RSA NETWITNESS® SUITE

Guía de introducción

para la versión 11.0

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 EMC, 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 EMC.

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

EMC 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 2018

Contenido

Introducción de NetWitness Suite

Descripción general

RSA NetWitness Suite es una suite eficaz de detección de amenazas que permite que los centros de operaciones de seguridad (SOC) realicen rápidamente tareas de localización, asignación de prioridades y triage de amenazas. NetWitness Suite lo ayuda a aislar y corregir las amenazas conocidas, así como aquellas que se desconocían. Proporciona información valiosa detallada de paquetes y registros que le brinda una vista sin igual de la empresa o el negocio.

NetWitness Suite es más eficaz que nunca, pero su uso es más sencillo para los analistas de nivel 1, ya que automatiza el proceso de identificar y dar prioridad a las amenazas sospechosas. Los usuarios de NetWitness Suite 10.6 pueden continuar buscando y localizando las amenazas de la misma manera que en el pasado mediante la vista Investigation que aún está disponible.

Arquitectura

RSA NetWitness Suite es un sistema distribuido y modular que permite arquitecturas de implementación altamente flexibles que escalan según las necesidades de la organización. Con NetWitness Suite, los administradores pueden recopilar dos tipos de datos desde la infraestructura de red, datos de paquetes y datos del registro. Si NetWitness Endpoint 4.4 esté instalado y configurado, también se recopilan datos de eventos de terminal. Los aspectos clave de la arquitectura son:

- **Recopilación de datos distribuidos**. El **Decoder** recopila datos de paquetes y el **Log Decoder**, datos del registro. Los Decoders analizan y reconstruyen todo el tráfico de red recopilado desde las capas 2 a la 7 o los datos de registros y eventos de cientos de dispositivos y orígenes de eventos, incluidos los datos de NetWitness Endpoint (si está instalado y configurado). **Concentrator** indexa metadatos extraídos de los datos de red o de registros y los pone a disposición para la analítica en tiempo real y la creación de consultas de toda la empresa, a la vez que facilita la creación de informes y alertas. **Broker** agrega datos que capturan otros dispositivos y orígenes de eventos. Los Brokers agregan datos de Concentrators configurados; los Concentrators agregan datos de Decoders. Por lo tanto, un Broker conecta las distintas áreas de almacenamiento de datos en tiempo real ubicadas en varios pares de Decoder/Concentrator a lo largo de la infraestructura.
- **Alertas en tiempo real**. El servicio NetWitness Suite **Event Stream Analysis (ESA)** proporciona analítica de flujo avanzada, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators. ESA utiliza un lenguaje de procesamiento de eventos (EPL) avanzado que permite a los analistas expresar filtrado, agregación,

combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. Event Stream Analysis ayuda a realizar detección de incidentes y alertas eficaces.

- **Analítica en tiempo real** (análisis automático de eventos). La funcionalidad Detección de amenazas automatizadas de RSA incluye módulos ESA Analytics preconfigurados para detectar el tráfico de comando y control.
- **Servidor de NetWitness**. En el Servidor de NetWitness se proporciona Reporting, Investigation, Administration y otros aspectos de la interfaz del usuario.
- **Capacidad**. NetWitness Suite cuenta con una arquitectura de capacidad modular, habilitada con capacidad de conexión directa (DAC) o redes de almacenamiento SAN, que se adapta a las necesidades de investigación a corto plazo y de retención de datos y analítica a más largo plazo.

NetWitness Suite ofrece gran flexibilidad de implementación. En el diseño de su arquitectura, puede usar varias docenas de hosts físicos o un único host físico en función de los detalles específicos de los requisitos de rendimiento y seguridad del cliente. Además, todo el sistema NetWitness Suite se optimizó para su ejecución en una infraestructura virtualizada.

La arquitectura del sistema incluye estos componentes principales: Decoders, Brokers, Concentrators, Archivers, ESA y Warehouse Connectors. Los componentes de NetWitness Suite se pueden utilizar en conjunto como un sistema o de manera individual.

- En una implementación de información de seguridad y administración de eventos (SIEM), la configuración básica requiere estos componentes: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA) y el Servidor de NetWitness.
- En una implementación de análisis forense, la configuración básica requiere estos componentes: Decoder, Concentrator, Broker, ESA y Malware Analysis. El servicio del servidor de Respond también se requiere y se utiliza para dar prioridad a las alertas.

La tabla proporciona una sinopsis de cada componente principal:

Componente del sistema	Descripción
Decoder/Log Decoder	• NetWitness Suite recopila dos tipos de datos: datos de paquetes y datos del registro. • Los datos de paquetes, es decir, paquetes de red, se recopilan mediante Decoder a través del puerto TAP o SPAN de la red, el cual normalmente se determina que es un punto de salida en la red de una organización. • Un Log Decoder puede recopilar cuatro tipos de registro diferentes: syslog, ODBC, eventos de Windows y archivos planos. • Eventos de Windows se refiere a la metodología de recopilación de Windows 2008 y los archivos planos puede obtenerse a través de SFTP. • Ambos tipos de Decoders recopilan datos transaccionales crudos que se enriquecen, cierran y agregan a otros componentes de NetWitness Suite. • El proceso de recopilación y análisis de datos transaccionales es una plataforma dinámica y abierta.
Concentrator	• Proporciona la funcionalidad de índice y consulta para las recopilaciones de NetWitness. • Opcionalmente, puede enviar datos a ESA.
Broker	• Distribuye el acceso a la recopilación de NetWitness en muchos Concentrators o Archivers, lo que hace que la empresa de NetWitness Suite completa aparezca como una única recopilación.
Archiver	• El servicio Archiver permite el archiving de registros a largo plazo mediante la indexación y la compresión de datos del registro y su envío a almacenamiento para archiving. • El almacenamiento de archiving se optimiza para la retención de datos a largo plazo y los informes de cumplimiento de normas. • Archiver almacena registros crudos y metadatos de registros de Log Decoders para la retención a largo plazo y utiliza capacidad de conexión directa (DAC) para el almacenamiento. **Nota:** Los paquetes crudos y los metadatos de paquetes no se almacenan en el Archiver.

Componente del sistema	Descripción
Event Stream Analysis (ESA)	• El servicio Event Stream Analysis proporciona analítica de flujo de eventos, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators. • ESA utiliza un lenguaje de procesamiento de eventos avanzado que permite a los usuarios expresar filtrado, agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. • ESA ayuda a ejecutar detección de incidentes y alertas eficaces. • La funcionalidad Detección de amenazas automatizadas de RSA incluye módulos ESA Analytics preconfigurados para detectar el tráfico de comando y control.

Componentes principales frente a descendentes

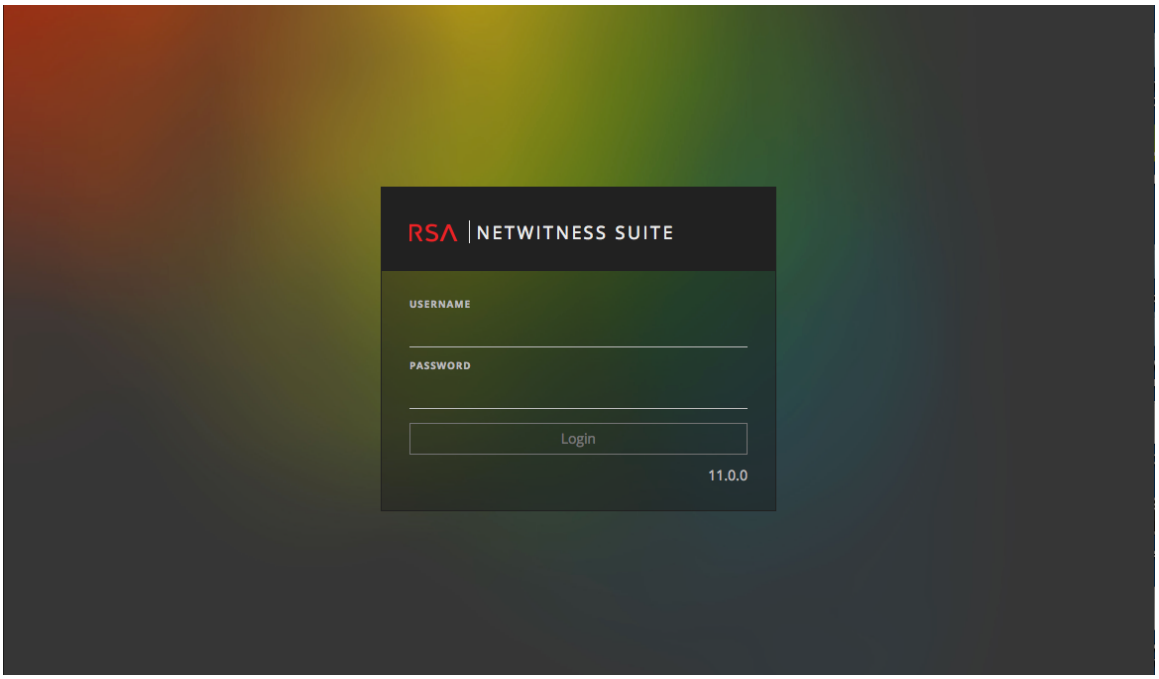
En NetWitness Suite, los servicios principales recopilan y analizan datos, generan metadatos y agregan los metadatos generados con los datos crudos. Entre los servicios Core se incluyen Decoder, Log Decoder, Concentrator y Broker. Los sistemas descendentes usan los datos almacenados en los servicios principales para analítica. Por lo tanto, las operaciones de los servicios descendentes dependen de los servicios principales. Los sistemas descendentes son Archiver, ESA, Malware Analysis, Investigate y Reporting.

Aunque los servicios principales pueden funcionar y proporcionar una buena solución de analítica sin los sistemas descendentes, los componentes descendentes ofrecen funciones de analítica adicionales. ESA proporciona correlación en tiempo real entre sesiones y eventos, y también entre distintos tipos de eventos, como datos de paquetes y registros. Investigate brinda la capacidad de desglosar a datos, examinar eventos y archivos, y reconstruir eventos en un ambiente seguro. El servicio de Malware Analysis ofrece inspección automatizada en tiempo real de actividad maliciosa en sesiones de red y archivos asociados.

Inicio de sesión en NetWitness Suite

El inicio de sesión en NetWitness Suite puede variar en función del ambiente. Puede tener una cuenta de usuario interna o una cuenta de usuario externa. Las cuentas de usuario internas son locales para NetWitness Suite y los usuarios internos pueden iniciar sesión en NetWitness Suite y recibir permisos basados en función. Las cuentas de usuario externas se autentican fuera de NetWitness Suite y se mapean a funciones de NetWitness Suite. Si es un usuario externo y no puede acceder a NetWitness Suite ni ver la información que necesita, póngase en contacto con el administrador del sistema. El administrador puede asignar las funciones apropiadas a su cuenta.

1. Use un ícono que proporcionó el administrador o escriba lo siguiente en el navegador web:
   `https://<hostname or IP address>/login`
   Donde `<hostname or IP address>` es la dirección IP o el nombre de host del servidor de NetWitness.
   Se muestra la pantalla de inicio de sesión de



   .

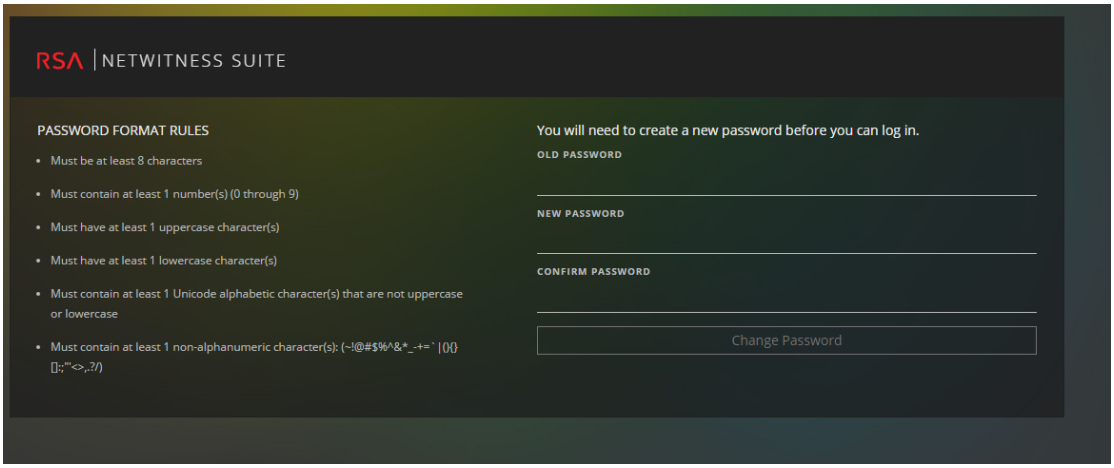
2. Escriba el nombre de usuario y la contraseña, y haga clic en **Inicio de sesión**.
   Si el inicio de sesión se realiza correctamente, iniciará sesión en la página principal especificada en las preferencias de usuario.

Si la cuenta está bloqueada:

Si hace demasiados intentos de inicio de sesión con un nombre de usuario o una contraseña incorrectos, la cuenta se bloqueará. Póngase en contacto con el administrador para que desbloquee la cuenta.

Si tiene una cuenta nueva o la cuenta venció:

1. En el cuadro de diálogo para crear una contraseña nueva, ingrese la contraseña anterior, escriba una contraseña nueva y confírmela. Las reglas de formato de contraseña (según lo define el administrador del sistema) se proporcionan a la izquierda y la contraseña nueva debe cumplir con las reglas de formato indicadas.



2. Haga clic en **Cambiar contraseña**.

Si no dispone del acceso apropiado a NetWitness Suite:

Si puede iniciar sesión correctamente, pero no puede ver la información que necesita, es posible que requiera que se asigne una función de usuario a su cuenta de usuario. Póngase en contacto con el administrador para obtener ayuda.

Cerrar sesión en NetWitness Suite

Para cerrar la sesión en la vista Respond:

1. En la barra menú principal, seleccione  .
2. En Preferencias de usuario, haga clic en **Cerrar sesión**.

Para cerrar la sesión en todas las demás vistas:

En la barra del menú principal, seleccione  **> Cerrar sesión**.

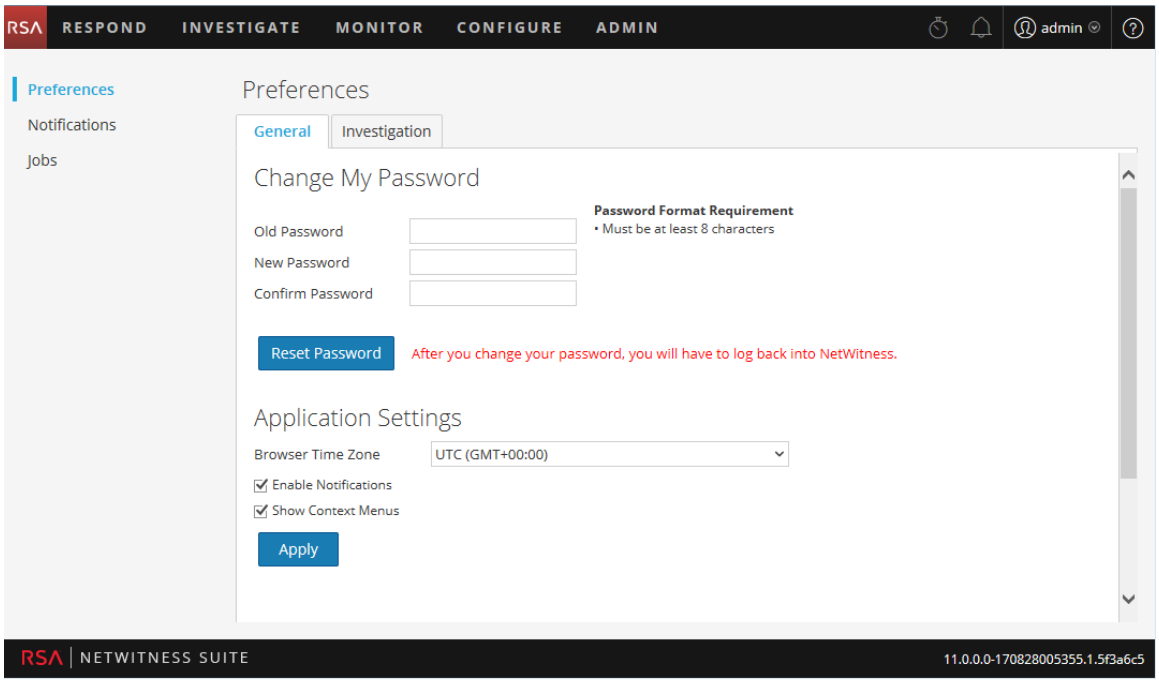
Cambio de la contraseña

Puede cambiar en cualquier momento la contraseña que utiliza para autenticarse en NetWitness Suite en las preferencias de usuario. El administrador define los requisitos apropiados de seguridad de la contraseña para su contraseña de NetWitness Suite, como la longitud mínima de la contraseña y la cantidad mínima de caracteres en mayúscula, en minúscula, decimales, alfabéticos no latinos y especiales. A continuación, estos requisitos se muestran cuando se cambia la contraseña.

Nota: Cuando un servicio principal usa una conexión de confianza, usted no ingresa una contraseña, de modo que no se requiere una actualización de las cuentas de los servicios principales.

Para cambiar la contraseña de :

1. Realice una de las siguientes acciones:
   - Para la mayoría de las vistas, como Investigate, Monitor, Configurar o Admin, seleccione > **Perfil**.
   - En la vista Respond, seleccione y, en el cuadro de diálogo Preferencias de usuario, haga clic en **Cambiar mi contraseña**.



2. En la sección **Cambiar mi contraseña**, ingrese la contraseña que usó para autenticarse en NetWitness Suite en el campo **Contraseña anterior**.
3. En el campo **Nueva contraseña**, ingrese la contraseña que desea usar para el siguiente

inicio de sesión.

4. En el campo **Confirmar contraseña**, vuelva a escribir la nueva contraseña.
5. Haga clic en **Restablecer contraseña**.
   Se cerrará su sesión de NetWitness Suite para que se apliquen los cambios. La contraseña nueva entra en vigor la próxima vez en que inicia sesión en NetWitness Suite.

Identificar su función

Las funciones que se muestran aquí son las funciones típicas de un centro de operaciones de seguridad (SOC). Determine la función o las funciones que desempeña en el SOC. Puede usar estas funciones como guía para decidir cómo configurar y navegar en NetWitness Suite, de modo que pueda realizar las tareas de su trabajo con eficiencia.

SOC Team

SOC Manager
(SOC Management and Reporting)

- Administrar la preparación del SOC
- Responder a incidentes
- Responder a las vulneraciones de datos

Data Privacy Officer

Monitorear y proteger información de privacidad y confidencial

Incident Reponder
(T1 Analyst)

- Responder a incidentes
- Corregir incidentes

Threat Hunter
(T2/T3 Analyst)

- Buscar amenazas
- Realizar análisis forense
- Señalar problemas que requieren corrección
- Corregir problemas

Content Expert
(Threat Intelligence)

- Investigar la inteligencia de amenazas nueva
- Evaluar y crear nuevos feeds
- Crear reglas de correlación para marcar los indicadores de riesgo

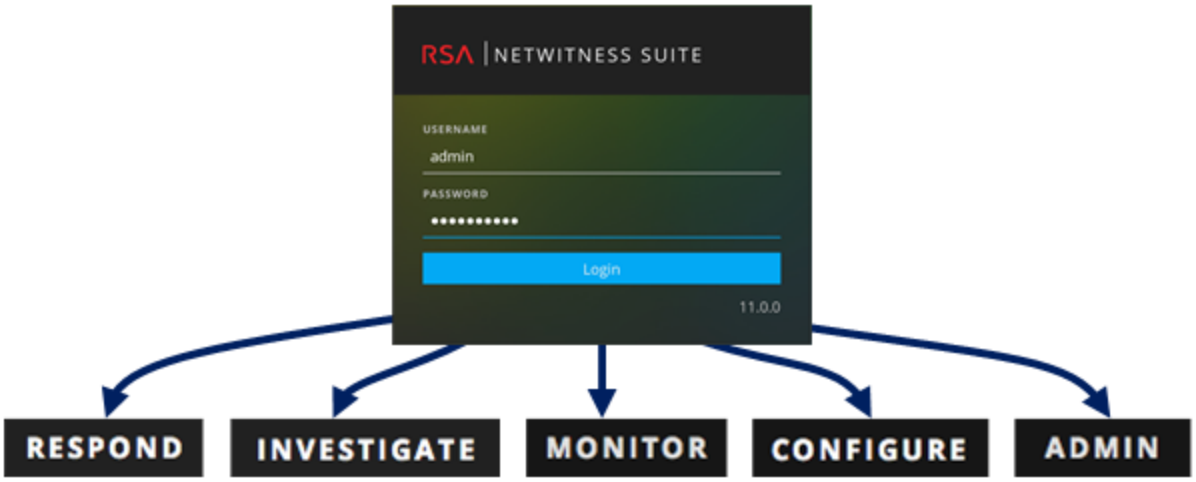
System Administrator

- Instalar y configurar software y equipos.
- Administrar el acceso de los usuarios
- Monitorear y ajustar el rendimiento
- Respaldar y restaurar datos
- Administrar el almacenamiento y los archivos
- Actualizar el software

- Crear informes para el cumplimiento de normas

Navegación básica en NetWitness Suite

La aplicación NetWitness Suite se divide en cinco áreas funcionales principales, conocidas como vistas, que se basan en las funciones típicas del centro de operaciones de seguridad (SOC).



- **RESPOND**: Esta vista es para los encargados de respuesta ante incidentes, quienes pueden ver una lista de incidentes ordenados por prioridad para la realización de tareas de triage. Estos incidentes provienen de orígenes, como reglas de ESA, NetWitness Endpoint o módulos de ESA Analytics para Detección de amenazas automatizadas. Aquí también se pueden ver todas las alertas que recibe NetWitness Suite.
  Para los usuarios existentes de 10.6, esta vista se conocía como la vista Administración de incidentes. La Lista de alertas en la vista Respond reemplaza a la vista Alertas > Resumen en ESA 10.6.
- **INVESTIGATE**: Esta vista es principalmente para los buscadores de amenazas avanzadas, quienes prefieren buscar amenazas manualmente mediante metadatos, análisis de eventos y reconstrucción de eventos de NetWitness Suite. Los encargados de respuesta ante incidentes también usan esta vista para obtener detalles acerca de los eventos asociados a un incidente que se investiga. Tanto los buscadores de amenazas como los encargados de respuesta ante incidentes pueden usar las funciones de análisis forense de reconstrucción y análisis de eventos en esta vista.
- **MONITOR**: Esta vista es para todos los usuarios. Puede ver tableros e informes en diferentes áreas de interés según los permisos de usuario. NetWitness Suite se abre en esta vista de manera predeterminada.
  Para los usuarios existentes de 10.6, esta es la vista Tablero.

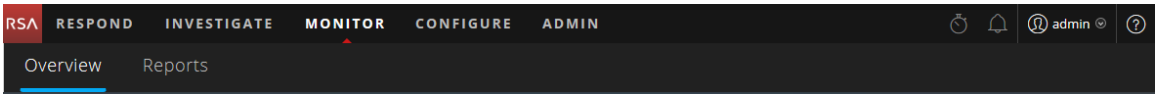
- **CONFIGURAR**: Esta vista es para el personal de inteligencia de amenazas (contenido), el cual configura orígenes de datos y entradas en NetWitness Suite. El personal de inteligencia de amenazas usa esta área para descargar y administrar contenido de Live. También puede crear y administrar reglas de incidentes y de ESA.
  Para los usuarios existentes de 10.6, esta vista contiene Live, Incidentes > Configurar y Alertas > Configurar de la versión anterior.
- **ADMIN**: Esta vista es para los administradores del sistema, quienes configuran y mantienen la aplicación en general.
  Para los usuarios existentes de 10.6, esta es la vista Administration, excepto por las secciones que se agregaron a la vista Configurar.

Acceso a las vistas principales

Las opciones que abren cada una de las vistas principales se enumeran en la parte superior de la ventana del navegador. Con los permisos adecuados, puede acceder a cualquiera de estas vistas en la parte superior de cada ventana del navegador en cualquier momento.

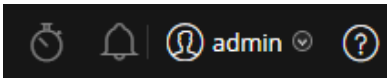
Menús secundarios

Algunas vistas tienen menús secundarios con vistas adicionales que puede seleccionar, las cuales varían según las tareas que puede realizar. En el siguiente ejemplo se muestra el menú MONITOR.

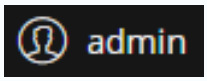
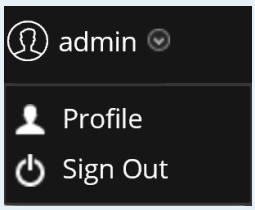


Opciones adicionales

Además de las vistas principales, existen opciones adicionales en la parte superior de la ventana del navegador que son comunes a toda la aplicación.



En la siguiente tabla se describen estas opciones comunes:

Opción común	Nombre	Descripción
	Trabajos	En las vistas INVESTIGATE, MONITOR, CONFIGURAR y ADMIN, haga clic en este ícono para ver y administrar los trabajos en la bandeja Trabajos. Los trabajos son tareas según demanda o programadas que tardan un tiempo en completarse en la aplicación NetWitness Suite.
	Notificaciones	Haga clic en este ícono para ver las notificaciones de la aplicación.
	Preferencias de usuario	Haga clic en este ícono para ver las opciones de preferencias de usuario disponibles. Puede administrar las preferencias de usuario y cerrar la sesión de NetWitness Suite.
	Perfil de usuario	Haga clic en su perfil de usuario para ver las opciones disponibles. Puede administrar las preferencias de usuario, cambiar la contraseña y cerrar la sesión de NetWitness Suite.

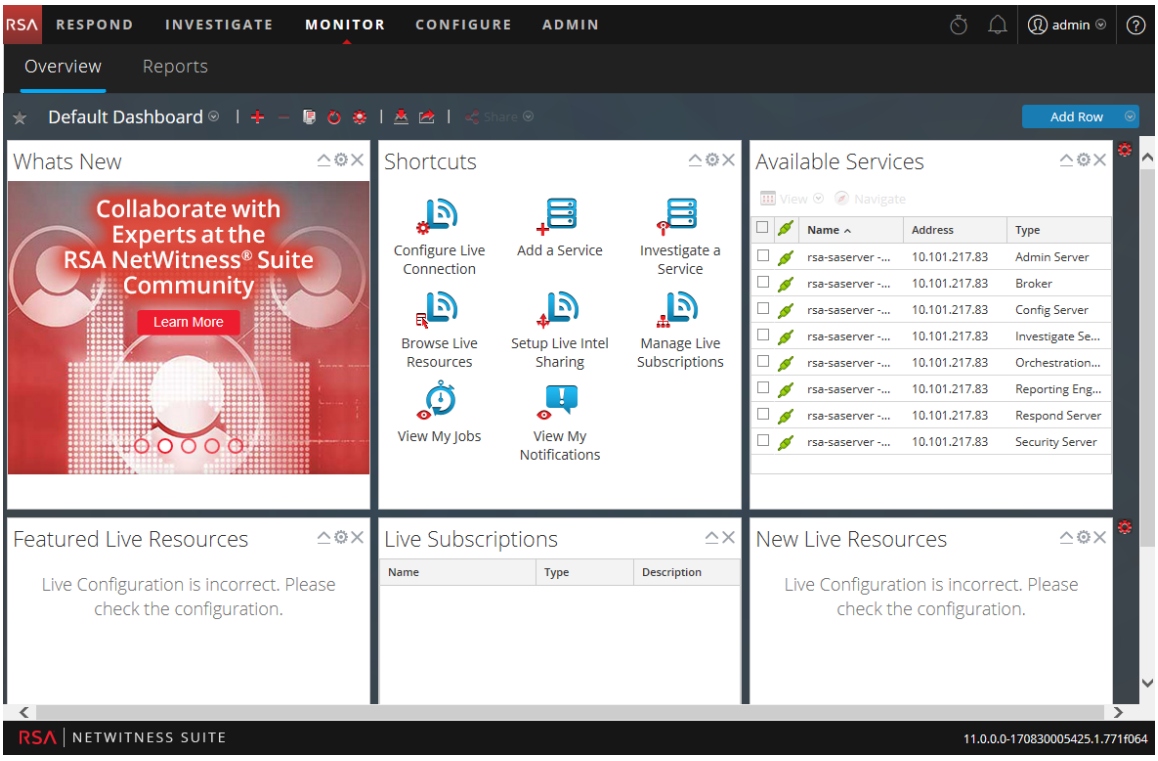
Opción común	Nombre	Descripción
	Ayuda	Haga clic en este ícono para ver los temas de ayuda de NetWitness Suite.

Vistas principales

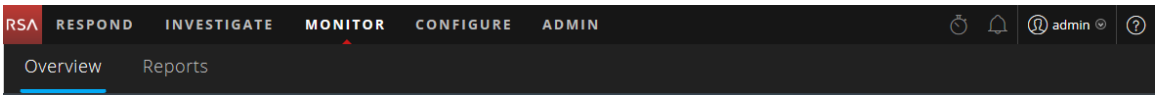
En las siguientes secciones se explican las vistas principales.

MONITOR

La vista MONITOR es el tablero clásico de NetWitness Suite. Monitor ofrece tableros e informes preconfigurados que usted puede usar, aunque también puede crear tableros e informes propios.



Menú de MONITOR



El menú MONITOR tiene las siguientes opciones:

- **Descripción general**: La vista Descripción general permite ver y administrar sus tableros. Puede seleccionar los siguientes tableros preconfigurados:
  - Valor predeterminado
  - Identidad
  - Investigation
  - Operaciones: Análisis de archivos
  - Operaciones: Registros
  - Operaciones: Red
  - Operaciones: Análisis de protocolos
  - Descripción general
  - RSA SecurID
  - Amenaza: Localización
  - Amenaza: Intrusión
  - Amenaza: Indicadores de malware

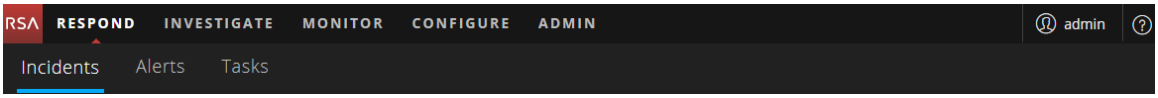
  Para los usuarios existentes de 10.6, esta era la vista Tablero.
- **Informes**: La vista Informes permite ver y administrar informes pertinentes a su función del SOC de acuerdo con sus permisos asignados.

¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Seleccionar un tablero	MONITOR > Descripción general	Consulte Configuración de un tablero.
Crear un tablero	MONITOR > Descripción general	Consulte Configuración de un tablero.
Administrar tableros	MONITOR > Descripción general	Consulte Configuración de un tablero.
Ver un informe	MONITOR > Informes > Ver	Consulte *Guía de Reporting*.
Administrar informes	MONITOR > Informes > Administrar	Consulte *Guía de Reporting*.

RESPOND

La vista Respond presenta a los analistas una línea de espera de incidentes en orden de gravedad. Cuando selecciona un incidente en la línea de espera, usted recibe los datos de soporte pertinentes que lo ayudarán a investigarlo. Desde ahí, puede determinar el alcance del incidente y elevarlo o corregirlo según corresponda.

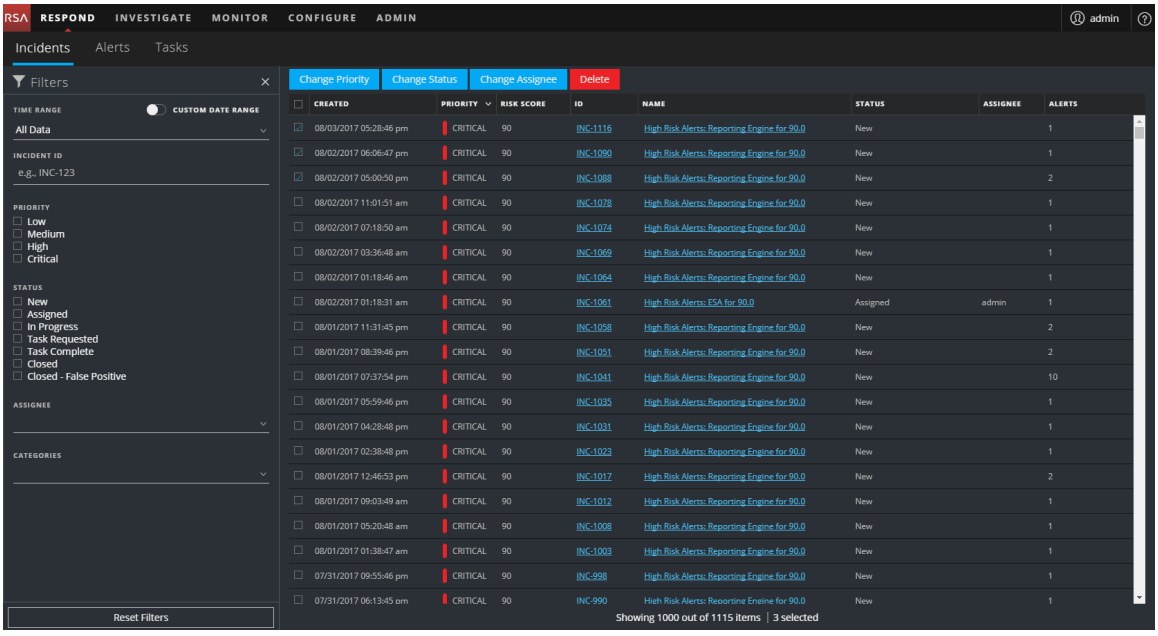
Menú de RESPOND



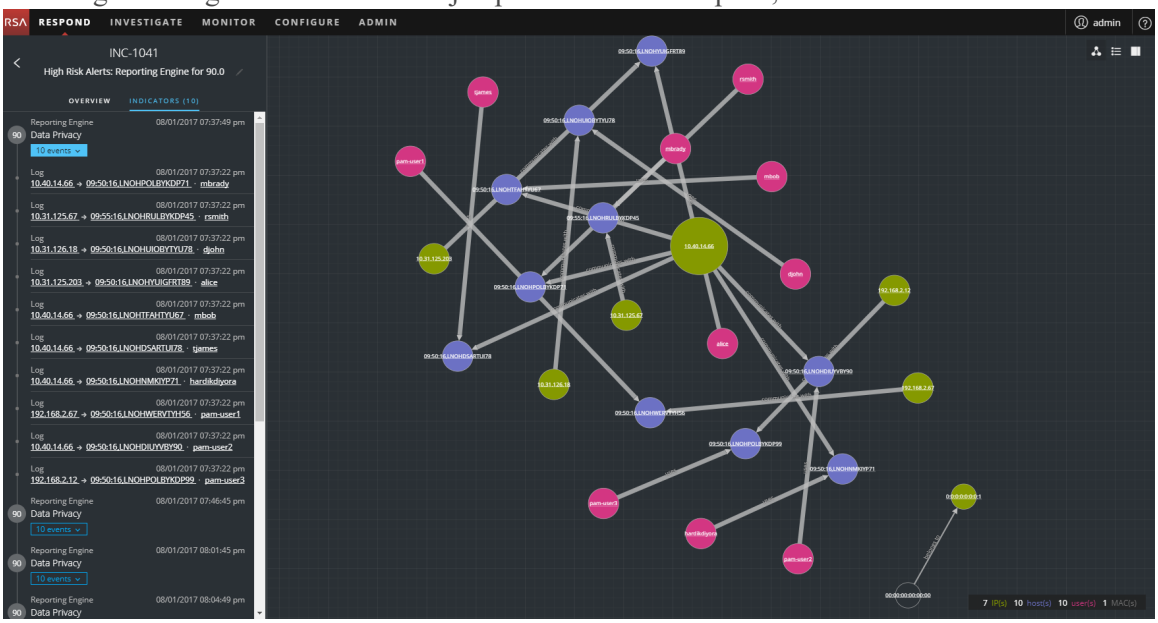
El menú RESPOND tiene las siguientes opciones:

- **Incidentes**: La vista Lista de incidentes contiene una lista de todos los incidentes con información básica. La vista Detalles de incidente proporciona amplios detalles sobre el incidente.
- **Alertas**: Las vistas Lista de alertas y Detalles de la alerta proporcionan información sobre todas las alertas y los indicadores de amenazas que recibe NetWitness Suite en una ubicación.
- **Tareas**: La vista Lista de tareas permite crear tareas y rastrearlas hasta su finalización.

En la siguiente figura se muestra la vista Respond, vista Lista de incidentes.

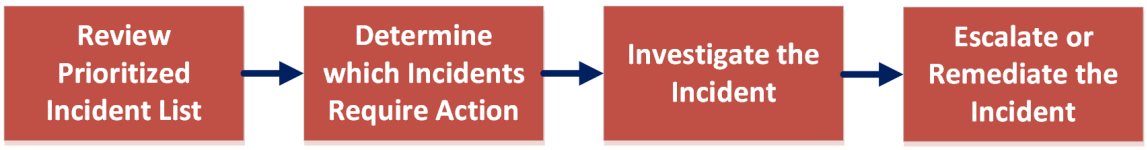


En la siguiente figura se muestra un ejemplo de la vista Respond, vista Detalles de incidente.



Cuando se usa NetWitness Suite como herramienta de administración de casos, esta vista también permite administrar incidentes. Los incidentes nuevos aparecen en orden de prioridad en la parte superior de la línea de espera de incidentes y los incidentes en curso se muestran debajo de los incidentes nuevos.

En la siguiente figura se muestra un flujo de trabajo general de la vista Respond.



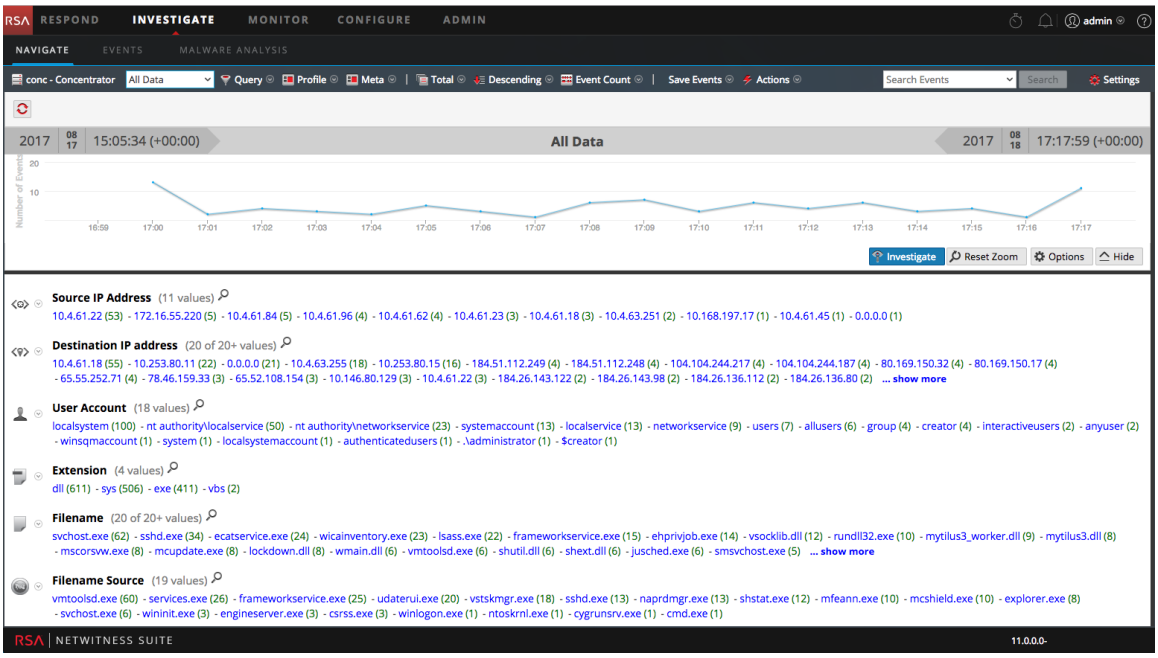
En la vista Respond, los analistas observan la lista de incidentes ordenados según su prioridad y determinan cuáles de ellos requieren una acción. Ellos hacen clic en un incidente para obtener un panorama claro de este con detalles de soporte, lo que les permite investigarlo más a fondo. A continuación, los analistas pueden determinar cómo responder ante la amenaza, ya sea con su escalación o su corrección.

¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Ver listas de incidentes ordenados según su prioridad	RESPOND > Incidentes (vista Lista de incidentes)	Consulte la *Guía del usuario de NetWitness Respond*.

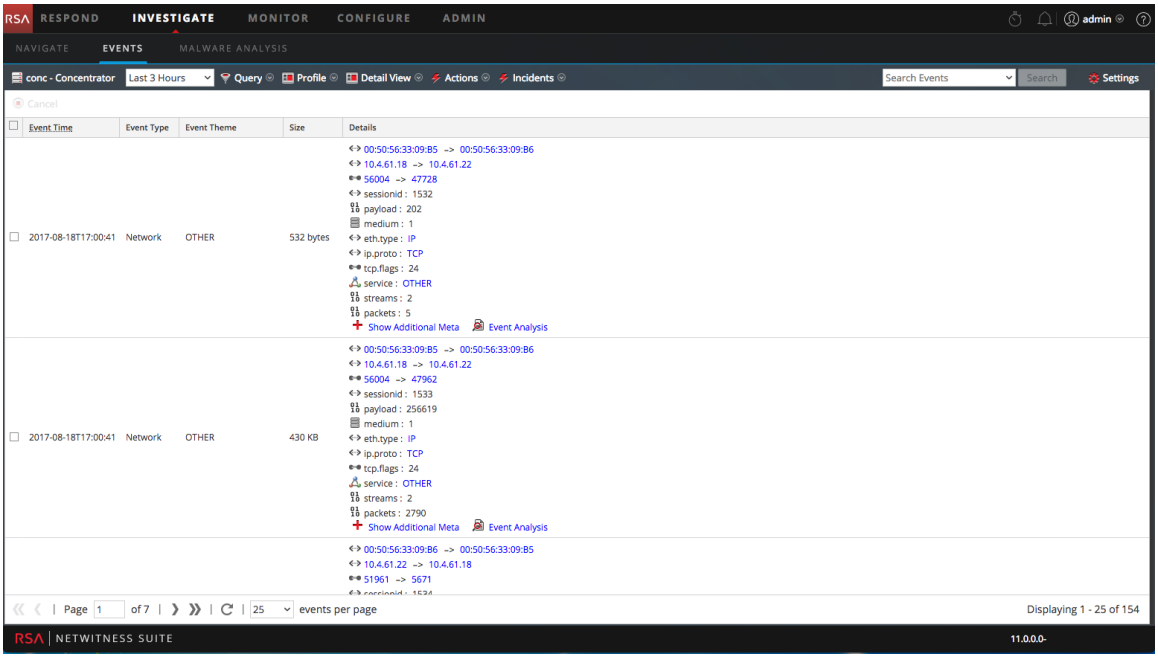
¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Determinar los incidentes que requieren acción (realizar tareas de triage de un incidente)	RESPOND > Incidentes (vista Detalles de incidente)	Consulte la *Guía del usuario de NetWitness Respond*.
Investigar el incidente	RESPOND > Incidentes (vista Detalles de incidente)	Consulte la *Guía del usuario de NetWitness Respond*. (También puede pasar a la vista Investigate).
Elevar o corregir el incidente	RESPOND > Incidentes (vista Detalles de incidente) y RESPOND > Tareas (vista Lista de tareas)	Consulte la *Guía del usuario de NetWitness Respond*.
Revisar alertas	RESPOND > Alertas (vistas Lista de alertas y Detalles de la alerta)	Consulte la *Guía del usuario de NetWitness Respond*.

INVESTIGATE

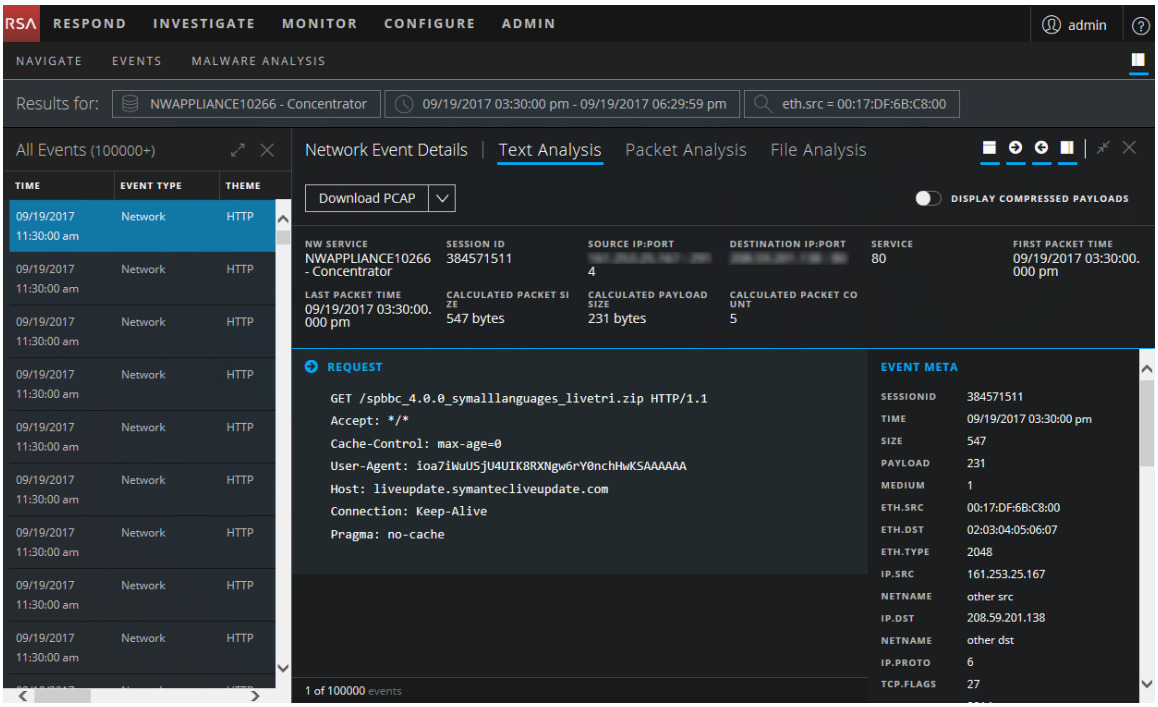
En la vista Investigate se presentan tres vistas diferentes de un conjunto de datos, lo que permite que los analistas vean los metadatos, los eventos y los posibles indicadores de riesgo. En esta figura se ilustra una de las vistas, la vista Navegar, que muestra todos los datos que se investigan en un Concentrator.



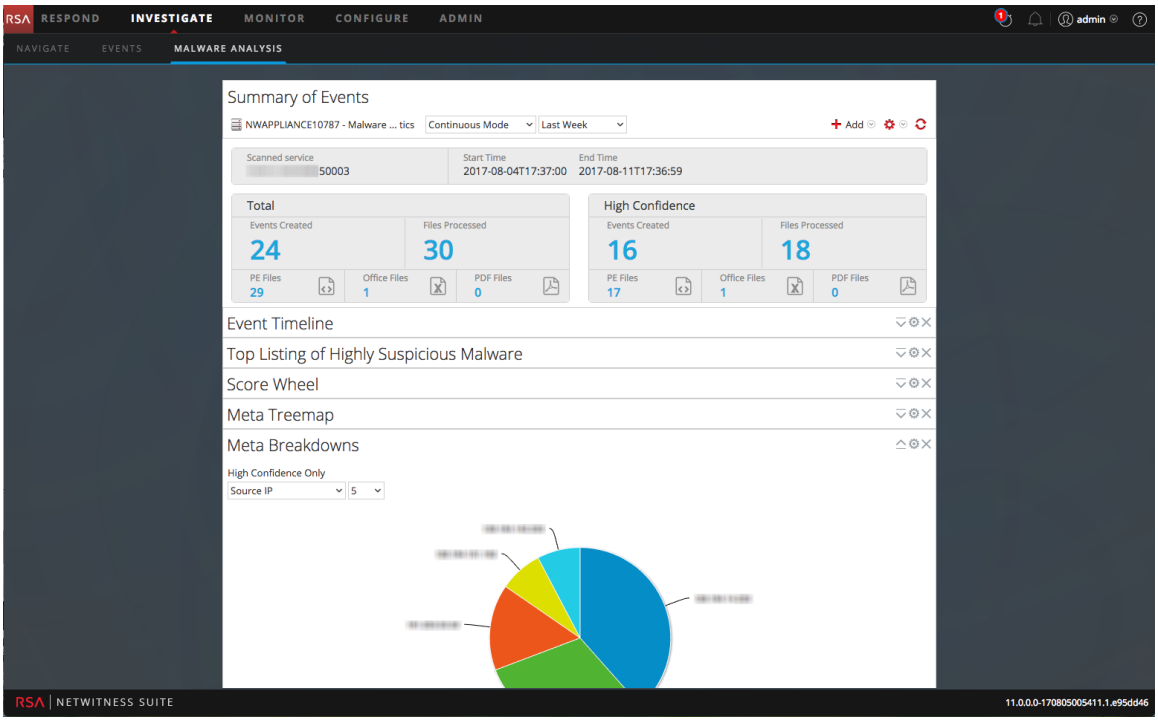
Este es un ejemplo de la vista Eventos.



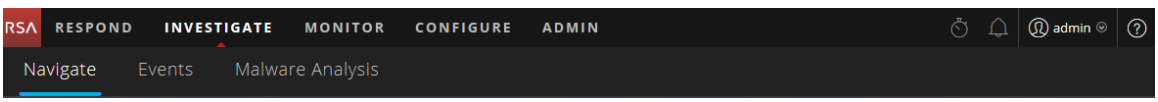
Cuando se hace clic en el vínculo **Análisis de eventos** para un evento específico en la vista Eventos, se abre la vista Detalles de eventos.



Este es un ejemplo del Resumen de eventos de Malware Analysis.



Menú INVESTIGATE

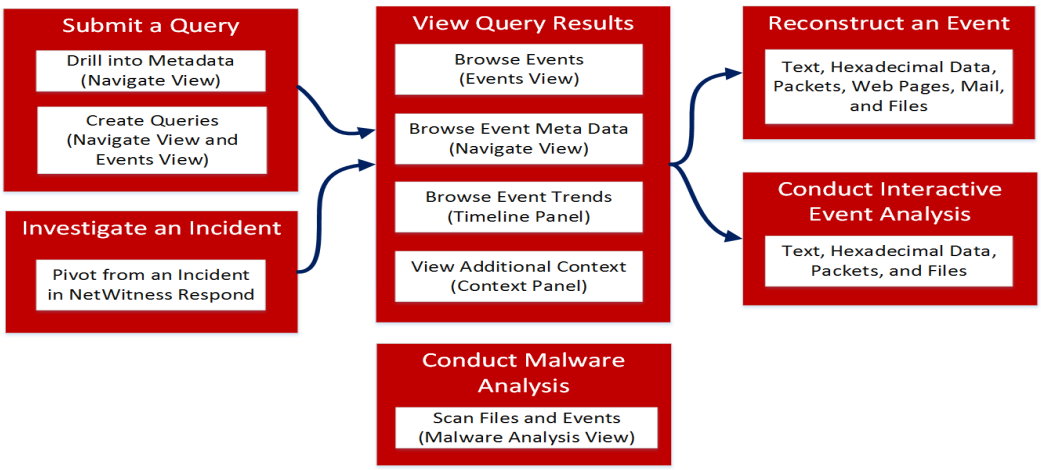


El menú INVESTIGATE tiene las siguientes opciones:

- **Navegar**: La vista Navegar proporciona una barra de herramientas para filtrar y consultar datos, junto con una vista de los metadatos y una visualización de cronograma. Los analistas pueden desglosar a los datos, abrir los eventos seleccionados en la vista Eventos y buscar contexto adicional que proviene del servicio Context Hub.
- **Vista Eventos**: La vista Eventos proporciona una barra de herramientas para limitar el conjunto de datos y una lista de eventos. Los analistas pueden navegar en una lista de eventos simple, una lista detallada y una lista de registros. Cuando se encuentra un evento interesante, pueden ver de forma segura una reconstrucción del evento y realizar un análisis de este.
- **Malware Analysis**: La vista Malware Analysis permite que los analistas analicen determinados tipos de objetos de archivos para evaluar la probabilidad de que un archivo sea malicioso. Malware Analysis es un procesador de análisis de malware automatizado diseñado para analizar determinados tipos de objetos de archivos (como Windows PE, PDF y MS Office) con el fin de evaluar la probabilidad de que un archivo sea malicioso. Mediante el uso de Malware Analysis, el analista de malware puede 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.

Para trabajar en Investigate, los analistas comienzan con la ejecución de una consulta para seleccionar un subconjunto de los datos recopilados. Los analistas pueden recorrer los datos de la vista Navegar, crear sus propias consultas, limitar los filtros y controlar la forma en que se ordenan y se muestran los metadatos. Después de encontrar un evento de interés, los analistas exploran y examinan los detalles del evento en busca de actividad sospechosa o maliciosa. Para obtener información detallada, consulte la *Guía del usuario de Investigation y Malware Analysis*.

En la siguiente figura se muestra un flujo de trabajo general de la vista Investigate.

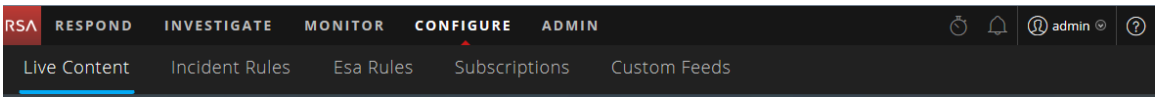


¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Consultar y ver claves y valores de metadatos que se encuentran en un conjunto de datos	Vista INVESTIGATE	Consulte “Realización de una investigación” en la *Guía del usuario de Investigation y Malware Analysis*.
Examinar, reconstruir y analizar eventos	Vista INVESTIGATE	Consulte “Examinar eventos” en la *Guía del usuario de Investigation y Malware Analysis*.
Buscar objetos de archivos que pueden contener código malicioso	Vista INVESTIGATE	Consulte “Realizar un análisis de malware” en la *Guía del usuario de Investigation y Malware Analysis*.

CONFIGURAR

La vista Configurar permite que el personal de inteligencia de amenazas (contenido) configure orígenes de datos y entradas en NetWitness Suite en una ubicación conveniente.

Menú de CONFIGURAR



El menú CONFIGURAR tiene las siguientes opciones:

- **Live Content**: (Servicios de Live) La vista Live Content permite buscar y suscribirse a recursos de Servicios de Live. Servicios de Live es el componente de NetWitness Suite que administra la comunicación y la sincronización entre los servicios de NetWitness Suite y una biblioteca de contenido de Live disponible para los clientes de RSA NetWitness Suite. Puede ver, buscar, implementar y suscribirse a contenido del sistema de administración de contenido (CMS) de RSA Live para los servicios y el software de NetWitness Suite. Cuando se suscribe a un recurso, acepta recibir actualizaciones de RSA Servicios de Live de manera habitual.
  Para los usuarios existentes de 10.6, esto era Live > Buscar.
- **Reglas de incidentes**: La vista Reglas de incidentes permite crear reglas de agregación con diversos criterios para la creación automática de incidentes. Puede ver los incidentes ordenados según su prioridad en la vista Respond.
  Para los usuarios existentes de 10.6, esto era Incidentes > Configurar.

- **Reglas de ESA**: La vista Reglas de ESA permite administrar las reglas de Event Stream Analysis (ESA) que especifican criterios para el comportamiento de problemas o eventos amenazantes en la red. Cuando ESA detecta una amenaza que coincide con los criterios de una regla, genera una alerta.
  Las reglas de ESA se pueden crear o descargar desde Servicios de Live. La Biblioteca de reglas muestra todas las reglas de ESA creadas o descargadas. Para activar las reglas, debe agregarlas a una implementación. Las implementaciones mapean reglas desde la biblioteca de reglas a los servicios de ESA correspondientes.
  Para los usuarios existentes de 10.6, esto era Alertas > Configurar.
- **Suscripciones**: (Servicios de Live) La vista Suscripciones permite administrar el contenido de Live al que se suscribió en la vista Live Content. Para configurar Servicios de Live en NetWitness Suite, configure la conexión y la sincronización entre el servidor de CMS y NetWitness Suite.
  Para los usuarios existentes de 10.6, esto era Live > Configurar.
- **Feeds personalizados**: (Servicios de Live) La vista Feeds personalizados optimiza la tarea de crear y administrar feeds personalizados, además de completar los feeds en los Decoders y los Log Decoders seleccionados. Puede configurar y mantener feeds personalizados y de identidad.
  NetWitness Suite utiliza feeds para crear metadatos en función de valores de metadatos definidos de forma externa. Un feed es una lista de datos que se compara con las sesiones a medida que se capturan o procesan. Para cada coincidencia, se crean metadatos adicionales. Puede crear feeds personalizados para proporcionar extracción de metadatos adicionales, por ejemplo, con el fin de admitir aplicaciones de red personalizadas.
  Para los usuarios existentes de 10.6, esto era Live > Feeds.

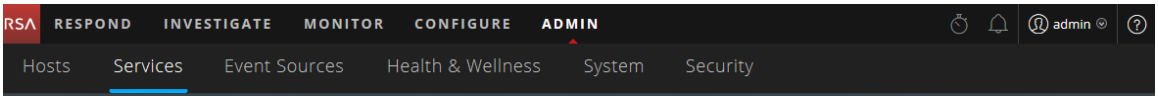
¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Crear una cuenta de Servicios de Live.	Portal de registro de RSA Live: https://cms.netwitness.com/registration/	Consulte la *Guía de administración de servicios de Live*.
Buscar e implementar recursos de Servicios de Live.	CONFIGURAR > Live Content	Consulte la *Guía de administración de servicios de Live*.

¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Crear incidentes automáticamente.	CONFIGURAR > Reglas de incidentes	Consulte la *Guía del usuario de NetWitness Respond*.
Configurar alertas.	CONFIGURAR > Reglas de ESA	Consulte la *Guía de alertas mediante ESA*.
Configurar los servicios de Servicios de Live en NetWitness Suite	CONFIGURAR > Suscripción	Consulte la *Guía de administración de servicios de Live*.
Configurar y mantener los feeds personalizados y de identidad.	CONFIGURAR > Feeds personalizados	Consulte la *Guía de administración de servicios de Live*.

ADMIN

En la vista Admin, los administradores pueden administrar los hosts de red y los servicios, monitorear el estado y la condición de NetWitness Suite y administrar la seguridad en el nivel del sistema. También pueden configurar los recursos globales del sistema y administrar los orígenes de eventos.

Menú de ADMIN



El menú ADMIN tiene las siguientes opciones:

- **Hosts**: La vista Hosts permite configurar y mantener los hosts. Un host es la máquina en la cual se ejecutan los servicios y puede ser una máquina física o virtual.
- **Servicios**: La vista Servicios permite administrar los servicios, administrar sus usuarios y sus funciones, mantener sus archivos de configuración y explorar y editar sus propiedades. Un servicio realiza una función única, como un servicio Decoder, que captura datos de red en forma de paquetes.

- **Orígenes de eventos**: La vista Orígenes de eventos permite administrar orígenes de eventos y configurar políticas de alerta para ellos. En general, las organizaciones monitorean los orígenes de eventos en grupos de acuerdo con la criticidad de estos. Puede crear políticas de monitoreo para cada grupo de orígenes de eventos y ordenarlos de acuerdo con su prioridad.
- **Estado y condición**: La vista Estado y condición permite monitorear el estado de los hosts y los servicios de NetWitness Suite en el ambiente de red.
- **Sistema**: La vista Sistema permite establecer las configuraciones globales de NetWitness Suite. Puede configurar el registro de auditoría global, el correo electrónico, el registro de sistema, los trabajos, RSA Servicios de Live, la integración de URL, Investigation, Event Stream Analysis (ESA), ESA Analytics y ajustes avanzados del rendimiento. Además, puede administrar las versiones de NetWitness Suite y configurar el servidor de licencia local.
- **Seguridad**: En la vista Seguridad de Administration se proporciona la funcionalidad para administrar cuentas de usuario, administrar funciones de usuario, mapear grupos externos a funciones de NetWitness Suite y modificar otros parámetros del sistema relacionados con la seguridad. Estos se aplican al sistema NetWitness Suite y se utilizan junto con los ajustes de seguridad de cada servicio.

¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Administrar hosts.	ADMIN > Hosts	Consulte la *Guía de introducción de hosts y servicios*.
Administrar los servicios, incluida la administración del acceso de los usuarios a los servicios y la seguridad.	ADMIN > Servicios	Consulte la *Guía de introducción de hosts y servicios*.
Administrar orígenes de eventos y configurar políticas de alerta para ellos.	ADMIN > Orígenes de eventos	Consulte la *Guía de administración de orígenes de eventos*.
Configurar y monitorear alarmas para los hosts y los servicios en el dominio de NetWitness Suite.	ADMIN > Estado y condición > Alarma	Consulte la *Guía de mantenimiento del sistema*.
Monitorear estadísticas de los hosts de NetWitness Suite y de los servicios que se ejecutan en los hosts.	ADMIN > Estado y condición > Monitoreo	Consulte la *Guía de mantenimiento del sistema*.

¿Qué puedo hacer aquí?	Ruta	Mostrarme cómo
Crear y aplicar políticas a los hosts y los servicios como ayuda para mantener el estado y la condición del dominio de NetWitness Suite.	ADMIN > Estado y condición > Políticas	Consulte la *Guía de mantenimiento del sistema.*
Establecer configuraciones globales para NetWitness Suite.	ADMIN > Sistema	Consulte *Guía de configuración del sistema.*
Configurar el registro de auditoría global.	ADMIN > Sistema > Auditoría global	Consulte *Guía de configuración del sistema.*
Configurar la seguridad del sistema.	ADMIN > Seguridad	Consulte la *Guía de administración de usuarios y de la seguridad del sistema.*
Administrar a los usuarios del sistema con funciones y permisos.	ADMIN > Seguridad	Consulte la *Guía de administración de usuarios y de la seguridad del sistema.*

Configuración de la vista predeterminada de acuerdo con la función del SOC

Después de iniciar sesión en NetWitness Suite, puede facilitar la navegación en la aplicación mediante la configuración de la vista predeterminada de acuerdo con su función en el centro de operaciones de seguridad (SOC). La vista predeterminada, también conocida como página principal, se configura en las preferencias de usuario.

En la siguiente figura se muestran las vistas principales de NetWitness Suite.

- **Respond**: Esta vista es para los encargados de respuesta ante incidentes, quienes pueden ver una lista de incidentes, para los cuales se realizarán tareas de triage, y alertas. Para los usuarios existentes de 10.6, esta vista se conocía como la vista Administración de incidentes y la vista Respond > Alertas reemplaza a la vista Alertas > Resumen de ESA 10.6.
  Respond es la vista inicial predeterminada. Si no tiene permiso para ver la vista Respond, la vista predeterminada será Monitor.
- **Investigate**: Esta vista es para los buscadores de amenazas, quienes investigan y buscan amenazas avanzadas.
- **Monitor**: Esta vista es para todos los usuarios y es la vista clásica de las versiones anteriores de la aplicación. Puede ver tableros e informes en diferentes áreas de interés según los permisos de usuario. Tiene la opción de seleccionar un tablero preconfigurado, importar un tablero o crear su propio tablero personalizado.
- **Configurar**: Esta vista es para el personal de inteligencia de amenazas (contenido), el cual configura orígenes de datos y entradas en NetWitness Suite. El personal de inteligencia de amenazas usa esta área para descargar y administrar contenido de Live. También puede crear y administrar reglas de incidentes y de ESA.
  Para los usuarios existentes de 10.6, esta vista era Live, Incidentes > Configurar y Alertas > Configurar.
- **Admin**: Esta vista es para los administradores del sistema, quienes configuran y mantienen la aplicación en general.

Puede seleccionar cualquiera de las vistas principales de NetWitness Suite como la vista predeterminada. Además de las vistas principales, NetWitness Suite tiene tableros predefinidos que puede seleccionar en la vista Monitor en función de las tareas que realiza:

- Tableros predeterminados
- Tablero Identidad
- Tablero Operaciones: Registros
- Tablero Operaciones: Red
- Tablero de descripción general
- Tablero Amenaza: Indicadores
- Tablero Amenaza: Intrusión

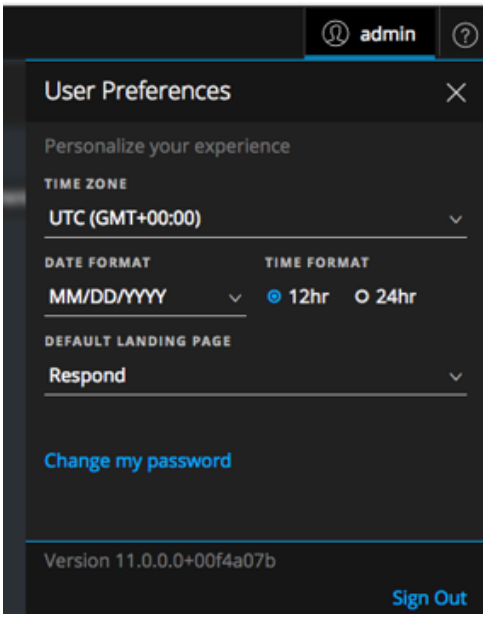
En la siguiente tabla se muestran las funciones típicas del SOC y las vistas disponibles que puede seleccionar como su página principal en las preferencias de usuario de acuerdo con su función del SOC. Si tiene más de una función, seleccione la vista con la cual le sea más útil comenzar cuando inicia sesión en NetWitness Suite.

Funciones del SOC	Descripción de la función	Considere esta página principal predeterminada
Encargado de respuesta ante incidentes (analista de nivel 1)	Se encarga de alertas e incidentes puestos en su línea de espera, para los cuales debe realizar tareas de revisión y moderación.	**RESPOND**
Buscador de amenazas (analista de nivel 2/nivel 3)	Investiga y busca amenazas avanzadas.	**INVESTIGATE**
Administrador del SOC (administración y creación de informes del SOC)	Administra la preparación del SOC y responde ante incidentes y vulneraciones de datos.	**MONITOR** (El tablero está en la vista MONITOR. Cuando inicie sesión, seleccione el tablero predefinido adecuado a su función del SOC. También puede importar un tablero o crear uno propio).

Funciones del SOC	Descripción de la función	Considere esta página principal predeterminada
Experto en contenido (inteligencia de amenazas)	Configura los orígenes de datos y las entradas en NetWitness Suite.	**MONITOR** o **CONFIGURAR** (El tablero está en la vista MONITOR. Cuando inicie sesión, seleccione el tablero predefinido adecuado a su función del SOC. También puede importar un tablero o crear uno propio. Si elige MONITOR como la vista predeterminada, puede navegar a la vista CONFIGURAR desde el menú principal).
Encargado de la privacidad de datos (DPO)	Es similar a un administrador, pero un DPO monitorea y protege la información de privacidad/confidencial.	**MONITOR** (El tablero está en la vista MONITOR. Cuando inicie sesión, seleccione el tablero predefinido adecuado a su función del SOC. También puede importar un tablero o crear uno propio).
Administrador del sistema	Se centra en la configuración y la estabilidad de la aplicación general. Administra el acceso de los usuarios.	**ADMIN**

Configuración de la vista predeterminada

1. (Solo en la vista Respond) En la barra de menú principal, seleccione  .
   En el cuadro de diálogo Preferencias de usuario se muestran las preferencias actuales.



2. En el campo **Página principal predeterminada**, seleccione la vista predeterminada que desea ver cuando inicia sesión en NetWitness Suite. Utilice la tabla anterior para realizar su selección de acuerdo con su función del SOC. Por ejemplo, si es un encargado de respuesta ante incidentes, puede seleccionar **Respond** y si es un buscador de amenazas, puede seleccionar **Investigate**.
   Las preferencias se aplican de inmediato. Puede cambiar la página principal predeterminada en cualquier momento. Para obtener información sobre otras preferencias, consulte Configuración de las preferencias del usuario.
3. Para verificar que pueda ver la vista predeterminada correcta, haga clic en **Cerrar sesión** para cerrar la sesión y, a continuación, vuelva a iniciarla en NetWitness Suite.

Consejos básicos de solución de problemas para la configuración de usuarios

En la siguiente tabla se proporcionan consejos básicos de solución de problemas que pueden ser útiles para la configuración de usuarios en NetWitness Suite.

Problema	Consejo para la solución de problemas
Cuando inicio sesión en NetWitness Suite, veo una vista predeterminada incorrecta.	Verifique que esté configurada la vista predeterminada correcta en el campo Página principal predeterminada de las preferencias de usuario. Si selecciona la vista MONITOR, puede elegir el tablero predefinido más adecuado para su función del SOC. También puede importar un tablero o crear uno propio.
Veo la vista correcta, pero los metadatos no se cargan.	Pruebe con otro navegador. Por ejemplo, si usa Safari, intente usar Firefox o Chrome.
Estoy usando Internet Explorer 10 y recibo el siguiente error: `The page can't be displayed.`	NetWitness Suite es compatible con las versiones modernas (o actuales) de los navegadores más recientes. Intente instalar una versión más reciente del navegador. Si no puede actualizarlo, intente habilitar el protocolo TLS 1.2 en el navegador: Navegue a **Opciones de Internet > Opciones avanzadas > Configuración > Seguridad**. Además de los otros protocolos, asegúrese de que el protocolo TLS 1.2 esté habilitado. Haga clic en **Aplicar**. Vuelva a cargar la página.
Cuando inicio sesión, no puedo ver nada.	Consulte al administrador. Es posible se deba asignar una función de usuario a su cuenta o que se requieran tareas adicionales de solución de problemas.
No puedo ver dónde cambiar mi página principal predeterminada.	Vaya a las Preferencias de usuario en la vista Respond o consulte al administrador.

Configuración de las preferencias del usuario

Puede ver y administrar sus preferencias globales para la aplicación NetWitness Suite desde su perfil de usuario. Sus opciones de preferencias globales varían en función de si accede a ellas desde la nueva vista Respond o de otras vistas, como Monitor, Configurar, Admin e Investigate. Puede:

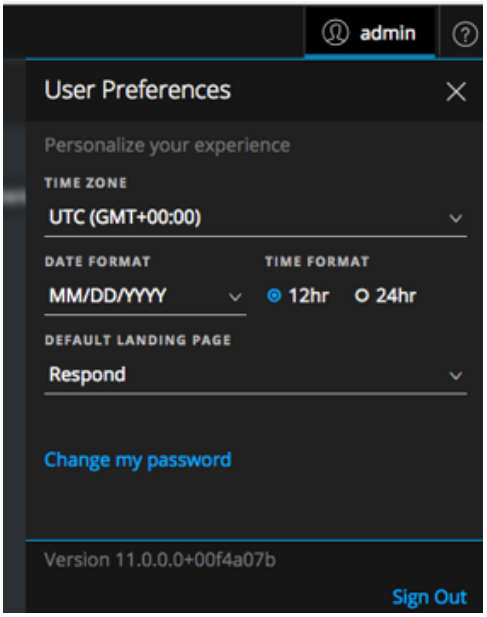
- Configurar la zona horaria de la aplicación
- Configurar el formato de fecha y hora de la aplicación (solo en la vista Respond)
- Seleccionar la ubicación de inicio predeterminada (solo en la vista Respond)
- Cambiar su contraseña (consulte Cambio de la contraseña para obtener más información).
- Habilitar o deshabilitar notificaciones (todas las vistas, excepto la vista Respond)
- Habilitar o deshabilitar menús contextuales (todas las vistas, excepto la vista Respond)

Nota: Los procedimientos de preferencias de usuario marcados con "vista Respond" y "solo en la vista Respond" también se pueden realizar en algunas vistas de Investigate.

Ver las preferencias de usuario (vista Respond)

En la esquina superior izquierda de la ventana del navegador de NetWitness Suite, seleccione  .

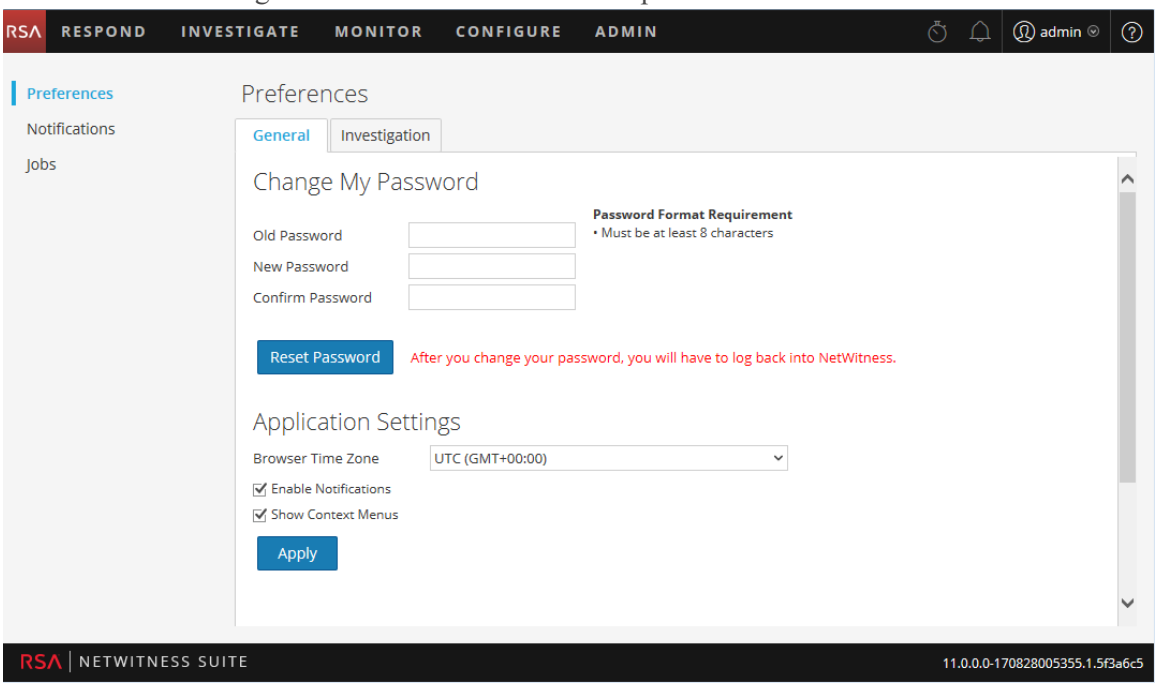
El cuadro de diálogo Preferencias de usuario muestra las preferencias actuales cuando se accede a través de la vista Respond.



Todas las selecciones que hace se aplican de inmediato.

Ver las preferencias de usuario (todas las vistas, excepto la vista Respond)

Para las siguientes vistas: Investigate, Monitor, Configurar y Admin: En la esquina superior izquierda de la ventana del navegador de NetWitness Suite, seleccione > **Perfil**.
En el cuadro de diálogo Preferencias se muestran las preferencias actuales.



Configurar la zona horaria y el formato de fecha y hora

Puede cambiar la zona horaria y el formato de fecha y hora correspondiente a su ubicación.

Nota: Solo puede cambiar las preferencias de fecha y hora de la ubicación en la vista Respond.

1. En el cuadro de diálogo Preferencias de usuario, seleccione las preferencias de localización:
   a. **Zona horaria**: Configure la zona horaria que se usará en NetWitness Suite.
   b. **(Solo en la vista Respond) Formato de fecha**: Configure el formato para el orden de visualización del mes (MM), el día (DD) y el año (AAAA). Por ejemplo, MM/DD/AAAA muestra la fecha en el formato 05/11/2017.

c. **(Solo en la vista Respond) Formato de hora**: Configure la hora en formato de 12 o 24 horas. Por ejemplo, las 2:00 p. m. en el formato de 12 horas son las 14:00 h en el formato de 24 horas.

Los cambios en la vista Respond se aplican de inmediato.

2. **(Todas las vistas, excepto Respond)** Haga clic en **Aplicar**.
   Las preferencias se aplican de inmediato.

Seleccionar la ubicación de inicio predeterminada

1. **(Solo en la vista Respond)** Abra el cuadro de diálogo Preferencias de usuario.
2. En el campo **Página principal predeterminada**, seleccione la vista inicial que desea ver cuando inicia sesión en NetWitness Suite. Según su función de usuario, puede elegir Respond, Investigate, Monitor, Configurar y Admin. Por ejemplo, puede elegir Respond para ir directamente a la sección que corresponde a los encargados de responder ante incidentes de la aplicación. Consulte Configuración de la vista predeterminada de acuerdo con la función del SOC como ayuda para seleccionar la vista predeterminada adecuada.
   Esta selección configura la vista predeterminada para toda la aplicación. Los cambios se aplican de inmediato.

Habilitar o deshabilitar las notificaciones del sistema para la cuenta de usuario

(Todas las vistas, excepto la vista Respond) De manera predeterminada, las notificaciones del sistema de NetWitness Suite se habilitan cuando se crea una nueva cuenta de usuario. Puede deshabilitar y habilitar estas notificaciones en cualquier momento.

1. En el cuadro de diálogo Preferencias:
   - Para habilitar las notificaciones para la cuenta de usuario, seleccione la casilla de verificación **Habilitar notificaciones**.
   - Para deshabilitar las notificaciones, deseleccione la casilla de verificación **Habilitar notificaciones**.
2. Haga clic en **Aplicar**.
   Su preferencia se aplica de inmediato.

Habilitar o deshabilitar menús contextuales para la cuenta de usuario

(Todas las vistas, excepto la vista Respond) De manera predeterminada, los menús contextuales se habilitan cuando se crea una nueva cuenta de usuario. Los menús contextuales proporcionan funciones adicionales para vistas específicas cuando hace clic con el botón secundario en una vista.

1. En el cuadro de diálogo Preferencias:
   - Para habilitar los menús contextuales para la cuenta de usuario, seleccione la casilla de verificación **Habilitar menús contextuales**.
   - Para deshabilitar los menús contextuales, deseleccione la casilla de verificación **Habilitar menús contextuales**.
2. Haga clic en **Aplicar**.
   Su preferencia se aplica de inmediato.

Nota: Los ajustes disponibles en la pestaña Investigate del cuadro de diálogo Preferencias (para todas las vistas, excepto Respond) se documentan en la *Guía del usuario de Investigation y Malware Analysis*.

Administración de tableros

Un tablero es un grupo de dashlets que brinda la capacidad de ver, en un solo espacio, las instantáneas clave de los diferentes componentes que se consideran importantes. En NetWitness Suite, puede crear tableros para obtener información general y métricas que retratan todo el panorama de una implementación de NetWitness Suite, en los cuales se muestra solo la información más pertinente a las operaciones diarias.

El tablero de NetWitness Suite predeterminado se muestra cuando inicia sesión en NetWitness Suite. Incluye algunos dashlets útiles que le permiten comenzar a hacer sus propias personalizaciones. Los tableros de todos los componentes de NetWitness Suite se encuentran disponibles para agregarlos al tablero de NetWitness Suite predeterminado o a un tablero de NetWitness Suite personalizado.

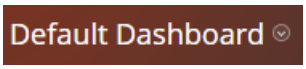
Puede ver tableros e informes en diferentes áreas de interés según los permisos de usuario. Tiene la opción de seleccionar un tablero preconfigurado, importar un tablero o crear su propio tablero personalizado. Los tableros lo ayudan a ver informes de manera rápida y sencilla. Puede configurar sus tableros para que muestren la información que apoya su flujo de trabajo. En este tema se explican las tareas generales que se pueden realizar durante la configuración de un tablero.

Aspectos básicos de los tableros

Si la vista Monitor es su página principal predeterminada después del inicio de sesión en NetWitness Suite, verá siempre el tablero predeterminado o el tablero configurado actualmente de inmediato después de completar el proceso de inicio de sesión. Para volver al tablero desde otro componente de NetWitness Suite, vaya a **Monitor** > **Descripción general**.

Título del tablero

El título del tablero refleja el tablero activo actualmente; por ejemplo, tablero predeterminado.



Lista de selección de tableros

Puede acceder a tableros preconfigurados y personalizados en la lista de selección de tableros. Cuando selecciona un tablero, su título se muestra debajo de la barra de herramientas de NetWitness Suite.

Un tablero tiene:

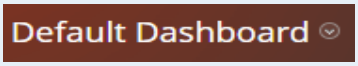
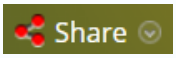
- La barra de herramientas del tablero
- El título del tablero y la lista de selección de tableros

Barra de herramientas del tablero

La barra de herramientas del tablero está disponible junto al título del tablero seleccionado. La barra de herramientas del tablero permite realizar varias operaciones en los tableros y los dashlets.

Nota: Las opciones Copiar, Eliminar, Importar, Exportar, Compartir y Agregar fila están deshabilitadas para los tableros preconfigurados.

Opción	Descripción
	Configura el tablero seleccionado como favorito.

Opción	Descripción
	Muestra la lista de tableros disponibles desde los cuales puede hacer una selección.
	Muestra el cuadro de diálogo Crear un tablero, donde puede definir o agregar un tablero personalizado.
	Elimina un tablero personalizado. El tablero predeterminado no se puede eliminar.
	Permite copiar un tablero.
	Muestra el cuadro de diálogo Administrar dashlet.
	Exporta un tablero como un archivo .zip.
	Importa un tablero como un archivo .zip o .cfg.
	Permite compartir un tablero con otro usuario.
	Permite que el usuario agregue filas y columnas al tablero según se requiera. Haga clic en el ícono  en una fila para agregar un dashlet.

El tablero predeterminado

El tablero predeterminado está configurado para mostrar dashlets específicos en posiciones específicas. El tablero predeterminado sirve como ejemplo de la composición de tableros y como punto de inicio para la personalización.

- Para personalizar la información del tablero predeterminado, puede editar, agregar, mover, maximizar y eliminar dashlets.
- Después de modificar el tablero predeterminado, puede restaurarlo () a su diseño original.
- El tablero predeterminado no se puede eliminar ni compartir.

Selección de un tablero preconfigurado

En la instalación de NetWitness Suite, los siguientes tableros preconfigurados se activan automáticamente y están disponibles para usted:

- Valor predeterminado
- Identidad
- Investigation
- Operaciones: Análisis de archivos
- Operaciones: Registros
- Operaciones: Red
- Operaciones: Análisis de protocolos
- Descripción general
- RSA SecurID
- Amenaza: Localización
- Amenaza: Indicadores de malware
- Amenaza: Intrusión
- Amenaza: Indicadores de malware

No puede realizar las siguientes acciones en un tablero preconfigurado:

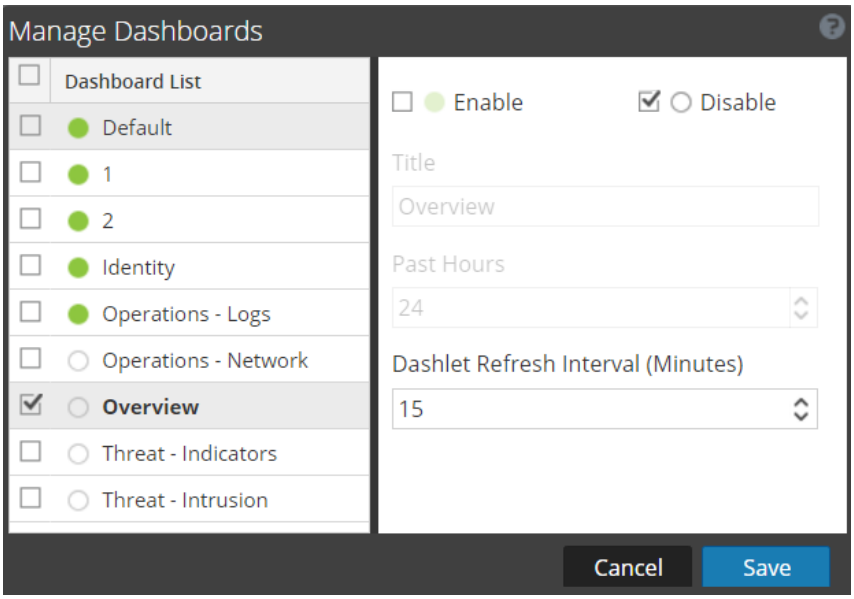
- Editar un tablero
- Exportar un tablero
- Compartir un tablero
- Eliminación de tableros

Para obtener más información sobre cada tablero preconfigurado, consulte el Catálogo de tableros en el espacio Contenido de RSA en RSA Link.

Habilitación o deshabilitación de tableros

Cuando habilita o deshabilita un tablero, se habilitan o se deshabilitan todos los dashlets dentro de este, así como los gráficos asociados, a menos que se usen en algún otro tablero.

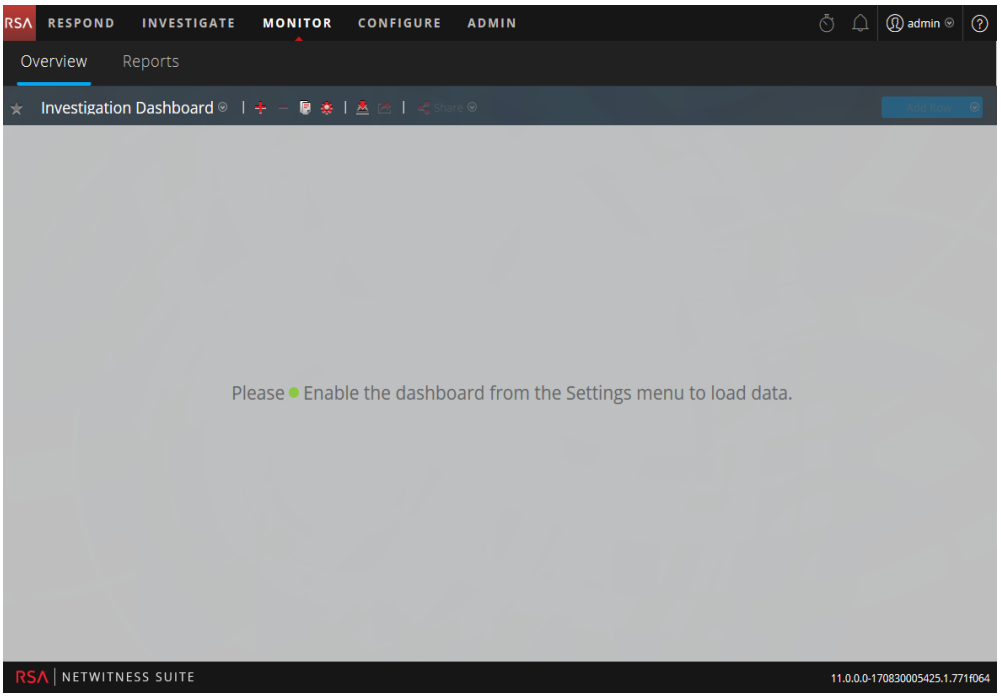
Los módulos de NetWitness Suite pueden mostrar solo los dashlets que se presentan en el cuadro de diálogo Administrar dashlet. El tablero principal ofrece todos los dashlets de NetWitness Suite. Este es un ejemplo de los dashlets actualmente disponibles.



Nombre	Descripción
Lista de tableros	Muestra una lista de los tableros predeterminados, preconfigurados y personalizados.
Enable	Muestra si el dashlet seleccionado está habilitado.
Disable	Muestra si el dashlet seleccionado está deshabilitado.
Título	Muestra el título del dashlet seleccionado. También puede cambiar el nombre del tablero.
Horas pasadas	Muestra la hora para la cual se recopilan datos.
Intervalos de actualización del dashlet (minutos)	Muestra el intervalo de tiempo de actualización de un dashlet.

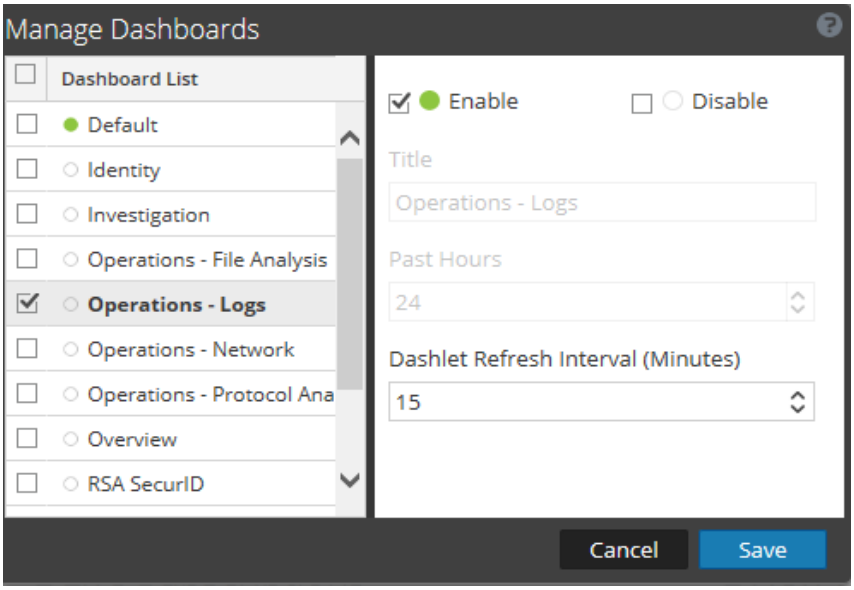
Habilitación de un tablero

Si selecciona un tablero que no está habilitado, se muestra una pantalla enmascarada.



Para habilitar uno o más tableros:

1. Navegue al tablero que se habilitará.
2. En la barra de herramientas del tablero, haga clic en  .
3. Seleccione la opción **Administrar tablero**.
   Se muestra el cuadro de diálogo Administrar tableros.



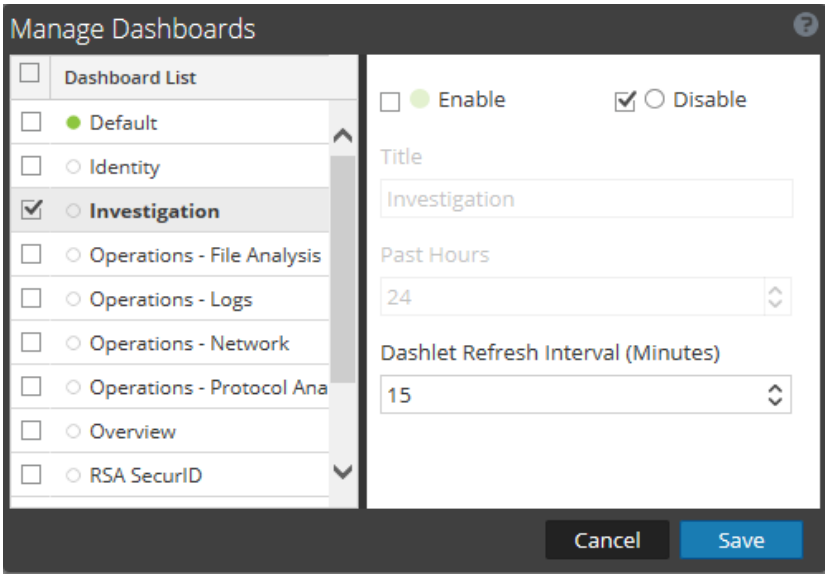
4. En la lista de tableros, seleccione los tableros que se habilitarán.

5. Haga clic en la casilla de verificación **Activado**.
6. Haga clic en **Guardar**.

Deshabilitación de un tablero

Para deshabilitar uno o más tableros:

1. Navegue al tablero que se deshabilitará.
2. En la barra de herramientas del tablero, haga clic en  .
3. Seleccione la opción **Administrar tablero**.
   Se muestra el cuadro de diálogo Administrar tableros.



4. En la lista de tableros, seleccione los tableros que se deshabilitarán.
5. Haga clic en la casilla de verificación **Deshabilitar**.
6. Haga clic en **Guardar**.

Configuración de un tablero como favorito

Para personalizar las vistas en NetWitness Suite, puede establecer un tablero preconfigurado o personalizado como favorito. El tablero de NetWitness Suite, como el nombre lo sugiere, ofrece todos los dashlets de NetWitness Suite. El cuadro de diálogo Favorito configura un tablero específico como el favorito y lo enumera como favorito cada vez que usted inicia sesión en NetWitness Suite.

1. Vaya a cualquier tablero.
2. En la barra de herramientas del tablero, haga clic en  .

   Si el ícono de favorito es de color rojo, indica que ese tablero seleccionado está configurado como favorito y se muestra en la parte superior por encima de la línea.

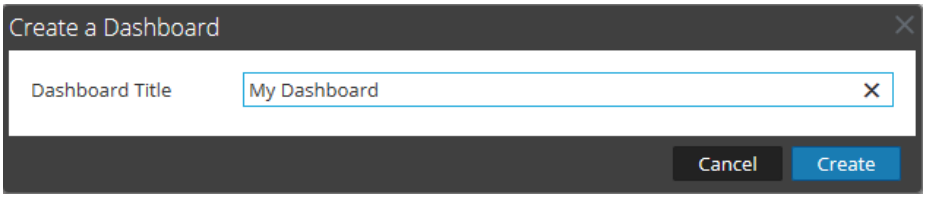
Creación de tableros personalizados

Puede crear tableros personalizados para desempeñar un propósito determinado, por ejemplo, para representar un área geográfica o funcional específica de la red. Cada tablero personalizado se agrega a la lista de selección de tableros.

Para crear un tablero personalizado:

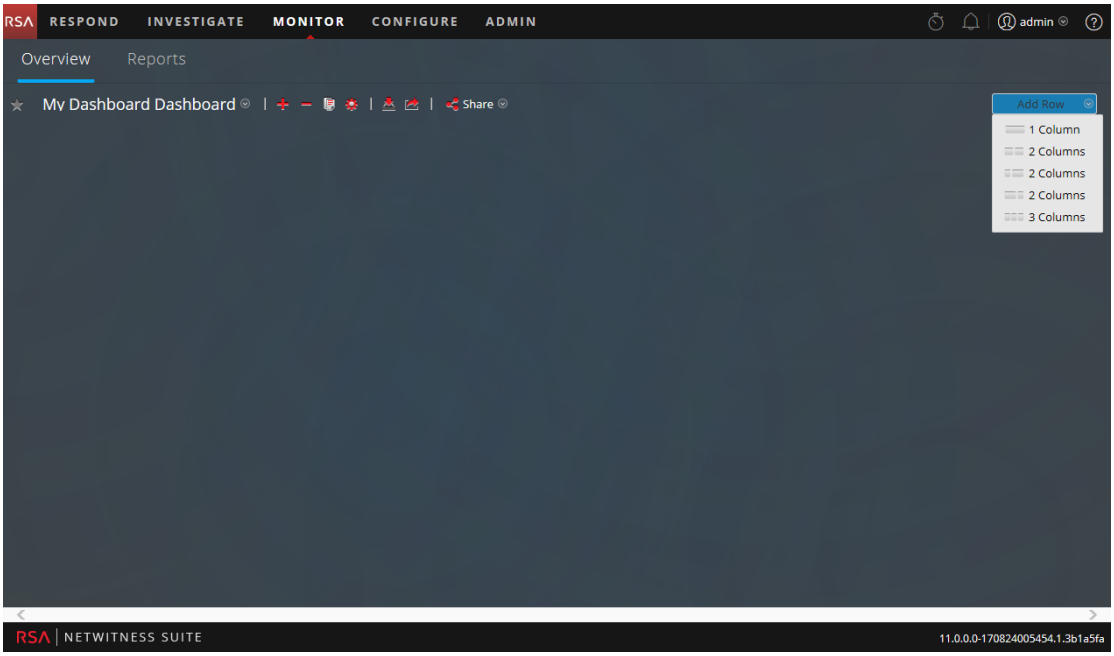
1. En la barra de herramientas del tablero, haga clic en  .

   Se muestra el cuadro de diálogo Crear un tablero.



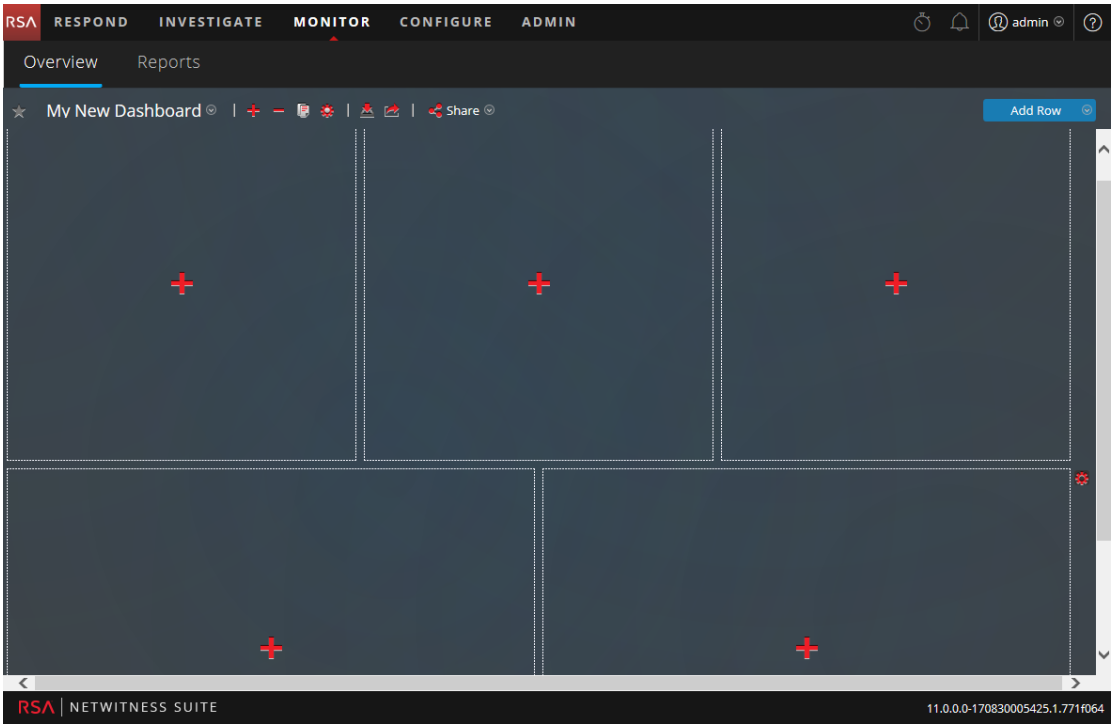
2. Escriba un título para el tablero nuevo y haga clic en **Crear**.

   El tablero nuevo se muestra como una pantalla en blanco.



3. Agregue filas al tablero, el que puede contener una o más columnas, mediante el control **Agregar fila** (

) del lado derecho de la pantalla. Simplemente haga clic en la configuración de la columna que desea en la lista desplegable para agregar una fila al tablero con la cantidad de columnas seleccionada. Repita el proceso para agregar más filas.



4. Ahora puede agregar los dashlets que desee al tablero, para lo cual debe hacer clic en  en un marcador de posición vacío en una fila. Para obtener información detallada sobre cómo agregar y administrar los dashlets, consulte Trabajo con dashlets.

Después de crear tableros personalizados, puede:

- Cambiar entre tableros mediante la selección de una opción en la lista de selección de tableros
- Eliminar cualquier tablero personalizado
- Importar o exportar un tablero

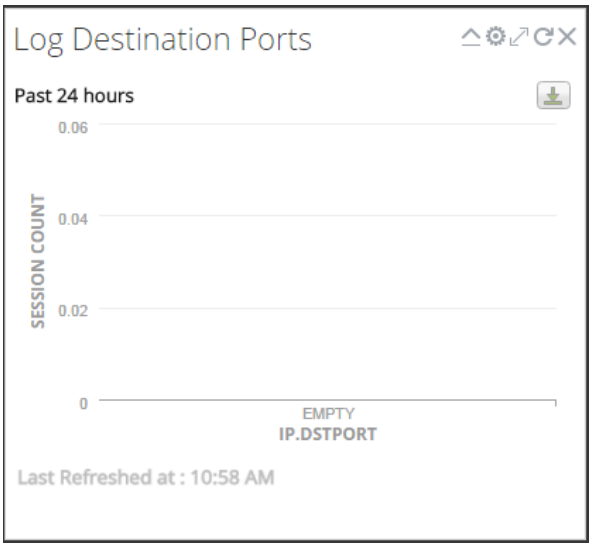
Cada tablero tiene:

- La barra de herramientas del tablero
- El título del tablero y la lista de selección de tableros
- Ninguno o más dashlets

Trabajo con dashlets

NetWitness Suite utiliza dashlets para mostrar subconjuntos centrados de información del sistema, servicios, trabajos, recursos, suscripciones, reglas y otra información.

Los controles para un dashlet están en la barra de título. Todos los dashlets utilizan un conjunto de controles común y solo aquellos que se aplican al dashlet específico se muestran en su barra de título.



En la siguiente tabla se muestra la descripción de cada ícono del dashlet.

Ícono	Nombre	Descripción
	Contraer verticalmente	Contrae el dashlet de forma vertical para que solo el título sea visible.
	Expandir verticalmente	Expande el dashlet a su tamaño original.
	Recargar	Vuelve a cargar el dashlet.
	Ajustes de configuración	Muestra ajustes configurables para el dashlet.
	Maximizar	En algunos dashlets con contenido que no cabe horizontalmente en el ancho del dashlet, maximiza un gráfico o un dashlet a pantalla completa.

Ícono	Nombre	Descripción
	Eliminar	Elimina el dashlet del tablero.
Hora de última actualización		Muestra la hora en que se sondean los datos desde el gráfico relacionado.
Ver más		Cuando se hace clic en esta opción, se navega al tablero correspondiente, el cual está vinculado al dashlet principal y muestra más detalles. Si no vinculó el tablero a un dashlet existente, este vínculo no estará disponible en el dashlet. Para configurar esta opción, haga clic en  y, en el campo Vínculo del tablero, seleccione un tablero relacionado para ver más detalles acerca del dashlet específico. **Nota:** Esta función solo está disponible para el dashlet Gráfica en tiempo real y los tableros preconfigurados en NetWitness Suite 11.0 o superior.

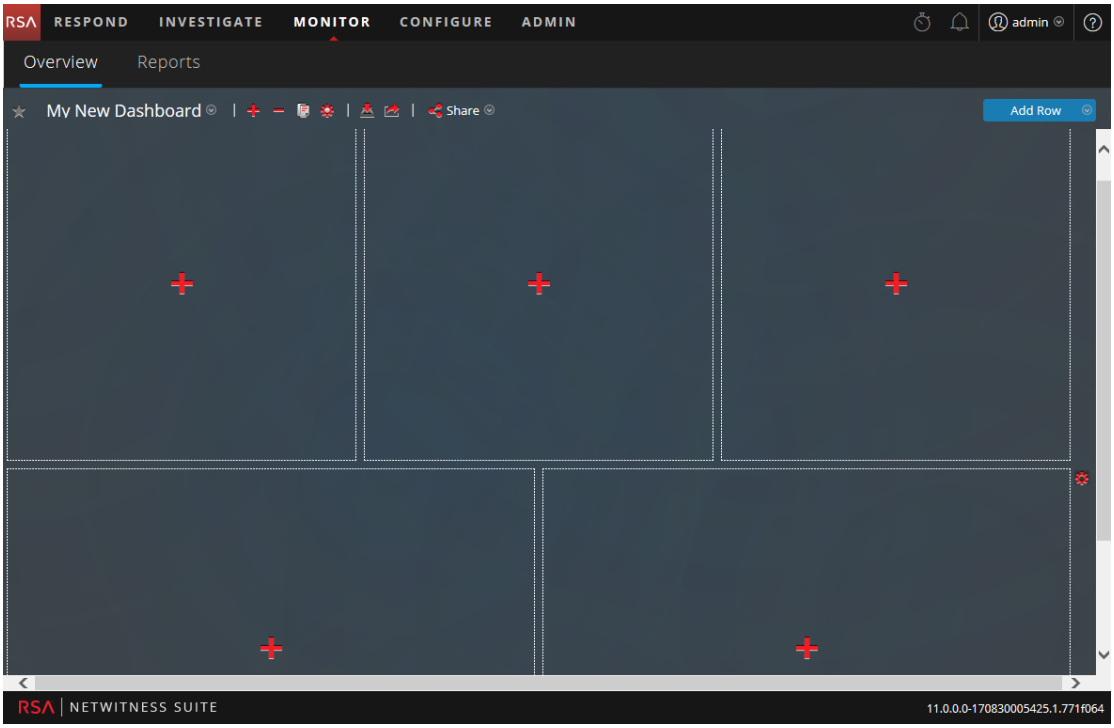
Puede agregar dashlets al tablero predeterminado o crear un tablero personalizado con su propio conjunto de dashlets útil para que el flujo de trabajo sea más eficiente.

Agregar un dashlet

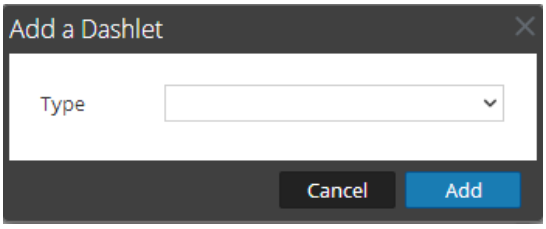
Para personalizar las vistas en NetWitness Suite, puede agregar dashlets a un tablero predeterminado o crear tableros personalizados. Sin embargo, no puede agregar dashlets a los tableros preconfigurados.

Para agregar un dashlet:

1. Navegue a cualquier tablero o cree un tablero nuevo.

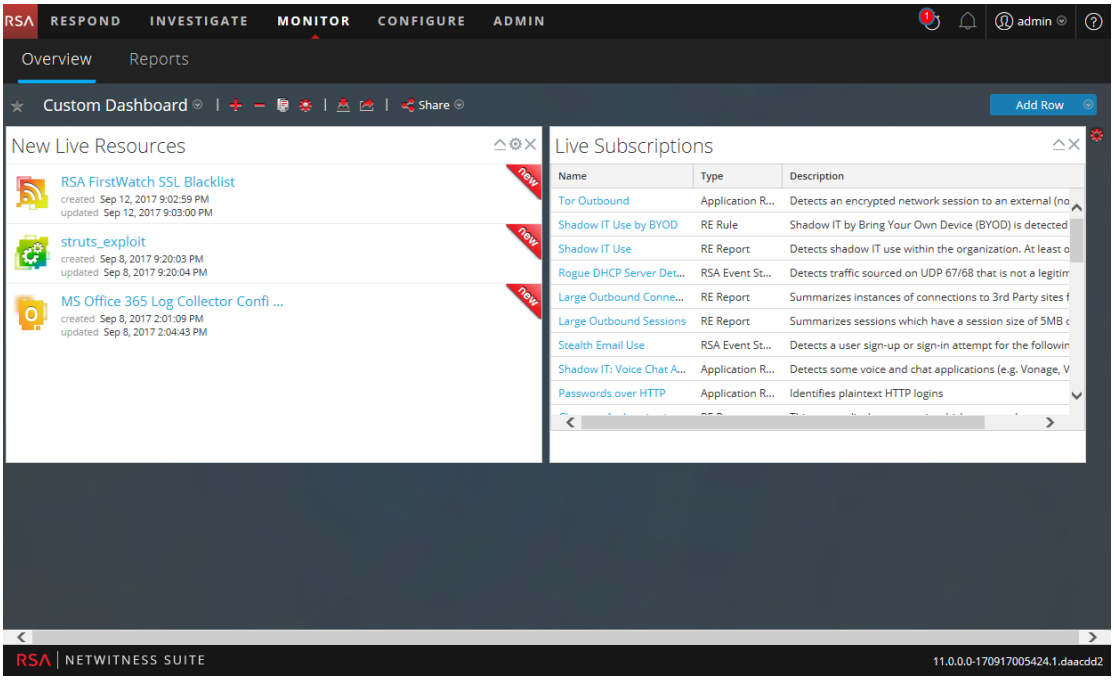


2. Haga clic en  en el marcador de posición donde desea agregar el dashlet.
   Se muestra el cuadro de diálogo Agregar un dashlet.



3. Haga clic en lista de selección **Tipo** de dashlet para ver los dashlets disponibles y seleccione el tipo de dashlet que desea agregar. Según el tipo de dashlet que está agregando, se mostrarán algunos campos configurables en el cuadro de diálogo **Agregar un dashlet**.
4. Ingrese un título para el dashlet. El título puede incluir letras, nombres, caracteres especiales y espacios.
5. Si hay campos configurables disponibles para el dashlet, configure los valores correspondientes.
6. Cuando se hayan configurado todos los campos obligatorios, haga clic en **Agregar**.
   El dashlet se agrega al tablero en el marcador de posición seleccionado y se guarda

automáticamente.



Editar las propiedades de un dashlet

Todos los dashlets preconfigurados son de solo lectura y sus propiedades no se pueden editar. Otros dashlets se pueden editar y permiten que los usuarios personalicen algunos aspectos de los datos que se muestran en ellos. Un dashlet con propiedades editables tiene un ícono de configuración ( ) que muestra todas las opciones de edición.

Una vez que se agregan, los dashlets se pueden arrastrar y soltar e intercambiar.

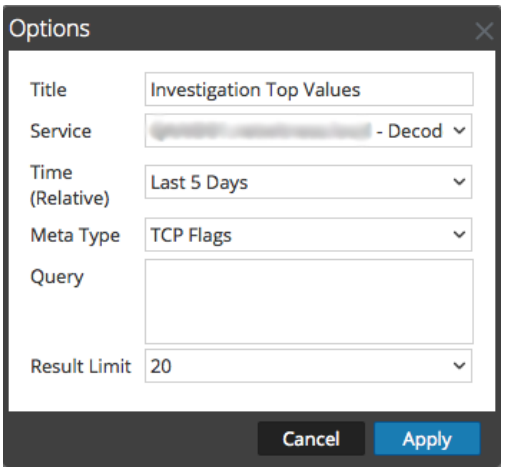
Un dashlet sin propiedades editables, como el dashlet Suscripciones de Live, no muestra la opción de configuración en la barra de título. Muchos dashlets tienen un título editable que permite editar las siguientes propiedades:

- Título de la pantalla del dashlet.
- Tipo de servicios que se monitorearán; por ejemplo, puede monitorear solo Decoders o Decoders y Concentrators.

Otros dashlets tienen parámetros que puede definir para especificar el tipo y la cantidad de información que desea ver en el dashlet. Por ejemplo, un dashlet Gráfica en tiempo real tiene la opción de configuración.

1. Para mostrar y modificar las opciones de un dashlet, haga clic en el ícono de configuración ( ) en la barra de título del dashlet.

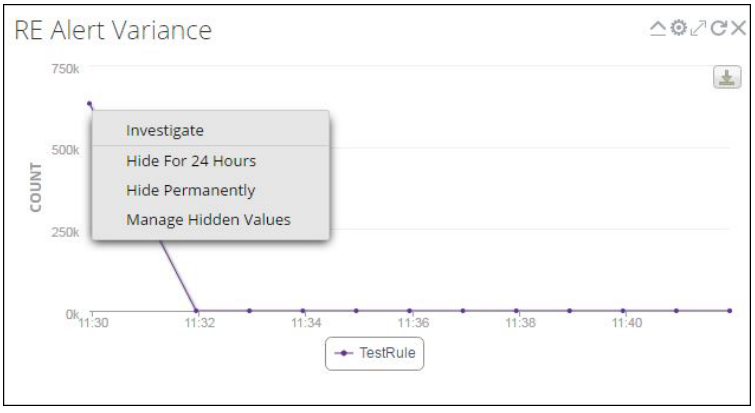
   Se muestra el cuadro de diálogo **Opciones**.



2. Edite cualquiera de las propiedades que se muestran. Por ejemplo, en un dashlet Valores principales de Investigation, puede editar el Límite de resultado de 20 a 40.
3. Haga clic en **Aplicar**.

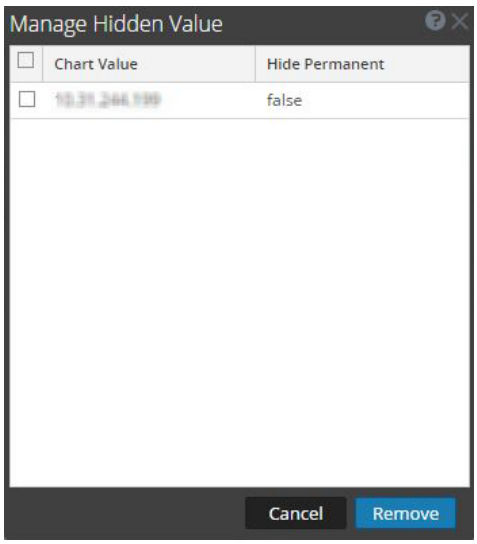
Algunos dashlets tienen opciones de configuración para adaptar la apariencia o el contenido del dashlet. Las siguientes opciones están disponibles para los dashlets Alertas principales de RE, Variación de alertas de RE y Gráficos en tiempo real de RE cuando se hace clic con el botón principal del mouse:

- **Ocultar durante 24 horas**: Esta opción permite ocultar el valor seleccionado durante las próximas 24 horas. Después de 24 horas, los datos se mostrarán automáticamente en el dashlet, si el valor se configura y se enumera en la parte superior.
- **Ocultar de forma permanente**: Esta opción permite ocultar el valor seleccionado de forma permanente hasta que lo vuelve a agregar mediante la opción Administrar valores ocultos.



- **Administrar valores ocultos**: Esta opción muestra una lista de todos los valores ocultos. Puede seleccionar la casilla de verificación correspondiente a un valor y hacer clic en **Quitar**

para volver a ver los datos en el gráfico.



Nota: Las opciones Ocultar durante 24 horas, Ocultar de forma permanente y Administrar valores ocultos no están disponibles para los gráficos de mapa geográfico.

Nota: Cuando edita un valor en un tablero preconfigurado, este es un cambio específico del usuario. Los cambios realizados en un tablero preconfigurado solo se aplicarán a su tablero y otros usuarios que usan el mismo tablero no podrán verlos. Por ejemplo, si oculta un valor en un tablero de descripción general, el cambio se aplicará solo a su tablero. Si otro usuario ve el mismo tablero de descripción general, el valor se mostrará. Lo mismo se aplica a un tablero personalizado. Cuando oculta un valor en el tablero personalizado y comparte el mismo tablero con otro usuario, los valores se muestran a pesar del uso compartido del tablero.

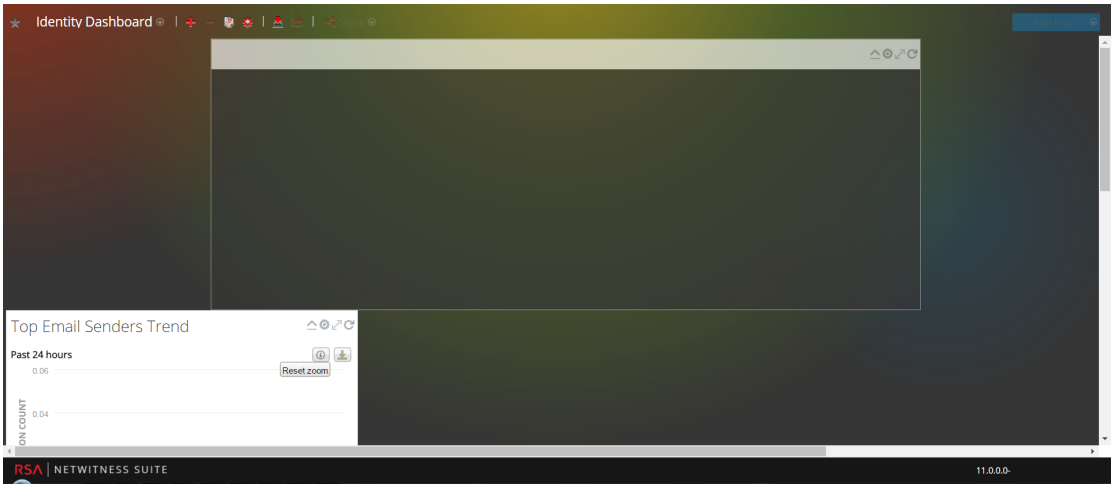
Para obtener más información sobre los tablero disponibles, consulte el Catálogo de tableros en el espacio Contenido de RSA en RSA Link.

Reorganizar un dashlet

Puede organizar los dashlets según su preferencia. Para esto, debe arrastrarlos y soltarlos en otro orden en el tablero.

1. Para mover un dashlet, mantenga el cursor sobre el encabezado del dashlet que desea mover. El cursor de dirección aparece sobre el dashlet. Haga clic y mantenga presionado el encabezado del dashlet que desee mover.
2. Siga presionando el botón izquierdo del mouse y arrastre la ventana hacia la nueva ubicación.

En la siguiente figura se muestra un dashlet que se reorganiza.



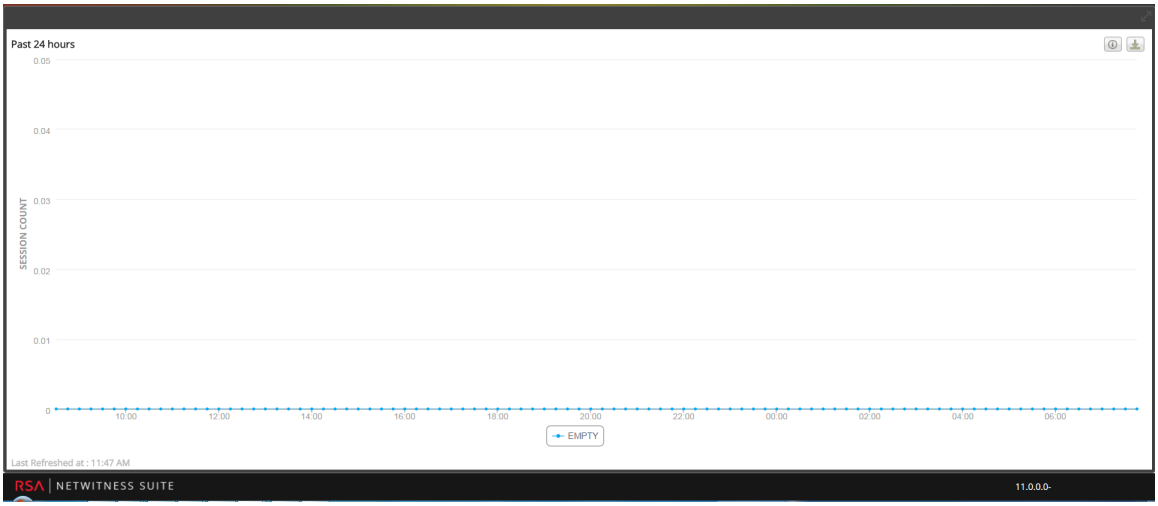
3. Suelte el botón del mouse cuando el dashlet esté en la ubicación deseada.
   El dashlet que ocupa actualmente esa posición se desplaza hacia abajo.

Maximizar un único dashlet

En esta sección se explica cómo abrir un dashlet en el área completa del tablero principal de NetWitness Suite con el mismo título del dashlet. Es más fácil ver los dashlets que tienen una gran cantidad de columnas o gráficos, por ejemplo, algunos dashlets de Reporting, cuando están maximizados. Esto permite ver todo el contenido sin necesidad de desplazarse.

Para maximizar un dashlet, haga clic en el ícono de control de maximización de la barra de título del dashlet: ⤢. El dashlet se muestra en pantalla completa.

Para minimizar un dashlet, haga clic en el mismo ícono de control de la barra de título del dashlet: ⤢. El dashlet se restaura a su tamaño anterior.



Eliminar un dashlet

1. Haga clic en ✕ en la barra de título del dashlet:

   Se muestra una ventana emergente de confirmación para confirmar su intención de eliminar el dashlet.

2. Si desea eliminarlo, haga clic en **Sí**. El dashlet se quita del tablero.
   Si no desea eliminarlo, haga clic en **No**.

Nota: Después de quitar el dashlet, el espacio vacío se reemplaza por un marcador de posición en el que puede agregar otro dashlet mediante el procedimiento Agregar un dashlet anterior.

Importación y exportación de tableros

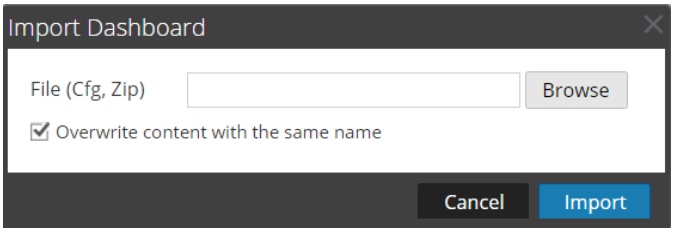
La capacidad para exportar tableros personalizados según las diferentes circunstancias y condiciones podría llevar a tener una gran cantidad de tableros que no se necesitan diariamente. En lugar de partir de cero cada vez que desee volver a crear un determinado tablero personalizado, puede exportar los tableros que no se estén utilizando actualmente. Cuando esté listo para utilizar un tablero exportado anteriormente, importe el tablero a NetWitness Suite.

Importar un tablero

Nota: Puede importar el tablero Gráficas en tiempo real de Reporter y sus gráficos relacionados en distintas instancias del servidor de NetWitness Suite y Reporting Engine desde donde se exportó.

1. En la barra de herramientas del tablero, seleccione **Importar tablero** .

   Se muestra el cuadro de diálogo **Importar tablero**.



2. Navegue al archivo de tablero en el cuadro de diálogo **Importar tablero**. Puede importar archivos .cfg y .zip.

3. Haga clic en **Importar tablero**.
   El tablero se muestra en NetWitness Suite

Nota: Si importa un tablero de Security Analytics 10.6.x en NetWitness Suite11.0, el tablero y las reglas y los gráficos asociados se deben importar por separado. Pero cuando importa un tablero de NetWitness Suite11.0 en NetWitness Suite, el tablero y todas las reglas y los gráficos asociados se importan en formato .zip.

Exportar un tablero

Los tableros exportados están diseñados para funcionar dentro de la misma instancia de NetWitness Suite. También es posible compartir los tableros personalizados con otros usuarios de la organización, siempre y cuando tengan permisos equivalentes.

Para exportar un tablero, este debe estar abierto de modo que se pueda acceder a la opción Exportar tablero del menú desplegable Editar en la barra de herramientas del tablero.

1. Vaya al tablero que desea exportar. Todos los tableros existentes aparecen en la **lista de selección de tableros** desplegable en el tablero mostrado actualmente.
2. Haga clic en Exportar tablero ( ) en la barra de herramientas del tablero.

   El archivo exportado se guarda en formato .zip.

Nota: La función Exportar no se aplica a los tableros preconfigurados.

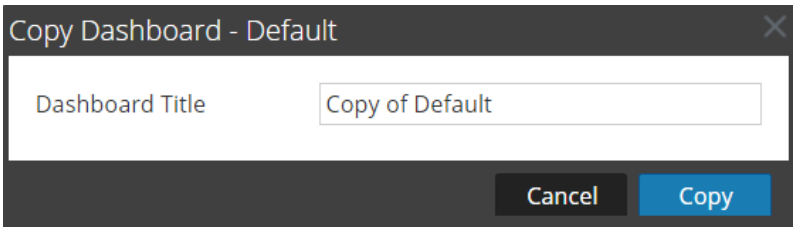
Copia de un tablero

Para personalizar las vistas de NetWitness Suite, puede copiar tableros al tablero de NetWitness o a un tablero personalizado. El tablero de NetWitness Suite, como el nombre lo sugiere, ofrece todos los dashlets de NetWitness Suite. El cuadro de diálogo Copiar tablero crea un tablero duplicado, el cual se puede personalizar. Cuando copia un tablero, al nombre predeterminado se le agregará el prefijo Copia de. Por ejemplo, si el nombre del tablero original es XYZ, el título predeterminado del tablero copiado será Copia de XYZ.

Para copiar un tablero:

1. Vaya a cualquier tablero
2. En la barra de herramientas del tablero, haga clic en .

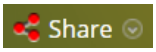
   Se muestra el cuadro de diálogo Copiar tablero: Predeterminado. La siguiente captura de pantalla es un ejemplo de la copia de un tablero.



3. Ingrese el Título de tablero.
4. Haga clic en **Copy**.

Uso compartido de un tablero

En NetWitness Suite, como administrador, puede compartir tableros con otras funciones, como administradores, analistas, operadores, etc., para su visualización. Cuando comparte un dashlet, los usuarios solo pueden ver el tablero, configurarlo como favorito, copiarlo y exportarlo. En el caso de otras funciones, como los analistas, los operadores, etc., puede compartir el tablero solo con funciones similares. Por ejemplo, un analista podrá compartir un tablero únicamente con otros analistas.

1. Vaya a cualquier tablero.
2. En la barra de herramientas del tablero, haga clic en 

y seleccione la casilla de verificación de la función con la cual desea compartir el tablero.

Nota: Si no desea compartir el tablero, deseleccione la casilla de verificación de la función.

Administración de trabajos

Inevitablemente, existen tareas, según demanda o programadas, en NetWitness Suite que tardan algunos minutos en completarse. El sistema de trabajos de NetWitness Suite le permite comenzar una tarea de ejecución prolongada y continuar utilizando otras partes de NetWitness Suite mientras el trabajo está ejecutándose. No solo puede monitorear el progreso de la tarea, sino que también puede recibir notificaciones cuando la tarea haya finalizado y si el resultado fue exitoso o falló.

Mientras está trabajando enNetWitness Suite, puede abrir una vista rápida de los trabajos desde la barra de herramientas de NetWitness Suite. Puede verla en cualquier momento, pero cuando el estado de un trabajo ha cambiado, el ícono de Trabajos () se marca con la cantidad de trabajos en ejecución. Una vez que todos los trabajos se han completado, el número desaparece.

También puede ver los trabajos en estas dos vistas.

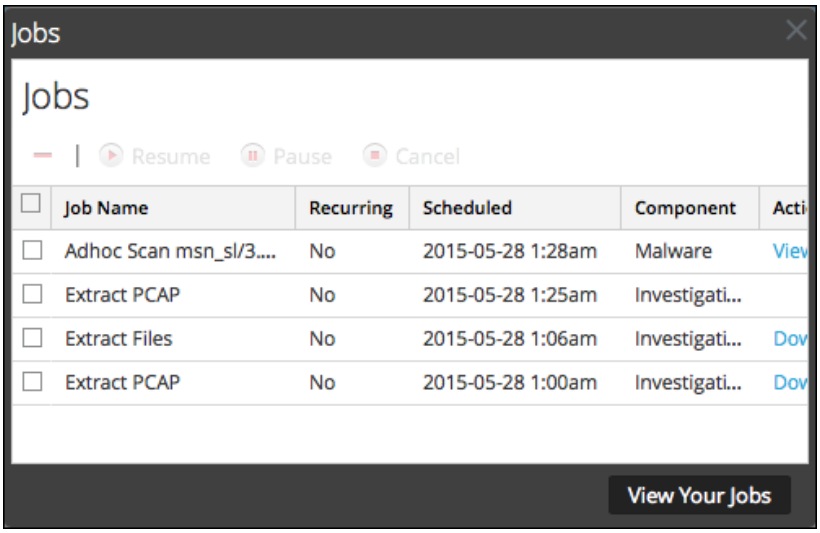
- En la vista Perfil, puede ver los mismos trabajos en un panel completo. Estos son trabajos solamente.
- En la vista Sistema, los usuarios con privilegios administrativos pueden ver y administrar todos los trabajos de todos los usuarios en un único panel de trabajos.

La estructura del panel de trabajos es igual en todas las vistas.

Mostrar la Bandeja de trabajos

En la barra de herramientas de NetWitness Suite, haga clic en el ícono Trabajos:  .

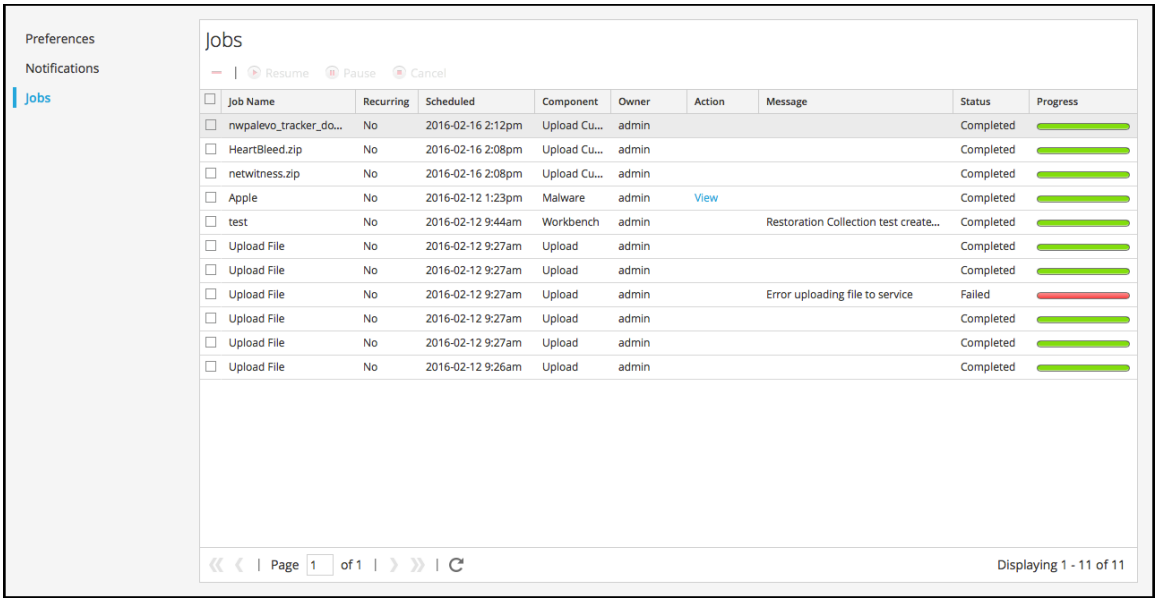
Se muestra la bandeja Trabajos.



La bandeja Trabajos muestra todos sus trabajos, recurrentes y no recurrentes, con el uso de un subconjunto de las columnas disponibles en el panel Trabajos. Por lo demás, la bandeja Trabajos y la vista Perfil > panel Trabajos son lo mismo. En la vista Sistema de Administration, el panel Trabajos muestra información acerca de todos los trabajos de NetWitness Suite de todos los usuarios.

Ver los trabajos en la vista Perfil > panel Trabajos

Para observar una vista más grande de sus trabajos, haga clic en **Ver sus trabajos**.
Se muestra la vista Perfil > panel Trabajos.



Pausar y reanudar ejecución programada de un trabajo recurrente

Las opciones Pausar y Reanudar se aplican solo a los trabajos recurrentes. Sin embargo, cuando pausa un trabajo recurrente que está en ejecución, la ejecución no se ve afectada. La próxima ejecución (si se asume que el trabajo sigue en pausa) se omite.

1. Para detener la próxima ejecución de un trabajo recurrente, en cualquier panel **Trabajos**, seleccione el trabajo y haga clic en **Pausar**.

   La siguiente ejecución del trabajo se omite y el programa se mantiene en pausa hasta que se hace clic en Reanudar.

2. Para reiniciar la ejecución de trabajos recurrentes en pausa, seleccione el trabajo y haga clic en **Reanudar**.

   La siguiente ejecución del trabajo se realiza según lo calendarizado y el calendario para el trabajo se reanuda.

Cancelar un trabajo

Para cancelar trabajos que estén en ejecución o en línea de espera para ejecutarse:

1. En la **Bandeja de trabajos** o en el panel **Trabajos**, seleccione uno o más trabajos.
2. Haga clic en **Cancelar**.

   Se muestra un cuadro de diálogo de confirmación.

3. Haga clic en **Sí**.

   Los trabajos se cancelan y las entradas permanecen en la cuadrícula con un estado de **cancelado**.

   Si cancela un trabajo recurrente, se cancela esa ejecución del trabajo. La próxima vez que se programa la ejecución del trabajo, este se ejecuta de manera normal.

Eliminar un trabajo

Precaución: Cuando elimina un trabajo, el trabajo se elimina de forma instantánea de la cuadrícula. No aparece un diálogo de confirmación. Si elimina un trabajo recurrente, también se eliminan todas las ejecuciones futuras.

Los usuarios pueden eliminar sus propios trabajos antes, durante o después de la ejecución. Los usuarios con la función ADMIN pueden eliminar cualquier trabajo. Para eliminar trabajos:

1. Seleccione uno o más trabajos.
2. Haga clic en **Eliminar**.

3. Los trabajos se eliminan de la cuadrícula.

Descargar un trabajo

Cuando un trabajo tiene el estado Descargar en la columna Acción, puede descargar el resultado del trabajo. Si está trabajando en el módulo Investigation y extrae los datos de paquete para una sesión como un archivo PCAP o extrae los archivos de carga (por ejemplo, documentos de Word e imágenes) de una sesión, se crea un archivo. Para descargar el archivo a su sistema local, haga clic en **Descargar**.

Visualización y eliminación de notificaciones

Mientras trabaja en NetWitness Suite, puede ver las notificaciones recientes del sistema sin salir del módulo en el cual está trabajando. Puede abrir una vista rápida de las notificaciones en la barra de herramientas de NetWitness Suite. Puede verla en cualquier momento, pero cuando recibe una notificación nueva, se marca el ícono Notificaciones.

Algunos ejemplos de notificaciones son:

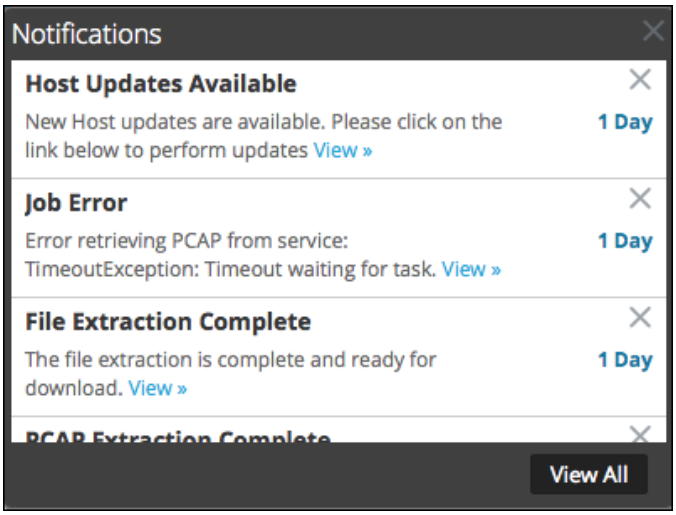
- Se completó una actualización del host.
- Una migración de analizador a decodificador que se ha completado.
- Hay disponible una versión de software más reciente.

En estas dos vistas, puede ver todas las notificaciones en un panel Notificaciones completo.

- En la vista Perfil, puede ver solo sus notificaciones.
- En la vista Sistema, los usuarios con privilegios administrativos pueden ver y administrar todas las notificaciones de todos los usuarios en un único panel.

Ver notificaciones

Para mostrar la bandeja Notificaciones, haga clic en el ícono Notificaciones ( ).

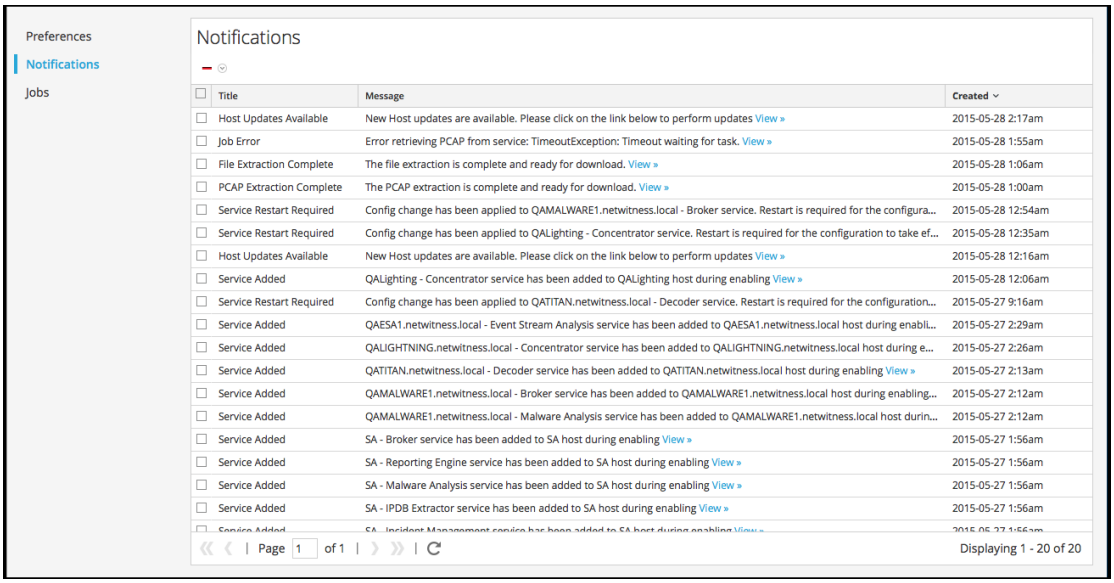


Ver todas las notificaciones

Para ver todas las notificaciones, realice una de las siguientes acciones:

1. Vaya a **Perfil** y, a continuación, en el panel de opciones de la vista Perfil, seleccione **Notificaciones**.
2. Vaya a **ADMIN > SISTEMA** y, a continuación, en el panel de opciones de la vista Sistema, seleccione **Notificaciones**.
3. Haga clic en  para abrir la bandeja Notificaciones y, a continuación, haga clic en **Ver todo** en esta bandeja.

   Se muestra el panel Notificaciones. Aquí aparecen todas las notificaciones y el formato es diferente al formato de la Bandeja de notificaciones.



Eliminar registros de notificaciones

Para eliminar registros de notificaciones:

1. En la tabla **Notificaciones de perfil**, seleccione las notificaciones que desea eliminar.
2. Haga clic en .

   Las notificaciones seleccionadas se eliminan de esta tabla y de la bandeja Notificaciones.

Visualización de la ayuda en la aplicación

Existen diferentes maneras de obtener ayuda mientras se usa NetWitness Suite. Puede usar la ayuda en pantalla, mensajes de globo y vínculos de ayuda en línea.

Ver la ayuda en pantalla

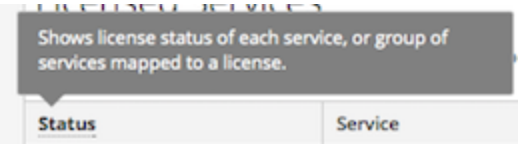
En la ayuda en pantalla se proporciona información adicional sobre lo que se debe hacer en las secciones o los campos que ve actualmente en la interfaz del usuario de NetWitness Suite. Para mostrar la ayuda en pantalla, coloque el cursor sobre . La ayuda en pantalla muestra una descripción breve del elemento.

Ejemplo de la ayuda en pantalla:

Ver mensajes de globo

Los mensajes de globo son una manera rápida de ver una descripción del texto o información adicional sobre una acción, un campo o un parámetro. Los mensajes de globo aparecen como texto subrayado. Para mostrar el mensaje de globo y ver una descripción breve del término, mantenga el mouse sobre el texto subrayado.

Ejemplo de un mensaje de globo:

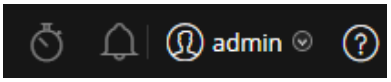


Ver la ayuda en línea

Los vínculos de la ayuda en línea lo llevan fuera de NetWitness Suite a la documentación en línea de RSA Link. Este sitio tiene un conjunto de documentación completo para NetWitness Suite y los vínculos lo llevan directamente al tema que describe la parte de la interfaz del usuario que está activa en la vista.

Para ver el tema de la ayuda en línea correspondiente a la ubicación actual, haga clic en en la barra de herramientas de NetWitness Suite o en un cuadro de diálogo. El tema de ayuda pertinente se muestra en una ventana del navegador por separado. En él se describen las características y las funciones de la vista o el cuadro de diálogo actuales. Desde ese tema, puede navegar rápidamente a los procedimientos relacionados.

La siguiente figura es un ejemplo del ícono de la ayuda en línea en la barra de herramientas de NetWitness Suite.



Búsqueda de documentos en RSA Link

La documentación de RSA NetWitness® Suite se encuentra en RSA Link, el portal y la comunidad de soporte de RSA. RSA Link reúne todos los recursos de RSA en un solo lugar. Incluye asesorías, documentación de productos, artículos de la base de conocimientos, descargas y capacitación. Para ver un *Recorrido guiado por RSA Link*, consulte https://community.rsa.com/videos/21554.

Localizar la documentación de NetWitness Suite

La documentación de registros y paquetes de NetWitness Suite está en el siguiente vínculo: https://community.rsa.com/docs/DOC-40370

Para navegar a la documentación de registros y paquetes de NetWitness Suite:

1. En la página de inicio de RSA Link (https://community.rsa.com), haga clic en **RSA NETWITNESS SUITE**.
2. En la página de RSA NetWitness Suite, haga clic en **DOCUMENTATION** y seleccione **RSA NETWITNESS LOGS AND PACKETS**.

Para navegar a la documentación de NetWitness Endpoint:

1. En la página de inicio de RSA Link (https://community.rsa.com), haga clic en **RSA NETWITNESS SUITE**.
2. En la página de RSA NetWitness Suite, haga clic en **DOCUMENTATION** y seleccione **RSA NETWITNESS ENDPOINT**.

Localizar contenido de RSA

El contenido de RSA está en el siguiente vínculo: https://community.rsa.com/community/products/netwitness/rsa-content

Para navegar al contenido de RSA:

1. En la página de inicio de RSA Link (https://community.rsa.com), haga clic en **RSA NETWITNESS SUITE**.
2. En la página de RSA NetWitness Suite, haga clic en **DOCUMENTATION** y seleccione **ADDITIONAL RESOURCES** > **RSA CONTENT**.

Localizar orígenes de eventos compatibles con RSA

Los orígenes de eventos compatibles con RSA están en el siguiente vínculo: https://community.rsa.com/community/products/netwitness/parser-network/event-sources

Para navegar a los orígenes de eventos compatibles con RSA:

1. En la página de inicio de RSA Link (https://community.rsa.com), haga clic en **RSA NETWITNESS SUITE**.
2. En la página de RSA NetWitness Suite, haga clic en **DOCUMENTATION** y seleccione **ADDITIONAL RESOURCES** > **EVENT SOURCE CONFIGURATION**.

Localizar guías de instalación de hardware

Las guías de instalación de hardware están en el siguiente vínculo: https://community.rsa.com/community/products/netwitness/hardware-setup-guides

1. En la página de inicio de RSA Link (https://community.rsa.com), haga clic en **RSA NETWITNESS SUITE**.
2. En la página de RSA NetWitness Suite, haga clic en **DOCUMENTATION** y seleccione **ADDITIONAL RESOURCES** > **HARDWARE SETUP GUIDES**.

Buscar documentos mediante NetWitness Navigator

Puede buscar la documentación de RSA NetWitness Suite que desea en RSA Link mediante la herramienta NetWitness Navigator.

1. En la página de inicio de RSA Link (https://community.rsa.com), haga clic en **RSA NETWITNESS SUITE**.
2. En PRODUCT RESOURCES (lado derecho de la página), haga clic en **RSA NetWitness Navigator**.
3. Seleccione los criterios de búsqueda que desea entre las opciones disponibles. Cuando busca documentación, debe seleccionar **User Documentation** como el tipo de contenido. Además, la opción Cost no se aplica a la documentación del usuario.
4. Haga clic en **VIEW RESULTS** para ver una lista de documentos coincidentes.
5. Haga clic en **RESET OPTIONS** para borrar las opciones de búsqueda anteriores.

Seguir el contenido para enterarse de las actualizaciones

Puede seguir páginas o documentos para recibir notificaciones sobre los cambios.

1. Inicie sesión en RSA Link.
2. Navegue a una página o a un documento y, en la esquina superior derecha, seleccione **Follow** o **Actions** > **Follow**.

Enviar sus comentarios a RSA

Sus comentarios son muy importantes para nosotros y nos ayudan a proporcionar una mejor experiencia para nuestros clientes. Envíe sus sugerencias a sahelpfeedback@rsa.com.

Referencias de introducción de NetWitness Suite

La siguiente sección contiene información de referencia de la interfaz del usuario relacionada con la introducción a la aplicación NetWitness Suite.

- Preferencias de usuario
- Panel Notificaciones y Bandeja de notificaciones
- Panel Trabajos y Bandeja de trabajos

Preferencias de usuario

Para que NetWitness Suite se ajuste de la mejor manera posible al ambiente y a las prácticas de trabajo, puede configurar preferencias globales propias para la aplicación. Puede:

- Configurar la zona horaria de la aplicación
- Configurar los formatos de fecha y hora (solo en la vista Respond)
- Seleccionar la ubicación de inicio predeterminada (solo en la vista Respond)
- Cambiar su contraseña
- Habilitar notificaciones
- Habilitar menús contextuales
- Cambiar las preferencias de Investigate, como se describe en la *Guía del usuario de Investigation y Malware Analysis*.

Sus opciones de preferencias globales varían en función de si accede a ellas desde la vista Respond o de otras vistas, como Investigate, Monitor, Configurar y Admin.

Nota: Los procedimientos de preferencias de usuario marcados con “vista Respond” y “solo en la vista Respond” también se pueden realizar en algunas vistas de Investigate.

¿Qué desea hacer?

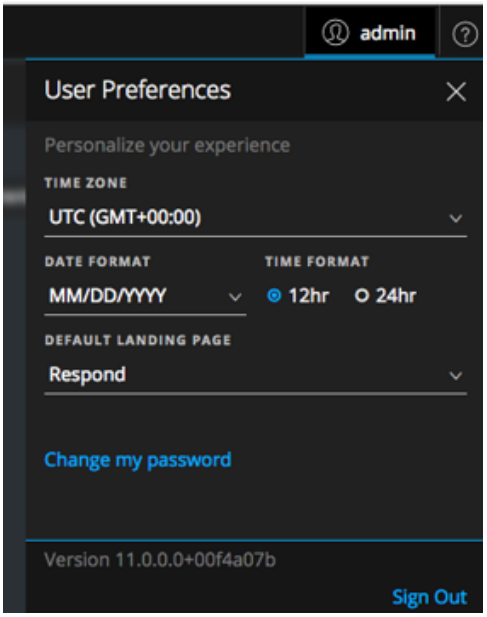
Función	Deseo…	Mostrarme cómo
Todas	Cambiar mi contraseña	Cambiar mi contraseña
Todas	Elegir la página principal predeterminada	Configuración de la vista predeterminada de acuerdo con la función del SOC
Todas	Configurar las preferencias del usuario	Configuración de las preferencias del usuario

Temas relacionados

- Navegación básica en NetWitness Suite

Preferencias de usuario (vista Respond)

Para acceder a las preferencias de usuario, haga clic en .
En el cuadro de diálogo Preferencias de usuario se muestran las preferencias actuales y la versión de NetWitness Suite. La barra de menú principal muestra la preferencia de la zona horaria actual junto con el ícono del perfil de usuario.



En la siguiente tabla se describen las opciones de preferencias globales de la aplicación a las que puede acceder desde la vista Respond.

Opción	Descripción
Zona horaria	Configura la zona horaria que se usará en NetWitness Suite.
Formato de fecha	Configura el formato para el orden de visualización del mes (MM), el día (DD) y el año (AAAA). Por ejemplo, MM/DD/AAAA muestra la fecha en el formato 05/11/2017.
Formato de hora	Configura la hora en formato de 12 o 24 horas. Por ejemplo, las 2:00 p. m. en el formato de 12 horas son las 14:00 h en el formato de 24 horas.

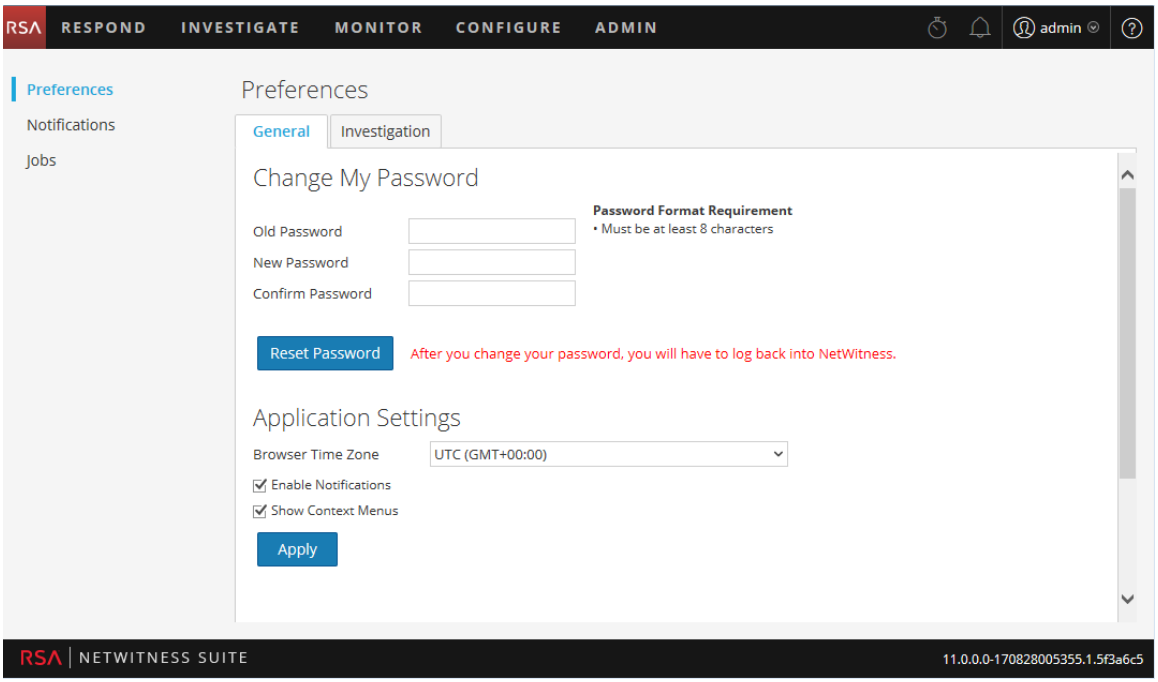
Opción	Descripción
Página principal predeterminada	Permite seleccionar la vista predeterminada cuando inicia sesión en NetWitness Suite. Según su función de usuario, puede elegir Respond, Investigate, Monitor, Configurar y Admin. Por ejemplo, puede elegir Respond para ir directamente a la sección que corresponde a los encargados de responder ante incidentes de la aplicación. Esta selección configura la vista predeterminada para toda la aplicación.
Cambiar mi contraseña	Abre el cuadro de diálogo Preferencias, en el cual puede cambiar su contraseña.
Versión	Muestra la versión de NetWitness Suite.
Cerrar sesión	Permite cerrar la sesión de NetWitness Suite.

Todas las selecciones que hace se aplican de inmediato.

Preferencias

Para acceder a las preferencias de usuario, realice una de las siguientes acciones:

- Para la mayoría de las vistas, como Investigate, Monitor, Configurar o Admin, vaya a  > **Perfil**.
- En la vista Respond, seleccione  y, en el cuadro de diálogo Preferencias de usuario, haga clic en **Cambiar mi contraseña**
  El cuadro de diálogo Preferencias muestra las preferencias actuales.



En las siguientes tablas se describen las opciones de preferencias globales de la aplicación a las que puede acceder desde estas vistas.

Cambiar mi contraseña

Esta sección permite cambiar su contraseña. El administrador define los requisitos apropiados de seguridad de la contraseña para su contraseña de NetWitness Suite, como la longitud mínima de la contraseña y la cantidad mínima de caracteres en mayúscula, en minúscula, decimales, alfabéticos no latinos y especiales. A continuación, estos requisitos se muestran cuando se cambia la contraseña.

En las siguientes tablas se describen las opciones de la sección Cambiar mi contraseña.

Opción	Descripción
Old Password	Escriba la contraseña que usó para iniciar sesión en NetWitness Suite.
Nueva contraseña	Escriba la contraseña que desea usar para el próximo inicio de sesión.
Confirmar contraseña	Vuelva a escribir la contraseña nueva.

Opción	Descripción
Restablecer contraseña	Actualiza el perfil de usuario con la nueva contraseña. Se cerrará su sesión de NetWitness Suite para que se apliquen los cambios. La contraseña nueva entra en vigor la próxima vez en que inicia sesión en NetWitness Suite. El cambio de contraseña se aplica al inicio de sesión en el sistema y en todos los servicios de NetWitness Suite en los cuales se agregó la cuenta.

Si cambió su contraseña, se cerrará su sesión de NetWitness Suite para que se apliquen los cambios. La contraseña nueva entra en vigor la próxima vez en que inicia sesión en NetWitness Suite.

Configuración de aplicación

En la siguiente tabla se describen las opciones de la sección Configuración de aplicación.

Opción	Descripción
Zona horaria del navegador	Configura la zona horaria que se usará en NetWitness Suite. La preferencia de zona horaria se muestra en la barra de herramientas.
Habilitar notificaciones	Esta casilla de verificación activa o desactiva notificaciones para su cuenta de usuario. De manera predeterminada, las notificaciones del sistema de NetWitness Suite se habilitan cuando se crea una nueva cuenta de usuario.
Habilitar menús contextuales	Esta casilla de verificación activa o desactiva menús contextuales para su cuenta de usuario. De manera predeterminada, los menús contextuales de se habilitan cuando se crea una nueva cuenta de usuario. Los menús contextuales proporcionan funciones adicionales para vistas específicas cuando hace clic con el botón secundario en una vista.
Aplicar	Actualiza las preferencias y aplica los cambios de inmediato.

Panel Notificaciones y Bandeja de notificaciones

NetWitness Suite proporciona notificaciones del sistema para informar a los usuarios acerca de ciertas acciones o condiciones.

- Se completó una actualización del host.
- Una migración de analizador a decodificador que se ha completado.
- Un servicio quedó inactivo (registro crítico de un tipo específico).
- Finalizó una visualización.
- Finalizó un informe.
- Hay disponible una versión de software más reciente.

Mientras trabaja en NetWitness Suite, puede ver las notificaciones recientes del sistema sin salir del módulo en el cual está trabajando. Puede abrir una vista rápida de las notificaciones en la barra de herramientas de NetWitness Suite. Puede verla en cualquier momento, pero cuando recibe una notificación nueva, se marca el ícono Notificaciones.

Cuando vea notificaciones en la Bandeja de notificaciones, solo aparecerán las notificaciones recientes. Puede ver todas las notificaciones en un formato de tabla en la vista Perfil o en la vista Sistema. En Visualización y eliminación de notificaciones se presentan procedimientos para ver notificaciones.

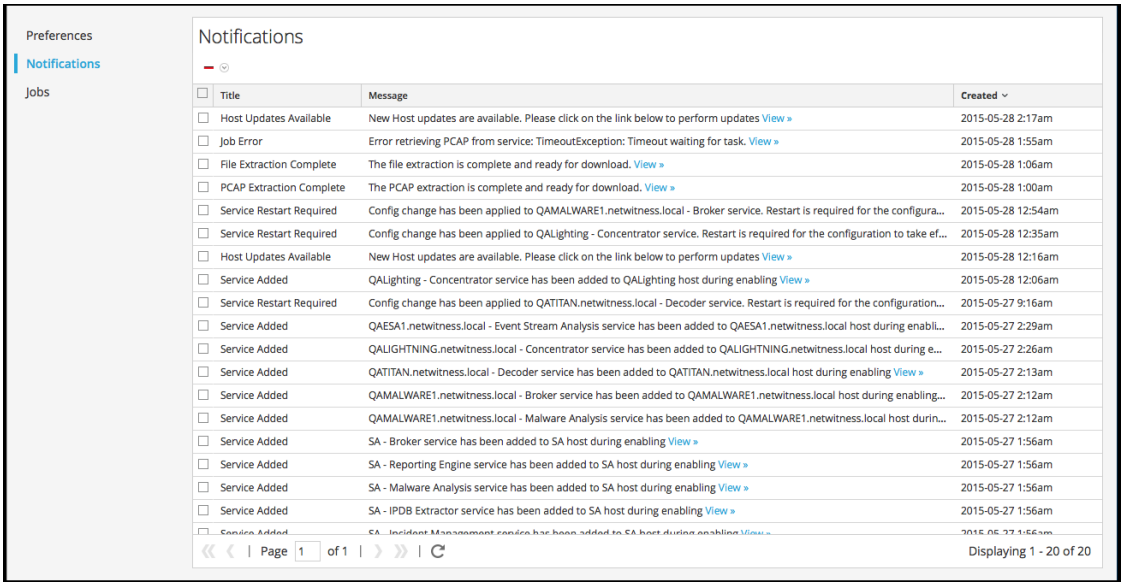
¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Todo	Ver todas las notificaciones	Visualización y eliminación de notificaciones
Todo	Eliminar notificaciones	Visualización y eliminación de notificaciones

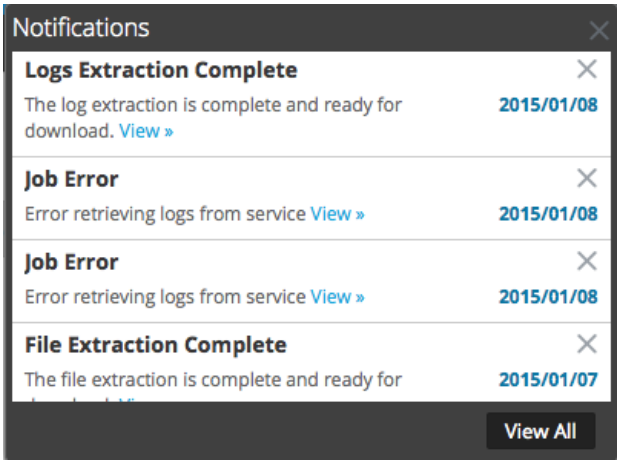
Para acceder al panel Notificaciones, realice una de las siguientes acciones:

- Vaya a **Perfil** y, a continuación, en el panel de opciones de la vista Perfil, seleccione **Notificaciones**.

- Vaya a **ADMIN > SISTEMA** y, a continuación, en el panel de opciones de la vista Sistema, seleccione **Notificaciones**.



- Haga clic en  y, a continuación, haga clic en **Ver todo** en la bandeja Notificaciones.



El panel y la bandeja Notificaciones tienen una barra de herramientas y una tabla. La Bandeja de notificaciones es un subconjunto de la información que se presenta en el panel Notificaciones. En la siguiente tabla se describen las funciones del panel Notificaciones.

Función	Descripción
	Muestra un menú desplegable que permite eliminar los registros de notificación seleccionados o todos los registros de notificación en la tabla **Notificaciones** y en la bandeja Notificaciones.
Título	El título de la notificación, por ejemplo, **Extracción de archivo completa**.
Mensaje	Todo el mensaje, por ejemplo, **La extracción de archivo está completa y lista para descarga.**
Ver	Algunos mensajes incluyen un vínculo que muestra una vista en la que puede tomar medidas. Por ejemplo, si hay un archivo para descargar, cuando se hace clic en este vínculo, se abre el panel Trabajos que muestra la vista donde puede descargar el archivo.
Creado	La fecha y la hora en que se creó la notificación. En la bandeja Notificaciones, esta columna es la cantidad de días desde que se creó la notificación.
Ver todo	Muestra la tabla Notificaciones de la vista Perfil.

Panel Trabajos y Bandeja de trabajos

Varios módulos de NetWitness Suite inician trabajos; por ejemplo, el módulo Live puede descargar recursos de CMS, el módulo Administration puede cargar un feed en un servicio y el módulo Investigation puede analizar y reconstruir paquetes en archivos de captura de paquetes.

En la vista Sistema de Administration, los usuarios del grupo ADMIN pueden administrar todos los trabajos de NetWitness Suite en el panel Trabajos. Otros usuarios no administrativos pueden ver sus propios trabajos en la vista Perfil.

Además, mientras está trabajando en NetWitness Suite, puede abrir una vista rápida de los trabajos desde la barra de herramientas de NetWitness Suite. Cuando el estado de un trabajo ha cambiado, el ícono de Trabajos () se marca con la cantidad de trabajos en ejecución. Una vez que todos los trabajos se han completado, el número desaparece.

En el panel Trabajos, puede:

- Ver y ordenar los trabajos
- Pausar o reanudar un trabajo
- Cancelar un trabajo
- Eliminar un trabajo
- Descargar un trabajo

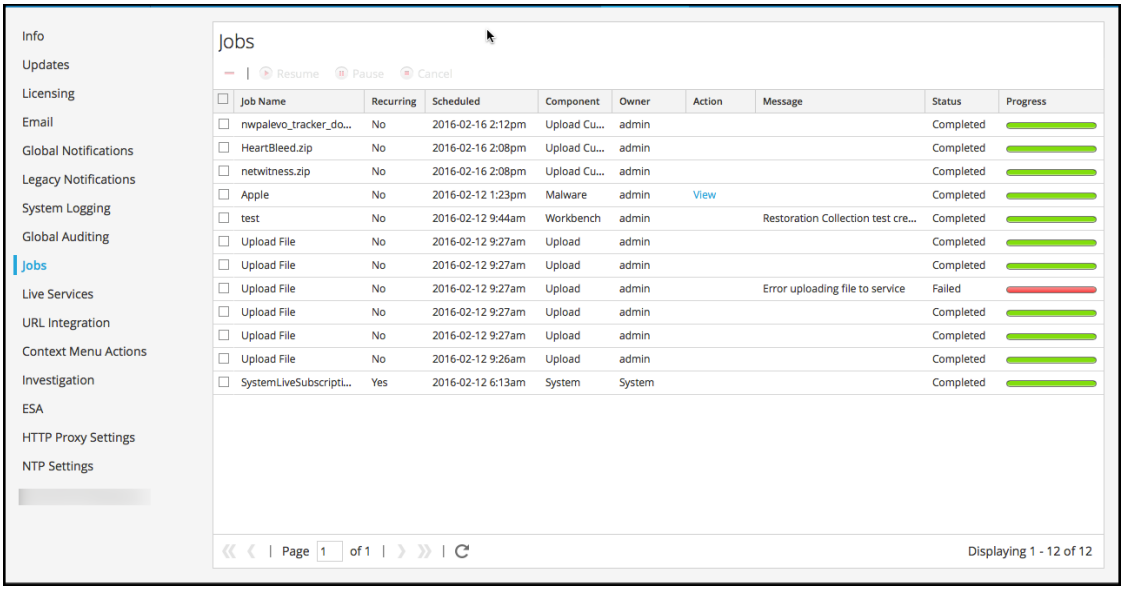
La estructura del panel de trabajos es igual en todas las vistas.

¿Qué desea hacer?

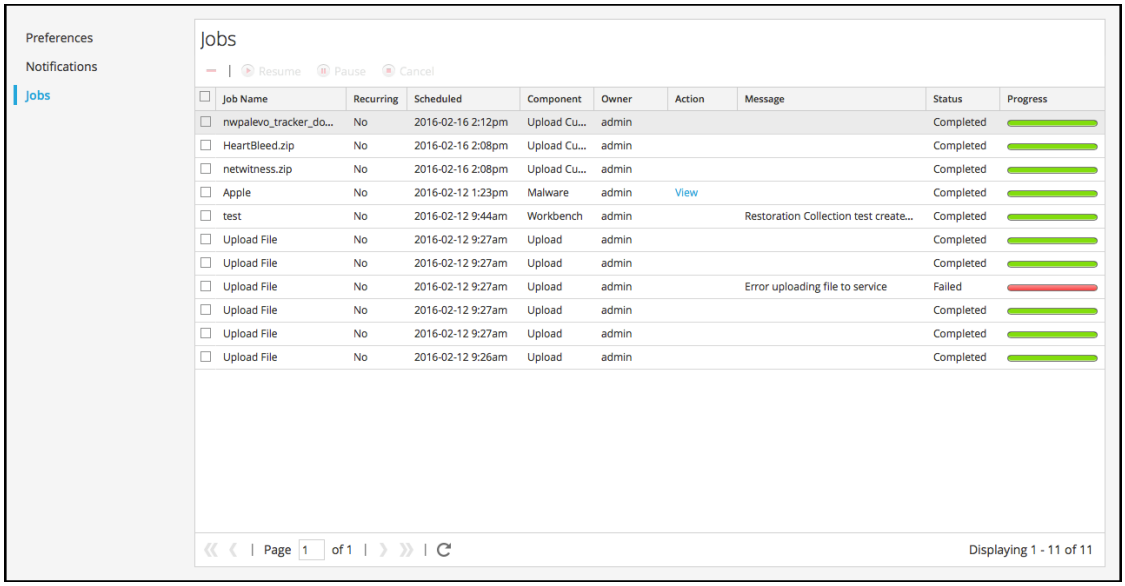
Función	Deseo…	Mostrarme cómo
Todo	Pausar y reanudar un trabajo programado	Administración de trabajos
Todo	Cancelar o eliminar un trabajo	Administración de trabajos
	Descargar un trabajo	Administración de trabajos

Para acceder al panel Trabajos, realice una de las siguientes acciones:

- Vaya a **ADMIN > SISTEMA** y, en el panel de opciones, seleccione **Trabajos**.

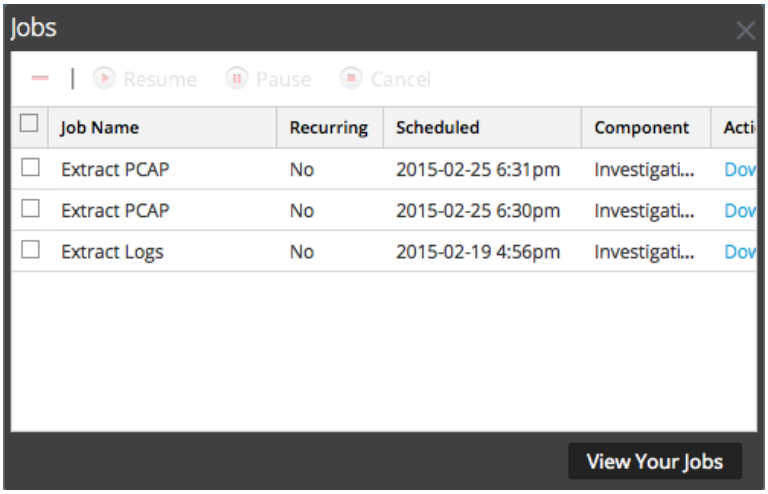


- Vaya a **Perfil** y, en el panel de opciones, seleccione **Trabajos**.



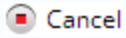
El panel Trabajos organiza la información acerca de los trabajos en una cuadrícula. Las columnas presentan una barra de progreso del trabajo, el nombre del trabajo, una indicación de que el trabajo es recurrente o no recurrente, el módulo de NetWitness Suite que controla el trabajo, el propietario del trabajo, el estado, cualquier mensaje asociado y un botón de descarga que permite descargar archivos de captura de paquetes o archivos de carga útil de un trabajo.

Para mostrar la Bandeja de trabajos, haga clic en el ícono **Trabajos** .



La bandeja Trabajos muestra todos sus trabajos, recurrentes y no recurrentes, con el uso de un subconjunto de las columnas disponibles en el panel **Trabajos**. Por lo demás, la bandeja Trabajos y la vista Perfil > panel Trabajos son lo mismo. En la vista Sistema de Administration, el panel Trabajos muestra información acerca de todos los trabajos de NetWitness Suite de todos los usuarios.

En la siguiente tabla se describen las opciones del panel Trabajos.

Función	Descripción
	La opción Reanudar se aplica solo a los trabajos recurrentes que están en pausa. Cuando reanuda un trabajo pausado, la próxima ejecución del trabajo se realiza según lo programado.
	La opción Pausar se aplica solamente a los trabajos recurrentes. Cuando pausa un trabajo recurrente que está en ejecución, la ejecución no se ve afectada. La próxima ejecución (si se asume que el trabajo sigue en pausa) se omite.
	Cancela un trabajo recurrente o no recurrente. Puede cancelar un trabajo mientras está en ejecución. Si cancela un trabajo recurrente, se cancela esa ejecución del trabajo. La próxima vez que se programa la ejecución del trabajo, este se ejecuta de manera normal.
	Elimina un trabajo recurrente o no recurrente del panel **Trabajos**. Cuando elimina un trabajo, este se elimina instantáneamente del panel Trabajos. No aparece un diálogo de confirmación. Si elimina un trabajo recurrente, también se eliminan todas las ejecuciones futuras.

En la siguiente tabla se describen las funciones de la Bandeja de trabajos y del panel Trabajos.

Función	Descripción
Cuadro de selección	Haga clic en este cuadro para seleccionar uno o más trabajos.
Progreso	Muestra el porcentaje completado de un trabajo.
Nombre del trabajo	Muestra el nombre del trabajo; por ejemplo, **Extraer archivos** o **Actualizar servicio**.
Recurrente	Indica si el trabajo es recurrente o no recurrente. **Sí** = recurrente, **No** = no recurrente.

Función	Descripción
Componente	Indica el componente en el cual se originó el trabajo; por ejemplo, **Investigation** o **Administration**.
Propietario	Indica el propietario del trabajo. El propietario del trabajo no está incluido en la **Bandeja de trabajos** predeterminada, ya que solo se muestran aquí los trabajos del usuario actual. La columna está disponible para agregarla.
Estado	Indica el estado del trabajo. Los valores comunes para el estado son **En pausa**, **En ejecución**, **Cancelado**, **Fallido**, **Completado**, mientras que también es posible tener otros valores de estado.
Mensaje	Muestra información adicional sobre el trabajo; por ejemplo, **Extracción de archivos** o **No se encontraron sesiones**.
Acción	Visualiza trabajos en las vistas Investigation y Malware Analysis, o descarga archivos de trabajos para el trabajo en el directorio **Descargas** predeterminado del sistema local. Solo los trabajos completados correctamente tienen el vínculo **Ver** en la columna **Acción**. Solo los trabajos que crean un archivo tienen el vínculo **Descargar** en la columna **Acción**.
Ver sus trabajos	Muestra trabajos en la **vista Perfil > panel Trabajos.**
Programado	Indica la fecha y hora en la que se calendarizó el inicio del trabajo.