RSA NETWITNESS® SUITE

Guía de integración de RSA NetWitness Endpoint

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.

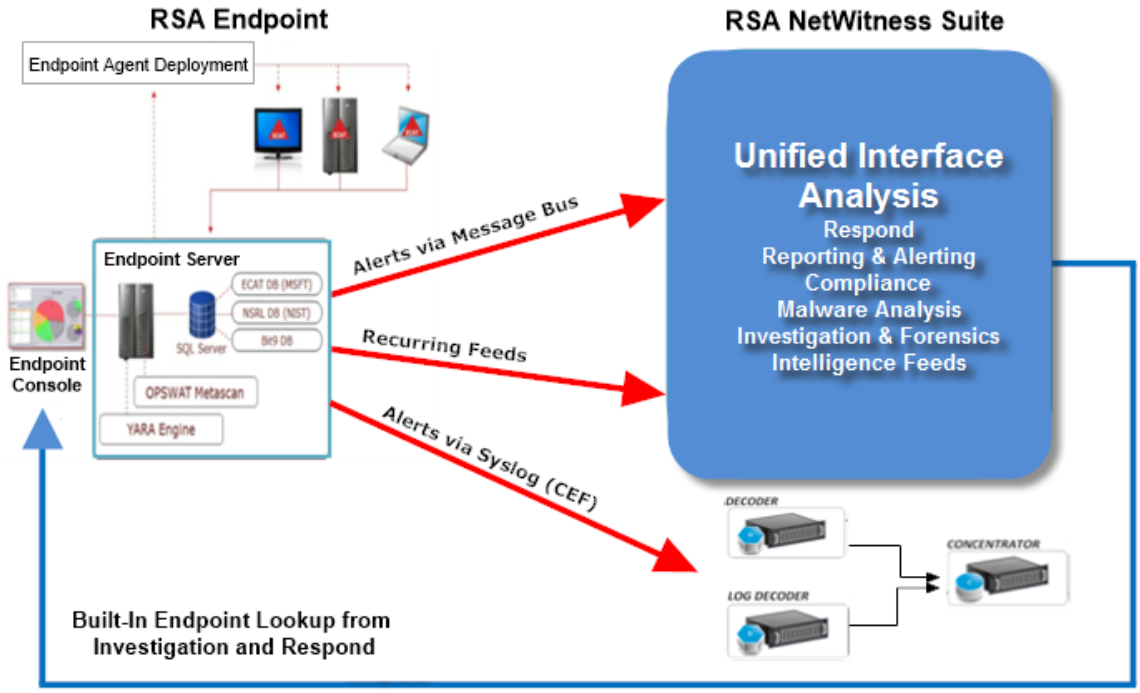
febrero 2018

Contenido

Integración de RSA NetWitness Endpoint

Los clientes de RSA que usan RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5 o 4.4 pueden integrar NetWitness Endpoint y RSA NetWitness Suite de varias formas distintas. Esta guía se aplica a RSA NetWitness Suite versión 11.0.

Opciones de integración



Búsqueda de NetWitness Endpoint incorporada

Con la interfaz del usuario de RSA NetWitness Endpoint instalada en la misma máquina donde el analista usa un navegador para acceder a NetWitness Suite, la búsqueda de NetWitness Endpoint incorporada de NetWitness Suite Investigation y NetWitness Suite Respond proporciona acceso con el botón secundario al servidor de la consola de NetWitness Endpoint para las siguientes claves de metadatos: Dirección IP (ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip), host (alias-host, domain.dst), client y file-hash. Esto se describe en el tema “Iniciar una búsqueda externa de una clave de metadatos” en la *Guía del usuario de Investigation y Malware Analysis* y en el tema “Ver alertas” en la *Guía del usuario de NetWitness Respond.*

No se requiere la configuración de NetWitness Suite para la búsqueda de terminal cuando usa uno de los analizadores incorporados, NetWitness Endpoint o CEF, y no ha personalizado las claves de metadatos predeterminadas que se usan cuando se cargan los metadatos en Investigation. Para obtener más información, consulte el tema “Administrar y aplicar claves de metadatos predeterminadas en una investigación" en la *Guía del usuario de Investigation y Malware Analysis*.

Nota: La excepción se produce si personaliza NetWitness Suite mediante la edición de los ajustes de pantalla para las claves de metadatos predeterminadas en Investigation, agrega claves de metadatos al archivo table-map-custom.xml o personaliza los feeds de NetWitness Endpoint. Se requiere cierta configuración para agregar las claves de metadatos personalizadas al menú contextual Consulta de NetWitness Endpoint en la vista **ADMIN** > **Sistema**, como se describe en el tema “Agregar acciones de menú contextual personalizadas” de la *Guía de configuración del sistema*.

Métodos de integración

Con un servidor de consola RSA NetWitness Endpoint 4.3.0.4, 4.3.0.5 o 4.4 instalado en un host de Windows y la configuración adecuada de NetWitness Endpoint y NetWitness Suite que realiza un administrador, son posibles tres integraciones adicionales de datos de análisis de NetWitness Endpoint.

Los siguientes son los métodos de integración de RSA NetWitness Endpoint:

- Configurar alertas de Endpoint mediante el bus de mensajes
- Configurar datos contextuales desde Endpoint a través de un feed recurrente
- Configurar alertas de Endpoint mediante syslog en un Log Decoder

Alertas de Endpoint mediante el bus de mensajes en NetWitness Respond. Esta integración proporciona la capacidad para el reenvío de alertas de Endpoint a Respond a través del bus de mensajes.

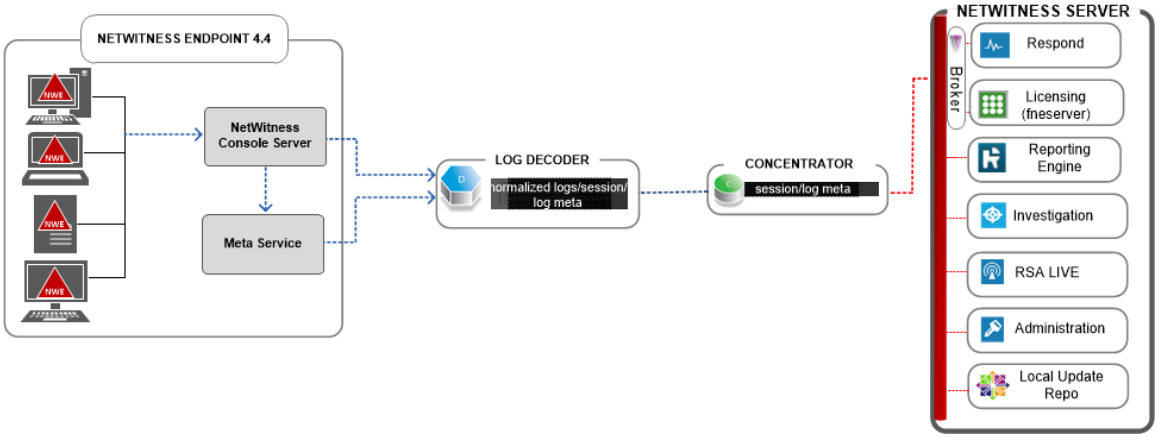
Datos contextuales desde Endpoint a través de un feed recurrente de NetWitness Suite Live. Esta integración puede enriquecer con información contextual la sesión que se muestra en NetWitness Suite Investigation; algunos ejemplos incluyen el sistema operativo del host, la dirección MAC, el puntaje de IIOC y otros datos que tal vez no estén presentes en los datos de registros o de paquetes.

Alertas de NetWitness Endpoint mediante syslog (CEF) en Log Decoders de NetWitness Suite. Esta integración proporciona la capacidad de reenviar eventos de Endpoint a través de Syslog y correlacionar los eventos con otros metadatos de registros o paquetes en el ecosistema de NetWitness Suite.

Integración de metadatos de NetWitness Endpoint

La integración de metadatos de NetWitness Endpoint con RSA NetWitness Suite ofrece a los clientes que tienen ambos productos una manera de aprovechar los productos en una sola interfaz del usuario con mayor facilidad. En el siguiente diagrama se ilustra la forma en que NetWitness Endpoint se integra con NetWitness Suite. Los metadatos de NetWitness Endpoint se recopilan y publican desde todas las máquinas donde se implementan agentes de NetWitness Endpoint y, a continuación, se envían al Log Decoder de NetWitness Suite.

Los metadatos se pueden ver en el NetWitness Suite Concentrator asociado y también en NetWitness Suite Investigate.



Alertas e indicadores de riesgo de NetWitness Endpoint

Un IIOC (Indicador de riesgo instantáneo) de NetWitness Endpoint es una consulta de base de datos que NetWitness Endpoint ejecuta en los datos de escaneo de NetWitness Endpoint recopilados para determinar la presencia de malware potencial en hosts escaneados. RSA NetWitness Endpoint 4.1.2 o superior viene con IOC que el usuario puede habilitar y marcar con la capacidad de generar alertas. RSA NetWitness Endpoint ejecuta consultas de IOC de forma periódica sobre nuevos datos de escaneo, que se recopilan y almacenan en la base de datos. Si se satisface la consulta de IOC, esto indica un posible indicador de riesgo, y el evento se puede informar a un usuario o se puede enviar a un sistema externo como una alerta.

Los posibles tipos de alertas son:

- Alerta de máquina: Esta alerta indica que la máquina en cuestión es sospechosa.
- Alerta de módulo: Esta alerta indica que un módulo, como un archivo, un archivo DLL o un archivo ejecutable, es sospechoso. Contiene detalles sobre el módulo en cuestión.

- Alerta de evento: Esta alerta representa cualquier otra actividad sospechosa que detecta NetWitness Endpoint que no entra en las categorías anteriores.

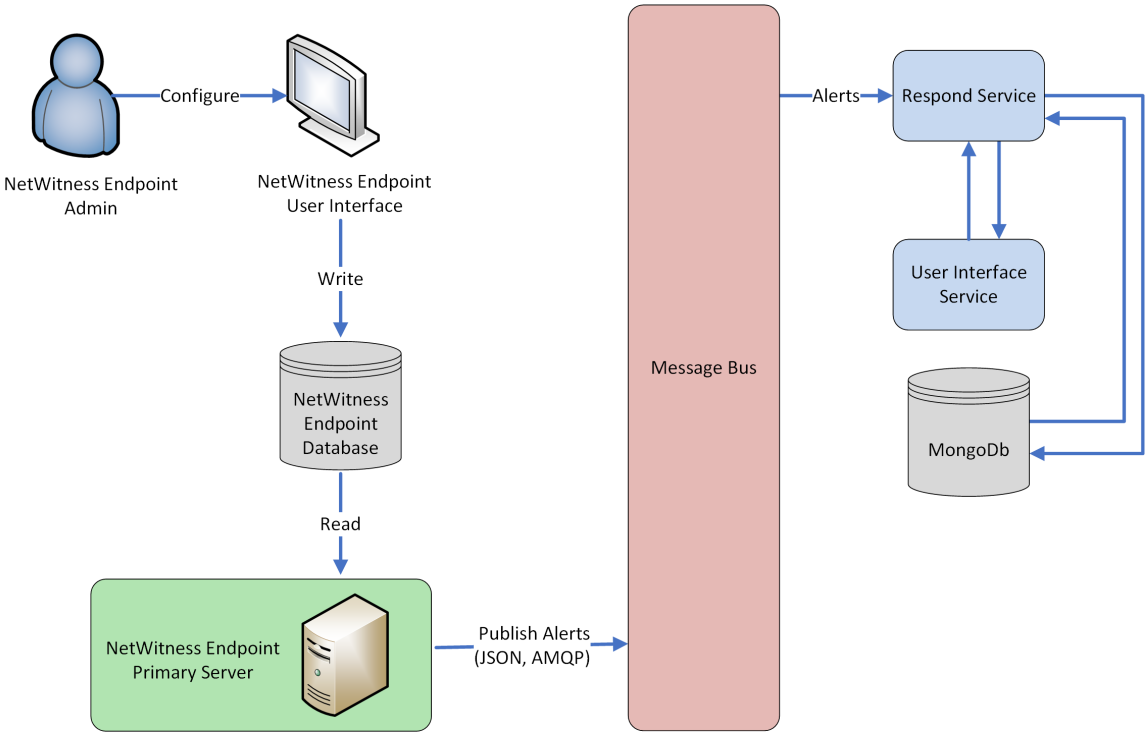
Cada uno de estos tipos de alerta se puede enviar a NetWitness Suite.

Configurar alertas de NetWitness Endpoint mediante el bus de mensajes

Este procedimiento se requiere para integrar NetWitness Endpoint con NetWitness Suite de modo que las alertas de NetWitness Endpoint se recopilen con el componente Respond de NetWitness Suite y se muestren en la vista **RESPOND > Alertas**.

Nota: RSA admite las versiones 4.3.0.4, 4.3.0.5 o 4.4 de NetWitness Endpoint para la integración de NetWitness Respond. Para obtener más información, consulte el tema "Integración de RSA NetWitness Suite" en la *Guía del usuario de NetWitness Endpoint*.

En el siguiente diagrama se representa el flujo de alertas de NetWitness Endpoint en la vista Lista de incidentes de Respond de NetWitness Suite y su visualización en la vista **RESPOND > Alertas**.



Requisitos previos

Asegúrese de disponer de lo siguiente:

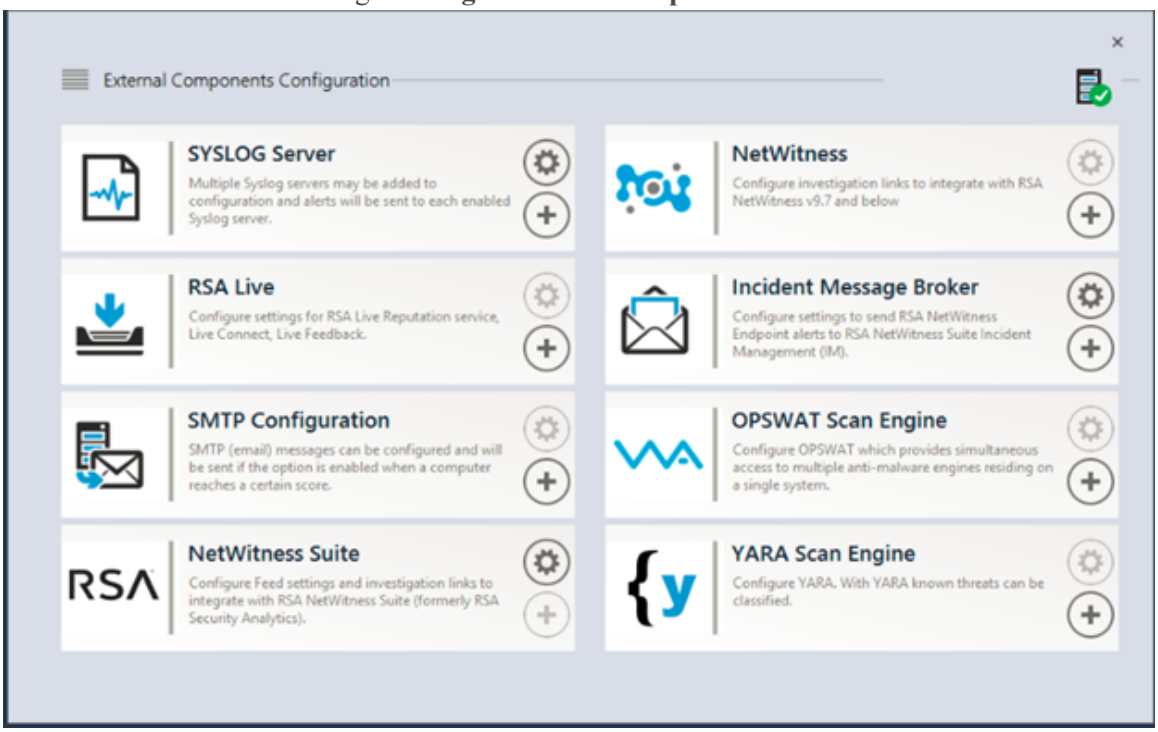
- El servicio Respond está instalado y en ejecución en NetWitness Suite 11.0.
- NetWitness Endpoint 4.3.0.4, 4.3.0.5 o 4.4 está instalado y en ejecución.

Configurar NetWitness Endpoint para reenviar alertas de NetWitness Endpoint

Para configurar NetWitness Endpoint para enviar alertas a través del bus de mensajes a la interfaz del usuario de NetWitness Suite:

1. En la interfaz del usuario de NetWitness Endpoint, haga clic en **Configurar > Monitoreo y componentes externos**.

   Se muestra el cuadro de diálogo **Configuración de componentes externos**.



   a. En los componentes enumerados, seleccione **Intermediador de mensajes de incidentes** y haga clic en + para agregar un nuevo intermediador de IM.

2. Ingrese los siguientes campos:

   a. **Nombre de instancia**: Escriba un nombre único para identificar al intermediador de IM.

   b. **Nombre de host o dirección IP del servidor**: Escriba la dirección IP o el DNS del host del intermediador de IM (Servidor de NetWitness).

   c. **Número de puerto**: El puerto predeterminado es 5671.

3. Haga clic en **Guardar**.

4. Navegue al archivo **ConsoleServer.exe.config** en **C:\Program Files\RSA\ECAT\Server**.

5. Modifique las configuraciones del host virtual en el archivo de la siguiente manera:
   `<add key="IMVirtualHost" value="/rsa/system" />`

   Nota: En NetWitness Suite 11.0, el host virtual es "/rsa/system". En la versión 10.6.x y anteriores, el host virtual es "/rsa/sa".

6. Reinicie el servidor de API y de la consola.

7. Para configurar SSL para las alertas de Respond, realice los siguientes pasos en el servidor de la consola primaria de NetWitness Endpoint con el fin de establecer las comunicaciones de SSL:

   a. Exporte el certificado de CA de NetWitness Endpoint al formato .CER (X.509 con codificación Base 64) desde el almacén de certificados personales de la computadora local (sin seleccionar la clave privada).

   b. Genere un certificado de cliente para NetWitness Endpoint mediante el certificado de CA de NetWitness Endpoint. (DEBE configurar nombre de CN en ecat).

   ```
   makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a
   sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "NweCA" -is MY -ir
   LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -
   cy end -sy 12 client.cer
   ```

   Nota: En el código de ejemplo anterior, si actualizó a Endpoint versión 4.3 desde una versión anterior y no generó nuevos certificados, debe sustituir "EcatCA" por "NweCA".

   c. Tome nota de la huella digital del certificado de cliente que se generó en el paso b. Ingrese el valor de la huella digital del certificado de cliente en la sección IMBrokerClientCertificateThumbprint del archivo ConsoleServer.Exe.Config como se muestra.

   ```
   <add key="IMBrokerClientCertificateThumbprint"
   value="896df0efacf0c976d955d5300ba0073383c83abc"/>
   ```

8. En el Servidor de NetWitness, copie el archivo de certificado de CA de NetWitness Endpoint en formato .CER en la carpeta de importación:
   `/etc/pki/nw/trust/import`

9. Emita el siguiente comando para iniciar la ejecución de Chef necesaria:
   `orchestration-cli-client --update-admin-node`
   Esto agrega todos esos certificados al almacén de confianza.

10. Reinicie el servidor de RabbitMQ:
    `systemctl restart rabbitmq-server`
    La cuenta de NetWitness Endpoint debe estar disponible en RabbitMQ de forma automática.

11. Importe los archivos `/etc/pki/nw/ca/nwca-cert.pem` y `/etc/pki/nw/ca/ssca-cert.pem` desde el Servidor de NetWitness y agréguelos a las áreas de almacenamiento de certificados raíz de confianza en el servidor de Endpoint.

Solución de problemas

En esta sección se sugiere la forma de resolver los problemas que puede encontrar al configurar alertas de NetWitness Endpoint mediante el bus de mensajes.

Problemas conocidos	Soluciones
Se produce un error de coordinación en el nodo de administración.	Debe copiar y pegar el contenido del certificado de EcatCA en `/etc/rabbitmq/ssl/truststore.pem` y reiniciar el servicio Rabbitmq.

Configurar datos contextuales desde NetWitness Endpoint a través de un feed recurrente

Puede configurar datos de RSA NetWitness Endpoint en RSA NetWitness Suite para proporcionar datos contextuales desde NetWitness Endpoint a sesiones de Decoder y Log Decoder. Esta configuración agrega valores de metadatos contextuales además de alertas de IOC instantáneos que se pueden usar para crear correlaciones con otros metadatos en el ecosistema de NetWitness Suite.

Los administradores pueden configurar NetWitness Suite para consumir datos contextuales de escaneos del sistema desde NetWitness Endpoint a través de un feed recurrente de NetWitness Suite Live. Esta integración puede enriquecer la sesión desde Decoder o Log Decoder con información contextual que se muestra en NetWitness Suite Investigation; algunos ejemplos incluyen el sistema operativo del host, la dirección MAC, el puntaje de IIOC y otros datos que tal vez no estén presentes en los datos de registros o de paquetes de sesiones que provienen de un Decoder o un Log Decoder.

Nota: Aunque esta función está destinada a clientes con un Packet Decoder, también es posible implementar un feed recurrente en Log Decoders.

Precaución: En ambientes con muchos hosts de NetWitness Endpoint, el uso de este feed recurrente puede dar lugar a un menor rendimiento en los dispositivos de recopilación de NetWitness Suite (Decoder y Log Decoder).

Requisitos previos

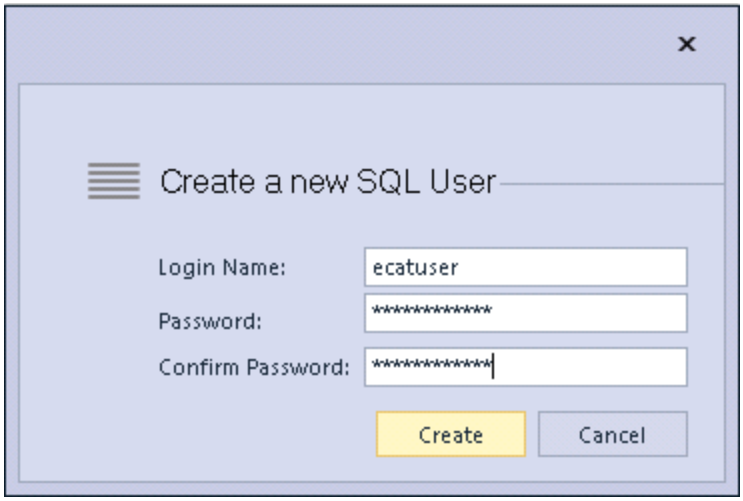
- Servidor de NetWitness Endpoint Console versión 4.3.0.4, 4.3.0.5 o 4.4 y Servidor de NetWitness versión 10.4 y superior instalados.
- RSA Decoder y Concentrator versión 11.0 conectados al Servidor de NetWitness en la red.

Para configurar datos contextuales desde NetWitness Endpoint a través de un feed recurrente, realice lo siguiente:

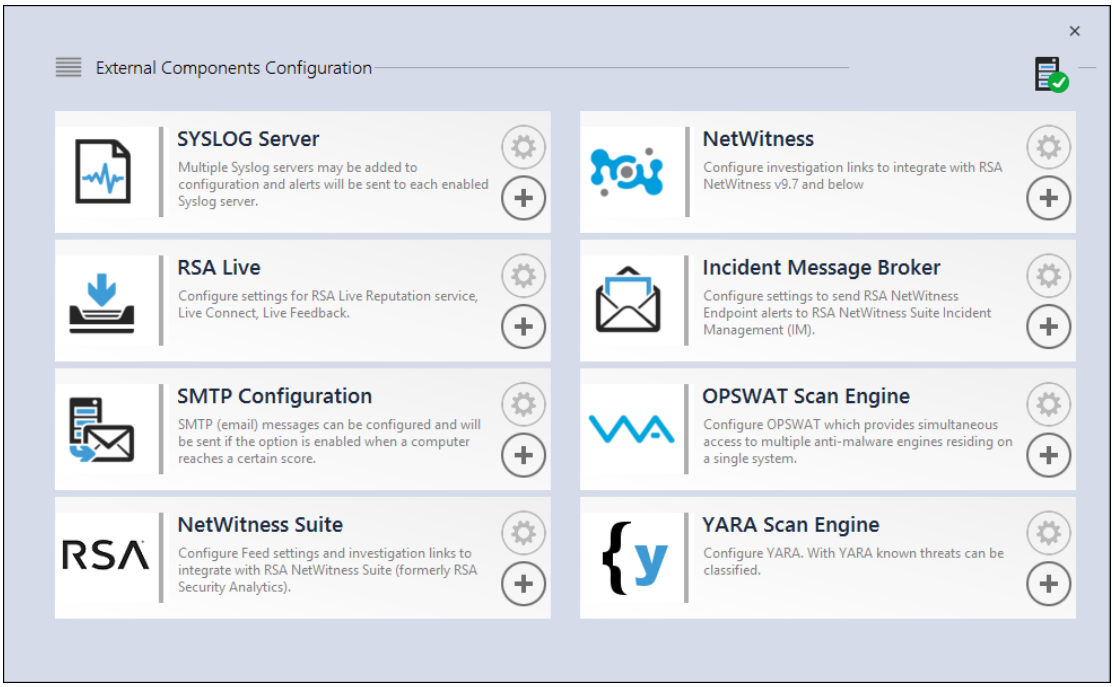
1. Habilite el feed de NetWitness Endpoint para NetWitness Suite en la interfaz del usuario de NetWitness Endpoint.
2. Exporte el certificado de CA de NetWitness Endpoint desde el servidor de NetWitness Endpoint Console e impórtelo en el almacén de confianza de NetWitness Suite.
3. Configure el servicio NetWitness Suite Concentrator para definir las claves de metadatos que se indexan.
4. Cree un feed recurrente en NetWitness Suite Live.

Habilitar el feed de NetWitness Endpoint para NetWitness Suite

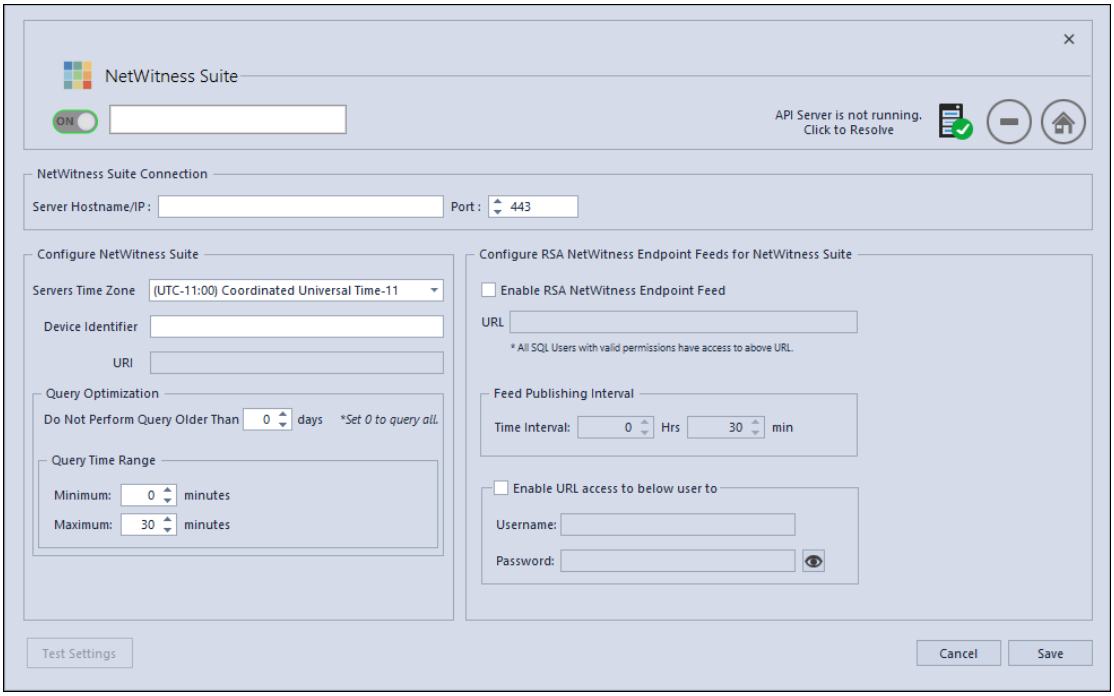
1. En la interfaz del usuario de NetWitness Endpoint, cree el usuario SQL en NetWitness Endpoint:
   a. Abra la interfaz del usuario de NetWitness Endpoint e inicie sesión con las credenciales apropiadas.
   b. En la barra de menú, seleccione **Configurar > Administrar usuarios y funciones**, haga clic con el botón secundario en el panel y seleccione **crear usuario de sql**.
   Se muestra el cuadro de diálogo Crear un nuevo usuario de SQL.



   c. Ingrese el **Nombre de inicio de sesión** y la **Contraseña**, y haga clic en **Crear**.
2. En la barra de menú, seleccione **Configurar > Monitoreo de componentes externos**.
   Aparece el cuadro de diálogo Configuración de componentes externos.



3. En NetWitness Suite, haga clic en +.
   Se muestra el cuadro de diálogo NetWitness Suite.



4. En el panel **NetWitness Suite**, en **Activado**, ingrese el nombre para identificar el componente NetWitness Suite.

5. En el panel **Conexión de NetWitness Suite**, realice lo siguiente.
   a. En el campo **Nombre de host/IP de servidor**, ingrese la dirección IP o el nombre de host del Servidor de NetWitness.
   b. Ingrese el número de puerto en el campo **Puerto**. El número de puerto predeterminado es 443.
6. En el panel **Configurar NetWitness Suite**, realice lo siguiente:
   a. En el campo **Zona horaria de los servidores**, seleccione la zona horaria para el componente en la lista desplegable.
   b. En el campo **Identificador del dispositivo**, ingrese el ID del dispositivo de NetWitness Suite Concentrator.

   Nota: Puede encontrar el identificador del dispositivo en NetWitness Suite cuando busca un Concentrator o un Broker en **Investigation > Navegar >***<Nombre de Broker o Concentrator>*. El identificador del dispositivo es el número en la URL después de "investigation". Por ejemplo, en la URL `https://<IP address>investigation/319/navigate/values`, el identificador del dispositivo es **319**.

   El campo **URI** se completa cuando hace clic en **Guardar**.
7. En el panel **Optimización de consulta**, en el campo **No realizar una consulta anterior a**, ingrese la cantidad de días para limitar el período de consulta. Ingrese **0** si desea descartar esta función.
8. En el panel **Rango de tiempo de consulta**, realice lo siguiente:
   a. En el campo **Mínimo**, ingrese la cantidad de minutos para el rango de tiempo de consulta mínimo. Este valor se usa para aumentar automáticamente el rango de tiempo que se envía a NetWitness Suite. Esto garantiza que una consulta devuelva una respuesta positiva si el tiempo informado del agente de NetWitness Endpoint es levemente diferente al tiempo de NetWitness Endpoint.
   b. En el campo **Máximo**, ingrese la cantidad de minutos para limitar el rango de tiempo. Este valor se usa para limitar automáticamente el rango de tiempo enviado a NetWitness Suite, de modo que una consulta no sobrecargue el Servidor de NetWitness.
9. En el panel **Configurar feeds de RSA NetWitness Endpoint para NetWitness Suite**, realice lo siguiente:

a. Seleccione **Habilitar feed de RSA NetWitness Endpoint**.

b. En el campo **URL**, ingrese el **Nombre de usuario** y la **Contraseña** de SQL (configurados en el paso 1) para acceder a la ubicación del feed.
El campo **URL** se completa cuando hace clic en **Guardar**.

c. Ingrese el intervalo de tiempo para la frecuencia con la que se publican los feeds.

10. En el panel **Intervalo de publicación de feed**, en el campo **Intervalo de tiempo**, seleccione el intervalo de tiempo en **horas** y **minutos** para la frecuencia en que se publican los feeds.
11. En el panel **Permitir el acceso a URL al usuario siguiente**, ingrese el **Nombre de usuario** y la **Contraseña** del usuario de NetWitness Endpoint.
12. Haga clic en **Guardar**.
Se crea un feed.

Exportar el certificado SSL de NetWitness Endpoint

Nota: Este procedimiento funciona solo con NetWitness Suite 10.5 y superior debido a que se agregó compatibilidad con Java 8 para 10.5. Si está usando una versión anterior de NetWitness Suite, consulte la versión correspondiente de esta guía.

Para exportar el certificado de CA de NetWitness Endpoint desde el servidor de NetWitness Endpoint Console y copiarlo al host de NetWitness Suite:

1. Inicie sesión en NetWitness Endpoint Console.
2. Abra **MMC**.
3. Agregue un snap-in de certificado para la **cuenta Computer**.
4. Exporte el certificado con el nombre **`EcatCA`**.
   a. Expórtelo sin una clave privada.
   b. Expórtelo en formato de codificación DER binario X.509 (`.CER`).
   c. Asígnele el nombre **`EcatCA.cer`**.
5. Copie el certificado de CA de NetWitness Endpoint al host de NetWitness Suite:
   - Para una instalación nueva de NetWitness Endpoint 4.3.0.4, 4.3.0.5 o 4.4:
     `scp NweCA.cer root@<sa-machine>:.`
   - Para NetWitness Endpoint actualizado de una versión anterior a 4.3.0.4 o 4.3.0.5:
     `scp EcatCA.cer root@<sa-machine>:.`

6. Para importar el certificado de CA de NetWitness Endpoint al almacén de confianza de NetWitness Suite, realice lo siguiente:

   a. Compruebe la versión de Java instalada en NetWitness Suite mediante el siguiente comando:
   `java -version`
   Se muestra la versión openjdk. Por ejemplo, la versión openjdk "`1.8.0_71`"

   b. Para configurar el parámetro JDK, navegue al directorio de Java. Ingrese los siguientes comandos:

   - `JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.141-1.b16.el7_3.x86_64/jre/`
   - Para una instalación nueva de NetWitness Endpoint:

     ```
     $JDK/bin/keytool -import -v -trustcacerts -alias nweca -file ~/NweCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
     ```

   - Para NetWitness Endpoint actualizado de una versión anterior:

     ```
     $JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
     ```

   Cuando se le solicite confirmar la actualización del certificado, ingrese **Sí**.

7. En el host de NetWitness Suite, realice una de las siguientes acciones:

   - Para una instalación nueva de NetWitness Endpoint 4.3.0.4, 4.3.0.5 o 4.4, edite **`/etc/hosts`** para mapear la dirección IP del servidor de NetWitness Endpoint Console al nombre **NweServerCertificate** mediante la adición de la siguiente línea al archivo:

     ```
     <ip-address-ecat-cs> NweServerCertificate
     ```

   - Para NetWitness Endpoint actualizado de una versión anterior a 4.3.0.4 o 4.3.0.5, edite **`/etc/hosts`** para mapear la dirección IP del servidor de NetWitness Endpoint Console actualizado al nombre **`ecatserverexported`** mediante la adición de la siguiente línea al archivo:

     ```
     <ip-address-ecat-cs> ecatserverexported
     ```

8. Para reiniciar NetWitness Suite, ingrese el siguiente comando:

   ```
   service jetty restart
   ```

Configurar el servicio NetWitness Suite Concentrator

1. Inicie sesión en NetWitness Suite y vaya a **ADMIN > Servicios**.
2. Seleccione un Concentrator en la lista y, a continuación, elija **Ver > Configuración.**

3. Seleccione la pestaña **Archivos** y, en el menú desplegable **Archivos para editar**, seleccione **index-concentrator-custom.xml**.
4. Agregue las siguientes claves de metadatos de NetWitness Endpoint al archivo y haga clic en **Aplicar**. Asegúrese de que este archivo incluya las secciones XML; si las líneas no se incluyen, agréguelas. Las siguientes líneas son ejemplos; asegúrese de que los valores coincidan con su configuración y con los nombres de columna que incluyó en la definición del feed, donde:
   description es el nombre de la clave de metadatos que desea mostrar en NetWitness Suite Investigation.
   level es “IndexValues”
   name coincide con el nombre de columna del archivo CSV que NetWitness Suite usa durante la definición del feed recurrente (consulte la tabla en *Configurar la tarea del feed personalizado recurrente en NetWitness Suite*, a continuación).

   ```
   <key description="Gateway" format="Text" level="IndexValues"
   name="gateway" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Risk Number" format="Float64" level="IndexValues"
   name="risk.num" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Strans Addr" format="Text" level="IndexValues"
   name="stransaddr" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="Domain" format="Text" level="IndexValues"
   name="domain" valueMax="250000" defaultAction="Open"/>
   ```

   ```
   <key description="User Account" format="Text" level="IndexValues"
   name="username" valueMax="250000" defaultAction="Open"/>
   ```

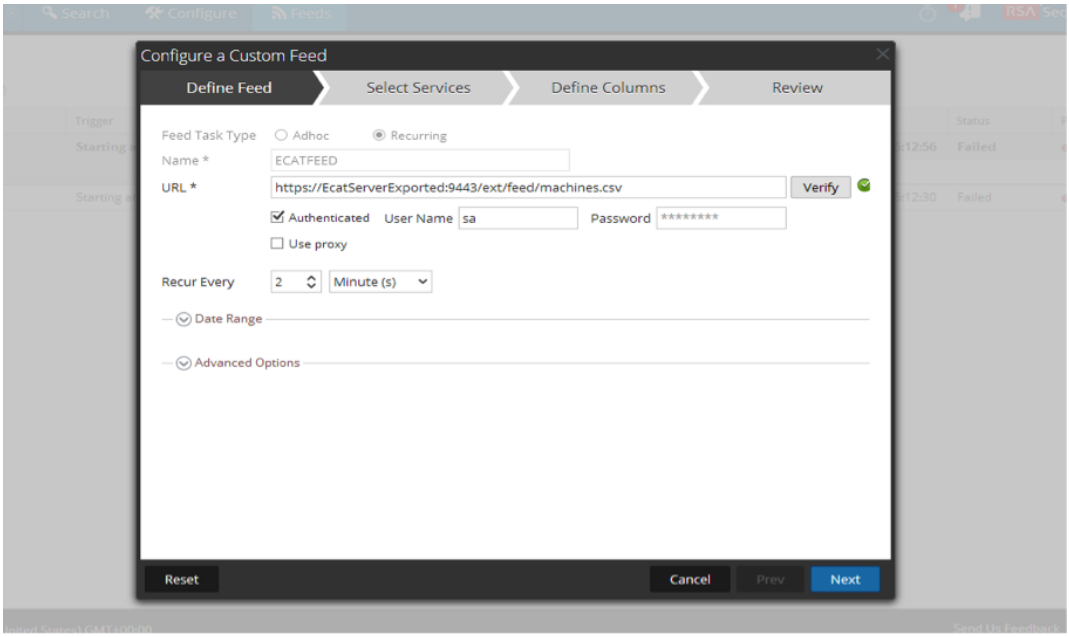
   ```
   <key description="Ecat Connectiontime" format="Text"
   level="IndexValues" name="ecat.ctime" valueMax="250000"
   defaultAction="Open"/>
   ```

   ```
   <key description="Ecat Scantime" format="Text" level="IndexValues"
   name="ecat.stime" valueMax="250000" defaultAction="Open"/>
   ```
5. Reinicie el Concentrator para activar las actualizaciones de claves personalizadas.

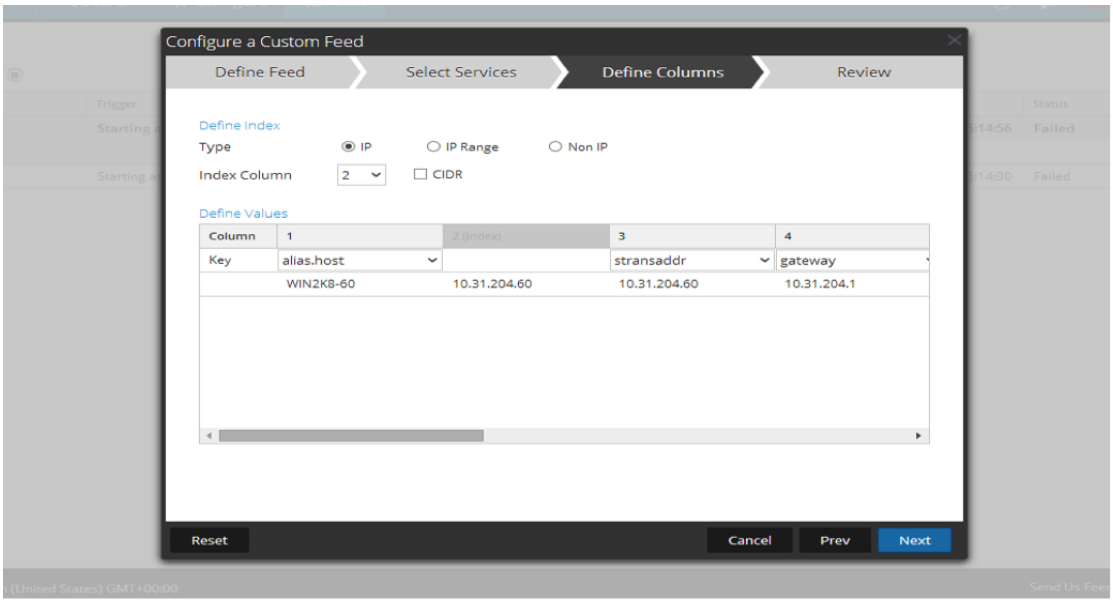
Configurar la tarea del feed personalizado recurrente en NetWitness Suite

1. Inicie sesión en NetWitness Suite y vaya a **CONFIGURAR > Feeds personalizados**.
   Se muestra la vista Feeds.
2. En la barra de herramientas, haga clic en  .
   Se muestra el cuadro de diálogo Configurar feed.
3. En el cuadro de diálogo Configurar feed, seleccione **Feed personalizado** y haga clic en **Siguiente**.
   El asistente Configurar un feed personalizado se muestra con el formulario Definir feed abierto.
4. En el campo **Definir feed**, realice lo siguiente:
   a. Seleccione **Recurrente** en el campo **Tipo de tarea de feed**.
   b. En el campo **Nombre**, ingrese el nombre del feed. Por ejemplo, EndpointFeed.
   c. En el campo **URL**, ingrese la dirección URL con el nombre de host del servidor de Windows donde está instalado NetWitness Endpoint:
      - Para una instalación nueva de NetWitness Endpoint 4.3.0.4, 4.3.0.5 o 4.4, use la dirección URL
        `https://NweServerCertificate:9443/api/v2/feed/machines.csv.`
      - Para NetWitness Endpoint actualizado de una versión anterior a 4.3.0.4 o 4.3.0.5, use la dirección URL
        `https://ecatserverexported:9443/api/v2/feed/machines.csv.`
   d. Active la casilla de verificación **Autenticado** e ingrese el nombre de usuario y la contraseña que anotó anteriormente en *Activar el feed de ECAT*.
   e. Haga clic en **Verificar** para comprobar que NetWitness Suite pueda acceder al recurso web.

f. Defina el programa y haga clic en **Siguiente**.



5. En la pestaña **Seleccionar servicios**, seleccione el Decoder o grupos para consumir el feed. Haga clic en **Siguiente**.
6. En la pestaña **Definir columnas**, ingrese los nombres de columna como aparecen en la tabla siguiente y guarde el feed.

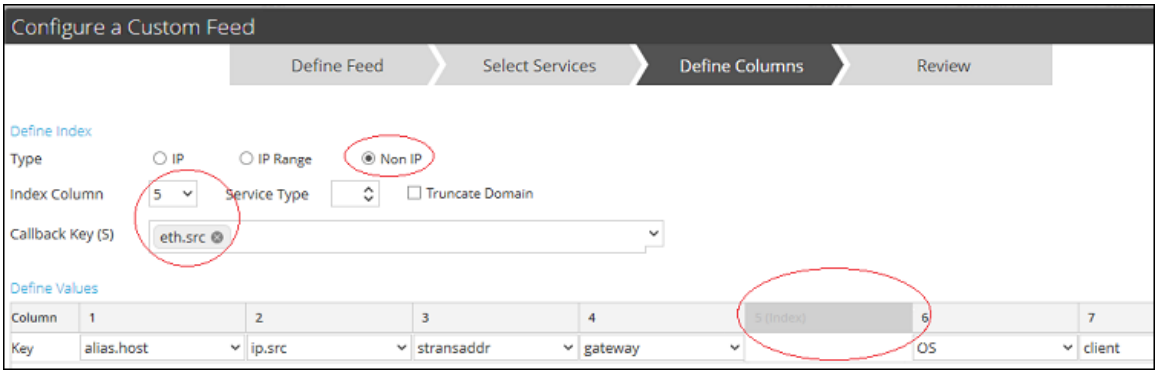


En la siguiente tabla se muestran las columnas del archivo CSV para el feed de NetWitness Endpoint.

Columna	Nombre	Descripción	Nombre de la columna en NetWitness Suite (nombre de clave de metadatos)
1	MachineName	Nombre de host del agente de Windows	alias.host
2	LocalIp	Dirección IPv4	Tipo de IP (columna indexada)
3	RemoteIp	Dirección IP del extremo lejano como la ve el enrutador	stransaddr
4	GatewayIp	Dirección IP del gateway	gateway
5	MacAddress	Dirección MAC	eth.src
6	OperatingSystem	Sistema operativo que usa el agente de Windows	SO
7	AgentID	ID del agente del host (ID único asignado al agente)	cliente
8	ConnectionUTCTime	Última vez que el agente se conectó al servidor de NetWitness Endpoint	ecat.ctime
9	Source Domain	Dominio	domain.src
10	ScanUTC time	Última vez que se escaneó el agente	ecat.stime

Columna	Nombre	Descripción	Nombre de la columna en NetWitness Suite (nombre de clave de metadatos)
11	Nombre de usuario	Nombre de usuario de la máquina cliente	username
12	Puntaje de la máquina	Puntaje del agente que indica el nivel sospechoso	risk.num

Nota: En la tabla, la configuración recomendada del índice es LocalIp. Sin embargo, si un servidor DHCP asigna el LocalIp para la computadora de agente de NetWitness Endpoint y el arrendamiento de DHCP venció, y si la dirección IP se reasigna a otra computadora, los metadatos que creó el feed estarán incorrectos. Para evitar este riesgo, use el nombre de la máquina o la dirección Mac en lugar de la dirección localIP como índice del feed. Por ejemplo, para usar una dirección Mac, podría ingresar los valores que se muestran en la siguiente figura.



Resultado

Cuando se ven los datos del feed en NetWitness Suite y tras una coincidencia del valor indexado (ip.src), se completan los metadatos en las interfaces de Investigation, Reporting y Alerting.

Configurar alertas de Endpoint mediante syslog en un Log Decoder

Puede configurar el uso de datos de RSA NetWitness Endpoint en RSA NetWitness Suite para proporcionar alertas de NetWitness Endpoint mediante Syslog a las sesiones de Log Decoder. Esto genera metadatos que se usan en NetWitness Suite Investigation, Alerts y Reporting Engine.

En el caso de las redes de NetWitness Suite que consumen registros, esta integración de NetWitness Endpoint con NetWitness Suite migra eventos de NetWitness Endpoint al Log Decoder a través de mensajes de syslog en formato de evento común (CEF) y genera metadatos que se usan en NetWitness Suite Investigation, Alerts y Reporting Engine. El caso de uso para esta integración es la integración de SIEM con el fin de permitir la administración centralizada de eventos, la correlación de eventos de NetWitness Endpoint con otros datos del Log Decoder, los informes de NetWitness Suite sobre eventos de NetWitness Endpoint y las alertas de NetWitness Suite relacionadas con eventos de NetWitness Endpoint.

Requisitos previos

Para esta integración se requiere lo siguiente:

- Versión 4.3.0.4, 4.3.0.5 o 4.4 de la interfaz del usuario de NetWitness Endpoint.
- Instalación de Servidor de NetWitness versión 11.0.
- Versión 10.4 o superior de RSA Log Decoder y Concentrator conectados al Servidor de NetWitness en la red.
- Puerto 514 UDP o 1514 TCP abiertos desde el servidor de NetWitness Endpoint al Log Decoder en el firewall.

Procedimiento

1. Implemente el analizador requerido (CEF o rsaecat) en el Log Decoder, como se describe en el tema “Administrar recursos de Live” en *Administración de servicios de Live*. Después de implementar el analizador, asegúrese de que esté habilitado. Para obtener más información, consulteVista Configuración de servicios: Pestaña General.

Nota: Use solo uno de estos analizadores. Cuando se implementa el analizador de CEF, este reemplaza al analizador de NetWitness Endpoint y todos los mensajes de CEF a NetWitness Suite los procesa el analizador de CEF. La activación de ambos analizadores es una carga innecesaria para el rendimiento.

2. Configure NetWitness Endpoint para que envíe la salida de syslog a NetWitness Suite y genere alertas de NetWitness Endpoint para el Log Decoder.
3. (Opcional) Edite el mapeo de tablas en `table-map-custom.xml` y en `index-concentrator-custom.xml` para agregar campos de acuerdo con las preferencias del usuario para los metadatos que se mapearán a NetWitness Suite.

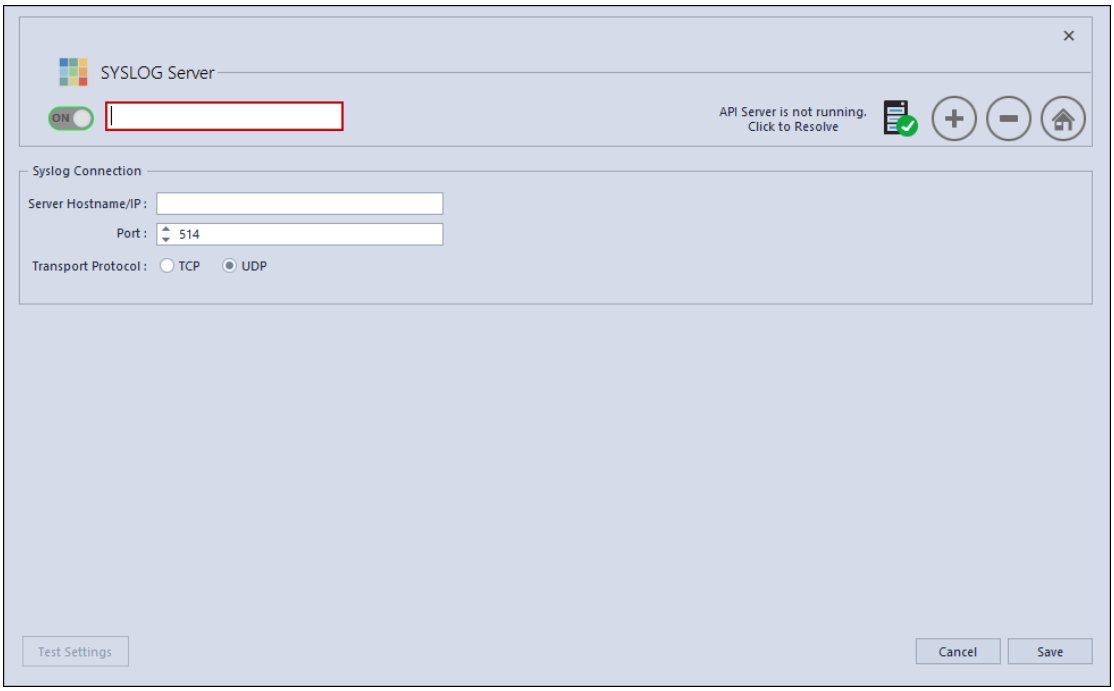
Configurar NetWitness Endpoint para enviar la salida de syslog a NetWitness Suite

Para agregar el Log Decoder como un componente externo de syslog y generar alertas de NetWitness Endpoint para Log Decoder:

1. Abra la interfaz del usuario de NetWitness Endpoint e inicie sesión con las credenciales apropiadas.
2. En la barra de menú, seleccione **Configurar > Monitoreo y componentes externos**.

   Aparece el cuadro de diálogo Configuración de componentes externos.
3. En **Servidor de SYSLOG**, haga clic en  .

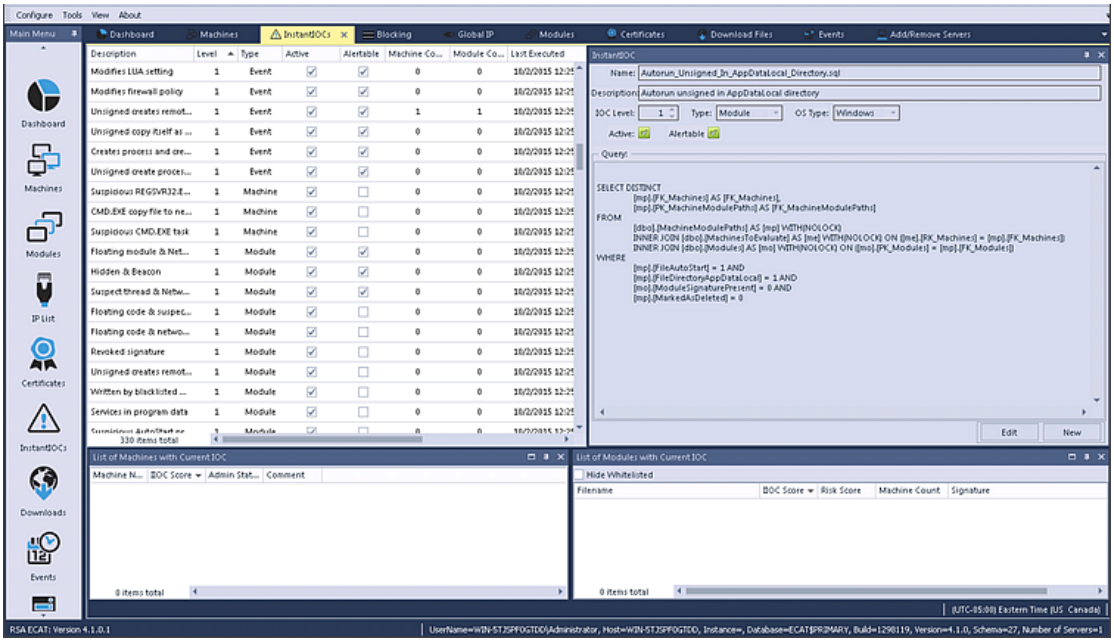
   Se muestra el cuadro de diálogo Servidor de SYSLOG.



4. En el panel **NetWitness Suite**, en **Activado**, escriba el nombre descriptivo del Log Decoder.
5. En el panel **Conexión de syslog**, realice lo siguiente para habilitar la mensajería de syslog:

   Nombre de host/IP de servidor = La dirección IP o el DNS del nombre de host del RSA Log Decoder
   Puerto = 514
   Protocolo de transporte = Seleccione **UDP** o **TCP** según corresponda para su servidor de syslog para el protocolo de transporte.

6. Haga clic en **Guardar**.
7. Abra la ventana **InstantIOCs** en la interfaz del usuario de NetWitness Endpoint y, en la columna **Generar alerta**, haga clic para habilitar cada IIOC para el cual desea que se envíen alertas al Log Decoder.



Cuando se activan los IOC instantáneos, se envían alertas de syslog del servidor de NetWitness Endpoint al Log Decoder. A continuación, las alertas de Log Decoder se agregan en Concentrator. Estos eventos se inyectarán en el Concentrator como metadatos.

Editar el mapeo de tablas en table-map-custom.xml

En table-map.xml de RSA predeterminado que proporciona RSA, las claves de metadatos del archivo `table-map.xml` están configuradas en `Transient`. Para ver las claves de metadatos en Investigation, estas se deben configurar en `None`. Para realizar cambios en el mapeo, debe agregar las entradas al `table-map-custom.xml` en el Log Decoder.

Esta es la lista de claves de metadatos en `table-map.xml`.

Campos de NetWitness Endpoint	Mapeo de NetWitness Suite	Transitorio en NetWitness Suite
agentid	cliente	No
CEF Header Hostname Field	alias.host	No
CEF Header Product Version	version	Sí
CEF Header Product Name	Producto	Sí
CEF Header Severity	severity	Sí
CEF Header Signature ID	event.type	No
CEF Header Signature Name	event.desc	No
destinationDnsDomain	ddomain	Sí
deviceDnsDomain	dominio	Sí
dhost	host.dst	No
dst	ip.dst	No
fin	endtime	Sí
fileHash	checksum	Sí
fname	filename	No
fsize	filename.size	Sí
gatewayip	gateway	Sí
instantIOCLevel	threat.desc	No
instantIOCName	threat.category	No
machineOU	dn	Sí
machineScore	risk.num	No

Campos de NetWitness Endpoint	Mapeo de NetWitness Suite	Transitorio en NetWitness Suite
md5sum	checksum	Sí
os	SO	Sí
puerto	ip.dstport	No
protocol	protocol	Sí
Raw Message	msg	Sí
remoteip	stransaddr	Sí
rt	alias.host	No
sha256sum	checksum	Sí
shost	host.src	No
smac	eth.src	Sí
src	ip.src	No
start	starttime	Sí
suser	-user|-u	No
timezone	timezone	Sí
totalreceived	rbytes	Sí
totalsent	bytes.src	No
useragent	user.agent	No
userOU	org	Sí

Las siete claves siguientes no están en `table-map.xml`; para usarlas en NetWitness Suite, debe agregarlas a `table-map-custom.xml` y configurar las marcas en `None`.

Campos de NetWitness Endpoint	Mapeo de NetWitness Suite	Transitorio en NetWitness Suite
moduleScore	cs.modulescore	Sí
moduleSignature	cs.modulesign	Sí
Target module	cs.targetmodule	Sí
YARA result	cs.yararesult	Sí
Source module	cs.sourcemodule	Sí
OPSWATResult	cs.opswatresult	Sí
ReputationResult	cs.represult	Sí

Las siguientes son las entradas que se deben agregar a `table-map-custom.xml` si es necesario.

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
 <mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
 <mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
 <mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
 <mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
 <mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
 <mapping envisionName="cs_yararesult" nwName="cs.yararesult" flags="None"
envisionDisplayName="YaraResult"/>
```

Nota: Reinicie Log Decoder o vuelva a cargar los analizadores de registros para que se apliquen los cambios.

Configurar el servicio NetWitness Suite Concentrator

1. Inicie sesión en NetWitness Suite y vaya a **ADMIN** > **Servicios**.
    1. Seleccione un Concentrator en la lista y, a continuación, elija **Ver > Configuración.**
2. Seleccione la pestaña **Archivos** y, en la lista desplegable **Archivos para editar**, seleccione **index-concentrator-custom.xml**.

3. Agregue las claves de metadatos de NetWitness Endpoint al archivo y haga clic en **Aplicar**. Asegúrese de que este archivo incluya las secciones XML; si las líneas no se incluyen, agréguelas.
4. Reinicie el Concentrator.
5. Para agregar el Concentrator como un origen de datos en Reporting Engine, en la vista **ADMIN** > **Servicios**, seleccione el Reporting Engine y elija **Ver> Configuración > Orígenes.**
   Los metadatos de NetWitness Endpoint se completan en Reporting Engine y puede ejecutar informes mediante la selección de las claves de metadatos correspondientes.

Ejemplo

Nota: Las siguientes líneas son ejemplos; asegúrese de que los valores coincidan con su configuración y con los nombres de columna que incluyó en la definición del feed, donde:
description es el nombre de la clave de metadatos que desea mostrar en NetWitness Suite Investigation.
level es "IndexValues"
name es el nombre de la clave de metadatos de NetWitness Endpoint de la tabla siguiente

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
 <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
 <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
 <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
 <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
 <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
 <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
 <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
 <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
 <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
 <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
 <key description="Module Sign" format="Text" level="IndexValues"
```

```
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
 <key description="opswat result" format="Text" level="IndexValues"
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
 <key description="source module" format="Text" level="IndexValues"
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
 <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
 <key description="yara result" format="Text" level="IndexValues"
name="cs.yararesult" valueMax="250000" defaultAction="Open"/>
 <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
 <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
 <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
 <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
 <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
 <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
 <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
 <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
 <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
 </language>
```

Resultado

Los analistas pueden:

- Crear alertas de NetWitness Suite basadas en eventos de NetWitness Endpoint mediante la configuración de eventos de NetWitness Endpoint como un origen de enriquecimiento.
- Crear reglas de ESA mediante el uso de metadatos de NetWitness Endpoint, como se describe en el tema “Agregar reglas a la biblioteca de reglas” en la *Guía de Alertas mediante ESA*.
- Informar sobre eventos de NetWitness Endpoint que usan metadatos de NetWitness Endpoint, como se describe en el tema "Configurar una regla” en la *Guía de Reporting*.
- Ver alertas de NetWitness Endpoint en NetWitness Respond, como se describe en el tema “Ver alertas” en la *Guía del usuario de NetWitness Respond*.
- Ver claves de metadatos de NetWitness Endpoint en Investigation, junto con claves de metadatos de NetWitness Suite Core estándar, como se describe en el tema “Realizar una investigación” en la *Guía del usuario de Investigation and Malware Analysis*.