RSA NETWITNESS® SUITE

Guía de configuración de Malware Analysis

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

Cómo funciona Malware Analysis

NetWitness Suite Malware Analysis es un procesador de análisis de malware automatizado que analiza determinados tipos de objetos de archivos (como portable ejecutable de Windows (PE), PDF y MS Office) para evaluar la probabilidad de que un archivo sea malicioso.

Malware Analysis detecta indicadores de riesgo mediante el uso de cuatro metodologías de análisis distintas:

- Análisis de sesión de red (red)
- Análisis de archivo estático (estático)
- Análisis de archivo dinámico (Sandbox)
- Análisis de seguridad comunitario (comunidad)

Cada una de las cuatro metodologías de análisis está diseñada para compensar las debilidades inherentes de las demás. Por ejemplo, el análisis de archivo dinámico puede compensar los ataques de día cero que no se detectan durante la fase de análisis de seguridad comunitario. Al evitar análisis de malware que se concentran estrictamente en una metodología, el analista tiene más probabilidades de protegerse contra falsos negativos en los resultados.

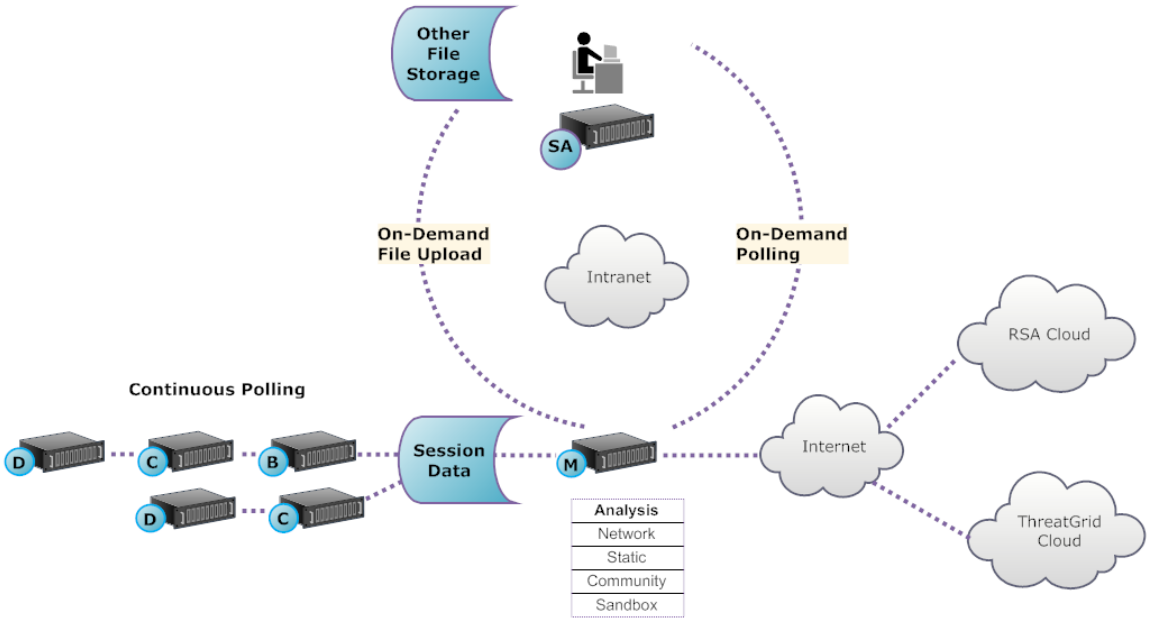
Además de los indicadores de riesgo incorporados, Malware Analysis es compatible con indicadores de riesgo escritos en YARA. YARA es un lenguaje de reglas que permite a los investigadores de malware identificar y clasificar muestras de malware. Esto permite que los autores de IOC agreguen funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live. Estos IOC basados en YARA en RSA Live se descargarán y se habilitarán automáticamente en el host suscrito con el fin de complementar el análisis existente que se ejecuta en cada archivo analizado.

Malware Analysis también tiene características compatibles con alertas para Incident Management.

Descripción funcional

En esta figura se ilustra la relación funcional entre los servicios principales (Decoder, Concentrator y Broker), el servicio Malware Analysis y el Servidor de NetWitness.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



El servicio Malware Analysis analiza objetos de archivos mediante cualquier combinación de los siguientes métodos:

- **Sondeo automático continuo de un Concentrator o un Broker** para extraer sesiones que identificó un analizador como posibles portadoras de contenido de malware.
- **Sondeo según demanda de un Concentrator o un Broker** para extraer sesiones que identificó un analista de malware como posibles portadoras de contenido de malware.
- **Carga según demanda de archivos** de una carpeta especificada por el usuario.

Cuando se habilita el sondeo automático de un Concentrator o un Broker, el servicio Malware Analysis extrae y da prioridad continuamente al contenido ejecutable, documentos PDF y documentos de Microsoft Office en su red, directamente de los datos que capturó y analizó el servicio Security Analytics Core. Dado que el servicio Malware Analysis se conecta a un Concentrator o un Broker para extraer solo los archivos ejecutables que están marcados como posible malware, el proceso es rápido y eficiente. Este proceso es continuo y no requiere monitoreo.

Si selecciona el sondeo según demanda de un Concentrator o un Broker, el analista de malware usa Security Analytics Investigation para desglosar a los datos capturados y seleccionar las sesiones que se analizarán. El servicio Malware Analysis utiliza esta información para sondear automáticamente el Concentrator o el Broker y descargar las sesiones especificadas para el análisis.

La carga según demanda de archivos proporciona un método para que el analista revise los archivos capturados de manera externa a la infraestructura de Core. El analista de malware selecciona una ubicación de carpeta e identifica uno o más archivos con el fin de cargarlos y someterlos al análisis de Security Analytics Malware Analysis. Estos archivos se analizan con el uso de la misma metodología que los archivos que se extraen automáticamente de las sesiones de red.

Método de análisis

Para el análisis de red, el servicio Malware Analysis busca características que parezcan desviarse de la norma, de manera muy similar a lo que hace un analista. Al observar cientos de miles de funciones y combinar los resultados en un sistema de puntaje ponderado, las sesiones legítimas que por coincidencia tienen algunos rasgos anormales se omiten, mientras que las sesiones realmente maliciosas se destacan. Un usuario puede aprender patrones que indican actividad anómala en las sesiones, como indicadores que requieren una investigación más detallada o indicadores de riesgo.

El servicio Malware Analysis puede ejecutar el análisis estático de objetos sospechosos que detecte en la red y determinar si esos objetos contienen código malicioso. En el caso del análisis comunitario, el nuevo malware detectado en la red se envía a RSA Cloud para compararlo con los análisis de malware propios de RSA y feeds de SANS Internet Storm Center, SRI International, el Departamento del tesoro y VeriSign. En el caso del análisis de Sandbox, los servicios también pueden enviar datos a importantes hosts de información de seguridad y administración de eventos (SIEM) (ThreatGrid Cloud).

Security Analytics Malware Analysis cuenta con un método de análisis exclusivo que se basa en asociaciones con líderes y expertos del sector, de modo que sus tecnologías puedan enriquecer el sistema de puntaje de Security Analytics Malware Analysis.

Acceso del Servidor de NetWitness al servicio Malware Analysis

El Servidor de NetWitness está configurado para conectarse al servicio Security Analytics Malware Analysis e importar datos etiquetados para un análisis más profundo en Security Analytics Investigation. El acceso se basa en tres niveles de suscripción.

- Suscripción gratuita: Todos los clientes de NetWitness Suite tienen una suscripción gratuita con una clave de prueba gratuita para análisis de ThreatGrid. El servicio Malware Analysis tiene un límite de 100 muestras de archivo por día. La cantidad de muestras (dentro del conjunto de archivos anterior) enviadas a la nube de ThreatGrid para el análisis de Sandbox se limita a cinco por día. Si una sesión de red tuviera 100 archivos, los clientes alcanzarían el límite después de procesar esa sesión de red. Si los 100 archivos se cargaran manualmente, se alcanzaría el límite.

- Nivel de suscripción estándar: La cantidad de envíos al servicio Malware Analysis es ilimitada. La cantidad de muestras enviadas a la nube de ThreatGrid para el análisis de Sandbox es de 1,000 por día.
- Nivel de suscripción empresarial: La cantidad de envíos al servicio Malware Analysis es ilimitada. El número de muestras enviadas a ThreatGrid Cloud para el análisis de Sandbox es de 5,000 por día.

Método de puntaje

De manera predeterminada, los indicadores de riesgo (IOC) se ajustan para reflejar las mejores prácticas del sector. Durante el análisis, los IOC que se activan hacen que el puntaje aumente o disminuya para indicar la probabilidad de que la muestra sea maliciosa. El ajuste de los IOC se expone en NetWitness Suite para que el analista de malware pueda elegir si desea sobrescribir el puntaje asignado o deshabilitar la evaluación de un IOC. El analista tiene la flexibilidad de usar el ajuste predeterminado o de personalizarlo completamente de acuerdo con necesidades específicas.

Los IOC basados en YARA se entrelazan con los IOC incorporados dentro de cada categoría incorporada y no se distinguen de los IOC nativos. Cuando los IOC se muestran en la vista Configuración de servicio, los administradores pueden seleccionar YARA en la lista de selección Módulo para ver una lista de reglas YARA.

Después de que se importa una sesión a NetWitness Suite, todas las funcionalidades de visualización y análisis de Security Analytics Investigation quedan disponibles para realizar un análisis más detallado de los indicadores de riesgo. Cuando se muestran en Investigation, los IOC de YARA se diferencian de los IOC nativos incorporados por la etiqueta `Yara rule.`.

Implementación

El servicio Security Analytics Malware Analysis se implementa como un host de RSA Malware Analysis independiente. El host de Malware Analysis exclusivo cuenta con un Broker incorporado que se conecta a la infraestructura de Security Analytics Core (que puede ser otro Broker o un Concentrator). Antes de esta conexión, se debe agregar un conjunto de analizadores y feeds a los Decoders que están conectados a los Concentrators y los Brokers desde los cuales extrae datos el servicio Malware Analysis. Esto permite que los archivos de datos sospechosos se marquen para extracción. Estos archivos son contenido etiquetado como `malware analysis` que está disponible a través del sistema de administración de contenido de RSA Live.

Módulos de puntaje

RSA NetWitness Suite Malware Analysis analiza y asigna puntajes a las sesiones y a los archivos integrados dentro de estas según cuatro categorías de puntaje: Red, Análisis estático, Comunidad y Sandbox. Cada categoría comprende muchas reglas y comprobaciones individuales que se usan para calcular un puntaje entre 1 y 100. Cuanto más alto es el puntaje, más probable es que la sesión sea maliciosa y que amerite una investigación de seguimiento más profunda.

Security Analytics Malware Analysis puede facilitar una investigación histórica de los eventos que conducen a una alarma o un incidente en la red. Si sabe que cierto tipo de actividad está ocurriendo en su red, puede seleccionar solo los informes de interés para examinar el contenido de recopilaciones de datos. También puede modificar el comportamiento de cada categoría de puntaje de acuerdo con la categoría de puntaje o el tipo de archivo (Windows PE, PDF y Microsoft Office).

Una vez que se haya familiarizado con los métodos de navegación de datos, podrá explorar los datos de manera más completa con:

- Búsqueda de tipos de información específicos
- Revisión de contenido específico en detalle.

Los puntajes de categoría de Red, Análisis estático, Comunidad y Sandbox se mantienen y se informan de manera independiente. Cuando los eventos se visualizan según los puntajes independientes, siempre que una categoría detecte malware, es evidente en la sección Análisis.

Red

La primera categoría examina cada sesión de red principal de Security Analytics Core para determinar si la distribución de los candidatos de malware era sospechosa. Por ejemplo, software benigno que se descarga desde un site seguro conocido, utilizando puertos y protocolos adecuados, se considera menos sospechoso que descargar software que se sabe que es malicioso desde un site de descarga dudoso. Los factores de muestra que se usan en el puntaje de este conjunto de criterios pueden incluir sesiones que:

- Contienen información de feed de amenazas
- Se conectan a sitios maliciosos bien conocidos
- Se conectan a dominios/países de alto riesgo (por ejemplo, el dominio .cc)
- Usan protocolos bien conocidos en puertos no estándar
- Contienen JavaScript oculto

Análisis estático

La segunda categoría analiza cada archivo de la sesión en busca de señales de ocultamiento para predecir la probabilidad de que el archivo se comporte de manera maliciosa si se ejecuta. Por ejemplo, software que se vincula con bibliotecas en red tiene más probabilidades de ejecutar actividades sospechosas en la red. Los factores de muestra que se usan en el puntaje de este conjunto de criterios pueden incluir:

- Archivos codificados con XOR
- Archivos detectados incorporados dentro de formatos que no son .EXE (por ejemplo, si se encuentra un archivo PE incorporado dentro de un formato GIF)
- Archivos que se vinculan a bibliotecas de importación de alto riesgo
- Archivos que se desvían considerablemente del formato PE

Comunidad

La tercera categoría asigna puntaje a la sesión y los archivos de acuerdo con el conocimiento colectivo de la comunidad de seguridad. Por ejemplo, los archivos cuya huella digital/hash ya se ha identificado como buena o maliciosa por proveedores de antivirus (AV) respetables reciben el puntaje que corresponde según eso. Los archivos también reciben puntaje según el conocimiento de que un archivo provenga de un sitio conocido como bueno o malicioso por la comunidad de seguridad.

El puntaje de la comunidad también indica si el antivirus de su red marcó los archivos como maliciosos. No indica que el producto antivirus residente actuara para proteger su sistema.

Sandbox

La cuarta categoría examina el comportamiento del software ejecutándolo en un ambiente de Sandbox. Al ejecutar el software para observar su comportamiento, se puede calcular un puntaje según la identificación de actividad maliciosa bien conocida. Por ejemplo, software que se configura a sí mismo para iniciarse automáticamente en cada reinicio y establecer conexiones IRC tendría un puntaje más alto que un archivo que no presente un comportamiento malicioso conocido.

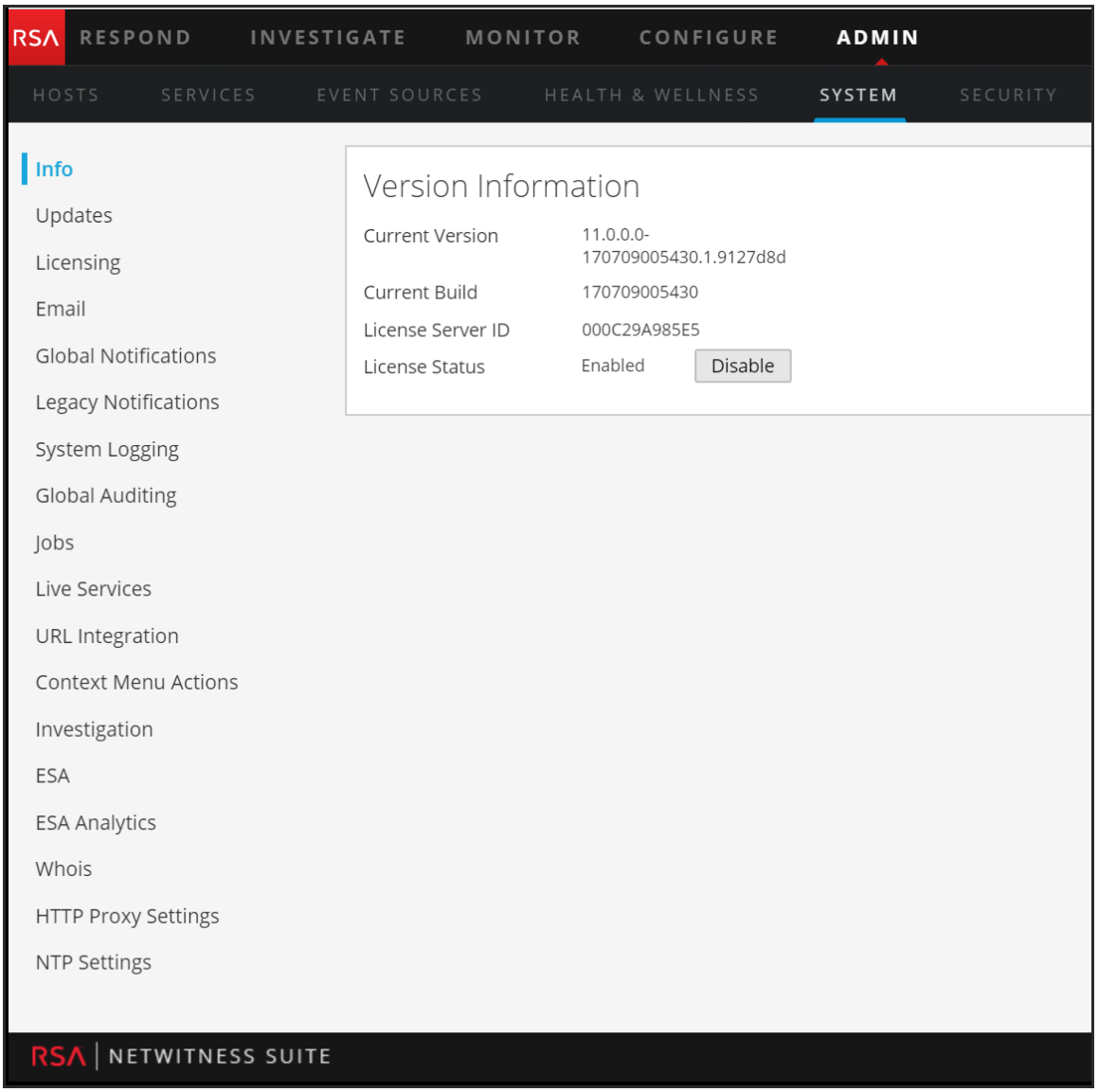
Funciones y permisos para los analistas

En este tema se identifican las funciones y los permisos que se necesitan para que un usuario realice análisis de malware en NetWitness Suite. Si no puede realizar una tarea de análisis o abrir una vista, es posible que el administrador necesite ajustar las funciones y los permisos configurados para usted.

Funciones y permisos requeridos

RSA NetWitness Suite administra la seguridad mediante el acceso a las vistas y las funciones con el uso de permisos del sistema y permisos de servicios individuales.

En el nivel del sistema, es necesario que se asigne al usuario una función del sistema, en la vista Administration > Sistema, que proporcione acceso a vistas y funciones específicas.



A la función predeterminada de `Malware_Analysts` en NetWitness Suite 11.0 se asignan todos los permisos que se enumeran a continuación. Si es necesario, un administrador puede crear una función personalizada con alguna combinación de los siguientes permisos:

- Acceder al módulo Investigation (requerido)
- Investigation: navegar por los eventos
- Investigation: navegar por los valores
- Acceder al módulo Incident
- Ver y administrar incidentes
- Ver eventos de malware (para ver eventos)

- Descarga de archivos (para descargar archivos desde el servicio Malware Analysis)
- Iniciar escaneo de malware (para iniciar un escaneo de servicio de una sola vez o una carga de archivos de una sola vez)
- Permisos de dashlet para mayor comodidad: Dashlet - Investigar dashlet de valores principales, Dashlet - Investigar dashlet de lista de servicios, Dashlet - Investigar dashlet de trabajos, Dashlet - Investigar dashlet de accesos directos.

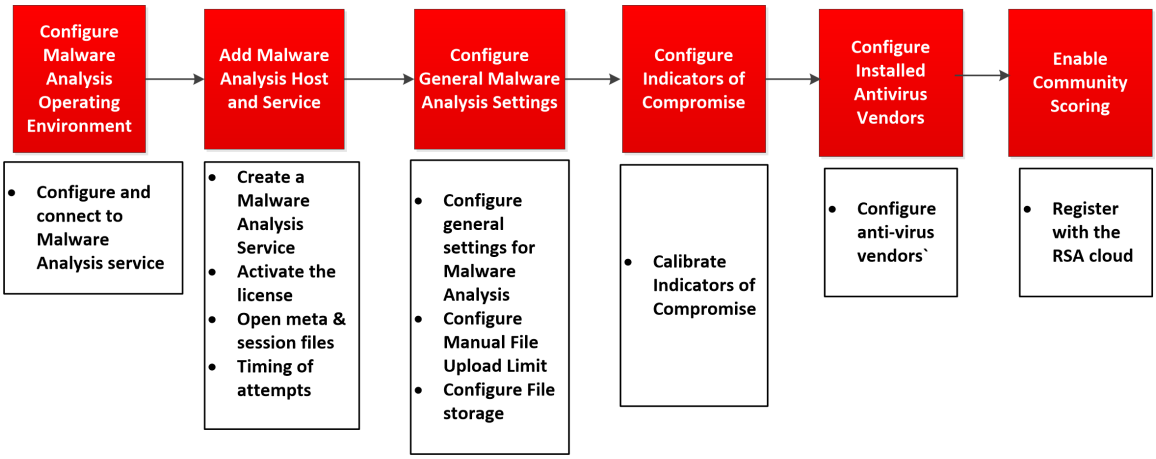
Un caso de uso para la creación de una función personalizada sería una función Analista de malware junior, con permisos limitados que no incluyen el permiso de descarga de archivos.

En servicios específicos, un analista de malware debe ser miembro del grupo **Analistas** o de un grupo que tenga los dos permisos predeterminados asignados al grupo Analista: **sdk.meta** y **sdk.content**. Los usuarios que tienen estos permisos pueden usar aplicaciones específicas, ejecutar consultas y ver el contenido para fines de análisis del servicio.

Configuración de Malware Analysis

Malware Analysis puede actuar como un servicio en un Decoder o como un servicio en un dispositivo exclusivo. En esta guía se incluyen instrucciones para configurar el ambiente operativo y, a continuación, configurar el servicio Malware Analysis. Una vez que esta configuración está lista, los analistas pueden realizar análisis de malware.

Estos son los pasos de configuración necesarios para Malware Analysis, así como para editar la configuración. Realice los pasos de la sección en la secuencia que se muestran.



Lista de verificación de la configuración básica

En la siguiente lista de verificación se proporciona la secuencia de las tareas que se requieren para configurar Malware Analysis que se agregó a NetWitness Suite de acuerdo con la *Guía de hosts y servicios*.

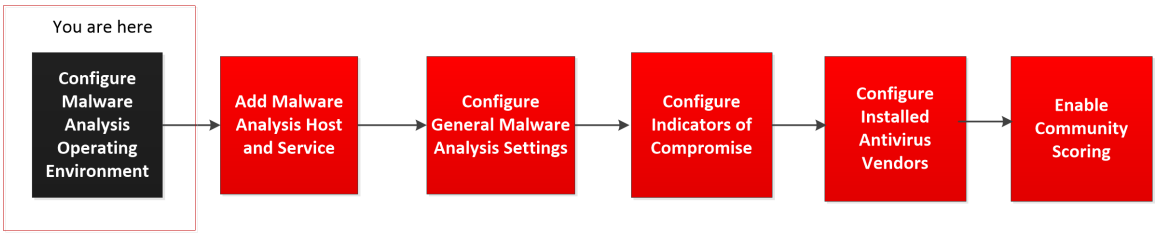
Paso	Tarea general
Paso 1: Configurar el ambiente operativo de Malware Analysis	Configurar el ambiente operativo de Malware Analysis En este tema se describen los procedimientos para configurar el ambiente necesario para conectarse al servicio Malware Analysis.

Paso	Tarea general
Paso 2: Agregar un host y un servicio Malware Analysis	Agregar un host y un servicio Malware Analysis **Nota:** Para completar este paso, debe tener la configuración del servidor de licencia de NetWitness Suite, como se describe en la Guía de licencia. En NetWitness Suite, cree un servicio Malware Analysis y active la licencia. El puerto REST predeterminado es 60007. Los sitios que usan la versión gratuita de Malware Analysis deben configurar la dirección IP del servicio como localhost o loopback.
Paso 3: Configurar ajustes generales de Malware Analysis	Configurar ajustes generales de Malware Analysis • Active el sondeo continuo. • Configure el límite de carga manual de archivos. • Configure el repositorio de almacenamiento de archivos y la base de datos. • Calibre los módulos de puntaje Estático, Red, Community y Sandbox.
Paso 4: Configurar los indicadores de riesgo	Configurar los indicadores de riesgo Calibre los Indicadores de riesgo que se aplican para cada módulo de puntaje (Estático, Red, Community y Sandbox) y para IOC basados en YARA.
Paso 5: Configurar los proveedores de antivirus instalados	Configurar los proveedores de antivirus instalados
Paso 6: Habilitar el puntaje de Community	Habilitar el análisis de Community Regístrese en RSA Cloud y pruebe las conexiones para habilitar el puntaje de la comunidad.
Paso 7: Configurar la auditoría en un host de Malware Analysis	(Opcional) Configurar la auditoría en un host de Malware Analysis Configure los umbrales de auditoría y habilite la auditoría de syslog, SNMP y archivo.

Paso	Tarea general
Paso 8: Configurar el filtro de hash	(Opcional) Configurar el filtro de hash Configure el filtrado de hash para optimizar el análisis de eventos de Malware Analysis en función de hashes de archivo legítimos o maliciosos conocidos.
Paso 9: Configurar ajustes de proxy de Malware Analysis	(Opcional) Configurar ajustes de proxy de Malware Analysis (Opcional) Configure Malware Analysis para que se comunique con RSA Cloud a través de un proxy web en lugar de hacerlo directamente.
Paso 10: Registrarse para una clave de API de ThreatGrid	(Opcional) Registrarse para una clave de API de ThreatGrid

Configurar el ambiente operativo de Malware Analysis

Puede configurar el ambiente operativo de NetWitness Suite para conectarse a un servicio NetWitness Suite Malware Analysis.



Malware Analysis funciona como un servicio en un dispositivo Malware Analysis exclusivo. Si el sitio usa un dispositivo exclusivo, realice una de las siguientes acciones:

- Si el sitio agrega un nuevo dispositivo NetWitness Suite Malware Analysis exclusivo, instale el dispositivo físico en su red y configure el ambiente operativo.
- Si el sitio actualiza un dispositivo Spectrum exclusivo a un dispositivo NetWitness Suite Malware Analysis exclusivo, vuelva a crear la imagen del dispositivo Spectrum como un dispositivo de Malware Analysis.

Malware Analysis depende de la infraestructura de Core para funcionar. Los siguientes pasos son necesarios para que Malware Analysis pueda analizar datos correctamente.

1. Configure el Broker incorporado en el dispositivo Malware Analysis para conectar otro Broker o Concentrator a la infraestructura de Core existente.

   Nota: Si la infraestructura de Core no existe, solo se pueden analizar los archivos cargados de forma manual.

2. Use NetWitness Suite Live para buscar todos los recursos de Live con la etiqueta `malware analysis`, e implemente estos recursos en cada servicio Decoder que capturará tráfico para las funciones de análisis de Malware Analysis. NetWitness Suite usa este conjunto de analizadores y feeds de propiedad para buscar eventos que probablemente correspondan a malware.
3. Configure los puertos de comunicaciones. Malware Analysis requiere que diversos puertos de comunicación estén abiertos, incluido TCP/443 para HTTPS. Estos puertos se describen más adelante en Conexiones de red.
4. Configure el origen de NextGen con el cual se conectará Malware Analysis. Este es el Broker o el Concentrator.
   Malware Analysis ya está listo para comenzar a analizar el tráfico de red.

Conexiones de red

Las conexiones de red entrantes y salientes se deben configurar para que el dispositivo Malware Analysis se comunique correctamente con los servicios, los orígenes de RSA para las actualizaciones de software y otra información importante.

El firewall de la red se debe configurar para permitir el acceso de Malware Analysis a Internet. De ser necesario, se pueden usar servidores proxy para facilitar estas conexiones.

Conexiones entrantes

TCP/22: Acceso del protocolo SSH al servidor de Malware Analysis para revisar archivos de registro y solucionar problemas. El acceso se puede limitar a las direcciones IP que administrarán Malware Analysis.

- TCP/443: Conexión web HTTPS para acceder a la interfaz del usuario de Malware Analysis.
- TCP/50008: puerto JMX para solucionar problemas de rendimiento mediante el uso de una aplicación como JVisualVM. Es opcional y el acceso se puede limitar a las direcciones IP que administrarán Malware Analysis.

Conexiones salientes

- TCP/443: conexiones HTTPS con servidores web basados en SSL. Entre algunas de las funciones, se incluye que Malware Analysis envíe archivos o documentos a servidores para

el análisis, lo cual requiere una conexión segura. Compatible con el uso de un servidor proxy web.

- (TCP/443: Conexión SSL desde Malware Analysis a RSA Cloud. Se admite el uso de un servidor proxy SOCKS. Pueden ser necesarios cambios en la infraestructura del cliente para garantizar que el puerto 443 esté abierto para cloud.netwitness.com).
- TCP/50103: Puerto de la API REST que se usa para comunicarse con un Broker (NetWitness Suite 10.3.x y anterior).
- TCP/50105: Puerto de la API REST que se usa para comunicarse con un Concentrator (NetWitness Suite 10.3.x y anterior).
- TCP/50003 TCP/56003: Puertos que se usan para comunicarse con un Broker (NetWitness Suite 10.4 y superior).
- TCP/50005 TCP/56005: Puertos que se usan para comunicarse con un Concentrator (NetWitness Suite 10.4 y superior).
- Conexión ICMP-JMS desde NetWitness Suite al servicio Malware Analysis para verificar si la dirección IP y el nombre de host ingresados son válidos para una conexión de prueba correcta.

Agregar un host y un servicio Malware Analysis

Puede agregar un host y un servicio Malware Analysis a NetWitness Suite. El ambiente de NetWitness Suite determina la forma en que se agrega un host. Consulte las instrucciones básicas para agregar un host (Agregar o actualizar un host) en la Guía de introducción de hosts y servicios. Use el procedimiento de esta sección solo si necesita agregar manualmente un host de Malware Analysis.

Nota: Para completar este paso, debe tener la configuración del servidor de licencia de NetWitness Suite, como se describe en la Guía de licencia.

- Agregue un host de Malware Analysis si hay un dispositivo de Malware Analysis físico o virtual.

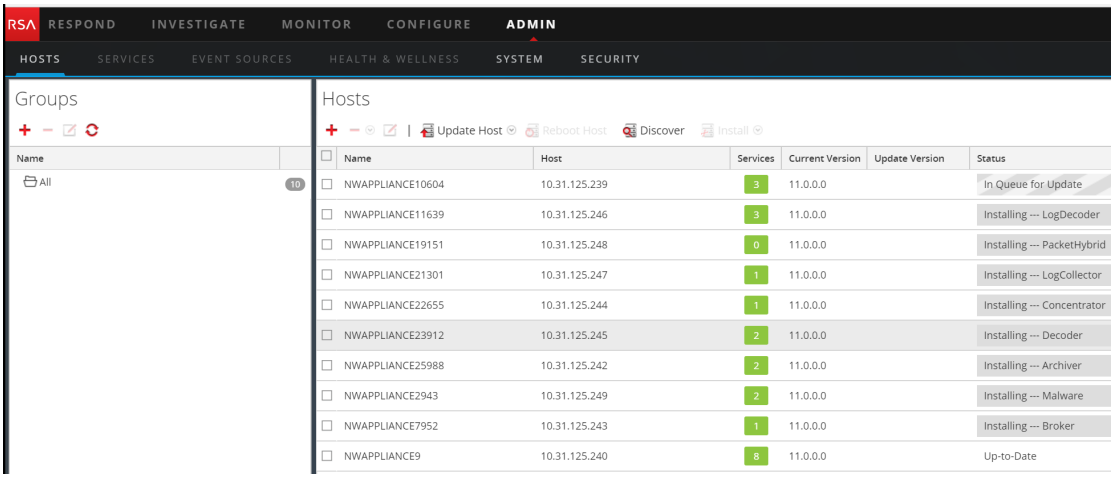
Requisito previo

Para agregar un host y un servicio en NetWitness Suite, debe haberse realizado la configuración de las operaciones y debe haber una instancia de NetWitness Suite instalada y en ejecución.

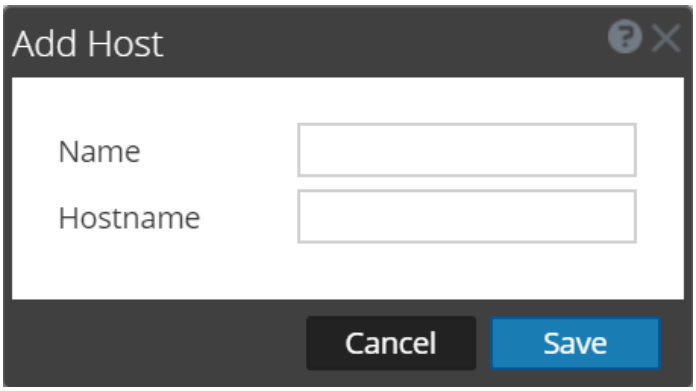
Procedimiento

Para agregar manualmente un host de Malware Analysis a NetWitness Suite:

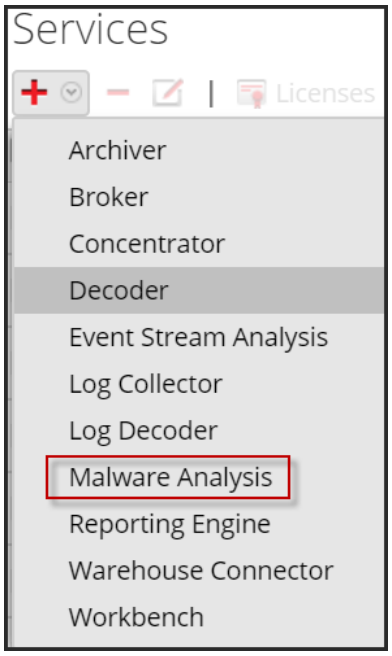
1. Inicie sesión en NetWitness Suite.
2. En el menú principal, seleccione **Administration > Hosts**. Se muestra la vista Administration > Hosts.



3. En la barra de herramientas del panel Hosts, haga clic en  .
   Se muestra el cuadro de diálogo Agregar host.

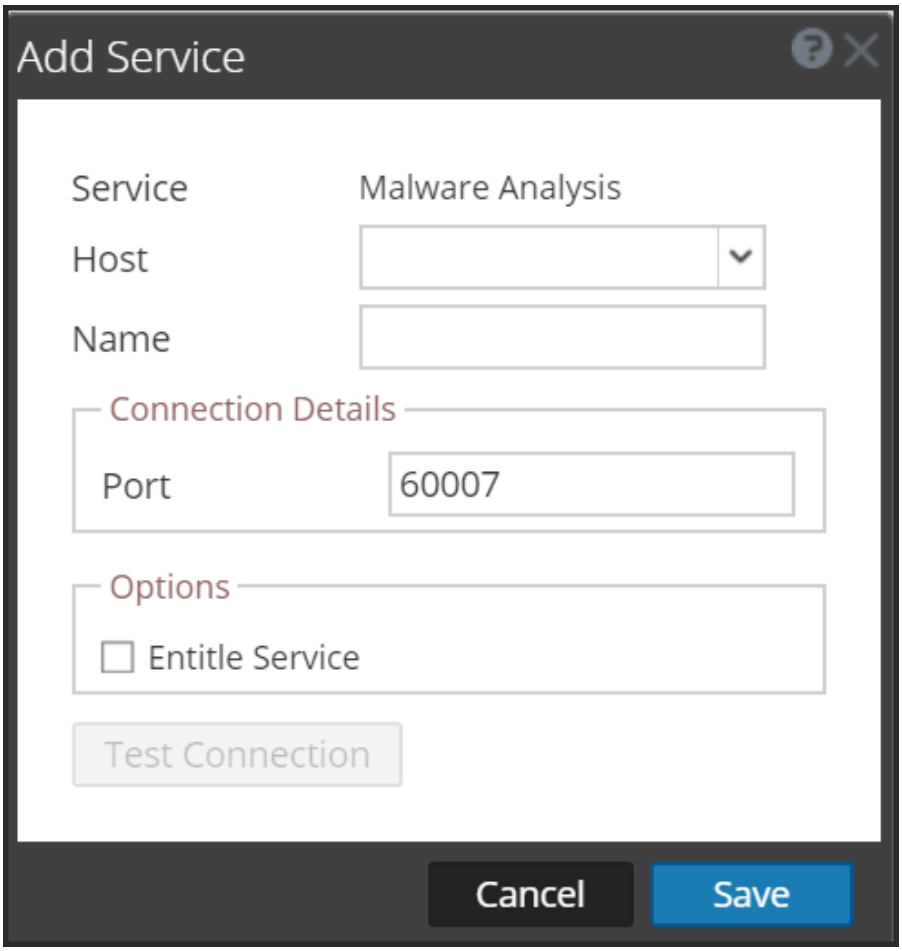


4. En el campo **Nombre**, ingrese un nombre para el host de Malware Analysis. En el campo **Nombre del host**, ingrese el nombre del host, la dirección IP virtual o la dirección IP en Malware Analysis. Haga clic en **Guardar**.
5. En la barra de herramientas, seleccione **Servicios**.
6. En la barra de herramientas del panel **Servicios**, haga clic en  y seleccione **Malware Analysis** en la lista desplegable resultante de servicios disponibles.



El cuadro de diálogo Agregar servicio se muestra con el tipo de servicio Malware Analysis

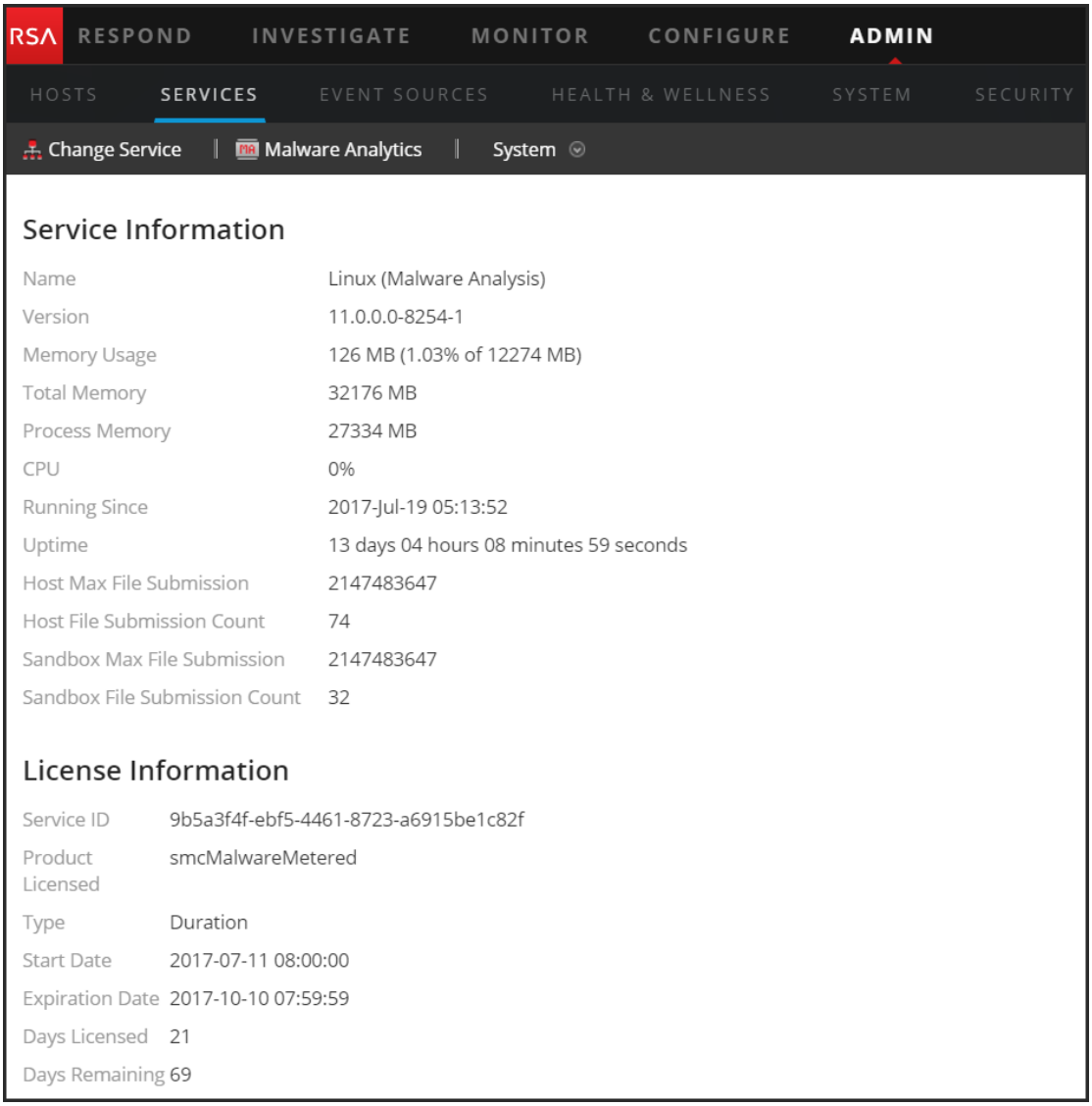
7. Ingrese la siguiente información:
   En el campo **Nombre**, ingrese un nombre para el servicio Malware Analysis.
   En el campo **Host**, ingrese el nombre del host, la dirección IP virtual o la dirección IP en Malware Analysis.
   En el campo **Puerto**, ingrese **60007**.
   (Opcional) En **Opciones**, seleccione **Conferir autorizaciones al servicio**.



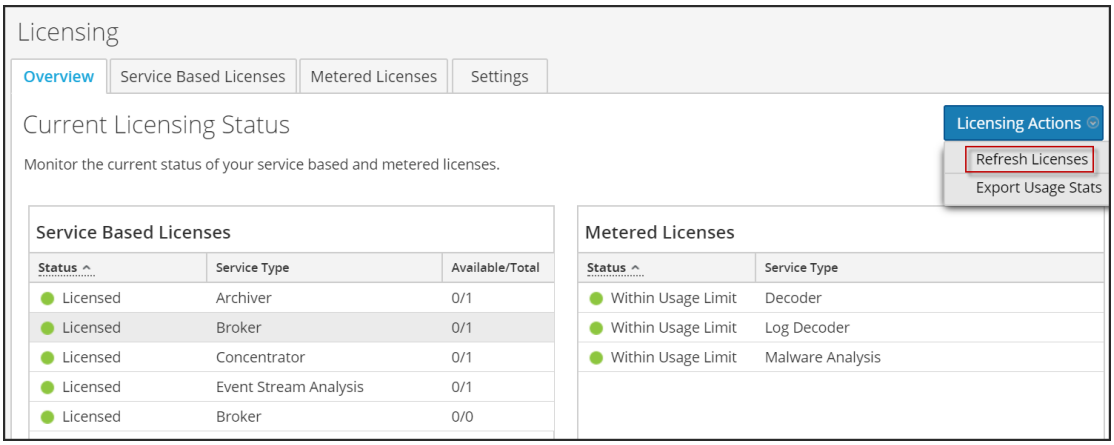
8. Haga clic en **Probar conexión**.

   Mientras agrega el servicio, NetWitness Suite le envía paquetes ICMP para verificar si el nombre de host y la dirección IP ingresados son válidos para una conexión de prueba correcta. El resultado de la prueba se muestra en el cuadro de diálogo Agregar servicio. si el resultado de la prueba no es satisfactorio, edite la información del servicio y vuelva a intentarlo.

9. Cuando el resultado esté correcto, haga clic en **Guardar**. El cuadro de diálogo Agregar servicio se cierra y el servicio Malware Analysis está disponible para NetWitness Suite. (Opcional) Verifique el estado del servicio Malware Analysis. En la vista Servicios de Administration, seleccione el servicio Malware Analysis y elija **Ver > Sistema**. El siguiente es un ejemplo de la información disponible para un servicio Malware Analysis.

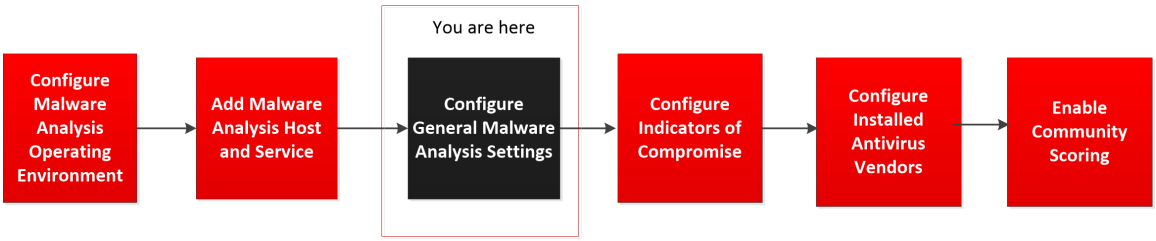


Si el servicio no tiene licencia, navegue a Administration > Sistema > panel Licencia y seleccione **Actualizar licencias** en el menú **Acciones de licencia**.



Configurar ajustes generales de Malware Analysis

Puede configurar varios ajustes básicos para habilitar y calibrar el consumo de sesiones, la carga manual de archivos y los diversos módulos de puntaje que Malware Analysis utiliza para analizar datos.



También puede configurar el uso compartido de archivos con el repositorio de datos. Malware Analysis tiene tres modos de consumo de sesiones y archivos. Puede usar cualquier combinación de las tres opciones para iniciar análisis en Malware Analysis. Las opciones son:

- **Sondeo continuo del servicio Core:** Puede habilitar y configurar el sondeo continuo del servicio Core. Cuando está habilitado y configurado, Malware Analysis sondea continuamente el servicio Core en busca de sesiones etiquetadas para análisis. De forma predeterminada, el sondeo continuo está deshabilitado. Puede activar la prevención de ataques de negación de servicio (DOS) para utilizarla durante el sondeo continuo. Puede probar la conexión al servicio Malware Analysis que se sondea continuamente mediante una opción de la pestaña Integración.

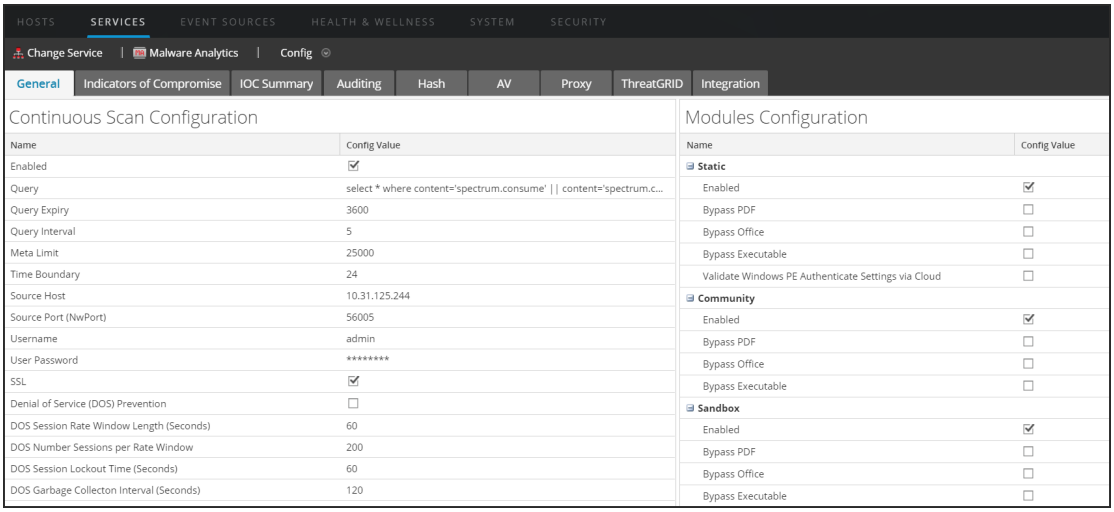
> **Nota:** Cuando agregue un servicio Core como un servicio para sondeo continuo en Malware Analysis 10.3.5 y anteriores, use el puerto REST; por ejemplo, agregue un Concentrator a Malware Analysis 10.3.5 con el puerto REST (50105) en lugar del puerto NextGen (50005) nativo.

- **Análisis según demanda del servicio Core:** Puede analizar sesiones según investigaciones iniciadas directamente en NetWitness Suite. Este método permite un consumo controlado de manera manual de las sesiones de Core y permite controlar mejor la manera en que se procesan los archivos de esas sesiones (por ejemplo, envío a Sandbox para el procesamiento). Ciertos tipos de documentos pueden evitar las restricciones predeterminadas y se envíen al procesamiento de Community o Sandbox independientemente del ajuste configurado.
- **Carga manual de archivos:** Puede cargar manualmente uno o más archivos para análisis mediante la navegación a una carpeta visible de su computadora y la selección de los archivos que desea cargar. El tamaño máximo para los archivos cargados es configurable.

Ver la configuración básica

Para ver la configuración básica:

1. En el **menú principal**, seleccione **Administration > Servicios**.
2. En la cuadrícula **Servicios**, seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
   Se muestra la Configuración del servicio para el servicio con la pestaña **General** abierta.



Configurar el sondeo continuo

Malware Analysis tiene un límite de frecuencia, de modo que solo se pueden enviar 1,000 archivos diarios a la nube de ThreatGrid para el procesamiento de Sandbox. Para optimizar el uso de Sandbox, la configuración de Malware Analysis permite elegir cuál de los diversos métodos de consumo utiliza Malware Analysis; puede habilitar o deshabilitar el sondeo continuo.

Una consideración importante cuando se configura el sondeo continuo son los parámetros de prevención de negación de servicio (DOS). De forma predeterminada, esta función está deshabilitada debido a que debe considerar cuidadosamente los ajustes para su ambiente antes de habilitarla.

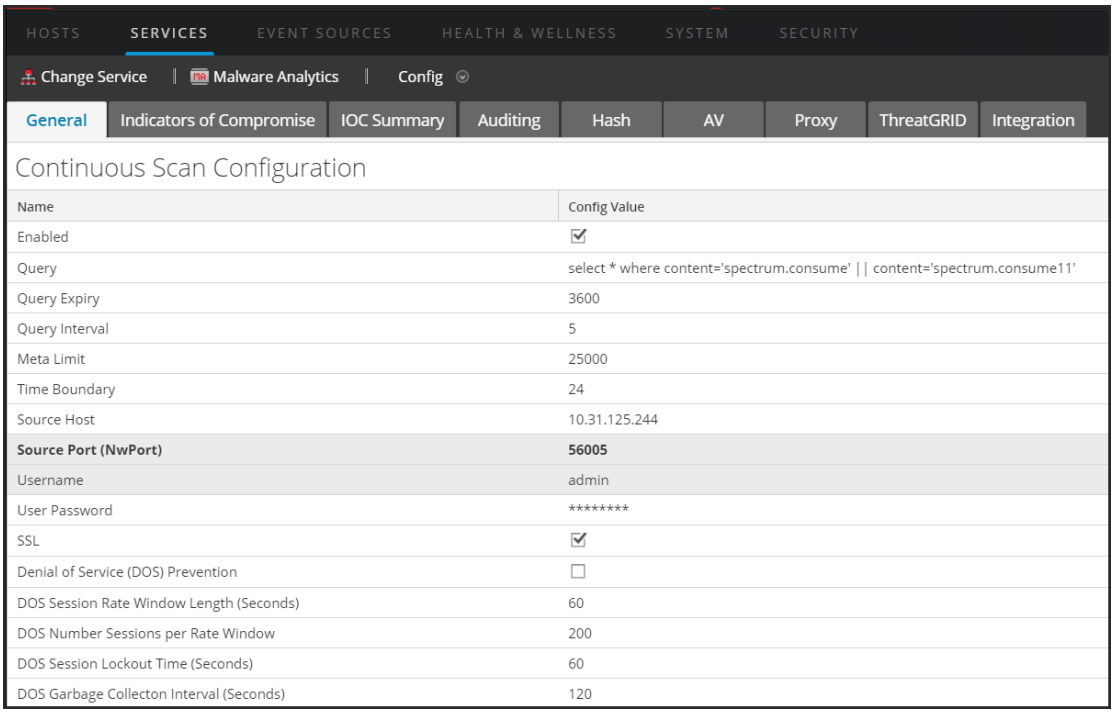
Cuando la prevención de DOS está deshabilitada, Malware Analysis analiza las sesiones en línea de espera en orden de primero en entrar, primero en salir. Un ataque de DOS puede llenar rápidamente la línea de espera, de modo que Malware Analysis está ocupado en el manejo de esas sesiones, mientras que se está produciendo un ataque de malware en una sesión posterior. Es posible que la sesión posterior con el ataque real no pueda llegar al principio de la línea de espera y se someta a un análisis después del inicio del ataque.

Cuando la prevención de DOS está habilitada, Malware Analysis considera que demasiadas sesiones de una única dirección IP son un ataque de DOS. Si una dirección IP supera la Cantidad de sesiones por ventana de tasa, Malware Analysis comienza a hacer caso omiso de las sesiones de esa dirección hasta que se alcanza el tiempo de bloqueo de la sesión. A continuación, Malware Analysis reanuda el análisis de las sesiones desde esa dirección IP. Las sesiones omitidas desde la dirección IP no se analizan en absoluto, razón por la cual un ataque de malware puede escabullirse durante el período de bloqueo de la sesión.

Si se usa el ajuste Intervalo de recolección de elementos no utilizados de DOS, Malware Analysis borra el almacenamiento en la memoria de un origen IP después de una cantidad de segundos especificada. Las direcciones IP con poca actividad durante este intervalo se borran de la memoria. Si una dirección IP está activa en intervalos que superan el Intervalo de recolección de elementos no utilizados de DOS, es posible que Malware Analysis no la identifique como un ataque de DOS.

Para configurar Malware Analysis para el sondeo continuo, en la sección Configuración de escaneo continuo:

1. En **Admin**, haga clic en **Servicios**.
2. En la pestaña **General**, bajo **Configuración de escaneo continuo** puede configurar el sondeo continuo.



3. Para habilitar el sondeo continuo, haga clic en **Habilitado**.
4. (Opcional) Si desea cambiar los valores predeterminados de las consultas, ingrese nuevos valores para **Vencimiento de la consulta**, **Intervalo de consultas**, **Límite de metadatos** y **Límite de tiempo**.
5. Para configurar el dispositivo Malware Analysis al cual consultará Malware Analysis para recuperar datos para análisis, especifique el **Host de origen** y el **Puerto de origen (NwPort)**.
6. (Opcional) Si desea cambiar las credenciales de inicio de sesión predeterminadas del dispositivo Malware Analysis, especifique el **Nombre de usuario** y la **Contraseña de usuario**.
7. Si desea usar SSL para la comunicación entre el dispositivo de Malware Analysis y el servicio Core, habilite **SSL**.
8. (Opcional) Si desea configurar la prevención de negación de servicio (DOS):
   a. Active el parámetro **Prevención de negación de servicio (DOS)**.
   b. Configure las limitaciones de sesión de la prevención de DOS:
      - Especifique la cantidad de segundos de la ventana de tiempo durante la cual Malware Analysis cuenta sesiones para una única dirección IP (**Duración de ventana de tasa de sesiones de DOS**). La ventana se denomina una ventana de tasa y se establece un

contador cuando se recibe la primera sesión desde ese origen IP. El valor predeterminado es de 60 segundos.

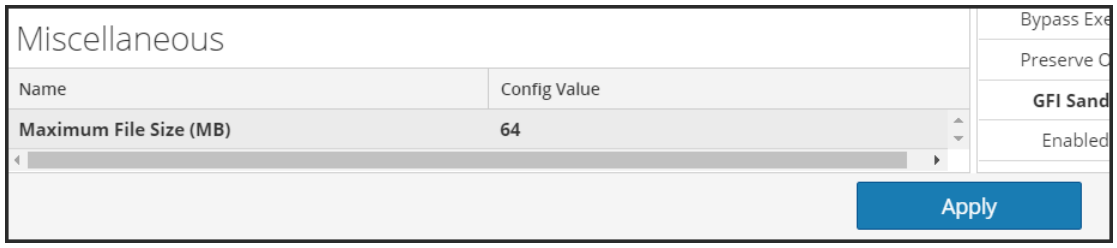
- Especifique la cantidad de sesiones permitidas por ventana de tasa en **Cantidad de sesiones de DOS por ventana de tasa**. El valor predeterminado es 200 sesiones. Cuando se alcanza la cantidad de sesiones dentro de la ventana de tasa, Malware Analysis comienza a hacer caso omiso de aquellas que provienen de la dirección IP, y las sesiones omitidas desde esa IP no se analizan en absoluto. Malware Analysis continúa haciendo caso omiso de las sesiones hasta que se alcanza el tiempo de bloqueo.
- Especifique la cantidad de tiempo de bloqueo (durante el cual se hace caso omiso de las sesiones desde la dirección IP, las cuales no se analizan) en **Tiempo de bloqueo de sesiones de DOS (segundos)**. El valor predeterminado es de 60 segundos. Cuando transcurre la duración del bloqueo, Malware Analysis reanuda el análisis de las sesiones de esa dirección IP.
- Especifique el intervalo de inactividad para una dirección IP antes de que NetWitness Suite elimine el objeto en la memoria para el origen IP en **Intervalo de recolección de elementos no utilizados de DOS (segundos)**. El valor predeterminado es 120 segundos.

9. Haga clic en **Aplicar** para aplicar los cambios.
   Los cambios se aplican de inmediato a medida que Malware Analysis recibe los paquetes nuevos.
10. Pruebe la conexión del servicio Malware Analysis al servicio Core seleccionado en la pestaña **Integración** mediante un clic en el botón **Probar conexión** de la sección **Prueba de conexión de escaneo continuo**.

Configurar los ajustes de carga manual de archivos

Para configurar el tamaño máximo de la carga manual de archivos:

1. En la sección Varios, escriba el tamaño máximo de archivos en Megabytes que se permite para los archivos que se cargan manualmente para el escaneo de Malware Analysis.



2. Haga clic en **Aplicar**.
   Los cambios se aplican de inmediato.

Configurar el repositorio de datos

Malware Analysis puede almacenar un número finito de archivos en el dispositivo. La configuración del repositorio de datos tiene un periodo de retención del sistema de archivos de 60 días. Este ajuste determina cuánto tiempo se conservan los archivos en el dispositivo de Malware Analysis. Cuando se eliminan archivos antiguos, no se pueden recuperar. Cada día, Malware Analysis elimina archivos que superan el período de retención del sistema de archivos para asegurarse de que no se desperdicie espacio en el disco.

El periodo de retención del sistema de archivos es el único ajuste que rige cuándo se eliminan los archivos. Los archivos no se eliminan según la cantidad de espacio en el disco que se ha utilizado. Si se debe cambiar el ajuste, el administrador debe configurar el período de retención basado en el uso de espacio anticipado durante la cantidad de días de retención especificada.

Los parámetros visibles del repositorio de datos de la interfaz del usuario de NetWitness Suite son:

- La ubicación del repositorio es **/var/lib/netwitness/malware-analytics-server/spectrum**. No modifique este valor.
- El protocolo de uso compartido de archivos que permite acceder a través de uno de los protocolos de uso compartido de archivos para copiar archivos del servicio Malware Analysis.
- El período de retención de archivos en cantidad de días.

Para configurar el uso compartido de archivos, en la sección Repositorio de datos:

1. Haga clic en el Protocolo de uso compartido de archivos para seleccionar FTP o SAMBA.
2. Seleccione la cantidad de días en que los archivos se mantendrán en el repositorio antes de eliminarse.
3. Haga clic en **Aplicar**.

Los cambios se aplican de inmediato.

Calibrar módulos de puntaje

La sección Configuración de módulos ayuda a configurar los siguientes componentes de Malware Analysis para:

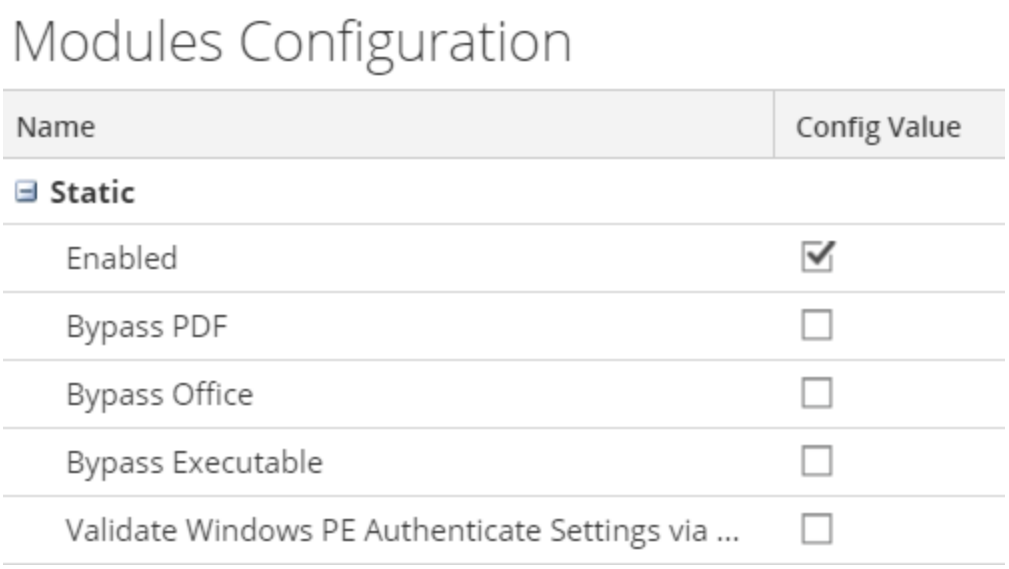
- Deshabilitar por completo cualquiera o los tres módulos de puntaje (Static, Community y Sandbox). Antes de deshabilitar o habilitar cualquier módulo de puntaje, asegúrese de

comprender lo que detecta cada uno.

- Malware Analysis etiqueta sesiones que contienen archivos de Microsoft Office, Windows PE y PDF para el consumo por parte del servicio Malware Analysis. Puede configurar Malware Analysis para que omita totalmente los documentos de Windows PE, Microsoft Office y PDF. Si este es el caso, una mejor opción es ajustar su configuración de Core para omitir estos archivos de modo que no se etiqueten para el consumo de Malware Analysis.

La siguiente es una aplicación de ejemplo para usar la calibración del módulo de puntaje: cuando se configuran grupos de reglas o se analiza el rendimiento del sistema, puede probar diversos escenarios donde los documentos PDF no se analizan, pero los documentos de Microsoft Office y Windows PE sí. Puede probar el escenario en cada uno de los tres módulos de puntaje. Si observa una mejora cuantificable en el rendimiento del sistema, puede aplicar este conocimiento en una escala más amplia.

Configurar el puntaje de análisis estático



Para configurar el puntaje de análisis estático, en la sección **Configuración de módulos**:

1. De manera predeterminada, el módulo Static está activado. Para activar o desactivar el análisis estático por completo, haga clic en la casilla de verificación **Activado**.
2. Para configurar el manejo de archivos PDF, de Microsoft Office y de Windows PE en una sesión, seleccione cualquiera de las casillas de verificación **Omitir PDF**, **Omitir Office** y **Omitir archivo ejecutable**.
3. Para configurar su preferencia para la validación de Authenticode de archivos Windows PE con firma digital, haga clic en la casilla de verificación **Validar configuración de Windows PE Authenticate a través de la nube**. Si desea evitar que los archivos de Windows PE con

firma digital se transmitan a RSA Cloud para la validación, deseleccione la casilla. Cuando la opción está deshabilitada, TODO el análisis estático se ejecuta de forma local (omitiendo la validación de Authenticode). Independientemente de este ajuste, los documentos PDF y MS Office no están sujetos a la validación de Authenticode y no se transmiten a través de la red durante el análisis estático.

4. Haga clic en **Aplicar.**Los cambios se aplican de inmediato a medida que Malware Analysis recibe los paquetes nuevos.

Configurar el puntaje de análisis de Community

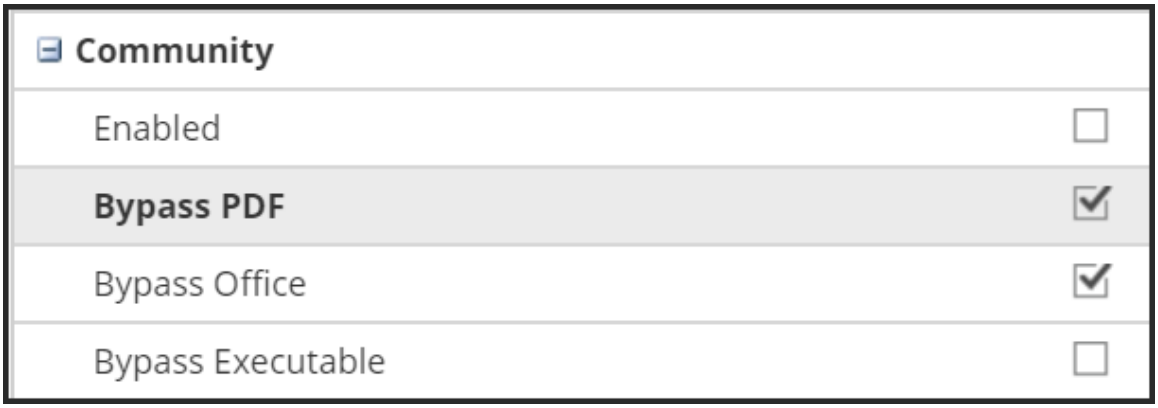
Una vez que el módulo Community está activado, la comunidad de seguridad analiza todos los documentos que no se excluyen del procesamiento. Esto se logra enviando atributos de sesión de red y de archivo a RSA Cloud para el procesamiento. Entonces, RSA Cloud puede establecer una conexión externa con los partners de la comunidad de seguridad según sea necesario para procesar la información.

El contenido del archivo nunca se envía a la comunidad para el análisis. En lugar de eso, el hash MD5/SHA-1 del archivo se envía para la detección de antivirus y la comparación con listas negras. Del mismo modo, los metadatos de sesión se obtienen y se analizan como parte de este proceso. Los elementos de metadatos, como URL y nombre de dominio, se examinan y se transmiten a RSA Cloud para identificar direcciones URL y dominios maliciosos conocidos.

Puede activar el análisis de Community y limitar los tipos de documentos que se procesan. No hay riesgo de que el contenido del archivo (a excepción de un hash) se envíe fuera de la red.

Nota: Para obtener acceso a RSA Cloud donde se produce el procesamiento, debe registrar el servicio Malware Analysis en el servicio al cliente de RSA. Hay dos métodos: registrar el servicio mediante las opciones de la pestaña Integración o ponerse en contacto con Atención al cliente de RSA.

Para configurar el puntaje de análisis de Community, en la sección Configuración de módulos:



1. Para activar o desactivar el análisis de Community por completo, haga clic en la casilla de verificación **Activado**. El valor predeterminado es **Desactivado**.

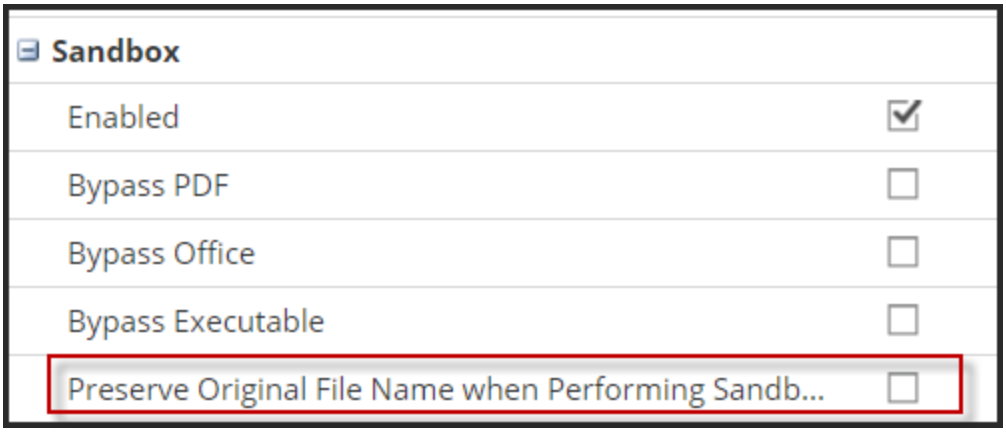
2. Para configurar el manejo de archivos PDF, de Microsoft Office y de Windows PE en una sesión, seleccione las casillas de verificación específicas **Omitir PDF**, **Omitir Office,** **Omitir archivo ejecutable.**
3. Haga clic en **Aplicar** para guardar los cambios e implementarlos inmediatamente a medida que Malware Analysis recibe los paquetes nuevos.

Configurar el puntaje de análisis de Sandbox

De manera predeterminada, el módulo Sandbox está deshabilitado y se impide el procesamiento de archivos PDF y de MS Office. El propósito es configurar los ajustes más restrictivos para obligar al usuario a especificar si se está enviando información posiblemente confidencial fuera de la red para el procesamiento. Si un tipo de documento no se excluye del procesamiento, el archivo completo (no solo el hash) se envía al servidor de Sandbox de destino.

Además, puede elegir conservar el nombre de archivo original al realizar el análisis de Sandbox.

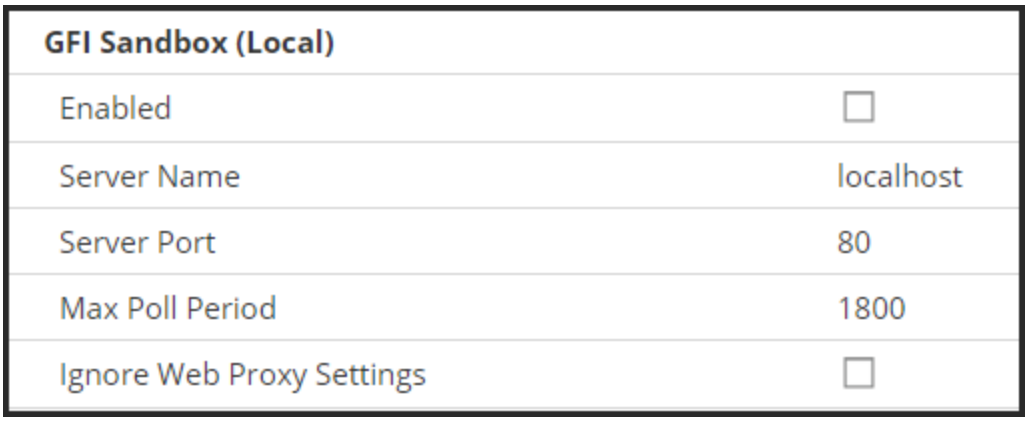
Nota: Si no especifica el parámetro **Conservar el nombre de archivo original cuando se realice un análisis de Sandbox**, NetWitness Suite aplica hashes a los archivos.



Cuando habilita el módulo Sandbox, debe especificar si el procesamiento de Sandbox se ejecuta usando un GFI Sandbox local, un Sandbox de ThreatGrid local o una versión en la nube de Sandbox de ThreatGrid. ThreatGrid proporciona directamente la versión en la nube de Sandbox de ThreatGrid y para esto se debe obtener una clave de activación de ThreatGrid, la cual se debe configurar en la pestaña ThreatGrid.

Configuración de GFI Sandbox

Para usar un GFI Sandbox instalado localmente, debe habilitar GFI y proporcionar el nombre del servidor y el puerto del servidor de GFI Sandbox. El Periodo máximo de encuesta y el Intervalo de sondeo determinan cuánto tiempo se debe esperar que una muestra enviada finalice el procesamiento y con cuánta frecuencia se debe verificar el estado (en segundos). La opción Omitir configuración de proxy web permite indicar que desea que Malware Analysis omita un proxy web cuando realice esta conexión. Si no se configuró un proxy web en Malware Analysis, no se hace caso de la configuración.



Configuración de ThreatGrid Sandbox

Nota: Antes de habilitar el puntaje de ThreatGrid, se debe configurar una clave de servicio que suministra ThreatGrid, de forma que ThreatGrid pueda reconocer que las muestras enviadas desde este sitio son legítimas. Use NetWitness Suite para registrarse con el fin de obtener una clave de API de ThreatGrid. A continuación, puede habilitar y configurar un Sandbox de ThreatGrid instalado localmente o el Sandbox en la nube de ThreatGrid. Consulte la siguiente tarea detallada: Registro de una clave de API de ThreatGrid.

La opción Omitir configuración de proxy web permite indicar que desea que Malware Analysis omita un proxy web cuando realice esta conexión. Si no se configuró un proxy web en Malware Analysis, no se hace caso de la configuración.

Para configurar el puntaje de Sandbox, en la sección Configuración de módulos:

1. Para habilitar o deshabilitar el análisis de Sandbox por completo, haga clic en la casilla de verificación **Habilitado**. El valor predeterminado es **Desactivado**.
2. Para configurar el manejo de archivos PDF, de Microsoft Office y de Windows PE en una sesión, seleccione cualquiera de las tres casillas de verificación **Omitir PDF**, **Omitir Office, Omitir archivo ejecutable.**
3. Configure el proveedor de Sandbox activo. Tiene tres opciones:
   a. Para usar una instancia de GFI Sandbox instalada localmente, indique el Nombre del servidor y el Puerto del servidor de GFI Sandbox, el Periodo máximo de encuesta y el Intervalo de sondeo y, si lo desea, seleccione la casilla de verificación Omitir proxy web.
   b. Para usar una instancia de ThreatGrid instalada localmente, active el puntaje de ThreatGrid, proporcione la clave de servicio de ThreatGrid y, si lo desea, seleccione la casilla de verificación Ignorar proxy web.

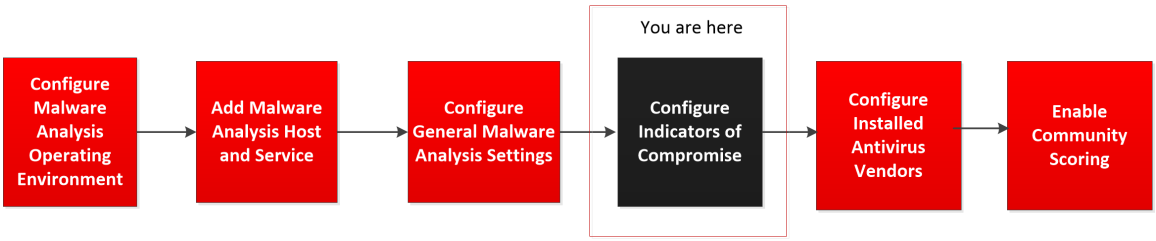
c. Para usar la nube de ThreatGrid, primero debe registrar una clave de API de ThreatGrid. Luego active el puntaje de ThreatGrid, proporcione la clave de servicio de ThreatGrid, ingrese la URL del servidor de ThreatGrid (https://panacea.threatgrid.com) y, si lo desea, seleccione la casilla de verificación Omitir proxy web.

4. Haga clic en **Aplicar**.

   Los cambios se aplican de inmediato.

Configurar los indicadores de riesgo

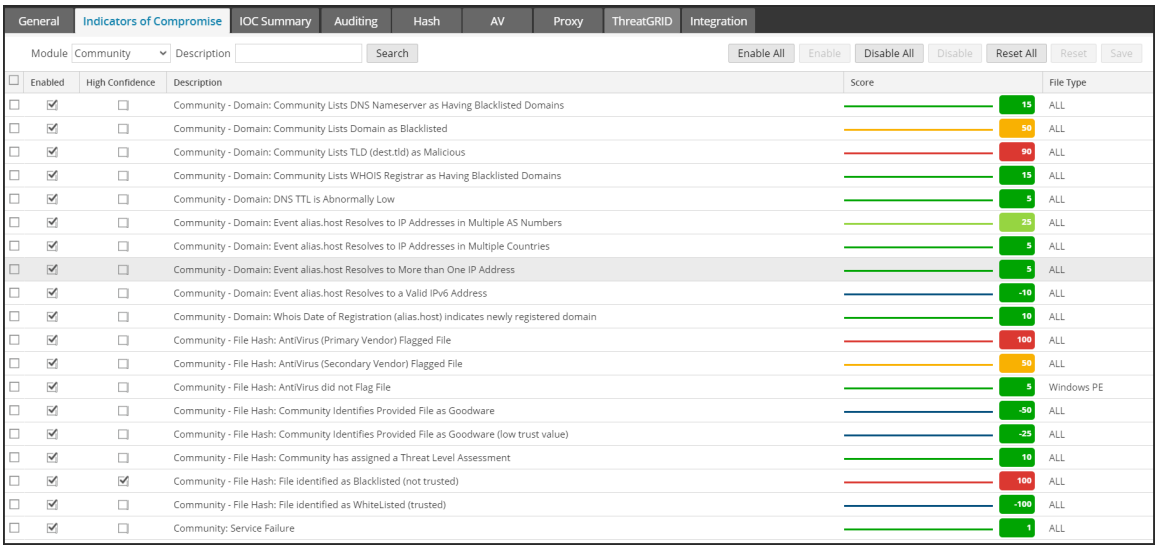
Los indicadores de riesgo (IOC) de los módulos de puntaje de Malware Analysis están configurados, porque cada módulo de puntaje de Malware Analysis, Red, Estático, Community, Sandbox y YARA, tiene un conjunto predeterminado de indicadores de riesgo (IOC) que usa para evaluar los datos de archivo y de sesión con el fin de evaluar la probabilidad de que incluyan malware.



A cada IOC se le asigna una ponderación de puntaje numérico que va desde -100 (bueno) a +100 (malo). Cuando se activa un IOC, la ponderación de puntaje numérico se toma en cuenta en el puntaje total de la sesión o del archivo que se están analizando. Las ponderaciones de puntaje individual de todos los IOC coincidentes se suman para producir el puntaje resultante de cada sesión o archivo. El puntaje sumado se ajusta para garantizar que no supere el rango de puntaje válido (entre -100 y 100).

Nota: La ponderación de puntaje asignada a un IOC no siempre es el valor de puntaje explícito que se suma (no es una simple adición de ponderaciones de puntaje para cada IOC que se activa). En lugar de eso, el puntaje de IOC es una ponderación o un indicador de importancia que se toma en cuenta para calcular un puntaje general.

Los ajustes de configuración de los indicadores de riesgo (IOC) para Malware Analysis se encuentran en la vista Configuración de servicio > pestaña Indicadores de riesgo. Este es un ejemplo de la pestaña.



Si usamos **Community: hash de archivo: Archivo marcado con AntiVirus (proveedor principal)** como ejemplo, la ponderación del puntaje de IOC podría definirse en 100. Sin embargo, Malware Analysis diluye este valor en función del porcentaje de proveedores de antivirus principales que están de acuerdo en que la muestra es maliciosa. Mientras más cerca esté del 100 % de los proveedores que afirman que la muestra es maliciosa, más cerca está de usar los 100 puntos completos para la suma de un puntaje. A medida que el porcentaje se acerca a 0 %, la proporción de los 100 puntos completos que se usa en el puntaje sumado disminuye.

Los IOC usan lógica implementada de forma nativa en Malware Analysis. No puede ajustar la lógica. En lugar de eso, solo puede ajustar el IOC para aumentar o disminuir su impacto en el puntaje, para indicar un ajuste de confianza o para activar o desactivar el IOC. El escenario típico es ajustar un conjunto limitado de valores de ponderación de puntaje de IOC hacia abajo para los IOC que inflan el puntaje final y producen resultados de análisis falsos positivos. Una versión extrema de ajuste sería desactivar los IOC por completo si constantemente contribuyen a entregar resultados falsos positivos. Además, esta flexibilidad le permite desactivar todos los IOC y seleccionar unos pocos para dejarlos activados. Por ejemplo, se pueden desactivar todos los IOC, excepto algunos pocos que detectan coincidencias con AntiVirus. Cuando usa Malware Analysis en esta configuración extremadamente limitada, puede reducir los resultados en Malware Analysis de tal manera que solo las coincidencias de antivirus conocidas generen resultados.

Puede configurar esta funcionalidad de diversas maneras:

- Desactivar IOC de modo que no se evalúen como parte del módulo de puntaje al cual están asignados.
- Ajustar la ponderación de puntaje de un IOC de manera que su impacto en el puntaje agregado aumente o disminuya.

- Marcar los IOC que espera que sean indicadores importantes de malware y mostrar una marca de alta confianza (HC) en las sesiones que activen estos IOC en los resultados de Malware Analysis.
- Personalizar los ajustes de puntaje y confianza de manera exclusiva para cada tipo de archivo que se analizará. Cada IOC tiene preasignado un tipo de archivo al cual se aplica. Los posibles valores son **TODOS**, **PDF**, **MS Office** y **Windows PE**. El IOC con el tipo de archivo más pertinente se usa durante el análisis basado en archivo. Por ejemplo, si se analiza un PDF, se seleccionará un IOC con el tipo de archivo definido en**PDF** en lugar del mismo IOC con un tipo de archivo definido en **TODOS.** Si no se encuentra una coincidencia con un tipo de archivo específico, se selecciona el IOC que tenga el tipo de archivo definido en **TODOS**.
- Buscar reglas para mostrar en la cuadrícula según una coincidencia con la descripción de la regla.

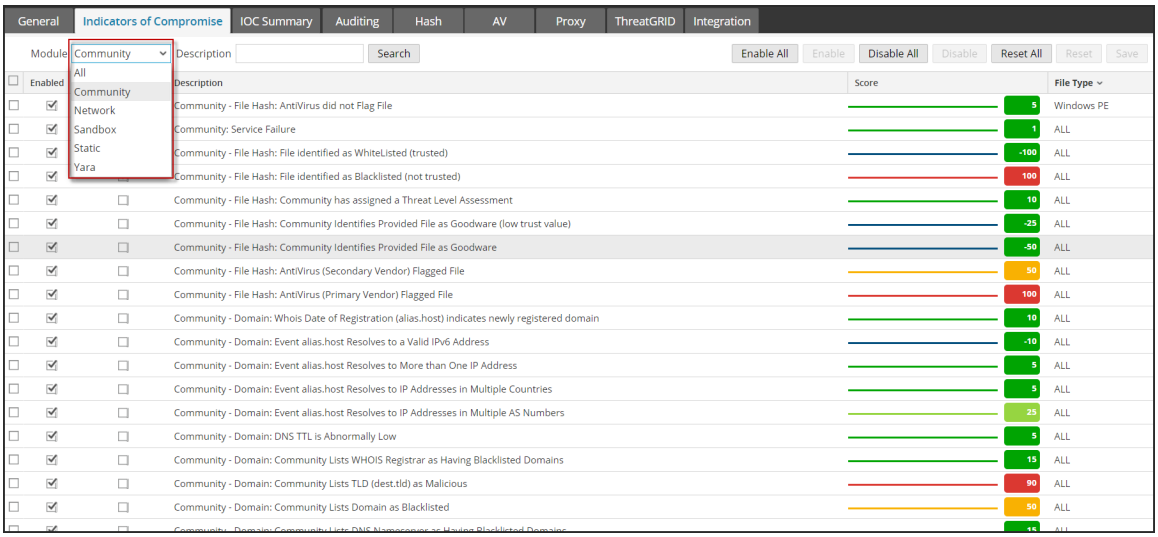
Filtrar IOC mostrados por módulo

Puede filtrar los IOC mostrados por módulo de puntaje: uno de los cuatro módulos incorporados o YARA. Los IOC basados en YARA se entrelazan con los IOC nativos con cada categoría. Aunque los IOC de YARA no se identifican como tales en las demás vistas, puede seleccionar YARA en la lista de selección de módulos para ver una lista de reglas YARA.

Para ver los IOC de uno o de los cuatro módulos de puntaje o de YARA:

1. En el **menú principal**, seleccione **Admin > Servicios.**
2. Seleccione un servicio Malware Analysis.
3. En la fila, seleccione  **> Ver > Configuración**.
4. Haga clic en la pestaña **Indicadores de riesgo**.
5. En la lista de selección **Módulo**, seleccione Todos, NextGen, Estático, Community, Sandbox o Yara.

   Se muestran las reglas y los ajustes configurados del módulo.



Filtrar módulos mostrados para mostrar solo los módulos modificados

La pestaña **Indicadores de riesgo** identifica visualmente los IOC que se modifican localmente. Cuando se ha modificado un IOC, por ejemplo, la ponderación del puntaje ha cambiado, y el nombre se muestra en rojo e incluye un indicador de modificación junto al nombre del IOC. El indicador de modificación es ++ y se puede utilizar como un mecanismo de filtrado en la búsqueda de los IOC.
Para limitar la visualización a los IOC modificados localmente:

1. En el campo **Descripción**, ingrese ++.
2. Haga clic en **Buscar**.

   La vista se filtra para mostrar solo los IOC modificados.

Activar y desactivar IOC para un módulo de puntaje

Cuando se desactiva un IOC, deja de afectar el puntaje agregado del módulo de puntaje al cual pertenece. Si el IOC tiene varias instancias (diferenciadas solo por el tipo de archivo), desactivar un IOC con un tipo de archivo más específico ocasiona el uso de la versión más independiente del IOC en el puntaje.
Por ejemplo, si existe el mismo IOC como tipo de archivo **TODOS** y tipo de archivo **Windows PE**, desactivar la instancia de **Windows PE** del IOC hace que se use la versión **TODOS** en el puntaje. Para desactivar por completo el IOC para **Windows PE** y dejarlo activado para otros tipos de archivo, defina la ponderación de puntaje de la instancia de **Windows PE** del IOC en un valor de cero, como se describe a continuación. Esto deja el IOC activado para los archivos de Windows PE (aunque tenga una ponderación de cero y no se muestre en los resultados de análisis), sin afectar los demás tipos de archivo. Los tipos de archivo restantes seguirán usando la instancia **TODOS** del IOC.

Para habilitar o deshabilitar un IOC de modo que ya no se tome en cuenta en un módulo de puntaje:

1. En el **menú principal**, seleccione **Admin > Servicios.**
2. Seleccione un servicio Malware Analysis y, en la fila, elija  > **Ver > Configuración**.
3. Haga clic en la pestaña **Indicadores de riesgo**.
4. En la lista de selección **Módulo**, seleccione un módulo de puntaje: Todos, Community, Red, Sandbox, Estático o Yara.
   Se muestran las reglas y los ajustes configurados del módulo.
5. Realice una de las siguientes acciones:
   a. Hacer clic en la casilla de verificación **Activado** en la columna que aparece junto a una regla que desee activar.
   b. Seleccione una o más reglas y haga clic en **Activar** o **Desactivar** en la barra de herramientas.
   c. Para alternar entre el estado activado y desactivado de todas las reglas que se muestran en la página, haga clic en la casilla de verificación **Activado** en el título de la columna.
   d. Para activar o desactivar todas las reglas del módulo de puntaje, haga clic en **Activar todo** o **Desactivar todo** en la barra de herramientas.
6. Para guardar los cambios de la página, haga clic en **Guardar** en la barra de herramientas.

Nota: Las reglas cuyos ajustes cambiaron se muestran con una esquina roja. Si navega hacia otra página de reglas antes de guardar, todos los cambios en la página se pierden.

Ajustar la ponderación de puntaje de un IOC

Ajustar la ponderación de puntaje de un IOC aumenta o disminuye el impacto general del IOC en el puntaje agregado del módulo en el cual se configuró. Para aumentar o disminuir el impacto general del IOC, disminuya el valor actual a un nuevo ajuste.

- Los valores que van de -100 a -1 indican que la sesión o el archivo que se están analizando probablemente no tienen malware (-100 es la probabilidad más baja).
- Los valores que van de 1 a 100 indican la probabilidad de que el archivo o la sesión que se están analizando sean malware (100 es la probabilidad más alta).
- Ajustar el valor en cero deja el IOC activado, pero hace que el IOC ya no afecte el puntaje agregado e impide que el IOC aparezca en los resultados de los análisis. Ajustar el valor en cero es un método que permite deshabilitar la instancia de un tipo de archivo específico de un IOC pero dejando la instancia general del tipo de archivo independiente de la regla intacta para el puntaje de los tipos de archivo restantes.

Para ajustar la ponderación de puntaje:

1. En el **menú principal**, seleccione **Admin > Servicios**.
2. Seleccione un servicio Malware Analysis.
3. En la **barra de herramientas**, seleccione **Ver > Configuración**.
4. Haga clic en la pestaña **Indicadores de riesgo**.
5. En la lista de selección **Módulo**, seleccione un módulo de puntaje: Todos, Red, Estático, Community, Sandbox o Yara.
   Se muestran las reglas y los ajustes configurados del módulo.
6. Realice una de las siguientes acciones:
   a. Arrastre el control deslizante de puntaje hacia la izquierda o la derecha para disminuir o aumentar la ponderación de puntaje.
   b. Haga clic directamente en la ponderación de puntaje que se muestra e ingrese una nueva ponderación de puntaje.
7. Para guardar los cambios de la página, haga clic en **Guardar** en la barra de herramientas.

Nota: Las reglas cuyos ajustes cambiaron se muestran con una esquina roja. Si navega hacia otra página de reglas antes de guardar, todos los cambios en la página se pierden.

Definir el indicador de Alta confianza para un IOC

La configuración de Alta confianza se usa como método para marcar IOC específicos como indicadores de alta confianza de que hay malware presente. Como ejemplo, **Community: hash de archivo: AntiVirus (proveedor principal) marcó con un indicador el archivo que** tiene una baja probabilidad de ser un falso positivo, en combinación con una alta probabilidad de ser una medición precisa de la presencia de malware. Cuando se marca este IOC (y otros) como de Alta confianza, puede usar un filtro en los resultados de Malware Analysis para limitar la visualización solo a aquellas sesiones que incluyen una o más reglas de alta confianza. Al hacerlo, la pantalla se limita a un subconjunto más pequeño de resultados a cuya precisión se le otorga un grado más alto de confianza. Mostrar los resultados no limitados a IOC de alta confianza de todas maneras le permite revisar los resultados que no son totalmente claros. Esto proporciona resultados que son menos propensos a dar resultados falsos negativos. La decisión de filtrar o no los resultados según el nivel de confianza tiene un caso de uso válido en el flujo de trabajo de NetWitness Suite.

Para definir el indicador de Alta confianza:

1. En la pestaña **Indicadores de riesgo**, seleccione un módulo de puntaje de la lista de selección **Módulo**: Todos, Red, Estático, Community, Sandbox o Yara.
   Se muestran las reglas y los ajustes configurados del módulo.
2. Haga clic en la casilla de verificación **Alta confianza** en la columna que aparece junto a la regla que desea marcar o desmarcar como con alta probabilidad de indicar la presencia de malware en una sesión.
3. Para guardar los cambios de la página, haga clic en **Guardar** en la barra de herramientas.

Nota: Las reglas cuyos ajustes cambiaron se muestran con una esquina roja. Si navega hacia otra página de reglas antes de guardar, todos los cambios en la página se pierden.

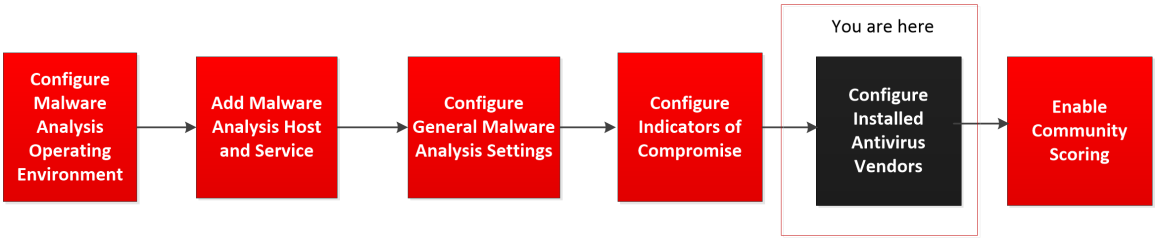
Restablecer los IOC a los valores predeterminados

1. En la pestaña **Indicadores de riesgo**, seleccione un módulo de puntaje de la lista de selección Módulo: Todos, Red, Estático, Community, Sandbox o Yara.
   Se muestran las reglas y los ajustes configurados del módulo.
2. Si desea restablecer todas las reglas de la página actual a sus valores predeterminados, haga clic en **Restablecer** en la barra de herramientas.
3. Si desea restablecer todas las reglas del módulo de puntaje seleccionado a sus valores predeterminados, haga clic en **Restablecer todo** en la barra de herramientas.
4. Para guardar los cambios de la página, haga clic en **Guardar** en la barra de herramientas.

Configurar los proveedores de antivirus instalados

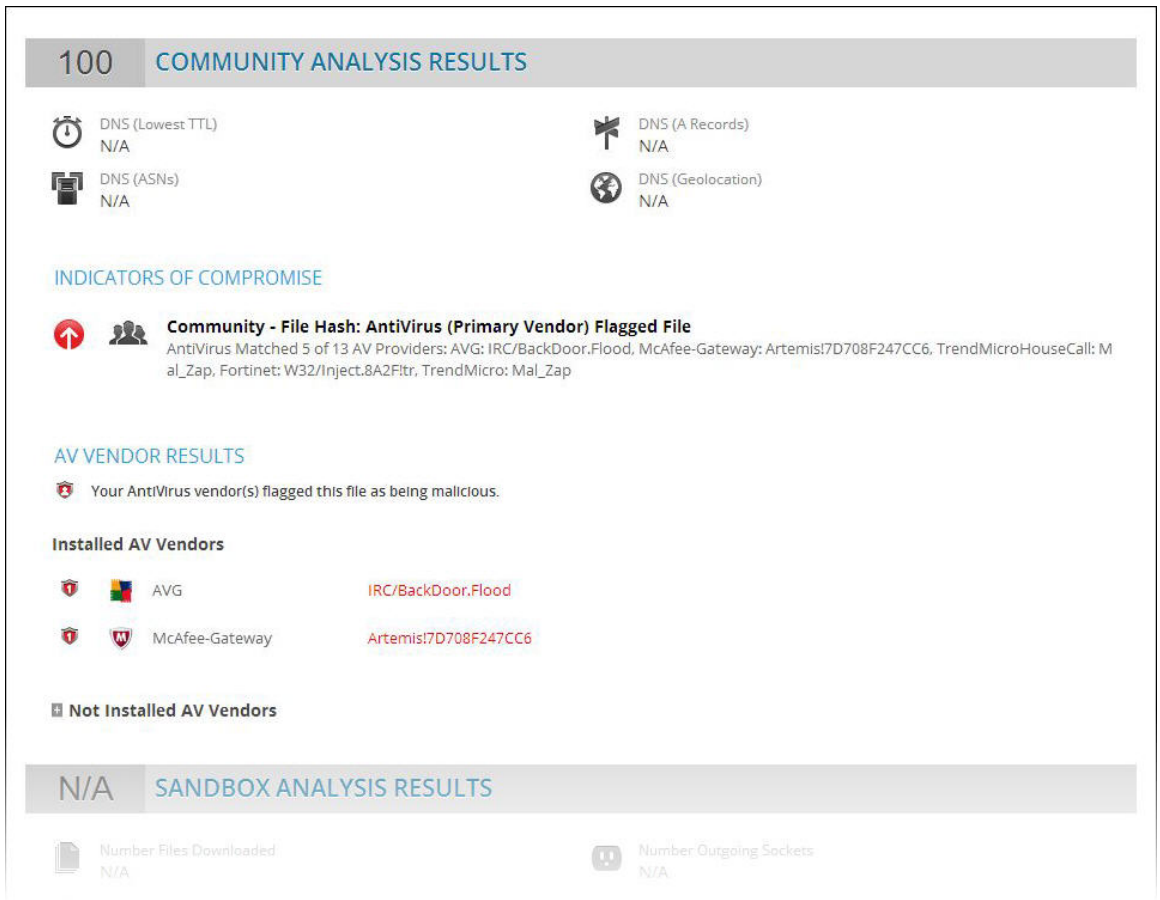
Puede comparar resultados de análisis de archivos de los proveedores de antivirus (AV) instalados con resultados de Community de la base de conocimientos de Malware Analysis. Mientras un análisis de Community analiza un archivo, Malware Analysis consulta una base de conocimientos de antivirus para determinar si la muestra ya se conoce como maliciosa. Si se sabe que el archivo es malicioso, NetWitness Suite lo marca para indicar si un proveedor de antivirus primario o uno secundario identificó la muestra. NetWitness Suite clasifica a los proveedores como primarios y secundarios para indicar el nivel de reputación que tienen en el sector, y los indicadores de riesgo tienen en cuenta la reputación para determinar el puntaje. Por ejemplo, la detección hecha exclusivamente por proveedores de antivirus secundarios puede tener un puntaje menor que la de los proveedores primarios.

Nota: Cuando se elige software de proveedor de antivirus para instalar en la red, se recomienda incluir por lo menos un proveedor de la lista de proveedores primarios de NetWitness Suite.



Puede identificar los proveedores de antivirus instalados en su red ante NetWitness Suite. NetWitness Suite compara los resultados del antivirus durante un análisis de Community con los resultados de los proveedores instalados que se seleccionaron en la pestaña Antivirus. Si se detecta una coincidencia, el archivo que se analiza se marca para indicar que el software antivirus primario o secundario instalado localmente detectó la muestra.

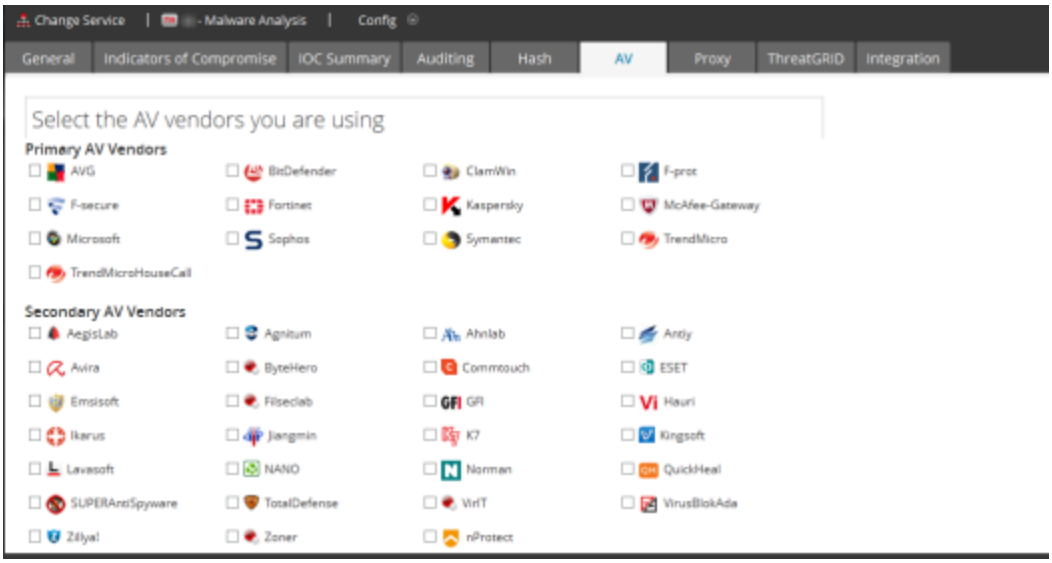
En el siguiente ejemplo se muestran los resultados de análisis de Community para un archivo que obtuvo un puntaje de 100. En **Indicadores de riesgo**, puede ver que los proveedores de antivirus enumerados marcaron el archivo en Community. En **Resultados de proveedor de antivirus**, NetWitness Suite indica si los proveedores de antivirus instalados en el ambiente marcaron el archivo como malicioso. Si los proveedores de antivirus instalados detectaron el virus, se muestra el nombre del malware. Si no lo detectaron, se muestra **--No detectado--** junto al nombre del proveedor de antivirus. En **Proveedores de antivirus no instalados**, puede hacer clic en + para expandir la sección y ver si otros proveedores no instalados en el sistema detectaron el virus.



Identificar software antivirus instalado

Para identificar software antivirus instalado en su red:

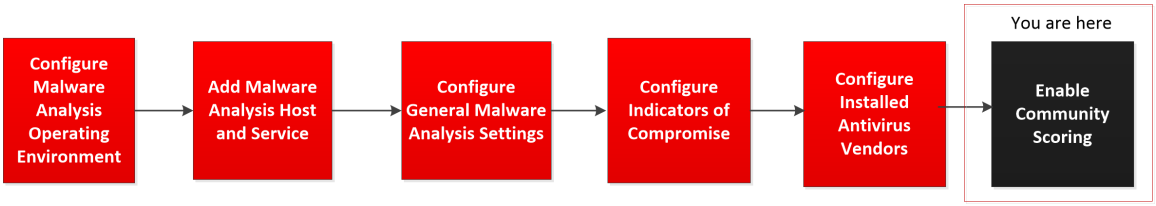
1. En el **menú principal**, seleccione **ADMIN > Servicios.**
2. Seleccione un servicio Malware Analysis y, en la fila, elija > **Ver** > **Configuración**.
3. En la **vista Configuración del servicio**, seleccione la pestaña **Antivirus**.



4. Seleccione la casilla de verificación que se encuentra junto a cada proveedor de antivirus (primario u otro) cuyo software está instalado en la red.
5. Para guardar los cambios, haga clic en **Aplicar**.
   Los Resultados de análisis de Community indicarán si el software marcó un evento.
6. (Opcional) Si desea restablecer la lista de software antivirus instalado al valor predeterminado (ninguno), haga clic en **Restablecer**.
   Todas las selecciones se eliminan.
7. Para guardar los cambios, haga clic en **Aplicar**.

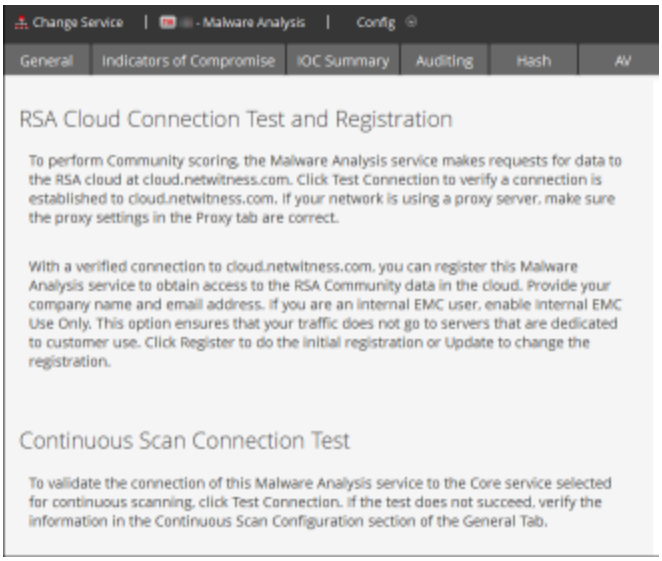
Habilitar el análisis de Community

Un administrador puede habilitar el análisis de Community. En el caso del análisis comunitario, el nuevo malware detectado en la red se envía a RSA Cloud para compararlo con los análisis de malware propios de RSA y feeds de SANS Internet Storm Center, SRI International, el Departamento del tesoro y VeriSign. Para habilitar el análisis de Community, debe registrarse en RSA Cloud y probar la conexión a la nube y, a continuación, probar la conexión entre RSA Cloud y el servicio que configuró para escaneo continuo.



Se proporciona una descripción completa de los métodos de análisis en Cómo funciona Malware Analysis.

1. En el **menú principal**, seleccione **ADMIN > Servicios.**
2. Seleccione un servicio Malware Analysis y, en la fila, elija **> Ver > Configuración**.
3. En la **vista Configuración del servicio**, seleccione la pestaña **Integración**.



4. Desplácese hasta Prueba de conexión de escaneo continuo y haga clic en **Prueba y registro de la conexión a RSA Cloud**.

   NetWitness Suite prueba las comunicaciones con el sitio en `https://cloud.netwitness.com`. Si su empresa utiliza un proxy para el tráfico saliente, compruebe la configuración de proxy. Se requiere una conexión válida para registrarse en el servicio de la comunidad de RSA.

5. Ingrese el nombre de la empresa y un correo electrónico de contacto. Haga clic en **Registrar**.

   Si todos los campos obligatorios están completos, el registro está completo. La etiqueta del botón que se utilizó para el registro cambia a Actualizar.

6. Para verificar que el servicio Malware Analysis pueda conectarse al servicio Core seleccionado para escaneo continuo, haga clic en **Prueba de conexión de escaneo continuo**.

   NetWitness Suite inicia una comprobación basada en el Host de origen, el Puerto de origen, el Nombre de usuario y la Contraseña de usuario especificados en la pestaña General. Cuando la prueba se ejecuta correctamente, los analistas pueden ver el puntaje de Community en Malware Analysis.

(Opcional) Configurar la auditoría en un host de Malware Analysis

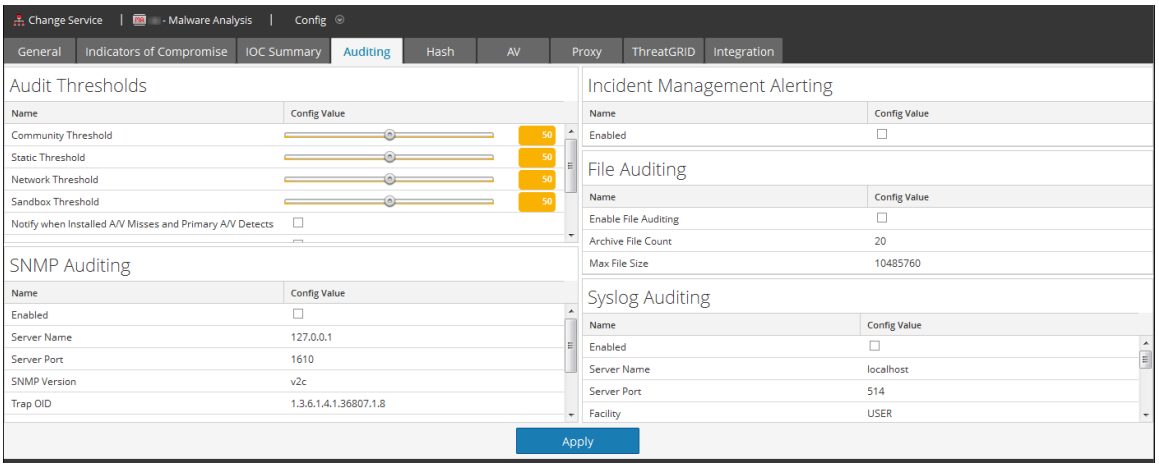
En este tema se presentan las funciones configurables del registro de auditoría de Malware Analysis y los procedimientos para configurarlas. Malware Analysis tiene la capacidad de generar alertas de auditoría basadas en umbrales configurados del módulo de puntaje. Cuando el puntaje de análisis de un archivo en una sesión de análisis coincide o supera los umbrales configurados, se genera una alerta de auditoría. Los umbrales permiten que las sesiones o los archivos que tienen un puntaje suficientemente alto como para ser candidatos de posible malware, generen una alerta de forma automática.

Las alertas se pueden configurar para que tengan formato de entradas de SNMP, syslog o archivo. La compatibilidad con distintos formatos de auditoría proporciona un método para que los sistemas externos consuman eventos de auditoría de acuerdo con su funcionalidad para analizar los formatos compatibles.

Además de auditar sesiones de análisis, los siguientes eventos activarán una alerta de auditoría:

- Casos correctos y fallidos de nombre de inicio de sesión de usuario
- Cambios en los ajustes de configuración del sistema
- Reinicio del servidor
- Actualización e instalación de la versión del servidor

Los ajustes de configuración de auditoría para Malware Analysis se encuentran en la vista Configuración de servicios > pestaña Auditoría.



Configurar el umbral de auditoría

El único propósito de los umbrales es especificar los criterios que se deben cumplir para que se genere una alerta para la sesión o archivo analizado. Si la auditoría está activada, cada archivo/sesión con puntaje se examina para determinar si el puntaje de cada módulo de puntaje coincide o supera el umbral de auditoría configurado. Si es así, se genera una alerta usando el formato de alerta de auditoría configurado (es decir, SNMP, syslog o archivo). Por ejemplo, si configura SNMP y define el umbral de Community en 90, todas las sesiones o archivos con un puntaje de 90 o más en el módulo de puntaje de Community generan un SNMP trap. Si todos los umbrales se definen en 90, no se genera ninguna alerta a menos que una sesión o un archivo tengan un puntaje de 90 o más en los módulos de puntaje Red, Estático, Community y Sandbox.

Para configurar el umbral de auditoría:

1. En el **menú principal**, seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. En la vista **Configuración de servicios**, haga clic en la pestaña **Auditoría**.
4. En la sección **Umbrales de auditoría**:
   a. Establezca el umbral de **Community**, **Estático**, **Red** y **Sandbox** mediante una de las siguientes acciones para cada módulo de puntaje:
      - En el control deslizante, haga clic y arrastre el control en cualquier dirección.
      - En el campo de valor, escriba un número entre 0 y 100, inclusive.
   b. (Opcional para 10.3 SP2) Seleccione uno o más activadores para registrar un mensaje y entregarlo mediante todos los métodos de auditoría activados.
   c. Haga clic en **Aplicar**.
      - El ajuste de umbral se aplica de inmediato a todos los métodos de auditoría activados: SNMP, archivo y syslog.
      - Los mensajes registrados se envían a través de todos los métodos de auditoría activados: SNMP, archivo y syslog.

Configurar alertas de Incident Management

Cuando se habilita, Incident Management puede auditar alertas de Malware Analysis para alimentar su flujo de trabajo.

1. En el **menú principal**, seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. En la vista **Configuración de servicios**, seleccione la pestaña **Auditoría**.

4. En la sección **Alertas de Incident Management**, seleccione la casilla de verificación Habilitado y haga clic en Aplicar.
   Las alertas entran en vigencia inmediatamente.

Configurar la auditoría de SNMP

El protocolo simple de administración de red (SNMP) es un protocolo estándar de Internet para administrar servicios en redes IP. Cuando una auditoría de SNMP está habilitada, Malware Analysis puede enviar un evento de auditoría como un SNMP trap a un host de SNMP trap configurado. Además del puntaje y el ID de evento, la alerta incluye todos los metadatos de sesión, así como los metadatos generados. Esto es útil para los usuarios que quieran enviar feeds de los datos de un evento a sistemas de otros fabricantes.

Para configurar la auditoría de SNMP:

1. En el menú principal, seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. En la vista **Configuración de servicios**, seleccione la pestaña **Auditoría**.
4. En la sección **Auditoría de SNMP**, haga clic en la casilla de verificación para activar la auditoría de SNMP.
5. Configure el nombre de servidor y puerto de SNMP.
6. Configure la versión de SNMP y el OID de trap para enviar traps.
7. Configure la comunidad de Malware Analysis y los parámetros de reintento y tiempo de espera para el envío de mensajes trap.
8. Haga clic en **Aplicar**.
   La configuración de auditoría de SNMP se aplica de inmediato.

Configurar los ajustes de auditoría de archivo

Cuando la auditoría de archivos está habilitada, el archivo de registro de auditoría se mantiene en el directorio principal de Malware Analysis. La ubicación predeterminada para este archivo de registro es:

`/var/lib/netwitness/malware-analytics-server/spectrum/logs/audit/audit.log`.

A medida que cada registro alcanza el tamaño de archivo máximo, se archiva y se crea un registro nuevo. Es posible configurar estos registros de auditoría y su cantidad.

Precaución: Evite configurar el tamaño máximo de archivo y el conteo de archivos en un valor muy alto, ya que esto puede tener un efecto desfavorable en el espacio disponible en disco en el dispositivo de Malware Analysis.

Para configurar la configuración de auditoría de archivo:

1. En el **menú principal**, seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. En la vista **Configuración de servicios**, seleccione la pestaña **Auditoría**.
4. En la sección **Auditoría de archivo**, haga clic en la casilla de verificación para activar la auditoría de archivo.
5. (Opcional) Defina el Conteo de archivos y el Tamaño máximo de archivo.
6. Haga clic en **Aplicar**.
   La configuración de auditoría de archivo se aplica de inmediato.

Configurar los ajustes de auditoría de syslog

Cuando está activado, syslog proporciona auditoría mediante el uso del protocolo RFC 5424 de syslog. Las normativas, como SOX, PCI DSS, HIPAA y muchas otras, requieren que las organizaciones implementen medidas de seguridad integrales, las cuales a menudo incluyen la recopilación y el análisis de registros de muchos orígenes distintos. Syslog ha demostrado ser un formato eficaz para consolidar registros, dado que existen muchas herramientas de propiedad o de código abierto para creación de informes y análisis.

Además del puntaje y el ID de evento, syslog incluye todos los metadatos de sesión, así como los metadatos generados. Esto es útil para los usuarios que quieran enviar feeds de los datos de un evento a sistemas de otros fabricantes.

Para configurar los ajustes de auditoría de syslog:

1. En el **menú principal**, seleccione **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. En la vista **Configuración de servicios**, seleccione la pestaña **Auditoría**.
4. En la sección **Auditoría de syslog**, haga clic en la casilla de verificación para activar la auditoría de syslog.
5. Configure el host donde se está ejecutando el proceso de syslog de destino y el puerto del host donde el proceso de syslog está escuchando.
6. Configure la instalación, la codificación, el formato, la longitud máxima y el registro de fecha y hora de los mensajes de syslog salientes.

> **Nota:** (Opcional) Configure una cadena de identidad para anteponer a cada alerta de syslog.
> Para el formato CEF, consulte Crear una alerta personalizada en formato CEF para conocer consideraciones adicionales.

7. Haga clic en **Aplicar**.

   La configuración de auditoría de syslog se aplica de inmediato.

(Opcional) Configurar el filtro de hash

En este tema se presentan los filtros de hash como un método para marcar archivos en Malware Analysis que se sabe que son legítimos o maliciosos. El filtrado de hash permite mantener una lista de hashes de archivos legítimos o maliciosos conocidos. En la pestaña Hash, puede ajustar con más detalle el análisis de eventos de Malware Analysis según los hashes de archivo. Cuando un hash de archivo está marcado como legítimo, Malware Analysis no analiza el archivo la próxima vez que aparece. Cuando un hash de archivo está marcado como malicioso, Malware Analysis aumenta automáticamente el puntaje de la comunidad para el archivo con una gran cantidad de puntos. Malware Analysis analiza el archivo de todos modos en caso de que pueda obtenerse nueva información.

Nota: Si un evento contiene un único archivo y el hash de ese archivo está marcado como legítimo, Malware Analysis filtra todo el evento y usted no lo ve en los resultados de Malware Analysis.

Para agregar filtros de hash a la lista de hash, puede usar cualquiera de estos métodos manuales:

1. Opción agregar del menú contextual en la vista Detalles del evento: Haga clic con el botón secundario en un archivo y un menú contextual permite marcar el hash del archivo seleccionado como bueno (normal) o malo (malicioso).
2. Barra de herramientas de la pestaña Hash: Haga clic en el botón Agregar de la pestaña Hash para agregar un hash de archivo, tamaño de archivo y, opcionalmente, marcar el hash como confiable.

También existe un método automatizado para agregar filtros de hash a Malware Analysis mediante la importación en masa de una lista de hash desde la carpeta inspeccionada. Los hashes importados a través de la carpeta inspeccionada no aparecen en la lista de hash. Con la importación en masa y el directorio inspeccionado (/var/netwitness/malware-analytics-server/spectrum/hashWatch) en la configuración del servidor de Malware Analysis, copie una lista de hash en la carpeta inspeccionada para que se importe automáticamente al sistema. Los hashes importando con el método de importación masiva sobrescriben a los hashes que se importaron anteriormente a través de la carpeta inspeccionada.

Ver la lista de hash

Para ver la lista de hash:

1. En el **menú principal**, seleccione **ADMIN > Servicios**.
2. En la vista Servicios, seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. Seleccione la pestaña **Hash**.

   La lista de hash se muestra en la pestaña Hash. Solo se muestran los hashes de archivos que se han agregado mediante uno de los métodos.

Agregar un hash de archivo al filtro de hash

Para agregar un hash de archivo al filtro de hash:

1. En la barra de herramientas de la pestaña **Hash**, haga clic en **Agregar**.

   Se muestra el cuadro de diálogo Agregar hash.
2. Si el hash es confiable, seleccione **Confiable**.
3. Ingrese el hash de MD5 y el tamaño del archivo en bytes.
4. Haga clic en **Guardar**.

   El hash de archivo se agrega a los hashes y se usa para ejecutar un filtrado de hash en Malware Analysis.

Marcar un hash como confiable o no confiable

Para marcar un hash de archivo como confiable o no confiable:

1. En la pestaña **Hash**, para alternar entre confiable y no confiable, haga clic en la columna **Confiable** del hash.
2. En la barra de herramientas, haga clic en **Guardar edición**.

Eliminar un hash de un filtro de hash

Para eliminar un hash de un filtro de hash:

1. En la pestaña **Hash**, seleccione uno o más hashes que desee eliminar del filtro de hash.
2. En la barra de herramientas, haga clic en **Eliminar**.

   Un cuadro de diálogo solicita confirmación y ofrece la oportunidad de cancelar la operación.
3. Para confirmar la eliminación, haga clic en **Sí**.

   El hash de archivo se elimina de la cuadrícula y se deja de usar para ejecutar el filtrado de hash en Malware Analysis.

Buscar un hash de archivo

La pestaña Hash permite buscar un hash de archivo que se muestra en la cuadrícula. En el campo MD5, escriba el hash de archivo que busca y haga clic en **Buscar**. La lista de archivos que contienen el hash se muestra en la cuadrícula.

Importar una lista de hash usando la carpeta inspeccionada

Para importar una lista de hash desde el directorio inspeccionado, la lista debe tener el formato especificado y estar clasificada por md5. Puede soltar un archivo con el formato que se describe a continuación en una carpeta (/var/netwitness/malware-analytics-server/spectrum/hashWatch) del dispositivo Malware Analysis y se importará automáticamente a la base de datos de hash local. Esta es la única manera de importar hashes de archivo a . Otro caso de uso es permitir que un administrador del sistema exponga el directorio inspeccionado a algún proceso que enviaría un archivo a este directorio. Este es un método de importación masiva diseñado para manejar un alto volumen de importaciones de hash.

Se trata de un archivo con formato csv que no tiene espacios entre los datos de cada fila. La suposición con los datos de la lista de hash es que no hay duplicados. Durante el procesamiento, se omiten los duplicados. Si se encuentran hashes duplicados, el archivo de registro mostrará el siguiente mensaje para indicar la cantidad de hashes duplicados del archivo:

2013-08-09 09:46:00,674 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processing - /var/lib/rsa>malware/hashWatch/test.csv
2013-08-09 09:47:56,619 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.services.file.hash.HashServiceImpl - Skipped 21 Duplicate Hashes Already on File
2013-08-09 09:48:06,638 [jobExecutor-2(HashFileWatch)] INFO com.netwitness.malware.core.scheduler.jobs.HashFileWatch - Processed - /var/lib/rsa>malware/hashWatch/test.csv

A continuación puede ver un ejemplo de una lista de hash en el formato de archivo predeterminado.

```
[BeginFileExample]
392126E756571EBF112CB1C1cdEDF926,98865,True
0E53C14A3E48D94FF596A2824307B492,2226,True
176308F27DD52890F013A3FD80F92E51,42748,False
9B3702B0E788C6D62996392FE3C9786A,32768,False
937ADE76A75712B7FF339403B4FCB5A6,4821,False
B47139415F735A98069ACE824A114399,1723,False
E6CAF205E602CFA9A65663DB1A087874,704,False
680CA0BCE1FC7BC4136ADF4E210869C5,2075,False
[EndFileExample]
```

Un archivo de configuración de NetWitness Suite (**/var/netwitness/malware-analytics-server/spectrum/conf/hashFileWatchConfig.xml**) especifica el formato y las opciones del proceso de importación de la lista de hash. La siguiente es una lista del archivo de configuración.

```
<config>
 <enabled>true</enabled>
 <distributedCacheEnabled>true</distributedCacheEnabled>

<watchDirectory>/
/var/lib/rsamalware/hashWatch</watchDirectory>

<processedDirectory>/
var/lib/rsamalware/hashWatch/processed</processedDirectory>

<erroredDirectory>/
var/lib/rsamalware/hashWatch/error</erroredDirectory>
 <md5Col>0</md5Col>
 <fileSizeCol>-1</fileSizeCol>
 <isTrustedCol>1</isTrustedCol>
 <isTrust>false</isTrust>
 <ignoreFirstLine>false</ignoreFirstLine>
 <frequencyInMinutes>1</frequencyInMinutes>
 <isGzipCompressed>false</isGzipCompressed>
 </config>
```

Línea	Descripción
<md5Col>0</md5Col>	La ubicación del hash md5 en cada entrada. El valor predeterminado es la posición **0**, o la primera posición.
<fileSizeCol>1</fileSizeCol>	La ubicación del tamaño del hash en cada entrada. El valor predeterminado es la posición **1**, o la segunda posición. Si el tamaño del hash no se incluye en el archivo csv, el valor debe ser **-1**.
<isTrustedCol>2</isTrustedCol>	La ubicación de la columna Trusted en cada entrada. El valor predeterminado es la posición **2**. Si el parámetro Trusted no se incluye en el archivo csv, el valor debe ser **-1**.

Línea	Descripción
<isTrust>false</isTrust>	La asunción predeterminada para **Trusted** en cada entrada es **false**.
<ignoreFirstLine>false</ignoreFirstLine>	La presencia o la ausencia de un encabezado en el hash. El valor predeterminado es **falso**. Si el hash tiene un encabezado, el valor se debe definir en **true**.
<frequencyInMinutes>1</frequencyInMinutes>	El intervalo entre comprobaciones de NetWitness Suite en el directorio inspeccionado. El valor predeterminado es **1** minuto.
<isGzipCompressed>false</isGzipCompressed>	El hash está comprimido con Gzip. El valor predeterminado es **falso**. Si el hash está comprimido con Gzip, el valor aquí se debe definir en **true**.

Cuando se ha importado la lista de hash, el registro del sistema muestra entradas similares a la siguiente:

```
2013-04-11 03:22:00,597 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 2013-04-11 03:22:00,600 [jobExecutor-9(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processed -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

Si hay un problema al cargar el archivo, el registro del sistema tiene entradas similares a la siguiente:

```
2013-04-11 03:17:00,597 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
 ... Verbose log
 2013-04-11 03:17:00,632 [jobExecutor-4(HashFileWatch)] INFO
com.netwitness.malware.core.scheduler.jobs.HashFileWatch -
Error Processing -
/var/lib/rsamalware/spectrum/hashWatch/simpleHash.csv
```

Para importar una lista de hash mediante el método de carpeta inspeccionada:

1. Copie las listas de hash que desea importar al directorio **/var/netwitness/malware-analytics-sever/spectrum/hashWatch**.
   Malware Analysis inspecciona automáticamente esta carpeta y procesa los archivos que contiene.
   Malware Analysis agrega cada hash encontrado en las listas de hash al filtro de hash.
   Si se producen errores de procesamiento, estos se registran en**/var/netwitness/malware-analytics-sever/spectrum/hashWatch/error**
   Los archivos procesados se catalogan en **/var/netwitness/malware-analytics-sever/spectrum/hashWatch/processed**
   Los archivos procesados no se quitan del directorio hashWatch.
2. Después de importar hashes de forma masiva, el administrador del sistema puede usar un cronjob para limpiar archivos procesados antiguos.

(Opcional) Configurar ajustes de proxy de Malware Analysis

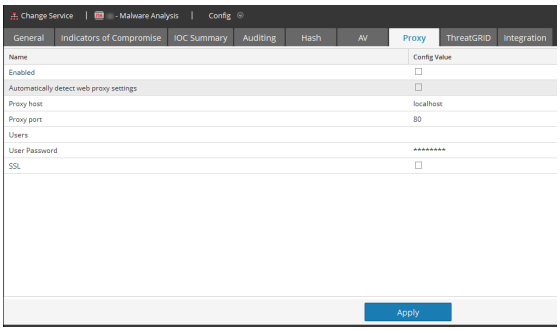
En este tema se describe la configuración de un proxy web para comunicarse con el servicio de RSA Cloud y el servicio de ThreatGrid o GFI local. Los ajustes de la vista Configuración de servicios > pestaña Proxy permiten configurar la comunicación mediante proxy web, la que puede usar Malware Analysis para comunicarse con RSA Cloud con fines de análisis de Community y Sandbox. Una vez que el proxy está configurado:

- Malware Analysis se comunica a través del proxy web con RSA Cloud para el análisis de Comunidad.
- Malware Analysis se comunica a través del proxy web con el servicio ThreatGrid o GFI Sandbox configurado. Usar un proxy web puede afectar negativamente el rendimiento. Las secciones de configuración de ThreatGrid y GFI en la pestaña General tienen una opción para omitir el proxy web y comunicarse directamente con Sandbox para mejorar el rendimiento.

Configurar un proxy web

Para configurar el proxy web para Malware Analysis:

1. Navegue a la vista **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija  **> Ver > Configuración**.
3. En la vista **Configuración de servicios**, seleccione la pestaña **Proxy**.



4. Para habilitar el proxy, seleccione la casilla de verificación **Habilitado**.
5. (Opcional) Para detectar automáticamente la configuración de proxy para el Servidor de NetWitness, seleccione la casilla de verificación.

   Los campos de host de proxy y puerto de proxy se completan automáticamente.
6. Si desea usar otro proxy, ingrese el **Host de proxy** y el **Puerto de proxy**.
7. Escriba el nombre de usuario y la contraseña que se usan para iniciar sesión en el host de proxy.
8. (Opcional) Seleccione **SSL** si el host de proxy se comunica a través de SSL.
9. Haga clic en **Aplicar**.

   La configuración se guarda y se aplica de inmediato.

Nota: Malware Analysis no es compatible con la autenticación de proxy web NTML.

(Opcional) Registrarse para una clave de API de ThreatGrid

En este tema se presenta el procedimiento para obtener una clave de API de ThreatGRID de prueba para usarla en la versión de nube de Sandbox de ThreatGrid. Antes de habilitar ThreatGrid como el servicio de Sandbox en el módulo Sandbox, se debe configurar una clave de servicio que suministra ThreatGrid, de forma que ThreatGrid pueda reconocer que las muestras enviadas desde este sitio son legítimas.

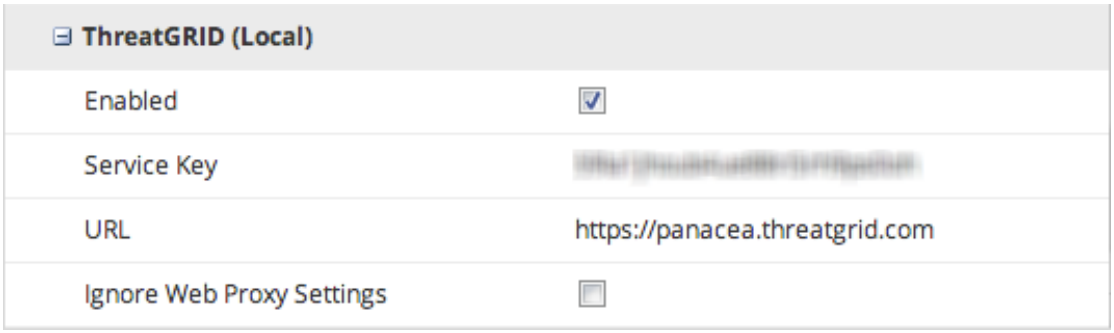
Si no tiene una clave de servicio suministrada por ThreatGrid, puede obtener una utilizando esta pestaña. La clave se proporciona a modo de evaluación.

Cuando completa la información del usuario y hace clic en **Registrarse**, aparece una clave en esta pestaña y se agrega automáticamente a la configuración de ThreatGrid en la pestaña **General**. Después de unos minutos, recibirá un correo electrónico de ThreatGrid con un vínculo a la página donde puede iniciar sesión. Después de aceptar los términos de la licencia en la página ThreatGrid, puede enviar archivos para análisis y ThreatGrid reconocerá los archivos que Malware Analysis envía para análisis de Sandbox.

Para obtener una clave de API de ThreatGrid de prueba:

1. En NetWitness Suite, vaya a **ADMIN > Servicios**.
2. Seleccione un servicio Malware Analysis y elija > **Ver** > **Configuración**.
3. En la vista **Configuración de servicios**, seleccione la pestaña **ThreatGrid**.
4. Escriba su nombre completo, cargo, nombre de la organización y dirección de correo electrónico.
5. En el campo ID de usuario y Contraseña, cree un ID de usuario y una contraseña para iniciar sesión en ThreatGrid.
6. Haga clic en **Registrar**.

   El registro se envía a ThreatGrid y una clave de API aparece debajo del botón Registrarse. La clave se completa automáticamente en la pestaña **General**.
7. Seleccione la pestaña **General** para confirmar que la configuración de ThreatGRID ahora incluya la clave de la API.



8. Cuando reciba un correo electrónico de ThreatGrid con un vínculo donde puede iniciar sesión, inicie sesión y acepte los términos del acuerdo.

   El período de prueba de ThreatGrid comienza y Malware Analysis puede enviar cinco archivos al día a la nube de ThreatGrid para el análisis de Sandbox.

Procedimientos adicionales para configurar Malware Analysis

En este tema se proporcionan procedimientos que puede realizar un administrador para alcanzar un objetivo que no es parte de una configuración básica de Malware Analysis. Después de configurar Malware Analysis, es posible que los administradores quieran optimizar el servicio e implementar una personalización avanzada; un ejemplo de esto es implementar contenido de YARA personalizado.

- Crear una alerta personalizada en formato CEF
- Activar contenido personalizado de YARA

Crear una alerta personalizada en formato CEF

En este tema se proporcionan instrucciones para crear alertas personalizadas en formato de evento común (CEF) que se envían a un servicio que recopila eventos como CEF. Esta es una tarea de configuración avanzada que requiere conocimiento suficiente para realizar una edición manual del archivo de configuración: `/var/netwitness/malware-analytics-server/spectrum/conf/malwareCEFDictionaryConfiguration.xml`. Antes de editar el archivo, debe detener el servicio Malware Analysis en el sistema operativo. La alerta de CEF se activa cuando se reinicia el servicio Malware Analysis.

La plantilla CEF

Para enviar eventos a un servicio que recopila eventos como CEF, NetWitness Suite los procesa con un archivo de configuración que sirve de plantilla CEF antes de alimentarlos a una tecnología de correlación. Puede ajustar el archivo de configuración, el cual especifica la secuencia y el mapeo de campos de syslog en cada alerta.

El siguiente ejemplo de mensaje de syslog muestra los campos de CEF en la sección de extensiones de la alerta (después del último "|" en la alerta). Cada campo se puede configurar para indicar la secuencia (que se describe en la sección Ejemplo, a continuación). Los campos se pueden excluir por completo de la alerta mediante un ajuste de configuración.

```
CEF:0|NetWitness|Spectrum|10.3.0.7995.1.0|Suspicious Event|Detected
suspicious network event ID 4 session ID n/a|2|static=100.0
nextgen=25.0 community=100.0 sandbox=25.0 file.name=myFile.exe
file.size=1234556 file.md5.hash=DEADBEEFBABECAFEDEADBEEFBABECAFE
event.source=spectrum://admin@0:0:0:0:0:0:0:1:64563
event.type=MANUAL_UPLOAD event.id=0 country.dst.code=--
country.dst=Unavailable ip.src=0:0:0:0:0:0:0:1
ip.dst=0:0:0:0:0:0:0:1 event.uuid=f7a6155a-31de-4fa6-ba16-
41fb9a8e5f26 ...
```

Comprender una entrada del archivo de auditoría de syslog

La descripción de la estructura del archivo se basa en el siguiente ejemplo.

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125

CEF: 0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected
suspicious
 network event ID 857 session ID 73|2|

static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307

com.netwitness.event.internal.id=73
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2
referer=http://qa-fc12-149/files/MALWAREMALW...fficeDocs/DOC/
risk.info=http client server version mismatch
```

Primera línea

```
Feb 6 10:02:28 10.10.10.125 SpectrumServer125
```

Información del registro	Descripción
Feb 6 10:02:28	El registro de fecha y hora de la entrada.
10.10.10.125	La dirección IP de origen del evento.
SpectrumServer125	El nombre de host de origen del evento.

Encabezado de formato de evento común (CEF) de auditoría

```
0|NetWitness|Spectrum|1.2.1.130|Suspicious Event|Detected suspicious
network event ID 857 session ID 73|2|
```

El encabezado de CEF de auditoría es una lista separada por barras verticales con los siguientes campos:

Información del registro	Descripción
0	La versión de formato de evento común (CEF) de ArcSight utilizada para el syslog de auditoría.
NetWitness	El servicio que creó el mensaje de syslog.
Spectrum	Malware Analysis es el registrador del evento.
1.2.1.130	Versión de Malware Analysis.
event ID 857	ID de evento de red único para este evento.
session ID 73	ID de sesión único de Core de la sesión que incluyó este evento.
2	Severidad, un entero entre 1 y 6 indica el nivel de severidad del mensaje. • 1 = INFORMATION_LEVEL • 2 = WARNING_LEVEL • 3 = ERROR_LEVEL • 4 = SUCCESS_LEVEL • 5 = FAILURE_LEVEL • 6 = AUDIT_FAILURE_LEVEL

Extensión de CEF de auditoría

```
static=100.0 network=29.0 community=8.0 sandbox=N/R

file.name=-CVE-00_DOC_2010-05-13_attachment.doc  file.size=0
file.md5.hash=20a29259c0e5958afb2f50c4177bb307
com.netwitness.event.internal.id=73
```

```
com.netwitness.event.internal.uuid=37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip=10.25.50.149 client=Wget/1.11.4 Red Hat modified payload=108872
packets=136 country.dst=Private time=Fri Jan 27 10:09:25 EST 2012
threat.source=netwitness tcp.srcport=43580 action=get
com.netwitness.event.internal.source=http://QASpectrum2:50104/sdk
filetype=rtf alias.host=qa-fc12-149 eth.src=00:25:90:18:76:E2 ip.proto=6
tcp.flags=27 ip.src=10.25.50.61 tcp.dstport=80 threat.category=spectrum
eth.dst=00:0C:29:F8:50:2D lifetime=0 alert.id=nw32535 sessionid=73
medium=1 size=117864 content=spectrum.consume11 extension=doc
directory=/files/MALWAREMALWARE/OfficeDocs/DOC/ eth.type=2048
ip.dst=10.25.50.149 service=80 filename=-CVE-00_DOC_2010-05-13_
attachment.doc server=Apache/2.2.13 (Fedora) streams=2 referer=http://qa-
fc12-149/files/MALWAREMALW...fficeDocs/DOC/ risk.info=http client server
version mismatch
```

Puntajes de análisis

La primera entrada de la extensión de CEF de auditoría proporciona los cuatro puntajes de Malware Analysis para el evento: Estático, Red, Community y Sandbox.

Información del registro	Valor de ejemplo
static	100.0
red	29.0
community	8.0 Un puntaje de 0.0 puede ser un puntaje de comunidad para el evento o puede indicar que no había servicios de comunidad habilitados.
sandbox	N/R R N/R significa que no se ejecuta. Esto indica que GFI Sandbox no estaba habilitado.

Información del archivo

Las tres entradas siguientes proporcionan información de archivo: nombre, tamaño y hash de archivo.

Información del registro	Valor de ejemplo
file.name	-CVE-00_DOC_2010-05-13_attachment.doc
file.size	0

Información del registro	Valor de ejemplo
file.md5.hash	20a29259c0e5958afb2f50c4177bb307

Metadatos del evento recuperados por NextGen

El registro continúa con los metadatos de Core para el evento. Los metadatos del mensaje dependen del evento. La cantidad de datos en el mensaje se trunca según la longitud máxima en bytes configurada en los ajustes de syslog. El valor predeterminado es 1,024.

Información del registro	Valor de ejemplo
com.netwitness.event.internal.id	73
com.netwitness.event.internal.uuid	37d2bad7-06bc-4b34-88e1-df43d9710204
alias.ip	10.25.50.149
cliente	Wget/1.11.4 Red Hat modified
payload	108872
packets	136
country.dst	Private
time	Fri Jan 27 10:09:25 EST 2012
threat.source	netwitness
tcp.srcport	43580
acción	obtener
com.netwitness.event.internal.source	http://QASpectrum2:50104/sdk
filetype	rtf
alias.host	qa-fc12-149
eth.src	00:25:90:18:76:E2
ip.proto	6

Información del registro	Valor de ejemplo
tcp.flags	27
ip.src	10.25.50.61
tcp.dstport	80
threat.category	spectrum
eth.dst	00:0C:29:F8:50:2D
ciclo de vida	0
alert.id	nw32535
sessionid	73
medium	1
tamaño	117864
contenido	spectrum.consume11
extension	doc
directorio	/files/MALWAREMALWARE/OfficeDocs/DOC/
eth.type	2048
ip.dst	10.25.50.149
Servicio	80
filename	-CVE-00_DOC_2010-05-13_attachment.doc
server	Apache/2.2.13 (Fedora)
streams	2
referer	http://qa-fc12-149/files/MALWAREMALWARE/OfficeDocs/DOC/
risk.info	diferencia de versión de servidor de cliente http

Editar el archivo de configuración

1. Detenga el servicio Malware Analysis.
2. Edite el archivo de configuración como se describe en el ejemplo.
3. Inicie el servicio Malware Analysis.
   El servicio Malware Analysis comienza a procesar las alertas con el archivo de configuración y a enviar alertas CEF a los servicios designados.

Ejemplo

El archivo de configuración se puede usar para indicar los campos que aparecen en la alerta resultante, así como la etiqueta asociada a cada campo y el orden en el cual aparecen los campos de datos. El archivo de configuración consta de uno o más bloques `MalwareCefExtension` XML, como se muestra en el siguiente ejemplo. El orden de estos bloques en el archivo de configuración implica el orden de los campos de datos en la alerta CEF.

En el siguiente ejemplo, la alerta CEF incluiría dos campos de datos, `ip.src` seguido de `ip.dst`. `customKey` se usa para indicar el etiquetado del campo de datos en la alerta. Esto permite que el usuario elija una etiqueta personalizada para forzar el formato de la alerta de modo que cumpla mejor con las expectativas del consumidor de la alerta. Es decir, el formato se puede ajustar para impedir cambios no deseados en un analizador de alertas existente. Por último, el ajuste `isDisplay` determina si el campo se incluye en la salida de la alerta. Esto permite que el usuario desactive los campos de datos sin necesidad de eliminar físicamente el bloque `MalwareCefExtension` de la configuración.

```
 <config>
 <malwareExtensionList>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.src</customKey>
   <malwareKey>ip.src</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>ip.dst</customKey>
   <malwareKey>ip.dst</malwareKey>
   <isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
 </malwareExtensionList>
</config>
```

Al final del archivo de configuración hay tres configuraciones adicionales que se pueden usar para ajustar adicionalmente el formato de la alerta. Estas son las siguientes:

Configuración	Descripción
`includesUnknownMeta`	Este ajuste verdadero o falso indica si se incluyen elementos de datos desconocidos en la alerta resultante. Cualquiera de los metadatos de sesión de NextGen se puede considerar para inclusión en una alerta CEF. Debido a que se pueden introducir metadatos de sesión adicionales con la creación de nuevos analizadores NextGen, se pueden encontrar metadatos que no se incluyen en la configuración predeterminada. Puede configurar `includesUnknownMeta` en true para incluir los metadatos desconocidos en la alerta y etiquetarlos con el nombre de clave de metadatos de NextGen. Para forzar una clave personalizada para los metadatos desconocidos, debe editar este archivo y agregar un nuevo bloque `MalwareCefExtension` al diccionario. Para omitir los metadatos desconocidos de la alerta, configure `includesUnknownMeta` en false.
`displayNulls`	Este ajuste verdadero o falso indica si los valores configurados en nulo se incluyen en la alerta. Si `displayNulls` se configura en false, los campos con valores nulos se omiten incluso si su propiedad `MalwareCefExtension isDisplay` está activada. Esto permite que el formateo dinámico de alertas excluya los campos nulos.
`valueIfNull`	Este ajuste verdadero o falso permite especificar un marcador de posición de cadena (`n/a` de forma predeterminada) que se usará como el valor para cualquier campo con valores nulos. Si `displayNulls` se configura en true, los campos con valores nulos se incluyen en las alertas. Su valor se configura en el valor especificado en `valueIfNull`.

A continuación se representa el archivo de configuración de CEF predeterminado. El archivo de configuración predeterminado incluye todos los metadatos de sesión de NextGen predeterminados.

```
<config>
  <malwareExtensionList>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>static</customKey>
   <malwareKey>static</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>nextgen</customKey>
   <malwareKey>nextgen</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>community</customKey>
   <malwareKey>community</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>sandbox</customKey>
   <malwareKey>sandbox</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>file.name</customKey>
   <malwareKey>file.name</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
   <com.netwitness.malware.core.cef.MalwareCefExtension>
   <customKey>file.size</customKey>
   <malwareKey>file.size</malwareKey>
   <isDisplay>true</isDisplay>
   </com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>file.md5.hash</customKey>
<malwareKey>file.md5.hash</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.source</customKey>
<malwareKey>event.source</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.type</customKey>
<malwareKey>event.type</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.id</customKey>
<malwareKey>event.id</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>event.uuid</customKey>
<malwareKey>event.uuid</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.primary.detected</customKey>
<malwareKey>antivirus.primary.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.secondary.detected</customKey>
<malwareKey>antivirus.secondary.detected</malwareKey>
<isDisplay>true</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>antivirus.other.detected</customKey>
<malwareKey>antivirus.other.detected</malwareKey>
<isDisplay>true</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst.code</customKey>
<malwareKey>country.dst.code</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>city.dst</customKey>
<malwareKey>city.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>org.dst</customKey>
<malwareKey>org.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>payload</customKey>
<malwareKey>payload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>packets</customKey>
<malwareKey>packets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.dst</customKey>
<malwareKey>country.dst</malwareKey>
```

```
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>time</customKey>
<malwareKey>time</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.source</customKey>
<malwareKey>threat.source</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcpport</customKey>
<malwareKey>tcp.srcpport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>filetype</customKey>
<malwareKey>filetype</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.dst</customKey>
<malwareKey>latdec.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src</customKey>
<malwareKey>eth.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>agency.dst</customKey>
```

```
<malwareKey>agency.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.proto</customKey>
<malwareKey>ip.proto</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.flags</customKey>
<malwareKey>tcp.flags</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.src</customKey>
<malwareKey>ip.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.dstport</customKey>
<malwareKey>tcp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.category</customKey>
<malwareKey>threat.category</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst</customKey>
<malwareKey>eth.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>lifetime</customKey>
<malwareKey>lifetime</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>latdec.src</customKey>
<malwareKey>latdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>did</customKey>
<malwareKey>did</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alert.id</customKey>
<malwareKey>alert.id</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>country.src</customKey>
<malwareKey>country.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>sessionid</customKey>
<malwareKey>sessionid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>longdec.src</customKey>
<malwareKey>longdec.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>medium</customKey>
<malwareKey>medium</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>size</customKey>
<malwareKey>size</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.computer.dst</customKey>
<malwareKey>ad.computer.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.src</customKey>
<malwareKey>ad.username.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpackets</customKey>
<malwareKey>rpackets</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>action</customKey>
<malwareKey>action</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.domain.src</customKey>
<malwareKey>ad.domain.src</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.src.vendor</customKey>
<malwareKey>eth.src.vendor</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rpayload</customKey>
<malwareKey>rpayload</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ad.username.dst</customKey>
<malwareKey>ad.username.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>content</customKey>
<malwareKey>content</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>extension</customKey>
<malwareKey>extension</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.dst.vendor</customKey>
<malwareKey>eth.dst.vendor</malwareKey>
```

```
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>rid</customKey>
<malwareKey>rid</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>directory</customKey>
<malwareKey>directory</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.suspicious</customKey>
<malwareKey>risk.suspicious</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>eth.type</customKey>
<malwareKey>eth.type</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>ip.dst</customKey>
<malwareKey>ip.dst</malwareKey>
<isDisplay>false</isDisplay>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>service</customKey>
<malwareKey>service</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<customKey>filename</customKey>
<malwareKey>filename</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>streams</customKey>
<malwareKey>streams</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.info</customKey>
<malwareKey>risk.info</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>dest.tld</customKey>
<malwareKey>dest.tld</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>alias.host</customKey>
<malwareKey>alias.host</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>tcp.srcport</customKey>
<malwareKey>tcp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.srcport</customKey>
<malwareKey>udp.srcport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
```

```
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>udp.dstport</customKey>
<malwareKey>udp.dstport</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>domain.dst</customKey>
<malwareKey>domain.dst</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.name</customKey>
<malwareKey>feed.name</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>feed.description</customKey>
<malwareKey>feed.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>threat.description</customKey>
<malwareKey>threat.description</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>referer</customKey>
<malwareKey>referer</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>client</customKey>
<malwareKey>client</malwareKey>
<isDisplay>false</isDisplay>
```

```
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>server</customKey>
<malwareKey>server</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>risk.warning</customKey>
<malwareKey>risk.warning</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>attachment</customKey>
<malwareKey>attachment</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrar</customKey>
<malwareKey>whois.registrar</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.registrant</customKey>
<malwareKey>whois.registrant</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.date.creation</customKey>
<malwareKey>whois.date.creation</malwareKey>
<isDisplay>false</isDisplay>
</com.netwitness.malware.core.cef.MalwareCefExtension>
<com.netwitness.malware.core.cef.MalwareCefExtension>
<customKey>whois.server</customKey>
<malwareKey>whois.server</malwareKey>
```

```
    <isDisplay>false</isDisplay>
    </com.netwitness.malware.core.cef.MalwareCefExtension>
  </malwareExtensionList>
  <includesUnknownMeta>false</includesUnknownMeta>
  <displayNulls>false</displayNulls>
  <valueIfNull>n/a</valueIfNull>
</config>
```

Activar contenido personalizado de YARA

En este tema se proporcionan instrucciones para habilitar el contenido personalizado de YARA en el host de NetWitness Suite en el cual se instaló el servicio Malware Analysis. Además de los indicadores de riesgo incorporados, Malware Analysis es compatible con indicadores de riesgo escritos en YARA. YARA es un lenguaje de reglas que permite a los investigadores de malware identificar y clasificar muestras de malware. En RSA Live están disponibles indicadores de riesgo (IOC) basados en YARA incorporados; estos se descargan y se activan automáticamente en dispositivos suscritos.

Los clientes con habilidades y conocimientos avanzados pueden agregar funcionalidades de detección a RSA Malware Analysis mediante la creación de reglas YARA y su publicación en RSA Live o la colocación de estas reglas en una carpeta inspeccionada para consumo del dispositivo. En esta sección se proporcionan instrucciones para el administrador que configura dispositivos para habilitar la creación de contenido personalizado de YARA.

Requisitos previos

Esta es una tarea de configuración avanzada, que requiere el privilegio y el conocimiento suficiente para configurar una recopilación de compilador de GNU (GCC) y una biblioteca de desarrollo de C++ Python para crear YARA. Además, debe estar completamente familiarizado con la documentación estándar de YARA. Se requieren los siguientes componentes:

- La biblioteca de la expresión regular compatible con Perl (PCRE): pcre-8.33.tar.bz2
- La línea de comandos yara 1.7 (rev:167) independiente YARA: yara-1.7.tar
- La extensión de YARA para Python: yara-python-1.7.tar.gz
- Documentación de reglas de YARA: YARA User's Manual 1.6.pdf

Los componentes se pueden descargar desde aquí: https://code.google.com/p/yara-project/downloads/list

Nota: En cuanto a la escritura, YARA 2.0 está disponible, pero no es compatible con Malware Analysis 10.5.

Instalar bibliotecas y aplicaciones requeridas para crear YARA en un dispositivo basado en CentOS

Como requisito previo de la creación de YARA en un host que ejecuta CentOS, debe instalar `make`, la recopilación de compilador GNU y la biblioteca de desarrollo de C++ `Python` en el dispositivo. Para instalar las aplicaciones y bibliotecas que se requieren para crear YARA:

1. Para asegurarse de que los archivos del repositorio de YUM estándar y no de otros repositorios estén en la carpeta /etc/yum.repos.d, ingrese el siguiente comando:

   `ls -al /etc/yum.repos.d`

   Los resultados deben ser similares a lo siguiente:

   ```
   -rw-r-r-. 1 root root 1926 Jun 26  2012 CentOS-Base.repo
   -rw-r-r-. 1 root root  637 Jun 26  2012 CentOS-Debuginfo.repo
   -rw-r-r-. 1 root root  626 Jun 26  2012 CentOS-Media.repo
   -rw-r-r-. 1 root root 2593 Jun 26  2012 CentOS-Vault.repo
   ```

2. Para instalar `make` en el dispositivo, ingrese los siguientes comandos:

   a. **`yum search make`**

      Se obtiene el siguiente mensaje: `make.x86_64 : A GNU tool which simplifies the build process for user`

   b. **`yum install make.x86_64`**

3. Para instalar y probar GCC en el host, ingrese los siguientes comandos:

   a. **`yum search gcc`**

      Se muestran los siguientes mensajes:

      ```
      gcc-c+.x86_64 : C+ support for GCC
      gcc.x86_64 : Various compilers (C, C++, Objective-C, Java, ...)
      ```

   b. Ingrese los siguientes comandos:

      `yum install gcc.x86_64`
      `yum install gcc-c++.x86_64`

   c. Para probar los comandos gcc, ingrese los siguientes comandos:

      `gcc -v`
      `cc -v`

4. Para instalar la biblioteca de desarrollo de C++ Python en el dispositivo, ingrese los siguientes comandos:

   a. **`yum search python dev`**

      Se obtiene el siguiente mensaje:

      ```
      python-devel.x86_64 : The libraries and header files needed for
      ```

Python development

b. **yum install python-devel.x86_64**

Configuración de Yara

Para crear una biblioteca de desarrollo de C++ Python y GCC en la cual pueda crear YARA en el host de NetWitness Suite que ejecuta Malware Analysis:

1. Realice una de las siguientes acciones:
   a. Si el host en el cual realiza la instalación ejecuta Mac OS, instale xCode para Mac OS.
   b. Si el host en el cual realiza la instalación ejecuta CentOS, instale make, GCC y la biblioteca de desarrollo de C++ Python mediante la línea de comandos de YUM.
2. Para instalar la biblioteca de PCRE en el host, abra una ventana terminal e ingrese los siguientes comandos:

```
tar -xvf pcre-8.33.tar.bz2
cd pcre-8.33
./configure
make
sudo make install
```

3. Para instalar la línea de comandos de YARA independiente, ingrese los siguientes comandos:

```
tar -xvf yara-1.7.tar
cd yara-1.7
./configure
make
sudo make install
```

4. Para probar la línea de comandos de YARA independiente:
   a. Escriba el siguiente comando:

      yara

   b. Si el comando es exitoso, continúe con el paso 7. Si el comando falla y devuelve el error `yara: error while loading shared libraries: libpcre.so.1: cannot open shared object file: No such file or directory`, escriba el siguiente comando para comprobar el archivo `/etc/ld.so.conf` o la variable de ambiente `LD_LIBRARY_PATH`.

      ldconfig -v

5. Para instalar la extensión de YARA para Python, ingrese los siguientes comandos:

```
tar -xvf yara-python-1.7.tar.gz
```

```
cd yara-python-1.7
python setup.py build
sudo python setup.py install
```

6. Para probar la extensión de YARA:

   a. Escriba el siguiente comando: **`python`**

   b. En el indicador Python (>>>), ingrese los siguientes comandos:

   ```
   import yara
   exit()
   ```

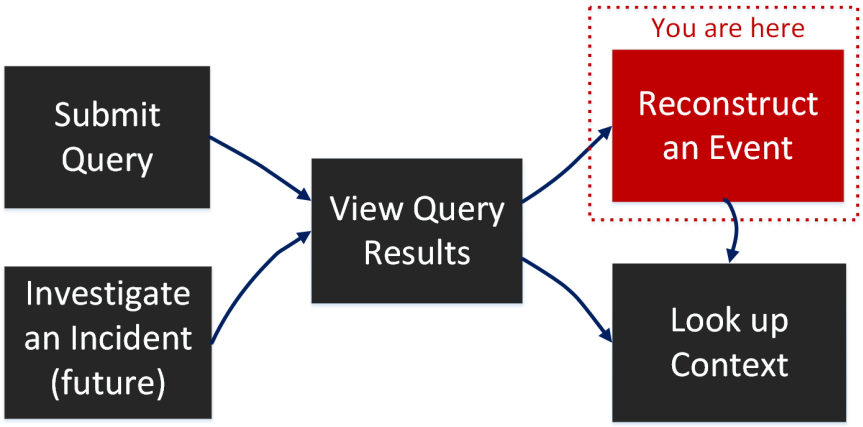
Cuando esta configuración está completa, los analistas pueden crear IOC personalizados de YARA para su consumo en un host de Malware Analysis, como se describe en “Implementar contenido personalizado de YARA” en la *Guía de Investigation y Malware Analysis*.

Referencias de Malware Analysis

Vista Configuración de servicios: Pestaña Auditoría

En la Vista Eventos y en la Vista Eventos nuevos, panel Reconstrucción (**Investigate > panel Eventos > haga clic en un evento),** puede ver de manera segura la reconstrucción de un evento de interés que encuentra en la vista Navegar o en el panel Eventos.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Buscador de amenazas	enviar consulta	Realización de una investigación
Buscador de amenazas	ver los resultados de una consulta	Analizar eventos en la vista Análisis de eventos
Buscador de amenazas	reconstruir un evento*	Reconstruir un evento
Buscador de amenazas	exportar archivos desde un evento	Reconstruir un evento
Buscador de amenazas	Buscar el contexto adicional de un evento	Búsqueda de información contextual

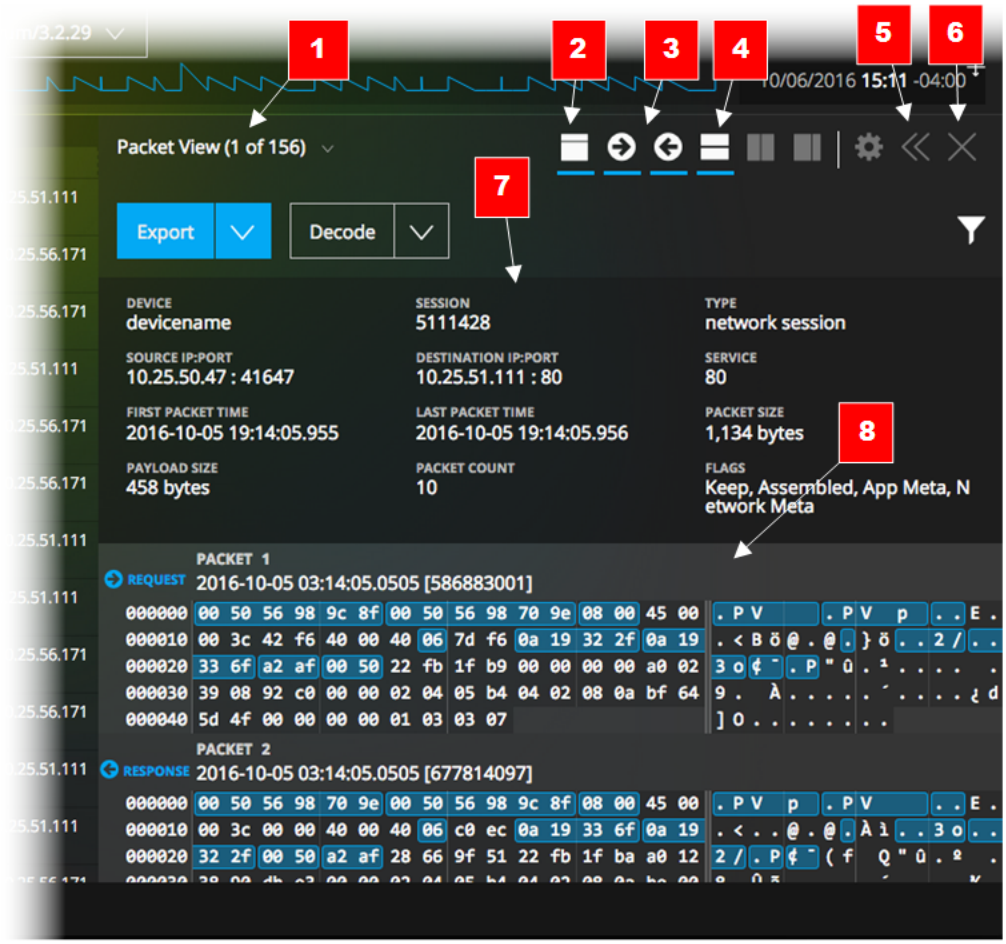
Temas relacionados

- Cómo funciona NetWitness Investigate
- Realización de una investigación
- Analizar eventos en la vista Análisis de eventos
- Vista Navegar
- Vista Análisis de eventos: Panel Análisis de texto

Vista rápida

En el panel Reconstrucción de Investigate se muestra la reconstrucción de un único evento en la vista de paquetes, la vista de archivos y la vista de texto. Cuando hace clic en un evento en el panel Eventos, en el panel Reconstrucción adyacente se muestra la reconstrucción de paquetes del evento. Puede usar las opciones de la barra de herramientas Reconstrucción de evento para cambiar el tipo y la dirección de la reconstrucción (solicitud o respuesta), ocultar o mostrar el panel de encabezado y ampliar, contraer y cerrar el panel Reconstrucción de evento. Según el tipo de reconstrucción seleccionado y el contenido de la carga útil, están disponibles opciones adicionales. Por ejemplo, puede mostrar la carga útil solo en la vista de texto, descargar archivos en la vista de archivos y descargar archivos PCAP en la vista de paquetes.

El siguiente es un ejemplo de una reconstrucción de paquetes.

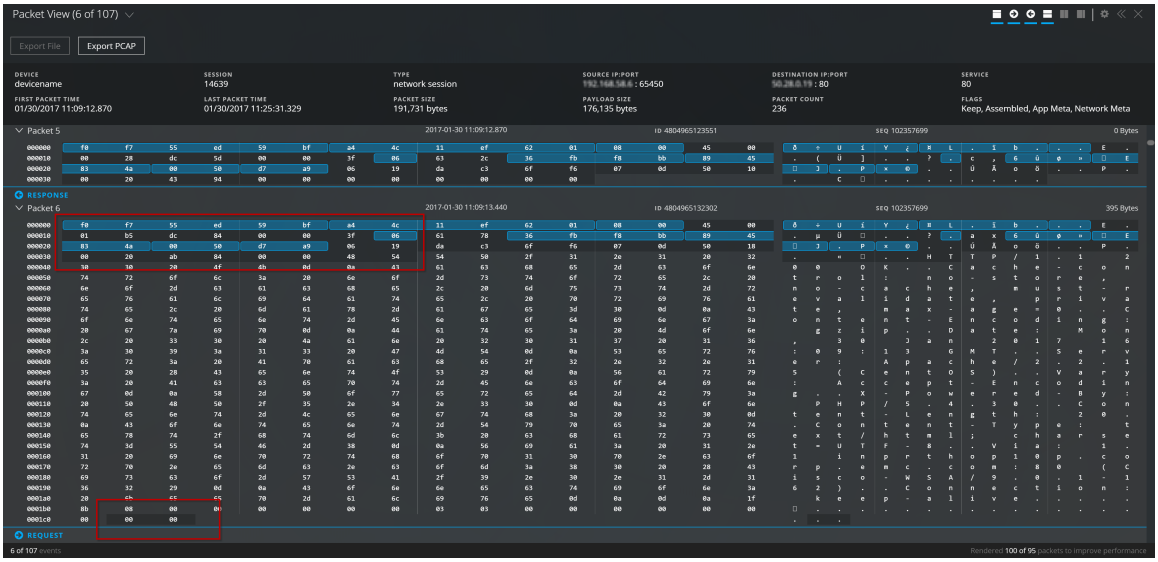


1	Pestañas o menú desplegable para seleccionar el tipo de reconstrucción: vista de paquetes, vista de archivos y vista de texto. El tipo seleccionado se muestra en la etiqueta.
2	Haga clic para ocultar o mostrar el panel del encabezado.
3	Haga clic en estos íconos para mostrar la solicitud, la respuesta o ambas.
4	Haga clic en este ícono para mostrar u ocultar el panel Metadatos de eventos, en el cual se proporciona una lista detallada de los metadatos asociados con el evento.
5	Una opción para expandir o contraer horizontalmente el panel Reconstrucción en la vista Navegar.
6	Una opción para cerrar el panel Reconstrucción.
7	El encabezado muestra información de resumen del evento que se está reconstruyendo.
8	Enumera cada paquete en el evento. Para cada paquete, puede ver el número del paquete, la dirección (solicitud o respuesta) y el contenido del paquete en formato binario a la izquierda, en formato hexadecimal en el centro y en formato de texto a la derecha.

Detalles de la reconstrucción de paquetes

En la reconstrucción de paquetes, Investigate proporciona el número del paquete, la dirección del paquete (solicitud o respuesta), la hora de inicio del paquete y, a continuación, el contenido del paquete.

Todos los paquetes comienzan con un encabezado y algunos de ellos tienen un pie de página. En la vista de paquetes, el encabezado y el pie de página tienen un fondo más oscuro, lo que le permite distinguirlos de la carga útil del paquete. El fondo más oscuro del encabezado y el pie de página aparece en formato hexadecimal y de texto.



El contenido del paquete se proporciona en formato hexadecimal y de texto. Los metadatos se resaltan en azul; cuando coloca el cursor sobre los metadatos, la información de clave/valor de metadatos se muestra como información en pantalla.

Opciones adicionales en la vista de paquetes incluyen la capacidad de descargar la PCAP del evento y mostrar solo las cargas útiles. Cuando solo se muestra la carga útil, puede usar la opción Sombrear bytes como ayuda para distinguir patrones en los datos.

Detalles de la reconstrucción de texto

En la reconstrucción de texto, los eventos de red y de registro se presentan de manera diferente. En el caso de los eventos de red, Investigate proporciona la dirección del paquete (Solicitud o Respuesta) y el contenido de cada paquete en formato de texto.

Para los eventos de registro (filtro por Media = Registro), no hay ninguna solicitud o respuesta; en la reconstrucción de texto solo se muestra el registro crudo.

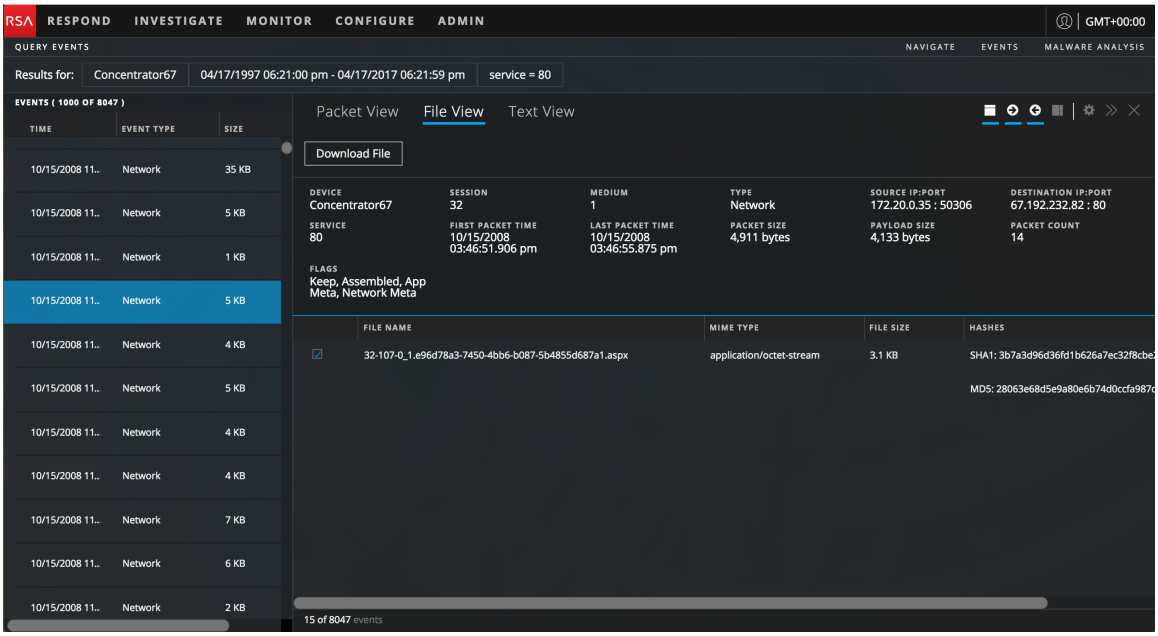
En la vista de texto está disponible un subconjunto de opciones de reconstrucción. Puede:

- Ocultar y mostrar el encabezado.
- Para los eventos de red, seleccionar la visualización solo de solicitudes, solo de respuestas o ambas.
- Para los eventos de red, exportar la sesión como un archivo PCAP.
- Para los eventos de registro, exportar el registro crudo.
- Cambiar entre una vista comprimida y descomprimida de las cargas útiles. Cuando la sesión está descomprimida, las partes comprimidas del texto se vuelven legibles.
- Seleccionar el texto que se decodificará o codificará.

Nota: Esta función no está disponible para la vista de archivos, las sesiones de red no HTTP y los datos del registro.

Detalles de la reconstrucción de archivos

En la reconstrucción de archivos, Investigate presenta una lista de archivos asociados con el evento de red seleccionado.



Puede seleccionar un archivo, varios archivos o todos ellos para exportarlos al sistema de archivos local. Cuando se seleccionan archivos, el botón Exportar archivos se activa y refleja la cantidad de archivos seleccionados. Cuando se hace clic en el botón, los archivos seleccionados se exportan como un archivo zip, lo cual garantiza que la aplicación predeterminada no abra ni ejecute archivos potencialmente maliciosos. El nombre del archivo exportado usa la siguiente convención:

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

donde:

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

Para impedir que un archivo se descomprima automáticamente cuando se descarga, NetWitness Suite lo exporta con protección con contraseña. Para abrir un archivo, escriba la siguiente contraseña: **netwitness**.

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

Descripción detallada

Función	Descripción
Menú Tipo de reconstrucción	En este menú, puede seleccionar el tipo de reconstrucción: **Paquete** o **Archivo**. Cuando abre una reconstrucción por primera vez, NetWitness Suite elige de manera predeterminada la mejor reconstrucción.
Opciones de descarga	Opciones para exportar un registro, una PCAP o archivos con el fin de realizar un análisis más detallado y compartir con otros.

Función	Descripción
	Controla la visualización de un encabezado sobre la lista de paquetes; puede hacer clic en este ícono para ocultar el encabezado o mostrarlo. Cuando el encabezado se oculta, queda más espacio para la lista de paquetes y se reduce la cantidad de desplazamiento necesario para ver más paquetes. El encabezado proporciona información sobre el evento reconstruido: el nombre del servicio que recopiló el paquete, el número de sesión o de evento, el tipo de evento (red), la IP y el puerto de origen, la IP y el puerto de destino, el tipo de servicio, la hora del primer paquete en el evento, la hora del último paquete en el evento, el tamaño del evento, el tamaño de la carga útil en bytes, el conteo de paquetes y las marcas aplicadas al evento (conservar, ensamblado, metadatos de aplicación y metadatos red).
	Dos controles activan y desactivan la visualización de solicitud y respuesta (consulte Reconstrucción de un evento).
	Muestra los detalles de metadatos para el evento en otro panel.
	(Futuro) Menú Ajustes de configuración.
	Controles de dimensionamiento para el panel Reconstrucción (consulte Reconstrucción de un evento).
	Cierra el panel Reconstrucción. Ahora, la vista muestra únicamente el panel Eventos.

Vista Configuración de servicios: Pestaña Antivirus

En este tema se presentan las características y las funciones de la pestaña Antivirus en la vista Configuración de servicios de un servicio Malware Analysis. La pestaña Antivirus proporciona una manera de identificar a los proveedores de software antivirus cuyos productos de software se utilizan en la red. NetWitness Suite puede incluir los resultados de estos proveedores en la vista de resultados detallados de un evento que se analizó mediante Malware Analysis.

Este es un ejemplo de la pestaña Antivirus.

Funciones

La pestaña AV muestra una lista de los proveedores de antivirus cuyo software posiblemente esté instalado en la red. Existen dos categorías de proveedores: Primario, que es el de más confianza, y Secundario, que es menos conocido. El nombre de cada proveedor tiene una casilla de verificación y un ícono. Si marca el nombre de un proveedor indica que ha instalado el software de AV seleccionado de ese proveedor en el ambiente.

Esta tabla describe las opciones de la pestaña AV.

Función	Descripción
Casilla de verificación del proveedor	Elija uno o más proveedores de antivirus en la lista que se proporciona para indicar los productos instalados en la organización local.
Aplicar	Guarda los cambios realizados en la pestaña AV.
Restablecer	Restablece la lista de antivirus a su estado predeterminado, en el cual no hay proveedores seleccionados.

Vista Configuración de servicios: Pestaña General

En este tema se presentan los ajustes de configuración de la vista Configuración de servicios > pestaña General para Malware Analysis, la cual tiene parámetros específicos del servicio Malware Analysis. En esta pestaña se configura lo siguiente:

- Los parámetros de procesamiento de los servicios Core que están capturando datos.
- El repositorio de los datos capturados.
- Las categorías de puntaje de Static, Community y Sandbox que se utilizan para analizar los datos.

La siguiente tarea proporciona procedimientos detallados: Configurar ajustes generales de Malware Analysis.

Este es un ejemplo de la pestaña General.

Esta pestaña tiene cuatro secciones: Configuración de escaneo continuo, Configuración de repositorio, Varios y Configuración de módulos.

Sección Configuración de escaneo continuo

Esta tabla describe las funcionalidades de la sección Configuración de escaneo continuo.

Parámetro	Descripción
Habilitado	Habilita o deshabilita completamente el sondeo continuo del servicio principal. De manera predeterminada, esta opción no está seleccionada (**deshabilitada**).

Parámetro	Descripción
Consulta	Mientras el Decoder está analizando el tráfico de red, este crea un campo de metadatos llamado Contenido con el valor **spectrum.consume** en las sesiones que probablemente contengan malware. De manera predeterminada, Malware Analysis solo realiza análisis en los eventos que tienen este valor de metadatos específico. Cuando se cambia esta consulta, Malware Analysis se puede configurar para que analice distintos tipos de eventos. Si esta consulta es demasiado general, puede hacer que Malware Analysis analice demasiados eventos, lo cual puede causar retrasos o un bajo rendimiento. La consulta predeterminada es **select * where content='spectrum.consume'**
Vencimiento de la consulta	Cuando Malware Analysis realiza una consulta de metadatos al servicio principal, obtiene el resultado en pocos segundos. Si hay un problema, como un inconveniente con la conectividad de red, Malware Analysis abandona la consulta después de esta cantidad de tiempo configurada. El valor predeterminado es **3600 segundos**.
Intervalo de consultas	La frecuencia, en minutos, con la cual se consulta sobre nuevos metadatos y archivos de sesión.
Límite de metadatos	Cada vez que Malware Analysis realiza una consulta al servicio principal, extrae una cantidad de metadatos hasta este límite de metadatos. Mediante este ajuste, junto con el intervalo de consulta, puede optimizar el rendimiento de Malware Analysis en la infraestructura principal. El valor predeterminado es **25,000**.

Parámetro	Descripción
Límite de tiempo	Malware Analysis analiza las sesiones que ocurrieron después del Límite de tiempo. Este ajuste es de mayor importancia cuando se instala un dispositivo Malware Analysis nuevo, dado que determina cuánto hay que retroceder en el tiempo para comenzar el análisis. Si configura el límite en demasiadas horas pasadas, puede hacer que Malware Analysis analice demasiados eventos pasados, lo cual provoca una gran demora antes de que se muestre cualquier tráfico que ocurre en tiempo real. El valor predeterminado es **24** horas.
Host de origen	Nombre de host del dispositivo Malware Analysis. Esta es la dirección IP, o el nombre de host, del servicio al cual Malware Analysis realiza consultas para recuperar sus datos para análisis. No utilice localhost como el host de origen. Según el modelo del dispositivo y la configuración de la infraestructura de NetWitness Suite, este host de origen puede variar.
Puerto de origen	Malware Analysis se comunica con la infraestructura de NetWitness Suite mediante el servicio REST que escucha en este puerto. Este número de puerto es específico para el tipo del servicio principal que se usa como el host de origen. Esto corresponde a las conexiones de salida del servicio principal.
Nombre de usuario	Nombre de usuario. El valor predeterminado es **admin**. Malware Analysis debe autenticar el host de origen cada vez que realiza consultas de datos. En la mayoría de los casos, la cuenta que utiliza Malware Analysis es la misma que se usa para acceder al servicio principal mediante NetWitness Suite. Sin embargo, se recomienda crear una cuenta nueva en el servicio principal que sea exclusiva para Malware Analysis.
Contraseña de usuario	Contraseña del usuario. El valor predeterminado es **netwitness**.

Parámetro	Descripción
SSL	Use SSL cuando se comunique con el servicio principal. Si Malware Analysis está usando una conexión SSL para comunicarse con un servicio principal, seleccione esta opción. El valor predeterminado es ninguna selección.
Prevención de negación de servicio (DOS)	La función Prevención de negación de servicio brinda protección contra malware que genera, intencionalmente, altos volúmenes de conexiones de red entre dos terminales con contenido de Windows PE. La generación de un alto volumen de conexiones aumenta artificialmente la cantidad de tráfico que deben consumir y analizar los servicios de seguridad que monitorean la red, lo cual da lugar a una negación de servicio. Esta función permite identificar estas sesiones de modo que el procesamiento del análisis las omita. El valor predeterminado es ninguna selección.
Duración de ventana de tasa de sesiones de DOS (segundos)	Malware Analysis usa este parámetro junto con los parámetros **Cantidad de sesiones de DOS por ventana de tasa** y **Tiempo de bloqueo de sesiones de DOS (segundos)** para identificar un ataque de negación de servicio y determinar el tiempo durante el cual se hace caso omiso de las sesiones de una única dirección IP. Para identificar un ataque de negación de servicio, Malware Analysis monitorea la cantidad de sesiones que establece una única dirección IP durante un intervalo de tiempo específico. La **Duración de ventana de tasa de sesiones de DOS (segundos)** define este intervalo de tiempo. Si la cantidad de sesiones supera la configuración de **Cantidad de sesiones de DOS por ventana de tasa** en la cantidad de segundos definida en **Duración de ventana de tasa de sesiones de DOS**, Malware Analysis identifica la actividad como un intento de negación de servicio. En este caso, el tráfico que proviene de la dirección IP no se considera durante el tiempo especificado en **Tiempo de bloqueo de sesiones de DOS (segundos)**. El valor predeterminado es **60** segundos.

Parámetro	Descripción
Cantidad de sesiones de DOS por ventana de tasa	Malware Analysis usa este parámetro junto con los parámetros **Duración de ventana de tasa de sesiones de DOS (segundos)** y **Tiempo de bloqueo de sesiones de DOS (segundos)** para identificar un ataque de negación de servicio y determinar el tiempo durante el cual se hace caso omiso de las sesiones de la dirección IP. Para identificar un ataque de negación de servicio, Malware Analysis monitorea la cantidad de sesiones que establece un único origen IP durante un intervalo de tiempo específico. La **Duración de ventana de tasa de sesiones de DOS (segundos)** define este intervalo de tiempo. Si la cantidad de sesiones supera la configuración de **Cantidad de sesiones de DOS por ventana de tasa** en la cantidad de segundos definida en **Duración de ventana de tasa de sesiones de DOS**, Malware Analysis identifica la actividad como un intento de negación de servicio. En este caso, el tráfico no se considera durante el tiempo especificado en **Tiempo de bloqueo de sesiones de DOS (segundos)**. El valor predeterminado es **200** sesiones.
Tiempo de bloqueo de sesiones de DOS (segundos)	Malware Analysis usa este parámetro junto con los parámetros **Duración de ventana de tasa de sesiones de DOS (segundos)** y **Cantidad de sesiones de DOS por ventana de tasa** para identificar un ataque de negación de servicio y determinar el tiempo durante el cual se hace caso omiso de él. Para identificar un ataque de negación de servicio, Malware Analysis monitorea la cantidad de sesiones que establece una única dirección IP durante un intervalo de tiempo específico. La **Duración de ventana de tasa de sesiones de DOS (segundos)** define este intervalo de tiempo. Si la cantidad de sesiones supera la configuración de **Cantidad de sesiones de DOS por ventana de tasa** en la cantidad de segundos definida en **Duración de ventana de tasa de sesiones de DOS**, Malware Analysis identifica la actividad como un intento de negación de servicio. En este caso, el tráfico no se considera durante el tiempo especificado en **Tiempo de bloqueo de sesiones de DOS (segundos)**. El valor predeterminado es **60** segundos.

Parámetro	Descripción
Intervalo de recopilación de residuos de DOS (segundos)	Ejecuta la recolección de elementos no utilizados en la estructura de la memoria interna que se usa para rastrear intentos de negación de servicio. Si el uso de la memoria es anormalmente alto, puede disminuir este ajuste para liberar memoria sin uso más a menudo. Si el uso de la CPU es anormalmente alto, puede aumentar este ajuste para eliminar la sobrecarga de procesamiento (a expensas del uso de la memoria). El valor predeterminado es **120** segundos.

Sección Configuración de repositorio

Malware Analysis almacena todos los archivos que se analizan para usarlos en el futuro. Estos archivos se pueden descargar mediante la interfaz del usuario o se puede tener acceso a ellos mediante uno de los protocolos de uso compartido de archivos.

Esta tabla describe las funcionalidades de la sección Configuración de repositorio.

Parámetro	Descripción
Ruta al directorio	Todos los archivos se almacenan en el siguiente directorio del dispositivo Malware Analysis: **/var/lib/netwitness/spectrum**
Protocolo de uso compartido de archivos	Los posibles valores para el protocolo de uso compartido de archivos son: FTP, SAMBA y Ninguno. Puede habilitar el acceso FTP y el uso compartido de archivos SAMBA para permitir a los usuarios acceder a los archivos almacenados en Malware Analysis desde una ubicación remota. No se necesitan credenciales para obtener acceso a estos archivos. El puerto que se requiere para el acceso FTP es TCP/21. El protocolo predeterminado de uso compartido de archivos es **Ninguno**.
Retención (en días)	Malware Analysis mantiene los archivos almacenados en el repositorio durante una cantidad específica de días. Puede establecer la cantidad de días durante los cuales se retendrán archivos antes de eliminarlos. El valor predeterminado es **60** días.

Sección Configuraciones varias (10.3 SP2 y superior)

En esta tabla se describen las funciones de la sección Configuraciones varias.

Parámetro	Descripción
Tamaño máximo de archivo	Limita el tamaño de cada archivo que se puede escanear manualmente. Este parámetro se aplica a la función que se describe en la sección "Cargar archivos para escaneo de malware" de la Guía de configuración de Investigation y Malware Analysis. El valor predeterminado es **64 MB**. Si se supera el límite del tamaño de archivo, le impide escanearlo.

Sección Configuración de módulos

La sección Configuración de módulos permite la configuración de las categorías de puntaje de Static, Community y Sandbox.

Configuración de análisis estático

El módulo Static es la única categoría de puntaje que está activada de forma predeterminada. Esta tabla describe los parámetros para configurar el análisis estático.

Función	Descripción
Habilitado	Activa o desactiva por completo el análisis estático. Esto está seleccionado de manera predeterminada (**activado**).
Omitir PDF	Desactiva el análisis de documentos PDF. De manera predeterminada, esto no está seleccionado; todos los archivos PDF se someten a un análisis estático.
Omitir Office	Desactiva el análisis de documentos de Office. De manera predeterminada, esto no está seleccionado; todos los archivos MS Office se someten a un análisis estático.

Función	Descripción
Omitir archivo ejecutable	Desactiva el análisis de documentos de Windows PE. De manera predeterminada, esto no está seleccionado; todos los archivos de Windows PE se someten a un análisis estático.
Validar configuración de Windows PE Authenticate a través de la nube	Especifica si los archivos de Windows PE se envían o no a la nube de RSA-NetWitness para una validación de Authenticode. El valor predeterminado es estar seleccionado. • Cuando esta función está seleccionada, cualquier archivo de Windows PE que esté firmado digitalmente se transmite a través de la red (en su totalidad) a la nube de RSA-NetWitness para que se valide. Si el propósito es evitar que los archivos de Windows PE salgan de la red del cliente, debe desactivar esta opción. • Cuando no está seleccionada, TODOS los análisis estáticos se ejecutan de manera local (se omite la validación de Authenticode). Independiente de este ajuste, los documentos PDF y de M/S Office no están sujetos a la validación de Authenticode y no se transmiten a través de la red durante el análisis estático.

Configuración de análisis de Community

De manera predeterminada, el módulo Community está desactivado y sus opciones se seleccionan para evitar que se procesen los documentos PDF y MS Office. El propósito es configurar los ajustes de manera predeterminada con las opciones más restrictivas, de manera que ningún documento confidencial salga de la red a menos que el usuario lo desee. Esta tabla describe los parámetros para configurar el análisis de Community.

Función	Descripción
Habilitado	Activa o desactiva por completo el análisis estático. De manera predeterminada, esta opción no está seleccionada (**deshabilitada**).
Omitir PDF	Desactiva el análisis de documentos PDF. Esta opción está seleccionada de manera predeterminada; no se procesan los archivos PDF.

Función	Descripción
Omitir Office	Desactiva el análisis de documentos de Office. Esta opción está seleccionada de manera predeterminada; no se procesan los documentos de Microsoft Office.
Omitir archivo ejecutable	Desactiva el análisis de documentos de Windows PE. Esta opción está seleccionada de manera predeterminada; los documentos de Windows PE no se procesan

Configuración del análisis de Sandbox

De manera predeterminada, el módulo Sandbox está desactivado y se impide el procesamiento de archivos PDF y de MS Office. El propósito es establecer los ajustes más restrictivos para obligar al usuario a seleccionar de manera específica si se envía o no información potencialmente confidencial fuera de la red para procesamiento. Si no se impide el procesamiento del tipo de documento, el archivo se envía en su totalidad al servidor Sandbox de destino (no se limita a un hash de los contenidos del archivo).

Esta tabla describe los parámetros para configurar el análisis de Sandbox.

Función	Descripción
Habilitado	Activa o desactiva por completo el análisis de Sandbox. De manera predeterminada, esta opción no está seleccionada (**deshabilitada**).
Omitir PDF	Desactiva el análisis de documentos PDF. Esta opción está seleccionada de manera predeterminada; no se procesan los archivos PDF. Cuando no está seleccionada, todos los archivos PDF se envían por completo a Sandbox para análisis.
Omitir Office	Desactiva el análisis de documentos de Office. Esta opción está seleccionada de manera predeterminada; no se procesan los documentos de Microsoft Office. Cuando no está seleccionada, todos los archivos de MS Office se envían por completo a Sandbox para análisis.

Función	Descripción
Omitir archivo ejecutable	Desactiva el análisis de documentos de Windows PE. Esta opción está seleccionada de manera predeterminada; los documentos de Windows PE no se procesan. Cuando no está seleccionada, todos los documentos de Windows PE se envían por completo a Sandbox para análisis
Conservar el nombre de archivo original cuando se realice un análisis de Sandbox	En 10.3 SP2 y superior, active la capacidad de aplicar hash a nombres de archivo cuando se envían a un Sandbox local. De forma predeterminada, esta opción no está seleccionada. **Nota:** Si no selecciona este parámetro, NetWitness Suite aplica hash a los archivos.

Configuración de GFI Sandbox

En la sección GFI Sandbox puede activar el procesamiento de Sandbox según GFI y configurar el GFI Sandbox instalado localmente. La tabla describe los parámetros para configurar GFI Sandbox.

Función	Descripción
Habilitado	Cuando está activado, una copia local de GFI ejecuta el procesamiento de Sandbox. El valor predeterminado es **deshabilitado**. Si activa GFI, debe configurar los parámetros restantes.
Nombre del servidor	El nombre de servidor de GFI Sandbox. No hay valor predeterminado.
Puerto del servidor	El puerto del servidor de GFI Sandbox. El valor predeterminado es **80**.
Periodo máximo de encuesta	Determina cuánto tiempo se debe esperar para que termine el procesamiento de una muestra enviada. El valor predeterminado es **600 segundos**.

Función	Descripción
Omitir configuración de proxy web	Indica a Malware Analysis que omita el proxy web, si hay uno configurado, en el momento en que se establece esta conexión. Si no se configuró un proxy web en Malware Analysis, no se hace caso de la configuración.

Configuración de ThreatGrid Sandbox

En la sección ThreatGrid Sandbox, puede habilitar el procesamiento de Sandbox por parte de ThreatGrid y seleccionar si desea usar el ThreatGrid instalado localmente o la nube de ThreatGrid para los análisis de Sandbox.

- Si tiene una copia local de ThreatGrid, configure el procesamiento de Sandbox para usar la copia local.
- Si no se han adquirido e instalado instancias locales de ThreatGrid, configure la nube de ThreatGrid.

En la tabla se describen los parámetros para configurar ThreatGrid Sandbox.

Nota: Antes de habilitar este servicio, debe configurar una clave de servicio que suministra ThreatGrid. La clave de servicio permite a ThreatGrid reconocer que las muestras enviadas desde este sitio son legítimas.

Función	Descripción
Habilitado	Cuando esta función está activada, el procesamiento de Sandbox lo ejecuta ThreatGrid, ya sea una copia local o la nube de ThreatGrid. El valor predeterminado es **deshabilitado**.
Clave de servicio	Antes de activar el módulo Sandbox, se debe configurar una clave de servicio suministrada por ThreatGrid. La clave de servicio permite a ThreatGrid reconocer que las muestras enviadas desde este sitio son legítimas.
URL	La dirección URL del servidor de ThreatGrid que se utilizará (si no se está utilizando un ThreatGrid instalado localmente). Se puede acceder a la nube de ThreatGrid en https://panacea.threatgrid.com.

Función	Descripción
Omitir configuración de proxy web	Indica a Malware Analysis que omita el proxy web, si hay uno configurado, en el momento en que se establece esta conexión. Si no se configuró un proxy web en Malware Analysis, no se hace caso de la configuración.

Vista Configuración de servicios: Pestaña Hash

En este tema se presentan las características y las funciones disponibles en la vista Configuración de servicios > pestaña Hash para Malware Analysis.

En esta pestaña, puede administrar el filtrado de hash en Malware Analysis. La cuadrícula de hash está inicialmente vacía; la cuadrícula muestra los filtros que se han agregado a Malware Analysis. En esta vista, puede agregar un filtro de hash, eliminar un filtro de hash, marcar un filtro de hash como confiable o no confiable y guardar los cambios.

Este es un ejemplo de la pestaña Hash.

Este es un ejemplo del cuadro de diálogo Agregar hash.

Funciones

La pestaña **Hash** consta de una barra de herramientas y de una cuadrícula de hash paginable.

En esta tabla se describe la barra de herramientas de la pestaña Hash.

Función	Descripción
Búsqueda de MD5	Ingrese un hash MD5 para el cual desea buscar resultados en el grid. La función de búsqueda no distingue mayúsculas de minúsculas.
Agregar	Muestra el cuadro de diálogo Agregar hash en el cual puede agregar un hash nuevo al grid de hash, especificar si el hash es confiable o no y proporcionar el tamaño del archivo de hash.
Guardar edición	Guarda las adiciones o ediciones realizadas a los hashes del grid.
Eliminar	Elimina los hashes seleccionados de la cuadrícula.

Esta tabla describe las columnas del grid de Hash.

Función	Descripción
Seleccione una casilla de verificación	Haga clic para seleccionar una fila. Haga clic en el encabezado de columna para seleccionar un encabezado.

Función	Descripción
Confiable	Marca un hash como confiable o no confiable.
MD5	Identifica el hash MD5.
Tamaño del archivo	Identifica el tamaño del archivo de hash en kilobytes.

Vista Configuración de servicios: Pestaña Indicadores de riesgo

En este tema se presentan las características y las funciones disponibles en la vista Configuración de servicios > pestaña Indicadores de riesgo que se aplican al servicio Malware Analysis. Esta pestaña permite configurar la forma en que cada uno de los cuatro módulos de puntaje usa las reglas disponibles para otorgar puntajes a los datos.

Este es un ejemplo de la pestaña Indicadores de riesgo.

Funciones

La pestaña Indicadores de riesgo consiste en una barra de herramientas y un grid paginable.

Esta tabla describe las funcionalidades del grid.

Función	Descripción
Lista de selección de módulo	Selecciona el módulo de puntaje cuyos indicadores de riesgo usted desea ver: Todos, Red, Estático, Community, Sandbox o Yara.
Campo Buscar	Escriba el texto que desee buscar en el campo Descripción.
Opción Buscar	Filtra el grid para mostrar solamente las descripciones que coinciden con el término de búsqueda de la descripción.
Opción Activar todo	Haga clic en este botón para activar todas las reglas del módulo de puntaje, en lugar de activar todas las reglas de la página utilizando las casillas de verificación.
Opción Habilitar	Haga clic en este botón para activar las reglas seleccionadas.
Opción Deshabilitar todo	Haga clic en este botón para desactivar todas las reglas del módulo de puntaje, en lugar de desactivar todas las reglas de la página utilizando las casillas de verificación.

Función	Descripción
Opción Deshabilitar	Haga clic en este botón para desactivar las reglas seleccionadas.
Opción Restablecer todo	Haga clic en este botón para restablecer todas las filas de la página a sus valores predeterminados.
Opción Restablecer	Haga clic en este botón para restablecer las filas seleccionadas a sus valores predeterminados.
Opción Guardar	Haga clic en este botón para guardar los cambios que realizó en esta página. Si sale de esta página sin guardar, los cambios se pierden. La descripción de cada fila con cambios sin guardar tiene una esquina roja.

Esta tabla describe las funcionalidades de la barra de herramientas.

Columna	Descripción
Casilla de verificación de selección	Las casillas de verificación para seleccionar filas individuales o para todas las filas de la página.
Casilla de verificación Activado	Si el indicador de riesgo está habilitado, Malware Analysis usa la regla para otorgar puntajes a los datos de la sesión.
Casilla de verificación Alta confianza	Si está seleccionada, Malware Analysis considera que la regla tiene muchas posibilidades de indicar la presencia de malware, y en la cuadrícula de resultados se marca un evento que la activa.
Descripción	Describe el Indicador de riesgo.

Columna	Descripción
Puntaje	Especifica el puntaje que desea factorizar en el puntaje total de cualquier evento que active la regla. Se muestra el puntaje predeterminado y puede aumentarlo o disminuirlo si arrastra el control deslizante o escribe un número en el cuadro de puntaje.
Tipo de archivo	Muestra los tipos de archivos a los cuales se aplican la regla. Los posibles valores son **TODOS**, **PDF**, **MS Office** y **Windows PE**.

Vista Configuración de servicios: Pestaña Integración

En este tema se presentan las características y las funciones de la pestaña Integración en la vista Configuración de servicios de Administration para Malware Analysis. Esta pestaña proporciona una manera de probar las conexiones y de habilitar el puntaje de Comunidad mediante el registro del servicio Malware Analysis. Un administrador puede probar la conexión a cloud.netwitness.com y a un servicio principal que se configuró para el escaneo continuo.

La siguiente figura es un ejemplo de la pestaña Integración.

Funciones

Esta pestaña tiene dos secciones: Prueba y registro de la conexión a RSA Cloud y Prueba de conexión de escaneo continuo. En la siguiente tabla se describen las funciones.

Función	Descripción
Botón Prueba y registro de la conexión a RSA Cloud	Si se hace clic en este botón, se prueba una conexión activa a cloud.netwitness.com. NetWitness Suite prueba las comunicaciones con el sitio y verifica la configuración de proxy. Se requiere una conexión válida para registrarse en el servicio de la comunidad de RSA.
Nombre de la empresa	El nombre de la empresa. Este campo es obligatorio.
Correo electrónico de contacto	El correo electrónico de contacto. Este campo es obligatorio.

Función	Descripción
Casilla de verificación Solo uso interno de EMC	Este es un campo opcional. Los clientes, los vendedores o los usuarios de demo de EMC deben seleccionar esta opción para asegurarse de que sus solicitudes no usen ancho de banda en el servidor de producción. Cuando se selecciona la casilla, se muestra la siguiente advertencia: `Checking this box may cause a less robust performance because the production server isn't being used.`
Botón Registrar	Cuando se hace clic en el botón Registrar, se realiza el registro en caso de que se hayan completado todos los campos obligatorios. Una vez finalizado el registro, el botón Registrar se convierte en el botón Actualizar.
Botón Update	El botón Actualizar se muestra una vez que se completa el registro.
Botón Prueba de conexión de escaneo continuo	Si se hace clic en este botón, se inicia una comprobación para verificar que el servicio Malware Analysis pueda conectarse al servicio principal seleccionado para escaneo continuo (el Host de origen, el Puerto de origen, el Nombre de usuario y la Contraseña de usuario especificados en la pestaña General).

Vista Configuración de servicios: Pestaña Resumen de IOC

En este tema se presentan las características y las funciones disponibles en la vista Configuración de servicios > pestaña Resumen de IOC. Esta pestaña proporciona una manera de ver información resumida para cualquier IOC. Una cuadrícula para cada módulo de puntaje enumera los IOCs configurados junto con las estadísticas asociadas con ese IOC de un rango de tiempo específico. Las estadísticas incluyen:

- La cantidad de eventos para una sesión de red o la cantidad de archivos para un evento estático, de Community o Sandbox que se marcaron con el IOC.
- El puntaje actual configurado para el IOC en la pestaña Indicadores de riesgo.
- Los puntajes devueltos por cada uno de los módulos de puntaje.

Cuando selecciona un evento, puede mostrar la vista Eventos de malware o la vista Archivos de malware del IOC. También puede abrir el IOC seleccionado en la pestaña Indicadores de riesgo para editar el puntaje actual.

Este es un ejemplo de la pestaña Resumen de IOC para el módulo de puntaje de red.

Funciones

El Resumen de IOC se compone de cuatro pestañas, una para cada módulo de puntaje: Red, Static, Comunidad y Sandbox. Cada pestaña tiene la misma forma y la misma información con una barra de herramientas y una cuadrícula paginable.

En esta tabla se describen las funcionalidades de cada pestaña.

Función	Descripción
Rango de tiempo	Selecciona el rango de tiempo para el Resumen de IOC. Los valores posibles son: Últimos 5 minutos, Últimos 15 minutos, Últimos 30 minutos, Última hora, Últimas 3 horas, Últimas 6 horas, Últimas 12 horas, Últimas 24 horas, Últimos 2 días, Últimos 5 días, Primera hora, Mañana, Tarde, Noche, Todo el día, Ayer, Esta semana, La semana pasada o Personalizado.
Columna Descripción	Lista las descripciones de los IOC.

Función	Descripción
Columna Conteo	Lista la cantidad de apariciones de los IOC. En la pestaña Red, el conteo es la cantidad de eventos en los que se encontró el IOC. En las otras pestañas, el conteo es la cantidad de archivos en los que se encontró el IOC.
Columna Puntaje actual	Lista el puntaje actual de los IOC como está configurado en la pestaña Indicadores de riesgo.
Columnas Estático, Red, Community y Sandbox.	Lista los puntajes que cada uno de los módulos de puntaje dio a los IOC.
Menú desplegable Acciones	El menú desplegable Acciones tiene dos opciones: Mostrar eventos/archivos y editar. Mostrar eventos abre el IOC en la vista Eventos de Investigation o en la vista Archivos. Esta vista también se puede abrir con doble clic en el IOC. Editar abre el IOC en la pestaña Indicadores de riesgo para editar el puntaje actual.

Vista Configuración de servicios: Pestaña Proxy

En este tema se presentan los parámetros configurados en la pestaña Proxy de la vista Configuración de servicios de un servicio Malware Analysis. En esta pestaña se configura la comunicación de Malware Analysis a través del proxy web con RSA Cloud para los análisis de Community y con el servicio Sandbox para los análisis de Sandbox, con el fin de conservar el anonimato. Si está utilizando un servicio de Sandbox local, no se necesitan las comunicaciones a través del proxy web y el rendimiento puede disminuir. Cuando se configura el módulo Sandbox en la pestaña **General**, puede elegir omitir el proxy web configurado.

Este es un ejemplo de la pestaña Proxy.

Funciones

Esta tabla describe las funcionalidades de la pestaña Proxy.

Función	Descripción
Habilitado	Seleccione la casilla de verificación para activar la comunicación a través del proxy web con la nube de RSA para realizar los análisis de Community y con el servicio de Sandbox para los análisis de Sandbox, con el fin de conservar el anonimato.
Detectar automáticamente la configuración del proxy web	Seleccione la casilla de verificación para usar los ajustes configurados en los ajustes del sistema.
Host proxy	Escriba el nombre de host para el host de proxy.
Puerto de proxy	Escriba el puerto que se utiliza para la comunicación en el host de proxy
Usuarios	Escriba el nombre de usuario utilizado para iniciar sesión en el host de proxy.
Contraseña de usuario	Escriba la contraseña para iniciar sesión en el host de proxy.

Función	Descripción
SSL	(Opcional) Seleccione la casilla de verificación para activar la comunicación utilizando SSL.
Botón Aplicar	Haga clic en el botón **Aplicar** para enviar la configuración seleccionada.

Vista Configuración de servicios: Pestaña ThreatGRID

En este tema se presentan los parámetros necesarios para obtener una clave de API de ThreatGrid de prueba en la pestaña **ThreatGRID** de Malware Analysis, lo cual proporciona un método para obtener una clave de API de ThreatGrid de prueba que se puede usar en el Sandbox de la nube de ThreatGrid. Antes de habilitar ThreatGrid como el servicio de Sandbox en el módulo Sandbox, se debe configurar una clave de servicio que suministra ThreatGrid, de forma que ThreatGrid pueda reconocer que las muestras enviadas desde este sitio son legítimas.

Si no tiene una clave de servicio suministrada por ThreatGrid, puede obtener una utilizando esta pestaña. La clave se proporciona a modo de evaluación.

Este es un ejemplo de la pestaña ThreatGrid.

Funciones

En esta tabla se describen las funciones de la pestaña **ThreatGrid**.

Función	Descripción
Nombre completo	Su nombre y apellidos.
Título	Su cargo.
Nombre de organización	El nombre de su organización.
Correo electrónico	Su dirección de correo electrónico.
ID de usuario	Su ID de usuario para obtener acceso a ThreatGrid.
Contraseña	Su contraseña para obtener acceso a ThreatGrid.
Botón Registrar	Haga clic en el botón **Registrar** para enviar la solicitud.