Citrix Analytics

Machine translated content

Disclaimer

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

Contents

Novedades

September 21, 2023

Un objetivo de Citrix es ofrecer nuevas funciones y actualizaciones de productos a los clientes de Citrix Analytics cuando estén disponibles. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar.

Para usted, como cliente, este proceso es transparente. Las actualizaciones iniciales solo se aplican en los sitios internos de Citrix; luego se aplican gradualmente en los entornos de los clientes. La entrega de actualizaciones incrementalmente en ondas ayuda a garantizar la calidad del producto y a maximizar la disponibilidad.

Citrix Analytics tiene los siguientes productos u ofertas. Consulte los artículos Novedades específicos de cada oferta para conocer las nuevas funciones y las actualizaciones de productos.

- Citrix Analytics for Security
- Citrix Analytics for Performance

En estas notas de la versión se destacan las nuevas funciones y actualizaciones de productos específicas de la plataforma Citrix Analytics.

21 de septiembre de 2023

Simplifique la incorporación de StoreFront mediante PowerShell Script

Se ha introducido un nuevo script de **PowerShell** que automatiza el proceso de comprobación de los requisitos previos y de instalación y configuración de StoreFront. El cliente debe ejecutar este script en modo administrador en StoreFront para incorporarlo, descartarlo, realizar autocomprobaciones, solucionar problemas y comprobar si la incorporación a la GUI de Citrix Analytics Service se ha realizado correctamente.

Para obtener más información, consulte Conectarse a una implementación de StoreFront.

28 de agosto de 2023

Servicio de microaplicaciones (fin de vida útil)

El servicio de microaplicaciones de Citrix ha llegado al final de su vida útil y ya no está disponible para los usuarios.

01 de agosto de 2023

Citrix Analytics: uso (fin de su vida útil)

Citrix Usage Analytics ha llegado al final de su vida útil y ya no está disponible para los usuarios.

23 de febrero de 2023

Problemas resueltos

Antes del lanzamiento de Citrix Virtual Apps and Desktops 2112, Citrix Analytics no descubre los sitios locales que están conectados desde Citrix Director y que se han registrado recientemente en Citrix Cloud. Por lo tanto, no ve estos sitios conectados en su tarjeta de sitio de **Virtual Apps and Desktops: Supervisión**. Este problema ya está solucionado. [CAS-63132]

28 de septiembre de 2022

Webhooks para notificaciones de alertas

Puede usar webhooks para enviar notificaciones de alertas de Citrix Analytics a cualquier aplicación de terceros que tenga configuradas las URL de webhook entrantes. Los webhooks son devoluciones de llamadas HTTP que permiten enviar mensajes en tiempo real entre las aplicaciones del proveedor de servicios y las aplicaciones para consumidores. Dado que las notificaciones de alerta se envían en tiempo real, se le notifica cuando se producen los eventos. Para obtener más información, consulte Webhooks para notificaciones de alertas.

8 de septiembre de 2022

Límite de exportaciones en CSV aumentado

El límite del número de filas que puede exportar mediante la función **Exportar a formato CSV** ahora se ha incrementado de 10 000 filas a 100 000 filas. Para obtener más información, consulte Exportar los eventos a un archivo CSV.

18 de agosto de 2022

Problema resuelto

- En la búsqueda de autoservicio de aplicaciones y escritorios, el valor de la versión de la aplicación Workspace se rellenó como **NA** (no disponible) en el archivo CSV descargado, mientras

que estaba disponible en la vista de página. Este problema ya se ha solucionado. [CAS-70361]

10 de agosto de 2022

Incorporación de StoreFront sin agregación de sitios

La dependencia de agregación de sitios para StoreFront se ha eliminado de la tarjeta de sitio de la **aplicación Aplicaciones y escritorios: Workspace**. Puede ver la opción **Conectar implementación de Storefront** en su aplicación de espacio de trabajo, aunque no tenga ningún sitio agregado a la agregación de sitios. Para obtener más información, consulte Fuente de datos de Citrix Virtual Apps and Desktops.

5 de abril de 2022

Se cambia el nombre de Secure Workspace Access a Secure Private Access

En los paneles e informes de Analytics, todas las etiquetas de **Secure Workspace Access** ahora se actualizan como **Secure Private Access** para alinearse con el nombre del producto con el que se ha cambiado la marca.

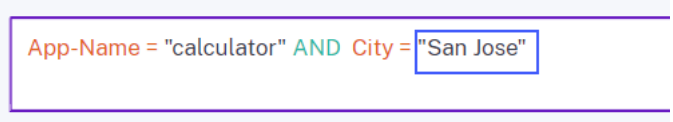
Por ejemplo, en la página **Orígenes de datos** y en la **página de búsqueda de autoservicio**, las etiquetas **Secure Workspace Access** se renombran como **Acceso privado seguro**.

21 de marzo de 2022

Problema resuelto

- En la página **Buscar**, las sugerencias automáticas de dimensiones y operadores no funcionan si la condición anterior de la consulta de búsqueda contiene un valor de dimensión que está separado por un espacio.

  Por ejemplo, en la siguiente consulta, las sugerencias automáticas dejan de funcionar después de seleccionar la ciudad como `San Jose`. Este problema ya se ha solucionado. [CAS-64126]

10 de febrero de 2022

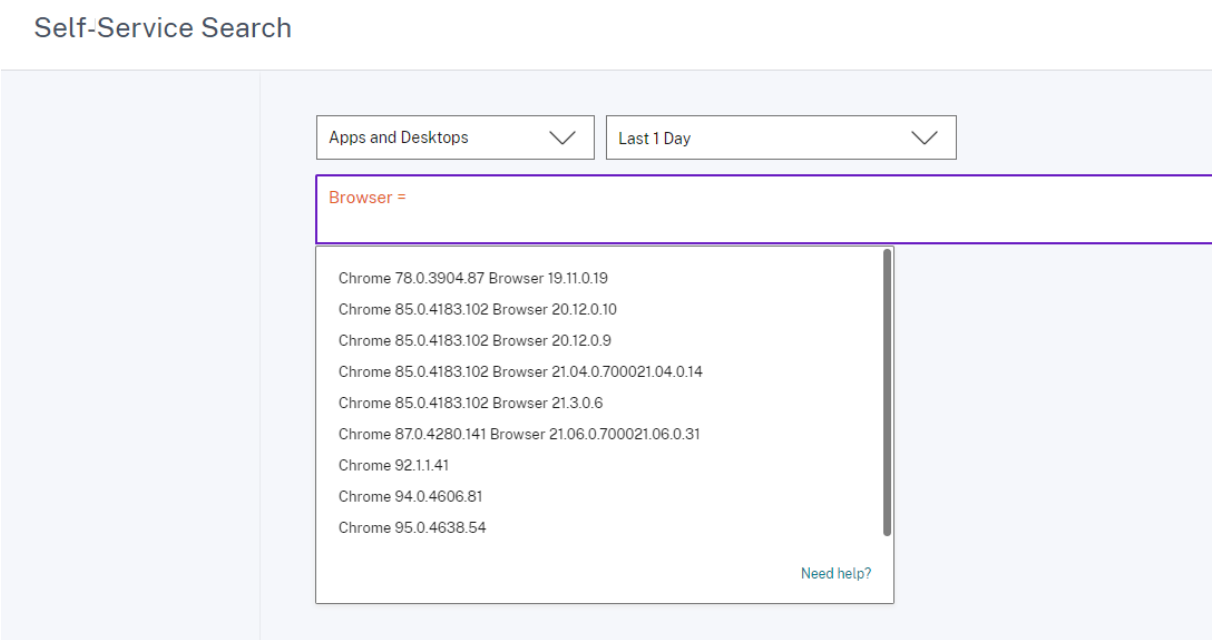
Novedades

Valores sugeridos automáticamente para las dimensiones en el cuadro de búsqueda de autoservicio En la página de búsqueda de autoservicio, cuando selecciona una dimensión y un operador válido en el cuadro de búsqueda, los valores de la dimensión se muestran automáticamente. Seleccione un valor de la lista de sugerencias automáticas o introduzca un valor manualmente en función de sus casos de uso. Cuando escribe un valor, los valores coincidentes disponibles en los registros se sugieren automáticamente.

La lista de valores sugeridos para una dimensión está predefinida (valores conocidos) en la base de datos o se basa en eventos históricos.

Por ejemplo, cuando selecciona la dimensión `Browser` y el operador de asignación, los valores conocidos se sugieren automáticamente. Puede seleccionar un valor en función de sus requisitos.

Para obtener más información, consulte Búsqueda de autoservicio.



20 de diciembre de 2021

Novedades

El nombre de Control de acceso cambia a Secure Workspace Access En los paneles e informes de Analytics, todas las etiquetas de **control de acceso** ahora se actualizan como **Secure Workspace Access** para alinearse con el nombre del producto con el que se ha cambiado la marca.

Por ejemplo, en la página **Orígenes de datos** y en la página de **búsqueda de autoservicio**, las etiquetas de **control de acceso** se renombran como **Secure Workspace Access**.

06 de diciembre de 2021

Novedades

Ahora se admite Citrix Analytics en la región Sur de Asia Pacífico

- Ahora puede elegir Asia Pacífico Sur como región de origen al incorporar su organización a Citrix Cloud y utilizar el servicio Citrix Analytics. Para obtener más información, consulte Consideraciones geográficas.
- Citrix Analytics ahora almacena los eventos de usuario y los metadatos de su organización en la región Sur de Asia Pacífico cuando la elige como su región de origen. Para obtener más información, consulte Gobernanza de datos.
- Para obtener información sobre los requisitos de red para la región Asia Pacífico Sur, consulte Descripción general de seguridad técnica.
- Para obtener información sobre los orígenes de datos compatibles en la región Asia Pacífico Sur, consulte Orígenes de datos.

19 de agosto de 2021

Novedades

Compatible con el operador IS EMPTY En la búsqueda de autoservicio, ahora puede utilizar el operador **IS EMPTY** en su condición para comprobar si hay una dimensión nula o vacía.

> **Nota**
>
> El operador solo funciona para dimensiones de tipo cadena como Nombre de aplicación, Explorador y País.

Para obtener más información, consulte Búsqueda de autoservicio.

14 de julio de 2021

Novedades

Compatible con el operador IS NOT EMPTY En la búsqueda de autoservicio, ahora puede utilizar el operador **NO ESTÁ VACÍO** en la consulta para comprobar si la dimensión no está vacía (ni en blanco).

> **Nota**
>
> El operador solo funciona para dimensiones de tipo cadena como Nombre de aplicación, Explorador y País.

Para obtener más información, consulte Búsqueda de autoservicio.

7 de junio de 2021

Función obsoleta

Se ha eliminado el entorno de demostración de Citrix Analytics Los enlaces **Probar demostración** para análisis de seguridad y análisis de rendimiento se han eliminado de la página de descripción general de Analytics. Ya no podrá acceder al entorno de demostración de cada oferta. Para obtener más información sobre cómo obtener acceso a las ofertas de Citrix Analytics, consulte Introducción.

18 de mayo de 2021

Novedades

Soporte para operador* con! = operador En su consulta de búsqueda, ahora puede usar el operador * con el operador ! = para encontrar los eventos del usuario. Por ejemplo:

- Para buscar todos los eventos de usuario que no comiencen con el nombre "John", utilice la consulta: Nombre de usuario. = John*
- Para buscar todos los eventos de usuario que no terminan con el nombre "Smith", utilice la consulta: User-Name! = *Herrero

> **Nota**
>
> Los resultados de la búsqueda distinguen entre mayúsculas y min

Para obtener más información, consulte Búsqueda de autoservicio.

Experiencia de barra de búsqueda mejorada en la página de búsqueda de autoservicio

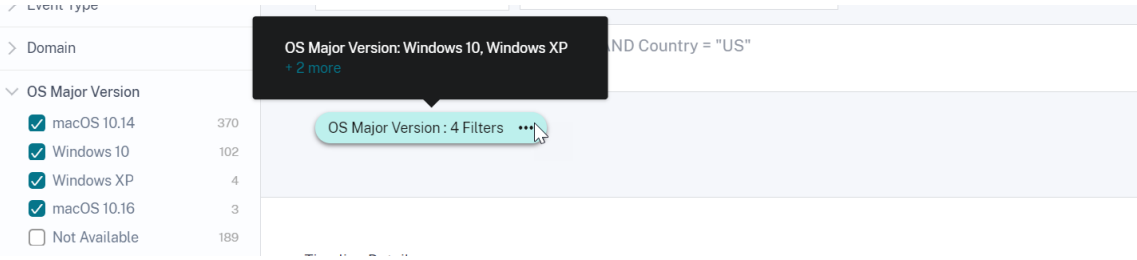
- La barra de búsqueda ahora proporciona una mejor vista de las consultas cuando se extiende a varias líneas. Utilice la barra de desplazamiento para desplazarse por las consultas multilínea. Anteriormente, era difícil ver las consultas multilínea.

- Se ha solucionado el problema de salto del cursor observado en el explorador Safari.

Para obtener más información, consulte Búsqueda de autoservicio.

Vista de chips rediseñada en la búsqueda de autoservicio

- Los chips rediseñados ahora le ofrecen una mejor visión de las múltiples facetas que ha seleccionado.



- Haga clic en un chip para seleccionar o anular la selección de las facetas según sus requisitos.

Problema resuelto

- En Citrix Director, el enlace **Ir a Analytics** no funciona. Este problema se observa para un usuario que ha registrado su organización en la región de la Unión Europea de Citrix Cloud. [CAS-50224]

31 de marzo de 2021

Compatibilidad con los operadores IN y NOT IN para consultas de búsqueda de aplicaciones y escritorios

Con las dimensiones Apps and Desktops- `Device ID`, `Domain`, `Event-Type`, y `User-Name`, ahora puede usar los siguientes operadores:

- **IN**: asigne varios valores a una dimensión para obtener los eventos relacionados con uno o más valores.
- **NO EN**: asigne varios valores a una dimensión y busque los eventos que no contengan los valores especificados.

> **Nota**
>
> Estos operadores solo se aplican a los valores de cadena.

Para obtener más información sobre los operadores, consulte Búsqueda de autoservicio.

18 de marzo de 2021

Novedades

Compatibilidad con el operador NOT LIKE (!~) Para la consulta de búsqueda de autoservicio, ahora puede usar el comando NO ME GUSTA (! ~) operador. El operador comprueba los eventos de usuario para el patrón coincidente que ha especificado. Devuelve los eventos que no contienen el patrón especificado en ninguna parte de la cadena de eventos.

Por ejemplo, la consulta `User-Name !~ "John"` muestra los eventos de los usuarios excepto John, John Smith o cualquier otro usuario que contenga el nombre coincidente "John".

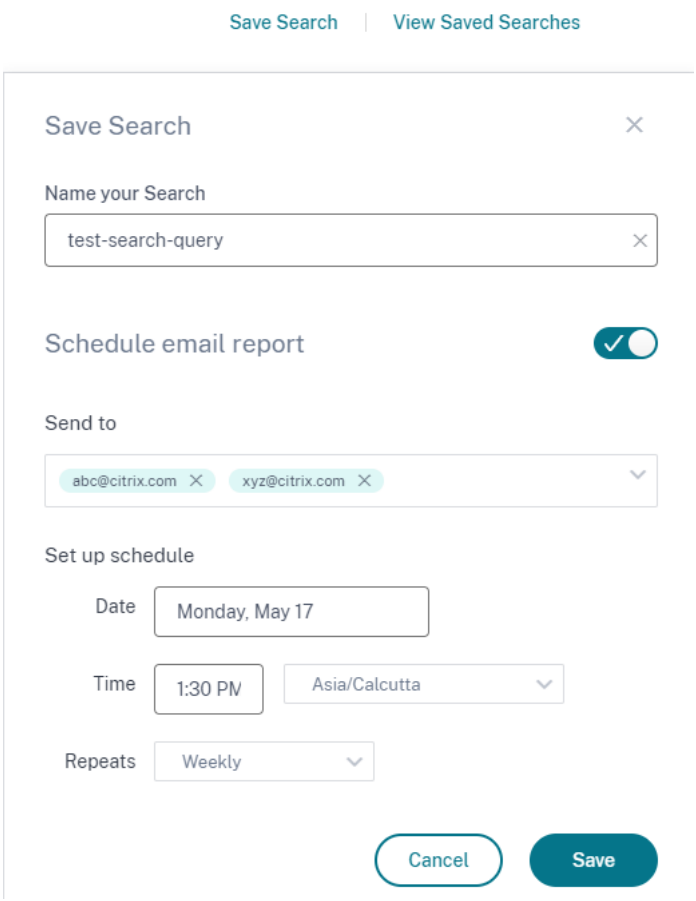
Para obtener más información, consulte Búsqueda de autoservicio.

23 de febrero de 2021

Novedades

Programar la entrega de correo electrónico para una consulta de búsqueda En la página de búsqueda de autoservicio, al guardar una consulta de búsqueda, también puede programar una entrega de correo electrónico para enviar una copia de la consulta de búsqueda guardada y el informe de resumen visual correspondiente a usted y a otros usuarios. Establezca la fecha, la hora y la frecuencia (diaria, semanal o mensual) para comenzar a enviar un correo electrónico. También puede programar la entrega por correo electrónico de las consultas de búsqueda que guardaste anteriormente.

Para obtener más información, consulte Búsqueda de autoservicio.

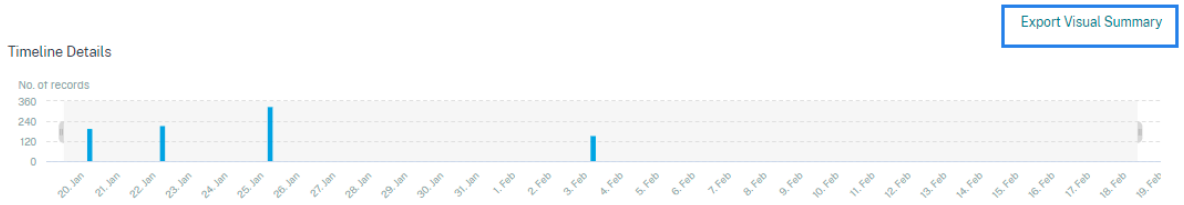


Descargar resumen visual de una consulta de búsqueda En la página de autoservicio, ahora puede descargar el informe resumido visual de la consulta de búsqueda durante un período de tiempo seleccionado y compartir una copia con otros usuarios. Haga clic en **Exportar resumen visual** para descargar el informe de resumen visual en formato PDF.

El informe contiene la siguiente información:

- Consulta de búsqueda que ha especificado para los eventos.
- Las facetas (filtros) que ha aplicado a los eventos.
- El resumen visual, como los gráficos de línea de tiempo, gráficos de barras o gráficos de los eventos de búsqueda.

Para obtener más información, consulte Búsqueda de autoservicio.

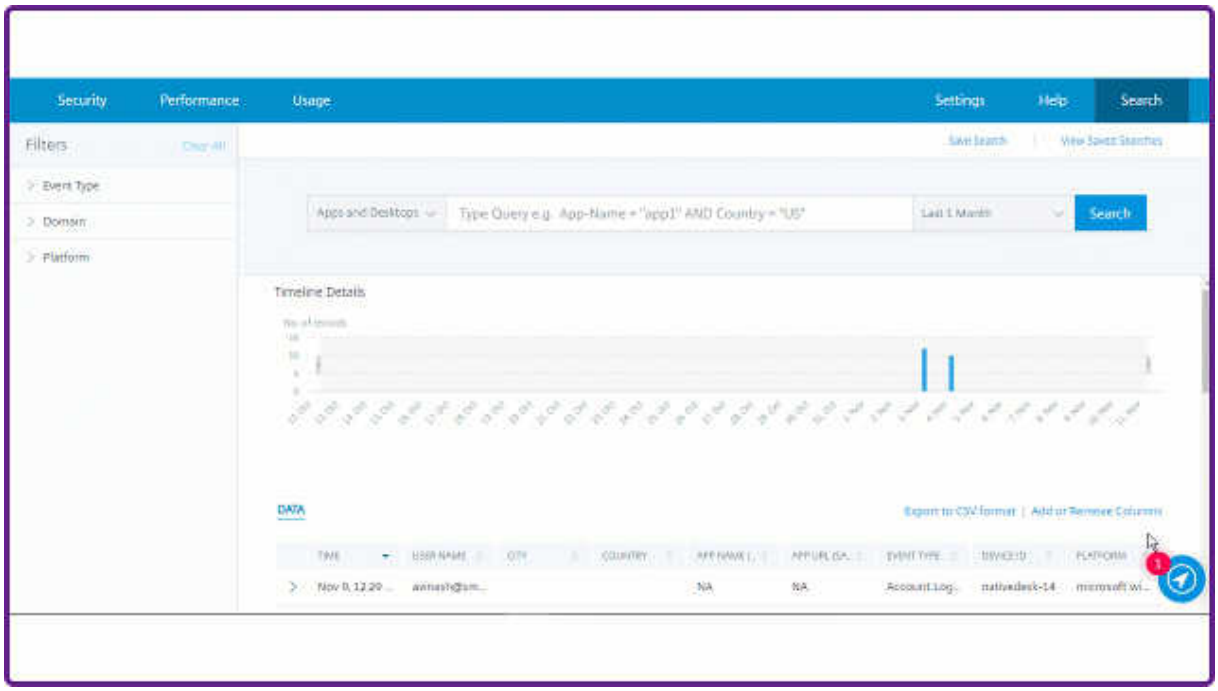


12 de noviembre de 2020

Nueva función

Guardar una consulta de autoservicio Después de crear una consulta de autoservicio, puede guardarla para usarla más adelante. Las siguientes opciones se guardan con la consulta:

- Filtros de búsqueda aplicados
- Fuente de datos seleccionada y duración



Para obtener más información, consulte Cómo guardar la búsqueda de autoservicio.

20 de octubre de 2020

Funciones nuevas

Compatibilidad con NetScaler Gateway en la región de la Unión Europea Citrix Analytics ahora es compatible con NetScaler Gateway en la región de la UE. Para obtener más información, consulte

Origen de datos de NetScaler Gateway.

9 de julio de 2020

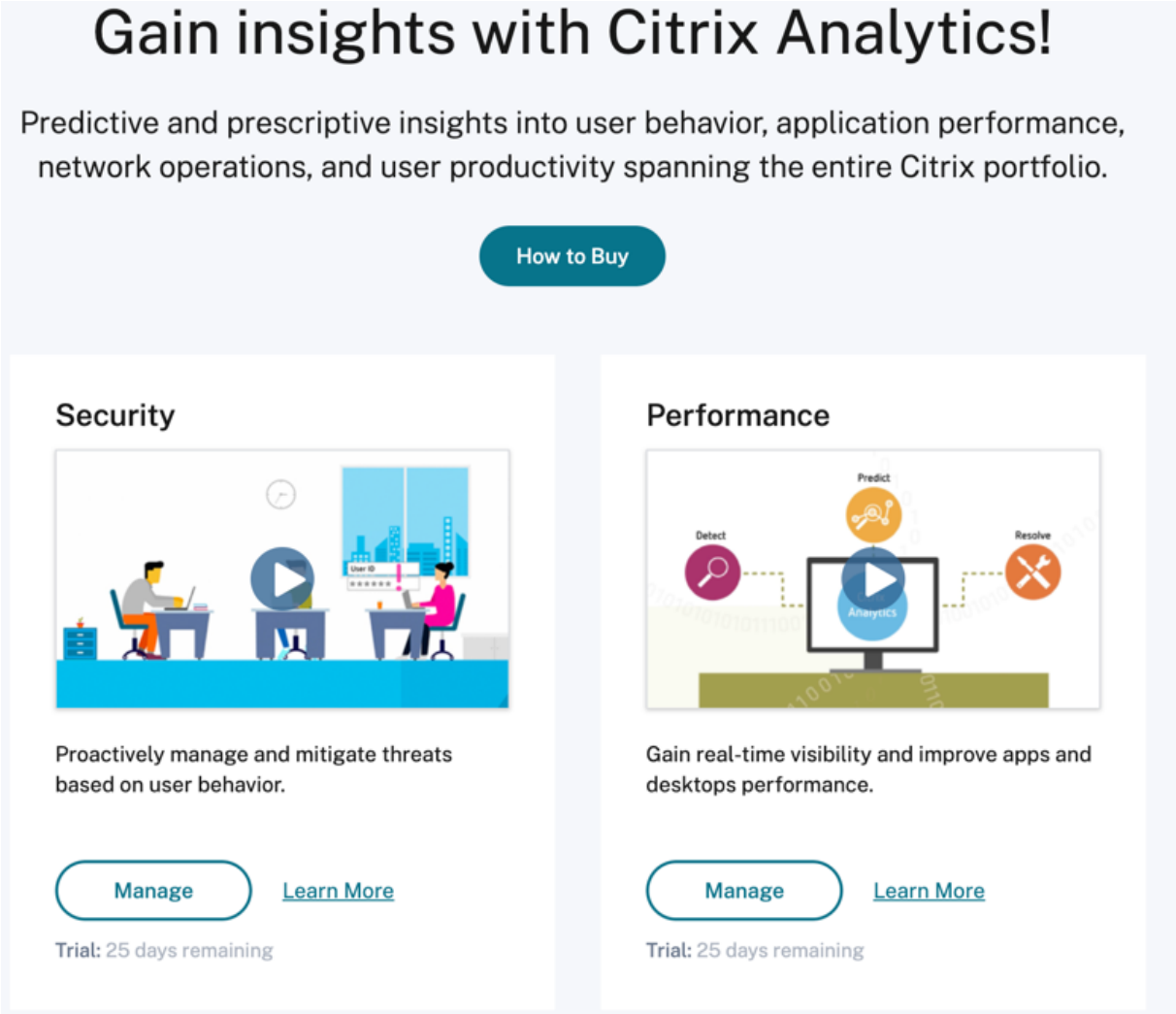
Compatibilidad retirada

Microsoft Internet Explorer 11 se ha eliminado de la lista de exploradores compatibles. Este desuso se debe a la vulnerabilidad de seguridad observada en el explorador. Para obtener la lista de exploradores compatibles, consulte Requisitos del sistema.

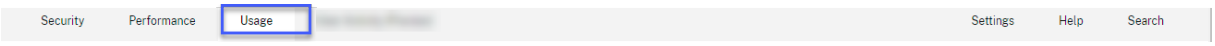
2 de junio de 2020

Funciones nuevas

Página de descripción general y barra superior rediseñadas en Analytics La página de descripción general de Analytics muestra el mosaico **Uso** que reemplaza el mosaico **Operaciones** que existía anteriormente. Además, el mosaico **Productividad** se elimina de esta página. Para ver la página de resumen, selecciona **Ayuda** > **Información general**.



Del mismo modo, en la barra superior, la ficha **Uso** sustituye a la ficha **Operaciones**.



20 de febrero de 2020

Funciones nuevas

Ofertas de suscripción de Citrix Analytics Al ofrecer opciones de compra flexibles a los usuarios, Citrix ahora ofrece tres productos Citrix Analytics individuales basados en suscripción. Citrix Analytics proporciona información única sobre seguridad o rendimiento (o ambos) basada en la oferta a la que se suscribe.

Puede adquirir las siguientes ofertas de suscripción de Citrix Analytics:

- Citrix Analytics for Security

- Citrix Analytics for Performance
- Citrix Analytics para seguridad y rendimiento (paquete)

Actualizaciones de los registros de gobierno Se han agregado nuevos registros para estos orígenes de datos:

- Proveedor de identidades Citrix
- Citrix Gateway
- Secure Browser
- Microsoft Graph Security
- Microsoft Active Directory

Para obtener más información, consulte Gobernanza de datos.

Problemas resueltos

- La búsqueda de autoservicio no funciona correctamente en Internet Explorer 11. Por lo tanto, no puede escribir la consulta de búsqueda ni realizar una operación de búsqueda. [CAS-18657]

9 de enero de 2020

Problemas resueltos

- La funcionalidad de recorrido de Citrix Analytics no funciona para los usuarios de la región de origen de la Unión Europea. [CAS-26297]

18 de diciembre de 2019

Problemas resueltos

El mosaico de **Analytics** de la página **Citrix Cloud** muestra el botón **Ver servicio**. Este botón se ha cambiado a **Administrar** para mejorar la experiencia del usuario. [CAS-27922]

12 de diciembre de 2019

Funciones nuevas

Soporte para eventos de servicio de microaplicaciones en Asia Pacífico Sur La plataforma Citrix Analytics procesa ahora las notificaciones del servicio de microaplicaciones de la región Asia Pacífico

Sur. Sin embargo, los registros que miden el rendimiento,
la estabilidad, el uso, la seguridad y el soporte se agregan y almacenan en Estados Unidos. Para obtener más información, consulte Gobernanza de datos.

> **Nota**
>
> El servicio de microaplicaciones se ofrece como parte de Citrix Workspace. Para obtener más información, consulte la documentación de Microaplicaciones.

04 diciembre 2019

Problemas resueltos

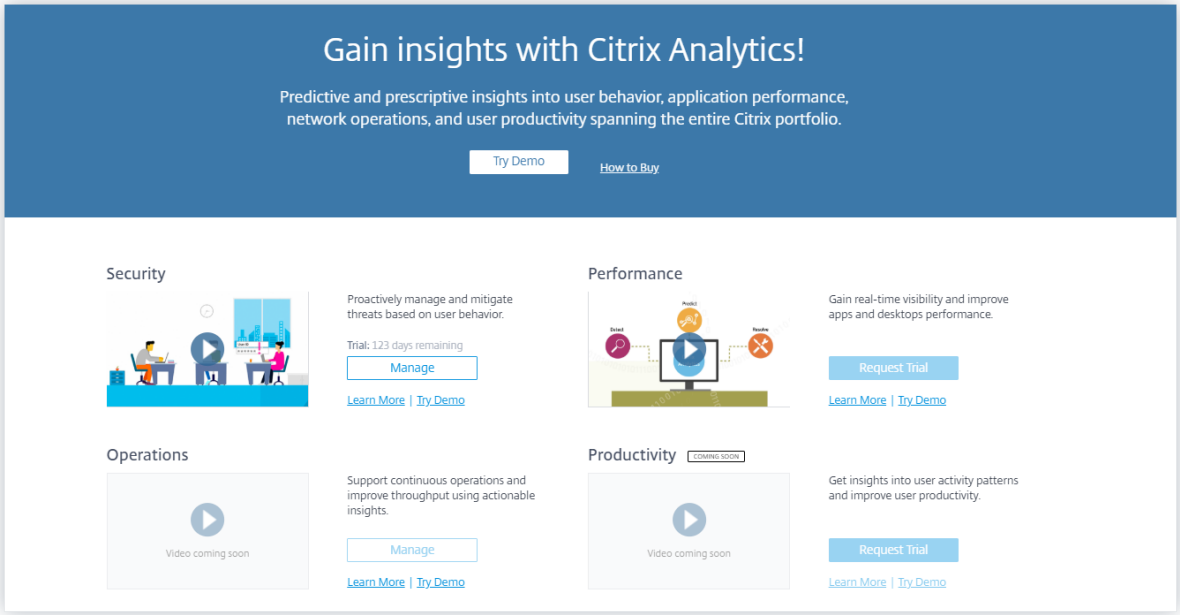
Algunos usuarios de la región Asia Pacífico Sur no pueden iniciar sesión en Citrix Analytics aunque se han inscrito en Citrix Cloud seleccionando **Estados Unidos** como región de origen. [CAS-27368]

22 noviembre 2019

Funciones nuevas

Página de descripción general rediseñada para Analytics La página de descripción general de Analytics se ha rediseñado para permitir el acceso a todas las ofertas de Analytics de esta página. Puede solicitar una prueba, probar la demostración o administrar su oferta de Analytics. Actualmente, solo los análisis de seguridad y análisis de operaciones están disponibles de forma general y, por lo tanto, están activos en esta página.

Para ver la página de resumen, selecciona **Ayuda** > **Información general**.



21 de octubre de 2019

Funciones nuevas

Información técnica general sobre la seguridad El resumen de seguridad técnica le proporciona información sobre las prácticas recomendadas de seguridad relacionadas con Citrix Analytics. Este documento describe el flujo de datos, la protección de datos, los requisitos de red y las responsabilidades de seguridad que deben tenerse en cuenta al utilizar Citrix Analytics.

11 de septiembre de 2019

Problemas resueltos

- Citrix Cloud no puede redirigir a los usuarios a la página de Citrix Analytics específica de la región. [CAS-20559]

20 de agosto de 2019

Problemas resueltos

- La funcionalidad de tutorial de Citrix Analytics no se carga correctamente en los exploradores Microsoft Edge y Safari. [CAS-20906]

31 julio 2019

Funciones nuevas

Apoyo a la región de la Unión Europea Citrix Analytics ahora es compatible con la región de la Unión Europea. Puede elegir **la Unión Europea** como región de origen al incorporar su organización a Citrix Cloud y utilizar el servicio Citrix Analytics. Citrix Analytics almacena los eventos de usuario y los metadatos de su organización en la región de la Unión Europea. Para obtener más información sobre las regiones de Citrix Cloud, consulte Consideraciones geográficas.

26 de junio de 2019

Problemas resueltos

- Citrix Analytics no se carga correctamente en Internet Explorer 11. [CAS-19867]

19 de junio de 2019

Problemas resueltos

- Citrix Analytics no se carga correctamente en Microsoft Edge. [CAS-19930]

16 de noviembre de 2018

Problemas resueltos

- Si accede a Citrix Analytics mediante Internet Explorer versión 11.0, la barra de navegación de **Citrix Cloud** no se carga y le impide acceder al menú de hamburguesas.

10 de octubre de 2018

Mejoras de arquitectura y plataforma

En esta versión se han realizado varias mejoras de arquitectura y plataforma para mejorar el rendimiento, la escalabilidad, la supervisión, la compatibilidad, la seguridad y la experiencia del usuario.

23 de agosto de 2018

Citrix Analytics es un servicio en la nube que se ofrece a través de Citrix Cloud. Recopila datos de los productos de la cartera de Citrix y proporciona información útil, lo que permite a los administradores gestionar de forma proactiva las amenazas a la seguridad, mejorar el rendimiento de las aplicaciones y contribuir a la continuidad de las operaciones. En la actualidad, Citrix Analytics ofrece las siguientes ofertas de análisis:

- **Análisis de seguridad**: recopila y proporciona visibilidad sobre el comportamiento de los usuarios y las entidades. Para obtener más información, consulte Análisis de seguridad.
- **Análisis de operaciones**: recopila y presenta información sobre las actividades de los usuarios, como los sitios web visitados y el ancho de banda gastado. Para obtener más información, consulte Análisis de operaciones.

Nuevos nombres de producto

Los productos Citrix compatibles con Citrix Analytics ahora se renombran como parte de la cartera de productos unificados de Citrix.

Es posible que veas nuevos nombres en nuestros productos y en la documentación del producto. Este cambio de marca es el resultado de la expansión de la cartera y la estrategia de nube de Citrix. Para obtener más información sobre la cartera unificada de Citrix, consulte la guía del producto Citrix.
La implementación de esta transición en nuestros productos y en su documentación es un proceso continuo.

- Con lo que el contenido y la documentación del producto aún puede contener los nombres anteriores. Por ejemplo, puede que vea instancias de nombres anteriores en texto de la consola, mensajes, nombres de directorios o archivos, capturas de pantalla y diagramas.
- Es posible que algunos elementos (como los comandos) sigan conservando sus nombres anteriores para evitar que se rompan los scripts de clientes existentes.
- Asimismo, la documentación de producto y otros recursos relacionados (como vídeos y entradas de blog) que se incluyan como enlaces en la documentación de este producto pueden contener todavía los nombres anteriores.

Problemas conocidos

September 21, 2023

Este artículo destaca los problemas conocidos que se aplican a todas las ofertas de Citrix Analytics (rendimiento y seguridad).

Para conocer los problemas específicos de cada oferta, consulte los artículos de problemas conocidos correspondientes: Seguridad y rendimiento.

- El **indicador Gateway: Acceso por primera vez desde una nueva IP** se activa para los usuarios que acceden a servicios o aplicaciones a través de Gateway la primera vez que inician sesión. [CAS-57963]

Orígenes de datos

September 21, 2023

Los orígenes de datos son los servicios en la nube y los productos locales que envían datos a Citrix Analytics.

Citrix Analytics recopila datos de estos orígenes de datos:

- **Orígenes de datos de Citrix**. Servicios de Citrix Cloud y productos locales que envían datos a Citrix Analytics. Citrix Analytics descubre automáticamente los servicios de Citrix Cloud, como Content Collaboration y Endpoint Management, que están asociados a su cuenta de Citrix Cloud.

  En el caso de los productos locales, como Citrix Gateway y Citrix Virtual Apps and Desktops, debe realizar una serie de configuraciones para conectarse a Citrix Analytics. Por ejemplo, las instancias de puerta de enlace local deben agregarse a Application Delivery Management. Además, los sitios de Virtual Apps and Desktops locales deben agregarse a Workspace o los servidores StoreFront deben configurarse.
- **Orígenes de datos externos**. Aplicaciones de terceros, como Microsoft Graph Security, Microsoft Active Directory que se pueden integrar con Citrix Analytics. Citrix Analytics recopila datos de estos orígenes de datos externos después de una integración satisfactoria.

Orígenes de datos compatibles

Según la oferta de Citrix Analytics que utilice, los orígenes de datos varían. Consulte los siguientes artículos para ver los orígenes de datos compatibles con cada oferta:

- Orígenes de datos compatibles con Citrix Analytics for Security
- Orígenes de datos compatibles con Citrix Analytics for Performance

Ambas ofertas admiten las fuentes de datos Citrix Gateway, Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops service) y Citrix Virtual Apps and Desktops: Citrix Analytics for Security y Citrix Analytics for Performance. Para obtener información sobre los pasos de incorporación aplicables a ambas ofertas, consulte los siguientes artículos:

- Origen de datos de NetScaler Gateway
- Origen de datos de Citrix Virtual Apps and Desktops

Origen de datos de NetScaler Gateway

April 12, 2024

La fuente de datos de **Gateway** representa las instancias de NetScaler Gateway locales en su entorno. Citrix Analytics detecta automáticamente los agentes de NetScaler Application Delivery Management (ADM) y las instancias de Gateway agregadas al servicio NetScaler ADM.

Cuando los usuarios acceden a cualquier servicio o aplicación a través de Gateway, Citrix Analytics recibe los eventos de acceso de los usuarios en tiempo real. Los eventos del usuario se procesan para detectar cualquier amenaza de seguridad.

En este artículo se describen los pasos para agregar NetScaler Gateway a Citrix Analytics. Estos pasos se aplican a las dos ofertas: Citrix Analytics for Performance y Citrix Analytics for Security.

Requisitos previos

- Suscríbase a NetScaler ADM que se ofrece en Citrix Cloud. Para obtener información sobre cómo empezar a utilizar NetScaler ADM, consulte Introducción.
- Licencia Citrix ADM verificada. Para obtener más información sobre las licencias de Citrix ADM, consulte Licencias.
- Revise los requisitos del sistema y asegúrese de que se cumplan los requisitos.

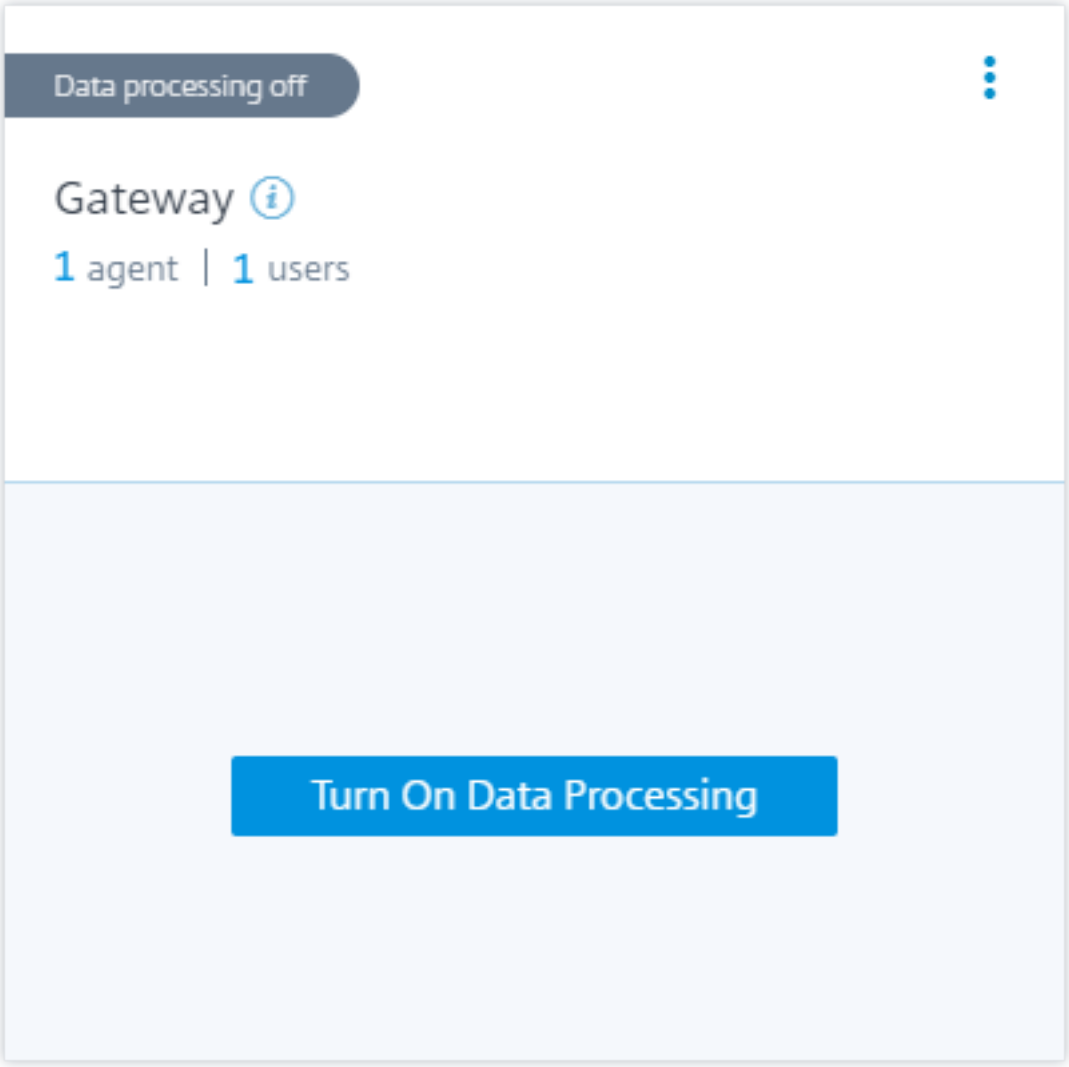
Orígenes de datos de puerta de enlace agregadas a NetScaler ADM

Citrix Analytics descubre automáticamente los agentes de NetScaler ADM y las instancias de NetScaler Gateway que ya se han agregado al servicio NetScaler ADM.

Para ver la fuente de datos:

En la barra superior, haga clic en **Configuración** > **Orígenes de datos**. En función de su oferta, seleccione **Seguridad** o **Rendimiento** para ver la tarjeta de sitio de Gateway.

Los agentes descubiertos y los usuarios se muestran en la tarjeta del sitio de Gateway. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics comience a procesar los datos de esta fuente de datos.

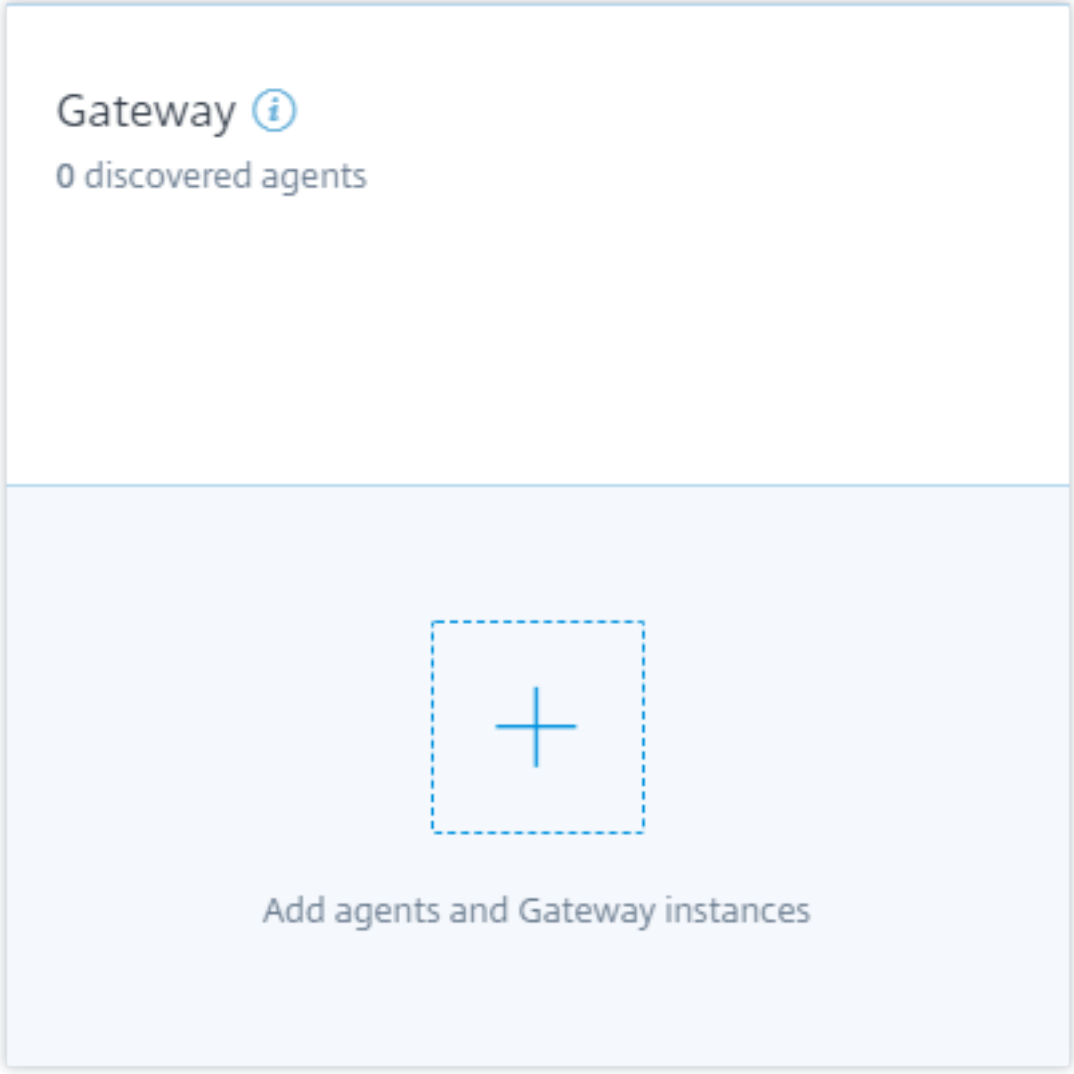


Puede ver los eventos recibidos.

Consulte Un proceso unificado para habilitar el análisis en servidores virtuales para habilitar Citrix Analytics si aún no está habilitado en el servicio Citrix ADM.

Los orígenes de datos de Gateway no se agregaron a NetScaler ADM

La tarjeta del sitio de Gateway muestra **0 agentes detectados** cuando los agentes de NetScaler ADM y las instancias de NetScaler Gateway no se agregan al servicio NetScaler ADM.

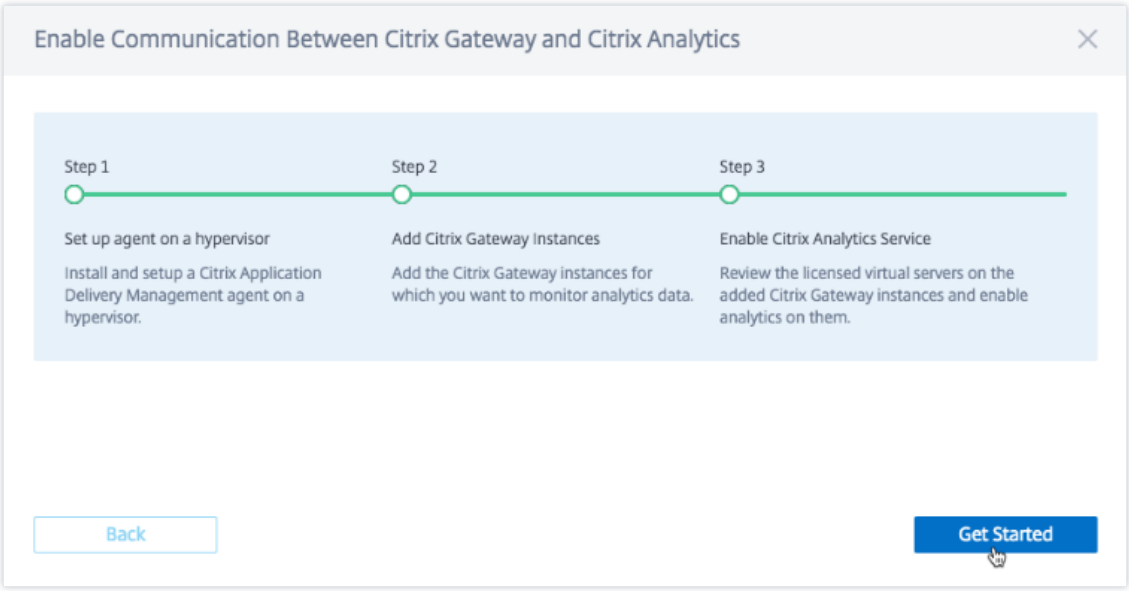


Para descubrir los agentes y las instancias de Gateway, haga lo siguiente:

1. Si ya tiene una suscripción al servicio NetScaler ADM, haga clic en **+** en la tarjeta del sitio para agregar los agentes y las instancias de Gateway.
2. Si no tiene una suscripción al servicio NetScaler ADM, debe suscribirse a ella. Vaya a su cuenta de Citrix Cloud y haga lo siguiente:
    a) En **Servicios disponibles**, haga clic en **Administrar** en el mosaico **Administración de entrega de aplicaciones**.
    b) Siga las instrucciones en pantalla para crear una cuenta Express para NetScaler ADM. Para obtener más información, consulte Introducción en la documentación de NetScaler ADM.
    c) Después de crear la cuenta Express, vuelva a iniciar sesión en Analytics y haga clic en **Configuración > Orígenes de datos > Seguridad**.

d) En la tarjeta del sitio de Gateway, haga clic en **+** para agregar los agentes y las instancias de Gateway.

3. En la siguiente página, haga clic en **Comenzar**.



4. Realice las siguientes tareas:

   - Instale un agente NetScaler ADM
   - Agregar sus instancias de Gateway
   - Habilitar análisis en servidores virtuales

Requisitos previos

- **Requisito de instalación del agente NetScaler ADM**: en su centro de datos, puede instalar un agente en Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM Server.

  En la siguiente tabla se enumeran los recursos informáticos virtuales que el hipervisor debe proporcionar para el agente.

Componente	Requisito
RAM	8 GB (se recomiendan 32 GB para un mejor rendimiento).
CPU virtual	4 (se recomiendan 8 CPU virtuales para un mejor rendimiento)
Espacio de almacenamiento	120 GB

Componente	Requisito
Interfaces de red virtual	1
Rendimiento	1 Gbps

- **Requisitos de puertos**: asegúrese de que los siguientes puertos estén abiertos para que el agente NetScaler ADM se comunique con las instancias de NetScaler Gateway.

Tipo	Puerto	Descripción
TCP	80/443	Para comunicación NITRO desde el agente a las instancias de NetScaler Gateway
TCP	22	Para la comunicación SSH del agente a la instancia de NetScaler Gateway.
UDP	4739	Para la comunicación de AppFlow de NetScaler Gateway
ICMP	Sin puerto reservado	Detectar la accesibilidad de red desde el agente hasta las instancias de NetScaler Gateway.
SNMP	161, 162	Para recibir eventos SNMP de la instancia de NetScaler Gateway al agente.
Syslog	514	Para recibir mensajes de syslog en el agente desde la instancia de NetScaler Gateway.
TCP	5557	Para la comunicación del flujo de registros desde las instancias de NetScaler Gateway

Para la comunicación entre el agente de NetScaler ADM y Citrix Analytics, asegúrese de que el siguiente puerto esté abierto:

Tipo	Puerto	Descripción
TCP	443	Para la comunicación NITRO entre el agente y el servicio NetScaler Application Delivery Management.

Para la comunicación entre el agente de NetScaler ADM y Citrix Analytics, asegúrese de que el siguiente dispositivo de punto final esté en la lista de permitidos:

Dispositivo de punto final	Región de EE. UU.	Región de la UE
Centro de eventos	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`

Instalar y configurar un agente

Instale y configure el agente de servicio NetScaler ADM en su entorno de red para permitir la comunicación entre Analytics y las instancias de Gateway en su centro de datos.

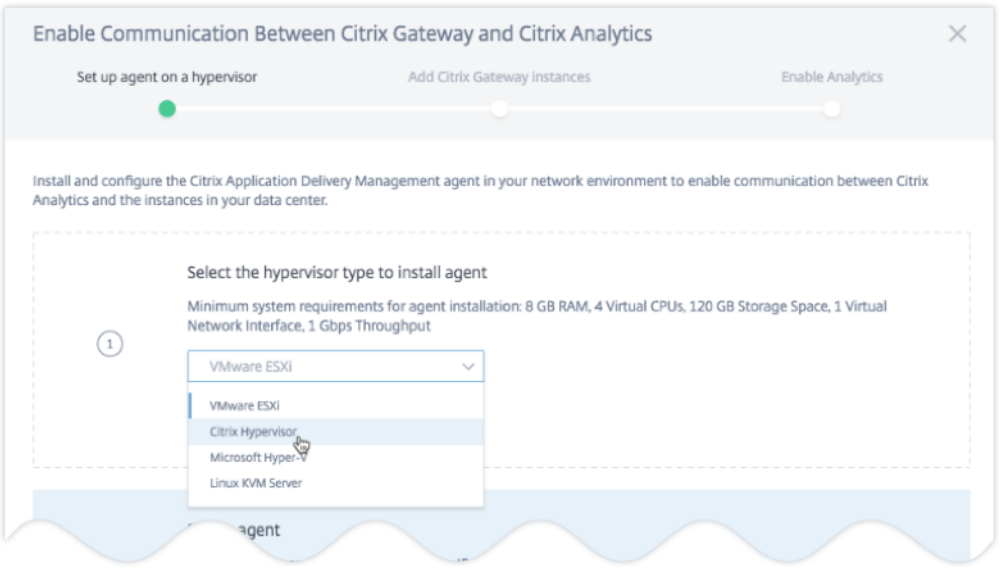
Puede instalar un agente en los siguientes hipervisores del centro de datos de su empresa:

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

Para instalar y configurar un agente, haga lo siguiente:

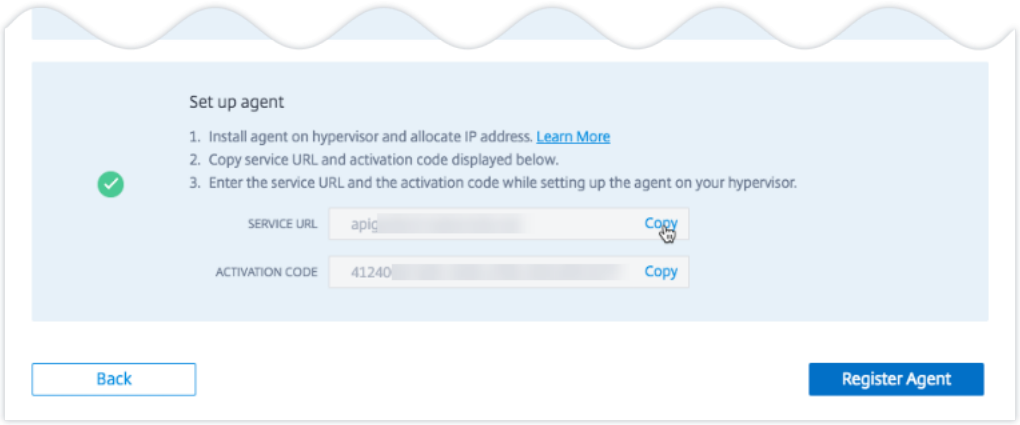
1. Descargue la imagen del agente.

   En la página **Configurar agente en un hipervisor**, seleccione el hipervisor y haga clic en **Descargar imagen** para descargar la imagen del agente en su sistema local.



2. Copie la URL del servicio y el código de activación.

   Se generan y muestran una URL de servicio y un código de activación en la interfaz de usuario, como se muestra en la siguiente imagen. (Este proceso puede tardar unos segundos). El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrarse en el servicio. Introduzca la URL de servicio y el código de activación mientras instala el agente en su hipervisor.

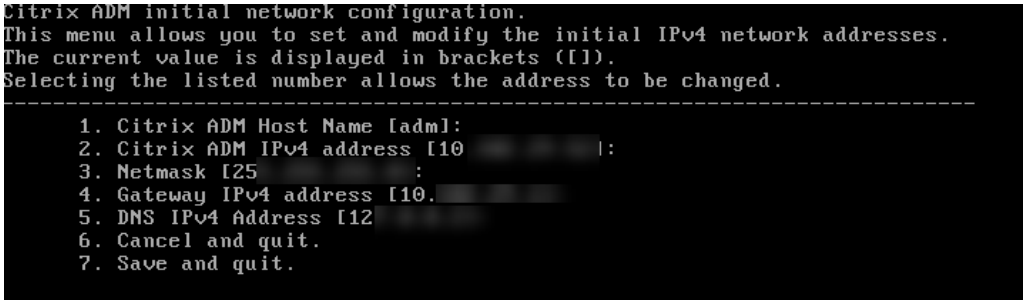


3. Instale el agente en un hipervisor.

> **Nota**
>
> Antes de comenzar la instalación del agente, asegúrese de que:
>
> - Tiene los recursos informáticos virtuales necesarios que el hipervisor debe proporcionar para cada agente: RAM: 8 GB, vCPU: 4, espacio de almacenamiento: 120 GB, interfaz de red virtual: 1 y rendimiento: 1 Gbps
> - Configura su DNS para permitir el acceso a Internet a su agente.

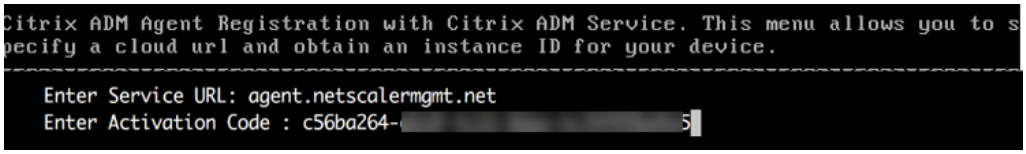
- En un Citrix Hypervisor, lleve a cabo lo siguiente:

  a) Importe el archivo de imagen del agente a su hipervisor. En la ficha **Consola**, configure las opciones de configuración de red iniciales como se muestra en el siguiente ejemplo.

  Si ha introducido valores incorrectos o quiere cambiar algún valor, inicie sesión en la solicitud de shell con las credenciales predeterminadas `nsrecover`/`nsroot`. A continuación, ejecute el comando `networkconfig`.

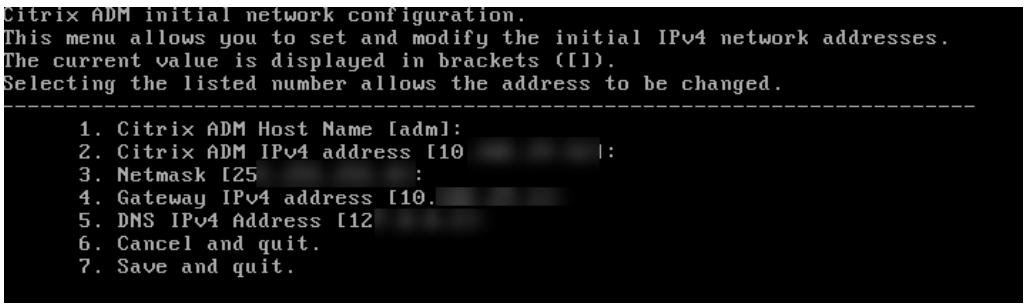
  b) Introduzca la **URL de servicio** y el **código de activación** que guardó al descargar la imagen del agente.

  Si ha introducido la URL de servicio o el código de activación de forma incorrecta, inicie sesión en el símbolo del sistema del shell del agente y, a continuación, ejecute el script: `deployment_type.py`. Este script le permite volver a introducir la URL del servicio y el código de activación.

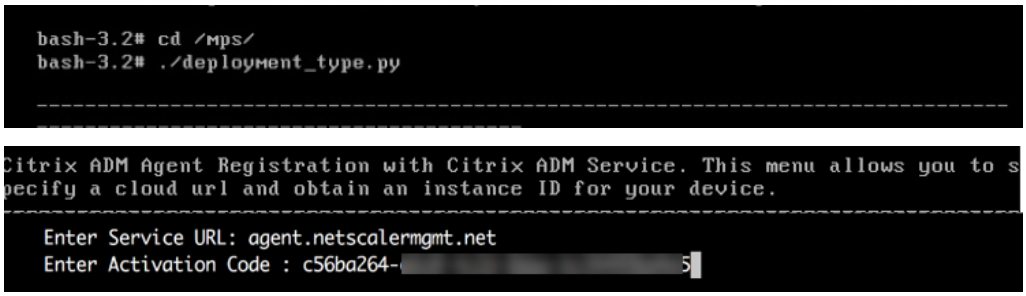
- En un hipervisor VMware ESXi, lleve a cabo lo siguiente:

  a) Importe el archivo de imagen del agente a su hipervisor. En la ficha **Consola**, configure las opciones de configuración de red iniciales como se muestra en el siguiente ejemplo.

  b) Después de configurar la red, cuando se le solicite, inicie sesión en la solicitud de shell del agente con las credenciales predeterminadas `nsrecover`/`nsroot`.

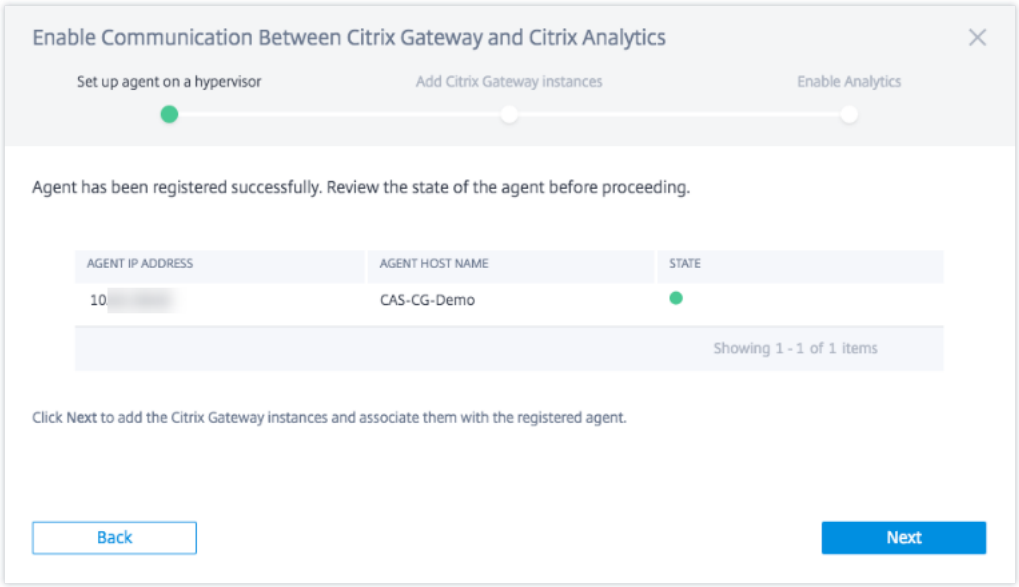
c) Navegue al directorio **/mps**, ejecute el script e introduzca la **URL de servicio** y el **código de activación** que guardó al descargar la imagen del agente.



> **Nota**
>
> Puede utilizar el mismo archivo de imagen para instalar varios agentes. Sin embargo, no puede usar el mismo código de activación en más de un agente. Para generar un nuevo código de activación, acceda a Citrix Analytics y, en el paso del agente de instalación en un hipervisor, haga clic en **Descargar imagen** nuevamente. Se genera un nuevo código de activación.

4. Agente de registro.

   Una vez que el registro del agente se realiza correctamente, el agente se reinicia para completar el proceso de instalación. Una vez que el agente se haya reiniciado, acceda a Citrix Analytics y haga clic en **Registrar agente**y, a continuación, verifique el estado del agente.

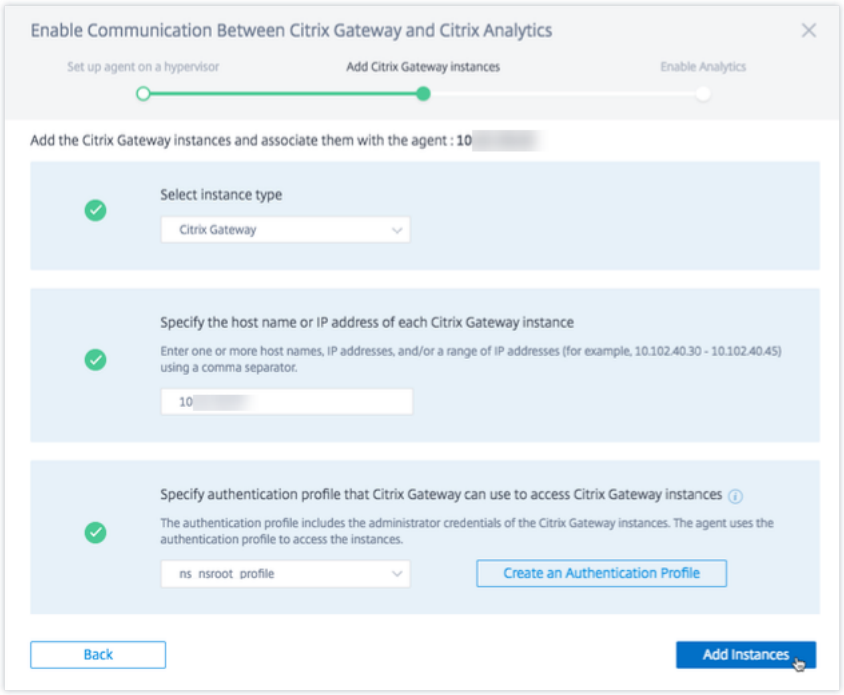


Cuando el estado del agente esté en el estado UP indicado por un punto verde junto a él, haga clic en **Siguiente** para comenzar a agregar instancias al servicio.

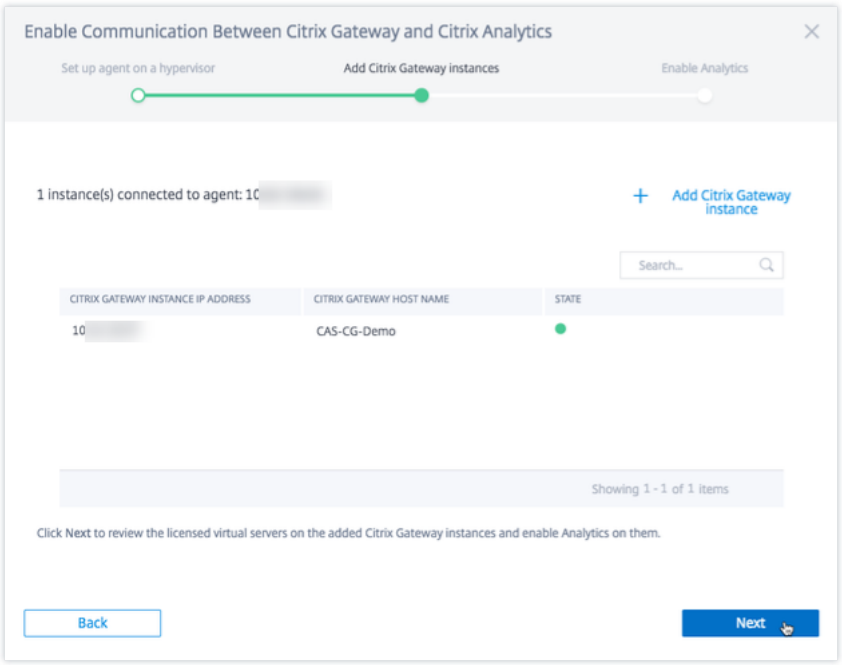
Cómo agregar instancias de NetScaler Gateway

Las instancias son dispositivos o dispositivos virtuales de NetScaler Gateway que son los orígenes de datos de Citrix Analytics.

1. En la página **Agregar instancias de NetScaler Gateway**, seleccione el tipo de instancia y especifique los nombres de host o las direcciones IP o el rango de direcciones IP de las instancias de Gateway para descubrir.
2. Cree un perfil de autenticación que el agente pueda utilizar para acceder a las instancias de Gateway. Este perfil son las credenciales de administrador de una instancia de Gateway. A continuación, haga clic en **Agregar instancias**.



Una vez agregadas las instancias, puede ver el número de instancias que se han descubierto correctamente. Para agregar más instancias, haga clic en **Agregar instancia de NetScaler Gateway**.



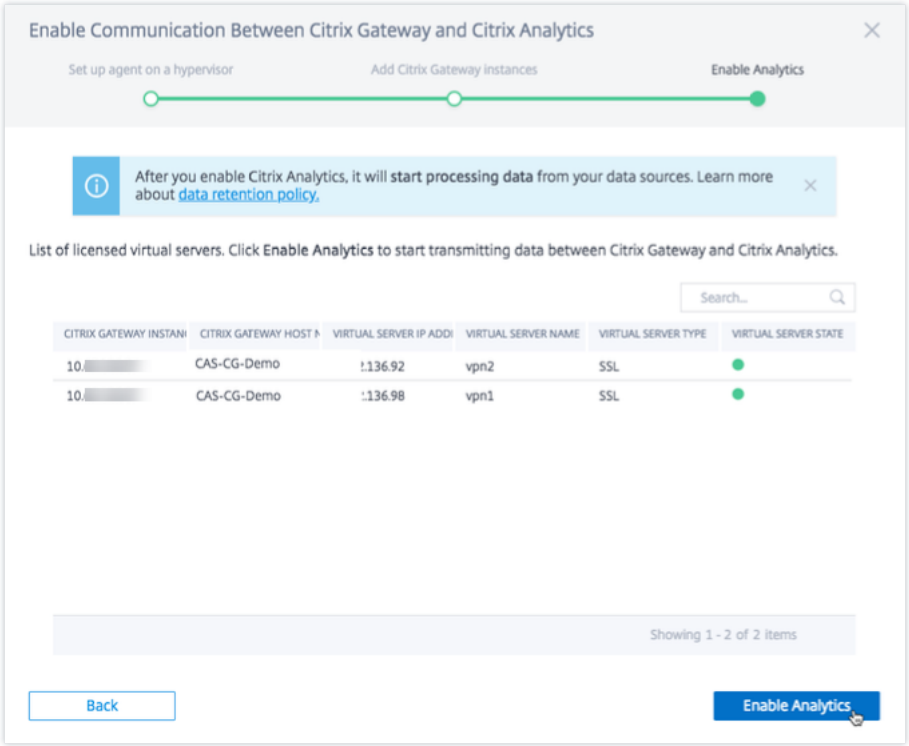
Haga clic en **Siguiente** para habilitar el análisis.

Habilitar análisis

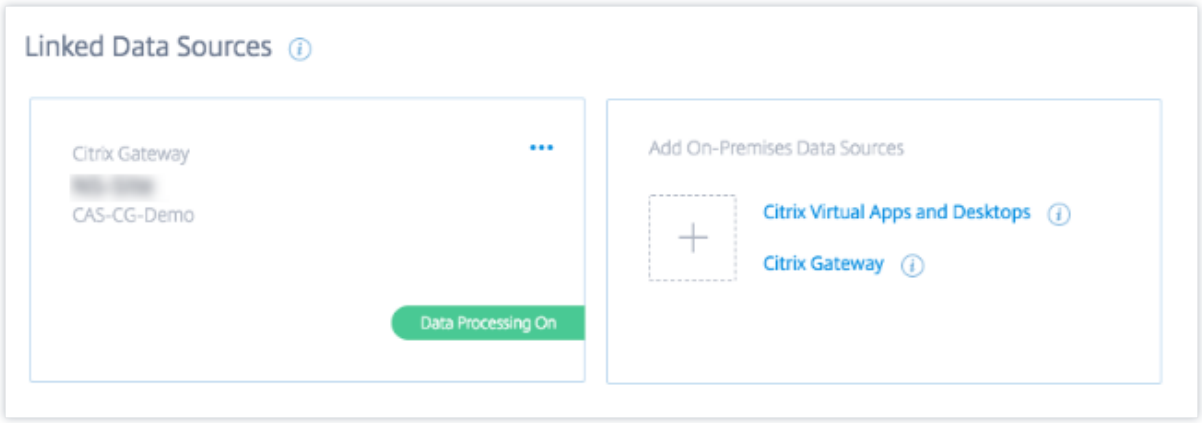
Citrix Analytics descubre automáticamente los servidores virtuales con licencia en las instancias de NetScaler Gateway agregadas. Habilite el análisis en todos los servidores virtuales descubiertos.

En la página **Enable Analytics**, de forma predeterminada, aparecen todos los servidores virtuales con licencia de las instancias de Gateway. Revise la lista de servidores virtuales con licencia y haga clic en **Habilitar análisis** para habilitar el análisis en los servidores virtuales.

> **Nota**
>
> Los servidores virtuales pueden tardar algún tiempo, aproximadamente 10 minutos, en aparecer en la página.



El estado de la tarjeta del sitio cambia a **Procesamiento de datos encendido**. Puede ver los eventos recibidos.



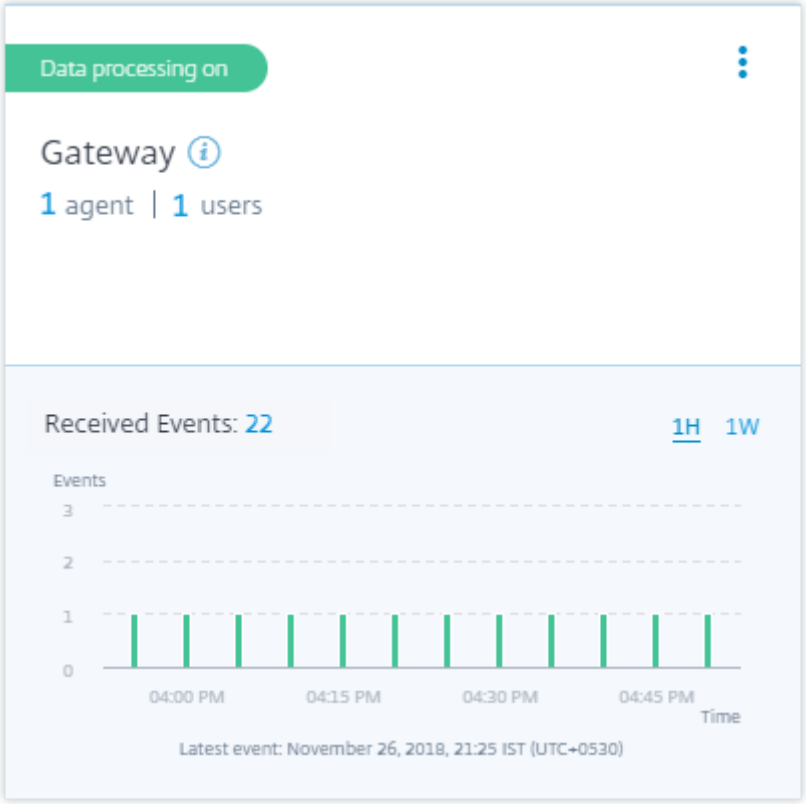
Vea el vídeo de incorporación

En el siguiente vídeo se muestran los pasos para incorporar una instancia de Gateway:

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

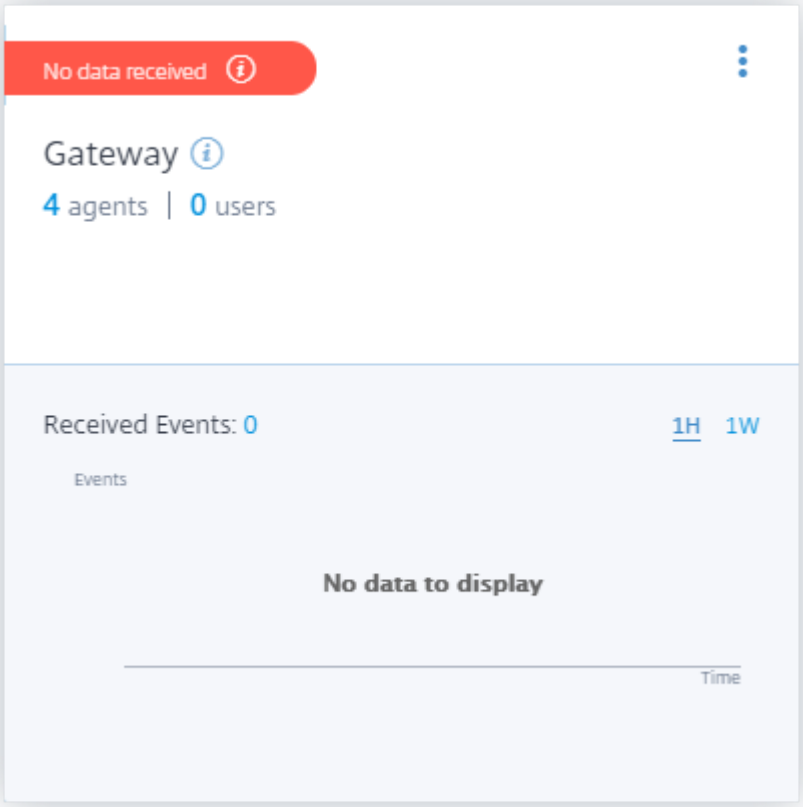
Ver eventos, usuarios y agentes recibidos

La tarjeta del sitio muestra el número de usuarios de Gateway, agentes de NetScaler ADM y los eventos recibidos del origen de datos durante la última hora, que es la selección de tiempo predeterminada. También puede seleccionar 1 semana (**1W**) y ver los datos. Haga clic en el número de usuarios que quiere ver en la página **Usuarios**. Haga clic en el número de agentes para ver las instancias de NetScaler Gateway y los agentes.



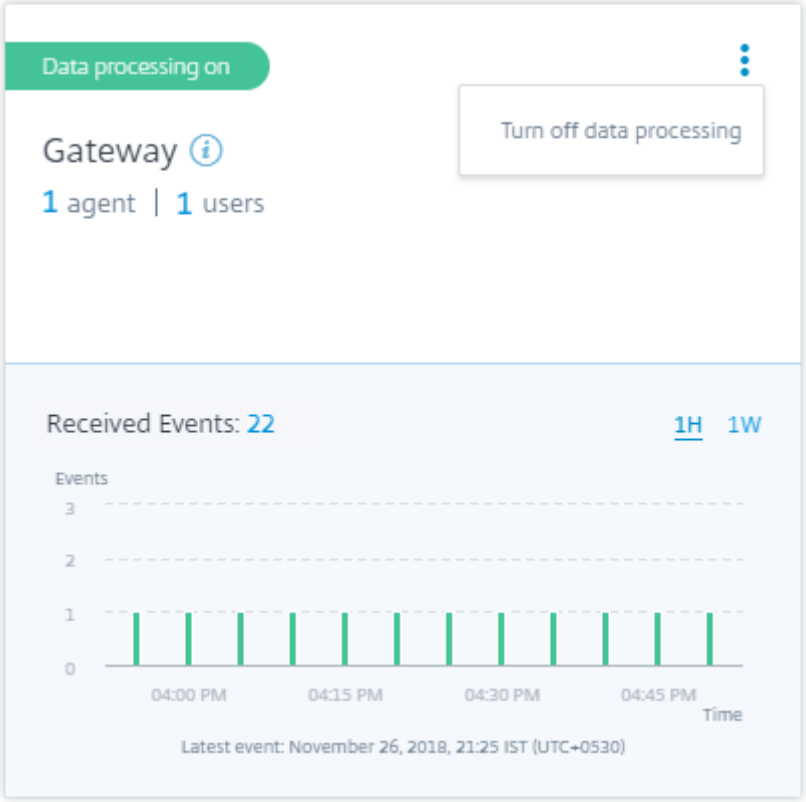
Después de habilitar el procesamiento de datos, es posible que la tarjeta del sitio muestre el estado **Sin datos recibidos**. Este estado aparece por dos motivos:

1. Si activó el procesamiento de datos por primera vez, los eventos tardan un tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Data processing on**. Si el estado no cambia después de algún tiempo, actualice la página **Orígenes de datos**.
2. Analytics no ha recibido ningún evento del origen de datos en la última hora.

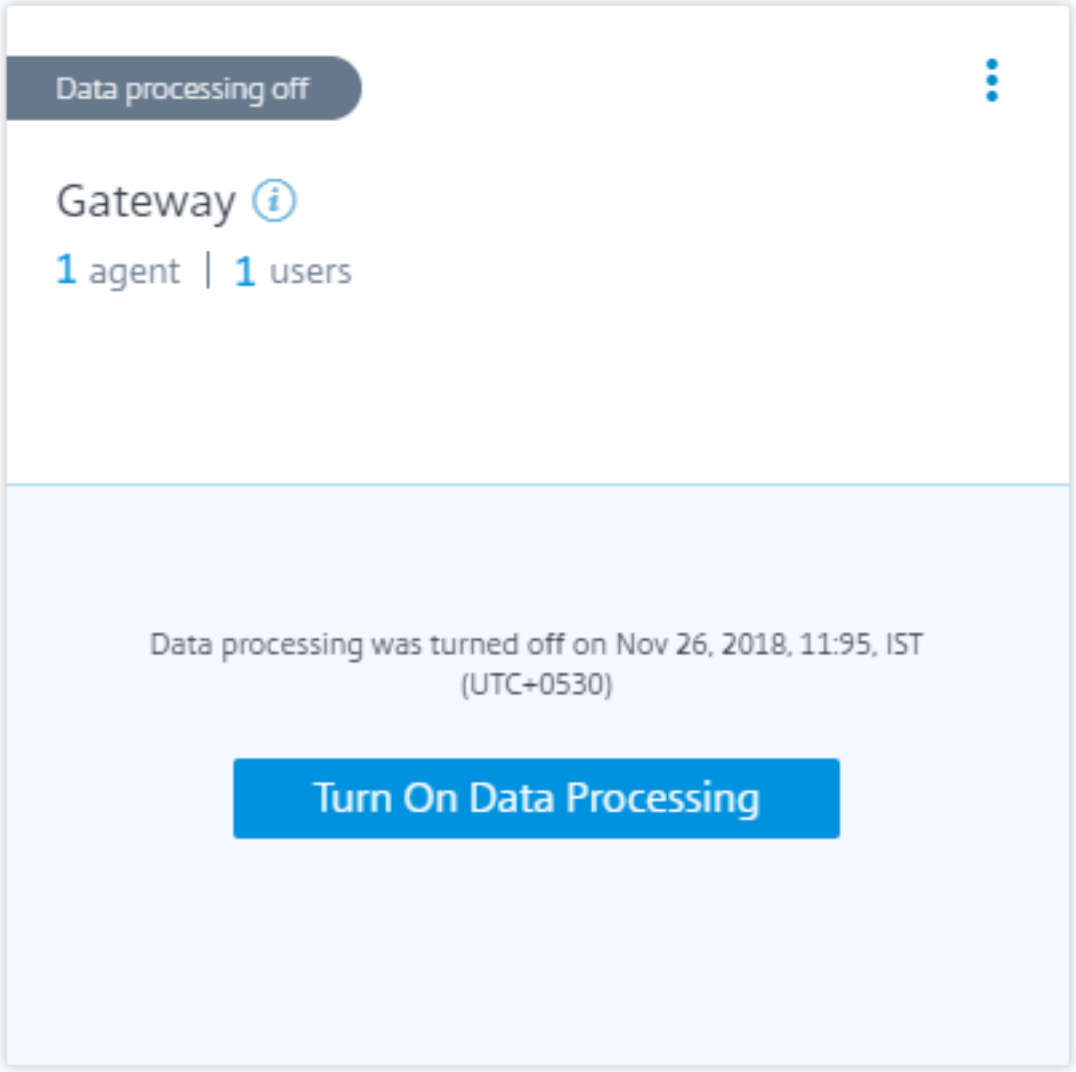


Activar o desactivar el procesamiento de datos

Para detener el procesamiento de datos, haga clic en los puntos suspensivos verticales () en la tarjeta del sitio y, a continuación, haga clic en **Desactivar el procesamiento de datos**. Citrix Analytics deja de procesar datos para este origen de datos.

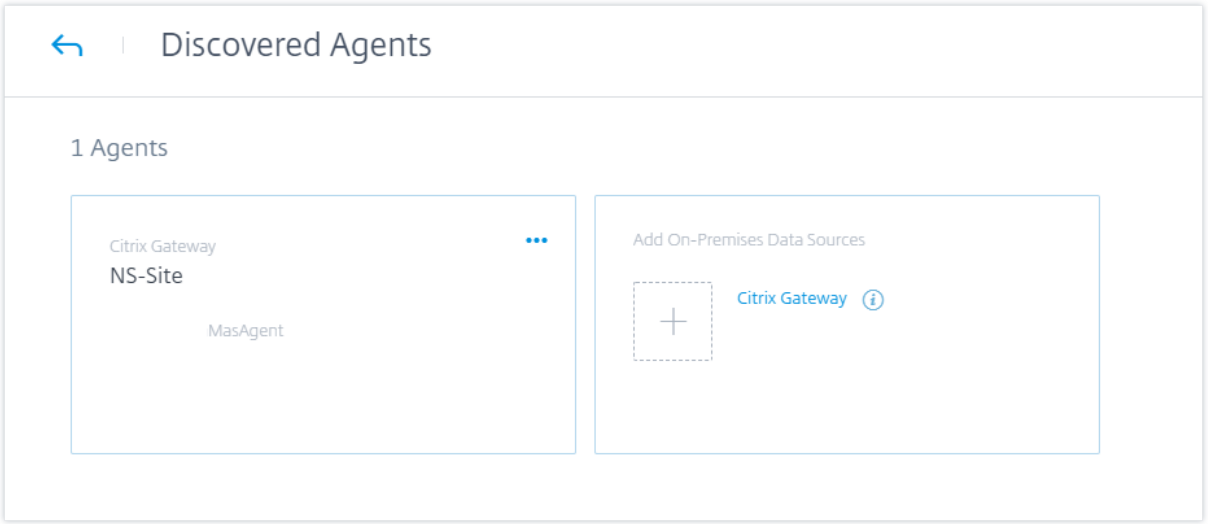


Para volver a habilitar el procesamiento de datos, haga clic **en Activar procesamiento de datos**.



Agregar más instancias de gateway

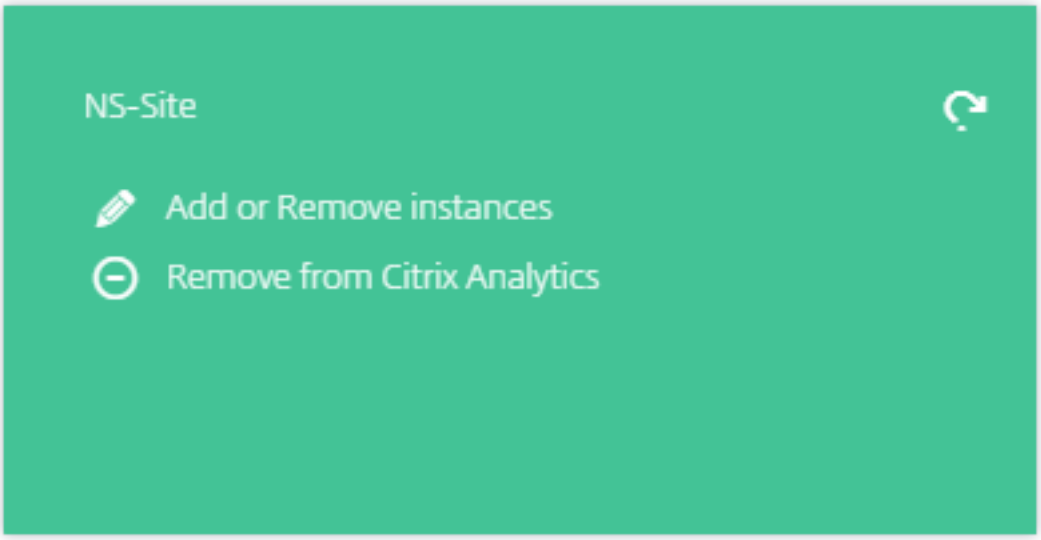
Si quiere agregar más instancias de Gateway, haga clic en el número de agentes en la tarjeta del sitio de Gateway para ver la página **Agentes descubiertos**. En el mosaico **Agregar orígenes de datos locales**, haga clic en **NetScaler Gateway**.



Administrar la fuente de datos

También puede agregar más instancias a un agente o eliminar instancias asociadas a un agente. También puede eliminar el agente y sus instancias asociadas de Citrix Analytics.

Voltee la tarjeta del sitio de un agente y realice una de las siguientes acciones:



- **Agregue o elimine instancias**. Puede agregar más instancias de Gateway a un agente y habilitar Analytics en los servidores virtuales configurados en esas instancias. También puede eliminar instancias agregadas a un agente. Al disociar una instancia de un agente, Citrix Analytics no puede comunicarse con esa instancia.
- **Eliminar de Citrix Analytics**. Después de eliminar un sitio de agente, Citrix Analytics deja de recopilar datos de las instancias asociadas a ese agente. Sin embargo, todos los datos procesados

anteriormente están disponibles durante el período de retención.

Origen de datos de Citrix Virtual Apps and Desktops

April 12, 2024

En este artículo se describen los pasos para conectar sus sitios locales de Citrix Virtual Apps and Desktops a Citrix Analytics mediante StoreFront. Los pasos de incorporación mencionados en este artículo se aplican tanto a las ofertas: Citrix Analytics for Performance (Performance Analytics) y Citrix Analytics for Security (Security Analytics).

Para conocer los pasos de incorporación específicos de cada oferta, consulte los siguientes artículos:

- Configuración de sitios locales de Citrix Virtual Apps and Desktops con Citrix Analytics for Performance
- Configuración del origen de datos Citrix Virtual Apps and Desktops y Citrix DaaS para Citrix Analytics for Security

Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante StoreFront

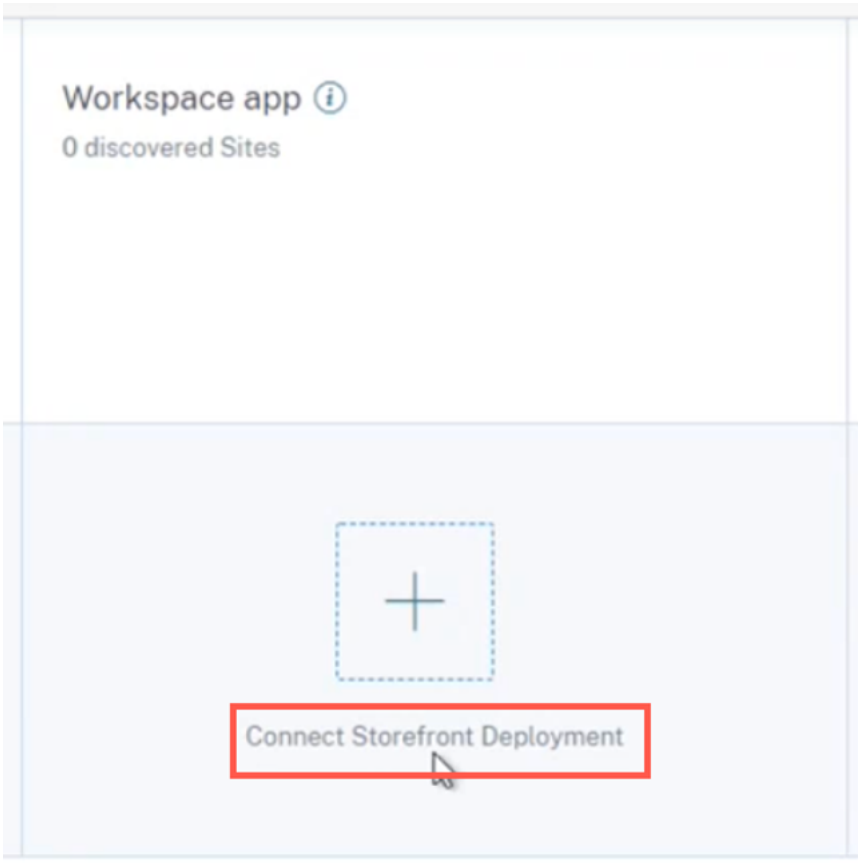
Si su organización usa una implementación local de StoreFront, debe configurar los servidores StoreFront para permitir que la aplicación Citrix Workspace envíe eventos a Citrix Analytics. Citrix Analytics procesa los eventos para proporcionar información útil sobre el rendimiento de la infraestructura de TI de Citrix y el comportamiento de los usuarios.

Para obtener más información sobre cómo configurar una implementación de StoreFront para Citrix Analytics, consulte el artículo del servicio Citrix Analytics en la documentación de StoreFront.

Anteriormente, se obligaba a los clientes que utilizaban los sitios locales de Citrix Apps and Desktops a usar la agregación de sitios para incorporar los sitios locales para Citrix Analytics for Security y Performance.

Ahora puede incorporar sitios locales de Citrix Apps and Desktops sin depender de la agregación de sitios.

Puede ver la opción **Conectar implementación de Storefront** en su aplicación de espacio de trabajo, aunque no tenga ningún sitio agregado a la agregación de sitios.



Requisitos previos

Antes de empezar, asegúrate de lo siguiente:

- La versión de StoreFront debe ser 1906 o posterior.
- La implementación de StoreFront debe poder conectarse a las siguientes direcciones:
  - https://*.cloud.com
  - https://api.analytics.cloud.com
- La implementación de StoreFront debe tener el puerto 443 abierto para las conexiones de Internet salientes. Todos los servidores proxy de la red deben permitir esta comunicación con Citrix Analytics.
- Si la implementación de StoreFront está alojada en un servidor web que utiliza un proxy web para conectarse a Internet, el proxy de cada almacén debe configurarse manualmente para permitir el tráfico saliente. StoreFront no utiliza automáticamente la configuración de proxy del servidor web host. Para obtener más información, consulte Configurar una implementación de StoreFront alojada en un servidor web que utiliza proxy HTTP.

- Se debe acceder a la implementación de StoreFront mediante uno de los siguientes clientes:
  - Citrix Receiver para sitios web en exploradores web compatibles con HTML5.

    > **Nota**
    >
    > Si es un usuario de HTML5, Citrix Virtual Apps and Desktops puede lanzar eventos cuando determinadas configuraciones estén habilitadas en StoreFront. Para obtener información sobre los pasos de configuración, consulte el artículo Instalar de la documentación de la aplicación Citrix Workspace para HTML5. Para eventos relacionados con la impresión, se deben configurar directivas adicionales en StoreFront. Para obtener más información, consulte el artículo Impresión de PDF en la documentación de la aplicación Citrix Workspace para HTML5.

  - Aplicación Citrix Workspace 1907 para Windows o posterior.
  - Aplicación Citrix Workspace 2006 para Linux o posterior.
  - Aplicación Citrix Workspace 2006 para Mac o posterior
- Si utiliza Citrix Virtual Apps and Desktops 7 1912 LTSR, la versión de StoreFront admitida es 1912.

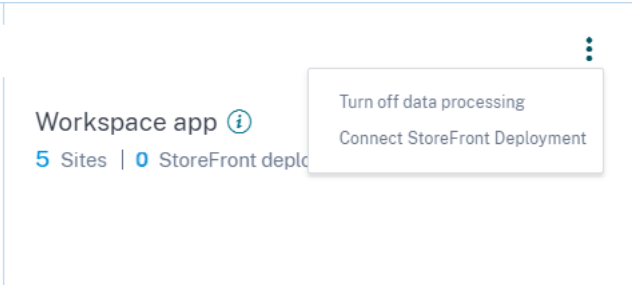
Conexión a una implementación de StoreFront

Puede conectarse a una implementación de StoreFront de las siguientes maneras:

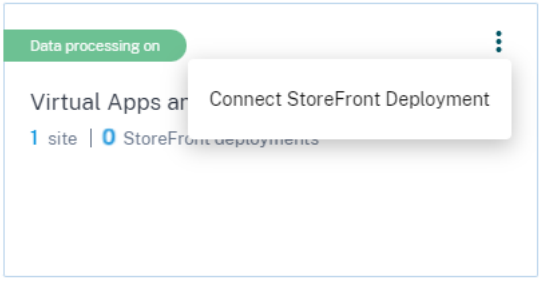
- Uso de las tarjetas de sitio **Aplicaciones y escritorios: Aplicación Workspace** y **Aplicaciones y escritorios: Supervisión**
- Uso del panel **Recomendaciones**

Conectarse mediante las tarjetas de sitio Aplicaciones y escritorios: Aplicación Workspace y Aplicaciones y escritorios: Supervisión

1. Vaya a **Configuración > Orígenes de datos > Seguridad**. En la tarjeta del sitio **Aplicaciones y escritorios: Aplicación Workspace**, haga clic en los puntos suspensivos verticales (⋮) y, a continuación, seleccione **Conectar implementación de StoreFront**.

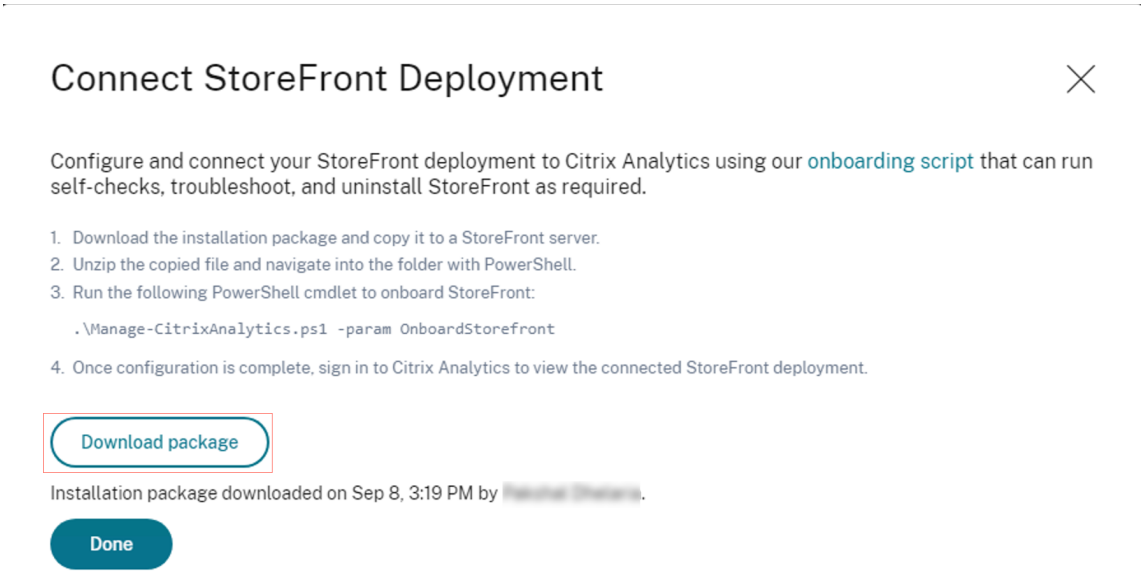


2. Vaya a **Configuración > Orígenes de datos > Rendimiento**. En la tarjeta del sitio **Aplicaciones y escritorios: Supervisión**, haga clic en los puntos suspensivos verticales (⋮) y, a continuación, seleccione **Conectar implementación de StoreFront**.



Aparece el asistente de incorporación de StoreFront o la ventana emergente **Conecar implementación de StoreFront**.

3. Haz clic en **Descargar paquete**.



> **Nota**
>
> El archivo contiene información confidencial. Guarde el archivo en un lugar seguro y protegido.

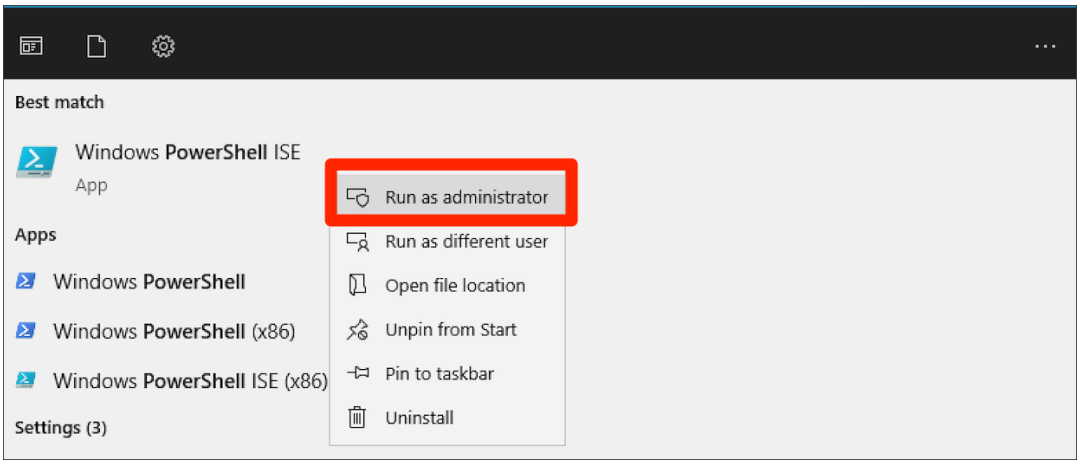
4. Para configurar la implementación de StoreFront,

   a) Copie el paquete de instalación en el servidor StoreFront.

   b) Descomprime el archivo copiado y navega hasta la carpeta de PowerShell.

   c) Debe ejecutar el siguiente comando como administrador para incorporar StoreFront:

.\Manage-CitrixAnalytics.ps1 –param OnboardStorefront



Para obtener más opciones o parámetros, consulte la secciónScript de PowerShell .

d) Abra el servidor StoreFront y ejecute el script de PowerShell.

e) Si el sitio de StoreFront no aparece en la GUI de Citrix Analytics Service incluso después de ejecutar OnBoardStoreFront, ejecute el comando iisreset.

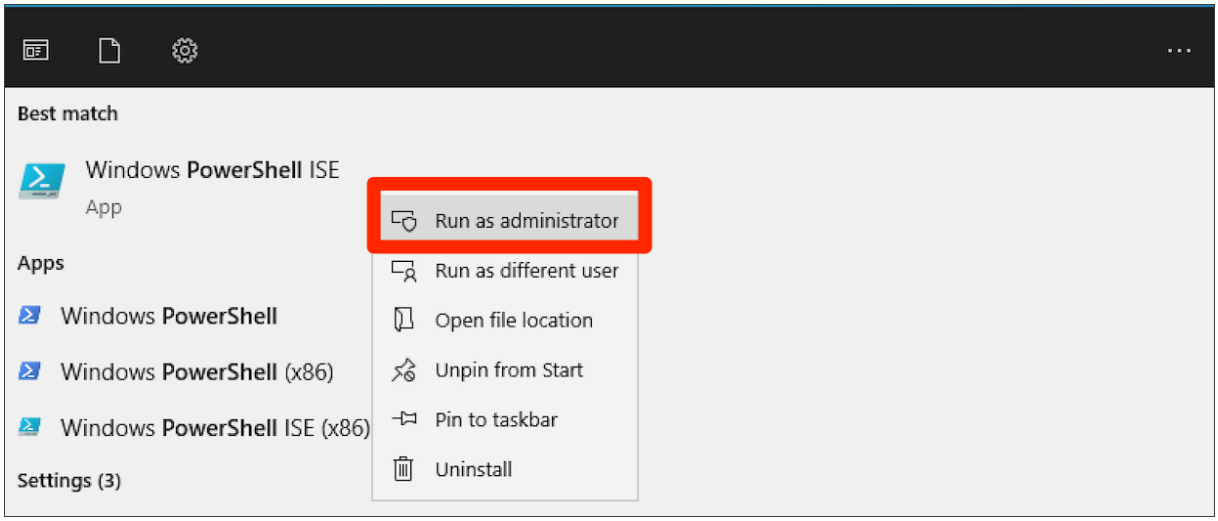
f) Inicie sesión en la GUI de Citrix Analytics Service y compruebe si el ID del clúster coincide con el registrado en la consola mediante el script.

g) Una vez realizada la configuración, inicie sesión en Citrix Analytics para ver la implementación de StoreFront conectada.

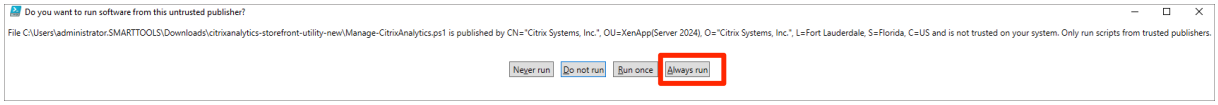
5. Cuando la configuración se haya realizado correctamente, haga clic en **Listo**.
6. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics procese los datos.

Script de PowerShell

Se ha introducido un nuevo script de PowerShell para simplificar el proceso de incorporación de StoreFront a Citrix Analytics Service. Este script de PowerShell automatiza el proceso de comprobación de requisitos previos, instalación y configuración de StoreFront. El script de PowerShell debe ejecutarse en modo administrador.



Los clientes pueden ejecutar este script de PowerShell en StoreFront para incorporarlo, eliminarlo, realizar autocomprobaciones, solucionar problemas y comprobar si la incorporación a la GUI de Citrix Analytics Service se ha realizado correctamente. Cuando un cliente ejecuta el script por primera vez, aparece un mensaje de advertencia de seguridad para confirmarlo en el editor. Seleccione la opción Ejecutar siempre si el publicador es de confianza.



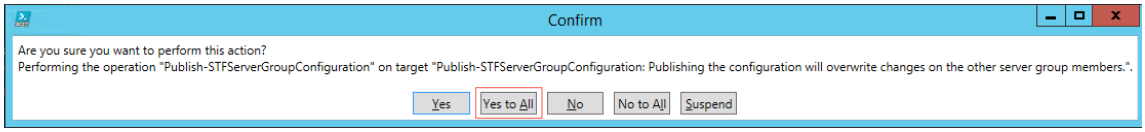
El script de PowerShell está disponible en la página de **implementación de Connect StoreFront** dentro de un archivo zip junto con el archivo StoreFrontConfiguration.json y algunos archivos CCAuth y DLL. Los registros de los scripts de PowerShell se guardan en el archivo cas-logs, en la carpeta **Descargas**.

El script de PowerShell admite los siguientes parámetros:

- **SelfCheck**: el parámetro **SelfCheck** se usa para validar que se cumplen los requisitos previos para la incorporación de StoreFront. Comprueba la instalación de StoreFront, la versión requerida, la conexión saliente, la conectividad de red del servidor cURL Analytics, la conectividad a Internet, la configuración del grupo de servidores y cualquier configuración existente de Citrix Analytics Service. Utilice el siguiente comando para ejecutar la **autocomprobación:**

  ```
  .\Manage-CitrixAnalytics.ps1 –param SelfCheck
  ```

- **OnboardStorefront**: el parámetro **OnboardStorefront** realiza rápidamente una autocomprobación para verificar la preparación para la configuración de Citrix Analytics Service. Si la configuración está lista, importa la configuración de Citrix Analytics Service y publica los cambios en otros servidores del grupo de servidores. Para un grupo de servidores, el comando PublishConfiguration se ejecuta automáticamente desde el script para publicar la configuración de StoreFront en todos los servidores de ese StoreFront. Aparecerá una ventana emergente para confirmar `PublishConfiguration` la acción. Seleccione el botón **Sí a todo**.



Una vez que la publicación de la configuración se haya completado correctamente, el script realiza una llamada a la API de Citrix Analytics Service para comprobar si StoreFront está integrado en la GUI de Citrix Analytics Service. Para invocar esta API, se requiere una clave privada para la autenticación. Para generar esta clave privada, necesita los archivos CCauth y dll, y la credencial que está disponible en el archivo JSON descargado.

> **Nota:**
>
> Una vez finalizado el proceso de incorporación de StoreFront, StoreFront puede tardar de dos a cinco minutos en aparecer en la GUI de Citrix Analytics Service. Si el sitio de StoreFront no aparece en la GUI de Citrix Analytics Service, debe realizar un IISRESET para restablecer los servicios de información de Internet.

Use el siguiente comando para ejecutar **OnboardStoreFront**:

```
.\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
```

- **ISonBoarded**: el parámetro **ISonBoarded** se usa para comprobar si StoreFront está incorporado a la GUI de Citrix Analytics Service. El script espera un minuto antes de salir; sin embargo, StoreFront puede tardar hasta cinco minutos en aparecer en la GUI una vez que se haya integrado correctamente. Debe ejecutar este comando para verificarlo. Este comando también tiene la dependencia de los archivos CCAuth y dll. Utilice el siguiente comando para ejecutar el **ISonBoarded**:

  ```
  .\Manage-CitrixAnalytics.ps1 –param IsOnboarded
  ```

- **Solución**de problemas: Tras esperar cinco minutos, si el sitio de StoreFront no aparece en la GUI de Citrix Analytics Service, debe realizar un IISRESET para restablecer los servicios de información de Internet. Si el sitio de StoreFront sigue sin aparecer en la GUI, use el parámetro **Troubleshoot**. Le ayuda a solucionar cualquier problema de conectividad y a recopilar registros. Utilice el siguiente comando para ejecutar la **solución de problemas**:

  ```
  .\Manage-CitrixAnalytics.ps1 –param TroubleShoot
  ```

  El parámetro de solución de problemas es útil para los dos casos de uso siguientes:

  - **Caso de uso 1**: Como parte de la autocomprobación, si el CURLAnalytics ha fallado, se crea una regla de firewall. Esta regla de firewall abre un puerto 443 y verifica su conectividad con Analytics. Si no es así, significa que no se puede acceder al servidor de Analytics y el script sale de aquí. Vuelva a ejecutar el script una vez que se restablezca la conectividad con Citrix Analytics Service.

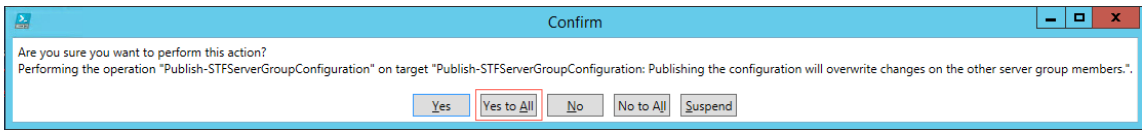
- **Caso de uso 2**: Si la cURL funciona correctamente y, sin embargo, el sitio de StoreFront no se refleja en la GUI, el administrador debe descargar el archivo zip de la herramienta DebugView desde Download DebugView, descomprimirlo y colocarlo en la carpeta **Descargas**. El script de PowerShell primero desinstala Citrix Analytics Service si ya está configurado. Permite el registro detallado. A continuación, inicia la herramienta DebugView y vuelve a instalar Citrix Analytics Service. Por último, detiene DebugView y desactiva el registro verboso.

Los registros de la vista de depuración se pueden capturar y compartir con Citrix Support. El administrador de Citrix sigue depurando e intenta averiguar el problema y resolverlo. Los registros se generan y guardan como un archivo de registro dentro de la carpeta DebugView.

Debe compartir los tres archivos de registro siguientes con el administrador de Citrix:

- El archivo de registro de DebugView (Downloads\ DebugView\ log)
- El archivo de registro de StoreFront (C:\Archivos de programa\Citrix\Receiver StoreFront\Admin\trace)
- El archivo de registros CAS. Estos registros se generan como parte de la ejecución del script y se guardan en la carpeta **Descargas > cas-logs**.

En el caso de un grupo de servidores, el `PublishConfiguration` comando se ejecuta automáticamente cuando el script intenta eliminar o incorporar StoreFront. El comando PublishConfiguration ayuda a publicar la configuración de StoreFront en todos los servidores de ese StoreFront. Aparecerá una ventana emergente para confirmar esta acción. Seleccione el botón **Sí a todo**.



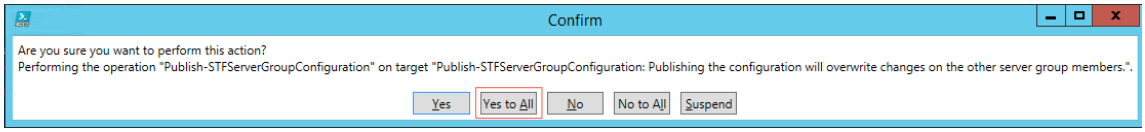
- **DeboardStorefront**: el parámetro DeboardStorefront se usa para anular la incorporación del servidor StoreFront de Citrix Analytics Service. Use el siguiente comando para ejecutar DeboardStoreFront:

```
.\Manage-CitrixAnalytics.ps1 –param DeboardStoreFront
```

El script de PowerShell primero elimina todas las configuraciones de Citrix Analytics Service de StoreFront y comprueba que la eliminación se ha realizado correctamente. A continuación, comprueba si el ServerGroup está presente y, a continuación, publica la configuración para que las configuraciones eliminadas se publiquen en todos los StoreFront. Por último, invoca DeleteSiteOnboarded. Si el sitio no se elimina de la GUI de Citrix Analytics Service, debe eliminar manualmente el sitio de StoreFront con StoreFront Deployment y de la tarjeta de sitio de la aplicación Workspace en la implementación de StoreFront.

Para un grupo de servidores, el comando PublishConfiguration se ejecuta automáticamente

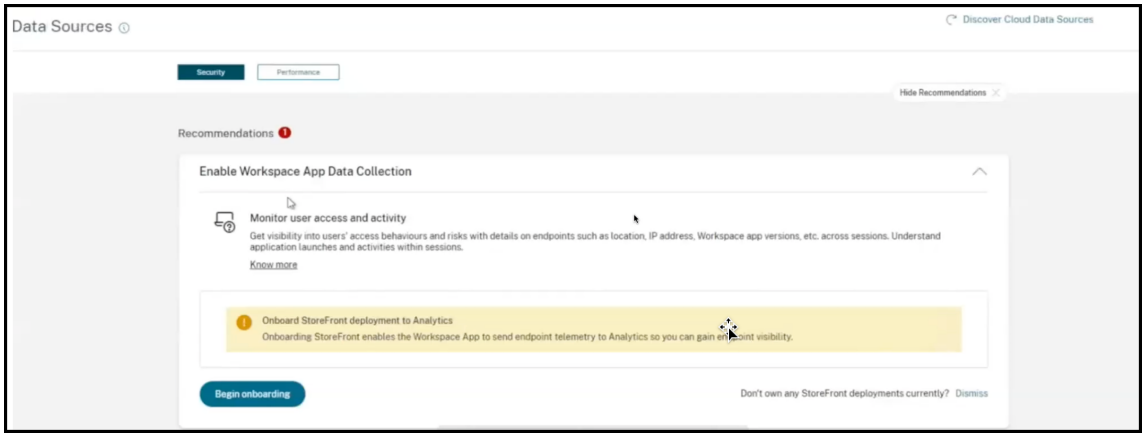
desde el script para publicar la configuración de StoreFront en todos los servidores de ese StoreFront. Aparecerá una ventana emergente para confirmar esta acción. Seleccione el botón **Sí a todo**.



Conéctese mediante el panel Recomendaciones

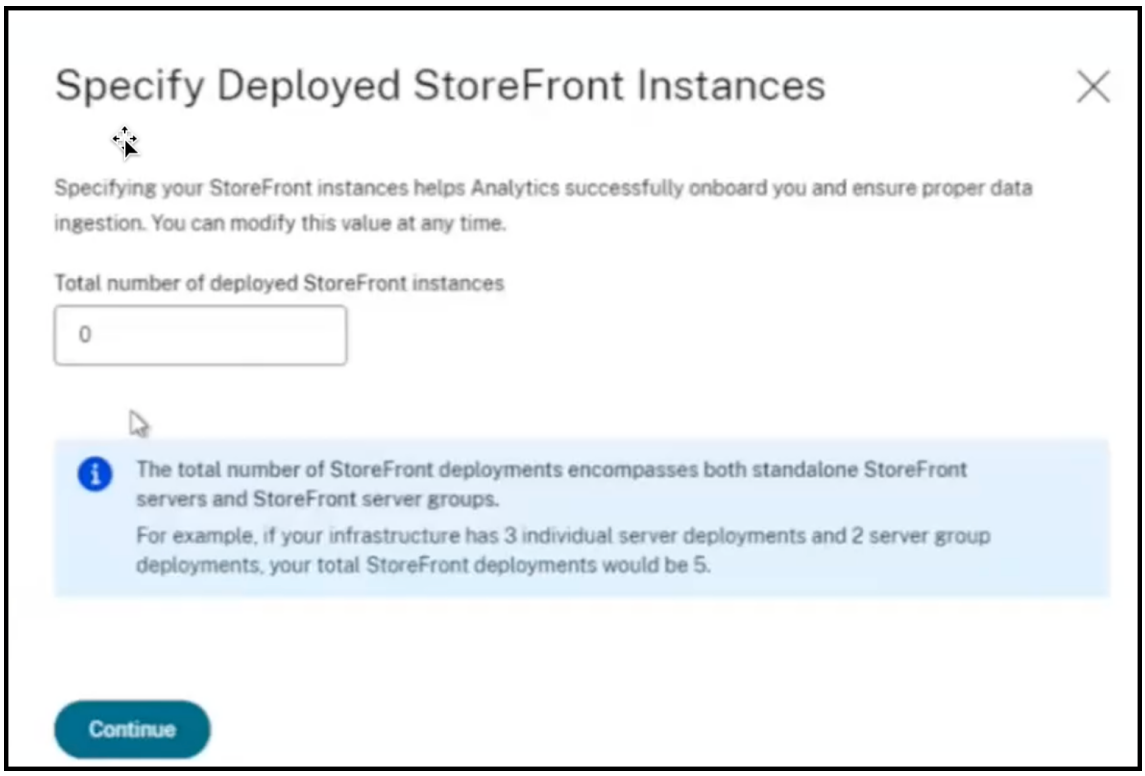
El panel **Recomendaciones** de la página **Orígenes de datos** informa al usuario sobre la importancia de incorporar los orígenes de datos. Ayuda al usuario a incorporar fácilmente los orígenes de datos y también le brinda la opción de revisar y asegurarse de que ha incorporado todos los orígenes de datos disponibles.

1. Si utiliza la oferta de análisis de seguridad, seleccione **Configuración > Orígenes de datos > Seguridad**.
2. Si utiliza la oferta Performance Analytics, vaya a **Configuración > Orígenes de datos > Rendimiento**.
3. En la página **Orígenes de datos**, revise la información y las recomendaciones del panel **Recomendaciones** para incorporar la implementación de Storefront.



> **Nota**
>
> La incorporación de un origen de datos de StoreFront permite a la aplicación Workspace enviar datos de telemetría sobre la visibilidad de los dispositivos de punto final a Analytics.

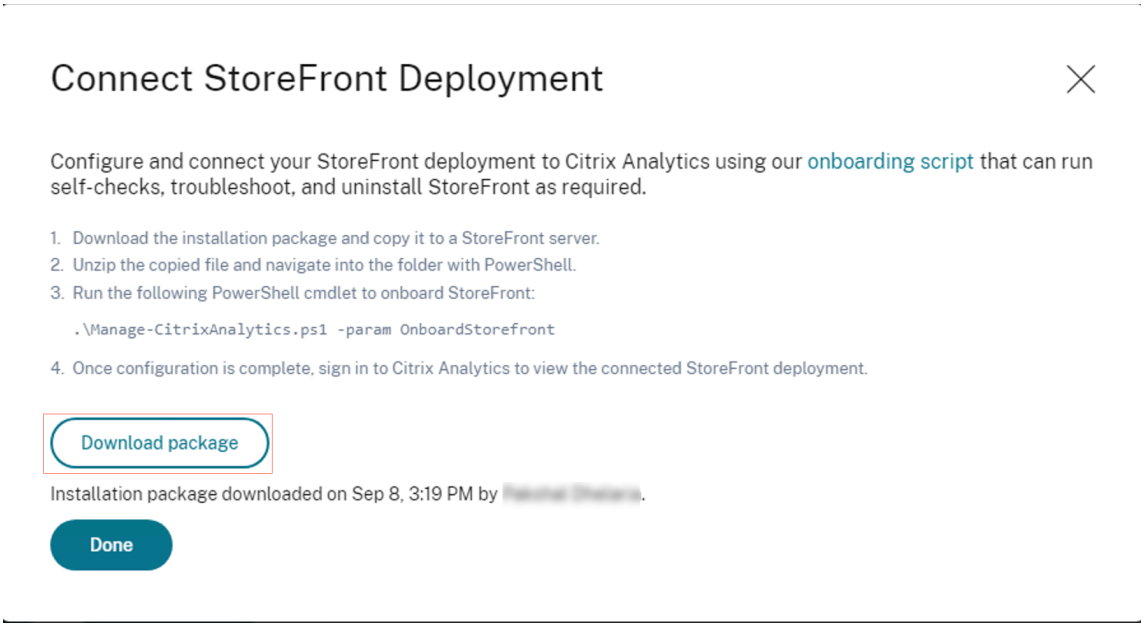
4. Haga clic en **Comenzar la incorporación**. Aparece la página **Especificar instancias de Storefront implementadas**.



5. Para garantizar que Analytics incorpore correctamente el origen de datos, especifique el **total de instancias de StoreFront implementadas**.

   > **Nota:**
   >
   > La **cantidad total de instancias de StoreFront implementadas** es la cantidad total de grupos de StoreFront y no la cantidad de servidores StoreFront individuales.

6. Haga clic en **Continuar**. Aparece el asistente de incorporación de StoreFront o la ventana emergente **Conecar implementación de StoreFront**.
7. En la página de **implementación de Connect StoreFront**, haga clic en Descargar paquete para descargar el paquete de instalación.



> **Notas**
>
> El archivo contiene información confidencial. Guarde el archivo en un lugar seguro y protegido.
>
> Puede descargar un paquete y usarlo solo para incorporar un grupo de StoreFront. Si tiene varios grupos de StoreFront, debe descargar el paquete por separado para cada grupo. Una vez finalizada la incorporación de un grupo de StoreFront con un paquete, vuelva a descargar el paquete y continúe con la incorporación del siguiente grupo de StoreFront.
>
> Si la incorporación de StoreFront no se completa correctamente en un plazo de dos días con un paquete debido a algún problema, debe volver a descargar un paquete nuevo transcurridos dos días. Esto se debe a que la clave del paquete caducará si no se ha incorporado correctamente en un plazo de dos días.

8. Para configurar la implementación de StoreFront,

   a) Copie el paquete de instalación en el servidor StoreFront.

   b) Descomprime el archivo copiado y navega hasta la carpeta de PowerShell.

   c) Ejecute el siguiente comando para incorporar StoreFront:

   ```
   .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
   ```

   d) Abra el servidor StoreFront y ejecute el script de PowerShell.

   e) Si el sitio de StoreFront no aparece en la GUI de Citrix Analytics Service, ejecute el siguiente comando:

   ```
   Execute iisreset
   ```


f) Registre y verifique el ID de clúster que está disponible en el script de PowerShell.

g) Una vez realizada la configuración, inicie sesión en Citrix Analytics para ver la implementación de StoreFront conectada.

9. Cuando la configuración se haya realizado correctamente, haga clic en **Listo**.

Si realiza la incorporación a través del panel **Recomendaciones**, el sistema obtiene el número de implementaciones de StoreFront que ha incorporado al servicio Citrix Analytics. Aparece el panel **Recomendaciones** y puede revisar las implementaciones de StoreFront integradas. Puede revisar el mensaje en el panel **Recomendaciones** y hacer clic en **Marcar como completado**.

> **Nota**
>
> El panel **Recomendaciones** y los mensajes solo desaparecen cuando se han incorporado todas las implementaciones declaradas de Storefront.

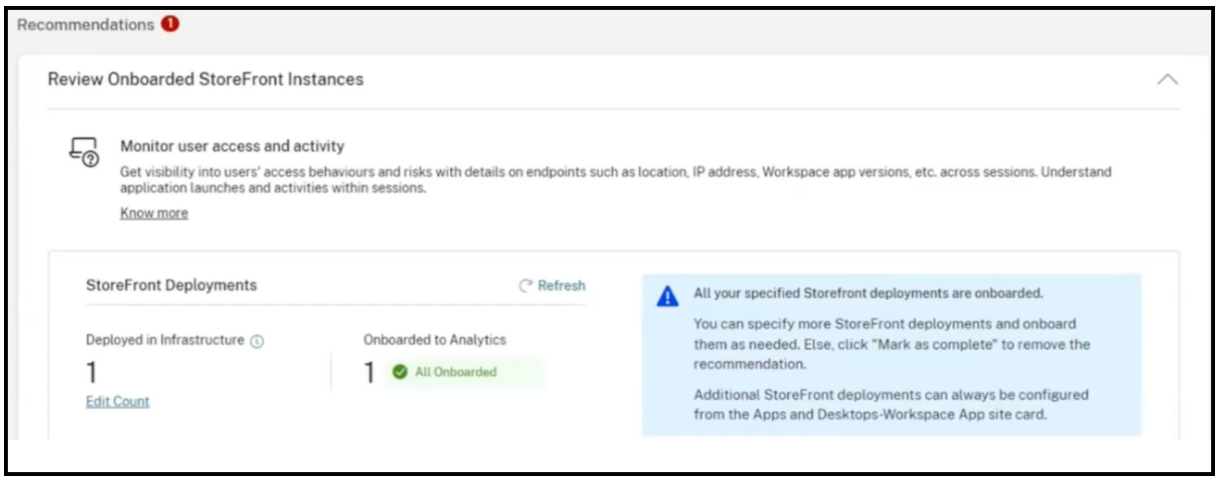
1. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics procese los datos.

Revisar el panel Recomendaciones

Puede comparar la cantidad de implementaciones de StoreFront declaradas con la cantidad de implementaciones de StoreFront incorporadas en el panel **Recomendaciones**.

Si la cantidad de implementaciones de StoreFront declarados es la misma que la cantidad de implementaciones de StoreFront incorporadas, aparece el mensaje **All Onboarded** que indica que todas las implementaciones de StoreFront están incorporadas. Puede revisar el mensaje en el panel **Recomendaciones** y hacer clic en **Marcar como completado**.

> **Nota**
>
> Si quiere incorporar más implementaciones de StoreFront, haga clic en **Ver los pasos de incorporación** y aparecerá de nuevo el asistente de incorporación de StoreFront o la ventana emergente **Conectar implementación de StoreFront**.



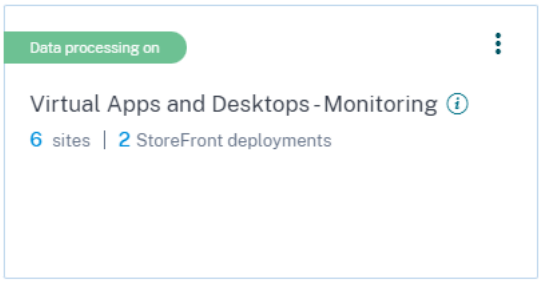
Si la cantidad de implementaciones de StoreFront declaradas es inferior a la cantidad de implementaciones de StoreFront incorporadas, haga clic en **Modificar recuento**, y aparecerá la página **Especificar instancias de StoreFront implementadas**. A continuación, puede introducir la **cantidad total de instancias de StoreFront implementadas** y hacer clic en **Continuar**. Aparecerán de nuevo el asistente de incorporación de StoreFront o la ventana emergente **Conectar implementación de StoreFront**. Siga los pasos para incorporar más implementaciones de StoreFront.

> **Nota:**
>
> La **cantidad total de instancias de StoreFront implementadas** es la cantidad total de grupos de StoreFront y no la cantidad de servidores StoreFront individuales.

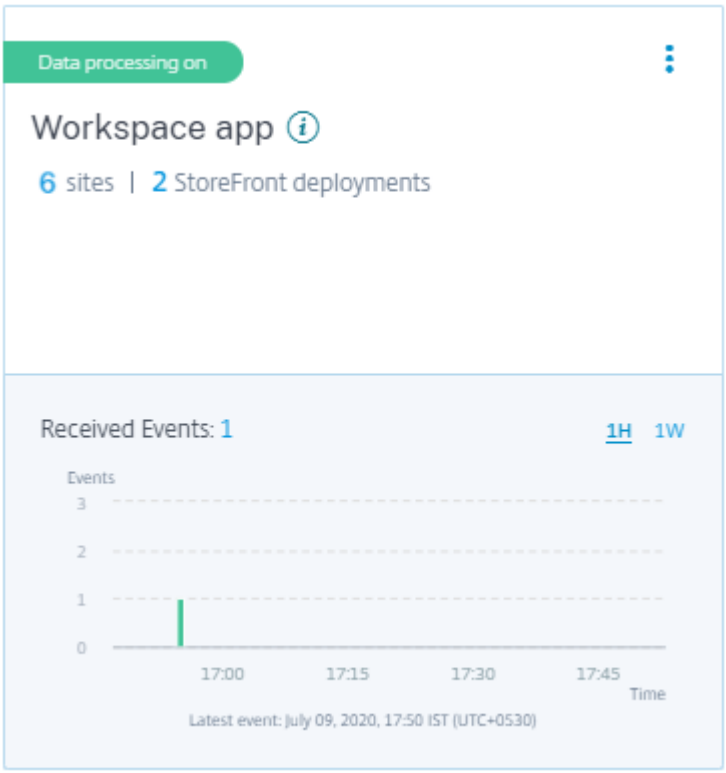
Ver implementaciones de StoreFront conectadas

Las implementaciones de StoreFront aparecen en la tarjeta del sitio solo si la configuración se realiza correctamente. La tarjeta del sitio muestra cuántas implementaciones de StoreFront han establecido conexiones con Citrix Analytics.

- Si utiliza la oferta Análisis de rendimiento, verá la siguiente información en la tarjeta de sitio de **supervisión de aplicaciones y escritorios** :

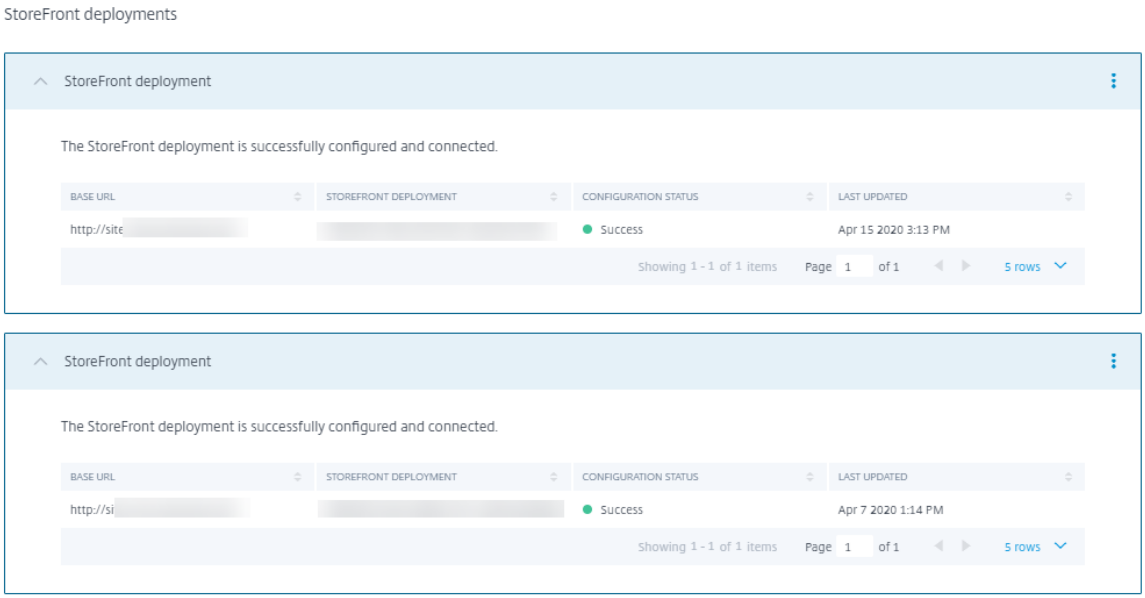


- Si utiliza la oferta Security Analytics, verá la siguiente información en la tarjeta del sitio de la **aplicación Workspace** :



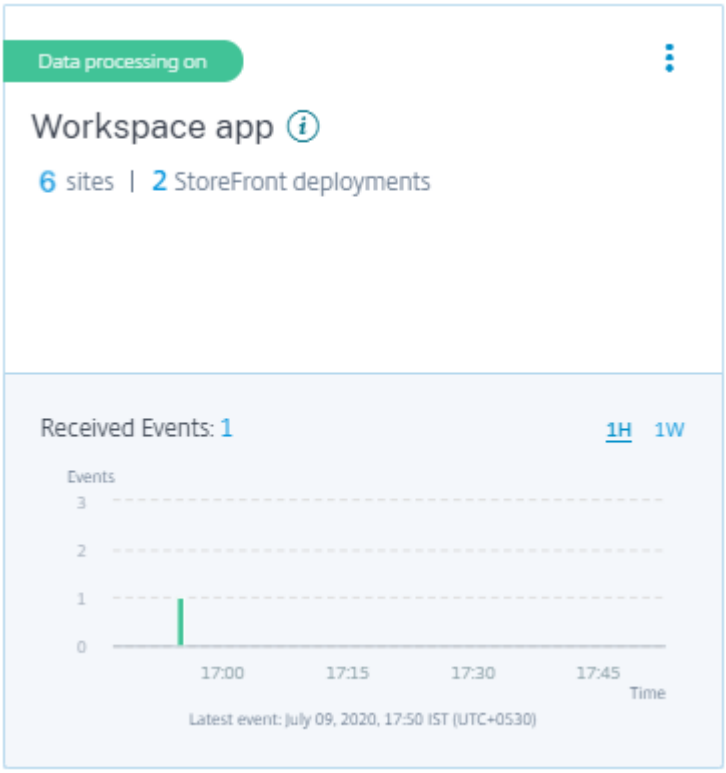
Haga clic en el número de implementaciones de StoreFront de la tarjeta de sitio para ver los grupos de servidores.

Cada implementación de StoreFront se representa mediante una URL base y un ServerGroupID.



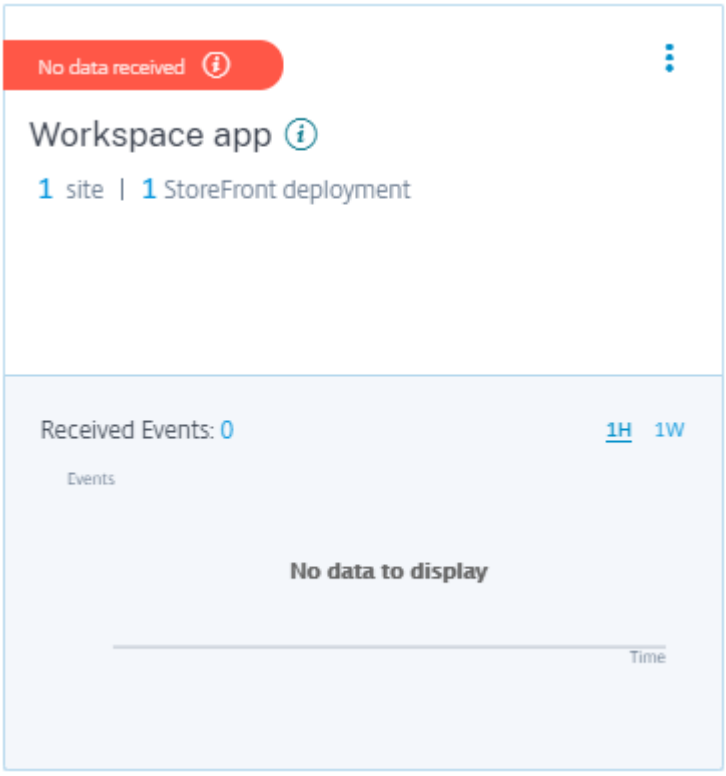
Si utiliza la oferta de Security Analytics, la tarjeta del sitio también muestra la siguiente información sobre los eventos recibidos:

- Los eventos recibidos de las implementaciones de StoreFront durante la última hora, que es la selección de tiempo predeterminada. También puede seleccionar 1 semana (1 W) y ver los datos. Haga clic en el número de eventos recibidos para verlos en la página de búsqueda de autoservicio.



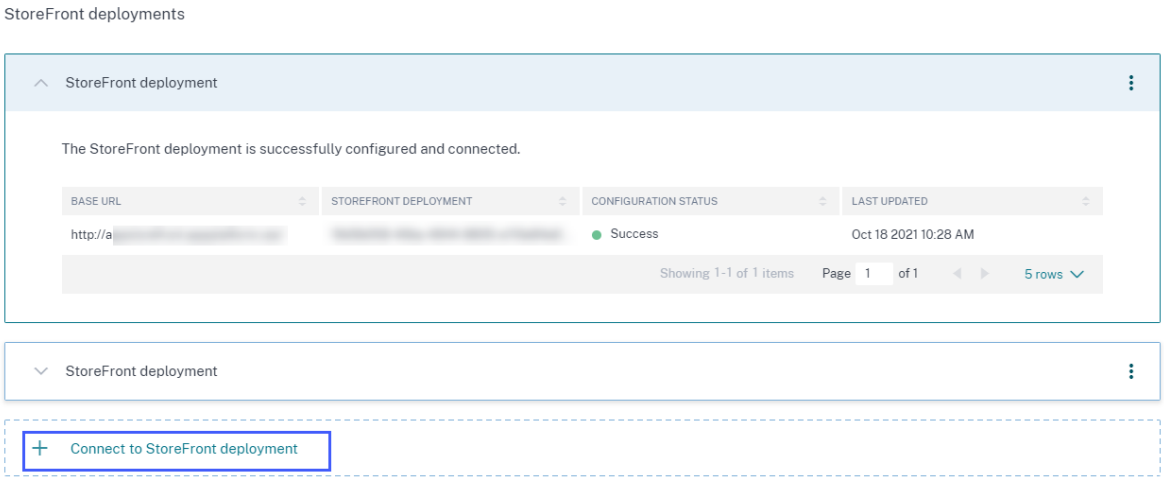
- Después de habilitar el procesamiento de datos, es posible que la tarjeta del sitio muestre el estado **Sin datos recibidos**. Este estado aparece por dos motivos:

  1. Si activó el procesamiento de datos por primera vez, los eventos tardan un tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Data processing on**. Si el estado no cambia después de algún tiempo, actualice la página **Orígenes de datos**.
  2. Citrix Analytics no recibió ningún evento del origen de datos en la última hora.



Agregar o quitar implementaciones de StoreFront

Para agregar una implementación de StoreFront, haga clic en **Conectarse a implementaciones de StoreFront** en la sección **Implementaciones de StoreFront**. Descargue el archivo de configuración y siga los pasos para configurar una implementación de StoreFront.



Para detener la transmisión de eventos desde una implementación de StoreFront configurada y quitarla de Citrix Analytics:

1. Vaya a la implementación de StoreFront que quiere quitar de Citrix Analytics. Ejecute el siguiente comando para eliminar los valores de configuración del servidor StoreFront:

```
Remove-STFCasConfiguration
```

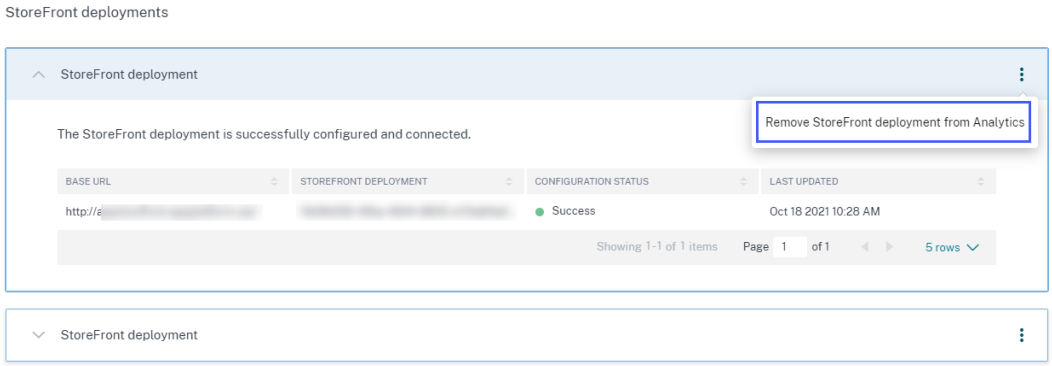
2. Si utiliza la implementación multiservidor, ejecute el siguiente comando para propagar los cambios y eliminar los valores de configuración de todos los servidores del grupo de servidores StoreFront:

```
Publish-STFServerGroupConfiguration
```

3. Ejecute el siguiente comando para comprobar que los valores de configuración se han quitado correctamente. El comando no devuelve nada si la configuración se ha quitado correctamente.

```
Get-STFCasConfiguration
```

4. Vuelva a iniciar sesión en Citrix Analytics y elija la implementación de StoreFront en la sección **Implementaciones de StoreFront**. Haga clic en los puntos suspensivos verticales (⋮) y seleccione **Eliminar implementaciones de StoreFront de Analytics**.



> **Nota**
>
> Ejecute los comandos especificados en la implementación de StoreFront antes de quitarlo de Citrix Analytics. Si no ejecuta los comandos, Citrix Analytics sigue recibiendo los eventos y la implementación de StoreFront se agrega de nuevo en el siguiente ciclo de agrupación de eventos.

Configurar una implementación de StoreFront alojada en un servidor web que utiliza proxy HTTP

Si un StoreFront está alojado en un servidor web que utiliza un proxy web para conectarse a Internet, el almacén debe configurarse manualmente para registrarse en Citrix Analytics. Esta configuración requiere que agregue una sección <system.net> al archivo web.config del almacén. Debe configurar todos los almacenes de la implementación de StoreFront que envían eventos a Citrix Analytics.

Hay dos métodos mediante los cuales puede agregar la sección <system.net> al archivo web.config del almacén:

- Establezca la configuración del proxy de almacén mediante PowerShell para uno o varios almacenes (método recomendado).
- Agregue manualmente una sección <system.net> al archivo web.config del almacén.

Para obtener más información sobre estos métodos, consulte el artículo Configurar StoreFront para usar un proxy web para ponerse en contacto con Citrix Cloud y registrarse en Citrix Analytics de la documentación de StoreFront.

Reglamentación de datos

December 7, 2023

En esta sección se proporciona información sobre la recopilación, el almacenamiento y la retención de registros por parte del servicio Citrix Analytics. Todos los términos en mayúsculas que no estén definidos en la sección Definiciones tienen el significado especificado en el Acuerdo de servicios de usuario final de Citrix.

Citrix Analytics está diseñado para proporcionar a los clientes información sobre las actividades de su entorno informático Citrix. Citrix Analytics permite a los administradores de seguridad elegir los registros que desean supervisar y tomar medidas directas en función de la actividad registrada. Esta información ayuda a los administradores de seguridad a administrar el acceso a sus entornos informáticos y a proteger el contenido del cliente en el entorno informático del cliente.

Residencia de datos

Los registros de Citrix Analytics se mantienen por separado de los orígenes de datos y se agregan en varios entornos de Microsoft Azure Cloud, que se encuentran en las regiones de Estados Unidos, la Unión Europea y Asia Pacífico Sur. El almacenamiento de los registros depende de la región de origen seleccionada por los administradores de Citrix Cloud al incorporar sus organizaciones a Citrix Cloud. Por ejemplo, si elige la **región europea** al incorporar su organización a Citrix Cloud, los registros de Citrix Analytics se almacenan en entornos Microsoft Azure de la Unión Europea.

Para obtener más información, consulte Administración de registros y contenido de clientes de Citrix Cloud Services y consideraciones geográficas.

Recopilación de datos

Los servicios de Citrix Cloud están instrumentados para transmitir registros a Citrix Analytics. Los registros se recopilan de estos orígenes de datos:

- Citrix ADC (local) junto con la suscripción a Citrix Application Delivery Management
- Citrix Endpoint Management
- Citrix Gateway (local)
- Proveedor de identidades Citrix
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

Transmisión de datos

Los registros de Citrix Cloud se transmiten de forma segura a Citrix Analytics. Cuando el administrador del entorno del cliente habilita explícitamente Citrix Analytics, estos registros se analizan y almacenan en una base de datos de clientes. Lo mismo se aplica a Citrix Virtual Apps and Desktops los orígenes de datos con Citrix Workspace configurado.

En el caso de los orígenes de datos de Citrix ADC, la transmisión de registros se inicia únicamente cuando el administrador habilita explícitamente Citrix Analytics para el origen de datos específica.

Control de datos

El administrador puede activar o desactivar los registros enviados a Citrix Analytics en cualquier momento.

Cuando se desactiva para los orígenes de datos locales de Citrix ADC, se detiene la comunicación entre el origen de datos ADC concreta y Citrix Analytics.

Cuando se desactiva todo para otros orígenes de datos, los registros del origen de datos concreta ya no se analizan ni se almacenan en Citrix Analytics.

Retención de datos

Los registros de Citrix Analytics se conservan de forma identificable durante un máximo de 13 meses o 396 días. Todos los registros y datos analíticos asociados, como perfiles de riesgo de usuario, detalles de puntuación de riesgo de usuario, detalles de eventos de riesgo de usuario, lista de seguimiento de usuarios, acciones de usuario y perfil de usuario, se conservan durante este período.

Por ejemplo, si ha habilitado Analytics en un origen de datos el 1 de enero de 2021, de forma predeterminada, los datos recopilados el 1 de enero de 2021 se conservarán en Citrix Analytics hasta el 31 de enero de 2022. Del mismo modo, los datos recopilados el 15 de enero de 2021 se conservarán hasta el 15 de febrero de 2022, etc.

Estos datos se almacenan durante el período de retención de datos predeterminado incluso después de haber desactivado el procesamiento de datos para el origen de datos o después de haber eliminado el origen de datos de Citrix Analytics.

Citrix Analytics elimina todo el contenido del cliente 90 días después del vencimiento de la suscripción o del período de prueba.

Exportación de datos

En esta sección se explican los datos exportados desde Citrix Analytics for Security y Citrix Analytics for Performance.

Citrix Analytics for Performance recopila y analiza las métricas de rendimiento de los orígenes de datos.

Puede descargar los datos de la página de búsqueda de autoservicio como un archivo CSV.

Citrix Analytics for Security recopila eventos de usuarios de varios productos (orígenes de datos). Estos eventos se procesan para proporcionar visibilidad del comportamiento con riesgos e inusual de los usuarios. Puede exportar estos datos procesados relacionados con las perspectivas de riesgo de los usuarios y los eventos de los usuarios a su servicio de Administración de eventos e información del sistema (SIEM).

Actualmente, los datos se pueden exportar de dos maneras desde Citrix Analytics for Security:

- Integración de Citrix Analytics for Security con su servicio SIEM
- Descargar los datos de la página de búsqueda de autoservicio como un archivo CSV.

Cuando integra Citrix Analytics for Security con su servicio SIEM, los datos se envían a su servicio SIEM mediante el tema Kafka en dirección norte o un conector de datos basado en Logstash.

Actualmente, puede integrarse con los siguientes servicios SIEM:

- Splunk (conectándose a través del complemento Citrix Analytics)

- Cualquier servicio SIEM que admita conectores de datos basados en temas de Kafka o Logstash, como Elasticsearch y Microsoft Azure Sentinel

También puede exportar los datos a su servicio SIEM mediante un archivo CSV. En la página de búsqueda de autoservicio, puede ver los datos (eventos de usuario) de una fuente de datos y descargar estos datos como un archivo CSV. Para obtener más información sobre el archivo CSV, consulte Búsqueda de autoservicio.

> **Importante**
>
> Después de exportar los datos a su servicio SIEM, Citrix no es responsable de la seguridad, el almacenamiento, la administración y el uso de los datos exportados en su entorno SIEM.

Puede activar o desactivar la transmisión de datos desde Citrix Analytics for Security a su servicio SIEM.

Para obtener información sobre los datos procesados y la integración de SIEM, consulte Integración de administración de eventos e información de seguridad (SIEM) y Formato de datos de Citrix Analytics para SIEM.

anexo de seguridad de Citrix Services

En la exposición de seguridad de Citrix Services se incluye información detallada sobre los controles de seguridad aplicados a Citrix Analytics, incluidos el acceso y la autenticación, la administración de programas de seguridad, la continuidad del negocio y la administración de incidentes.

Definiciones

Por**contenido del cliente** se entiende cualquier dato cargado en una cuenta de cliente para su almacenamiento o datos en un entorno de cliente al que Citrix tenga acceso para prestar los Servicios.

Registro significa un registro de eventos relacionados con los servicios mencionados, incluidos los registros que miden el rendimiento, la estabilidad, el uso, la seguridad y la asistencia.

Servicios significa los Citrix Cloud Services descritos anteriormente para los fines de Citrix Analytics.

Acuerdo de recopilación de datos

Al cargar sus datos en Citrix Analytics y utilizar las funciones de Citrix Analytics, acepta y acepta que Citrix recopile, almacene, transmita, mantenga, procese y use información técnica, de usuario o relacionada sobre sus productos y servicios Citrix.

Citrix siempre trata la información recibida de acuerdo con la Directiva de privacidad de Citrix.

Apéndice: registros recopilados

- Registros de Citrix Analytics para seguridad
- Registros de Citrix Analytics para rendimiento

Registros de Citrix Analytics para seguridad

Registros generales

En general, los registros de Citrix Analytics contienen los siguientes puntos de datos de identificación de encabezados:

- Claves de encabezado
- Identificación de dispositivos
- Identificación
- Dirección IP
- Organización
- Producto
- Versión del producto
- Hora del sistema
- Identificación del arrendatario
- Tipo
- Usuario: correo electrónico, ID, nombre de cuenta SAM, dominio, UPN
- Versión

Registros del servicio Citrix Endpoint Management

Los registros del servicio Citrix Endpoint Management contienen los siguientes puntos de datos:

- Cumplimiento de normativas
- Propiedad corporativa
- ID de dispositivo
- Modelo de dispositivo
- Tipo de dispositivo

- Latitud geográfica
- Longitud geográfica
- Nombre de host
- IMEI
- Dirección IP
- Prisión rota
- Última actividad
- Modo de gestión
- Sistema operativo
- Versión del sistema operativo
- Información de la plataforma
- Motivo
- Número de serie
- Supervisado

Registros de Citrix Secure Private Access

- AAA User Name
- Auth Policy Action Name
- Authentication Session ID
- Request URL
- URL Category Policy Name
- VPN Session ID
- Vserver IP
- AAA User Email ID
- Actual Template Code
- App FQDN
- Nombre de la aplicación
- App Name Vserver LS
- Application Flags

- Authentication Type
- Authentication Stage
- Authentication Status Code
- Dirección IPv4 Dst del servidor back-end
- Dirección IPv4 del servidor back-end
- Dirección IPv6 del servidor back-end
- Category Domain Name
- Category Domain Source
- Client IP
- Client MSS
- Client Fast Retx Count
- Client TCP Jitter
- Client TCP Packets Retransmited
- Client TCP RTO Count
- Client TCP Zero Window Count
- Clt Flow Flags Rx
- Clt Flow Flags Tx
- Clt TCP Flags Rx
- Clt TCP Flags Tx
- Connection Chain Hop Count
- Connection Chain ID
- Egress Interface
- Exporting Process ID
- Flow Flags Rx
- Flow Flags Tx
- HTTP Content Type
- HTTP Domain Name
- HTTP Req Authorization
- HTTP Req Cookie

- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP Req Host
- HTTP Req Method
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP Req Referer
- HTTP Req URL
- HTTP Req XForwarded For
- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP Res Location
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie
- HTTP Rsp Len
- HTTP Rsp Status
- HTTP Transaction End Time
- HTTP Transaction ID
- IC Cont Grp Name
- IC Flags
- IC No Store Flags
- IC Policy Name
- Ingress Interface Client
- ID de aplicación del NetScaler Gateway Service
- Nombre de aplicación del NetScaler Gateway Service
- Tipo de aplicación del NetScaler Gateway Service
- ID de partición de NetScaler
- Observation Domain ID

- Observation Point ID
- Origin Res Status
- Origin Rsp Len
- Protocol Identifier
- Rate Limit Identifier Name
- Tipo de registro
- Responder Action Type
- Response Media Type
- Srv Flow Flags Rx
- Srv Flow Flags Tx
- Srvr Fast Retx Count
- Fluctuación del servidor TCP
- Paquetes TCP de Srvr retransmitidos
- Recuento Rto de TCP de servidor
- Recuento cero de ventanas Srvr TCP
- SSL Cipher Value BE
- SSL Cipher Value FE
- SSL Client Cert Size BE
- SSL Client Cert Size FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL Err App Name
- SSL Err Flag
- SSL Flags BE
- SSL Flags FE
- SSL Handshake Error Msg
- SSL Server Cert Size BE
- SSL Server Cert Size FE
- SSL Session ID BE

- SSL Session ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain Category Group
- SSL iDomain Name
- SSL iDomain Reputation
- SSL iExecuted Action
- SSL iPolicy Action
- SSL iReason For Action
- SSL iURL Set Matched
- SSL iURL Set Private
- Subscriber Identifier
- Svr Tcp Flags Rx
- Svr Tcp Flags Tx
- Tenant Name
- Tracing Req Parent Span ID
- Tracing Req Span ID
- Tracing Trace ID
- Trans Clt Dst IPv4 Address
- Trans Clt Dst IPv6 Address
- Trans Clt Dst Port
- Trans Clt Flow End Usec Rx
- Trans Clt Flow End Usec Tx
- Trans Clt Flow Start Usec Rx
- Trans Clt Flow Start Usec Tx
- Trans Clt IPv4 Address

- Trans Clt IPv6 Address
- Trans Clt Packet Tot Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- Trans Clt RTT
- Trans Clt Src Port
- Trans Clt Tot Rx Oct Cnt
- Trans Clt Tot Tx Oct Cnt
- Trans Info
- Trans Srv Dst Port
- Trans Srv Packet Tot Cnt Rx
- Trans Srv Packet Tot Cnt Tx
- Trans Srv Src Port
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- ID de transacción
- URL Category
- URL Category Group
- URL Category Reputation
- URL Category Action Reason
- URL Set Matched
- URL set Private
- URL Object ID
- VLAN Number

Registros de Citrix Virtual Apps and Desktops y Citrix DaaS

Los registros de Citrix Virtual Apps and Desktops y Citrix DaaS contienen los siguientes puntos de datos:

- Nombre de la aplicación
- Explorador web
- ID de cliente
- Detalles: Tamaño de formato, Tipo de formato, Iniciador, Resultado
- ID de dispositivo
- Tipo de dispositivo
- Comentarios
- ID de comentario
- Nombre del archivo
- Ruta de archivo
- Tamaño de archivo
- Es como
- Prisión rota
- Detalles del trabajo: nombre de archivo, formato, tamaño
- Ubicación: estimación, latitud, longitud

  > **Nota**
  >
  > La información de ubicación se proporciona a nivel de ciudad y país y no representa una geolocalización precisa.

- Línea CMD larga
- Ruta del archivo del módulo
- Operación
- Sistema operativo
- Información adicional sobre la plataforma
- Nombre de impresora
- Pregunta
- ID de pregunta

- Nombre de la aplicación SaaS
- Dominio de sesión
- Nombre del servidor de sesión
- Nombre de usuario de sesión
- GUID de sesión
- Timestamp
- Zona horaria: sesgo, horario de verano, nombre
- Total de copias impresas
- Total de páginas impresas
- Tipo
- URL
- Agente de usuario

Registros de Citrix ADC

Los registros de Citrix ADC contienen los siguientes puntos de datos:

- Contenedor
- Archivos
- Formato
- Tipo

Registros de Citrix DaaS Standard for Azure

Los registros de Citrix DaaS Standard for Azure contienen los siguientes puntos de datos:

- Nombre de la aplicación
- Explorador web
- Detalles: Tamaño de formato, Tipo de formato, Iniciador, Resultado
- ID de dispositivo
- Tipo de dispositivo
- Nombre del archivo
- Ruta de archivo

- Tamaño de archivo
- Prisión rota
- Detalles del trabajo: nombre de archivo, formato, tamaño
- Ubicación: estimación, latitud, longitud

  > **Nota**
  >
  > La información de ubicación se proporciona a nivel de ciudad y país y no representa una geolocalización precisa.

- Línea CMD larga
- Ruta del archivo del módulo
- Operación
- Sistema operativo
- Información adicional sobre la plataforma
- Nombre de impresora
- Nombre de la aplicación SaaS
- Dominio de sesión
- Nombre del servidor de sesión
- Nombre de usuario de sesión
- GUID de sesión
- Timestamp
- Zona horaria: sesgo, horario de verano, nombre
- Tipo
- URL
- Agente de usuario

Registros del proveedor de identidad de Citrix

- Inicio de sesión de usuario:
  - Dominios de autenticación: nombre, producto, tipo de proveedor de identidad, nombre para mostrar del proveedor de identidad
    - Propiedades del IdP: aplicación, tipo de autenticación, ID de cliente, ID de cliente, directorio, emisor, logotipo, recursos, TID

        * Extensiones:
            - Espacio de trabajo: color de fondo, logotipo de encabezado, logotipo de inicio de sesión, color de enlace, color de texto, dominios de StoreFront
            - ShareFile: ID de cliente, geometría del cliente
            - Token de larga duración: habilitado, tipo de caducidad, segundos de caducidad absoluta, segundos de caducidad deslizantes
    - Resultado de autenticación: nombre de usuario, mensaje de error
    - Mensaje de inicio de sesión: ID de cliente, nombre del cliente
    - Reclamación de usuario: AMR, hash de token de acceso, Aud, tiempo de autenticación, credo CIP, alias de autenticación, dominios de autenticación, grupos, producto, alias del sistema, correo electrónico, correo electrónico verificado, Exp, apellido, nombre de pila, IAT, IdP, ISS, configuración regional, nombre, NBF, SID, sub
        * Reclamaciones de alias de autenticación: nombre, valor
        * Contexto de directorio: dominio, Forrest, proveedor de identidad, ID de arrendatario
        * Usuario: Clientes, correo electrónico, OID, SID, UPN
        * Campos adicionales del proveedor de identidades: Azure AD OID, Azure AD TID
- Cierre de sesión de usuario: ID de cliente, nombre de cliente, nombre de usuario, sub
- Actualización del cliente: acción, ID de cliente, nombre del cliente

registros de Citrix Gateway

- Eventos de transacción:
    - Aplicación ICA: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
    - Evento ICA: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup,

Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type

- Actualización de ICA: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
- Configuración de AppFlow: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5
- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw

Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment

- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow

Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

- Eventos métricos:
  - Equilibrio de carga de vServer: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer LB: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Clt Ttlb Pkt Rcvd, RATE Si Tot Clt Ttlb Pkt Sent, RATE Vsvr Tot Hits, Si Cur Clients, Si Cur Conn Established, Si Cur Servers, Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions, Vsvr Active Svcs, Vsvr Tot Hits, Vsvr tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped
  - CPU: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User
  - Grupo de servicios del servidor: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
  - CFG del SVC de servidor: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot

Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions

- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts
- Grupo de memoria: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available
- Enlace del servicio de supervisión: Bind Entity Name, Entity Name, NetScalerId, SchemaType, Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler,

Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes

- Interfaz: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets
- CS de vServer: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, VServer Cs: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb,RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Vsvr Tot Hits, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Tlb Tolerating Transactions, Vsvr Tot Hits, Vsvr Tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped

Registros del explorador seguro

- Publicación de aplicación:
  - Registros antes de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Registros después de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Eliminación de aplicaciones:
  - Registros antes de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Re-

source Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect

- Registros después de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL

- Actualización de aplicaciones:
  - Registros antes de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Registros después de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL

- Creación de derechos:
  - Registros antes de la creación de derechos: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Registros después de la creación de derechos: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

- Actualización de derechos:
  - Registros antes de la actualización de derechos: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Registros después de la actualización de derechos: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

- Host de acceso a sesiones: Accept Host, Client IP, Date Time, Host, Session, User Name
- Conexión de sesión:

  - Registros antes de la conexión de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Registros después de la conexión de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

- Inicio de sesión:
  - Registros antes del inicio de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Registros después del inicio de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

- Marca de sesión:
  - Registros antes de la marca de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Registros después de la marca de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Registros de Microsoft Graph Security

- ID de arrendatario
- ID de usuario
- ID del indicador
- Indicador UUID
- Hora del evento
- Crear tiempo
- Categoría de alerta
- Ubicación de inicio de sesión
- IP de inicio de sesión
- Tipo de inicio de sesión
- Tipo de cuenta de usuario

- Información del proveedor
- Información de proveedor del vendedor
- Estados de vulnerabilidad
- Gravedad de vulnerabilidad

Registros de Microsoft Active Directory

- ID de arrendatario
- Recoger tiempo
- Tipo
- Contexto de directorio
- Grupos
- Identidad
- Tipo de usuario
- Nombre de cuenta
- Recuento de contraseña incorrecta
- City
- Nombre común
- Empresa
- País
- Días hasta el vencimiento de la contraseña
- Departamento
- Descripción
- Nombre simplificado
- Nombre distinguido
- Correo electrónico
- Número de fax
- Nombre
- Categoría de grupo
- Ámbito de grupo

- Teléfono de casa
- Iniciales
- Teléfono IP
- ¿Está habilitada la cuenta
- Está bloqueada la cuenta
- Es un grupo de seguridad
- Apellido
- Gestor
- Miembro de
- Teléfono móvil
- Buscapersonas
- La contraseña nunca caduca
- Nombre de la oficina de entrega física
- Oficina de correos
- Código postal
- ID de grupo principal
- State
- Dirección
- Título
- Control de cuentas de usuario
- Lista de grupos de usuarios
- Nombre principal del usuario
- Teléfono de trabajo

Registros de Citrix Analytics para rendimiento

- actionid
- actionreason
- actiontype
- adminfolder

- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent

- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- nombre_cliente
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid

- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype
- faultstate

- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing

- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole

- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype
- publishedname

- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username
- usersid

- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

Información técnica general sobre la seguridad

April 12, 2024

El servicio de análisis alojado en Citrix Cloud recopila datos de los productos de la cartera de Citrix y los productos de terceros. Estos productos se denominan orígenes de datos. Citrix Analytics admite orígenes de datos tanto en la nube como en las instalaciones. La información de este documento se aplica a Citrix Analytics y a sus orígenes de datos.

Flujo de datos

Citrix Analytics descubre automáticamente los orígenes de datos de Citrix Cloud que están suscritas a los clientes. Sin embargo, los orígenes de datos locales requieren una configuración adicional para integrarse con Citrix Analytics. Por ejemplo, debe agregar sus sitios de Citrix Virtual Apps and Desktops a Citrix Workspace antes de que Citrix Analytics pueda detectarlos. Del mismo modo, Citrix Gateway local requiere que configure un agente de Citrix ADM. Para obtener más información sobre cómo habilitar Citrix Analytics en los orígenes de datos, consulte Habilitar Analytics en los orígenes de datos de Citrix.

Puede integrar algunos productos de terceros, como Microsoft Graph Security y Microsoft Active Directory con Citrix Analytics. Para obtener más información, consulte estos temas:

- Habilitar el análisis en Microsoft Graph Security
- Integración de análisis con Microsoft Active Directory

Citrix Analytics también puede enviar información de inteligencia de riesgos a un entorno de Splunk propiedad del cliente. Esta integración requiere implementar y configurar el **complemento Citrix**

Analytics para Spunk en el entorno de Splunk. Para obtener más información, consulte Integración de Splunk.

Sin el consentimiento del cliente, Citrix Analytics no procesa ningún evento recibido de los orígenes de datos. Para procesar los eventos de los orígenes de datos, el administrador de Analytics debe habilitar el procesamiento de datos. Para obtener más información sobre la recopilación, el almacenamiento y la retención de datos por parte de Analytics, consulte Gobierno de datos.

Requisitos de la red

- **Requisitos de los servicios**de Citrix Cloud: Para usar los servicios de Citrix Cloud, debe poder conectarse a las direcciones Citrix requeridas a través del puerto HTTPS 443. Para obtener más información, consulte Requisitos de conectividad a Internet.
- **Requisitos de Citrix Analytics**: revise los requisitos del sistema antes de usar Citrix Analytics. Además de los requisitos de Citrix Cloud, se debe poder acceder a las siguientes direcciones de extremo a través del puerto HTTPS 443 para usar el servicio Citrix Analytics.

Dispositivo de punto final	Región de los Estados Unidos	Región de la Unión Europea	Región Asia-Pacífico Sur
IU de administrador	https://analytics.cloud.com/	https://analytics-eu.cloud.com/	https://analytics-aps.cloud.com/
Interfaz de usuario de administración (CDN)	https://cas-api-cdn-ep.azureedge.net/	https://cas-api-cdn-ep-eu.azureedge.net/	https://cas-api-cdn-ep-aps.azureedge.net/
Servicios de API	https://api.analytics.cloud.com/	https://api.analytics-eu.cloud.com/	https://api.analytics-aps.cloud.com/
Servicios de API (análisis de rendimiento)	https://api-a.was.cloud.com/	https://api-eu-a.was.cloud.com/	https://api-ap-s-a.was.cloud.com/
	https://api-b.was.cloud.com/	https://api-eu-b.was.cloud.com/	https://api-ap-s-b.was.cloud.com/
Obtener IP pública	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/	https://locus.analytics.cloud.com/

Dispositivo de punto final	Región de los Estados Unidos	Región de la Unión Europea	Región Asia-Pacífico Sur
Event Hub (no se aplica al agente de Citrix ADM)	https://citrixanalyticseh-alias.servicebus.windows.net/ https://citrixanalyticseh2-alias.servicebus.windows.net/	https://citrixanalyticseheu-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/
Event Hub (para agente de Citrix ADM)	https://cas-eh-ns-alias.servicebus.windows.net/ yhttps://cas-eh-ns2-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/	https://cas-eh-ns-aps-alias.servicebus.windows.net/
Subida masiva	https://casstoragebulk.blob.core.windows.net/	https://casstorebulkeu.blob.core.windows.net/	https://casstorebulkaps.blob.core.windows.net/

> **Nota**
>
> Citrix Analytics ha dejado de admitir TLS 1.0 y TLS 1.1 para la mayoría de los puntos finales anteriores.

- **Instalación de Citrix Cloud Connector**: algunas fuentes de datos, como Citrix Endpoint Management, Citrix Virtual Apps and Desktops y Microsoft Active Directory, requieren que instale un Citrix Cloud Connector en la ubicación de sus recursos. Citrix Cloud Connector es un canal de comunicación entre Citrix Cloud y las ubicaciones de recursos. Después de instalar Citrix Cloud Connector, debe configurar los parámetros del proxy web. Para obtener más información, consulte Configurar el proxy y el firewall de Cloud Connector.
- **Puntos finales de Citrix Analytics para la integración de SIEM**: Para integrar Citrix Analytics con la Administración de eventos e información de seguridad (SIEM), asegúrese de que los siguientes puntos de enlace estén en la lista de permitidos de la red:

Dispositivo de punto final	Región de los Estados Unidos	Región de la Unión Europea	Región Asia-Pacífico Sur
Intermediarios de Kafka	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

Administración de acceso e identidad

- Para acceder a Citrix Analytics, debe usar su cuenta de Citrix Cloud. De forma predeterminada, Citrix Cloud utiliza el proveedor de identidades Citrix para administrar la información de identidades de todos los usuarios de la cuenta de Citrix Cloud. También puede utilizar otros proveedores de identidad como se menciona en Administración de identidades y accesos.
- Citrix Analytics admite los permisos de administrador delegado. Puede asignar un permiso de administrador de solo lectura a un usuario para administrar Analytics en su empresa. Para obtener más información, consulte Administrar funciones de administrador.

Residencia de datos

Citrix Cloud administra el plano de control de Citrix Analytics. Los datos recibidos de los orígenes de datos se almacenan en varios entornos de Microsoft Azure. Estos entornos se encuentran en los Estados Unidos, la Unión Europea y las regiones de Asia Pacífico Sur. La ubicación de almacenamiento depende de la región principal seleccionada por los administradores de Citrix Cloud al incorporar sus organizaciones a Citrix Cloud. Para obtener más información, consulte estos temas:

- Consideraciones geográficas
- Gobierno de datos

Protección de datos

Citrix Analytics recibe datos de los orígenes de datos suscritas de Citrix Cloud, los orígenes de datos locales y los productos de terceros. Los datos recibidos se procesan solo si el cliente tiene un derecho

de Citrix Cloud y el administrador de Analytics ha habilitado explícitamente el procesamiento de datos para cada una de los orígenes de datos suscritas.

Citrix Analytics protege los datos de los clientes mediante las siguientes medidas de seguridad:

- Autenticación de Citrix Cloud para usuarios de Analytics. Para obtener información, consulte Administración de identidades y accesos.
- Controles de acceso a datos basados en arrendatarios aplicados por el servicio de datos y la capa de acceso a datos.
- Aislamiento de datos sólido por cliente o arrendatario en todos los almacenes de datos del lago de datos y el almacén de datos.
- Transferencia de datos cifrados con TLS entre los diversos microservicios y almacenes de datos, aplicable para los puntos finales públicos (APTs/entradas/salidas) de la plataforma y dentro de la plataforma.
- Altos estándares en los puntos finales de TLS. TLS 1.0 y TLS 1.1 están inhabilitados.
- Almacenamiento de datos cifrados mediante claves de cifrado y secretos que se almacenan en las bóvedas de claves apropiadas.
- Controles de acceso de administración de usuarios sólidos para las operaciones de servicio y el soporte mientras se protegen los registros de
- Análisis de vulnerabilidades, detección de intrusiones, antimalware, análisis de rootkits utilizados junto con Azure Security Center.

Al igual que con todos los servicios de Citrix Cloud, la recopilación de datos está estrictamente sujeta al Acuerdo de servicio para el usuario final (EUSA). Para obtener más información, consulte los siguientes acuerdos:

- Acuerdos de usuario
- directiva de privacidad de Citrix
- Contrato de procesamiento de datos de Citrix
- anexo de seguridad de Citrix Services
- Citrix Cloud Services: gestión de registros y contenido de clientes
- Información de privacidad y cumplimiento de Citrix

Responsabilidad de seguridad

Responsabilidad de Citrix

Citrix es responsable de proteger toda la infraestructura y los datos que residen en los entornos de nube administrados por Citrix que alojan Citrix Analytics. Citrix es responsable de aplicar actualizaciones y parches de software regulares en el entorno de la nube para abordar las vulnerabilidades de seguridad.

Responsabilidad del cliente

Los clientes de Citrix son responsables de proteger sus orígenes de datos, puntos de aplicación de directivas y sistemas de administración de eventos e información de seguridad (SIEM) que se integran con Citrix Analytics, que incluyen:

- Orígenes de datos locales que son propiedad de los clientes y las administran:
  - **Fuentes de datos locales**: Citrix Gateway, Citrix Virtual Apps and Desktops, Microsoft Active Directory
  - **SIEM**: Splunk y cualquier otro producto de terceros que utilice los agentes de Kafka para leer eventos de Citrix Analytics.
- Credenciales de administrador proporcionadas por el cliente para administrar los servicios de Citrix Cloud, incluido Citrix Analytics.
- Cuentas de administrador propiedad del cliente que reciben correos electrónicos o notificaciones de los servicios de Citrix Cloud.
- Credenciales de administrador proporcionadas por el cliente para implementar e integrar los agentes, como los agentes Citrix ADM. El acceso a estos agentes debe restringirse porque almacenan las claves localmente para comunicarse con Citrix Analytics.
- Credenciales generadas por Citrix Analytics para configurar el **complemento Citrix Analytics para Splunk**.
- Dispositivos de usuario final que se ejecutan en Windows, Mac, Android, iOS para conectarse a Citrix Cloud o Citrix Workspace e integrarse con orígenes de datos.

Para obtener más información sobre las disposiciones de seguridad, consulte los siguientes documentos:

- Guía de implementación segura de la plataforma Citrix Cloud
- documentación de Citrix Workspace

- Descripción general de la seguridad técnica de Citrix DaaS (anteriormente, Citrix Virtual Apps and Desktops Service)
- Consideraciones de seguridad para Citrix Virtual Apps and Desktops
- Documentación para proteger implementaciones de StoreFront
- Descripción general de seguridad técnica para Citrix Endpoint Management
- Documentación de Citrix Secure Private Access Service
- Guía de implementación segura para Citrix ADC
- Requisitos del sistema Citrix ADM

Requisitos del sistema

September 21, 2023

Antes de empezar a utilizar Citrix Analytics, debe revisar la información de licencia, los requisitos de software y los requisitos del explorador.

Suscripciones Citrix Analytics

Debe tener suscripciones válidas para usar los siguientes productos de Analytics:

- Citrix Analytics for Security
- Citrix Analytics for Performance

Para obtener más información, consulte Servicios de Citrix Cloud.

Requisitos de orígenes de datos

Los orígenes de datos son los productos que envían eventos a Citrix Analytics. Según las ofertas de Citrix Analytics que utilice, los orígenes de datos varían. Consulte los siguientes artículos para ver los orígenes de datos compatibles con cada oferta:

- Orígenes de datos compatibles con Citrix Analytics for Security
- Orígenes de datos compatibles con Citrix Analytics for Performance

Exploradores web compatibles

Para acceder a Citrix Analytics, su estación de trabajo debe tener el siguiente explorador web compatible:

- La versión más reciente de Google Chrome
- La versión más reciente de Mozilla Firefox
- La versión más reciente de Microsoft Edge
- La versión más reciente de Apple Safari

Administrar las funciones de administrador de Citrix Analytics

May 2, 2023

De forma predeterminada, un administrador de Citrix Cloud tiene permisos de acceso total a todos los servicios suscritos en su cuenta de Citrix Cloud. Con los permisos de acceso completos, el administrador puede usar todas las características y funcionalidades de un servicio suscrito.

Como administrador de Citrix Cloud con acceso completo, puede invitar a otros administradores a su cuenta de Citrix Cloud para administrar los servicios suscritos de su organización. A continuación, puede definir sus permisos de acceso y permitirles administrar funciones específicas en los servicios suscritos.

Se pueden agregar nuevos administradores de dos maneras:

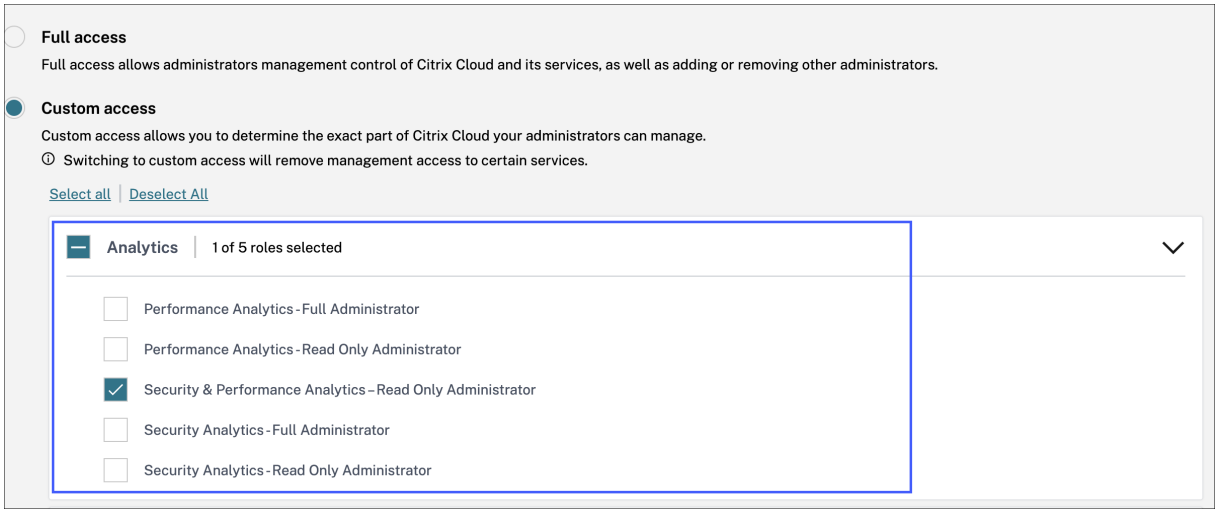
1. Individualmente como usuarios de Citrix Identity y Azure AD/Active Directory. Para obtener más información, consulte Administrar administradores de Citrix Cloud.
2. Uso de grupos en Azure Active Directory. Para obtener más información, consulte Administrar grupos de administradores.

Los administradores pueden iniciar sesión en Citrix Cloud con sus cuentas de Citrix Cloud, Active Directory o Azure Active Directory y acceder a funciones específicas y realizar tareas según sus funciones.

Para Citrix Analytics, puede asignar las siguientes funciones personalizadas a sus administradores:

Rol	Permiso
Análisis de rendimiento: administrador total	Asigna permisos de acceso completo a los administradores de Performance Analytics de Citrix Cloud.

Rol	Permiso
Análisis de rendimiento: administrador de solo lectura	Asigna permisos de acceso de solo lectura a los administradores de Citrix Cloud de Performance Analytics.
Análisis de seguridad y rendimiento: administrador de solo lectura	Asigna permisos de acceso de solo lectura a los administradores de Citrix Cloud tanto de Security Analytics como de Performance Analytics.
Análisis de seguridad: administrador total	Asigna permisos de acceso completo a los administradores de Security Analytics de Citrix Cloud.
Análisis de seguridad: administrador de solo lectura	Asigna permisos de acceso de solo lectura a los administradores de Citrix Cloud de Security Analytics.



Notas

- Si selecciona varios roles para un administrador, se aplicará el rol con mayor acceso.
- Si a un usuario se le concede acceso directamente como usuario y a través de un grupo de Azure Active Directory, el acceso otorgado individualmente al usuario surtirá efecto.
- Los grupos de Azure Active Directory solo se pueden agregar como administradores personalizados. La función de administrador de acceso completo no está disponible para los grupos.
- Los administradores con la función de **administrador de solo lectura** que estaba disponible anteriormente se renombran a **Seguridad y rendimiento: administrador de**

> **solo lectura**.
>
> - Los administradores con la función **Security & Performance Analytics: administrador de solo lectura** y la función **Performance Analytics: administrador de solo lectura** no reciben ninguna notificación por correo electrónico de Citrix Analytics.

Para obtener más información sobre la oferta de funciones específicas, consulte los siguientes artículos:

- Administrar las funciones de administrador para Performance Analytics
- Gestionar las funciones de administrador para Security

Introducción

April 12, 2024

En este documento se describe cómo empezar a utilizar Citrix Analytics por primera vez.

Paso 1: Inicie sesión en Citrix Cloud

Para usar Citrix Analytics, debe tener una cuenta de Citrix Cloud. Vaya a https://citrix.cloud.com e inicie sesión con su cuenta de Citrix Cloud existente.

Si no tiene una cuenta de Citrix Cloud, primero debe crear una cuenta de Citrix Cloud o unirse a una cuenta existente creada por otra persona de su organización. Para obtener información detallada sobre los procesos e instrucciones sobre cómo proceder, consulte Inscribirse en Citrix Cloud.

Paso 2: Obtenga acceso a Analytics

Puede acceder a Analytics de una de las siguientes formas:

- **Solicite una prueba de la oferta de Citrix Analytics**. Tras iniciar sesión en Citrix Cloud, en la sección **Servicios disponibles**, en el mosaico de **Analytics**, haga clic en **Administrar** para ver la página de información general de Analytics.

  La página de resumen muestra las ofertas de Analytics: **Security** y **Performance**.

  - Para Security Analytics y Performance Analytics, haga clic en **Solicitar prueba** para usar la versión de prueba de la oferta. Recibirá un correo electrónico cuando se apruebe su solicitud y la versión de prueba esté disponible. Puede usar la versión de prueba durante un período máximo de 60 días. Para obtener más información sobre las pruebas de servicios, consulte Pruebas de Citrix Cloud Service.

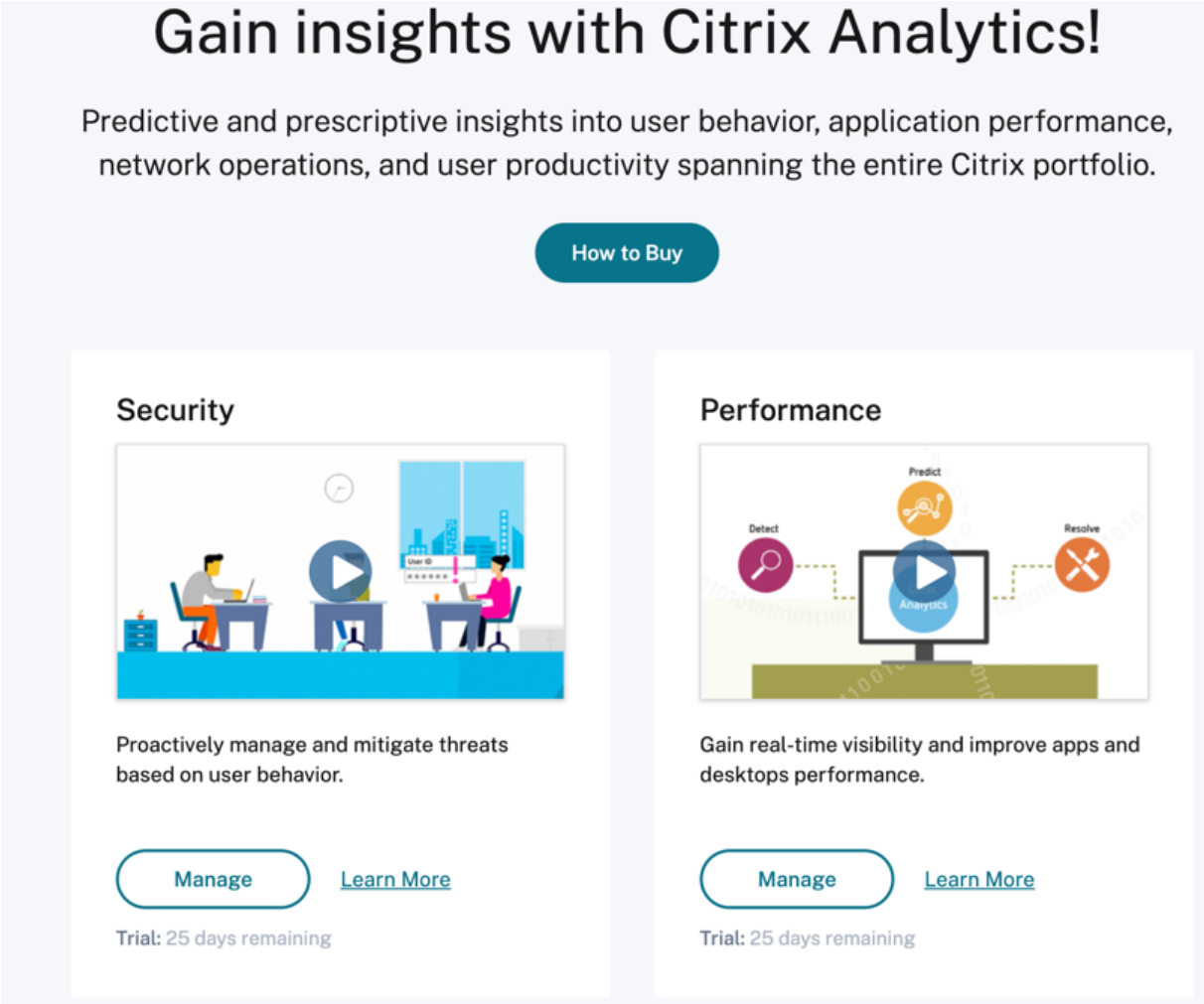
En la página Citrix Cloud, el mosaico **Analytics** se mueve a la sección **Mis servicios**.

- **Suscríbase a Citrix Analytics**. Puede adquirir las siguientes suscripciones a Citrix Analytics:
  - Citrix Analytics for Security
  - Citrix Analytics for Performance
  - Citrix Analytics for Security y Performance

  Citrix Analytics for Security y Citrix Analytics for Performance se ofrecen como un servicio complementario con los paquetes de Citrix Workspace: Workspace Standard, Workspace Premium y Workspace Premium Plus. Para obtener más información, consulte Servicios de Citrix Cloud.

Paso 3: Administrar Analytics

En el caso de Security Analytics y Performance Analytics, cuando tenga las suscripciones necesarias o esté autorizado a acceder a la versión de prueba, en la página de información general de Analytics, el botón **Solicitar prueba** de la oferta cambia a **Administrar**. Haga clic en **Administrar** para ver el panel de usuario correspondiente a cada oferta.



Analytics descubre automáticamente los servicios de Citrix Cloud (fuentes de datos) asociados a su cuenta de Citrix Cloud. Para ver las fuentes de datos detectadas, haga clic en **Parámetros > Fuentes de datos** y haga clic en la ficha requerida: **Security** o **Performance**.

Para obtener más información sobre cada oferta de Analytics, consulte

- Citrix Analytics for Security
- Citrix Analytics for Performance

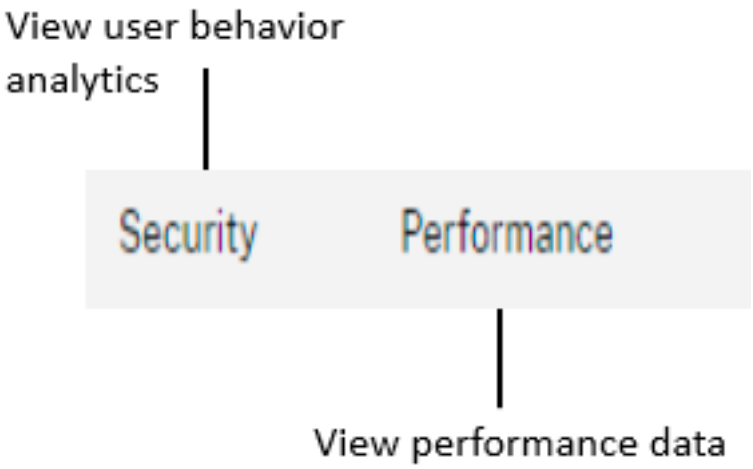
Familiarización

May 9, 2022

Familiarícese con los principales controles de la interfaz de usuario de Analytics.

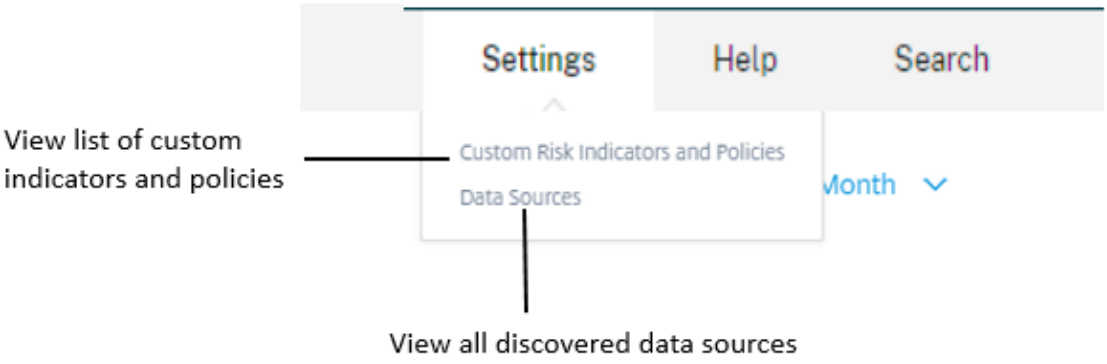
Barra superior

Navegue a las distintas ofertas de Analytics en la barra superior.

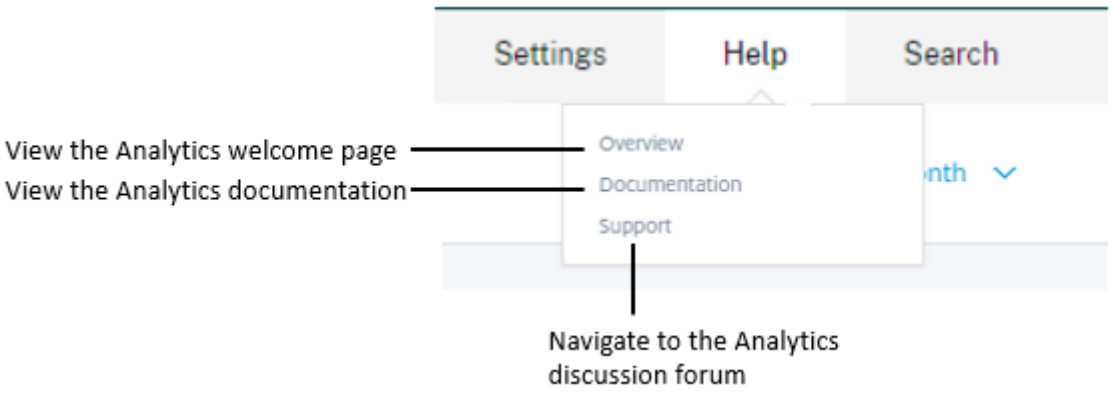


Menú Parámetros

En el menú **Configuración**, vaya a la página Indicadores y políticas o a la página Orígenes de datos .

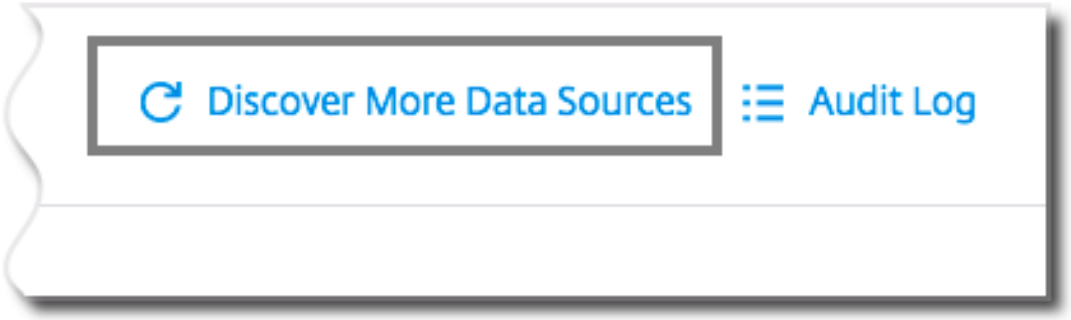


Menú de ayuda



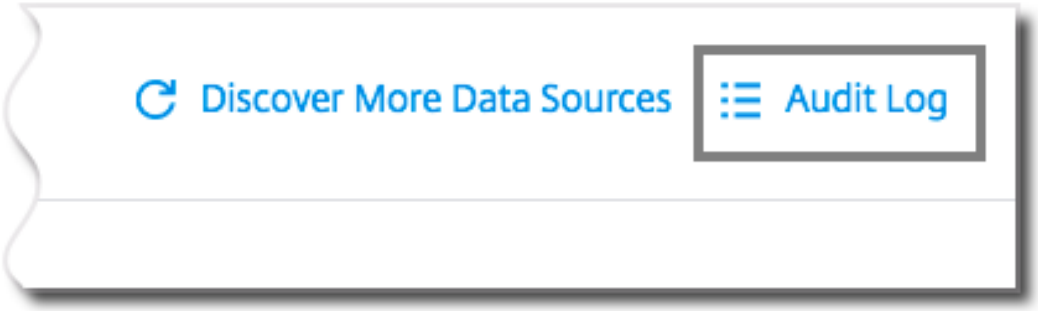
Descubra más orígenes de datos

Descubra orígenes de datos agregados recientemente u orígenes de datos eliminados anteriormente.



Audit log

Navegue hasta la página Registro de auditoría que enumera todos los eventos generados en Analytics.



Búsqueda de autoservicio

December 7, 2023

¿Qué es la búsqueda de autoservicio?

La función de búsqueda de autoservicio le permite buscar y filtrar los eventos de usuario recibidos de sus orígenes de datos. Puede explorar los eventos de usuario subyacentes y sus atributos. Estos eventos le ayudan a identificar cualquier problema de datos y solucionarlo. La página de búsqueda muestra varias facetas (dimensiones) y métricas de una fuente de datos. Puede definir la consulta de búsqueda y aplicar filtros para ver los eventos que coinciden con los criterios definidos. De forma predeterminada, la página de búsqueda de autoservicio muestra los eventos de usuario del último día.

Actualmente, la función de búsqueda de autoservicio está disponible para estos orígenes de datos:

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- Aplicaciones y escritorios
- Usuarios, máquinas y sesiones de rendimiento

Además, puede realizar búsquedas de autoservicio en los eventos que cumplen las directivas definidas. Para obtener más información, consulte Búsqueda de autoservicio de directivas.

Cómo acceder a la búsqueda de autoservicio

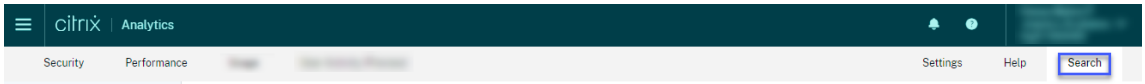
Puede acceder a la búsqueda de autoservicio mediante las siguientes opciones:

- **Barra superior**: haga clic en **Buscar** en la barra superior para ver todos los eventos de usuario del origen de datos seleccionado.
- **Cronología de riesgos en una página de perfil de usuario**: haga clic en **Búsqueda** de eventos para ver los eventos del usuario respectivo.

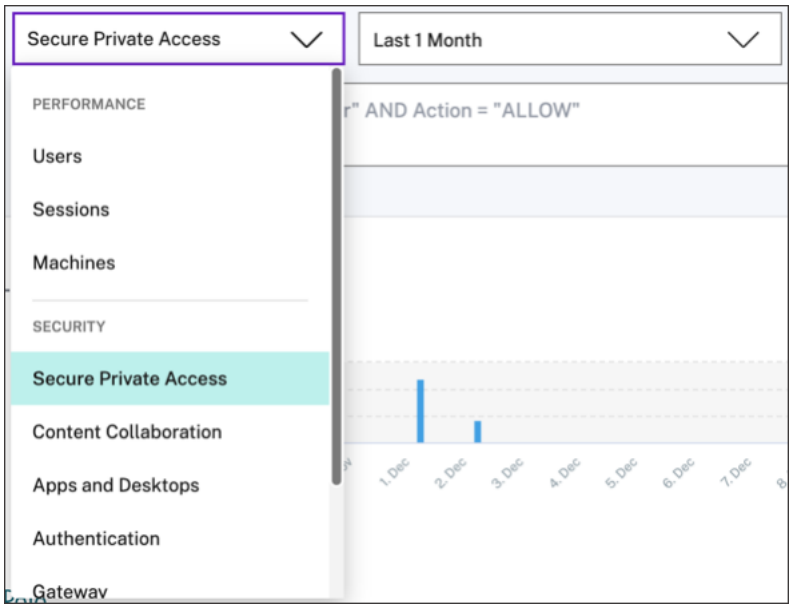
Búsqueda de autoservicio desde la barra superior

Utilice esta opción para ir a la página de búsqueda de autoservicio desde cualquier lugar de la interfaz de usuario.

1. Haga clic en **Buscar** para ver la página de autoservicio.



2. Seleccione el origen de datos y el período de tiempo para ver los eventos correspondientes.

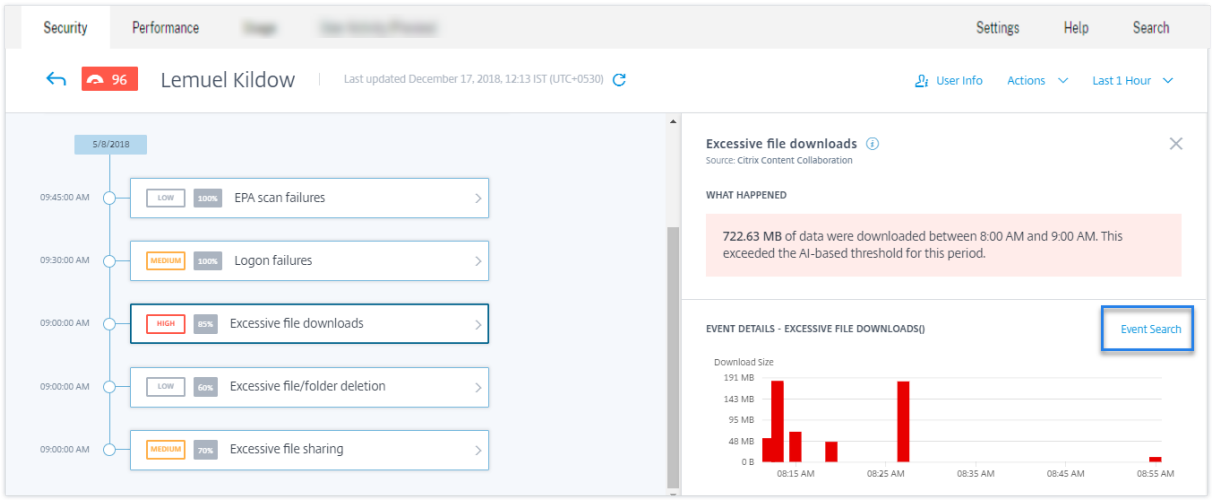


Búsqueda de autoservicio desde el cronograma de riesgos del usuario

Utilice esta opción si quiere ver los eventos de usuario asociados a un indicador de riesgo.

Al seleccionar un indicador de riesgo del cronograma de un usuario, la sección de información del indicador de riesgo se muestra en el panel derecho. Haga clic en **Búsqueda de eventos** para explorar

los eventos asociados al usuario y el origen de datos (para la que se activa el indicador de riesgo) en la página de búsqueda de autoservicio.



Para obtener más información sobre el cronograma de riesgo del usuario, consulte Cronología de riesgos.

Cómo utilizar la búsqueda de autoservicio

Utilice las siguientes funciones de la página de búsqueda de autoservicio:

- Facetas para filtrar sus eventos.
- Cuadro de búsqueda para introducir la consulta y filtrar los eventos.
- Selector de tiempo para seleccionar el período de tiempo.
- Detalles del cronograma para ver los gráficos de eventos.
- Datos de eventos para ver los eventos.
- Expórtelo en formato CSV para descargar sus eventos de búsqueda en un archivo CSV.
- Exporta un resumen visual para descargar el informe de resumen visual de su consulta de búsqueda.
- Clasificación de varias columnas para ordenar los eventos por varias columnas.

Usar facetas para filtrar eventos

Las facetas son el resumen de los puntos de datos que constituyen un evento. Las facetas varían según el origen de datos. Por ejemplo, las facetas del origen de datos de acceso privado seguro son la reputación, las acciones, la ubicación y el grupo de categorías. Mientras que las facetas de Apps y escritorios son el tipo de evento, el dominio y la plataforma.

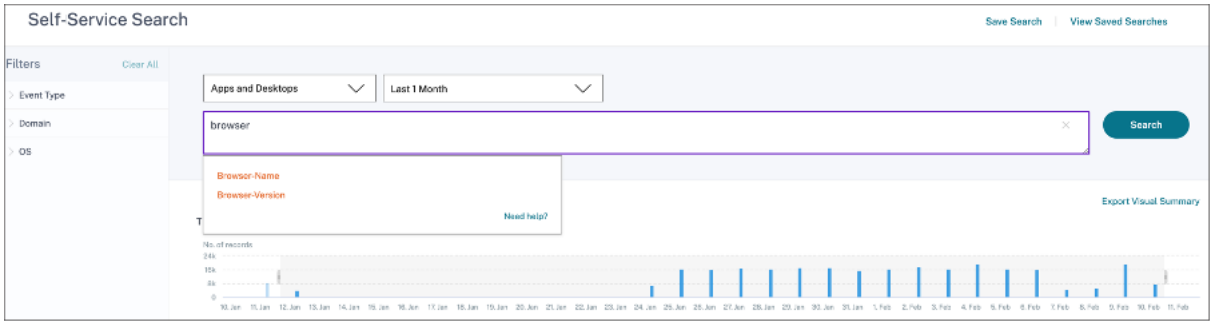
Seleccione las facetas para filtrar los resultados de la búsqueda. Las facetas seleccionadas se muestran como fichas.

Para obtener más información sobre las facetas correspondientes a cada origen de datos, consulte el artículo de búsqueda de autoservicio para el origen de datos mencionado anteriormente en este artículo.

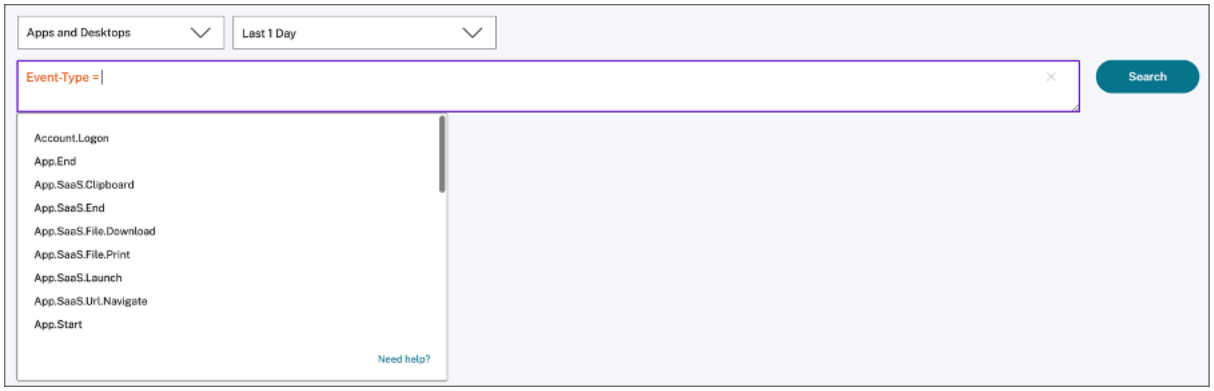
Utilizar la consulta de búsqueda en el cuadro de búsqueda para filtrar eventos

Al colocar el cursor en el cuadro de búsqueda, el cuadro de búsqueda muestra una lista de dimensiones basada en los eventos del usuario. Estas dimensiones varían según el origen de datos. Utilice las dimensiones y los operadores válidos para definir los criterios de búsqueda y buscar los eventos necesarios.

Por ejemplo, en la búsqueda de autoservicio de Apps y escritorios, obtiene los siguientes valores para la dimensión `Browser`. Use la dimensión para escribir la consulta, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.



Al seleccionar determinadas dimensiones, como `Event-Type` y `Clipboard-Operation` junto con un operador válido, los valores de la dimensión se muestran automáticamente. Puede elegir un valor de las opciones sugeridas o introducir un valor nuevo según sus requisitos.



Operadores compatibles en la consulta de búsqueda Utilice los siguientes operadores en las consultas de búsqueda para refinar los resultados de la búsqueda.

Operador	Descripción	Ejemplo	Resultado
	Asigne un valor a una dimensión de búsqueda.	User-Name: John	Muestra los eventos del usuario John.
=	Asigne un valor a una dimensión de búsqueda.	User-Name = John	Muestra los eventos del usuario John.
~	Busca eventos con valores similares.	User-Name ~ test	Muestra los eventos con nombres de usuario similares.
" "	Encierra valores separados por espacios.	User-Name = "John Smith"	Muestra los eventos del usuario John Smith.
< >	Búsqueda de valor relacional.	Volumen de datos > 100	Muestra los eventos en los que el volumen de datos es superior a 100 GB.
AND	Buscar eventos en los que se cumplan las condiciones especificadas.	User-Name: John AND Data Volume > 100	Muestra los eventos del usuario John en los que el volumen de datos es superior a 100 GB.
! ~	Comprueba los eventos del patrón coincidente que especifique. Este operador NOT LIKE devuelve los eventos que no contienen el patrón coincidente en ninguna parte de la cadena de eventos.	User-Name !~ John	Muestra los eventos de los usuarios excepto John, John Smith o cualquier otro usuario que contenga el nombre coincidente "John".

Operador	Descripción	Ejemplo	Resultado
! =	Comprueba los eventos de la cadena exacta que especifique. Este operador NOT EQUAL devuelve los eventos que no contienen la cadena exacta en ninguna parte de la cadena de eventos.	Country != USA	Muestra los eventos de los países excepto EE. UU.
*	Buscar eventos que coincidan con las cadenas especificadas. Actualmente, el operador * solo se admite con los siguientes operadores :, = y ! =. Los resultados de la búsqueda distinguen entre mayúsculas y min	User-Name = John*	Muestra los eventos de todos los nombres de usuario que empiezan por John.
		User-Name = *John*	Muestra los eventos de todos los nombres de usuario que contienen John.
		User-Name = *Smith	Muestra los eventos de todos los nombres de usuario que terminan en Smith.
		Nombre de usuario: John*	Muestra los eventos de todos los nombres de usuario que empiezan por John.
		Nombre de usuario: *John*	Muestra los eventos de todos los nombres de usuario que contienen John.

Operador	Descripción	Ejemplo	Resultado
		Nombre de usuario: *Smith	Muestra los eventos de todos los nombres de usuario que terminan en Smith.
		Nombre de usuario! = John*	Muestra los eventos de todos los nombres de usuario que no empiezan por John.
		Nombre de usuario! = *Herrero	Muestra los eventos de todos los nombres de usuario que no terminan en Smith.
`IN`	Asigne varios valores a una dimensión de búsqueda para obtener los eventos relacionados con uno o varios valores. **Nota**: Actualmente, puede usar este operador con las siguientes dimensiones de Aplicaciones y escritorios: `Device ID`, `Domain`, `Event-Type` y `User-Name`. Este operador solo se aplica a los valores de cadena.	User-Name IN (John, Kevin)	Busca todos los eventos relacionados con John o Kevin.

Operador	Descripción	Ejemplo	Resultado
`NOT IN`	Asigne varios valores a una dimensión de búsqueda y busque los eventos que no contienen los valores especificados. **Nota**: Actualmente, puede usar este operador con las siguientes dimensiones de Aplicaciones y escritorios: `Device ID`, `Domain`, `Event-Type` y `User-Name`. Este operador solo se aplica a los valores de cadena.	User-Name NOT IN (John, Kevin)	Busca los eventos para todos los usuarios excepto John y Kevin.
`IS EMPTY`	Comprueba si hay un valor nulo o un valor vacío para una dimensión. Este operador solo funciona para dimensiones de tipo cadena como `App-Name`, `Browser` y `Country`. No funciona para dimensiones de tipo no cadena (número) como `Upload-File-Size`, `Download-File-Size` y `Client-IP`.	Country IS EMPTY	Busca eventos en los que el nombre del país no está disponible o está vacío (no especificado).

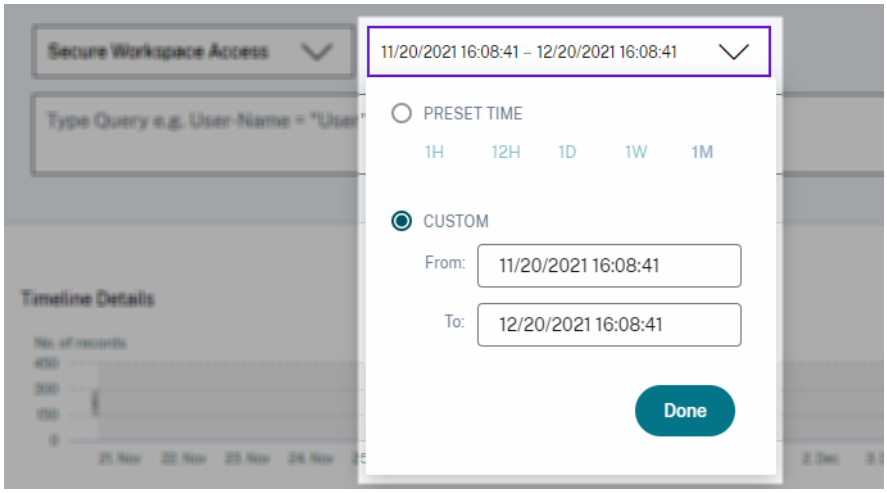
Operador	Descripción	Ejemplo	Resultado
`IS NOT EMPTY`	Comprueba si hay un valor no nulo o un valor específico para una dimensión. Este operador solo funciona para dimensiones de tipo cadena como `App-Name`, `Browser` y `Country`. No funciona para dimensiones de tipo no cadena (número) como `Upload-File-Size`, `Download-File-Size` y `Client-IP`.	Country IS NOT EMPTY	Busca eventos en los que el nombre del país esté disponible o especificado.
`OR`	Busca valores en los que una o ambas condiciones son verdaderas.	(User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = "Session.Logon"	Muestra eventos de `Session.Logon` para todos los nombres de usuario que comienzan por John o terminan por Smith.

> **Nota**
>
> Para el operador **NOT EQUAL**, al introducir los valores de las dimensiones de la consulta, utilice los valores exactos disponibles en la página de búsqueda de autoservicio de un origen de datos. Los valores de cota distinguen entre mayúsculas y minúsculas

Para obtener más información sobre cómo especificar la consulta de búsqueda para el origen de datos, consulte el artículo de búsqueda de autoservicio del origen de datos mencionado anteriormente en este artículo.

Seleccione la hora para ver el evento

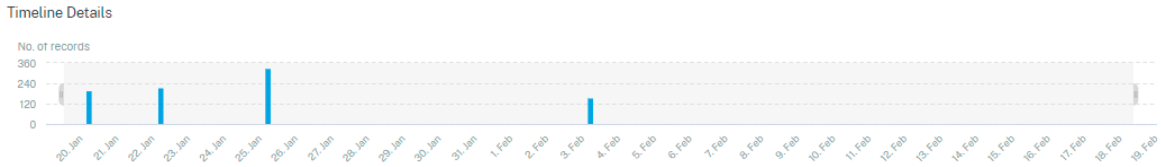
Seleccione una hora preestablecida o introduzca un intervalo de tiempo personalizado y haga clic en **Buscar** para ver los eventos.



Ver los detalles del cronograma

La línea de tiempo proporciona una representación gráfica de los eventos del usuario durante el período de tiempo seleccionado. Mueva las barras de selección para elegir el intervalo de tiempo y ver los eventos correspondientes al intervalo de tiempo seleccionado.

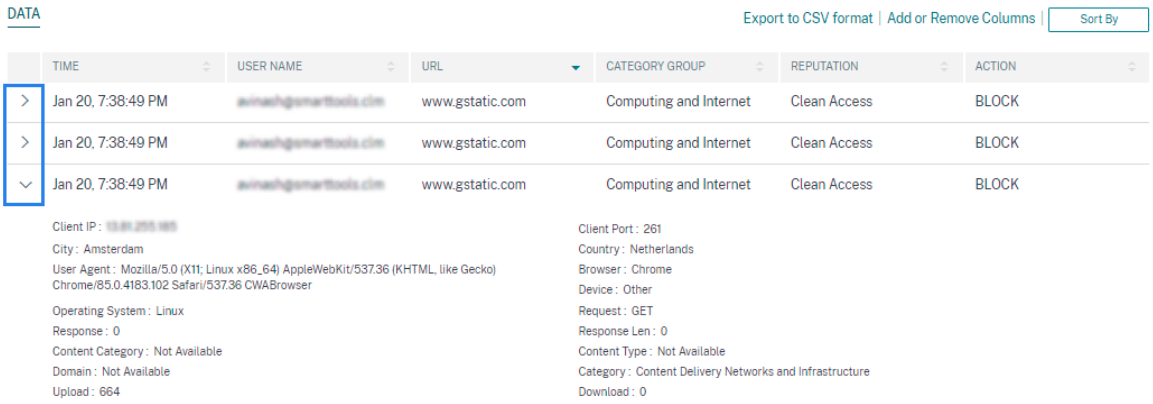
En la ilustración se muestran los detalles del cronograma de los datos de acceso.



Ver el evento

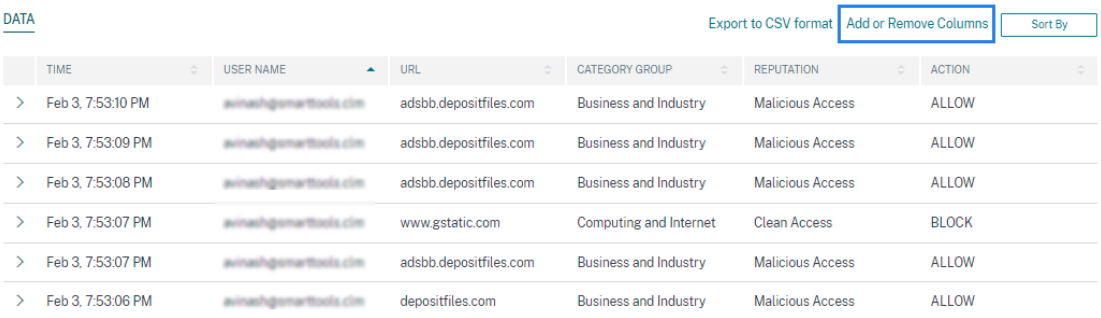
Puede ver la información detallada sobre el evento de usuario. En la tabla **DATOS**, haga clic en la flecha de cada columna para ver los detalles del evento de usuario.

En la ilustración se muestran los detalles sobre los datos de acceso del usuario.

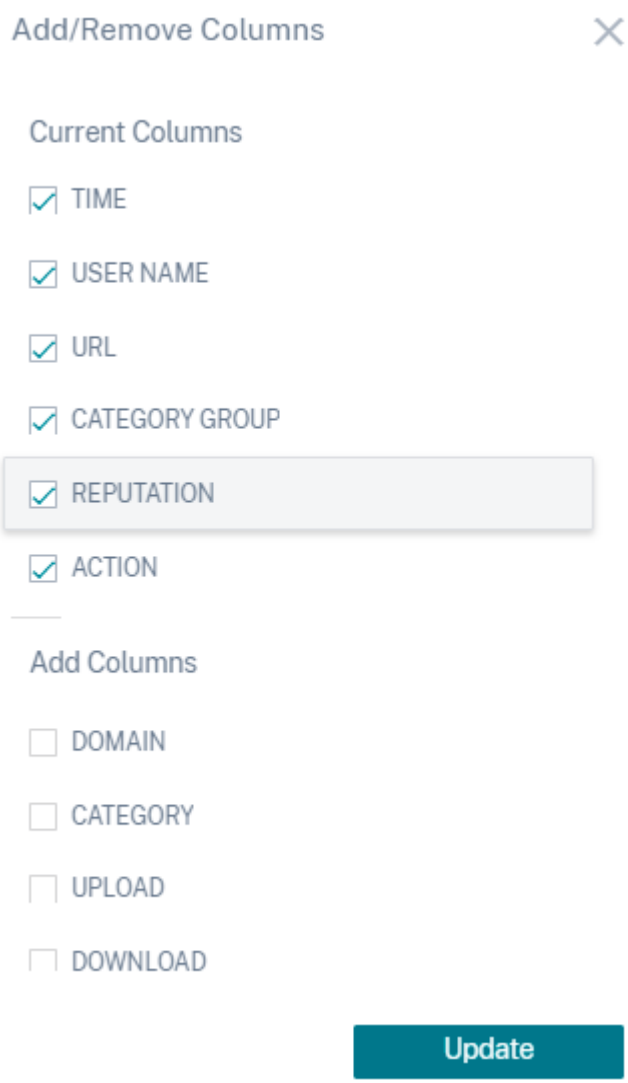


Agregar o quitar columnas Puede agregar o quitar columnas de la tabla de eventos para mostrar u ocultar los puntos de datos correspondientes. Haga lo siguiente:

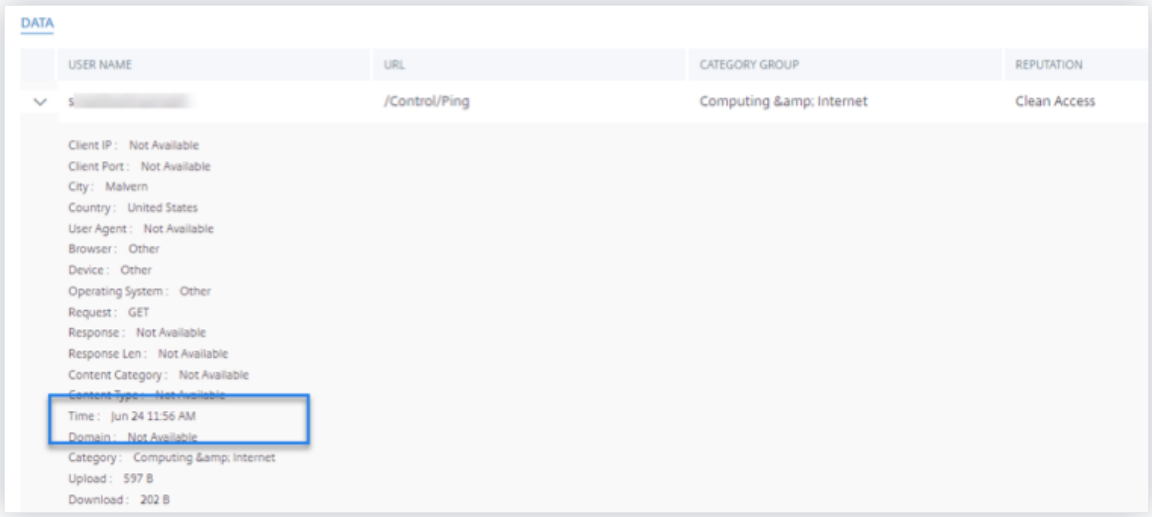
1. Haga clic en **Agregar o quitar columnas**.



2. Seleccione o anule la selección de los elementos de datos de la lista y, a continuación, haga clic en **Actualizar**.

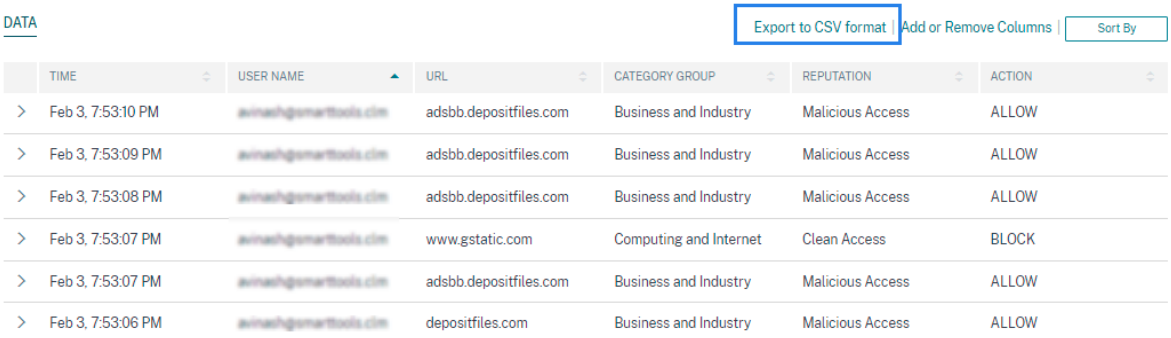


Si anula la selección de un punto de datos de la lista, la columna correspondiente se elimina de la tabla de eventos. Sin embargo, puede ver ese punto de datos expandiendo la fila de eventos de un usuario. Por ejemplo, si anula la selección del punto de datos **TIME** de la lista, la columna **TIME** se quita de la tabla de eventos. Para ver el registro de tiempo, expanda la fila de eventos de un usuario.



Exportar los eventos a un archivo CSV

Exporta los resultados de la búsqueda a un archivo CSV y guárdalo como referencia. Haga clic en **Exportar a formato CSV** para exportar los eventos y descargar el archivo CSV generado. Puede exportar 100 000 filas mediante la función **Exportar a formato CSV**.



Resumen visual de exportación

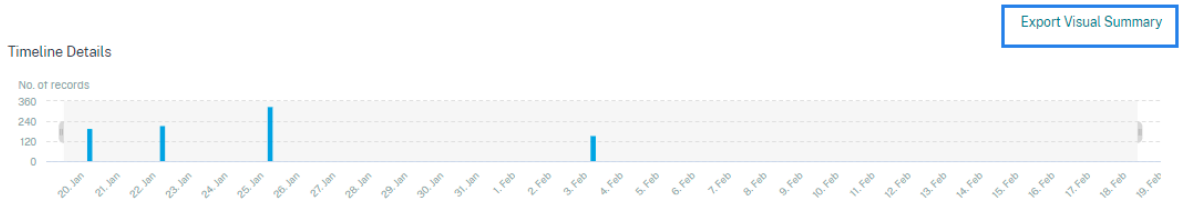
Puede descargar el informe resumido visual de su consulta de búsqueda y compartir una copia con otros usuarios, administradores o su equipo ejecutivo.

Haga clic en **Exportar resumen visual** para descargar el informe de resumen visual en formato PDF. El informe contiene la siguiente información:

- Consulta de búsqueda que ha especificado para los eventos del período de tiempo seleccionado.
- Las facetas (filtros) que ha aplicado a los eventos durante el período de tiempo seleccionado.

- El resumen visual, como los gráficos de línea de tiempo, gráficos de barras o gráficos de los eventos de búsqueda para el período de tiempo seleccionado.

Para una fuente de datos, puede descargar el informe de resumen visual solo si los datos se muestran en formatos visuales como gráficos de barras o detalles de línea de tiempo. De lo contrario, esta opción no está disponible. Por ejemplo, puede descargar el informe de resumen visual de los orígenes de datos, como Aplicaciones y escritorios, Sesiones, donde ve los datos como detalles de la línea de tiempo y gráficos de barras. Para los orígenes de datos como Usuarios y Equipos, los datos solo se ven en formato tabular. Por lo tanto, no se puede descargar ningún informe de resumen visual.

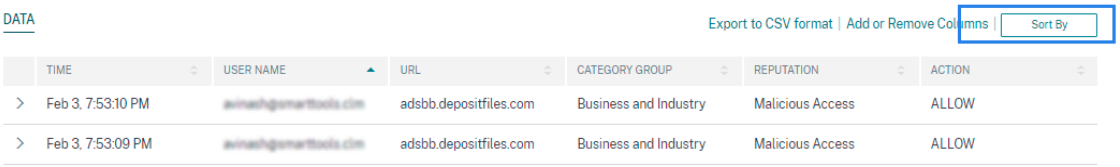


Clasificación de varias columnas

La clasificación ayuda a organizar los datos y proporciona una mejor visibilidad. En la página de búsqueda de autoservicio, puede ordenar los eventos de usuario por una o varias columnas. Las columnas representan los valores de varios elementos de datos, como nombre de usuario, fecha y hora y URL. Estos elementos de datos varían según los orígenes de datos seleccionadas.

Para realizar una ordenación de varias columnas, haga lo siguiente:

1. Haga clic en **Ordenar por**.

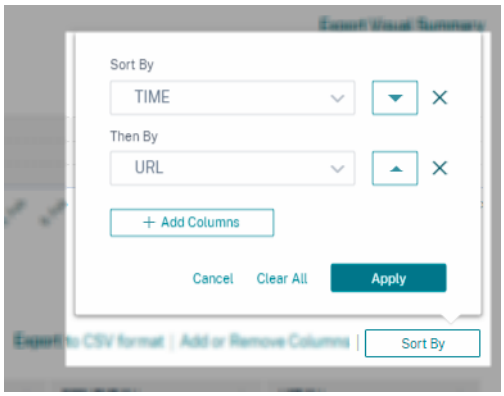


2. Seleccione una columna de la lista **Ordenar por**.
3. Seleccione el orden de clasificación: ascendente (flecha hacia arriba) o descendente (flecha abajo) para ordenar los eventos de la columna.
4. Haga clic en **+ Agregar columnas**.
5. Seleccione otra columna de la lista **Entonces por**.
6. Seleccione el orden de clasificación: ascendente (flecha hacia arriba) o descendente (flecha hacia abajo) para ordenar los eventos de la columna.

> **Nota**
>
> Puede agregar hasta seis columnas para realizar la ordenación.

7. Haga clic en **Aplicar**.
8. Si no quiere aplicar la configuración anterior, haga clic en **Cancelar**. Para quitar los valores de las columnas seleccionadas, haga clic en **Borrar todo**.

En el siguiente ejemplo se muestra una ordenación de varias columnas en los eventos Secure Private Access. Los eventos se ordenan por hora (en orden más reciente a más antiguo) y, a continuación, por URL (en orden alfabético).



Alternativamente, puede ordenar varias columnas con la tecla **Mayús**. Pulse la tecla **Mayús** y haga clic en los encabezados de columna para ordenar los eventos de usuario.

Cómo guardar la búsqueda de autoservicio

Como administrador, puede guardar una consulta de autoservicio. Esta función ahorra el tiempo y el esfuerzo de volver a escribir la consulta que utiliza con frecuencia para el análisis o la solución de problemas. Las siguientes opciones se guardan con la consulta:

- Filtros de búsqueda aplicados
- Fuente de datos seleccionada y duración

Haga lo siguiente para guardar una consulta de autoservicio:

1. Seleccione el origen de datos y la duración necesarios.
2. Escriba una consulta en la barra de búsqueda.
3. Aplica los filtros necesarios.
4. Haga clic en **Guardar búsqueda**.
5. Especifique el nombre para guardar la consulta personalizada.

> **Nota**
>
> Asegúrese de que el nombre de la consulta sea exclusivo. De lo contrario, la consulta no se guarda.

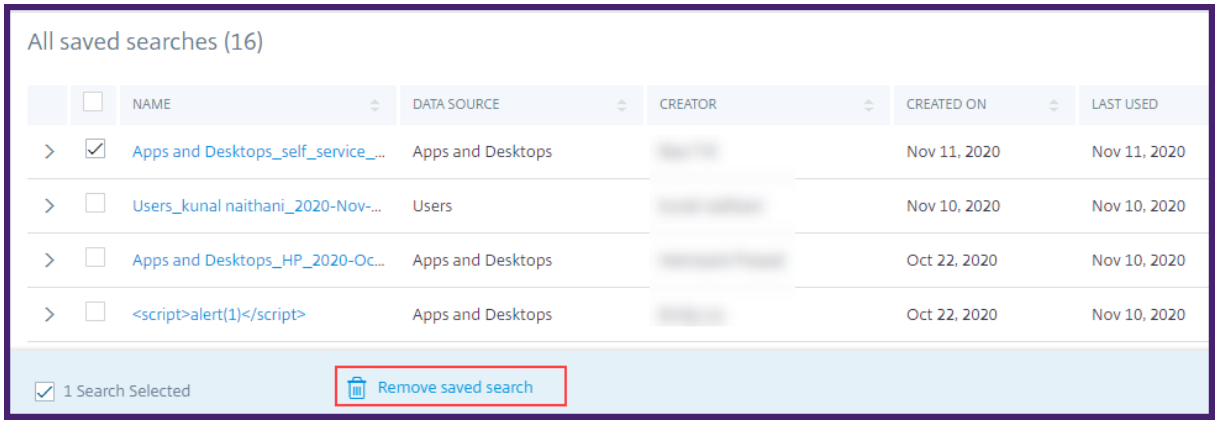
6. Active el botón **Programar informe por correo electrónico** si quiere enviar una copia del informe de consulta de búsqueda a sí mismo y a otros usuarios a intervalos regulares. Para obtener más información, consulte Programar un correo electrónico para una consulta de búsqueda.
7. Haga clic en **Guardar**.

Para ver las búsquedas guardadas:

1. Pulse **Ver búsquedas guardadas**.
2. Haga clic en el nombre de la consulta de búsqueda.

Para eliminar una búsqueda guardada:

1. Pulse **Ver búsquedas guardadas**.
2. Seleccione la consulta de búsqueda que ha guardado.
3. Haga clic en **Eliminar búsqueda guardada**.



Para modificar una búsqueda guardada:

1. Pulse **Ver búsquedas guardadas**.
2. Haga clic en el nombre de la consulta de búsqueda que ha guardado.
3. Modifique la consulta de búsqueda o la selección de facetas en función de su requisito.
4. Haga clic en **Actualizar búsqueda > Guardar** para actualizar y guardar la búsqueda modificada con el mismo nombre de consulta de búsqueda.

5. Si quiere guardar la búsqueda modificada con un nombre nuevo, haga clic en la flecha hacia abajo y haga clic en **Guardar como nueva búsqueda > Guardar como**.

Si reemplaza la búsqueda por un nuevo nombre, la búsqueda se guardará como una nueva entrada. Si conserva el nombre de búsqueda existente durante la sustitución, los datos de búsqueda modificados anulan los datos de búsqueda existentes.

> **Nota**
>
> - Solo el propietario de una consulta puede modificar o eliminar sus búsquedas guardadas.
> - Puede copiar la dirección de enlace de búsqueda guardada para compartirla con otro usuario.

Programar un correo electrónico para una consulta de búsqueda

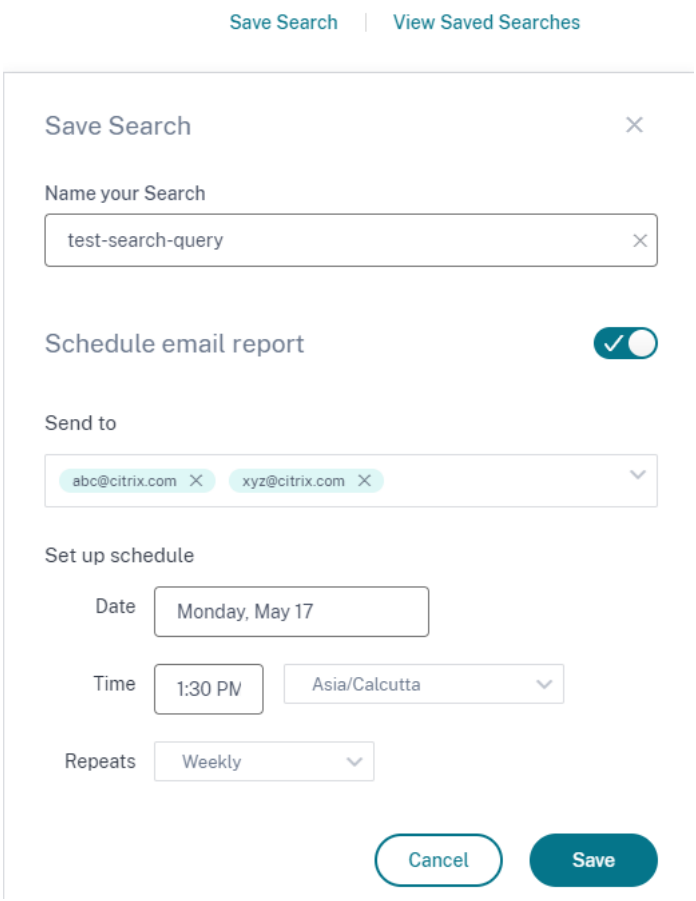
Puede enviarte una copia del informe de consultas de búsqueda a ti mismo y a otros usuarios a intervalos regulares configurando un calendario de entrega de correo electrónico.

Esta opción solo está disponible si el informe de consulta de búsqueda contiene datos en formatos visuales como gráficos de barras o detalles de línea de tiempo. De lo contrario, no puede programar una entrega por correo electrónico. Por ejemplo, puede programar un correo electrónico para los orígenes de datos, como Aplicaciones y escritorios, Sesiones, donde verá los datos como detalles de la línea de tiempo y gráficos de barras. Para los orígenes de datos como Usuarios y Equipos, los datos solo se ven en formato tabular. Por lo tanto, no puede programar un correo electrónico.

Programar un correo electrónico mientras se guarda una consulta de búsqueda

Al guardar una consulta de búsqueda, configura un calendario de entrega de correo electrónico de la siguiente manera:

1. En el cuadro de diálogo **Guardar búsqueda**, active el botón **Programar informe por correo electrónico**.



2. Introduce o pega las direcciones de correo electrónico de los destinatarios.

> **Nota**
>
> Los grupos de correo electrónico no son compatibles.

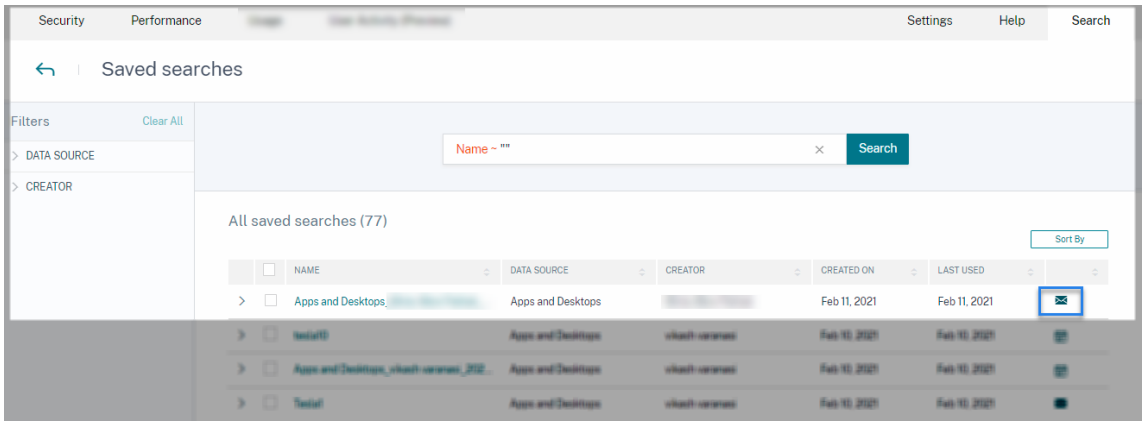
3. Establece la fecha y la hora de entrega del correo electrónico.
4. Seleccione la frecuencia de entrega: diaria, semanal o mensual.
5. Haga clic en **Guardar**.

Programar un correo electrónico para una consulta de búsqueda ya guardada

Si quiere configurar un calendario de entrega de correo electrónico para una consulta de búsqueda que guardaste anteriormente, haga lo siguiente:

1. Pulse **Ver búsquedas guardadas**.
2. Vaya a la consulta de búsqueda que ha creado. Haga clic en el icono **Enviar esta consulta por correo electrónico**.

> **Nota**
>
> Solo el propietario de una consulta puede programar la entrega por correo electrónico de su consulta de búsqueda guardada.



3. Active el botón **Programar informe por correo electrónico**.
4. Introduce o pega las direcciones de correo electrónico de los destinatarios.

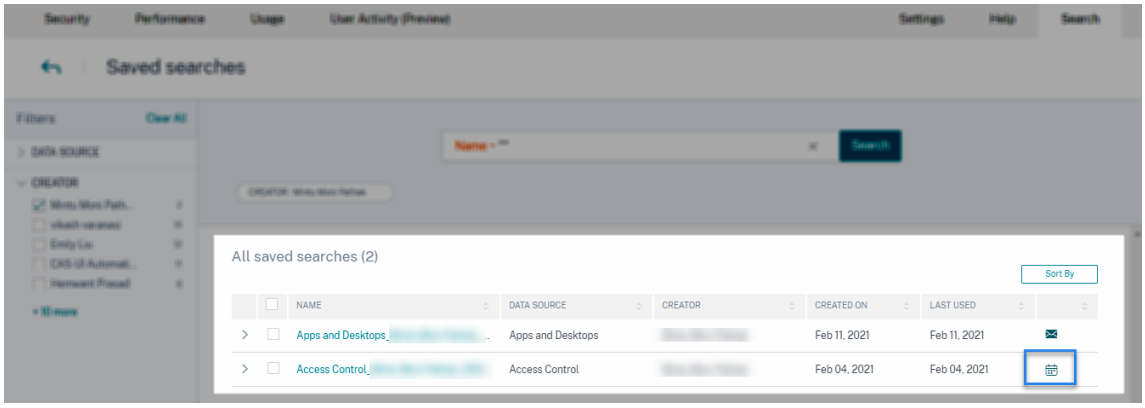
> **Nota**
>
> Los grupos de correo electrónico no son compatibles.

5. Establece la fecha y la hora de entrega del correo electrónico.
6. Seleccione la frecuencia de entrega: diaria, semanal o mensual.
7. Haga clic en **Guardar**.

Detener un programa de entrega de correo electrónico para una consulta de búsqueda

1. Pulse **Ver búsquedas guardadas**.
2. Vaya a la consulta de búsqueda que ha creado. Haga clic en el icono **Ver calendario de entrega de correo electrónico**.

> **Nota**
>
> Solo el propietario de una consulta puede detener la programación de correo electrónico de su consulta de búsqueda guardada.



3. Desactive el botón **Programar informe por correo electrónico**.
4. Haga clic en **Guardar**.

Contenido del correo electrónico

Los destinatarios reciben un correo electrónico de "Citrix Cloud - Notificaciones < donotreplynotifications@citrix.com >"sobre el informe de consultas de búsqueda. El informe se adjunta como documento PDF. El correo electrónico se envía a intervalos regulares definidos por usted en la configuración **Programar informe de correo electrónico**.

El informe de consultas de búsqueda contiene la siguiente información:

- Consulta de búsqueda que ha especificado para los eventos del período seleccionado.
- Las facetas (filtros) que ha aplicado a los eventos.
- El resumen visual, como los gráficos de línea de tiempo, gráficos de barras o gráficos de los eventos de búsqueda.

Permisos para administradores de acceso total y acceso de solo lectura

- Si es administrador de Citrix Cloud con acceso completo, puede usar todas las funciones disponibles en la página **Buscar**.
- Si es administrador de Citrix Cloud con acceso de solo lectura, solo puede realizar las siguientes actividades en la página **Buscar**:
  - Para ver los resultados de la búsqueda, seleccione una fuente de datos y el período de tiempo.
  - Introduzca una consulta de búsqueda y consulte los resultados de la búsqueda.
  - Permite ver los resultados de búsqueda guardados de otros administradores.

- Exporte el resumen visual y descargue los resultados de la búsqueda en un archivo CSV.

Para obtener información sobre las funciones de administrador, consulte Administrar funciones de administrador para Citrix Analytics.

Parámetros de alertas

December 7, 2023

Citrix Analytics genera alertas en función de los criterios de la directiva de alertas. Puede configurar la recepción de notificaciones de alerta de Citrix Analytics for Security and Performance por correo electrónico y Webhook.

- Lista de distribución de correo electrónico
- Webhook para notificaciones de alertas

Puede formatear la notificación por correo electrónico para las alertas de Citrix Analytics for Security.

- Configuración del correo electrónico del usuario final

Listas de distribución de correo electrónico

December 7, 2023

Cuando se aplica la acción **Notificar a los administradores** ya sea manualmente o mediante la creación de una directiva, se envía una notificación a los administradores seleccionados sobre el indicador de riesgo.

> **IMPORTANTE**
>
> Puede seleccionar administradores de los dominios de Citrix Cloud y otros dominios de su organización que no sean de Citrix Cloud.

Para enviar notificaciones a los grupos de administradores apropiados, cree una lista de distribución con sus direcciones de correo electrónico.

Con la lista de distribución de correo electrónico, puede hacer lo siguiente:

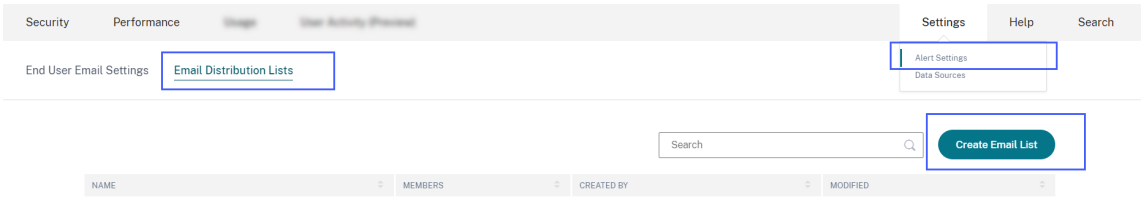
- Cree una lista de distribución de correo electrónico común con miembros de diferentes dominios de su organización.

- Notifica a todos los miembros de una vez.
- Ahorre tiempo y esfuerzo al seleccionar los administradores de diferentes dominios.
- Administre y mantenga las listas de distribución de correo electrónico en función de sus requisitos, como agregar nuevos miembros o eliminar miembros existentes.

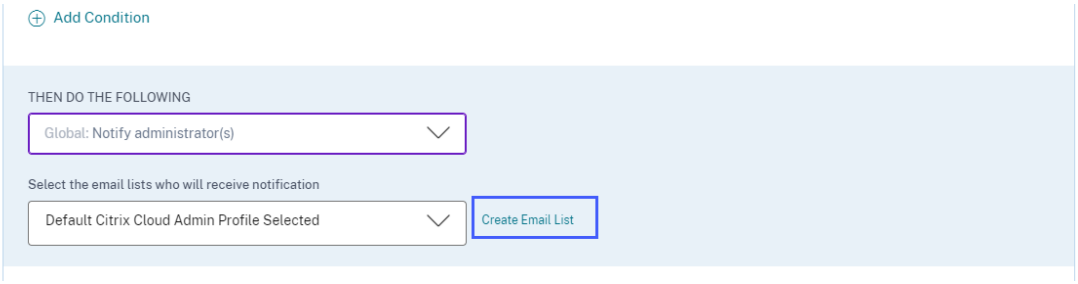
Crear lista de distribución de correo electrónico

Para crear una lista de distribución de correo electrónico:

1. Haga clic en **Configuración > Configuración de alertas > Listas de distribución de correo electrónico > Crear lista de correo electrónico**.



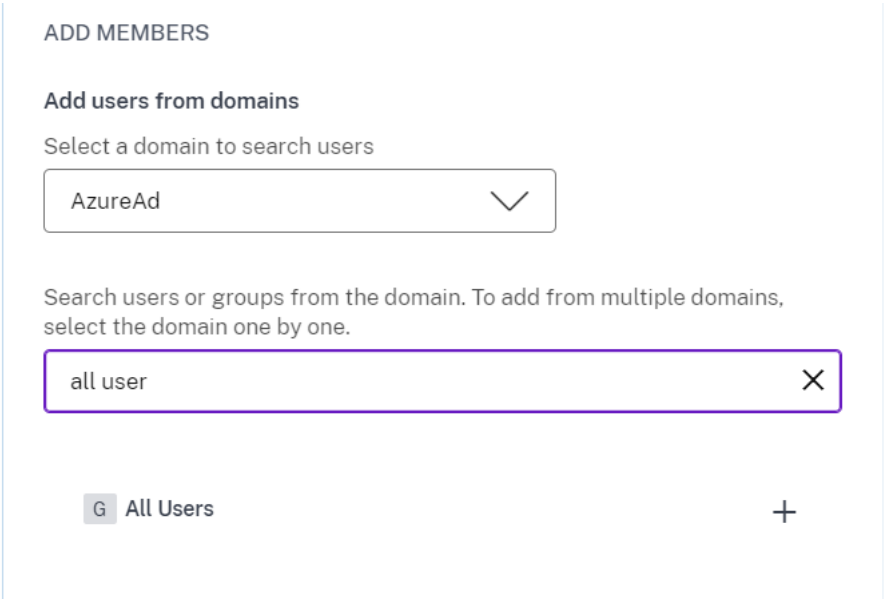
   Como alternativa, también puede crear una lista de distribución de correo electrónico a partir de una directiva. Modifique una directiva existente o cree una directiva y seleccione la acción **Notificar a los administradores**. Haga clic en el enlace **Crear lista de correos electrónicos**.



2. Introduzca un nombre y una descripción de la lista de distribución de correo electrónico para identificar su propósito.
3. Use las siguientes opciones para agregar miembros a la lista de distribución de correo electrónico:
   - **Agrega usuarios de dominios**. Esta opción requiere que los dominios estén conectados con Citrix Cloud.
   - **Agregue usuarios por direcciones de correo electrónico**. Usa esta opción si quiere agregar usuarios que están fuera de los dominios seleccionados.
4. Para agregar usuarios de dominios, seleccione un dominio y busque los usuarios o los grupos de usuarios.

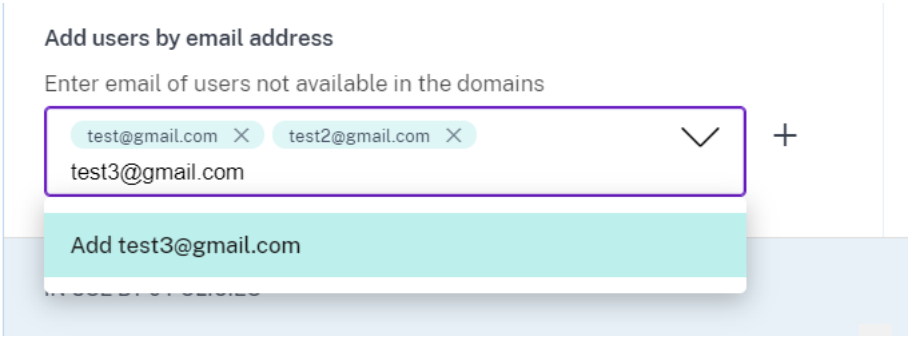
> **Nota**
>
> También puede agregar usuarios y grupos de usuarios de varios dominios seleccionando los dominios uno por uno. Para cada dominio, busque y agregue los usuarios o el grupo de usuarios.

5. Haga clic en el icono **Agregar** junto al usuario o al grupo de usuarios.



6. Para agregar usuarios que no estén disponibles en el dominio seleccionado, introduzca las direcciones de correo electrónico de los usuarios o las listas de distribución de correo electrónico.

> **Nota**
>
> Antes de entrar en una lista de distribución de correo electrónico, asegúrese de que puede acceder a la lista de distribución de correo electrónico desde fuera de la red de su organización. Si agrega una lista de distribución de correo electrónico que es interna en su organización, los miembros de la lista no pueden recibir ninguna notificación de Citrix Analytics.



7. Haga clic en **Crear lista de correos electrónicos**.

Ver lista de distribución de correo electrónico

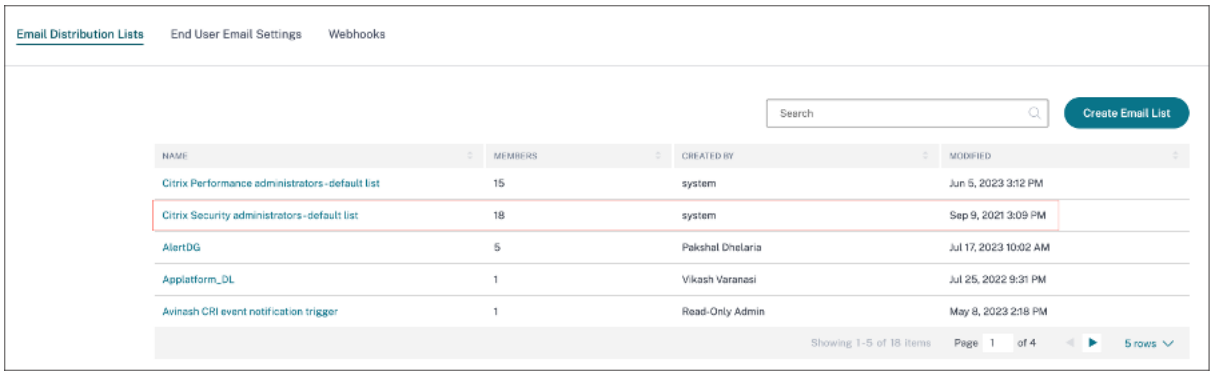
Para ver las listas de distribución de correo electrónico, haga clic en **Configuración > Configuración de alertas > Listas de distribución de correo electrónico**.

La página muestra todas las listas de distribución de correo electrónico creadas en su cuenta. Seleccione una lista de distribución de correo electrónico para ver los miembros o modificar la lista.

Verás una lista de distribución de correo electrónico creada de forma predeterminada en su cuenta. Contiene los administradores de Citrix Cloud cuya opción **Notificaciones por correo electrónico** está habilitada en sus cuentas de Citrix Cloud. No puede eliminar ni modificar la lista predeterminada.

> **Nota**
>
> Para la lista de distribución de correo electrónico predeterminada, Citrix Analytics almacena en caché la información sobre los administradores cuyas notificaciones por correo electrónico están habilitadas. La memoria caché se actualiza una vez cada 24 horas. Por lo tanto, si algún administrador cambia las preferencias de notificación por correo electrónico, este cambio se actualiza en Citrix Analytics después de 24 horas.
>
> Por ejemplo, si un administrador de Citrix Cloud habilita sus notificaciones por correo electrónico, comenzarán a recibir notificaciones pasadas 24 horas, no de forma instantánea. Del mismo modo, si un administrador de Citrix Cloud inhabilita sus notificaciones por correo electrónico, dejará de recibirlas después de 24 horas.

La lista de distribución predeterminada para los administradores de seguridad ahora incluye administradores completos y personalizados que tienen habilitada la opción **Notificaciones por correo electrónico** en sus cuentas de Citrix Cloud.



Modificar una lista de distribución de correo electrónico

Para modificar una lista de distribución de correo electrónico:

1. Haga clic en **Configuración > Configuración de alertas > Listas de distribución de correo electrónico**

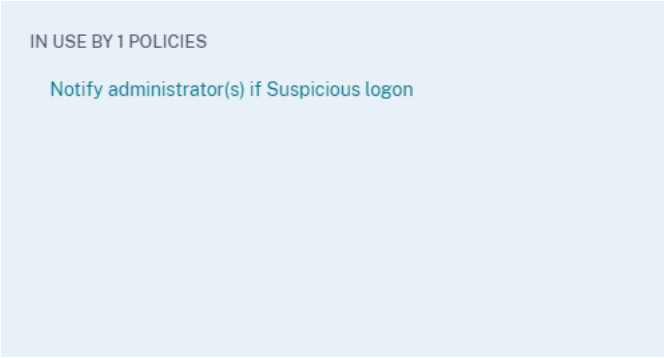
2. Haga clic en la lista de distribución de correo electrónico que quiere modificar.
3. En la lista de distribución de correo electrónico, actualice los detalles requeridos, como el nombre, la descripción, y agregue o elimine miembros.
4. Haga clic en **Guardar cambios**.

Eliminar una lista de distribución de correo electrónico

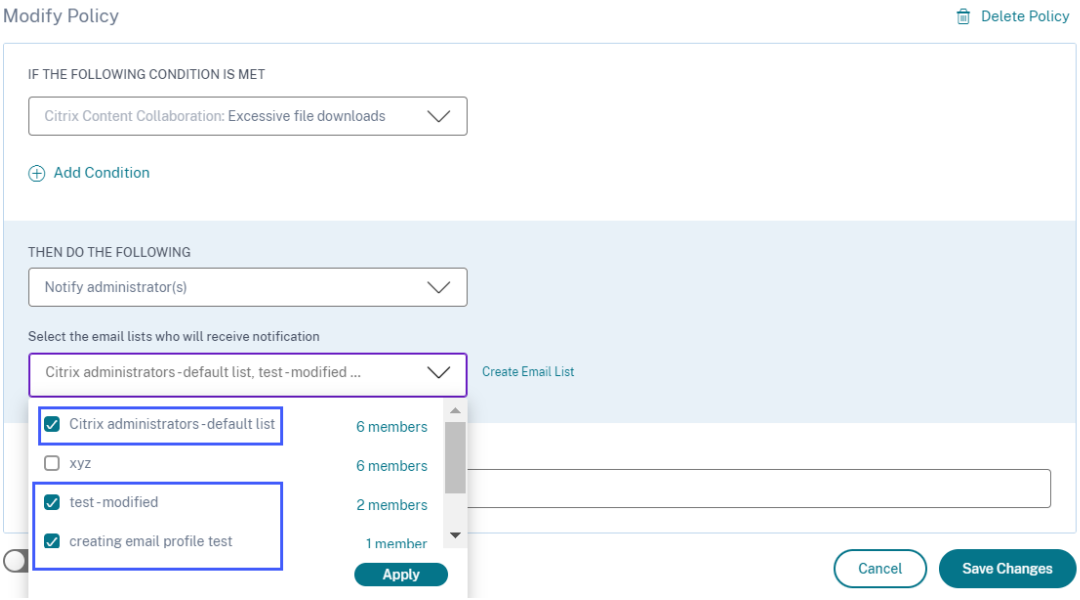
Puede eliminar una lista de distribución de correo electrónico solo si no está vinculada a ninguna directiva. Si está vinculado a algunas directivas, primero debe eliminar la lista de distribución de correo electrónico de las directivas asociadas.

Para eliminar una lista de distribución de correo electrónico:

1. Haga clic en **Configuración > Configuración de alertas > Listas de distribución de correo electrónico**
2. Haga clic en la lista de distribución de correo electrónico que deseas eliminar.
3. En la lista de distribución de correo electrónico, vea las directivas asociadas.



4. Haga clic en la directiva para abrirla y eliminar las listas de distribución de correo electrónico. También puede eliminar la directiva si lo quiere.



5. Haga clic en **Guardar cambios** y vuelve a la lista de distribución de correo electrónico.
6. Abra la lista de distribución de correo electrónico y haga clic en el icono **Eliminar**.

Webhook para notificaciones de alertas

June 19, 2023

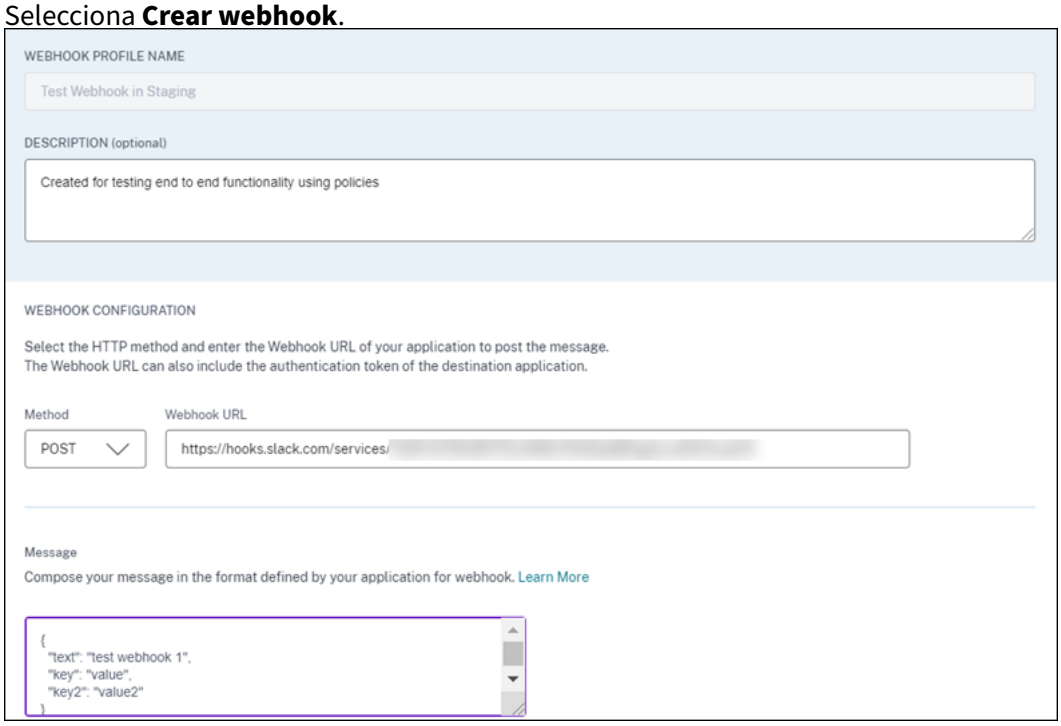
Puede usar webhooks para enviar notificaciones de alertas de Citrix Analytics a cualquier aplicación de terceros que tenga configuradas las URL de webhook entrantes. Los webhooks son devoluciones de llamadas HTTP que permiten enviar mensajes en tiempo real entre las aplicaciones del proveedor de servicios y las aplicaciones para consumidores. Dado que las notificaciones de alerta se envían en tiempo real, se le notifica cuando se producen los eventos.

Cuando Citrix Analytics activa una alerta, el webhook asociado envía el mensaje de alerta a la URL de la aplicación de destino. La alerta se envía en forma de carga JSON a través de la solicitud HTTP POST o PUT. Por ejemplo, cuando un usuario activa un indicador de riesgo o el rendimiento de una máquina de VDI disminuye, puede configurar un webhook para enviar las notificaciones de alertas a su canal de Slack.
La configuración de webhooks para la gestión de alertas le ayuda a recibir notificaciones en tiempo real en sus aplicaciones. Puede tomar medidas oportunas para mitigar el riesgo de seguridad o mejorar el rendimiento de su implementación de Citrix Virtual Apps and Desktops.

Crear perfil de Webhook

Para crear los perfiles de webhook en Citrix Analytics:

1. Inicie sesión en Citrix Analytics.
2. Según la oferta a la que se haya suscrito, haga clic en **Administrar** para acceder a Security Analytics o Performance Analytics.
3. En la barra superior, haga clic en **Configuración > Configuración de alertas > Webhook**.
4. Selecciona **Crear webhook**.



5. Introduzca un nombre de perfil y una descripción del webhook para identificar su propósito.
6. Seleccione el método HTTP y la URL del webhook de su aplicación para enviar el mensaje de alerta.

> **Nota:**
> Por lo general, los webhooks salientes se envían a través de la solicitud HTTP POST. También puede incluir un token de autenticación en la URL del webhook de su aplicación.

7. Introduzca el mensaje sobre la alerta que quiere enviar a la URL del webhook. El mensaje debe estar estructurado en los formatos, como JSON o XML, tal como los define la aplicación de destino. Para obtener más información, consulte los ejemplos de Webhook.
8. (Opcional) Introduzca las claves de encabezado y los valores del mensaje. El encabezado puede incluir tokens de autenticación u otros pares clave-valor personalizados para enviar la carga a

la aplicación de forma segura.

9. Para validar la configuración del webhook, haga clic en **Probar**.
   La prueba valida la URL del webhook saliente, la estructura de carga y las claves de encabezado. Si no se encuentra ningún problema en la configuración, aparecerá el mensaje "La prueba se ha realizado correctamente".

Ejemplos de configuración de webhook

La sección proporciona ejemplos de configuración de webhooks para enviar alertas a aplicaciones de terceros, como Slack y Microsoft Teams.

> **Nota:**
> Consulte la documentación del producto de las aplicaciones de terceros para obtener la URL del webhook y las configuraciones necesarias para el webhook.

Enviar un mensaje de alerta a Slack

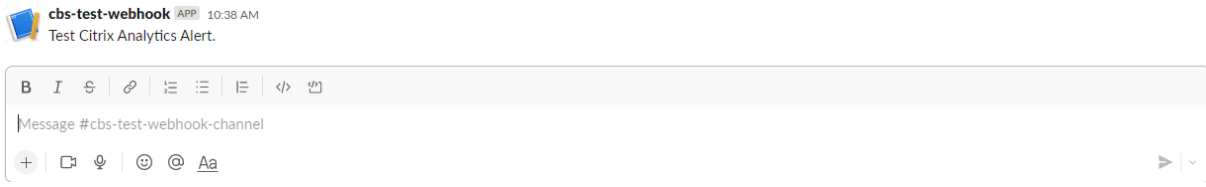
En Slack, asegúrate de haber completado las siguientes tareas antes de enviar una alerta:

1. Crea una aplicación de Slack para Citrix Analytics si aún no tienes una.
2. Para la aplicación, habilita la función Webhook entrante y crea un Webhook entrante.
3. Selecciona el canal en el que la aplicación publique el mensaje.
4. Cuando autorizas la aplicación, obtienes la URL del Webhook para enviar el mensaje.
   Para obtener más información, consulte Introducción a los webhooks entrantes.

Formato de mensaje de ejemplo

```
curl --location --request POST 'WEBHOOK URL'
--header 'Content-Type: application/json'--data-raw '{ "text": "Test
Citrix Analytics Alert." }
```

Resultado



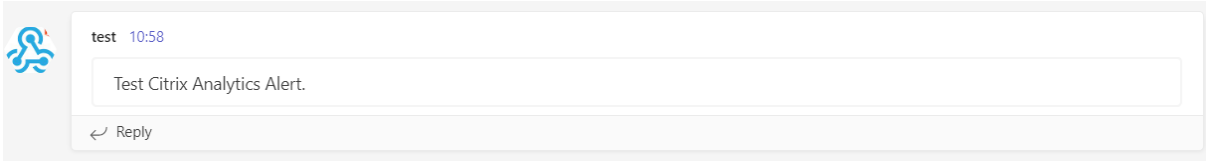
Enviar un mensaje de alerta a Microsoft Teams

En Microsoft Teams, asegúrese de haber completado las siguientes tareas antes de enviar una alerta:

1. Crea un grupo de equipos dentro de Teams si aún no tienes uno.
2. Crea un conector Webhook. Consulte los pasos que se describen en el artículo Crear y enviar mensajes .
3. Obtenga la URL del webhook.

Formato de mensaje de ejemplo `curl --location --request POST 'WEBHOOK URL' --header 'Content-Type: application/json'--data-raw '{ "text": "Test Citrix Analytics Alert." }`

Resultado



Citrix Analytics para la seguridad (análisis de seguridad)

February 12, 2024

Con la ventaja de trabajar desde cualquier lugar, en cualquier momento y dispositivo en cualquier red, los datos corporativos confidenciales quedan más expuestos que cuando los usuarios solo trabajaban desde una oficina corporativa aislada. Los usuarios malintencionados tienen una gran superficie de ataque a la que dirigirse. Los equipos de TI se encargan de ofrecer una excelente experiencia de usuario sin comprometer la seguridad. Citrix Analytics for Security puede ayudar a cerrar esa brecha centrándose en la seguridad del usuario.

¿Qué es el análisis de seguridad?

Citrix Analytics for Security evalúa continuamente el comportamiento de los usuarios de Citrix Virtual Apps and Desktops, los usuarios de Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) y los usuarios de Citrix Workspace. Aplica acciones para proteger la información corporativa confidencial. La agregación y correlación de datos entre redes, aplicaciones virtualizadas y herramientas de escritorios permite generar información valiosa y acciones más específicas para abordar las amenazas a la seguridad de los usuarios. Además, el aprendizaje automático admite enfoques altamente predictivos para identificar comportamientos malintencionados de los usuarios.

Funciones

- Perspectivas optimizadas de los productos Citrix y las integraciones de socios. Para obtener más información, consulte Búsqueda de autoservicio.
- Los paneles de control fáciles de consumir proporcionan una visión completa del comportamiento de los usuarios. Para obtener más información, consulte Panel de control de usuarios.
- Detecte y mitigue el comportamiento malintencionado de los usuarios mediante el aprendizaje automático y las directivas personalizadas con acciones automatizadas. Para obtener más información, consulte Directivas y acciones.
- La supervisión continua del comportamiento de los usuarios después de la autenticación inicial en las redes corporativas equilibra la seguridad completa y la excelente experiencia del usuario. Para obtener más información, consulte Evaluación continua de riesgos.

Paneles

Puede ver detalles sobre el comportamiento de los usuarios o entidades en los siguientes paneles de seguridad:

- Usuarios: proporciona visibilidad de los patrones de comportamiento de los usuarios en una organización.
- Acceso del usuario: resume la cantidad de dominios de riesgo a los que se accede y el volumen de datos cargados y descargados por los usuarios de su red.
- Acceso a aplicaciones: resume los detalles de los dominios, las URL y las aplicaciones a las que acceden los usuarios de la red.

- Ubicación de Access Assurance: resume los detalles de acceso y los detalles de inicio de sesión de los usuarios de Citrix Virtual Apps and Desktops y los usuarios de Citrix DaaS.
- Informes: cree informes personalizados basados en las dimensiones y métricas disponibles en los orígenes de datos incorporadas.

A continuación

- Requisitos del sistema: requisitos mínimos que deben cumplirse antes de empezar.
- Orígenes de datos: conozca los productos que admite Analytics.
- Control de datos: conozca la recopilación, el almacenamiento y la retención de registros por parte de Analytics.
- Comenzar: cómo empezar a utilizar Analytics en su organización.

Citrix Analytics para el rendimiento (Performance Analytics)

September 21, 2023

Qué es Performance Analytics

Performance Analytics es una oferta de Citrix Analytics que le permite realizar un seguimiento, agregar y visualizar los indicadores clave de rendimiento de su entorno de aplicaciones y escritorios.

- Performance Analytics agrega métricas de rendimiento del sitio en paneles de experiencia de usuario e infraestructura fáciles de ver. Los paneles le ayudan a analizar la experiencia del usuario y a optimizar el uso de sus sitios de Apps y escritorios.
- Performance Analytics admite la agregación y los informes de varios sitios. Agrega métricas de rendimiento en las configuraciones en la nube y en las instalaciones. Por lo tanto, puede ver los datos de todos los sitios de su entorno en una sola consola.
- Performance Analytics cuantifica los factores de rendimiento de los usuarios y los clasifica en función de estos factores. Proporciona información útil para solucionar problemas de fallos, retrasos de pantalla, retrasos en los inicios de sesión y otros indicadores de rendimiento.
- Performance Analytics le permite buscar y filtrar métricas para reducir las métricas a usuarios o sesiones específicos que enfrentan problemas de rendimiento.

Cómo utilizar Performance Analytics

Panel de experiencia del usuario

El panel de control de experiencia del usuario muestra el rendimiento del sitio en relación con factores como la capacidad de respuesta de la sesión, la duración del inicio de sesión, los errores de sesión y las reconexiones de sesiones que definen conjuntamente la experiencia del usuario.

Si es compatible con varios usuarios de aplicaciones y escritorios virtuales de su organización y, en ocasiones, experimentan retrasos al iniciar aplicaciones o escritorios, la métrica de duración de los inicios de sesión puede proporcionarle información sobre el problema. El desglose puede ayudar a identificar los factores que conducen a los problemas.

Panel de control de infraestructura

El panel de infraestructura muestra el estado y el estado de las máquinas de su sitio. Cuando se usan juntos, los paneles de usuario e infraestructura pueden ayudarle a comprobar de forma proactiva la disponibilidad de los recursos e identificar cuellos de botella de rendimiento en los sitios.

- Si las tendencias de usuarios o sesiones muestran una caída, lo que indica una reducción en el número de usuarios o sesiones iniciadas en el sitio, utilice este indicador para comprobar si se ha reiniciado un hipervisor o si el número de equipos es insuficiente.
- Si vaya varios casos en los que las sesiones no se inician, desglose para establecer la causa del error. Puede haber una escasez en el número de licencias o problemas con la conexión de la máquina al Delivery Controller.

> **Nota:**
>
> El **panel de mandos de análisis de infraestructura** se encuentre actualmente en Tech Preview.

Con Performance Analytics puede analizar rápidamente los problemas, solucionarlos y resolverlos, y mantener un nivel óptimo de servicio de aplicaciones y escritorios.

Introducción

Requisitos previos

1. Compruebe si su estación de trabajo tiene un explorador web compatible que aparece en el artículo Exploradores compatibles. Para obtener información sobre los requisitos del sistema, consulte el artículo Requisitos del sistema de Citrix Analytics.

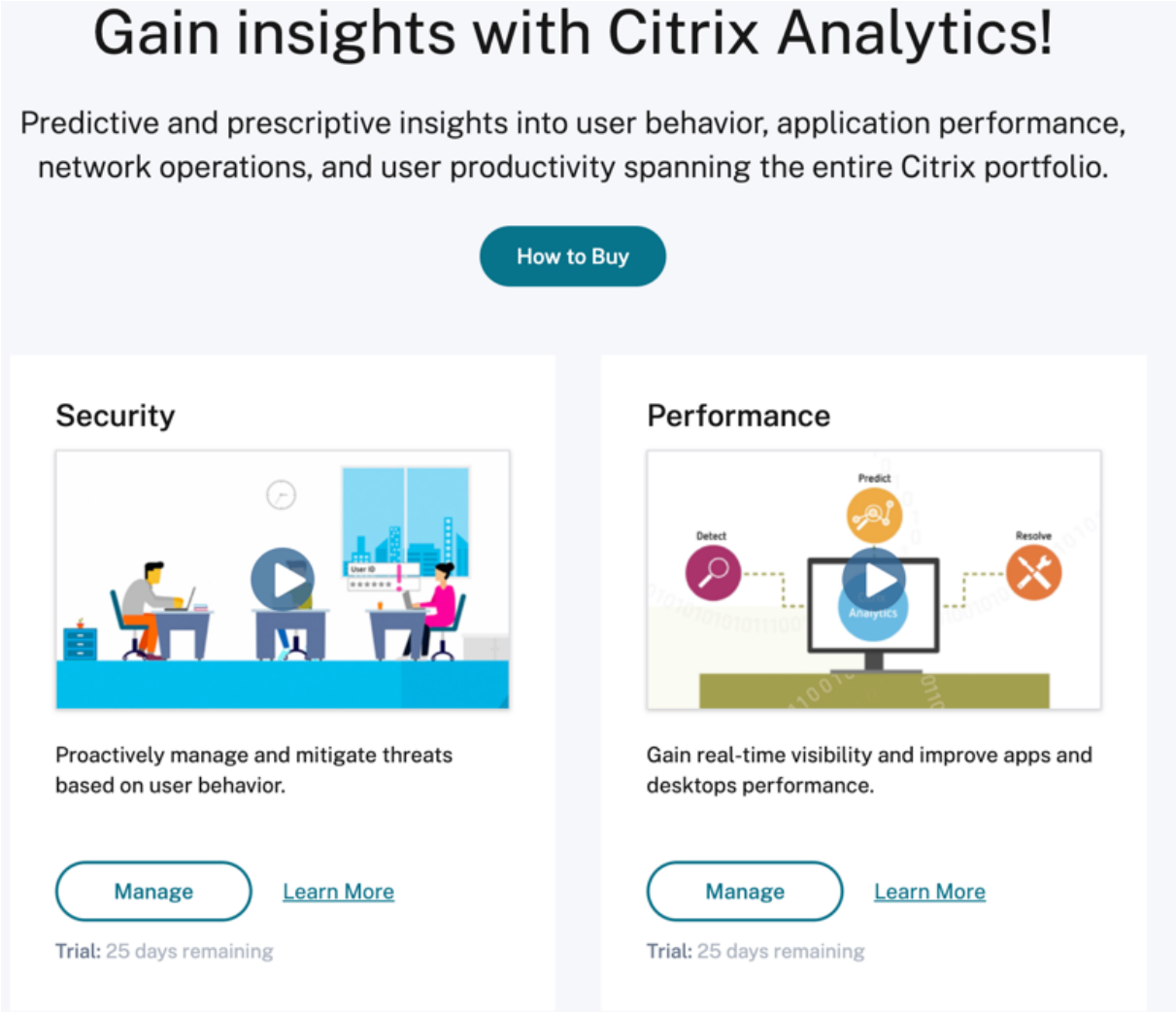
2. Debe tener una cuenta de Citrix Cloud para utilizar el servicio Analytics. Para obtener instrucciones detalladas sobre cómo crear una cuenta de Citrix Cloud, consulte Inscribirse en Citrix Cloud. Vaya a https://citrix.cloud.com e inicie sesión con su cuenta de Citrix Cloud.
3. Citrix Analytics for Performance está disponible como oferta basada en suscripción, ya sea como oferta independiente o en paquete junto con Citrix Analytics for Security. Para suscribirse a Citrix Analytics for Performance, consulte `https://www.citrix.com/products/citrix-analytics-performance.html)`.
4. Las versiones compatibles de los orígenes de datos están disponibles en el artículo Orígenes de datos.
5. Citrix Profile Management debe estar instalado en todas las máquinas.
6. El servicio End User Experience Monitoring (EUEM) debe estar en ejecución y las directivas correspondientes deben configurarse en todos los equipos. Para obtener más información, consulte Configuración de directivas de supervisión de usuarios finales.
7. La directiva de **recopilación de datos de VDA para análisis de rendimiento** debe establecerse en **Permitido** en las máquinas para permitir que el servicio de supervisión recopile métricas de rendimiento relacionadas con las máquinas, como estadísticas de ancho de banda y latencia. Para obtener más información, consulte Directiva de recopilación de datos para Performance Analytics.
8. Habilite la directiva de supervisión de procesos de Citrix Studio para obtener visibilidad de los procesos que consumen muchos recursos en la ficha **Estadísticas de máquinas > Procesos**. Para obtener más información, consulte Habilitar la supervisión de procesos.
9. Garantizar la accesibilidad a estas URL desde todos los dispositivos de punto final (o proxies, si están configurados)

Dispositivo de punto final	Región de los Estados Unidos	Región de la Unión Europea	Región Asia-Pacífico Sur
Registro de claves de Citrix	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`
Citrix Cloud	`https://trust.citrixworkspacesapi.net`	`https://trust-eu.citrixworkspacesapi.net`	`https://trust-aps.citrixworkspacesapi.net`
Citrix Analytics	`https://api.was.cloud.com`	`https://api-eu.was.cloud.com`	`https://api-aps.was.cloud.com`

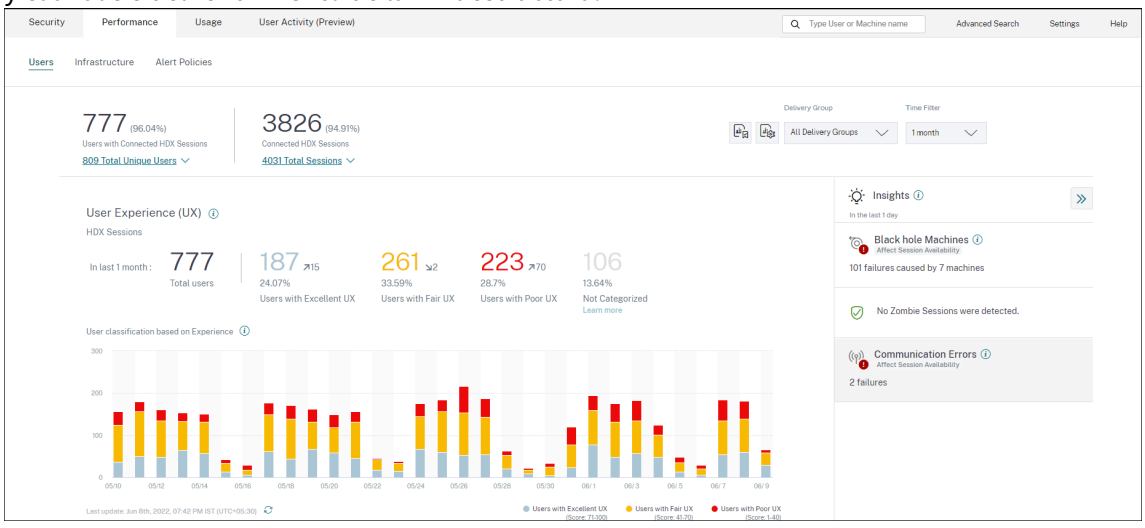
Dispositivo de punto final	Región de los Estados Unidos	Región de la Unión Europea	Región Asia-Pacífico Sur
Subida masiva	https://citrixanalyticseh-alias.servicebus.windows.net/	https://citrixanalyticsehe-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/

Acceso

1. Inicie sesión en Citrix Cloud. Busque el mosaico del servicio Analytics y haga clic en **Administrar**. La página de resumen muestra las ofertas disponibles en la cartera de Analytics.
2. En la oferta de **rendimiento**, para utilizar la versión de prueba de la oferta, haga clic en **Solicitar prueba**. Si ha adquirido la oferta de Citrix Analytics for Performance, haga clic en el enlace **Administrar** en su lugar.



1. Citrix Analytics para el rendimiento se abre con paneles que muestran la experiencia del usuario y el análisis del rendimiento de la infraestructura.



Acceso desde la región Asia Pacífico Sur Citrix Analytics for Performance ahora se incorpora automáticamente para los clientes de prueba y los clientes basados en suscripción en la región Asia Pacífico Sur (APS). Para obtener más información sobre las regiones admitidas en Citrix Cloud, consulte Consideraciones geográficas.

Para acceder a Performance Analytics desde la región APS, elija la región Asia Pacífico Sur al incorporar su arrendatario a Citrix Cloud. Inicie sesión en Citrix Cloud y seleccione su arrendatario en la región APS de Citrix Cloud. Utilice la URL `https://analytics-aps.cloud.com` para acceder a su servicio Citrix Analytics Cloud.

- Citrix Analytics for Performance ahora almacena los eventos de usuario y los metadatos de su organización en la región Sur de Asia Pacífico cuando la elige como su región de origen. Para obtener más información, consulte Gobernanza de datos.
- Para obtener información sobre los requisitos de red para la región Asia Pacífico Sur, consulte Descripción general de seguridad técnica.

Configurar orígenes de datos

Puede utilizar Performance Analytics para supervisar sitios locales o en la nube. Puede usar esta oferta tanto si es un cliente local, un cliente de Cloud o un cliente híbrido con una combinación de sitios locales y Cloud Sites.

Performance Analytics detecta automáticamente su Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).
Si es cliente local,

- Primero incorpore sus sitios de Citrix Virtual Apps and Desktops a Performance Analytics.
- Para obtener información relacionada con la red en Performance Analytics, también debe incorporarse su NetScaler Gateway local.

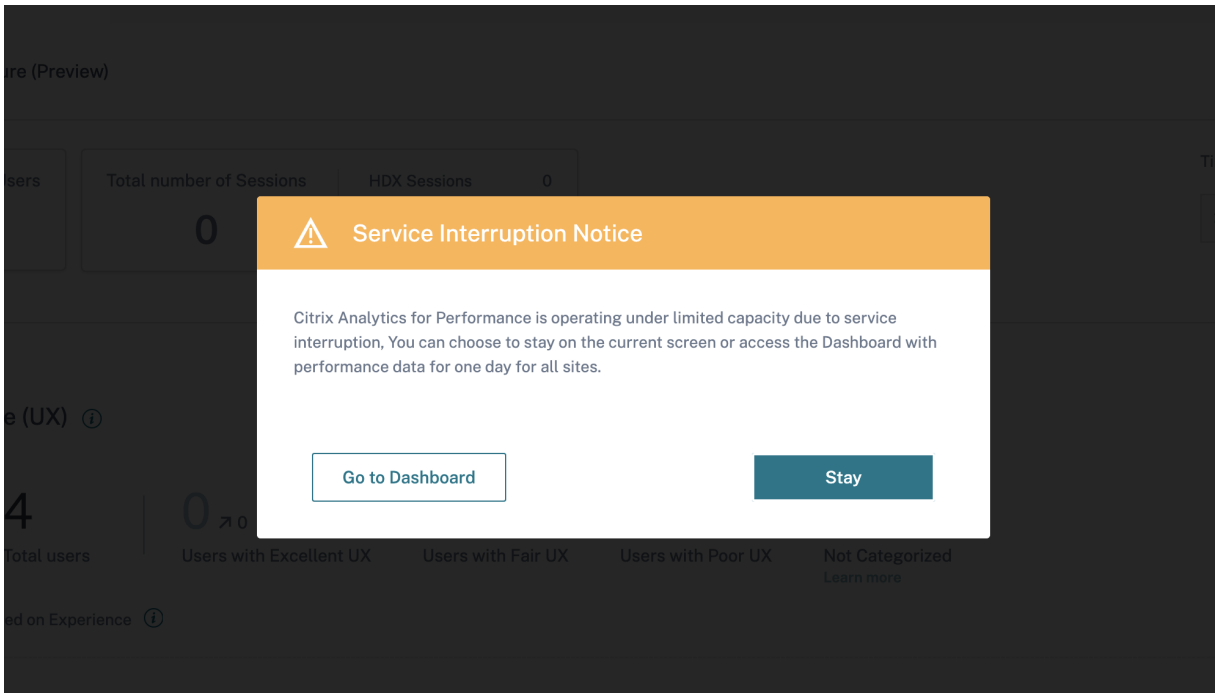
Configure los orígenes de datos necesarios como se describe en el artículo Orígenes de datos.

> **Nota:**
>
> - Citrix Analytics for Performance recopila y almacena registros de puntos de datos según se indica en Registros recopilados para Citrix Analytics for Performance.
> - Los límites recomendados para el servicio Citrix Analytics for Performance se enumeran en el artículo Límites.

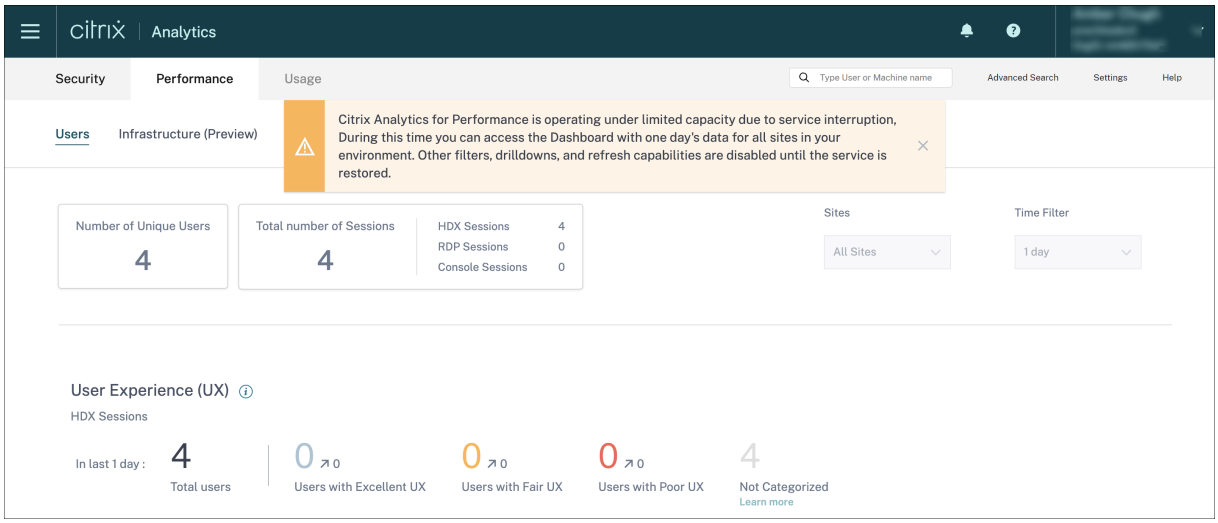
Continuidad del servicio

En caso de interrupción del servicio, Citrix Analytics for Performance funciona con una capacidad limitada.

El administrador puede elegir **quedarse** y ver los datos disponibles en la pantalla actual o **Ir al panel de control** en modo degradado.



En el modo degradado, el usuario cambia al panel de control que contiene los datos de todos los sitios del último día.
Todos los filtros y los desniveles se desactivan hasta que el servicio vuelva a funcionar normalmente en cualquier caso.



Esta actualización mejora la resiliencia del producto y ayuda a alinearse con el acuerdo de nivel de servicio.

Solución de problemas de seguridad y rendimiento de Citrix Analytics

December 7, 2023

En esta sección se explica cómo resolver los siguientes problemas que pueden surgir al utilizar Citrix Analytics for Security.

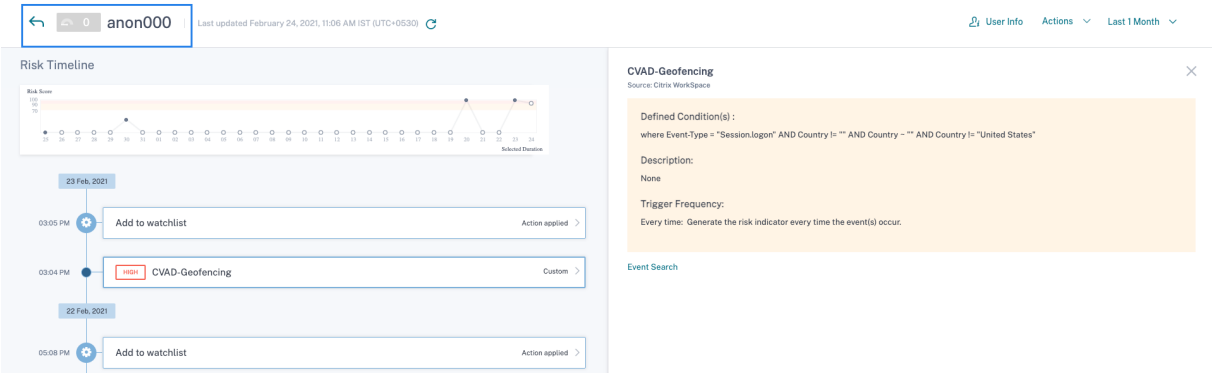
- Verificar a los usuarios anónimos como usuarios legítimos.
- Solucionar problemas de transmisión de eventos desde un origen de datos.
- Active eventos de Virtual Apps and Desktops, eventos SaaS y verificación de la transmisión de eventos a Citrix Analytics for Security.
- Elservidor de grabación de sesiones no se puede conectar.
- Problemas de configuración con el complemento Citrix Analytics para Splunk

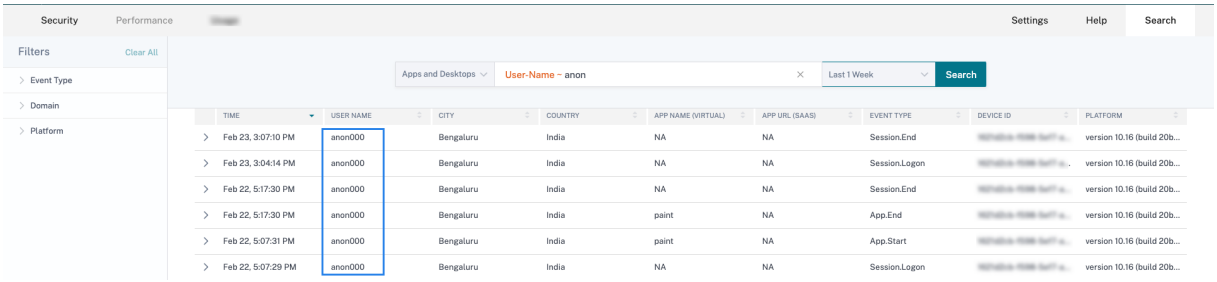
Comprobar que los usuarios anónimos son usuarios legítimos

August 23, 2022

Como administrador, puede observar que algunos usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) se muestran como anónimos en Citrix Analytics for Security. Estos usuarios se identifican como usuarios descubiertos. Sin embargo, sus nombres de usuario aparecen como anonXYZ (donde "XYZ"representa un número de tres dígitos) en las siguientes páginas:

- Usuarios
- Cronología del usuario
- Usuarios con riesgos
- Búsqueda de autoservicio de la fuente de datos de Apps y escritorios





Cuando consulte a estos usuarios, es posible que quiera saber:

- ¿Quiénes son estos usuarios?
- ¿Son estos usuarios legítimos o de naturaleza maliciosa?
- ¿Cómo verificarlas?
- ¿Qué acciones debo aplicar para estos usuarios?

Puede ver usuarios anónimos en su entorno de TI de Citrix en los siguientes escenarios:

- Cuando un usuario utiliza una aplicación de explorador segura publicada
- Cuando un usuario utiliza un almacén no autenticado

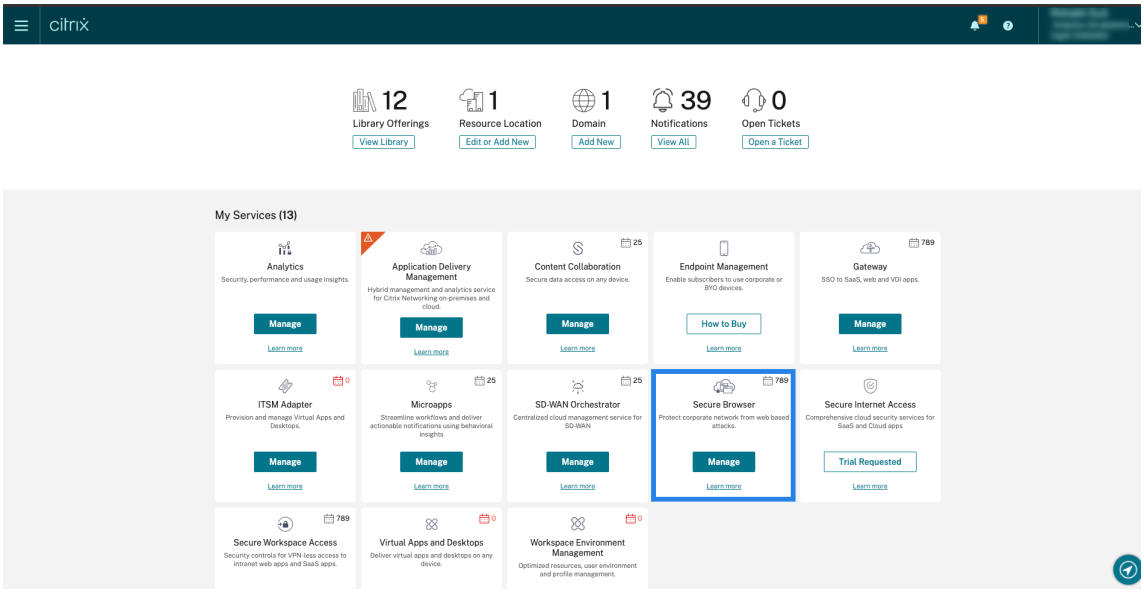
Usuario que usa aplicaciones de explorador seguras publicadas

Las aplicaciones de explorador seguro son aplicaciones web que se publican mediante Citrix Secure Browser Service. Estas aplicaciones aíslan sus eventos de navegación web y protegen su red corporativa de los ataques basados en el explorador. Para obtener más información, consulte Secure Browser Service.

Las aplicaciones de explorador seguras utilizan la capacidad de sesión anónima de Citrix DaaS.

Para comprobar si Secure Browser está configurado en su cuenta de Citrix Cloud:

1. Inicie sesión en Citrix Cloud.
2. En la tarjeta **Secure Browser**, haga clic en **Administrar**.



3. En la página **Administrar**, compruebe si hay aplicaciones de explorador seguras publicadas.

Si un usuario accede a un almacén de StoreFront a través de sitios de Citrix Receiver para Web mediante un explorador web y utiliza las aplicaciones de explorador seguras publicadas, la identidad del usuario se oculta. Por lo tanto, Citrix Analytics muestra al usuario como anónimo.

Si un usuario accede a un almacén de StoreFront a través de una aplicación Citrix Receiver o Citrix Workspace que está instalada en su dispositivo y utiliza las aplicaciones de explorador seguras publicadas, Citrix Analytics muestra al usuario como el nombre de usuario especificado en StoreFront.

Por lo tanto, puede considerar al usuario como un usuario legítimo de su organización. No necesita aplicar ninguna acción si no se asocia ningún comportamiento de riesgo con el usuario.

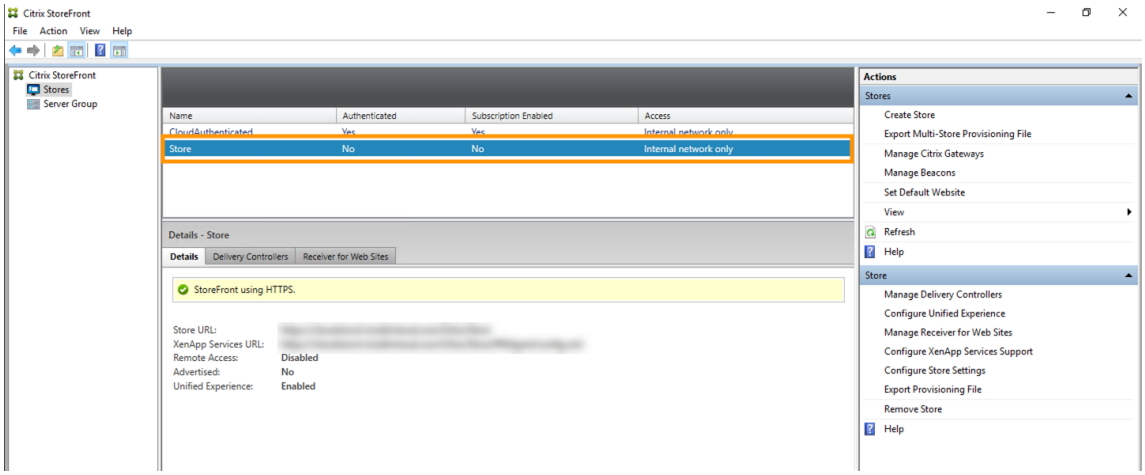
Usuario que usa un almacén no autenticado

El almacén no autenticado es una función de Citrix StoreFront y se aplica a los almacenes administrados por el cliente. Esta función admite el acceso de usuarios no autenticados (anónimos).

Para verificar si su organización tiene un almacén sin autenticar:

1. Abra Citrix Studio.

2. Haga clic en **Almacenes**.
3. Para sus almacenes, compruebe el estado de autenticación en la columna Autenticado.



Si un almacén no está autenticado y el usuario accede a ese almacén no autenticado, la identidad del usuario permanece anónima. Por lo tanto, Citrix Analytics muestra al usuario como anónimo. Puede considerar a este usuario como un usuario legítimo de su organización. No necesita aplicar ninguna acción si no se asocia ningún comportamiento de riesgo con el usuario.

Solucionar problemas de transmisión de eventos desde un origen de datos

April 12, 2024

Esta sección le ayuda a solucionar problemas de transmisión de datos en Citrix Analytics for Security. Cuando una fuente de datos no transmite los eventos de los usuarios con precisión, puede encontrar problemas como la no detección de usuarios y los indicadores de riesgo.

Lista de comprobación

Secuencia	Cheques
1	¿Tiene el derecho correcto para usar Security Analytics?
2	¿La fuente de datos se admite en su región de origen?

Secuencia	Cheques
3	¿Su entorno cumple con todos los requisitos del sistema?
4	¿Se detectan todas los orígenes de datos y se habilita el procesamiento de datos en Analytics?
5	¿Las actividades de los usuarios en la fuente de datos transmiten eventos de forma precisa a Analytics?
6	¿Los eventos de escritorios y aplicaciones virtuales se transmiten a Analytics?
7	¿Los eventos de los usuarios aparecen en la página de búsqueda de autoservicio de Analytics?
8	¿Analytics descubre a los usuarios?

Comprobación 1: ¿Tiene el derecho correcto para utilizar Security Analytics?

Citrix Analytics for Security es una oferta basada en suscripción. Para obtener más información, consulte Introducción.

Comprobación 2: ¿se admite la fuente de datos en su región de origen?

Citrix Analytics for Security se admite en las siguientes regiones de origen:

- Estados Unidos (EE. UU.)
- Unión Europea (UE)
- Sur de Asia Pacífico (APS)

Según la ubicación de su organización, puede incorporarse a Citrix Cloud en una de las regiones de origen.

Sin embargo, ciertos orígenes de datos no se admiten en todas las regiones de origen. Los [orígenes de datos](/en-us/security-analytics/data-sources.html) son los productos desde los que Citrix Analytics for Security recibe los eventos de los usuarios.

Si su organización se incorpora a Citrix Cloud en una región de origen donde no se admite una fuente de datos, no obtendrá eventos de usuario de la fuente de datos.

Use la siguiente tabla para ver los orígenes de datos y las regiones en las que se admiten.

Origen de datos	Apoyado en la región de EE. UU.	Apoyado en la región de la UE	Se admite en la región APS
Citrix Endpoint Management	Sí	Sí	Sí
Citrix Gateway (local)	Sí	Sí	Sí
Proveedor de identidades Citrix	Sí	Sí	Sí
Citrix Secure Browser	Sí	Sí	Sí
Citrix Secure Private Access	Sí	No	No
Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)	Sí	Sí	Sí
Citrix Virtual Apps and Desktops local	Sí	Sí	Sí
Microsoft Active Directory	Sí	Sí	Sí
Microsoft Graph Security	Sí	Sí	Sí

Comprobación 3: ¿Su entorno cumple con todos los requisitos del sistema?

Citrix Analytics puede tardar unos minutos en recibir los eventos de usuario de los orígenes de datos. Si no ve ningún evento de usuario en las tarjetas de sitio de origen de datos, asegúrese de que el entorno cumpla con los requisitos previos y los requisitos del sistema.

Requisitos previos

1. Todas sus suscripciones a Citrix Cloud deben estar activas. En la página de Citrix Cloud, asegúrese de que todos los servicios de Citrix Cloud estén activos.
2. Si usa local Citrix Virtual Apps and Desktops, debe agregar sus sitios a Citrix Workspace y configurar la agregación de sitios. Citrix Analytics descubre automáticamente los sitios agregados a Citrix Workspace. Para obtener más información, consulte Agregación de escritorios y aplicaciones virtuales locales en espacios de trabajo.
3. Si utiliza una implementación de StoreFront para sus sitios, configure los servidores de StoreFront para permitir que la aplicación Citrix Workspace envíe eventos de usuario a Citrix Analyt-

ics. Asegúrese de que la versión de StoreFront sea 1906 o posterior. Si no configura el servidor StoreFront, Citrix Analytics no recibe eventos de usuario de las instalaciones locales Citrix Virtual Apps and Desktops. Para configurar la implementación de StoreFront, consulte el artículo del servicio Citrix Analytics en la documentación de StoreFront.

4. Los usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS los usuarios deben usar la versión especificada de las aplicaciones Citrix Workspace o Citrix Receiver en sus puntos finales. De lo contrario, Analytics no recibe los eventos del usuario de los puntos finales del usuario. La lista de versiones compatibles de la aplicación Citrix Workspace o Citrix Receiver está disponible en Citrix Virtual Apps and Desktops y en el origen de datos de Citrix DaaS.
5. Para recibir los eventos de los usuarios de una sesión de Secure Browser publicada, habilite la configuración de **seguimiento de nombres de host** en Secure Browser. De forma predeterminada, esta configuración está inhabilitada. Para obtener más información, consulte Administrar exploradores seguros publicados.
6. Incorpore sus orígenes de datos como se menciona en los siguientes artículos:
    - Origen de datos de Citrix Endpoint Management
    - Origen de datos de Citrix Gateway
    - Origen de datos de Citrix Secure Private Access
    - Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS
    - Integración Microsoft Active Directory
    - Integración de Microsoft Graph Security

Comprobación 4: ¿Se detectan todas los orígenes de datos y se habilita el procesamiento de datos en Analytics?

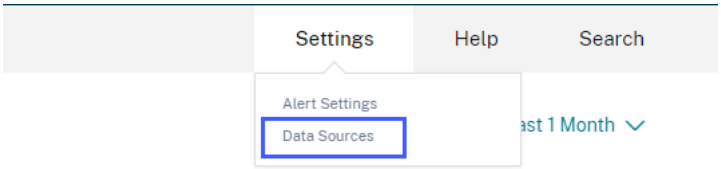
Asegúrese de que se descubran todos sus orígenes de datos y de que haya habilitado el procesamiento de datos para ellos. Si no habilita el procesamiento de datos para una fuente de datos, los usuarios que utilizan la fuente de datos no se detectan. Esta situación puede crear un riesgo potencial para la seguridad.

Habilitar el procesamiento de datos garantiza que Citrix Analytics procese los eventos de los usuarios. Los eventos se envían a Citrix Analytics solo cuando los usuarios utilizan activamente la fuente de datos.

> **Nota**
>
> Citrix Analytics no extrae datos de su entorno de forma activa.

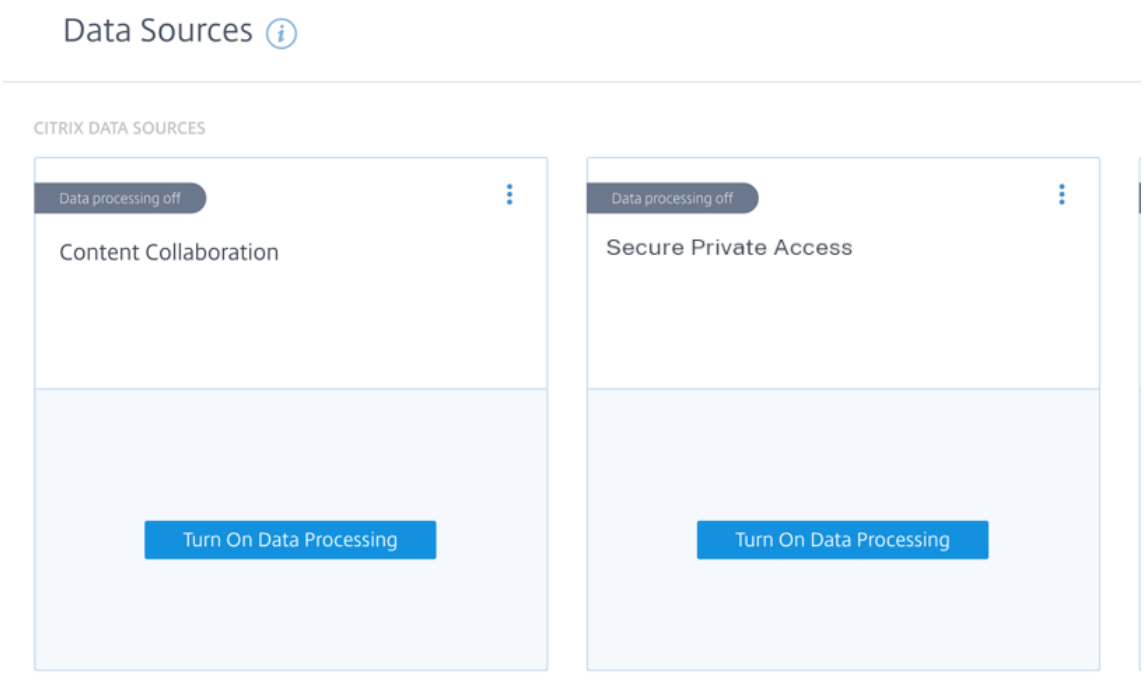
Para detectar sus orígenes de datos y habilitar el análisis, haga lo siguiente:

1. Haga clic en **Configuración** > **Orígenes de datos** > **Seguridad** para ver los orígenes de datos descubiertas. Citrix Analytics descubre automáticamente las fuentes de datos a las que se ha suscrito a su cuenta de Citrix Cloud.

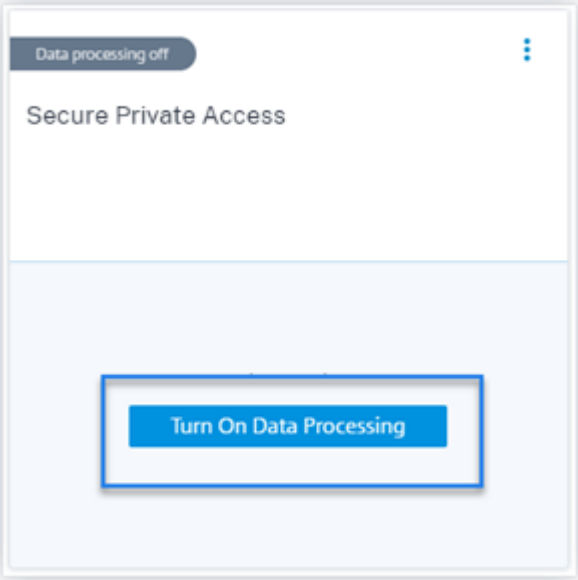


2. En la página **Orígenes de datos**, los orígenes de datos descubiertas aparecen como tarjetas de sitio. De forma predeterminada, el procesamiento de datos está desactivado.

> **Importante**
>
> Citrix Analytics procesa sus datos después de haber dado su consentimiento.



3. Haga clic **en Activar procesamiento de datos** en la tarjeta del sitio para la que quiere que Citrix Analytics procese los eventos. Por ejemplo, en la tarjeta del sitio Citrix Secure Private Access, haga clic **en Activar procesamiento de datos**.



4. Después de activar el procesamiento de datos, Citrix Analytics procesa los eventos del origen de datos. El estado de la tarjeta del sitio cambia a Procesamiento de datos. Puede ver el número de usuarios y los eventos recibidos en función del período de tiempo seleccionado.

5. Para todas los orígenes de datos detectadas, siga los pasos especificados en Introducción para habilitar el análisis.

Comprobación 5: ¿Las actividades de los usuarios en la fuente de datos transmiten eventos de forma precisa a Analytics?

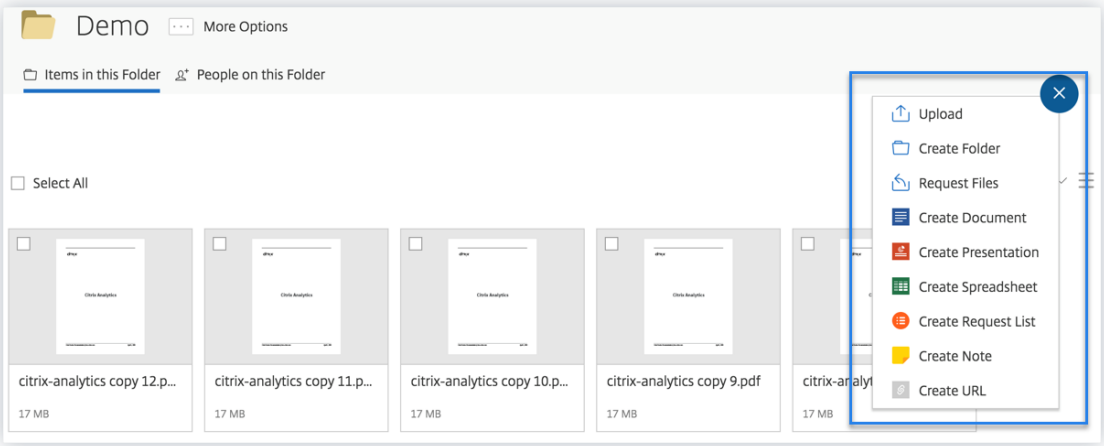
Citrix Analytics recibe eventos de usuario de los orígenes de datos cuando los usuarios utilizan activamente los orígenes de datos. Los usuarios deben realizar algunas actividades en la fuente de datos para generar eventos. Por ejemplo, para recibir eventos de la fuente de datos de Apps and Desktops, los usuarios de Apps and Desktops deben compartir, cargar o descargar algunos archivos.

> **Nota**
>
> Citrix Analytics no extrae datos de su entorno de forma activa.

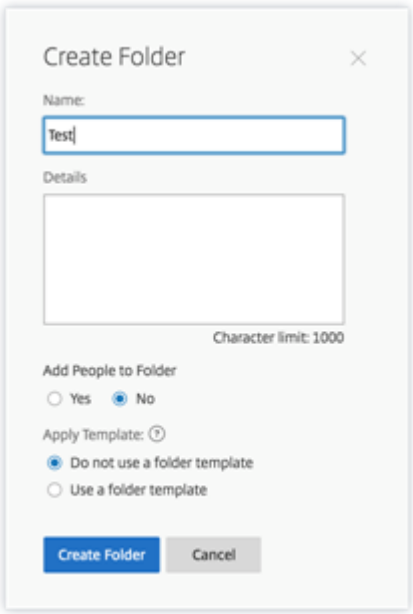
Si no ve ningún evento de usuario en Citrix Analytics para su fuente de datos, hay una alta probabilidad de que los usuarios no estén activos en ese momento.

Para comprobar que Citrix Analytics recibe correctamente los eventos del usuario, lleve a cabo la siguiente actividad. Esta actividad utiliza la fuente de datos de Citrix Apps and Desktops. Puede realizar una actividad similar con otros productos Citrix (orígenes de datos) en función de su suscripción.

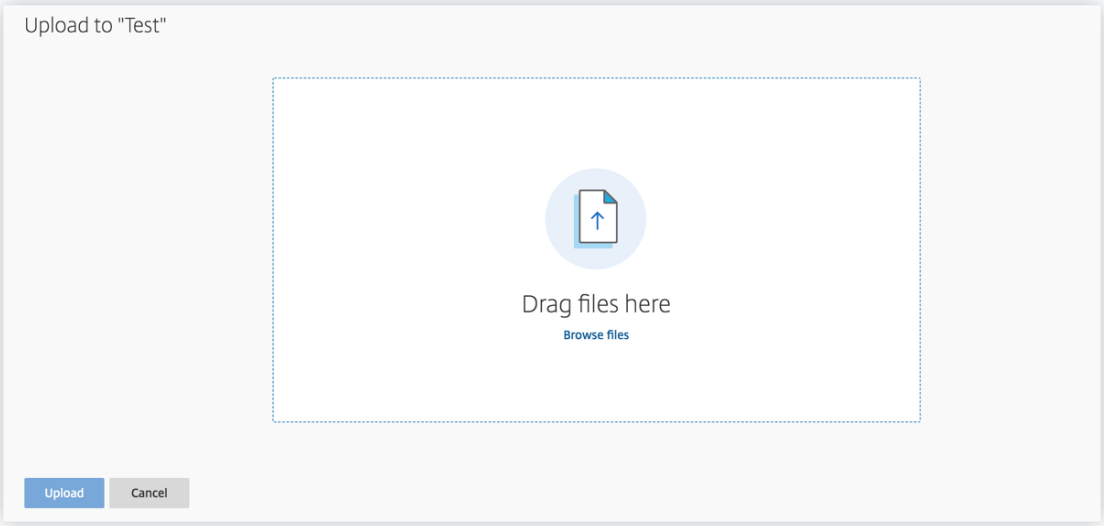
1. Inicie sesión en el servicio Citrix Apps and Desktops.
2. Realice algunas actividades habituales de usuario, como crear carpetas, descargar archivos, cargar archivos o eliminar archivos.



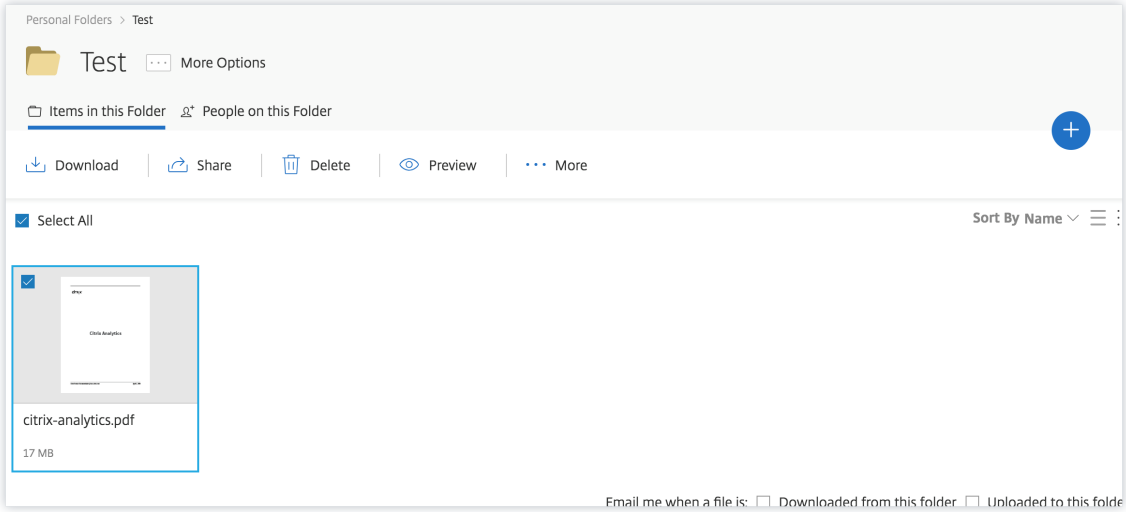
3. Por ejemplo, cree una carpeta de prueba.



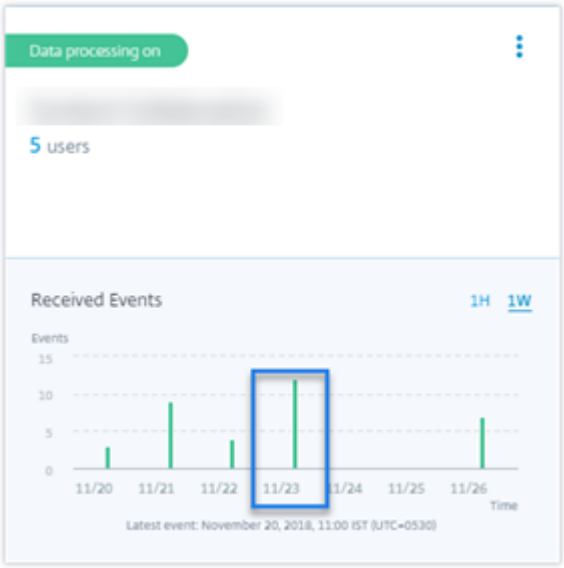
4. Sube algunos archivos locales.



5. Elimina algunos archivos de la carpeta.



6. Vuelva a Citrix Analytics y consulte la tarjeta lateral de **Apps and Desktops** en la página Fuente de datos. Citrix Analytics recibe los eventos de usuario de la fuente de datos de Apps and Desktops y los muestra en la tarjeta del sitio.



Comprobación 6: ¿se transmiten los eventos de escritorios y aplicaciones virtuales a Analytics?

Algunas versiones de la aplicación Citrix Workspace o del cliente Citrix Receiver no pueden enviar eventos de usuario a Citrix Analytics. Cuando los usuarios inician aplicaciones y escritorios virtuales a través de estos clientes, Citrix Analytics no detecta a los usuarios hasta que realizan los eventos compatibles.

Por ejemplo, la aplicación Citrix Workspace para Linux 2006 o posterior no envía los eventos de ***inicio de la aplicación SaaSy finalización de la aplicación SaaS*** a Citrix Analytics. Un usuario que lanza

una aplicación SaaS mediante la aplicación Citrix Workspace para Linux no se detecta en Citrix Analytics.

Eventos admitidos

Consulte la siguiente tabla para comprobar los eventos de usuario admitidos por cada versión de cliente.

- **Sí**. El cliente envía el evento a Citrix Analytics.
- **No**: el cliente no envía el evento a Citrix Analytics.
- **NA**- El evento no es aplicable al cliente.

Evento	Aplicación Workspace para Windows 1907 o posterior	Aplicación Workspace para Mac 1910.2 o una versión posterior	Aplicación Workspace para Linux 2006 o posterior	Aplicación Workspace para Android: la última versión disponible en Google Play	La última versión de la aplicación Workspace para iOS está disponible en Apple App Store	Aplicación Workspace para Chrome: la versión más reciente está disponible en Chrome Web Store	Aplicación Workspace para HTML5 2007 o posterior
Inicio de sesión de cuenta	Sí	Sí	Sí	Sí	Sí	No	No
Inicio de sesión	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Inicio de sesiones	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Fin de sesión	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Inicio de aplicación	Sí	Sí	Sí	No	Sí	Sí	Sí

Evento	Aplicación Workspace para Windows 1907 o posterior	Aplicación Workspace para Mac 1910.2 o una versión posterior	Aplicación Workspace para Linux 2006 o posterior	Aplicación Workspace para Android: la última versión disponible en Google Play	La última versión de la aplicación Workspace para iOS está disponible en Apple App Store	Aplicación Workspace para Chrome: la versión más reciente está disponible en Chrome Web Store	Aplicación Workspace para HTML5 2007 o posterior
Cierre de aplicación	Sí	Sí	Sí	No	Sí	Sí	Sí
Descarga de archivos	Sí	Sí	Sí	No	No	Sí	Sí
Impresión	No	Sí	Sí	No	No	Sí	Sí
Lanzamiento de aplicaciones SaaS	Sí	Sí	No	No	No	No	No
Fin de la aplicación SaaS	Sí	Sí	No	No	No	No	No
Navegación URL de aplicaciones SaaS	Sí	Sí	No	No	No	No	No
Acceso al portapapeles de aplicaciones SaaS	Sí	Sí	No	No	No	No	No

Evento	Aplicación Workspace para Windows 1907 o posterior	Aplicación Workspace para Mac 1910.2 o una versión posterior	Aplicación Workspace para Linux 2006 o posterior	Aplicación Workspace para Android: la última versión disponible en Google Play	La última versión de la aplicación Workspace para iOS está disponible en Apple App Store	Aplicación Workspace para Chrome: la versión más reciente está disponible en Chrome Web Store	Aplicación Workspace para HTML5 2007 o posterior
Descarga de archivos de aplicaciones SaaS	Sí	Sí	No	No	No	No	No
Impresión de archivos de aplicaciones SaaS	Sí	Sí	No	No	No	No	No

Según el estado de transmisión del evento, es posible que se produzcan los siguientes problemas:

- Cuando los usuarios se conectan a Citrix Virtual Apps and Desktops o Citrix DaaS con los clientes, es posible que no los descubran en Citrix Analytics hasta que realicen un evento (actividad) compatible. Por ejemplo, considere dos eventos de usuario: Inicio de aplicaciones e Inicio de aplicaciones SaaS. Un usuario que usa la aplicación Citrix Workspace para iOS, Citrix Analytics recibe el evento App Start pero no el evento SaaS App Launch. Por lo tanto, cuando el usuario inicia cualquier aplicación virtual, el evento Inicio de la aplicación se transmite a Citrix Analytics y se descubre al usuario. Sin embargo, si el usuario inicia una aplicación SaaS, Citrix Analytics no recibe el evento SaaS App Launch y no se descubre al usuario. Para obtener información sobre los usuarios detectados, consulte Usuarios descubiertos.
- Los eventos marcados como **No** en la tabla no aparecen en la página de búsqueda de autoservicio. Para obtener información sobre cómo utilizar la página de autoservicio, consulte Acerca

de la búsqueda de autoservicio.

Recomendación

Para obtener los máximos beneficios de Analytics, Citrix recomienda lo siguiente:

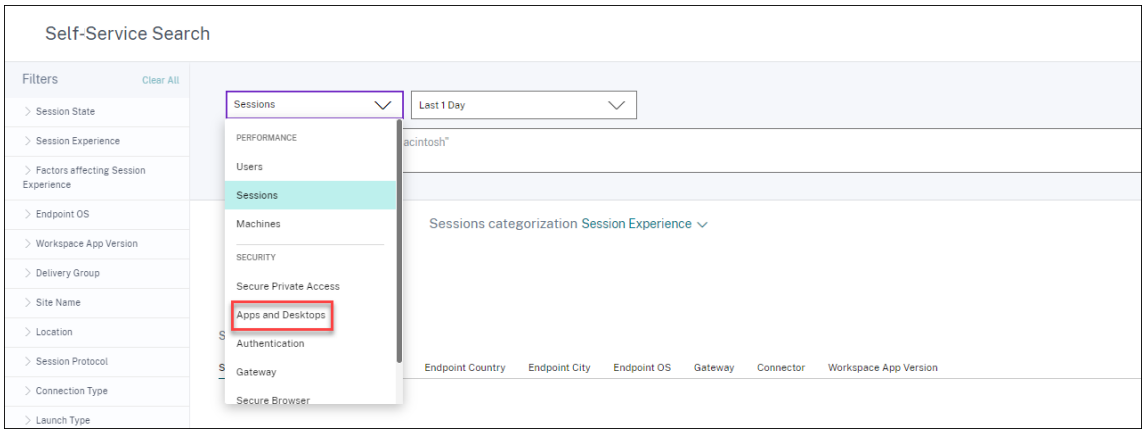
- **Usuario de Windows**: Conéctese a Citrix Virtual Apps and Desktops y Citrix DaaS con la aplicación Citrix Workspace para Windows 1907 o posterior.
- **Usuario de Mac**: Conéctese a su Citrix Virtual Apps and Desktops y Citrix DaaS mediante la aplicación Citrix Workspace para Mac 1910.2 o posterior.

Comprobación 7: ¿Los eventos de los usuarios aparecen en la página de búsqueda de autoservicio de Analytics?

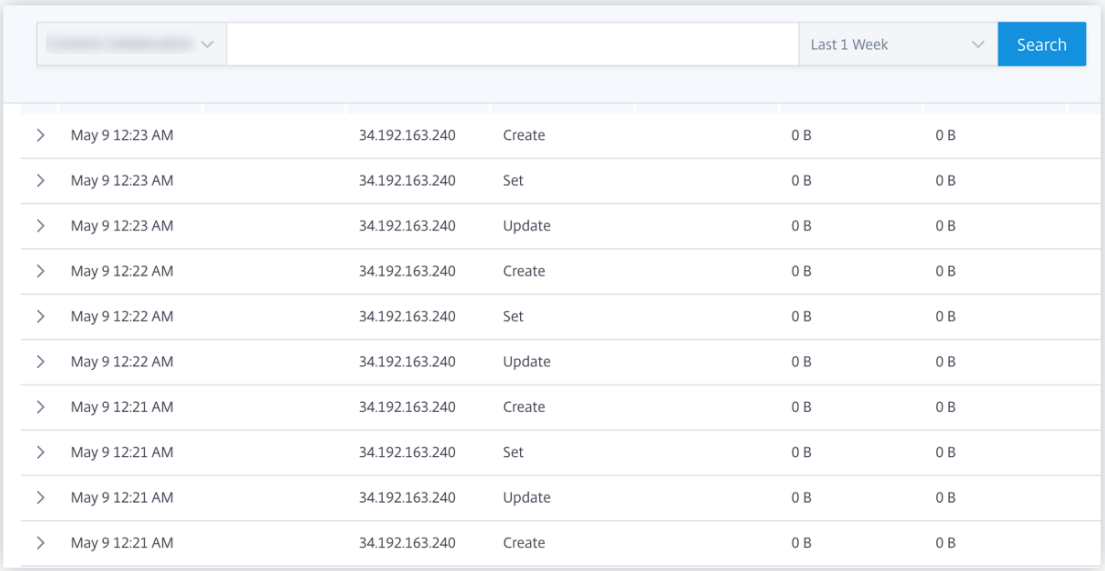
Realice esta comprobación final para asegurarse de que los eventos se transmiten con precisión a Citrix Analytics.

1. En la barra superior, haz clic en **Búsqueda avanzada** para ir a la página de búsqueda de autoservicio.

2. Seleccione la fuente de datos para ver la página de búsqueda correspondiente y los eventos.



3. Para ver los datos asociados a los eventos de Apps and Desktops, seleccione **Apps and Desktops** en la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.



Para obtener más información, consulte Búsqueda de autoservicio.

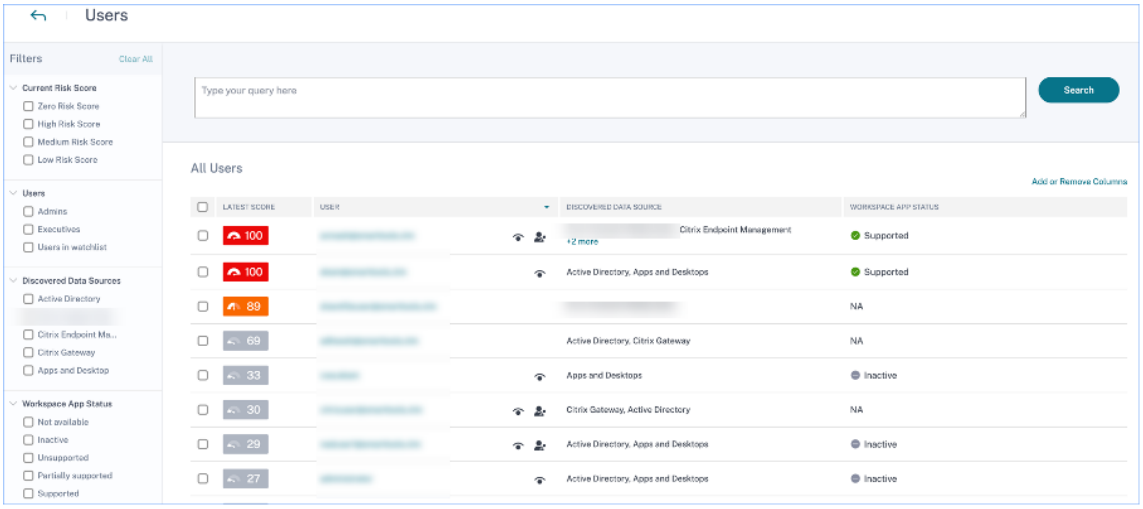
Comprobación 8: ¿Analytics descubre a los usuarios?

Cuando los eventos comienzan a fluir a Citrix Analytics, los usuarios que generan los eventos se detectan y se muestran en el panel **Usuarios**. Este proceso suele tardar unos minutos antes de que puedas verlos en el panel de control.

1. Haga clic en el enlace **Usuarios descubiertos** en el panel **Usuarios** para ver la lista completa de los usuarios detectados por Citrix Analytics.

2. La página **Usuarios** muestra la lista de todos los usuarios descubiertos en los últimos 31 días. Seleccione el período de tiempo para ver las ocurrencias del indicador de riesgo.

> **Nota:**
>
> Si intenta establecer un valor superior a 31 días, el sistema mostrará un mensaje de error que indica: **Intervalo de fechas no válido. El intervalo máximo permitido entre la fecha de inicio y la de finalización es de 31 días**.



Si los eventos se transmiten correctamente, el entorno de Citrix Analytics funciona según lo esperado. Los indicadores de riesgo se generan cuando se detectan anomalías.

Desencadenar eventos de Virtual Apps and Desktops y SaaS, y verificar la transmisión de eventos

April 12, 2024

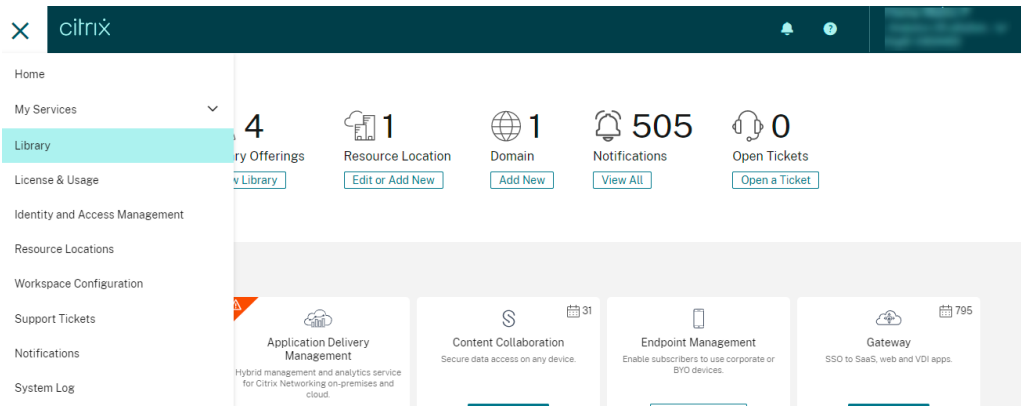
En esta sección se describen los procedimientos para activar eventos de aplicaciones y escritorios, eventos de SaaS, y para comprobar que Citrix Analytics for Security recibe estos eventos de usuario de forma activa.

Requisitos previos

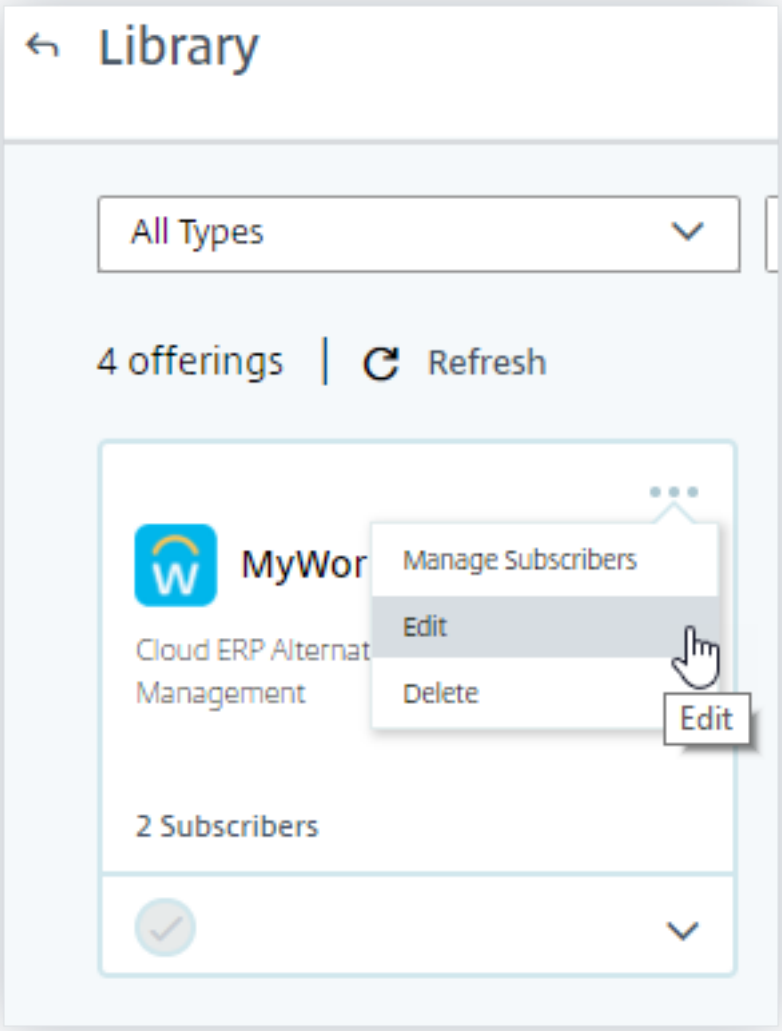
- Si usa local Citrix Virtual Apps and Desktops, incorpore sus sitios locales en Citrix Analytics y habilite el procesamiento de datos desde la tarjeta del sitio. Si utiliza Citrix DaaS (anteriormente el Citrix Virtual Apps and Desktops Service), habilite el procesamiento de datos directamente desde la tarjeta del sitio. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Use las versiones correctas de la aplicación Citrix Workspace o Citrix Receiver en los dispositivos de punto final de los usuarios para que los eventos se envíen con precisión a Citrix Analytics. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Antes de desencadenar el evento de impresión desde el escritorio virtual, asegúrese de que una impresora esté configurada y aprovisionada en su entorno de aplicaciones y escritorios. Para

obtener más información sobre la administración de una impresora, consulte Imprimir.

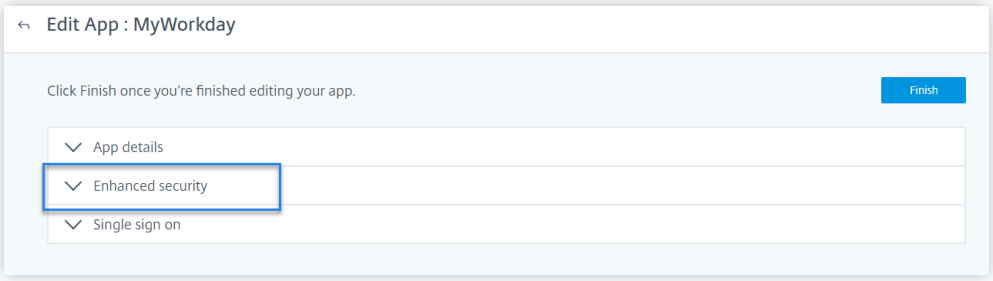
- Para activar los eventos SaaS, como el lanzamiento de aplicaciones SaaS, la navegación URL de aplicaciones SaaS, la descarga de archivos de aplicaciones SaaS, debe usar una aplicación SaaS configurada desde Workspace. Las aplicaciones SaaS más utilizadas incluyen Salesforce, Workday, Concur y GoTo Meeting.
  - Si no hay aplicaciones SaaS configuradas, debe configurar y publicar una aplicación SaaS. Para obtener más información, consulte Compatibilidad con aplicaciones de software como servicio. Al configurar una aplicación SaaS, asegúrese de que las siguientes opciones de seguridad estén inhabilitadas:
    - Restringir acceso al portapapeles
    - Restringir impresión
    - Restringir navegación
    - Limitar la descarga
  - Si quiere utilizar una aplicación SaaS ya configurada desde su Workspace para desencadenar los eventos, asegúrese de que las opciones de seguridad mejoradas especificadas estén inhabilitadas para la aplicación SaaS:
    1. Vaya a su cuenta de Citrix Cloud y seleccione **Biblioteca**.



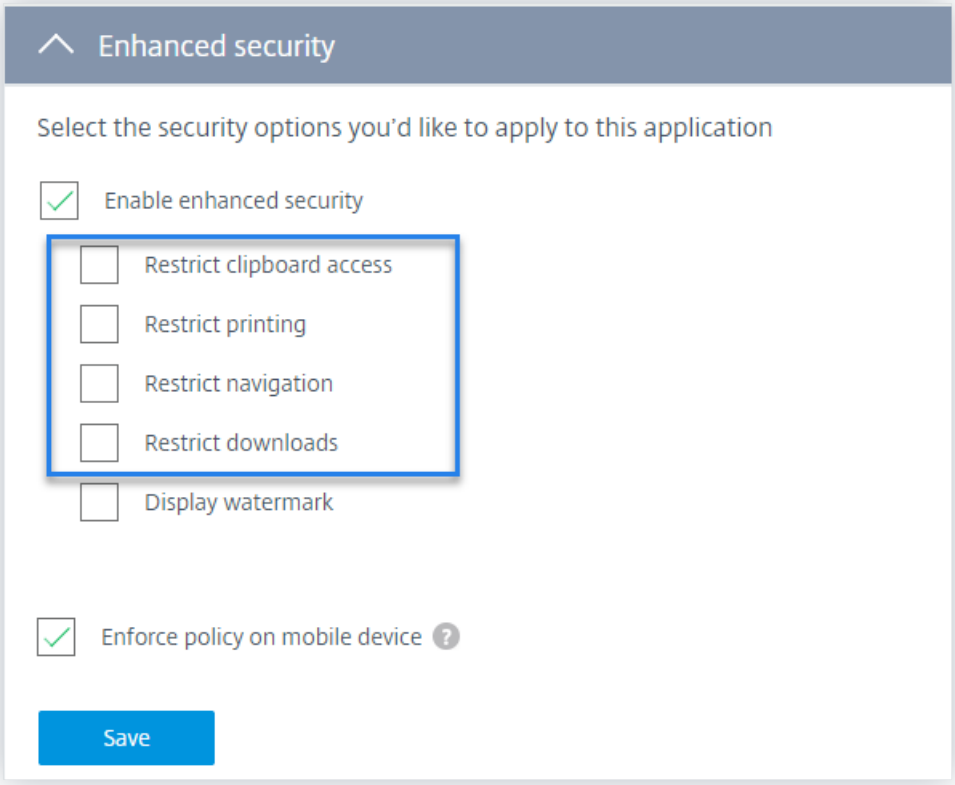
    2. En la página **Biblioteca**, identifique la aplicación SaaS que quiere usar para verificar los eventos. Por ejemplo, Workday.
    3. Haga clic en los puntos suspensivos y seleccione **Modificar**.



4. En la página **Modificar aplicación**, haga clic en la flecha hacia abajo para Seguridad mejorada.



5. Asegúrese de que las siguientes opciones de seguridad no estén seleccionadas.



Problema conocido

Algunas versiones de la aplicación Citrix Workspace y Citrix Receiver no pueden enviar algunos eventos a Citrix Analytics. Por lo tanto, Citrix Analytics no puede proporcionar información ni generar indicadores de riesgo para estos eventos. Para obtener más información sobre el problema y su solución alternativa, consulte el problema conocido: CAS-16151.

Procedimiento

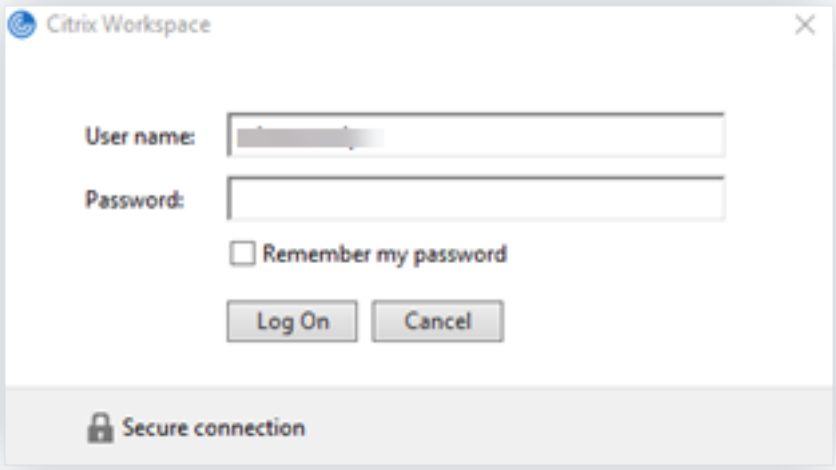
Realice los siguientes pasos en secuencia para desencadenar los eventos en su entorno de Apps and Desktops y comprobar que Citrix Analytics for Security recibe estos eventos de forma activa.

> **Nota**
>
> - Es posible que los eventos tarden algún tiempo en llegar a Citrix Analytics. Actualice la página de Citrix Analytics si no ve los eventos desencadenados.
> - Para desencadenar los eventos SaaS, este procedimiento utiliza la aplicación Workday como ejemplo. Puede usar cualquier aplicación SaaS configurada desde su Workspace

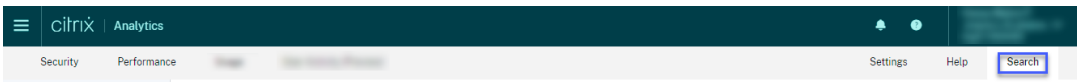
> para desencadenar los eventos SaaS.

- **Inicio de sesión de cuenta**

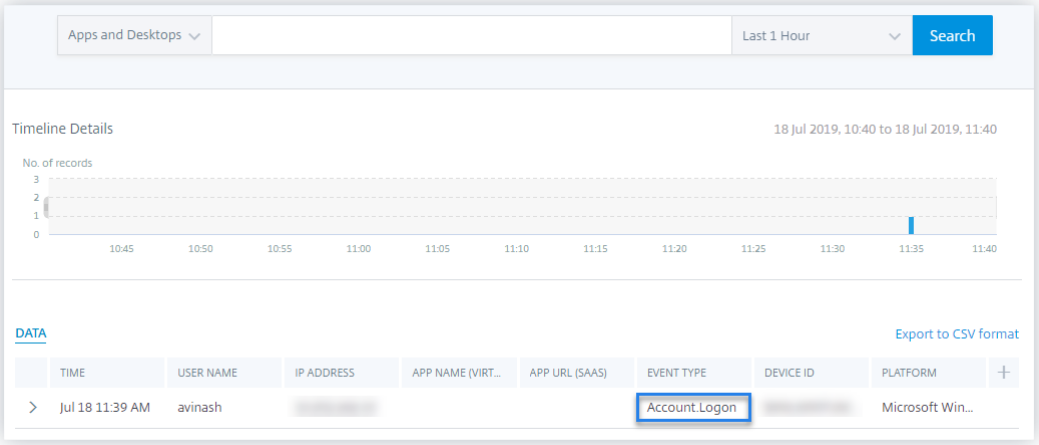
  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
  2. Introduzca sus credenciales para iniciar sesión en la aplicación Citrix Workspace o en Citrix Receiver.



  3. Vaya a Citrix Analytics.
  4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios** en la lista.

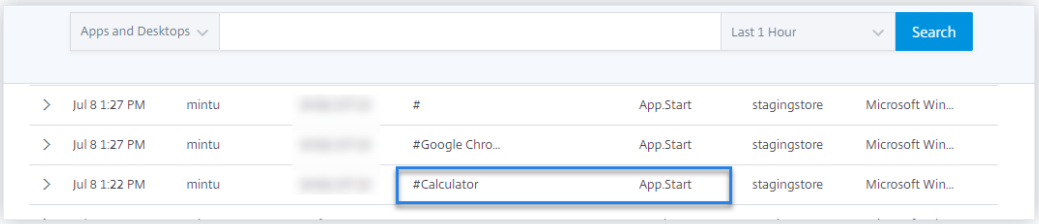


  5. En la página de búsqueda, consulte los datos del evento **Account.Logon**. Expanda la fila para ver los detalles del evento.



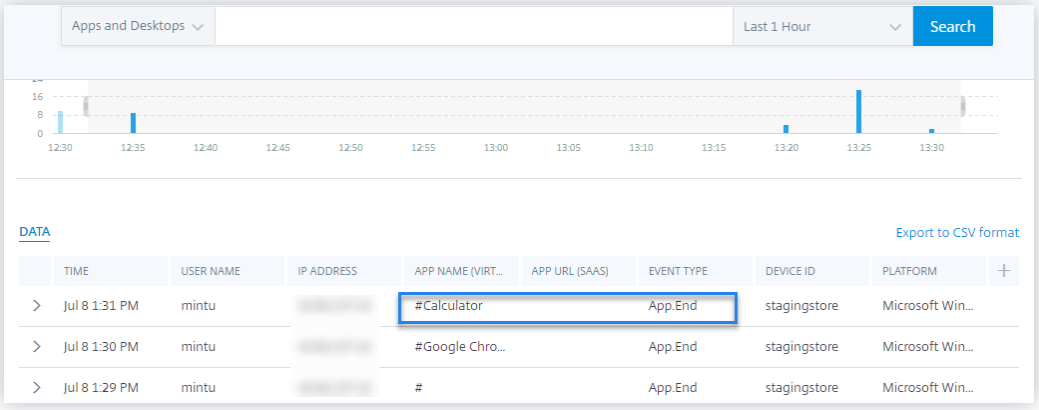
- **Inicio de aplicación**

  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
  2. Inicie una aplicación como la calculadora.
  3. Vaya a Citrix Analytics.
  4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
  5. En la página de búsqueda, consulte los datos de los datos del evento **App.Start**. Expanda la fila para ver los detalles del evento.



- **Cierre de aplicación**

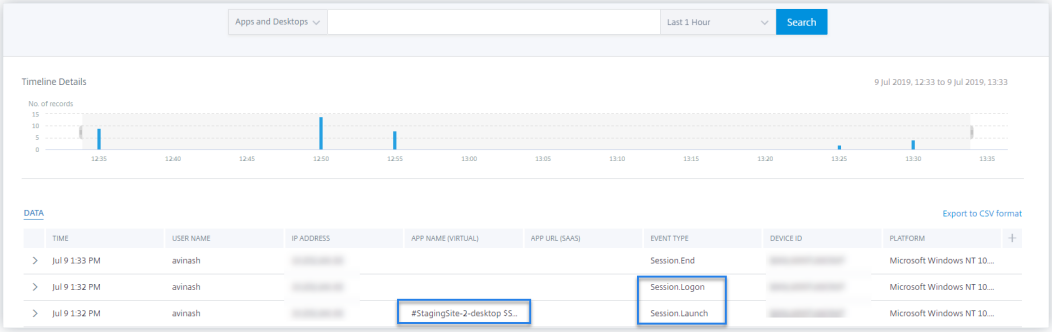
  1. Cierre la calculadora que ya ha lanzado en su Workspace o StoreFront.
  2. Vaya a Citrix Analytics.
  3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
  4. En la página de búsqueda, consulte los datos de los datos del evento **App.End**. Expanda la fila para ver los detalles del evento.



- **Inicio de sesión e inicio de sesión**

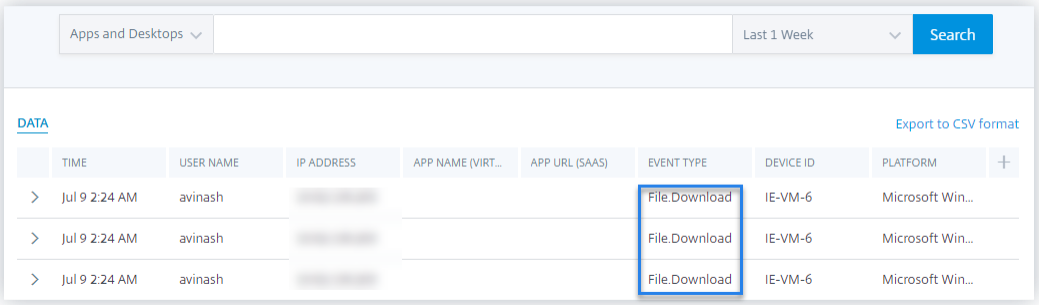
  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.

2. Inicie su escritorio virtual.
3. Vaya a Citrix Analytics.
4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
5. En la página de búsqueda, consulte los datos de los eventos **Session.Logon** y **Session.Launch**. Expanda la fila para ver los detalles del evento.



- **Descarga de archivos**

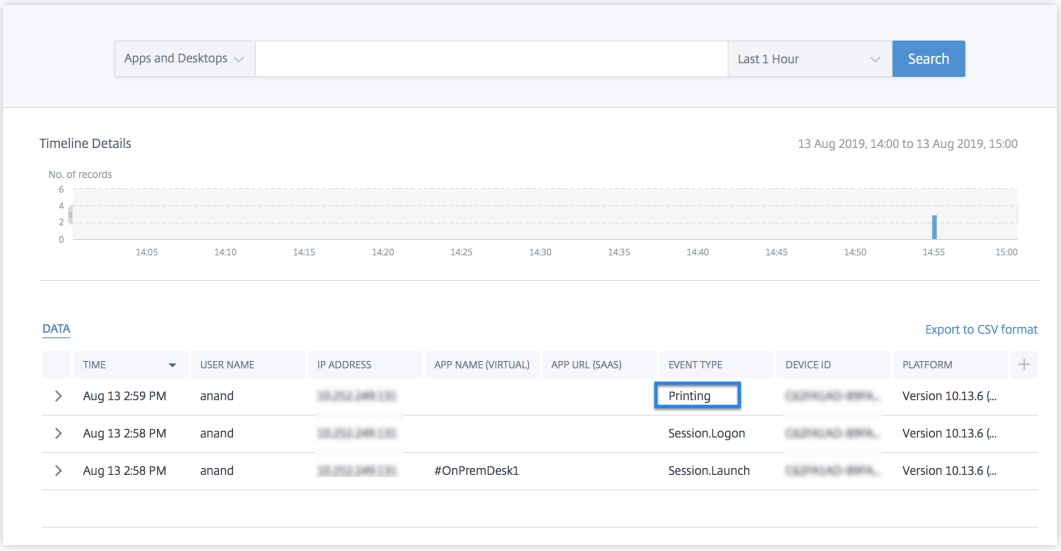
1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
2. Inicie su escritorio virtual.
3. Copie un archivo del escritorio virtual en el equipo local.
4. Vaya a Citrix Analytics.
5. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
6. En la página de búsqueda, consulte los datos del evento **File.Download**. Expanda la fila para ver los detalles del evento.



- **Impresión**

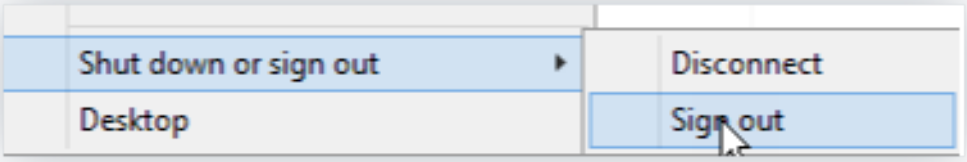
1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace.
2. Inicie su escritorio virtual.

3. Imprima un documento con una impresora que esté configurada con su escritorio virtual.
4. Vaya a Citrix Analytics.
5. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
6. En la página Buscar, consulte los datos del evento **Printing**. Expanda la fila para ver los detalles del evento.

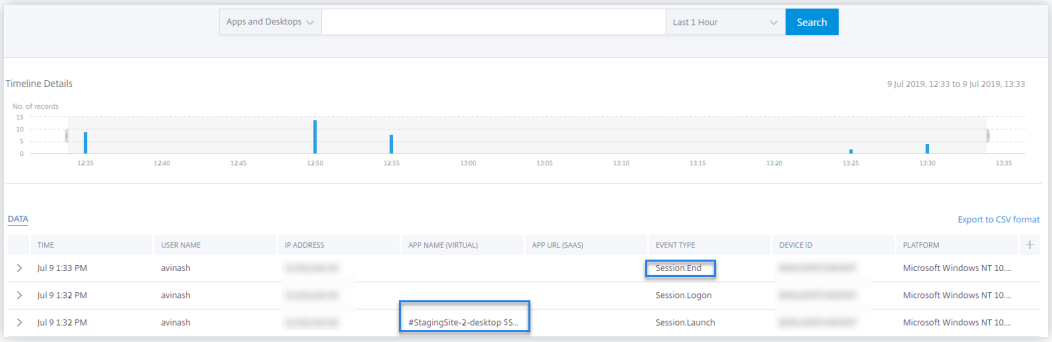


- **Fin de sesión**

1. Cierre sesión en su escritorio virtual. Por ejemplo, si usa un escritorio virtual de Windows, seleccione la opción **Cerrar sesión**.



2. Vaya a Citrix Analytics.
3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
4. En la página de búsqueda, consulte los datos del evento **Session.End**. Expanda la fila para ver los detalles del evento.

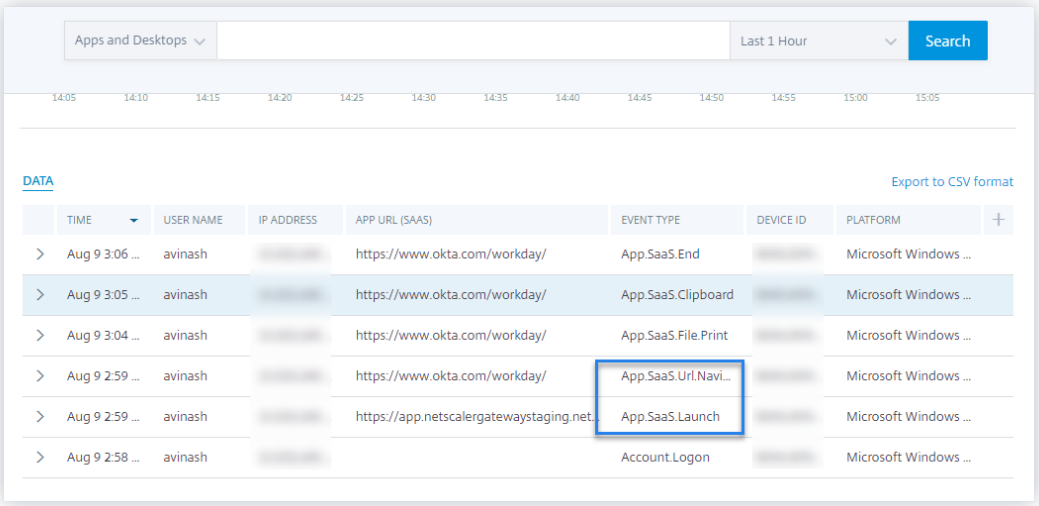


- **Lanzamiento de aplicaciones SaaS y navegación URL de aplicaciones SaaS**

  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
  2. Inicie una aplicación SaaS como Workday y espere hasta que se cargue la página de Workday. Navegue por las páginas web de Workday.

     > **Nota**
     >
     > Asegúrese de que la opción **Restringir navegación** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte **Requisitos previos**.

  3. Vaya a Citrix Analytics.
  4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
  5. En la página de **búsqueda**, consulte los datos de los eventos **App.SaaS.Launch** y **App.SaaS.URL.Navigation**. Expanda la fila para ver los detalles del evento.

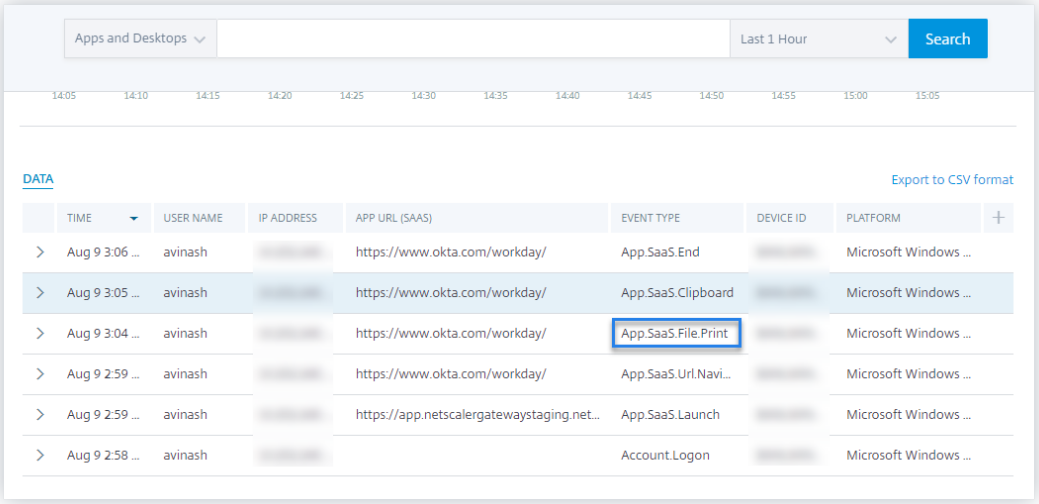


- **Impresión de archivos de aplicaciones SaaS**

  1. Imprima la página de Workday que está viendo actualmente.

> **Nota**
>
> Asegúrese de que la opción **Restringir impresión** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte los **requisitos previos**.

2. Vaya a Citrix Analytics.
3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
4. En la página de búsqueda, consulte los datos del evento **App.SaaS.File.Print**. Expanda la fila para ver los detalles del evento.

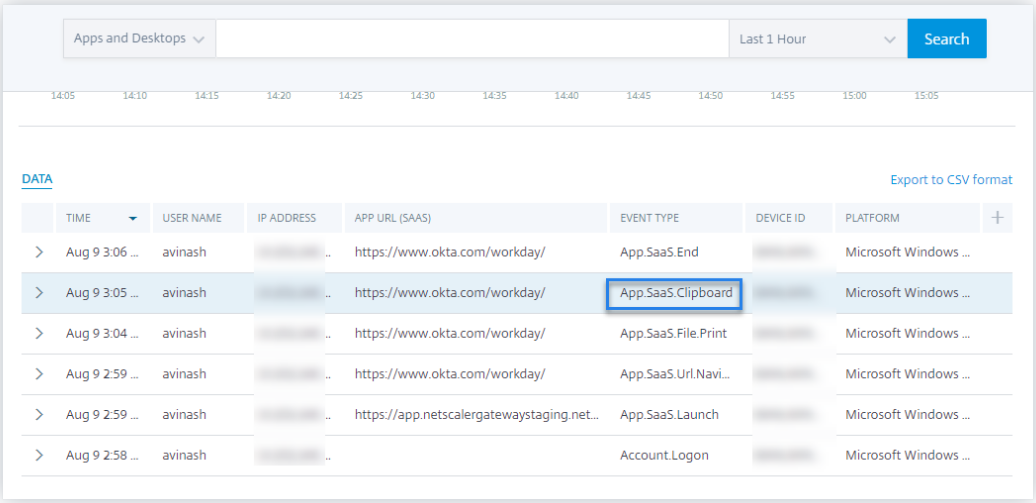


- **Acceso al portapapeles de aplicaciones SaaS**

1. En la página de Workday, copie texto en el portapapeles del sistema.

> **Nota**
>
> Asegúrese de que la opción **Restringir acceso al portapapeles** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte los **requisitos previos**.

2. Vaya a Citrix Analytics.
3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
4. En la página de búsqueda, consulte los datos del evento **App.SaaS.Clipboard**. Expanda la fila para ver los detalles del evento.

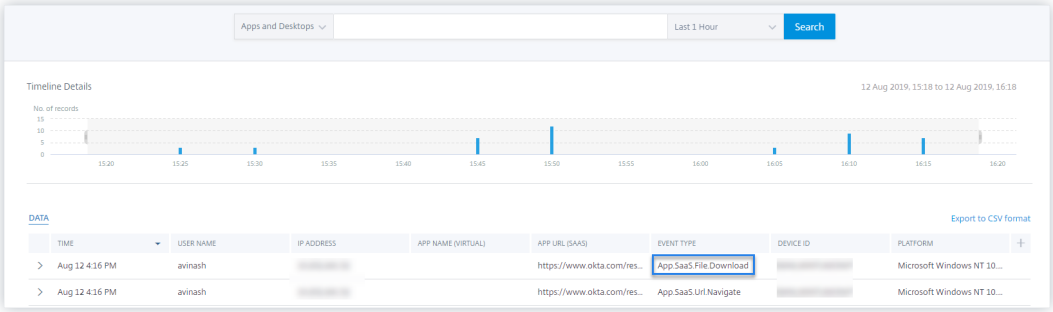


- **Descarga de archivos de aplicaciones SaaS**

  1. En la página Workday, busque un documento público, como un documento técnico, y descargue el documento.

     > **Nota**
     >
     > Asegúrese de que la opción **Restringir descargas** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte los **requisitos previos**.

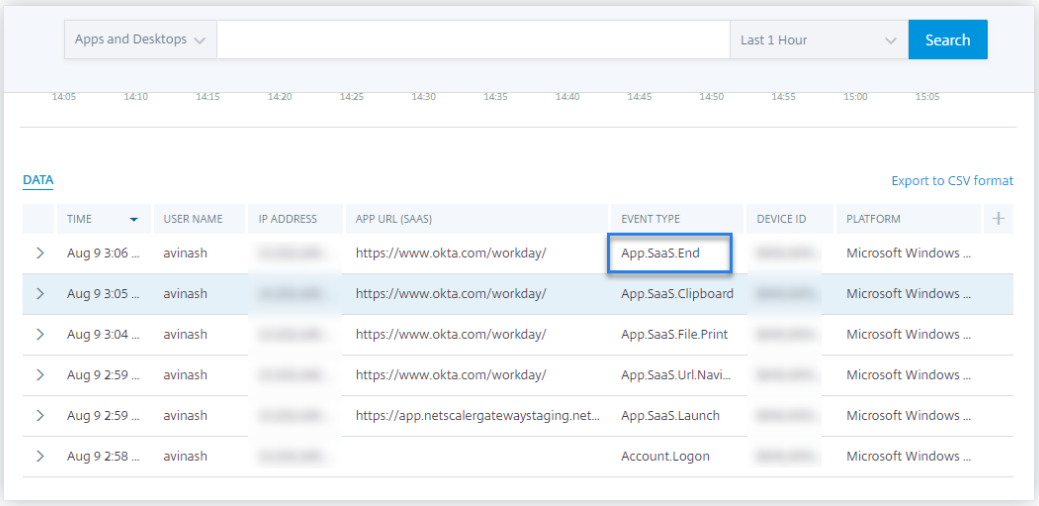
  2. Vaya a Citrix Analytics.
  3. Haga clic en Buscar y seleccione **Aplicaciones y escritorios**.
  4. En la página Buscar, consulte los datos del evento **App.SaaS.file.download**. Expanda la fila para ver los detalles del evento.



- **Fin de la aplicación SaaS**

  1. Cierre la página de Workday.
  2. Vaya a Citrix Analytics.
  3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.

4. En la página de búsqueda, consulte los datos del evento **App.SaaS.End**. Expanda la fila para ver los detalles del evento.



- **VDA.Print**

  Requisitos previos

  Antes de desencadenar el evento de impresión, consulte Habilitar la telemetría de impresión para Citrix DaaS.

  Para activar un evento de impresión, realice las siguientes acciones:

  1. Abra un documento de texto con un bloc de notas o cualquier otra aplicación en la que se permita imprimir.
  2. Haga clic en **Archivo > Imprimir** o presione **Ctrl + P**.
  3. En Seleccionar impresora, elija su impresora, haga clic en **Aplicar** y, a continuación, imprima.

- **VDA.Clipboard**

  Requisitos previos

  Antes de activar el evento de impresión, consulte Habilitar la telemetría del portapapeles para Citrix DaaS.

  Para activar un evento de portapapeles, realice las siguientes acciones:

  1. Abra un documento de texto con un bloc de notas o cualquier editor de texto.
  2. Seleccione el contenido que quiere copiar.
  3. Haga clic con el botón secundario en copiar o presione Ctrl+C.

El servidor de grabación de sesiones configurado no se conecta

July 12, 2022

El servidor de grabación de sesiones no se conecta a Citrix Analytics después de la configuración. Por lo tanto, no ve el Servidor configurado en la tarjeta del sitio **Session Recording**.

Para solucionar este problema, haga lo siguiente:

1. En el servidor de Grabación de sesiones configurado, ejecute el siguiente comando de PowerShell para comprobar la identificación del equipo cliente (CMID).

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```

2. Si el CMID está vacío, agregue los siguientes archivos de registro en las rutas especificadas.

Nombre en el Registro	Ruta del Registro	Tipo de clave	Valor
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	Cadena	Introduzca su UUID.
EnableCASUseAuditorUniqueID	Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. Reinicie estos servicios:
   - Servicio Citrix Session Recording Analytics
   - Administrador de almacenamiento de grabación de sesiones de Citrix

Problemas de configuración con el complemento Citrix Analytics para Splunk

July 12, 2022

La configuración del complemento Citrix Analytics no está

Después de instalar Citrix Analytics Add-on for Splunk en su entorno de Splunk Forwarder o Splunk Standalone, no verá la configuración del **complemento de Citrix Analytics** en **Configuración > Entradas de datos**.

Motivo

Este problema se produce cuando se instala el complemento Citrix Analytics para Splunk en un entorno de Splunk no compatible.

Correcciones

Instale el complemento Citrix Analytics para Splunk en un entorno de Splunk compatible. Para obtener información sobre las versiones compatibles, consulte Integración de Splunk.

No hay datos disponibles en los paneles de Splunk

Después de instalar y configurar Citrix Analytics Add-on for Splunk en su entorno de Splunk Forwarder o Splunk Standalone, no verá ningún dato de Citrix Analytics en los paneles de Splunk.

Cheques

Para solucionar el problema, verifique lo siguiente en su entorno de Splunk Forwarder o Splunk Standalone:

1. Asegúrese de que se cumplan los requisitos previos para la integración de Splunk.
2. Vaya a **Configuración > Entradas de datos > Complemento de Citrix Analytics**. Asegúrese de que los detalles de configuración de Citrix Analytics estén disponibles.
3. Si los detalles de configuración están disponibles, ejecute la siguiente consulta para comprobar los registros en busca de errores relacionados con el complemento Citrix Analytics para Splunk:


```
index=_internal sourcetype=splunkd log_level=ERROR component=
    ExecProcessor cas_siem_consumer
```

4. Si no encuentra ningún error, el complemento Citrix Analytics para Splunk funciona como se esperaba. Si encuentra algún error en los registros, puede deberse a una de las siguientes razones:

   - No se pudo establecer la conexión entre el entorno de Splunk y los puntos finales de Citrix Analytics Kafka. Este problema puede deberse a la configuración del firewall.

     Correcciones: consulte con el administrador de red para resolver este problema.

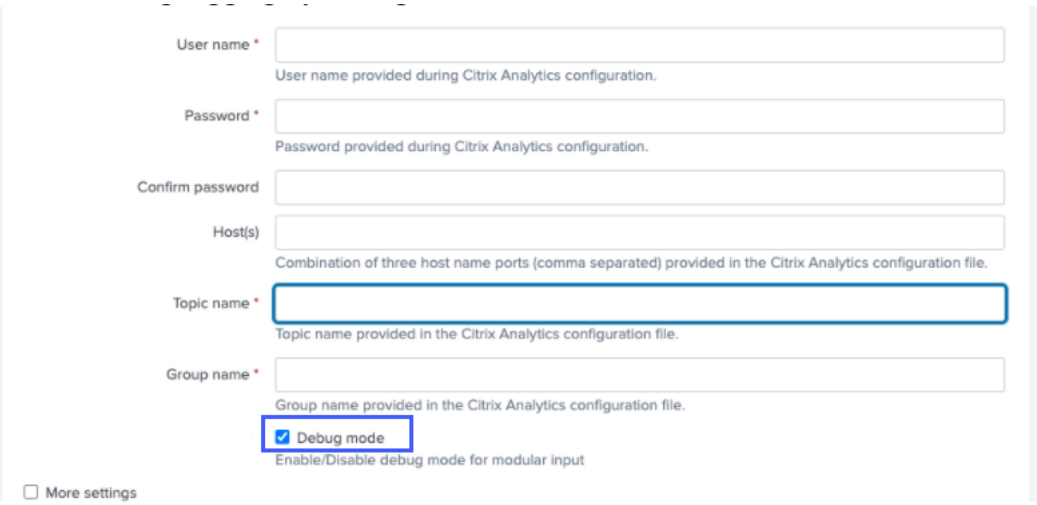
   - Detalles de configuración incorrectos en **Configuración > Entradas de datos > Complemento de Citrix Analytics**.

     Correcciones: Asegúrese de que los detalles de configuración de Citrix Analytics, como el nombre de usuario, la contraseña, los puntos finales del host, el tema y el grupo de consumidores, se escriben correctamente según el archivo de configuración de Citrix Analytics. Para obtener más información, consulte Configurar el complemento Citrix Analytics para Splunk.

5. Si no puede encontrar la causa del problema en los registros anteriores y quiere investigar más a fondo:

   a) Habilite el **modo de depuración** en **Configuración > Entradas de datos > Complemento de Citrix Analytics**.

   > Nota
   >
   > De forma predeterminada, el **modo de depuración** está inhabilitado. Al habilitar este modo, se generan demasiados registros. Por lo tanto, use esta opción solo cuando sea necesario y desactívela después de completar la tarea de depuración.



b) Busque los registros de depuración generados en la siguiente ubicación y compruebe si hay algún error:

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

c) (Opcional) Use el script de depuración `splunk cmd python cas_siem_consumer_debug.py` que está disponible con el complemento Citrix Analytics para Splunk. Este script genera un archivo de registro que contiene los detalles de su entorno de Splunk y las comprobaciones de conectividad. Puede usar los detalles para depurar el problema. Ejecute el script con el siguiente comando:

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

Mensaje de error

En los registros relacionados con el complemento Citrix Analytics para Splunk, es posible que consulte el siguiente error:

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

Este error se debe a un problema de conectividad de red o a un problema de autenticación.

Para depurar el problema:

1. En su entorno Splunk Forwarder o Splunk Standalone, habilite el **modo de depuración** para obtener los registros de depuración. Consulte el paso anterior 5.a.
2. Ejecute la siguiente consulta para encontrar cualquier problema de autenticación en los registros de depuración:

   ```
   index=_internal source="*
      splunk_citrix_analytics_add_on_debug_connection.log*" "
      Authentication failure"
   ```

3. Si no encuentra ningún problema de autenticación en los registros de depuración, el error se debe a un problema de conectividad de red.
4. Busque y resuelva el problema mediante telnet o el script de depuración mencionado en el paso anterior 5.c.

La actualización del complemento falla desde una versión anterior a la 2.0.0

En su entorno de Splunk Forwarder o Splunk Standalone, cuando actualiza el complemento Citrix Analytics para Splunk a la última versión desde una versión anterior a la 2.0.0, la actualización falla.

Correcciones

1. Elimine los siguientes archivos y carpetas ubicados en la carpeta de instalación `/bin` del complemento Citrix Analytics para Splunk:
   - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`
   - `rm -rf splunklib`
   - `rm -rf mac`
   - `rm -rf linux_x64`
   - `rm CARoot.pem`
   - `rm certificate.pem`
2. Reinicie su entorno Splunk Forwarder o Splunk Standalone.

No se puede conectar el servidor StoreFront con Citrix Analytics

January 4, 2023

Después de importar los valores de configuración de Citrix Analytics a su servidor StoreFront, el servidor StoreFront no se conecta a Citrix Analytics.

Para obtener información sobre cómo importar los valores de configuración a un servidor StoreFront, consulte Incorporar sitios de Virtual Apps and Desktops mediante StoreFront.

El Asistente de incorporación de CAS ayuda a comprobar y solucionar los problemas descritos en este artículo. Para obtener más información, consulte Asistente de incorporación de Citrix Analytics Service (CAS).

Para solucionar el problema, haga lo siguiente:

1. En el servidor StoreFront, haga ping a los puntos finales específicos de la región de Citrix Analytics para probar la conectividad entre el servidor StoreFront y el servidor Citrix Analytics. Además, asegúrese de que se cumplan los requisitos previos.

   > **Nota**
   >
   > En su servidor StoreFront, puede probar la conectividad haciendo ping directamente a los puntos finales específicos de la región o abriendo un explorador web y accediendo a los puntos finales específicos de la región.

2. Habilite el registro detallado en el servidor StoreFront para rastrear los registros. Para obtener más información sobre el registro detallado, consulte el artículo CTX139592.

3. Abra el Administrador de Internet Information Services (IIS) y compruebe lo siguiente:
    - Si el sitio de StoreFront se encuentra en el sitio predeterminado de IIS, IIS reinicia el sitio de StoreFront.
    - Si el sitio de StoreFront está en otros controladores o no está en el sitio predeterminado, abra la ventana de comandos y escriba `iisreset`.
4. Ejecute el siguiente comando para importar la configuración de Citrix Analytics:

    ```
    Import-STFCasConfiguration -Path "configuration file path"
    ```

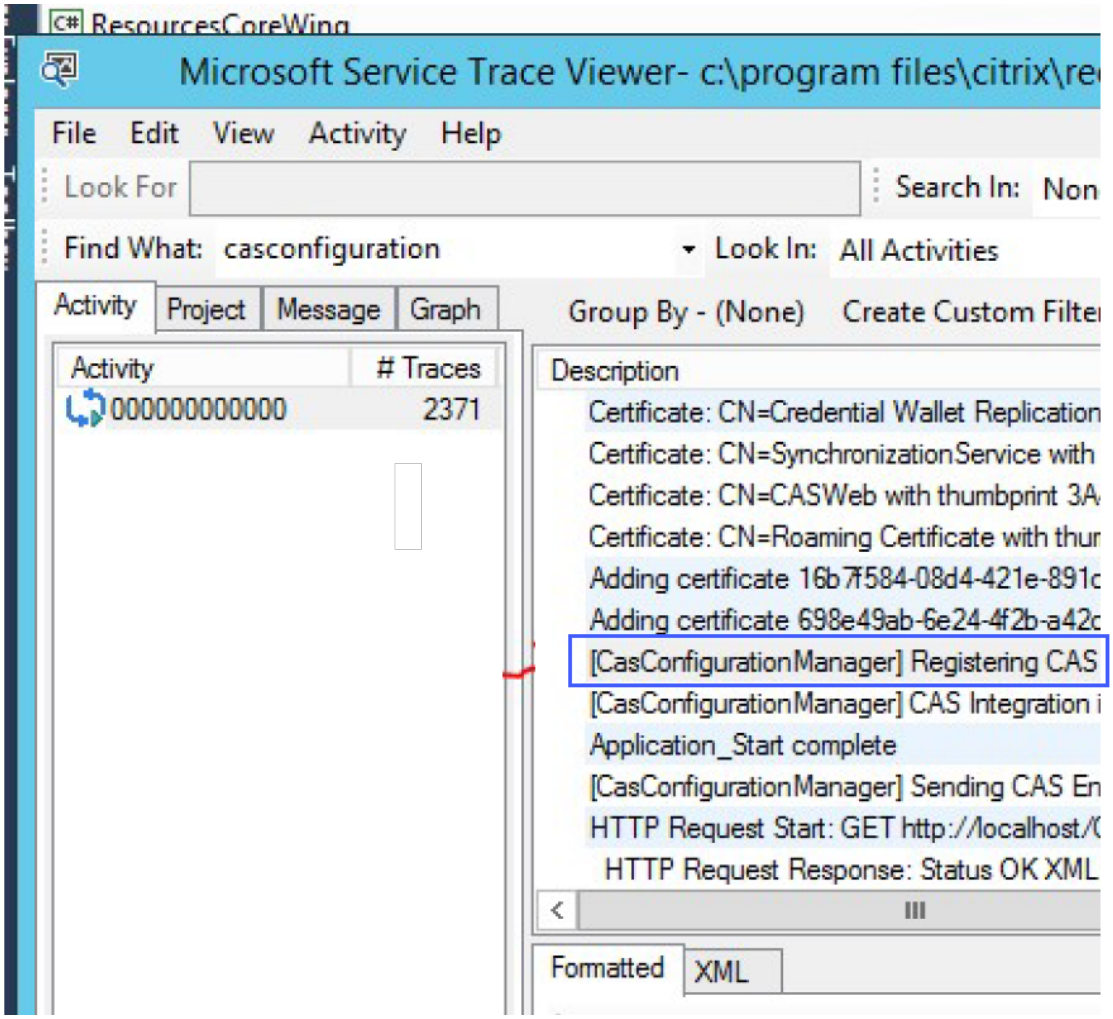
5. Ejecute el siguiente comando para verificar la configuración importada:

    ```
    Get-STFCasConfiguration
    ```

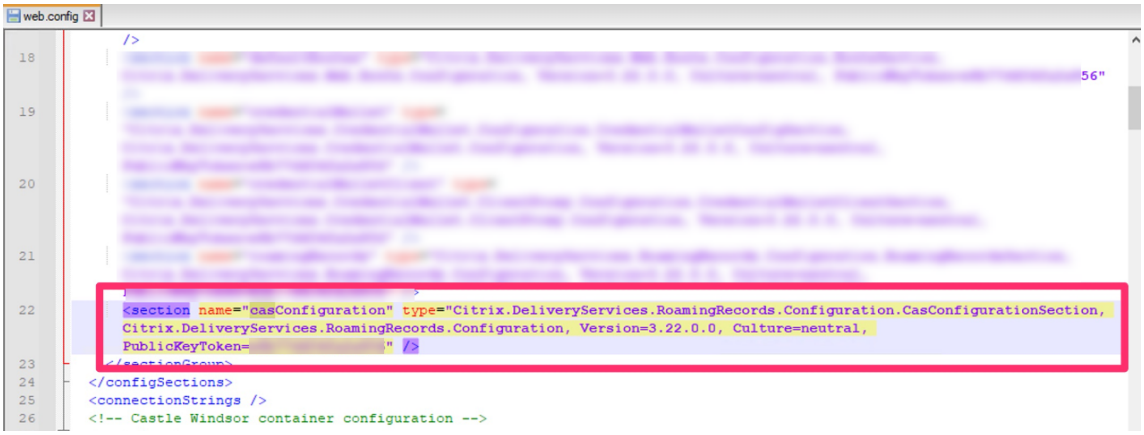
6. Si el sitio de StoreFront se encuentra en otros controladores o no está en el sitio predeterminado, abra la ventana de comandos. Escriba `iisreset` para permitir que el sitio de StoreFront lea la configuración de Citrix Analytics.
7. Obtenga los archivos de registro detallados de StoreFront en la siguiente ubicación:

    ```
    C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
    ```

    En la ubicación mencionada anteriormente, puede encontrar varios archivos svclog que se pueden abrir en Event Viewer.
8. Use Microsoft Service Trace Viewer para abrir los siguientes registros:
    - Registros de StoreFront
    - Registros detallados de sitios móviles
9. En los registros, asegúrese de que las secciones **CasConfigurationManager** y la información del servidor Citrix Analytics estén disponibles.



10. Si las secciones CasConfigurationManager no están disponibles, abra el archivo web.config para el sitio móvil que se encuentra en `roaming site\folder`.
11. En el archivo `web.config`, busque la sección **casConfiguration** y asegúrese de que la información del servidor Citrix Analytics esté disponible.



12. En las máquinas Windows Server en las que esté instalado el servidor StoreFront, asegúrese de

lo siguiente:

- El cliente de TLS 1.2 está habilitado.
- Al menos uno de los siguientes conjuntos de cifrado está habilitado:
  - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
  - `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`

Para obtener información sobre cómo configurar el orden del conjunto de cifrado TLS, consulte la documentación de Microsoft.

13. Si utiliza máquinas con Windows Server 2012, asegúrese de que Diffie-Hellman Exchange (ECDHE/DHE) esté habilitado.
14. Asegúrese de que las máquinas Windows Server en las que está instalado el servidor StoreFront deben contener la configuración del registro mencionada en la documentación de Microsoft.

> **IMPORTANTE**
>
> Actualice los conjuntos de cifrado TLS/SSL mediante la directiva de grupo. No modifique manualmente los conjuntos de cifrado TLS/SSL. Para obtener más información sobre cómo usar la directiva de grupo, consulte la documentación de Microsoft.

Por ejemplo, la siguiente configuración del registro debe estar disponible en su equipo con Windows Server:

Cliente TLS 1.2:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000

<!--NeedCopy-->
```

KEA de Diffie-Hellman:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
   ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff
```



```
5
6 <!--NeedCopy-->
```

Cifrados AES-128/AES-256:

```
1 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
     SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
2 "Enabled"=dword:ffffffff
3 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
     SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
4 "Enabled"=dword:ffffffff
5
6 <!--NeedCopy-->
```

Funciones hash SHA256/SHA384:

```
1 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
     SecurityProviders\SCHANNEL\Hashes\SHA256]
2 "Enabled"=dword:ffffffff
3 [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
     SecurityProviders\SCHANNEL\Hashes\SHA384]
4 "Enabled"=dword:ffffffff
5
6 <!--NeedCopy-->
```

Preguntas frecuentes

November 17, 2023

Origen de datos

¿Qué es un origen de datos?

Los orígenes de datos son productos y servicios de Citrix que envían datos a Citrix Analytics.

Más información: Orígenes de datos

¿Cómo agrego un origen de datos?

Después de iniciar sesión en Citrix Analytics, en la pantalla de **bienvenida**, seleccione **Comenzar** para agregar un origen de datos a Citrix Analytics. Como alternativa, también puede agregar un origen de datos desde **Parámetros > Orígenes de datos**.

Agente de Citrix ADM

¿Cuáles son los requisitos mínimos de recursos para instalar un agente en un hipervisor local?

8 GB de RAM, 4 CPU virtuales, 120 GB de almacenamiento, 1 interfaz de red virtual, 1 Gbps de rendimiento

¿Tengo que asignar un disco adicional al agente de Citrix ADM durante el aprovisionamiento?

No, no es necesario agregar un disco adicional. El agente solo se usa como intermediario entre Citrix Analytics y las instancias del centro de datos de su empresa. No almacena datos de inventario o análisis que requieran un disco adicional.

¿Cuáles son las credenciales predeterminadas para iniciar sesión en un agente?

Las credenciales predeterminadas para iniciar sesión en el agente son `nsrecover`/`nsroot`. Esto iniciará sesión en el intérprete de comandos del agente.

¿Cómo cambio la configuración de red de un agente si he introducido un valor incorrecto?

Inicie sesión en la consola del agente del hipervisor y acceda a la línea de comandos del shell con las credenciales `nsrecover`/`nsroot` y, a continuación, ejecute el comando `networkconfig`.

¿Por qué necesito una URL de servicio y un código de activación?

El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrar el agente en el servicio.

¿Cómo puedo volver a introducir la URL del servicio si la he escrito incorrectamente en la consola del agente?

Inicie sesión en el intérprete de comandos del agente con las credenciales `nsrecover`/`nsroot` y, a continuación, escriba: `deployment_type.py`. Este script le permite volver a introducir la URL del servicio y el código de activación.

¿Cómo puedo obtener un nuevo código de activación?

Puede obtener un nuevo código de activación del servicio Citrix ADM. Inicie sesión en el servicio Citrix ADM y vaya a **Redes > Agentes**. En la página **Agentes**, en la lista **Seleccionar acción**, seleccione **Generar código de activación**.

¿Puedo reutilizar mi código de activación con varios agentes?

No, no puede.

¿Cuántos agentes de Citrix ADM 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 instalo varios agentes de Citrix ADM?

En la página Fuentes de datos, haga clic en el signo más (+) situado junto a Citrix Gateway y siga las instrucciones para instalar otro agente.

Como alternativa, puede acceder a la GUI de Citrix ADM y navegar a Redes > Agentes y hacer clic en **Configurar agente** para instalar varios agentes.

¿Puedo instalar dos agentes en una configuración de alta disponibilidad?

No, no puede.

¿Qué hago si falla el registro de mi agente?

- Asegúrese de que su agente tenga acceso a Internet (configure DNS).
- Asegúrese de haber copiado el código de activación correctamente.
- Asegúrese de haber introducido correctamente la URL del servicio.
- Asegúrese de tener abiertos los puertos necesarios.

El registro se ha realizado correctamente, pero ¿cómo puedo saber si el agente funciona correctamente?

Puede hacer lo siguiente para comprobar si el agente funciona correctamente:

- Una vez que el agente se haya registrado correctamente, acceda a Citrix ADM y vaya a **Redes > Agentes**. Puede ver los agentes descubiertos en esta página. Si el agente funciona correctamente, el estado se indica con un icono verde. Si no se está ejecutando, el estado se indica con un icono rojo.
- Inicie sesión en el intérprete de comandos del agente y ejecute los siguientes comandos: `ps -ax | grep mas` y `ps -ax | grep ulfd`. Asegúrese de que se estén ejecutando los siguientes procesos.

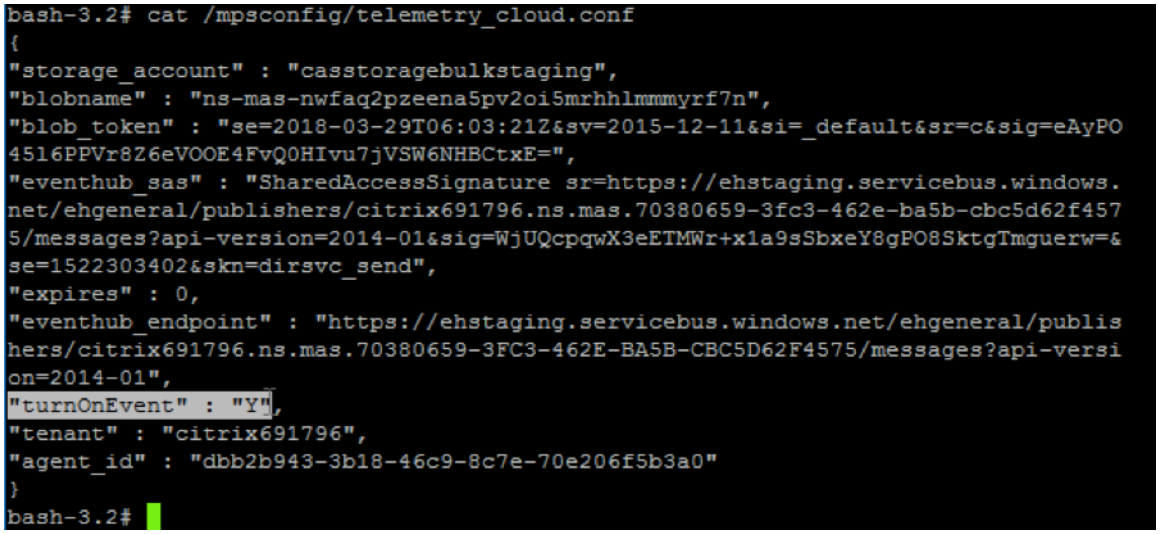
- Si alguno de los procesos no se está ejecutando, ejecute el comando **masd restart**. Es posible que tarde algún tiempo en iniciar todos los demonios (aproximadamente 1 minuto).
- Asegúrese de que `agent.conf` se haya creado en `/mpsconfig` después del registro correcto del agente.

Incorporación de instancias de Citrix Gateway

Las instancias de Citrix Gateway se agregan a Citrix Analytics, pero ¿cómo puedo saber si Analytics está habilitada en el agente?

Puede comprobar si el análisis está habilitado en el agente mediante el indicador de shell del agente. Si los análisis se habilitan correctamente en el agente, el parámetro `turnOnEvent` se establecería en `Y` en el archivo `/mpsconfig/telemetry_cloud.conf`.

Inicie sesión en el intérprete de comandos del agente y ejecute el siguiente comando: `cat /mpsconfig/telemetry_cloud.conf` y verifique el valor del parámetro `turnOnEvent`.



He cerrado accidentalmente el asistente de incorporación de Citrix Gateway. ¿Tengo que iniciar mi configuración desde el principio?

No. Citrix Analytics guarda el progreso y muestra la configuración incompleta como un mosaico en la página **Orígenes de datos > Parámetros**. Haga clic en **Continuar configuración** para completar la configuración.

Incorporación del sitio de Virtual Apps and Desktops

¿Cómo desactivo el procesamiento de datos?

Si desea inhabilitar temporalmente el procesamiento de datos de su sitio a Citrix Analytics, simplemente haga clic en la tarjeta **Sitio** y, a continuación, haga clic en **Desactivar el procesamiento de datos**.

Cuando agrego mi sitio a Workspace y hago clic en "Probar STA", la prueba falla. ¿Qué debo hacer?

Es posible que haya un problema de conectividad entre Citrix Gateway y Cloud Connectors. Para solucionar problemas, consulte CTX232517 en el Knowledge Center de soporte de Citrix.

¿Dónde puedo obtener ayuda con Citrix Analytics?

Puede hacer preguntas y ponerse en contacto con expertos de Citrix Analytics en el foro de debate de Citrix Analytics en https://discussions.citrix.com/forum/1710-citrix-analytics/.

Para participar en el foro, debe iniciar sesión con su ID de Citrix.

Garantía de acceso —Geolocalización

¿Cómo obtiene Analytics los detalles de geolocalización?

Citrix Analytics usa la dirección IP del dispositivo desde el que se inicia el cliente de Workspace. Citrix Analytics aprovecha un proveedor de datos de geolocalización IP de terceros para derivar la ubicación de un usuario a partir de su dirección IP. Cuando inicia sesión, resuelve su ubicación (dirección IPv4) en un país o ciudad, y la asignación se actualiza periódicamente. Las organizaciones pueden usar estas ubicaciones definidas por países para monitorear los patrones de acceso desde donde no hacen negocios.

¿Cuál es el nivel de precisión para derivar la ubicación de un usuario?

Citrix Analytics aprovecha un proveedor de datos de geolocalización IP de terceros para derivar la ubicación de un usuario a partir de su dirección IP. Los servicios GeoIP pueden resolver en la ciudad o ubicación correcta la mayor parte del tiempo, pero las búsquedas de GeoIP nunca son completamente precisas. A veces, la ubicación que se muestra a un usuario puede ser diferente de su ubicación precisa de acceso.

Según la documentación de IP GeoPoint, el nivel de cobertura es de aproximadamente el 99,99% de las direcciones IP asignadas en todo el mundo (direcciones IP enrutables IPv4). En términos de precisión de ubicación, acompaña a cada uno de los campos de ubicación esenciales (país, estado, ciudad, código postal) con un factor de confianza.

¿En qué casos es inexacta la determinación de la ubicación?

La precisión de los datos de geolocalización depende de cómo se conecte el dispositivo a Internet. Un dispositivo puede conectarse a Internet a través de:

- Puertas de enlace móviles
- VPN o servicio de alojamiento
- Servidor proxy o anonimizador regional o internacional

En tales casos, los datos de geolocalización no son precisos, independientemente de que se utilice el software del proveedor de geolocalización IP.

¿Cuáles son las versiones compatibles de la aplicación Citrix Workspace?

Hay versiones mínimas de la aplicación Citrix Workspace necesarias para que el sistema operativo envíe el atributo de **dirección IP** a Citrix Analytics for Security. Consulte la tabla de matriz o las ubicaciones identificadas como no disponibles para obtener más información.

¿En qué casos no recibimos los detalles geológicos?

Para ver los detalles de geolocalización, consulte la sección Ubicaciones identificadas como no disponibles para obtener más información.

¿Qué servicio de geolocalización utiliza Citrix Analytics para informar de la ubicación de un usuario? ¿Cómo informar de una ubicación incorrecta para una IP?

Citrix Analytics utiliza los servicios de geolocalización basados en archivos de Neustar para proporcionar datos de geolocalización para los accesos entrantes. Tiene una página de corrección de IP pública que se puede utilizar para enviar una solicitud de corrección por cuenta propia. Una vez que se envía una solicitud de corrección, Neustar revisa la solicitud para verificar su precisión y la procesa.

El proveedor de GeoIP ayuda a mostrar la información más precisa posible. Desafortunadamente, puede haber casos en los que los datos de GeoIP sean inexactos debido a la naturaleza innata de GeoIP.

Glosario de términos

April 12, 2024

- **Acciones**: respuestas de bucle cerrado a eventos sospechosos. Se aplican acciones para evitar que ocurran eventos anómalos en el futuro. Obtenga más información.
- **Agente de seguridad de acceso a la nube (CASB)**: punto de aplicación de la directiva de seguridad local o basado en la nube ubicado entre los consumidores de servicios en la nube y los proveedores de servicios Los CASB combinan e interponen directivas de seguridad empresarial a medida que se accede a los recursos basados en la nube. También ayudan a las organizaciones a ampliar los controles de seguridad de su infraestructura local a la nube.
- **Citrix ADC (Application Delivery Controller)**: Dispositivo de red que vive en un centro de datos, ubicado estratégicamente entre el firewall y uno o más servidores de aplicaciones. Maneja el equilibrio de carga entre servidores y optimiza el rendimiento y la seguridad del usuario final para las aplicaciones empresariales. Obtenga más información.

- **Citrix ADM (Application Delivery Management)**: Solución centralizada de administración, análisis y orquestación de redes. Desde una única plataforma, los administradores pueden ver, automatizar y administrar los servicios de red para arquitecturas de aplicaciones escalables. Obtenga más información.
- **Agente de Citrix ADM**: Proxy que permite la comunicación entre Citrix ADM y las instancias administradas en un centro de datos. Obtenga más información.
- **Citrix Analytics**: Servicio en la nube que recopila datos en servicios y productos (locales y en la nube) y genera información procesable, lo que permite a los administradores gestionar de forma proactiva las amenazas a la seguridad de los usuarios y las aplicaciones, mejorar el rendimiento de las aplicaciones y admitir operaciones continuas. Obtenga más información.
- **Citrix Cloud**: plataforma que se conecta a los recursos a través de Citrix Cloud Connector en cualquier nube o infraestructura (local, nube pública, nube privada o nube híbrida). Obtenga más información.
- **Citrix Gateway**: Solución de acceso remoto consolidada que consolida la infraestructura de acceso remoto para proporcionar un inicio de sesión único en todas las aplicaciones, ya sea en un centro de datos, en la nube o entregadas como SaaS. Más información.
- **Citrix Hypervisor**: Plataforma de administración de virtualización optimizada para infraestructuras de virtualización de aplicaciones, escritorios y servidores. Obtenga más información.
- **Aplicación Citrix Workspace** (anteriormente conocida como Citrix Receiver): Software cliente que proporciona un acceso seguro y sin problemas a las aplicaciones, escritorios y datos desde cualquier dispositivo, incluidos smartphones, tabletas, PC y Mac. Obtenga más información.
- **DLP (Prevención de pérdida de datos)**: Solución que describe un conjunto de tecnologías y técnicas de inspección para clasificar la información contenida en un objeto, como un archivo, correo electrónico, paquete, aplicación o un almacén de datos. Además, el objeto también puede estar en almacenamiento, en uso o en una red. Las herramientas de DLP pueden aplicar directivas de forma dinámica, como registrar, informar, clasificar, reubicar, etiquetar y cifrar. Las herramientas de DLP también pueden aplicar protecciones de administración de derechos de datos empresariales. Obtenga más información.
- **DNS (Sistema de nombres de dominio)**: Servicio de red que se utiliza para localizar nombres de dominio de Internet y traducirlos a direcciones de protocolo de Internet (IP). El DNS mapea los nombres de sitios web que los usuarios proporcionan, a sus direcciones IP correspondientes que proporcionan las máquinas, para ubicar un sitio web independientemente de la ubicación física de las entidades.
- **Procesamiento de datos**: Método de procesamiento de datos desde una fuente de datos a Citrix Analytics. Obtenga más información.

- **Origen de datos**: Producto o servicio que envía datos a Citrix Analytics. Un origen de datos puede ser interno o externo. [Más información]/en-us/citrix-analytics/data-sources.html).
- **Exportación de datos**: Producto o servicio que recibe datos de Citrix Analytics y proporciona información. Obtenga más información.
- **Usuarios descubiertos**: Total de usuarios de una organización que utilizan orígenes de datos. Obtenga más información.
- **FQDN (nombre de dominio completo)**: Nombre de dominio completo para el acceso interno (StoreFront) y externo (Citrix ADC).
- **Aprendizaje automático**: Tipo de tecnología de análisis de datos que extrae conocimiento sin programarse explícitamente para hacerlo. Los datos de una amplia variedad de fuentes potenciales, como aplicaciones, sensores, redes, dispositivos y dispositivos, se introducen en un sistema de aprendizaje automático. El sistema utiliza los datos y aplica algoritmos para construir su propia lógica para resolver un problema, obtener información o hacer una predicción.
- **Microsoft Graph Security**: puerta de enlace que conecta la seguridad del cliente y los datos organizativos Proporciona alertas y opciones de corrección fáciles de revisar cuando se debe tomar una medida. Obtenga más información.
- **Análisis de rendimiento**: servicio que proporciona visibilidad de los detalles de las sesiones de los usuarios en toda la organización. Obtenga más información.
- **Directiva**: Conjunto de condiciones que deben cumplirse para que una acción se aplique en el perfil de riesgo de un usuario. Obtenga más información.
- **Indicador de riesgo**: Métrica que proporciona información sobre el nivel de exposición a un riesgo empresarial que la organización tiene en un momento dado. Obtenga más información.
- **Puntuación de riesgo**: Valor dinámico que indica el nivel agregado de riesgo que un usuario o una entidad representa para una infraestructura de TI durante un período de supervisión predeterminado. Obtenga más información.
- **Cronograma de riesgo**: Registro del comportamiento de riesgo de un usuario o una entidad que permite a los administradores investigar un perfil de riesgo y comprender el uso de datos, el uso del dispositivo, el uso de la aplicación y el uso de la ubicación. Obtenga más información.
- **Usuario con riesgos**: Usuario que ha actuado de manera arriesgada o ha presentado un comportamiento con riesgos. Obtenga más información.
- **Análisis de seguridad**: Análisis avanzado de datos que se utilizan para lograr resultados de seguridad convincentes, como la supervisión de la seguridad y la búsqueda de amenazas. Obtenga más información.
- **Secure Private Access**: Servicio que proporciona integración de inicio de sesión único, acceso remoto e inspección de contenido en una única solución para el control de acceso de extremo

a extremo. Obtenga más información.

- **Splunk**: software SIEM (Administración de eventos e información de seguridad) que recibe datos inteligentes de Citrix Analytics y proporciona información sobre los posibles riesgos empresariales. Obtenga más información.
- **UBA (Análisis del comportamiento del usuario)**: Proceso de referencia de la actividad y el comportamiento de los usuarios en combinación con el análisis de grupos de pares, para detectar posibles intrusiones y actividades maliciosas.
- Lista de**seguimiento: lista**de usuarios o entidades a los que los administradores quieren supervisar en busca de actividades sospechosas. Obtenga más información.