# NetWitness® Plataforma

Versión 12.5

# Notas de la versión

NETWITNESS
Platform

## Información de contacto

La comunidad de NetWitness en https://community.netwitness.com contiene una base de conocimientos que responde preguntas comunes y proporciona soluciones a problemas conocidos, documentación de productos, debates de la comunidad y gestión de casos.

## Marcas comerciales

RSA y otras marcas comerciales pertenecen a RSA Security LLC o sus filiales (“RSA”). Para obtener una lista de las marcas comerciales de RSA, vaya a https://www.rsa.com/en-us/company/rsa-trademarks. Las demás marcas comerciales pertenecen a sus respectivos propietarios.

## Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de RSA Security LLC o sus filiales, se suministran bajo licencia y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con la inclusión del aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal. Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por RSA.

Se recomienda no implementar repositorios de terceros ni realizar ningún cambio en el sistema operativo subyacente de NetWitness que no sea parte de la versión compatible de NetWitness. Cualquier cambio de este tipo fuera de la imagen aprobada de NetWitness puede generar un conflicto de servicio o funcionalidad y requerir una nueva imagen del sistema NetWitness para que NetWitness vuelva a un estado funcional optimizado. En el caso de que se implemente un repositorio de terceros o el cliente realice otro cambio no compatible sin la aprobación de NetWitness, el cliente asume toda la responsabilidad por cualquier mal funcionamiento del sistema hasta que el problema pueda solucionarse mediante esfuerzos de resolución de problemas o una nueva imagen del servicio.

## Licencias de otros fabricantes

Este producto puede incluir software desarrollado por terceros ajenos a RSA. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en NetWitness Community. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

## Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las normativas actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

## Distribución

El uso, la copia y la distribución de cualquier software de RSA Security LLC o sus filiales (“RSA”) descrito en esta publicación requieren la licencia de software correspondiente.

RSA considera que la información aquí contenida es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA “TAL CUAL”. RSA NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

## Misceláneo

Este producto, este software, la documentación asociada y los contenidos están sujetos a los Términos y condiciones estándar de NetWitness vigentes a partir de la fecha de emisión de esta documentación y que se pueden encontrar en https://www.netwitness.com/standard-form-agreements/.



Septiembre de 2024

# Contenido

# Novedades de la versión 12.5.0.0

Las notas de la versión de NetWitness 12.5.0.0 describen nuevas características, mejoras, actualizaciones de seguridad, rutas de actualización, problemas solucionados, problemas conocidos, funcionalidades de fin de vida útil, números de compilación y recursos de autoayuda.

## Mejoras

Las siguientes secciones son una lista completa y una descripción de las mejoras a capacidades específicas:

- Dashboard
- Investigate
- Respond
- Insight
- User and Entity Behavior Analytics
- Funcionalidad SASE
- Endpoint
- Administración de contenido centralizada (CCM) basada en políticas
- Servicios de Concentrator, Decoder, Log Collector y Archiver
- Integraciones de registros
- Context Hub
- Live Cloud Service

Para localizar los documentos a los que se hace referencia en esta sección, consulte https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246.

La sección Documentación del producto tiene enlaces a la documentación de esta versión.

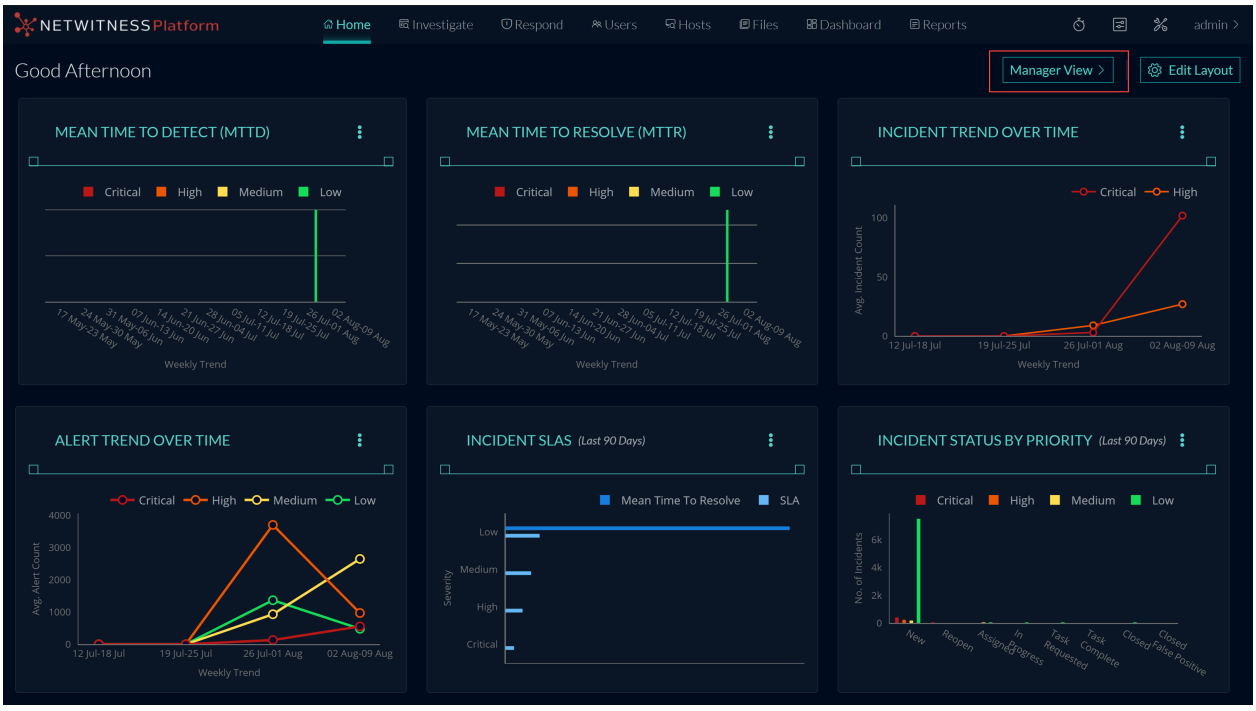
## Dashboard

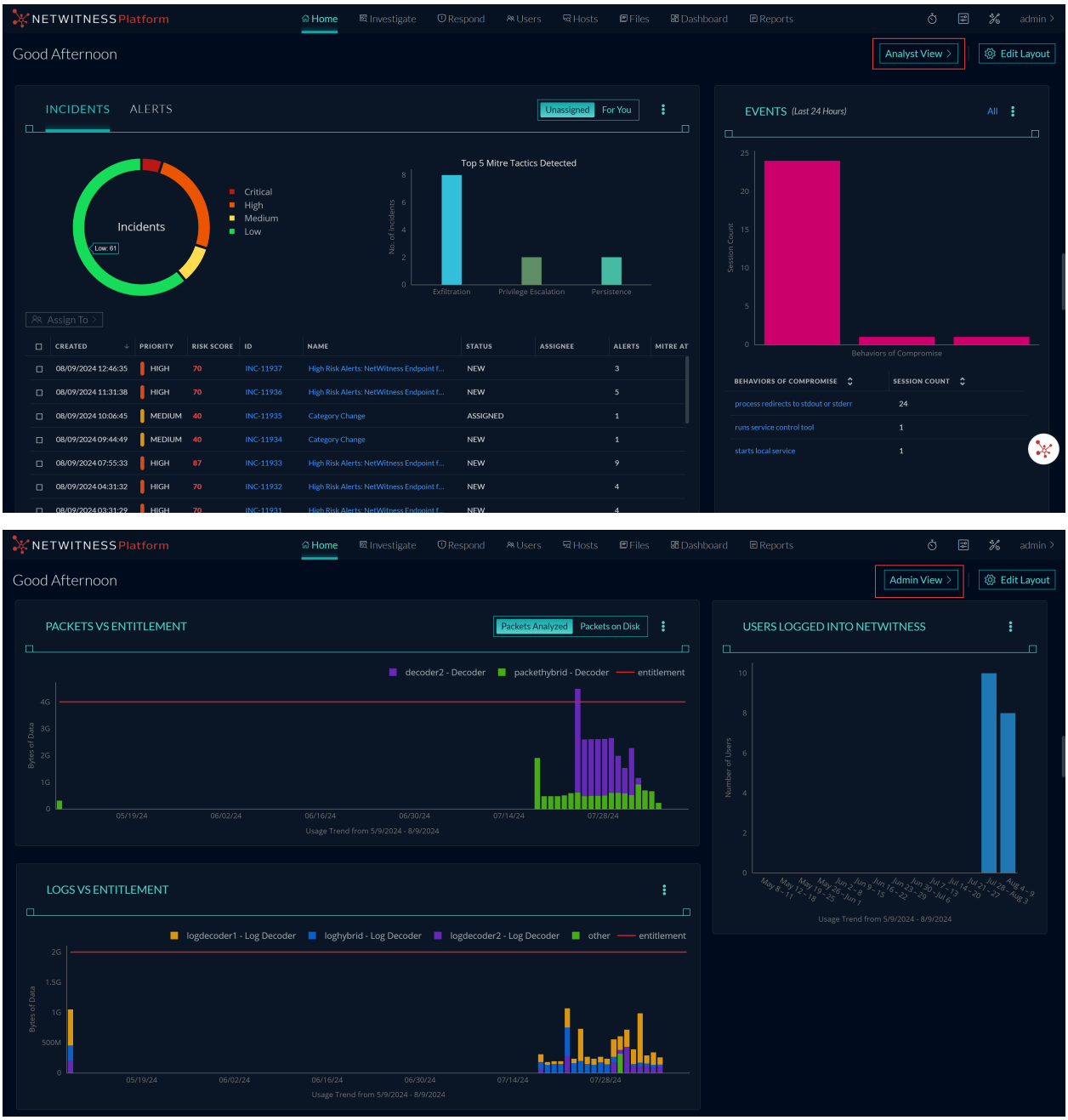
La siguiente sección describe las nuevas mejoras para el componente Dashboard:

### Nuevas páginas de inicio

NetWitness presenta un nuevo menú en la página de **Inicio** que consta de las vistas **Admin**, **Analista** y **Administrador**. Cada página de inicio se compone de varios widgets. Los administradores, analistas y gerentes de SOC pueden acceder a los widgets respectivos que muestran ciertos datos en forma gráfica. Los datos se pueden asociar con terminales, usuarios, recursos, contenido, incidentes, alertas, MITRE ATT&CK, retención y mucho más.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
INCIDENTS
9
NEW INCIDENTS
8
CLOSED INCIDENTS
0
ALERTS
40
MEAN TIME TO RESOLVE
0 Sec
MITRE ATT&CK® OVERVIEW
MEDIUM
CONTENT TYPE
EXPAND ALL SUB TECHNIQUES
Deployed
Partially Deployed
Not Deployed
Unavailable
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
5 of 10 techniques
2 of 8 techniques
7 of 10 techniques
7 of 14 techniques
15 of 20 techniques
13 of 14 techniques
25 of 43 techniques
7 of 17 techniques
16 of 32 techniques
3 of 9 techniques
9 of 17 techniques
7 of 17 techniques
6 of 9 techniq


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
MEAN TIME TO DETECT (MTTD)
Critical
High
Medium
Low
Weekly Trend
MEAN TIME TO RESOLVE (MTTR)
Critical
High
Medium
Low
Weekly Trend
INCIDENT TREND OVER TIME
Critical
High
Avg. Incident Count
100
50
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
ALERT TREND OVER TIME
Critical
High
Medium
Low
Avg. Alert Count
4000
3000
2000
1000
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
INCIDENT SLAS (Last 90 Days)
Mean Time To Resolve
SLA
Severity
Low
Medium
High
Critical
INCIDENT STATUS BY PRIORITY (Last 90 Days)
Critical
High
Medium
Low
No. of Incidents
6k
4k
2k
0
New
Reopen
Assigned
In Progress
Task Requested
Task Complete
Closed
Closed False Positive



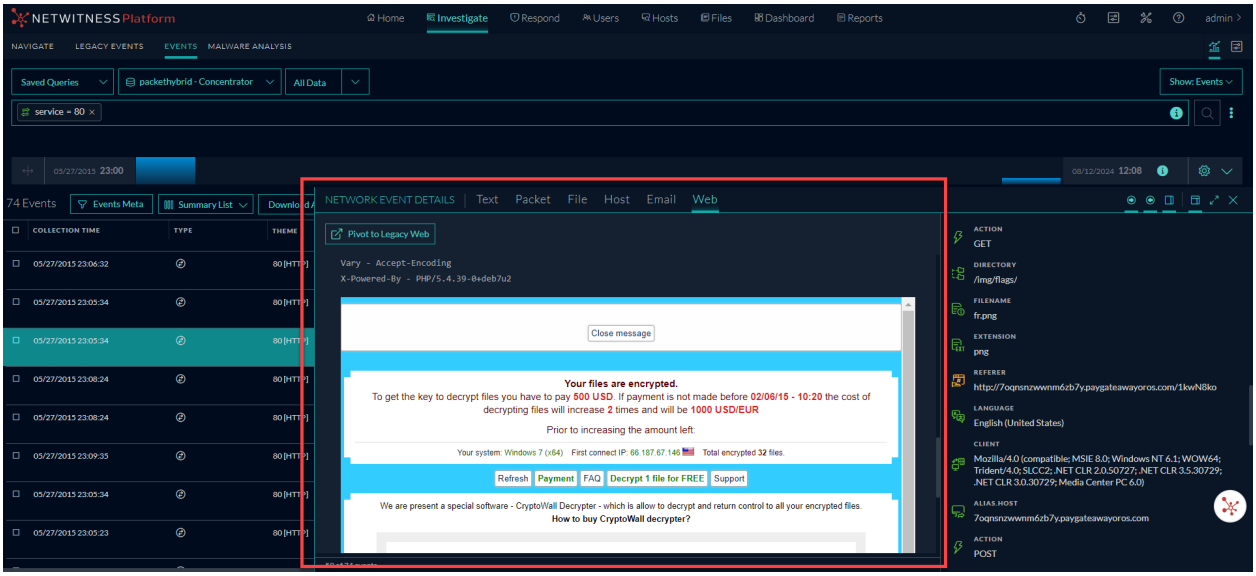

Para obtener más información, consulte el tema **Administrar widgets de inicio** en la Guía de introducción de NetWitness para 12.5.

## Investigate

La siguiente sección describe las nuevas mejoras para el componente Investigate:

## Reconstrucción web desde la vista Eventos

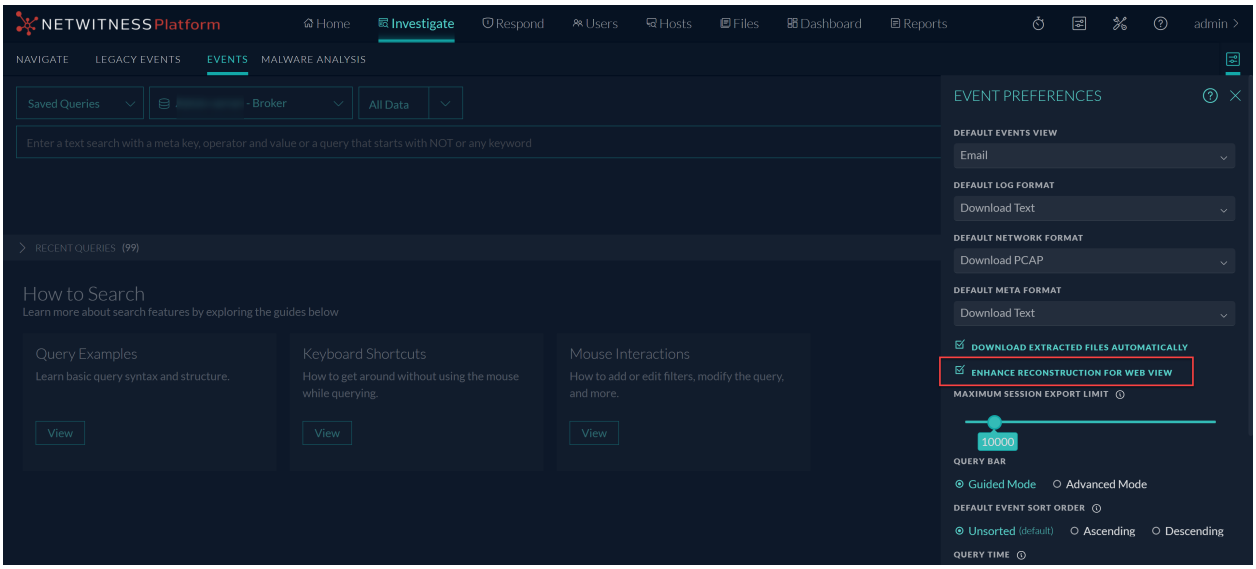
Los analistas pueden reconstruir de forma segura la vista web del evento de destino desde la vista **Eventos > Reconstrucción web** si un usuario ha visitado páginas web relacionadas con un evento en particular. NetWitness puede reconstruir la misma página web con los datos disponibles en paquetes, mostrando esa página web y relacionándola con las imágenes y los estilos CSS con la mayor precisión posible. Este proceso de reconstrucción web permite a los analistas obtener información valiosa sobre la actividad web realizada, lo que facilita un análisis y una investigación eficaces.




Para obtener más información, consulte la sección **Reconstrucción web** del tema **Examinar detalles de eventos en la vista Eventos** de la Guía del usuario de NetWitness Investigate para 12.5.

## Reconstrucción mejorada de eventos en la vista web

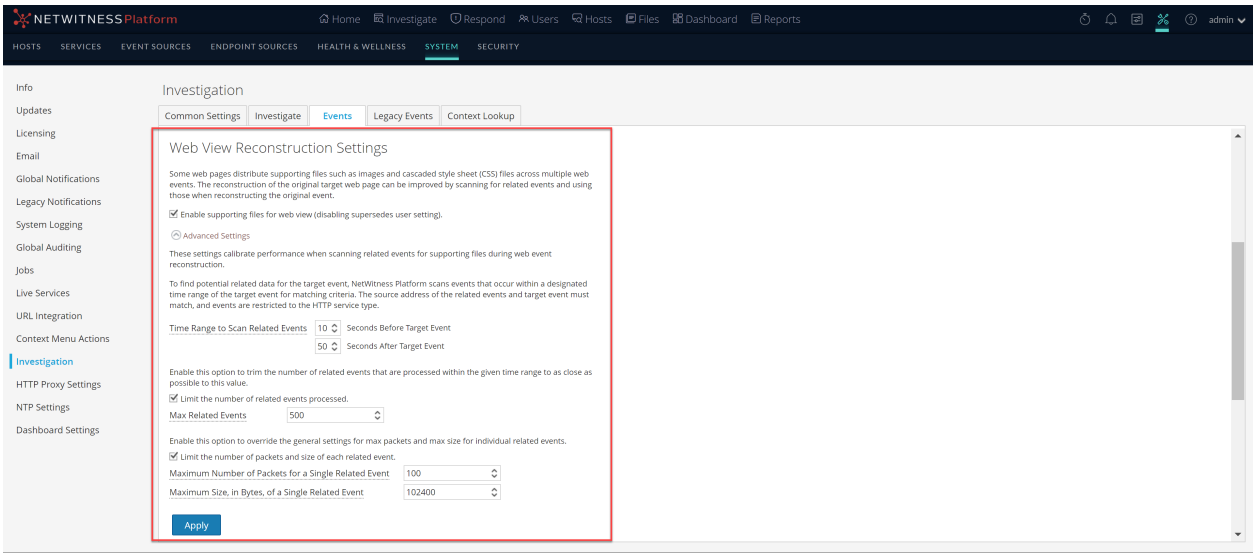
Se ha agregado una nueva preferencia de usuario, **Mejorar reconstrucción para vista web**, al panel **Preferencias de eventos** en la vista **Investigate** > **Eventos**. Esta preferencia está habilitada de forma predeterminada para todos los usuarios. Esta opción mejora la reconstrucción de sitios web que reconstruyen un evento mediante el uso de CSS, imágenes y enlaces para formatear la vista de manera eficaz, permitiendo así a los analistas comprender mejor el contexto y los detalles de los eventos que están reconstruyendo. Esta mejora permite a los analistas realizar un análisis más informado y preciso y tomar las medidas adecuadas.




Para obtener más información, consulte el tema **Establecer preferencias de usuario para la vista Eventos** en la *Guía del usuario de NetWitness Investigate*.

## Presentación de la configuración de reconstrucción de vista web desde la vista del sistema

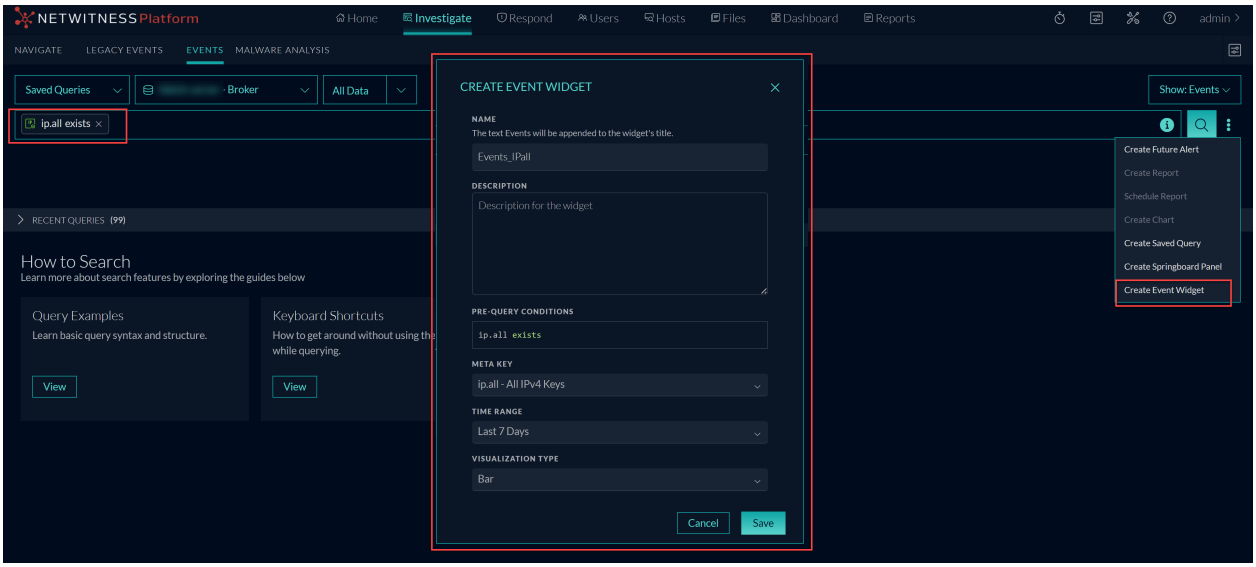
NetWitness presenta la nueva **Configuración de reconstrucción de vista web** desde la vista  **(Administrador)** > **Sistema** > **Investigación**. Esta configuración de la pestaña **Eventos** permite a los administradores mejorar la reconstrucción de vistas web escaneando y reconstruyendo eventos relacionados con los mismos archivos de soporte. Al reconstruir una vista web que abarca varios eventos, el sistema puede mejorar la reconstrucción del evento de destino incluyendo eventos relacionados que contienen imágenes y archivos CSS relevantes. Solo se escanearán los eventos de tipo servicio HTTP con la misma dirección de origen que el evento de destino y una marca de tiempo dentro de un rango de tiempo específico antes y después del evento de destino. Los administradores también pueden configurar el número máximo de eventos relacionados para escanear, lo que proporciona mayor flexibilidad y precisión en la reconstrucción de la vista web. La opción Configuración avanzada muestra todos los ajustes configurables de esta sección.




Para obtener más información, consulte la sección **Configuración de reconstrucción de vista web** del tema **Panel de configuración de Investigation** en la Guía de configuración del sistema.

## Crear un widget de eventos personalizado a partir de una consulta

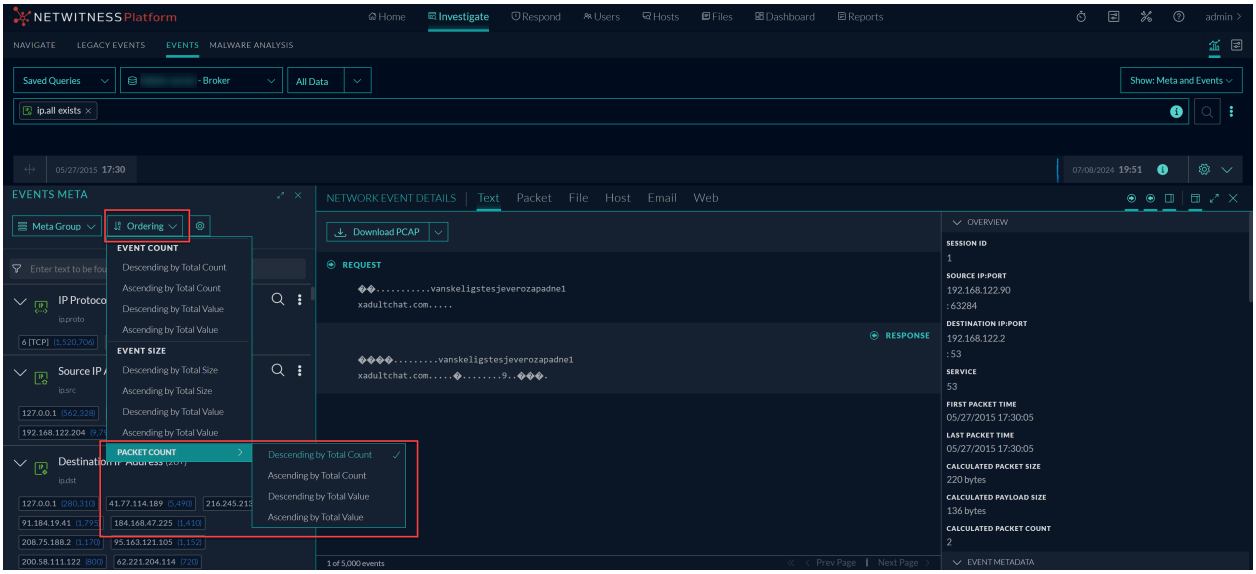
Durante la investigación, los administradores y analistas ahora pueden crear un widget de eventos desde la vista **Investigate** > **Eventos**. Los usuarios pueden agregar cualquier cantidad de filtros a la barra de búsqueda de consultas y convertir estas búsquedas en widgets de eventos para una mejor detección y monitoreo. El widget recién creado se guardará para un acceso rápido en la biblioteca de la página de inicio. Luego, los usuarios pueden agregar el widget de Evento a la vista Diseño del tablero (**Administrador**, **Analista** o **Gerente**) en la página de inicio y personalizar su configuración para adaptarla a sus necesidades. Esta característica mejora el monitoreo y análisis de eventos, lo que permite a los usuarios rastrear y observar eventos relevantes e importantes en tiempo real.




Para obtener más información, consulte el tema **Crear widget de eventos desde la vista de investigación** en la Guía del usuario de NetWitness Investigate para 12.5.

## Ordenar los resultados de claves de metadatos por cantidad de paquetes

Los analistas ahora pueden ordenar los resultados de cada clave de metadatos por la cantidad de paquetes de la sesión en la página **Investigate** > **Eventos**. Puede ordenar los resultados por Valor o Total y en orden ascendente o descendente. Al ordenar los resultados de claves de metadatos por cantidad de paquetes, se pueden encontrar fácilmente los valores de metadatos más o menos frecuentes que ocurrieron en el entorno del usuario y que pueden usarse para investigaciones o análisis adicionales.




Para obtener más información, consulte la sección **Establecer el método de orden para valores de metadatos** del tema **Desglosar a metadatos en la vista Eventos** de la Guía del usuario de NetWitness Investigate para 12.5.

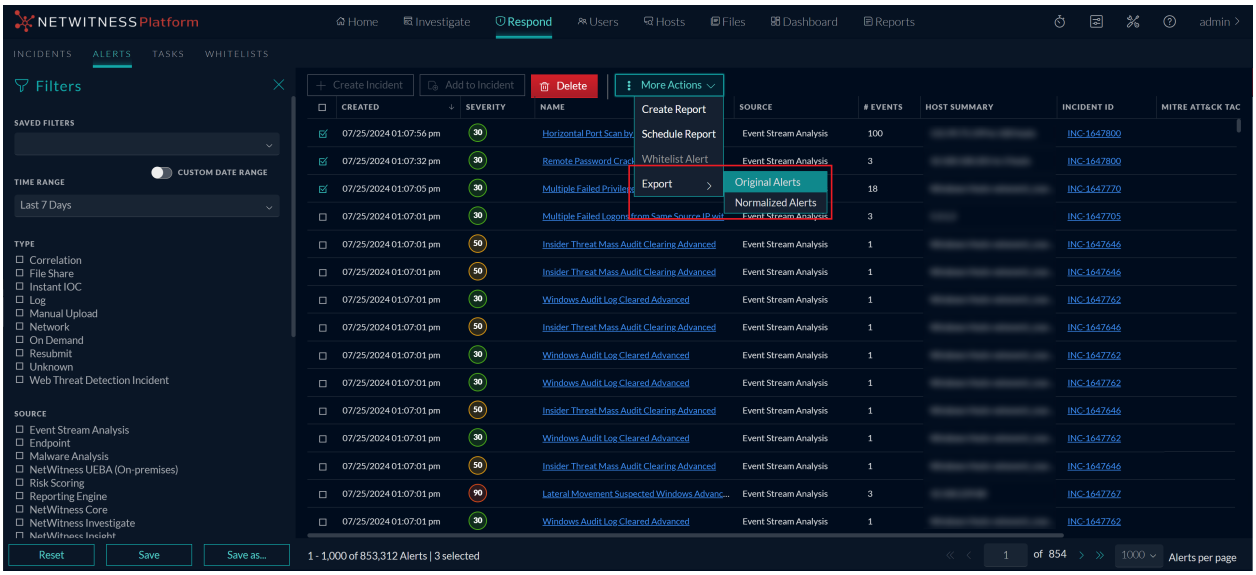
# Respond

La siguiente sección describe las nuevas mejoras para el componente Respond:

## Mejora de la vista Alertas

La opción **Exportar** en **Respond** > **Alertas** > Seleccionar una alerta > **Más acciones** le permite exportar y descargar las alertas originales y normalizadas junto con los eventos en formato JSON. NetWitness Platform le permite exportar hasta **1000** alertas a la vez para una investigación sin conexión.

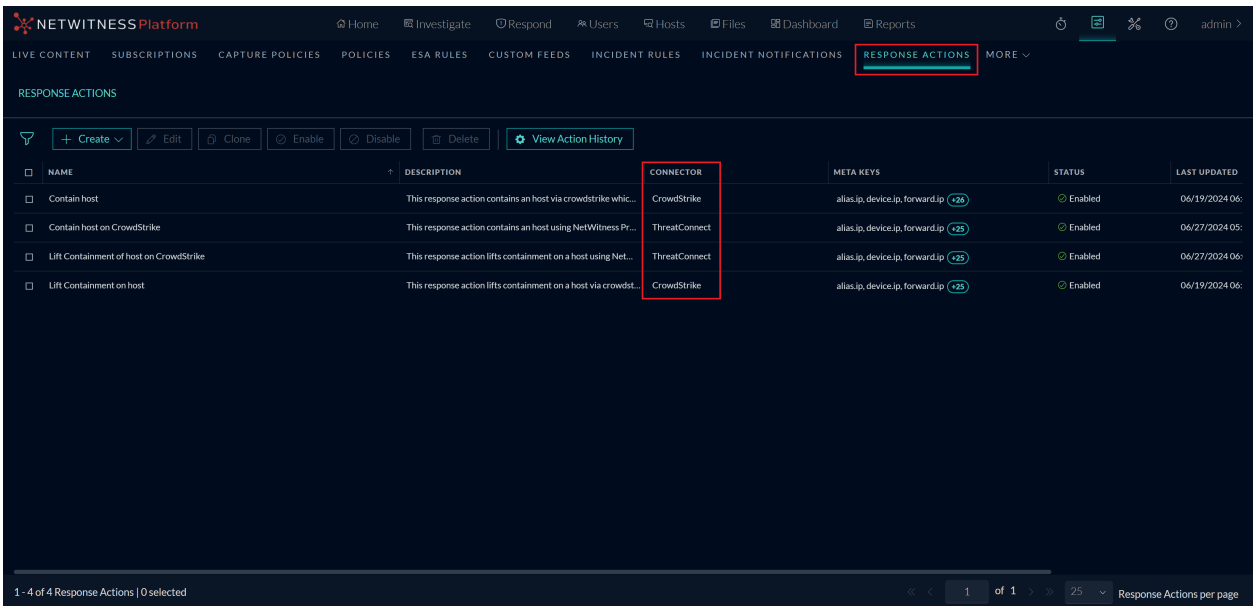
Para obtener más información, consulte **Exportar datos de alertas** en la *Guía del usuario de NetWitness Respond para 12.5*.




## Acciones de respuesta OOTB

Introducción de acciones listas para usar (OOTB) como parte del Servicio de Acciones de Respuesta. Las acciones OOTB "Contener host" y "Levantar contención en host" están habilitadas para CrowdStrike y CrowdStrike integrado a través de NetWitness Orchestrator. Esta mejora permite a los analistas ejecutar acciones de respuesta manualmente después de revisar un incidente o automáticamente como parte de un incidente activado. Las acciones de respuesta con CrowdStrike están disponibles directamente o a través de NetWitness Orchestrator.

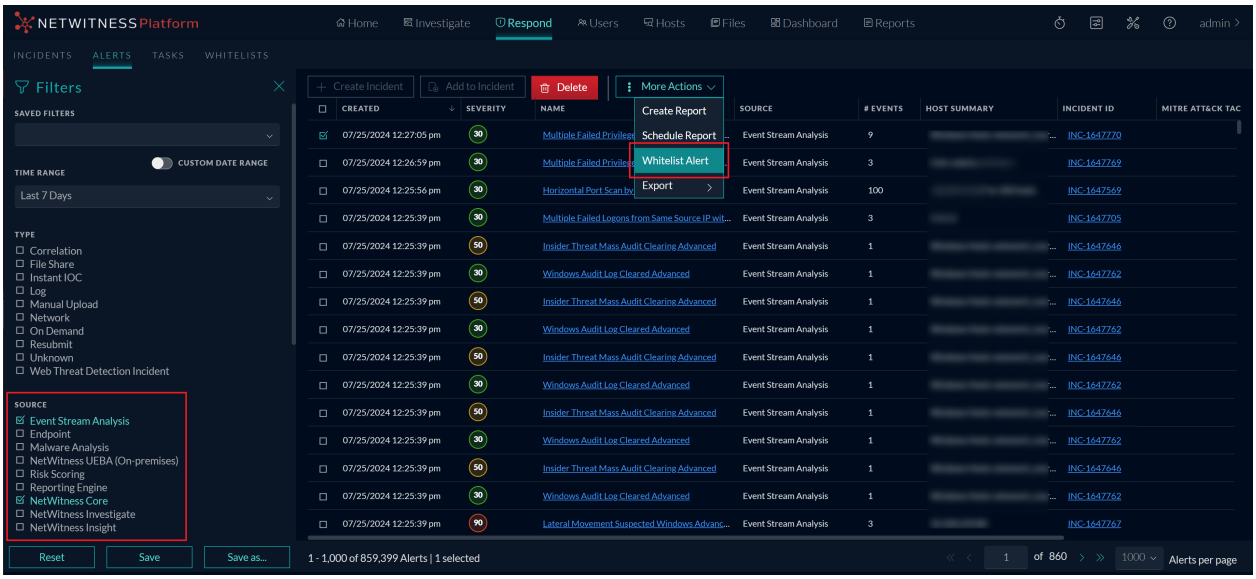
Para obtener más información, consulte **Acciones de respuesta** en la *Guía de configuración de NetWitness Respond para 12.5*.



## Mejora de la lista blanca

Se ha mejorado la característica Lista blanca para incluir alertas para los servicios de Event Stream Analysis y NetWitness Core. Ahora puede incluir en la lista blanca las alertas no sospechosas recurrentes y no deseadas para estos servicios. Esto le permite seleccionar entidades específicas y establecer condiciones de lista blanca para evitar alertas no deseadas para esas entidades.

Para obtener más información, consulte la **vista Lista de listas blancas** en la *Guía del usuario de NetWitness Respond para 12.5*.

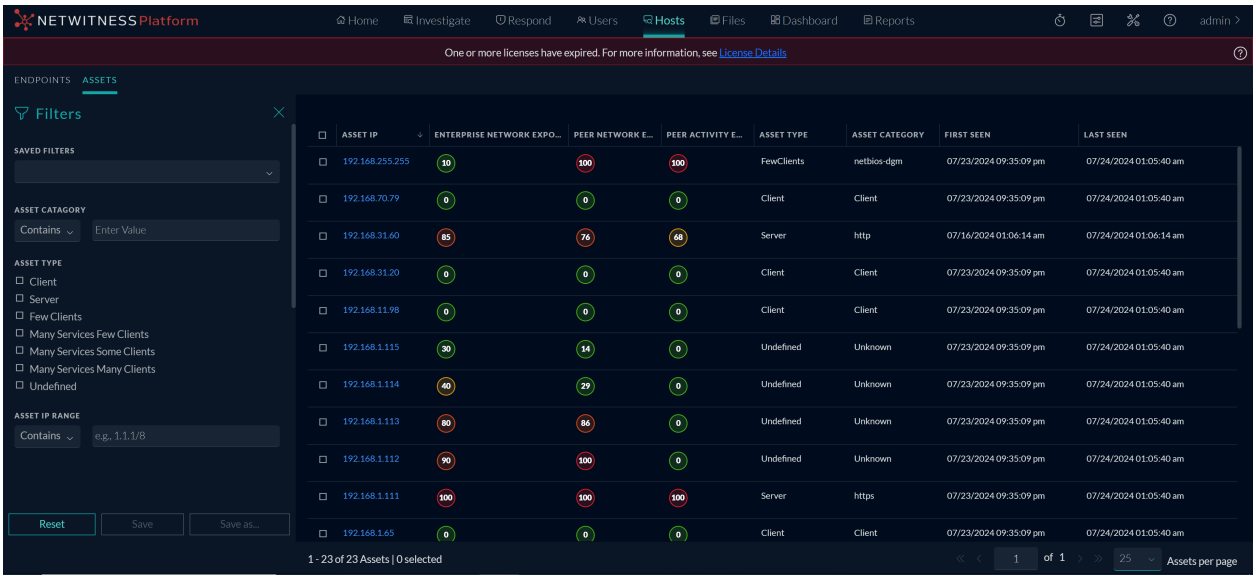



# Insight

La siguiente sección describe las nuevas mejoras del componente Insight:

## Nueva vista de activos para la detección e investigación de activos de red

NetWitness presenta una nueva vista de activos dentro del menú **Hosts > Activos**. Esta vista proporciona una ubicación centralizada donde se detectan todos los activos de red dentro de su entorno junto con los detalles asociados, como IP del activo, tipo de activo, categoría de activo, exposición de red empresarial, exposición de red par, exposición de actividad de pares, visto por primera vez y visto por última vez. Puede utilizar filtros para limitar los activos según diferentes criterios. Esta vista ayuda a los analistas a identificar y priorizar fácilmente los activos que se comportan de manera anormal o desconocidos, lo que les permite tomar medidas inmediatas para mitigar cualquier riesgo de seguridad potencial.



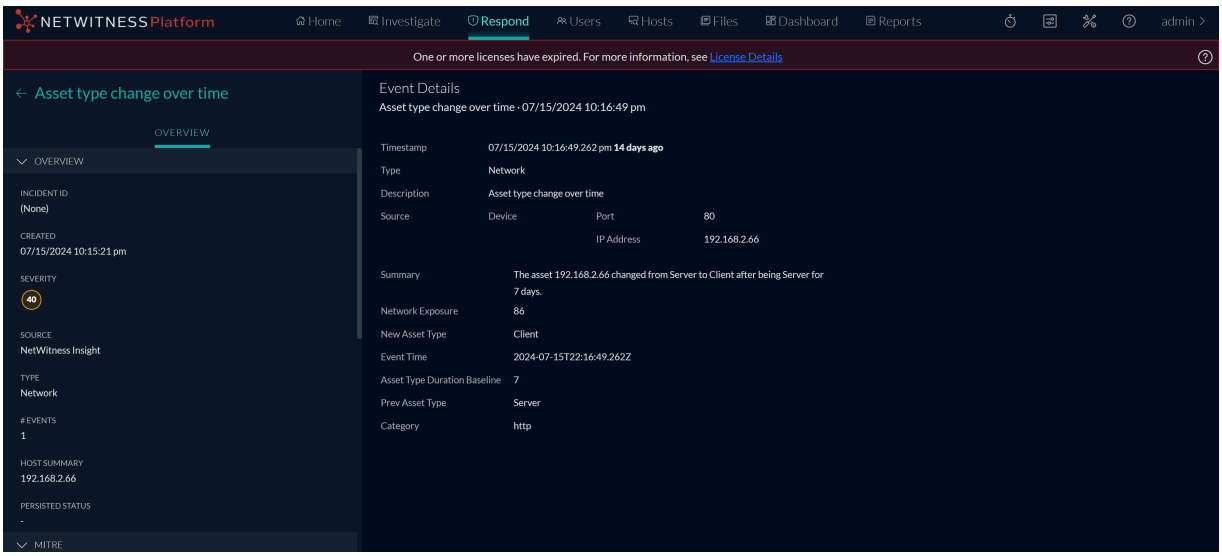

## Nuevas alertas de Insight para activos de red

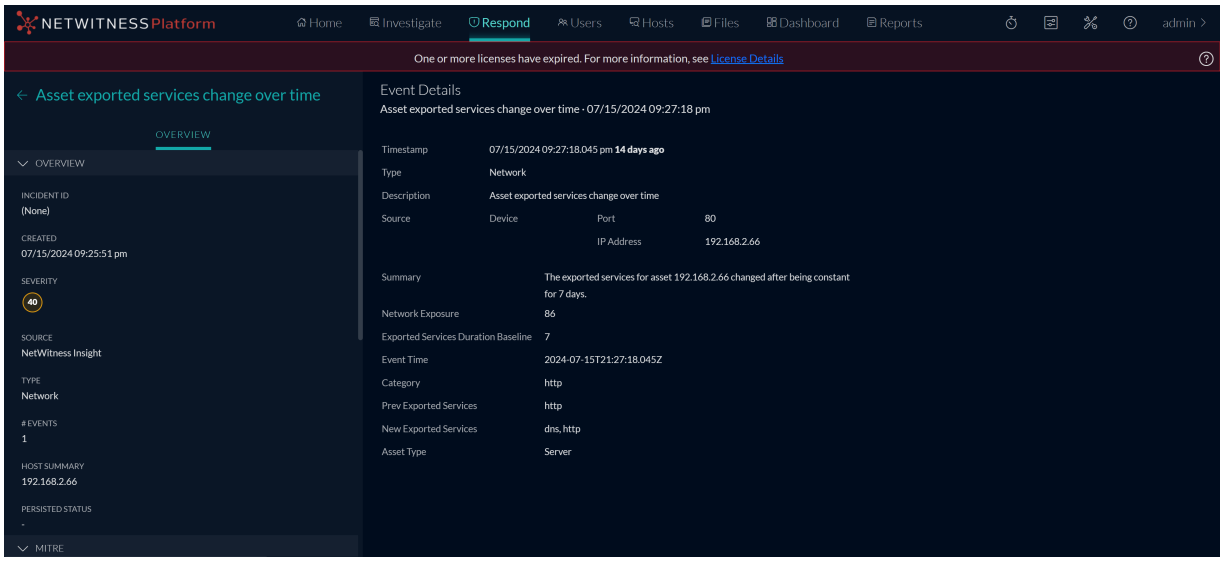
NetWitness presenta dos nuevas alertas Insight para ayudarle a monitorear y responder a los cambios en los activos de su red. Estas alertas están disponibles en la vista **Respond** > **Alertas** y se basan en el tipo de activo y los servicios exportados de cada activo.

- **Cambio del tipo de activo a lo largo del tiempo**: Esta alerta se genera cuando hay un cambio en el tipo de un activo (por ejemplo, de cliente a servidor) después de que se haya observado el mismo tipo durante 7 días consecutivos.

- **Cambio de servicios exportados por activo a lo largo del tiempo**: Esta alerta se genera si hay un cambio en la cantidad de servicios exportados por un activo después de observar la misma cantidad de servicios durante 7 días consecutivos, incluso si la categoría del activo permanece sin cambios.

  Estas alertas ayudan a los analistas a identificar e investigar cualquier anomalía o amenaza potencial en su entorno.






Para obtener más información, consulte la sección **NetWitness Insight** en el *Portal de documentación de NetWitness*.

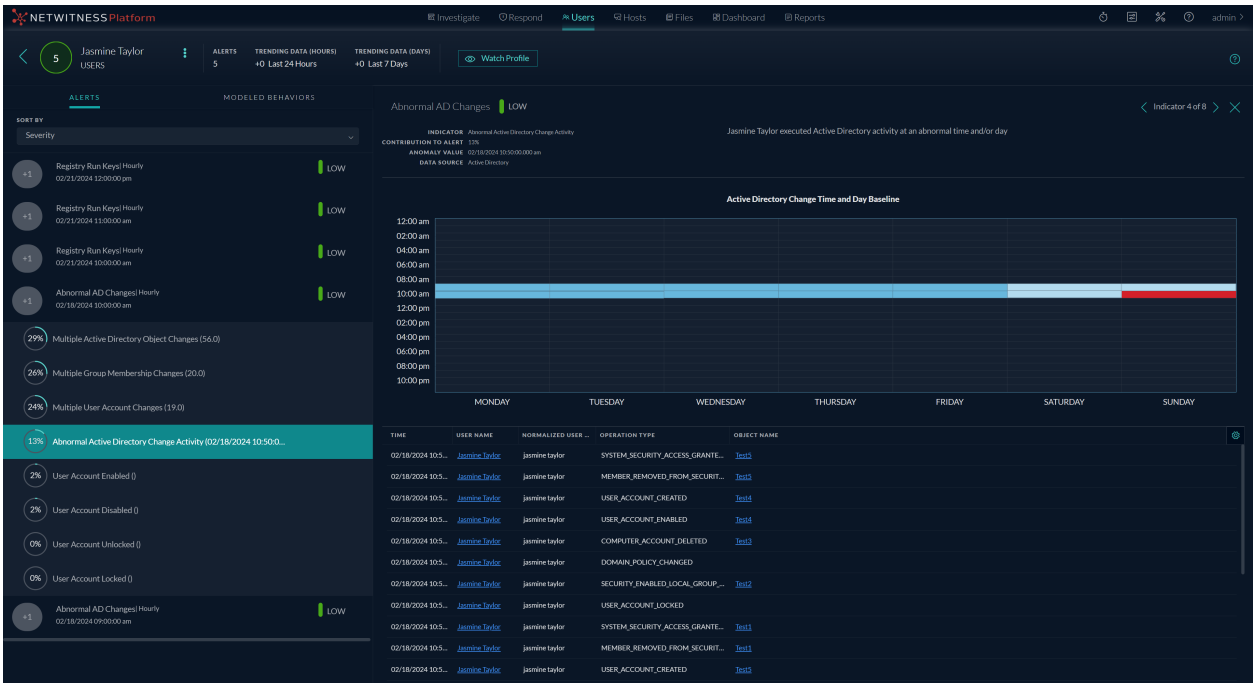
## User and Entity Behavior Analytics

La siguiente sección describe las nuevas mejoras para el componente UEBA:

### Detección de anomalías UEBA mediante el día de la semana

NetWitness UEBA mejora las funcionalidades de detección de anomalías al introducir la característica Día de la semana. Esta característica permite la detección de patrones de acceso no estándar que pueden indicar una cuenta comprometida o una amenaza interna. Cuando la actividad de un usuario monitoreado o de una entidad de red en un día particular de la semana difiere de su línea base habitual, UEBA lo marca como una anomalía, genera una alerta de Acceso no estándar o Actividad no estándar y notifica a los analistas para una mayor investigación y verificación. Para obtener más información sobre las actividades monitoreadas rastreadas para Acceso no estándar y Actividad no estándar, consulte el tema **Tipos de alerta** en la *Guía del usuario de NetWitness UEBA*.

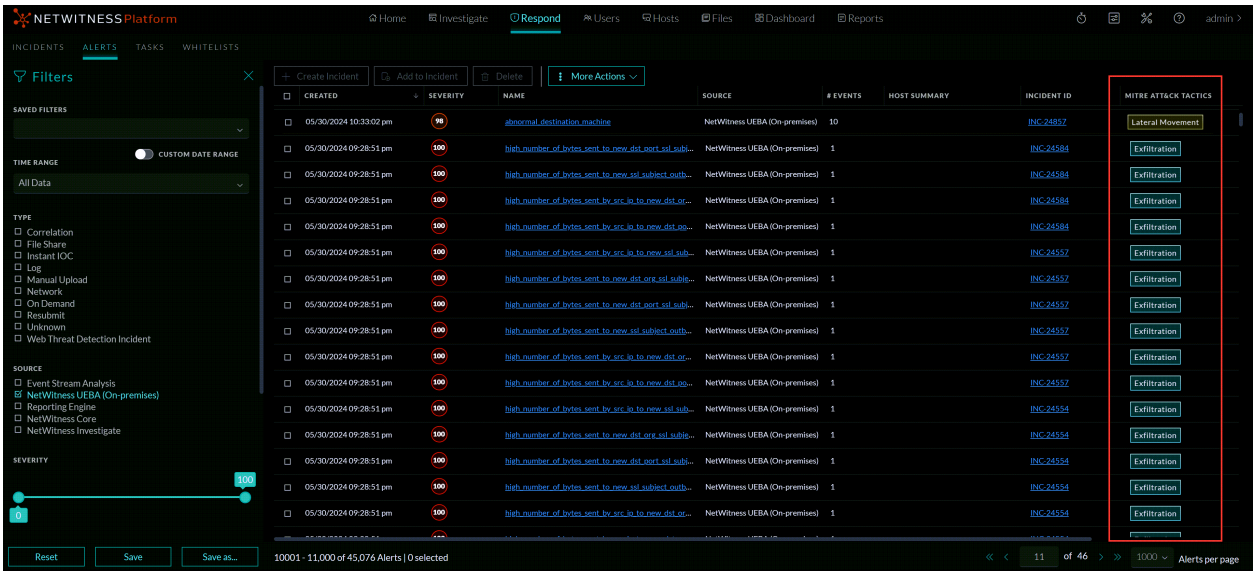
Por ejemplo, el usuario accedió a Active Directory en un día anormal. El usuario normalmente trabaja de lunes a viernes, pero inició sesión un domingo y realizó cambios en Active Directory. NetWitness UEBA detectó este comportamiento como una anomalía basándose en la mejora de día de la semana, lo que indica que ese es un día inusual para que este usuario realice cambios en AD, lo que genera una alerta para que los analistas investiguen.




## Mapeo MITRE ATT&CK para UEBA

NetWitness ahora integra el mapeo del marco MITRE ATT&CK para alertas e incidentes de UEBA. Este mapeo ayuda a los analistas a comprender las posibles tácticas, técnicas y subtécnicas del atacante detrás de las actividades detectadas al correlacionarlas con comportamientos conocidos. Al investigar alertas e incidentes de UEBA, los analistas pueden ver una lista de tácticas y técnicas asignadas desde la vista **Respond**, junto con un panel **ATT&CK Explorer** dedicado que proporciona más contexto e información relacionada, lo que elimina la necesidad de visitar el sitio web de MITRE para obtener información sobre ATT&CK. Esta mejora proporciona información valiosa sobre la gravedad y la naturaleza de las amenazas, lo que permite tomar decisiones de respuesta más rápidas e informadas.

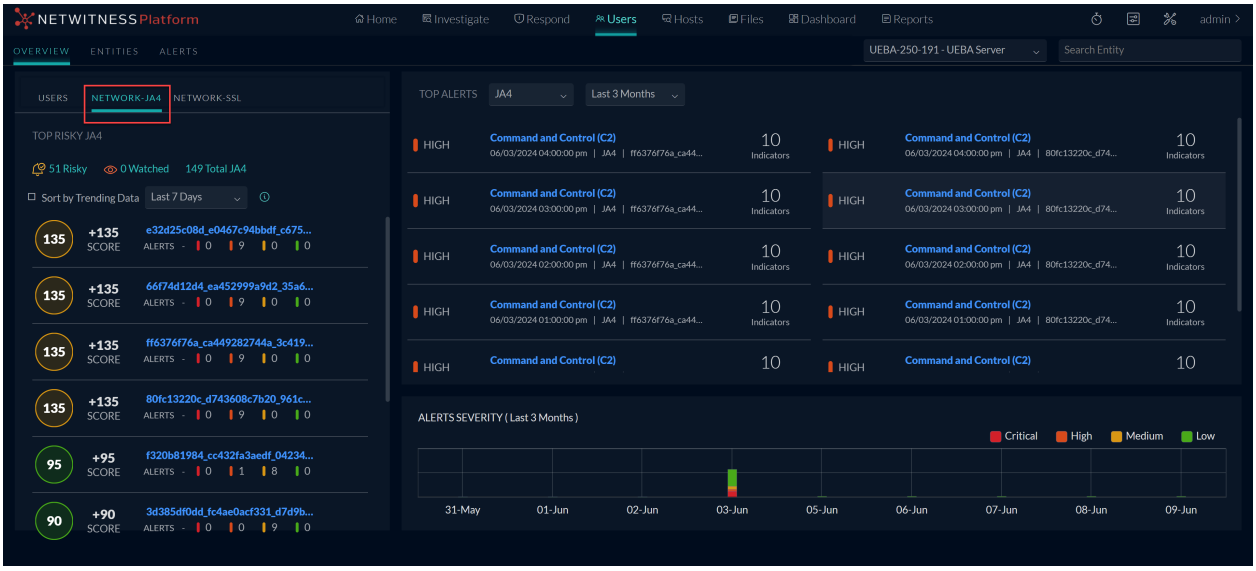
Por ejemplo, una alerta UEBA identificó un comportamiento de acceso remoto sospechoso desde una cuenta de usuario. Este comportamiento se alinea con la táctica MITRE ATT&CK de **Movimiento lateral** y la técnica que utiliza **Servicios remotos**, alertando a los analistas para que investiguen un posible intento de obtener datos y tomen las medidas necesarias.




Para obtener más información sobre el uso del marco Mitre ATT&CK para UEBA, consulte el tema **Usar el marco MITRE ATT&CK®** en la Guía de NetWitness Respond 12.5.

## Se agregó compatibilidad con JA4 en UEBA para mejorar la identificación de clientes y la detección de amenazas

NetWitness ha agregado soporte para la huella digital JA4 y es el valor predeterminado para UEBA a partir de la versión 12.5 o posterior. Este cambio se implementa porque JA4 se identifica como el método de identificación de clientes más confiable y avanzado. JA4 aprovecha los paquetes TLS Client Hello para identificar patrones de tráfico específicos de aplicaciones y crear huellas digitales únicas para cada aplicación. Esto reduce el número total de huellas digitales únicas para los navegadores modernos. Como resultado, un solo cliente tendrá solo una huella digital JA4 en lugar de varias, lo que hará más fácil su seguimiento y monitoreo. Esta mejora en UEBA con JA4 ayuda a identificar las huellas digitales de aplicaciones maliciosas y permite a los analistas identificar y mitigar de forma proactiva las amenazas ocultas dentro del tráfico cifrado.

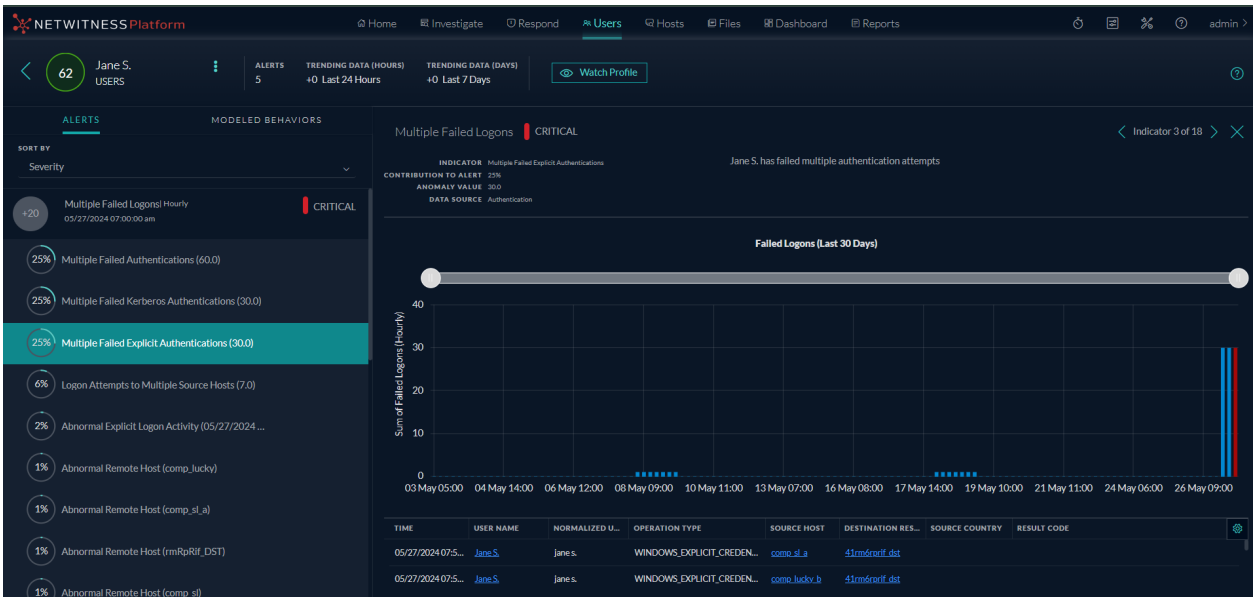


Para obtener más información sobre la compatibilidad con JA4, consulte la Guía del usuario de NetWitness UEBA para 12.5.

### UEBA mejorado para la detección de Kerberos y actividad de inicio de sesión explícita

NetWitness UEBA ha mejorado sus funcionalidades de detección de actividades de inicio de sesión al introducir dos nuevos indicadores y comportamientos modelados específicamente para el inicio de sesión **explícito** y en **Kerberos**. Esta mejora permite una diferenciación más precisa entre varios eventos de inicio de sesión dentro de su entorno, lo que reduce significativamente los falsos positivos y las inconsistencias relacionadas con actividades de inicio de sesión explícito y en Kerberos. Al separar estos tipos de inicio de sesión, los analistas pueden identificar con mayor eficacia comportamientos de inicio de sesión anormales y proteger su entorno de posibles amenazas. Estos nuevos indicadores brindan información más profunda sobre las actividades de inicio de sesión, lo que ayuda a los analistas a monitorear e investigar de manera eficaz cualquier comportamiento sospechoso o malicioso.

Por ejemplo, se puede activar una alerta de **Varios inicios de sesión fallidos** cuando se identifica una actividad anómala para varios intentos de autenticación fallidos tanto en la actividad de **Kerberos** como en la de **inicio de sesión explícito**.




Para obtener más información, consulte la sección **Indicadores de actividad de inicio de sesión** del tema **Casos de uso de NetWitness UEBA** en la Guía del usuario de NetWitness UEBA para 12.5.

## Funcionalidad SASE

La siguiente sección describe la nueva mejora para SASE:

### Integración de NetWitness SASE con Netskope (modo de vista previa privada)

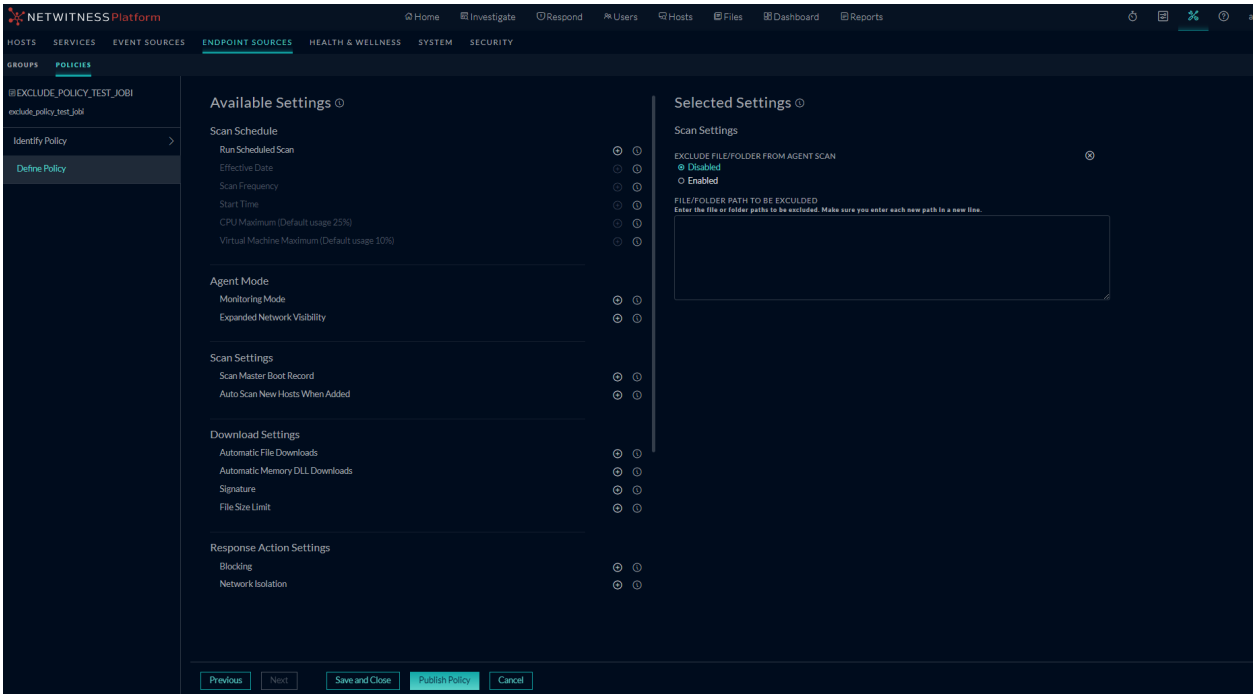
Presenta la integración de NetWitness con Netskope SASE para proporcionar visibilidad completa de la red y los registros. Con esta integración técnica personalizada, los usuarios de NetWitness obtienen información sobre el comportamiento y la comunicación entre dispositivos y servicios en redes remotas y distribuidas en implementaciones en las instalaciones, híbridas y en la nube. La integración NetWitness-Netskope SASE permite a los clientes aprovechar la flexibilidad de SASE y sus ventajas de seguridad inherentes, manteniendo al mismo tiempo una visibilidad completa para la detección y respuesta a amenazas. En la versión 12.5, la integración de NetWitness SASE con Netskope está en modo de vista previa privada.

## Endpoint

La siguiente sección describe las nuevas mejoras para el componente Endpoint

### Exclusión de archivos y carpetas específicos de los análisis completos del sistema del agente

Puede configurar la plataforma NetWitness para excluir archivos y carpetas específicos de los análisis completos del sistema de NetWitness Endpoint Agent. Cuando excluye archivos o carpetas, NetWitness Endpoint Agent los ignora cuando analiza en busca de riesgos de seguridad. Si excluye archivos y carpetas de gran tamaño, es posible que el tiempo de análisis de Endpoint Agent se reduzca. Excluir un archivo o carpeta de los análisis de NetWitness Endpoint Agent reduce el nivel de protección de los hosts en su red. Debe usarse solo si tiene una necesidad específica y está seguro de que los artículos no están infectados. Puede excluir archivos y carpetas únicamente de un análisis completo del sistema.



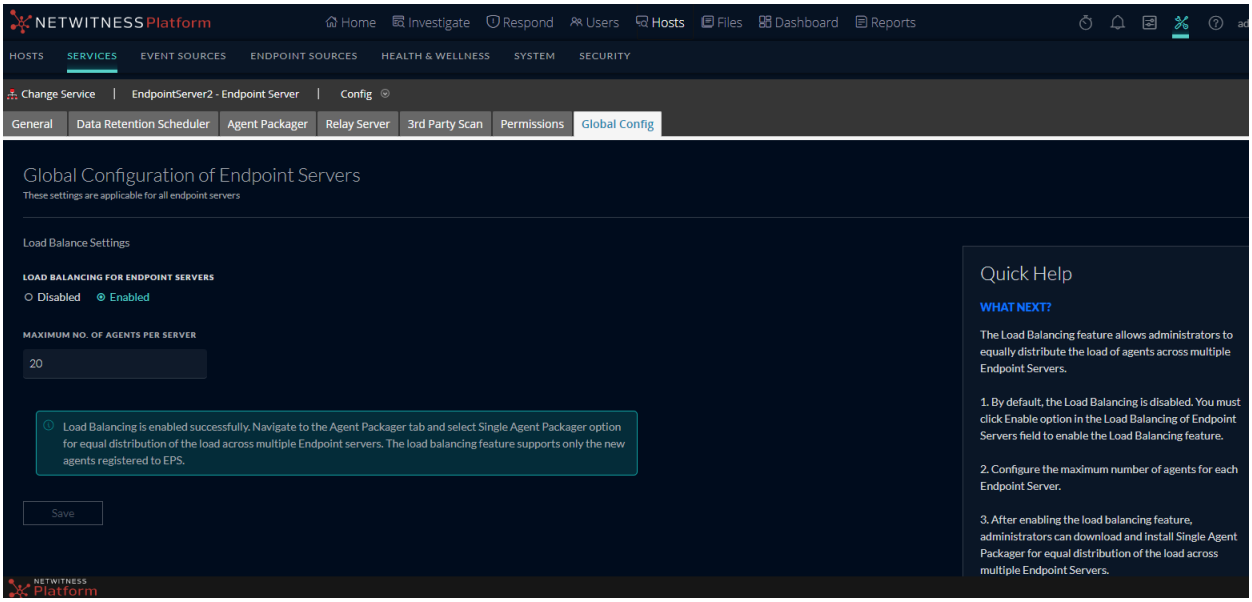

Para obtener más información sobre cómo excluir archivos y carpetas del análisis completo del sistema de NetWitness Agent, consulte la Guía de configuración de NetWitness Endpoint.

## Optimización del rendimiento: Funcionalidades de equilibrio de carga en servidores Endpoint

La función de equilibrio de carga recientemente introducida permite a los administradores distribuir las cargas de los agentes de manera equitativa entre los servidores de puntos finales del entorno.

Cuando las organizaciones se hacen más grandes, aumenta la necesidad de agregar nuevos agentes para las implementaciones, y la distribución de agentes entre servidores Endpoint se vuelve difícil. Los administradores deben descargar un empaquetador diferente para cada servidor de punto final y usar políticas para distribuir la carga según las condiciones. Al utilizar la función de equilibrio de carga, los clientes solo necesitan descargar un empaquetador de agente y enviarlo a todos los agentes de punto final. En función de la carga y los parámetros definidos, los agentes se distribuirán equitativamente entre los servidores Endpoint.

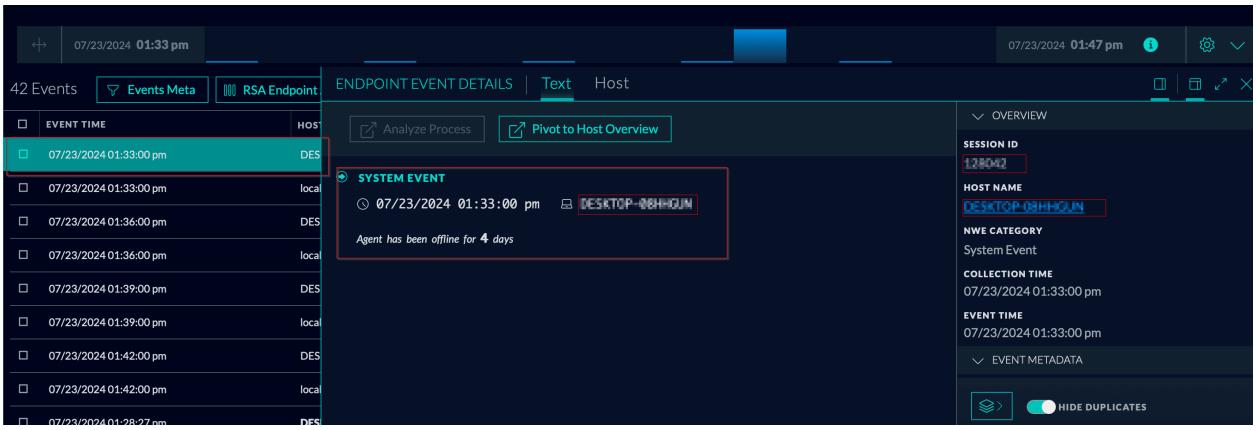
Al implementar el equilibrio de carga, las organizaciones pueden garantizar que su implementación escala de manera eficiente, lo cual reduce el riesgo de sobrecargar cualquier servidor de punto final y mantiene un rendimiento óptimo en toda la red. Para utilizar la capacidad de equilibrio de carga, debe habilitar el equilibrio de carga.




Para obtener más información sobre el equilibrio de carga, consulte los temas "Acerca del equilibrio de carga" y "Habilitar el equilibrio de carga" en la *Guía del usuario de NetWitness Endpoint.*

## Capacidad de monitorear los detalles de la última vez que se vieron los agentes de Endpoint

NetWitness Platform permite a los administradores y analistas crear periódicamente informes que detallan la cantidad de agentes de Endpoint que no han informado durante un intervalo de días especificado, lo que garantiza el cumplimiento y la gobernanza en la organización. Comprender cuándo el agente de Endpoint estuvo activo por última vez proporciona información sobre el rendimiento general de los dispositivos terminales. Monitorear el estado de la última vez que se vieron los agentes de Endpoint es crucial para garantizar la seguridad, el cumplimiento, la eficiencia operativa y la gestión eficaz de los recursos dentro de una organización.




Para obtener más información, consulte el tema "Monitorear los detalles de la última vez que se vieron los agentes de Endpoint" en la Guía del usuario de NetWitness Endpoint.

### Mejoras del sistema operativo compatible

Los administradores tienen la opción de implementar agentes de Endpoint en la siguiente versión del sistema operativo Windows:

- **Windows 11 (hasta la versión 23H2)**

Para obtener más información, consulte el tema **Introducción a la instalación de agentes de Endpoint** en la *Guía de instalación de agentes de NetWitness Endpoint*.

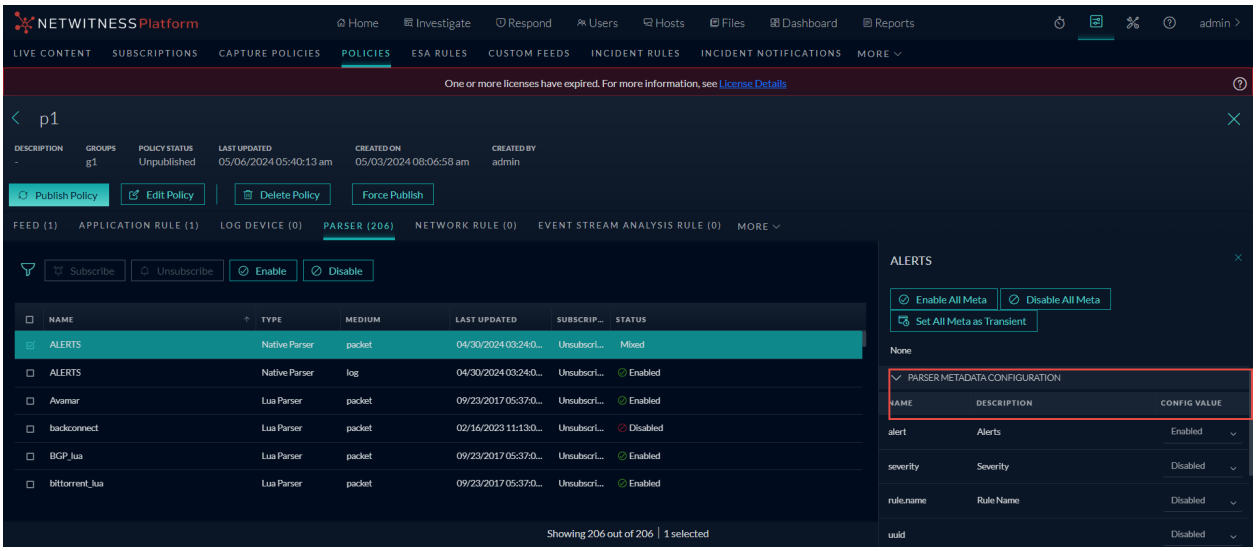
## Administración de contenido centralizada (CCM) basada en políticas

Se realizan las siguientes mejoras para CCM en la versión 12.5.0.0:

### Compatibilidad con analizadores nativos

#### Ver la configuración de metadatos del analizador

La vista **Detalles de política** > **Parser** se ha mejorado para ver la **Configuración de metadatos parser** en el panel lateral derecho que muestra todos los metadatos del parser seleccionado.

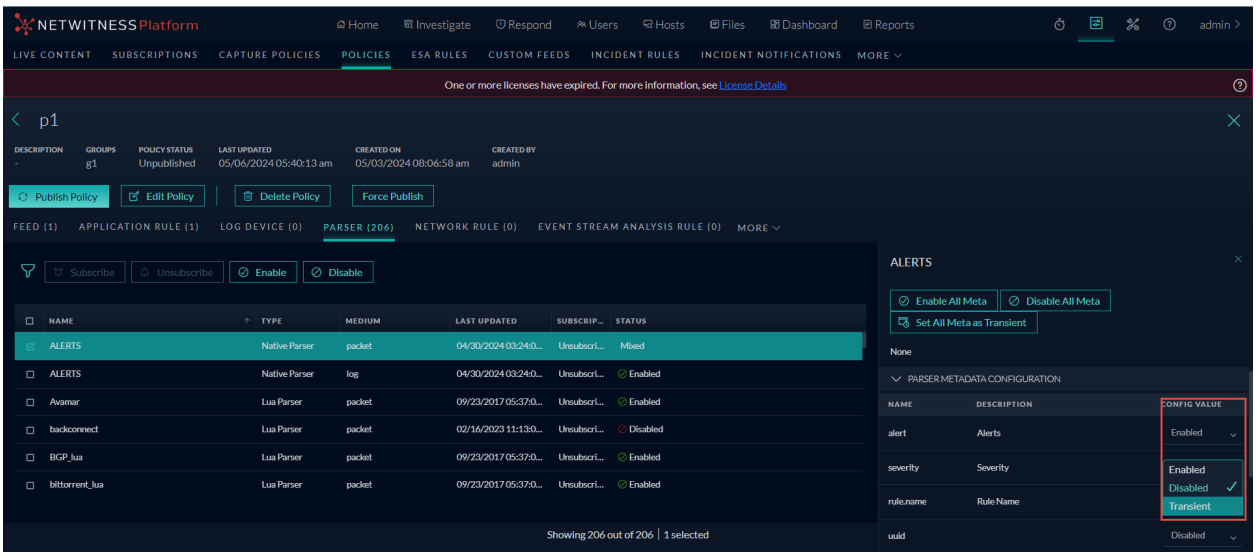


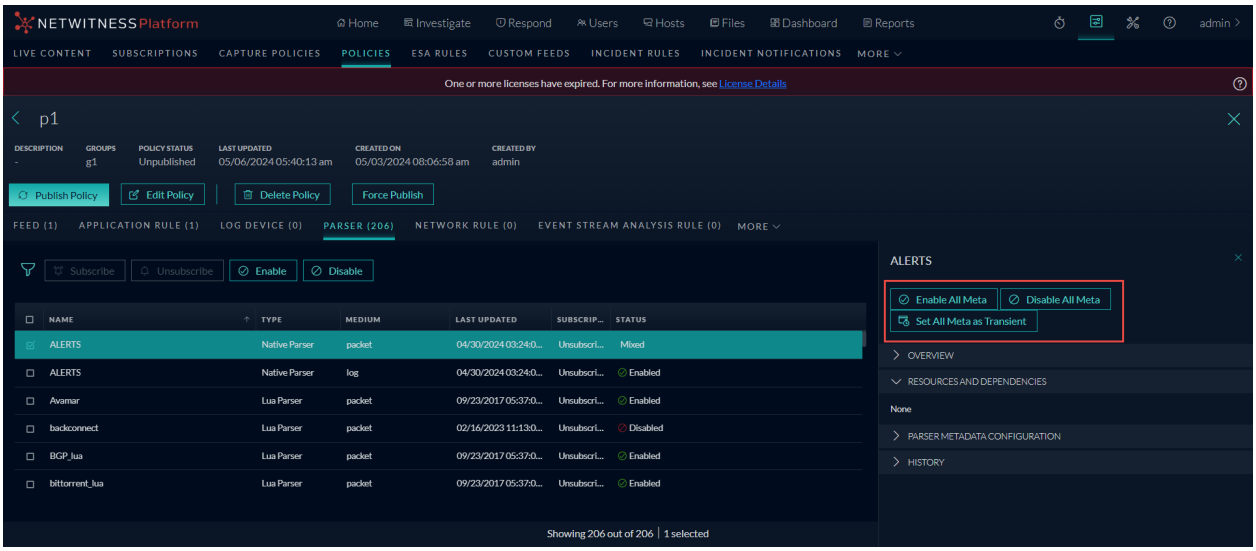

Para obtener más información, consulte el tema **Ver una política** en la *Guía de administración de contenido centralizada basada en políticas*.

### Habilitar o deshabilitar metadatos Parser

La vista **Detalles de política** > **Parser** se ha mejorado para habilitar o deshabilitar metadatos parser específicos, lo que le brinda la capacidad de decidir si desea utilizar parsers nativos o no. Puede:

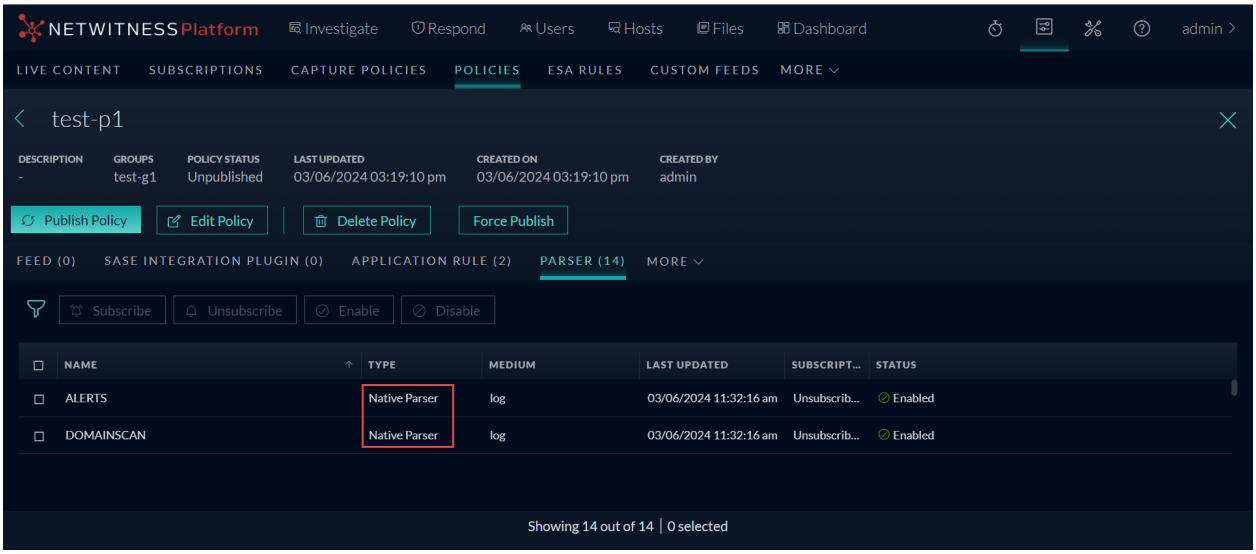
- Habilitar todos los metadatos
- Deshabilitar todos los metadatos
- Hacer que todos los metadatos sean transitorios
- Habilitar metadatos individuales
- Deshabilitar metadatos individuales
- Hacer que los metadatos individuales sean transitorios






### Ver Parsers nativos habilitados para servicios y asociados a una política

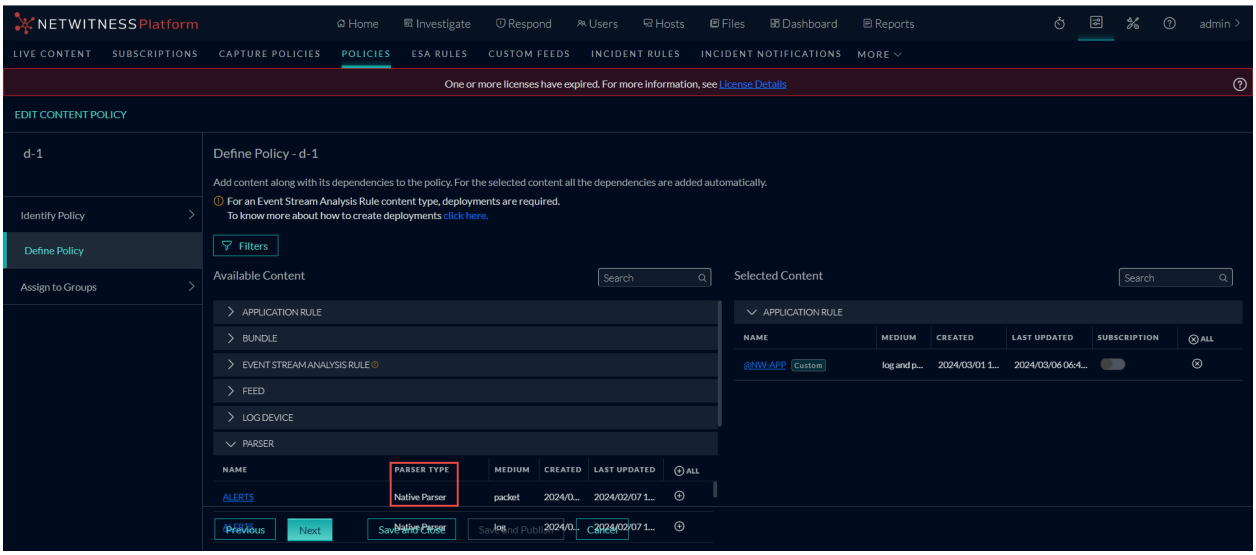
Puede ver fácilmente los Parsers nativos habilitados para servicios y asociados a una política, ya que se muestran automáticamente en la página **Detalles de política**.




Para obtener más información, consulte el tema **Ver una política** en la *Guía de administración de contenido centralizada basada en políticas*.

### Distinguir entre Parsers nativos y Parsers LUA al crear una política

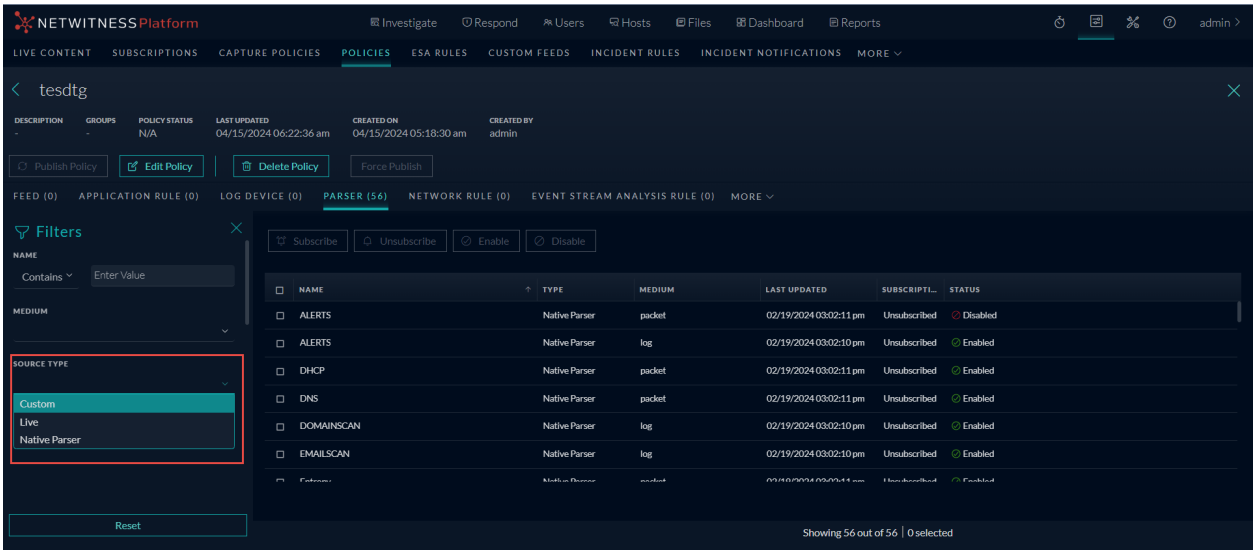
Se crea un identificador distinguible para un Parser nativo en la página **Crear política** o **Editar política** para ayudarlo a distinguir entre Parser nativo y Parser LUA al crear una política.




Para obtener más información, consulte el tema **Crear y publicar políticas** en la *Guía de administración de contenido centralizada basada en políticas*.

### Filtrar Parsers nativos

Puede filtrar los Parsers nativos en las páginas **Crear política**, **Editar política** y **Detalles de política**, lo que permite seleccionar o ver fácilmente los Parsers nativos necesarios para la política. Esto optimizará el proceso y le permitirá agregar o eliminar fácilmente Parsers nativos durante la creación o modificación de políticas.




Para obtener más información, consulte el tema **Crear y publicar políticas** en la *Guía de administración de contenido centralizada basada en políticas*.

## Servicios de Concentrator, Decoder, Log Collector y Archiver

Se realizan las siguientes mejoras para los servicios de Concentrator, Decoder, Log Collector y Archiver en la versión 12.5.0.0:

### Presentación de huellas digitales TLS JA4

JA4 identifica patrones de tráfico específicos de aplicaciones mediante el análisis de las negociaciones del protocolo de enlace TLS (Client Hello), mejorando así las funcionalidades de detección de amenazas de UEBA.

Para obtener más información, consulte el tema **Compatibilidad con la entidad JA4 para UEBA** en la *Guía de configuración de Decoder*.

### Fuentes de eventos de Logstash

Se introdujo el soporte del complemento NetWitness JDBC Logstash Input para recopilar registros de bases de datos MSSQL, IBMDB2 y Oracle.

Para obtener más información, consulte el tema **Configurar fuentes de eventos de Logstash en NetWitness** en la *Guía de recopilación de registros*.

### Extended Meta

Una configuración opcional para aumentar la longitud de los valores que se pueden almacenar en la base de datos de metadatos para proporcionar mayor precisión cuando se trata de ciertos casos de uso que requieren coincidencias de cadenas largas.

Extended Meta proporciona una forma de configurar selectivamente ciertas claves meta para admitir valores superiores a 256 bytes. Con esta característica, los valores de metadatos que antes estaban truncados por el límite de 256 bytes ahora se pueden ampliar hasta 4096 bytes de longitud.

Para obtener más información, consulte las Pautas de Extended Meta mencionadas en la *Guía del usuario de NetWitness Extended Meta para 12.5*.

### Seguimiento de reglas de aplicación

Cuenta la frecuencia con la que se cumple una regla de aplicación, así como la capacidad de restablecer el contador para solucionar problemas.

Para obtener más información, consulte la *Guía de API para 12.5*.

## Integraciones de registros

NetWitness Platform admite la integración de los siguientes orígenes de eventos para recopilar y analizar registros. A menos que se especifique lo contrario, estos servicios son compatibles con NetWitness Platform 12.2.0.0 o posterior.

- Amazon AWS CloudWatch
- Okta Workforce Identity Cloud

Para obtener más información sobre la integración de los servicios del analizador, consulte la Guía de integraciones de NetWitness Platform.

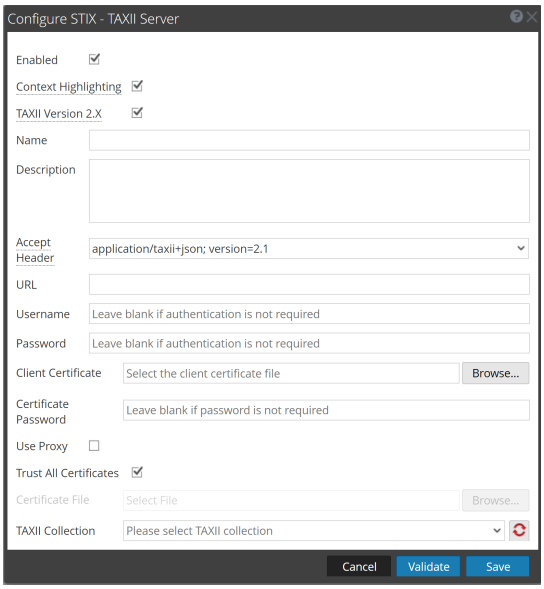
## Context Hub

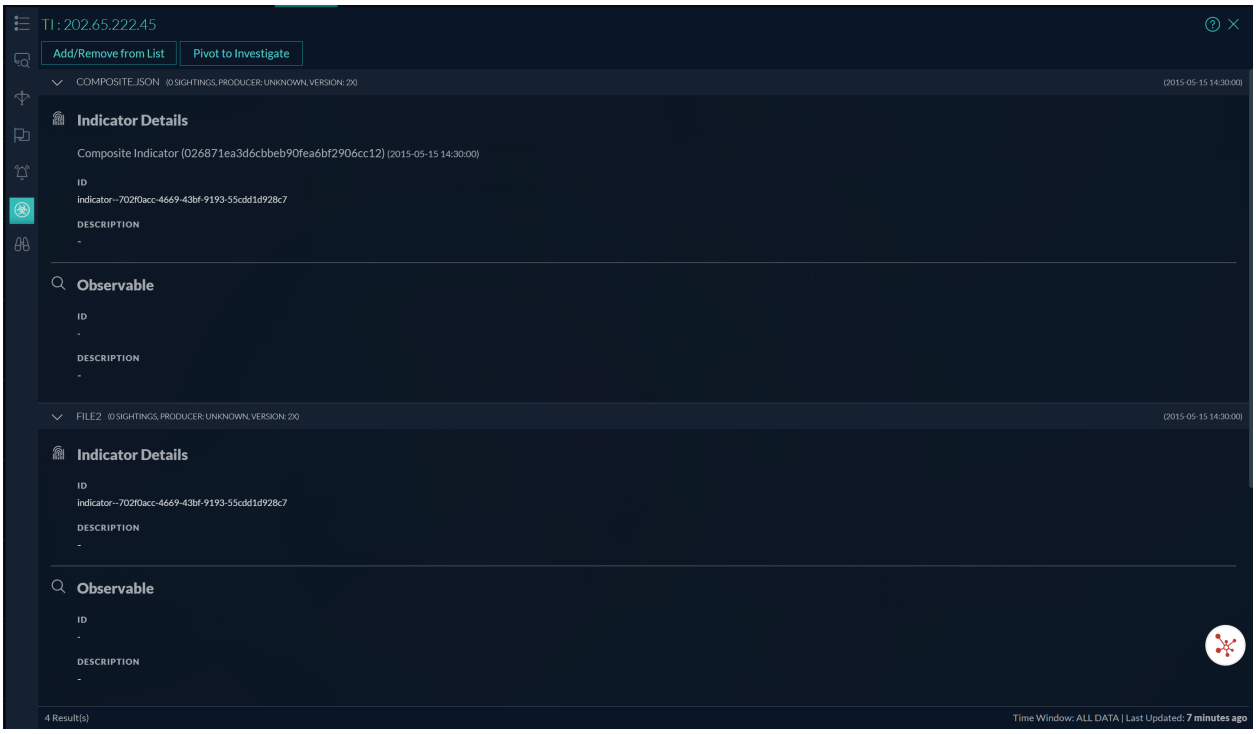
La siguiente sección describe las nuevas mejoras del componente Context Hub:

## Inteligencia de amenazas mejorada con la integración de STIX 2.x

NetWitness ha mejorado sus capacidades de detección de amenazas y monitoreo de seguridad al integrar soporte para feeds STIX 2.x, incluidas las versiones 2.0 y 2.1. Los administradores ahora pueden utilizar STIX 2.x (formato JSON) para configurar los servidores de archivos, REST y TAXII como indicadores de origen de datos para Context Hub. Esta mejora le permite crear feeds personalizados utilizando fuentes de datos STIX 2.x. NetWitness Platform analiza datos en segundo plano para extraer una valiosa inteligencia de amenazas e identificar patrones maliciosos, brindando un contexto enriquecido a través de la Búsqueda de contexto en las páginas **Investigate** y **Respond** y ayudando a los analistas a realizar investigaciones con mayor eficacia.

Esta mejora simplifica la utilización de inteligencia de amenazas estructurada al eliminar muchas restricciones anteriores, lo que permite informes más descriptivos y efectivos de los avistamientos. Esta integración implica la conversión de inteligencia de amenazas estructurada del formato STIX a un formato que el sistema SIEM puede entender y utilizar fácilmente, mejorando así su eficacia en la protección contra amenazas.






Para obtener más información, consulte el tema **Configurar STIX como origen de datos** en la Guía de configuración de Context Hub.

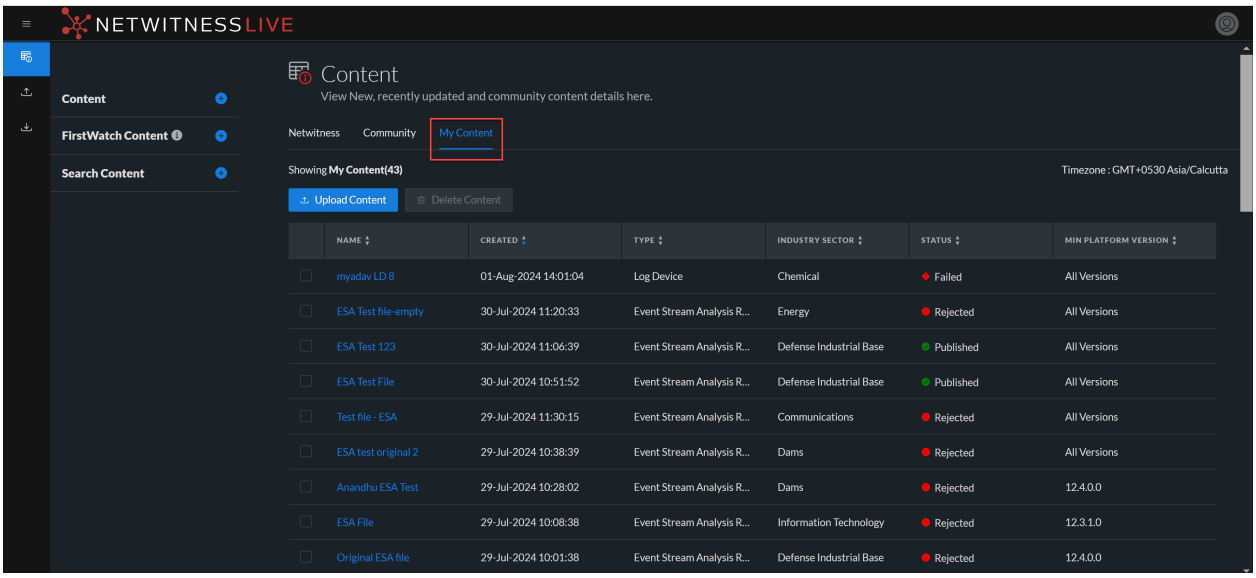
## Live Cloud Service

La siguiente sección describe las nuevas mejoras del componente Live Cloud Service:

### Administrar contenido personalizado de la comunidad en NetWitness Live

NetWitness presenta la nueva función Mi contenido, que permite a los usuarios administrar sin problemas contenido personalizado directamente desde la interfaz de usuario de NetWitness Live. Esto incluye cargar, eliminar y descargar contenido creado por el usuario, como dispositivos de registro, reglas de análisis de flujo de eventos, analizadores, feeds, etc. Esta función proporciona a los usuarios una forma más eficiente de compartir contenido personalizado útil y relevante entre usuarios, lo que reduce el tiempo y el esfuerzo necesarios para publicar contenido a través de equipos de publicación de contenido. Los usuarios pueden elegir entre una variedad de opciones de contenido que se adapten a sus necesidades y casos de uso.

**Nota:** La función Mi contenido de NetWitness Live solo admite contenidos de ESA y de dispositivos de registro en esta versión.




Para obtener más información, consulte el tema **Administrar contenido personalizado** en la Guía de administración de servicios de NetWitness Live.

## Actualizaciones de seguridad

Aborda las últimas vulnerabilidades de seguridad reportadas contra diversas bibliotecas que utiliza NetWitness Platform, incluidas una vulnerabilidad crítica (CVE-2016-1000027), 35 vulnerabilidades importantes, 103 moderadas y 16 vulnerabilidades menores.

Para obtener más información sobre correcciones de seguridad, consulte https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security.

## Rutas de actualización

Las siguientes rutas de actualización son compatibles con NetWitness Platform 12.5.0.0

- NetWitness 12.4.2.0 a 12.5.0.0
- NetWitness 12.4.1.0 a 12.5.0.0
- NetWitness 12.4.0.0 a 12.5.0.0
- NetWitness 12.3.1.0 a 12.5.0.0
- NetWitness 12.3.0.0 a 12.5.0.0
- NetWitness 12.2.0.1 a 12.5.0.0
- NetWitness 12.2.0.0 a 12.5.0.0

Para obtener más información sobre la actualización a 12.5.0.0, consulte la Guía de actualización para NetWitness 12.5.0.0

**IMPORTANTE:** NetWitness recomienda a los usuarios que comprueben las versiones de su software y señala que las versiones hasta la 12.2 alcanzaron el final del ciclo de vida (EOL) a partir del 31 de marzo de 2024. Para obtener más información, consulte https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. Para aprovechar las últimas funciones y actualizaciones de seguridad, NetWitness recomienda actualizar a la versión 12.5.

**IMPORTANTE:** Si desea actualizar desde las versiones 11.7.x u 11.7.xx a la versión 12.5.0.0, primero debe actualizar a la versión 12.2.0.0 o 12.3.0.0 antes de actualizar a 12.5.

**IMPORTANTE:** Warehouse Connector utiliza una caja de seguridad para almacenar credenciales de forma segura para orígenes y destinos de integración de datos. Sin embargo, los usuarios que actualicen desde versiones anteriores a la versión 12.5 no podrán iniciar los flujos configurados sin migrar sus credenciales existentes en la nueva caja de seguridad. Como resultado, los usuarios deben crear manualmente una nueva clave de caja de seguridad y luego actualizar la contraseña para sus orígenes y destinos configurados en Warehouse Connector, cuando corresponda. Para obtener instrucciones detalladas sobre cómo crear la nueva clave de caja de seguridad, consulte la sección **Warehouse Connector** en las **Tareas posteriores a la actualización** de la Guía de actualización para NetWitness 12.5.0.0.

## Ciclo de vida del producto de NetWitness Platform

Consulte el Ciclo de vida de la versión del producto para NetWitness Platform para conocer una lista de versiones que alcanzan el fin del soporte primario (EOPS).

# Novedades de versiones anteriores

La sección proporciona nuevas funciones y mejoras para todas las versiones anteriores compatibles.

Para obtener más información, consulte https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-12-x/ta-p/695650.

# Problemas resueltos en la versión 12.5.0.0

Esta sección enumera los problemas resueltos en la versión 12.5.0.0.

Para obtener información adicional sobre problemas resueltos, consulte la columna Versión reparada en la lista de problemas conocidos de NetWitness® Platform (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) en el portal de NetWitness Community.

## Reparaciones en Endpoint

| Número de rastreo | Descripción |
|---|---|
| SACE-21629 | El tiempo de espera del mecanismo de sondeo del servidor de Endpoint no se agotó según lo previsto al verificar la línea de espera de mensajes del servidor de retransmisión, debido a un límite de tiempo de espera excesivo. |

## Correcciones de la página de inicio

| Número de rastreo | Descripción |
|---|---|
| ASOC-148336 | Los usuarios ahora pueden seleccionar "Página de inicio" como su página de destino predeterminada en la opción de configuración de Preferencias de usuario sin encontrarse con una pantalla en blanco. |

## Reparaciones en la plataforma

| Número de rastreo | Descripción |
|---|---|
| ASOC-146908 | Durante la actualización, el host no puede iniciarse en el kernel el8 una vez completada la migración del sistema operativo. |

## Correcciones del decodificador

| Número de rastreo | Descripción |
|---|---|
| ASOC-147188 | Al ejecutar el comando Prune opcional como parte de la migración de DPDK, se muestran mensajes de falla continuos relacionados con algunas interfaces de los registros. |
| ASOC-144467 | Al volver a cargar el plug-in alojado, la instancia del plug-in se elimina en lugar de volver a cargarse desde el árbol decodificador/alojado. |
| ASOC-154781 | La actualización del decodificador a 12.4.x eventualmente llena la partición /var/netwitness/decoder con datos de parsestatdb. |

# Problemas conocidos en la versión 12.5.0.0

Los problemas que siguen sin resolverse en esta versión están documentados en la lista de problemas conocidos de NetWitness® Platform en el portal de la comunidad de NetWitness: https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

# Números de compilación para componentes 12.5.0.0

En la siguiente tabla se muestran los números de compilación de los diversos componentes de NetWitness 12.5.0.0.

| Componente | Número de versión |
|---|---|
| NetWitness Servidor de administración | rsa-nw-admin-server-12.5.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm |
| NetWitness Contenido de análisis avanzado | rsa-nw-advanced-analytics-content-12.5.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm |
| NetWitness Servidor de análisis avanzado | rsa-nw-advanced-analytics-server-12.5.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm |
| NetWitness Appliance | rsa-nw-appliance-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Archiver | rsa-nw-archiver-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Complemento de auditoría | rsa-audit-plugins-12.5.0.0-4892.5.9d0750b41.el8.noarch.rpm |
| NetWitness RT de auditoría | rsa-audit-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm |
| NetWitness Bootstrap | rsa-nw-bootstrap-12.5.0.0-2401240926.5.a3d68ef.el8.noarch.rpm |
| NetWitness Broker | rsa-nw-broker-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Carlos RT | rsa-carlos-rt-12.5.0.0-2787.5.721a8daa7.el7.x86_64.rpm |
| NetWitness Nube | rsa-nw-cloud-12.5.0.0-12867.5.957818c84.el8.x86_64.rpm |
| NetWitness Servidor de Cloud Connector | rsa-nw-cloud-connector-server-12.5.0.0-240116135943.5.4220688.el8.alma.noarch.rpm |
| NetWitness Servidor de enlace de la nube | rsa-nw-cloud-link-server-12.5.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm |
| NetWitness Collectd | rsa-collectd-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm |
| NetWitness Collectd SMS | rsa-collectd-sms-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm |
| NetWitness Descripción del componente | Descriptor de componentes rsa-nw-12.5.0.0-2402280945.5.4c3391a.el8.noarch.rpm |
| NetWitness Concentrator | rsa-nw-concentrator-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |

| | |
|---|---|
| NetWitness Gestión de configuración | rsa-nw-config-management-12.5.0.0-2402050947.5.b7e9f64.el8.noarch.rpm |
| NetWitness Servidor de Config | rsa-nw-config-server-12.5.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm |
| NetWitness Consola | rsa-nw-console-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Servidor de contenido | rsa-nw-content-server-12.5.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm |
| NetWitness Servidor de Context Hub | rsa-nw-contexthub-server-12.5.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm |
| NetWitness Servidor de correlación (ESA) | rsa-nw-correlación-server-12.5.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm |
| NetWitness Contenido de Dashboard | rsa-nw-dashboard-content-20231220155210-5.noarch.rpm |
| NetWitness Decoder | rsa-nw-decoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Contenido analítico de Decoder | rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm |
| NetWitness Contenido de Decoder | rsa-nw-decodercontent-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Actualización de implementación | rsa-nw-deployment-upgrade-12.5.0.0-2402150604.5.dbd95e3.el8.noarch.rpm |
| NetWitness Agentes de Endpoint | rsa-nw-endpoint-agents-12.5.0.0-2402061657.5.db93b9a.el8.x86_64.rpm |
| NetWitness Servidor de Endpoint Broker | rsa-nw-endpoint-broker-server-12.5.0.0-240103053136.5.8430874.el8.alma.noarch.rpm |
| NetWitness Contenido analítico de Endpoint Decoder | rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm |
| NetWitness Servidor de terminal | rsa-nw-endpoint-server-12.5.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm |
| NetWitness Empresa Esper | rsa-nw-esper-enterprise-12.5.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm |
| NetWitness Servidor de integración | rsa-nw-integration-server-12.5.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm |
| NetWitness Servidor de Investigate | rsa-nw-investigate-server-12.5.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm |
| NetWitness Servidor web heredado | rsa-nw-legacy-web-server-12.5.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm |
| NetWitness Servidor de licencias | rsa-nw-license-server-12.5.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm |

| | |
|---|---|
| NetWitness Log Collector | rsa-nw-logcollector-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm |
| NetWitness Contenido de Log Collector | rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm |
| NetWitness Perl de Log Collector | rsa-nw-logcollector-perl-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm |
| NetWitness Herramientas de Log Collector | rsa-nw-logcollector-tools-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm |
| NetWitness Log Decoder | rsa-nw-logdecoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Contenido analítico de Log Decoder | rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm |
| NetWitness Contenido base de Log Decoder | rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm |
| NetWitness Log Player | rsa-nw-logplayer-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm |
| NetWitness Servidor de Malware Analytics | rsa-nw-malware-analytics-server-12.5.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm |
| NetWitness Utilidad de exportación de metadatos | rsa-nw-metaexport-utility-12.5.0.0-110124.5.el8.x86_64.rpm |
| NetWitness Servidor de métricas | rsa-nw-metrics-server-12.5.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm |
| NetWitness Servidor de infraestructura de nodo | rsa-nw-node-infra-server-12.5.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm |
| NetWitness Interfaz de línea de comandos (CLI) de organización | rsa-nw-orchestration-cli-12.5.0.0-2401091103.5.7317baa.el8.noarch.rpm |
| NetWitness Servidor de Orchestration | rsa-nw-orchestration-server-12.5.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm |
| NetWitness Marcador de posición | rsa-nw-placeholder-12.5.0.0-2310040926.5.cebd204.el8.noarch.rpm |
| NetWitness Flujo de aire Presidio | rsa-nw-presidio-airflow-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness Servidor de configuración de Presidio | rsa-nw-presidio-configserver-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness Núcleo del Presidio | rsa-nw-presidio-core-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness Inicio de búsqueda elástica de Presidio | rsa-nw-presidio-elasticsearch-init-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness Presidio Ext NetWitness | rsa-nw-presidio-ext-netwitness-12.5.0.0-2401151152.5.18bd06b.el8.noarch.rpm |

| | |
|---|---|
| NetWitness Gerente de Presidio | rsa-nw-presidio-manager-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness Salida de Presidio | rsa-nw-presidio-output-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm |
| NetWitness UI de Presidio | rsa-nw-presidio-ui-12.5.0.0-2402270745.5.0844250.el8.noarch.rpm |
| NetWitness Protobufs | rsa-protobufs-rt-12.5.0.0-928.5.6254aabd8.el8.x86_64.rpm |
| NetWitness Herramientas de recuperación | rsa-nw-recovery-tool-12.5.0.0-2401230435.5.f34a9fd.el8.noarch.rpm |
| NetWitness Servidor de retransmisión | rsa-nw-relay-server-12.5.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm |
| NetWitness Servidor de Reporting Engine | rsa-nw-re-server-12.5.0.0-5996.5.b76234be4.el8.x86_64.rpm |
| NetWitness Servidor de Respond | rsa-nw-respond-server-12.5.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm |
| NetWitness Servidor de acciones de respuesta | rsa-nw-respuesta-acciones-serv-12.5.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm |
| NetWitness Actualización de CA raíz | rsa-nw-root-ca-update-12.5.0.0-2401221231.5.96cd15b.el8.noarch.rpm |
| NetWitness Herramientas SA | rsa-sa-tools-12.5.0.0-2401251338.5.89600eb.el8.noarch.rpm |
| NetWitness CLI de seguridad | rsa-nw-security-cli-12.5.0.0-2401091103.5.18ab320.el8.noarch.rpm |
| NetWitness Servidor de seguridad | rsa-nw-security-server-12.5.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm |
| NetWitness Shell | rsa-nw-shell-12.5.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm |
| NetWitness Complementos de informes SOS | rsa-nw-sosreport-plugins-12.5.0.0-2401162235.5.af21a76.el8.noarch.rpm |
| NetWitness Tiempo de ejecución (RT) de SMS | rsa-sms-runtime-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm |
| NetWitness Servidor de SMS | rsa-sms-server-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm |
| NetWitness Servidor de origen | rsa-nw-source-server-12.5.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm |
| NetWitness Contenido del servidor de origen | rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm |
| NetWitness Interfaz de usuario | rsa-nw-ui-12.5.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm |

| | |
|---|---|
| NetWitness Workbench | rsa-nw-workbench-12.4.5.0-12866.5.1aefe557c.el8.x86_64.rpm |

# Cómo obtener ayuda con NetWitness Platform

## Documentación del producto

Con esta versión se proporciona la siguiente documentación.

| Documentación | Dirección URL de ubicación |
|---|---|
| Tabla de contenidos principal de NetWitness Platform | https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation |
| Documentación de producto de NetWitness Platform 12.5.0.0 | https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation |
| Guía de actualización de NetWitness Platform 12.5.0.0 | https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308 |
| Análisis de NetWitness en la nube | Para obtener más información sobre las nuevas funciones y mejoras en las versiones de NetWitness Analytics on Cloud, consulte la siguiente sección Novedades:<br>Para UEBA Cloud, consulte https://docs.netwitness.com/netwitnessueba/release_information/whats_new/.<br>Para obtener información, consulte https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/. |

## Recursos de autoayuda

Hay varias opciones que le brindan ayuda según la necesite para instalar y usar NetWitness:

- Consulte la documentación para conocer todos los aspectos de NetWitness aquí: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Utilice los campos **Buscar** y **Crear una publicación** en el portal de NetWitness Community para buscar información específica aquí: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- Ver la NetWitness base de conocimientos: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- consulte la sección Solución de problemas en las guías.

- Consulte también Publicaciones del blog de NetWitness® Platform.
- Si necesita más ayuda, póngase en contacto con el servicio de soporte de NetWitness.

## Comuníquese con Soporte de NetWitness

Si se comunica con el soporte de NetWitness, debe encontrarse en su computadora. Prepárese para proporcionar la siguiente información:

- Número de versión de la aplicación o el producto NetWitness Platform que está usando.
- El tipo de hardware que está usando.

Use la siguiente información de contacto si tiene preguntas o necesita ayuda.

| | |
|---|---|
| Portal de NetWitness Community | https://community.netwitness.com<br>En el menú principal, haga clic en **Soporte > Portal de casos > Ver mis casos**. |
| Contactos internacionales (cómo comunicarse con soporte de NetWitness) | https://community.netwitness.com/t5/support/ct-p/support |
| Comunidad | https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions |
| Actualización de NW | https://update.netwitness.com/ |
| UI de Live | https://live.netwitness.com |

## Servicios educativos de NetWitness

Regístrese para acceder a los cursos de NetWitness y a recursos adicionales en los servicios educativos y de capacitación de NetWitness.

| | |
|---|---|
| Portal educativo de NetWitness | https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog |
| Catálogo de cursos de servicios educativos de NetWitness | https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training |
| Programa de capacitación de servicios educativos de NetWitness | https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826 |
| Contacto de soporte de servicios educativos de NetWitness | education.support@netwitness.com |

# Comentarios sobre la documentación del producto

Puede enviar un correo electrónico a feedbacknwdocs@netwitness.com para proporcionar comentarios sobre la documentación de NetWitness Platform.