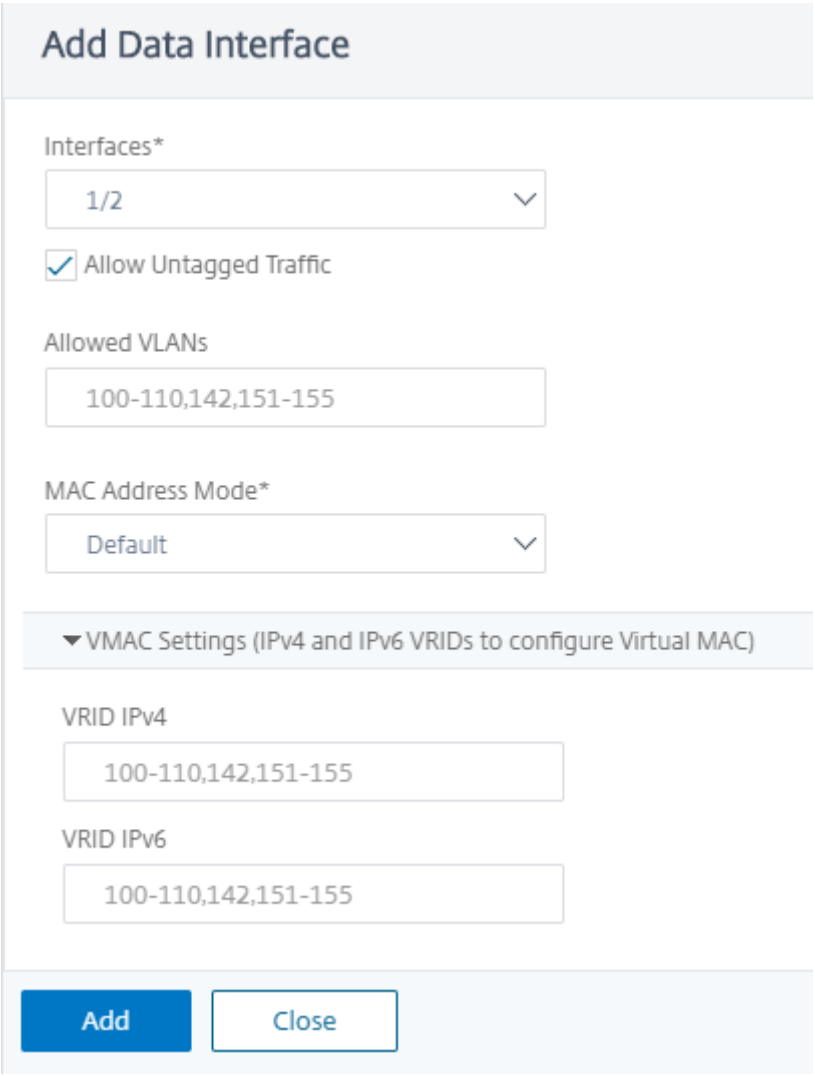


En **Interfaces de datos**, haga clic en **Agregar** para agregar interfaces de datos y especifique lo siguiente:

- **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 Citrix ADC.
- **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.

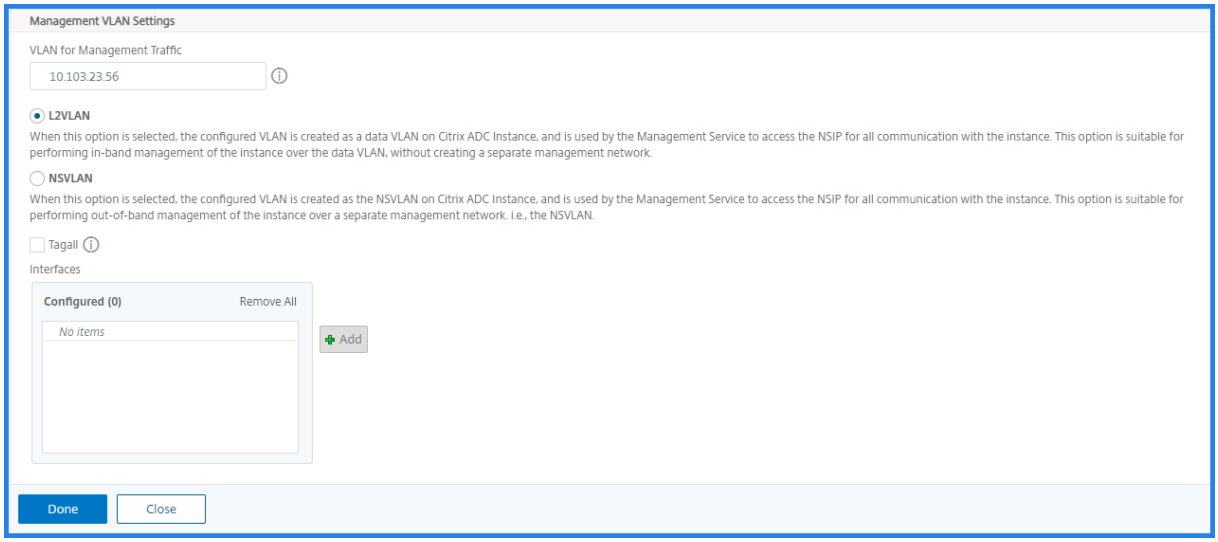
Si el Servicio de administración y la instancia se encuentran en subredes diferentes, especifique un ID de VLAN mientras aprovisione una instancia VPX. Por lo tanto, la instancia es accesible a través de la red cuando está activa.

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**.

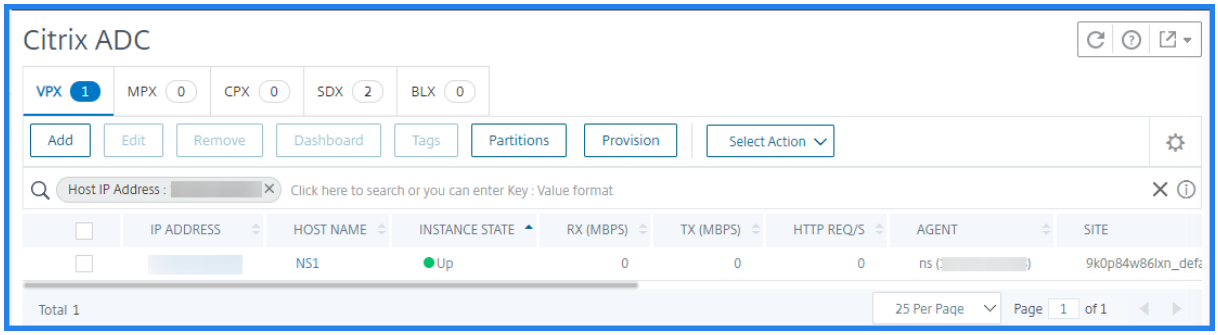


Haga clic en **Listo** para aprovisionar una instancia VPX.

Ver la instancia VPX aprovisionada

Para ver la instancia recién aprovisionada, haga lo siguiente:

1. Vaya a**Infraestructura > Instancias > Citrix ADC**.
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.



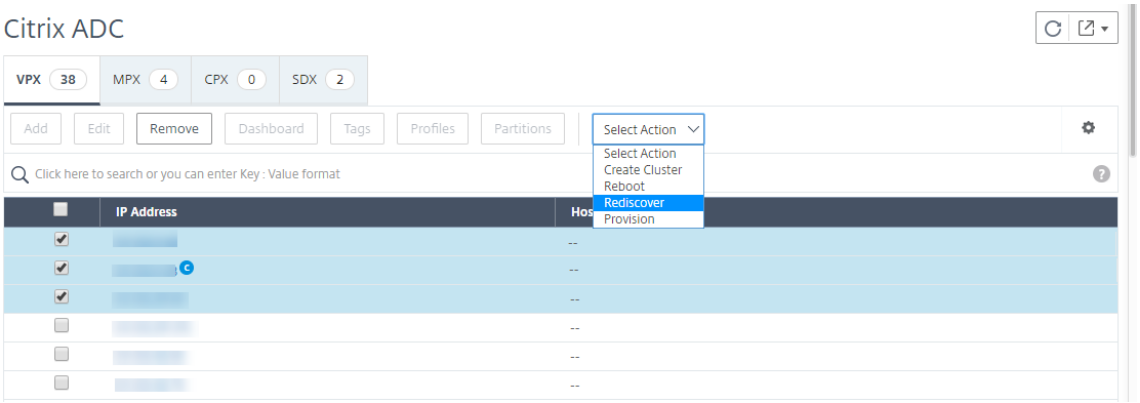
Redescubra varias instancias de Citrix ADC

November 16, 2022

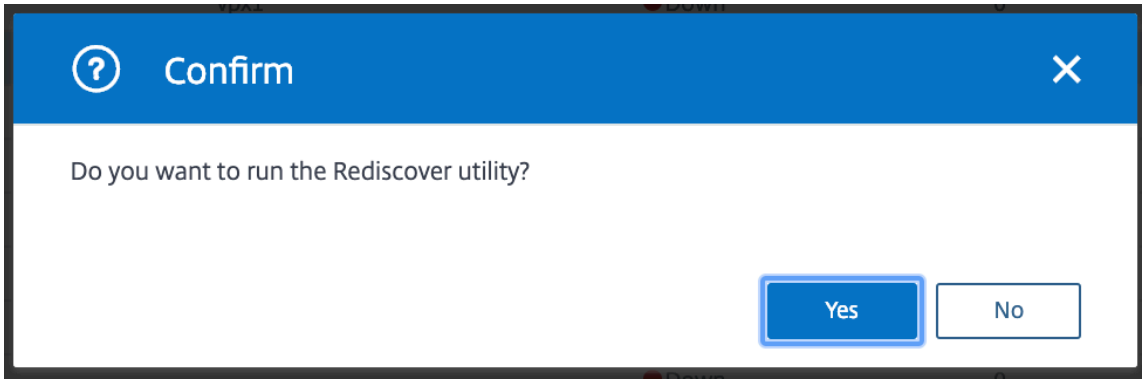
Puede volver a descubrir varias instancias de Citrix Application Delivery Controller (Citrix ADC) (VPX, MPX, SDX, BLX y CPX) en su configuración de Citrix ADM. Tras volver a descubrir las instancias, podrá ver los estados y configuraciones más recientes de esas instancias. El servidor Citrix ADM vuelve a descubrir todas las instancias de ADC y comprueba si se puede acceder a las instancias.

Para volver a descubrir varias instancias de Citrix ADC VPX:

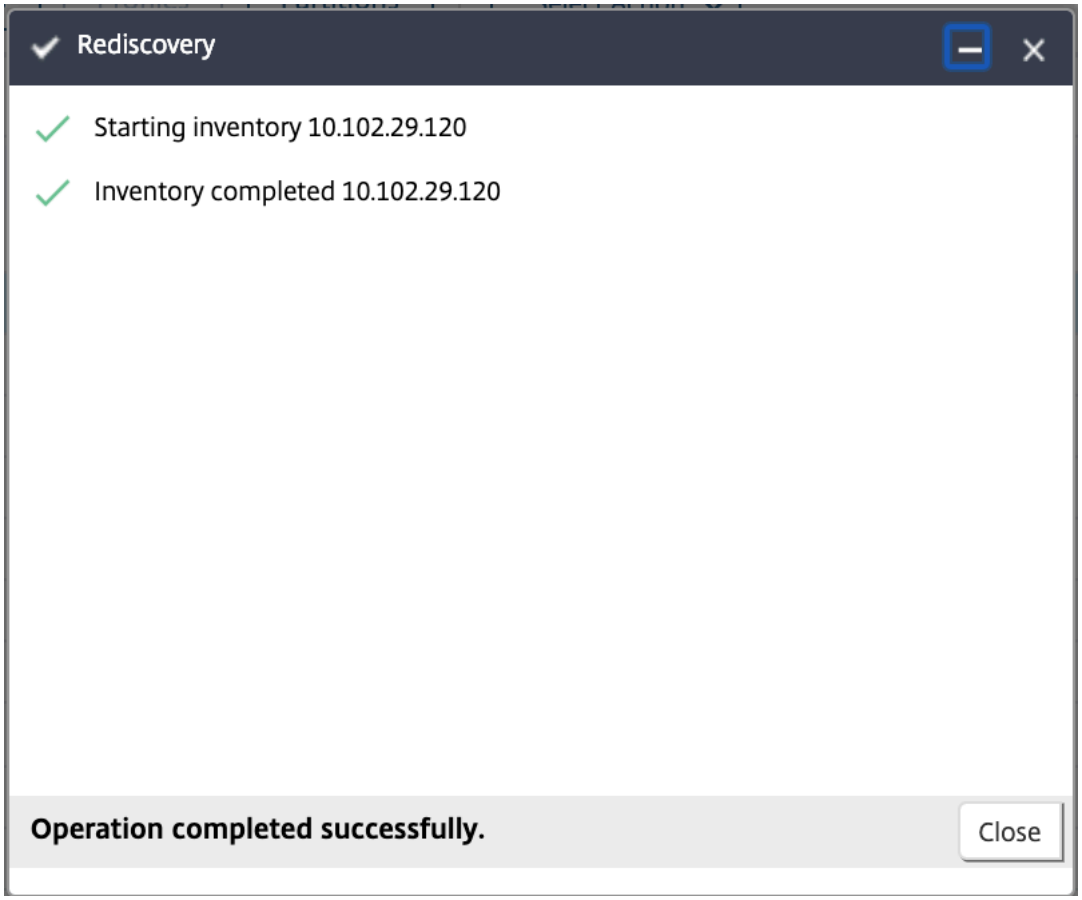
1. Vaya a**Infraestructura > Instancias > Citrix ADC**. Selecciona la ficha de instancias (VPX, MPX, SDX, BLX y CPX) y selecciona las instancias que deseas redescubrir.
2. En el cuadro **Acción**, haga clic en **Redescubrir**. Las siguientes capturas de pantalla muestran cómo redescubrir varias instancias 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 de ADC.



Visión general de sondeo

November 16, 2022

El sondeo es un proceso en el que Citrix ADM recopila cierta información de las instancias de Citrix ADC. Es posible que haya configurado varias instancias de Citrix ADC para su organización en todo el mundo. Para supervisar sus instancias a través de Citrix ADM, Citrix ADM tiene que recopilar cierta información, como el uso de CPU, el uso de memoria, los certificados SSL, las características con licencia y los tipos de licencia de todas las instancias de ADC administradas. Los siguientes son los diferentes tipos de sondeo que se producen entre Citrix ADM y las instancias administradas:

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

- Sondeo de certificados SSL
- Sondeo de entidades

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

Cómo Citrix ADM sondea las instancias y entidades administradas

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

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

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

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
Encuesta de respaldo de instancias	Cada 12 horas (por defecto)	El archivo de copia de seguridad del estado actual de las instancias ADC administradas	Llamadas NITRO, SSH y SCP.	Sí. Vaya a**Infraestructura > Instancias > Citrix ADC**. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Copia de seguridad/restauración**.
Encuesta de auditoría de configuración	Cada 10 horas (por defecto)	Cambios de configuración que se producen en las instancias de ADC (por ejemplo, configuración en ejecución o configuración guardada)	Llamada SSH, SCP y NITRO	Sí. Vaya a **Infraestructura > 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 agregar todas las auditorías de configuración de las instancias inmediatamente a Citrix ADM. 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.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
sondeo de certificados SSL	Cada 24 horas (de forma predeterminada)	Certificados SSL que se instalan en las instancias de Citrix ADC.	Llamadas NITRO y SCP	Sí. Vaya a **Infraestructura > Panel de control SSL**. En la página Tablero SSL, haga clic en **Configuración** para configurar el intervalo de sondeo
				Puede sondear los certificados SSL manualmente y agregar todos los certificados de las instancias inmediatamente a Citrix ADM. Para 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 directiva, un servidor virtual, un servicio o una acción asociada a una instancia de ADC. Para habilitar el sondeo de entidades, consulte Habilitar o deshabilitar las funciones de Citrix ADM.	NITRO llama.	Sí, pero no se puede establecer en menos de 10 minutos. Para configurar, vaya a **Infraestructura > Funciones de red**. En la página Función de redes, haga clic en **Configuración** para configurar el intervalo de sondeo.

Tipo de sondeo	Intervalo de sondeos	Información encuestada	Protocolo utilizado	Configuración de intervalos de votación
				Puede sondear entidades manualmente y agregar todas las entidades de las instancias inmediatamente a Citrix ADM. 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, Citrix ADM recibe eventos generados por instancias de ADC administradas a través de capturas SNMP enviadas a las instancias. Por ejemplo, se genera un evento cuando hay un error del sistema o un cambio en la configuración.

Durante la copia de seguridad de la instancia, se descargan en Citrix ADM los archivos SSL, los archivos de certificados de CA, las plantillas de ADC, la información de la base de datos, Durante una auditoría de configuración, los archivos ns.conf se descargan y almacenan en el sistema de archivos. Toda la información recopilada de las instancias administradas de Citrix ADC se almacena internamente en la base de datos.

Diferentes formas de sondear instancias

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

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

Sondeo global de instancias

Citrix ADM sondea automáticamente todas las instancias administradas en la red, dependiendo del intervalo configurado por usted. Aunque el intervalo de sondeo predeterminado es de 60 minutos, puede configurar el intervalo en función de sus requisitos yendo a **Infraestructura > Funciones de red > Configuración**.

Sondeo manual de instancias

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

En Citrix ADM, hay un período mínimo de intervalo de sondeo en el que no se realiza el sondeo automático. Si agrega una nueva instancia de Citrix ADC o si se actualiza una entidad, Citrix ADM no reconoce la nueva instancia ni las actualizaciones realizadas en una entidad hasta que se realice el siguiente sondeo. Además, no hay forma de obtener inmediatamente una lista de direcciones IP virtuales para futuras operaciones. Debe esperar a que transcurra el intervalo mínimo de sondeo. Si bien puede realizar una encuesta manual para descubrir las instancias recién agregadas, esto lleva a que se sondee toda la red Citrix ADC, lo que genera una carga pesada en la red. En lugar de sondear toda la red, Citrix ADM ahora le permite sondear solo instancias y entidades seleccionadas en un momento dado.

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

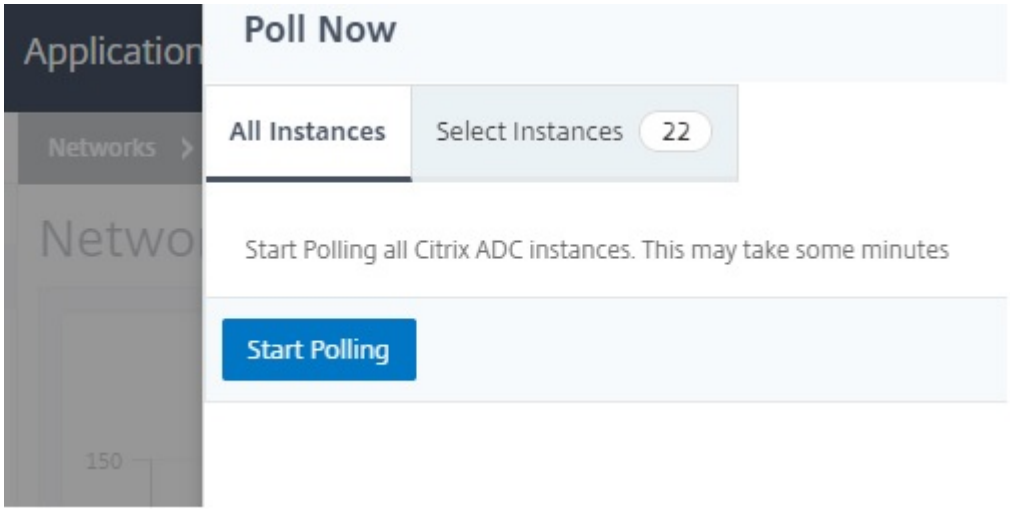
Para sondear instancias específicas en Citrix ADM:

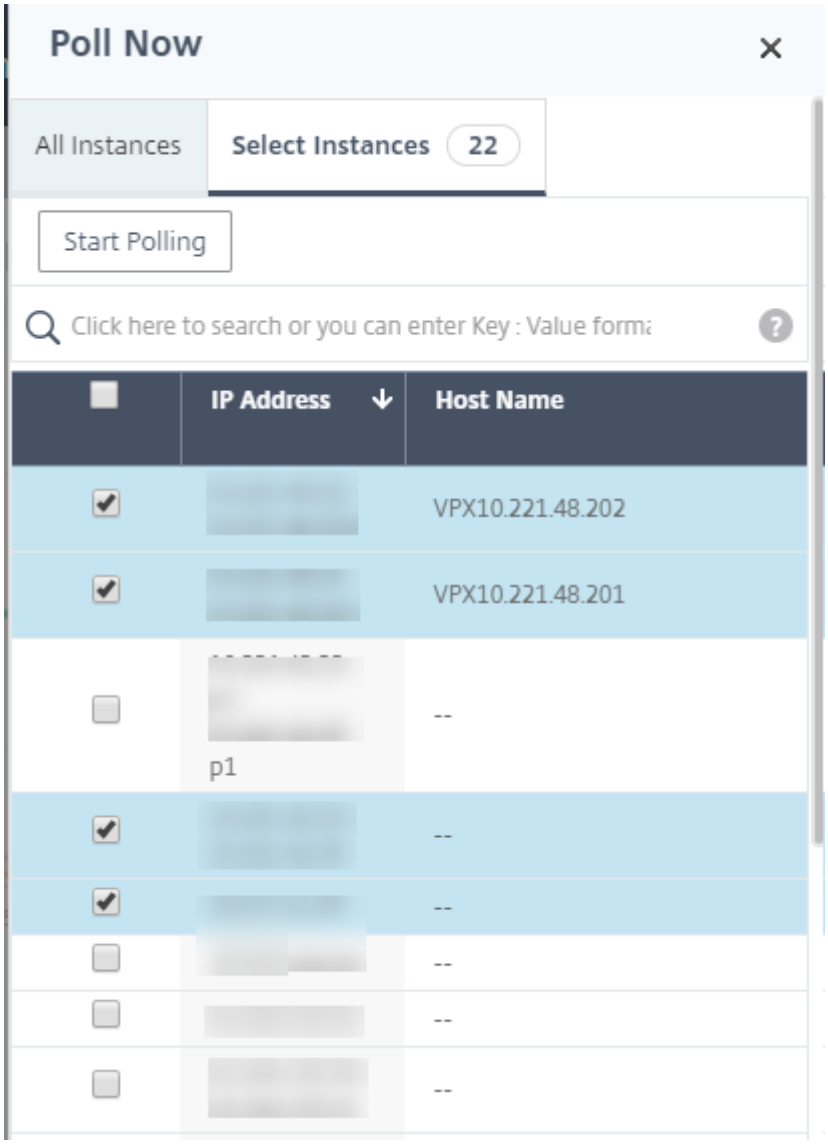
1. En Citrix ADM, vaya a **Infraestructura > Funciones de red**.
2. En la página **Funciones de red**, en la esquina superior derecha, haga clic en **Sondear ahora**.
3. La página emergente **Poll Now** ofrece la opción de sondear todas las instancias de Citrix ADC de la red o sondear las instancias seleccionadas.

a) Ficha**Todas las instancias** : haga clic en **Iniciar sondeo** para sondear todas las instancias.

b) **Seleccione la ficha Instancias** : seleccione las instancias de la lista

4. Haga clic en **Iniciar sondeo**.





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

Encuesta manual de entidades

Citrix ADM también permite sondear sólo 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, Citrix ADM sondea solo esa entidad y actualiza el estado en la GUI de Citrix ADM.

Considere un ejemplo de un servidor virtual que está **INACTIVO**. Es posible que el estado de ese servidor virtual haya cambiado a ACTIVO antes de que **se**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.

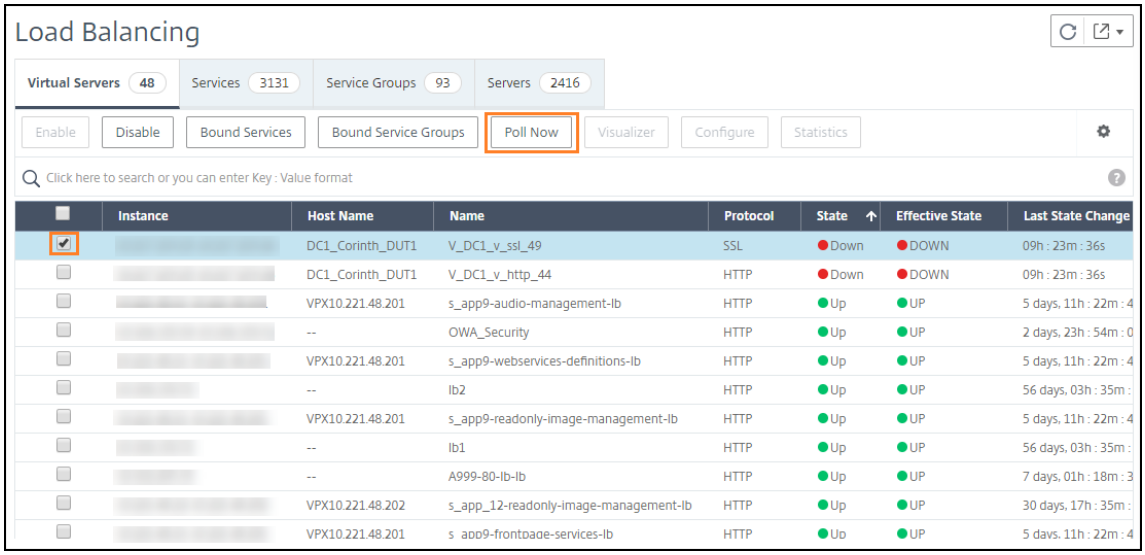
Ahora puede sondear las siguientes entidades para obtener cualquier actualización en su estado, servicios, grupos de servicios, servidores virtuales de equilibrio de carga, servidores virtuales de reducción de caché, servidores virtuales de conmutación de contenido, servidores virtuales de autenticación, 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 Citrix ADM:

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

1. En Citrix ADM, vaya a **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 **UP**.



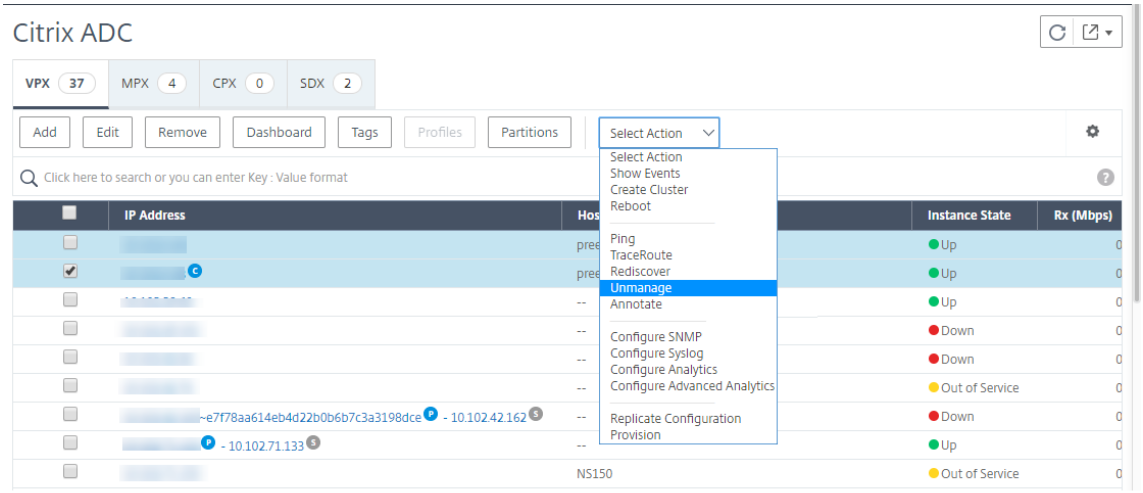
Desadministrar una instancia

November 16, 2022

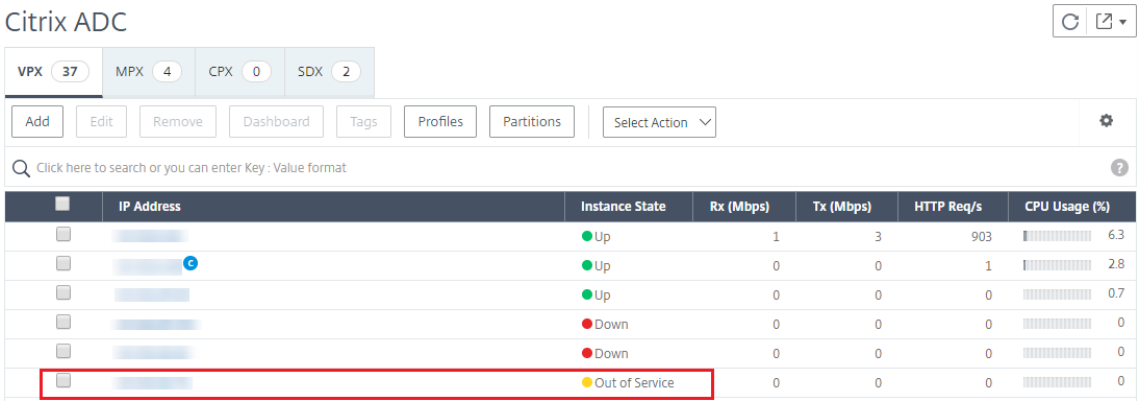
Si quiere detener el intercambio de información entre Citrix ADM y las instancias de su red, puede anular la administración de las instancias.

Para anular la gestión de una instancia:

1. Vaya a**Infraestructura > Instancias > Citrix ADC**.
2. Seleccione la ficha de instancias de ADC (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**.



Citrix ADM ya no administra la instancia y ya no intercambia datos con Citrix ADM.

Rastrear la ruta a una instancia

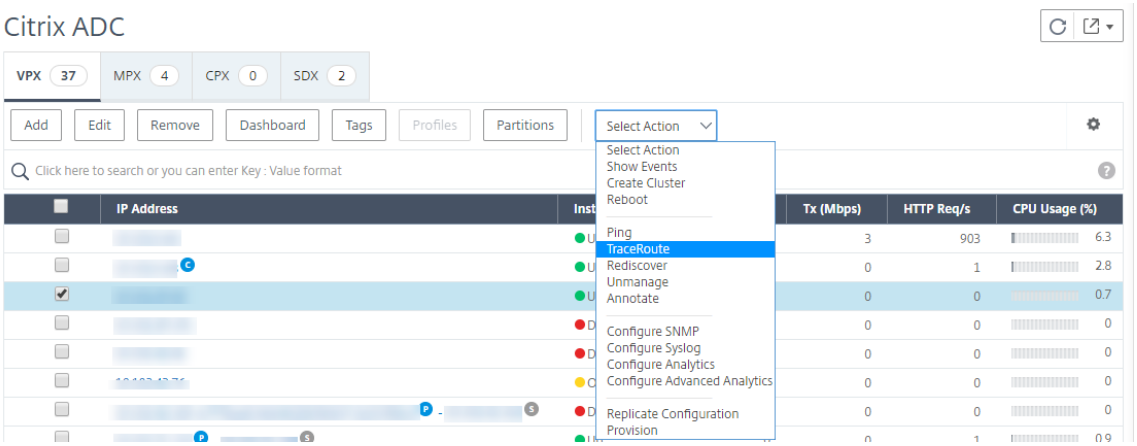
November 16, 2022

Al rastrear la ruta de un paquete desde el Citrix ADM 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.

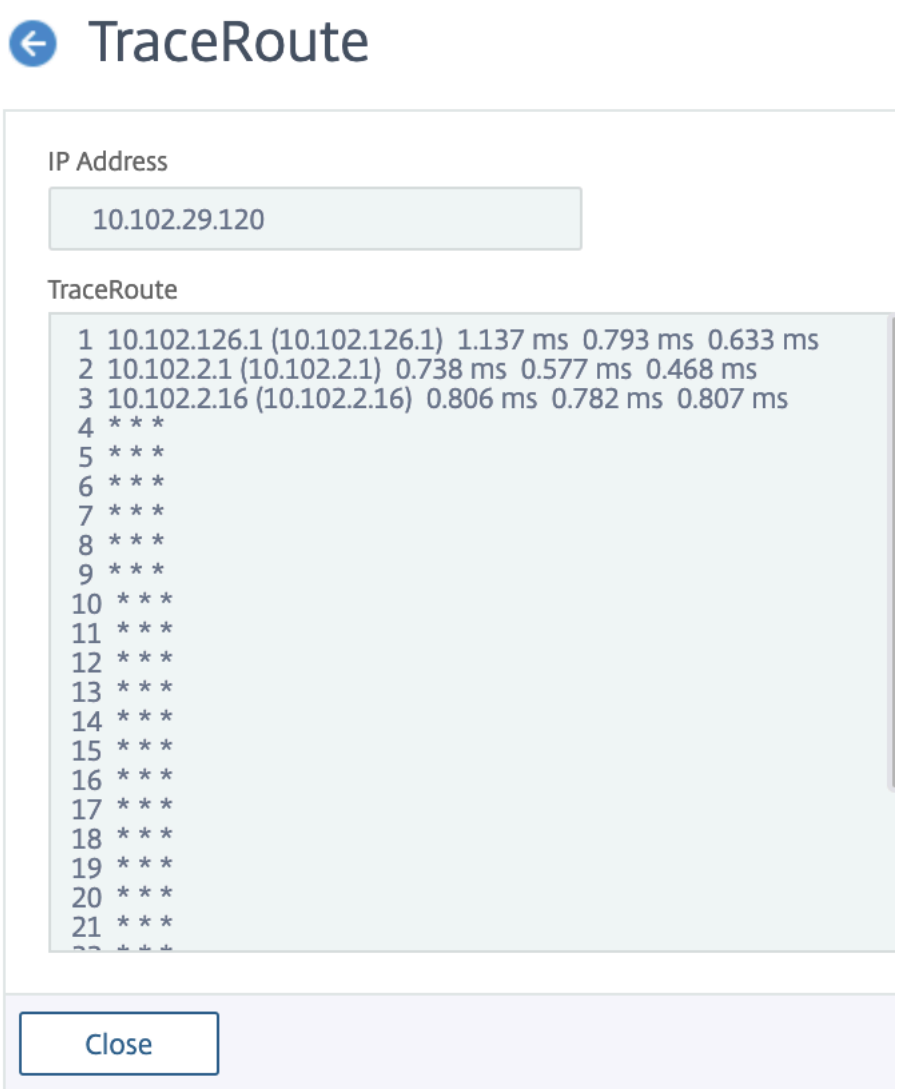
Traceroute también registra el tiempo que tarda un paquete en viajar de un salto a otro. Si hay alguna interrupción en la transferencia de paquetes, el traceroute muestra dónde existe el problema.

Para rastrear la ruta de una instancia:

1. Vaya a**Infraestructura > Instancias > Citrix ADC**.
2. Seleccione la ficha de instancias de ADC (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.



Cómo cambiar la contraseña raíz de Citrix ADC MPX o VPX

November 16, 2022

Ocasionalmente, debe cambiar la contraseña raíz del dispositivo Citrix ADC 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 MPX y VPX de Citrix ADC administrados a través de Citrix ADM cloud.

Si cambia la contraseña del ADC, debe modificar el perfil de administrador de Citrix ADM que está asociado al ADC. Un perfil de administrador de Citrix ADM mantiene las credenciales de ADC para la comunicación basada en la API REST, SSH, SCP o SNMP con el dispositivo ADC. A través de perfiles de administración, Citrix ADM administra los dispositivos Citrix ADC MPX y VPX.

Cambie la contraseña mediante la función Trabajos de configuración

Al utilizar la función Tareas de configuración de Citrix ADM, puede simplificar el proceso repetitivo de cambio de contraseña y aplicar los cambios a los dispositivos Citrix ADC, sin acceder a las instancias individuales.

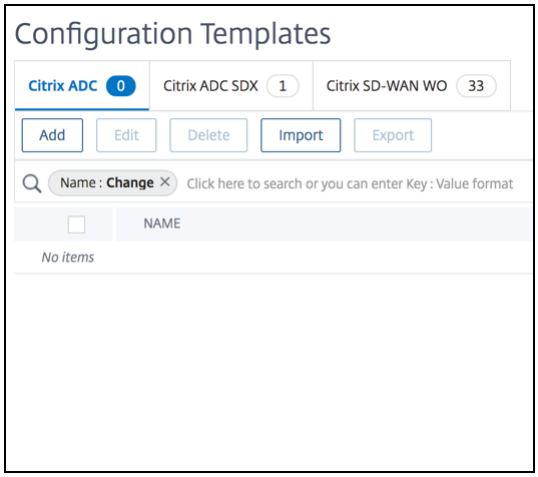
Siga estos pasos para cambiar la contraseña:

- Paso 1. Cree una plantilla de configuración.
- Paso 2. Cree un trabajo de configuración.
- Paso 3. Crea un perfil de administrador y modifícalo.

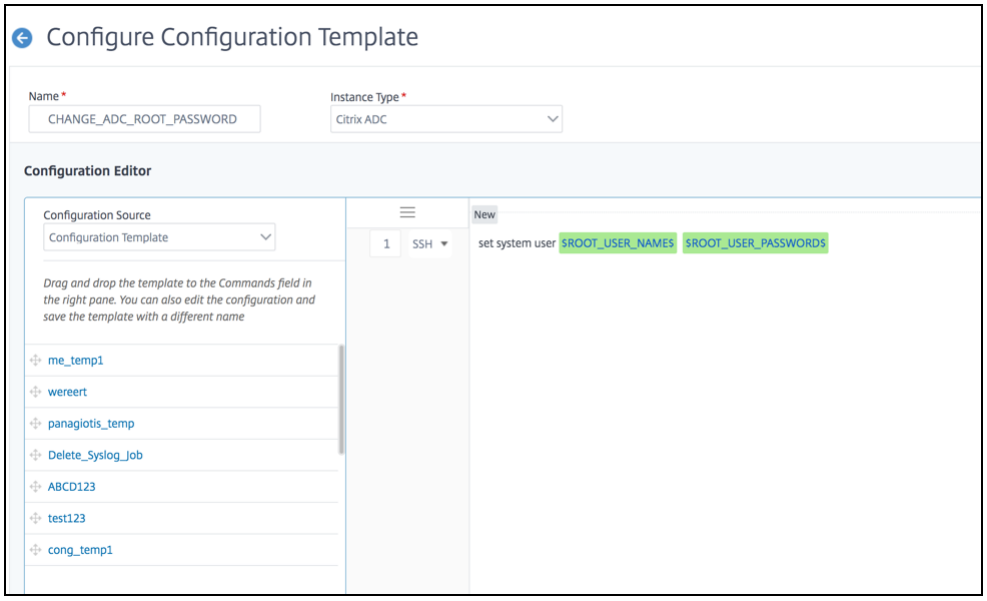
> Nota: Si los dispositivos ADC también están administrados por otras herramientas, también debe cambiar las credenciales de esas herramientas.

Crear una plantilla de configuración

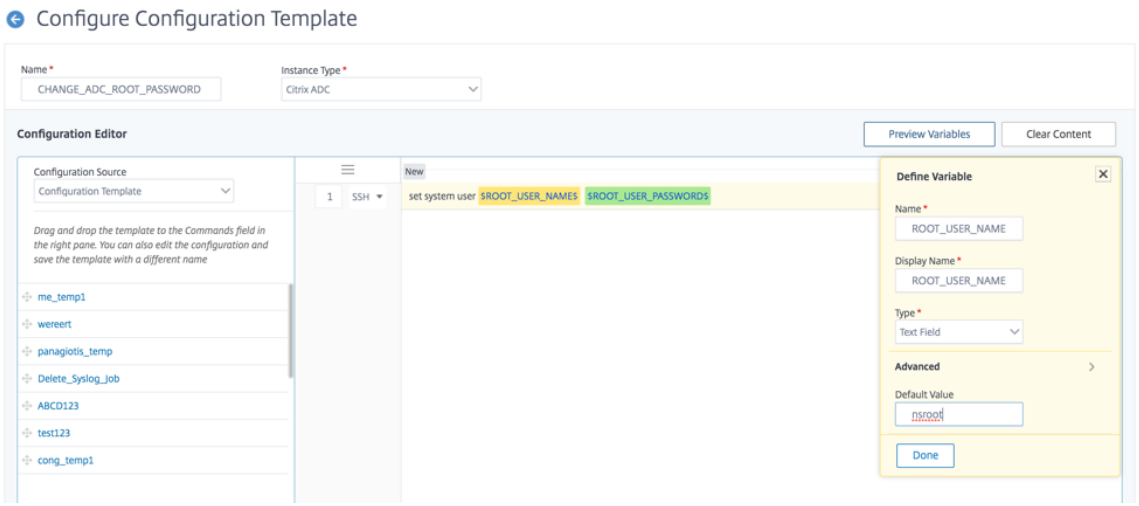
1. Desde la GUI de Citrix ADM, vaya a **Infraestructura > Trabajos de configuración > Plantillas de configuración**.



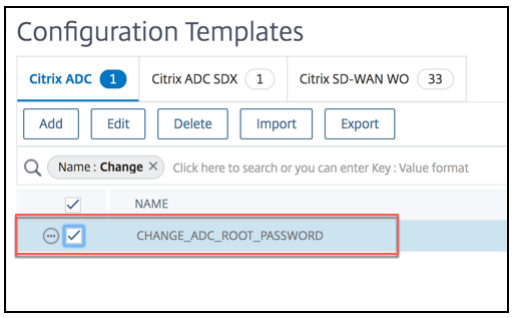
2. Seleccione **Agregar**. Cree una plantilla de configuración con escribiendo el comando SSH `set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`.



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.

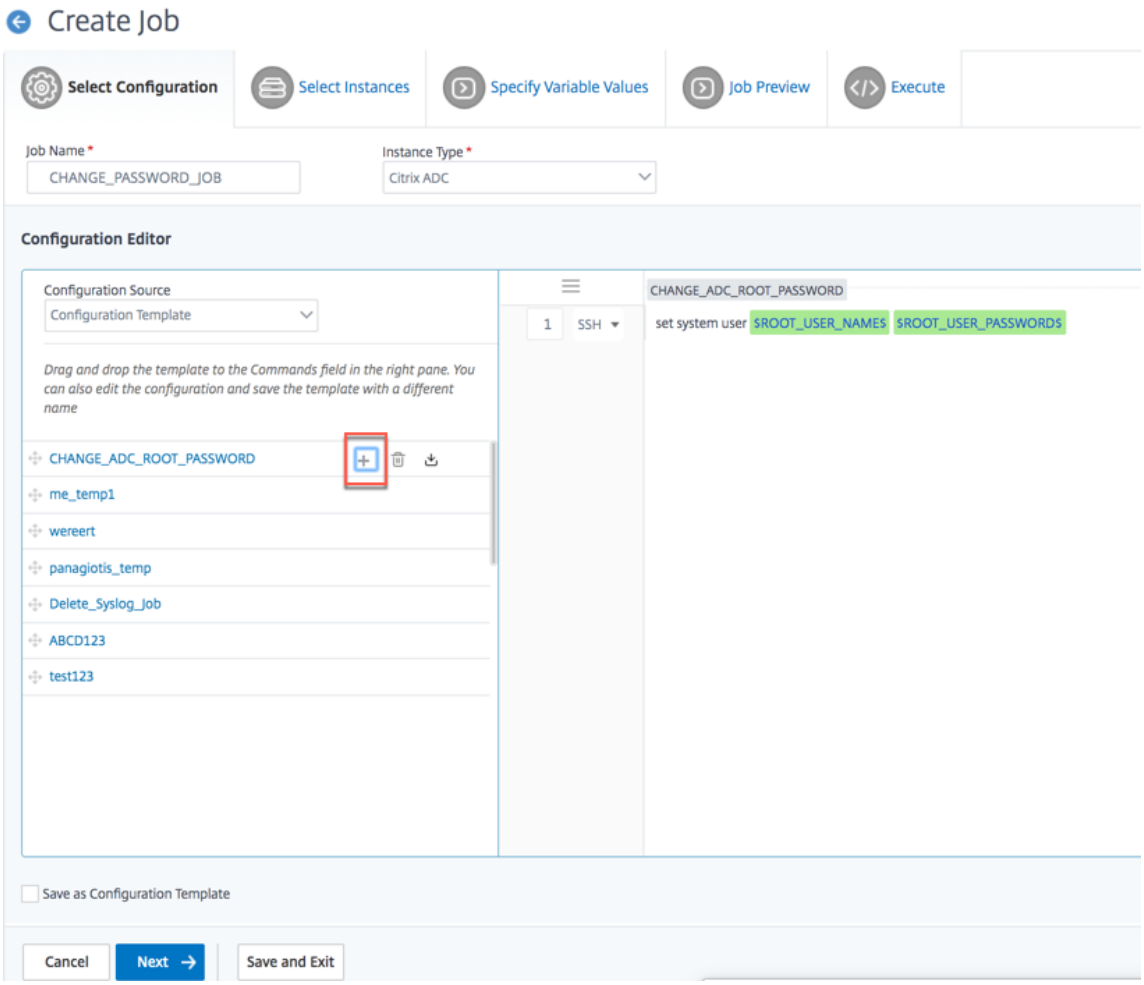


5. Seleccione la variable $ROOT_USER_PASSWORD$ y seleccione **Campo de contraseña como Tipo**. Seleccione **Listo** para guardar la configuración de la variable.
6. Seleccione **Aceptar** para guardar la plantilla de configuración.
7. La nueva plantilla de configuración aparece en **Plantillas de configuración**.

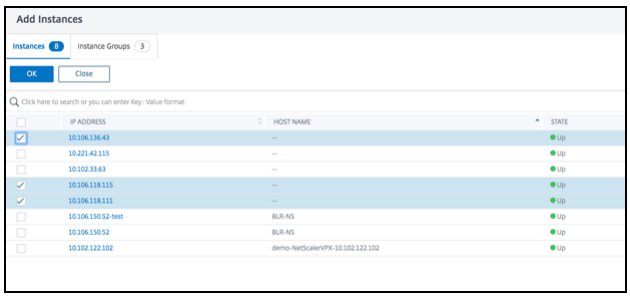


Crear un trabajo de configuración

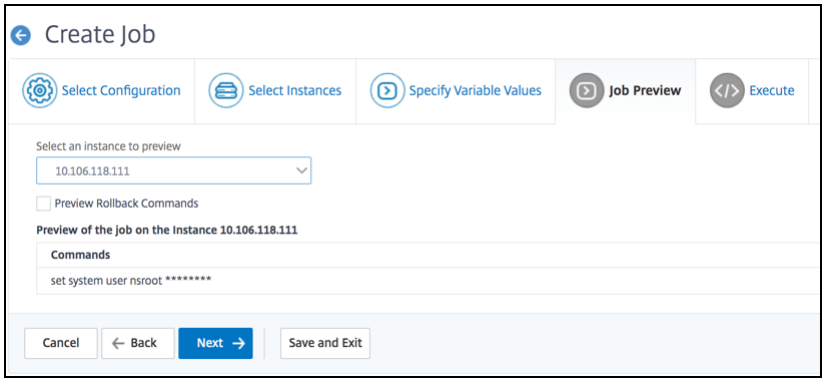
1. Desde la GUI de Citrix ADM, vaya a **Infraestructura > Trabajos de configuración**.
2. Seleccione **Crear trabajo** y haga clic en el icono «+» de la nueva plantilla de configuración. Seleccione **Finalizar**.



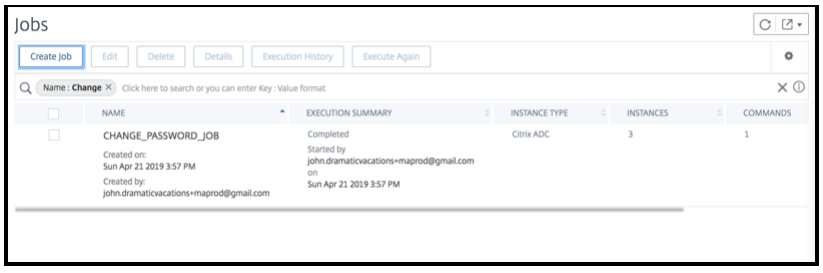
3. Seleccione la instancia o instancias de ADC para las que se debe modificar la contraseña.



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 CLI reales que el Citrix ADM ejecutará en las instancias de ADC. 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.

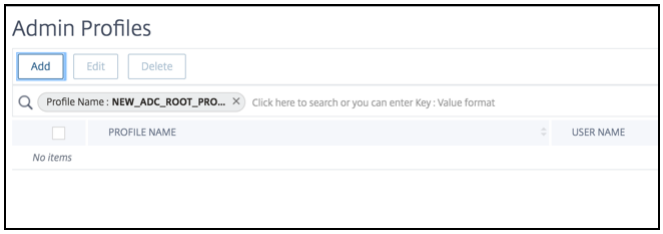


9. Seleccione el **trabajo** y haga clic en **Detalles**. Los detalles de ejecución muestran el estado a nivel de instancia individual.

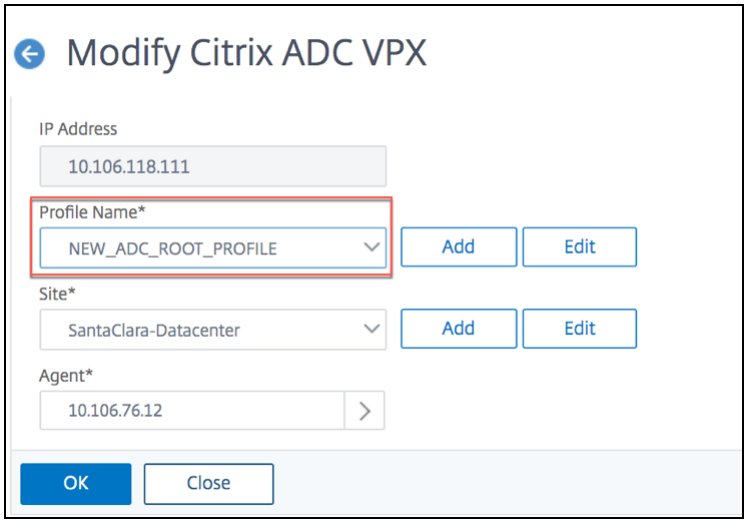
Modificar el perfil de administrador

Después de modificar las contraseñas de ADC, debe agregar y modificar los perfiles de administración de las instancias. Siga estos pasos:

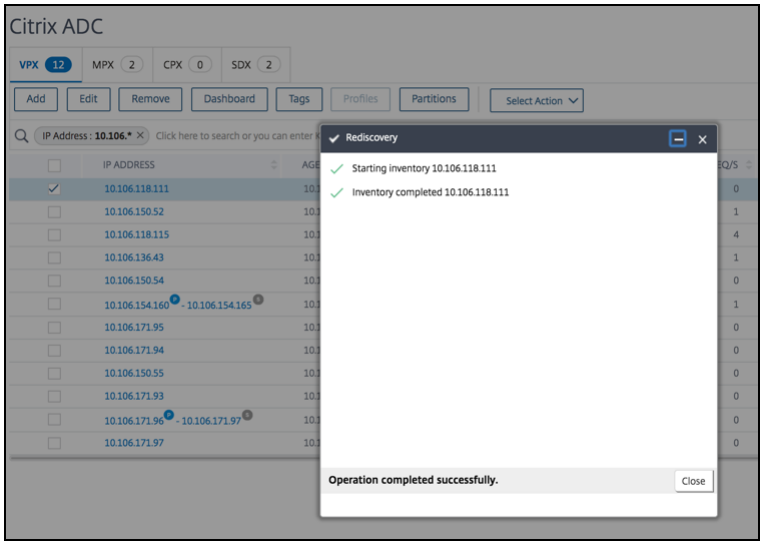
1. Vaya a**Infraestructura > Instancias > Citrix ADC**.
2. Haga clic en **Perfiles** para ver todos los perfiles de administración.
3. Seleccione **Agregar** para crear un perfil de administrador y proporcionar nuevas credenciales de Citrix ADC.



4. El perfil recién creado aparece en **Perfiles de administración**.
5. Vaya a **Red > Instancias > Citrix ADC**. Seleccione la instancia de Citrix ADC 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 Citrix ADC.

Cómo cambiar una contraseña nsroot de Citrix ADC SDX

November 16, 2022

Ocasionalmente, debe cambiar la contraseña nsroot del dispositivo Citrix ADC 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 Citrix ADC SDX administrado a través de Citrix ADM cloud.

Si cambia la contraseña del ADC, debe modificar el perfil de administrador de Citrix ADM que está asociado al ADC. Un perfil de administrador de Citrix ADM mantiene las credenciales de ADC para la comunicación basada en la API REST, SSH, SCP o SNMP con el dispositivo ADC. A través de los perfiles de administrador, Citrix ADM administra los dispositivos Citrix ADC SDX.

Cambiar contraseña

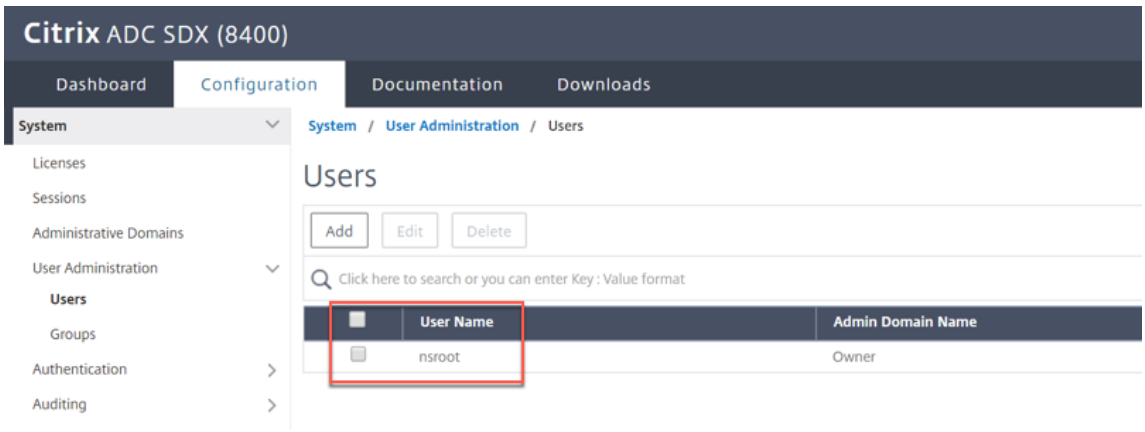
Siga estos pasos para cambiar la contraseña:

- Paso 1. Cambie la contraseña de SDX desde la GUI del servicio de administración de SDX.
- Paso 2. Modifique el perfil de administrador de Citrix ADM asociado al SDX.

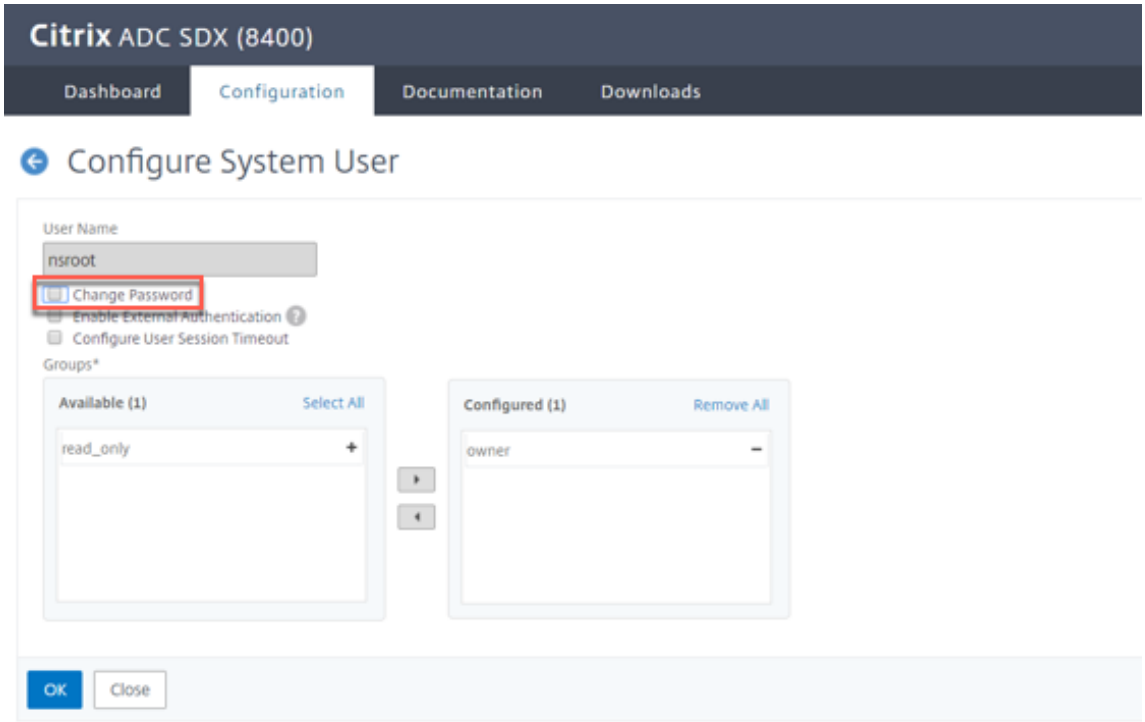
> Nota: Si el dispositivo SDX también se administra mediante otras herramientas, también debe cambiar las credenciales de esas herramientas.

Cambie la contraseña de SDX desde la GUI del servicio de administración de SDX

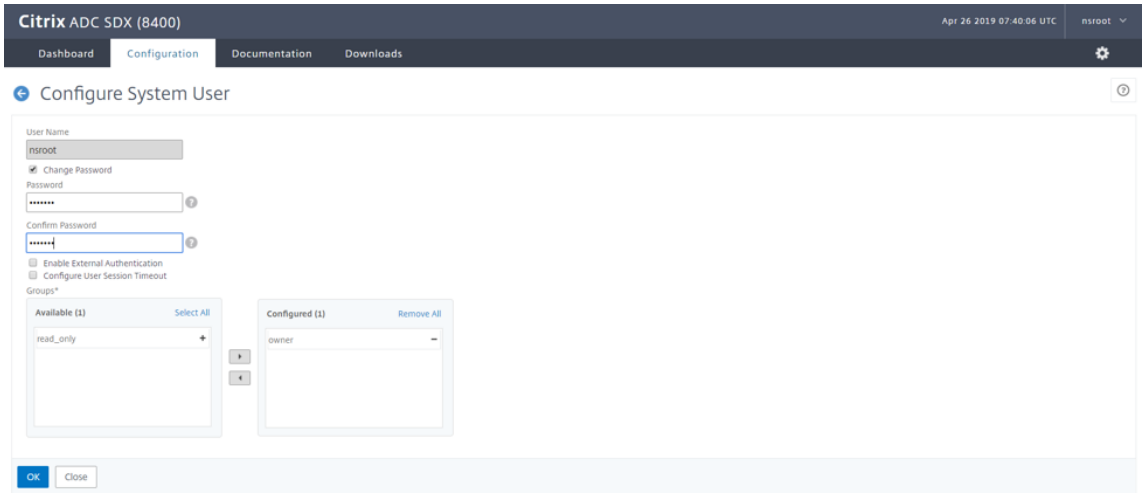
1. Desde SDX Management Service, vaya a **Sistema > Administración de usuarios > Usuarios**.
2. Seleccione el nombre de usuario para el que quiere cambiar la contraseña y haga clic en **Modificar**.



3. Selecciona **Cambiar contraseña**.



4. Introduzca una contraseña nueva y haga clic en **Aceptar**.

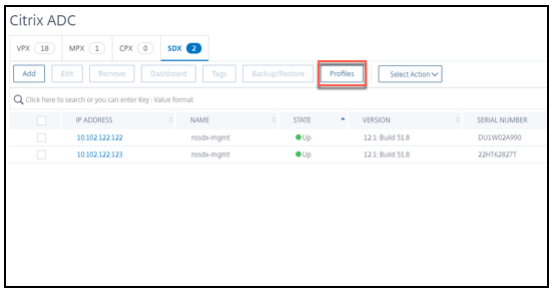


5. Se ha cambiado la contraseña de SDX

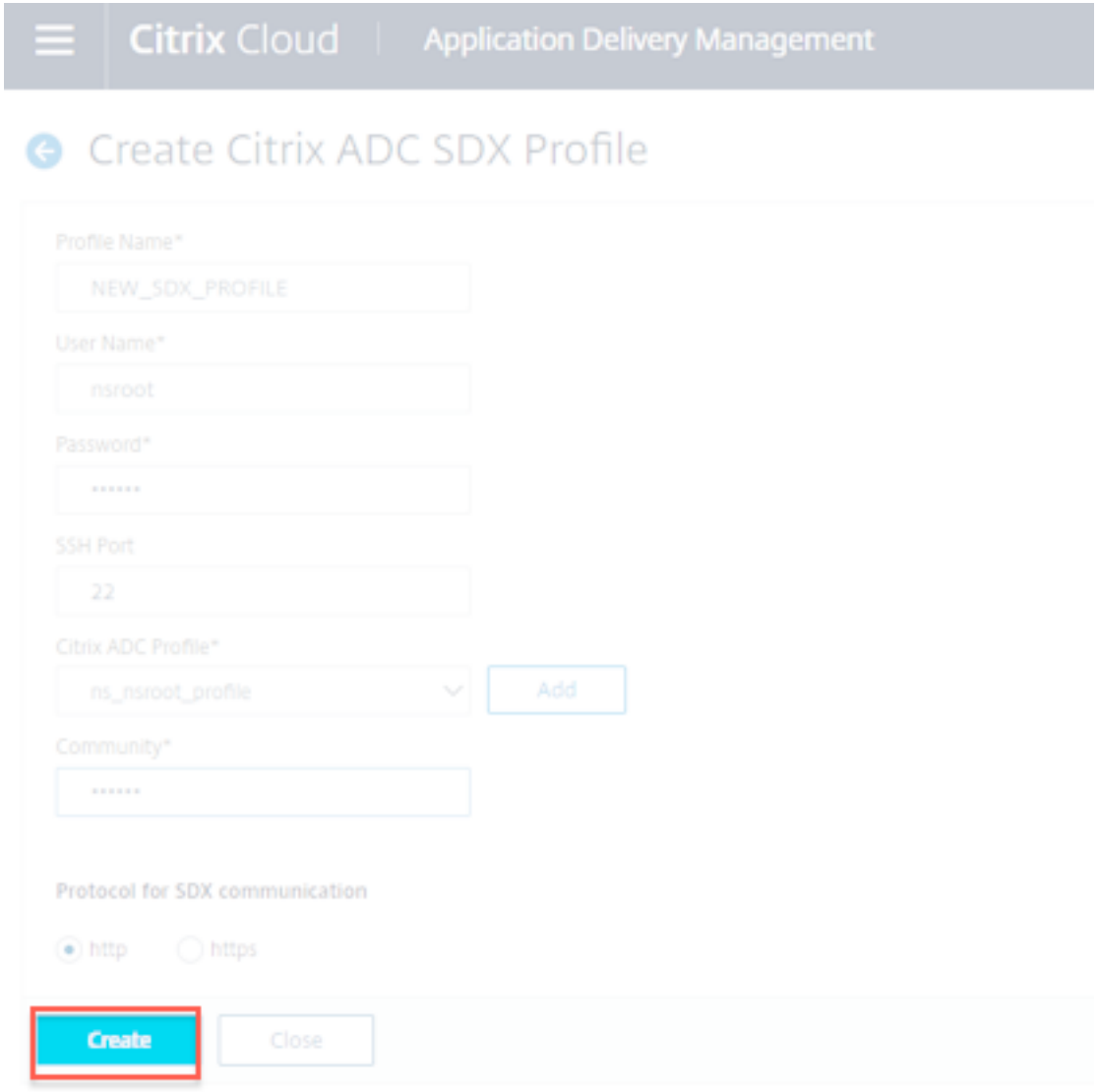
Modificar el perfil de administrador de Citrix ADM

Después de modificar las contraseñas de SDX, debes modificar los perfiles de administrador de las instancias. Siga estos pasos:

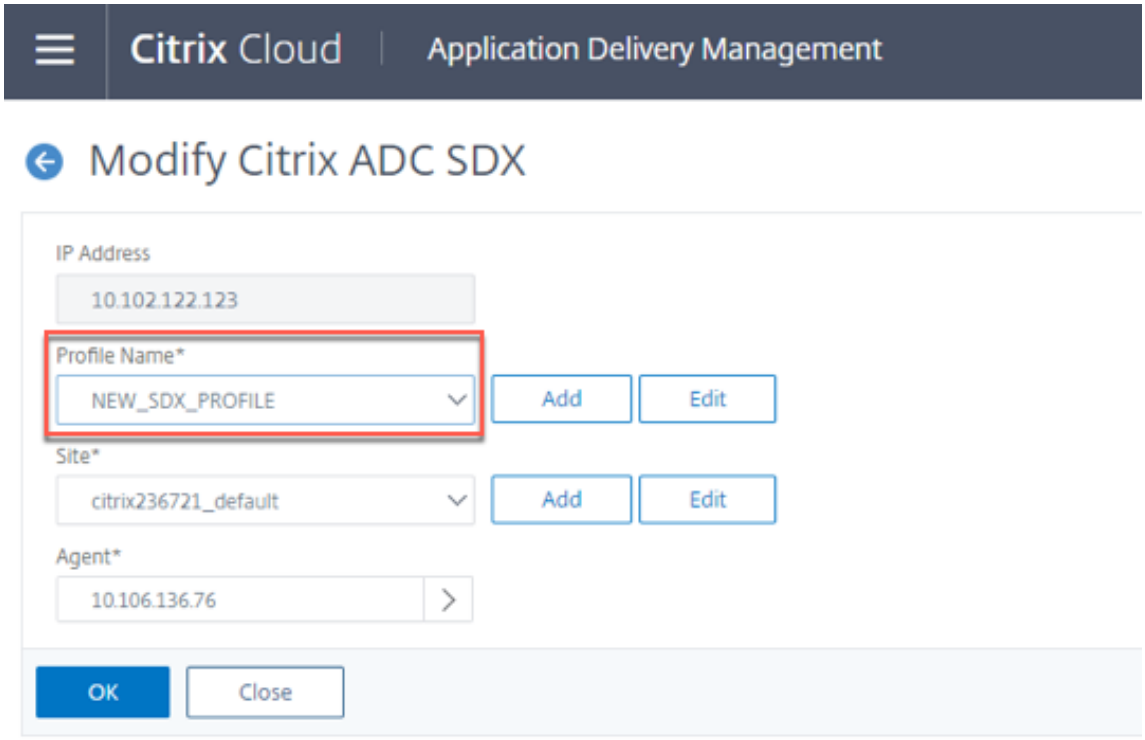
1. Vaya a **Infraestructura > Panel de instancias > Citrix ADC > SDX**.
2. Selecciona **Perfiles** para ver todos los perfiles de administración.



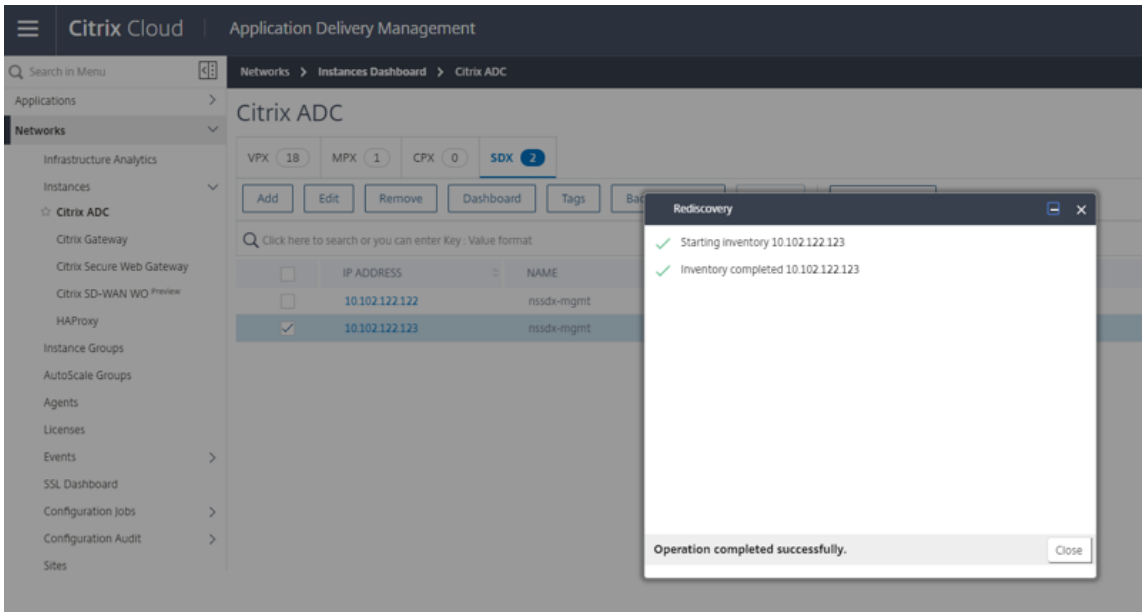
3. Selecciona **Agregar** para crear un perfil de administrador.
4. Proporcione las nuevas credenciales de Citrix ADC y haga clic en **Crear**.



5. El perfil recién creado aparece en **Perfiles de administración**.
6. Vaya a **Red > Instancias > Citrix ADC > 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 Citrix ADC MPX o VPX.

Eventos

November 16, 2022

Cuando la dirección IP de una instancia de Citrix Application Delivery Controller (Citrix ADC) se agrega a Citrix ADM, Citrix ADM envía una llamada NITRO e implícitamente se agrega a sí mismo como destino de captura para que la instancia reciba sus capturas o eventos.

Los eventos representan ocurrencias de eventos o errores en una instancia administrada de Citrix ADC. Por ejemplo, cuando se produce un error del sistema o un cambio en la configuración, se genera un evento y se registra en el servidor Citrix ADM. Los eventos recibidos en Citrix ADM 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**).

Citrix ADM también comprueba los eventos generados en las instancias para formar alarmas de diferentes niveles de gravedad y los 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 Citrix ADC.

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 Citrix ADC, categoría, objetos de error, comandos de configuración y mensajes.

También puede asegurarse de que se activan varias notificaciones para un intervalo de tiempo específico para un evento hasta que se borre el evento. Como medida adicional, 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

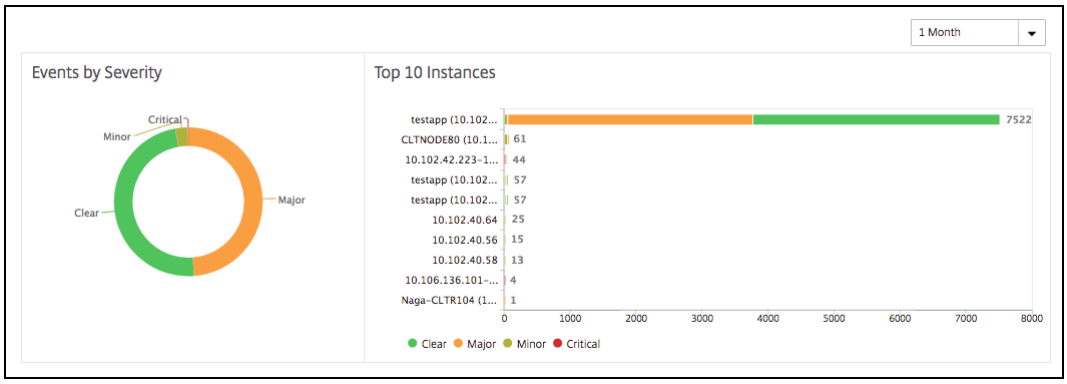
December 2, 2022

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 (Citrix ADC), junto con los eventos y su gravedad en instancias específicas. Puede utilizar el panel de eventos de Citrix ADM para ver los informes generados con detalles sobre la gravedad de los eventos críticos en todas sus instancias de Citrix ADC.

Para ver los detalles en el panel de eventos:

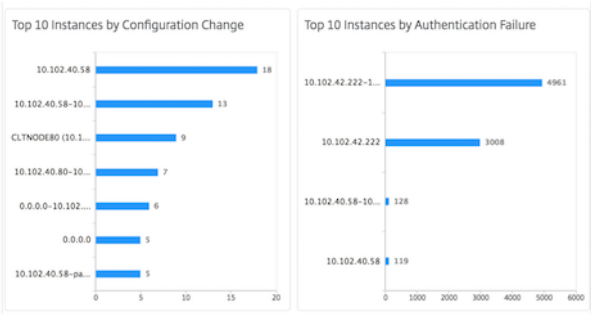
Vaya a **Infraestructura > Eventos > Informes**.

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.

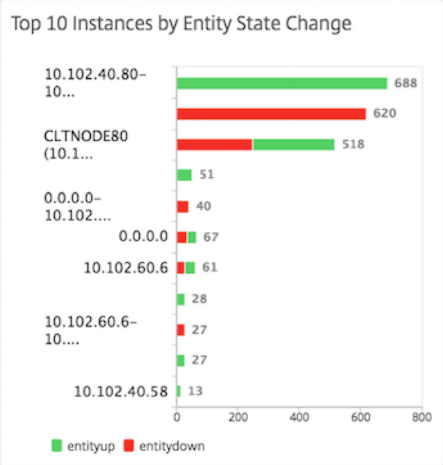


Para ver más detalles, vaya al tipo de instancia de Citrix ADC (**Infraestructura > Eventos > Informes** > **Citrix ADC/ Citrix ADC SDX/ Citrix ADC**) para ver lo siguiente:

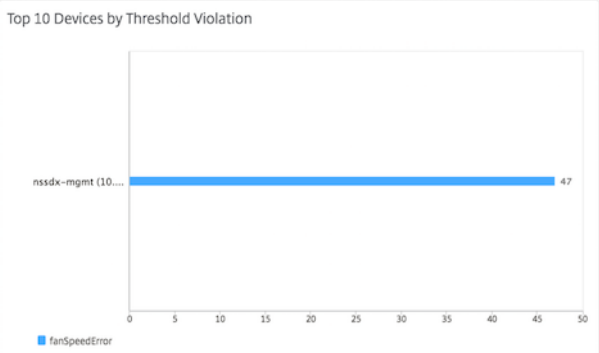
- Los 10 dispositivos principales por fallo de hardware
- Los 10 dispositivos principales por cambio de configuración
- Los 10 dispositivos principales por error de autenticación



- 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 especificar todos los días que quiere programar el informe separados por comas.

Establecer la edad del evento para los eventos

November 16, 2022

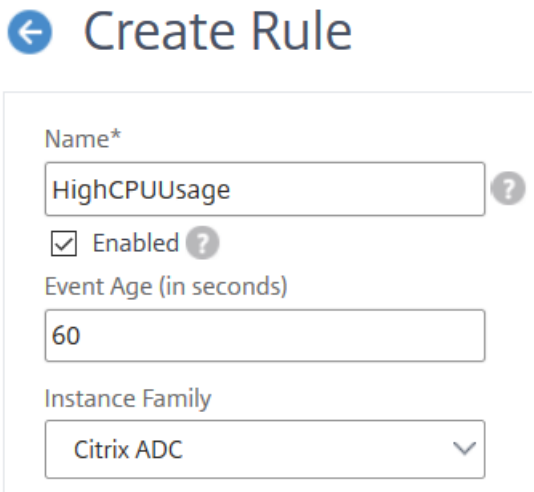
Puede configurar la opción de antigüedad del evento para especificar el intervalo de tiempo (en segundos). Citrix ADM supervisa los dispositivos hasta la duración establecida y genera un evento solo si la antigüedad del evento supera la duración establecida.

> Nota:
>
> El valor mínimo para la antigüedad del evento es de 60 segundos. Si mantiene el campo **Edad del evento** en blanco, la regla de evento se aplica inmediatamente después de que se produzca el evento.

Por ejemplo, considere que quiere administrar varios dispositivos ADC y recibir una notificación por correo electrónico cuando alguno de sus servidores virtuales deje de funcionar durante 60 segundos o más. Puede crear una regla de evento con los filtros necesarios y establecer la edad del evento de la regla en 60 segundos. A continuación, siempre que un servidor virtual permanezca inactivo durante 60 segundos o más, recibirá una notificación por correo electrónico con detalles como el nombre de la entidad, el cambio de estado y la hora.

Para establecer la edad del evento en Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Eventos > Reglas**y haga clic en **Agregar**.
2. En la página **Crear regla**, establezca los parámetros de regla.
3. Especifique la edad del evento en segundos.



Programar un filtro de eventos

November 16, 2022

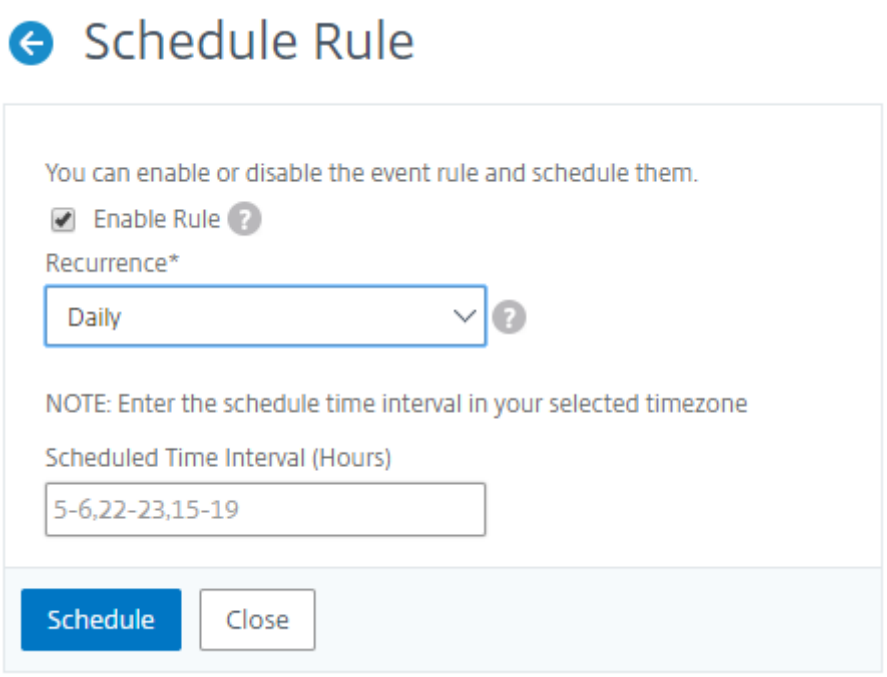
Después de crear un filtro para su regla, si no quiere que Citrix ADM envíe una notificación cada vez que el evento generado cumpla con los criterios del filtro, puede programar el filtro para que se active solo en intervalos de tiempo específicos, como diario, semanal o mensual.

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 de correo electrónico cuando Citrix ADM recibe estas capturas. 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 Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Eventos > Reglas**.
2. Seleccione la regla para la que quiere programar un filtro y haga clic en **Ver planificación**.
3. En la página **Regla programada**, haga clic en **Programar** y especifique los siguientes parámetros:
    - **Habilitar regla** : active esta casilla de verificación para habilitar la regla de evento programado.
    - **Periodicidad**: Intervalo en el que se planifica la regla.
    - **Intervalo de tiempo programado (horas)** : horas en las que programar la regla (utilice el formato de 24 horas).
4. Haga clic en **Programar**.



Establecer notificaciones de correo electrónico repetidas para eventos

November 16, 2022

Para garantizar que se aborden todos los eventos críticos y que no se pierda ninguna notificación importante por correo electrónico, puede optar por enviar notificaciones por correo electrónico repetidas para las reglas de eventos que cumplan con los criterios que ha seleccionado. Por ejemplo, si ha creado una regla de evento para las instancias que implican errores de disco y quiere recibir una notificación hasta que se resuelva el problema, puede optar por recibir notificaciones por correo electrónico repetidas sobre esos eventos.

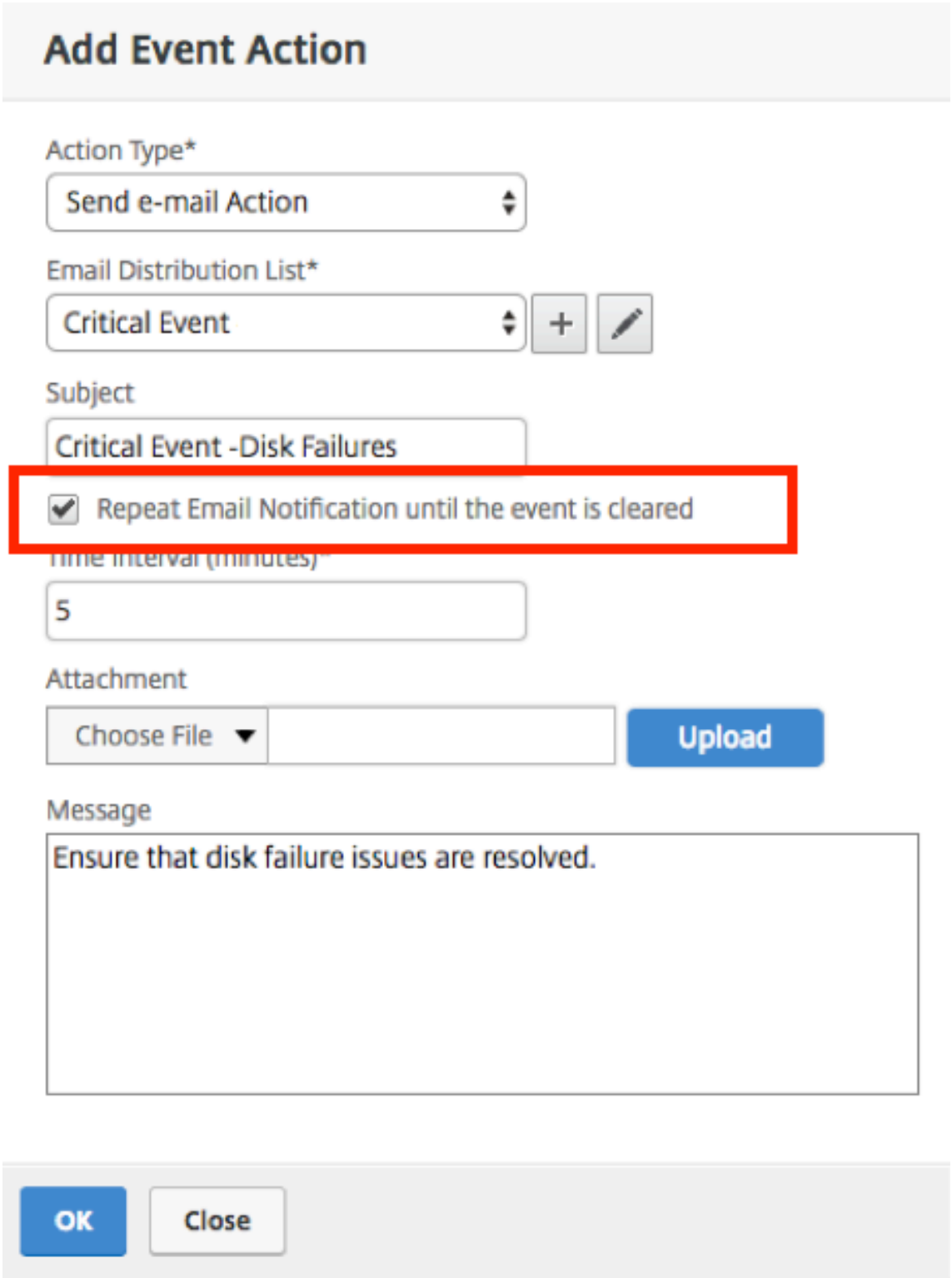
Estas notificaciones por correo electrónico se envían repetidamente, a intervalos predefinidos, hasta que el destinatario reconoce haber visto la notificación o se borra la regla de evento.

> **Nota**
>
> Los eventos solo se pueden borrar automáticamente si hay un conjunto de capturas «borrar» equivalente y se envían desde su instancia de Citrix ADC.
>
> Para borrar un evento manualmente, puede hacer lo siguiente:
>
> - Vaya a **Infraestructura > Eventos > Resumen del evento**, seleccione **Categoría**y, a continuación, seleccione un evento de la categoría y haga clic en **Borrar**.
> - O bien, vaya a **Infraestructura > Eventos > Mensajes de eventos**. Elija un tipo de instancia

> y, a continuación, seleccione un evento de la siguiente cuadrícula y haga clic en **Borrar**.

Para configurar notificaciones de correo electrónico repetidas desde Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Eventos > Reglas**y haga clic en **Agregar** para crear una regla.
2. En la página **Crear regla**, establezca los parámetros de regla.
3. En Acciones de **reglas de eventos**, haga clic en **Agregar acción**. A continuación, seleccione **Enviar acción de correo electrónico** en la lista desplegable **Tipo de acción** y seleccione una lista de **distribución de correo electrónico**.
4. También puede agregar una línea de asunto personalizada y un mensaje de usuario, y cargar un archivo adjunto al correo electrónico cuando un evento entrante coincida con la regla configurada.
5. Active la casilla de verificación **Repetir notificación por correo electrónico hasta que se desactive el evento**.



Suprimir eventos

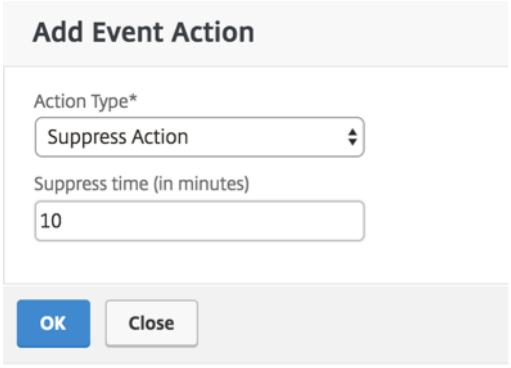
November 16, 2022

Al elegir la **acción de evento Suprimir** acción, puede configurar un período de tiempo, en minutos, para el que se suprime o elimina un evento. Puede suprimir el evento durante un mínimo de 1 minuto.

> Nota:
>
> También puede configurar el tiempo de supresión como 0 minutos y significa tiempo infinito. Si no especifica ninguna duración de tiempo, Citrix ADM considerará el tiempo de supresión como cero y nunca caduca.

Para suprimir eventos mediante Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Eventos > Reglas**.
2. Vaya a la página **Crear regla** o **Configurar regla** . Especifique todos los parámetros necesarios para crear una regla.
3. En **Acciones de regla de evento**, haga clic en **Agregar acción** para asignar acciones de notificación al evento.
4. En la página **Agregar acción de evento**, seleccione **Suprimir acción** en el menú desplegable **Tipo de acción** y especifique el período de tiempo, en minutos, para el que debe suprimirse un evento.
5. Haga clic en **Aceptar**.



Crear reglas de eventos

December 2, 2022

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan el filtrado de los eventos generados en la infraestructura.

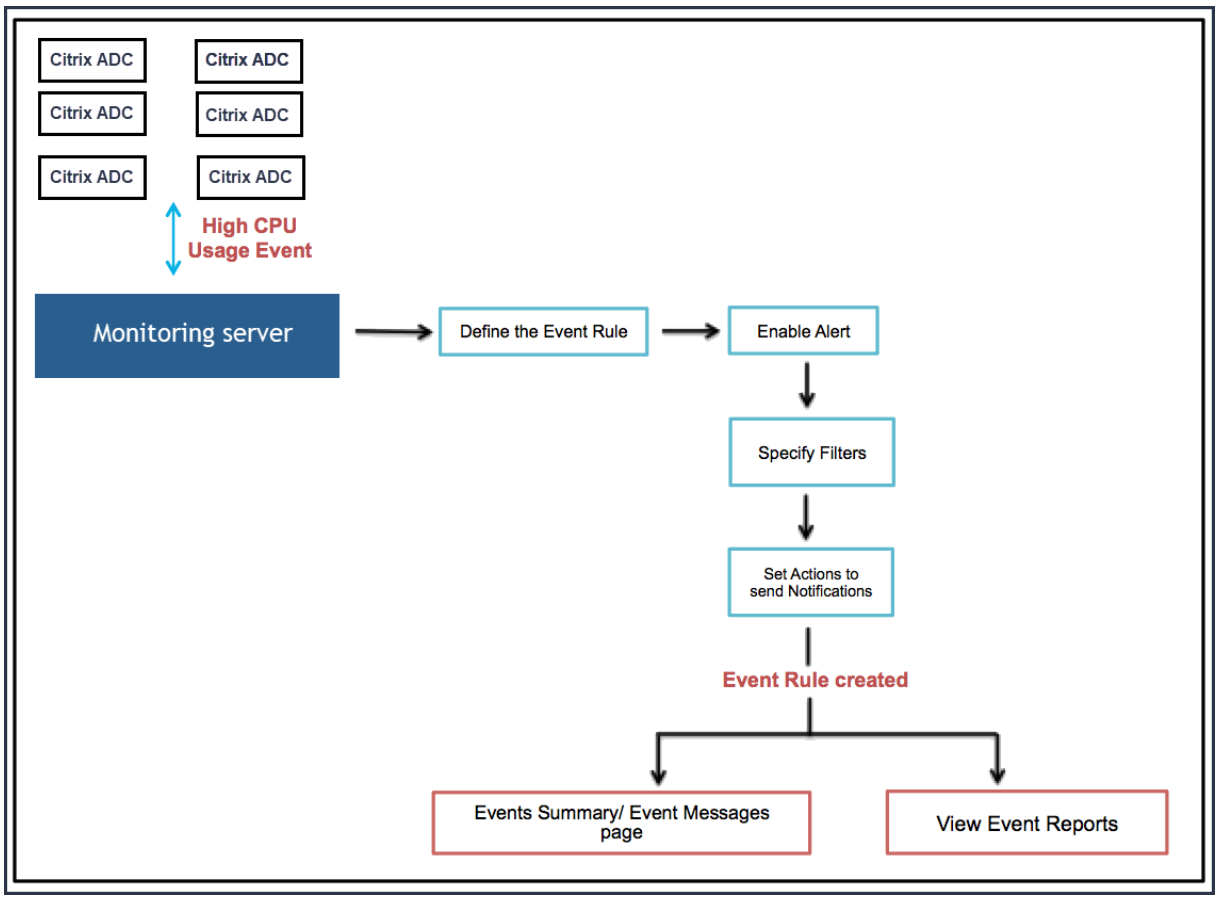
Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen los criterios de filtro de la regla, se ejecuta la acción asociada a la regla. Las condiciones para las que puede crear filtros son: gravedad, instancias de Citrix Application Delivery Controller (Citrix ADC), categoría, objetos de error, comandos de configuración y mensajes.

Puede asignar las siguientes acciones a los eventos:

- **Acción de envío de correo electrónico**: Enviar un correo electrónico para los eventos que coinciden con los criterios de filtrado.
- **Enviar acción de captura**: Enviar o reenviar capturas SNMP a un destino de captura externo
- **Ejecutar acción de comando**: Ejecute un comando cuando un evento entrante cumpla con la regla configurada.
- **Ejecutar acción de trabajo**: Ejecutar un trabajo es para eventos que coinciden con los criterios de filtro especificados.
- **Suprimir acción**: Suprime la eliminación de un evento durante un período de tiempo específico.
- **Enviar notificaciones de Slack**: envía notificaciones en el canal de Slack configurado para los eventos que coincidan con los criterios del filtro.
- **Enviar notificaciones de PagerDuty**: Envíe notificaciones de eventos basadas en las configuraciones de PagerDuty para los eventos que coincidan con los criterios de filtro.
- **Enviar notificaciones de ServiceNow**: Generar automáticamente incidentes de ServiceNow para un evento que coincida con los criterios de filtro.

Para obtener más información, consulte Agregar acciones de reglas de eventos.

También puede hacer que las notificaciones se reenvíen en un intervalo especificado hasta que se borre un evento. Además, puede personalizar el correo electrónico con una línea de asunto específica, un mensaje de usuario y un archivo adjunto.



Por ejemplo, como administrador, es posible que quiera supervisar los eventos de “alto uso de CPU” en instancias de ADC que podrían provocar una interrupción. Puede realizar cualquiera de las siguientes acciones para recibir notificaciones:

- Crea una regla para supervisar las instancias. Además, 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 configuración de una regla de evento implica las siguientes tareas:

1. Defina la regla
2. Elija la gravedad del evento que detecta la regla
3. Especifica la categoría del evento
4. Especificar instancias Citrix ADC a las que se aplica la regla
5. Seleccionar objetos de error
6. Especificar filtros avanzados
7. Especificar las acciones que se deben realizar cuando la regla detecta un evento

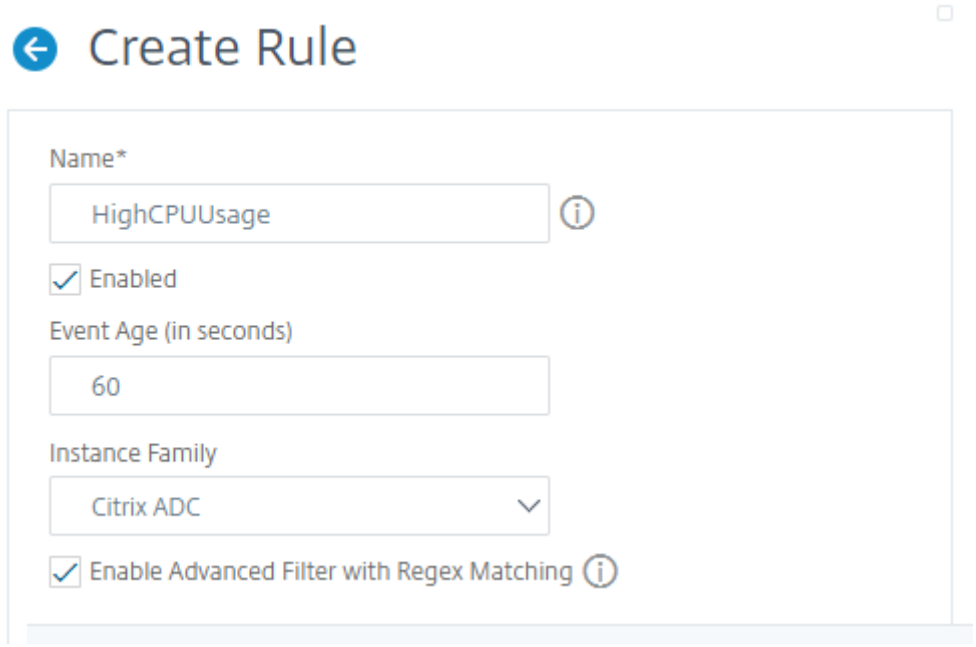
Paso 1: Definir una regla de evento

Vaya a **Infraestructura > Eventos > Reglas**y haga clic en **Agregar**. Si quiere habilitar la regla, active la casilla de verificación **Habilitar regla**.

Puede configurar la opción **Event Age** para especificar el intervalo de tiempo (en segundos) tras el cual Citrix ADM actualiza una regla de eventos.

> Nota:
>
> El valor mínimo para la antigüedad del evento es de 60 segundos. Si mantiene el campo **Edad del evento** en blanco, la regla de evento se aplica inmediatamente después de que se produzca el evento.

Según el ejemplo anterior, es posible que quiera recibir una notificación por correo electrónico cada vez que su instancia de Citrix ADC tenga un evento de «alto uso de CPU» durante 60 segundos o más. Puede establecer la antigüedad del evento en 60 segundos, de modo que cada vez que su instancia de Citrix ADC tenga un evento de «alto uso de CPU» durante 60 segundos o más, reciba una notificación por correo electrónico con detalles del evento.



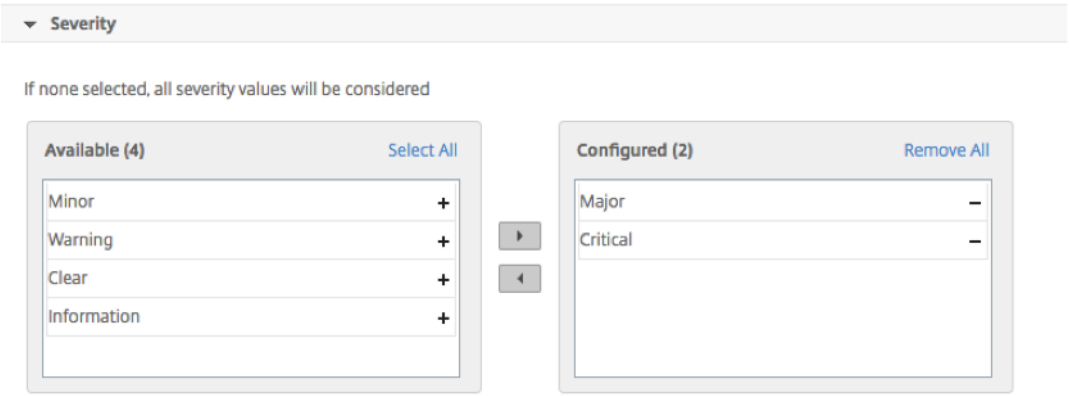
También puede filtrar las reglas de eventos por **familia de instancias** para rastrear la instancia de Citrix ADC desde la que Citrix ADM recibe un evento.

Si quiere incluir una expresión regular distinta de la coincidencia de patrones de asterisco (*), seleccione **Habilitar filtro avanzado con coincidencia de expresiones regulares**.

Paso 2: Elige la gravedad del evento

Puede crear reglas de evento que utilicen la configuración de gravedad predeterminada. La gravedad especifica la gravedad actual de los eventos a los que quiere agregar la regla de eventos.

Puede definir los siguientes niveles de gravedad: Crítico, Mayor, Menor, Advertencia, Borrar e Información.

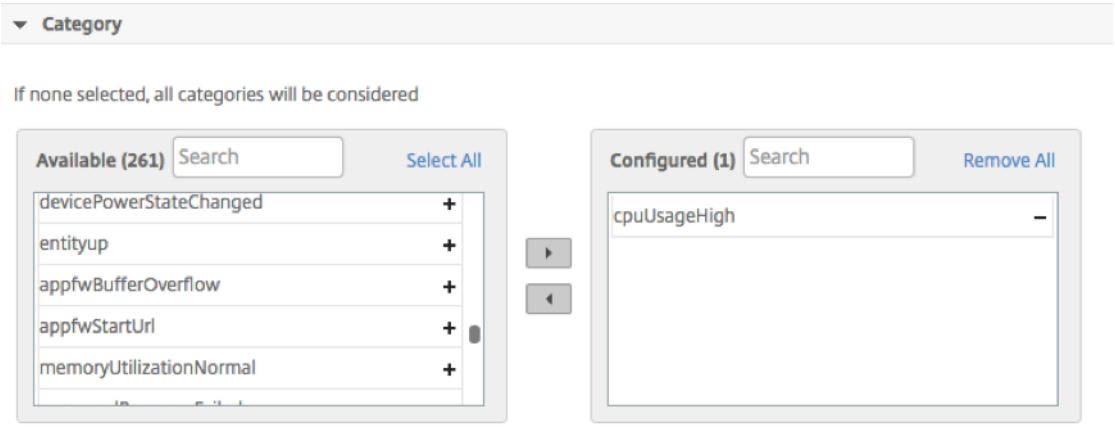


> **Nota**
>
> Puede configurar la gravedad para eventos genéricos y específicos de Advanced. Para modificar la gravedad de los eventos de las instancias de Citrix ADC administradas en Citrix ADM, vaya a **Infraestructura > Eventos > Configuración de eventos**. Elija la **categoría** para la que quiere configurar la gravedad del evento y haga clic en **Configurar gravedad**. Asigne un nuevo nivel de gravedad y haga clic en **Aceptar**.

Paso 3: Especifica la categoría del evento

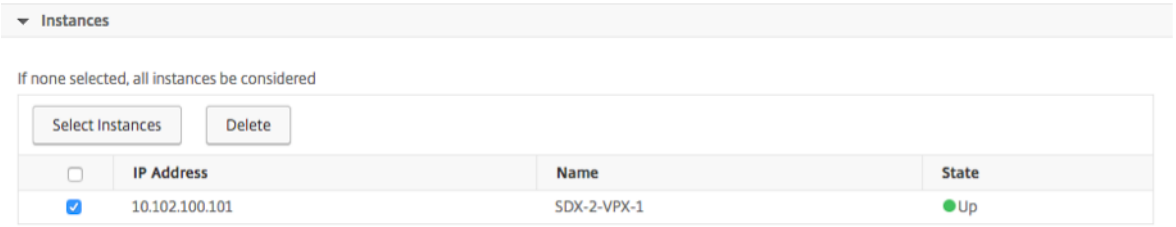
Puede especificar la categoría o las categorías de los eventos generados por las instancias Citrix ADC. Todas las categorías se crean en instancias de Citrix ADC. A continuación, estas categorías se asignan con Citrix ADM que se puede utilizar para definir reglas de eventos. Seleccione la categoría que quiera considerar y muévalo de la tabla **Disponible** a la tabla **Configurada**.

En el ejemplo anterior, debe elegir «CPUusageHigh» como categoría de evento de la tabla mostrada.



Paso 4: Especificar instancias de Citrix ADC

Seleccione las direcciones IP de las instancias de Citrix ADC para las que quiere definir la regla de eventos. En la sección **Instancias**, haga clic en **Seleccionar instancias**. En la página **Seleccionar Instancias**, elija las instancias y haga clic en **Seleccionar**.



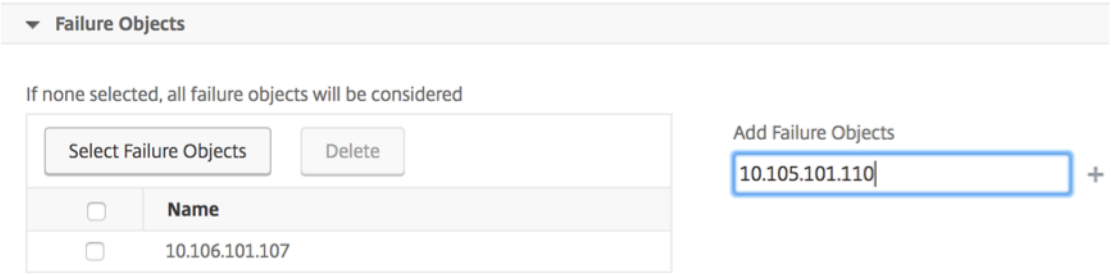
Paso 5: Seleccione objetos de error

Puede seleccionar un objeto de error de la lista proporcionada o agregar un objeto de fallo para el que se haya generado un evento. También puede especificar una expresión regular para agregar objetos de error. Según la expresión regular especificada, los objetos de error se añaden automáticamente a la lista. Los objetos de error son instancias de entidad o contadores para los que se ha generado un evento.

> **Importante**
>
> Para enumerar objetos con errores mediante expresiones regulares, seleccione **Habilitar filtro avanzado con coincidencia de expresiones** regulares en el paso 1.

El objeto de error afecta a la forma en que se procesa un evento y garantiza que refleje el problema exacto tal como se notifica. Con este filtro, puede realizar un seguimiento rápido de los problemas en los objetos de falla e identificar la causa de un problema. Por ejemplo, si un usuario tiene problemas para iniciar sesión, el objeto de error aquí es el nombre de usuario o la contraseña, por ejemplo `nsroot`.

Esta lista puede contener nombres de contador para todos los eventos relacionados con umbrales, nombres de entidades para todos los eventos relacionados con entidades, nombres de certificados para eventos relacionados con certificados, etc.

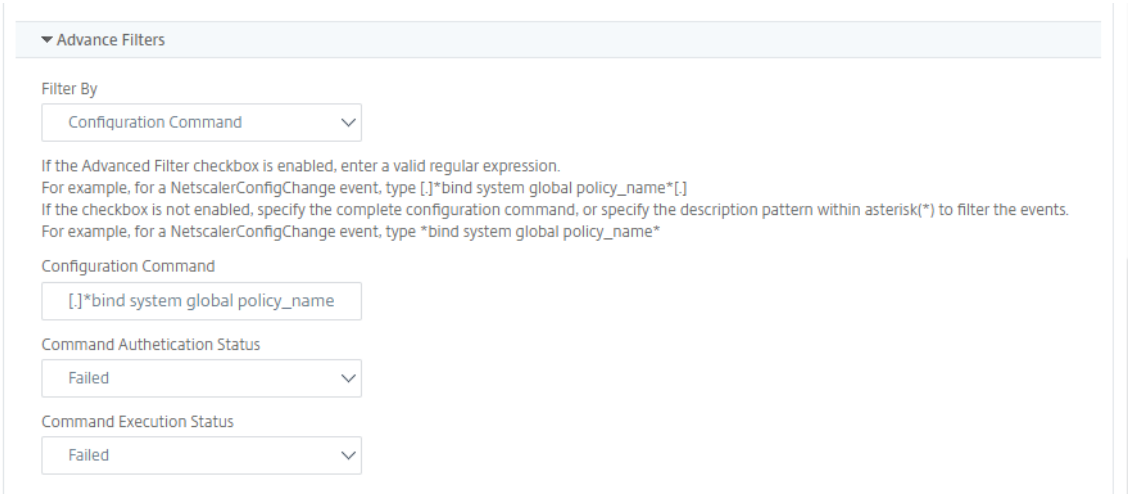


Paso 6: Especificar filtros avanzados

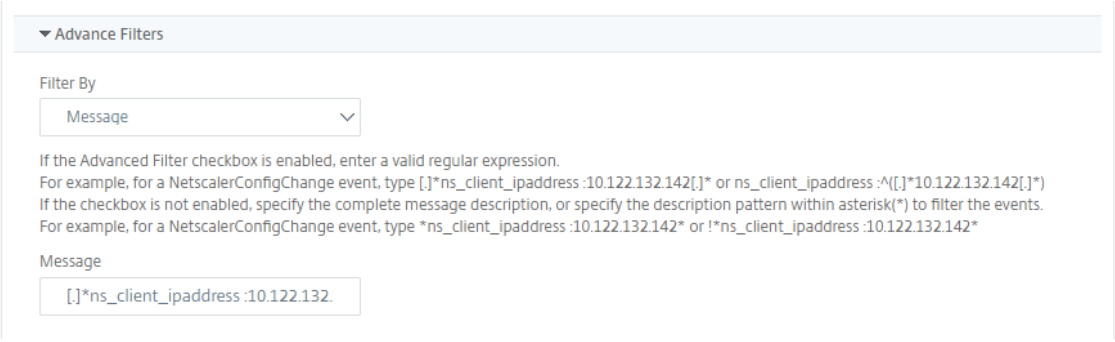
Puede filtrar aún más una regla de evento por:

- **Comandos de configuración** : puede especificar el comando de configuración completo o especificar una expresión regular para filtrar los eventos.

  Puede filtrar aún más la regla de eventos según el estado de autenticación y/o el estado de ejecución del comando. Por ejemplo, para a `NetscalerConfigChange event`, escriba `[.]* bind system global policy_name[.]*`.



- **Mensajes** : puede especificar la descripción completa del mensaje o especificar una expresión regular para filtrar los eventos.
  Por ejemplo, para un evento `NetscalerConfigChange`, escriba `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)`.



> **Importante**
>
> Para filtrar los comandos y mensajes de configuración mediante expresiones regulares distintas de la coincidencia de patrones de asterisco (*), seleccione **Activar filtro avanzado con coincidencia de expresiones** regulares en el paso 1.

Paso 7: Agregar acciones de reglas de eventos

Puede agregar acciones de regla de evento para asignar acciones de notificación a un evento. Estas notificaciones se envían o realizan cuando un evento cumple con los criterios de filtro definidos anteriormente. Puede agregar las siguientes acciones de evento:

- Enviar correo electrónico Action
- Acción de captura de envío
- Ejecutar acción de comando
- Ejecutar acción de trabajo
- Acción de supresión
- Enviar notificaciones de Slack
- Enviar notificaciones de PagerDuty
- Enviar notificaciones de ServiceNow

Para establecer la acción de regla de evento de correo electrónico

Al elegir **Enviar acción de correo electrónico**, se activa un correo electrónico cuando los eventos cumplen los criterios de filtro definidos. Debe crear una lista de distribución de correo electrónico proporcionando los detalles del servidor de correo o del perfil de correo, o bien puede seleccionar una lista de distribución de correo electrónico que haya creado previamente.

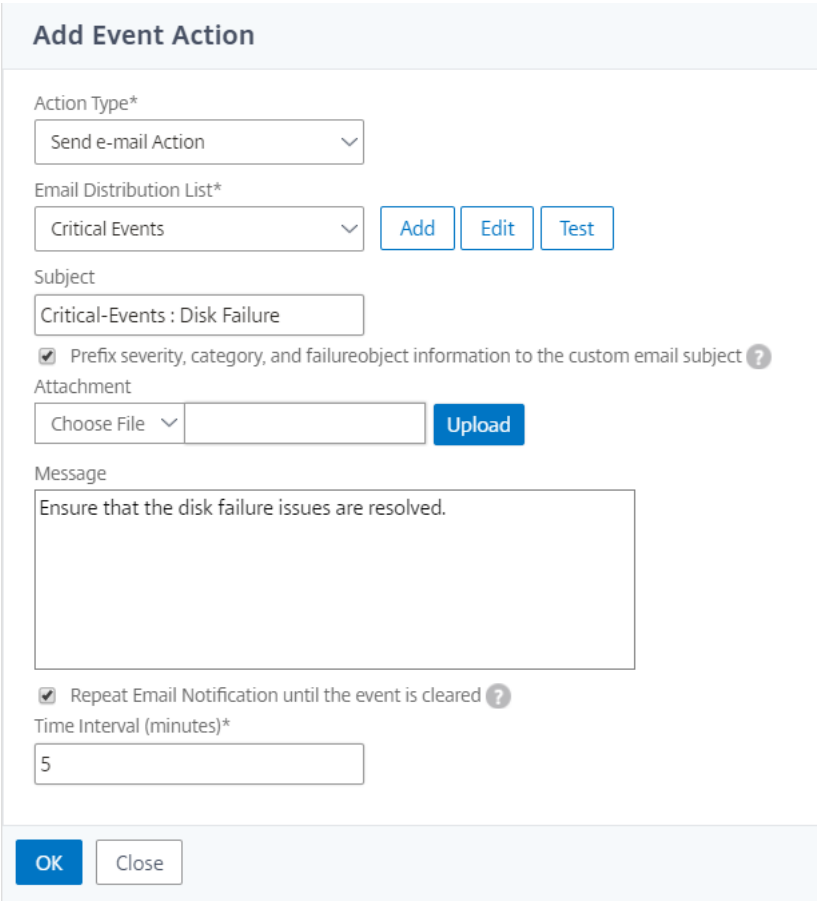
Debido a la gran cantidad de servidores virtuales que se configuran en Citrix ADM, es posible que reciba un gran número de correos electrónicos cada día. Los correos electrónicos tienen una línea de asunto predeterminada que proporciona información sobre la gravedad del evento, la categoría del

evento y el objeto de error. Sin embargo, la línea de asunto no contiene información sobre el nombre del servidor virtual en el que se originan estos eventos. Ahora tiene la opción de incluir información adicional, como el nombre de la entidad afectada, es decir, el nombre del objeto de error.

También puede agregar una línea de asunto personalizada y un mensaje de usuario, y subir un archivo adjunto a tu correo electrónico cuando un evento entrante coincida con la regla configurada.

Al enviar correos electrónicos para notificaciones de eventos, es posible que quiera enviar un correo electrónico de prueba para probar los ajustes configurados. El botón «Probar» ahora le permite enviar un correo electrónico de prueba después de configurar un servidor de correo electrónico, las listas distribuidas asociadas y otros ajustes. Esta función garantiza que la configuración funcione bien.

También puede asegurarse de que se solucionen todos los eventos críticos y de que no se pierda ninguna notificación importante por correo electrónico. Para ello, active la casilla **Repetir notificación por correo electrónico hasta que se desactive el evento** para enviar notificaciones por correo electrónico repetidas para las reglas de eventos que cumplan con los criterios que ha seleccionado. Por ejemplo, si ha creado una regla de evento para las instancias que implican errores de disco y quiere recibir una notificación hasta que se resuelva el problema, puede optar por recibir notificaciones por correo electrónico repetidas sobre esos eventos.



Para establecer la acción de regla de evento de reventado

Al elegir el tipo de **acción de evento Enviar acción de captura**, las capturas SNMP se envían o reenvían a un destino de captura externo. Al definir una lista de distribución de capturas (o un destino de captura y detalles de perfil de captura), los mensajes de captura se envían a un detector de capturas específico cuando los eventos cumplen los criterios de filtro definidos.

Para establecer la acción Ejecutar comando

Al elegir la acción del evento **Ejecutar acción de comando**, puede crear un comando o un script que se pueda ejecutar en Citrix ADM para eventos que coincidan con un criterio de filtro determinado.

También puede establecer los siguientes parámetros para el script **Ejecutar acción de comando** :

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 refleja el problema exacto tal como se ha notificado. Esto se puede usar para rastrear problemas rápidamente e identificar el motivo de la falla, en lugar de simplemente informar eventos sin procesar.

> **Nota**
>
> Durante la ejecución del comando, estos parámetros se reemplazan con valores reales.

Por ejemplo, considere que quiere establecer una acción de comando de ejecución cuando el estado de un servidor virtual de equilibrio de carga es **Inactivo**. Como administrador, puede considerar la posibilidad de ofrecer una solución rápida añadiendo otro servidor virtual. En Citrix ADM, puede:

- Escriba un archivo de script (.sh).

  A continuación se muestra un archivo de script (.sh) de ejemplo:

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- Guarde el archivo.sh en cualquier ubicación persistente del agente Citrix ADM. Por ejemplo: `/var`.
- Proporcione la ubicación del archivo.sh en Citrix ADM que se ejecutará cuando se cumplan los criterios de regla.

Para configurar la acción **Ejecutar comando** para crear un nuevo servidor virtual:

1. Defina la regla
2. Seleccione la gravedad del evento
3. Selecciona la categoría de eventos **entitydown**
4. Seleccione la instancia que tiene configurado el servidor virtual
5. Seleccione o cree un objeto de error para el servidor virtual

6. En **Acciones de reglas de eventos**, haga clic en **Agregar acción** y seleccione **Ejecutar acción de comando** en la lista de **tipos de acciones** .
7. En **Lista de ejecución de comandos**, haga clic en **Agregar**.

   Aparece la página Crear lista de distribución de comandos.

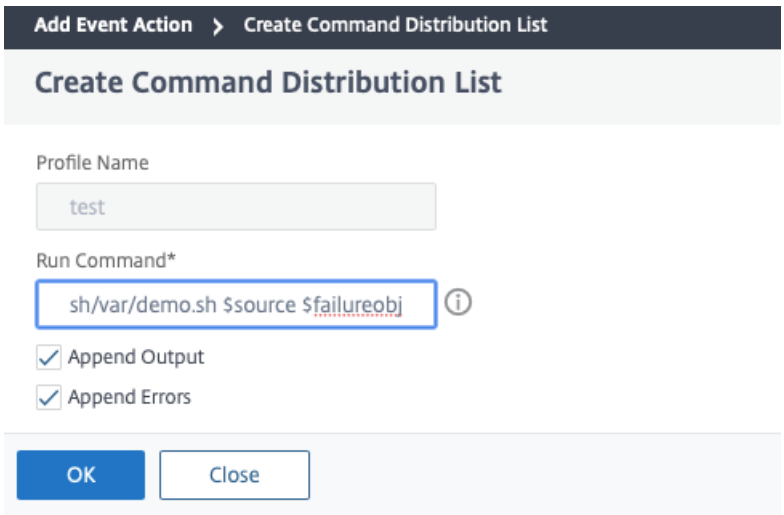
   a) En **Nombre del perfil**, especifique un nombre de su elección

   b) En **Ejecutar comando**, especifique la ubicación del agente de Citrix ADM, donde debe ejecutarse el script. Por ejemplo: `/sh/var/demo.sh $source $failureobj`.

   c) Seleccione **Anexar salida** y **Anexar errores**

   > **Nota**
   >
   > Puede habilitar las opciones **Anexar salida** y **Anexar errores** si quiere almacenar la salida y los errores generados (si los hay) al ejecutar un script en los archivos de registros del servidor Citrix ADM. Si no habilita estas opciones, Citrix ADM descarta todas las salidas y errores generados al ejecutar el script.

   d) Haga clic en **Crear**.
8. En la página **Agregar acción de evento**, haga clic en **Aceptar**.

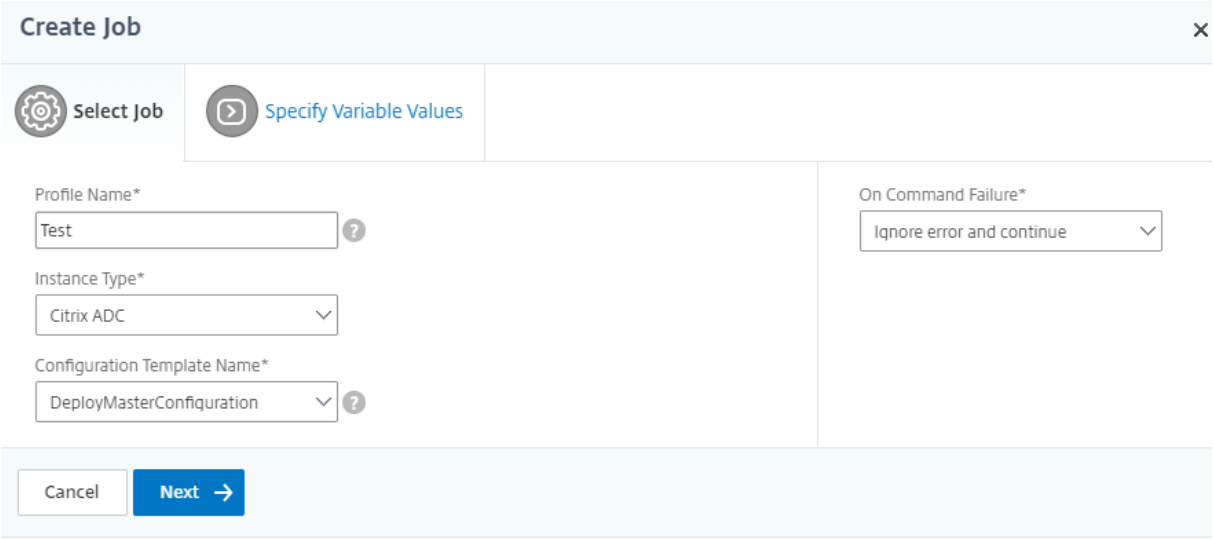


> **Nota**
>
> Puede habilitar las opciones **Anexar salida** y **Anexar errores** si quiere almacenar la salida y los errores generados (si los hay) al ejecutar un script en los archivos de registros del servidor Citrix ADM. Si no habilita estas opciones, Citrix ADM descarta todas las salidas y errores generados al ejecutar el script.

Para establecer la acción Ejecutar trabajo

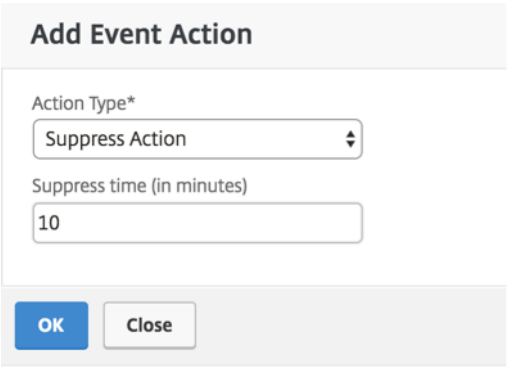
Al crear un perfil con trabajos de configuración, un trabajo se ejecuta como un trabajo integrado o personalizado para Citrix ADC, y las instancias SDX de Citrix ADC para eventos y alarmas que coinciden con los criterios de filtro que ha especificado.

1. En **Acciones de regla de evento**, haga clic en **Agregar acción** y seleccione **Ejecutar acción de trabajo** en la lista **Tipo de acción**.
2. Cree un perfil con el trabajo que quiera ejecutar cuando los eventos cumplan con los criterios de filtro definidos.
3. Al crear un trabajo, especifique un nombre de perfil, el tipo de instancia, la plantilla de configuración y la acción que quiere realizar si fallan los comandos del trabajo.
4. En función del tipo de instancia seleccionado y de la plantilla de configuración elegida, especifique los valores de las variables y haga clic en **Finalizar** para crear el trabajo.



Para establecer la acción de supresión

Al elegir la **acción de evento Suprimir** acción, puede configurar un período de tiempo, en minutos, para el que se suprime o elimina un evento. Puede suprimir el evento durante un mínimo de 1 minuto.



Para configurar notificaciones de Slack desde Citrix ADM

Configure el canal Slack requerido proporcionando el nombre del perfil y la URL de webhook en la GUI de Citrix ADM. Las notificaciones de eventos se envían a este canal. Puede configurar varios canales de Slack para recibir estas notificaciones

1. En Citrix ADM, vaya a **Infraestructura > Eventos > Reglas**y haga clic en **Agregar** para crear una regla.
2. En la página **Crear regla**, defina los parámetros de la regla, como la gravedad y la categoría. Seleccione las instancias y también los objetos de error que quiera supervisar.
3. En **Acciones de reglas de eventos**, haga clic en **Agregar acción**. A continuación, selecciona **Enviar notificaciones de Slack** en la lista de **tipos de acciones** y selecciona **Lista de perfiles de Slack.**
4. También puede agregar una lista de perfiles de Slack haciendo clic en **Agregar** junto al campo **Lista de perfiles de Slack** .
5. Escriba los siguientes parámetros para crear una lista de perfiles:
    a) **Nombre del perfil**. Escriba un nombre para la lista de perfiles que se configurará en Citrix ADM
    b) **Nombre del canal**. Escribe el nombre del canal de Slack al que se van a enviar las notificaciones de eventos.
    c) **URL del webhook**. Escribe la URL del Webhook del canal que has introducido anteriormente. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal y todas las notificaciones de eventos se envían a esta URL para que se publiquen en el canal de Slack designado. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Haga clic en **Crear** y haga clic en **Aceptar** en la ventana **Agregar acción de evento**.

> **Nota**
>
> También puede agregar los perfiles de Slack yendo a **Cuenta** > **Notificaciones** > **Perfiles de Slack**. Haga clic en **Agregar** y cree el perfil como se describe en la sección anterior.

Puedes ver el estado de los perfiles de Slack que has creado.

La regla de evento se crea ahora con filtros apropiados y acciones de regla de evento bien definidas.

Para establecer notificaciones de PagerDuty desde Citrix ADM

Puede agregar un perfil de PagerDuty como opción en Citrix ADM para supervisar las notificaciones de incidentes en función de las configuraciones de PagerDuty. PagerDuty le permite configurar notificaciones a través de correo electrónico, SMS, notificaciones push y llamadas telefónicas en un número registrado.

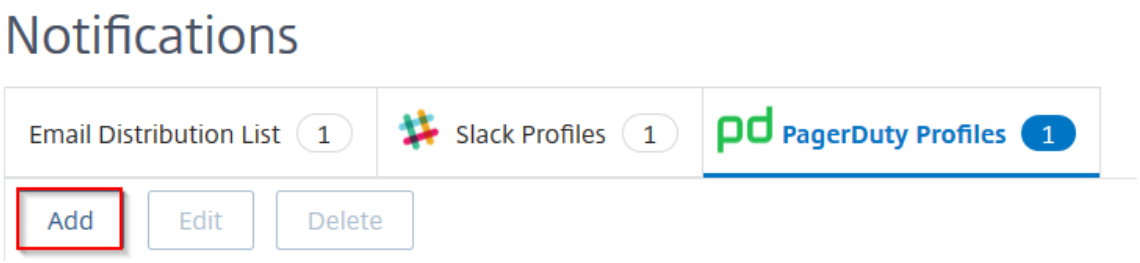
Antes de agregar un perfil de PagerDuty en Citrix ADM, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para obtener más información, consulte la documentación de PagerDuty.

Puede seleccionar su perfil de PagerDuty como una de las opciones para recibir notificaciones de las siguientes funciones:

- **Eventos** : lista de eventos que se generan para las instancias de Citrix ADC.
- **Licencias** : lista de licencias que están actualmente activas, a punto de caducar, etc.
- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias Citrix ADC.

Para agregar un perfil de PagerDuty en Citrix ADM:

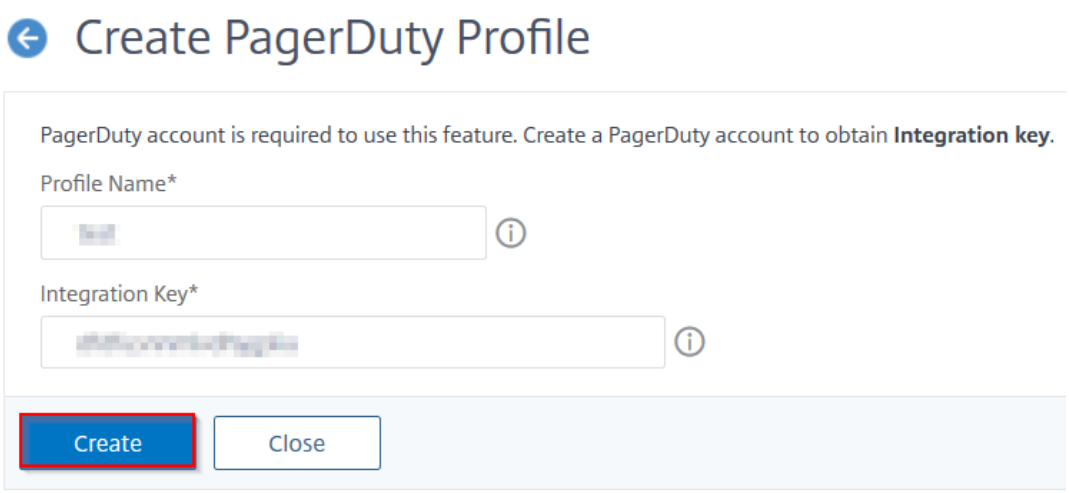
1. Inicie sesión en Citrix ADM mediante credenciales de administrador.
2. Vaya a **Cuenta** > **Notificaciones** > **Perfiles de PagerDuty**.
3. Haga clic en **Agregar** para crear un perfil.



4. En la página Crear Perfil de PagerDuty:
   a) Proporcione un nombre de perfil de su elección.
   b) Introduzca la **clave de integración**.

Puede obtener la clave de integración en su portal de PagerDuty.

c) Haga clic en **Crear**.



Caso de uso:

Considere un caso que:

- quiere enviar notificaciones a su perfil de PagerDuty.
- han configurado la llamada telefónica como una opción en PagerDuty para recibir notificaciones.
- quiere recibir alertas de llamadas telefónicas para eventos de Citrix ADC.

Para llevar a cabo la configuración:

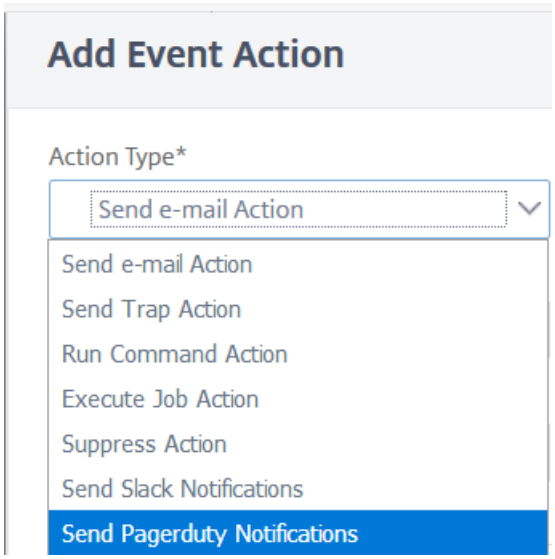
a) Diríjase a **Eventos** > **Reglas**

b) En la página **Crear regla**, configure todos los demás parámetros para crear una regla.

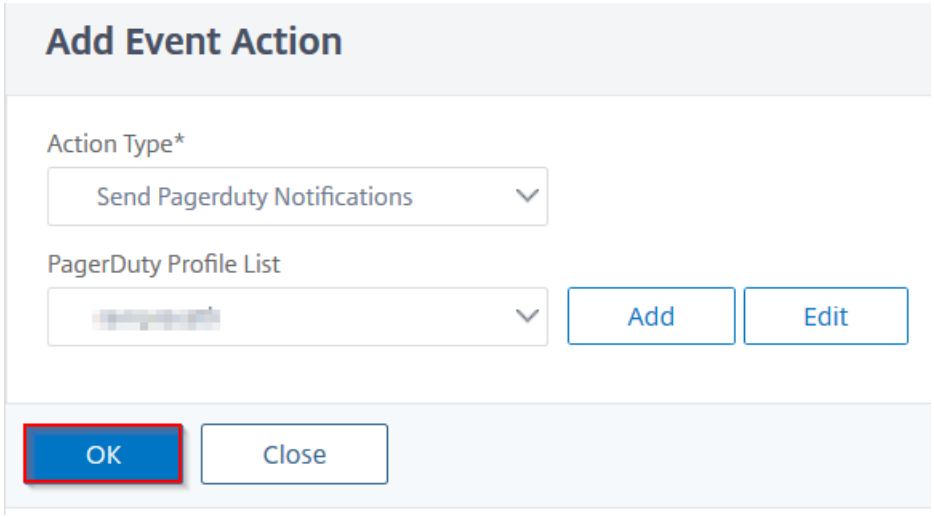
c) En **Crear acciones de regla**, haga clic en **Agregar acción**.

Aparece la página **Agregar acción de evento** .

i. En **Tipo de acción**, seleccione **Enviar notificaciones de tareas de pager.**



ii. Seleccione su perfil de PagerDuty y haga clic en **Aceptar**.



Una vez completada la configuración, siempre que se genere un nuevo evento para la instancia de Citrix ADC, recibirá una llamada telefónica. Desde la llamada telefónica, puede decidir:

- Reconoce el evento
- Marcarlo como resuelto
- Escalar a otro miembro del equipo

Para generar automáticamente incidentes de ServiceNow desde Citrix ADM

Puede generar automáticamente incidentes de ServiceNow para eventos de Citrix ADM seleccionando el perfil de ServiceNow en la GUI de Citrix ADM. Debe elegir el perfil de **ServiceNow** en Citrix ADM para configurar una regla de eventos.

Antes de configurar una regla de eventos para generar automáticamente los incidentes de ServiceNow, integre el Citrix ADM con la instancia de ServiceNow. Para obtener más información, consulte Configurar el adaptador ITSM para ServiceNow.

Para configurar una regla de evento, vaya a **Eventos** > **Reglas**.

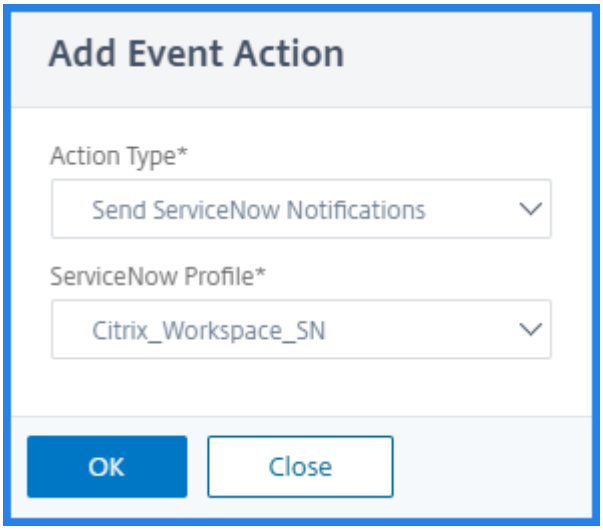
1. En la página **Crear regla**, configure todos los demás parámetros para crear una regla.
2. En **Crear acciones de regla**, haga clic en **Agregar acción**.

   Aparece la página **Agregar acción de evento** .

   a) En **Tipo de acción**, seleccione **Enviar notificaciones de ServiceNow**.

   b) En el **perfil de ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.

   c) Haga clic en **Aceptar**.



Modificar la gravedad reportada de los eventos que se producen en instancias de Citrix ADC

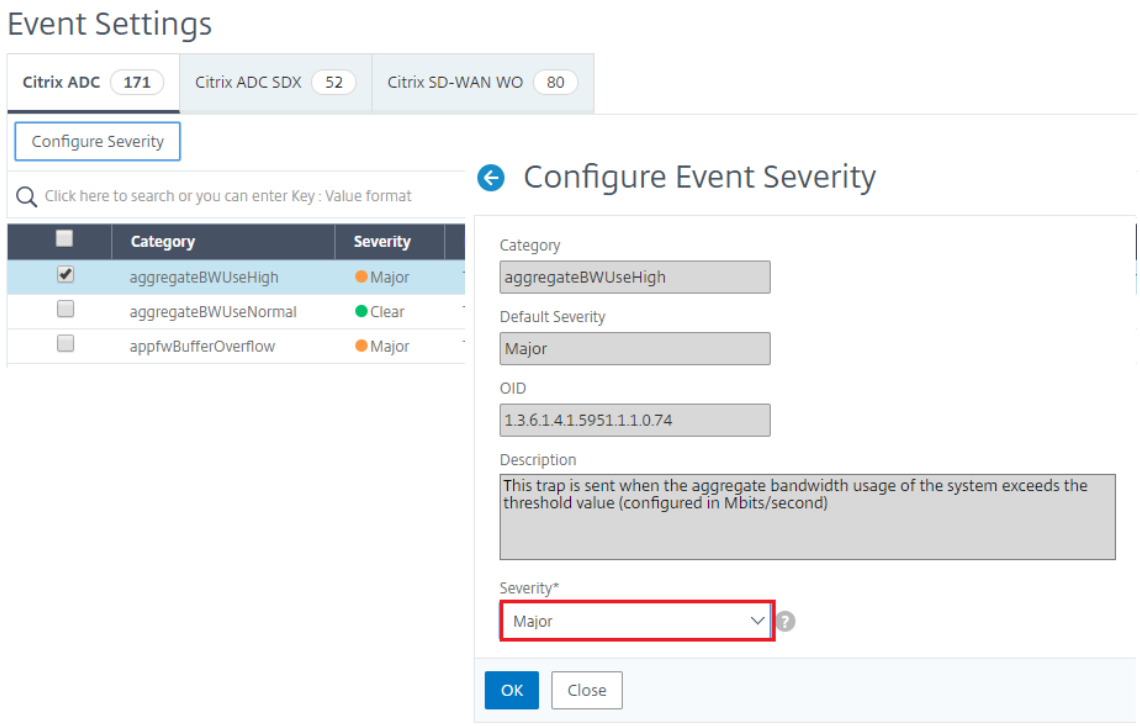
November 16, 2022

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 del evento**.
2. Haga clic en la ficha del tipo de instancia de Citrix ADC 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**.



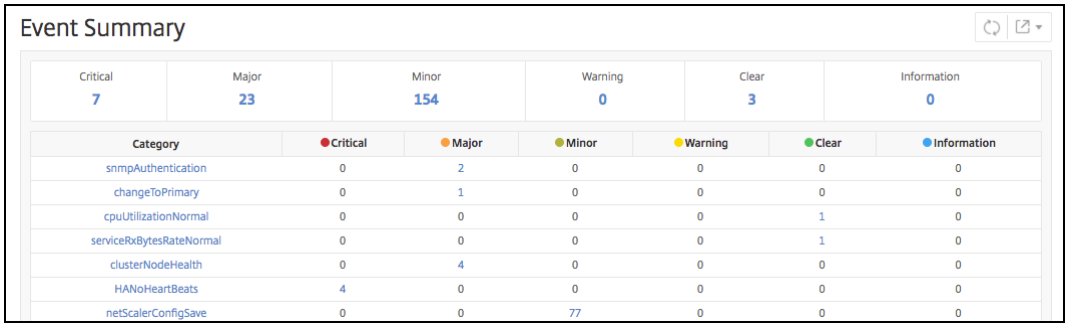
Ver resumen de eventos

November 16, 2022

Ahora puede ver una página de resumen de eventos para supervisar los eventos y las capturas recibidos en su Citrix ADM. Diríjase a **Infraestructura > Eventos**. La página Resumen de Eventos muestra la siguiente información en formato de tabla:

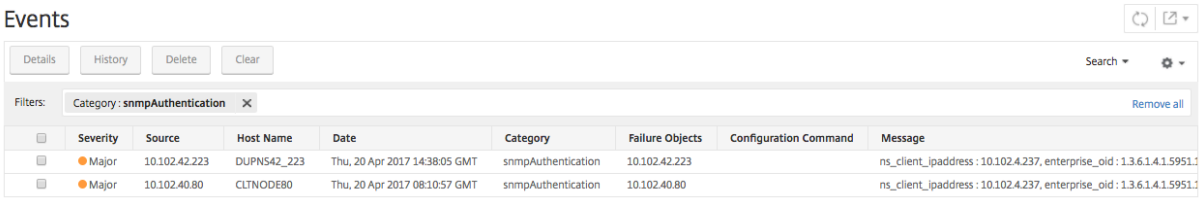
- **Resumen de todos los eventos recibidos por Citrix ADM**. Los eventos se enumeran por categoría y las diferentes grados de gravedad se muestran en diferentes columnas: Crítico, Principal, Menor, Advertencia, Borrar e Información. Por ejemplo, se produce un evento crítico cuando una instancia de Citrix Application Delivery Controller (Citrix ADC) deja de funcionar y deja de enviar información al Citrix ADM. Durante el evento, se envía una notificación a un administrador en la que se explica el motivo por el que la instancia está inactiva, el tiempo du-

rante 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 instancias de Citrix ADC a Citrix ADM tiene asignada una gravedad, pero como administrador de red, puede especificar su gravedad en la GUI de Citrix ADM.

Si hace clic en un tipo de categoría o una captura, se le lleva a la página **Eventos**, en la que se preseleccionan filtros como Categoría y Gravedad. Esta página muestra más información sobre el evento, como la dirección IP y el nombre de host de una instancia de Citrix ADC, la fecha en la que se recibió la captura, la categoría, los objetos de error, la ejecución del comando de configuración y la notificación del mensaje.



Puede configurar el número de días entre 1 y 40, para los que quiere ver los eventos en Citrix ADM. Por ejemplo, si selecciona 30 días, Citrix ADM muestra los eventos durante 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 especificar todos los días que quiere programar el informe separados por comas.

Mostrar severidades de eventos y detalles de capturas SNMP

November 16, 2022

Al crear un evento y su configuración en Citrix ADM, puede verlo 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 (Citrix ADC) agregadas a su servidor Citrix ADM con todo detalle en el panel de infraestructura.

En el panel Infraestructura, ahora puede enmascarar valores irrelevantes para que pueda ver y supervisar con más facilidad información como eventos por severidades, estado, tiempo de actividad, modelos y versión de instancias de Citrix ADC en detalle.

Por ejemplo, los eventos con un nivel de gravedad **crítico** pueden ocurrir con poca frecuencia. Sin embargo, cuando se produzcan estos eventos críticos en la red, es posible que quiera investigar más a fondo, solucionar problemas y supervisar dónde y cuándo ocurrió el evento. Si selecciona todos los niveles de gravedad excepto Crítico, el gráfico muestra solo las ocurrencias de eventos críticos. Además, al hacer clic en el gráfico, 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 Citrix ADC 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.

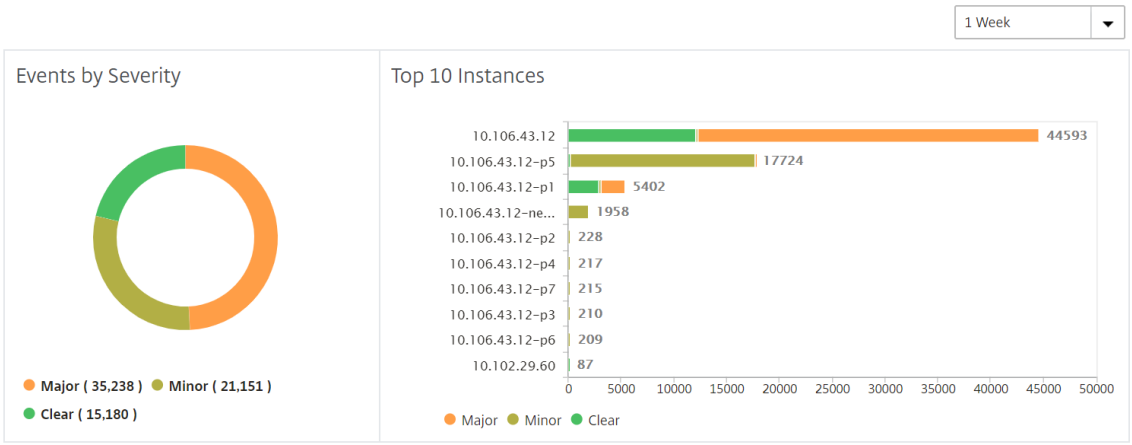
Para seleccionar eventos específicos por gravedad en Citrix ADM:

1. Inicie sesión en Citrix ADM 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.

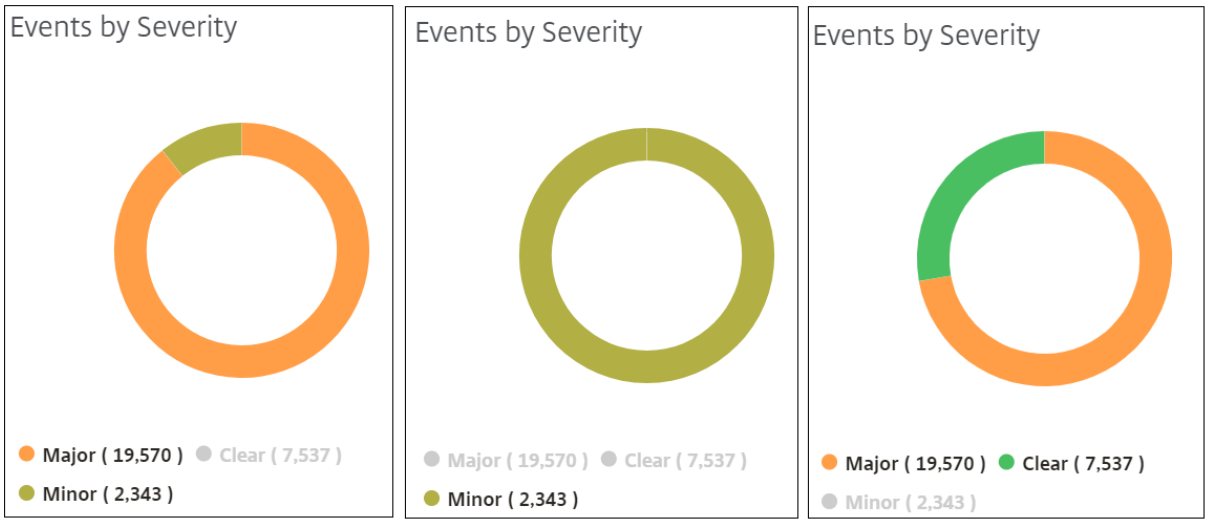


4. El gráfico de donut **Eventos por gravedad** muestra una representación visual de todos los eventos según su gravedad. Los diferentes tipos de eventos se representan como secciones de colores diferentes, y la longitud de cada sección corresponde al número total de eventos de ese tipo de gravedad.

5. Puede hacer clic en cada sección del gráfico de donut para mostrar la página de **eventos basados en gravedad** correspondiente, que muestra los siguientes detalles de la gravedad seleccionada para la duración seleccionada:

   - Origen de instancia
   - Datos del evento
   - Categoría de eventos generados por la instancia de Citrix ADC
   - 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. Puede alternar los tipos de gravedad para ver y supervisar la gravedad elegida con mayor facilidad.

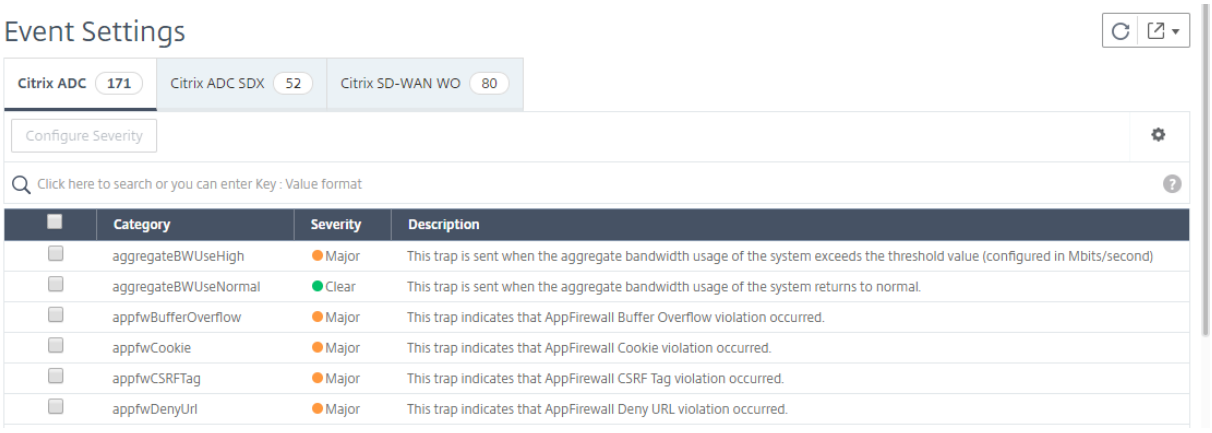


Para ver los detalles de la captura SNMP de Citrix ADC en Citrix ADM:

Ahora puede ver los detalles de cada captura SNMP recibida de sus instancias de Citrix ADC administradas en Citrix ADM en la página **Configuración de eventos** . Vaya a **Infraestructura > Eventos > Configuración del evento**. 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, un evento con la categoría de captura **monRespTimeoutBelowThresh**, la descripción de la captura se muestra como “Esta captura se envía cuando el tiempo de espera de respuesta para un sondeo de monitor vuelve a la normalidad, menor que el umbral establecido. “



Ver y exportar mensajes de syslog

November 16, 2022

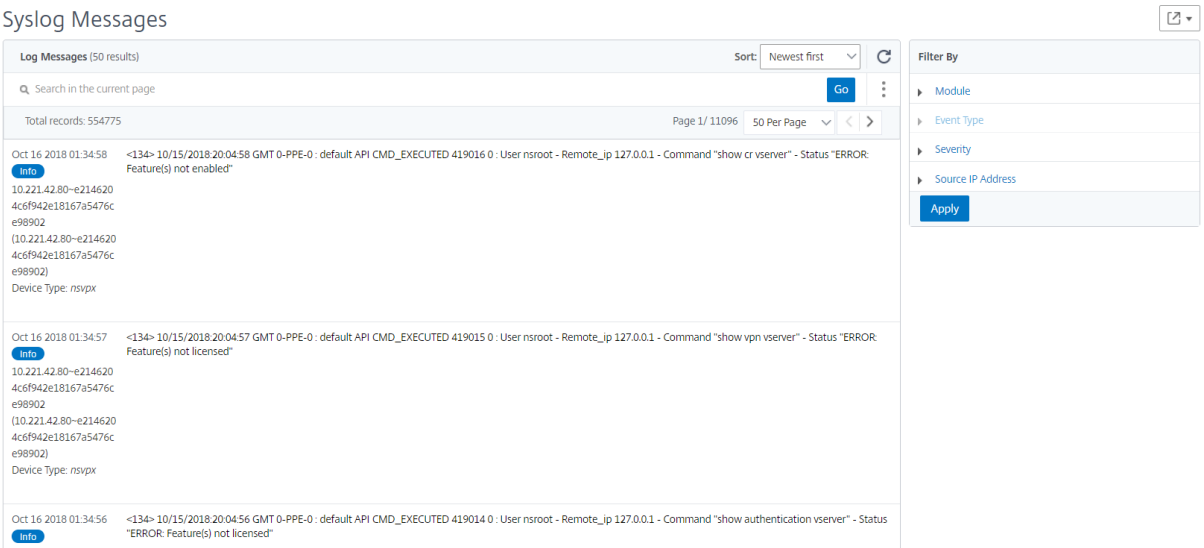
Puede ver los mensajes de syslog sin iniciar sesión en Citrix ADM, programando una exportación de todos los mensajes de syslog recibidos en el servidor. Puede exportar los mensajes de syslog que se generan en las instancias de Citrix Application Delivery Controller (Citrix ADC) en formatos PDF, CSV, 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 Citrix ADC. Para ver los mensajes, debe configurar las instancias para redirigir los mensajes de syslog al servidor Citrix ADM. 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.

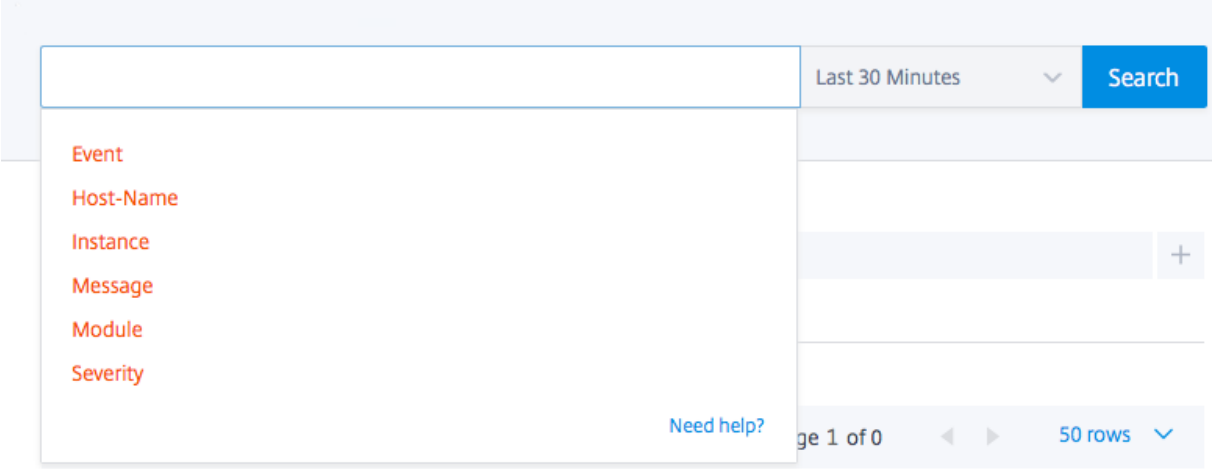
Para ver el visor de Syslog, vaya a **Infraestructura > Eventos > Mensajes de Syslog**. Elija los filtros adecuados para ver los mensajes de registro del sistema.



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 ADC presentes en el software Citrix ADM, desde la GUI de Citrix ADM, vaya a **Infraestructura > Eventos > Mensajes de syslog**. Las nuevas categorías de filtros son instancia, módulo, evento, gravedad y mensaje.



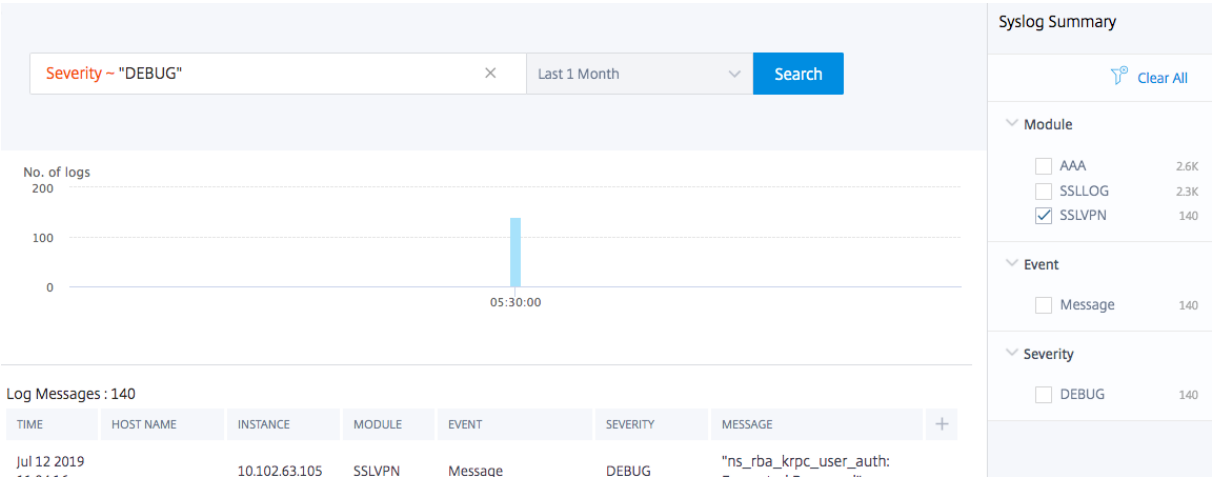
Para buscar todos los mensajes de registro de auditoría del sistema Citrix ADM presentes en el software Citrix ADM, desde la GUI de Citrix ADM, vaya a **Configuración > Mensajes de registro de auditoría**. Las nuevas categorías de filtros son instancia, módulo, evento, gravedad y mensaje.

Para buscar mensajes de registro de auditoría para todas las aplicaciones presentes en Citrix ADM, desde la GUI de Citrix ADM, vaya a **Infraestructura > Funciones de red > Auditoría**.

Para buscar los mensajes del registro de auditoría de una aplicación específica en Citrix ADM, desde la GUI de Citrix ADM, vaya a **Aplicación > Panel de control** y seleccione el servidor virtual en el que quiere 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.

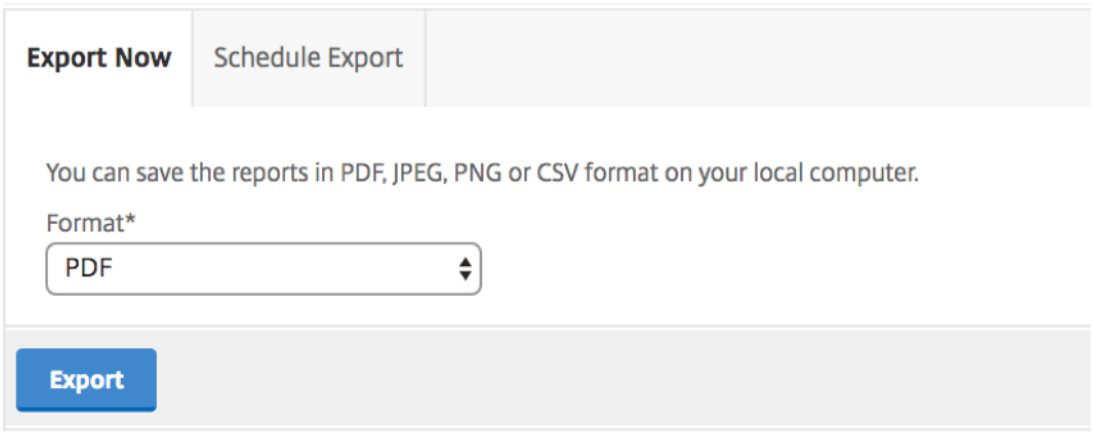
A continuación, agregue el término de búsqueda. Para algunas categorías, se muestra una lista precompletada de términos de búsqueda. De forma predeterminada, el tiempo de búsqueda es de 1 día. Puede cambiar la hora y el intervalo de fechas haciendo clic en la flecha hacia abajo. Puede reducir aún más 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 Citrix ADM:

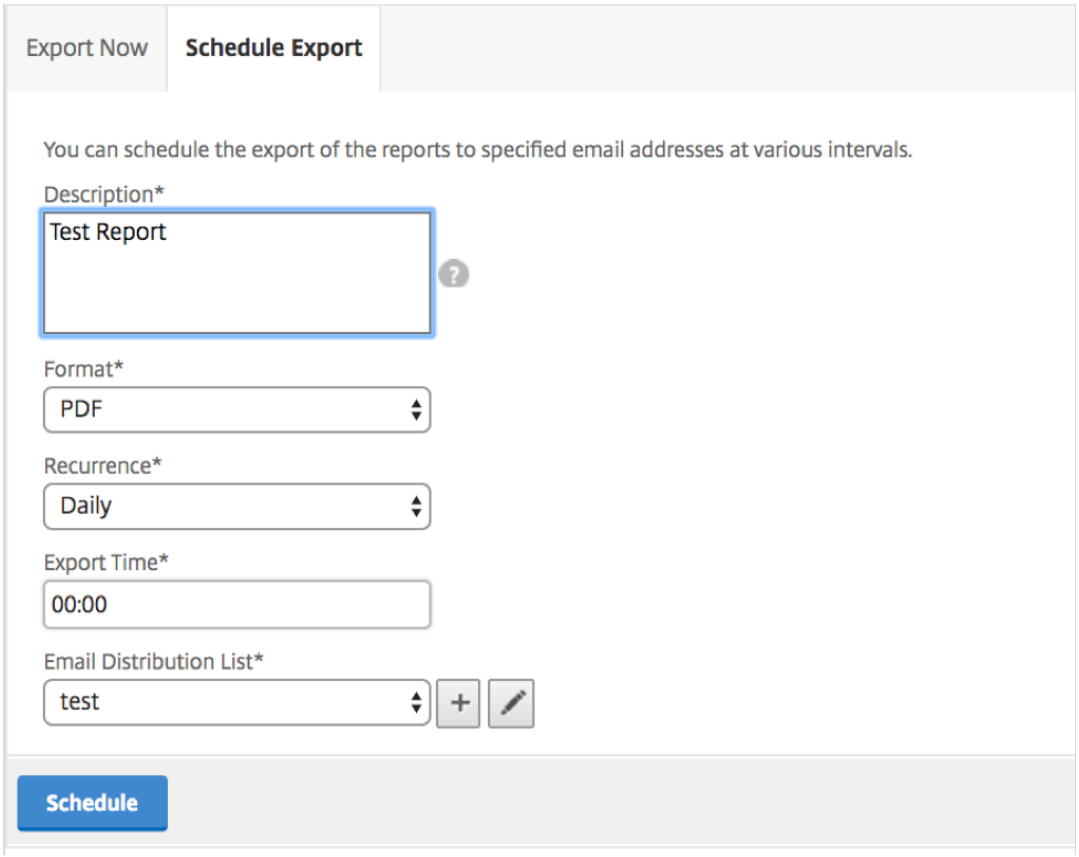
1. Vaya a **Infraestructura > Eventos > Mensajes de Syslog**.
2. En el panel derecho, haga clic en el botón Exportar situado en la esquina superior derecha de la página Mensajes de Syslog.
3. En **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.



Para programar la exportación del informe de mensajes de syslog mediante Citrix ADM:

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

November 16, 2022

Cuando se configura como un servidor syslog, Citrix ADM recibe todos los mensajes de syslog de las instancias configuradas de Citrix Application Delivery Controller (Citrix ADC). 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 Citrix ADM configurando algunos filtros. Citrix ADM elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de Citrix ADM y estos mensajes tampoco se almacenan en la base de datos de Citrix ADM del cliente.

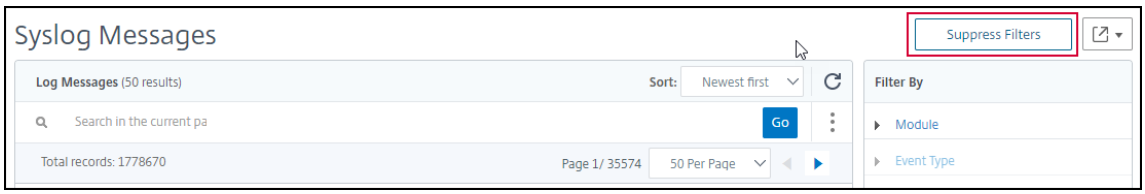
Puede suprimir algunos de los mensajes de syslog registrados que llegan a Citrix ADM configurando algunos filtros. Los dos filtros que se pueden utilizar para suprimir mensajes syslog son gravedad y facilidad. También puede suprimir los mensajes procedentes de una instancia concreta de Citrix ADC o de varias instancias. También puede proporcionar un patrón de texto para que Citrix ADM busque y suprima mensajes. Citrix ADM elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de Citrix ADM y estos mensajes tampoco se almacenan en la base de datos del cliente. Por lo tanto, se ahorra una buena cantidad de espacio en el servidor de almacenamiento.

Algunos casos de uso para suprimir los mensajes de syslog son los siguientes:

- Si quiere ignorar todos los mensajes de nivel de información, suprima el nivel 6 (informativo)
- Si solo quiere registrar las condiciones de error del firewall, suprima todos los niveles que no sean el nivel 3 (errores)

Supresión de mensajes de syslog mediante la creación de filtros

1. En Citrix ADM, vaya a **Infraestructura > Eventos > Mensajes de Syslog**.
2. Haga clic en **Suprimir filtros**.

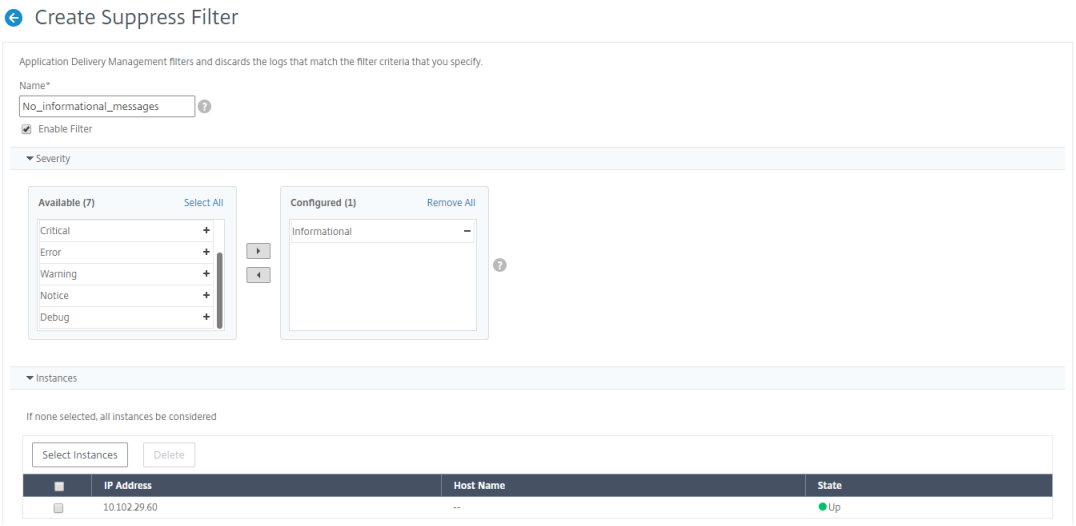


3. En la página **Suprimir filtros**, haga clic en **Agregar**.
4. En la página **Crear filtro de supresión**, actualice la siguiente información:
   a) **Nombre** : escriba un nombre para el filtro.

   > **Nota:**
   >
   > Si los diferentes usuarios tienen diferentes accesos a varias instancias de Citrix ADC, se deben crear diferentes filtros para diferentes instancias, ya que los usuarios solo pueden ver los filtros en los que tienen acceso a todas las instancias.

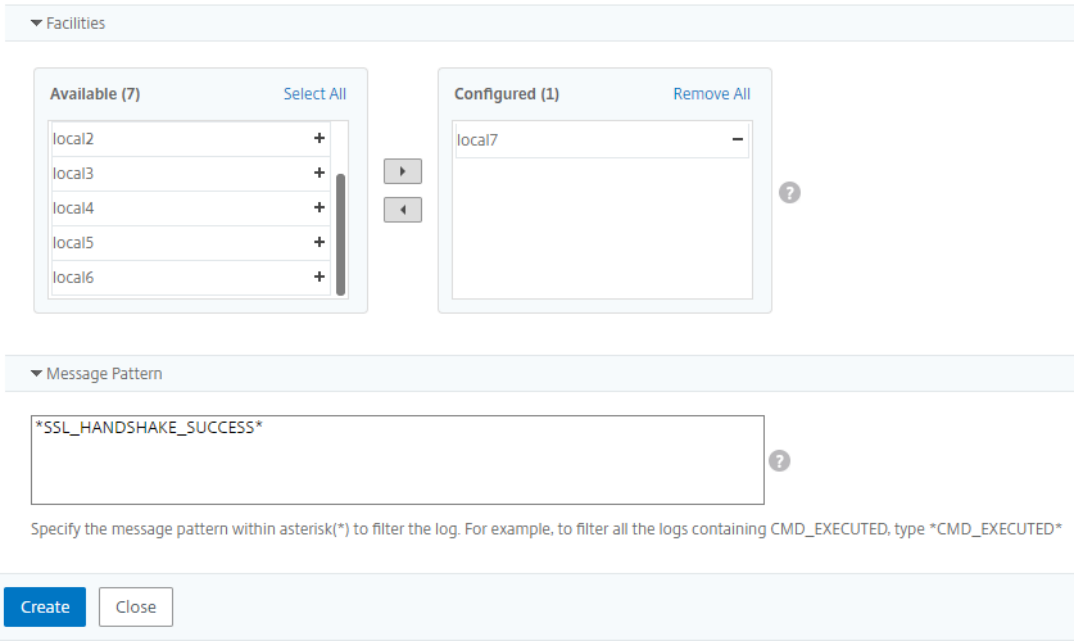
   b) **Gravedad** : seleccione y agregue los niveles de registro para los que debe suprimir los mensajes.
   Por ejemplo, si no quiere ver ningún mensaje informativo que llegue, puede seleccionar **Informativo** para suprimirlos.

c) **Instancias**: Seleccione las instancias Citrix ADC 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.

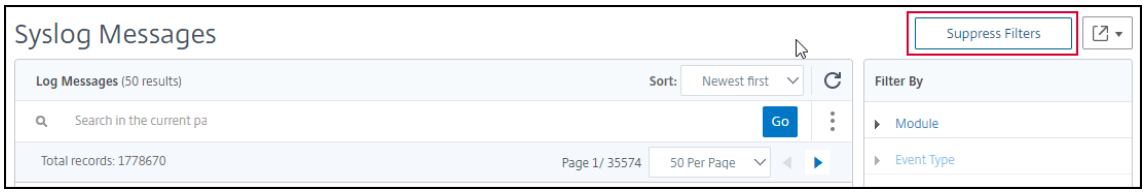
e) **Patrón de mensajes** : también puede escribir un patrón de texto rodeado de asteriscos (*) para suprimir los mensajes. En los mensajes se busca la cadena de patrón de texto y se suprimen los mensajes que contienen este patrón.



Inhabilitar el filtro

Para permitir que los mensajes se vean en Citrix ADM, debe inhabilitar el filtro.

1. Vaya a **Infraestructura > Eventos > Mensajes de Syslog**.
2. Haga clic en **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 deshabilitar el filtro.

Tablero SSL

November 16, 2022

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

Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

- De una autoridad de certificación autorizada (CA)
- Al generar un nuevo certificado SSL y una clave en el dispositivo Citrix ADC

Citrix ADM proporciona una vista centralizada de los certificados SSL instalados en todas las instancias administradas de Citrix ADC. En el panel de control de SSL, puede ver gráficos que le ayudan a rastrear los emisores de certificados, los puntos fuertes clave, los algoritmos de firma, los certificados caducados o no utilizados, etc. También puede ver la distribución de los protocolos SSL que se ejecutan en sus servidores virtuales y las claves que están habilitadas en ellos.

También puede configurar notificaciones para informarle cuando los certificados están a punto de caducar e incluir información sobre las instancias Citrix ADC que utilizan dichos certificados.

Puede vincular un certificado de instancia de Citrix ADC 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 utilizar un servidor Venafi Trust Protection Platform con Citrix ADM 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

November 16, 2022

Puede utilizar el panel de certificados SSL de Citrix ADM para ver gráficos que le ayuden 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:

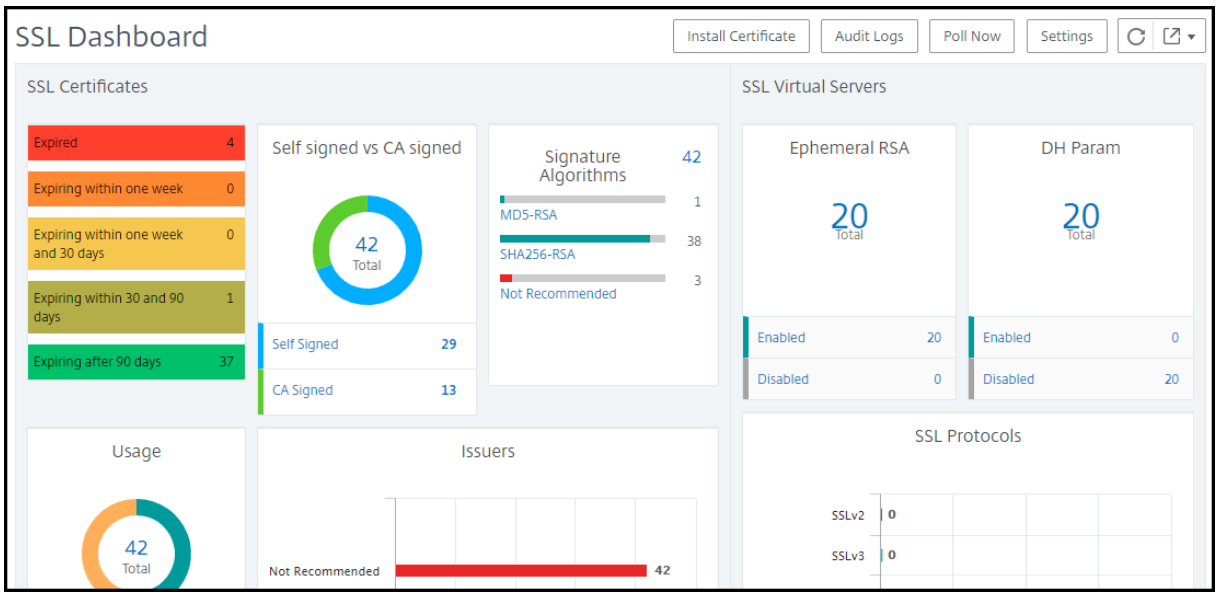
- Número de días después de los cuales caducan los certificados
- Número de certificados usados y no utilizados
- Número de certificados autofirmados y firmados por una CA
- Número de emisores
- algoritmos de firma
- Protocolos SSL
- Las 10 instancias principales por número de certificados en uso

Supervisar certificados SSL

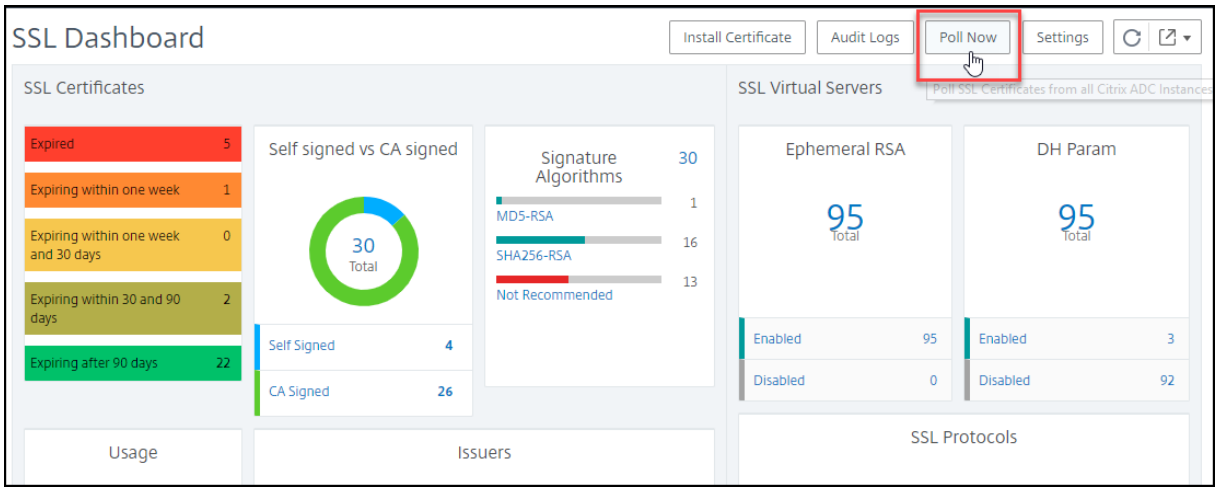
Puede utilizar el panel SSL de Citrix ADM para supervisar los certificados si su empresa tiene una directiva SSL en la que ha definido ciertos requisitos de certificado SSL, como todos los certificados deben tener una intensidad clave mínima de 2048 bits y una autoridad de CA de confianza debe autorizarlo.

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.

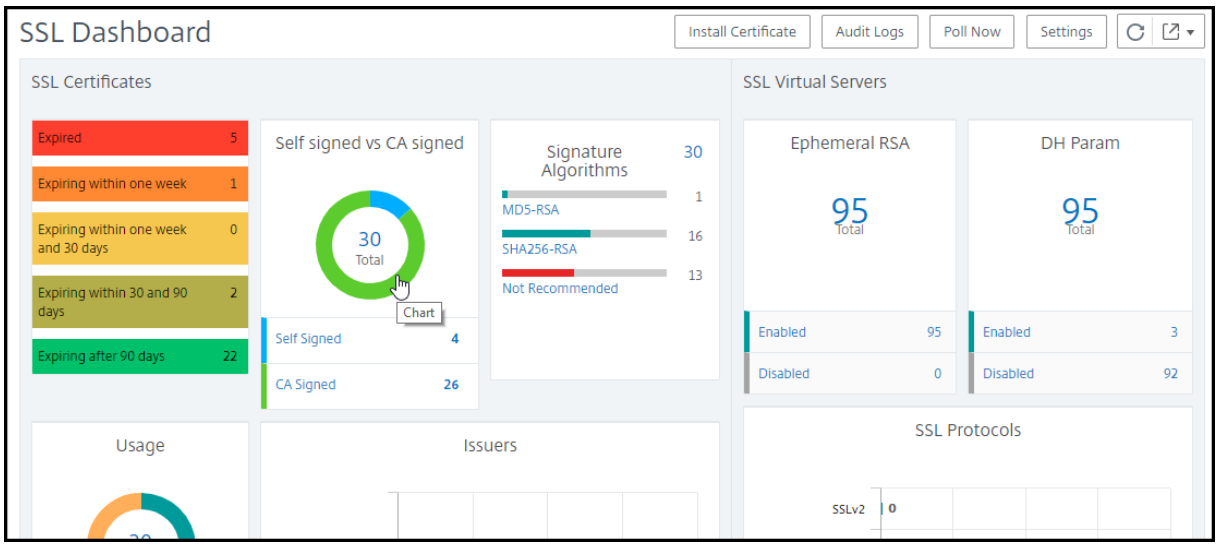
Para supervisar los certificados SSL en Citrix ADM, vaya a **Infraestructura > Panel de control SSL**.



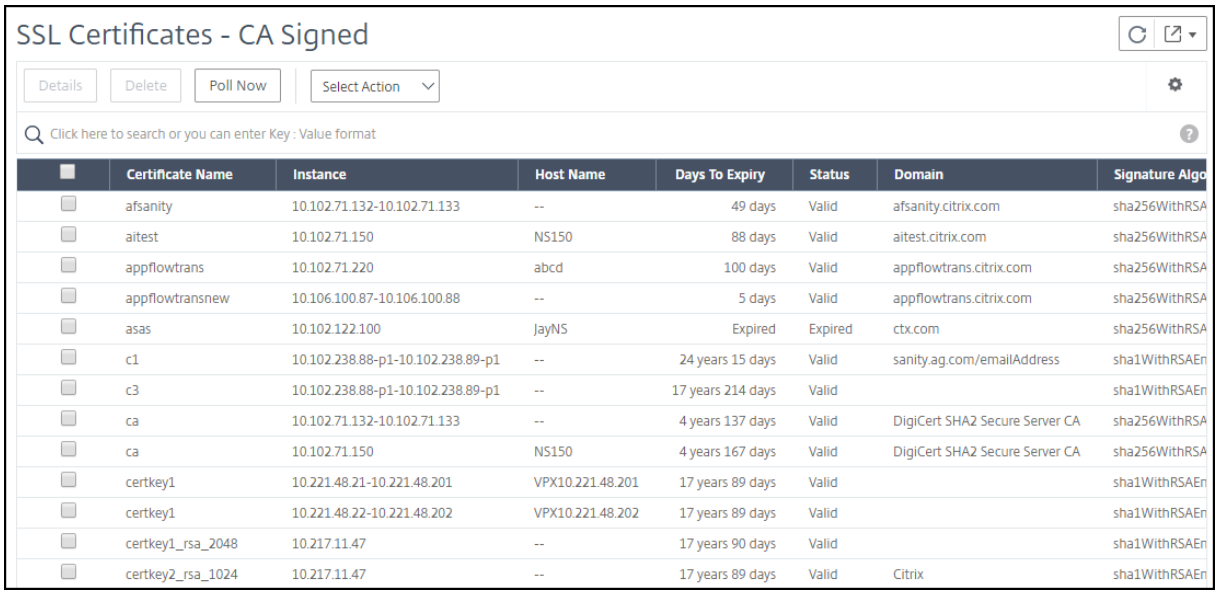
Citrix ADM le permite sondear certificados SSL y agregar todos los certificados SSL de las instancias inmediatamente a Citrix ADM. Para hacerlo, vaya a **Infraestructura > Panel de control SSL** y haga clic en **Sondear ahora**. Aparece la página **Encuesta ahora**, que presenta la opción de sondear todas las instancias de Citrix ADC en la red o sondear las instancias seleccionadas.



Puede usar el panel de control SSL de Citrix ADM para ver o supervisar los detalles de los certificados SSL, los servidores virtuales SSL y los protocolos SSL. Los números “totales” son hipervínculos, en los que puede hacer clic para mostrar detalles relacionados con certificados SSL, servidores virtuales SSL o protocolos SSL.



Por ejemplo, cuando un usuario hace clic en el número 30 en «Autofirmado vs. CA firmada" en la figura anterior, aparece una nueva ventana que muestra los detalles de los 30 certificados SSL en las instancias Citrix ADC.

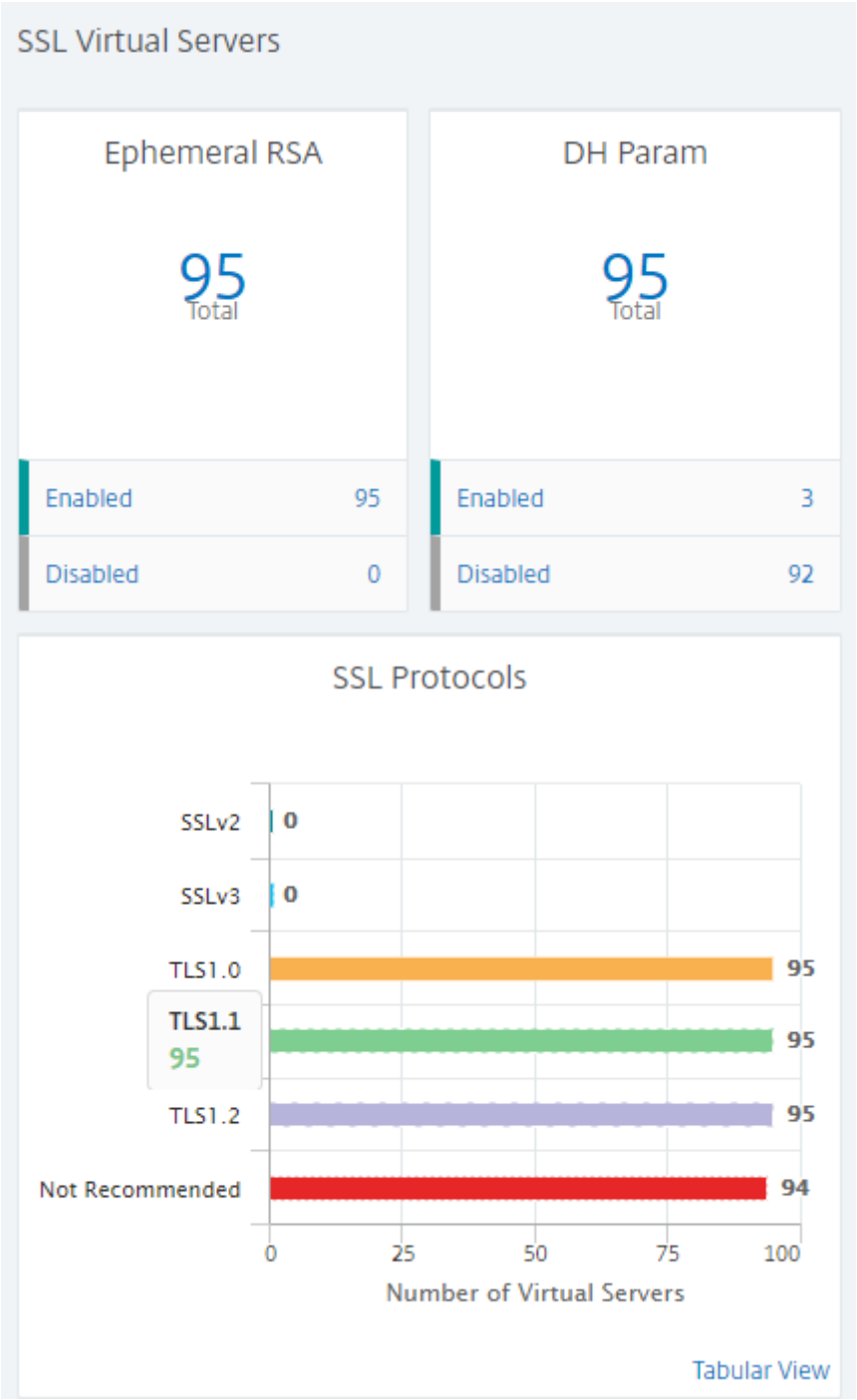


Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	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 de control SSL de Citrix ADM también muestra la distribución de los protocolos SSL que se ejecutan en los servidores virtuales. Como administrador, puede especificar los protocolos que 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 deshabilitar 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.

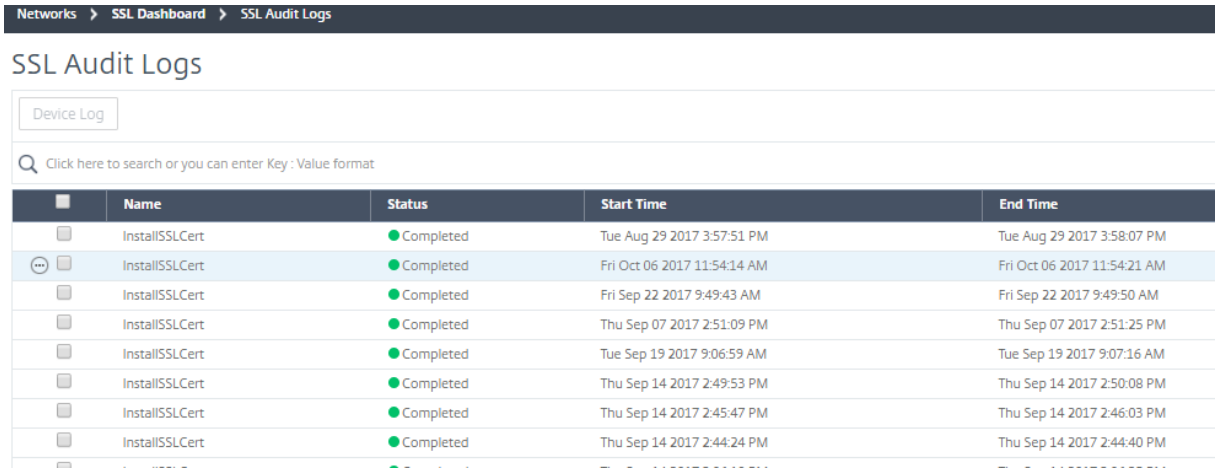


Ver registros de auditoría de certificados SSL

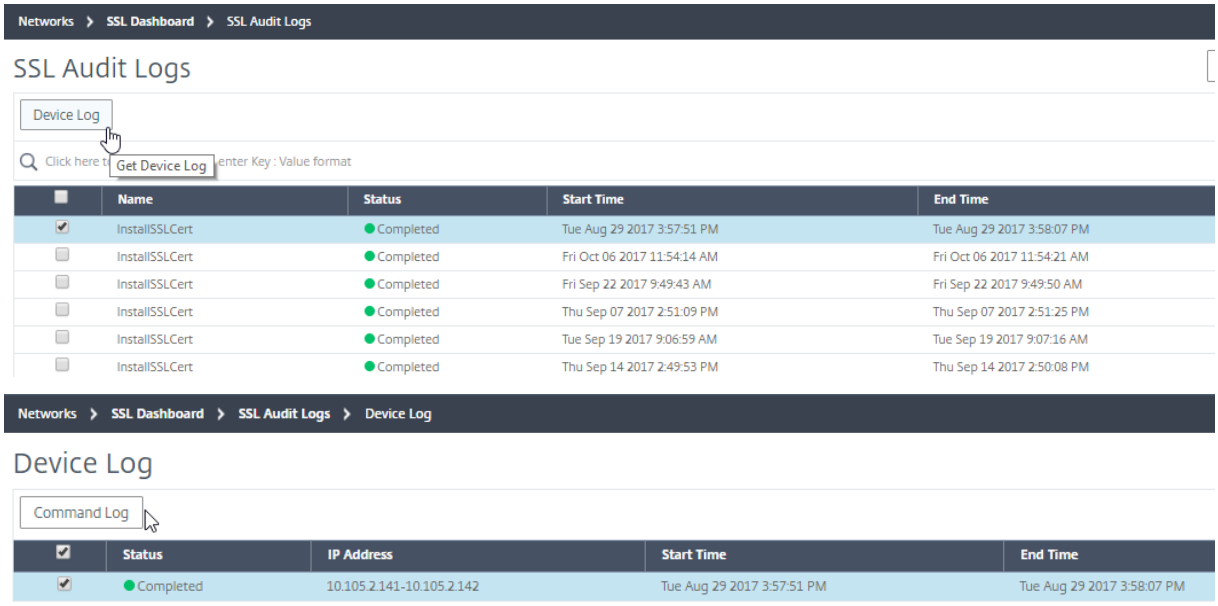
Ahora puede ver los detalles de registro de certificados SSL en Citrix ADM. Los detalles del registro muestran las operaciones realizadas con certificados SSL en Citrix ADM, como la instalación de certifi-

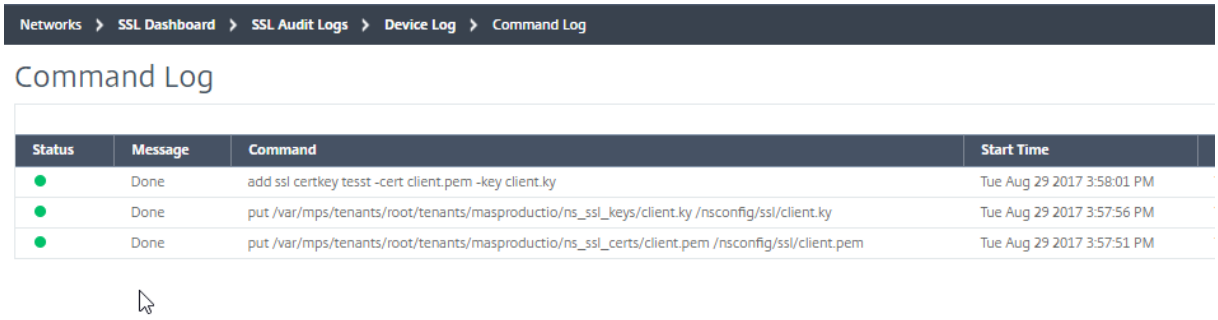
cados SSL, la vinculación y desvinculación de certificados SSL, la actualización de los certificados SSL y la eliminación de certificados SSL. La información del registro de auditoría es útil para supervisar los cambios en los certificados SSL realizados en una aplicación con varios propietarios.

Para ver un registro de auditoría de una operación concreta realizada en Citrix ADM mediante 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.



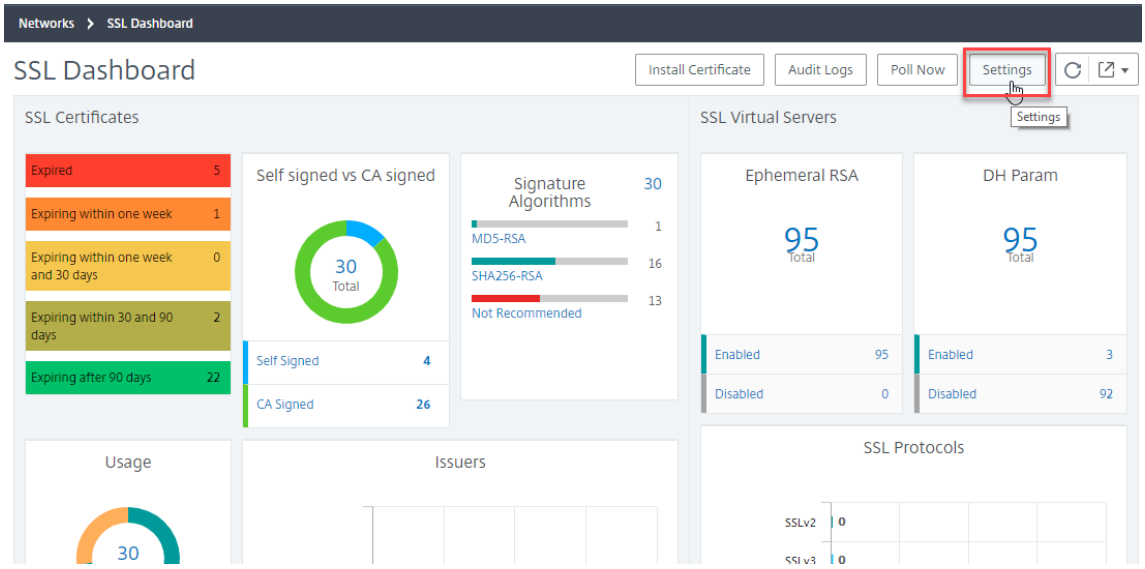


Excluir certificados Citrix ADC predeterminados en el panel SSL

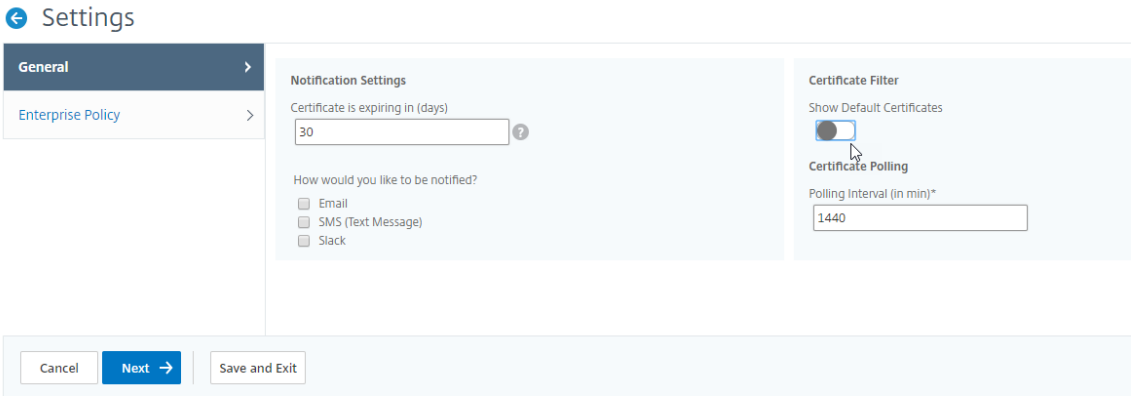
Citrix ADM le permite mostrar u ocultar los certificados predeterminados que aparecen en los gráficos del panel de control SSL según sus preferencias. De forma predeterminada, todos los certificados se muestran en el panel SSL, incluidos los certificados predeterminados.

Para mostrar u ocultar certificados predeterminados en el panel SSL:

1. Vaya a **Infraestructura > Panel SSL** en la GUI de Citrix ADM.
2. En la página **Tablero de SSL**, haga clic en **Configuración**.



3. En la página **Configuración**, seleccione **General**.
4. En la sección **Filtro de certificados**, inhabilite **Mostrar certificados predeterminados** y seleccione **Guardar y salir**.



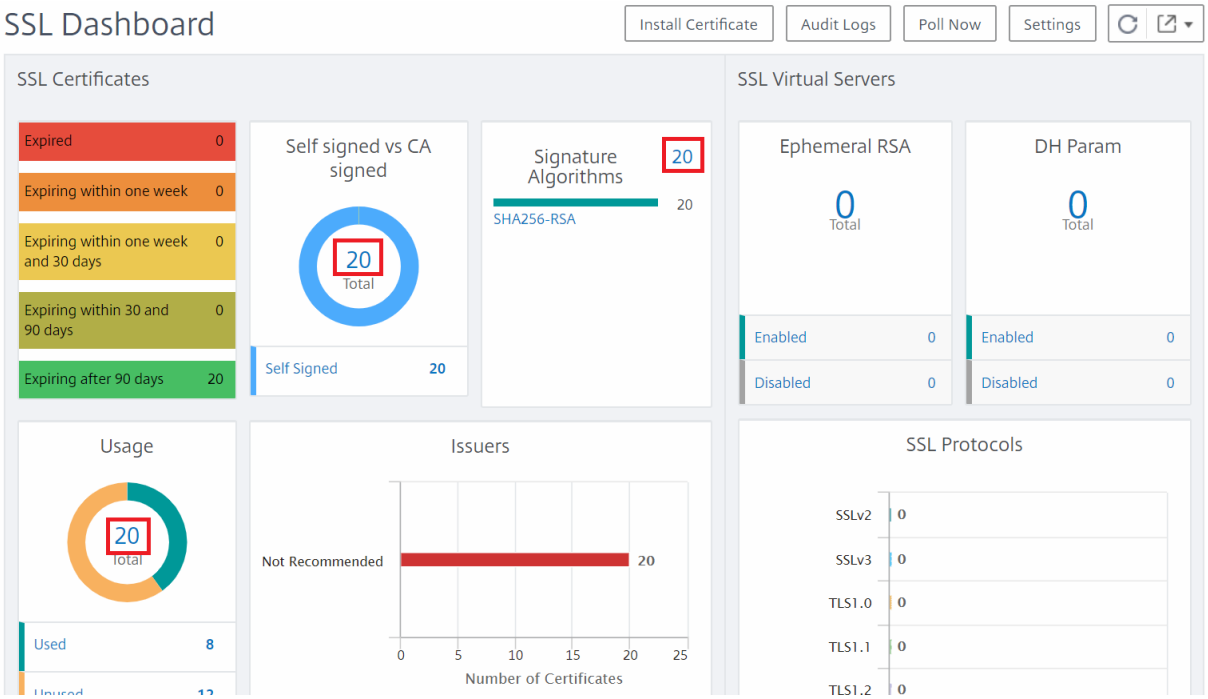
Descargar certificados SSL

Los certificados SSL se deben administrar de forma individual por instancia. Citrix ADM 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 SSL** en la GUI de Citrix ADM.
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**, haga clic en el certificado que quiera descargar. Por ejemplo, quiere descargar el que caduca en la próxima semana.
2. En el cuadro de lista **Seleccionar acción**, selecciona **Descargar**.
3. 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 especificar todos los días que quiere programar el informe separados por comas.

Configurar notificaciones para la caducidad del certificado SSL

November 16, 2022

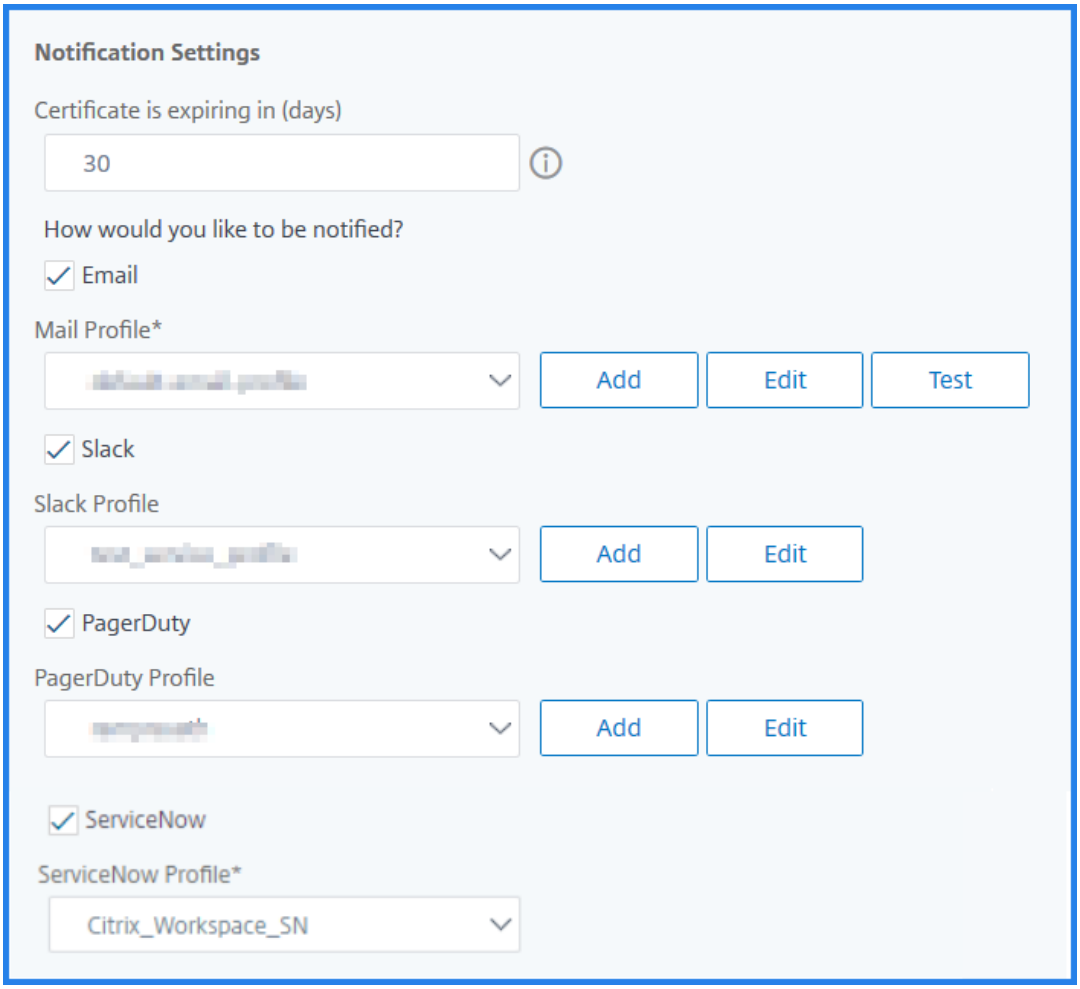
Como administrador de seguridad, puede configurar las notificaciones cuando los certificados estén a punto de caducar e incluir información sobre qué instancias de Citrix ADC utilizan esos certificados. Al habilitar las notificaciones, puede renovar sus certificados SSL a tiempo.

Por ejemplo, puede configurar una notificación por correo electrónico para que se envíe una lista de distribución por correo electrónico 30 días antes de la fecha de caducidad del certificado.

Para configurar notificaciones desde Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Panel 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 Citrix Cloud ITSM Adapter esté configurado para ServiceNow e integrado con Citrix ADM. Para obtener más información, consulte Integrar Citrix ADM con la instancia de ServiceNow.



6. Haga clic en **Guardar y salir**.

Actualizar un certificado instalado

November 16, 2022

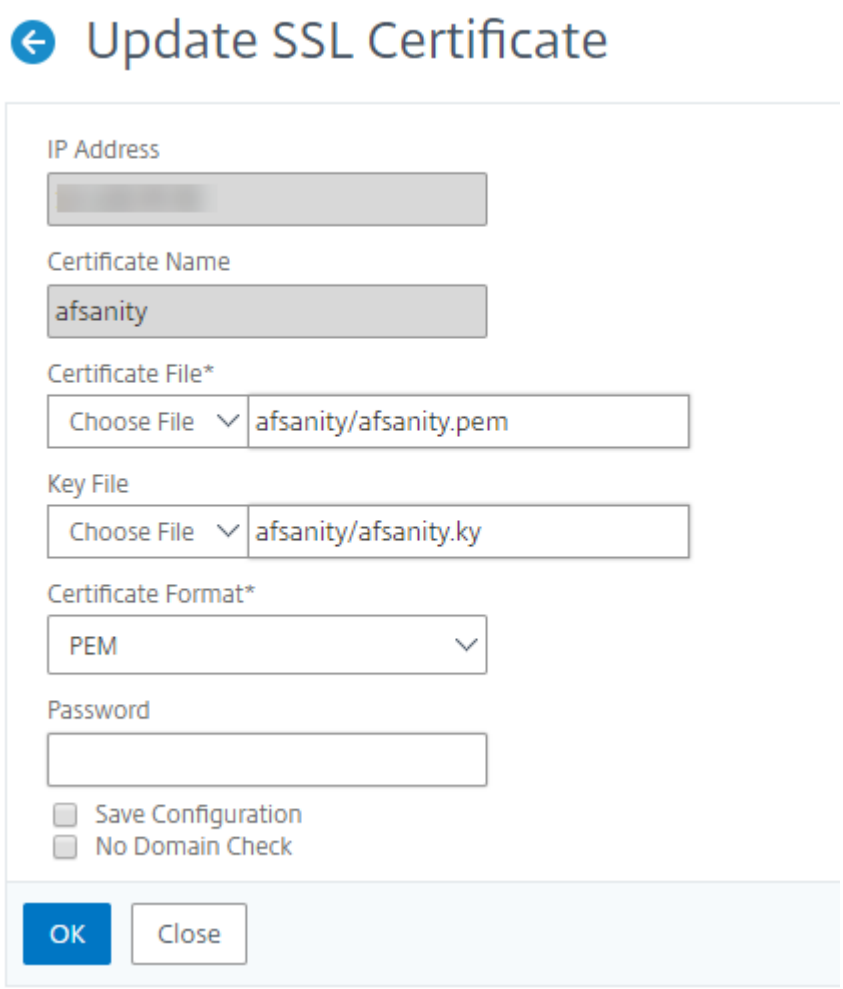
Tras recibir un certificado renovado de la autoridad de certificación (CA), puede actualizar los certificados existentes de Citrix ADM sin necesidad de iniciar sesión en instancias individuales de Citrix ADC.

Para actualizar un certificado SSL, una clave o ambos desde Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Panel SSL**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. En la página **Certificados SSL**, seleccione un certificado y haga clic en **Actualizar**. También

puede hacer clic en el certificado SSL para ver sus detalles y, a continuación, haga clic en **Actualizar** en la esquina superior derecha de la página **Certificado SSL**.

4. En la página **Actualizar el certificado SSL**, realice las modificaciones necesarias en el certificado, la clave o ambos y haga clic en **Aceptar**.



Instalar certificados SSL en una instancia de Citrix ADC

November 16, 2022

Antes de instalar certificados SSL en instancias Citrix ADC, 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 Citrix ADC:

También puede importar un certificado de una instancia de Citrix ADC elegida y aplicarlo a otras instancias de Citrix ADC de destino desde la GUI de Citrix ADM.

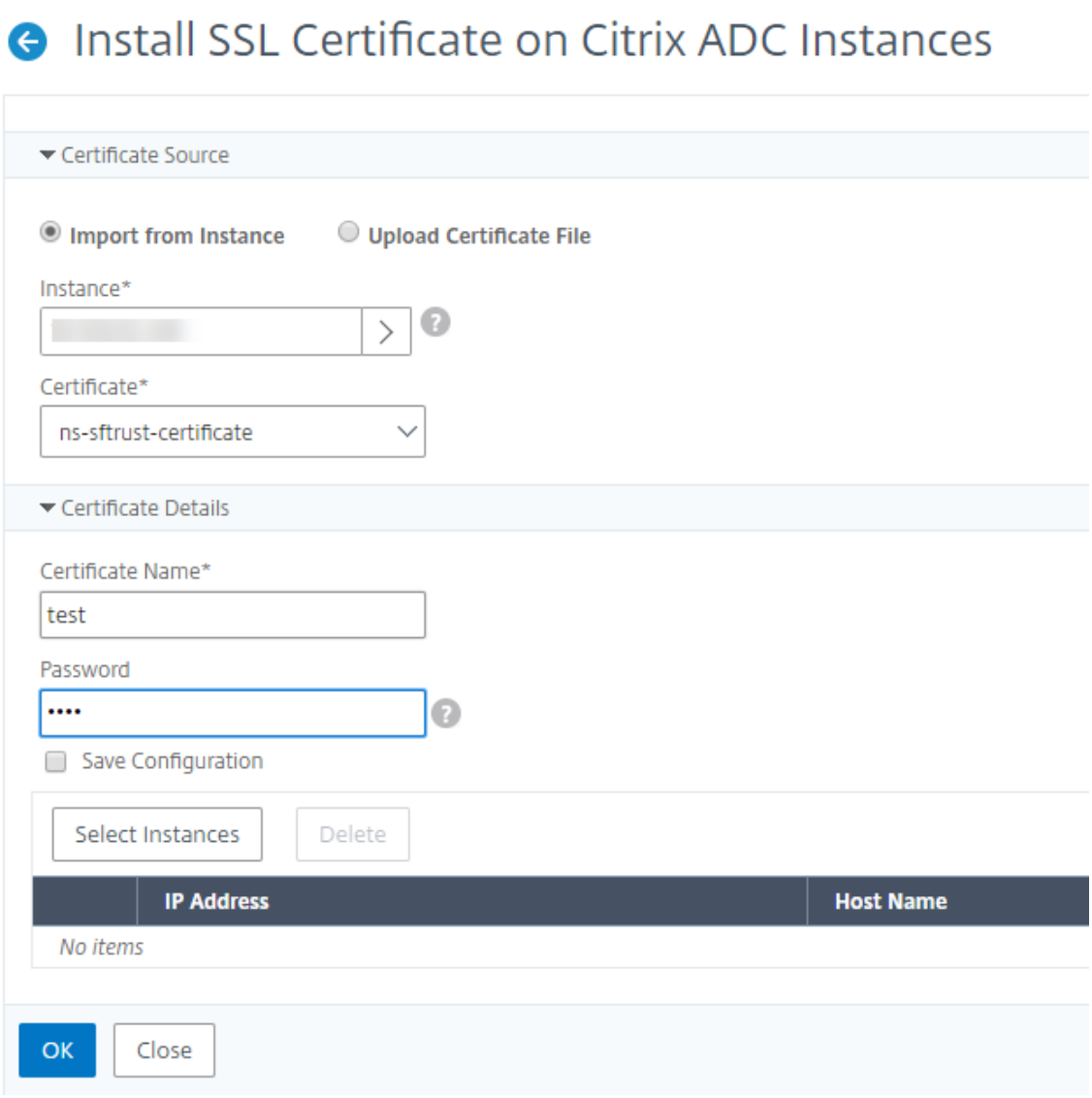
1. Vaya a **Infraestructura > Panel de control SSL**.
2. En la esquina superior derecha del panel de control de SSL, haga clic en **Instalar certificado**.
3. En la página **Instalar el certificado SSL en las instancias de Citrix ADC**, especifique los siguientes parámetros:
   a) Origen del certificado

      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 Citrix ADC en las que quiere instalar sus certificados.
5. Haga clic en **Aceptar**.

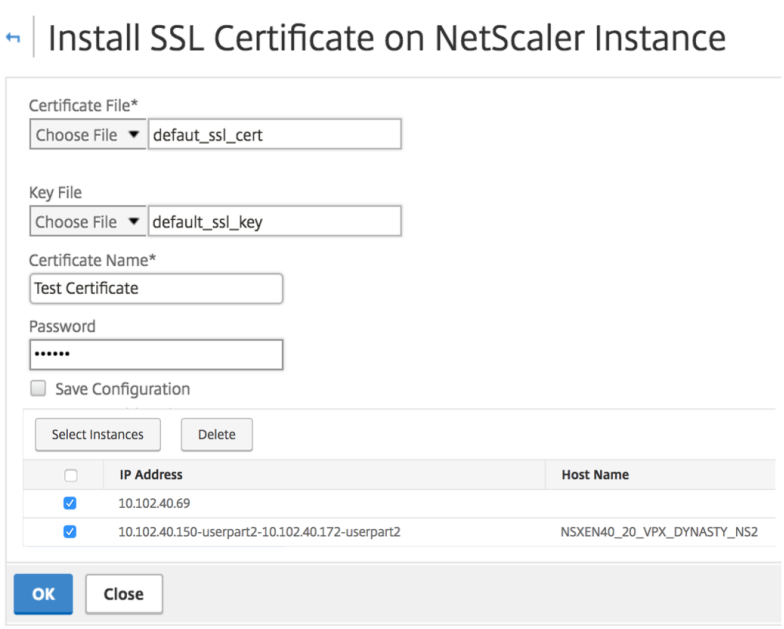


Para instalar un certificado SSL desde Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Panel SSL**.
2. En la esquina superior derecha del panel de control, haga clic en **Instalar certificado**.
3. En la página **Instalar certificado SSL en Citrix ADC Instance**, especifique los siguientes parámetros:
   - **Archivo de certificado** : cargue un archivo de certificado SSL seleccionando **Local** (su equipo local) o **Appliance** (el archivo de certificado debe estar presente en la instancia virtual de Citrix ADM).
   - **Archivo clave** : cargue el archivo clave.
   - **Nombre del certificado** : especifique un nombre para la clave del certificado.

- **Contraseña** : contraseña para cifrar la clave privada. Puede utilizar esta opción para cargar claves privadas cifradas.
- **Seleccione instancias** : seleccione las instancias de Citrix ADC 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)

November 16, 2022

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 Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Panel 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 **Appliance** (el archivo de claves debe estar presente en la instancia virtual Citrix ADM).
   - **Crear una clave** : seleccione la opción **No tengo una clave** y, a continuación, especifique los siguientes parámetros:

Algoritmo de cifrado	Tipo de llave. Por ejemplo, RSA.
Nombre de archivo de clave	Nombre del archivo en el que está almacenada la clave RSA.
Tamaño de clave	Tamaño de la clave en bits.
Valor del exponente público	Elija **3** o **F4** de la lista desplegable proporcionada. Este valor es parte del algoritmo de cifrado que se requiere para crear la clave RSA.
Formato de clave	Por defecto, se selecciona PEM. PEM es el formato de clave recomendado para su certificado SSL.
Algoritmo de codificación PEM	En la lista desplegable, seleccione el algoritmo (**DES** o **DES3**) que quiere utilizar para cifrar la clave RSA generada. Si 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	Confirma tu contraseña de PEM.

5. Haga clic en **Continue**.
6. En la siguiente página, proporcione más detalles.

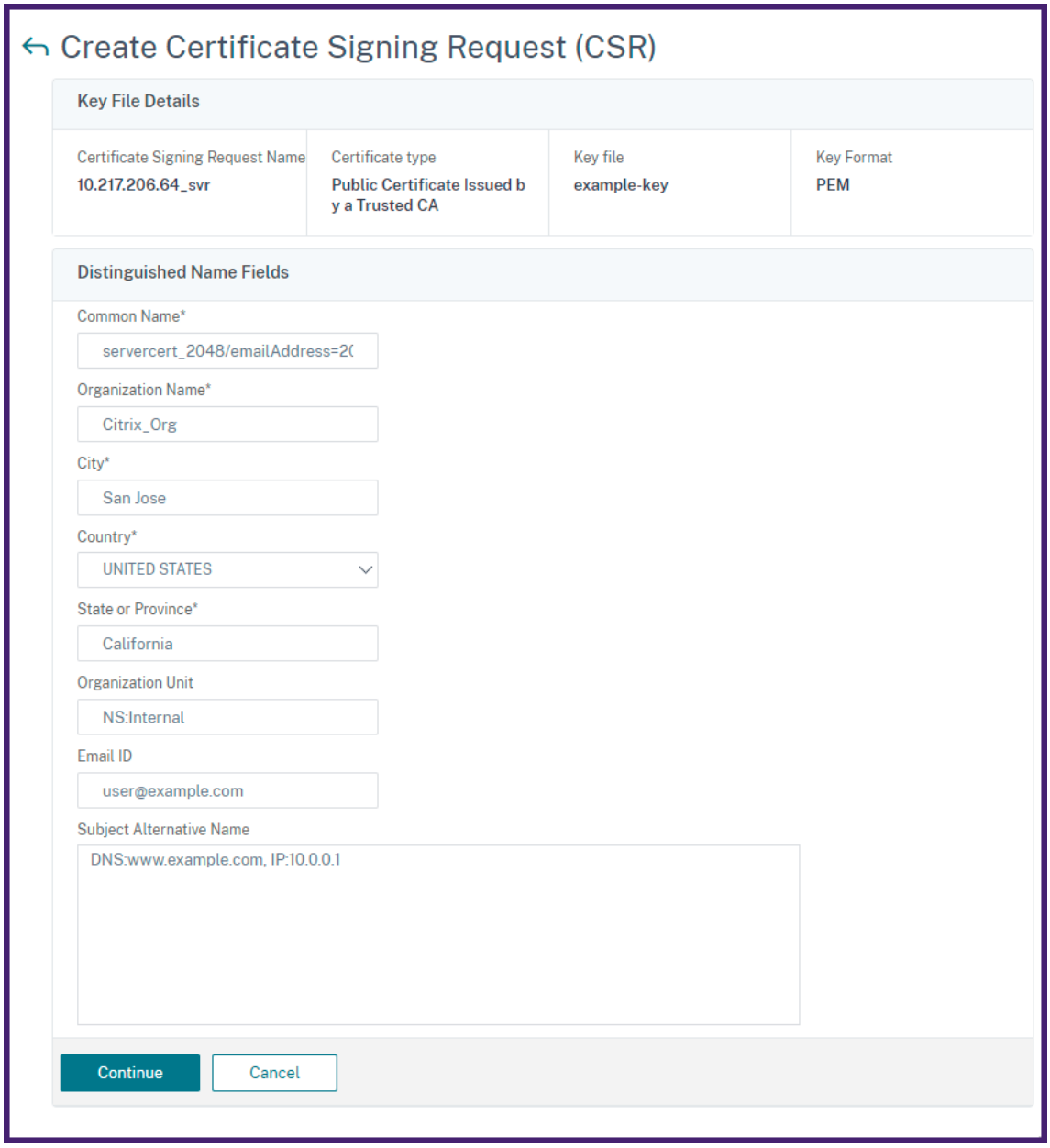
   La mayoría de los campos tienen valores predeterminados extraídos del asunto del certificado seleccionado. El asunto contiene detalles como el nombre común, el nombre de la organización, el estado y el país.

   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 ayu-

dan a proteger varios dominios con un único certificado.

Especifique los nombres de dominio y las direcciones IP en el siguiente formato:

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```



En este ejemplo, protege `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

November 16, 2022

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 Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Panel 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 Citrix ADM:

1. En Citrix ADM, vaya a **Infraestructura > Panel SSL**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Elija uno de los certificados vinculados que 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

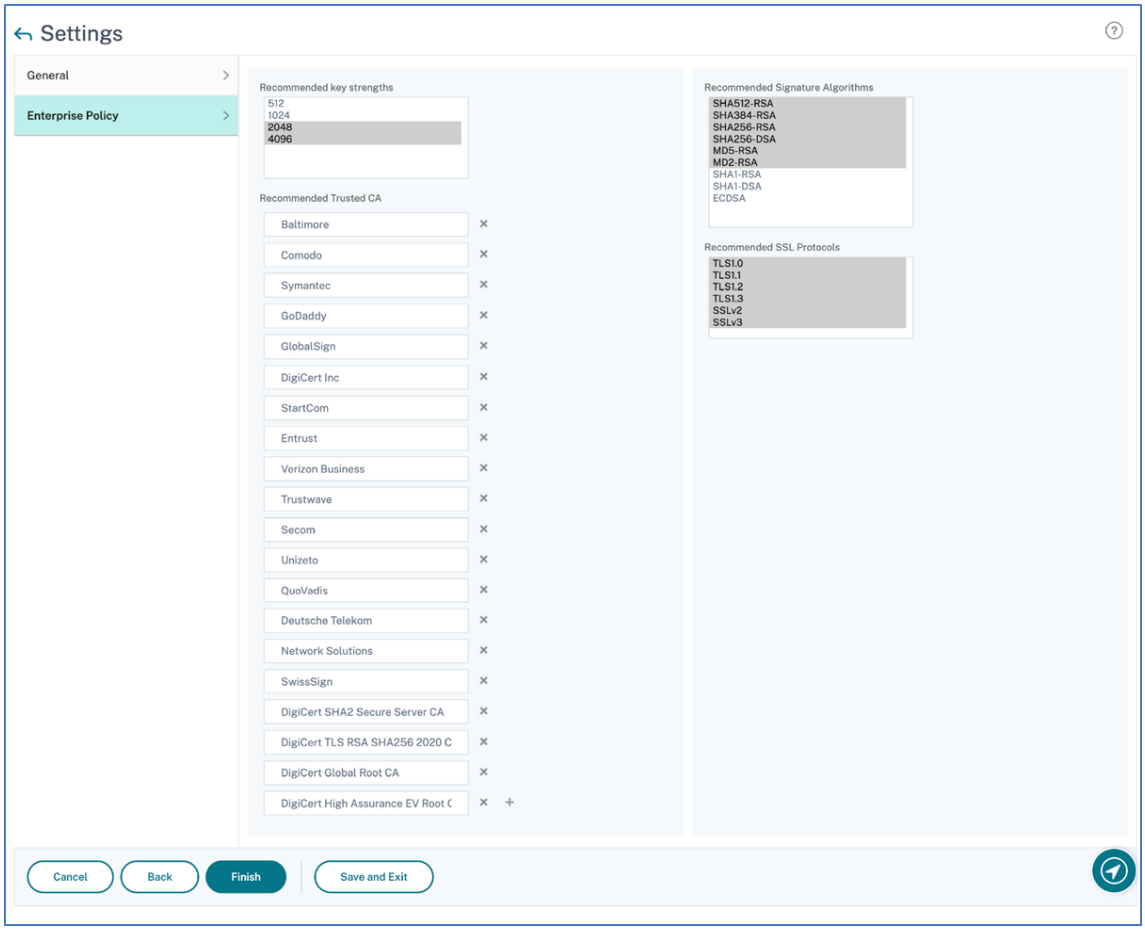
November 16, 2022

Puede configurar una directiva empresarial y agregar todas las CA confiables, algoritmos de firma segura y seleccionar la seguridad clave recomendada para sus claves de certificado en Citrix ADM. Si alguno de los certificados instalados en su instancia de Citrix ADC 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 seguridad de la clave del certificado no coincide con la fuerza de clave recomendada en la directiva empresarial, el panel de certificados SSL muestra los puntos fuertes de esas claves como No recomendado.

Para configurar una directiva de empresa en Citrix ADM:

1. En Citrix ADM, 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.
    - **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 Citrix ADC

November 16, 2022

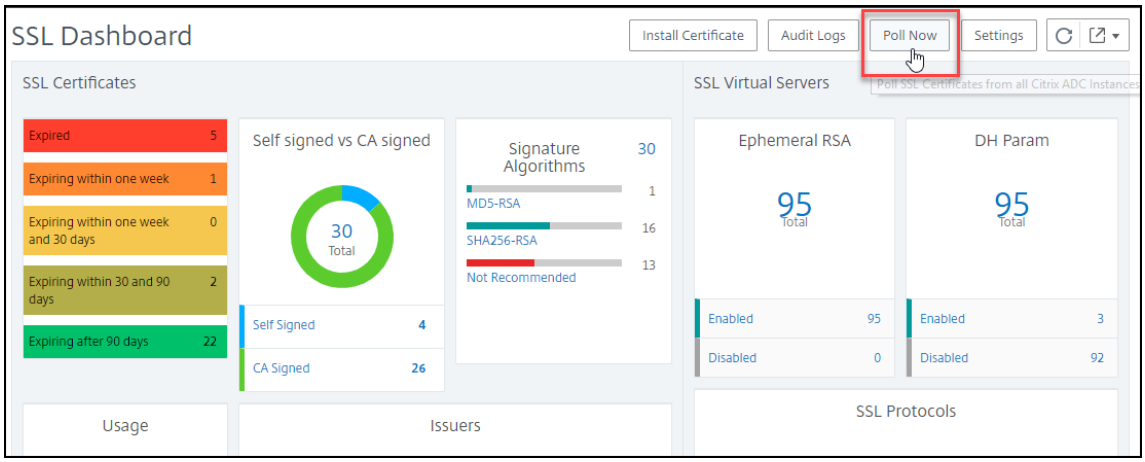
Citrix ADM sondea automáticamente los certificados SSL una vez cada 24 horas mediante llamadas NITRO y el protocolo Secure Copy (SCP). También puede sondear manualmente los certificados SSL para descubrir los certificados SSL recién agregados en las instancias de Citrix ADC. El sondeo de todos los certificados SSL de instancias Citrix ADC coloca una carga pesada en la red.

En lugar de sondear todos los certificados SSL de las instancias de Citrix ADC, puede sondear manualmente solo los certificados SSL de una o varias instancias seleccionadas.

Para sondear certificados SSL en instancias Citrix ADC:

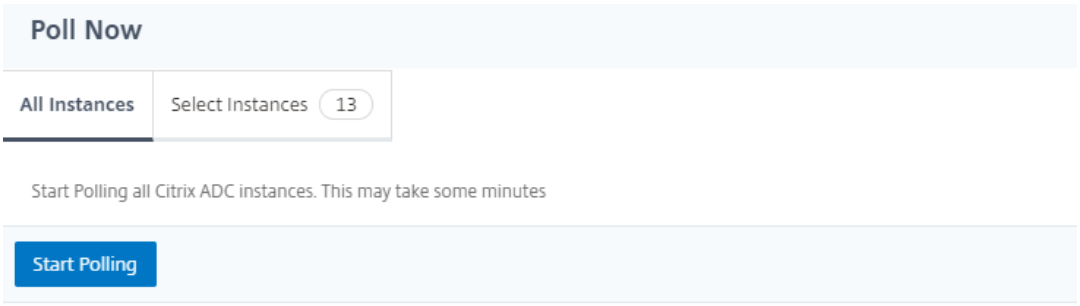
1. En Citrix ADM, vaya a **Infraestructura > Panel SSL**.

2. En la página **SSL Dashboard**, en la esquina superior derecha, haga clic en **Sondear ahora**.

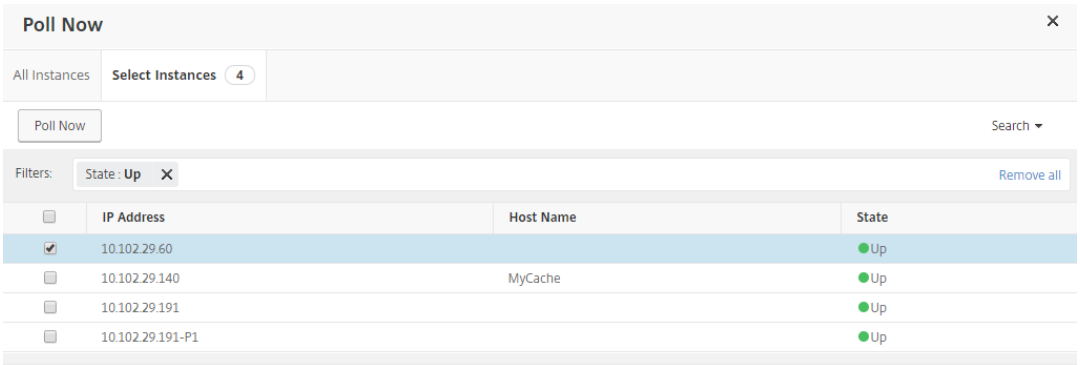


3. Aparece la página **Encuesta ahora**, que le da la opción de sondear todas las instancias de Citrix ADC en la red o sondear las instancias seleccionadas.

   - Para sondear los certificados SLL de todas las instancias de Citrix ADC, seleccione la ficha **Todas las instancias** y haga clic en **Iniciar sondeo**.



   - Para sondear instancias específicas, seleccione la ficha **Seleccionar instancias**, seleccione las instancias de la lista y haga clic en **Sondear ahora**.



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.

Trabajos de configuración

November 16, 2022

El proceso de administración de configuración de Citrix ADM garantiza la replicación adecuada de los cambios de configuración, las actualizaciones del sistema y otras actividades de mantenimiento en varias instancias de Citrix ADC de la red.

Citrix ADM le permite crear trabajos de configuración que le ayudarán a realizar todas estas actividades con facilidad en varios dispositivos como una sola tarea. Las plantillas y los trabajos de configuración simplifican las tareas administrativas más repetitivas en una sola tarea en Citrix ADM. Un trabajo de configuración contiene un conjunto de comandos de configuración que se pueden ejecutar en uno o varios dispositivos gestionados.

Los trabajos de configuración pueden usar comandos SSH para ejecutar los comandos de configuración o usar SCP para copiar archivos de forma local o a otro dispositivo; por ejemplo, podemos programar una conmutación por error de HA o una actualización de HA.

Puede crear un trabajo de configuración mediante una de las cuatro opciones siguientes en Citrix ADM. Utilice uno de estos para crear un origen reutilizable de comandos e instrucciones para el sistema para ejecutar un trabajo de configuración.

1. Plantilla de configuración
2. Instancia
3. Archivo
4. Grabar y reproducir

Plantilla de configuración

Puede crear plantillas de configuración mientras crea un trabajo y guarda un conjunto de comandos de configuración como plantilla. Al guardar estas plantillas en la página Crear Trabajos, se mostrarán automáticamente en la página Crear Plantilla. Para obtener más información, consulte Cómo utilizar la plantilla de configuración maestra en Citrix ADM.

> **Nota**
>
> La opción **Cambiar nombre** está deshabilitada para las plantillas de configuración predeterminadas. Sin embargo, puede cambiar el nombre de las plantillas de configuración personalizadas.

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 Citrix ADC SDX que ejecuten Citrix ADC versión 11.0 y posterior. Para realizar una actualización de un solo paquete, utilice una tarea integrada en Citrix ADM. También puede actualizar una instancia de Citrix ADC extrayendo la configuración en ejecución o una configuración guardada y ejecutando los comandos en otra instancia de Citrix ADC del mismo tipo. 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 Citrix ADC. Cuando ejecuta el trabajo, los cambios en ns.conf en la instancia seleccionada se registran y copian en Citrix ADM. 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

November 16, 2022

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 configuraciones en varias instancias de la red y grabar y reproducir tareas de configuración mediante la GUI de Citrix ADM y convertirlas en comandos de CLI.

Puede utilizar la función Trabajos de configuración de Citrix ADM para crear un trabajo de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados.

Para crear un trabajo de configuración en Citrix ADM:

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 Citrix ADC, 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 especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
   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 **En caso de error de comando** que Citrix ADM debe realizar si falla el comando:

- **Ignorar error y continuar**: Citrix ADM omite el comando fallido y ejecuta los comandos restantes para la instancia seleccionada.

  > **Nota**
  >
  > Esta acción no permite anular un trabajo de configuración en curso.

- **Detener la ejecución adicional**: Citrix ADM detiene los comandos restantes si algún comando falla durante la ejecución.
- **Reversión correcta de comandos**: Citrix ADM restaura los comandos ejecutados correctamente si algún comando falla durante la ejecución.

  Si la rollback personalizada está habilitada, Citrix ADM ejecuta los comandos de rollback correspondientes para los comandos fallidos.

9. Haga clic en **Finalizar**.

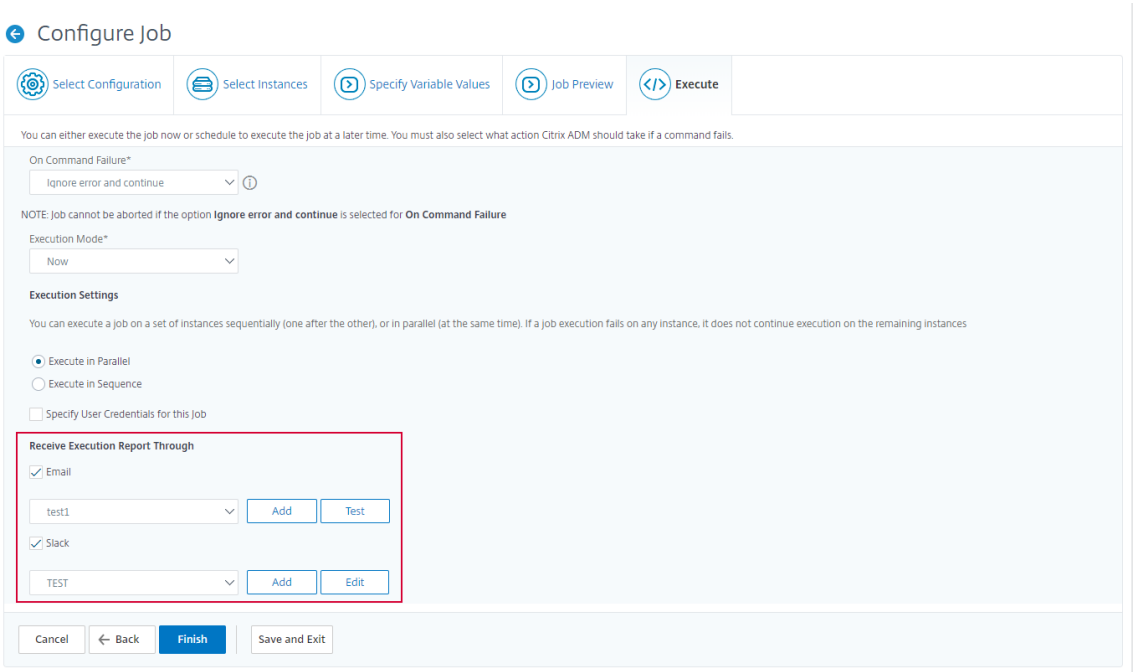
Para enviar un correo electrónico y una notificación de Slack para un trabajo:

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.

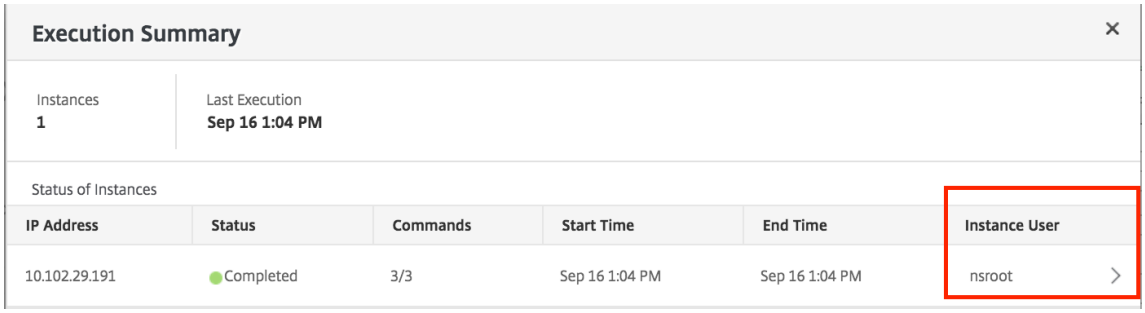
     Si quiere agregar un perfil de Slack, haga clic en **Agregar** y especifique el **nombre del perfil**, el **nombre del canal** y el **token** del canal de Slack requerido.



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

November 16, 2022

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 Citrix ADM
- Generar diferencias de auditoría de configuración para capturas SNMP de ConfigChange

Trabajos de mantenimiento

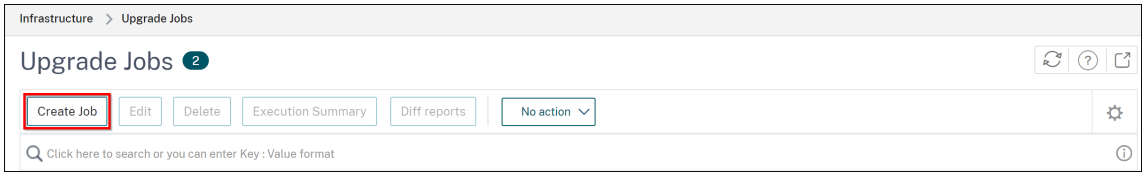
January 18, 2023

Puede crear las siguientes tareas de mantenimiento mediante Citrix ADM. A continuación, puede programar las tareas de mantenimiento en una fecha y hora específicas.

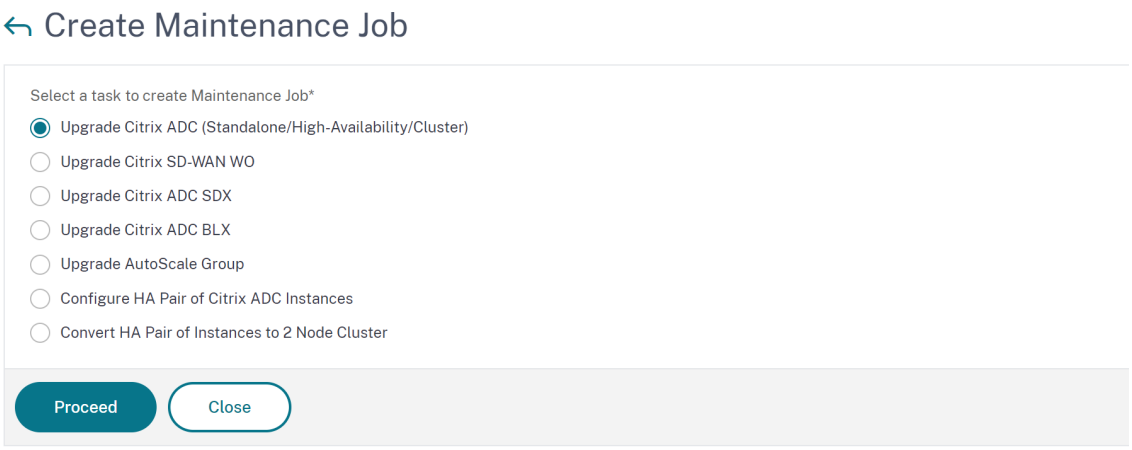
- Actualizar instancias de Citrix ADC
- Actualizar instancias SDX de Citrix ADC
- Actualización de instancias Citrix ADC BLX
- Actualización de instancias de Citrix ADC en el grupo de Autoscale
- Configurar el par HA de instancias Citrix ADC
- Convertir un par de instancias de HA en clúster

Programar la actualización de instancias Citrix ADC

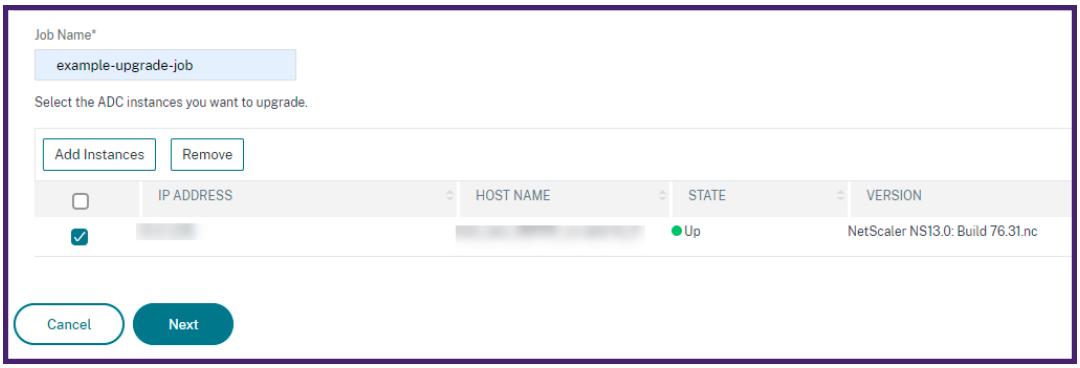
1. En Citrix ADM, vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.



2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar Citrix ADC (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.



3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar instancias ADC que quiera actualizar.
   - Para actualizar un par HA, especifique la dirección IP de un nodo principal o secundario. Sin embargo, se recomienda utilizar la instancia principal para actualizar el par HA.
   - Para actualizar un clúster, especifique la dirección IP del clúster.



5. Haga clic en **Siguiente** para seleccionar la imagen. Seleccione una de las siguientes opciones 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 Citrix ADM. La GUI de Citrix ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.
     - **Omitir la carga de imágenes a ADC si la imagen seleccionada ya está disponible**: Seleccione esta opción si la imagen ya está presente en la instancia de Citrix ADC.

- **Limpiar la imagen de software de Citrix ADC en una actualización correcta**: Seleccione esta opción para borrar la imagen cargada en la instancia de ADC después de la actualización de la instancia.

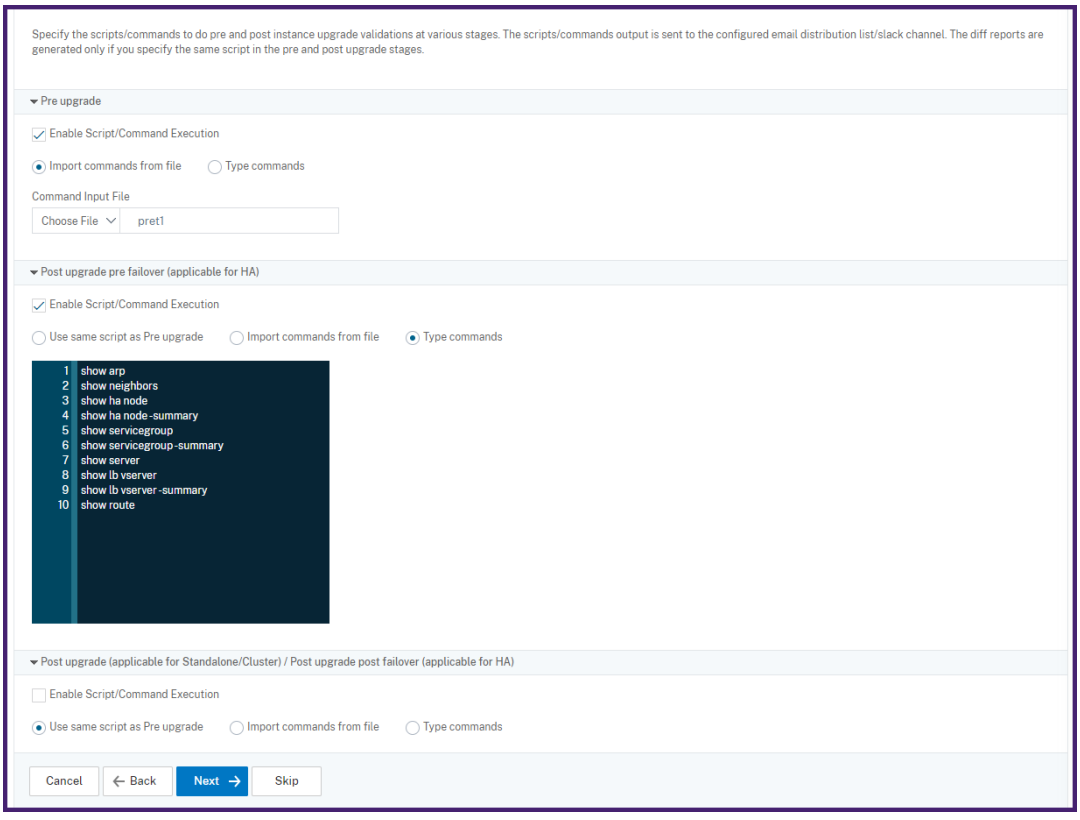
6. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   La ficha **Validación previa a la actualización** muestra las instancias fallidas. Quite las instancias con errores y haga clic en **Siguiente**.

   > **Importante**
   >
   > Si especifica la dirección IP del clúster, Citrix ADM 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.

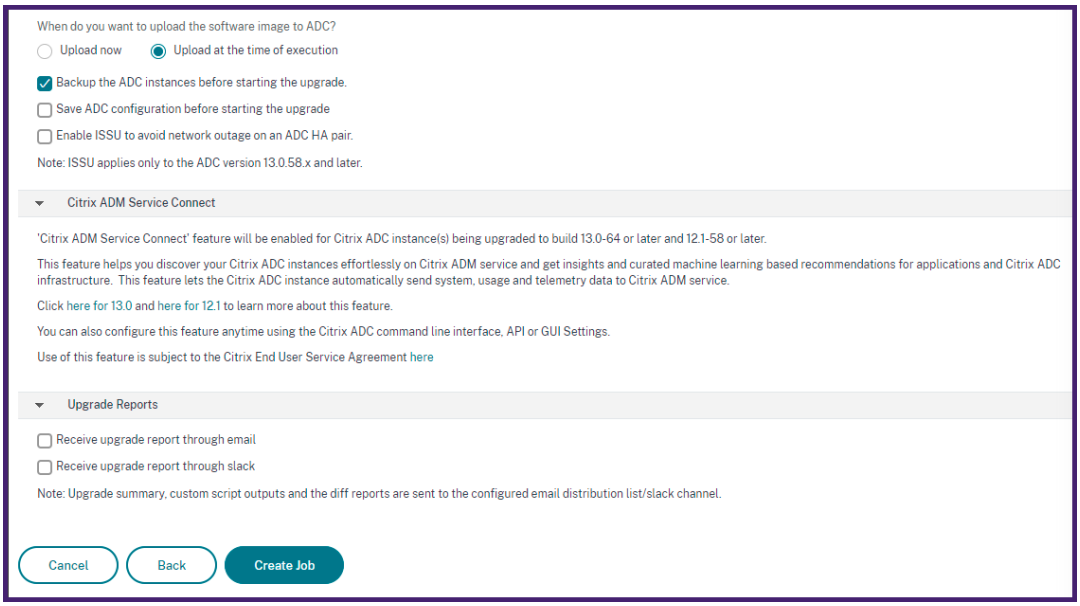
8. Haga clic en **Siguiente**. En **Planificar tarea**, seleccione una de las siguientes opciones:
   - **Actualizar ahora**: El trabajo de actualización se ejecuta inmediatamente.
   - **Programar más tarde**: Seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.

     Si quiere actualizar un par ADC HA en dos etapas, seleccione **Realizar actualización de dos etapas para nodos en HA**.

     Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia en el par HA.
9. Haga clic en **Siguiente**. En **Crear trabajo**, especifique los siguientes detalles:
   a) Especifique cuándo quiere cargar la imagen en una instancia:
      - **Cargar ahora**: Seleccione esta opción para cargar la imagen inmediatamente. Sin embargo, el trabajo de actualización se ejecuta a la hora programada.
      - **Cargar en el momento de la ejecución**: Seleccione esta opción para cargar la imagen en el momento de la ejecución del trabajo de actualización.
      - **Realice una copia de seguridad de las instancias ADC antes de iniciar la actualización.** - Crea una copia de seguridad de las instancias ADC seleccionadas.
      - **Guardar la configuración de ADC antes de iniciar la actualización**: Guarda los trabajos de configuración que están configurados en la instancia antes de la actualización.
      - **Habilite ISSU para evitar cortes de red en el par ADC HA**: ISSU garantiza la actualización de tiempo de inactividad cero en un par de alta disponibilidad de ADC. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par ADC HA sin tiempo de inactividad. Especifique el tiempo de espera de migración ISSU en minutos.
   - **Conexión del servicio Citrix ADM** : si se actualiza a la compilación **13.0-64 o posterior** y a la **12.1-58 o posterior**, el servicio Citrix ADM Connect se habilita automáticamente. Para

obtener más información, consulte Incorporación con poco toque de instancias Citrix ADC mediante Citrix ADM service connect.

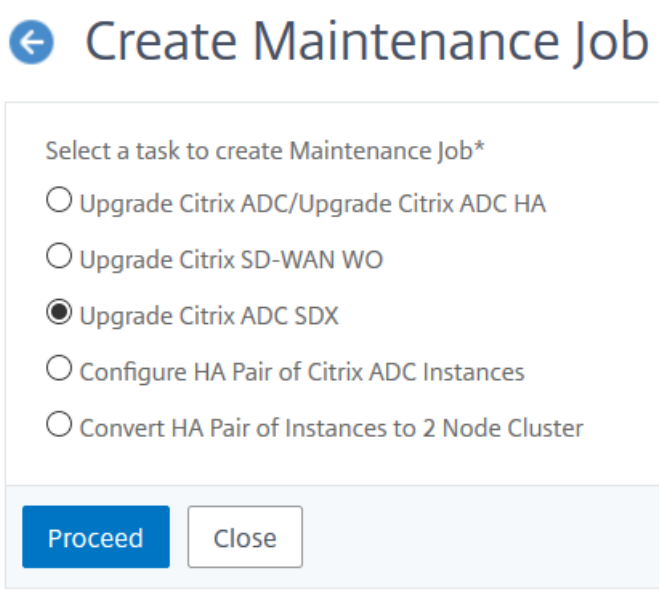
- **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.
- **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.



10. Haga clic en **Crear trabajo**.

Programar la actualización de instancias de Citrix ADC SDX

1. En Citrix ADM, vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Actualizar Citrix ADC SDX** y haga clic en **Continuar**.

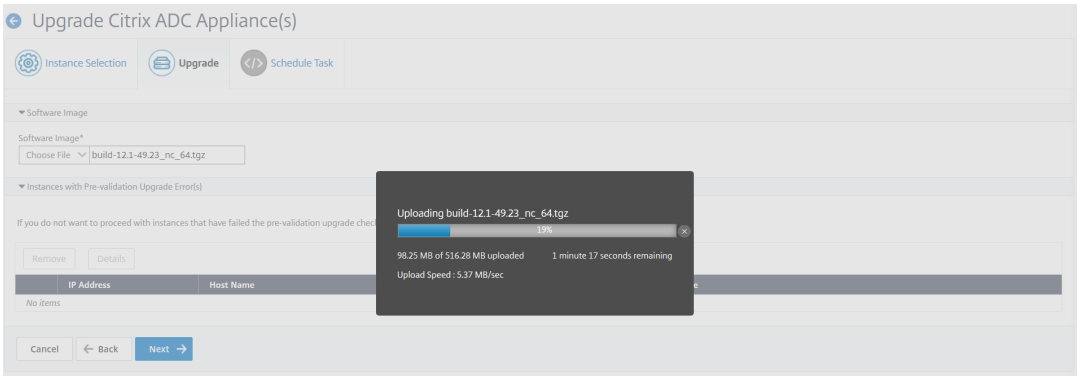


3. En la página **Actualizar Citrix ADC SDX**, en la ficha **Selección de instancias** :

   a) Agregue un **nombre de tarea**.

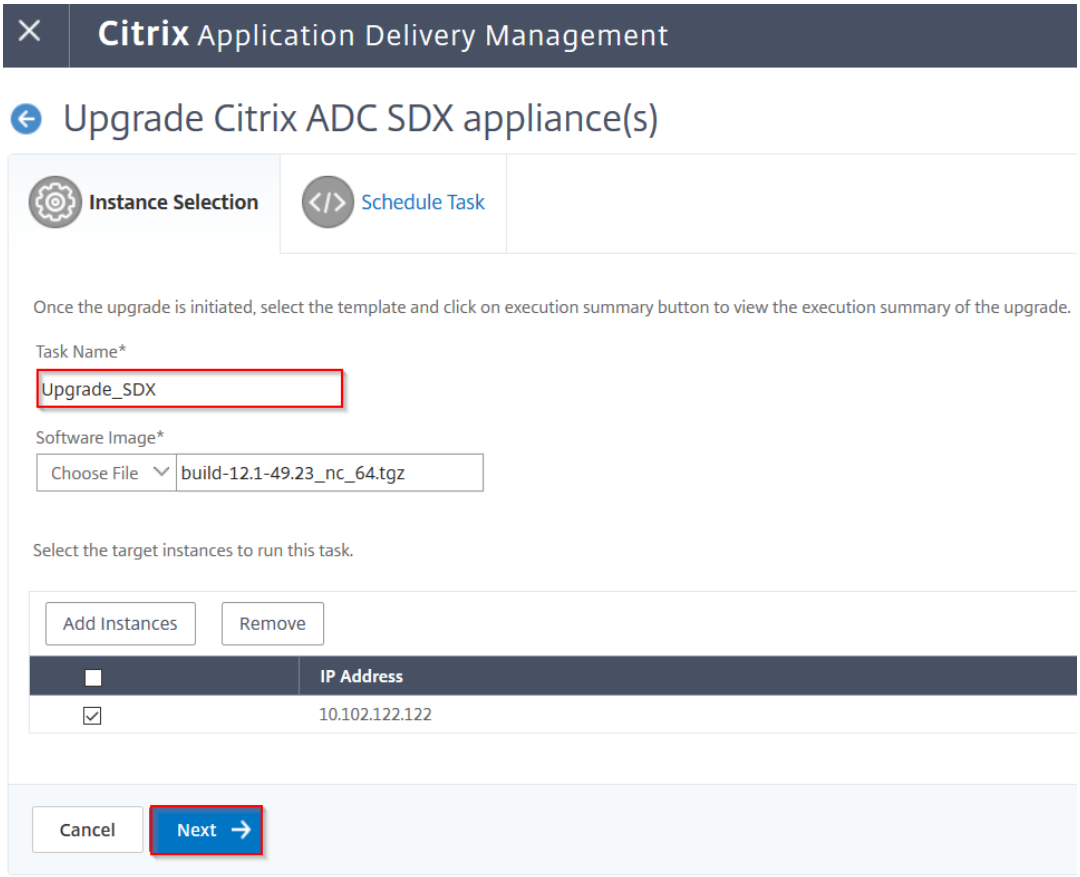
   b) En la lista de **imágenes de software**, seleccione **Local** (su máquina local) o **Dispositivo** (el archivo de compilación debe estar presente en el dispositivo virtual Citrix ADM).

   Comienza el proceso de carga.

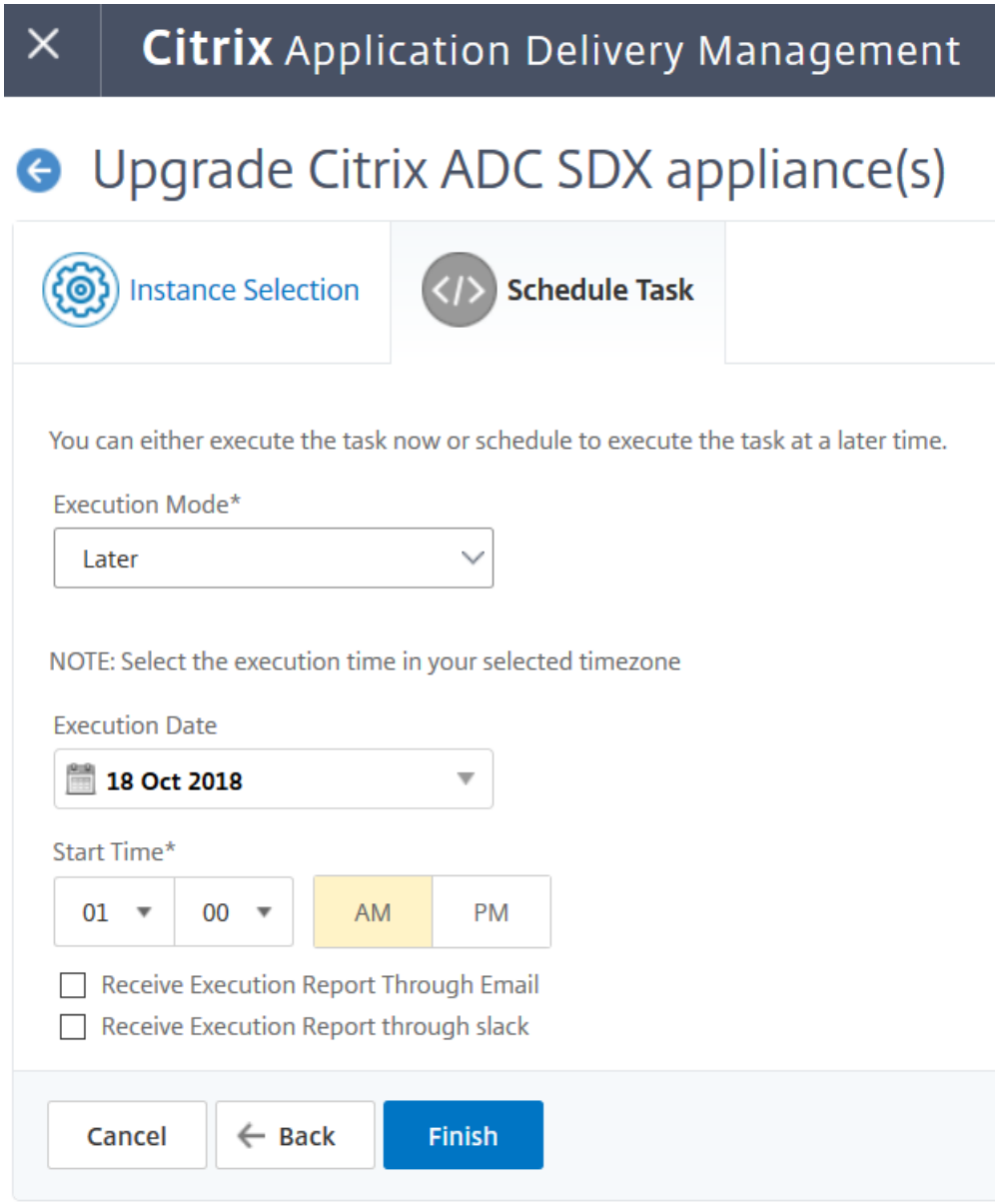


   c) Agregue las instancias de Citrix ADC SDX en las que quiere ejecutar el proceso de actualización.

   d) Haga clic en **Siguiente**.



4. En la ficha **Programar tarea**, seleccione **Ahora** en la lista **Modo de ejecución** para actualizar una instancia de Citrix SDX ahora y haga clic en **Finalizar**.
5. Para actualizar una instancia de Citrix ADC SDX más adelante, seleccione **Más tarde** en la lista **Modo de ejecución**. A continuación, puede elegir la fecha de ejecución y la hora de inicio para actualizar la instancia de Citrix ADC y hacer clic en **Finalizar**.

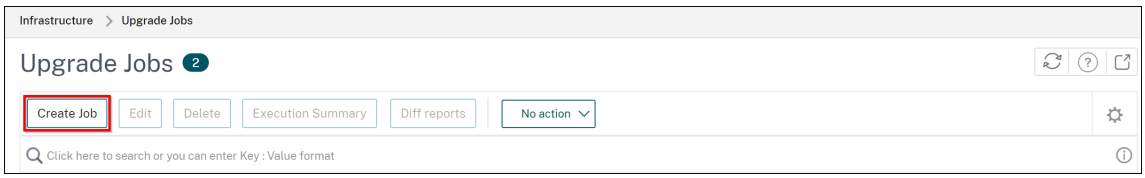


6. También puede habilitar las notificaciones de correo electrónico y de demora para recibir el informe de ejecución de la instancia de Citrix ADC SDX de actualización. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar las notificaciones.

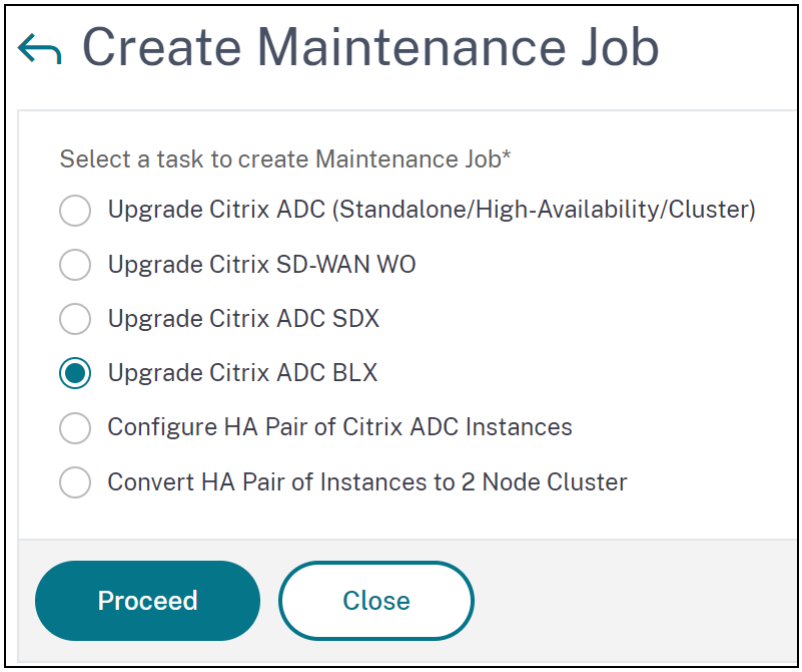
   Para obtener más información sobre cómo configurar la lista de distribución de correo electrónico y el canal de Slack, consulte el **paso 8** de Programar la actualización de instancias de Citrix ADC.

Programar la actualización de las instancias BLX de Citrix ADC

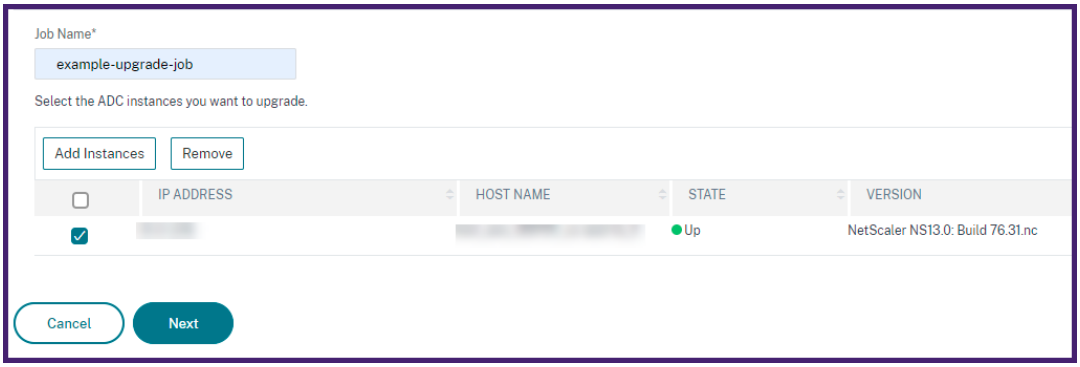
1. En Citrix ADM, vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.



2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar Citrix ADC BLX** y haga clic en **Continuar**.

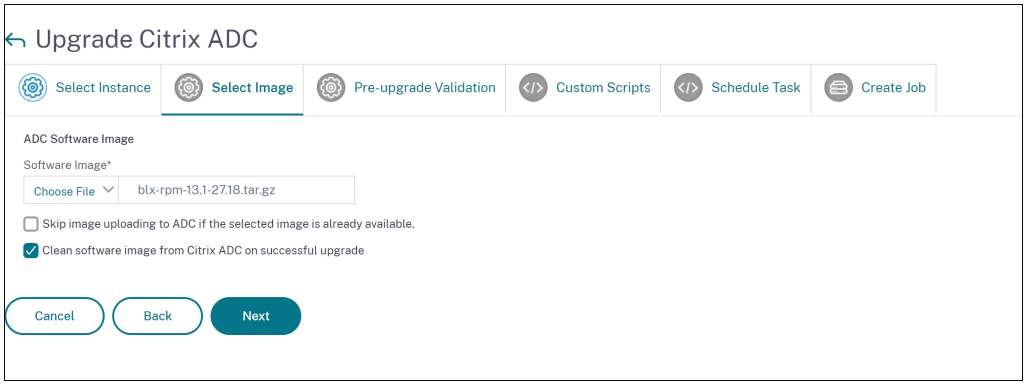


3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar las instancias BLX que quiera actualizar.
   - Para actualizar un par HA, especifique la dirección IP de un nodo principal o secundario. Sin embargo, se recomienda utilizar la instancia principal para actualizar el par HA.
   - Para actualizar un clúster, especifique la dirección IP del clúster.



5. Haga clic en **Siguiente** para seleccionar la imagen. Seleccione una de las siguientes opciones en la lista **Imagen de software**:

- **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
- **Dispositivo** : seleccione el archivo de actualización de la instancia en un explorador de archivos Citrix ADM. La GUI de Citrix ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.
  - **Omitir la carga de imágenes a ADC si la imagen seleccionada ya está disponible**: Seleccione esta opción si la imagen ya está presente en la instancia de Citrix ADC.
  - **Limpiar la imagen de software de Citrix ADC en una actualización correcta**: Seleccione esta opción para borrar la imagen cargada en la instancia de ADC después de la actualización de la instancia.

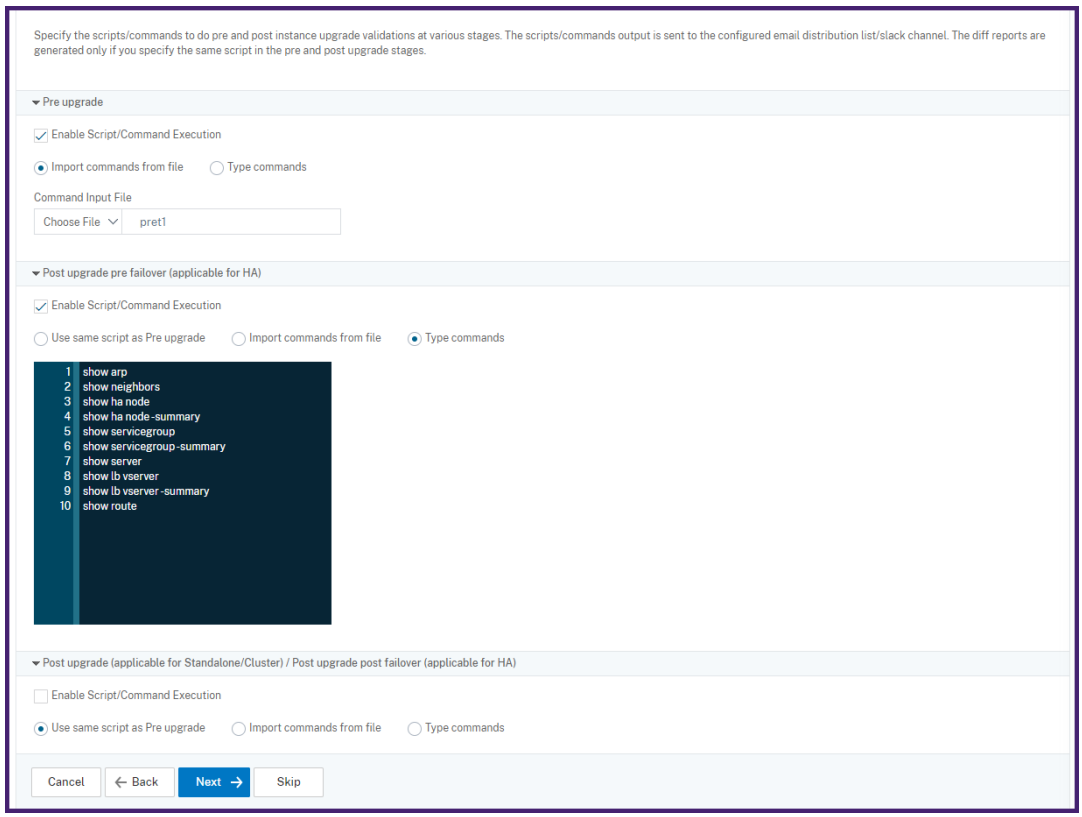


6. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   La ficha **Validación previa a la actualización** muestra las instancias fallidas. Quite las instancias con errores y haga clic en **Siguiente**.

   > **Importante**
   >
   > Si especifica la dirección IP del clúster, Citrix ADM 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.

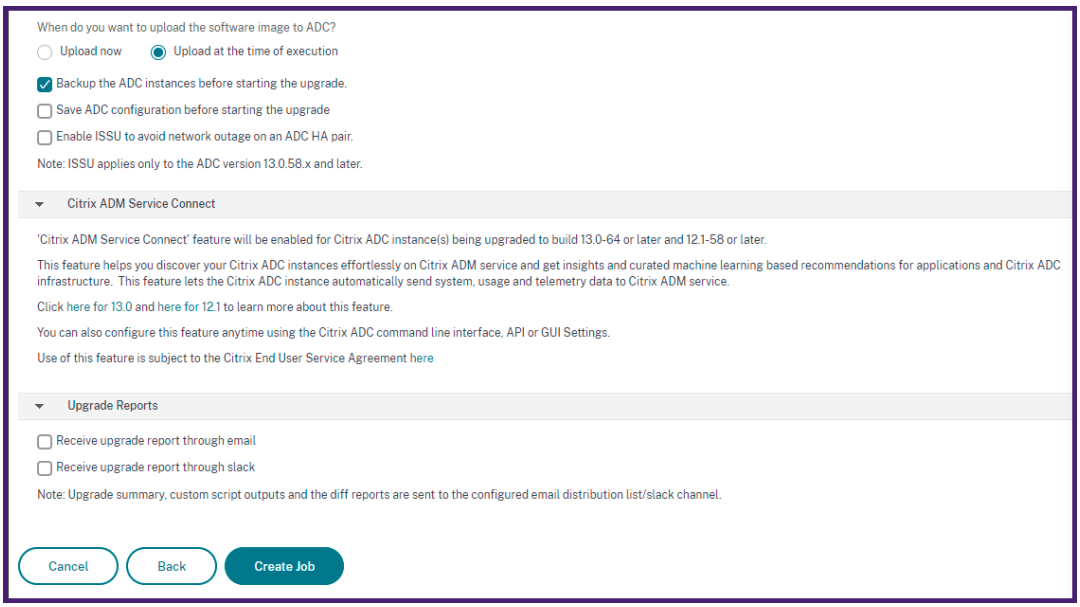
     Si quiere actualizar un par de HA en dos etapas, seleccione **Realizar actualización de dos etapas para los nodos de HA**.

     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.
- **Copia de seguridad de las instancias de ADC antes de iniciar la actualización**: Crea una copia de seguridad de las instancias de ADC seleccionadas.
- **Guardar la configuración de ADC antes de iniciar la actualización**: Guarda los trabajos de configuración que están configurados en la instancia antes de la actualización.
- **Habilite ISSU para evitar cortes de red en el par ADC HA**: ISSU garantiza la actualización de tiempo de inactividad cero en un par de alta disponibilidad de ADC. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par ADC HA sin tiempo de inactividad. Especifique el tiempo de espera de migración ISSU en minutos.

- **Conexión del servicio Citrix ADM** : si se actualiza a la compilación **13.0-64 o posterior** y a la **12.1-58 o posterior**, el servicio Citrix ADM Connect se habilita automáticamente. Para obtener más información, consulte Incorporación con poco toque de instancias Citrix ADC mediante Citrix ADM service connect.
- **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.
- **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.



10. Haga clic en **Crear trabajo**.

Programar la actualización del grupo Autoscale

Realice los siguientes pasos para actualizar todas las instancias de los servicios en la nube que forman parte del grupo Autoscale:

1. En Citrix ADM, vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Actualizar grupo de escala automática** y haga clic en **Continuar**.
3. En la ficha **Configuración de actualización** :
   a) Selecciona el **grupo de escalabilidad automática** que quiere actualizar.
   b) En **Imagen**, seleccione la versión de Citrix ADC. Esta imagen es la versión existente de las instancias de Citrix ADC en el grupo Autoscale.
   c) En **Citrix ADC Image**, examine el archivo de versión de Citrix ADC 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 Citrix ADC, actualice inmediatamente.
      - **Más tarde:** Para iniciar la actualización de las instancias de Citrix ADC más adelante.

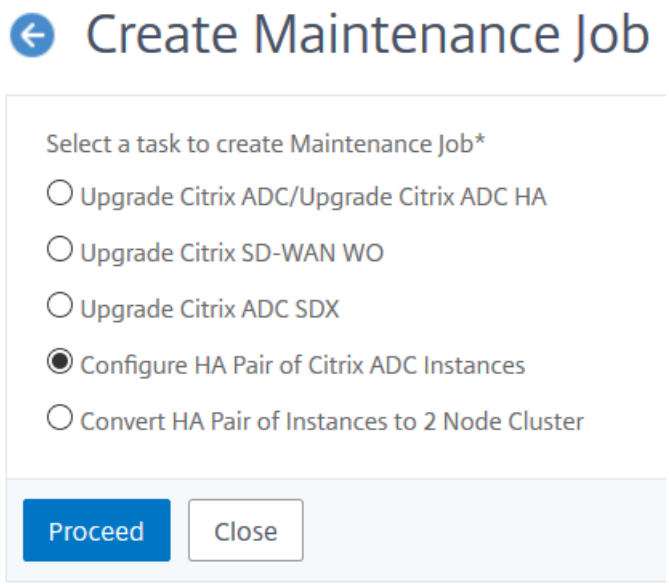
b) Si selecciona la opción **Más tarde**, seleccione Fecha de ejecución y Hora de inicio cuando quiera iniciar la tarea de actualización.

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.

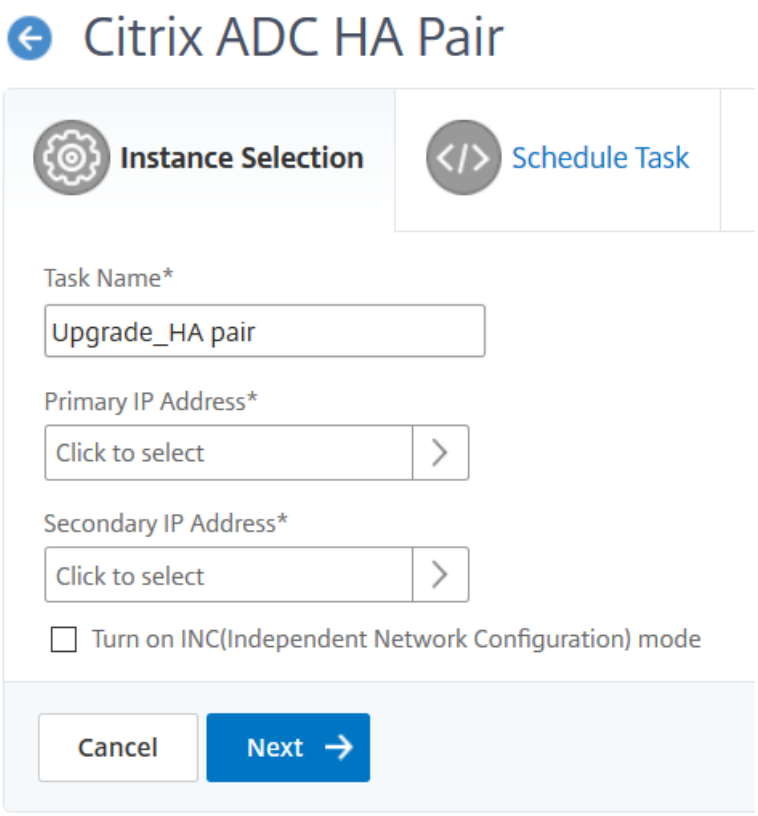
5. Haga clic en **Finalizar**.

Programar la configuración del par de instancias de Citrix ADC de HA

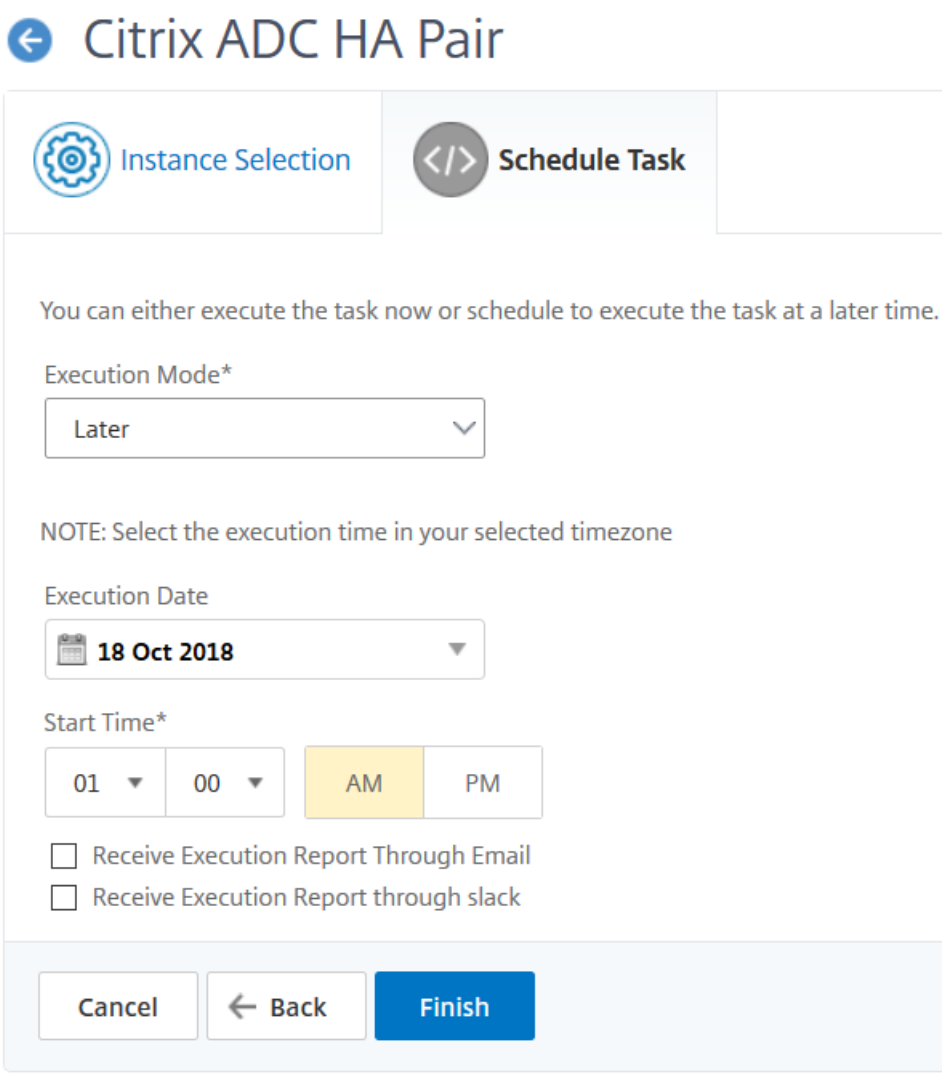
1. En Citrix ADM, vaya a **Infraestructura > Trabajos de actualización**. Haga clic en **Crear trabajo**.
2. Seleccione **Configurar Par HA de Instancias de Citrix ADC** y haga clic en **Continuar**.



3. En la página **Citrix ADC 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 Citrix ADC ahora y haga clic en **Finalizar**.
5. Para actualizar un par de Citrix ADC 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 Citrix ADC y hacer clic en **Finalizar**.

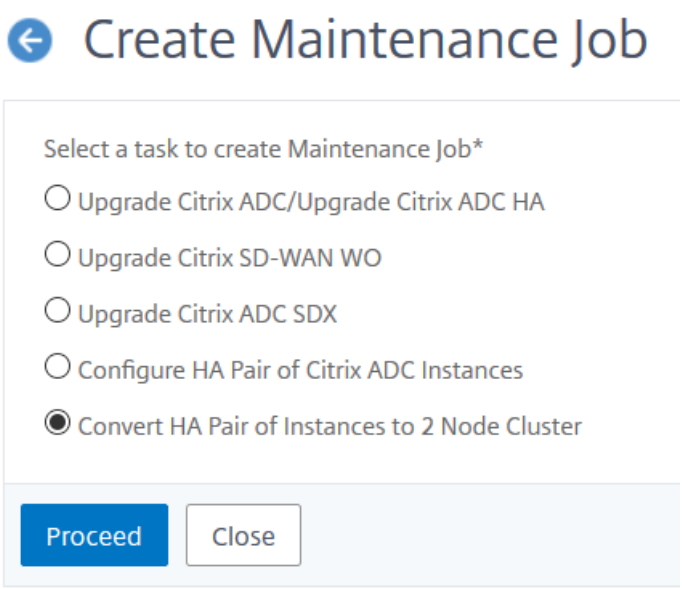


6. También puede habilitar las notificaciones de correo electrónico y de demora para recibir el informe de ejecución de la creación del par ADC HA. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar las notificaciones.

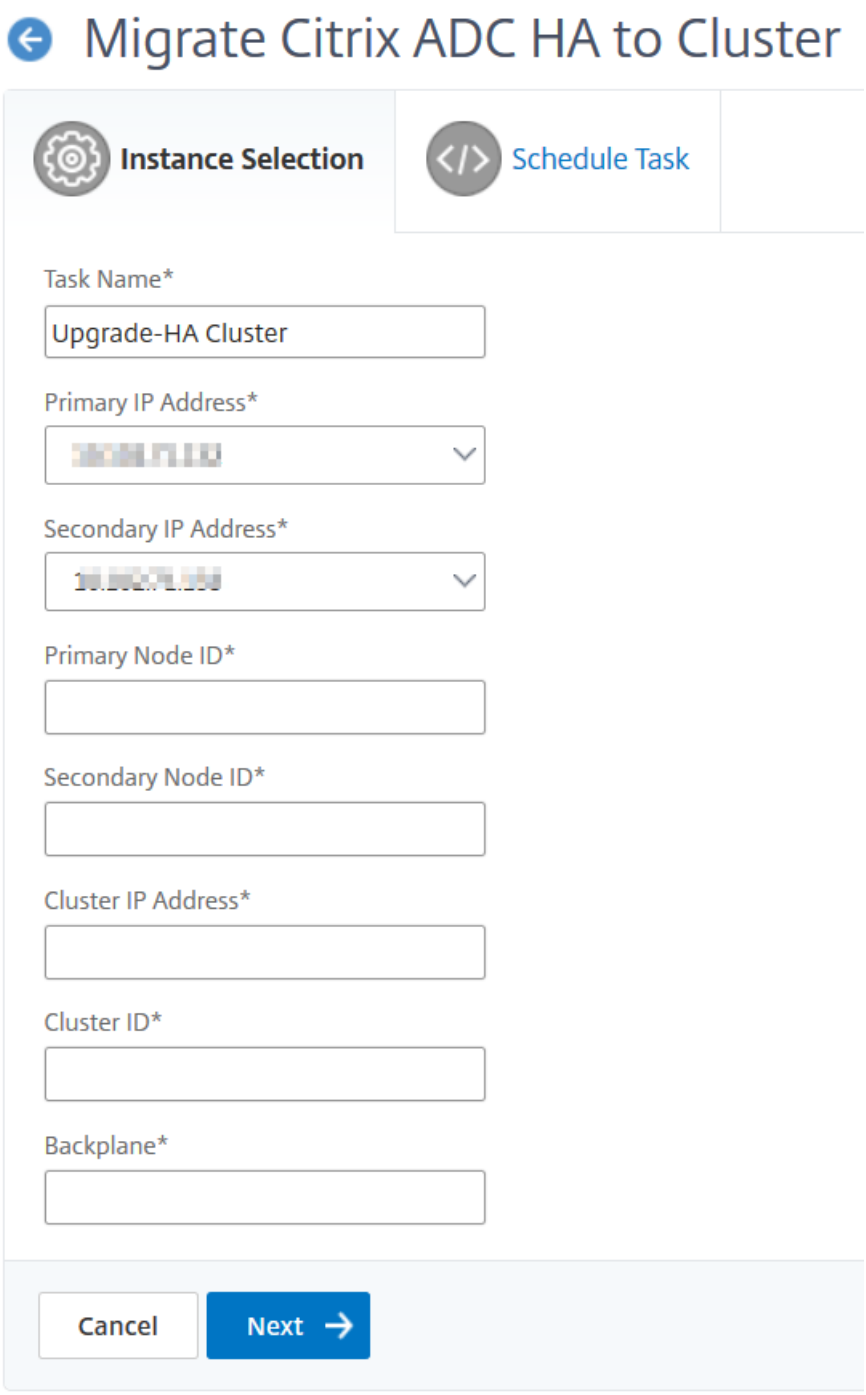
   Para obtener más información sobre cómo configurar la lista de distribución de correo electrónico y el canal de Slack, consulte el **paso 8** de Programar la actualización de instancias de Citrix ADC.

Programar la conversión del par de instancias de HA en clúster

1. En Citrix ADM, 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 Citrix ADC 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 Citrix ADC 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 Citrix ADC 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 instancias de Citrix ADC.

Usar trabajos para actualizar instancias de Citrix ADC

November 17, 2022

En Citrix ADM, puede actualizar una o más instancias de Citrix ADC. Debe conocer el marco de licencias y los tipos de licencias antes de actualizar una instancia.

Requisitos previos

ADM realizará las siguientes comprobaciones previas a la validación en la instancia que quiere 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. Puede volver a aplicar las personalizaciones de copia de seguridad después de la actualización de la instancia.
4. **Problemas de directiva**: ADC 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 de actualización para configuraciones ADC personalizadas

Es importante que tanto los cambios de actualización como las personalizaciones se apliquen a un dispositivo Citrix ADC actualizado. Por lo tanto, si tiene archivos de configuración personalizados en el directorio /etc, consulte Consideraciones de actualización para los archivos de configuración personalizados antes de continuar con la actualización del dispositivo Citrix ADC. Los siguientes son los pasos generales que debe realizar:

1. Pasos previos a la actualización en ADC
    - Realice una copia de seguridad del archivo personalizado antes
    - Elimine el enlace simbólico del archivo personalizado antes de la actualización
2. Actualice ADC con ADM. Para actualizar, siga las instrucciones disponibles al principio de la página.
3. Pasos posteriores a la actualización en ADC
    - Restaurar las personalizaciones después de la actualización

Tanto los pasos previos a la actualización como los posteriores a la actualización se deben realizar en cada ADC. Sin embargo, en el paso 2, para actualizar el ADC mediante ADM, todas las instancias de ADC vulnerables se pueden seleccionar y actualizar juntas.

Par de alta disponibilidad ADC

Cuando actualice un par de alta disponibilidad de ADC, 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 el nodo principal y el secundario está inhabilitada.

Puede actualizar un par de alta disponibilidad de ADC 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 ADC

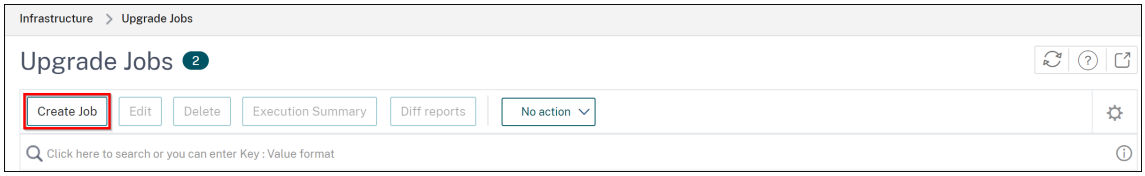
Al actualizar un clúster de ADC, en la etapa de validación previa a la actualización, Citrix ADM solo valida la instancia especificada. Por lo tanto, compruebe y resuelva los siguientes problemas en los nodos del clúster:

- Personalización
- Uso del disco
- problemas de hardware

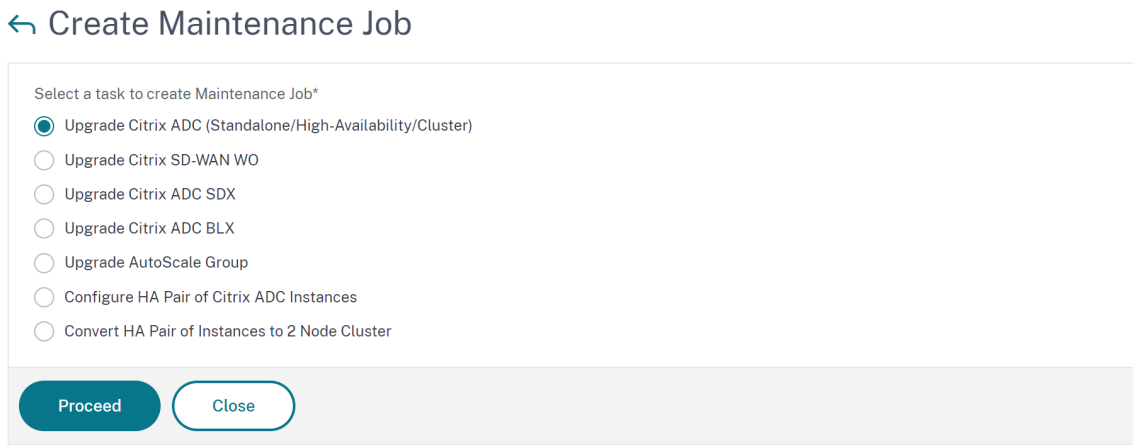
Crear un trabajo de actualización de ADC

Para crear un trabajo de actualización de ADC, haga lo siguiente:

1. Vaya a **Infraestructura > Trabajo de configuración > Trabajos de mantenimiento**.

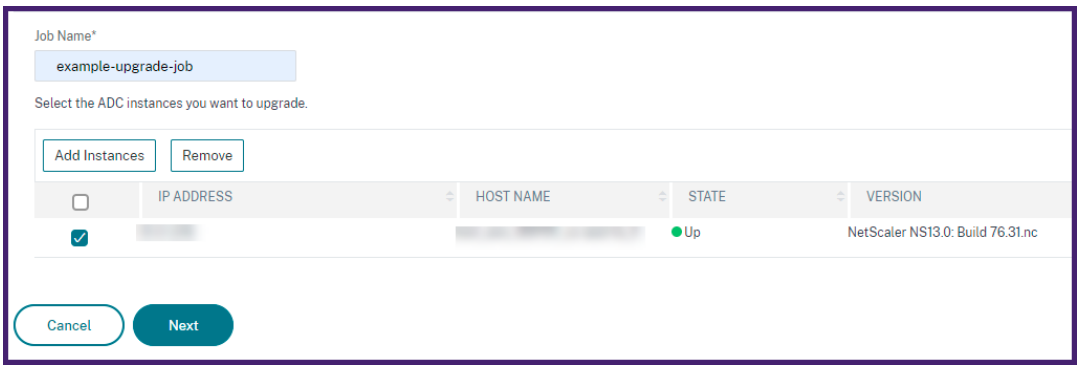


2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar Citrix ADC (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.



> **Nota**
>
> Para actualizar los grupos de Autoscale, consulte Actualizar un grupo de Autoscale.

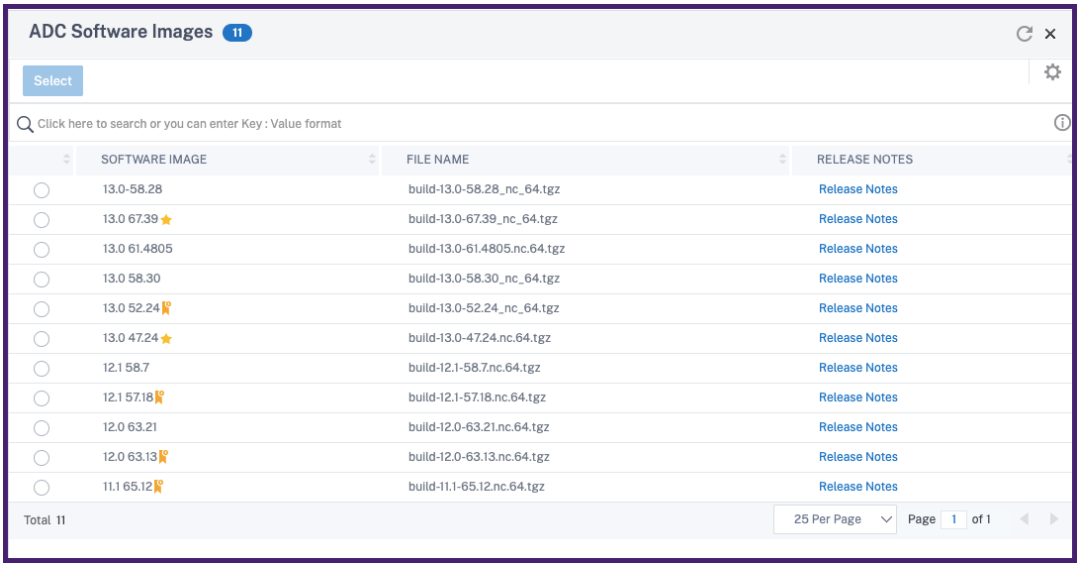
3. En la ficha **Seleccionar instancia**,
   a) Especifique el nombre de su elección para el **nombre del trabajo**.
   b) Haga clic en **Agregar instancias** para agregar instancias ADC que quiera actualizar.
      - Para actualizar un par de alta disponibilidad de ADC, especifique la dirección IP del nodo principal o secundario.
      - Para actualizar un clúster, especifique la dirección IP del clúster.



c) Haga clic en **Siguiente**.

4. En la ficha **Seleccionar imagen**, seleccione una imagen ADC de la biblioteca de imágenes o local o del dispositivo.

   - **Seleccione de la biblioteca de imágenes**: seleccione una imagen ADC de la lista. Esta opción muestra todas las imágenes ADC que están disponibles en el sitio web de descargas de Citrix.



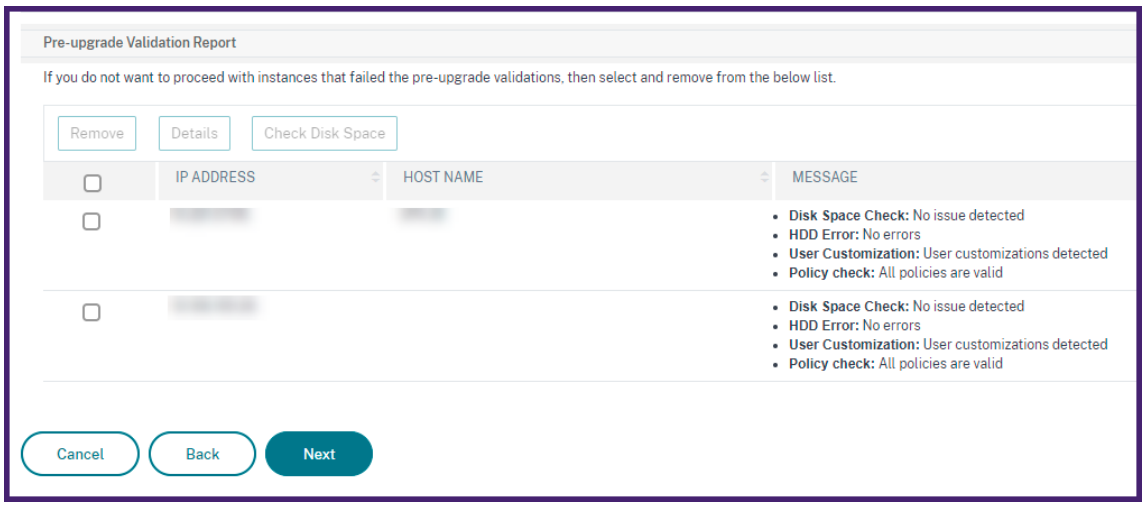
   Las imágenes del software ADC muestran las compilaciones preferidas con el icono de estrella. Y, la mayoría de las compilaciones descargadas con el icono de marcador.

   - **Seleccione entre local o dispositivo**: puede cargar la imagen desde su ordenador local o desde el dispositivo ADC. Al seleccionar el dispositivo ADC, la GUI de Citrix ADM muestra los archivos de instancia que están presentes en `/var/mps/ns_images`. Seleccione la imagen de la GUI de Citrix ADM.
   - **Omitir la carga de imágenes a ADC si la imagen seleccionada ya está disponible** : esta opción comprueba si la imagen seleccionada está disponible en ADC. El trabajo de actualización omite la carga de una imagen nueva y utiliza la imagen disponible en ADC.

- **Limpiar la imagen de software de Citrix ADC tras la actualización correcta** : esta opción borra la imagen cargada en la instancia de ADC después de 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**.



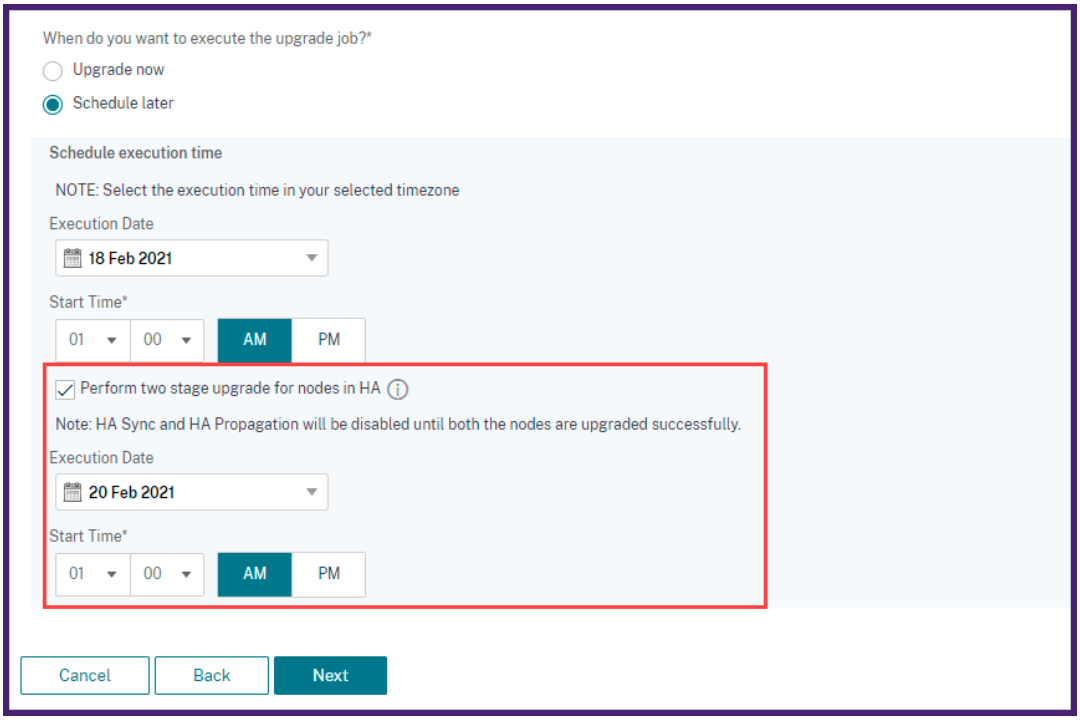
- **Comprobación de espacio**en disco: si no tiene suficiente espacio en disco en una instancia, puede comprobar y limpiar el espacio en disco. Consulte Limpiar espacio en disco ADC.
- **Verificación de directivas**: si Citrix ADM encuentra directivas clásicas no compatibles, puede eliminarlas para crear un trabajo de actualización.

> **Importante** Si especifica la dirección IP del clúster, Citrix ADM realiza la validación previa a la actualización solo en la instancia especificada, no en los demás nodos del clúster.

6. Opcional, en **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 **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 alta disponibilidad de ADC en dos etapas, seleccione **Realizar actualización en dos etapas para nodos en 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 el par ADC de alta disponibilidad.

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 obtener más información sobre otras opciones de actualización, consulte Opciones de actualización de ADC.

9. Haga clic en **Crear trabajo**.

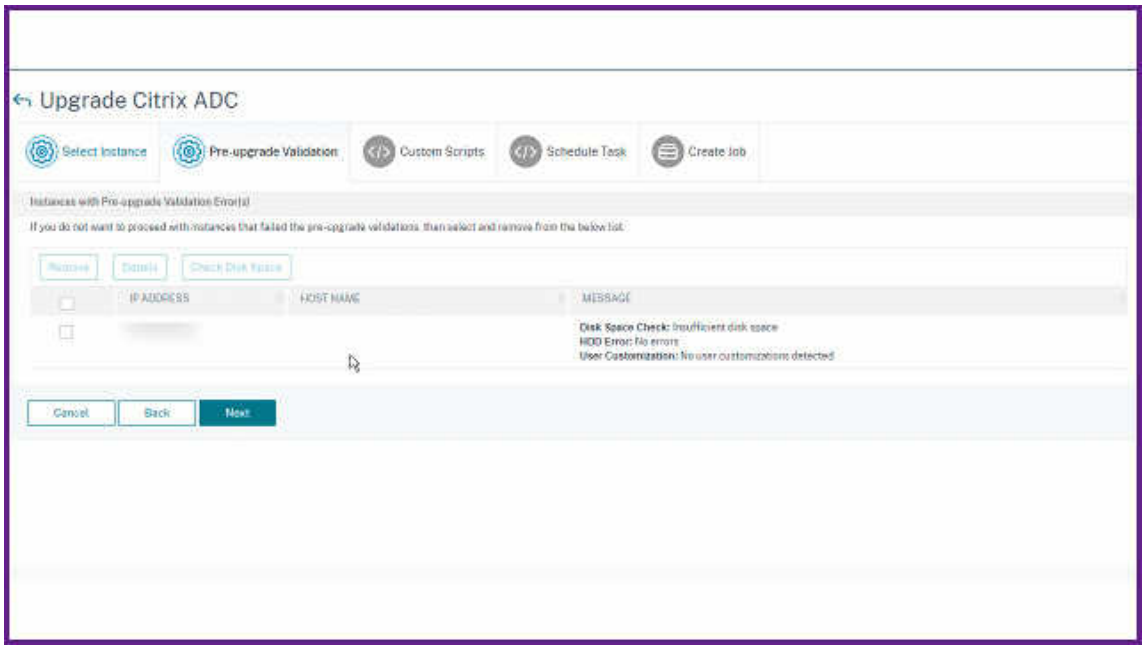
El trabajo de actualización aparece en **Infraestructura > Trabajo de configuración > Trabajos de mantenimiento**. Cuando modifique un trabajo existente, puede cambiar a cualquier ficha si los campos obligatorios ya están rellenados. Por ejemplo, si se encuentra en la ficha **Seleccionar configuración**, puede cambiar a la ficha **Vista previa del trabajo**.

Limpiar el espacio en disco ADC

Si tiene un problema de espacio en disco insuficiente al actualizar una instancia de ADC, limpie el espacio en disco de la propia GUI de Citrix ADM.

1. En la ficha **Validación previa a la actualización**, seleccione la instancia que tiene el problema de espacio en disco.
2. Seleccione **Comprobar espacio en disco**.

   Este panel muestra el disco de la instancia que tiene poco espacio. También muestra cuánta memoria se utiliza y está disponible en el disco.
3. En el panel **Comprobar espacio en disco**, seleccione la instancia que requiere limpieza.
4. Haga clic en **Liberar espacio en disco**.



5. Seleccione los archivos que quiere borrar.
6. Haga clic en **Eliminar**

Usar scripts personalizados

Puede especificar scripts personalizados al crear un trabajo de actualización de ADC. Los scripts personalizados se utilizan para comprobar los cambios antes y después de una actualización de instancia de ADC. 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 las secuencias de comandos personalizadas que se van a ejecutar en las siguientes etapas:

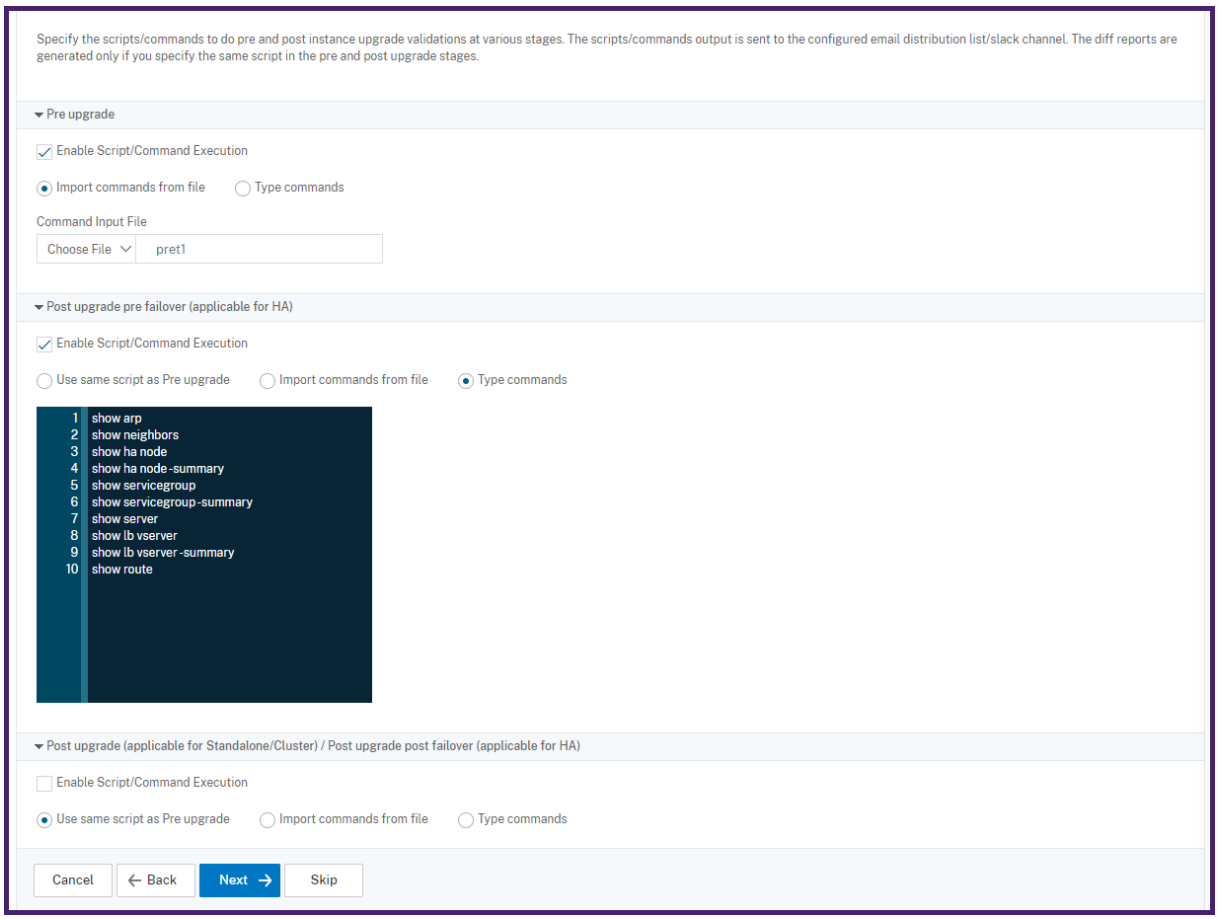
- **Preactualización**: el script especificado se ejecuta antes de actualizar una instancia.
- **Después de la actualización previa a la conmutación por error (aplicable para HA)**: esta etapa solo se aplica a la implementación de alta disponibilidad. El script especificado se ejecuta después de actualizar 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 sólo 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 ADC.

Puede importar un archivo de script o escribir comandos directamente en la GUI de Citrix ADM.

- **Importar comandos de archivo**: seleccione el archivo de entrada de comandos desde el equipo local.
- **Escriba comandos**: Introduzca los comandos directamente en la interfaz gráfica de usuario.

En las etapas posteriores a la actualización, puede utilizar el mismo script especificado en la etapa previa a la actualización.



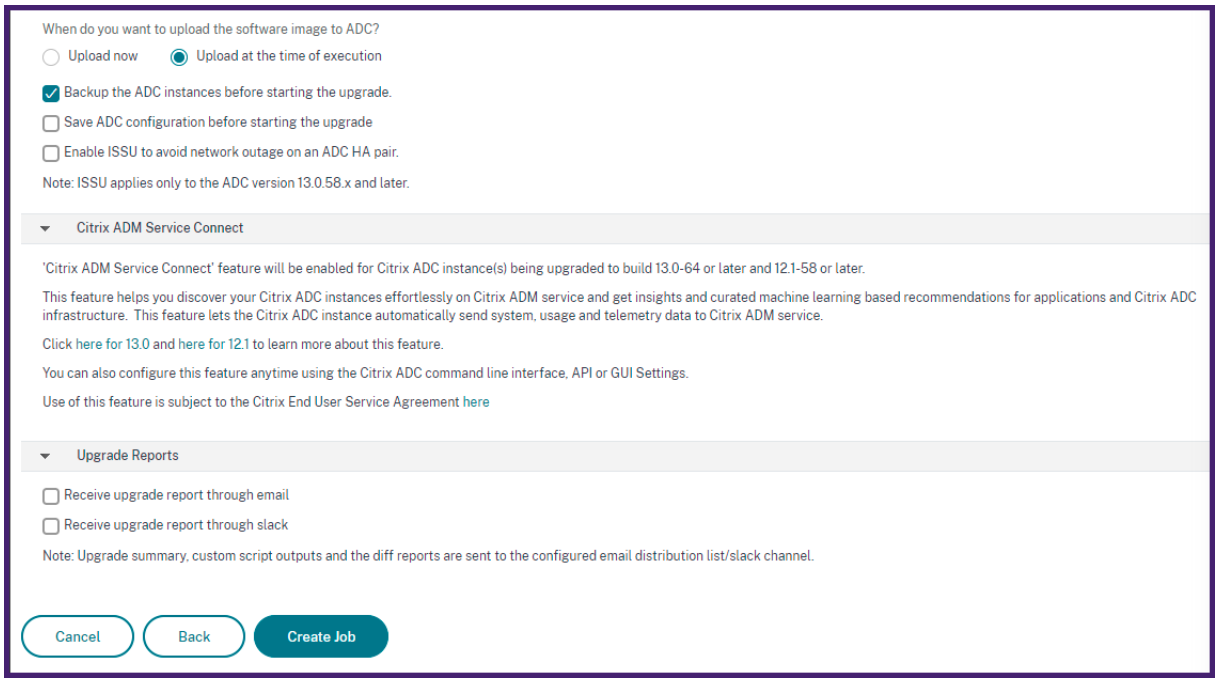
Opciones de actualización de ADC

Al crear un trabajo de actualización de ADC, puede seleccionar las siguientes opciones en la ficha **Crear trabajo** :

- **Realice una copia de seguridad de las instancias ADC antes de iniciar la actualización.**: crea una copia de seguridad de las instancias ADC 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 configuración de ADC antes de iniciar la actualización** : guarda la configuración ADC en ejecución antes de actualizar las instancias de ADC.
- **Habilite ISSU para evitar cortes de red en el par ADC HA**: ISSU garantiza la actualización de tiempo de inactividad cero en un par de alta disponibilidad de ADC. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par de alta disponibilidad de ADC 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.



Descargar un informe diff consolidado de un trabajo de actualización de ADC

En Citrix ADM, puede descargar un informe diff de un trabajo de actualización de ADC. 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 han producido en la instancia de ADC posterior a la actualización.

> **Nota**
>
> El informe diff solo se genera si especifica el mismo script en las etapas anterior a la actualización y posterior a la actualización.

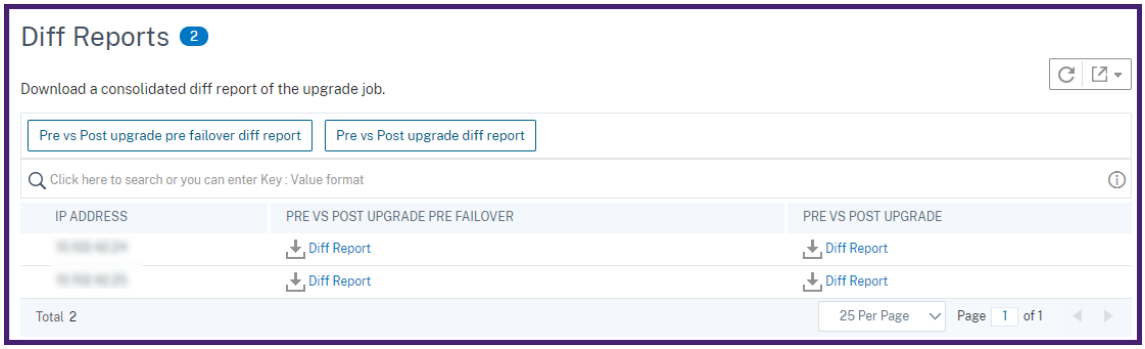
Para descargar un informe diff de un trabajo de actualización, haga lo siguiente:

1. Vaya a **Infraestructura > Trabajos de configuración > Trabajos de mantenimiento**.
2. Seleccione el trabajo de actualización para el que quiere descargar un informe de diferencias.
3. Haga clic en **Diff Reports**.

4. En **Informes de diferencias**, descargue un informe diff consolidado del trabajo de actualización seleccionado.

   En esta página, puede descargar cualquiera de los siguientes tipos de informes diff:

   - **Informe de diferencia de conmutación por error anterior a posterior a la actualización**
   - **Informe de diferencia anterior y posterior a la actualización**



Funciones de red

December 2, 2022

Con la función Funciones de red, puede supervisar el estado de las entidades configuradas en las instancias administradas de Citrix Application Delivery Controller (Citrix ADC). Puede ver estadísticas como detalles de transacciones, detalles de conexión y rendimiento de un servidor virtual de equilibrio de carga. También puede habilitar o deshabilitar 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

November 16, 2022

Citrix ADM le permite ver los informes de las entidades de instancia de Citrix Application Delivery Controller (Citrix ADC) en todos los niveles. Hay dos tipos de informes que puede descargar en **Citrix ADM > Network Functions** : informes consolidados e informes individuales.

Informes consolidados: puede descargar y ver un informe consolidado o resumido de todas las entidades que se administran en instancias de Citrix ADC.

Este informe le permite tener una vista de alto nivel de la asignación entre las instancias, particiones y las entidades de equilibrio de carga correspondientes (servidores virtuales, grupos de servicios y servicios) que están presentes en la red.

La siguiente imagen muestra un ejemplo de un informe resumido.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb1#0.0.0.0:0		cs_svc1#192.168.4.56:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	cs_lb2#0.0.0.0:0		cs_svc2#192.168.4.57:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s1#192.168.4.51:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s3#192.168.4.53:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s5#192.168.4.55:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s4#192.168.4.54:80	
10.221.48.22-10.221.48.202	VPX10.221.48.202		Load Balancing	v1#192.168.3.100:80		s2#192.168.4.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	cs_lb3#0.0.0.0:0		cs_svc3#192.168.2.58:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s4#192.168.2.54:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s1#192.168.2.51:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s2#192.168.2.52:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s3#192.168.2.53:80	
10.221.48.21-10.221.48.201	VPX10.221.48.201		Load Balancing	vs1#192.168.1.100:443		s5#192.168.2.55:80	

El informe consolidado está en formato CSV. Las entradas de cada columna se describen de la siguiente manera:

- **Dirección IP de Citrix ADC**: la dirección IP de la instancia de Citrix ADC se muestra en el informe
- **Nombre de host de Citrix ADC**: 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

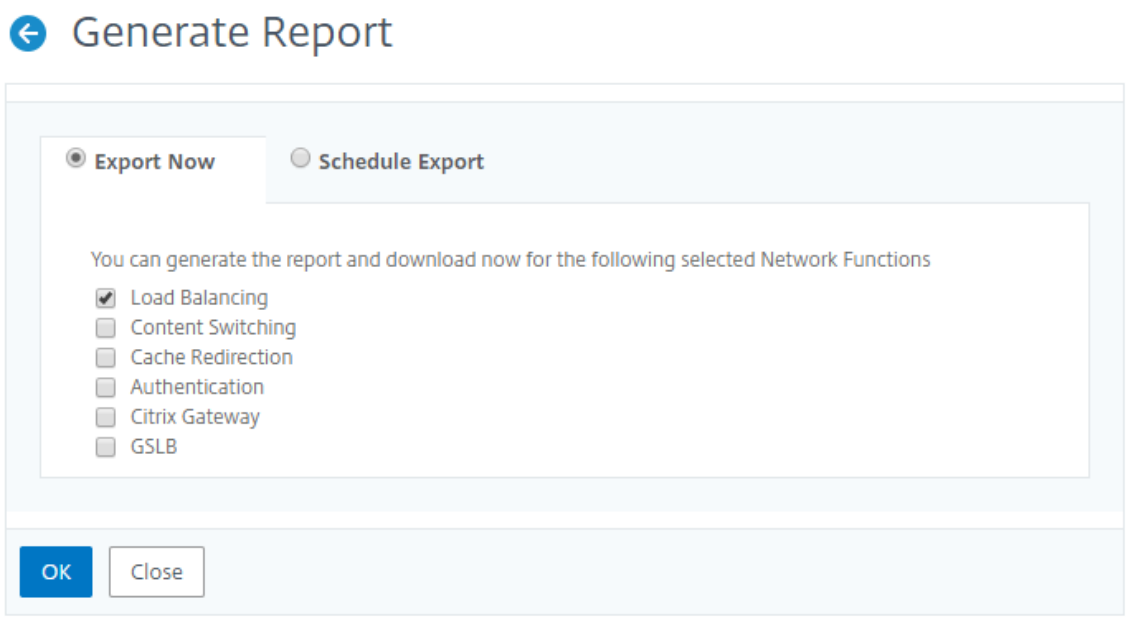
> **Nota**
>
> - Si no hay ningún nombre de host disponible, se muestra la dirección IP correspondiente.
> - Las columnas en blanco indican que las entidades respectivas no están configuradas para esa instancia de Citrix ADC.

Informes individuales: también puede descargar y ver informes independientes de todas las instancias y entidades. Por ejemplo, puede descargar un informe solo para servidores virtuales o servicios de equilibrio de carga o grupos de servicios de equilibrio de carga.

Citrix ADM le permite descargar el informe al instante. También puede programar el informe para que se genere a una hora fija una vez al día, una vez a la semana o una vez al mes.

Generar un informe de equilibrio de carga combinado

1. En Citrix ADM, vaya a **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**.

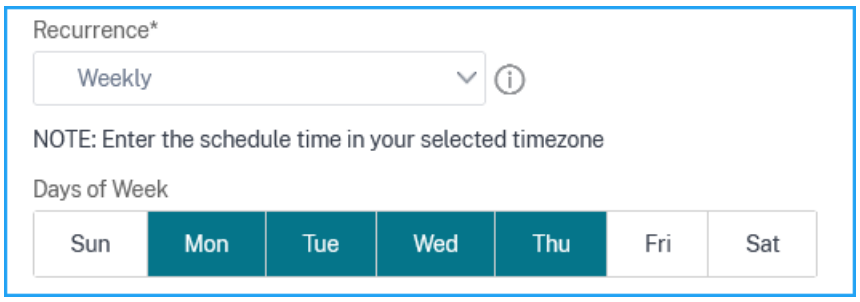
      El informe consolidado se descarga en su sistema.

   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.



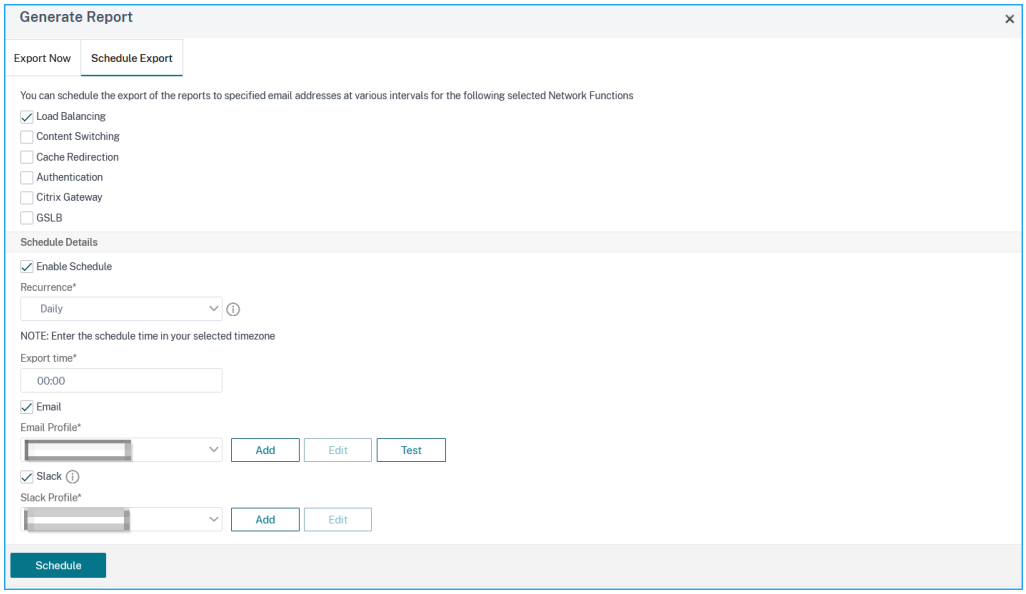
> **Nota**
>
> Si selecciona Periodicidad **mensual**, asegúrese de especificar días del mes, con valores comprendidos entre 1 y 31.

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.

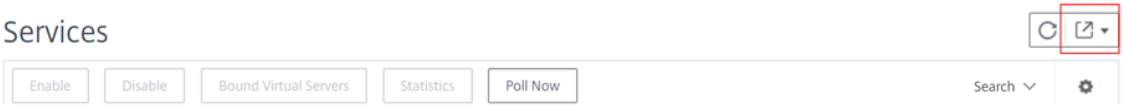
vi. Haga clic en **Programar** para completar el proceso.



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 Citrix ADM, vaya a **Infraestructura > Funciones de red > Equilibrio de carga > Servicios**.
2. En la página **Servicios**, haga clic en el botón **Exportar** en la esquina superior derecha.



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 Citrix ADM.

Exportar o programar la exportación de informes de funciones de red

December 21, 2022

Puede generar un informe completo para funciones de red seleccionadas, como el equilibrio de carga, el cambio de contenido, la redirección de caché, el equilibrio de carga global de servidores (GSLB), la autenticación y Citrix Gateway en Citrix ADM. 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 Citrix ADC
- 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.

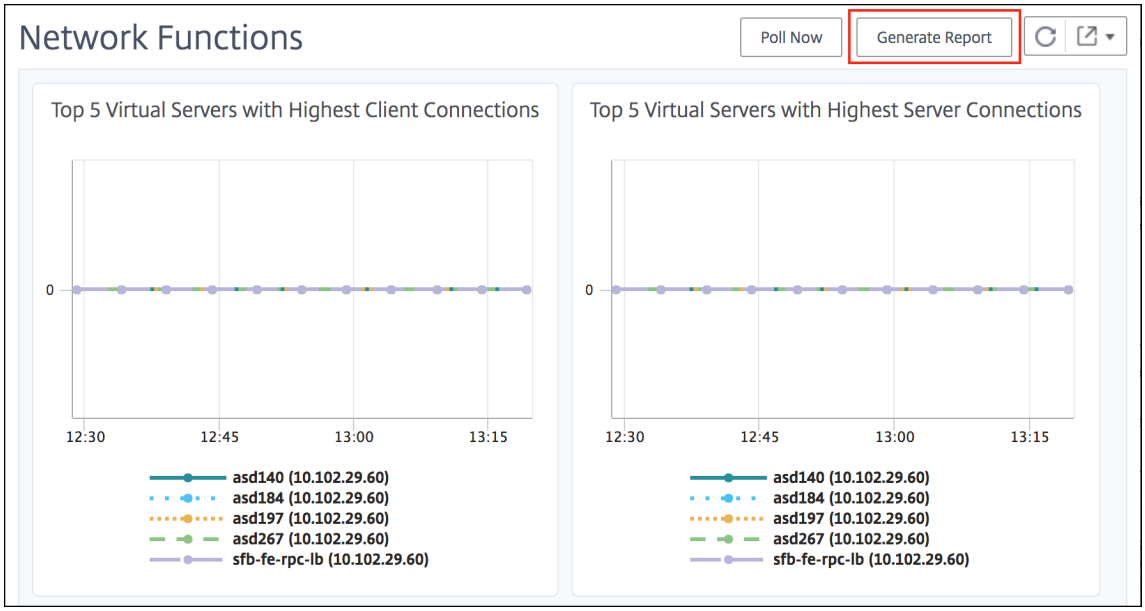
- Nombre del servicio
- Nombre del grupo de servicios

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 Citrix ADM no mantiene una lista independiente de servidores virtuales SSL.
> - Cuando se genera un nuevo informe, los informes antiguos se depuran automáticamente de su cuenta.

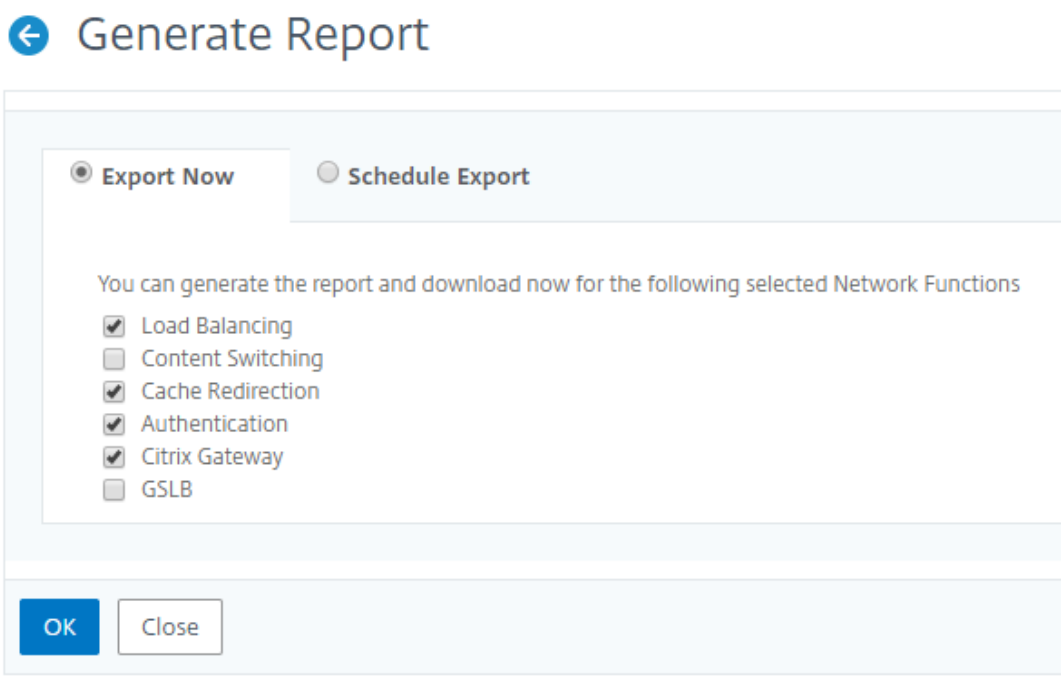
Para exportar y programar informes de funciones de red:

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.

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
121.123.020.85	121.123.020.85		Load Balancing				
121.123.020.100	NS		Load Balancing				
121.123.020.101	admin-NetScalerVPX-10.102.122.101		Load Balancing				
121.123.020.111	PartitionsHost-sp-final-NetScalerVPX	121.123.020.111-partition_	Load Balancing				
121.123.020.115	121.123.020.115	121.123.020.115-partition-	Load Balancing				
121.123.020.139	NS1		Load Balancing				
121.123.020.49	NS1		Load Balancing				

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.

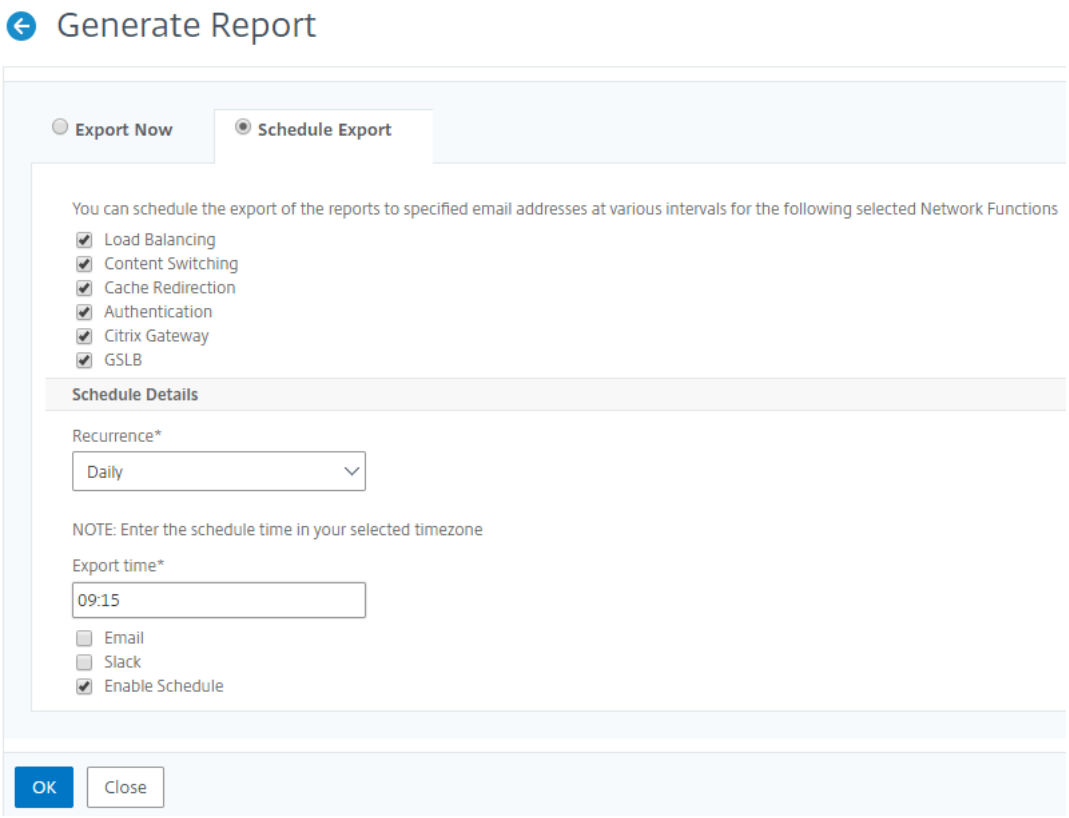
   i. **Periodicidad**: Seleccione **Diario**, **Semanal** o **Mensual** en el cuadro de lista desplegable.

   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

December 2, 2022

Puede optimizar el uso de los recursos mediante la supervisión de los informes de red en Citrix ADM. Es posible que tenga una implementación distribuida con muchas aplicaciones implementadas en varias ubicaciones. Para garantizar un rendimiento óptimo de sus aplicaciones, también ha implementado varias instancias de Citrix Application Delivery Controller (Citrix ADC) para equilibrar la carga, cambiar el contenido o comprimir el tráfico. El rendimiento de la red puede afectar al rendimiento de la aplicación. Para continuar manteniendo el rendimiento de sus aplicaciones, debe supervisar regularmente el rendimiento de la red y asegurarse de que todos los recursos se utilizan de manera óptima.

Citrix ADM permite generar informes no solo para instancias a nivel global, sino también para entidades como los servidores virtuales y las interfaces de red. Los servidores virtuales para los que puede generar informes son los siguientes:

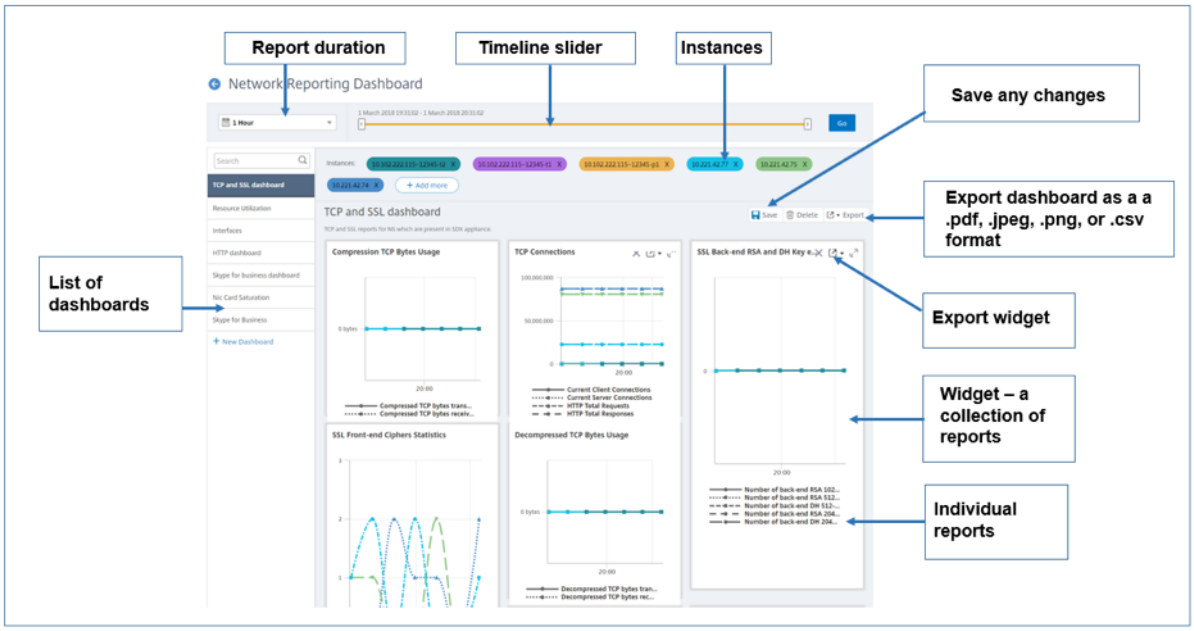
- Servidores, servicios y grupos de servicios de equilibrio de carga
- Servidores de conmutación de contenido
- Servidores de redirección de caché

- Equilibrio de carga de servicio global (GSLB)
- Autenticación
- Citrix Gateway

El panel de informes de red de Citrix ADM es altamente personalizable. Puede crear varios paneles para varias instancias, servidores virtuales y otras entidades.

Panel de informes de red

La siguiente imagen muestra las distintas funciones del panel de control:



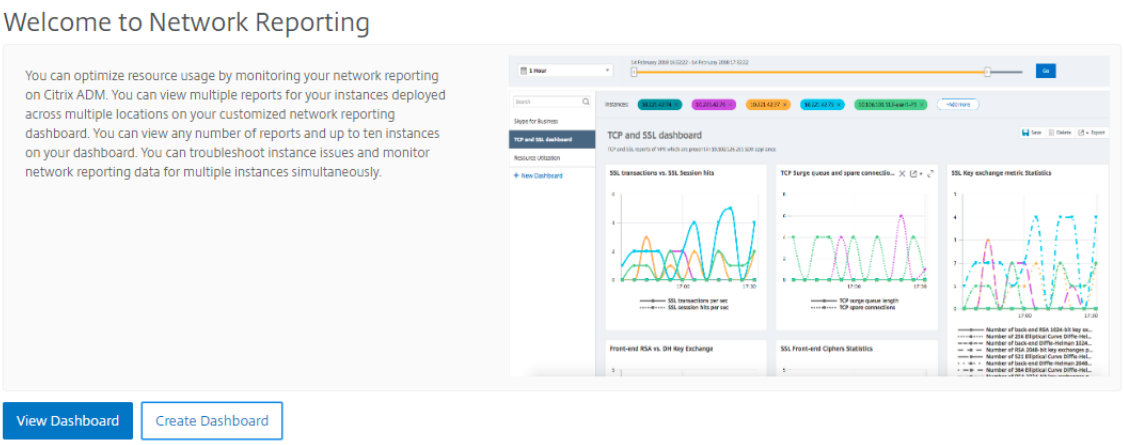
- El panel del lado izquierdo muestra todos los paneles personalizados creados en Citrix ADM. Puede hacer clic en uno de ellos para ver los diversos informes de los que está compuesto el panel. Por ejemplo, un panel TCP y SSL contiene varios informes relacionados con protocolos TCP y SSL.
- Puede personalizar cada panel con varios widgets para mostrar varios informes. Un widget representa un informe en el panel, es decir, una colección de informes más relacionados. Por ejemplo, un informe de uso de bytes TCP de compresión contiene informes de bytes TCP comprimidos transferidos y recibidos por segundo.
- Puede mostrar informes de una hora, un día, una semana o un mes. Además, ahora puede usar la opción de control deslizante de la línea de tiempo para personalizar la duración de los informes que se generan en Citrix ADM.
- Para eliminar un informe, haga clic en la «X». También puede exportar el informe como formato.pdf,.jpeg,.png o.csv al sistema. También puede programar una hora y una periodicidad de cuándo 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 Citrix ADM le permite ver informes de 10 instancias.
- También puede exportar todo el panel de control en formato .pdf, .jpeg, png o .csv a su sistema. Se deben guardar todos los cambios realizados en el panel de control. Haga clic en Guardar para guardar los cambios.

En la siguiente sección se explican en detalle las tareas para crear un panel, generar informes y exportar informes.

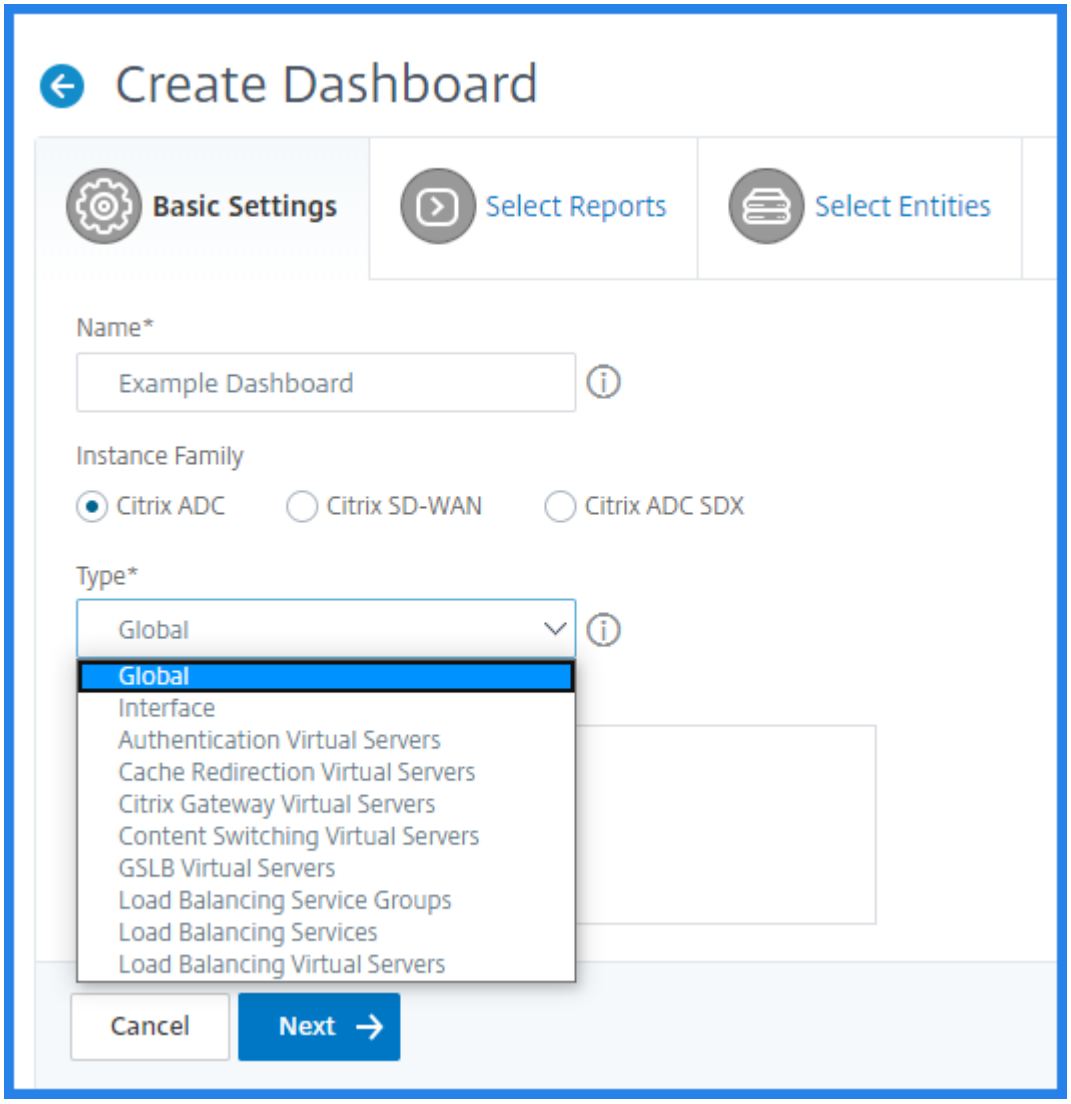
Para ver o crear un tablero de mandos:

1. En Citrix ADM, vaya a **Infraestructura > Informes de red**.



2. Para ver los paneles existentes, haga clic en **Ver panel**. Se abre la página **Panel** de informes de red, donde puede ver todos los paneles y widgets de informes.
3. Para crear un panel, haga clic en **Crear panel**.

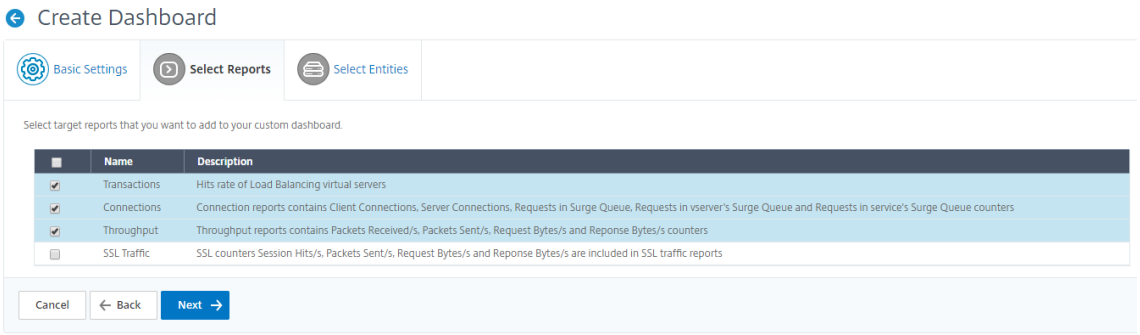
   Se abre la página **Crear panel** de control.



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: Citrix ADC o Citrix ADC SDX.

   <!–1. **Familia de instancias**. Seleccione el tipo de instancia: Citrix ADC, Citrix SD-WAN o Citrix ADC SDX. —>

   a) **Tipo**. 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.

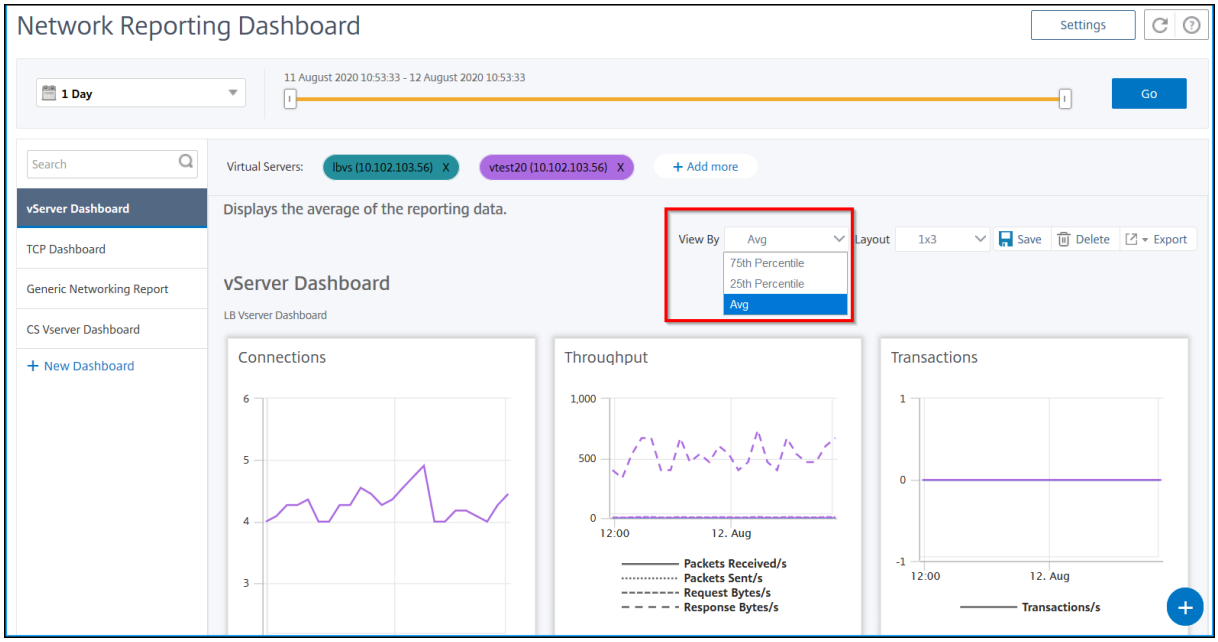
9. Haga clic en **Crear**.

Se crea el panel de control y muestra todos los informes que ha seleccionado.

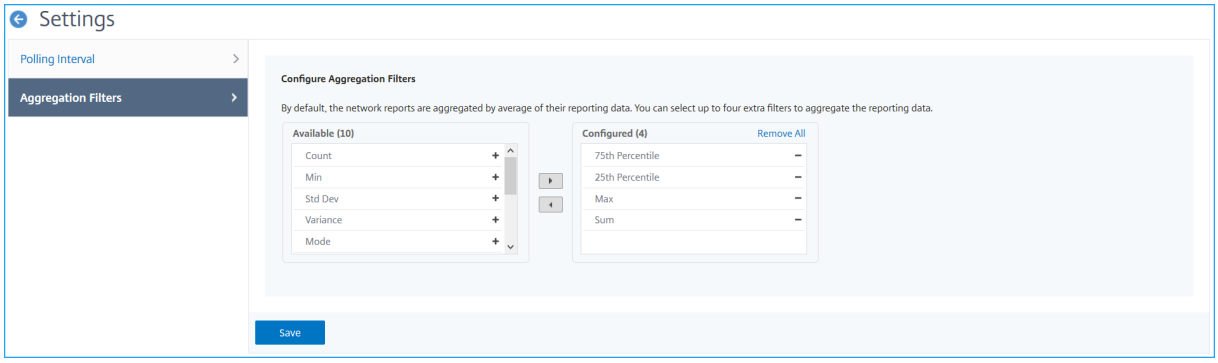
> **Nota**
>
> Actualmente, los cambios que realice en leyendas o filtros no se pueden guardar.

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. Mediante estas agregaciones aplicadas a los datos, puede analizar y garantizar si todos los recursos se utilizan de forma óptima. Vaya a **Red > Informes de red** y seleccione la duración de 1 día o más para obtener la opción **Ver por**.



En los datos medios existentes, puede aplicar agregaciones seleccionando la opción de la lista **Ver por**. Cuando se aplica la agregación, los datos se actualizan para cada métrica en el tablero de mandos. Haga clic en **Configuración** y seleccione **Filtros de agregación**.



Las siguientes son las agregaciones que puede agregar:

- Recuento
- Máx.
- Mín.

- Suma
- Desarrollo de Std
- Desviación
- Modo
- Mediana
- Percentil 25
- Percentil 75
- Percentil 95
- Percentil 99
- Primera
- Última

Puede agregar hasta 4 opciones de agregación al panel. Después de agregar las opciones de agregación, Citrix ADM tarda aproximadamente 1 hora en generar informes para las opciones de agregación seleccionadas.

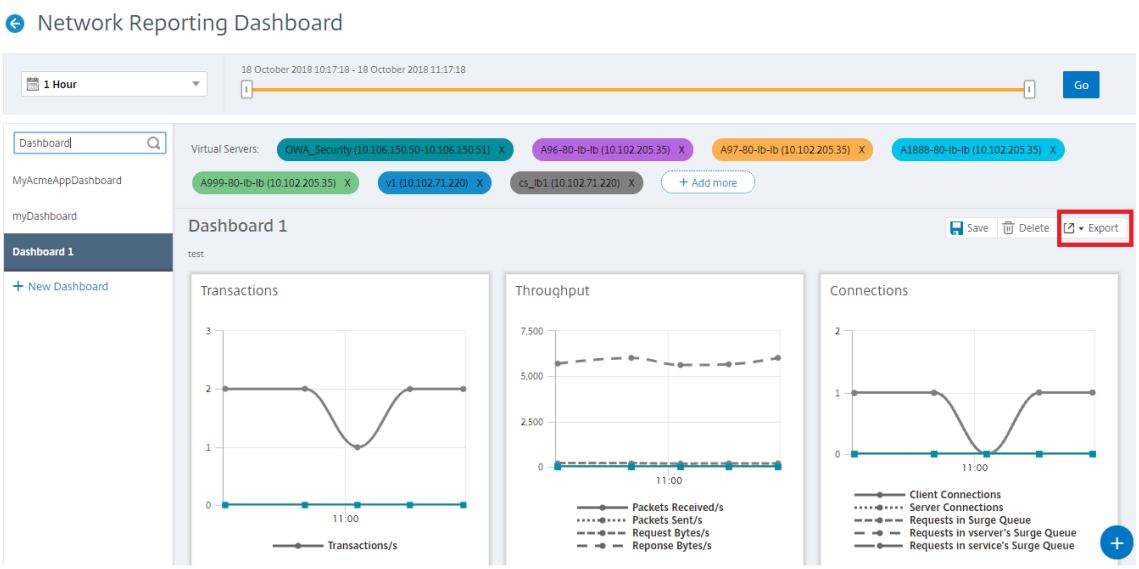
Exportación de informes de red

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 Citrix ADM si tiene permisos de solo lectura. Necesita un permiso de edición para poder crear un archivo en Citrix ADM y poder exportarlo.

Para exportar informes de paneles:

1. Vaya a **Infraestructura > Informes de red**
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, haga clic en **Panel 1**.
4. Haga clic en el botón de exportación situado en la esquina superior derecha de la página.
5. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.



En la página **Exportar**, puede realizar una de las siguientes acciones:

6. Seleccione la ficha **Exportar ahora** . Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
7. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

   Puede programar una exportación de la página **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, asegúrese de seleccionar los días de la semana en los que quiere que se programe el informe.
> - Si selecciona Periodicidad mensual, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

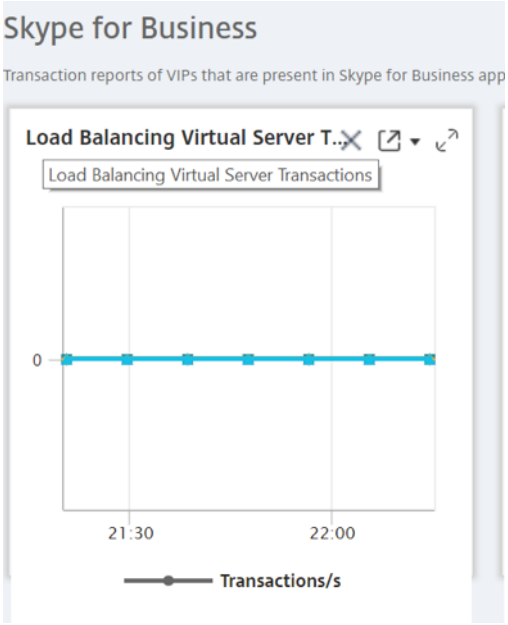
Al programar informes de red, puede personalizar el encabezado del informe escribiendo una cadena de texto en el campo **Asunto**. El informe creado a la hora programada tiene esta cadena como nombre.

Por ejemplo, para los informes de red que se originan en un servidor virtual concreto, puede escribir el asunto «authentication-reports-10.106.118.120», donde 10.106.118.120 es la dirección IP del servidor virtual supervisado.

> **Nota:**
>
> Actualmente, esta opción solo está disponible cuando se programa la exportación de informes. No puede agregar un encabezado al informe cuando los exporta al instante.

Para exportar informes de widgets:

1. Vaya a **Infraestructura > Informes de red**.
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, también haga clic en **Skype Empresarial**.
4. Seleccione un widget. Por ejemplo, seleccione **Load Balancing Virtual Server Transactions**.
5. Haga clic en el botón de exportación en la esquina superior derecha de la página
6. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.



Cómo administrar Umbrales para Informes de Red en Citrix ADM

Para supervisar el estado de una instancia de Citrix ADC, puede establecer umbrales en los contadores y recibir notificaciones cuando se supera un umbral. En Citrix ADM, puede configurar los umbrales y verlos, modificarlos y eliminarlos.

Por ejemplo, puede recibir una notificación por correo electrónico cuando el contador de conexiones de un servidor virtual de conmutación de contenido alcance un valor especificado. Puedes 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 **recuadro Eventos por gravedad** para ver los eventos por gravedad.

También puede asociar una acción a un umbral, como enviar un mensaje de correo electrónico o SMS cuando se incumple el umbral.

Para crear un umbral:

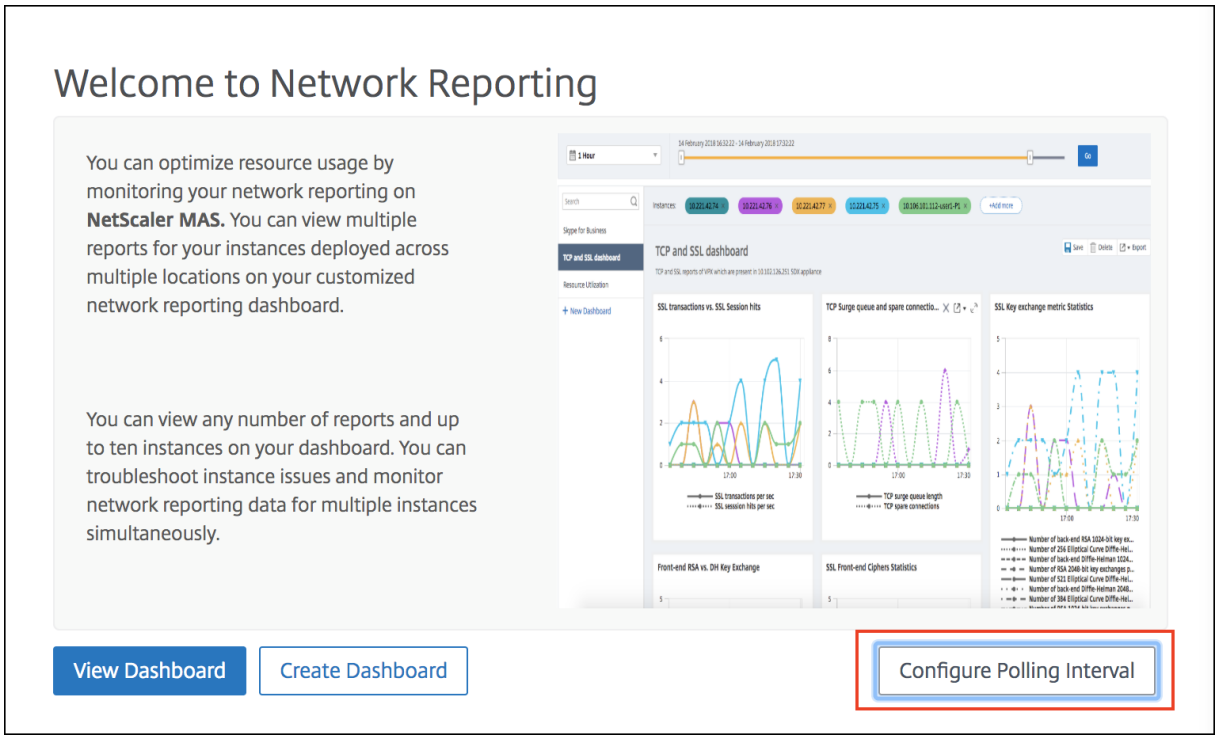
1. En Citrix ADM, vaya a **Infraestructura > Informes de red > Umbrales**. En **Umbrales**, haga clic en **Agregar**.
2. En la página **Crear umbral**, especifique los siguientes detalles:
    - **Nombre**. Nombre del umbral.
    - **Tipo de instancia**. Elija Citrix ADC.
    - **Nombre del informe**. 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 **recuadro Eventos por gravedad** para ver los eventos por 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. Elija la dirección IP de la instancia o instancias para las que quiere establecer el umbral.
5. También puede agregar un **mensaje de evento**. Escriba el mensaje que quiera que aparezca cuando se alcance el umbral. Citrix ADM agrega el valor supervisado y el valor umbral a este mensaje.
6. Seleccione **Activar** para habilitar el umbral para generar alarmas.

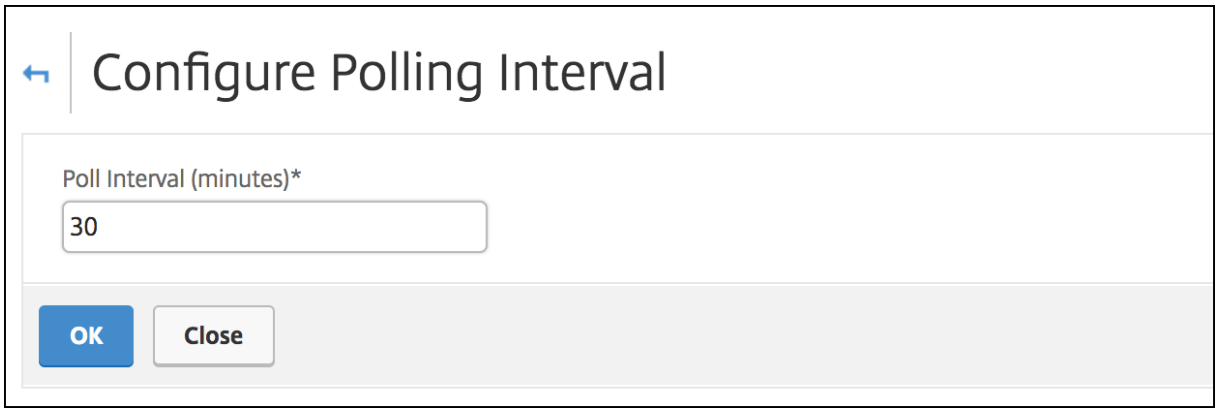
7. Opcionalmente, puede configurar **Acciones** como notificaciones de correo electrónico o Slack.
8. Haga clic en **Crear**.

Establecer el intervalo de sondeo de rendimiento para los informes

De forma predeterminada, cada 5 minutos, las llamadas NITRO recopilan datos de rendimiento para la generación de informes de red. El Citrix ADM recupera las estadísticas de las instancias, como la información de los contadores, y las agrega según el minuto, la hora, el día o la 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 depuración de los datos de informes de red en Citrix ADM. Este intervalo limita la cantidad de datos de informes de red que se almacenan en la base de datos del servidor Citrix ADM. De forma predeterminada, la poda ocurre cada 24 horas (a las 01.00 horas) para la red que informa de datos históricos.

> **Nota**
>
> El valor que puede especificar no puede superar los 90 días ni ser inferior a 1 día.

Provisioning de instancias VPX de Citrix ADC en AWS

November 16, 2022

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 Citrix ADC en AWS, puede ampliar sin problemas su pila de red L4-L7 a AWS. Con Citrix ADC VPX, AWS se convierte en una extensión natural de su infraestructura de TI local. Puede usar Citrix ADC 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 Citrix ADM que supervisa sus instancias de Citrix ADC, 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.

Término	Definición
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.
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:

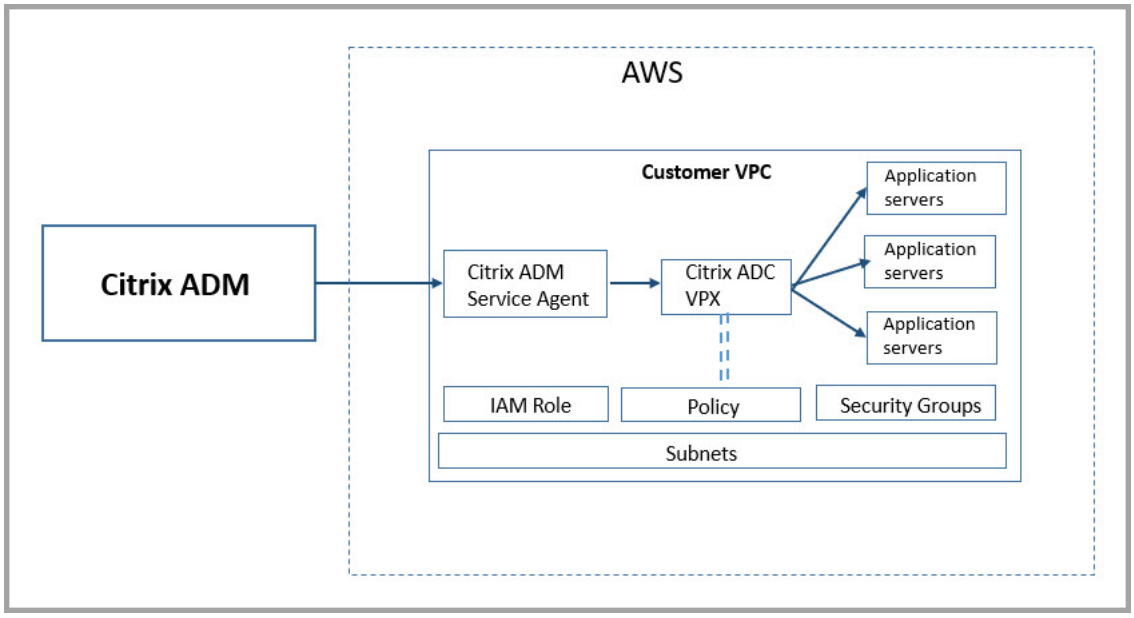
- Posee una cuenta de AWS.
- Ha creado la VPC necesaria y ha seleccionado las zonas de disponibilidad.
- Ha agregado el agente Citrix ADM en AWS.

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

Para obtener más información sobre cómo instalar el agente Citrix ADM en AWS, consulte Instalación del agente Citrix ADM en AWS.

Diagrama de arquitectura

La siguiente imagen proporciona una descripción general de cómo Citrix ADM se conecta con AWS para aprovisionar instancias de Citrix ADC VPX en AWS.



Tareas de configuración

Realice las siguientes tareas en AWS antes de aprovisionar instancias de Citrix ADC VPX en Citrix ADM:

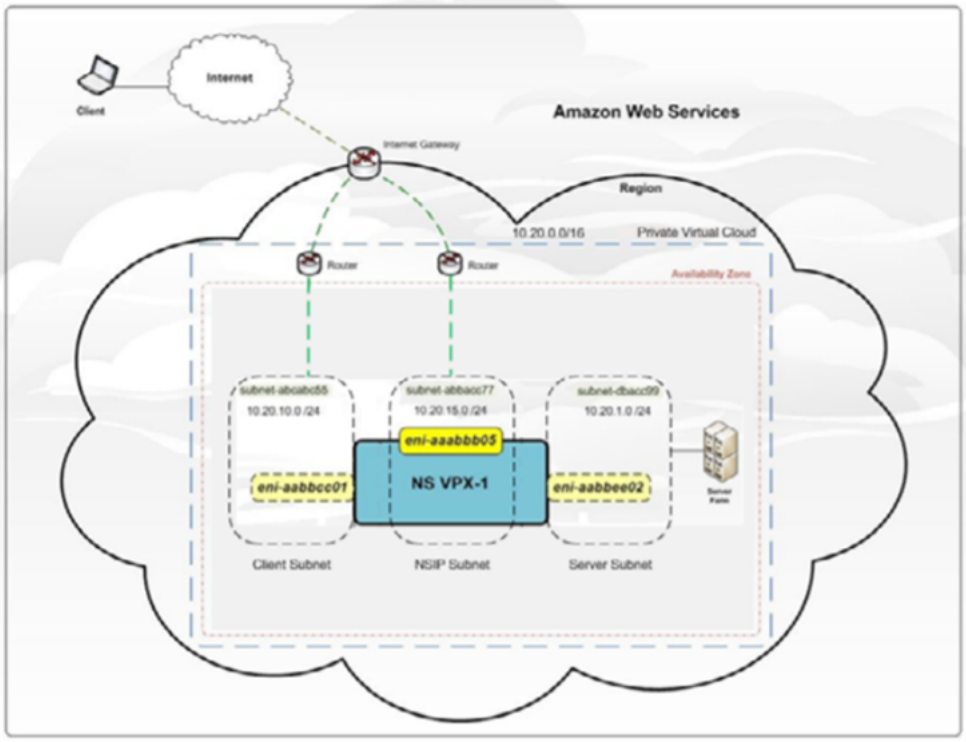
- Crear subredes
- Crear grupos de seguridad
- Crear un rol de IAM y definir una directiva

Realice las siguientes tareas en Citrix ADM para aprovisionar las instancias en AWS:

- Crear sitio
- Aprovisione la instancia Citrix ADC VPX en AWS

Para crear subredes

Crea tres subredes en tu VPC. Las tres subredes que se requieren para aprovisionar instancias de Citrix ADC 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 Citrix ADC 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 tus instancias, es posible que desees crear tus 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.

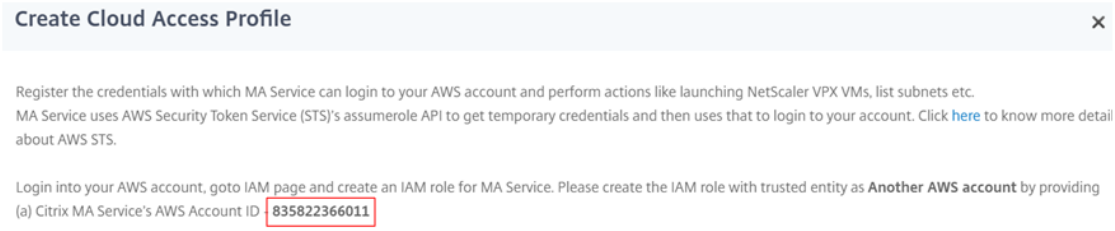
Para obtener más información sobre los grupos de seguridad, consulte Grupos de seguridad para su VPC.

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. Está conectando su cuenta de AWS con la cuenta de AWS en Citrix ADM. Por lo tanto, seleccione **Otra cuenta de AWS** para permitir que Citrix ADM realice acciones en su cuenta de AWS.

   Escriba el ID de cuenta de AWS de Citrix ADM de 12 dígitos. El ID de Citrix es 835822366011. También puede encontrar el ID de Citrix en Citrix ADM 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":
[
    {

```



```
8            "Effect": "Allow",
9           "Action": [
10              "ec2:DescribeInstances",
11              "ec2:DescribeImageAttribute",
12              "ec2:DescribeInstanceAttribute",
13              "ec2:DescribeRegions",
14              "ec2:DescribeDhcpOptions",
15              "ec2:DescribeSecurityGroups",
16              "ec2:DescribeHosts",
17              "ec2:DescribeImages",
18              "ec2:DescribeVpcs",
19              "ec2:DescribeSubnets",
20              "ec2:DescribeNetworkInterfaces",
21              "ec2:DescribeAvailabilityZones",
22              "ec2:DescribeNetworkInterfaceAttribute",
23              "ec2:DescribeInstanceStatus",
24              "ec2:DescribeAddresses",
25              "ec2:DescribeKeyPairs",
26              "ec2:DescribeTags",
27              "ec2:DescribeVolumeStatus",
28              "ec2:DescribeVolumes",
29              "ec2:DescribeVolumeAttribute",
30              "ec2:CreateTags",
31              "ec2:DeleteTags",
32              "ec2:CreateKeyPair",
33              "ec2:DeleteKeyPair",
34              "ec2:ResetInstanceAttribute",
35              "ec2:RunScheduledInstances",
36              "ec2:ReportInstanceStatus",
37              "ec2:StartInstances",
38              "ec2:RunInstances",
39              "ec2:StopInstances",
40              "ec2:UnmonitorInstances",
41              "ec2:MonitorInstances",
42              "ec2:RebootInstances",
43              "ec2:TerminateInstances",
44              "ec2:ModifyInstanceAttribute",
45              "ec2:AssignPrivateIpAddresses",
46              "ec2:UnassignPrivateIpAddresses",
47              "ec2:CreateNetworkInterface",
48              "ec2:AttachNetworkInterface",
49              "ec2:DetachNetworkInterface",
50              "ec2:DeleteNetworkInterface",
51              "ec2:ResetNetworkInterfaceAttribute",
52              "ec2:ModifyNetworkInterfaceAttribute",
```



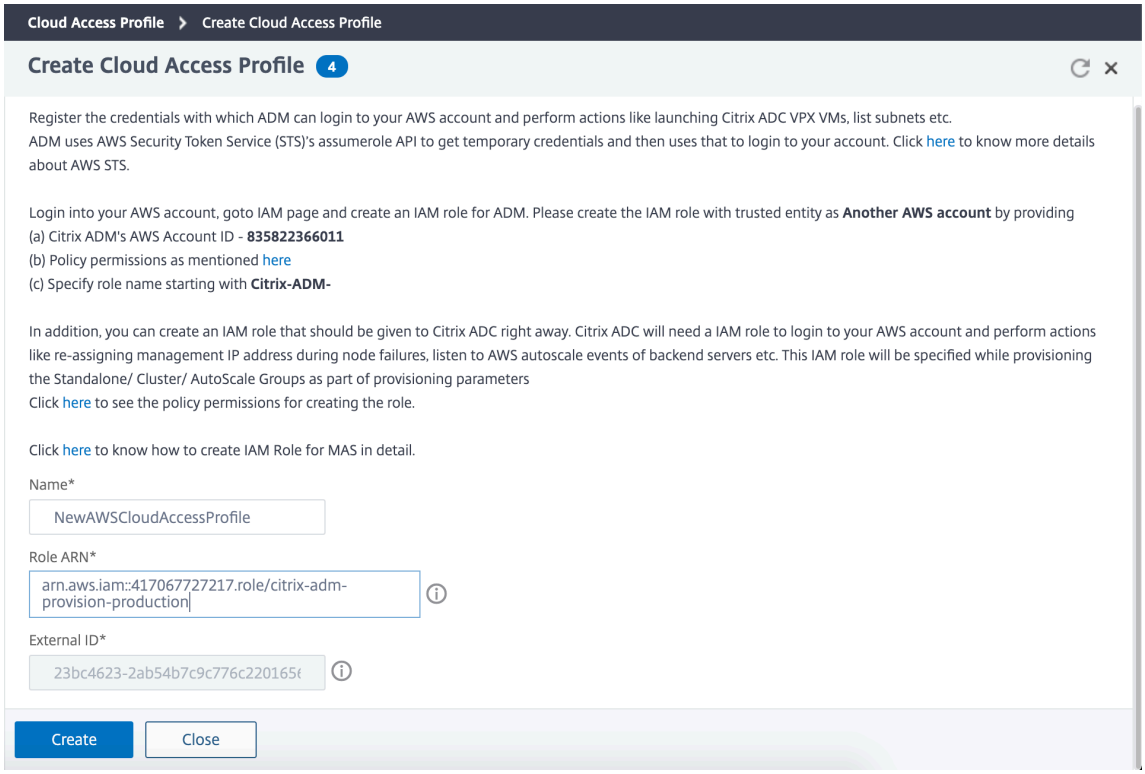
```
53              "ec2:AssociateAddress",
54              "ec2:AllocateAddress",
55              "ec2:ReleaseAddress",
56              "ec2:DisassociateAddress",
57              "ec2:GetConsoleOutput"
58          ],
59              "Resource": "*"
60      }
61
62 ]
63  }
64
65 <!--NeedCopy-->
```

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 Citrix ADM

Cree un sitio en Citrix ADM y agregue los detalles de la VPC asociada a su rol de AWS.

1. En Citrix ADM, 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 CIDR, asociados a su rol de IAM en AWS, se importan en Citrix ADM.

6. Escriba un nombre para el sitio.
7. Haga clic en **Crear**.

Para aprovisionar Citrix ADC VPX en AWS

Utilice el sitio que creó anteriormente para aprovisionar las instancias VPX de Citrix ADC en AWS. Proporcione los detalles del agente Citrix ADM para aprovisionar las instancias que están enlazadas a ese agente.

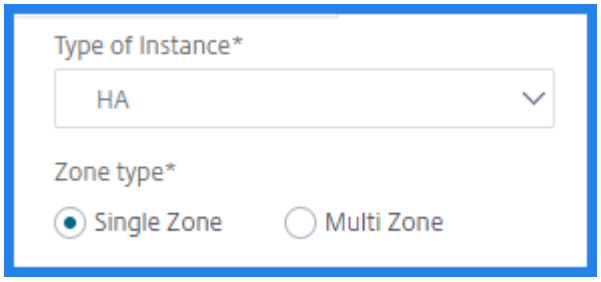
1. En Citrix ADM, vaya a **Infraestructura > Instancias > Citrix ADC**.
2. En la ficha **VPX**, haga clic en **Aprovisionar**.

   Esta opción muestra la página **Provisionar Citrix ADC 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 aprovisiona una instancia de Citrix ADC VPX independiente en AWS.

- **HA:** Esta opción aprovisiona las instancias de Citrix ADC VPX de alta disponibilidad en AWS.

  Para aprovisionar las instancias VPX de Citrix ADC en la misma zona, seleccione la opción **Zona única** en **Tipo de zona**.

  Para aprovisionar las instancias de Citrix ADC 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 ADC VPX.

c) En **Sitio**, seleccione el sitio que creó anteriormente.

d) En **Agente**, seleccione el agente que se crea para administrar la instancia VPX de ADC.

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.

Citrix ADM utiliza el perfil del dispositivo cuando requiere iniciar sesión en la instancia de Citrix ADC VPX.

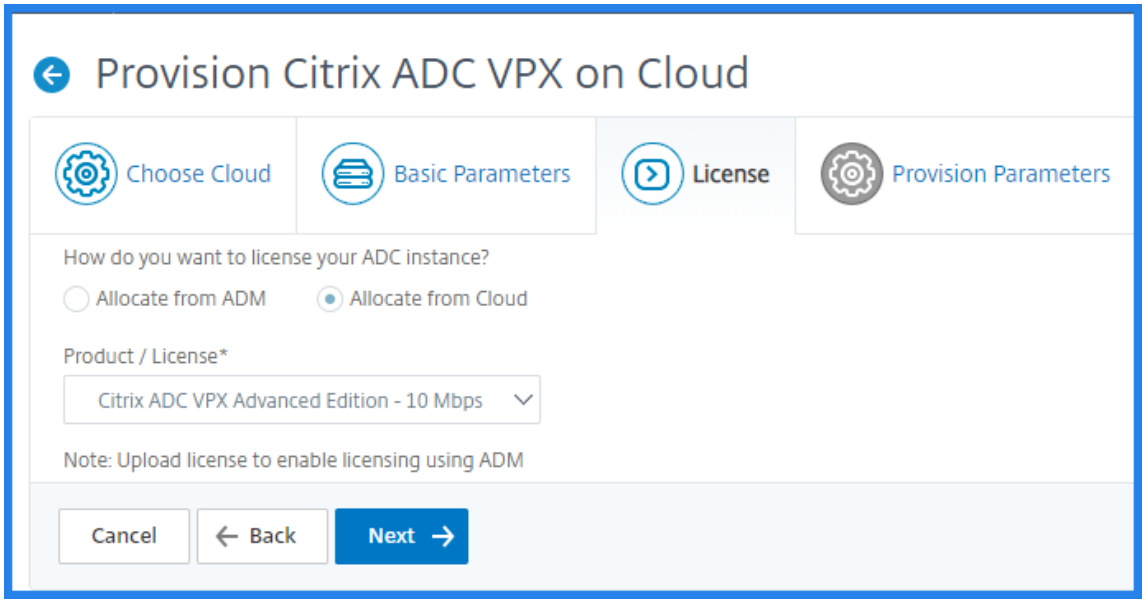
g) Haga clic en **Siguiente**.

5. En la ficha **Licencia**, seleccione uno de los siguientes modos para aplicar la licencia a una instancia de ADC:

   - **Uso de Citrix ADM**: la instancia que quiere aprovisionar comprueba las licencias de Citrix ADM.
   - **Uso de la nube de AWS**: la opción **Asignar desde la nube** utiliza las licencias de productos Citrix 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 ficha **Licencia**, si selecciona **Asignar desde Citrix ADM**, 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 ADC desprotege una licencia de instancia y sólo se especifica tanto ancho de banda.

     - **Licencias VPX:** Cuando se aprovisiona una instancia de Citrix ADC VPX, la instancia retira la licencia del Citrix ADM.

     Licencias de CPU virtuales: la instancia de Citrix ADC VPX aprovisionada comprueba las licencias en función del número de CPU que se ejecutan en la instancia.

     > **Nota**
     >
     > Cuando se quitan o destruyen las instancias aprovisionadas, las licencias aplicadas vuelven al grupo de licencias Citrix ADM. Estas licencias se pueden reutilizar para aprovisionar nuevas instancias.

   a) En **Edición de licencia**, seleccione la edición de licencia. El Citrix ADM usa la edición especificada para aprovisionar 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 Citrix ADC que quiere aprovisionar.

c) Seleccione el tipo de instancia EC2 de la lista de **tipos de instancia** .

En esta lista se muestran los tipos de instancias de AMI compatibles con el producto ADC seleccionado.

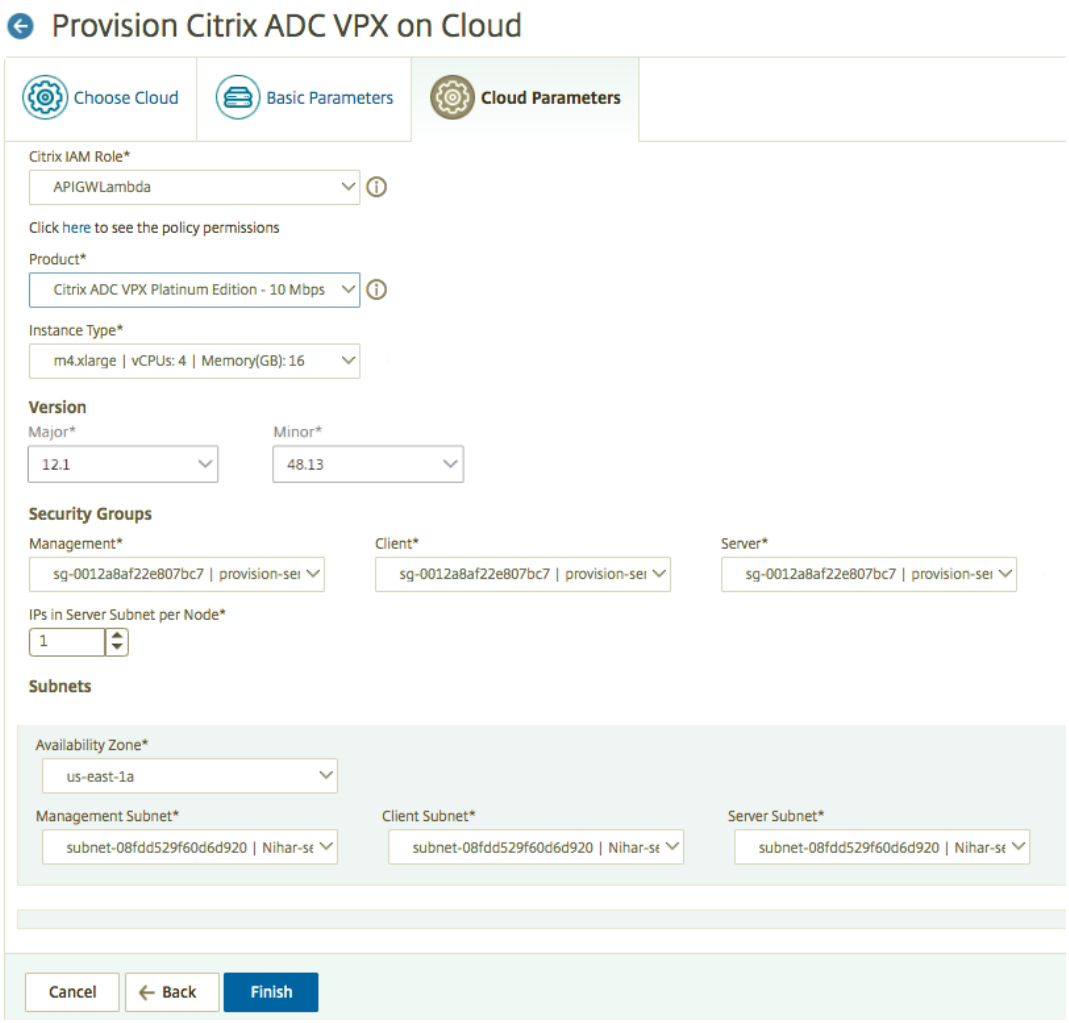
d) Seleccione la **versión** de Citrix ADC que quiere aprovisionar. Seleccione la versión **principal** y la **secundaria** de Citrix ADC.

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 Citrix ADC VPX se aprovisiona ahora en AWS.

> **Nota:**
>
> Actualmente, Citrix ADM no admite el desaprovisionamiento de instancias de Citrix ADC de AWS.

Para ver Citrix ADC 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 Citrix ADC VPX aprovisionado en AWS.

El nombre de la instancia de Citrix ADC VPX es el mismo que proporcionó al aprovisionar una instancia en Citrix ADM.

Para ver Citrix ADC VPX aprovisionado en Citrix ADM

1. En Citrix ADM, vaya a **Infraestructura > Instancias > Citrix ADC**.
2. Seleccione la ficha **Citrix ADC VPX** .
3. La instancia de Citrix ADC VPX aprovisionada en AWS se muestra aquí.

Capacidad agrupada

November 16, 2022

La capacidad agrupada en Citrix ADC es un marco de licencias que incluye un ancho de banda común y un grupo de instancias que está alojado y gestionado por Citrix ADM. Desde este grupo común, cada instancia ADC del centro de datos, independientemente de la plataforma o el factor de forma, extrae una licencia de instancia y solo el ancho de banda que necesite. El archivo de licencia y, por lo tanto, el ancho de banda no están vinculados 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 Citrix ADM, 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 ADC 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.

Derechos autogestionados del servicio CADS

January 18, 2023

CADS Service Self-Managed es la nueva forma de consumir licencias agrupadas, con un alto grado de automatización en la gestión de licencias y capacidad. 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 Citrix ADM registrado en el servicio Citrix ADM
> - Las versiones de Citrix ADC 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 Citrix ADM 13.1 - 32.x o posterior

Como parte de la función de autogestión del servicio CADS, la información de la licencia se carga automáticamente en el servicio Citrix ADM una vez que el cliente realiza una compra y crea un agente Citrix ADM en el servicio Citrix ADM. Las licencias se descargan directamente al agente servidor de licencias (LSA) o al agente ADM de su VPC o centro de datos, como parte de la infraestructura de ADM.

> **Nota**
>
> El servicio autogestionado CADS solo está disponible en el servicio ADM.

Citrix ADM puede alojar las autorizaciones agrupadas y autoadministradas del servicio CADS existentes. Para usar la licencia requerida, configure un servidor de licencias en el dispositivo Citrix ADC y extraiga o asigne la capacidad del grupo correspondiente.

CADS Service Self Managed incluye las siguientes funciones:

- Disponible en las ediciones Standard, Advanced y Premium
- CADS Citrix gestionó una autorización premium de 100 TB más de 8 millones de consultas de 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 de ADM como complementos

Para obtener más información sobre las autorizaciones autogestionadas del servicio CADS disponibles, vaya a **Infraestructura > Autogestionado**.

Puede configurar la dirección IP de un servidor de licencias en Citrix ADC 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 rastrear información como el vencimiento y el uso de la licencia en el servicio ADM.

Asigne la capacidad autogestionada del servicio CADS a las instancias de ADC

November 16, 2022

Puede asignar los derechos y la capacidad autogestionados del servicio CADS de dos maneras:

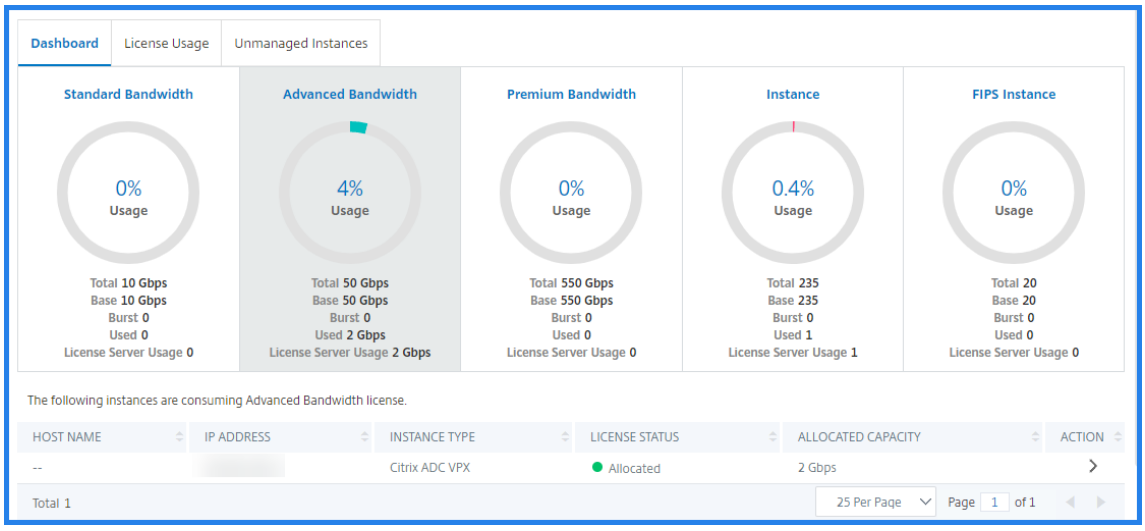
- Uso de la instancia ADC
- Uso de ADM, si ADC es administrado por ADM.

Para asignar la capacidad autoadministrada del servicio CADS desde la GUI de Citrix ADM:

1. Inicie sesión en Citrix ADM.
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 después del reinicio en caliente del ADC.
   >
   > En **Detalles de asignación**, los campos **Solicitado** y **Aplicado se** actualizan al cambiar la asignación de ancho de banda de la instancia.

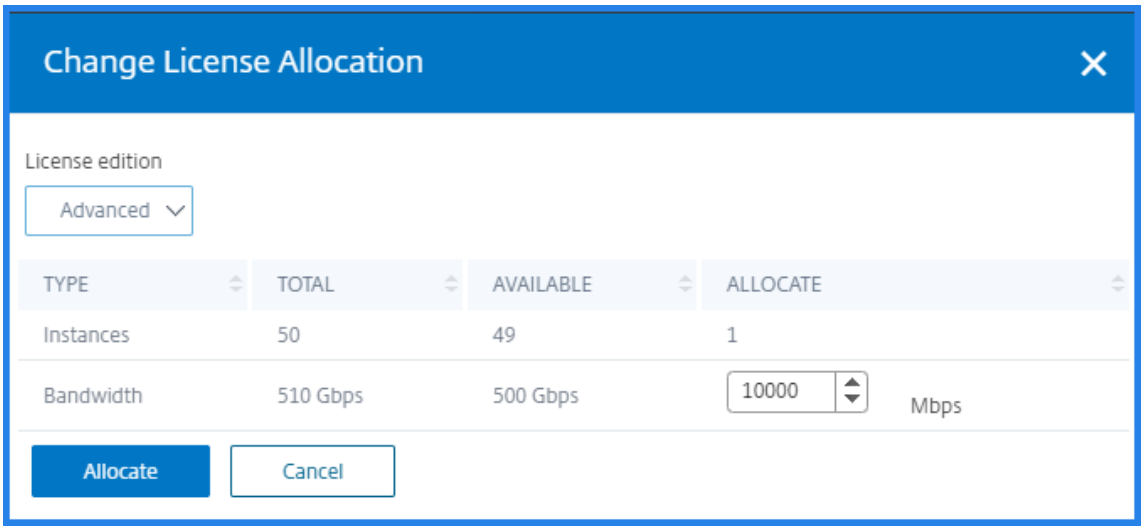
4. Seleccione una instancia ADC de la lista de instancias disponibles haciendo clic en el botón **>**.



   La columna Estado de la licencia muestra los mensajes de estado de asignación de derechos correspondientes.

> **Nota**
>
> La ficha **Instancias no administradas** muestra las instancias detectadas pero no administradas en Citrix ADM.
>
> 
>

5. Haga clic en **Cambiar asignación** o **Liberar asignación** para modificar la asignación de licencias.
6. Aparecerá una ventana emergente con las licencias disponibles en el servidor de licencias.
7. 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**.

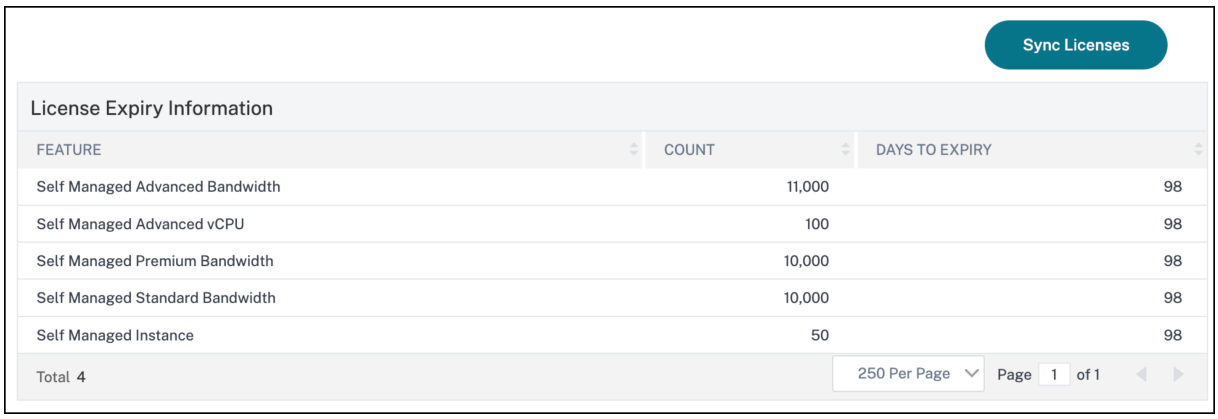


> **Nota**
>
> Reinicie en caliente una instancia si cambia la edición de la licencia.

Consulte la información de derechos autogestionados del servicio CADS

November 18, 2022

Para comprobar los derechos autogestionados del servicio CADS disponibles en Citrix ADM, vaya a **Infraestructura > Autogestión**.



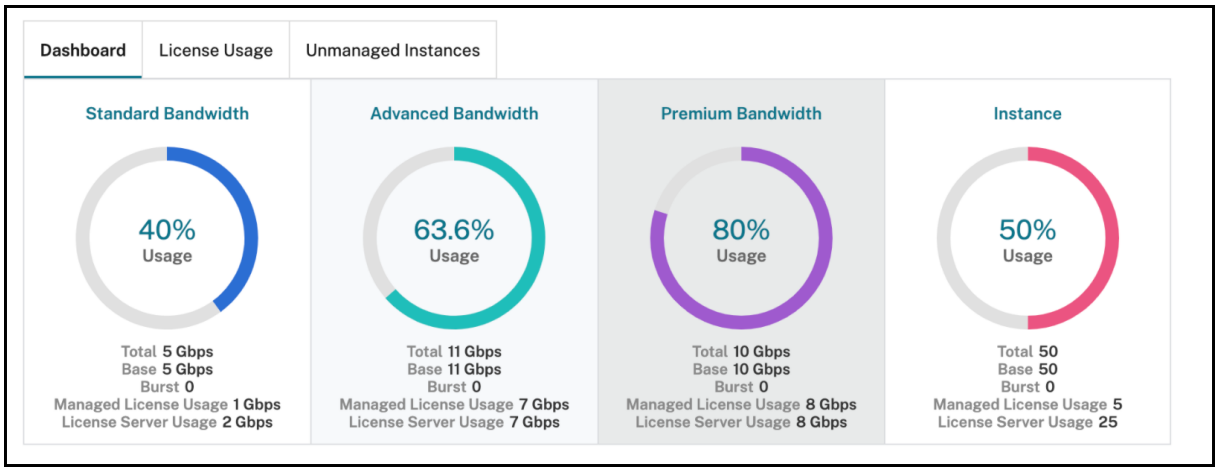
El panel muestra la información sobre las autorizaciones autogestionadas del servicio CADS. Si la información de derechos no aparece en el panel de control o hay un retraso en la adición de la información de derechos, haga clic en el botón **Sincronizar licencias** y aparecerá la información sobre los 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

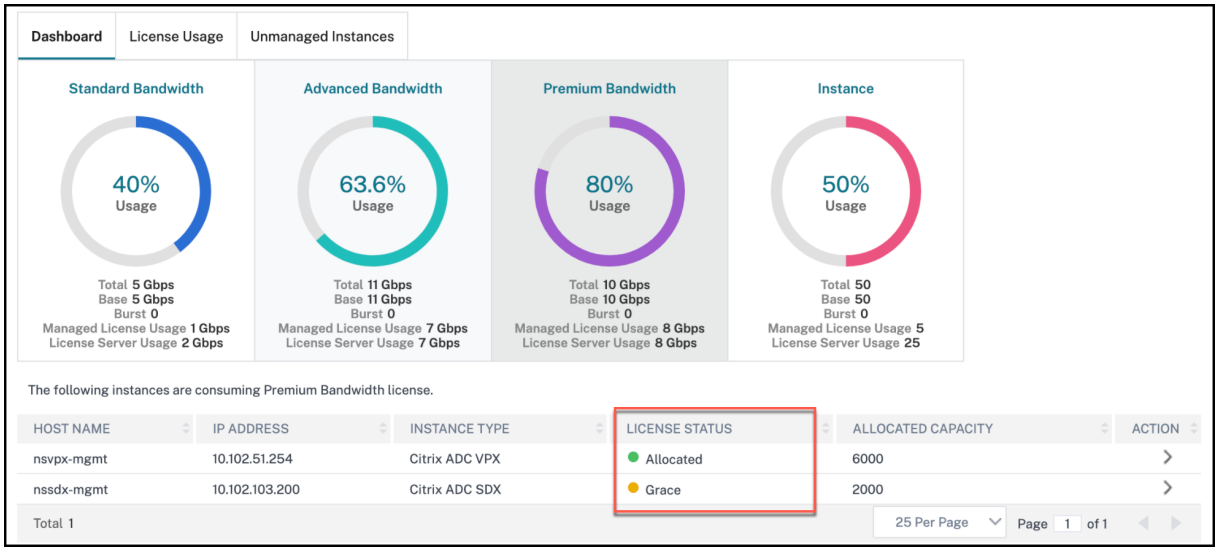
- **Función** : tipo de licencia que va a caducar.
- **Recuento** : número de servidores o instancias virtuales que se verán afectados.
- **Días hasta el vencimiento** : número de días antes del vencimiento de la licencia.

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 Citrix ADM como servidor de licencias para la licencia de capacidad agrupada de ADC, puede utilizar la GUI de Citrix ADM 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

November 16, 2022

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**
>
> - Citrix ADM admite la visibilidad de los clústeres para Service Graph con las versiones 1.14 a 1.23 de Kubernetes.

Puede especificar los siguientes aspectos de la integración de Kubernetes en Citrix ADM:

- **Clúster** : puede registrar o anular el registro de clústeres de Kubernetes para los que Citrix ADM supervisa todos los microservicios y completa el gráfico de servicios. Cuando registre un clúster en Citrix ADM, especifique la información del servidor de la API de Kubernetes. A continuación, seleccione un agente Citrix ADM que pueda acceder 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 Citrix ADM está instalado y configurado para permitir la comunicación entre Citrix ADM y el clúster o las instancias administradas de Kubernetes. Puede usar las instancias administradas que están presentes en su centro de datos o en la nube.
- Cluster Kubernetes registrado en Citrix ADM.

Configure el agente Citrix ADM para que se registre en el clúster de Kubernetes

Para habilitar la comunicación entre el clúster de Kubernetes y Citrix ADM, debe instalar y configurar un agente Citrix ADM. 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 Citrix ADM existente si ya hay uno implementado.

Configurar Citrix ADM con un token secreto para administrar un clúster de Kubernetes

Para que Citrix ADM pueda recibir eventos de Kubernetes, debe crear una cuenta de servicio en Kubernetes para Citrix ADM. Además, configure la cuenta de servicio con los permisos RBAC necesarios en el clúster.

1. Cree una cuenta de servicio para Citrix ADM. Por ejemplo, el nombre de la cuenta de servicio puede ser`citrixadm-sa`. Para crear una cuenta de servicio, consulte Usar varias cuentas de servicio.
2. Utilice el rol `cluster-admin` para vincular la cuenta de Citrix ADM. Este enlace concede un valor `ClusterRole` en todo el clúster a una cuenta de servicio. A continuación, se muestra un comando de ejemplo para vincular un rol `cluster-admin` a la cuenta de servicio.

```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
   =cluster-admin --serviceaccount=default:citrixadm-sa
<!--NeedCopy-->
```

   Tras vincular la cuenta Citrix ADM al rol `cluster-admin`, la cuenta de servicio tiene acceso a todo el clúster. Para obtener más información, consulte [`kubectl` create

`clusterrolebinding`] (https://kubernetes.io/docs/reference/access-authn-authz/rbac/#kubectl-create-clusterrolebinding).

3. Obtenga el token de la cuenta de servicio creada.

   Por ejemplo, ejecute el siguiente comando para ver el token de la cuenta de servicio `citrixadm-sa`:

   ```
   kubectl describe sa citrixadm-sa
   <!--NeedCopy-->
   ```

4. Ejecute el siguiente comando para obtener la cadena secreta del token:

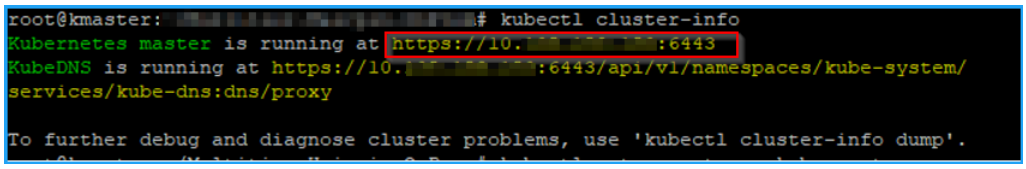
   ```
   kubectl describe secret <token-name>
   <!--NeedCopy-->
   ```

Agregar el clúster de Kubernetes en Citrix ADM

Después de configurar un agente Citrix ADM y configurar rutas estáticas, debe registrar el clúster de Kubernetes en Citrix ADM.

Para registrar el clúster de Kubernetes:

1. Inicie sesión en Citrix ADM con credenciales de administrador.
2. Vaya a **Orchestration** > **Kubernetes** > **Clúster**.
   Se muestra la página Clústeres.
3. Haga clic en **Agregar**.
4. En la página **Agregar clúster**, especifique los siguientes parámetros:
   a) **Nombre** : especifique un nombre de su elección.
   b) **URL del servidor 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 que se obtiene al configurar Citrix ADM para administrar un clúster de Kubernetes. El token de autenticación es necesario para validar el acceso a la comunicación entre el clúster de Kubernetes y Citrix ADM. Para generar un token de autenticación:

i. En el nodo principal de Kubernetes, ejecuta los siguientes comandos:

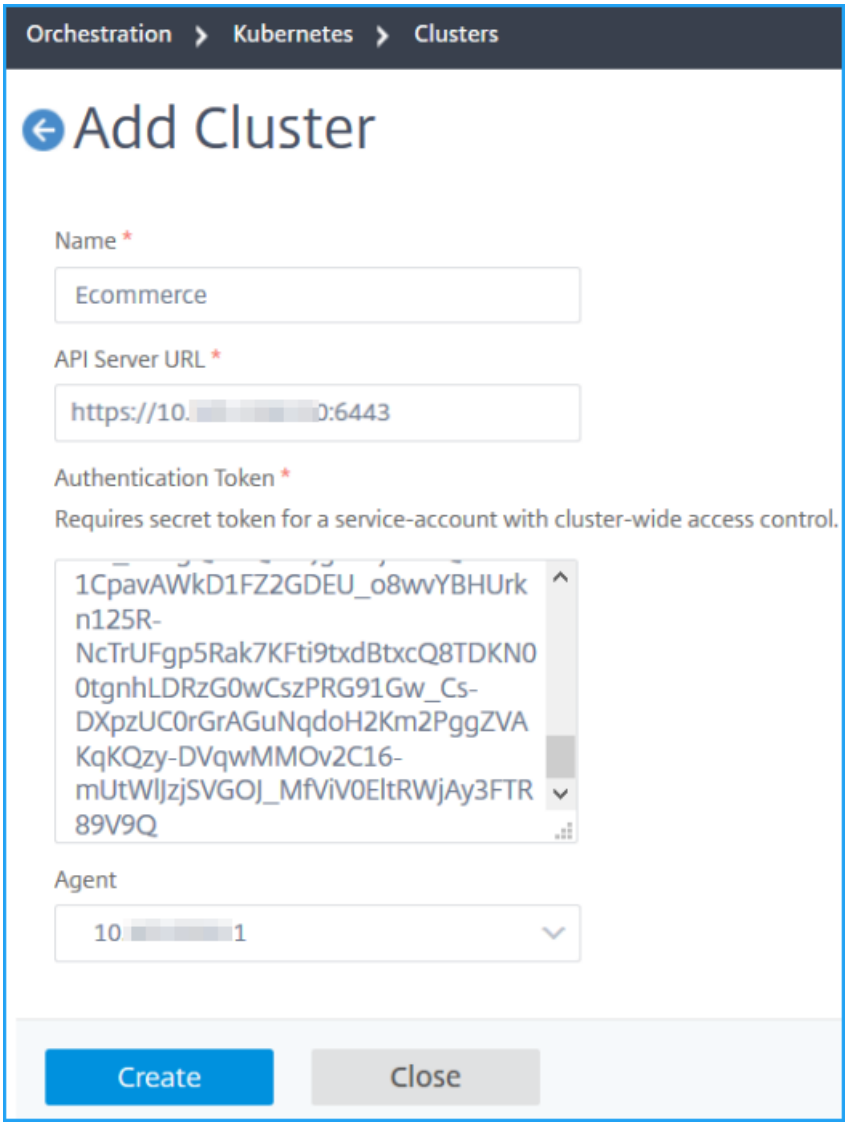
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. Copie el token que se genera y péguelo como token de autenticación

Para obtener más información, consulte la documentación de Kubernetes.

d) Seleccione el agente de la lista.

e) Haga clic en **Crear**.



Información TCP

November 16, 2022

La función TCP Insight de Citrix ADM proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias de control de la congestión (o algoritmos) utilizadas en los dispositivos Citrix ADC a fin de evitar la congestión de la red en la transmisión de datos. Esta función utiliza la función «Informe de velocidad de TCP», que mide el rendimiento de carga o descarga de archivos TCP con y sin optimización de TCP.

Puede ver las métricas clave de la capa de transporte, como el volumen de datos, el rendimiento y la velocidad, y utilizar esa información para medir el volumen de tráfico servido por las instancias de Citrix ADC y validar los beneficios de la optimización de TCP. Para las métricas anteriores, se proporcionan desgloses por dirección de transmisión (del cliente a Citrix ADC y de Citrix ADC al servidor de origen), puerto TCP y LAN virtual.

Requisitos previos

Antes de empezar a configurar la función TCP Insight, asegúrese de que se cumplen los siguientes requisitos previos:

- Las instancias de Citrix ADC se ejecutan en la versión 11.1 del software, compilación 51.21 o posterior.
- Ha instalado Citrix ADM en la versión 11.1 del software, compilación 51.21 o posterior.
- Todos los servidores virtuales configurados para una aplicación tienen licencia para administración y supervisión en Citrix ADM. Para obtener información sobre las licencias de Citrix ADM, consulte Licencias.

Requisitos de hardware para Citrix ADM:

Componente	Requisito
RAM	8 GB
CPU virtual	4
	Nota: Citrix recomienda utilizar 8 CPU para obtener un mejor rendimiento.
Espacio de almacenamiento	120 GB
	Nota: Citrix recomienda utilizar 500 GB para obtener un mejor rendimiento.

Habilitación de TCP Insight

Antes de poder ver las métricas de TCP Insight, debe habilitar la función en Citrix ADM.

Para habilitar TCP Insight:

1. Vaya a **Configuración > Configuración de Analytics**y haga clic en **Habilitar funciones para Analytics**.
2. En la página **Habilitar funciones para Analytics**, seleccione **Habilitar TCP Insight**.
3. En la ventana de confirmación, haga clic en **Aceptar**.

Vea las métricas de TCP Insight en Citrix ADM

Después de habilitar TCP Insight en Citrix ADM, puede ver información clave de la capa de transporte, como el modo de tráfico (datos de Internet o móviles), el volumen de datos, el rendimiento, las interfaces, los puertos, la velocidad media de carga y la velocidad media de descarga.

Para mostrar métricas de TCP Insight en Citrix ADM:

Vaya a **Infraestructura** > **TCP Insight**.

Puede colocar el puntero del ratón sobre los gráficos de barras para ver el volumen de datos de las técnicas de transporte correspondientes. También puede ver el volumen de datos y otras métricas en la tabla debajo del gráfico.

> **Nota** Puede personalizar las métricas que se muestran en el gráfico mediante el icono de configuración de la tabla. También puede seleccionar el período de tiempo al que pertenecen las métricas y utilizar el control deslizante de tiempo para ajustar el período de tiempo.

También puede ver las métricas de elementos como las interfaces, los puertos y las velocidades de bits seleccionándolos de la lista **TCP Insight** .

Casos de uso

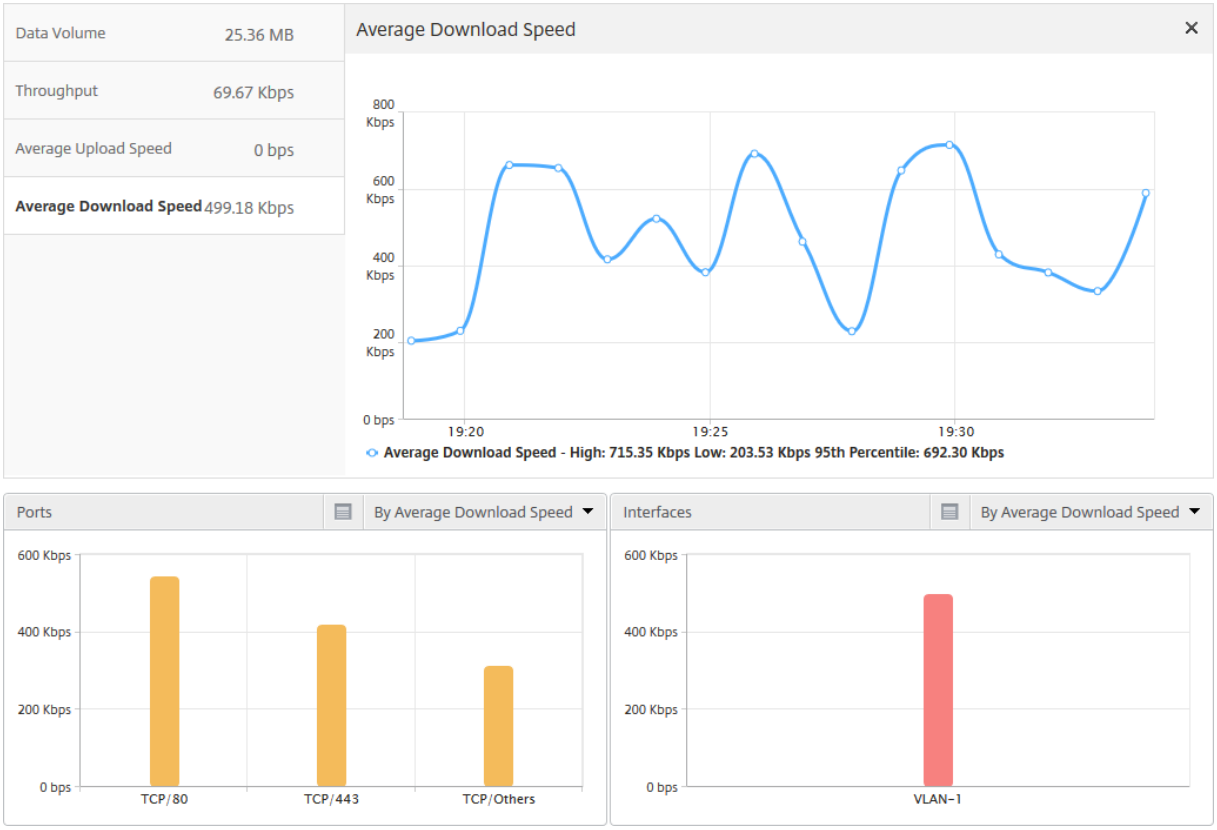
Los siguientes casos de uso ilustran algunas de las formas de usar TCP Insight en los dispositivos Citrix ADC:

- Evalúe los beneficios de la optimización
- Ajustar parámetros TCP
- Medir el impacto de la optimización TCP en el volumen de tráfico

Evalúe los beneficios de la optimización

¿En qué medida beneficia realmente la optimización TCP de Citrix ADC a una red móvil (radio) o empresarial (Internet)? Puede ver la velocidad de las transferencias de datos que se realizan a través de TCP y comparar el rendimiento optimizado y no optimizado. Estas mediciones se muestran por separado para las instrucciones de descarga y carga (siempre en el lado de la radio/cliente), y para diferentes puertos de destino, HTTP (80) y HTTPS (443).
Al examinar las métricas de TCP Insight, puede cuantificar la mejora de velocidad obtenida al optimizar los flujos de TCP.

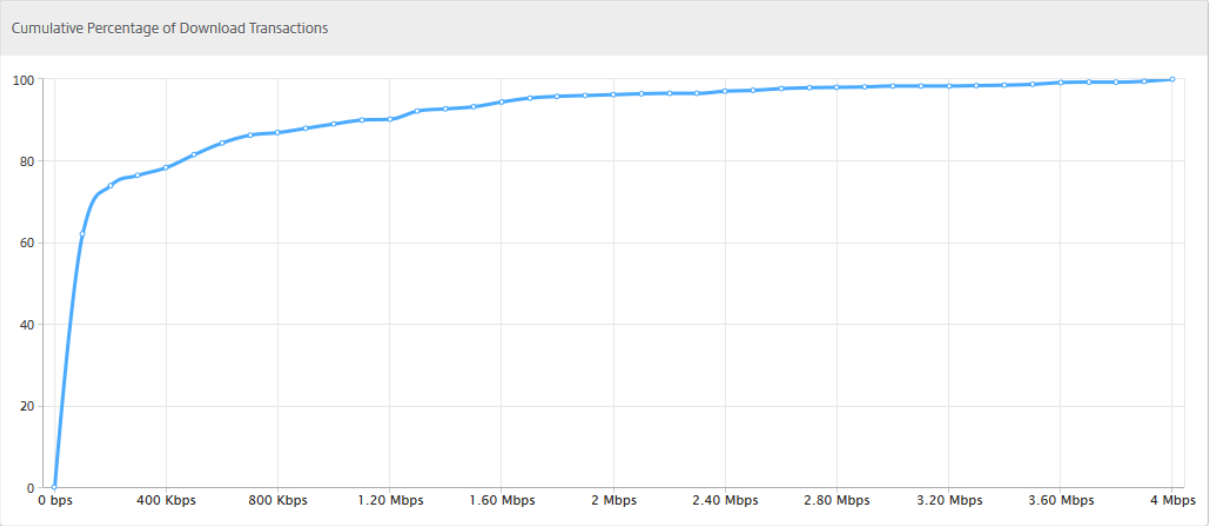
Para ver un resumen de estos parámetros, inicie sesión en Citrix ADM y haga clic en la ficha **TCP Insight**. A continuación, haga clic en **Lados** y seleccione **Internet** o **Radio** en el gráfico de barras o en la tabla debajo del gráfico.



Ajustar parámetros TCP

El uso de diferentes perfiles TCP puede generar diferentes salidas para el mismo tráfico. En tales situaciones, es posible que quiera ver y comparar las mediciones de velocidad de los períodos en los que Citrix ADC ejecuta diferentes perfiles de optimización de TCP. Puede utilizar los resultados para ajustar los parámetros de TCP para una transmisión más rápida y desarrollar un perfil TCP que maximice la experiencia percibida por el usuario en una red de cliente específica.

Para ver los informes, inicie sesión en Citrix ADM. A continuación, en la ficha **TCP Insight**, haga clic en **Bitrates**y seleccione la velocidad de bits deseada en el gráfico de barras o en la tabla situada debajo del gráfico.

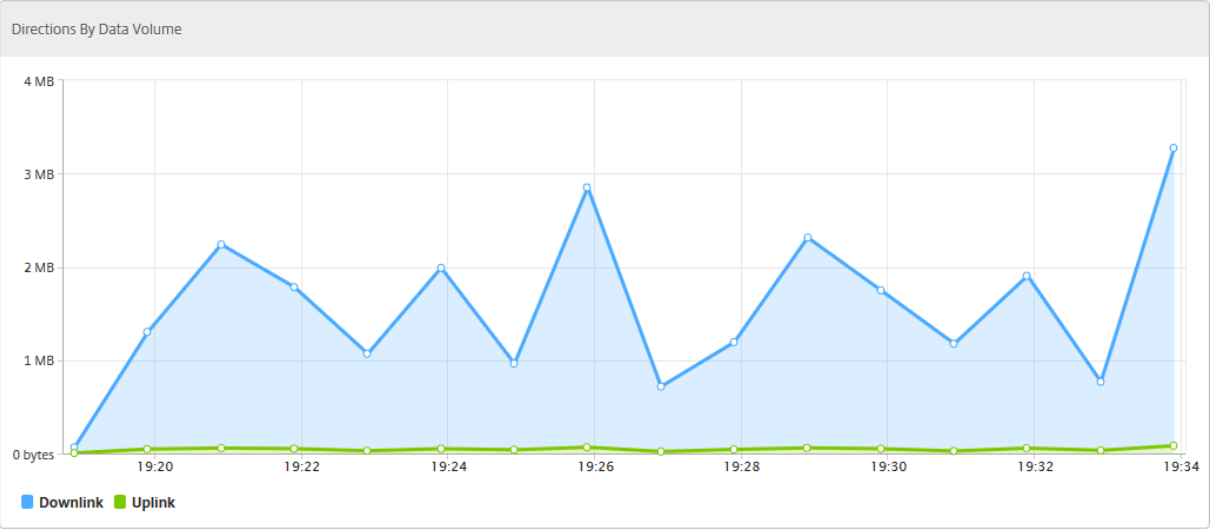


Medir el impacto de la optimización TCP en el volumen de tráfico

Las mediciones del volumen/rendimiento de datos de la capa IP gestionadas por una instancia de Citrix ADC se pueden comparar entre diferentes períodos de tiempo para evaluar el efecto de la optimización de TCP en el consumo de datos de los suscriptores. Las mediciones se pueden aplicar por separado para cada lado de la red (lado de la radio frente al lado de Internet), para diferentes segmentos de tráfico (delineados por diferentes interfaces o VLAN), para cada dirección (enlace descendente o enlace ascendente) y para diferentes puertos de destino (HTTP y HTTPS). La comparación se puede utilizar para confirmar que la optimización de TCP alienta a los suscriptores a consumir más datos.

Para obtener un resumen de las mediciones, inicie sesión en Citrix ADM y, en la ficha **TCP Insight**, haga clic en **Lados**y, a continuación, seleccione **Internet** o **Radio** en el gráfico de barras o en la tabla situada debajo del gráfico.

También puede seleccionar un período de tiempo diferente de la lista de tiempos. Puede personalizar el marco de tiempo mediante el control deslizante de marco de tiempo.



Video Insight

November 16, 2022

La función Video Insight proporciona una solución fácil y escalable para monitorear las métricas de las técnicas de optimización de vídeo utilizadas por los dispositivos Citrix ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa, y ofrece beneficios como:

- Administre la red durante la congestión en las horas pico.
- Mejore la coherencia de la reproducción de vídeo y reduzca el bloqueo de vídeo
- Habilite nuevas ofertas de servicios de video (por ejemplo, los servicios de video Binge-on).
- Permita que los clientes seleccionen la mejor calidad de vídeo sostenible.
- Ofrezca una experiencia de usuario coherente para el suscriptor.

Mientras optimiza el tráfico de vídeo, el dispositivo Citrix ADC utiliza un mecanismo especial para acelerar dinámicamente la velocidad de bits de vídeo y una técnica de muestreo aleatorio para estimar los ahorros derivados de la técnica de optimización. Para obtener más información sobre la función de optimización de vídeo de Citrix ADC, consulte Optimización de vídeo. Al integrar el dispositivo Citrix ADC con Citrix ADM, este recopila información clave de los datos de vídeo que fluyen a través del dispositivo Citrix ADC. Puede utilizar esta información para comparar el rendimiento optimizado y no optimizado del tráfico de vídeo ABR, determinar el ahorro debido a la optimización, etc.

> **Nota**
>
> Las estadísticas de las sesiones no optimizadas proporcionadas en Citrix ADM corresponden a las sesiones seleccionadas de muestreo aleatorio en Citrix ADC Appliance. Para obtener más

> información sobre el muestreo aleatorio, consulte Optimización de vídeo.

Video Insight en Citrix ADM proporciona métricas para los siguientes tipos de tráfico de vídeo:

- Descarga progresiva (PD) de vídeos a través de HTTP
- Vídeos de ABR a través de HTTP
- Vídeos de ABR a través de HTTPS
- Vídeos ABR de YouTube a través de QUIC

Configuración de Video Insight

> **Nota**
>
> Video Insight es compatible con las instancias de Citrix ADC con licencia Citrix ADC Premium. La licencia Citrix ADC Premium es compatible con las plataformas Citrix ADC Telco (VPX T1000 y VPX-T).

Para configurar Video Insight en una instancia de Citrix ADC, primero habilite la función AppFlow, configure un recopilador, una acción y una directiva de AppFlow y enlace la directiva de forma global. Al configurar el recopilador, debe especificar la dirección IP del servidor Citrix ADM en el que quiere supervisar los informes.

Para configurar la información de vídeo en una instancia de Citrix ADC, ejecute los siguientes comandos para configurar un perfil y una directiva de AppFlow y enlazar la directiva de AppFlow globalmente.

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

set appflow param -videoInsight ENABLED

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode ulfd

enable feature AppFlow

Muestra

```
1 add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
     Transport logstream
2 set appflow param -videoInsight ENABLED
3 add appflow action act1 -collectors col1 -videoAnalytics ENABLED
4 add appflow policy appol true act1
```

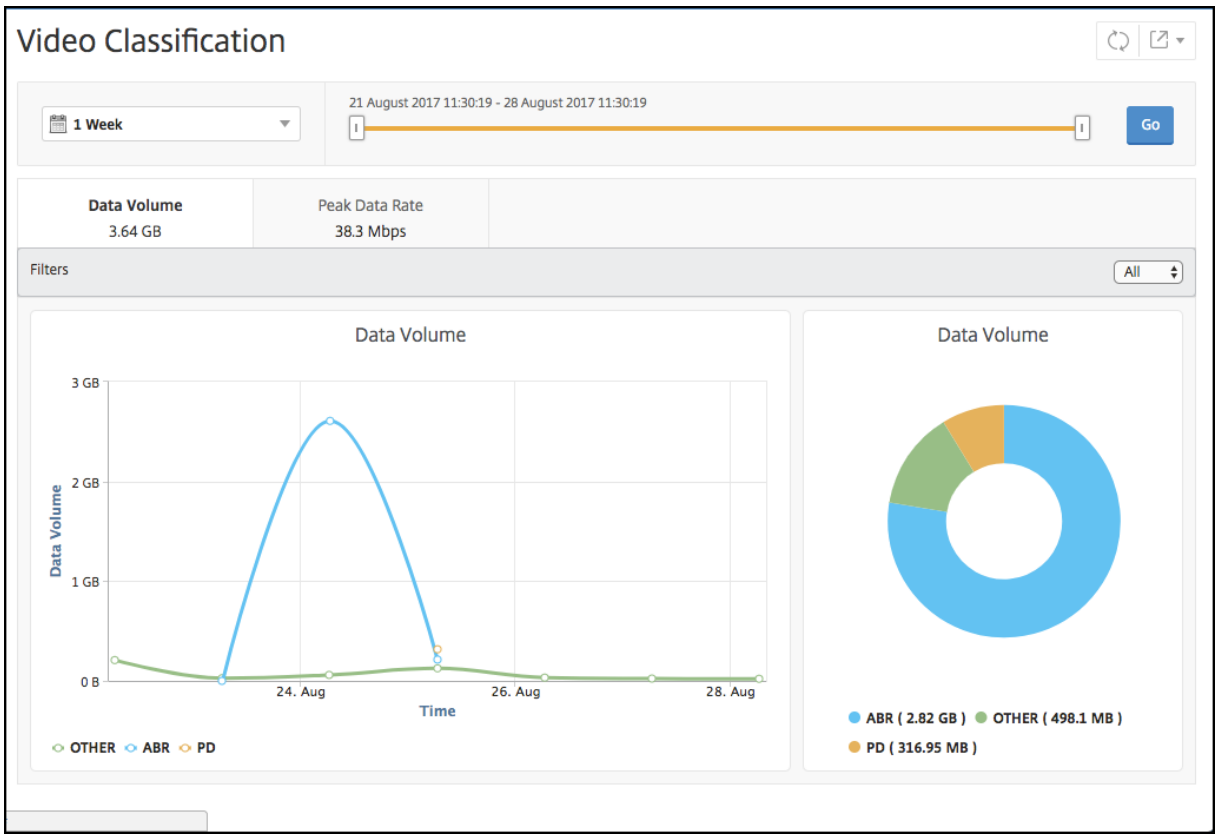


```
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

Visualización de las métricas de Video Insight en Citrix ADM

Después de habilitar Video Insight en Citrix ADM, puede ver métricas de optimización de vídeo, como clasificación de vídeo, volumen de datos, velocidad máxima de datos y reproducciones de vídeo ABR. Estas métricas le ayudan a analizar su red y optimizar los vídeos para mejorar la experiencia del suscriptor, la eficiencia operativa y otros criterios de rendimiento.

Para ver las métricas de Video Insight en Citrix ADM, vaya a **Infraestructura > Video Insight**.



Nota

Los valores proporcionados por la leyenda **OTHER** en los gráficos representan los datos que no son ABR ni PD en el tráfico de vídeo, según el filtro que haya seleccionado:

- **All**: Suma de datos no ABR (HTTP, HTTPS y QUIC) y no PD (HTTP) en el tráfico de vídeo.
- **HTTP** : suma de los datos que no son ABR y que no son PD en el tráfico de vídeo.
- **HTTPS** : suma de los datos de vídeo que no son ABR en el tráfico de vídeo.

- **QUIC** : suma de los datos de vídeo que no son ABR en el tráfico de vídeo.

Ver la eficiencia de la red

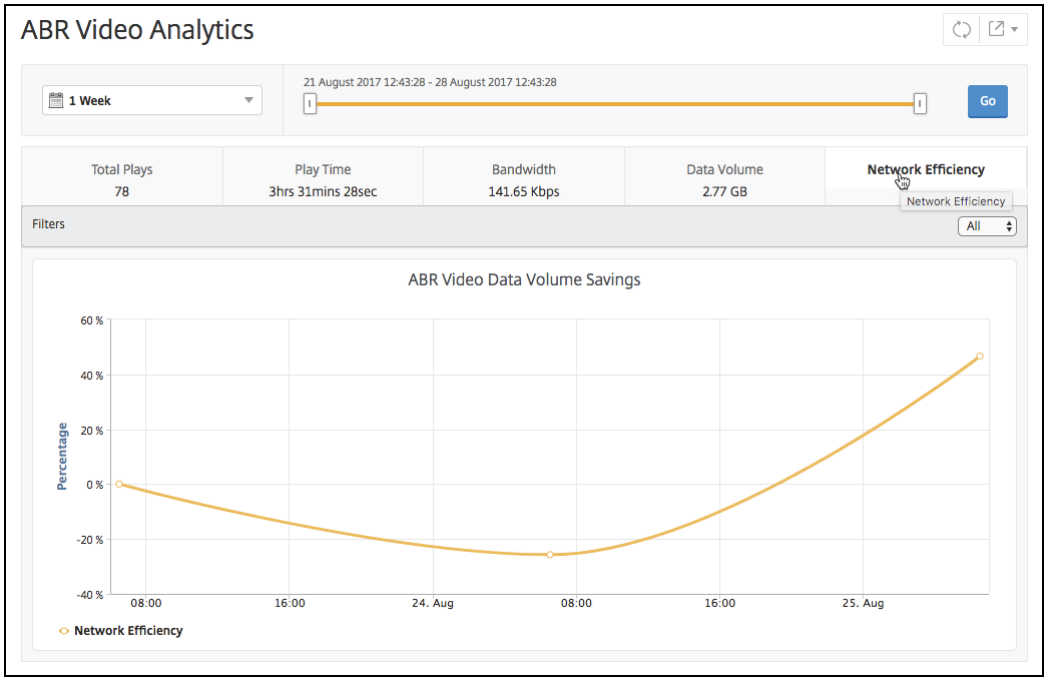
November 16, 2022

Para un período de tiempo determinado, Citrix ADM proporciona un gráfico que muestra la proporción de sesiones de vídeo optimizadas y no optimizadas en el período de tiempo. También muestra el porcentaje de ancho de banda ahorrado por la optimización. El porcentaje de ancho de banda ahorrado se calcula con la siguiente fórmula:

Porcentaje de ancho de banda ahorrado = Volumen de **datos de vídeo ABR optimizado promedio/Volumen de datos de vídeo ABR no optimizado**.

Para ver el porcentaje de ancho de banda ahorrado por la optimización:

1. Vaya a **Infraestructura > Video Insight**y haga clic en **ABR Video**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Eficiencia de la red** .



Compare el volumen de datos utilizado por los videos ABR optimizados y no optimizados

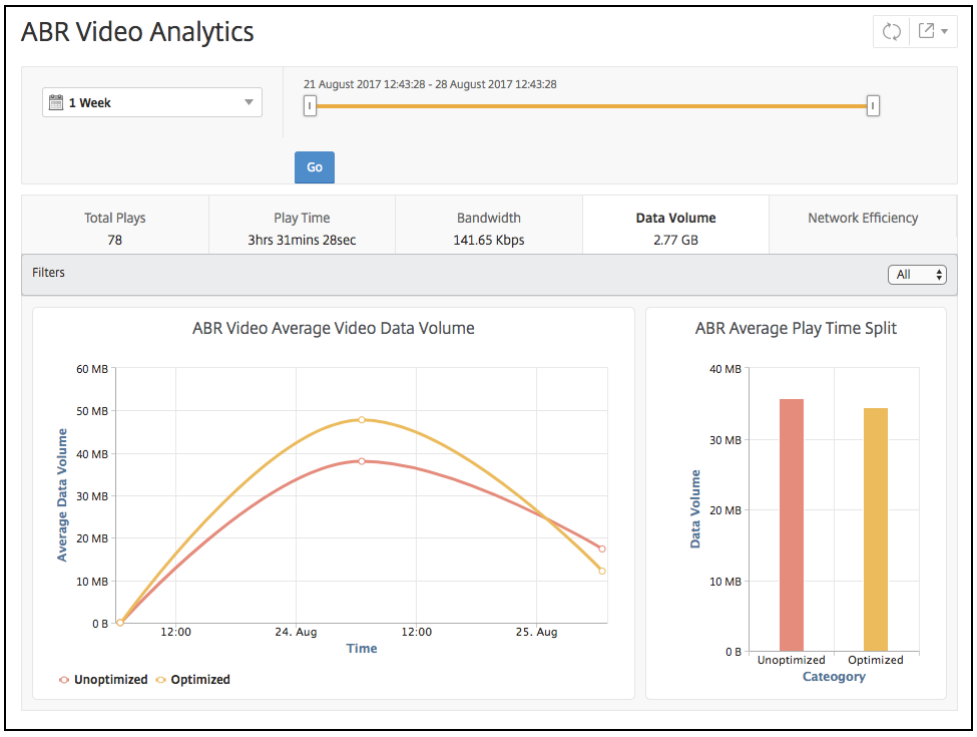
November 16, 2022

Durante un período de tiempo determinado, Citrix ADM muestra el volumen de datos que utilizan los vídeos ABR optimizados y no optimizados, de modo que pueda comparar los dos volúmenes.

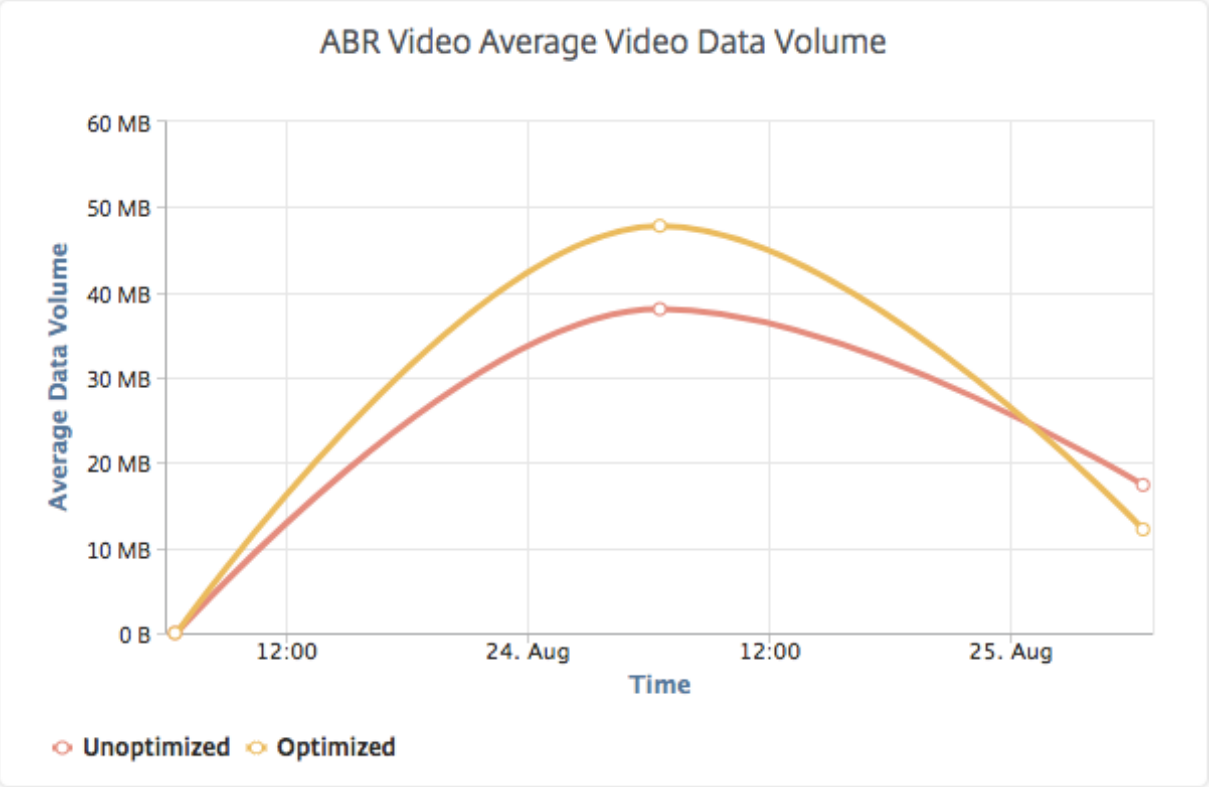
Para ver el volumen de datos que utilizan los vídeos de ABR:

1. Vaya a **Infraestructura > Video Insight**y haga clic en **ABR Video**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Volumen de datos**.

Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.



La ficha **Volumen de datos** proporciona un gráfico de líneas y un gráfico circular que describe el volumen de datos promedio utilizado por los vídeos ABR y el volumen de datos consumido por los vídeos ABR optimizados y no optimizados de la red para el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver el volumen de datos promedio utilizado durante un período de tiempo determinado:



Ver el tipo de vídeos transmitidos y el volumen de datos consumido de la red

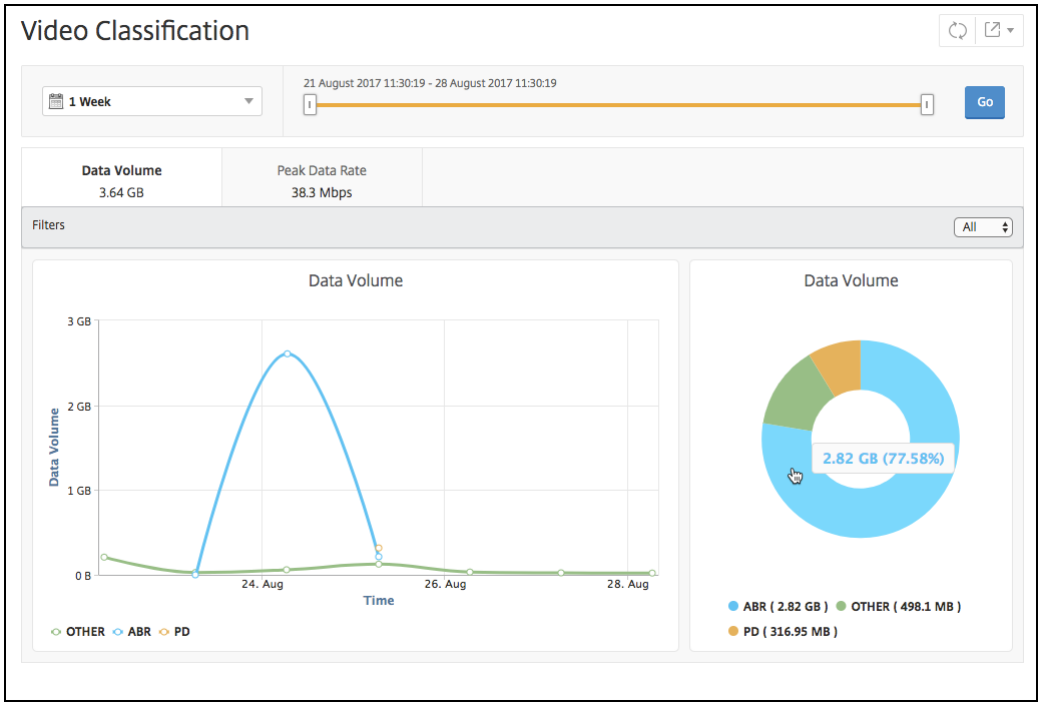
November 16, 2022

El dispositivo Citrix ADC detecta el tráfico de vídeo cifrado o no cifrado de la red y el tipo de transmisión de vídeo (PD o ABR). Citrix ADM muestra estas métricas y el volumen de datos consumido por el tráfico de vídeo durante un período de tiempo definido.

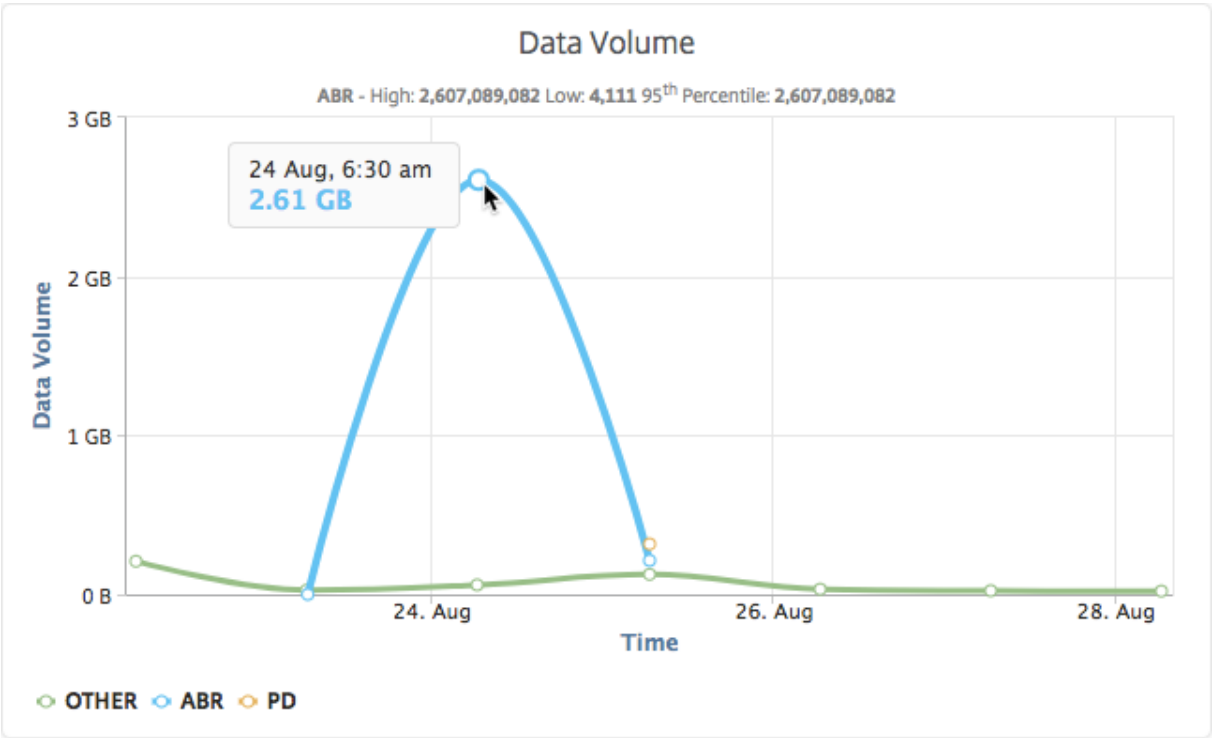
Para ver los tipos de vídeos y el volumen de datos consumido:

1. Vaya a **Infraestructura > Video Insight** y haga clic en **Clasificación de vídeos**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir**.

Puede utilizar la lista **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.

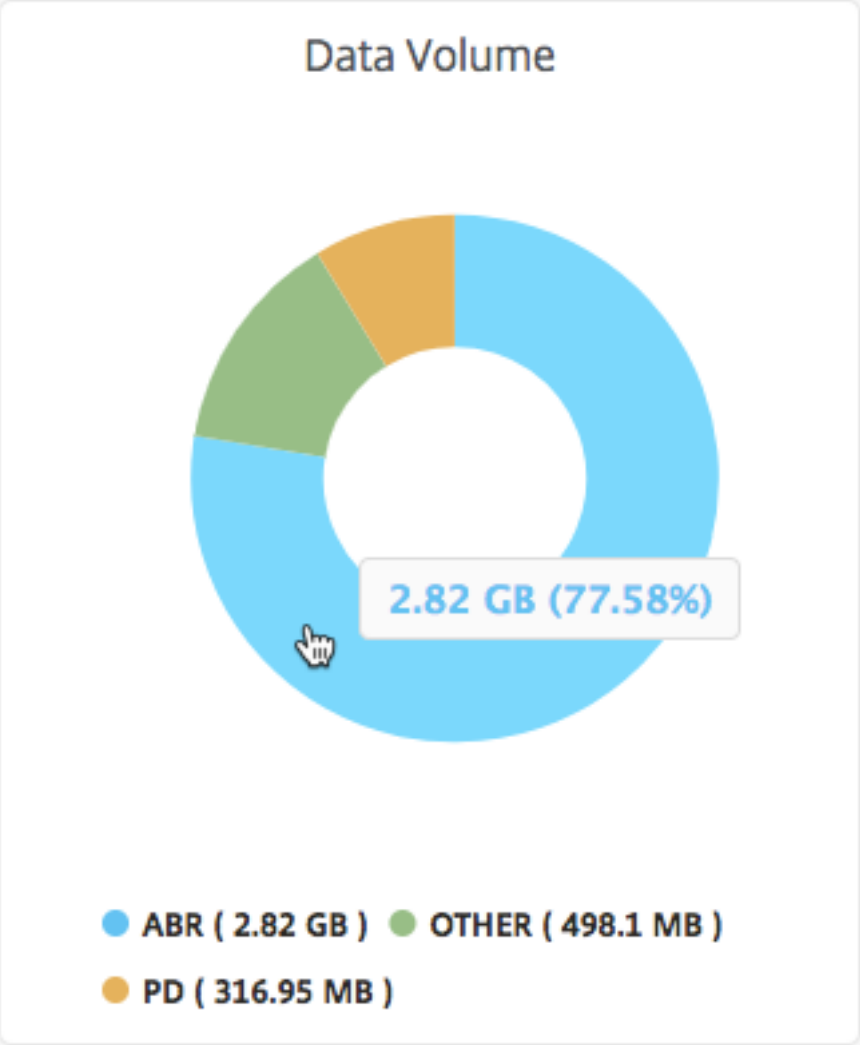


La ficha **Volumen de datos** proporciona un gráfico de líneas y un gráfico circular que muestra los tipos de transmisión de tráfico de vídeo desde la red y el volumen de datos consumido por la red. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver los datos consumidos durante un período de tiempo determinado:



Además, puede colocar el puntero del mouse sobre el gráfico circular para ver el porcentaje de volu-

men de datos consumido por un tipo determinado de tráfico de vídeo.



Compare el tiempo de reproducción optimizado y no optimizado de los vídeos ABR

November 16, 2022

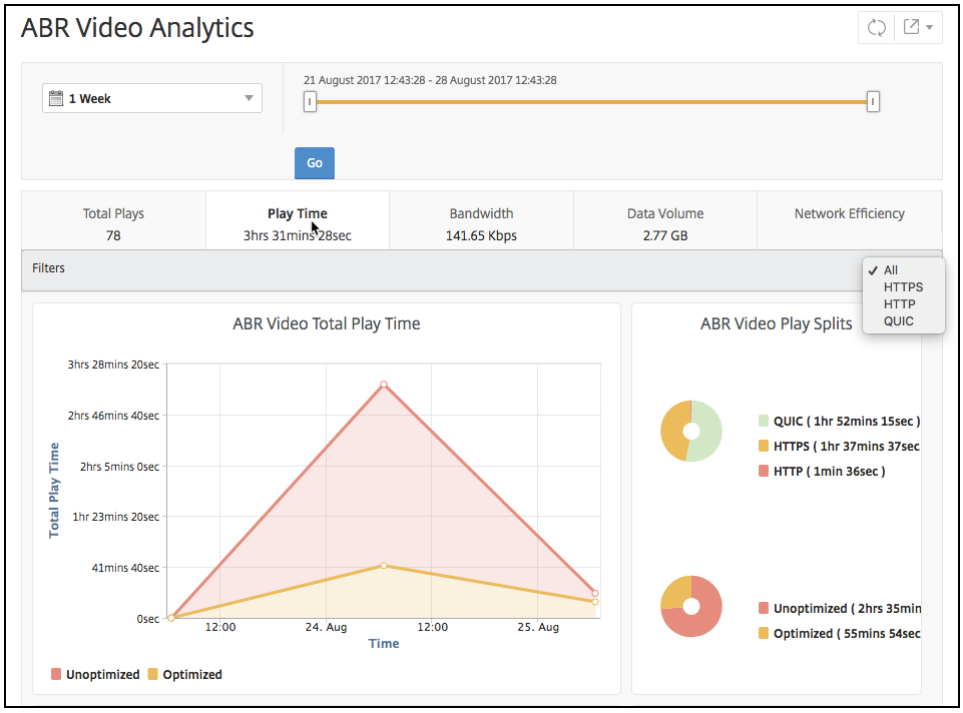
Durante un período de tiempo determinado, Citrix ADM proporciona el tiempo de reproducción de los vídeos ABR y también le permite comparar el tiempo de reproducción de los vídeos ABR optimizados y no optimizados de su red.

Para ver el tiempo de juego:

1. Vaya a **Infraestructura > Video Insight** y haga clic en **ABR Video**.

2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Tiempo de reproducción**.

   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.



Para el marco de tiempo seleccionado, la ficha **Tiempo de reproducción** proporciona un gráfico de líneas y un gráfico circular que describe:

- Tiempo total de reproducción de los vídeos ABR de su red
- Tiempo total de reproducción de las reproducciones optimizadas y no optimizadas de vídeos ABR de su red durante el período de tiempo seleccionado
- Tiempo total de reproducción de vídeos ABR cifrados y no cifrados
- Tiempo medio de reproducción de los vídeos ABR
- Tiempo de reproducción promedio de reproducciones optimizadas y no optimizadas de vídeos ABR
- Tiempo medio de reproducción de vídeos ABR cifrados y no cifrados
- Distribución del tiempo de reproducción entre vídeos ABR optimizados y no optimizados

Compare el consumo de ancho de banda de vídeos ABR optimizados y no optimizados

November 16, 2022

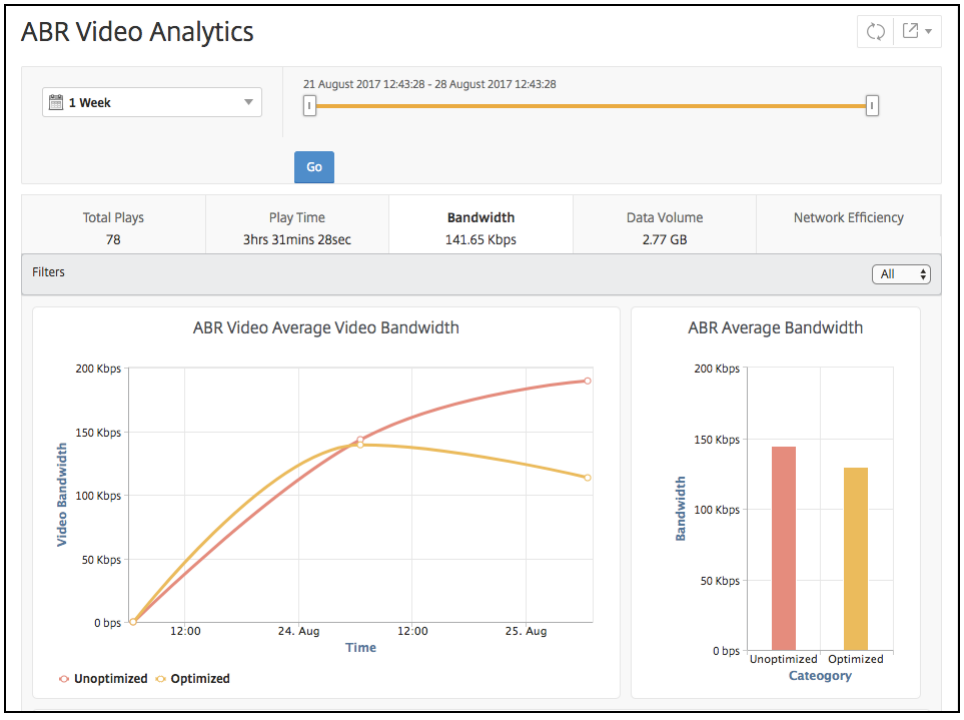
Durante un período de tiempo determinado, Citrix ADM proporciona el ancho de banda que consumen los vídeos ABR optimizados y no optimizados y también le permite comparar el ancho de banda consumido por los vídeos ABR optimizados y no optimizados en su red en función de:

- Tiempo de reproducción
- Volumen de datos

Para ver el consumo de ancho de banda:

1. Vaya a **Infraestructura > Video Insight** y haga clic en **ABR Video Analytics**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Ancho de banda**.

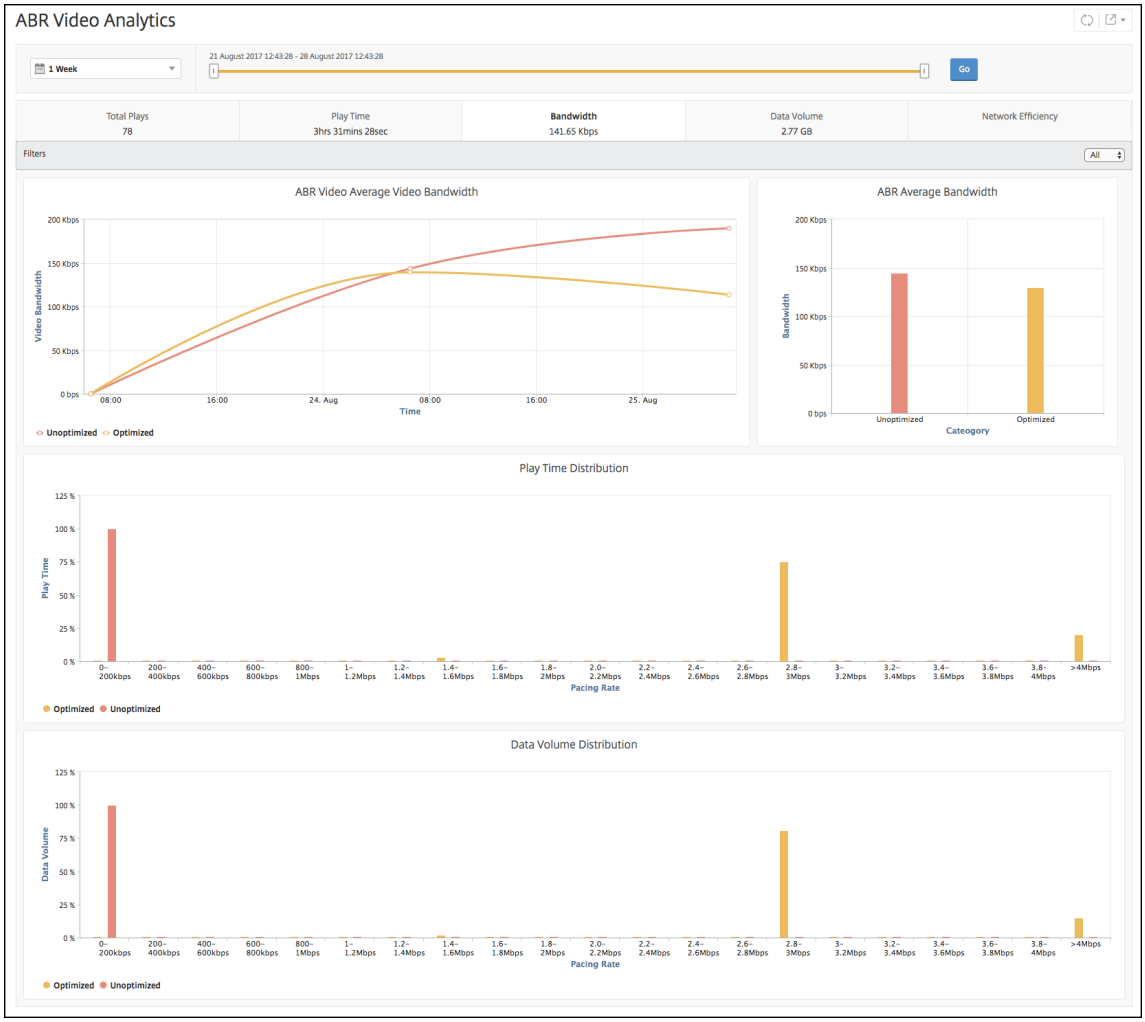
   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.



Para el período de tiempo seleccionado, la ficha **Ancho de banda** proporciona un gráfico de líneas y un gráfico circular que describe:

- Ancho de banda promedio consumido por los vídeos ABR optimizados y no optimizados.

- El ancho de banda consumido depende de la distribución del tiempo de reproducción entre vídeos ABR optimizados y no optimizados.
- Ancho de banda consumido en función del volumen de datos distribuido entre los vídeos ABR optimizados y no optimizados.



Compare el número optimizado y no optimizado de reproducciones de videos ABR

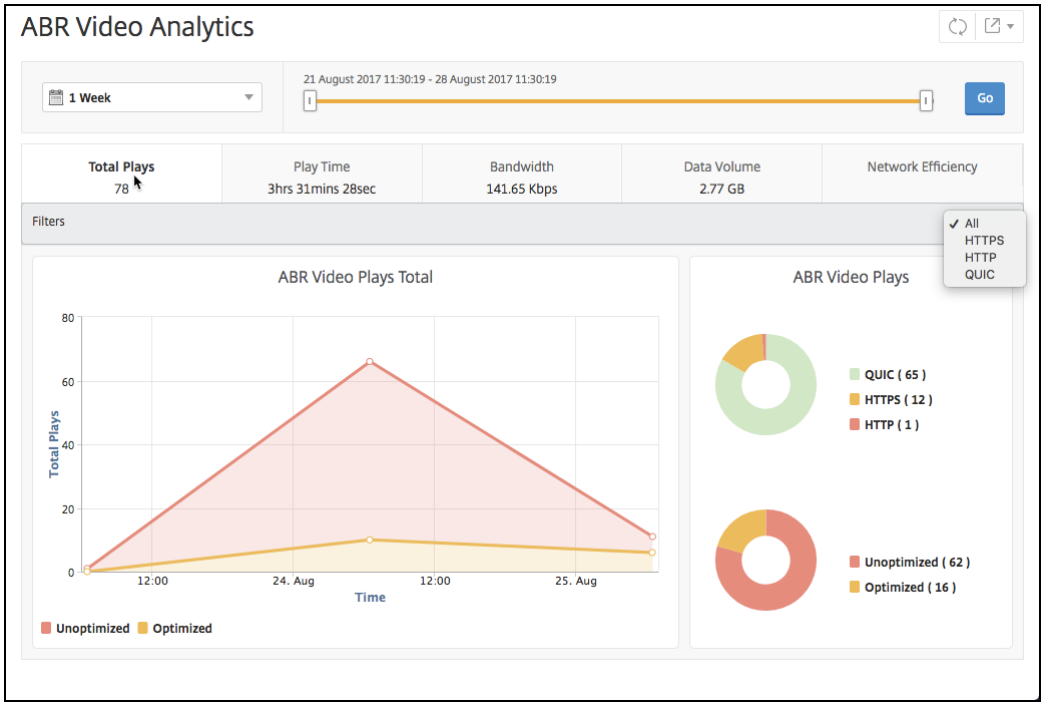
November 16, 2022

Durante un período de tiempo determinado, Citrix ADM muestra el número de reproducciones de vídeos ABR y le permite comparar el número de reproducciones optimizadas y no optimizadas en su red.

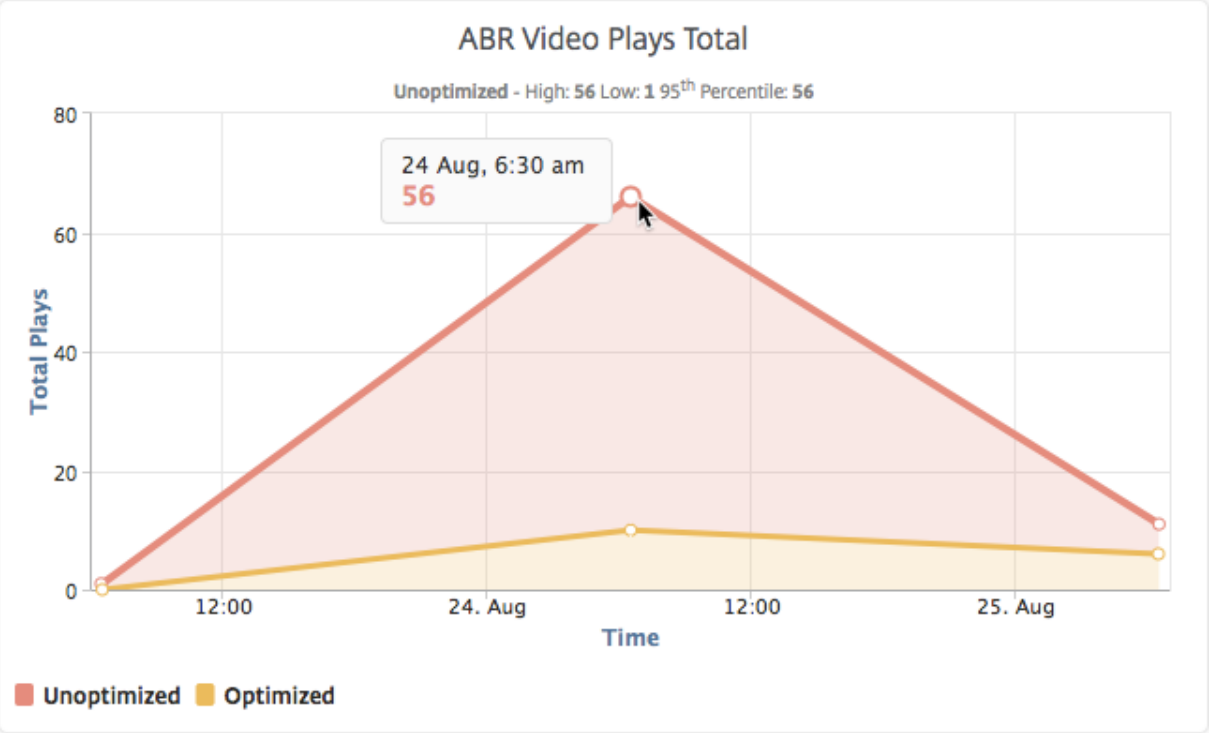
Para ver el número de jugadas:

1. Vaya a **Infraestructura > Video Insight**y haga clic en **ABR Video Analytics**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **N.º de reproducciones**.

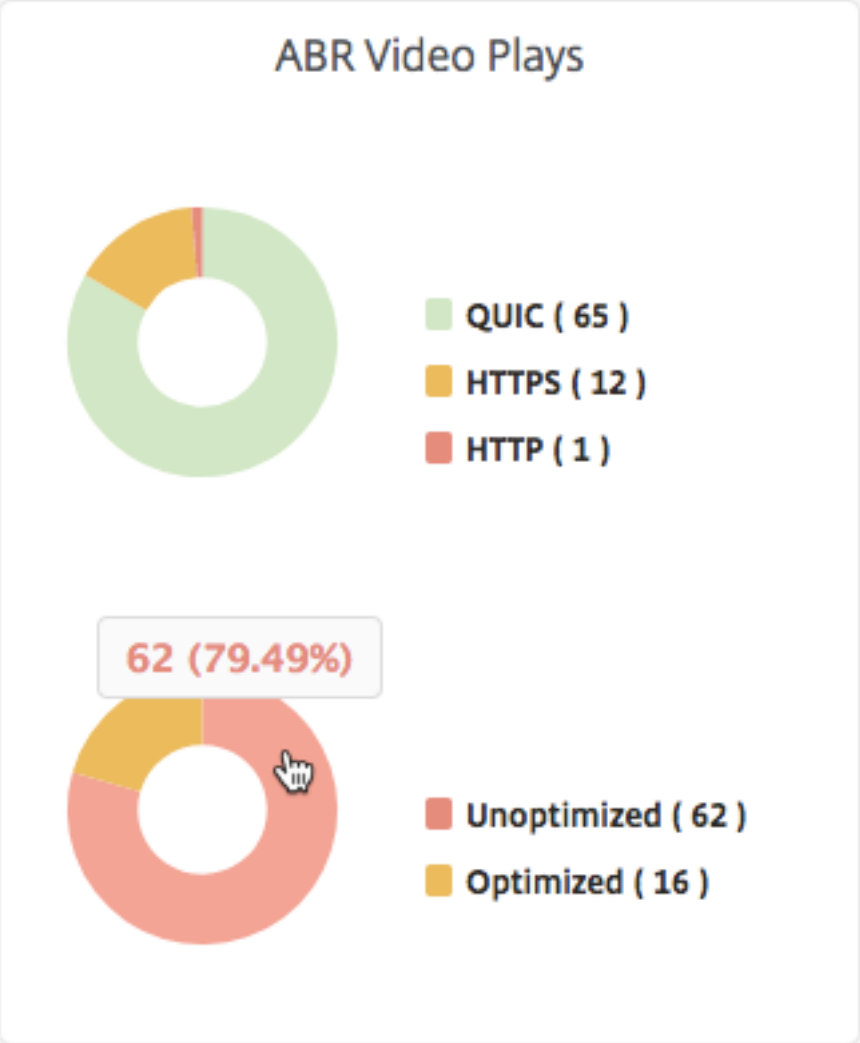
   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.



La ficha **N.º de reproducciones** proporciona un gráfico de líneas y un gráfico circular que describe el número de reproducciones de vídeos ABR de la red y el número de reproducciones optimizadas y no optimizadas de vídeos ABR de la red para el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver el número de reproducciones durante un período de tiempo determinado:



Además, puede colocar el puntero del mouse sobre el gráfico circular para mostrar el porcentaje de reproducciones optimizadas y no optimizadas y el porcentaje de vídeos ABR cifrados y no cifrados para el período de tiempo seleccionado.



Ver la velocidad máxima de datos para un período de tiempo específico

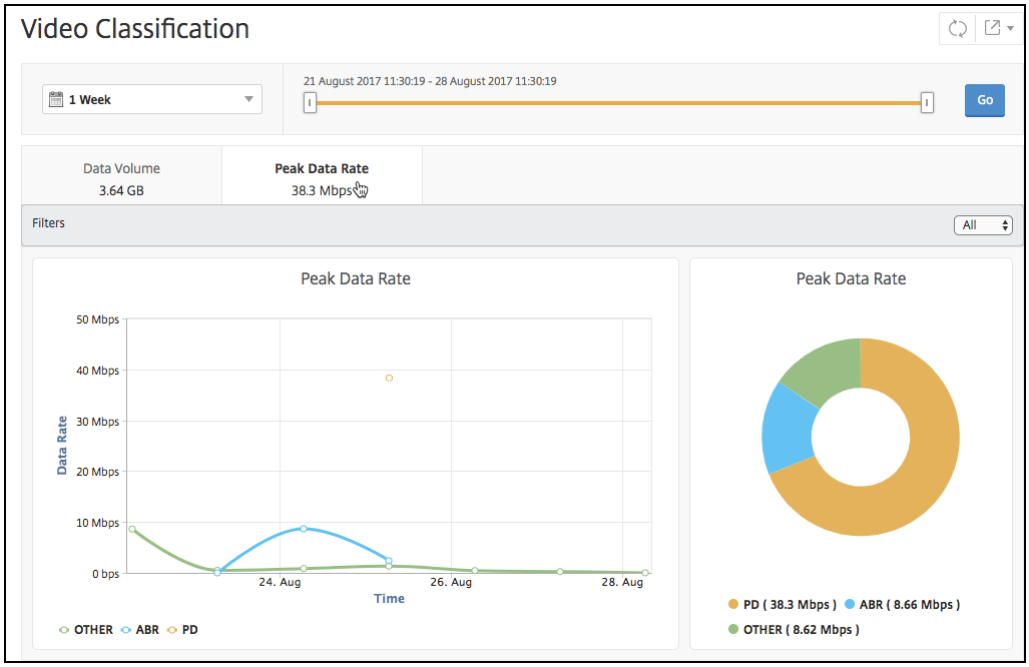
November 16, 2022

Citrix ADM le muestra el rendimiento máximo o la velocidad de datos del tráfico de vídeo de la red.

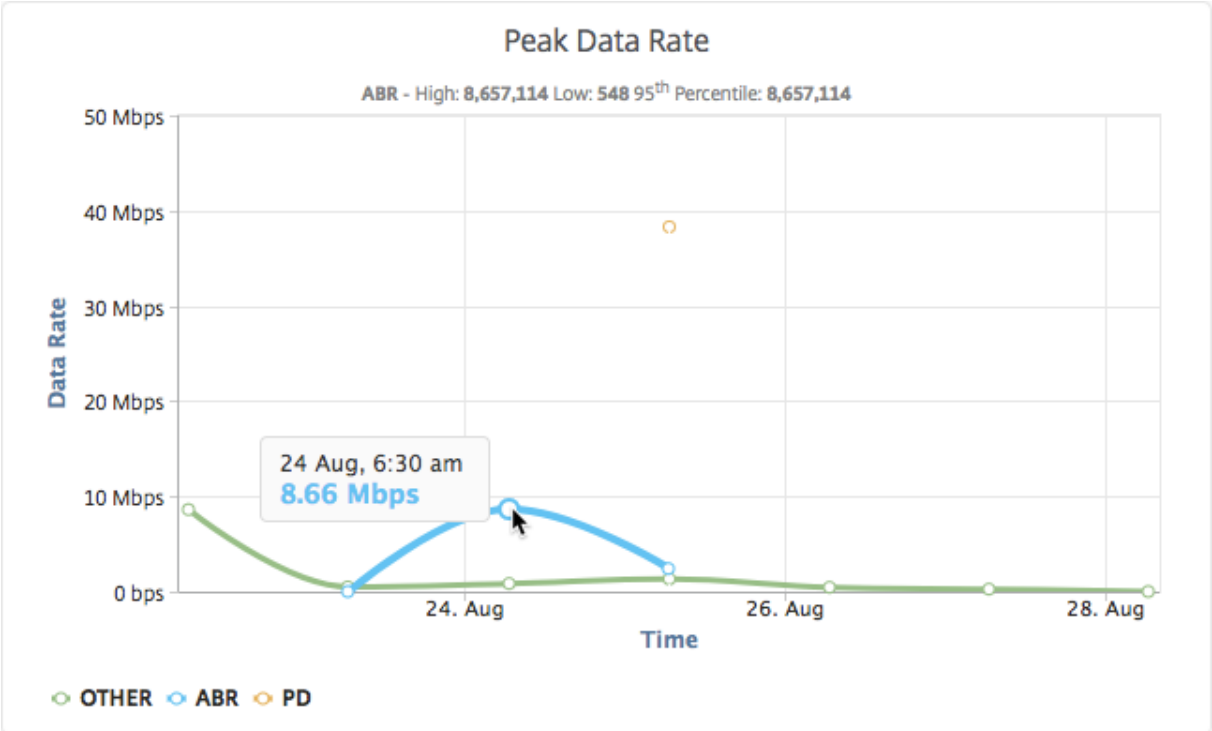
Para ver la velocidad máxima de datos del tráfico de vídeo:

1. Vaya a **Infraestructura > Video Insight**y haga clic en **Clasificación de vídeos**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Tasa de datos máxima**.

Puede utilizar la lista **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.

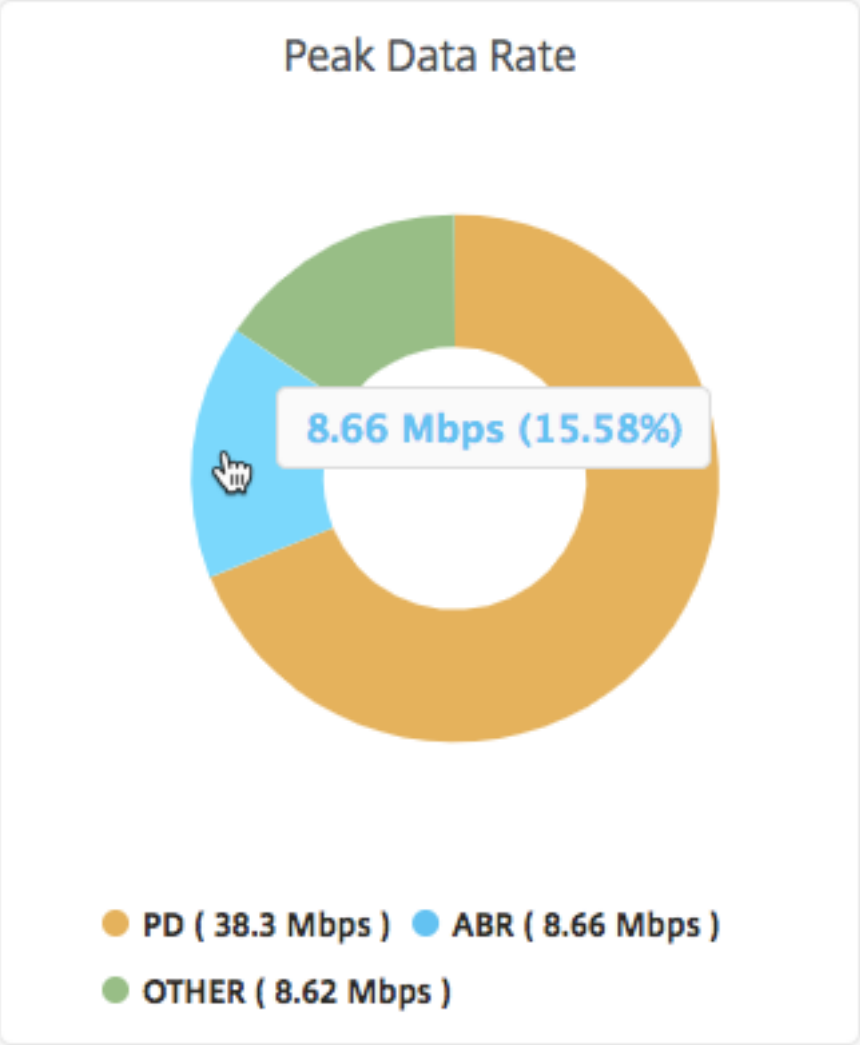


La ficha **Velocidad máxima de datos** proporciona un gráfico de líneas y un gráfico circular que describe la velocidad máxima de datos del tipo de transmisión de tráfico de vídeo desde la red y la velocidad máxima de datos del tráfico de vídeo en la red durante el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para mostrar la velocidad máxima de datos durante un período de tiempo determinado.



Además, puede colocar el puntero del mouse sobre el gráfico circular para mostrar el porcentaje de la

velocidad máxima de datos consumida por el tipo de tráfico de vídeo transmitido durante el período de tiempo seleccionado.



Administrar licencias y habilitar análisis en servidores virtuales

November 16, 2022

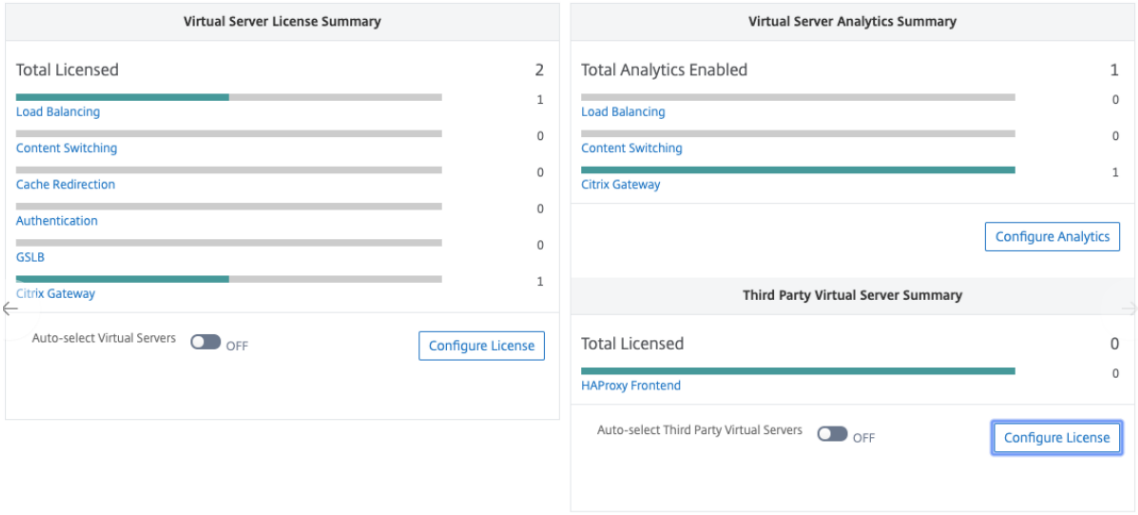
> Nota
>
> De forma predeterminada, la opción **Servidores virtuales con licencia automática** está habilitada. Debe asegurarse de tener licencias suficientes para licenciar los servidores virtuales. Si tiene licencias limitadas y quiere licenciar solo los servidores virtuales selectivos según sus requisitos, inhabilite la opción **Servidores virtuales con licencia automática**. Vaya a **Configuración > Configuración de licencias y análisis** y desactive la opción **Servidores virtuales con licencia**

> **automática en Asignación de licencias de servidoresvirtuales**.

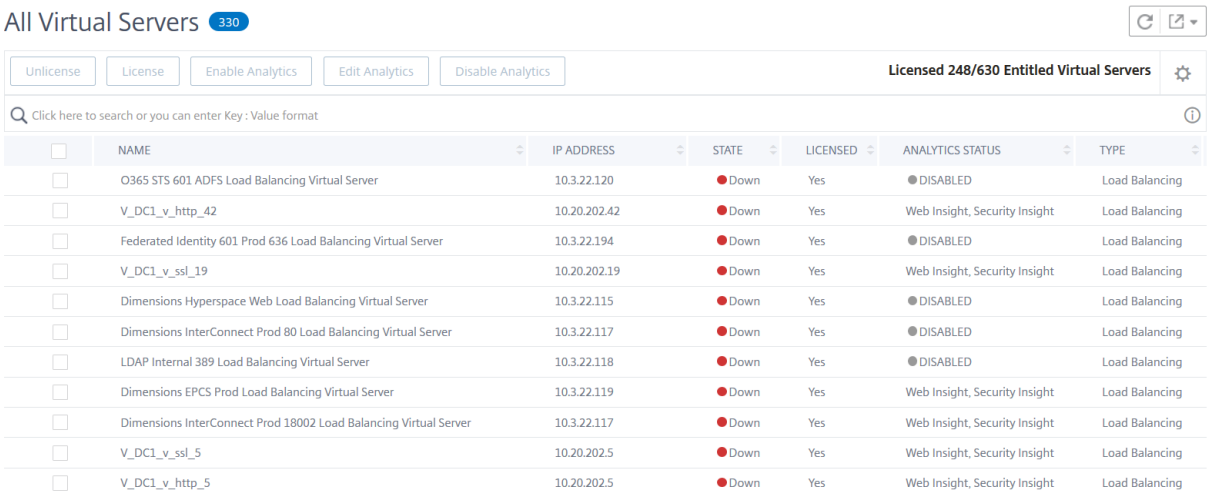
El proceso de habilitación de análisis se simplifica. Ahora puede licenciar el servidor virtual y habilitar el análisis en un único flujo de trabajo.

Vaya a **Configuración > Configuración de licencias y análisis** para:

- Ver el **resumen de licencia del servidor virtual**
- Ver el **resumen de análisis del servidor virtual**



Al hacer clic en **Configurar licencia** o **Configurar análisis**, aparece la página **Todos los servidores virtuales** .



En la página **Todos los servidores virtuales**, puede:

- Solicitar licencia para servidores virtuales sin licencia
- Eliminar la licencia de los servidores virtuales con licencia
- Habilite el análisis en servidores virtuales con licencia

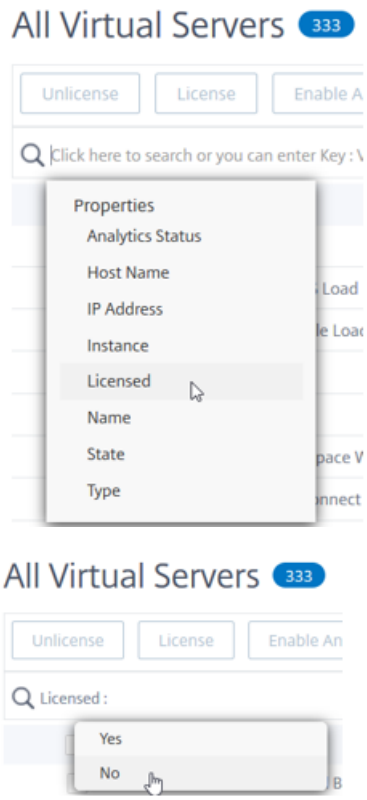
- Modificar análisis
- Desactivar la analítica

> **Nota**
>
> Los servidores virtuales compatibles que permiten el análisis son el equilibrio de carga, la conmutación de contenido y Citrix Gateway.

Administrar licencias en servidores virtuales

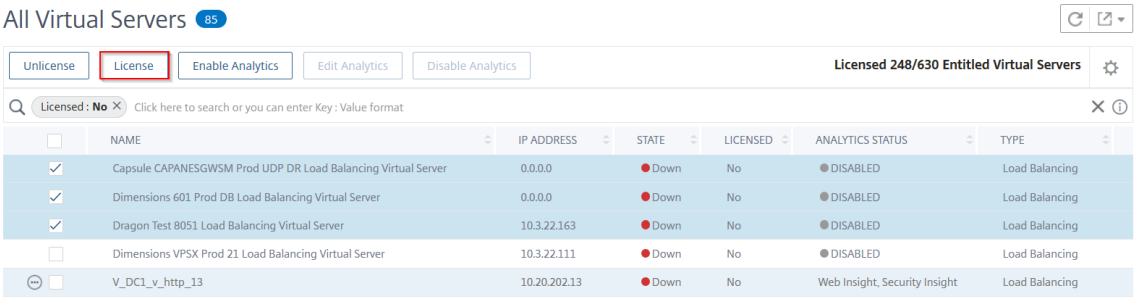
Para licenciar los servidores virtuales, desde la página **Todos los servidores virtuales** :

1. Haga clic en la barra de búsqueda, seleccione **Con licencia** y seleccione **No**.



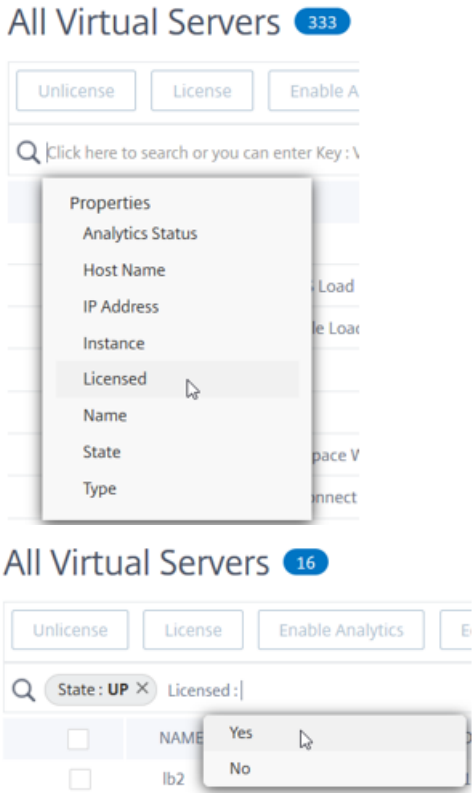
   Ahora se aplica el filtro y solo se muestran los servidores virtuales sin licencia.

2. Seleccione los servidores virtuales y, a continuación, haga clic en **Licencia**.

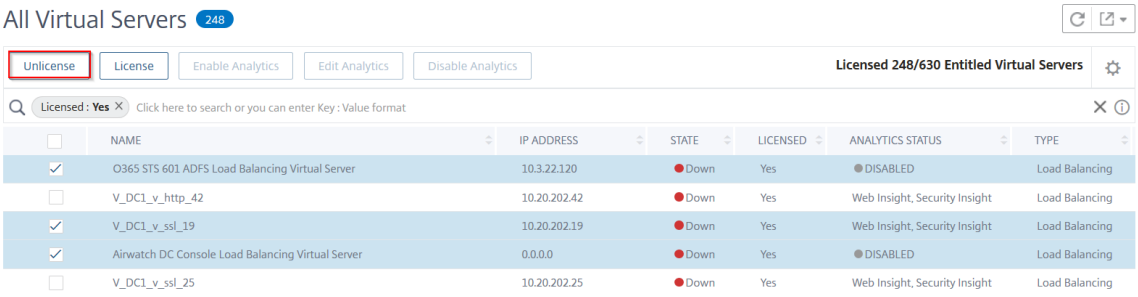


Para anular la licencia de los servidores virtuales, desde la página **Todos los servidores virtuales** :

1. Haga clic en la barra de búsqueda, seleccione **Licencia** y seleccione **Sí**.



2. Seleccione los servidores virtuales y haga clic en **Anular licencia**.



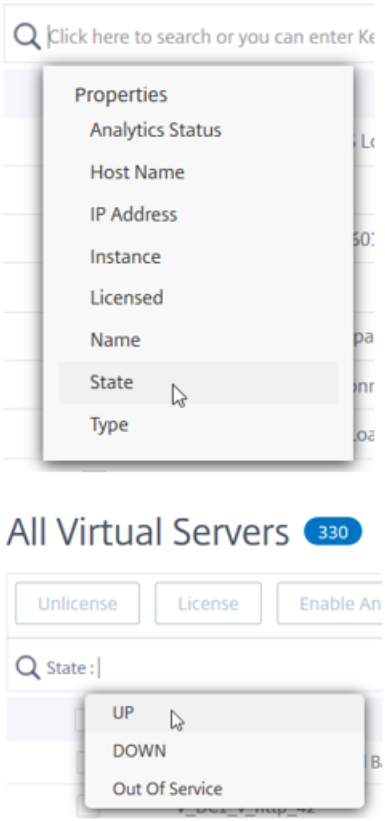
Habilitar análisis

Los siguientes son los requisitos previos para habilitar el análisis de los servidores virtuales:

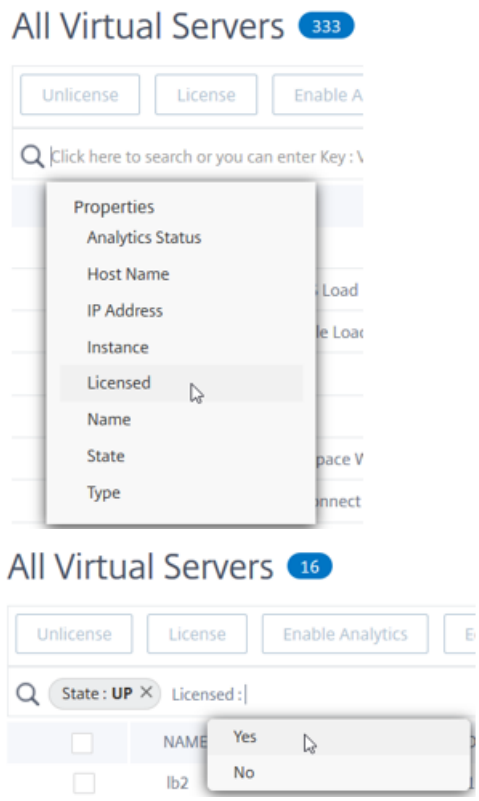
- Asegúrese de que los servidores virtuales tengan **licencia**
- Asegúrese de que el estado de los análisis **esté**
- Asegúrese de que los servidores virtuales estén en estado **UP**

Puede filtrar los resultados para identificar los servidores virtuales que se mencionan en los requisitos previos.

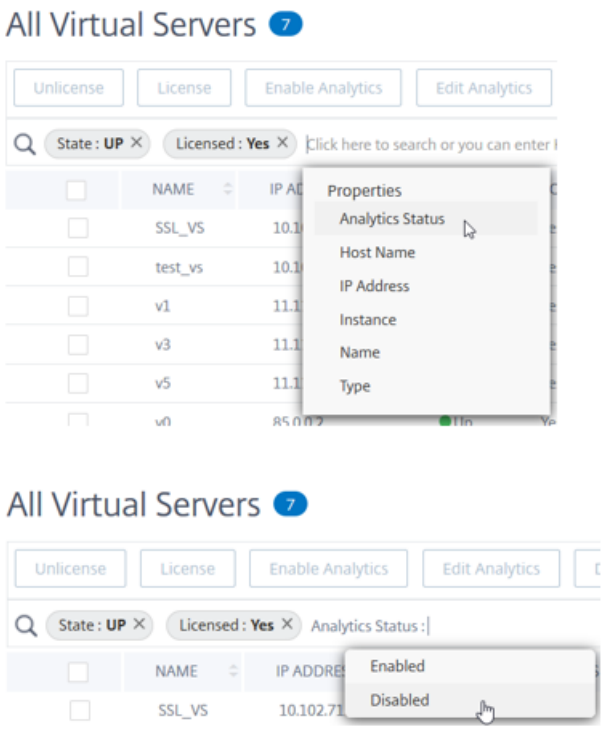
1. Haga clic en la barra de búsqueda, seleccione **Estado** y, a continuación, seleccione **UP**.



2. Haga clic en la barra de búsqueda, seleccione **Licencia** y, a continuación, seleccione **Sí**.

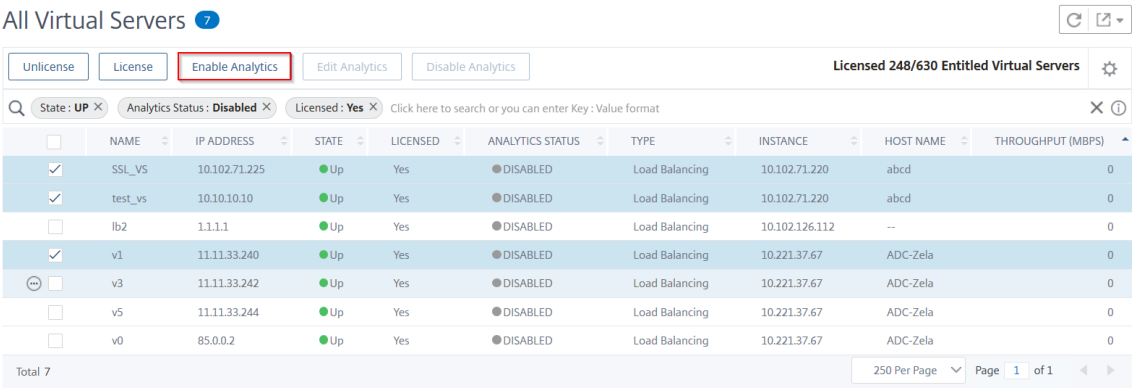


3. Haga clic en la barra de búsqueda, seleccione **Estado de análisis**y, a continuación, seleccione **Desactivado**.



4. Tras aplicar los filtros, seleccione los servidores virtuales y, a continuación, haga clic en **Habil-**

itar análisis.



5. En la ventana **Habilitar análisis**:

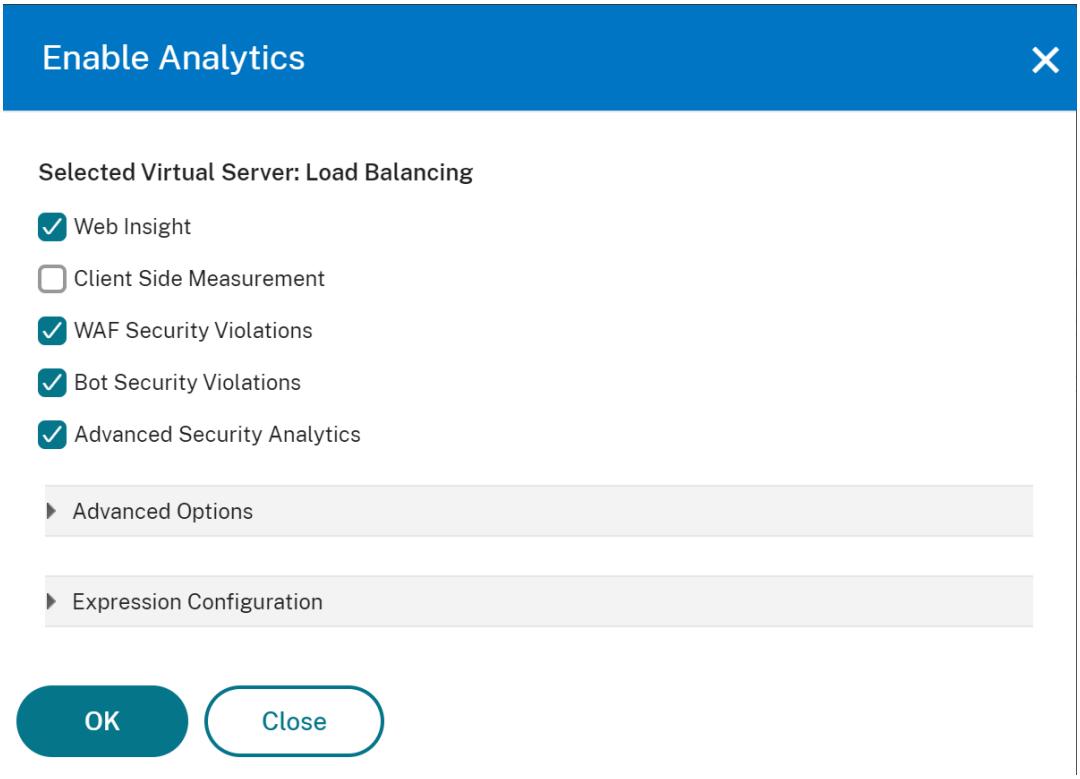
   a) Seleccione los tipos de información (Web Insight, violaciones de seguridad de WAF, infracciones de seguridad de bots)

   b) Seleccione **Logstream** o **IPFIX** como modo de transporte

   > **Nota**
   >
   > Para Citrix ADC 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para Citrix ADC 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
   >
   > Para obtener más información sobre **IPFIX** y **Logstream**, consulte **Introducción a Logstream**.

   c) La expresión es verdadera por defecto

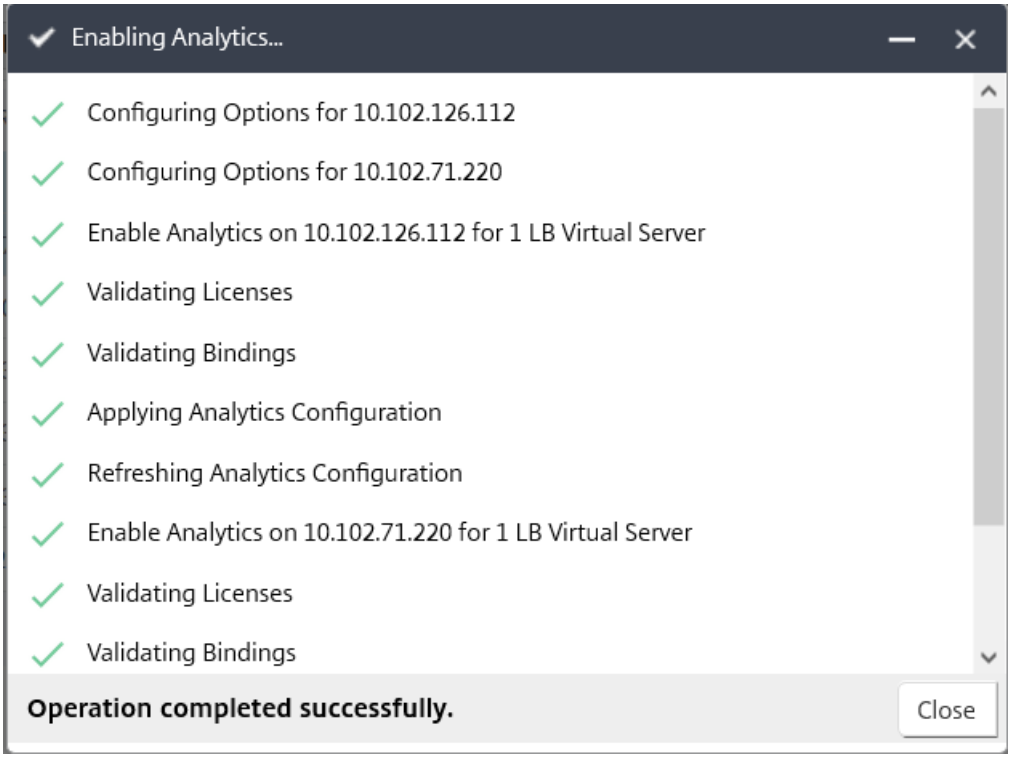
   d) Haga clic en **OK**.



Nota

- Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
- Para las particiones de administración, solo se admite **Web Insight**
- En el caso de los servidores virtuales, como el **redireccionamiento de caché**, la **autenticación**y el **GSLB**, no se pueden habilitar los análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, Citrix ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

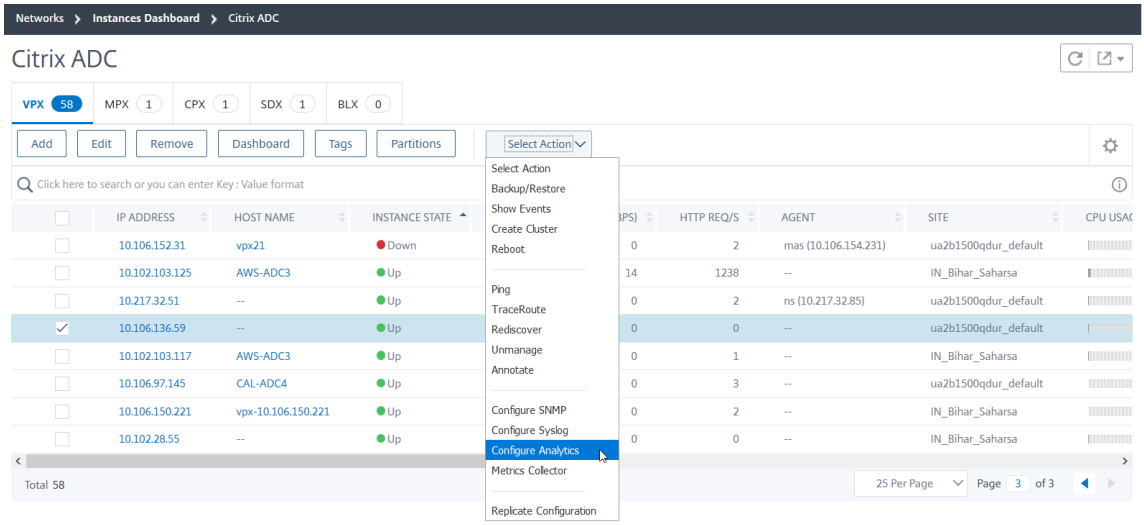


> **Nota**
>
> Citrix ADM utiliza Citrix ADC SNIP para **Logstream** y NSIP para **IPFIX**. Si hay un firewall habilitado entre el agente Citrix ADM y la instancia de Citrix ADC, asegúrese de abrir el siguiente puerto para permitir que el agente Citrix ADM recopile el tráfico de AppFlow:
>
> | Modo de transporte | IP de origen | Tipo |
> Port| |—| —|—| |
> | **IPFIX** | NSIP | UDP | 4739|
> | | **Logstream** | SNIP | TCP | 5557|

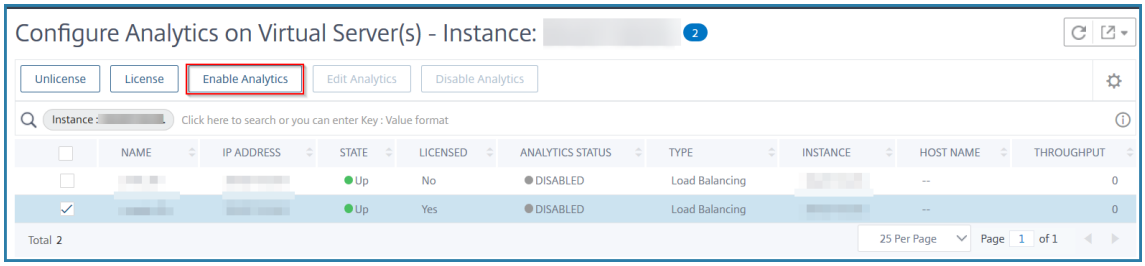
Habilitar el análisis para una instancia

Como alternativa, también puede habilitar el análisis para una instancia en particular:

1. Vaya a **Infraestructura > Instances > Citrix ADC** y, a continuación, seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Configurar análisis**.



3. En la página **Configurar análisis en servidores virtuales**, seleccione el servidor virtual y haga clic en **Habilitar análisis**.



4. En la ventana **Habilitar análisis**:

   a) Seleccione el tipo de información (Web Insight, violaciones de seguridad de WAF, infracciones de seguridad de bots)

   b) Seleccione **Logstream** o **IPFIX** como modo de transporte

   > **Nota**
   >
   > Para Citrix ADC 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para Citrix ADC 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
   >
   > Para obtener más información sobre **IPFIX** y **Logstream**, consulte **Introducción a Logstream**.

   c) La expresión es verdadera por defecto

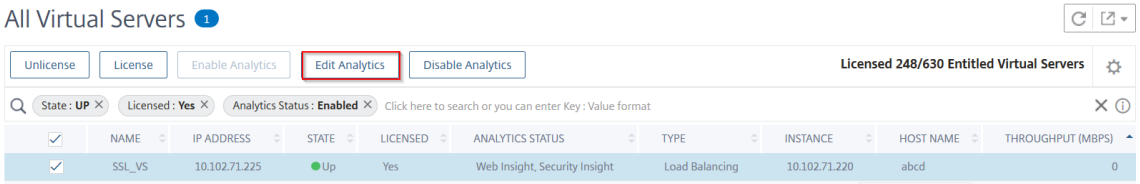
   d) Haga clic en **OK**

   .

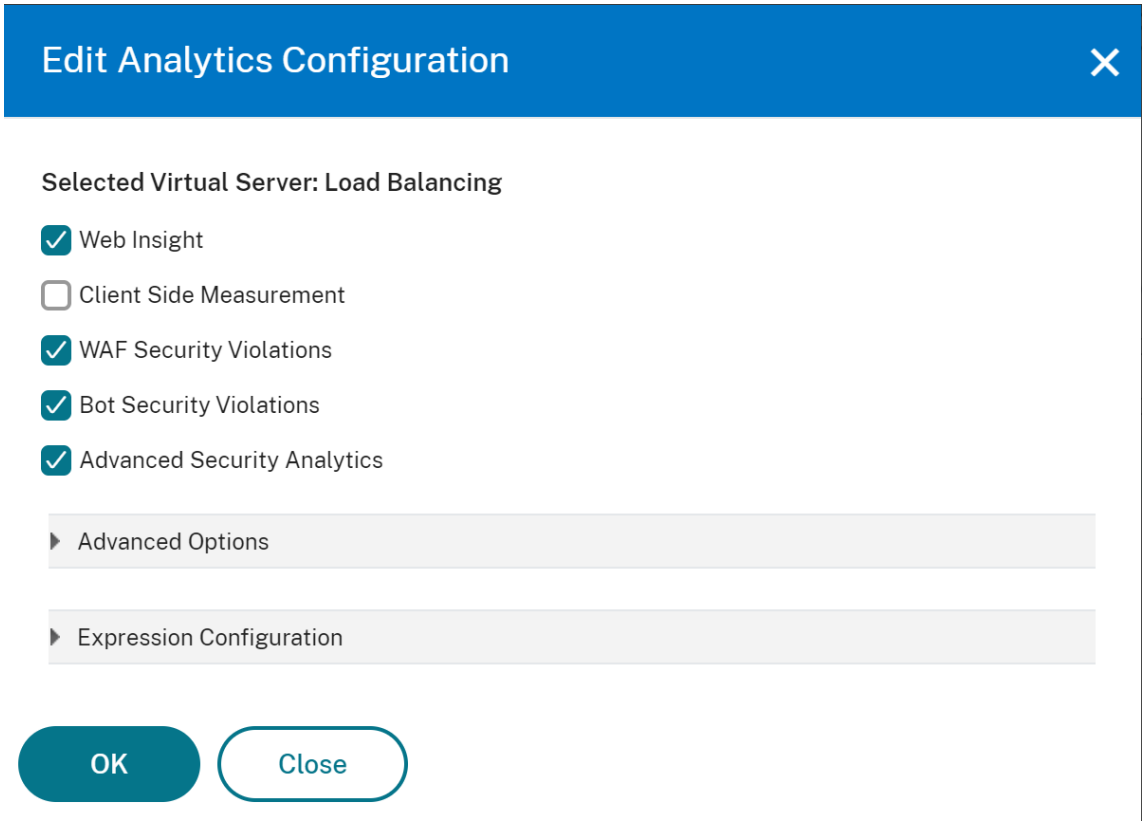
Modificar análisis

Para modificar los análisis en los servidores virtuales:

1. Seleccione los servidores virtuales
2. Haga clic en **Modificar análisis**



3. Modifique los parámetros que quiere aplicar en la ventana **Modificar configuración de Analytics**
4. Haga clic en **Aceptar**.



Modificar los análisis de una instancia

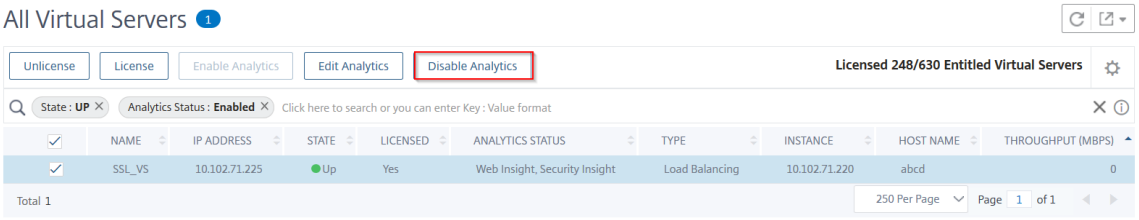
Como alternativa, también puede deshabilitar los análisis para una instancia en particular:

1. Vaya a **Red > Instancia > Citrix ADC** y seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y haga clic en **Modificar análisis**.

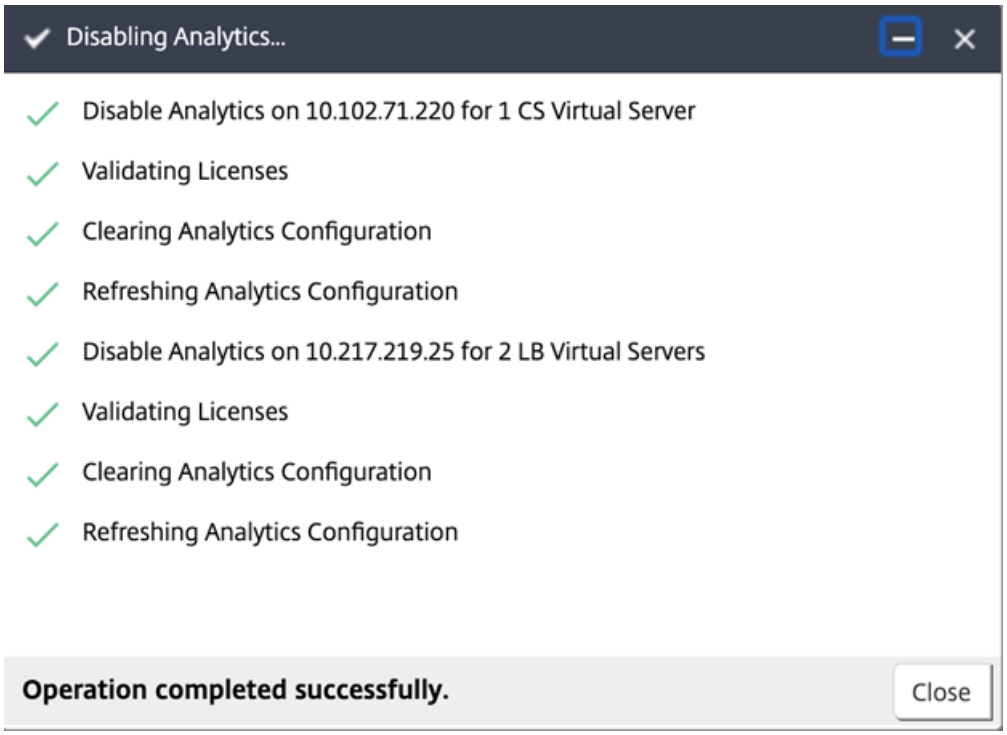
Desactivar la analítica

Para deshabilitar los análisis en los servidores virtuales seleccionados:

1. Seleccione los servidores virtuales
2. Haga clic en **Desactivar**



Citrix ADM desactiva los análisis en los servidores virtuales seleccionados



Un proceso unificado para permitir el análisis en servidores virtuales

November 16, 2022

Además del proceso existente para habilitar el análisis, también puede utilizar un flujo de trabajo de panel único para configurar el análisis en:

- Todos los servidores virtuales con licencia existentes
- Los servidores virtuales con licencia posteriores

Después de la configuración, esta función elimina la necesidad de habilitar manualmente el análisis en los servidores virtuales existentes y posteriores.

Puntos a tener en cuenta:

Antes de configurar los análisis, debe comprender los siguientes comportamientos de Citrix ADM:

- Al configurar esta función por primera vez, debe asegurarse de que se cumplen los requisitos previos mencionados en este documento.
- Modifique la configuración de análisis más adelante.

  Tenga en cuenta que ha configurado los ajustes de análisis por primera vez al seleccionar Web Insight, HDX Insight y Gateway Insight. Si quiere modificar la configuración de análisis más adelante y anular la selección de Gateway Insight, los cambios no afectan a los servidores virtuales que ya están habilitados con análisis.
- Los servidores virtuales que ya están habilitados con análisis.

  Tenga en cuenta que tiene 10 servidores virtuales con licencia y dos de ellos ya están habilitados con análisis. En este caso, esta función permite el análisis solo para los ocho servidores virtuales restantes.
- Los servidores virtuales que se inhabilitan manualmente con análisis.

  Tenga en cuenta que tiene 10 servidores virtuales con licencia y que ha inhabilitado manualmente el análisis para dos servidores virtuales. En este caso, esta función permite el análisis solo para los ocho servidores virtuales restantes y omite los servidores virtuales que se inhabilitan manualmente con el análisis.
- Las opciones**Infracciones de seguridad de bots** e **Infracciones de seguridad de WAF** solo se admiten en servidores virtuales con licencia premium. Si los servidores virtuales no tienen licencia premium, las violaciones de **seguridad de bots y las violaciones** de **seguridad de WAF** no están habilitadas.

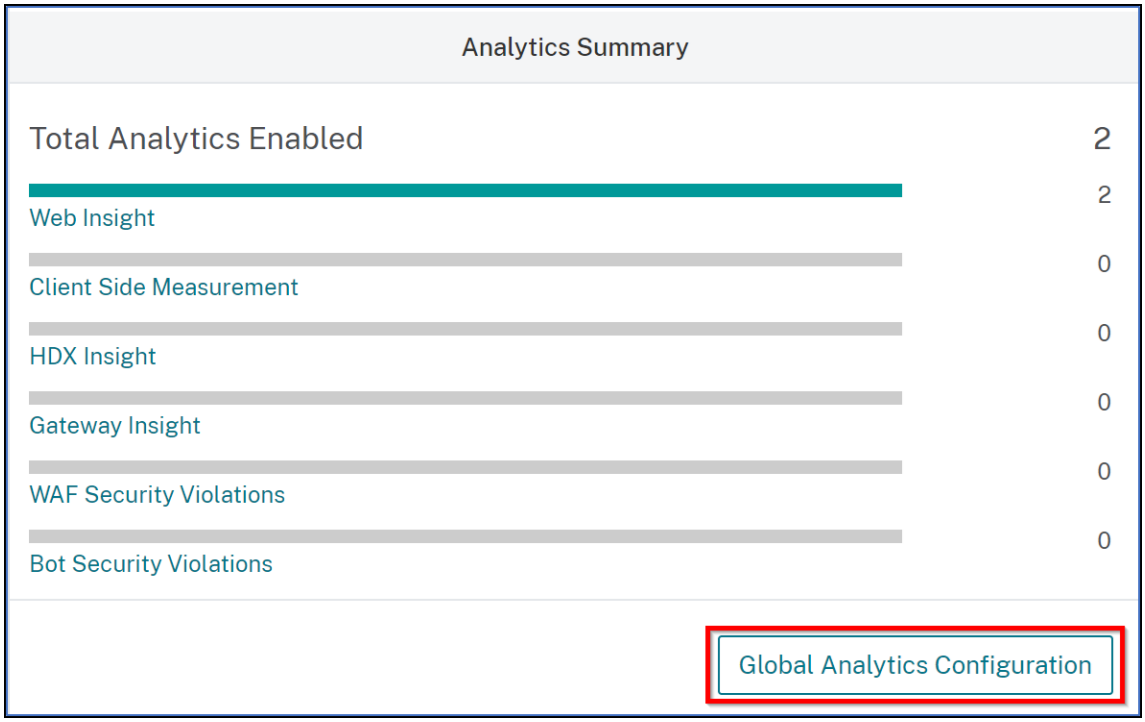
Requisitos previos

Compruebe que:

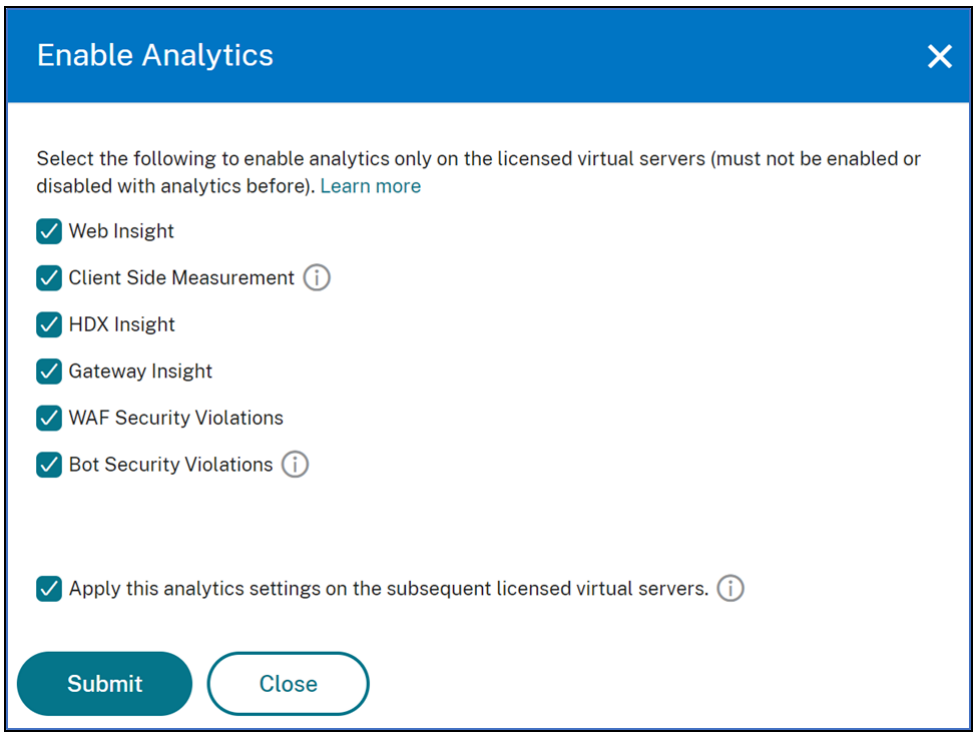
- Todos los servidores virtuales existentes tienen licencia.
- La opción de licencia automática está habilitada para licenciar todos los servidores virtuales posteriores. Vaya a **Configuración > Configuración de licencias y análisis** y, en **Asignación de licencias de servidores virtuales**, active la opción **Servidores virtuales con licencia automática**.

Habilitar análisis

1. Vaya a **Configuración > Configuración de licencias y análisis**.
2. En **Resumen de análisis**, haga clic en **Configuración de análisis global**.



3. Seleccione las funciones de análisis que quiere habilitar para el análisis en los servidores virtuales.
4. Para habilitar el análisis en los servidores virtuales posteriores, seleccione la casilla **Aplicar esta configuración de análisis en los servidores virtuales con licencia posteriores**.
5. Haga clic en **Submit**.



Configurar el control de acceso basado en roles

December 2, 2022

Citrix ADM proporciona un control de acceso detallado y basado en roles (RBAC) con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales dentro de su empresa.

En Citrix ADM, 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 Citrix ADM con las credenciales de Citrix Cloud. Se le concede la función de superadministrador y, de forma predeterminada, tiene todos los permisos de acceso en Citrix ADM. Más adelante, puede crear otros usuarios en su organización en Citrix Cloud.

Los usuarios que se crean más adelante y que inician sesión en Citrix ADM como usuarios normales se conocen como 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 a estos usuarios administradores delegados. Para ello, puede crear las directivas adecuadas y asignarlas 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.

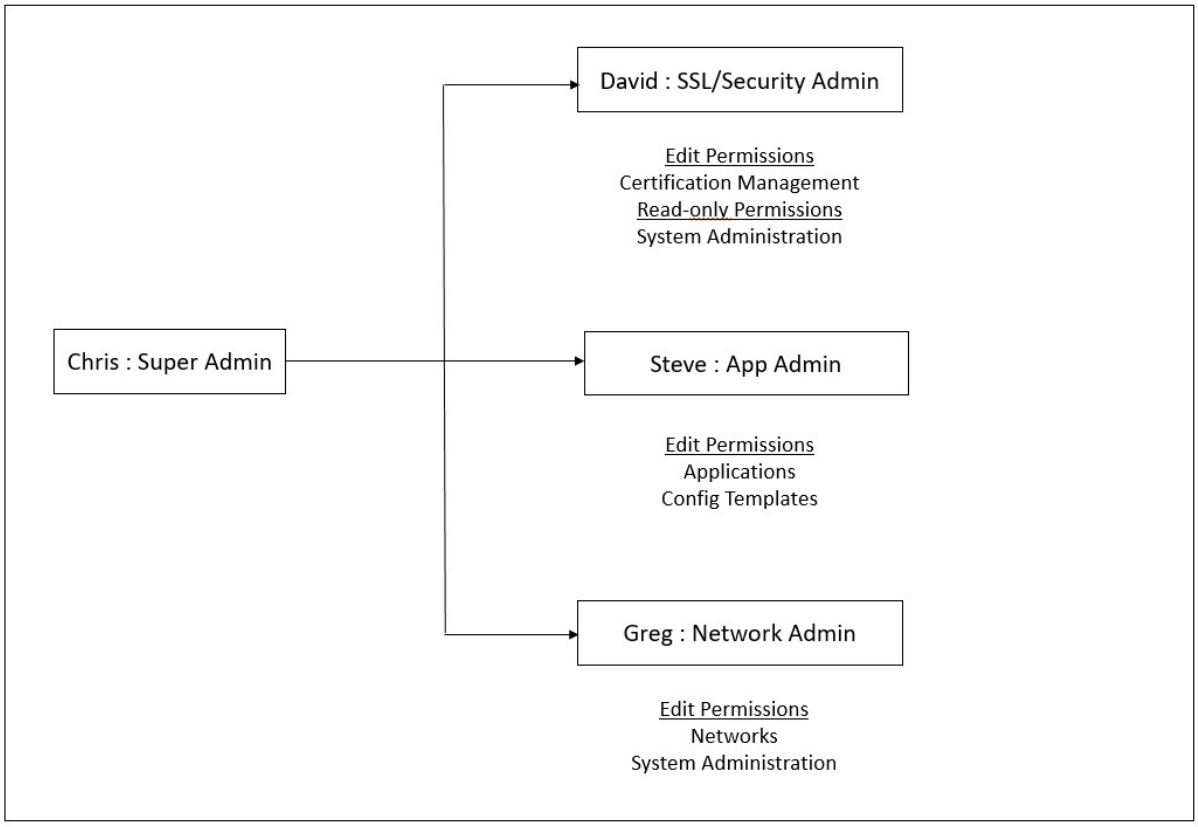
Ejemplo:

El siguiente ejemplo ilustra cómo se puede lograr el RBAC en Citrix ADM.

Chris, el jefe del grupo ADC, es el superadministrador de Citrix ADM en su organización. Crea tres funciones de administrador: Administrador de seguridad, administrador de aplicaciones y administrador de red.

- David, el administrador de seguridad, debe tener acceso completo para la administración y supervisión de certificados SSL, pero debe tener acceso de solo lectura para las operaciones de administración del sistema.
- Steve, un administrador de aplicaciones, necesita acceso solo a aplicaciones específicas y a plantillas de configuración específicas.
- Greg, un administrador de red, necesita acceso a la administración de sistemas y redes.
- Chris también debe proporcionar RBAC 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 proporcionar un control de acceso basado en roles a sus usuarios, Chris primero debe agregar

usuarios en Citrix Cloud y solo después podrá verlos en Citrix ADM. 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.

Los roles están determinados por las directivas. 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 Citrix ADM, la creación de roles y directivas es específica de la función RBAC en Citrix ADC. Los roles y las directivas se pueden crear, cambiar o interrumpir fácilmente a medida que evolucionan las necesidades de la empresa, sin tener que actualizar individualmente los privilegios de cada usuario.

Los roles pueden estar basados en funciones o en recursos. Por ejemplo, considere un administrador SSL/Security y un administrador de aplicaciones. Un administrador de SSL/Security debe tener acceso completo a las funciones de supervisión y administración de certificados SSL, pero debe tener acceso de solo lectura para las operaciones de administración del sistema. Los administradores de aplicaciones solo pueden acceder a los recursos dentro de su ámbito.

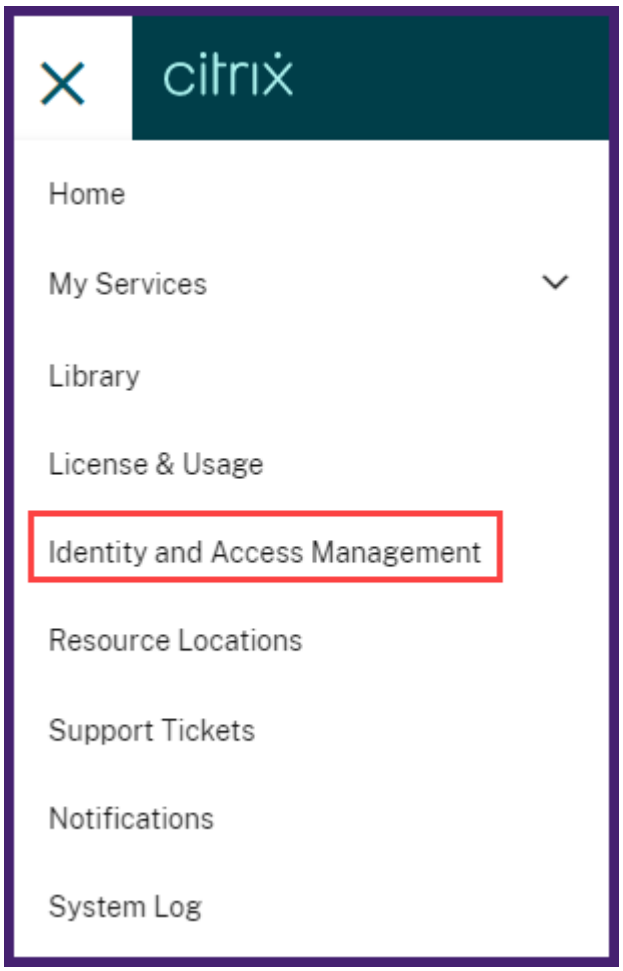
Por lo tanto, en su papel de Chris, el superadministrador, realice las siguientes tareas de ejemplo en Citrix ADM para configurar las directivas de acceso, las funciones y los grupos de usuarios para David, que es el administrador de seguridad de su organización.

Configurar usuarios en Citrix ADM

Como superadministrador, puede crear más usuarios configurando cuentas para ellos en Citrix Cloud y no en Citrix ADM. Cuando los nuevos usuarios se agregan a Citrix ADM, solo puede definir sus permisos asignando los grupos apropiados al usuario.

Para agregar nuevos usuarios en Citrix Cloud:

1. En la GUI de Citrix ADM, haga clic en el icono de hamburguesa en la parte superior izquierda y seleccione **Administración de identidades y accesos**.

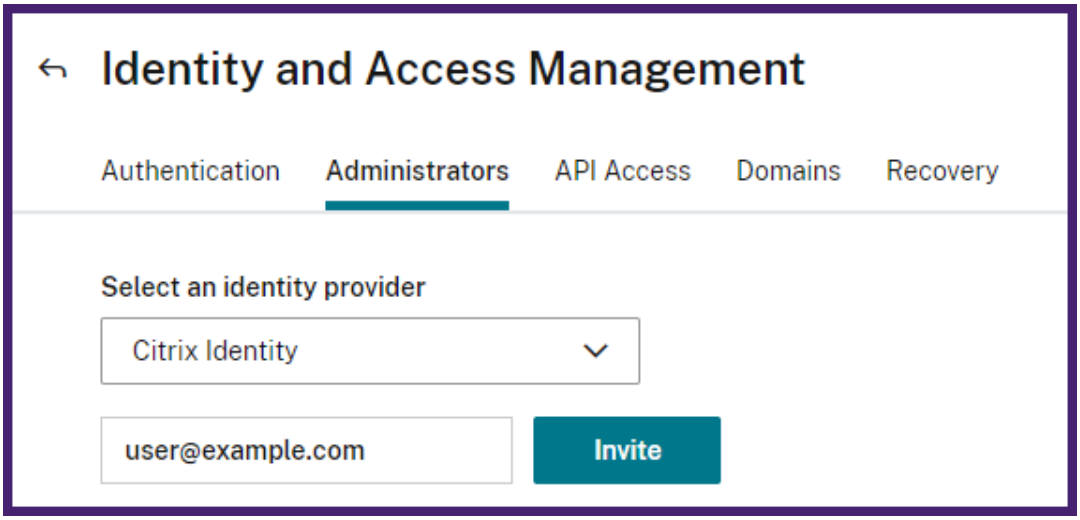


2. En la página Administración de identidades y acceso, seleccione la ficha **Administradores**.

   Esta ficha muestra los usuarios creados en Citrix Cloud.

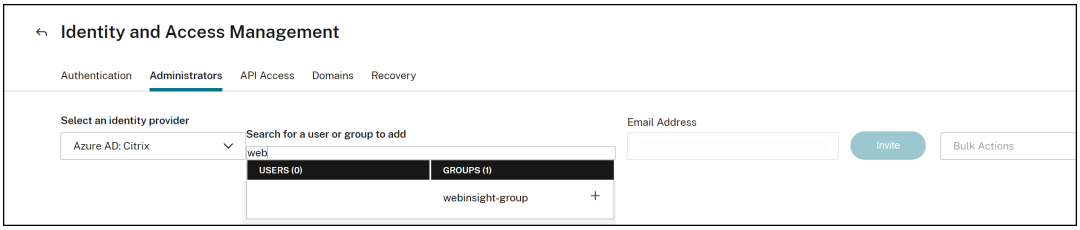
3. Seleccione el proveedor de identidad de la lista.

   - **Citrix Identity**: escriba la dirección de correo electrónico del usuario que quiere agregar en Citrix ADM y haga clic en **Invitar**.



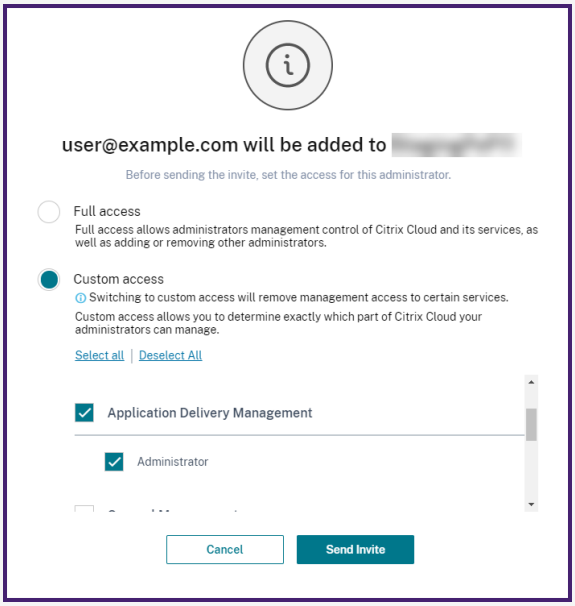
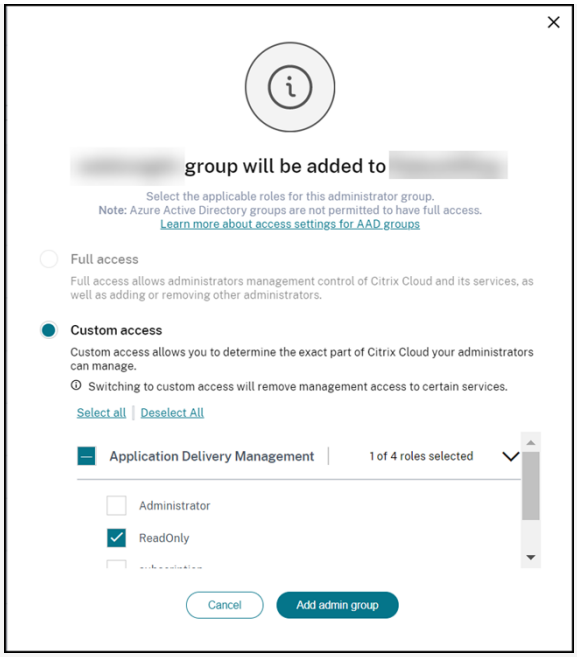
> **Nota**
>
> El usuario recibe una invitación por correo electrónico de Citrix Cloud. El usuario debe hacer clic en el enlace proporcionado en el correo electrónico para completar el proceso de registro proporcionando su nombre completo y contraseña, y luego iniciar sesión en Citrix ADM con sus credenciales.

- **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 Citrix ADM 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 Citrix ADM con las credenciales de Azure AD.



4. Seleccione **Acceso personalizado** para el usuario o grupo especificado.
5. Seleccione **Administración de entrega de aplicaciones**.

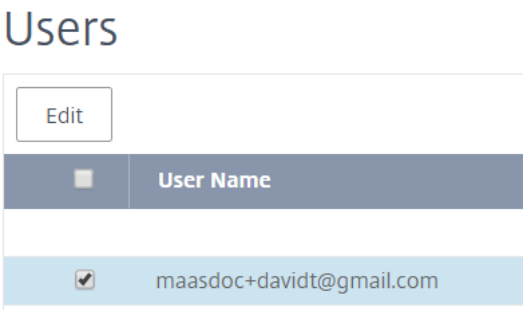
   Esta opción muestra los grupos de usuarios creados en Citrix ADM. Seleccione el grupo al que quiere agregar el usuario.

Identidad de Citrix	Azure AD
	
Haga clic en **Enviar invitación**.	Haga clic en **Agregar grupo de administradores**.

Como administrador, verá el nuevo usuario en la lista Usuarios de Citrix ADM sólo después de que el usuario inicie sesión en Citrix ADM.

Para configurar usuarios en Citrix ADM:

1. En la GUI de Citrix ADM, 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 Citrix ADM únicamente desde Citrix Cloud. Por lo tanto, aunque tenga permisos de administrador, no puede agregar o eliminar usuarios en la GUI de Citrix ADM. 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 Citrix ADM al menos una vez.

Configurar directivas de acceso en Citrix ADM

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. Los roles están determinados por las directivas. Después de crear directivas, debe crear roles, enlazar cada rol a una o varias directivas y asignar roles a grupos de usuarios. Citrix ADM proporciona cinco directivas de acceso predefinidas:

- **admin_policy**. Otorga acceso a todos los nodos de Citrix ADM. El usuario tiene permisos de visualización y edición, puede ver todo el contenido de Citrix ADM y puede realizar todas las operaciones de edición. Es decir, el usuario puede agregar, modificar y eliminar operaciones en los recursos.
- **adminExceptSystem_Policy**. Otorga acceso a los usuarios a todos los nodos de la GUI de Citrix ADM, excepto el acceso al nodo de configuración.
- **readonly_policy**. Otorga permisos de solo lectura. El usuario puede ver todo el contenido de Citrix ADM, pero no está autorizado a realizar ninguna operación.
- **appadmin_policy**. Otorga permisos administrativos para acceder a las funciones de la aplicación en Citrix ADM. Un usuario vinculado a esta directiva puede agregar, modificar y eliminar aplicaciones personalizadas, y puede habilitar o deshabilitar los servicios, los grupos de servicios y los distintos servidores virtuales, como el cambio 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, cuando asignaba directivas a roles y enlazaba los roles a grupos de usuarios, puede proporcionar permisos para los grupos de usuarios a nivel de nodo en la GUI de Citrix ADM. Por ejemplo, solo puede proporcionar permisos de acceso a todo el nodo Equilibrio de carga. Los usuarios tenían permiso para acceder a todos los subnodos específicos de la entidad en el nodo Equilibrio de carga (por ejemplo, servidor virtual, servicios y otros) o no tenían permiso para acceder a ningún nodo en **Equilibrio de carga**.

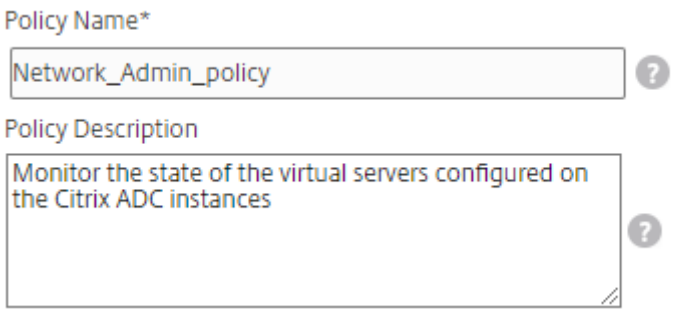
En la compilación de Citrix ADM 507.x y en las versiones posteriores, la administración de directivas de acceso se amplía para proporcionar también permisos para los subnodos. La configuración de directiva de acceso se puede configurar para todos los subnodos, como servidores virtuales, servicios, grupos de servicios y servidores.

Actualmente, puede proporcionar un permiso de acceso de nivel granular sólo para subnodos bajo un nodo Equilibrio de carga y también para subnodos bajo el nodo GSLB.

Por ejemplo, como administrador, puede que quiera conceder al usuario un permiso de acceso solo para ver servidores virtuales, pero no los servicios back-end, los grupos de servicios y los servidores de aplicaciones en el nodo 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 Citrix ADM, vaya a **Configuración** > **Usuarios y funciones** > **Directivas 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** .



La sección **Permisos** enumera todas las funciones de Citrix ADM, con opciones para especificar el acceso de solo lectura, habilitar-deshabilitar o modificar.

a) Haga clic en el icono (+) para expandir cada grupo de entidades en varias entidades.

b) Seleccione la casilla de verificación de permisos situada junto al nombre de la función para conceder permisos a los usuarios.

- **Ver:** Esta opción permite al usuario ver la función en Citrix ADM.
- **Activar-Inhabilitar:** Esta opción solo está disponible para las **funciones Funciones de red** que permiten habilitar o inhabilitar acciones en Citrix ADM. El usuario puede habilitar o inhabilitar la función. Además, un 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.

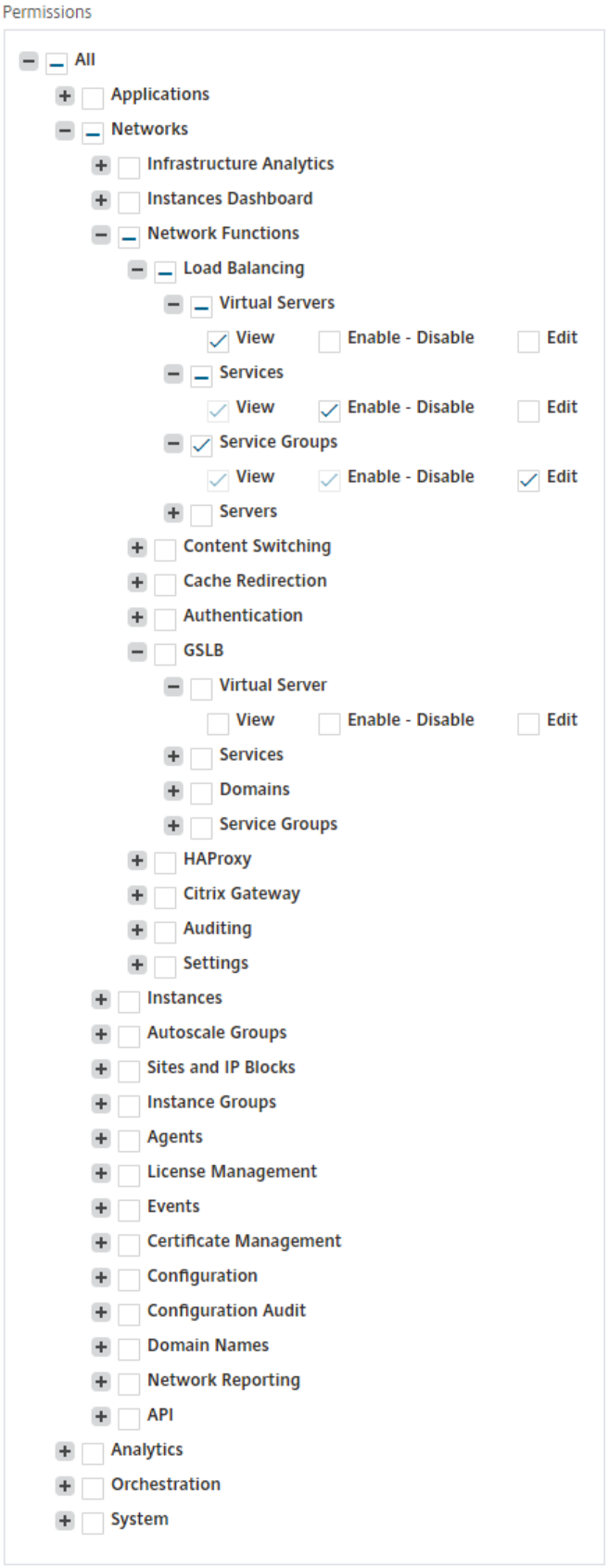
- **Modificar:** esta opción otorga el acceso total al usuario. El usuario puede modificar la función y sus funciones.

  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 Citrix ADM. Para ver los servidores virtuales, vaya a **Infraestructura > Funciones de red > Equilibrio de carga** y seleccione la ficha **Servidores virtuales**.

El permiso **Habilitar-Inhabilitar** se concede a un usuario para la función **Servicios**. Este permiso también otorga el permiso de **visualización** . El usuario puede habilitar o inhabilitar los servicios enlazados a un servidor virtual de equilibrio de carga. Además, el usuario puede realizar **la acción 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 Habilitar o inhabilitar en 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**.

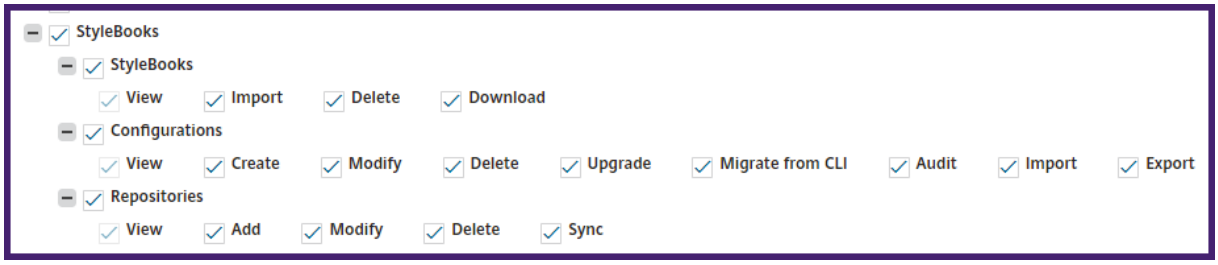
4. Haga clic en **Crear**.

> **Nota**
>
> Al seleccionar **Modificar**, es posible que se asignen internamente permisos dependientes que no se muestran como habilitados en la sección Permisos. Por ejemplo, cuando habilita permisos de edición para la administración de errores, Citrix ADM proporciona internamente permisos para configurar un perfil de correo o para crear configuraciones de servidor SMTP, de modo que el usuario pueda enviar el informe como correo.

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 habilita automáticamente cuando concede otros permisos de StyleBook.



Configurar roles en Citrix ADM

En Citrix ADM, cada función está vinculada a una o más directivas de acceso. Puede definir relaciones uno a uno, uno a varios y muchos a muchos entre directivas y roles. Puede vincular un rol a varias directivas y puede vincular varios roles a una directiva.

Por ejemplo, un rol puede estar enlazado a dos directivas, con una directiva que defina los permisos de acceso para una función y la otra que defina los permisos de acceso para otra función. Una directiva puede conceder permiso para agregar instancias de Citrix ADC en Citrix ADM, y la otra directiva puede conceder permiso para crear e implementar un StyleBook y configurar instancias de Citrix ADC.

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.

Citrix ADM proporciona cinco funciones predefinidas:

- **admin_role**. Tiene acceso a todas las funciones de Citrix ADM. (Esta función está vinculada a`adminpolicy`.)
- **adminExceptSystem_role**. Tiene acceso a la GUI de Citrix ADM, 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 Citrix ADM. (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).

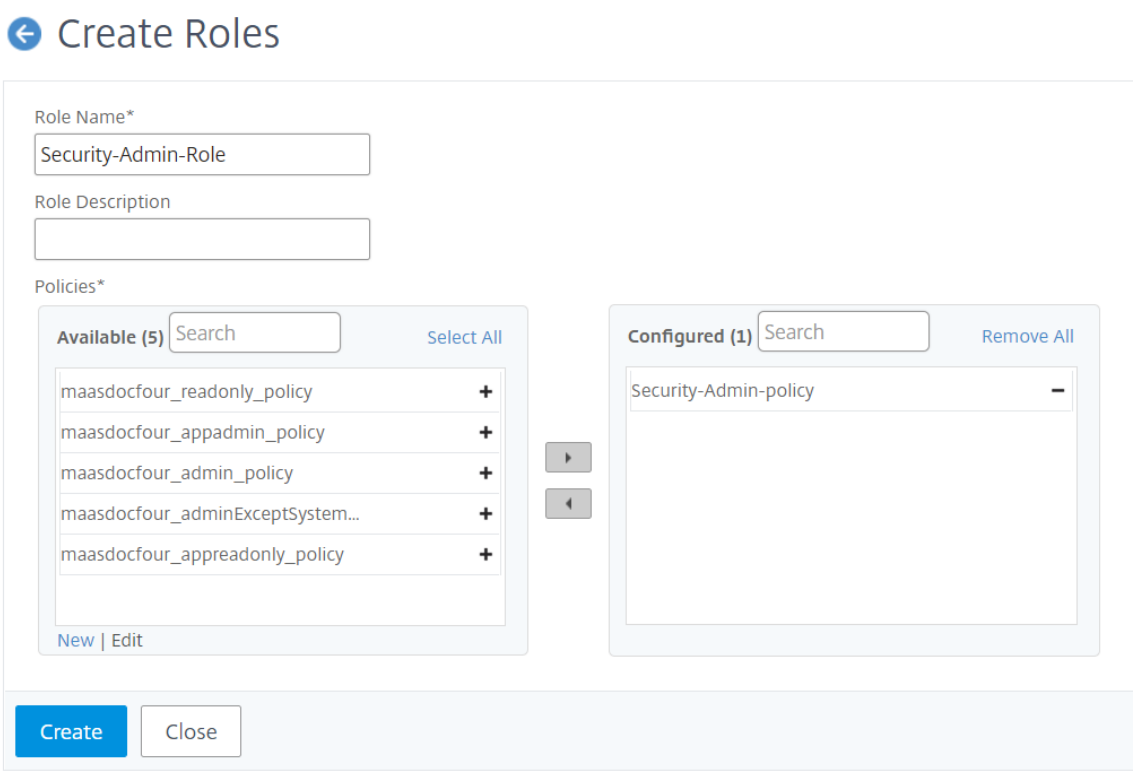
Aunque no puede modificar las funciones predefinidas, puede crear las suyas propias (definidas por el usuario).

Para crear roles y asignarles directivas:

1. En la GUI de Citrix ADM, 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 inquilino (por ejemplo, `maasdocfour`) que es único para todos los inquilinos.



> **Nota**
>
> Puede crear una directiva de acceso haciendo clic en **Nueva**o ir a **Configuración** > **Usuarios y funciones** > **Directivas de acceso** y crear directivas.

5. Haga clic en **Crear**.

Configurar grupos en Citrix ADM

En Citrix ADM, un grupo puede tener acceso tanto a nivel de entidad como a nivel de recursos. Por ejemplo, un grupo de usuarios puede tener acceso solo a instancias seleccionadas de Citrix ADC; 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 Citrix ADM.

Puede administrar el acceso de un usuario en Citrix ADM a nivel individual de las entidades de funciones de red. Puede asignar dinámicamente permisos específicos al usuario o al grupo a nivel de entidad.

Citrix ADM trata el servidor virtual, los servicios, los grupos de servicios y los servidores como entidades de función de red.

- **Servidor virtual (Aplicaciones)** : Equilibrio de carga (`lb`), GSLB, conmutación de contexto (`CS`), redirección de caché (`CR`), autenticación (`Auth`) y Citrix Gateway (`vpn`)
- **Servicios**: Equilibrio de carga y servicios GSLB
- **Grupo de servicios: grupos** de servicios GSLB y equilibrio de carga
- **Servidores: servidores** de equilibrio de carga

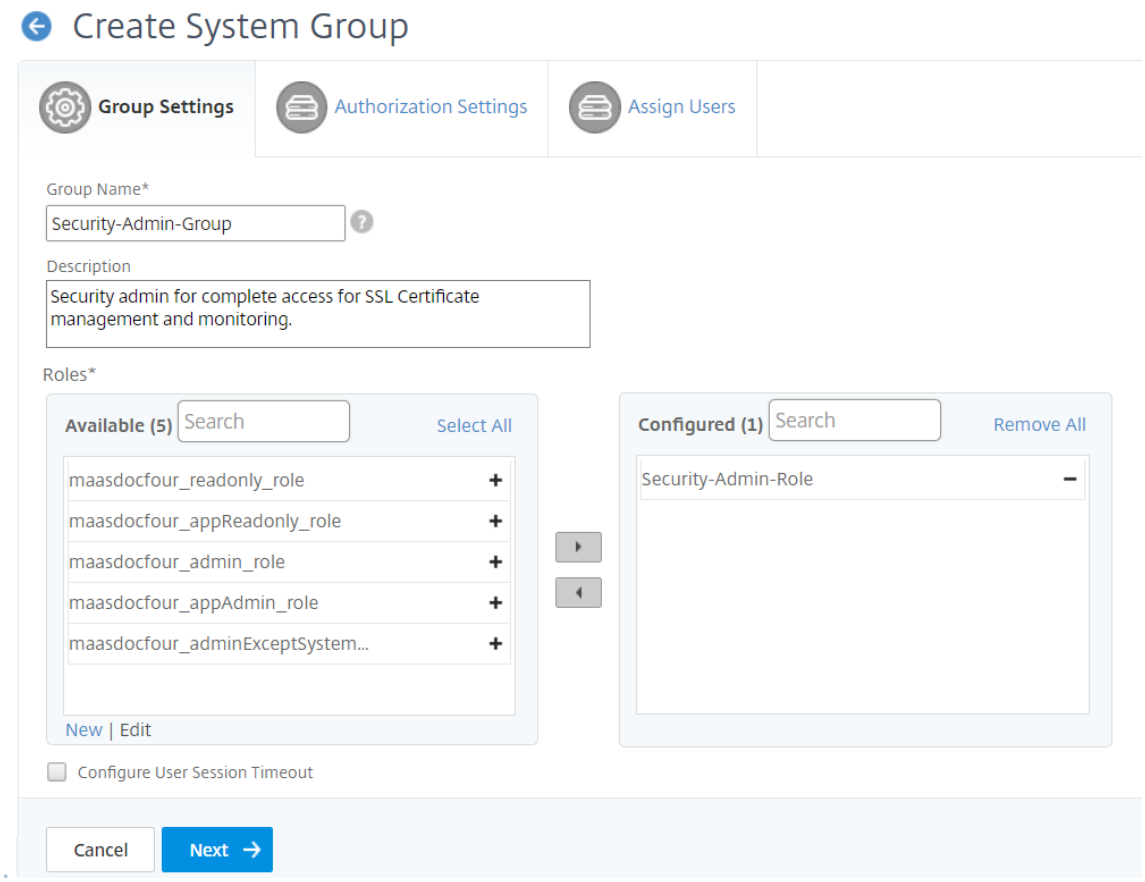
Para crear un grupo:

1. En Citrix ADM, vaya a **Configuración** > **Usuarios y funciones** > **Grupos**.
2. Haga clic en **Agregar**.

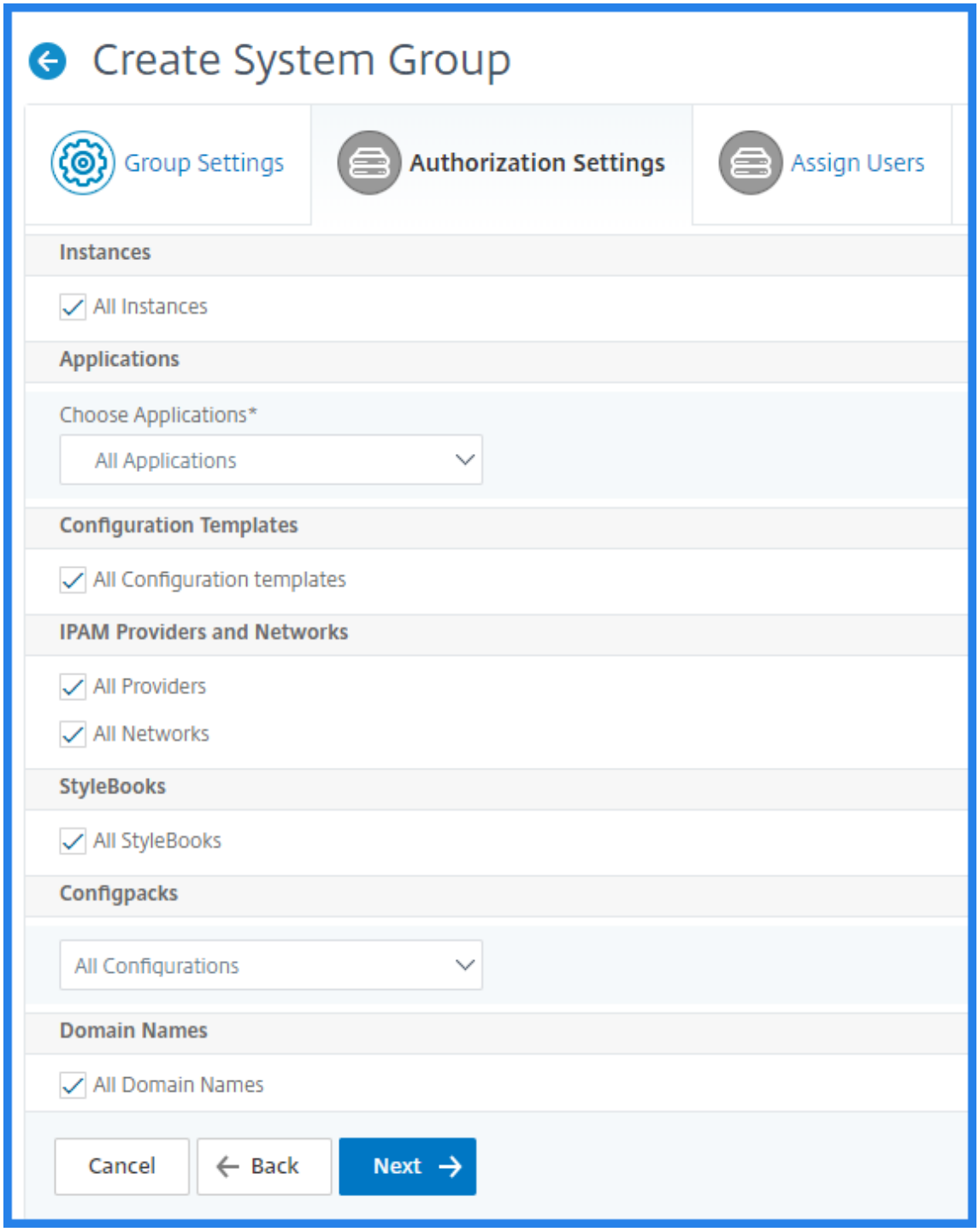
   Aparece la página **Crear grupo de sistemas** .
3. En el campo **Nombre de grupo**, escriba el nombre del grupo.
4. En el campo **Descripción del grupo**, escriba una descripción del grupo. Proporcionar una buena descripción le ayuda a entender el rol y la función del grupo.
5. En la sección **Funciones**, mueva una o más funciones a la lista de funciones **configuradas** .

   > **Nota**
   >
   > Los roles llevan como prefijo un identificador de inquilino (por ejemplo, `maasdocfour`) que es único para todos los inquilinos.
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**



Es posible que quiera seleccionar recursos específicos de las categorías a las que los usuarios pueden tener acceso.

Grupos de Autoscale:

Si quiere seleccionar los grupos de Autoscale específicos que el usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los grupos de AutoScale** y haga clic en **Agregar grupos de AutoScale**.

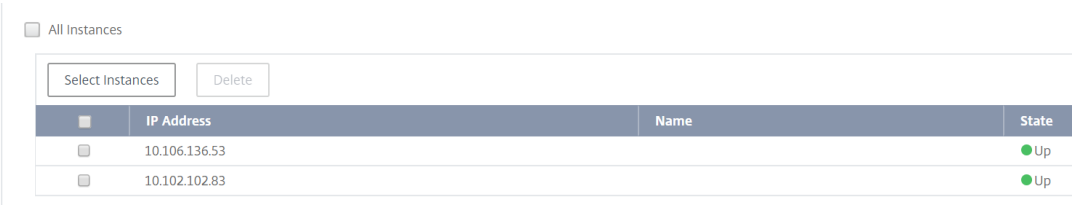
b) Seleccione los grupos de Autoscale necesarios de la lista y haga clic en **Aceptar**.

Instancias:

Si quiere seleccionar las instancias específicas que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todas las instancias** y haga clic en **Seleccionar instancias**.

b) Seleccione las instancias necesarias de la lista y haga clic en **Aceptar**.



Aplicaciones:

La lista **Elegir aplicaciones** le permite conceder acceso a un usuario a las aplicaciones necesarias.

Puede conceder acceso a las aplicaciones sin seleccionar sus instancias. 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 el Citrix ADM.
- **Todas las aplicaciones de instancias seleccionadas:** Esta opción solo aparece si selecciona instancias de la categoría **Todas las instancias**. Agrega todas las aplicaciones presentes en la instancia seleccionada.
- **Aplicaciones específicas:** esta opción le permite agregar las aplicaciones necesarias a las que quiere que accedan los usuarios. Haga clic en **Agregar aplicaciones** y seleccione las aplicaciones necesarias de la lista.
- **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**, Citrix ADM autoriza todas las entidades que están enlazadas a la aplicación seleccionada.

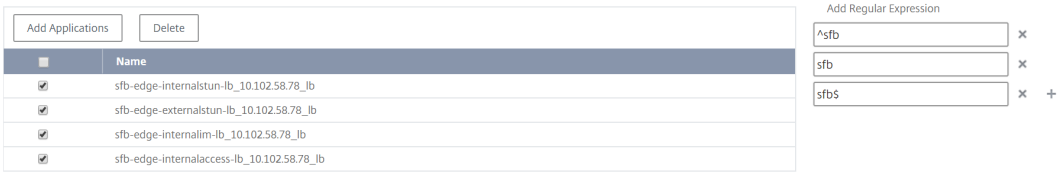
> **Nota**
>
> Asegúrese de haber seleccionado solo un tipo de entidad si quiere autorizar las entidades enlazadas.

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 de expresiones regulares especificada se conserva en Citrix ADM. Para agregar una expresión regular, lleve a cabo los siguientes pasos:

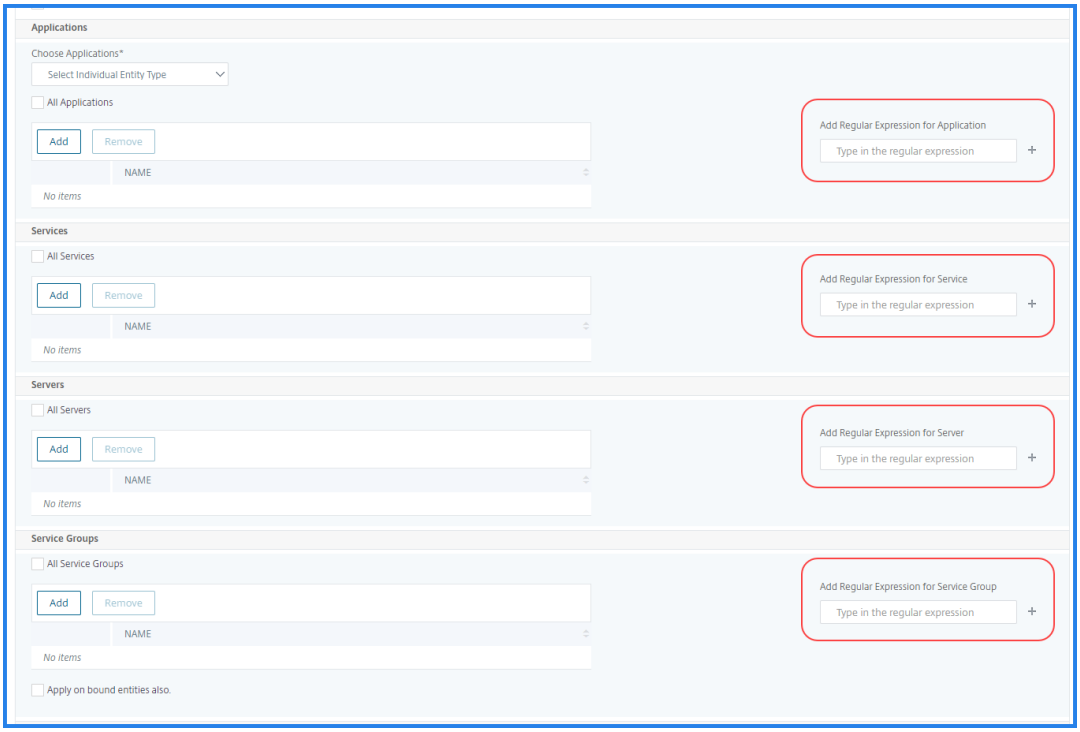
a) Haga clic en **Agregar expresión regular**.

b) Especifique la expresión regular en el cuadro de texto.

En la siguiente imagen se explica cómo utilizar la expresión regular para agregar una aplicación cuando se selecciona la opción **Aplicaciones específicas** :



En la siguiente imagen se explica cómo utilizar la expresión regular para agregar entidades de función de red al elegir la opción **Seleccionar el tipo de entidad individual** :



Si quiere agregar más expresiones regulares, haga clic en el icono **+** .

> **Nota**
>
> La expresión regular solo coincide con el nombre del servidor para el tipo de entidad **Servidores** 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.

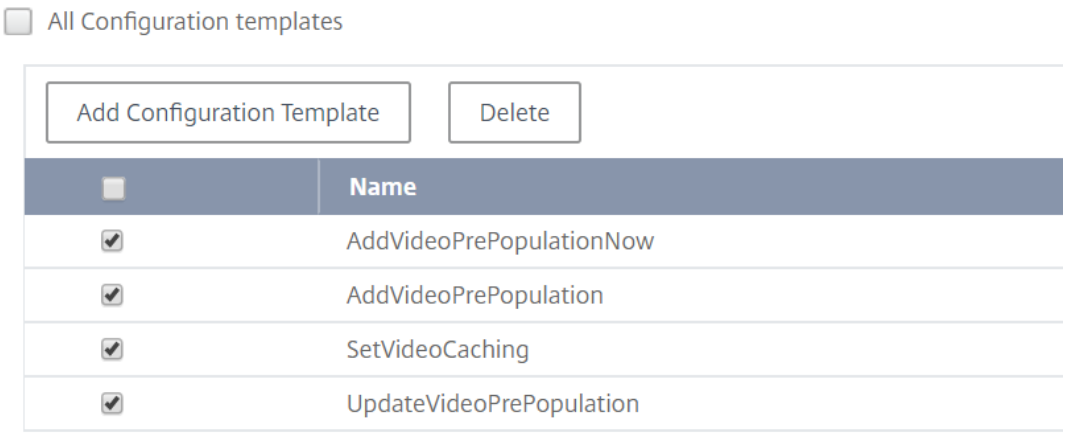
La expresión regular se almacena en el sistema para actualizar el alcance de la autorización. Cuando las nuevas entidades coinciden con la expresión regular de su tipo de entidad, Citrix ADM actualiza el alcance de la autorización para las nuevas entidades.

Plantillas de configuración:

Si quiere seleccionar la plantilla de configuración específica que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todas las plantillas de configuración** y haga clic en **Agregar plantilla de configuración**.

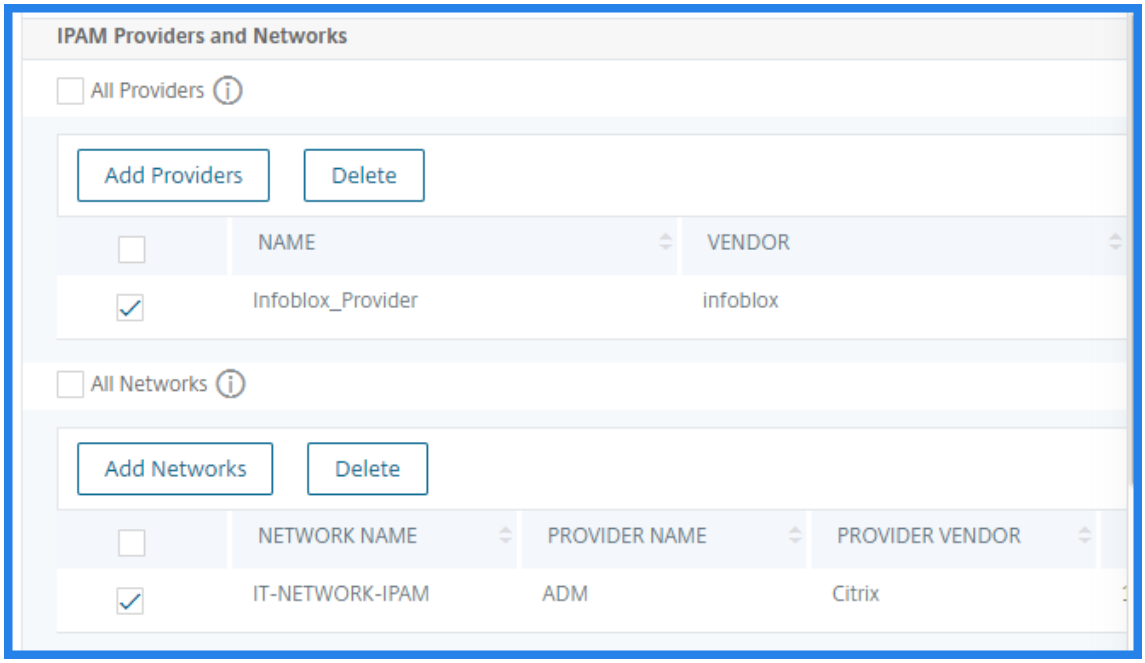
b) Seleccione la plantilla necesaria de la lista y haga clic en **Aceptar**.



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** : desactive la casilla **Todos los proveedores** y haga clic en **Agregar proveedores**. Puede seleccionar los proveedores necesarios y hacer clic en **Aceptar**.
- **Agregar redes** : desactive la casilla **Todas las redes** y haga clic en **Agregar redes**. Puede seleccionar las redes necesarias y hacer clic en **Aceptar**.



StyleBooks:

Si quiere seleccionar el StyleBook específico que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los StyleBooks** y haga clic en **Agregar StyleBook al grupo**.

Puede seleccionar StyleBooks individuales o especificar una consulta de filtro para autorizar StyleBooks.

Si quiere seleccionar los StyleBooks individuales, seleccione los StyleBooks en el panel **Individuales StyleBooks** y haga clic en **Guardar selección**.

Si quiere utilizar una consulta para buscar StyleBooks, seleccione el panel **Filtros personalizados**. Una consulta es una cadena de pares clave-valor donde las claves son `name`, `namespace`, y `version`.

También puede utilizar expresiones regulares como valores para buscar y agregar StyleBooks que cumplan los criterios de expresiones regulares para los grupos. Una consulta de filtro personalizada para buscar StyleBooks admite las operaciones `And` y `Or`.

Ejemplo:

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
     version=1.0
2 <!--NeedCopy-->
```

Esta consulta enumera los StyleBooks que cumplen las condiciones siguientes:

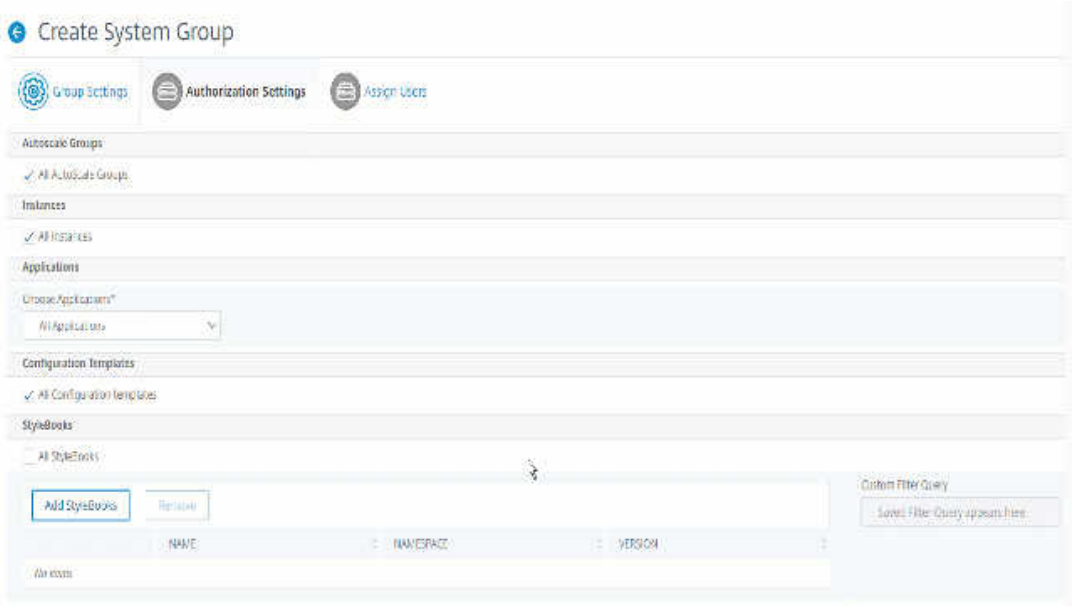
- El nombre de StyleBook es `lb-mon` o `lb`.
- El espacio de nombres StyleBook es `com.citrix.adc.stylebooks`.
- La versión de StyleBook es `1.0`.

Utilice una operación `Or` entre expresiones de valor definidas para la expresión clave.

Ejemplo:

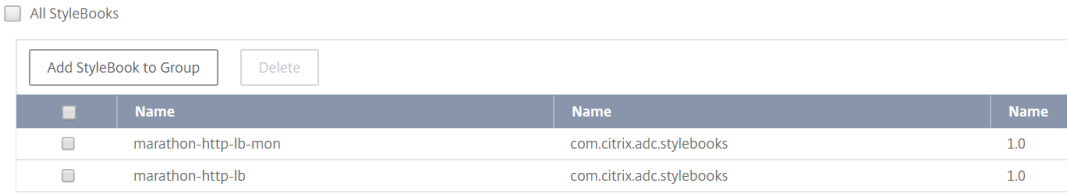
- La consulta `name=lb-mon|lb` es válida. Devuelve los StyleBooks que tienen un nombre `lb-mon` o `lb`.
- La consulta `name=lb-mon | version=1.0` no es válida.

Presione `Enter` para ver los resultados de la búsqueda y haga clic en **Guardar consulta**.



La consulta guardada aparece en la **consulta de filtros personalizados**. Según la consulta guardada, Citrix ADM proporciona a los usuarios acceso a esos StyleBooks.

b) Seleccione los StyleBooks necesarios de la lista y haga clic en **Aceptar**.

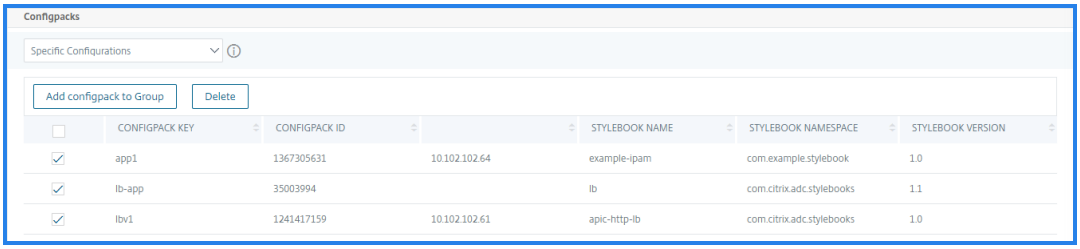


Puede seleccionar los StyleBooks necesarios cuando cree grupos y agregue usuarios a ese grupo. Cuando el usuario selecciona el StyleBook permitido, también se seleccionan todos los StyleBooks dependientes.

Paquetes de configuración:

En **Configpacks**, seleccione una de las siguientes opciones:

- **Todas las configuraciones**: esta opción está seleccionada de forma predeterminada. Agrega todos los paquetes de configuración que se encuentran en Citrix 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 los paquetes de configuración necesarios.



Puede seleccionar los paquetes de configuración necesarios al crear grupos y agregar usuarios a ese grupo.

Nombres de dominio:

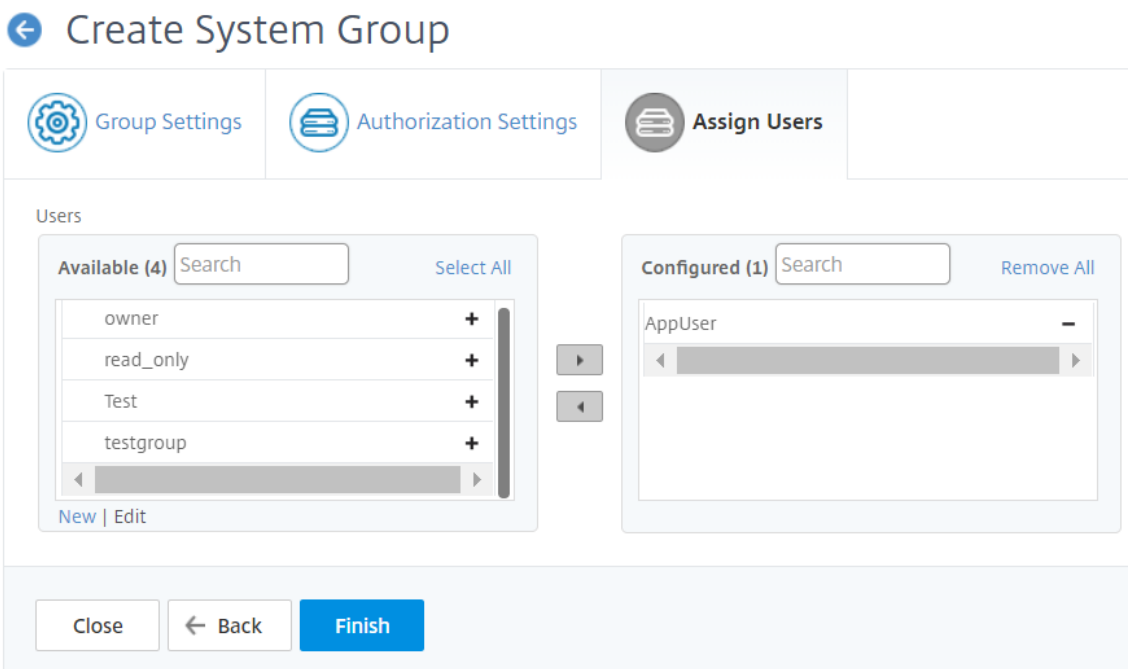
Si quiere seleccionar el nombre de dominio específico que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

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**.

9. Haga clic en **Crear grupo**.
10. En la sección **Asignar usuarios**, seleccione el usuario en la lista **Disponible** y agréguelo a la lista **Configurado** .

> **Nota**
>
> También puede agregar nuevos usuarios haciendo clic en **Nuevo**.



11. Haga clic en **Finalizar**.

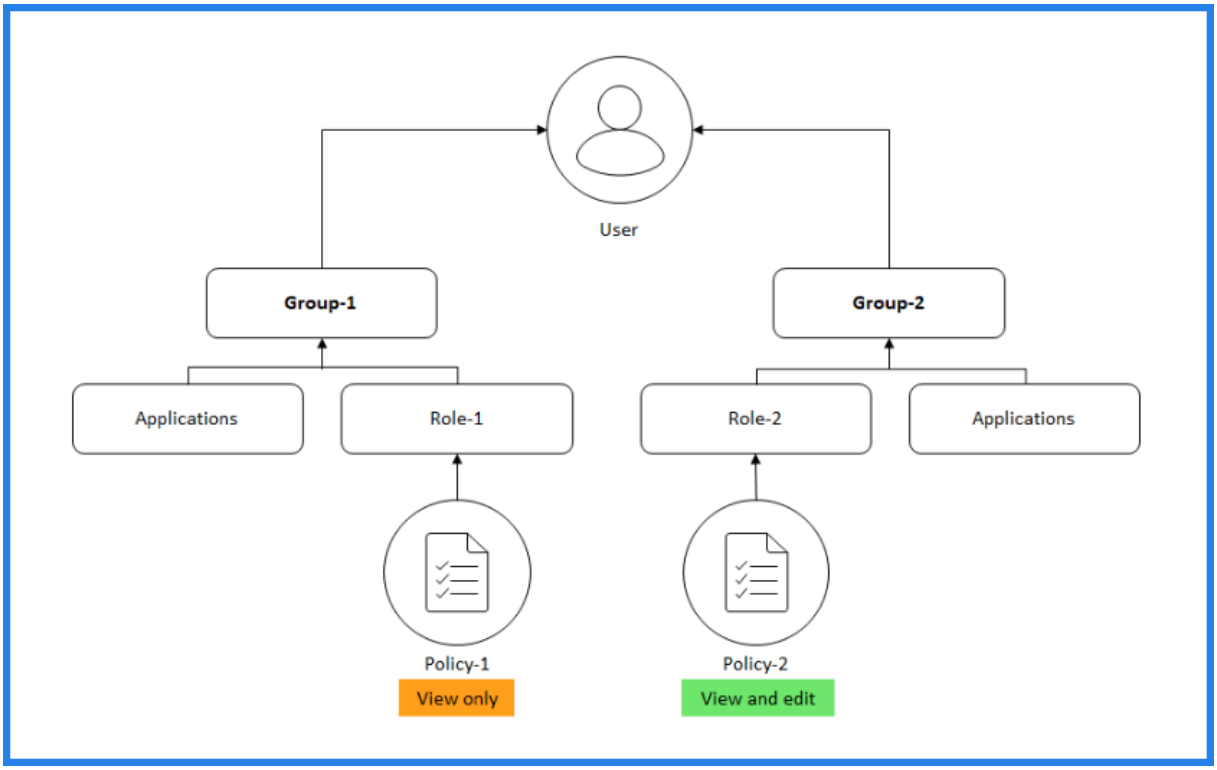
Cómo cambia el acceso de usuario en función del ámbito de autorización

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, el Citrix ADM concede al usuario acceso a las aplicaciones según el alcance de la autorización específica.

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

El RBAC no es totalmente compatible con las siguientes funciones de Citrix ADM:

- Análisis: los módulos de análisis no admiten completamente el 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 : el RBAC no es totalmente compatible con StyleBooks.
  - Considere una situación en la que varios usuarios tienen acceso a un único StyleBook pero tienen permisos de acceso para diferentes instancias de Citrix ADC. Los usuarios pueden crear y actualizar paquetes de configuración en sus propias instancias, pero no en otras, ya que no tienen acceso a esas instancias que no son las suyas. Pero todavía pueden ver los paquetes de configuración y los objetos creados en instancias de Citrix ADC que no sean las suyas.

Configurar los ajustes de Analytics

November 16, 2022

Antes de empezar a utilizar la función de análisis de Citrix ADM para obtener visibilidad de los datos de la instancia y la aplicación, 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, Citrix ADM genera un evento que significa una brecha de umbral.

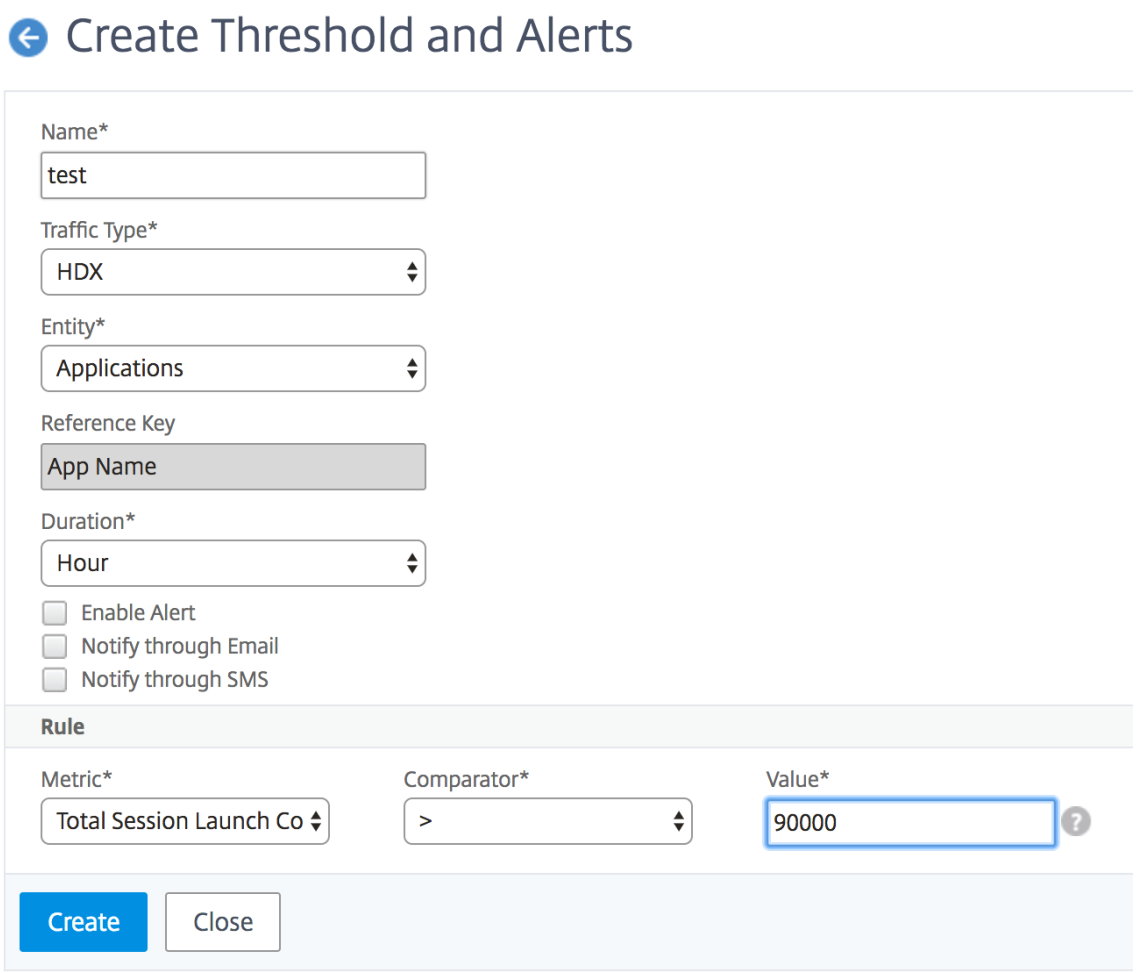
También puede asociar acciones con los umbrales establecidos. Las acciones incluyen mostrar una alerta en la GUI y enviar el correo electrónico tal como está configurado.

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

November 16, 2022

Puede seleccionar un tipo de notificación para recibir notificaciones para las siguientes funciones:

- **Eventos** : lista de eventos que se generan para las instancias de Citrix ADC. 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 Citrix ADM.
- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias Citrix ADC. Para obtener más información, consulte Caducidad del certificado SSL

Citrix ADM admite los siguientes tipos de notificaciones:

- Email

- SMS
- Slack
- PagerDuty
- ServiceNow

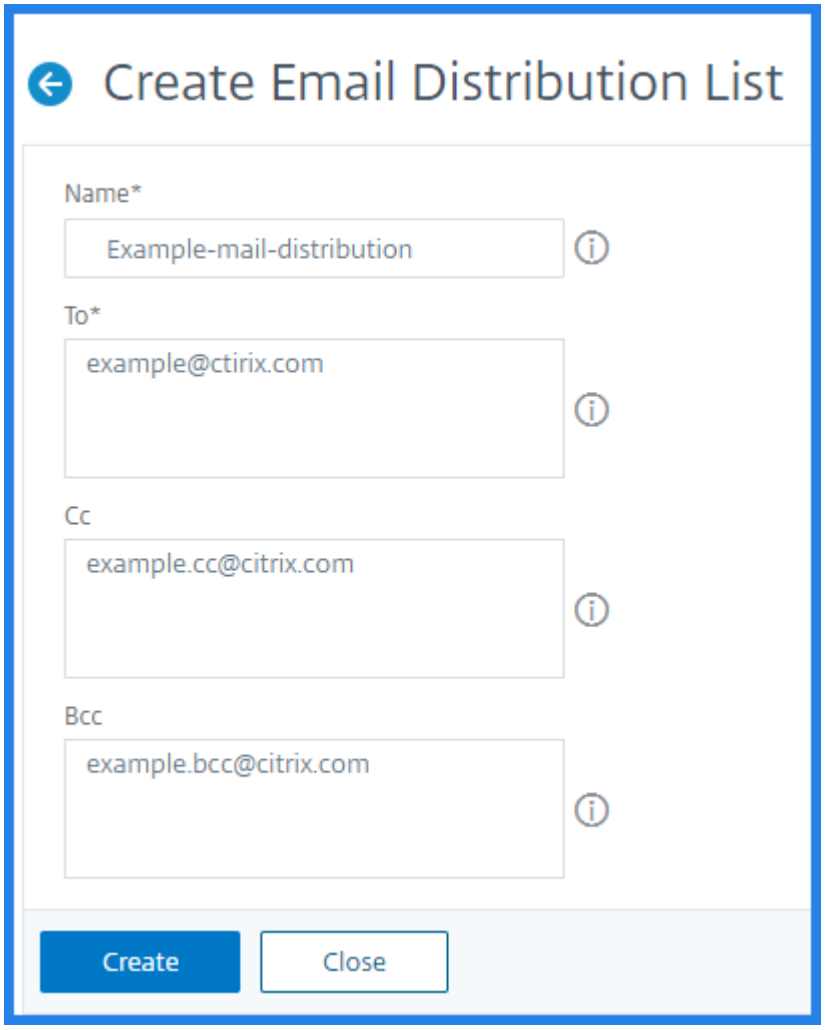
Para cada tipo de notificación, la GUI de Citrix ADM muestra la lista o el perfil de distribución configurados. El Citrix ADM envía notificaciones a la lista o perfil de distribución seleccionado.

Crea una lista de distribución de correo electrónico

Para recibir notificaciones por correo electrónico para las funciones de Citrix ADM, debe agregar un servidor de correo electrónico y una lista de distribución.

Realice los siguientes pasos para crear una lista de distribución de correo electrónico:

1. Vaya a **Configuración > Notificaciones**.
2. En **Correo electrónico**, haga clic en **Agregar**.
3. En **Crear lista de distribución de correo electrónico**, especifique los siguientes detalles:
    - **Nombre**: Especifique el nombre de la lista de distribución.
    - **Para** : especifique las direcciones de correo electrónico a las que Citrix ADM debe enviar los mensajes.
    - **Cc** : especifique las direcciones de correo electrónico a las que Citrix ADM debe enviar copias de los mensajes.
    - **Bcc** : especifique las direcciones de correo electrónico a las que Citrix ADM debe enviar copias de los mensajes sin mostrar las direcciones.



4. Haga clic en **Crear**.

Repita este procedimiento para crear varias listas de distribución de correo electrónico. La ficha **Correo electrónico** muestra todas las listas de distribución de correo electrónico presentes en Citrix ADM.

Crea una lista de distribución de SMS

Para recibir notificaciones por SMS para las funciones de Citrix ADM, debe agregar 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 Citrix ADM debe enviar los mensajes.

4. Haga clic en **Crear**.

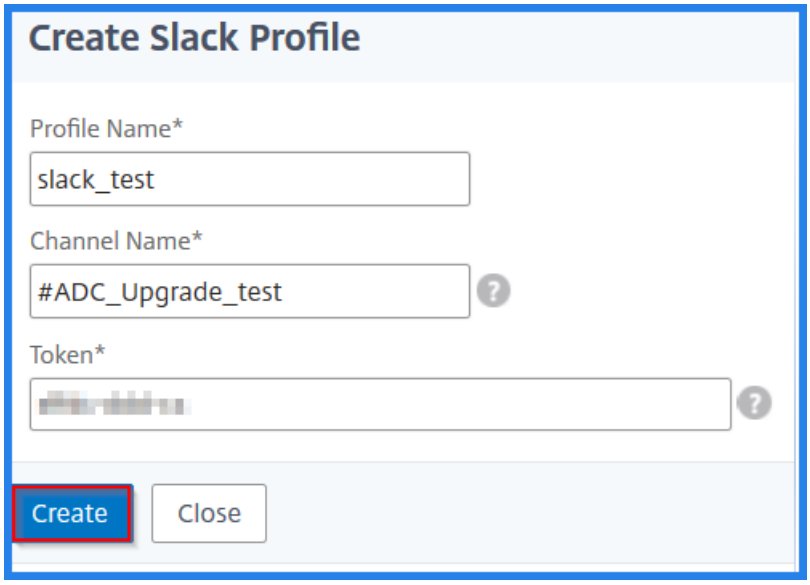
Repita este procedimiento para crear varias listas de distribución de SMS. La ficha **SMS** muestra todas las listas de distribución de SMS presentes en Citrix ADM.

Crear un perfil de Slack

Para recibir notificaciones de Slack sobre las funciones de Citrix ADM, debe 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 Citrix ADM debe enviar las notificaciones.
   - **URL del webhook** : especifique la URL del webhook del canal. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal. Además, todas las notificaciones de eventos se envían a esta URL se publican en el canal Slack designado. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. Haga clic en **Crear**.

Repite este procedimiento para crear varios perfiles de Slack. La ficha **Slack** muestra todos los perfiles de Slack presentes en Citrix ADM.

Crear un perfil de PagerDuty

Puede agregar un perfil de PagerDuty para supervisar las notificaciones de incidentes en función de las configuraciones de PagerDuty. PagerDuty le permite configurar notificaciones a través de correo electrónico, SMS, notificaciones push y llamadas telefónicas en un número registrado.

Antes de agregar un perfil de PagerDuty en Citrix ADM, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para empezar a usar PagerDuty, consulta la documentación de PagerDuty.

Realice los siguientes pasos para crear un perfil de PagerDuty:

1. Vaya a **Configuración > Notificaciones**.
2. En **PagerDuty**, haga clic en **Agregar**.
3. En **Crear perfil de PagerDuty**, especifique los siguientes detalles:
   - **Nombre de perfil** : especifique un nombre de perfil de su elección.
   - **Clave de integración** : especifique la clave de integración. Puede obtener esta clave en su portal PagerDuty.
4. Haga clic en **Crear**.

Para obtener más información, consulte Servicios e integraciones en la documentación de PagerDuty.

Repita este procedimiento para crear varios perfiles de PagerDuty. La ficha **PagerDuty** muestra todos los perfiles de PagerDuty presentes en Citrix ADM.

Ver el perfil de ServiceNow

Cuando quiera habilitar las notificaciones de ServiceNow para los eventos de Citrix ADC y los eventos de Citrix ADM, debe integrar Citrix ADM con el ServiceNow mediante el conector ITSM. Para obtener más información, consulte Integrar Citrix ADM con la instancia de ServiceNow.

Realice los siguientes pasos para ver y verificar el perfil ServiceNow:

1. Vaya a **Configuración > Notificaciones**.
2. En **ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.
3. Haga clic en **Probar** para generar automáticamente un tíquet de ServiceNow y verificar la configuración.

   Si quiere ver los tíquets de ServiceNow en la GUI de Citrix ADM, seleccione **Tíquets de ServiceNow**.

Exportar o programar informes de exportación

November 16, 2022

En Citrix ADM, puede exportar un informe completo para la función Citrix ADM seleccionada. Este informe proporciona una visión general de la asignación entre las instancias, las particiones y los detalles correspondientes.

Citrix ADM muestra los informes de exportación programados específicos de cada función en las funciones individuales de Citrix ADM, que puede ver, modificar o eliminar. Por ejemplo, para ver los informes de exportación de las instancias de Citrix ADC, vaya a **Infraestructura > Instancias > Citrix ADC** y haga clic en el icono de exportación. Puede exportar estos informes en formato PDF, JPEG, PNG y CSV.

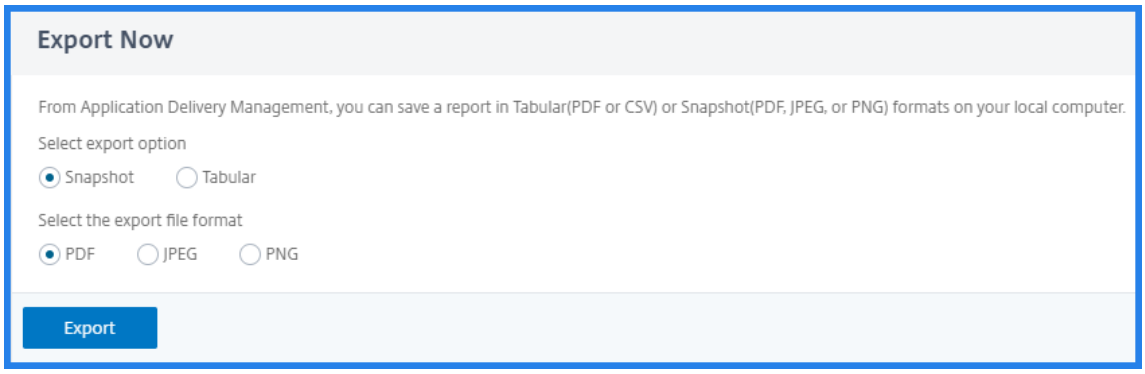
En **Exportar informes**, puede realizar las siguientes acciones:

- 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 desde Citrix ADM 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 Citrix ADM como una instantánea.
   - **Tabular** : esta opción exporta los informes de Citrix ADM en formato tabular. También puede elegir cuántos registros de datos exportar en formato tabular



4. Seleccione el formato de archivo que quiere guardar el informe en el equipo local.
5. Haga clic en **Exportar**.

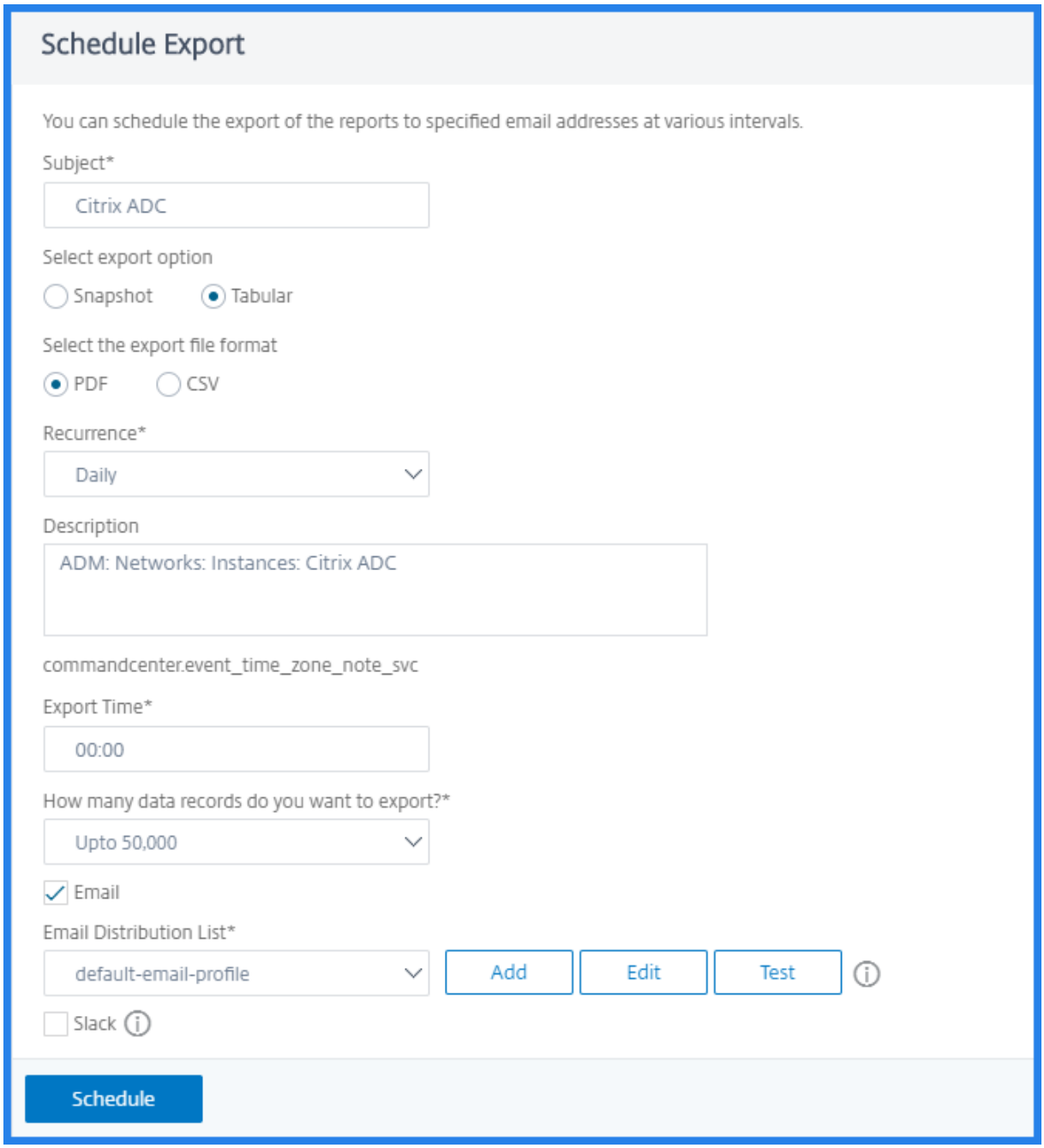
Programar informe de exportación

Para programar el informe de exportación a intervalos regulares, especifique el intervalo de recurrencia. Citrix ADM envía el informe exportado al perfil de correo electrónico o de Slack configurado.

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.
2. Seleccione **Programar exportación** y especifique lo siguiente:
   - **Asunto** : de forma predeterminada, este campo rellena automáticamente el nombre de la función seleccionada. Sin embargo, puede reescribirlo con un título significativo.
   - **Opción** de exportación: exporte los informes de Citrix ADM en formato instantáneo 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** : active la casilla de verificación y seleccione el perfil en el cuadro de lista. Si quiere agregar un perfil, haga clic en **Agregar**.

- **Slack** : selecciona 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

November 16, 2022

Puede administrar las instancias detectadas en Citrix ADM y configurar los ajustes de respaldo de la instancia.

Gestiona la configuración de la instancia

En **Administración de instancias**, puede modificar las siguientes configuraciones de instancias:

- **Comunicación con instancias** : puede elegir el canal de comunicación HTTP o HTTPS entre Citrix ADM y las instancias detectadas.
- **Habilitar la descarga de certificados** : le permite descargar los certificados SSL de una instancia detectada.
- **Solicitar credenciales para iniciar sesión en la instancia** : cuando accede a la instancia a través de la GUI de Citrix ADM, aparece la página de inicio de sesión de la instancia Especifica tus credenciales de inicio de sesión para acceder a una instancia.

Configurar las opciones de copia de seguridad de instancia

En **Instance Backup Settings**, puede configurar los ajustes de copia de seguridad para las instancias de ADC detectadas en Citrix ADM.

En **Configurar los ajustes de copia de seguridad**de la **instancia, seleccione Habilitar las copias**

- **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 copia de seguridad en Citrix ADM 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 el formato `hours:minutes` en el que quiere que Citrix ADM realice la copia de seguridad de la instancia.

- **Configuración de Citrix ADC** : con esta opción, puede iniciar una copia de seguridad en función de la captura e incluir archivos de GeoDB con 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 se reciba la captura de NetScalerConfigSave** : de forma predeterminada, Citrix ADM no crea un archivo de respaldo cuando recibe la captura «NetScalerConfigSave». Sin embargo, puede habilitar la opción de crear un archivo de respaldo cada vez que una instancia de Citrix ADC envíe una captura `NetScalerConfigSave` a Citrix ADM.

    Se envía una instancia de Citrix ADC `NetScalerConfigSave` cada vez que se guarda la configuración de la instancia.

    Especifique el **retraso de Backup on trap** en minutos. Si la captura `NetScalerConfigSave` recibida persiste durante los minutos especificados en Citrix ADM, Citrix ADM realiza una copia de seguridad de la instancia.
  - **Incluir archivos de GeoDB** : de forma predeterminada, Citrix ADM no realiza copias de seguridad de los archivos de la GeoDatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.
- **Configuración de Citrix SDX** : para hacer una copia de seguridad de las instancias SDX, especifique el **tiempo de espera de la copia** de seguridad Durante una copia de seguridad de una instancia de SDX, la conexión entre Citrix ADM y SDX se mantiene durante el período especificado.

  Si el tamaño del archivo de copia de seguridad de la instancia SDX es grande, es posible que quiera mantener la conexión entre Citrix ADM y la instancia SDX durante un período más largo para completar la copia de seguridad de la instancia SDX.

  > **Importante**
  >
  > La copia de seguridad falla si la conexión se agota.

- **Transferencia externa** : Citrix ADM le permite transferir los archivos de respaldo de la instancia de Citrix ADC 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

November 16, 2022

Puede administrar las instancias detectadas en Citrix ADM y configurar los ajustes de respaldo de la instancia.

Gestiona la configuración de la instancia

En **Administración de instancias**, puede modificar las siguientes configuraciones de instancias:

- **Comunicación con instancias** : puede elegir el canal de comunicación HTTP o HTTPS entre Citrix ADM y las instancias detectadas.
- **Habilitar la descarga de certificados** : le permite descargar los certificados SSL de una instancia detectada.
- **Solicitar credenciales para iniciar sesión en la instancia** : cuando accede a la instancia a través de la GUI de Citrix ADM, aparece la página de inicio de sesión de la instancia Especifica tus credenciales de inicio de sesión para acceder a una instancia.

Configurar las opciones de copia de seguridad de instancia

En **Instance Backup Settings**, puede configurar los ajustes de copia de seguridad para las instancias de ADC detectadas en Citrix ADM.

En **Configurar los ajustes de copia de seguridad**de la **instancia, seleccione Habilitar las copias**

- **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 copia de seguridad en Citrix ADM 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 el formato `hours:minutes` en el que quiere que Citrix ADM realice la copia de seguridad de la instancia.
- **Configuración de Citrix ADC** : con esta opción, puede iniciar una copia de seguridad en función de la captura e incluir archivos de GeoDB con 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 se reciba la captura de NetScalerConfigSave** : de forma predeterminada, Citrix ADM no crea un archivo de respaldo cuando recibe la captura «NetScalerConfigSave». Sin embargo, puede habilitar

la opción de crear un archivo de respaldo cada vez que una instancia de Citrix ADC envíe una captura `NetScalerConfigSave` a Citrix ADM.

Se envía una instancia de Citrix ADC `NetScalerConfigSave` cada vez que se guarda la configuración de la instancia.

Especifique el **retraso de Backup on trap** en minutos. Si la captura `NetScalerConfigSave` recibida persiste durante los minutos especificados en Citrix ADM, Citrix ADM realiza una copia de seguridad de la instancia.

- **Incluir archivos de GeoDB** : de forma predeterminada, Citrix ADM no realiza copias de seguridad de los archivos de la GeoDatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.

- **Configuración de Citrix SDX** : para hacer una copia de seguridad de las instancias SDX, especifique el **tiempo de espera de la copia** de seguridad Durante una copia de seguridad de una instancia de SDX, la conexión entre Citrix ADM y SDX se mantiene durante el período especificado.

  Si el tamaño del archivo de copia de seguridad de la instancia SDX es grande, es posible que quiera mantener la conexión entre Citrix ADM y la instancia SDX durante un período más largo para completar la copia de seguridad de la instancia SDX.

  > **Importante**
  >
  > La copia de seguridad falla si la conexión se agota.

- **Transferencia externa** : Citrix ADM le permite transferir los archivos de respaldo de la instancia de Citrix ADC 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

November 16, 2022

Puede modificar el intervalo de mantenimiento activo del agente Citrix ADM y la zona horaria del servidor Citrix ADM.

Establecer el intervalo de mantenimiento-vivo del agente

El servidor y el agente de Citrix ADM mantienen la misma conexión TCP para el intervalo keep-alive especificado. Un agente usa esta conexión para enviar los datos de las instancias administradas al servidor Citrix ADM.

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**.

Establecer la zona horaria de Citrix ADM

Puede elegir la zona horaria en la que quiere mostrar la hora en la página web, las notificaciones y los informes de Citrix ADM.

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 Citrix ADM.
4. Haga clic en **Guardar**.

suscripciones por correo electrónico

November 16, 2022

Citrix ADM envía notificaciones por correo electrónico a todos los usuarios nuevos e inactivos.

Los clientes inactivos reciben una notificación por correo electrónico si:

- Las instancias ADC no están configuradas
- La licencia de inquilino vence en menos de 30 días

> **Nota:**
>
> De forma predeterminada, todos los clientes inactivos reciben una notificación por correo electrónico.

Los nuevos clientes de ADM reciben un correo electrónico de Citrix ADM en el que se les invita a incorporar las instancias de ADC al servicio ADM, donde pueden administrar y supervisar los eventos críticos en las instancias de ADC, solucionar problemas y automatizar tareas como la configuración de ADC.

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

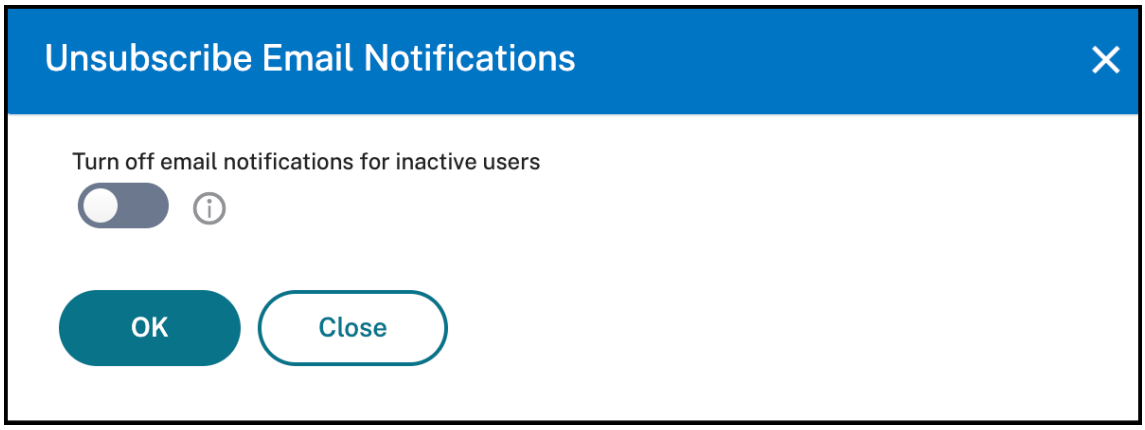
- Get bird's eye visibility into entire ADC infra and debug critical issues on your ADC instances.
- Manage the complete SSL cert lifecyle using Citrix ADM.
- Always stay on top of critical events with Citrix ADM ServiceNow integration.

Join ADM community

Notificaciones por correo electrónico de cancelación

Puede suscribirse o darse de baja de las notificaciones por correo electrónico que recibe del Servicio ADM. Para **cancelar la suscripción a las notificaciones por correo electrónico**:

1. En Citrix Application Delivery and Management, vaya a **Configuración > Configuración global > Configuraciones del sistema**y, después, haga clic en **Suscripciones por correo** 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 a las instancias de Onboard ADC.

Habilite o inhabilite las funciones

November 16, 2022

Como administrador, puede habilitar o deshabilitar 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, Citrix ADM redistribuye las instancias de ADC del agente inactivo con otros agentes activos. Para obtener más información, consulte Configurar los agentes Citrix ADM para la implementación en varios sitios.

- **Función de red de sondeo** de entidad: Una entidad es una directiva, un servidor virtual, un servicio o una acción asociada a una instancia de ADC. De forma predeterminada, Citrix ADM sondea automáticamente las entidades de función de red configuradas cada 60 minutos. Para obtener más información, consulte Descripción general de sondeos.
- **Copia de seguridad de instancia: Realice** una copia de seguridad del estado actual de una instancia de Citrix ADC y, posteriormente, utilice los archivos de copia de seguridad para restaurar la instancia de ADC al mismo estado. Para obtener más información, consulte Realizar copias de seguridad y restaurar instancias de Citrix ADC.
- **Auditoría de configuración de instancias**: Supervise los cambios de configuración en las instancias administradas de Citrix ADC, 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 Citrix ADC administrada. Los eventos recibidos en Citrix ADM 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**: Citrix ADM proporciona una vista centralizada de los certificados SSL instalados en todas las instancias administradas de Citrix ADC. Para obtener más información, consulte Panel de control SSL.
- **Syslog de instancias**: Puede supervisar los eventos syslog generados en sus instancias Citrix ADC si ha configurado el dispositivo para redirigir todos los mensajes syslog a Citrix ADM. 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 inhabilitada, el usuario no puede realizar las operaciones asociadas a esa función.

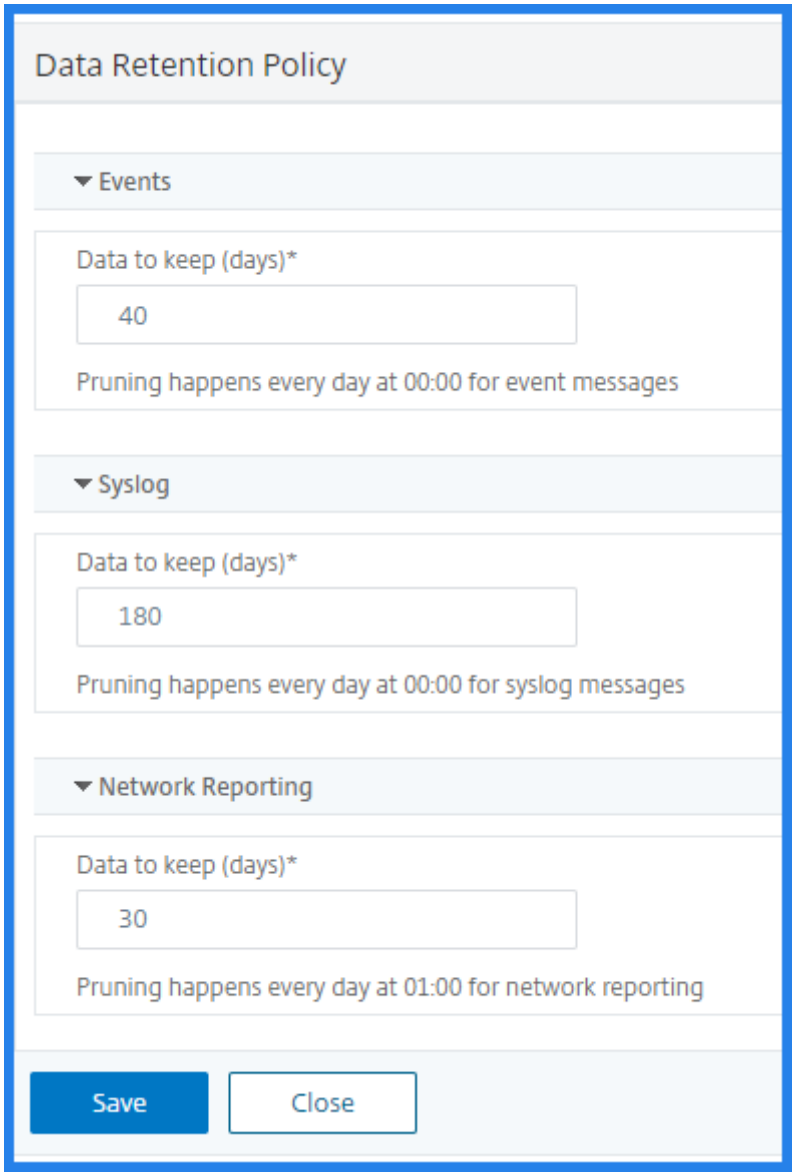
Directiva de retención de datos

November 16, 2022

Puede acceder a los eventos del sistema, a los mensajes de syslog y a los datos de informes de red durante un período específico en Citrix ADM.

1. Vaya a **Configuración > Configuración global > Directiva de retención de datos** para configurar la retención de datos.
2. Haga clic en el botón de edición.
3. Especifique los días para las siguientes opciones para conservar los datos en Citrix ADM:

Opciones	Descripción
Eventos	Le permite limitar los mensajes de eventos almacenados en Citrix ADM hasta 40 días. Los eventos se eliminan de Citrix ADM una vez caducada la directiva de retención. Los eventos borrados se eliminan después de un día. Para obtener más información, consulte Eventos.
Syslog	Le permite limitar la cantidad de datos de syslog almacenados en la base de datos hasta 180 días. Para obtener más información, consulta Configurar syslog en las instancias.
Informes de red	Le permite limitar los datos de informes de red almacenados en Citrix ADM hasta 30 días. Para obtener más información, consulte Informes de red.



Importante

No puede modificar la directiva de retención de datos con una cuenta Express.

Cuando su cuenta se convierte en una cuenta Express, Citrix ADM conserva los datos de almacenamiento de hasta 500 MB o datos de un día, lo que sea menor. Para obtener más información, consulte Administrar los recursos de Citrix ADM mediante una cuenta Express.

Configurar una directiva de acción para recibir notificaciones de eventos de la aplicación

December 12, 2022

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:
  - **Todas las infracciones de seguridad**
    - **Todas las infracciones de bots**

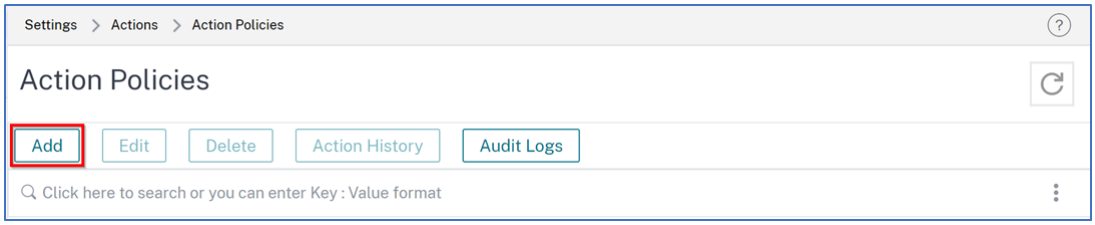
      (Para obtener más información sobre la lista de infracciones de bots, consulta las categorías de infracciones).
    - **Todas las infracciones de WAF**
      - **Infracciones de SQL de WAF**
      - **Infracciones de WAF XSS**
      - **WAF deduce infracciones de XML**
  - **Todas las infracciones de seguridad por cliente**
    - **Infracciones de bots por cliente**
    - **Infracciones de WAF por cliente**

      > **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.
  - **Infracción de la puntuación**
  - **Latencia de red del cliente**
  - **Latencia de red del servidor**

- **Tiempo de procesamiento del servidor**
- **Infracción del gráfico de**

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

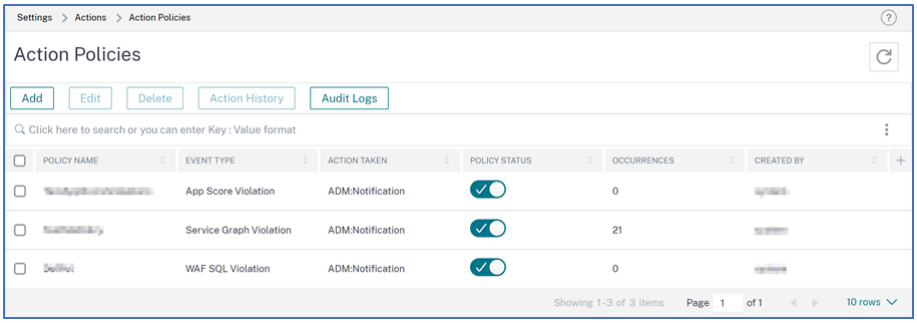
e) **A continuación, haga lo siguiente** : seleccione **Notificar**. Tras seleccionar **Notificar**, aparece la opción Tipo de notificación.

f) **Tipo de notificación** : selecciona 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 ADC. Seleccione la dirección IP de la lista.

Nombre de la infracción	Condición	Descripción
	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 bots	Perfil de bot	El nombre del perfil del bot que se utiliza para configurar la administración de bots en la instancia ADC.
	IP de instancia	Dirección IP de la instancia ADC. 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 WAF, infracción de SQL de WAF, infracción de WAF XSS, infracción de WAF Infer XML	Perfil WAF	El nombre del perfil WAF que se utiliza para configurar los ajustes de seguridad de WAF en la instancia ADC.
	IP de instancia	Dirección IP de la instancia ADC. 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.

Nombre de la infracción	Condición	Descripción
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 ADC.
	IP de instancia	Dirección IP de la instancia ADC. 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 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 ADC.
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 ADC.

Nombre de la infracción	Condición	Descripción
	IP de instancia	Dirección IP de la instancia ADC. 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	Selecciona 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 ADC.
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 ADC.
	IP de instancia	Dirección IP de la instancia ADC. Seleccione la dirección IP de la lista.
	Client IP	La fuente de donde se origina el Bot. Especifique la dirección IP.

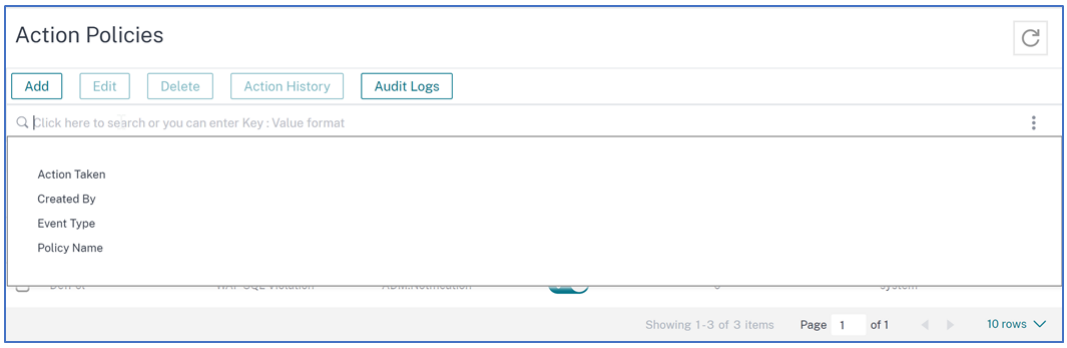
Nombre de la infracción	Condición	Descripción
	Ataques totales	El total de ataques de los que quiere recibir una notificación.
	Tipo de infracción	Seleccione la infracción del WAF de la lista.
	Request URL	La URL que quiere configurar para bloquear. Especifique la URL.
	Nombre de vserver	Las aplicaciones 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 ADC.
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.
	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 infracción	Condición	Descripción
	Nombre de la aplicación	Seleccione la aplicación a la que quiere que se le notifique la infracción de puntuación de la aplicación. Si no agrega esta condición, se tendrán en cuenta todas las aplicaciones de la instancia ADC.
Latencia de red cliente	Latencia de red del cliente (milisegundos)	Especifique el valor de latencia del cliente (de cliente a ADC) en milisegundos para el que quiere recibir una notificación.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Latencia de la red	Latencia de red del servidor (milisegundos)	Especifique el valor de latencia del servidor (de servidor a ADC) en milisegundos para el que quiere recibir una notificación.
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Tiempo de procesamiento del servidor	Tiempo de procesamiento del servidor (milisegundos)	Especifique el valor de procesamiento del servidor (de servidor a ADC) en milisegundos para el que quiere recibir una notificación.

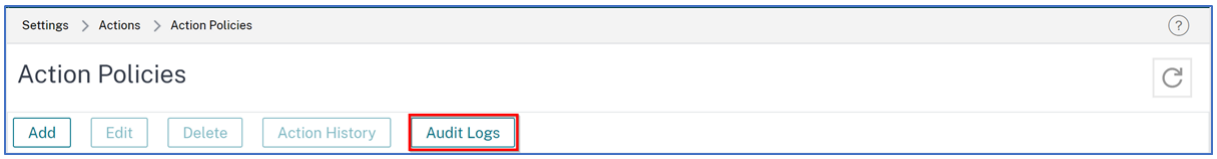
Nombre de la infracción	Condición	Descripción
	Nombre de la aplicación	Haga clic en **Seleccionar aplicaciones** para seleccionar las aplicaciones a las que quiere que se notifique la infracción.
Infracción del gráfico de		Microservicios que infringen los umbrales configurados. Para obtener más información, consulte Configurar umbrales en el gráfico de servicios.

Usa la barra de búsqueda

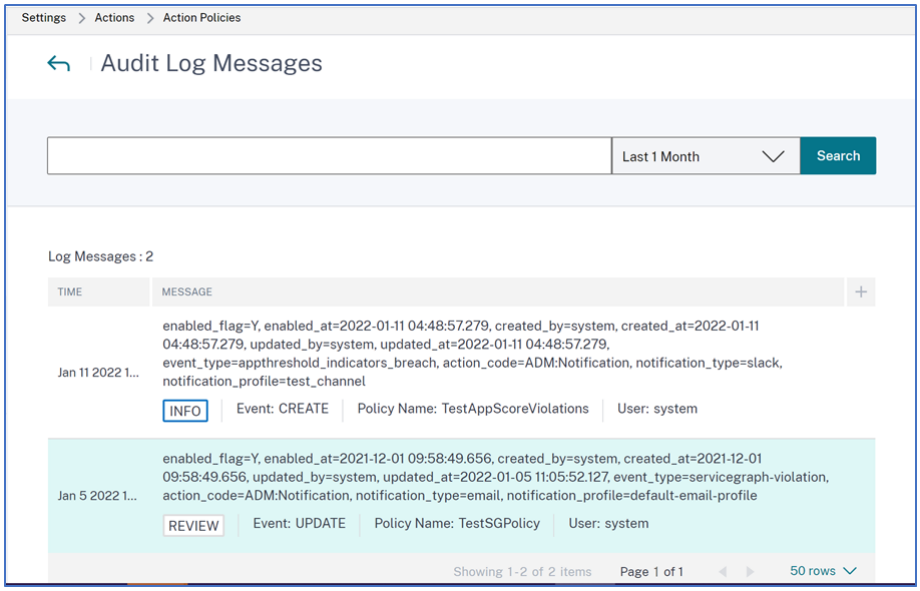
La barra de búsqueda permite filtrar los resultados. Al hacer clic en la barra de búsqueda, aparece una lista de sugerencias de búsqueda. Puede seleccionar el componente y filtrar los resultados según sus requisitos.



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 la duración seleccionada.



Utilice los registros de auditoría para administrar y monitorear su infraestructura

November 16, 2022

Puede usar Citrix ADM para realizar un seguimiento de todos los eventos de Citrix ADM y syslog generados en las instancias de Citrix ADM ADC. Estos mensajes pueden ayudarlo a administrar y monitorear su infraestructura. Sin embargo, los mensajes de registro son una excelente fuente de información solo si los revisa, y Citrix ADM simplifica la forma de revisar los mensajes de registro.

Puede usar filtros para buscar mensajes de registro de auditoría y syslog de Citrix ADM. Los filtros ayudan a acotar los resultados y a encontrar exactamente lo que busca en tiempo real. La Ayuda de búsqueda integrada le guía para filtrar los registros. Otra forma de ver los mensajes de registro es exportarlos en formato PDF, CSV, PNG y JPEG. Puede programar la exportación de estos informes a direcciones de correo electrónico especificadas en distintos intervalos.

Puede revisar los siguientes tipos de mensajes de registro en la GUI de Citrix ADM:

- Registros de auditoría relacionados con instancias de ADC
- Registros de auditoría relacionados con Citrix ADM
- Registros de auditoría de aplicaciones

Registros de auditoría relacionados con instancias de ADC

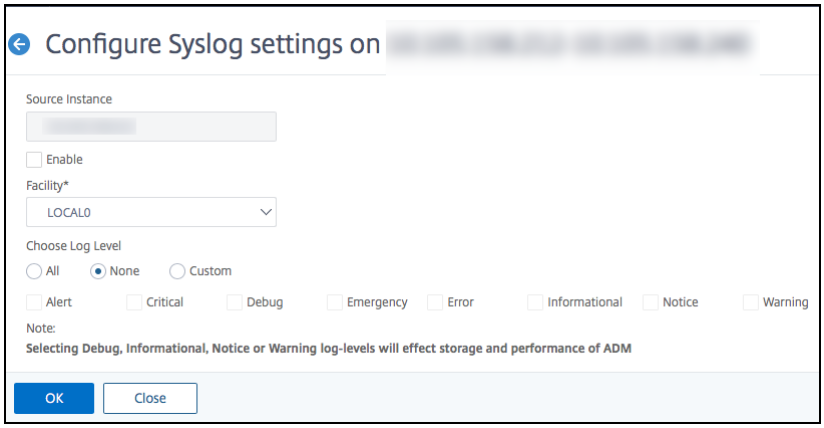
Antes de poder ver los mensajes de syslog relacionados con la instancia de ADC de Citrix ADM, configure Citrix ADM como servidor de syslog para su instancia de Citrix ADC. Una vez completada la config-

uración, todos los mensajes de syslog se redirigen desde la instancia a Citrix ADM.

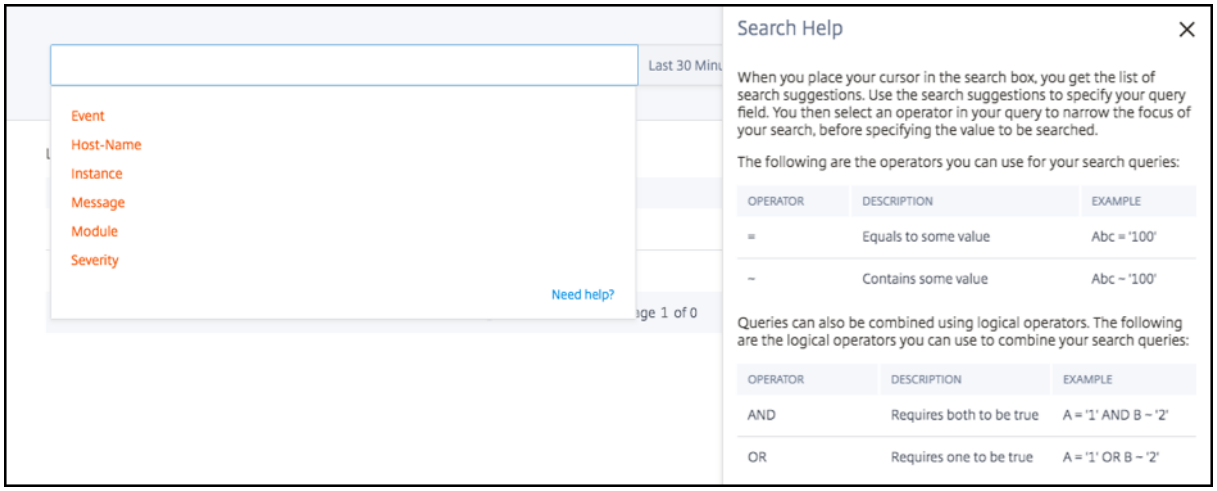
Configurar Citrix ADM como servidor syslog

Siga estos pasos para configurar Citrix ADM como servidor syslog:

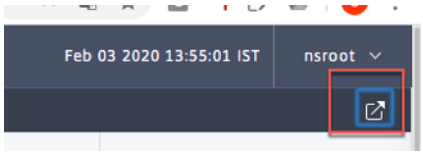
1. Desde la GUI de Citrix ADM, vaya a **Infraestructura > Instancias**.
2. Seleccione la instancia de Citrix ADC desde la que quiere que se recopilen y muestren los mensajes syslog en Citrix ADM.
3. En la lista **Seleccionar acción**, seleccione **Configurar Syslog**.
4. Haga clic en **Activar**.
5. En la lista desplegable de **instalaciones**, seleccione una instalación local o a nivel de usuario.
6. Seleccione el nivel de registro requerido para los mensajes de syslog.
7. Haga clic en **Aceptar**.



Estos pasos configuran todos los comandos syslog en la instancia de Citrix ADC y Citrix ADM comienza a recibir los mensajes syslog. Para ver los mensajes, vaya a **Infraestructura > Eventos > Mensajes de Syslog**. Haga clic en **¿Necesita ayuda?** para abrir la ayuda de búsqueda integrada. Para obtener más información, consulte Ver y exportar mensajes de syslog.



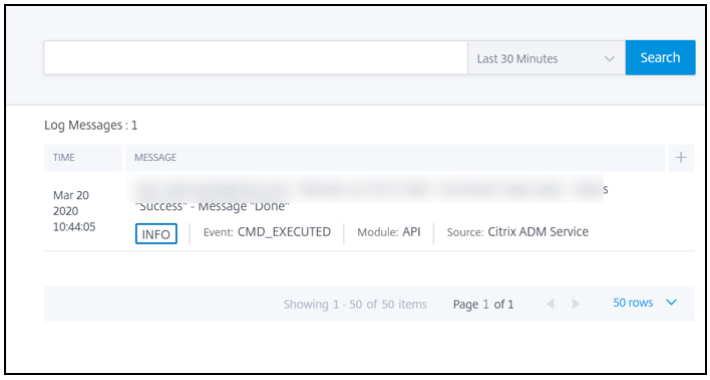
Para exportar los mensajes de registro, haga clic en el icono de flecha de la esquina superior derecha.



A continuación, haga clic en **Exportar ahora** o **Planificar exportación**. Para obtener más información, consulte Exportar mensajes de syslog.

Registros de auditoría relacionados con Citrix ADM

Basándose en reglas preconfiguradas, Citrix ADM genera mensajes de registro de auditoría para todos los eventos de, lo que le ayuda a supervisar el estado de su infraestructura. Para ver todos los mensajes del registro de auditoría presentes en Citrix ADM, vaya a **Configuración -> Mensajes de registro de auditoría**.

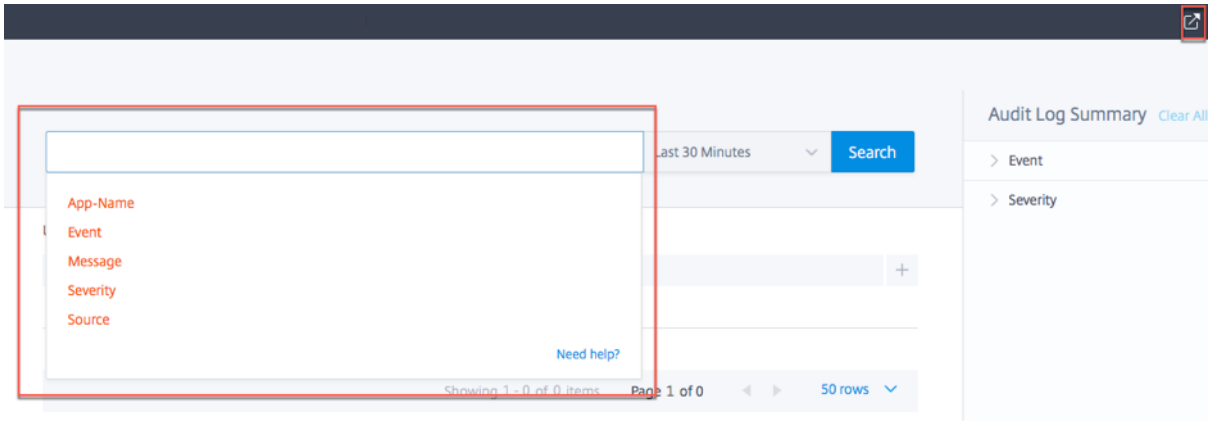


Para exportar los mensajes de registro, haga clic en el icono de flecha de la esquina superior derecha.

Registros de auditoría relacionados con aplicaciones

Puede ver los mensajes del registro de auditoría de todas las aplicaciones Citrix ADM o de una aplicación específica.

- Para ver todos los mensajes de registro de auditoría de todas las aplicaciones presentes en Citrix ADM, vaya a **Infraestructura > Funciones de red > Auditoría**.



- Para ver los mensajes del registro de auditoría de cualquier aplicación específica en Citrix ADM, vaya a **Aplicaciones > Panel de control > haga doble clic en el servidor virtual > Registro de auditoría**.

> Nota:
>
> Puede reenviar los mensajes del registro de auditoría de Citrix ADM a un servidor externo. Para obtener más información, consulte Ver información de auditoría.

Configurar la administración de direcciones IP (IPAM)

November 16, 2022

Citrix ADM IPAM le permite asignar y liberar automáticamente direcciones IP en las configuraciones administradas de Citrix ADM. Puede asignar direcciones IP desde redes o rangos de IP definidos mediante los siguientes proveedores de IP:

- Proveedor de IPAM integrado de Citrix ADM.
- Solución IPAM de Infoblox. Para obtener más información, consulte DDI de Infoblox.

Actualmente, puede usar Citrix ADM IPAM en:

- **StyleBooks**: asigna automáticamente las IP a los servidores virtuales al crear configuraciones.
- **Entrada de Kubernetes**: Asignar automáticamente una dirección IP virtual a una configuración de Ingress en un clúster de Kubernetes.
- Puerta de**enlace de API**: Asigne automáticamente una dirección IP al proxy de API.

También puede realizar un seguimiento de las direcciones IP asignadas y disponibles en cada red o rango de IP administrado por Citrix ADM.

Agregar un proveedor de direcciones IP externo

Citrix ADM tiene un proveedor de IPAM integrado para administrar las IP y los rangos de IP. También puede agregar un proveedor de direcciones IP externo a Citrix ADM.

> **Importante**
>
> Antes de empezar, asegúrese de que los siguientes permisos estén habilitados en el proveedor de direcciones IP externo:
>
> - Capacidad para consultar redes que están presentes en el proveedor.
> - Registrar una nueva red.
> - Anule el registro de una red existente.
> - 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 IP externo en Citrix ADM:

1. Vaya a **Configuración > IPAM**.
2. En **Proveedores**, haga clic en **Agregar**.
3. Especifique los siguientes detalles para agregar un proveedor de IP:
   - **Nombre** : especifique el nombre del proveedor de IP que se utilizará en Citrix ADM.
   - **Proveedor**: Seleccione un proveedor IPAM de la lista.
   - **URL** : especifique la URL de la solución de IPAM que asigna direcciones IP en un entorno Citrix ADM. Asegúrese de especificar la dirección URL en el siguiente formato:

     ```
     https://<host name>
     <!--NeedCopy-->
     ```

     Ejemplo:`https://myinfoblox.example.com`
   - **Nombre de usuario** : especifique el nombre de usuario para iniciar sesión en la solución IPAM.
   - **Contraseña** : especifique la contraseña para iniciar sesión en la solución IPAM.
4. Haga clic en **Agregar**.

Agregar una red

Agregue una red para usar IPAM con las configuraciones administradas de Citrix ADM.

1. Vaya a **Configuración > IPAM**.

2. En **Redes*, haga clic en **Agregar**.
3. Especifique los siguientes detalles:
   - **Nombre de red** : especifique el nombre de la red para identificar la red en Citrix ADM.
   - **Proveedor** : seleccione el proveedor de la lista.

     En esta lista se muestran los proveedores agregados a Citrix ADM.
   - **Tipo de red** : seleccione el **rango de IP** o **CIDR** de la lista según sus requisitos.
   - **Valor de red** : especifique el valor de la red.

     > **Nota:**
     >
     > Citrix ADM IPAM solo admite direcciones IPv4.

     Para el **intervalo de IP**, especifique el valor de red en el siguiente formato:

     ```
     <first-IP-address>-<last-IP-address>
     <!--NeedCopy-->
     ```

     Ejemplo:

     ```
     10.0.0.20-10.0.0.100
     <!--NeedCopy-->
     ```

     Para **CIDR**, especifique el valor de la red en el siguiente formato:

     ```
     <IP-address>/<subnet-mask>
     <!--NeedCopy-->
     ```

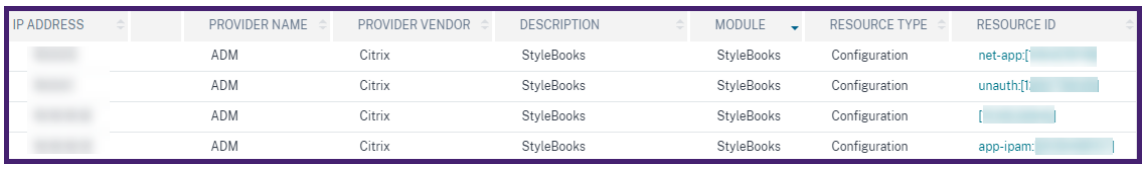
     Ejemplo:

     ```
     10.70.124.0/24
     <!--NeedCopy-->
     ```
4. Haga clic en **Crear**.

Ver direcciones IP asignadas

Para ver más detalles acerca de las direcciones IP asignadas desde la red IPAM, siga estos pasos:

1. Vaya a **Configuración > IPAM**.
2. En la ficha **Redes**, haga clic en **Ver todas las IP asignadas**.



IP ADDRESS		PROVIDER NAME	PROVIDER VENDOR	DESCRIPTION	MODULE	RESOURCE TYPE	RESOURCE ID
		ADM	Citrix	StyleBooks	StyleBooks	Configuration	net-app:[
		ADM	Citrix	StyleBooks	StyleBooks	Configuration	unauth:[1
		ADM	Citrix	StyleBooks	StyleBooks	Configuration	[
		ADM	Citrix	StyleBooks	StyleBooks	Configuration	app-ipam:

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 Citrix ADM que reservó la dirección IP. Por ejemplo, si StyleBooks reservó la dirección IP, esta columna muestra StyleBooks como módulo.
- **Tipo de Recurso**: Muestra el tipo de recurso de ese módulo. Para el módulo StyleBooks, solo el tipo de recurso de configuraciones utiliza la red IPAM. Por lo tanto, muestra Configuraciones bajo esta columna.
- **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 quiere liberar y haga clic en **Liberar IP asignadas**.

Artículos de procedimientos

December 2, 2022

Los «artículos prácticos» de Citrix ADM son artículos simples, relevantes y fáciles de implementar sobre las funciones disponibles con el servicio. Estos artículos contienen información sobre algunas de las funciones populares de Citrix ADM, como la administración de instancias, la administración de configuración, la administración de eventos, la administración de aplicaciones, los 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 Citrix ADC

Cómo agregar instancias a Citrix ADM

Cómo crear grupos de instancias en Citrix ADM

Cómo sondear instancias y entidades de Citrix ADC en Citrix ADM

Cómo configurar sitios para Geomaps en Citrix ADM

Cómo forzar una conmutación por error a la instancia secundaria de Citrix ADC

Cómo forzar que una instancia secundaria de Citrix ADC permanezca secundaria

Cómo cambiar una contraseña raíz de Citrix ADC MPX o VPX

Cómo cambiar una contraseña raíz de Citrix ADC SDX

Administración de la configuración

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

Cómo actualizar instancias de Citrix ADC SDX mediante Citrix ADM

Cómo programar los trabajos creados mediante plantillas integradas en Citrix ADM

Cómo reprogramar trabajos configurados mediante plantillas integradas en Citrix ADM

Reutilizar trabajos de configuración de ejecución

Cómo actualizar instancias de Citrix ADC con Citrix ADM

Cómo crear un trabajo de configuración en Citrix ADM

Cómo usar variables en trabajos de configuración en Citrix ADM

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

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

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

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

Cómo utilizar la plantilla de configuración maestra en Citrix ADM

Administración de certificados

Cómo configurar una directiva empresarial en Citrix ADM

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

Cómo actualizar un certificado instalado desde Citrix ADM

Cómo vincular y desvincular certificados SSL mediante Citrix ADM

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

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

Cómo utilizar el panel SSL en Citrix ADM

StyleBooks

Cómo usar los StyleBooks predeterminados en Citrix ADM

Cómo crear sus propios StyleBooks

Cómo usar StyleBooks definidos por el usuario en Citrix ADM

Cómo usar la API para crear configuraciones a partir de StyleBooks

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

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

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 configurar la edad de los eventos en Citrix ADM

Cómo programar un filtro de eventos mediante Citrix ADM

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

Cómo suprimir eventos mediante Citrix ADM

Cómo utilizar el panel de eventos para supervisar eventos

Cómo crear reglas de eventos en Citrix ADM

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

Cómo ver el resumen de eventos en Citrix ADM

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

Cómo exportar mensajes syslog mediante Citrix ADM

Cómo suprimir mensajes de Syslog en Citrix ADM

Preguntas frecuentes

February 27, 2023

¿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 Citrix ADM admite 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 su agente está instalado en un hipervisor o en la nube de Microsoft Azure, las credenciales de inicio de sesión predeterminadas del agente Citrix ADM son `nsrecover`/`nsroot`las que abren la línea de comandos del agente.

Si su agente está instalado en AWS, las credenciales predeterminadas para iniciar sesión en el agente Citrix ADM 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 utiliza como intermediario entre Citrix ADM y las instancias del centro de datos de la empresa o en 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 Citrix ADM y vaya a 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 agentes a Citrix ADM mediante un servidor proxy?

Puede conectar los agentes a Citrix ADM 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 Citrix ADM 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 Citrix ADM 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 del usuario antes de reenviarlos a Citrix ADM.

Para obtener más información, consulte Citrix ADM como servidor proxy de API.

> **Nota:**
>
> Citrix ADM admite servidores proxy con la autenticación básica habilitada. Citrix ADM 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 Citrix ADC son compatibles con Citrix ADM?

Para las funciones de administración y supervisión, se admiten las instancias de Citrix ADC que ejecutan la versión 10.5 y versiones posteriores. Algunas funciones solo son compatibles con determinadas versiones de Citrix ADC. Para obtener más información, consulte Requisitos del sistema.

¿Cómo exporto informes de panel en Citrix ADM?

Para exportar el informe de cualquier panel de Citrix ADM, 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.
   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 especificar todos los días que quiere programar 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, Citrix ADM captura las métricas del tiempo de carga y el tiempo de renderización de las páginas HTML mediante la inyección de HTML Mediante estas métricas, los administradores pueden identificar problemas de latencia L7.

