RSA NETWITNESS® PLATFORM

Guía del usuario de NetWitness Investigate

para la versión 11.2

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de Dell, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el 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 Dell.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. 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 RSA Link. 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 regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

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

febrero 2019

Contenido

Cómo funciona NetWitness Investigate

NetWitness Investigate ofrece funcionalidades de análisis de datos en RSA NetWitness® Platform de modo que los analistas puedan analizar datos de paquetes, registros y terminales, e identificar posibles amenazas internas o externas a la seguridad y la infraestructura de IP.

Nota: En la versión 11.1 y superior, las vistas Hosts y Archivos proporcionan una vista de los datos de terminales. Las versiones anteriores ofrecen acceso a datos de terminales mediante un servidor de NetWitness Endpoint independiente.

Metadatos, claves de metadatos, valores de metadatos y entidades de metadatos

RSA NetWitness Platform audita y monitorea todo el tráfico de una red. Un tipo de servicio, un Decoder, recopila, analiza y almacena los paquetes, los registros y los datos de terminales que recorren la red.

Los analizadores y los feeds configurados en el Decoder crean *metadatos* que los analistas pueden usar para investigar los registros y los paquetes recopilados. Otro tipo de servicio, denominado un Concentrator, indexa y almacena los metadatos.

Los metadatos tienen el formato de una *clave de metadatos* y *valores de metadatos* para la clave. Por ejemplo, `ip.src` es una clave de metadatos y una dirección IP que es el origen del tráfico está etiquetada como `ip.src`. Al ver los datos en Investigate, verá la clave de metadatos `ip.src` y todas las direcciones IP (valores) que están etiquetadas con esa clave. Algunas claves de metadatos están incorporadas y otras pueden ser claves personalizadas que define el administrador.

Las entidades de metadatos están disponibles en la versión 11.1 y superior. Una *entidad de metadatos* es un alias que agrupa los resultados de otras claves de metadatos. Las entidades de metadatos organizan claves de metadatos similares en un único tipo de metadatos que es más fácil de usar. Algunas entidades de metadatos ya se incluyen de manera predeterminada, y el administrador puede crear entidades de metadatos personalizadas. Los analistas pueden usar una entidad de metadatos en una consulta, un grupo de metadatos, un grupo de columnas y un perfil. Las visualizaciones de coordenadas paralelas no son compatibles con las entidades de metadatos. Los administradores pueden usar entidades de metadatos para definir un prefijo de consulta que se aplica a una función de usuario y un usuario. En la *Guía de configuración de Decoder* se proporciona información adicional sobre la creación de entidades de metadatos y cómo se pueden utilizar en reglas.

Por ejemplo, el idioma predeterminado de la base de datos de Core incluye claves de metadatos distintas para el origen y el destino de IP. Una de las entidades de metadatos incorporadas, denominada `ip.all`, representa el conjunto combinado de todos los orígenes y los destinos de IP.

Por lo general, los analistas consultan al Concentrator para descubrir las amenazas. El Concentrator maneja las consultas, las cuales solo se dirigen al Decoder cuando se requiere una reconstrucción completa de sesiones o registros crudos. ESA, Malware Analysis y Reporting Engine también consultan al Concentrator, donde pueden obtener rápidamente todos los metadatos pertinentes asociados a un evento y generar información sobre este sin tener que dirigirse a cada Decoder. En algunos casos especiales, los analistas pueden consultar a un Decoder.

Nota: Aunque un dispositivo híbrido puede desempeñar la función del Concentrator, cualquier ambiente grande que necesite un mayor nivel de ancho de banda o de eventos por segundo (EPS) requiere un dispositivo Concentrator por separado. El dispositivo Concentrator cuenta con diseño de almacenamiento que usa unidades de estado sólido para el índice, lo cual aumenta el rendimiento de lectura.

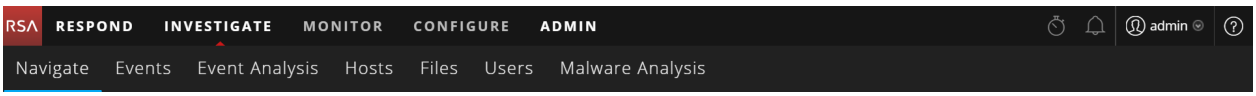
Desencadenantes de una investigación

Estos son algunos ejemplos de desencadenantes de una investigación:

- Usted recibe inteligencia de un tercero acerca de un nuevo hackeo de Active Directory. A partir de la vista Eventos, usa esa inteligencia para ejecutar una búsqueda en todos los datos del registro crudos de Active Directory en las últimas 24 horas.
- El administrador del SOC le solicita que busque el malware Pokemon Go debido a su popularidad actual. A partir de la vista Navegar, usted crea una consulta para buscar una sesión de HTTP que usa un agente de usuario específico relacionado con el malware que él encontró en un blog de seguridad.
- Un encargado de respuesta ante incidentes eleva un vale que muestra algunos indicadores extraños relacionados con un host. A partir de la vista Hosts, usted examina ese host para obtener detalles específicos.
- Está buscando el siguiente ataque de día cero y comienza por analizar los metadatos de red en la vista Navegar para encontrar sesiones automatizadas anormales que salen de la empresa.
- El administrador del SOC le solicita que busque información relacionada con el usuario `jarvis`, un empleado que se acaba de ir. A partir de la vista Hosts, usted consulta ese nombre de usuario en el transcurso de la semana pasada.

Flujo de trabajo de una investigación

Los analistas pueden investigar datos que captura NetWitness Platform y realizar análisis en profundidad a partir de información en un tablero de NetWitness Platform, un incidente o una alerta de NetWitness Respond, un informe que crea NetWitness Platform Reporting Engine o una aplicación de otros fabricantes. Durante el transcurso de una investigación, los analistas pueden desplazarse sin inconvenientes entre las vistas de Investigation: la vista Navegar, la vista Eventos, la vista Análisis de eventos, la vista Hosts, la vista Archivos, la vista Usuarios y la vista Malware Analysis. En esta figura se ilustran los submenús de NetWitness Investigate.



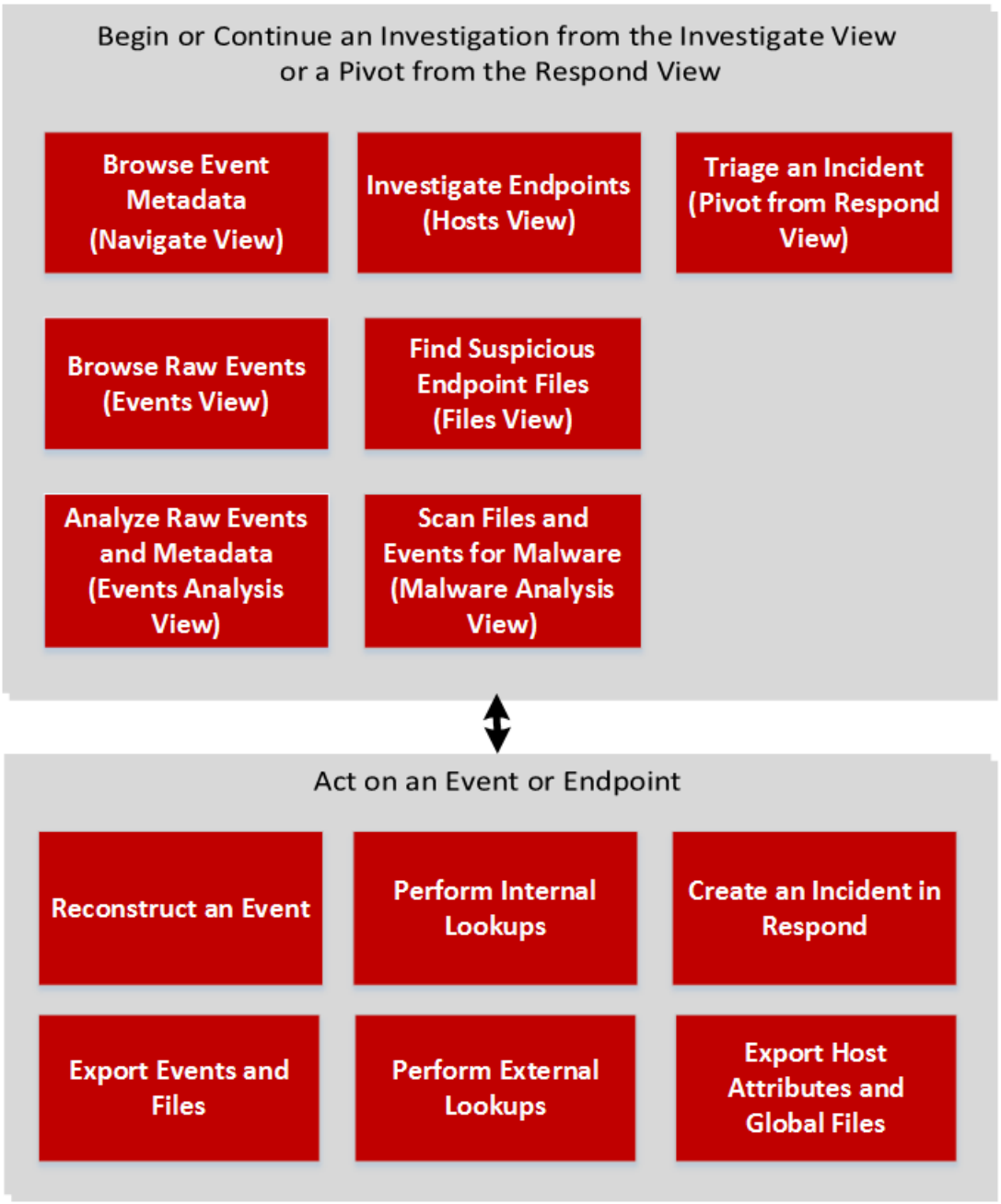
Nota: Las vistas Archivos y Hosts están disponibles en la versión 11.1 y superior. La vista Usuarios está disponible en la versión 11.2 y superior. Se requieren funciones y permisos de usuario específicos para que un usuario realice investigaciones y análisis de malware en NetWitness Platform. Si no puede realizar una tarea de análisis o abrir una vista, es posible que el administrador necesite ajustar las funciones y los permisos configurados para usted.

Puede acceder a cada vista desde el submenú de Investigate y desde otras vistas de Investigate. También puede ir directamente a una vista de Investigate desde NetWitness Respond y pasar directamente desde NetWitness Investigate a NetWitness Respond y a NetWitness Endpoint independiente. Su caso de uso determina el punto de partida de su investigación. En esta tabla se proporciona orientación general acerca de la vista inicial para distintos casos de uso.

Vaya a…	Enfoque
Vista Navegar	Todas las claves y los valores de metadatos para registros, terminales y paquetes se agrupan por clave de metadatos. Puede recorrer los datos para limitar los resultados, ir después a las vistas Eventos o Análisis de eventos, o buscar en Malware Analysis o Live. Esta es la vista predeterminada de NetWitness Investigate. (Consulte Investigación de metadatos en la vista Navegar).
Vista Eventos	Los eventos enumerados se ordenan por hora. Puede ver el evento crudo y los metadatos relacionados, ver una reconstrucción y descargar eventos y archivos. Puede ir a la vista Análisis de eventos. (Consulte Análisis de eventos crudos en la vista Eventos).
Vista Análisis de eventos	Los eventos enumerados se ordenan por hora. Puede ver todas las claves y los valores de metadatos para registros, terminales y paquetes. Puede ver el evento crudo y los metadatos relacionados y ver una reconstrucción que ofrece indicaciones útiles para identificar puntos de interés en una reconstrucción. Puede ir a la vista Hosts, cambiar a Endpoint independiente, buscar en Live y realizar búsquedas externas. Las búsquedas externas le permiten buscar en Internet valores de metadatos con los que interactuó, determinar información de DNS pasivo relacionada con una dirección IP, verificar si una dirección URL está en una lista negra y otras integraciones de contexto de terceros. (Consulte Análisis de eventos crudos y metadatos en la vista Análisis de eventos).Análisis de eventos crudos y metadatos en la vista Análisis de eventos
(Versión 11.1 y superior) Vista Hosts	Se enumeran los hosts en los cuales se ejecutan los agentes de NetWitness Endpoint Insights. Para cada host, puede ver los procesos, los controladores, los archivos DLL, los archivos (ejecutables), los servicios y las ejecuciones automáticas que se ejecutan, así como la información relacionada con los usuarios que iniciaron sesión. Desde la vista Hosts, puede ir a las vistas Navegar y Análisis de eventos. (Consulte Investigar los hosts).
(Versión 11.1 y superior) Vista Archivos	Se enumeran archivos, como PE, Macho y ELF, que son únicos en la implementación. Para cada archivo, puede ver detalles como el tamaño de archivo, la entropía, el formato, el nombre de la empresa, la firma y la suma de comprobación. Desde la vista **Archivos**, puede ir a las vistas Navegar y Análisis de eventos. (Consulte Investigar los archivos)
Vista Malware Analysis	Si está ejecutando un dispositivo Malware Analysis, puede escanear los archivos de manera manual o automática y ver los resultados de cuatro tipos de análisis: red, estático, comunidad y sandbox. Si un archivo es malware, puede ir a la vista Hosts para ver qué hosts descargaron el archivo. (Consulte Realización de un análisis de malware

Vaya a…	Enfoque
(Versión 11.2 y superior) Vista Usuarios	NetWitness UEBA proporciona visibilidad de comportamientos riesgosos de los usuarios en toda la empresa. Puede ver una lista de usuarios de alto riesgo y un resumen de las alertas principales para el comportamiento riesgoso en el ambiente y, a continuación, seleccionar un usuario o una alerta y ver detalles sobre el comportamiento riesgoso y la cronología en que este se produjo. Los usuarios de NetWitness Platform asignados a la función Administradores o Analistas de UEBA tienen acceso a esta vista. Para obtener información sobre esta característica, consulte la *Guía del usuario de NetWitness UEBA*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Cada situación es única en términos de los tipos de información que el analista intenta encontrar. Muchas de las investigaciones comienzan en una vista y terminan en otra a medida que el analista aprende algo y, a continuación, debe seguir ese resultado hacia otra línea de indagación. En esta figura se muestra el flujo de trabajo general de una investigación.



Enfoque en los metadatos, la consulta y el tiempo

Los analistas usan NetWitness Investigate para buscar eventos que impulsen el flujo de trabajo de respuesta ante incidentes y para realizar análisis estratégico después de que otra herramienta ha generado un evento. Comienzo en las vistas Navegar, Eventos o Análisis de eventos:

- Lo primero es ejecutar una consulta en un servicio para un rango de tiempo específico y, a continuación, filtrar mediante metadatos a un subconjunto de eventos, reconstruir o analizar un evento y repetir el proceso para reconstruir o analizar otro evento.
- Cuando encuentra un evento que presenta un examen más detallado, usted observa el contexto en torno al evento y decide si desea crear un incidente o agregar el evento a un incidente. Si decide no agregar el evento a un incidente, debe ejecutar otra consulta para obtener más información valiosa, con lo cual se vuelve a comenzar al principio del flujo de trabajo.
- Si observa actividad o archivos sospechosos en un host específico en la red, puede recopilar información adicional sobre el host y los archivos que se encuentran en el host en las vistas Hosts y Archivos o en un servidor de NetWitness Endpoint independiente.
- Si encuentra un archivo o un evento que posiblemente contiene malware, puede realizar un escaneo de Malware Analysis del archivo o puede abrir Malware Analysis e iniciar un escaneo del servicio en el cual se observó el evento.

Por ejemplo, si hay alguna preocupación respecto de tráfico sospechoso con otros países, la clave de metadatos País de destino revela todos los destinos y la frecuencia del contacto. El desglose a estos valores genera los datos específicos del tráfico, como la dirección IP del originador y el destinatario. La comprobación de otros metadatos puede exponer la naturaleza los archivos adjuntos intercambiados entre las dos direcciones IP.

Enfoque en el análisis de terminales

Los analistas usan las vistas Hosts y Archivos para investigar o realizar un análisis de los hosts o los archivos mediante atributos, como dirección IP, nombre de host, dirección Mac, etc.

- Durante un triage de incidentes en la vista Respond, revise la información clave (como el nombre de host o el nombre de archivo) y vea los puntos destacados de contexto.
- Cambie a Investigate para abrir la vista Navegar. Seleccione el grupo de metadatos Análisis de Endpoint y revise los metadatos creados.
- Vea los metadatos en la vista Análisis de eventos para analizar los eventos. Seleccione la búsqueda de hosts mediante el panel Metadatos de eventos.
- En la vista Hosts, haga clic en el nombre de host para ver el resumen de los datos de terminales, las instantáneas, las configuraciones de seguridad, etc.
- Realice un escaneo según demanda para obtener la información más reciente (si es necesario).
- Busque en todas las instantáneas un nombre de archivo, una ruta o un hash específicos para limitar la búsqueda.

- Revise los procesos, las ejecuciones automáticas, los archivos, las bibliotecas, los controladores y la información del sistema para realizar una investigación más detallada.
- En la vista Archivos, filtre los archivos mediante algunos indicadores (por ejemplo, nombre de archivo, tamaño de archivo, entropía, formato, nombre de la empresa, firma y suma de comprobación) y cambie a la vista Navegar para ver si existen en otros hosts de la red.

Enfoque en incidentes y alertas de NetWitness Respond

Un analista que trabaja en un incidente o una alerta en NetWitness Respond puede abrir el incidente en NetWitness Investigate (vista Navegar) para realizar un análisis más detallado del evento o la alerta.

- El flujo de trabajo para responder a un incidente suele comenzar en la vista Respond, donde el analista que investiga un incidente debe reunir inteligencia sobre el incidente en NetWitness Investigate. Puede colocar el cursor sobre una entidad subrayada en un incidente o una alerta, como una dirección IP, y, a continuación, seleccionar la acción Cambiar a Investigate > Navegar. La vista Navegar se abre y se filtra para la entidad seleccionada. Después de iniciar una investigación desde NetWitness Respond, las claves de metadatos definidas se consultan y el contenido de eventos de paquetes, registros y terminales capturados se muestra en la vista Navegar.
- Si encuentra eventos que son pertinentes al incidente, puede agregarlos a este en Respond. También puede crear un nuevo incidente en Respond en función de uno o más eventos encontrados en Investigate.
- (Versión 11.2 y superior) En el panel Indicadores de la vista Detalles de incidente de Respond, puede abrir la vista Análisis de eventos para obtener una mejor comprensión de un evento de indicador.

Vistas de NetWitness Investigate

En esta sección se proporciona una breve descripción y un ejemplo de cada vista principal (Navegar, Eventos, Análisis de eventos, Hosts, Archivos y Malware Analysis), además de vistas que ofrecen contexto adicional para los datos encontrados: el panel Búsqueda de contexto y la vista Reconstrucción de evento.

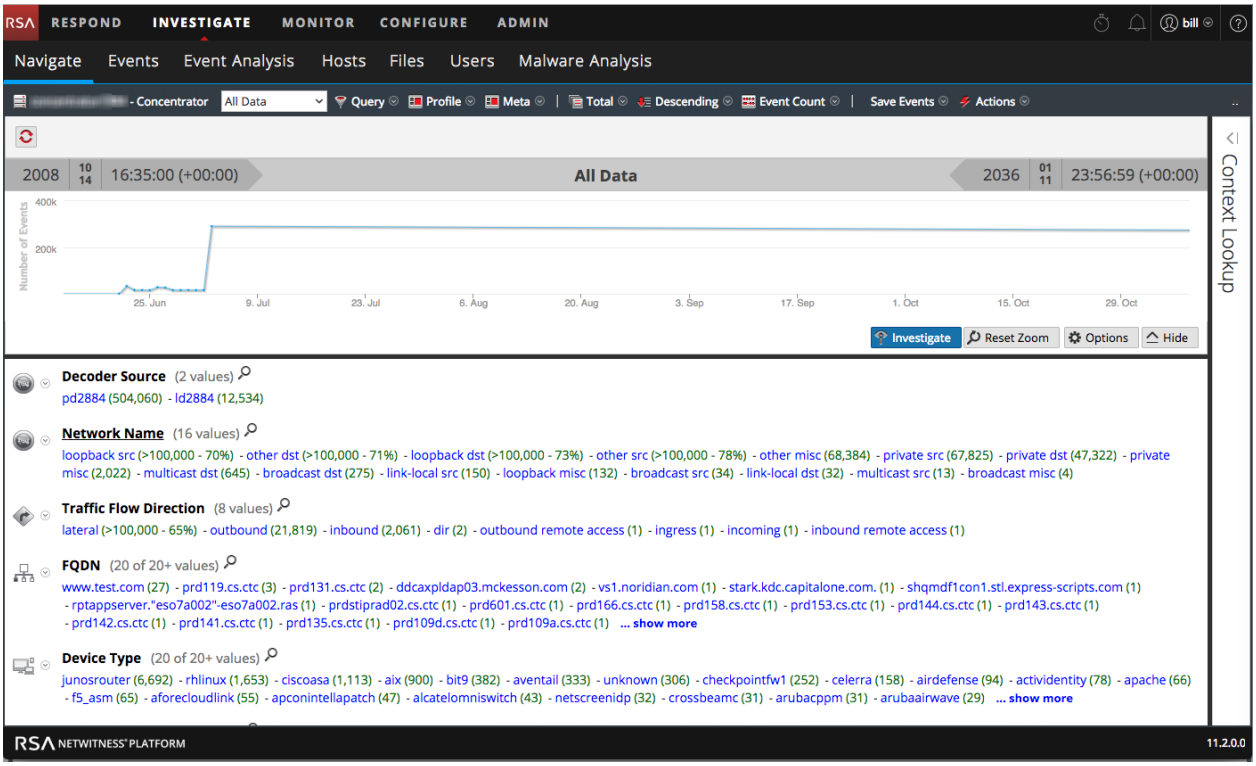
Vista Navegar

La vista Navegar permite desglosar a eventos de paquetes, registros y terminales capturados, y consultar su contenido en un Broker, un Concentrator o un Decoder (aunque la investigación de un Decoder no es común).

- Cuando selecciona un servicio, se consultan las claves de metadatos definidas para ese servicio y se devuelven los valores junto con la cantidad de eventos. Si se hace clic en un valor en cualquier nivel determinado, se revelan los resultados en detalle.

- Para ciertas claves de metadatos configuradas, como la dirección IP o el nombre de host, puede buscar información de contexto adicional en torno a un valor mediante Context Hub. El contexto adicional puede incluir incidentes, alertas y otros orígenes en los cuales se mencionó el valor.
- La vista Navegar también proporciona una visualización secuencial de los datos en una cronología. Aquí puede acercar un período seleccionado.

En esta figura se ilustra la vista Navegar.



Vista Eventos

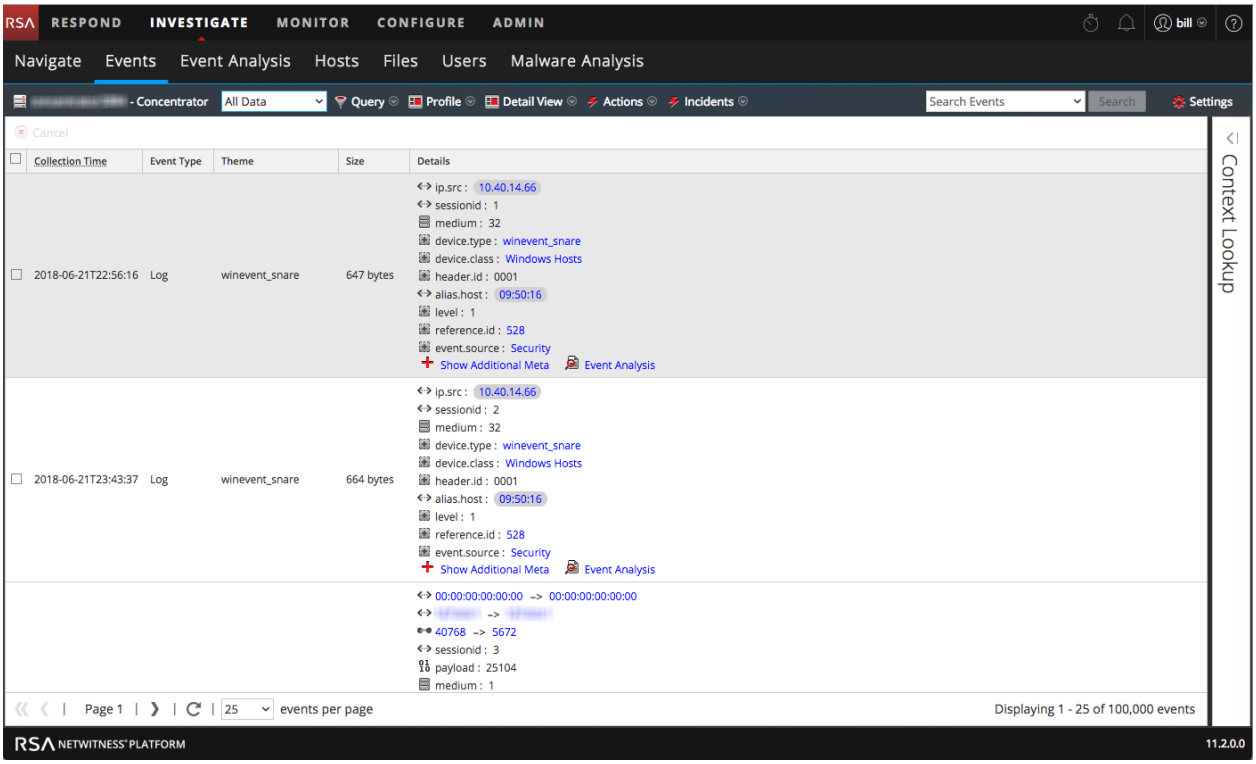
La vista Eventos proporciona una vista de eventos de paquetes, registros y terminal en formato de lista que permite ver los eventos de manera secuencial y reconstruirlos con seguridad.

- Puede abrir la vista Eventos para un valor de metadatos que ve en la vista Navegar.
- Para aquellos analistas que no tienen los privilegios suficientes para navegar a un servicio, la vista Eventos es una vista de investigación independiente en la cual pueden acceder a una lista de eventos de red, registro y terminal desde un servicio NetWitness Platform Core sin necesidad de desglosar primero a través de los metadatos.
- La vista Eventos presenta información de eventos en tres formatos estándar: una lista de eventos simple, una lista de eventos detallada y una vista de registros.
- Para ciertas claves de metadatos configuradas, como la dirección IP o el nombre de host, puede buscar información de contexto adicional en torno a un valor mediante Context Hub. El contexto

adicional puede incluir incidentes, alertas y otros orígenes en los cuales se mencionó el valor.

- Puede exportar eventos y archivos asociados, y crear un incidente a partir de un evento.

En esta figura se ilustra la vista Eventos.

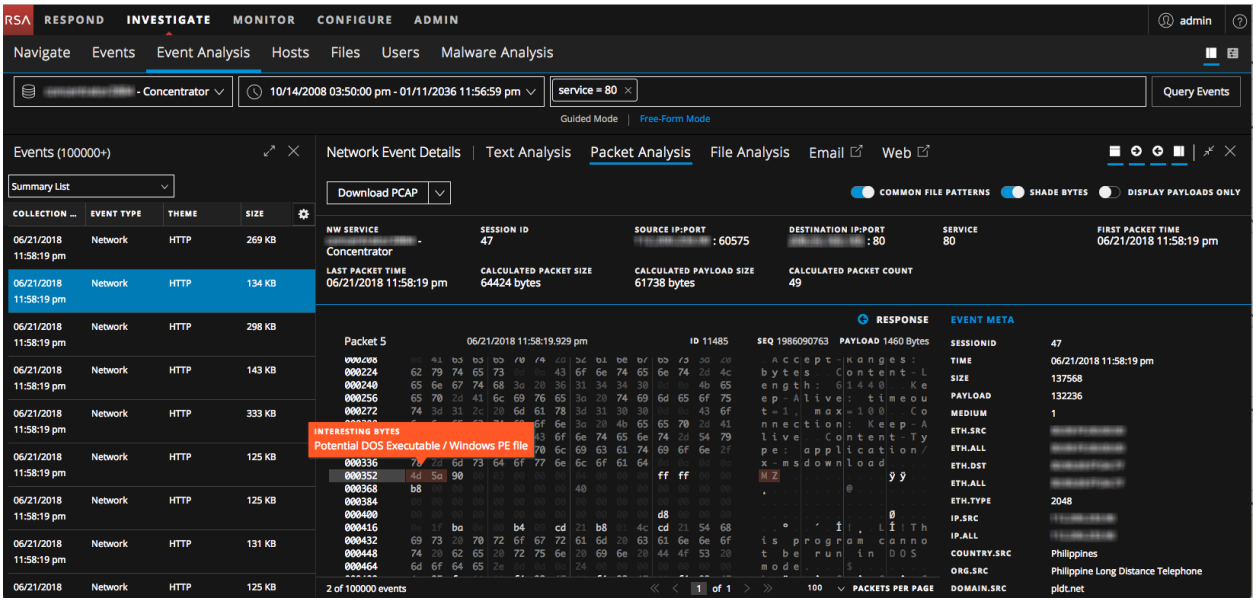


Vista Análisis de eventos

La vista Análisis de eventos es una herramienta interactiva que permite que los analistas vean los paquetes, el texto o los archivos de un evento con indicaciones visuales para destacar ciertos tipos de información. Distinta información es pertinente según el tipo de reconstrucción: paquetes, texto o archivos.

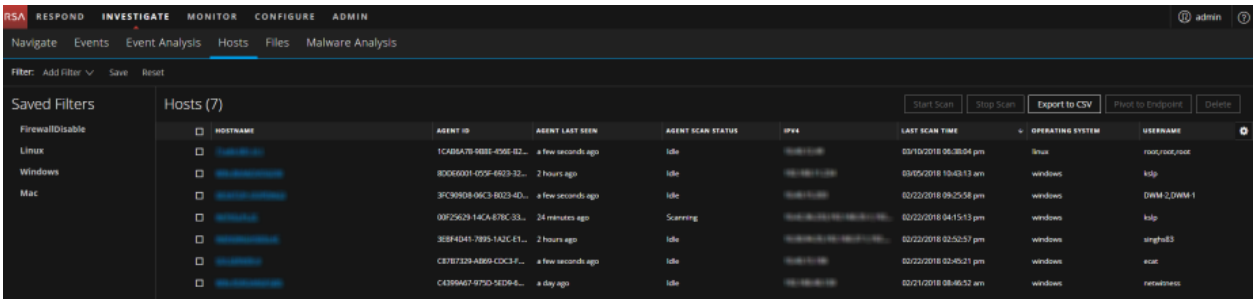
- Para ciertas claves de metadatos configuradas, como la dirección IP o el nombre de host, puede buscar información de contexto adicional en torno a un valor mediante Context Hub. El contexto adicional puede incluir incidentes, alertas y otros orígenes en los cuales se mencionó el valor.
- Cuando se observan archivos, puede exportarlos en un archivo zip al sistema de archivos local.
- Puede descargar registros desde la vista de texto y exportar paquetes desde la vista de paquetes.

Esta figura es un ejemplo de la vista Análisis de eventos.



Vista Hosts

La vista Investigar > Hosts enumera todos los hosts que tienen un agente. De forma predeterminada, los hosts se enumeran en función de la hora del último escaneo, y los hosts escaneados más recientemente ocupan la parte superior de la lista. Esta vista proporciona la funcionalidad de desglosar a los detalles del host. Esta figura es un ejemplo de la vista Hosts.

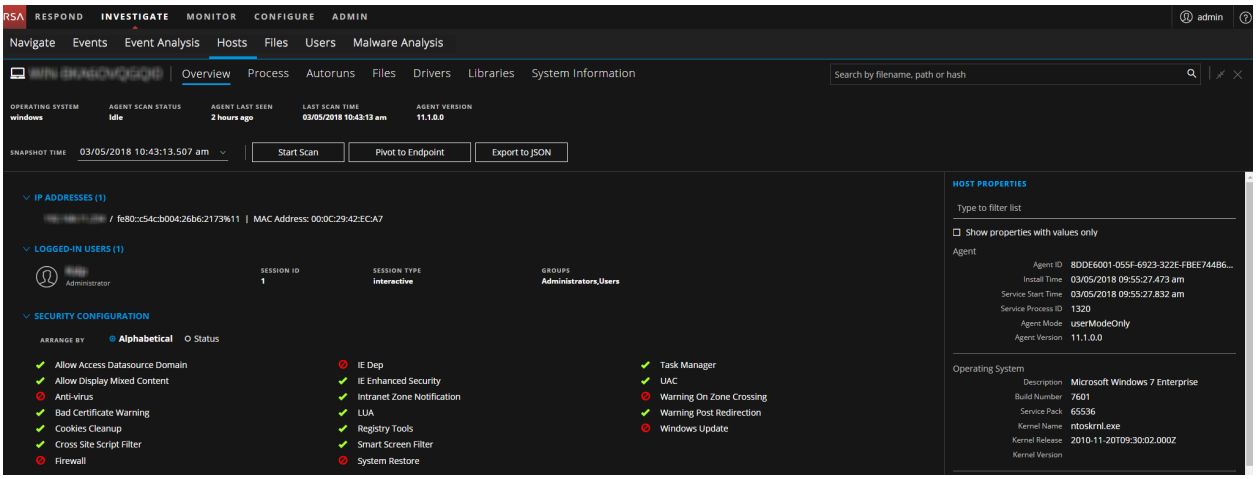


En esta vista, puede:

- Filtrar y ordenar hosts para acotar la investigación de hosts, ver detalles de hosts y eliminar hosts.
- Exportar los atributos de los hosts a un archivo CSV.
- Iniciar o detener un escaneo de los hosts seleccionados.
- Cambiar a las vistas Navegar o Análisis de eventos para investigar los hosts.

Nota: Si su implementación cuenta con NetWitness Endpoint 4.4.0.2 o superior, se enumeran los hosts en los cuales está instalado el agente 4.4.0.2, los que se pueden identificar mediante la versión del agente. Para obtener más información sobre cómo puede investigar estos hosts, consulte Investigar los hosts de NetWitness Endpoint 4.4.0.2 o superior.

Puede ver los resultados detallados del escaneo de un host haciendo clic en el nombre de host. Esta figura es un ejemplo de los resultados detallados del escaneo en la pestaña Descripción general.



Puede realizar lo siguiente:

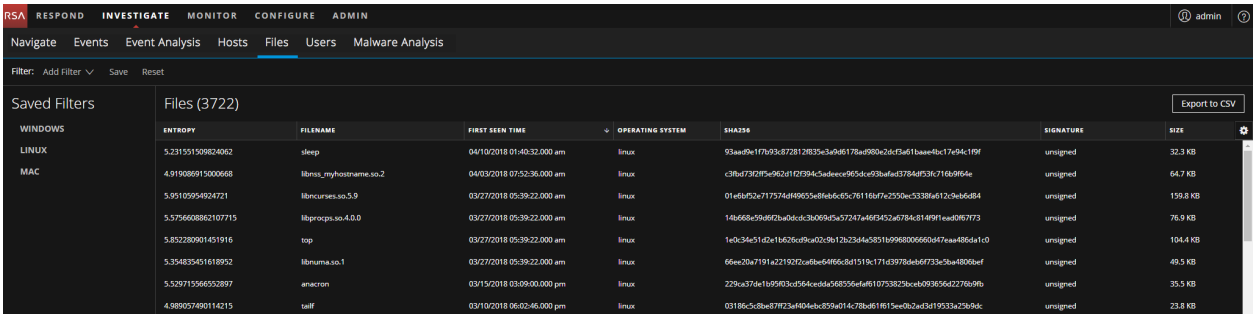
- Buscar en todas las instantáneas; nombre de archivo, ruto de archivo y suma de comprobación SHA-256 de archivo son los campos de búsqueda compatibles.
- Ver múltiples instantáneas. De forma predeterminada, se muestran los datos de la instantánea más reciente.
- Ver información adicional acerca de los hosts en las siguientes pestañas: Descripción general, Procesos, Ejecuciones automáticas, Archivos, Controlador, Bibliotecas e Información del sistema.
- Exportar todas las categorías de datos de terminales del host seleccionado para una instantánea específica en el formato JSON.

Vista Archivos

La vista Archivos proporciona una lista de archivos únicos que se encuentran en la implementación y sus propiedades asociadas. De forma predeterminada, los archivos se enumeran en función de la hora en que se vieron por primera vez. Durante el escaneo se recopilan los siguientes tipos de archivos cargados en la memoria.

- Archivo portable ejecutable (PE) (Windows): Estos son archivos `exe`, `dll` y `sys`. Puede ver las siguientes propiedades para cada archivo: suma de comprobación, detalles de compilación, diferentes secciones presentes en el archivo, bibliotecas importadas y detalles del certificado (firmante, huella digital y nombre de la empresa).
- Macho (Mac): Estos son paquetes de aplicaciones, dylibs y extensiones de kernel. Puede ver las siguientes propiedades para cada archivo: suma de comprobación, diferentes secciones presentes en el archivo, bibliotecas importadas y detalles del certificado (firmante, huella digital y nombre de la empresa).
- Formato ejecutable y vinculable (ELF) (Linux): Cada archivo contiene información acerca de la suma de comprobación, diferentes secciones presentes en el archivo y bibliotecas importadas.

Esta figura es un ejemplo de la vista Archivos.

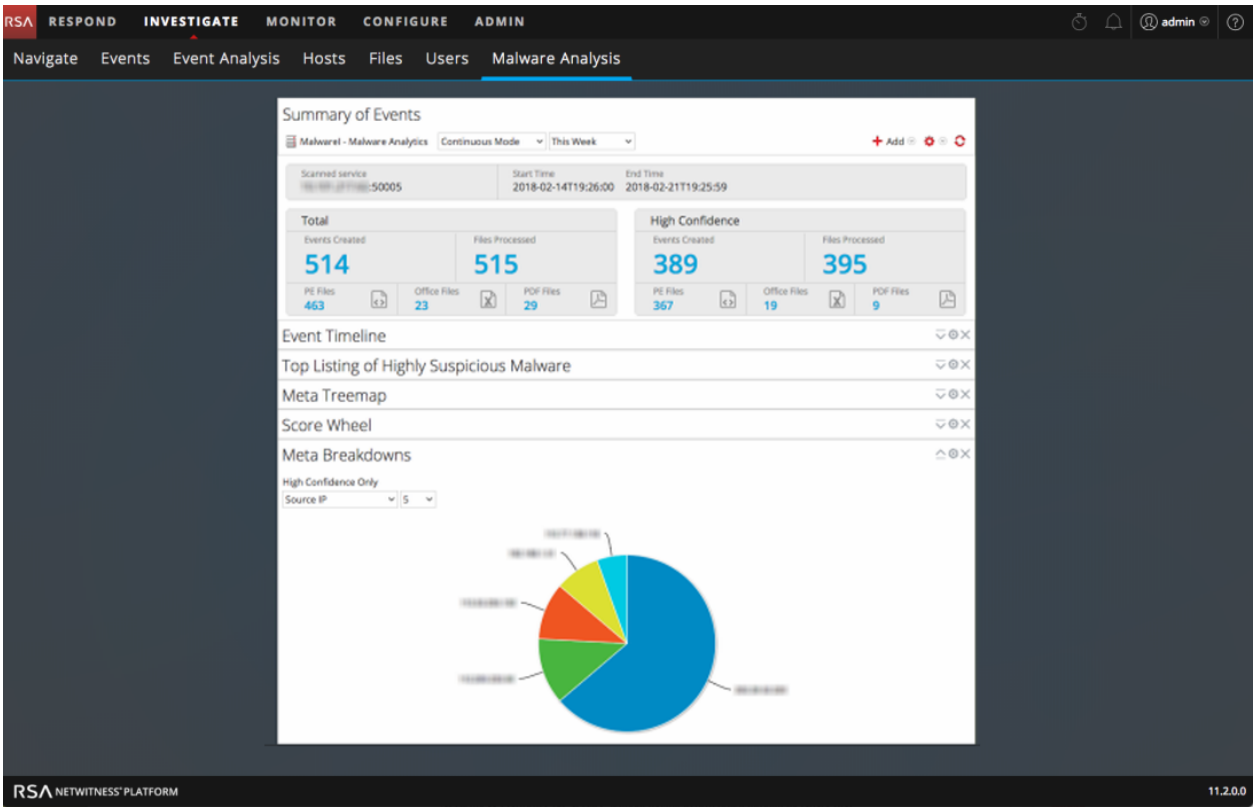


En la vista Archivos, puede realizar lo siguiente:

- Filtrar y ordenar los archivos para limitar la investigación.
- Cambiar a las vistas Navegar o Análisis de eventos para investigar acerca de los archivos.
- Exportar los archivos a un archivo CSV.

Vista Malware Analysis

La vista Malware Analysis proporciona una forma de analizar determinados tipos de objetos de archivos (como archivo ejecutable portátil de Windows (PE), PDF y MS Office) para evaluar la probabilidad de que un archivo sea malicioso. En esta figura se ilustra la vista Malware Analysis.



Puede abrir la vista Malware Analysis directamente o puede usar una acción del menú contextual para Escanear para encontrar malware a partir de un valor de metadatos en un punto de desglose actual desde la vista Navegar. Puede aprovechar los módulos de puntaje de múltiples niveles para establecer prioridades entre la enorme cantidad de archivos capturados, con el fin de concentrar los esfuerzos de análisis en los archivos que tienen más probabilidad de ser maliciosos.

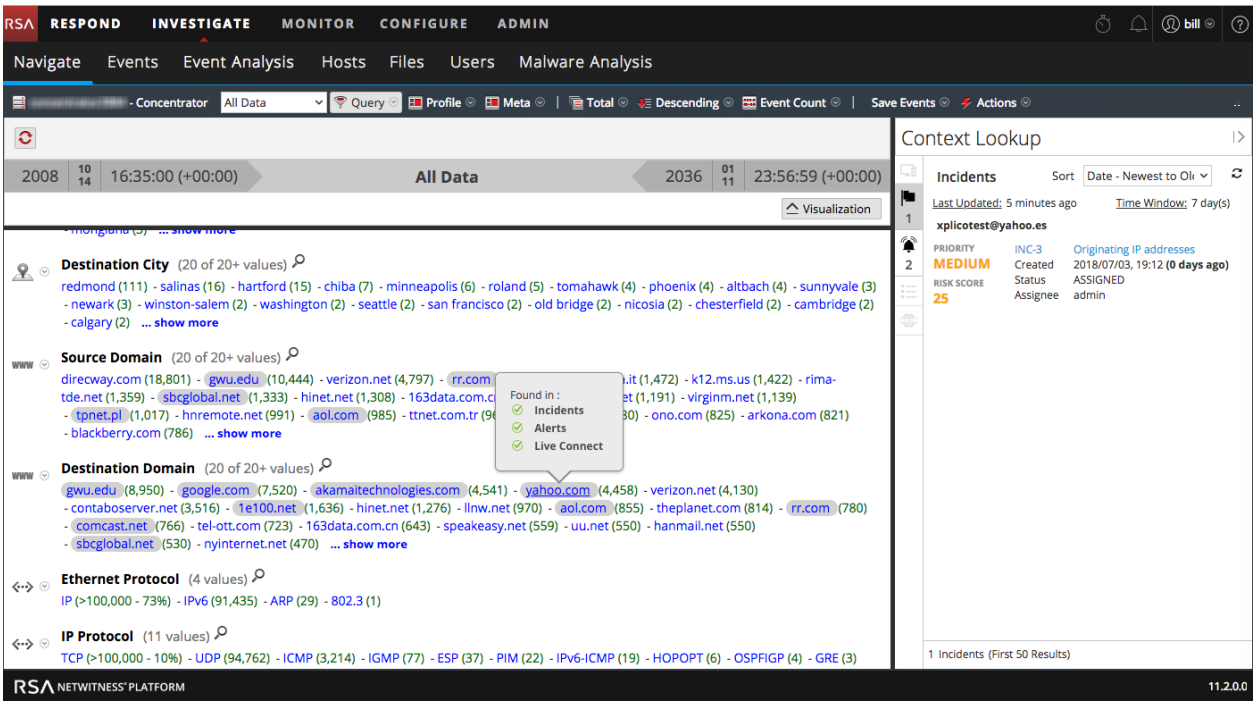
Información contextual para un evento

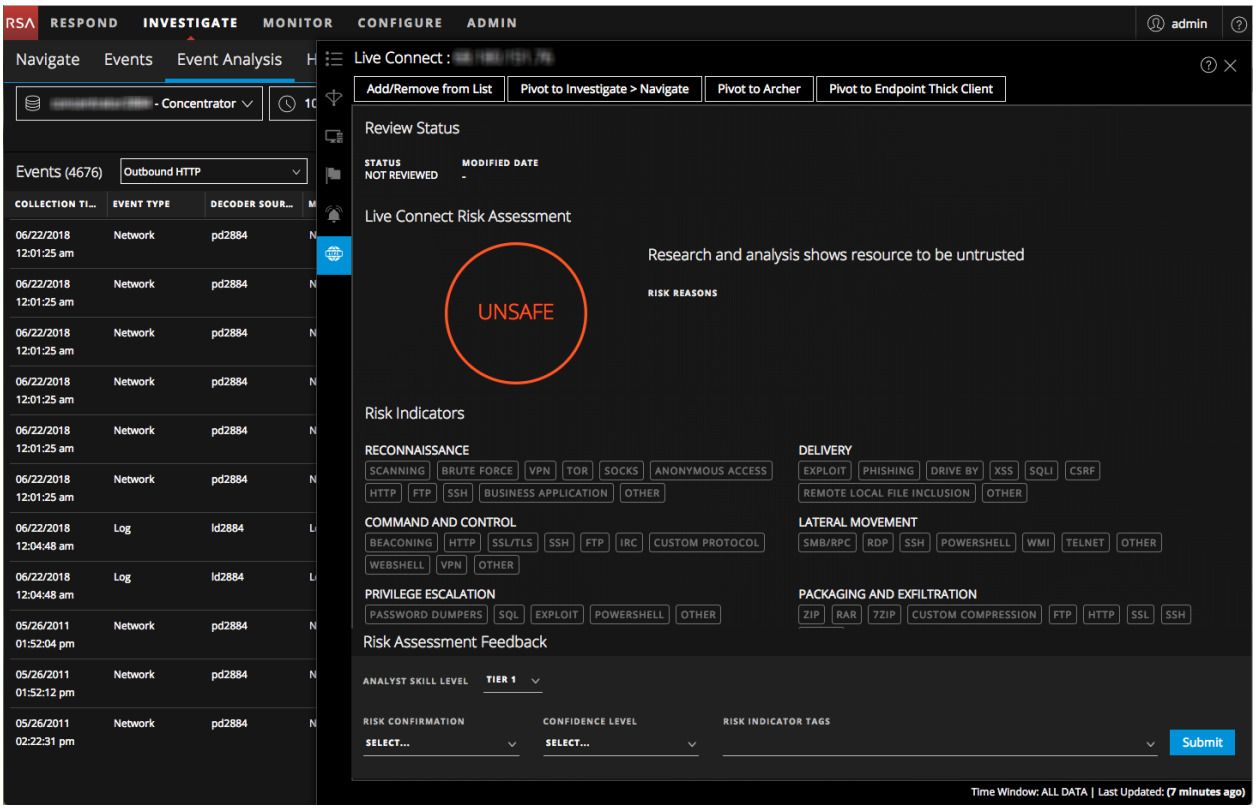
En las vistas Navegar, Eventos y Análisis de eventos (versión 11.2 y superior), el panel Búsqueda de contexto muestra detalles acerca de los elementos asociados con un evento (dirección IP, usuario, host, dominio, dirección MAC, nombre de archivo y hash de archivo) en Context Hub.

- Puede interactuar con los elementos de un evento para obtener más información valiosa, la cual incluye incidentes relacionados, alertas, listas personalizadas, recursos de Archer, detalles de Active Directory e IIOC de NetWitness Endpoint.
- Puede hacer clic en un punto de datos para ir a la vista Navegar.

Nota: Los recursos de Archer y los detalles de Active Directory están disponibles en la búsqueda de contexto de la vista Análisis de eventos. La búsqueda de contexto de Endpoint está disponible para los hosts de NetWitness Endpoint 4.4.0.2 o superior, pero no para los hosts de NetWitness Endpoint 11.1.

En las siguientes figuras se muestran el panel Búsqueda de contexto en la Vista Navegar y la vista Análisis de eventos.

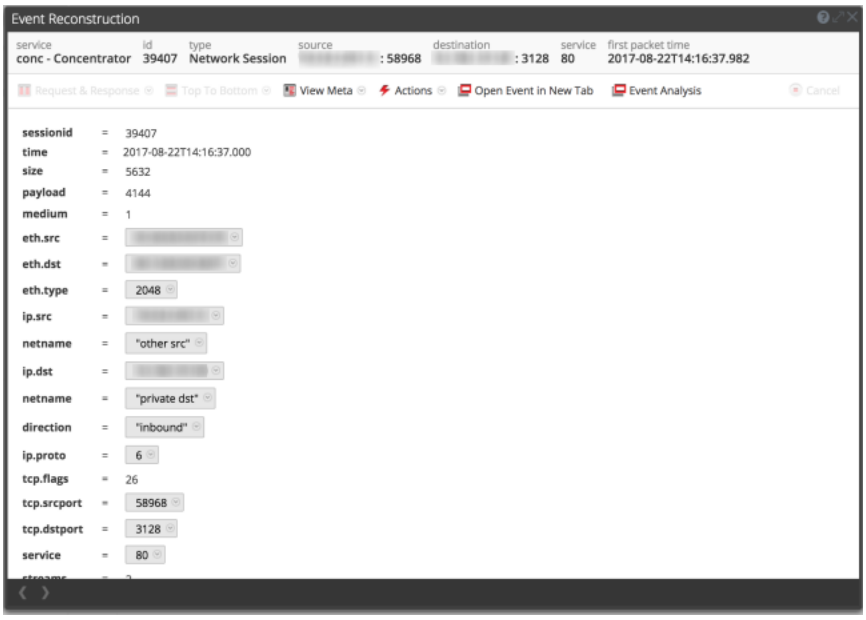




Reconstrucción de evento

Tres vistas de NetWitness Investigate ofrecen la capacidad de reconstruir un evento: las vistas Navegar, Eventos y Análisis de eventos. Cuando descubre un evento que amerita una investigación adicional, puede reconstruirlo de forma segura en un formato similar a su forma nativa. La representación de eventos restringe el uso de código dinámico o activo que podría incluir el evento para limitar cualquier resultado adverso en el sistema o el navegador. La caché se utiliza para mejorar el rendimiento cuando se observan eventos vistos anteriormente. Cada analista tiene una caché de datos de reconstrucción por separado y solo se puede acceder a eventos reconstruidos en la caché propia.

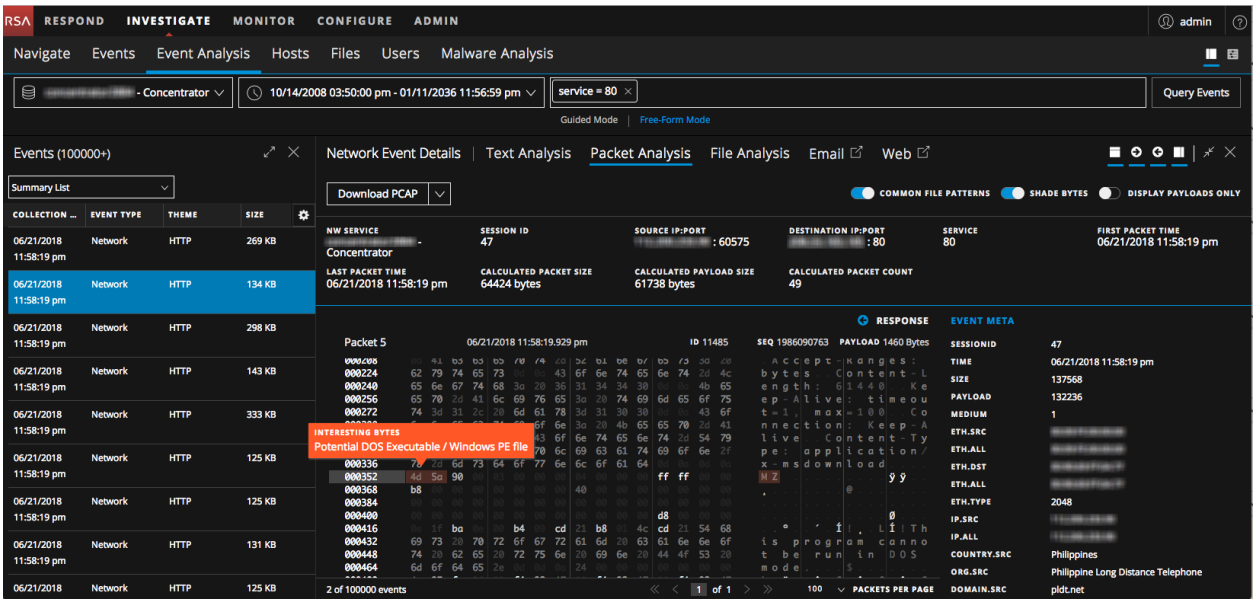
La Reconstrucción de evento en las vistas Eventos o Navegar presenta los datos crudos y las claves y los valores de metadatos para un evento en un formato de lista. Esta figura es un ejemplo de la Reconstrucción de evento.



En la Reconstrucción de evento en las vistas Navegar o Eventos:

- Puede navegar por las páginas de la reconstrucción para ver el evento siguiente en este formato.
- Los eventos se pueden reconstruir con diferentes métodos según el tipo de datos: metadatos, texto, hexadecimal, paquetes, web, correo, archivos o la mejor reconstrucción seleccionada automáticamente.
- Puede exportar archivos de captura de paquetes, extraer archivos y exportar los valores de metadatos para el evento.

En la vista Análisis de eventos se presenta una reconstrucción interactiva del evento, la que incluye datos crudos, claves de metadatos y valores. Esta figura es un ejemplo de una reconstrucción en la vista Análisis de eventos.



En la reconstrucción de la vista Análisis de eventos:

- Los eventos se pueden reconstruir con diferentes métodos según el tipo de datos: metadatos, texto, hexadecimal, paquetes y archivos.
- Se destaca la información de los encabezados y las cargas útiles.
- Puede ver las cargas útiles decodificadas y codificadas, y ver las firmas de archivos comunes.
- Puede buscar ubicaciones de claves de metadatos o valores en la reconstrucción.
- Puede exportar eventos y archivos.

Configuración de vistas y preferencias de NetWitness Investigate

Los analistas pueden configurar algunos aspectos de las vistas y el comportamiento de NetWitness Investigate. Puede personalizar la forma en que aparecen las vistas de Investigate, los tipos de información que se muestran y los factores que afectan el rendimiento en la devolución de resultados y la reconstrucción de eventos. Todos los ajustes configurables tienen valores predeterminados que son eficaces en la mayoría de las implementaciones; sin embargo, los analistas tienen la opción de ajustarlos si es necesario.

Las cuentas de usuario de los analistas que realizan análisis mediante Investigate deben tener configuradas las funciones y los permisos correspondientes del sistema. Un administrador debe configurar las funciones y los permisos como se describe en la *Guía de administración de usuarios y de la seguridad del sistema*. (Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.)

Se proporciona información detallada en los siguientes temas:

- Configurar la vista Navegar y la vista Eventos
- Configurar la vista Análisis de eventos
- Configurar la vista Resumen de eventos de Malware Analysis

Configurar la vista Navegar y la vista Eventos

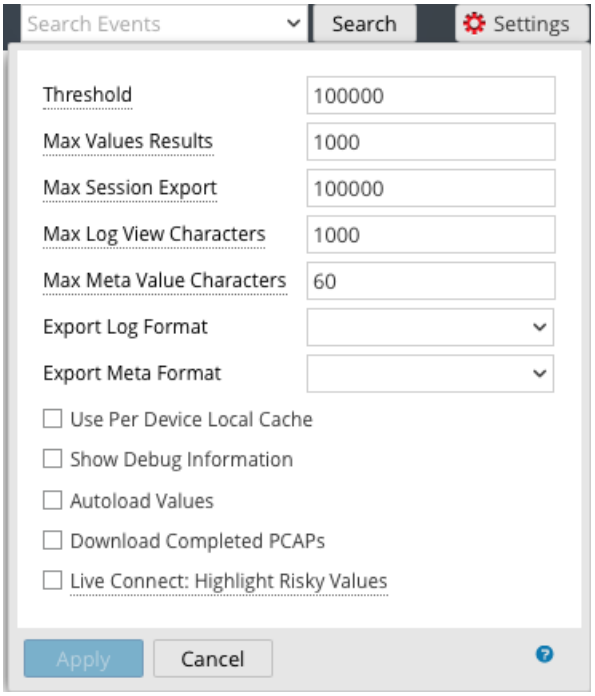
Los analistas pueden configurar las preferencias que afectan el rendimiento y el comportamiento de NetWitness Platform cuando se analizan datos en las vistas Navegar y Eventos. Algunas de estas configuraciones están disponibles en dos lugares de NetWitness Platform y los cambios realizados en cualquiera de ellos se aplican en la otra vista:

- Vista Investigar > cuadro de diálogo Ajustes de configuración para las vistas Navegar y Eventos.
- Perfiles > panel Preferencias > pestaña Investigación.
- Menú desplegable Opciones de búsqueda de las vistas Navegar y Eventos

Acceder a la configuración de las vistas Navegar y Eventos

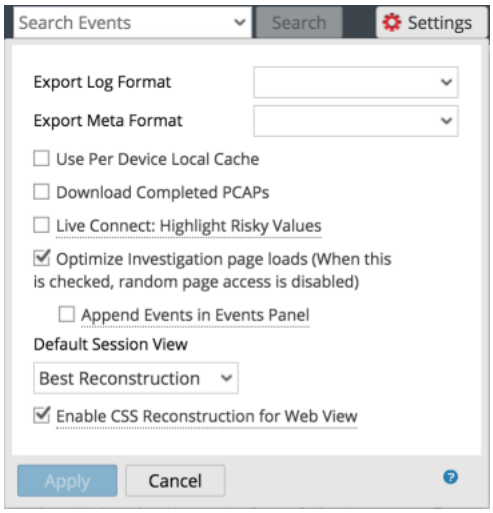
Para acceder a la configuración, realice una de las siguientes acciones:

- En la barra de herramientas de la vista **Navegar**, seleccione la opción **Ajustes de configuración**. Se muestra el cuadro de diálogo Configuración de la vista Navegar.



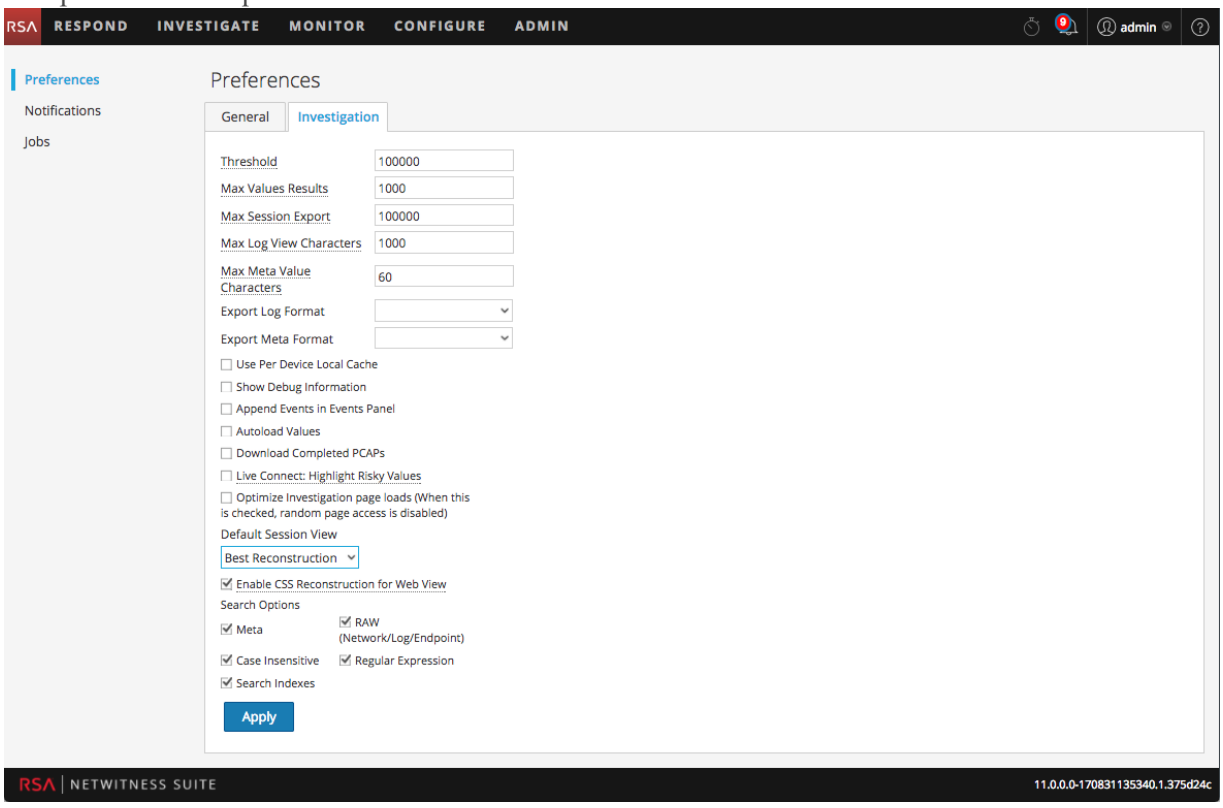
Nota: La versión 11.0 incluía la opción Agregar eventos en el panel de eventos, y esta se cambió al panel de configuración de la vista Eventos en la versión 11.1.

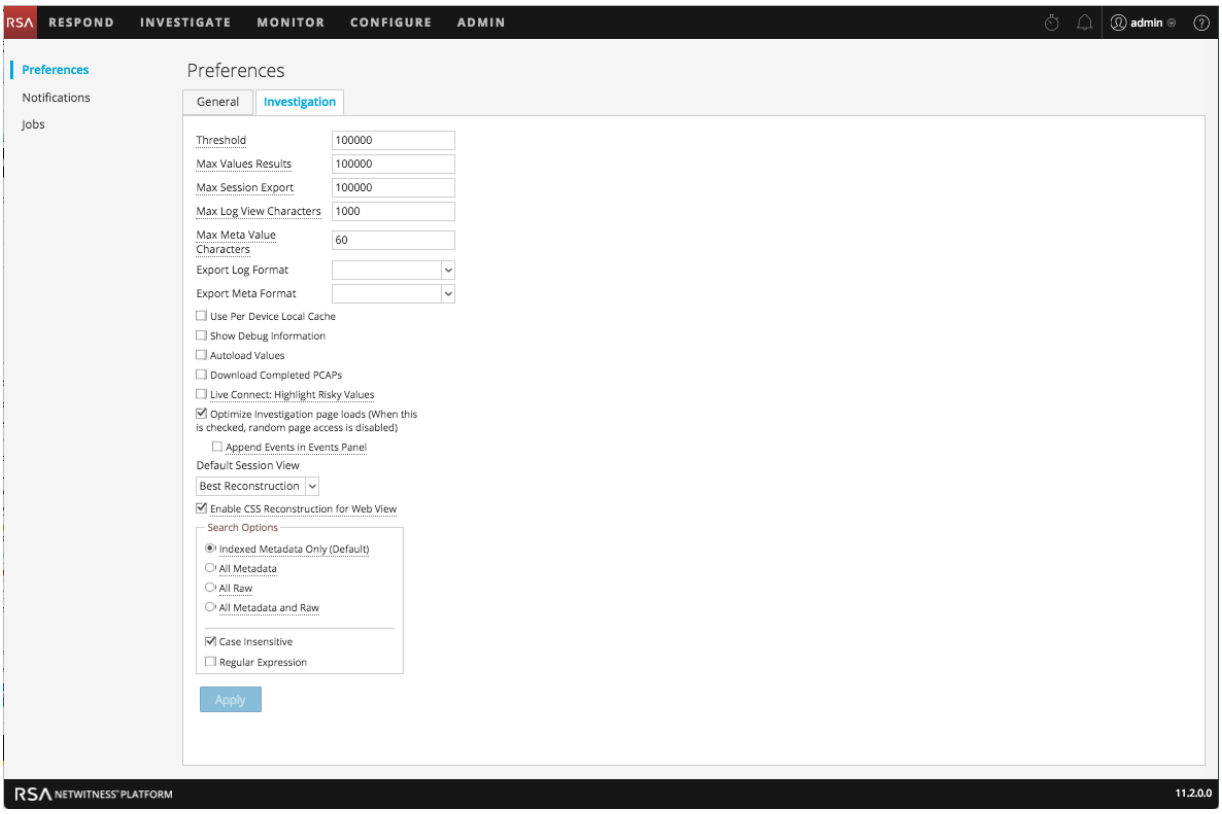
- En la barra de herramientas de la vista **Eventos**, seleccione la opción **Ajustes de configuración**. Se muestra el cuadro de diálogo Ajustes de configuración de la vista Eventos.



Nota: La versión 11.1 y superior incluye la opción Agregar eventos en el panel de eventos.

- En la esquina superior derecha de NetWitness Platform, vaya a > Profile y, en el panel **Preferencias**, haga clic en la pestaña **Investigación**.
  Se muestra el panel Investigación. En la primera figura que se muestra a continuación se ilustra el panel Investigación de la versión 11.1, y en la segunda, el panel de 11.2 con un diseño mejorado de las opciones de búsqueda.





Calibrar los parámetros de carga de valor de la vista Navegar

Varios ajustes influyen en el rendimiento de NetWitness Platform cuando se realiza la carga de valores en el panel Valores. Los valores predeterminados se configuran en función del uso común, y los analistas individuales pueden ajustar estas configuraciones para sus propias investigaciones. Para ajustar estas configuraciones:

1. Vaya a la pestaña **Investigación** o al cuadro de diálogo **Ajustes de configuración** de la vista Navegar.
2. Ajuste los siguientes parámetros:
   - **Umbral:** Ajuste el umbral para la cantidad máxima de sesiones cargadas de un valor clave de metadatos en el panel Valores. Un umbral más alto permite conteos precisos de un valor y también produce tiempos de carga mayores. El valor predeterminado es **100000**.
   - **Número máximo de resultados de valores:** Ajuste la cantidad máximo de valores para cargar en la vista Navegar cuando la opción Resultados máximos está seleccionada en el menú Clave de metadatos para una Clave de metadatos abierta. El valor predeterminado es **1,000**.
   - **Máximo de exportación de sesiones:** Especifique la cantidad de eventos que se pueden exportar en una única PCAP o archivo de registro.
   - **Caracteres de vista de registro máximos:** Configure la cantidad máxima de caracteres que desea mostrar en **Investigar > Eventos > Texto del registro**. El valor predeterminado es **1,000**.

- **Caracteres de valores de metadatos máximos:** Configure la cantidad máxima de caracteres en un nombre de valor de metadatos que se muestra en el panel Valores de la vista Navegar. El valor predeterminado es **60**.
- **Mostrar información de depuración:** Si desea que NetWitness Platform muestre la cláusula `where` debajo de la ruta de navegación en la vista Navegar y el tiempo de carga transcurrido para cada servicio agregado en un Broker, seleccione esta opción. El valor predeterminado es **Desactivado**.
- **Agregar eventos en el panel Eventos:** Esta opción afecta a la paginación en la vista Eventos y se describe a continuación en "Calibrar la recuperación de la vista Eventos y la reconstrucción predeterminada".
- **Cargar valores automáticamente:** Si desea que NetWitness Platform cargue valores automáticamente para el servicio seleccionado en la vista Navegar, seleccione esta opción. Cuando no está seleccionada, NetWitness Platform muestra un botón **Cargar valores**, el cual da la oportunidad de modificar las opciones. El valor predeterminado es **Desactivado**.

3. Haga clic en **Aplicar**.

Estos ajustes se aplican de inmediato y los podrá ver la próxima vez que cargue valores.

Configurar los parámetros de las vistas Navegar y Eventos

Varios ajustes influyen en el rendimiento de NetWitness Platform cuando se realiza la carga de valores en las vistas Navegar y Eventos. Los valores predeterminados se configuran en función del uso común, y los analistas individuales pueden ajustar estas configuraciones para sus propias investigaciones. Puede configurar estos parámetros por separado en las vistas Navegar y Eventos. Cuando se configuran en una vista, la configuración no se aplica automáticamente en la otra. Para ajustar estas configuraciones:

1. Vaya a la pestaña **Investigación** o al cuadro de diálogo **Ajustes de configuración** de las vistas Navegar o Eventos.
2. Ajuste los siguientes parámetros:
   - **Live Connect: Resaltar los valores riesgosos:** Si desea que NetWitness Platform resalte y muestre solo las direcciones IP que la comunidad de RSA considera riesgosas, seleccione esta opción. Cuando no está seleccionada, NetWitness Platform muestra todas las direcciones IP. De forma predeterminada, esta opción no está seleccionada (**Desactivado**).
   - **Uso por caché local de dispositivo:** Puede especificar el uso de los datos almacenados en caché localmente desde el servicio seleccionado. De forma predeterminada, esta opción no está seleccionada (**Desactivado**). Cuando esta función está deseleccionada, Investigate envía una consulta nueva a la base de datos en lugar de mostrar los datos almacenados en caché en las vistas de Investigate después de la carga inicial. Si está seleccionada, Investigate utiliza los datos de la caché local.
   - **Descargar PCAP finalizadas:** Puede automatizar la descarga de las PCAP extraídas en las vistas Navegar y Eventos a fin de que el navegador descargue la PCAP extraída y la abra en la aplicación predeterminada para la apertura de archivos PCAP, como Wireshark. De forma predeterminada, esta opción no está seleccionada (**Desactivado**). Si va a habilitar esta opción,

asegúrese de que el sistema de archivos local tenga instalada una aplicación que pueda abrir PCAP y que la aplicación esté configurada como la predeterminada para manejar formatos de archivos PCAP.

- **Live Connect: Resaltar los valores riesgosos:** Si esta opción está deseleccionada, todos los valores de metadatos que tienen contexto disponible en Live Connect se resaltan en el panel Valores de la vista Navegar. Si la opción está seleccionada, entre los valores que tienen contexto en Live Connect, solo se resaltan aquellos que la comunidad considera riesgosos/sospechosos/inseguros. De manera predeterminada, esta opción está deseleccionada (**Desactivado**).

3. Haga clic en **Aplicar**.
   Los cambios se implementan de inmediato.

Configurar el formato predeterminado de exportación de registros

Puede exportar registros desde las vistas Navegar y Eventos en distintos formatos. Las opciones disponibles son Texto, XML, valores separados por comas (CSV) y JSON. No hay valor predeterminado incorporado para el formato de exportación de registro. Si no selecciona un formato aquí, NetWitness Platform muestra un cuadro de diálogo de selección cuando invoca la exportación de registros. Para seleccionar el formato de los registros exportados:

1. Vaya a la pestaña **Investigación** o al cuadro de diálogo **Ajustes de configuración** de las vistas Navegar o Eventos.
2. Seleccione una de las opciones del menú desplegable **Formato de registro de exportación**.
3. Haga clic en **Aplicar**.
   El ajuste se aplica de inmediato.

Configurar el formato predeterminado de exportación de metadatos

Puede exportar valores de metadatos desde las vistas Navegar y Eventos en distintos formatos. Las opciones disponibles son Texto, CSV, valores separados por tabulaciones (TSV) y JSON. No hay ningún valor predeterminado incorporado para el formato de exportación de metadatos. Si no selecciona un formato aquí, NetWitness Platform muestra un cuadro de diálogo de selección cuando usted invoca la exportación de valores de metadatos. Para seleccionar el formato de los valores de metadatos exportados:

1. Vaya a la pestaña **Investigación** o al cuadro de diálogo **Ajustes de configuración** de las vistas Navegar o Eventos.
2. Seleccione una de las opciones del menú desplegable **Formato de metadatos de exportación**.
3. Haga clic en **Aplicar.**
   El ajuste se aplica de inmediato.

Calibrar la recuperación de la vista Eventos y la reconstrucción predeterminada

Puede configurar varios parámetros que controlan la manera en que NetWitness Platform recupera y reconstruye eventos en la vista Eventos. Para ajustar estos parámetros:

1. Vaya a la pestaña **Investigación** o al cuadro de diálogo **Ajustes de configuración** de la vista Eventos.
2. Configure los siguientes parámetros.
   - **Optimizar las cargas de páginas de Investigation**: Establezca una opción de paginación. Cuando está optimizada, los resultados se devuelven lo más rápidamente posible, pero se renuncia a la capacidad original de ir a una página específica de la lista de eventos. La deselección de esta casilla cambia la paginación en la Lista de eventos y permite ir a una página específica de la lista (o a la última página). El valor predeterminado es **habilitado**.
   - **Vista de sesión predeterminada:** Selecciona el tipo de reconstrucción predeterminado para la reconstrucción inicial en la vista Eventos. El valor predeterminado es **Mejor reconstrucción**, con el cual los eventos se reconstruyen mediante el método de reconstrucción más apropiado para el evento.
3. Navegue a la pestaña **Investigación** o al cuadro de diálogo **Ajustes de configuración** de la vista Navegar (11.1) o de la vista Eventos (11.2) y configure la opción **Agregar eventos en el panel de eventos**. Cuando se selecciona esta opción, los eventos que se muestran en el **Panel de eventos** se agregan de manera incremental. Por ejemplo, cada vez que hace clic en el ícono de la página siguiente, se agrega el siguiente incremento de eventos; en primer lugar, verá 1 a 25, a continuación, 1 a 50, después, 1 a 75 y así sucesivamente. Esta opción está disponible solo si la opción **Optimizar cargas de la página Investigation** está habilitada.
4. Para activar los cambios de inmediato, haga clic en **Aplicar**.

Habilitar o deshabilitar la generación de hojas de estilo en cascada en reconstrucciones de contenido web

Los analistas pueden habilitar el uso de hojas de estilo en cascada (CSS) cuando reconstruyen contenido web. Si está habilitada, la reconstrucción web incluye imágenes y estilos de CSS, de modo que su aspecto coincide con la vista original en un navegador web. Esto incluye el escaneo y la reconstrucción de eventos relacionados y la búsqueda de hojas de estilo e imágenes que se usan en el evento objetivo. Esta opción está habilitada de manera predeterminada. Deshabilítela si hay problemas para ver sitios web específicos.

Nota: Es posible que el aspecto del contenido reconstruido no coincida perfectamente con la página web original si no se pudo encontrar imágenes y hojas de estilo relacionadas o si estas se cargaron desde la caché del navegador web. Además, el diseño o el estilo que se ejecutan dinámicamente a través de JavaScript en el lado del cliente no se generan en la reconstrucción debido a que todo el JavaScript del lado del cliente se quita por motivos de seguridad.

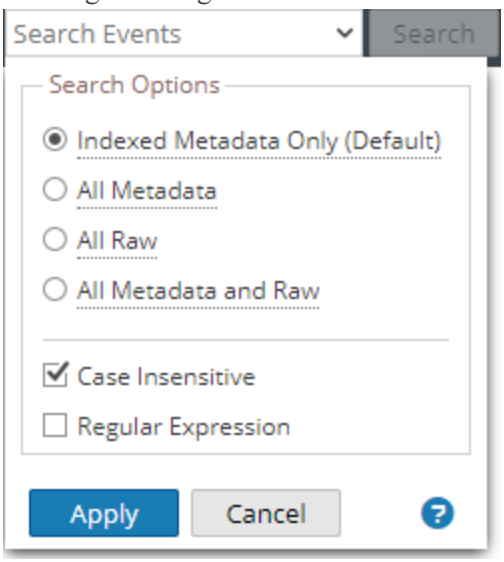
Para habilitar o deshabilitar esta opción:

1. Vaya a la pestaña **Investigación**.
2. Seleccione la casilla de verificación **Activar reconstrucción de CSS para vista web**.
3. Haga clic en **Aplicar**.
   La configuración se aplica de inmediato y se puede ver en la siguiente reconstrucción de contenido web.

Configurar opciones de búsqueda

Puede configurar opciones de búsqueda que se aplicarán cuando escriba una cadena de búsqueda en el campo Buscar. Edite las Opciones de búsqueda en Perfil > panel Preferencias > pestaña Investigación o en el menú desplegable Opciones de búsqueda de las vistas Navegar y Eventos. Para configurar las opciones de búsqueda:

1. Navegue a Opciones de búsqueda.
   En la siguiente figura se ilustra el menú desplegable Opciones de búsqueda para la versión 11.2.



2. Seleccione una o más opciones de búsqueda para aplicar a la búsqueda. En Buscar patrones de texto se proporciona información detallada acerca de cada opción.
3. Para guardar la configuración de la búsqueda, haga clic en **Aplicar**.
   Las preferencias se guardan y se aplican de inmediato.

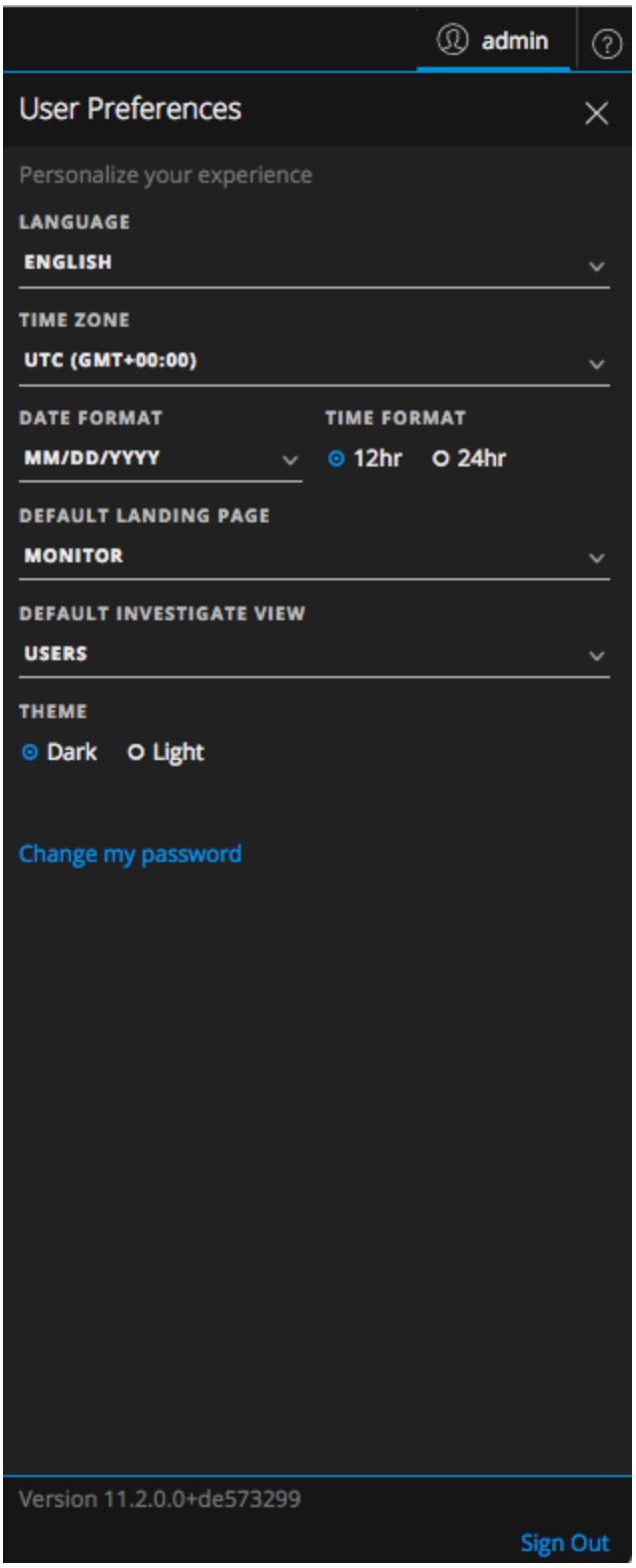
Configurar la vista Análisis de eventos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

A partir de la versión 11.1, los analistas pueden configurar preferencias que afectan el comportamiento de NetWitness Platform cuando se analizan datos mediante la vista Investigar > Análisis de eventos. La barra de herramientas principal de Investigate tiene un aspecto distinto cuando está abierta la vista Análisis de eventos; estos dos botones permiten el acceso a cuadros de diálogo de preferencias:  y  . El menú Usuario () se centra en las preferencias globales del usuario, como la zona horaria. En cambio, el menú de preferencias de Análisis de eventos () lo hace en las preferencias del usuario para el comportamiento en la vista Análisis de eventos. En el resto de esta sección se describen ambos conjuntos de preferencias.

Configurar la vista predeterminada de Investigate

La vista predeterminada de Investigate se configura en el cuadro de diálogo Preferencias de usuario globales (en la esquina superior derecha de la ventana del navegador de NetWitness Platform, seleccione ).
En el cuadro de diálogo Preferencias de usuario se muestran las preferencias actuales para la vista Investigate. En las siguientes vistas puede seleccionar la vista predeterminada de Investigate cuando se abre: Vista Análisis de eventos, vista Hosts o vista Archivos.



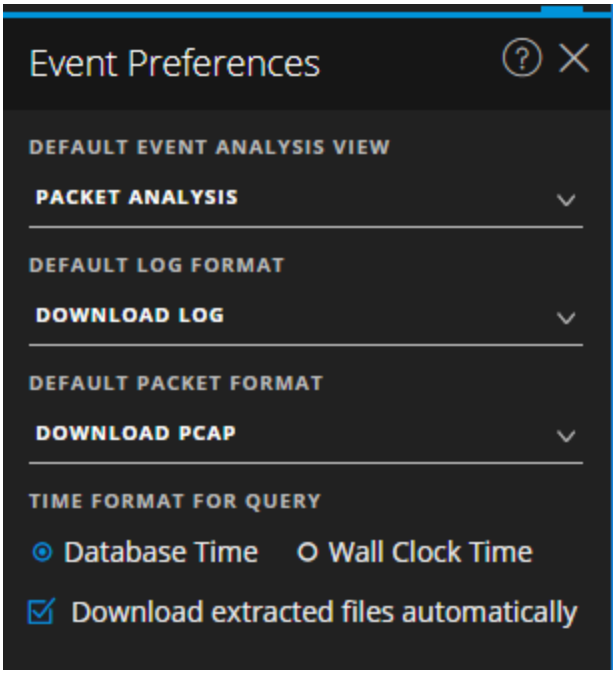
Las preferencias de usuario globales se describen en detalle en la *Guía de introducción de NetWitness Platform*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Configurar las preferencias de usuario para la vista Análisis de eventos

En la versión 11.1 y superior, puede configurar las preferencias pertinentes a la vista Análisis de eventos. Las preferencias que selecciona aquí persisten por usuario y están disponibles cada vez que el usuario específico inicia sesión en la aplicación.

Para configurar los valores predeterminados para trabajar en la vista Análisis de eventos:

1. Con la vista Análisis de eventos abierta, haga clic en .



2. En el menú desplegable **Vista Análisis de eventos predeterminada**, seleccione el tipo de reconstrucción predeterminado cuando abre un evento en el panel Análisis de eventos: **Análisis de texto**, **Análisis de paquetes** o **Análisis de archivos**.
   Si no selecciona un tipo de análisis predeterminado, cuando abra un evento, el tipo de reconstrucción predeterminado será el Análisis de paquetes, excepto para los eventos de registro y terminal, los cuales se abren en el Análisis de texto. Si selecciona un tipo de reconstrucción predeterminado, el tipo de reconstrucción es la reconstrucción predeterminada que especificó. En ambos casos, el valor predeterminado es el punto de partida y, si cambia el tipo mientras está trabajando, el tipo que selecciona se utiliza para la reconstrucción siguiente.
3. En la lista desplegable **Formato de registro predeterminado**, seleccione el formato de descarga para la exportación de registros: **Descargar registro**, **Descargar XML**, **Descargar CSV** o **Descargar JSON**. Si no selecciona un formato aquí, el formato de descarga predeterminada es **Descargar registro**. Estas opciones también están disponibles en un menú desplegable en el momento de la descarga.
4. En el menú desplegable **Descargar PCAP**, seleccione el formato predeterminado para la descarga de paquetes. Estas opciones también están disponibles en un menú desplegable en el momento de la descarga:

- **Descargar PCAP** para descargar el evento completo como un archivo de captura de paquetes (*.pcap)
- **Descargar todas las cargas útiles** para descargar la carga útil como un archivo *.payload
- **Descargar carga útil de la solicitud** para descargar la carga útil de la solicitud como un archivo *.payload1
- **Descargar carga útil de la respuesta** para descargar la carga útil de la respuesta como un archivo *.payload2

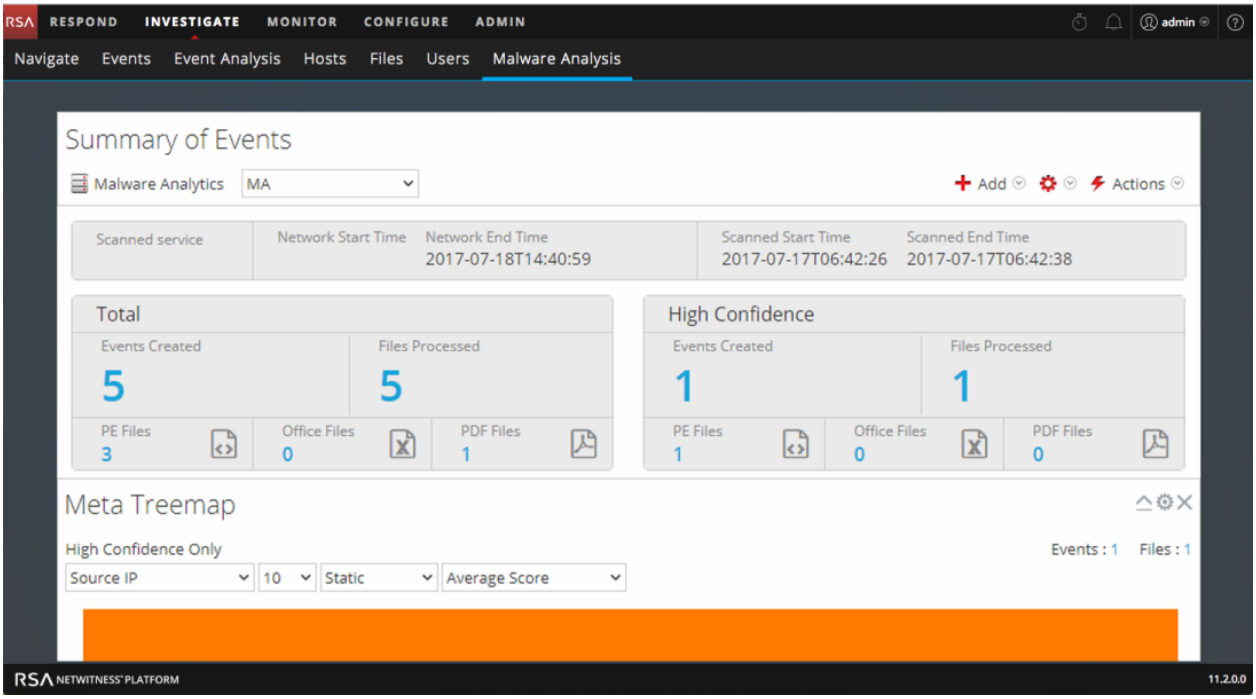
5. En **Formato de hora para la consulta**, elija **Hora de la base de datos** u **Hora del reloj**. La vista Análisis de eventos puede mostrar los resultados en función de la hora de la base de datos o la hora actual del reloj. Cuando configura el formato de hora aquí, la preferencia del usuario individual se guarda hasta que se vuelve a cambiar. La configuración predeterminada de esta preferencia es **Hora de la base de datos**, que es el mismo formato de hora que se usa para mostrar los resultados de consulta en las vistas Navegar y Eventos.
   - Cuando se selecciona **Hora de la base de datos**, la hora de inicio y finalización de una consulta se basa en la hora en que se almacenó el evento.
   - Cuando se selecciona **Hora del reloj**, la consulta se ejecuta con la hora actual según la zona horaria configurada en las preferencias del usuario.

Configurar la vista Resumen de eventos de Malware Analysis

En el Resumen de eventos se ofrece un resumen del escaneo que se investiga, y bajo el resumen se presentan dashlets configurables, como gráficos de visualización y listas. De forma predeterminada, se abre el Resumen de eventos para un escaneo, el cual muestra los dashlets predeterminados. Puede personalizar la vista mediante la adición, la modificación y la eliminación de dashlets predeterminados. La personalización de dashlets configurada persiste en distintas investigaciones de escaneos y los dashlets predeterminados se pueden restaurar en cualquier momento. Los dashlets predeterminados son:

- Resumen de eventos (fijo)
- Cronograma de evento
- Lista del malware altamente sospechoso principal
- Mapa de árbol de metadatos
- Rueda de puntaje
- Desgloses de metadatos

En la siguiente figura se muestra un ejemplo del Resumen de eventos predeterminado.



El resto de este tema proporciona instrucciones para administrar y configurar los dashlets.

Agregar un dashlet

Puede agregar múltiples copias de dashlets en el Resumen de eventos de Malware Analysis. Para agregar un dashlet:

1. En la barra de herramientas, seleccione **Agregar**.
   Se muestra la lista desplegable de dashlets. Hay cuatro opciones de visualización: Rueda de puntaje,

Mapa de árbol de metadatos, Desgloses de metadatos y Cronograma de evento. Los otros tres dashlets son los mismos dashlets disponibles en el tablero NetWitness Platform: Malware con IOC de alta confianza y altos puntajes, Lista del malware altamente sospechoso principal y Lista del posible malware de día cero principal. En la sección "Dashlets" de Contenido de RSA para RSA NetWitness Platform se proporcionan detalles acerca de estos dashlets comunes.

2. Seleccione un dashlet.
   El nuevo dashlet se agrega como el último debajo de los dashlets existentes.
3. Si el dashlet es un duplicado de otro existente, cambie el nombre del nuevo dashlet para que sea único.

Modificar o eliminar un dashlet mediante opciones de la barra de herramientas

Cada dashlet tiene una barra de herramientas que ofrece opciones para modificarlo. Los gráficos de visualización tienen los mismos ajustes de configuración, aunque algunos de los otros dashlets tienen distintos ajustes adicionales.

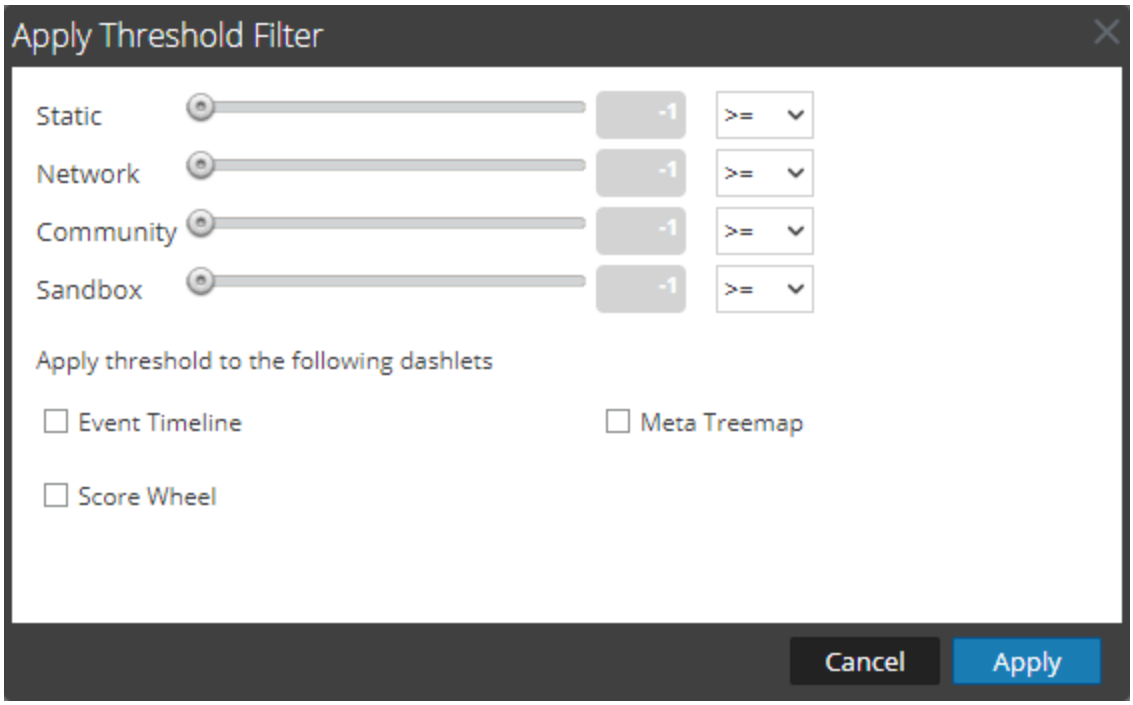
Para usar las opciones de la barra de herramientas:

- Para cerrar un dashlet de modo que solo se muestre la barra de título, haga clic en .
- Para abrir un dashlet que está cerrado, haga clic en .
- Para mostrar los ajustes configurables de un dashlet, haga clic en .
  Se muestra el cuadro de diálogo de configuración del dashlet.
- Para eliminar un dashlet, haga clic en .

Aplicar un filtro de umbral a múltiples dashlets

Dentro de los dashlets, puede configurar un umbral para mostrar únicamente eventos iguales a, por sobre o por debajo de cierto puntaje en las cuatro categorías (Estático, Red, Community y Sandbox). Este procedimiento configura los umbrales por tipo de dashlet para estos dashlets: Cronograma de evento, Rueda de puntaje y Mapa de árbol de metadatos. También puede configurar el umbral para dashlets individuales.

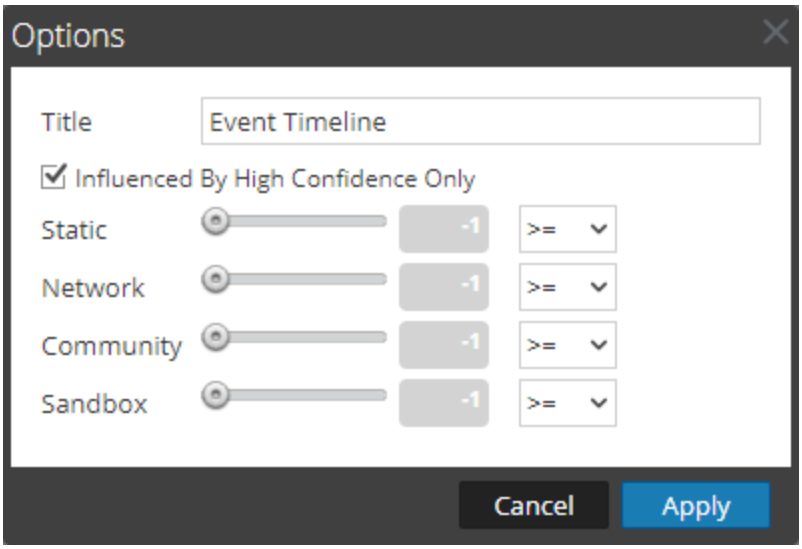
1. En la barra de herramientas, seleccione > **Aplicar filtro de umbral**.
   Se muestra el cuadro de diálogo Aplicar filtro de umbral.



2. Seleccione uno o más tipos de dashlets: Cronograma de evento, Rueda de puntaje y Mapa de árbol de metadatos.
3. Arrastre el control deslizante correspondiente o ingrese un valor numérico y, a continuación, seleccione un operador en la lista desplegable: =, >= o <=.
4. Haga clic en **Aplicar**.
   Los filtros de umbral se aplican a los tipos de dashlets seleccionados en el Resumen de eventos.

Establecer opciones de título y categoría para un dashlet

1. Para mostrar los ajustes configurables de un dashlet, haga clic en ⚙.
   Se muestra el cuadro de diálogo Opciones del dashlet.

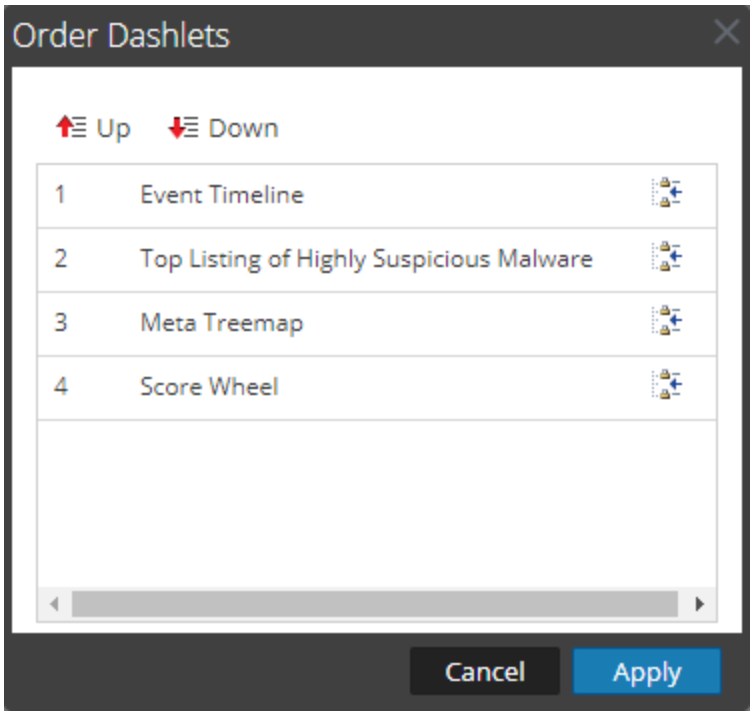


2. Escriba un nuevo título para el dashlet en el campo **Título**.
3. Si solo desea ver eventos con influencia de una etiqueta Alta confianza, lo cual significa que existe alta confianza de que el evento contiene código dañino, seleccione la opción **Solo con influencia de alta confianza**.
4. Si solo desea ver eventos que obtuvieron un puntaje por sobre determinado valor en las cuatro categorías (Estático, Red, Comunidad y Sandbox), arrastre el control deslizante correspondiente o ingrese un valor numérico y, a continuación, seleccione un operador en la lista desplegable: =, >= o <=.
5. Haga clic en **Aplicar**.
   El título y los filtros se aplican al dashlet.

Ordenar dashlets

Para cambiar el orden de los dashlets que aparecen debajo del Resumen de eventos:

1. En la barra de herramientas, seleccione > **Ordenar dashlets**.
   Se muestra el cuadro de diálogo Ordenar dashlets.



2. Seleccione un dashlet que desee subir o bajar y haga clic en Up o en Down.
3. Cuando esté conforme con el orden, haga clic en **Aplicar**.
   El cuadro de diálogo se cierra y el orden de los dashlets debajo del Resumen de eventos cambia de acuerdo con sus opciones.

Restaurar dashlets predeterminados

Cuando haya agregado, modificado y ordenado los dashlets, puede volver a la configuración predeterminada de presentación de los dashlets. Para restaurar los dashlets predeterminados:

1. En la barra de herramientas, seleccione > **Restaurar configuración predeterminada**.
   En un cuadro de diálogo se solicita confirmar la intención de restaurar la configuración.
2. Realice una de las siguientes acciones:
   a. Si decide mantener el orden de los dashlets que configuró, haga clic en **No**.
   b. Si realmente desea restaurar los valores predeterminados, haga clic en **Sí**.
      La presentación de los dashlets vuelve al valor predeterminado.

Inicio de una investigación

NetWitness Platform ofrece distintos puntos de partida en función de la pregunta que está intentando responder: Vista Navegar, vista Eventos, vista Análisis de eventos, vista Hosts, vista Archivos y vista Malware Analysis.

Nota: Se requieren funciones y permisos de usuario específicos para que un usuario realice investigaciones en NetWitness Platform. Si no puede realizar una tarea de análisis o abrir una vista, es posible que el administrador necesite ajustar las funciones y los permisos configurados para usted. Las vistas Hosts y Archivos están disponibles en la versión 11.1 y superior. La vista Análisis de eventos estaba disponible en la versión 11.0, pero el método de acceder a ella era a través de la vista Eventos. En la versión 11.1 y superior, se puede acceder directamente a la vista Análisis de eventos.

Enfoque en los metadatos, los eventos y el análisis de eventos

Para buscar eventos que impulsen el flujo de trabajo de respuesta ante incidentes y realizar un análisis estratégico después de que otra herramienta haya generado un evento, debe comenzar en la vista Navegar, vista Eventos o vista Análisis de eventos. Investigue los metadatos para un solo Broker o Concentrator. En cada una de estas vistas, inicie la investigación abriendo la vista, donde puede ejecutar una consulta y filtrar los resultados mediante la limitación del rango de tiempo y la creación de consultas de metadatos. En los siguientes temas se ofrece información detallada sobre el comienzo de una investigación en cada vista:

- Comenzar una investigación en las vistas Navegar o Eventos
- Comenzar una investigación en la vista Análisis de eventos

Enfoque en los hosts y los archivos

Para buscar información en los hosts en que se ejecuta el agente, comience la investigación en la vista Hosts (**Investigar > Hosts**). Para cada host, puede ver los procesos, los controladores, los archivos DLL, los archivos (ejecutables), los servicios y las ejecuciones automáticas que se ejecutan, así como la información relacionada con los usuarios que iniciaron sesión. (Consulte Investigar los hosts).

Puede comenzar la investigación en los archivos de su implementación en la vista Archivos (**Investigar > Archivos**). (Consulte Investigar los archivos).

Nota: Para cargar las vistas Hosts y Archivos, debe tener el permiso `endpoint-server.filter.manage`.

Enfoque en el escaneo de archivos para encontrar malware

Para escanear archivos para encontrar malware potencial o configurar un escaneo continuo de un servicio, comience en la vista Malware Analysis. Los resultados se expresan como cuatro tipos de análisis: Red, Estático, Community y Sandbox con una clasificación de indicadores de riesgo (IOC). Existen varias maneras de comenzar a trabajar en Malware Analysis:

- Puede comenzar Malware Analysis desde los dashlets de Malware Analysis en la vista Monitorear para ver rápidamente las amenazas potenciales más riesgosas.
- Puede ir a **Investigar > Malware Analysis** para abrir Resumen de eventos de Malware Analysis.
- Puede hacer clic con el botón secundario en una clave de metadatos en la vista Navegar y seleccionar **Escanear para encontrar malware**.

Consulte Realización de un análisis de malware para obtener detalles sobre cómo trabajar en la vista Malware Analysis.

Comenzar una investigación en las vistas Navegar o Eventos

La vista Navegar es la vista predeterminada de Investigate, a menos que haya seleccionado otra vista como la vista inicial. Esta preferencia del usuario se configura en el nivel de la aplicación, como se describe en Configuración de vistas y preferencias de NetWitness Investigate. En las vistas Navegar y Eventos, se buscan eventos de interés en función de una consulta. En la vista Navegar, también puede limitar los resultados, para lo cual debe hacer clic en las claves y los valores de metadatos. Cuando encuentra eventos de interés, puede observarlos más detenidamente en las demás vistas de Investigate.

Para comenzar una investigación en las vistas Navegar o Eventos, se debe especificar un servicio.

- NetWitness Platform abre las vistas Navegar o Eventos con el servicio predeterminado especificado por el usuario seleccionado.
- Si actualmente no se ha especificado ningún servicio predeterminado y el ID del servicio no se encuentra en la URL, NetWitness Platform presenta un cuadro de diálogo que permite seleccionar el servicio o la recopilación que se investigará.
- Cuando un servicio se seleccionó de forma manual o predeterminada en las vistas Navegar o Eventos, puede cambiar el servicio o la recopilación que se investigará mediante la selección del nombre del servicio en la barra de herramientas. NetWitness Platform presenta un cuadro de diálogo que permite seleccionar el servicio que se investigará.

Nota: El servicio Archiver no aparece en la vista Navegar para minimizar la experiencia del usuario de bajo rendimiento cuando se realizan investigaciones. Archiver está disponible en la vista Eventos para exportaciones de registros y mejora de funcionalidades de búsqueda.

Con una recopilación o un servicio seleccionados, NetWitness Platform está listo para cargar datos para el servicio o la recopilación. Se recomienda seleccionar también un rango de tiempo de modo que los resultados se carguen con mayor rapidez. Varios ajustes en el cuadro de diálogo Ajustes de configuración de las vistas Navegar y Eventos o en Perfiles > panel Preferencias > pestaña Investigaciones afectan el proceso de carga: Umbral, Número máximo de resultados de valores, Mostrar información de depuración, Cargar valores automáticamente y Optimizar cargas de la página Investigation (consulte Configuración de vistas y preferencias de NetWitness Investigate).

Nota: En la vista Eventos, los datos se cargan automáticamente. Si especificó Cargar valores automáticamente en las preferencias de la vista Navegar, NetWitness Platform completa los datos de forma automática. De lo contrario, debe seleccionar el botón Cargar valores. NetWitness Platform completa los metadatos en el panel Valores de la vista Navegar y los resultados se pueden ver casi de inmediato.

En el resto de este tema se proporcionan instrucciones para comenzar la investigación de datos de un servicio.

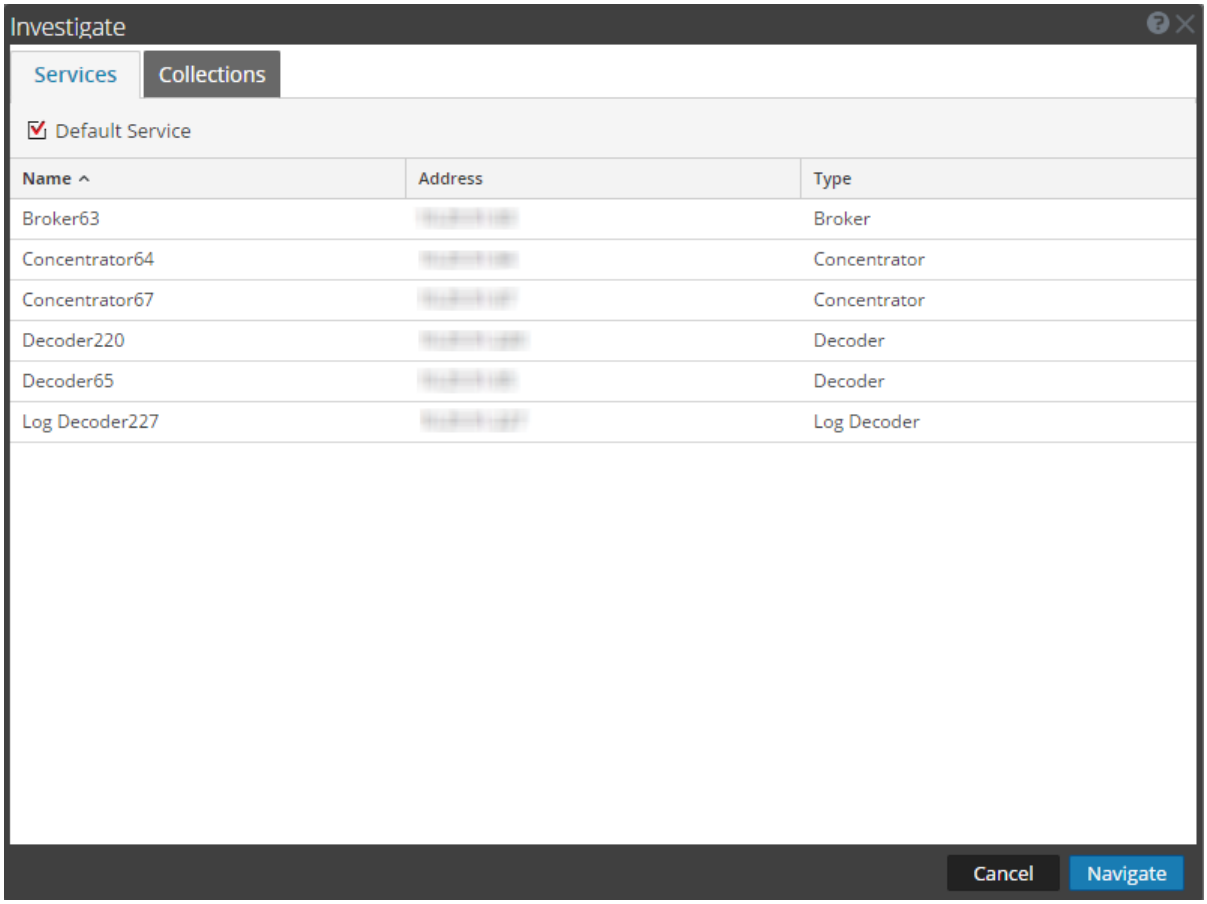
Nota: Solo los usuarios a los cuales se asignó la función de administrador pueden crear una recopilación y solo el creador de la recopilación puede investigarla.

Después de la carga de datos en las vistas Navegar o Eventos:

1. Limite los resultados, visualice datos y realice acciones en un punto de desglose (consulte Investigación de metadatos en la vista Navegar y Análisis de eventos crudos en la vista Eventos). Por ejemplo, puede Buscar contexto adicional en las vistas Navegar y Eventos, Iniciar un escaneo de Malware Analysis desde la vista Navegar o Agregar eventos a un incidente para Response.
2. Reconstruya un evento (consulte Reconstruir un evento) o vea el Análisis de eventos interactivo de un evento (consulte Comenzar una investigación en la vista Análisis de eventos).

Comenzar una investigación (sin servicio predeterminado)

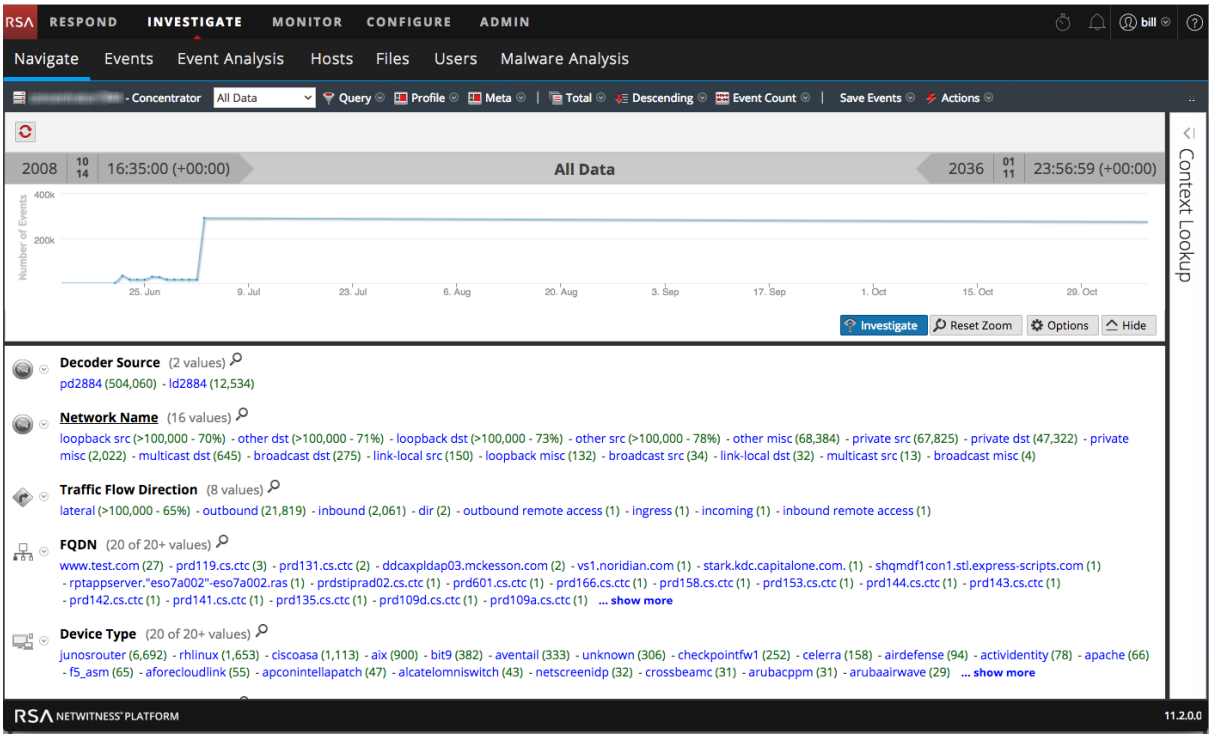
1. Vaya a **INVESTIGAR > Navegar** o **Eventos**.
   Se muestra el cuadro de diálogo Investigate.



2. Haga doble clic en un servicio o seleccione uno, por lo general, un Concentrator, y haga clic en **Navegar**.
   En la vista Eventos, los datos se cargan automáticamente. Si está trabajando en la vista Navegar, el panel resultante muestra la actividad que corresponde al servicio seleccionado, pero los datos no se cargan automáticamente.
3. (Recomendado) Seleccione un rango de tiempo específico de modo que los resultados se carguen con mayor rapidez.

4. Si desea modificar opciones de la investigación antes de realizar la carga, puede crear o modificar un perfil personalizado, aplicar otro rango de tiempo, crear o aplicar un grupo de metadatos y realizar una consulta personalizada como se describe en Consulta y realización de acciones en datos en las vistas Navegar y Eventos. También puede modificar las opciones en cualquier momento durante la investigación.

5. Para cargar datos en la vista Navegar, haga clic en Load Values.
   Comienza la carga de los datos del servicio seleccionado.

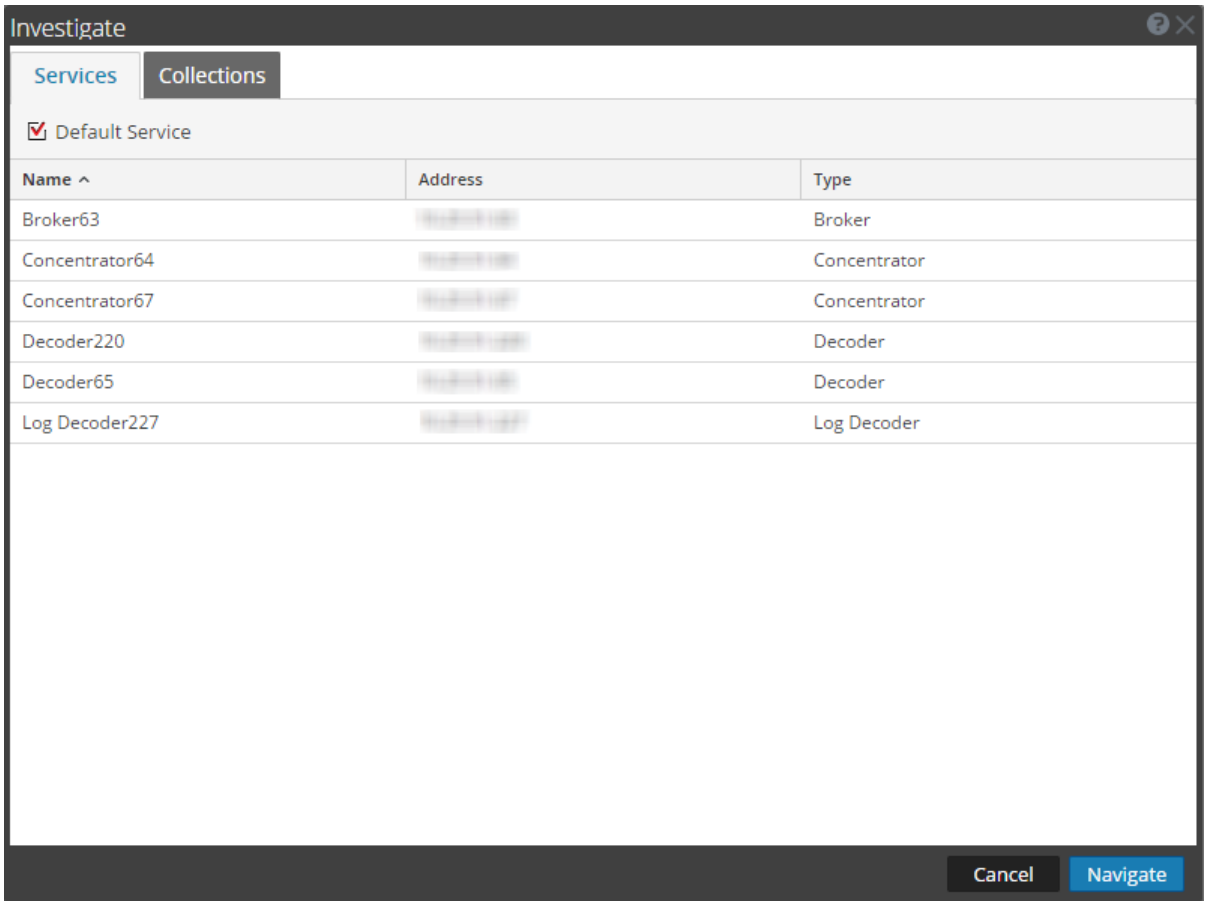


   Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos.

Configurar o borrar el servicio predeterminado

Puede configurar o borrar el servicio predeterminado en el cuadro de diálogo Investigar un servicio.

1. Haga clic en el nombre del servicio en la barra de herramientas.
   Se muestra el cuadro de diálogo Investigate.



2. Seleccione un servicio en la cuadrícula **Servicios** y haga clic en Default Service.
   El servicio se convierte en el valor predeterminado (como lo indica **Valor predeterminado** entre paréntesis después del nombre del servicio).
3. Para borrar el servicio predeterminado, selecciónelo en la cuadrícula y haga clic en Default Service y, a continuación, haga clic en **Cancelar** para cerrar el cuadro de diálogo.
   No se configura un servicio predeterminado.

> **Nota:** El botón Cancelar no cancela la selección del servicio predeterminado. Simplemente cierra el cuadro de diálogo sin tener que navegar al servicio seleccionado actualmente en la cuadrícula. La configuración de un servicio predeterminado que es diferente del servicio que se investiga en la actualidad, no actualiza la vista Navegar. Debe seleccionar explícitamente y navegar a un servicio diferente.

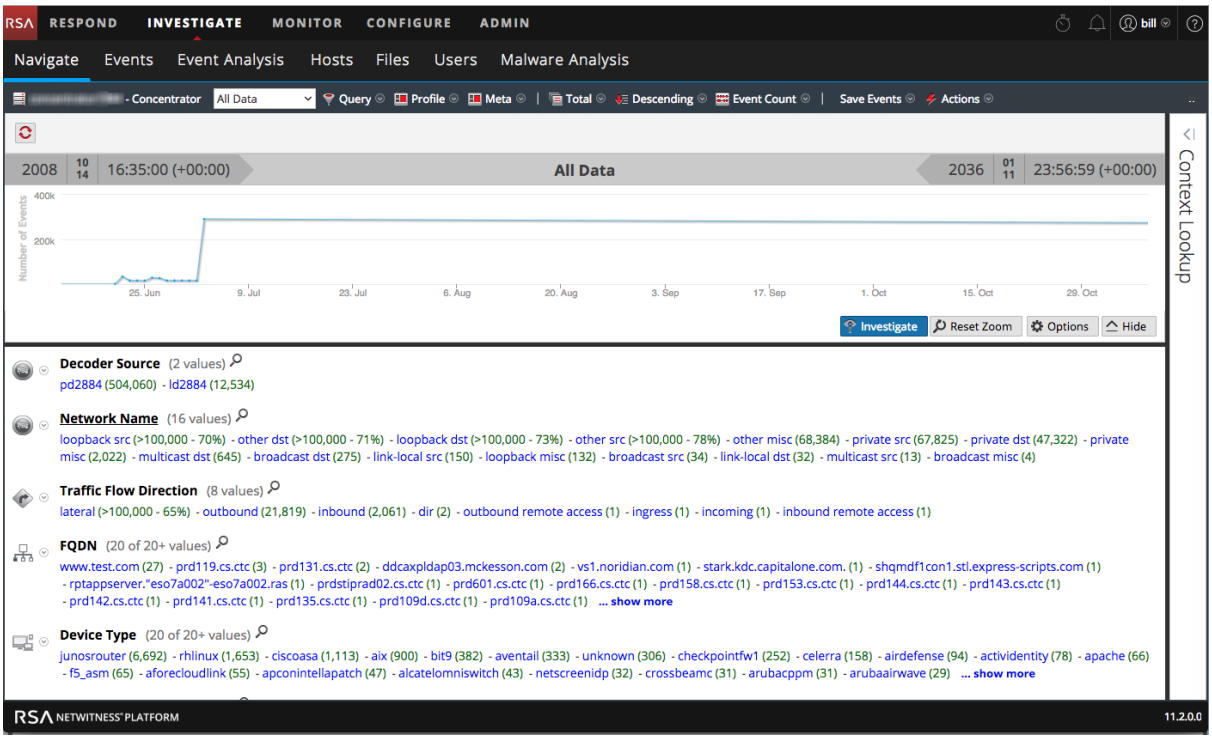
Comenzar una investigación (se especifica el servicio predeterminado)

1. Vaya a **INVESTIGAR > Navegar** o **Eventos**.
   Si el ajuste de Cargar valores automáticamente está desactivado, la vista Navegar se muestra con el servicio predeterminado seleccionado y listo para cargar datos. Si el ajuste Cargar valores automáticamente está activado, los valores se cargan como se muestra en el paso 3. En la vista

Eventos, los datos se cargan automáticamente.

2. Si desea modificar opciones de la investigación en la vista Navegar antes de realizar la carga, puede crear o modificar un perfil personalizado, aplicar otro rango de tiempo, crear o aplicar un grupo de metadatos y realizar una consulta personalizada.

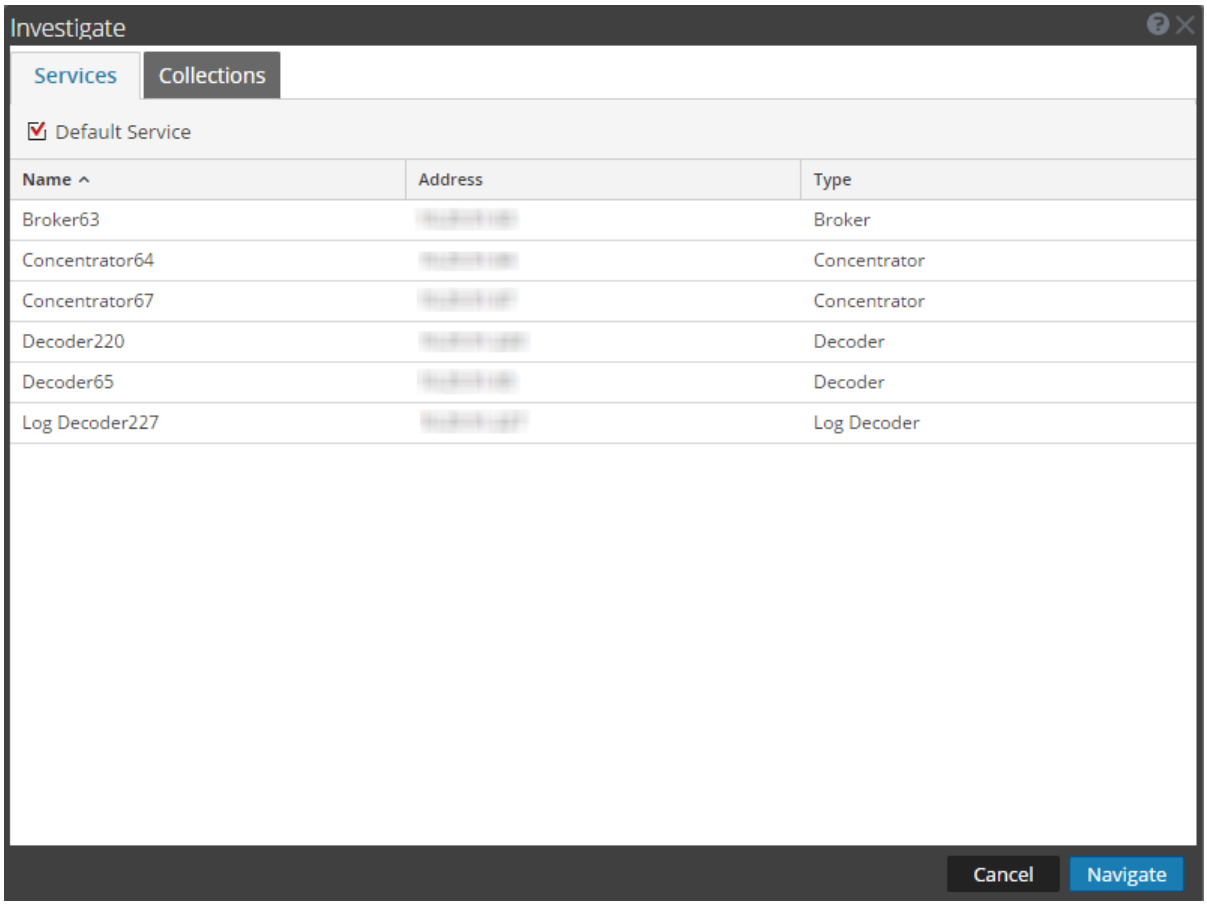
3. Cuando esté listo, haga clic en Load Values.
   Los valores del servicio se cargan de acuerdo con las opciones seleccionadas.



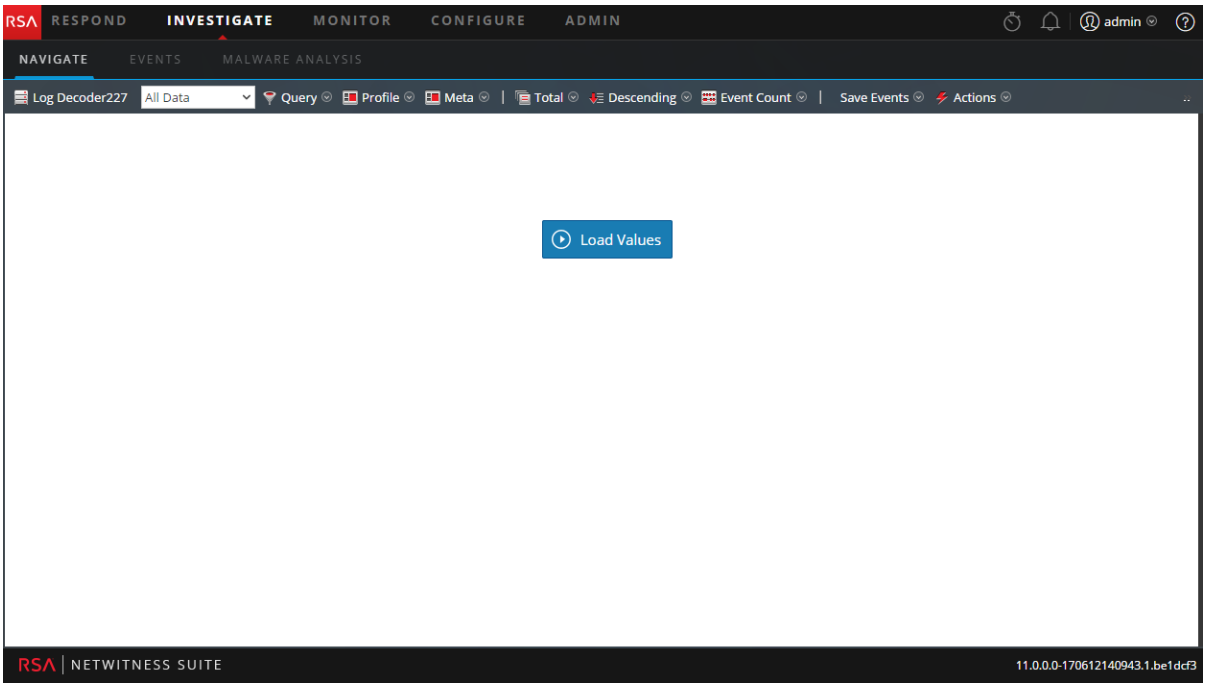
Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos.

Cambiar el servicio o la recopilación que se investigará

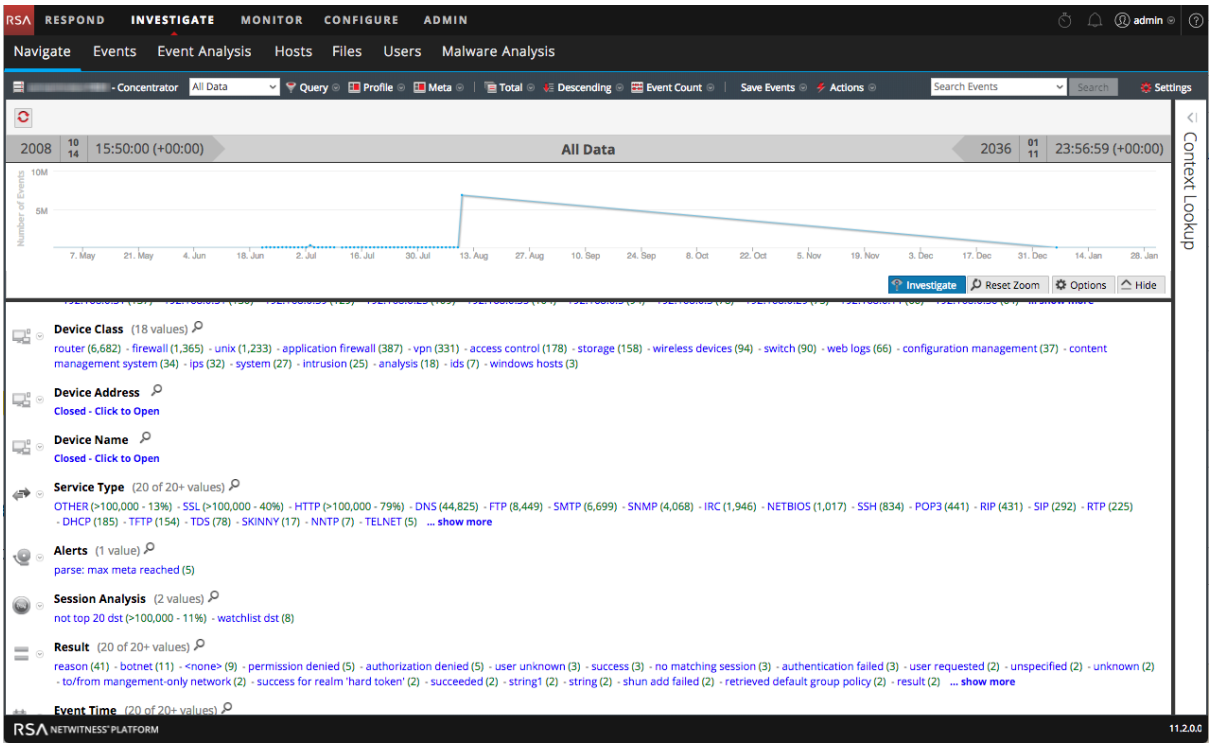
1. En las vistas Navegar o Eventos, haga clic en el nombre del servicio en la parte superior del panel de opciones.
   Se muestra el cuadro de diálogo Investigate.



2. Haga doble clic en un servicio o seleccione uno y haga clic en **Navegar**. El panel resultante muestra la actividad del servicio seleccionado.
   Si el ajuste Cargar valores automáticamente está activado, los valores se cargan como se muestra en el paso 3. De lo contrario, la vista Navegar se muestra con el servicio predeterminado seleccionado y los datos listos para cargarse. En la vista Eventos, los datos se cargan automáticamente.



3. Cuando esté listo, haga clic en Load Values.
   Los valores del servicio comienzan a cargarse de acuerdo con las opciones seleccionadas.



Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos.

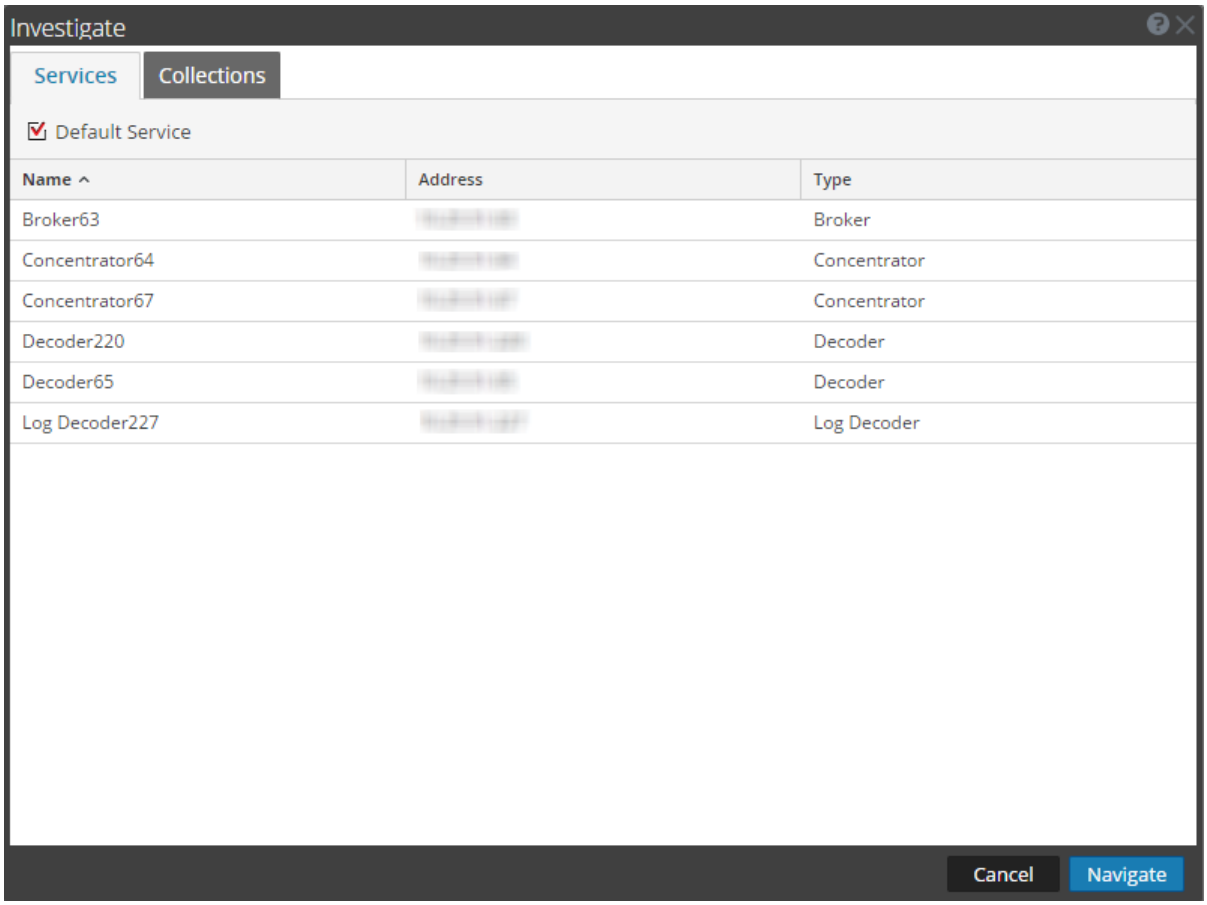
Investigar recopilaciones de restauración de Workbench

Este procedimiento permite que los administradores seleccionen contenido de una recopilación existente que se volverá a procesar para realizar una investigación más detallada. Esto se aplica a los Decoders que usan servicios de Workbench.

Nota: Solo un usuario con privilegios administrativos puede crear una recopilación y usted solo puede ver las recopilaciones que creó.

Para volver a procesar los datos con el fin de realizar una investigación más detallada:

1. Vaya a **INVESTIGAR > Navegar** o **Eventos**.
   Se muestra el cuadro de diálogo Investigate.



2. Seleccione un servicio de Workbench y un nombre de Workbench que desee investigar.
3. Haga clic en **Navegar** para realizar una investigación sobre el servicio de Workbench que seleccionó.
   Haga clic en **Cancelar** para seleccionar otro servicio de Workbench que se investigará.
   Se muestra la vista Investigación.
   Con la recopilación seleccionada y los datos cargados, está listo para comenzar a analizar los datos.

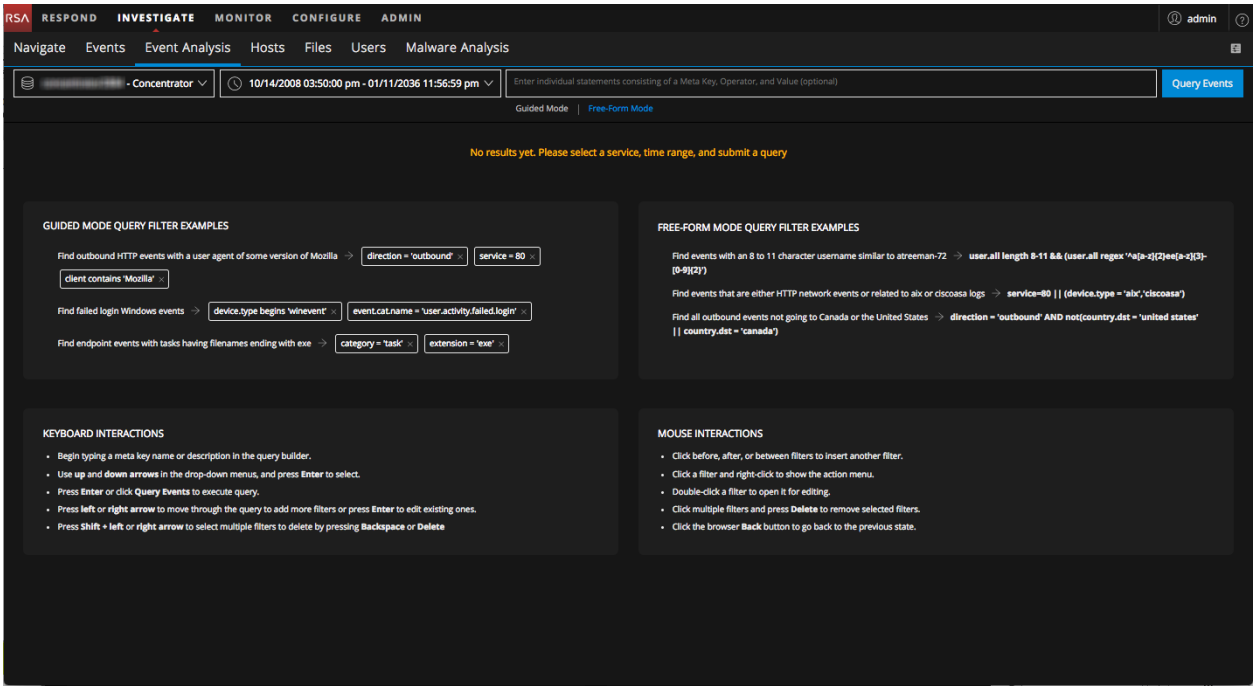
Comenzar una investigación en la vista Análisis de eventos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

La vista Análisis de eventos ofrece la mayoría de las funciones que están disponibles en las vistas Navegar y Eventos. De manera similar a la vista Navegar, hay una vista de las claves y los valores de metadatos para los registros, los terminales y los paquetes. Al igual que en la vista Eventos, una lista de eventos muestra los eventos enumerados por hora y permite ver el evento crudo, los metadatos relacionados y una reconstrucción de un evento. La reconstrucción de Análisis de eventos tiene algunas indicaciones útiles para identificar los puntos de interés en una reconstrucción. Consulte Análisis de eventos crudos y metadatos en la vista Análisis de eventos.

Nota: En la versión 11.0, no puede comenzar una investigación en la vista Análisis de eventos. En lugar de esto, debe comenzar la investigación en las vistas Navegar o Eventos y, a continuación, abrir un evento en la vista Análisis de eventos. En la versión 11.1, un submenú INVESTIGAR otorga acceso directo a la vista Análisis de eventos, junto con la capacidad de seleccionar un servicio y un rango de tiempo diferentes, y de crear una consulta.

En la siguiente ilustración se muestra la vista Análisis de eventos inicial con un mensaje de globo en el que se proporcionan ejemplos de consultas.



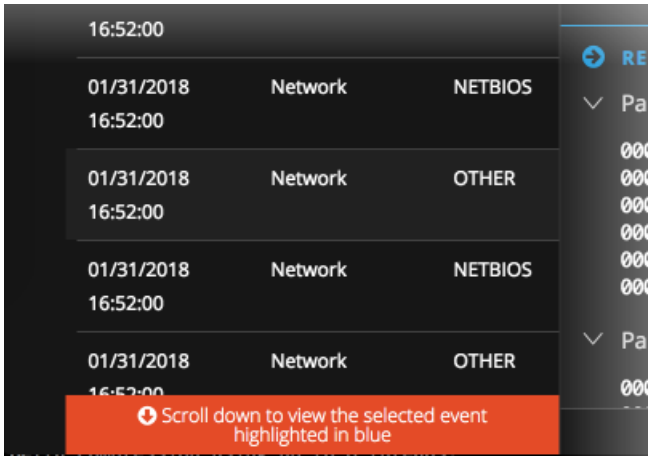
Acceder a la vista Análisis de eventos (versión 11.1 y superior)

En la versión 11.1 están disponibles varias maneras de acceder a la vista Análisis de eventos.

- Cuando utiliza la opción **Acciones > Ir a evento en Análisis de eventos** en la vista Navegar e ingresa un ID de evento, la vista Análisis de eventos abre este evento como una reconstrucción. Para

simplificar la vista, la barra de herramientas no incluye las opciones innecesarias para ampliar, contraer y cerrar ventanas. Puede comenzar a trabajar como se describe en Análisis de eventos crudos y metadatos en la vista Análisis de eventos.

- Cuando coloca el cursor sobre un conteo (el número verde después de un valor de metadatos) en la vista Navegar y hace clic en **Abrir Análisis de eventos en una pestaña nueva**, la vista Análisis de eventos se abre con la lista de eventos para el punto de desglose seleccionado y usted puede comenzar a trabajar como se describe en Análisis de eventos crudos y metadatos en la vista Análisis de eventos. La lista de eventos puede ser muy grande y existe la posibilidad de que el evento que seleccionó no esté visible en la página de eventos actual. En este caso, un mensaje le advierte de debe desplazarse hacia abajo para ver el evento.

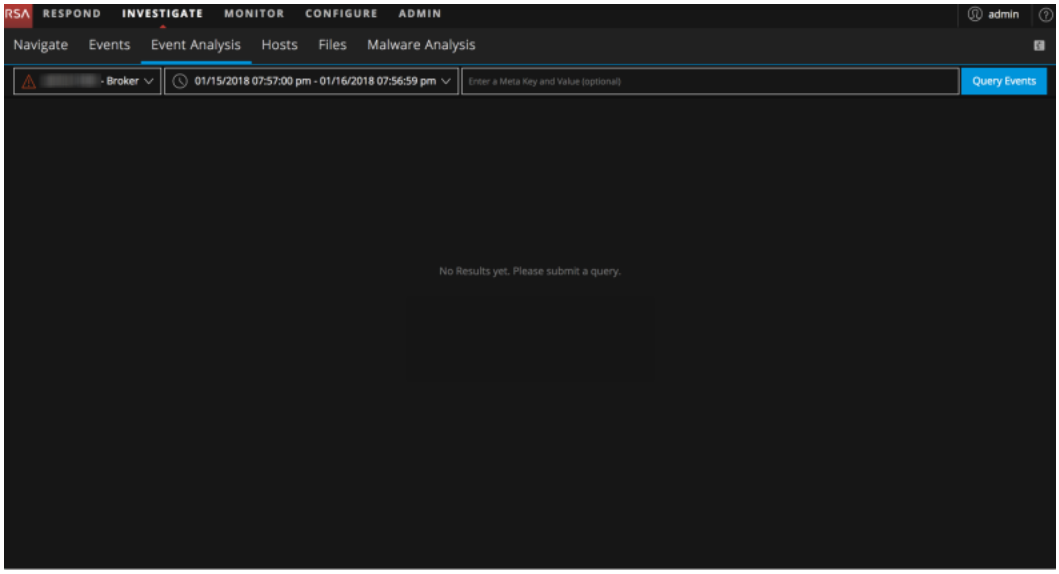


- También puede acceder a la vista Análisis de eventos si va directamente a **INVESTIGAR > Análisis de eventos** o si va a **INVESTIGAR** en caso de que haya configurado la vista Análisis de eventos como la vista inicial de Investigate. Cuando abre la vista Análisis de eventos por primera vez, debe seleccionar un servicio para comenzar el análisis. Si esta no es la primera vez que abre Análisis de eventos, se recuerda el último servicio utilizado hasta que se borra la caché del navegador. Cuando abre la vista Análisis de eventos desde una de las otras vistas de Investigate, el servicio y la consulta de esa vista están vigentes. Puede cambiar el servicio, seleccionar un rango de tiempo e ingresar una consulta si desea limitar los resultados antes de abrir la vista Análisis de eventos, como se describe en Filtrar los resultados en la vista Análisis de eventos.

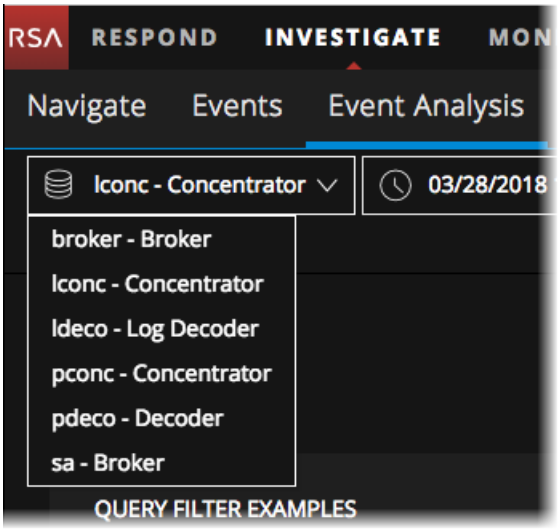
Para acceder directamente a la vista Análisis de eventos:

1. Vaya a **INVESTIGAR** > **Análisis de eventos**.
   La vista Análisis de eventos se abre con el primer servicio de la lista de servicios seleccionado y sin datos mostrados. El campo **Seleccionar un servicio** se completa inicialmente con el primer servicio de la lista o con el último servicio seleccionado. Un menú desplegable ofrece una lista de servicios disponibles en orden alfabético. De forma predeterminada, la lista de servicios disponibles se recupera cada 12 horas y se almacena en caché en el servidor de NetWitness. Si un servicio se agrega o se quita del servidor de NetWitness, la caché se actualiza con la lista de servicios más reciente. Al principio del campo, un icono proporciona el estado de la consulta.

- y sin nombre de servicio = no hay ningún servicio seleccionado.
- y nombre de servicio seleccionado = el servicio está seleccionado.
- = Investigate está intentando conectarse al servicio seleccionado.
- = Investigate no puede conectarse al servicio seleccionado o no hay datos. En este estado, el control del selector de servicios también se vuelve rojo y un mensaje de globo explica por qué falló el intento de conexión y recomienda elegir otro servicio.

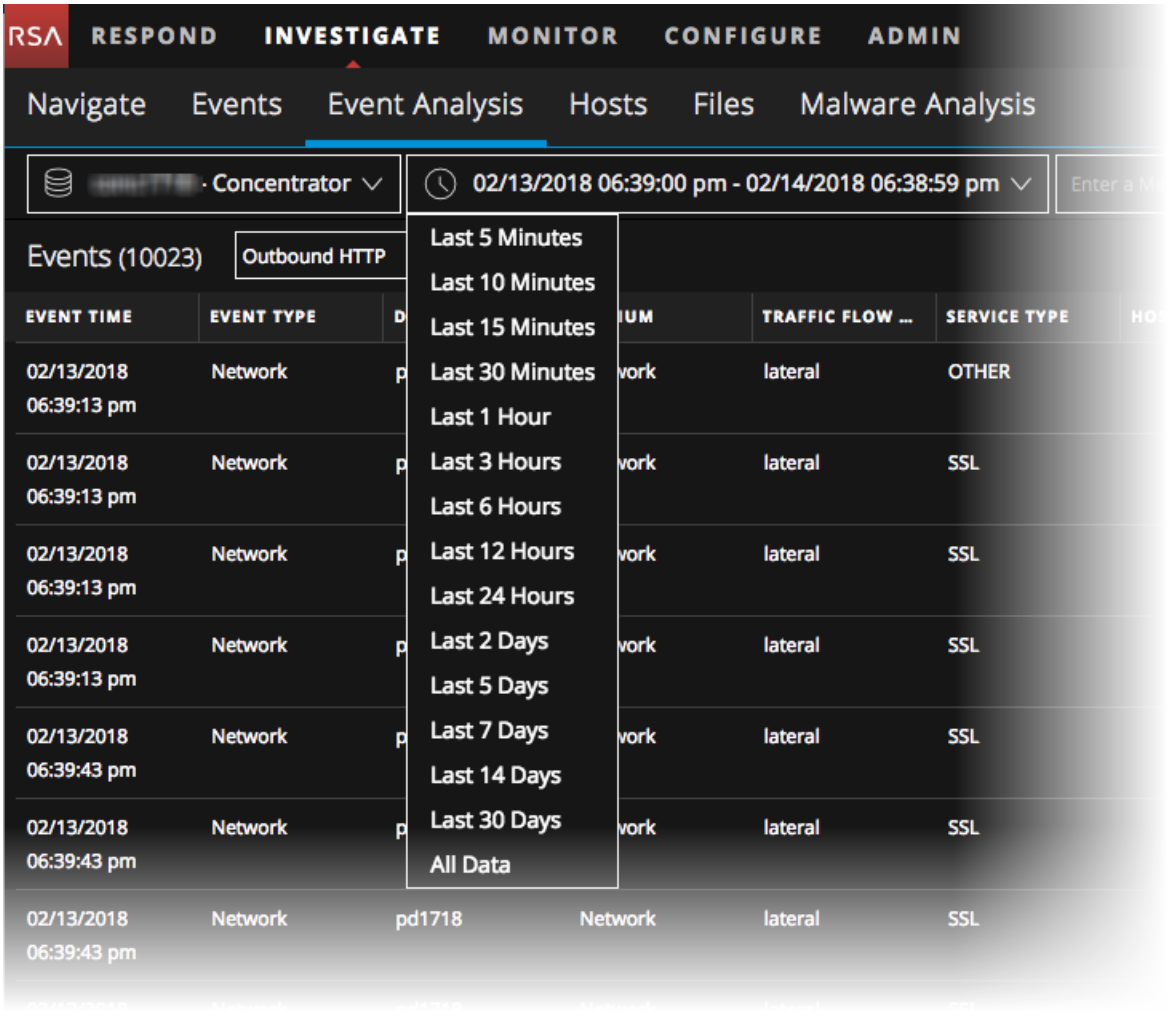


2. (Opcional) Seleccione un servicio, por lo general, un Concentrator, en la lista desplegable.



El selector del rango de tiempo muestra el rango de tiempo predeterminado de 24 horas o el rango de tiempo que usted seleccionó por última vez para este servicio. El botón Consultar eventos se activa y usted puede ingresar filtros. Si inicia una consulta ahora, se utiliza la hora seleccionada.

3. (Opcional) Para seleccionar un rango de tiempo desde el selector de Rango de tiempo, haga clic en el selector de **Rango de tiempo** y seleccione un rango de tiempo en la lista desplegable. Las opciones son Últimos 5, 10, 15 o 30 minutos; las Últimas 1, 3, 6, 12 o 24 horas; los Últimos 2, 5, 7, 14 o 30 días o Todos los datos. (El rango de tiempo se basa en las preferencias configuradas para la vista Análisis de eventos. La base predeterminada para el rango de tiempo es la hora de la base de datos; puede cambiarla a la hora del reloj).
   El rango de tiempo seleccionado se almacena en el navegador para este servicio; puede configurar distintos rangos de tiempo para distintos servicios.

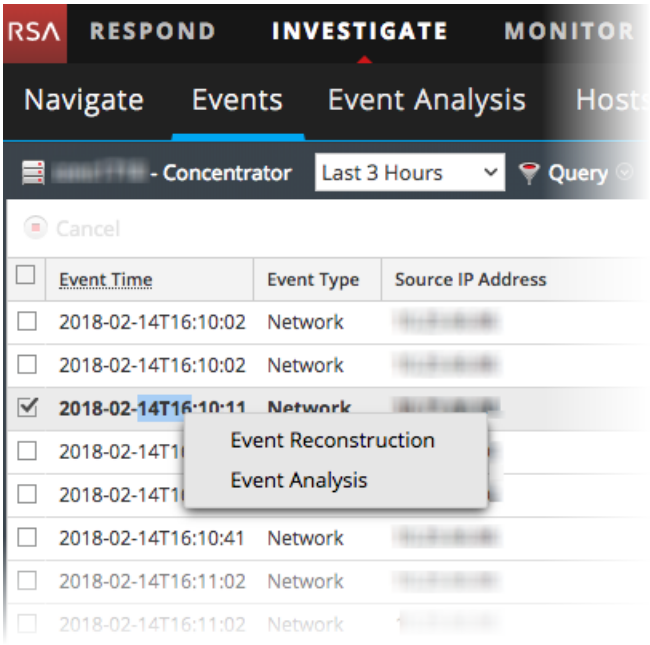


4. Escriba una consulta mediante la creación de uno o más filtros que incluyan, como mínimo, una clave o una entidad de metadatos, un operador y un valor opcional. Consulte Filtrar los resultados en la vista Análisis de eventos para obtener detalles acerca del ingreso de consultas.
5. Haga clic en **Consultar eventos**.
   La vista Análisis de eventos muestra la actividad del servicio seleccionado y el rango de tiempo, de acuerdo con los permisos que el administrador asignó a su función. Con el servicio seleccionado y los datos cargados, está listo para comenzar a analizar los datos. Consulte Análisis de eventos crudos y metadatos en la vista Análisis de eventos para aprender a trabajar en la vista Análisis de eventos.

Acceder a la vista Análisis de eventos (versión 11.0)

Para abrir un evento en la vista Análisis de eventos:

1. Vaya a **INVESTIGAR** > **Eventos**.
2. Haga clic con el botón secundario en un evento entre los enumerados y seleccione **Análisis de eventos**.



Consulte Análisis de eventos crudos y metadatos en la vista Análisis de eventos para aprender a trabajar en la vista Análisis de eventos.

Investigación de metadatos en la vista Navegar

Cuando se realiza una investigación en la vista Navegar, los analistas tienen varios métodos, específicos de la vista Navegar, para limitar los resultados, visualizar los datos y actuar sobre los datos.

- Filtrar resultados en la vista Navegar
- Administrar grupos de metadatos
- Visualizar metadatos como coordenadas paralelas
- Abrir un evento en la lista de eventos
- Exportar o imprimir un punto de desglose
- Iniciar una búsqueda externa de una clave de metadatos
- Iniciar un escaneo de Malware Analysis desde la vista Navegar
- Visualizar el punto de desglose actual en Informer

Además, puede utilizar estos métodos para consultar datos y actuar sobre los resultados que son comunes para las vistas Navegar y Eventos.

- Buscar patrones de texto
- Crear una consulta personalizada
- Ver y modificar consultas mediante la integración de URL
- Usar perfiles para encapsular vistas personalizadas
- Administrar listas y valores de lista de Context Hub en las vistas Navegar y Eventos
- Buscar contexto adicional en las vistas Navegar y Eventos
- Reconstruir un evento

Filtrar resultados en la vista Navegar

Cuando se realiza una investigación en la vista Navegar, están disponibles varios métodos para limitar los resultados que se muestran cuando se cargan valores de claves de metadatos en esta vista. Los métodos básicos de filtrado disponibles para los analistas son los siguientes:

- Establecer el rango de tiempo
- Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos
- Administrar y aplicar claves de metadatos predeterminadas en una investigación
- Desglosar a datos en gráfico de tiempo de la vista Navegar
- Desglosar a datos en el panel Valores

El resto de este tema se centra en los métodos básicos de filtrado de datos. Además, métodos más avanzados permiten configurar grupos de metadatos, perfiles y visualizaciones de coordenadas paralelas.

- Visualizar metadatos como coordenadas paralelas
- Administrar grupos de metadatos
- Usar perfiles para encapsular vistas personalizadas

Se proporciona un tema aparte para cada uno de los métodos más avanzados.

Establecer el rango de tiempo

Cuando se realiza una investigación en la vista Navegar, las opciones de rango de tiempo limitan los resultados devueltos. Puede seleccionar:

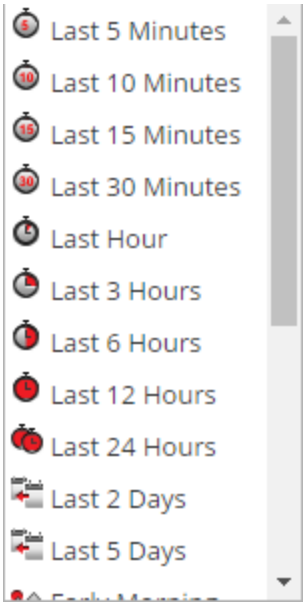
- Un rango de tiempo relativo a la recopilación. Los rangos relativos a la recopilación se basan en la última hora de recopilación de datos.
- Un rango de tiempo relativo al calendario.
- Un rango de fechas personalizado.
- Todos los datos.

El Rango de fechas seleccionado se muestra en la barra de herramientas de la vista Navegar como la etiqueta Rango de tiempo; de forma predeterminada, la etiqueta es **Últimas 3 horas**. El Rango de tiempo que aparece en el anuncio de cronología muestra el primer y el último registro de fecha y hora del rango de fechas que se está utilizando para los metadatos.

Nota: El rango de tiempo se basa en la zona horaria configurada en el panel Preferencias de perfil, como se describe en “Configuración de las preferencias del usuario” en la *Guía de introducción de RSA NetWitness Platform*.

Para seleccionar un rango de tiempo incorporado:

1. Haga clic en la opción **Rango de tiempo** de la barra de herramientas de la vista Navegar. El rango de tiempo predeterminado es para las **Últimas 3 horas**, pero es posible que ya haya un valor distinto seleccionado en la lista de selección, por ejemplo, **Todos los datos** o **Última hora**, y puede que se utilice como etiqueta en el panel de opciones.
   Se muestra la lista de selección Rango de tiempo.



2. Realice una de las siguientes acciones:
   - Si desea ver todos los datos, seleccione **Todos los datos**.
   - Si desea establecer un rango de tiempo relativo a la recopilación en minutos, horas o días, seleccione un valor como **Últimos 10 minutos**, **Últimas 3 horas** o **Últimos 5 días**.
   - Si desea establecer un rango de tiempo relativo a hoy, seleccione **Ayer**, **Esta semana** (versión 11.1), **La semana pasada** (versión 11.1), **Todo el día** o una parte del día, como **Primera hora**, **Mañana**, **Tarde** o **Noche**.
   - Si desea establecer un rango de fechas único, seleccione **Personalizado** en el menú **Rango de tiempo** y siga el procedimiento que aparece a continuación.
     El rango de tiempo seleccionado se aplica a los resultados actuales del panel Valores.

Para especificar un rango de tiempo personalizado:

1. Seleccione **Personalizado** en el menú **Rango de tiempo**.
   Las opciones de selección de fecha se muestran en la barra de herramientas.

2. Dentro de los campos de tiempo **Fecha inicial** y **Fecha de finalización**, realice lo siguiente para especificar la fecha y la hora:

a. Haga clic en una fecha del calendario.

b. (Opcional) Seleccione la hora en los campos Hora y Minuto o haga clic en **Ahora**. La selección de la hora se configura de manera predeterminada en la hora actual.

Nota: El valor de la hora de inicio en segundos se configura siempre de manera predeterminada en :00 y el valor de la hora de finalización en segundos se configura siempre de manera predeterminada en :59. Por ejemplo, si está usando la hora para desglosar a un problema, la hora de desglose se interpreta como "HH:MM:00 - HH:MM:59".

3. Para aplicar el rango, haga clic en **Ir**.
   El rango de tiempo seleccionado se aplica a los resultados actuales del panel Valores.

Establecer el método de cuantificación y la secuencia de clasificación de resultados de claves de metadatos

Puede seleccionar la forma en que se cuantifican y se secuencian los resultados de cada clave de metadatos en la vista Navegar.

Nota: Si se utilizan entidades de metadatos (versión 11.1 y superior) en grupos de metadatos, los resultados mostrarán los 20 valores principales que coincidieron con cualquiera de las claves de metadatos contenidas en la entidad de metadatos.

Cada sección de clave de metadatos en la vista Navegar contiene una lista de valores ordenada que muestra cada valor de clave de metadatos (Valor) y su conteo (Total). Puede especificar si:

- Los resultados de cada sección Clave de metadatos se clasifican según Valor o Total.
- Los resultados se clasifican en orden ascendente o descendente.
- Los valores que se muestran para cada clave de metadatos se cuantifican por cantidad de paquetes (Conteo de paquetes), cantidad de sesiones o registros (Cuantificar por conteo de eventos) o tamaño de los eventos (Cuantificar por tamaño de evento).

Nota: Si tiene un Log Decoder y un Packet Decoder cuyos metadatos observa, el cálculo de lo que se cuenta realmente depende del tipo de clave. Si opta por Cuantificar por conteo de paquetes y observa los registros, la salida de la vista Navegar es la misma que si hubiera seleccionado Cuantificar por conteo de eventos (consulte Vista Navegar para obtener detalles).

En esta imagen se muestra la clave de metadatos `Event Type` clasificada por **Total** en orden **Descendente**. El valor con el mayor conteo de coincidencias se presenta primero. El valor `failure audit` tiene 71 coincidencias y se enumera primero. El valor `logon` solo tiene una coincidencia y se presenta al final. El método de cuantificación es **Conteo de eventos**.

En esta imagen se muestran las claves de metadatos `Event Type` clasificadas por **Valor** en orden **Descendente**. Los nombres de los valores se presentan en orden alfabético a partir del final del alfabeto. El valor `success audit` se enumera primero. El valor `connect` se presenta al final. El método de cuantificación es **Conteo de eventos**.

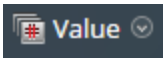
Para seleccionar el método de cuantificación de conteo de claves de metadatos y el orden de los resultados de claves de metadatos que se muestran en la vista Navegar:

1. En la barra de herramientas, seleccione **Conteo de eventos, Tamaño de evento** o **Conteo de paquetes** y elija una de las opciones de cuantificación del menú desplegable. La etiqueta del menú muestra la opción seleccionada.

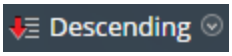
   La vista actual se vuelve a cargar de acuerdo con su selección.

2. En la barra de herramientas, seleccione **Total** o **Valor** y elija uno de los métodos de orden en el menú desplegable. La etiqueta del menú muestra la opción seleccionada.

   La vista actual se vuelve a cargar de acuerdo con su selección.

3. En la barra de herramientas, seleccione **Ascendente** o **Descendente** y elija una de las opciones de orden de clasificación del menú desplegable. La etiqueta del menú muestra la opción seleccionada.
   La vista actual se vuelve a cargar de acuerdo con su selección.

Administrar y aplicar claves de metadatos predeterminadas en una investigación

Cuando los analistas realizan una investigación de datos capturados en Investigation, se carga un conjunto de claves de metadatos predeterminado, el cual se muestra en una secuencia predeterminada en la vista Navegar > panel Valores. La secuencia y el contenido predeterminados se basan en las claves de metadatos del servicio que se investiga. Los analistas pueden especificar las claves de metadatos para mostrar durante la navegación mediante la selección de las claves de metadatos predeterminadas o de un grupo de claves de metadatos definido por el usuario, que proporciona una gran flexibilidad para definir claves de metadatos. Esto puede ayudar a desglosar más directamente los datos deseados y reducir el tiempo de carga mediante la prevención de la carga de metadatos que no es de interés en la investigación actual.

Nota: En la versión 11.1 y superior, cuando se usan claves de metadatos, también se pueden usar entidades de metadatos configuradas.

Si ningún grupo de metadatos personalizado está vigente, la vista Navegar se muestra con la visibilidad de claves de metadatos especificada en el cuadro de diálogo Claves de metadatos predeterminadas. Para optimizar la carga de claves de metadatos en la vista Navegar > panel Valores, NetWitness Platform no abre claves de metadatos no indexadas de forma predeterminada. Cuando abre una clave de metadatos no indexada en la vista Valores, NetWitness Platform comienza a cargar valores para esa clave de metadatos. Si el tiempo de carga es excesivo, el tiempo de espera de la carga de las claves de metadatos se agota con un mensaje. El título, los valores y los conteos de las claves de metadatos no indexadas no se pueden desglosar en el panel Valores. El etiquetado adicional en Investigation identifica las claves de metadatos no indexadas.

Para seleccionar las claves de metadatos que se aplicarán en su investigación, puede realizar lo siguiente:

- Seleccionar las claves de metadatos predeterminadas.
- Seleccionar un conjunto de claves de metadatos, lo que se denomina un grupo de metadatos.

Nota: Investigate tiene grupos de metadatos incorporados y grupos de metadatos definidos por el usuario. Una vez creados, los grupos de metadatos definidos por el usuario se pueden editar, eliminar, exportar para su uso en otros servicios e importar al servicio que se está investigando. Todos estos procedimientos están dentro de un tema aparte: Administrar grupos de metadatos.

El cuadro de diálogo Claves de metadatos predeterminadas permite especificar la vista predeterminada y mostrar la secuencia de claves de metadatos durante la navegación en la vista Investigate > Navegar para un servicio específico. En el caso de cada clave o de todas las claves, puede establecer la vista predeterminada en:

- Oculta: Los resultados de la clave de metadatos predeterminada se ocultan y no están disponibles para carga.
- Abierto: Los resultados de la clave de metadatos predeterminada son abiertos y se muestran todos los valores y conteos.
- Cerrada: Los resultados de la clave de metadatos predeterminada son cerrados, solamente se puede ver el nombre de los metadatos.
- Automática: La carga de claves de metadatos predeterminadas se controla mediante el nivel de índice, el cual debe indexarse según valor.

Cuando use las claves de metadatos predeterminadas, tenga presente que se pueden modificar para distintos servicios y que es posible que no vea el mismo conjunto de claves de metadatos predeterminadas cuando navegue a un punto de desglose en diferentes servicios. Si no ve los datos que espera, puede ser necesario cambiar la vista inicial de las claves de metadatos predeterminadas.

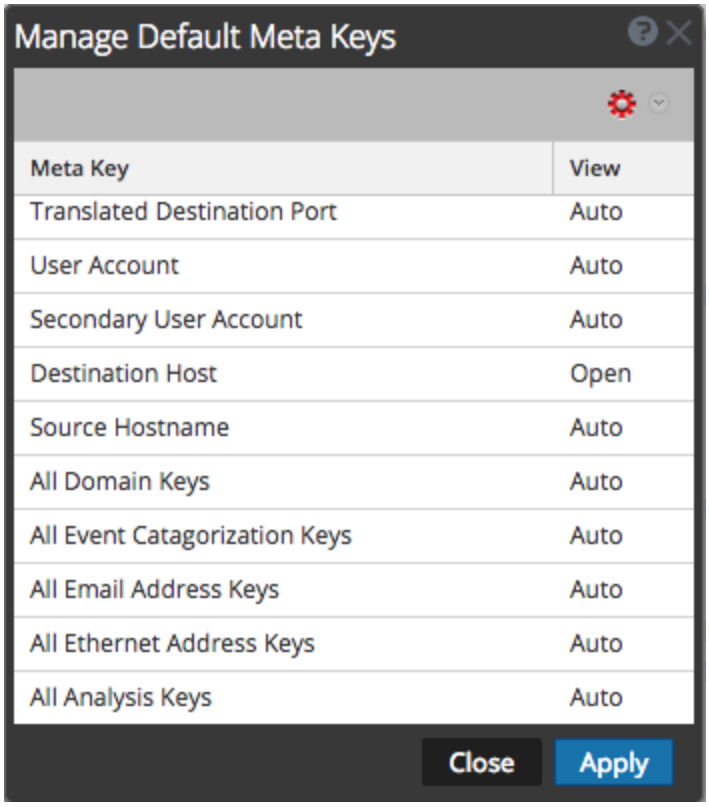
Cuando cambia el estado inicial de las claves de metadatos predeterminadas en la vista Navegar, el cambio persiste para ese servicio. Cuando se agregan claves nuevas al archivo de índice personalizado para un servicio principal (por ejemplo, `concentrator-custom-index.xml` o `decoder-custom-index.xml`), las claves nuevas se agregan a la lista de claves de metadatos predeterminadas. Los cambios que hace en la vista Navegar se aplican solo al servicio actual.

Para especificar que la vista Navegar inicial se abra con las claves de metadatos predeterminadas:

1. Vaya a **INVESTIGAR** > **Navegar**.
2. Seleccione un servicio y elija **Navegar**.
3. En el menú **Metadatos**, seleccione **Usar claves de metadatos predeterminadas**.
   Si hay una investigación en curso, los datos se vuelven a cargar en la vista actual y un ícono resalta la opción seleccionada. Si aún no se cargan datos, las claves de metadatos predeterminadas se usan para la carga siguiente.

Para configurar la vista predeterminada de claves de metadatos predeterminadas en la vista Navegar:

1. En la barra de herramientas de la vista **Navegar**, seleccione **Metadatos** > **Administrar claves de metadatos predeterminadas**.
   El cuadro de diálogo Administrar claves de metadatos predeterminadas se muestra con la lista de claves de metadatos disponibles para el servicio.



2. (Opcional) Para cambiar el orden de las claves, seleccione una o más claves y arrastre los valores hacia arriba o hacia abajo por la lista de claves.
3. Realice una de las siguientes acciones:
   - (Opcional) Para cambiar la vista predeterminada de todas las claves de metadatos, asegúrese de que no se haya seleccionado ninguna clave y, en la barra de herramientas, seleccione .
   - (Opcional) Para cambiar la vista predeterminada de una o más claves, seleccione las claves y, en la barra de herramientas, seleccione .
     Se muestra una lista desplegable de las posibles vistas iniciales de todas las claves de metadatos predeterminadas.
   - (Opcional) Para volver a la vista predeterminada de claves de metadatos como se especifica en el archivo de índice del servicio, asegúrese de que no esté seleccionada ninguna clave y, en la barra de herramientas, seleccione > **Automático**.
     Cuando modifica la vista predeterminada para una clave de metadatos no indexada, no puede configurar la clave en ABIERTO. Si cambia a ABIERTO la vista predeterminada para un grupo

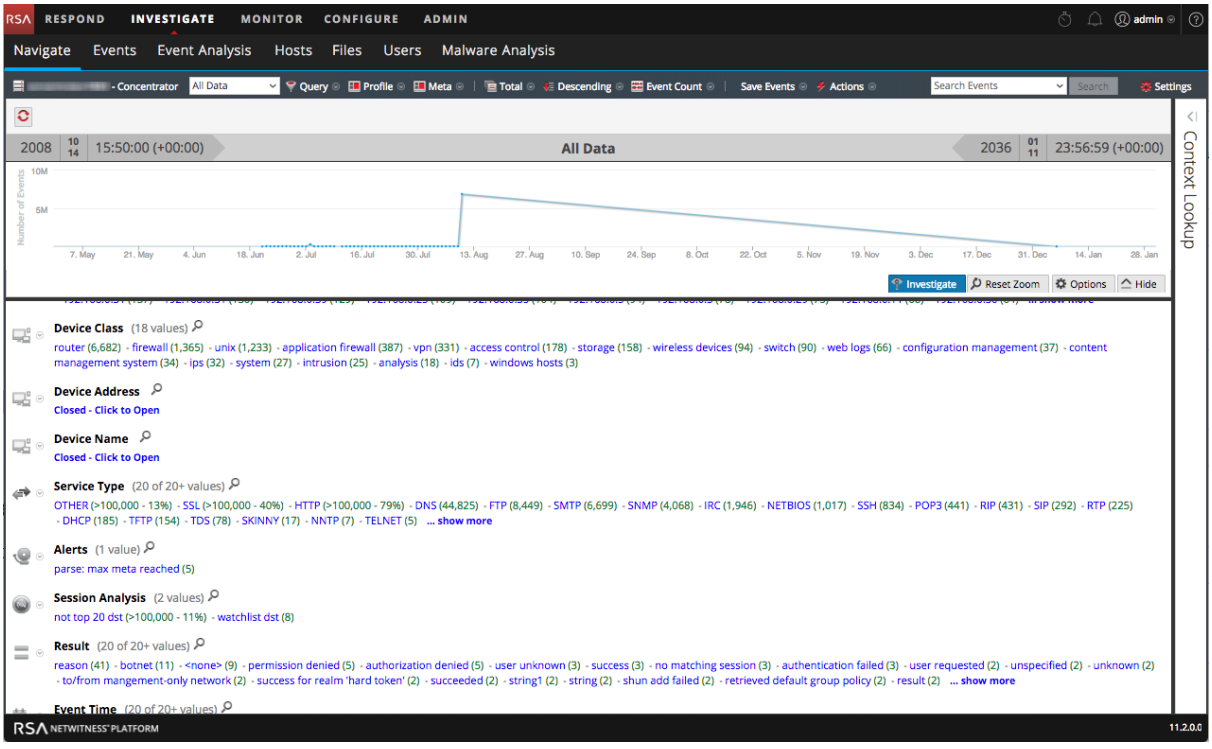
de claves de metadatos y algunas de las claves de metadatos no están indexadas, estas claves vuelven a AUTOMÁTICO. En consecuencia, la clave de metadatos se carga automáticamente solo si está indexada, y las claves de metadatos no indexadas se CIERRAN hasta que se abren de forma manual.

4. Seleccione una de las vistas.
5. Para guardar los cambios, haga clic en **Aplicar**.
   Las claves de metadatos que se muestran en la vista Navegar están ajustadas a sus especificaciones. Si las claves de metadatos predeterminadas están ocultas, los valores de las claves de metadatos no se muestran en la investigación en absoluto. Si las claves de metadatos predeterminadas están cerradas, los valores de las claves de metadatos no se cargan de forma predeterminada, pero puede cargar las claves de metadatos individuales de forma manual en la vista Navegar.

Desglosar a datos en gráfico de tiempo de la vista Navegar

La visualización Gráfico de tiempo permite a los analistas visualizar actividades en el transcurso del tiempo. Puede acercar la vista a los datos mediante la selección de una ventana de tiempo y la opción Investigar. A continuación, puede restablecer la navegación al rango de tiempo que esta aplicado antes de acercar la vista.

1. Vaya a **INVESTIGAR > Navegar**.
   Se muestran el gráfico de tiempo para el punto de desglose actual y el rango de tiempo seleccionado.



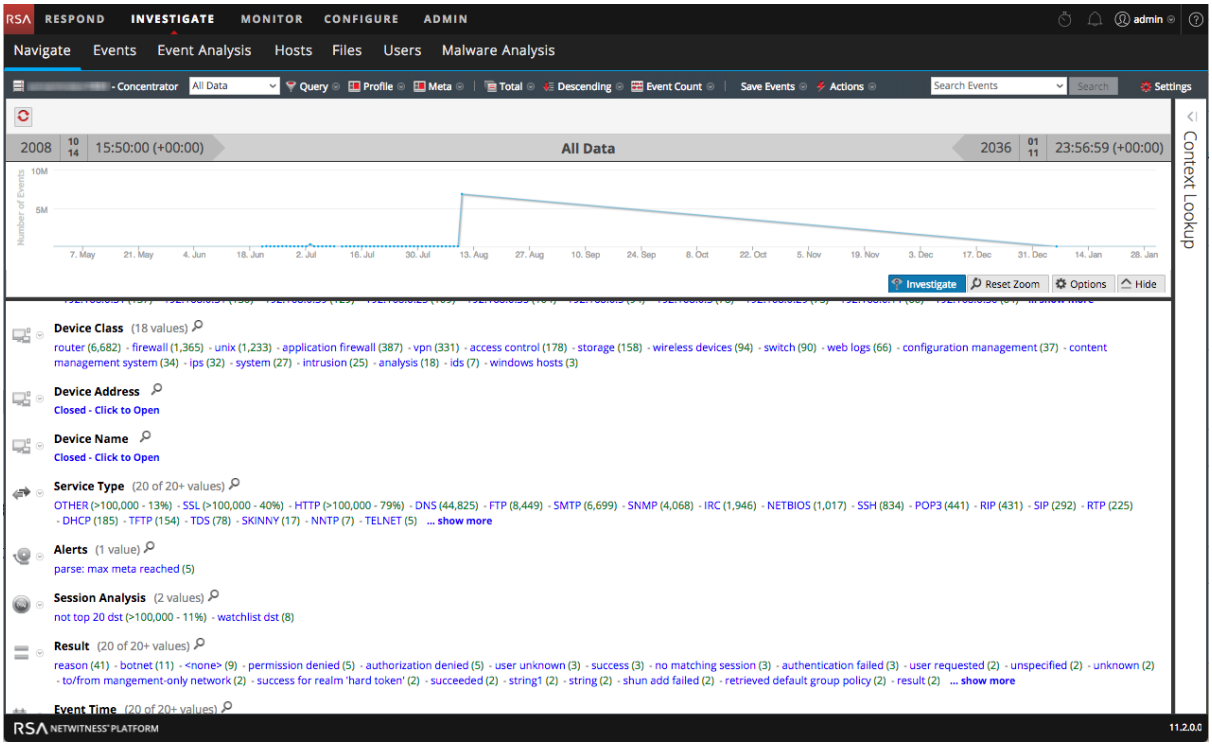
2. Para destacar un período en el gráfico de tiempo, haga clic en el período de tiempo deseado y arrastre el mouse.
   El gráfico de tiempo se vuelve a crear para el rango de tiempo seleccionado; sin embargo, los valores de metadatos no se alteran.
3. Para desglosar a datos en el rango de tiempo seleccionado, haga clic en **Investigate**.
   La URL se actualiza para reflejar el reemplazo del rango de tiempo, al igual que el panel de opciones de Investigation para reflejar el rango de tiempo personalizado. El gráfico de tiempo se vuelve a crear y se cargan los valores de metadatos para el rango de tiempo seleccionado.
4. Para restablecer el gráfico de tiempo al rango de tiempo original, haga clic en **Restablecer zoom**.
   La URL se actualiza para reflejar la URL original antes de acercar la vista a los datos, al igual que el panel de opciones de Investigation para reflejar el rango de tiempo seleccionado antes del acercamiento. Se vuelve a crear el gráfico de tiempo para el rango de tiempo seleccionado y se cargan los valores de metadatos para ese rango de tiempo.

Desglosar a datos en el panel Valores

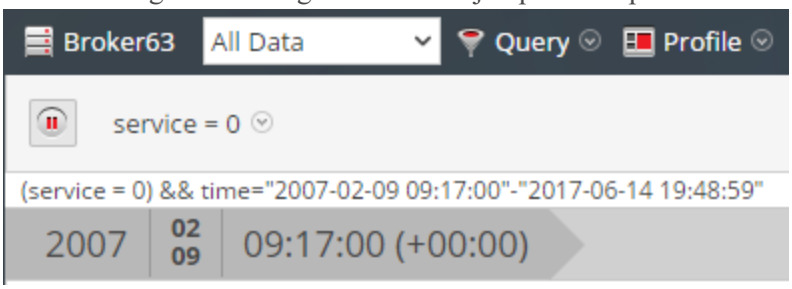
NetWitness Platform muestra la actividad y los valores del servicio seleccionado en la vista Investigation > Navegar. Para investigar los datos, los analistas desglosan a estos, para lo cual hacen clic en una clave de metadatos o en un valor de metadatos, lo que se trata como una consulta. En el panel Valores, cada consulta se agrega a los datos de la ruta de navegación. Esto da como resultado una ruta de navegación en la parte superior, con una ruta de navegación para cada consulta. Puede editar la ruta de navegación para insertar o quitar una consulta.

Para desglosar a un subconjunto de los metadatos:

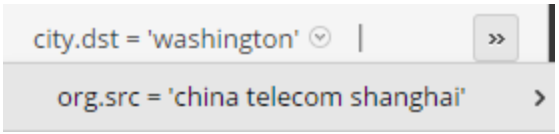
1. Inicie una investigación para mostrar los metadatos en la vista Navegar.



2. Para desglosar a los metadatos, realice cualquier combinación de las siguientes acciones:
   a. Haga clic en una **clave de metadatos**, por ejemplo, **Tipo de servicio**.
   b. Haga clic en un **valor de metadatos**, el texto de color azul en los resultados. Por ejemplo, **OTRO**.
      Cada vez que hace clic en una clave de metadatos o en un valor de metadatos, la consulta de investigación cambia a un punto focal restringido, o punto de desglose, en los datos. En cada punto de desglose, el panel Valores se actualiza y el nuevo punto de desglose se muestra en la ruta de navegación. El siguiente es un ejemplo de la primera ruta de navegación.



      Este es un ejemplo de una ruta de navegación larga que no cabe en la barra de herramientas. A la última consulta que cabe le sigue un menú desplegable que muestra consultas adicionales. Para seleccionar un punto de desglose dentro del desbordamiento, haga clic en el icono de desbordamiento y en una consulta de la lista desplegable.

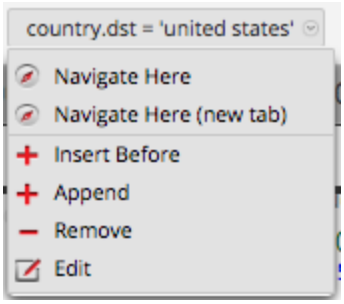


Para agregar una consulta en la ruta de navegación:

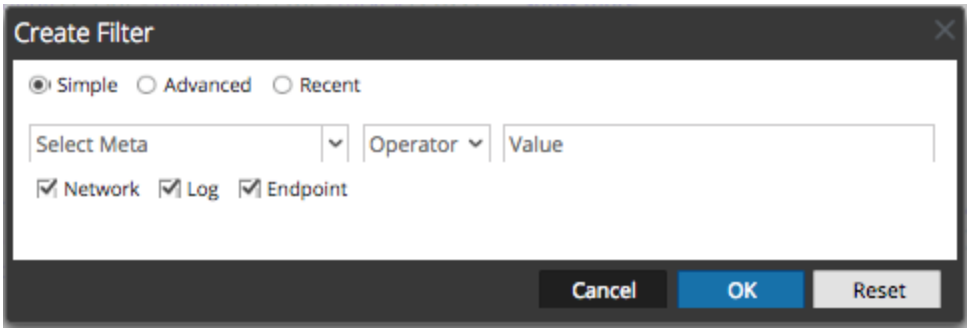
En la ruta de navegación, puede hacer clic en cualquiera de las rutas para mostrar el menú Consulta. Puede insertar una nueva consulta antes de una ruta de navegación y agregar una nueva consulta al final de la ruta. Después de cada edición en la ruta de navegación, NetWitness Platform actualiza los resultados.

Para agregar una consulta en la ruta de navegación:

1. Haga clic en una ruta de navegación.
   Se muestra el menú Ruta de navegación.



2. Para agregar una consulta en la ruta de navegación, seleccione **Agregar** o **Insertar antes**.
   Se muestra el cuadro de diálogo Crear filtro.



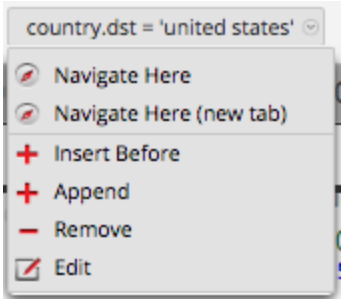
3. Cree la consulta como se describe en Crear una consulta personalizada.

Para editar una consulta en la ruta de navegación:

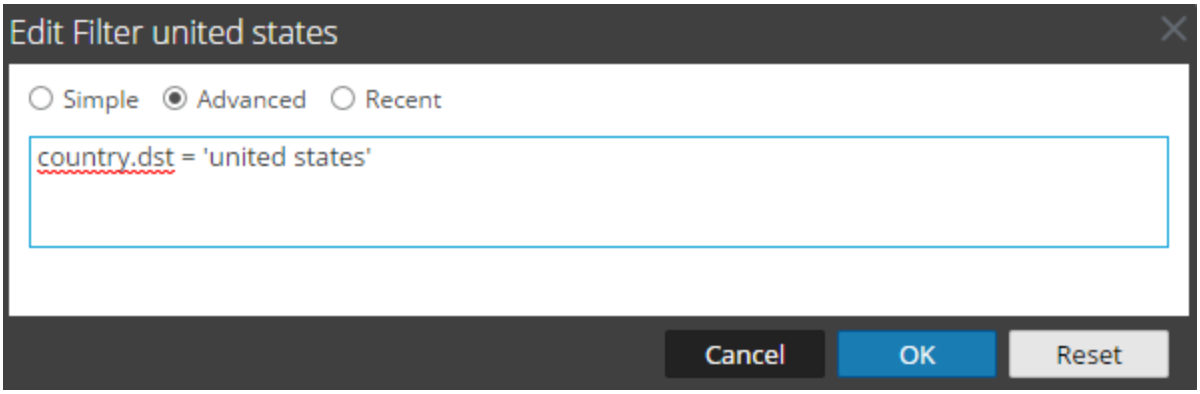
En la ruta de navegación, puede hacer clic en cualquiera de las rutas para mostrar el menú Consulta. Puede eliminar una ruta de navegación y editar una consulta en una ruta de navegación. Después de cada edición en la ruta de navegación, NetWitness Platform actualiza los resultados.

Para trabajar con consultas en la ruta de navegación:

1. Haga clic en una ruta de navegación.
   Se muestra el menú Ruta de navegación.



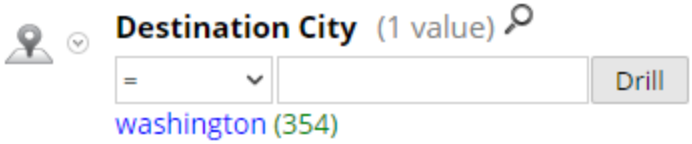
2. Para editar una consulta en la ruta de navegación, seleccione **Editar**.
   El cuadro de diálogo Crear se muestra con la consulta seleccionada abierta para edición.



3. Edite los campos como se describe en Crear una consulta personalizada.

Para realizar una búsqueda rápida dentro de una clave de metadatos:

1. Mantenga el mouse sobre una sección de clave de metadatos y haga clic en la lupa.
   Se muestra el formulario Búsqueda rápida, el cual contiene un comparador y un operando opcional para la búsqueda.

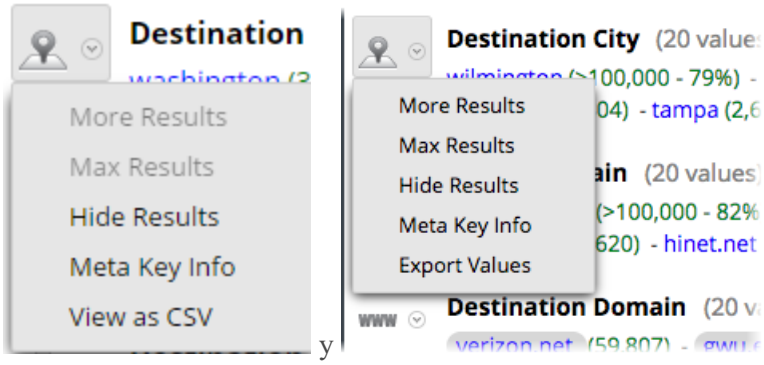


2. (Opcional) Si desea cerrar el formulario de búsqueda, vuelva a hacer clic en la lupa.
3. Seleccione la operación en la lista desplegable de la izquierda y escriba el valor de texto que desea buscar. A continuación, haga clic en **Desglosar** para realizar la ejecución.
   Los metadatos de esa clave de metadatos se utilizan para desglosar a los metadatos actuales.

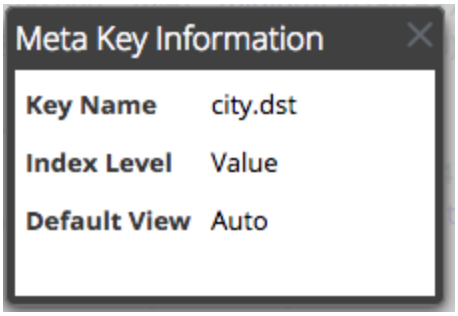
Para ver la información de la clave de metadatos:

Para ver detalles sobre una clave de metadatos, específicamente el nombre de la clave, el nivel de índice configurado para mostrar la clave de metadatos y la vista predeterminada configurada para la clave de metadatos:

1. Haga clic en el menú desplegable junto a la clave de metadatos. En estas dos figuras se muestra el menú desplegable de las versiones 11.0.0.x, 11.1 y superior.

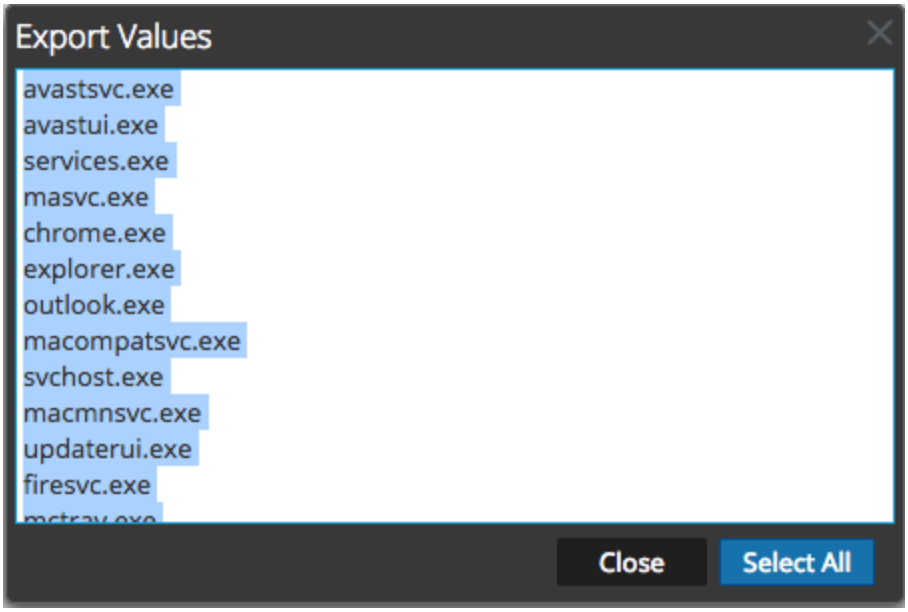


2. Seleccione **Información de clave de metadatos**.
   Se muestra el cuadro de diálogo Información de clave de metadatos.



3. Una vez que haya finalizado la visualización, haga clic en .

4. (Opcional para la versión 11.0) Para ver nombres de metadatos encontrados para la clave de metadatos como una lista de valores separados por comas, haga clic en el menú desplegable junto a la clave de metadatos y seleccione **Ver como CSV**.
   Se muestra el cuadro de diálogo Mostrando valores en formato CSV. Una vez que haya finalizado la visualización, haga clic en **Cerrar**.
5. (Opcional para la versión 11.1) Para ver nombres de metadatos encontrados para la clave de metadatos en una lista, haga clic en el menú desplegable junto a la clave de metadatos y seleccione **Exportar valores**.
   Se muestra el cuadro de diálogo Exportar valores.



6. (Opcional) Si desea ocultar los resultados de la clave de metadatos en el punto de desglose actual, haga clic en el menú desplegable junto a la clave de metadatos y, a continuación, haga clic en **Ocultar resultados**.

Para mostrar eventos asociados a un valor de metadatos:

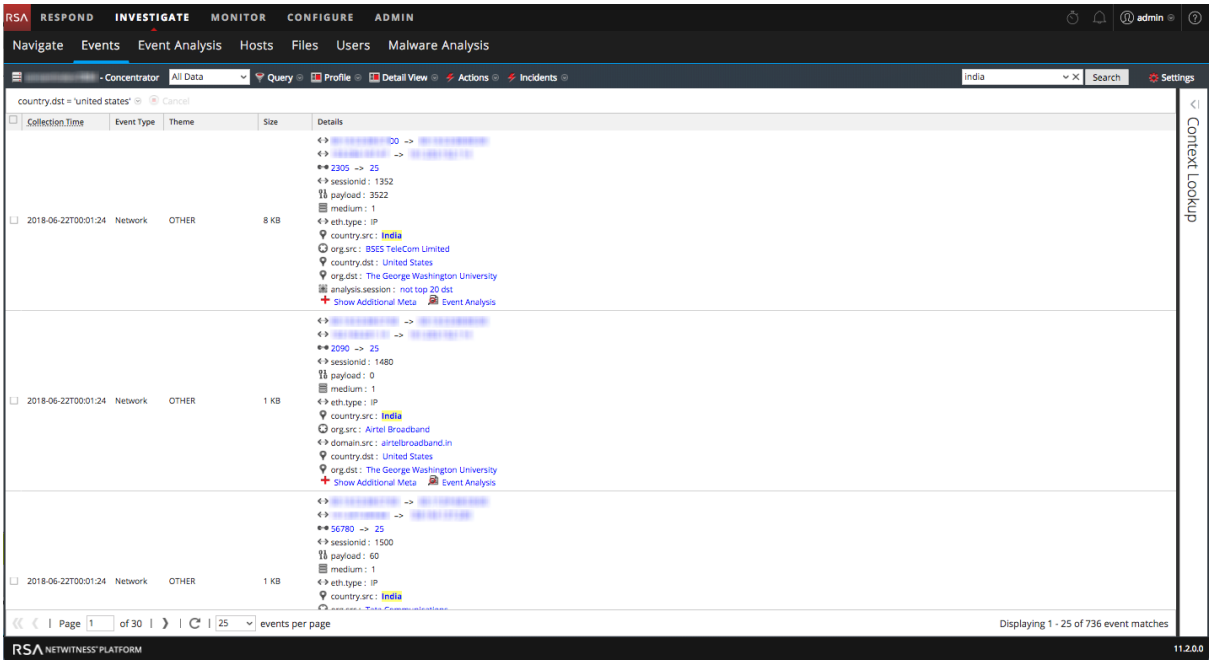
La vista Eventos proporciona detalles adicionales para un evento en dos vistas distintas: Lista Eventos y Vista detallada.

1. En la vista Navegar, desglose a los metadatos que sean el centro de la investigación.
2. Haga clic en el conteo (el número de color verde) junto a un valor de metadatos de color azul.
   Se muestra la vista Eventos correspondiente al punto de desglose actual.
   Las operaciones que puede realizar en la vista Eventos se describen en Análisis de eventos crudos en la vista Eventos.

Para buscar eventos específicos asociados a un valor de metadatos:

1. En la vista Navegar, desglose a los metadatos que sean el centro de la investigación (haga clic en el valor de metadatos o agregue una consulta).
2. Escriba una cadena de búsqueda en el cuadro Buscar y presione **Intro** o haga clic en **Buscar**.
   También puede seleccionar y configurar preferencias del modo de búsqueda. Consulte Buscar

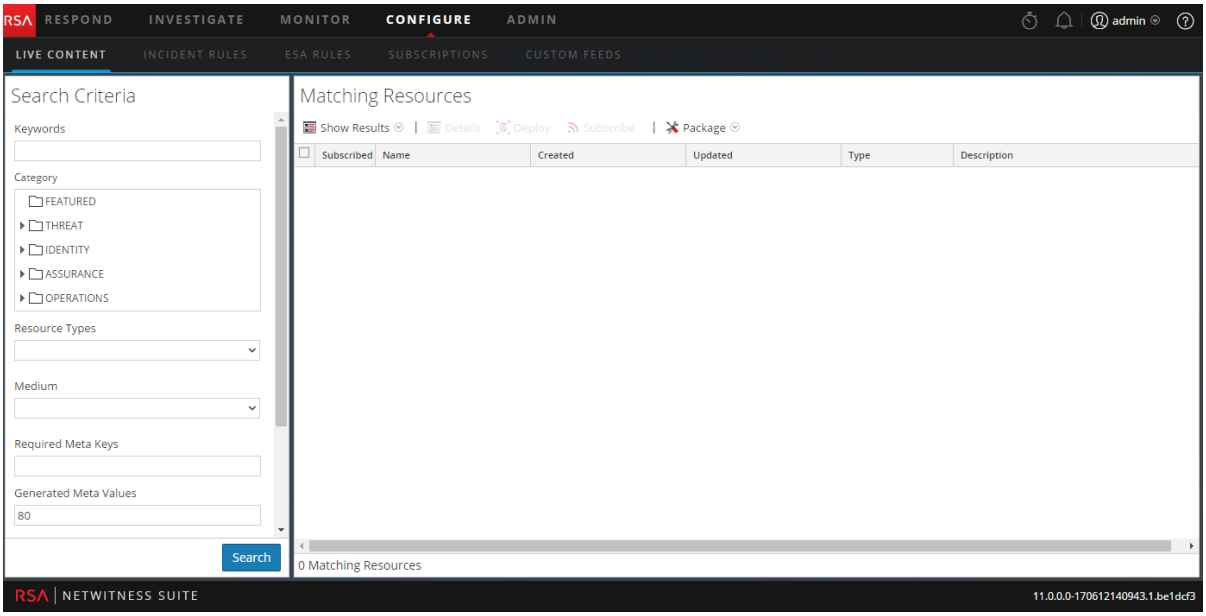
patrones de texto para obtener información detallada sobre la búsqueda.
La vista Eventos se abre en una pestaña nueva y muestra los resultados de búsqueda. Si no ve el término de búsqueda resaltado, haga clic en **Mostrar metadatos adicionales**. Su selección de rango de tiempo y los desgloses (consultas) se transfieren a la vista Eventos.



Para ver un valor de metadatos seleccionado en RSA Live:

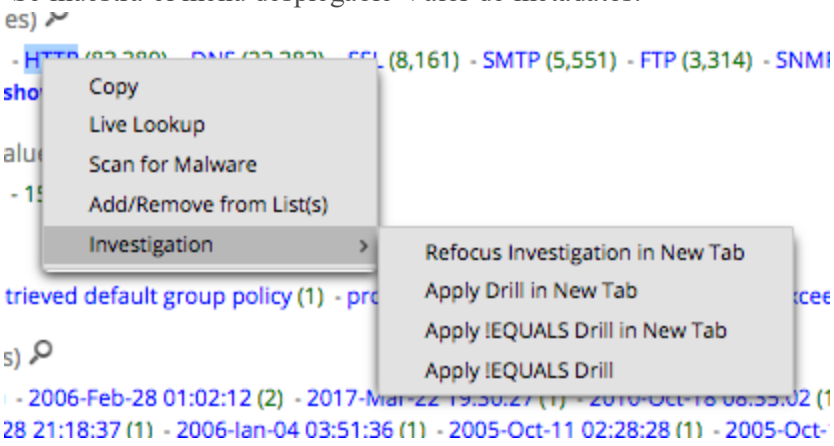
1. En la vista Navegar, desglose a los metadatos que sean el centro de la investigación.
2. Haga clic con el botón secundario en un valor de metadatos (el texto de color azul).
   Se muestra el menú desplegable Valor de metadatos.

3. Para buscar el valor de metadatos en RSA Live, seleccione **Búsqueda en Live**.
   La vista Búsqueda en Live se muestra con el valor de metadatos ingresado en el campo Valores de metadatos generados, el cual está listo para realizar una búsqueda.



Para volver a enfocar la investigación en un punto de desglose:

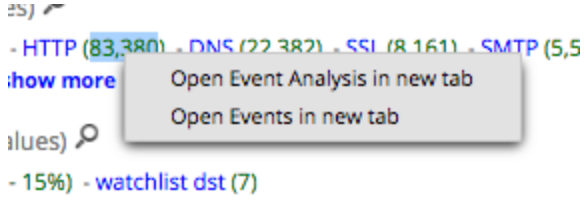
1. Haga clic con el botón secundario en un valor de metadatos (el texto de color azul).
   Se muestra el menú desplegable Valor de metadatos.



2. Elija una de las opciones cambio de enfoque.
   El desglose se vuelve a enfocar según la opción elegida.

Para observar un conteo específico en una nueva pestaña:

Para ver un conteo de un valor de metadatos en la vista Eventos o en la vista Análisis de eventos, haga clic con el botón secundario en el conteo de un valor de metadatos (el número de color verde después del valor de metadatos de color azul).
Se muestra el menú contextual.



Administrar grupos de metadatos

Un grupo de metadatos combina claves de metadatos seleccionadas en un grupo para mostrar solo los datos en los cuales se encontraron claves y entidades de metadatos.

Nota: En la versión 11.1 y superior, también puede usar entidades de metadatos configuradas en grupos de metadatos.

En la vista Investigate > Navegar, puede usar grupos de metadatos para filtrar los datos que se muestran en una investigación. Una instalación nueva de NetWitness Platform incluye grupos de metadatos de uso inmediato (OOTB) para ayudarlo a encontrar conjuntos de datos interesantes en Investigate. Los grupos de metadatos de uso inmediato tienen el prefijo RSA que permite su identificación y se pueden duplicar, pero no editar ni eliminar. Puede crear sus propios grupos, así como duplicar y editar un grupo de uso inmediato para crear un grupo personalizado.

Con un grupo de metadatos en vigor durante una investigación, la información del panel Valores muestra solo las claves de metadatos del grupo seleccionado. Cuando abre una visualización de coordenadas paralelas, las claves y las entidades de metadatos en un grupo aparecen como ejes de izquierda a derecha. Puede ser útil crear dos versiones de cada grupo de metadatos personalizado; una para el análisis de valores de metadatos y otra para crear un gráfico de coordenadas paralelas que se centre en un subconjunto más pequeño del mismo caso de uso.

Los grupos de metadatos personalizados están visibles para todos los usuarios de un servicio y se pueden exportar para importarlos en cualquier servicio, con la limitación de las claves de metadatos disponibles para ese servicio.

Nota: Cuando un administrador agrega manualmente grupos de metadatos personalizados mediante la edición del archivo de índice personalizado para un servicio, los grupos nuevos quedan disponibles para Investigate después del reinicio del servicio.

En esta sección se describe cómo agregar, editar, importar, exportar y eliminar los grupos de metadatos personalizados que se utilizarán durante la navegación en un servicio específico.

Grupos de metadatos de uso inmediato

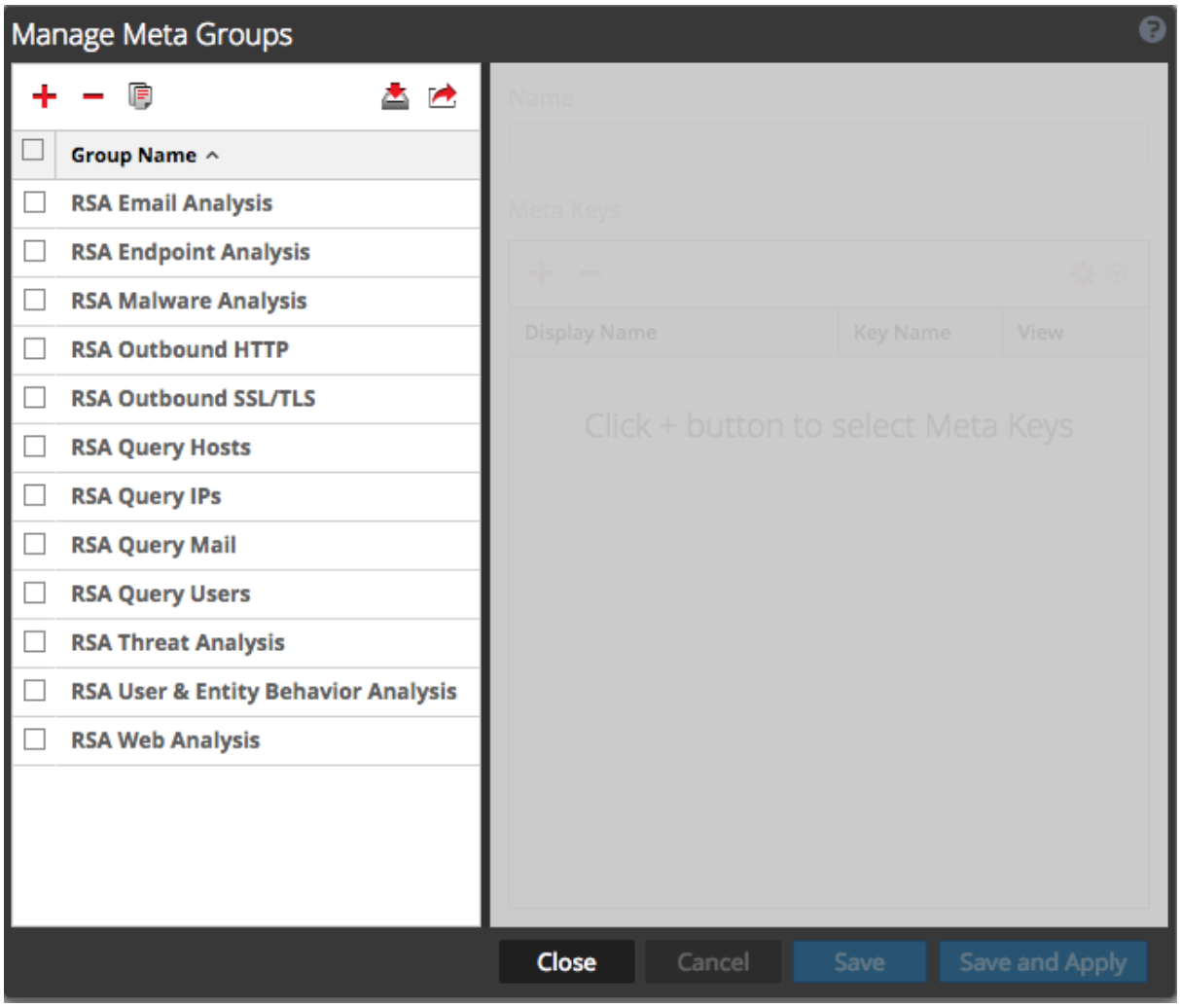
Los grupos de metadatos de uso inmediato están incorporados en RSA NetWitness Platform. Los grupos de metadatos de uso inmediato son útiles para centrar una investigación en casos de uso comunes y para admitir la detección de amenazas mediante RSA Hunting Pack. Estos son los grupos de metadatos de uso inmediato:

- Análisis de correo electrónico de RSA incluye claves de metadatos que describen las interacciones de correo electrónico.
- Análisis de Endpoint de RSA contiene claves de metadatos que proporcionan información valiosa sobre los procesos, los archivos, los usuarios y las conexiones desde hosts de NetWitness Endpoint (NWE).
- RSA Malware Analysis incluye claves de metadatos que marcan indicadores de riesgo en archivos contenidos en eventos.

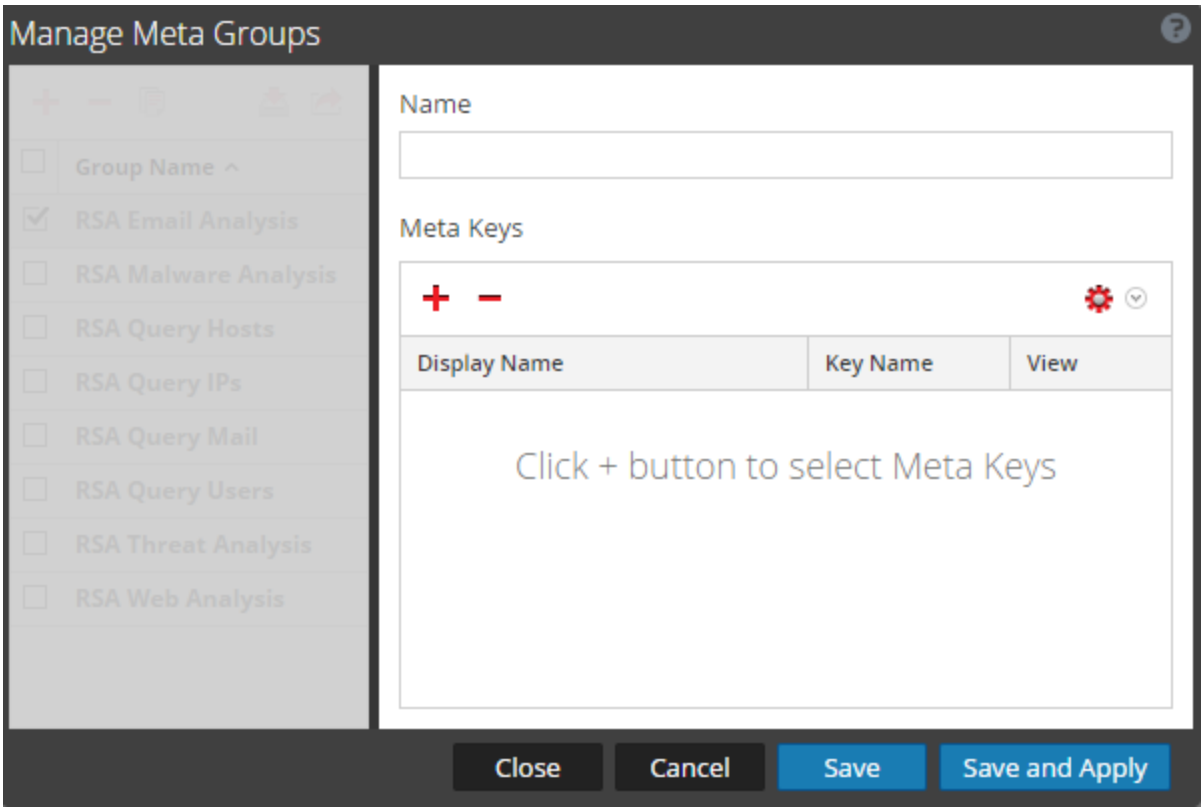
- HTTP de salida de RSA incluye claves de metadatos que proporcionan información valiosa sobre el tráfico web de salida.
- Protocolos SSL/TLS de salida de RSA incluye claves de metadatos que se centran en el tráfico web cifrado.
- Hosts de consulta de RSA incluye claves de metadatos que abarcan todas las claves de metadatos para buscar hosts.
- IP de consulta de RSA incluye claves de metadatos que abarcan todas las claves de metadatos para buscar direcciones IP.
- Correo de consulta de RSA incluye claves de metadatos que abarcan todas las claves de metadatos para buscar correo electrónico.
- Usuarios de consulta de RSA incluye claves de metadatos que abarcan todas las claves de metadatos para buscar usuarios.
- Análisis de amenazas de RSA incluye claves de metadatos que marcan amenazas potenciales en el conjunto de datos.
- RSA User and Entity Behavior Analysis incluye claves de metadatos que abarcan todas las claves de metadatos para analizar el comportamiento de los usuarios y las entidades.
- Análisis web de RSA incluye claves de metadatos que marcan anomalías en el tráfico web.

Crear un grupo de metadatos y agregar claves de metadatos

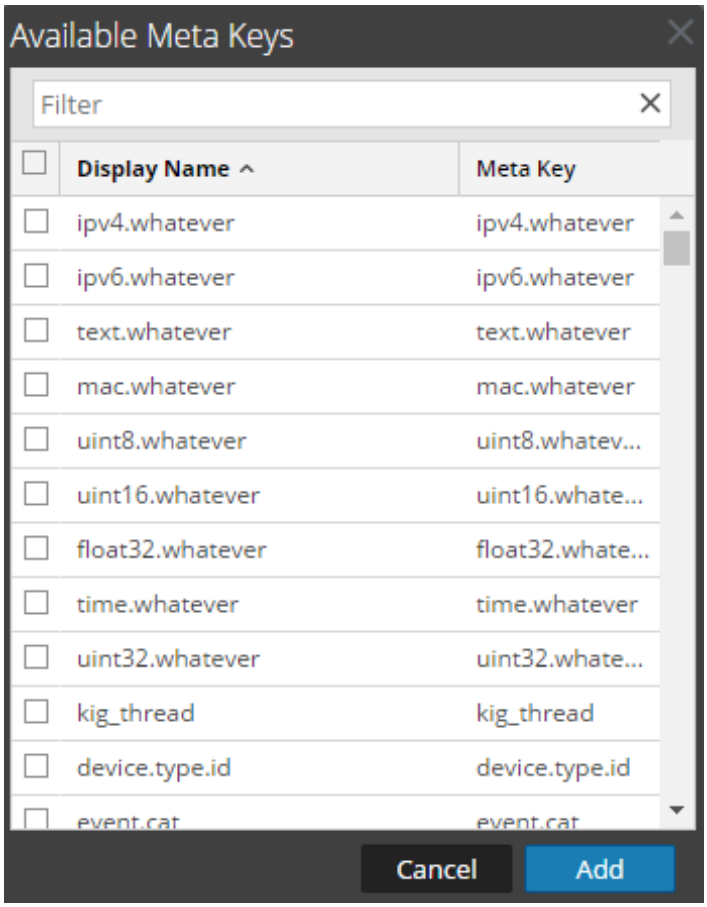
1. Mientras investiga un servicio en la vista **Investigate > Navegar**, seleccione **Metadatos > Administrar grupos de metadatos** en la barra de herramientas.
   Se muestra el cuadro de diálogo Administrar grupos de metadatos. Inicialmente, solo los grupos de uso inmediato están configurados para un servicio y se enumeran en Nombre del grupo. Si ya se configuraron otros grupos personalizados, estos también se enumeran en Nombre del grupo.



2. En la barra de herramientas de la parte superior de la lista Grupos de metadatos, haga clic en +.
   Se inserta una nueva fila en la parte superior de la lista Grupos de metadatos.
3. Escriba un nombre para el grupo de metadatos nuevo y presione **Intro**.
   El formulario de la derecha se abre para su edición.



4. (Opcional) Si desea cambiar el nombre del grupo de metadatos, escriba un nuevo valor en el campo **Nombre** .
5. En la barra de herramientas **Claves de metadatos**, haga clic en +.
   Se muestra el cuadro de diálogo Claves de metadatos disponibles con las claves en orden alfabético.

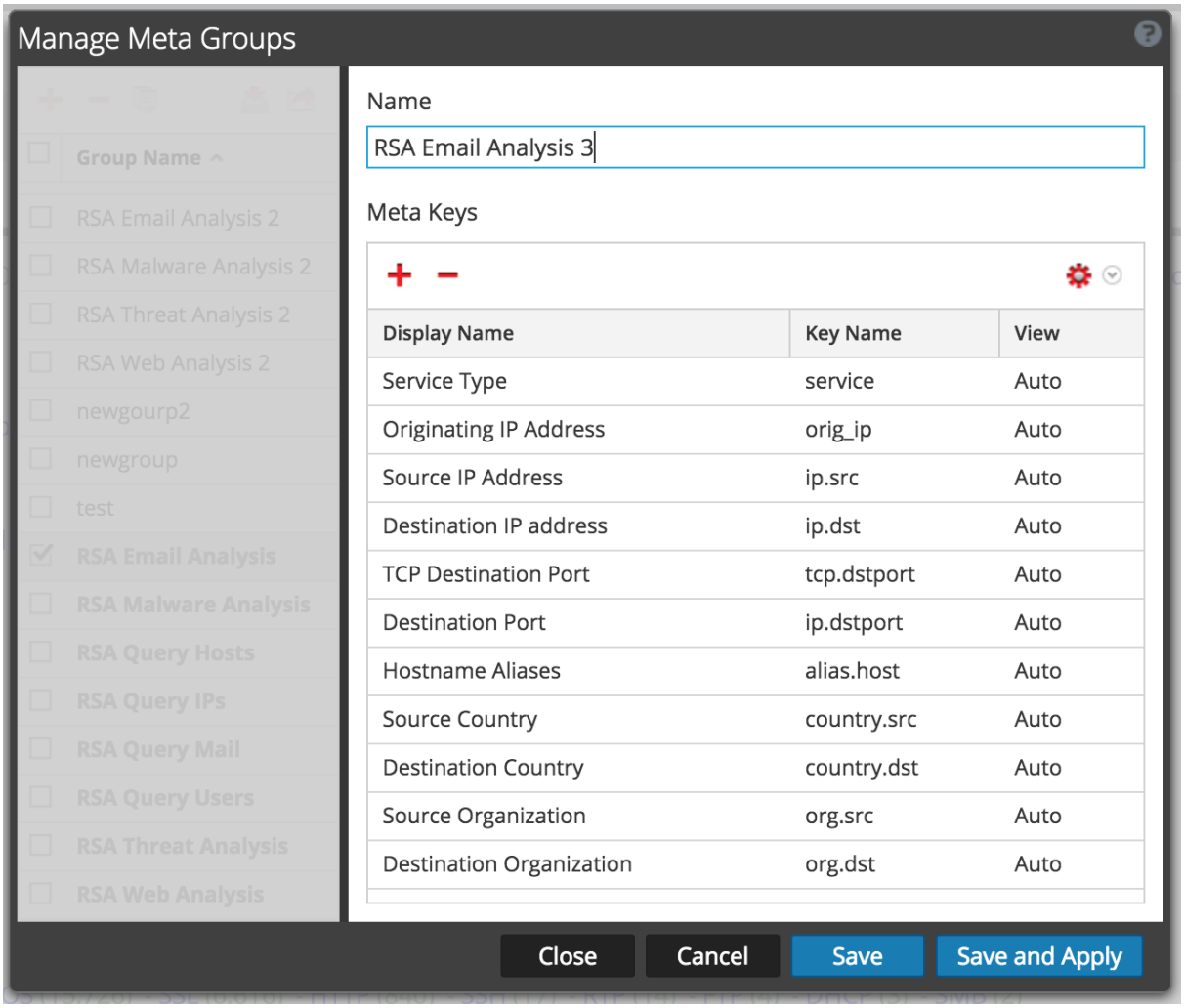


6. Para filtrar la lista de claves de metadatos, escriba una palabra o una frase en el campo **Filtrar** y seleccione **Intro**.
   La lista muestra claves de metadatos coincidentes de acuerdo con una búsqueda que no distingue mayúsculas de minúsculas. Elimine el texto del filtro y presione **Intro** para extraer el filtro.
7. Para elegir las claves de metadatos que se incluirán en el grupo de metadatos, seleccione las casillas de verificación. Para elegir todas las claves de metadatos, seleccione la casilla de verificación de la barra de título y haga clic en **Agregar**.
   Las claves de metadatos seleccionadas se agregan a la lista Claves de metadatos.
8. (Opcional) Si desea cambiar el orden en que las claves de metadatos se cargan y enumeran en una investigación, haga clic y arrastre una o más claves de metadatos a una nueva posición.
9. Para terminar de crear el grupo de metadatos, realice una de estas acciones:
   a. Para guardar el grupo de metadatos, haga clic en **Guardar**.
      Se crea el grupo y está disponible para utilizar.
   b. Para guardar y aplicar el grupo de metadatos a la vista Investigation actual, haga clic en **Guardar y aplicar**.
      El grupo se crea y se aplica de inmediato a la vista Investigation actual.
10. Haga clic en **Cerrar**.

Duplicar y editar un grupo de metadatos de uso inmediato

Si desea personalizar un grupo de metadatos de uso inmediato, debe duplicarlo y, a continuación, editar el duplicado.

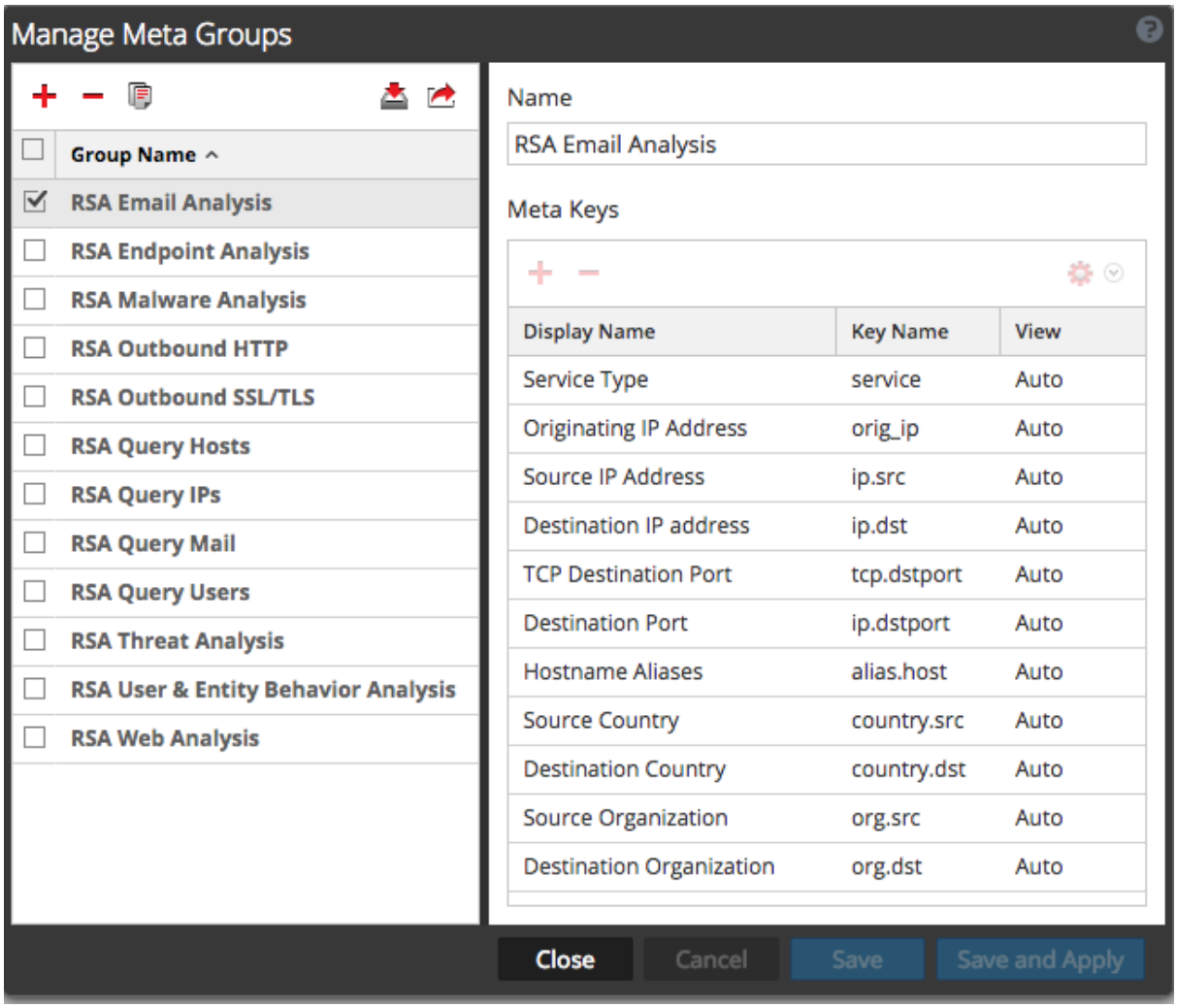
1. Seleccione un grupo de metadatos de uso inmediato en la lista Administrar grupos de metadatos y haga clic en .
   El formulario de la derecha se abre para su edición con todas las claves de metadatos presentes en el grupo de uso inmediato.



2. Ingrese un nombre para el grupo nuevo y continúe con la edición como se describe en “Editar un grupo de metadatos”, a continuación.

Editar un grupo de metadatos

1. Seleccione un grupo en la lista **Grupos de metadatos**.
   El formulario de la derecha se abre para su edición.



2. (Opcional) Editar el nombre del grupo.
3. (Opcional) Agregar nuevas claves de metadatos, como se describe anteriormente en “Crear un grupo de metadatos y agregar claves de metadatos”.
4. (Opcional) Para establecer el orden de las claves, arrastre y suelte una o más claves.
5. (Opcional) Para cambiar la vista inicial de una clave de metadatos, haga clic en y seleccione una de las vistas posibles.
   Cuando modifica el grupo de metadatos, no puede establecer la clave en ABIERTO. Si cambia a ABIERTO la vista predeterminada para un grupo de claves de metadatos y algunas de las claves de metadatos no están indexadas, estas claves vuelven a AUTOMÁTICO. En consecuencia, la clave de metadatos se carga automáticamente solo si está indexada, y las claves de metadatos no indexadas se CIERRAN hasta que se abren de forma manual.
   El valor de la vista inicial se muestra en la columna Vista.
6. Para guardar los cambios, haga clic en **Guardar**.
7. Para aplicar los cambios a la vista Navegar actual, haga clic en **Guardar y aplicar**.

Eliminar un grupo de metadatos

1. En la lista **Grupos de metadatos**, seleccione el grupo que desea quitar.
2. Haga clic en .
   Un cuadro de diálogo de confirmación brinda la oportunidad de cancelar o completar la solicitud.
3. Haga clic en **Aceptar**.
   Se elimina el grupo de metadatos. Cuando cierra la ventana, si el grupo eliminado era el grupo de metadatos que se aplicaba actualmente, se elimina y las claves de metadatos predeterminadas se utilizan para crear la vista.

Exportar un grupo de metadatos

Los grupos de metadatos definidos por el usuario se crean en servicios individuales. Para que los grupos de metadatos estén disponibles para otro servicio, debe exportarlos a su sistema de archivos local. Para exportar uno o más grupos de metadatos:

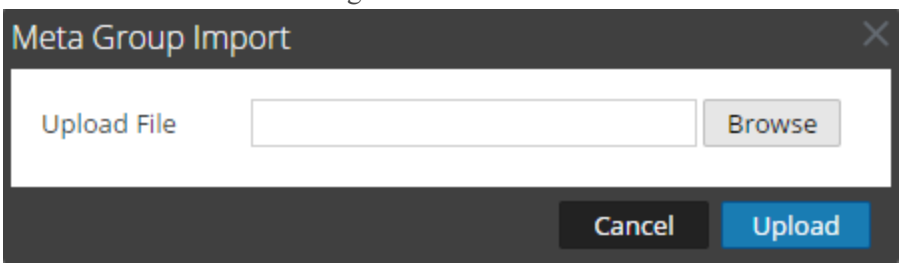
1. En la lista **Grupos de metadatos**, seleccione uno o más grupos para exportar.
2. Haga clic en .
   Los grupos seleccionados se descargan en el sistema de archivos local como un **archivo MetaGroups.jsn**. Todas las descargas de grupos de metadatos tienen el mismo nombre con un número anexado para evitar sobrescribir las descargas anteriores.

Importar un grupo de metadatos

Para hacer que los grupos de metadatos definidos por el usuario desde otro servicio estén disponibles para el servicio que se investiga actualmente, debe importar el archivo `MetaGroups.jsn` desde el sistema de archivos local. Cuando se importan grupos de metadatos, se muestra un mensaje de error si alguno de los grupos ya está presente. Para importar un grupo que es un duplicado, primero debe eliminar el grupo existente. Si desea eliminar un grupo de metadatos, un perfil no puede estar usándolo.

Para importar grupos de metadatos:

1. En la lista **Grupos de metadatos**, seleccione un archivo para importar y haga clic en .
   Se muestra el cuadro de diálogo de selección.



2. Haga clic en **Navegar** y navegue al directorio del sistema de archivos local donde se almacenan los archivos `MetaGroups.jsn` descargados. Seleccione un archivo y haga clic en **Abrir**.
   El nombre de archivo se muestra en el campo Cargar archivo.

3. Haga clic en **Cargar**.
   El proceso de carga comienza y un mensaje indica que la carga se ha realizado correctamente. Los grupos de metadatos se agregan a la lista Grupo de metadatos. Si el archivo es un duplicado de un grupo de metadatos existente, un cuadro de diálogo le indica que ya existe el grupo de metadatos.

Visualizar metadatos como coordenadas paralelas

Los analistas pueden usar la visualización de coordenadas paralelas de la vista Navegar para centrar la investigación en combinaciones de valores y claves de metadatos que pueden indicar que los eventos son anormales y que ameritan una investigación.

Nota: En la versión 11.1 y superior, cuando se usan claves de metadatos, también se pueden usar entidades de metadatos configuradas.

El gráfico de coordenadas paralelas es una manera de visualizar el punto de desglose actual en Investigate para examinar más de dos claves de metadatos simultáneamente. La visualización simultánea de varias claves de metadatos puede ayudar a identificar problemas de seguridad asociados a comparaciones y patrones multivariantes, como cuando los valores y las claves de metadatos individuales no causan preocupación, pero si se combinan, pueden revelar un patrón o una relación anormales. Los grupos de metadatos (consulte Administrar grupos de metadatos) se puede utilizar de manera eficaz para definir un conjunto de claves de metadatos que se desean visualizar como coordenadas paralelas.

Mejores prácticas para obtener gráficos de coordenadas paralelas eficaces

Para crear gráficos de coordenadas paralelas eficaces, siga estas recomendaciones:

- Comience desde un punto de desglose en lugar de intentar visualizar todos los datos.
- Limite el rango de tiempo si es necesario.
- Elija el conjunto útil de claves de metadatos más pequeño para mostrar como ejes.
- Especifique la secuencia de ejes para resaltar las anomalías entre los valores de metadatos a medida que sigue una línea que cruza el gráfico.
- Cuando pueda identificar un conjunto de claves de metadatos útil y una secuencia, cree un grupo de metadatos personalizado para usarlo en investigaciones futuras. Por ejemplo, puede crear un grupo de metadatos personalizado para tipos de archivos ejecutables de Windows.
- Utilice los grupos de metadatos de uso inmediato de RSA que se incluyen en una instalación nueva.
- Vuelva a utilizar y comparta los grupos de metadatos personalizados mediante su importación y exportación como archivos `.jsn`.
- Puede ser útil crear dos versiones de cada grupo de metadatos personalizado. Una para el análisis de valores de metadatos y otra para crear un gráfico de coordenadas paralelas que se centre en un subconjunto más pequeño del mismo caso de uso.

Nota: Cuando se importan grupos de metadatos, se muestra un mensaje de error si alguno de los grupos ya está presente. Para importar un grupo que es un duplicado, primero debe eliminar el grupo existente. Si desea eliminar un grupo de metadatos, un perfil no puede estar usándolo.

Como ayuda para optimizar la creación de gráficos de coordenadas paralelas, en NetWitness Platform se incluyen varias optimizaciones.

- Los analistas pueden especificar que en el gráfico solo se representen las sesiones en las cuales existen todas las claves de metadatos.
- El administrador puede aumentar la cantidad de valores de metadatos que se representan en Configuración de coordenadas paralelas en la vista Sistema de Administration > panel Investigación > pestaña Navegar.

Casos de uso de grupos de metadatos de RSA para coordenadas paralelas

En NetWitness Platform se incluye un conjunto de grupos de metadatos predefinidos. Si desea obtener la versión más reciente, puede importar el archivo de grupos de metadatos, `MetaGroups_ootb_w_query.jsn`, en el cuadro de diálogo Administrar grupos de metadatos. Algunas de las actividades dirigidas que se prestan para las visualizaciones de coordenadas paralelas son:

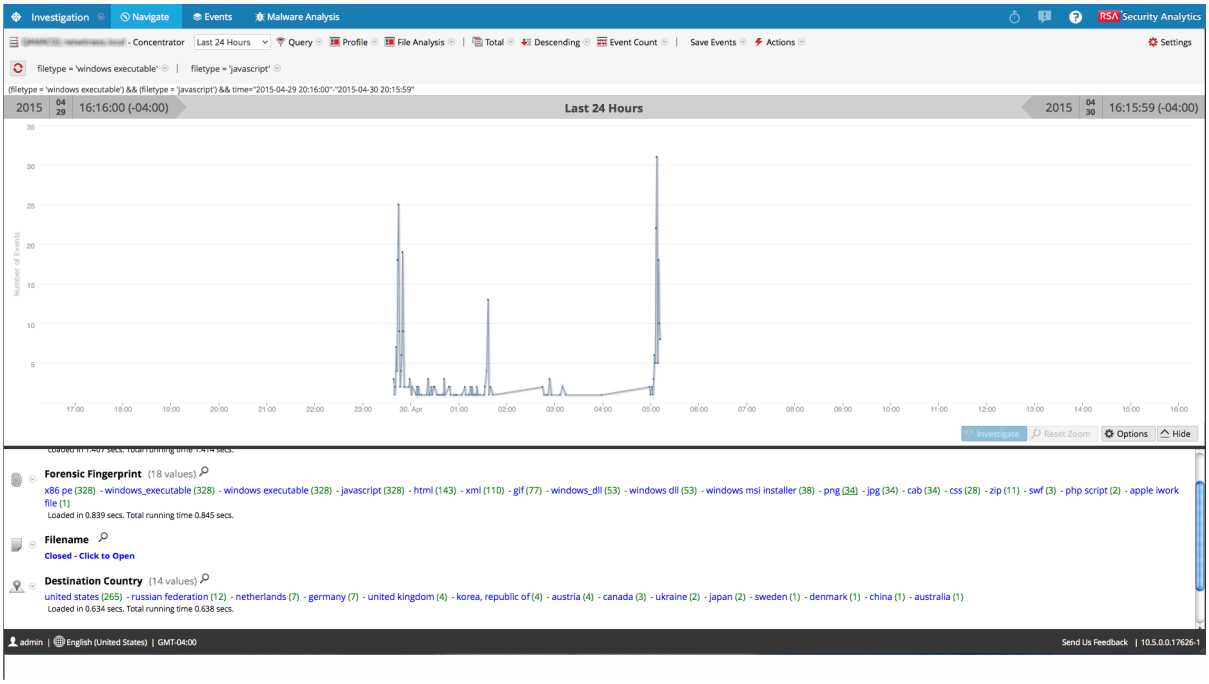
- Señalización por botnet
- Canales encubiertos
- Correo electrónico
- Sesiones cifradas
- Análisis de Endpoint
- Análisis de archivos
- Malware Analysis
- HTTP de salida
- Protocolos SSL/TLS de salida
- Ataques de inyección SQL
- Análisis de amenazas
- Análisis web

Ver una visualización de coordenadas paralelas

Desde una investigación en la vista Investigar > Navegar:

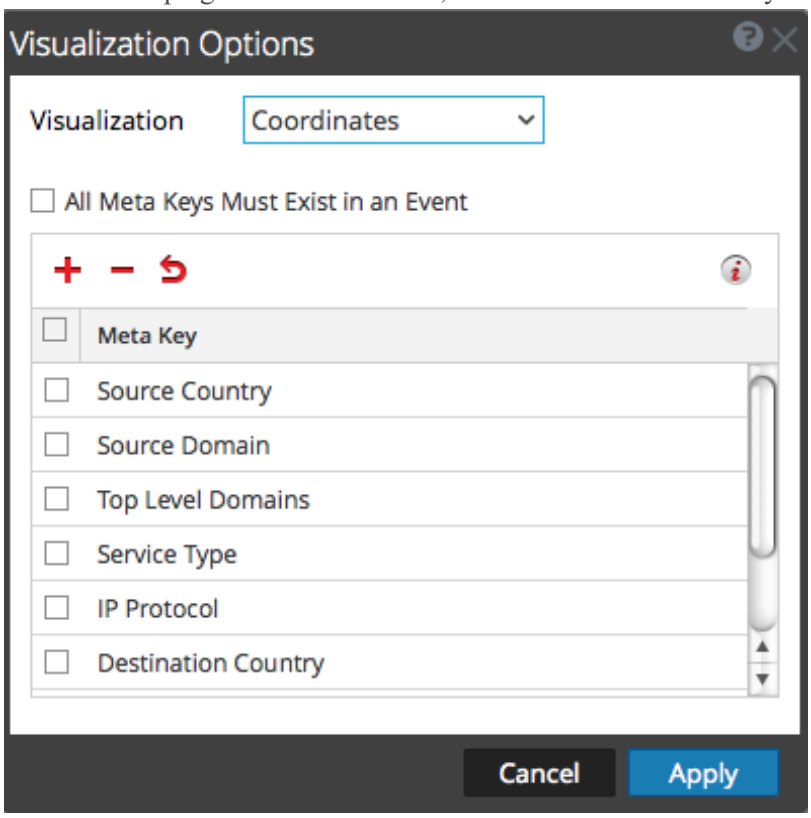
1. Si el panel Visualización sobre el panel Valores está cerrado, seleccione **Visualización**.
2. En la barra de herramientas, seleccione **Metadatos** > **Usar grupo de metadatos > Análisis de archivos (Malware)**.
3. En el panel **Valores**, en la clave de metadatos **Huella digital forense**, haga clic en `windows_executable` y en `x86 pe`, de modo que la ruta de navegación indique `filetype = 'windows_executable' | filetype = 'x86 pe'`.

4. Una visualización predeterminada para el punto de desglose actual se muestra como un cronograma.

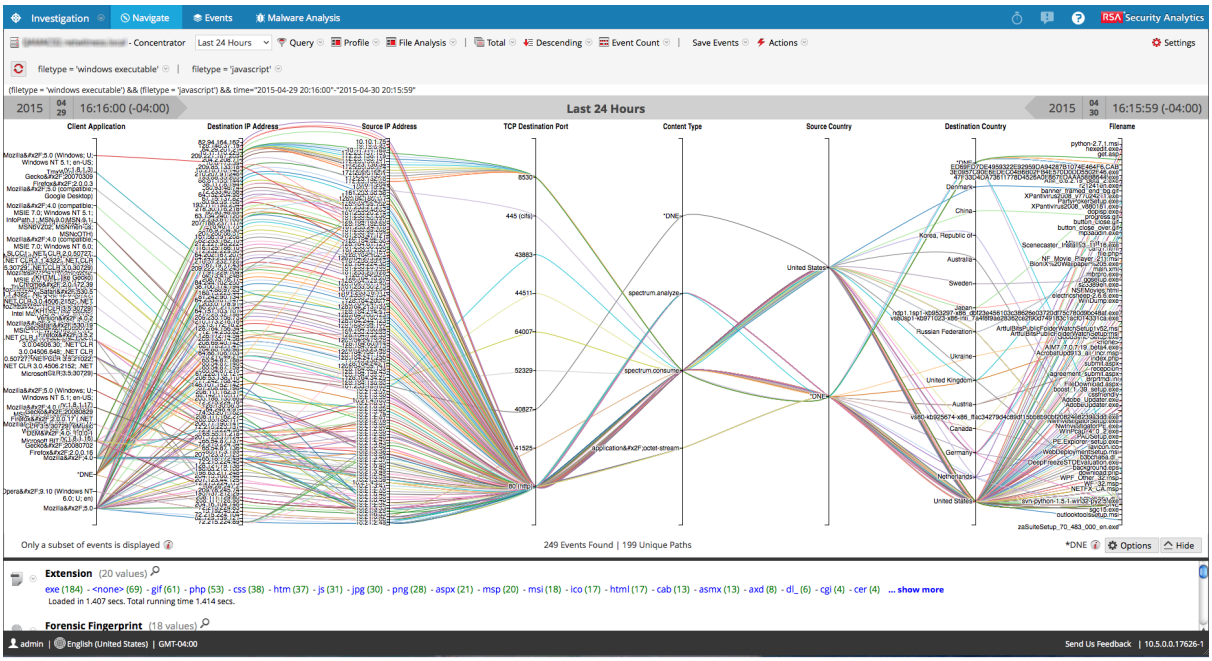


5. En el panel **Visualización**, seleccione **Opciones**.
   Se muestra el cuadro de diálogo Opciones de visualización.

6. En la lista desplegable **Visualización**, seleccione **Coordenadas** y haga clic en **Aplicar**.



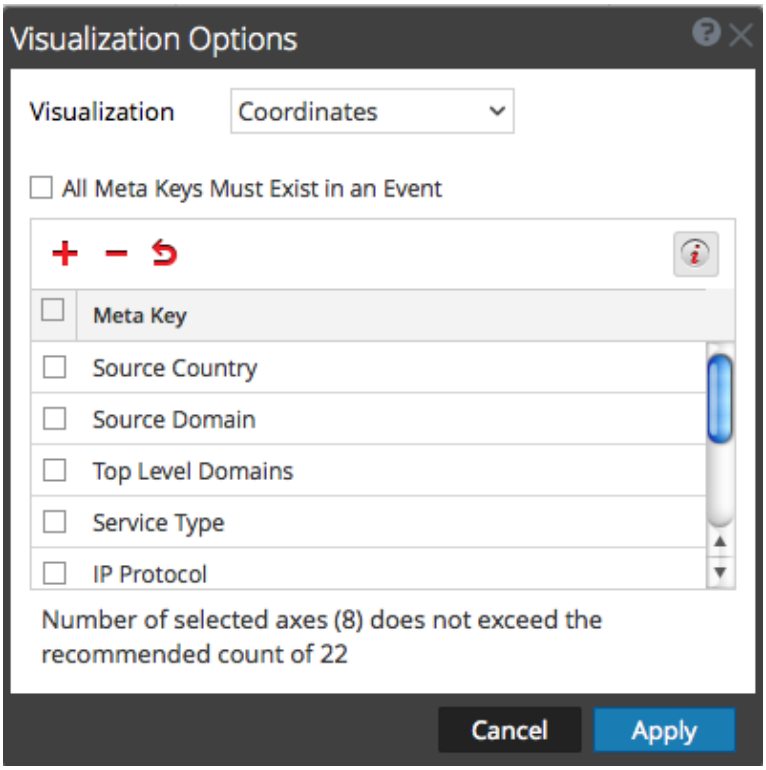
La visualización se carga. En este ejemplo, se encuentran 249 eventos y se visualizan 199 rutas únicas.



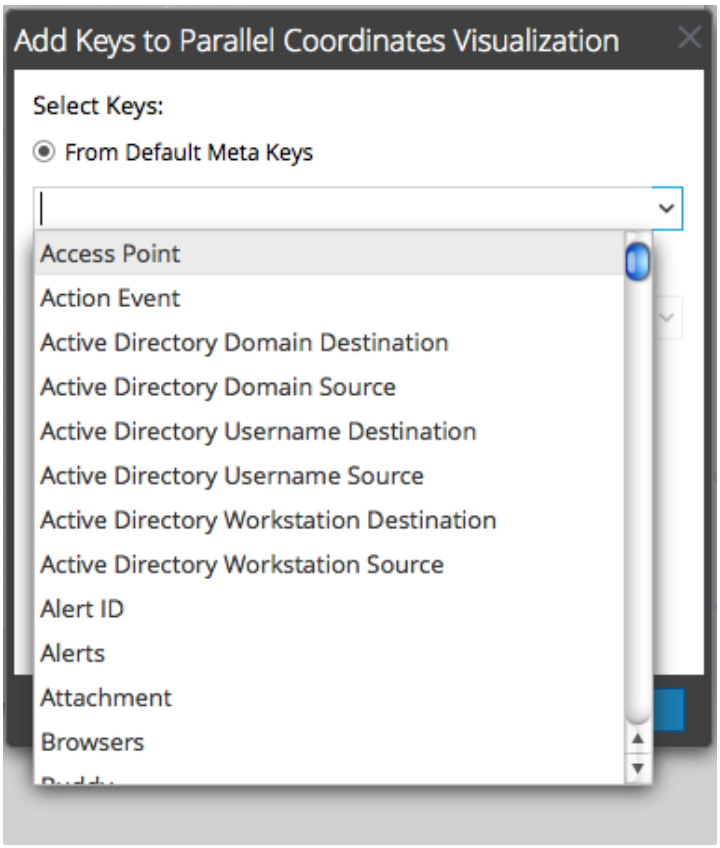
Seleccionar claves de metadatos para una visualización de coordenadas paralelas

Con una visualización de coordenadas paralelas abierta, realice lo siguiente:

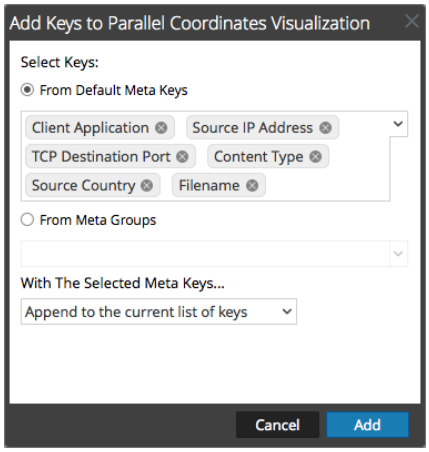
1. En el panel Visualización, seleccione **Opciones**.
   Se muestra el cuadro de diálogo Opciones de visualización. En la barra de herramientas, haga clic en con el fin de mostrar la cantidad recomendada de ejes para una visualización legible. Cuando se muestra un conteo de claves recomendado, el conteo cambia en función del tamaño del navegador. Si agranda la ventana del navegador, el conteo recomendado aumenta.



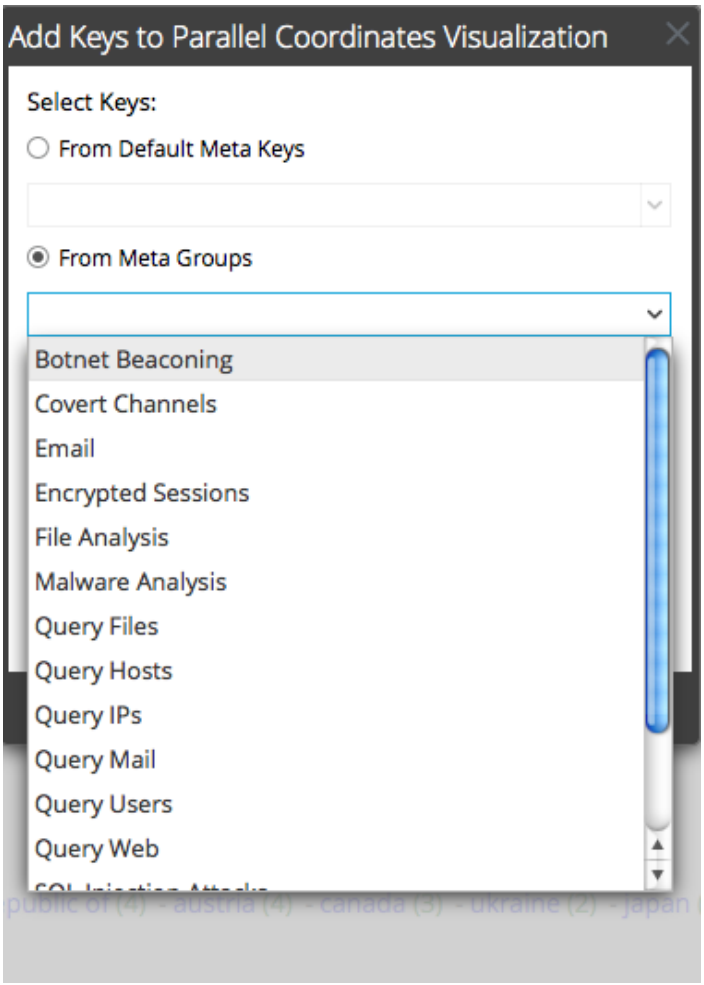
2. Si desea cambiar la secuencia de claves de metadatos, arrastre las claves de metadatos hacia arriba o hacia abajo para disponerlas en la secuencia deseada.
3. Si desea eliminar las claves de metadatos, haga clic en el cuadro de selección y, a continuación, en .
   Las claves de metadatos se quitan, pero el cambio aún no se aplica.
4. Si desea revertir al estado anterior, haga clic en .
   Las claves de metadatos que eliminó se restauran y los cambios que hizo se quitan.
5. Si desea seleccionar claves de metadatos individuales, haga clic en , seleccione **Desde claves predeterminadas** y, en la lista desplegable, seleccione las claves de metadatos.



Las claves seleccionadas se enumeran.

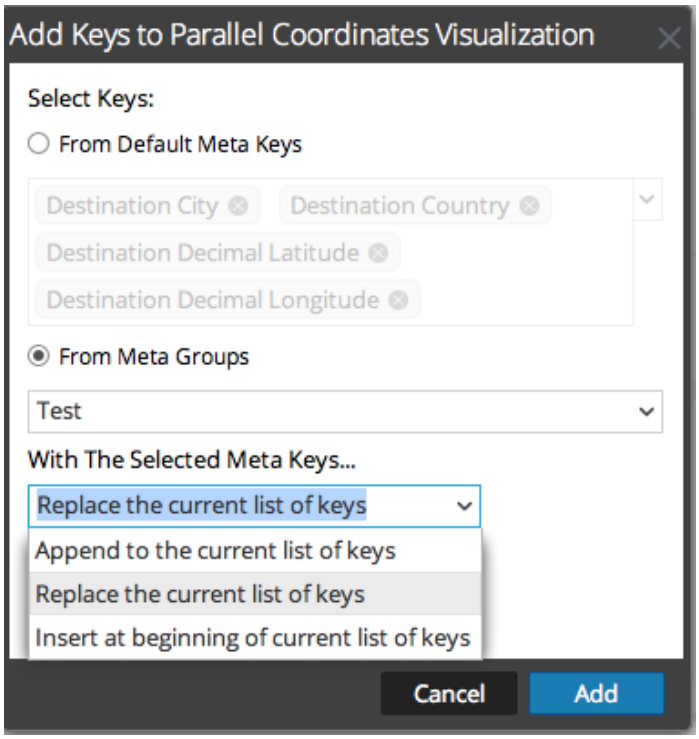


6. Si desea agregar todas las claves de un grupo de metadatos, no puede agregar claves de metadatos individuales. Seleccione **Desde grupos de metadatos** y elija un grupo en la lista desplegable.

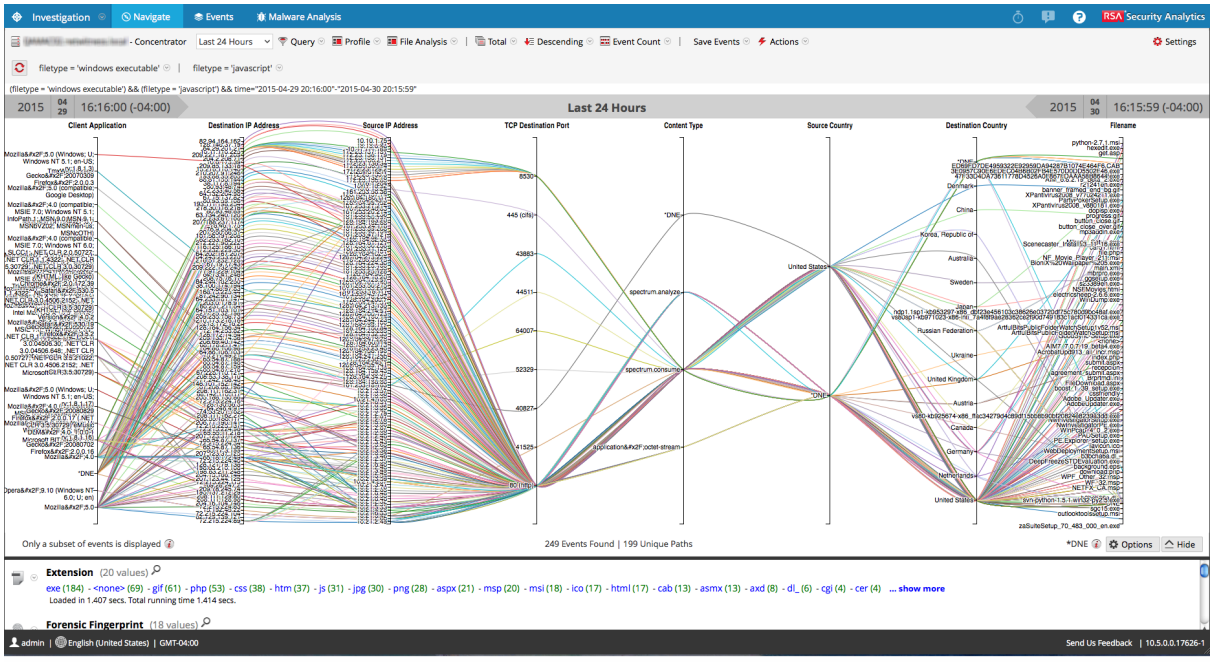


Los grupos de metadatos seleccionados se enumeran en el campo.

7. Seleccione el método para agregar las claves o los grupos: **Reemplazar la lista actual de claves**, **Agregar a la lista actual de claves** (al final) o **Insertar al comienzo de la lista actual de claves.**

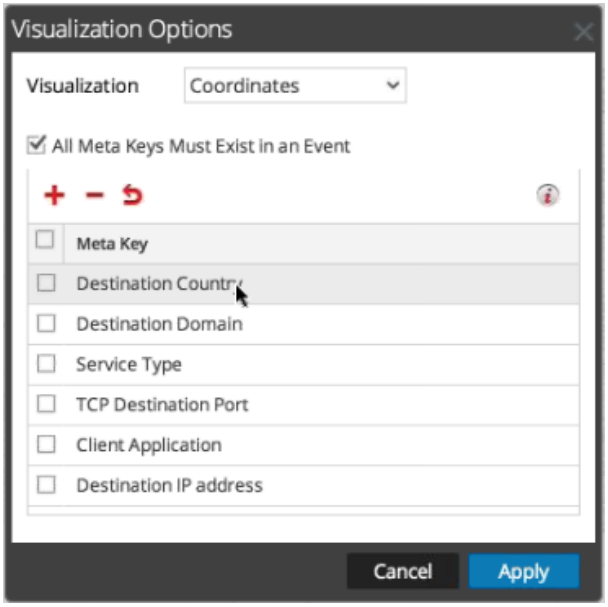


8. Para completar el procedimiento, haga clic en **Agregar**.
   El cuadro de diálogo Opciones de visualización se muestra con los grupos o las claves de metadatos que seleccionó.
9. Para mostrar el nuevo gráfico de visualización, haga clic en **Aplicar**.

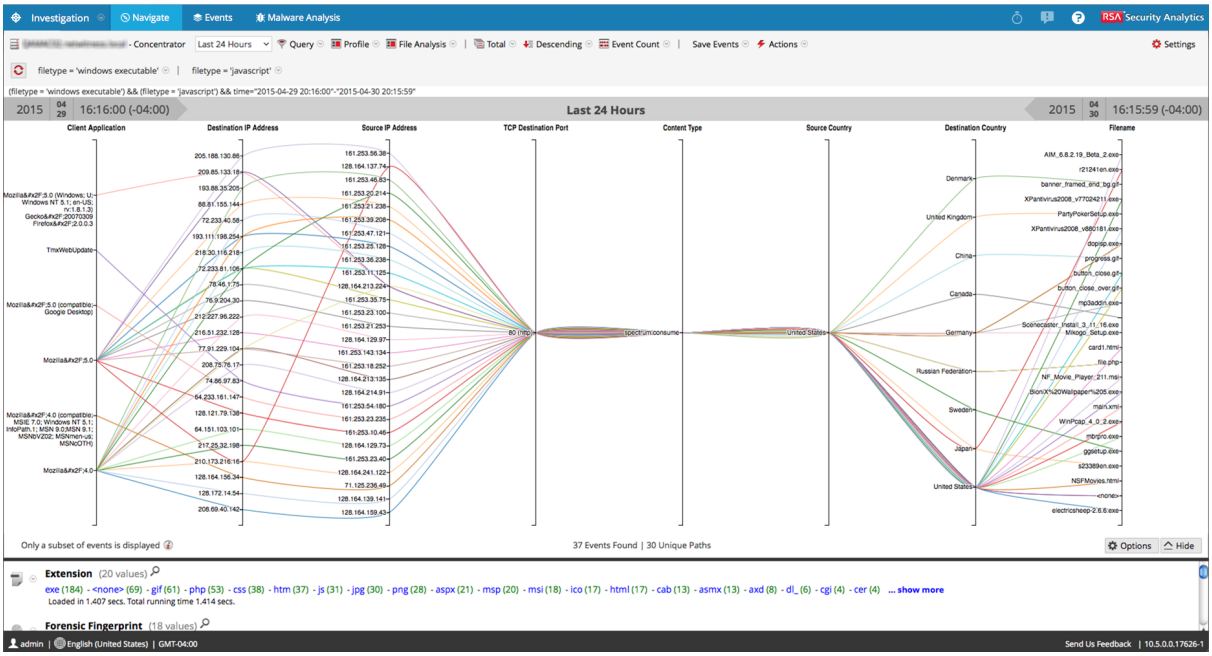


Optimizar una visualización de coordenadas paralelas

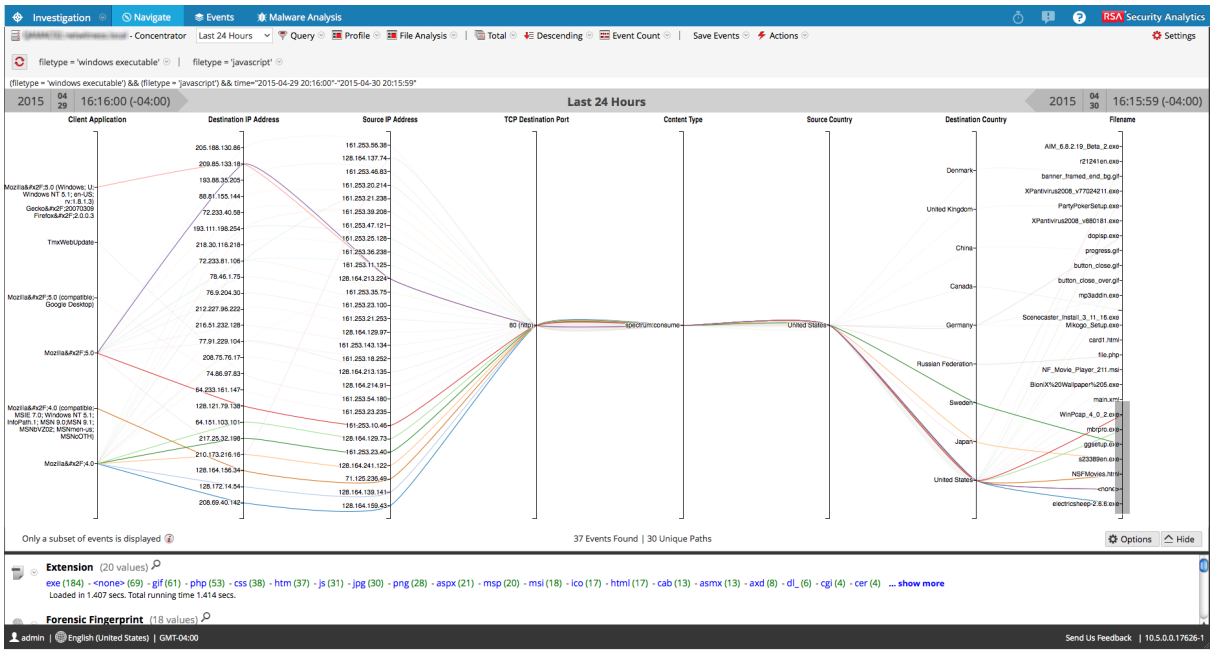
1. Para optimizar la visualización mediante la eliminación de eventos en los cuales no existen todas las claves de metadatos, seleccione **Opciones.**



2. En el cuadro de diálogo Opciones de visualización, seleccione **Todas las claves de metadatos deben existir en un evento**. Haga clic en **Aplicar**.
   El gráfico resultante es más legible y útil, y tiene menos rutas únicas.



3. Si desea resaltar un conjunto de puntos pequeño para ver la ruta de la línea de derecha a izquierda, haga clic en un eje. El cursor cambia a una mira, la cual puede arrastrar para seleccionar uno o más valores. Cuando suelta el mouse, las líneas se resaltan. En el siguiente ejemplo, el tipo de servicio SSL se resalta con un cuadro de color gris.



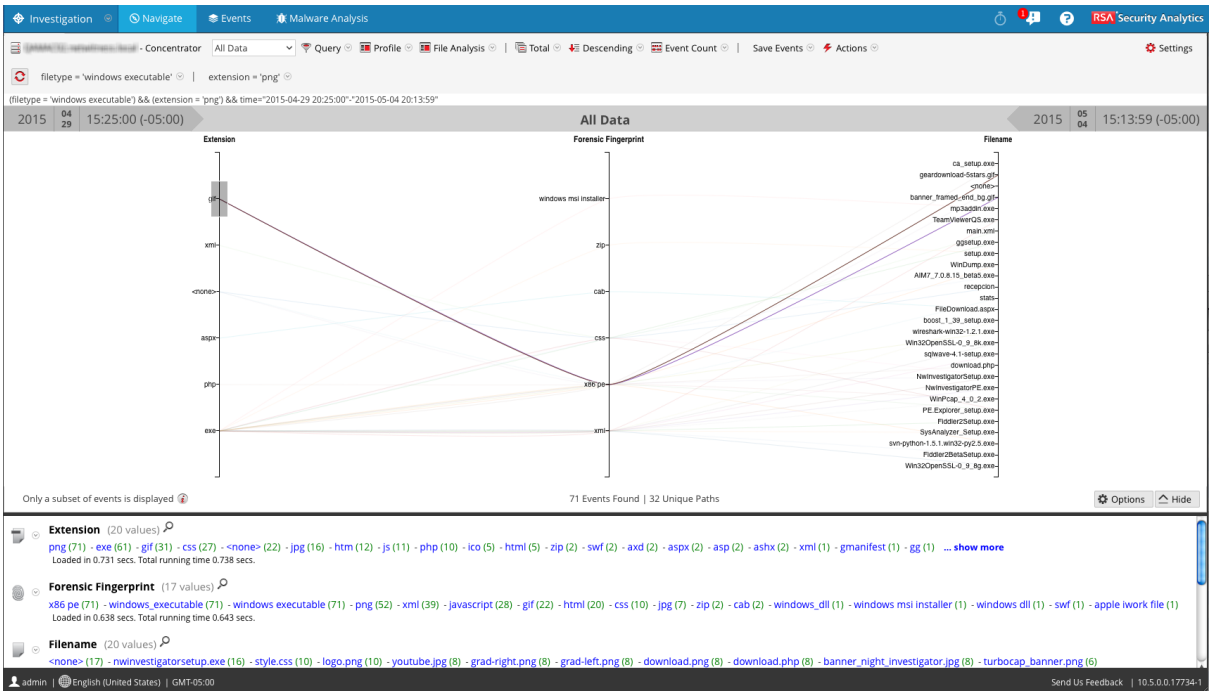
4. Si desea ampliar la visualización, arrastre hacia abajo el borde inferior del panel y ensanche la ventana del navegador desde el borde derecho.

Ejemplo de caso de uso

El siguiente es un ejemplo de una visualización de coordenadas paralelas de claves de metadatos que representa metadatos de archivo en una sesión. Hay tres claves de metadatos o ejes de izquierda a derecha: Extensiones, Huella digital forense y Nombre de archivo con valores que se enumeran a lo largo de cada eje. Los valores del eje Extensión muestran la extensión de archivo y los valores del eje Huella digital forense son archivos ejecutables de Windows. Normalmente, el tipo de archivo coincide con la huella digital forense prevista; sin embargo, es anormal que un tipo de archivo `gif` esté en combinación con la huella digital de archivo ejecutable de Windows. Se selecciona el tipo de archivo `gif` para resaltar las correlaciones de ese tipo de archivo, `x86pe`, y dos nombres de archivo en el tercer eje, de modo que un analista pueda identificar rápidamente los archivos que ameritan una investigación.

Para llegar a esta vista:

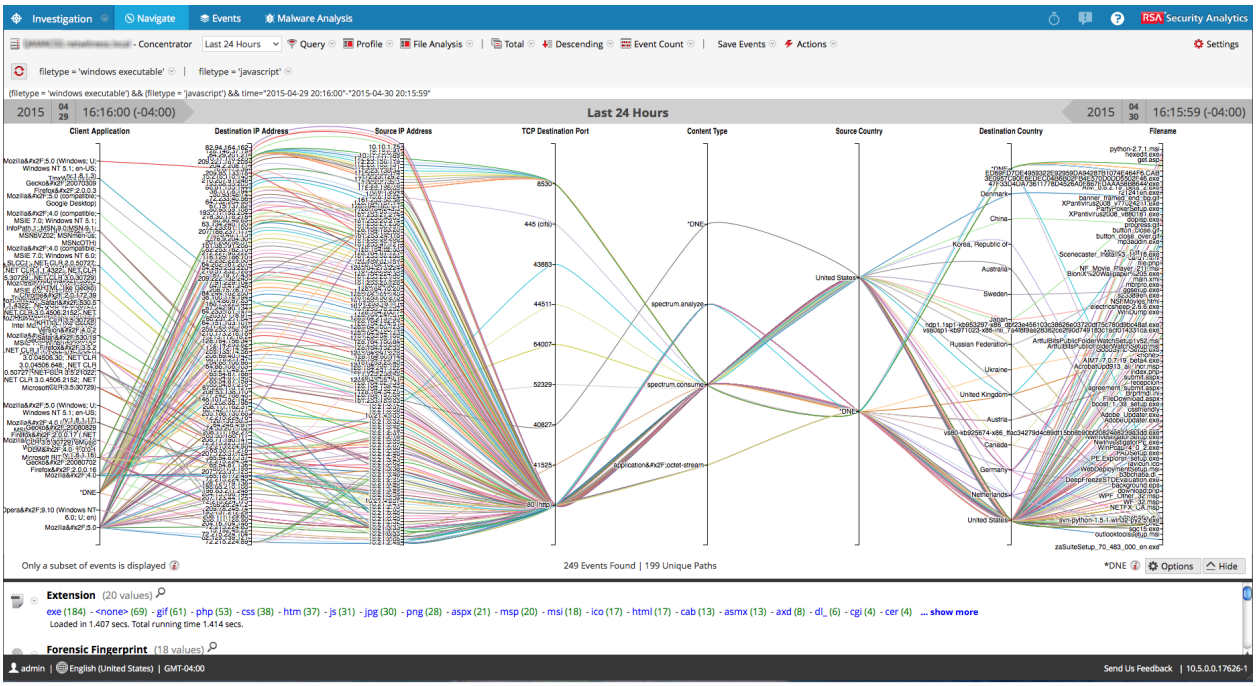
1. Ordene por valor y clasifique en orden ascendente.
2. Aplique dos filtros (file type = 'windows executable' y extension = 'gif') en la vista Navegar para limitar la cantidad de datos.
3. Configure un gráfico de coordenadas paralelas con la selección de tres ejes: `file extension`, `forensic fingerprint` y `filename`.



Ejemplo de la visualización de un conjunto de datos grande

En este ejemplo de una visualización de coordenadas paralelas aplicada a un conjunto de datos más grande se ilustran varios mensajes que ayudan a los analistas a comprender lo que se graficó.

- Para crear un gráfico, NetWitness Platform comienza a escanear valores de metadatos y a devolver resultados. Un rango de tiempo típico podría tener hasta 10,000,000 valores de metadatos. Cuando la cantidad de valores de metadatos devueltos alcanza el Límite de resultados de valores de metadatos, el gráfico se genera incluso si NetWitness Platform no ha escaneado una cantidad de valores de metadatos equivalente al Límite de escaneo de valores de metadatos.
- Hay un límite fijo en la cantidad de datos que se pueden representar como un gráfico de coordenadas paralelas. En NetWitness Platform 10.4 y versiones anteriores, el límite se basa en la cantidad de ejes por los valores de datos: 1,000 x la cantidad de ejes para proteger el rendimiento, pero en NetWitness Platform 10.5 y superior, el administrador configura límites de coordenadas paralelas como parte de los ajustes de Investigation en la vista Sistema de Administration.



Con un conjunto de datos más grande, el procesamiento del gráfico de coordenadas paralelas tarda más que con un conjunto de datos y claves de metadatos más pequeño. Para preservar el rendimiento, NetWitness Platform representa los valores de metadatos del panel Valores de abajo hasta que se alcanzan los límites que estableció el administrador. Un mensaje informativo indica: **Solo se muestra un subconjunto de eventos.**

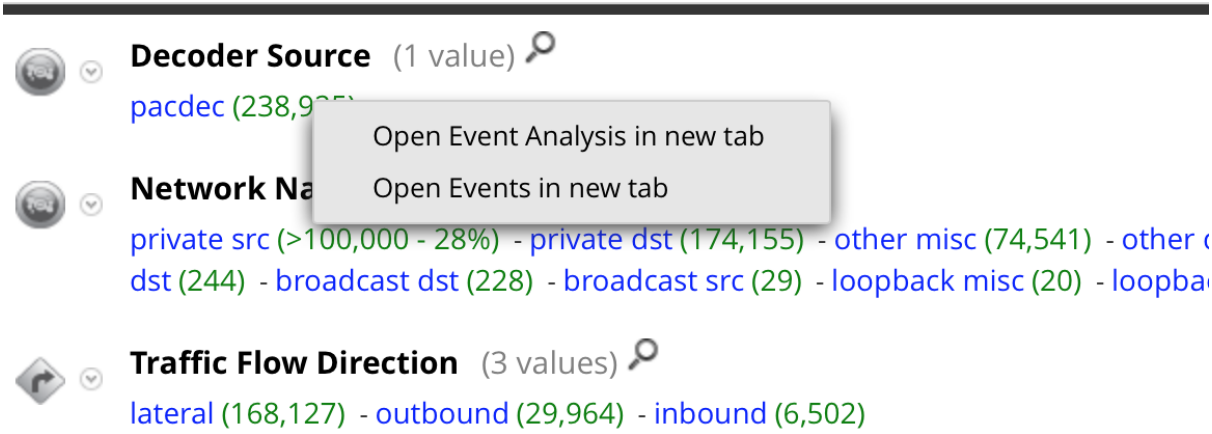
De todos los datos visualizados para 249 eventos, solo hubo 199 rutas de coordenadas paralelas únicas. Ciertos eventos se incluyen aunque no contienen algunas de las claves de metadatos; estos se etiquetan **DNE** debido a que los metadatos no existen en el evento.

Abrir un evento en la lista de eventos

Los analistas pueden ver una lista de eventos asociados a una sesión en la vista Investigar > Eventos o en la vista Análisis de eventos.

Para ver eventos en la vista Eventos, realice una de las siguientes acciones:

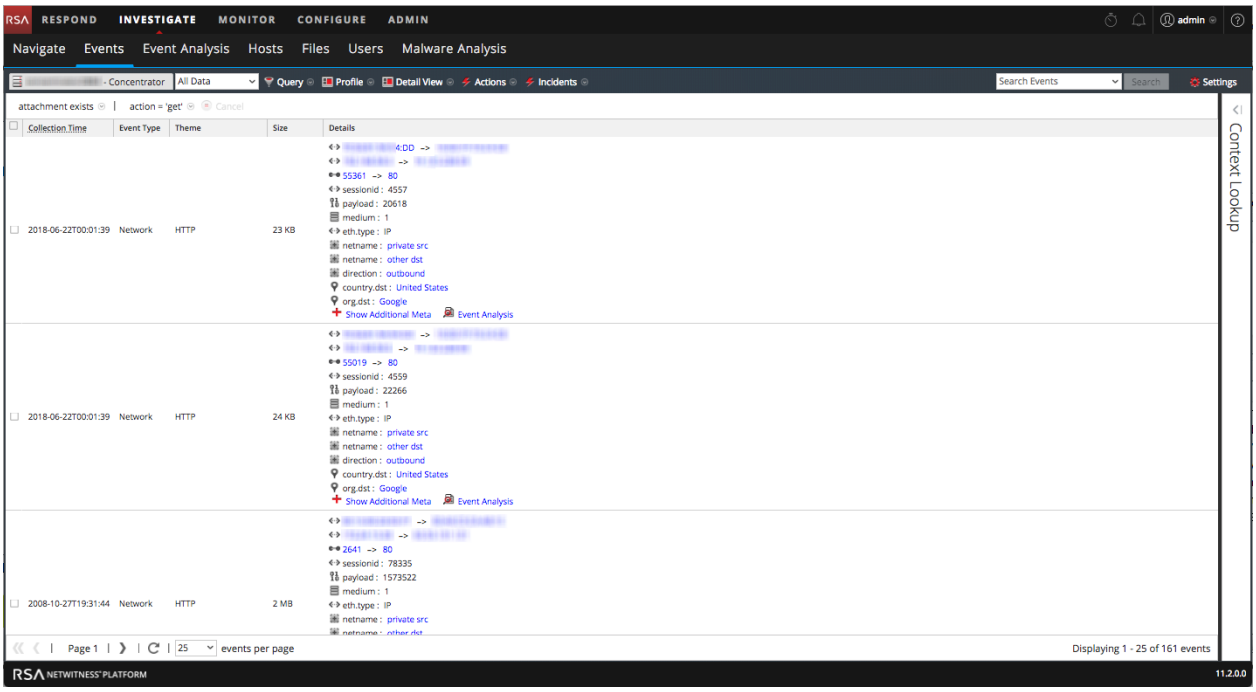
1. Para usar la consulta predeterminada para el servicio predeterminado, vaya a **INVESTIGAR** > **Eventos**.
   NetWitness Platform ejecuta una consulta predeterminada acerca de las últimas tres horas para el servicio predeterminado (si hay uno configurado) o muestra un cuadro de diálogo en el cual puede seleccionar un servicio y, a continuación, ejecuta la consulta predeterminada. La consulta predeterminada selecciona todos los eventos y la vista Eventos muestra los pertinentes al servicio seleccionado, con los más antiguos en primer lugar.
2. Para ver eventos para un valor de metadatos específico, vaya a **INVESTIGAR > Navegar** y, cuando los eventos se hayan cargado en el panel Valores, haga clic en un conteo de metadatos (el conteo de metadatos está en texto de color verde). También puede hacer clic con el botón secundario en el conteo de metadatos de un valor de metadatos. Cuando se muestre el menú contextual, haga clic en **Abrir Eventos en una pestaña nueva**. (La opción Abrir Análisis de eventos en una pestaña nueva está disponible en la versión 11.1 y superior).



La vista Eventos muestra los eventos correspondientes al valor de metadatos seleccionado.

Esta vista proporciona tres presentaciones incorporadas de datos de eventos: la Vista detallada, la Vista de lista y la Vista de registro.

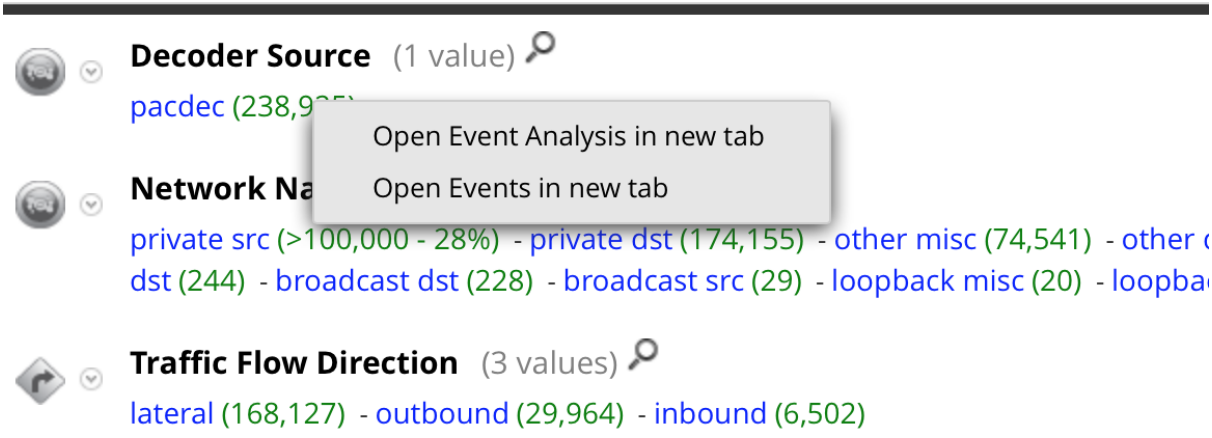
Esta figura es un ejemplo de la vista detallada.



Puede utilizar consultas, la configuración del rango de tiempo y perfiles para filtrar los eventos mostrados en la vista Eventos. Desde cualquier tipo de vista de la vista Eventos, puede extraer archivos, exportar eventos, exportar registros y abrir el panel Reconstrucción de evento si hace doble clic en un evento. Consulte Análisis de eventos crudos en la vista Eventos para obtener información detallada sobre estas funcionalidades.

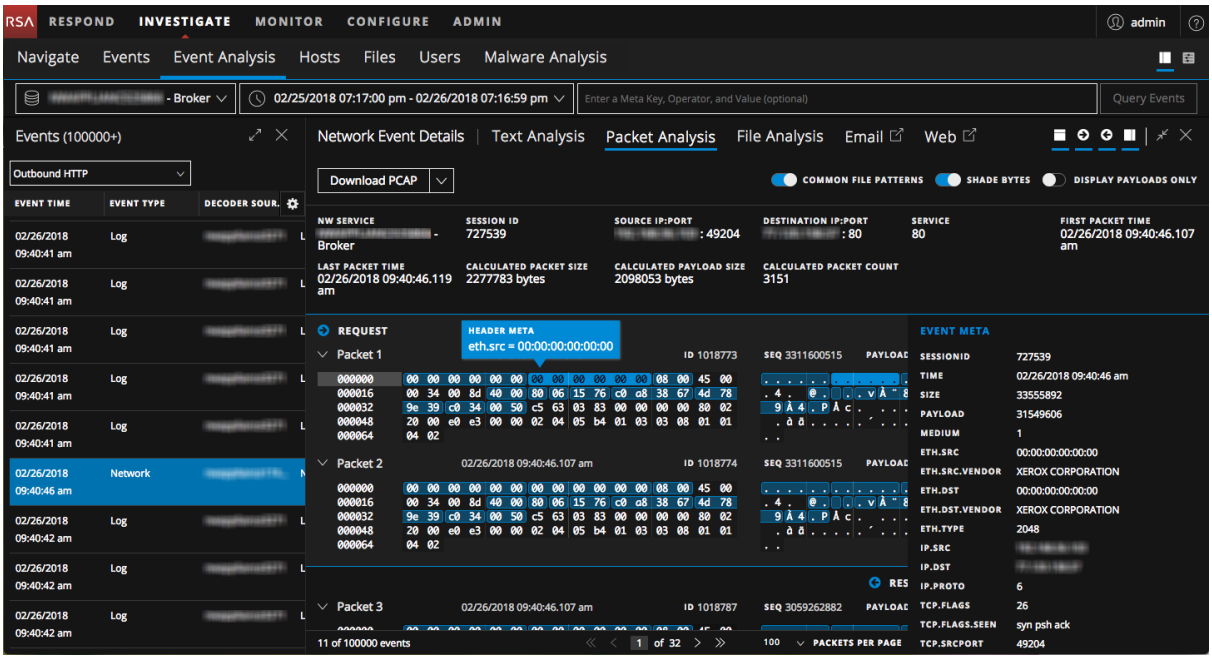
Para ver eventos en la vista Análisis de eventos, realice una de las siguientes acciones:

1. En la versión 11.0 y superior, vaya a **INVESTIGAR > Navegar** y haga clic con el botón secundario en el conteo de metadatos correspondiente a un valor de metadatos (el conteo de metadatos está en texto de color verde). Cuando se muestre el menú contextual, seleccione **Abrir Análisis de eventos** en una pestaña nueva.



La vista Análisis de eventos muestra los eventos correspondientes al valor de metadatos

seleccionado.



Para obtener información detallada acerca de los tipos de análisis que puede usar en esta vista, consulte Análisis de eventos crudos y metadatos en la vista Análisis de eventos.

Exportar o imprimir un punto de desglose

En NetWitness Investigate, cuando se muestran los datos para un punto de desglose en la vista Navegar, puede realizar lo siguiente:

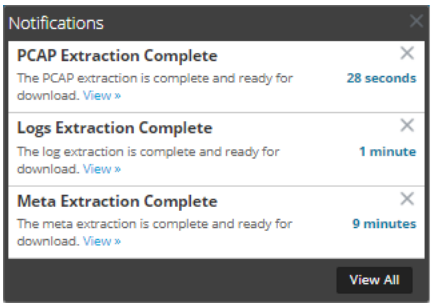
- Extraer archivos desde una sesión y escoger el tipo de archivos que desea extraer: archivos, BitTorrent de audio, documentos, archivos ejecutables, imágenes, otros, videos y archivos web.
- Exportar el punto de desglose como un archivo de captura de paquete (PCAP), un archivo de registro o un archivo de metadatos.
- Imprimir el punto de desglose.

Los detalles que se exporten se verán afectados por el rango de tiempo y el punto de desglose en el momento de la exportación.

Nota: cuando exporta el punto de desglose como un archivo de registro, solo se exportan las sesiones de registro. El mensaje de la línea de espera de trabajos se refiere a la cantidad total de sesiones en el punto de desglose y no a la cantidad de registros. Por ejemplo, si el punto de desglose tiene 505 sesiones y solo cinco sesiones de registro, el mensaje de la línea de espera de trabajos indica que NetWitness Platform está extrayendo registros para 505 sesiones.

Para exportar un punto de desglose desde la vista Navegar:

1. Realice una investigación hasta llegar al punto de desglose deseado.
2. Para la versión 11.0, en la barra de herramientas, seleccione **Acciones > Exportar** y seleccione una de las opciones de exportación: **PCAP**, **Registros** o **Metadatos**.
   Se extrae el punto de desglose y un mensaje informa que el trabajo está programado. Puede revisar la página de trabajos para el estado.
3. Para la versión 11.1, en la barra de herramientas, seleccione **Guardar eventos** y elija una de las opciones de exportación: **PCAP**, **Registros**, **Archivos** o **Metadatos**.
   Un cuadro de diálogo le brinda la oportunidad de editar el nombre de archivo predeterminado para el archivo. El valor predeterminado es el formato `investigation-Feb-21-15-44-33`. Cuando exporta un PCAP, el archivo se exporta sin opción de formato. Si está utilizando una de las otras opciones de exportación, se muestra un cuadro de diálogo.
4. En el cuadro de diálogo, seleccione lo siguiente:
   - El formato de registro de exportación: **Texto**, **XML**, **CSV** o **JSON**.
   - Los tipos de archivos que se exportarán: archivos, audio, BitTorrent, documentos, archivos ejecutables, imágenes, otros, video y Web.
   - El formato de los metadatos: **Texto**, **CSV**, **TSV** o **JSON**.
5. Cuando se completa la extracción de archivos programada, se muestra en la bandeja Notificaciones de trabajos.



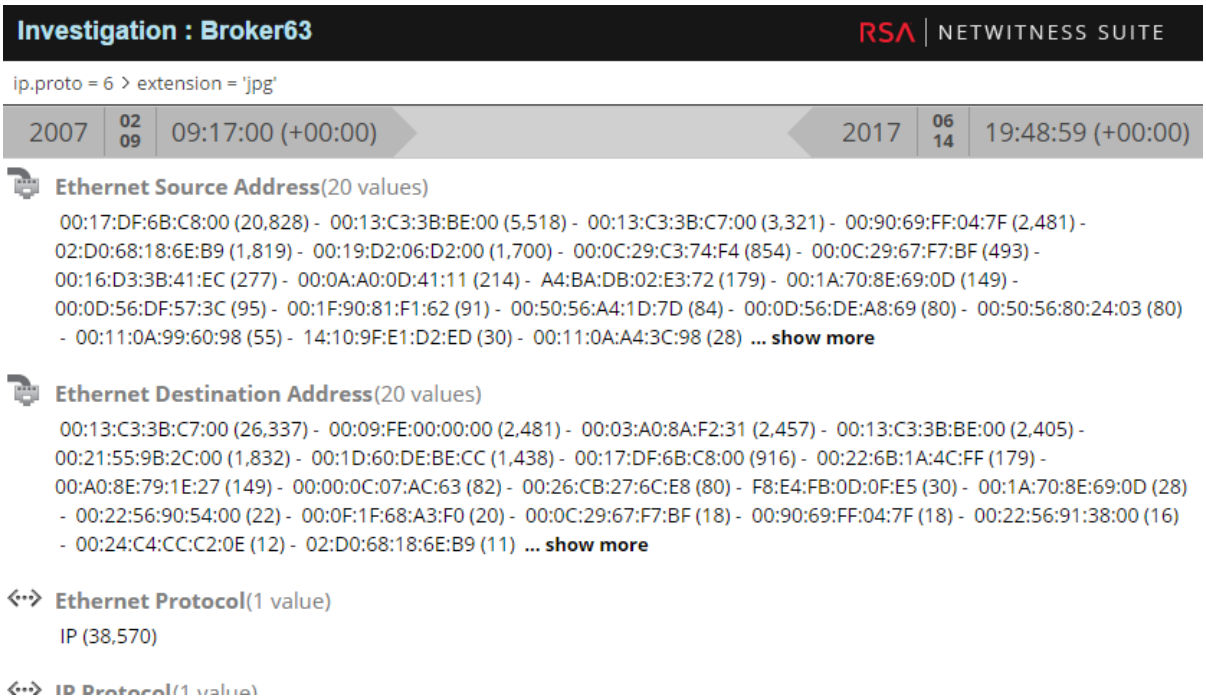
6. Haga clic en el vínculo **Ver** de la bandeja Trabajos y descargue el archivo de extracción específico solicitado.

Para imprimir el punto de desglose actual:

En la vista Navegar, puede mostrar el contenido del punto de desglose actual en formato para impresión en la ventana del navegador.

Para mostrar el punto de desglose en una vista de impresión:

1. Con un punto de desglose abierto en la vista **Navegar**, seleccione **Acciones** > **Imprimir** en la barra de herramientas.
   Se crea una nueva pestaña con la vista de impresión del punto de desglose actual.



2. Use la opción de impresión en el navegador para enviar la vista imprimible a la impresora.

Iniciar una búsqueda externa de una clave de metadatos

En este tema se proporcionan instrucciones para usar plug-ins de Investigate de manera inmediata con el fin de iniciar una búsqueda externa de claves de metadatos específicas mediante herramientas externas a NetWitness Platform durante la investigación de datos en las vistas Navegar o Eventos.

Los analistas pueden usar búsquedas externas a NetWitness Platform Investigate de manera inmediata para ahorrar tiempo durante las investigaciones. Las búsquedas de uso inmediato están disponibles cuando se hace clic con el botón secundario en una de estas claves de metadatos: Dirección IP (`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`), `host (alias-host, domain.dst)`, `client`, y `file-hash`.

En el caso de todas las claves de metadatos `IP` y `host`, las siguientes búsquedas están incorporadas en NetWitness Platform:

- Google Malware: abre una búsqueda en Google Malware en una nueva pestaña.
- Historial de IP SANS: Abre una búsqueda en el historial de IP SANS en una nueva pestaña.
- McAfee SiteAdvisor: abre una búsqueda en McAfee SiteAdvisor en una nueva pestaña.
- Búsqueda del cliente grueso de Endpoint: Abre una búsqueda en el cliente grueso de NetWitness Endpoint en una nueva pestaña.
- Recopilación de DNS pasivo de BFK: Abre una búsqueda en una recopilación de DNS pasivo de BFK en una nueva pestaña.
- CentralOps Whois para direcciones IP y nombres de host: Abre una búsqueda en CentralOps Whois de direcciones IP y nombres de host en una nueva pestaña.
- Búsqueda en Malwaredomainlist.com: abre una búsqueda en Malwaredomainlist.com en una nueva pestaña
- Búsqueda de dirección IP en Robtex: Abre una búsqueda de dirección IP en Robtex en una nueva pestaña.
- Búsqueda en ThreatExpert: abre una búsqueda en ThreatExpert en una nueva pestaña
- Búsqueda en IPVoid: abre una búsqueda en UrlVoid en una nueva pestaña

Para las claves de metadatos `file-hash` y `alias-host`, la búsqueda en Google abre una búsqueda en Google en una nueva pestaña.

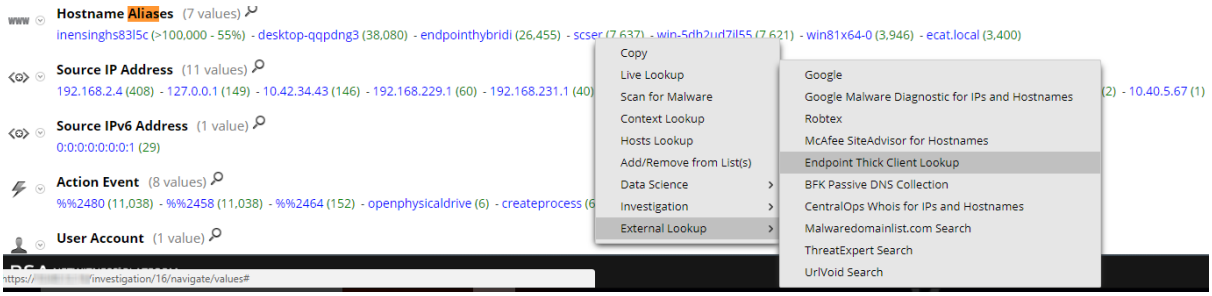
Para la clave de metadatos `client`, la opción Búsqueda en NetWitness Endpoint abre un cliente de grueso de Endpoint en una nueva pestaña si el cliente está instalado en el mismo sistema en el cual se usa el navegador.

Los administradores pueden agregar búsquedas externas adicionales y otras acciones personalizadas, como se describe en "Agregar acciones de menú contextual personalizadas" en la *Guía de configuración del sistema*.

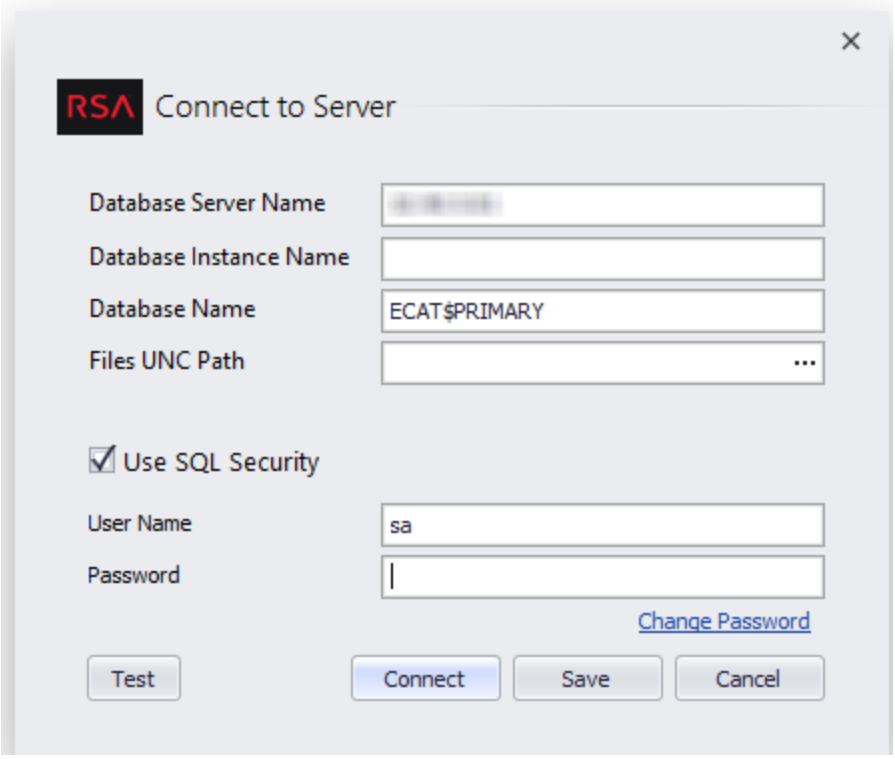
Iniciar una búsqueda en el cliente grueso de Endpoint

Para iniciar una búsqueda de datos en el cliente grueso de Endpoint desde la vista Navegar:

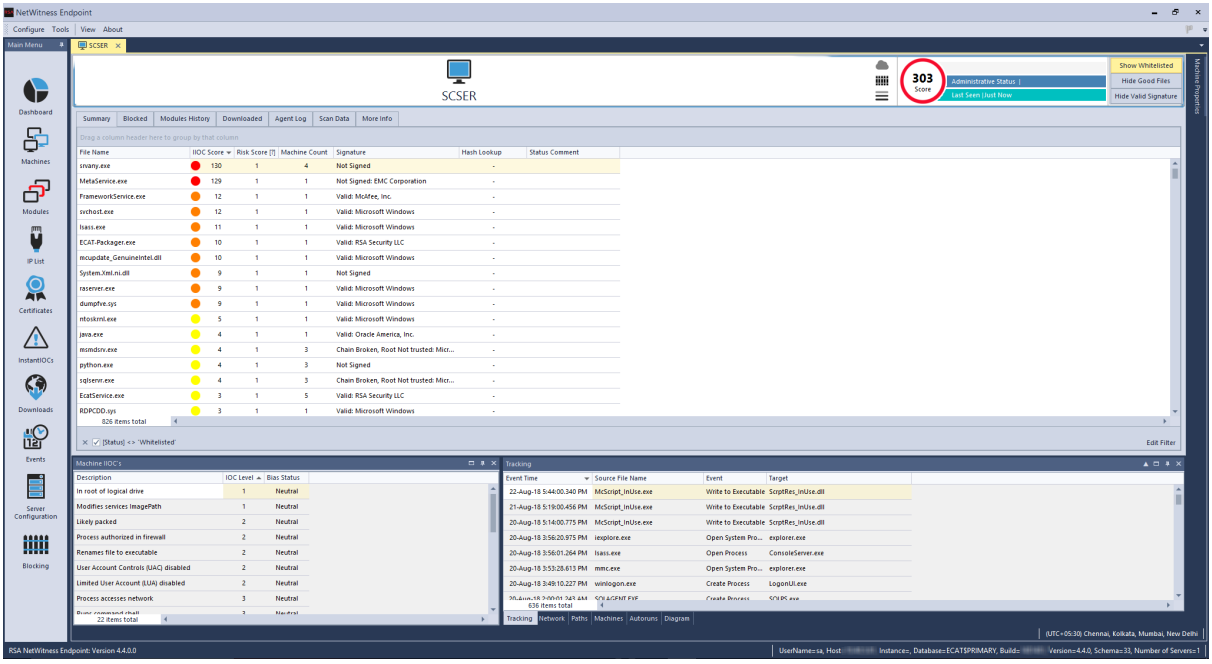
1. Haga clic con el botón secundario en un valor de metadatos para una de las siguientes claves de metadatos: `ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`, `alias-host`, `domain.dst`, `client`.
2. Seleccione **Búsqueda externa** en el menú contextual.
   Se muestra un submenú de opciones de la búsqueda externa.



3. Seleccione **Búsqueda del cliente grueso de Endpoint**.
   Se muestra el cuadro de diálogo Conectar a servidor.



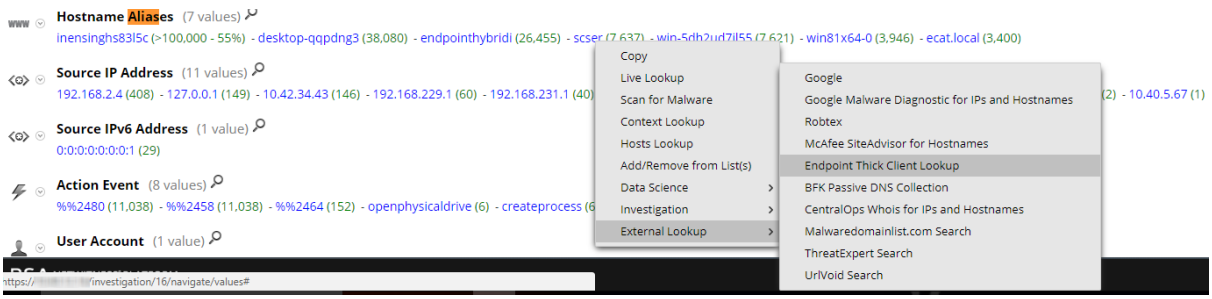
4. Ingrese el nombre de usuario y la contraseña que se requieren para iniciar sesión en el cliente grueso de Endpoint y haga clic en **Conectar.**
   El punto de desglose se abre en NetWitness Endpoint.



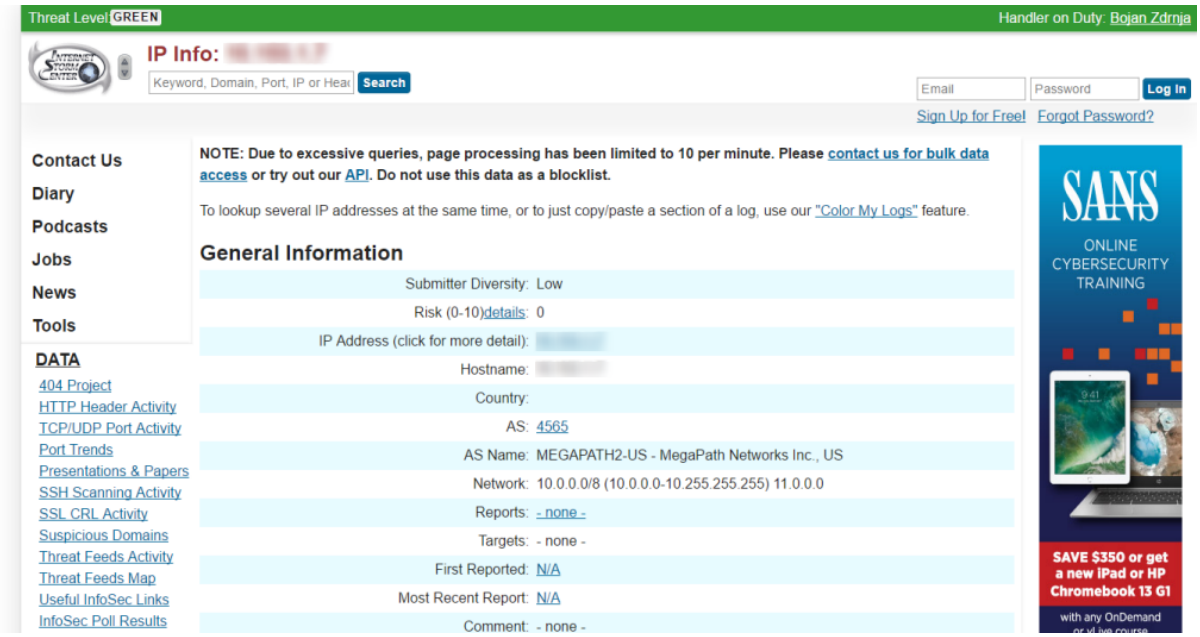
Iniciar otras búsquedas externas

Para iniciar una búsqueda externa de datos (distinta de la búsqueda del cliente de grueso de NetWitness Endpoint) desde la vista Navegar:

1. Haga clic con el botón secundario en un valor de metadatos para una de las siguientes claves de metadatos: `ip-src`, `ip-dst`, `ipv6-src`, `ipv6-dst`, `orig_ip`, `alias-host`, `domain.dst`, `client`.
2. Seleccione **Búsqueda externa** en el menú contextual.
   Se muestra un submenú de opciones de la búsqueda externa.



3. Seleccione una de las opciones de búsqueda.
   El valor de metadatos seleccionado se abre en la búsqueda seleccionada. Por ejemplo, si seleccionó Historial de IP SANS, la información del punto de desglose se muestra en SANS Internet Storm Center.

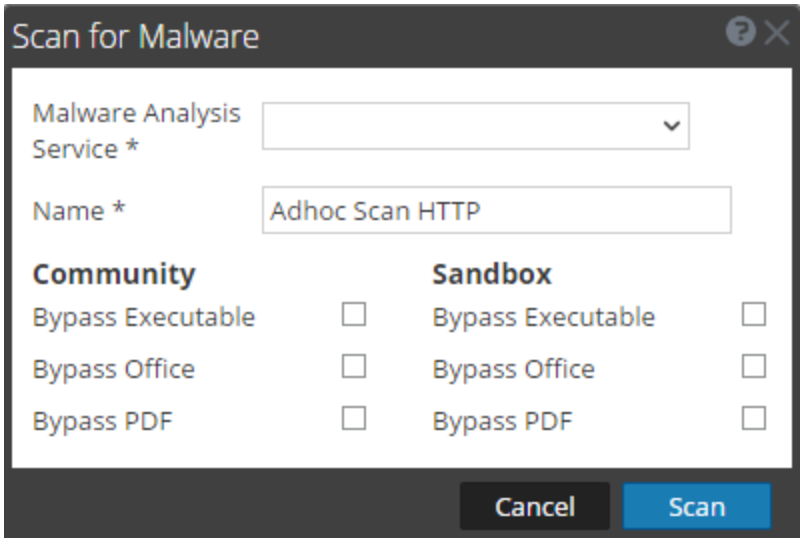

Threat Level: GREEN
Handler on Duty: Bojan Zdrnja
IP Info:
Keyword, Domain, Port, IP or Head
Search
Email
Password
Log In
Sign Up for Free!
Forgot Password?
Contact Us
Diary
Podcasts
Jobs
News
Tools
DATA
404 Project
HTTP Header Activity
TCP/UDP Port Activity
Port Trends
Presentations & Papers
SSH Scanning Activity
SSL CRL Activity
Suspicious Domains
Threat Feeds Activity
Threat Feeds Map
Useful InfoSec Links
InfoSec Poll Results
NOTE: Due to excessive queries, page processing has been limited to 10 per minute. Please contact us for bulk data access or try out our API. Do not use this data as a blocklist.
To lookup several IP addresses at the same time, or to just copy/paste a section of a log, use our "Color My Logs" feature.
General Information
Submitter Diversity: Low
Risk (0-10)details: 0
IP Address (click for more detail):
Hostname:
Country:
AS: 4565
AS Name: MEGAPATH2-US - MegaPath Networks Inc., US
Network: 10.0.0.0/8 (10.0.0.0-10.255.255.255) 11.0.0.0
Reports: - none -
Targets: - none -
First Reported: N/A
Most Recent Report: N/A
Comment: - none -
SANS
ONLINE CYBERSECURITY TRAINING
SAVE $350 or get a new iPad or HP Chromebook 13 G1
with any OnDemand

Iniciar un escaneo de Malware Analysis desde la vista Navegar

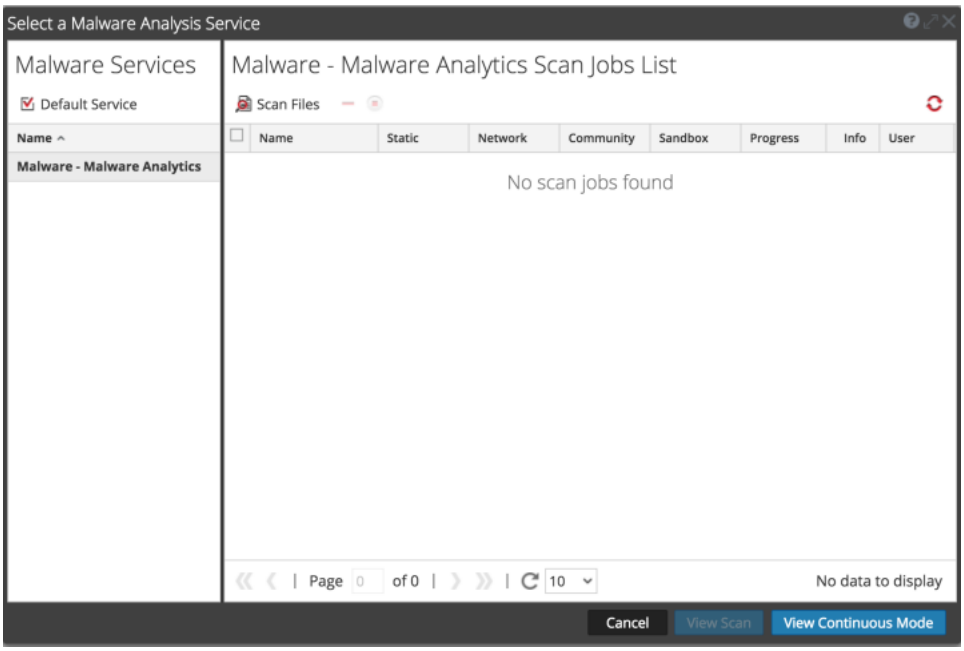
Desde Investigate, los analistas pueden iniciar un escaneo de Malware Analysis según demanda mediante la selección de un servicio y un valor de metadatos, así como de una opción del menú contextual. Cuando finaliza el sondeo, los datos escaneados están disponibles para Malware Analysis.

Para iniciar un escaneo de datos de Malware Analysis en la vista INVESTIGAR > Navegar:

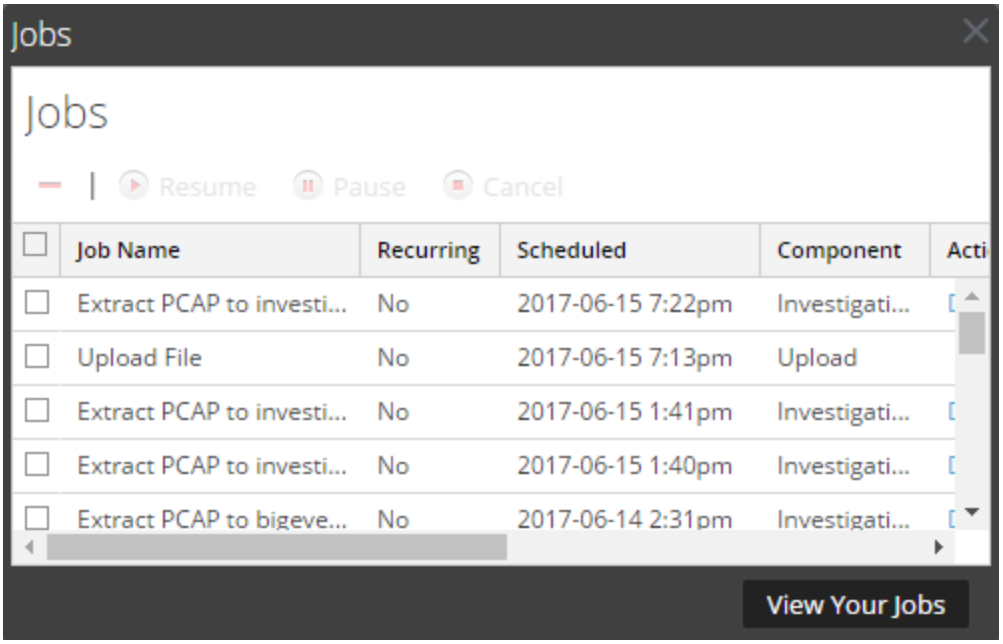
1. Haga clic con el botón secundario en un valor de metadatos (por ejemplo, OTHER, DNS o FTP) y seleccione **Escanear para encontrar malware** en el menú contextual.
   Se muestra el cuadro de diálogo Escanear para encontrar malware con un nombre sugerido para el escaneo según demanda y ningún servicio seleccionado.
2. En el cuadro de diálogo Escanear para encontrar malware, seleccione un servicio para ejecutar el escaneo, edite el nombre y seleccione los tipos de archivos que desea omitir en Comunidad y Sandbox.



3. Haga clic en **Escanear**.
   La solicitud de escaneo se agrega al dashlet Lista de trabajos de escaneo y a la bandeja de trabajos. La configuración de omisión en este cuadro de diálogo reemplaza a la configuración predeterminada definida en los ajustes de configuración básicos de Malware Analysis.
4. Para ver los trabajos, realice una de las siguientes acciones:
   a. Vaya a la Lista de trabajos de escaneo en la vista Malware Analysis o en el tablero Unified. Haga doble clic en un escaneo para verlo.



b. Para ver el trabajo en la bandeja de trabajos, haga clic en  en la barra de herramientas de NetWitness Platform. Cuando el trabajo se complete, desplácese a la izquierda y haga clic en **Ver**.



Se muestra el Resumen de eventos de malware del escaneo seleccionado. El escaneo también se agrega a la lista de escaneos disponibles en el cuadro de diálogo para seleccionar escaneos en la pestaña Investigation > Malware.

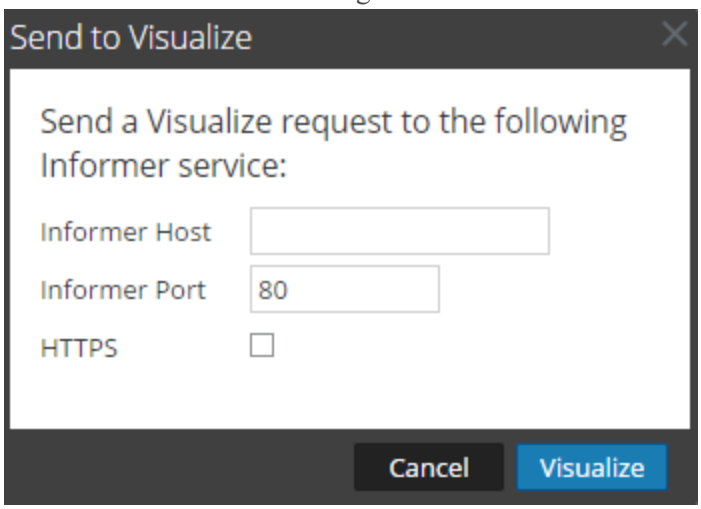
Visualizar el punto de desglose actual en Informer

En este tema se proporcionan instrucciones para enviar un punto de desglose en la vista Navegar a una visualización de Informer.

Informer debe estar instalado en la red y el servicio que se está investigado debe poder acceder a él. Necesita proporcionar el nombre de host y el puerto que se usa en el host de Informer para comunicarse con NetWitness Platform.

Para mostrar una visualización en Informer del punto de desglose actual:

1. Con un punto de desglose abierto en la vista Navegar, haga clic en **Acciones > Visualizar**.
   Se muestra el cuadro de diálogo Enviar a visualización.



2. Escriba el nombre de host o la dirección IP de Informer y verifique el puerto del servidor de NetWitness Platform que se utiliza para comunicarse con el host de Informer.
3. (Opcional) Seleccione la opción HTTPS si el host de Informer utiliza comunicaciones seguras.
4. Haga clic en **Visualizar**.
   La visualización se muestra en una pestaña nueva.

Análisis de eventos crudos en la vista Eventos

Los analistas que investigan datos en Investigar pueden ver y reconstruir eventos asociados con una sesión.

- Los analistas que realizan análisis con NetWitness Platform Investigate y que tienen configuradas las funciones y los permisos del sistema correspondientes para sus cuentas de usuario pueden ir desde el punto de desglose de la vista Navegar a la vista Eventos.
- Los analistas que no tienen acceso a la vista Navegar o que desean ir directamente a la vista Eventos pueden abrir sesiones y examinar los eventos que componen la sesión en la vista Eventos.
- Los analistas pueden seleccionar consultas en su ventana de “historial de consultas”.

Cada tema describe los métodos de trabajo en la vista Eventos:

- Filtrar y buscar resultados en la vista Eventos
- Administrar grupos de columnas en la vista Eventos
- Exportar eventos en la vista Eventos
- Agregar eventos a un incidente para Response
- Combinar eventos desde sesiones divididas

Además, puede utilizar estos métodos para consultar datos y actuar sobre los resultados que son comunes para las vistas Navegar y Eventos.

- Buscar patrones de texto
- Crear una consulta personalizada
- Ver y modificar consultas mediante la integración de URL
- Usar perfiles para encapsular vistas personalizadas
- Administrar listas y valores de lista de Context Hub en las vistas Navegar y Eventos
- Buscar contexto adicional en las vistas Navegar y Eventos
- Reconstruir un evento

Filtrar y buscar resultados en la vista Eventos

Los analistas pueden filtrar los resultados en la vista Eventos y, mediante la búsqueda de eventos o la selección del servicio en el cual se verán, configurar el rango de tiempo y consultar metadatos.

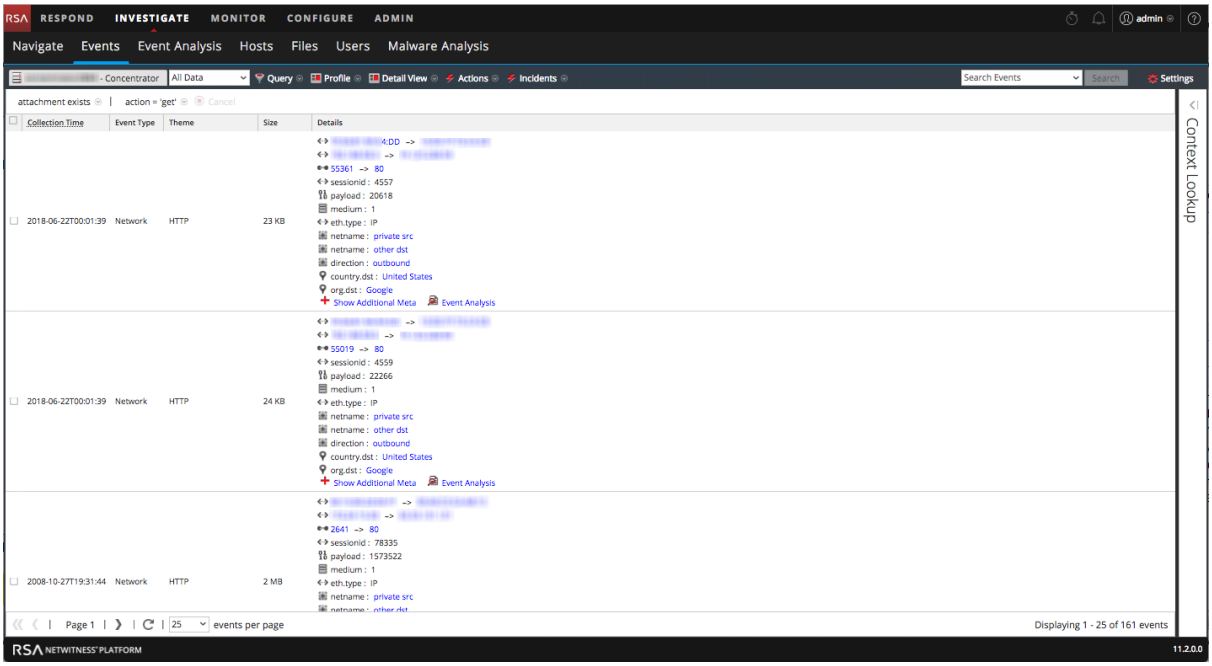
Si abrió la vista Eventos desde un punto de desglose de la vista Navegar, de forma predeterminada la vista se abre en la Vista detallada de eventos. Los analistas que no tienen permisos para utilizar la vista Navegar pueden consultar servicios directamente en la vista Eventos. Hay varias opciones de configuración para filtrar la información que se muestra en la vista Eventos.

Nota: Cuando un Archiver es el servicio seleccionado actualmente en la vista Eventos y se busca contra un Broker o un Concentrator, la búsqueda es más lenta que si se busca contra un Broker o un Concentrator porque los datos del Archiver están comprimidos y normalmente son más.

Filtrar los eventos que se muestran en la vista Eventos

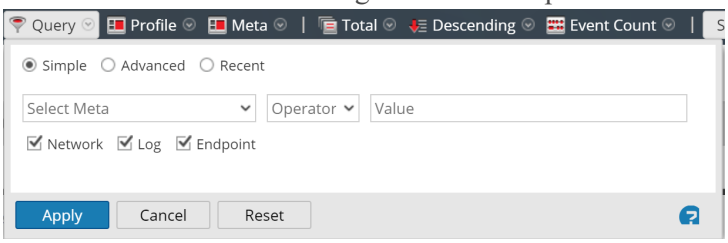
Para filtrar los datos que se muestran en la vista Eventos:

1. Vaya a **INVESTIGAR** > **Eventos**.
   La vista Eventos se muestra de manera predeterminada con la vista Detalle.

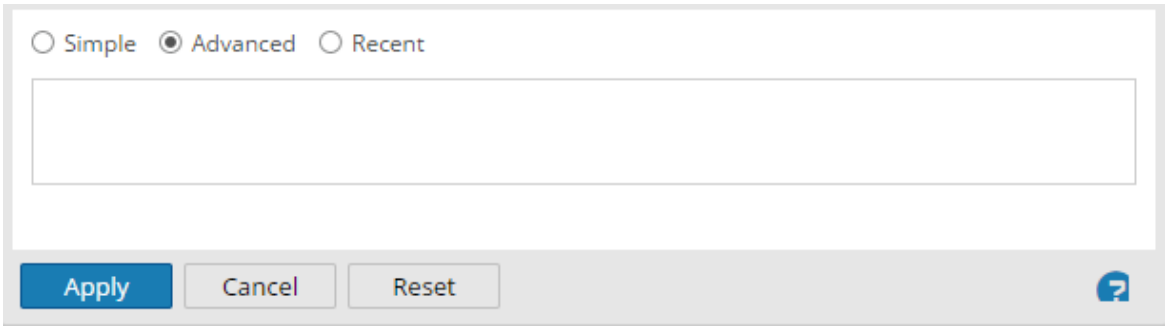


2. Para seleccionar un rango de tiempo distinto del predeterminado (**Últimas 3 horas**), haga clic en el campo de rango de tiempo de la barra de herramientas y seleccione un valor. Por ejemplo, **Última hora**.
   La vista Eventos se actualiza con el rango de tiempo seleccionado.
3. Para ingresar una consulta para el servicio y el rango de tiempo seleccionados, en la barra de herramientas, haga clic en **Consulta**.

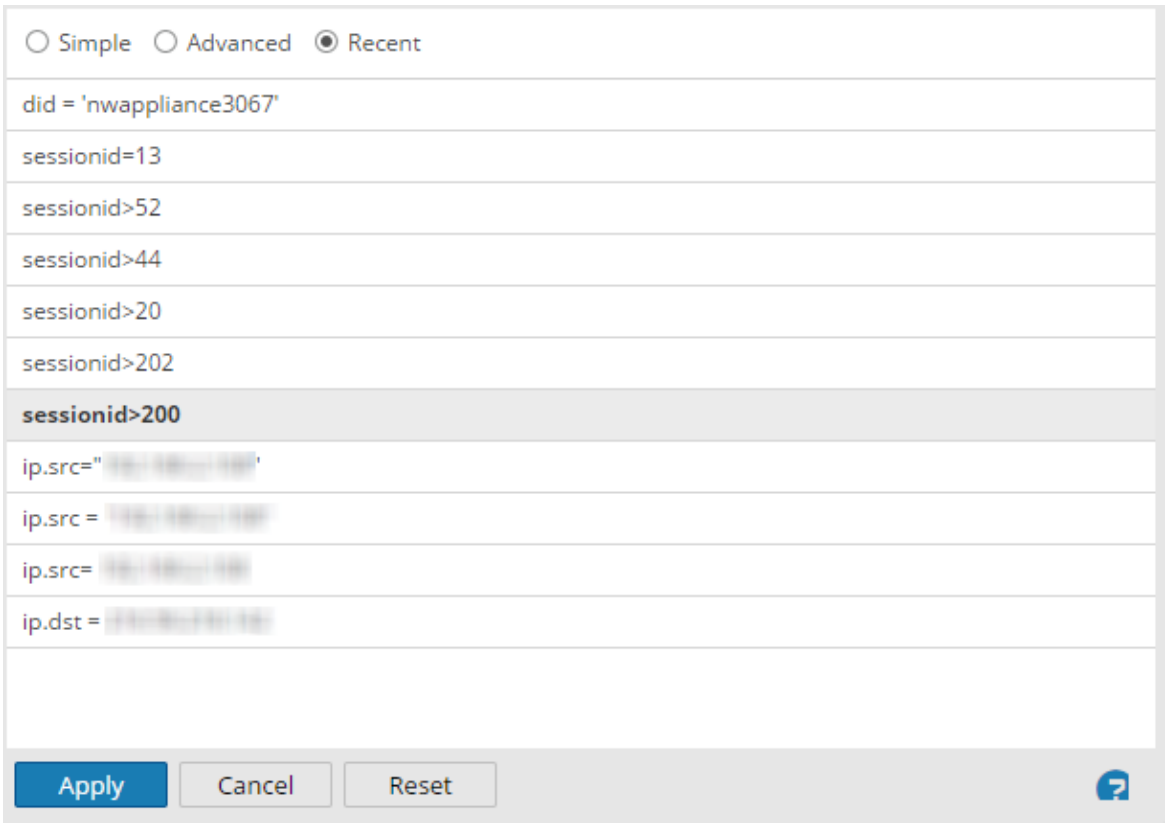
Se muestra el cuadro de diálogo Consulta simple.



4. Si desea ingresar una consulta simple con la función de autocompletado para seleccionar metadatos y operadores, realice una de las siguientes acciones:
   a. Haga clic en el campo **Seleccionar metadatos** y seleccione una clave de metadatos de la lista desplegable.
   b. En el campo **Operador**, seleccione un operador de la lista desplegable.
   c. Escriba un valor que coincida en el campo **Valor**.
   d. Seleccione datos de **Red, Registro** o **Terminal** y haga clic en **Aplicar**.
      Los datos coincidentes se muestran en la vista Eventos.
5. Si desea ingresar una consulta más compleja en función de su conocimiento de los metadatos y operadores:
   a. Haga clic en **Avanzada**.
      Se muestra el cuadro de diálogo Consulta avanzada.



   b. Escriba una consulta. A medida que escribe la consulta, a partir de la clave de metadatos, se muestran listas desplegables de claves de metadatos y operadores disponibles. Cuando termine, haga clic en **Aplicar**.
6. Si desea seleccionar una consulta en una lista de consultas recientes:
   a. Seleccione **Reciente**.
      Se muestra el cuadro de diálogo Consulta reciente.



b. Seleccione una consulta y haga clic en **Aplicar**.
Los resultados coincidentes de la consulta se muestran en la vista Detalle de la vista Eventos. La ruta de navegación refleja la consulta.

c. En la ruta de navegación, puede hacer clic en cualquiera de las rutas para mostrar el menú Consulta. Puede insertar una nueva consulta antes de una ruta de navegación y agregar una nueva consulta al final de la ruta. Después de cada edición en la ruta de navegación, NetWitness Platform actualiza los resultados.

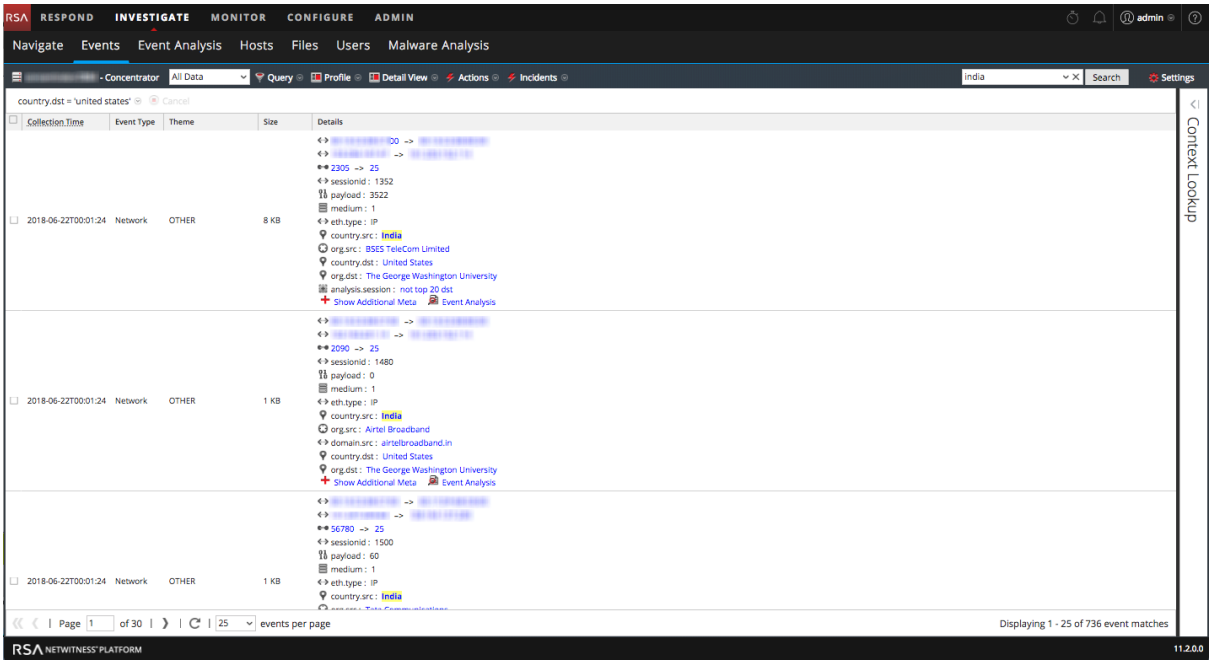
Buscar eventos en la vista Eventos

Puede buscar los datos que se muestran actualmente en la vista Eventos mediante el ingreso de una cadena de búsqueda en el campo Buscar. La cadena de búsqueda puede ser regex (expresión regular) o puede ser una búsqueda de texto simple. Se proporciona información detallada sobre estos tipos de búsqueda.

Para buscar en los datos que se muestran actualmente en la vista Eventos:

1. Para ejecutar la búsqueda, coloque el cursor en el cuadro Buscar, escriba una cadena de búsqueda y presione **Intro** o haga clic en **Buscar**.
Los resultados de búsqueda se muestran en la vista Eventos. Los eventos que coinciden con los criterios de búsqueda se muestran en la cuadrícula de la vista Eventos. En la vista Detalles y en la vista Lista, las coincidencias se resaltan en la columna Detalles. Además, cuando busca RAW, las coincidencias se resaltan en el columna Registros de la vista Registro. A continuación se muestra un

ejemplo de los resultados de búsqueda para el término **India** en la vista Detalles de eventos. Observe que las coincidencias de la búsqueda no se destacan en ninguna reconstrucción de evento.



2. Si desea limitar la búsqueda, cambie la consulta y la hora como se describe en Filtrar los eventos que se muestran en la vista Eventos.
3. Si desea detener la búsqueda y volver a la vista Eventos, haga clic en **Cancelar**.
   Se conserva cualquier resultado que se muestre.
4. Para borrar el cuadro de búsqueda y volver a la vista Eventos normal, haga clic en **X** en el cuadro de búsqueda.

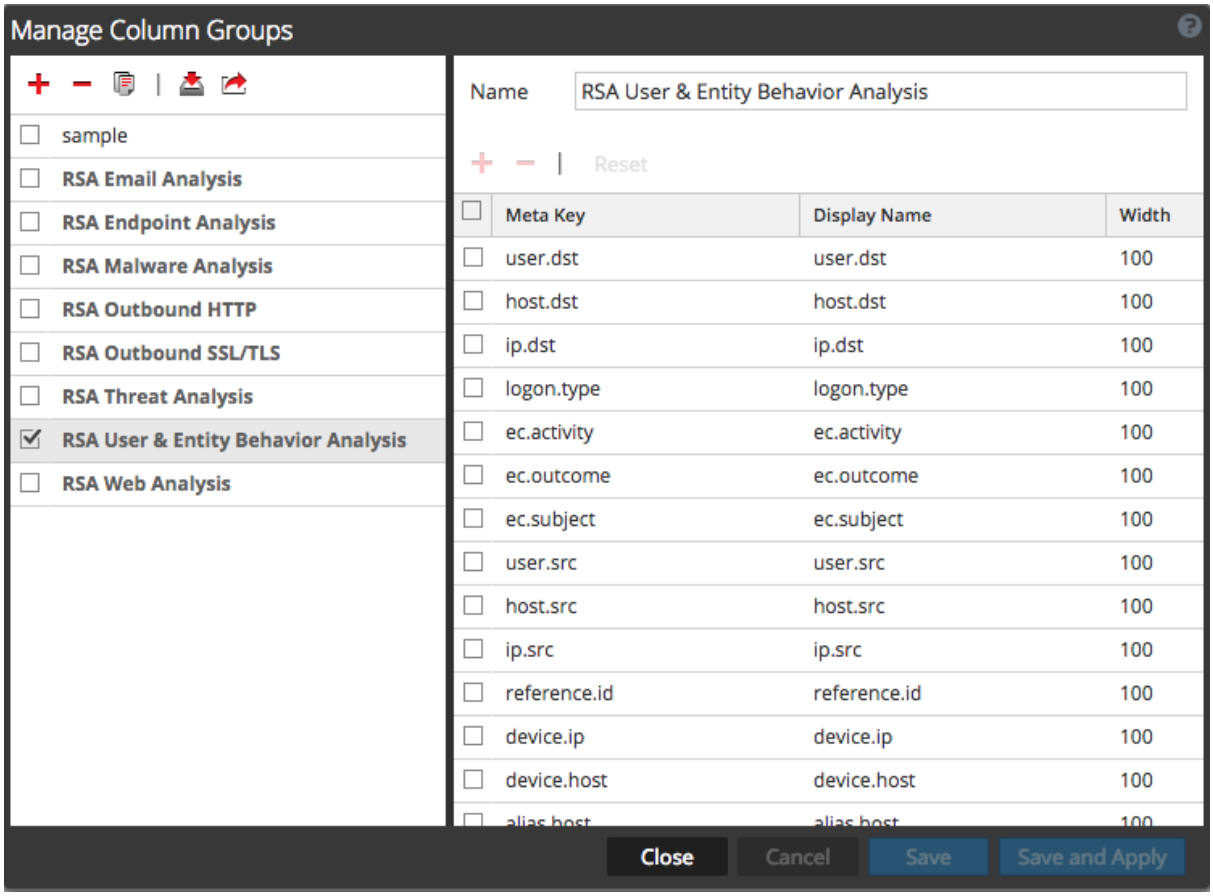
Administrar grupos de columnas en la vista Eventos

Cuando observa una lista de eventos en la vista Eventos, puede personalizar la manera en que se muestran los datos mediante la definición de la clave de metadatos que se muestra en una columna, la posición de la columna en la cuadrícula y el ancho predeterminado de la columna.

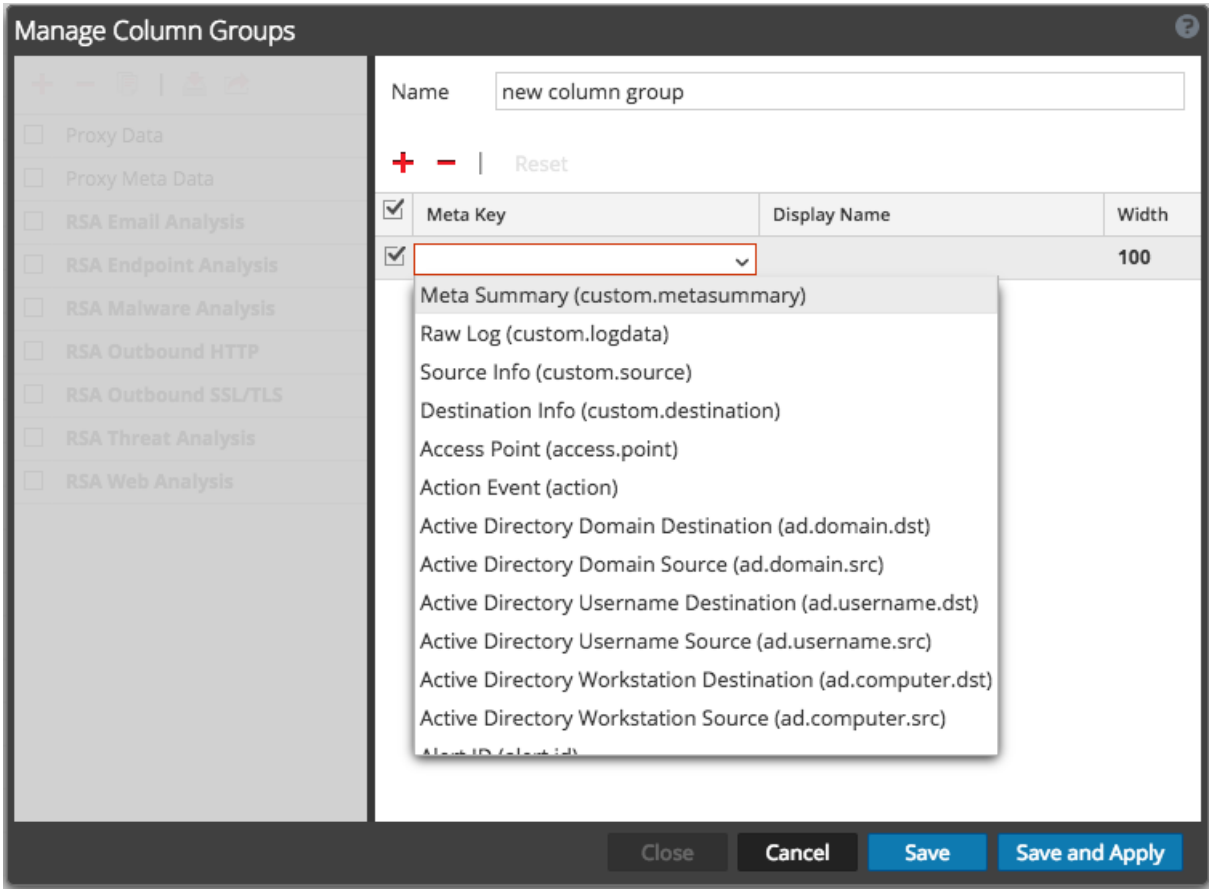
Nota: En la versión 11.1 y superior, cuando se usan claves de metadatos, también se pueden usar entidades de metadatos configuradas.
Los perfiles de Investigate pueden incluir grupos de columnas personalizados. Si se utiliza un grupo de columnas personalizado en un perfil y se observan eventos en la vista Eventos con el uso de un grupo de columnas personalizado, no se puede cambiar el tipo de vista (Detalle, Lista o Registro).

Crear un grupo de columnas personalizado

1. Vaya a **NAVEGAR** > **Eventos**.
2. Seleccione **Administrar grupos de columnas** en el menú desplegable **Ver**. El nombre de la opción Ver tiene relación con el valor actual, por ejemplo, la Vista detallada, la Vista de lista y la Vista de registro, o con el grupo de columnas seleccionado.
   Se muestra el cuadro de diálogo Administrar grupos de columnas.

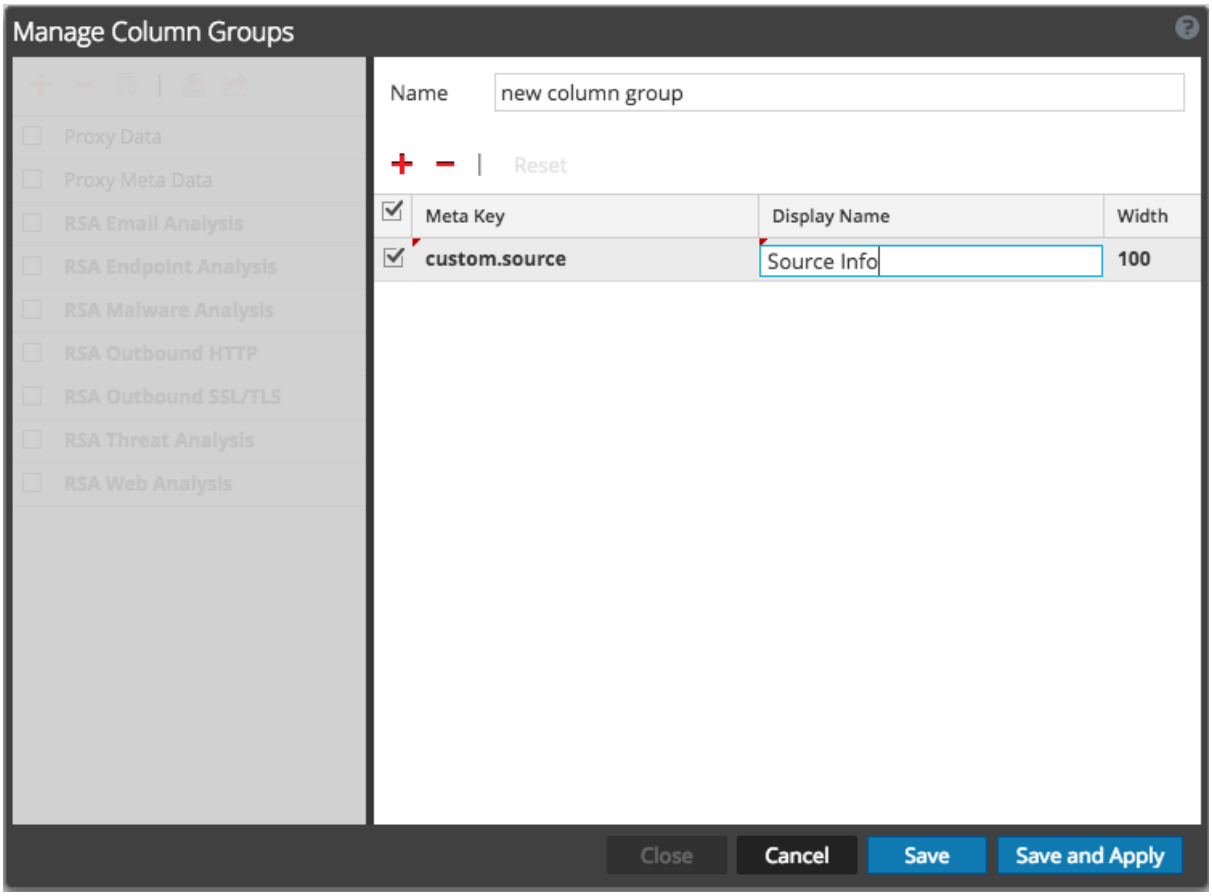


3. Para agregar un nuevo grupo de columnas en el panel de grupos de columnas, haga clic en + e ingrese el nombre del nuevo grupo en el campo resultante.
   El panel de definición de columnas se abre en el lado derecho y el nombre del grupo aparece completado. Puede editar el nombre del grupo.
4. Para agregar una columna al grupo, haga clic en + y, a continuación, haga clic en el campo vacío **Clave de metadatos** para mostrar la lista desplegable **Clave de metadatos**. Seleccione un campo de clave de metadatos en la lista y repita este paso hasta que el conjunto de columnas esté completo.



5. (Opcional) Para eliminar una clave de metadatos del grupo de columnas, haga clic en −.
6. (Opcional) Para volver a ordenar la secuencia en la cual aparecen las columnas en la lista Eventos, arrastre claves de metadatos a la posición que desee.

7. (Opcional) Para configurar el ancho predeterminado de una columna, haga clic en el valor correspondiente en la columna **Ancho** e ingrese un nuevo ancho de columna.

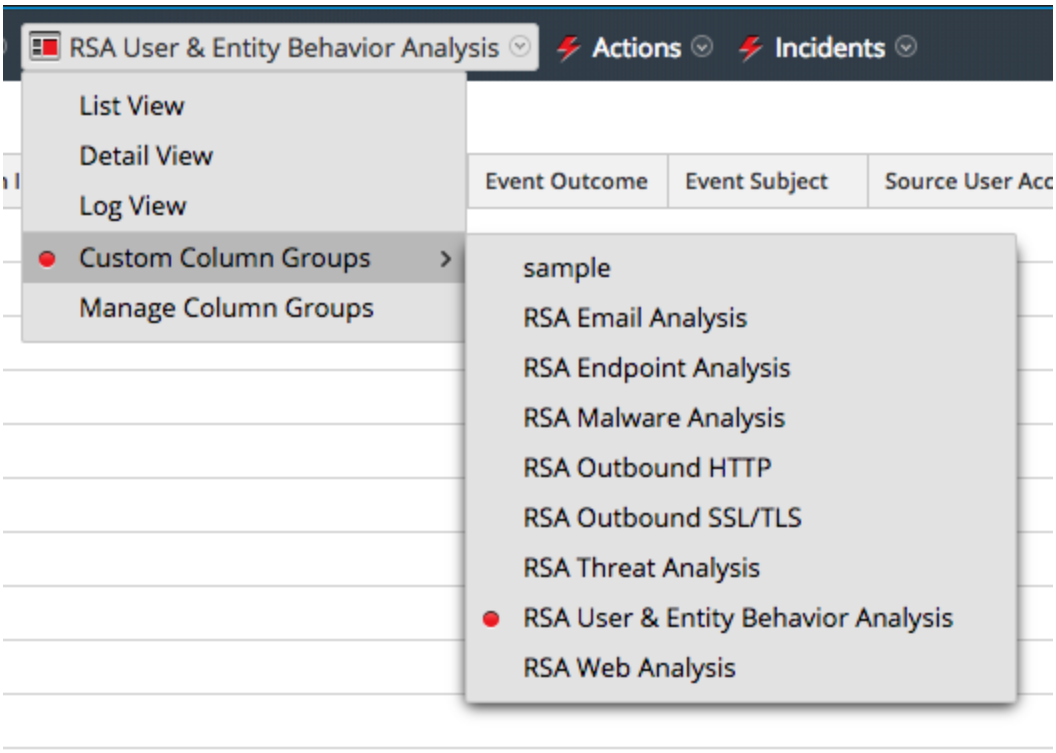


8. (Opcional) Para volver a la configuración anterior del grupo de columnas y deshacer todos los cambios, haga clic en **Restablecer**.
9. Cuando esté listo para guardar, realice una de las siguientes acciones:
   a. Para guardar el grupo de columnas editado y actualizar la vista Eventos con los ajustes del grupo de columnas, haga clic en **Guardar y aplicar**.
   b. Para guardar el grupo de columnas editado sin actualizar la vista Eventos, haga clic en **Guardar**.

Seleccionar un grupo de columnas

Para seleccionar un grupo de columnas:

1. Con la vista Eventos abierta, seleccione **Grupos de columnas personalizados** en el menú desplegable **Ver**. El nombre de la opción es el valor predeterminado (Vista detallada o el valor actual).



2. Seleccione uno de los grupos de columnas en el submenú.
   La vista Eventos se actualiza para reflejar el grupo de columnas personalizado.

Exportar eventos en la vista Eventos

En la vista Eventos, el menú Acciones tiene una opción para exportar eventos desde el evento que se observa a un archivo.

Nota: Solo puede exportar archivos a los cuales puede acceder o que tiene permiso para ver.

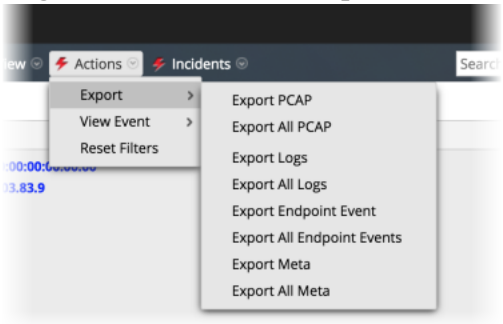
La función de exportación consulta al servicio todas las sesiones dentro del rango de tiempo y el punto de desglose seleccionados para extraer el contenido de cada sesión. El rango de tiempo y el punto de desglose en el momento de la exportación afectan los detalles que se exportan. En el cuadro de diálogo Extracción de archivo, puede optar por exportar:

- PCAP
- Registros
- Evento de NetWitness Endpoint
- Valores de metadatos

El formato del archivo exportado: Archivo ZIP o GZIP. Una vez que se envía la solicitud, se programa un trabajo, el cual se puede rastrear en la bandeja de trabajos. Si hay un error cuando se recupera el registro o la PCAP del servicio, NetWitness Platform muestra una notificación de error.

Para extraer archivos de un evento:

1. Mientras está en la **vista Eventos**, haga clic en un evento.
2. Haga clic en **Acciones** > **Exportar**.



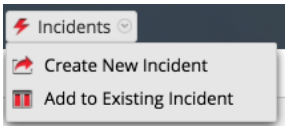
3. Seleccione la opción de exportación y el formato de archivo.
   Un mensaje le informa que los datos seleccionados se están descargando.

Agregar eventos a un incidente para Response

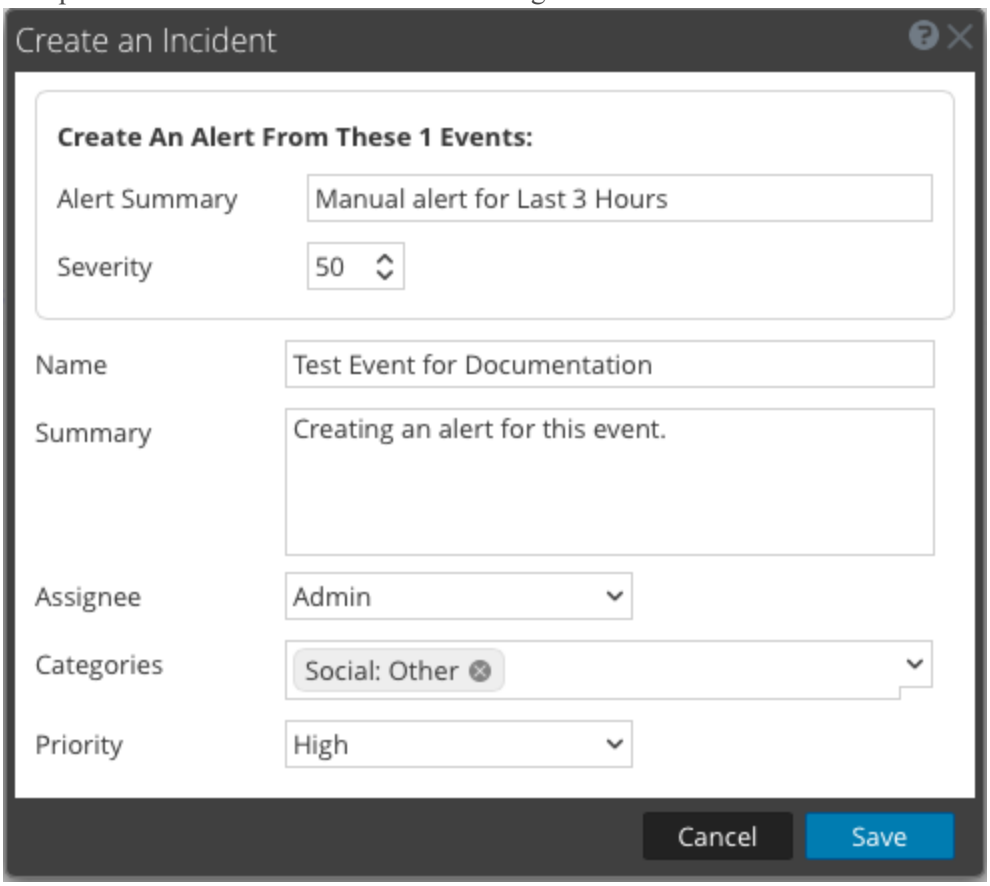
Cuando realiza una investigación en la Vista Eventos, puede seleccionar uno o más eventos y crear un incidente que está disponible para los encargados de respuesta ante incidentes en Respond. También puede agregar eventos a un incidente existente en Respond al cual tiene acceso.

Nota: Un administrador debe configurar las funciones y los permisos requeridos como se describe en "Permisos de función" y "Administrar usuarios con funciones y permisos" en la *Guía de administración de usuarios y seguridad del sistema.*

1. Vaya a **INVESTIGAR** > **Eventos**.
2. En la vista Eventos, seleccione uno o más eventos y, a continuación, **Incidentes** > **Crear nuevo incidente**.



3. Complete la información del cuadro de diálogo Crear un incidente.



   a. Seleccione la gravedad, un entero entre 1 y 100, donde 100 es la gravedad máxima.
   b. Escriba un nombre para el incidente y describa el incidente en el campo **Resumen**.

c. Seleccione un usuario asignado para el incidente en la lista desplegable. Esta lista incluye las funciones incorporadas que tienen acceso a Respond, además de las funciones personalizadas que se han agregado al sistema. Por ejemplo, esta lista podría incluir funciones para el administrador, el analista, el DPO y el operador, y funciones para los encargados de respuesta ante incidentes.

d. En la lista desplegable **Categorías**, seleccione una o más categorías de alertas que se aplican a este incidente.

e. En la lista desplegable **Prioridades**, seleccione una categoría para el incidente. Por ejemplo, un incidente puede tener una prioridad crítica, alta, media o baja.

f. Haga clic en **Guardar**.
El incidente nuevo se crea y está disponible de inmediato en las líneas de espera de incidentes para la función seleccionada en Respond.

4. Para agregar uno o más eventos a un incidente, seleccione uno o más eventos y, a continuación, **Incidentes > Agregar a incidente existente**.

5. En el cuadro de diálogo Agregar eventos a un incidente, seleccione la gravedad y elija uno o más incidentes a los cuales se agregarán los eventos. Puede buscar un incidente existente por ID del incidente o Nombre del incidente. Cuando esté listo, haga clic en **Agregar a incidente**.
Los eventos se agregan a los incidentes seleccionados y se actualizan en Respond.

Combinar eventos desde sesiones divididas

Los analistas pueden identificar sesiones que se dividieron debido a su tamaño en la vista Eventos, y combinar las sesiones fragmentadas de modo que se pueda ver la sesión completa como un único resultado de consulta en la vista Eventos. Cuando las sesiones divididas se vuelven a combinar, una única exportación de paquete de la sesión en la vista Eventos incluye todos los fragmentos de la sesión.

La versión 10.4 y los Decoders anteriores están configurados con un tamaño de sesión predeterminado de 32 MB. Cuando una sesión supera el límite de 32 MB, el Decoder la divide y todos los paquetes subsiguientes pasan a ser parte de una nueva sesión, lo cual fragmenta la sesión de red real en varias sesiones de Decoder. Las sesiones divididas se analizan sin el contexto de que es un fragmento de la sesión de red más grande, lo cual a veces da como resultado fragmentos de sesiones con direcciones y puertos de origen y destino invertidos y con protocolos de aplicación no identificados. Otro resultado de las sesiones divididas puede ser la dificultad de ver todos los fragmentos de una sesión como un único resultado de consulta o de crear la exportación de un paquete de todos los fragmentos de la sesión.

Las mejoras de Decoder en NetWitness Platform 10.5 brindan un procesamiento mejorado de las sesiones fragmentadas:

- Análisis contextual de fragmentos.
- Resaltado de fragmentos de sesión.
- Búsqueda de fragmentos de sesiones.
- Exportación de todos los paquetes a una única PCAP.

Análisis contextual de fragmentos

El Decoder completa el análisis de sesiones antes de dividir la sesión según el tamaño máximo de sesión configurado (32 MB) o el tiempo de espera configurado (60 segundos). Cuando se completa el análisis, los resultados analizados incluyen la direccionalidad de las direcciones y el protocolo de aplicación correctos, los cuales se propagan a cada fragmento de sesión subsiguiente para garantizar la coherencia con la sesión de red lógica que representan.

Nota: Todos los cambios en la configuración de Decoder necesarios se realizan cuando se actualiza a 10.5. Sin embargo, Buscar fragmentos de sesión requiere que las claves de metadatos de los puertos de origen tcp y udp (tcp.srcport y udp.srcport) estén totalmente indexadas, lo cual no era la configuración predeterminada antes de 10.5. Esto limita funcionalmente la capacidad de buscar fragmentos de sesión en sesiones capturadas después de la actualización de Decoder a 10.5.

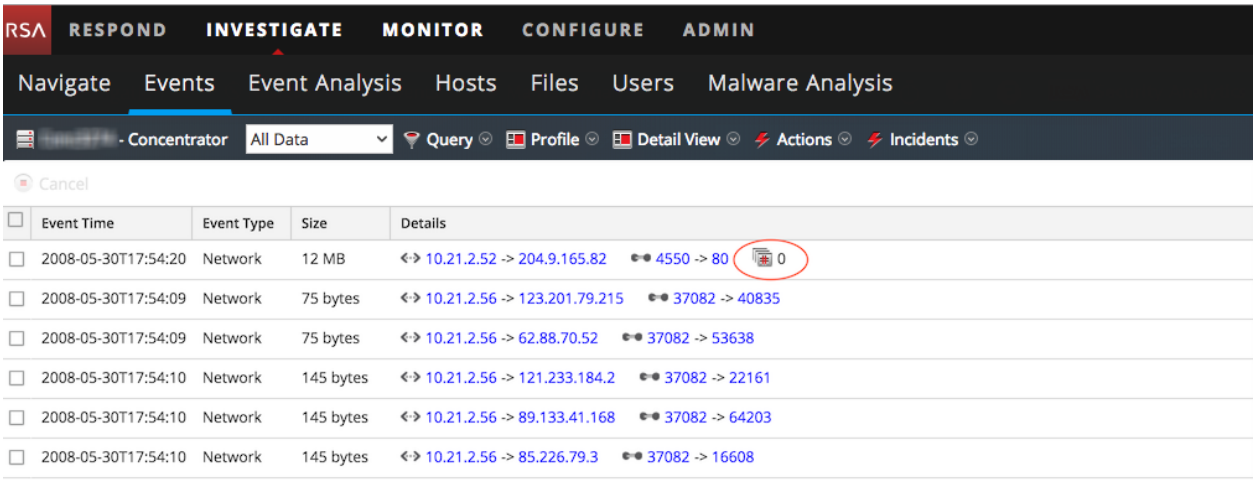
Resaltado de fragmentos de sesión

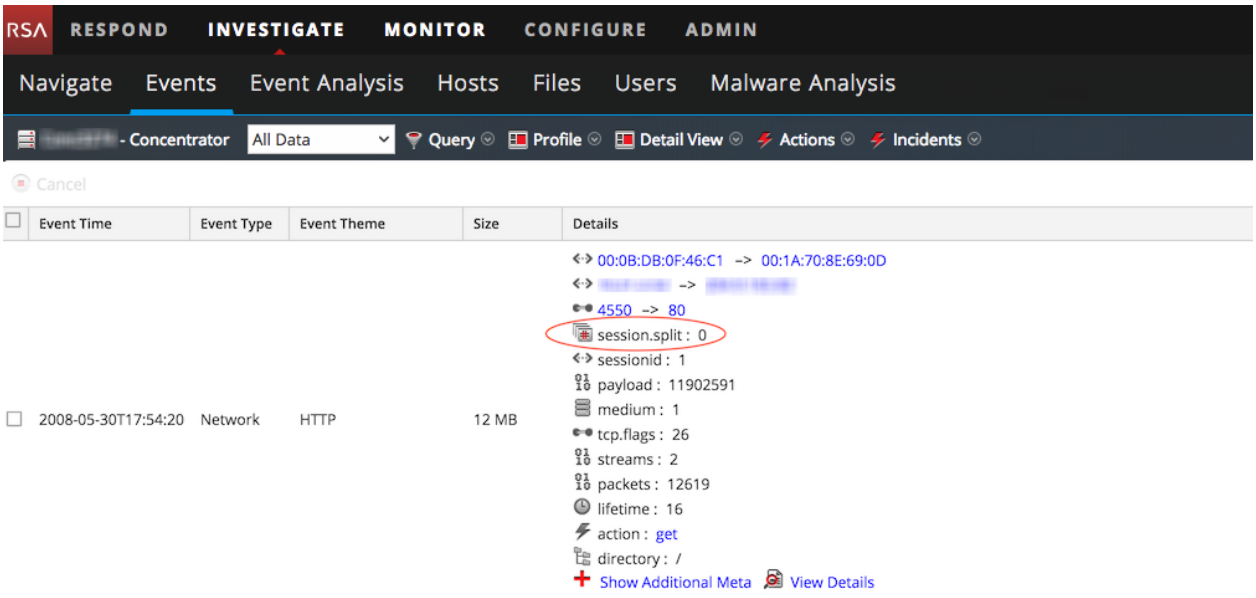
Cada fragmento de sesión tiene metadatos adicionales, `session.split`. El valor de los metadatos `session.split` para un fragmento de sesión específico indica cuántos fragmentos preceden a ese fragmento. Cuando se ven sesiones en la vista Eventos, el elemento de metadatos `session.split` identifica claramente las sesiones que son fragmentos en la vista Lista de eventos y en la vista Detalles de eventos.

La división de la sesión se produce cuando se alcanzan los valores de `assembler.size.max` o `assembler.timeout.session` (latencia entre sesiones) configurados del Decoder. El primer fragmento es la sesión 0 y las sesiones con un registro de fecha y hora posterior se numeran incrementalmente 1, 2, 3, etc. Los metadatos `session.split` indican la cantidad de fragmentos de sesión precedentes; sin embargo, no siempre indican que hay fragmentos de sesión subsiguientes, incluso con un valor de 0. También es posible que el primer fragmento de la sesión no tenga el elemento de metadatos `session.split` si la sesión se analiza antes de que se supere su tamaño máximo.

Después de ver los fragmentos de la sesión, puede determinar el tamaño máximo o el tiempo de espera agotado de la sesión necesarios para el análisis con el fin de volver combinar las sesiones divididas en una sola. Por ejemplo, si tiene cuatro fragmentos de 32 MB, debe configurar el Decoder de prueba (generalmente una máquina virtual configurada por separado del servicio de producción principal) con un tamaño máximo de sesión mayor que 128 MB. Los pasos son los mismos para todos los fragmentos en función de un tiempo de espera agotado de sesión. En las siguientes figuras se muestra la vista Lista de eventos y la vista Detalles de eventos con la información de sesión fragmentada resaltada.

Nota: cuando se crearon las siguientes capturas de pantalla, estaba configurado un tamaño máximo de sesión de 12 MB.





Los metadatos `session.split` se muestran siempre inmediatamente después de los metadatos de dirección y puerto en la vista de detalles. Nunca se ocultan como metadatos adicionales. Estas mejoras permiten hacer lo siguiente de manera rápida:

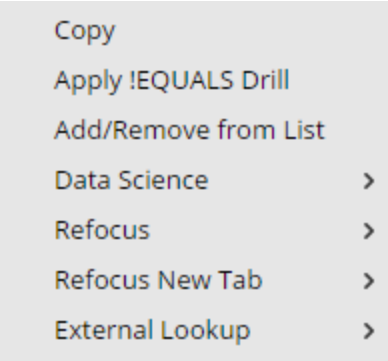
- Identificar sesiones que son fragmentos de sesiones de red.
- Ver todos los fragmentos de una sesión de red o un único fragmento de sesión.
- Exportar los paquetes de la sesión de red completa como un único archivo PCAP.

Buscar y combinar fragmentos

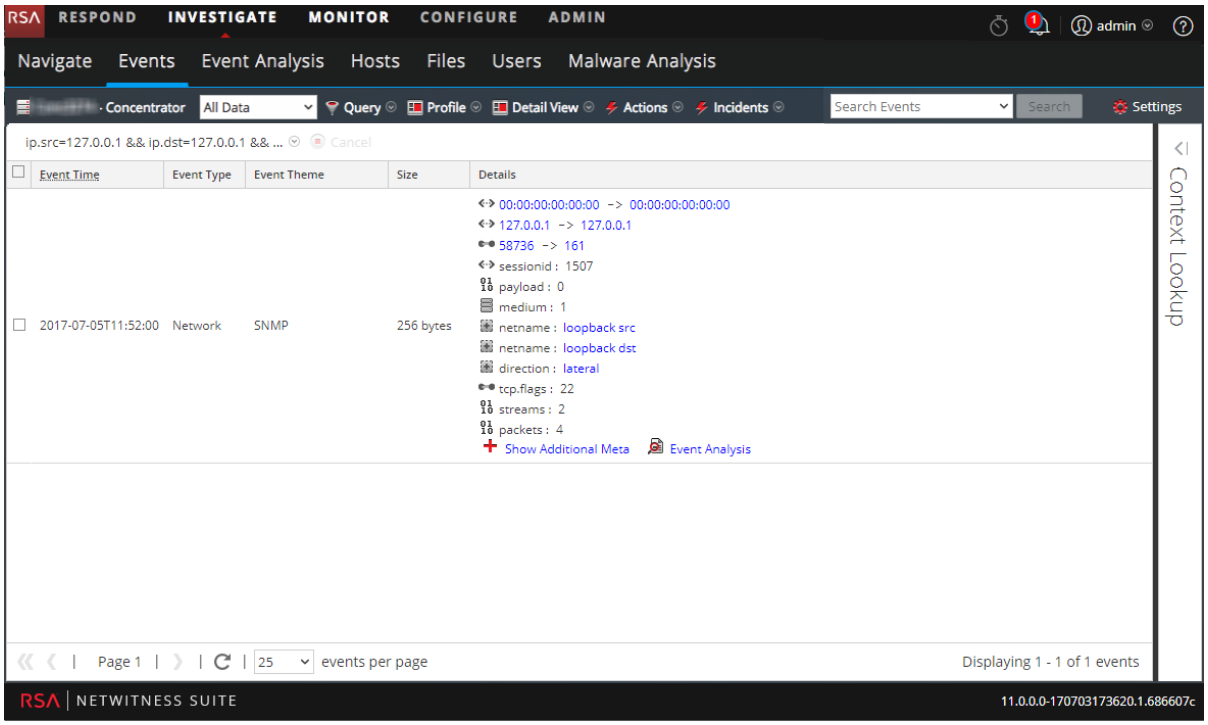
Dentro de la vista Eventos, puede buscar fragmentos de una sesión mediante la opción del menú contextual Reenfocar > Buscar fragmentos de sesión. NetWitness Platform crea una consulta con el uso de las direcciones y los puertos de origen y destino de la sesión seleccionada y muestra todas las sesiones que coinciden con esa consulta en la ventana de tiempo actual.

Para buscar fragmentos de sesión:

1. En la vista **Eventos**, haga clic con el botón secundario en cualquiera de los valores de dirección y puerto de origen y destino: `ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport` y `udp.dstport`), así como en los valores `session.split`.
   Se muestra el menú contextual.



2. Seleccione **Reenfocar > Buscar fragmentos de sesión** o **Reenfocar pestaña nueva > Buscar fragmentos de sesión**.
   NetWitness Platform vuelve a completar la Lista de eventos con fragmentos de sesión para una única sesión dentro del rango de tiempo actual. Según la opción que seleccionó, el reenfoque reemplaza a la vista actual o se abre en una pestaña nueva. (En estos ejemplos se usan todos los datos, pero esto no se recomienda en los sistemas de producción).



3. Si es necesario, ajuste el rango de tiempo para incluir los fragmentos de sesión que pueden preceder o seguir a la ventana de tiempo actual. Puede determinar que es necesario ampliar el rango de tiempo si los fragmentos ocurren cerca del límite de tiempo, en especial si el primer fragmento visible no tiene un valor de división de 0 (o ninguno). Como alternativa, la inspección de los paquetes de la última sesión visible puede hacerlo pensar que la sesión continúa. El siguiente es un ejemplo:

   a. Si observa fragmentos que obviamente no corresponden al primero, por ejemplo, 1, 2, 3 y 4 en el rango de tiempo entre las 10:30 y las 10:35 h, debe haber un fragmento 0. Puede aumentar el rango de tiempo de modo que comience más temprano (en este ejemplo, 10:25 h) con el fin de buscar el fragmento adicional.

   b. Si el tamaño de la sesión del último fragmento se acerca al tamaño máximo (12 MB en este ejemplo), busque fragmentos adicionales mediante el aumento de la ventana de tiempo para incluir una hora posterior (en este ejemplo, 10:40 h).
   Cuando todos los fragmentos de una sesión de red se incluyen en una única lista Eventos, la lista puede abarcar varias páginas.

4. (Opcional) Para exportar los paquetes de cada fragmento de la sesión a un único archivo PCAP, seleccione **Acciones > Exportar todas las PCAP**.
   Un mensaje le informa que el PCAP se está descargando. Cuando se completa la descarga, el archivo PCAP incluye la sesión de red completa que se fragmentó.

Consulta y realización de acciones en datos en las vistas Navegar y Eventos

En este tema se describen métodos para consultar datos y actuar sobre los resultados que son comunes para las vistas Navegar y Eventos. Los analistas pueden:

- Buscar patrones de texto
- Crear una consulta personalizada
- Ver y modificar consultas mediante la integración de URL
- Usar perfiles para encapsular vistas personalizadas
- Administrar listas y valores de lista de Context Hub en las vistas Navegar y Eventos
- Buscar contexto adicional en las vistas Navegar y Eventos
- Reconstruir un evento

Crear una consulta personalizada

En Investigar > vista Navegar o vista Eventos, puede crear una consulta en lugar de hacer clic en las claves y los valores de metadatos para desglosar a los metadatos. Los cuadros de diálogo para la creación de una consulta ofrecen ayuda de sintaxis con listas desplegables de las claves y los operadores de metadatos aplicables. Cuando observa la lista desplegable, puede expandir y contraer cada grupo de metadatos para ver u ocultar las claves de metadatos individuales en ese grupo.

Nota: En la versión 11.1 y superior, puede consultar las entidades de metadatos y también las claves de metadatos.

Cuando selecciona un grupo de metadatos, NetWitness Platform genera la consulta compleja igual a una consulta con todas las claves de metadatos en ese grupo reunidas mediante OR. Entonces, si un grupo de metadatos contiene `ip.src` e `ip.dst`, la consulta generada es `ip.src = <value> OR ip.dst = <value>`. Si el grupo de metadatos contiene claves de metadatos que tienen diferentes tipos de valores de metadatos, el valor de entrada se deshabilita y la consulta utiliza declaraciones `exists`. Por ejemplo, un grupo de metadatos que contiene `ip.src`, `ip.dst` y `alias.host` incluye claves de metadatos que tienen diferentes tipos de valores; `ip.src` e `ip.dst` son las direcciones IP y `alias.host` es el texto. La consulta generada es `ip.src exists OR ip.dst exists OR alias.host exists`.

Una consulta básica tiene el siguiente formato:

```
<metakey> <operator> [<metavalue>]
```

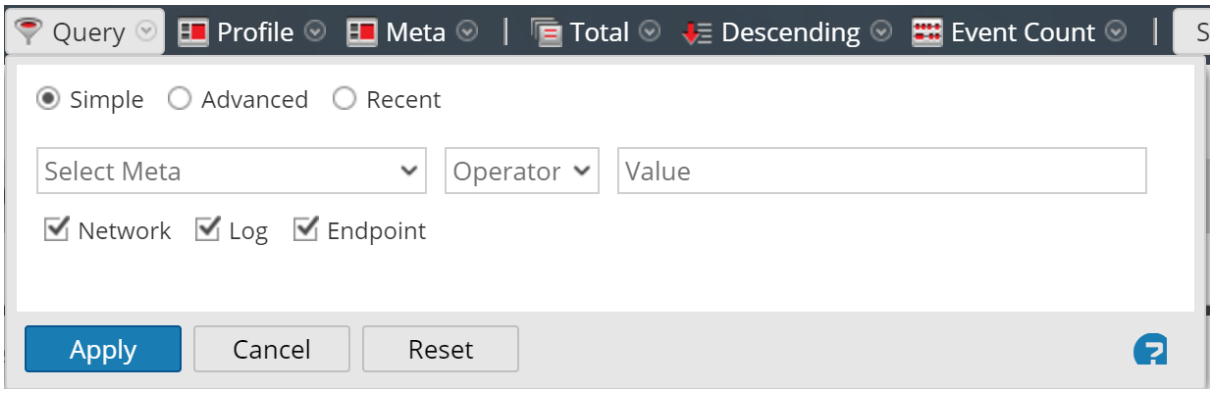
Estos son algunos ejemplos:

```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Crear una consulta con el método básico

Cuando crea una consulta con el método básico, NetWitness Platform proporciona listas desplegables de metadatos y operadores.

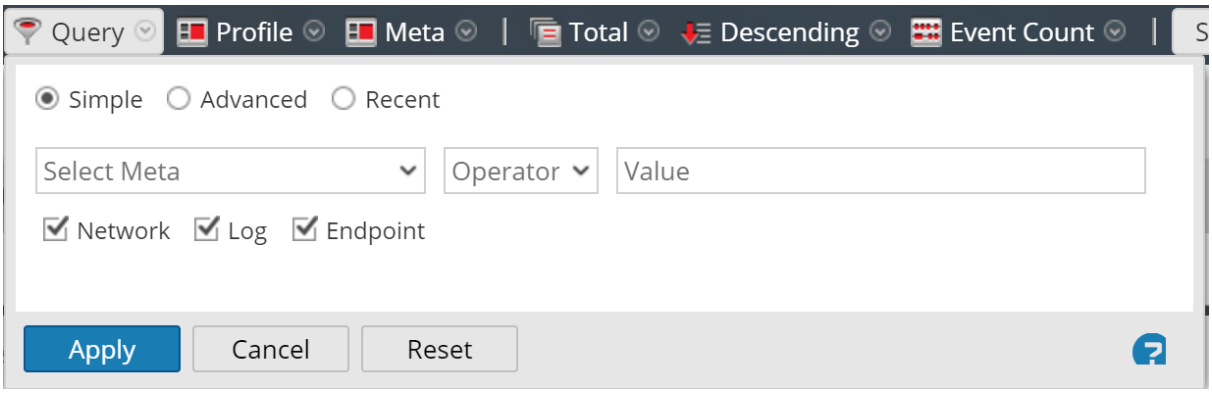
1. En la barra de herramientas de la **vista Navegar** o de la **vista Eventos**, seleccione **Consulta.**
   El cuadro de diálogo Consulta se muestra con la opción Simple seleccionada.



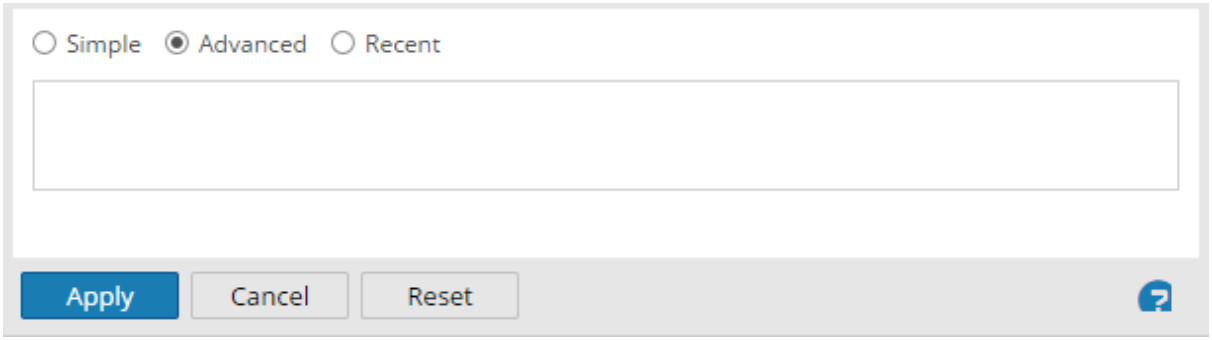
2. En el campo **Seleccionar metadatos**, haga clic para mostrar la lista desplegable. La lista desplegable tiene dos secciones: Grupos de metadatos y Todos los metadatos.
3. Seleccione una única clave de metadatos bajo **Todos los metadatos** o seleccione un grupo de metadatos bajo **Grupos de metadatos**. También puede ingresar en el campo una clave de metadatos o un grupo de metadatos.
4. En el campo **Operador**, escriba un operador o haga clic en la lista desplegable para seleccionar un operador válido.
5. (Opcional) Si ha seleccionado un operador que requiere un valor, por ejemplo, comienza, en el tercer campo escriba el valor de la clave de metadatos.
6. En las casillas de verificación Red, Registro y Terminal, seleccione el tipo de datos para consultar. Realice una de las siguientes acciones:
   a. Para limitar la consulta a paquetes, seleccione **Red** y deseleccione **Registro** y **Terminal**.
   b. Para limitar la consulta a registros, seleccione **Registro** y deseleccione **Red** y **Terminal**.
   c. Para limitar la consulta a eventos de terminal, seleccione **Terminal** y deseleccione **Red** y **Registro**.
   d. Para aplicar la consulta a paquetes, registros y terminales, seleccione **Red**, **Registro** y **Terminal**.
7. Realice una de las siguientes acciones:
   a. Haga clic en **Aplicar**.
      La ventana se cierra y la vista se actualiza con los resultados de la nueva consulta. La consulta se muestra en la ruta de navegación.
   b. Haga clic en **Cancelar**.
      La ventana se cierra y no se realizan cambios en la vista ni en la consulta actual.

Crear una consulta con el método avanzado

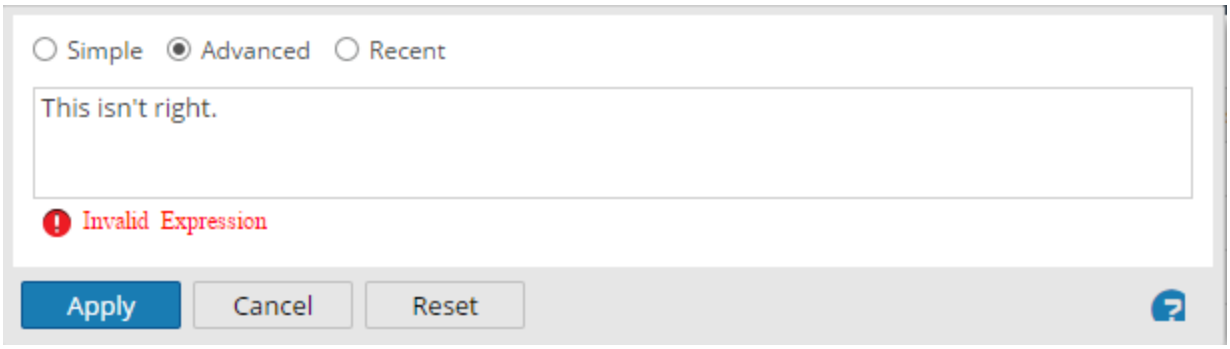
1. En la barra de herramientas de la **vista Navegar** o de la vista Eventos, seleccione **Consulta.**
   Se muestra el cuadro de diálogo Consulta.



2. Seleccione **Avanzada**.
   Se muestra el campo de consulta avanzada.



3. En el campo, cree una consulta que pueda incluir la clave de metadatos, el operador y un valor. Cuando comienza a escribir una clave de metadatos en el campo, se muestra una lista desplegable de las claves de metadatos disponibles para el servicio seleccionado.
4. Seleccione la clave de metadatos para la consulta.
   Se actualiza la pantalla. Si la expresión no se ha completado, el estado indica que la consulta no es válida.
5. Continúe con un operador, de la lista desplegable y, a continuación un valor si es necesario. La pantalla se actualiza a medida que sigue ingresando la consulta. Si ingresa un operador, como **exists** o **!exists**, que no utiliza el campo de valor, el campo de valor se desactiva y el estado no válido se borra. Si ingresa un operador, como =, que requiere el campo de valor, el estado no válido permanece hasta que se ingresa un valor. Cuando la consulta es válida, ya no se muestra el estado no válido.

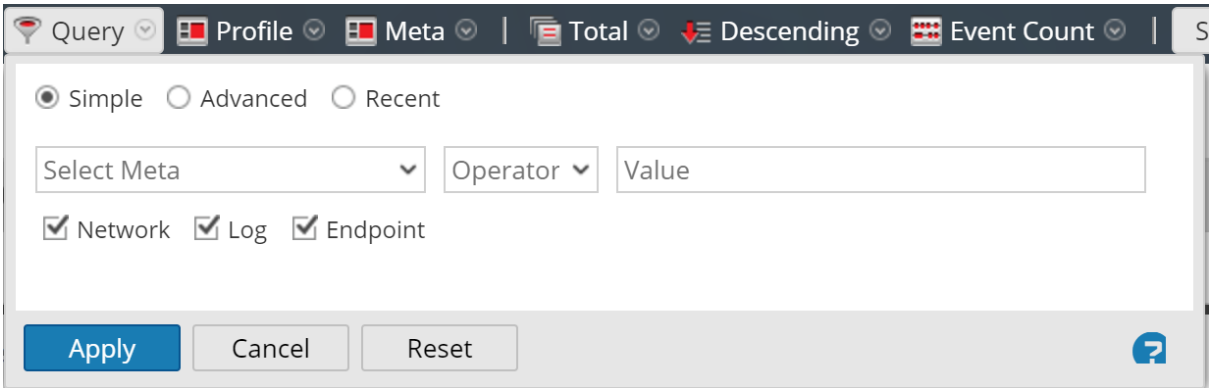


6. Realice una de las siguientes acciones:
   - Haga clic en **Aplicar**.
     La ventana se cierra y la vista se actualiza con los resultados de la nueva consulta. La consulta se muestra en la ruta de navegación.
   - Haga clic en **Cancelar**.
     La ventana se cierra y no se realizan cambios en la vista ni en la consulta actual.

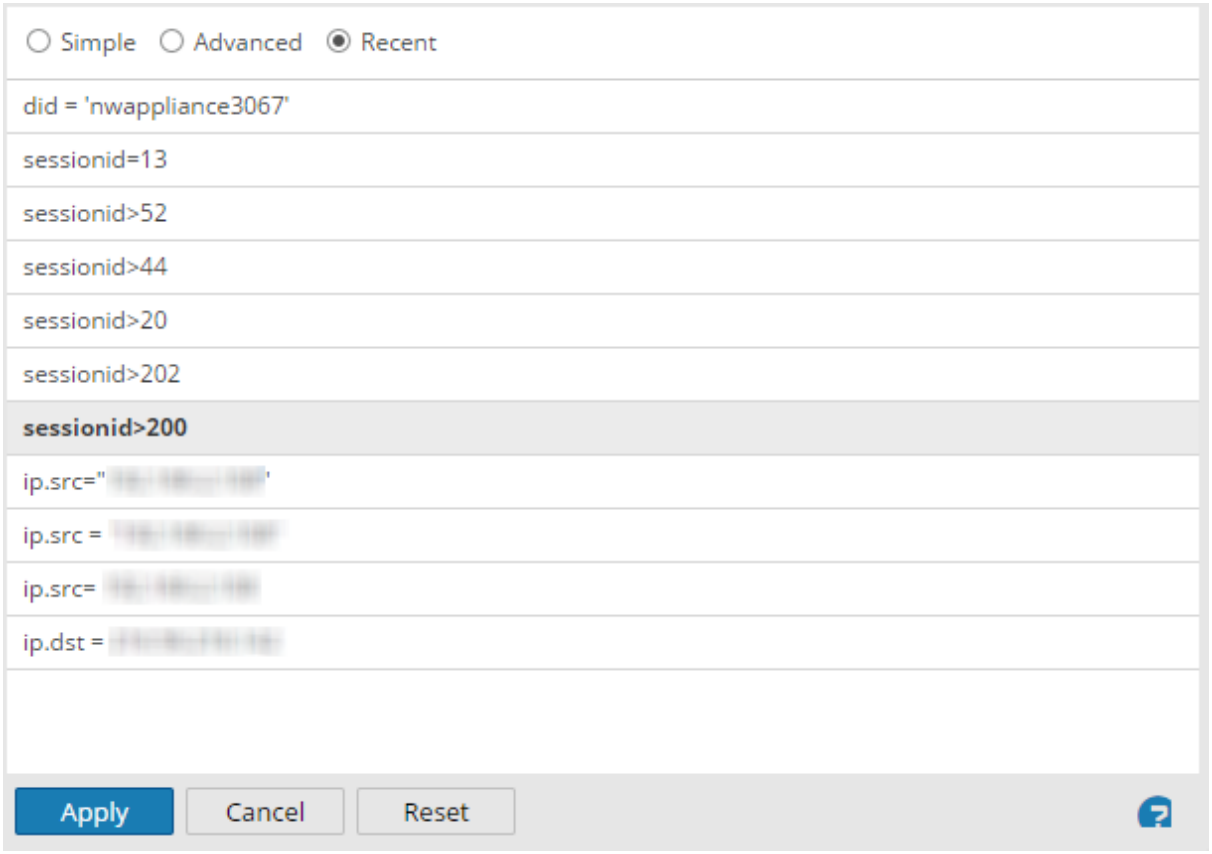
Aplicar una consulta reciente

Puede ver consultas recientes y seleccionar una para aplicar al servicio actual que se investiga. Para seleccionar una consulta reciente:

1. En la barra de herramientas de la **vista Navegar** o de la vista Eventos, seleccione **Consulta.**
   El cuadro de diálogo Consulta se muestra con la opción Simple seleccionada.



2. Seleccione la opción **Reciente**.
   La lista de consultas recientes se muestra en la parte inferior del cuadro de diálogo.



3. En la lista de consultas recientes, haga clic para seleccionar una consulta.
4. Realice una de las siguientes acciones:
   - Haga doble clic en una consulta.
   - Seleccione una consulta y haga clic en **Aplicar**.
     La ventana se cierra y la vista se actualiza con los resultados de la nueva consulta. La consulta se muestra en la ruta de navegación.
   - Haga clic en **Cancelar**.
     La ventana se cierra y no se realizan cambios en la vista ni en la consulta actual.

Administrar listas y valores de lista de Context Hub en las vistas Navegar y Eventos

Los analistas pueden agregar listas y valores de lista para el enriquecimiento de Context Hub en las vistas Navegar y Eventos. (En la versión 11.2 y superior, los analistas pueden agregar listas y valores de lista en la vista Análisis de eventos, como se describe en Buscar contexto adicional en la vista Análisis de eventos).

Cuando el servicio Context Hub está habilitado y configurado, NetWitness Platform proporciona datos de enriquecimiento de Incident Management, listas personalizadas y NetWitness Endpoint directamente en las vistas Navegar y Eventos. Una indicación visual destaca los valores de metadatos para los cuales están disponibles datos de enriquecimiento en las vistas de Investigate, y puede hacer clic en el valor destacado para buscar información contextual e inteligencia.

Además, desde el panel Valores en las vistas Navegar y Eventos, puede ver listas, editar valores de metadatos de una lista existente o crear una lista nueva. Cuando agrega valores de metadatos a una lista, puede investigar los valores de metadatos con la opción de búsqueda de contexto.

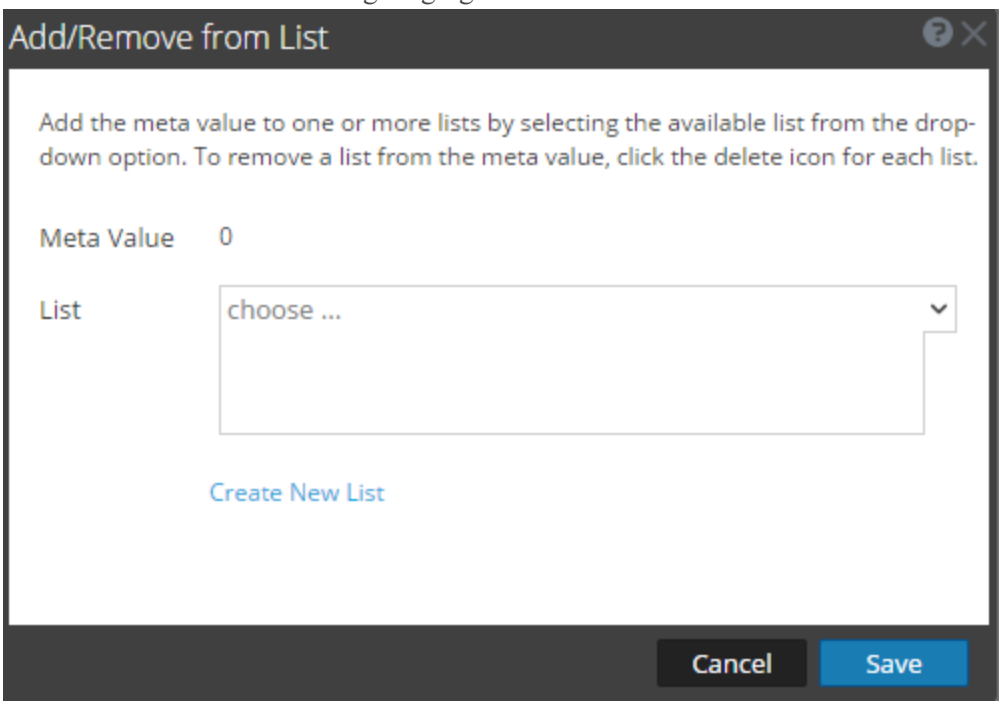
Para que un analista administre listas en Investigate, el administrador debe:

- Habilitar el servicio Context Hub.
- Asignar una función de analista con permiso `Manage List from Investigation` al usuario que llevará a cabo la búsqueda de contexto en las vistas de Investigation.
- Configurar funciones y permisos adecuados, como se describe en "Permisos de función" y "Administrar usuarios con funciones y permisos" en la *Guía de administración de usuarios y seguridad del sistema*.

Agregar valores de metadatos a una lista existente

Para agregar un valor de metadatos a una lista existente en Context Hub:

1. Mientras investiga un servicio en las vistas **Navegar** o **Eventos**, haga clic con el botón secundario en un valor de metadatos (por ejemplo, los valores bajo Dirección IP de origen, Dirección IP de destino o Nombre de usuario) y seleccione **Agregar/eliminar de la lista** en el menú contextual.
   Se muestra el cuadro de diálogo Agregar/eliminar de la lista.



2. En el campo **Lista**, seleccione una o más listas de la opción del menú desplegable a las cuales se debe agregar el valor de metadatos.
3. Haga clic en **Guardar**.
   El valor de metadatos se agrega a las listas seleccionadas.

Quitar un valor de metadatos de una lista de Context Hub

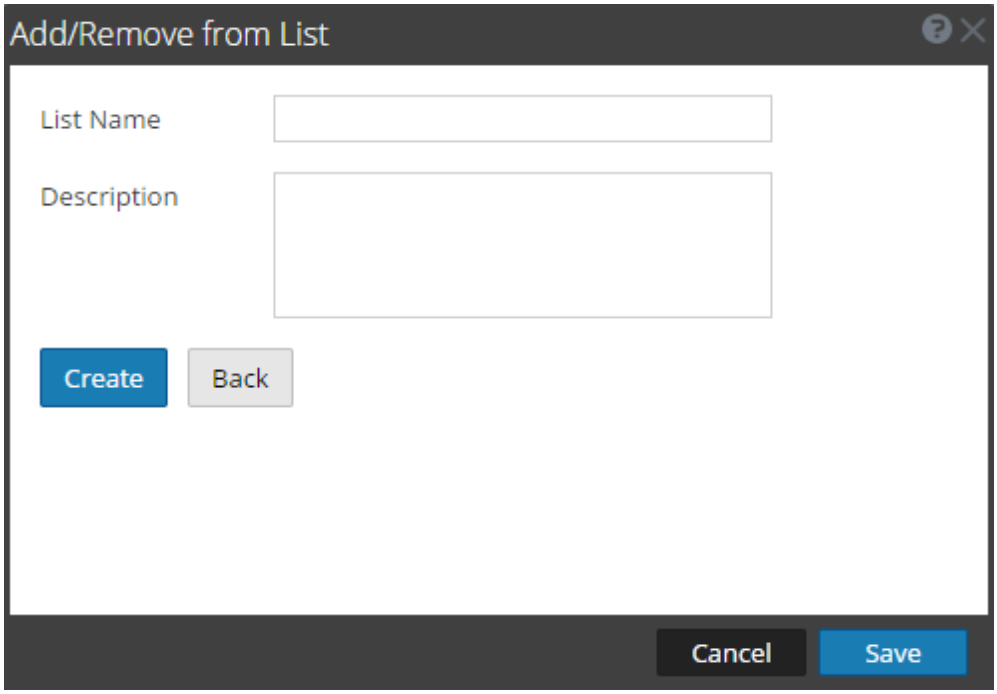
Para quitar un valor de metadatos de la lista:

1. En el cuadro de diálogo **Agregar/eliminar de la lista**, en el campo **Lista**, vea las listas que incluyen el valor de metadatos.
2. Haga clic en el icono Eliminar (x) de cada lista que no debe incluir el valor de metadatos.
3. Haga clic en **Guardar**.
   El valor de metadatos se elimina de la lista eliminada.

Crear una lista nueva

Para crear una lista de Context Hub en Investigate:

1. En el cuadro de diálogo **Agregar/eliminar de la lista**, haga clic en **Crear lista nueva**.



2. En el campo **Nombre de lista**, ingrese un nombre único para la lista.
3. En el campo **Descripción**, ingrese una descripción de la lista.
4. Haga clic en **Crear** para crear la lista.
5. Haga clic en **Guardar** para agregar el valor de metadatos a la lista creada.
   Estas listas se consideran orígenes de datos para la recuperación de información de contexto.

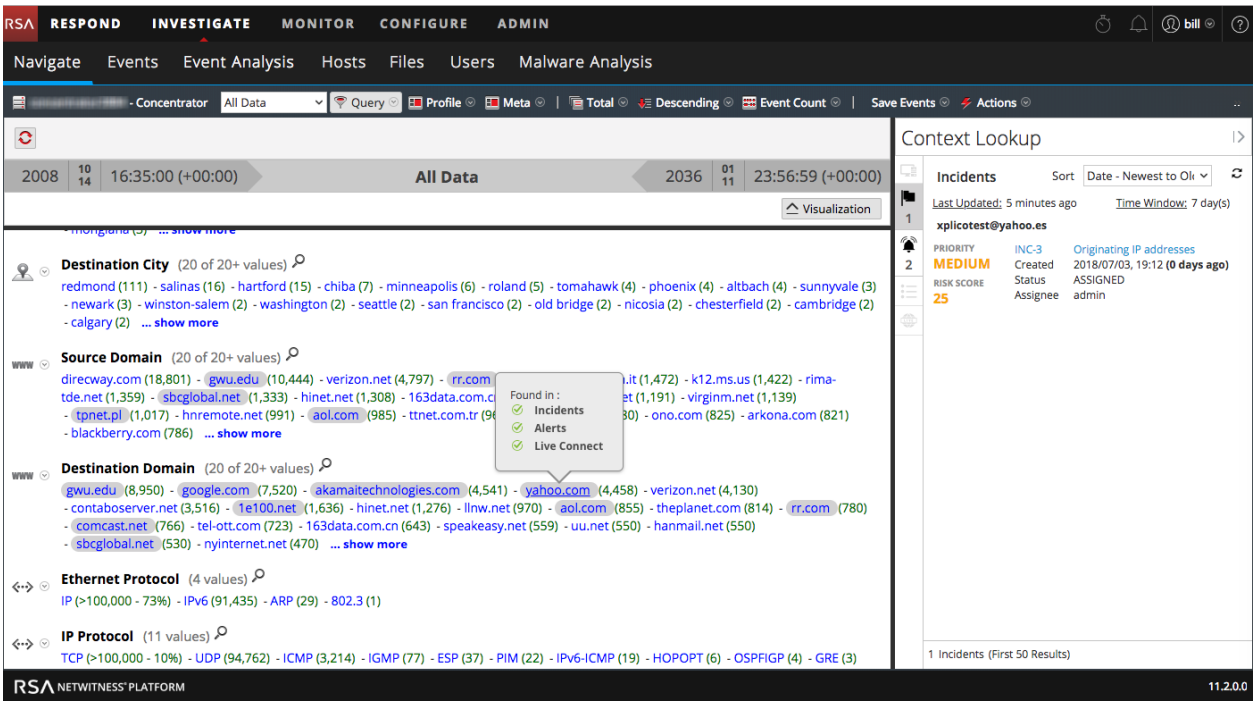
Buscar contexto adicional en las vistas Navegar y Eventos

En las vistas Eventos y Navegar, puede buscar detalles e inteligencia acerca de los elementos asociados a un evento en Context Hub. (En la versión 11.2 y superior, también puede buscar contexto adicional en la vista Análisis de eventos, como se describe en Buscar contexto adicional en la vista Análisis de eventos). Estos elementos, o entidades, son identificadores; por ejemplo, una dirección IP, un nombre de usuario, un nombre de host, un nombre de dominio, un nombre de archivo o un hash de archivo. Los datos de los orígenes configurados, como RSA NetWitness Endpoint, pueden ayudarlo a comprender lo que está sucediendo.

Nota: Para habilitar la visualización de información contextual, el administrador debe agregar el servicio Context Hub en RSA NetWitness Platform y configurar orígenes de datos para este servicio, como se describe en la *Guía de configuración de Context Hub*. Los analistas también necesitan una función que tenga el permiso `Context Lookup`, como se describe en "Permisos de funciones" y en "Administrar usuarios con funciones y permisos" en la *Guía de administración de usuarios y de la seguridad del sistema*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Context Hub es un servicio centralizado que agrega datos acerca de las entidades de varios orígenes de datos configurables. Estos datos pueden ampliar su investigación con contexto adicional más allá de los resultados inmediatos de una consulta específica. Por ejemplo, Context Hub puede indicar si una entidad determinada se ha mencionado en incidentes, alertas, feeds o publicaciones de inteligencia de comunidades.

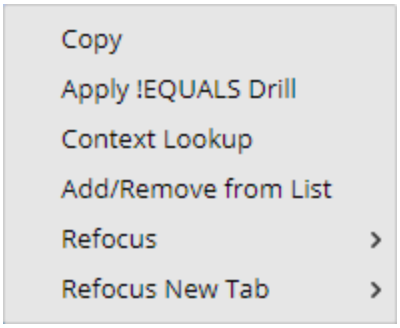
En las vistas Navegar y Eventos, las entidades para las que están disponibles datos de contexto asociados se destacan con un fondo gris; si se coloca el cursor sobre una entidad, se activa un cuadro que proporciona un resumen de los datos disponibles. Cuando se hace clic con el botón secundario en la entidad, Context Hub consulta la información pertinente en los orígenes de datos configurados y el panel Búsqueda de contexto se abre desde el lado derecho de la ventana del navegador. Este panel se completa con la información de Context Hub a medida que queda disponible. Puede realizar otra búsqueda haciendo clic con el botón secundario en otra entidad. El panel Búsqueda de contexto se actualiza con la información de esa entidad.



En el panel Búsqueda de contexto, puede ver y explorar orígenes de datos individuales para realizar una investigación más a fondo. Para obtener una descripción detallada de la información que se muestra para cada origen de datos, consulte Panel Búsqueda de contexto.

Para ver información en el panel Búsqueda de contexto de las vistas Navegar o Eventos:

1. Coloque el cursor sobre distintos valores de metadatos para ver los orígenes de datos en los que hay datos disponibles.
   Un cuadro activado con el puntero muestra una lista de los orígenes de datos que tienen datos de contexto disponibles para el valor de metadatos. Los siguientes son los posibles orígenes de datos: NetWitness Endpoint, Incidentes, Alertas, Hosts, Archivos, Feeds y Live Connect.
2. Haga clic con el botón secundario en un valor de metadatos y haga clic en **Búsqueda de contexto** en el menú desplegable para abrir el panel Búsqueda de contexto.



   El panel Búsqueda de contexto se abre desde el lado derecho de la ventana del navegador. Este panel

se completa con la información de Context Hub a medida que queda disponible.

3. Para realizar acciones desde el panel Búsqueda de contexto, haga clic con el botón secundario en una entidad, como una dirección IP.
   Las siguientes opciones se encuentran disponibles: Abrir el vínculo en una nueva pestaña, Consultar en Investigate, Copiar vínculo, Pegar, Búsqueda de Google, Búsqueda de VirusTotal y Consultar en Endpoint.
4. Para cerrar el panel Búsqueda de contexto, haga clic en ✉ en el panel.

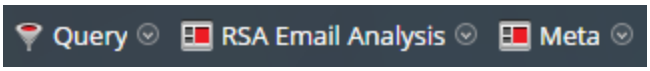
Usar perfiles para encapsular vistas personalizadas

El uso de perfiles es una manera rápida y fácil de personalizar los datos que se muestran en las vistas Navegar y Eventos. En el cuadro de diálogo Administrar perfiles, puede usar un perfil para especificar los grupos de metadatos y los grupos de columnas que se muestran de forma predeterminada, para agregar consultas a una investigación y para importar o exportar perfiles.

Nota: Los perfiles se comparten entre usuarios en la misma red de NetWitness Platform. Si un usuario modifica o elimina un perfil, esto afecta lo que está disponible para los demás usuarios.

Si tiene múltiples perfiles, puede alternar entre ellos para cambiar rápidamente a las preferencias del perfil seleccionado. Si un perfil está activo actualmente, el título del menú Perfil se reemplaza por el nombre del perfil.

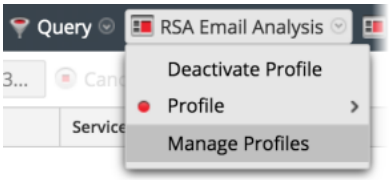
En la siguiente figura, esto se ilustra en la vista Navegar. El nombre del perfil se muestra a la derecha de la opción Consulta. Esto también es así en la vista Eventos.



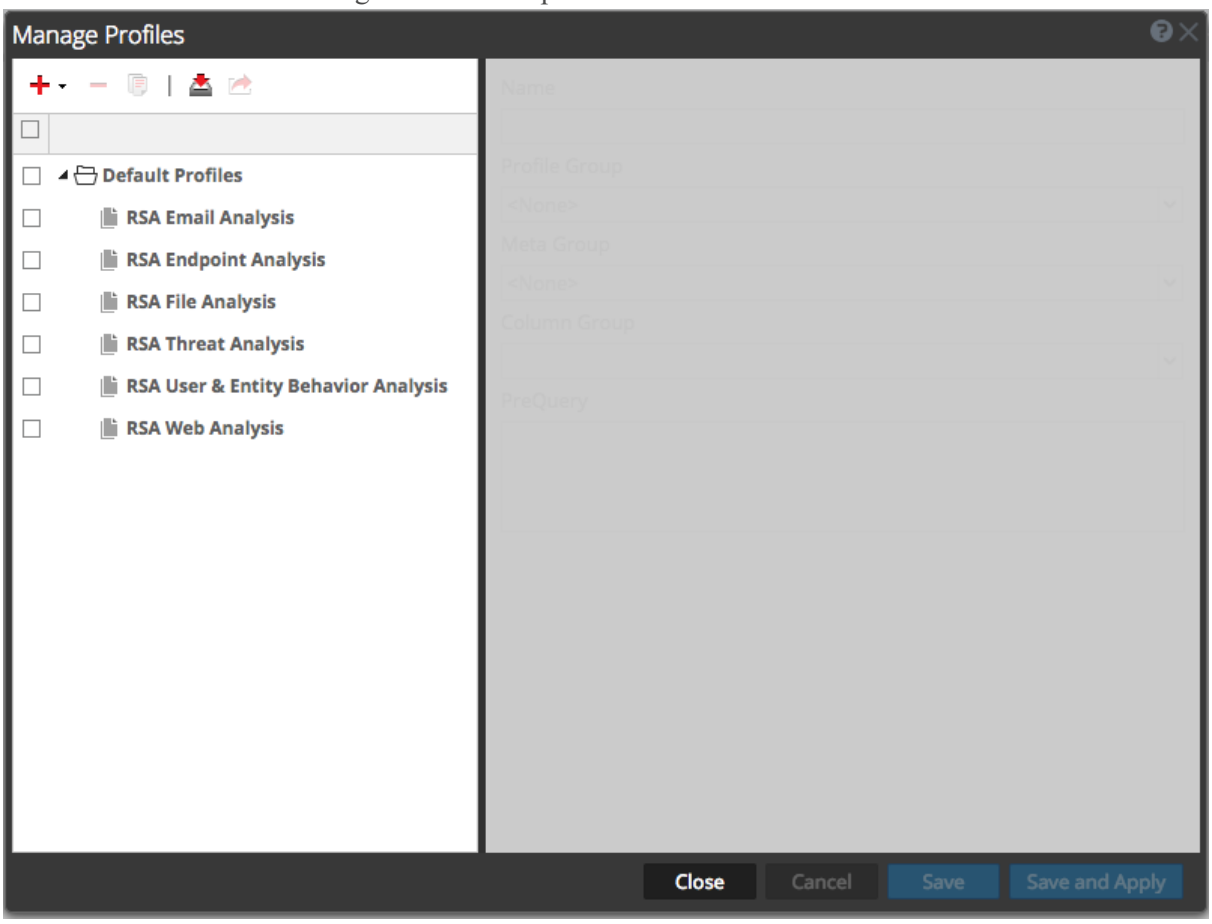
A partir de la versión 11.2, los perfiles se organizan en grupos de perfiles. Los perfiles incorporados se encuentran en el grupo Perfiles predeterminados, el que no se puede editar. Los analistas pueden crear nuevos grupos de perfiles que cualquiera puede usar. Una vez creado, puede editar un grupo de perfiles para agregar perfiles, quitarlos o transferirlos de un grupo a otro. Cuando crea un perfil, este no se agrega a ningún grupo de perfiles de manera predeterminada. Cuando exporta perfiles, la información sobre el grupo de perfiles se guarda y los perfiles se importan al mismo grupo desde el que se exportaron.

Navegar al cuadro de diálogo Administrar perfiles

1. Vaya a INVESTIGAR > **Eventos** o **INVESTIGAR** > **Navegar**. (Si se muestra el cuadro de diálogo **Investigar**, seleccione un servicio y haga clic en **Navegar**).
2. En la barra de herramientas, seleccione **Perfil > Administrar perfiles**.



Se muestra el cuadro de diálogo Administrar perfiles.



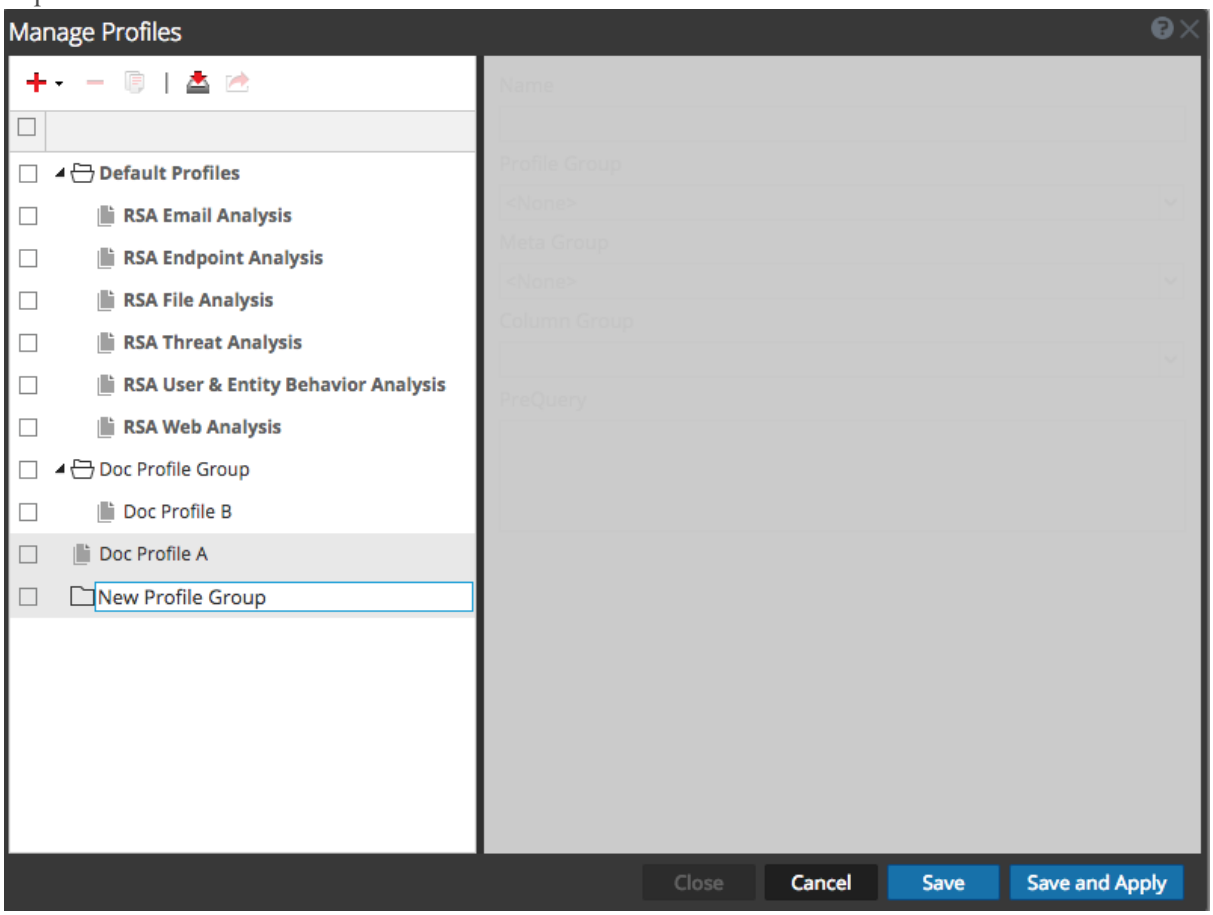
Crear, editar o eliminar un grupo de perfiles (versión 11.2 y superior)

Puede crear un grupo de perfiles personalizado para organizar distintos perfiles. Una vez creado, la única edición que puede realizar directamente en un grupo de perfiles es la edición de su nombre. Para agregar o quitar un perfil de un grupo, edite el perfil y asígnelo a otro grupo de perfiles, como se describe en Crear y editar perfiles.

1. En el cuadro de diálogo **Administrar perfiles**, realice una de las siguientes acciones:
   - Para seleccionar un grupo de perfiles existente con el fin de editarlo, haga doble clic en el grupo de perfiles.
   - Para agregar un nuevo grupo de perfiles, haga clic en + y seleccione **Agregar nuevo grupo de perfiles**.

Nota: Si desea editar uno de los grupos de perfiles incorporados, haga clic en para crear una copia editable.

Se muestra una carpeta con un campo en blanco en la parte inferior de la lista Perfiles de la columna izquierda.



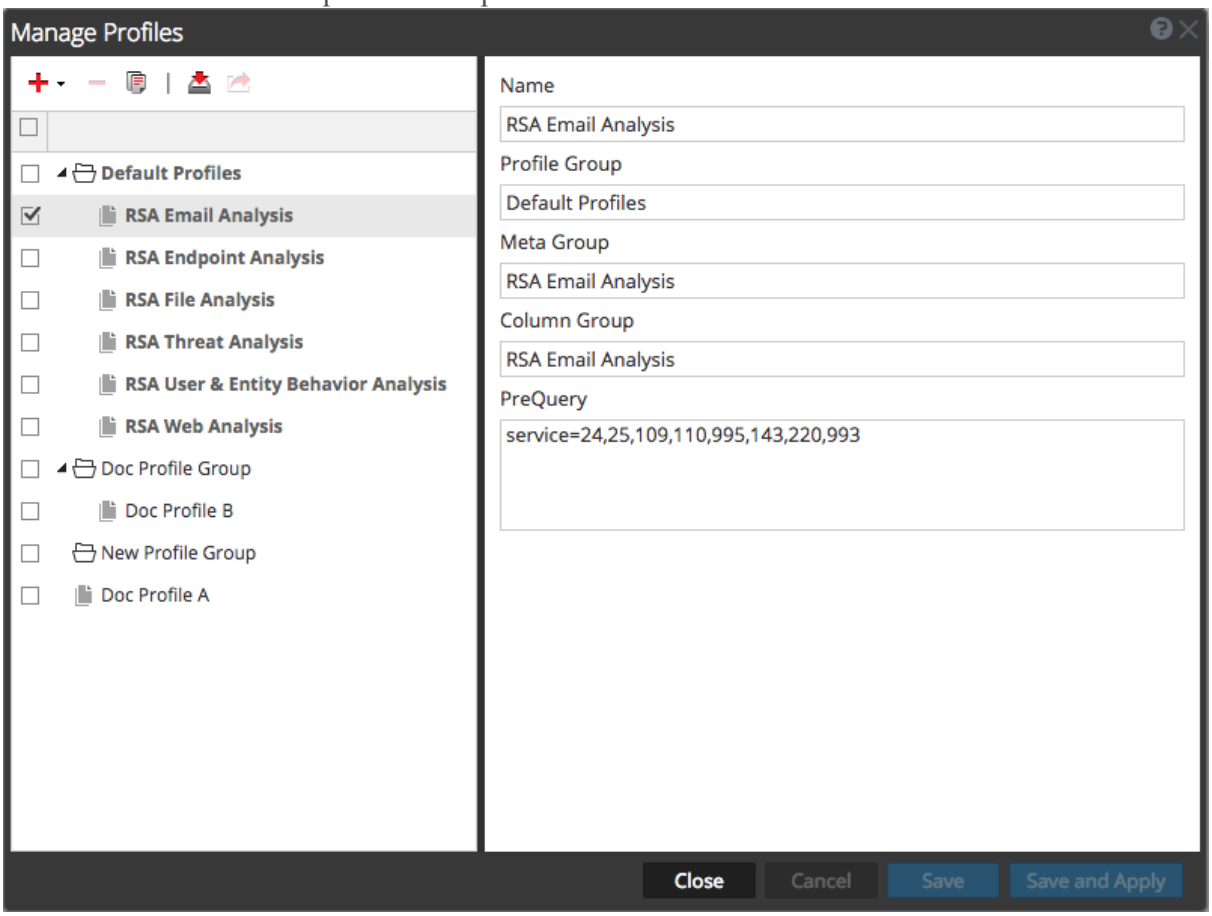
2. Para editar o ingresar el nombre del grupo de perfiles, haga doble clic en el Grupo de perfiles y escriba en el campo de entrada. El nombre debe tener entre 2 y 80 caracteres.
   El nombre del grupo de perfiles se aplica a un nuevo grupo de perfiles o al grupo de perfiles que editó. Ahora, el grupo de perfiles está disponible cuando se configura un perfil.
3. Para eliminar un grupo de perfiles, realice una de las siguientes acciones:
   - Si desea eliminar un grupo de perfiles, pero conservar los perfiles, seleccione la casilla de verificación para elegir el grupo, deseleccione las casillas de verificación de los perfiles del grupo y haga clic en Eliminar.
   - Si desea eliminar un grupo de perfiles y los perfiles que contiene, seleccione la casilla de verificación para elegir el grupo y no deseleccione las casillas de verificación de los perfiles que desea eliminar.
     Un cuadro de diálogo solicita confirmar la intención de eliminar el grupo. Si no deseleccionó la marca en la casilla de verificación junto a los perfiles, el grupo y sus perfiles se eliminan. Si deseleccionó las casillas de verificación de los perfiles, solamente se elimina el grupo de perfiles y los perfiles se quitan del grupo y quedan disponibles para agregarlos a otro grupo de perfiles.

Crear y editar perfiles

1. En el cuadro de diálogo **Administrar perfiles**, realice una de las siguientes acciones:
   - Para seleccionar un perfil existente con el fin de editarlo, seleccione la casilla de verificación junto al nombre.
   - Para agregar un nuevo perfil en la versión 11.2 y superior, haga clic en + o en la flecha hacia abajo junto a + y seleccione **Agregar nuevo perfil**.
   - Para crear un nuevo perfil en versiones anteriores a 11.2, haga clic en +.

   Nota: Si desea editar uno de los perfiles incorporados, haga clic en para crear una copia y edite la copia.

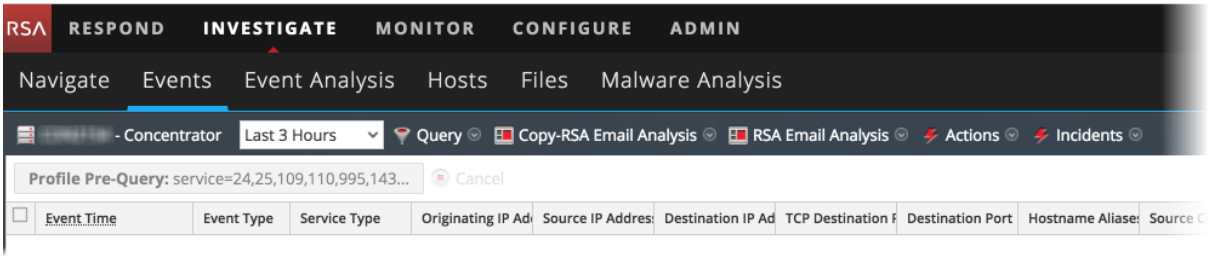
   La definición del perfil está disponible para su edición en el panel derecho. En esta figura se ilustra la definición de uno de los perfiles incorporados.



2. Edite o ingrese el nombre del perfil. Para esto, escríbalo en el campo **Nombre**. El nombre debe tener entre 2 y 80 caracteres.
3. (Opcional para la versión 11.2 y superior) Si desea agregar el perfil a un grupo de perfiles, seleccione un grupo de perfiles en la lista desplegable **Grupo de perfiles**.

Si selecciona un grupo de perfiles, el perfil se agrega al grupo cuando se guardan los cambios. Si no selecciona un grupo de perfiles, el perfil no forma parte de un grupo.

4. Seleccione un grupo de metadatos en la lista desplegable **Grupo de metadatos**. Puede agregar grupos de metadatos personalizados como se describe en Administrar grupos de metadatos.
5. Seleccione un grupo de columnas para la lista desplegable **Grupo de columnas**. Puede agregar grupos de columnas personalizados como se describe en Administrar grupos de columnas en la vista Eventos.
6. Escriba consultas para filtrar los resultados en el campo **Consulta previa**. Consulta previa sigue la misma sintaxis que el generador de consultas. La consulta previa de la figura utiliza un grupo de metadatos llamado **service = 24,25,109,110,995,143,220,993**.
7. Haga clic en **Guardar** para guardar el perfil sin usarlo o haga clic en **Guardar y aplicar** para guardar el perfil y usarlo de inmediato.
   Si hace clic en **Guardar y aplicar**, se muestra un cuadro de diálogo de confirmación antes de que el perfil seleccionado se aplique. Para la versión 11.2 y superior, la consulta previa que ingresó en el cuadro de diálogo Administrar perfiles se muestra en la ruta de navegación.



Eliminar un perfil

1. En el cuadro de diálogo **Administrar perfiles**, elija un perfil seleccionando la casilla de verificación junto al nombre.

   Nota: No puede eliminar ninguno de los perfiles incorporados.

2. Haga clic en .
   Un indicador solicita confirmar la intención de eliminar el perfil y este se elimina. El nombre de la opción en la barra de herramientas vuelve a **Perfil** para mostrar que ningún perfil está vigente.

Cambiar el perfil activo

Si no ve resultados suficientes o los resultados correctos en las vistas Navegar o Eventos, es posible que haya un perfil activo que está aplicando una consulta previa. Si no desea usar ningún perfil, puede hacer clic en **Desactivar perfil** en el menú desplegable **Perfil**.

Para usar otro perfil:

1. En la barra de herramientas de las vistas **Navegar** o **Eventos**, abra el menú desplegable **Perfiles**.
2. Mantenga el mouse sobre la opción **Perfil** para mostrar una lista desplegable de perfiles disponibles.

3. Seleccione el perfil que desea usar.
   La configuración del perfil se aplica de inmediato.

Si desea cambiar el perfil activo en el cuadro de diálogo Administrar perfil:

1. En la barra de herramientas de las vistas **Navegar** o **Eventos**, seleccione **Perfiles > Administrar perfiles**.
   Se muestra el cuadro de diálogo Administrar perfiles.
2. Seleccione un perfil en el panel izquierdo y haga clic en **Guardar y aplicar**.
   Se muestra un cuadro de diálogo de confirmación.
3. Haga clic en **Sí**.
   La configuración del perfil se aplica de inmediato.

Importar perfiles

Puede cargar o importar archivos `.jsn` que se descargaron desde otro servicio. Cuando los grupos de perfiles se exportan y, a continuación, se importan, se mantiene la agrupación de perfiles.

1. En el cuadro de diálogo **Administrar perfiles**, haga clic en  en la barra de herramientas del panel izquierdo.
   Se muestra el cuadro de diálogo Importación de perfil.
2. Haga clic en **Navegar** o en el campo **Cargar archivo** para seleccionar un archivo de la computadora.
3. Cuando se haya seleccionado el archivo, haga clic en **Cargar**.
   El perfil se muestra en el panel de la izquierda.

Descargar perfiles

Los perfiles se descargan como archivos .jsn.

1. En el cuadro de diálogo **Administrar perfiles**, seleccione uno o más perfiles en el panel de la izquierda.
2. En la barra de herramientas del panel izquierdo, haga clic en  .
   La descarga comienza de inmediato.

Buscar patrones de texto

Puede buscar patrones de texto en el conjunto de eventos actual en las vistas Navegar y Eventos. Puede ejecutar una búsqueda de texto por palabra clave o una coincidencia de regex (expresión regular). En la vista Navegar, puede hacer clic en un valor de metadatos, como HTTP, para desglosar a los datos y, a continuación, ingresar una cadena de búsqueda en el campo Buscar para buscar eventos en ese subconjunto de datos. La búsqueda abre una pestaña en la vista Eventos, presenta el desglose y el rango de tiempo hacia delante y muestra los resultados de búsqueda. También puede desglosar a los datos mediante consultas antes de iniciar una búsqueda. Para ejecutar la búsqueda, ingrese una cadena de búsqueda en el cuadro Buscar y presione **Intro** o haga clic en **Buscar**.

Búsqueda por palabra clave

La búsqueda de texto proporciona estas funcionalidades:

- A cada palabra delimitada por un espacio en blanco se le agrega Y para que se encuentren todas las palabras, pero el orden o la ubicación con relación a las otras palabras es irrelevante. Por ejemplo, si busca `Mark Albert`, tanto Mark como Albert se deben encontrar en la sesión, pero no es necesario que estén juntas o en un orden específico.
- La palabra O es especial. Si busca `Mark OR Albert`, se debe encontrar Mark o Albert como coincidencia en la sesión, pero no se requieren ambos.
- Puede combinar o hacer coincidir Y y O implícitos juntos en la cadena de búsqueda. Un O explícito tiene mayor prioridad que Y implícito (espacio en blanco). En los siguientes ejemplos se hace la misma declaración lógica, que requiere que los términos cheese y dumplings estén presentes en una coincidencia, además de toast o bread:
  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```
- Puede excluir palabras de los resultados de la búsqueda con el operador −. Por ejemplo, la búsqueda de `cheese -toast` arrojará cualquier resultado que tenga la palabra cheese, a menos que la palabra toast también esté presente.
- La búsqueda por palabra clave puede coincidir con los metadatos almacenados en los siguientes patrones:
  - **Direcciones IPv4 e IPv6**. Cualquier término que se puedan reconocer como una dirección IP se convertirán al formato nativo de metadatos, de modo que puede encontrarse en los metadatos indexados.
  - **Rangos de IPv4 CIDR**. Puede usar la notación CIDR para localizar las direcciones IPv4 dentro de un rango.
  - **Registros de fecha y hora**. Los registros de fecha y hora se comparan con los metadatos de tiempo nativo y cualquier campo de metadatos de tiempo adicional se almacena con el tipo de tiempo.

- **Números**. La función de búsqueda intentará automáticamente identificar los términos de búsqueda decimal y hacerlos coincidir con campos numéricos de datos de metadatos.

Opciones para controlar el comportamiento de la búsqueda

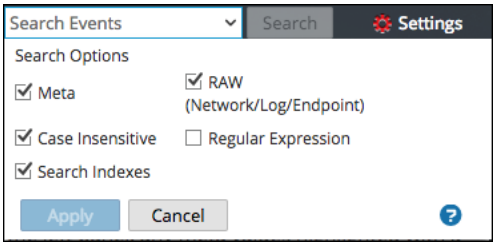
Para acceder al cuadro de búsqueda y a las opciones de búsqueda en las vistas Navegar o Eventos:

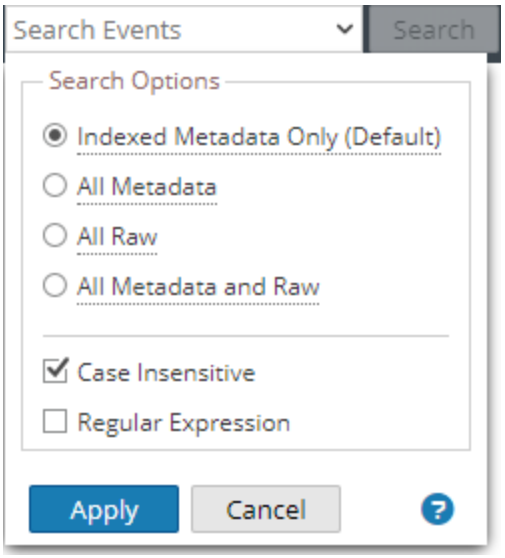
1. Puede ver el campo Buscar eventos en la barra de herramientas.

   Solución de problemas: Si no puede ver el campo Buscar eventos en la barra de herramientas, haga clic en  a la derecha de la barra de herramientas.

2. Haga clic en el campo Buscar para ver el menú desplegable Opciones de búsqueda. En la versión 11.2 y superior, las opciones del menú son ligeramente diferentes. En la primera figura se ilustra el menú de la versión 11.1 e inferior; en la segunda figura, el menú de la versión 11.2 y superior.

Las opciones seleccionadas en este cuadro cambiarán la forma en que se ejecuta la búsqueda. El modo de búsqueda predeterminado es buscar índices únicamente para metadatos indexados y datos crudos.

Nota: Debido a que la casilla de verificación Índice o metadatos indexados únicamente (valor predeterminado) está seleccionada de manera predeterminada, la búsqueda devuelve resultados en función de los datos que están indexados. Si desea buscar un conjunto de metadatos completo o datos crudos, seleccione estas casillas de verificación y deseleccione la casilla de verificación Índice o metadatos indexados únicamente (valor predeterminado). Este tipo de búsqueda tarda más, pero contiene un conjunto de datos más completo.

En la siguiente tabla se describen las opciones de búsqueda de Investigation.

Función	Descripción
Casilla de verificación **Metadatos indexados únicamente (valor predeterminado)** (versión 11.2) Botón de opción **Índice** (versión 11.1)	Esta búsqueda devuelve resultados únicamente de los datos indexados. Buscar en el índice es la manera más rápida de buscar palabras clave en un conjunto de datos de gran tamaño. La búsqueda de índice utiliza cualquier índice pertinente presente en la recopilación de datos. **Precaución:** Las búsquedas de índice no encuentran coincidencias de subcadena. Si necesita coincidencias de subcadena, desactive esta casilla de verificación y utilice un modo de búsqueda sin índice.
Botón de opción **Todos los metadatos** (versión 11.2) Casilla de verificación **Metadatos** (versión 11.1)	Busca en los metadatos. Su patrón de regex o palabra clave se compara con los metadatos analizados.
Botón de opción **Todos los datos crudos** (versión 11.2) Casilla de verificación **RAW** (red/registro/terminal) (versión 11.1)	Busca en el texto de eventos de red, registro y terminal. Cada evento se decodifica y se busca en el contenido coincidencias con el patrón de regex o la palabra clave. Si selecciona todos los datos sin filtros en un Archiver, el tiempo de ejecución puede ser excesivo y se puede mostrar una advertencia. **Precaución:** La búsqueda cruda de sesiones de red hace que las sesiones se decodifiquen, lo cual requiere mucho tiempo. Es posible que desee deshabilitar las búsquedas crudas cuando busca recopilaciones solo de red.
Botón de opción **Todos los metadatos y datos crudos** (versión 11.2)	Busca en los metadatos y en el texto de registros o eventos. Esta opción es una combinación de dos opciones de la versión 11.1: Metadatos y RAW (red/registro/terminal), las que se podían seleccionar juntas. En la versión 11.2, puede seleccionar solamente un botón de opción.
No distingue mayúsculas de minúsculas	Omite mayúsculas y minúsculas en la búsqueda.
Expresión regular	Búsquedas que usan una expresión regular de Perl en lugar de texto. De forma predeterminada, ejecuta una búsqueda de texto. Para ejecutar una búsqueda de expresión regular, seleccione la opción Expresión regular. **Precaución:** - Las búsquedas de expresiones regulares pueden ser muy lentas. - Al combinar las expresiones regulares y las opciones de búsqueda en índices, el patrón de expresión regular se compara con valores de índice únicos en lugar de valores de metadatos. Esto genera resultados con mayor rapidez, pero no es una búsqueda exhaustiva de todos los metadatos o datos crudos.

Función	Descripción
Aplicar	Configura las opciones de búsqueda predeterminadas que se aplicarán a una búsqueda en la vista Navegar y en la vista Eventos. Esto también actualiza las preferencias de Investigation en su perfil (Perfil > Preferencias > pestaña Investigation). Las preferencias se guardan y se aplican de inmediato. Puede seleccionar opciones de búsqueda para una determinada búsqueda sin cambiar las preferencias de búsqueda predeterminadas.

Sintaxis de búsqueda de expresiones regulares

La búsqueda de una expresión regular utiliza sintaxis de expresión regular de Perl, que se documenta detalladamente en http://perldoc.perl.org/perlre.html.

Búsqueda por palabra clave en texto crudo

El Log Decoder tiene la capacidad de crear un índice de texto crudo para eventos de registro sin analizar. Esta funcionalidad crea elementos de metadatos que forman una indexación de texto completo en los servicios descendentes como Concentrators y Archivers. Cuando se habilita la opción Buscar en índices en las preferencias de búsqueda, la búsqueda utiliza automáticamente el índice de texto. Tenga en cuenta que el índice de texto genera elementos de metadatos que tienen una granularidad gruesa. Por ejemplo, la configuración predeterminada del indexador de texto trunca los términos de texto. Al comparar las coincidencias de índice con datos crudos, el motor de búsqueda encontrará resultados precisos para la búsqueda. Sin embargo, puede mejorar los tiempos de búsqueda si deshabilita la casilla de verificación de la búsqueda cruda. Si lo hace, se devolverá resultados con mayor rapidez, pero es posible que vea falsos positivos en los resultados de la búsqueda.

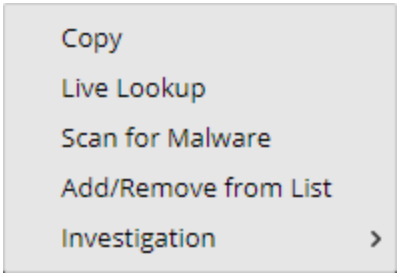
Ejemplos de búsqueda

Los siguientes ejemplos muestran búsquedas en las vistas Navegar y Eventos.

Búsqueda en la vista Navegar

Para buscar en los datos que se muestran actualmente en la vista Navegar:

1. Para desglosar a los datos, haga clic en un valor de metadatos, como HTTP, en el panel Valores.



2. Escriba una cadena de búsqueda en el campo Buscar y presione **Intro** o haga clic en **Buscar**.
3. Para borrar el cuadro de búsqueda y volver a la vista Eventos normal, haga clic en **X** en el cuadro de búsqueda.

Buscar en la vista Eventos

Para buscar en los datos que se muestran actualmente en la vista Eventos:

1. Escriba una cadena de búsqueda en el cuadro Buscar y presione **Intro** o haga clic en **Buscar**.
   Los resultados de búsqueda se muestran en la vista Eventos. Los eventos que coinciden con los criterios de búsqueda se muestran en la Lista de eventos. En la vista Detalles y en la vista Lista, las coincidencias se destacan en la columna Detalles. Además, cuando busca RAW, las coincidencias se resaltan en el columna Registros de la vista Registro.
2. Si desea limitar la búsqueda, cambie la consulta y la hora.
3. Si desea detener la búsqueda y volver a la vista Eventos, haga clic en **Cancelar**.
   Se conserva cualquier resultado que se muestre.
4. Para borrar el cuadro de búsqueda y volver a la vista Eventos normal, haga clic en **X** en el cuadro de búsqueda.

Ver y modificar consultas mediante la integración de URL

NetWitness Investigate incluye una integración de URL externa que facilita la integración con productos de otros fabricantes, ya que permite una búsqueda contra la arquitectura de NetWitness Platform. Cuando utiliza una consulta en un URI, puede ir directamente desde cualquier producto que permita vínculos personalizados a un punto de desglose específico en la vista Investigar. Esta integración proporciona una presentación interna de la consulta del usuario.

La integración de URL permite al usuario identificar el servicio, ya sea por el ID de host o por el servicio y el puerto, como se define en NetWitness Platform. Si NetWitness Platform no puede resolver el servicio, se redirige al analista a la vista Navegar, la cual muestra el cuadro de diálogo Selección de servicios. Una vez seleccionado el servicio, la vista Navegar se carga con el punto de desglose, definido por la consulta.

ID de servicio conocido

Cuando se conoce el ID del servicio que se usará para la investigación, el formato para ingresar un URI mediante una consulta con codificación URL es:

```
http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

donde

- `<sa host: port>` es la dirección IP o DNS, con o sin un puerto, según corresponda (ssl o no). Esta designación solo se necesita si el acceso está configurado sobre un puerto no estándar a través de un proxy.
- `<deviceId>` es el ID de servicio interno en la instancia de NetWitness Platform para el servicio que se consultará. El ID de servicio solo se puede representar como un entero. Puede ver el ID de servicio pertinente en la URL cuando accede a la vista Investigation en NetWitness Platform. Este valor cambia según el servicio al cual se conecta para el análisis.
- `<encoded query>` es la consulta de NetWitness Platform con codificación de URL. El largo de la consulta está restringido por las limitaciones de HTML URL.
- `<start date>` y `<end date>` definen el rango de fechas de la consulta. El formato es `<yyyy-mm-dd>T<hh:mm:ss>Z`.. Las fechas de inicio y finalización son obligatorias. Si no se proporciona ninguna fecha, se usan los valores predeterminados del usuario para ese servicio. Los rangos relativos (por ejemplo, última hora) no son compatibles con esta versión. Todas las horas se ejecutan como UTC.
  Por ejemplo:
  `http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Host y puerto conocidos

Cuando se conoce el host y el puerto del servicio que se usará para la investigación, el formato para ingresar un URI mediante una consulta con codificación URL es:

```
http://<sa host:port>/investigation/<device host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

donde

- `<sa host: port>` es la dirección IP o DNS, con o sin un puerto, según corresponda (ssl o no). Esta designación solo se necesita si el acceso está configurado sobre un puerto no estándar a través de un proxy.
- `<device host:port>` es el host y el puerto de un servicio definido en la instancia de NetWitness Platform para el servicio que se consultará. NetWitness Platform intenta resolver el host y el puerto como un ID de servicio definido en NetWitness Platform.
- `<encoded query>` es la consulta de NetWitness Platform con codificación de URL. El largo de la consulta está restringido por las limitaciones de HTML URL.
- `<start date> and <end date>` definen el rango de fechas de la consulta. El formato es `<yyyy-mm-dd>T<hh:mm:ss>Z`. Las fechas de inicio y finalización son obligatorias. Si no se proporciona ninguna fecha, se usan los valores predeterminados del usuario para ese servicio. Los rangos relativos (por ejemplo, última hora) no están soportado en esta versión. Todas las horas se ejecutan como UTC.
  Por ejemplo:
  `http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Ejemplos

Estos son ejemplos de consultas donde el servidor de NetWitness es 192.168.1.10 y el ID de dispositivo está identificado como 2.

Toda actividad realizada el 12/03/13 entre las 5:00 y 06:00 a.m. con un nombre host registrado

- Cambio personalizado: `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

Toda actividad realizada el 12/03/13 entre las 5:00 y 05:10 p.m. con tráfico http hacia y desde la dirección IP 10.10.10.3

- Cambio personalizado: `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Dirección con codificación diseccionada:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-12T17:00:00Z/2013-03-12T17:10:00Z`

Notas adicionales

Es posible que algunos valores no necesiten codificarse como parte de la consulta. Por ejemplo, normalmente se utiliza la IP src y dst para este punto de integración. Si aprovecha una aplicación de otros fabricantes para la integración de esta funcionalidad, es posible hacer referencia a ella sin aplicar la codificación.

Reconstruir un evento

Cuando observa una lista de eventos en la vista Eventos, puede crear con seguridad una reconstrucción del evento en un formato legible que coincide con el original. De forma predeterminada, la vista inicial de un evento reconstruido es el formato más adecuado (Mejor reconstrucción); por ejemplo, el contenido web se reconstruye como una página web; una conversación por IM se muestra con ambas partes de la conversación. Cada usuario puede seleccionar una reconstrucción predeterminada distinta en la vista Perfil > Preferencias.

También puede abrir una reconstrucción desde la vista Navegar si conoce el ID de evento.

En la reconstrucción, puede:

- Seleccionar la información del evento que desea ver. Los valores posibles son: datos de solicitud, datos de respuesta, datos de solicitud y de respuesta.
- Seleccione el tipo de reconstrucción: detalles, texto, hexadecimal, paquetes, web, correo o IM.
- Exportar registros crudos.
- Exportar el evento como un archivo PCAP.
- Extraer los archivos disponibles en el evento.
- Extraer todos los metadatos asociados al evento.

  Precaución: tenga cuidado cuando haga clic en un vínculo a un archivo en la reconstrucción. Si el sistema tiene una aplicación asociada al archivo o el navegador puede abrirlo y los archivos adjuntos son maliciosos, estos pueden afectar negativamente al sistema.

- Mostrar el evento en una ventana o pestaña independiente (dependiendo de la configuración del navegador).
- Si visualiza la reconstrucción como una vista previa en la vista actual, puede avanzar al próximo evento y retroceder al evento anterior mediante los botones de navegación en la esquina inferior izquierda.

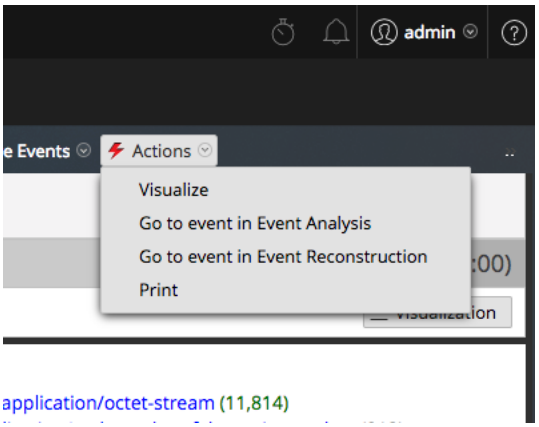
Nota: Las opciones Configuración de la reconstrucción y Configuración de caché de reconstrucción permiten que un administrador administre el rendimiento de las aplicaciones para Investigation. A medida que los analistas reconstruyen las sesiones que están investigando, dos situaciones pueden afectar el rendimiento y los resultados.
- Algunos eventos pueden ser muy grandes e incluir muchos miles de paquetes de origen. La reconstrucción de estos tipos de sesiones puede degradar el rendimiento de las aplicaciones.
- En algunos casos, la caché de reconstrucción puede presentar contenido incorrecto; por esta razón, NetWitness Platform limpia cada 24 horas la caché que tiene más de un día. Entre las limpiezas diarias de la caché, ciertas acciones pueden dejar obsoleta la caché que se usa en una reconstrucción y, si es necesario, los administradores pueden limpiar manualmente la caché para uno o más servicios que están conectados al NetWitness Server actual.

Reconstruir un evento desde la vista Navegar

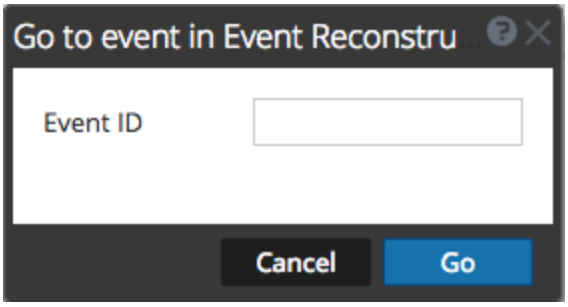
Puede reconstruir un evento directamente desde la vista Navegar si se conoce su ID. Puede usar esta opción sin ejecutar una consulta, como se hace normalmente cuando se inicia una investigación. Se debe seleccionar un servicio y un rango de tiempo para poder ir de manera directa a un evento únicamente con su `eventid`.

Para ver una reconstrucción o un análisis de eventos directamente en la vista Navegar:

1. Vaya a **INVESTIGAR** > **Navegar** y seleccione **Acciones** > **Ir a evento en Análisis de eventos** o **Ir a evento en Reconstrucción de evento**.



Se muestra el cuadro de diálogo Ir a evento. Hay dos cuadros de diálogo, uno para Análisis de eventos y otro para Reconstrucción de evento. Ambos solicitan el ID de evento.

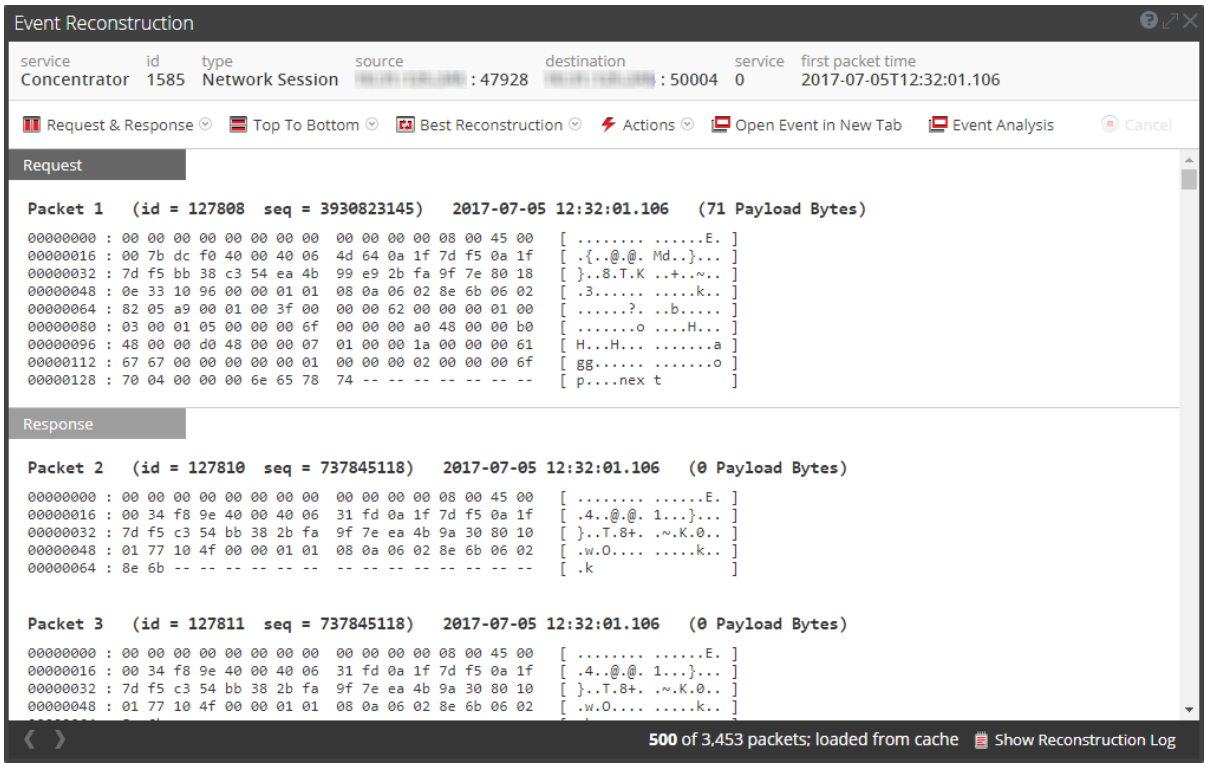


2. En el campo **ID de evento**, escriba el ID y haga clic en **Ir**.
   El evento especificado se reconstruye en la vista Reconstrucción de evento o en la vista Análisis de eventos.

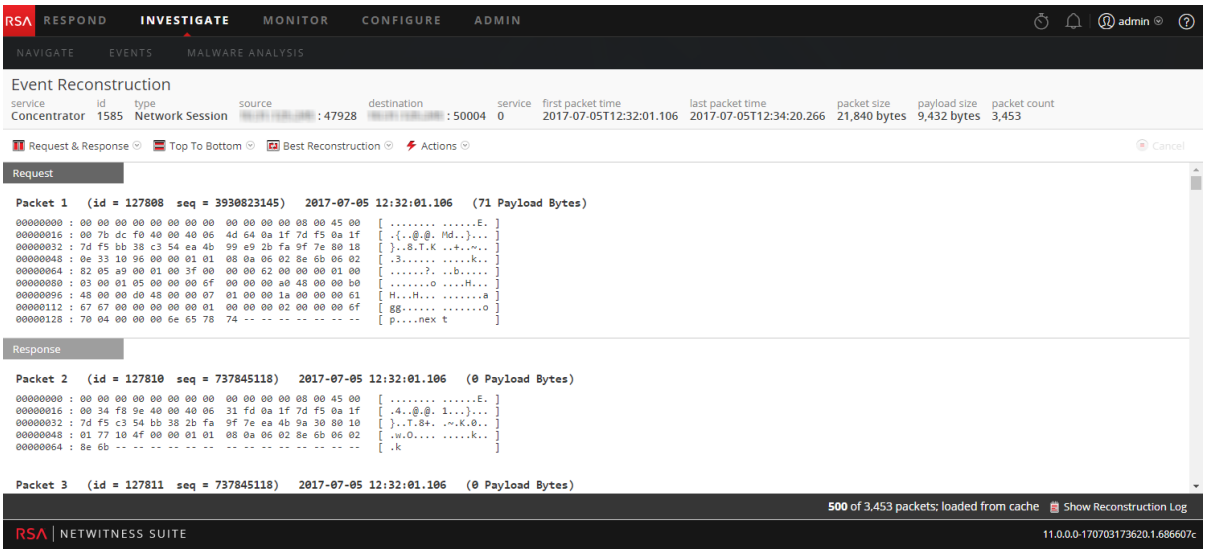
Reconstruir un evento desde la vista Eventos

1. Abrir un punto de desglose en la vista **Eventos**.
2. Para mostrar todos los metadatos, haga clic en + Show Additional Meta .
3. Para abrir una reconstrucción de evento en la vista actual, seleccione un evento que desee reconstruir y elija **Acciones** > **Ver evento** > **Vista previa en línea**.
   La Reconstrucción de evento se abre en una ventana emergente en la misma vista. De forma predeterminada, NetWitness Platformmuestra la mejor reconstrucción para el evento, según lo determina el contenido del evento, o la reconstrucción que seleccionó en la configuración Vista de

sesión predeterminada para Investigation. Puede utilizar las opciones de la barra de herramientas Reconstrucción de evento para cambiar el método de reconstrucción, ver los resultados en paralelo, exportar un evento, abrir archivos adjuntos del correo electrónico, extraer archivos y abrir el evento en una nueva pestaña. Las opciones de la barra de herramientas varían según el tipo de evento que se reconstruye (evento de red, evento de registro o evento de terminal). Este es un ejemplo de la reconstrucción de un evento de red.



4. Para tener una vista previa de una reconstrucción del siguiente evento, haga clic en  o para una vista previa de una reconstrucción del evento anterior, haga clic en  .
5. Para abrir una reconstrucción de evento en una nueva pestaña, realice una de las siguientes acciones:
   a. En la vista **Eventos**, seleccione un evento para reconstruir y elija **Acciones** > **Ver evento** > **Abrir en una nueva pestaña**.
   b. En la barra de herramientas **Reconstrucción de evento** de la reconstrucción con vista previa, haga clic en **Abrir evento en nueva pestaña** en la barra de herramientas.
      La Reconstrucción de evento se abre en una pestaña nueva.



Ver en paralelo o de arriba abajo

Para seleccionar la forma en que se muestran las solicitudes y respuestas para un evento:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **De arriba abajo** o **En paralelo**.
2. En el menú desplegable, seleccione la información que desea ver en el evento: **En paralelo** o **De arriba abajo.**
   La reconstrucción se actualiza con la información seleccionada.

Seleccione la información del evento que desea ver

Para seleccionar la información de evento que desea ver:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **Solicitud y respuesta**.
2. En el menú desplegable, seleccione la información que desea ver en el evento: **Solicitud y respuesta**, **Solicitud** o **Respuesta**.
   La reconstrucción se actualiza con la información seleccionada.

Seleccionar el tipo de reconstrucción de evento

Para seleccionar el tipo de reconstrucción de un evento:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **Mejor reconstrucción**.
2. En el menú desplegable, seleccione el tipo de reconstrucción que desea ver: **metadatos**, **texto**, **formato hexadecimal**, **paquetes**, **web**, **correo** o **archivos**.
   La reconstrucción se actualiza con el tipo de reconstrucción seleccionado.

Abrir o descargar archivos adjuntos del correo electrónico

Cuando observa una reconstrucción de un correo electrónico que tiene archivos adjuntos, puede abrir tipos de archivos compatibles o descargarlos al sistema local.

Precaución: tenga cuidado cuando seleccione los archivos adjuntos. Si el sistema tiene una aplicación asociada a los archivos adjuntos o el navegador puede abrirlos y son maliciosos, estos pueden afectar negativamente al sistema.

Para abrir o descargar archivos adjuntos del correo electrónico:

1. En la barra de herramientas **Reconstrucción de evento**, seleccione el menú desplegable **Ver** y elija **Ver correo**.
   Se muestra la sección Reconstrucción de evento.
2. En la sección **Reconstrucción de evento** del correo electrónico, haga clic en Archivo adjunto.
   Si el tipo de archivo es compatible con el navegador, el archivo adjunto se abre en una pestaña nueva.
   Si no lo es, se muestra el cuadro de diálogo Descargar que permite descargar el archivo adjunto.

Exportar un evento como un archivo PCAP

La opción Exportar PCAP descarga las sesiones del rango de tiempo actual y del punto de desglose a un archivo PCAP. Para exportar un evento como un archivo pcap:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **Acciones**.
2. Haga clic en **Exportar PCAP**.
3. Se muestra un cuadro de diálogo de confirmación.
4. Haga clic en **Aceptar**.
   El trabajo se programa y, cuando se completa, el PCAP se descarga en el sistema de archivos local. En la pestaña Perfil > Trabajos, puede descargar la PCAP.

Extraer archivos de un evento reconstruido

La opción Extraer archivos extrae y descarga los archivos asociados con el evento. Para extraer archivos:

1. En la barra de herramientas **Reconstrucción de evento**, haga clic en **Acciones**.
2. Haga clic en **Extraer archivos**.
   Aparece el cuadro de diálogo Extracción de archivo.
3. Seleccione los tipos de archivos que desea extraer y haga clic en **Aceptar**.
4. El trabajo se programa y, cuando se completa, los tipos de archivo seleccionados se descargan en el sistema de archivos local. En la pestaña Perfil > Trabajos, puede descargar los archivos.

Análisis de eventos crudos y metadatos en la vista Análisis de eventos

Es posible analizar eventos crudos y datos en la misma vista cuando se trabaja en la vista Análisis de eventos. Después de que comprenda Tipos de reconstrucción en la vista Análisis de eventos, puede:

- Filtrar los resultados en la vista Análisis de eventos
- Examinar eventos en la vista Análisis de eventos
- Buscar contexto adicional en la vista Análisis de eventos
- Descargar los datos en la vista Análisis de eventos
- Realizar acciones en datos en la vista Análisis de eventos

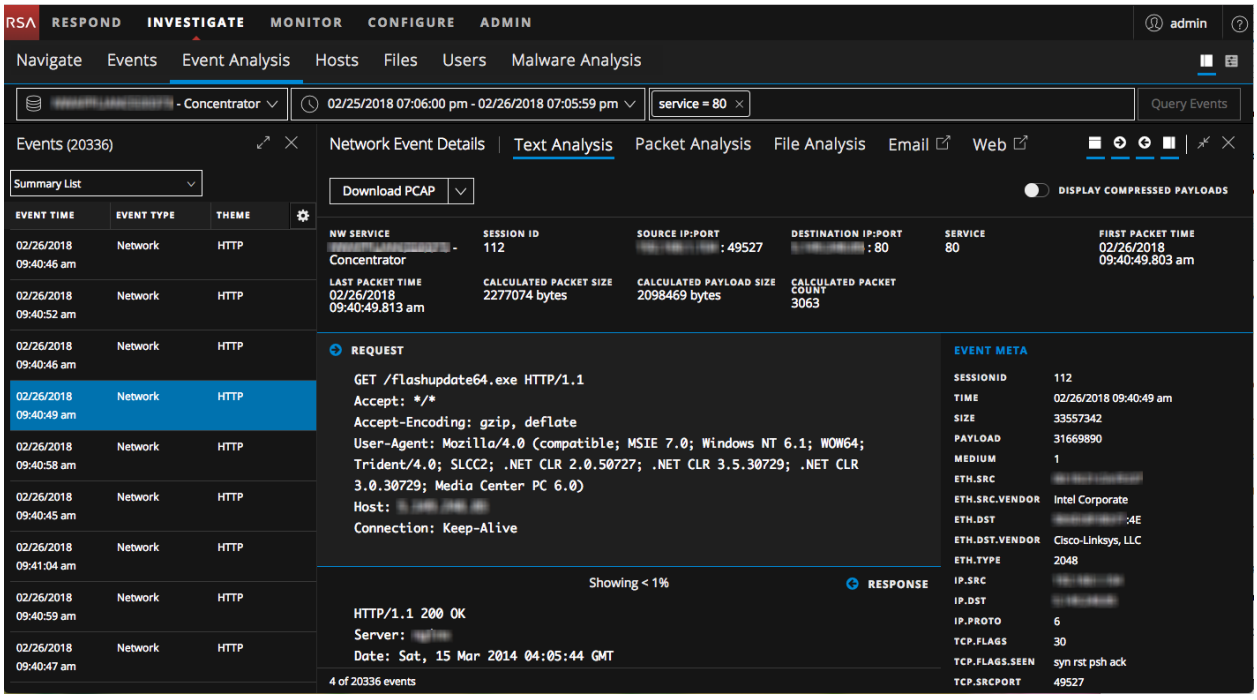
Tipos de reconstrucción en la vista Análisis de eventos

Durante la búsqueda de posibles amenazas en datos de red capturados, puede desglosar a distintos puntos de interés en los datos. Si una sesión contiene eventos sospechosos, puede examinar la lista de eventos de la sesión y también puede ver de manera segura una reconstrucción del evento con funciones que ayudan a identificar patrones. (Consulte Inicio de una investigación para conocer los distintos métodos de acceso a la vista Análisis de eventos).

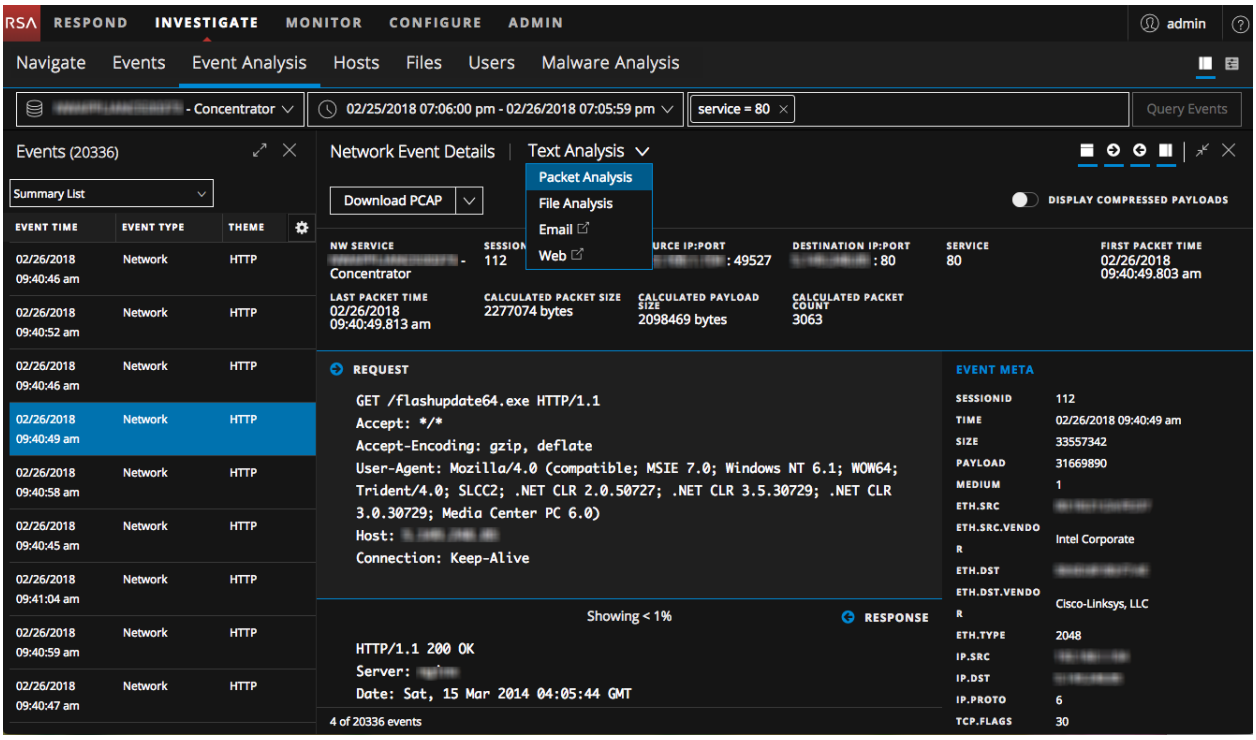
Nota: Si está analizando eventos un servicio 10.6.x u 11.0.0.x desde un servidor de NetWitness 11.1 u 11.2, el comportamiento de la descarga en la vista Análisis de eventos varía para los archivos, las PCAP, los registros, las cargas útiles y los valores de metadatos. Puede ver una carga útil de evento en un servicio 10.6.x u 11.0.0.x para el cual no tiene permiso, pero no podrá descargar los archivos ni las cargas útiles.

En la vista Análisis de eventos, puede seleccionar el formato de la reconstrucción: Análisis de paquetes, Análisis de archivos o Análisis de texto, **Correo electrónico** (versión 11.1 y superior) y **Web** (versión 11.1 y superior). Cuando la clave de metadatos `medium` etiqueta un evento como un evento de registro o un evento de terminal, solo está disponible el Análisis de texto. La reconstrucción predeterminada para los eventos de red es Análisis de texto; sin embargo, para un evento de red, el último formato de reconstrucción que se abrió reemplaza el valor predeterminado. Las reconstrucciones de correo electrónico y web abren el evento en la vista Eventos y se describen en “Seleccionar el tipo de análisis de eventos” en Examinar eventos en la vista Análisis de eventos

Esta figura es un ejemplo del panel Detalles del evento de red: Análisis de texto en una ventana del navegador web que es lo suficientemente ancha para mostrar las opciones de formato de reconstrucción en una fila.



Cuando la ventana del navegador es demasiado angosta para mostrar todas las opciones de visualización horizontalmente, estas se presentan en una lista desplegable.



Dentro de cada tipo de análisis, hay ajustes de configuración disponibles para mejorar el análisis. Si cambia una configuración, esta se conserva entre actualizaciones del navegador e inicios de sesión dentro del mismo navegador. Estos son los ajustes de configuración que se conservan:

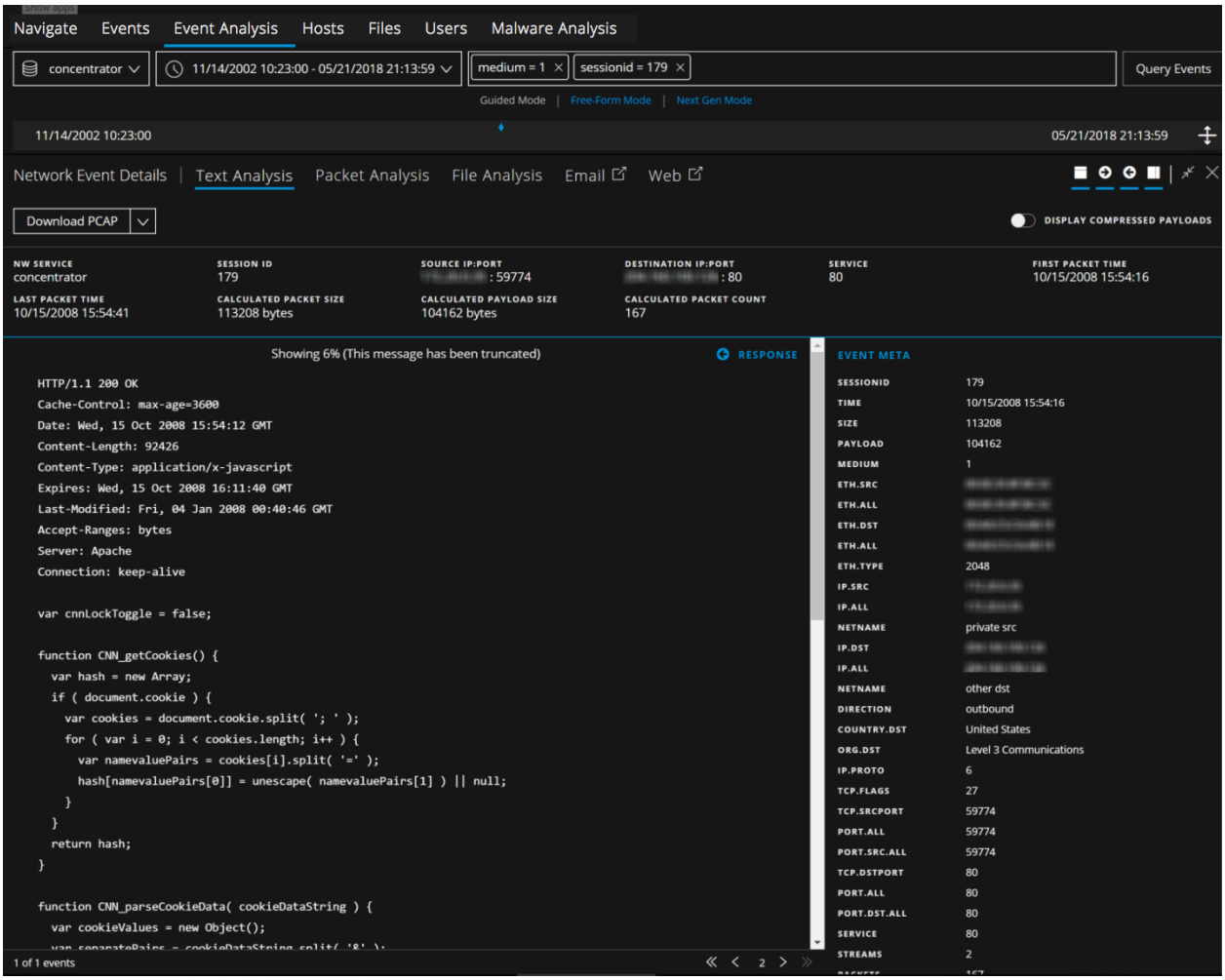
- La reconstrucción seleccionada: Análisis de texto, Análisis de paquetes o Análisis de archivos.
- Si el Panel Metadatos de eventos está abierto o cerrado.
- Si el encabezado del evento está abierto o cerrado.
- Si se muestra la Solicitud, la Respuesta o ambas.
- Si se muestran cargas útiles de paquetes en el panel Análisis de paquetes.
- Si se muestran bytes sombreados en el panel Análisis de paquetes.
- Si se resaltan otros tipos de archivo comunes en el panel Análisis de paquetes.
- La cantidad de paquetes por página en el panel Análisis de paquetes.
- Si se muestra texto comprimido o sin comprimir en el panel Análisis de texto.
- La configuración de decodificación de texto en el panel Análisis de texto de un evento de red.

El panel Análisis de texto

Puede ver todos los tipos de eventos (eventos de red, eventos de registro y eventos de terminal) en su formato de texto original en el panel Análisis de texto. Los controles de paginación agregan flexibilidad cuando se navega por el texto reconstruido de un evento.

Nota: Los eventos de terminal están disponibles para su investigación en la versión 11.1 y superior. Los controles de paginación están disponibles en la versión 11.2 y superior.

El panel Análisis de texto para algunos eventos de red puede ser bastante grande. Para garantizar la mejor representación, una carga útil excesivamente grande se trunca de modo que quepa. Si una única solicitud o respuesta reconstruidas en el evento reconstruido superan la cantidad máxima de bytes, el encabezado indica que el mensaje se truncó. En esta figura se ilustra una única respuesta que se truncó porque supera la cantidad máxima de bytes (versión 11.2).



En la versión 11.1, las cargas útiles grandes se manejan de otra manera; la carga útil de un único evento se limita a 2,500 paquetes. Cuando se alcanza el límite de paquetes, una advertencia en el pie de página advierte que se llegó al límite y proporciona la cantidad total de paquetes en el evento. En esta figura se muestra el mensaje de globo que aparece cuando se pasa el cursor sobre la advertencia.

Nota: La opción Mostrar más continúa disponible para los mensajes que se truncan; sin embargo, el texto completo del mensaje no se puede ver sin descargar la carga útil cruda.

En el panel Análisis de texto, los eventos de red, los eventos de registro y los eventos de terminal se presentan de manera diferente.

- En el caso de los eventos de red, Investigate proporciona la dirección del paquete (Solicitud o Respuesta) y el contenido de cada paquete en formato de texto. Si está reconstruyendo un evento de

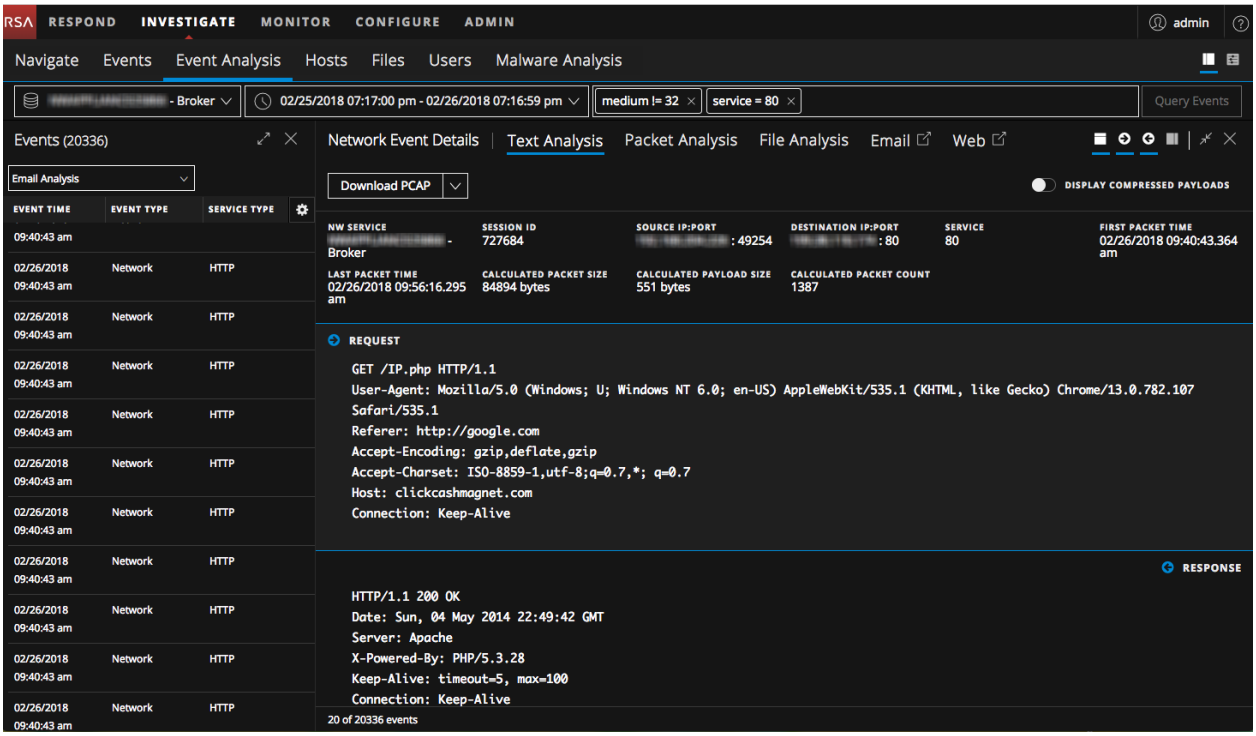
red, el panel Análisis de texto es desplazable. Cuando se desplaza, la información de identificación de texto, así como las etiquetas Solicitud y Respuesta, permanecen visibles en lugar de desplazarse fuera de la vista.

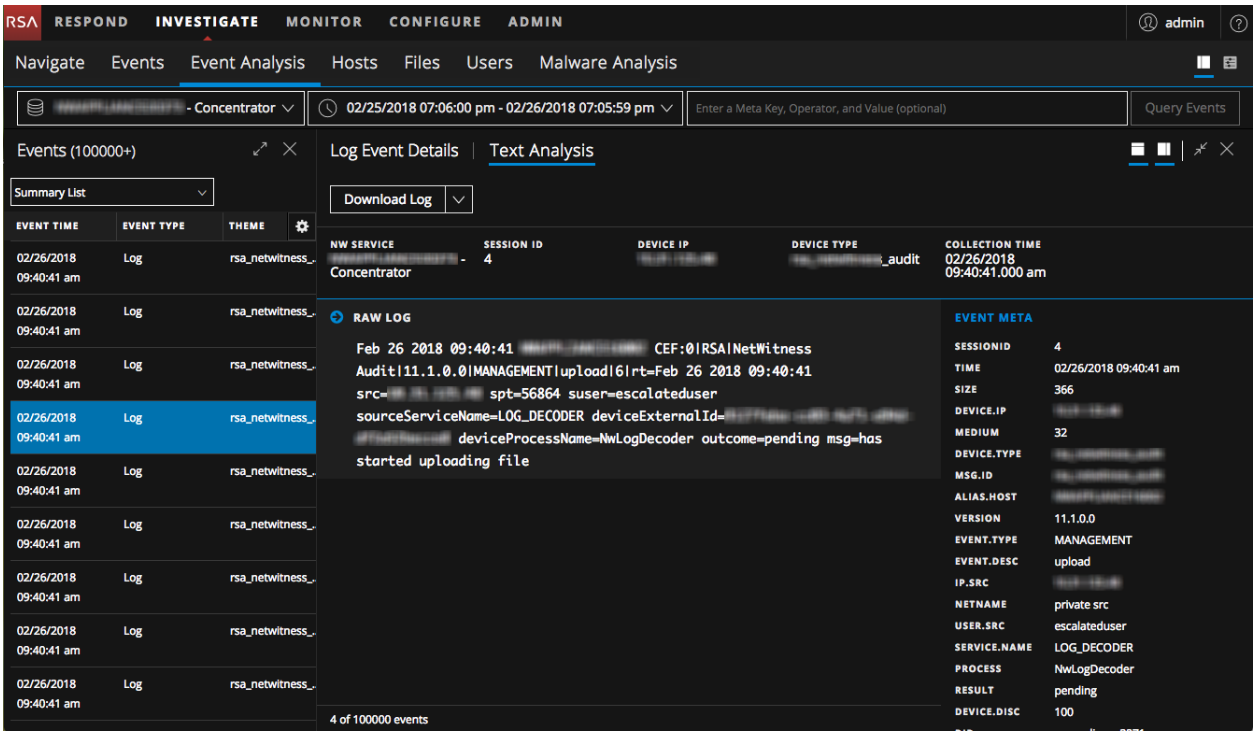
- Los eventos de registro y los eventos de terminal no tienen ninguna solicitud o respuesta; solo se muestra el evento crudo en el panel Análisis de texto.

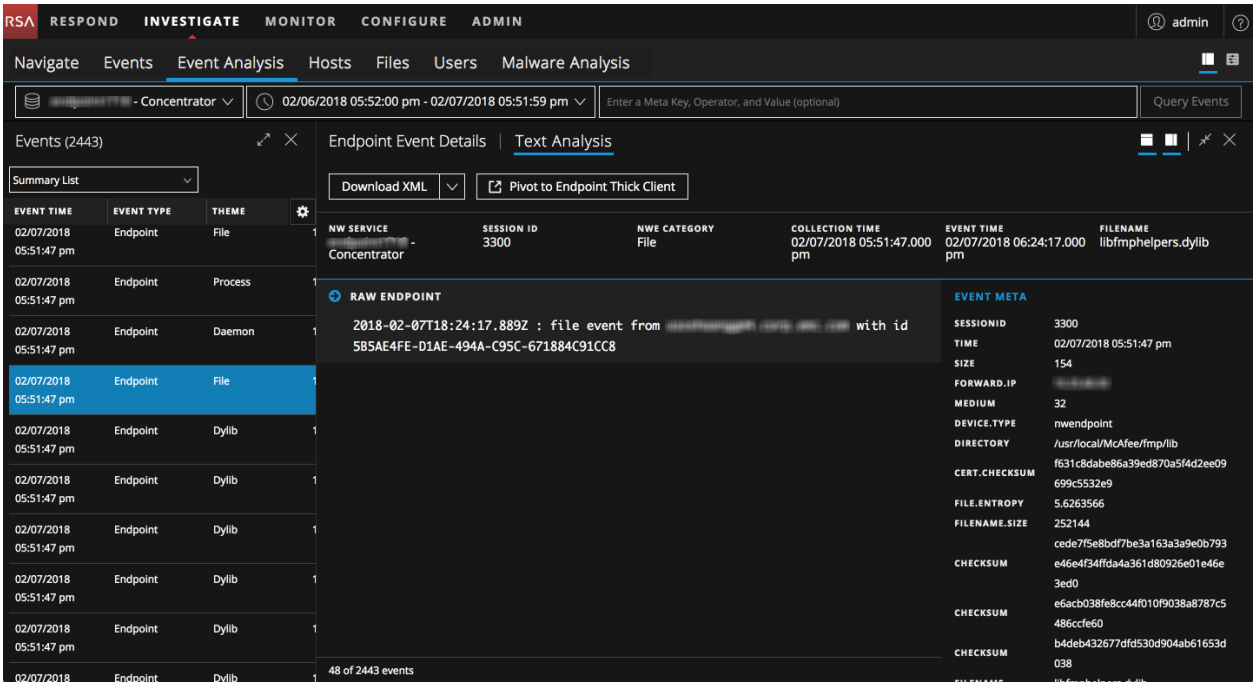
Para cada tipo de evento (red, registro o terminal), existen varias diferencias:

- El encabezado del evento incluye información pertinente a cada tipo de evento.
- Existen diferentes opciones de exportación.

El siguiente es un ejemplo del panel Análisis de texto para cada tipo de evento, un evento de red, un evento de registro y un evento de terminal.



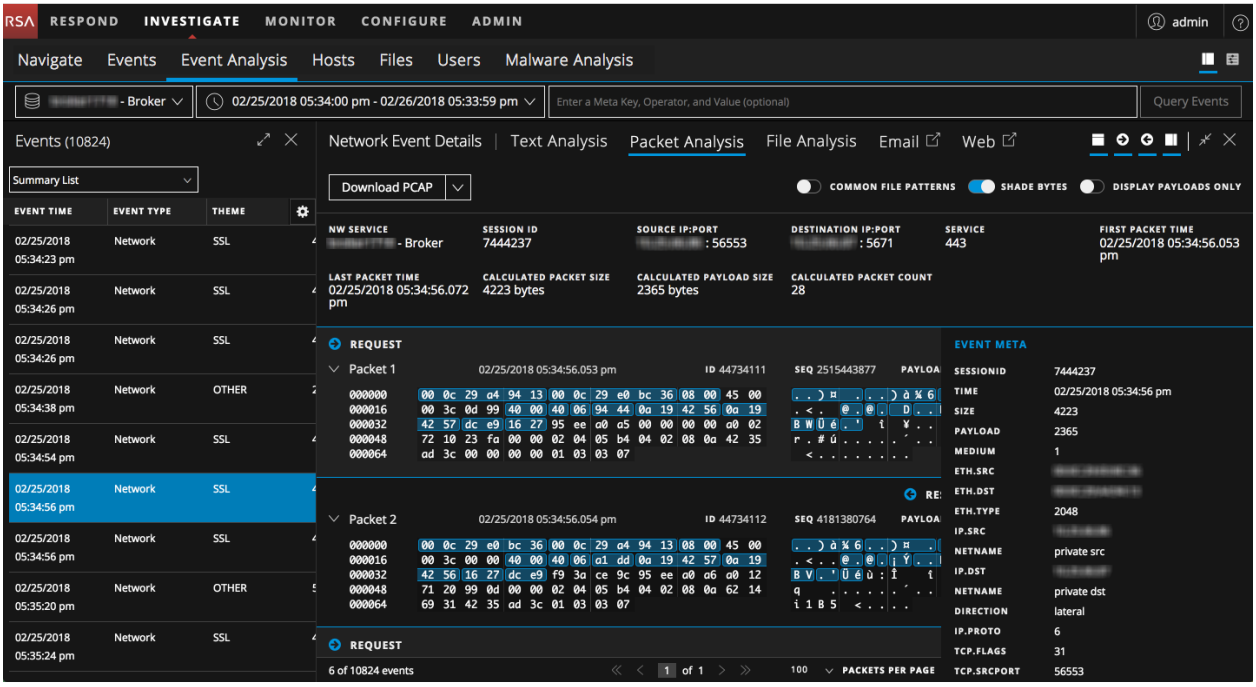




Nota: El conteo de paquetes calculado, el tamaño de paquetes calculado y el tamaño de cargas útiles calculado en el encabezado del evento puede ser distinto a las mismas estadísticas en el Panel Metadatos de eventos, porque, en ocasiones, los metadatos se escriben antes de que se complete el análisis de eventos y pueden incluir duplicados de paquetes.

El panel Análisis de paquetes

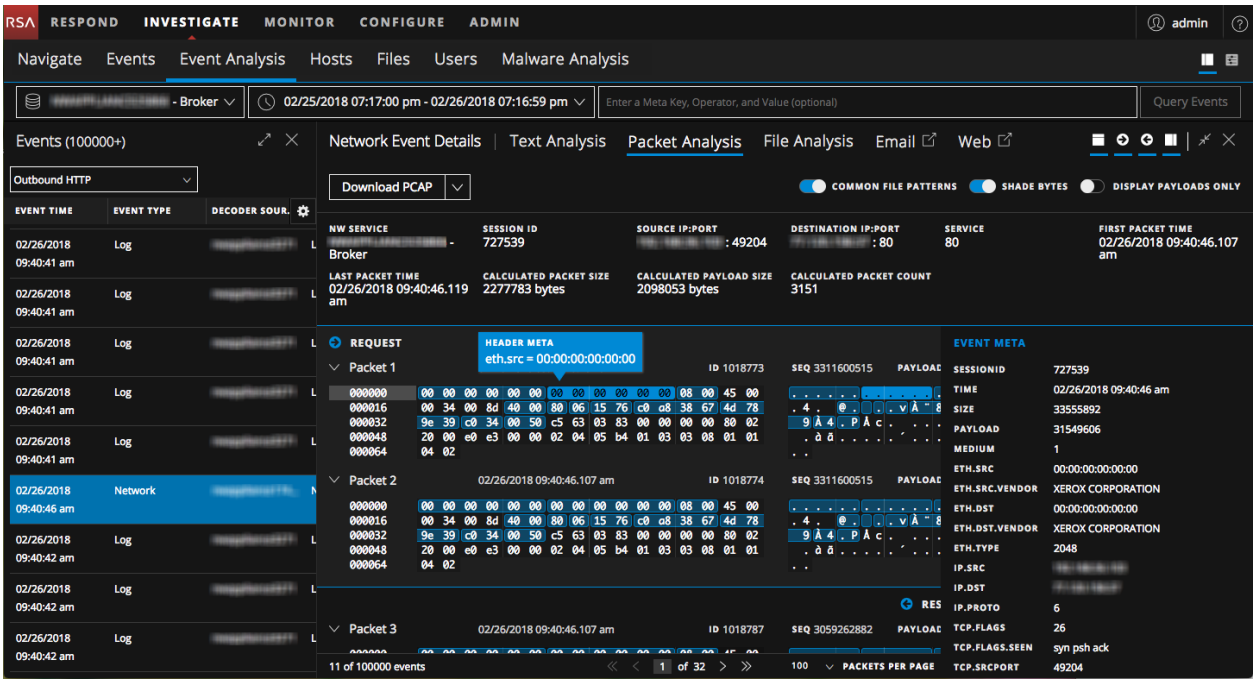
El panel Análisis de paquetes es solo para los eventos de red. El panel Análisis de paquetes es desplazable y la información de identificación de paquetes, así como las etiquetas Solicitud y Respuesta, permanecen visibles en lugar de desplazarse fuera de la vista.



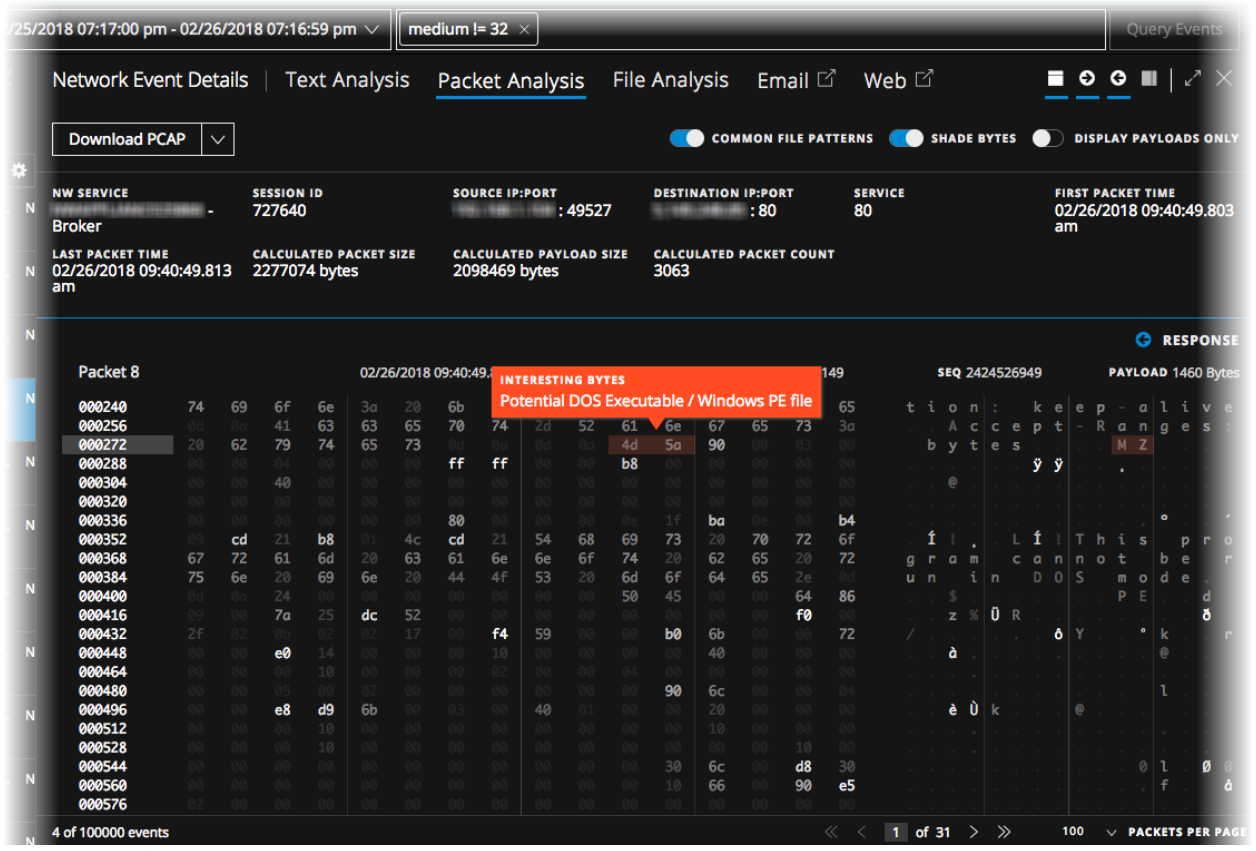
En el panel Análisis de paquetes, los encabezados proporcionan la dirección del paquete (Solicitud o Respuesta), el número del paquete, la hora de inicio del paquete, el ID del paquete y la secuencia, además del tamaño de la carga útil. Todos los paquetes comienzan con un encabezado y algunos de ellos tienen un pie de página. Algunos paquetes tienen una carga útil.

En la versión 11.1, los controles de paginación agregan flexibilidad cuando se navega por las páginas de los paquetes.

Los metadatos en los datos hexadecimales y ASCII se resaltan en azul; cuando coloca el cursor sobre los metadatos resaltados, se activa un cuadro que muestra la información de clave de metadatos/valor de metadatos.

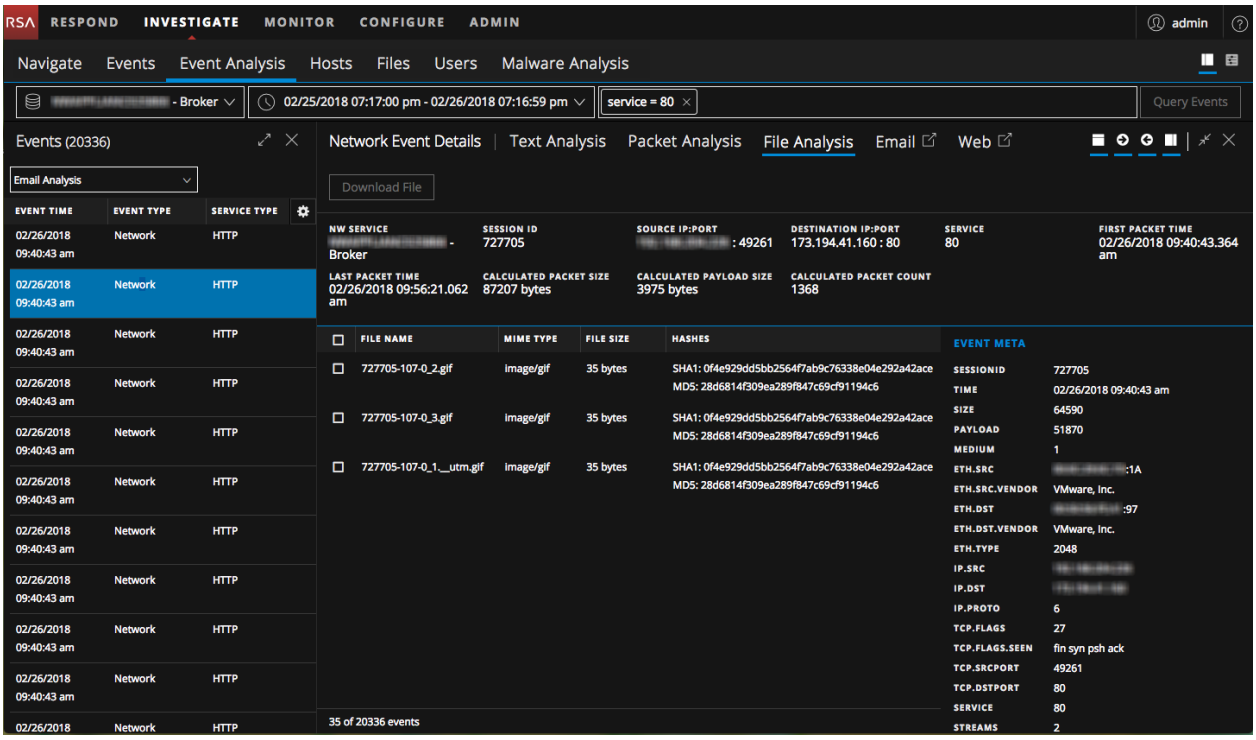


Las firmas de archivos comunes se resaltan con un fondo de color naranja. Cuando coloca el cursor sobre el texto resaltado, se activa un cuadro que muestra la descripción del tipo de archivo.

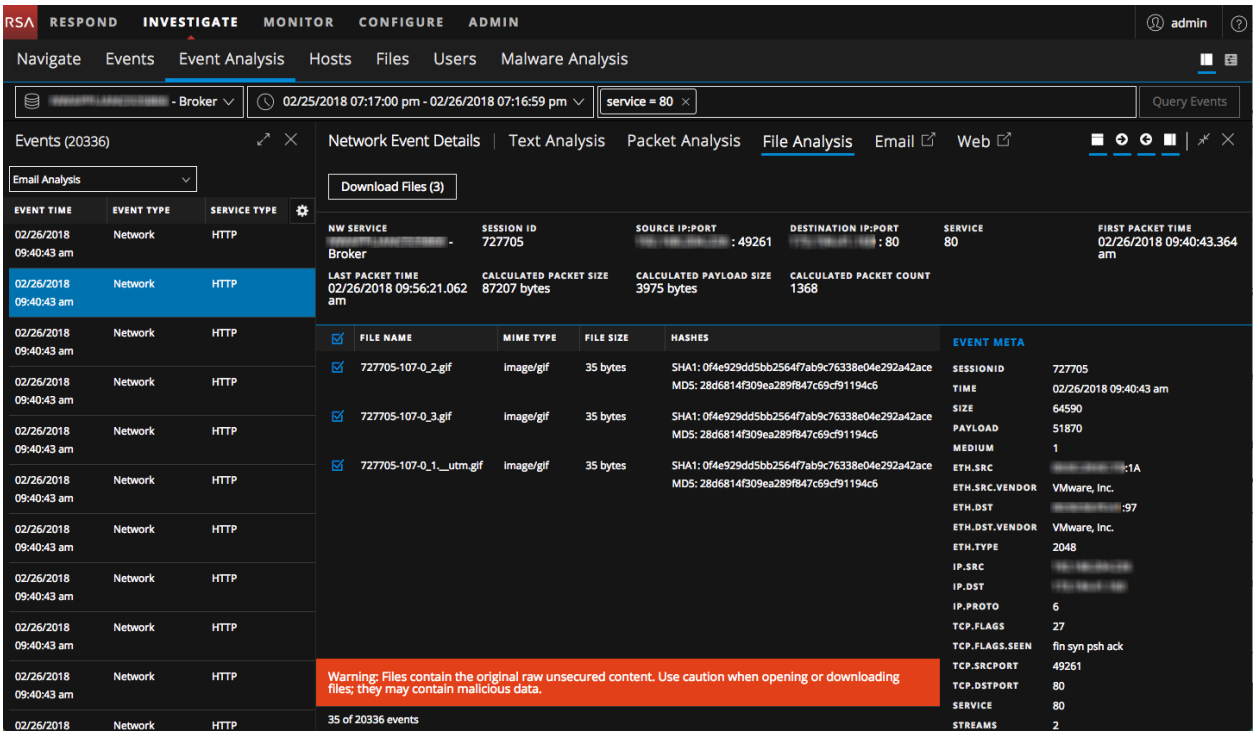


El panel Análisis de archivos

El panel Análisis de archivos muestra una lista de archivos asociados con el evento de red seleccionado. Este es un ejemplo del panel Análisis de archivos.



Puede seleccionar un archivo, varios archivos o todos ellos para exportarlos al sistema de archivos local. Cuando se seleccionan archivos, el botón Exportar archivos se activa y refleja la cantidad de archivos seleccionados.



Precaución: Se recomienda tener precaución al descomprimir y abrir archivos asociados con una aplicación predeterminada; por ejemplo, una hoja de cálculo de Excel se puede abrir automáticamente en Excel antes de que usted tenga la oportunidad de verificar su seguridad.

Herramientas analíticas para cada tipo de análisis de eventos

Las herramientas analíticas en la vista Análisis de eventos están diseñadas para ayudar a los analistas a encontrar información pertinente para los distintos tipos de eventos (evento de red, evento de registro y evento de terminal). En esta tabla se enumeran las acciones que puede realizar según el tipo de evento. En el resto de esta sección se proporcionan procedimientos para llevar a cabo las acciones.

Acción	Evento de red	Evento de registro	Evento de terminal
Ver el panel Análisis de texto	✓	✓	✓
Ver el panel Análisis de archivos	✓		
Ver el panel Análisis de paquetes	✓		
Abrir, cerrar y ajustar el tamaño de los paneles	✓	✓	✓
Ajustar la visualización de las solicitudes y las respuestas	✓		
Mostrar u ocultar el encabezado del evento en el panel Análisis de texto	✓	✓	✓

Acción	Evento de red	Evento de registro	Evento de terminal
Expandir las entradas de texto truncadas en el panel Análisis de texto	✓		
Cambiar entre una vista comprimida y descomprimida de las cargas de trabajo en el panel Análisis de texto	✓		
Ver bytes resaltados en el panel Análisis de paquetes	✓		
Resaltar los tipos de archivo comunes en el panel Análisis de paquetes	✓		
Mostrar solo la carga útil en el panel Análisis de paquetes	✓		
Sombrear los bytes en el panel Análisis de paquetes cuando solo se observa la carga útil	✓		
Realizar la codificación y la decodificación de URL y Base64 en el panel Análisis de texto	✓		
Ver texto descomprimido de una sesión de red HTTP en el panel Análisis de texto	✓		
Ver los metadatos de un evento en el panel Análisis de texto	✓	✓	✓
Descargar un evento de red (como un archivo PCAP, solo la carga útil, solo la solicitud o solo la respuesta) en los paneles Análisis de paquetes o Análisis de texto	✓		
Exportar archivos desde un evento de red en el panel Análisis de archivos	✓		
Descargar el archivo de un evento de registro en el panel Análisis de texto		✓	
Descargar el archivo de un evento de terminal en el panel Análisis de texto			✓
Abrir el evento de terminal actual en el panel Análisis de texto			✓

Filtrar los resultados en la vista Análisis de eventos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

En NetWitness Platform versión 11.0, cuando envía una consulta en las vistas Navegar o Eventos y se dirige a la vista Análisis de eventos, una ruta de navegación de solo lectura muestra la consulta enviada. Debe volver a la Vista Eventos o a la vista Navegar si desea ingresar una consulta diferente.

En la versión 11.1 y superior, un generador de consultas completa la ruta de navegación interactiva en la vista Análisis de eventos, de modo que usted puede crear y editar cada filtro `<meta key> <operator> <meta value>` en la ruta de navegación. Además, puede seleccionar un servicio y un rango de tiempo diferentes sin necesidad de volver a las vistas Navegar o Eventos. En el resto de esta sección se proporciona información sobre el uso de las funciones del generador de consultas.

Cómo funciona la ruta de navegación

Cuando hace clic en la opción Análisis de eventos en Investigate para abrir la vista, se muestra el selector de servicios y rango de tiempo. De forma predeterminada, el primer servicio se selecciona automáticamente (a menos que haya seleccionado un servicio con anterioridad y el servicio seleccionado se recuerde en el navegador). Si no selecciona un rango de tiempo, se usa el rango de tiempo predeterminado (3 horas). El campo del generador de consulta es un campo vacío que está a la derecha del rango de tiempo.

Cuando abre la vista Análisis de eventos desde las vistas Eventos o Navegar, el servicio, el rango de tiempo y los filtros que se seleccionaron en las vistas Eventos o Navegar se muestran en la ruta de navegación. El servicio, el rango de tiempo y los filtros individuales se pueden modificar.

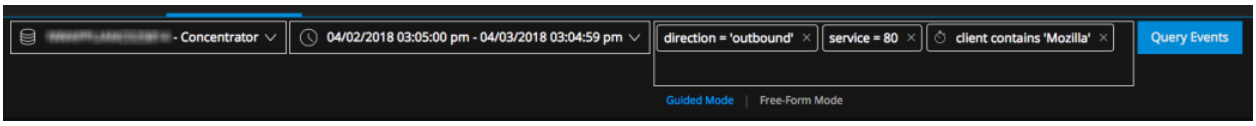
A partir de la versión 11.2, además de crear una consulta en el Modo guiado, los analistas avanzados pueden ingresar una consulta en el Modo de formato libre. El modo predeterminado es el Modo guiado, el cual incluye opciones de sugerencias automáticas y validación. El Modo de formato libre permite escribir una consulta compleja; la validación se realiza cuando esta se ejecuta.

Nota: Una consulta compleja es cualquier consulta distinta de un filtro básico de <clave de metadatos> <operador> <valor> que contiene los operadores `()`, `||`, `&&`, `length` o `regex`.

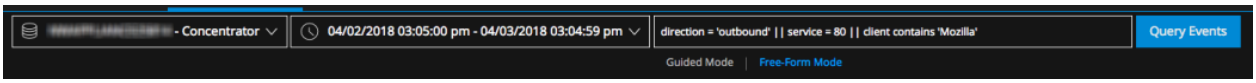
Dos botones alternan entre los modos y colocan un cursor en la barra de consulta que permite comenzar a crear una consulta de inmediato. Si seleccionó el Modo de formato libre la última vez que inició sesión, esta opción estará vigente en su próximo inicio de sesión.

- Cuando cambia del Modo guiado al Modo de formato libre, los filtros que creó en el Modo guiado se transforman en una consulta de texto en el campo Formato libre.
- Cuando cambia del Modo de formato libre al Modo guiado, la consulta que estaba escribiendo se agrega al generador de consultas como un único filtro no editable.
- Si comienza a crear una consulta con varios filtros en el Modo guiado, luego cambia al Modo de formato libre y regresa al Modo guiado sin cambios, los diversos filtros aparecen en el mismo estado en que los dejó.

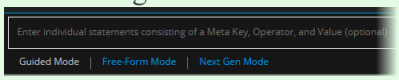
La siguiente figura es un ejemplo de la vista Análisis de eventos con el Modo guiado vigente en el generador de consultas.



La siguiente figura es un ejemplo del Formato libre en el generador de consultas.

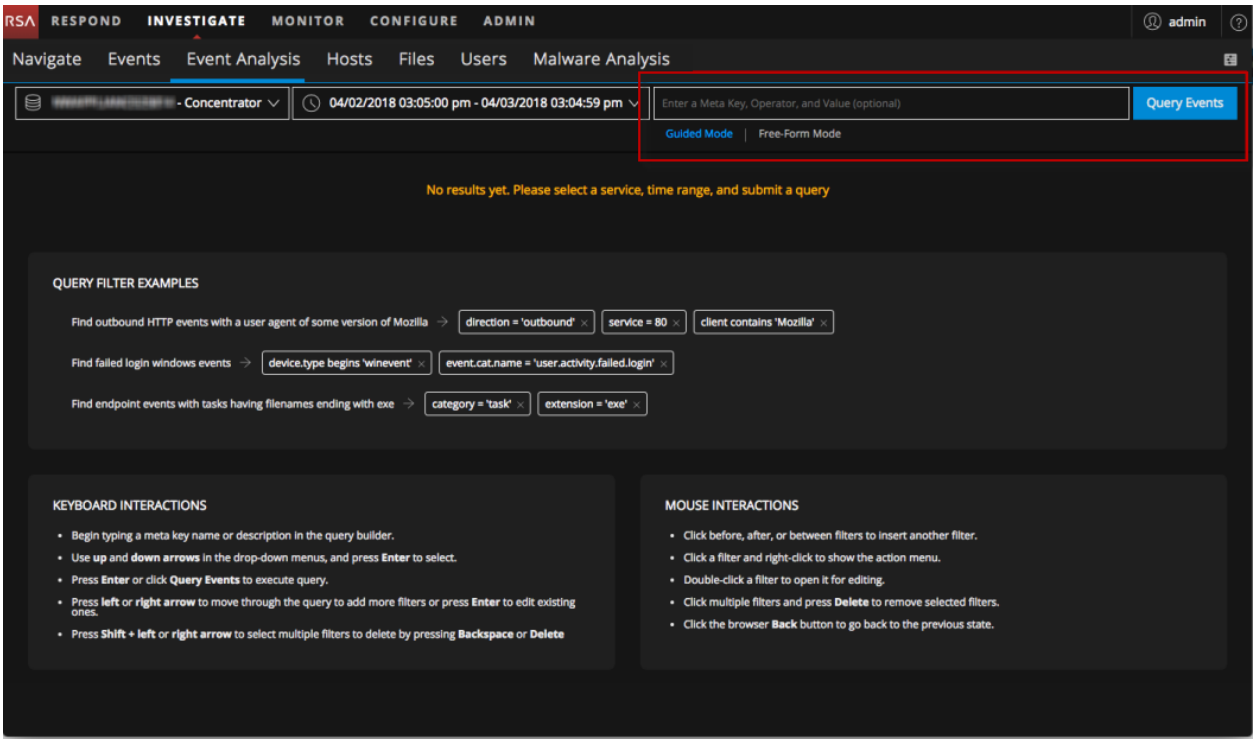


Nota: En la versión 11.2 se incluyó una característica beta no documentada, denominada modo de Última generación, en la vista Análisis de eventos del generador de consultas, que aún estaba en fase de desarrollo y pruebas. El modo de Última generación se deshabilitó en el parche 11.2.0.1. Si ve el modo de Última generación, no lo use; debe utilizar solamente el Modo guiado y el Modo de formato libre en el generador de consultas para asegurarse de obtener resultados coherentes y predecibles.



Modo guiado en el generador de consultas

El Modo guiado es la forma más sencilla de crear una consulta, ya que incluye características que ayudan a los analistas a ingresar consultas válidas. En la siguiente figura se ilustra la vista Análisis de eventos inicial con el Modo guiado vigente en el generador de consultas.



Nota: El Modo guiado del generador de consultas es compatible solamente con filtros en el formato `<meta key><operator><meta value>`. Si las vistas Eventos o Navegar tienen un filtro con más de un operador, `not`, `>`, `<`, `<=`, `>=`, `||`,`&&`, `()`, `REGEX` o `LENGTH`, el filtro se agrega, pero no se puede editar en la vista Análisis de eventos. Esto también es así para un filtro que proviene del Formato libre del generador de consultas.

A medida que crea filtros en el Modo guiado del generador de consultas, la ruta de navegación se actualiza con cada filtro en un campo editable. Cuando envía la consulta, se usa el operador Y con todos los filtros para generar resultados. La consulta no se envía hasta que usted hace clic en Consultar eventos. Los filtros se alinean de izquierda a derecha, lo que representa la secuencia en la que se crearon. Cada filtro es una expresión simple del formato `<meta key> <operator> <optional value>`. A medida que se agregan más filtros y no se pueden mostrar en una sola línea, se ajustan de manera automática en otra línea y el área de entrada se expande verticalmente para que todos los filtros estén visibles sin tener que desplazarse hacia la derecha.

A medida que crea y edita filtros, recibe sugerencias de completado automático que muestran únicamente claves de metadatos y operadores válidos en la lista desplegable. Puede escribir o seleccionar valores en la lista desplegable. En la lista desplegable, las operaciones cuya ejecución tarda más tiempo se marcan con un icono de cronómetro. Los filtros no válidos se marcan con un contorno rojo, y si coloca el cursor sobre el filtro, se muestra un mensaje de globo que explica el error.

El botón Consultar eventos está en el lado derecho de la entrada de la ruta de navegación y queda activo según sea necesario para el envío de una consulta. Se envía una consulta cuando se hace clic en Consultar eventos o se presiona Intro después de crear un filtro. Cuando hay un conjunto de resultados cargado y se cambia el servicio, el rango de tiempo o un filtro, el botón Consultar eventos se vuelve azul para indicar que los datos de la vista ahora están obsoletos. En la versión 11.2 y superior, el botón Consultar eventos también se volverá azul si ha pasado más de un minuto, debido a que el rango de tiempo de la consulta original ya no genera el mismo conjunto de resultados.

Nota: Si cambia el servicio, una llamada de red para datos en reconstrucciones o más datos en el panel Eventos (por ejemplo, Cargar más) usa los filtros anteriores de servicio/rango de tiempo/metadatos. La llamada de red continúa usando estos parámetros de consulta anteriores hasta que usted envía la nueva consulta.

Acciones del teclado que se usan en el Modo guiado

En el Modo guiado, el generador de consultas permite la entrada, la edición y la eliminación de filtros desde el teclado sin tener que utilizar un puntero. Aunque puede utilizar el puntero, tiene la opción de mantener sus dedos en el teclado. En esta tabla se identifican las acciones del teclado disponibles cuando el cursor está situado en la parte de la ruta de navegación del Modo guiado del generador de consultas; estas acciones no se aplican al selector de servicios ni al rango de tiempo.

Acción	Entrada del teclado
Enviar una consulta.	Con el foco en el generador de consultas y sin filtros pendientes, presione **Intro.**
Seleccionar el filtro que está inmediatamente a la izquierda, si existe uno.	Sin ninguna selección en el generador de consultas, presione la tecla **Flecha hacia la izquierda**.
Seleccionar el filtro que está inmediatamente a la derecha, si existe uno.	Sin ninguna selección en el generador de consultas, presione la tecla **Flecha hacia la derecha**.
Insertar un nuevo filtro inmediatamente a la izquierda del filtro seleccionado.	Con un filtro seleccionado, presione la tecla de **Flecha hacia la izquierda**.

Acción	Entrada del teclado
Insertar un nuevo filtro inmediatamente a la derecha del filtro seleccionado.	Con un filtro seleccionado, presione la tecla de **Flecha hacia la derecha**.
Insertar un nuevo filtro inmediatamente a la izquierda del filtro seleccionado y abrirlo para su edición.	Con un filtro seleccionado, presione las teclas **Mayús + Flecha hacia la izquierda**.
Insertar un nuevo filtro inmediatamente a la izquierda del filtro seleccionado y abrirlo para su edición.	Con un filtro seleccionado, presione las teclas **Mayús + Flecha hacia la derecha**.
Seleccionar todos los filtros a la derecha del filtro actual.	Con un filtro seleccionado, presione las teclas **Mayús + Flecha hacia abajo**.
Seleccionar todos los filtros a la izquierda del filtro actual.	Con un filtro seleccionado, presione las teclas **Mayús + Flecha hacia arriba**.
Editar un filtro seleccionado.	Con un único filtro seleccionado, presione la tecla **Intro**.
Deseleccionar todos los filtros.	Con un filtro seleccionado, presione la tecla **Esc**.
Eliminar los filtros seleccionados.	Con los filtros seleccionados, elija la opción **hacer clic con el botón secundario > Eliminar los filtros seleccionados**, presione **Eliminar** o presione la **Tecla de retroceso**.
Actualizar una consulta solo con los filtros seleccionados.	Con los filtros seleccionados, elija la opción **hacer clic con el botón secundario > Consultar con filtros seleccionados**.
Abrir una nueva pestaña con los filtros seleccionados.	Con los filtros seleccionados, elija la opción **hacer clic con el botón secundario > Consultar con filtros seleccionados en una pestaña nueva**.

Retroalimentación en el Modo guiado

El Modo guiado proporciona retroalimentación visual durante la creación de consultas. En esta tabla se identifica y se describe la posible retroalimentación.

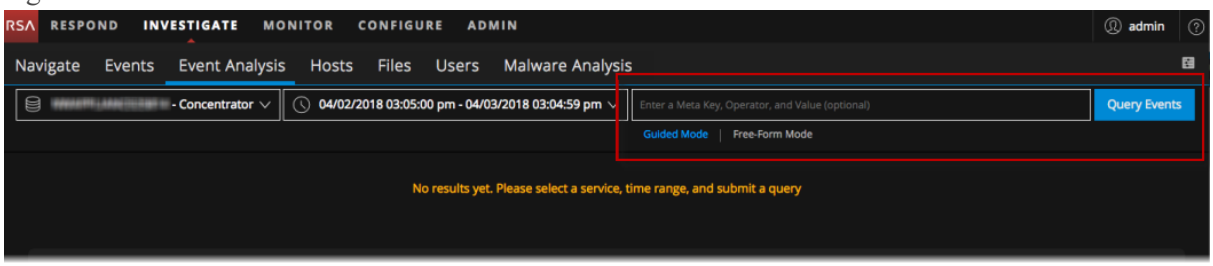
COMENTARIOS	Icono	Descripción
Círculo verde		El cursor se colocó entre dos filtros existentes. Si se hace clic, se inserta un nuevo filtro en esta ubicación.

COMENTARIOS	Icono	Descripción
Contorno rojo de un filtro		El tipo de valor no es válido para la clave de metadatos seleccionada; por ejemplo, un valor de cadena para una clave de metadatos que espera un entero. Se muestra un mensaje de globo en el que se explica el error.
Cronómetro		El procesamiento de la combinación de clave de metadatos/operador seleccionada requiere tiempo extra. Aunque la consulta se puede ejecutar de todos modos, se recomienda una clave de metadatos o un operador más eficientes.

Agregar un filtro en el Modo guiado

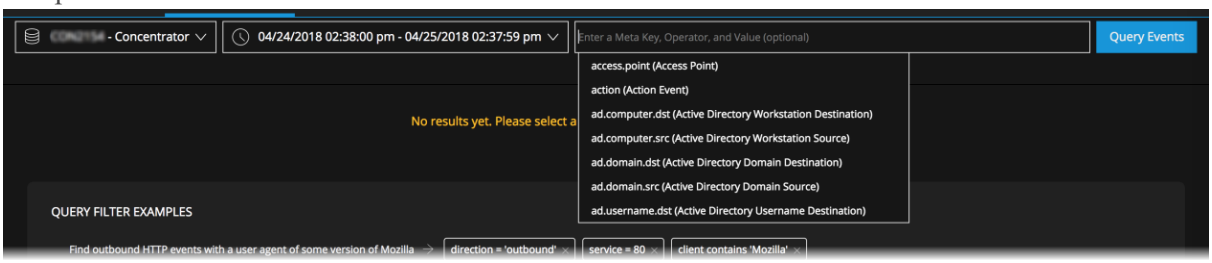
Para filtrar los datos que se muestran en la vista Análisis de eventos en el Modo guiado:

1. Vaya a la vista **Análisis de eventos** y seleccione **Modo guiado** debajo del generador de consultas. Este es un ejemplo del generador de consultas vacío en el Modo guiado antes de que se comience a ingresar un filtro.

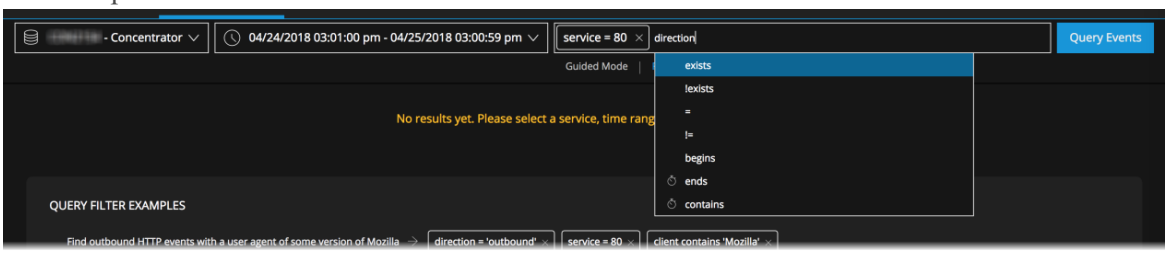


2. Para insertar un filtro, haga clic en el campo del generador de consultas o antes o después de un filtro existente.
   Si el punto de inserción está entre dos filtros, este se marca con un punto verde. Si el punto de inserción está al final de la ruta de navegación existente, se abre el campo de entrada del filtro con un cursor parpadeante en el punto de entrada. Un menú desplegable enumera las claves de metadatos disponibles para el servicio seleccionado en orden alfabético. Las claves de metadatos disponibles provienen del servicio que se investiga, y las claves de metadatos cuyo procesamiento requiere más

tiempo se marcan con un icono de cronómetro.

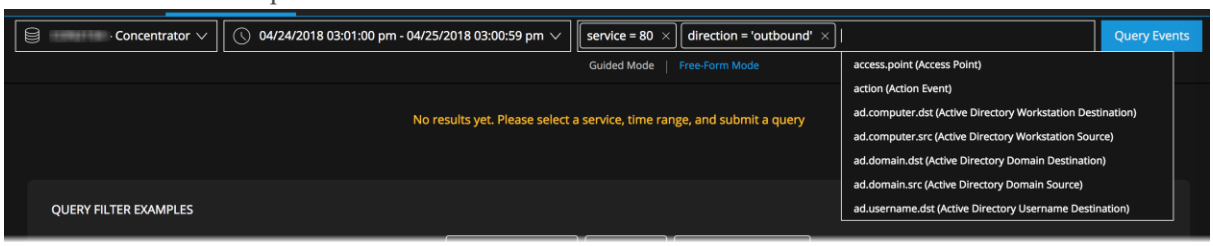


3. Para seleccionar una clave de metadatos, realice una de las siguientes acciones:
   a. Si solamente hay una opción en el menú desplegable, presione **Intro**.
   b. Si hay dos o más opciones en el menú desplegable, haga clic en la clave de metadatos o utilice la flecha hacia arriba/abajo y presione **Intro**.
   c. Comience a escribir la clave de metadatos. A medida que escribe la clave de metadatos, la lista se actualiza. Para seleccionar la clave de metadatos, presione **Intro**.
   d. Si desea editar o eliminar la clave de metadatos, presione la **Tecla de retroceso** o **Eliminar.**
   A medida que usa la Tecla de retroceso y elimina un carácter, la lista desplegable de claves de metadatos se filtra para incluir claves de metadatos que comienzan con esos caracteres. Para seleccionar una clave de metadatos, presione **Intro**.
   La clave de metadatos se agrega al generador de consultas y se muestra una lista de operadores válidos para la clave de metadatos seleccionada. Las operaciones cuyo procesamiento requiere más tiempo se marcan con un icono de cronómetro.



4. Para seleccionar un operador, realice una de las siguientes acciones:
   a. Si solamente hay una opción en el menú desplegable, presione **Intro**.
   b. Si hay dos o más opciones en el menú desplegable, haga clic en el operador o utilice la flecha hacia arriba/abajo y presione **Intro**.
   c. Escriba el operador y presione **Intro**.
   La lista desplegable se cierra y usted puede agregar un valor si el operador lo acepta.
5. (Opcional) Escriba un valor y presione **Intro**.
6. Para crear el filtro, presione **Intro**. Si hace clic en cualquier lugar fuera del cuadro antes de presionar **Intro**, el filtro no se crea.
   Se inserta el filtro nuevo, el cursor parpadeante se sitúa después del último filtro y se muestran las claves de metadatos. Si hay un error en el filtro, este se marca con un contorno rojo. Puede colocar el cursor sobre el filtro para ver un mensaje de globo en el que se explica el error. En esta figura se

muestra una consulta que se crea sin errores.



7. Corrija todos los filtros que tengan errores.
8. Cuando esté listo para ejecutar la consulta en la ruta de navegación, haga clic en **Consultar eventos**.
9. La Lista de eventos se actualiza para reflejar la consulta.

Editar un filtro en el Modo guiado

Cuando hay una consulta en el Modo guiado del generador de consultas, puede editar un filtro. Para editar un filtro:

1. Haga doble clic en el filtro o haga clic en él y presione **Intro**.
2. Edite el filtro. Cuando haya terminado de editar, presione **Intro** para actualizar el filtro.
3. Si desea volver a ejecutar la consulta, haga clic en el botón **Consulta**.
   La Lista de eventos se actualiza para reflejar el filtro actualizado.

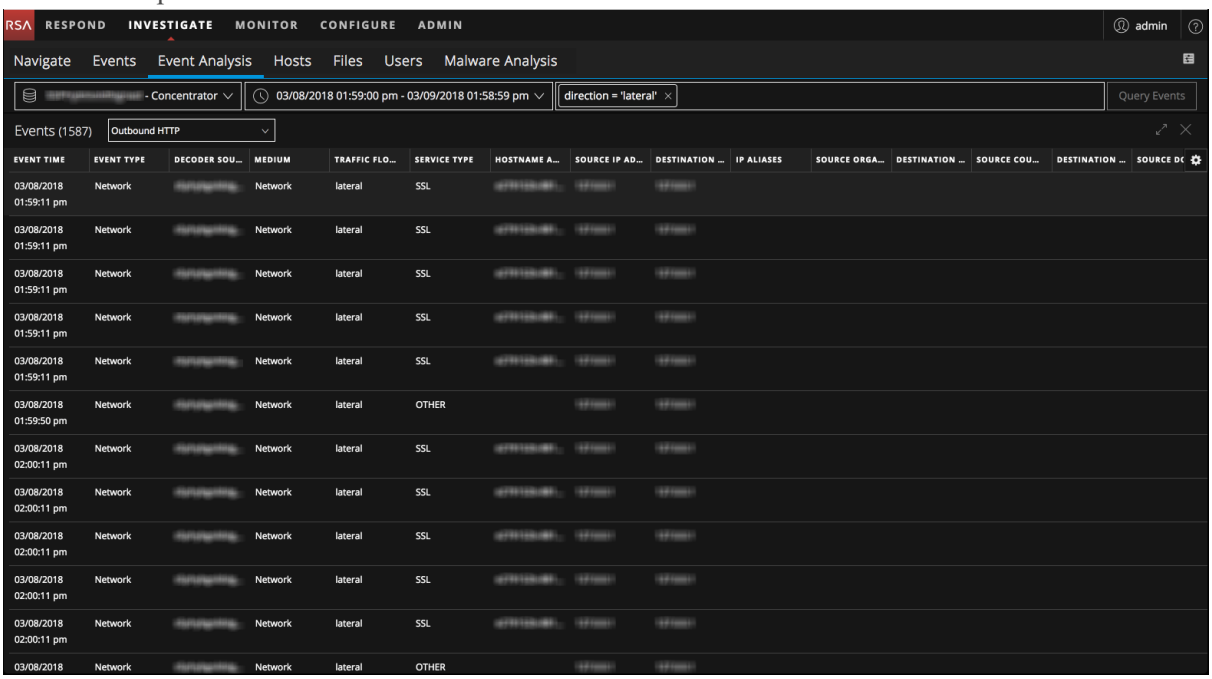
Consulta con los filtros seleccionados en el Modo guiado

Cuando hay uno o más filtros en el Modo guiado del generador de consultas, puede devolver el foco a la misma consulta para incluir únicamente los filtros seleccionados. Los resultados se muestran en la pestaña actual del navegador o en una nueva pestaña del navegador. Para actualizar la consulta solo con los filtros seleccionados:

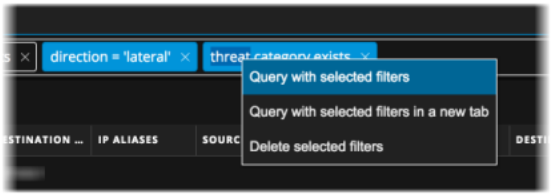
1. Comience con una consulta en el Modo guiado que incluya uno o más filtros; por ejemplo, una consulta tiene tres filtros: `risk.info = exists`, `direction ="lateral"` y `threat.category exists`.
2. Para abrir una pestaña nueva con los filtros seleccionados, elija `direction = "lateral"`, haga clic con el botón secundario en el filtro y seleccione **Consultar con filtros seleccionados en una pestaña nueva** en el menú desplegable.

   Se abre una nueva pestaña con los resultados del filtro seleccionado y la consulta original queda

intacta en la pestaña anterior.



3. Para consultar los filtros seleccionados en la misma pestaña, elija `direction = "lateral"` y `threat.category exists`. A continuación, haga clic con el botón secundario y seleccione **Consultar con filtros seleccionados** en el menú desplegable.



Se envía una consulta únicamente con los filtros seleccionados y se quitan todos los filtros restantes.

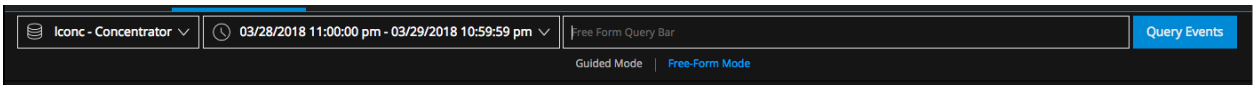
Eliminar un filtro en el Modo guiado

Para eliminar un filtro:

1. Haga clic en **X** en un filtro, haga clic en el filtro para seleccionarlo y presione **Eliminar** o haga clic con el botón secundario en uno o más filtros y seleccione **Eliminar los filtros seleccionados** en el menú desplegable.
2. Si desea volver a ejecutar la consulta, haga clic en el botón **Consulta**.
   El filtro seleccionado se elimina y la Lista de eventos se actualiza.

Formato libre en el Generador de consultas

Las consultas en Formato libre son más útiles cuando se tiene en mente una consulta compleja que se desea ingresar rápidamente y se conocen las claves de metadatos, los operadores válidos y la sintaxis válida para el ingreso de valores. En la siguiente figura se ilustra la vista Análisis de eventos inicial con la consulta en Formato libre vacía en el generador de consultas.



El cursor parpadeante indica que está lista para el ingreso de una consulta. Aquí puede ingresar texto libre. A medida que se agregan más expresiones y no se pueden mostrar en una sola línea, se ajustan de manera automática en otra línea y el área de entrada se expande verticalmente para que todos los filtros estén visibles sin tener que desplazarse hacia la derecha.

Estos son algunos ejemplos de consultas que puede ingresar en modo de Formato libre:

Para buscar eventos con un nombre de usuario de 8 a 11 caracteres similar a atreeman-72:
`user.all length 8-11 && (user.all regex '^a[a-z]{2}ee[a-z]{3}-[0-9]{2}')`

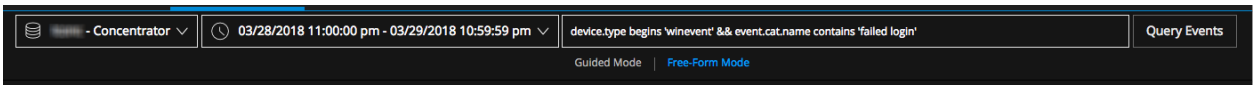
Para buscar eventos que son eventos de red HTTP o relacionados con registros de aix o ciscoasa:
`service=80 || (device.type = 'aix','ciscoasa')`

Para buscar todos los eventos salientes que no se dirigen a Canadá ni a Estados Unidos:
`direction = 'outbound' AND not(country.dst = 'united states' || country.dst = 'canada')`

Si tiene una consulta enviada en el Modo guiado, esta se transforma en texto cuando hace clic en Cambiar al modo de Formato libre. Este es un ejemplo de una consulta enviada en el Modo guiado.

Aquí puede ingresar texto libre. A medida que se agregan más expresiones y no se pueden mostrar en una sola línea, se ajustan de manera automática en otra línea y el área de entrada se expande verticalmente para que todos los filtros estén visibles sin tener que desplazarse hacia la derecha.

El botón Consultar eventos está en el lado derecho de la entrada de la ruta de navegación y se destaca en azul según sea necesario para el ingreso de una consulta. La consulta se aplica cuando se hace clic en Consultar eventos. En ese momento, la consulta se valida para mostrar errores de sintaxis y lógicos.



Las operaciones cuyo procesamiento requiere más tiempo no se destacan cuando están en el Modo guiado, pero en esta tabla se proporciona un resumen de operaciones con uso intensivo de recursos como referencia.

Método de índice	Valor no de texto	Valor de texto	Operaciones regulares	Operaciones con uso intensivo de recursos
Por clave	✓		`exists, !exists`	`eq, !eq`
Por clave		✓	`exists, !exists`	`eq, !eq, begins, ends, contains`

Método de índice	Valor no de texto	Valor de texto	Operaciones regulares	Operaciones con uso intensivo de recursos
Por valor	✓		`exists`, `!exists`, `eq`, `!eq`	no hay operadores con uso intensivo de recursos
Por valor		✓	`exists`, `!exists`, `eq`, `!eq`, `begins`	`ends`, `contains`
Por ninguno	caso especial para `sessionid`		`exist`, `!exits`, `eq`, `!eq`	no hay operadores con uso intensivo de recursos

Examinar eventos en la vista Análisis de eventos

Cuando se examinan eventos crudos y metadatos en la vista Análisis de eventos, puede realizar ajustes simples en la visibilidad y el tamaño de los paneles. Dentro de los paneles Análisis de paquetes y Análisis de texto, utilice funciones adicionales para ajustar la manera en que se muestra la reconstrucción y centrarse en datos interesantes.

Seleccionar el tipo de análisis de eventos

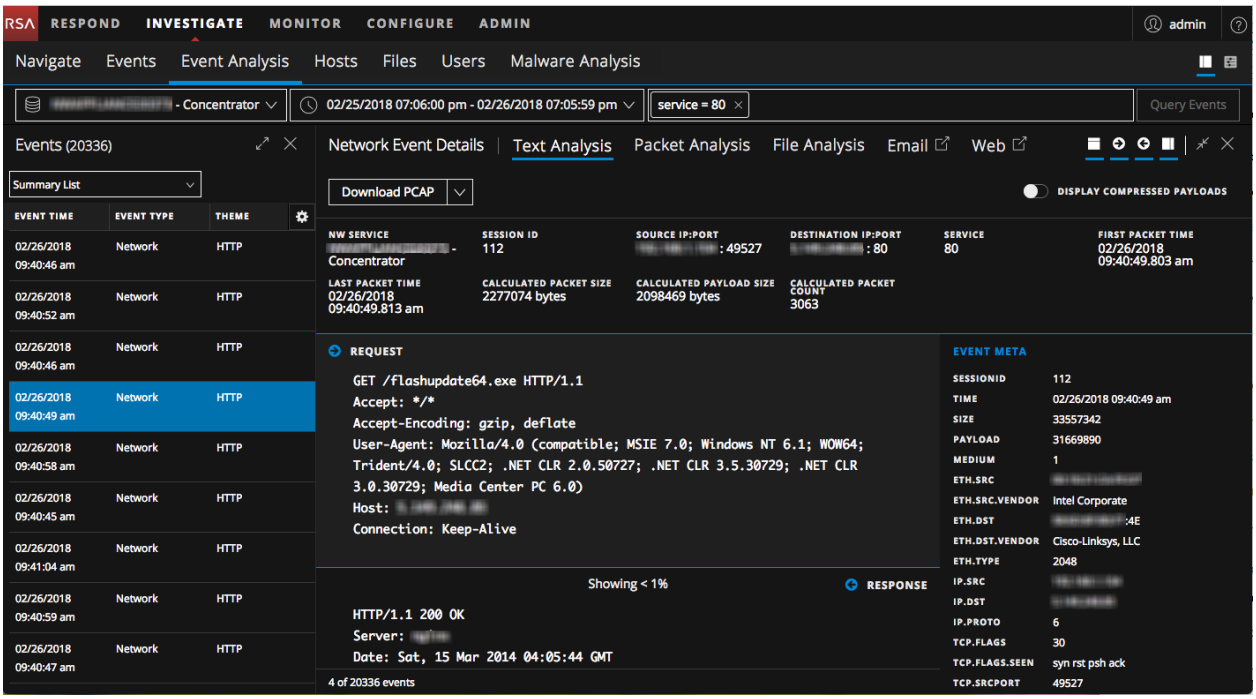
Para seleccionar el tipo de análisis para un evento, realice una de las siguientes acciones:

1. En la barra de herramientas de la **vista Análisis de eventos**, haga clic en el tipo de análisis.
2. En el menú desplegable, seleccione el tipo de análisis: **Análisis de archivos**, **Análisis de texto**, **Análisis de paquetes**, **Correo electrónico** (versión 11.1 y superior) o **Web** (versión 11.1 y superior).
   Si eligió **Análisis de archivos**, **Análisis de texto** o **Análisis de paquetes**, la vista se actualiza con el panel Análisis de paquetes, Análisis de archivos o Análisis de texto abierto.
   Si eligió **Correo electrónico** o **Web**, la reconstrucción de correo electrónico o web de la vista Eventos del evento único se abre en una pestaña nueva. Esta es la misma reconstrucción de una sesión de correo electrónico o web que se utiliza en la vista Eventos. La vista Eventos proporciona mayor funcionalidad cuando se ve una reconstrucción de correo electrónico o web, lo que le permite navegar por las páginas de los eventos de esa vista en lugar de ver un solo evento (consulte Reconstruir un evento).

Nota: El panel Análisis de paquetes solo está disponible para los eventos de red.

Abrir, cerrar y ajustar el tamaño de los paneles de la vista Análisis de eventos

La vista Análisis de eventos se abre con la Lista de eventos y ningún evento seleccionado o reconstruido. Cuando selecciona un evento, el panel Detalles del evento de red, Detalles del evento de registro o Detalles del evento de Endpoint se abre a la derecha. Inicialmente, el panel Detalles del evento de red, Detalles del evento de registro o Detalles del evento de Endpoint ocupa de forma predeterminada el 75 % del ancho de la ventana.



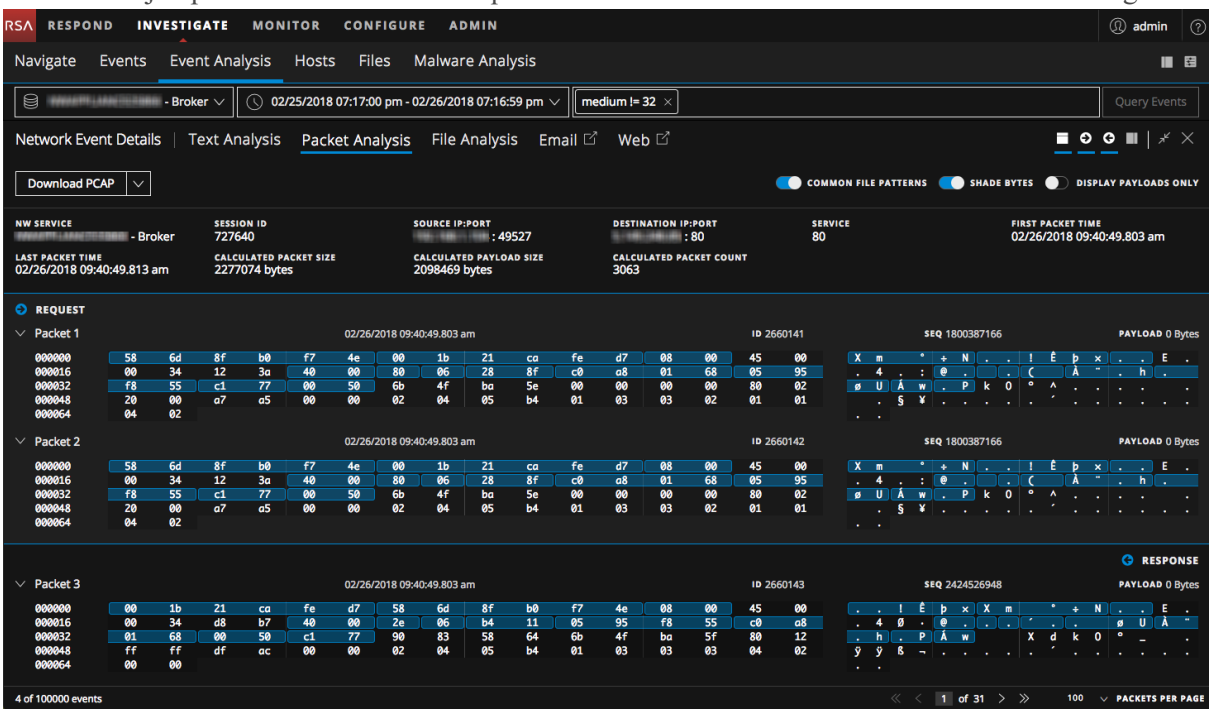
Puede ajustar la relación de tamaño de los dos paneles para mejorar la legibilidad mediante la expansión, la contracción o el cierre de uno de los paneles. Después de cerrar cualquiera de los paneles, puede volver a abrirlo. La relación que selecciona persiste hasta que la cambia o actualiza el navegador.

- Para volver a abrir el Panel Eventos, haga clic en ☐ en la esquina superior derecha.

Para optimizar la vista:

1. Para ajustar la relación de tamaño de los dos paneles, realice cualquiera de las siguientes acciones:
   a. Haga clic en ⤢ en la barra de herramientas del panel que desea expandir.
   b. Haga clic en ⤡ en la barra de herramientas del panel que desea contraer.
2. Para cerrar cualquiera de los paneles y restaurar el panel abierto a su ancho completo, haga clic en ✕.

Este es un ejemplo de la reconstrucción que se muestra a todo el ancho de la ventana del navegador.



3. Para volver a abrir el Panel Eventos después del cierre, haga clic en ☐ en la esquina superior derecha de la Vista Navegar.
   El Panel Eventos se abre en el último estado (25 %:75 % o 50 %:50 %).
4. Para volver a abrir el panel Detalles de eventos, haga clic en un evento en el Panel Eventos.

Seleccionar un grupo de columnas y columnas en Análisis de eventos

En la versión 11.1 y superior, puede usar grupos de columnas incorporados o personalizados en el panel Eventos. Los grupos de columnas se crean y se administran en la vista Eventos (consulte Administrar grupos de columnas en la vista Eventos); estos grupos se reflejan en la vista Análisis de eventos. Cuando cambia el grupo de columnas, los cambios que realiza en un grupo de columnas son solo para la vista actual. Cuando sale de la vista Análisis de eventos y regresa a esta, los cambios en las columnas no persisten en el panel Eventos.

Estos son los grupos de columnas incorporados.

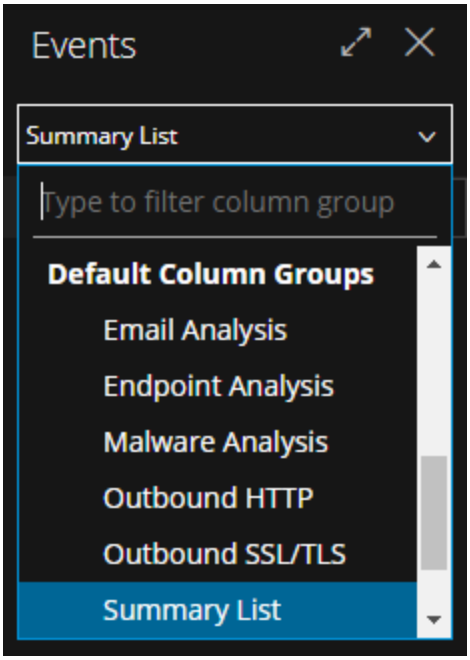
- **Análisis de correo electrónico**: Incluye claves de metadatos que son útiles para investigar metadatos relacionados con el correo electrónico.
- **Análisis de terminales**: Incluye claves de metadatos que son útiles para investigar metadatos relacionados con terminales.
- **Malware Analysis**: Incluye claves de metadatos que son útiles para investigar metadatos relacionados con malware.
- **HTTP de salida**: Incluye claves de metadatos que son útiles para investigar metadatos relacionados con HTTP de salida.

- **Protocolos SSL/TLS de salida**: Incluye claves de metadatos que son útiles para investigar metadatos relacionados con el análisis de SSL/TLS de salida.
- **Lista de resumen**: Incluye claves de metadatos que son útiles en una investigación general. **Este es el grupo de columnas predeterminado.**
- **Análisis de amenazas**: Incluye claves de metadatos que marcan amenazas potenciales en el conjunto de datos.
- **Análisis web**: Incluye claves de metadatos que marcan anomalías en el tráfico web.

Un grupo de columnas puede contener más columnas de las que se ven sin desplazarse hacia la derecha. En la versión 11.1, puede seleccionar las columnas que aparecen en la vista Análisis de eventos. El orden de las columnas refleja el orden en la vista Eventos del grupo de columnas predeterminado. De forma predeterminada, cuando se selecciona un grupo de columnas, se muestran las primeras 15 columnas. Para una visualización optimizada, se recomienda ver solo 15 columnas a la vez; sin embargo, puede seleccionar columnas adicionales para ver y quitar las columnas que se muestran.

Para seleccionar un grupo de columnas:

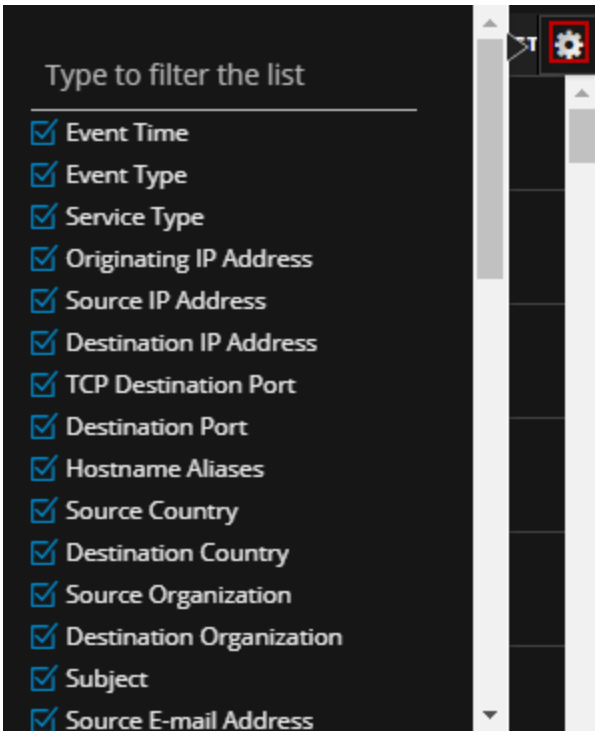
1. En el menú desplegable junto a Eventos, seleccione un grupo de columnas (por ejemplo, **Lista de resumen**). También puede comenzar a escribir el nombre del grupo de columnas y seleccionar un grupo a medida que estos aparecen en el menú desplegable.



   El panel Eventos muestra datos en las columnas que pertenecen al grupo de columnas seleccionado.

Para seleccionar columnas que desea ver:

1. Mientras trabaja en la vista Análisis de eventos, con un grupo de columnas seleccionado, haga clic en ⚙ para mostrar el selector de columnas.



2. Seleccione las claves de metadatos o ingrese el nombre de una clave de metadatos que desea mostrar en columnas adicionales.
3. Si no desea mostrar una clave de metadatos en una columna, deselecciónela.
   Los datos se vuelven a mostrar en función de las columnas seleccionadas.

Ajustar la visualización de las solicitudes y las respuestas

Para los tipos de evento que incluyen solicitudes y respuestas, puede realizar varios ajustes.

Nota: Si el tipo de análisis no tiene solicitudes y respuestas, la opción no se puede seleccionar. El panel Análisis de archivos es un ejemplo de un tipo de reconstrucción sin solicitudes ni respuestas. Un evento de registro reconstruido en la vista de texto es otro ejemplo.

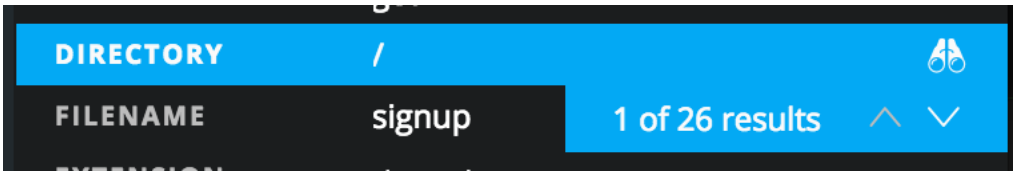
Para seleccionar qué lado de la conversación desea mostrar (Solicitud, Respuesta o ambos), haga clic en uno o en ambos iconos de dirección ( ). La reconstrucción se actualiza con la información seleccionada.

Nota: Si no ve ningún dato, es posible que haya deseleccionado tanto la Solicitud y como la Respuesta. Debe seleccionar una de las dos para ver los datos.

Ver los metadatos de un evento

Cuando se examinan eventos en los paneles Análisis de texto, Análisis de paquetes o Análisis de archivos, puede hacer clic en para mostrar los metadatos asociados en un panel adyacente, el panel Metadatos de eventos.

Cuando se observan los paneles Análisis de texto y Metadatos de eventos y se coloca el puntero sobre los pares de claves de metadatos/valores de metadatos, se muestran unos binoculares si el valor de metadatos se puede buscar en el texto crudo. Este es un ejemplo del ícono de binoculares que se muestra cuando se coloca el puntero sobre el par de clave de metadatos/valor de metadatos **Directorio** y /.



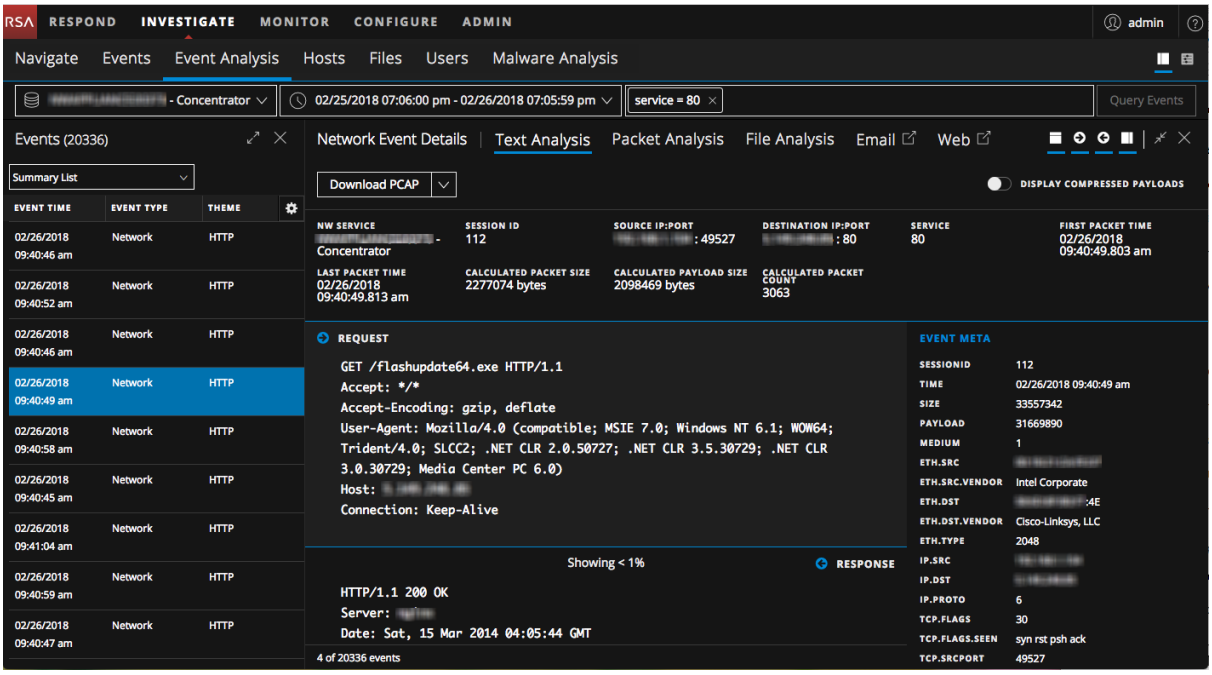
Cuando se hace clic en el ícono, se activa una búsqueda del par de clave de metadatos/valor de metadatos (que no distingue mayúsculas de minúsculas) en el panel Análisis de texto y se resalta cada instancia. En el Panel Metadatos de eventos, la fila resaltada muestra un conteo de los resultados y una barra de desplazamiento que puede utilizar para buscar rápidamente cada resultado en el panel Análisis de texto. Aparece resaltada cada una de las ubicaciones de los datos que activaron la generación de la clave de metadatos, y puede avanzar para ver la siguiente y retroceder para ver la anterior.

Solo se pueden buscar en el texto crudo las claves de metadatos que tienen valores pertinentes. Puede buscar solo una clave de metadatos por vez. Si el valor está oculto debido al truncamiento de una entrada de texto con más de 3,000 caracteres, la entrada de texto se expande para revelar el valor de metadatos encontrado.

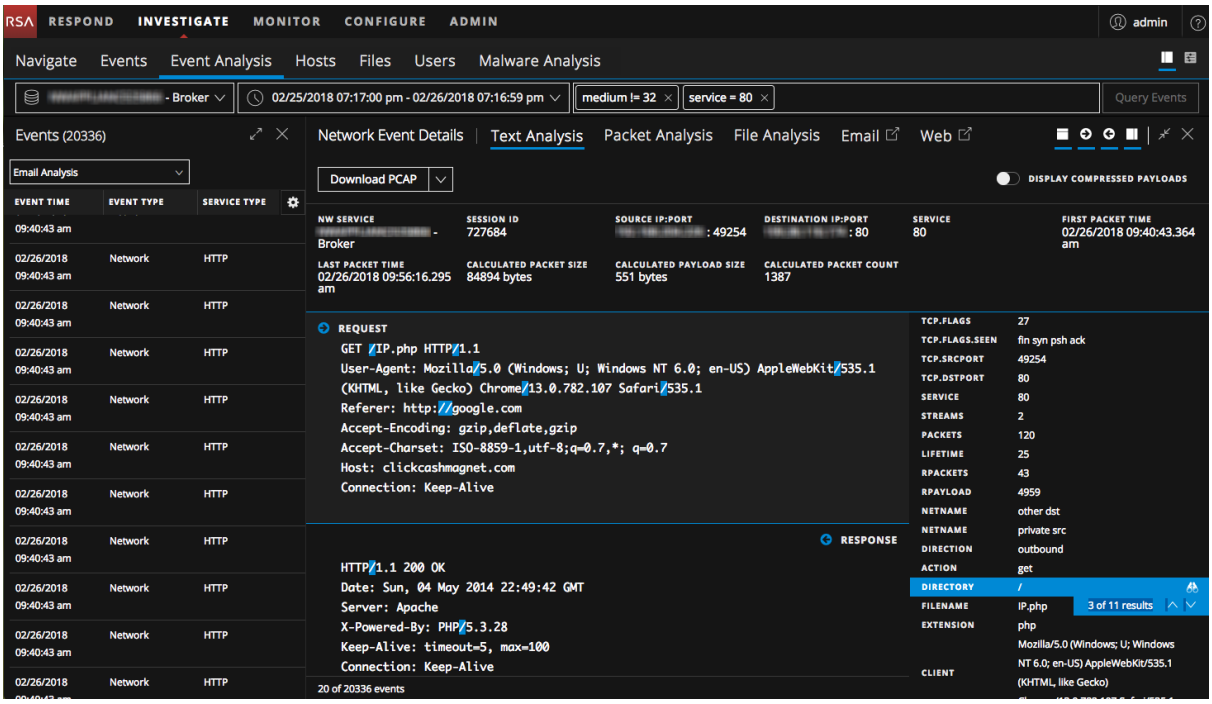
Cuando se hace clic en el mismo par de clave de metadatos/valor de metadatos o en otro par en el Panel Metadatos de eventos, el resaltado se quita del texto crudo. El resaltado también se quita si cierra el Panel Metadatos de eventos.

Para buscar en el texto crudo los valores de metadatos que activaron una clave de metadatos:

1. Abra un evento de red en el panel Análisis de texto.



2. En la barra de herramientas, haga clic en  para abrir el Panel Metadatos de eventos. A medida que pasa el cursor sobre los pares de claves de metadatos:valores de metadatos en la lista, un icono de binoculares identifica los valores que se pueden buscar en el panel Análisis de texto.
3. Para buscar el valor en el texto crudo, haga clic en una fila que tenga el ícono de binoculares, lo cual indica que permite realizar búsquedas.
   Si en el texto no hay ninguna aparición pertinente del valor, el valor que está buscando se resalta en el Panel Metadatos de eventos y no se resalta nada en el panel Análisis de texto.
   Si se encuentra una o más instancias pertinentes del valor en el panel Análisis de texto, se resalta cada aparición. El valor que está buscando se resalta en el Panel Metadatos de eventos y la barra de desplazamiento está visible.



4. Para quitar el resaltado, cierre el Panel Metadatos de eventos, haga clic en el mismo par de clave de metadatos/valor de metadatos en el Panel Metadatos de eventos o haga clic en otro par en el Panel Metadatos de eventos.
   El resaltado se quita del texto crudo.

Mostrar u ocultar el encabezado del evento

Para ocultar el encabezado del evento en los paneles Análisis de paquetes, Análisis de texto o Análisis de archivos y dejar más espacio vertical para los datos, haga clic en  .

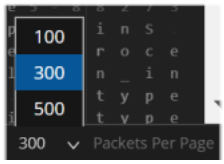
Navegar por páginas de eventos en los paneles Análisis de paquetes y Análisis de texto

Los controles de paginación permiten una mayor flexibilidad en la paginación a través de una lista de paquetes o texto. En el panel Análisis de paquetes, puede seleccionar la cantidad de paquetes que se muestran por página y la selección se guarda de un inicio de sesión a otro en la aplicación NetWitness. Cuando un control no está disponible, este aparece atenuado; por ejemplo, mientras ve la página 1, los controles < y << aparecen atenuados.

Nota: Para el Análisis de paquetes, los controles de paginación están disponibles en la versión 11.1 y superior. Para el Análisis de texto, los controles de paginación están disponibles en la versión 11.2 y superior.

Para utilizar los controles de paginación:

1. (Únicamente Análisis de paquetes) Con un evento abierto en la vista Análisis de eventos, haga clic en la actual cantidad de paquetes por página (**100**, **300** o **500**) y seleccione la nueva cantidad de paquetes por página en el menú desplegable.

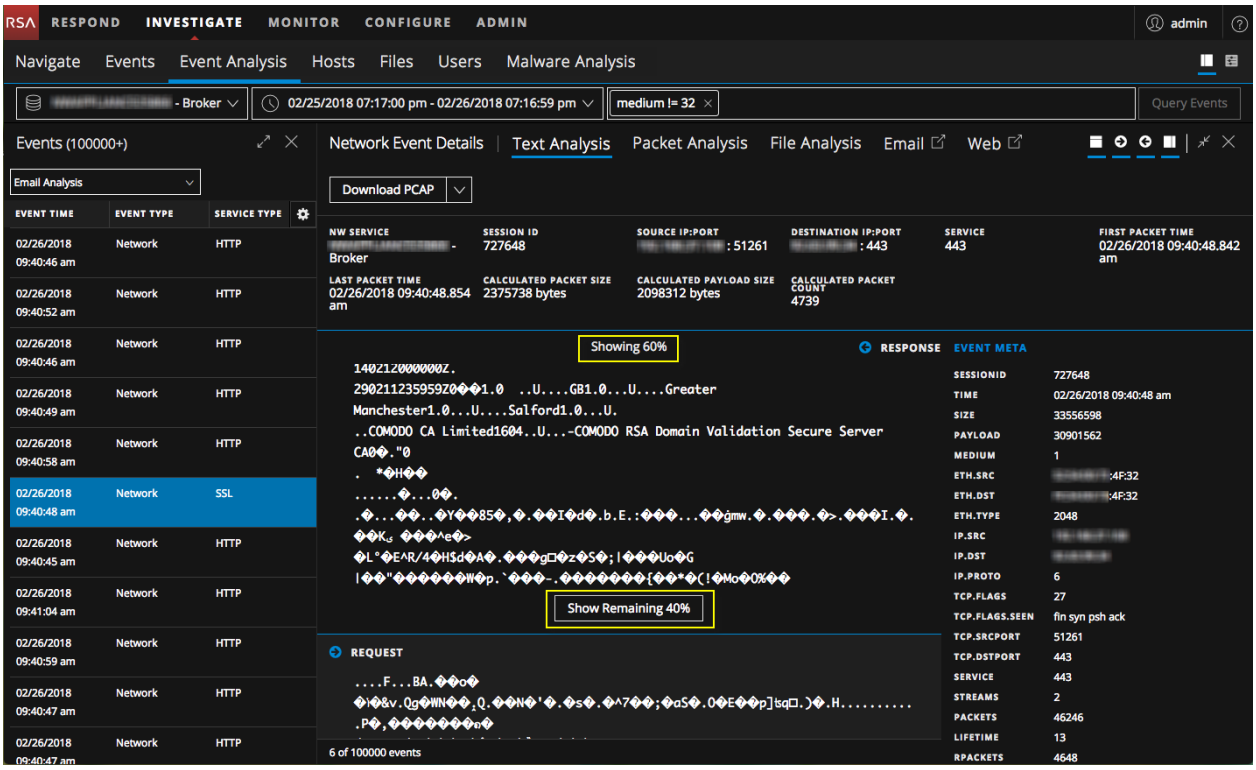


2. Para ir a páginas siguientes o anteriores, use los iconos de control de páginas:
   Haga clic en > para ir a la página siguiente.
   Haga clic en >> para ir a la última página.
   Haga clic en < para ir a la página anterior.
   Haga clic en << para ir a la primera página.
3. (Únicamente Análisis de paquetes) Para ir a una página específica, escriba un número de página en el campo de número de página  .

Nota: Cuando esté en el panel Análisis de texto, debe navegar manualmente a la última página antes de que el icono de control de la última página esté disponible.

Expandir las entradas de texto truncadas en el panel Análisis de texto

Una reconstrucción de un evento de red en el panel Análisis de texto puede incluir solicitudes y respuestas de varios cientos de miles de caracteres, y el desplazamiento a través de una entrada larga de más de 6,000 caracteres que no son de interés puede ser una pérdida de tiempo. Con el fin de mejorar la experiencia para los analistas, todas las entradas de texto que tienen más de 6,000 caracteres se truncan y solo muestran los primeros 2,000. En este ejemplo se muestra una entrada que tiene más de 2,000 caracteres y un mensaje en el encabezado indica el porcentaje del total de caracteres que se presenta.



Puede ver que se muestra el 60 % de los caracteres (los primeros 2,000). Haga clic en **Mostrar 40 % restante** para visualizar el resto de la entrada.

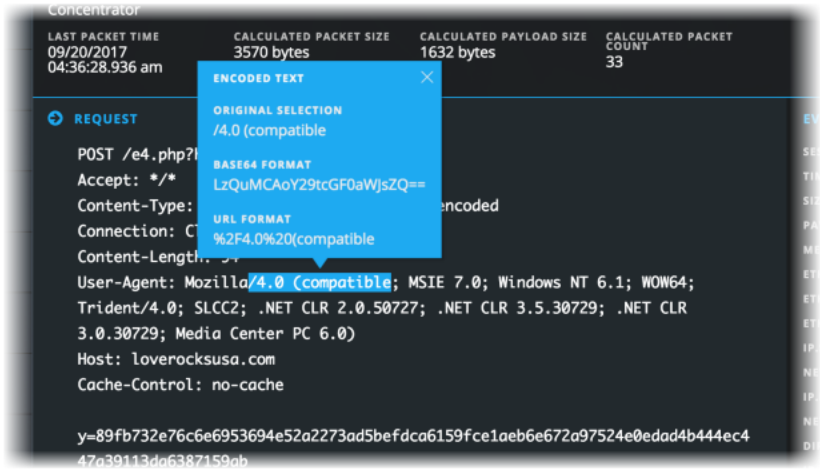
Si busca metadatos vistos en el Panel Metadatos de eventos mientras el texto está truncado en el panel Análisis de texto, se busca en el texto truncado. Si los metadatos existen dentro del texto oculto, la entrada de texto se expande para mostrar el texto con los metadatos encontrados.

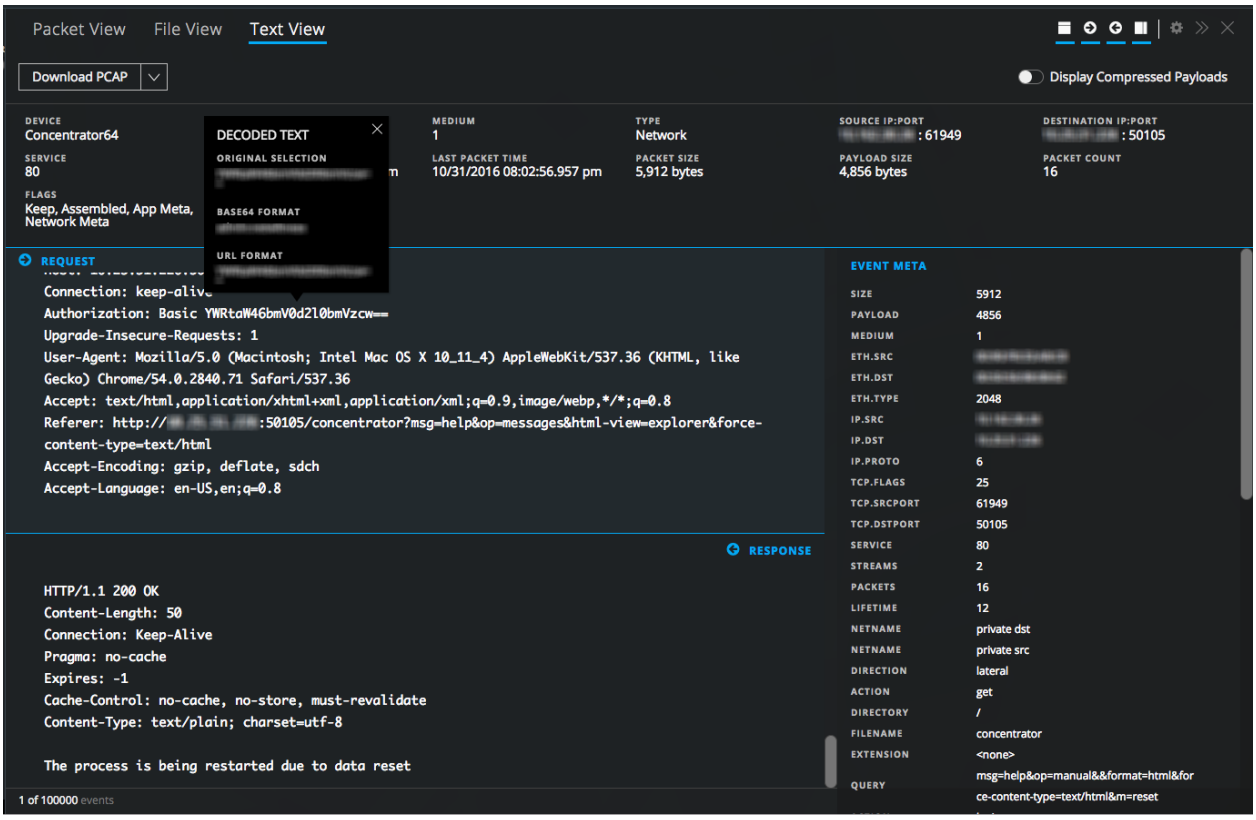
Realizar la codificación y la decodificación de URL y Base64 en el panel Análisis de texto

Si una sesión de red que se reconstruye en el panel Análisis de texto contiene cadenas codificadas en Base64 o URL, puede decodificarlas para comprender mejor la sesión. Si la sesión contiene cadenas decodificadas para Base64 o URL, puede ver una cadena en su forma codificada a fin de buscar instancias adicionales del texto codificado en otras sesiones.

Cuando observa una sesión de red que contiene texto codificado en el panel Análisis de texto, puede seleccionar un subconjunto del texto dentro de una única Solicitud o Respuesta para verlo en su forma codificada o decodificada. Según el contenido que se carga en el Decoder, puede haber metadatos adicionales que describan la inclusión de datos codificados en Base64 o URL dentro de la sesión.

Los siguientes son ejemplos de un cuadro activado con el puntero que muestra la codificación URL y texto codificado en Base64.

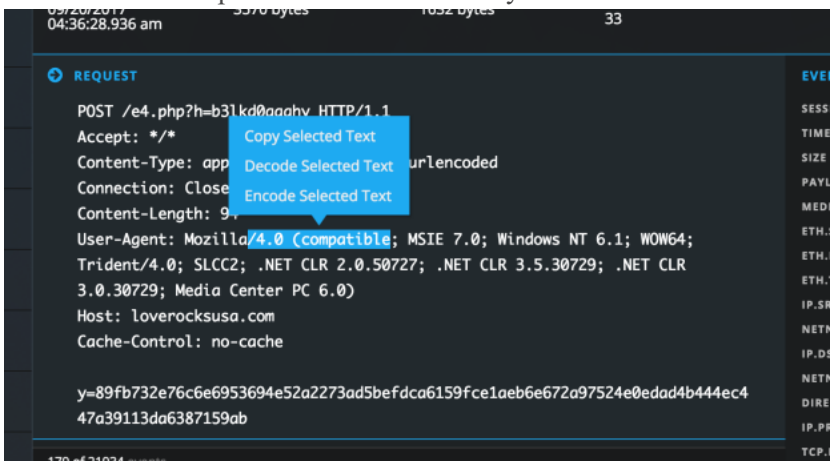




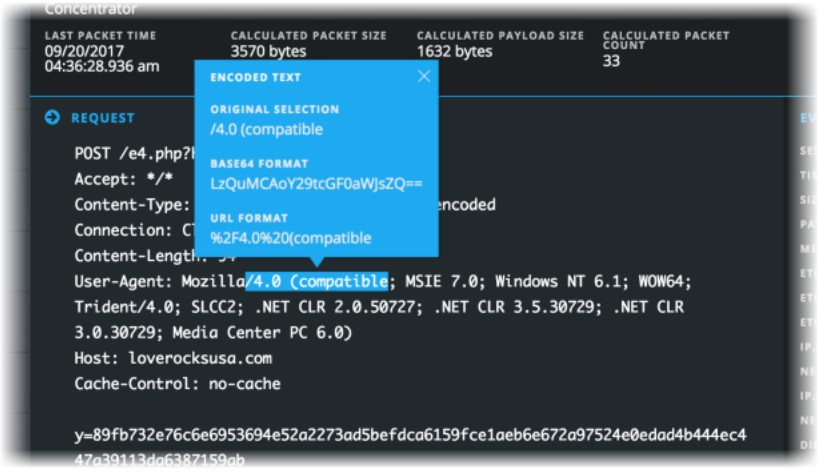
Para realizar la codificación y la decodificación en el panel Análisis de texto:

1. En la **vista Análisis de eventos**, vaya al panel Análisis de texto de una sesión que incluya contenido codificado o decodificado.
2. Si desea ver parte del texto decodificado en su forma codificada, arrastre para seleccionar el texto dentro de una única Solicitud o Respuesta.

Un menú ofrece opciones de codificación y decodificación.



3. Haga clic en **Codificar el texto seleccionado.**
   El texto codificado se muestra en un cuadro activado con el puntero, el cual permanece en su lugar hasta que usted hace clic en ■, selecciona otro texto en el panel Análisis de texto, cierra el Panel Eventos, selecciona otro evento para su reconstrucción o cambia a otra vista de reconstrucción.



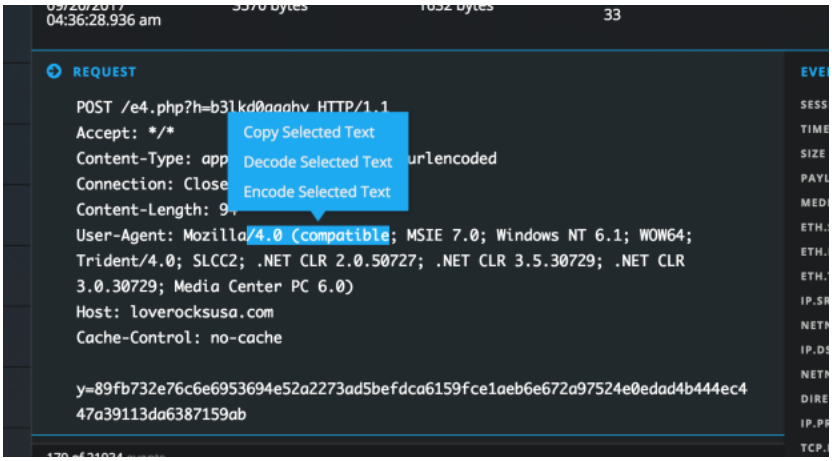
   Cuando se selecciona un texto más largo, el cuadro activado con el puntero es desplazable y lo suficientemente grande para mostrar todo el texto seleccionado, así como el texto decodificado.

4. Si la sesión contiene texto codificado que desea ver en su forma decodificada, arrastre para seleccionar el texto dentro de una única Solicitud o Respuesta.
   Un menú ofrece opciones de codificación y decodificación.

5. Haga clic en **Decodificar el texto seleccionado.**
   El texto decodificado se muestra en un cuadro activado con el puntero, el cual permanece en su lugar hasta que usted hace clic en ■, selecciona otro texto en el panel Análisis de texto, cierra el Panel Eventos, selecciona otro evento para su reconstrucción o cambia a otra vista de reconstrucción.

6. Si desea copiar parte del texto de la reconstrucción del texto, realice una de las siguientes acciones:

   a. Arrastre para seleccionar parte del texto, haga clic con el botón secundario y seleccione **Copiar texto seleccionado** en el menú.



b. Arrastre para seleccionar parte del texto y, a continuación, seleccione **Decodificar el texto seleccionado** o **Codificar el texto seleccionado**. Dentro del cuadro activado con el puntero, seleccione el texto que desee y presione **Ctrl+C**.
El texto seleccionado se copia al portapapeles y queda disponible para pegarlo en una consulta.

7. Cuando finalice, haga clic en ■ para cerrar el cuadro activado con el puntero.

Ver texto descomprimido de una sesión de red HTTP en el panel Análisis de texto

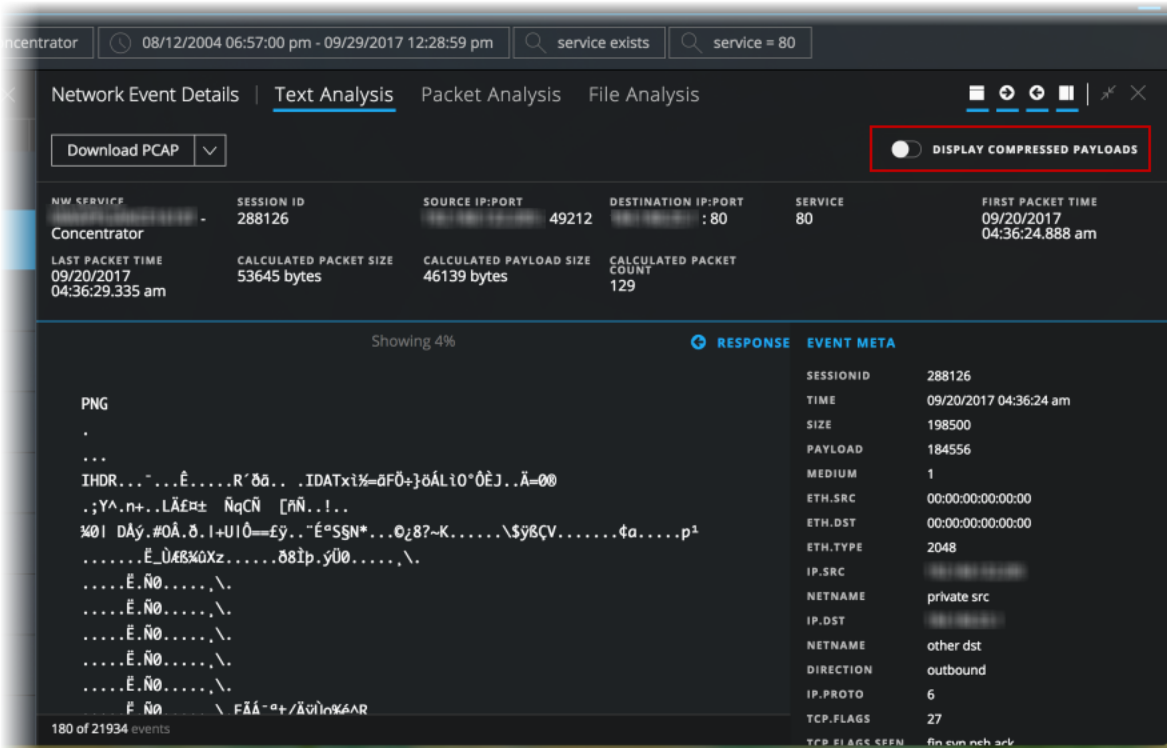
Cuando el contenido de una sesión de red HTTP está comprimido y usted ve el panel Análisis de texto, NetWitness Platform muestra el contenido descomprimido de forma predeterminada. Esto permite determinar si hay patrones y ver los caracteres legibles. Puede alternar entre una vista comprimida y descomprimida del texto comprimido.

Nota: El texto descomprimido no está disponible para el panel Análisis de paquetes, el panel Análisis de archivos, las sesiones de red no HTTP y los datos del registro.

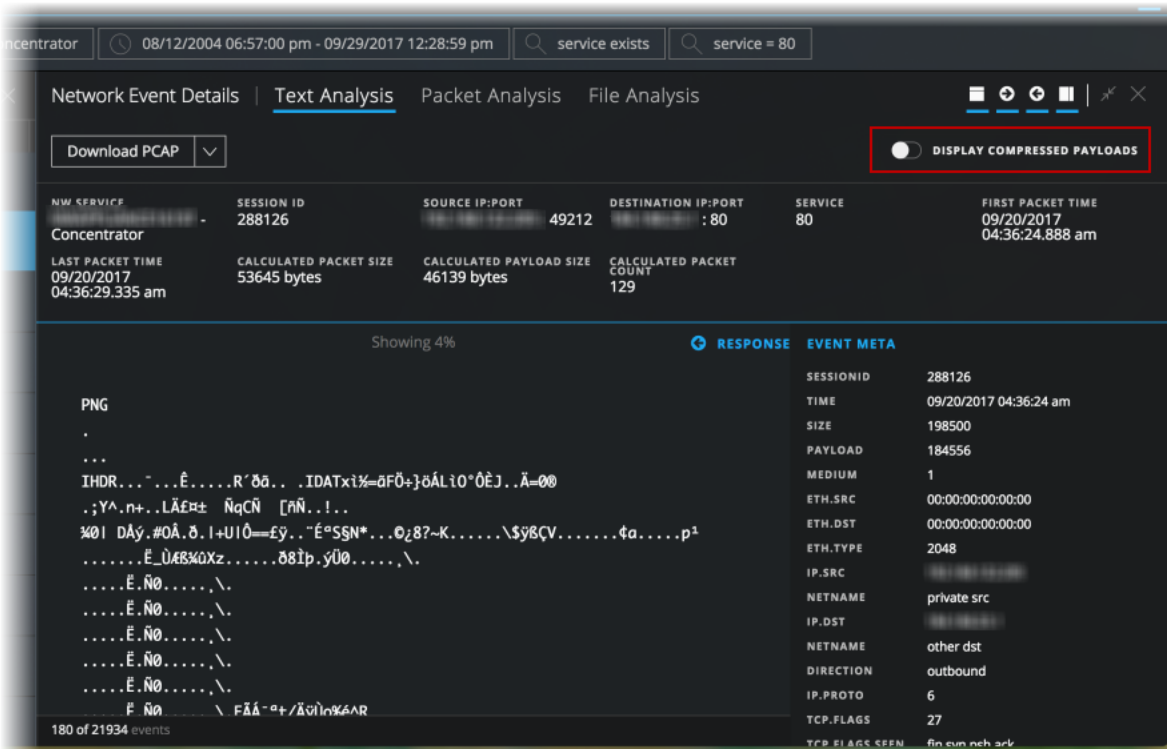
La alternancia entre el texto comprimido y descomprimido solo se muestra en el panel Análisis de texto y se habilita solo si hay contenido de texto comprimido.

Para ver el texto descomprimido:

1. Abra el panel Análisis de texto de una sesión HTTP que contenga contenido comprimido.
De forma predeterminada, la sesión se reconstruye con el texto descomprimido y sobre la reconstrucción aparece el switch de alternancia **Mostrar cargas útiles comprimidas**.



2. Para ver el mismo texto en su forma comprimida, haga clic en el switch de alternancia.
   La vista cambia de modo que el texto comprimido ya no es legible y el switch indica que la opción Mostrar paquetes comprimidos está activada.



3. Para volver a la vista de texto descomprimido, vuelva a hacer clic en el switch.

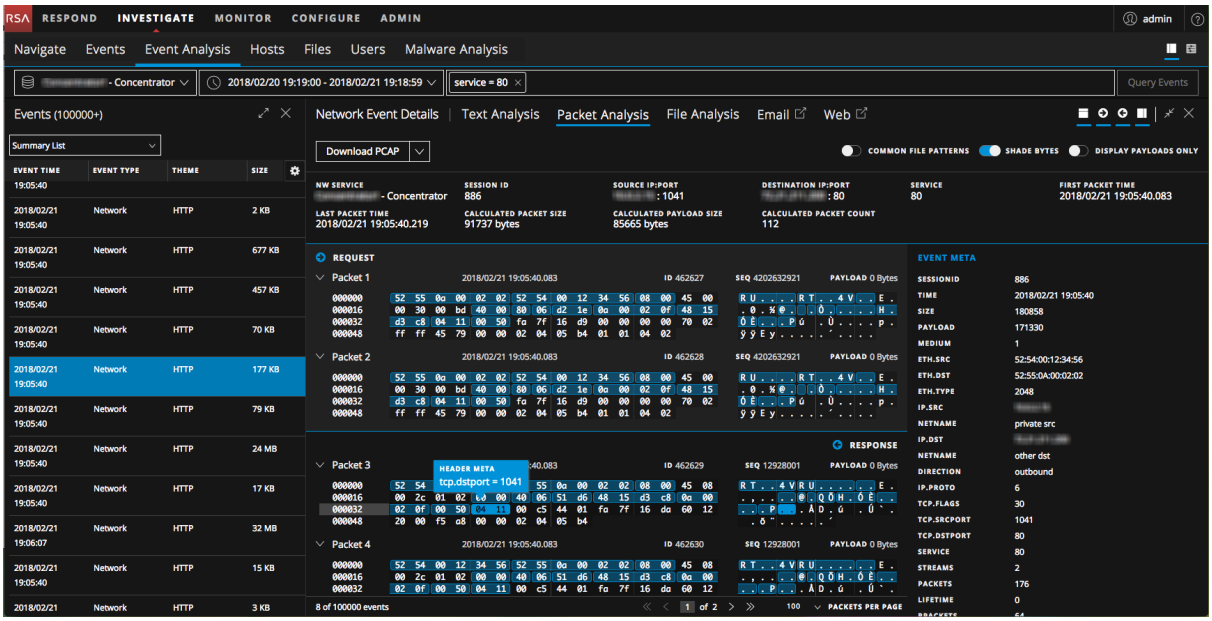
Usar la opción Solo carga útil del panel Análisis de paquetes de una sesión de red

Cuando observa una reconstrucción de una sesión de red en el panel Análisis de paquetes, puede optar por ver solo la carga útil principal de cada paquete. De forma predeterminada, se muestran los bytes del encabezado y el pie de página de cada paquete. Puede ocultarlos, para lo cual debe hacer clic en el switch de alternancia Mostrar solo cargas útiles. Si observa solo los bytes de carga útil, puede volver a la configuración predeterminada mediante el ajuste del switch de alternancia Mostrar solo cargas útiles en activado. Esta configuración persiste hasta que la cambia o actualiza el navegador.

- Con la opción Mostrar solo cargas útiles desactivada, se muestra la cantidad de paquetes, el encabezado de los paquetes, el pie de página de los paquetes y la carga útil.
- Con la opción Mostrar solo cargas útiles activada, no se muestra ningún byte de encabezado y pie de página de los paquetes. Solo se muestra el contenido de los paquetes de 16 bytes hexadecimales por línea y el código ASCII correspondiente por línea.

Para ver únicamente la carga útil:

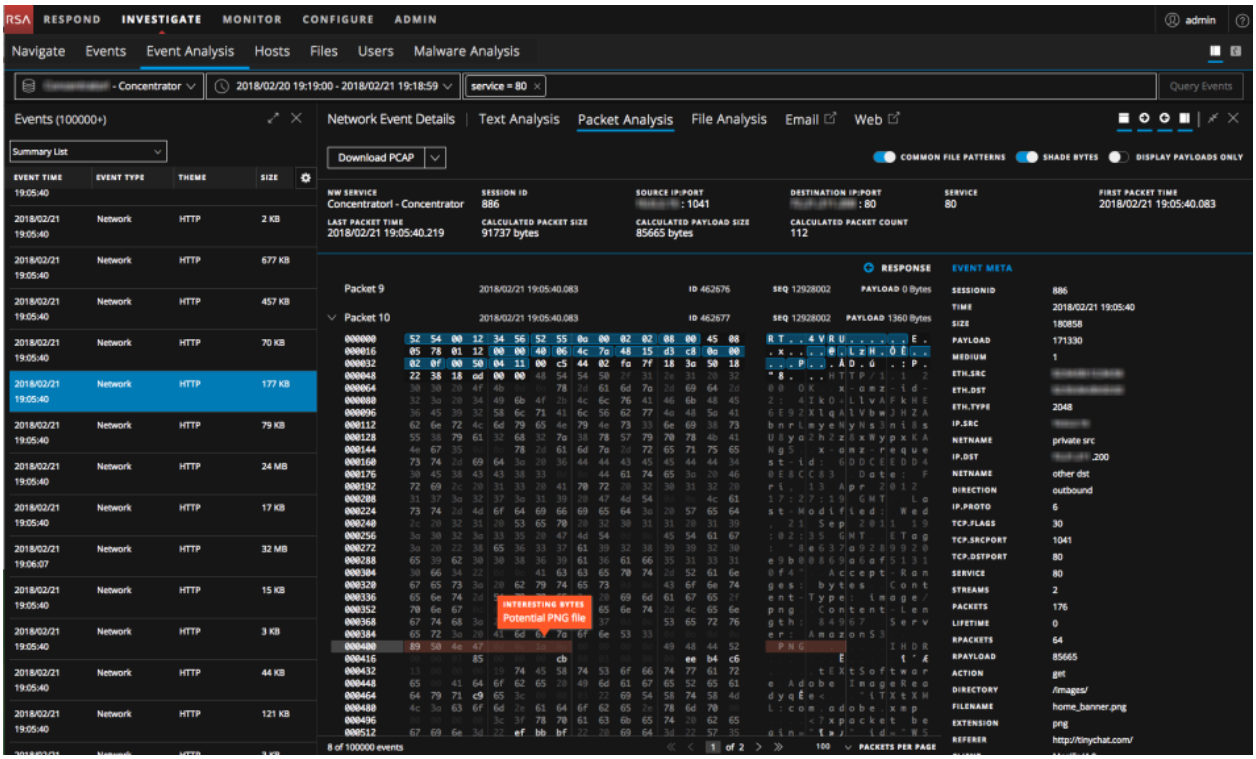
1. En la vista **Análisis de eventos**, vaya al panel Análisis de paquetes de una sesión de red.
   De forma predeterminada, la sesión se reconstruye y muestra el encabezado, el pie de página y la carga útil del paquete.



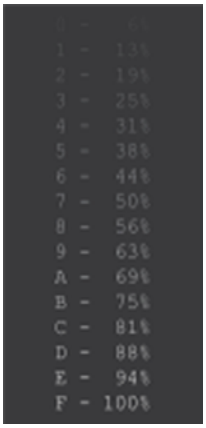
2. Para cambiar la vista con el fin de mostrar solo la carga útil de cada paquete, haga clic en el switch de alternancia **Mostrar solo cargas útiles**.
   La vista cambia de modo que solamente la carga útil esté visible y los paquetes contiguos del mismo lado se concatenan para que la carga útil sea más legible y comprensible.

Ver bytes resaltados en el panel Análisis de paquetes

Cuando abre por primera vez una reconstrucción en el panel Análisis de paquetes, los bytes significativos del encabezado de cada paquete se resaltan en azul y los bytes de carga útil se diferencian mediante sombreado que ayuda a comprender el contenido del paquete. En esta figura se muestra el Análisis de paquetes predeterminado con resaltado y sombreado de bytes.



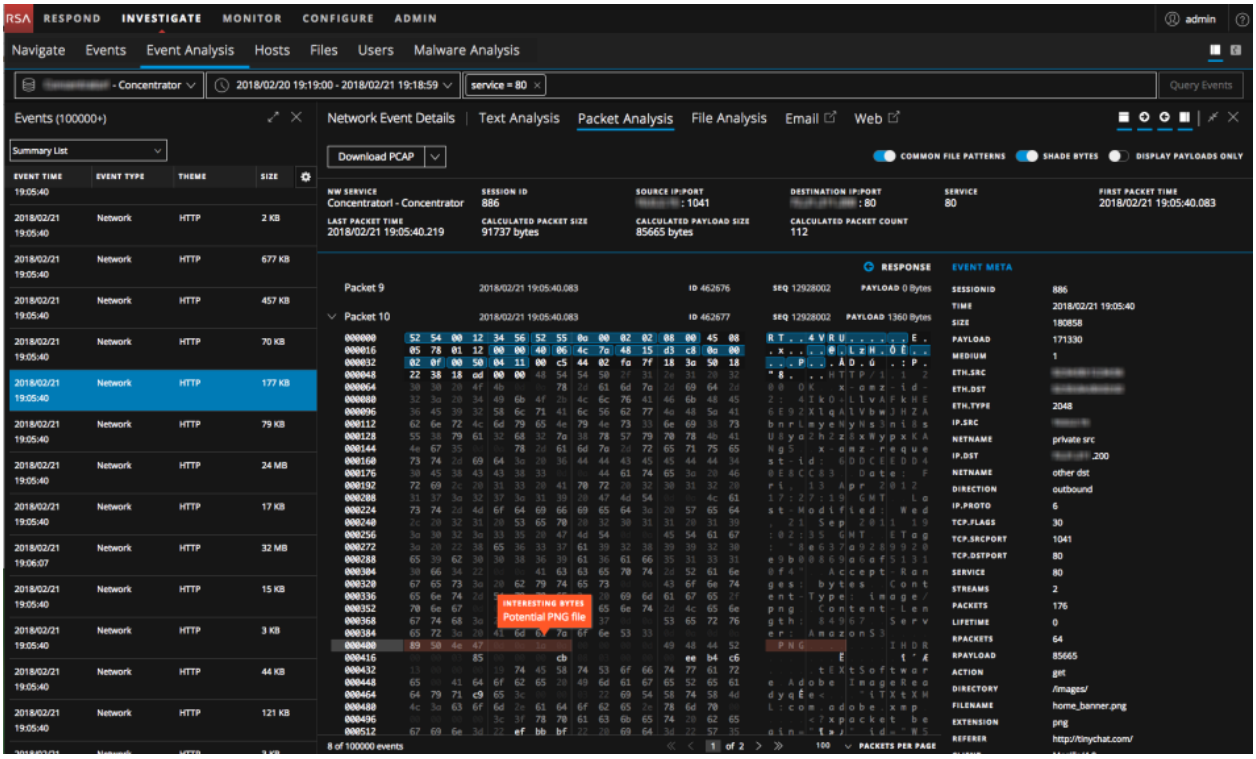
La opción Sombrear bytes agrega sombreado para identificar los distintos bytes hexadecimales (de 00 a FF) mediante grados de resaltado. Los bytes cerca del rango inferior son más transparentes y los más cercanos a 255 son más opacos. Los bytes hexadecimales y ASCII aparecen sombreados. Este es un ejemplo del sombreado aplicado a cada byte hexadecimal.



El switch Sombrear bytes controla el sombreado de los bytes. Cuando activa o desactiva Sombrear bytes, la configuración persiste hasta que la cambia o actualiza el navegador.

Resaltar los tipos de archivo comunes en el panel Análisis de paquetes

En el panel Análisis de paquetes, los analistas pueden mostrar u ocultar el resaltado de ciertos tipos de archivo comunes en función de la firma de los archivos. Cuando la función Patrones de archivo comunes está activada, los bytes de número mágico en la firma del archivo se resaltan en la carga útil y usted puede colocar el cursor sobre el resaltado para ver el posible tipo de archivo. En este ejemplo, `89 50 4e 47` está resaltado en la carga útil hexadecimal y `PNG` está resaltado en la carga útil ASCII. Cuando coloca el cursor sobre los bytes resaltados, un cuadro muestra el posible tipo de archivo asociado con el número mágico.



Estos son los tipos de archivo y los números mágicos correspondientes que se resaltan si están presentes en la carga útil:

Tipo de archivo	Firma hexadecimal	Codificación ASCII
Archivo ejecutable de DOS/Windows PE	4D 5A	MZ
Gráficos de red portátiles (PNG)	89 50 4E 47 0D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/Exif	45 78 69 66	Exif
GIF	47 49 46 38 37 61	GIF87a

Tipo de archivo	Firma hexadecimal	Codificación ASCII
GIF	47 49 46 38 39 61	GIF89a
Archivo ejecutable no portátil	5A 4D	ZM
BMP	42 4D	BM
PDF	25 50 44 46	%PDF
Documento de Office antiguo (doc, xls, ppt, msg y otros)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
Formatos de archivo ZIP y formatos basados en él, como JAR, ODF y OOXML	50 4B	PK..
Formato de archivo 7-Zip (7z)	37 7A BC AF 27 1C	7z¼¯'
Archivo de clase Java, binario multiarquitectura Mach-O	CA FE BA BE	Êþº¾
Postscript	25 21 50 53	%!PS
Script de shell de UNIX/Linux	23 21	#!
Archivos ejecutables en formato ejecutable y vinculable (ELF)	7F 45 4C 46	.ELF

Para ver las firmas de archivo comunes en el panel Análisis de paquetes:

1. Vaya al panel Análisis de paquetes y active la opción **Patrones de archivo comunes**.
   Si hay más de un elemento resaltado en la vista, se muestran todos.
2. Para ver el cuadro activado con el cursor, coloque el cursor sobre el elemento resaltado.

Buscar contexto adicional en la vista Análisis de eventos

La información de este tema se aplica a RSA NetWitness® Platform versión 11.2 y superior. En versiones anteriores, también puede buscar contexto adicional en la vista Navegar o en la vista Eventos, como se describe en Buscar contexto adicional en las vistas Navegar y Eventos.

En la vista Análisis de eventos, puede buscar detalles e inteligencia acerca de elementos asociados a un evento en Context Hub. Estos elementos, o entidades, son identificadores, por ejemplo, una dirección IP, un nombre de usuario, un nombre de host, un nombre de dominio, un nombre de archivo o un hash de archivo. Los datos de los orígenes configurados, como RSA NetWitness Endpoint, pueden ayudarlo a comprender lo que está sucediendo.

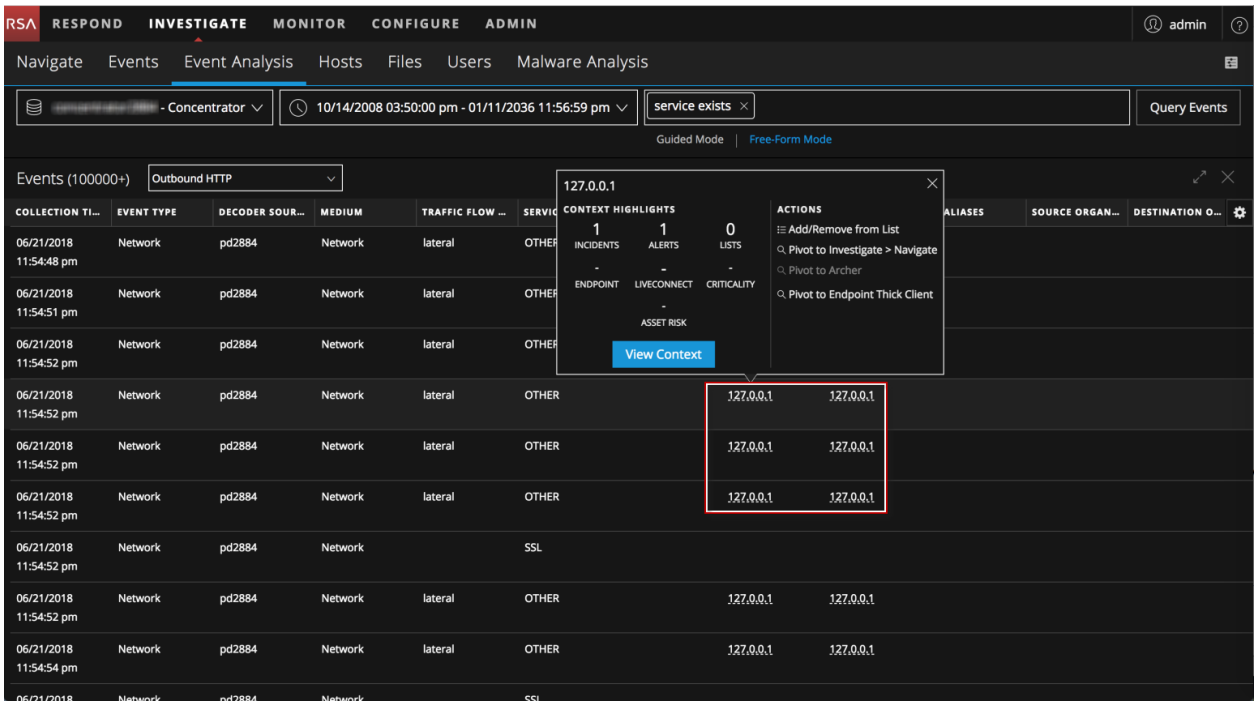
Nota: Para habilitar la visualización de información contextual, el administrador debe agregar el servicio Context Hub en RSA NetWitness Platform y configurar orígenes de datos para este servicio, como se describe en la *Guía de configuración de Context Hub*. Los analistas también necesitan una función que tenga el permiso `Context Lookup`, como se describe en "Permisos de funciones" y en "Administrar usuarios con funciones y permisos" en la *Guía de administración de usuarios y de la seguridad del sistema*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Context Hub es un servicio centralizado que agrega datos acerca de las entidades de varios orígenes de datos configurables. Estos datos pueden ampliar su investigación con contexto adicional más allá de los resultados inmediatos de una consulta específica. Por ejemplo, Context Hub puede indicar si una entidad determinada se ha mencionado en incidentes, alertas, feeds o publicaciones de inteligencia de comunidades.

En el panel Eventos, en el encabezado del evento o en el panel Metadatos de eventos, puede ver entidades subrayadas. Si una entidad está subrayada, NetWitness Platform está completando información acerca de ese tipo de entidad en Context Hub. Puede estar disponible información adicional sobre esa entidad en Context Hub.

Nota: Las entidades de Active Directory con información de contexto disponible no están subrayadas, pero es posible colocar el cursor sobre ellas para ver si hay información de contexto disponible.

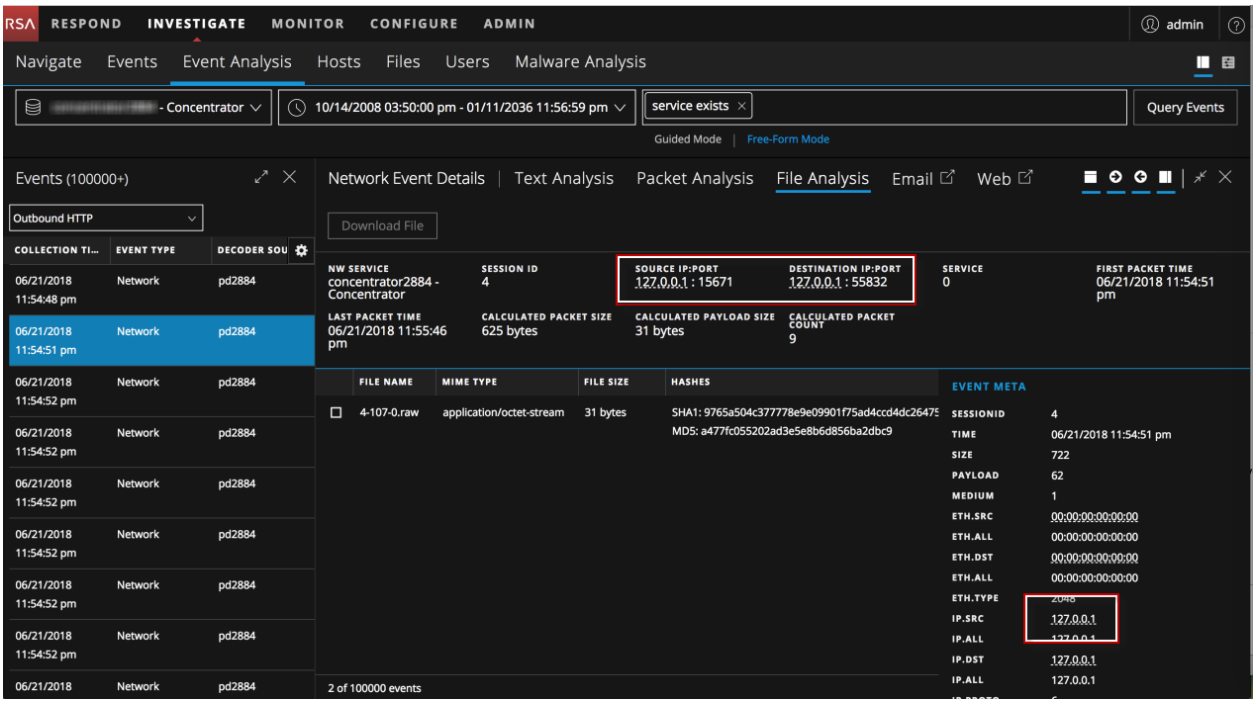
En la siguiente figura se muestran entidades subrayadas en el panel Eventos con el mensaje de globo de contexto abierto.



El mensaje de globo de contexto tiene dos secciones: Puntos destacados de contexto y Acciones.

- La información de la sección Puntos destacados de contexto lo ayuda a determinar las acciones que desea realizar. Puede mostrar datos relacionados de incidentes, alertas, listas, Endpoint, Live Connect, criticidad y riesgo de recurso. Según los datos, tal vez pueda hacer clic en estos elementos para obtener más información.
- En la sección Acciones se enumeran las acciones disponibles. En el ejemplo, están disponibles las opciones Agregar/eliminar de la lista, Cambiar a Investigate > Navegar, Cambiar a Archer y Cambiar a cliente grueso de Endpoint.

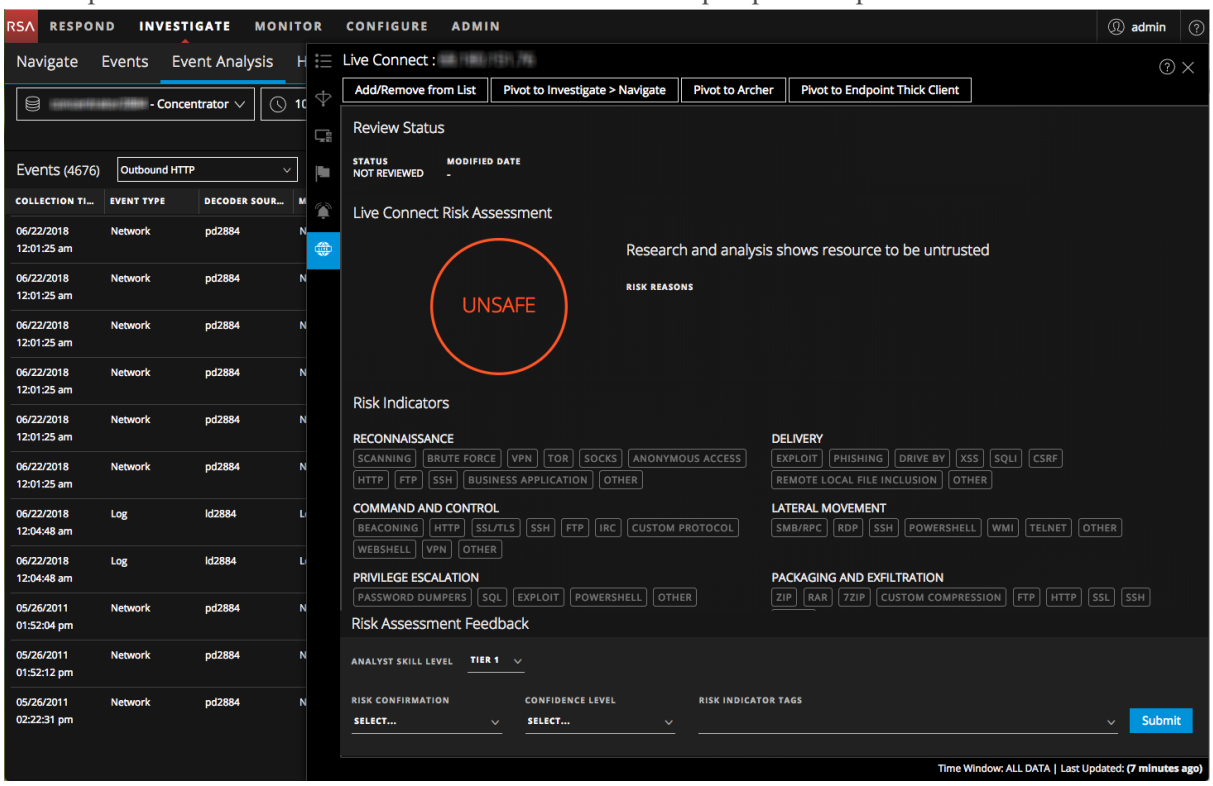
En la siguiente figura se muestran entidades subrayadas en el encabezado del evento y en el panel Metadatos de eventos.



Cuando se hace clic en Ver contexto en el mensaje de globo de contexto, Context Hub consulta la información pertinente en los orígenes de datos configurados y el panel Búsqueda de contexto se abre desde el lado derecho de la ventana del navegador. Este panel se completa con la información de Context Hub a medida que queda disponible. En el panel Búsqueda de contexto, puede ver y explorar orígenes de datos individuales para realizar una investigación más a fondo. Para obtener una descripción detallada de la información que se muestra para cada origen de datos en el panel Búsqueda de contexto, consulte Panel Búsqueda de contexto. También puede realizar cualquier acción disponible en la sección Acciones.

Para ver información en el panel Búsqueda de contexto de la vista Análisis de eventos:

1. Coloque el cursor sobre distintos valores de metadatos para ver los orígenes de datos en los que hay datos disponibles.
   Un mensaje de globo de contexto muestra una lista de los datos de contexto disponibles para el valor de metadatos seleccionado.
2. Haga clic en **Ver contexto** en el mensaje de globo de contexto para abrir el panel Búsqueda de contexto.
   El panel Búsqueda de contexto se abre desde el lado derecho de la ventana del navegador. Este panel se completa con la información de Context Hub a medida que queda disponible.



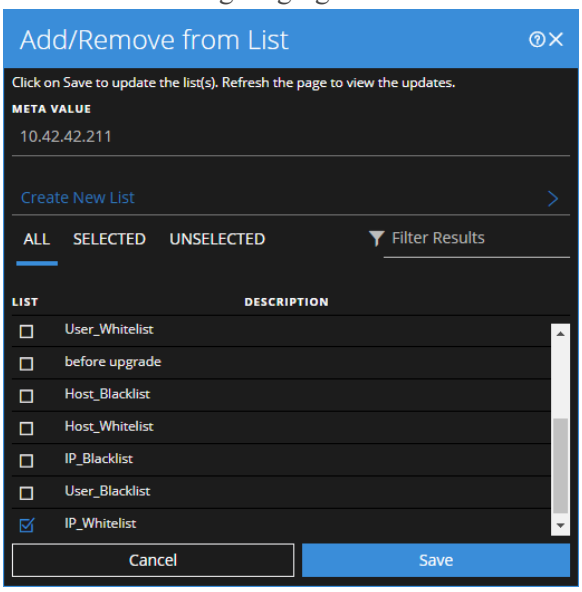
3. Para realizar acciones en una entidad, seleccione una de las acciones disponibles en el mensaje de globo de contexto: Agregar/eliminar de la lista, Cambiar a Investigate > Navegar, Cambiar a Archer y Cambiar a cliente grueso de Endpoint. Para obtener más información, consulte Cambiar a Investigate > Navegar, Cambiar a Archer, Cambiar a cliente grueso de NetWitness Endpoint y Agregar una entidad a una lista blanca.

> **Nota:** La acción Cambiar a Archer se deshabilita cuando no están disponibles datos de Archer o cuando el origen de datos de Archer no responde. Compruebe que la configuración de RSA Archer esté habilitada y configurada correctamente. Lo mismo sucede con la acción Cambiar a cliente grueso de NetWitness Endpoint; si la opción está deshabilitada, verifique que el cliente grueso de NetWitness Endpoint esté instalado y configurado correctamente.

Agregar una entidad a una lista blanca

Puede agregar cualquier entidad subrayada a una lista, como una lista blanca o una lista negra, desde un mensaje de globo de contexto. Por ejemplo, para reducir los falsos positivos, tal vez desee incluir en la lista blanca un dominio subrayado con el fin de excluirlo de las entidades relacionadas.

1. En el panel Eventos, en el encabezado del evento o en el panel Metadatos de eventos, coloque el cursor sobre la entidad subrayada que desee agregar a una lista de Context Hub. (Las entidades de Active Directory con datos de contexto también se pueden agregar, pero no se subrayan). Aparece un mensaje de globo de contexto que muestra las acciones disponibles.
2. En la sección **ACCIONES** del mensaje de globo, haga clic en **Agregar/eliminar de la lista**. El cuadro de diálogo Agregar/eliminar de la lista muestra las listas disponibles.



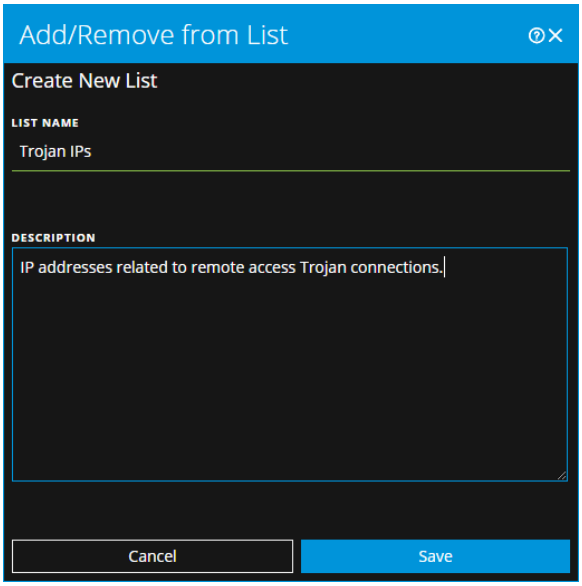
3. Seleccione una o más listas y haga clic en **Guardar**.
   La entidad se agrega a las listas seleccionadas. El Cuadro de diálogo Agregar/eliminar de la lista proporciona información adicional.

Crear una lista

Puede crear listas en Context Hub desde la vista Análisis de eventos. Además de usar listas para ingresar entidades en listas blancas y negras, puede usarlas para monitorear el comportamiento anormal en las entidades. Por ejemplo, para mejorar la visibilidad de una dirección IP y un dominio sospechosos que se están investigando, tal vez desee incluirlos en dos listas por separado. Una lista podría incluir dominios que posiblemente tengan relación con conexiones de comando y control, y la otra, direcciones IP relacionadas con conexiones de troyanos de acceso remoto. A continuación, puede identificar indicadores de riesgo mediante estas listas.

Para crear una lista en Context Hub:

1. En el panel Eventos, en el encabezado del evento o en el panel Metadatos de eventos, coloque el cursor sobre la entidad subrayada que desee agregar a una lista de Context Hub. (Las entidades de Active Directory con datos de contexto también se pueden agregar a una lista nueva, pero no se subrayan).
   Aparece un mensaje de globo de contexto que muestra las acciones disponibles.
2. En la sección **ACCIONES** del mensaje de globo, haga clic en **Agregar/eliminar de la lista**.
3. En el cuadro de diálogo Agregar/eliminar de la lista, haga clic en **Crear lista nueva**.



4. Escriba un **NOMBRE DE LISTA** único para la lista. El nombre de lista no distingue mayúsculas de minúsculas.
5. (Opcional) Escriba una **DESCRIPCIÓN** para la lista.
   Los analistas con los permisos adecuados también pueden exportar listas en formato CSV para enviarlas a otros analistas, quienes pueden realizar tareas adicionales de rastreo y análisis. En la *Guía de configuración de Context Hub* se proporciona información adicional.

Cambiar a Investigate > Navegar

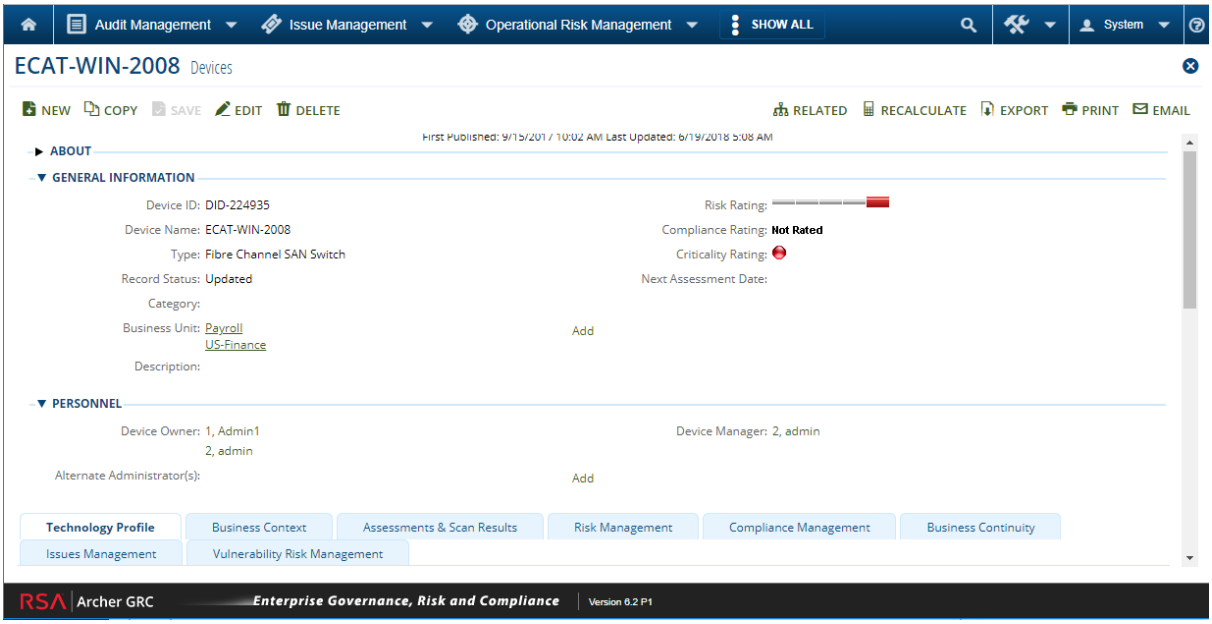
Si desea realizar una investigación más completa de una entidad, puede abrir la vista Navegar.

1. En el panel Eventos, en el encabezado del evento o en el panel Metadatos de eventos, coloque el cursor sobre cualquier entidad subrayada. (Las entidades de Active Directory con datos de contexto también se pueden investigar, pero no se subrayan).
2. En la sección **ACCIONES** del mensaje de globo, seleccione **Cambiar a Investigate > Navegar**.
   Se abre la vista Navegar, la que permite realizar una investigación más detallada. Para obtener más información, consulte Investigación de metadatos en la vista Navegar.

Cambiar a Archer

Para ver más detalles sobre el dispositivo en RSA Archer® Cyber Incident & Breach Response, puede cambiar a la página de detalles del dispositivo. Esta información se muestra solamente para la dirección IP, el host y la dirección Mac.

1. En el panel Eventos, en el encabezado del evento o en el panel Metadatos de eventos, coloque el cursor sobre cualquier entidad subrayada (dirección IP, host y dirección Mac).
2. En la sección **ACCIONES** del mensaje de globo de contexto, seleccione **Cambiar a Archer**.
3. La página de detalles del dispositivo en **Incidente cibernético y respuesta ante vulneración de RSA Archer** se abre si inició sesión en la aplicación; de lo contrario, se muestra la pantalla de conexión.



Nota: El vínculo Cambiar a Archer se deshabilita cuando no están disponibles datos de Archer o cuando el origen de datos de Archer no responde. Compruebe que la configuración de RSA Archer esté habilitada y configurada correctamente.

Para obtener más información, consulte la *Guía de integración de Archer*.

Cambiar a cliente grueso de NetWitness Endpoint

Si la aplicación del cliente grueso de NetWitness Endpoint está instalada, puede iniciarla mediante el mensaje de globo de contexto. Desde allí, puede investigar más a fondo una dirección IP, una dirección MAC o un host sospechosos.

1. En el panel Eventos, en el encabezado del evento o en el panel Metadatos de eventos, coloque el cursor sobre cualquier entidad subrayada.
2. En la sección **ACCIONES** del mensaje de globo, seleccione **Cambiar a cliente grueso de Endpoint**.
   La aplicación del cliente grueso de NetWitness Endpoint se abre fuera del navegador web.

Nota: La versión 4.4 del cliente grueso de NetWitness Endpoint (NWE) debe estar instalada en el mismo servidor, las claves de metadatos de NWE deben existir en el archivo `table-map.xml` en el Log Decoder y las claves de metadatos de NWE deben existir en el archivo `index-concentrator-custom.xml`. El cliente grueso de NWE es una aplicación solo de Windows. En la *Guía del usuario de NetWitness Endpoint* para la versión 4.4 se proporcionan instrucciones de configuración completas.

Descargar los datos en la vista Análisis de eventos

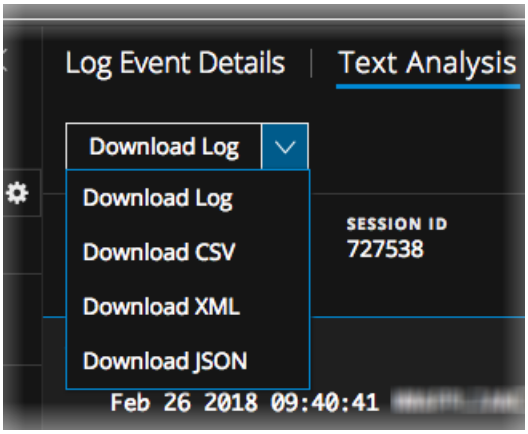
En la vista Análisis de eventos, puede descargar eventos, registros y archivos.

Descargar un registro en el panel Análisis de texto

Cuando observa una reconstrucción de registro en el panel Análisis de texto, puede descargar un archivo de registro en los siguientes formatos mediante las opciones del menú desplegable Descargar registro:

- Registro crudo (registro) mediante la opción **Descargar registro**
- Valores separados por comas (CSV) mediante la opción **Descargar CSV**
- Lenguaje de marcado extensible (XML) mediante la opción **Descargar XML**
- JavaScript Object Notation (JSON) mediante la opción **Descargar JSON**

Este es un ejemplo de una reconstrucción de registro en la que se muestran las opciones del menú Descargar registro.



Nota: La opción Descargar registro se aplica únicamente a eventos de terminal que tienen al menos un valor de metadatos superior a 256 caracteres. Para un evento de terminal, el registro crudo se completa solamente cuando el valor de metadatos supera los 256 caracteres. Los archivos de ejecución prolongada o descargados históricamente no están disponibles para su descarga.
Por ejemplo, los valores de metadatos como argumentos de inicio pueden superar los 256 caracteres. En este caso, los 256 caracteres están disponibles como un valor de metadatos, mientras que el valor completo está disponible y se puede ver en el registro crudo.

El archivo de registro descargado contiene el registro y su nombre permite identificar el servicio en el cual se recopiló, el ID de la sesión y el tipo de archivo. Este es un ejemplo del nombre de archivo de un registro crudo: **Concentrator_SID2.log**. El nombre del archivo de registro exportado usa la siguiente convención:

```
<service-ID or host name>_SID<n>.<filetype>
```

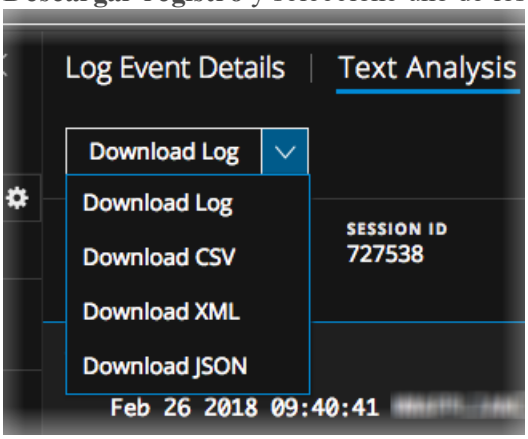
donde:

- `<service-ID or host name>` es el nombre del servicio (por ejemplo, un Concentrator o un Broker) donde se guardó la sesión.
- `SID<n>` es el número de ID de sesión.
- `<filetype>` identifica el formato del registro descargado. Estos son los posibles tipos de registro: registro crudo, CSV, XML y JSON. De forma predeterminada, el formato es un registro crudo.

Nota: Algunos formatos no tienen registros de fecha y hora o la dirección IP del dispositivo donde se generó el evento, por lo que un registro que se descarga en formato CSV, XML o JSON tiene un valor adicional denominado `timestamp` junto con el contenido del registro crudo. La información adicional dentro del registro tiene este formato: `Log timestamp="1490824512" source="10.12.35.65"`.

Para descargar el registro de una sesión:

En el panel Análisis de texto de un evento de registro, seleccione uno de los formatos de archivo para el registro descargado.
-Para descargar el registro como un registro crudo (el formato predeterminado), haga clic en **Descargar registro**.
-Para descargar el registro en uno de los otros formatos, haga clic en la flecha hacia abajo del botón **Descargar registro** y seleccione uno de los formatos de archivo para el registro descargado.



El archivo de registro se descarga en el sistema de archivos local en el formato especificado. Si inicia una descarga y sale de la vista mientras el registro se está extrayendo y antes de que comience a descargarse, el registro no se descarga en el navegador. Un mensaje le informa que puede encontrar el registro descargado en la línea de espera de trabajos.

Descargar datos de eventos de red en el panel Análisis de texto o en el panel Análisis de paquetes

Cuando observa un evento de red reconstruido en los paneles Análisis de paquetes o Análisis de texto, puede exportar archivos de datos de red para realizar un análisis más a fondo. La descarga incluye eventos del rango de tiempo actual y el punto de desglose. Puede descargar los datos de las siguientes maneras:

- El evento completo como un archivo de captura de paquetes (`*.pcap`) mediante la opción **Descargar PCAP**.
- La carga útil como un archivo `*.payload` mediante la opción **Descargar todas las cargas útiles**.

- La carga útil de la solicitud como un archivo `*.payload1` mediante la opción **Descargar carga útil de la solicitud**.
- La carga útil de la respuesta como un archivo `*.payload2` mediante la opción **Descargar carga útil de la respuesta**.

Este es un ejemplo del nombre de archivo de un archivo PCAP: `C01 - Concentrator_SID1697309.pcap`. El nombre del archivo de datos de red exportado usa la siguiente convención:

`<service-ID or host name>_SID<n>.<filetype>`

donde:

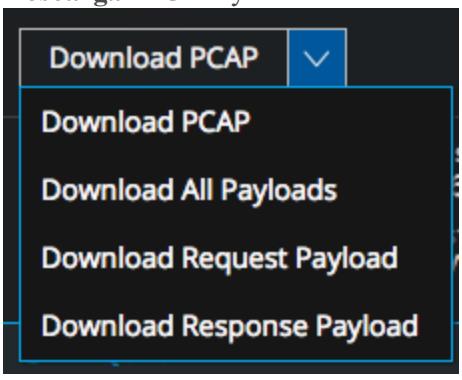
- `<service-ID or host name>` es el nombre del servicio (por ejemplo, un Concentrator o un Broker) donde se guardó la sesión.
- `SID<n>` es el número de ID de sesión.
- `<filetype>` es pcap, payload, payload1 o payload2.

Si la descarga es rápida, los datos de red se descargan directamente en el navegador. Si la descarga tarda más tiempo debido a factores de red o al tamaño del archivo, el archivo se descarga en segundo plano y la tarea se rastrea en la línea de espera de Jobs. En este caso, puede comprobar los trabajos en la línea de espera y obtener el archivo una vez que se complete la descarga.

Nota: Si inicia una descarga y sale de la vista mientras el archivo se está extrayendo y antes de que comience a descargarse, el archivo no se descarga en el navegador. Un mensaje le informa que puede encontrar el documento descargado en la línea de espera de trabajos.

Para exportar un evento como un archivo de datos de red:

Vaya al panel Análisis de paquetes de un evento de red y seleccione uno de los formatos de archivo para el archivo descargado.
-Para descargar el evento como un archivo PCAP (el formato predeterminado), haga clic en **Descargar PCAP**.
-Para descargar el evento en uno de los otros formatos, haga clic en la flecha hacia abajo del botón **Descargar PCAP** y seleccione uno de los formatos de archivo para los datos de evento descargados.



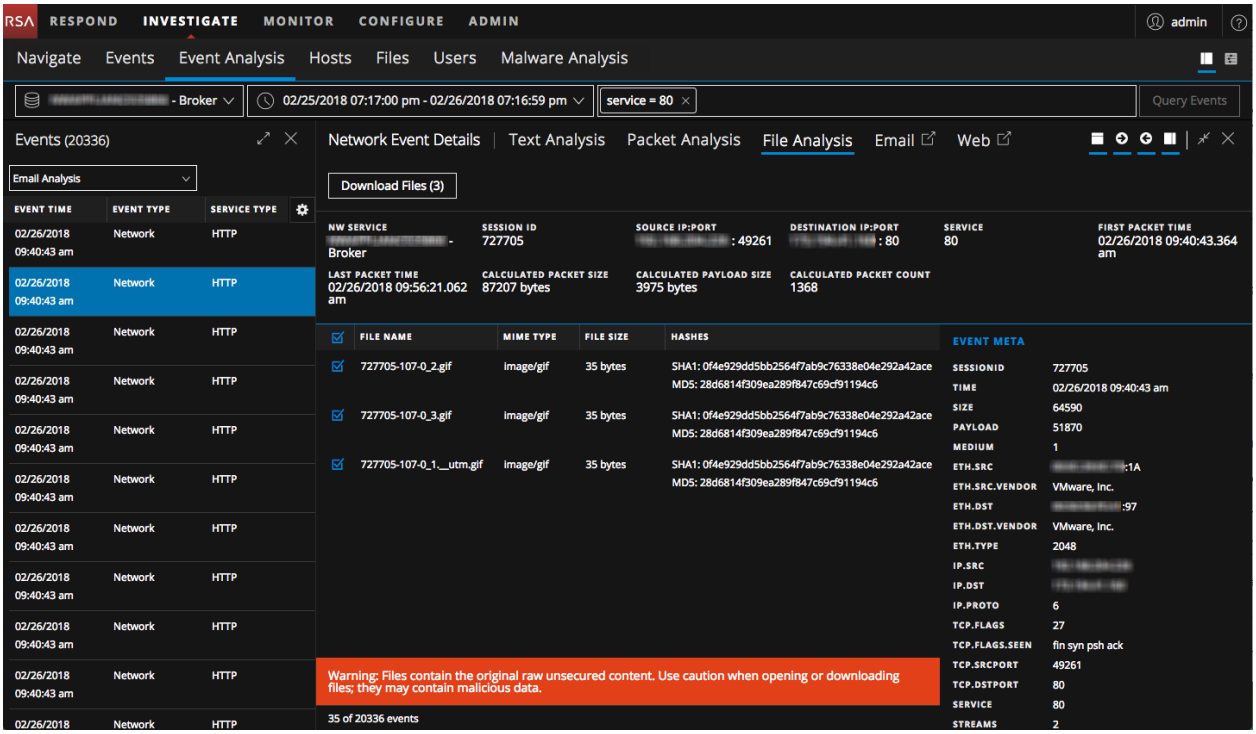
El archivo de datos de red se descarga en el sistema de archivos local en el formato especificado.

Descargar archivos desde un evento de red en el panel Análisis de archivos

Cuando observa eventos de red reconstruidos que contienen archivos en el panel Análisis de archivos, puede seleccionar un archivo, varios archivos o todos ellos para descargarlos en su sistema de archivos local.

Nota: Si inicia una descarga y sale de la vista mientras el archivo se está extrayendo y antes de que comience a descargarse, el archivo no se descarga en el navegador. Un mensaje le informa que puede encontrar el archivo descargado en la línea de espera de trabajos.

Cuando se seleccionan archivos, el botón Descargar archivos se activa y refleja la cantidad de archivos seleccionados.



Cuando se hace clic en el botón, los archivos seleccionados se exportan como un archivo zip protegido por contraseña. La contraseña para abrir el archivo exportado es `netwitness`. La exportación de los archivos de esta manera garantiza que:

- Un software antivirus no tenga el archivo en cuarentena.
- La aplicación predeterminada no abra ni ejecute automáticamente los archivos potencialmente dañinos.

Este es un ejemplo del nombre de un archivo: `C01 - Concentrator_SID1697309_FC1.zip`. El nombre del archivo exportado usa la siguiente convención:

`<service-ID or host name>_SID<n>_FC<n>.zip`

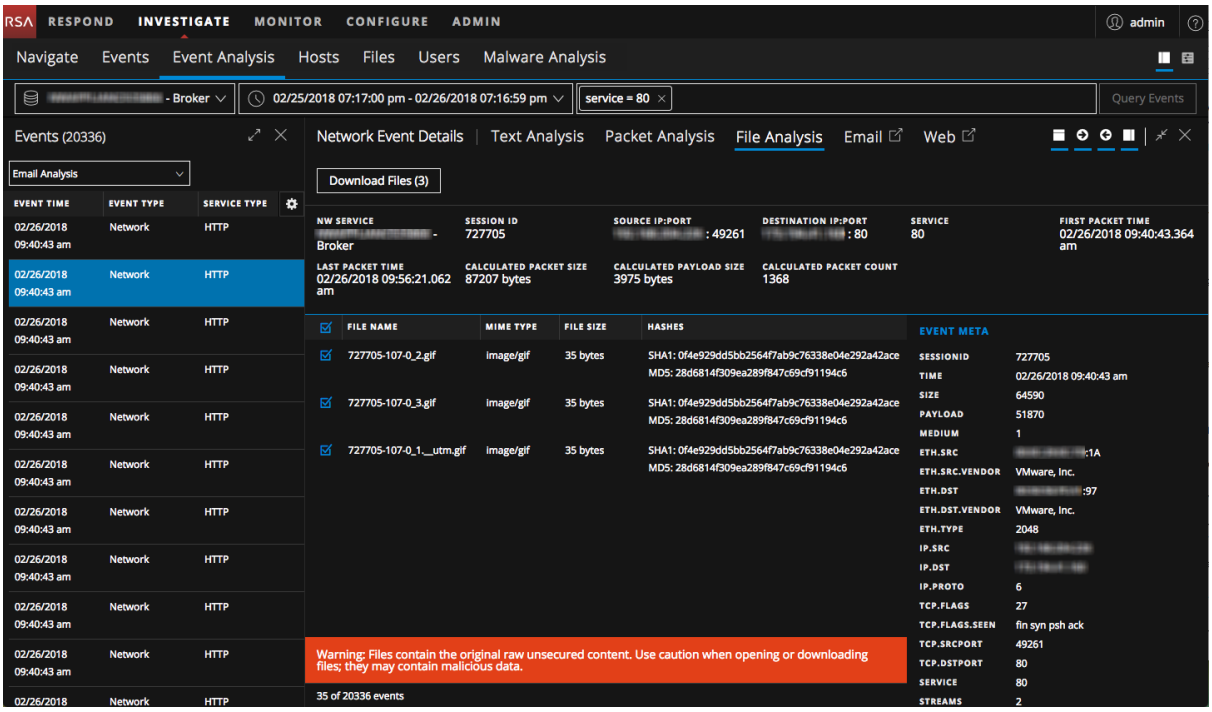
donde:

- `<service-ID or host name>` es el nombre del servicio (por ejemplo, un Concentrator o un Broker) donde se guardó la sesión.
- `SID<n>` es el número de ID de sesión.
- `FC<n>` es el conteo de archivos o la cantidad de archivos que contiene el archivo.

Precaución: Se recomienda tener precaución al descomprimir y abrir archivos asociados con una aplicación predeterminada; por ejemplo, una hoja de cálculo de Excel se puede abrir automáticamente en Excel antes de que usted tenga la oportunidad de verificar su seguridad.

Para exportar archivos en un evento reconstruido:

1. En la vista **Análisis de eventos**, vaya al panel Análisis de archivos de un evento que contenga archivos.



2. Haga clic en uno o más archivos que desee extraer y haga clic en **Descargar archivos**.
   El trabajo se programa y, cuando se completa, el archivo seleccionado se descarga en el sistema de archivos local en la forma de un archivo zip protegido por contraseña.
3. Para abrir el archivo en su sistema de archivos local, ingrese la siguiente contraseña cuando se le solicite: `netwitness`.

Realizar acciones en datos en la vista Análisis de eventos

Cuando encuentra datos de interés en la vista Análisis de eventos, puede realizar búsquedas internas en NetWitness Endpoint y RSA Live, así como búsquedas externas de valores de metadatos en recursos de la comunidad, como el Historial de IP SANS y la Búsqueda en ThreatExpert.

Abrir un evento de terminal en el cliente grueso de NetWitness Endpoint

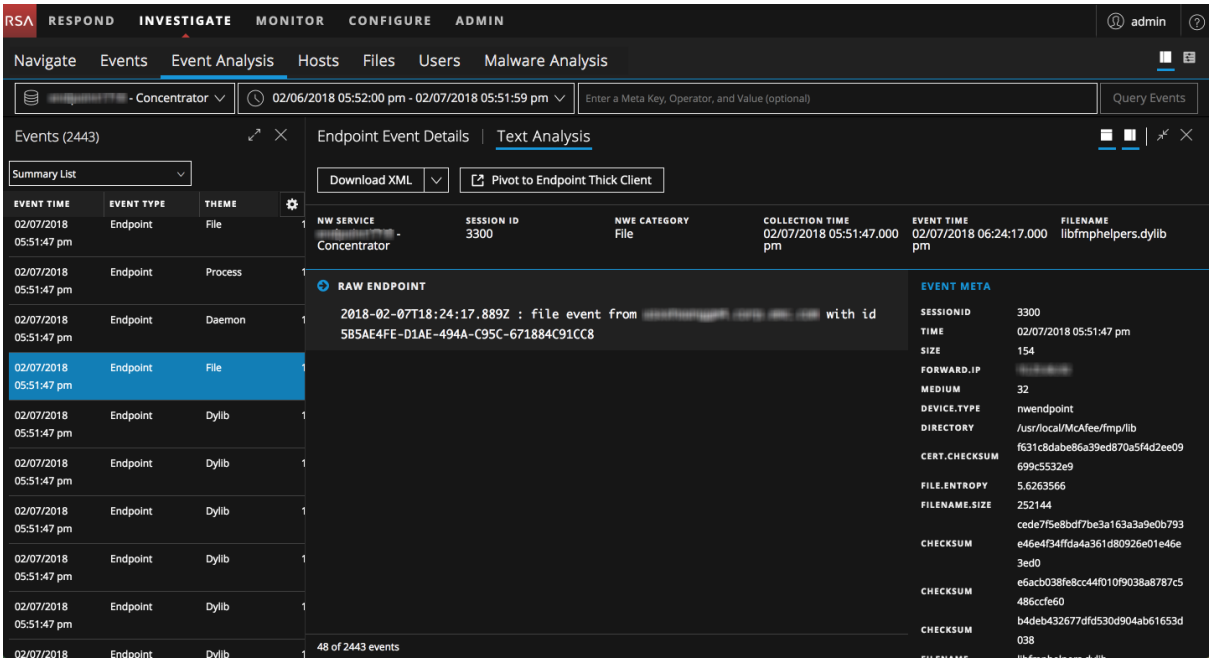
Cuando observa un evento de terminal en el panel Análisis de texto, puede cambiar a NetWitness Endpoint para analizar el mismo evento. El cliente grueso de NWE ofrece funciones adicionales más allá de las funcionalidades incorporadas de NetWitness Endpoint Insights.

Nota: La versión 4.4 del cliente grueso de NetWitness Endpoint (NWE) debe estar instalada en el mismo servidor, las claves de metadatos de NWE deben existir en el archivo `table-map.xml` en el Log Decoder y las claves de metadatos de NWE deben existir en el archivo `index-concentrator-custom.xml`. El cliente grueso de NWE es una aplicación solo de Windows. En la *Guía del usuario de NetWitness Endpoint* para la versión 4.4 se proporcionan instrucciones de configuración completas.

Para abrir un evento en NetWitness Endpoint:

1. (Versión 11.0 y superior) Vaya a **INVESTIGAR** > **Navegar** y realice estos pasos:
   a. En la lista desplegable **Consulta**, seleccione **Avanzada** e ingrese una de las siguientes consultas: `nwe.callback_id exists o device.type='nwendpoint'`
      Los datos de Endpoint se muestran en el panel Valores.
   b. Haga clic con el botón secundario en un evento y seleccione **Análisis de eventos** en el menú.
2. (Versión 11.1 y superior) Vaya a **INVESTIGAR** > **Análisis de eventos**. En la lista desplegable **Consulta**, seleccione **Avanzada** e ingrese una de las siguientes consultas: `nwe.callback_id exists o device.type='nwendpoint'`
   Los datos de Endpoint se muestran en el panel Eventos.

3. Seleccione un evento.
   La vista Análisis de eventos se abre y el evento seleccionado se muestra en el Análisis de texto.

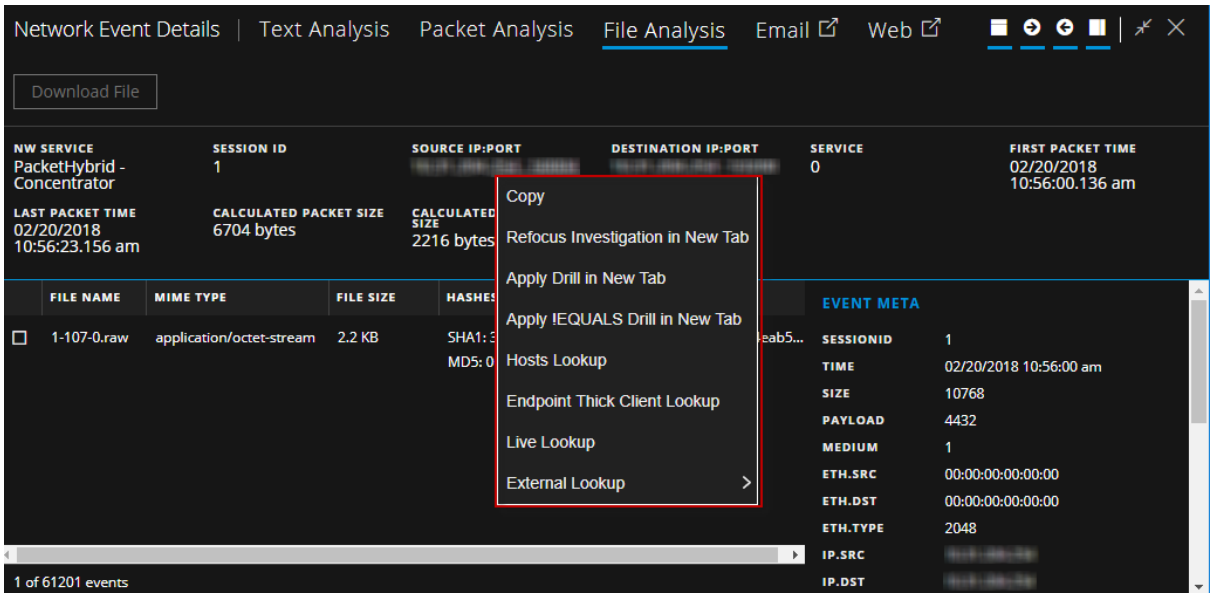


4. En el encabezado del evento, haga clic en **Cambiar a Endpoint.** Se abre una nueva pestaña del navegador con la dirección URL `ecatui://<id>` y se inicia el cliente grueso de NWE. Si el cliente grueso de NetWitness Endpoint no está instalado, no se muestran datos y aparece el siguiente mensaje: `Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

Realizar búsquedas de valores de metadatos en Análisis de eventos

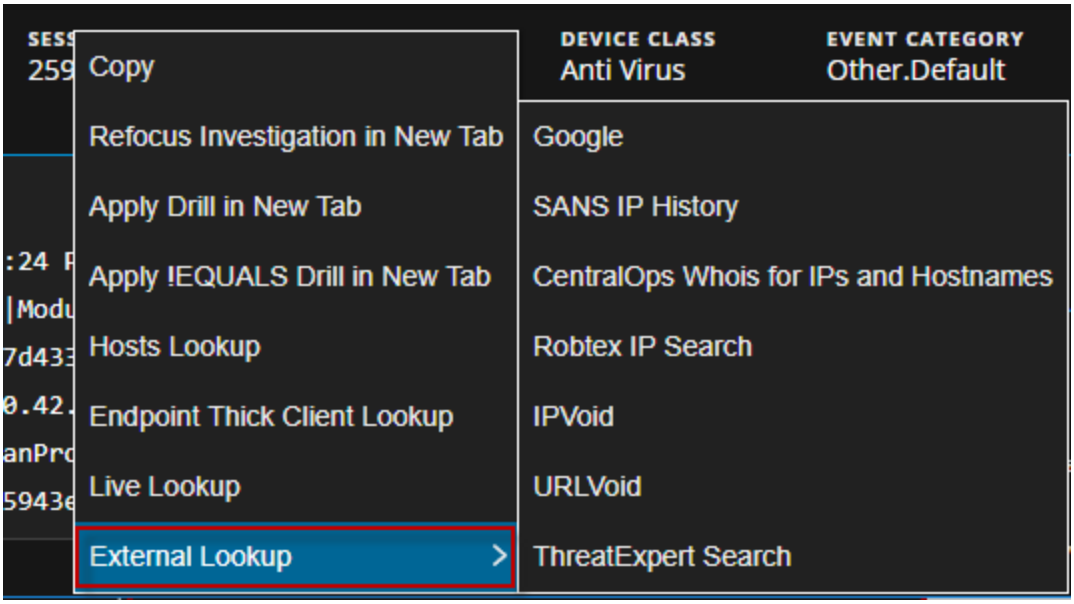
En la vista Análisis de eventos, puede investigar más a fondo los valores de metadatos de un evento, para lo cual debe hacer clic con el botón secundario en ciertos valores de metadatos y usar las opciones de un menú desplegable. No todos los campos tienen acciones del botón secundario. Para realizar búsquedas internas y externas:

1. En la vista Análisis de eventos, haga clic con el botón secundario en un valor de metadatos de la Lista de eventos, el panel Metadatos de eventos o el encabezado del evento. Algunos valores de metadatos tienen un menú desplegable.



2. Seleccione una de las siguientes acciones internas:
   - **Copiar**: Copia el valor de metadatos al portapapeles.
   - **Volver a centrar la investigación en una pestaña nueva**: Inicia otra investigación en una pestaña nueva con el foco en el valor de metadatos seleccionado.
   - **Aplicar desglose en pestaña nueva**: Aplica el desglose y lo inicia en una pestaña nueva para desglosar a los datos en la vista Navegar.
   - **Aplicar desglose !EQUALS en pestaña nueva**: Aplica (!EQUALS) al valor de metadatos e inicia una pestaña nueva, con la exclusión concreta del valor de metadatos de los resultados.
   - **Búsqueda de hosts**: Busca el valor en la vista Investigar > Hosts.
   - **Búsqueda del cliente grueso de Endpoint**: Analiza el valor de metadatos en el cliente grueso de Endpoint (para los clientes que tienen el agente de Endpoint).
   - **Búsqueda en Live**: Busca un valor de metadatos en RSA Live para realizar un análisis más a fondo.

3. Para una búsqueda externa, coloque el cursor sobre un valor de metadatos, haga clic con el botón secundario y seleccione **Búsqueda externa**.



4. En el submenú, seleccione una de las búsquedas externas disponibles:
   - **Google**: Busca un valor de metadatos en Google.com.
   - **Historial de IP SANS**: Busca un valor de metadatos en el historial de IP SANS, dominio = `http://isc.sans.org/ipinfo.html?ip=ipaddress`
   - **CentralOps Whois para direcciones IP y nombres de host**: Busca un valor de metadatos en CentralOps Whois para direcciones IP y nombres de host, dominio = `http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true`
   - **Búsqueda de dirección IP en Robtex**: Busca un valor de metadatos en la búsqueda de direcciones IP en Robtext, dominio = `https://www.robtex.com/cidr/domain.ipaddress`
   - **IPVoid**: Busca un valor de metadatos en IPVoid, dominio = `http://www.ipvoid.com/scan/domain/`
   - **URLVoid**: Busca un valor de metadatos en URLVoid, dominio = `http://www.urlvoid.com/scan/ipaddress/`
   - **Búsqueda en ThreatExpert**: Busca un valor de metadatos de IP en la búsqueda de ThreatExpert, dominio = `http://www.threatexpert.com/reports.aspx?find=IP address`

Investigación de los hosts y los archivos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

Los analistas pueden usar las vistas Hosts y Archivos de RSA NetWitness Platform para investigar los hosts o los archivos.

Las cuentas de usuario de los analistas que realizan análisis mediante Investigate deben tener configuradas las funciones y los permisos correspondientes del sistema. Un administrador debe configurar funciones y permisos como se describe en Funciones y permisos para analistas de Endpoint. Para obtener más información sobre las funciones y los permisos, consulte la *Guía de administración de usuarios y de la seguridad del sistema*.

Los analistas pueden:

- Investigar los hosts
- Investigar los hosts de NetWitness Endpoint 4.4.0.2 o superior
- Investigar los archivos

Investigar los hosts

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

Para realizar una investigación sobre hosts:

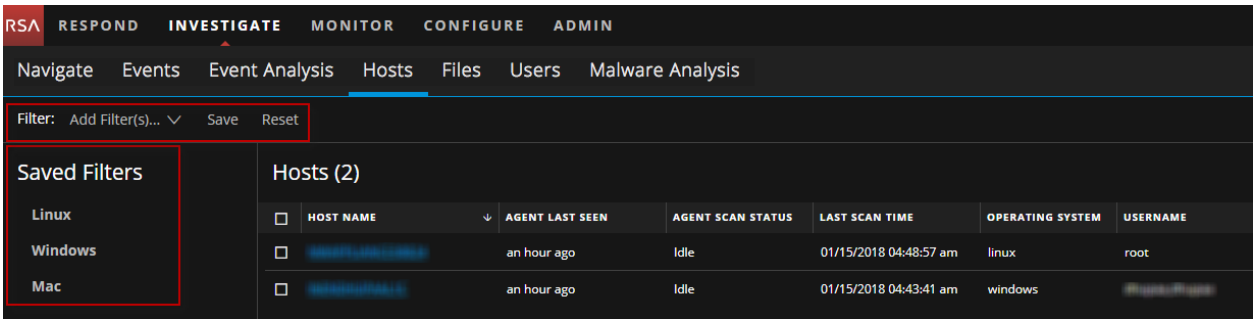
1. Vaya a **INVESTIGAR** > **Hosts**.
   Se muestra una lista de hosts en los que está instalado un agente de Endpoint.
2. Seleccione los hosts que desea escanear y haga clic en **Iniciar escaneo**. Para obtener más información, consulte Escanear los hosts.
3. Después de completar el proceso de escaneo de los hosts, haga clic en el nombre de host para investigar los resultados del escaneo. Para obtener más información, consulte Investigar los detalles de los hosts.

Nota: Para investigar hosts de NetWitness Endpoint 4.4, consulte Investigar los hosts de NetWitness Endpoint 4.4.0.2 o superior.

Filtrar los hosts

Puede filtrar los hosts en el sistema operativo o seleccionar los campos del menú desplegable Agregar filtro.

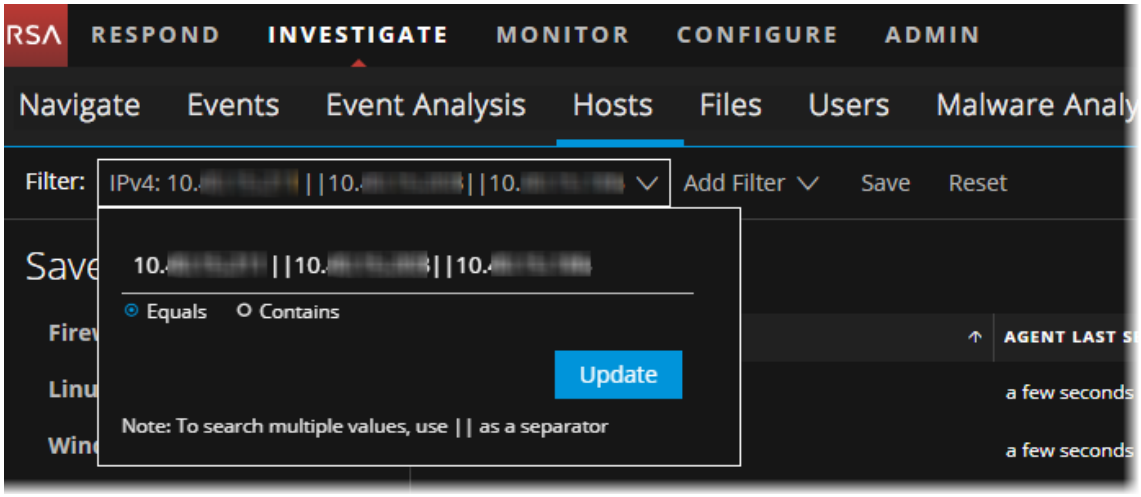
Nota: Cuando filtre una gran cantidad de datos, use al menos un campo indexado con el operador `Equals` para mejorar el rendimiento. Los siguientes campos están indexados en la base de datos: `Hostname`, `IPV4`, `Operating System` y `Last Scan Time`.



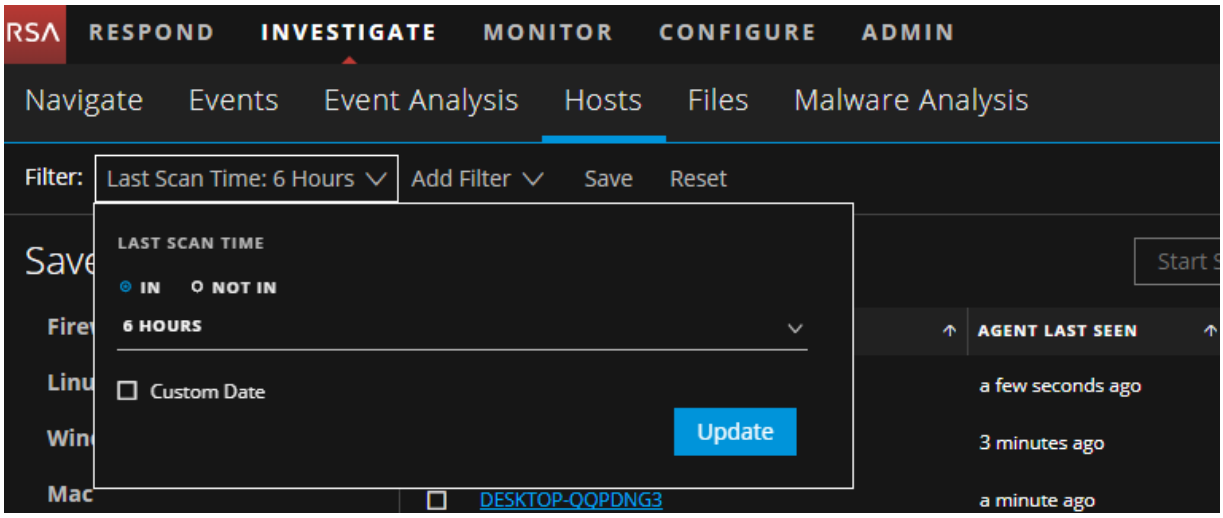
Para buscar valores múltiples dentro de un campo, configure la opción de filtro en `Equals` y use `||` como separador.

Estos son algunos ejemplos:

- Uso del operador `Equals` para valores múltiples IPv4 con un separador `||`.



- Uso del operador `IN` para Hora de último escaneo con el fin de filtrar agentes que se escanean en las últimas 6 horas.



Haga clic en **Guardar** para guardar la búsqueda y proporcione un nombre (hasta 250 caracteres alfanuméricos). El filtro se agrega al panel Filtros guardados de la izquierda. Para eliminar un filtro, coloque el cursor sobre el nombre y haga clic en  .

Nota: Cuando se guarda el filtro, no se permiten caracteres especiales, excepto guion bajo (_) y guion (-).

Escanear los hosts

Puede realizar un escaneo según demanda o programar uno que se ejecute de manera diaria o semanal. Para obtener información sobre la programación de un escaneo, consulte la *Guía de configuración de Endpoint Insights*.

Nota: No puede realizar un escaneo para los agentes de NetWitness Endpoint 4.4 desde la interfaz del usuario de NetWitness Platform.

Escaneo según demanda

Es posible que desee ejecutar un escaneo según demanda si:

- Se determina que un archivo en la sección Archivos globales es malicioso.
- Un archivo malicioso está presente en diferentes hosts de la red.
- Usted desea investigar un host que está infectado.
- Usted desea obtener la instantánea más reciente del host.

Cuando se escanean los hosts, el agente de Endpoint recupera los siguientes datos que se pueden utilizar para la investigación:

- Controladores, procesos, archivos DLL, archivos (ejecutables), servicios y ejecuciones automáticas que se ejecutan en el host.
- Entradas del archivo host y tareas programadas.
- Información del sistema, como recurso compartido de red, parches de Windows instalados, tareas de Windows, usuarios que iniciaron sesión, historial de Bash y productos de seguridad instalados.

Para iniciar un escaneo:

1. Vaya a **INVESTIGAR** > **Hosts**.
2. Seleccione uno o más hosts (hasta 100) para un escaneo según demanda y haga clic en **Iniciar escaneo**.
3. Haga clic en **Iniciar escaneo** en el cuadro de diálogo.
   Esto ejecuta un escaneo rápido de todos los módulos ejecutables cargados en la memoria. Este proceso tarda aproximadamente 10 minutos.

Los siguientes son los estados de escaneo:

Estado	Descripción
Inactivo	No hay ningún escaneo en curso.
Escaneando	Hay un escaneo en curso.
Iniciando escaneo	La solicitud de escaneo se envía al servidor, pero el agente la recibe la próxima vez que se comunica con el servidor.
Deteniendo escaneo	La solicitud de detención se envía al servidor, pero el agente la recibe la próxima vez que se comunica con el servidor.

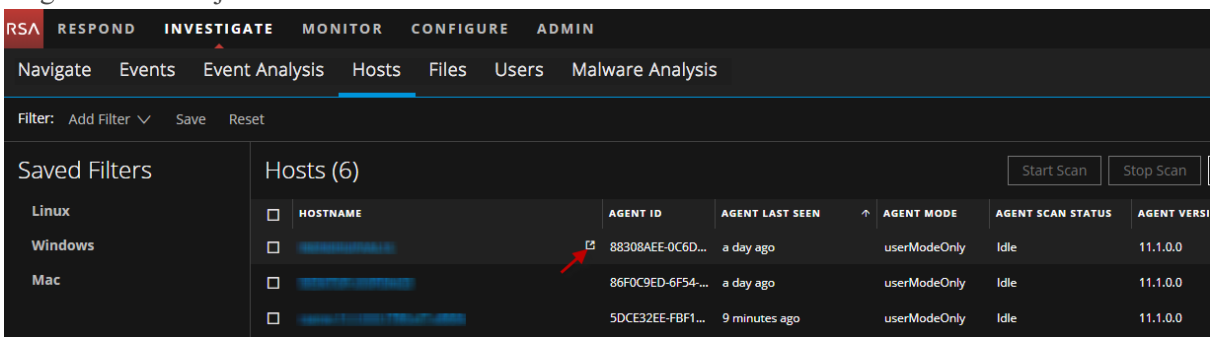
Cambiar a las vistas Navegar y Análisis de eventos

Si debe investigar un host, una dirección IP (IPv4) o un nombre de usuario determinados para buscar actividad relacionada en un rango de tiempo, puede ir a las vistas Navegar y Análisis de eventos para obtener el contexto completo de la actividad. De forma predeterminada, el rango de tiempo está configurado en 1 día. Puede cambiar el rango de tiempo.

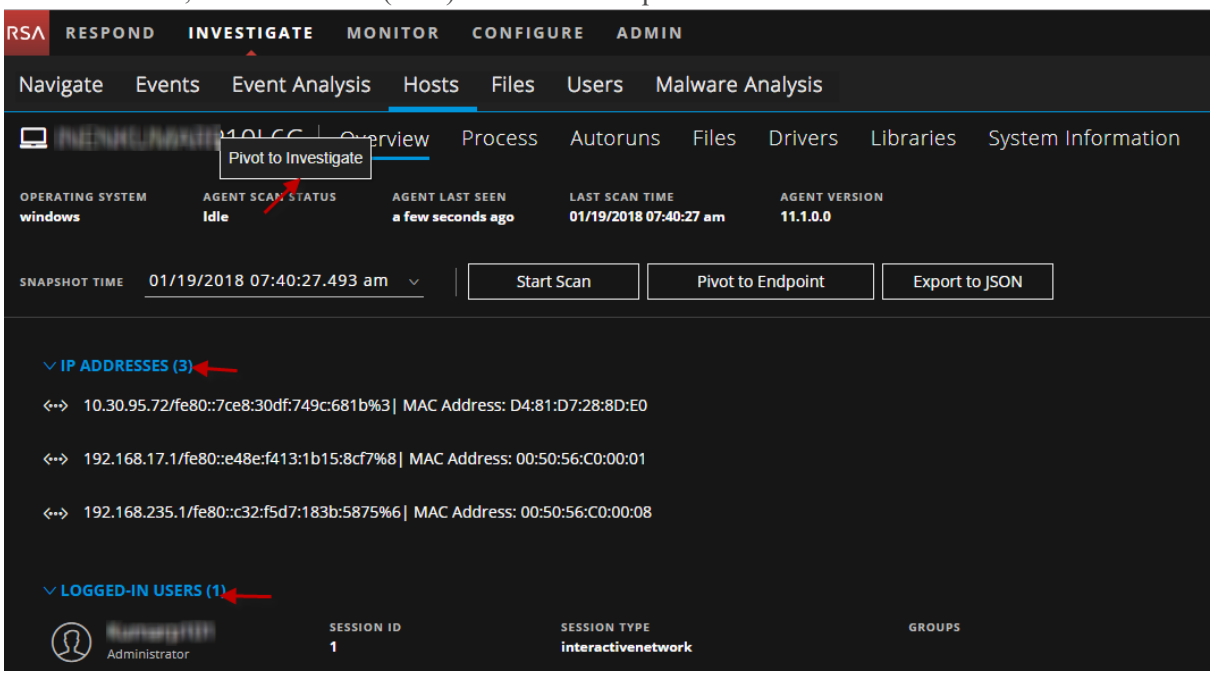
Nota: El cambio a las vistas Navegar o Análisis de eventos no es compatible con IPv6.

Para cambiar a las vistas Navegar o Análisis de eventos:

1. Vaya a **INVESTIGAR** > **Hosts** o **INVESTIGAR** > **Archivos**.
2. Haga clic en  junto al nombre de host.



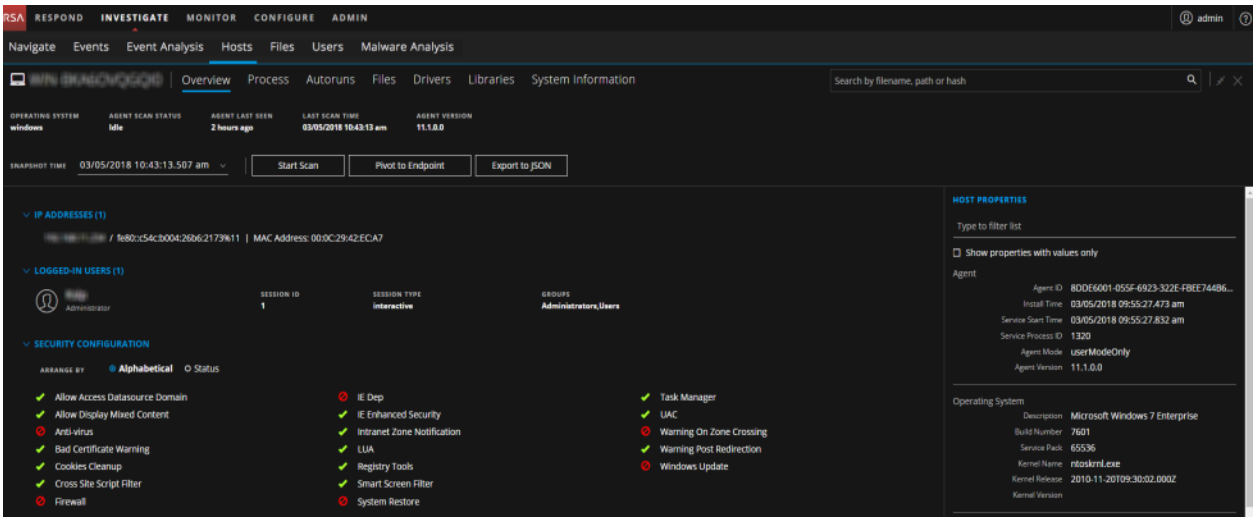
Como alternativa, en la pestaña Descripción general, puede hacer clic con el botón secundario en el nombre de host, la dirección IP (IPv4) o los usuarios que iniciaron sesión a los cuales cambiará.



3. En el cuadro de diálogo Seleccionar servicio, seleccione cualquiera de los servicios necesarios para la investigación.
4. Haga clic en **Navegar** o **Análisis de eventos** para analizar los datos.

Investigar los detalles de los hosts

Para buscar archivos sospechosos en un host, haga clic en el nombre de host y vea los detalles del host o inicie un escaneo según demanda para obtener la información más reciente.



Buscar en las instantáneas

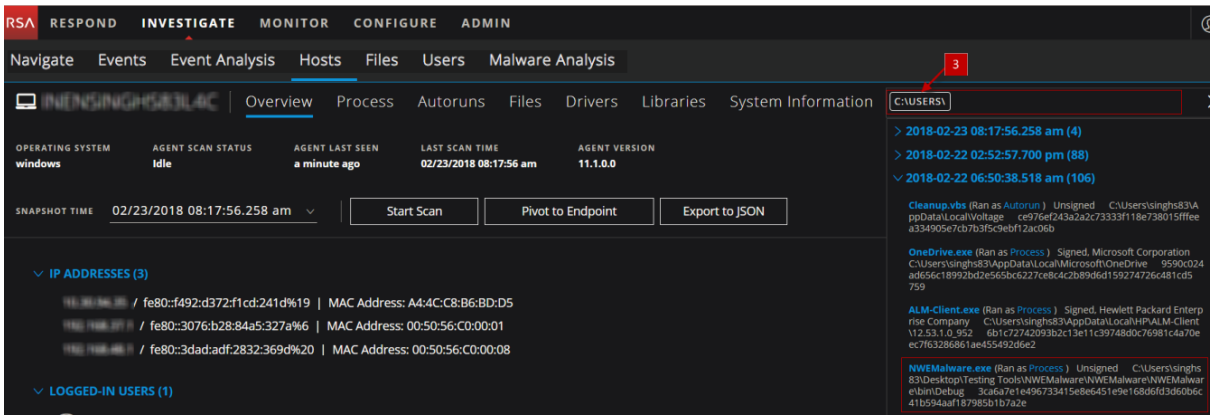
Para investigar un host o ver si está infectado con malware conocido, puede buscar las apariciones del nombre de archivo, la ruta de archivo o la suma de comprobación SHA-256.

Nota: Para buscar una suma de comprobación SHA-256, proporcione la cadena de hash completa en el cuadro de búsqueda.

El resultado muestra detalles, como el nombre de archivo y la información de firma, junto con su interacción con el sistema (se ejecutó como proceso, biblioteca, ejecución automática, servicio, tarea o controlador). Para ver más detalles de estos resultados, haga clic en la categoría.

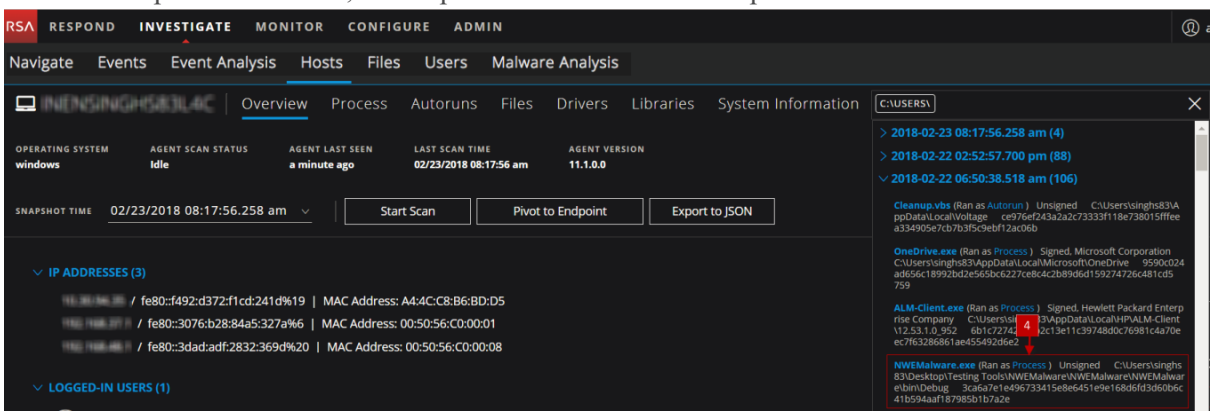
Por ejemplo, un usuario hizo clic y ejecutó un archivo adjunto malicioso a través de un correo electrónico de robo de identidad y lo descargó en `C:\Users`. Para investigar este archivo:

1. Vaya a **INVESTIGAR** > **Hosts**.
2. Seleccione el host que desea investigar.
3. En la pestaña **Descripción general**, ingrese la ruta de archivo `C:\Users` en el cuadro de búsqueda. La búsqueda muestra todos los archivos ejecutables de esta carpeta. En este ejemplo, el archivo `NWEMalware.exe` es un archivo sin firmar que podría ser malicioso.



Este archivo se ejecutó como un proceso.

4. Para ver los detalles de este archivo, haga clic en **Proceso** en el resultado.
   Esto abre la pestaña Proceso, donde puede ver los detalles del proceso.



Analizar los procesos

En la vista Hosts, seleccione la pestaña **Proceso**. Puede ver los procesos que estaban en ejecución para el host seleccionado en el momento del escaneo. Las columnas Nombre de proceso e ID de proceso (PID) se muestran como:

- Vista de árbol: Puede desglosar a cada proceso y ver el proceso secundario o primario asociado a él.
- Vista de lista: Puede ordenar las columnas Nombre de proceso y PID.

Haga clic en para cambiar las vistas.

El siguiente es un ejemplo de la vista de árbol:

Cuando se revisan los procesos, es importante ver los Argumentos de lanzamiento. Incluso los archivos legítimos se pueden utilizar con fines malintencionados, por lo que es importante verlos todos para determinar si hay alguna actividad maliciosa.

Por ejemplo,

- `rundll32.exe` es un archivo ejecutable legítimo de Windows que se categoriza como un archivo válido. Sin embargo, un adversario puede usar este archivo ejecutable para cargar un archivo DLL malicioso. Por lo tanto, al ver los procesos, debe ver los argumentos del archivo `rundll32.exe`.
- `LSASS.EXE` es un elemento secundario de `WININIT.EXE`. No debe tener procesos secundarios. A menudo, el malware usa este archivo ejecutable para volcar contraseñas o crea una imitación para ocultarse en un sistema (`lass.exe`, `lssass.exe`, `lsasss.exe`, etc.).
- La mayoría de las aplicaciones de usuario legítimas, como Adobe, navegadores web, etc., no generan procesos secundarios como `cmd.exe`. Si encuentra esto, investigue los procesos.

Analizar las ejecuciones automáticas

En la vista Hosts, seleccione la pestaña **Ejecuciones automáticas**. Puede ver las ejecuciones automáticas, los servicios, las tareas y los trabajos cron que están en ejecución para el host seleccionado.

Por ejemplo, en la pestaña Servicios, puede buscar la hora de creación del archivo. La hora de compilación se encuentra dentro de cada archivo portable ejecutable (PE) en el encabezado PE. Es raro que se altere el registro de fecha y hora, a pesar de que un adversario puede cambiarlo fácilmente antes de realizar una implementación en el terminal de una víctima. Este registro de fecha y hora puede indicar si se introduce un nuevo archivo. Puede comparar el registro de fecha y hora del archivo con la hora de creación en el sistema para buscar la diferencia. Si un archivo se compiló hace algunos días, pero su registro de fecha y hora en el sistema muestra que se creó hace algunos años, esto indica que el archivo se alteró.

Analizar los archivos

En la vista Hosts, seleccione la pestaña **Archivos**. Puede ver la lista de archivos escaneados en el host en el momento del escaneo. De forma predeterminada, la tabla muestra 100 archivos. Para mostrar más archivos, haga clic en **Cargar más** en la parte inferior de la página.

Por ejemplo, muchos troyanos escriben nombres de archivo aleatorios cuando colocan sus cargas útiles para evitar una búsqueda sencilla en los terminales de la red en función del nombre de archivo. Si un archivo se llama `svch0st.exe`, `scvhost.exe` o `svchosts.exe`, esto indica que se creó una imitación del archivo legítimo de Windows denominado `svchost.exe`.

Analizar las bibliotecas

En la vista Hosts, seleccione la pestaña **Bibliotecas**. Puede ver la lista de bibliotecas cargadas en el momento del escaneo.

Por ejemplo, un archivo con entropía alta se marca como empaquetado. Un archivo empaquetado significa que se comprimió para reducir su tamaño (o para ocultar cadenas maliciosas e información de configuración).

Analizar los controladores

En la vista Hosts, seleccione la pestaña **Controladores**. Puede ver la lista de controladores en ejecución en el host en el momento del escaneo.

Por ejemplo, este panel permite comprobar si el archivo está firmado o sin firmar. Un archivo con la firma de un proveedor de confianza, como Microsoft y Apple, con el término `valid`, indica que es un archivo válido.

Analizar la información del sistema

En la vista Hosts, seleccione la pestaña **Información del sistema**. Este panel enumera la información del sistema del agente. Para el sistema operativo Windows, el panel muestra las entradas del archivo host y los recursos compartidos de red de ese host.

Por ejemplo, el malware podría usar las entradas del archivo host para bloquear las actualizaciones de los antivirus.

Eliminar un host

Para eliminar los hosts manualmente desde la interfaz del usuario:

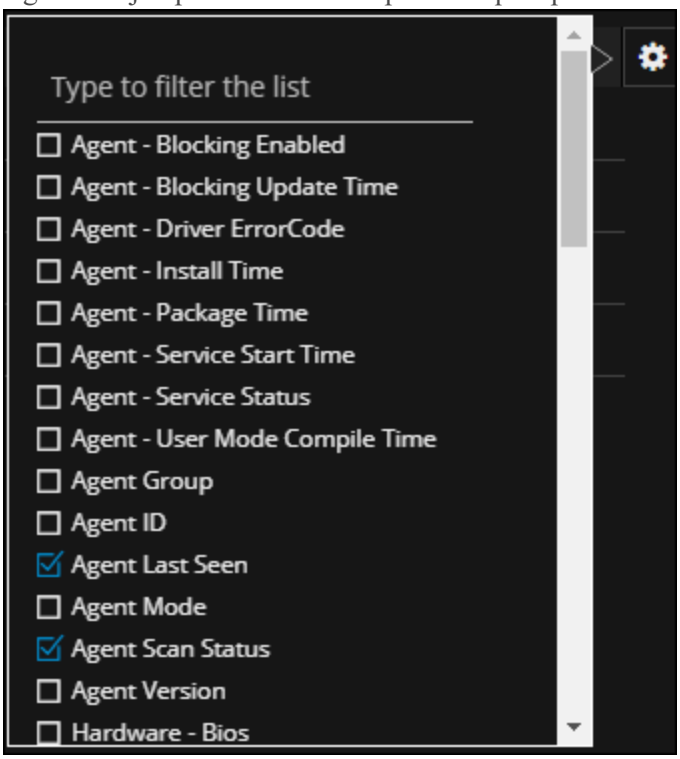
1. Vaya a **INVESTIGAR > Hosts**.
2. Seleccione los hosts que desea eliminar en la vista Hosts y haga clic en **Eliminar**.
   Esto elimina todos los datos de terminales recopilados en los hosts seleccionados.

Nota: Si elimina accidentalmente un host desde la vista Hosts, el servidor de Endpoint prohíbe todas las solicitudes desde este agente. El agente se debe desinstalar manualmente desde el host y reinstalar para que aparezca en la vista Hosts.

Configurar las preferencias de los hosts

De forma predeterminada, la vista Hosts muestra algunas columnas y los hosts se ordenan en función de la hora del último escaneo. Si desea ver columnas específicas y ordenar los datos por un campo determinado:

1. Vaya a la vista **INVESTIGAR > Hosts**.
2. Seleccione las columnas, para lo cual debe hacer clic en en la esquina de la derecha. En el siguiente ejemplo se muestra la pantalla que aparece durante la adición de columnas:



3. Ordene los datos por la columna requerida.

Nota: Este valor se configura como la vista predeterminada cada vez que inicia sesión en la vista Hosts.

Exportar los atributos de los hosts

Puede exportar hasta 100,000 atributos de hosts por vez. Para extraer los atributos de hosts a un archivo de valores separados por comas (csv):

1. Vaya a **INVESTIGAR > Hosts**.
2. Filtre los hosts mediante la selección de las opciones de filtro requeridas.

3. Agregue columnas, para lo cual debe hacer clic en  en la esquina de la derecha.
4. Haga clic en **Exportar a CSV**.

Puede guardar o abrir el archivo csv.

Investigar los hosts de NetWitness Endpoint 4.4.0.2 o superior

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

Si tiene NetWitness Endpoint 4.4.0.2 o superior en la implementación, puede ver los datos de Endpoint de estos hosts en las vistas **INVESTIGAR > Hosts** e **INVESTIGAR > Archivos**.

Si no ve los hosts de NetWitness Endpoint 4.4.0.2 que se enumeran aquí, consulte "Integración de NetWitness Endpoint 4.4.0.2 o superior con NetWitness Endpoint 11.1" en la *Guía de configuración de Endpoint Insights*.

Los hosts de NetWitness Endpoint 4.4.0.2 se pueden identificar en la vista Hosts mediante la versión del agente. No puede realizar un escaneo según demanda en estos hosts. Para investigar estos hosts, debe utilizar la interfaz del usuario de NetWitness Endpoint 4.4.0.2 o superior.

Nota: Para cambiar al cliente grueso desde la interfaz del usuario de NetWitness Suite, NetWitness Endpoint 4.4.0.2 o superior deben estar instalados.

Para investigar un host en la interfaz del usuario de NetWitness Endpoint:

1. Vaya a **INVESTIGAR** > **Hosts**.
2. Seleccione el host 4.4 en la tabla.
3. Haga clic en **Cambiar a Endpoint**.

Nota: La opción **Cambiar a Endpoint** no se aplica para los hosts de NetWitness Endpoint Insights 11.1.

Investigar los archivos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

Los analistas pueden usar la vista Archivos (**INVESTIGAR > Archivos**) para identificar los archivos sospechosos con el examen del nombre de archivo, el tamaño de archivo, la entropía, el formato, el nombre de la empresa, la firma y la suma de comprobación.

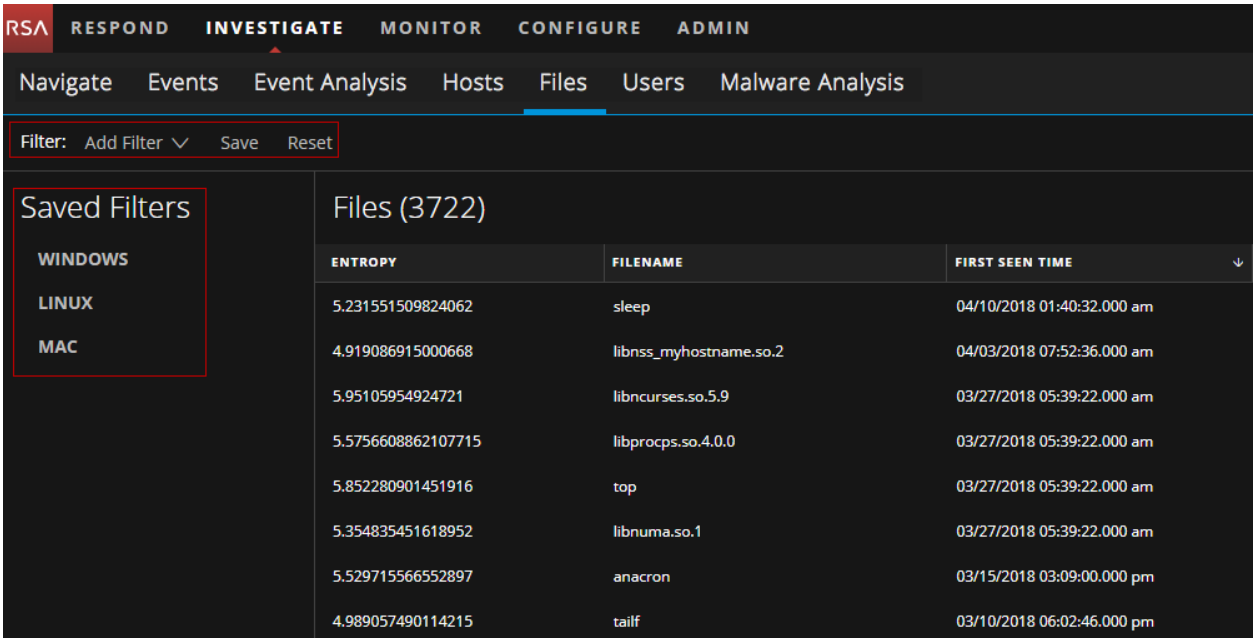
Por ejemplo, cuando se observa un nombre de archivo, si el ransomware WannaCry infectó un ambiente, el analista puede filtrar la lista por este nombre de archivo. También puede buscar este ransomware mediante la suma de comprobación.

El tamaño del archivo puede ser un indicador durante la evaluación de un archivo. Los troyanos suelen tener menos de 1 MB y la mayoría de ellos tiene menos de 500 KB.

Filtrar los archivos

Puede filtrar los archivos en el sistema operativo o seleccionar los campos del menú desplegable Agregar filtro.

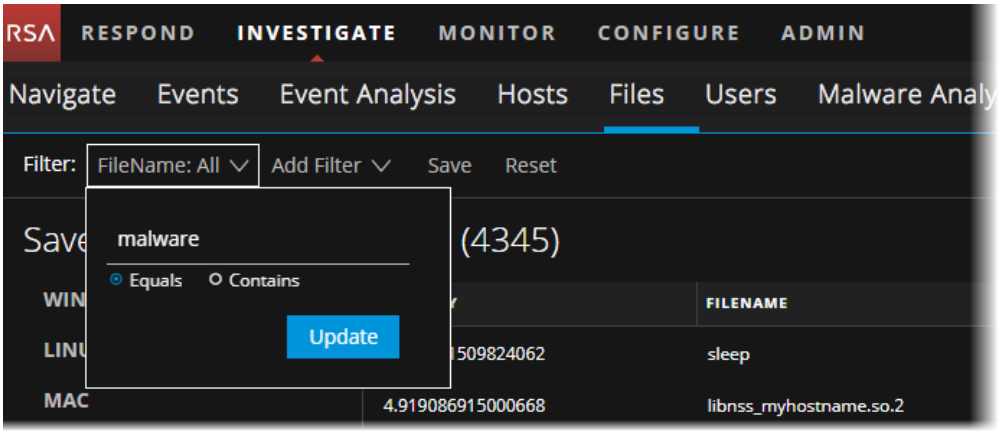
Nota: Cuando use el filtrado en un conjunto de datos grande, use al menos un campo indexado con el operador `Equals` para mejorar el rendimiento. Los siguientes campos están indexados en la base de datos: Nombre de archivo, MD5, Sistema operativo, Hora en que se vio por primera vez y Formato.



Haga clic en **Guardar** para guardar la búsqueda y proporcione un nombre (hasta 250 caracteres alfanuméricos). El filtro se agrega al panel Filtros guardados de la izquierda. Para eliminar un filtro, coloque el cursor sobre el nombre y haga clic en  .

Nota: Cuando se guarda el filtro, no se permiten caracteres especiales, excepto guion bajo (_) y guion (-).

Por ejemplo, filtrado de archivos con el nombre de archivo `malware` y el uso del operador `Equals`.



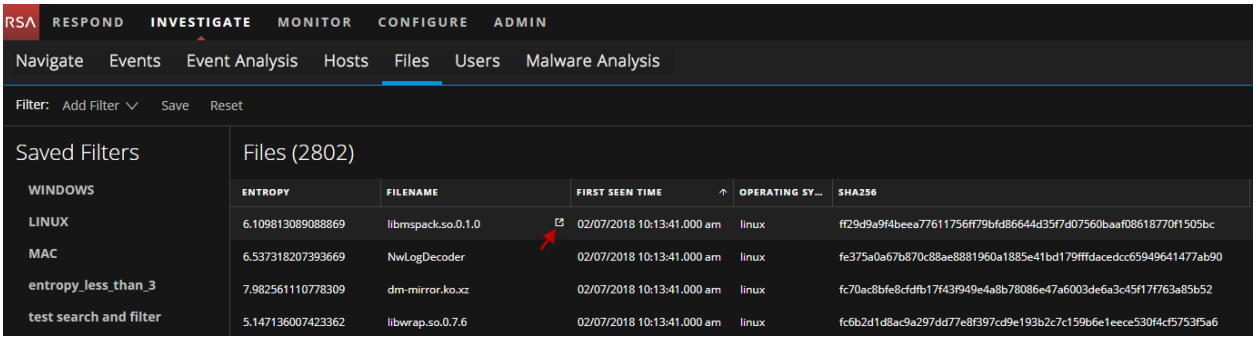
Nota: Para el tamaño de archivo, 1 KB se calcula como 1,024 bytes. Por ejemplo, si el tamaño real del archivo es 8,421 bytes, la interfaz del usuario lo mostrará como 8.2 KB en lugar de 8.22 KB. Cuando se usa el operador `Equals`, se recomienda realizar búsquedas en las cuales se utilice el formato de bytes.

Cambiar a las vistas Navegar y Análisis de eventos

Si debe investigar un nombre de archivo o un hash (SHA256 y MD5) determinados en los archivos globales para buscar actividad relacionada en un rango de tiempo, puede ir a las vistas Navegar y Análisis de eventos para obtener el contexto completo del archivo. De forma predeterminada, el rango de tiempo está configurado en 1 día. Puede cambiar el rango de tiempo según corresponda.

Para cambiar a las vistas Navegar o Análisis de eventos:

1. Vaya a **INVESTIGAR > Archivos**.
2. Haga clic en  junto al nombre de archivo o hash.



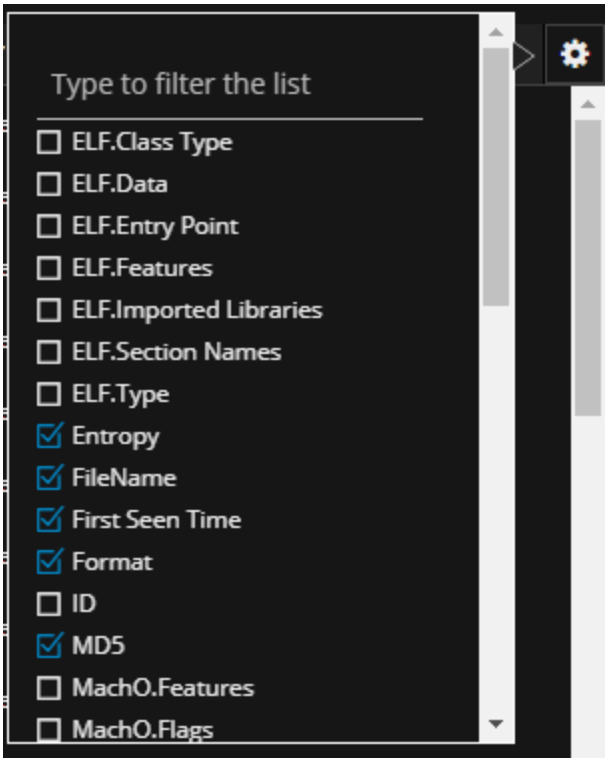
3. En el cuadro de diálogo Seleccionar servicio, seleccione cualquiera de los servicios necesarios para la investigación.
4. Haga clic en **Navegar** o **Análisis de eventos** para analizar los datos.

Nota: Mientras cambia a las vistas Navegar o Análisis de eventos, si los valores no están indexados, los resultados tardan en cargarse. Para obtener más información, consulte Solución de problemas de NetWitness Investigate.

Configurar preferencias de archivos

De forma predeterminada, la vista Archivos muestra algunas columnas y los archivos se ordenan en función de la hora en que se vieron por primera vez. Si desea ver columnas específicas y ordenar los datos por un campo determinado:

1. Vaya a **INVESTIGAR > Archivos**.
2. Seleccione las columnas, para lo cual debe hacer clic en en la esquina de la derecha. En el siguiente ejemplo se muestra la pantalla que aparece durante la adición de columnas:



3. Ordene los datos por la columna requerida.

Nota: Este valor se configura como la vista predeterminada cada vez que inicia sesión en la vista Archivos.

Exportar archivos globales

Para extraer la lista de archivos globales a un archivo CSV:

Nota: Cuando use el filtrado en un conjunto de datos grande, use al menos un campo indexado con el operador `Equals` para mejorar el rendimiento. Puede exportar hasta 100,000 archivos por vez.

1. Vaya a **INVESTIGAR > Archivos**.
2. Filtre los archivos mediante la selección de la opción de filtro requerida.

3. Agregue columnas, para lo cual debe hacer clic en  en la esquina de la derecha.
4. Haga clic en **Exportar a CSV**.

Puede guardar o abrir el archivo CSV.

Realización de un análisis de malware

Los analistas pueden usar el servicio RSA NetWitness Platform Malware Analysis para detectar malware en datos y archivos seleccionados.

Las cuentas de usuario de los analistas que realizan análisis mediante NetWitness Platform Malware Analysis deben tener configuradas las funciones y los permisos del sistema correspondientes.

En los siguientes procedimientos se proporcionan instrucciones para el uso de Malware Analysis:

- Comenzar una investigación de Malware Analysis.
- Cargar archivos para escaneo de Malware Analysis.
- Implementar contenido personalizado de YARA.
- Filtrar datos de dashlets en la vista Resumen de eventos.
- Examinar archivos y eventos de escaneo en formato de lista
- Ver detalles de Malware Analysis de un evento.

Funciones de Malware Analysis

NetWitness Platform Malware Analysis es un procesador de análisis de malware automatizado que analiza determinados tipos de objetos de archivos (como portable ejecutable de Windows (PE), PDF y MS Office) para evaluar la probabilidad de que un archivo sea malicioso.

Malware Analysis detecta indicadores de riesgo mediante el uso de cuatro metodologías de análisis distintas:

- Análisis de sesión de red (red)
- Análisis de archivo estático (estático)
- Análisis de archivo dinámico (Sandbox)
- Análisis de seguridad comunitario (comunidad)

Cada una de las cuatro metodologías de análisis está diseñada para compensar las debilidades inherentes de las demás. Por ejemplo, el análisis de archivo dinámico puede compensar los ataques de día cero que no se detectan durante la fase de análisis de seguridad comunitario. Al evitar análisis de malware que se concentran estrictamente en una metodología, el analista tiene más probabilidades de protegerse contra falsos negativos en los resultados.

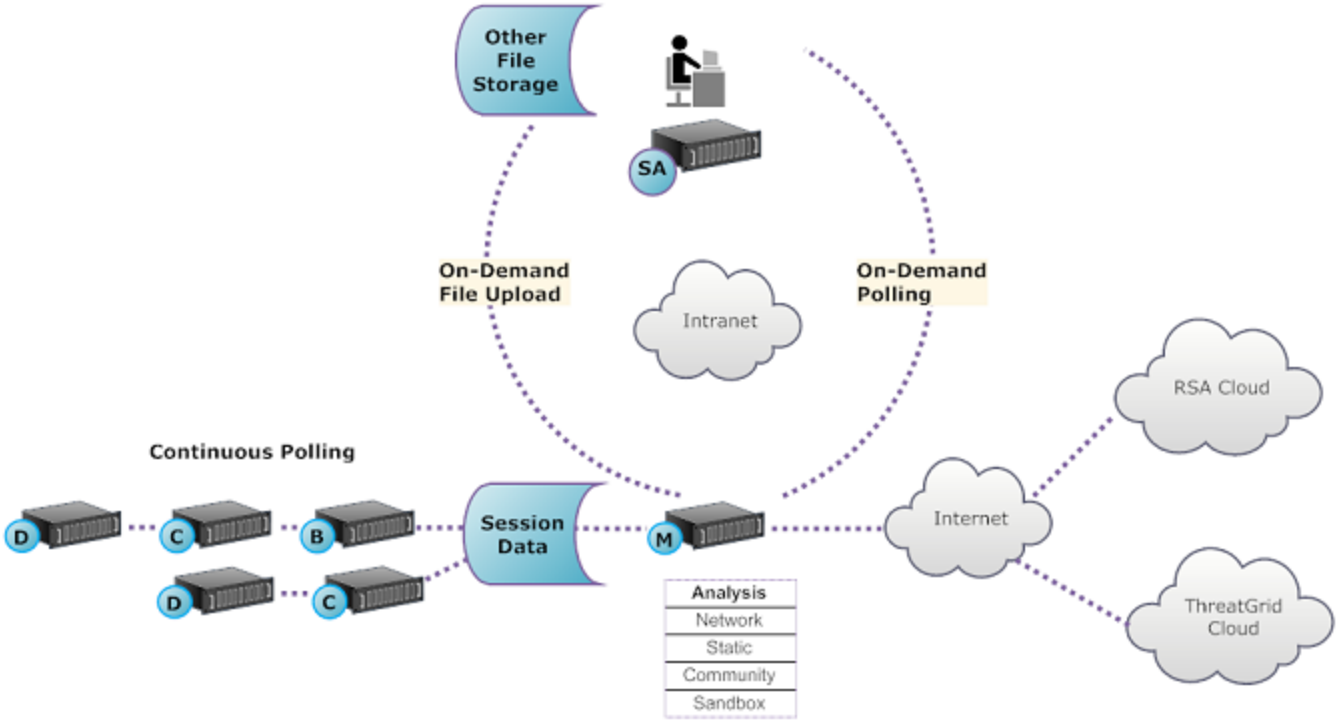
Además de los indicadores de riesgo incorporados, Malware Analysis es compatible con indicadores de riesgo escritos en YARA. YARA es un lenguaje de reglas que permite a los investigadores de malware identificar y clasificar muestras de malware. Esto permite que los autores de IOC agreguen funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live. Estos IOC basados en YARA en RSA Live se descargarán y se habilitarán automáticamente en el host suscrito con el fin de complementar el análisis existente que se ejecuta en cada archivo analizado.

Malware Analysis también tiene características compatibles con alertas para Incident Management.

Descripción funcional

En esta figura se ilustra la relación funcional entre los servicios principales (Decoder, Concentrator y Broker), el servicio Malware Analysis y el NetWitness Server.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



El servicio Malware Analysis analiza objetos de archivos mediante cualquier combinación de los siguientes métodos:

- **Sondeo automático continuo de un Concentrator o un Broker** para extraer sesiones que identificó un analizador como posibles portadoras de contenido de malware.
- **Sondeo según demanda de un Concentrator o un Broker** para extraer sesiones que identificó un analista de malware como posibles portadoras de contenido de malware.
- **Carga según demanda de archivos** de una carpeta especificada por el usuario.

Cuando se habilita el sondeo automático de un Concentrator o un Broker, el servicio Malware Analysis extrae y da prioridad continuamente al contenido ejecutable, documentos PDF y documentos de Microsoft Office en su red, directamente de los datos que capturó y analizó el servicio Security Analytics Core. Dado que el servicio Malware Analysis se conecta a un Concentrator o un Broker para extraer solo los archivos ejecutables que están marcados como posible malware, el proceso es rápido y eficiente. Este proceso es continuo y no requiere monitoreo.

Si selecciona el sondeo según demanda de un Concentrator o un Broker, el analista de malware usa Security Analytics Investigation para desglosar a los datos capturados y seleccionar las sesiones que se analizarán. El servicio Malware Analysis utiliza esta información para sondear automáticamente el Concentrator o el Broker y descargar las sesiones especificadas para el análisis.

La carga según demanda de archivos proporciona un método para que el analista revise los archivos capturados de manera externa a la infraestructura de Core. El analista de malware selecciona una ubicación de carpeta e identifica uno o más archivos con el fin de cargarlos y someterlos al análisis de Security Analytics Malware Analysis. Estos archivos se analizan con el uso de la misma metodología que los archivos que se extraen automáticamente de las sesiones de red.

Método de análisis

Para el análisis de red, el servicio Malware Analysis busca características que parezcan desviarse de la norma, de manera muy similar a lo que hace un analista. Al observar cientos de miles de funciones y combinar los resultados en un sistema de puntaje ponderado, las sesiones legítimas que por coincidencia tienen algunos rasgos anormales se omiten, mientras que las sesiones realmente maliciosas se destacan. Un usuario puede aprender patrones que indican actividad anómala en las sesiones, como indicadores que requieren una investigación más detallada o indicadores de riesgo.

El servicio Malware Analysis puede ejecutar el análisis estático de objetos sospechosos que detecte en la red y determinar si esos objetos contienen código malicioso. En el caso del análisis comunitario, el nuevo malware detectado en la red se envía a RSA Cloud para compararlo con los análisis de malware propios de RSA y feeds de SANS Internet Storm Center, SRI International, el Departamento del tesoro y VeriSign. En el caso del análisis de Sandbox, los servicios también pueden enviar datos a importantes hosts de información de seguridad y administración de eventos (SIEM) (ThreatGrid Cloud).

Security Analytics Malware Analysis cuenta con un método de análisis exclusivo que se basa en asociaciones con líderes y expertos del sector, de modo que sus tecnologías puedan enriquecer el sistema de puntaje de Security Analytics Malware Analysis.

Acceso del NetWitness Server al servicio Malware Analysis

El NetWitness Server está configurado para conectarse al servicio Security Analytics Malware Analysis e importar datos etiquetados para un análisis más profundo en Security Analytics Investigation. El acceso se basa en tres niveles de suscripción.

- Suscripción gratuita: Todos los clientes de NetWitness Platform tienen una suscripción gratuita con una clave de prueba gratuita para análisis de ThreatGrid. El servicio Malware Analysis tiene un límite de 100 muestras de archivo por día. La cantidad de muestras (dentro del conjunto de archivos anterior) enviadas a la nube de ThreatGrid para el análisis de Sandbox se limita a cinco por día. Si una sesión de red tuviera 100 archivos, los clientes alcanzarían el límite después de procesar esa sesión de red. Si los 100 archivos se cargaran manualmente, se alcanzaría el límite.
- Nivel de suscripción estándar: La cantidad de envíos al servicio Malware Analysis es ilimitada. La cantidad de muestras enviadas a la nube de ThreatGrid para el análisis de Sandbox es de 1,000 por día.
- Nivel de suscripción empresarial: La cantidad de envíos al servicio Malware Analysis es ilimitada. El número de muestras enviadas a ThreatGrid Cloud para el análisis de Sandbox es de 5,000 por día.

Método de puntaje

De manera predeterminada, los indicadores de riesgo (IOC) se ajustan para reflejar las mejores prácticas del sector. Durante el análisis, los IOC que se activan hacen que el puntaje aumente o disminuya para indicar la probabilidad de que la muestra sea maliciosa. El ajuste de los IOC se expone en NetWitness Platform para que el analista de malware pueda elegir si desea sobrescribir el puntaje asignado o deshabilitar la evaluación de un IOC. El analista tiene la flexibilidad de usar el ajuste predeterminado o de personalizarlo completamente de acuerdo con necesidades específicas.

Los IOC basados en YARA se entrelazan con los IOC incorporados dentro de cada categoría incorporada y no se distinguen de los IOC nativos. Cuando los IOC se muestran en la vista Configuración de servicio, los administradores pueden seleccionar YARA en la lista de selección Módulo para ver una lista de reglas YARA.

Después de que se importa una sesión a NetWitness Platform, todas las funcionalidades de visualización y análisis de Security Analytics Investigation quedan disponibles para realizar un análisis más detallado de los indicadores de riesgo. Cuando se muestran en Investigation, los IOC de YARA se diferencian de los IOC nativos incorporados por la etiqueta `Yara rule.`.

Implementación

El servicio Security Analytics Malware Analysis se implementa como un host de RSA Malware Analysis independiente. El host de Malware Analysis exclusivo cuenta con un Broker incorporado que se conecta a la infraestructura de Security Analytics Core (que puede ser otro Broker o un Concentrator). Antes de esta conexión, se debe agregar un conjunto de analizadores y feeds a los Decoders que están conectados a los Concentrators y los Brokers desde los cuales extrae datos el servicio Malware Analysis. Esto permite que los archivos de datos sospechosos se marquen para extracción. Estos archivos son contenido etiquetado como `malware analysis` que está disponible a través del sistema de administración de contenido de RSA Live.

Módulos de puntaje de malware

RSA NetWitness Platform Malware Analysis analiza y asigna puntajes a las sesiones y a los archivos integrados dentro de estas según cuatro categorías de puntaje: Red, Análisis estático, Comunidad y Sandbox. Cada categoría comprende muchas reglas y comprobaciones individuales que se usan para calcular un puntaje entre 1 y 100. Cuanto más alto es el puntaje, más probable es que la sesión sea maliciosa y que amerite una investigación de seguimiento más profunda.

Security Analytics Malware Analysis puede facilitar una investigación histórica de los eventos que conducen a una alarma o un incidente en la red. Si sabe que cierto tipo de actividad está ocurriendo en su red, puede seleccionar solo los informes de interés para examinar el contenido de recopilaciones de datos. También puede modificar el comportamiento de cada categoría de puntaje de acuerdo con la categoría de puntaje o el tipo de archivo (Windows PE, PDF y Microsoft Office).

Una vez que se haya familiarizado con los métodos de navegación de datos, podrá explorar los datos de manera más completa con:

- Búsqueda de tipos de información específicos
- Revisión de contenido específico en detalle.

Los puntajes de categoría de Red, Análisis estático, Comunidad y Sandbox se mantienen y se informan de manera independiente. Cuando los eventos se visualizan según los puntajes independientes, siempre que una categoría detecte malware, es evidente en la sección Análisis.

Red

La primera categoría examina cada sesión de red principal de Security Analytics Core para determinar si la distribución de los candidatos de malware era sospechosa. Por ejemplo, software benigno que se descarga desde un sitio seguro conocido, utilizando puertos y protocolos adecuados, se considera menos sospechoso que descargar software que se sabe que es malicioso desde un sitio de descarga dudoso. Los factores de muestra que se usan en el puntaje de este conjunto de criterios pueden incluir sesiones que:

- Contienen información de feed de amenazas
- Se conectan a sitios maliciosos bien conocidos
- Se conectan a dominios/países de alto riesgo (por ejemplo, el dominio .cc)
- Usan protocolos bien conocidos en puertos no estándar
- Contienen JavaScript oculto

Análisis estático

La segunda categoría analiza cada archivo de la sesión en busca de señales de ocultamiento para predecir la probabilidad de que el archivo se comporte de manera maliciosa si se ejecuta. Por ejemplo, software que se vincula con bibliotecas en red tiene más probabilidades de ejecutar actividades sospechosas en la red. Los factores de muestra que se usan en el puntaje de este conjunto de criterios pueden incluir:

- Archivos codificados con XOR
- Archivos detectados incorporados dentro de formatos que no son .EXE (por ejemplo, si se encuentra un archivo PE incorporado dentro de un formato GIF)
- Archivos que se vinculan a bibliotecas de importación de alto riesgo
- Archivos que se desvían considerablemente del formato PE

Comunidad

La tercera categoría asigna puntaje a la sesión y los archivos de acuerdo con el conocimiento colectivo de la comunidad de seguridad. Por ejemplo, los archivos cuya huella digital/hash ya se ha identificado como buena o maliciosa por proveedores de antivirus (AV) respetables reciben el puntaje que corresponde según eso. Los archivos también reciben puntaje según el conocimiento de que un archivo provenga de un sitio conocido como bueno o malicioso por la comunidad de seguridad.

El puntaje de la comunidad también indica si el antivirus de su red marcó los archivos como maliciosos. No indica que el producto antivirus residente actuara para proteger su sistema.

Sandbox

La cuarta categoría examina el comportamiento del software ejecutándolo en un ambiente de Sandbox. Al ejecutar el software para observar su comportamiento, se puede calcular un puntaje según la identificación de actividad maliciosa bien conocida. Por ejemplo, software que se configura a sí mismo para iniciarse automáticamente en cada reinicio y establecer conexiones IRC tendría un puntaje más alto que un archivo que no presente un comportamiento malicioso conocido.

Comenzar una investigación de Malware Analysis

Puede investigar datos que Malware Analysis haya escaneado, marcado y clasificado por su contenido de indicadores de riesgo. Esto incluye todos los tipos de escaneos de Malware Analysis: sondeo en modo continuo, sondeo según demanda y archivos cargados según demanda. El sondeo en modo continuo se debe habilitar cuando el administrador configura ajustes básicos para el servicio Malware Analysis.

NetWitness Platform proporciona varios métodos para iniciar una investigación de Malware Analysis.

Más veloz: Inicio inmediato desde dashlets de Malware Analysis

La manera más rápida de comenzar una investigación de Malware Analysis es un inicio inmediato desde NetWitness Platform Dashboard mediante uno de los dashlets de Malware Analysis que enumera eventos o archivos que probablemente contienen malware. Los dashlets se describen como parte del contenido de RSA NetWitness en Dashlets. Desde uno de estos dashlets, puede ir directamente a los resultados de análisis de un evento específico que se ha enumerado como digno de investigación:

- Lista del malware altamente sospechoso principal
- Lista del posible malware de día cero principal
- Dashlet Malware con IOC de alta confianza y altos puntajes

Sondeo según demanda desde un valor de metadatos en la vista Navegar

Puede iniciar un sondeo según demanda en una investigación si hace clic con el botón secundario en un valor de metadatos en la vista Navegar y selecciona una opción en el menú contextual. Cuando finaliza el sondeo, los datos escaneados quedan disponibles para Malware Analysis (consulte Iniciar un escaneo de Malware Analysis desde la vista Navegar.

Investigar un servicio de RSA específico

También puede iniciar una investigación de Malware Analysis de un servicio en la vista Investigate > Malware Analysis. Para una investigación de Malware Analysis por servicio, se debe especificar un servicio en la vista Investigate > Malware Analysis:

1. Investigate abre la vista de Malware Analysis, donde está seleccionado el servicio predeterminado que especifica el usuario.
2. Si no se especifica ningún servicio predeterminado, un cuadro de diálogo permite seleccionar el servicio de Malware Analysis que se investigará.
3. Cuando se selecciona un servicio en la vista Malware Analysis, se muestra el Resumen de eventos para el servicio seleccionado y sus datos de escaneo continuo.

En este tema se proporcionan instrucciones para todos los métodos de inicio de una investigación de Malware Analysis.

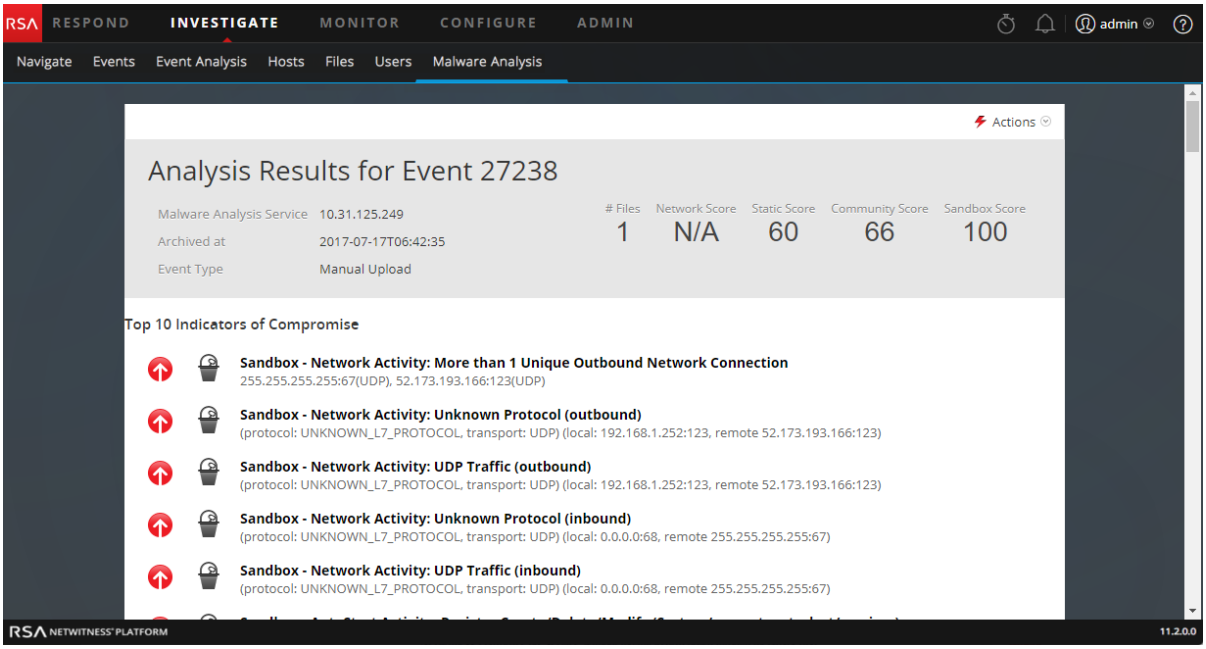
Comenzar una investigación de malware desde un dashlet de Malware Analysis

Este procedimiento tiene el requisito previo de que uno de los siguientes dashlets debe estar visible en el tablero de NetWitness Platform o en la vista Malware Analysis, y se debe completar con eventos o archivos enumerados. Si no ve los dashlets, agréguelos y configúrelos.

- Lista del malware altamente sospechoso principal
- Lista del posible malware de día cero principal
- Dashlet Malware con IOC de alta confianza y altos puntajes

Para iniciar una investigación de Malware Analysis desde un dashlet:

1. Inicie sesión en NetWitness Platform y busque uno de los dashlets mencionados anteriormente en la vista Monitor o en la vista Malware Analysis
2. En el dashlet, haga doble clic en un evento o un archivo para realizar un análisis más profundo. La vista Malware Analysis presenta un análisis detallado del evento en la Lista de eventos o el evento con el cual está asociado el archivo en la Lista de archivos.



Para obtener más información sobre cómo configurar los dashlets de Malware Analysis en el tablero Monitor, consulte “Dashlets” en la *Guía de introducción de NetWitness Platform*.

Para conocer los métodos para configurar y filtrar la información de los dashlets en la vista Malware Analysis, consulte Filtrar datos de dashlets en la vista Resumen de eventos.

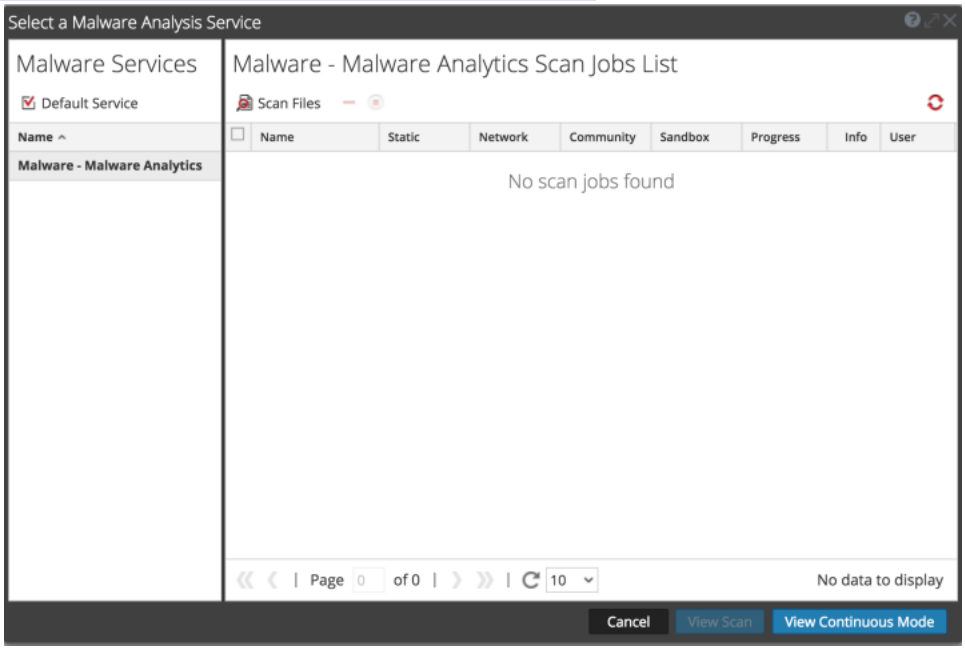
Para obtener información sobre las acciones que puede realizar en los Resultados del análisis, consulte Ver detalles de Malware Analysis de un evento.

Comenzar una investigación de Malware Analysis (sin servicio predeterminado)

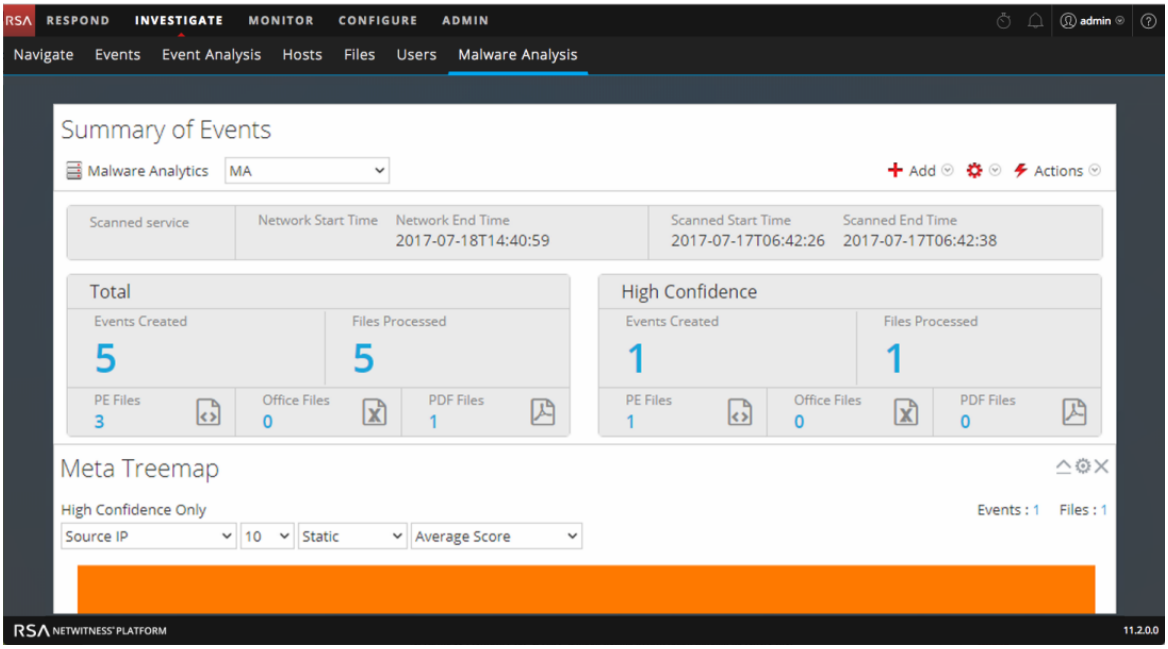
Para comenzar una investigación sin especificar algún servicio predeterminado:

1. Vaya a **INVESTIGAR** > **Malware Analysis**.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis con los hosts y los servicios de Malware Analysis disponibles para el usuario actual en el panel de la izquierda y los trabajos de escaneo disponibles en el panel de la derecha. Este panel de trabajos de escaneo contiene

las mismas columnas que el dashlet Trabajos de escaneo de malware en el tablero Unified. Además, tiene una barra de herramientas y opciones de visualización, las cuales se describen en Cuadro de diálogo Seleccionar un servicio Malware Analysis.



2. En la lista de hosts de Malware Analysis, seleccione un host. Se muestra una lista de trabajos de escaneo en el panel de la derecha. Estos trabajos se crean cuando se escanea un evento o un archivo (consulte Cargar archivos para escaneo de Malware Analysis e Iniciar un escaneo de Malware Analysis desde la vista Navegar).
3. Para comenzar a analizar un escaneo, realice lo siguiente:
   a. Seleccione un escaneo y haga clic en **Ver escaneo**.
   b. Haga clic en **Ver modo continuo**.
      El Resumen de eventos para el escaneo seleccionado se muestra con los dashlets predeterminados abiertos. Cada usuario puede agregar, modificar y eliminar dashlets predeterminados, lo cual persiste en las distintas investigaciones de escaneos. Los usuarios también pueden restaurar los dashlets predeterminados como se describe en Filtrar datos de dashlets en la vista Resumen de eventos.

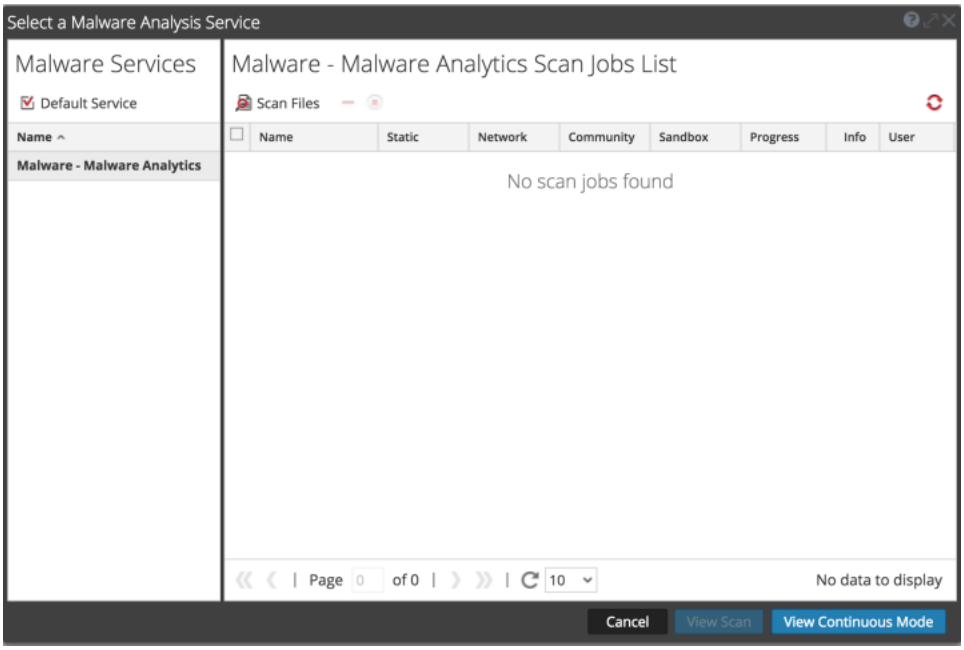


Configurar o borrar el servicio predeterminado

Puede configurar y borrar el servicio predeterminado en el cuadro de diálogo Seleccionar un servicio Malware Analysis.

Para configurar un servicio predeterminado:

1. Haga clic en el nombre del servicio en la barra de herramientas Resumen de eventos.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis.



2. Seleccione un servicio en la lista de servicios de malware disponibles y haga clic en Default Service.

   El servicio se convierte en el valor predeterminado (lo cual se indica con ☑ delante del nombre de host).

3. Para borrar el servicio predeterminado, selecciónelo en la cuadrícula y haga clic en Default Service.

   No se configura ningún servicio predeterminado.

Cargar y escanear archivos

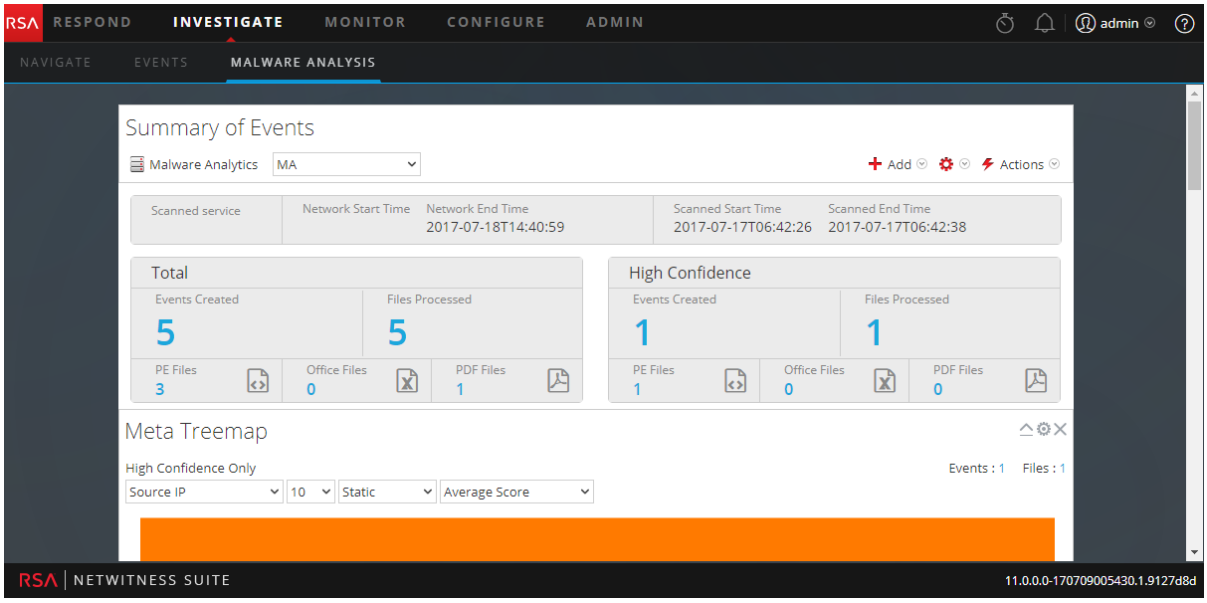
Un analista de malware con permiso para `Initiate Malware Analysis Scan` puede cargar archivos para escanear mediante la opción Escanear archivos del cuadro de diálogo Seleccionar un servicio Malware Analysis (consulte Cargar archivos para escaneo de Malware Analysis). Un administrador puede cargar archivos de captura de paquete en un Decoder para Malware Analysis en la vista Sistema de servicios, como se describe en "Cargar archivo de captura de paquete" en la *Guía de configuración de Decoder y Log Decoder*.

Comenzar una investigación (se especifica el servicio predeterminado)

Para comenzar una investigación con un servicio predeterminado especificado:

1. Vaya a **INVESTIGAR** > **Malware Analysis**.

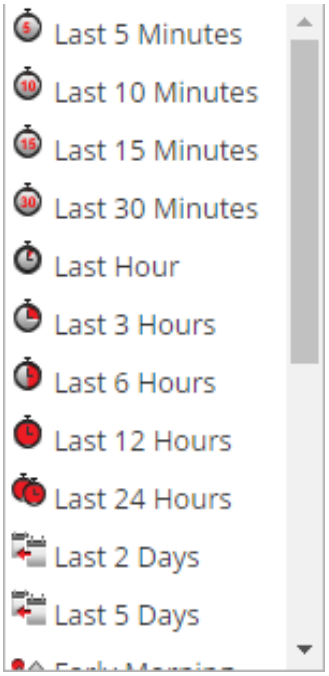
   El Resumen de eventos para un escaneo continuo del servicio seleccionado se muestra con los dashlets predeterminados abiertos. Cada usuario puede agregar, modificar y eliminar dashlets predeterminados, lo cual persiste en las distintas investigaciones de escaneos. Los usuarios también pueden restaurar los dashlets predeterminados como se describe en Filtrar datos de dashlets en la vista Resumen de eventos.



Aplicar un filtro de parámetros de tiempo a los resultados

Puede aplicar un filtro de umbral para actualizar los resultados de los dashlets seleccionados.

1. Para seleccionar un rango de tiempo distinto, seleccione **Modo continuo** u otro escaneo en la barra de herramientas.
   Se muestra el Resumen de eventos de malware del escaneo seleccionado.
2. Para seleccionar un nuevo rango de tiempo para el escaneo, haga clic en la lista de selección de rangos en la barra de herramientas. Los rangos disponibles son: Últimos 5 minutos, Últimos 10 minutos, Últimos 15 minutos, Últimos 30 minutos, Última hora, Últimas 3 horas, Últimas 6 horas, Últimas 12 horas, Últimas 24 horas, Últimos 2 días, Últimos 5 días, Primera hora, Mañana, Tarde, Noche, Todo el día, Ayer, Esta semana, La semana pasada o Personalizado.



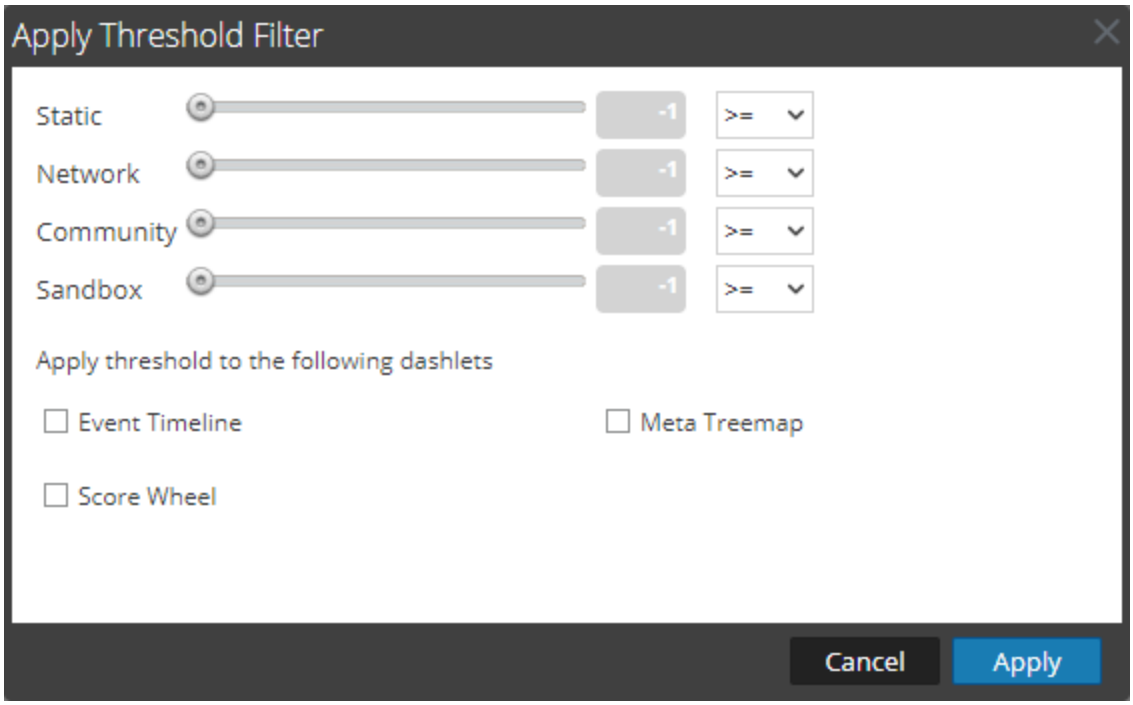
   Los resultados se actualizan de inmediato.
3. Para actualizar un escaneo en modo continuo con nuevos datos, haga clic en .

Aplicar un filtro de umbral a los resultados del modo continuo

Puede aplicar un nuevo filtro de umbral a una instancia de los dashlets Malware con IOC de alta confianza y altos puntajes, Mapa de árbol de metadatos, Rueda de puntaje y Cronograma de evento.

Para personalizar el puntaje que se aplica al escaneo, realice lo siguiente en la barra de herramientas:

1. Seleccione > **Aplicar filtro de umbral.**
   Se muestra el cuadro de diálogo Aplicar filtro de umbral.



2. Si desea limitar la cantidad de eventos que se muestran a aquellos que obtuvieron un puntaje superior a un determinado número, realice lo siguiente:
   a. Arrastre el control deslizante en las barras Static, Red, Comunidad y Sandbox.
   b. Para seleccionar los dashlets a los cuales se aplican los umbrales, seleccione las casillas de verificación apropiadas.
   c. Haga clic en **Aplicar**.

Eliminar o volver a enviar un escaneo según demanda con una nueva configuración de omisión

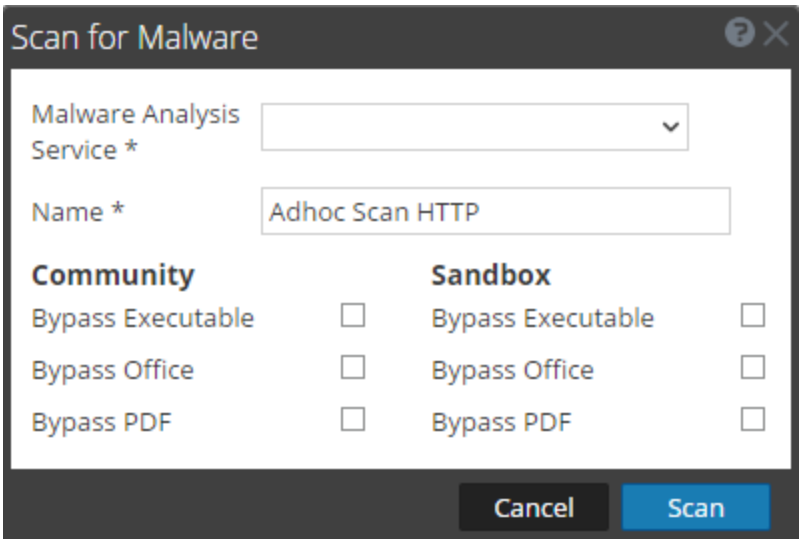
Puede eliminar o volver a enviar un escaneo según demanda con una configuración de omisión distinta a la que se especificó en la vista Configuración del servicio para un servicio Malware Analysis.

Para eliminar un escaneo mientras observa un escaneo según demanda, realice lo siguiente:

1. Seleccione **Acciones** > **Eliminar escaneo**.
   Un cuadro de diálogo solicita que confirme su intención de eliminar el escaneo.
2. Haga clic en **Sí**.
   El escaneo seleccionado se elimina.

Para aplicar una configuración de omisión distinta al escaneo actual:

1. Seleccione **Acciones > Volver a enviar escaneo**.
   Se muestra el cuadro de diálogo Escanear para encontrar malware.



2. Seleccione la configuración de omisión que desea utilizar en el escaneo nuevo y haga clic en **Escanear**.
   Malware Analysis restablece la caché y vuelve a enviar el archivo para un escaneo nuevo, y los trabajos de escaneo se agregan a la línea de espera de trabajos.
3. Cuando el trabajo se complete, desplácese a la izquierda y seleccione **Ver**.
   Se muestra el Resumen de eventos de malware del escaneo seleccionado.

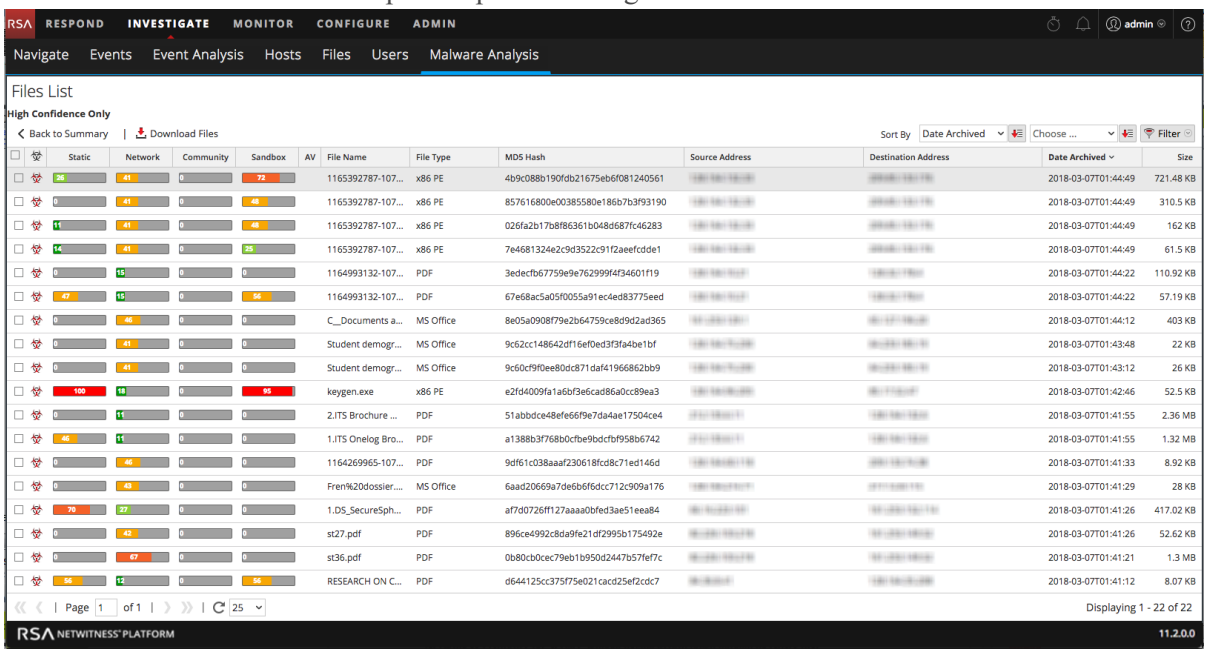
Ver la lista de archivos

Puede ver una lista de archivos para un evento desde el Resumen de eventos de Malware Analysis y desde cada uno de los gráficos de visualización: Cronograma de evento, Desgloses de metadatos, Mapa de árbol de metadatos y Rueda de puntaje.

Para ver la Lista de archivos, realice una de las siguientes acciones:

- En el Resumen de eventos, haga clic en la cantidad de archivos en la fila **Total** o en la fila **Alta confianza** bajo **Archivos procesados**, **Archivos de PE**, **Archivos de Office** o **Archivos PDF**. Se muestra la Lista de archivos.
- En cualquier dashlet de visualización, haga clic en el número junto al campo **Archivos** en la esquina superior derecha del dashlet.

Se muestra la Lista de archivos para el punto de desglose seleccionado.



En la Lista de archivos, puede buscar un archivo por nombre de archivo o hash de archivo MD5, clasificar la lista según dos criterios y orden ascendente o descendente y descargar archivos como se describe en Examinar archivos y eventos de escaneo en formato de lista.

Para volver al Resumen de eventos, haga clic en **Volver al resumen**.

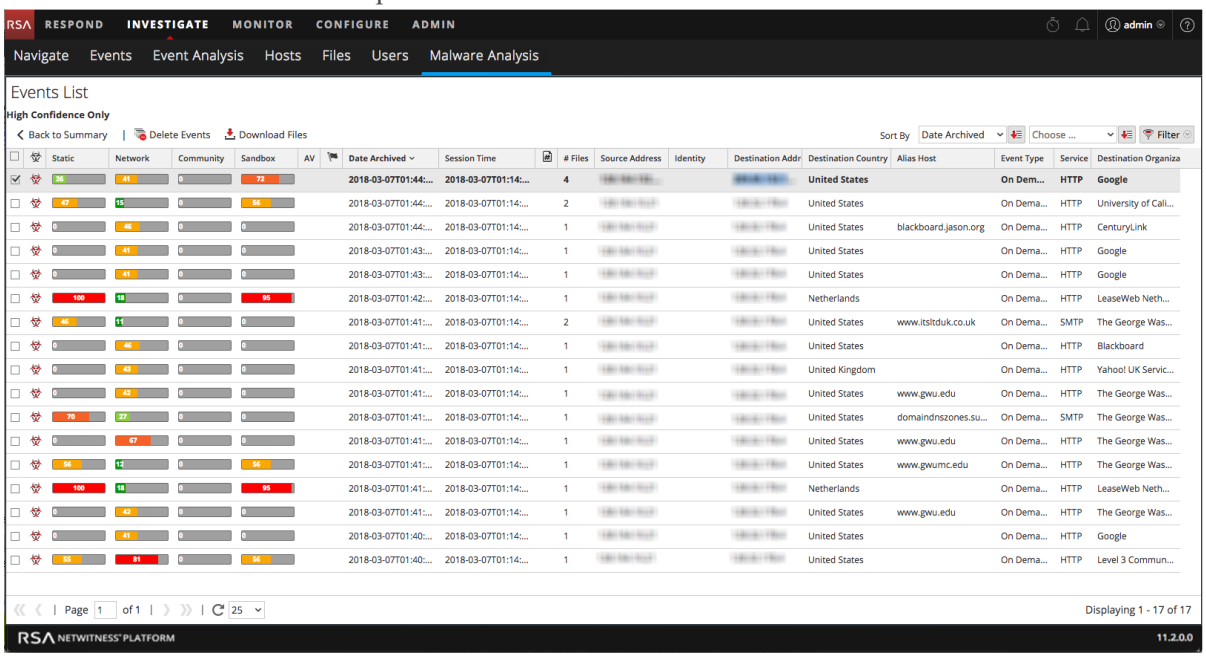
Ver la lista de eventos

En el Resumen de eventos de Malware Analysis y desde cada uno de los gráficos de visualización (Cronograma de evento, Desgloses de metadatos, Mapa de árbol de metadatos y Rueda de puntaje), puede seleccionar eventos para ver en la cuadrícula Eventos.

Para ver la Lista de eventos, realice una de las siguientes acciones:

- En el Resumen de eventos, haga clic en la cantidad de Eventos creados en la fila **Total** o en la fila **Alta confianza**. Se muestra la Lista de eventos.
- En cualquier dashlet de visualización, haga clic en el número junto al campo Eventos en la esquina superior derecha del dashlet.

Se muestra la Lista de eventos para la hora seleccionada.



Implementar contenido personalizado de YARA

Además de los indicadores de riesgo incorporados, Malware Analysis es compatible con indicadores de riesgo escritos en YARA. YARA es un lenguaje de reglas que permite a los investigadores de malware identificar y clasificar muestras de malware. En RSA Live están disponibles indicadores de riesgo (IOC) basados en YARA incorporados; estos se descargan y se habilitan automáticamente en hosts suscritos.

Los clientes con habilidades y conocimientos avanzados pueden agregar funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live o la colocación de estas reglas en una carpeta inspeccionada para consumo del host.

A medida que el malware y el panorama de amenazas evolucionan, es importante revisar y examinar las reglas personalizadas existentes. A menudo se requieren actualizaciones para incorporar nuevos métodos de detección. RSA también actualiza ocasionalmente las reglas YARA en Live. Para recibir actualizaciones, puede suscribirse al blog de RSA y a RSA Live en http://blogs.rsa.com/feed.

En este documento se proporciona información para ayudar a los clientes a implementar reglas personalizadas de YARA en Malware Analysis.

Requisitos previos

El host en el cual está agregando reglas personalizadas debe estar configurado para ser compatible con la creación de reglas YARA, como se describe en “Habilitar contenido personalizado de YARA” en la *Guía de configuración de Malware Analysis*.

Versión y recursos de YARA

RSA Malware Analysis viene empaquetado con YARA versión 3.7 (rev.: 167). Para descubrir la versión exacta, puede ejecutar `yara -v` en el host de Malware Analysis, como se muestra en este ejemplo:

```
[root@TESTHOST yara] # yara -v
 yara 3.7 (rev:167)
```

Claves de metadatos en las reglas YARA

Malware Analysis es compatible con otros orígenes de reglas YARA y también consume claves de metadatos adicionales que son específicas de Malware Analysis. Cada regla YARA es equivalente a un indicador de riesgo (IOC) dentro de Malware Analysis. En el siguiente ejemplo se ilustran las definiciones de metadatos en una regla:

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Clave de metadatos	Descripción
iocName	(Requerido) Este es el nombre que usa MA como nombre de la regla. Es específico de Malware Analysis y se requiere para agregar la regla a la lista de IOC.
fileType	Especifica el tipo de archivo. Los valores posibles son: WINDOWS_PE, MS_OFFICE y PDF. Si no se especifica, el valor predeterminado es WINDOWS_PE.
puntaje	Este valor se agrega al puntaje estático si se activa la regla YARA. Si no se especifica, el valor predeterminado es 10.
ceiling	Esta es la cantidad máxima que se agrega a los puntajes estáticos cuando una regla se activa varias veces en una sesión. Por ejemplo, si cada vez que se activa una regla se agregan 20 puntos al puntaje estático y no se desea que se agreguen más de 40 puntos cuando la regla se activa más de dos veces, se puede especificar un límite de 40. Si no se especifica, el valor predeterminado es 100.
highConfidence	Esto configura el indicador de Alta confianza, el cual se establece en IOC cuando hay indicadores de alta confianza que delatan la presencia de malware. Si no se especifica, el valor de archivo predeterminado es false.

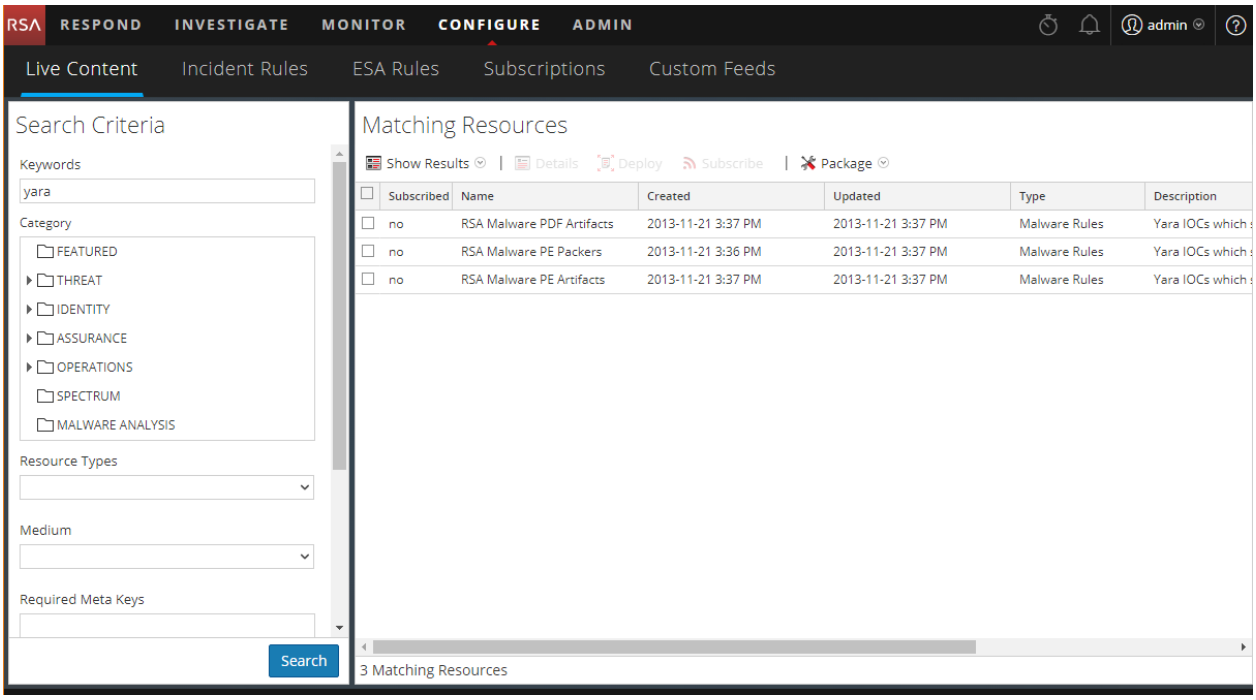
Nota: Consulte la siguiente URL para los recursos YARA: https://code.google.com/p/yara-project/downloads/list. NetWitness Platform usa YARA 3.7, no YARA 2.0.

Contenido de YARA

RSA Live incluye tres conjuntos de reglas Yara:

- PE Packers
- PDF Artifacts
- PE Artifacts

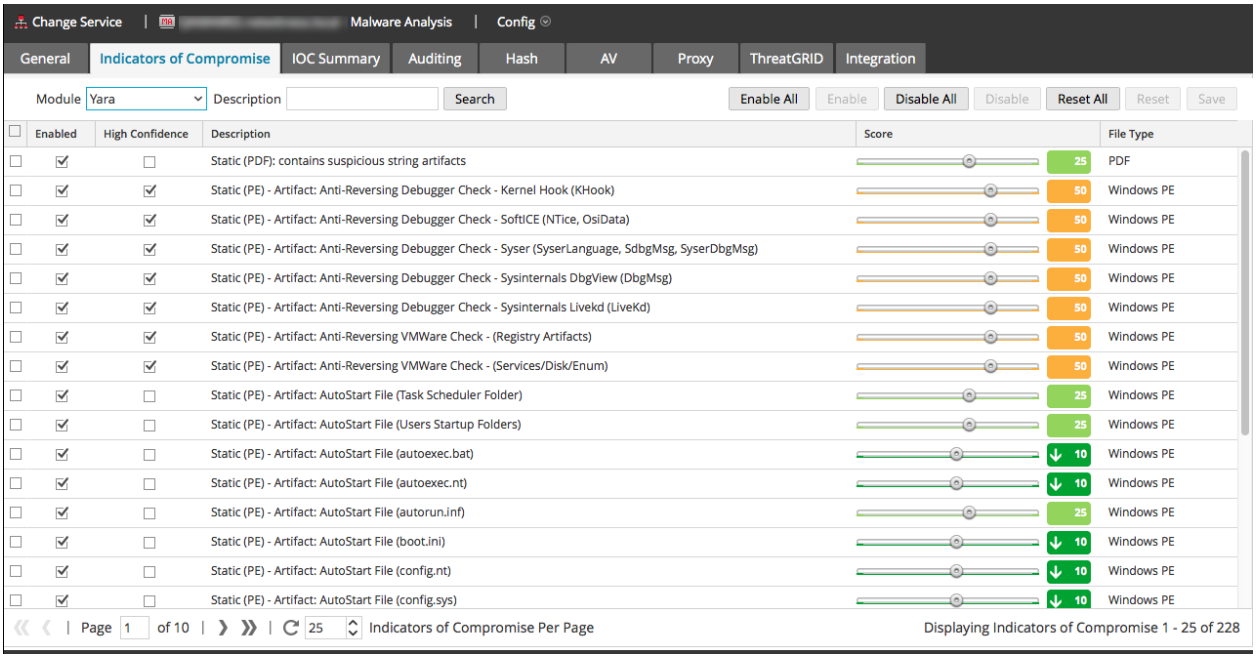
En la siguiente figura se ilustra el contenido de YARA disponible como reglas YARA en NetWitness Platform Live.



En el host de Malware Analysis, las reglas YARA residen en `/var/lib/netwitness/malware-analytics-server/spectrum/yara`, como se muestra en el siguiente ejemplo.

```
[root@TESTHOST yara]# pwd
 /var/lib/netwitness/malware-analytics-server/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_packers.yara
```

Las reglas individuales se muestran como IOC en la vista Configuración del servicio Malware Analysis > pestaña Indicadores de riesgo. Para verlas, use el módulo Yara como filtro. Puede ajustar la configuración de una regla de la misma manera que configura otros IOC.



Agregar reglas YARA personalizadas

Para presentar reglas YARA personalizadas desde otros orígenes:

1. Para asegurarse de que las reglas YARA sigan la sintaxis y el formato correctos, use el comando YARA con el fin de compilar la regla YARA como se muestra en el siguiente ejemplo. Si la regla YARA se compila sin errores, esto indica que tiene la sintaxis correcta.

   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
   [root@TESTHOST yara]#
   ```

2. Asegúrese de que las reglas personalizadas no dupliquen reglas YARA existentes de RSA o de otros orígenes. Todas las reglas YARA se encuentran en `/var/lib/netwitness/malware-analytics-server/spectrum/yara`

3. Asegúrese de que se incluyan las claves de metadatos compatibles con RSA para organizar las reglas YARA como parte de los IOC configurables y dé al archivo un nombre con la extensión yara (<filename>.yara). Para una mejor organización, asegúrese de que los metadatos `iocName` se incluyan en la sección de metadatos, como se muestra en el siguiente ejemplo.

   Ejemplo:

   ```
   rule HEX_EXAMPLE
   {
       meta:
           author = "RSA"
           info = "HEX Detection"
          iocName = "Hex Example"
       strings:
           $hex1 = { E2 34 A1 C8 23 FB }
           $wide_string = "Ausov" wide ascii
       condition:
           $hex1 or $wide_string
   }
   ```

4. Cuando esté listo, coloque el archivo de YARA personalizado en la carpeta que inspecciona el servicio Malware Analysis:

   `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`

   El archivo se consume en un minuto.

   Cuando se consume, NetWitness Platform lo transfiere a la carpeta `processed` y la nueva regla se agrega a la vista Configuración de servicios > pestaña Indicadores de riesgo de Malware Analysis.

Examinar archivos y eventos de escaneo en formato de lista

Cuando observa el Resumen de eventos en un escaneo de Malware Analysis, puede hacer clic en un conteo de archivos o en un conteo de eventos para ver la Lista de archivos o la Lista de eventos del escaneo (consulte Comenzar una investigación de Malware Analysis). En la Lista de archivos y la Lista de eventos, puede buscar un archivo por nombre de archivo o hash de archivo MD5, clasificar la lista mediante dos criterios y orden ascendente o descendente, y descargar archivos. Cuando encuentra un evento o archivo que el interesa en la Lista de eventos o Lista de archivos, puede ver muchos detalles sobre el evento en la vista Detalles de eventos.

Para cada evento de la Lista de eventos, NetWitness Platform proporciona la siguiente información:

- Marcado como un evento de alta confianza, que probablemente contenga indicadores de riesgo.
- El puntaje numérico de cada módulo de puntaje: Estático, Red, Community y Sandbox.
- Puntajes del proveedor de antivirus.
- El indicador Influido por regla personalizada.
- La fecha en que se archivó el evento.
- La hora de sesión.
- El filtro de hash de MD5.
- Cantidad de archivos en el evento.
- La dirección IP de origen del evento.
- La identidad.
- La dirección IP de destino.
- El país de destino.
- El nombre del host de alias.
- El tipo de evento, por ejemplo, Network.
- El servicio que utiliza el evento.
- La organización de destino

Para cada archivo en la Lista de archivos, NetWitness Platform proporciona la siguiente información:

- Marcado como un evento de alta confianza, que probablemente contenga indicadores de riesgo.
- El puntaje numérico de cada módulo de puntaje: Estático, Red, Community y Sandbox.
- Puntajes del proveedor de antivirus.
- El nombre de archivo.
- El tipo de archivo.
- El filtro de hash de MD5.
- La dirección IP de origen del evento que contenía el archivo.

- La dirección IP de destino.
- La fecha en que se archivó el evento que contenía el archivo.
- El tamaño del archivo.

Clasificar la Lista de archivos o la Lista de eventos

Puede clasificar la Lista de archivos y la Lista de eventos por nombre de columna en orden ascendente y descendente. Puede elegir una o dos columnas.

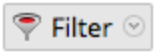
Para clasificar la lista:

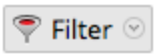
1. En la primera lista desplegable **Ordenar por**, elija un nombre de columna y una dirección de clasificación:  para el orden descendente o  para el orden ascendente.
2. (Opcional) En la segunda lista desplegable **Ordenar por**, elija un nombre de columna y una dirección de clasificación,  para el orden descendente o  para el orden ascendente.
   Los títulos de las columnas reflejan el orden de clasificación seleccionado.

Filtrar la lista por nombre de archivo o hash de archivo MD5

Puede filtrar la Lista de archivos y la Lista de eventos por nombre de archivo o hash de archivo. Con esta función, puede especificar un subconjunto limitado de los datos originales en función de los criterios de búsqueda.

Nota: Cuando realiza una búsqueda, se busca el escaneo que está visualizando actualmente, no todos los escaneos.

1. Haga clic en 

   .
   Se muestra el cuadro de diálogo Filtrar.
2. Ingrese un valor en **Nombre de archivo** o **Hash de MD5** y haga clic en **Filtrar**. Los campos Nombre de archivo y Hash de archivo no distinguen mayúsculas de minúsculas. No se admiten comodines o expresiones regulares. El filtro se basa en coincidencias exactas. Puede arrastrar un nombre de archivo o hash que desee seleccionar desde la Lista de archivos o la Lista de eventos y, a continuación, copiarlo y pegarlo en el cuadro de diálogo.
3. Haga clic en **Filtrar**.
   Malware Analysis filtra la lista para mostrar solo archivos o eventos con el hash seleccionado.
4. Para volver a la lista no filtrada, haga clic en 

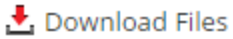
   . Cuando aparezca el cuadro de diálogo Filtrar, haga clic en **Restablecer**.

Descargar archivos de la Lista de archivos

NetWitness Platform permite seleccionar y descargar archivos de la Lista de archivos o la Lista de eventos.

Precaución: Sea precavido cuando descargue archivos desde Malware Analysis; algunos archivos pueden contener código dañino. La descarga de archivos es un permiso específico que se puede configurar. Consulte "Definir funciones y permisos para analistas de malware" en la *Guía de configuración de Malware Analysis* para obtener más detalles.

Para descargar archivos de la Lista de archivos o la Lista de eventos:

1. En la **Lista de archivos** o la **Lista de eventos**, seleccione la casilla de verificación junto a una o más filas.
2. En la barra de herramientas, seleccione 

.
   Se muestra el cuadro de diálogo Descarga de archivo de malware.
3. Realice una de las siguientes acciones:
   a. Si decide no descargar el archivo, haga clic en **Cancelar**.
   b. Si desea descargar el archivo, haga clic en el botón **Descargar**.
      El archivo o los archivos seleccionados se descargar en un archivo zip con el nombre `Malware_Files.zip`.

Eliminar eventos del escaneo

En la Lista de eventos, seleccione uno o más eventos y elimínelos del escaneo. Esto es útil para eliminar eventos que no le interesan.

Para eliminar un evento del escaneo que se visualiza:

1. En la **Lista de eventos**, seleccione uno o más eventos.
2. En la barra de herramientas, haga clic en 

.
   NetWitness Platform solicita que confirme su intención de eliminar los eventos.
3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.
   Se eliminan los eventos seleccionados.

Volver al resumen de eventos

Para salir de la Lista de archivos o la Lista de eventos y volver al Resumen de eventos, haga clic en **Volver al resumen**.

Abra el análisis detallado de un evento

Mientras examina eventos o archivos en la Lista de archivos o la Lista de eventos, puede hacer doble clic en cualquier evento o archivo para abrir un análisis detallado del evento en la Lista de eventos o el evento con el cual está asociado el archivo en la Lista de archivos (consulte Ver detalles de Malware Analysis de un evento).

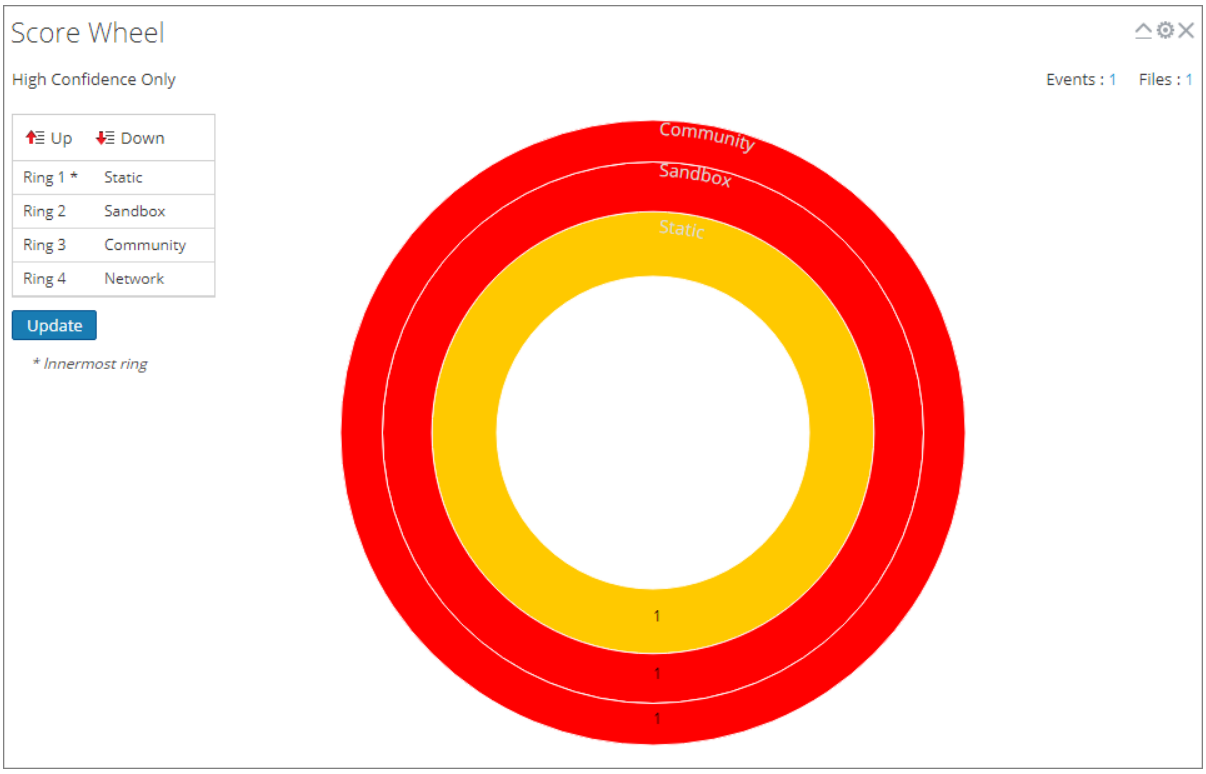
Filtrar datos de dashlets en la vista Resumen de eventos

La vista Resumen de eventos ofrece un resumen del escaneo que se investiga e incluye dashlets seleccionables. El Resumen de eventos es fijo, pero los analistas pueden configurar cada dashlet para filtrar la información y desglosar los datos.

El resto de este tema proporciona instrucciones para administrar y configurar los dashlets.

Configurar el dashlet Rueda de puntaje

La Rueda de puntaje es una visualización general de las sesiones analizadas que puntuaron alto, medio o bajo en cada una de las categorías de puntaje: Estático, Red, Community y Sandbox. La Rueda de puntaje es una forma rápida de desglosar las sesiones para revisarlas. Cada anillo representa una categoría de puntaje diferente, de modo que pueda comparar visualmente los resultados por categoría.



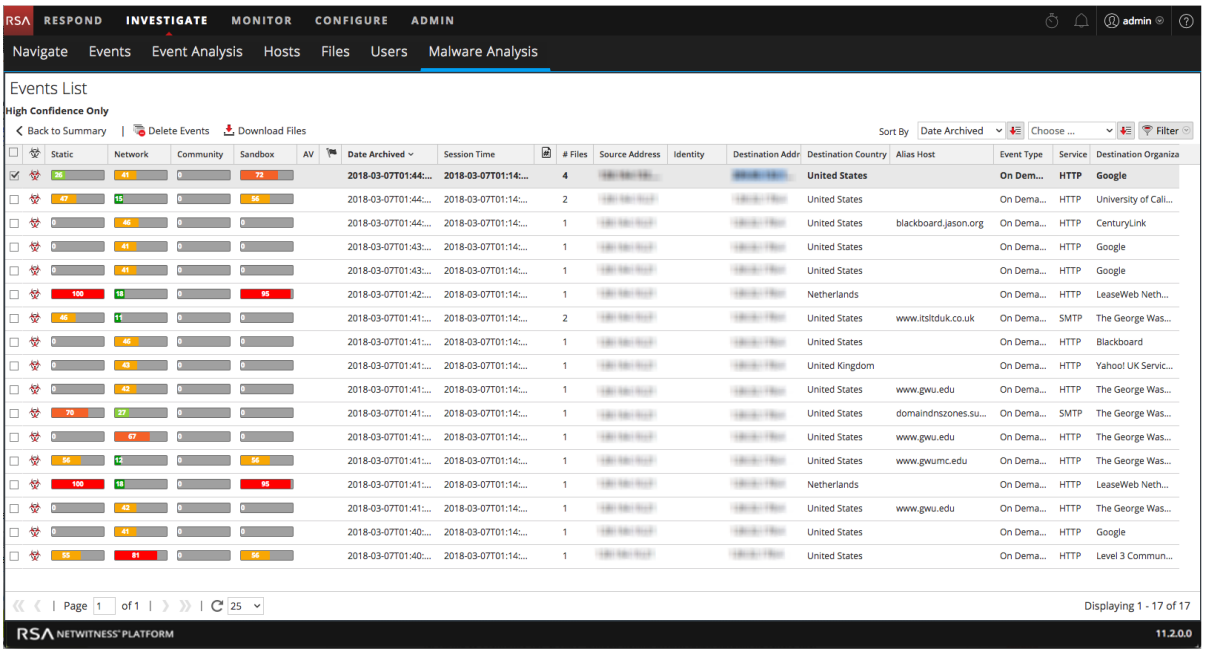
Puede cambiar el orden de los anillos para resaltar los indicadores de riesgo que se marcaron en una categoría, pero no en otra. La comparación de los mismos resultados en una secuencia de anillos diferente proporciona visibilidad de las vulnerabilidades adicionales en una sesión y se permite desglosar a sesiones de interés. En los siguientes ejemplos se muestran dos posibles casos de uso.

Ejemplo de candidatos de día cero

En este ejemplo se muestra cómo desglosar sesiones que Community no marcó como maliciosas, pero que todas las demás categorías de puntaje marcaron como maliciosas. La lista de sesiones resultante resalta los candidatos de día cero.

1. Configure los anillos de la rueda de puntaje en la siguiente secuencia:
   Comunidad (más interior) > **Estático** > **Red** > **Sandbox** (más exterior)

2. Haga clic en el segmento rojo del anillo más exterior (Sandbox) que se alinea con un segmento verde del anillo más interior (Comunidad): verde (más interior) -> **Estático**: rojo -> **Red**: rojo -> **Sandbox**: rojo (más exterior).



Ejemplo de sesiones maliciosas

En este ejemplo se muestra cómo desglosar sesiones en las que todas las categorías de puntaje identifican la lista de sesiones resultante como maliciosa, lo cual indica que Malware Analysis tiene la máxima confianza de que corresponden a malware.

1. Configure los anillos de la rueda de puntaje en la siguiente secuencia:
   Comunidad (más interior) > **Estático** > **Red** > **Sandbox** (más exterior)
2. Haga clic en el segmento rojo del anillo más exterior (Sandbox) que se alinea con un segmento rojo del anillo más interior (Comunidad): rojo (más interior) -> Estático: rojo -> Red: rojo -> Sandbox: rojo (más exterior).

Organizar la secuencia de los anillos por módulo de puntaje

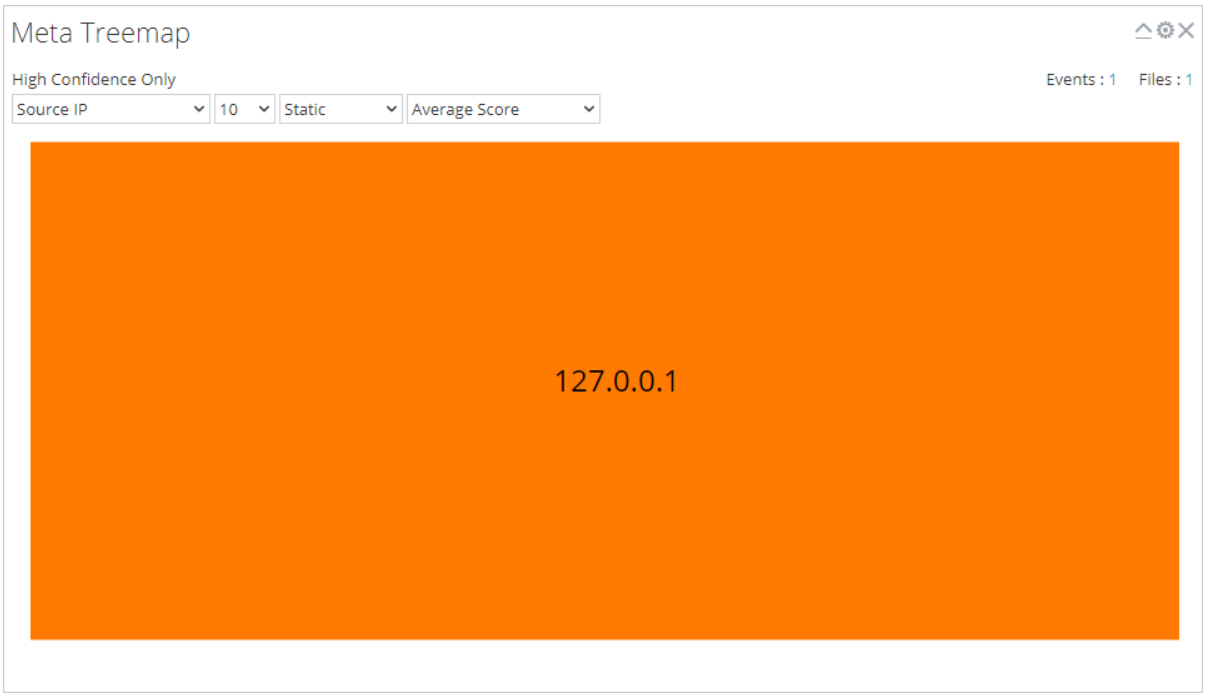
En la Rueda de puntaje, puede organizar la secuencia de los anillos por módulo de puntaje. Inicialmente, la secuencia de anillos del interior al exterior es Estático, Red, Community y Sandbox.

Para cambiar la secuencia de los anillos:

1. Realice una de las siguientes acciones:
   a. Haga clic y arrastre cada módulo de puntaje hacia arriba o abajo.
   b. Seleccione cada módulo de puntaje y utilice los botones Arriba y Abajo para transferirlo.
2. Cuando esté conforme con la secuencia de anillos, haga clic en el botón **Actualizar**.
   La Rueda de puntaje se actualiza con la secuencia nueva.

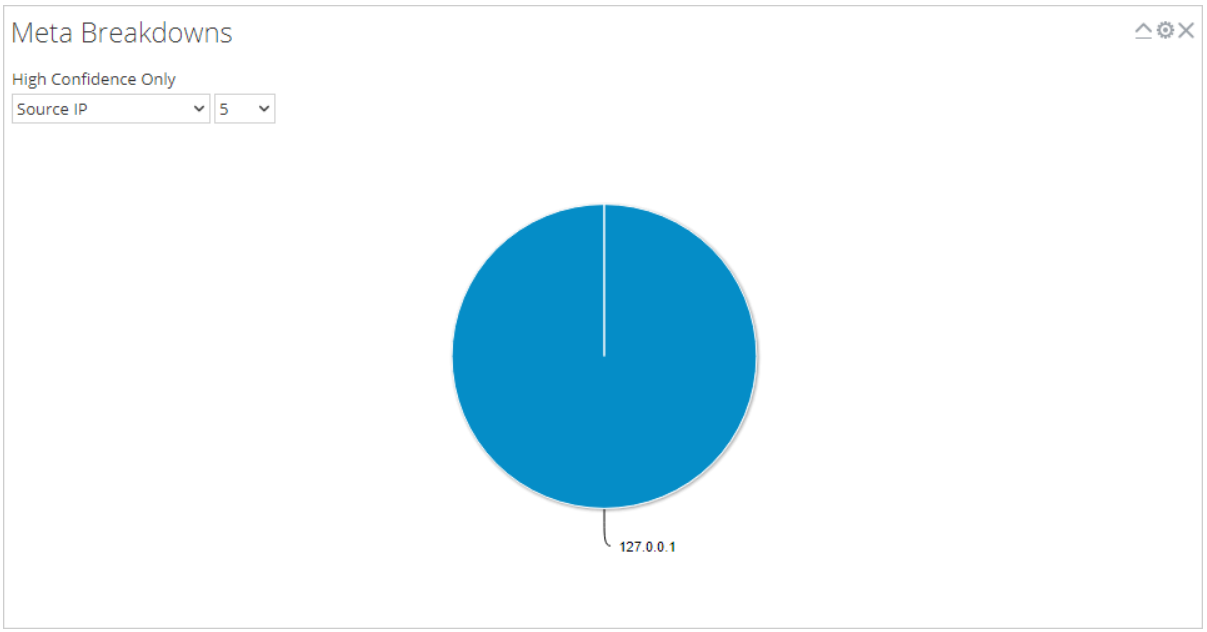
Configurar el dashlet Mapa de árbol de metadatos

En el gráfico Mapa de árbol de metadatos, puede visualizar y filtrar desgloses de metadatos por tipo, conteo y tipo de análisis de metadatos. Utilice las tres listas de selección para definir el filtro y el gráfico Mapa de árbol de metadatos se actualiza inmediatamente.



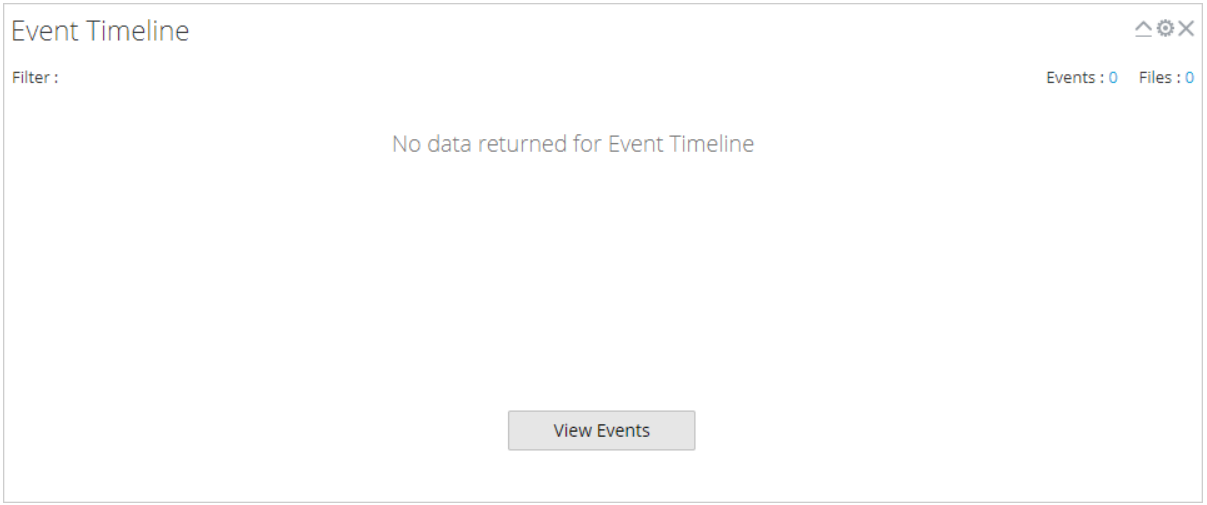
Configurar el dashlet Desgloses de metadatos

El dashlet Desgloses de metadatos es una visualización de valores para una clave de metadatos específica en un gráfico circular. En el gráfico Desgloses de metadatos, puede filtrar desgloses de metadatos por tipo y conteo de metadatos. Utilice las dos listas de selección para definir el filtro y el gráfico Desgloses de metadatos se actualiza inmediatamente.



Configurar el dashlet Cronograma de eventos

El dashlet Cronograma de eventos es una visualización de los eventos en un cronograma. No hay filtros adicionales disponibles para el Cronograma de evento.

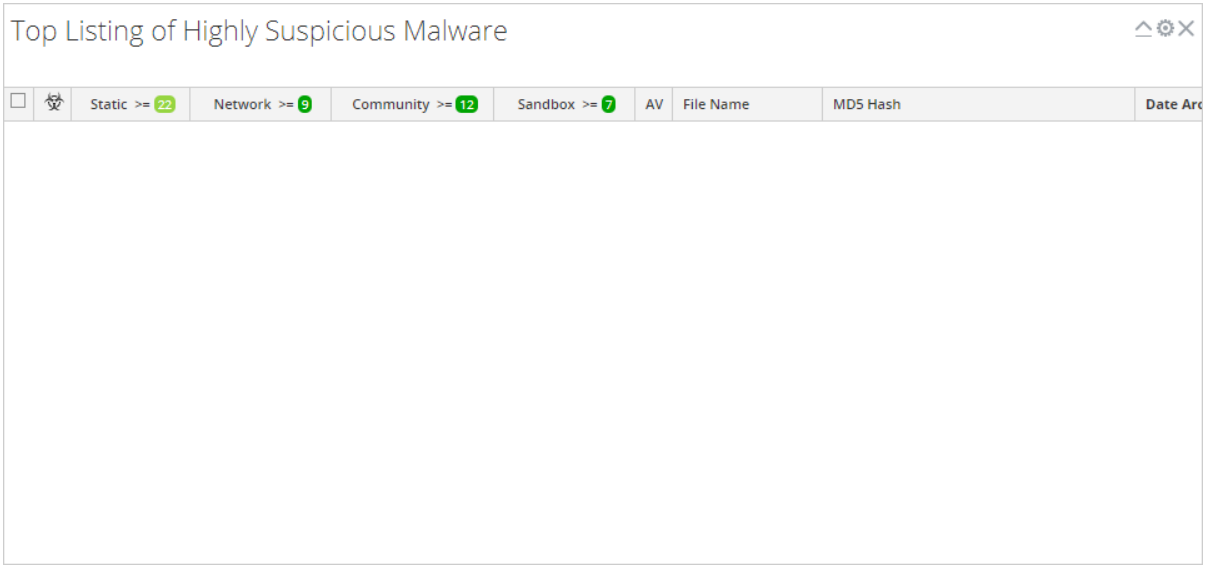


Abrir todos los eventos en la lista de eventos

Desde el Cronograma de evento, puede abrir la lista de eventos completa en la Lista de eventos. Para ello, haga clic en **Ver eventos**. Esta opción no es igual que hacer clic en el conteo junto a Eventos, que es el mismo para todos los gráficos de visualización y abre el punto de desglose actual en la Lista de eventos.

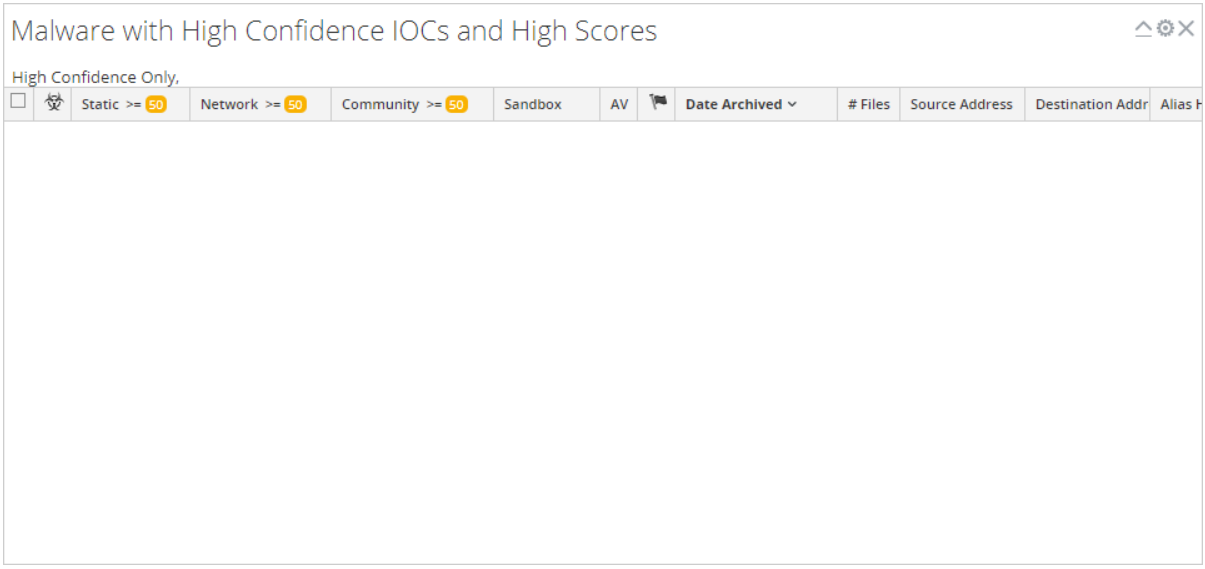
Configure el dashlet Lista del malware altamente sospechoso principal

El dashlet Lista del malware altamente sospechoso principal presenta los 10 eventos más sospechosos en la Lista de eventos o en la Lista de archivos. Este dashlet también está disponible en el tablero Monitor y las opciones de configuración se describen como parte del contenido de RSA NetWitness en Dashlets.



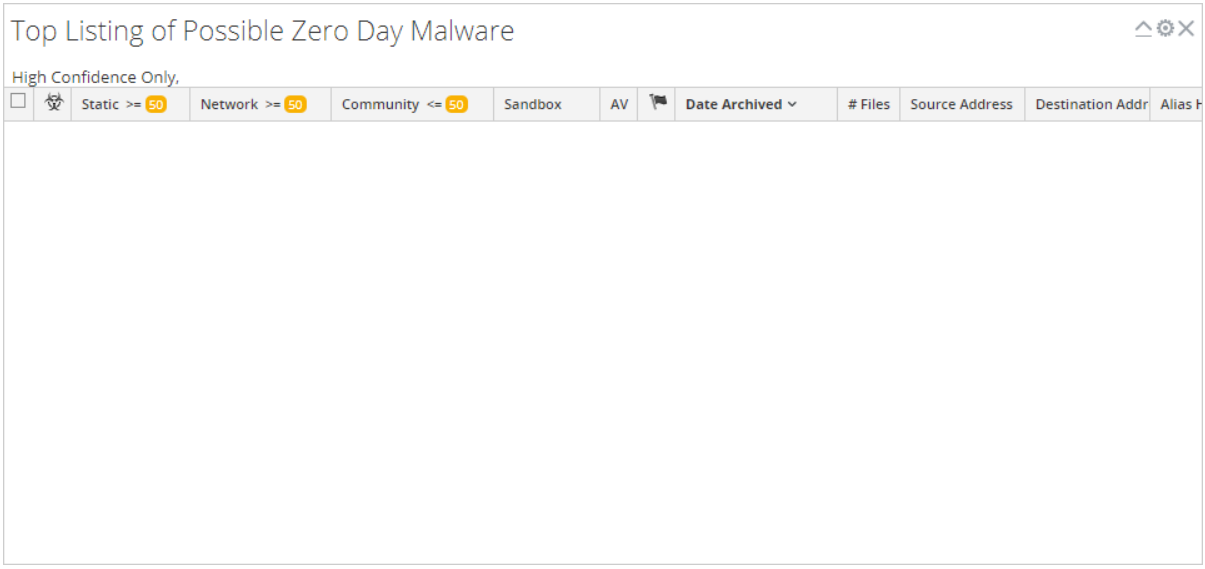
Configurar el dashlet Malware con IOC de alta confianza y altos puntajes

El dashlet Malware con IOC de alta confianza y altos puntajes presenta indicadores de riesgo que tienen puntajes altos y confianza alta de que es probable que los eventos contengan malware. El dashlet también está disponible en el tablero Unified y las opciones de configuración se describen como parte del contenido de RSA NetWitness en Dashlets.



Configurar el dashlet Lista del posible malware de día cero principal

El dashlet Lista del posible malware de día cero principal presenta posibles eventos de día cero en la Lista de eventos o la Lista de archivos. El dashlet también está disponible en el tablero Unified y las opciones de configuración se describen como parte del contenido de RSA NetWitness en Dashlets.



Cargar archivos para escaneo de Malware Analysis

Existen dos métodos para que los analistas carguen archivos para su escaneo en Malware Analysis.

Un analista de malware con permiso para Iniciar escaneo de Malware Analysis puede cargar archivos para escanear mediante la opción Escanear archivos del cuadro de diálogo Seleccionar un servicio Malware Analysis.

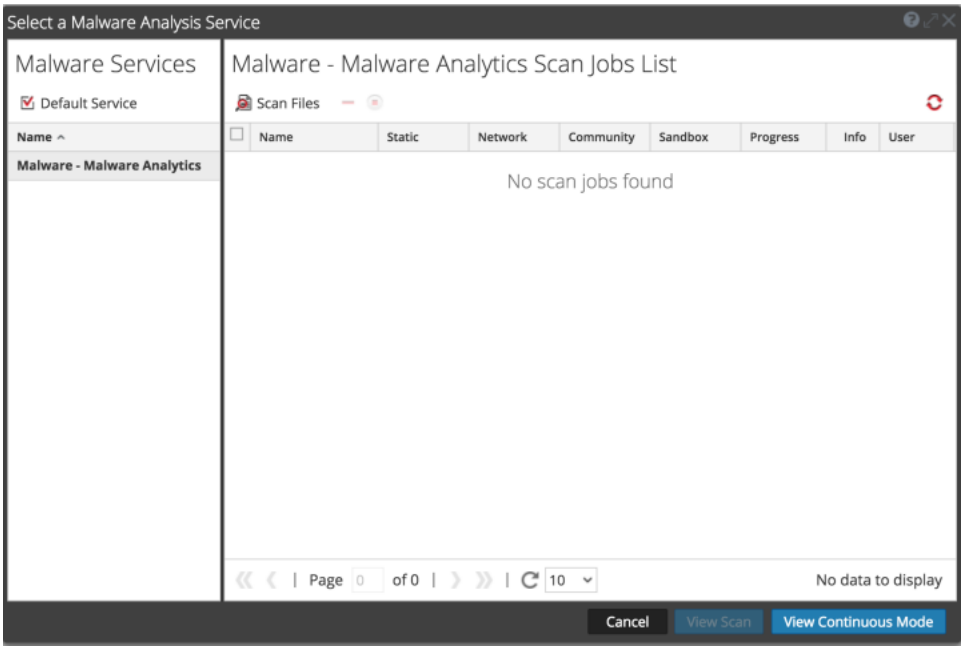
También es posible cargar un archivo para su escaneo mediante un recurso compartido de archivos inspeccionados.

Cargar archivos manualmente

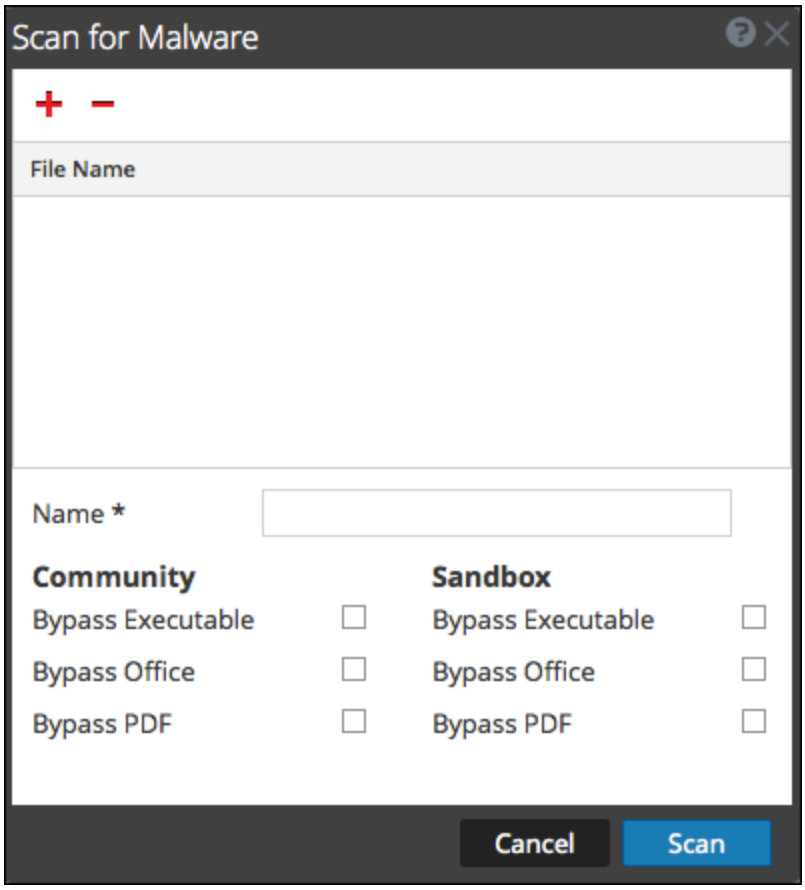
En este tema se proporcionan instrucciones para iniciar un escaneo por demanda de un archivo cargado. Al cargar un archivo para escanear, NetWitness Platform inicia el trabajo de carga y lo agrega a la línea de espera de trabajos. Cuando el trabajo ha finalizado, puede ver el escaneo en Malware Analysis.

Para cargar un archivo para escanear:

1. Vaya a **INVESTIGAR > Malware Analysis**.
   Se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis con hosts y servicios de Malware Analysis disponibles para el usuario actual en el panel de la izquierda.



2. Haga clic en **Ver escaneo**.
   Se muestra el cuadro de diálogo Escanear para encontrar malware.



3. Haga clic en +
   Se muestra una vista del sistema de archivos que permite elegir los archivos que cargará.
4. Seleccione uno o más archivos de la lista y haga clic en **Abrir**.
   Se agregan los nombres de archivo. Malware Analysis agrega un carácter de escape a los caracteres del nombre de archivo antes de procesar un archivo. La cantidad máxima de caracteres del nombre de archivo después del carácter de escape es 200. Si el nombre de archivo tiene más de 200 caracteres, Malware Analysis trunca caracteres del nombre de archivo y muestra el nombre de archivo truncado en la interfaz del usuario de NetWitness Platform.
5. Continúe agregando y eliminando archivos hasta que tenga una lista de los archivos que desea cargar.
6. Nombre el escaneo y seleccione los tipos de archivos que desea omitir. Esto es útil para un archivo .zip que contenga tipos de archivos diferentes y sobrescribe la configuración de omisión predeterminada.
7. Haga clic en **Escanear**.
   El trabajo de escaneo se envía y NetWitness Platform muestra un mensaje de confirmación que indica que el envío se realizó correctamente. La solicitud de escaneo se agrega al dashlet Lista de trabajos de escaneo. La configuración de omisión en este cuadro de diálogo reemplaza a la configuración predeterminada definida en los ajustes de configuración básicos de Malware Analysis.

8. El trabajo se agrega a la Lista de trabajos de escaneo del cuadro de diálogo Seleccionar un servicio Malware Analysis y del dashlet Lista de trabajos de escaneo del tablero Unified.
9. Para ver el escaneo cuando finalice, haga doble clic en él.
   Se muestra el Resumen de eventos de malware del escaneo seleccionado.

Cargar archivos desde una carpeta inspeccionada

Para cargar archivos desde una carpeta inspeccionada, puede soltarlos en un recurso compartido de archivo inspeccionado para Malware Analysis. Los analistas pueden compartir reglas YARA, archivos de hash y archivos zip infectados con Malware Analysis.

Malware Analysis inspecciona un recurso compartido de archivo y consume automáticamente los archivos que se colocan en carpetas específicas de dicho recurso compartido. Esta función es útil para:

- La importación en masa de archivos de hash desde `/var/lib/rsamalware/spectrum/hashWatch`.
- La adición de reglas YARA personalizadas a la lista de indicadores de riesgo (IOC) en el host desde `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`.
- La creación de trabajos de escaneo según demanda a partir de un archivo Zip de archivos Zip infectados desde `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Los analistas deben preparar los archivos para el consumo de acuerdo con los requisitos, la extensión del archivo debe estar correcta y el archivo debe copiarse a la carpeta inspeccionada correcta en el recurso compartido de archivo.

Importar una lista de hash

Para importar una lista de hash desde el directorio inspeccionado, la lista debe tener el formato especificado y estar clasificada por md5. Puede soltar un archivo con formato en una carpeta (`/var/lib/rsamalware/spectrum/hashWatch`) del host de Malware Analysis y se importará automáticamente a la base de datos de hash local. Esto se describe en “Configurar el filtro de hash” en la *Guía de configuración de Malware Analysis*.

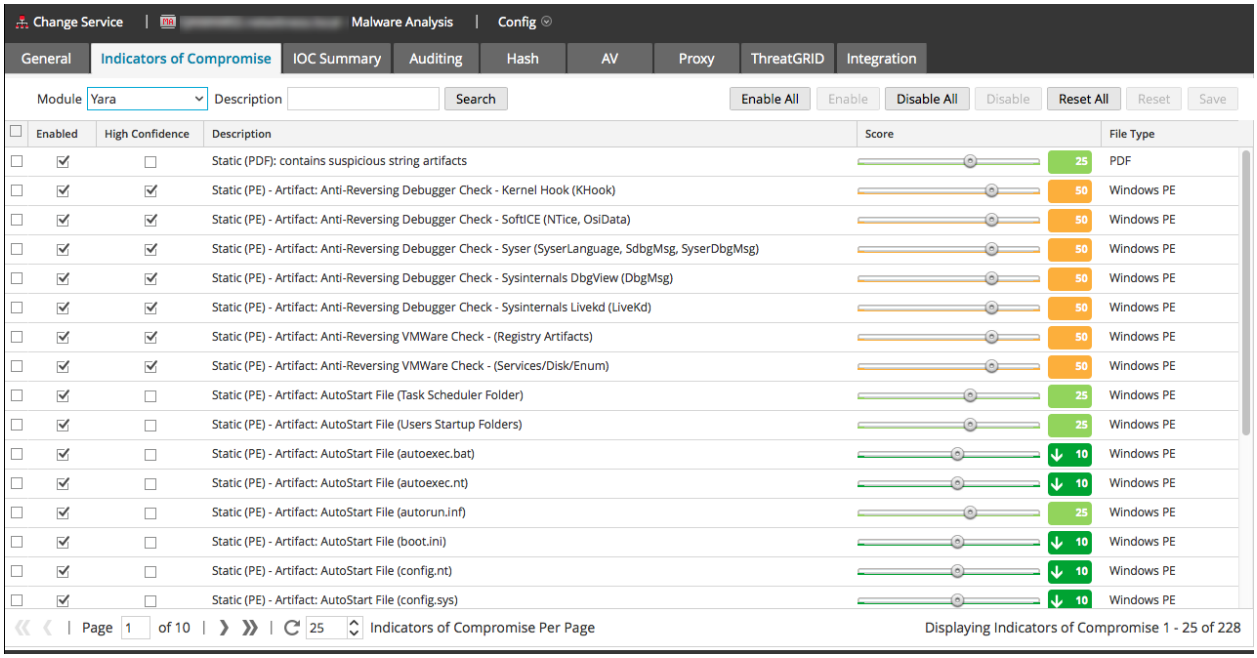
Para importar una lista de hash mediante el método de carpeta inspeccionada:

1. Copie las listas de hash que desea importar en el directorio **`/var/lib/rsamalware/spectrum/hashWatch`** .
   NetWitness Platform Malware Analysis inspecciona automáticamente esta carpeta y procesa los archivos que contiene.
   a. Malware Analysis agrega cada hash encontrado en las listas de hash al filtro de hash.
   b. Si se producen errores de procesamiento, se registran en: `/var/lib/rsamalware/spectrum/hashWatch/error`
   c. Los archivos procesados se catalogan aquí: `/var/lib/rsamalware/spectrum/hashWatch/processed`
   d. Los archivos procesados no se eliminan del directorio hashWatch.
2. Después de importar hashes de forma masiva, el administrador del sistema puede usar un cronjob para limpiar archivos procesados antiguos.

Importar reglas YARA a la lista de IOC

Los clientes con habilidades y conocimientos avanzados pueden agregar funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live o la colocación de estas reglas en una carpeta inspeccionada para consumo del host. En Implementar contenido personalizado de YARAse proporciona información completa sobre los requisitos previos para el uso de contenido personalizado de YARA y reglas de autoría.

Cuando las reglas estén listas, coloque los archivos de YARA personalizados en la carpeta que inspecciona el servicio Malware Analysis:
`/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
El archivo se consume en un minuto.
Cuando se consume, NetWitness Platform lo transfiere a la carpeta `processed` y la nueva regla se agrega a la vista Configuración de servicios > pestaña Indicadores de riesgo de Malware Analysis.



Importar archivos a la Lista de trabajos de escaneo

Cuando obtiene muestras de soluciones de seguridad perimetral y desea realizar un análisis adicional de los archivos, puede comprimirlos y proteger el archivo con `infected` y, a continuación, agregarlo a la carpeta inspeccionada para que Malware Analysis lo consuma. Este archivo comprimido se puede colocar en la carpeta inspeccionada:
`/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Nota: El tamaño máximo del archivo es 100 MB.

Para analizar archivos zip protegidos con contraseña que están infectados, Malware Analysis consume los archivos que se colocan en una carpeta inspeccionada y crea un trabajo según demanda que se agrega a la Lista de trabajos de escaneo.

1. Cuando haya iniciado sesión como administrador, coloque los archivos que se procesarán en un archivo zip con la contraseña `infected` en
   `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`
   En uno o dos minutos, Malware Analysis consumirá el archivo y creará un trabajo según demanda

en la Lista de trabajos de escaneo. El nombre del trabajo de escaneo es el nombre del archivo, el usuario es **file share**, y el tipo de evento es 1. El archivo se transfiere a `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`

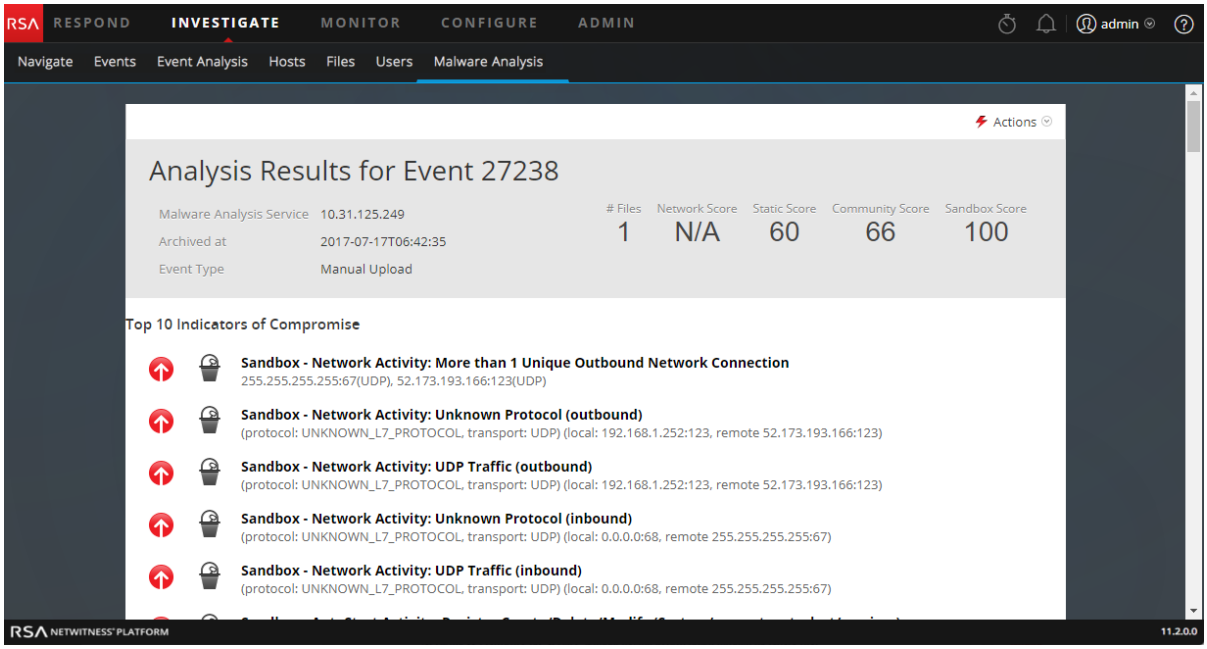
2. Cuando el trabajo se haya agregado a la Lista de trabajos de escaneo, ejecute un script o un cronjob para limpiar el archivo Zip en `/var/lib/rsamalware/spectrum/infectedZipWatch/processed`.

Ver detalles de Malware Analysis de un evento

Cuando observa la lista de eventos individuales en un escaneo de Malware Analysis en la cuadrícula Eventos de Malware Analysis, puede hacer doble clic en un evento para ver sus resultados de análisis detallados.

Ver detalles de Malware Analysis para un evento

1. Inicie una investigación en la pestaña **Malware Analysis**.
   Se muestra el Resumen de eventos de malware, el cual incluye cuatro gráficos, entre ellos, el Cronograma de evento.
2. Realice una de las siguientes acciones:
   a. Para ver todos los eventos en el Cronograma de evento, haga clic en el botón **Ver eventos**.
   b. Haga doble clic en los datos en el **Desglose de metadatos**, **Gráfico Mapa de árbol de metadatos** o **Rueda de puntaje**.
      Se muestra la Lista de eventos.
3. Haga doble clic en un evento.
   Se muestran los Resultados de análisis para el evento.

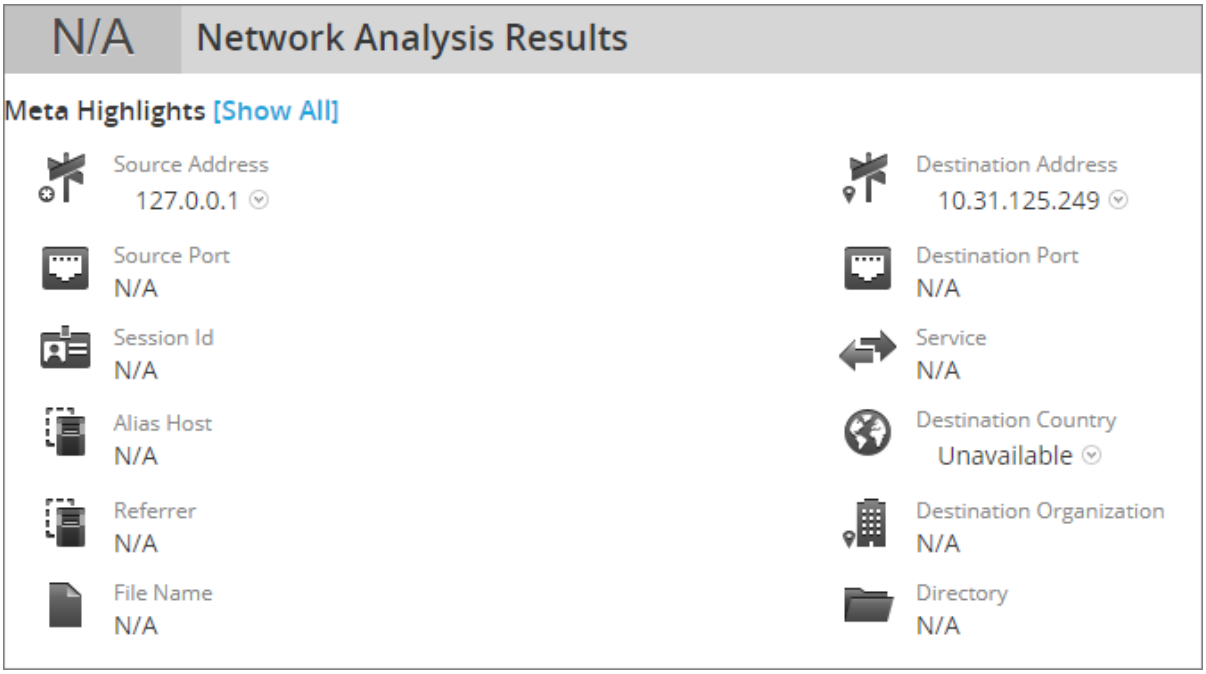


4. (Opcional) Si desea eliminar un evento, seleccione **Acciones > Eliminar evento**.
5. Si desea ver una reconstrucción de la sesión de red, seleccione **Acciones > Ver sesión de red**.
   La sesión se abre en la vista Navegar > Reconstrucción de evento.

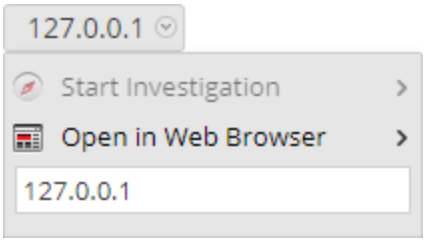
Agilizar resultados de análisis de la red

Puede agilizar los resultados de análisis de la red de varias formas:

1. Desplácese hacia abajo hasta Resultados de análisis de la red.



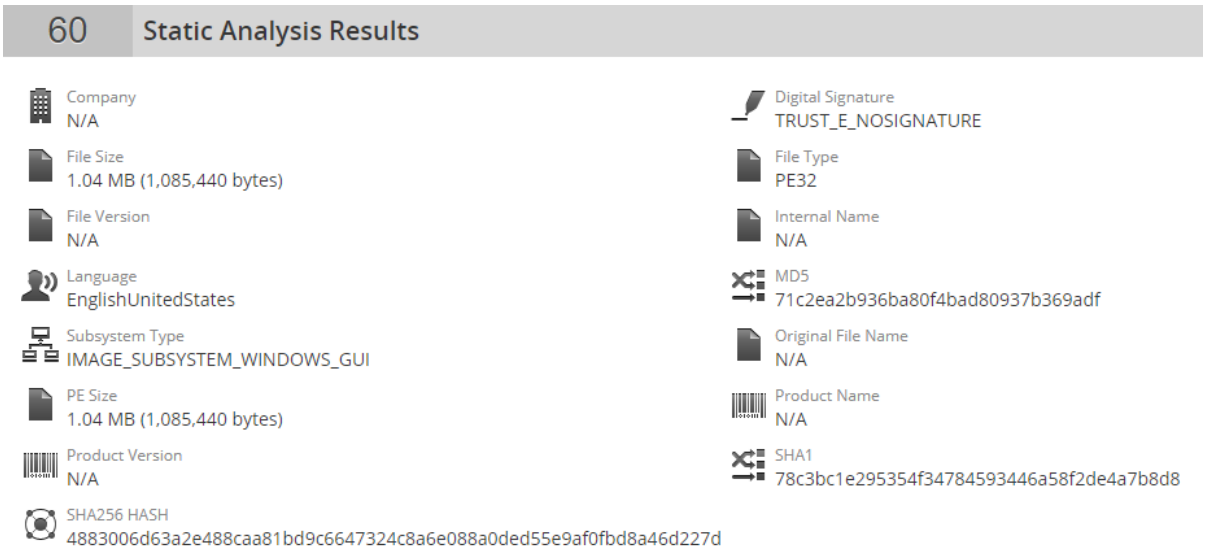
2. Coloque el cursor sobre un valor de metadatos y haga clic con el botón primario.
   Se muestra el menú contextual.



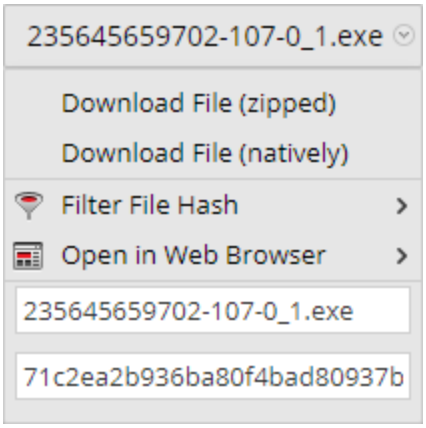
3. Para ver el valor de metadatos seleccionado en la vista **Navegar**, seleccione **Iniciar investigación** y una opción de tiempo.
4. Para ver el valor de metadatos seleccionado en un navegador, seleccione **Abrir en el navegador web > Abrir en Google**.

Utilizar acciones de archivo en los resultados de análisis estático.

1. Desplácese hacia abajo hasta Resultados del análisis estático.



2. Si desea descargar un archivo, seleccione el nombre de archivo y **Descargar archivo (comprimido)** o **Descargar archivo (nativamente)** en el menú desplegable. Es más seguro descargar un archivo en formato comprimido.



3. Si desea marcar el archivo como seguro o no seguro en la lista de hash, seleccione **Filtrar hash de archivo** y **Marcar hash como correcto** o **Marcar hash como incorrecto**.

Ver detalles de Resultados de análisis de Community

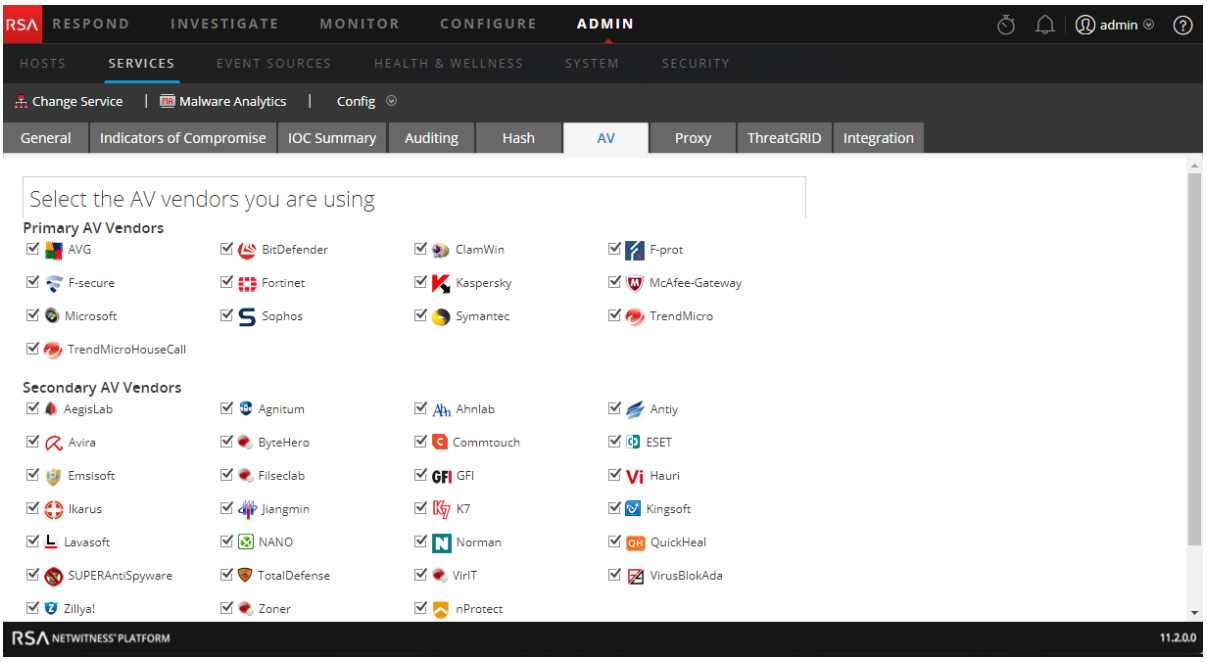
Los Resultados de análisis de Community resumen los resultados de la comunidad y muestran indicadores de riesgo que se señalaron como un riesgo o se identificaron como seguros.

Además, en esta vista se indican los resultados de los proveedores de antivirus instalados y no instalados. Puede comparar los resultados de los proveedores de antivirus instalados que se configuraron para el servicio Malware Analysis actual con los de la Comunidad. También puede ver los resultados de una lista de proveedores de antivirus que no están configurados como instalados para el servicio Malware Analysis actual.

Cada fila de los resultados de los proveedores de antivirus incluye el ícono de escudo para mostrar si al IOC lo descubrió un proveedor de antivirus primario ( ) o uno secundario ( ) en la comunidad, el nombre del proveedor instalado o no instalado y el nombre del malware o del riesgo que detectó la comunidad y el proveedor de antivirus. Si el proveedor de antivirus no detectó un riesgo, se muestra **-- No detectado --** en lugar del nombre del riesgo.

La sección Proveedores de antivirus no instalados se puede expandir para ver todas las entradas, pero está contraída de manera predeterminada para minimizar la necesidad de desplazamiento. Para expandir la lista, haga clic en el signo +.

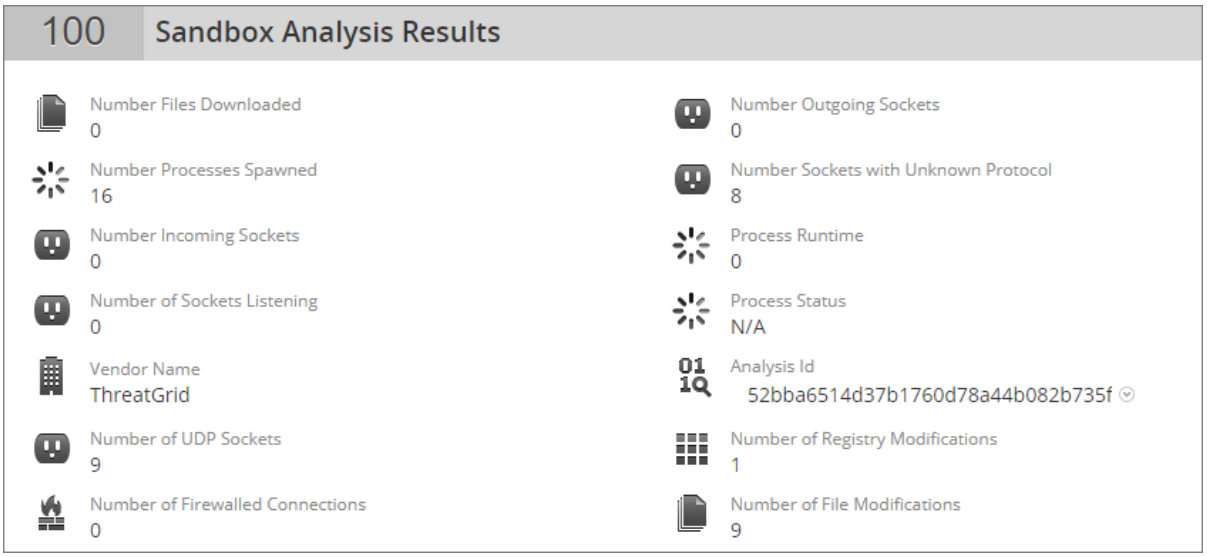
Si no se configuraron proveedores de antivirus instalados para el servicio de Malware Analysis actual, se muestra el siguiente mensaje: Ningún proveedor de antivirus se marcó como instalado. Vaya a la página Configuración del servicio Malware Analysis para identificar a los proveedores de antivirus instalados.



Ver resultados de análisis de Sandbox en la interfaz del usuario de ThreatGrid

Si se registró en ThreatGrid, puede ver los resultados de Sandbox directamente en ThreatGrid.

1. Desplácese hacia abajo hasta Resultados de análisis de Sandbox.



2. Haga clic en el **ID de análisis** y seleccione **Abrir en ThreatGrid**.
   Se muestra el informe de análisis en ThreatGrid.

Solución de problemas de NetWitness Investigate

En esta sección se proporciona información sobre posibles problemas durante el uso de NetWitness Investigate.

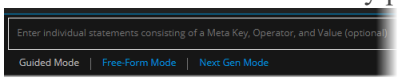
Problemas de las vistas Navegar y Eventos

Mensaje	`Not indexed; will experience longer than usual load times.` en el cuadro de diálogo Administrar grupos de metadatos.
Problema	Las claves de metadatos del cuadro de diálogo Administrar grupos de metadatos se marcan con un signo de exclamación rojo y se muestra el mensaje de error. Esto puede ocurrir cuando se investiga un Broker o un Decoder y se agrega un grupo de metadatos con claves de metadatos que no están indexadas en el archivo de índice ni en el archivo de índice personalizado para el servicio. Para un Broker, podría significar que este no ha comenzado a agregar datos desde un Concentrator. En este caso, el Broker no tendrá el contenido del archivo de índice personalizado de los servicios agregados y las claves no estarán indexadas. Para un Decoder, significa que las claves de metadatos no están indexadas en el índice del Decoder ni en el archivo de índice personalizado.
Explicación	Para corregir el problema en un Broker, cierre la sesión, inicie sesión y reinicie el servicio Broker para que pueda agregar la información de claves de metadatos de Concentrators conectados. Para corregir el problema en un Decoder, edite el archivo de índice personalizado para indexar las claves de metadatos, cierre sesión, inicie sesión y reinicie el servicio Decoder.

Comportamiento	Cuando se descargan desde la vista Reconstrucción de evento, los registros y los metadatos siempre están en formato de texto, independientemente del formato seleccionado en la vista Eventos.
Problema	Cuando descarga metadatos o un registro en la vista Reconstrucción de evento, el formato que seleccionó en la vista Eventos no se utiliza. Los datos exportados siempre están en formato de texto.
Explicación	Descargue metadatos y registros desde la vista Eventos si desea usar un formato distinto del formato de texto.

Problemas de la vista Análisis de eventos

Comportamiento	El generador de consultas en la versión 11.2 incluye el Modo de última generación, una característica beta no documentada.
Problema	En la versión 11.2 se incluyó una característica beta no documentada, denominada

Explicación	modo de Última generación, en la vista Análisis de eventos del generador de consultas, que aún estaba en fase de desarrollo y pruebas. El modo de Última generación se deshabilitó en el parche 11.2.0.1. Si ve el modo de Última generación, no lo use; debe utilizar solamente el Modo guiado y el Modo de formato libre en el generador de consultas para asegurarse de obtener resultados coherentes y predecibles. 

Mensaje	`Investigation Profiles/OOTB column groups are not present in Event Analysis`
Problema	Posterior a la actualización a RSA NetWitness v11.1, los grupos de columnas predeterminados (Análisis de Endpoint, Protocolo SSL de salida y HTTP de salida) no se agregaron bajo los grupos de columnas. Además, después de la actualización, faltan algunos de los perfiles de Investigation.
Explicación	Se puede observar que este problema ocurre solo cuando crea un grupo de columnas personalizado con un nombre que es igual al nombre del nuevo grupo de columnas personalizado de uso inmediato de 11.1. Por ejemplo, si crea un grupo de columnas personalizado en 11.0 con el nombre **Análisis de RSA Endpoint**, entonces este después se actualiza a 11.1. Debido a que el mismo nombre ya existe en 11.1, los grupos de columnas de uso inmediato y los perfiles de uso inmediato no estarán disponibles en la interfaz del usuario. Para solucionar esto, cambie el nombre del grupo de columnas personalizado por otro nombre y reinicie el servidor Jetty mediante el siguiente comando en el servidor de NetWitness: `systemctl restart jetty`

Mensaje	`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`
Problema	Cuando hace clic en **Cambiar a Endpoint** en la vista Análisis de eventos, no se muestran datos y aparece el mensaje.
Explicación	La versión 4.4 del cliente grueso de NetWitness Endpoint debe estar instalada en el mismo servidor, las claves de metadatos de NWE deben existir en el archivo `table-map.xml` en el Log Decoder y las claves de metadatos de NWE deben existir en el archivo `index-concentrator-custom.xml`. El cliente grueso de NWE es una aplicación solo de Windows. En la *Guía del usuario de NetWitness Endpoint* para la versión 4.4 se proporcionan instrucciones de configuración completas.

Mensaje	`Event Analysis requires all core services to be NetWitness 11.1. Connecting prior versions of services to the 11.1 NetWitness Server results in limited functionality (see "Investigate in Mixed Mode" in the *Physical Host Upgrade Guide*).`

Problema	Cuando intenta investigar un servicio que no se ha actualizado a la versión 11.1 en la vista Análisis de eventos, se muestra el mensaje informativo.
Explicación	Cuando un analista abre la vista Análisis de eventos en modo mixto (es decir, algunos servicios están actualizados a 11.1 y otros aún están en 11.0.0.x o 10.6.x), el acceso basado en funciones (RBAC) no se aplica de manera uniforme. Esto afecta el proceso de ver y descargar el contenido y la validación de los filtros en la ruta de navegación interactiva. Verá este mensaje informativo cuando abra Análisis de eventos. Cuando selecciona un servicio, los servicios que no están actualizados se muestran en un recuadro rojo, con el mensaje que indica que el servicio no está actualizado. Cuando el administrador ha actualizado todos los servicios conectados a 11.1, estas funciones funcionan según lo previsto.

Mensaje	`Forbidden. You cannot access the requested page.`
Problema	Al intentar acceder a la vista Análisis de eventos, la vista se abre con el mensaje.
Explicación	El administrador ha impedido el acceso a la vista Análisis de eventos con función y permisos.

Mensaje	`Insufficient permissions for the requested data.`
Problema	Al intentar acceder a un evento en Análisis de eventos por cualquier medio, no se muestra la reconstrucción y aparece el mensaje.
Explicación	Ingresó un ID de evento para un evento que no tiene permiso para verlo. Es posible que el administrador haya aplicado algunas restricciones para limitar el acceso por función y permisos.

Mensaje	`Invalid session ID: <<eventId>>`
Problema	Ningún `sessionId` coincide con el `sessionId` que consultó.
Explicación	El motivo por el cual un ID de sesión no es válido puede variar. Tal vez editó el ID de sesión manualmente y no existe esa sesión. Otro caso puede ser cuando consulta un Broker y no se han actualizado los datos agregados; este error se puede ver para una sesión que ya no existe.

Mensaje	`No text data was generated during content reconstruction. This could mean that the event data was corrupt/invalid, or that an administrator has disabled the transmission of raw endpoint events in the Endpoint server configuration. Check the other reconstruction views.`
Problema	Cuando reconstruye un evento como texto en la vista Análisis de eventos, no se muestran datos y aparece el mensaje.
Explicación	Si no ve el texto crudo en otras reconstrucciones en las vistas Análisis de eventos o

	Eventos y considera que los datos no están dañados ni son no válidos, es probable que el administrador haya deshabilitado la transmisión de eventos de Endpoint crudos en el servidor de NetWitness Endpoint. Para obtener información adicional, póngase en contacto con el administrador.

Mensaje	`Session is unavailable for viewing.`
Problema	Al consultar un ID de evento, no se muestra la reconstrucción y aparece el mensaje.
Explicación	La consulta que ingresó está intentando ver datos restringidos, por ejemplo, si tiene permiso para ver solamente los datos del registro y está utilizando un vínculo a los datos de red para los que tenía permiso para ver ayer.

Mensaje	`The session id is too large to be handled:<<eventId>`
Problema	El entero sessionId que escribió o editó en las vistas Eventos o Navegar, o que obtuvo de estas, es demasiado grande.
Explicación	Si escribió manualmente el sessionId o editó un sessionId en la vista Análisis de eventos, es posible que haya creado un entero que es demasiado grande para que Análisis de eventos lo pueda procesar.

Comportamiento	Durante la creación de un filtro en la vista Análisis de eventos, no puede ingresar una expresión compleja mediante el operador `AND` o `OR` en el generador de consultas.
Problema	El generador de consultas en la vista Análisis de eventos admite solo expresiones simples en el formulario `<meta key><operator><meta value>`.
Explicación	Si desea ingresar un filtro que utiliza el operador `AND` o `OR`, debe ingresar la consulta desde las vistas Navegar o Eventos y abrirla en la vista Análisis de eventos. Puede ingresar algunas expresiones complejas como dos filtros separados en la vista Análisis de eventos. Se usará el operador Y en los filtros cuando ejecute la consulta.

Problemas en la vista Hosts

Mensaje	`An error has occurred. The Endpoint Server may be offline or inaccessible.`
Problema	Al intentar acceder a las vistas Hosts o Archivos, la vista se abre con el mensaje.
Explicación	El servidor de Endpoint o el servidor de Nginx no están en ejecución. Compruebe el estado del servidor de Endpoint en **Administrar** > **Servicio** o compruebe si la dirección IP del host del servidor de Endpoint está registrada en el servidor de Admin. Para obtener más información, consulte la *Guía de instalación de hosts físicos* o la *Guía de instalación de hosts virtuales*. Si el servicio no está en ejecución, inicie el servidor de

	Endpoint.

Problema	Las vistas Hosts y Archivos no se cargan en el navegador Safari.
Explicación	Cuando abre las páginas de Ember en el navegador Safari con un certificado SSL no confiable, las vistas Hosts y Archivos no se cargan. Para cargar las vistas. 1. Haga clic en el menú emergente **Mostrar certificado**. 2. Habilite la casilla de verificación **Siempre confiar en NetWitness al conectarse a <IP Address>**. 3. Haga clic en **Continuar**. 4. Escriba el nombre de usuario y la contraseña. 5. Haga clic en **Actualizar configuración**.

Mensaje	`No process information was found.`
Problema	Al intentar acceder a la pestaña Proceso o Bibliotecas de la vista Detalles del host, la información detallada del host no está disponible y la vista se abre con el mensaje.
Explicación	Los datos de escaneo no están disponibles debido a alguno de los siguientes motivos: • El escaneo por primera vez no está completo • La política de retención de datos ha eliminado todas las instantáneas de escaneo

Problemas en la vista Archivos

Comportamiento	La carga de valores de metadatos se demora.
Problema	Los valores de metadatos no están configurados para indexarse por valores.
Explicación	Durante la investigación, mientras se cambia a las vistas Navegar o Análisis de eventos desde la vista Archivos, si el nombre de archivo o el hash (SHA256 y MD5) no están configurados para indexarse por valores, los resultados coincidentes tardan en cargarse porque el Concentrator debe generar el índice accediendo a la base de datos de metadatos y recuperando el valor de los metadatos para cada evento. Tendrá que indexar los valores manualmente antes del cambio.

Problema	El filtrado de archivos tarda más en cargar los resultados en la interfaz del usuario.
Explicación	En la vista Archivos, durante el filtrado de archivos con el operador `Contains`, los resultados tardan algunos segundos en cargarse en la interfaz del usuario. Debe utilizar al menos un valor de indexación con el operador `Equals` durante el filtrado de los archivos.

Materiales de referencia de Investigate

Esta sección tiene como objetivo ayudarlo a comprender el propósito y la aplicación de las vistas de NetWitness Investigate. Para cada vista hay una breve introducción y una tabla Qué desea hacer que incluye vínculos a procedimientos relacionados. Además, algunos de los materiales de referencia incluyen flujos de trabajo y vistas rápidas para resaltar las funciones importantes de la interfaz del usuario.

Estas son las vistas principales:

- Vista Investigar
- Vista Navegar
- Vista Eventos
- Vista Análisis de eventos
- Vista Archivos
- Vista Hosts
- Vista Malware Analysis

Esta es una lista alfabética de las otras vistas, paneles y cuadros de diálogo.

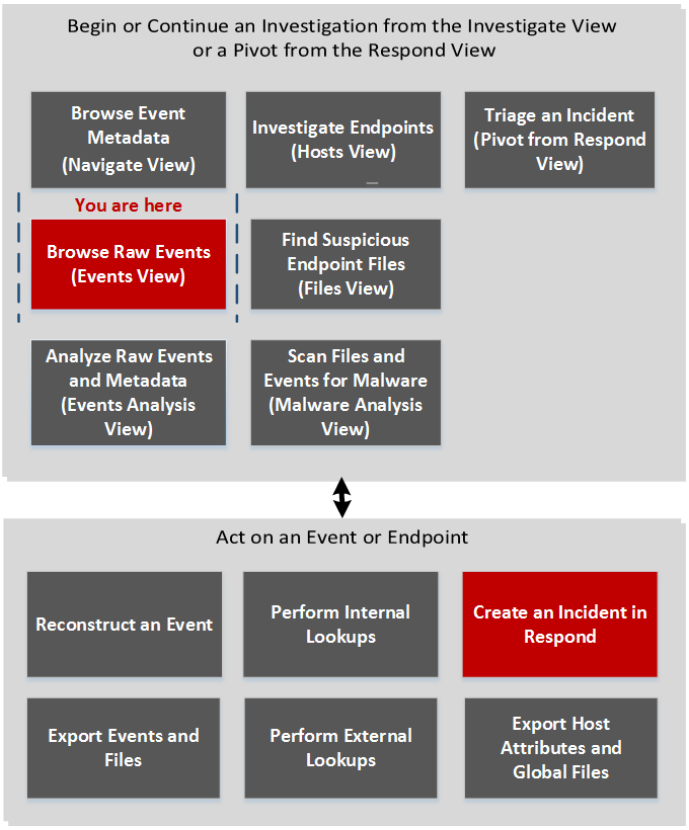
- Cuadro de diálogo Agregar/eliminar de la lista
- Panel Búsqueda de contexto
- Cuadro de diálogo Crear un incidente
- Vista Análisis de eventos
- Vista Análisis de eventos: Panel Análisis de texto
- Vista Análisis de eventos: Panel Análisis de paquetes
- Vista Análisis de eventos: Panel Análisis de archivos
- Vista Reconstrucción de evento
- Vista Hosts: Pestaña Ejecuciones automáticas
- Vista Hosts: Pestaña Controladores
- Vista Hosts: Pestaña Archivos
- Vista Hosts: Pestaña Bibliotecas
- Vista Hosts: Pestaña Descripción general
- Vista Hosts: Pestaña Proceso
- Vista Hosts: Pestaña Información del sistema
- Cuadro de diálogo Investigar
- Pestaña Investigación: Panel Preferencias de usuario

- Lista de eventos y Lista de archivos de Malware Analysis
- Cuadro de diálogo Administrar grupos de columnas
- Cuadro de diálogo Administrar claves de metadatos predeterminadas
- Cuadro de diálogo Administrar grupos de metadatos
- Cuadro de diálogo Administrar perfiles
- Vista Navegar
- Cuadro de diálogo Consulta
- Cuadro de diálogo Escanear para encontrar malware
- Cuadro de diálogo Seleccionar un servicio Malware Analysis
- Cuadros de diálogo de configuración de las vistas de Investigate

Cuadro de diálogo Agregar eventos a un incidente

En el cuadro de diálogo Agregar eventos a un incidente, los analistas pueden agregar alertas a un incidente existente para que los encargados de responder ante incidentes busquen en los eventos asociados como parte de una respuesta ante incidentes. Para acceder a este cuadro de diálogo mientras investiga un servicio en la vista Eventos, seleccione **Incidentes > Agregar a incidente existente** en la barra de herramientas.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas o encargado de respuesta ante incidentes	agregar uno o más eventos a un incidente existente o a un incidente nuevo*	Agregar eventos a un incidente para Response

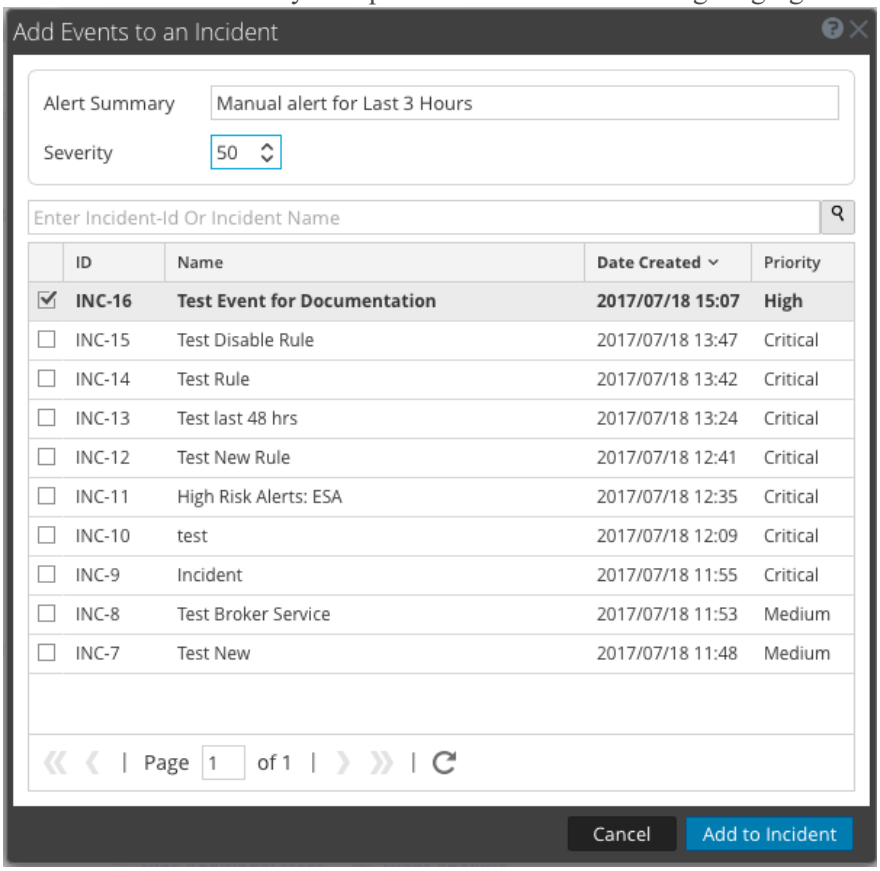
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Eventos

Vista rápida

La siguiente figura es un ejemplo del cuadro de diálogo Agregar eventos a un incidente. En la tabla se describe la información y las opciones del cuadro de diálogo Agregar alertas a un incidente.



Función	Descripción
Resumen de alerta	El campo Resumen de alerta se rellena con la consulta que produjo las alertas seleccionadas, las cuales seleccionó para crear este incidente. El campo Gravedad refleja la gravedad de la alerta seleccionada, un entero entre 1 y 100.
Buscar	Le permite buscar un evento existente.
ID	El ID del incidente. Puede ordenar los ID en orden ascendente o descendente.
Nombre	El nombre del incidente. Puede ordenar el nombre en orden ascendente o descendente.
Fecha de creación	Muestra la fecha y la hora de creación del incidente. Puede ordenar las fechas en orden ascendente o descendente.
Prioridad	Muestra la prioridad del incidente: baja o crítica.
Cancelar	Cierra el cuadro de diálogo sin guardar los cambios.
Agregar a incidente	Agrega las alertas al incidente. Un cuadro de diálogo confirma que las alertas se agregaron correctamente

Cuadro de diálogo Agregar/eliminar de la lista

El cuadro de diálogo Agregar/eliminar de la lista permite agregar una entidad o un valor de metadatos a una lista de Context Hub existente, quitar una entidad o un valor de metadatos o crear una lista de Context Hub nueva que los contiene. Cuando observa una dirección IP u otra entidad y las encuentra sospechosas o interesantes, puede agregarlas a una lista que se ha agregado como un origen de datos. Un ejemplo de una lista de uso común es una lista blanca o una lista negra. Esto mejora la visibilidad de las direcciones IP sospechosas y reduce los falsos positivos que no necesitan una investigación más profunda.

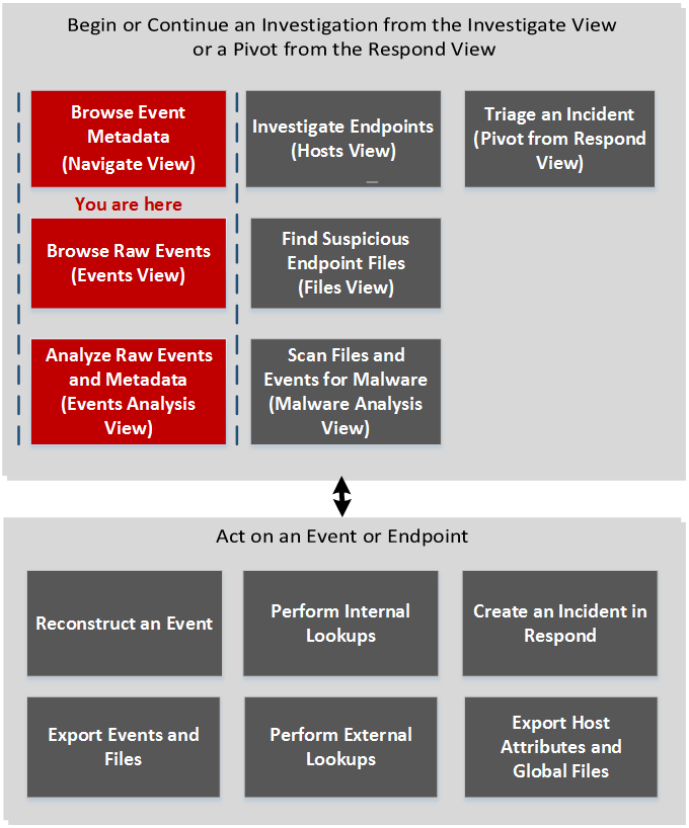
Puede agregar entidades o valores de metadatos a más de una lista. Por ejemplo, puede agregarlos a una lista de dominios sospechosos relacionados con conexiones de comando y control y a otra lista de direcciones IP de conexiones de troyanos relacionadas con el acceso remoto. Si no hay una lista disponible, puede crearla.

El cuadro de diálogo está disponible en NetWitness Investigate y en NetWitness Respond. Cuando trabaja en las vistas Navegar, Eventos o Análisis de eventos de Investigate (versión 11.2), puede agregar valores de metadatos para las claves de metadatos `Source IP`, `Destination IP` o `Username` a una lista de Context Hub existente o crear una nueva lista que contenga los valores de metadatos. Cuando agrega valores de metadatos a una lista, puede buscar contexto adicional en esos valores de metadatos.

- Para mostrar el cuadro de diálogo en las vistas Navegar o Eventos, haga clic con el botón secundario en un valor de metadatos en `Source IP`, `Destination IP` o `Username` y seleccione **Agregar/eliminar de la lista** en el menú contextual.
- Para mostrar el cuadro de diálogo en la vista Análisis de eventos, coloque el cursor sobre un valor y seleccione **Agregar/eliminar de la lista** en la sección Acciones del mensaje de globo de contexto.

Flujo de trabajo

En el siguiente diagrama de flujo de trabajo se muestra el flujo de trabajo general para Investigate con la ubicación de la tarea Agregar a lista resaltada.



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware

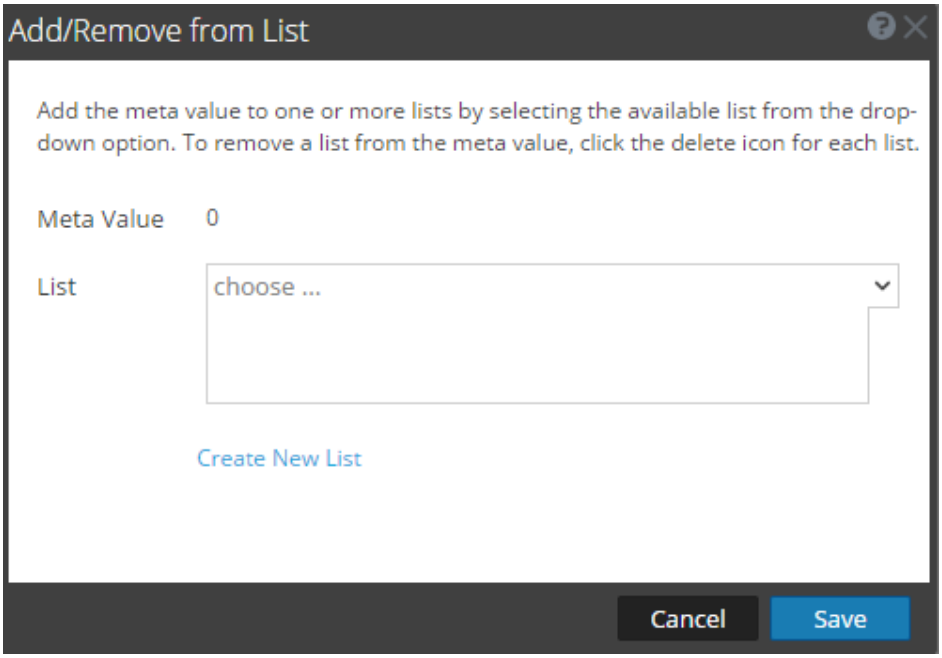
Función de usuario	Deseo…	Mostrarme cómo
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	crear o agregar valores de metadatos a una lista de Context Hub*	Administrar listas y valores de lista de Context Hub en las vistas Navegar y Eventos o Buscar contexto adicional en la vista Análisis de eventos

Temas relacionados

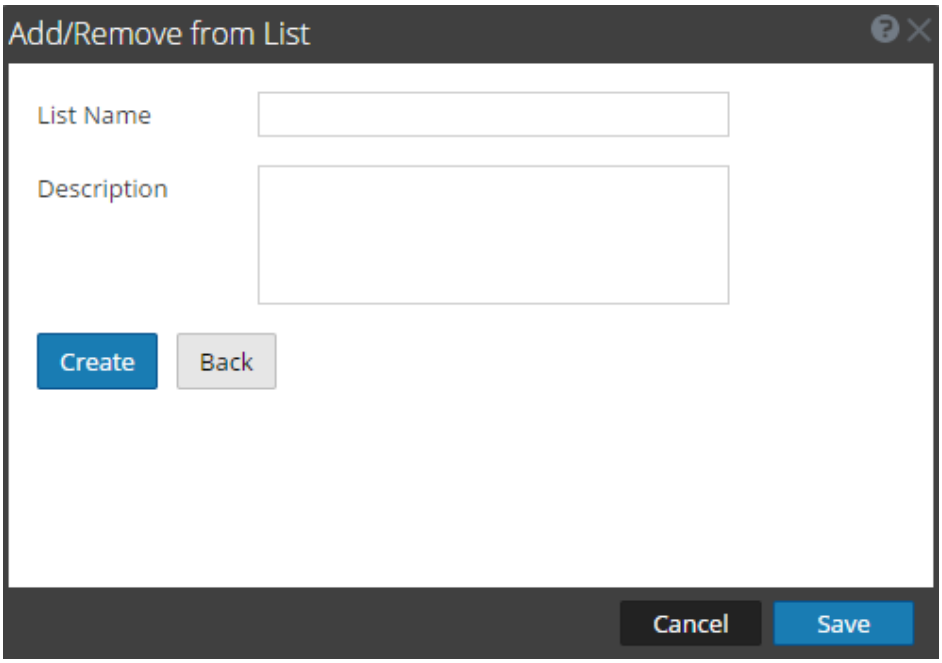
- Buscar contexto adicional en las vistas Navegar y Eventos
- Vista Navegar
- Vista Eventos
- Vista Análisis de eventos

Vista rápida en las vistas Navegar y Eventos

La siguiente figura es un ejemplo del cuadro de diálogo Agregar/eliminar de la lista cuando se abre inicialmente.



En la siguiente figura se muestra el cuadro de diálogo Crear lista nueva.

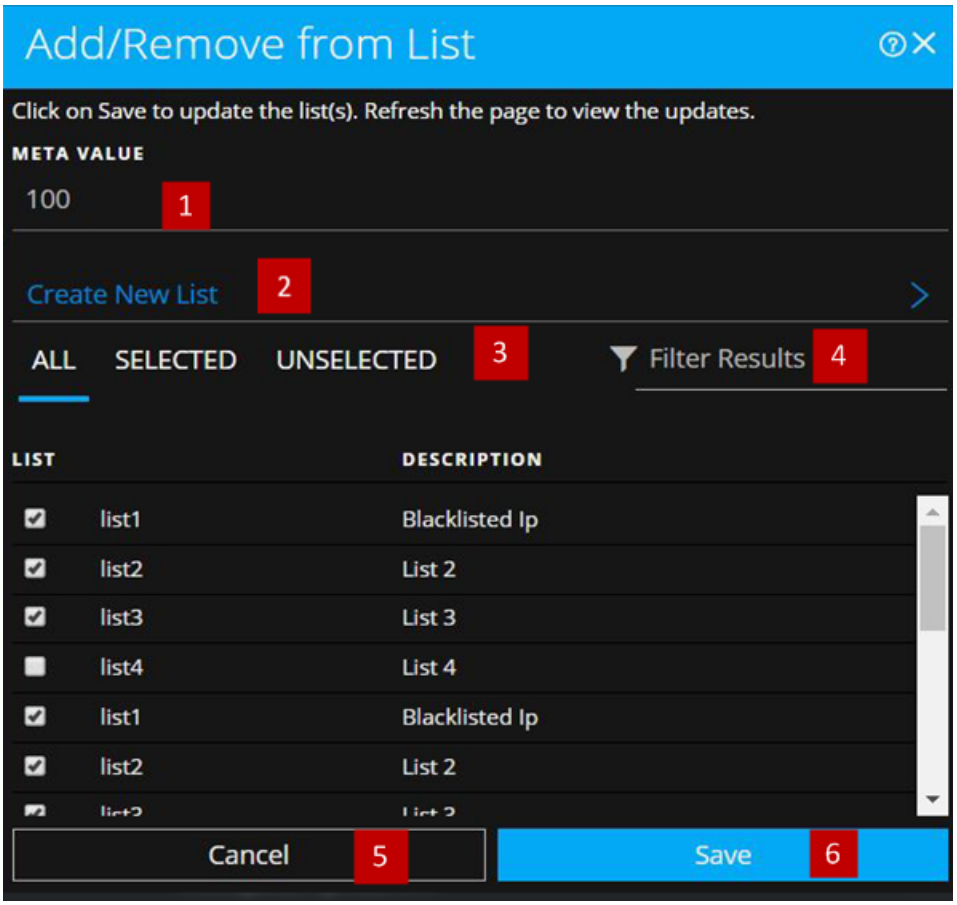


En la siguiente tabla se describen las características de los cuadros de diálogo Agregar/eliminar de la lista y Crear lista nueva.

Función	Descripción
Valor de metadatos	El valor de metadatos seleccionado que se agregará a la lista nueva o existente.
Lista	La lista a la cual se debe agregar el valor de metadatos seleccionado. Un menú desplegable proporciona una lista de las listas disponibles a las cuales puede agregar el valor de metadatos.
Crear lista nueva	Se abre un cuadro de diálogo nuevo en el que puede crear una nueva lista para el valor de metadatos seleccionado.
Nombre de lista	El nombre de la lista.
Descripción	La descripción de la nueva lista.
Crear	Crear una nueva lista después de ingresar los campos obligatorios.
Atrás	En el nuevo modo de lista, cancela la nueva creación de listas y regresa al cuadro de diálogo original.
Cancelar	Cancela la adición del valor de metadatos a una lista y cierra el cuadro de diálogo.
Guardar	Guarda los cambios realizados en las listas y cierra el cuadro de diálogo.

Vista rápida en la vista Análisis de eventos (versión 11.2 y superior)

El siguiente es un ejemplo del cuadro de diálogo **Agregar/eliminar de la lista** en la vista Análisis de eventos.



1 Entidades o valores de metadatos que se agregarán o se quitarán.
2 Cree una lista nueva mediante los metadatos seleccionados.
3 Seleccione cualquiera de las pestañas: Todo, Seleccionado o No seleccionado.
4 Busque mediante el nombre de la lista o la descripción.
5 Cancele la acción.
6 Guarde para actualizar las listas o crear una lista nueva.

En la siguiente tabla se muestran las opciones del cuadro de diálogo Agregar/eliminar de la lista.

Opción	Descripción
VALOR DE METADATOS	Muestra la entidad o el valor de metadatos seleccionados que se deben agregar a una o más listas o eliminar de estas. También puede crear una lista nueva mediante el valor seleccionado.
Crear lista nueva	Muestra un cuadro de diálogo que permite crear una lista nueva mediante el valor de metadatos seleccionado.
TODO	Muestra todas las listas de Context Hub disponibles. Se seleccionan las listas que contienen la entidad o el valor de metadatos seleccionados. Seleccione una casilla de verificación para agregar una entidad o un valor de metadatos a una lista. Deseleccione una casilla de verificación para quitarlos de la lista.

Opción	Descripción
SELECCIONADO	Muestra solo las listas que contienen la entidad o el valor de metadatos seleccionados. (Se seleccionan todas las listas).
NO SELECCIONADO	Muestra solo las listas que no contienen la entidad o el valor de metadatos seleccionados. (Se deseleccionan todas las listas).
Filtrar resultados	Ingrese el nombre o la descripción de una lista específica para buscar en varias listas.
LISTA	Muestra el nombre de todas las listas.
DESCRIPCIÓN	Muestra información acerca de la lista seleccionada. En este cuadro de diálogo aparece la descripción que proporciona cuando crea una lista. Por ejemplo: Esta lista contiene todas las direcciones IP incluidas en la lista negra.
Cancelar	Cancela la operación.
Guardar	Guarda los cambios.

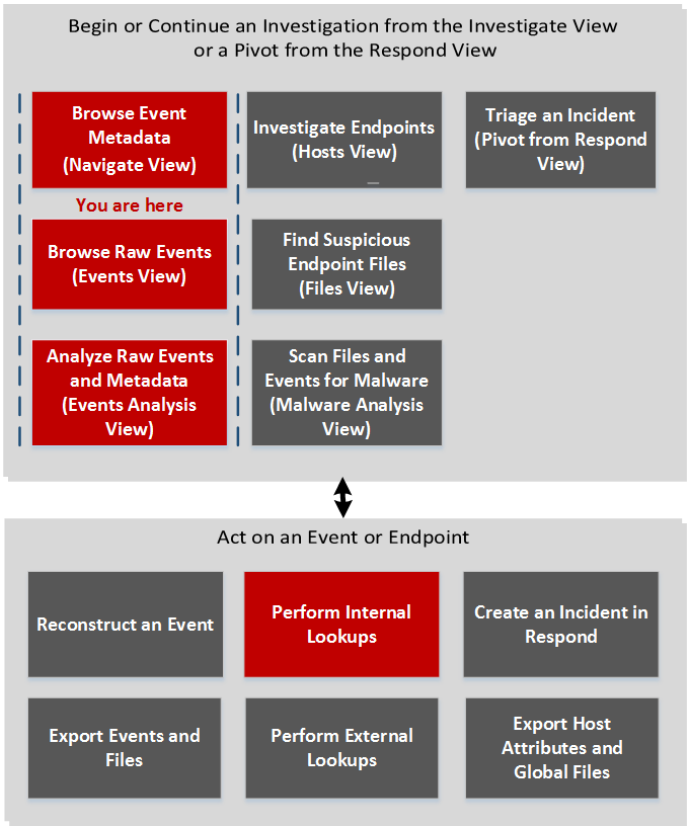
Panel Búsqueda de contexto

Después de que un administrador configura el servicio Context Hub, puede ver la información contextual para los valores de metadatos en las vistas Navegar, Eventos y Análisis de eventos (versión 11.2). El servicio Context Hub está preconfigurado con un mapeo predeterminado de tipos de metadatos y claves de metadatos. Para obtener información sobre el mapeo del valor de metadatos de Context Hub con la clave de metadatos de Investigation, consulte "Administrar el mapeo de tipos de metadatos y claves de metadatos" en la *Guía de configuración de Context Hub*.

El panel Búsqueda de contexto se muestra al lado derecho de las vistas Navegar y Eventos. Los valores de metadatos que se agregaron a una lista de Context Hub se resaltan en gris en los resultados de las vistas Navegar o Eventos. En la vista Análisis de eventos, se marcan con un guion bajo. Cuando haga clic con el botón secundario en un valor resaltado y seleccione **Búsqueda de contexto** en el menú contextual resultante, los resultados de la búsqueda se mostrarán en el panel Búsqueda de contexto para los orígenes configurados para el valor de metadatos seleccionado. Puede seleccionar un origen en la barra de íconos del panel Búsqueda de contexto para ver la información contextual.

Hay algunas diferencias entre la apariencia y el contenido del panel Búsqueda de contexto cuando se abre en las vistas Navegar o Eventos y cuando se abre en la vista Análisis de eventos.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	buscar contexto adicional para un valor de metadatos	Buscar contexto adicional en las vistas Navegar y Eventos y Buscar contexto adicional en la vista Análisis de eventos

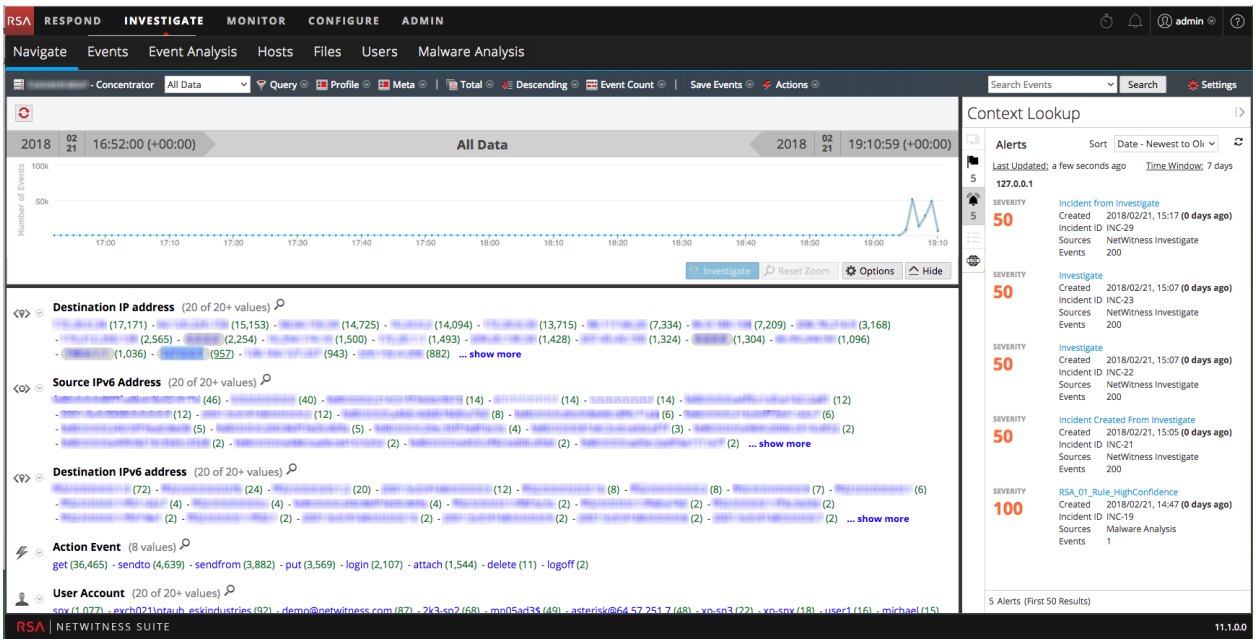
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Eventos
- Vista Navegar
- Vista Análisis de eventos
- "Comentarios y uso compartido de datos de NetWitness" en la *Guía de administración de servicios de Live*

Vista rápida (en las vistas Navegar y Eventos)

La siguiente figura es un ejemplo del panel Búsqueda de contexto como aparece en las vistas Navegar y Eventos. Los controles y las funciones se describen en la tabla.



Función	Descripción
Barra de opciones de origen	Muestra los íconos de los orígenes disponibles: Endpoint, incidentes, alertas y listas.
Nombre de fuente	Muestra el nombre de origen según el ícono seleccionado: • Terminal • Incidentes • Alertas • Listas • Live Connect
Clasificar	Proporciona una lista desplegable de opciones de clasificación para la información de contexto detallada. Las opciones de clasificación posibles son Severidad: alta a baja, Severidad: baja a alta, Fecha: Más antiguo a más reciente y Fecha: Más reciente a más antiguo. Las opciones de clasificación varían según el tipo de origen.
	Actualiza los resultados de búsqueda.
<n elementos> (primeros <n> resultados)	El pie de página proporciona un conteo de los resultados que se muestran actualmente y la cantidad total de resultados. Por ejemplo, 5 alertas (primeros 50 resultados).

Incidentes

Se muestran los incidentes, en primer lugar según la hora (más recientes a más antiguos) y, a continuación, según el estado de prioridad. Se muestra la siguiente información para las búsquedas de incidentes:

- ID y nombre del incidente
- Estado de prioridad de los incidentes.
- Valor de puntaje de riesgo de los incidentes
- La fecha de creación del incidente.
- Estado del incidente.
- Usuario asignado al incidente
- Última actualización: Indica la última vez en que se recuperaron datos contextuales del origen de datos y se actualizaron en la caché.
- Ventana de tiempo: Se basa en el valor que se configura para el campo "Consultar últimos (días)" en la ventana Configurar Respond. Para obtener detalles, consulte el tema "Configurar Respond como un origen de datos" en la *Guía de configuración de Context Hub*.
- Clasificar: Este campo desplegable proporciona opciones para cambiar el orden de los resultados según la hora o la prioridad.

Alertas

Las alertas se muestran en función de la gravedad. Se muestra la siguiente información para búsquedas de alertas:

- Nombre de alerta
- Valor de gravedad de las alertas
- Fecha en que se creó la alerta
- ID del incidente: Este es el ID del incidente con el cual está asociada la alerta (si corresponde).
- Orígenes: Nombre del origen de eventos.
- Número de eventos asociados con la alerta.
- Última actualización: Indica la última vez en que se recuperaron datos contextuales del origen de datos y se actualizaron en la caché.
- Ventana de tiempo: Se basa en el valor que se configura para el campo "Consultar últimos (días)" en la ventana Configurar Respond. Para obtener detalles, consulte el tema "Configurar Respond como un origen de datos" en la *Guía de configuración de Context Hub*.
- Clasificar: Este campo desplegable proporciona la opción para cambiar el orden de los resultados según la hora o la prioridad.

Listas

Se muestra la siguiente información para búsquedas de listas.

- Nombre de lista
- Propietario que creó la lista
- Fecha de creación
- Fecha de la última actualización
- Descripción de la lista

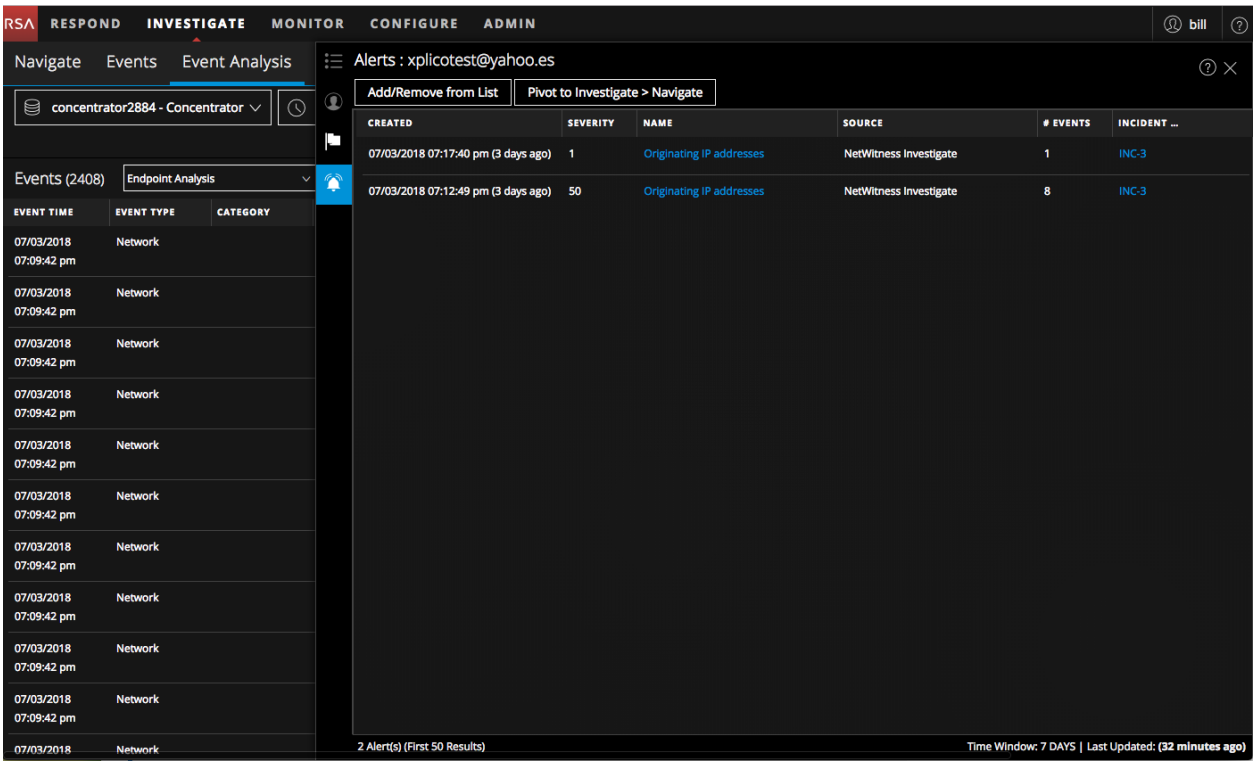
Terminal

Se muestra la siguiente información para búsquedas de Endpoint.

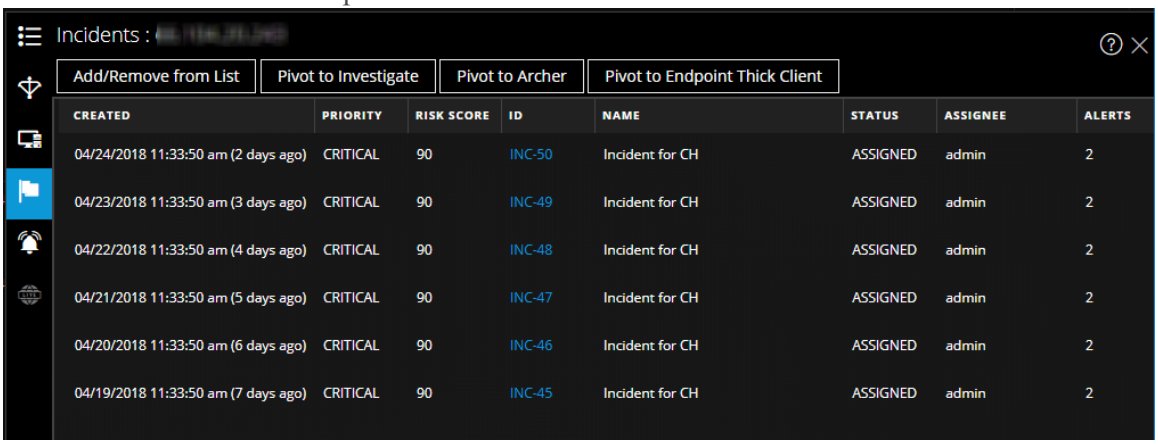
- Nombre y dirección IP de la máquina.
  Si hace clic en la dirección IP o en el nombre de la máquina de Endpoint, se desplazará hasta la interfaz del usuario de Endpoint para realizar una investigación más a fondo.
- Última actualización: Indica la última vez en que se recuperaron datos contextuales del origen de datos y se actualizaron en la caché.
- Puntaje de la máquina: Un puntaje de IIOC de la máquina se agrega en función de los puntajes del módulo.
- Cantidad de módulos: Cantidad de archivos activos para la máquina seleccionada.
- Última actualización: Indica cuándo se actualizaron por última vez los resultados del escaneo en la base de datos de Endpoint.
- Último usuario de inicio de sesión
- Dirección MAC de la máquina
- Versión del sistema operativo
- Notas administrativas (si corresponde)
- Estado administrativo (si corresponde)
- Principales módulos sospechosos (módulos que tienen un puntaje de IIOC > 500). Esto se basa en el valor configurado para el campo “Puntaje de IIOC mínimo” en la ventana Configurar Endpoint. El valor predeterminado para “Puntaje de IIOC mínimo” es 500.
- Niveles de IIOC de la máquina

Vista rápida en la vista Análisis de eventos (versión 11.2 y superior)

La siguiente figura es un ejemplo del panel Búsqueda de contexto como aparece en la vista Análisis de eventos.



La información contextual o los resultados de consulta que se muestran en el panel Búsqueda de contexto dependen de la entidad seleccionada y de los orígenes de datos asociados. El panel Búsqueda de contexto tiene pestañas por separado para cada uno de los orígenes de datos. Las pestañas son: Origen de datos de Lista, Archer, Active Directory, Endpoint, Incidentes, Alertas y Live Connect. En la siguiente figura se muestra el panel Búsqueda de contexto para una entidad seleccionada en la vista Detalles de incidente con la pestaña Incidentes abierta.

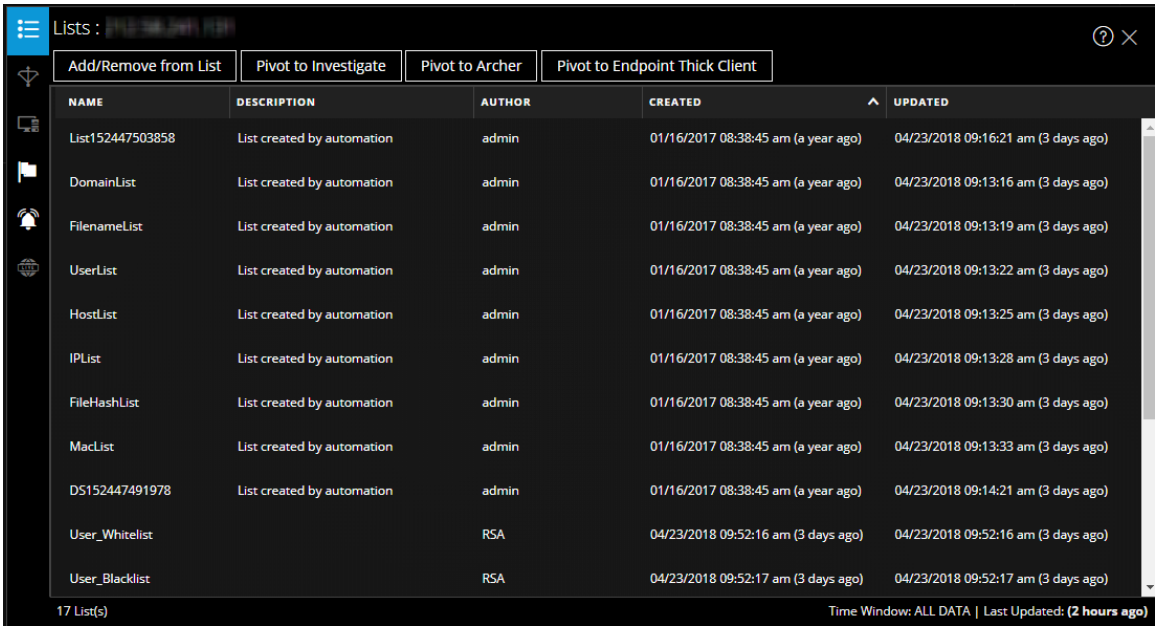


En la siguiente tabla se describen los datos disponibles en cada pestaña y las entidades compatibles.

Pestaña	Descripción	Entidades compatibles
 (Listas)	Muestra todos los datos de lista asociados con la entidad o el valor de metadatos seleccionados. El resultado se ordena por la lista que se actualizó por última vez.	Todas las entidades
 (Archer)	Muestra información sobre los recursos, junto con clasificaciones de criticidad que usan el origen de datos Archer.	IP, host y dirección Mac
 (Active Directory)	Muestra toda la información del usuario seleccionado.	Usuario
 (NetWitness Endpoint)	Muestra la información del origen de datos NetWitness Endpoint para la entidad o el valor de metadatos seleccionados, la cual incluye las máquinas, los módulos y los niveles de IIOC. Los módulos se muestran del puntaje de IOC más alto al puntaje de IIOC más bajo y los niveles de IIOC, de los más altos a los más bajos.	IP, dirección de MAC y host
 (Incidentes)	Muestra la lista de incidentes asociados con la entidad o el valor de metadatos seleccionados. El resultado se ordena de los incidentes más recientes a los más antiguos.	Todas las entidades
 (Alertas)	Muestra la lista de alertas asociadas con la entidad o el valor de metadatos seleccionados. El resultado se ordena de las alertas más recientes a las más antiguas.	Todas las entidades
 (Live Connect)	Muestra información relacionada con Live Connect.	IP, dominio y hash de archivo

Pestaña Listas

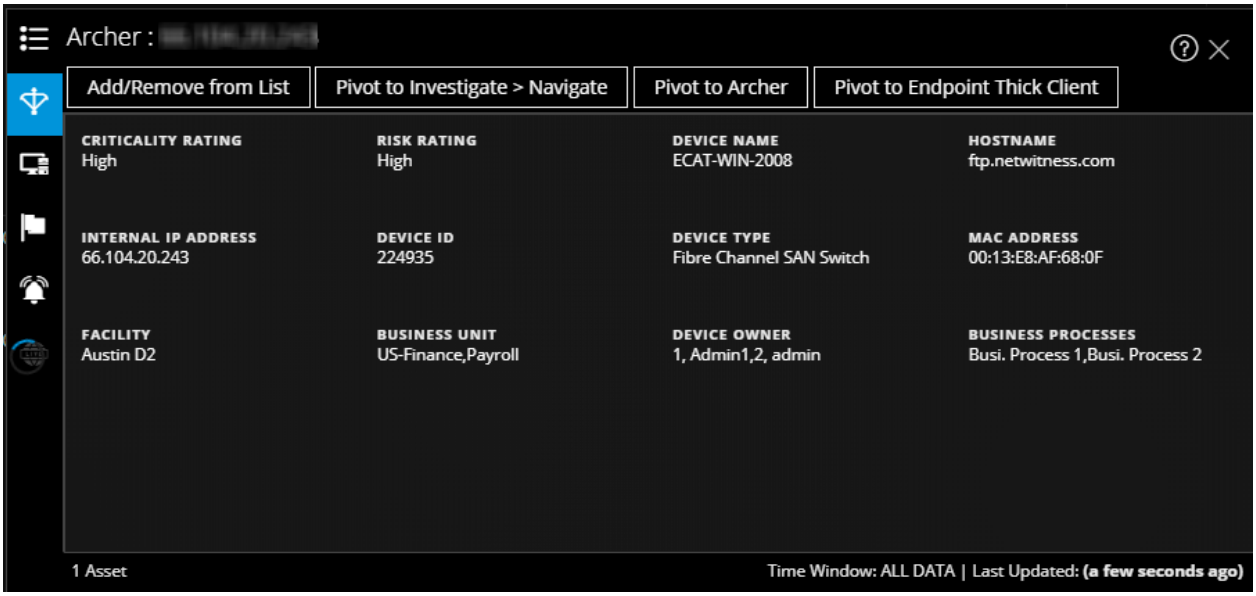
El panel Búsqueda de contexto para Listas muestra una o más listas asociadas con la entidad o el valor de metadatos seleccionados. La siguiente figura es un ejemplo del panel de contexto para Listas y en la tabla se describen los campos.



Campo	Descripción
Nombre	El nombre de la lista (definido durante la creación de la lista).
Descripción	La descripción de la lista (definida durante la creación de la lista).
Autor	El propietario que creó la lista.
Creado	La fecha en que se creó la lista.
Actualizado	La fecha en que la lista se actualizó o se modificó por última vez.
Conteo	La cantidad de listas en las cuales está disponible la entidad o el valor de metadatos seleccionados.
Ventana de tiempo	La ventana de tiempo en función del valor configurado para el campo “Consultar últimos” del cuadro de diálogo Configurar respuestas. De forma predeterminada, se obtienen todos los datos de Listas.
Última actualización	La hora en que Context Hub obtuvo y almacenó los datos de búsqueda en la caché.

Pestaña Archer

El panel Búsqueda de contexto para Archer muestra información sobre los recursos, junto con calificaciones de criticidad que usan el origen de datos Archer para las entidades de IP, host y dirección Mac. La siguiente figura es un ejemplo del panel Búsqueda de contexto para Archer y en la tabla se describe cada campo.



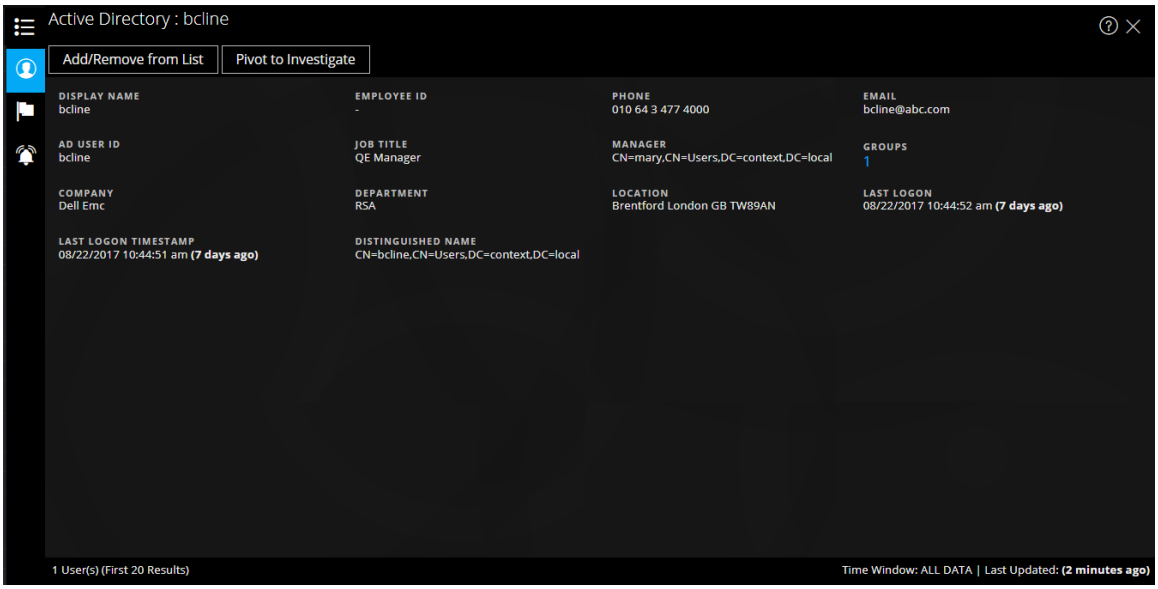
Campo	Descripción
Clasificación de criticidad	La criticidad operacional del dispositivo en función de las aplicaciones que apoya. Las clasificaciones de criticidad se pueden configurar en No clasificado, Baja, Media-baja, Media, Media-alta o Alta.
Clasificación de riesgo	La clasificación de riesgo calculada del dispositivo según la evaluación más reciente y la clasificación de riesgo promedio de las instalaciones que utilizan el dispositivo. La clasificación de riesgo se puede configurar en Grave, Alta, Mediana, Baja o Mínima.
Nombre del dispositivo	El nombre único del dispositivo.
Nombre del host	El nombre de host del dispositivo.
Dirección IP	La dirección IP interna primaria del dispositivo.
ID de dispositivo	El valor completado automáticamente que identifica de manera única el registro en todas las aplicaciones del sistema.
Tipo	El tipo de dispositivo, por ejemplo, servidor, laptop, escritorio y otros.
Instalaciones	Vínculos a los registros de la aplicación Instalaciones que se relacionan con este dispositivo.

Campo	Descripción
Unidad de negocios	Vínculos a los registros de la aplicación Unidad de negocios que se relacionan con este dispositivo. Si hay más de tres valores de unidad de negocios, puede colocar el cursor sobre el campo para verlos.
Propietario de dispositivos	La persona responsable del dispositivo, quien recibe derechos de lectura y actualización del registro.
Conteo	La cantidad de recursos disponibles.
Ventana de tiempo	La ventana de tiempo en función del valor configurado para el campo “Consultar últimos” del cuadro de diálogo Configurar respuestas. De forma predeterminada, se obtienen todos los datos para Archer.
Última actualización	La hora en que Context Hub obtuvo y almacenó los datos de búsqueda en la caché.

Nota: En las versiones localizadas, solamente se muestran estos doce campos: Clasificación de criticidad, Clasificación de riesgo, Propietario de dispositivos, Unidad de negocios, Nombre del host, Dirección MAC, Instalaciones, Dirección IP, Tipo, ID de dispositivo, Nombre del dispositivo y Procesos de negocios.

Pestaña Active Directory

La siguiente figura es un ejemplo del panel Búsqueda de contexto para Active Directory.



El panel Búsqueda de contexto para Active Directory muestra toda la información, las alertas y los incidentes relacionados para un usuario. Puede realizar una búsqueda mediante los siguientes formatos:

- userPrincipalName
- Domain\UserName
- sAMAccountName

Si el usuario existe en dominios múltiples o bosques múltiples, se muestra toda la información contextual relacionada para el usuario específico.

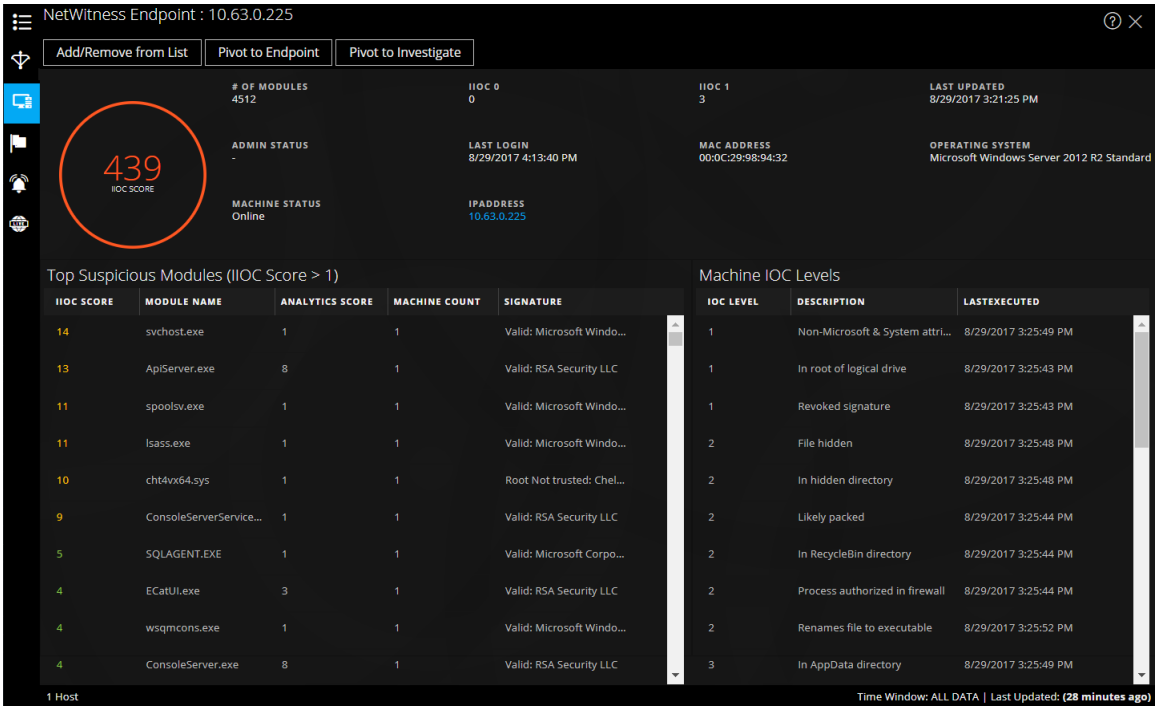
La siguiente información se muestra para Active Directory.

Campo	Descripción
Nombre para mostrar	El nombre del usuario.
ID de empleado	El ID de empleado del usuario.
Teléfono	El número de teléfono del usuario.
Correo electrónico	El ID de correo electrónico del usuario.
ID de usuario de AD	La identificación única del usuario dentro de una organización.
Cargo	La designación del usuario.
Administrador	El nombre del administrador del usuario.
Grupos	La lista de grupos de los cuales el usuario es miembro.
Empresa	El nombre de la empresa del usuario.

Campo	Descripción
Departamento	El nombre del departamento dentro de la organización al cual pertenece el usuario.
Ubicación	La ubicación del usuario.
Último inicio de sesión	La hora en que el usuario inició sesión en el sistema, solamente si el Catálogo global está definido.
Último registro de fecha y hora de inicio de sesión	La hora en que el usuario inició sesión en el sistema.
Nombre distinguido	El nombre único asignado al usuario.
Conteo	La cantidad de usuarios.
Ventana de tiempo	La ventana de tiempo se basa en el valor que se configura para el campo "Consultar últimos" del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se obtienen todos los datos de Active Directory.
Última actualización	La hora en que Context Hub obtuvo y almacenó los datos de búsqueda en la caché.

Pestaña NetWitness Endpoint

La siguiente figura es un ejemplo del panel Búsqueda de contexto para NetWitness Endpoint.



La siguiente información se muestra para IIOC.

Campo	Descripción
Cantidad de módulos	La cantidad de módulos que se buscan.
Estado administrativo	El estado administrativo (si corresponde).
Última actualización	La hora en que los datos se actualizaron por última vez.
Último inicio de sesión	La hora en que el usuario inició sesión por última vez.
Dirección MAC	La Dirección MAC de la máquina.
Sistema operativo	La versión del sistema operativo que usa la máquina de NetWitness Endpoint.
Estado de la máquina	El estado del módulo que se está viendo: En línea, Offline, Activo o Inactivo.
Dirección IP	La dirección IP del módulo específico.

La siguiente información se muestra para los módulos.

Campo	Descripción
Puntaje de IIOC	Un puntaje de IIOC de la máquina es un puntaje agregado que se basa en los puntajes del módulo. Esto se basa en el valor configurado para el campo Puntaje de IIOC mínimo en el cuadro de diálogo Ajustes de orígenes de datos de Context Hub. El valor predeterminado para Puntaje de IIOC mínimo es 500. Consulte “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.
Nombre de módulo	El nombre del módulo que se busca.
Puntaje de análisis	La cantidad de archivos activos para la máquina seleccionada.
Conteo de máquinas	La cantidad de máquinas en las que se activó ese IOC específico.
Firma	Indicador que señala si el archivo está o no firmado y si es o no válido, y que proporciona información acerca del signatario. Por ejemplo, Google, Apple, etc.

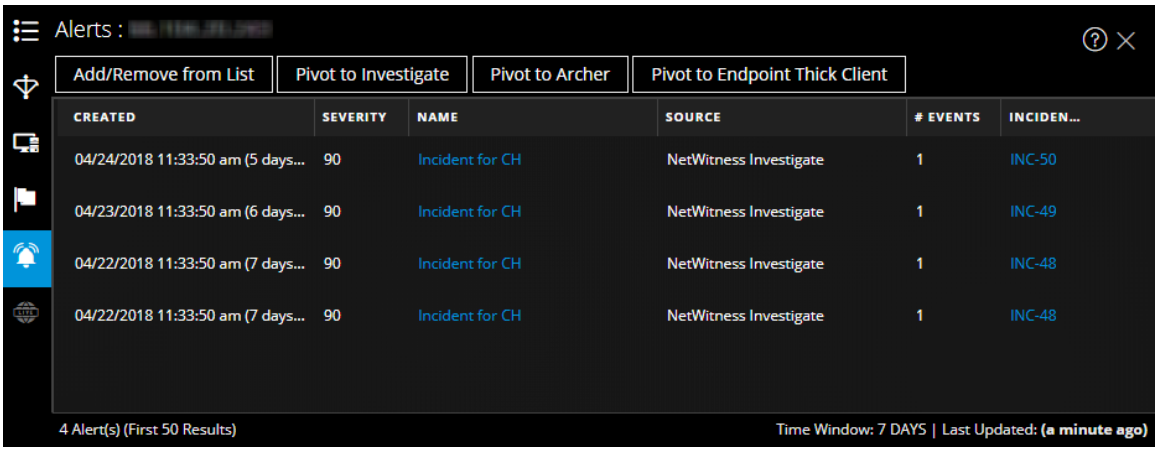
La siguiente información se muestra para las máquinas.

Campo	Descripción
Niveles de IIOC	Los niveles de IOC.
Descripción	La descripción del nivel de IOC, si está disponible.
Última ejecución	La hora en que se ejecutó la acción.
Conteo	La cantidad de hosts que se buscan.

Campo	Descripción
Ventana de tiempo	La ventana de tiempo se basa en el valor que se configura para el campo Consultar últimos del cuadro de diálogo Configurar ajustes de orígenes de datos. De manera predeterminada, se obtienen todos los datos de NetWitness Endpoint.
Última actualización	La hora en que se actualizaron por última vez los resultados del escaneo en la base de datos de NetWitness Endpoint.

Pestaña Alertas

La siguiente figura es un ejemplo del panel de contexto para Alerts que se muestra, en primer lugar, en función del tiempo (más recientes a más antiguas) y, a continuación, la gravedad.



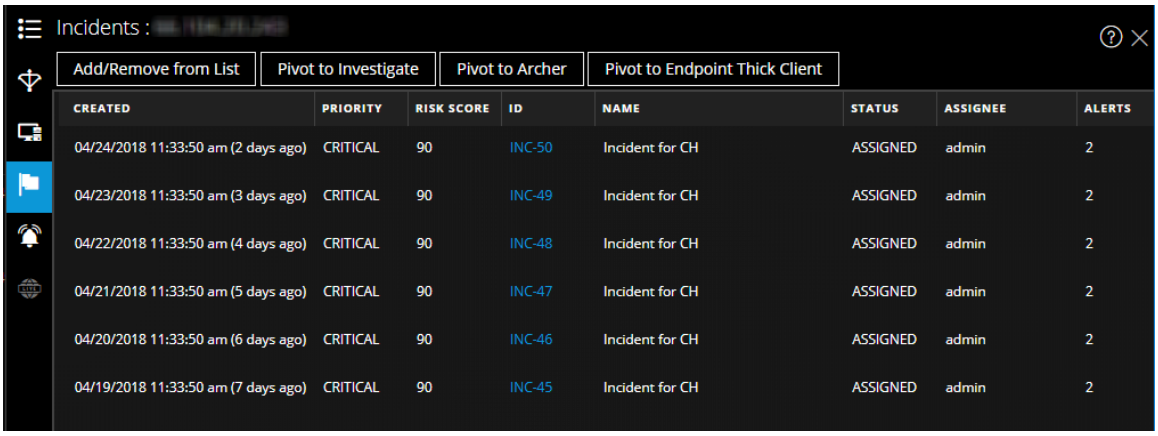
En el panel Búsqueda de contexto para Alertas se muestra la siguiente información.

Campo	Descripción
Creado	La fecha y la hora en que se creó la alerta.
Gravedad	El valor de gravedad de las alertas.
Nombre	El nombre de la alerta Puede hacer clic en el nombre para ver los detalles de una alerta específica.
Origen	El nombre del origen de alerta desde el cual se activó la alerta.
Cantidad de eventos	La cantidad de eventos asociados con la alerta.
ID del incidente	El ID del incidente (si corresponde) con el cual está asociada la alerta. Puede hacer clic en el ID para ver los detalles de una alerta específica.
Conteo	La cantidad de alertas. De forma predeterminada, solo se muestran las primeras 100 alertas. Para obtener más información acerca de cómo configurar los ajustes, consulte “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.

Campo	Descripción
Ventana de tiempo	La ventana de tiempo se basa en el valor que se configura para el campo Consultar últimos del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se recupera los datos de alertas de los últimos 7 días.
Última actualización	La hora en que se recuperaron por última vez datos contextuales desde el origen de datos.

Pestaña Incidentes

La siguiente figura es un ejemplo del panel de contexto para Incidentes que se basa, en primer lugar, en el tiempo (más recientes a más antiguos) y, a continuación, en el estado de prioridad.



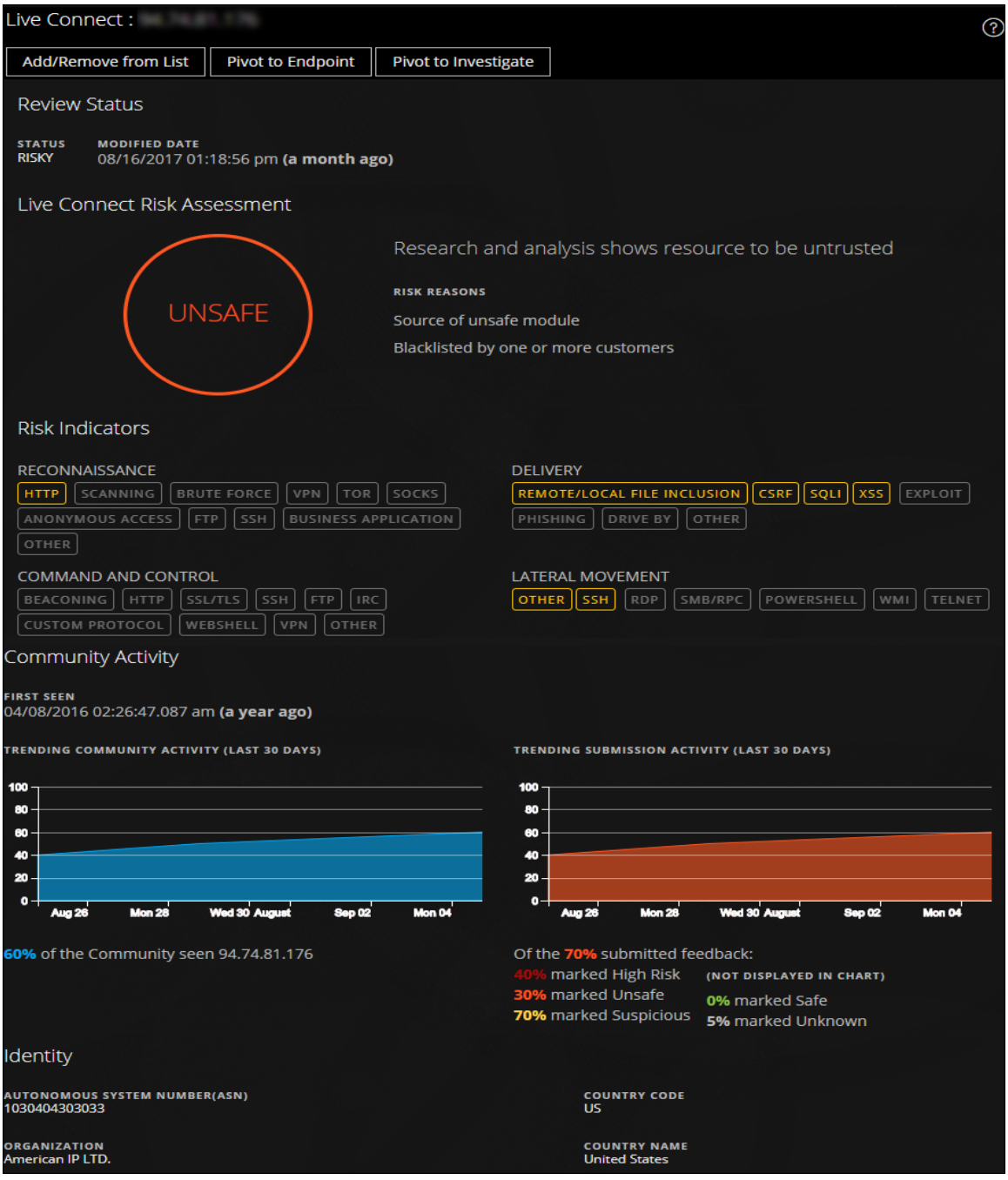
En el panel Búsqueda de contexto para Incidentes se muestra la siguiente información.

Campo	Descripción
Creado	La fecha en que se creó el incidente.
Prioridad	El estado de prioridad de los incidentes.
Puntaje de riesgo	El puntaje de riesgo de los incidentes.
ID	El ID del incidente. Puede hacer clic en el ID para mostrar detalles adicionales acerca del incidente.
Nombre	El nombre del incidente.
Estado	El estado del incidente.
Usuario asignado	El propietario actual del incidente.
Alertas	La cantidad de alertas asociadas con el incidente.
Conteo	La cantidad de incidentes. De manera predeterminada, se muestran solamente los primeros 100 incidentes. Para obtener más información acerca de cómo configurar los ajustes, consulte “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.

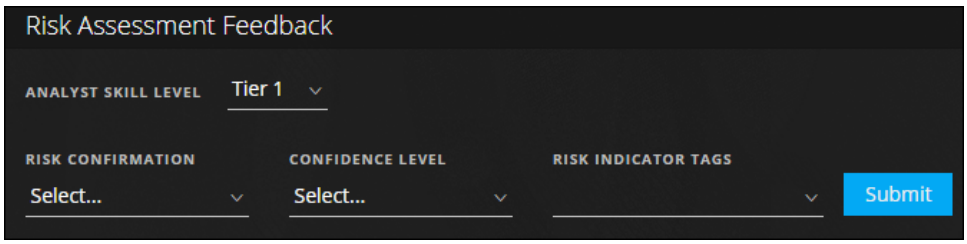
Campo	Descripción
Ventana de tiempo	La ventana de tiempo se basa en el valor que se configura para el campo Consultar últimos del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se recupera los datos de alertas de los últimos 7 días.
Última actualización	La hora en que se recuperaron por última vez datos contextuales desde el origen de datos.

Pestaña Live Connect

La siguiente figura es un ejemplo de un panel de contexto para Live Connect y en la tabla se describe la información que se muestra.



Campo	Descripción
Estado de revisión	El estado de revisión de la entidad de Live Connect seleccionada (IP, archivo o dominio) en función de la actividad de los analistas. Esto proporciona visibilidad de la actividad de los analistas dentro de una organización. **Estado** Los siguientes son los tipos de estado: • **Nuevo:** Los resultados de búsqueda de una dirección IP se ven por primera vez dentro de la organización. • **Vistos:** Un analista dentro de la organización ya vio los resultados de búsqueda de una dirección IP. • **Marcada como segura:** Un analista dentro de la organización ya vio los resultados de búsqueda y marcó la dirección IP como segura. • **Marcada como riesgosa:** Un analista dentro de la organización ya vio los resultados de búsqueda y marcó la dirección IP como riesgosa.
Evaluación del riesgo	La evaluación del riesgo para la entidad de Live Connect seleccionada (IP, archivo o dominio) de acuerdo con el análisis y los comentarios de los analistas de Live Connect. Las categorías de evaluación del riesgo son: • **Segura:** La entidad de Live Connect se considera segura. • **Desconocido:** Live Connect no tiene suficiente información acerca de esta entidad para calcular el riesgo. • **Alto riesgo**: Se marca como de alto riesgo en función del análisis y los motivos de riesgo que proporciona la comunidad. Las entidades marcadas como de alto riesgo requieren atención inmediata. • **Sospechoso**: Se marca como sospechoso en función del análisis y los motivos de riesgo que proporciona la comunidad. El análisis indica actividad potencialmente amenazante que requiere una acción. • **Inseguro:** Se marca como inseguro en función del análisis y los motivos de riesgo que proporciona la comunidad. La entidad se clasifica como Alto riesgo, Sospechoso o Inseguro y muestra los motivos de riesgo asociados según corresponde.

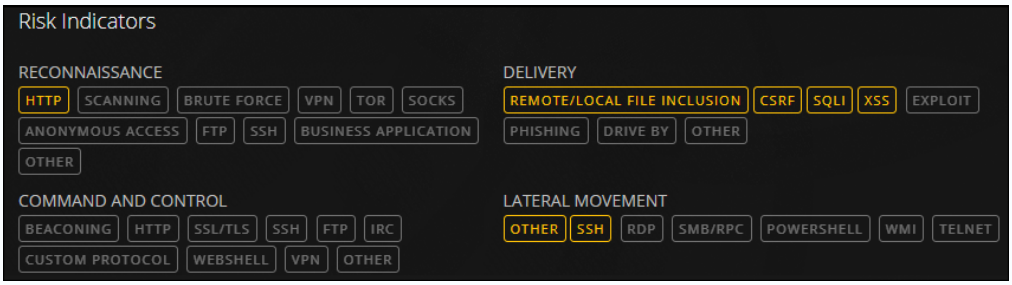
Campo	Descripción
Comentarios sobre la evaluación del riesgo	

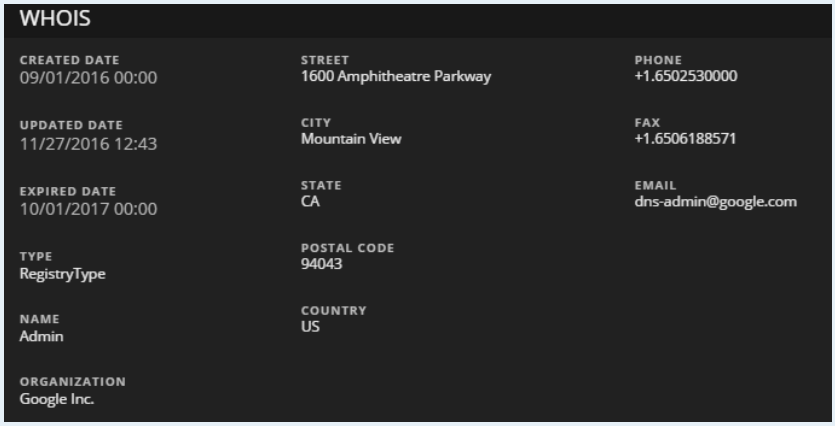
Comentarios sobre la evaluación del riesgo permite que el analista envíe comentarios de inteligencia de amenazas acerca de una entidad al servidor de Live Connect.

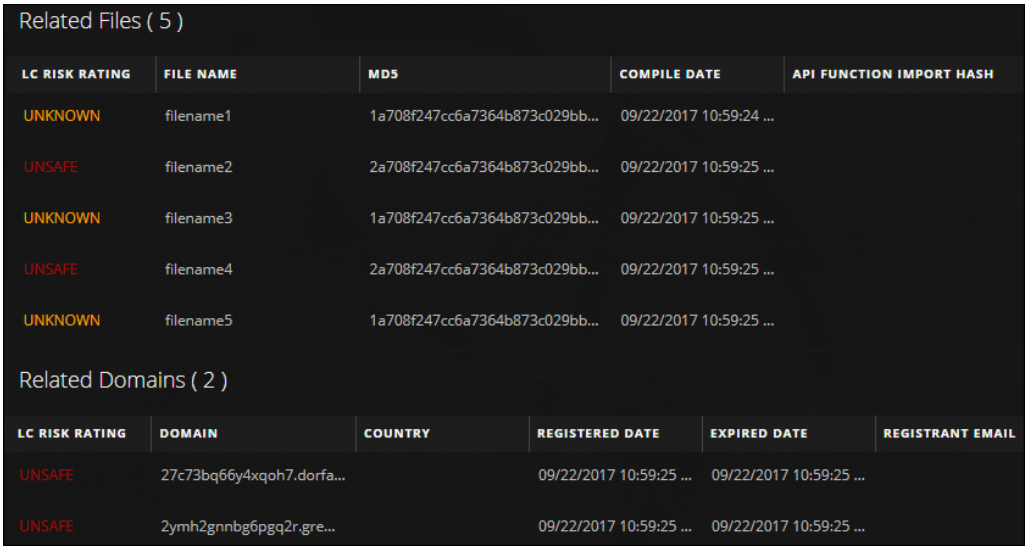
- **Nivel de habilidad del analista**
  Las siguientes son las opciones para el nivel de habilidad del analista:
  - **Nivel 1**: Los analistas de este nivel definen procedimientos para las correcciones y deciden si un incidente se debe elevar a otras áreas de un centro de operaciones de seguridad (SOC). Este es el valor predeterminado.
  - **Nivel 2**: Los analistas que investigan incidentes y capturan inteligencia de una investigación para enviarla a los diversos flujos de trabajo en un SOC.
  - **Nivel 3**: Los analistas que comparten los resultados de la investigación con la organización del SOC. Por lo general, administran incidentes y disponen de amplitud y profundidad en las habilidades y las herramientas necesarias para la respuesta ante incidentes.

  Nota: Mientras se crea un nuevo usuario para NetWitness Platform (analista), un administrador debe poder identificar al usuario como un analista de nivel 1, nivel 2 o nivel 3.

- **Confirmación de riesgo**: La confirmación de riesgo de la entidad de Live Connect seleccionada (IP, archivo o dominio). Las categorías de confirmación de riesgo son:
  - **Segura**: La entidad de Live Connect se considera segura.
  - **Desconocido**: El analista no tiene información suficiente para proporcionar una confirmación de riesgo.
  - **Alto riesgo**: Se marca como de alto riesgo en función del análisis y los motivos de riesgo que proporciona la comunidad. Las entidades marcadas como de alto riesgo requieren atención inmediata.
  - **Sospechoso**: Se marca como sospechoso en función del análisis y los motivos de riesgo que proporciona la comunidad. El análisis indica actividad potencialmente amenazante que requiere una acción.
  - **Inseguro**: Se marca como inseguro en función del análisis y los motivos de riesgo que proporciona la comunidad.
- **Nivel de confianza**: El nivel de confianza de un analista en la entrega de comentarios para la entidad de Live Connect. Las categorías de nivel de confianza

Campo	Descripción
	son las siguientes: Alta, Media y Baja. • **Etiquetas de indicador de riesgo**: Permite seleccionar una categoría de etiqueta en función del análisis.
Actividad de la comunidad	Actividades de la comunidad, como las siguientes: • Fecha en que se vio por primera vez en la comunidad. • Tiempo desde que la dirección IP, el archivo o el dominio se vieron por primera vez (Hora actual: hora en que se vio por primera vez). **Actividad de la comunidad de tendencias:** Si la dirección IP se conoce dentro de la comunidad de RSA, se muestra una representación gráfica de la tendencia de actividad de la comunidad para lo siguiente: • Usuarios (en %) que vieron la dirección IP en la comunidad de Live Connect con el tiempo. • Usuarios (en %) que enviaron comentarios para la dirección IP. • Usuarios (en %) que marcaron la dirección IP como insegura con el tiempo.
Indicadores de riesgo	 Los indicadores de riesgo se destacan en función de las etiquetas que asigna la comunidad a las entidades (direcciones IP, archivos o dominios). Las etiquetas se clasifican de la siguiente manera: Reconocimiento, Distribución, Comando y control, Movimiento lateral, Escalación de privilegios y Empaquetado y extracción. Estas etiquetas son ejemplos y varían en función de las entradas recibidas de la comunidad en el servidor de Live Connect. El analista puede elegir las etiquetas de indicadores de riesgo apropiadas y proporcionar los comentarios de revisión. Una etiqueta resaltada indica que la entidad seleccionada está asociada a esa categoría y etiqueta específicas. Cuando se hace clic en una etiqueta resaltada, se muestra su descripción.

Campo	Descripción
Identidad	Proporciona la siguiente información de identidad para la entidad o el valor de metadatos seleccionados: Para la dirección IP: Número de sistema autónomo (ASN), Prefijo, Código de país y Nombre de país, Inscrito (organización) y Fecha. Para hash de archivo: Nombre de archivo, Tamaño de archivo, MD5, SH1, SH256, Hora de compilación y Tipo MIME. Para un dominio: Nombre de dominio y Dirección IP asociada.
Información del certificado	Proporciona la siguiente información del certificado para el hash de archivo seleccionado: Emisor del certificado, Validez del certificado, Algoritmo de firma y Número de serie del certificado.
Información WHO IS	 La información **WHO IS** proporciona los detalles de propiedad de un dominio determinado. Se muestra la siguiente información acerca del propietario del dominio: Fecha de creación, Fecha de actualización, Fecha de vencimiento, Tipo (tipo de registro), Nombre, Organización, Dirección con código postal, País, Teléfono, Fax y Correo electrónico.
Archivos relacionados	Se muestran los archivos relacionados para la dirección IP y el dominio de los tipos de entidad. Se muestra una lista de archivos asociados conocidos, junto con la siguiente información: Clasificación de riesgo de Live Connect (Seguro, Riesgoso o Desconocido), Nombre de archivo, MD5, Fecha y hora de compilación, Función de API, Hash de importación y Tipo MIME.
Dominios relacionados	Se muestran los dominios relacionados para la dirección IP y los archivos de los tipos de entidad. Se muestra una lista de dominios asociados conocidos, junto con la siguiente información: Clasificación de riesgo de Live Connect (Seguro, Riesgoso o Desconocido), Nombre de dominio, Nombre de país, Fecha de registro, Fecha de vencimiento y Dirección de correo electrónico del inscrito.

Campo	Descripción
IP relacionadas	

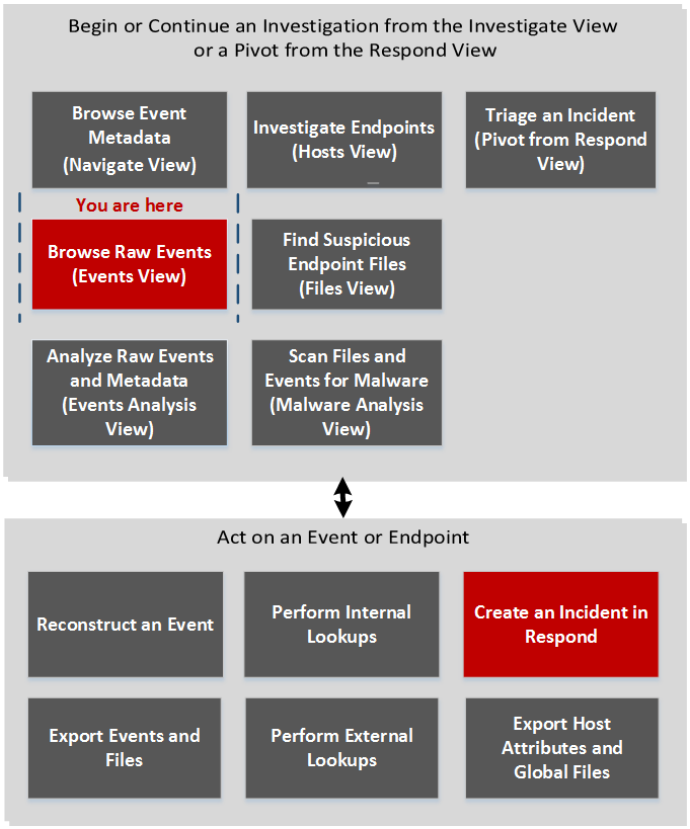
Se muestran las direcciones IP relacionadas para el dominio y los archivos de los tipos de entidad. Se muestra una lista de direcciones IP asociadas conocidas, junto con la siguiente información: Clasificación de riesgo de Live Connect (Seguro, Riesgoso o Desconocido), Dirección IP, Nombre de dominio, Código de país y Nombre de país, Fecha de registro, Fecha de vencimiento y Dirección de correo electrónico del inscrito.

Cuadro de diálogo Crear un incidente

En el cuadro de diálogo Crear un incidente, los analistas pueden crear un incidente a partir de eventos seleccionados en la vista Eventos. A continuación, el incidente está disponible para los encargados de respuesta ante incidentes que trabajan en Respond.

Para acceder a este cuadro de diálogo mientras investiga un servicio en Investigation > vista Eventos, seleccione **Incidentes > Crear nuevo incidente** en la barra de herramientas.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

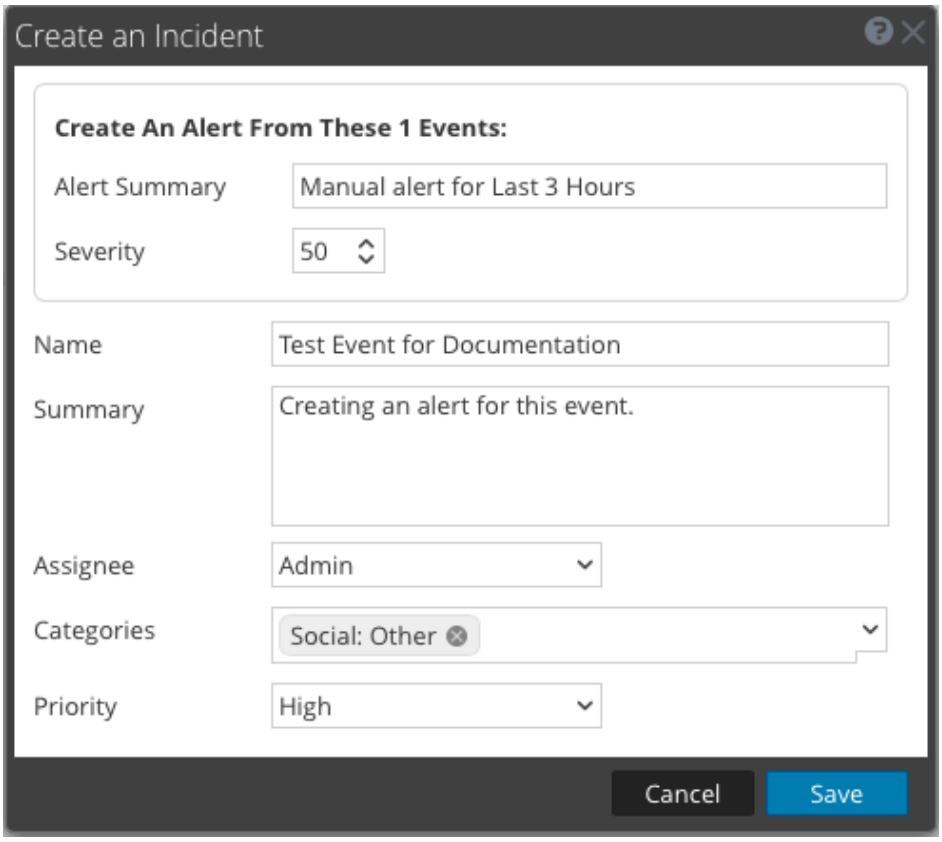
Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas o encargado de respuesta ante incidentes	agregar uno o más eventos a un incidente existente o a un incidente nuevo*	Agregar eventos a un incidente para Response

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Navegar
- Vista Eventos

Vista rápida

La siguiente figura es un ejemplo del cuadro de diálogo Crear un incidente y las funciones se describen en la tabla.



Función	Descripción
Crear una alerta de estos eventos	El campo Resumen de alerta se rellena con la consulta que produjo las alertas seleccionadas, las cuales seleccionó para crear este incidente. El campo Gravedad refleja la gravedad de la alerta seleccionada, un entero entre 1 y 100.
Nombre	(Obligatorio) Especifica un nombre para identificar el incidente. En el ejemplo, el nombre es Incidente de muestra. Puede proporcionar un nombre que identifique claramente la naturaleza de los eventos que se agregarán a este incidente
Resumen	(Opcional) Especifica una descripción del incidente. Un buen resumen identifica claramente el incidente para otros analistas y encargados de responder.
Usuario asignado	(Opcional) Asigna el incidente a un usuario en el SOC. Si hace clic en Usuario asignado, se abre una lista desplegable que muestra los nombres de usuario del personal del SOC que responden ante incidentes.
Categorías	(Opcional) Identifica las categorías de incidentes. Si hace clic en Categorías, se abre una lista desplegable de categorías y subcategorías de incidentes. Puede seleccionar una o más categorías a las cuales pertenece el incidente. Las categorías se dividen en estos grupos principales: Ambiental, error, hacking, malware, uso indebido y redes sociales.
Prioridad	Identifica la prioridad del incidente. Si hace clic en Prioridad, se abre una lista desplegable de prioridades: En la lista desplegable, se muestra crítica, alta, media o baja.

Función	Descripción
Cancelar	Cierra el cuadro de diálogo sin guardar los cambios.
Guardar	Guarda el incidente y cierra el cuadro de diálogo. Un mensaje confirma que el incidente se creó correctamente.

Vista Análisis de eventos

En la vista Análisis de eventos, los analistas pueden ver eventos crudos y metadatos con funciones interactivas que mejoran la capacidad de encontrar patrones significativos en los datos. Esta es una alternativa a la vista Reconstrucción de evento estática. En esta vista, puede examinar eventos de red, registros y terminales. La vista Análisis de eventos ofrece reconstrucción de paquetes, texto y registros, y no es compatible directamente con la reconstrucción de correo electrónico y web. Sin embargo, en la versión 11.1 y superior, puede abrir una reconstrucción de correo electrónico o web de los resultados actuales en la reconstrucción de correo electrónico o web de la vista Eventos.

Nota: El administrador configura el permiso para que los analistas accedan a esta vista. Si el administrador no le otorgó acceso y usted navega a la vista Análisis de eventos de cualquier otra forma, se muestra el siguiente mensaje: `Forbidden. You cannot access the requested page.` Por ejemplo, si está viendo una reconstrucción en la vista Eventos e intenta ver la misma reconstrucción en la vista Análisis de eventos, verá el mensaje `Forbidden`.

Los eventos que se muestran en la vista Análisis de eventos corresponden al punto de desglose actual en la Vista Navegar o en la vista Eventos. A partir de la versión 11.1, los eventos pueden ser los resultados de una consulta ingresada en la ruta de navegación de la vista Análisis de eventos. Independientemente del origen de la consulta, la vista Análisis de eventos enumera los eventos por hora. Puede volver a ordenar y cambiar el tamaño de las columnas. En la versión 11.1 y superior, también puede elegir las columnas que desea ver y seleccionar uno de los grupos de columnas incorporados o un grupo de columnas personalizado.

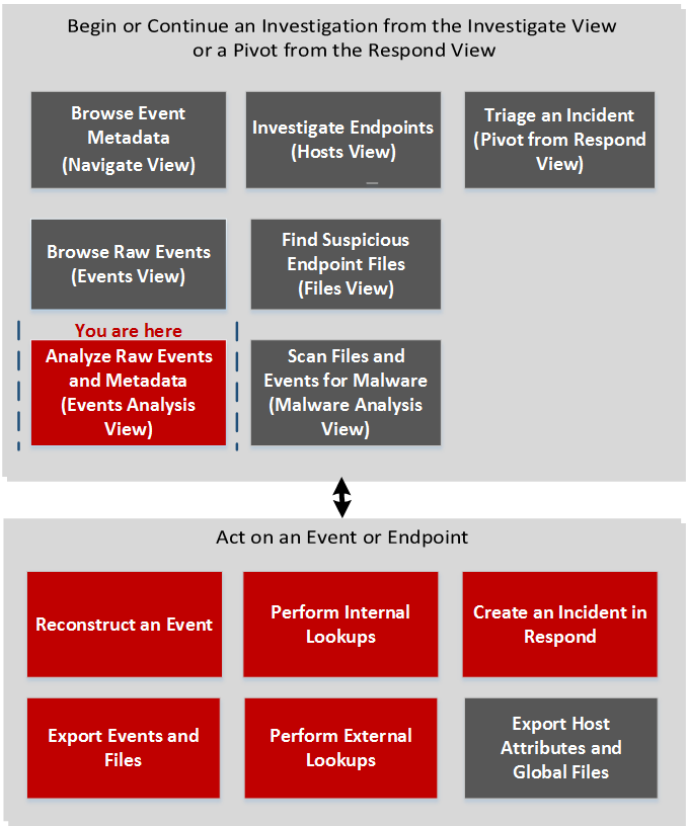
Cuando hace clic en un evento, el panel Detalles del evento de red, Detalles del evento de registro o Detalles del evento de Endpoint se abre en la misma ventana del navegador. Cada tipo de evento tiene uno o más tipos de análisis: Análisis de texto, Análisis de paquetes y Análisis de archivos.

En esta vista hay varios puntos de acceso, los que se describen en Comenzar una investigación en la vista Análisis de eventos.

Nota: Si tiene acceso a Análisis de eventos desde la vista Respond, puede ver el Análisis de eventos para un evento seleccionado en un incidente; las opciones son un subconjunto de las opciones disponibles cuando abre un evento desde la vista Investigar. Para obtener la funcionalidad completa y examinar otros eventos, puede ir directamente a la vista Análisis de eventos (INVESTIGAR > Análisis de eventos).

Flujo de trabajo

La siguiente figura es un flujo de trabajo general que ilustra las tareas que puede realizar en NetWitness Investigate. Las tareas de la vista Análisis de eventos se resaltan en rojo.



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos*	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	consultar eventos en la vista Análisis de eventos (versión 11.1) *	Filtrar los resultados en la vista Análisis de eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	exportar eventos y archivos en la vista Análisis de eventos*	Descargar los datos en la vista Análisis de eventos
Buscador de amenazas	reconstruir eventos en la vista Análisis de eventos*	Examinar eventos en la vista Análisis de eventos
Buscador de amenazas	realizar búsquedas externas desde la vista Análisis de eventos (versión 11.1)*	Realizar acciones en datos en la vista Análisis de eventos
Buscador de amenazas	consultar eventos en la vista Navegar	Investigación de metadatos en la vista Navegar
Buscador de amenazas	consultar eventos en la vista Eventos	Análisis de eventos crudos en la vista Eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Análisis de eventos: Panel Análisis de paquetes
- Vista Análisis de eventos: Panel Análisis de texto
- Vista Análisis de eventos: Panel Análisis de archivos

Vista rápida

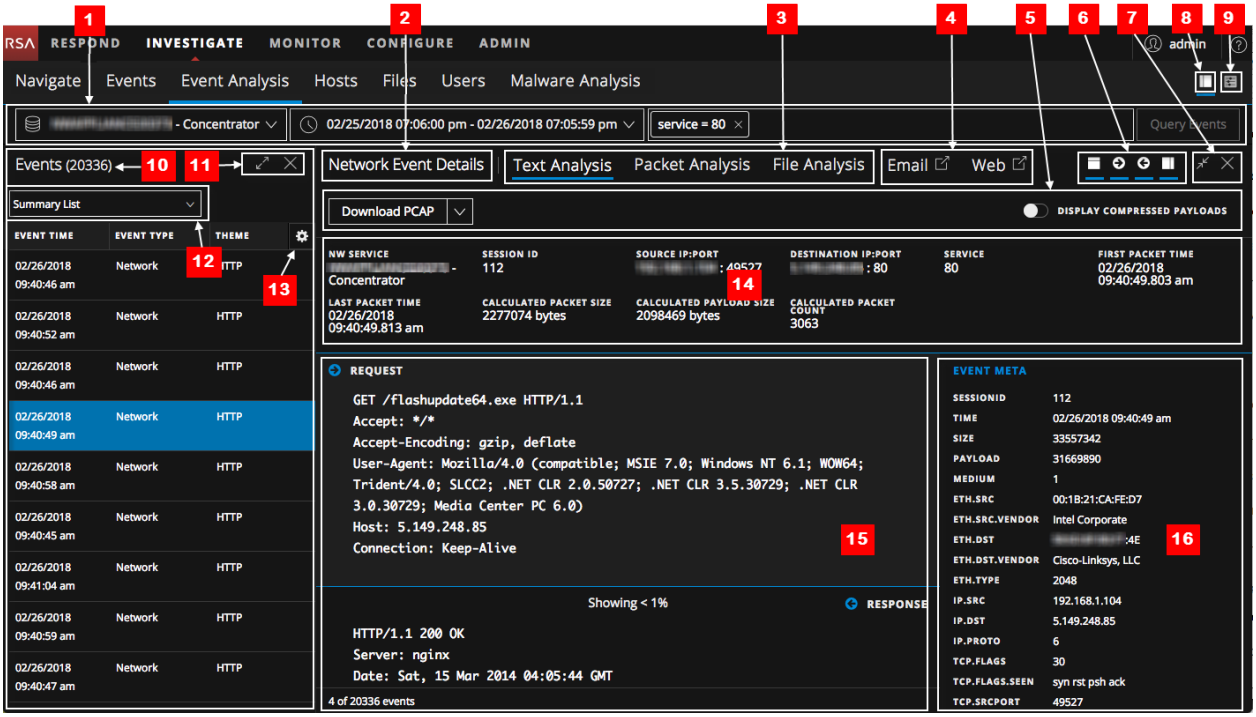
Cuando abre Investigate por primera vez, se muestran los campos de entrada de una consulta, lo que le permite seleccionar un servicio y un rango de tiempo, además de escribir una consulta opcional.

- En la versión 11.0, los campos de entrada están en las vistas Navegar y Eventos.
- En la versión 11.1, los campos de entrada están en las vistas Navegar, Eventos y Análisis de eventos.

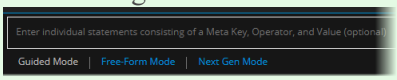
Cuando abre un punto de desglose en la vista Análisis de eventos, el servicio que se investiga cuenta los resultados de la consulta inicial hasta un límite de 100,000 eventos, y los primeros 100 eventos (paquetes, registros y terminales) se cargan en el panel Eventos. Las columnas del panel Eventos son Hora del evento, Tipo de evento (red, registro o terminal), Tamaño de evento y Resumen. Puede realizar lo siguiente:

- Desplazarse por la lista y hacer clic en **Cargar más** para ver los próximos 100 eventos.
- Seleccionar un grupo de columnas (versión 11.1 y superior).
- Seleccionar las columnas que desea incluir (versión 11.1 y superior).
- Arrastrar las columnas para cambiar el orden.
- Hacer que las columnas sean más anchas o angostas.
- Ver el análisis de un evento.

En la siguiente figura se resaltan las funciones principales de la vista Análisis de eventos para la versión 11.1 y superior.



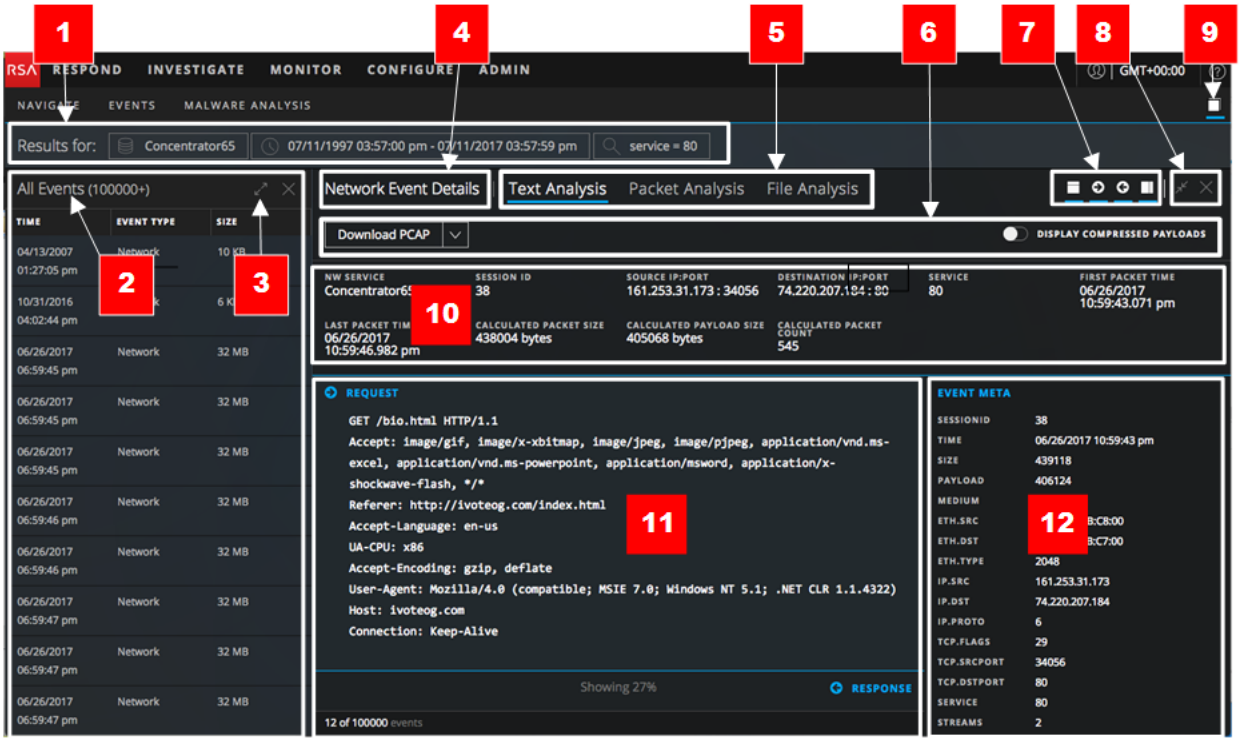
Nota: En la versión 11.2 se incluyó una característica beta no documentada, denominada modo de Última generación, en la vista Análisis de eventos del generador de consultas, que aún estaba en fase de desarrollo y pruebas; el modo de Última generación se deshabilitó en el parche 11.2.0.1. Si ve el modo de Última generación, no lo use; debe utilizar solamente el Modo guiado y el Modo de formato libre en el generador de consultas para asegurarse de obtener resultados coherentes y predecibles.



1 **Ruta de navegación interactiva**: Cuando se selecciona un servicio, muestra el selector de

	servicios, el selector de rango de tiempo y las consultas que se ingresaron. En la versión 11.1 y superior, puede seleccionar un servicio, como se describe en Comenzar una investigación en la vista Análisis de eventos, y acotar la consulta, como se describe en Filtrar los resultados en la vista Análisis de eventos. Cuando hace clic en el botón **Enviar consulta**, se envía la consulta y se solicita al servicio seleccionado que cargue los datos.
2	El tipo de evento que se analiza se refleja en el encabezado: **Detalles del evento de red**, **Detalles del evento de registro** o **Detalles del evento de Endpoint**. Cada vista se analiza en detalle en Examinar eventos en la vista Análisis de eventos.
3	Los tipos de análisis disponibles para el tipo de evento. Los eventos de red pueden usar todos los tipos de análisis: texto, paquetes y archivos. Los eventos de registro y terminal usan únicamente el análisis de texto.
4	Los tipos de análisis Correo electrónico y Web abren el evento actual como una reconstrucción de correo electrónico o web en la vista Eventos.
5	Estas opciones varían para los distintos tipos de análisis. Se analizan en detalle en Examinar eventos en la vista Análisis de eventos.
6	Controles para mostrar u ocultar el encabezado del evento, mostrar u ocultar solicitudes y respuestas, y abrir el panel Metadatos de eventos (16). Estos controles se describen en Examinar eventos en la vista Análisis de eventos.
7, 11	Controles para cambiar el tamaño del panel y cerrarlo.
8	Vuelve a abrir el panel Eventos o el Panel Metadatos de eventos si lo cerró.
9	Configura las preferencias de la vista Análisis de eventos (consulte Configurar la vista Análisis de eventos).
10	El panel Eventos para la versión 11.1 es interactivo y muestra los resultados de las consultas a medida que se envían consultas actualizadas. El panel Eventos incluye un conteo de los eventos. Puede volver a ordenar y cambiar el tamaño de las columnas. Puede desplazarse hasta la parte inferior de la lista y cargar más eventos (consulte Examinar eventos en la vista Análisis de eventos).
12	La lista desplegable Grupo de columnas enumera grupos de columnas incorporados y personalizados que se pueden aplicar al panel Eventos. Los grupos de columnas incorporados son Análisis de correo electrónico, Análisis de terminales, Análisis de malware, HTTP de salida, Protocolos SSL/TLS de salida y Lista de resumen. Lista de resumen es el grupo de columnas predeterminado.
13	Configuración para seleccionar las columnas que se incluyen en el panel Eventos.
14	El encabezado del evento proporciona información resumida acerca del evento. Esta información es diferente para los distintos tipos de eventos (paquetes, registros y terminal).
15	Los datos de eventos (en ocasiones denominados carga útil para los paquetes). Los datos de eventos para un evento de registro o de terminal suelen ser una línea de texto desde el registro crudo en lugar de una solicitud y una respuesta que se muestra para un paquete.
16	El Panel Metadatos de eventos enumera las claves y los valores de metadatos que se encuentran en los datos. Algunos metadatos permiten búsquedas; tienen un icono de binoculares en el que puede hacer clic para ver los datos asociados destacados en los datos del evento (consulte Examinar eventos en la vista Análisis de eventos).

En la siguiente figura se resaltan las funciones principales de la vista Análisis de eventos para la versión 11.0.0.x.



1	La ruta de navegación de solo lectura muestra el servicio seleccionado, el rango de tiempo y la consulta ingresada en las vistas Navegar o Eventos.
2	Esta es una lista de eventos de solo lectura que se basa en la consulta realizada en la vista Navegar o en la vista Eventos. El panel Eventos incluye un conteo de los eventos. Puede volver a ordenar y cambiar el tamaño de las columnas. Puede desplazarse hasta la parte inferior de la lista y cargar más eventos (consulte Examinar eventos en la vista Análisis de eventos).
3, 8	Controles para cambiar el tamaño del panel y cerrarlo.
4	El tipo de evento que se analiza se refleja en el encabezado: Detalles del evento de red, Detalles del evento de registro o Detalles del evento de Endpoint. Cada vista se analiza en detalle en Examinar eventos en la vista Análisis de eventos.
5	Los tipos de análisis disponibles para el tipo de evento. Los eventos de red pueden usar los tres tipos de análisis: texto, paquetes y archivos. Los eventos de registro y terminal usan únicamente el análisis de texto.
6	Estas opciones varían para los distintos tipos de análisis. Se analizan en detalle en Examinar eventos en la vista Análisis de eventos.
7	Controles para mostrar u ocultar el encabezado del evento, mostrar u ocultar solicitudes y respuestas, y abrir el panel Metadatos de eventos (12). Estos controles se describen en Examinar eventos en la vista Análisis de eventos.
9	Vuelve a abrir el panel Eventos o el Panel Metadatos de eventos si lo cerró.
10	El encabezado del evento proporciona información resumida acerca del evento. Esta información es diferente para los distintos tipos de eventos (paquetes, registros y terminal).
11	Los datos de eventos (en ocasiones denominados carga útil para los paquetes). Los datos de eventos para un evento de registro o de terminal suelen ser una línea de texto desde el registro

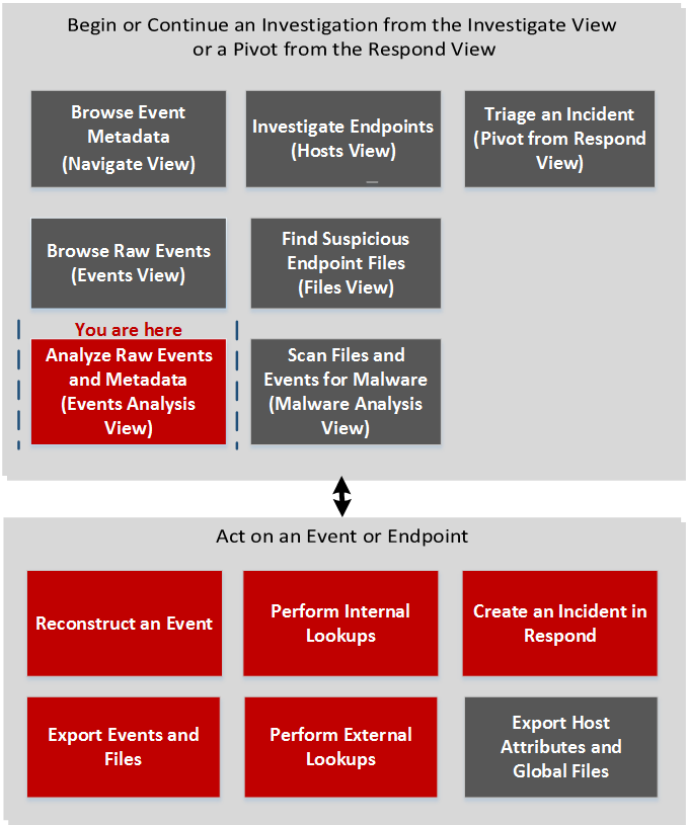
crudo en lugar de una solicitud y una respuesta que se muestra para un paquete.

12 El Panel Metadatos de eventos enumera las claves y los valores de metadatos que se encuentran en los datos. Algunos metadatos permiten búsquedas; tienen un icono de binoculares en el que puede hacer clic para ver los datos asociados destacados en los datos del evento (consulte Examinar eventos en la vista Análisis de eventos).

Vista Análisis de eventos: Panel Análisis de archivos

El panel Análisis de archivos (**Análisis de eventos** > **Análisis de archivos),** permite ver una lista de archivos de manera segura y descargar uno o más archivos en un evento.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	consultar eventos en la vista Análisis de eventos (versión 11.1)	Filtrar los resultados en la vista Análisis de eventos
Buscador de amenazas	exportar eventos y archivos en la vista Análisis de eventos*	Descargar los datos en la vista Análisis de eventos
Buscador de amenazas	reconstruir eventos en la vista Análisis de eventos	Examinar eventos en la vista Análisis de eventos
Buscador de amenazas	realizar búsquedas externas desde la vista Análisis de eventos (versión 11.1)	Realizar acciones en datos en la vista Análisis de eventos
Buscador de amenazas	consultar eventos en la vista Navegar	Investigación de metadatos en la vista Navegar
Buscador de amenazas	consultar eventos en la vista Eventos	Análisis de eventos crudos en la vista Eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*

*Puede realizar esta tarea en la vista actual.

Temas relacionados

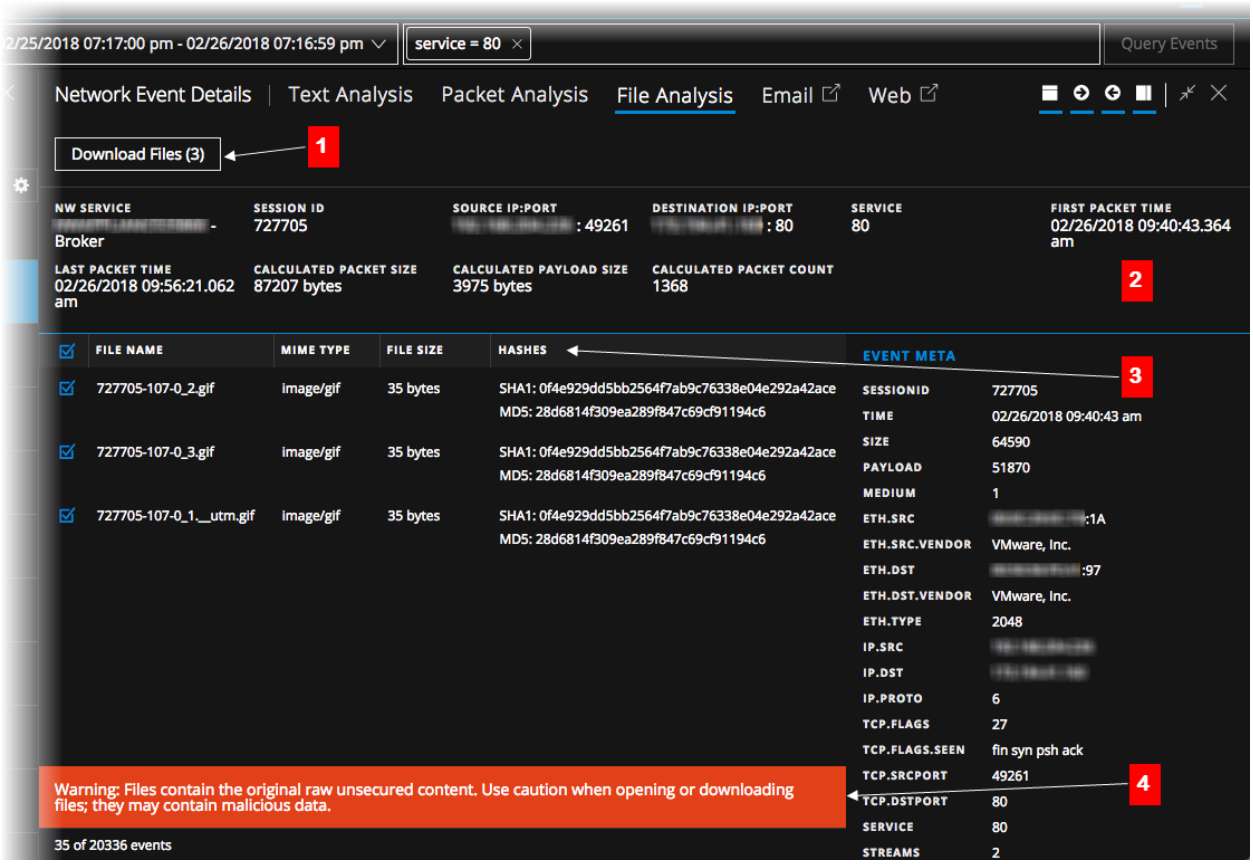
- Cómo funciona NetWitness Investigate
- Vista Análisis de eventos
- Vista Análisis de eventos: Panel Análisis de texto
- Vista Análisis de eventos: Panel Análisis de paquetes

Vista rápida

En el panel Análisis de archivos se muestra una lista de archivos asociados con un evento de red. Puede descargar archivos en esta vista.

Este es un ejemplo del panel del análisis de archivos con funciones con las etiquetas.

Nota: Los tipos de reconstrucción Correo electrónico y Web en la parte superior de la figura están disponibles en la versión 11.1 y superior.

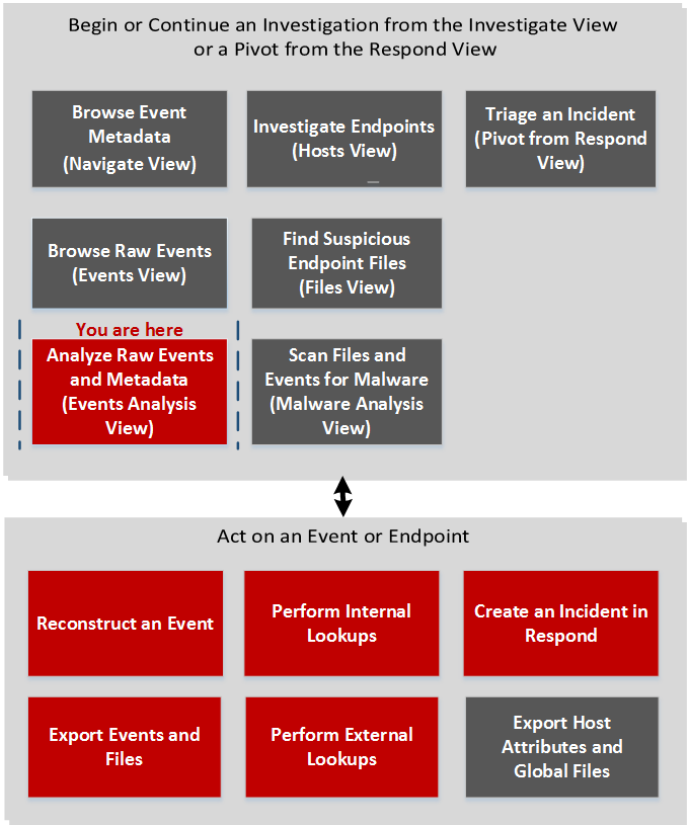


1. Haga clic para descargar uno o más archivos seleccionados.
2. El encabezado del evento muestra información de resumen acerca del evento de red que contiene los archivos.
3. Lista desplazable de archivos asociados que puede seleccionar y descargar.
4. Recuerde que se requiere precaución cuando se descargan archivos potencialmente maliciosos.

Vista Análisis de eventos: Panel Análisis de paquetes

El panel Análisis de paquetes (**Análisis de eventos > Análisis de paquetes)** permite ver de manera segura y analizar de manera interactiva los paquetes y la carga útil de un evento.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	consultar eventos en la vista Análisis de eventos (versión 11.1)	Filtrar los resultados en la vista Análisis de eventos
Buscador de amenazas	exportar eventos y archivos en la vista Análisis de eventos*	Descargar los datos en la vista Análisis de eventos
Buscador de amenazas	reconstruir eventos en la vista Análisis de eventos *	Examinar eventos en la vista Análisis de eventos
Buscador de amenazas	realizar búsquedas externas desde la vista Análisis de eventos (versión 11.1)*	Realizar acciones en datos en la vista Análisis de eventos
Buscador de amenazas	consultar eventos en la vista Navegar	Investigación de metadatos en la vista Navegar
Buscador de amenazas	consultar eventos en la vista Eventos	Análisis de eventos crudos en la vista Eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Análisis de eventos
- Vista Análisis de eventos: Panel Análisis de texto
- Vista Análisis de eventos: Panel Análisis de archivos

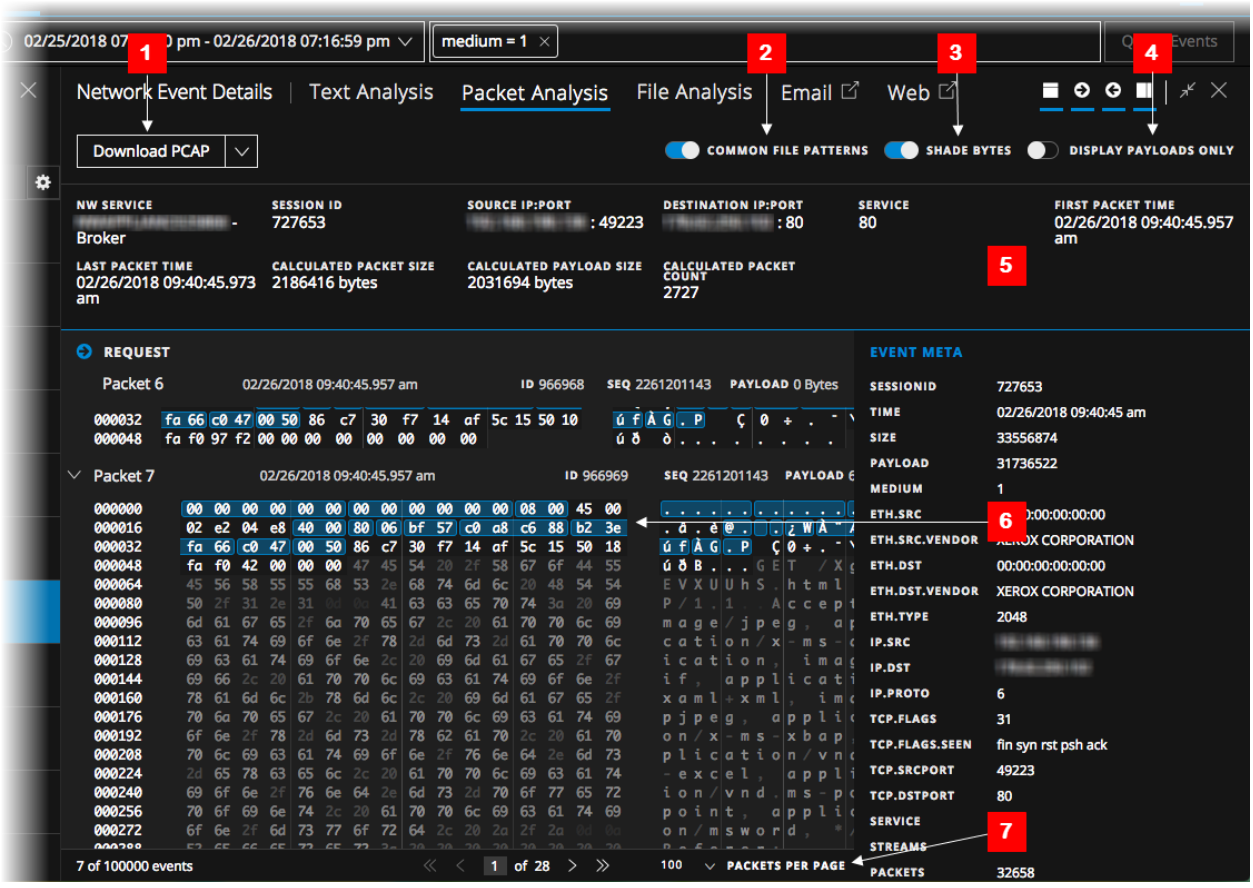
Vista rápida

Solo se pueden analizar eventos de red en el panel Análisis de paquetes. El panel Análisis de paquetes enumera cada paquete en el evento. La lista de paquetes permite el desplazamiento. Cuando se desplaza, la información de identificación de texto o del paquete, así como las etiquetas Solicitud y Respuesta, permanecen visibles en lugar de desplazarse fuera de la vista.

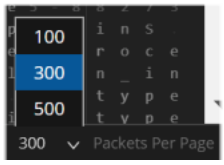
En la versión 11.1 y superior, puede usar controles de paginación para avanzar y retroceder en las páginas, ir a una página específica y seleccionar la cantidad de paquetes que se muestran por página (100, 300 o 500).

Cada paquete se muestra con sombreado y resaltado como ayuda para identificar patrones de archivo comunes: bytes de encabezado y carga útil significativos, bytes hexadecimales y ASCII, y firmas de archivo comunes. Además, puede ajustar la visualización de solicitudes/respuestas y mostrar u ocultar el resumen del paquete.

Este es un ejemplo del panel Análisis de paquetes con etiquetas para identificar las funciones. Para obtener detalles y ejemplos de cada función, consulte Examinar eventos en la vista Análisis de eventos.



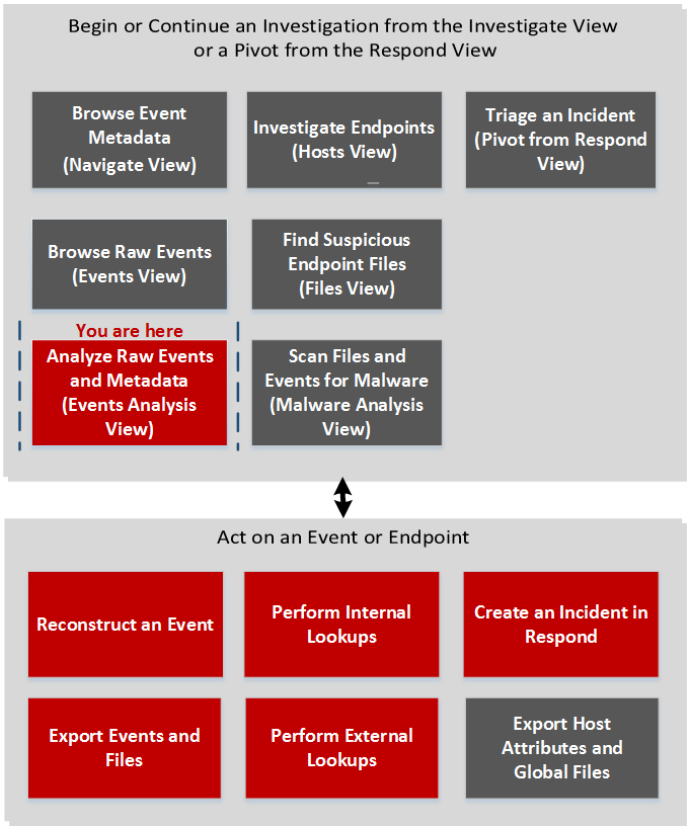
1	Opciones para exportar un evento de red. Puede exportar una PCAP, todas las cargas útiles, las cargas útiles de solicitud o las cargas útiles de respuesta para realizar un análisis más detallado y compartir con otros.
2	De forma predeterminada, la opción para identificar firmas de archivo comunes está activada. Las firmas de archivo comunes se resaltan de color naranja; cuando se coloca el cursor sobre el resaltado, se revela el tipo de archivo.

3	La opción Sombrear bytes agrega sombreado para identificar los distintos bytes hexadecimales (de 00 a FF) mediante grados de resaltado.
4	La opción de mostrar solo las cargas útiles oculta los encabezados de los paquetes, lo que deja más espacio para la carga útil.
5	El encabezado del evento.
6	Los bytes significativos se resaltan con un fondo azul; a medida que pasa el cursor sobre el resaltado, los metadatos se muestran en un cuadro activado con el puntero.
7	(Versión 11.1 y superior) Los controles de paginación de paquetes permiten una mayor flexibilidad en la paginación a través de una lista de paquetes. Cuando un control no está disponible, la imagen aparece atenuada; por ejemplo, mientras ve la página 1, los controles ⟪ y ⟨ aparecen atenuados. ⟪: Ir a la primera página ⟨: Ir a la página anterior 1 of 206: Ir a una página específica ⟩: Ir a la página siguiente ⟫: Ir a la última página  : Seleccione la cantidad de paquetes por página

Vista Análisis de eventos: Panel Análisis de texto

El panel Análisis de texto (**Análisis de eventos > Análisis de texto)** permite ver y analizar de manera segura la carga útil de texto crudo de un evento. El panel Análisis de texto incluye funciones que pueden mostrar texto descomprimido o comprimido, ampliar entradas truncadas, realizar codificación y decodificación URL y Base64, y descargar eventos de red, registros y eventos de terminal. El panel Análisis de texto está disponible para todos los tipos de eventos: red, registro y terminal.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	consultar eventos en la vista Análisis de eventos (versión 11.1)	Filtrar los resultados en la vista Análisis de eventos
Buscador de amenazas	exportar eventos y archivos en la vista Análisis de eventos*	Descargar los datos en la vista Análisis de eventos
Buscador de amenazas	reconstruir eventos en la vista Análisis de eventos*	Examinar eventos en la vista Análisis de eventos
Buscador de amenazas	realizar búsquedas externas desde la vista Análisis de eventos (versión 11.1)*	Realizar acciones en datos en la vista Análisis de eventos
Buscador de amenazas	consultar eventos en la vista Navegar	Investigación de metadatos en la vista Navegar
Buscador de amenazas	consultar eventos en la vista Eventos	Análisis de eventos crudos en la vista Eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*

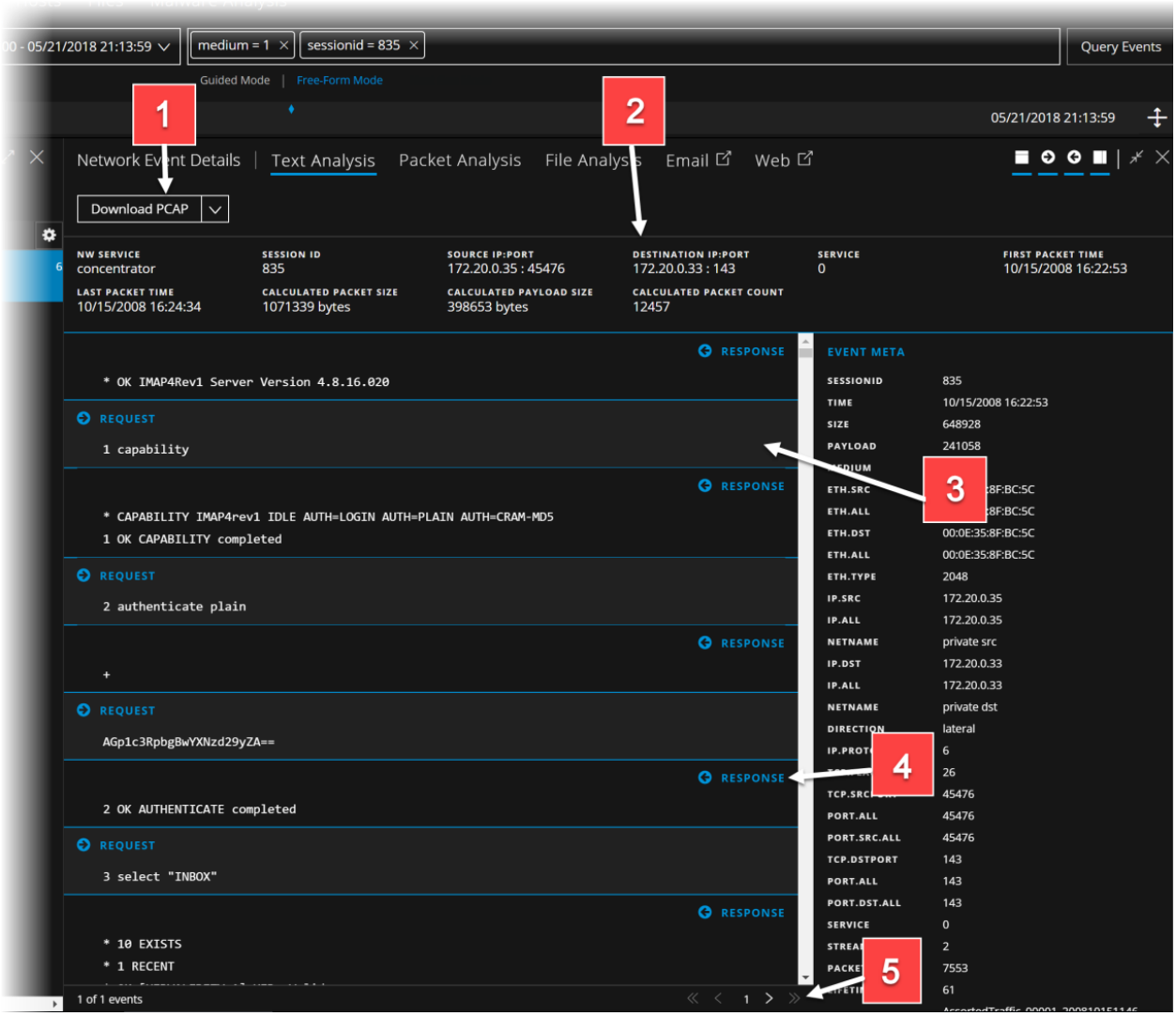
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Análisis de eventos
- Vista Análisis de eventos: Panel Análisis de paquetes
- Vista Análisis de eventos: Panel Análisis de archivos

Vista rápida

La vista Análisis de eventos muestra el texto de un único evento en el panel Análisis de texto. Cuando hace clic en un evento del panel Lista de eventos, el panel adyacente muestra el Análisis de texto. En el panel Análisis de texto solo se muestra el registro crudo para eventos de registro y de terminal. En el caso de los eventos de red, la dirección del paquete (Solicitud o Respuesta) y el contenido de cada paquete se proporciona en formato de texto. Para obtener más ejemplos del Análisis de texto, consulte Análisis de eventos crudos y metadatos en la vista Análisis de eventos. Para conocer los procedimientos detallados, consulte Examinar eventos en la vista Análisis de eventos.



1	Opciones para exportar un registro, una PCAP o archivos con el fin de realizar un análisis más detallado y compartir con otros. Este menú de descarga es para los datos de red.
2	La información de encabezado del evento.
3	La carga útil de un evento de red incluye solicitudes y respuestas. Este es el lado de la solicitud del paquete.
4	Este es el lado de la respuesta del paquete.
5	(Versión 11.2 y superior) Los controles de paginación de eventos permiten una mayor flexibilidad

en la paginación a través de una lista de eventos. Cuando un control no está disponible, la imagen aparece atenuada; por ejemplo, mientras ve la página 1, los controles y aparecen atenuados.

: Ir a la primera página

: Ir a la página anterior

: Ir a la página siguiente

: Ir a la última página (está disponible solamente después de que se ha navegado a la última página)

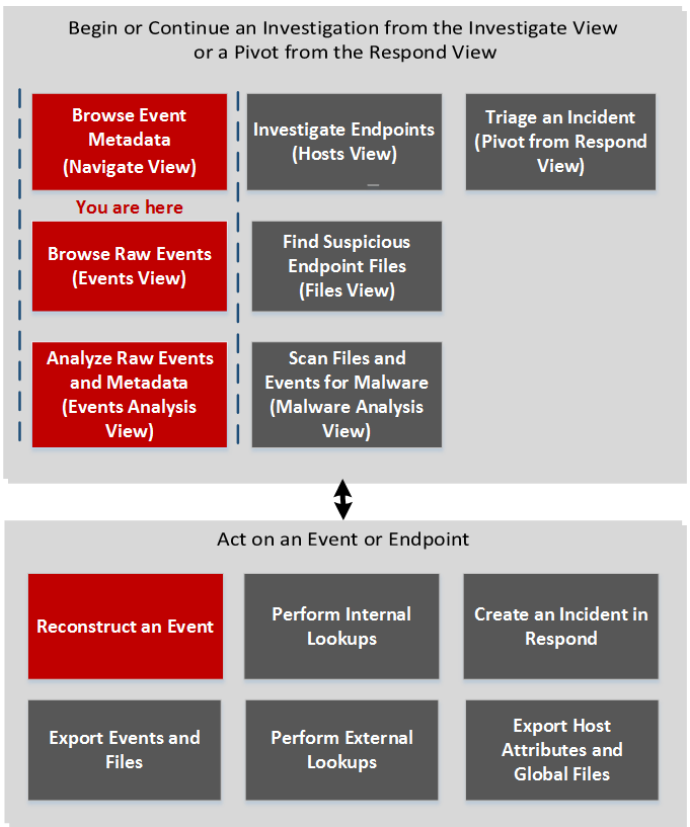
Vista Reconstrucción de evento

En la vista Reconstrucción de evento se proporciona la reconstrucción de un evento seleccionado desde la Vista Eventos. De forma predeterminada, NetWitness Platform muestra la mejor reconstrucción para el evento, según lo determina el contenido del evento, o la reconstrucción predeterminada que seleccionó en la configuración Vista de sesión predeterminada para Investigate. Puede utilizar las opciones de la barra de herramientas Reconstrucción de evento para cambiar el método de reconstrucción, ver los resultados de arriba abajo o en paralelo, exportar un evento, exportar valores de metadatos, extraer archivos, abrir archivos adjuntos del correo electrónico y abrir el evento en una nueva pestaña.

Para tener acceso a esta vista, realice una de las opciones siguientes:

- En cualquier vista Eventos, haga doble clic en un evento.
- En la vista Eventos con la Vista detallada seleccionada, haga clic con el botón secundario en **Análisis de eventos** al final del evento y seleccione **Reconstrucción de evento.**
- En la barra de herramientas Reconstrucción de evento de la reconstrucción con vista previa, haga clic en **Abrir evento en nueva pestaña**.
- En la vista Navegar, seleccione **Acciones > Ir a evento en Reconstrucción de evento** e ingrese un ID de evento.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	reconstruir un evento	Reconstruir un evento
Buscador de amenazas	extraer archivos de un evento reconstruido	Reconstruir un evento

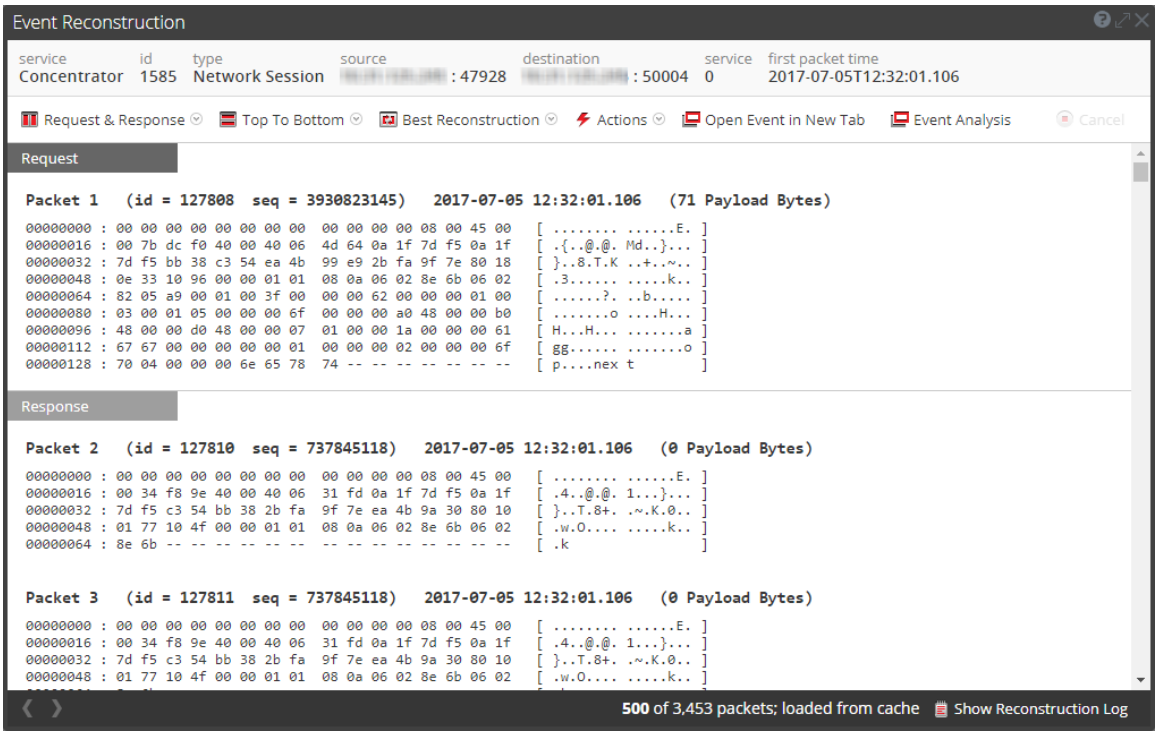
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Análisis de eventos

Vista rápida

Esta figura es un ejemplo de la vista Reconstrucción de evento. En la siguiente tabla se describen las opciones de la barra de herramientas.



Función	Descripción
Solicitud y respuesta	Muestra un menú desplegable que permite seleccionar si la vista muestra: • Solicitud y respuesta • Solicitud • Respuesta
Organización	Muestra un menú desplegable que permite seleccionar si la información se presenta de arriba abajo o en paralelo.
Ver	Muestra un menú desplegable que permite seleccionar la información que se presenta. De forma predeterminada, la opción Mejor reconstrucción está seleccionada. Otras opciones son: • Ver metadatos • Ver texto • Ver valor hexadecimal • Ver paquetes • Ver web • Ver correo • Ver archivos

Función	Descripción
Acciones	Muestra un menú desplegable con las acciones disponibles en la vista Reconstrucción de evento.
Abrir evento en nueva pestaña	Abre el evento en una nueva pestaña del navegador.

Debajo de la barra de herramientas hay una lista de claves de metadatos y valores. Algunas de las claves ofrecen un menú desplegable con acciones disponibles.

La barra de la parte inferior de la vista ofrece varias opciones.

Función	Descripción
	Muestra el evento anterior.
	Muestra el evento siguiente.
Mostrar registro de reconstrucción	Muestra el registro de reconstrucción en la parte inferior de la vista. Cuando hace clic en el botón, este cambia a Ocultar registro de reconstrucción.

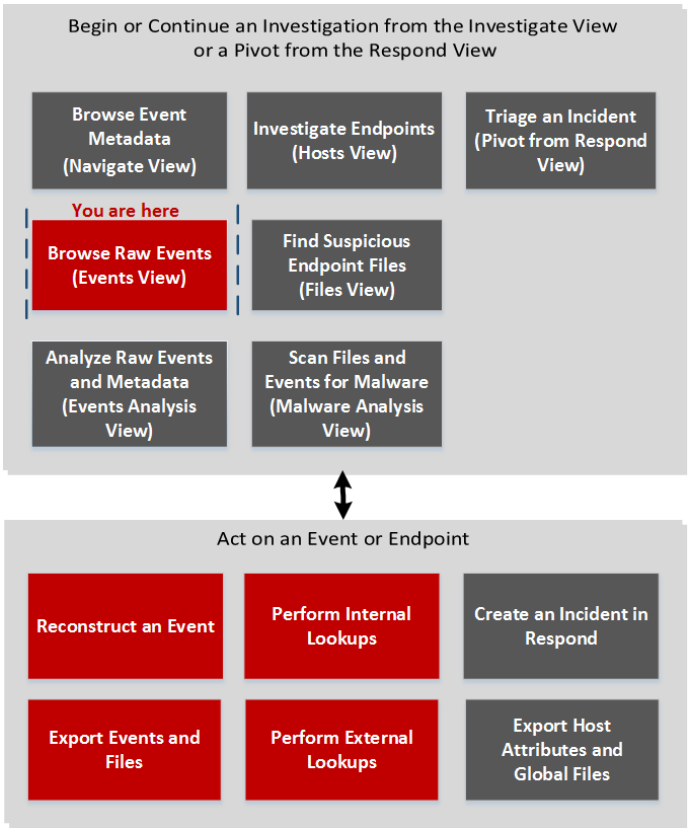
Vista Eventos

En la Vista Eventos está disponible una lista de eventos asociados a una sesión; esta vista está optimizada para ver eventos crudos en secuencia por hora. Puede mostrar la lista de eventos en varios formatos, filtrar eventos, buscar eventos y abrir una reconstrucción de un evento.

Existen dos maneras de mostrar la vista Eventos:

- Vaya a **INVESTIGAR > Eventos.** NetWitness Platform ejecuta una consulta predeterminada acerca de las últimas tres horas para el servicio predeterminado (si hay uno configurado) o muestra un cuadro de diálogo en el cual puede seleccionar un servicio y, a continuación, ejecuta la consulta predeterminada. La consulta predeterminada selecciona todos los eventos y la vista Eventos muestra los pertinentes al servicio seleccionado, con los más antiguos en primer lugar.
- En la vista **Navegar**, haga doble clic en un evento. La vista Eventos muestra los eventos en el servicio seleccionado según el punto de desglose en la vista Navegar.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos*	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	configurar las preferencias de usuario para la vista Eventos*	Configurar la vista Navegar y la vista Eventos
Buscador de amenazas	reconstruir un evento*	Reconstruir un evento
Buscador de amenazas	exportar eventos y archivos*	Exportar eventos en la vista Eventos
Buscador de amenazas	realizar búsquedas internas	Buscar contexto adicional en las vistas Navegar y Eventos
Buscador de amenazas	realizar búsquedas externas	Iniciar una búsqueda externa de una clave de metadatos
Buscador de amenazas o encargado de respuesta ante incidentes	agregar uno o más eventos a un incidente existente o a un incidente nuevo*	Agregar eventos a un incidente para Response

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Análisis de eventos crudos en la vista Eventos
- Consulta y realización de acciones en datos en las vistas Navegar y Eventos

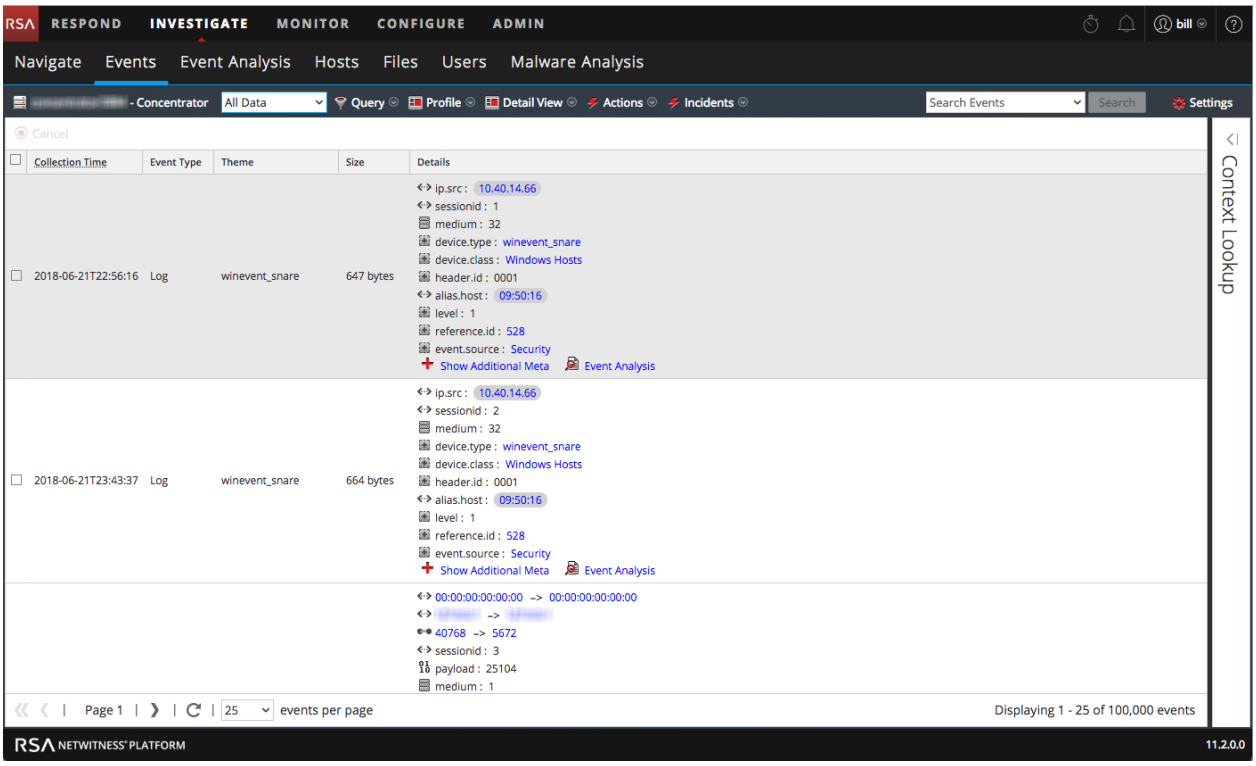
Vista rápida

Esta vista proporciona tres presentaciones incorporadas de datos de eventos: la Vista detallada, la Vista de lista y la Vista de registro. La vista Lista y la Vista detallada están destinadas a la visualización de eventos de paquetes de datos y proporcionan más información para cada evento, que incluye registro de fecha y hora, tipo de evento, tema del evento y tamaño.

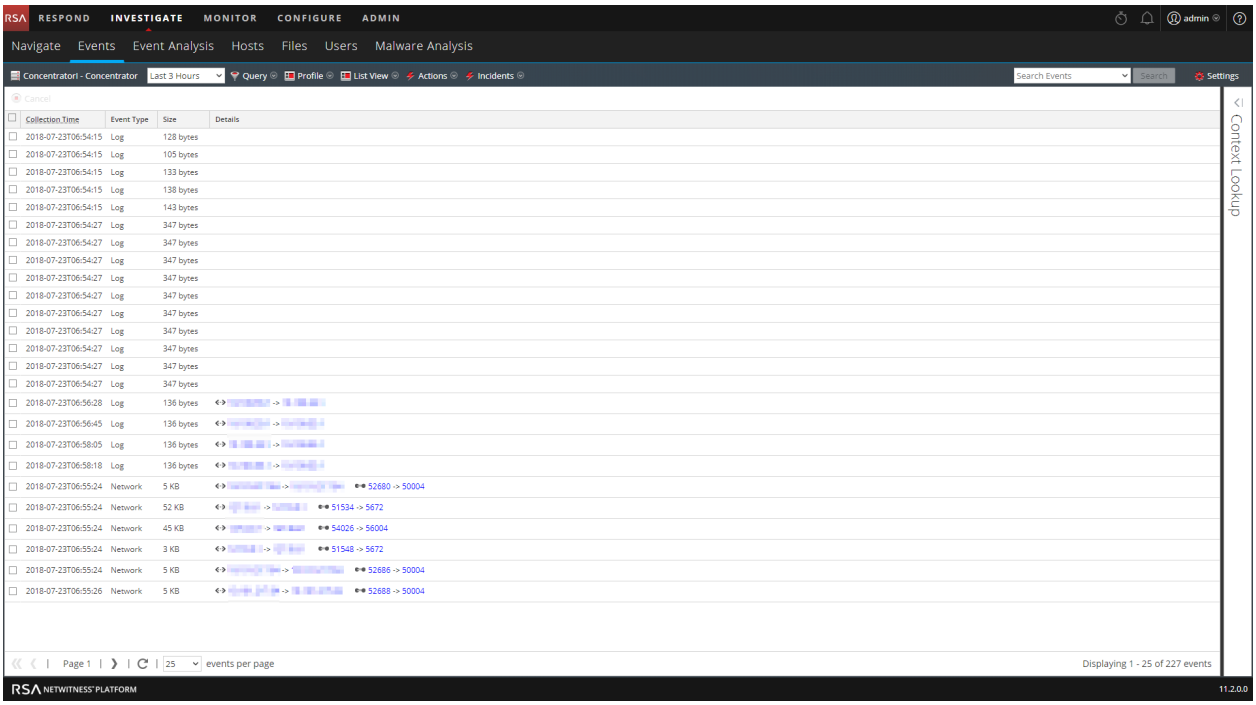
- La vista Lista muestra la información de las direcciones y los puertos de origen y destino correspondientes de los eventos en forma de resumen en un grid.
- La Vista detallada muestra todos los metadatos recopilados del evento en una vista paginada.
- La Vista de registro está optimizada para mostrar información de registro y proporciona más información para cada registro, incluido el registro de fecha y hora, el tipo de evento, el tipo de servicio, la clase de servicio y los registros.

Puede utilizar consultas, la configuración del rango de tiempo y perfiles para filtrar los eventos mostrados en la vista Eventos. Desde cualquier tipo de vista de la vista Eventos, puede extraer archivos, exportar eventos, registros y valores de metadatos, abrir el panel Reconstrucción de evento y abrir el Análisis de eventos.

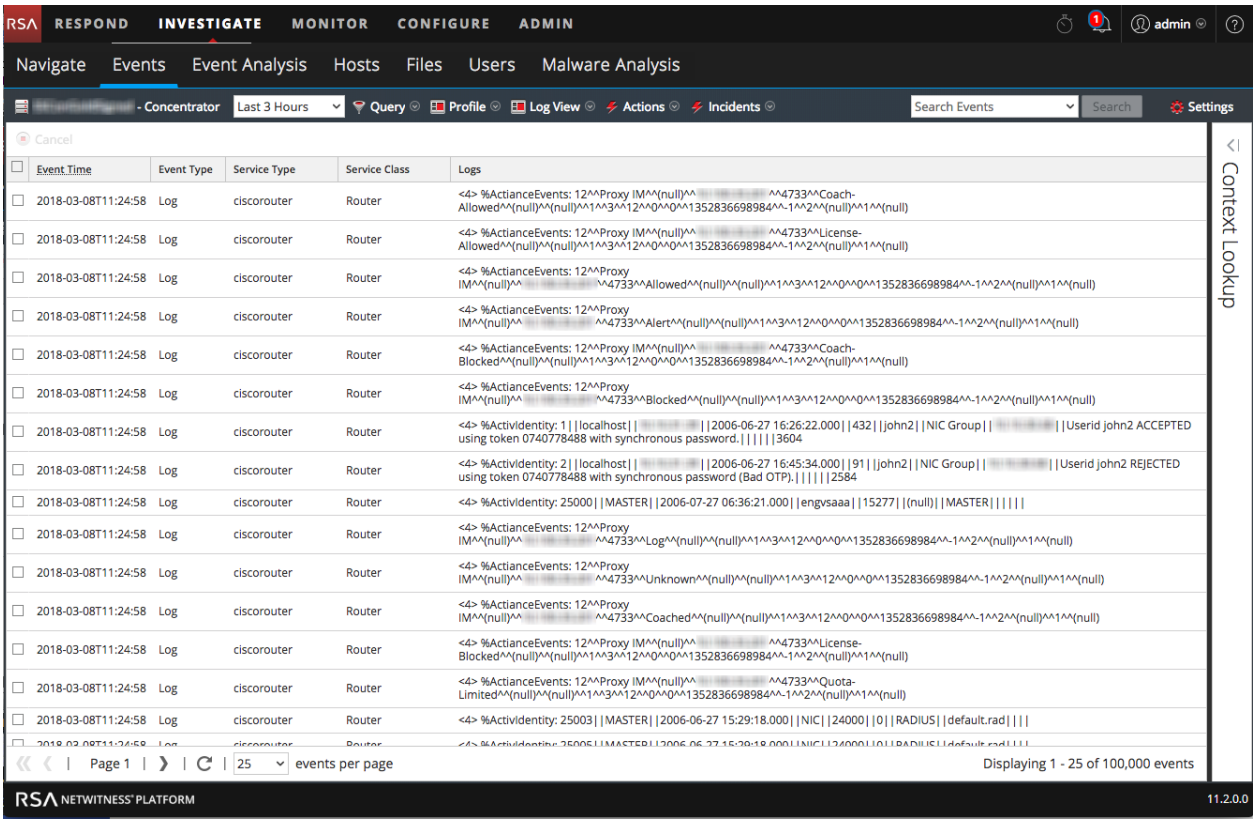
En la siguiente figura se muestra un ejemplo de eventos en la vista detallada. El panel Búsqueda de contexto es visible solo si está configurado el servicio Context Hub.



La siguiente figura es un ejemplo de eventos en la Vista de lista.



La siguiente figura es un ejemplo de la vista de registro.



Descripción detallada

La vista Eventos tiene una barra de herramientas en la parte superior con las siguientes opciones.

Función	Descripción
Seleccionar servicio	Muestra el nombre del servicio seleccionado junto al ícono. Abre el cuadro de diálogo Seleccionar un servicio, donde puede seleccionar un servicio para el cual se muestra la lista de eventos.
Rango de tiempo	Muestra un menú desplegable para seleccionar el rango de tiempo para aplicar a la lista de eventos. Puede elegir una de las opciones estándar o especificar un rango de tiempo personalizado.
Consulta	Se muestra el cuadro de diálogo Crear filtro, en el cual puede ingresar directamente una consulta personalizada en lugar de desglosar a los datos (consulte Crear una consulta personalizada)
Perfil	Muestra el menú Usar perfil; el perfil seleccionado se muestra en la barra de herramientas. Un perfil permite administrar y usar perfiles que pueden incluir grupos de metadatos personalizados, un grupo de columnas predeterminado y una consulta inicial. Los perfiles se aplican a la vista Navegar (consultas y grupos de metadatos) y a la vista Eventos (consultas y grupos de columnas).

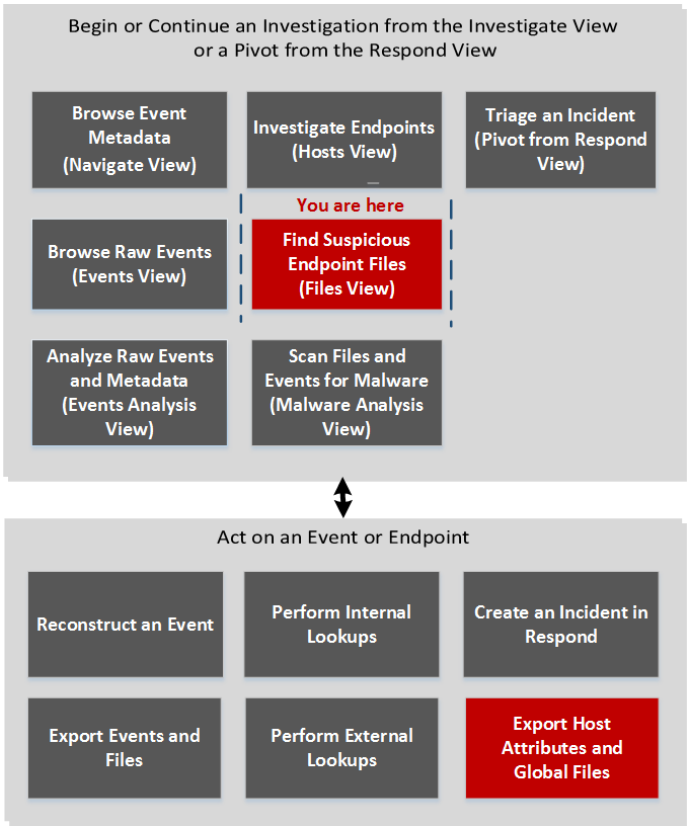
Función	Descripción
Ver el menú despegable de tipo	Muestra un menú desplegable para seleccionar el tipo de vista de evento. • La Vista detallada muestra los eventos en un formato paginado con información detallada de cada evento. • La vista Lista muestra los eventos en formato de cuadrícula con un resumen de cada evento en una fila por separado. • La Vista de registro muestra una cuadrícula de eventos orientados a registros con un resumen de cada registro en una fila por separado. • Grupos de columnas personalizados muestra la lista de eventos mediante el uso de un grupo de columnas seleccionado en una lista desplegable de grupos de columnas personalizados. • Administrar grupos de columnas muestra el cuadro de diálogo para crear y editar grupos de columnas personalizados.
Acciones	Muestra un menú desplegable con acciones en la vista Eventos: • Extraer archivos, exportar eventos como un archivo PCAP, exportar registros o exportar valores de metadatos. • Ver una reconstrucción de evento en una ventana emergente o en una pestaña nueva. • Ver el Análisis de eventos • Restablecer todos los filtros en la ventana Eventos.
Incidentes	Cree un incidente nuevo en Respond y agregue los eventos seleccionados, o agréguelos a un incidente existente en Respond.
Buscar	Muestra las opciones de Buscar eventos, las cuales permiten especificar el formato de exportación de registros y valores de metadatos con opciones adicionales que se explican en Buscar patrones de texto.
Ajustes de configuración	Muestra los ajustes de Investigation para la vista Eventos (los cuales también se pueden editar en la vista Perfil), de modo que puede cambiarlos sin salir de la vista Eventos. Cuando cambia un ajuste en la vista Eventos, este también se cambia en la vista Perfil (consulte Configurar la vista Navegar y la vista Eventos).

Vista Archivos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

En la **vista Archivos** está disponible una lista de archivos ejecutables únicos presentes en la implementación. Para acceder a esta vista, vaya a **INVESTIGAR > Archivos**. De forma predeterminada, la vista Archivos muestra 100 archivos. Para mostrar más archivos, haga clic en **Cargar más** en la parte inferior de la página.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)*	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	exportar atributos de hosts y archivos globales*	Investigar los archivos

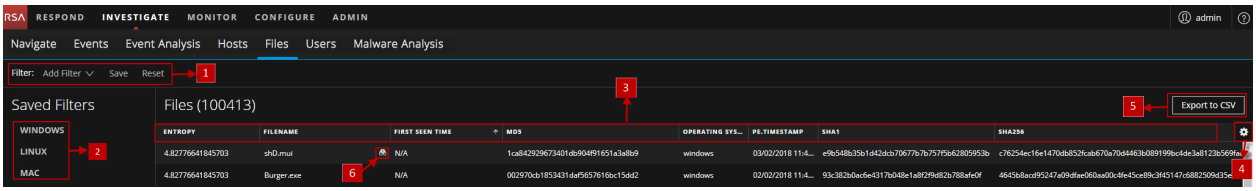
*Puede realizar esta tarea en la vista actual

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos

Vista rápida

Este es un ejemplo de la vista Archivos:



1	**Menú desplegable Agregar filtro**. Puede filtrar los archivos mediante la selección de un sistema operativo (Windows, Linux o Mac) o filtros guardados, o la selección de las opciones del menú desplegable Agregar filtro. Para obtener más información, consulte Filtrar los archivos.
2	**Filtros guardados.** El panel Filtros guardados enumera los filtros guardados. Para obtener más información, consulte Filtrar los archivos.

3 **Ordenar columnas.** Puede ordenar la lista por lo siguiente:

Nombre de archivo: Nombre del archivo.

Hora en que se vio por primera vez: Primera vez que se vio el hash en el host.

Firma: Indica si el archivo está o no firmado y si es o no válido, y proporciona información acerca del signatario.

Tamaño: Tamaño del archivo.

Entropía: Determina si el contenido está comprimido o cifrado.

Formato: Formato del archivo: Windows (PE), Linux (ELF y scripts) y Mac (Macho).

PE.Resources.Company: Nombre de la empresa.

Nota: El orden por columnas distingue mayúsculas de minúsculas. Ordena primero el número y después las mayúsculas y las minúsculas.

4 **Menú Ajustes de configuración.** Puede configurar las preferencias de la vista Archivos mediante la selección de columnas en el menú Ajustes de configuración. Para obtener más información, consulte Configurar preferencias de archivos.

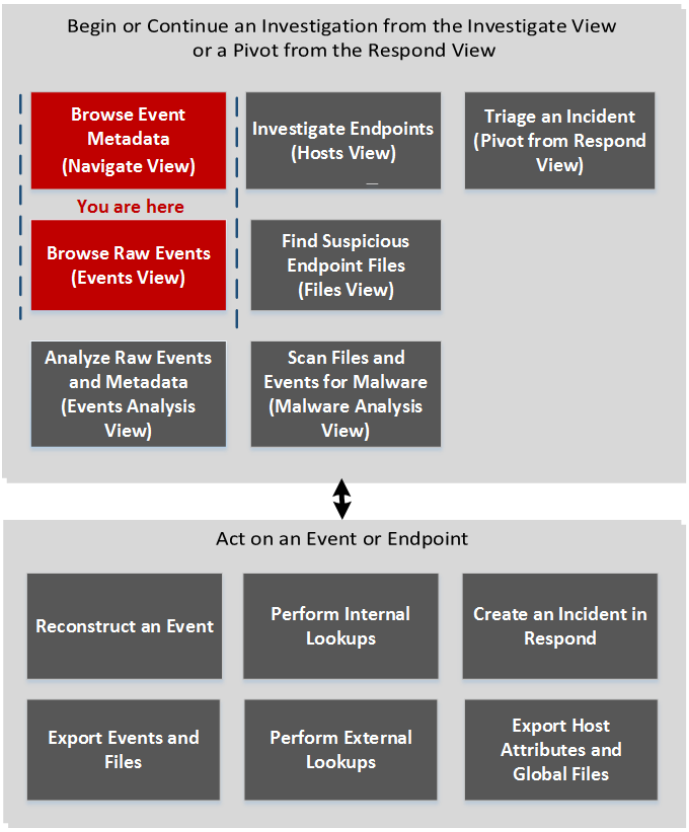
5 **Exportar a CSV**: Extrae archivos globales a un archivo CSV. Para obtener más información, consulte Investigar los archivos.

6 **Cambiar a las vistas Navegar y Análisis de eventos.** Para investigar un nombre de archivo o un hash (SHA256 y MD5) determinados, puede ir a las vistas Navegar y Análisis de eventos. Para obtener más información, consulte Cambiar a las vistas Navegar y Análisis de eventos.

Cuadro de diálogo Investigar

El cuadro de diálogo Investigar permite a los analistas seleccionar un servicio o una recopilación para investigar. El cuadro de diálogo se muestra automáticamente cuando se dirige en primer lugar a la vista Navegar o a la vista Eventos y no ha seleccionado un servicio predeterminado para investigar. Para acceder al cuadro de diálogo desde una investigación actual, seleccione el nombre actual del servicio en la barra de herramientas.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

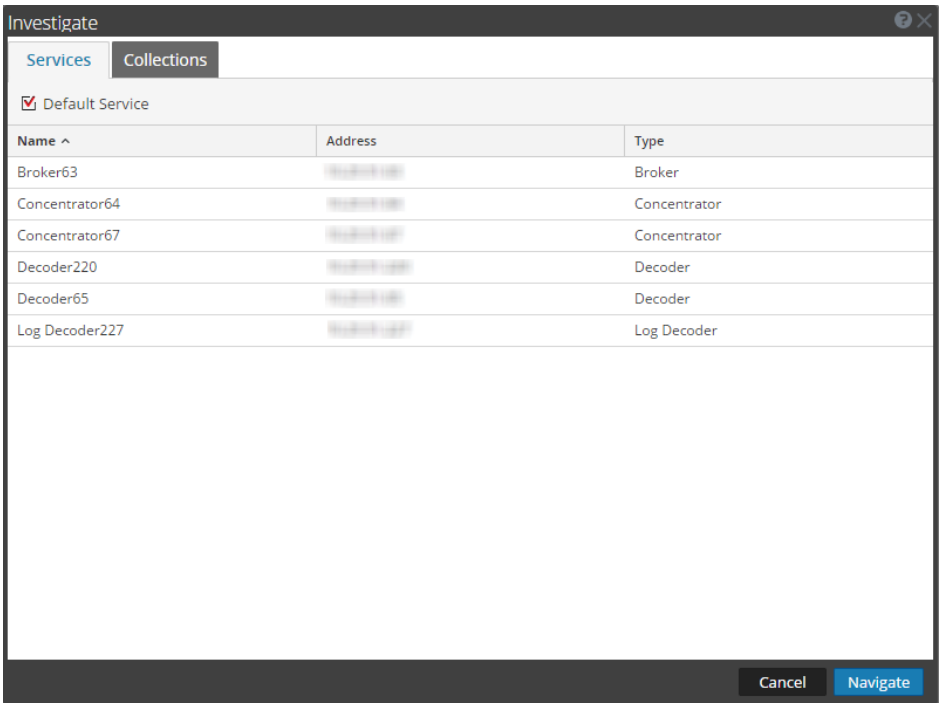
Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	seleccionar un servicio para investigar*	Comenzar una investigación en las vistas Navegar o Eventos

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Navegar
- Vista Eventos

Vista rápida



El cuadro de diálogo Investigar tiene dos pestañas: Servicios y Recopilaciones.

Nota: Las recopilaciones también se conocen como recopilaciones de Workbench. Solo puede ver recopilaciones de Workbench que ha creado y solo los administradores pueden crear una recopilación de Workbench.

La pestaña Servicios incluye una lista de servicios disponibles para investigación y tres botones. En la siguiente tabla se describen todas las funciones.

Función	Descripción
Servicio predeterminado	Si se hace clic en este botón, se establece o se borra el servicio predeterminado para investigar. Cuando un servicio se configura como el predeterminado, la palabra (Predeterminado) se añade al nombre del servicio.
Nombre	El nombre del servicio.
Dirección	La dirección IP del servicio.
Tipo	Tipo de servicio.
Cancelar	Cierra el cuadro de diálogo.
Navegar	Abre el servicio seleccionado en la vista Navegar o Eventos.

La pestaña Recopilaciones incluye dos botones y dos paneles: Workbench y Recopilaciones.

En el panel Workbench, los servicios Workbench disponibles se enumeran por nombre. Una vez que se selecciona un servicio Workbench, puede seleccionar una recopilación en el panel Recopilaciones.

En el panel Recopilaciones se muestran las recopilaciones disponibles para investigar. Una vez que se selecciona una recopilación, puede hacer clic en Navegar para verla.

En la siguiente tabla se describen las funciones del panel Recopilaciones.

Función	Descripción
Nombre	El nombre de la recopilación.
Tipo	El tipo de recopilación.
Tamaño	El tamaño de la recopilación.
Tipo de datos	El tipo de datos dentro de la recopilación.
Fecha de creación	La fecha en que se creó la recopilación.

Pestaña Investigación: Panel Preferencias de usuario

En la vista Perfil > panel Preferencias > pestaña Investigación, los usuarios pueden configurar varias preferencias que afectan el rendimiento y el comportamiento de NetWitness Platform cuando se analizan datos, se ven eventos y se reconstruyen eventos en NetWitness Investigate. Para acceder a esta pestaña, seleccione  > Profile. Cuando se muestre la vista Perfil, seleccione **Preferencias > Investigación**. Puede cambiar las preferencias de usuario en cualquier momento durante su trabajo en NetWitness Platform.

¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	ver y cambiar las preferencias de usuario para Investigate*	Configurar la vista Navegar y la vista Eventos

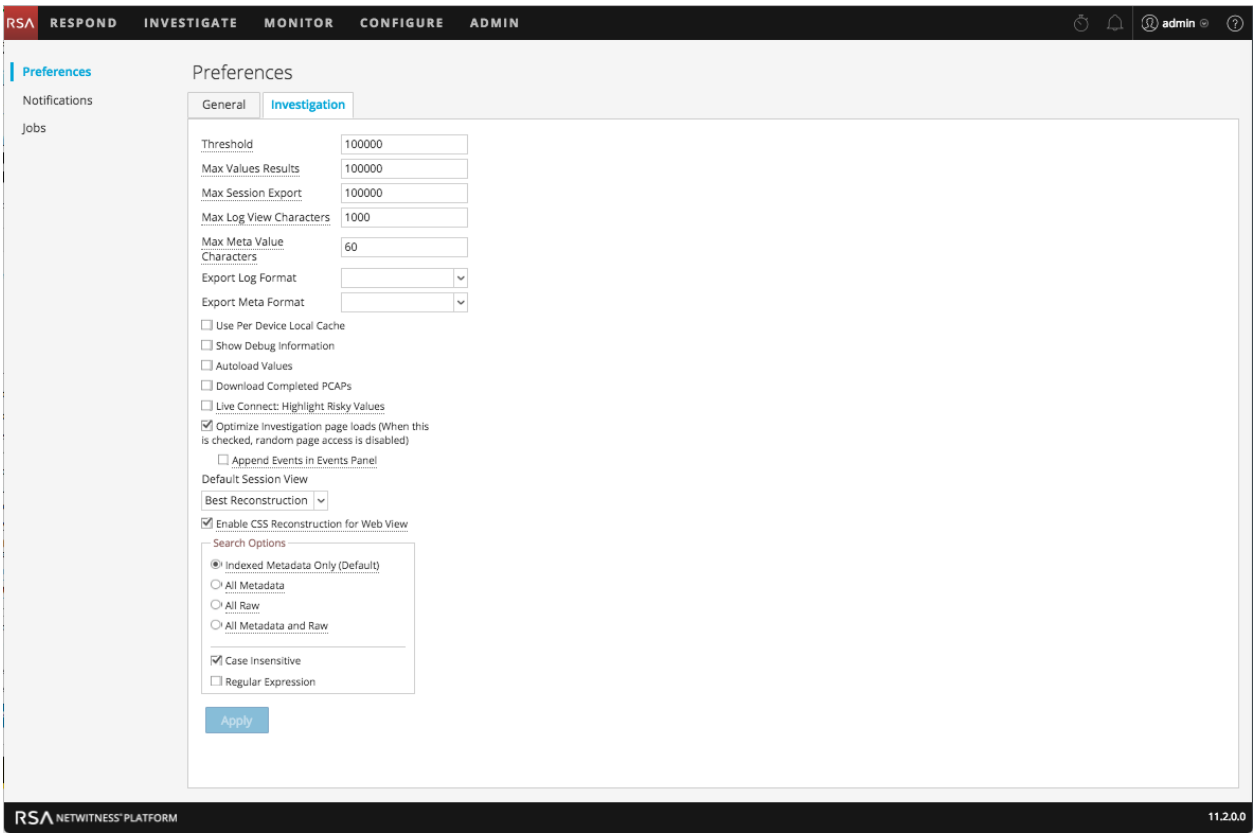
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Navegar
- Vista Eventos

Vista rápida

Esta figura es un ejemplo de la pestaña Investigación y en la siguiente tabla se describen las preferencias que afectan a Investigate. Hay ligeras diferencias entre las versiones 11.1 y 11.2 de la configuración de búsqueda y estas se explican en Buscar patrones de texto.



Función	Descripción
Umbral	Esta configuración controla el conteo que se muestra para un valor de clave de metadatos en la vista Navegar durante la carga. Un umbral mayor permite conteos más precisos para un valor. Sin embargo, un umbral mayor provoca que los tiempos de carga sean más extensos. Cuando se alcanza el umbral, NetWitness Platform muestra el conteo y el porcentaje de tiempo usado para alcanzar el conteo en comparación con el tiempo necesario para cargar todas las sesiones con ese valor. Por ejemplo, **(> 100,000 - 18 %)** indica que el umbral se estableció en 100,000 y que esta carga tardó solamente el 18 % del tiempo que hubiese tardado sin un umbral definido. El valor predeterminado es **100000**.
Número máximo de resultados de valores	Esta configuración controla el número máximo de valores para cargar en la vista Navegar cuando la opción Resultados máximos está seleccionada en el menú Clave de metadatos para una Clave de metadatos abierta. El valor predeterminado es **1,000**.
Máximo de exportación de sesiones	Esta configuración controla la cantidad máxima de sesiones que se pueden exportar. El valor predeterminado es **100000**.
Caracteres de vista de registro máximos	Este ajuste controla la cantidad máxima de caracteres que se mostrarán en **Investigation > Eventos > Texto del registro**. El valor predeterminado es **1,000**.

Función	Descripción
Formato de registro de exportación	Este ajuste especifica el formato predeterminado para exportar registros desde Investigation. Las opciones disponibles son **Texto**, **XML**, **CSV** y **JSON**. No hay valor predeterminado incorporado para el formato de exportación de registro. Si no selecciona un formato aquí, NetWitness Platform muestra un cuadro de diálogo de selección cuando invoca la exportación de registros. Cuando selecciona una de las opciones del menú desplegable Formato de registro de exportación y hace clic en Aplicar, el ajuste se aplica de inmediato.
Formato de metadatos de exportación	Este ajuste especifica el formato predeterminado para exportar valores de metadatos desde Investigation. Las opciones disponibles son Texto, XML, CSV y JSON. No hay ningún valor predeterminado incorporado para el formato de exportación de metadatos. Si no selecciona un formato aquí, NetWitness Platform muestra un cuadro de diálogo de selección cuando usted invoca la exportación de metadatos. Cuando selecciona una de las opciones del menú desplegable Formato de metadatos de exportación y hace clic en Aplicar, la configuración surte efecto de inmediato.
Uso por caché local de dispositivo	
Mostrar información de depuración	Cuando se selecciona esta opción, NetWitness Platform muestra la cláusula `where` debajo de la ruta de navegación en la vista Navegar. Para cada carga de valor de metadatos se muestra el tiempo de carga. Si el servicio es un Broker, se informa el tiempo transcurrido para cada servicio agregado. El valor predeterminado es **Desactivado**.
Agregar eventos en el panel de eventos	Cuando se selecciona esta opción, los eventos que se muestran en el **Panel de eventos** se agregan de manera incremental, en lugar de sobrescribir los eventos visualizados actualmente. Cada vez que hace clic en el ícono de la página siguiente, se agregan eventos adicionales a los eventos anteriores; 1-25, después 1-50, después 1-75, etc. **Nota:** Esta opción está disponible solo si la opción Optimizar cargas de la página Investigation está habilitada.
Cargar valores automáticamente	Cuando se selecciona esta opción, los valores del servicio se cargan automáticamente en la vista Navegar. Cuando no está seleccionada, NetWitness Platform muestra un botón **Cargar valores** que da al usuario la oportunidad de modificar las opciones. El valor predeterminado es **Desactivado**.
Descargar PCAP finalizadas	Este ajuste automatiza la descarga de PCAP extraídas del módulo Investigate de modo que no sea necesario descargar ni abrir manualmente estos archivos en una aplicación que pueda manejar la visualización de datos en formato PCAP, como Wireshark.
Live Connect: Resaltar los valores riesgosos	

Función	Descripción
Optimizar las cargas de páginas de Investigation	Esta opción está habilitada de forma predeterminada (marcada) y controla la forma en que la vista Eventos recupera eventos. Una vez optimizados, los resultados se devuelven lo más rápidamente posible. Esto dificulta la capacidad original de ir a una página específica en la lista de eventos. La deselección de esta casilla cambia la paginación en la lista de eventos y permite ir a una página específica de la lista (o a la última página). La capacidad de ir a cualquier página de la lista hace que se pierda velocidad en la entrega de resultados debido a la sobrecarga adicional para determinar los eventos por adelantado.
Vista de sesión predeterminada	Este ajuste selecciona el tipo de reconstrucción predeterminado para la vista de reconstrucción inicial. De manera predeterminada, los eventos se reconstruyen con el tipo de reconstrucción más apropiado para el evento.
Activar reconstrucción de CSS para vista web	Esta configuración controla la forma en que se ejecuta la reconstrucción del contenido web. Si está habilitada, la reconstrucción web incluye imágenes y estilos de hoja de estilo en cascada (CSS), de modo que su aspecto coincide con la vista original en un navegador web. Esto incluye el escaneo y la reconstrucción de eventos relacionados y la búsqueda de hojasde estilo e imágenes que se usan en el evento objetivo. Esta opción está habilitada de manera predeterminada. Deseleccione esta opción si hay problemas para ver sitios web específicos. **Nota:** Es posible que el aspecto del contenido reconstruido no coincida perfectamente con la página web original si no se pudo encontrar imágenes y hojas de estilo relacionadas o si estas se cargaron desde la caché del navegador web. Además, el diseño o el estilo que se ejecuta dinámicamente a través de JavaScript en el lado del cliente no se generarán en la reconstrucción debido a que todo el JavaScript del lado de cliente se elimina por motivos de seguridad.
Opciones de búsqueda	Esta configuración establece las opciones de búsqueda predeterminadas que se aplicarán a una búsqueda en las vistas Navegar y Eventos. En Buscar patrones de texto se proporciona información detallada.
Aplicar	Guarda las preferencias y las aplica de inmediato.

Vista Investigar

La vista Investigate (INVESTIGAR) es el punto de entrada principal a NetWitness Investigate. Esta vista tiene seis submenús, los cuales abren diferentes vistas que permiten analizar los eventos desde distintas perspectivas. Los submenús son los siguientes: Navegar, Eventos, Análisis de eventos, Hosts, Archivos, Usuarios y Malware Analysis.

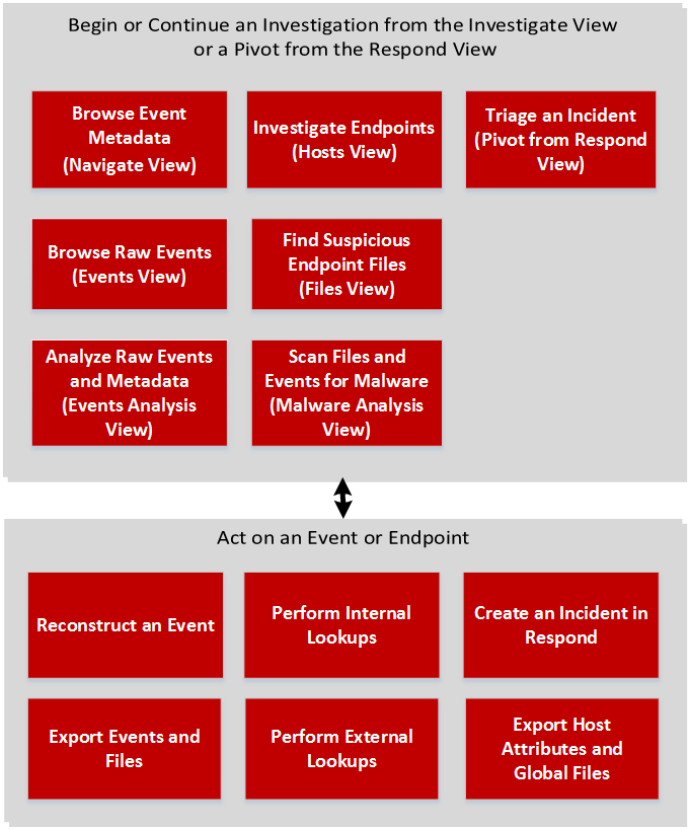
Nota: Los submenús Análisis de eventos, Hosts y Archivos están disponibles en la versión 11.1 y superior. El menú Usuarios está disponible en la versión 11.2 y superior. Los permisos configurados por función de usuario y usuario determinan los submenús que se muestran.

Puede usar las opciones de los submenús para desplazarse entre las distintas vistas.

- Las vistas Navegar, Eventos y Análisis de eventos ofrecen vínculos entre sí para ver los resultados actuales desde distintas perspectivas, lo cual proporciona cierta continuidad para la investigación a medida que va de una vista a otra.
- Las vistas Hosts y Archivos integran NetWitness Endpoint en Investigate y ofrecen una vista de todos los hosts en los que está instalado un agente de NetWitness Endpoint y una vista de archivos ejecutables únicos encontrados en el ambiente implementado.
- La vista Usuarios proporciona visibilidad de comportamientos riesgosos de los usuarios en toda la empresa mediante NetWitness UEBA. Puede ver una lista de usuarios de alto riesgo y un resumen de las alertas principales para el comportamiento riesgoso en el ambiente y, a continuación, seleccionar un usuario o una alerta y ver detalles sobre el comportamiento riesgoso y la cronología en que este se produjo.
- La vista Malware Analysis permite escanear los archivos que se encontraron en una de las demás vistas o que se recopilaron mediante el escaneo continuo del tráfico de red.

Flujo de trabajo

El siguiente flujo de trabajo describe las tareas generales para la investigación de eventos.



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos*	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos*	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)*	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos*	Realización de un análisis de malware

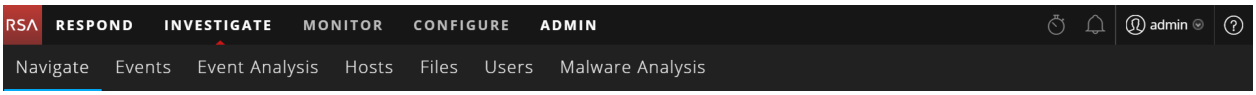
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Inicio de una investigación
- Configuración de vistas y preferencias de NetWitness Investigate
- Vista Navegar
- Vista Eventos
- Vista Análisis de eventos
- Vista Hosts
- Vista Archivos
- Vista Malware Analysis
- *Guía del usuario de NetWitness UEBA*

Vista rápida

La vista Investigar consta de seis vistas y cada una de ellas representa un enfoque diferente para analizar los datos. De forma predeterminada, Investigate se abre en la vista Navegar. Puede cambiar la vista predeterminada a una de las demás vistas. Consulte Cómo funciona NetWitness Investigate para obtener una introducción acerca de los usos de cada vista. En la siguiente figura se ilustran los submenús de INVESTIGAR.



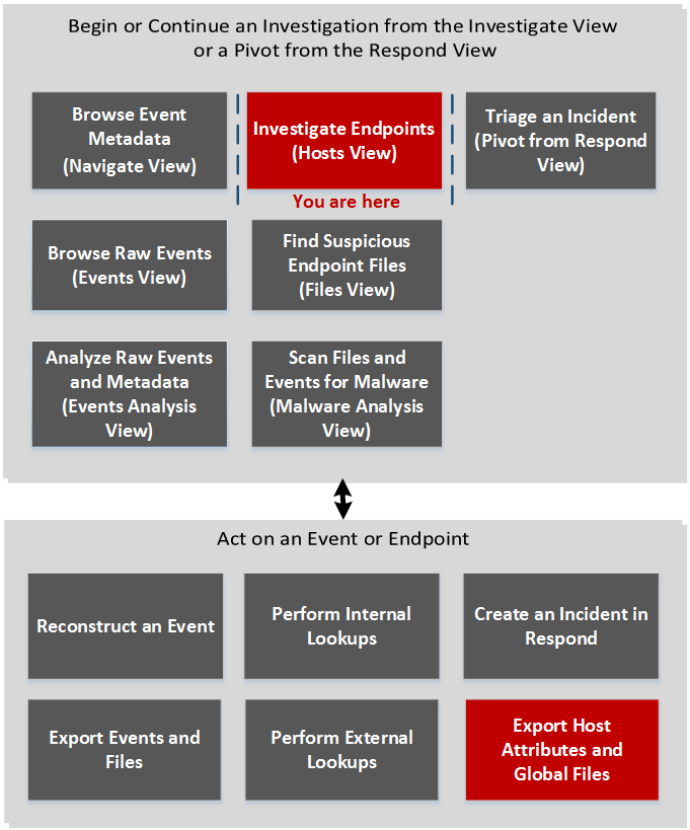
Vista Hosts

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

En NetWitness Investigate, la vista Hosts proporciona una lista de todos los hosts en los que está instalado un agente de Endpoint. La tabla muestra un conjunto de columnas predeterminadas para el host. Puede personalizar esta vista mediante la configuración de las preferencias de los hosts. Para acceder a esta vista, vaya a **INVESTIGAR > Hosts**.

Flujo de trabajo

En la siguiente figura se muestra el flujo de trabajo general de Investigate y se destacan las tareas de investigación de terminales.



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	exportar atributos de hosts y archivos globales*	Investigar los hosts

*Puede realizar esta tarea en la vista actual.

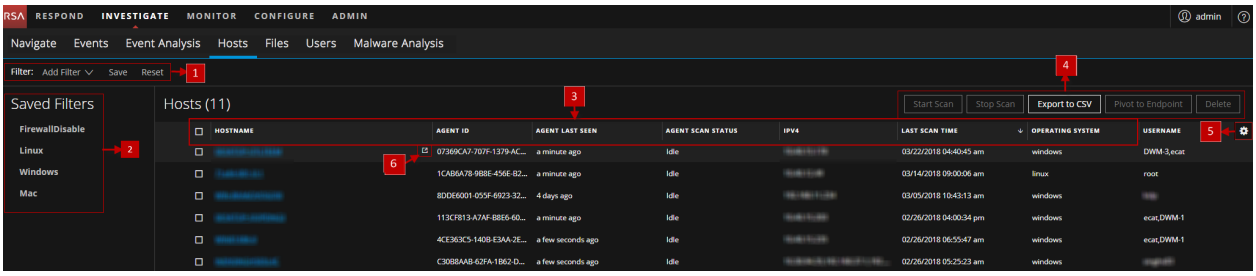
Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts: Pestaña Descripción general
- Vista Hosts: Pestaña Proceso
- Vista Hosts: Pestaña Ejecuciones automáticas
- Vista Hosts: Pestaña Archivos
- Vista Hosts: Pestaña Controladores
- Vista Hosts: Pestaña Bibliotecas
- Vista Hosts: Pestaña Información del sistema

Vista rápida

En la vista Hosts, puede exportar atributos de hosts y archivos globales, realizar un escaneo según demanda, configurar preferencias de los hosts, ver una lista de hosts e investigar en las vistas Navegar o Eventos.

Este es un ejemplo de la vista Hosts:



1 **Menú desplegable Agregar filtro**. Puede filtrar los hosts mediante la selección de un sistema operativo (Windows, Linux o Mac) o filtros guardados, o la selección de las opciones del menú desplegable Agregar filtro. Para obtener más información, consulte Filtrar los hosts.

2 **Filtros guardados.** El panel Filtros guardados enumera los filtros guardados. Para obtener más información, consulte Filtrar los hosts.

3 **Ordenar columnas**. Permite ordenar por columnas.

> **Nota:** El orden por columnas distingue mayúsculas de minúsculas. Ordena primero el número y después las mayúsculas y las minúsculas.
> El orden basado en los campos Estado de escaneo de agente y Agente visto por última vez no es el correcto.

4 **Acciones de la barra de herramientas:**
Iniciar escaneo: Inicia un escaneo de los hosts seleccionados.
Detener exploración: Detiene un escaneo de los hosts seleccionados.
Exportar a CSV: Extrae atributos de hosts a un archivo CSV. Para obtener más información, consulte Exportar los atributos de los hosts.
Cambiar a Endpoint: Permite investigar el host de NetWitness Endpoint (versión 4.4.0.2 o superior). Para obtener más información, consulte Investigar los hosts de NetWitness Endpoint 4.4.0.2 o superior.
Eliminar: Permite eliminar los hosts manualmente desde la interfaz del usuario. Después de la eliminación, el servidor de Endpoint no procesa ninguna solicitud desde este host.

> **Nota:** Asegúrese de que el agente se desinstale del host antes de eliminarlo de la interfaz del usuario. Para obtener más información, consulte Eliminar un host.

5 **Menú Ajustes de configuración.** Puede configurar las preferencias de la vista Hosts mediante la selección de columnas en el menú Ajustes de configuración. Para obtener más información, consulte Configurar las preferencias de los hosts.

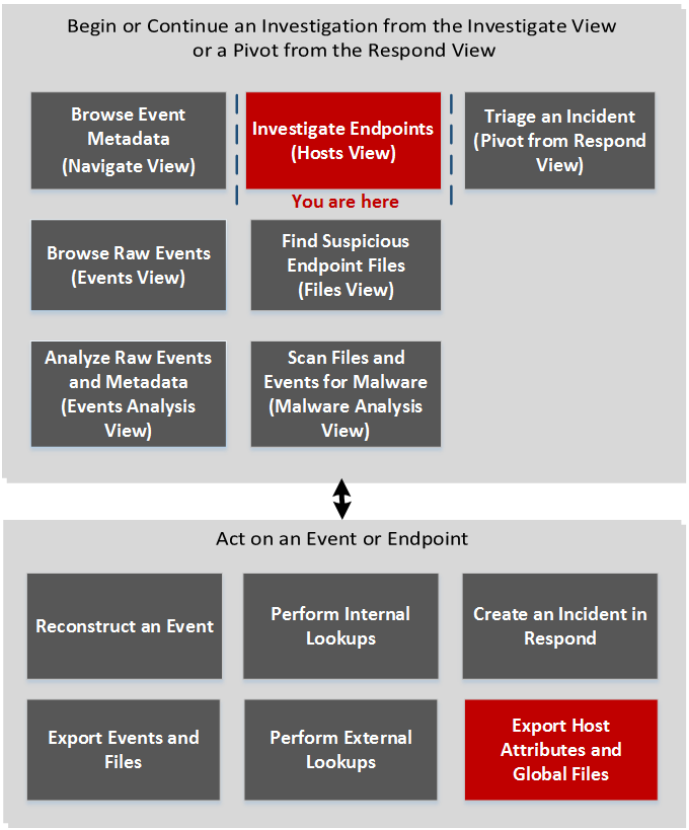
6 **Cambiar a las vistas Navegar y Análisis de eventos**. Para investigar un host, una dirección IP o un nombre de usuario específicos, puede ir a las vistas Navegar y Análisis de eventos. Para obtener más información, consulte Cambiar a las vistas Navegar y Análisis de eventos.

Vista Hosts: Pestaña Ejecuciones automáticas

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

El panel Ejecuciones automáticas proporciona una lista de ejecuciones automáticas, servicios, tareas y trabajos cron que se ejecutan en el host. Para acceder a esta pestaña, seleccione un host en la vista **Hosts** y haga clic en la pestaña **Ejecuciones automáticas**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver las ejecuciones automáticas, los servicios, las tareas y los trabajos cron que están en ejecución en el host*	Analizar las ejecuciones automáticas

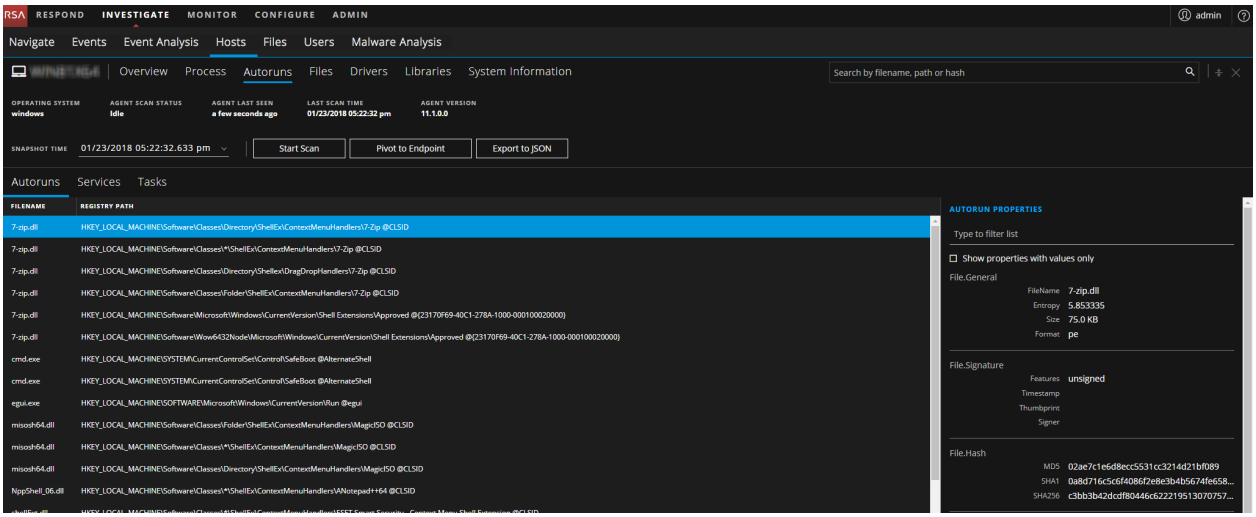
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Ejecuciones automáticas:



Categoría	Descripción
Ejecuciones automáticas	Archivos que se ejecutan en el arranque. Muestra las siguientes columnas: • Nombre del archivo: `cmd.exe` • Ruta del registro: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot @AlternateShell`
Servicios	Archivos que se ejecutan como servicio para el host seleccionado. Muestra las siguientes columnas: • Nombre del servicio: `acsock` • Estado de ejecución: `stopped` • Hora de creación del archivo: `07/11/2017 11:47:00 am` • Firma: `Microsoft, signed, valid` • Ruta del archivo: `C:\Windows\System32\drivers`
Tareas/trabajos cron	Archivos que están configurados para ejecutarse como tareas programadas junto con el desencadenante. Muestra las siguientes columnas: • Nombre: `shell32.dll` • Hash: `cafa6e7b6a9220e7c805ea476a89a78800f48bb48c66fe5f935057940df3909c` • Hora de última ejecución: `01/19/2018 05:34:50 pm` • Próxima hora de ejecución: `12/30/1899 05:30:00 am` • Desencadenante: `No Trigger`

Panel Propiedades de ejecución automática

Este panel muestra todas las propiedades del archivo seleccionado. Se agrupa de la siguiente manera:

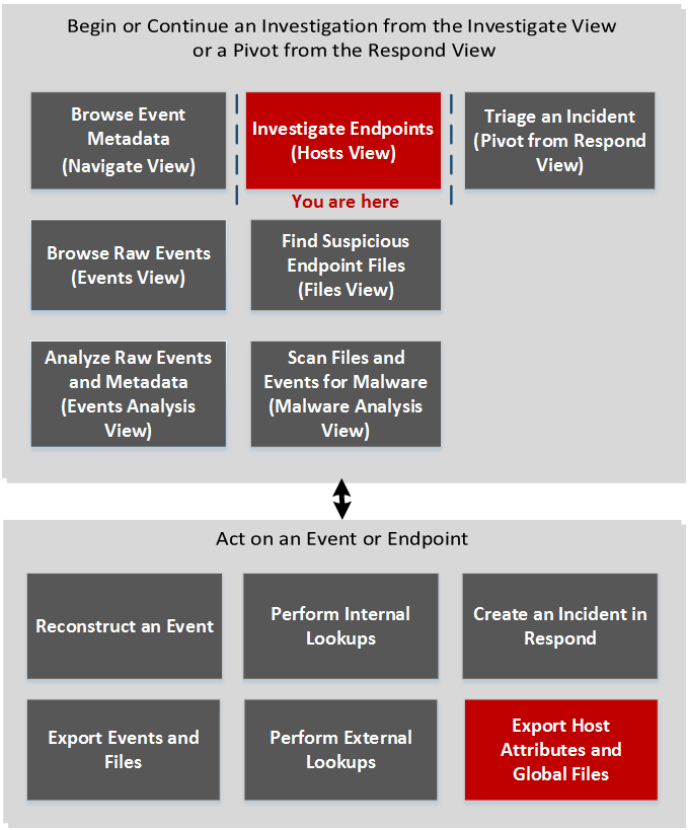
Categoría	Descripción
Firma	Proporciona información acerca del signatario.
Hash	Tipo de hash del archivo (MD5, SHA256 y SHA1).
Tiempo	Hora en que se creó o se modificó el archivo, o en que se accedió a él.
Ubicación	Ubicación del archivo.
Imagen	Cargar imagen.

Vista Hosts: Pestaña Controladores

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

La pestaña Controladores enumera los controladores que se ejecutan en los hosts en el momento del escaneo. Para acceder a esta pestaña, seleccione un host en la vista **Hosts** y haga clic en la pestaña **Controladores**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver los controladores que se ejecutan en el host*	Investigar los hosts

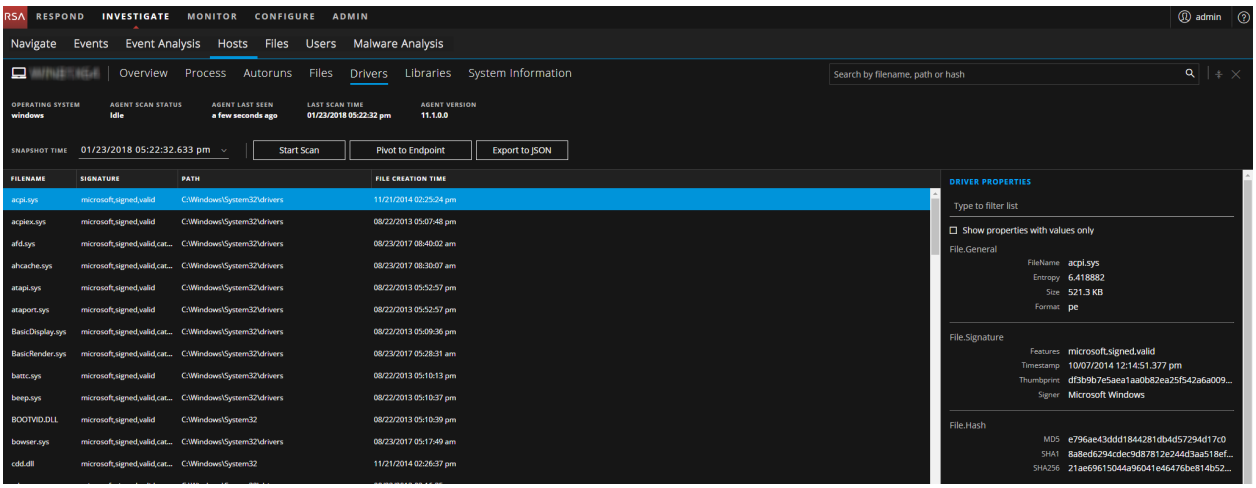
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Controladores:



Campo	Descripción
Nombre del archivo	Nombre del archivo. Por ejemplo, `acpi.sys`.
Firma	Indica si el archivo está o no firmado y si es o no válido, y proporciona información acerca del signatario.
Ruta	Ruta del archivo. Por ejemplo, `C:\Windows\System32\drivers`.
Hora de creación del archivo	Hora en que se creó el archivo.

Panel Propiedades de controlador

Este panel muestra todas las propiedades del archivo seleccionado. Se agrupa de la siguiente manera:

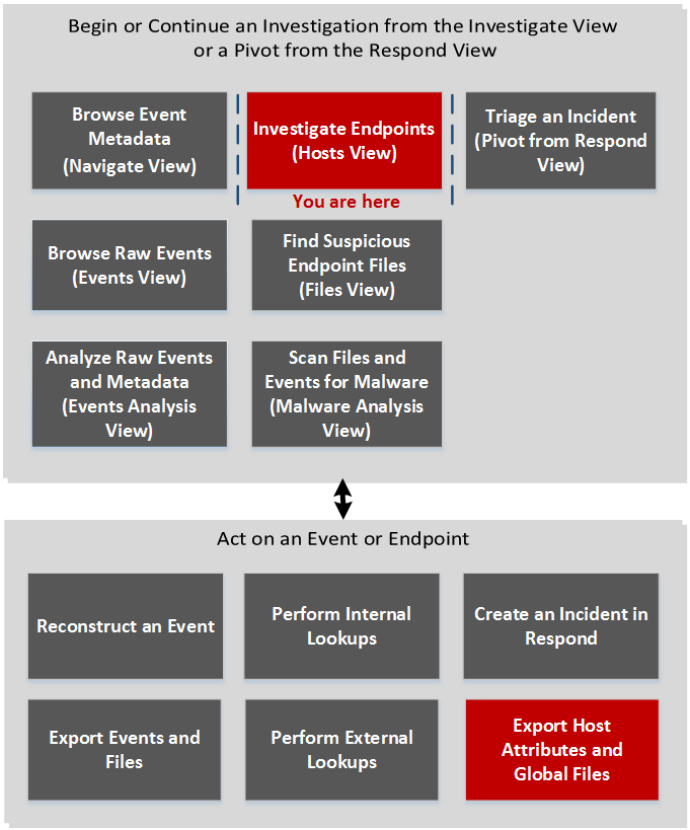
Categoría	Descripción
General	Información general acerca del archivo, como nombre de archivo, entropía, tamaño y formato.
Firma	Proporciona información acerca del signatario.
Hash	Tipo de hash del archivo (MD5, SHA256 y SHA1).
Tiempo	Hora en que se creó o se modificó el archivo, o en que se accedió a él.
Ubicación	Ubicación del archivo.
Imagen	Imagen cargada.

Vista Hosts: Pestaña Archivos

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

La pestaña Archivos muestra todos los archivos escaneados en el host. Para acceder a esta pestaña, seleccione un host en la vista **Hosts** y haga clic en la pestaña **Archivos**. De forma predeterminada, se muestran 100 archivos. Para mostrar más archivos, haga clic en **Cargar más** en la parte inferior de la página.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver los archivos escaneados en el host*	Analizar los archivos

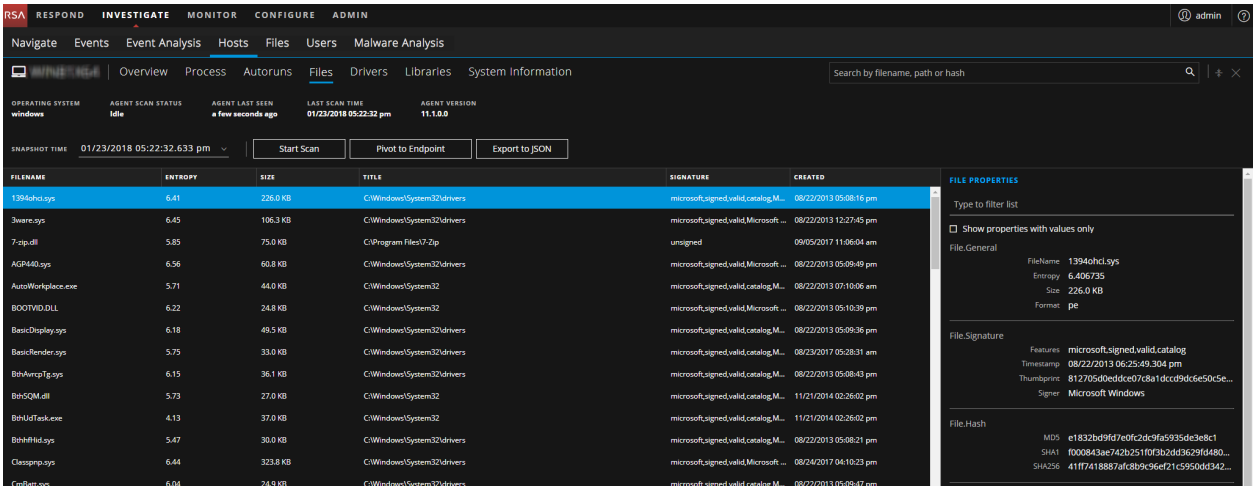
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Archivos:



Campo	Descripción
Nombre del archivo	Nombre del archivo. Por ejemplo, `7-zip.dll`.
Entropía	Entropía de los datos de la imagen, sin incluir los encabezados PE. Determina si el contenido está empaquetado (comprimido o cifrado).
Tamaño	Tamaño del archivo. Puede ser un indicador durante la evaluación de un archivo.
Ruta	Ruta del archivo. En ocasiones, los autores de malware colocan el archivo en directorios donde no suele haber este tipo de archivos. En general, los archivos maliciosos son archivos independientes (por ejemplo, un archivo en la raíz `C:\ProgramData`) en comparación con un grupo de archivos en una carpeta legítima (por ejemplo, los archivos en `C:\Program Files\<folder name>\`).
Firma	Indica si el archivo está o no firmado y si es o no válido, y proporciona información acerca del signatario.
Creado	Registro de fecha y hora del archivo.
Nombre de usuario	Usuario del archivo (para Linux). Por ejemplo, `root`.
Nombre del grupo	Grupo al cual pertenece el usuario (para Linux). Por ejemplo, `root (0)`.

Panel Propiedades de archivo

Este panel muestra todas las propiedades del archivo seleccionado. Se agrupa de la siguiente manera:

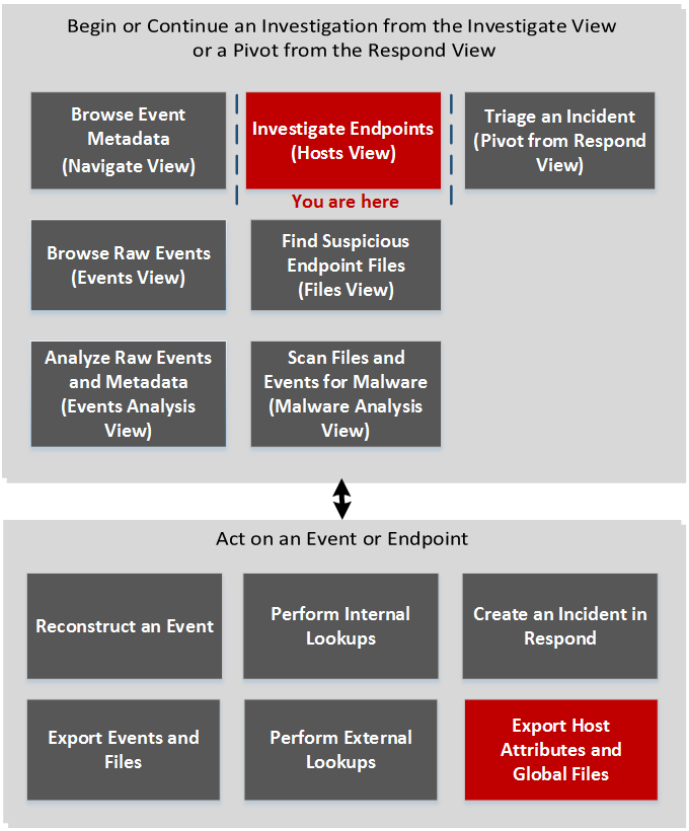
Categoría	Descripción
General	Información general acerca del archivo, como nombre de archivo, entropía, tamaño y formato.
Firma	Proporciona información acerca del signatario.
Hash	Tipo de hash del archivo (MD5, SHA256 y SHA1).
Tiempo	Hora en que se creó o se modificó el archivo, o en que se accedió a él.
Ubicación	Ubicación del archivo.

Vista Hosts: Pestaña Bibliotecas

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

La pestaña Bibliotecas enumera las bibliotecas que se cargan en el momento del escaneo. Para acceder a esta pestaña, seleccione un host en la vista **Hosts** y haga clic en la pestaña **Bibliotecas**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver las bibliotecas cargadas*	Analizar las bibliotecas

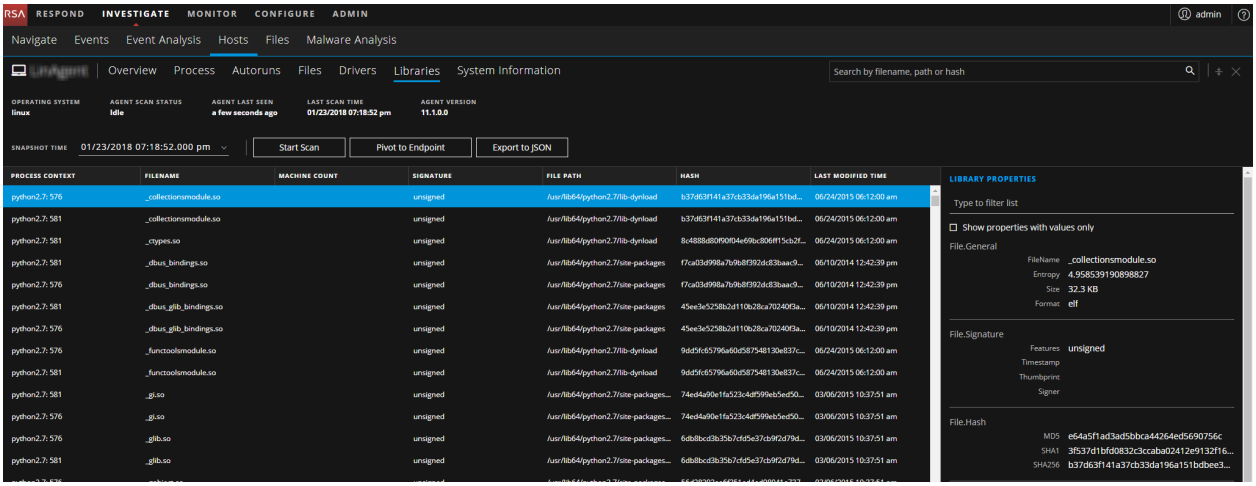
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Bibliotecas:



Campo	Descripción
Contexto del proceso	Nombre y PID del proceso que cargó la biblioteca en la memoria. Por ejemplo, `explorer.exe: 1916`.
Nombre del archivo	Nombre del archivo. Por ejemplo, `7-zip.dll`.
Firma	Indica si el archivo está o no firmado y si es o no válido, y proporciona información acerca del signatario. Por ejemplo, `signed, valid`.
Ruta del archivo	Ruta del archivo. Por ejemplo, `C:\Program Files\7-Zip`.
Hash	SHA256 del archivo. Por ejemplo, `c3bb3b42dcdf80446c622219513070757e618c06afd9ee0ac37cbce5befcb897`.
Hora de creación del archivo	Hora en que se creó el archivo.
Fecha de la última modificación	Hora en que se modificó el archivo.

Panel Propiedades de biblioteca

Este panel muestra todas las propiedades del archivo seleccionado. Se agrupa de la siguiente manera:

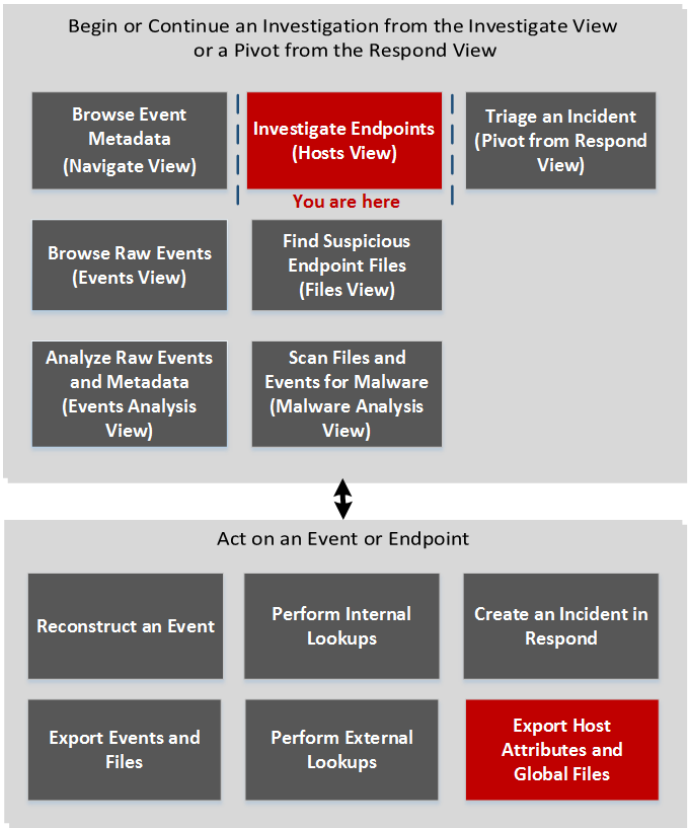
Categoría	Descripción
General	Información general acerca del archivo, como nombre de archivo, entropía, tamaño y formato.
Firma	Proporciona información acerca del signatario.
Hash	Tipo de hash del archivo (MD5, SHA256 y SHA1).
Tiempo	Hora en que se creó o se modificó el archivo, o en que se accedió a él.
Ubicación	Ubicación del archivo.
Proceso	Detalles del proceso, como el tamaño de la imagen y el PID.

Vista Hosts: Pestaña Descripción general

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

La pestaña Descripción general proporciona resultados detallados del escaneo del host seleccionado. De forma predeterminada, se muestra el resultado del escaneo más reciente. Para acceder a esta vista, vaya a **INVESTIGAR > Hosts** y seleccione un host en la vista **Hosts**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver un resumen del host*	Investigar los hosts

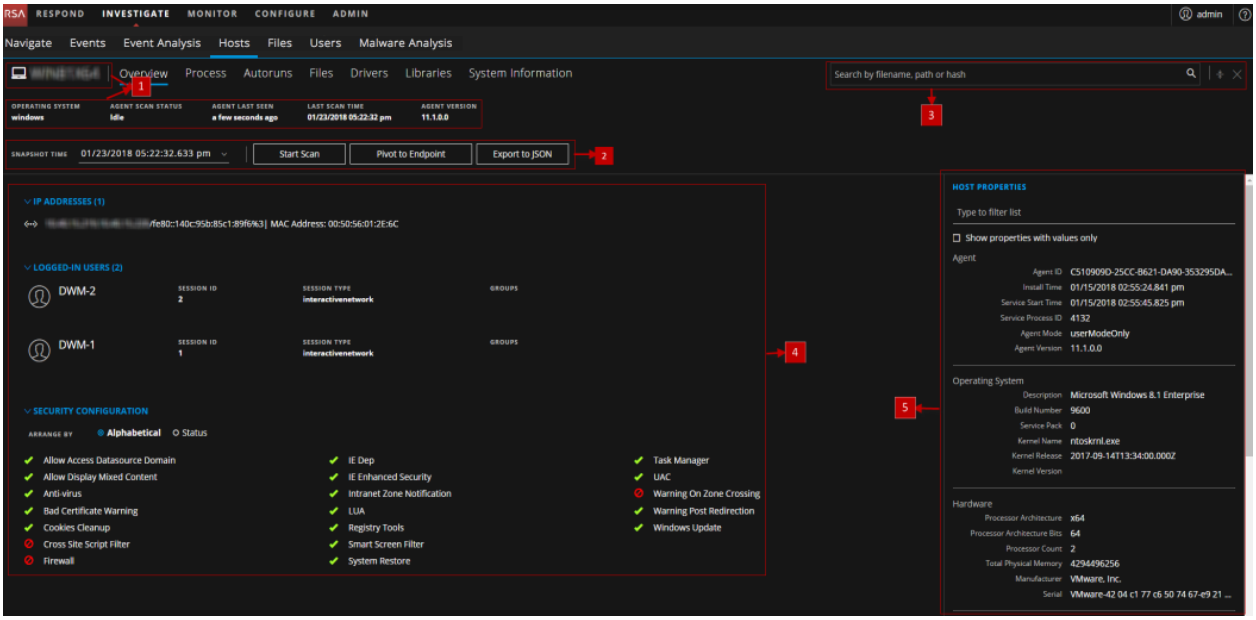
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Descripción general:



1	**Detalles de agentes y escaneos**. Puede ver los siguientes detalles de agentes y escaneos del host seleccionado: **Nombre del host**: Nombre del host. Por ejemplo, `WIN-ABC`. **Sistema operativo**: Sistema operativo en el que se ejecuta el agente (Linux, Windows o Mac). **Estado de escaneo de agente**: Estado actual del escaneo: Inactivo, Escaneando, Iniciando escaneo o Deteniendo escaneo. Para obtener más información, consulte Investigar los hosts. **Agente visto por última vez**: La hora en que el agente se comunicó por última vez con el servidor. **Hora de último escaneo**: Última vez que se escaneó el agente. La fecha y la hora corresponden a la zona horaria configurada en las Preferencias de usuario y son las locales del servidor. **Versión de agente**: Versión del agente. Por ejemplo, `11.1.0.0`.
2	**Acciones de la barra de herramientas:** **Hora de instantánea**: Enumera los registros de fecha y hora escaneados. Para ver el historial de escaneos, seleccione la hora de la instantánea en el menú desplegable. **Iniciar escaneo**: Inicia un escaneo de los hosts seleccionados. Para obtener más información, consulte Investigar los hosts. **Exportar a CSV**: Extrae atributos de hosts a un archivo CSV. Para obtener más información, consulte Exportar los atributos de los hosts. **Cambiar a Endpoint**: Permite investigar el host de NetWitness Endpoint (versión 4.4.0.2 o superior). Para obtener más información, consulte Investigar los hosts de NetWitness Endpoint 4.4.0.2 o superior. **Exportar a JSON**: Extrae atributos de hosts y datos de terminales a un archivo JSON de la instantánea seleccionada.
3	**Buscar en las instantáneas**. Permite buscar en todas las instantáneas (nombre de archivo, ruta de archivo y suma de comprobación SHA-256). Para obtener más información, consulte Buscar en las instantáneas.
4	**Resumen del host seleccionado**. Muestra los siguientes campos: **Direcciones IP**: Las direcciones IP asociadas al host. Por ejemplo, `10.10.10.3`. **Usuarios que iniciaron sesión**: Los usuarios que iniciaron sesión en el host. Por ejemplo, `abc`. **Configuración de seguridad**: Detalles de la configuración de seguridad del host. Por ejemplo, firewall deshabilitado o activado y filtro de pantalla inteligente deshabilitado o activado. Este campo solo se aplica a Windows y Mac. **Nota:** Los campos Versión de agente, Direcciones IP, Usuarios que iniciaron sesión y Configuración de seguridad pueden cambiar para cada escaneo.

5 **Panel Propiedades del host**. Muestra todas las propiedades del host seleccionado. Se agrupa de la siguiente manera:

Agente: Información relacionada con el agente, como ID del agente, código de error del controlador, hora de instalación y modo del agente.

Sistema operativo: Versión del sistema operativo e información sobre la compilación.

Hardware: Información relacionada con la arquitectura.

Interfaces de red: Información sobre el adaptador de red, como la dirección Mac y la puerta de enlace.

Usuario: Información relacionada con el usuario.

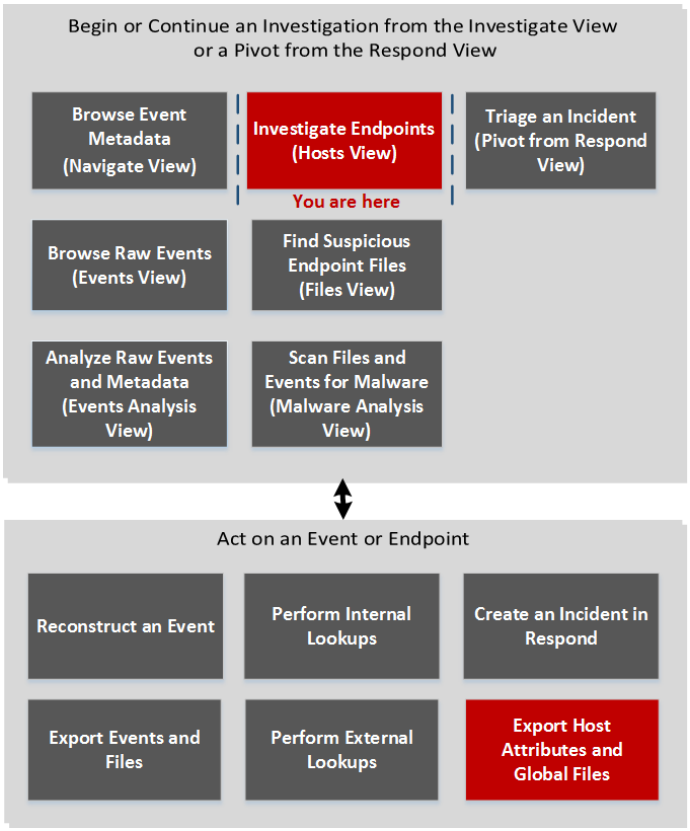
Configuración regional: Zona horaria e idioma locales del host.

Vista Hosts: Pestaña Proceso

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

El panel de proceso proporciona una lista de procesos que se ejecutan en el host. Para acceder a esta pestaña, seleccione un host en la vista **Hosts** y haga clic en la pestaña **Proceso**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver los procesos en ejecución en el host*	Investigar los hosts

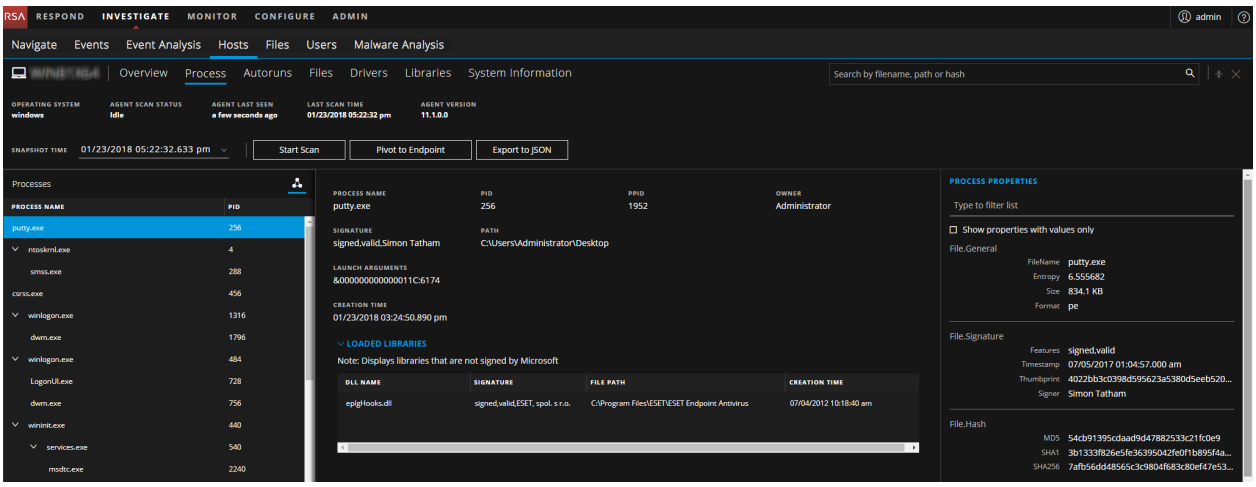
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Proceso:



El panel Proceso muestra la siguiente información bajo Detalles del proceso:

Campo	Descripción
Nombre de proceso	Nombre del proceso. Por ejemplo, `server.exe`.
PID	ID del proceso. Por ejemplo, `492`.
Proceso primario (PPID)	Nombre e ID de proceso del elemento primario. Por ejemplo, `4`.
Propietario	Propietario del proceso. Por ejemplo, `SYSTEM`.
Firma	Indica si el archivo está o no firmado y si es o no válido, y proporciona información acerca del signatario.
Ruta	Ruta del archivo asociado al proceso en el disco. Por ejemplo, `C:\Windows\System32`.
Argumentos de lanzamiento	Argumentos de la línea de comandos transmitidos al proceso cuando se inicia. Por ejemplo, `-k LocalServiceNoNetwork`.
Hora de creación	Hora en que se creó el proceso. Por ejemplo, `01/19/2018 11:32:29.908 am`.

- Lista de bibliotecas cargadas para el proceso seleccionado, como archivos DLL (para Windows), Dylibs (para Mac) o .SO (para Linux).
- Lista de ejecuciones automáticas (si están configuradas).

Panel Propiedades de proceso

Este panel muestra todas las propiedades del proceso seleccionado. Se agrupa de la siguiente manera:

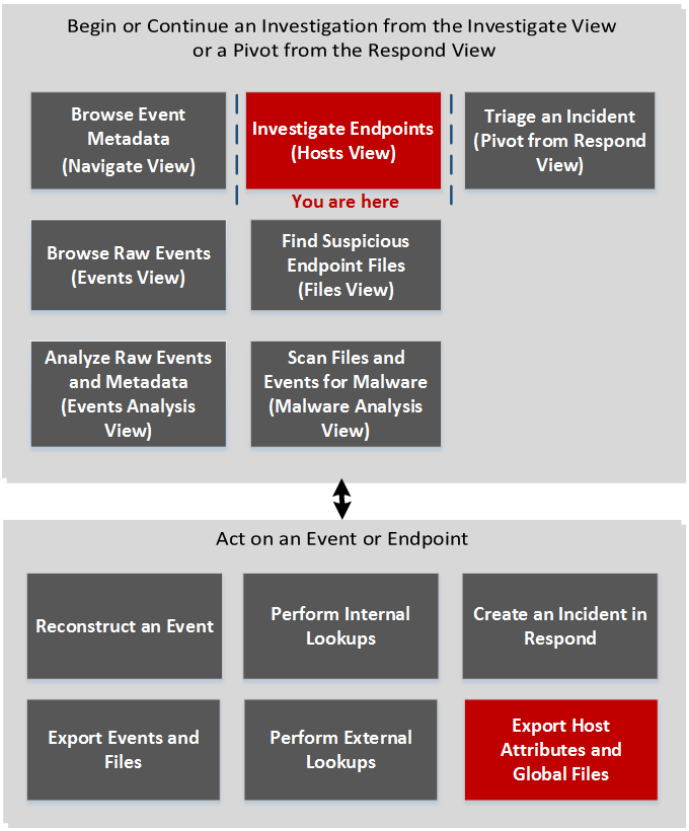
Categoría	Descripción
General	Información general acerca del archivo, como nombre de archivo, entropía, tamaño y formato.
Firma	Proporciona información acerca del signatario.
Hash	Tipo de hash del archivo (MD5, SHA1 y SHA256).
Tiempo	Hora en que se creó o se modificó el archivo, o en que se accedió a él.
Ubicación	Ubicación del archivo.
Proceso	Detalles del proceso, como el tamaño de la imagen y el PID.
Imagen	Detalles de la imagen que carga el proceso.

Vista Hosts: Pestaña Información del sistema

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.1 y superior.

La pestaña Información del sistema enumera la información del sistema del agente. Para acceder a esta pestaña, seleccione un host en la vista **Hosts** y haga clic en la pestaña **Información del sistema**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)*	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	ver la información del sistema del agente*	Analizar la información del sistema

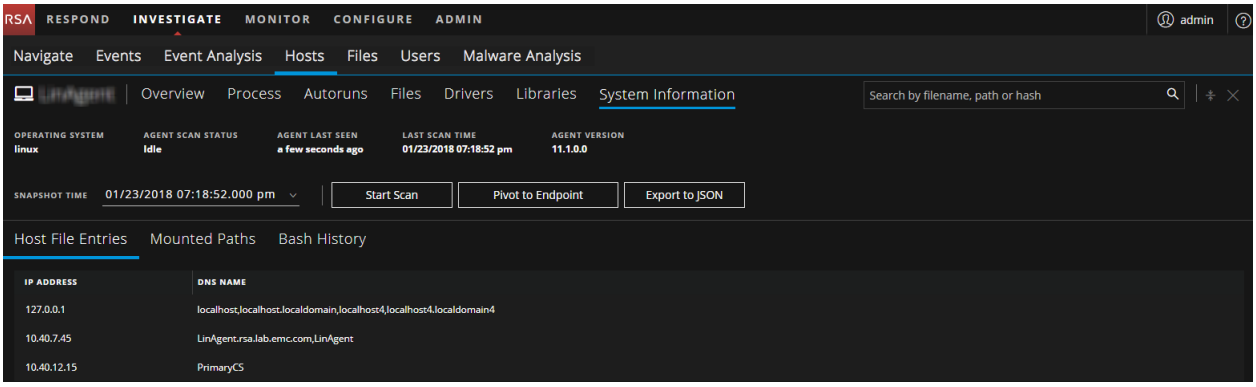
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Investigación de los hosts y los archivos
- Vista Hosts

Vista rápida

Este es un ejemplo de la pestaña Información del sistema:



Campo	Descripción
Entradas del archivo host	Todas las redirecciones de red, escritas en el archivo host. Por ejemplo, Dirección IP: `10.10.10.3` y Nombre de DNS: `localhost,localhost.localdomain,localhost4,localhost4.localdomain4`

Campo	Descripción
Recursos compartidos de red	Nombre de red del recurso compartido (solo para Windows). Por ejemplo, Nombre: `Admin$`, Descripción: `Remote Admin`, Ruta: `C:\`, Permisos: `None`, Tipo: `disk, special`, Máx. de usuarios: `4294967295` y Usuarios actuales: `0`.
Productos de seguridad	Productos de seguridad instalados (solo para Windows). Por ejemplo, Nombre para mostrar: `Windows Defender`, Instancia: `D68DDC3A-831F-4FAE-9E44-DA132C1ACF46`, Funciones: `Enabled` y Tipo: `antiVirus`.
Parches de Windows	Lista de parches que aplicó la actualización de Windows (solo para Windows). Por ejemplo, `KB2959936`.
Rutas montadas	Ruta en la que se realizó el montaje. Por ejemplo, Ruta: `/`, Sistema de archivos: `rootfs`, Ruta remota: `rootfs` y Opciones: `rw`.
Historial de Bash	Nombre de usuario y comando ejecutado. Por ejemplo, Nombre de usuario: `root` y Comando: `ls`.

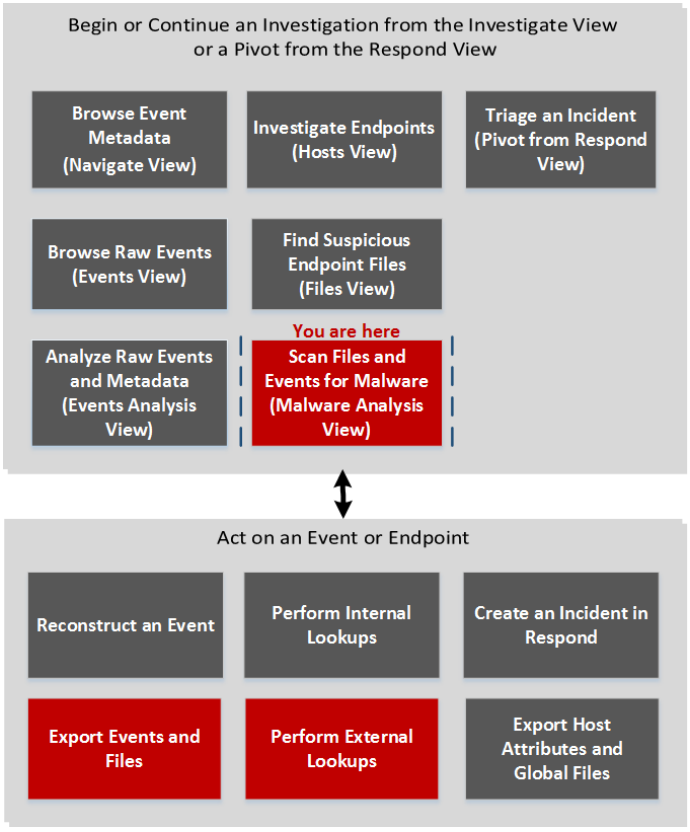
Nota: Para los hosts Mac, los campos Rutas montadas e Historial de Bash están vacíos.

Vista Malware Analysis

En NetWitness Investigate, la vista Malware Analysis proporciona la interfaz del usuario para realizar un análisis de malware. Esta vista tiene un formato de tablero personalizable, en el cual los dashlets predeterminados de la vista inicial se basan en la función del usuario (Administración o Analista) y en sus personalizaciones. Inicialmente, en la vista Malware Analysis se muestra el dashlet Resumen de eventos. Los dashlets adicionales presentan distintas visualizaciones de los eventos que se ven, y cada representación se puede configurar para refinar aún más la vista a medida que usted busca indicadores de riesgo. Los dashlets de Malware Analysis disponibles en el tablero de también están disponibles en la vista Malware.

Para acceder a esta vista, seleccione **INVESTIGAR > Malware Analysis**. Si no se seleccionó un servicio predeterminado, se muestra el cuadro de diálogo Seleccionar un servicio Malware Analysis. Seleccione un servicio y haga clic en **Ver modo continuo**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos*	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	exportar eventos y archivos*	Examinar archivos y eventos de escaneo en formato de lista
Buscador de amenazas	realizar búsquedas externas*	Ver detalles de Malware Analysis de un evento

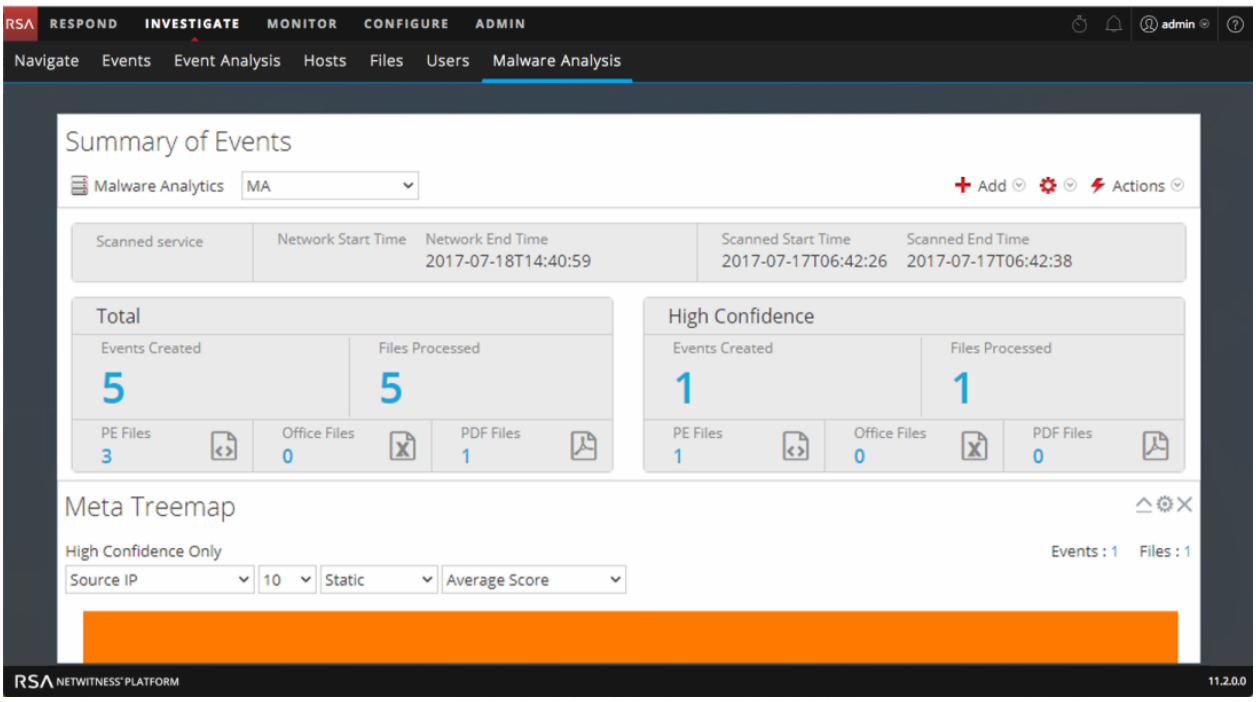
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Iniciar un escaneo de Malware Analysis desde la vista Navegar

Vista rápida

El siguiente es un ejemplo de la vista Malware Analysis.



La vista Malware Analysis consta del panel Resumen de eventos y de cuatro dashlets exclusivos. Cada uno de los dashlets únicos tiene cuadros de diálogo Opciones idénticos. Los dashlets de Malware Analysis en la vista MONITOREAR también están disponibles y se describen en el tema Dashlets del espacio Contenido de RSA para RSA NetWitness Platform.

Panel Resumen de eventos

El panel Resumen de eventos permite seleccionar el servicio, el modo de escaneo y el rango de tiempo. Además, puede seleccionar un punto de datos y ver los eventos asociados al evento.

En la siguiente tabla se describen todas las funciones del panel Resumen de eventos.

Función	Descripción
	Selecciona un servicio para mostrar.
Modo de escaneo	Muestra una lista desplegable de modos de escaneo disponibles.
Rango de tiempo	Muestra una lista desplegable de rangos de tiempo para ver eventos.
Fecha de inicio	Cuando Rango de tiempo se configura en personalizado, ofrece un calendario que permite elegir la fecha inicial del rango de tiempo.
Fecha de finalización	Cuando Rango de tiempo se configura en personalizado, ofrece un calendario que permite elegir la fecha final del rango de tiempo.
	Muestra una lista desplegable de dashlets que puede agregar a la vista.

Función	Descripción
	Muestra una lista desplegable de acciones que puede realizar en esta vista: • Restaurar configuración predeterminada • Ordenar dashlets • Aplicar filtro de umbral
	Actualiza la vista Malware Analysis.

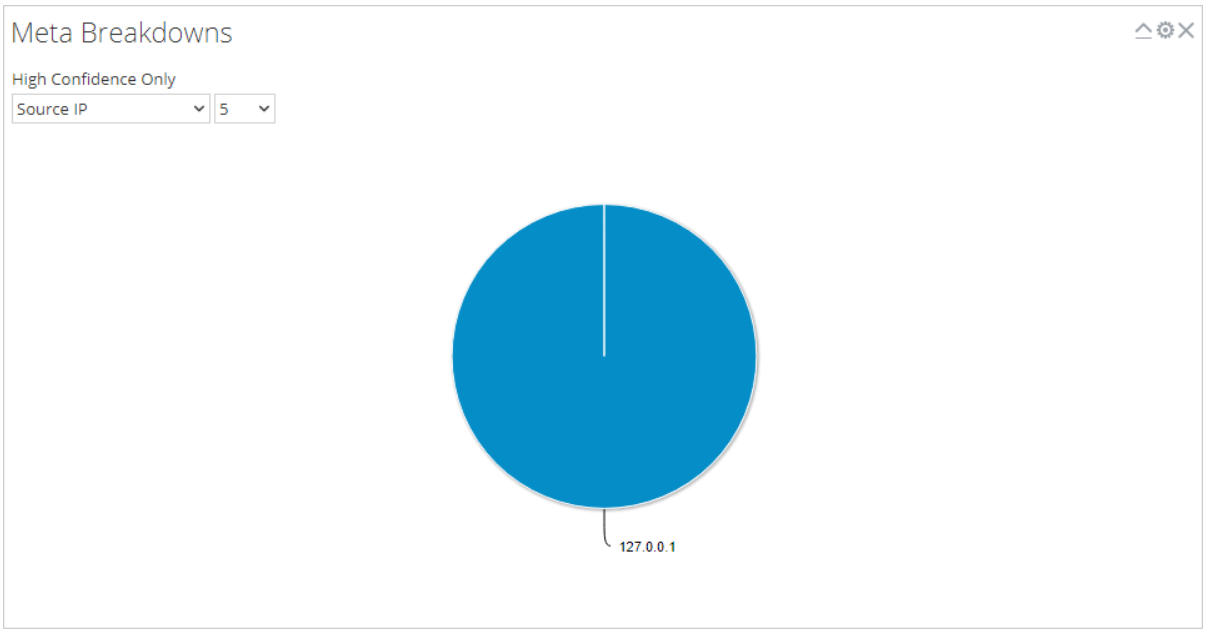
Cuadro de diálogo Opciones

El cuadro de diálogo Opciones permite personalizar los resultados que se muestran en el dashlet. Se puede acceder a él si se hace clic en el ícono  de la esquina superior derecha de cada dashlet. En la siguiente tabla se describen las funciones del cuadro de diálogo Opciones.

Función	Descripción
Título	Indica si los datos mostrados se restringen o no a eventos marcados como de alta confianza. Si los datos no están restringidos, esta línea no se muestra.
Solo con influencia de alta confianza	Indica si los datos mostrados se restringen a eventos marcados como de alta confianza.
Estático, Red, Comunidad y Sandbox	Permite filtrar los resultados en función de los puntajes de los módulos de puntaje.
Cancelar	Cierra el cuadro de diálogo sin guardar los cambios.
Aplicar	Aplica los cambios al dashlet de inmediato y cierra el cuadro de diálogo.

Desgloses de metadatos

Desgloses de metadatos presenta eventos en forma de un gráfico circular, en el cual cada segmento representa un valor de metadatos para la clave de metadatos especificada. Puede seleccionar la clave de metadatos y el conteo de valores de metadatos para esa clave que se generará en el gráfico, comenzando por el valor de metadatos que tiene más eventos. Si mantiene el mouse sobre un evento se muestra el conteo.

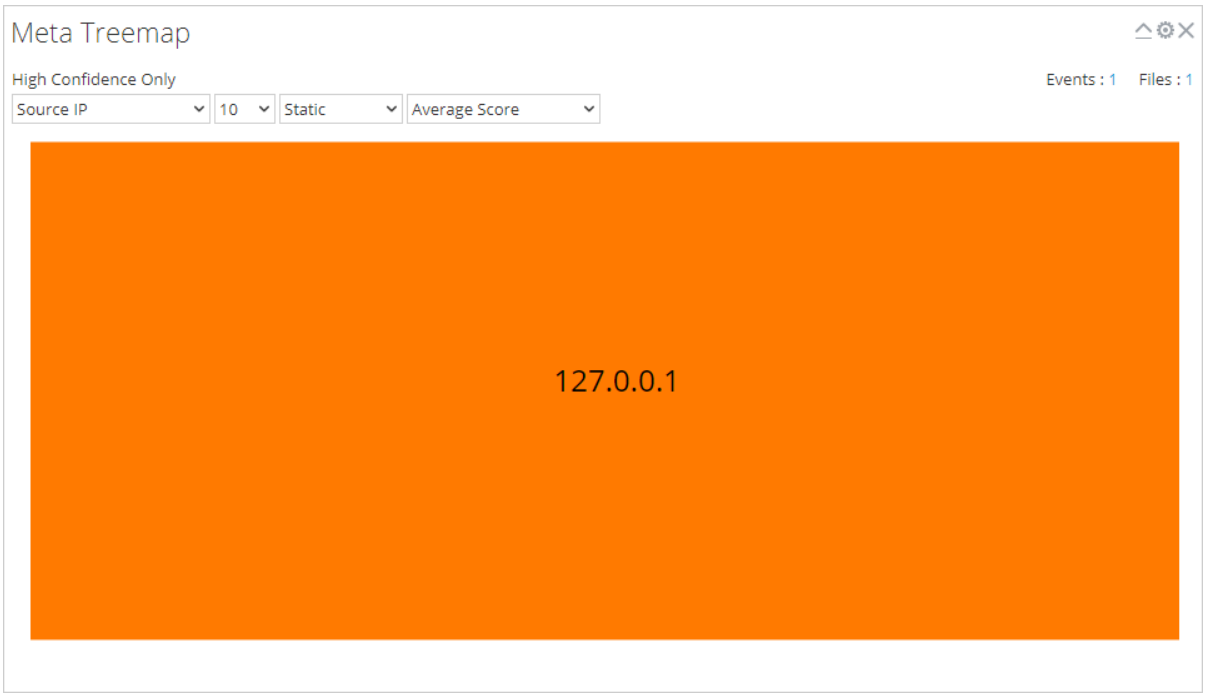


En la siguiente tabla se describen las opciones del dashlet Desgloses de metadatos.

Función	Descripción
Solo alta confianza	Indica si los datos mostrados se restringen o no a eventos marcados como de alta confianza. Si los datos no están restringidos, esta línea no se muestra.
Clave de metadatos	Lista desplegable de claves de metadatos disponibles.
Conteo	Lista desplegable que especifica cuántos de los resultados principales se muestran.

Mapa de árbol de metadatos

El Mapa de árbol de metadatos presenta eventos en forma de un mapa de riesgos. Puede seleccionar la clave de metadatos y el conteo de valores de metadatos para esa clave que se generará en el gráfico, comenzando por los valores de metadatos que tienen más eventos. Además, puede seleccionar el módulo que detectó el valor de metadatos en los eventos: estático, red, Community o Sandbox.

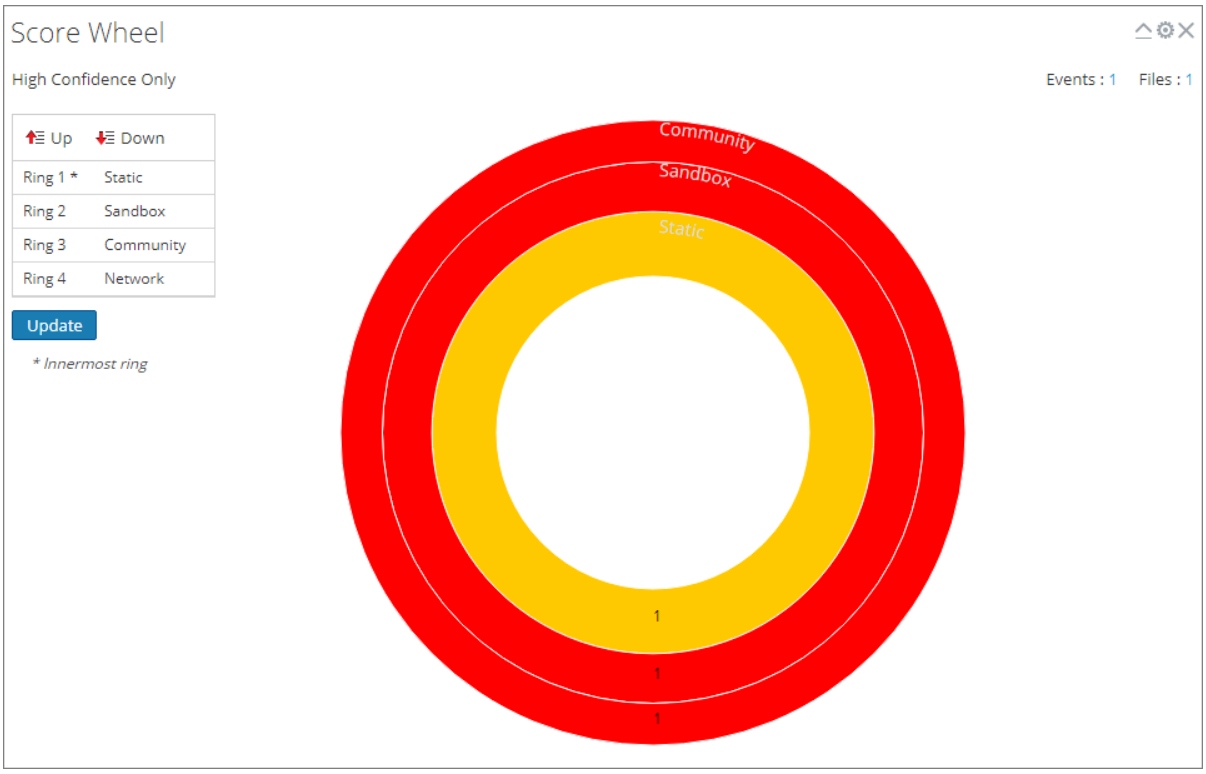


En la siguiente tabla se describen las opciones del dashlet Mapa de árbol de metadatos.

Función	Descripción
Solo alta confianza	Indica si los resultados se restringen o no a eventos marcados como de alta confianza. Si los resultados no están restringidos, esta línea no se muestra.
Clave de metadatos	Lista desplegable de claves de metadatos disponibles para seleccionar como filtro.
Conteo	Lista desplegable que especifica cuántos de los resultados principales se muestran.
Módulo	Lista desplegable que especifica de qué módulo se extraerán resultados.
Valor	Lista desplegable que especifica la información que se mostrará cuando se mantenga el mouse sobre un resultado (por ejemplo, Puntaje promedio).

Rueda de puntaje

La rueda de puntaje ofrece una vista de eventos como anillos concéntricos con colores que representan los puntajes de los eventos de acuerdo con indicadores de riesgo y el módulo de puntaje. Puede cambiar la posición de los anillos mediante las flechas hacia arriba y hacia abajo para obtener una vista que resalta los eventos que detectó un módulo de puntaje (rojo) y que no detectaron otros módulos de puntaje.

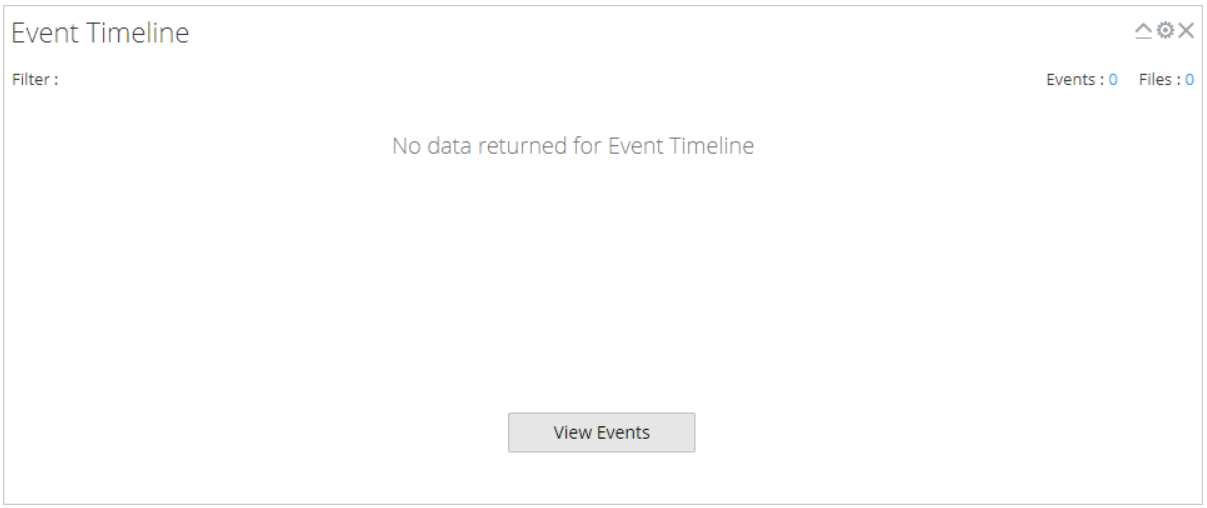


En la siguiente tabla se describen las funciones del dashlet Rueda de puntaje.

Función	Descripción
Solo alta confianza	Indica si los resultados se restringen o no a eventos marcados como de alta confianza. Si los resultados no están restringidos, esta línea no se muestra.
Cuadrícula Orden de módulos	Muestra el orden de los anillos en la rueda de puntaje. Anillo 1 es el anillo interior y Anillo 4, el exterior. Puede hacer clic en los botones **Arriba** y **Abajo** para reordenar los módulos y, a continuación, hacer clic en **Actualizar** para aplicar los cambios.

Cronograma de evento

El Cronograma de evento ofrece una vista de eventos organizados por el momento de la aparición en un gráfico de barras. Si se hace clic y se arrastra para seleccionar un rango de tiempo dentro del gráfico, se realiza un acercamiento al tiempo seleccionado.



En la siguiente tabla se describen las funciones del dashlet Cronograma de evento.

Función	Descripción
Solo alta confianza	Indica si los resultados se restringen o no a eventos marcados como de alta confianza. Si los resultados no están restringidos, esta línea no se muestra.
Ver eventos	Muestra la vista Investigation > Eventos.

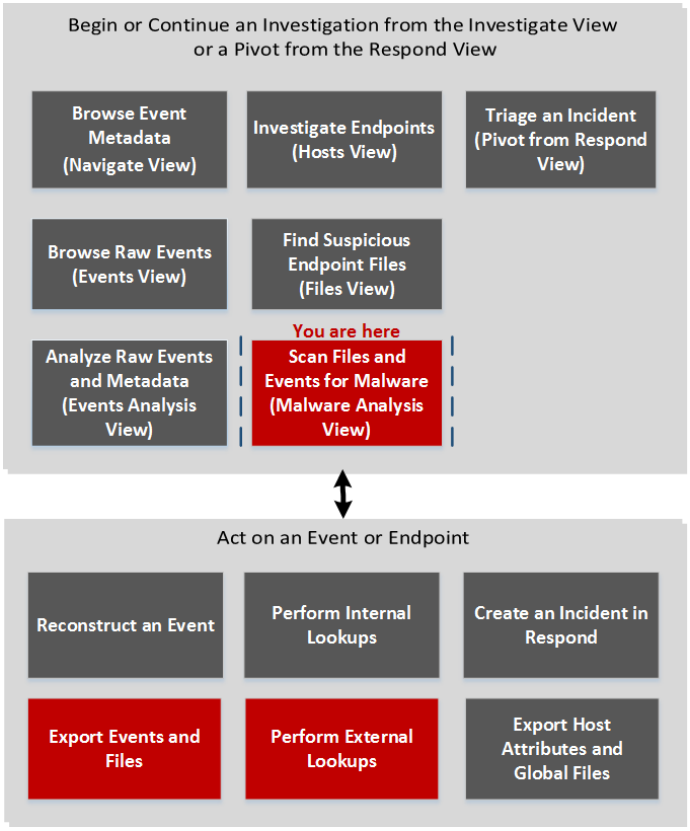
Lista de eventos y Lista de archivos de Malware Analysis

La Lista de eventos y la Lista de archivos de Malware Analysis proporcionan una vista detallada de eventos o archivos. Puede hacer doble clic en un evento o un archivo en cualquiera de las listas para mostrar la vista Resultados del análisis en una nueva pestaña del navegador.

Para acceder a esta vista, vaya a **INVESTIGAR > Malware Analysis** > cuadro de diálogo **Seleccionar un servicio Malware Analysis**. Seleccione un servicio en el panel izquierdo, seleccione un trabajo en el panel derecho y haga clic en **Ver escaneo**. En la vista Resumen de eventos, realice una de las siguientes acciones:

- En el panel **Total** o en el panel **Alta confianza**, haga clic en el número de la sección **Eventos creados**.
- Si desea ver la Lista de archivos, haga clic en el número de la sección **Archivos procesados**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos*	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	exportar eventos y archivos*	Examinar archivos y eventos de escaneo en formato de lista
Buscador de amenazas	realizar búsquedas externas*	Ver detalles de Malware Analysis de un evento

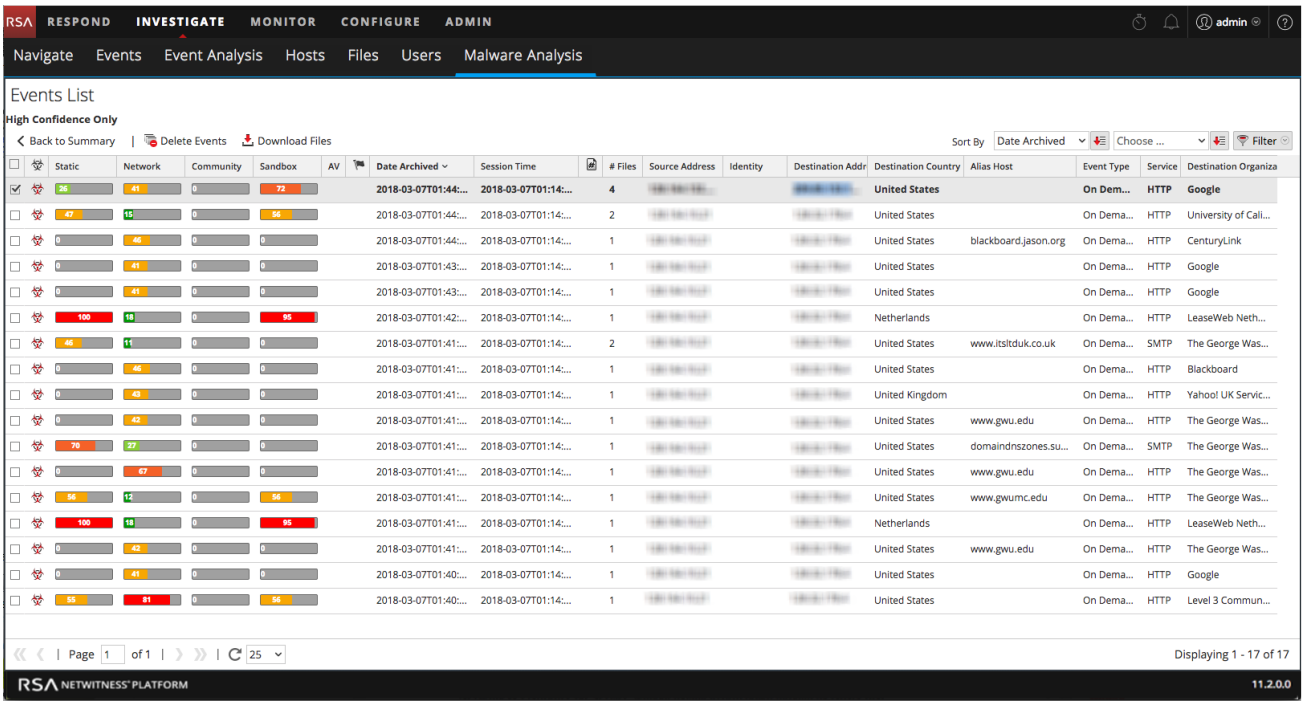
*Puede realizar esta tarea en la vista actual.

Temas relacionados

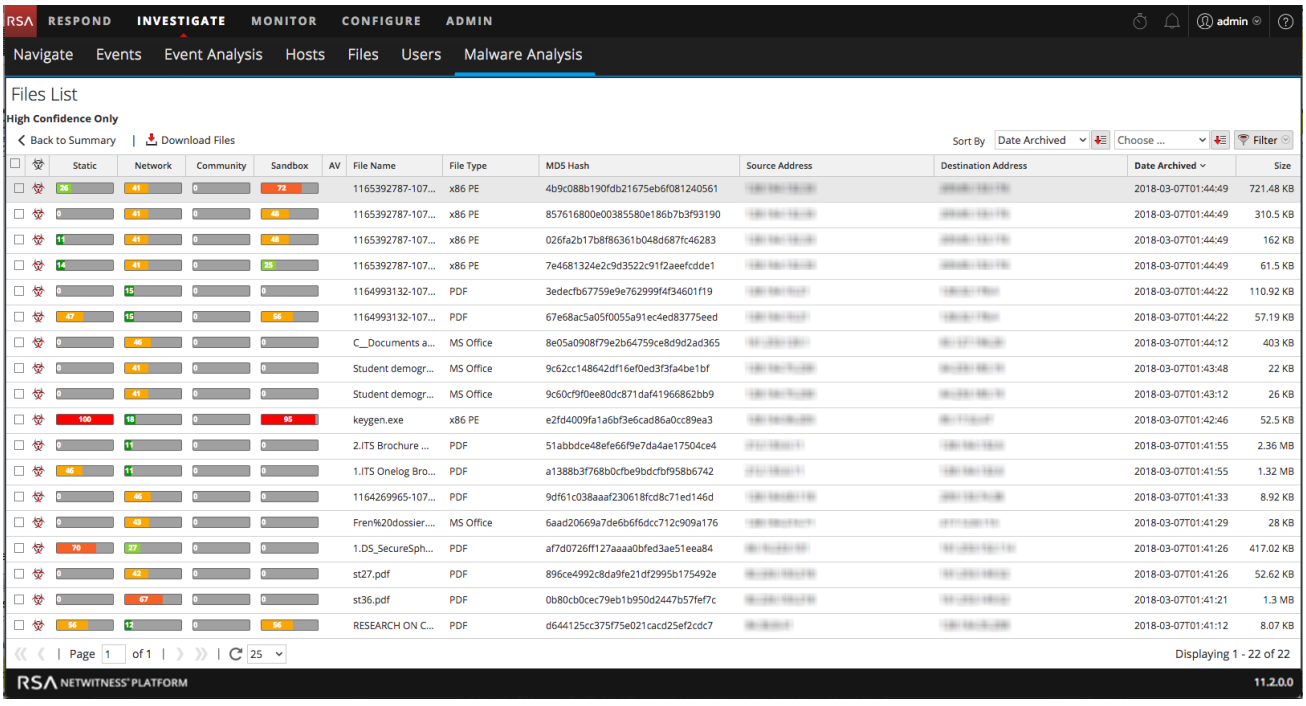
- Cómo funciona NetWitness Investigate

Vista rápida

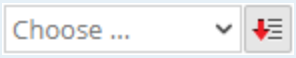
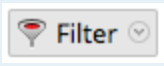
Este es un ejemplo de la vista Lista de eventos.



Este es un ejemplo de la vista Lista de archivos.



Estas son las funciones de la barra de herramientas de la Lista de eventos y la barra de herramientas de la Lista de archivos es la misma, salvo que no tiene ninguna opción de eliminación de eventos.

Función	Descripción
Volver al resumen	Regresa a la vista Resumen de eventos.
Eliminar eventos	Quita los eventos seleccionados de la lista de eventos actual.
Descargar archivos	Muestra el cuadro de diálogo Descarga de archivo de malware, el cual permite descargar los archivos disponibles.
	Muestra un menú desplegable desde el cual puede decidir cómo ordenar la lista. Estas son las opciones disponibles para ordenar la lista: • Alta confianza • Estático • Red • Comunidad • Sandbox • AV • Nombre de archivo • Tipo de archivo • Hash • Fecha de archivado • Tamaño El botón directamente a la derecha de esta lista desplegable indica si la lista se ordenará por valores ascendentes o descendentes.
	Muestra un menú desplegable desde el cual puede seleccionar un orden de clasificación secundario. Este menú incluye una opciónNetWitness Platform**Ninguno** que hace innecesaria la selección de un orden de clasificación secundario.
	Muestra una ventana desplegable en la cual puede filtrar la lista por nombre de archivo o hash de MD5.

Estas son las funciones de la Lista de eventos.

Función	Descripción
	Indica si el evento tiene influencia de la marca de alta confianza.
Estático, Red, Comunidad y Sandbox	Muestra los puntajes de cada módulo de puntaje.
AV	Indica si el antivirus marcó este evento como sospechoso.

Función	Descripción
	Indica si el evento tiene influencia de una regla personalizada.
Fecha de archivado	Muestra la fecha y la hora en que se archivó el evento.
Tiempo de sesión	Muestra el tiempo de la sesión del evento.
	Indica si el valor de hash está marcado como de confianza.
Número de archivos	Muestra la cantidad de archivos que se incluyen en el evento.
Dirección de origen	Muestra la dirección del origen de eventos.
Identidad	Muestra la identidad del origen de eventos.
Dirección de destino	Muestra la dirección del destino del evento.
País de destino	Muestra el país del destino del evento.
Host de alias	Muestra el nombre de host del alias.
Tipo de evento	Muestra el tipo de evento. Por ejemplo, Carga manual.
Servicio	Muestra el servicio en el cual se produjo el evento.
Organización de destino	Muestra la organización del destino.

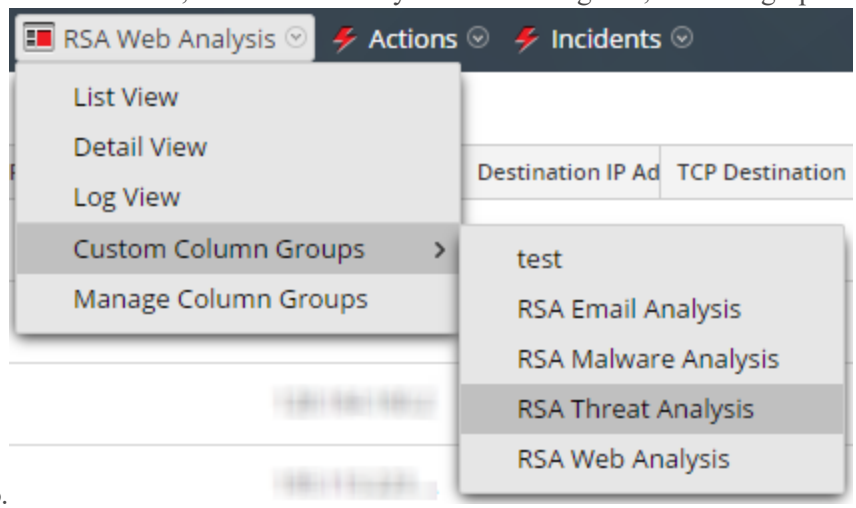
Estas son las funciones de la cuadrícula de la Lista de archivos.

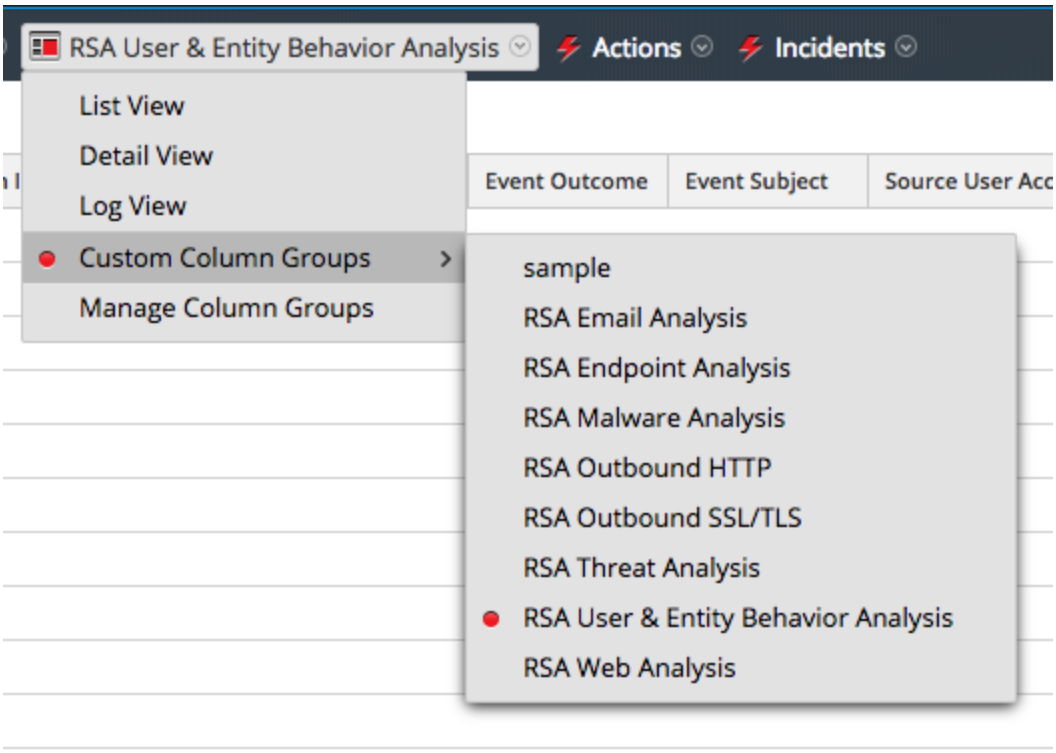
Función	Descripción
	Indica si el evento tiene influencia de la marca de alta confianza.
Estático, Red, Comunidad y Sandbox	Muestra los puntajes de cada módulo de puntaje.
AV	Indica si el antivirus marcó este evento como sospechoso.
Nombre de archivo	Muestra el nombre del archivo.
Tipo de archivo	Muestra el tipo del archivo (por ejemplo, PDF o x86 PE)
Hash de MD5	Muestra el hash de MD5.
Dirección de origen	Muestra la dirección del origen del archivo.
Dirección de destino	Muestra la dirección del destino del archivo.
Fecha de archivado	Muestra la fecha y la hora en que se archivó el archivo.
Tamaño	Indica el tamaño del archivo.

Cuadro de diálogo Administrar grupos de columnas

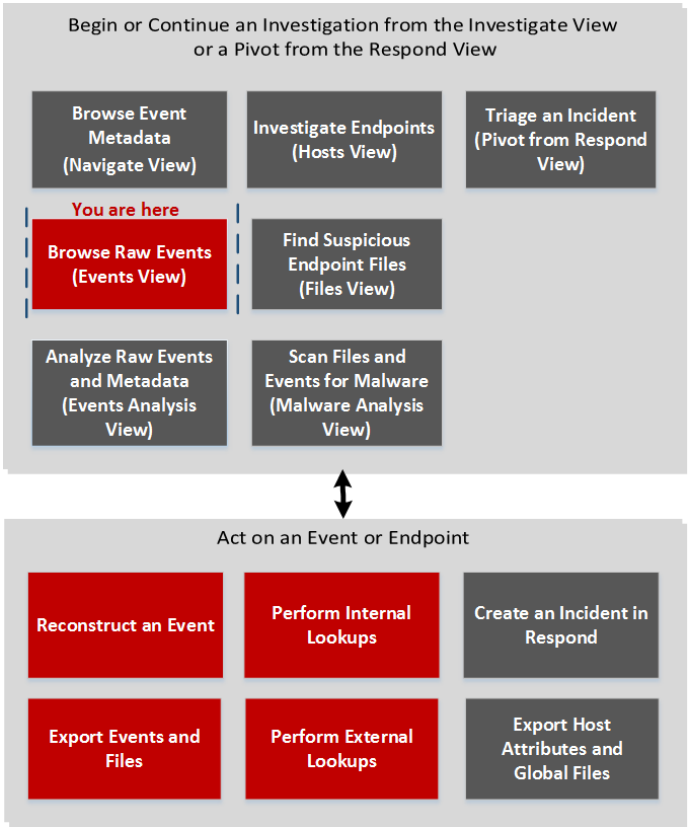
Puede personalizar la manera en que se muestran los datos mediante la definición de los metadatos que se muestran en una columna, la posición de la columna en la cuadrícula y el ancho predeterminado de la columna. El cuadro de diálogo Administrar grupos de columnas permite agregar, eliminar, importar, exportar y editar grupos de columnas para mostrar claves de metadatos específicas. En una instalación nueva, los grupos de columnas de uso inmediato (OOTB) están disponibles en el cuadro de diálogo Administrar grupos de columnas. Los grupos de columnas de uso inmediato tienen el prefijo RSA que permite su identificación y se pueden duplicar, pero no editar ni eliminar. También puede crear grupos de columnas personalizados.

Para acceder a este cuadro de diálogo, vaya a **INVESTIGAR > Eventos** y, en la lista desplegable **Ver**, seleccione **Administrar grupos de columnas**. El nombre de la opción **Ver** tiene relación con el valor actual, por ejemplo, la Vista detallada, la Vista de lista y la Vista de registro, o con el grupo de columnas seleccionado.





Flujo de trabajo



¿Qué desea hacer?

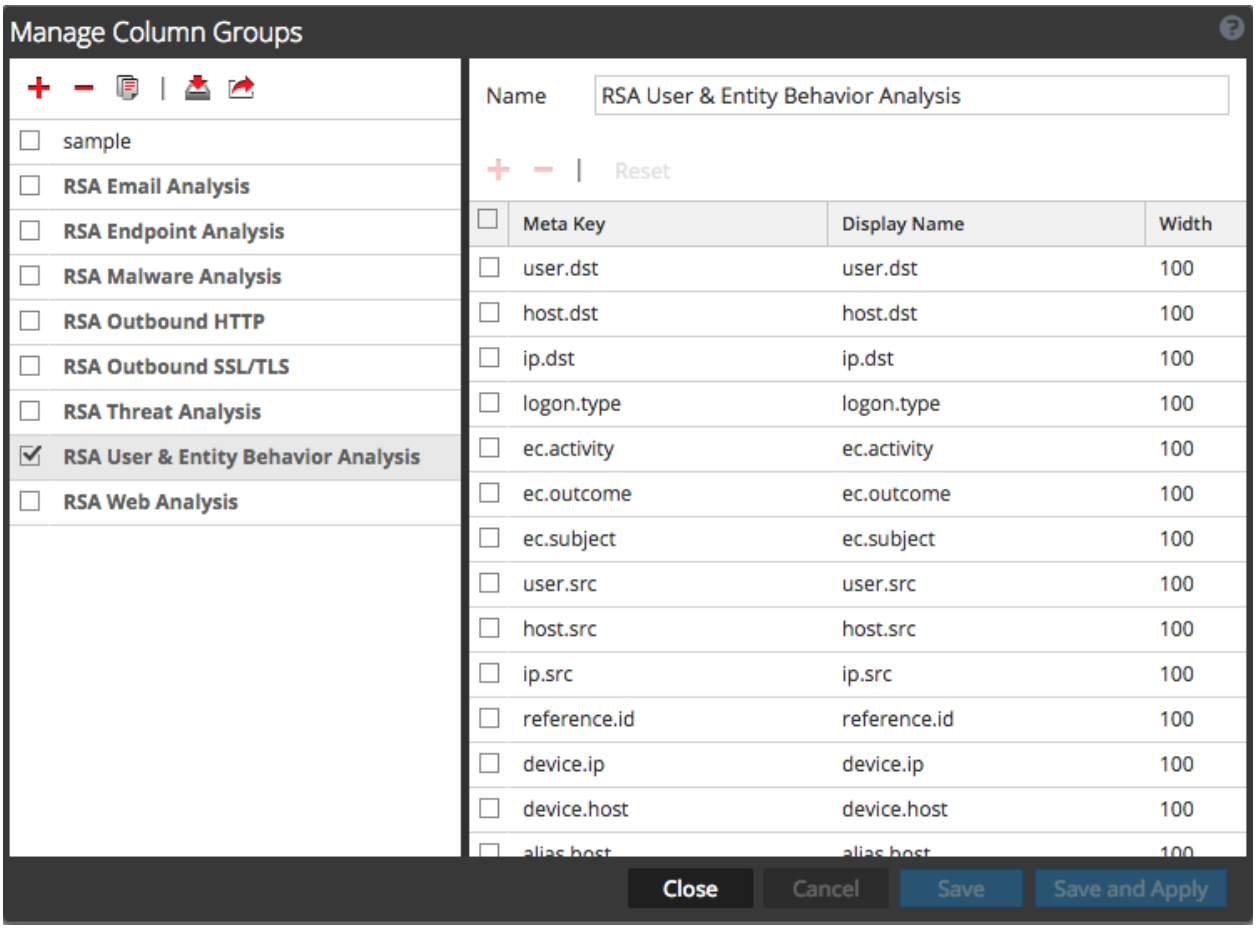
Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	configurar grupos de columnas	Administrar grupos de columnas en la vista Eventos

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Eventos

Vista rápida



El cuadro de diálogo Administrar grupos de columnas tiene dos paneles: Grupos y Configuración.

En la parte inferior de este cuadro diálogo hay cuatro botones: Cerrar, Cancelar, Guardar y Guardar y aplicar. En la siguiente tabla se proporcionan descripciones de estos botones.

Función	Descripción
Cerrar	Cierra el cuadro de diálogo sin guardar.
Cancelar	Cancela todos los cambios no guardados.
Guardar	Guarda todos los cambios sin cerrar el cuadro de diálogo.
Guardar y aplicar	Guarda y aplica todos los cambios de inmediato y cierra el cuadro de diálogo.

Panel Grupos

El panel izquierdo es el panel Grupos. Este panel permite agregar, eliminar, importar o exportar grupos de columnas. En la parte superior del panel hay una barra de herramientas que proporciona acciones. Debajo de la barra de herramientas encontrará una lista de grupos de columnas agregados que permite seleccionar uno o más grupos.

En la siguiente tabla se indican las acciones de la barra de herramientas.

Acción	Descripción
	Agrega un grupo de columnas. Si se hace clic en este botón, se resalta el panel Configuración de la derecha que permite dar un nombre al grupo de columnas y agregar o eliminar claves de metadatos. Para agregar un grupo, se requiere por lo menos una clave de metadatos.
	Elimina un grupo de columnas. Se muestra un cuadro de diálogo de confirmación antes de la eliminación del grupo seleccionado.
	Muestra el cuadro de diálogo Importar grupos de columnas que permite seleccionar un archivo para cargar.
	Exporta uno o más grupos seleccionados a la computadora.

Panel Configuración

El panel de la derecha es el panel Configuración. Aquí puede crear y editar grupos de columnas. Este panel incluye el campo Nombre, una barra de herramientas y una cuadrícula.

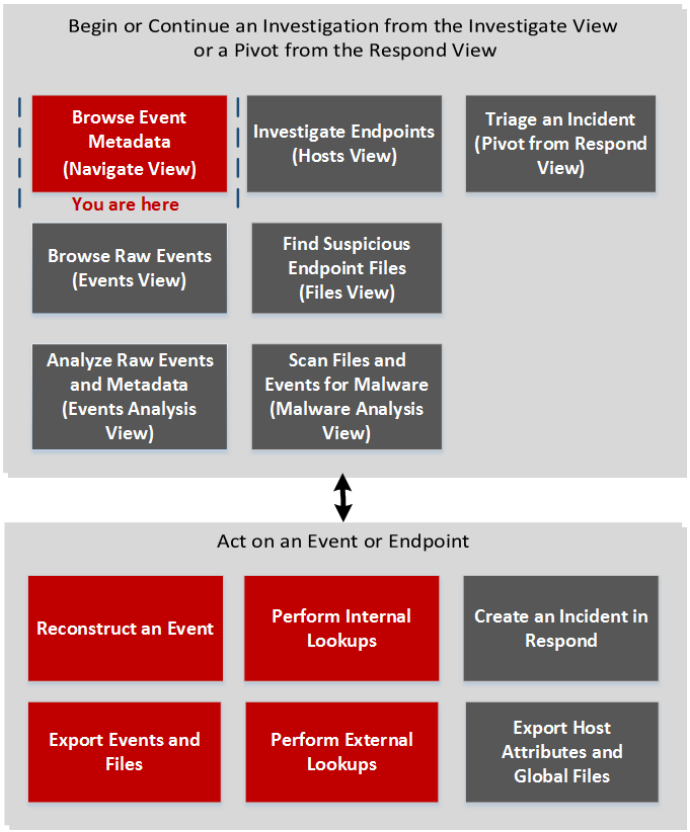
En la siguiente tabla se describen las funciones del panel Configuración.

Función	Descripción
Nombre	El nombre del grupo de columnas seleccionado.
	Agrega una nueva fila a la lista de claves de metadatos, donde puede abrir un menú desplegable para seleccionar una nueva clave de metadatos.
	Elimina una o más claves de metadatos seleccionadas. Muestra un cuadro de diálogo de confirmación antes de la eliminación.
Restablecer	Devuelve el grupo de columnas a la configuración guardada más reciente.
Clave de metadatos	Indica las claves de metadatos agregadas al grupo de columnas seleccionado.
Nombre para mostrar	Indica los nombres de las claves de metadatos como se mostrarán en la vista Eventos.
Ancho	Especifica el ancho de la columna de cada clave de metadatos. El ancho se puede configurar entre **10** y **1000**. El ancho predeterminado es **100**.

Cuadro de diálogo Administrar claves de metadatos predeterminadas

En el cuadro de diálogo Administrar claves de metadatos predeterminadas, los analistas pueden especificar las claves de metadatos que se mostrarán durante la navegación para un servicio específico. Esto puede ayudarlo a encontrar los datos que desea con mayor rapidez e impide la carga de metadatos que no son de interés. Para acceder a este cuadro de diálogo, en la barra de herramientas de la **vista Navegar**, seleccione **Metadatos > Administrar claves de metadatos predeterminadas**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	configurar claves de metadatos predeterminadas para un servicio*	Filtrar resultados en la vista Navegar

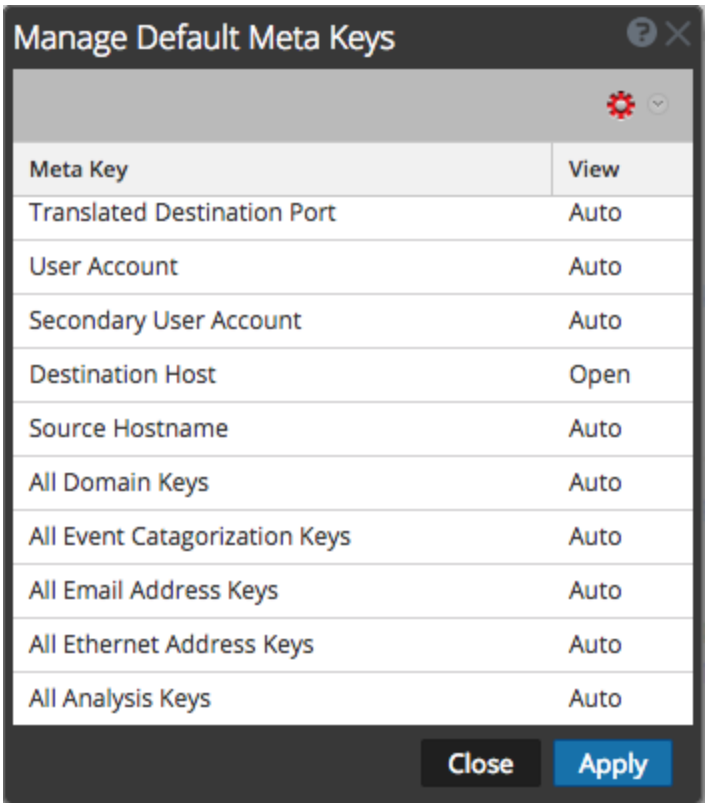
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Administrar grupos de metadatos
- Administrar grupos de metadatos

Vista rápida

En la siguiente figura se ilustra el cuadro de diálogo Administrar claves de metadatos predeterminadas, el cual incluye una lista de claves de metadatos, una barra de herramientas, un botón Cerrar y un botón Aplicar. En la lista, puede ver, ordenar y administrar las claves de metadatos predeterminadas. Si hace clic y arrastra las claves de metadatos, puede cambiar su orden. En la siguiente tabla se describen las columnas de la lista.



Columna	Descripción
Clave de metadatos	En esta columna se muestran las claves de metadatos disponibles para el servicio. En la versión 11.1 y superior, también se incluyen entidades de metadatos predeterminadas, como Todas las claves de dominios y Todas las claves de direcciones de correo electrónico.

Columna	Descripción
Ver	En esta columna se muestra el tipo de vista asignado a cada clave de metadatos. Si hace clic en la vista en cada fila, puede asignar otra vista predeterminada a la clave de metadatos. Hay cuatro vistas: • Automática: revierte a la vista predeterminada para las claves de metadatos según se especifica en el archivo de índice del servicio. • Cerrada: los valores de esta clave de metadatos están cerrados de manera predeterminada y se pueden abrir manualmente. • Oculta: estas claves de metadatos están ocultas de manera predeterminada y no se muestran en absoluto en Investigation. • Abierto: Los valores de esta clave de metadatos se muestran de manera predeterminada. Cuando modifica las claves de metadatos predeterminadas para una clave de metadatos no indexada, no puede configurar la clave en **Abierto**. Si cambia a **Abierto** la vista predeterminada para un grupo de claves de metadatos y algunas de las claves de metadatos no están indexadas, estas claves vuelven a **Automático**. En consecuencia, la clave de metadatos se carga automáticamente solo si está indexada, y las claves de metadatos no indexadas se **Cierran** hasta que se abren de forma manual.

En la siguiente tabla se describen las opciones de la barra de herramientas y los botones.

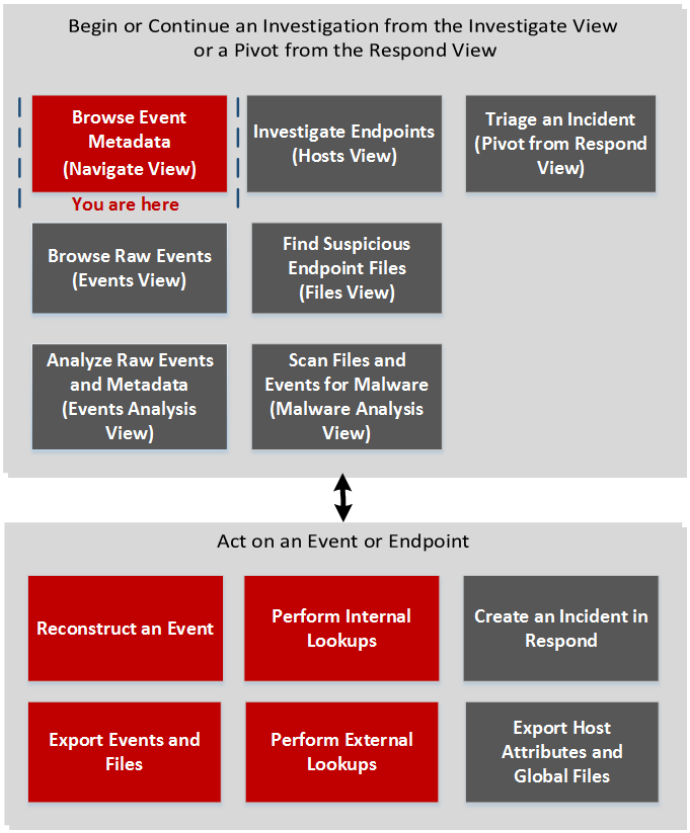
Función	Descripción
	Si hace clic en el menú Acciones, puede cambiar la vista predeterminada de todas las claves de metadatos. Hay cuatro vistas: • Automática: revierte a la vista predeterminada para las claves de metadatos según se especifica en el archivo de índice del servicio. • Cerrada: los valores de esta clave de metadatos están cerrados de manera predeterminada. • Oculta: los valores de esta clave de metadatos están ocultos de manera predeterminada. • Abierto: los valores de esta clave de metadatos se muestran de manera predeterminada.
Cerrar	Cierra el cuadro de diálogo. Los cambios sin guardar se pierden.
Aplicar	Aplica los cambios y estos se implementan de inmediato.

Cuadro de diálogo Administrar grupos de metadatos

En una instalación nueva, los grupos de metadatos de uso inmediato están disponibles en el cuadro de diálogo Administrar grupos de metadatos. Los grupos de metadatos de uso inmediato tienen el prefijo RSA que permite su identificación y se pueden duplicar, pero no editar ni eliminar. El cuadro de diálogo Administrar grupos de metadatos permite agregar, eliminar, importar y exportar grupos de metadatos.

Para acceder a este cuadro de diálogo, en la barra de herramientas de **Investigation > vista Navegar**, seleccione **Metadatos > Administrar grupos de metadatos**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	agregar, editar y eliminar grupos de metadatos*	Administrar grupos de metadatos

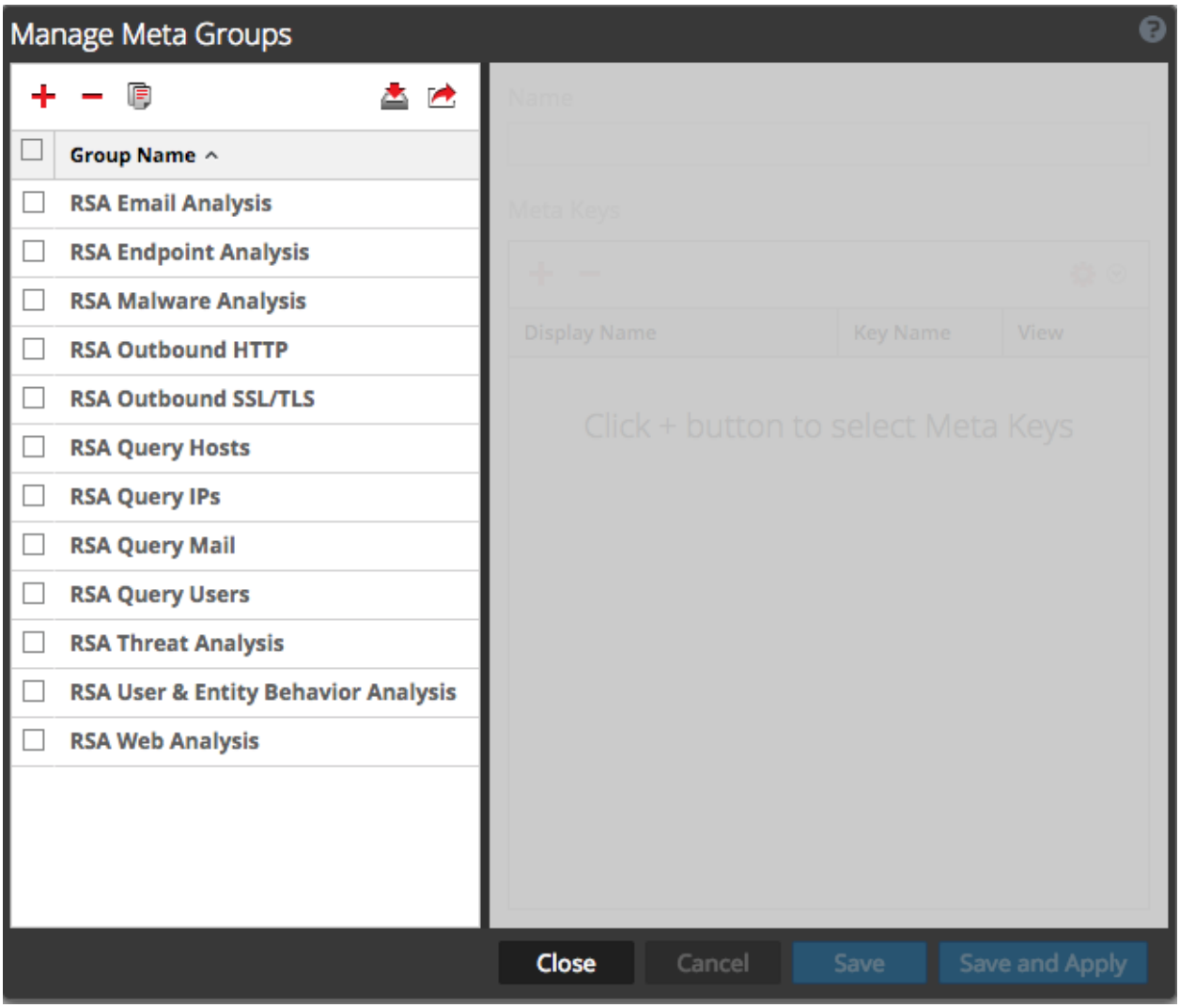
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Filtrar resultados en la vista Navegar
- Cómo funciona NetWitness Investigate

Vista rápida

Este es un ejemplo del cuadro de diálogo para la versión 11.1, en el que están disponibles grupos de metadatos de uso inmediato adicionales: Análisis de Endpoint de RSA, HTTP de salida de RSA y Protocolos SSL/TLS de salida de RSA. El cuadro de diálogo Administrar grupos de metadatos tiene dos paneles. En la siguiente tabla se describen los botones de la parte inferior del cuadro de diálogo.



Función	Descripción
Cerrar	Cierra el cuadro de diálogo.
Cancelar	Cancela todos los cambios.
Guardar	Guarda todos los cambios.
Guardar y aplicar	Guarda todos los cambios y los aplica de inmediato.

El panel Grupos de metadatos está en el lado izquierdo del cuadro de diálogo Administrar grupos de metadatos. Aquí puede agregar, eliminar, importar y exportar grupos de metadatos.

En la siguiente tabla se describen las funciones del panel Grupos de metadatos.

Función	Descripción
+	Agrega un grupo de metadatos mediante el panel Configuración del lado derecho del cuadro de diálogo Administrar grupos de metadatos.
−	Elimina los grupos de metadatos seleccionados. Se muestra un cuadro de diálogo de confirmación antes de la eliminación del grupo de metadatos.
	Muestra el cuadro de diálogo Importación de grupo de metadatos, en el cual puede cargar un archivo.
	Exporta el grupo de metadatos seleccionado a la computadora.
Nombre del grupo	Enumera todos los nombres de grupos de metadatos.

El panel Configuración está en el lado derecho del cuadro de diálogo Administrar grupos de metadatos. Aquí puede crear y editar grupos de metadatos. Debajo del campo Nombre se encuentra la cuadrícula Claves de metadatos.

En la siguiente tabla se describen las funciones del panel Configuración.

Función	Descripción
Nombre	Muestra el nombre del grupo de metadatos seleccionado.
+	Muestra el cuadro de diálogo Claves de metadatos disponibles, en el cual puede seleccionar las claves de metadatos que agregará al grupo.
−	Elimina las claves de metadatos seleccionadas.
	Muestra un menú desplegable que permite seleccionar la vista para todas las claves de metadatos. Hay cuatro opciones de acuerdo con los posibles valores de la propiedad `defaultAction` que se usa para definir una clave en el archivo de índice personalizado para el servicio: • Oculta: estas claves de metadatos están ocultas de manera predeterminada y no se muestran en absoluto en Investigation. • Abierto: los valores de esta clave de metadatos se muestran de manera predeterminada. • Cerrada: los valores de esta clave de metadatos están cerrados de manera predeterminada y se pueden abrir manualmente. • Automática: revierte a la vista predeterminada para las claves de metadatos según se especifica en el archivo de índice del servicio.
Nombre para mostrar	Indica el nombre que se muestra para la clave en las vistas de Investigation y se define mediante la propiedad `description` para la clave en el archivo de índice personalizado del servicio.
Nombre de clave	Indica el valor `name` de la clave de metadatos según se define en el archivo de índice personalizado del servicio.

Función	Descripción
Ver	Indica para qué vista está configurada la clave de metadatos. Para cambiar esto: • Haga clic en **v** en el encabezado de la columna Ver y seleccione una vista para cambiar todas las vistas de la clave de metadatos. • Haga clic en una única clave de metadatos en la columna Vista y abra el menú desplegable en el cual se muestran todas las vistas disponibles para cambiar una vista de clave de metadatos individual.

Cuadro de diálogo Administrar perfiles

Los perfiles permiten configurar vistas personalizadas en la vista Navegar y en la vista Eventos. En una instalación nueva, los perfiles de uso inmediato están disponibles en el cuadro de diálogo Administrar perfiles. Los grupos de perfiles de uso inmediato tienen el prefijo RSA que permite su identificación y se pueden duplicar, pero no editar ni eliminar. El cuadro de diálogo Administrar perfiles permite configurar, agregar, eliminar, importar y exportar perfiles. En la versión 11.2 y superior, puede organizar los perfiles en grupos de perfiles.

Para acceder a este cuadro de diálogo, en la barra de herramientas de las vistas **Investigation** > **Navegar** o **Eventos**, seleccione **Perfil** > **Administrar perfiles**.

¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	configurar perfiles para las vistas Navegar o Eventos*	Usar perfiles para encapsular vistas personalizadas

*Puede realizar esta tarea en la vista actual.

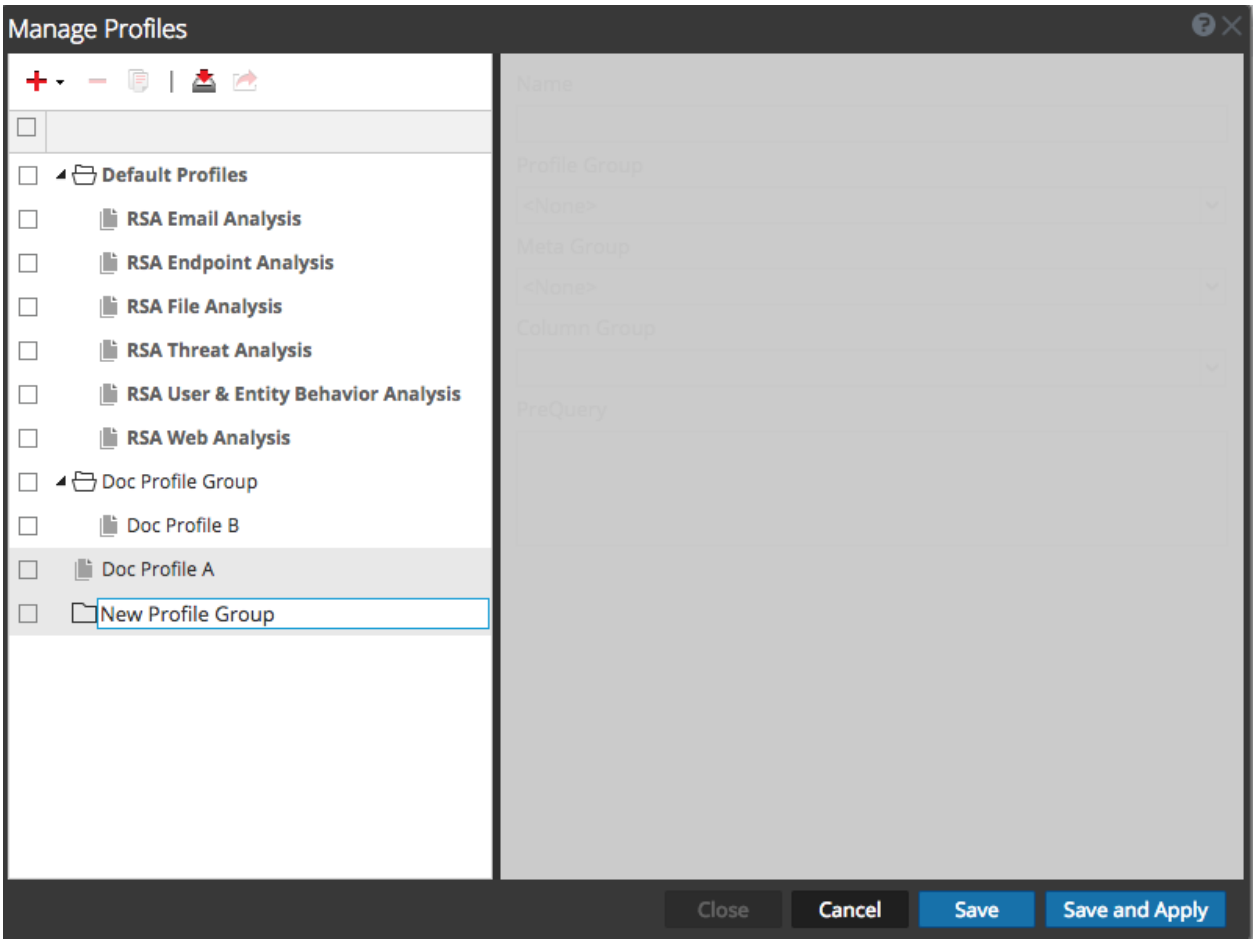
Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Navegar

- Vista Eventos

Vista rápida

Este es un ejemplo del cuadro de diálogo Administrar perfiles en el que se muestran varios grupos de perfiles.



El cuadro de diálogo Administrar perfiles tiene dos paneles. En la parte inferior del cuadro de diálogo se incluye una fila de botones. En la siguiente tabla se describen los botones.

Campo	Descripción
Cerrar	Cierra el cuadro de diálogo.
Cancelar	Cancela todos los cambios.
Guardar	Guarda todos los cambios.
Guardar y aplicar	Guarda y aplica todos los cambios de inmediato.

El panel Perfil del lado izquierdo del cuadro de diálogo muestra los perfiles disponibles y permite agregar, eliminar, importar y exportar perfiles. En la siguiente tabla se describen los campos del panel Perfil.

Campo	Descripción
	Agrega un nuevo perfil mediante el panel Configuración del lado derecho del cuadro de diálogo Administrar perfiles.
	Elimina el perfil seleccionado. Antes de que se elimine el perfil, se muestra un cuadro de diálogo de confirmación.
	Muestra el cuadro de diálogo Importación de perfil, el cual permite cargar un archivo.
	Exporta el perfil seleccionado a una computadora.
Nombre de perfil	Enumera todos los nombres de perfil.

El panel Configuración del lado derecho del cuadro de diálogo ofrece opciones para configurar perfiles. Solo se puede usar cuando hay un perfil seleccionado. En la siguiente tabla se describen los campos del panel Configuración.

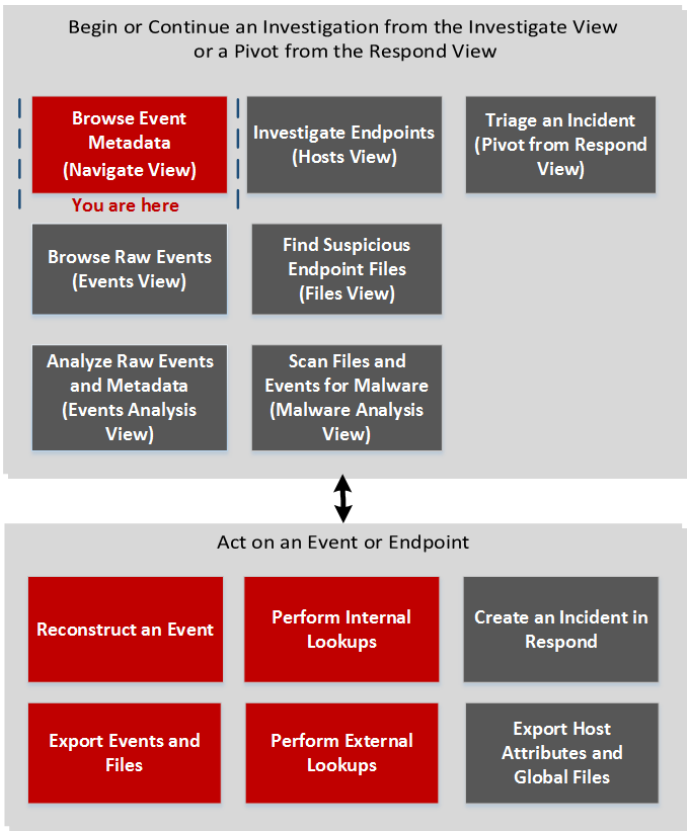
Función	Descripción
Nombre	Muestra el nombre del perfil.
Grupo de metadatos	Muestra un menú desplegable que enumera los grupos de metadatos disponibles.
Grupo de columnas	Muestra un menú desplegable que enumera los grupos de columnas disponibles. De manera predeterminada, hay tres grupos disponibles: • Vista de lista • Vista detallada • Vista de registro
Consulta previa	Define una consulta restrictiva para filtrar los resultados de Investigation. Esta consulta se usa cuando el perfil asociado está habilitado y la consulta previa se aplica a cualquier consulta utilizada en las vistas Navegar y Eventos de Investigation. Este es un ejemplo de una consulta previa: `'service=80,25,110'.`

Vista Navegar

La Vista Navegar (**INVESTIGAR** > Navegar) muestra los metadatos de eventos, las claves y los valores de metadatos, que se encontraron en los datos capturados del servicio seleccionado. Los datos se filtran y se muestran de acuerdo con las opciones que configuró para el perfil, el rango de tiempo, el grupo de metadatos y la consulta. También puede desglosar a los datos, para lo cual debe hacer clic en las claves y los valores de metadatos. La vista Navegar es el punto de entrada predeterminado a NetWitness Investigate; puede cambiar el punto de entrada predeterminado a una de las demás vistas en las preferencias del Perfil.

Flujo de trabajo

En la siguiente figura se describe el flujo de trabajo general para la investigación de metadatos de eventos.



Estas son las tareas que puede realizar en Vista Navegar:

- Seleccione un servicio para investigar y cargar datos.
- Vea los resultados de la consulta y filtre por rango de tiempo, perfil y grupo de metadatos.
- Ordene los resultados y seleccione un método de cuantificación.
- Guarde los eventos, vaya a un evento mediante el ID de evento, visualice un evento e imprímalo.

- Vea datos contextuales adicionales para claves y valores de metadatos específicas.
- Vaya a la Vista Eventos o a la vista Análisis de eventos, donde puede ver una lista cronológica de eventos, reconstruirlos y realizar un análisis interactivo de estos. Cuando visualiza y analiza eventos, puede exportar eventos, archivos y registros al sistema de archivos local.

¿Qué desea hacer?

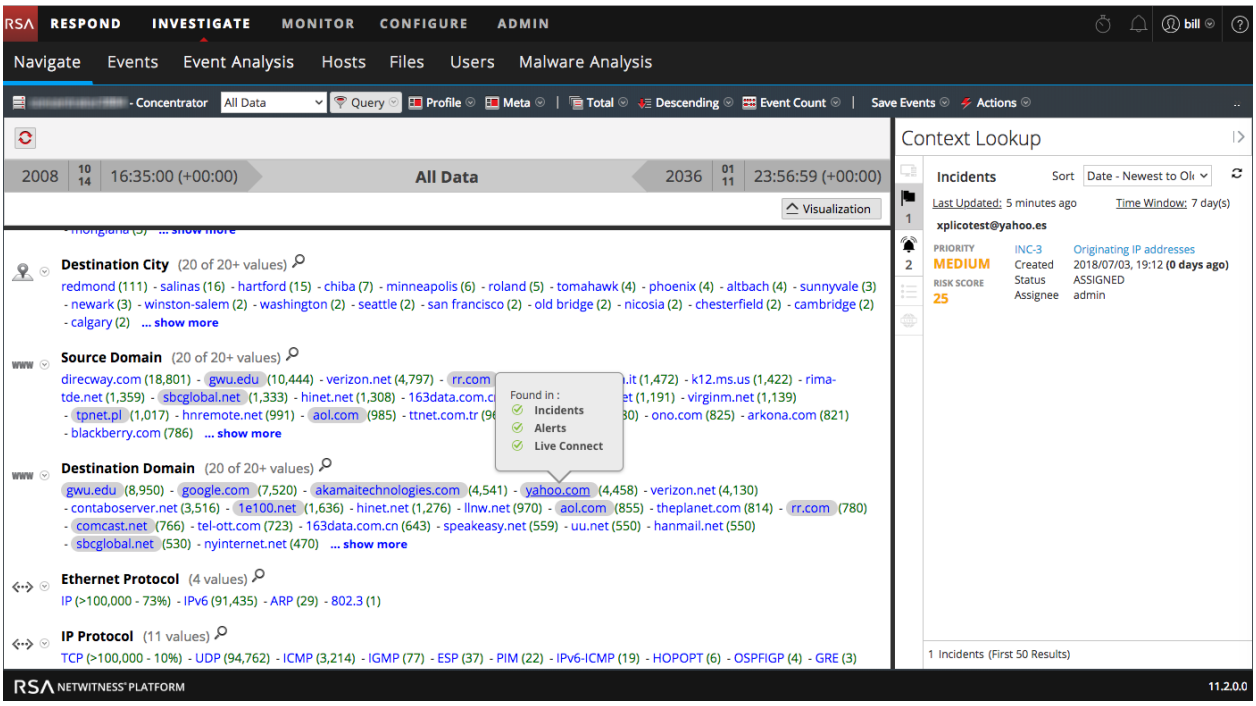
Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos*	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos*	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	configurar las preferencias de usuario para la vista Navegar*	Configurar la vista Navegar y la vista Eventos
Buscador de amenazas	enviar una consulta o desglosar al conjunto de datos*	Investigación de metadatos en la vista Navegar
Buscador de amenazas	limitar los resultados de consulta*	Consulta y realización de acciones en datos en las vistas Navegar y Eventos
Buscador de amenazas	realizar búsquedas internas*	Buscar contexto adicional en las vistas Navegar y Eventos
Buscador de amenazas	realizar búsquedas externas*	Iniciar una búsqueda externa de una clave de metadatos

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Eventos
- Vista Análisis de eventos
- Vista Malware Analysis

Vista rápida



La vista Navegar consta de las siguientes características:

- Barra de herramientas
- Botón Pausa/Recarga y ruta de navegación
- Anuncio de tiempo
- Información de depuración opcional.
- Panel Visualización contraíble
- Panel Valores
- Panel Búsqueda de contexto
- Menús contextuales

Barra de herramientas

La barra de herramientas proporciona una manera de:

- Cambiar el servicio que se investiga.
- Controlar el rango de datos que se muestra: puede seleccionar perfiles de uso, establecer un rango de tiempo, usar grupos de metadatos y crear consultas para aplicar a los datos.
- Establecer el método de cuantificación y el método de clasificación de los datos en el panel Valores.
- Realizar acciones en función de los resultados. Puede exportar e imprimir resultados, abrir un evento para el cual tiene un ID de evento en las vistas Eventos o Análisis de eventos y transmitir una consulta a Informer.
- Configurar ajustes de Investigate sin salir de las vistas de Investigate.

Algunas de las opciones de la barra de herramientas están etiquetadas con el valor predeterminado o el valor seleccionado en lugar de mostrar el nombre de la opción. Por ejemplo, la opción de rango de tiempo del ejemplo anterior está etiquetada **Últimos 5 minutos** para reflejar el valor seleccionado actualmente. Estas son las opciones de la barra de herramientas.

Opción	Descripción
	Muestra el nombre del servicio seleccionado junto al ícono. Si hace clic en el icono, se abre un cuadro de diálogo Investigar un servicio, en el cual puede seleccionar un servicio para investigar y establecer el servicio predeterminado que se investigará (consulte Comenzar una investigación en las vistas Navegar o Eventos). El cambio del servicio no hace que se vuelvan a cargar los datos.

Opción	Descripción
Rango de tiempo	Muestra las opciones de Rango de tiempo; la opción seleccionada actualmente aparece en la barra de herramientas (consulte Filtrar resultados en la vista Navegar). Las posibles opciones son: • Todos los datos • Últimos 5, 10, 15 o 30 minutos • Última hora, últimas 3, 6, 12 o 24 horas • Últimos 2 o 5 días • Primera hora • Mañana • Tarde • Noche • Todo el día • Ayer • Esta semana • La semana pasada • Personalizado **Nota:** Si se especifican horas de inicio o finalización personalizadas en segundos, siempre el valor de la hora de inicio en segundos se configura de manera predeterminada en :00 y siempre el valor de la hora de finalización en segundos se configura de manera predeterminada en :59. Por ejemplo, si está usando la hora para desglosar a un problema, la hora de desglose se interpretará como `HH:MM:00 - HH:MM:59`. Los segundos se muestran en este formato en las funciones de Investigate.
Consulta	Se muestra el cuadro de diálogo Consulta, en el cual puede ingresar directamente una consulta personalizada, en lugar de desglosar los datos. Consulte Cuadro de diálogo Consulta para obtener una descripción del cuadro de diálogo.
Perfil	Muestra el menú Perfil; el perfil seleccionado se muestra en la barra de herramientas. Un perfil permite administrar y usar perfiles que pueden incluir grupos de metadatos personalizados, un grupo de columnas predeterminado y una consulta inicial. Los perfiles se aplican a la vista Navegar (consultas y grupos de metadatos) y a la vista Eventos (consultas y grupos de columnas). Consulte Usar perfiles para encapsular vistas personalizadas para obtener más información.
Metadatos	Muestra el menú Grupo de metadatos. Puede usar claves de metadatos predeterminadas o un grupo de metadatos personalizado. También tiene la opción de realizar cambios en ambos tipos de grupos (consulte Administrar grupos de metadatos).

Opción	Descripción
Campo de clasificación	Muestra el menú Campo de clasificación; la opción actualmente seleccionada se muestra en la barra de herramientas. Este menú tiene dos opciones: Ordenar por total y Ordenar por valor. El Campo de clasificación es un complemento de la opción Orden de clasificación; los datos de cada clave de metadatos se ordenan de acuerdo con el total (número verde) o con el valor de metadatos (texto azul) (consulte Filtrar resultados en la vista Navegar).
Orden de clasificación	Muestra el menú Orden de clasificación; la opción seleccionada actualmente se muestra en la barra de herramientas. Este menú tiene dos opciones: Clasificar en orden ascendente y Clasificar en orden descendente. El Orden de clasificación es un complemento de la opción Campo de clasificación; el campo seleccionado de cada clave de metadatos se clasifica en orden ascendente o descendente (consulte Filtrar resultados en la vista Navegar).
Método de cuantificación	Muestra el menú Método de cuantificación; la opción seleccionada actualmente se muestra en la barra de herramientas. El método de cuantificación solo se aplica a los resultados de claves de metadatos del panel Valores. No se aplica al cronograma. El menú desplegable contiene tres opciones para calcular la cantidad (el número verde entre paréntesis) para un valor de metadatos: Cuantificar por conteo de eventos, Cuantificar por tamaño de evento y Cuantificar por conteo de paquetes (consulte Filtrar resultados en la vista Navegar). Estas opciones se aplican de manera diferente según el tipo de datos de la vista. Para datos de paquetes: • Cuantificar por conteo de eventos muestra la cantidad de sesiones. • Cuantificar por tamaño de evento muestra el tamaño en bytes. • Cuantificar por conteo de paquetes muestra la cantidad de paquetes. Para datos del registro: • Cuantificar por conteo de eventos muestra la cantidad de registros. • Cuantificar por tamaño de evento muestra el tamaño en bytes. • Cuantificar por conteo de paquetes muestra la cantidad de registros.
Guardar eventos	Muestra el menú Guardar eventos, en el cual pude utilizar opciones para: extraer archivos asociados con un evento, exportar el punto de desglose actual como un archivo PCAP y exportar el punto de desglose actual como un archivo de registro (consulte Exportar un punto de desglose).
Acciones	El menú Acciones incluye acciones que puede realizar en la vista Navegar (consulte Investigación de metadatos en la vista Navegar). En la versión 11.0.0.x, las opciones son las siguientes: Visualizar, Ir a evento e Imprimir. En la versión 11.1 y superior, las opciones son Visualizar, Ir a evento en Reconstrucción de evento, Ir a evento en Análisis de eventos e Imprimir.

Opción	Descripción
Buscar eventos	Permite buscar patrones de texto en el conjunto de eventos actual. Si hace clic en el campo de búsqueda, se muestra un menú desplegable con opciones de búsqueda. Si hace clic en Aplicar, guarda las opciones seleccionadas y también actualiza las opciones de búsqueda en la vista Eventos y en el perfil de investigaciones (consulte Buscar patrones de texto).
Ajustes de configuración	Muestra la configuración de la vista Navegar (la cual también se pueden editar en la vista Perfil), de modo que puede cambiar la configuración de Investigate sin salir de la vista Navegar. Cuando cambia un ajuste en la vista Navegar, este también se cambia en la vista Perfil (consulte Configurar la vista Navegar y la vista Eventos).

Botón Pausa/Recarga y ruta de navegación

La ruta de navegación rastrea cada consulta a medida que se desglosa a través de los metadatos del servicio. Cada consulta se enumera con un menú desplegable en una cadena separada por barras verticales. El último punto es el punto actual, que también se llama punta. El ícono frente a la ruta de navegación permite poner en pausa la carga de valores de metadatos y volver a cargarlos.

La ruta de navegación no incluye el nombre del servicio y solo se muestra si hay una consulta vigente. Si existen demasiados puntos de desglose para mostrar, el desbordamiento se indica como paréntesis angulares dobles, >>, al final de la ruta de navegación.

Cada menú desplegable en la ruta de navegación es igual, pero presenta una leve variación en función de la posición en la ruta de navegación.

En la siguiente tabla se describen los controles y las opciones de menú en la ruta de navegación.

Función	Descripción
	Botón Pausa y Recarga. Controla la carga de datos en la vista. Tiene tres funciones posibles: pausar carga, continuar carga y volver a cargar.
Navegar aquí	Abre el punto de desglose seleccionado en el panel Valores actual.
Navegar aquí (nueva pestaña)	Abre el punto de desglose seleccionado en una nueva pestaña.
Insertar antes	Inserta una consulta antes del punto de desglose actual. Se abre el cuadro de diálogo Crear filtro, en el cual puede definir una consulta personalizada para insertar en la ruta de navegación (consulte Crear una consulta personalizada).
Agregar	Agrega una consulta después del punto de desglose actual. Se abre el cuadro de diálogo Crear filtro, en el cual puede definir una consulta personalizada para agregar al final de la ruta de navegación (consulte Crear una consulta personalizada).
Quitar	Elimina el punto de desglose seleccionado de la ruta de navegación.
Editar	Abre el punto de desglose seleccionado en el cuadro de diálogo Crear filtro, lo cual le permite editar la consulta.

Función	Descripción
>>	Si hace clic en los paréntesis angulares, se muestra un menú desplegable del desbordamiento de la ruta de navegación.

(Opcional) Información de depuración

Si activó el ajuste Mostrar información de depuración y el servicio en el cual está navegando es un Broker 10.4 o superior, NetWitness Platform muestra la información de depuración debajo de la ruta de navegación.

La información de depuración es la cláusula `where` de la consulta actual. La única vez que no hay una cláusula `where` es cuando el rango de tiempo corresponde a todos los datos y no hay puntos de desglose. Si el Broker tiene por lo menos un servicio agregado que está offline, la información de depuración también incluye el servicio offline.

Por ejemplo:

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)$$time='2014-05-
04 18:50:00"-"2014-05-09 18:59:59(attachment exists) && (tcp.dstport = '80')
&& (risk.info exists) && time="2014-05-04 18:50:00"-"2014-05-09 18:50:59"
```

Además, el tiempo de carga se muestra al final de cada clave de metadatos en el panel Valores.

Anuncio de tiempo

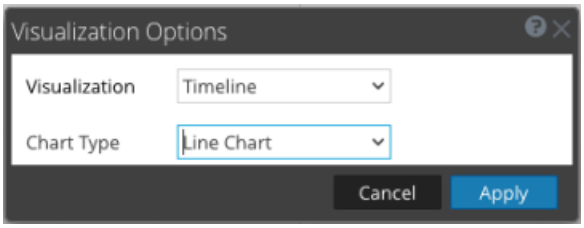
Inmediatamente debajo de la ruta de navegación y de la información de depuración (si está presente), el anuncio de tiempo muestra el rango de tiempo que se usó para crear el gráfico.

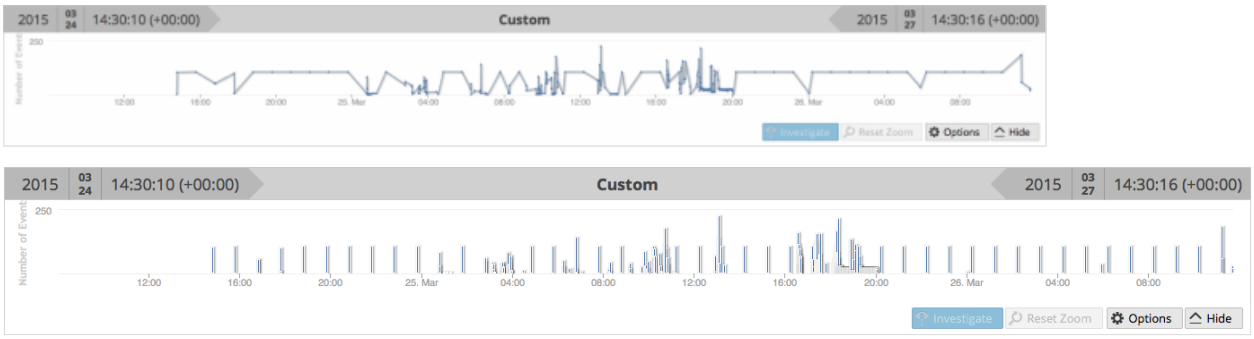
Visualizaciones

En la parte superior de la vista Navegar hay una visualización del punto de desglose actual. Puede usarlo para desglosar a datos desde el panel Visualización (consulte Filtrar resultados en la vista Navegar). Puede mostrar u ocultar la visualización y elegir una de las opciones de visualización: Cronograma o Coordenadas. La visualización se abre inicialmente en la última visualización guardada.

Gráfico de cronograma

El cronograma es el conteo de la cantidad de eventos que ocurren en una instancia específica. El cronograma proporciona conteos de eventos que le permiten ver si la cantidad de eventos aumenta considerablemente en un punto en el tiempo determinado. El cronograma muestra actividad del servicio y el rango de tiempo especificados como un gráfico de líneas o un gráfico de barras, de acuerdo con la selección en el menú Opciones. En la segunda figura se ilustra un gráfico de líneas y en la tercera, un gráfico de barras.



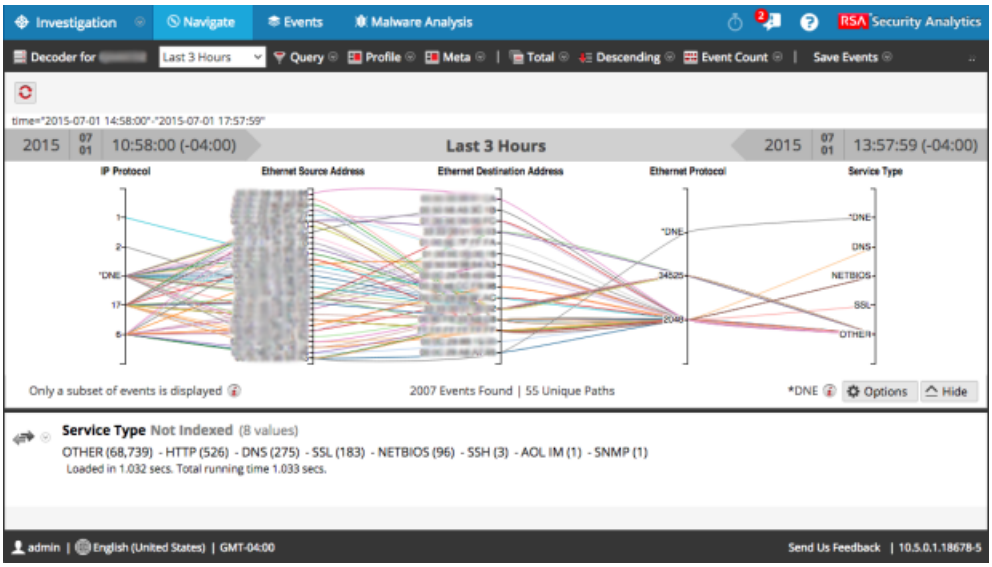


El cronograma muestra actividad del servicio y el rango de tiempo especificados como un gráfico de líneas o un gráfico de barras, de acuerdo con la selección en el menú Opciones.

Función	Descripción
Número de eventos (Cronograma)	El eje Y del gráfico, basado en miles de eventos.
Cronograma (Cronograma)	El eje X del gráfico, basado en la hora en que ocurrieron los eventos.
Punto de evento (Cronograma)	Si desea explorar una sección específica, seleccione simplemente el rango en el gráfico. El nuevo rango de tiempo se reflejará en el gráfico.
Investigar (Cronograma)	Muestra los valores de metadatos del subconjunto seleccionado.
Restablecer zoom (Cronograma)	Para volver al rango de tiempo original, haga clic en Restablecer zoom.
Opciones	Muestra el cuadro de diálogo Opciones de visualización. Los puntos de datos se pueden mostrar como un gráfico de líneas (predeterminado), un gráfico de barras o un gráfico de coordenadas. Cuando se selecciona un tipo de gráfico, se muestran las opciones pertinentes.
Ocultar	Contrae el gráfico.

Gráfico de coordenadas paralelas

El gráfico de coordenadas paralelas es una de las alternativas del menú Opciones para visualizar el punto de desglose actual. Si se selecciona Coordenadas en el cuadro de diálogo Opciones de visualización, puede elegir los metadatos que se mostrarán (consulte Visualizar metadatos como coordenadas paralelas).



Función	Descripción
Ejes	Cada eje es una clave de metadatos. La cantidad de claves de metadatos afecta el tiempo de carga del gráfico. Se cargan todas las claves de metadatos, pero la cantidad de eventos por clave de metadatos es limitada.
Líneas	Las líneas representan eventos y conectan valores en los ejes para mostrar la correlación entre varias claves de metadatos.
Opciones	Muestra el cuadro de diálogo Opciones de visualización. Los puntos de datos se pueden mostrar como un gráfico de líneas (predeterminado), un gráfico de barras o un gráfico de coordenadas. Cuando se selecciona un tipo de gráfico, se muestran las opciones pertinentes.
Solo se muestra un subconjunto de eventos.	Este mensaje es una notificación que indica que en el gráfico no se representan todos los eventos del panel Valores. La eliminación de ejes o el filtrado de los datos en el panel Valores pueden ayudar a mostrar todos los eventos.
Eventos encontrados | Rutas únicas	Muestra la cantidad total de eventos graficados en comparación con la cantidad de rutas únicas graficadas. La configuración de la opción Todas las claves de metadatos deben existir en un evento vuelve a generar el gráfico en una versión más concreta y legible.
DNE	Indica que no hay valores para esta clave de metadatos en el evento.

El cuadro de diálogo Opciones de visualización para Coordenadas permite seleccionar las claves de metadatos que se graficarán.

Función	Descripción
Selección de visualización	Muestra una lista desplegable de tipos de visualización: Cronograma y Coordenadas

Función	Descripción
Todas las claves de metadatos deben existir en un evento	Limita los datos representados en la visualización solo a aquellos eventos que incluyen todas las claves de metadatos seleccionadas. Esto puede dar lugar a una visualización más clara y concreta.
	Muestra el cuadro de diálogo Agregar claves a visualización de coordenadas paralelas, el cual permite agregar ejes a la visualización. Esto es útil si busca relaciones entre las claves de metadatos predeterminadas y otras adicionales.
	Elimina las claves seleccionadas de modo que no aparezcan como ejes en la visualización. Esto puede contribuir a que la visualización sea menos desordenada y permitir que incluya más puntos de datos.
	Revierte a las claves de metadatos predeterminadas para visualización, lo cual representa todas las claves de metadatos en el punto de desglose actual.
	Controla la presentación de información adicional sobre la cantidad de ejes seleccionados en comparación con el conteo recomendado. Esto contribuye a que tenga en cuenta posibles mejoras en el rendimiento debido a la eliminación de ejes.
Ejes	Enumera las claves de metadatos seleccionadas como ejes en la visualización.
Cancelar	Cancela los cambios hechos en las opciones de visualización.
Aplicar	Guarda los cambios hechos en las opciones de visualización y los aplica a la visualización actual.

En el cuadro de diálogo Agregar claves a visualización de coordenadas paralelas, puede seleccionar las claves de metadatos o los grupos de metadatos que se usarán como ejes en la visualización de coordenadas paralelas.

Función	Descripción
Selección de visualización	Seleccionar claves: Las dos opciones para seleccionar claves de metadatos son: • Desde claves de metadatos predeterminadas • Desde grupos de metadatos Cada opción ofrece una lista desplegable en la cual se hace una selección.
Con las claves de metadatos seleccionadas…	Las opciones del método de adición de claves de metadatos permiten: • Reemplazar la lista actual de claves • Agregar a la lista actual de claves • Insertar en el comienzo de la lista actual de claves
Cancelar	Cierra el cuadro de diálogo y no agrega ninguna clave.
Agregar	Cierra el cuadro de diálogo y agrega las claves seleccionadas según lo especificado.

Panel Valores

La función principal de la vista Navegar es el panel Valores, el cual se puede usar para analizar datos (consulte Filtrar resultados en la vista Navegar).

La vista predeterminada corresponde a las últimas tres horas de recopilación, con uso de las claves de metadatos predeterminadas y las claves de metadatos no indexadas cerradas. Las claves de metadatos dentro de los grupos de metadatos se muestran en el orden en que NetWitness Platform las consulta. A medida que los datos se cargan en el panel Valores, NetWitness Platform se optimiza para mostrar resultados parciales, el progreso de la carga y el estado de los servicios durante la carga de datos.

El comportamiento de la carga lo determinan varios ajustes de configuración. Los ajustes de nivel más alto los configura el administrador para cada usuario. Son los siguientes:

- La cantidad máxima de tiempo que se permite ejecutar una consulta a este usuario (Tiempo de espera agotado de consulta).
- El límite en el cual NetWitness Platform deja de contar la cantidad de valores de metadatos en una sesión (Umbral de sesión). Si se establece un umbral para una sesión, la vista Navegar muestra que el umbral se alcanzó y el porcentaje de resultados cargados. Cualquier sesión que no muestre un porcentaje es precisa y se procesó hasta que se completó. Si hay un porcentaje, este refleja la cantidad de procesamiento que se completó. El porcentaje que se muestra se calcula mediante la extrapolación del valor en el momento en que finaliza el procesamiento, lo cual considera la cantidad de trabajo restante. Los porcentajes mayores suelen ser más precisos, ya que requieren menos extrapolación.
- El límite en el cual NetWitness Platform deja de contar la cantidad de valores de metadatos en una sesión (Umbral de sesión). Si se establece un umbral para una sesión, la vista Navegar muestra que el umbral se alcanzó y el porcentaje del tiempo de consulta utilizado para alcanzarlo.

Nota: los valores de las claves de metadatos no indexadas tardan más en cargarse en el panel Valores. Para optimizar la carga, NetWitness Platform no abre las claves de metadatos no indexadas de manera predeterminada. Consulte Administrar y aplicar claves de metadatos predeterminadas en una investigación para obtener una descripción detallada de las claves de metadatos no indexadas en Investigation.

Cuando ha iniciado la investigación de un servicio, NetWitness Platform muestra los resultados en el panel Valores.

1. NetWitness Platform carga claves de metadatos y valores de metadatos en el panel Valores. Para cada carga de clave de metadatos, las etapas de carga son:
    a. **En espera de carga** o **Cerrado**. En el caso de Cerrado, no se cargan datos para esa clave.
    b. **Cargando**
        i. **Progreso de carga**: NetWitness Platform recibe y muestra mensajes de progreso.
        ii. **Resultados parciales**: NetWitness Platform recibe mensajes de valores y se muestran resultados parciales en el panel Valores.
    c. **Carga finalizada**: terminó la carga de todos los resultados.

2. A medida que termina la carga de cada clave de metadatos y que se muestran los valores finales, se inicia la clave de metadatos siguiente. El valor Hilos de ejecución de representación en la configuración Preferencias de Investigation especifica la cantidad o los valores que se generan para cada clave de metadatos. La carga continúa hasta que finalizan todas las claves que se cargarán.
3. Si la opción **Mostrar información de depuración** está activa y el servicio en el cual está navegando es un Broker 10.4 o superior, NetWitness Platform muestra la información del tiempo de carga debajo de los valores para cada clave de metadatos y muestra detalles de carga adicionales para los servicios agregados. NetWitness Platform también muestra la información de depuración debajo de la ruta de navegación.

Resultados iterativos

Los resultados iterativos proporcionan retroalimentación sobre el estado de consultas dentro de las interfaces para ofrecer contexto adicional en cuanto a la duración de la carga de datos y si faltan datos de servicios. Por ejemplo, si está consultando un Broker que realiza la agregación desde dos Concentrators, NetWitness Platform comienza a mostrar los resultados del primer Concentrator tan pronto están disponibles, incluso si el segundo Concentrator continúa en espera de resultados.

Los resultados iterativos también incluyen una notificación que informa que faltan datos del servicio porque no está accesible.

Resultados parciales

Cuando se devuelven valores parciales del servicio Core, sin que haya finalizado, un mensaje al final de la lista de claves de metadatos muestra el progreso de los valores cargados. Por ejemplo, Currently looking at 38 ip.src values 71% indica que la carga de valores para la clave de metadatos lleva un 71 %.

Información de depuración

Si el ajuste Mostrar información de depuración está activo, un campo al final de los valores muestra el estado de los diversos sistemas contra los cuales realiza la consulta dentro de NetWitness Platform. Por ejemplo, cuando realiza una consulta contra un Broker 10.4 que extrae datos de múltiples Concentrators, NetWitness Platform muestra el estado de la consulta en cada uno de los Concentrators, lo cual proporciona información sobre la velocidad relativa de carga de datos desde cada Concentrator. Cada servicio que participó en la consulta se muestra con el tiempo total transcurrido para la consulta.

Cada servicio que participó en la consulta se muestra con el tiempo total transcurrido para la consulta. En el ejemplo anterior, dos servicios devolvieron resultados en 3.207 segundos; localhost:50005 tardó dos segundos en devolver los resultados. Además, la cláusula Where de la consulta se muestra debajo de la ruta de navegación. Puede copiar esta sintaxis directamente en una regla de aplicación o en la cláusula Where de Reporting de una regla.

Carga finalizada

Para cada clave de metadatos, hay una lista de valores (texto azul) y conteos (texto verde) en el punto de desglose actual. Cuando hace clic en un valor para desglosar a un subconjunto de los datos seleccionados actualmente, la pantalla se actualiza y el nuevo punto de desglose se registra en la ruta de navegación. Puede especificar los métodos de clasificación y cuantificación de la lista de valores mediante la opción de la barra de herramientas.

Nota: el título, los valores y los conteos de claves de metadatos no indexadas no se pueden desglosar; los valores y los conteos se muestran en negro.

Función	Descripción
Clave de metadatos	El nombre de los metadatos que se enumeran; por ejemplo, **Tipo de servicio** es una clave de metadatos.
Cantidad de valores generados frente a cantidad de valores disponibles para cargar	El valor Hilos de ejecución de representación en la configuración Preferencias de Investigation especifica la cantidad o los valores que se generan. En el ejemplo anterior, la clave de metadatos es **Tipo de servicio** y se muestran 20 de más de 20 valores. Puede mostrar valores adicionales si hace clic en **...mostrar más**.
🔎	Si hace clic en 🔎 en una clave de metadatos indexada, se abre el cuadro de diálogo Buscar, en el cual puede ingresar un filtro para la clave de metadatos actual. La función de búsqueda no está disponible para claves de metadatos no indexadas y se basa en el valor de metadatos real, no en el alias. El desglose mediante alias en el cuadro de diálogo Buscar no es compatible. NOTA: Consulte al administrador para obtener una lista de los alias que se usan para una clave de metadatos en Investigation. Cuando se usa un alias, este cuadro de diálogo de búsqueda no proporciona resultados. En lugar de esto, debe consultar la clave de metadatos mediante la funcionalidad de consulta de clic con el botón secundario o el cuadro de diálogo Consulta.
Servicios offline: xxx.xxx.xxx.xxx:50004	Enumera los servicios offline que consulta un Broker 10.4.
Conteo de metadatos, por ejemplo (3)	La cantidad de instancias que se encuentran para un metadato específico en la sesión.
Valor de metadatos, por ejemplo other src	El nombre específico asociado con los metadatos encontrados.
...mostrar más	Si se limitó la cantidad de valores de metadatos (por ejemplo, 20) y se hace clic en esta opción, se muestran valores de metadatos adicionales para la clave de metadatos seleccionada.
Se cargó en 0.418 s Tiempo de ejecución total 0.434 s (localhost:50005 se cargó en 1 s…	Las estadísticas de depuración muestran los tiempos de carga de acuerdo con la configuración de Mostrar información de depuración.

Menús desplegables Clave de metadatos

Las claves de metadatos en el panel Valores tienen menús desplegables. Al lado de cada etiqueta de metadatos, una flecha desplegable muestra las opciones que se pueden aplicar a ese elemento. Puede usar esto para cambiar la manera en que se muestran los resultados de la clave de metadatos en la vista actual. Los cambios que se hacen en las claves de metadatos se muestran en la vista actual y persisten hasta que se actualiza la página o se selecciona un nuevo servicio en la barra de herramientas de la vista Navegar. Consulte Desglosar a datos en el panel Valores

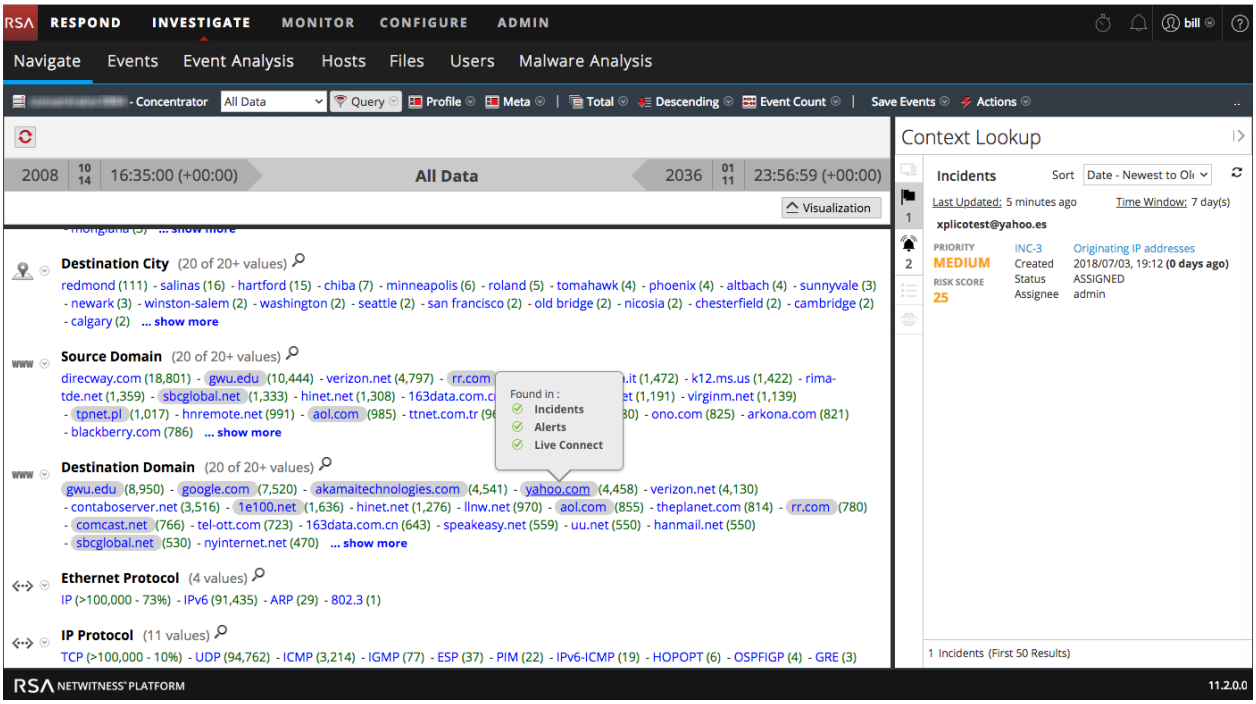
La actualización revierte a la vista actual de claves de metadatos según lo definido en el cuadro de diálogo Administrar claves de metadatos predeterminadas (consulte Administrar y aplicar claves de metadatos predeterminadas en una investigación). Si nunca ha hecho modificaciones en el cuadro de diálogo Administrar claves de metadatos predeterminadas, NetWitness Platform restaura las claves de metadatos predeterminadas desde el servicio principal.

- Más resultados
- Resultados máximos
- Ocultar resultados
- Información de clave de metadatos
- Ver como CSV (versión 11.0.0.x) o Exportar valores (versión 11.1 y superior)

Panel Búsqueda de contexto

Las vistas Navegar y Eventos tienen un panel Búsqueda de contexto en el lado derecho. El panel Búsqueda de contexto es visible solo si ha instalado el servicio Context Hub, el cual debe estar configurado. Para obtener más información sobre cómo configurar el servicio Context Hub, consulte la *Guía de configuración de Context Hub*.

En el panel Búsqueda de contexto se muestran los datos pertinentes cuando un analista busca datos contextuales para un valor de metadatos en el panel Valores.

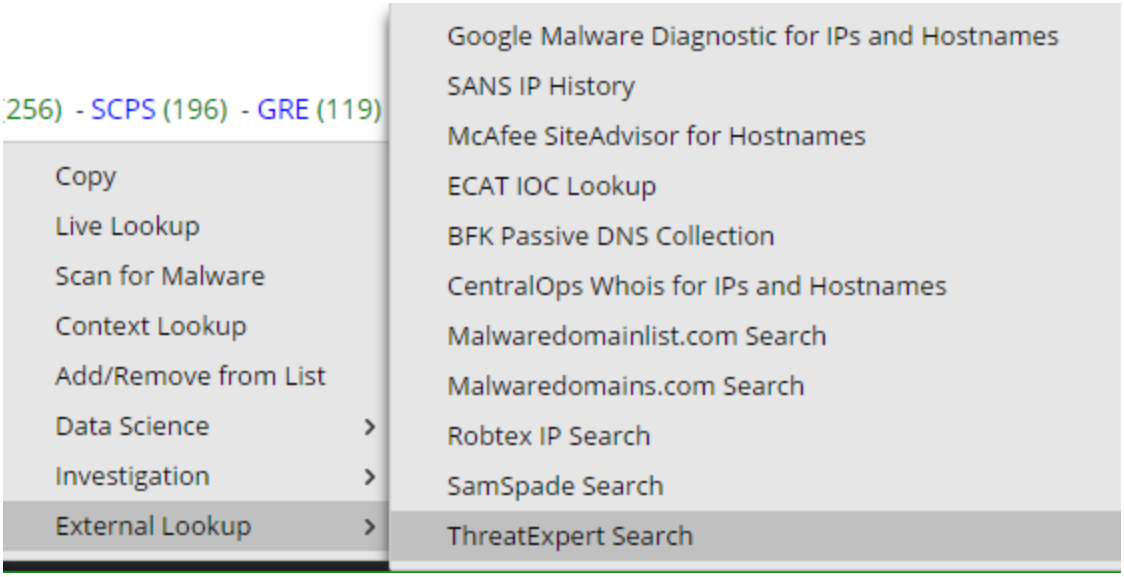


Después de que el administrador configura el servicio Context Hub, puede ver la información contextual para los valores de metadatos en la vista Navegar y en la vista Eventos. Para obtener más información sobre cómo configurar el servicio Context Hub, consulte la *Guía de configuración de Context Hub*. Para obtener información acerca de cómo realizar la búsqueda de contexto de valores de metadatos, consulte Buscar contexto adicional en las vistas Navegar y Eventos.

El servicio Context Hub está preconfigurado con un mapeo predeterminado de tipos de metadatos y claves de metadatos. Para obtener información sobre el mapeo del valor de metadatos de Context Hub con clave de metadatos de Investigation, consulte "Administrar el mapeo de tipos de metadatos y claves de metadatos" en la *Guía de configuración de Context Hub*.

Puede ver el tipo de datos de contexto que está disponible para un valor de metadatos resaltado si mantiene el mouse sobre un valor de metadatos resaltado. Un indicador de en línea muestra qué tipo de datos de contexto están disponibles para los metadatos: Endpoint, incidentes, alertas o listas.

Cuando se hace clic con el botón secundario en un valor de metadatos, se abre un menú con la opción de búsqueda de contexto. En la siguiente figura se muestra la opción Búsqueda de contexto cuando hace clic con el botón secundario en un valor de metadatos.



En el caso de las claves de metadatos, como IP, host y dirección MAC, los detalles de los valores que se marcan se recopilan de Endpoint, incidentes, alertas y listas.

En el caso de las claves de metadatos, como archivo, hash de archivo, dominio y usuario, los detalles de los valores que se marcan se recopilan de incidentes, alertas y listas.

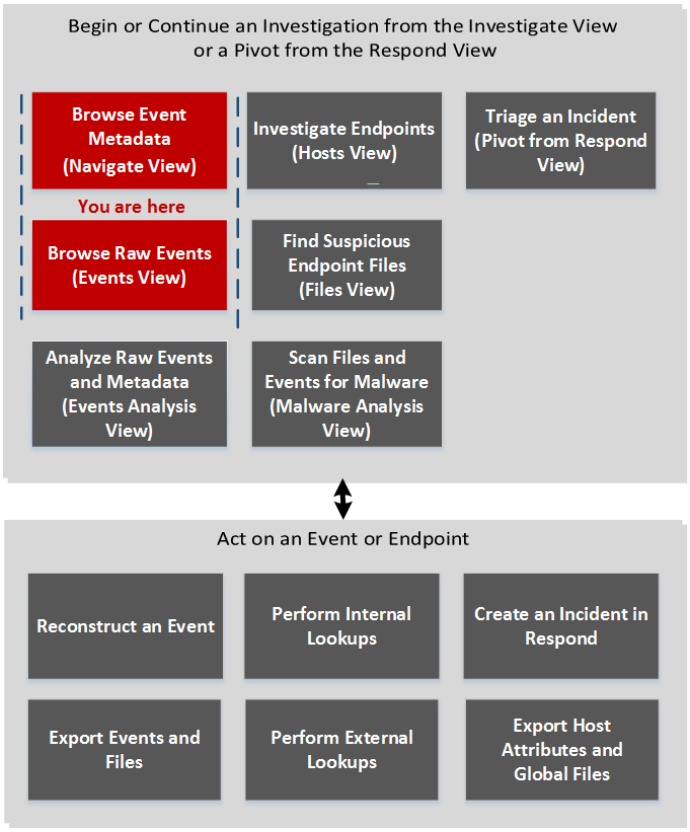
Los datos se muestran en el panel de contexto solo si están disponibles.

Para obtener más información sobre los resultados de búsqueda y la información contextual de distintos orígenes de datos, consulte Panel Búsqueda de contexto.

Cuadro de diálogo Consulta

En la vista Navegar o en la vista Eventos, puede crear una consulta en lugar de hacer clic en las claves y los valores de metadatos para desglosar a los metadatos. Los cuadros de diálogo para la creación de una consulta ofrecen ayuda de sintaxis con listas desplegables de las claves y los operadores de metadatos aplicables. Para acceder a este cuadro de diálogo, en la barra de herramientas de la vista **Navegar** o **Eventos**, seleccione **Consulta**.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos*	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos*	Comenzar una investigación en las vistas Navegar o Eventos

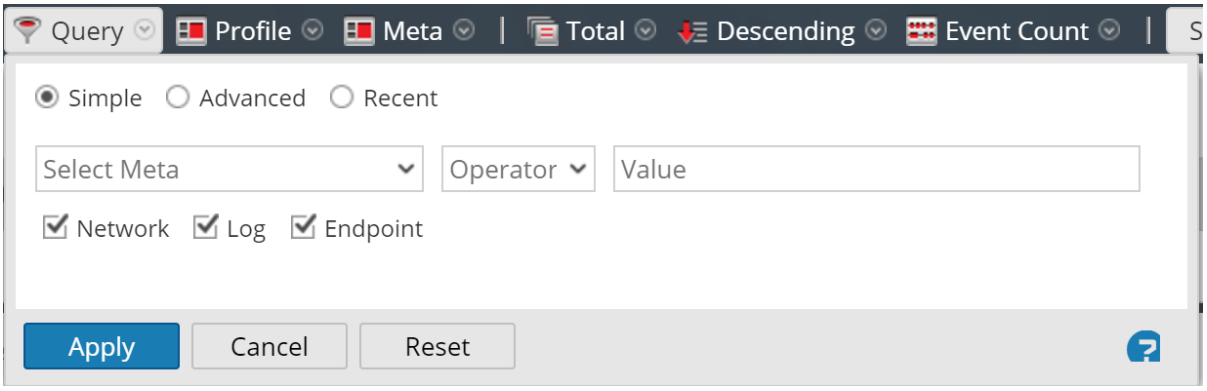
Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	crear una consulta personalizada*	Crear una consulta personalizada

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Vista Navegar
- Vista Eventos

Vista rápida



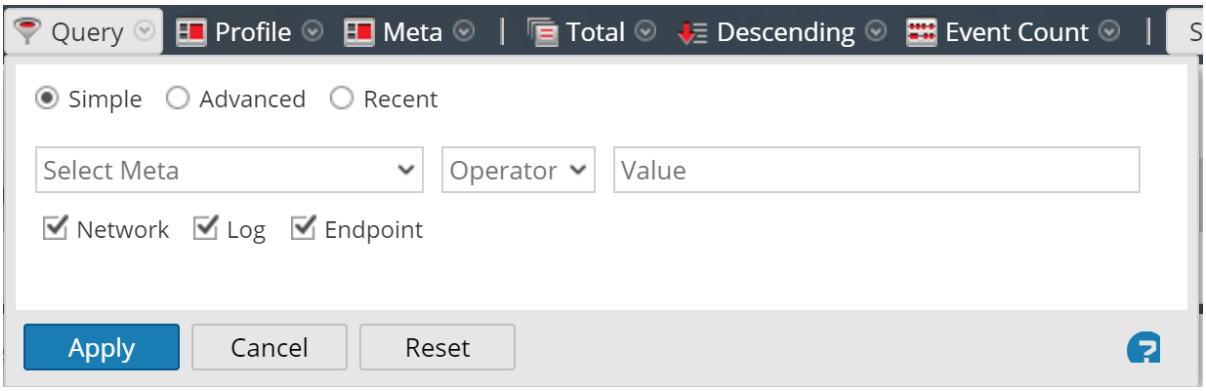
El cuadro de diálogo Consulta tiene tres vistas:

- Simple
- Avanzada

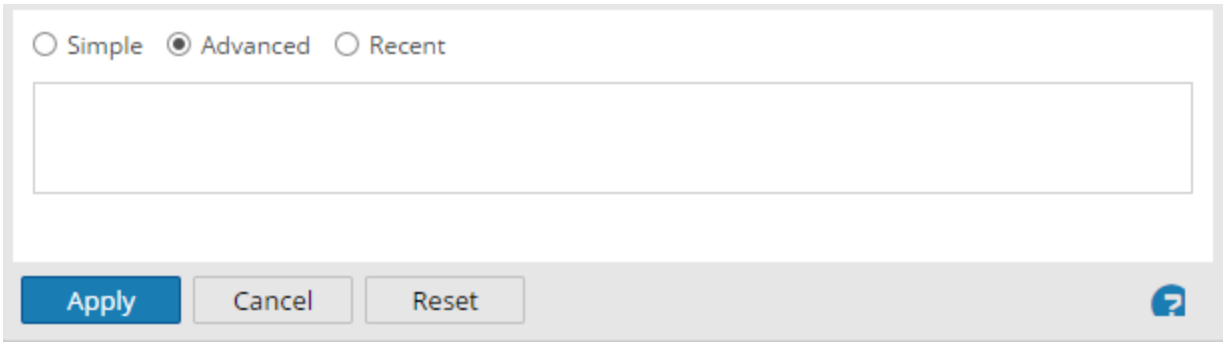
- Recientes

En la vista Simple, puede crear una consulta a partir de las opciones que se muestran en el cuadro de diálogo. En la vista Avanzada, puede crear una consulta sin orientación. En la vista Reciente, puede seleccionar una consulta en una lista desplegable de consultas recientes.

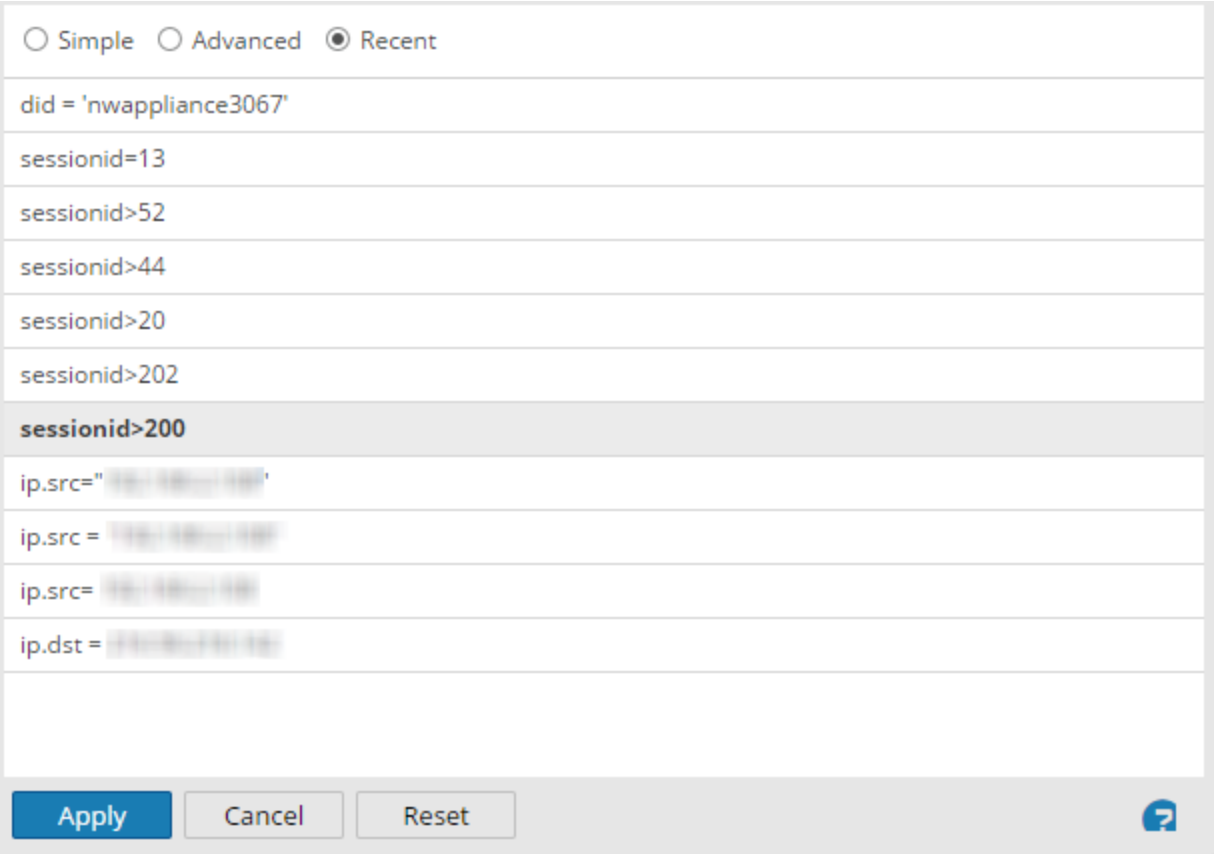
Vista Simple



Vista Avanzada



Vista Reciente



En la siguiente tabla se describen las funciones del cuadro de diálogo Consulta.

Función	Descripción
Seleccionar metadatos	Muestra una lista desplegable de grupos de metadatos.
Operador	Muestra una lista desplegable de operadores (=,NetWitness Platform!=,NetWitness Platformexists,NetWitness Platform!exists)
Valor	Permite ingresar un valor para completar la consulta.
Red	Limita la consulta a paquetes si no se selecciona la opción Registro.
Log	Limita la consulta a registros si no se selecciona la opción Red.
Cuadro Consulta	Permite ingresar una consulta en la vista Avanzada. Cuando comienza a escribir, se muestra una lista desplegable de claves de metadatos disponibles para el servicio y, a medida que escribe, se muestra una lista desplegable de operadores. Si la expresión ingresada actualmente en el cuadro Consulta no es válida, aparece una advertencia junto al cuadro. Cuando la consulta es válida, la advertencia se elimina.

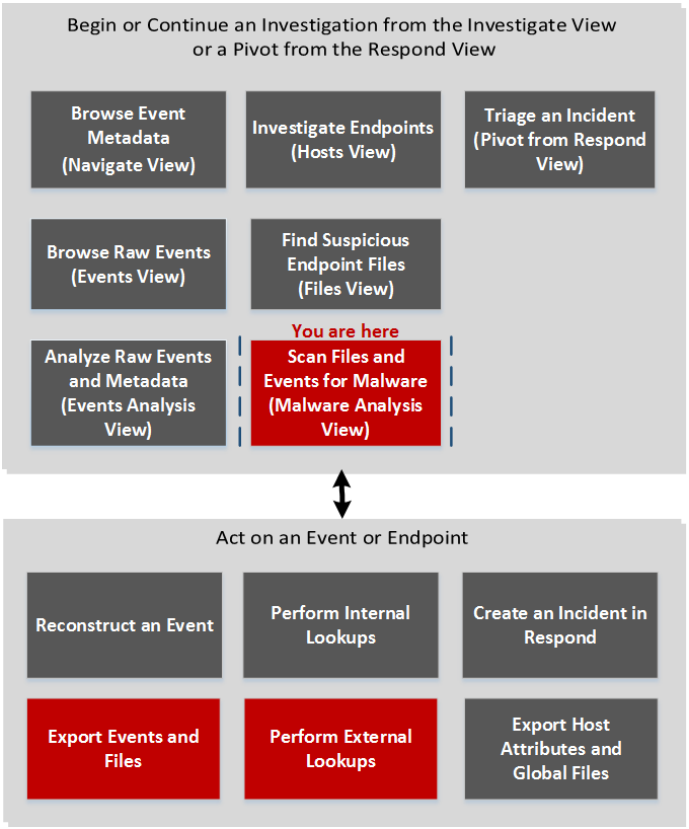
Función	Descripción
Lista Consulta	Permite seleccionar una consulta en una lista de consultas recientes de la vista Reciente. Si se hace doble clic en una consulta, esta se aplica automáticamente.
Aplicar	Aplica la nueva consulta a la vista actual de Investigation.
Cancelar	Cierra el cuadro de diálogo sin aplicar cambios.
Restablecer	Restablece todos los campos.

Cuadro de diálogo Escanear para encontrar malware

En el cuadro de diálogo Escanear para encontrar malware, los analistas de Malware Analysis pueden cargar archivos para investigar en Malware Analysis.

Para acceder a este cuadro de diálogo, vaya a la vista **Malware Analysis**. En el cuadro de diálogo **Seleccionar un servicio Malware Analysis**, seleccione un servicio en el panel de la izquierda y haga clic en Scan Files en el panel de la derecha.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos*	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*

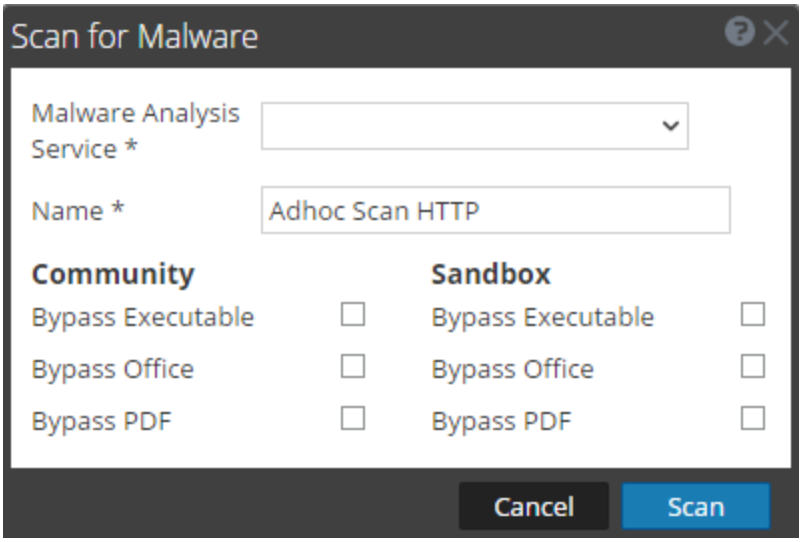
*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Comenzar una investigación de Malware Analysis
- Iniciar un escaneo de Malware Analysis desde la vista Navegar

Vista rápida

En la siguiente figura se ilustra el cuadro de diálogo Escanear para encontrar malware y en la siguiente tabla se describen las funciones disponibles en el cuadro de diálogo.

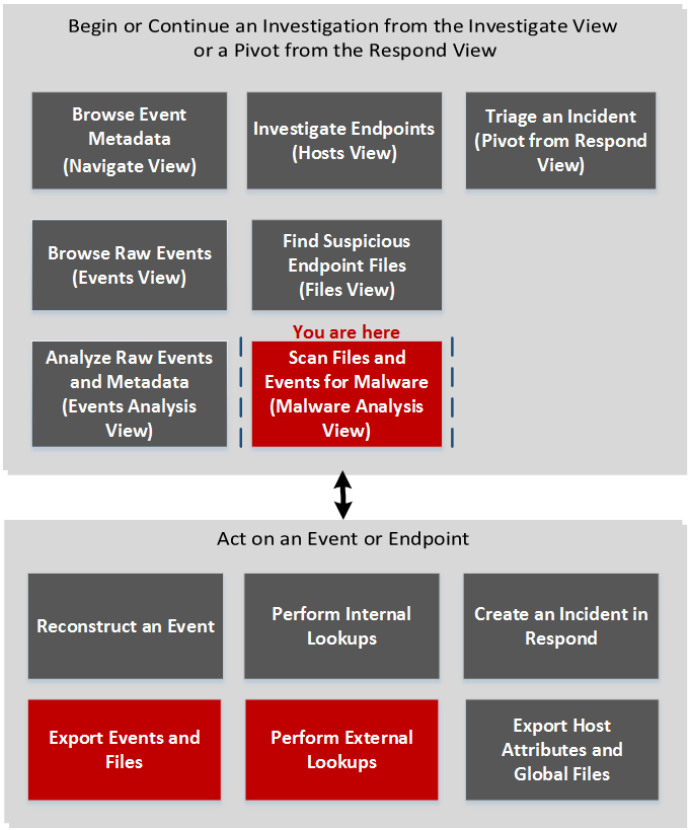


Función	Descripción
	Carga un archivo desde la computadora.
	Elimina un archivo de la lista.
Nombre de archivo	Muestra los nombres de los archivos agregados a la lista.
Nombre	Permite asignar un nombre al trabajo de escaneo.
Comunidad	Muestra opciones de Comunidad con el fin de saltar u omitir ciertos tipos de archivos: • Omitir archivo ejecutable • Omitir Office • Omitir PDF
Sandbox	Muestra opciones de Sandbox con el fin de saltar u omitir ciertos tipos de archivos: • Omitir archivo ejecutable • Omitir Office • Omitir PDF
Cancelar	Cierra el cuadro de diálogo sin realizar ninguna acción.
Analizar	Escanea los archivos cargados.

Cuadro de diálogo Seleccionar un servicio Malware Analysis

Se puede acceder al cuadro de diálogo Seleccionar un servicio Malware Analysis en la vista Malware Analysis. En este cuadro de diálogo, los analistas de Malware Analysis pueden seleccionar un servicio para investigar, elegir un escaneo en ese servicio, cargar un archivo para escanear e iniciar un escaneo continuo del servicio.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos

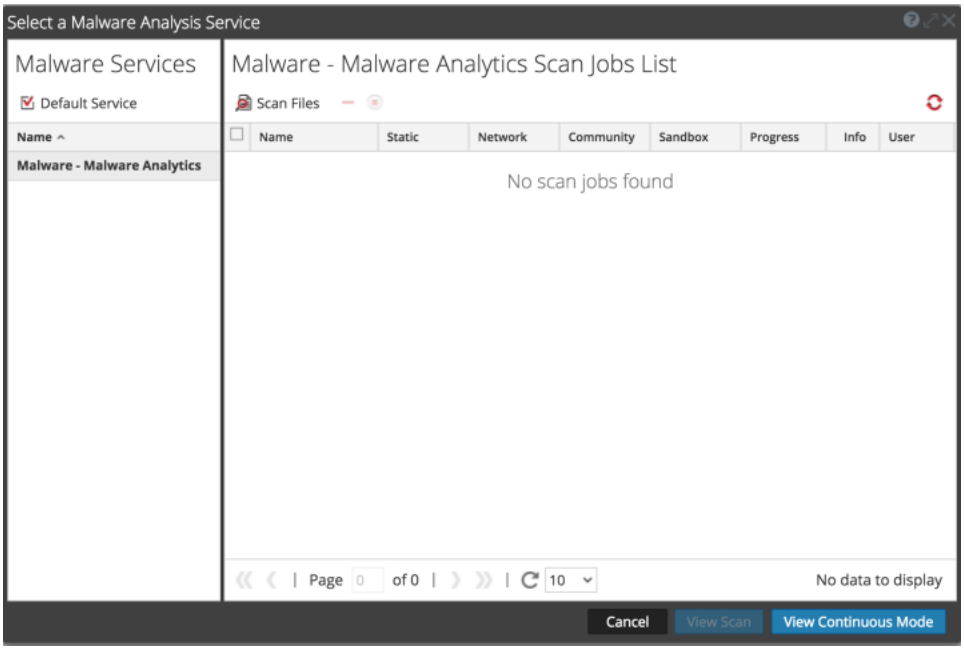
Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos*	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*

*Puede realizar esta tarea en la vista actual.

Temas relacionados

- Cómo funciona NetWitness Investigate
- Comenzar una investigación de Malware Analysis
- Iniciar un escaneo de Malware Analysis desde la vista Navegar

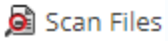
Vista rápida



El cuadro de diálogo Seleccionar un servicio Malware Analysis consta de un panel Servicios de malware en el lado izquierdo y de una Lista de trabajos de escaneo en el lado derecho. El panel Lista de trabajos de escaneo tiene una barra de herramientas, una lista y botones para ver escaneos.

El panel Servicios de malware es una lista de servicios disponibles para análisis de malware. En este panel, puede seleccionar el servicio que desea investigar y establecer un servicio predeterminado mediante el ícono Servicio predeterminado. Cuando selecciona un servicio, los trabajos de escaneo disponibles para ese servicio se muestran en la Lista de trabajos de escaneo.

Estas son las funciones de la barra de herramientas de Lista de trabajos de escaneo.

Función	Descripción
	Muestra el cuadro de diálogo Escanear para encontrar malware, en el cual puede cargar un archivo en el servicio para su escaneo.
Eliminar trabajo de escaneo ( )	Elimina una o más trabajos de escaneo seleccionadas, NetWitness Platform muestra un cuadro de diálogo de confirmación antes de eliminar los trabajos de escaneo.
Cancelar trabajo de escaneo ()	Pausa o continúa una o más trabajos de escaneo.
Actualizar ()	Actualiza la lista de trabajos de escaneo.

Estas son las columnas de la Lista de trabajos de escaneo. Esta lista también está disponible en el dashlet Trabajos de escaneo de malware.

Función	Descripción
Nombre	Muestra el nombre del trabajo.
Estático, Red, Comunidad y Sandbox	Filtra los resultados en función de los puntajes para cada módulo de puntaje.
Progreso	Muestra el progreso actual del trabajo. • Verde: El trabajo está finalizado. • Negro: El trabajo está en curso. • Rojo: Se produjo un error.
Información	Proporciona información adicional. Muestra la consulta del trabajo. Si el trabajo no está completo, también muestra una descripción más detallada del estado.
Usuario	Muestra el nombre del usuario que creó el trabajo.
Eventos	Realiza un conteo de la cantidad de eventos del trabajo.
Descartados	Realiza un conteo de la cantidad de archivos/eventos en el trabajo que se descartaron debido a que los puntajes estaban por debajo del umbral configurado.
Tipo de evento	Muestra el tipo de trabajo: Carga manual, Según demanda o Volver a enviar.
Programado	Muestra la fecha y hora en que se ejecutó el trabajo.

Estas son las acciones disponibles en el cuadro de diálogo.

Función	Descripción
Botón Cancelar	Cancela el trabajo de escaneo seleccionado.
Botón Ver escaneo	Muestra el Resumen de eventos del escaneo seleccionado con los dashlets predeterminados abiertos.
Botón Ver modo continuo	Muestra el Resumen de eventos del escaneo seleccionado con los dashlets predeterminados abiertos.

Cuadros de diálogo de configuración de las vistas de Investigate

NetWitness PlatformLa versión 11.0 tiene dos cuadros de diálogo de configuración, uno para la vista Navegar y otro para la vista Eventos. Con la adición del cuadro de diálogo de configuración para la vista Análisis de eventos en la versión 11.1, Investigate tiene tres cuadros de diálogo de configuración.

La configuración en los cuadros de diálogo Ajustes de configuración de las vistas Navegar y Eventos es un subconjunto de la configuración de Investigation que se establece en Perfiles > panel Preferencias > pestaña Investigaciones. Si la configuración se proporciona en la vista Investigation, NetWitness Platform permite ahorrar tiempo a los analistas. Si cambia una configuración aquí, la misma configuración se cambia en la vista Perfiles, y si cambia una configuración en la vista Perfiles, la misma configuración se cambia aquí.

Para acceder a este cuadro de diálogo, vaya a las vistas **Navegar** o **Eventos** y seleccione la opción **Ajustes de configuración** en la barra de herramientas.

La configuración en la vista Análisis de eventos no tiene ninguna configuración correspondiente en el panel Perfiles > Preferencias.

¿Qué desea hacer?

Función de usuario	Deseo…	Mostrarme cómo
Buscador de amenazas	navegar por metadatos de eventos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	navegar por eventos crudos	Comenzar una investigación en las vistas Navegar o Eventos
Buscador de amenazas	analizar eventos crudos y metadatos	Comenzar una investigación en la vista Análisis de eventos
Buscador de amenazas	investigar terminales (versión 11.1)	Investigar los hosts
Buscador de amenazas	buscar archivos sospechosos en terminales (versión 11.1)	Investigar los archivos
Buscador de amenazas	buscar malware en archivos y eventos	Realización de un análisis de malware
Encargado de respuesta ante incidentes	realizar triage a un incidente en Investigate	*Guía del usuario de NetWitness Respond*
Buscador de amenazas	configurar las preferencias de Investigate*	Configuración de vistas y preferencias de NetWitness Investigate

*Puede realizar esta tarea en la vista actual.

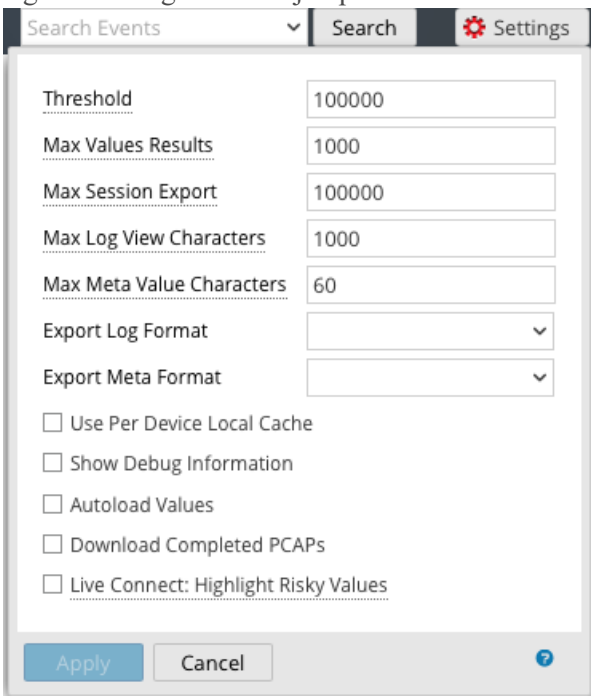
Temas relacionados

- Cómo funciona NetWitness Investigate

Vista rápida

Los cuadros de diálogo Ajustes de configuración de las vistas Navegar y Eventos tienen varias funciones en común.

Varios ajustes de Investigation en la vista Navegar influyen en el rendimiento cuando se realiza la carga de valores en el panel Valores. Los valores predeterminados se configuran en función del uso común, y los analistas individuales pueden ajustar estas configuraciones para sus propias investigaciones. La siguiente imagen es un ejemplo del cuadro de diálogo y en la siguiente tabla se describen las funciones.



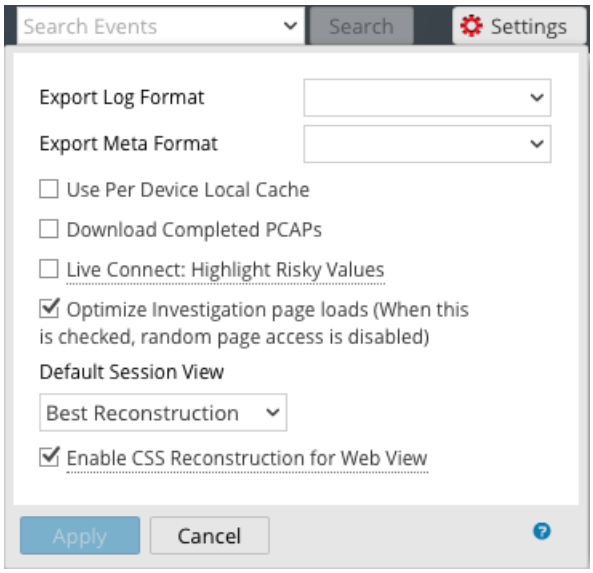
Función	Descripción
Umbral	Ajusta el umbral de la cantidad máxima de sesiones cargadas para un valor clave de metadatos en el panel Valores. Un umbral más alto permite conteos precisos de un valor y también produce tiempos de carga mayores. El valor predeterminado es **100000**.
Número máximo de resultados de valores	Ajusta la cantidad máxima de valores para cargar en la vista Navegar cuando la opción Resultados máximos está seleccionada en el menú Clave de metadatos para una Clave de metadatos abierta. El valor predeterminado es **1,000**.
Máximo de exportación de sesiones	Ajusta la cantidad máxima de sesiones que se pueden exportar. El valor predeterminado es **100000**.

Función	Descripción
Formato de registro de exportación	Ajusta el formato de archivo de los registros exportados. Hay cuatro formatos disponibles: • Texto • SML • CSV • JSON
Formato de metadatos de exportación	Ajusta el formato de archivo de los valores de metadatos exportados. Hay cuatro formatos disponibles: • Texto • SML • CSV • JSON
Uso por caché local de dispositivo	Cuando esta función está deseleccionada, Investigate envía una consulta nueva a la base de datos en lugar de mostrar los datos almacenados en caché en las vistas de Investigate después de la carga inicial. Si está seleccionada, Investigate utiliza los datos de la caché local.
Mostrar información de depuración	Esta opción controla la visualización de la cláusula `where` debajo de la ruta de navegación en la vista Navegar y el tiempo de carga transcurrido para cada servicio agregado en un Broker. Cuando está seleccionada, se muestra la información de depuración. El valor predeterminado es **Desactivado** (deseleccionada).
Agregar eventos en el panel de eventos	Esta opción afecta la paginación en el panel Eventos. Cuando está seleccionada, se agrega el siguiente grupo de eventos a los eventos que ya se muestran. Cuando está deseleccionada, la página de eventos siguiente reemplaza a la anterior. El valor predeterminado es **Desactivado** (deseleccionada).
Cargar valores automáticamente	Esta opción controla la carga automática de valores del servicio seleccionado en la vista Navegar. Si está seleccionada, los valores se cargan automáticamente cuando usted selecciona un servicio para investigar. Cuando no está seleccionada, Investigate muestra un botón **Cargar valores**, el cual da la oportunidad de modificar las opciones. El valor predeterminado es **Desactivado**.
Descargar PCAP finalizadas	Este ajuste automatiza la descarga de PCAP extraídas del módulo Investigation de modo que no sea necesario descargar ni abrir manualmente estos archivos en una aplicación que permite la visualización de datos en formato PCAP, como Wireshark.

Función	Descripción
Live Connect: Resaltar las IP riesgosas	Si esta opción está deseleccionada, todos los valores de metadatos que tienen contexto disponible en Live Connect se resaltan en el panel Valores de la vista Navegar. Si la opción está seleccionada, entre los valores que tienen contexto en Live Connect, solo se resaltan aquellos que la comunidad considera riesgosos/sospechosos/inseguros. De manera predeterminada, esta opción está deseleccionada (**Desactivado**).
Aplicar	La configuración se aplica de inmediato y estará visible la próxima vez que cargue valores. Los mismos cambios también se aplican en la vista Perfiles.
Cancelar	Cancela la operación de edición y cierra el cuadro de diálogo. La configuración permanece sin cambios.

Cuadro de diálogo Configuración de la vista Eventos

La siguiente imagen es un ejemplo del cuadro de diálogo Ajustes de configuración de la vista Eventos y en la siguiente tabla se describen las funciones.

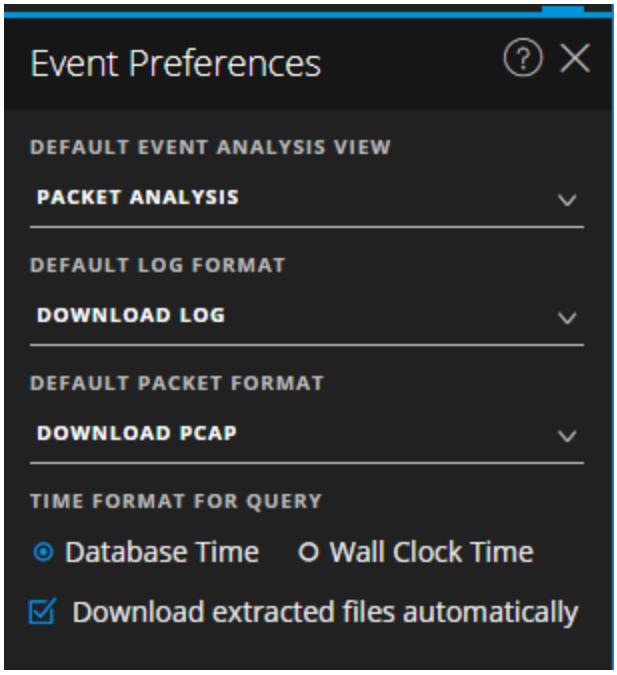


Función	Descripción
Formato de registro de exportación	Ajusta el formato de archivo de los registros exportados. Hay cuatro formatos disponibles: • Texto • SML • CSV • JSON

Función	Descripción
Formato de metadatos de exportación	Ajusta el formato de archivo de los valores de metadatos exportados. Hay cuatro formatos disponibles: • Texto • SML • CSV • JSON
Descargar PCAP finalizadas	Este ajuste automatiza la descarga de PCAP extraídas del módulo Investigation de modo que no sea necesario descargar ni abrir manualmente estos archivos en una aplicación que permite la visualización de datos en formato PCAP, como Wireshark.
Live Connect: Resaltar las IP riesgosas	Cuando esta función está seleccionada, Investigate usa un filtro para obtener solo las direcciones IP que la comunidad de RSA considera riesgosas. Cuando no está seleccionada, NetWitness Platform muestra todas las direcciones IP. De forma predeterminada, esta opción no está seleccionada (**Desactivado**).
Optimizar las cargas de páginas de Investigation	Establece una opción de paginación. Cuando está optimizada, los resultados se devuelven lo más rápidamente posible, pero se renuncia a la capacidad original de ir a una página específica de la lista de eventos. La deselección de esta casilla cambia la paginación en la lista de eventos y permite ir a una página específica de la lista (o a la última página). El valor predeterminado es **Habilitado**.
Vista de sesión predeterminada	Selecciona el tipo de reconstrucción predeterminado para la reconstrucción inicial en la vista Eventos. El valor predeterminado es **Mejor reconstrucción**, con el cual los eventos se reconstruyen mediante el método de reconstrucción más apropiado para el evento.
Activar reconstrucción de CSS para vista web	Esta configuración controla la forma en que se ejecuta la reconstrucción del contenido web. Si está habilitada, la reconstrucción web incluye imágenes y estilos de hoja de estilo en cascada (CSS), de modo que su aspecto coincide con la vista original en un navegador web. Esto incluye el escaneo y la reconstrucción de eventos relacionados y la búsqueda de hojas de estilo e imágenes que se usan en el evento objetivo. Esta opción está habilitada de manera predeterminada. Deseleccione esta opción si hay problemas para ver sitios web específicos.
Aplicar	La configuración se aplica de inmediato y estará visible la próxima vez que vea eventos. Los mismos cambios también se aplican en la vista Perfiles.
Cancelar	Cancela la operación de edición y cierra el cuadro de diálogo. La configuración permanece sin cambios.

Panel Preferencias de la vista Análisis de eventos

A partir de la versión 11.1, la vista Análisis de eventos incluye preferencias de usuario que se pueden configurar en la vista Análisis de eventos > panel Preferencias de eventos. Esta configuración persiste, de modo que se aplica cada vez que usted inicia sesión y se dirige a la vista Análisis de eventos. La siguiente figura es un ejemplo del cuadro de diálogo y en la siguiente tabla se describen las opciones.



Función	Descripción
Vista Análisis de eventos predeterminada	Selecciona la vista Análisis de eventos predeterminada que se muestra cada vez que usted abre la vista Análisis de eventos. Por ejemplo, si selecciona Análisis de archivos, el panel Análisis de archivos se resalta y se muestra cada vez que investiga un evento en la vista Análisis de eventos. Las opciones son las siguientes: • **Análisis de texto**: Vea y analice la carga útil del texto crudo de un evento. • **Análisis de paquetes**: Vea y analice de manera interactiva los paquetes y la carga útil de un evento. • **Análisis de archivos**: Vea una lista de archivos y descargue uno o más archivos de un evento.

Función	Descripción
Formato de registro predeterminado	Selecciona el formato predeterminado para descargar registros: • **Descargar registro**: Registro crudo (log) mediante esta opción. • **Descargar CSV**: Valores separados por comas (CSV) mediante esta opción. • **Descargar XML**: Lenguaje de marcado extensible (XML) mediante esta opción. • **Descargar JSON**: JavaScript Object Notation (JSON) mediante esta opción.
Formato de paquete predeterminado	Selecciona el formato de paquete predeterminado para descargar paquetes. • **Descargar PCAP**: Permite descargar el evento completo como un archivo de captura de paquetes (*.pcap). • **Descargar todas las cargas útiles**: Permite descargar la carga útil como un archivo *.payload. • **Descargar carga útil de la solicitud**: Permite descargar la carga útil de la solicitud como un archivo *.payload1. • **Descargar carga útil de la respuesta**: Permite descargar la carga útil de la respuesta como un archivo *.payload2.
Formato de hora para la consulta	La vista Análisis de eventos puede mostrar los resultados en función de la hora de la base de datos o la hora actual del reloj. La configuración predeterminada de esta preferencia es Hora de la base de datos, que es el mismo formato de hora que se usa para mostrar los resultados de consulta en las vistas Navegar y Eventos. Cuando se selecciona **Hora de la base de datos**, la hora de inicio y finalización de una consulta se basa en la hora en que se capturó el evento. Cuando se selecciona **Hora del reloj**, la consulta se ejecuta con una hora de finalización basada en la hora actual del navegador; la hora de inicio se calcula según esa hora de finalización y el rango de tiempo.
Descargar archivos extraídos automáticamente	Permite la descarga automática de archivos si están en el formato predeterminado seleccionado en los campos **Formato de registro predeterminado** y **Formato de paquete predeterminado** del panel Preferencias de eventos. Seleccione la casilla de verificación para habilitar la descarga automática del formato seleccionado a una carpeta local. De lo contrario, el trabajo de descarga se dirige a la línea de espera de trabajos y usted puede descargarlo manualmente.