RSA NETWITNESS® PLATFORM

Decoder y Log Decoder Guía de configuración

para la versión 11.2

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por Dell.

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

febrero 2019

Contenido

Configuración rápida de Decoder y Log Decoder

Una red básica de RSA NetWitness® Platform incluye como mínimo Brokers, Concentrators y Decoders. Los Brokers agregan datos de los Concentrators y los Concentrators consumen datos de al menos un Network Decoder o un Log Decoder. La red básica puede incluir ambos tipos de Decoders. Por lo general, los Network Decoders se conocen como Decoders y capturan datos de red en forma de paquetes. Los Log Decoders capturan datos del registro como eventos.

La adición de un Decoder lo hace visible y lo pone a disposición para su uso con NetWitness Platform Administration, Live Services y Investigate. Para agregar un servicio en NetWitness Platform, seleccione el tipo de servicio, proporcione información de conexión de servicio y valide que se pueda acceder al servicio. La *Guía de introducción de hosts y servicios* proporciona la información que necesita para comprender e instalar todos los servicios de NetWitness Platform.

Después de agregar los servicios, debe configurar cada uno de ellos. Este es el orden recomendado para configurar su sistema:

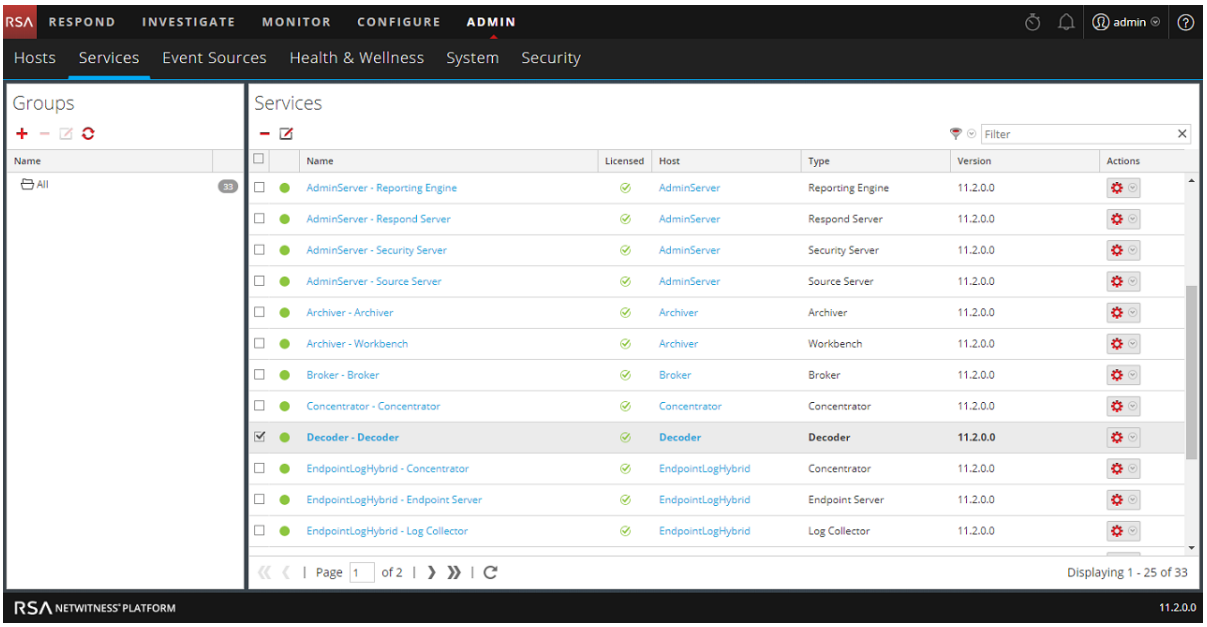
1. Decoders
2. Log Decoders
3. Concentrators (consulte la *Guía de configuración de Broker y Concentrator*)
4. Brokers (consulte la *Guía de configuración de Broker y Concentrator*)

Nota: Un Log Decoder es un tipo especial de Decoder y se configura y administra de manera similar a un Decoder. La mayor parte de la información en esta guía se refiere a ambos tipos de Decoders. “Decoder” se refiere a ambos tipos de Decoders. Se identifica claramente la información que se aplica de manera exclusiva a Network Decoders o Log Decoders.

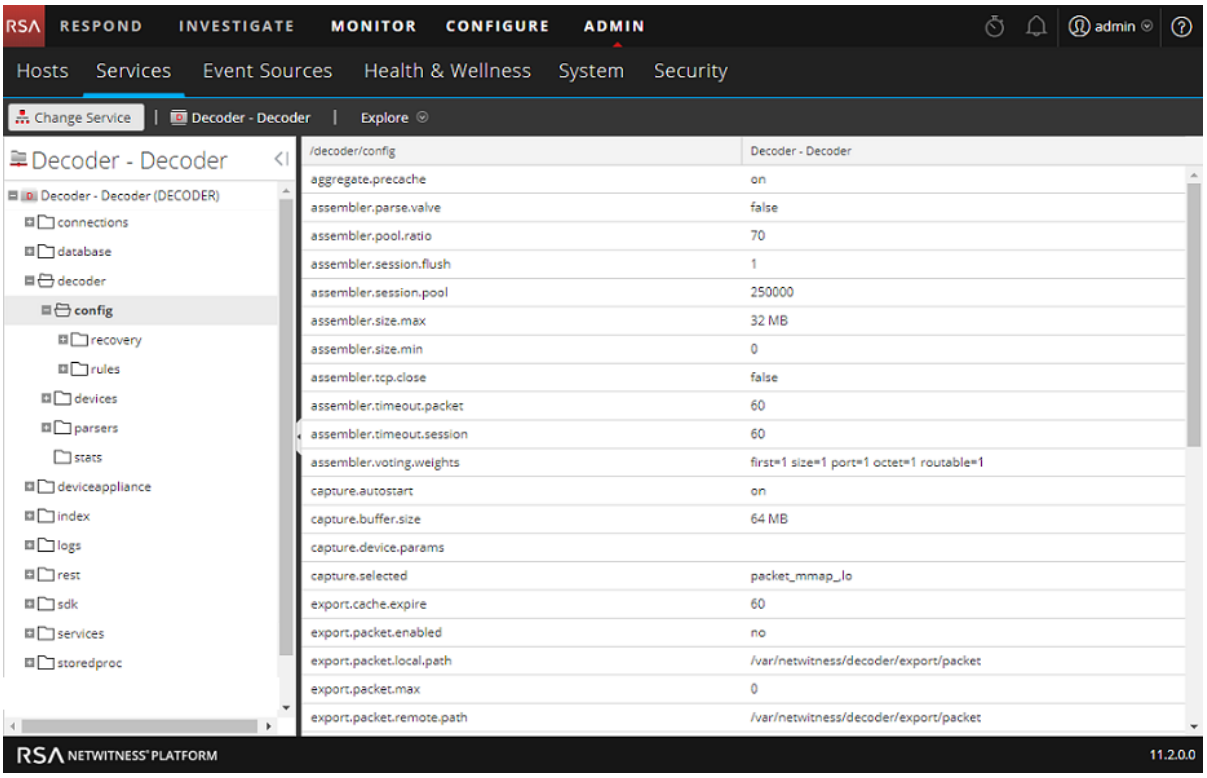
La configuración básica del Decoder implica seleccionar una interfaz del adaptador de red y comenzar la captura de datos.

Además, puede configurar cada Decoder para controlar el tipo de tráfico capturado mediante el uso de reglas, feeds y analizadores. Las tareas de configuración avanzada habilitan funciones adicionales que son pertinentes a aplicaciones específicas. Por ejemplo, configurar un Decoder 10 G, crear claves de metadatos personalizados o descifrar los paquetes entrantes.

La manera más fácil de configurar todos los ajustes de Decoder y Log Decoder es usar las opciones en la interfaz del usuario de NetWitness Platform. En general, la configuración se realiza en la Vista Servicios de Administration (ADMINISTRAR > Servicios).



Los administradores que se sienten cómodos trabajando fuera de la interfaz del usuario pueden configurar los parámetros básicos y los ajustes avanzados mediante la edición de nodos de la base de datos en el árbol de nodos del Decoder en la Vista Explorar de servicios.

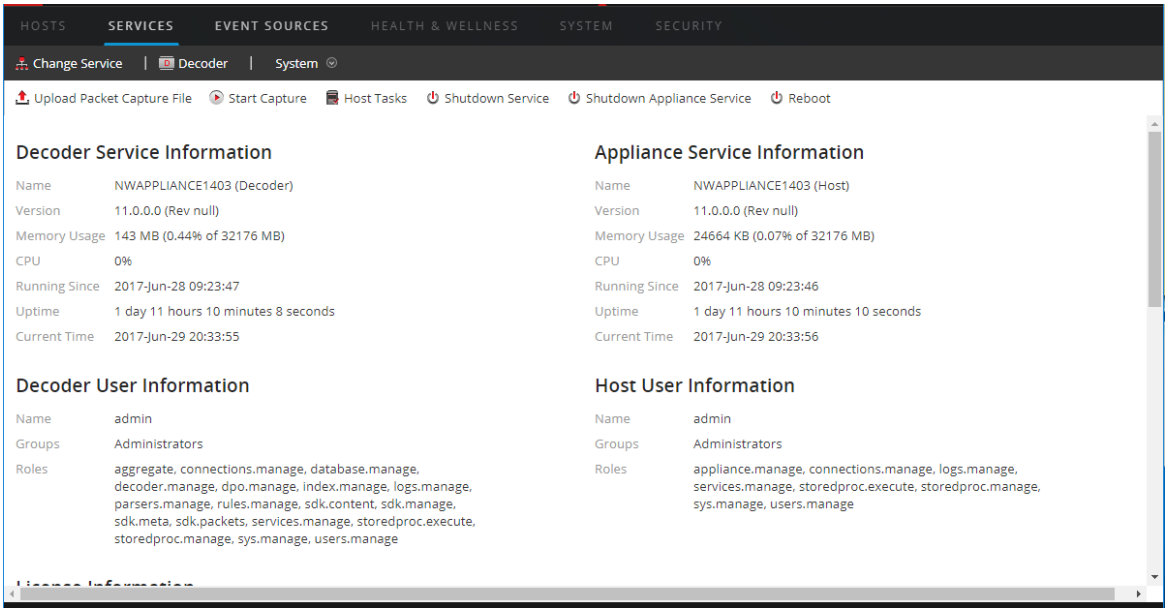


Ejecutar la configuración rápida inicial

Este procedimiento realiza la configuración inicial básica de un Decoder e inicia la captura de datos. Una vez finalizada la configuración básica, el Decoder comienza a capturar datos para que el Concentrator los consuma.

Para configurar un Decoder e iniciar la captura de datos:

1. Asigne una interfaz de red para capturar datos. Para obtener más información, consulte "Seleccionar un adaptador de red" en Configurar ajustes de captura.
2. Realice una de las siguientes acciones:
   a. Para iniciar la captura, seleccione el Decoder y > **Ver** > **Sistema**. En la barra de herramientas, haga clic en Start Capture.



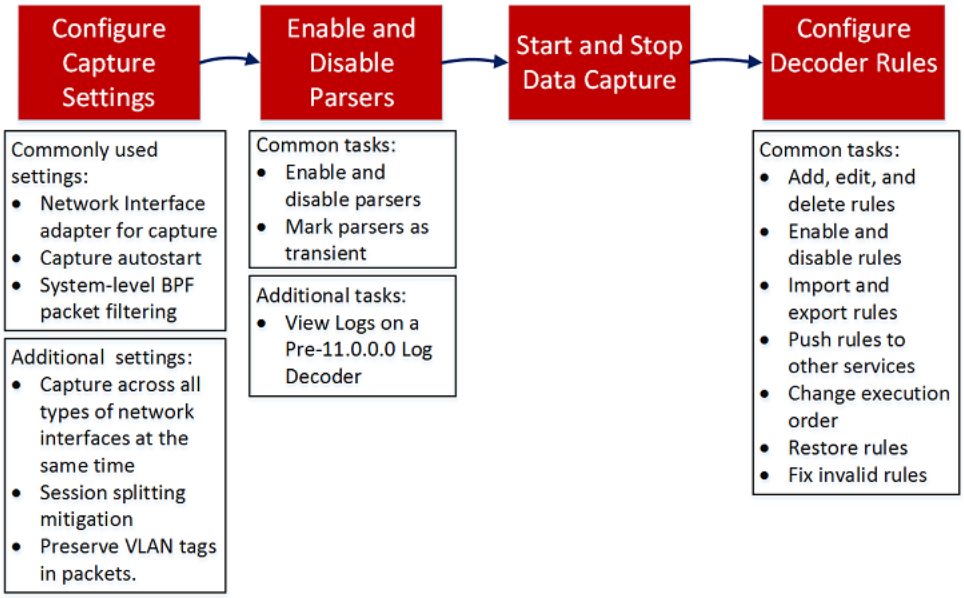
   b. Para habilitar el inicio automático de captura, consulte "Configurar un Decoder para comenzar a capturar datos automáticamente" en Configurar ajustes de captura.
   El Decoder comienza a capturar datos para el consumo de un Concentrator. Para las opciones de configuración adicionales, consulte Configurar ajustes comunes en un Decoder y Procedimientos adicionales de Decoder y Log Decoder

Configurar ajustes comunes en un Decoder

En esta sección se presentan los ajustes de configuración de uso frecuente en un Decoder con procedimientos e información adicional. Después de finalizar la Configuración rápida de Decoder y Log Decoder, puede acotar la configuración mediante el uso de analizadores, feeds y reglas para limitar los datos capturados.

Nota: Un Log Decoder es un tipo especial de Decoder y se configura y administra de manera similar a un Decoder. La mayor parte de la información en esta guía se refiere a ambos tipos de Decoders. "Decoder" se refiere a ambos tipos de Decoders. Se identifica claramente la información que se aplica de manera exclusiva a Network Decoders o Log Decoders.

El flujo de trabajo siguiente ilustra los ajustes de uso general y divide el proceso de configuración en cuatro pasos.

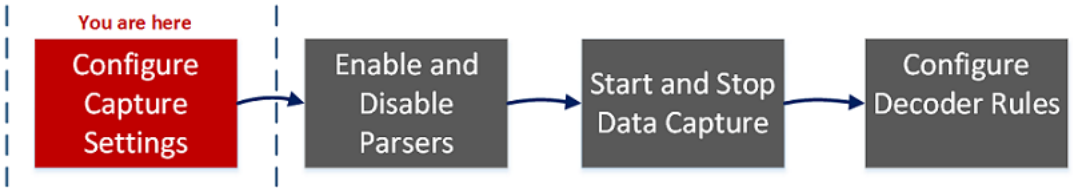


Paso de configuración	Descripción
Configurar ajustes de captura	Cuando se configura inicialmente el Decoder, es necesario configurar la interfaz del adaptador de red. Hay ajustes de captura opcionales adicionales disponibles; uno que se usa con frecuencia es el inicio automático de captura.
Habilitar y deshabilitar analizadores y analizadores de registros	Vea los analizadores que se descargaron y se implementaron desde Live y administre los que están habilitados o deshabilitados.

Paso de configuración	Descripción
Iniciar y detener la captura de datos	Cuando se inicia un Decoder, este comienza a agregar datos automáticamente si el Inicio automático de la captura está habilitado. Si el inicio automático no está activado, puede iniciar y detener la captura de datos de forma manual.
Configurar reglas de Decoder	Las reglas de captura pueden agregar alertas o información contextual a sesiones o registros. También pueden definir los datos que filtra un Decoder o un Log Decoder. De manera predeterminada, no hay reglas de captura definidas cuando configura NetWitness Platform por primera vez. A menos que se especifiquen reglas y que estas sean válidas, los paquetes no se filtran. Puede implementar las reglas más recientes desde Live como se describe en la *Guía de administración de servicios de Live*. Puede definir reglas de captura en cualquier momento y puede corregir las reglas que usan sintaxis no válida (Corregir las reglas con sintaxis no válida).

Configurar ajustes de captura

Cuando se configura inicialmente el Decoder, es necesario configurar la interfaz del adaptador de red. Se dispone de ajustes de captura opcionales adicionales; dos que se usan con frecuencia son el filtro de paquetes Berkeley y el inicio automático de captura.



Además de la configuración básica de la interfaz del adaptador de red, puede optar por usar una de las configuraciones de fines especiales que se describe en (Opcional) Conservar las etiquetas de VLAN cuando se usa la interfaz de captura de MMAP de paquetes o (Opcional) Configurar un Decoder para capturar los datos en todos los tipos de interfaces de red

El resto de la configuración de captura tiene valores predeterminados elegidos para que sea eficaz en la mayoría de los casos (consulte una lista detallada en Vista Configuración de servicios: Pestaña General). Puede ajustarla en algunas circunstancias, por ejemplo, si el servicio al cliente aconseja un cambio. Puede editar la configuración de captura en cualquier momento.

Seleccionar un adaptador de red

La siguiente tabla describe la configuración del adaptador de red de un Decoder. El administrador del sistema configura los adaptadores de red predeterminados cuando está instalado el Decoder. Consulte al administrador del sistema para obtener más información.

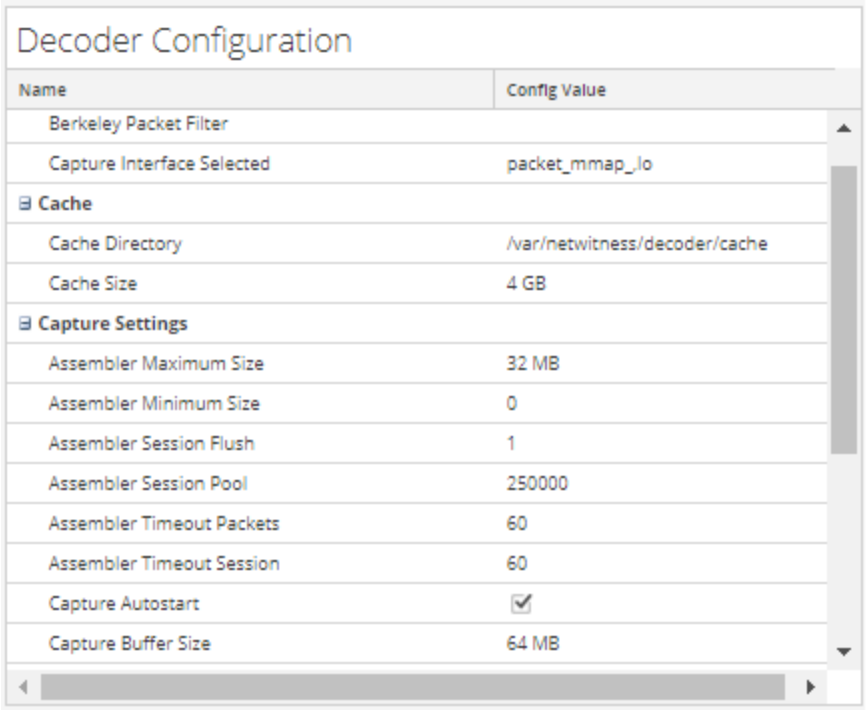
Parámetro de adaptador	Descripción
Filtro de paquetes Berkeley	Los Berkeley Packet Filters (BPF) se aplican al flujo de paquetes antes de que los paquetes se copien al adaptador de Decoder para el análisis. Esto permite que el tráfico no deseado se elimine de manera eficiente. Sin embargo, los paquetes descartados no se toman en cuenta en ninguna estadística del Decoder (velocidad de captura, paquetes descartados, paquetes filtrados y total de paquetes).

Parámetro de adaptador	Descripción
Interfaz de captura seleccionada	Seleccione un adaptador a través del cual el Decoder captura paquetes. Para la interfaz de captura interna de menor velocidad, utilice el adaptador `packet_mmap_,7,eth1` , que corresponde al puerto de monitoreo ubicado en la placa madre. Existen seis puertos de captura adicionales: • `packet_mmap_,1,lo (bpf)` • `packet_mmap_,2,eth2 (bpf)` • `packet_mmap_,3,eth3 (bpf)` • `packet_mmap_,4,eth4 (bpf)` • `packet_mmap_,5,eth5 (bpf)` • `packet_mmap_,8,ALL (bpf)` Existen tres servicios de captura inalámbricos disponibles: • `packet_netmon_ (Microsoft Netmon)` • `packet_mac80211_ (Linux mac80211)` • `packet_airport_ (Mac OS X AirPort)`
Interfaz de captura seleccionada para Log Decoder	El siguiente servicio de captura está disponible: • `log_events,Log Events`

Para configurar el adaptador de red en un Decoder:

1. Vaya a **ADMINISTRAR > Servicios**.

2. En la **Vista Servicios de Administration**, seleccione el Decoder y > **Ver** > **Configuración.** La Vista Configuración de servicios se muestra con la pestaña General abierta.

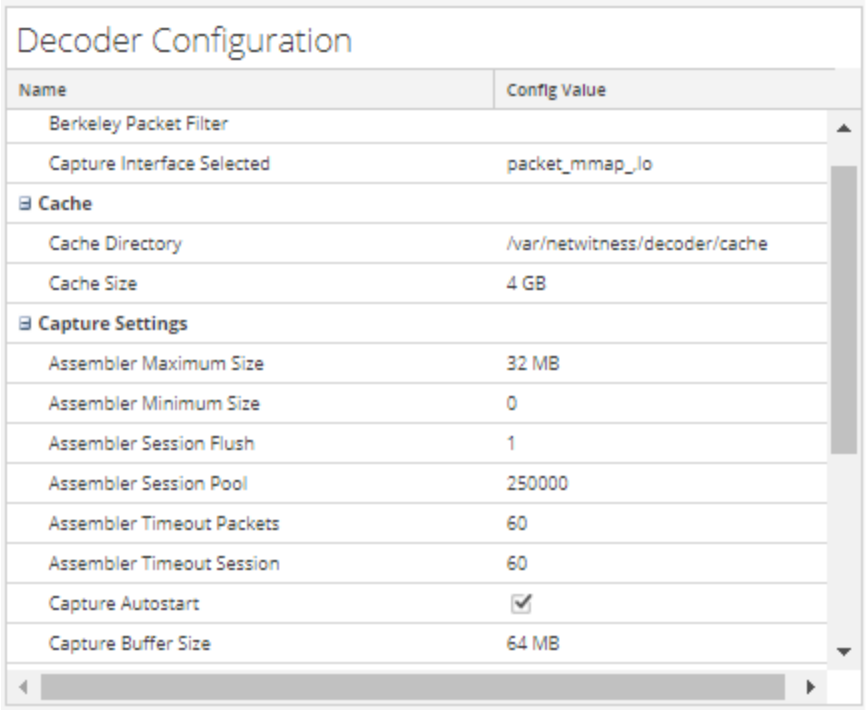


3. En el campo **Interfaz de captura seleccionada**, seleccione el adaptador de red que mejor se adapte al Decoder.
4. Para guardar los cambios, haga clic en **Aplicar.**
5. Si es necesario aplicar los cambios, regrese a la **Vista Servicios de Administration**, seleccione el Decoder y elija > **Reiniciar**.

Configurar un Decoder para que comience a capturar datos automáticamente

1. Vaya a **ADMINISTRAR** > **Servicios**.

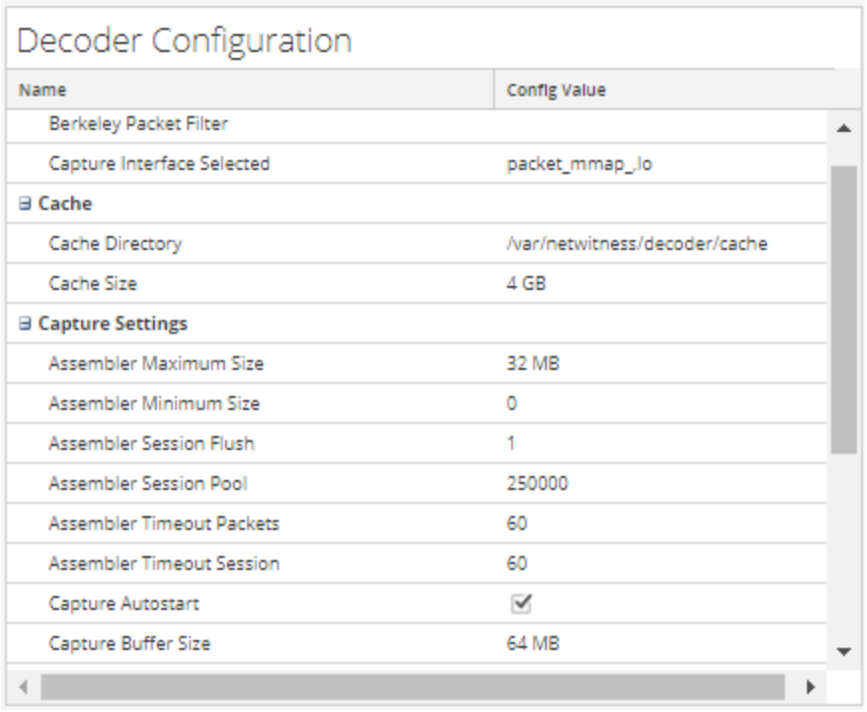
2. En la **Vista Servicios de Administration**, seleccione el Decoder y > **Ver** > **Configuración.** La Vista Configuración de servicios se muestra con la pestaña General abierta

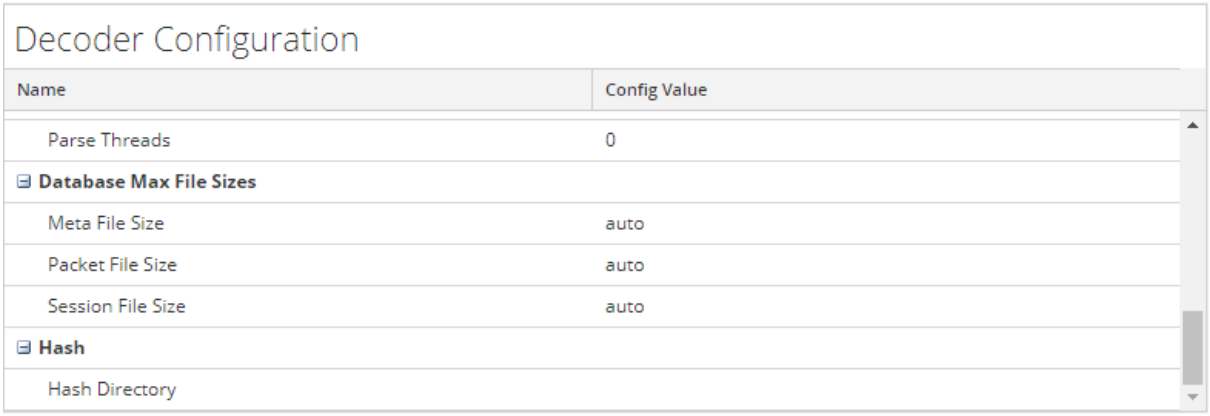


3. En **Configuración de captura**, seleccione la casilla de verificación **Inicio automático de captura**.
4. Para guardar los cambios, haga clic en **Aplicar.**
5. Si es necesario aplicar los cambios, regrese a la **Vista Servicios de Administration**, seleccione el Decoder y elija > **Reiniciar**.

Configurar ajustes de captura opcionales

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. En la **Vista Servicios de Administration**, seleccione el Decoder y > **Ver** > **Configuración.** La Vista Configuración de servicios se muestra con la pestaña General abierta.





3. Si desea aplicar un filtro de nivel de sistema al flujo de paquetes antes de que los paquetes se copien en el adaptador de Decoder para el análisis, configure el filtro de paquetes Berkeley como se describe en (Opcional) Configurar filtrado de paquetes a nivel del sistema (BPF).
4. En las secciones **Configuración de captura**, revise los valores predeterminados. Cuando un servicio se agrega por primera vez, los valores predeterminados están vigentes y deben cambiarse solo en circunstancias especiales, por ejemplo, si el servicio al cliente aconseja un cambio. Consulte Vista Configuración de servicios: Pestaña General para obtener una explicación de estos ajustes.
5. En la sección **Tamaños máximos de archivo de base de datos**, revise los valores predeterminados. Cuando un servicio se agrega por primera vez, los valores predeterminados están vigentes y deben cambiarse solo en circunstancias especiales, por ejemplo, si el servicio al cliente aconseja un cambio. Consulte Vista Configuración de servicios: Pestaña General para obtener una explicación de estos ajustes.

6. En la sección **Hash**, defina un directorio para los archivos hash si está usando esta función. Consulte Vista Configuración de servicios: Pestaña General para obtener una explicación de estos ajustes.

(Opcional) Configurar filtrado de paquetes a nivel del sistema (BPF)

Puede usar los Berkeley Packet Filters para controlar los paquetes y los registros que procesa un Decoder.

Los Berkeley Packet Filters (BPF) se aplican al flujo de paquetes antes de que los paquetes se copien al adaptador de Decoder para el análisis. Esto permite que el tráfico no deseado se elimine de manera eficiente. Estos paquetes descartados no se toman en cuenta en ninguna estadística del Decoder (velocidad de captura, paquetes descartados, paquetes filtrados y total de paquetes).

El Decoder admite además el filtrado de paquetes en el nivel de sistema que se define con la sintaxis `tcpdump/libpcap`. Especificar un filtro `Libpcap` puede reducir de manera eficaz el volumen del paquete según atributos de Capa 2-Capa 4. Un filtro `Libpcap` es adecuado para usarse cuando un Decoder está recibiendo un volumen de tráfico que impone una carga sobre los recursos físicos de la plataforma. En este escenario, el Decoder puede descartar paquetes constantemente y tener una gran cantidad de páginas de captura disponibles (`/decoder/stats/capture.pagefree` es alto).
El siguiente es un ejemplo de un filtro `libpcap` para conservar solo los paquetes que no tienen tanto la dirección de origen como la de destino en la subred 10.21.0.0/16.

```
not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)
```

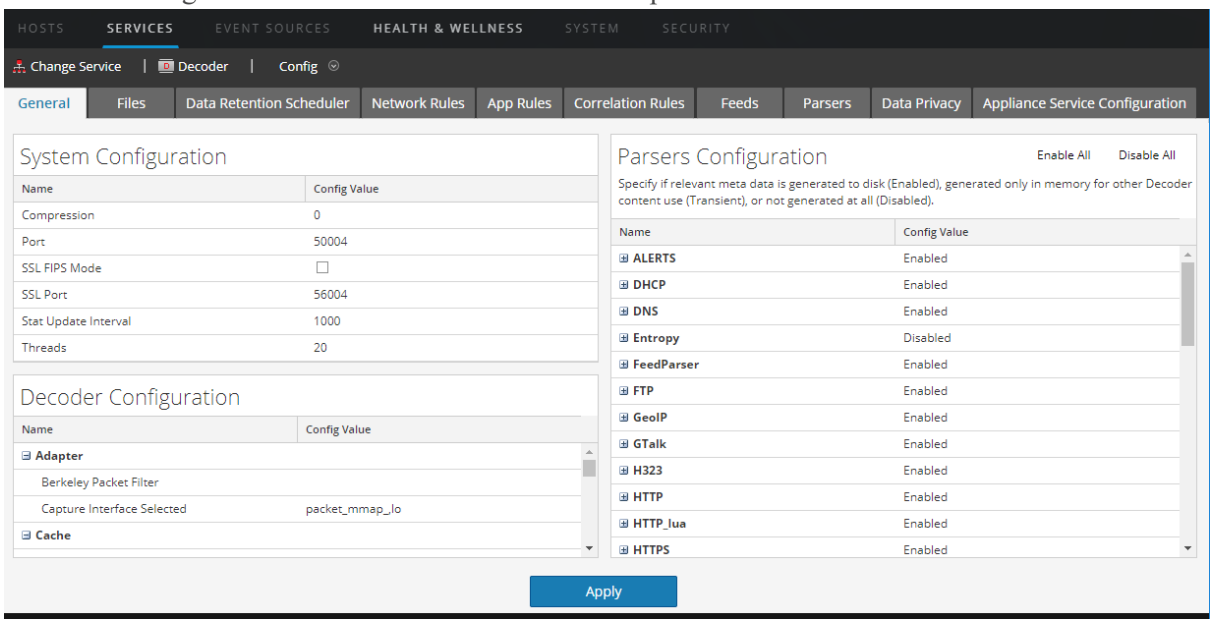
Para obtener una referencia completa de la sintaxis del filtro `Libpcap`, consulte las páginas principales de:

- tcpdump (http://www.tcpdump.org/tcpdump_man.html).
- pcap-filter (http://www.unix.com/man-page/FreeBSD/7/pcap-filter/).

Para agregar un filtro de paquetes Berkeley en el nivel del sistema:

1. Vaya a **ADMINISTRAR > Servicios.**
2. En la Vista Servicios de Administration, seleccione un servicio Decoder y  **> Ver > Configuración.**

La Vista Configuración de serviciosse muestra con la pestaña General abierta.



3. En la sección **Configuración de Decoder**, bajo **Adaptador**, haga clic en el campo que aparece junto a **Filtro de paquetes Berkeley**.
4. Ingrese solo un filtro en el campo. Si desea filtrar varios elementos, una varias expresiones usando `and`. A continuación se proporcionan varios ejemplos.
   La interfaz del usuario valida la entrada cuando ingresa la cadena de filtro.
5. Para guardar el filtro, haga clic en **Aplicar**.
   Si la sintaxis está correcta, se muestra un mensaje de confirmación.
   Si no lo está, se muestra un mensaje **El filtro de paquetes no es válido**, seguido de un mensaje de registro correspondiente en los mensajes de registro del Decoder:
   ```
   164474800 2015-May-01 19:03:08 warning Decoder Failed to parse filter 'example_badrule': syntax error
   ```
6. Para activar el filtro, debe detener e iniciar la captura en el Decoder:
   a. Pase de la vista **Configurar** a la vista **Sistema**.
   b. Haga clic en **Detener captura**.
   c. Haga clic en **Iniciar captura**.
      El filtro activo se mostrará en los registros de Decoder.

Ejemplos

Los siguientes son varios ejemplos de filtros:

- Descartar paquetes hacia o desde cualquier dirección de la subred 10.21.0.0/16:
  `not (net 10.21.0.0/16)`
- Descartar paquetes que tienen direcciones de origen y de destino en la subred 10.21.0.0/16:
  `not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`

- Descartar paquetes que provienen de 10.21.1.2 o se dirigen a 10.21.1.3.
  `not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Combinar IP y HOST:
  `not (host 192.168.1.10) and not (host api.wxbug.net)`
- Descartar todo el tráfico del puerto 53, tanto de TCP como UDP:
  `not (port 53)`
- Descartar solo el tráfico del puerto 53 de UDP:
  `not (udp port 53)`
- Descartar todo el tráfico IP protocolo 50 (IPSEC):
  `not (ip proto 50)`
- Descartar todo el tráfico en los puertos TCP 133 a 135.
  `not (tcp portrange 133-135`

Los siguientes filtros combinan algunos de los filtros anteriores para demostrar cómo poner varias instrucciones en un solo filtro:

- Descargar el tráfico del puerto 53(DNS) que se origina en 10.21.1.2 o se destina a 10.21.1.3.
  `not (port 53) and not (src host 10.21.1.2 or dst host 10.21.1.3)`
- Descartar cualquier tráfico que use el protocolo IP 50 o el puerto 53, o cualquier tráfico proveniente de la red 10.21.0.0/16 con destino a la red 10.21.0.0/16
  `not (ip proto 50 or port 53) or not (src net 10.21.0.0/16 and dst net 10.21.0.0/16)`

Precaución: El uso de paréntesis puede tener un amplio efecto potencialmente disruptivo en la utilización de filtros de paquetes. Como mejor práctica, mantenga las operaciones "not" fuera de paréntesis y pruebe siempre las reglas antes de implementarlas. Si no escribe las reglas con el formato correcto (a pesar de la validación de la entrada), puede que un filtro de paquete descarte TODO el tráfico o presente otros comportamientos inesperados. Esto se debe a la manera en que funcionan los filtros de paquetes `Libpcap` y no sucede a causa de ninguna lógica del software NetWitness Platform.

Pruebas

Los filtros BPF se pueden y se deben probar usando `tcpdump` o `windump` para asegurarse de que presenten el comportamiento esperado antes de su implementación. Este ejemplo muestra la prueba de un filtro usando windump:

```
windump -nni 2 not (port 53 or port 443) or not (ip proto 50)
```

Conversiones

Si por motivos de rendimiento decide que sería mejor ejecutar un filtro de regla de red existente como un filtro de paquetes en el nivel del sistema, puede convertirlo. Cuando haga conversiones, debe tener en cuenta algunos puntos.

- `&&` se convierte en `and`
- `ip.addr` se convierte en `host` si se trata de un solo host o en **net** si se trata de una red.

- `ip.src` se convierte en `src host` si se trata de un solo host o en `src net` si se trata de una red.
- `ip.dst` se convierte en `dst host` si se trata de un solo host o en `dst net` si se trata de una red.
- Utilice la notación CIDR cuando enumere una red (es decir, 10.10.10.0/24).
- `||` se convierte en `or`
- `!` se convierte en `not`
- Para unir varias reglas, debe usar `and`.

El manual de TCPDump también proporciona ejemplos de filtros y cadenas que puede usar: http://www.tcpdump.org/tcpdump_man.html

Además, el siguiente sitio ofrece una excelente referencia para los filtros de paquetes de tipo BPF: http://biot.com/capstats/bpf.html

Precaución: Si captura paquetes etiquetados `vlan`, es posible que el filtro bpf estándar anterior no funcione. Por ejemplo, si usa `not (udp port 123)` para filtrar el tráfico NTP etiquetado `vlan` en el puerto udp 123, no funcionará. Esto se debe a que el sistema de filtro bpf es simple y no toma en cuenta protocolos a los que no se hace referencia en la regla. Por lo tanto, el sistema operativo que ejecuta el filtro bpf buscará los valores de `udp port` con la compensación de bytes que ocurriría en un paquete Ethernet/udp estándar; pero los campos de etiqueta `vlan` opcionales en el encabezado Ethernet migran estos valores por 4 bytes, lo que hará que la regla de filtro bpf falle. Para repararlo, debe cambiar el filtro bpf a: `not (vlan and udp port 123)`.

(Opcional) Configurar un Decoder para capturar los datos en todos los tipos de interfaces de red

El adaptador de `packet_mmap_,ALL` es capaz de capturar en todos los tipos de interfaces de red al mismo tiempo. Por ejemplo, esto puede incluir elementos como interfaces de red física en diferentes tipos de medios e interfaces de túnel.

El comportamiento predeterminado del adaptador de `ALL` es capturar de todas las interfaces del sistema, a excepción de los valores predeterminados codificados de `lo`, `eth0` y `em1`.

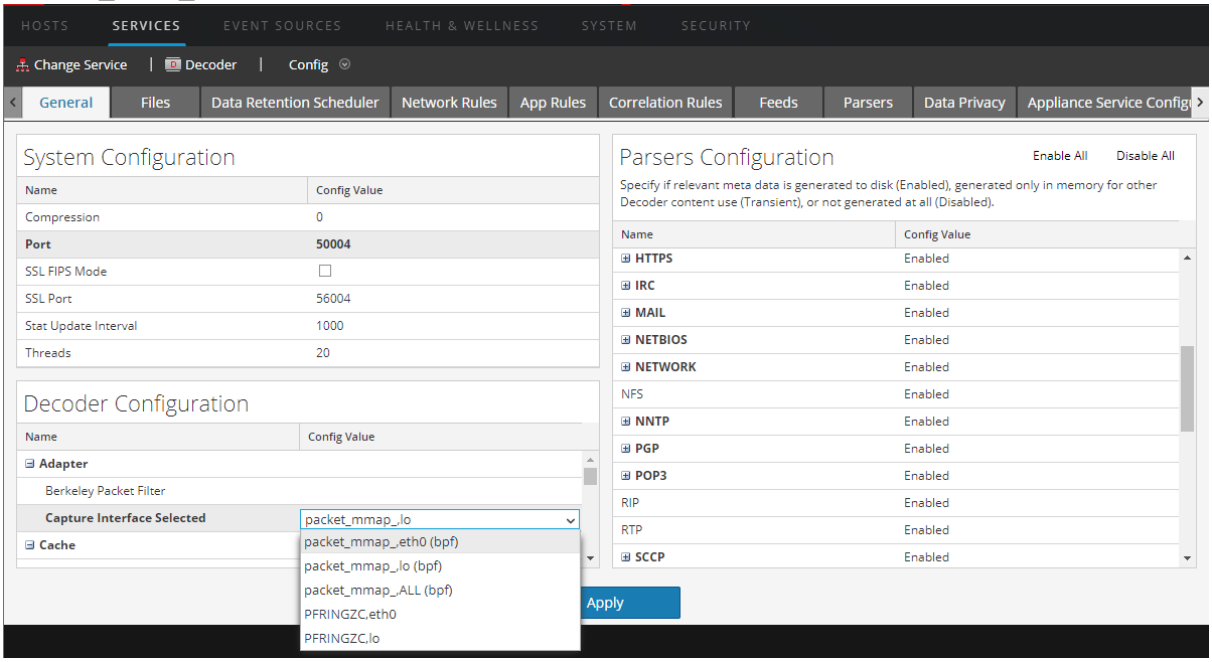
Puede seleccionar cualquier subconjunto de las interfaces de captura mediante la edición del nodo de configuración `/decoder/config/capture.device.params` de Decoder para incluir un parámetro `interfaces=`. El parámetro `interfaces` contiene una lista separada por comas de las interfaces que se usan para la captura. En lugar de usar todas las interfaces para la captura, solo se usan las interfaces especificadas.

Por ejemplo, si desea forzar la captura en las interfaces `em1`, `em2` y `em4`, y pasar por alto `em3`, puede seleccionar el adaptador de `packet_mmap_,ALL` y, a continuación, agregar esta línea a `capture.device.params`: `interfaces=em1,em2,em4`

Nota: El uso del parámetro `interfaces` para seleccionar `eth0`, `lo` o `em1` sobrescribe el comportamiento predeterminado, que consiste en descartar el tráfico de esos puertos.

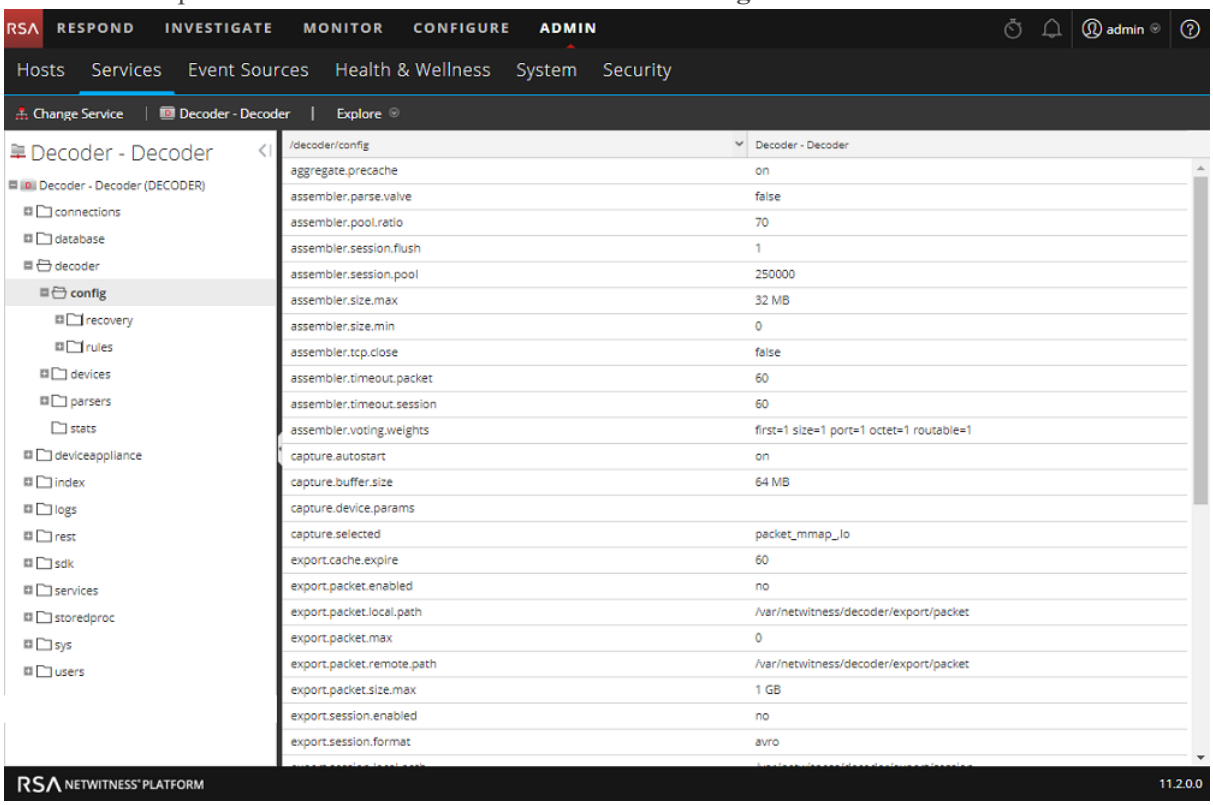
Para configurar el adaptador `packet_mmap_,ALL` para capturar desde interfaces específicas en lugar de todas las interfaces:

1. Vaya a **ADMINISTRAR** > **Servicios**, seleccione el servicio Decoder y > **Ver** > **Configuración.**
2. En **Vista Configuración de servicios**, configure **Interfaz de captura seleccionada** en el adaptador `packet_mmap_,ALL`.

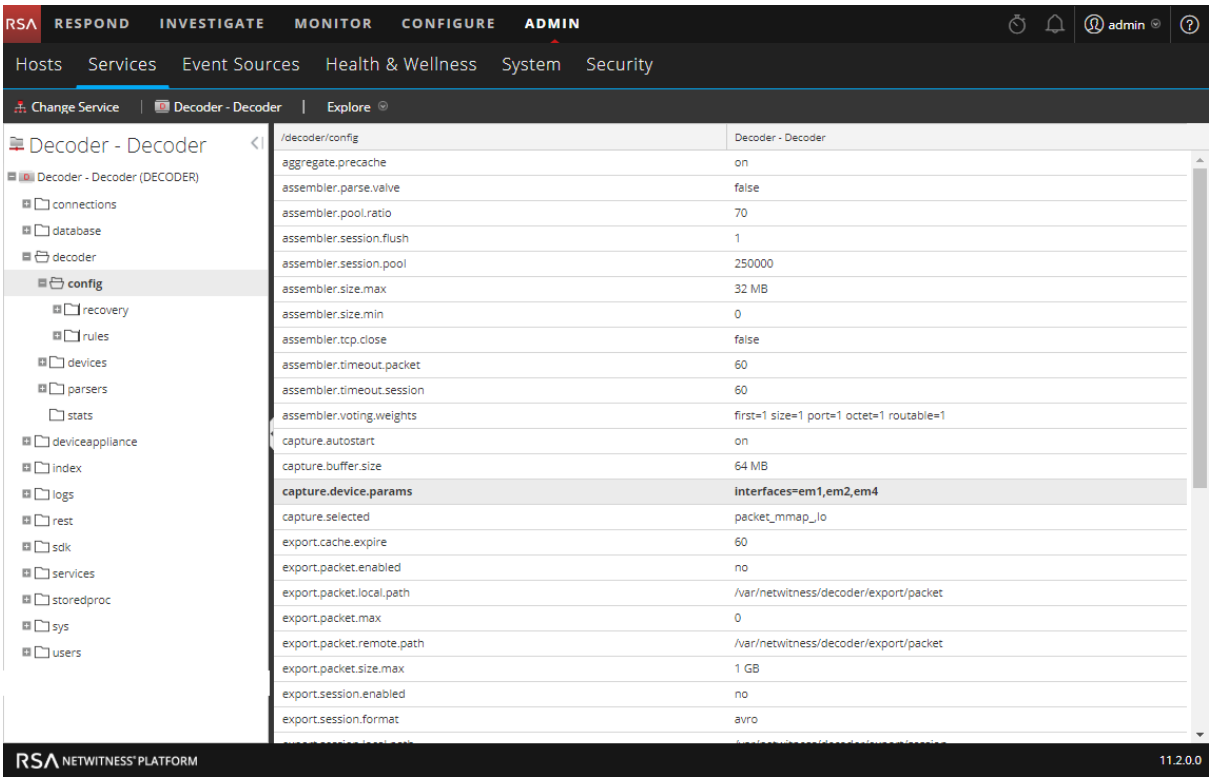


3. Para ir a la Vista Explorar de servicios, haga clic en **Configuración** en la barra de herramientas y seleccione **Explorar** en la lista desplegable.

4. En la Vista Explorar de servicios seleccione **decoder** > **configuración**.



5. Haga clic en la columna Valores junto a `capture.device.params`, escriba **`interfaces=em1,em2,em4`** y presione **Intro**.



El cambio surte efecto de inmediato; solo se captura el tráfico en las interfaces `em1`, `em2` y `em4`.

(Opcional) Configurar un Decoder para escribir archivos con formato pcap estándar

Nota: La información de este tema se aplica a RSA NetWitness® Platform versión 11.2 y superior.

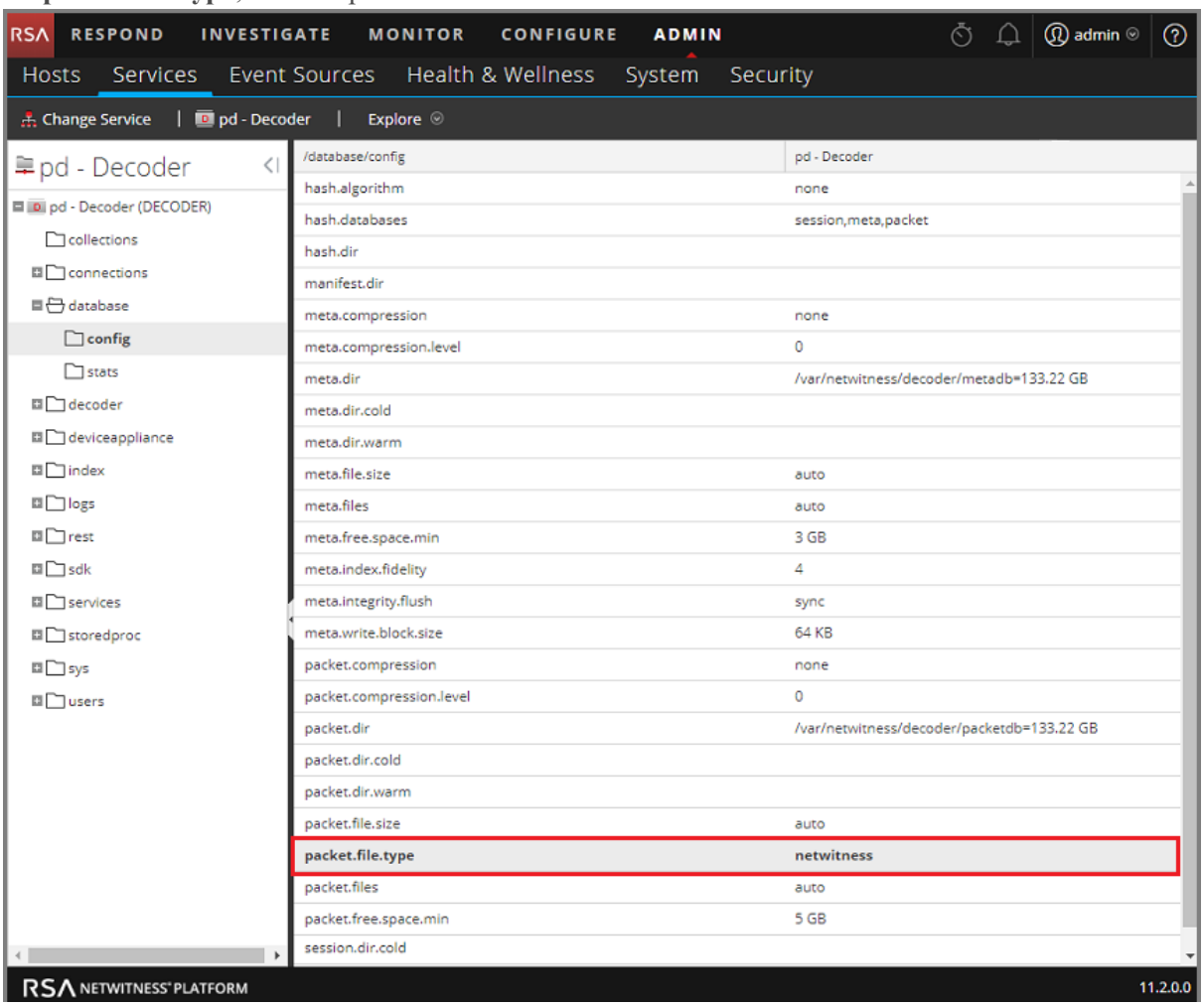
Para proporcionar un formato de base de datos más abierto, Network Decoder ahora puede escribir archivos con formato pcap estándar. Puede habilitar archivos de base de datos con formato pcapng con el nuevo nodo de configuración:
`/database/config/packet.file.type = 'netwitness' or 'pcapng'`

Nota: Esta funcionalidad está habilitada de manera predeterminada si 11.2 se instala directamente. Si actualiza desde una versión anterior a 11.2, debe habilitar manualmente los archivos de base de datos con formato pcapng, lo que puede dar lugar a una disminución aproximada del 4 % en el espacio en disco (ya que los archivos pcapng requieren más espacio que los archivos nwdb). También puede utilizar el formato pcapng con captura de 10 Gbps, lo que no reduce considerablemente el rendimiento (<1 %).

Para habilitar la escritura de archivos con formato pcap estándar:

1. Vaya a **ADMINISTRAR** > **Servicios**, seleccione un servicio Network Decoder y elija  > **Ver** > **Explorar**.
2. Vaya a **database** > **config**.

3. En **packet.file.type**, el valor predeterminado es **netwitness**.



4. Para cambiar el tipo de archivo de paquete al formato pcap estándar, escriba **pcapng**. Este cambio surtirá efecto de inmediato cuando se cree el siguiente archivo de paquete.

Nota: En el formato de archivo de base de datos pcapng, los datos están en texto no cifrado y nuestro formato de propiedad no los oculta, lo que puede mejorar la seguridad.

Precaución: No toque ninguno de los archivos de los directorios de la base de datos de paquetes. No debe leer ni editar ningún archivo `pcapng` de los directorios de la base de datos de paquetes, ya que siempre están en uso mientras Decoder está en ejecución. Decoder siempre espera acceso completo y exclusivo a esos archivos, y otros procesos que los leen impiden su operación normal. La manera correcta de acceder a los archivos `pcapng` es configurar un directorio de almacenamiento inactivo. Esto permite que Decoder copie los archivos `pcapng` al directorio de almacenamiento inactivo antes de su eliminación. En ese momento, usted es responsable de administrar los archivos `pcapng`, incluida la tarea de asegurarse de que el volumen de almacenamiento inactivo nunca se llene. Tenga en cuenta que la copia de los archivos `pcapng` al almacenamiento inactivo requiere una cantidad no menor de I/O y podría interferir con la captura de paquetes. El almacenamiento inactivo para `pcapng` no es compatible a velocidades de 10G.

(Opcional) Conservar las etiquetas de VLAN cuando se usa la interfaz de captura de MMAP de paquetes

Cuando captura tráfico que contiene etiquetas de VLAN, puede configurar la interfaz de captura de MMAP de paquetes para conservar las etiquetas VLAN en los paquetes (corrección de VLAN). De forma predeterminada, el hardware de captura de red quita las etiquetas. La ejecución de este procedimiento conserva las etiquetas en los paquetes y los valores de las etiquetas se analizan en metadatos de VLAN para un análisis avanzado.

Existen dos mecanismos para habilitar la corrección de VLAN.

- Opción 1: Configurar `vlan-fix=true` dentro de `capture.device.params`. Esta opción realiza la corrección de VLAN en todo el tráfico que ingresa al Decoder. Esta opción es adecuada en la mayoría de los casos, ya que se supone que todo el tráfico estará etiquetado como VLAN. Este mecanismo funciona en modo de una sola interfaz o en modo de todas las interfaces. Esta opción reemplaza a la configuración de corrección de VLAN en interfaces individuales; incluso las interfaces que no están configuradas para realizar la corrección de VLAN tendrán habilitada la función.
- Opción 2: Usar el parámetro `interfaces` dentro de `capture.device.params` en cada dispositivo. El parámetro `interfaces` acepta una lista de nombres de interfaz separada por comas en la cual se capturan paquetes. Mediante la adición de `:vlan` a un nombre de interfaz, puede habilitar la corrección de VLAN en interfaces individuales. Si no se agregó el sufijo `:vlan` a la interfaz, no se realizará la corrección de VLAN.

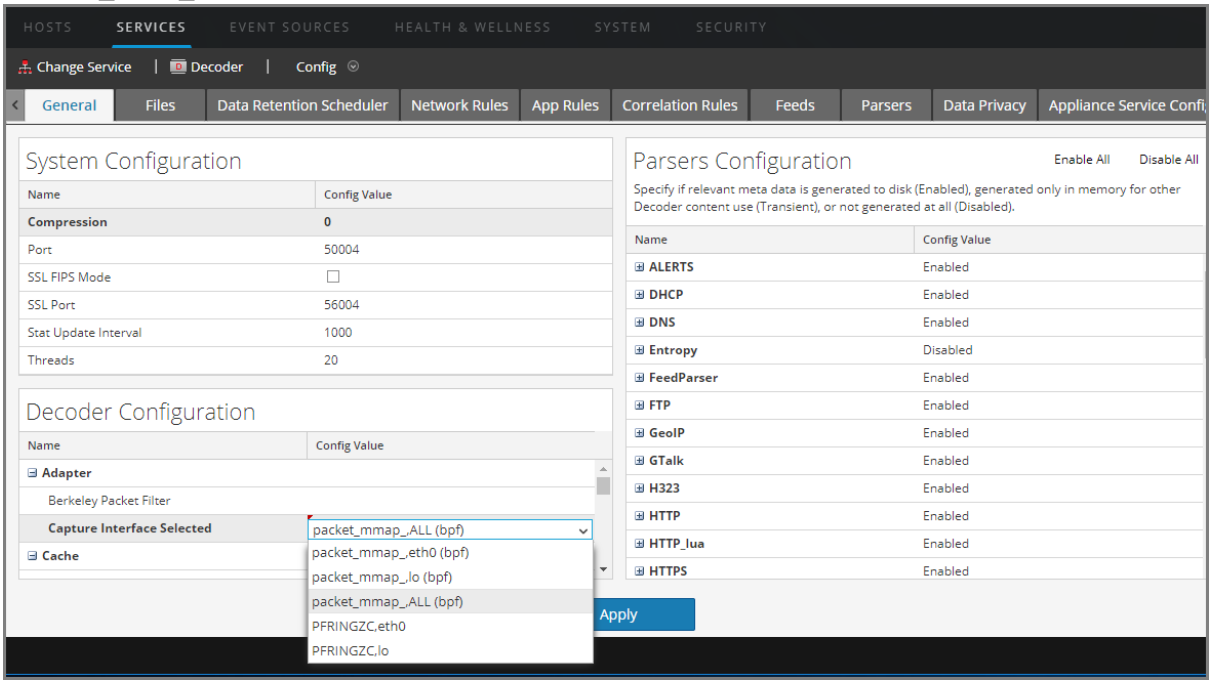
Después de editar este parámetro, debe reiniciar la captura en el Decoder para que los cambios a `capture.device.params` surtan efecto.

Estos son ejemplos de `vlan` de ambas opciones. Si es necesario pasar varias configuraciones para `capture.device.params`, use la siguiente sintaxis. Tenga en cuenta que se usan comillas para los valores con espacios en blanco, consulte *Guía de ajuste de la base de datos de Core*. `name1="value1" name2="value2"`.

Parámetro	Valor	Efecto
`capture.device.params`	`vlan-fix=true`	La corrección de VLAN siempre se ejecuta en todas las interfaces. El valor predeterminado es `vlan-fix=false`.
`capture.device.params`	`interfaces=eth0:vlan,eth1`	La corrección de VLAN se ejecuta en la captura de tráfico solo en la interfaz `eth0`
`capture.device.params`	`interfaces=eth0:vlan,eth1 vlan-fix=true`	La corrección de VLAN siempre se ejecuta porque la configuración de `vlan-fix` reemplaza la configuración de las interfaces.

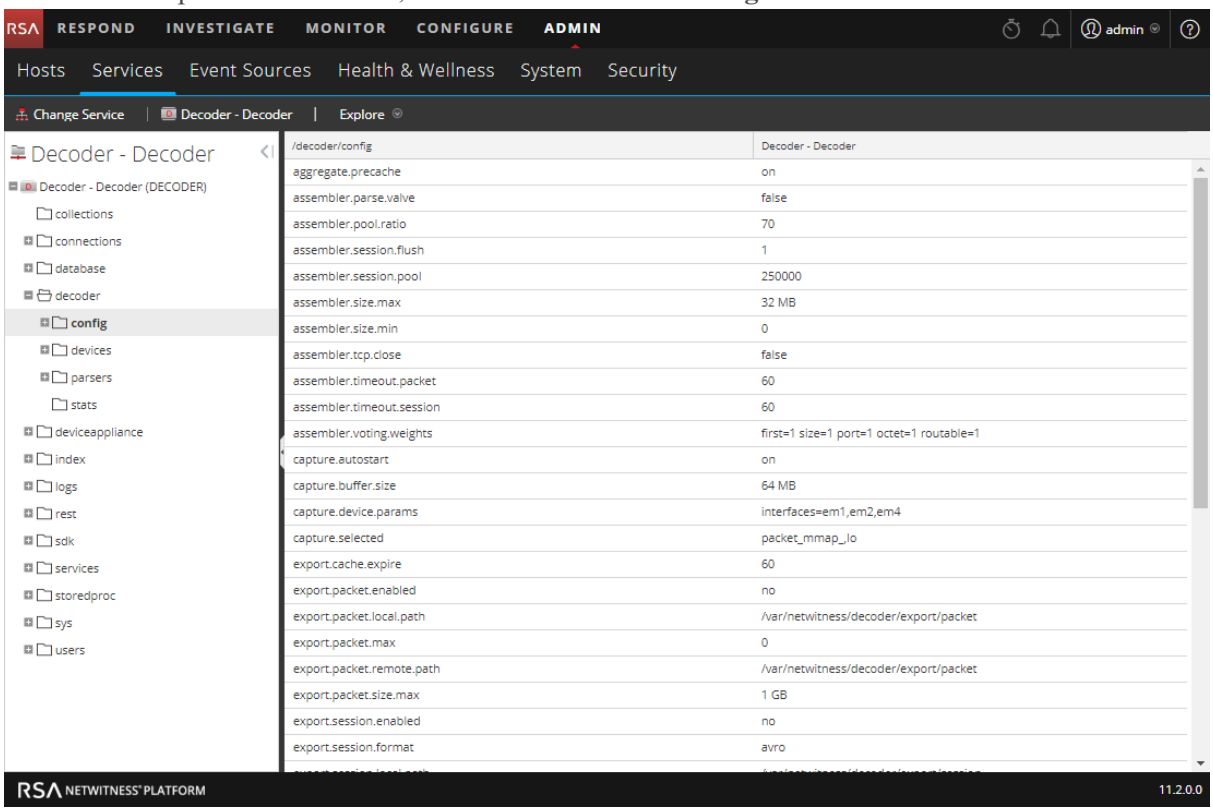
Para configurar el adaptador `packet_mmap_` con el fin de conservar las etiquetas de VLAN en los paquetes:

1. En **Vista Servicios de Administration**, seleccione el servicio Decoder y > **Ver** > **Configuración.**
2. En **Vista Configuración de servicios**, configure **Interfaz de captura seleccionada** en el adaptador `packet_mmap_,ALL`.



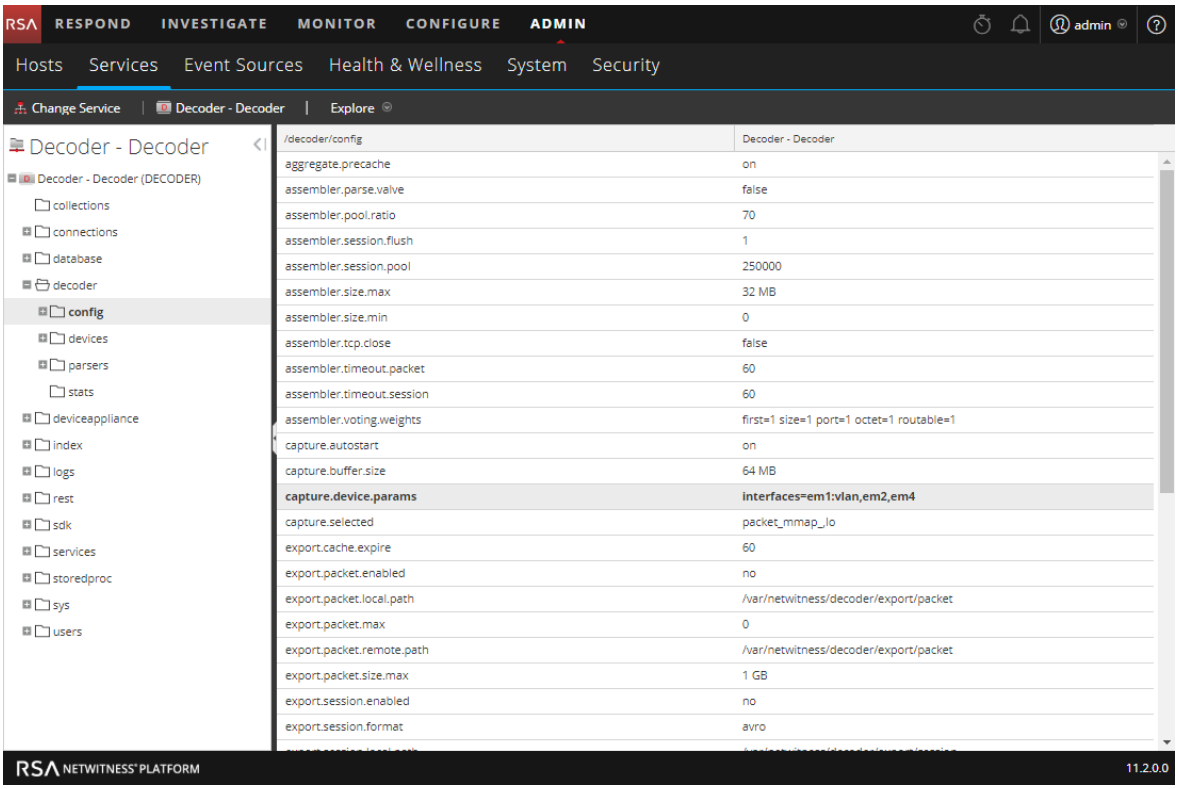
3. Para ir a la Vista Explorar de servicios, haga clic en **Configuración** en la barra de herramientas y seleccione **Explorar** en la lista desplegable.

4. En la Vista Explorar de servicios, seleccione **decoder** > **configuración**.



5. Haga clic en la columna de valores junto a `capture.device.params` y realice una de las siguientes acciones:

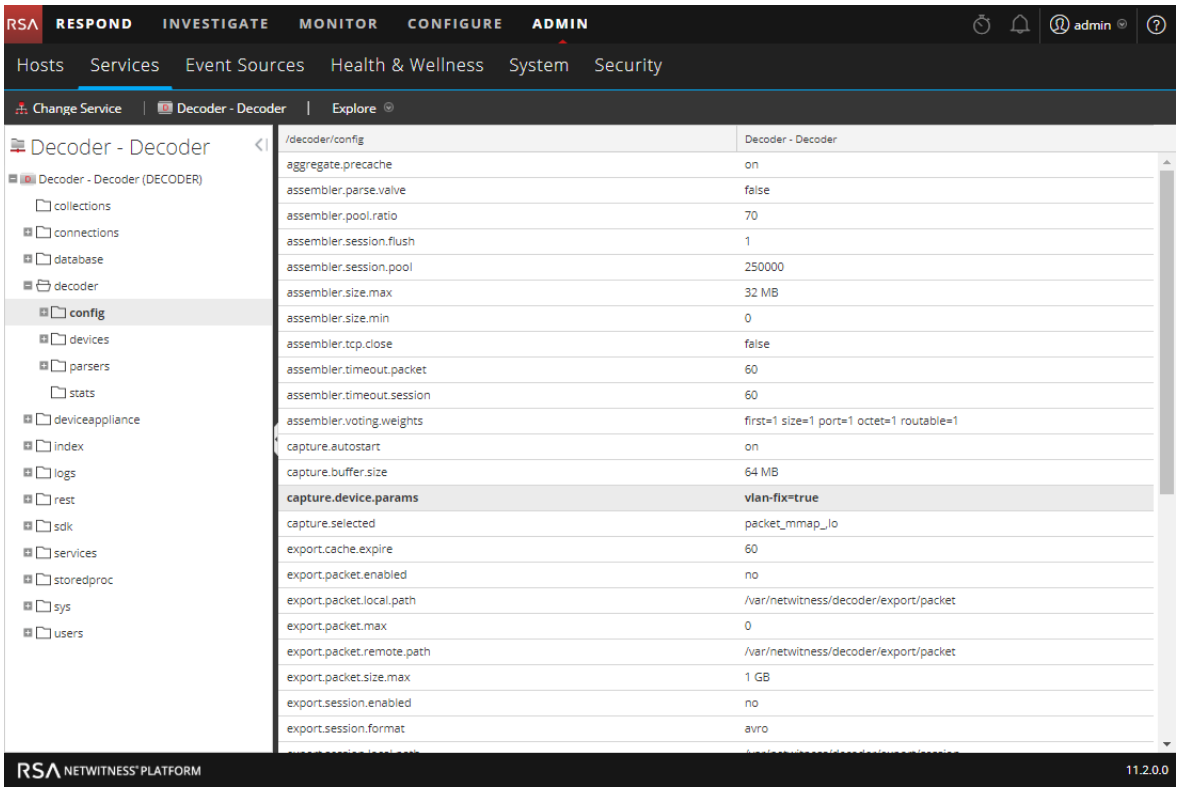
   - Para conservar las etiquetas de VLAN en una interfaz en la lista de interfaces, agregue **`:vlan`** después del nombre de la interfaz y presione **Intro**. Por ejemplo, esto especifica que se conservan las etiquetas de VLAN en `em1`, pero no en `em2` y `em4`:
     `interfaces=em1:vlan,em2,em4`



El cambio se aplica de inmediato; solo el tráfico en `em1` conserva las etiquetas de VLAN.

- Para conservar las etiquetas de VLAN en todas las interfaces, ingrese lo siguiente y presione **Intro**:

  `vlan-fix=true`

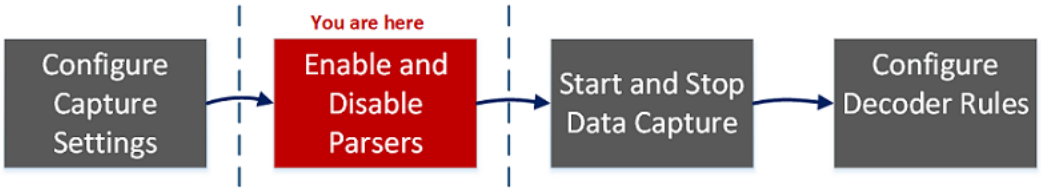


El cambio se aplica de inmediato; las etiquetas de VLAN se conservan en todas las interfaces de captura.

Habilitar y deshabilitar analizadores y analizadores de registros

Los administradores pueden ver qué analizadores se descargaron desde Live y se implementaron en un Decoder o un Log Decoder, pueden ver cuáles de ellos están habilitados y habilitar o deshabilitar analizadores y analizadores de registros.

La siguiente figura ilustra las configuraciones de uso general en un Decoder. Para una rápida configuración básica con los pasos requeridos solamente, consulte Configuración rápida de Decoder y Log Decoder.



Solo debe descargar e implementar los analizadores que necesita por las siguientes razones:

- El rendimiento se ve afectado a medida que aumenta la cantidad de analizadores implementados.
- Mientras más analizadores implementa, más metadatos se crean, lo cual afecta la retención de datos
- Si no se implementan analizadores de registros adicionales (innecesarios), se reduce el potencial de identificación errónea de mensajes.

En el panel Configuración de analizadores se proporciona una forma de seleccionar los analizadores que se usarán en el Decoder. En algunos analizadores, también puede configurar los metadatos que crea el analizador. Estas son las opciones en el panel Configuración de analizadores.

Opción	Descripción
Habilitar todos Deshabilitar todos	Estas opciones proporcionan una manera de seleccionar rápidamente todos los analizadores o ningún analizador.
Nombre	Los nombres de los analizadores disponibles para el Decoder. Un signo más indica que los metadatos generados por el analizador se pueden configurar. Al hacer clic en el signo más se muestran los metadatos que el analizador puede crear.

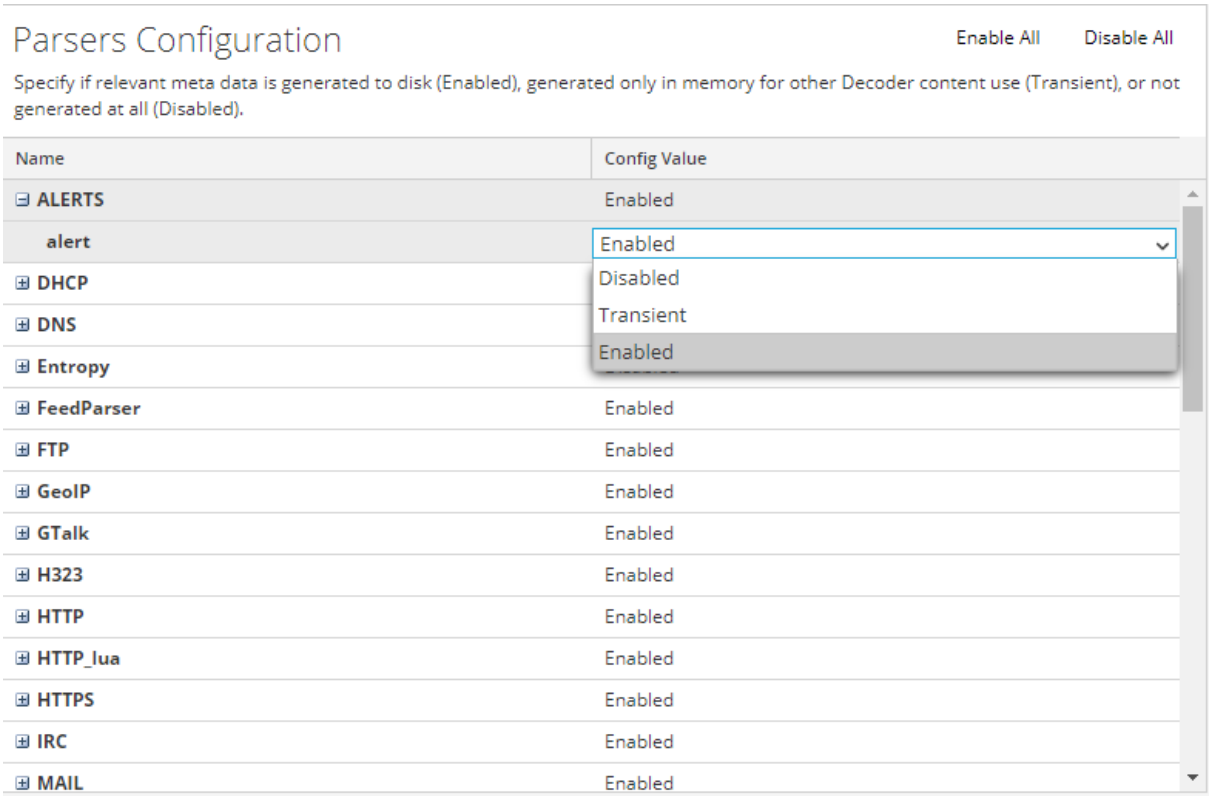
Opción	Descripción
Valor de configuración	Una lista desplegable cambia la configuración del analizador o de los metadatos a **Activado**, **Desactivado** o **Transitorio**. • Cuando se selecciona **Activado**, el Decoder usa el analizador para filtrar el tráfico. • Cuando se selecciona **Transitorio**, el Decoder usa el analizador para filtrar el tráfico y los metadatos generados no se almacenan en disco. Los metadatos transitorios están disponibles en la memoria para el contenido adicional (es decir, analizadores, feeds y reglas de aplicación) de ese Decoder. Esto ayuda a los administradores a proteger ciertos datos y suele ser parte de un plan de privacidad de datos (consulte *Guía de Administración de la privacidad de datos*). • Cuando se selecciona **Desactivado**, el Decoder no usa el analizador. Si los metadatos generados para el analizador son configurables, cuando se hace clic en el signo más para expandir el analizador, se muestran las claves de metadatos configurables y la misma lista desplegable selecciona la clave de metadatos que creará el analizador.

Nota: Para un Log Decoder, debe haber implementado analizadores de registros desde Live con anterioridad. Para obtener detalles, consulte el tema **Buscar e implementar recursos de Live** en la guía *Administración de servicios de Live*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Para habilitar o deshabilitar un analizador o para ver el estado de cada analizador:

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. En la **Vista Servicios de Administration**, seleccione un Log Decoder o un Decoder, y  **>Ver** > **Configuración**.

3. En el panel **Configuración de analizadores**, busque el analizador de Decoder o el analizador de origen de eventos de Log Decoder.



4. En la columna **Valor de configuración**, observe el estado actual del analizador.

   Puede actualizar el estado de cualquier analizador individual mediante la selección de su **Valor de configuración** y la sección de **Deshabilitado**, **Transitorio** o **Habilitado** en el menú desplegable. Como alternativa, puede seleccionar **Habilitar todo** o **Deshabilitar todo** para actualizar el estado de todos los analizadores de registros a la vez.

5. Haga clic en **Aplicar**.

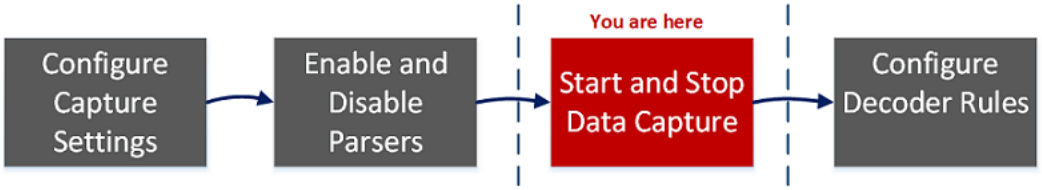
Cuando hace clic en **Aplicar**, todos los analizadores se vuelven a cargar en NetWitness Platform. El estado de cada analizador se actualiza de acuerdo con lo que se selecciona.

Iniciar y detener la captura de datos

Cuando se inicia un Decoder, este comienza automáticamente a agregar datos si el **AutoStart de la captura** está habilitado. Si el inicio automático no está activado, puede iniciar y detener la captura de datos de forma manual.

Nota: Los ajustes de configuración de captura en la vista Configuración de servicios para un Decoder determinan si el AutoStart de la captura está habilitado.

La siguiente figura ilustra las configuraciones de uso general en un Decoder. Para una rápida configuración básica con los pasos requeridos solamente, consulte Configuración rápida de Decoder y Log Decoder. Posiblemente quiera detener e iniciar la captura en otras ocasiones, por ejemplo, antes de apagar el servicio.



Para iniciar y detener la captura:

1. Vaya a **ADMINISTRAR > Servicios.**
2. En la vista **Servicios de Administration**, seleccione un servicio Decoder o Log Decoder y elija  **>Ver > Sistema**.
3. En la barra de herramientas, haga clic en **Iniciar captura**.

   Si el servicio es un Decoder, comienza a capturar paquetes Si el servicio es un Log Decoder, comienza a capturar registros.

   Cuando la captura de paquetes o registros está en progreso, la opción en la barra de herramientas cambia a **Detener captura** y la opción para cargar un archivo no está disponible.
4. Cuando quiera interrumpir la captura de tráfico en un Decoder, haga clic en **Detener captura**.

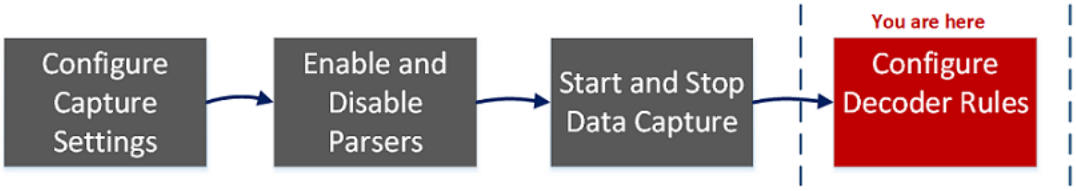
   La captura de paquetes o registros finaliza y la opción para cargar un archivo al servicio vuelve a estar disponible.

Nota: Al detener el servicio de Log Decoder mientras la captura está en ejecución, todos los eventos actualmente en la memoria de Log Decoder se procesarán y persistirán. En caso de que se produzca un problema que exija apagar rápidamente el servicio, use la vista Explorar de servicios para detener la captura (`/decoder stop`) y pasar los parámetros `flush=false` antes de detener el servicio de Log Decoder. Para obtener más información, consulte el tema “Vista Explorar de servicios” de la *Guía de introducción de hosts y servicios*.

Configurar reglas de Decoder

En este tema se proporcionan procedimientos para crear y administrar reglas para la captura de tráfico de Decoder o Log Decoder en la vista Configuración de servicios > pestañas Reglas. La Vista Configuración de servicios: pestañas Reglas proporciona detalles de las opciones de la pestaña Reglas.

La siguiente figura ilustra las configuraciones de uso general en un Decoder. Para una rápida configuración básica con los pasos requeridos solamente, consulte Configuración rápida de Decoder y Log Decoder.



Las reglas de captura pueden agregar alertas o información contextual a sesiones o registros. También pueden definir los datos que filtra un Decoder o un Log Decoder. Las reglas se crean para patrones de metadatos específicos, los cuales dan como resultado acciones predefinidas cuando se encuentran coincidencias. Por ejemplo, para mantener todo el tráfico que cumple determinados criterios, pero descartar todo el otro tráfico, puede crear una regla que lleve a cabo las acciones necesarias. Cuando se aplican, las reglas afectan tanto la importación de archivos de captura de paquetes como la captura de red en vivo.

En Guía de reglas y consultas se proporciona una guía que deben seguir todas las consultas y las condiciones de regla en los servicios principales de NetWitness Platform.

De manera predeterminada, no hay reglas definidas cuando instala NetWitness Platform por primera vez. Hasta que se especifiquen reglas, los paquetes no se filtran. Puede implementar las reglas más recientes desde Live. Puede definir tres tipos de reglas: Reglas de red, Reglas de aplicación y Reglas de correlación.

- Las reglas de red se aplican en el nivel de paquete y se componen de conjuntos de reglas de capa 2, capa 3 y capa 4. Es posible aplicar varias reglas al Decoder. Las reglas se pueden aplicar a varias capas (por ejemplo, cuando una regla de red filtra puertos específicos de una dirección IP específica). Las reglas de red están disponibles únicamente en Network Decoders.
- Las reglas de aplicación se aplican en el nivel de la sesión. Si la primera regla de la lista no es una coincidencia, Decoder intenta hacer coincidir la regla siguiente hasta que encuentra una coincidencia.
- Las reglas de correlación se aplican en una ventana de tiempo móvil configurable. Cuando se encuentra una coincidencia, el servicio crea una nueva supersesión que identifica a otras sesiones que coinciden con la regla y, a continuación, crea una lista de sesiones para análisis.

Los dos usos más comunes de las reglas son:

- Generar alertas y crear de este modo un valor de metadatos de alerta personalizado cuando se detectan ciertas condiciones.
- Filtrar ciertos tipos de tráfico que no agregan valor al análisis de los datos.

Los grupos de reglas de captura forman conjuntos de reglas, que puede importar y exportar. Esta funcionalidad permite usar varios conjuntos de reglas para diversos escenarios. Puede importar el conjunto de reglas exportado, con el formato de archivo .nwr, a otros servicios de NetWitness Platform, lo cual simplifica la implementación y la configuración de varios servicios.

Procesamiento de reglas

Estos son los principios que rigen el procesamiento de reglas de captura:

- Es posible aplicar varias reglas al Decoder.
- Las reglas de captura se ejecutan una tras otra, en secuencia.
- El procesamiento de reglas se detiene cuando se han procesado todas las reglas o cuando se encuentra una coincidencia con una regla configurada para detener el procesamiento de reglas.
- Se puede usar una regla predeterminada para incluir o excluir todo el tráfico que, de otro modo, no es seleccionado por una regla. Una regla predeterminada, si se usa, se debe ubicar al final de la lista de reglas. De lo contrario, el procesamiento de reglas se detiene en cuanto se evalúa la regla predeterminada, ya que, por definición, la regla predeterminada selecciona todo el tráfico.
- Cuando el procesamiento de reglas se detiene, la sesión se guarda usando las opciones de sesión y las opciones de depuración configuradas.

Guía de reglas y consultas

Todas las consultas y las condiciones de regla en los servicios de RSA NetWitness Core deben seguir estas pautas:

Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los números ni las direcciones MAC o IP.

- `extension = 'torrent'`
- `time='2015-jan-01 00:00:00'`
- `service=80`
- `ip.src = 192.168.0.1`

Nota: El espacio a la derecha y a la izquierda de un operador es opcional. Por ejemplo, puede escribir una regla como `service=80` o `service = 80 .`

Ejemplos de reglas

En la siguiente tabla se muestran ejemplos de las condiciones de regla. Puede usar las condiciones de regla para recopilaciones de retención de registros en un Archiver y para las reglas de aplicación, red y correlación en un Decoder, Log Decoder o Concentrator. Las condiciones de regla también se usan en todas las cláusulas `WHERE` de todas las consultas a la base de datos de Core.

Para obtener información detallada sobre la sintaxis de regla en NetWitness Platform, consulte "Cláusulas `WHERE`" en la sección "Consultas" de la *Guía de ajuste de la base de datos de Core*.

Nombre de la regla	Condición
ComplianceDevices	`device.group='PCI Devices' || device.group='HIPPA Devices'`
HighValueWindows	`device.group='Windows Compliance'`
MediumValueWindows	`device.type='winevent_nic' && msg.id='security_4624_security'`
LowValueWinLogs	`device.type='winevent_nic' && msg.id='security_4648_security'`
LowValueProxyLogs	`device.class='proxy' && msg.id='antivirus_license_expired'`
GeneralWindows	`device.type='winevent_nic'`

Reglas no válidas

NetWitness Platform usa un analizador de regla que define estrictamente la sintaxis válida para las reglas y las consultas. Cuando un servicio principal encuentra una sintaxis no válida, escribe una advertencia en los registros de NetWitness Platform que indica el error.

Nota: NetWitness Platform 11.x no es compatible con el análisis de reglas de sintaxis heredadas (como ocurría en la versión 10.6). Después de actualizar a NetWitness Platform 11.x, las reglas con sintaxis no válida se destacan en la interfaz del usuario y no se aplican reglas hasta que se corrigen las reglas no válidas. En el Editor de regla se proporcionan mensajes de globo adicionales. Después de corregir las reglas, los elementos resaltados desaparecen. Consulte Corregir las reglas con sintaxis no válida.

Las estadísticas `/decoder/config/rules/rule.errors` y `/concentrator/config/rules/rule.errors` contienen el conteo de reglas con errores. Si `rule.errors` es distinto de cero, NetWitness Platform genera una alerta de Estado y condición para indicar que debe corregir las reglas.

Reglas de sintaxis generales

- En todos los valores de texto, los valores literales deben ir entre comillas. Ejemplo: `username = 'user1'`
- Las comillas pueden ser simples o dobles; pero deben coincidir. (no puede comenzar con comillas simples y terminar con comillas dobles).

- Si el valor literal incluye una comilla, puede anteponerle un carácter de escape (mediante una barra invertida) o usar un carácter de comillas iniciales diferente. Los dos ejemplos siguientes son válidos:
  `username = "User's",username = 'User\'s'`

Las siguientes son reglas de sintaxis válida:

- Para usar una barra invertida en una cadena literal, antepóngale un carácter de escape de barra invertida adicional: `\`
- Todos los valores de hora deben usar comillas para las fechas en este formato:
  `time = 'YYYY-MM-DD HH:MM:SS'`
- Todos los valores de hora que representan la cantidad de segundos transcurridos desde EPOCH (1.º de enero de 1970) no deben ir entre comillas.
  Ejemplo: `time = 1448034064`
- **Todo** lo demás no lleva comillas: direcciones IP, direcciones MAC, valores numéricos, etc. Ejemplo:
  `service = 80 && ip.src = 192.168.1.1/16`

Sintaxis de reglas de captura

Las reglas de captura comparan campos con valores o con otros campos. Este es un ejemplo de una expresión simple con una clave de metadatos en el lado izquierdo del operador y un valor en el lado derecho.

```
ip.dst=192.168.1.1
```

La sintaxis permite una clave de metadatos en el lado derecho del operador en Decoders y Log Decoders para las reglas de aplicación y red. La comparación de claves de metadatos no se aplica en la cláusula `where` en las consultas. Este es un ejemplo de una expresión simple con una clave de metadatos en el lado izquierdo del operador y una clave de metadatos en el lado derecho.

```
ip.src=ip.dst
```

Las reglas que incluyen una comparación de claves de metadatos admiten claves de metadatos cuyo nombre ha cambiado; si una regla realiza una consulta de una clave de metadatos cuyo nombre ha cambiado, se analiza la regla para la clave de metadatos a la cual se cambió el nombre. Por ejemplo, si en una regla se usa la clave de metadatos `ip_dst`, se mapea de manera transparente a la clave de metadatos cuyo nombre ha cambiado: `ip.dst`. Las reglas existentes que contienen claves originales activarán las alertas que incluyen datos para la clave de metadatos cuyo nombre ha cambiado.

Este es un ejemplo de una regla que busca paquetes que tienen la misma dirección `ip.src` y la dirección `ip.dst` en un Decoder, y genera una alerta en el Concentrator.

```
alert=alert.id name=testRule8 rule="ip.src=ip.dst" order=38
```

Esta regla generará un error debido a que `eth.src` y `ip.src` son formatos incompatibles.

```
rule="eth.src=ip.src" name="testRule99" alert=alert.id
```

Los valores se pueden expresar como valores discretos, un rango de valores, un límite superior o inferior o una combinación de estos tres. Puede crear una comparación mayor que o menor que y probar la igualdad o la desigualdad contra un rango de valores o un límite superior/inferior.

`key 0-5` (un rango de valores)

`key = 0-u` es igual que `key >= 0` (límite superior, mayor o igual)

En la siguiente tabla se resumen los operadores de claves de metadatos.

Formato de operando de la izquierda	Operador	Formato de operando de la derecha	Descripción
cualquiera	=	compatible con el operando de la izquierda	Operador de igualdad. Puede usar valores o claves de metadatos en el lado derecho del operador de igualdad.
cualquiera	!=	compatible con el operando de la izquierda	Operador de desigualdad. Puede usar valores o claves de metadatos en el lado derecho del operador de desigualdad.
cualquiera	<	compatible con el operando de la izquierda	Operador Menor que. Puede usar valores o claves de metadatos en el lado derecho de este operador.
cualquiera	<=	compatible con el operando de la izquierda	Operador Menor o igual que. Puede usar valores o claves de metadatos en el lado derecho de este operador.
cualquiera	>	compatible con el operando de la izquierda	Operador Mayor que. Puede usar valores o claves de metadatos en el lado derecho de este operador.
cualquiera	>=	compatible con el operando de la izquierda	Operador Mayor o igual que. Puede usar valores o claves de metadatos en el lado derecho de este operador.
texto	contains	texto	Buscar valores que contengan el operando de la derecha. Puede usar valores o claves de metadatos en el lado derecho de este operador.
texto	begins	texto	Buscar valores que comienzan con el operando de la derecha. Puede usar valores o claves de metadatos en el lado derecho de este operador.
texto	ends	texto	Buscar valores que terminan con el operando de la derecha. Puede usar valores o claves de metadatos en el lado derecho de este operador.
texto	length	entero	Buscar cadenas de cierta longitud. Puede usar valores o claves de metadatos en el lado derecho de este operador.

Formato de operando de la izquierda	Operador	Formato de operando de la derecha	Descripción
cualquiera	`count`	entero	Buscar valores con una cantidad específica de apariciones dentro de la sesión. Puede usar valores o claves de metadatos en el lado derecho de este operador.
cualquiera	`ucount` y `unique`	entero	Busca una cantidad de valores que ocurren de forma única. Puede usar valores o claves de metadatos en el lado derecho de este operador. Por ejemplo, si los resultados incluyen instancias de una clave de metadatos con cinco valores únicos y tres del mismo valor, `ucount` es seis.
N/D	`exists`	cualquiera	Encuentra todos los valores para la clave de metadatos. Puede usar valores o claves de metadatos en el lado derecho de este operador.
N/D	`!exists`	cualquiera	Busca todas las sesiones en la que la clave de metadatos no se produce. Puede usar valores o claves de metadatos en el lado derecho de este operador.
texto	`regex`	texto	Busca valores que coinciden con una expresión regular. Puede usar valores en el lado derecho de este operador.

En la siguiente tabla se resumen otros elementos de la sintaxis que se usan en las reglas.

Elemento de sintaxis	Descripción
*	Regla predeterminada Con el uso de un asterisco (*) como el único carácter de una regla, esa regla seleccionará todo el tráfico.
`u`	Límite superior de un rango de horas, direcciones IP o formatos numéricos. Por ejemplo, para seleccionar todos los puertos TCP sobre 40000, la sintaxis sería: `tcp.port = 40000-u`
`l`	Límite inferior de un rango de horas, direcciones IP o valore numéricos. Por ejemplo, para seleccionar todos los puertos TCP por debajo de 40000, la sintaxis sería: `tcp.port = l-40000`
- (guion)	Denota un rango. Esto solo es aplicable a valores de hora, direcciones IP o MAC o valores numéricos. Separe los límites inferiores y superiores del rango con un carácter de guion (-). Por ejemplo, para seleccionar los puertos TCP entre 25 y 443, la sintaxis sería: `tcp.port = 25-443`

Elemento de sintaxis	Descripción
, (coma)	Denota una lista de rangos o valores o claves de metadatos. Se pueden usar valores únicos, así como cualquier combinación de rangos y límites superiores o inferiores. En una lista se pueden usar claves de metadatos únicas. Las claves de metadatos y los valores literales no pueden aparecer en el lado derecho de un operador. Por ejemplo, la siguiente sintaxis es válida: `tcp.port = 1-10,25,110,143-225,40000-u`
( )	Operador de agrupación. Una expresión se puede incluir entre paréntesis para crear una nueva expresión lógica. Por ejemplo, lo siguiente seleccionaría el tráfico en el puerto 80 hacia/desde 192.168.1.1 O el tráfico en el puerto 443 hacia/desde 10.10.10.1: `(ip.addr=192.168.1.1 && tcp.port=80) || (ip.addr=10.10.10.1 && tcp.port=443)`
~	Operador NOT lógico, una negación de una expresión.
&&	Operador AND lógico, un conjunto de dos expresiones.
||	Operador OR lógico, una disyunción de dos expresiones.

Configurar reglas de captura

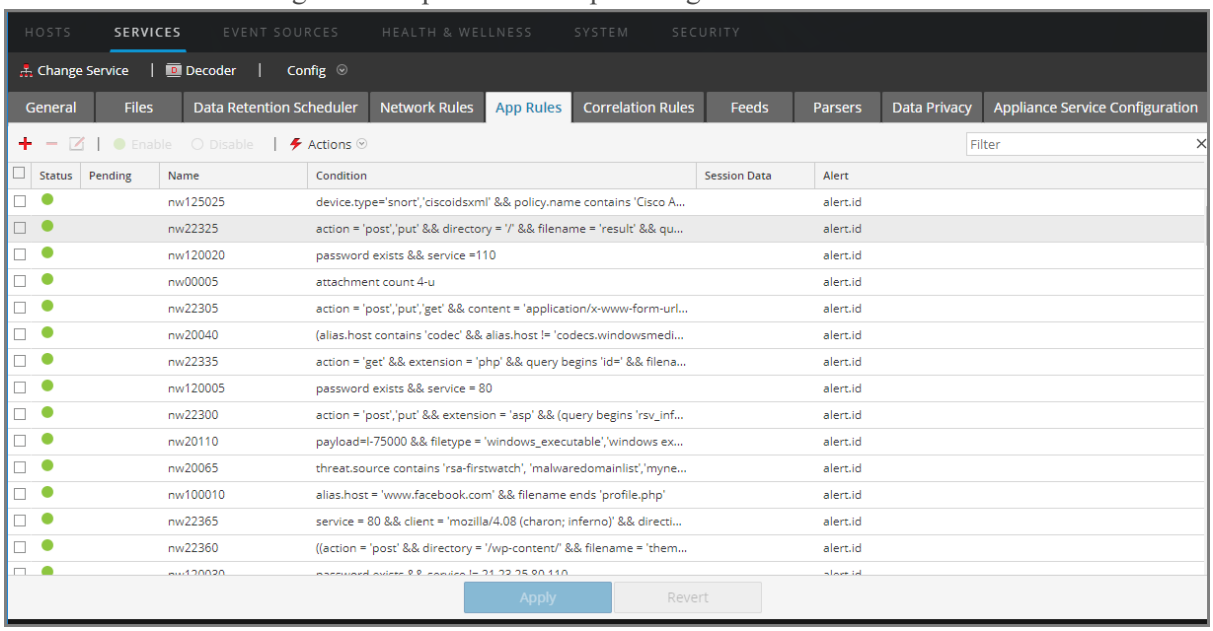
Las reglas de Decoder y Log Decoder se pueden editar en la vista Configuración de servicios. A pesar de que cada tipo de regla (red, aplicación y correlación) tiene su propia pestaña, las funciones son similares para todos los tipos de reglas. Puede realizar lo siguiente:

- Agregar, editar y eliminar reglas
- Habilitar e inhabilitar reglas
- Cambiar la secuencia de ejecución de las reglas
- Importar reglas desde un archivo
- Exportar reglas a un archivo
- Migrar reglas a otro servicio
- Revertir o aplicar los cambios en las reglas
- Restaurar una de las últimas diez configuraciones de reglas a partir de una instantánea

Para configurar reglas en las pestañas Reglas

1. Vaya a **ADMINISTRAR > Servicios**.
2. En la vista **Servicios**, seleccione un servicio Decoder y  **> Ver > Configurar**.
3. En la vista **Configuración de servicios**, seleccione una de las pestañas Reglas: Reglas de red, Reglas de aplicación o Reglas de correlación.

Se muestra la lista de reglas correspondiente al tipo de regla seleccionado.



Cada tipo de regla tiene una lista con columnas levemente diferentes y distintos parámetros. Diversas reglas básicas se aplican a todas las actividades de administración de reglas:

- Las reglas se ejecutan en la secuencia de aparición en la lista. Para cambiar la secuencia de ejecución de las reglas, arrastre y suelte las reglas en la ubicación correspondiente de la lista o use las opciones del menú contextual para organizarlas.
- Para seleccionar una única fila, haga clic en ella.
- Para seleccionar un grupo de filas adyacentes, haga clic en la primera fila y, a continuación, mantenga presionada la tecla Mayús y haga clic en la última fila del grupo.
- Para seleccionar varias filas no adyacentes, haga clic en la primera fila y, a continuación, mantenga presionada la tecla Ctrl y haga clic en las demás.
- Cuando edite reglas en la pestaña de reglas, debe aplicar los cambios en la configuración para que se activen.
- Antes de aplicar los cambios, puede descartar las modificaciones de la lista y revertirlas para dejar las reglas sin editar.
- Una vez que aplica las reglas, puede recuperar las últimas diez configuraciones de reglas usando la opción **Historial** en el menú **Acciones**.

Para agregar una regla en cualquier pestaña de reglas, ejecute una de las siguientes acciones:

- Haga clic en + .
- Haga clic con el botón secundario en una regla y seleccione **Insertar arriba** o **Insertar debajo** en el menú contextual.
  Se muestra el cuadro de diálogo Editor de regla para ese tipo de regla.

Para quitar una regla:

1. En cualquier pestaña Reglas, seleccione las reglas que desea quitar de la lista de reglas.
2. Haga clic en .
   Las reglas seleccionadas se quitan de la lista, pero siguen existiendo en el servicio.

Para editar una regla

1. En cualquier pestaña Reglas, seleccione las reglas que desea editar.
2. Haga clic en o doble clic en la fila de la regla.
   Se muestra el cuadro de diálogo Editor de regla para ese tipo de regla.

Para deshabilitar una regla:

1. Desde cualquier pestaña Reglas, seleccione las reglas que desea deshabilitar.
2. Haga clic en Disable.
   El estado cambia a deshabilitado en la lista de reglas, pero la regla sigue habilitada en el servicio.

Para habilitar una regla:

1. Desde cualquier pestaña Reglas, seleccione las reglas que desea habilitar.
2. Haga clic en Enable.
   El estado cambia a habilitado en la lista de reglas, pero la regla sigue deshabilitada en el servicio.

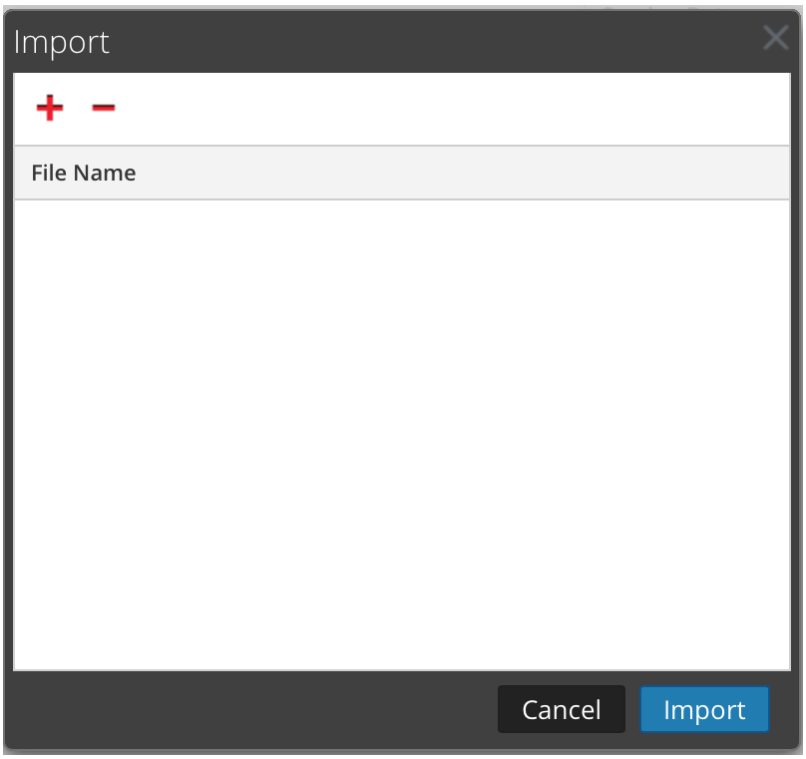
Importar reglas desde un archivo y exportar reglas

Puede importar reglas de red, aplicación y correlación a un Decoder desde un archivo que contiene reglas del mismo tipo. Después de importar las reglas, puede editarlas y administrarlas como lo haría con cualquier otra regla.

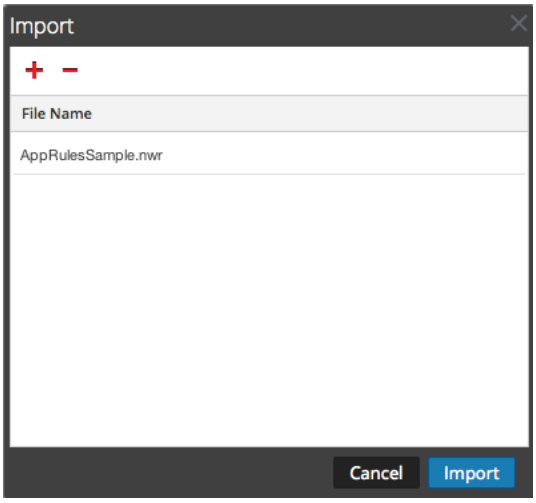
Cuando intenta importar un grupo de reglas, NetWitness Platform Administration comprueba el tipo de reglas importadas. Si lo hace correctamente, aparece un mensaje que indica la cantidad de reglas importadas. Si el tipo de regla es diferente al tipo de pestaña activa, las reglas no se importan. Debe volver a importar las reglas en la pestaña correcta o seleccionar otro archivo para importar.

Para importar reglas a un servicio:

1. En cualquier pestaña Reglas, seleccione Actions > Import.
   Aparece el cuadro de diálogo Importar.



2. Haga clic en +.
   Se muestra una vista de la estructura de directorios.
3. Seleccione uno o más archivos de reglas de NetWitness (.nwr) para importar y haga clic en **Abrir**.
   El archivo se agrega a la lista en el cuadro de diálogo Importar.



4. Haga clic en **Importar**.
   Las reglas se importan a la interfaz del usuario. Las reglas importadas tienen una esquina roja en cada columna editada.
5. Edite o reorganice las reglas si es necesario.
6. Para guardar las reglas en el servicio, haga clic en **Aplicar**.
   Las reglas del servicio se actualizan con los cambios.

Para exportar una regla a un archivo:

1. Para exportar un subconjunto de las reglas, seleccione las reglas que desea exportar.
2. Realice una de las siguientes acciones:
   - En la barra de herramientas, seleccione Actions > **Exportar** > **Selección**. (**Exportar** > **Todo** exporta todas las reglas de la lista de reglas, incluso si tiene seleccionado un subconjunto para exportación).
   - Haga clic con el botón secundario en las reglas seleccionadas y elija **Exportar selección**.

     Se muestra un indicador que solicita el nombre de archivo.
3. Ingrese el nombre de archivo y haga clic en **Exportar**.
   Se descarga el archivo .**nwr**.

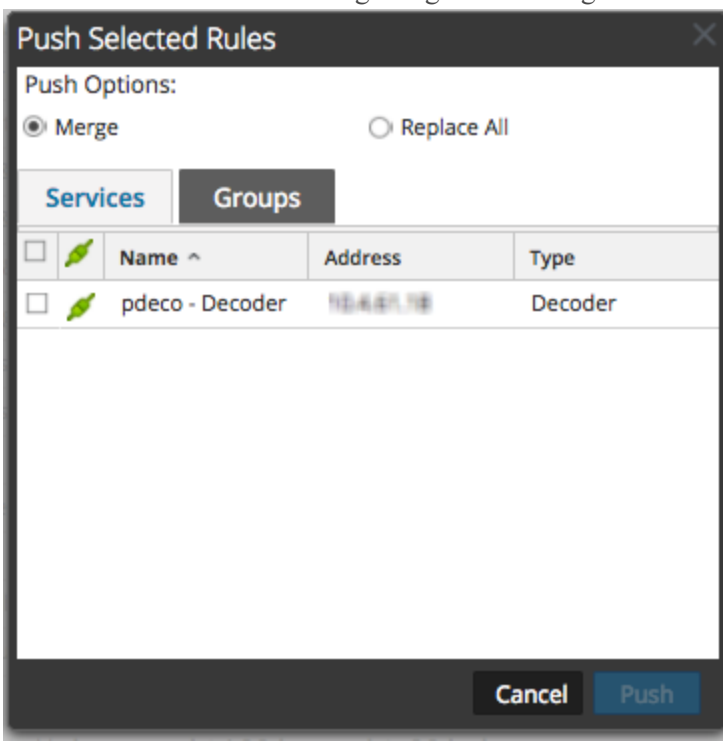
Migrar reglas a otros servicios

Puede aplicar (migrar) las reglas o las reglas seleccionadas a otros servicios (Decoders o Log Decoders) o a grupos de servicios. Cuando migra todas las reglas a otros servicios, todas las reglas de los servicios objetivo se eliminan y se reemplazan por todas las reglas del servicio de origen.

Para migrar las reglas seleccionadas desde este Decoder a otros Decoders:

1. Seleccione la pestaña Reglas y elija las reglas que desea migrar a otro Decoder.
2. Realice una de las siguientes acciones:
   - Seleccione Actions > **Migrar** > **Selección**.
   - Haga clic con el botón secundario en las reglas seleccionadas y elija **Migración de reglas seleccionadas**.

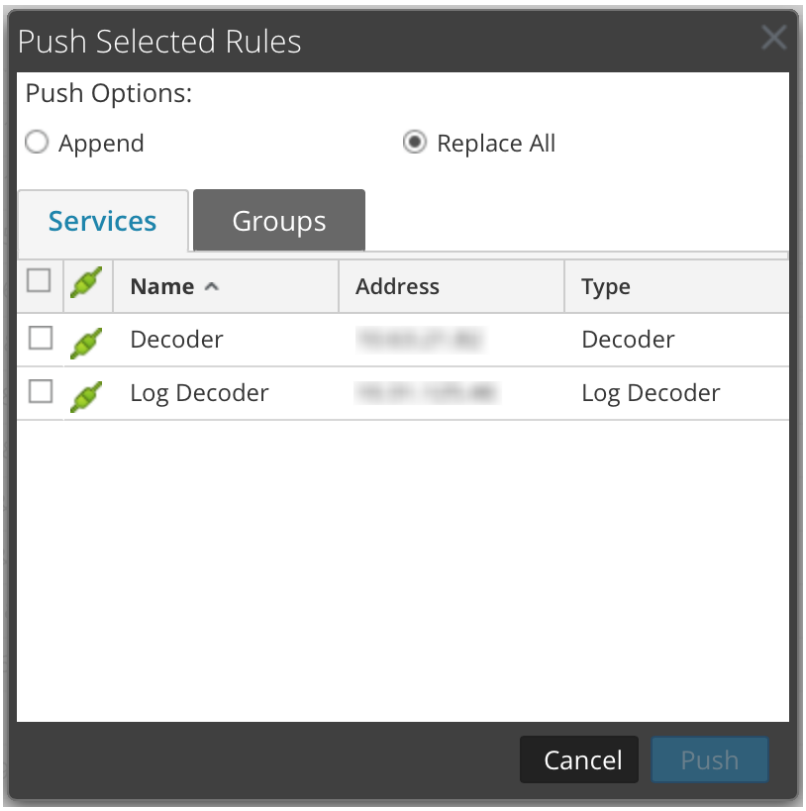
Se muestra el cuadro de diálogo Migración de reglas seleccionadas.



3. Seleccione una opción de migración:
   - Seleccione **Reemplazar todo** para eliminar todas las reglas en los servicios de destino y reemplazarlas por las reglas seleccionadas. Esta opción es la selección predeterminada.
   - Seleccione **Combinar** para combinar las reglas seleccionadas con las reglas existentes en los servicios objetivo.
4. En la pestaña **Servicios**, seleccione los servicios objetivo que recibirán las reglas migradas o seleccione los grupos de servicios en la pestaña **Grupos**.
5. Haga clic en **Migrar**.
   Las reglas se migran a los servicios seleccionados y se aplican de inmediato.

Para migrar todas las reglas desde este Decoder a otros Decoders:

1. En cualquier pestaña Reglas, seleccione Actions > **Migrar** > **Todo**.
   (**Migrar** > **Todo** migra todas las reglas de la lista de reglas, incluso si tiene seleccionado un subconjunto para migración). Se muestra el cuadro de diálogo Migración de reglas seleccionadas.



2. En la pestaña **Servicios**, seleccione los servicios objetivo que recibirán las reglas migradas o seleccione los grupos de servicios en la pestaña **Grupos**.
3. Haga clic en **Migrar**.
   Todas las reglas de los servicios de destino se eliminan y se reemplazan por todas las reglas del servicio de origen. Las reglas se aplican de inmediato.

Cambiar el orden de ejecución de las reglas

Las reglas de captura se aplican en el orden en que aparecen en la lista de reglas. Para reorganizar las reglas, use cualquiera de estos métodos:

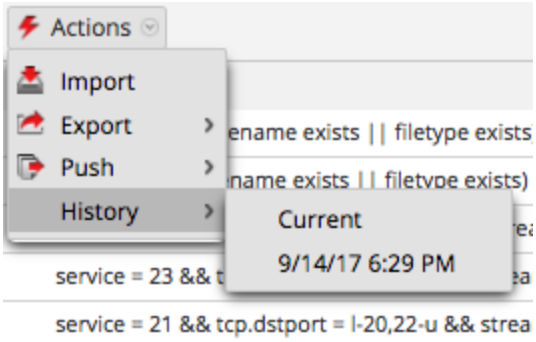
- Arrastre y suelte las reglas en la ubicación deseada de la lista de reglas.
- Haga clic con el botón secundario en una regla para abrir el menú contextual y use las opciones **Cortar** y **Pegar**.

Restaurar la instantánea de una regla desde el Historial

NetWitness Platform mantiene las últimas diez instantáneas de las reglas que se aplican a un servicio.

Para restaurar la instantánea de una regla desde el historial:

1. Seleccione Actions > **Historial**.
   Se muestra un submenú de instantáneas.



2. Seleccione la fecha de la instantánea en el submenú.
   Las reglas de la instantánea se cargan en la lista de reglas y reemplazan al conjunto actual. Sin embargo, el conjunto actual sigue en uso en el servicio.
3. Para aplicar las reglas al servicio, haga clic en **Aplicar**.
   Las reglas se aplican al servicio.

Configurar reglas de aplicaciones

Las reglas de capa de aplicación se aplican en el nivel de la sesión. Los siguientes son ejemplos de reglas de aplicación.

Para truncar paquetes transportados mediante el protocolo de bloque de mensajes del servidor (SMB), cree una regla como la siguiente:

- Nombre de la regla: Truncar SMB
- Condición: `service=139`
- Acción de regla: Truncar todo

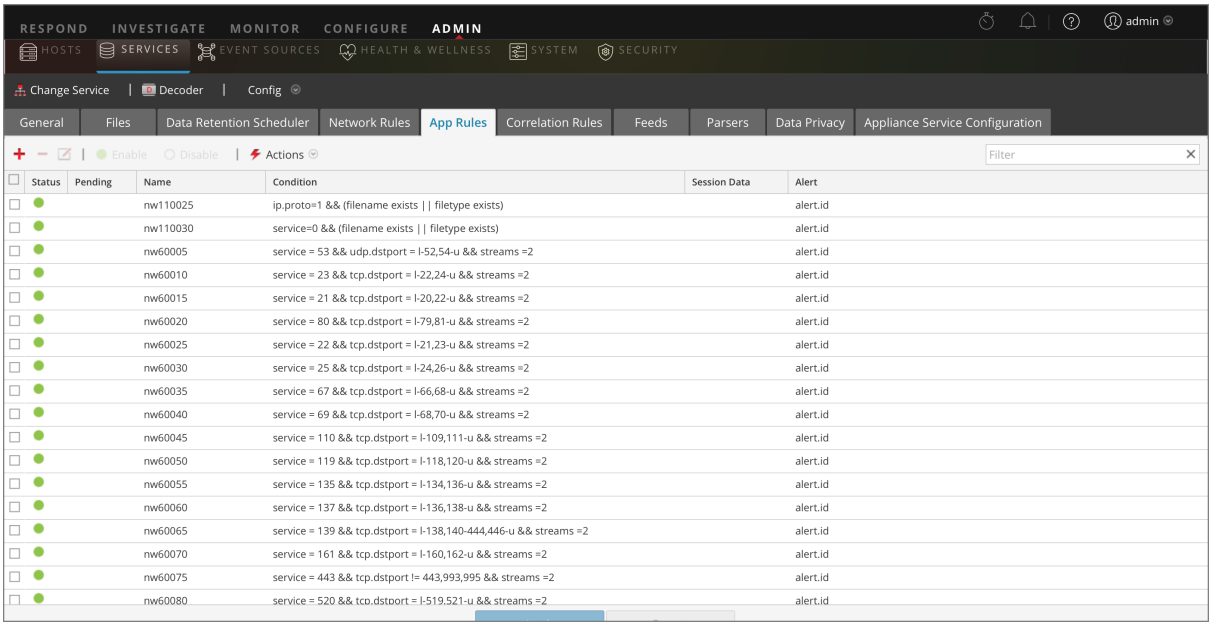
Para conservar correo electrónico hacia y desde una dirección de correo electrónico específica, cree una regla como la siguiente:

- Nombre de la regla: Filtro de correo electrónico Tom Jones
- Condición: `email='Tom.Jones@TheShop.com'`
- Acción de regla: Filtrar

Para agregar o editar una regla de aplicación:

1. Vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio Decoder o Log Decoder y  **> Ver > Configurar**.

   Se muestra la vista Configuración de sistemas del servicio seleccionado.
3. Seleccione la pestaña **Reglas de aplicación**.

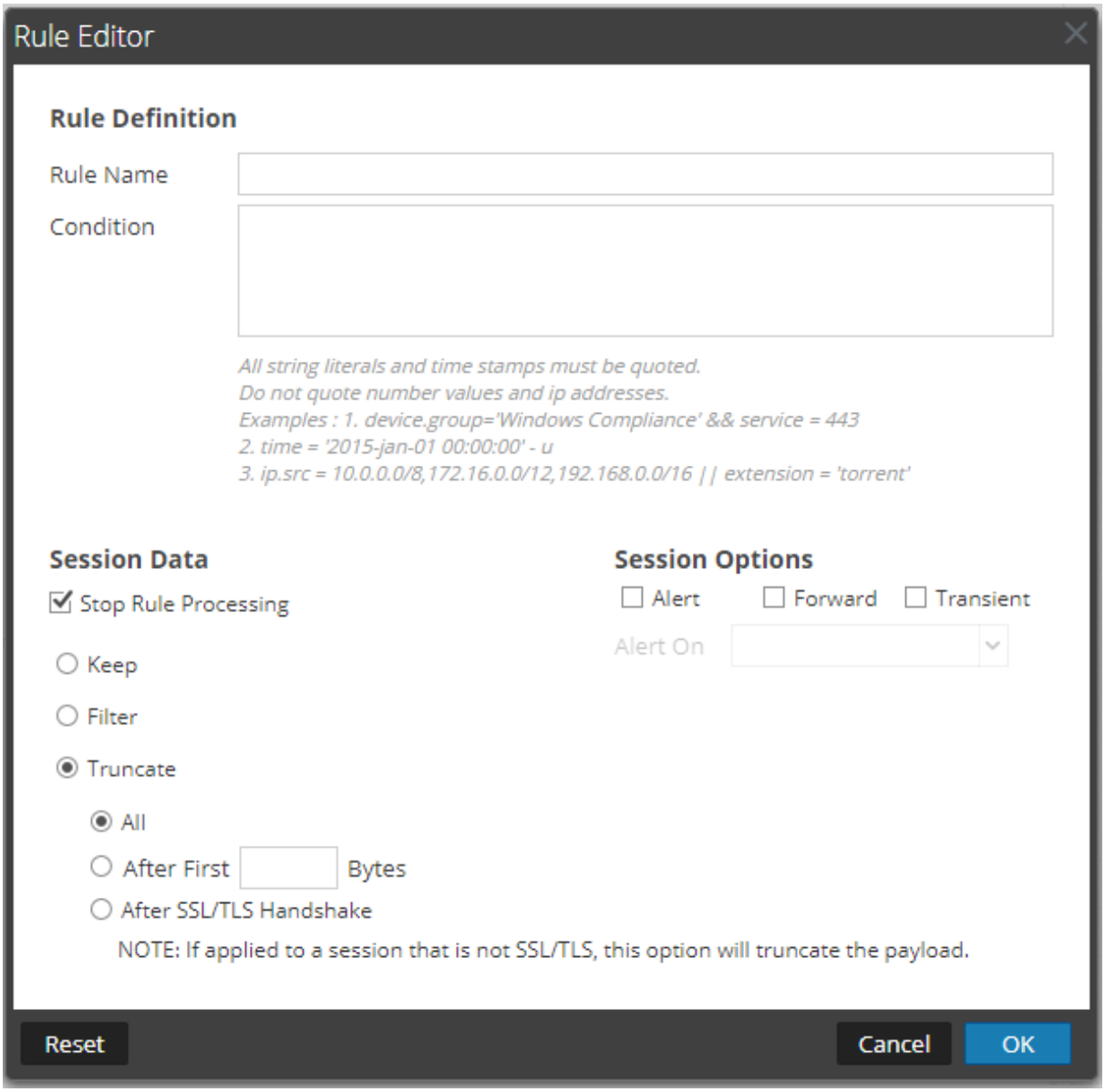


Status	Pending	Name	Condition	Session Data	Alert
		nw110025	ip.proto=1 && (filename exists || filetype exists)		alert.id
		nw110030	service=0 && (filename exists || filetype exists)		alert.id
		nw60005	service = 53 && udp.dstport = l-52,54-u && streams =2		alert.id
		nw60010	service = 23 && tcp.dstport = l-22,24-u && streams =2		alert.id
		nw60015	service = 21 && tcp.dstport = l-20,22-u && streams =2		alert.id
		nw60020	service = 80 && tcp.dstport = l-79,81-u && streams =2		alert.id
		nw60025	service = 22 && tcp.dstport = l-21,23-u && streams =2		alert.id
		nw60030	service = 25 && tcp.dstport = l-24,26-u && streams =2		alert.id
		nw60035	service = 67 && tcp.dstport = l-66,68-u && streams =2		alert.id
		nw60040	service = 69 && tcp.dstport = l-68,70-u && streams =2		alert.id
		nw60045	service = 110 && tcp.dstport = l-109,111-u && streams =2		alert.id
		nw60050	service = 119 && tcp.dstport = l-118,120-u && streams =2		alert.id
		nw60055	service = 135 && tcp.dstport = l-134,136-u && streams =2		alert.id
		nw60060	service = 137 && tcp.dstport = l-136,138-u && streams =2		alert.id
		nw60065	service = 139 && tcp.dstport = l-138,140-444,446-u && streams =2		alert.id
		nw60070	service = 161 && tcp.dstport = l-160,162-u && streams =2		alert.id
		nw60075	service = 443 && tcp.dstport != 443,993,995 && streams =2		alert.id
		nw60080	service = 520 && tcp.dstport = l-519,521-u && streams =2		alert.id

4. Realice una de las siguientes acciones:

- Si desea agregar una regla nueva, haga clic en +.
- Si edita una regla, seleccione la regla en la lista de reglas y haga clic en .

5. Se muestra el cuadro de diálogo Editor de regla con parámetros de reglas de aplicación.



a. En el campo **Nombre de la regla**, escriba un nombre para la regla. Por ejemplo, para crear una regla que trunque todo el tráfico de SMB, escriba **Truncate SMB**.

b. En el campo **Condición**, cree la condición de la regla que desencadena una acción cuando hay una coincidencia. Puede escribir directamente en el campo o crear la condición en él mediante metadatos de las acciones de la ventana. A medida que crea la definición de la regla, NetWitness Platform muestra errores de sintaxis y advertencias. Por ejemplo, para truncar todo el tráfico de SMB, escriba **service=139**.

Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. En Configurar reglas de Decoder se proporcionan detalles adicionales.

c. Si desea que la evaluación de reglas termine con esta regla, marque la casilla de verificación **Detener procesamiento de regla**.

d. En la sección **Datos de sesión**, elija una de las siguientes acciones que se aplicará cuando se encuentre un paquete coincidente:

- **Mantener**: La carga útil del paquete y los metadatos asociados se guardan cuando coinciden con la regla.
- **Filtrar**: El paquete no se guarda cuando coincide con la regla.
- **Truncar**: Seleccione una opción de truncado que se debe ejecutar cuando un paquete coincida con la regla. En el ejemplo se utiliza la opción **Todo**.
- **Truncar todo** para guardar los encabezados del paquete y los metadatos asociados, y no guardar su carga útil.
- **Truncar después de los primeros <n> bytes** para guardar los encabezados del paquete y los metadatos asociados, y no guardar su carga útil después de los primeros <n> bytes especificados, donde <n> es una cantidad de bytes.
- **Truncar el protocolo de enlace SSL/TLS** para truncar la carga útil de todas las sesiones, excepto en el caso de una sesión SSL/TLS, donde el intercambio de SSL se conserva, pero el resto de la carga útil no se guarda. Esta opción se usa con los analizadores SSL.

e. En la sección **Opciones de sesión**, realice cualquiera de las siguientes acciones:

- **Para generar una alerta personalizada** cuando los metadatos de una sesión coincidan con la regla, habilite la marca Alerta y seleccione el nombre de los metadatos de la alerta en la lista desplegable **Alerta en**.
- **Para ejecutar el reenvío de syslog** cuando el registro coincida con la regla, habilite la marca **Reenvío**. Asegúrese de:
  - Haber habilitado las marcas Alerta y Reenvío para realizar el reenvío de syslog.
  - Que el nombre de la regla mencionado en el cuadro de diálogo Editor de regla coincida con el nombre del destino de reenvío de syslog especificado en Log Decoder > Ver > Explorar > parámetro `/decoder/config/logs.forwarding.destination`.
- **Para impedir que los metadatos de la alerta que se crea se escriban en el disco**, habilite la marca **Transitorio**.

6. Para guardar la regla y agregarla a la cuadrícula, haga clic en **Aceptar**.

   La regla se agrega al final de la cuadrícula o se inserta donde especificó en el menú contextual. Se muestra el signo más en la columna **Pendiente**.

7. Verifique que la regla está en la secuencia de ejecución correcta con otras reglas en la cuadrícula. Si es necesario, transfiera la regla.

8. Para aplicar el conjunto de reglas actualizado a Decoder o Log Decoder, haga clic en **Aplicar**.

NetWitness Platform guarda una instantánea de las reglas que se aplican actualmente y, a continuación, aplica el conjunto actualizado a Decoder y quita el indicador de pendiente de las reglas que estaban pendientes.

Monitorear las reglas de aplicación

Decoder y Log Decoder rastrean la cantidad de veces que cada regla de aplicación coincide con una sesión. Estas estadísticas se pueden ver estableciendo una conexión a la vista Explorar de Decoder o Log Decoder y viendo las propiedades en la carpeta `/decoder/config/rules/application`. A continuación, envíe el comando "`statdump`" a esa carpeta. La salida de este mensaje es una lista de la cantidad de veces que hay coincidencias con cada regla de aplicación. Se da a la lista el mismo orden que el del contenido de las definiciones de regla en la carpeta `/decoder/config/rules/application`. Por ejemplo, en un sistema con tres reglas de aplicación:

```
0001: hits=6543 loaded=true
0002: hits=9294 loaded=true
0003: hits=43 loaded=true
```

Los contadores de coincidencias de las reglas de aplicación se restablecen cada vez que se vuelven a cargar los analizadores.

Configurar reglas de correlación

Las reglas de correlación básicas se aplican en el nivel de sesión y advierten al usuario sobre actividades específicas que pueden estar ocurriendo en su ambiente. NetWitness Platform aplica reglas de correlación en una ventana de tiempo móvil configurable. Cuando se cumplen las condiciones, se crean metadatos de alerta para esta actividad y se muestra un indicador visible de la actividad sospechosa.

Los siguientes son ejemplos de reglas de correlación que ilustran dos casos de uso y la sintaxis.

Objetivo: En sesiones en las que exista tcp.dstport, si hay alguna combinación de ip.src e ip.dst donde el conteo de instancias únicas de `tcp.dstport > 5` dentro de 1 minuto, entonces generar una alerta. Para lograr este objetivo, cree una regla como la siguiente:

- Nombre de la regla: Escaneo de puerto TCP vertical IPv6 5
- Regla: `tcp.dstport exists`
- Clave de instancia: `ip.src,ip.dst`
- Umbral: `u_count(tcp.dstport)>5`
- Ventana de tiempo: 1 minuto

Objetivo: En sesiones donde `action==login` y `error==fail`, si hay cualquier combinación de `ip.src` y `ip.dst` que aparezca en más de 10 sesiones dentro de cinco minutos, entonces generar una alerta. Para lograr este objetivo, cree una regla como la siguiente:

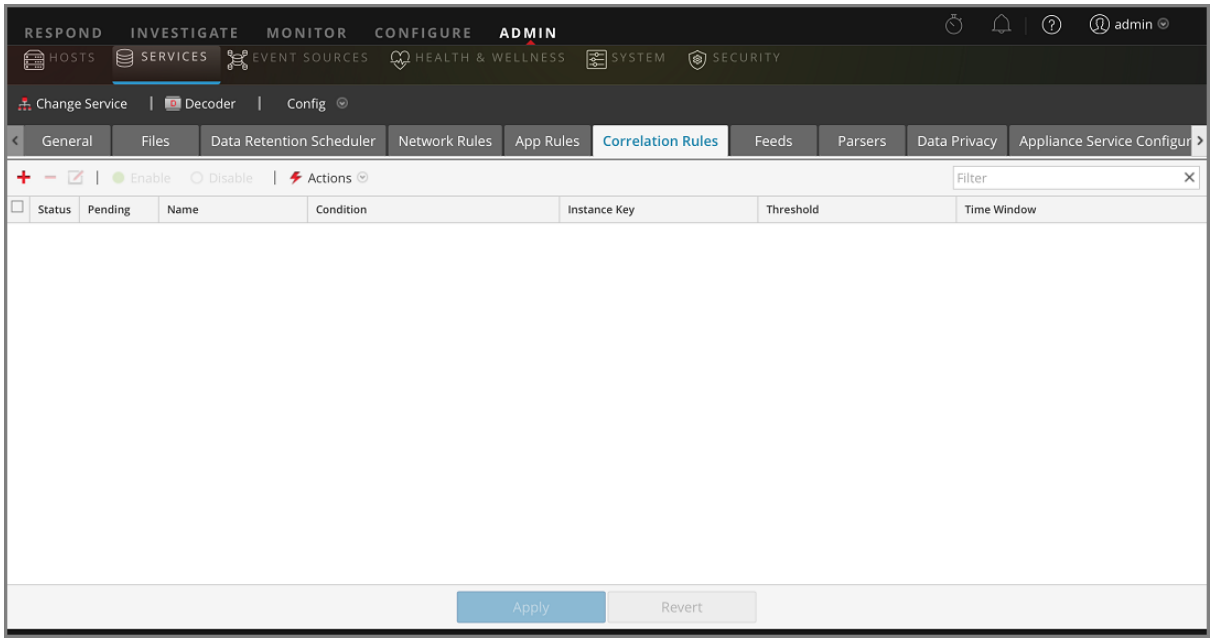
- Nombre de la regla: Fuerza bruta potencia IPv4 10
- Regla: acción=`'login' && error='fail'`
- Clave de instancia: `ip.src,ip.dst`
- Umbral: `count()>10`
- Ventana de tiempo: 5 minutos

Ambos ejemplos de reglas tienen la misma clave de instancia: `ip.src` y `ip.dst`. Dado que se buscan combinaciones únicas de `ip.src` y `ip.dst` que coincidan con la condición de correlación, **`ip.src`** y **`ip.dst`** son **claves primarias**.
El umbral puede incluir una **clave asociada** que identifica el tipo de metadatos que se cuenta para determinar si se cumple la condición. En el primer ejemplo, la clave asociada que se especifica en Umbral es `tcp.dstport`. Se cuentan las instancias únicas de `tcp.dstport` para cada par `ip.src/ip.dst`. En el segundo ejemplo, la clave asociada no se especifica en el umbral porque se trata solamente de un conteo de sesiones. Es útil pensar en este escenario como un conteo de ID de sesión únicos y los metadatos asociados son implícitamente session.id. Se cuentan las `session.id` únicas para cada par `ip.src/ip.dst`.

Caso de uso no válido: En sesiones donde (regla), si hay cualquier combinación de `ip.src` e `ip.dst` que tenga un conteo único de `ipv6.dst > 5` dentro de (ventana de tiempo), entonces generar alerta. Este caso no funciona porque la clave asociada `ipv6.dst` es un tipo de metadatos IPv6. Los tipos de metadatos IPv4 e IPv6 no se pueden usar como claves asociadas.

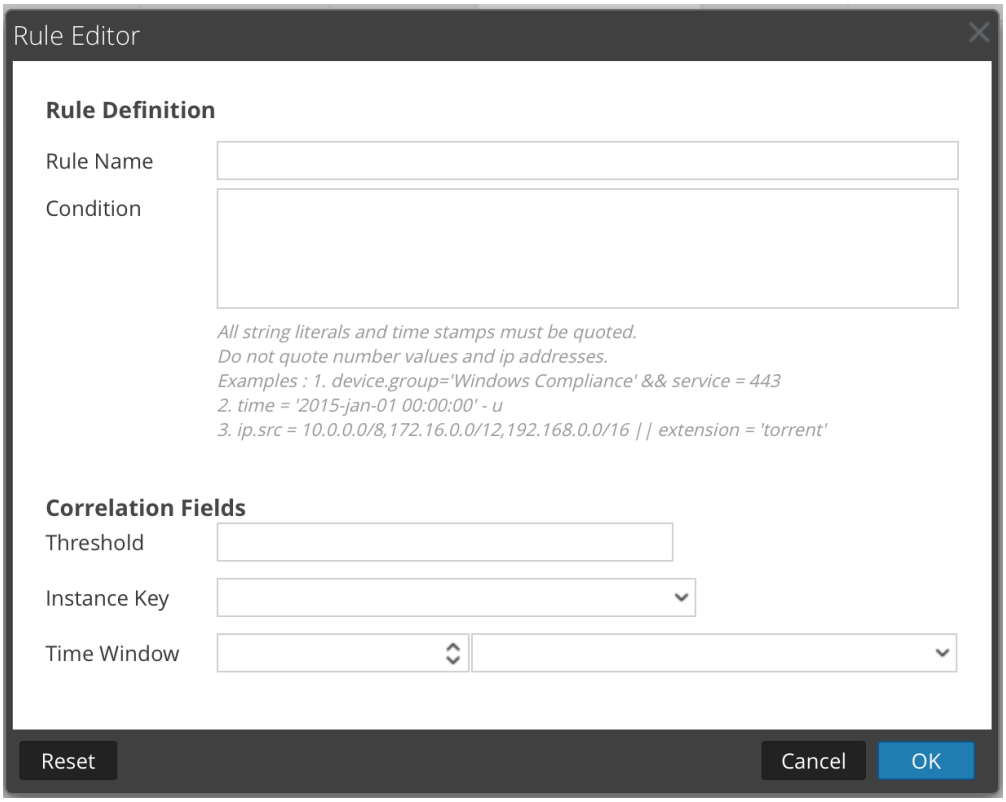
Para agregar o editar una regla de correlación

1. Vaya a **ADMIN > Servicios**, seleccione un servicio y > **Ver > Configuración**.
   Se muestra la vista Configuración de servicios del servicio seleccionado.
2. Seleccione la pestaña **Reglas de correlación**.



3. En la pestaña **Reglas de correlación**, realice una de las siguientes acciones:
   - Si desea agregar una regla nueva, haga clic en .

- Si edita una regla, selecciónela en la cuadrícula de reglas y haga clic en .
  Se muestra el cuadro de diálogo Editor de regla con los parámetros de reglas de correlación.



4. En el campo **Nombre de la regla**, escriba un nombre para la regla. Por ejemplo, para crear la regla de muestra, **Escaneo de puerto TCP vertical IPv6 5**.
5. En el campo **Condición**, cree la condición de la regla que desencadena una acción cuando hay una coincidencia. Puede escribir directamente en el campo o crear la condición en él mediante metadatos de las acciones de la ventana. A medida que crea la definición de la regla, NetWitness Platform muestra errores de sintaxis y advertencias. Por ejemplo, para crear la regla de muestra, escriba **tcp.dstport exists**. Cuando esta condición se cumpla, se ejecutará la acción de los datos de sesión. Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. En Configurar reglas de Decoder se proporcionan detalles adicionales.
6. En el campo **Umbral**, use uno de los parámetros de umbral para especificar la cantidad mínima de apariciones que se necesitan para crear una sesión de correlación y una clave asociada, si es necesario. La clave asociada no puede ser un tipo de metadatos IPv4 o IPv6.
   - `u_count(associated_key)` = el conteo de valores únicos de la clave especificada
   - `sum(associated_key)` = los valores de la clave especificada
   - `count` = cantidad de sesiones (no se especifica ninguna clave asociada)
7. En el campo **Clave de instancia**, seleccione el indicador de destino en el cual basar el evento. Puede ser una sola clave o una clave compuesta (dos claves principales, separadas por una coma).

8. En **Ventana de tiempo**, defina el periodo durante el cual el umbral se debe alcanzar para crear una sesión de correlación.
9. Para guardar la regla y agregarla a la cuadrícula, haga clic en **Aceptar**.
   La regla se agrega al final de la cuadrícula o se inserta donde especificó en el menú contextual. Se muestra el signo más en la columna **Pendiente**.
10. Verifique que la regla está en la secuencia de ejecución correcta con otras reglas en la cuadrícula. Si es necesario, transfiera la regla.
11. Para aplicar el conjunto de reglas actualizadas al servicio, haga clic en **Aplicar**.
    NetWitness Platform guarda una instantánea de las reglas aplicadas actualmente, a continuación, aplica el conjunto actualizado al Decoder o Log Decoder.

Configurar reglas de red

Las reglas de red se aplican en el nivel de paquete en un Decoder y se componen de conjuntos de reglas de Capa 2, Capa 3 y Capa 4. Es posible aplicar varias reglas en el nivel de paquete a un Decoder. Las reglas de red se pueden aplicar a varias capas de red (por ejemplo, cuando una regla de red filtra puertos específicos de una dirección IP específica). Las reglas de red no se aplican a Log Decoders, solamente se aplican a Network Decoders.

Puede crear y administrar reglas de red en la vista Configuración de servicios > pestaña Reglas de red.

Claves de metadatos compatibles en condiciones de reglas de red

En la siguiente tabla se describen las claves de metadatos compatibles con NetWitness Platform que se pueden usar en condiciones de reglas de red.

Clave de metadatos	Descripción
eth.addr	Dirección de origen o destino de Ethernet. Comúnmente se conoce como la dirección MAC.
eth.dst	Dirección Ethernet de destino. Es lo mismo que el campo de dirección Ethernet, excepto que solo selecciona paquetes en los cuales la dirección de destino coincide con los valores seleccionados.
eth.src	Es lo mismo que el destino de Ethernet, excepto que se centra en la dirección de origen.
eth.type	Tipo de trama Ethernet.
hdlc.type	Tipo de la trama HDLC.
ip.addr	Dirección IPv4 de origen o destino en formato estándar. Las direcciones IP se pueden ingresar en notación CIDR para las subredes.
ip.dst	Dirección IPv4 de destino en formato estándar. Las direcciones IP se pueden ingresar en notación CIDR para las subredes.
ip.proto	Campo de protocolo IPv4.
ip.src	Dirección IPv4 de origen en formato estándar. Las direcciones IP se pueden ingresar en notación CIDR para las subredes.
ipv6.addr	Dirección IPv6 de origen o destino en formato hexadecimal. Por lo general, las direcciones IPv6 se escriben como ocho grupos de cuatro dígitos hexadecimales, lo cual expresa la longitud de la dirección de 128 bits completa. Es compatible con la notación para representar múltiples bloques de 0000 en una dirección. No es compatible con la notación CIDR.
ipv6.dst	Dirección IPv6 de destino en formato hexadecimal.

Clave de metadatos	Descripción
ipv6.proto	Campo de protocolo IPv6. Esto se mapea al campo Encabezado siguiente en el encabezado de IPv6 y usa los mismos valores que el campo de protocolo IPv4.
ipv6.src	Dirección IPv6 de origen en formato hexadecimal.
tcp.dstport	Puerto TCP de destino.
tcp.port	Puerto TCP de origen o destino.
tcp.srcport	Puerto TCP de origen.
udp.dstport	Puerto UDP de destino.
udp.port	Puerto UDP de origen o destino.
udp.srcport	Puerto UDP de origen.

Los siguientes son ejemplos de reglas de red.

Para truncar todo SSL del puerto de origen, cree una regla como la siguiente:

- Nombre de la regla: Truncar SSL
- Condición: `tcp.srcport=443`
- Acción de regla: Truncar

Para filtrar el tráfico de subred, cree una regla como la siguiente:

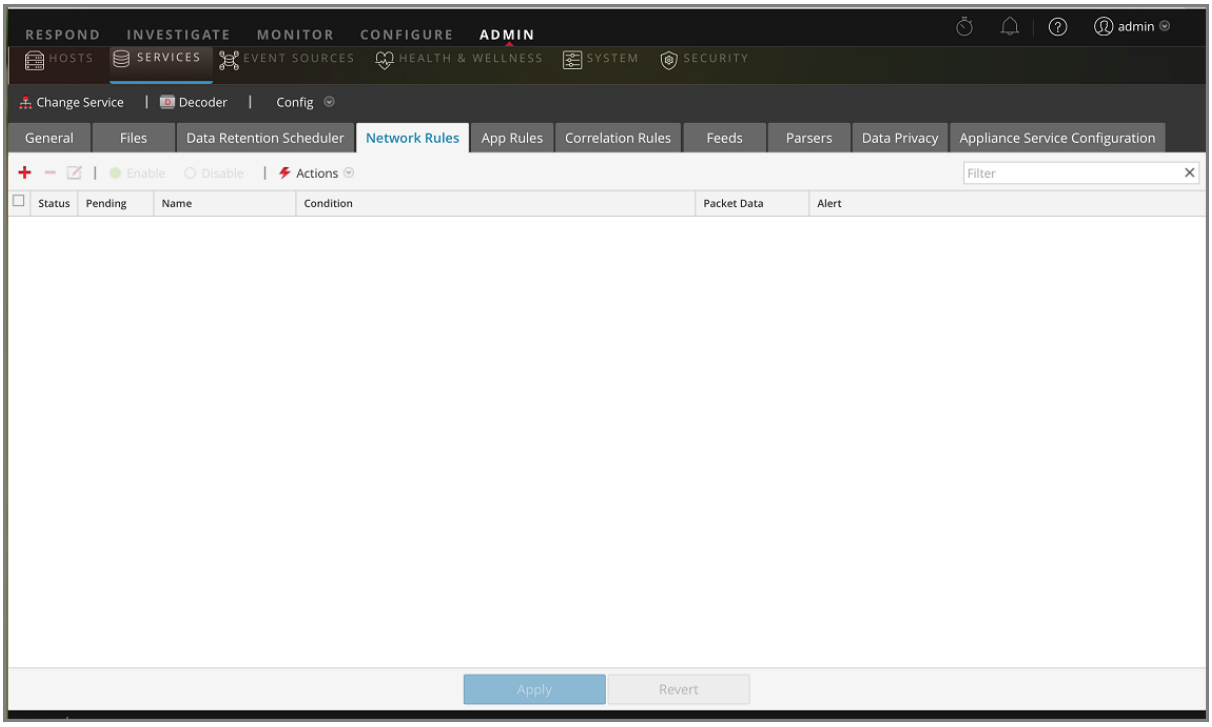
- Nombre de la regla: Filtro de subred
- Condición: `ip.addr=192.168.2.0/24`
- Acción de regla: Filtrar

Las entidades de metadatos, que proporcionan una manera de trabajar con varias claves de metadatos al mismo tiempo, se pueden usar en reglas de aplicación, pero no son compatibles en reglas de red, ya que los metadatos disponibles son demasiado limitados. Para obtener más información sobre las entidades de metadatos, consulte la *Guía de ajuste de la base de datos de Core*.

Para agregar o editar una regla de red:

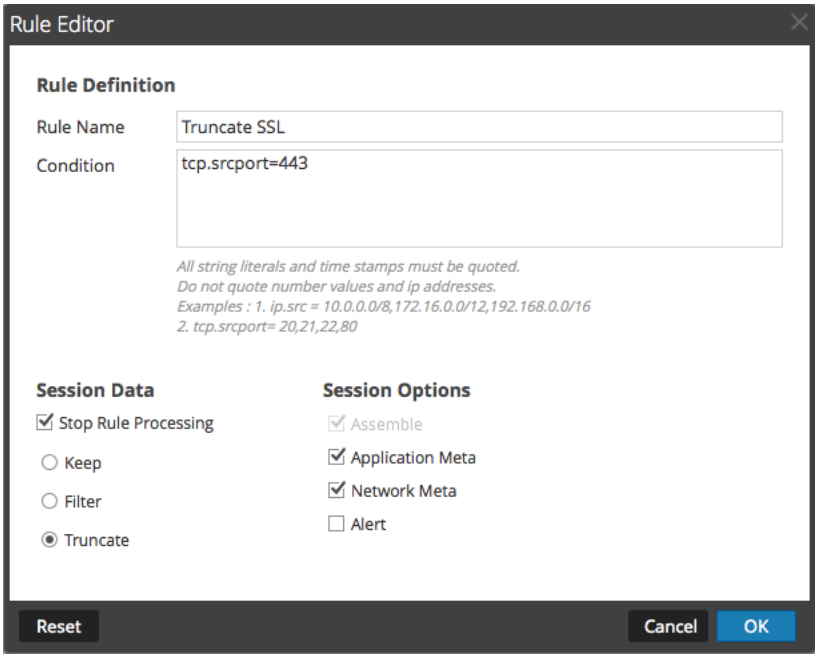
1. Vaya a **ADMIN > Servicios**, seleccione un servicio de Decoder y  **> Ver > Configuración**.
   Se muestra la vista Configuración de Servicios del servicio seleccionado.

2. Seleccione la pestaña **Reglas de red**.
   Se abre la pestaña Reglas de red.



3. En la pestaña **Reglas de red**, realice una de las siguientes acciones:

   - Si desea agregar una regla nueva, haga clic en  .
   - Si edita una regla, selecciónela en la lista de reglas y haga clic en  .
     Se muestra el cuadro de diálogo Editor de regla.



4. En el campo **Nombre de la regla**, escriba un nombre para la regla. Por ejemplo, en el caso de una regla que trunca todo SSL desde el puerto de origen, escriba **Truncar SSL**.
5. En el campo **Condición**, cree la condición de la regla que desencadena una acción cuando hay una coincidencia. Puede escribir directamente en el campo o crear la condición en él mediante metadatos de las acciones de la ventana. A medida que crea la definición de la regla, NetWitness Platform muestra errores de sintaxis y advertencias. Por ejemplo, para truncar todo SSL desde el puerto de origen, `tcp.srcport=443`.
   Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. En Configurar reglas de Decoder se proporcionan detalles adicionales.Claves de metadatos compatibles en condiciones de reglas de red describe las claves de metadatos que admite NetWitness Platform para usarlas en condiciones de reglas de red.
6. Si desea que la evaluación de reglas termine con esta regla, seleccione la casilla de verificación **Detener procesamiento de regla**.
7. En la sección **Datos de sesión**, elija una de las siguientes acciones que se aplicará cuando se encuentre un paquete coincidente:
   - **Mantener**: La carga útil del paquete y los metadatos asociados se guardan cuando coinciden con la regla.
   - **Filtrar**: El paquete no se guarda cuando coincide con la regla.
   - **Truncar**: La carga útil del paquete no se guarda cuando coincide con la regla, pero los encabezados del paquete y los metadatos asociados se mantienen.

8. En la sección **Opciones de sesión**, seleccione todas las opciones que se apliquen de estas cuatro.
   - **Ensamblaje**: El ensamblador ensambla la cadena de paquetes cuando coincide con la regla.
   - **Metadatos de red:** El paquete genera metadatos de red cuando coincide con la regla.
   - **Metadatos de aplicación**: El paquete genera metadatos de aplicación cuando coincide con la regla.
   - **Alerta**: El paquete genera una alerta personalizada cuando los metadatos coinciden con la regla.

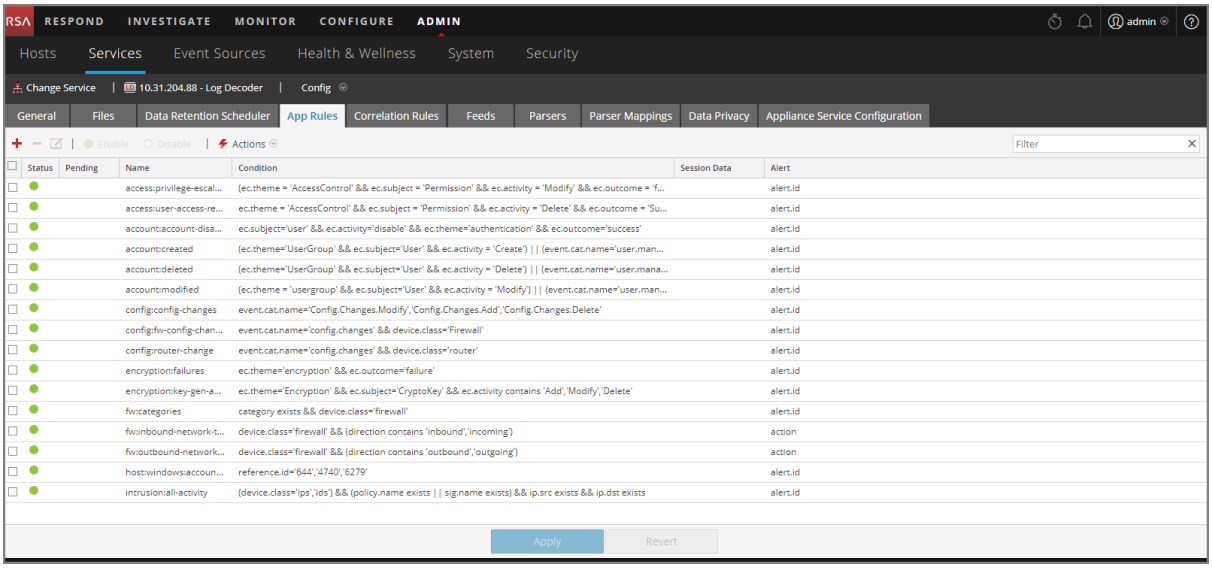
9. Para guardar la regla y agregarla a la lista de reglas, haga clic en **Aceptar**.
   La regla se agrega al final de la lista o se inserta donde especificó en el menú contextual.
10. Verifique que la regla está en la secuencia de ejecución correcta con otras reglas de la lista. Si es necesario, transfiera la regla.
11. Para aplicar el conjunto de reglas actualizadas al Decoder, haga clic en **Aplicar**.
    NetWitness Platform guarda una instantánea de las reglas aplicadas actualmente, a continuación, aplica el conjunto actualizado al Decoder y quita el indicador de pendiente de las reglas que estaban pendientes.

Corregir las reglas con sintaxis no válida

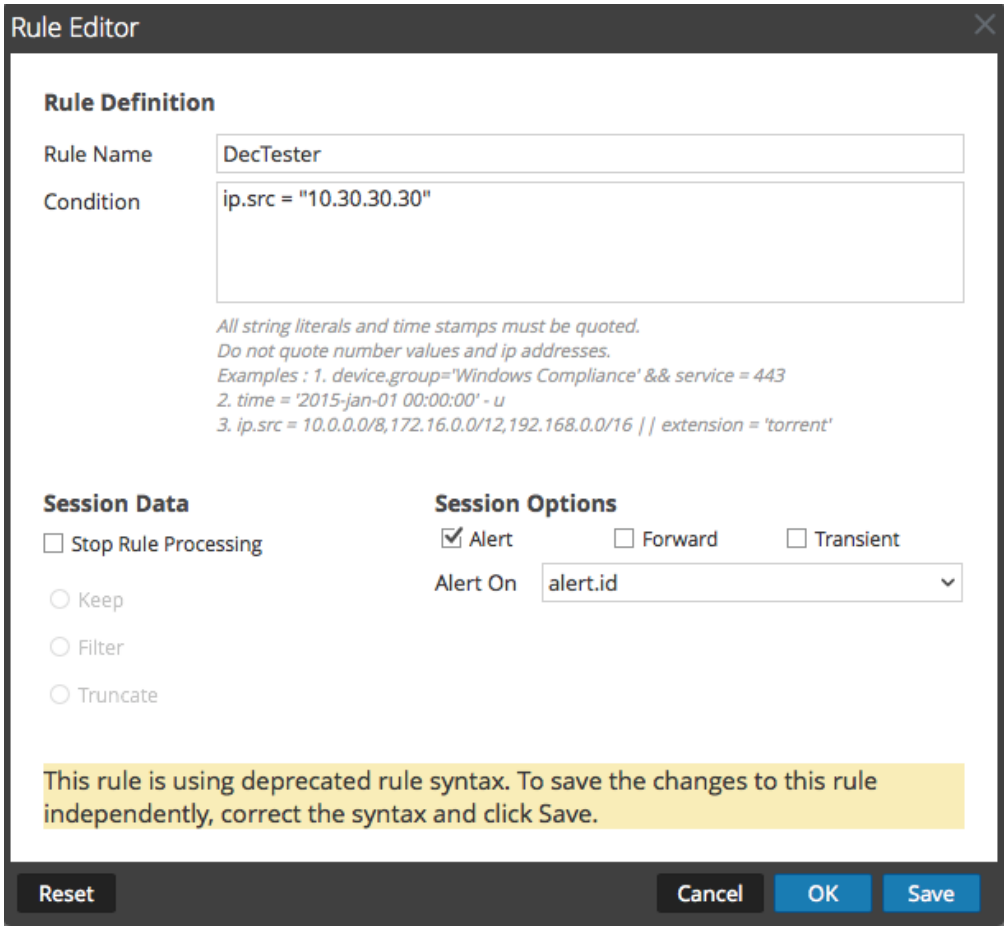
Después de una actualización a NetWitness Platform 11.x, la interfaz del usuario destaca cualquier regla que tenga una sintaxis no válida. En el Editor de regla se proporcionan mensajes de globo adicionales. Después de corregir las reglas, los elementos resaltados desaparecen. Configurar reglas de Decoder proporciona reglas que deben seguir todas las consultas y las condiciones de regla en NetWitness Platform.

Para corregir las reglas con sintaxis no válida:

1. Vaya a **ADMINISTRAR > Servicios**.
2. En la vista **Servicios**, seleccione un Decoder y elija > **Ver > Configuración**.
3. En la vista **Configuración de servicios**, seleccione una de las pestañas Reglas: Reglas de red, Reglas de aplicación o Reglas de correlación.
   La pestaña Reglas correspondiente al tipo de regla seleccionado muestra la cantidad de reglas que usan sintaxis no válida y las reglas no válidas están resaltadas.



4. Seleccione una regla no válida y haga clic en .
   El Editor de reglas muestra información adicional para la regla no válida e incluye una opción Guardar adicional.



5. En el campo **Condición**, corrija la sintaxis de la regla.
   Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. En Configurar reglas de Decoder se proporcionan detalles adicionales.
   Por ejemplo, si la condición de regla no válida es `ip.src="10.30.30.30"`, corrija la sintaxis mediante la eliminación de las comillas: `ip.src=10.30.30.30`
6. Realice una de las siguientes acciones:
   - Para corregir la regla de forma individual, haga clic en **Guardar**.
     La regla corregida se aplica de manera independiente al Decoder. La regla corregida aparece sin resaltar en la pestaña Reglas.
   - Para corregir la regla y aplicarla al Decoder más adelante con otras reglas, haga clic en **Aceptar**.
     La regla corregida aparece sin resaltar en la pestaña Reglas. La regla no se aplica al Decoder.

Comandos del Decoder para administrar reglas

En la base de datos de NetWitness Core, el árbol de reglas tiene la funcionalidad principal relacionada con la administración de reglas para todos los servicios de Core que tienen reglas: Concentrators, Decoders, Log Decoders y Archivers. A pesar de que puede administrar reglas en la interfaz del usuario de NetWitness Platform, es probable que los usuarios avanzados prefieran administrar reglas mediante una línea de comandos para agregar, combinar, reemplazar, eliminar y validar reglas en un servicio. Esta sección proporciona una breve descripción general de los comandos y su uso. Estos son los comandos disponibles:

- `add`: agrega una sola regla en la posición especificada.
- `clear`: elimina todas las reglas existentes en el nodo actual en el servicio. Por ejemplo, el comando en el nodo `/decoder/config/rules/application` elimina todas las reglas de aplicación existentes en el Decoder.
- `delete`: elimina una o más reglas en una posición especificada y el conteo.
- `merge`: combina un conjunto de reglas migrado con un conjunto de reglas existente. Se reemplazan las reglas existentes que coinciden con las reglas entrantes (por nombre o regla); de lo contrario, las reglas se insertan según la posición indicada, como se describe en comando Combinar.
- `replace`: elimina todas las reglas existentes y las reemplaza con el conjunto de reglas entrantes.
- `validate`: valida la sintaxis de una regla, pero no valida las claves de metadatos.

Comando Agregar

El comando `add` agrega la regla al conjunto de reglas existente. El formato es importante debido a que la API usa comillas dobles en el idioma de la regla y también las usa como parámetros en todas las API RSA NetWitness® Platform. Por lo tanto, debe omitir todas las comillas dobles en la regla, para ello comience con un carácter de barra invertida (\). La sintaxis del comando es la siguiente:

```
add rule=<string> name=<string> alert=<string, optional> atPos=<<uint32, optional>
```

- `rule` es la regla para agregar. Asegúrese de colocar todas las reglas con un espacio en blanco entre comillas dobles y de omitir con una barra invertida todas las comillas dobles que forman parte de la regla.
- `name` es el nombre de la regla.
- `alert` es la alerta para la regla (si corresponde).
- `atPos` es la posición en la que se debe agregar la regla (con base 1). Cero es la parte superior de la lista y cualquier número mayor que el tamaño actual de la lista se anexa a ella.

Este es un ejemplo del comando para agregar una regla mediante NwConsole

```
send /decoder/config/rules/application add rule="ip.src exists" order=1
alert=alert.id name=testrule
```

Por ejemplo, considere la siguiente regla:

```
alias.host = "myPC" && country.src="china","russian federation"
```

Para agregar esto como una regla, debe enviar los parámetros siguientes:

```
rule="alias.host = \"myPC\" && country.src=\"china\",\"russian federation\""
name=myRule filter
```

Observe cómo se tuvo que omitir todas las comillas dobles dentro del parámetro de la regla. Un truco simple para que esto sea más legible es usar comillas simples dentro de la regla. Las comillas dobles y simples son intercambiables en la regla y el idioma de consulta, pero no en los parámetros de la API (allí solo se admiten comillas dobles). Por lo tanto, esto es más legible:

```
rule="alias.host = 'myPC' && country.src='china','russian federation'"
name=myRule filter
```

comando Combinar

El comando `merge` se usa para combinar una lista de reglas entrante con las reglas existentes en el servicio. Así es como funciona:

- Encuentra las reglas existentes que coinciden mediante el nombre o por medio de una regla de coincidencia, actualiza el nombre de la regla existente y mantiene la misma posición.
- Inserta las reglas nuevas en la lista de reglas en función de la posición del NÚMERO. Si el número es cero, se dirige a la parte superior de la lista.
- Procesa las reglas en el orden de recepción de modo que, si tiene dos reglas con la numeración de cero, la segunda regla se procesa después de la primera y se asegura el puesto principal. Todas las reglas existentes bajan dos lugares. Cualquier número mayor que las posiciones de regla existentes se agrega después de la última regla existente y se numera en secuencia.
- Cualquier regla sin número se agrega después de la última regla existente y se numera en secuencia.

La sintaxis del comando Combinar es la siguiente:

```
merge --file-data=<string> --file-format<string>
```

- `file-data` es la ruta de acceso completa y el nombre del archivo de reglas para combinar.
- `file-format` es el formato del archivo de reglas. Los valores válidos son `params-list`, `string`, `params`, `binary` y `params-binary`.

Métodos de envío de una lista de reglas a un servicio

Existen dos maneras para enviar una lista de reglas. Puede enviarlas como un archivo `.nwr` (regla de NetWitness) o como un conjunto numerado de parámetros, cada número indica la posición para insertar la regla, además de la regla codificada. Si desea ver la lista de reglas actual en un servicio, debe ejecutar el comando `ls` en la categoría de regla (por ejemplo, las reglas de aplicación en un Decoder se encuentran en `/decoder/config/rules/application`).

Este es un ejemplo de los comandos para listar las reglas existentes mediante NwConsole:

```
login <hostname>:50004 <username> <password>
cd /decoder/config/rules/application
ls
```

Este es otro ejemplo para listar las reglas existentes en NwConsole:

```
send /decoder/config/rules/application ls
```

Este es un ejemplo del comando para apuntar a las reglas de red en el puerto RESTful, que admite una aplicación admin HTML básica.

```
http[s]://<decoder>:50104/decoder/config/rules/network
```

Enviar un archivo de reglas de NetWitness

Comencemos con un ejemplo del archivo nwr, cada regla debe estar en una línea independiente:

```
rule="ip.src=192.168.0.1" name=first keep
rule="ip.src=192.168.1.1" name=second alert=risk.info
rule="ip.src=192.168.2.1" name=third filter
```

Para migrar y combinar reglas mediante NwConsole, use los siguientes comandos:

```
login <hostname>:50004 <username> <password>
send /decoder/config/rules/application merge --file-data=/root/App_
Rules.nwr --file-format=params-list
```

Para reemplazar las reglas existentes con las reglas en el archivo, en lugar de usar el comando merge, use el comando replace.

```
send /decoder/config/rules/application replace --file-
data=<pathname> --file-format=params-list
```

Para combinar las reglas en un archivo nwr mediante el puerto RESTful, puede usar un comando curl que migra las reglas:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-
stream" --data-binary @<pathname> -X POST
"http://<hostname>:50104/decoder/config/rules/application?msg=merge"
```

Los ejemplos tienen relación con la migración de reglas de aplicación. Para migrar reglas de red, envíe las reglas a /decoder/config/rules/network. Para las reglas de correlación, envíe las reglas a /decoder/config/rules/correlation.

Enviar parámetros numerados

La otra manera de enviar una lista de reglas es enviarlas como parámetros numerados. La dificultad de este método es recordar que se deben omitir las comillas dentro de cada regla numerada. Aunque es el único problema si intenta hacerlo manualmente. Por ejemplo, para enviar las mismas reglas anteriores como parámetros a través de NwConsole, use el siguiente comando:

```
send /decoder/config/rules/application merge
1="rule=\"ip.src=192.168.0.1\" name=first keep"
2="rule=\"ip.src=192.168.1.1\" name=second alert=risk.info"
3="rule=\"ip.src=192.168.2.1\" name=third filter"
```

Este comando es difícil de leer porque tiene que omitir las comillas internas con una barra invertida (\). De lo contrario, estos dos comandos realizan lo mismo. Combinar o agregar tres reglas en las posiciones 1, 2 y 3. Si piensa que fue difícil leer lo anterior, el comando curl equivalente se ve así:

```
curl -u "<username>:<password>"
"http://<hostname>:50104/decoder/config/rules/application?msg=merge&1=rule%3D%
22ip.src%3D192.168.0.1%22%20name%3Dfirst%20keep&2=rule%3D%22ip.src%3D192.168.1
.1%22%20name%3Dsecond%20alert%3Drisk.info&3=rule%3D%22ip.src%3D192.168.2.1%22%
20name%3Dthird%20filter"
```

Para obtener más detalles sobre cómo omitir las comillas dobles dentro de los parámetros, consulte Comando Agregar.

Orden de las reglas cuando se migran

Las reglas migradas se ordenan en una de dos maneras. Cuando se pasan como parámetros, el número de cada parámetro determina el orden de inserción. Si no es realmente un número, `merge` comprueba si hay un parámetro `order` dentro de la regla y usa ese valor si se encuentra.

Nota: Usar `order` es la única manera de configurar el orden de un archivo `.nwr`. Si no se encuentra ni un número ni un parámetro `order` , no hay ninguna garantía del orden de inserción.

Ejemplo

Un Decoder tiene las siguientes reglas de aplicación instaladas; observe que SIEMPRE la numeración es consecutiva y comienza en 1:

```
0001 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep
0002 : rule="ip.src=192.168.1.1" name=second alert=risk.info
0003 : rule="ip.src=192.168.2.1" name=third filter
```

Y desea combinar las cuatro reglas siguientes:

```
rule="ip.src=192.168.3.1" name=third keep
rule="ip.dst=192.168.4.1" name=NewRule filter order=0
rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append
rule="service=80,443" name=web filter order=3
```

Use cualquier método para migrar las reglas y el resultado será el siguiente:

```
0001 : rule="ip.dst=192.168.4.1" name=NewRule filter order=1
0002 : rule="ip.src = 192.168.0.1 || ip.dst = 192.168.0.1 || alias.host = 'My-PC'" name=first keep order=2
0003 : rule="service=80,443" name=web filter order=3
0004 : rule="ip.src=192.168.1.1" name=second alert=risk.info order=4
0005 : rule="ip.src=192.168.3.1" name=third keep order=5
0006 : rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=6
```

¿Hay sorpresas aquí? Así es como se procesó cada regla.

`1. rule="ip.src=192.168.3.1" name=third keep`

Esta regla tenía el mismo nombre que una regla existente en el Decoder (tercero). Por lo que la regla actualizó la regla existente, `changing _filter_ to _keep_`.

`2. rule="ip.dst=192.168.4.1" name=NewRule filter order=0`

Esta regla es nueva y tenía `order=0` en ella, lo cual significa que se inserta en la parte superior.

`3. rule="alias.host = 'pc1','pc2'" name=filterTheseNames filter order=append`

Esta regla tenía un valor no numérico `append` para `order`, por lo tanto, quedó al final de la lista. Puede lograr lo mismo con un número grande, como `999999`.

`4. rule="service=80,443" name=web filter order=3`

Esta regla es la última, pero tiene `order=3`, por lo tanto, si no coincide con una regla existente por el nombre o el texto de la regla, se debe colocar en la posición 3. Y ahí la tiene, la tercera regla en la lista. Las reglas que seguían se colocaron más abajo.

Comando Reemplazar

El comando `replace` quita todas las reglas existentes y las reemplaza por la lista de reglas entrantes. Consulte comando Combinar para obtener más información sobre cómo dar formato a la lista de reglas entrantes y cómo funciona el orden.

Este es un ejemplo del comando `replace` con un archivo de regla de NetWitness:

```
send /decoder/config/rules/application replace --file-data=/root/Decoder-AppRules.nwr --file-format=string
```

Este es un ejemplo del comando `replace` mediante parámetros numerados:

```
send /decoder/config/rules/application replace 1="rule=\"ip.src exists\" name=\"test rule\" order=1 alert=alert.id"
```

Comando Borrar

El comando `clear` quita todas las reglas existentes en el servicio. Este es un ejemplo del comando:

```
send /decoder/config/rules/application clear
```

Comando Eliminar

El comando `delete` elimina una o más reglas en el servicio.

```
delete atPos <uint32> count <uint32, optional>
```

- `atPos` elimina la regla en la posición especificada. Las reglas se enumeran empezando por 1 y se ordenan en secuencia.
- `count` elimina una o más reglas comenzando en `atPos`. Este es un parámetro opcional que define la cantidad de reglas para eliminar a partir de `atPos`. El valor predeterminado es 1.

En este ejemplo del comando se eliminan cuatro reglas comenzando en la posición 0003:

```
send /decoder/config/rules/application delete atPos=0003 count=4
```

Comando Validar

El comando `validate` toma la regla proporcionada y verifica que analiza correctamente. Tenga en cuenta que este comando no puede verificar si las claves de idioma y las entidades son válidas.

```
validate rule <string>
```

`rule`: es el nombre de la regla para validar. Asegúrese de que colocar todas las reglas con un espacio en blanco entre comillas dobles.

Configurar feeds y analizadores

Los feeds y los analizadores son responsables de analizar los paquetes y los registros cuando se capturan o se importan en Decoder o Log Decoder. Su uso más común es en la extracción de metadatos estáticos y la identificación de servicios. La definición flexible permite la extensión personalizada de los servicios principales definidos para proporcionar extracción de metadatos e identificación de tipo de servicio adicional. Esto es importante debido al volumen de aplicaciones personalizadas que se utilizan en las redes.

Nota: A menos que se indique lo contrario, todas las referencias a los Decoders se aplican también a los Log Decoders.

Configurar analizadores

NetWitness Platform dispone de un conjunto de analizadores principales definidos por el sistema y también permite agregar analizadores adicionales. Cada analizador se puede configurar en la Vista Configuración de servicios: Pestaña General. El panel Configuración de analizador proporciona una manera de habilitar o inhabilitar el uso de analizadores en el Decoder, además de limitar los metadatos que crea el analizador.

Además, existen varios tipos de analizadores configurables personalizados:

- GeoIP2 o GeoIP: estos analizadores asocian las direcciones IP con ubicaciones geográficas. Para las instalaciones y las actualizaciones nuevas, el analizador GeoIP2 está habilitado de manera predeterminada. Solamente uno de estos analizadores se puede habilitar a la vez. Para obtener más información sobre estos analizadores, consulte Analizadores GeoIP2 y GeoIP.
- Búsqueda: el usuario configura este analizador para generar metadatos mediante el escaneo de palabras clave predefinidas y expresiones regulares.
- FLEXPARSE (obsoleto): este es un lenguaje de definición de analizador genérico para extender la compatibilidad del protocolo de aplicación existente del Decoder. De forma predeterminada este analizador está deshabilitado (consulte Habilitar o deshabilitar los sistemas de análisis Lua y Flex).
- Lua: este analizador se define mediante el lenguaje de script Lua para extender la compatibilidad del protocolo de aplicación existente del Decoder.
- enVision: este analizador de aplicación admite el Log Decoder y está configurado para generar metadatos mediante el escaneo de archivos de registro.
- Snort®: este analizador es compatible con las funcionalidades de detección de carga útil de las reglas IDS de Snort. Las reglas y la configuración de Snort se agregan al directorio `parsers/snort` para Investigation y Decoder (consulte Analizadores Snort).

En la vista Configuración de servicios > pestaña Analizadores, puede ver los analizadores implementados en un Decoder, cargar analizadores y eliminar los analizadores implementados. La interfaz del usuario incluye un indicador si el analizador se originó en Live Services, se instaló a través de NetWitness Platform o se cargó manualmente. Es posible agregar y eliminar analizadores mientras un Decoder está en funcionamiento sin afectar la captura.

Además, puede descargar analizadores mediante NetWitness Platform Live Services.

Configurar feeds

NetWitness Platform utiliza feeds para crear metadatos basados en valores de metadatos definidos de forma externa. Un feed es una lista de datos que se compara con las sesiones a medida que se capturan o procesan. Para cada coincidencia, se crean metadatos adicionales. Estos datos pueden identificar y clasificar direcciones IP maliciosas o incorporar información adicional, como departamento y ubicación según la asignación de redes internas. Algunos ejemplos de feed incluyen feeds de amenazas para identificar BOTNets, mapeos de DHCP o incluso información de Active Directory, como una ubicación física o un departamento lógico.

Puede utilizar el módulo Live en NetWitness Platform para obtener feeds de orígenes externos. El tema "Contenido de Live en NetWitness Platform" en la *guía* de *Administración de servicios de Live* se proporciona una descripción general de la herramienta de administración de contenido de Live.

En la interfaz del usuario de NetWitness Platform, puede ver la lista de feeds implementados actualmente, junto con un indicador de si el feed originado en Live se instaló a través de NetWitness Platform o de forma manual. Puede agregar, eliminar y actualizar feeds, mientras se ejecuta un Decoder, sin afectar la captura.

Hay un asistente Feed personalizado que permite la creación y la implementación de feeds de Decoder personalizados en función de una lógica determinista que ofrece las claves de metadatos específicas para los Decoders y los Log Decoders seleccionados. A pesar de que el asistente guía a los usuarios por el proceso de crear feeds según demanda y recurrentes, es útil comprender la forma y el contenido de un archivo de feed cuando crea un feed.

NetWitness Platform ofrece un asistente Feed personalizado, el cual optimiza la tarea de crear y administrar feeds personalizados, además de completar los feeds en los Decoders y los Log Decoders seleccionados. Además, puede descargar archivos de feed existentes y editarlos, y después editar el feed o crear un feed nuevo con el archivo editado.

Estructura de archivos de definición de feed personalizado

El asistente Feed personalizado de NetWitness Platform permite la creación y la implementación de feeds de Decoder personalizados basados en lógica determinista que ofrece las claves de metadatos específicas para los Decoders y los Log Decoders seleccionados. A pesar de que el asistente guía a los usuarios por el proceso de crear feeds según demanda y recurrentes, es útil comprender la forma y el contenido de un archivo de feed cuando crea un feed.

Los nombres de archivo de feed en RSA NetWitness Platform tienen el formato `<filename>.feed`. Para crear un feed, NetWitness Platform requiere un archivo de datos de feed en el formato `.csv` o `.xml` y un archivo de definición de feed en el formato `.xml`, el cual describe la estructura de un archivo de datos de feed. Con el asistente Feed personalizado, se puede crear un archivo de definición de feed basado en un archivo de datos de feed, o basado en un archivo de datos de feed y el archivo de definición de feed correspondiente.

Los archivos que se utilizan para crear un feed según demanda deben estar almacenados en el sistema de archivos local. Los archivos que se usan para crear un feed recurrente deben estar almacenados en una URL accesible, en la cual NetWitness Platform pueda buscar la versión más reciente del archivo para cada recurrencia. Después de la creación de un feed de NetWitness Platform, puede descargar el feed al sistema de archivos local, editar los archivos de feed y, a continuación, editar el feed de NetWitness Platform para usar los archivos de feed actualizados.

Archivo de definición de feed de muestra

Este es un ejemplo de un archivo de definición de feed denominado `dynamic_dns.xml`, que NetWitness Platform crea en función de las entradas del asistente Feed personalizado. Define la estructura del archivo de datos del feed denominado `dynamic_dns.csv`.

Nota: La ruta de archivo de feed debe ser `.csv` independientemente del Tipo de feed (Valor predeterminado o STIX).

```
<?xml version="1.0" encoding="utf-8"?>
 <FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">

   <FlatFileFeed name="Dynamic DNS Domain Feed"
   path="dynamic_dns.csv"
   separator=","
   comment="#"
   version="1">

   <MetaCallback
   name="alias.host"
   valuetype="Text"
   apptype="0"
   truncdomain="true"/>

   <LanguageKeys>
            <LanguageKey name="threat.source" valuetype="Text" />
            <LanguageKey name="threat.category" valuetype="Text" />
            <LanguageKey name="threat.desc" valuetype="Text" />
   </LanguageKeys>
```

```
    <Fields>
    <Field index="1" type="index" key="alias.host" />
    <Field index="4" type="value" key="threat.desc" />
    <Field index="2" type="value" key="threat.source" />
    <Field index="3" type="value" key="threat.category" />
    </Fields>
    </FlatFileFeed>

</FDF>
```

Equivalentes de definición de feed para los parámetros del asistente Feed personalizado

En el asistente Feed personalizado de NetWitness Platform se proporcionan opciones para definir la estructura del archivo de feed de datos. Esto se corresponde directamente con los atributos en el archivo (.xml) de definición del feed.

Parámetro de NetWitness Platform	Equivalente en el archivo de definición del feed
(Pestaña Definir feed) Tipo de feed	Seleccione: **Valor predeterminado**: para definir un feed basado en un archivo de datos de feed con formato .csv. **STIX**: para definir un feed basado en un archivo .xml con formato STIX.
(Pestaña Definir feed) Tipo de tarea de feed	Seleccione: **Ad hoc**: para crear un feed según demanda. **Recurrente**: para actualizar el archivo .csv o .xml de manera persistente y almacenarlo en una ubicación accesible para NetWitness Platform , de modo que NetWitness Platform descargue un archivo a intervalos regulares y lo inserte en los dispositivos descendentes.
(Pestaña Definir feed) **Nombre**	El nombre del feed personalizado en el archivo de datos del feed. Corresponde al atributo `flatfeedfile name` en el archivo de definición del feed. Por ejemplo, Feed de prueba de DNS dinámico. **Nota:** Ahora puede usar caracteres especiales para definir el nombre del feed personalizado.
(Pestaña Definir feed) **Archivo /Navegar**	Este es el nombre del archivo de datos del feed. Corresponde al atributo `flatfeedfile path` en el archivo de definición del feed. Por ejemplo, `dynamic_dns.csv`.

Parámetro de NetWitness Platform	Equivalente en el archivo de definición del feed
(Pestaña Opciones avanzadas) **Archivo de feed XML**	El nombre del archivo de definición del feed. Por ejemplo, `dynamic_dns.xml`.
(Pestaña Opciones avanzadas) **Separador**	El carácter separador que se utiliza para separar atributos en el archivo de datos del feed. Corresponde al atributo `latfeedfile separator` en el archivo de definición del feed. Por ejemplo, una coma.
(Pestaña Opciones avanzadas) **Comentario**	El carácter que se utiliza para identificar un comentario en el archivo de datos del feed. Corresponde al atributo `flatfeedfile comment` en el archivo de definición del feed. Por ejemplo, `#`.
(Pestaña Definir columnas, Definir índice) **Tipo**	El tipo de valor de búsqueda en la posición del índice del archivo de datos de feed. **IP** significa que cada fila del archivo de datos del feed contiene una dirección IP en la posición del valor de búsqueda. El valor de la dirección IP está en formato de punto decimal (por ejemplo, 10.5.187.42). **Rango de IP** significa que cada columna del archivo de datos de feed contiene un rango de direcciones IP en la posición del valor de búsqueda. El rango de direcciones IP está en formato CIDR (por ejemplo, 192.168.2.0/24). **No IP** significa que cada fila del archivo de datos de feed contiene un valor de metadatos distinto a una dirección IP en la posición del valor de búsqueda. Los campos Tipo de servicio, Truncar dominio y Claves de devolución de llamadas se activan en los índices No IP.
(Pestaña Definir columnas, Definir índice) **CIDR**	Especifica que el valor de la dirección IP en la posición de búsqueda está en formato CIDR. El atributo **CIDR** define el formato de dirección IP del campo en notación Classless Inter-Domain Routing (CIDR).
(Pestaña Definir columnas, Definir índice) **Tipo de servicio**	Para un índice No IP, el tipo de servicio entero para filtrar las búsquedas de metadatos. Corresponde al atributo `MetaCallback apptype` en el archivo de definición del feed. Un valor de `0` indica que no hay filtrado por tipo de servicio.

Parámetro de NetWitness Platform	Equivalente en el archivo de definición del feed
(Pestaña Definir columnas, Definir índice) **Truncar dominio**	Para un índice No IP, en los valores de metadatos que contienen nombres de dominio (por ejemplo, nombres de host), el sistema puede quitar el elemento específico de host en los datos. Truncar dominio corresponde al atributo `MetaCallback truncdomain`. Si el valor es `www.example.com`, se trunca a `example.com`. Con un valor **Falso** se selecciona sin truncamiento y con un valor **Verdadero**, truncamiento.
(Pestaña Definir columnas, Definir índice) **Claves de devolución de llamadas**	En un índice No IP, se pueden seleccionar en la lista desplegable las claves de metadatos disponibles para coincidencia en lugar de ip.src/ip.dst (los valores predeterminados para un tipo de índice IP). Clave de devolución de llamadas corresponde al atributo `MetaCallback name` y la columna de índice del archivo csv debe contener datos que puedan coincidir con la clave de metadatos seleccionada. Por ejemplo, si elige la clave de metadatos de nombre de usuario, la columna de índice del archivo csv debe completarse con los usuarios que se deban hacer coincidir.
(Pestaña Definir columnas, Definir índice) **Columna de índice**	Identifica la columna en el archivo de datos de feed que proporciona el valor de búsqueda para la fila. Cada posición en cada fila del archivo de datos de feed se identifica con un atributo **Field index** en el archivo de definición de feed. Un campo con un índice de **1** es la primera entrada en una fila, el segundo campo tiene un índice de **2**, el tercer campo tiene un índice de **3** y así sucesivamente.
(DEFINIR VALORES) **Clave**	El nombre de `LanguageKey`, según se define en el archivo de definición del feed, para el cual se crean los metadatos a partir de esta fila del archivo de datos del feed. Corresponde al atributo `Field key` en el archivo de definición del feed. Una clave se aplica solamente a un campo cuyo tipo está configurado en `value`. En el archivo de definición del feed, hay una lista de `LanguageKeys` desde `index.xml` o un nombre de resumen si se usan Nombre de fuente y Nombre del destino. Por ejemplo, `reputation` es un nombre de resumen de `reputation.src` y `reputation.dst`. El atributo Field key hace referencia a este valor.

Archivos de ejemplo para un feed MetaCallback con rango de índice CIDR para IPv4 e IPv6

Estos archivos de ejemplo muestran cómo usar rangos de índice CIDR para IPv4 e IPv6 en feeds MetaCallback personalizados. Al igual que con otros feeds personalizados, debe crear el archivo de datos de feed en formato .csv y un archivo de definición de feed en formato .xml.

Nota: El uso de feeds MetaCallback con rangos de índice CIDR solo se admite mediante el asistente Configuración avanzada o la interfaz de REST.

En el siguiente ejemplo se muestra el contenido de un archivo `.csv` y un archivo `.xml` para un feed MetaCallback con rangos de índice CIDR para IPv4 o IPv6.

`.csv file:`

```
192.168.0.0/24, Sydney
192.168.1.0/24, Melbourne
```

`.xml file:`

```
<?xml version="1.0" encoding="UTF-8"?>
<FDF xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="feed-definitions.xsd">
<FlatFileFeed name="ip_test" path="ip_test.csv" separator="," comment="#">
      <MetaCallback name="DstIP" valuetype="IPv4" apptype="0"
truncdomain="false">
            <Meta name="ip.dst"/>
      </MetaCallback>
      <LanguageKeys>
            <LanguageKey name="alert" valuetype="Text" />
      </LanguageKeys>
      <Fields>
            <Field index="1" type="index" range="cidr"/>
            <Field index="2" type="value" key="alert" />
      </Fields>
</FlatFileFeed>
</FDF>
```

Nota: Para configurar un rango de índice CIDR para los feeds con uno o varios MetaCallbacks de tipo de valor IPv4 o IPv6, el campo de índice de tipo DEBE contener un atributo de rango con `range="cidr"`. Además, la configuración de rangos de índice “cidr” para los feeds con MetaCallbacks de varios tipos de valores diferentes no es compatible.

Crear un feed personalizado

Puede crear un feed personalizado mediante el asistente Feed personalizado. Para realizar este procedimiento, necesita un archivo de datos de feed en formato `.csv` o `.xml`. Si también tiene un archivo de definición de feed relacionado en formato `.xml`, que describe la estructura del archivo de datos del feed, puede usarlo para crear un feed. Con el asistente Feed personalizado, se pueden crear feeds basados en un archivo de datos de feed o basados en este y el archivo de definición de feed correspondiente.

Nota: A partir de 10.6.1 o superior, NetWitness Platform es compatible con Structured Threat Information Expression (STIX). Para obtener más información acerca de STIX y la creación de un feed personalizado de STIX, consulte "Crear un feed personalizado de STIX" en la *Guía de configuración de Decoder y Log Decoder*.

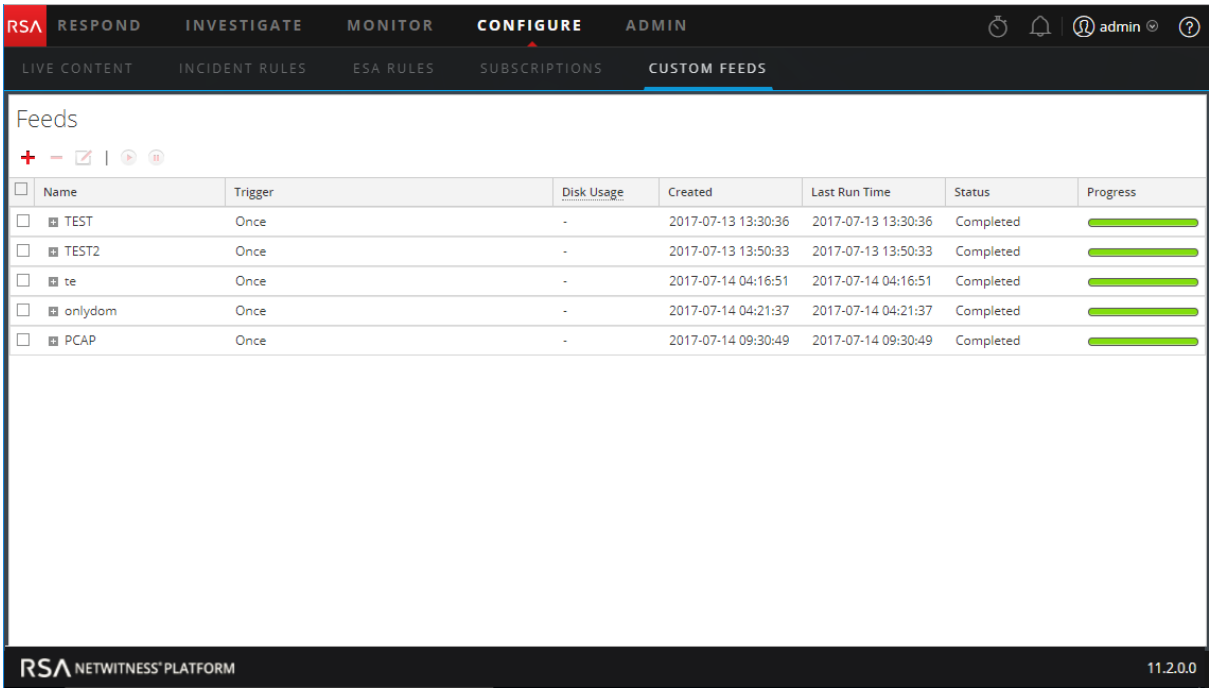
El archivo de datos de feed y, de manera opcional, el archivo de definición de feed (`.xml`) deben estar disponibles en el sistema de archivos local para crear un feed personalizado según demanda. Para crear un feed personalizado recurrente, los archivos deben estar disponibles en una URL a la que se pueda acceder desde el servidor de NetWitness Platform.

Nota: Cuando crea un feed basado en origen y destino en un Log Decoder, este completa solamente la clave de metadatos de origen. No puede utilizar feed de CIDR o basado en rango. Debe enumerar cada dirección IP. Para resolver este problema, cree dos feeds distintos con el uso de direcciones IP. En ellos puede usar CIDR.

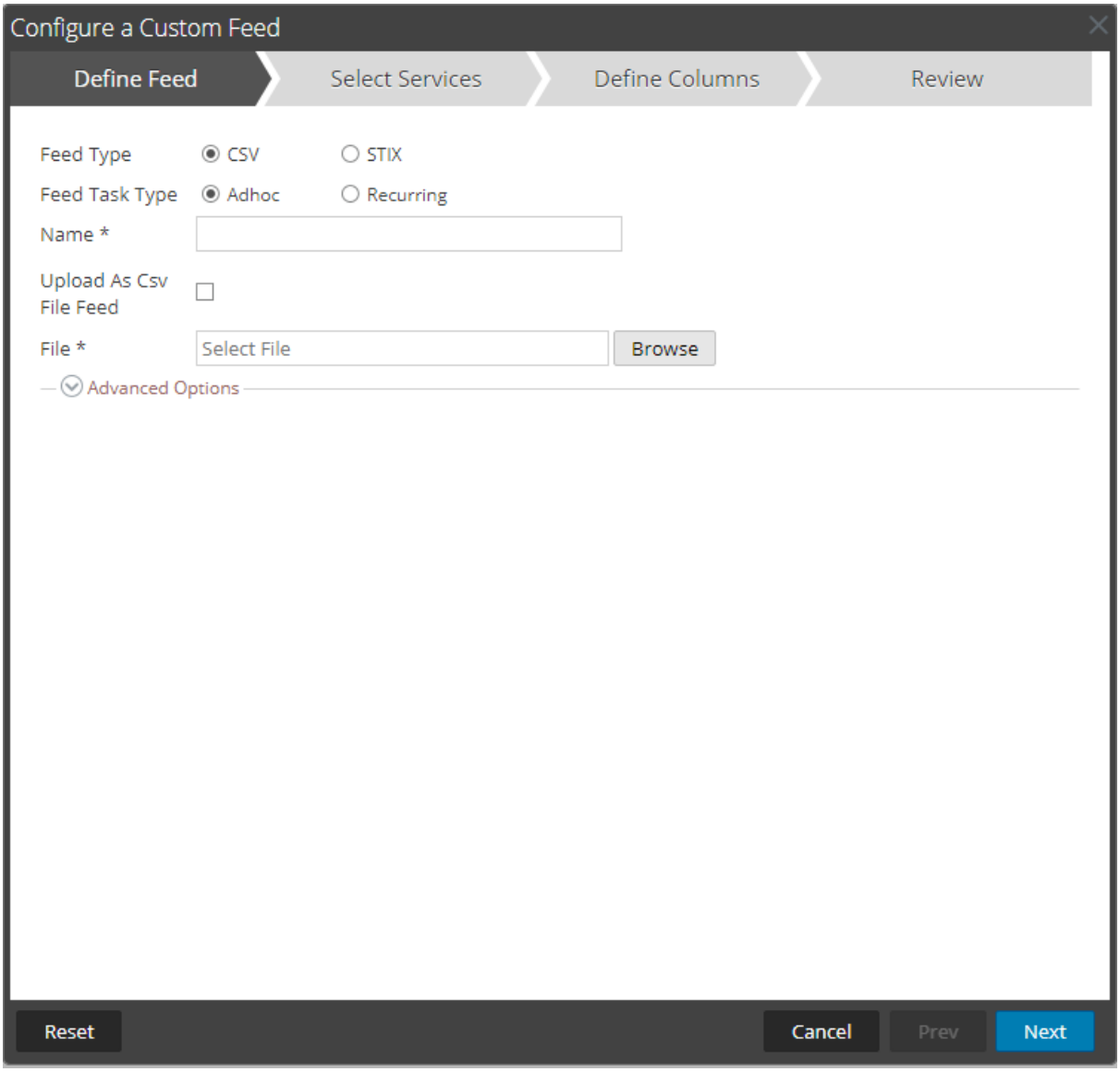
Para crear un feed personalizado:

1. Vaya a **CONFIGURAR > Feeds personalizados.**

2. En el panel **Feeds**, haga clic en +.
   Se muestra la vista Feeds personalizados.



3. Haga clic en **Feed personalizado** y en **Siguiente**.
   El asistente Configurar un feed personalizado se muestra con el formulario Definir feed abierto.



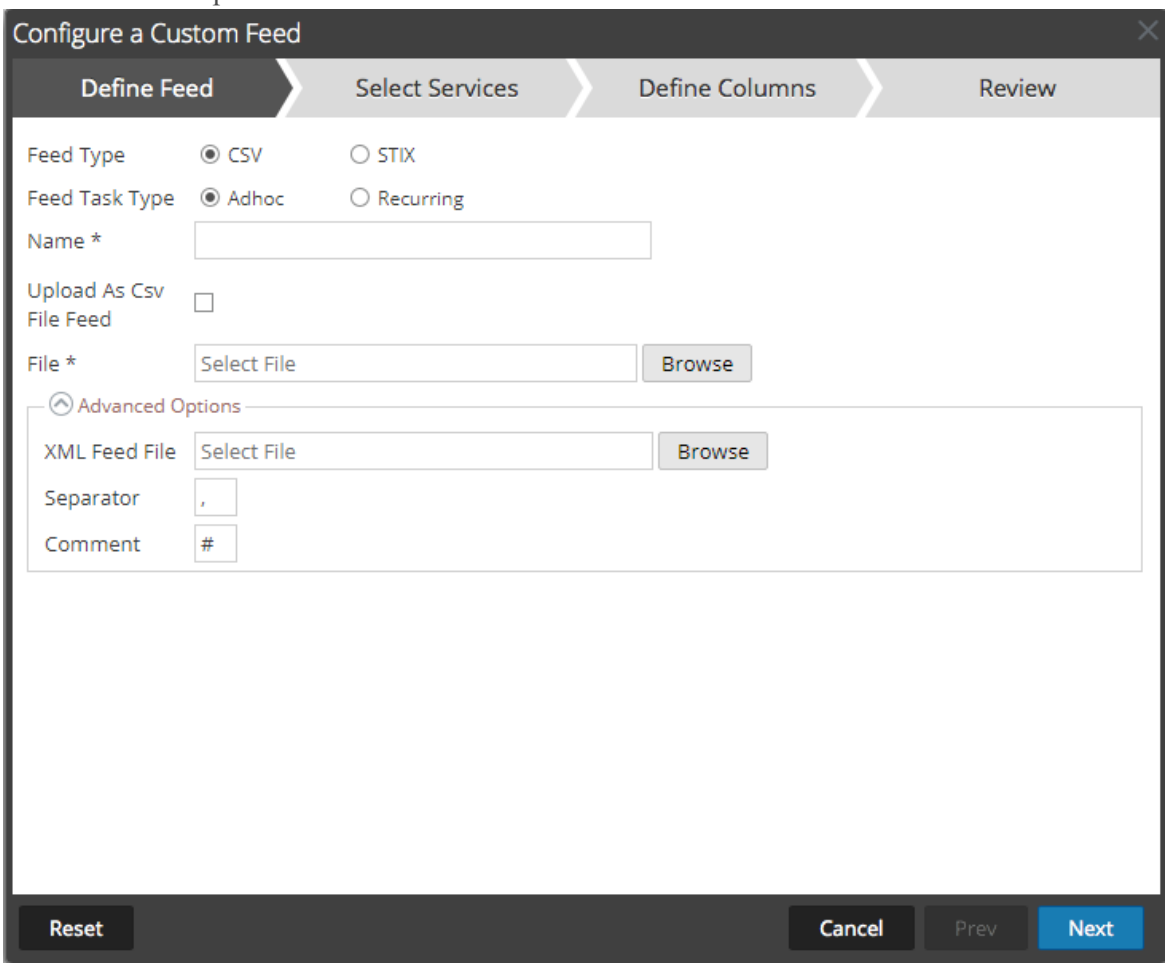
4. Seleccione el Tipo de feed: **CSV** o **STIX**.
5. Para definir un feed basado en un archivo de datos de feed con formato `.csv`, seleccione **CSV** (que es el valor predeterminado) en el campo **Tipo de feed**.
6. Para definir una tarea de feed según demanda que se ejecute una sola vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed** y realice una de las siguientes acciones:
   a. (Condicional) Para definir un feed basado en un archivo CsvFileFeed, seleccione la casilla de verificación **Cargar como feed de archivo csv**, escriba el **Nombre** del feed, seleccione un archivo de contenido .csv en el sistema de archivos local y haga clic en **Siguiente**. Si no selecciona la casilla de verificación, el archivo .csv será un archivo FlatFileFeed.

Nota: Cuando selecciona la casilla de verificación Cargar como feed de archivo csv, las opciones del feed XML en Avanzada no están disponibles.

b. (Condicional) Para definir un feed basado en un archivo de feed XML, seleccione **Opciones avanzadas**.

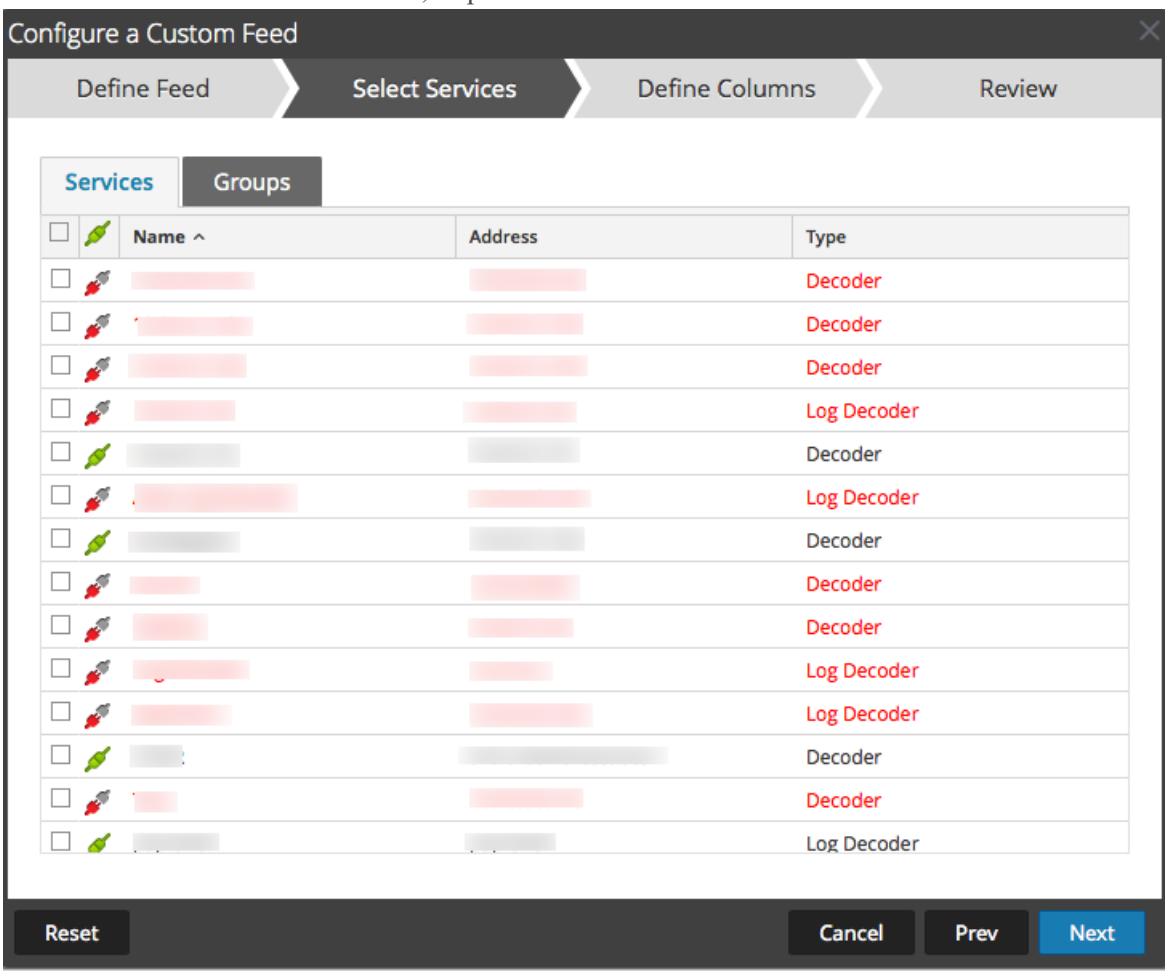
Nota: Asegúrese de que la casilla de verificación Cargar como feed de archivo csv esté deseleccionada.

c. Se muestran las opciones avanzadas:



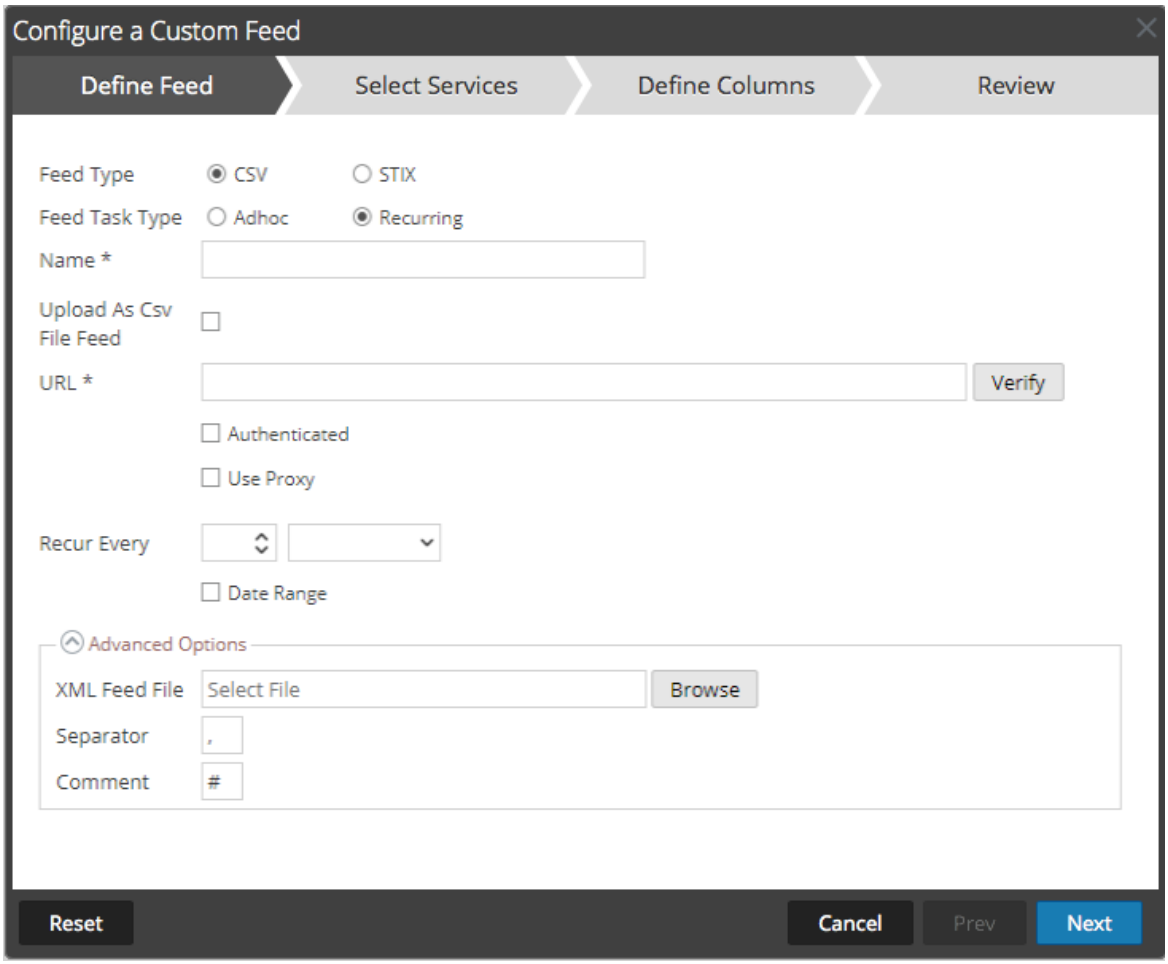
d. Seleccione un archivo de feed XML en el sistema de archivos local, elija el Separador (el valor predeterminado es coma), especifique los caracteres de Comentario que se utilizan en el archivo de datos del feed (el valor predeterminado es #) y haga clic en **Siguiente**.
Se muestra el formulario Seleccionar servicios. Este es un ejemplo del formulario de un feed basado en un archivo de datos de feed sin archivo de definición de feed. Si define un feed basado

en un archivo de definición de feed, la pestaña Definir columnas no es necesaria.



7. Para definir una tarea de feed recurrente que se ejecute de manera repetida en intervalos especificados durante un período especificado, haga lo siguiente:

   a. Seleccione **Recurrente** en el campo **Tipo de tarea de feed**.
   En el formulario Definir feed se incluyen los campos de un feed recurrente.



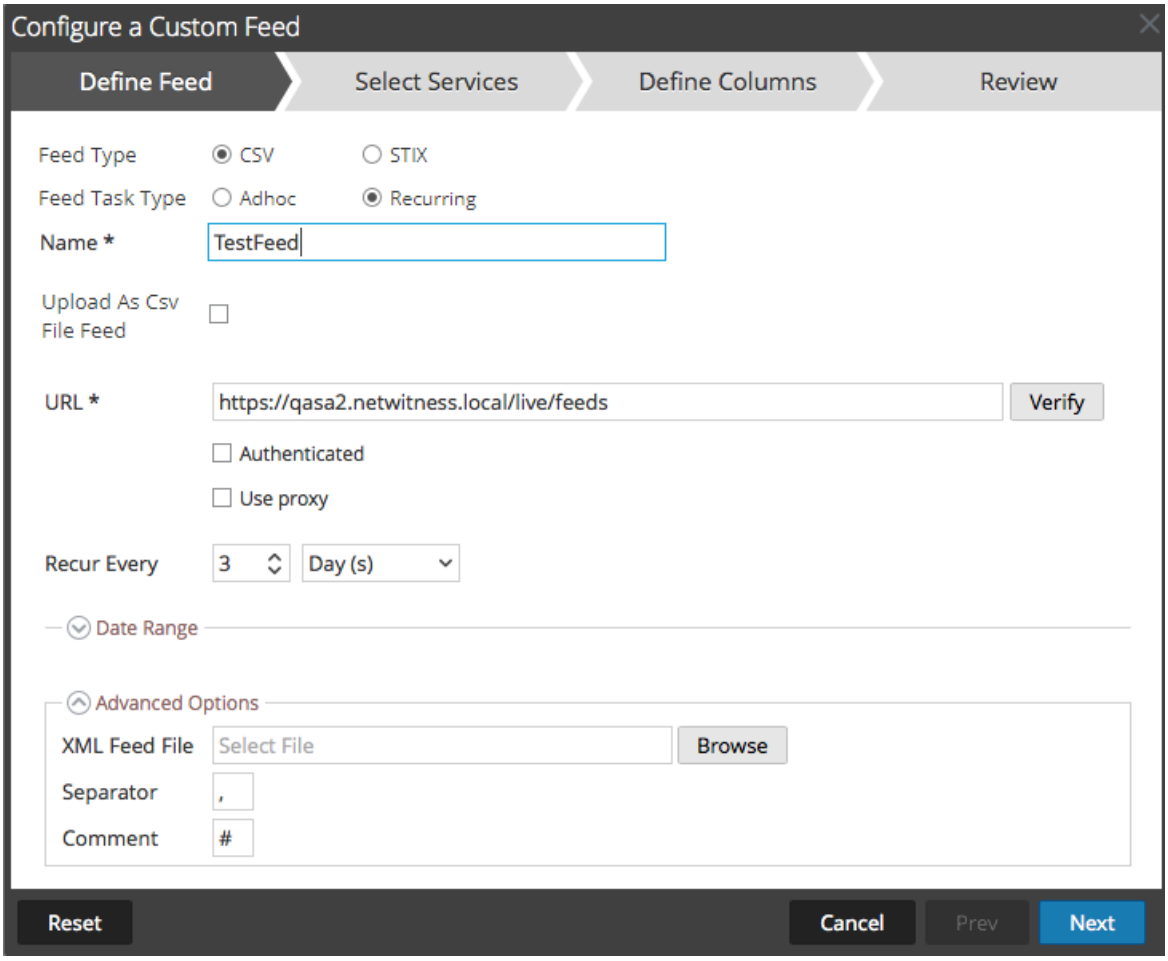
b. En el campo **URL**, ingrese la dirección URL donde se encuentra el archivo de feed de datos, por ejemplo, `http://<hostname>/<feeddatafile>.csv`, y haga clic en **Verificar**. NetWitness Platform verifica la ubicación en la cual está almacenado el archivo para permitir la comprobación automática el archivo más reciente antes de cada recurrencia.

c. (Opcional) Si la URL tiene acceso restringido y se solicita autenticación con nombre de usuario y contraseña, seleccione **Autenticada**.
NetWitness Platform proporciona a la dirección URL su nombre de usuario y contraseña para la autenticación.

d. Si desea que el servidor de NetWitness acceda a la dirección URL del feed a través de un proxy, seleccione **Usar proxy**. Para obtener más información sobre la configuración de un proxy, consulte "Configurar el proxy de NetWitness Platform" en la *Guía de configuración del sistema*.
De manera predeterminada, la casilla de verificación **Usar proxy** no está seleccionada.

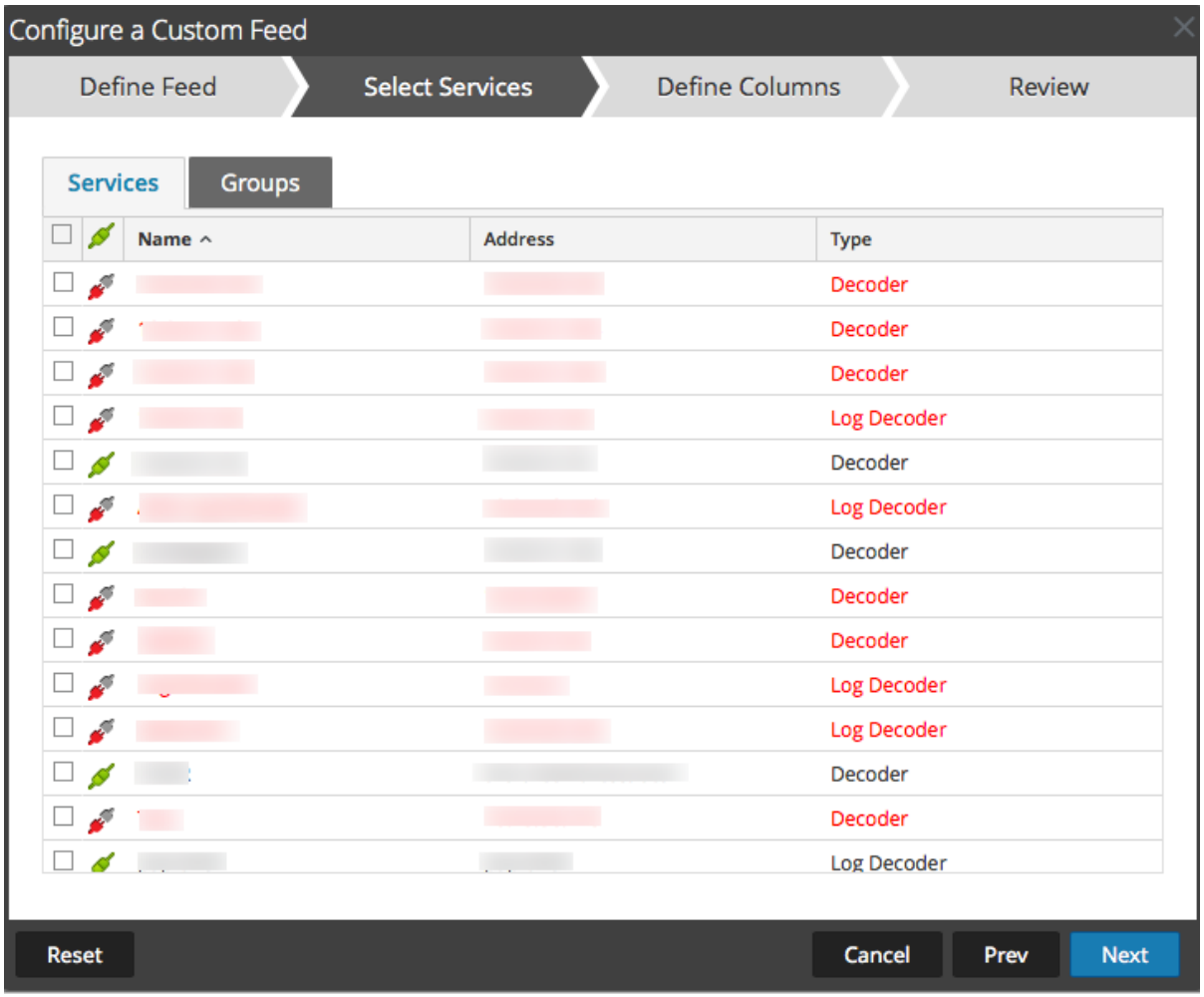
e. Para definir el intervalo de recurrencia, puede realizar alguna de las siguientes acciones:
- Especifique la cantidad de minutos, horas o días entre cada recurrencia del feed.
- Especifique la recurrencia semanal y seleccione los días de la semana.

f. Para definir el rango de fechas para la ejecución recurrente del feed, especifique la hora y la **Fecha de inicio** y la hora y la**Fecha de finalización**.

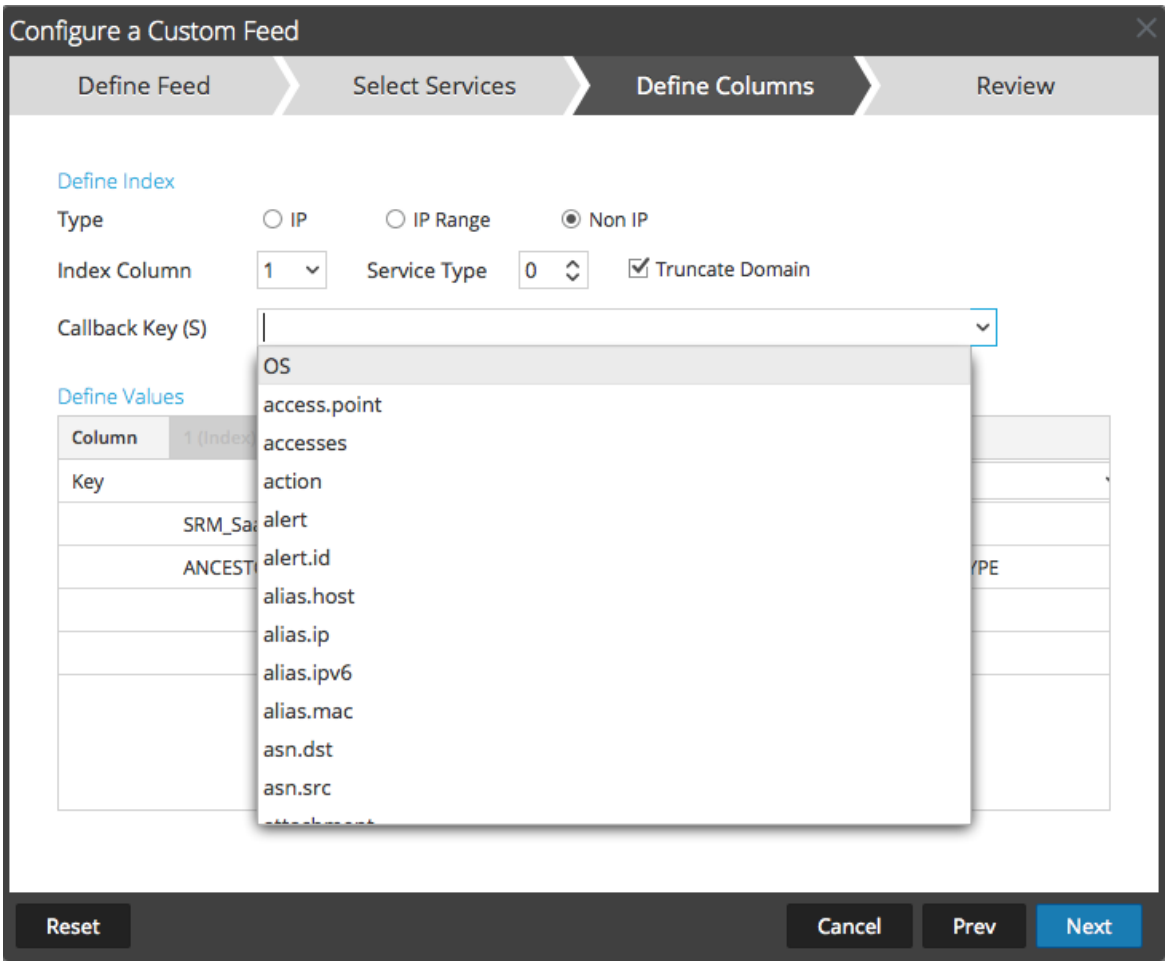


8. (Condicional) Si desea definir un feed basado en un archivo de feed XML:
   - Escriba el **Nombre** del feed y seleccione **Opciones avanzadas**. Se muestran los campos Opciones avanzadas.
   - Seleccione un archivo de feed XML en el sistema de archivos local, elija el **Separador** (el valor predeterminado es coma), especifique los caracteres de **Comentario** que se utilizan en el archivo de datos del feed (el valor predeterminado es #) y haga clic en **Siguiente**. Se muestra el formulario

Seleccionar servicios.

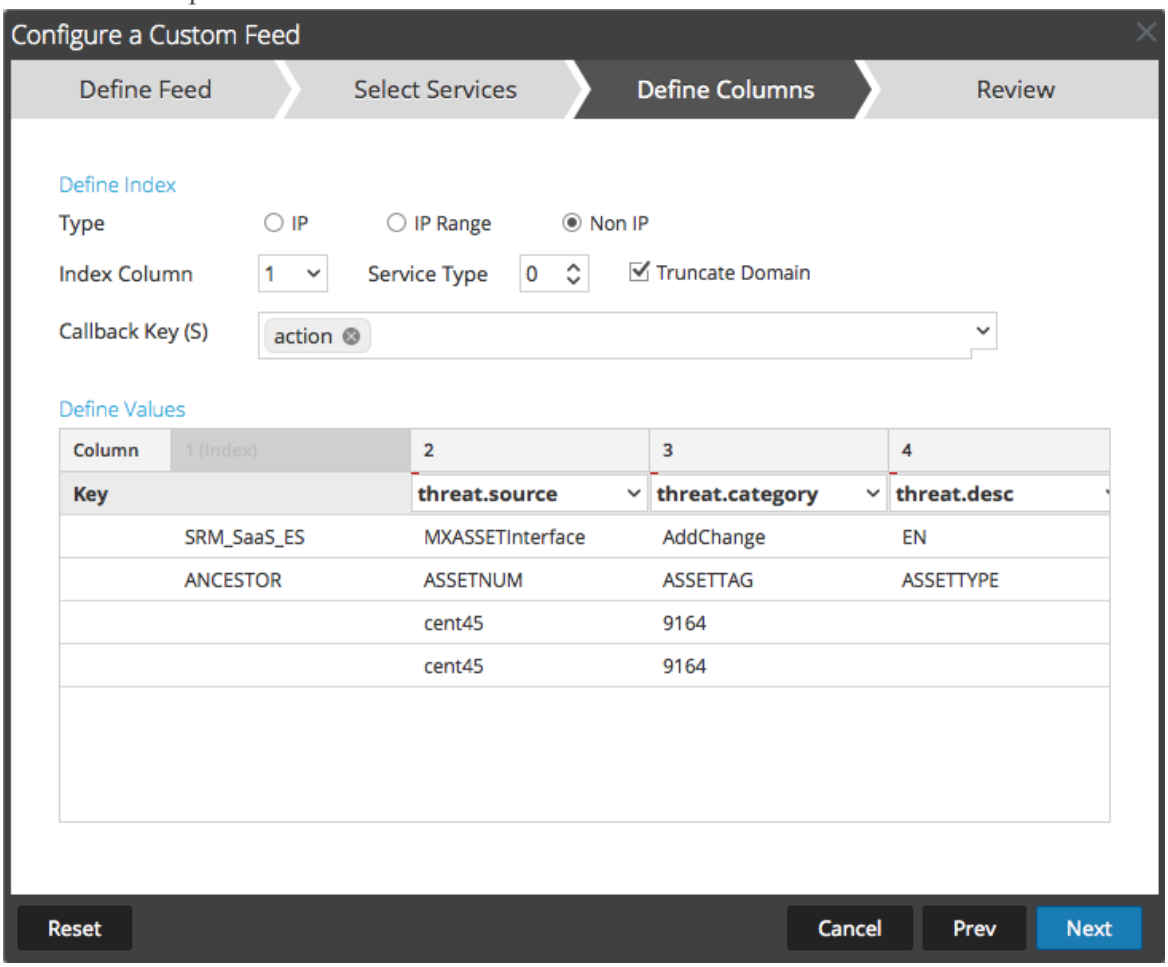


9. Para identificar los servicios en los cuales se implementará el feed, realice una de las siguientes acciones:
   a. Seleccione uno o más Decoders y Log Decoders y haga clic en **Siguiente**
   b. Haga clic en la pestaña **Grupos** y seleccione un grupo. Haga clic en **Siguiente**.
   Se muestra el formulario Definir columnas.
10. Para asignar columnas en el formulario Definir columnas, haga lo siguiente:
   a. Defina el tipo de Índice: **IP**, **Rango de IP** o **No IP**, y seleccione la columna de índice.
   b. (Condicional) Si el tipo de índice es **IP** o **Rango de IP** y la dirección IP está en notación CIDR, seleccione **CIDR.**
   c. (Condicional) Si el tipo de índice es **No IP**, se muestran ajustes adicionales. Seleccione el tipo de servicio, las **Claves de devolución de llamadas** y, de manera opcional, la opción **Truncar dominio**.

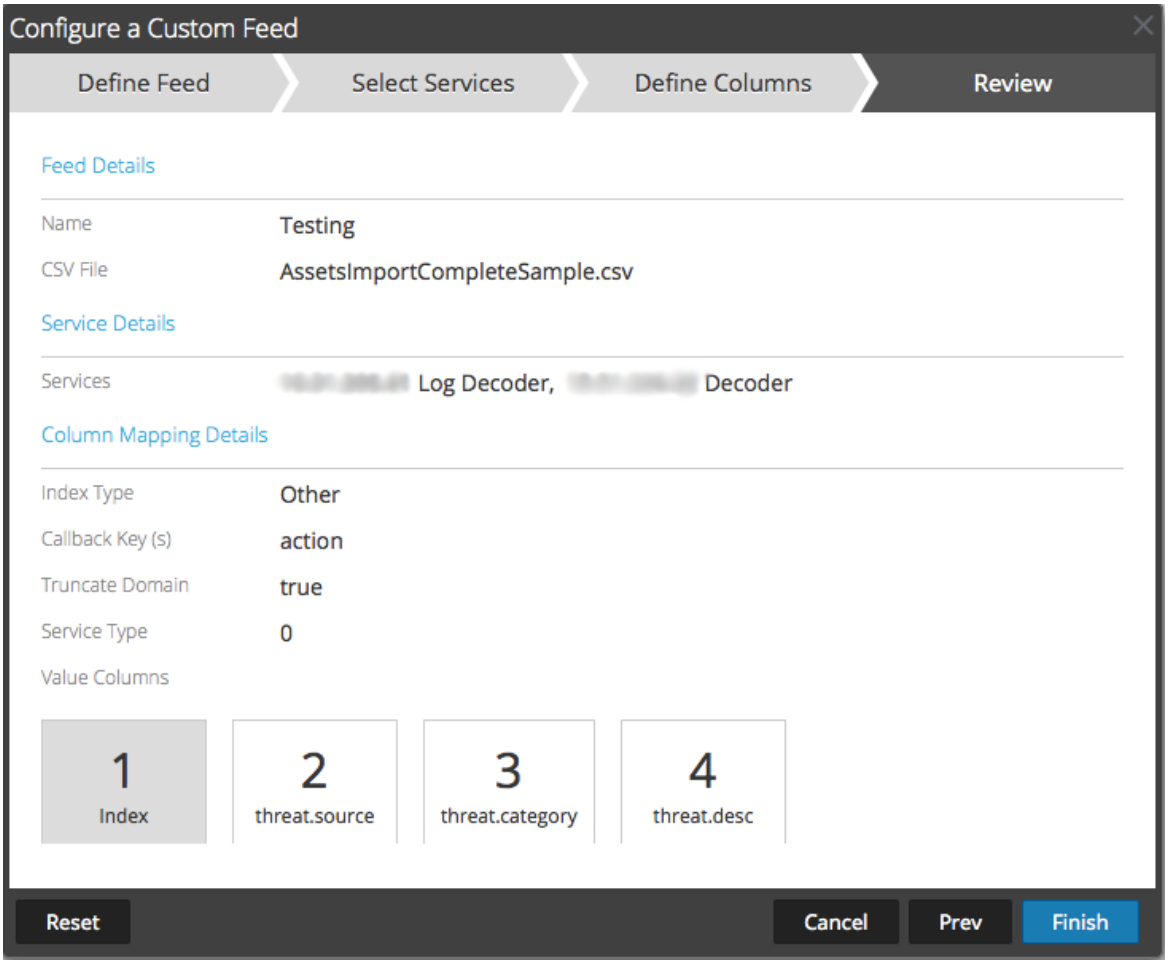


d. En la lista desplegable, seleccione la clave de idioma que se aplicará a los datos en cada columna. Los metadatos que se muestran en la lista desplegable se basan en los metadatos disponibles para los valores definidos del servicio. También puede agregar otros metadatos de

acuerdo con su pericia avanzada.



e. Haga clic en **Siguiente**.
Se muestra el formulario Revisión.

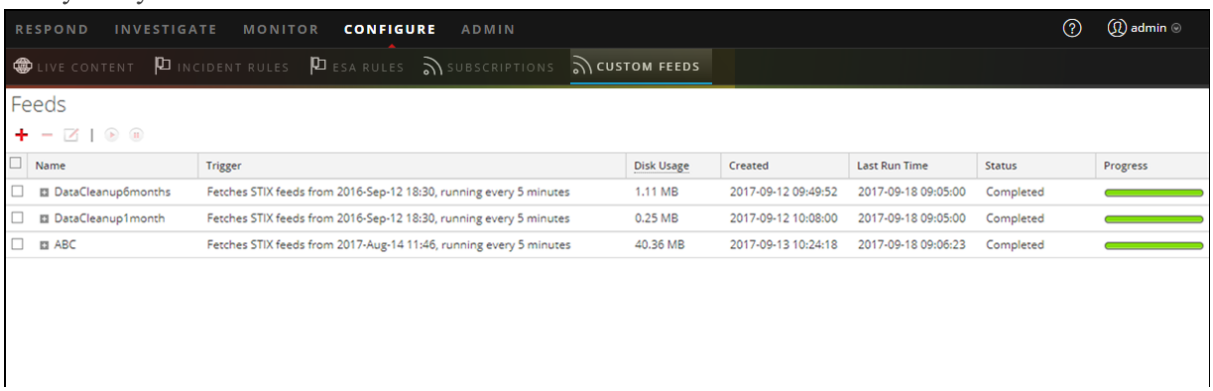


11. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:

- Hacer clic en **Cancelar** para cerrar el asistente sin guardar la definición del feed.
- Hacer clic en **Restablecer** para borrar los datos del asistente.
- Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
- Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario)

11. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.
12. Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, el feed y el archivo de token correspondiente aparecen en la cuadrícula Feed y la barra de progreso muestra que se completó la tarea. Puede expandir o contraer la entrada para ver cuántos servicios se

incluyeron y cuáles tuvieron éxito.



Crear un feed personalizado de STIX

Structured Threat Information Expression (STIX™) es un lenguaje estructurado para describir información de amenazas cibernéticas, de modo que se pueda compartir, almacenar y analizar de manera coherente. Para obtener más información acerca de STIX, consulte https://stixproject.github.io/.

Puede crear un feed personalizado con un archivo de datos de feed con formato STIX (`.xml`) en RSA NetWitness Platform. NetWitness Platform es compatible con Structured Threat Information Expression (STIX) versiones 1.0, 1.1 y 1.2 solamente.

Precaución: Si se configura un feed recurrente STIX y se actualiza Security Analytics de 10.6.x a NetWitness Platform 11.x, debe volver a configurar el feed recurrente STIX.

En NetWitness Platform, se admiten los feeds STIX de tipo Indicador u Observable, que contienen propiedades como direcciones IP, hashes de archivo, nombres de dominio, URI y direcciones de correo electrónico. Solo se admiten los valores de propiedades en el operador Es igual a. Los atributos, como Tipo y Título, también se leen desde STIX. Se admite un archivo STIX con un solo STIX_Package.

TAXII (Trusted Automated eXchange of Indicator Information) es el mecanismo de transporte principal para obtener información de amenazas cibernéticas que se representa en STIX. Mediante los servicios TAXII, las organizaciones pueden compartir la información sobre amenazas cibernéticas de manera segura y automatizada.

Las comunidades de STIX y TAXII trabajan en estrecha colaboración para asegurarse de proporcionar de forma constante una plataforma completa para el uso compartido de inteligencia de amenazas.

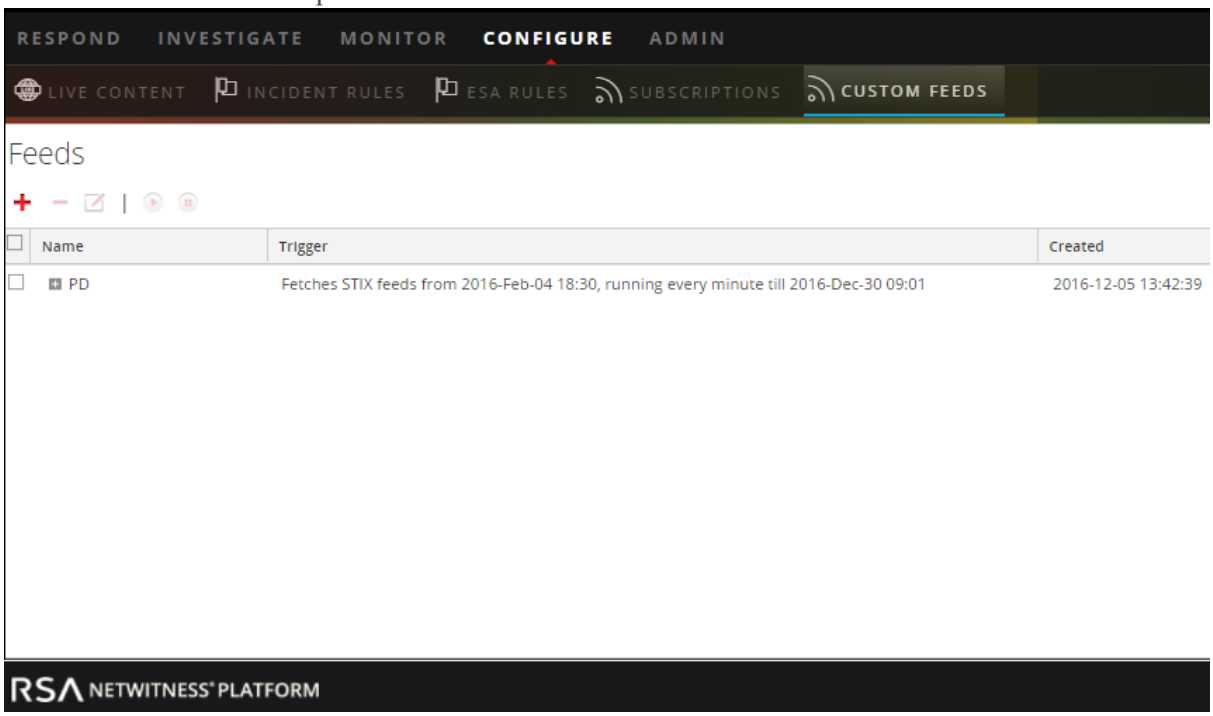
Aparte del servidor TAXII, los datos STIX también pueden residir en un servidor de REST y puede buscar el archivo STIX desde el servidor de REST mediante la dirección URL del servidor de REST. Por ejemplo, `http://stixrestserver.internal.com`.

El archivo de datos de feed STIX y, de manera opcional, el archivo de definición de feed, ambos en formato `.xml`, deben estar disponibles en el sistema de archivos local para un feed personalizado según demanda. Para crear un feed personalizado recurrente, los archivos deben estar disponibles en una URL a la que se pueda acceder desde el servidor de NetWitness Platform.

Para crear un feed personalizado de STIX:

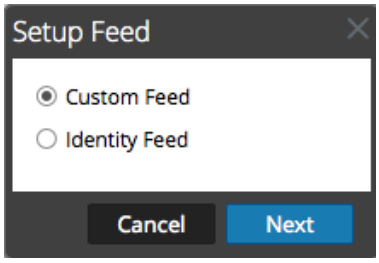
1. Vaya a **Configurar > Feeds personalizados**.

   Se muestra la vista Feeds personalizados.



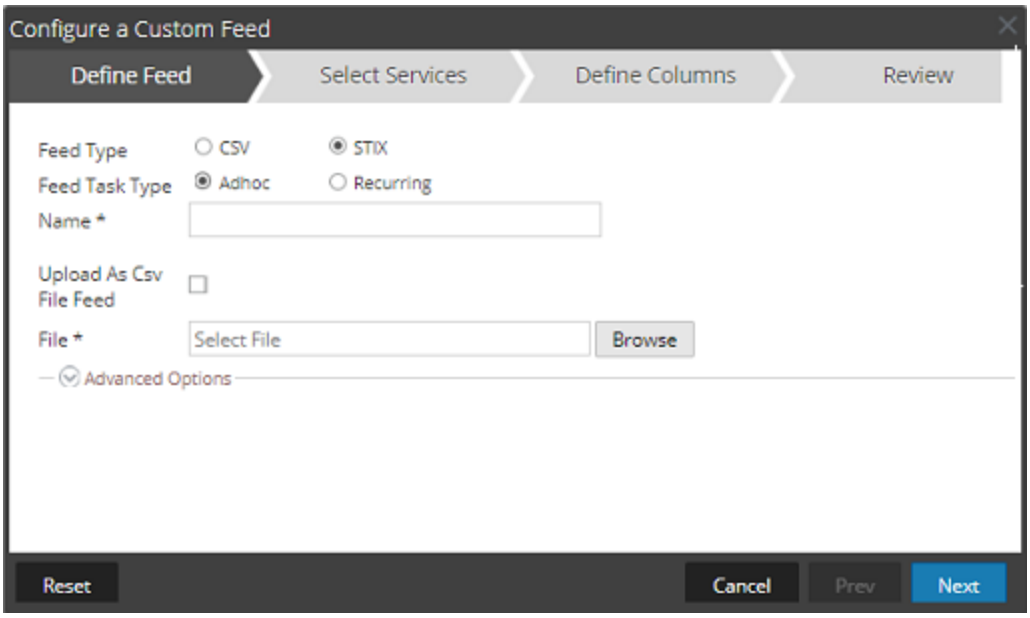
2. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo Configurar feed.



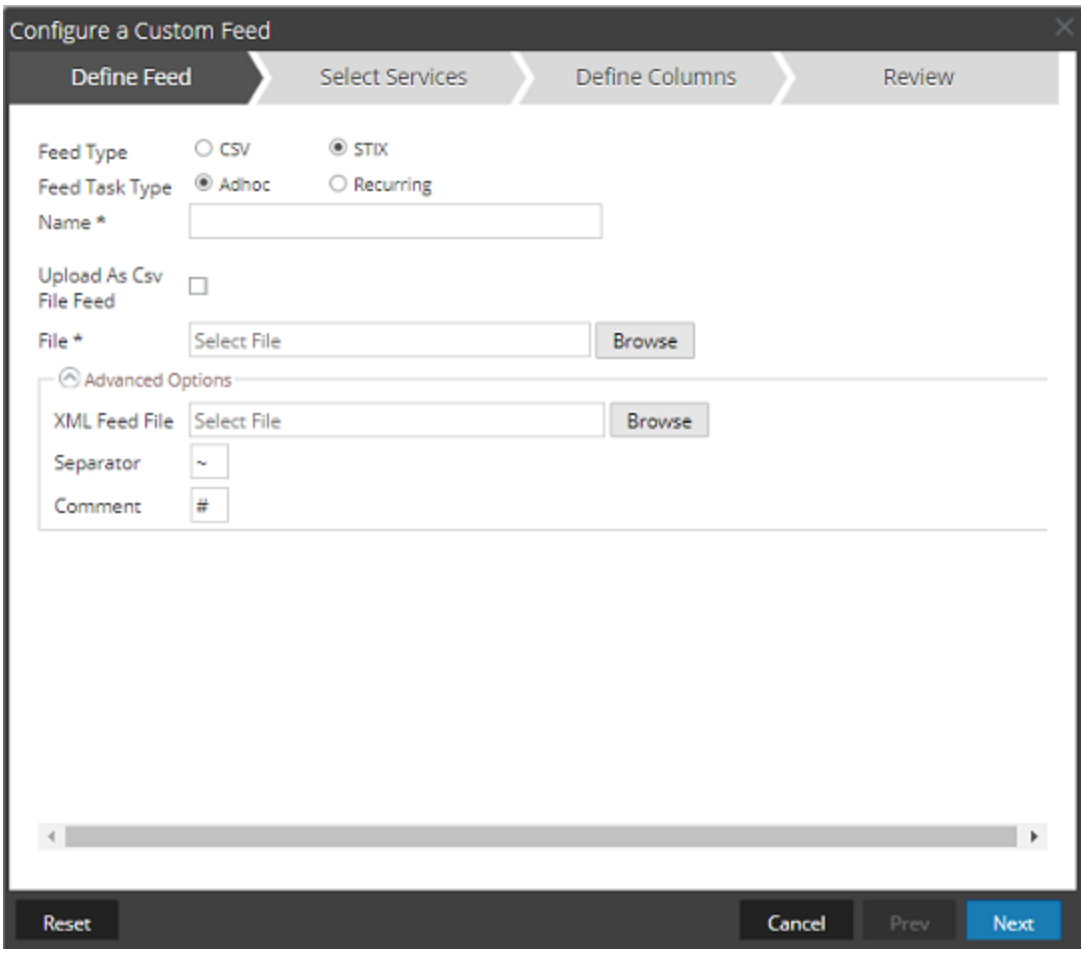
3. Para seleccionar el tipo de feed, haga clic en **Feed personalizado** y luego en **Siguiente**.

   El asistente Configurar un feed personalizado se muestra con el formulario Definir feed abierto.

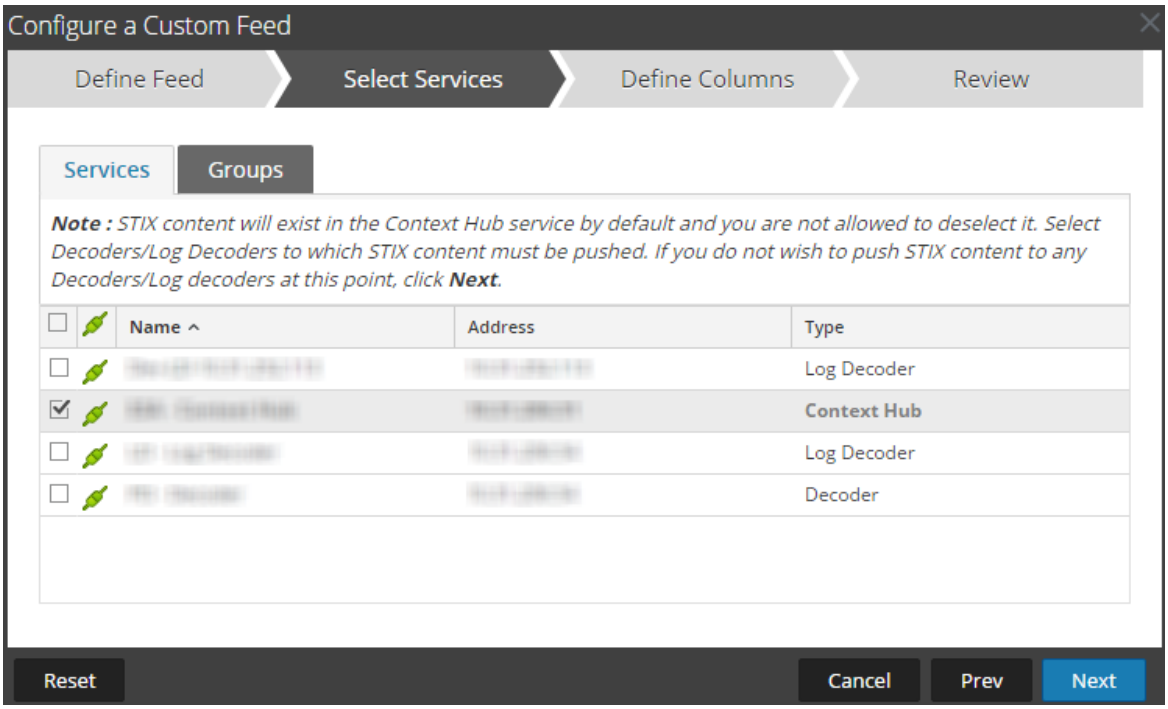


4. Para definir un feed basado en un archivo `.xml` con formato STIX, seleccione **STIX** en el campo **Tipo de feed**.
5. Para definir una tarea de feed según demanda que se ejecute una sola vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed** y realice una de las siguientes acciones:
   a. (Condicional) Para definir un feed basado en un archivo `.xml` con formato STIX, escriba el **Nombre** del feed, seleccione un archivo de contenido `.xml` con formato STIX en el sistema de archivos local y haga clic en **Siguiente**.
   b. (Condicional) Para definir un feed basado en un archivo de feed XML, seleccione **Opciones avanzadas**.

      Se muestran las opciones avanzadas.



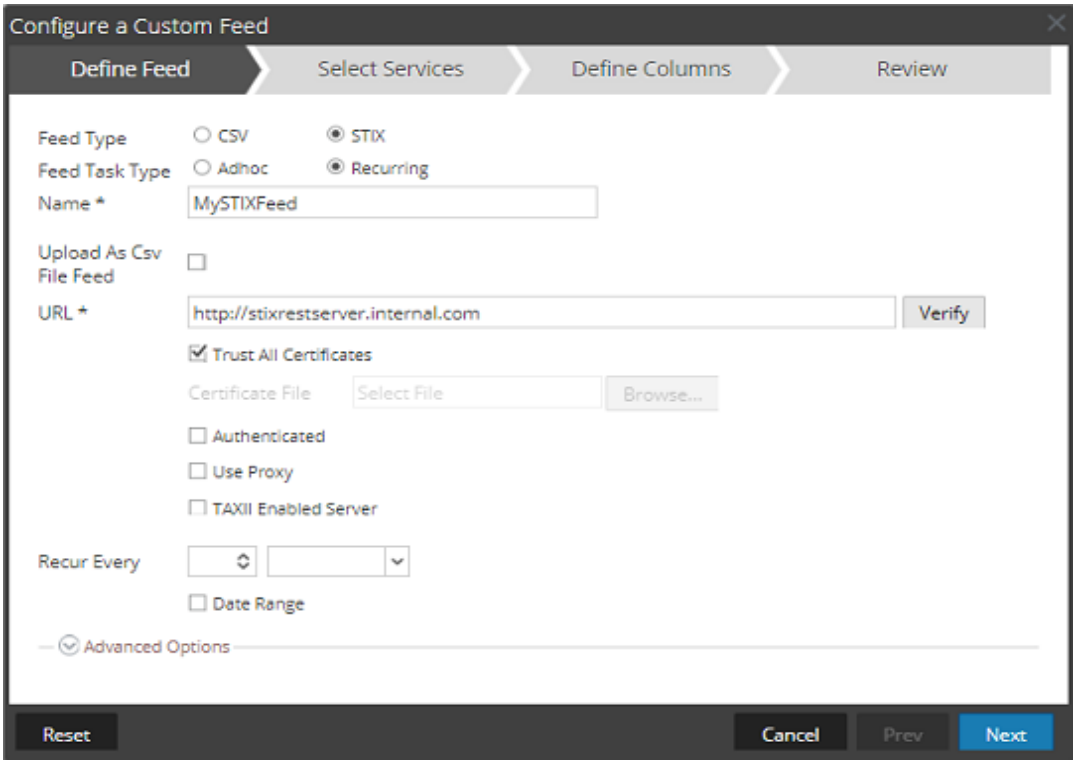
c. Seleccione un archivo de feed XML en el sistema de archivos local, elija el Separador (el valor predeterminado es coma), especifique los caracteres de Comentario que se utilizan en el archivo de datos del feed (el valor predeterminado es #) y haga clic en **Siguiente**.
Se muestra el formulario Seleccionar servicios. Este es un ejemplo del formulario de un feed basado en un archivo de datos de feed sin archivo de definición de feed. Si define un feed basado en un archivo de definición de feed, la pestaña Definir columnas no es necesaria.



6. Para definir una tarea de feed recurrente que se ejecute de manera repetida a intervalos especificados durante un rango de fechas especificado:

   a. Seleccione **Recurrente** en el campo **Tipo de tarea de feed**.

   En el formulario Definir feed se incluyen los campos de un feed recurrente.

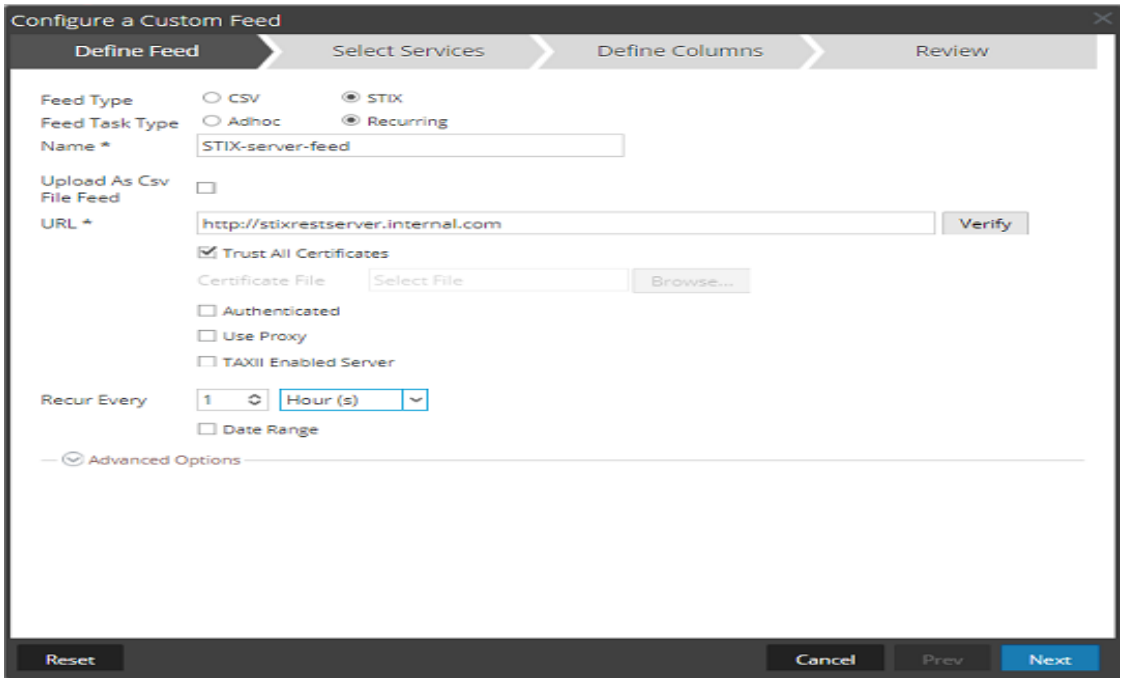


b. En el campo **URL**, realice una de las siguientes acciones:

- Para definir un feed recurrente basado en STIX que extrae paquetes de STIX desde un servidor de TAXII, ingrese la URL del servicio de descubrimiento del servidor de TAXII, por ejemplo, `http://hailataxii.com/taxii-discovery-service`.

  Nota: El servicio Context Hub instalado en el host de Event Stream Analysis debe ser accesible para el servidor de TAXII especificado.

- Para definir un feed recurrente basado en un archivo `.xml` con formato STIX mediante el servidor de REST, ingrese la dirección URL del servidor de REST donde se encuentra el archivo de datos STIX, por ejemplo, `http://stixrestserver.internal.com`.



NetWitness Platform verifica la conexión con el servidor, para que NetWitness Platform pueda comprobar automáticamente el archivo más reciente antes de cada recurrencia.

c. Si no desea que NetWitness Platform verifique el certificado SSL del servidor de REST, seleccione **Confiar en todos los certificados**. Esta opción está habilitada de manera predeterminada (seleccionada).

d. Para la autenticación de cliente con la URL de REST, en el campo **Certificado**, haga clic en **Navegar** y seleccione el certificado autofirmado. Los formatos de certificados compatibles son `.cer`, `.crt` con archivos con codificación `Base64` y `DER`.

e. (Opcional) Si la URL tiene acceso restringido y se solicita autenticación con nombre de usuario y contraseña, seleccione **Autenticada**.

NetWitness Platform proporciona su nombre de usuario y contraseña para autenticación en la dirección URL.

f. Seleccione **Servidor habilitado para TAXII** si desea seleccionar una recopilación de TAXII de la lista.
Para una URL válida, en función de sus credenciales se muestra una o más recopilaciones

TAXII que contienen el archivo de datos STIX. Seleccione la recopilación TAXII requerida en la lista. Solo se puede agregar una recopilación desde un servidor de TAXII para un feed.

Nota: Aunque se admiten varios feeds de múltiples servidores de TAXII, solo se admite una cuenta (nombre de usuario y contraseña) con cada servidor de TAXII.

g. Si desea que el servidor de NetWitness Platform acceda a la dirección URL del feed a través de un proxy, seleccione **Usar proxy**. Para obtener más información sobre la configuración de un proxy, consulte "Configurar el proxy de NetWitness Platform" en la *Guía de configuración del sistema*. (Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.) De forma predeterminada, la casilla de verificación **Usar proxy** no está seleccionada.

h. (Opcional) Haga clic en **Verificar** para probar la configuración.

Nota: Asegúrese de que todos los parámetros de conexión requeridos, como Autenticación, Proxy, Confianza de certificados, Servidor habilitado para TAXII, etc., estén configurados antes de hacer clic en Verificar.

i. Para definir el intervalo de recurrencia para migrar a Decoder o Log Decoder, realice alguna de las siguientes acciones:

- Especifique la cantidad de minutos, horas o días entre cada recurrencia del feed.
- Especifique la recurrencia cada semana y seleccione los días de la semana.

j. Para definir el rango de días para la ejecución recurrente del feed, especifique la hora y la **Fecha inicial** y la hora y la **Fecha de finalización**. La Fecha de inicio debe definirse desde cuando desea buscar los datos.

7. (Condicional) Si desea definir un feed basado en un archivo de feed XML:

- Escriba el **Nombre** del feed y seleccione **Opciones avanzadas**.

  Se muestran los campos Opciones avanzadas.

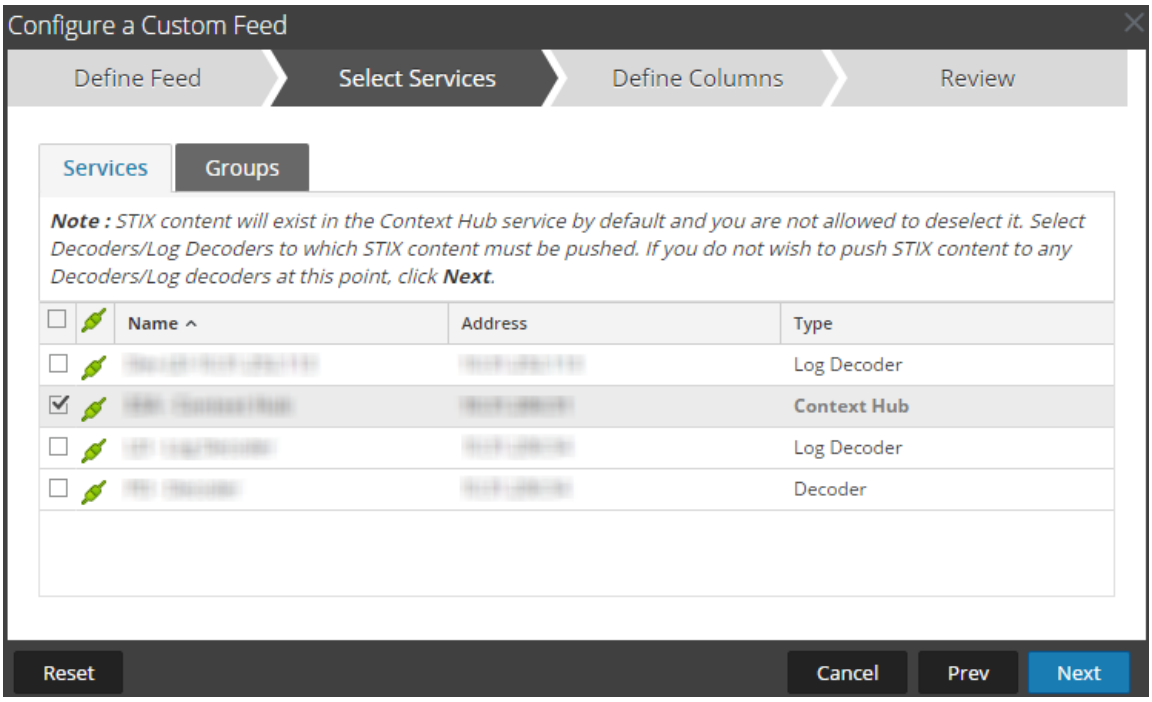
- Seleccione un archivo de feed XML en el sistema de archivos local, elija el **Separador** (el valor predeterminado es coma), especifique los caracteres de **Comentario** que se utilizan en el archivo de datos del feed (el valor predeterminado es #).
- En el campo **Quitar datos de STIX más antiguos que**, especifique la cantidad de días durante los cuales se almacenarán los paquetes de STIX que se extraen del servidor de TAXII. Los paquetes de STIX más antiguos que la cantidad especificada de días se eliminan automáticamente.
- Haga clic en **Siguiente**.

  Se muestra el formulario Seleccionar servicios.

8. Para identificar los servicios en los cuales se implementará el feed, realice una de las siguientes acciones:

a. Seleccione uno o más Decoders y Log Decoders y haga clic en **Siguiente**.

b. En el caso del feed STIX, Context Hub se selecciona de manera predeterminada y no se permite deseleccionar la opción. Además, puede seleccionar uno o más Decoders y Log Decoders y hacer clic en **Siguiente** o en la pestaña **Grupos** y seleccionar un grupo. Haga clic en **Siguiente**.



Si los datos del servidor de STIX son de gran tamaño, se muestra el siguiente mensaje: "La búsqueda de datos de ejemplo está tardando más de lo previsto. Elija una de las siguientes opciones". Tiene dos opciones: continuar esperando o mapear sin datos de ejemplo.

- Si hace clic en **Continuar esperando**, el asistente Feed continúa esperando hasta que se buscan los datos de ejemplo o se agota el tiempo de espera (10 minutos), lo que primero ocurra. Si se agota el tiempo de espera, no se recuperan datos de ejemplo.
- Si hace clic en **Mapear sin datos de ejemplo**, se muestra la columna de mapeo sin los datos de ejemplo.

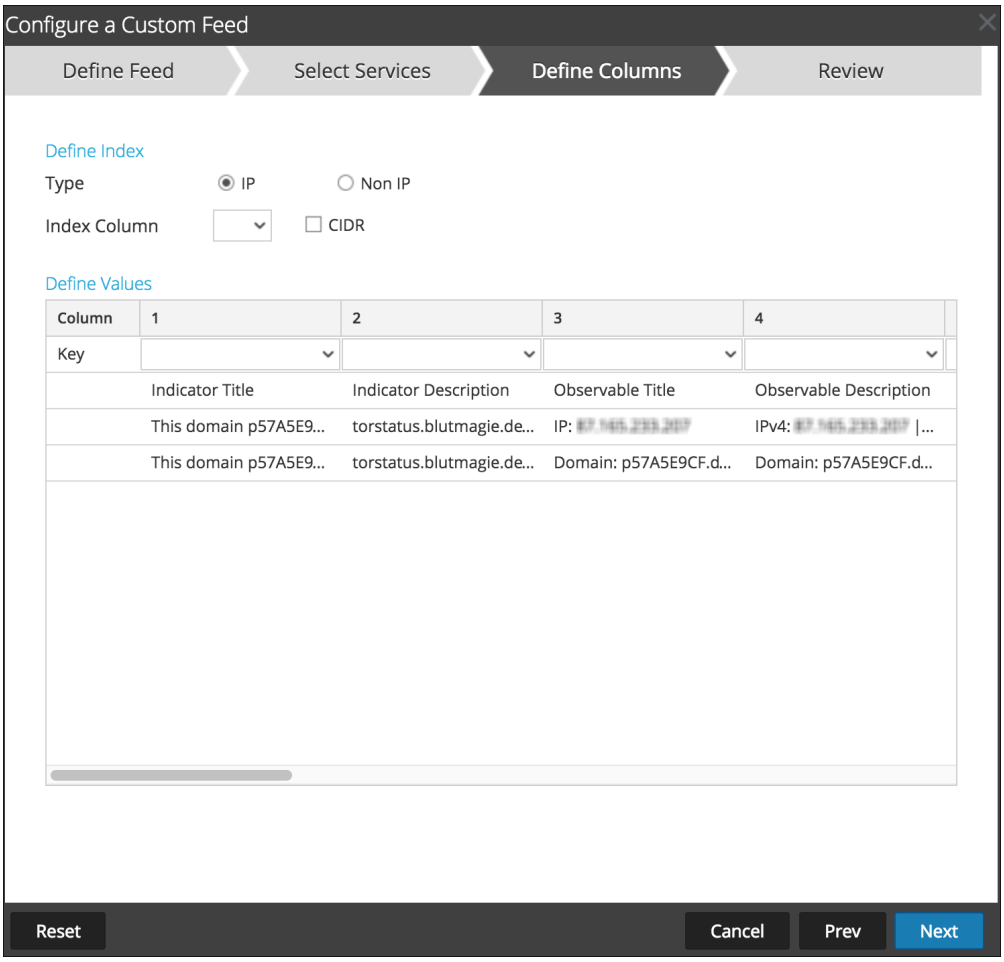
Se muestra el formulario Definir columnas.

9. Para asignar columnas en el formulario Definir columnas, haga lo siguiente:

   a. Defina el tipo de Índice: **IP**, Rango de IP **o** No IP
   y seleccione la columna de índice.

   b. (Condicional) Si el tipo de índice es **IP** o **Rango de IP** y la dirección IP está en notación CIDR, seleccione **CIDR.**

   c. (Condicional) Si el tipo de índice es **No IP**, se muestran ajustes adicionales. Seleccione el tipo de servicio, las **Claves de devolución de llamadas** y, de manera opcional, la opción **Truncar dominio**.

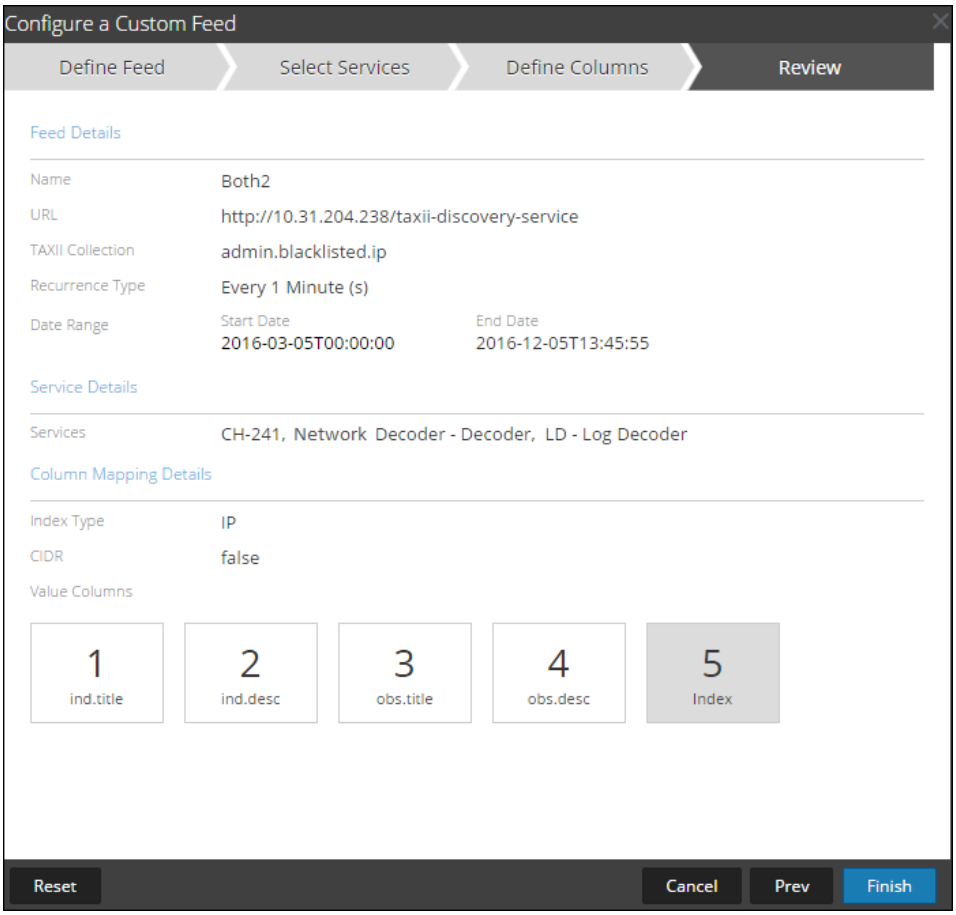


- Si el tipo de índice es No IP, puede seleccionar varias columnas de índice en las columnas de índice. Los valores de todas las columnas seleccionadas se combinan en la primera columna de índice que seleccionó y los valores combinados se envían a Log Decoder para análisis. Por ejemplo, en las columnas de índice si selecciona 2,4,7 como columnas de índice, los valores de las columnas 2,4, y 7 se combinan en la columna 2 y los valores se envían a Log Decoder para análisis.
- La indexación no se puede realizar para las columnas como Título del indicador, Descripción del indicador, Título observable y Descripción observable, ya que esas columnas no permiten realizar la búsqueda.

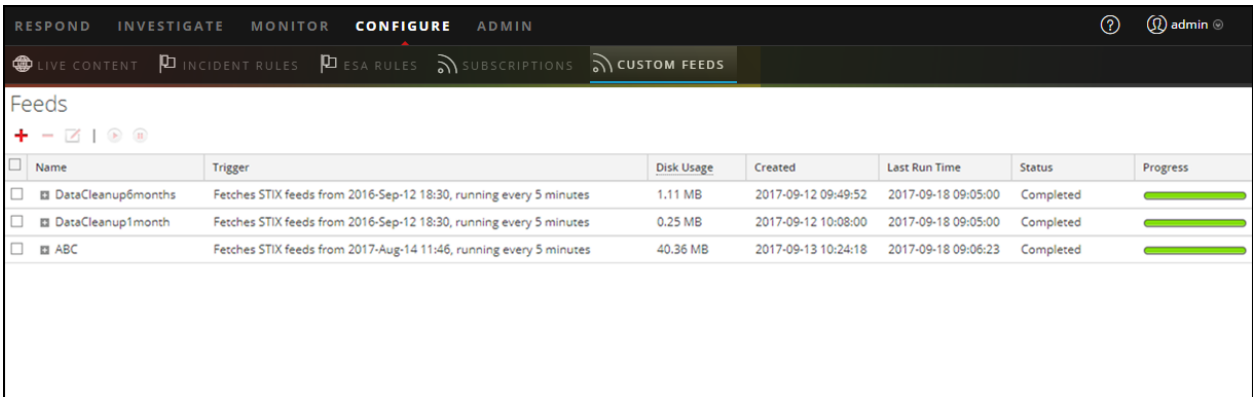
d. En la lista desplegable, seleccione la clave de idioma que se aplicará a los datos en cada columna. Los metadatos que se muestran en la lista desplegable se basan en los metadatos disponibles para los valores definidos del servicio. También puede agregar otros metadatos de acuerdo con su pericia avanzada.

e. Haga clic en **Siguiente**.

Se muestra el formulario Revisión.



10. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
    - Hacer clic en **Cancelar** para cerrar el asistente sin guardar la definición del feed.
    - Hacer clic en **Restablecer** para borrar los datos del asistente.
    - Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
    - Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).
11. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.
12. Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, el feed y el archivo de token correspondiente aparecen en la cuadrícula Feed y la barra de progreso rastrea la finalización de la tarea. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles tuvieron éxito.



Nota: Estado y condición genera alertas cuando la memoria en montón disponible del servidor de Context Hub está en un nivel críticamente bajo. Si el servidor de Context Hub está en mal estado debido a la falta de memoria. Para obtener más información sobre cómo solucionar problemas de `OutOfMemoryError` en el servidor de `Contexthub`, consulte "Solución de problemas" en la *Guía de administración de servicios de Live*.

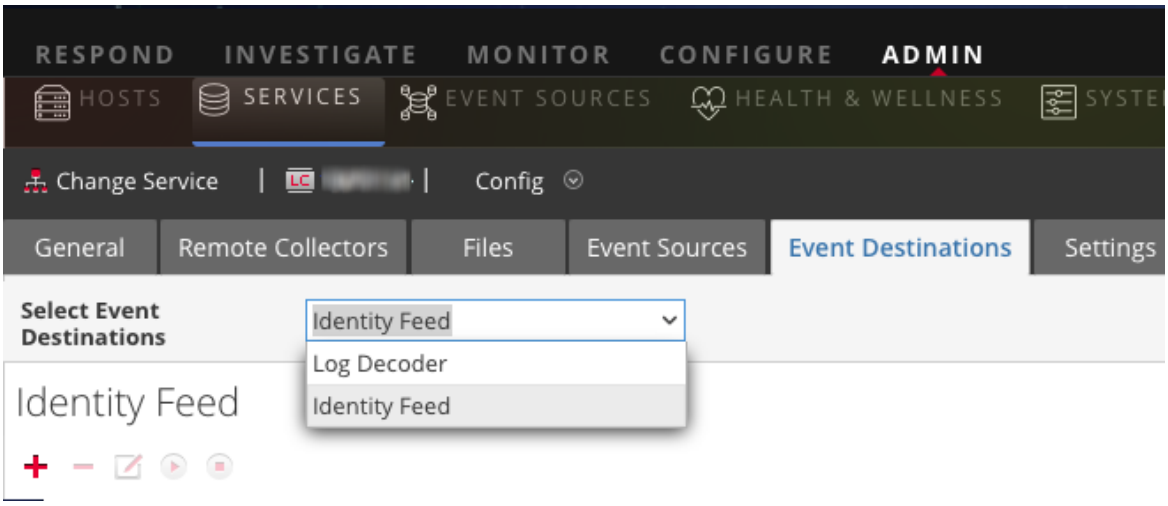
Crear un feed de identidad

Puede crear un feed de identidad y completarlo para los Decoders y los Log Decoders seleccionados. Para crear un feed de identidad, debe tener:

- Un servicio Log Collector con un procesador de eventos de feed de identidad
- Un servicio Log Collector con la recopilación de Windows configurada y habilitada

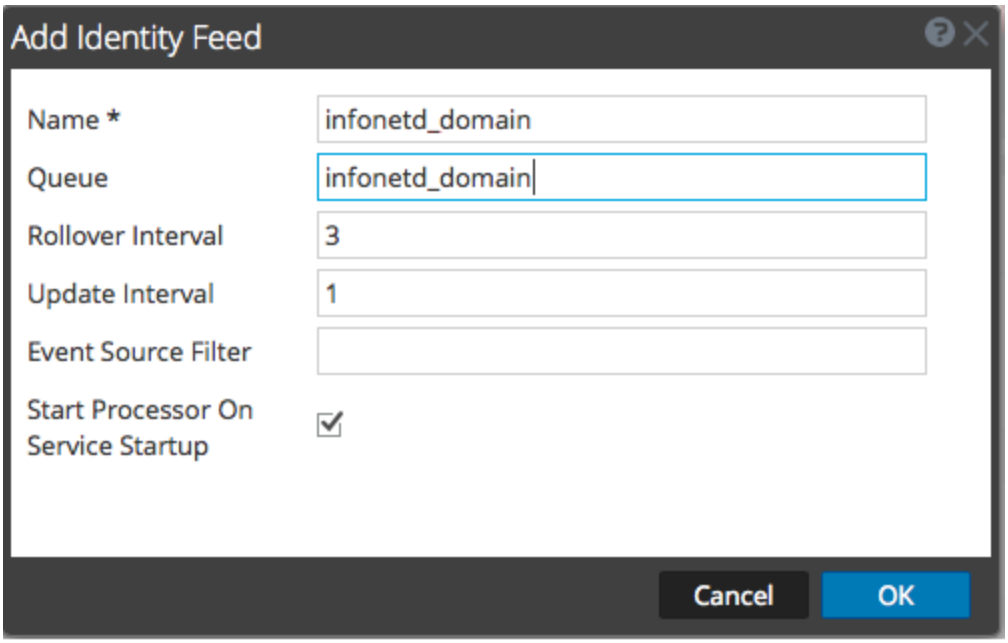
Para crear un feed de identidad:

1. Agregue un destino para el feed.
   a. Vaya a **ADMINISTRAR > Servicios** y en la lista **Servicios**
   b. Seleccione un servicio **Log Collector** y elija **Ver > Configuración**.
   c. Seleccione la pestaña **Destinos de evento**.
   d. En el campo **Seleccionar destinos de evento**, seleccione **Feed de identidad**.



   e. Haga clic en + e ingrese un nombre único para el feed.

      El nombre de la Línea de espera identifica el feed en el Log Collector. Use el nombre del feed para la Línea de espera.

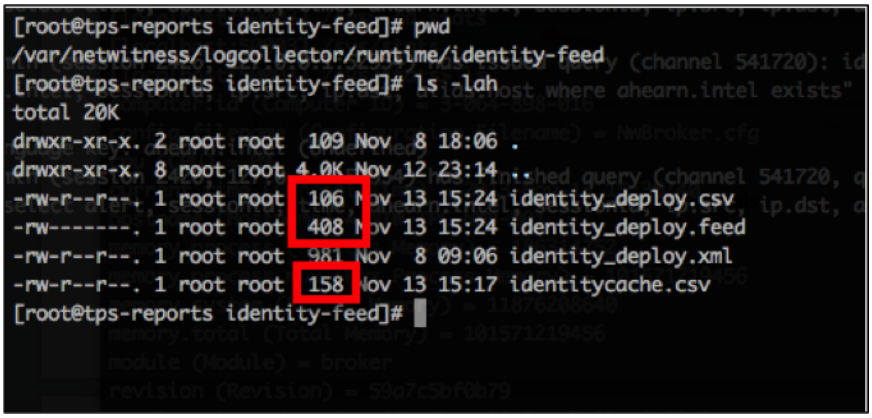


f. Haga clic en **Aceptar**.

2. Pruebe la generación de mensajes.

a. Compruebe que los usuarios hayan iniciado sesión en los cuadros de Windows en el dominio para generar los mensajes de registro correspondientes en los controladores de dominio para las pruebas.

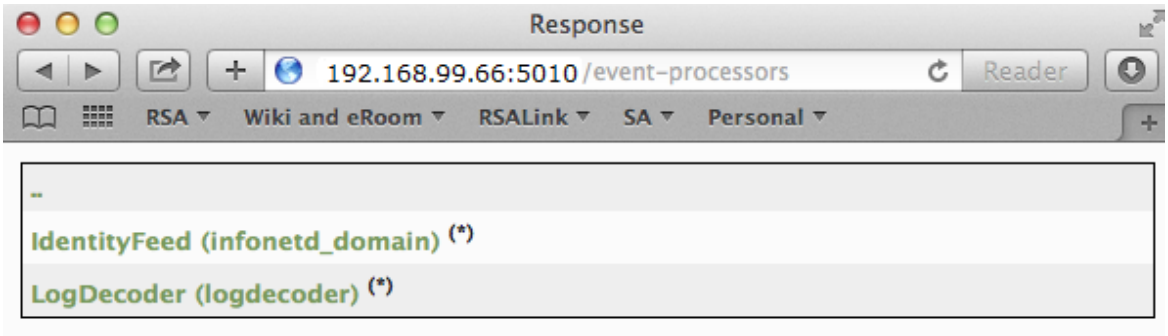
b. Verifique que los datos estén escritos en los archivos de feed. Acceda mediante el protocolo SSH a Log Decoder/Collector o a Virtual Log Collector que se están configurando. Navegue a `/var/netwitness/logcollector/runtime/identity-feed` y verifique que los archivos `Identity_deploy` se completen con los datos.



c. Abra un navegador web (se recomienda usar un navegador distinto de Internet Explorer) e inicie sesión en la interfaz de REST de Log Collector. Use las credenciales administrativas cuando inicie sesión. Por ejemplo, si la dirección IP de su Log Collector es 192.168.99.66, entonces la dirección URL sería:

- SSL no habilitado: **http://192.168.99.66:50101/event-processors**
- SSL habilitado: **https://192.168.99.66:50101/event-processors**

La pantalla del navegador debe verse así:

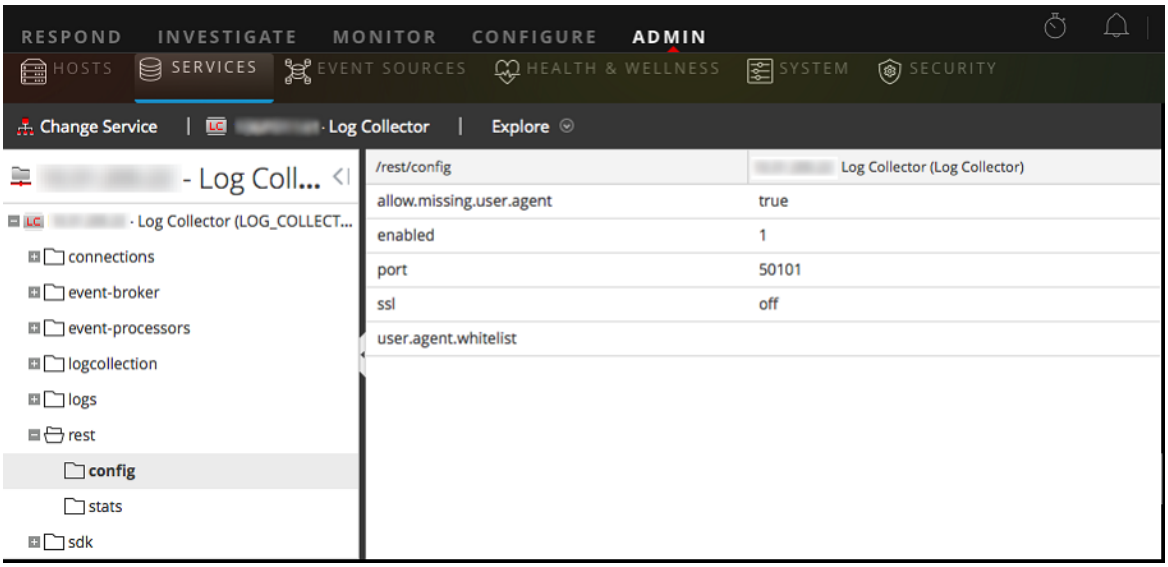


Observe que la pantalla contiene el nombre del feed de identidad del feed que creó anteriormente (`infonetd_domain`, en este ejemplo).

Para que el feed de identidad funcione correctamente, el puerto 50101 debe estar activo en el Log Collector y debe determinar si el cifrado SSL está activo.

d. Vaya a **ADMINISTRAR > Servicios > *<Log Collector que se debe configurar>***  **> Ver > Explorar**.

e. En el panel izquierdo, expanda **rest > configuración**.



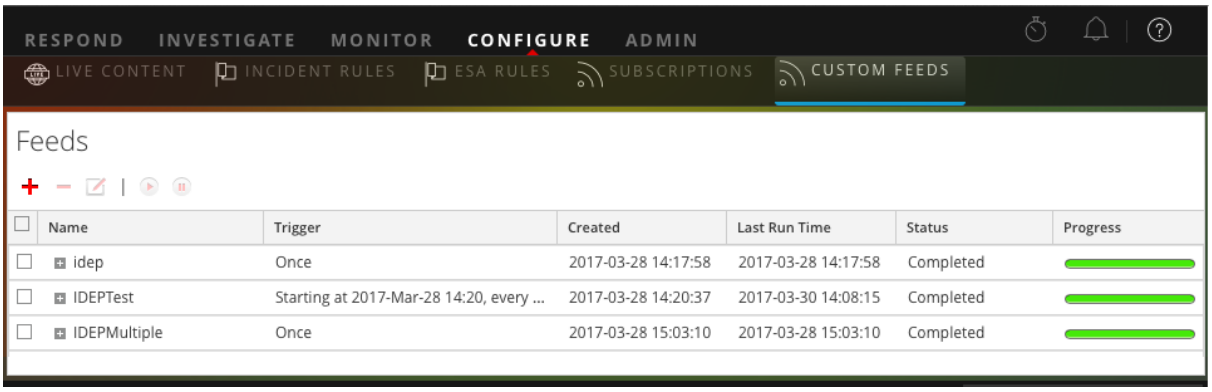
Para que REST esté activo, **habilitado** se debe configurar en **1**.

f. Observe el valor para **ssl**. Si SSL debe estar habilitado para su ambiente, se debe configurar en **activado**.

Nota: Si cambió la configuración para la opción **habilitado** o la opción **ssl**, debe reiniciar el servicio Log Collector antes de continuar.

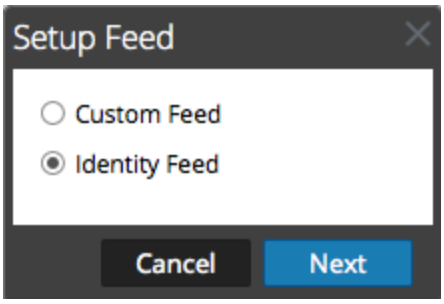
3. Vaya a **CONFIGURAR > Feeds personalizados**.

Se muestra el cuadro de diálogo Feeds.



4. En la barra de herramientas, haga clic en +.

   Se muestra el cuadro de diálogo Configurar feed.



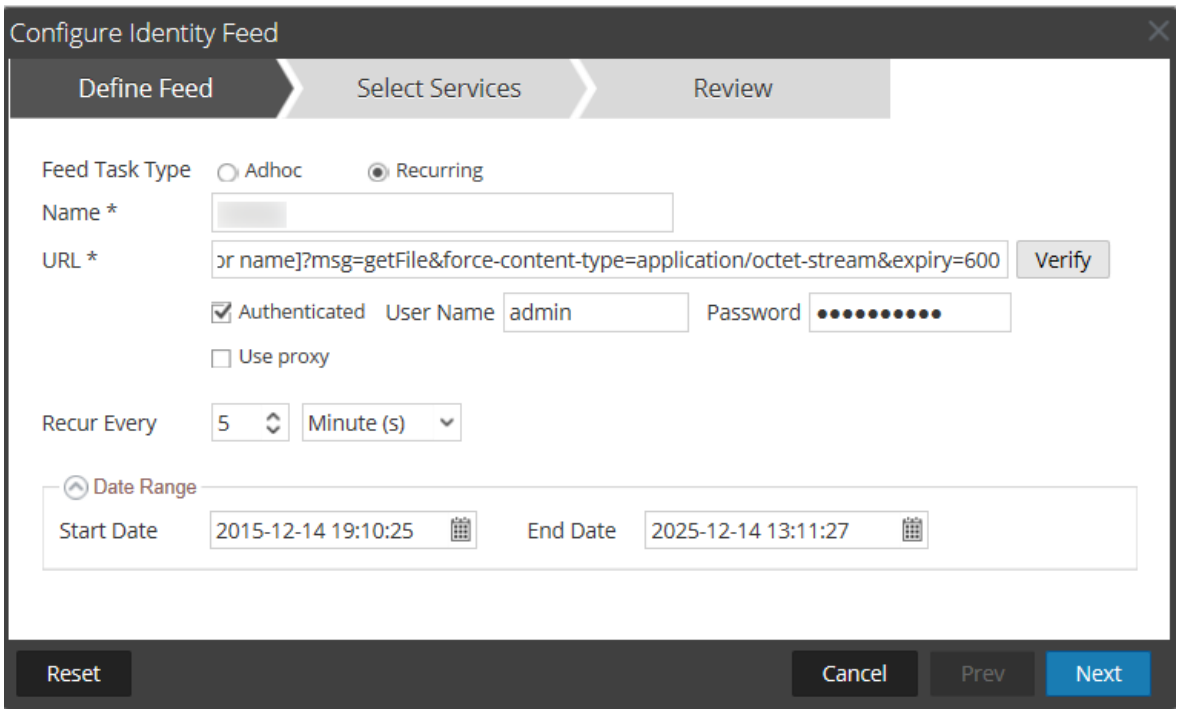
5. Asegúrese de que la opción **Feed de identidad** esté seleccionada y haga clic en **Siguiente**.

   El panel Configurar feed de identidad se abre con la pestaña **Definir feed** abierta.

6. (Condicional) Puede crear un feed según demanda o recurrente.

   - Para definir una tarea de feed de identidad según demanda que se ejecute una vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed**, escriba el **Nombre** del feed y, a continuación, busque y abra el feed.
   - Para definir una tarea recurrente de feed de identidad que se ejecuta de manera recurrente, seleccione **Recurrente** en el campo **Tipo de tarea de feed**.

     En el cuadro de diálogo **Definir feed** se incluyen los campos de un feed recurrente.



Nota: RSA NetWitness Platform verifica la ubicación en la cual está almacenado el archivo con el fin de que NetWitness Platform pueda comprobar el archivo más reciente automáticamente antes de cada recurrencia.

7. Rellene y verifique el campo URL.
   a. En el campo **URL**, escriba la dirección URL en la cual está ubicado el archivo de datos del feed. Esta es la interfaz de API REST que se configuró anteriormente. Asegúrese de contar con la siguiente información para construir la dirección URL:
      - La dirección IP del Log Collector que se usa para construir el archivo de feed de identidad.
      - El nombre de la línea de espera de identidad, como se configuró en el paso 2c.
      - Si SSL está habilitado o no en el puerto REST del Log Collector, como se configuró en el paso 2f.

      Puede construir este valor de la siguiente manera:

      - SSL habilitado: `https://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`
      - SSL no habilitado: `http://<LogCollector>:50101/event-processors/<ID Event processor name>?msg=getFile&force-content-type=application/octet-stream&expiry=600`

      Por lo tanto, si se usa el ejemplo anterior, el valor completo que debe ingresar en este campo es el siguiente:

```
http://192.168.99.66:50101/event-processors/infonetd_
domain?msg=getFile&force-content-type=application/octet-
stream&expiry=600?msg=getFile&force-content-
type=application/octet-stream&expiry=600
```

b. Para que la verificación de la dirección URL funcione correctamente, es importante que el servidor de interfaz del usuario de NetWitness Platform pueda acceder al puerto de API REST del Log Collector (50101). Esto se puede probar al acceder mediante el protocolo SSH al servidor de interfaz del usuario de NetWitness Platform. Una vez que esté ahí, ejecute el siguiente comando:

- SSL habilitado: `curl -vk https://<ip of log collector>:50101`
- SSL no habilitado: `curl -v http://<ip of log collector>:50101`

Si el comando `curl` no se conecta, entonces puede haber un problema de firewall de la red o de enrutamiento entre el servidor de interfaz del usuario de NetWitness Platform y el Log Collector.

Ejemplo de mala conexión:

```
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... No route to host
* couldn't connect to host
* Closing connection #0
curl: (7) couldn't connect to host
Example of Good connection:
* About to connect() to 192.168.99.66 port 50105 (#0)
* Trying 192.168.99.66... connected
* Connected to 192.168.99.66 (192.168.99.66) port 50105 (#0)
> GET / HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu)
libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18
libssh2/1.4.2
> Host: 192.168.99.66:50105
> Accept: */*
>
< HTTP/1.1 401 Unauthorized
< Content-Length: 71
< Connection: Keep-Alive
< Pragma: no-cache
< Expires: -1
< Cache-Control: no-cache, no-store, must-revalidate
< WWW-Authenticate: Basic realm="NetWitness"
```

```
< Content-Type: text/xml; charset=utf-8
<
<?xml version="1.0" encoding="utf-8"?>
<error>401 Unauthorized</error>
* Connection #0 to host 192.168.99.66 left intact
* Closing connection #0
```

8. La API REST requiere un nombre de usuario y una contraseña al intentar extraer el archivo `identity_deploy.csv` del Log Collector. Puede ser cualquier nombre de usuario y contraseña que estén disponibles en el propio servicio. Para obtener más información, consulte el tema "Vista Seguridad de servicios" en la *Guía de hosts y servicios*.

   Para ver las cuentas que están disponibles, vaya a **ADMIN > Servicios > <Log Collector que se debe configurar> > Acciones > Ver > Seguridad**.

   En la tabla Usuarios, verá todos los usuarios que se pueden usar en este paso. Se sugiere crear una cuenta de usuario separada específicamente para esta configuración, que no se usa en ninguna otra parte en el ambiente para brindar mayor seguridad. Para obtener detalles, consulte "Agregar un usuario y asignar una función" en la *Guía de administración de usuarios y seguridad del sistema*. (Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.)

9. Para definir el intervalo de recurrencia, puede realizar alguna de las siguientes acciones:

   - Especifique la cantidad de minutos, horas o días entre cada recurrencia del feed.
   - Para definir el rango de días para la ejecución recurrente del feed, especifique la hora y la **Fecha inicial** y la hora y la **Fecha de finalización**.

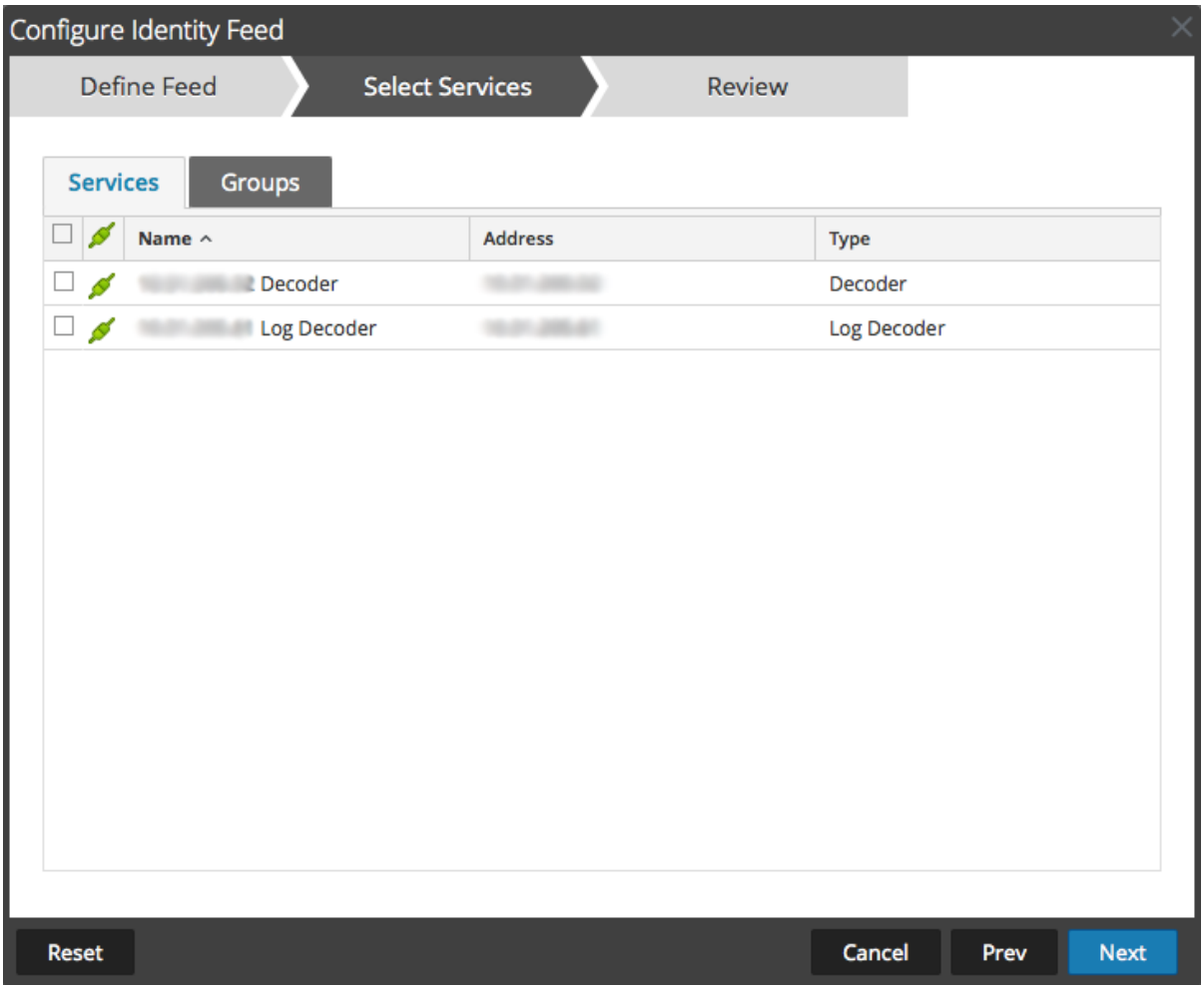
10. Si usa el cifrado SSL, debe instalar el certificado SSL de API REST para el Log Collector en el servidor de interfaz del usuario de NetWitness Platform. Para obtener más información, consulte Importar el certificado SSL.

    Si, después de importar el certificado SSL, aún falla la verificación de la dirección URL, consulte No se puede verificar la dirección URL del feed de identidad.

11. Haga clic en **Verificar** para verificar su configuración de feed de identidad antes de continuar con el cuadro de diálogo Seleccionar servicios.

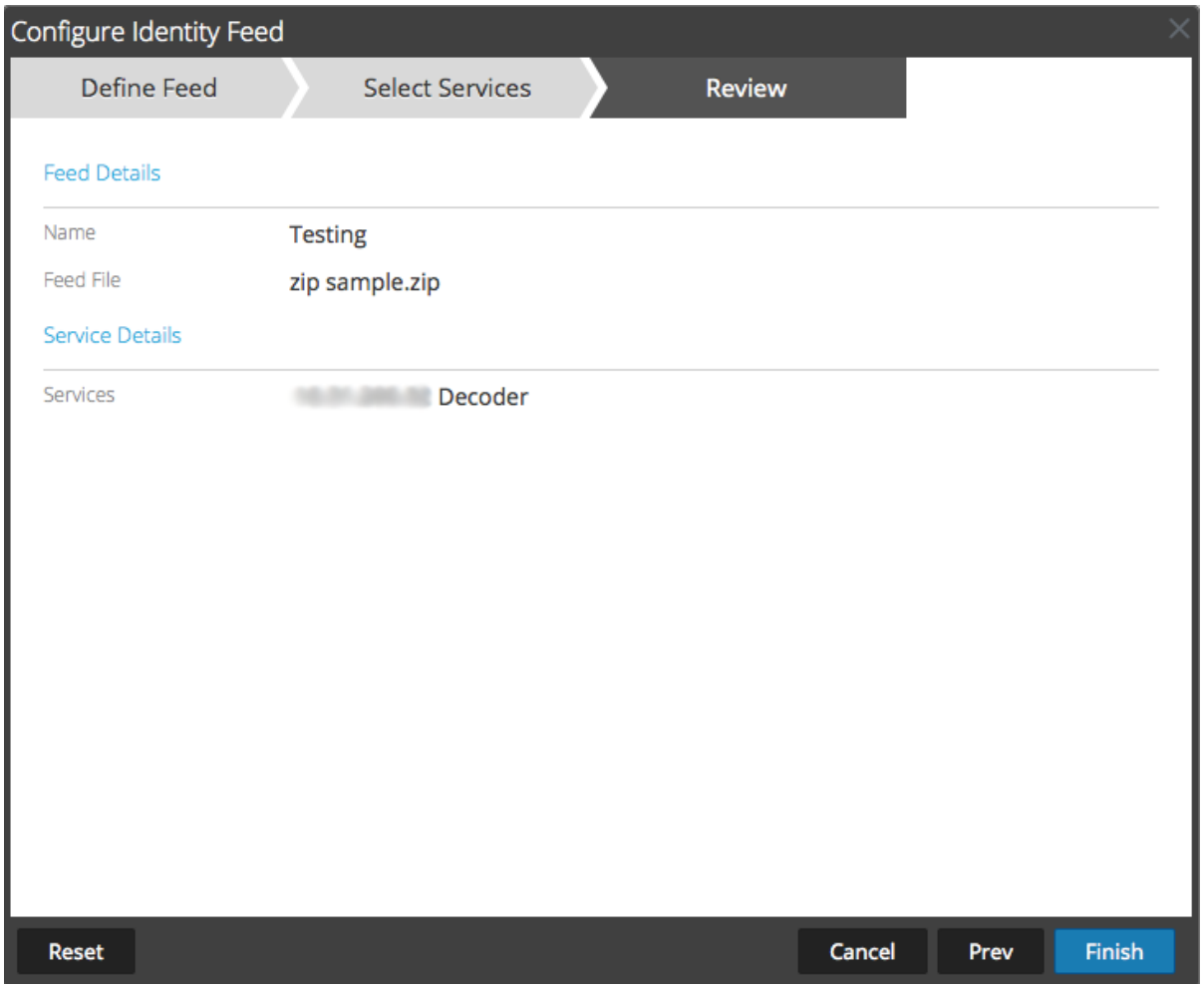
12. Haga clic en **Siguiente**.

    Se muestra el cuadro de diálogo Seleccionar servicios.



13. Para identificar los servicios en los cuales se implementará el feed, seleccione uno o más Decoders y Log Decoders, y haga clic en **Siguiente**.
14. Haga clic en la pestaña **Grupos**, seleccione un grupo y haga clic en **Siguiente**.

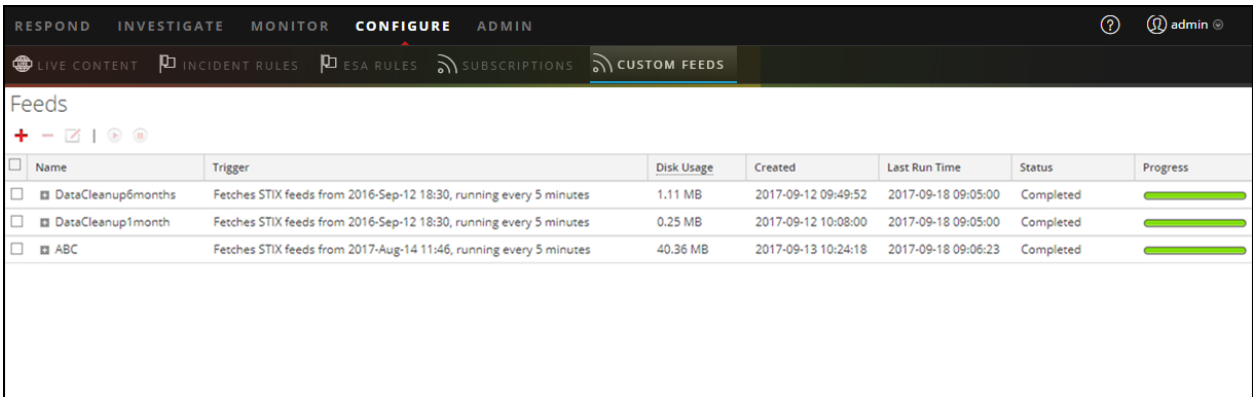
    Se muestra el cuadro de diálogo Revisar.



Nota: Si un grupo de dispositivos con Decoders y Log Decoders se usa para crear feeds personalizados o recurrentes y se puede eliminar este grupo, puede editar el feed y agregarle un grupo nuevo.

15. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
    - Hacer clic en **Cancelar** para cerrar el asistente sin guardar la definición del feed.
    - Hacer clic en **Restablecer** para borrar los datos del asistente.
    - Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).
    - Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).
16. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.

Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, el feed y el archivo de token correspondiente aparecen en la cuadrícula Feed y la barra de progreso muestra que se completó la tarea. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles tuvieron éxito.



Importar el certificado SSL

Si SSL está configurado en el Log Collector del feed de identidad, siga estos pasos para importar el certificado SSL del Log Collector al almacenamiento de claves del servidor de interfaz del usuario de NetWitness Platform. Si este certificado no se importa, el servidor de interfaz del usuario de NetWitness Platform no podrá extraer el archivo de feed de identidad del Log Collector.

1. Para extraer el certificado SSL del Log Collector, acceda mediante el protocolo SSH al servidor de interfaz del usuario de NetWitness Platform y ejecute el siguiente comando:

   ```
   echo -n | openssl s_client -connect <HOST>:<PORT> | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/<SERVERNAME>.cert
   ```

   Este comando guarda el certificado SSL en `/tmp/<SERVERNAME>.cert`.

   Por ejemplo:

   ```
   echo -n | openssl s_client -connect 192.168.99.66:50101 | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /tmp/logcollector.cert
   ```

2. Para importar el certificado SSL al servidor de interfaz del usuario de NetWitness Platform, acceda mediante el protocolo SSH al servidor de interfaz del usuario y ejecute el siguiente comando:

   ```
   keytool -importcert -alias <name an alias for the cert> -file <the cert file pathname> -keystore /etc/pki/java/cacerts
   ```

   Por ejemplo:

   ```
   keytool -importcert -alias logcollector01 -file /tmp/logcollector.cert -keystore /etc/pki/java/cacerts
   ```

3. El sistema solicita una contraseña. Ingrese la contraseña para el almacenamiento de claves del servidor de interfaz del usuario de NetWitness Platform, no para el almacenamiento de claves de jetty. La contraseña predeterminada es **changeit**.

4. Reinicie **jettysrv** para permitir que jetty lea el nuevo certificado en el almacenamiento.

No se puede verificar la dirección URL del feed de identidad

Si no puede verificar la dirección URL del feed de identidad y está usando SSL, asegúrese de haber seguido los pasos descritos en Importar el certificado SSL.

Si aún hay problemas, es posible que el nombre interno del certificado no coincida con el nombre de host del Log Collector. El siguiente procedimiento comprueba esto.

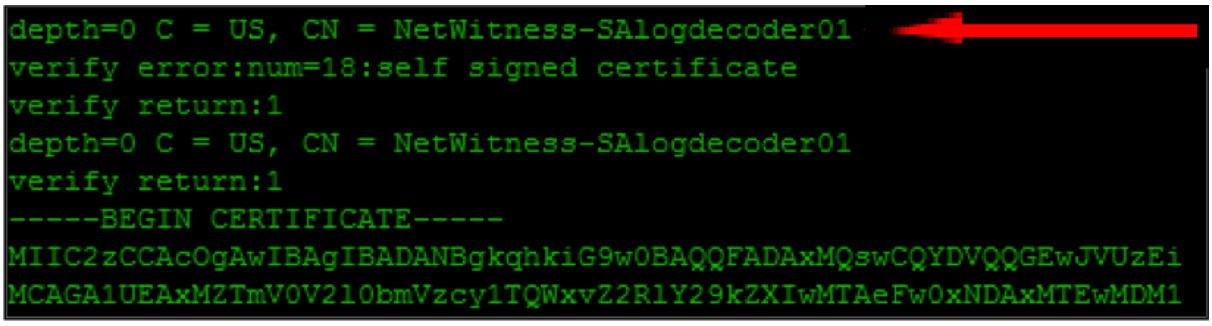
1. Acceda mediante el protocolo SSH al servidor de interfaz del usuario de NetWitness Platform.
2. Ejecute el siguiente comando para generar el nombre de CN del certificado SSL:

   ```
   echo -n | openssl s_client -connect <log decoder>:50101 | sed -ne
   '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

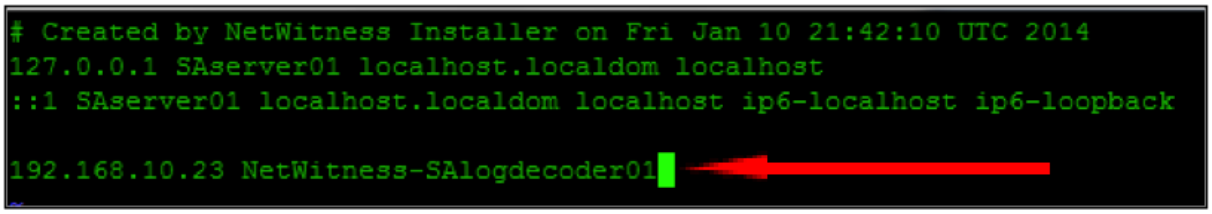
   Ejemplo:

   ```
   echo -n | openssl s_client -connect salogdecoder01:50101 | sed -ne
   '/BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p'
   ```

3. Recupere el nombre de CN del certificado SSL.

4. Edite el archivo `/etc/hosts` y agregue la dirección IP y el nombre de CN al archivo.

5. Reinicie el servicio de red en el dispositivo.
6. Confirme que el nombre colocado en el archivo **/etc/hosts** se use en lugar del nombre de dominio calificado o de la dirección IP en la dirección URL del feed de identidad.
7. Vuelva a verificar la dirección URL del feed de identidad.

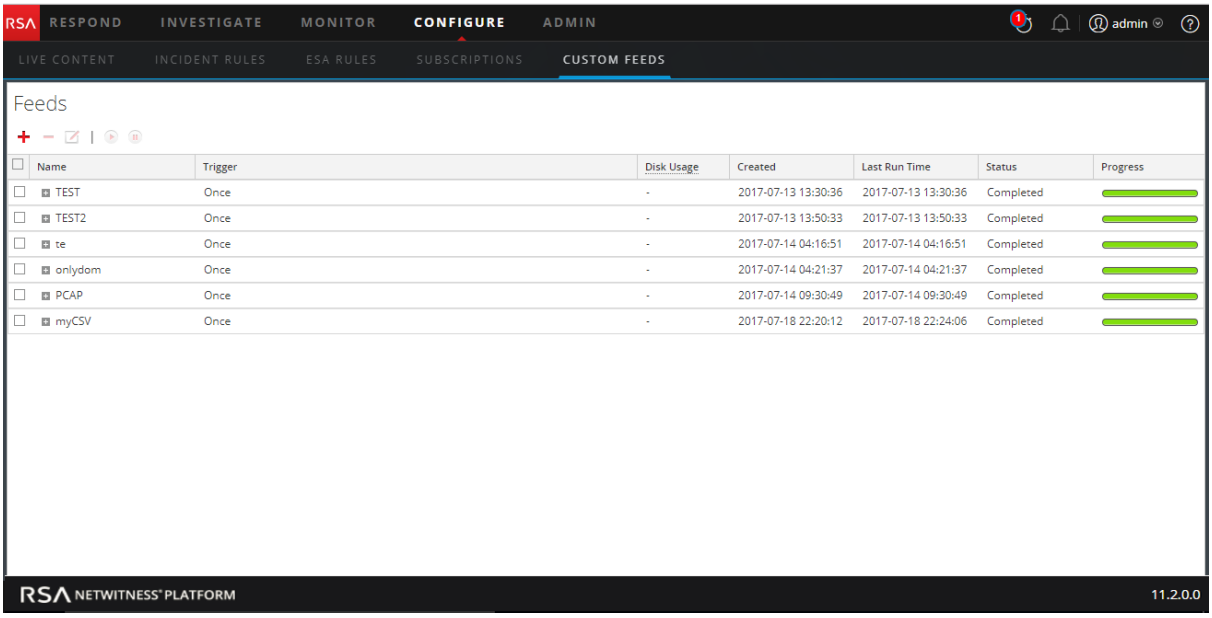
Editar, cargar o quitar un feed

Puede cargar un feed, editar un feed existente o quitar un feed.

Para editar un feed existente:

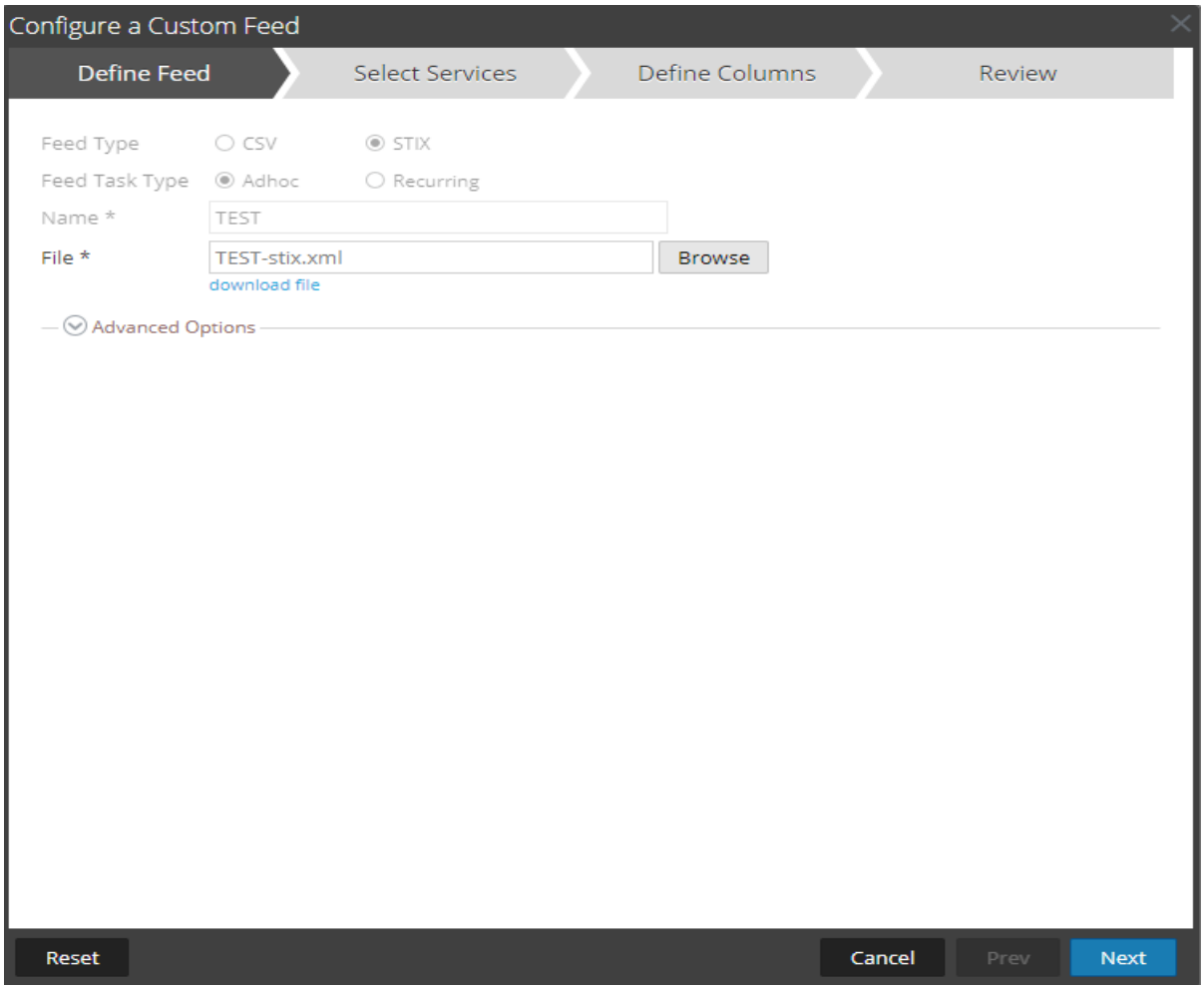
1. Vaya a **CONFIGURAR > Feeds personalizados**.

   Se muestra la vista Feeds.



2. En la barra de herramientas, seleccione un feed y haga clic en .

   Se abre el panel Configurar feed personalizado o Configurar feed de identidad en el asistente Feed personalizado.



3. Si desea editar el archivo de feed:
   a. Haga clic en **Descargar archivo**.

      En el caso de un feed de identidad, se descarga el archivo .zip. En el caso de los feeds personalizados, se descarga el archivo .csv o .xml en el sistema de archivos local. En el caso de un feed STIX, se descarga el archivo .xml en el sistema de archivos local.

   b. Edite y guarde el archivo.
   c. En la pestaña **Definir feed**, busque y abra el archivo editado.
4. Edite cualquier otro parámetro en las pestañas **Definir feed**, **Seleccionar servicios** y **Definir columnas** que se aplique al tipo de feed.
5. Antes de hacer clic en **Finalizar**, puede hacer lo siguiente:
   - Hacer clic en **Cancelar** para cerrar el asistente sin guardar los cambios.
   - Hacer clic en **Restablecer** para borrar los datos del asistente.
   - Hacer clic en **Siguiente** para ver el formulario siguiente (si no se encuentra en el último formulario).

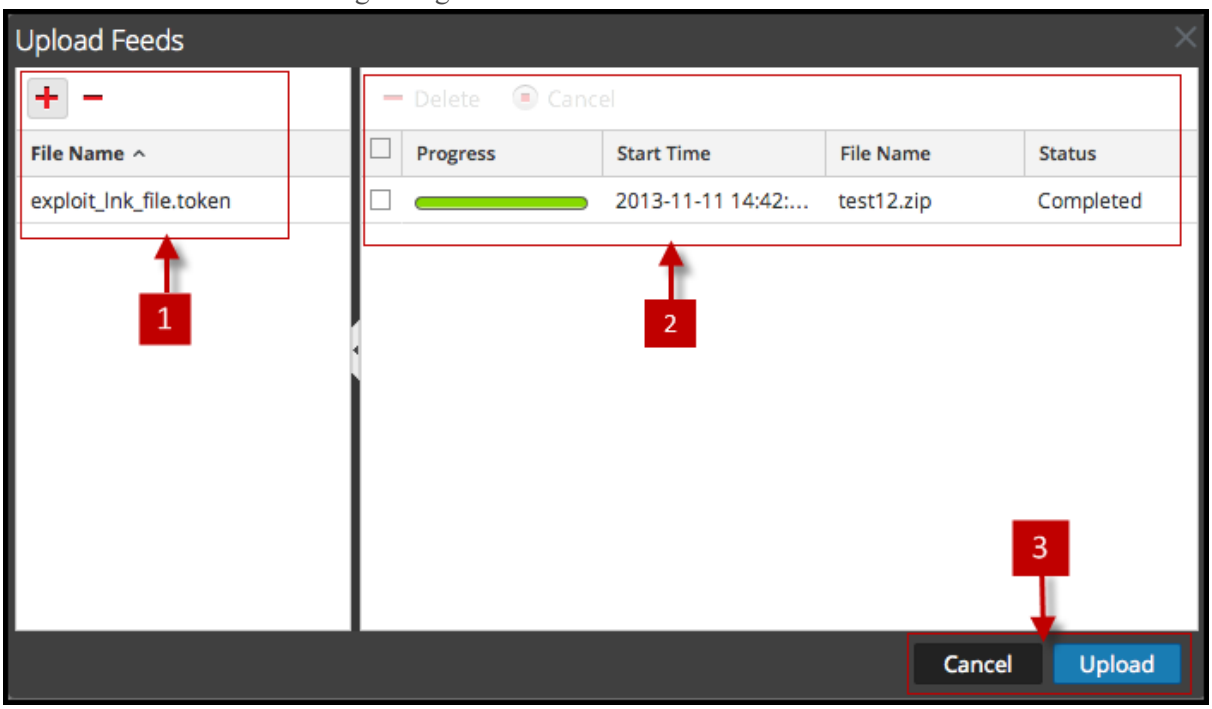
- Hacer clic en **Anterior** para ver el formulario anterior (si no se encuentra en el primer formulario).

6. En la pestaña **Revisión**, revise la información del feed y, si los datos son correctos, haga clic en **Finalizar**.

El feed se vuelve a crear con el archivo actualizado y las nuevas especificaciones del feed. El feed se agrega a la lista Feeds y la barra de progreso rastrea la finalización de la tarea. Después de crear correctamente el archivo de definición del feed, el asistente Crear feed se cierra, y el feed y el archivo de token correspondiente aparecen en la lista Feeds. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles se ejecutaron correctamente.

Para cargar un feed a un Decoder o Log Decoder:

1. Vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un servicio y haga clic en > **Ver** > **Configuración**.
   La vista Configuración de servicios se muestra con la pestaña General abierta.
3. Seleccione la pestaña **Feeds**.
4. En la barra de herramientas de la pestaña Feeds, haga clic en Upload.
   Se muestra el cuadro de diálogo Cargar feeds.

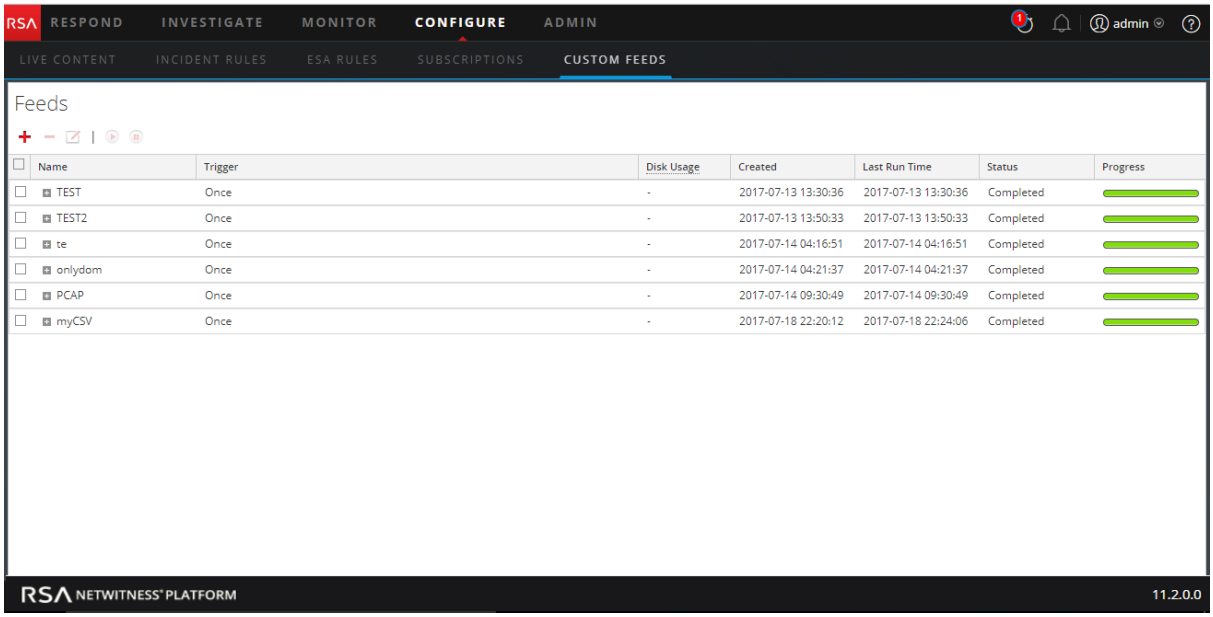


5. En la cuadrícula **Archivo**, haga clic en + y seleccione un archivo de feed. Los archivos compatibles son *.feed, *.token y *.filter.
6. Seleccione el archivo de feed de la lista **Archivos** y haga clic en **Cargar**.
   La lista Trabajo de carga se actualiza para mostrar el progreso y el estado del feed cargado.

Para eliminar un feed:

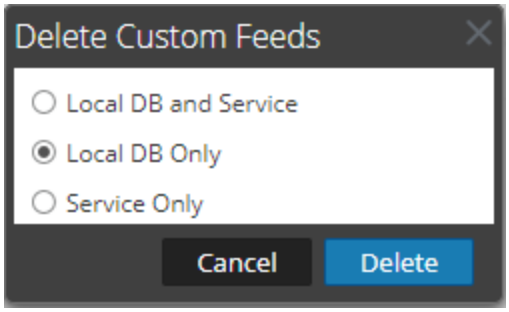
1. Vaya a **CONFIGURAR > Feeds personalizados**.

   Se muestra la vista Feeds personalizados.



2. En la barra de herramientas, seleccione un feed y haga clic en .

   Se muestra el cuadro de diálogo Eliminar feeds personalizados.



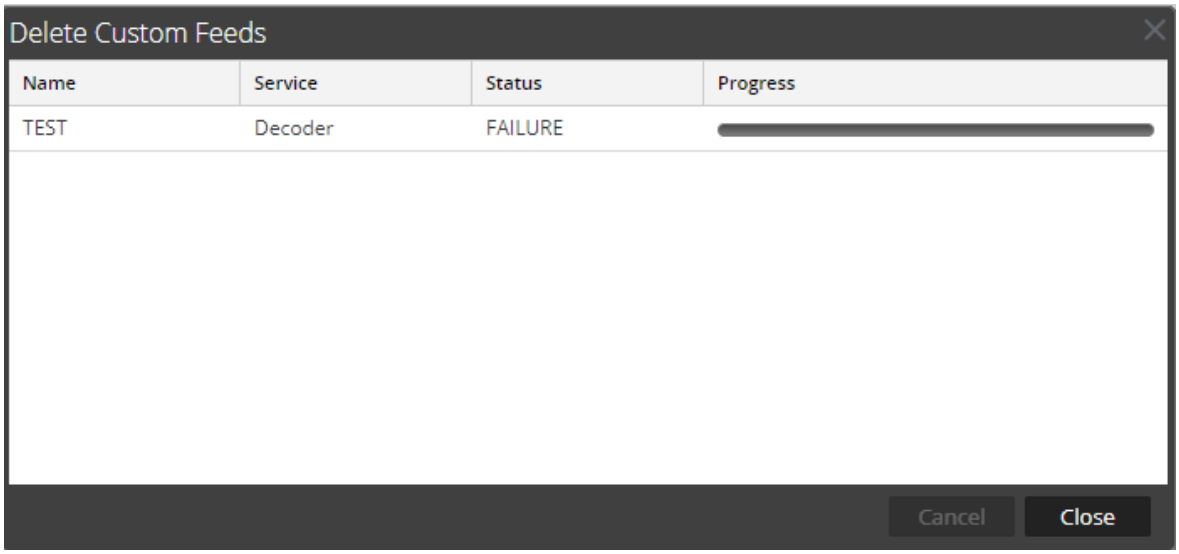
   Puede seleccionar una de las siguientes opciones para eliminar el feed:

   - Si opta por eliminar el feed desde **Base de datos local y servicio**, este se elimina del servicio y de la computadora local de NetWitness Platform. El feed eliminado ya no se verá en la interfaz del usuario de NetWitness Platform.
   - Si opta por eliminar el feed desde **Solo base de datos local**, este se elimina de la computadora local de NetWitness Platform. El feed eliminado no se verá en la interfaz del usuario de NetWitness Platform; sin embargo, la última versión implementada de los feeds estará presente en el servicio. Los feeds no implementados se eliminarán permanentemente.
   - Si opta por eliminar el feed desde **Solo servicio**, el feed se elimina del servicio. El feed eliminado aparecerá en la interfaz del usuario de NetWitness Platform y se puede implementar nuevamente

3. Seleccione dónde desea eliminar el feed y haga clic en **Eliminar**.

Se muestra un cuadro de diálogo de advertencia.

4. Haga clic en **sí** para confirmar que desea eliminar el feed desde las áreas seleccionadas.
   - Si escoge eliminar el feed desde **Solo base de datos local**, el feed se elimina.
   - Si decide eliminar el feed desde **Base de datos local y servicio** o **Solo servicio**, se muestra la vista Eliminar feeds personalizados, donde aparece el progreso de la eliminación del servicio.



Crear claves de metadatos personalizados mediante un feed personalizado

En este tema se proporciona información sobre cómo agregar claves de metadatos personalizados mediante un feed personalizado en el Log Decoder.

Puede crear claves de metadatos personalizados para recuperar datos, para investigar y analizar los registros y paquetes. Las claves de metadatos personalizados permiten agregar un contexto de enriquecimiento para los datos de paquetes y registros. En este documento se destacan los cambios en la configuración necesarios para reflejar las claves de metadatos personalizados en el esquema de Concentrator, ESA, Archiver, Warehouse Connector y Reporting Engine.

El siguiente es un ejemplo de creación de la clave de metadatos personalizados en el Log Decoder. En este escenario, una organización desea rastrear la ubicación de un recurso, como una impresora. Por lo tanto, se introduce una clave de metadatos personalizados **source location**, la cual indica la ubicación del recurso, por ejemplo, la Impresora1 que se encuentra en el "Ala A del quinto piso".

Nota: También se pueden crear claves de metadatos personalizados en Decoder. Seleccione el archivo `index-decoder-custom.xml` cuando cree metadatos personalizados en el Decoder.

Agregar una clave de metadatos personalizados en el Log Decoder

Para agregar claves de metadatos personalizados mediante un feed personalizado:

1. Vaya a **ADMIN** > Servicios**.**
2. Seleccione un servicio Log Decoder y haga clic en > **Ver** > **Configuración** > pestaña **Archivos** > **index-logdecoder-custom.xml.**

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexNone"
name="location.src" format="Text"/>
 </Language>
```

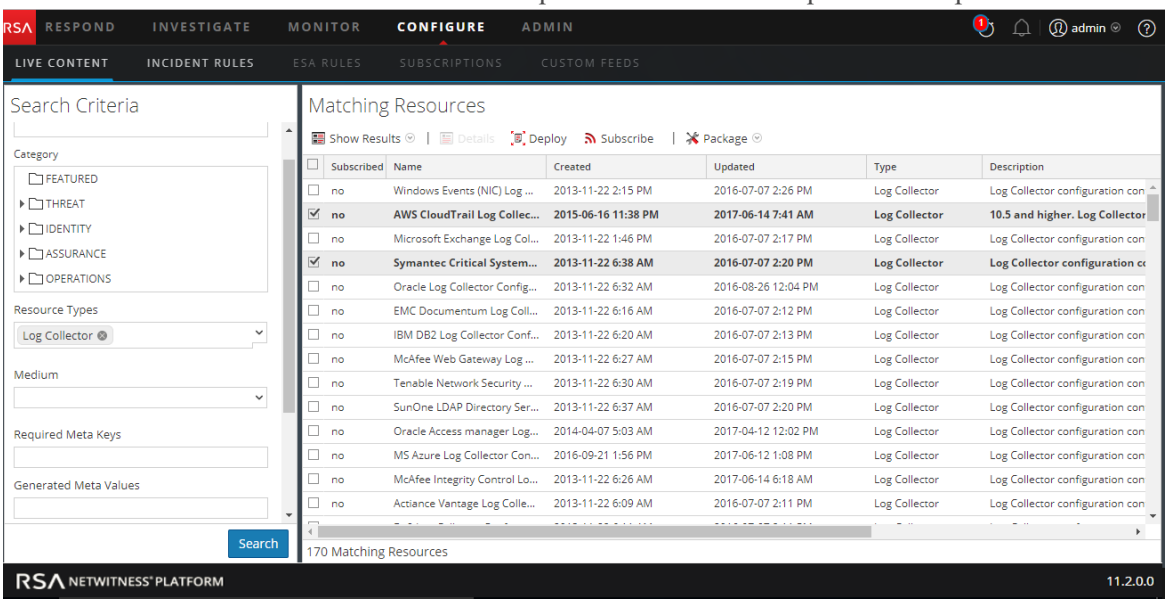
3. Reinicie el servicio Log Decoder. En la vista Servicios, haga clic en > **Reiniciar**.

Implementar un feed de Log Decoder en Live

Para implementar el feed en el ambiente Live:

1. Vaya a **CONFIGURAR > Contenido de Live.**
2. Seleccione un grupo de recursos o un paquete de recursos creado previamente. Para seleccionar un recurso o un grupo de recursos:
   a. En la **vista Buscar en Live,** navegue por el recurso de Live (por ejemplo, busque el tipo de recurso **Log Collector**).
   b. En el panel **Coincidencias de recursos**, seleccione **Mostrar resultados > Cuadrícula**.

c. Seleccione la casilla de verificación de la izquierda o los recursos que desee implementar.

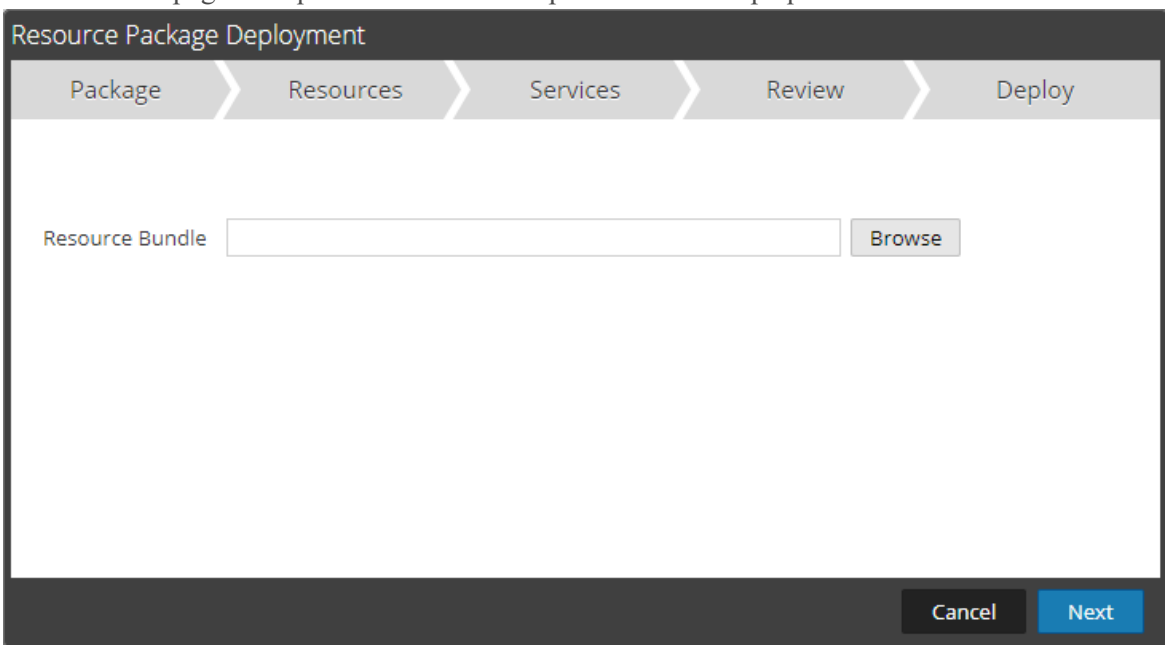


d. En la barra de herramientas Coincidencias de recursos, haga clic en 

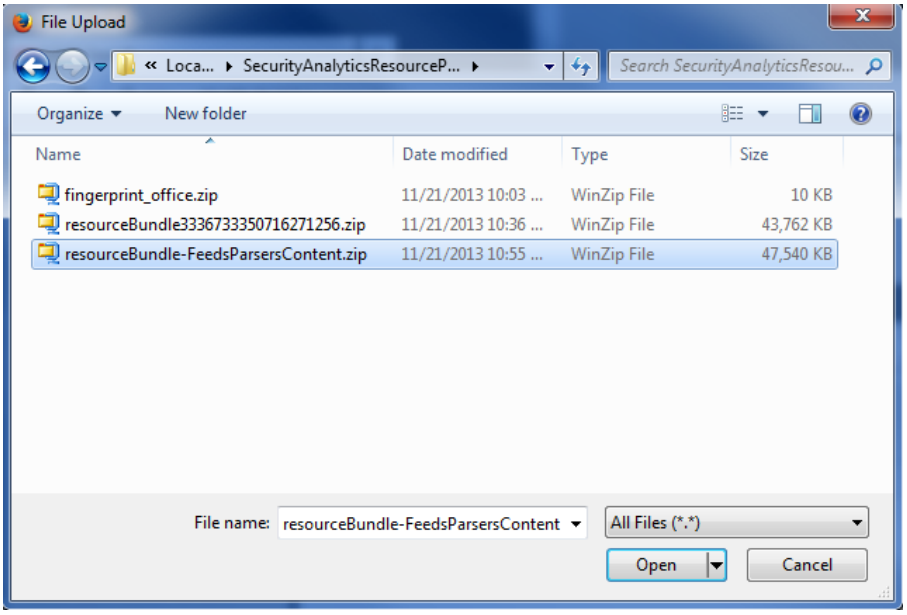
.

3. Para seleccionar un paquete de recursos para implementar:

a. En la vista **Buscar en Live**, barra de herramientas **Coincidencias de recursos**, seleccione **Paquete** > **Implementar**:
Se muestra la página Paquete del asistente Implementación de paquete de recursos.



b. Haga clic en **Navegar** y seleccione un paquete de la red (por ejemplo **resourceBundle-FeedsParsersContent.zip**).



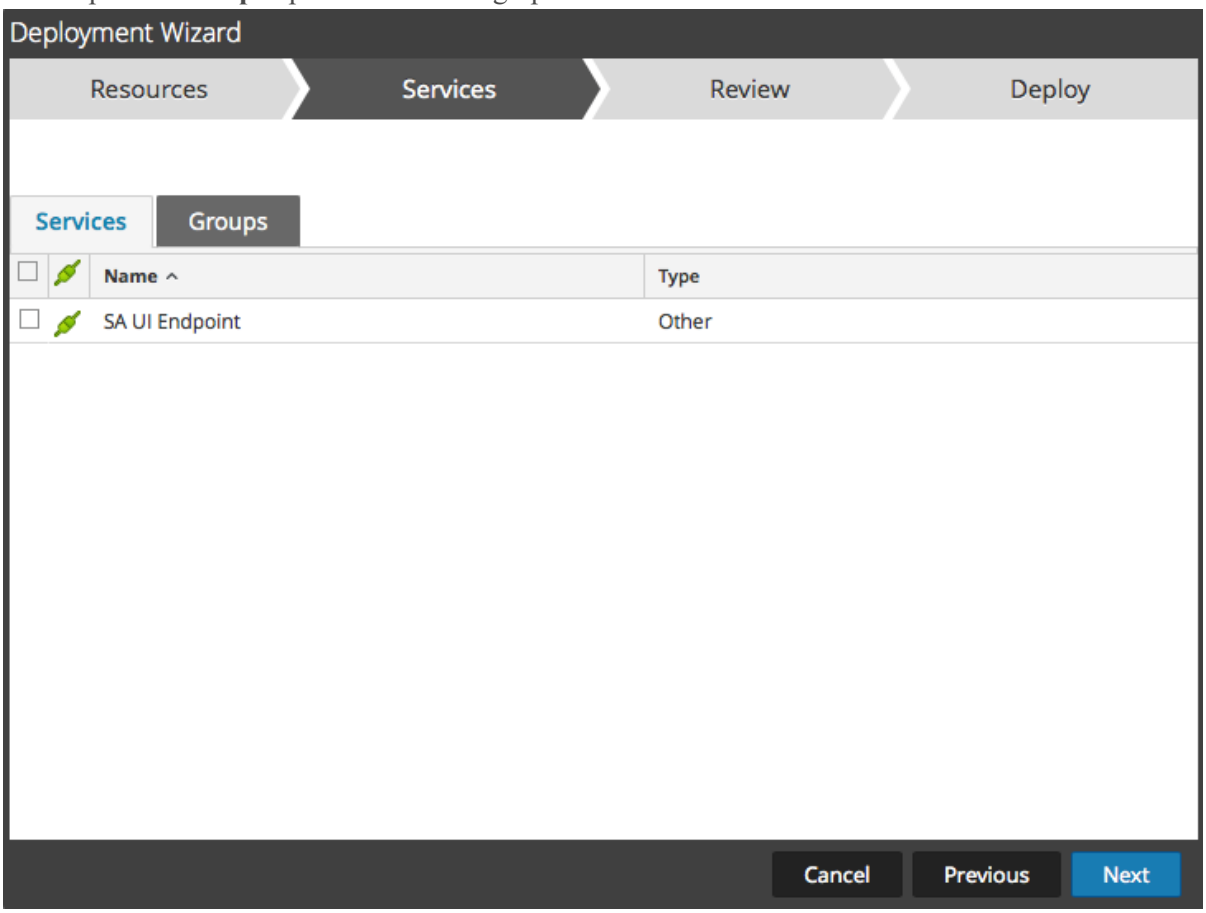
c. Haga clic en **Abrir.**
En este punto, si está implementando un paquete o un grupo de recursos, se abre el Asistente de implementación y se muestra la página Recursos.

3. Haga clic en **Siguiente**.
Se muestra la página **Servicios**, la cual tiene dos pestañas, **Servicios** y **Grupos**. Estas proporcionan una lista de servicios y grupos de servicios que se configuran en Administration > vista Servicios. Las columnas son un subconjunto de las columnas disponibles en la vista Servicios.

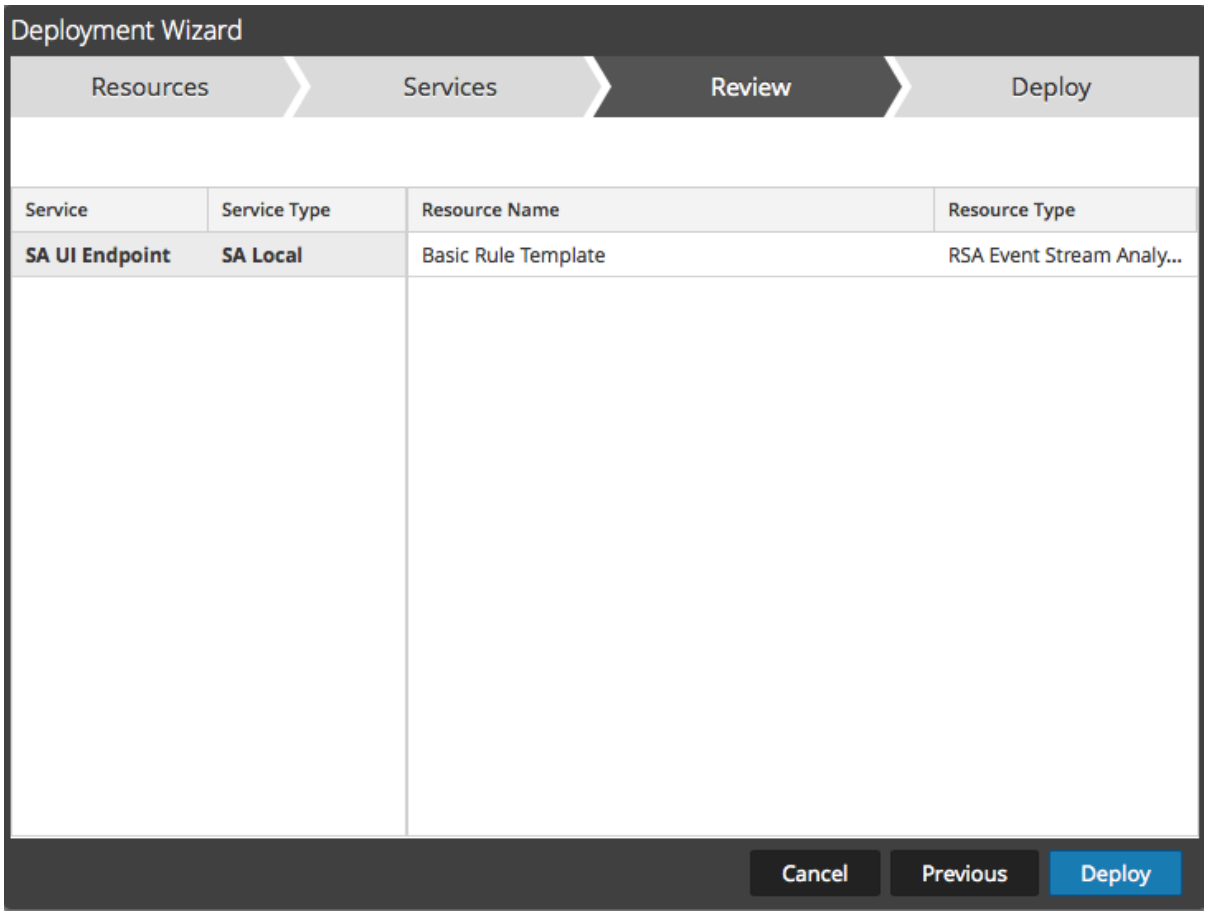
Nota: El servidor de Live es "inteligente" acerca de cómo implementar recursos en servicios. Por ejemplo, no implementa recursos que tienen un medio de paquetes en ningún Log Decoder. Esto significa que solo los recursos de contenido aplicable se implementan en cada servicio.

4. Seleccione los servicios en los cuales desea implementar el contenido. Puede seleccionar cualquier combinación de servicios y grupos de servicios.
Use la pestaña **Servicios** para seleccionar servicios individuales, la lista de servicios y grupos de servicios que se configuran en la vista Servicios de Admin.

Use la pestaña **Grupos** para seleccionar grupos de servicios.

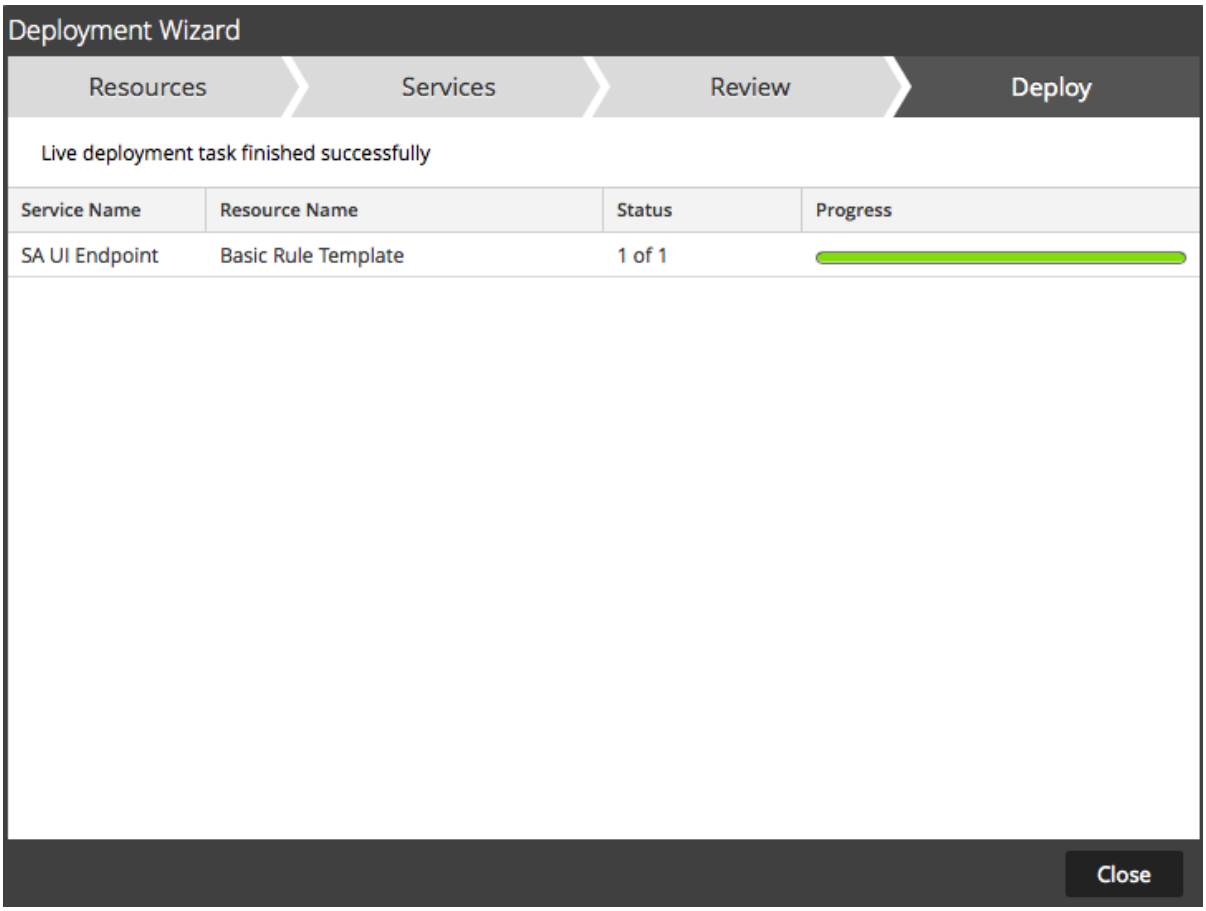


5. Haga clic en **Siguiente**.
   Se muestra la página **Revisión**.

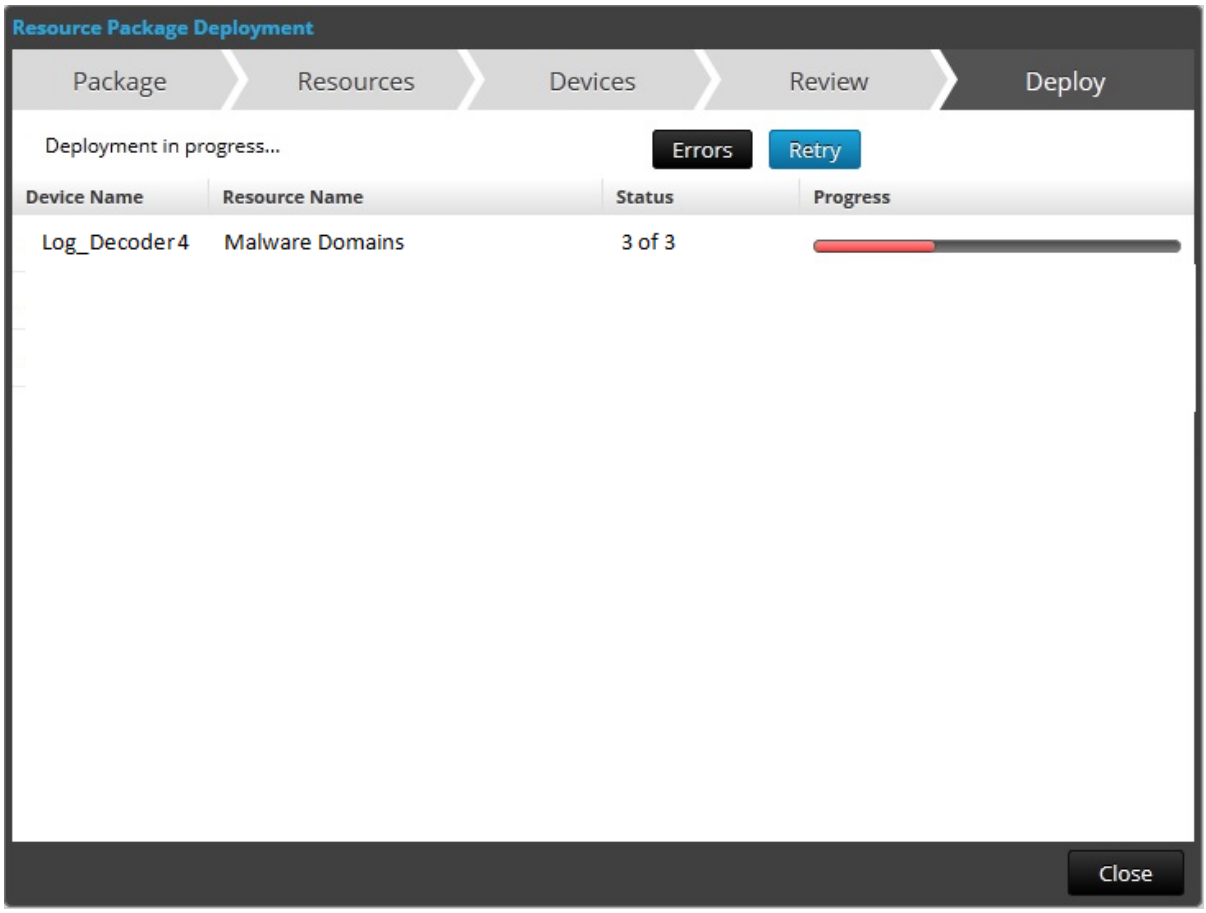


Asegúrese de haber seleccionado los recursos correctos y los servicios en los cuales desea implementarlos.

6. Haga clic en **Implementar**.
   Se muestra la página **Implementar**. La barra de progreso se vuelve verde cuando los recursos se implementan correctamente en los servicios seleccionados.



Si intenta implementar recursos y servicios que no son compatibles, NetWitness Platform muestra los botones Errores y Reintentar en los cuales puede hacer clic para revisar los errores y volver a intentar la implementación.



7. Haga clic en **Cerrar**.

Nota: Es necesario indexar la dirección IP de origen mediante la selección del tipo como "IP", ya que ip.src e ip.dst están en formato IPv4.

En este escenario, se agrega una clave de metadatos personalizados location.src (origen de la ubicación) mediante la indexación del nombre de host (alias.host). En este ejemplo, el nombre de host de la impresora se completa en la clave de metadatos "alias.host". Seleccione **alias.host** como clave de devolución de llamada y tipo de índice como "No IP" en el asistente de feed, como se muestra a continuación. En la sección Definir valores, seleccione la clave de metadatos personalizados en el menú desplegable.

Agregar la entrada de clave de metadatos personalizados en el archivo de índice de Concentrator

Para agregar la entrada de metadatos personalizados en el archivo de índice de Concentrator:

1. Vaya a **ADMIN** > **Servicios** > **Concentrator**.
2. Haga clic en ⚙ > **Ver** > **Configuración** > pestaña **Archivos** > **index-concentrator-**

custom.xml.

3. Agregue la entrada de clave de metadatos personalizados en el archivo de índice de Concentrator.

```
<Language>
 <?xml version="1.0" encoding="utf-8"?>
 <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location"  level="IndexValues"
name="location.src" format="Text"  valueMax="10000"
defaultAction="Open"/>
  </Language>
```

4. Para reiniciar el servicio Concentrator, en la vista Servicios, haga clic en > **Reiniciar**.

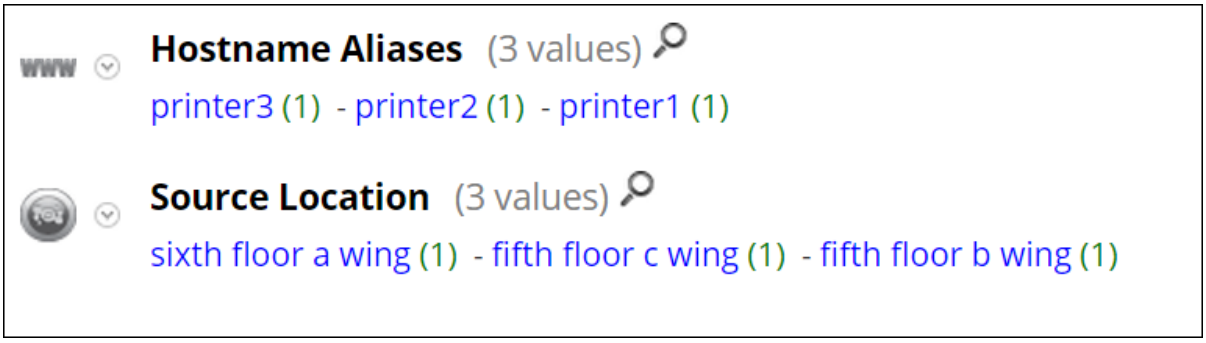
Nota: En el caso de Broker, el Broker deriva su índice del Concentrator desde el cual realiza la agregación. Por lo tanto, no es necesario crear metadatos personalizados en el Broker. Si no indexó la clave de metadatos en el Concentrator, el Broker no se mostrará en Investigation.

Investigar con la clave de metadatos personalizados

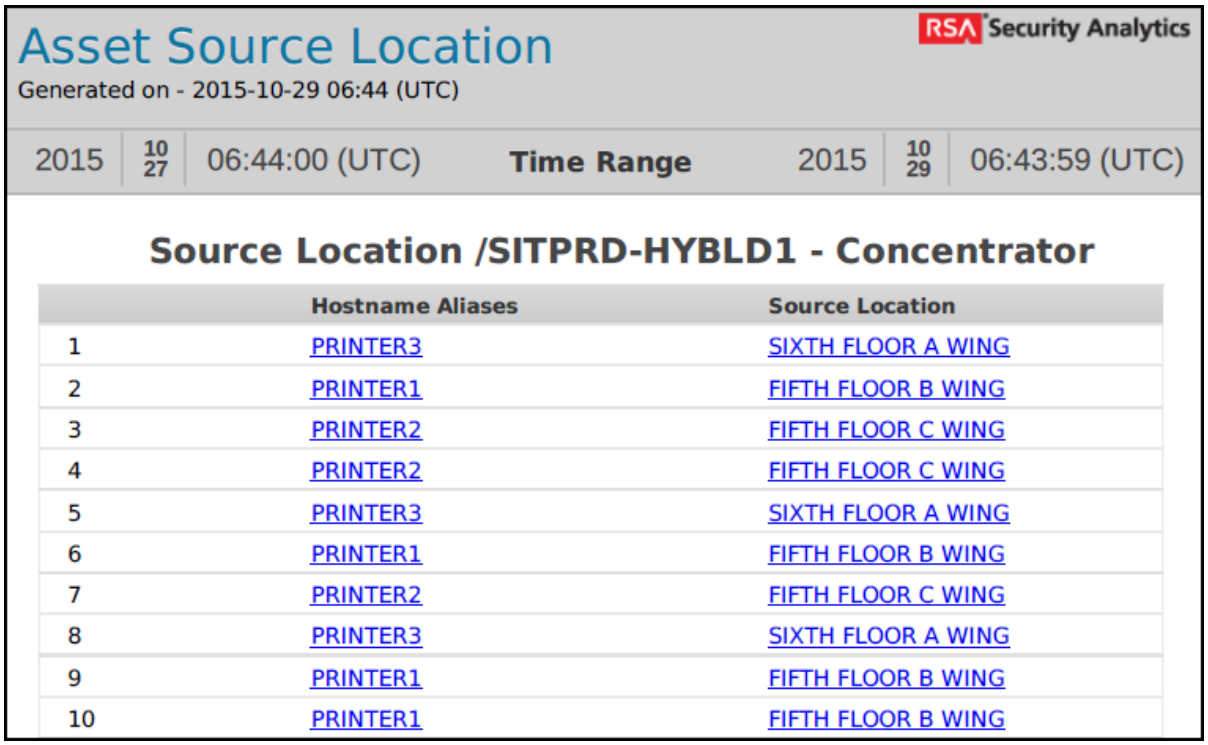
Nota: Debe cerrar e iniciar sesión en la interfaz del usuario de NetWitness Platform para poder ver la clave de metadatos personalizados en Investigation.

Para investigar con la clave de metadatos personalizados:

1. Vaya a **INVESTIGAR**. Se muestra un cuadro de diálogo con servicios para seleccionar.
2. Seleccione un servicio de Concentrator haga clic en **Navegar**.



El siguiente es un ejemplo de un informe ejecutado en el Concentrator.



Asset Source Location

RSA Security Analytics

Generated on - 2015-10-29 06:44 (UTC)

2015	10 27	06:44:00 (UTC)	Time Range	2015	10 29	06:43:59 (UTC)

Source Location /SITPRD-HYBLD1 - Concentrator

	Hostname Aliases	Source Location
1	PRINTER3	SIXTH FLOOR A WING
2	PRINTER1	FIFTH FLOOR B WING
3	PRINTER2	FIFTH FLOOR C WING
4	PRINTER2	FIFTH FLOOR C WING
5	PRINTER3	SIXTH FLOOR A WING
6	PRINTER1	FIFTH FLOOR B WING
7	PRINTER2	FIFTH FLOOR C WING
8	PRINTER3	SIXTH FLOOR A WING
9	PRINTER1	FIFTH FLOOR B WING
10	PRINTER1	FIFTH FLOOR B WING

Procedimientos adicionales

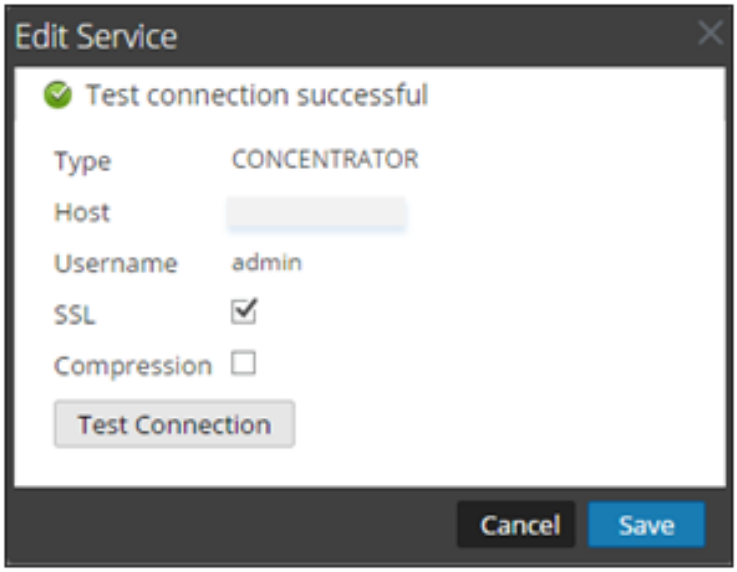
Se deben ejecutar los siguientes procedimientos si Warehouse Connector, Archiver, Reporting Engine y ESA están configurados.

Actualizar el esquema en ESA

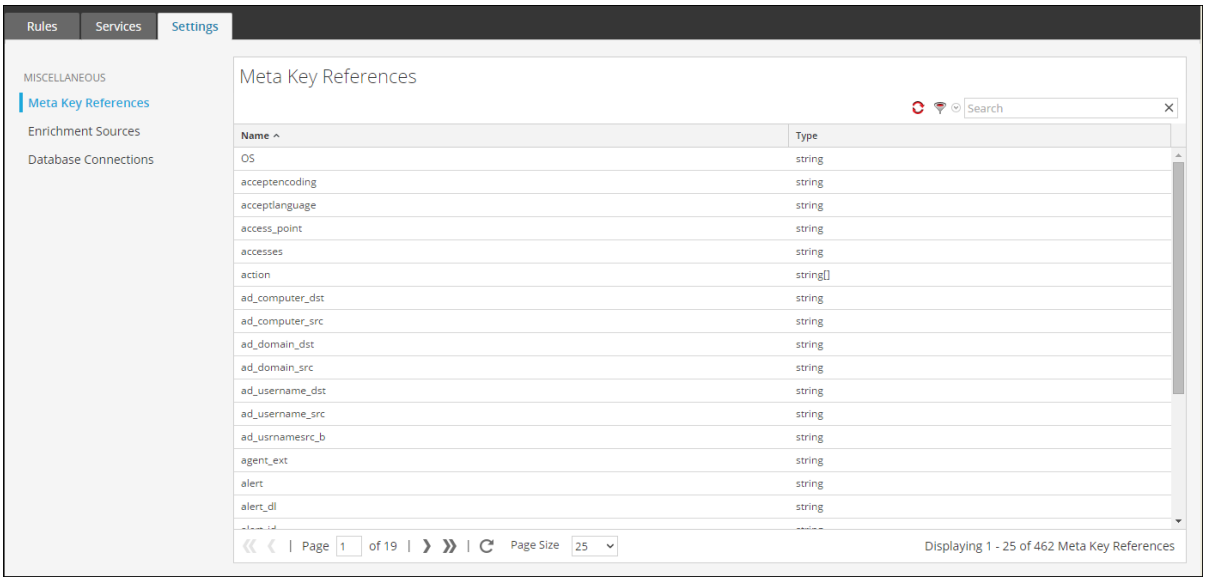
Antes de actualizar el esquema en ESA, la clave de metadatos personalizados se debe indexar en el Concentrator.

Para actualizar las reglas de ESA del esquema y poder usar las nuevas claves de metadatos personalizados:

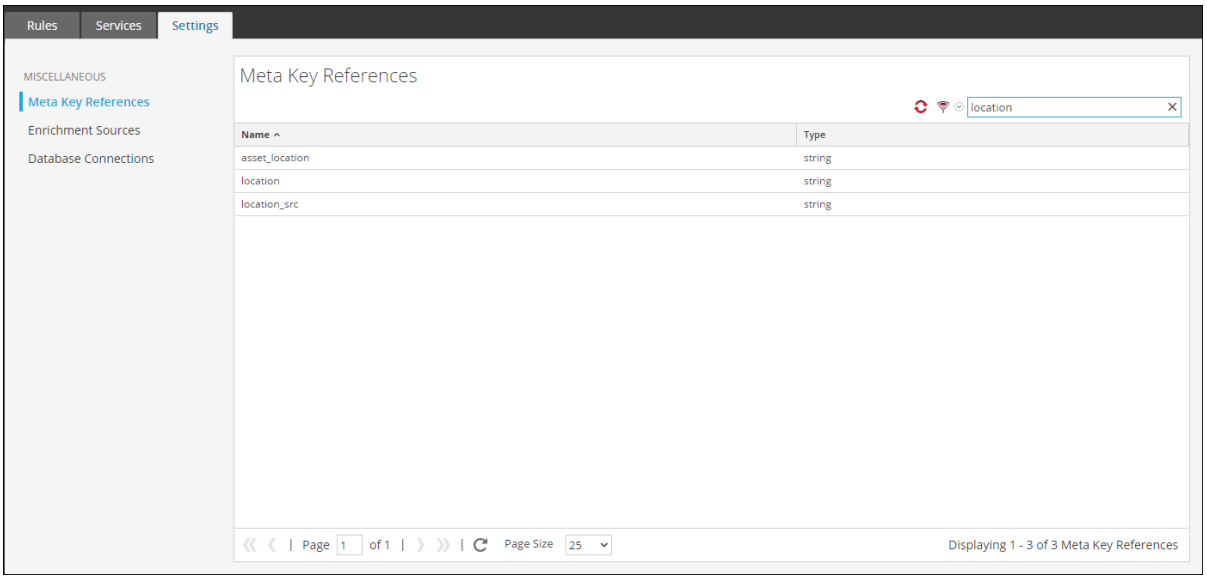
1. Vaya a **ADMIN** > **Servicios** > **ESA: Event Stream Analysis** > **Ver** > **Configuración**.
2. Edite el origen de datos de Concentrator.
3. Haga clic en **Probar conexión.**



4. Haga clic en **Guardar** una vez que la conexión se haya establecido correctamente.
5. Haga clic en **Aplicar**.
6. Navegue a **Configurar** > **Reglas de ESA** > **Ajustes de configuración**.



7. Haga clic en la pestaña **Buscar** y busque el nombre de la clave de metadatos personalizados. Se muestra el nombre y el tipo de la clave de metadatos personalizados.



Actualizar el esquema en Archiver

Si desea configurar Archiver con las nuevas claves de metadatos personalizados, debe actualizar el esquema de Archiver en Reporting Engine. Para actualizar el esquema de Archiver en Reporting Engine:

1. Vaya a **ADMIN** > **Servicios** > **Archiver**.
2. Seleccione > **Ver** > **Configuración** > **Archivos** > **index-archiver-custom.xml**.
3. Agregar la entrada de clave de metadatos personalizados en el archivo de índice de Archiver.

```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexValues"
name="location.src" format="Text"
  valueMax="10000" defaultAction="Open"/>
 </Language>
```

4. Para reiniciar el servicio de Archiver, haga clic en > **Reiniciar.**
   El esquema de Archiver se actualiza con la clave de metadatos personalizados.

Actualizar el esquema en Warehouse Connector

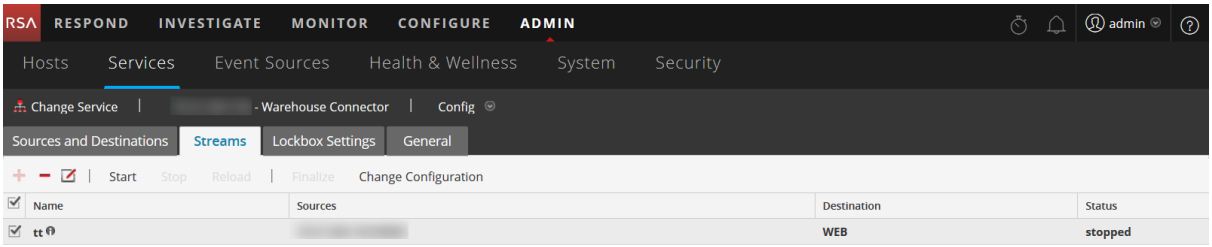
Si desea configurar Warehouse Connector con metadatos personalizados y utilizarlos en un informe de Warehouse Connector, debe actualizar el esquema de Warehouse Connector en Reporting Engine.

Si el Log Decoder o el Decoder en los cuales se agregó la clave de metadatos personalizados corresponden a uno de los orígenes en el flujo de Warehouse Connector, debe actualizar el esquema en el Warehouse Connector.

Para actualizar el esquema de Warehouse Connector en Reporting Engine:

1. Vaya a **ADMIN** > **Servicios** > **Warehouse Connector**.
2. Haga clic en > **Ver** >**Configuración** > **pestaña Archivos** > **index-logdecoder-custom.xml.**

3. Seleccione el flujo y haga clic en **Recargar**.
   Warehouse Connector extrae el esquema de los dispositivos descendentes (Log Decoder/Decoder).



Para obtener más información sobre los flujos, consulte "Configurar flujos" de la *Guía de configuración de Warehouse Connector*.

Actualizar el esquema en Reporting Engine

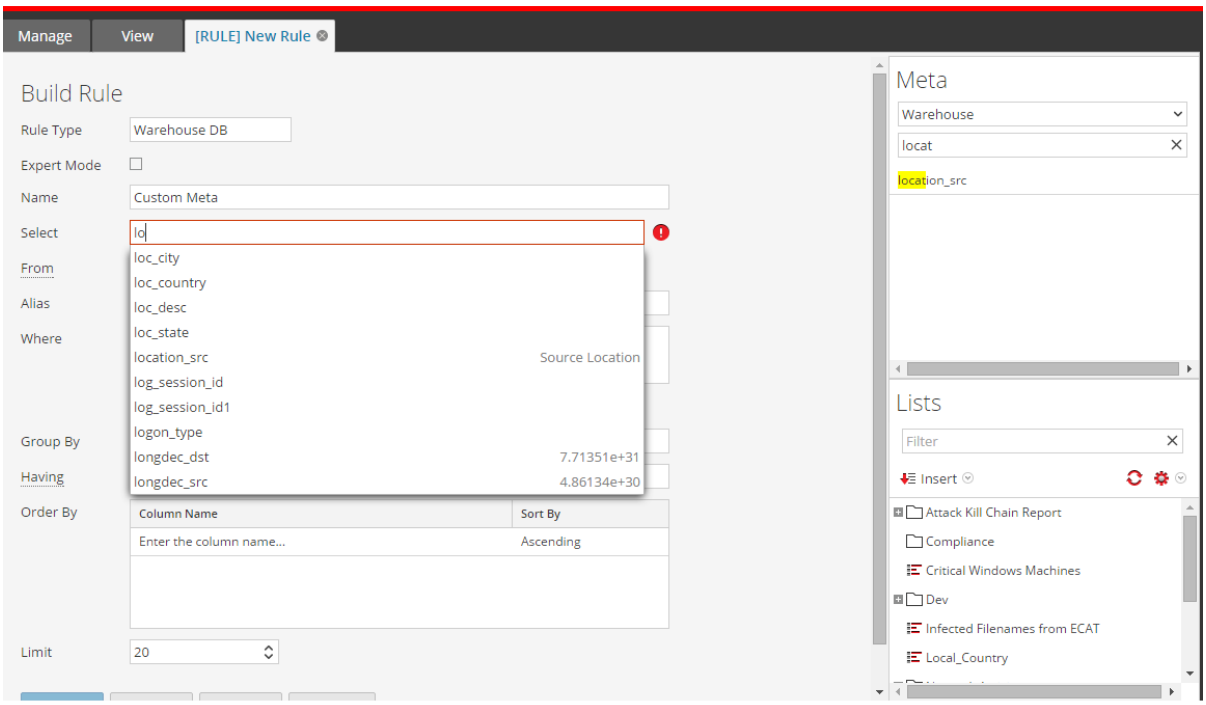
Para actualizar el esquema en Reporting Engine:

1. Vaya a **ADMIN** > **Servicios** > **Reporting Engine.**
2. Haga clic en > **Reiniciar.**

Nota: Reinicie Reporting Engine o espere 30 minutos hasta que el esquema se actualice.

Para ver la clave de metadatos personalizados:

1. Navegue a **Monitorear** > **Informes** > **Reglas**.
2. En la barra de herramientas, haga clic en .
3. Seleccione **Base de datos de Warehouse**.
4. En la pestaña Crear regla, busque los metadatos personalizados en el panel derecho.
   Se muestra la clave de metadatos personalizados.



Cargar y eliminar analizadores personalizados

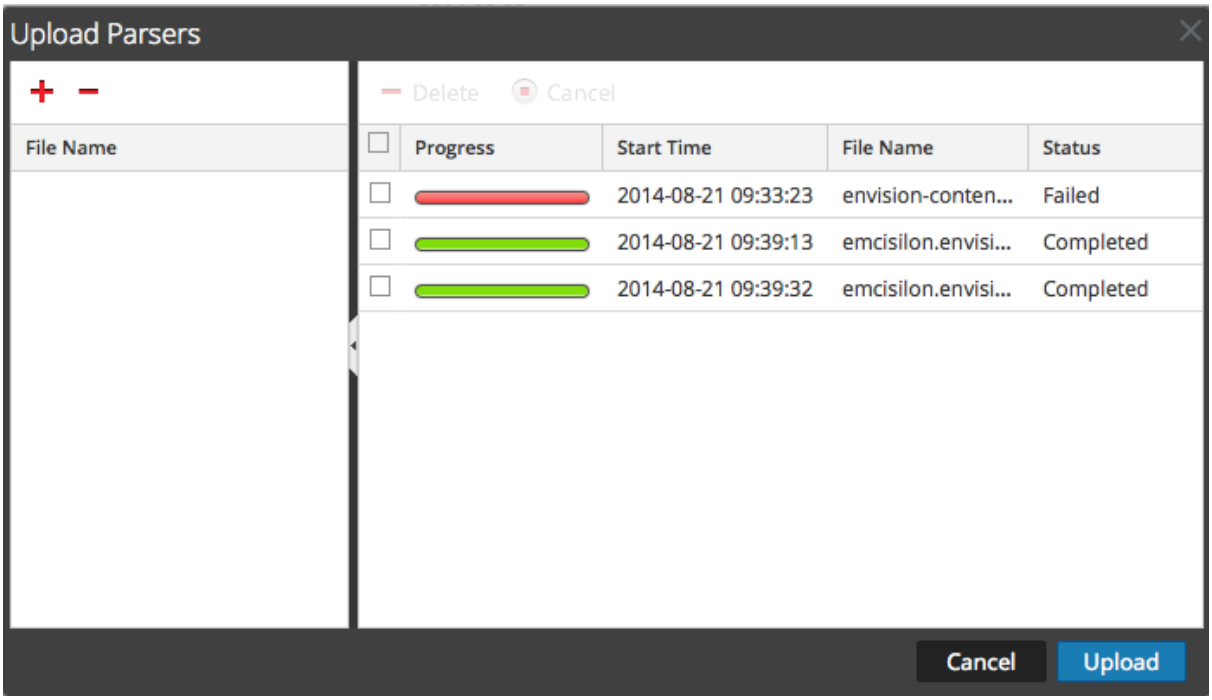
RSA NetWitness Platform tiene la capacidad de cargar analizadores desde el sistema local y eliminar estos analizadores.

Cargar analizadores a un Decoder o Log Decoder

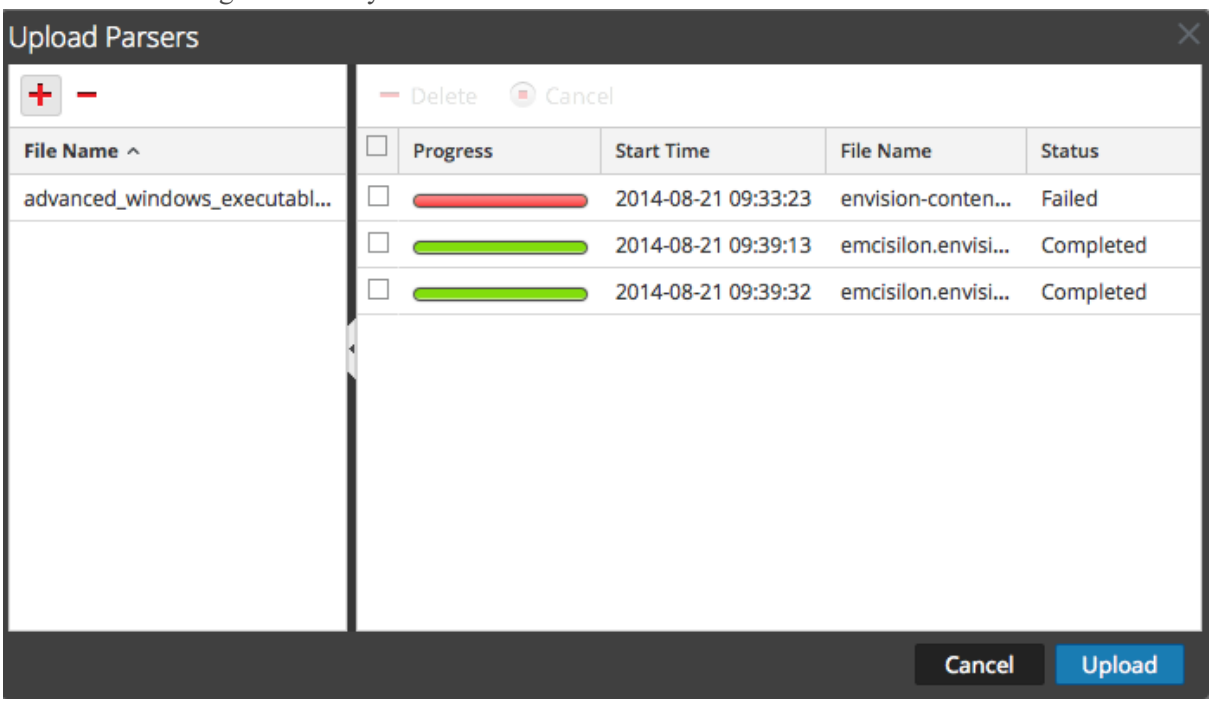
La opción Cargar en la vista Configuración de servicios > pestaña Analizadores muestra el cuadro de diálogo Cargar analizadores, en el cual puede administrar la carga de analizadores en un Decoder o Log Decoder. En la lista de archivos, puede preparar una lista de analizadores para cargar. Puede agregar archivos de una estructura de directorio y eliminar archivos de la lista, si decide que no desea cargar un archivo en especial. Cuando la lista está preparada, el proceso de carga se inicia si se hace clic en Cargar.

1. Vaya a **ADMINISTRAR > Servicios**, seleccione un servicio y **> Ver > Configuración.**
   Se muestra la vista Configurar del servicio seleccionado.
2. Haga clic en la pestaña **Analizadores**.

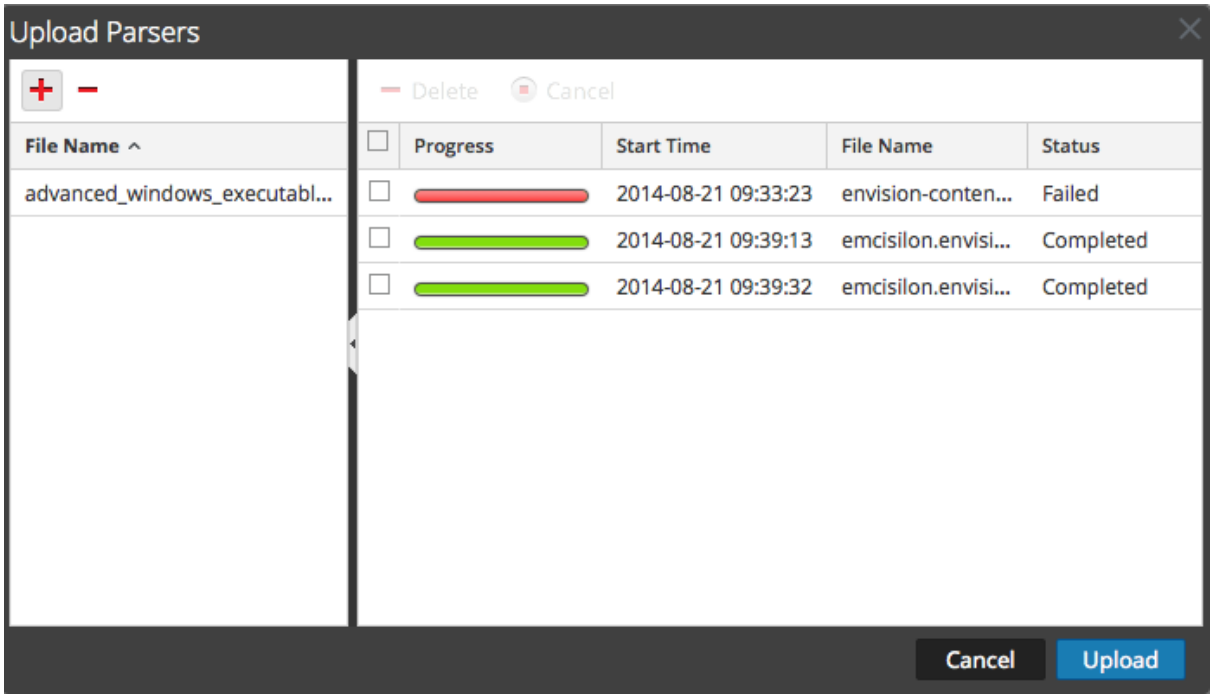
3. Haga clic en Upload.
   Aparecerá el cuadro de diálogo Cargar analizadores.



4. Haga clic en .
   Aparece un cuadro de diálogo de selección de archivo.
5. Seleccione los archivos **.flex**, **.parser** y **.lua** que se actualizarán y haga clic en **Abrir**.
   El cuadro de diálogo se cierra y los archivos seleccionados se muestran en la lista de archivos.



6. Haga clic en **Cargar**.
   La cuadrícula Trabajo de carga muestra el progreso de los trabajos de carga y cada trabajo representa un archivo que se está cargando.



7. Use cualquiera de las herramientas de la cuadrícula Cargar para administrar la carga de trabajos seleccionados: pausa y reanudar, cancelar y eliminar.
   Después de finalizar un trabajo, se implementa en el Decoder y se muestra con los analizadores implementados en la pestaña Analizadores.

Administrar trabajos de carga

Puede usar cualquiera de las herramientas de la cuadrícula Cargar para administrar la carga de los trabajos seleccionados: pausa, reanudar, cancelar y eliminar.

- Para cancelar la carga de un conjunto de analizadores mientras la carga está en línea de espera o en progreso, haga clic en Cancel.
- Para pausar la carga de un conjunto de analizadores, si aún no ha finalizado, haga clic en Pause.
- Para reanudar la carga de un conjunto de analizadores después de una pausa, haga clic en Resume.
- Para eliminar un trabajo cargado, haga clic en .

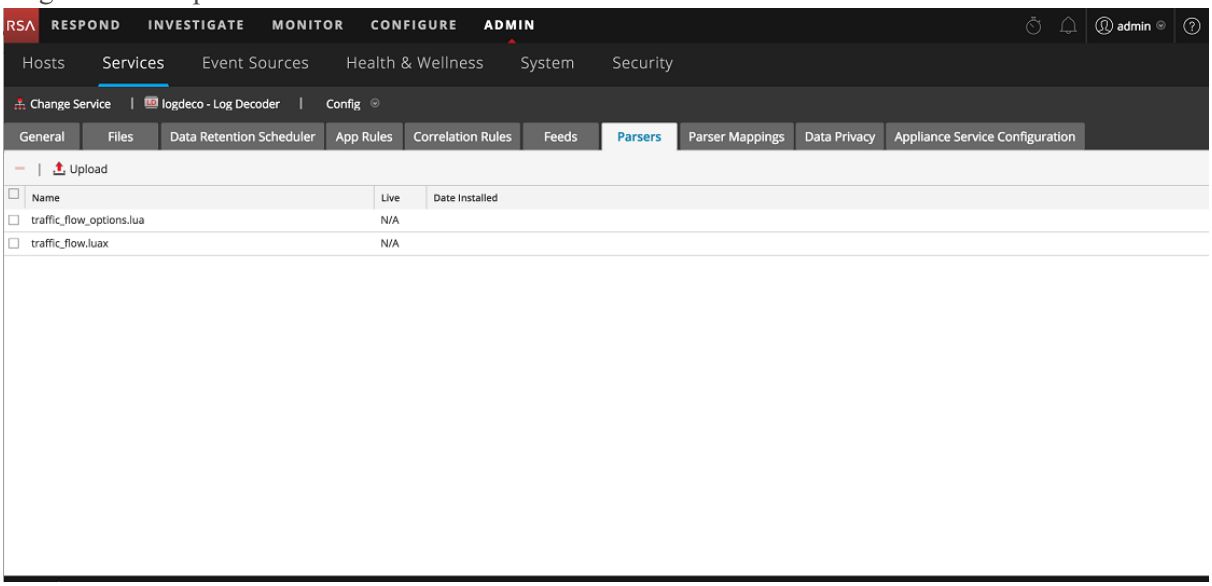
Eliminar analizadores implementados

La opción Eliminar de la vista Configuración de servicios > pestaña Analizadores, proporciona una manera de eliminar los analizadores implementados de un Decoder o Log Decoder. Es posible agregar y eliminar analizadores mientras un Decoder está en funcionamiento sin afectar la captura.

Nota: A menos que se indique lo contrario, todas las referencias a los Decoders se aplican también a los Log Decoders.

Para eliminar un analizador de un Decoder:

1. Vaya a **ADMINISTRAR > Servicios**, seleccione un servicio y > **Ver > Configuración.**
   Se muestra la vista Configuración de servicios del servicio seleccionado.
2. Haga clic en la pestaña **Analizadores**.



3. En la pestaña **Analizadores**, seleccione uno o más analizadores para eliminar.
4. Haga clic en .
   En un cuadro de diálogo, se solicita la confirmación de que desea eliminar los analizadores.
5. Si desea eliminar los analizadores, haga clic en **Sí**.
   Los analizadores se eliminan del Decoder inmediatamente.

Habilitar y configurar el analizador de entropía

A partir de NetWitness Platform 11.0, el administrador puede configurar un Decoder para que use un analizador nativo de NetWitness, conocido como el analizador de entropía. Cuando el analizador de entropía está habilitado, los analistas tienen visibilidad de los canales que intentan fusionar con el resto del tráfico, pero no se siguen un comportamiento normal del protocolo. Esto ayuda a identificar los canales que no se ajustan a la base de tráfico del ambiente normal y que pueden ameritar una investigación.

El analizador crea claves de metadatos en función de las estadísticas recopiladas por el analizador nativo de NetWitness Platform, que ayudan a identificar el comportamiento de un canal que está experimentando una gran cantidad de tráfico de red. Cuando el analizador se habilita por primera vez, el analista debe familiarizarse con el comportamiento general de los distintos canales que se ven en la captura de una sesión para comprender la frecuencia de bytes y la carga útil normal del cliente y el servidor. Una vez que se conoce el comportamiento normal, los analistas pueden usar las claves de metadatos para buscar un comportamiento que no coincida con la expectativa.

De forma predeterminada, el analizador de entropía genera 10 claves de metadatos adicionales que no aumentan significativamente la carga de un Decoder y que son útiles para este caso especializado. De forma predeterminada, el analizador está deshabilitado.

Habilite la indexación si le interesa explorar interesantes sesiones en función del análisis de bytes de carga útil de los paquetes. De forma predeterminada, para facilitar la indexación, el valor normal de `Float32` para `entropy.req` y `entropy.res` se multiplica por 10,000 y se almacenen en un `UInt16` (lo cual ofrece cuatro dígitos de precisión, 0 y 10,000).

Sin embargo, si define los campos `entropy.*` en el idioma de Decoder para que sean `Float32`, el Decoder lo almacenará como un número flotante con un rango de 0.0 a 1.0. Tenga cuidado con cambiar el idioma en todas partes si decide mantenerlo como un `Float32`.

RSA no recomienda la indexación como un `Float32` debido a los altos conteos únicos a causa de cambios de minuto en la precisión.

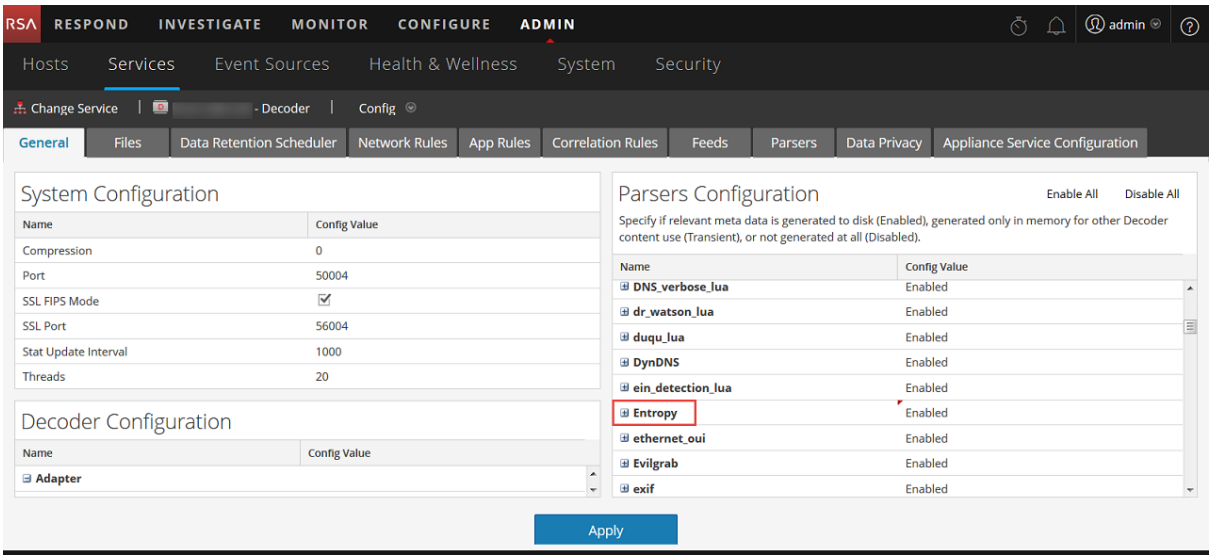
Estas son las nuevas claves de metadatos que genera de forma predeterminada el analizador de entropía:

- `entropy.req` y `entropy.res`: Estas claves de metadatos capturan la entropía mediante la ecuación de entropía de Shannon, que tiene como resultado un valor de punto flotante. El valor de punto flotante de 0 a 1,000 se multiplica por 10,000 y se escribe en NetWitness Platform como `UInt 16`, un entero sin signo de 0 a 10,000.
- `mcb.req` y `mcb.res`: El byte más común es simplemente aquel byte por cada lado (0 a 255) que más se observó.
- `mcbc.req` y `mcbc.res`: El conteo de bytes más común es la cantidad de veces que se observó el byte más común (más arriba) en los flujos de sesión.
- `ubc.req` y `ubc.res`: El conteo de bytes únicos es la cantidad de bytes únicos que se observan en cada flujo. 256 significaría que todos los valores de bytes comprendidos entre 0 y 255 se observaron al menos una vez.

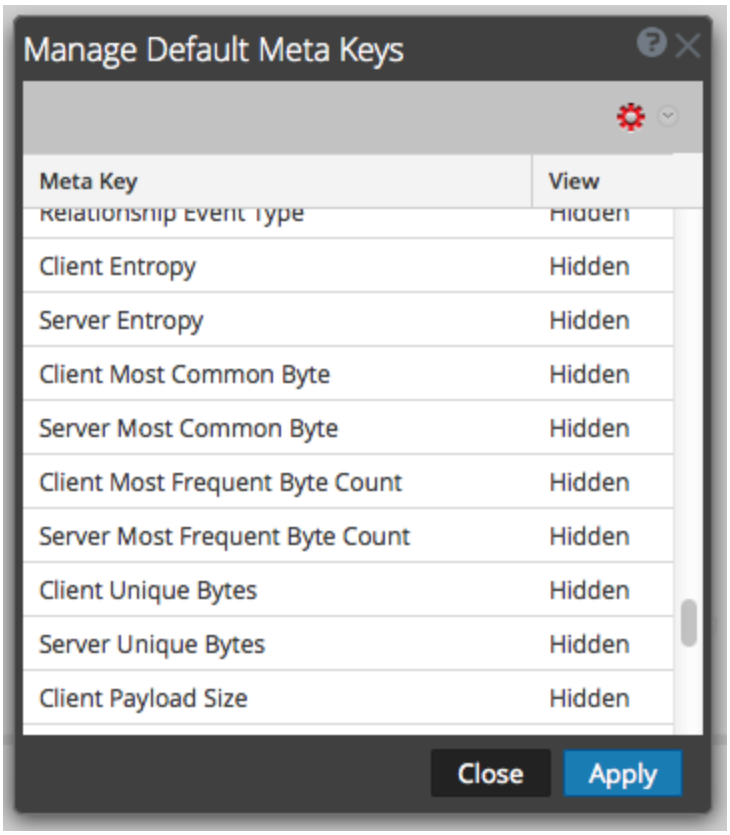
Para habilitar y configurar el analizador de entropía en un Decoder:

1. Inicie sesión en RSA NetWitness y seleccione **ADMIN > Servicios** en el menú NetWitness Platform.
2. En la vista Servicios, seleccione el Decoder que desea configurar y, a continuación,  **Ver > Configuración**.
   Se muestra la vista Configuración de servicios para el Decoder seleccionado.
3. De forma predeterminada, el analizador de entropía está deshabilitado. Haga clic en la lista desplegable en **Valor de configuración** y seleccione **Habilitado**. Si desea deshabilitar algunas de las claves de metadatos, haga clic en la lista desplegable y seleccione **Deshabilitado** junto a la clave de

metadatos.



4. Haga clic en **Aplicar**.
   El analizador de entropía se habilita y comienza a crear las nuevas claves de metadatos según la configuración en el archivo de índice personalizado de Concentrator.
5. En la vista Configuración de servicios, seleccione el Concentrator que agrega tráfico desde este Decoder. Seleccione **Ver > Archivos** y abra el archivo de índice personalizado del Concentrator. Busque las claves de metadatos del analizador de entropía para ver si se incluyen sin comentarios. De forma predeterminada, las claves están comentadas y, por lo tanto, no están habilitadas. Para habilitar esa parte del lenguaje, el administrador debe copiar esa parte del archivo de índice en `index-concentrator-custom.xml` y dejar sin comentarios la línea de `key description` para cada clave de metadatos. A continuación se muestra un ejemplo del archivo de índice personalizado con las claves del analizador de entropía y las instrucciones.
6. Cuando las claves de metadatos de entropía están habilitadas, están disponibles para los analistas en Investigate, pero ocultas de forma predeterminada. Para hacer que las claves de metadatos se puedan ver en la vista Valores de Investigate, edite las claves de metadatos predeterminadas en el cuadro de diálogo Claves de metadatos predeterminadas, de modo que estén abiertas y no ocultas. Puede administrar estas claves de metadatos de la misma forma en que administra otras claves de metadatos.



Configuración del analizador de entropía en el archivo de índice personalizado de Concentrator

El siguiente es un extracto de las líneas del archivo de índice de Concentrator que el administrador debe copiar en el archivo de índice personalizado. Los comentarios proporcionan orientación sobre cómo configurar el analizador.

```
<!-- This section is commented out because it's only used by the Entropy
parser which is disabled by default. To enable this part of the language, copy
to index-concentrator-custom.xml and uncomment the keys. HOWEVER, take note
that depending on how the Entropy parser is configured, the entropy.req and
entropy.res format might be a Float32 instead of a UInt16. So make sure to
change to the correct type if necessary.-->

<!-- Entropy parser meta - enable indexing if you have interest in exploring
this for interesting sessions based on payload byte analysis of the packets.
By default, to make indexing easier, the normal Float32 value for entropy.req
and entropy.res is multiplied by 10k and stored in a UInt16 (thus giving 4
digits of precision, 0 to 10,000). However, if you define the entropy.* fields
in the Decoder language to be Float32, it will store it as a float with a
range of 0.0 to 1.0. Take care to change the language everywhere if you decide
to keep it as a Float32. We do not recommend indexing as a Float32 because of
the high unique counts due to minute changes in precision. -->

<!--

<key description="Entropy Request (Client)" format="UInt16" level="IndexNone"
name="entropy.req" valueMax="10001"/>
```

```
<key description="Entropy Response (Server)" format="UInt16" level="IndexNone"
name="entropy.res" valueMax="10001"/>

-->

<!-- The most common byte is simply which byte for each side (0 thru 255) was
seen the most -->

<!--

<key description="Most Common Byte Request" format="UInt8" level="IndexNone"
name="mcb.req"/>

<key description="Most Common Byte Response" format="UInt8" level="IndexNone"
name="mcb.res"/>

-->

<!-- The most common byte count is the number of times the most common byte
(above) was seen in the session streams -->

<!--

<key description="Most Common Byte Count Request" format="UInt32"
level="IndexNone" name="mcbc.req" valueMax="500000"/>

<key description="Most Common Byte Count Response" format="UInt32"
level="IndexNone" name="mcbc.res" valueMax="500000"/>

-->

<!-- Unique byte count is the number of unique bytes seen in each stream. 256
would mean all byte values of 0 thru 255 were seen at least once -->

<!--

<key description="Unique Byte Count Request" format="UInt16" level="IndexNone"
name="ubc.req"/>

<key description="Unique Byte Count Response" format="UInt16"
level="IndexNone" name="ubc.res"/>

-->

<!-- The payload size metrics are the payload sizes of each session side at
the time of parsing. However, in order to keep indexing from having high
unique counts (bad for performance), the two payload size metas below are
indexed in buckets. -->

<!--

<key description="Payload Size Request" format="UInt32" level="IndexNone"
bucket="true" name="payload.req" valueMax="500000"/>

<key description="Payload Size Response" format="UInt32" level="IndexNone"
bucket="true" name="payload.res" valueMax="500000"/>

-->
```

Procedimientos adicionales de Decoder y Log Decoder

Este tema explica los procedimientos adicionales que debería seguir un administrador y que no son esenciales para la configuración de Decoder o Log Decoder.

Temas

Configurar la funcionalidad 10G

En este tema se indica a los administradores cómo ajustar específicamente un Network Decoder para la captura de paquetes a alta velocidad con NetWitness Platform 11.x. Esto se aplica cuando se capturan paquetes en una tarjeta de interfaz 10G. La captura de paquetes a altas velocidades requiere una configuración cuidadosa y lleva el hardware de Decoder a sus límites, razón por la cual debe leer este tema completo cuando implemente una solución de captura 10G.

RSA NetWitness Platform ofrece compatibilidad con la recopilación a alta velocidad de Decoder. Puede capturar datos de paquetes de redes de mayor velocidad y optimizar el Network Decoder para capturar tráfico de red con ráfagas continuas de hasta 8 Gb/s y 10 Gb/s, según los analizadores y los feeds que haya activado.

Las mejoras que facilitan la captura en estos ambientes incluyen las siguientes:

- Utilización de la funcionalidad del driver de captura `pf_ring` para aprovechar la tarjeta NIC Intel 10G genérica con el fin de lograr una captura a alta velocidad.
- Introducción de la configuración `assembler.parse.valve`, que deshabilita automáticamente los analizadores de aplicación cuando se superan determinados umbrales con el fin de limitar el riesgo de pérdida de paquetes. Cuando se deshabilitan los analizadores de aplicación, los analizadores de capa de red permanecen activos. Cuando las estadísticas bajan de los umbrales superados, los analizadores de aplicaciones se vuelven a habilitar automáticamente.

Requisitos previos del hardware

- Un Decoder serie 4S o serie 5
- Una tarjeta Ethernet basada en Intel 82599, como Intel x520. Todas las tarjetas 10G que proporciona RSA cumplen con este requisito. Dos ejemplos son:
  - Todas las tarjetas de SMC-10GE que proporciona RSA.
  - Una tarjeta secundaria de red de Dell que usa una controladora Intel para proporcionar interfaces de red 10G. Esto se incluye en todo el hardware serie 5.
- Para la serie 4S/Dell R620 solamente: 96 GB de memoria DD3-1600 en DIMM de **doble rango**. Los DIMM de rango único pueden disminuir el rendimiento hasta en un 10 %. Para determinar la velocidad y el rango de los DIMM instalados, ejecute este comando:
  `dmidecode -t 17`.
- Almacenamiento suficientemente grande y rápido para satisfacer el requisito de captura. Las consideraciones de almacenamiento se analizan más adelante en este tema.
- Cada Network Decoder configurado con un mínimo de dos DAC o conectividad SAN.

Requisitos previos del software

- Los sistemas basados en Dell R620, por ejemplo, la serie 4S, deben tener su BIOS actualizado a v1.2.6 o superior.

- La funcionalidad de Decoder 10G solo es compatible con las imágenes de instalación de Decoder que proporciona RSA. Todo el software requerido se instala de forma predeterminada.
- Si actualiza desde una versión anterior, realice la actualización en primer lugar antes de continuar con la configuración

Instalar Decoder 10G

Nota: Puede dirigirse a "Configurar Decoder 10G" si está comenzando con el nuevo hardware serie 5.

Ejecute los siguientes pasos para instalar el Decoder 10G de NetWitness:

Descargar y actualizar el BIOS

Nota: Las revisiones de BIOS anteriores a v1.2.6 tienen problemas para identificar correctamente la ubicación de la tarjeta de captura 10G dentro del sistema. Se recomienda que los clientes actualicen al BIOS v2.2.3 más reciente, pero no es requisito para 10G si ejecutan v1.2.6 o superior.

1. Descargue el BIOS v2.2.3 desde la siguiente ubicación:

   http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=V7P04
2. Descargue el archivo Update Package for the Red Hat Linux.
3. Copie el archivo en el servidor de NetWitness.
4. Inicie sesión como `root`.
5. Cambie los permisos en el archivo a ejecutar.
6. Ejecute el siguiente archivo:

   ```
   ./BIOS_V7P04_LN_2.2.3.BIN
   ```
7. Reinicie el sistema cuando se complete la ejecución y se solicite un reinicio.

Nota: El procedimiento de instalación del BIOS tarda aproximadamente 10 minutos.

Localizar los paquetes Decoder 10G

Los paquetes requeridos para configurar Decoder 10G deben estar presentes en la imagen de instalación de Decoder. No debe ser necesario instalar ningún paquete adicional.

Verificar que los paquetes de Decoder 10G estén instalados

La instalación de los paquetes de Decoder 10G se maneja de forma automática. Por lo tanto, no debe haber ninguna acción para habilitar la funcionalidad 10G.

- Si actualizó los paquetes de kernel como parte de una actualización, se requiere un reinicio. El sistema operativo volverá a compilar e instalar los drivers para el kernel actualizado.
- Puede verificar que la instalación se realizó correctamente si ve interfaces `PFRINGZC` adicionales disponibles al seleccionar el adaptador de puertos de captura, como se describe a continuación.

Configurar Decoder 10G

Realice los siguientes pasos para configurar Decoder 10G:

1. En la vista **Explorar del Decoder**, haga clic con el botón secundario en **Decoder** y seleccione **Propiedades**.
2. En el menú desplegable Propiedades, seleccione **reconfig** e ingrese los siguientes parámetros:
   `update=1 op=10g`
   Esto ajusta la canalización de procesamiento de paquetes de Decoder para permitir un mayor rendimiento de datos crudos, pero menos capacidad de análisis.
3. En la vista **Explorar del Decoder**, haga clic con el botón secundario en **database** y seleccione **Propiedades**.
4. En el menú desplegable **Propiedades**, seleccione **reconfig** e ingrese los siguientes parámetros:
   `update=1 op=10g`
   Estos parámetros ajustan la base de datos de paquetes para usar tamaños de archivos muy grandes y operaciones de I/O directas.
5. Seleccione el adaptador de puertos de captura. Entre las opciones para esto se incluyen las siguientes (en los siguientes ejemplos, “p1p1” y “p1p2” son marcadores de posición y se deben reemplazar con nombres de interfaz propios):
   - Captura de un único puerto: **PFRINGZC,p1p1** o **PFRINGZC,p1p2**
   - Captura de ambos puertos: seleccione **PFRINGZC,P1P1** y en la vista **Explorar**, configure `capture.device.params = device=zc:p1p2,zc:p1p1`.
6. Si el hilo de ejecución de escritura tiene problemas para mantener la velocidad de la captura, puede intentar lo siguiente:

   Cambie `/datebase/config/packet.integrity.flush` a `normal`.

   Nota: Puede intentar ajustar `packet.file.size` a un valor mayor, pero debe mantener el tamaño del archivo en menos de 10 GB, ya que el archivo completo se coloca en el búfer de memoria.
7. (Opcional) El análisis de aplicaciones consume mucho CPU y puede hacer que Decoder pierda paquetes. Para moderar las pérdidas inducidas por el análisis de aplicaciones, puede configurar `/decoder/config/assembler.parse.valve` en `true`. Estos son los resultados:
   - Cuando el análisis de sesiones se transforme en un cuello de botella, los analizadores de aplicación (HTTP, SMTP, FTP, etc.) se deshabilitarán temporalmente.
   - Las sesiones no se pierden cuando se deshabilitan los analizadores de aplicaciones, solo la fidelidad del análisis ejecutado en ellas.
   - Las sesiones analizadas con los analizadores de aplicación deshabilitados tendrán metadatos de red asociados (del analizador de red).
   - La estadística `/decoder/parsers/stats/blowoff.count` muestra el conteo de todas las sesiones que no se sometieron a los analizadores de aplicación (el análisis de red se ejecuta de todos modos).

- Cuando el análisis de sesiones deja de ser un posible cuello de botella, los analizadores de aplicación se reactivan automáticamente.
- El pool de sesiones del ensamblador debe ser lo suficientemente grande de modo que las sesiones no se fuercen.
- Puede determinar si las sesiones se están forzando con la estadística `/decoder/stats/assembler.sessions.forced` (que irá en aumento). Además, `/decoder/stats/assembler.sessions` estará dentro de varios cientos de `/decoder/config/assembler.session.pool`.

8. (Opcional) Si necesita ajustar la MTU para la captura, agregue el parámetro `snaplen` a `capture.device.params`. A diferencia de las versiones anteriores, no es necesario que `snaplen` se redondee hacia arriba a algún límite específico. El Decoder ajusta automáticamente la MTU configurada en las interfaces de captura.
9. Los siguientes parámetros de configuración están obsoletos y ya no son necesarios:
   - `core= parameter` en `capture.device.params`
   - Cualquier archivo de configuración en el directorio `/etc/pf_ring`

   Nota: Un dispositivo Ethernet instalado después de una digitalización no requiere ninguna configuración para su uso como un dispositivo de captura. Si se usa como una interfaz de red o para que las herramientas del sistema accedan a él sin configuración manual, requiere configuración.

Parámetros de configuración habituales

A continuación se enumeran los parámetros de configuración habituales. Los parámetros reales pueden variar según la cantidad de memoria y los recursos de CPU disponibles.

1. Ajustes de pool de sesiones y paquetes (en `/decoder/config`):
   - `pool.packet.pages = 1000000`
   - `pool.session.pages = 300000`
2. Tamaño del bloque de escritura de paquetes bajo (tamaño `/database/config/packet.write.block`) configurado en `filesize`.

   Nota: Esto configura el Decoder para que coloque en el búfer el archivo con páginas gigantes y escriba mediante I/O directos para lograr el máximo rendimiento.
3. Conteo de hilos de ejecución de análisis (en `/decoder/config`).

   `parse.threads =12`

Consideraciones de almacenamiento

Cuando se captura a velocidades de línea de 10G, el sistema de almacenamiento que aloja las bases de datos de paquete y metadatos debe tener capacidad para un rendimiento de escritura sostenido de 1,400 MB/s.

Uso del hardware serie 4S (con dos o más unidades de DAC)

La serie 4S cuenta con una controladora SAS RAID de hardware con capacidad de 48 Gbit/s agregados de rendimiento de I/O. Dispone de ocho puertos de 6 Gbit externos, organizados en dos cables SAS de 4 pistas. La configuración recomendada para 10G es balancear por lo menos dos unidades DAC en estos dos conectores externos. Por ejemplo, conecte una DAC a un puerto de la tarjeta SAS y, a continuación, otra DAC al otro puerto de la tarjeta SAS.

Para los ambientes con más de dos DAC, conéctelas a cada puerto de manera balanceada. Esto puede requerir el recableado de las DAC en una implementación existente, pero no debería afectar a los datos que ya se capturaron en Decoder.

Si agrega nueva capacidad, use el script `NwMakeArray` actualmente disponible para aprovisionar las unidades de DAC. El script agrega automáticamente una DAC por ejecución (es decir, si se agregan tres DAC, el script se debe ejecutar tres veces) y las agrega a la configuración de `NwDecoder10G` como puntos de montaje por separado. Los puntos de montaje independientes son importantes, ya que permiten a `NwDecoder10G` segregar las I/O de escritura de captura de las I/O de lectura necesarias para cumplir con solicitudes de contenido de paquetes.

Uso de SAN y otras configuraciones de almacenamiento

Decoder permite cualquier configuración de almacenamiento que pueda cumplir con el requisito de rendimiento sostenido. El vínculo Fibre Channel de 8 Gbit estándar a una SAN no es suficiente para almacenar datos de paquetes a 10G; para usar una SAN, puede ser necesario realizar una agregación en múltiples destinos mediante un esquema de RAID por software. Por lo tanto, para configurar la conectividad a la SAN mediante varios FC, se requieren ambientes que usen SAN.

Consideraciones de análisis y contenido

El análisis de paquetes crudos a altas velocidades presenta retos únicos. Dadas las altas tasas de sesiones y paquetes, la eficiencia del análisis es primordial. Un único analizador ineficiente (que tarde demasiado en examinar los paquetes) puede retrasar el sistema completo hasta el punto en que los paquetes se pierden en la tarjeta.

Para las pruebas iniciales de 10G, comience solo con analizadores nativos (excepto SMB/WebMail). Use los analizadores nativos para establecer el rendimiento de base y con una pérdida de paquetes mínima o nula. No descargue contenido de Live hasta que se haya hecho esto y se compruebe que el sistema captura sin problema a altas velocidades.

Una vez que el sistema haya estado operacional y en correcta ejecución, se debe agregar contenido de Live de manera muy lenta, en especial los analizadores.

Mejores prácticas

Si actualiza un sistema actualmente implementado o implementa un sistema nuevo, la recomendación es usar las siguientes mejores prácticas para minimizar el riesgo de pérdida de paquetes. Preste atención si actualiza una implementación actual de 10G, pero no agrega tráfico adicional. Por ejemplo, un Decoder actual que captura de una tarjeta 10G a 2G constantes no debería percibir una diferencia en el rendimiento, a menos que parte de la actualización también implique agregar tráfico adicional para la captura.

- Incorpore analizadores de base (excepto SMB/Webmail, los cuales generalmente tienen una alta utilización del CPU) y compruebe que la pérdida de paquetes sea escasa o nula.

- Cuando agregue analizadores adicionales, agregue solo uno o dos por vez.
- Mida el impacto en el rendimiento del contenido recientemente agregado, en especial durante periodos de máximo tráfico.
- Si se comienzan a producir pérdidas en circunstancias en que antes no se producían, inhabilite todos los analizadores recientemente agregados, habilite solo uno por vez y mida el impacto. Esto ayuda a detectar analizadores individuales que tienen efectos perjudiciales en el rendimiento. Tal vez sea posible reestructurarlos para que tengan un mejor funcionamiento o reducir su conjunto de funciones solo a aquellas que son necesarias para el caso de uso del cliente.
- Aunque tienen impactos menores en el rendimiento, los feeds también se deben revisar y agregar en etapas con el fin de medir su impacto.
- Las reglas de aplicaciones también tienden a tener un impacto mínimo observable, pero, nuevamente, es mejor no agregar una gran cantidad de ellas de una sola vez sin medir su impacto en el rendimiento.

Finalmente, la aplicación de los cambios recomendados en la configuración, los cuales se describen en la sección Configuración, ayudará a minimizar los posibles problemas.

Contenido de Live probado

Todos los analizadores siguientes (no cada uno de ellos) se pueden ejecutar a 10G en el conjunto de datos de prueba utilizado:

- Contenido de MA (7 analizadores Lua, 1 feed y 1 regla de aplicación)
- 4 feeds (alert ids info, nwmalwaredomains, warning y suspicious)
- 41 reglas de aplicación
- DNS_verbose_lua (inhabilitar DNS)
- fingerprint_javascript_lua
- fingerprint_pdf_lua
- fingerprint_rar_lua
- fingerprint_rtf_lua
- MAIL_lua (inhabilitar MAIL)
- SNMP_lua (inhabilitar SNMP)
- spectrum_lua
- SSH_lua (inhabilitar SSH)
- TLS_lua
- windows_command_shell
- windows_executable

NO PROBADOS:

- SMB_lua, SMB nativo deshabilitado de manera predeterminada
- html_threat

OTROS:

- HTTP_lua reduce la velocidad de captura de más de 9G a menos de 7G. A un poco menos de 5G, se puede usar este analizador en lugar del nativo sin pérdidas (además de la lista anterior).
- xor_executable lleva la CPU de análisis al 100 % y el sistema puede disminuir considerablemente debido al respaldo del análisis.

Ajustes de agregación en función del contenido de Live probado

Un Decoder 10G puede gestionar la agregación a un único Concentrator mientras se ejecuta a velocidades de 10G. Se espera que las implementaciones que usan Malware Analysis, Event Stream Analysis, Warehouse Connector y Reporting Engine afecten el rendimiento y puedan provocar la pérdida de paquetes.

En el caso del escenario de prueba, Concentrator agrega entre 45,000 y 70,000 sesiones/s. El Decoder 10G captura entre 40,000 y 50,000 sesiones/s. Con el contenido antes identificado, esto equivale aproximadamente a entre 1.5 y 2 millones de metadatos/s. Debido al alto volumen de tasas de sesiones, se recomienda aplicar los siguientes cambios en la configuración:

- Una agregación de tipo nice en Concentrator limita el impacto en el rendimiento en Decoder 10G. El siguiente comando activa la agregación de tipo nice.
  `/concentrator/config/aggregate.nice = true`
- Debido al alto volumen de sesiones en Concentrator, puede considerar la activación del modo valores paralelos en el Concentrator mediante la configuración de `/sdk/config/parallel.values` en `16`. Esto mejora el rendimiento de Investigation cuando la cantidad de sesiones por segundo sea mayor que 30,000.
- Si se requieren múltiples flujos de agregación, la agregación desde el Concentrator tiene un menor impacto en el Decoder.
- Se requerirá una revisión adicional del contenido y el análisis en aquellas implementaciones en las cuales se deseen usar otros componentes de NetWitness Platform (Warehouse Connector, Malware Analysis, ESA y Reporting Engine).

Optimizar las operaciones de lectura/escritura al agregar almacenamiento nuevo

Un Decoder 10G está optimizado para escalonar las operaciones de lectura y escritura en varios volúmenes, de modo que el archivo actual que se escribe esté en un volumen diferente del archivo siguiente que se escribirá. Esto permite el rendimiento máximo en el volumen RAID cuando se leen datos desde el último archivo que se escribe mientras se escribe el archivo actual en un volumen diferente. Sin embargo, si los volúmenes se agregan después de que ha estado en uso un Decoder, la capacidad de escalonar se ve limitada debido a que uno o más volúmenes ya están llenos y el volumen nuevo es el único lugar en el que se pueden escribir nuevos archivos.

Para corregir esta situación, un administrador puede ejecutar un comando `stagger` en una base de datos de NetWitness Platform existente (paquete, registro, metadatos o sesión), que tenga al menos dos volúmenes, con el fin de escalonar los archivos entre todos los volúmenes en el patrón de lectura/escritura más óptimo. El principal caso de uso es cuando se agrega nuevo almacenamiento a un Decoder existente y se desean escalonar los volúmenes ANTES de reiniciar la captura.

Los nodos de configuración para este comando son las bases de datos de sesión, metadatos y paquete. Cada una de estas reside en `/database/config`, que suele ser un nodo raíz. Los nodos de configuración para un Decoder son los siguientes:

- `/database/config/packet.dir`
- `/database/config/meta.dir`
- `/database/config/session.dir`

Consulte información sobre cómo se formatean esas configuraciones en la *Guía de ajuste de la base de datos de NetWitness Platform Core*.

En general, el comando `stagger` es útil únicamente para un Decoder 10G y suele serlo solo para la base de datos de paquete. El máximo rendimiento se logra para el almacenamiento y la recuperación de paquetes cuando están presentes varios volúmenes. En este escenario, el Decoder completa siempre el volumen con más espacio libre. Cuando los volúmenes tienen aproximadamente el mismo tamaño, esto da como resultado un patrón de escritura escalonado que permite un rendimiento máximo para la lectura y la escritura en todos los volúmenes. Sin embargo, esto ocurre naturalmente solo cuando están presentes varios volúmenes de almacenamiento de paquetes en el momento en que el Decoder se implementa por primera vez.

Un caso de uso típico es la adición de más almacenamiento a un Decoder existente para aumentar la retención. Sin embargo, cuando se agrega almacenamiento a una implementación en la que ya se completaron los volúmenes existentes con paquetes almacenados, el Decoder completará naturalmente el almacenamiento nuevo con paquetes antes de implementar paquetes en el almacenamiento existente. Esto da como resultado un patrón de lectura/escritura poco satisfactorio debido a que la mayoría de las lecturas ocurrirá en el mismo volumen en el que se escribe actualmente. En una implementación de 10G, las lecturas tienen bloqueado el acceso al volumen mientras se producen las escrituras. Esto no detiene TODAS las lecturas en ese volumen porque el archivo se pone en el búfer en la memoria antes de que se escriba, pero da lugar a un rendimiento de lectura poco satisfactorio.

Con el comando `stagger`, puede agregar más almacenamiento y, a continuación, hacer que el servicio escalone naturalmente los archivos en TODOS los volúmenes (existentes y nuevos), de modo que el rendimiento de lectura se optimice.

Precaución: Este comando se debe ejecutar solamente DESPUÉS de que se monta el almacenamiento y se configura el Decoder para usarlo (por ejemplo, después de que se agregan puntos de montaje a `packet.dir`).

La desventaja de este comando es que el escalonamiento puede tardar y el Decoder no debe estar capturando durante la operación de escalonamiento.

Flujo de trabajo recomendado:

1. Agregue todo el almacenamiento y configure los puntos de montaje.
2. Agregue nuevos puntos de montaje de almacenamiento a `packet.dir` (o `session.dir/meta.dir`) y reinicie el servicio (muy importante).
3. Asegúrese de que la captura esté detenida.

4. Ejecute la operación de escalonamiento, pero asegúrese de que la conexión que inició esta operación nunca se termine hasta que se complete. Si la conexión se termina, la operación de escalonamiento se cancelará. Si se cancela, los archivos que ya se escalonaron permanecerán en su lugar. La operación se puede reanudar con la reejecución del mismo comando (no será necesario volver a realizar el trabajo ya realizado). Si el escalonamiento se ejecuta desde NwConsole, ejecute el comando `timeout 0` antes de enviar el comando `stagger`. Esto evitará el tiempo de espera del comando normal de 30 segundos.
5. Inicie la captura después de que finalice el comando `stagger`.

Los siguientes son los parámetros para el comando:

- `type`: La base de datos que se escalonará (sesión, metadatos o paquete). En general, solamente la base de datos de paquete es útil para el escalonamiento, pero es posible aplicarlo a la base de datos de sesión o metadatos cuando están presentes varios volúmenes para ellas. Dado que las bases de datos de sesión y metadatos escriben mucho menos datos que la base de datos de paquete, en general, el escalonamiento de esas bases de datos produce aumentos de rendimiento menos evidentes.
- `dryRun`: Si es `true` (el valor predeterminado), devolverá solamente una descripción de las operaciones que se realizarían. Si es `false`, los archivos se transferirán realmente a un patrón de lectura/escritura óptimo. DEBE pasar false para escalonar realmente los archivos.

Ejemplo de uso desde NwConsole:

```
login <decoder>:50004 <username> <password>
timeout 0
send /database stagger type=packet dryRun=false
```

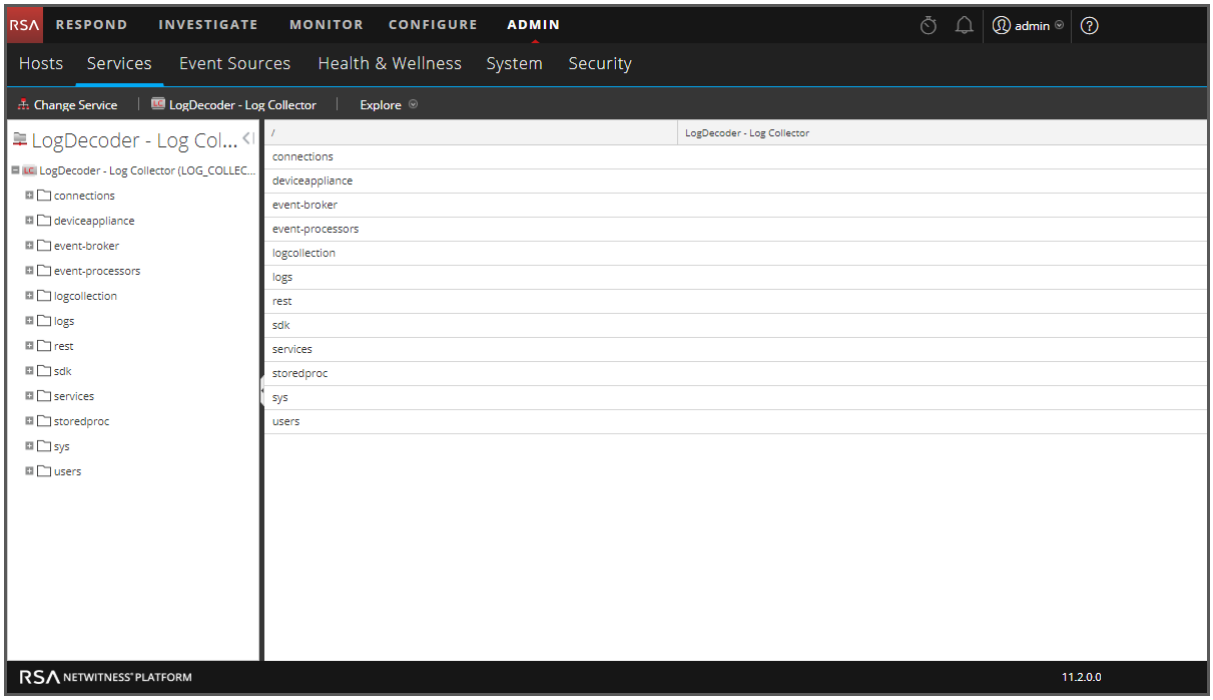
Si ejecuta este comando a través de la API RESTful, pase el parámetro `expiry=0` adicional para evitar un tiempo de espera desde el servicio. También tendrá que asegurarse de que el cliente HTTP no se desconecte antes de que se complete la operación.

Configurar un Log Decoder para que acepte Protobuf

Hay momento en que se desea analizar archivos de registro que están en formato protobuf (búfer de protocolo). Puede configurar un Log Decoder con un servicio Log Collector para aceptar registros en formato protobuf (búfer de protocolo).

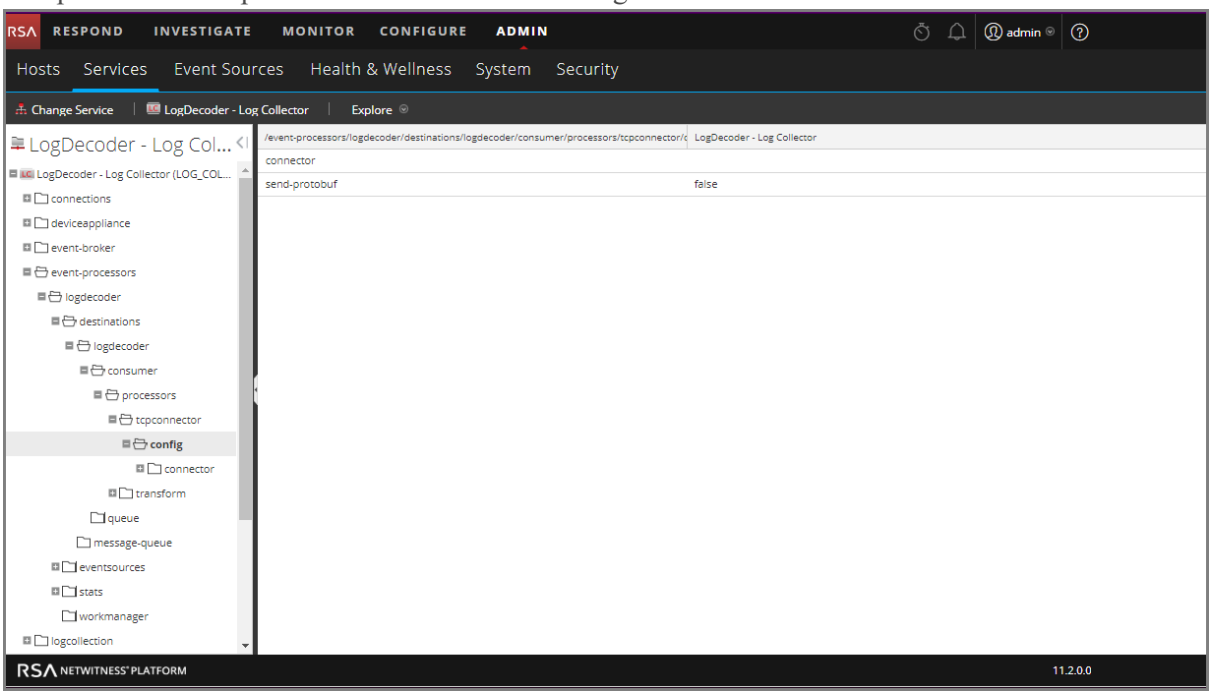
Para importar un archivo de registro a un Log Decoder:

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. Seleccione un Log Decoder con un servicio Log Collector en la lista de **Servicios** y elija > **Ver** > **Explorar**.
   Se muestra la vista Explorar para el Log Decoder: Log Collector.



3. Vaya a **`event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config`**

La apariencia de la pantalla debe ser similar a la siguiente.



4. En el campo **send-protobuf**, seleccione **false** y cambie el valor a **true.**
5. Vaya a `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/channel/tcp` y cambie el valor del **puerto** a **50202**.
6. Vaya a `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/event` y cambie los siguientes parámetros:
   - Borre el campo **delimiter**
   - Cambie **format** a **%text%**

Configurar los tiempos de espera divididos de la sesión

El comportamiento predeterminado del Decoder es finalizar automáticamente las sesiones que superen un tamaño configurado o hayan estado inactivas durante un período de tiempo. Cuando la sesión finaliza debido al tiempo de espera, todos los paquetes subsiguientes recibidos en esa sesión parecen almacenarse en una nueva sesión. Puede mitigar el efecto de la división de la sesión debido a largos períodos de inactividad entre los paquetes mediante este procedimiento.

Cuando una sesión de Decoder supera un tamaño configurado (32 MB de manera predeterminada, el valor `/decoder/config/assembler.max.size`) o ha estado inactiva durante un tiempo, la sesión se divide. NetWitness Platform tiene el paquete anterior y el paquete siguiente, y puede propagar el estado de la sesión a partir del fragmento de sesión inicial al fragmento de sesión subsiguiente.

Se anota cada fragmento de sesión (metadatos `session.split`) para que se pueda identificar y asociar con otros fragmentos de la sesión real de la red. La direccionalidad, según lo determina la sesión inicial, reduce la aparición de fragmentos con direccionalidad invertida.

Si hay una brecha de tiempo entre los paquetes que es lo suficientemente grande como para que ya no haya paquetes para la sesión en la memoria, la sesión se quita del Decoder. Si después de que esto ocurre se muestra un paquete posterior, se crea una nueva sesión sin ningún contexto de la sesión anterior. El problema es la incapacidad para continuar una sesión cuando se producen una brecha entre los paquetes de una sesión que es más grande que los paquetes que colocamos en el búfer (según las configuraciones disponibles de memoria y tiempo de espera). Una vez que se quita de la memoria el último paquete de una sesión, también se quita la sesión y con ella el contexto necesario para garantizar una direccionalidad coherente.

Hay dos ajustes de configuración de tiempo de espera en un Network Decoder, `/decoder/config/assember.timeout.session` y `assembler.timeout.packet`. Ambos se configuran de manera predeterminada en 60 segundos. La configuración `assembler.timeout.session` controla cuánto tiempo dura una sesión en el ensamblador sin recibir otro paquete. La configuración `assembler.timeout.packet` controla cuánto tiempo espera una sesión antes de su análisis. Si la sesión se extrae del ensamblador antes de este tiempo de espera, se analiza automáticamente.

El tiempo de espera de la sesión es la cantidad de segundos desde que el último paquete se agregó a esa sesión. Por lo tanto, este tiempo de espera se restablece en cada paquete que se agrega a esa sesión. El tiempo de espera del paquete es la cantidad de segundos transcurridos desde que se agregó el primer paquete para esa sesión (en otras palabras, el paquete que creó la sesión). Esto nunca se restablece y una vez que vence el tiempo de espera, la sesión se analiza.

El punto importante es que se puede analizar una sesión, pero permanece en el ensamblador. Una sesión en el ensamblador aún puede tener los paquetes que se le agregaron incluso si ya se analizó. Los analizadores nunca verán los paquetes que se agregan después del análisis de la sesión, pero estarán conectados a la sesión y se podrán ver en una llamada `/sdk content` o `/sdk packets` posterior.

Después de que se analiza una sesión, la sesión Y sus metadatos se escriben en el disco. En este punto, se pueden agregar y "ver" mediante los comandos `sdk`. Los paquetes se escriben en orden de captura y no se reordenan según la sesión a la que pertenecen. Tampoco se escriben cuando se escribe la sesión y los metadatos.

Puede deshabilitar ambos nodos de tiempo de espera agotado, `/decoder/config/assembler.timeout.session` y `assembler.timeout.packet`, para ello configúrelos en cero en la Vista Explorar de servicios.

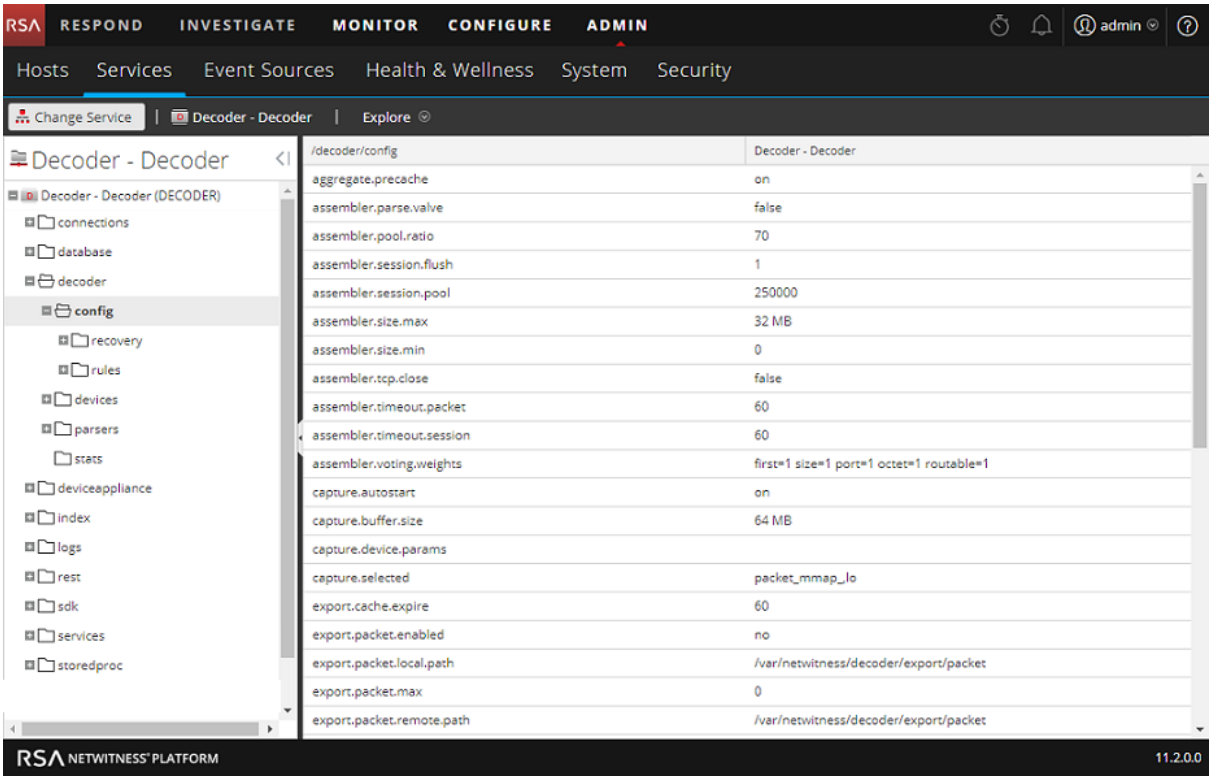
Si ambos tiempos de espera están deshabilitados, las sesiones permanecen divididas debido al vencimiento del tiempo o del tamaño. Sin embargo, el Decoder rastrea el flujo de red mientras tiene suficiente memoria. Por lo tanto, cuando llegan más paquetes en el mismo flujo de red, el Decoder agrega elementos de metadatos `split` a las sesiones posteriores. Mediante una combinación de los metadatos `split` y la clave de flujo, es posible volver a construir el flujo de red a partir de las múltiples sesiones.

La cantidad de tiempo durante el cual se rastrean las sesiones tiene como límite la cantidad de entradas de pool de sesión disponibles en el Decoder y, por lo tanto, la ventana de tiempo real varía según la tasa a la que se agregan nuevas sesiones. Si se agregan nuevas sesiones a alta velocidad, se reduce el tamaño de la ventana de tiempo. El tamaño del pool se establece mediante la entrada de configuración `/decoder/config/assembler.session.pool`, que establece la cantidad máxima de sesiones que se rastrearán a la vez.

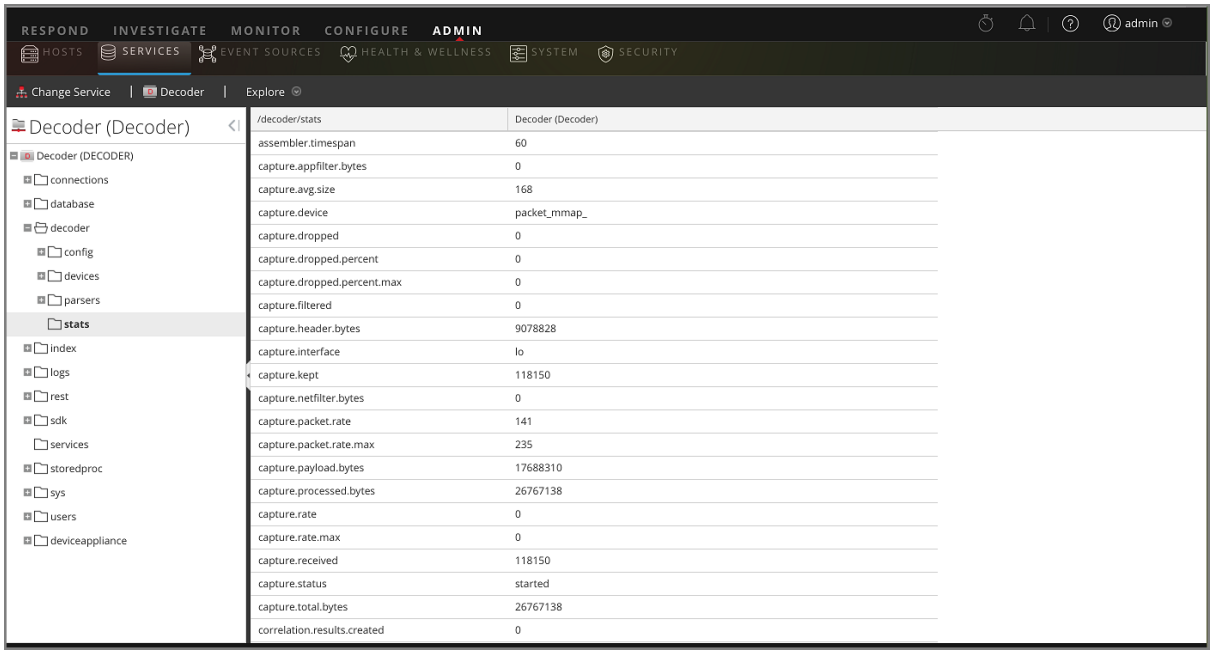
La estadística `/decoder/stats/assembler.timespan` permite ver cuándo el Decoder ya no rastrea las divisiones de las sesiones debido a que la tasa de recopilación es demasiado alta y el Decoder no tiene suficiente memoria para rastrear. Esta estadística indica la cantidad de segundos que se rastrean dentro de la tabla de sesiones, que es la ventana de tiempo efectivo en el cual el Decoder puede vincular las sesiones. En una operación normal esta estadística coincide con el valor de `/decoder/config/assembler.timeout.session`, pero cuando se ejecuta en el modo de división de tiempo, la estadística `/decoder/stats/assembler.timespan` aumenta o disminuye según la tasa de recopilación.

Para configurar el modo de división de tiempo, ajuste los siguientes parámetros de configuración y reinicie el Decoder:

1. En la vista Administration > Servicios, seleccione el servicio Decoder y elija  **> Ver > Explorar.**
2. En la Vista Explorar de servicios seleccione **decoder** > **configuración**.



3. Haga clic en la columna **Valor** junto al parámetro y configure estos dos parámetros:
   `/decoder/config/assembler.session.flush = 0`
   `/decoder/config/assembler.timeout.session = 0`
4. Para ver cuándo el Decoder ya no rastrea las divisiones de las sesiones debido a que la tasa de recopilación es demasiado alta y el Decoder no tiene suficiente memoria para rastrear, vea la estadística `/decoder/stats/assembler.timespan`, en el Vista Explorar de servicios seleccione **decoder** > **estadística**.



Configurar el reenvío de syslog a un destino

Además de recopilar mensajes de syslog, puede configurar Log Decoder para que reenvíe los mensajes de syslog a otro receptor de syslog. NetWitness Platform reenvía mensajes de syslog después de analizarlos y antes de escribirlos en Log Decoder.

Nota: Debe configurar el reenvío de syslog mediante los pasos que se definen en este tema bajo **Procedimiento** y con el uso de la vista **Explorar**.

El Log Decoder debe estar en el estado **Iniciado** antes de poder configurar el reenvío de Syslog. Para configurar el reenvío de syslog:

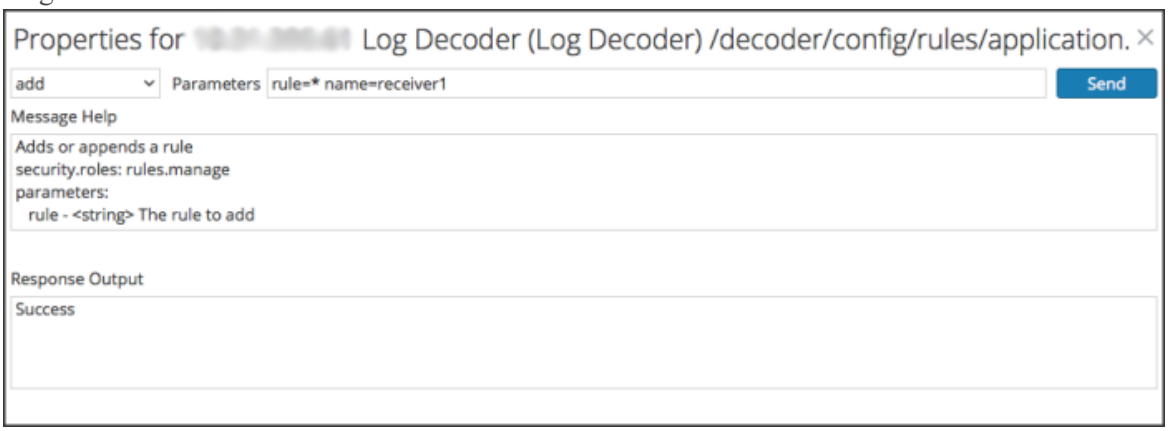
1. Configure reglas de capa de aplicación (reglas de aplicaciones) de Log Decoder para etiquetar los mensajes de syslog con metadatos que den a NetWitness Platform la instrucción de reenviar los mensajes:

   a. Seleccione un Log Decoder en la vista **Servicios** y seleccione > **Ver** > **Explorar** en la columna Acciones.

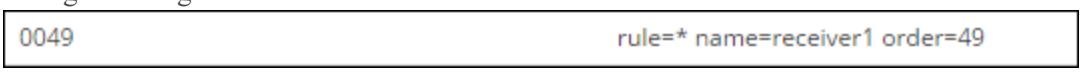
   b. Vaya al nodo **/decoder/config/rules/application**, haga clic con el botón secundario en **application** y haga clic en **Propiedades**.

   c. En la vista **Propiedades**, especifique el comando **add** con los siguientes parámetros:
   `rule=<query> name=<name>`
   Ejemplo 1: `rule=*name=receiver1`
   Ejemplo 2: `rule="device.type='winevent_nic'" name=receiver`)

   d. Haga clic en **Enviar**.



   NetWitness Platform crea la regla `name=receiver1 rule=* order=<n>`. NetWitness Platform inserta el número de orden (por ejemplo, `order=49`) de acuerdo con la fecha en que se configuró la regla.



   e. Vaya al nodo `/decoder/config/rules/application` y haga clic en la regla `name=receiver1 rule=* order=49`.

f. Agregue parámetros **alert forward** a los parámetros de la regla.

```
rule=* name=receiver1 order=49 alert forward
```

Los demás parámetros de la regla tienen el mismo significado que en otras reglas de aplicación.

El siguiente ejemplo de regla de aplicación selecciona todos los registros con la regla `*`. Crea metadatos de alerta con el valor "**`receiver1`**" y etiqueta el registro completo de modo que se reenvíe al destino de reenvío de syslog. Puede definir tantas reglas de reenvío distintas como necesite con el mismo nombre o con nombres únicos.

2. Defina destinos de reenvío de syslog y active el reenvío.

   a. Seleccione un Log Decoder en la vista **Servicios** y elija > **Ver** > **Explorar**.

   b. Los destinos de reenvío de syslog se definen en el nodo de configuración `/decoder/config/logs.forwarding.destination`.
   Este nodo de configuración contiene uno o más pares de nombre/valor. El nombre corresponde a los parámetros de nombre de la regla de aplicación que usó para etiquetar los registros con metadatos de reenvío. El valor es un trío de transporte, host y puerto separados por dos puntos y seguidos de un parámetro de formato opcional.
   `name=(udp|tcp|tls):host:port[:(retainsource|rfc3164)]`
   El primer parámetro indica el protocolo de transporte y debe ser udp, tcp o tls. La especificación de udp reenviará los registros a través del protocolo de syslog RFC 3164 / RFC 5426 UDP. La especificación de tcp reenviará los registros a través de una conexión TCP con tramas RFC 6587. La especificación de tls reenviará los registros de acuerdo con RFC 5425.
   El host es una dirección IPv4, una dirección IPv6 o un nombre de host.

   El puerto es aquél al cual se envían los registros. Por lo general, este es el puerto 514 para syslog UDP y 6514 para las conexiones del protocolo TLS. No hay ninguna asignación de puerto estándar para syslog mediante TCP.

   De manera opcional, `retainsource` o `rfc3164` pueden especificarse al final de la cadena de destino para indicar que se debe incluir formato e información adicionales con cada registro que se reenvía. La especificación de `retainsource` incluirá los encabezados de conector z al principio del registro y se completará con los metadatos `time`, `device.(ip|ipv6|host)` y `lc.cid`, y se utiliza mejor para su reenvío a otros Log Decoders. La opción `rfc3164` antepondrá un encabezado RFC3164 válido a todos los eventos reenviados compuestos por los metadatos `syslog.pri`, `time` y `device.(ip|ipv6|host)`. En ambos casos, el texto del registro original permanece sin modificaciones.

   Destino de reenvío de ejemplo:

   ```
   gears=tls:gears.netwitness.local:6514
   ```

   Reenvío de ejemplo mediante tcp a la falta de disponibilidad en el puerto 514 con encabezados de conector z:

   ```
   fwdrule=tcp:blackout.netwitness.local:514:retainsour
   ```

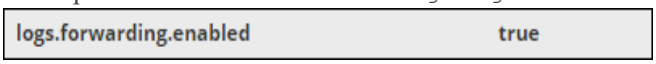
   En el parámetro `/decoder/config/logs.forwarding.destination`, especifique el destino. Por ejemplo:
   Conexiones TLS: `receiver1=tls:receiver1.netwitness.local:6514`
   Conexiones UDP: `receiver1=udp:receiver1.netwitness.local:514`

Conexiones TCP: **`receiver1=tcp:receiver1.netwitness.local:514`**

Nota:
Puede configurar:
- Múltiples reglas para reenviar registros al mismo destino.
- Múltiples reglas para reenviar registros a múltiples destinos.

Para las conexiones del protocolo TLS, el certificado del destino de reenvío se debe validar. La autoridad de certificación que firmó el certificado del destino debe estar presente en el área de almacenamiento de confianza de CA de Log Decoder y el certificado debe residir en el destino o en el receptor de syslog. Consulte "Configurar certificados" en la *Guía de configuración de la recopilación de registros* para obtener información sobre la manipulación del almacén de confianza de CA de Log Decoder. (Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.)

c. En el parámetro `/decoder/config/logs.forwarding.enabled`, especifique **verdadero**.



Configurar el manejo de las transacciones en un Decoder

A partir de la versión 11.0, los administradores pueden configurar un Decoder para que las sesiones entrantes se subdividan en sesiones de transacción más pequeñas cuando usan analizadores LUA, diseñados para crear transacciones. La función permite que los analistas ejecuten analítica de las sesiones divididas en los servicios descendentes como Investigate.

Manejo de transacciones

El nodo de configuración del servicio de Decoder tiene un parámetro nuevo para la configuración del manejo de transacciones: `/decoder/parsers/config/parser.transaction.mode`. Este nodo controla el comportamiento del Decoder cuando un analizador define una transacción dentro de una sesión de red.

Los valores de `parser.transaction.mode` corresponden a los modos de funcionamiento:

- `off` (transacciones desactivadas)
- `meta` (transacciones representadas como elementos de metadatos)
- `split` (sesiones divididas de transacciones)

Transacciones desactivadas

Cuando el modo de transacciones está desactivado, se omiten las transacciones de nivel de aplicación creadas por los analizadores y nada se almacena en la colección para representar la transacción.

Transacciones representadas como elementos de metadatos

En este modo de operación, cuando un analizador genera una transacción de nivel de aplicación, un nuevo elemento de metadatos de tipo `{{trans}}` se agrega a la sesión en el cual se realizó la transacción. El elemento de metadatos `{{trans}}` contiene una lista de otros elementos de metadatos que constituyen la transacción.

Sesiones divididas de transacciones

En este modo de operación, cuando un analizador genera una transacción de nivel de aplicación, se divide la sesión. La división de la sesión se logra de esta forma:

1. Se crea un nuevo elemento de sesión.
2. Los elementos de metadatos de red se copian de la sesión analizada en la nueva sesión.
3. Los elementos de metadatos marcados en la transacción se transfieren de la sesión original a la nueva sesión.

Los siguientes elementos de metadatos se duplican en la sesión dividida desde la sesión que se analizó:

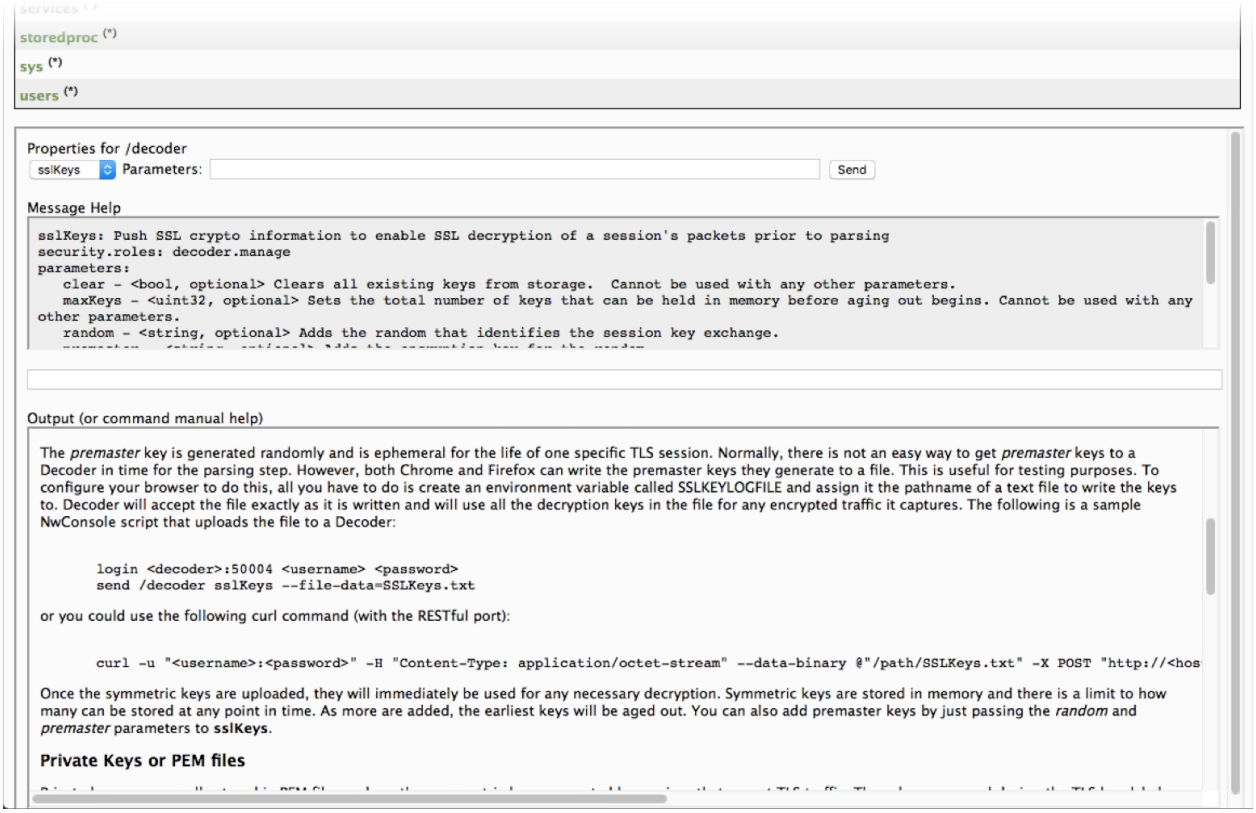
- `time`
- `medium`
- `eth.src`
- `eth.dst`
- `eth.type`
- `ip.proto`
- `ip.src`
- `ip.dst`
- `ipv6.src`
- `ipv6.dst`
- `ipv6.proto`
- `tcp.srcport`
- `tcp.dstport`
- `tcp.flags`
- `udp.srcport`
- `udp.dstport`
- `service`
- `udp.srcport`
- `udp.srcport`
- `tls.premaster`

Descifrar los paquetes entrantes

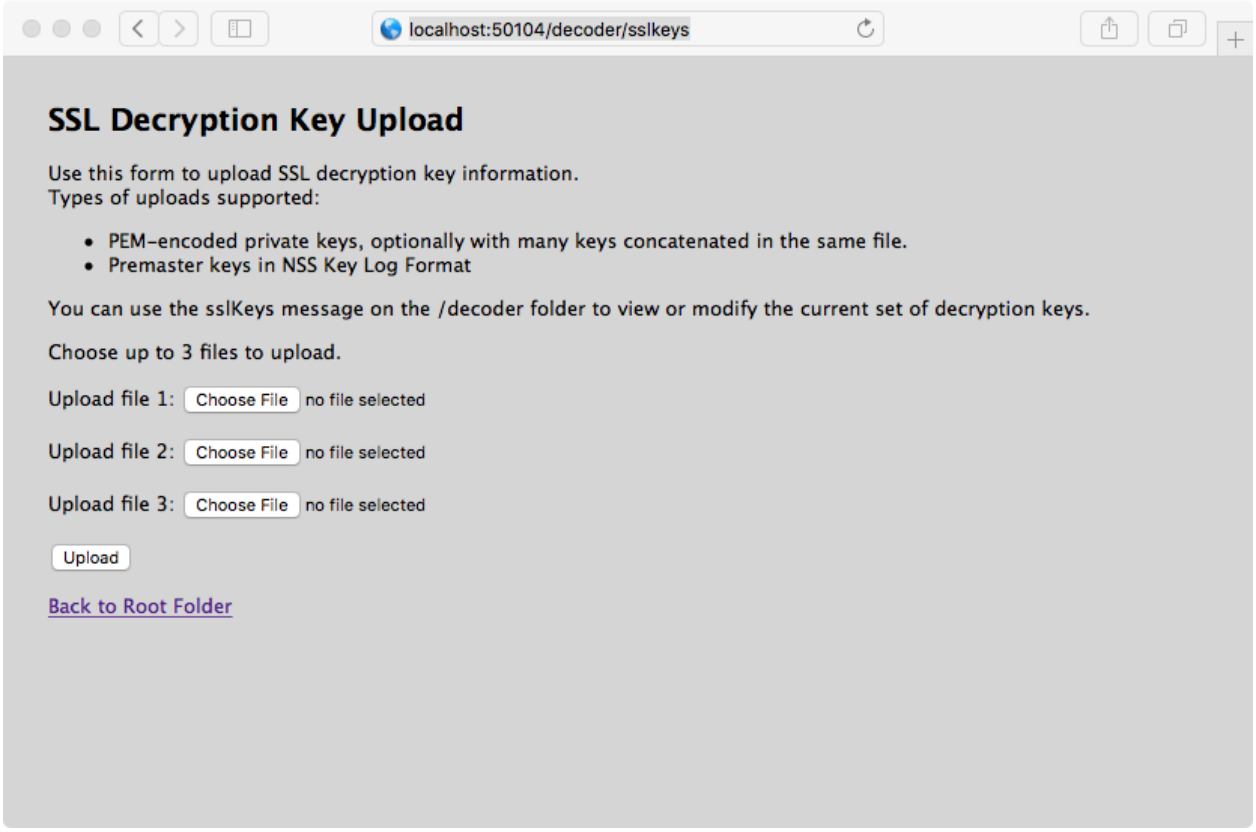
A partir de NetWitness Platform 11.0, los administradores pueden configurar un Network Decoder para descifrar paquetes entrantes mediante el comando `sslKeys`. Los analizadores habilitados verán la carga útil de los paquetes sin cifrar y crearán metadatos según corresponda. Si el Decoder no está configurado para descifrar los paquetes entrantes, la mayoría de los analizadores habilitados verán solo elementos no utilizados cifrados y no podrán crear metadatos significativos.

Nota: Si FIPS está habilitado, la lista de cifrados para descifrado está restringida solo a aquellos que aprueba FIPS.

El comando `sslKeys` proporciona una manera de cargar las claves premaster o privadas en el Decoder, para que los paquetes cifrados capturados que coincidan con las claves puedan descifrarse antes de su análisis. Los administradores configuran el Decoder mediante el ingreso del comando `sslKeys` con la interfaz de la línea de comandos de NwConsole o la interfaz RESTful del Decoder.



El formulario de la interfaz RESTful en la ruta: `/decoder/sslkeys` permite cargar una única clave privada con codificación PEM, un solo archivo que contiene varias claves privadas concatenadas o un único archivo de varias claves de premaster.



A pesar de que los paquetes se descifran durante la etapa de análisis, solo los paquetes cifrados se escriben en el disco. La clave de premaster coincidente que se usa para descifrar se escribe en la clave de metadatos `tls.premaster`, que los analistas pueden usar para ver posteriormente los paquetes sin cifrar según demanda.

A continuación, se proporcionan detalles para que los administradores configuren el descifrado de paquetes entrantes y para que los analistas vean los paquetes sin cifrar según demanda.

Consideraciones de rendimiento

El descifrado de paquetes en tiempo real requiere trabajo adicional en la etapa de análisis. Antes de implementar esta función, planee cuidadosamente a fin de garantizar que el ancho de banda de tráfico entrante no supere la potencia de procesamiento disponible. Puede que necesite más Decoders para descifrar el tráfico en relación con lo que necesitaría si no descifrara.

Los paquetes capturados en un Decoder normalmente tienen un tiempo de espera de aproximadamente 60 segundos en la etapa de ensamblaje antes de que se envíen a la etapa de análisis. Si el Decoder está bajo presión de memoria debido al ancho de banda muy alto, puede disminuir el ciclo de vida de los paquetes en el ensamblador. Para solucionar esta situación, puede configurar un valor de tiempo de espera mayor y aumentar la cantidad de memoria disponible para almacenar los paquetes en el ensamblaje. Además, a fin de llevar a cabo el descifrado de los paquetes, el Decoder debe recibir la clave de descifrado antes de la etapa de análisis.

Nota: Actualmente, se pueden descifrar solo los protocolos TLS 1.2 y anteriores

Sin tener ningún feed cargado, los siguientes analizadores habilitados y un 50 % de las sesiones que se descifran, un Decoder puede procesar el tráfico a 3 GB/s.

Nombre del analizador	Descripción
SYSTEM	Detalles de la sesión
NETWORK	Capa de red
ALERTAS	Alertas
GeoIP	Datos geográficos en función de ip.src e ip.dst
GeoIP2	Datos geográficos de manera predeterminada basados en claves de metadatos IPv4 (ip.src y ip.dst) e IPv6 (ipv6.src y ipv6.dst)
HTTP	Protocolo de transporte de hipertexto (HTTP)
HTTP_Lua	Protocolo de transporte de hipertexto (HTTP) Lua
FTP	Protocolo de transferencia de archivos (FTP)
TELNET	Protocolo TELNET
SMTP	Protocolo simple de transferencia de correo (SMTP)
POP3	Protocolo de oficina de correos (POP3)
NNTP	Protocolo de transporte de noticias de red (NNTP)
DNS	Servicio de nombres de dominio (DNS)
HTTPS	Protocolo de capa de conexión segura (SSL)
MAIL	Formato de correo electrónico estándar (RFC822)
VCARD	Extrae la información de correo electrónico y el nombre completo de VCARD
PGP	Identifica los bloques PGP dentro del tráfico de red
SMIME	Identifica los bloques SMIME dentro del tráfico de red
SSH	Protocolo SSH
TFTP	Protocolo de transferencia de archivos trivial (TFTP)
DHCP	Protocolo de configuración de host dinámico (DHCP y BOOTP)
NETBIOS	Extrae información de nombre de computadora de NETBIOS.
SNMP	Protocolo de administración de redes (SNMP)
NFS	Protocolo de Network File System (NFS)
RIP	Protocolo de información de enrutamiento (RIP).

Nombre del analizador	Descripción
TDS	Protocolo de base de datos MSSQL y Sybase (TDS)
TNS	Protocolo de base de datos de Oracle (TNS)
IRC	Protocolo de Internet Relay Chat (IRC)
RTP	Protocolo de tiempo real (RTP) de audio/video
SIP	Protocolo de inicio de sesión (SIP)
H323	Protocolo de teleconferencia H.323
SCCP	Protocolo de control de cliente ligero de Cisco
GTalk	Google Talk (GTalk)
VlanGre	ID de VLAN y direcciones de túnel GRE/EtherIP
BITTORRENT	Protocolo de uso compartido de archivos de BitTorrent
FIX	Protocolo de intercambio de información financiera
GNUTELLA	Protocolo de uso compartido de archivos de Gnutella
IMAP	Protocolo de acceso a mensajes de Internet
MSRPC	Protocolo de llamada a procedimiento remoto de Microsoft
RDP	Protocolo de escritorio remoto
SHELL	Identificación del shell de comandos
TLSv1	TLSv1
SearchEngines	Un analizador que extrae términos de búsqueda
FeedParser	Analizador de alimentación externa

Claves de cifrado

El comando `sslKeys` acepta dos tipos de claves de cifrado:

- Clave de premaster: la clave simétrica que se usa en el flujo de la carga útil TLS para el cifrado y descifrado.
- Clave privada: la clave privada asimétrica que se usa durante el protocolo de enlace de TLS que cifra la premaster.

Clave de premaster

La clave de premaster se genera aleatoriamente y es efímera durante la vida útil de una sesión específica de TLS. Por lo general, no hay una buena forma de obtener las claves de premaster para un Decoder en el tiempo para la etapa de análisis. Sin embargo, Chrome y Firefox pueden escribir en un archivo las claves de premaster que se generan. Esto es útil para fines de prueba. Para configurar el navegador para que lo haga, cree una variable de ambiente llamada SSLKEYLOGFILE y asígnele el nombre de ruta de un archivo en el que se escribirán las claves. El Decoder aceptará el archivo exactamente como se escribe y usará todas las claves de descifrado en el archivo para todo el tráfico cifrado que capture.

Este es un ejemplo del script NwConsole que el archivo carga en un Decoder:

```
login <decoder>:50004 <username> <password>
send /decoder sslKeys --file-data=SSLKeys.txt
```

Este es un ejemplo del uso de un comando curl (con el puerto RESTful) para cargar el archivo en un Decoder:

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --
data-binary @"/path/SSLKeys.txt" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys"
```

Después de que se cargan las claves simétricas, se usan inmediatamente para cualquier descifrado que sea necesario. Las claves simétricas se almacenan en la memoria y hay un límite para la cantidad que se puede almacenar en cualquier momento específico. Cuando se agregan más claves, las claves más antiguas quedan obsoletas. También puede agregar claves de premaster pasando los parámetros `random` y `premaster` a `sslKeys`.

Claves privadas o archivos PEM

Normalmente, las claves privadas se almacenan en archivos PEM y son las claves asimétricas generadas por los servicios que aceptan el tráfico de TLS. Estas claves se usan durante el protocolo de enlace TLS para cifrar la clave simétrica de premaster que se usará para el resto del cifrado de carga útil.

Por ejemplo, si tiene un servidor web donde desea ver el tráfico, debe cargar la clave privada que usa para cifrar el tráfico. Solo debe hacerlo una vez, puesto que se almacena permanentemente (o hasta que se quita con un comando de eliminación). Las claves privadas se cifran automáticamente antes de almacenarlas para protegerlas. Después de la carga, debe emitir un comando de recarga de analizador de modo que la clave recién instalada se vuelva visible para el analizador HTTPS. Ahora, todos los protocolos de enlace TLS que usan esa clave privada se podrán descifrar con el Decoder.

Nota: No todos los conjuntos de aplicaciones de cifrado usan una clave privada “conocida” (por ejemplo, Ephemeral Diffie Hellman). No se puede descifrar el tráfico cifrado con esos cifrados, a menos que la clave de premaster se cargue en el Decoder antes del análisis de la sesión.

Estos son algunos ejemplos de comandos que cargan un archivo PEM que se usará para el descifrado.

Uso de NwConsole:

```
send /decoder sslKeys pemFilename=MyKey.pem --file-data=/path/MyKey.pem
```

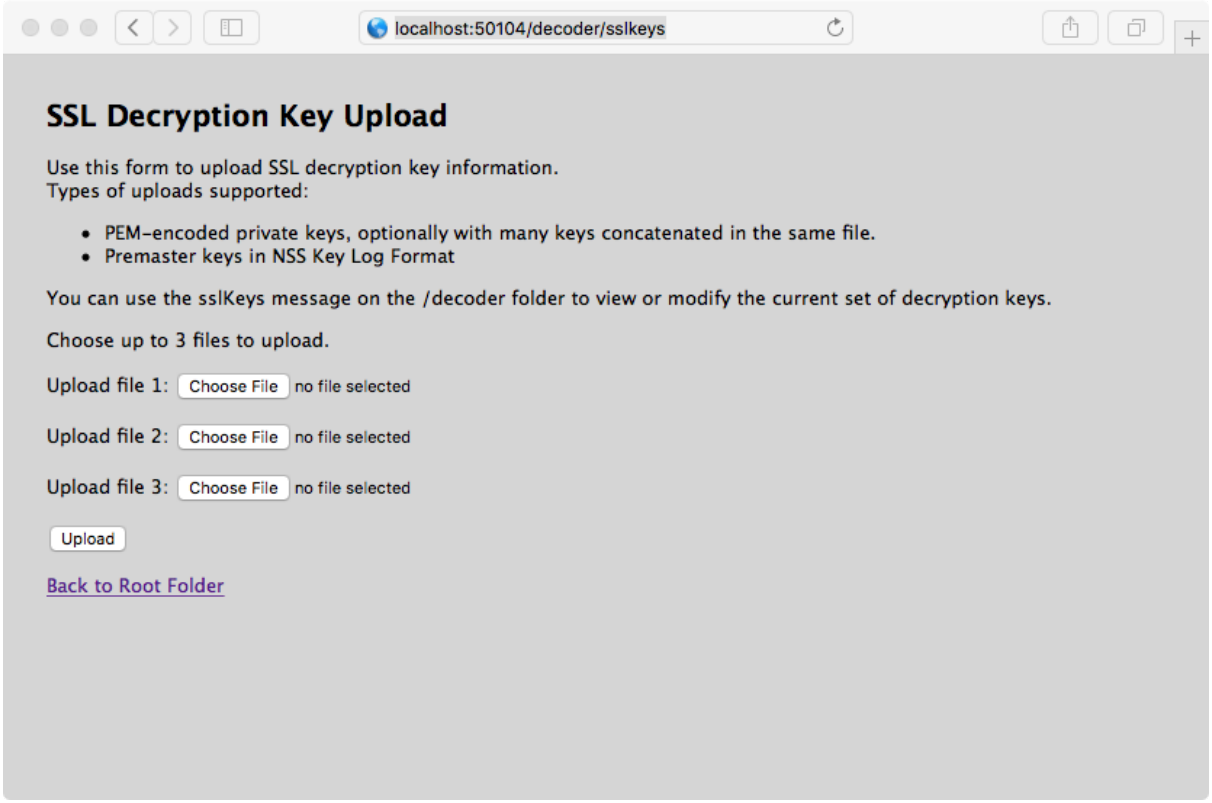
Mediante la interfaz RESTful (debe proporcionar el parámetro `pemFilename` en la URL):

```
curl -u "<username>:<password>" -H "Content-Type: application/octet-stream" --
data-binary @"/path/MyKey.pem" -X POST
"http://<hostname>:50104/decoder?msg=sslKeys&pemFilename=MyKey.pem"
```

Cargar varias claves de premaster y privadas

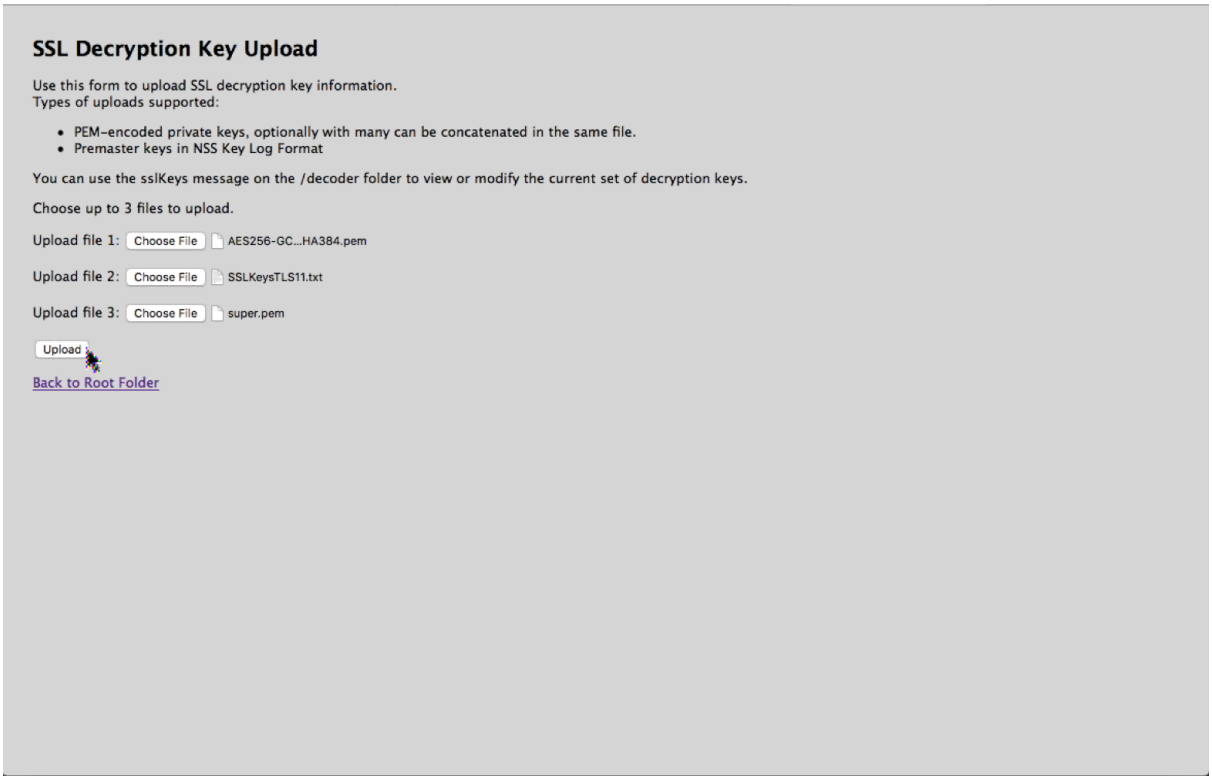
Puede usar el formulario de la interfaz RESTful para facilitar la carga de varias claves, premaster y privadas, al mismo tiempo.

1. Abra la API RESTful en el navegador y vaya a esta ruta en el Decoder que desea configurar: `/decoder/sslkeys`.

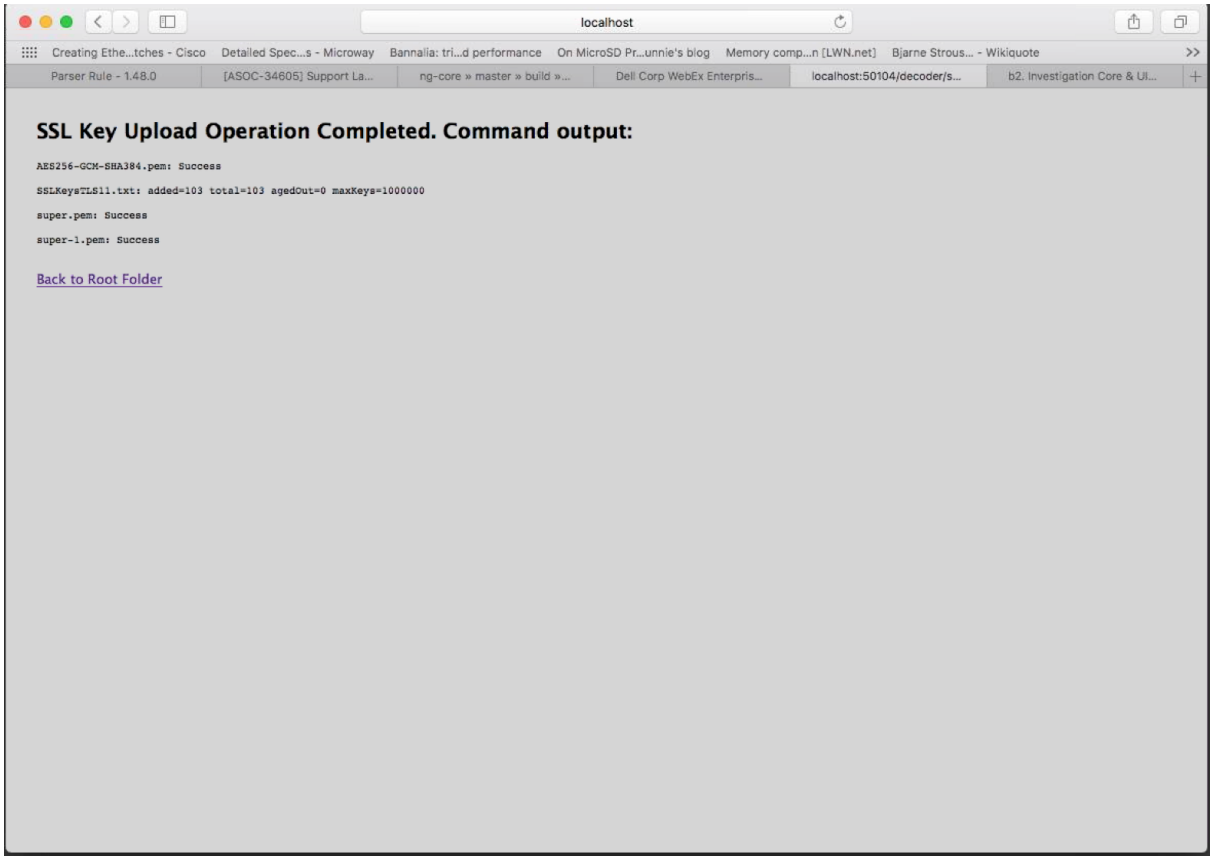


2. Junto a **Cargar archivo 1**, haga clic en **Elegir archivo** y busque el archivo de clave de premaster o el archivo PEM que desea cargar en el sistema de archivos local.

3. (Opcional) Repita estos pasos para **Cargar archivo 2** y **Cargar archivo 3**.



4. Haga clic en **Cargar**.
   Los archivos se cargan en el Decoder y los resultados se muestran en el formulario.



Parámetros para la administración de claves

El comando `sslKeys` tiene varios parámetros para la administración de claves de premaster y privadas. Esta es la lista completa de parámetros:

Parámetro	Descripción
`clear`	Quita todas las claves de premaster de la memoria. No elimina ningún archivo PEM instalado en el sistema.
`maxKeys`	Cambia el número máximo de claves de premaster que se almacenan en la memoria.
`listPems`	Muestra una lista de todos los archivos PEM de claves privadas instalados.
`deletePem`	Elimina el archivo PEM con nombre desde el sistema de archivos. Este parámetro se puede pasar más de una vez para quitar varios archivos.
`random`	El hash aleatorio que se usa para identificar la clave de premaster.

Parámetro	Descripción
premaster	La clave de premaster que se instalará para el parámetro random anterior. Se deben mostrar en pares y random debe estar en primer lugar.

Valores de retorno

La mayoría de los comandos sslKeys devuelve pares de nombre/valor de estadísticas acerca de las claves de premaster en la memoria. Las estadísticas se enumeran en la siguiente tabla.

Nombre	Descripción
added	La cantidad de claves de premaster que se acaba de agregar durante este comando.
total	La cantidad total de claves de premaster cargadas en la memoria.
agedOut	La cantidad total de claves de premaster que se quitaron durante este comando; esta no es una estadística de duración.
maxKeys	El máximo permitido de claves de premaster

Visualización del tráfico sin cifrar

Si los paquetes se descifran durante la etapa de análisis, los paquetes cifrados se escriben en el disco y la clave de premaster coincidente que se usa para descifrar se escribe en la clave de metadatos tls.premaster, los analistas pueden ver los paquetes sin cifrar mediante la clave de metadatos tls.premaster.

Una API del Decoder que puede usar para ver los paquetes sin cifrar es el servicio RESTful /sdk/content. Debe conocer el ID de sesión de los paquetes cifrados y el parámetro flags enmascarado en el valor 128 (o 0x80 en hexadecimal). Dirija el navegador a la interfaz RESTful del Decoder y escriba el siguiente comando, sustituyendo el ID de sesión real por <id>:

http://<decoder>:50104/sdk/content?session=<id>&flags=128&render=text

El Decoder despliega una página web simple que muestra los paquetes después de que se descifran.

Si desea ver el aspecto de los paquetes cifrados, escriba uno de los siguientes comandos, sustituyendo el ID de sesión por <id>:

http://<decoder>:50104/sdk/content&session=<id>&render=text

http://<decoder>:50104/sdk/content&session=<id>&flags&render=text

Para obtener más información sobre el servicio /sdk/content, consulte la página del manual de /sdk content.

Suites de cifrado compatibles

En la siguiente tabla se enumeran las suites de cifrado que son compatibles con el uso de claves privadas.

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	[0xc030]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	[0xc02c]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	[0xc028]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	[0xc024]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	[0xc014]	SSLv3	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	[0xc00a]	SSLv3	Kx=ECDH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	DHE-DSS-AES256-GCM-SHA384	[0xa3]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	[0x9f]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	[0x6b]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	DHE-DSS-AES256-SHA256	[0x6a]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	[0x39]	SSLv3	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA	[0x38]	SSLv3	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	DHE-RSA-CAMELLIA256-SHA	[0x88]	SSLv3	Kx=DH	No cumple con las normas	No compatible
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	DHE-DSS-CAMELLIA256-SHA	[0x87]	SSLv3	Kx=DH	No cumple con las normas	No compatible
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	ECDH-RSA-AES256-GCM-SHA384	[0xc032]	SSLv3	Kx=ECDH/RSA	Cumple con la norma	No compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	ECDH-ECDSA-AES256-GCM-SHA384	[0xc02e]	TLSv1.2	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	ECDH-RSA-AES256-SHA384	[0xc02a]	TLSv1.2	Kx=ECDH/RSA	Cumple con la norma	No compatible
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	ECDH-ECDSA-AES256-SHA384	[0xc026]	TLSv1.2	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	ECDH-RSA-AES256-SHA	[0xc00f]	SSLv3	Kx=ECDH/RSA	Cumple con la norma	No compatible
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	ECDH-ECDSA-AES256-SHA	[0xc005]	SSLv3	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384	[0x9d]	TLSv1.2	Kx=RSA	Cumple con la norma	Compatible
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256	[0x3d]	TLSv1.2	Kx=RSA	Cumple con la norma	Compatible
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA	[0x35]	SSLv3	Kx=RSA	Cumple con la norma	Compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	CAMELLIA256-SHA	[0x84]	SSLv3	Kx=RSA	No cumple con las normas	Compatible
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	[0xc012]	SSLv3	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	[0xc008]	SSLv3	Kx=ECDH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	[0x16]	SSLv3	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	EDH-DSS-DES-CBC3-SHA	[0x13]	SSLv3	Kx=DH	Cumple con la norma	No compatible
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	ECDH-RSA-DES-CBC3-SHA	[0xc00d]	SSLv3	Kx=ECDH/RSA	Cumple con la norma	No compatible
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH-ECDSA-DES-CBC3-SHA	[0xc003]	SSLv3	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA	[0x0a]	SSLv3	Kx=RSA	Cumple con la norma	Compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	[0xc02f]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	[0xc02b]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	[0xc027]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	[0xc023]	TLSv1.2	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	[0xc013]	SSLv3	Kx=ECDH	Cumple con la norma	No compatible
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	[0xc009]	SSLv3	Kx=ECDH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	DHE-DSS-AES128-GCM-SHA256	[0xa2]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	[0x9e]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	[0x67]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	DHE-DSS-AES128-SHA256	[0x40]	TLSv1.2	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	[0x33]	SSLv3	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA	[0x32]	SSLv3	Kx=DH	Cumple con la norma	No compatible
TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE-RSA-SEED-SHA	[0x9a]	SSLv3	Kx=DH	No cumple con las normas	No compatible
TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE-DSS-SEED-SHA	[0x99]	SSLv3	Kx=DH	No cumple con las normas	No compatible
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	DHE-RSA-CAMELLIA128-SHA	[0x45]	SSLv3	Kx=DH	No cumple con las normas	No compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	DHE-DSS-CAMELLIA128-SHA	[0x44]	SSLv3	Kx=DH	No cumple con las normas	No compatible
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	ECDH-RSA-AES128-GCM-SHA256	[0xc031]	TLSv1.2	Kx=ECDH/RSA	Cumple con la norma	No compatible
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	ECDH-ECDSA-AES128-GCM-SHA256	[0xc02d]	TLSv1.2	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	ECDH-RSA-AES128-SHA256	[0xc029]	TLSv1.2	Kx=ECDH/RSA	Cumple con la norma	No compatible
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	ECDH-ECDSA-AES128-SHA256	[0xc025]	TLSv1.2	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	ECDH-RSA-AES128-SHA	[0xc00e]	SSLv3	Kx=ECDH/RSA	Cumple con la norma	No compatible
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH-ECDSA-AES128-SHA	[0xc004]	SSLv3	Kx=ECDH/ECDSA	Cumple con la norma	No compatible
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256	[0x9c]	TLSv1.2	Kx=RSA	Cumple con la norma	Compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256	[0x3c]	TLSv1.2	Kx=RSA	Cumple con la norma	Compatible
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA	[0x2f]	SSLv3	Kx=RSA	Cumple con la norma	Compatible
TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA	[0x96]	SSLv3	Kx=RSA	No cumple con las normas	Compatible
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	CAMELLIA128-SHA	[0x41]	SSLv3	Kx=RSA	No cumple con las normas	Compatible
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA	[0x07]	SSLv3	Kx=RSA	No cumple con las normas	Compatible
TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA	[0xc011]	SSLv3	Kx=ECDH	No cumple con las normas	No compatible
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	[0xc007]	SSLv3	Kx=ECDH	No cumple con las normas	No compatible
TLS_ECDH_RSA_WITH_RC4_128_SHA	ECDH-RSA-RC4-SHA	[0xc00c]	SSLv3	Kx=ECDH/RSA	No cumple con las normas	No compatible

Nombre de la suite de cifrado (RFC)	Nombre (OpenSSL)	Suite de cifrado	Versión de TLS	Intercam. de claves	FIPS	Clave privada
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	ECDH-ECDSA-RC4-SHA	[0xc002]	SSLv3	Kx=ECDH/ECDSA	No cumple con las normas	No compatible
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA	[0x05]	SSLv3	Kx=RSA	No cumple con las normas	Compatible
TLS_DHE_RSA_WITH_DES_CBC_SHA	EDH-RSA-DES-CBC-SHA	[0x15]	SSLv3	Kx=RSA	No cumple con las normas	No compatible
TLS_DHE_DSS_WITH_DES_CBC_SHA	EDH-DSS-DES-CBC-SHA	[0x12]	SSLv3	Kx=DSS	No cumple con las normas	No compatible
TLS_RSA_WITH_DES_CBC_SHA	DES-CBC-SHA	[0x09]	SSLv3	Kx=RSA	No cumple con las normas	Compatible
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-RSA-DES-CBC-SHA	[0x14]	SSLv3	Kx=DSS	No cumple con las normas	No compatible
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA	EXP-EDH-DSS-DES-CBC-SHA	[0x11]	SSLv3	Kx=DSS	No cumple con las normas	No compatible
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	EXP-DES-CBC-SHA	[0x08]	SSLv3	Kx=DES	No cumple con las normas	Compatible

Aplicación de hash al certificado TLS

El Network Decoder puede producir hashes de certificados que se ven en el flujo de paquetes. Estos hashes son el valor SHA-1 de cualquier certificado con codificación DER encontrado durante un protocolo de enlace TLS. Los hashes producidos se pueden utilizar para comparar el tráfico de red con hashes de listas negras SSL públicas, como la de sslbl.abuse.ch.

La característica de aplicación de hash al certificado TLS está deshabilitada de manera predeterminada. Se puede habilitar agregando la opción del analizador:

```
HTTPS="cert.sha1=true"
```

a la configuración `/decoder/parsers/config/parsers.options` de un Network Decoder.

Cuando esta opción está habilitada, el valor SHA-1 se almacena como un valor de texto en la clave metadatos:

```
cert.checksum
```

Editar la configuración del sistema de Decoder

Cuando un servicio se agrega por primera vez a NetWitness Platform, se aplican los valores predeterminados para los parámetros de configuración del sistema. En la mayoría de los casos, los valores predeterminados para la compresión, el intervalo de actualización de estadísticas y la cantidad de hilos de ejecución en el pool se definen en un buen punto para obtener un rendimiento óptimo del sistema. No es necesario editar estas configuraciones a menos que un técnico de servicio al cliente de RSA recomiende cambiarlas.

System Configuration

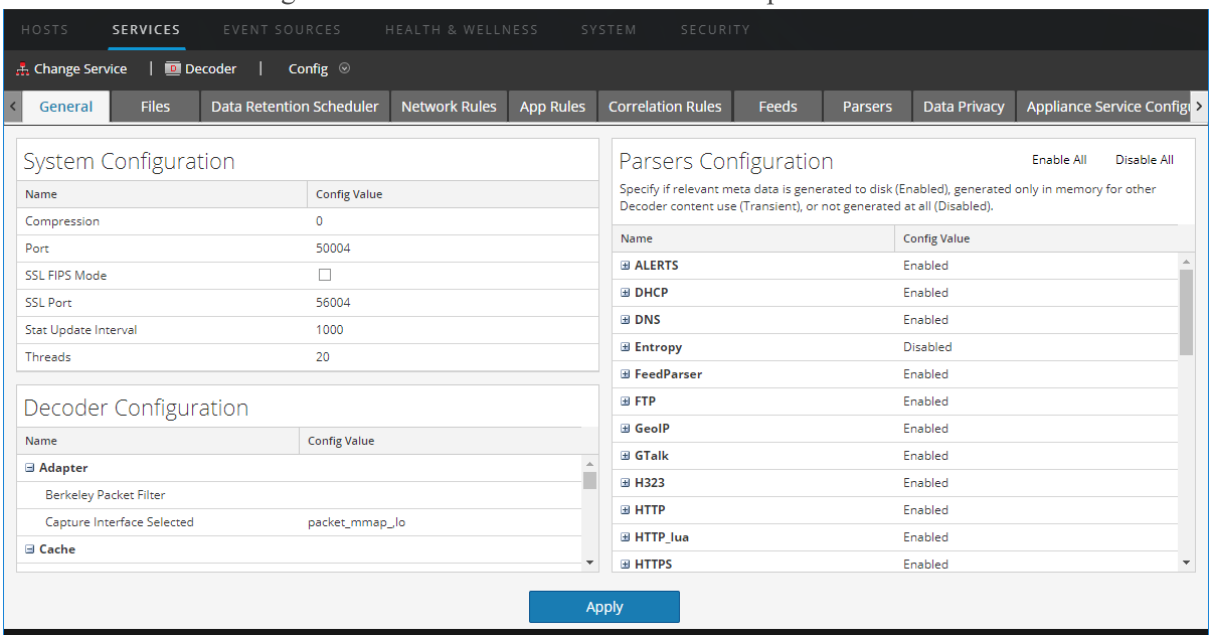
Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	☐
SSL Port	56004
Stat Update Interval	1000
Threads	20

Un parámetro que posiblemente desee cambiar para su ambiente es el ajuste del SSL, el cual no está activado de manera predeterminada. Cuando se habilita, la seguridad de la transmisión de datos se administra mediante el cifrado de información y la entrega de autenticación con certificados SSL.

Para editar parámetros de configuración del sistema para un Decoder o un Log Decoder:

1. Vaya a **ADMINISTRAR > Servicios**.
2. En la vista Admin > Sistema, seleccione un servicio Decoder o Log Decoder y elija  **> Ver > Configuración**.

Se muestra Vista Configuración de servicios del servicio con la pestaña General abierta.



3. En **Configuración del sistema**, haga clic en un campo que desee editar **(Compresión**, **Puerto**, **Modo SSL FIPS**, **Puerto SSL**, **Intervalos de actualización de estadísticas** o **Subprocesos**). Escriba un nuevo valor.
4. Cuando haya completado la edición, haga clic en **Aplicar.**
   Los cambios se implementan de inmediato.

Habilitar las estadísticas de uso de CPU para el contenido instalado

A partir de RSA NetWitness® Platform 11.0, el Decoder proporciona estadísticas de uso de CPU para todo el contenido instalado, que puede usar para dar a conocer cuánto tiempo de CPU usan los analizadores, los feeds, las reglas de aplicación y el análisis léxico. Las estadísticas se pueden ver como nodos de estadísticas en el árbol de servicios en la vista Explorar cuando `/decoder/parsers/config/detailed.stats` está habilitado y el Decoder las está capturando.

Cada contenido se considera como un valor de porcentaje único (0 a 100) independientemente del número de subprocesos de análisis que se ejecutan. El porcentaje representa un promedio del uso de CPU para el contenido a través de todos los subprocesos.

Para habilitar el monitoreo de estadísticas de uso:

1. Navegue a la vista Explorar de Decoder y seleccione el parámetro `/decoder/parsers/config/detailed.stats`.
2. Cambie el valor a **habilitado**. Si el Decoder no captura datos, inicie la captura.
   Cuando abra el nodo de estadísticas de Decoder en la vista Explorar, podrá ver la nueva estadística.

Habilitar mapeos de analizadores

En este tema se indica a los administradores cómo habilitar el mapeo de orígenes de eventos en un Log Decoder.

El Log Collector descubre el tipo de origen de eventos por mensaje. Si no se identifica el analizador correcto para el origen de eventos, un pequeño porcentaje de los registros se puede identificar erróneamente. Los mensajes clasificados incorrectamente no completan las reglas y las alertas de orígenes de eventos y los informes no tienen los datos correctos. Si hay múltiples tipos de orígenes de eventos asociados con una dirección IP, es difícil para los analizadores identificar el origen de eventos exacto desde el cual se generan los registros.

Si mapea una dirección IP a su tipo de origen de eventos, el Log Decoder puede identificar el origen de eventos desde el cual se genera el registro. Cuando se distribuyen mensajes al Log Decoder desde un origen de eventos mapeado, solo se consultan los analizadores asignados para encontrar coincidencias de eventos.

Puede asignar tipos de orígenes de eventos a IPV4, IPV6 o al valor de nombre de host del origen de eventos. También puede asignar múltiples tipos de orígenes de eventos a una única dirección IP. También puede usar el ID de Log Collector cuando se envían distintos tipos de orígenes de eventos con la misma dirección IP a los distintos Log Collectors.

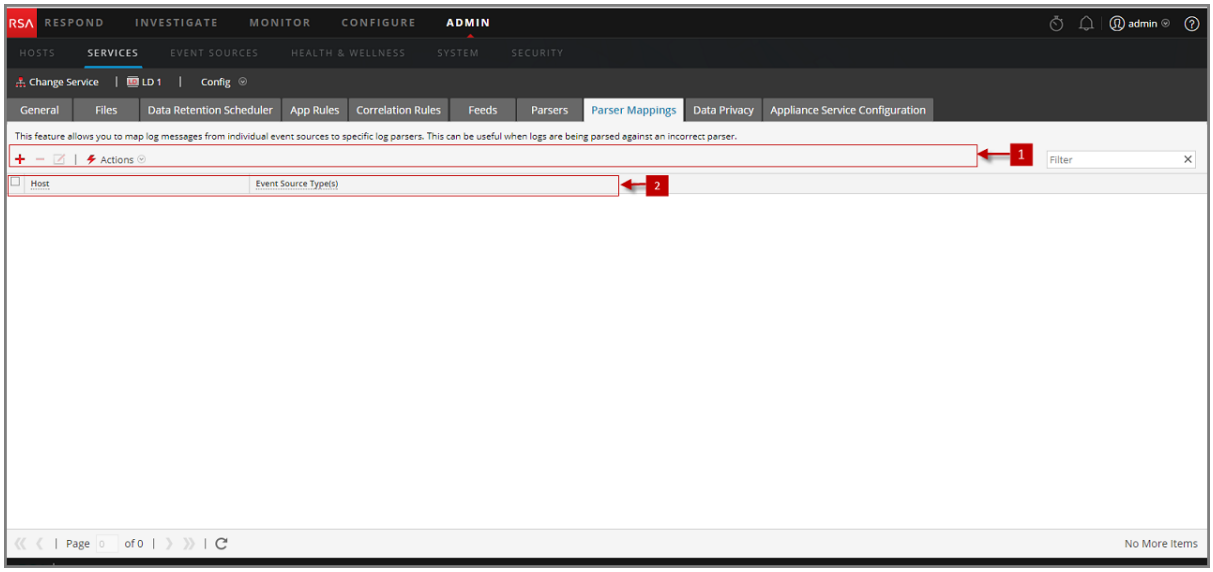
Nota: También puede habilitar las funciones de mapeo del analizador desplazándose a **ADMINISTRAR > Orígenes de eventos > Descubrimiento.**

Habilitar un mapeo de dirección IP a origen de eventos

Para habilitar un mapeo de dirección IP a origen de eventos:

1. Vaya a **ADMINISTRAR > Servicios** y seleccione un Log Decoder.
2. Seleccione  **> Ver > Configuración**.

3. En la página Configuración, seleccione la pestaña **Mapeos de analizador**.
   La pestaña Mapeos de analizador se muestra en la vista Configuración de servicios.

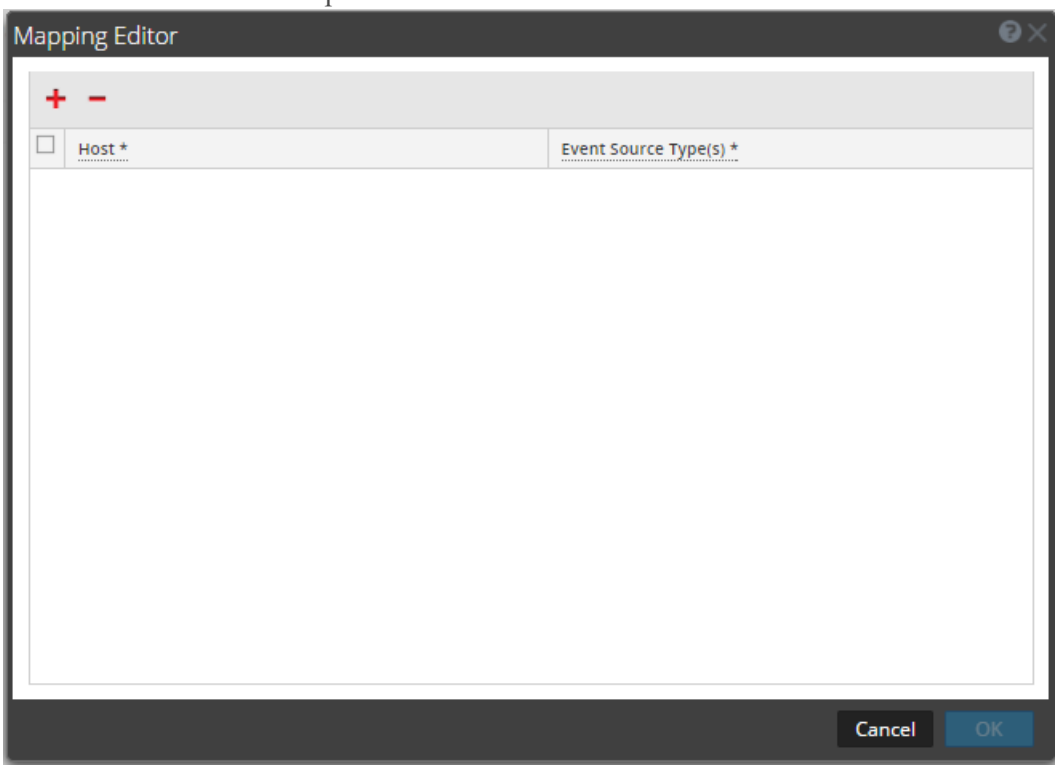


Actualizar un mapeo de dirección IP a origen de eventos

Para actualizar un mapeo de dirección IP a origen de eventos:

1. Vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un **Log Decoder** y, en la columna **Acciones**, elija > **Ver > Configuración**.
   Se muestra la vista Configuración de servicios.
3. Seleccione la pestaña **Mapeo de analizadores**.
4. Haga clic en .

Se muestra el Editor de mapeos.



5. Es posible definir cualquiera de los siguientes mapeos:

- **Un host y un tipo de origen de eventos**
  En el campo **Host**, ingrese el nombre de host.
  Por ejemplo: `10.0.0.1`
- En el campo **Orígenes de eventos**, ingrese el tipo de origen de eventos.
  Por ejemplo: `apache`
- **Un host y uno o más tipos de orígenes de eventos**
  En el campo **Host**, ingrese el nombre de host.
  Por ejemplo: `10.0.0.1`
- En el campo **Orígenes de eventos**, ingrese el tipo de origen de eventos.
  Por ejemplo: `apache,sap,aix`
- **Un host, un Log Collector y un tipo de origen de evento**
  En el campo **Host**, ingrese el nombre de host y el ID de Log Collector.
  Por ejemplo: `10.0.0.1,LC-1`
- En el campo **Orígenes de eventos**, ingrese el tipo de origen de eventos.
  Por ejemplo: `apache`
- **Un host, un ID de Log Collector y uno o más tipos de orígenes de eventos**
  En el campo **Host**, ingrese el nombre de host y el ID de Log Collector.
  Por ejemplo: `10.0.0.1,LC-1`

- En el campo **Orígenes de eventos**, ingrese el tipo de origen de eventos.
  Por ejemplo: `apache,sap,aix`

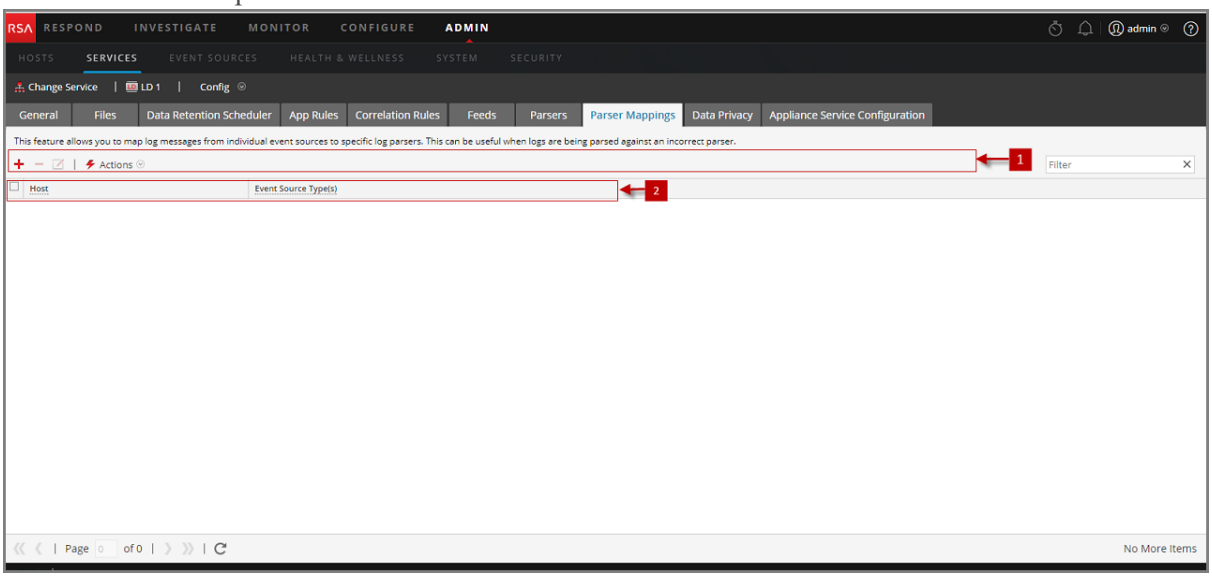
> **Nota:** Los tipos de orígenes de eventos se procesan en el orden en que se ingresan los analizadores y, si uno o más analizadores coinciden con un registro, se consulta el primer analizador de la lista. El host/IP puede ser IPv4, IPv6 o nombre de host.

9. Haga clic en **Aceptar**.
   El mapeo de analizadores se agrega.
7. Para cancelar la selección de mapeos de analizadores, haga clic en **Cancelar**.

Leer mapeos de dirección IP a tipo de origen de eventos

Para leer mapeos de dirección IP a tipo de origen de eventos:

1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración de servicios.
3. Seleccione la pestaña **Mapeo de analizadores**.
   Se muestran los mapeos.



Editar un mapeo de dirección IP a tipo de origen de eventos

Para editar un mapeo de dirección IP a tipo de origen de eventos:

1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
3. Seleccione la pestaña **Mapeos de analizadores**.

4. Seleccione el mapeo que desea editar.
   Nota: Solo puede editar un mapeo a la vez.
5. Haga clic en 
6. En el campo **Orígenes de eventos**, modifique los orígenes de eventos.
   Nota: El host no se puede editar y el campo está deshabilitado.
7. Haga clic en **Aceptar** para aceptar el origen de evento editado.
8. Para cancelar los cambios, haga clic en **Cancelar**.

Eliminar un mapeo de dirección IP a tipo de origen de eventos

Para eliminar un mapeo de dirección IP a tipo de origen de eventos:

1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
3. Seleccione la pestaña **Mapeos de analizadores**.
4. Seleccione el mapeo que desea eliminar.
5. Haga clic en .
   Se elimina el mapeo y se actualiza la cuadrícula.
6. Para cancelar los cambios, haga clic en **Cancelar**.

Ordenar el nombre de host o el tipo de origen de eventos

Para ordenar el nombre de host o el tipo de origen de eventos:

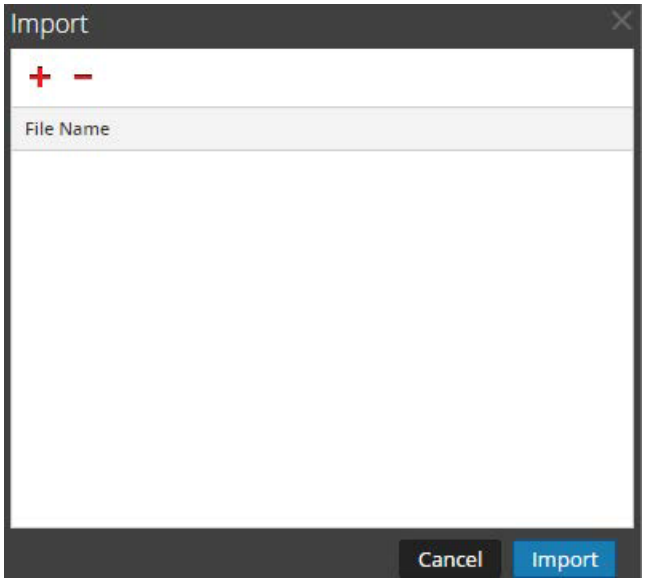
1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
3. Seleccione la pestaña **Mapeos de analizadores**.
4. Para ordenar una columna, haga clic en
   en su encabezado.Los tipos de origen de eventos se aplican para la dirección IP seleccionada. Los registros se analizan en los analizadores en el orden en que aparecen.

Importar entradas de mapeo de dirección IP a origen de eventos

Para importar entradas de mapeo de dirección IP a origen de eventos:

1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
3. Seleccione la pestaña **Mapeos de analizadores**.

4. Seleccione **Acciones > Importar**.
   Se muestra el cuadro de diálogo Importar.



5. Haga clic en + .
6. Seleccione el archivo que desea importar y haga clic en **Aceptar**.
7. Para cargar el analizador, haga clic en **Importar**.

Nota: Solo puede importar un archivo .csv por vez.

Exportar entradas de mapeo de dirección IP a origen de eventos

Para exportar entradas de mapeo de dirección IP a origen de eventos:

1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
3. Seleccione la pestaña **Mapeos de analizadores**.
4. Seleccione los mapeos que desea exportar.
5. Seleccione **Acciones > Exportar > Selección**.
   Se muestra el cuadro de diálogo Exportar selección.

6. Ingrese el nombre de archivo y haga clic en **Exportar**.

Buscar entradas de mapeo de dirección IP a origen de eventos

Para buscar entradas de mapeo de dirección IP a origen de eventos:

1. Vaya a **ADMIN > Servicios** y seleccione un servicio Log Decoder.
2. En la columna Acciones, seleccione **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
3. Seleccione la pestaña **Mapeos de analizadores**.
4. En la barra de herramientas Mapeo de analizadores, ingrese el host o el origen de eventos en el campo **Filtro**.
5. Haga clic en **Intro**.
   Se muestran los hosts o los orígenes de eventos que coinciden con los nombres ingresados en el campo **Filtro**.

Habilitar o deshabilitar los sistemas de análisis Lua y Flex

En este tema se indica a los administradores cómo habilitar o deshabilitar los sistemas de análisis Lua y Flex en un Decoder o un Log Decoder. Los analizadores flexibles están en desuso y deshabilitados de manera predeterminada.

Los ajustes para habilitar o deshabilitar los sistemas de análisis Lua y Flex están configurados correctamente de manera predeterminada y, por lo general, no es necesario cambiarlos. Sin embargo, es posible que deba ajustar está configuración a solicitud de Atención al cliente de RSA o con fines de solución de problemas.

Además de configurar analizadores individuales, puede habilitar y deshabilitar todo el análisis Lua y todo el análisis Flex en la vista Explorar de los servicios. Los ajustes de los sistemas de análisis Lua y Flex se habilitan y deshabilitan por separado, pero funcionan de la misma manera.

- Si **deshabilita** el sistema de análisis Lua o Flex, estos quedan deshabilitados y no se cargan analizadores.
- Si **habilita** el sistema de análisis Lua o Flex, estos quedan habilitados y los analizadores individuales se habilitan y deshabilitan de acuerdo con las configuraciones individuales actuales.

Para habilitar o deshabilitar los sistemas de análisis Lua y Flex en un Decoder o un Log Decoder:

1. Vaya a **ADMINISTRAR > Servicios.**
2. Seleccione un Decoder o un Log Decoder y elija  **> Ver > Explorar.**
   Se muestra la vista Explorar del servicio seleccionado.
3. En la lista Nodo, navegue a **`/decoder/parsers/config`** selecciónelo.
4. En el panel Monitor:
   - Para habilitar el sistema de análisis Lua, en el campo de valor correspondiente a `lua.enabled`, escriba **yes**.
   - Para deshabilitar el sistema de análisis Lua, en el campo de valor correspondiente a `lua.enabled`, escriba **no**.
   - Para habilitar el sistema de análisis Flex, en el campo de valor correspondiente a `flex.enabled`, escriba **yes**.
   - Para deshabilitar el sistema de análisis Flex, en el campo de valor correspondiente a `flex.enabled`, escriba **no**.

Mapear una dirección IP a un tipo de servicio para análisis de registros

En este tema se describe el procedimiento para mapear una dirección IP a un tipo de servicio para análisis de registros.

El Log Collector describe el tipo de origen de eventos por mensaje. Si no se usa el analizador correcto para el origen de eventos específico, los mensajes que son comunes entre los tipos de orígenes de eventos se clasifican en forma equívoca. Los mensajes mal identificados no completarán reglas y alertas de servicio, y los informes no tendrán información adecuada. Además, si hay múltiples servicios asociados con una dirección IP, puede ser difícil para los analizadores identificar el servicio exacto desde donde se generó el registro.

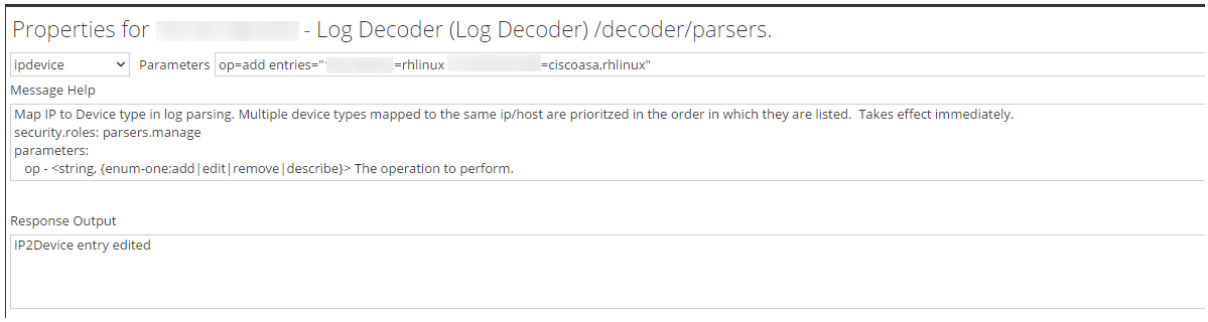
Si mapea una dirección IP a sus servicios, el Log Decoder puede identificar el servicio desde donde se genera el registro. Cuando llegan los mensajes a Log Decoder desde un servicio mapeado, se cargan los analizadores asignados para buscar coincidencias de eventos.

Puede asignar tipos de servicios a IPV4, IPV6 o al valor de nombre de host del origen de eventos. También puede asignar múltiples tipos de servicio a una única dirección IP. Además, puede usar CollectorID cuando se envían distintos tipos de servicio con la misma dirección IP a los distintos recopiladores.

Mapear una dirección IP a un tipo de servicio

Para mapear una dirección IP a un tipo de servicio, realice lo siguiente:

1. Vaya a **ADMINISTRAR > Servicios**.
2. En la vista **Servicios**, seleccione un Log Decoder y en la columna **Acciones**, seleccione  **> Ver > Explorar**.
3. Vaya al nodo **/decoder/parsers**, haga clic con el botón secundario en **parsers** y seleccione **Propiedades**.
4. En la vista **Propiedades**, especifique el comando **ipdevice** con los siguientes parámetros: `op=add/remove entries="ipaddress=service"` (por ejemplo, `op=add entries="10.100.201.300=ciscoasa"`)
5. Haga clic en **Enviar**.



Comando IPdevice

En el comando `ipdevice`, hay tres operaciones disponibles:

- `add`: esta operación agrega o actualiza las entradas en el mapa de ipdevice. Se pueden especificar varios pares de dirección/tipo delimitados por espacios.
  `op=add entries="<address>=<service type>"`
- `remove`: esta operación quita las entradas del mapa de ipdevice. Se pueden especificar varios pares de dirección/tipo delimitados por espacios.
  `op=remove entries="<address>"`
- `describe`: esta operación devuelve los valores que están actualmente en el mapa de ipdevice.

Asignar una dirección IP a una zona horaria

A menudo los registros de tiempo no especifican registros de fecha y hora, y es probable que no tengan información de zona horaria. Para normalizar correctamente dichos registros de fecha y hora en UTC, el Log Decoder proporciona la capacidad para asociar los dispositivos desde una dirección específica (IPv4 o IPv6) o el nombre de host a una zona horaria o una compensación fija.

Actualmente, se aceptan tres formatos de zona horaria, los que se muestran en los siguientes ejemplos:

- Formato de Olson: América/Anguila
- Formato POSIX: AST2:45ADT0:45,M4.1.6/1:45,M10.5.6/2:45
- Formato de compensación por horas: = -500

NetWitness Platform asigna la dirección del dispositivo (IPv4 o IPv6) o el nombre de host a una zona horaria o compensación específicas. Los metadatos de hora del evento que se analizan desde un registro proveniente de una dirección asignada que no incluye una compensación o una zona horaria como parte del registro de fecha y hora se ajustan a la hora UTC según el mapeo.

Para mapear una dirección IP a una zona horaria, realice lo siguiente:

1. Vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un Log Decoder en la vista **Servicios** y en la columna **Acciones**, seleccione **> Ver > Explorar**.
3. Vaya al nodo **/decoder/parsers**, haga clic con el botón secundario en **parsers** y seleccione **Propiedades**.
4. En la vista **Propiedades**, especifique el comando `iptmzone` con los siguientes parámetros:
   `op=add entries="ipaddress=timezone" (por ejemplo, op=add entries="10.10.10.10=Africa/Addis Ababa")`
5. Haga clic en **Enviar**.

Comando iptmzone

En el comando `iptmzone`, hay tres operaciones disponibles:

- `add`: esta operación agrega o actualiza las entradas en el mapa de iptmzone. Se pueden especificar varios pares de dirección/tipo delimitados por espacios.
  `op=add entries="<address>=<time zone>"`

- `remove`: esta operación quita las entradas en el mapa de iptmzone. Se pueden especificar varios pares de dirección/tipo delimitados por espacios.
  `op=remove entries="<address>"`
- `describe`: esta operación devuelve los valores que están actualmente en el mapa de iptmzone.

Ejemplos

Los siguientes ejemplos proporcionan instancias para mapear direcciones IP a zonas horarias:

- Si desea mapear dos entradas distintas con distintos valores IPV4 y zona horaria, ingrese el siguiente parámetro en el comando **iptmzone** y haga clic en **Enviar**
  "op=add entries=”10.10.10.10=America/Anguilla 10.10.10.11=Pacific/Rarotonga”
- Si desea quitar una entrada para un solo valor IPV4 y zona horaria, ingrese el siguiente parámetro en el comando **iptmzone** y haga clic en **Enviar**.
  "op=remove entries=10.5.245.9"
- Si desea crear una sola entrada para un valor IPV6 y zona horaria, ingrese el siguiente parámetro en el comando **iptmzone** y haga clic en **Enviar**.
  op=add entries=”2001:DB8:85A3::8A2E:370:7334=America/Anguilla”
- Si desea crear una sola entrada para mapear una dirección IPV4, IPV6 o un nombre de host con el formato de compensación de minutos, Olson o POSIX, ingrese el siguiente parámetro en el comando **iptmzone** y haga clic en **Enviar**.
  op=add entries="10.168.0.2=America/Anguilla 2001:DB8:85A3::8A2E:370:7334=0500nwappliance21=EST5EDT,M3.2.0/2,M11.1.0'

Obtener archivos de registro de Log Decoder anterior a 11.0

NetWitness 11.0 agregó la capacidad de ver una pequeña muestra de registros recientes para dispositivos específicos a través de las pestañas de detalles de la vista Descubrimiento. De forma predeterminada, antes de la versión 11.0 los Log Decoders no tienen la configuración necesaria para habilitar esta función, pero algunos cambios menores pueden hacer que esté disponible.

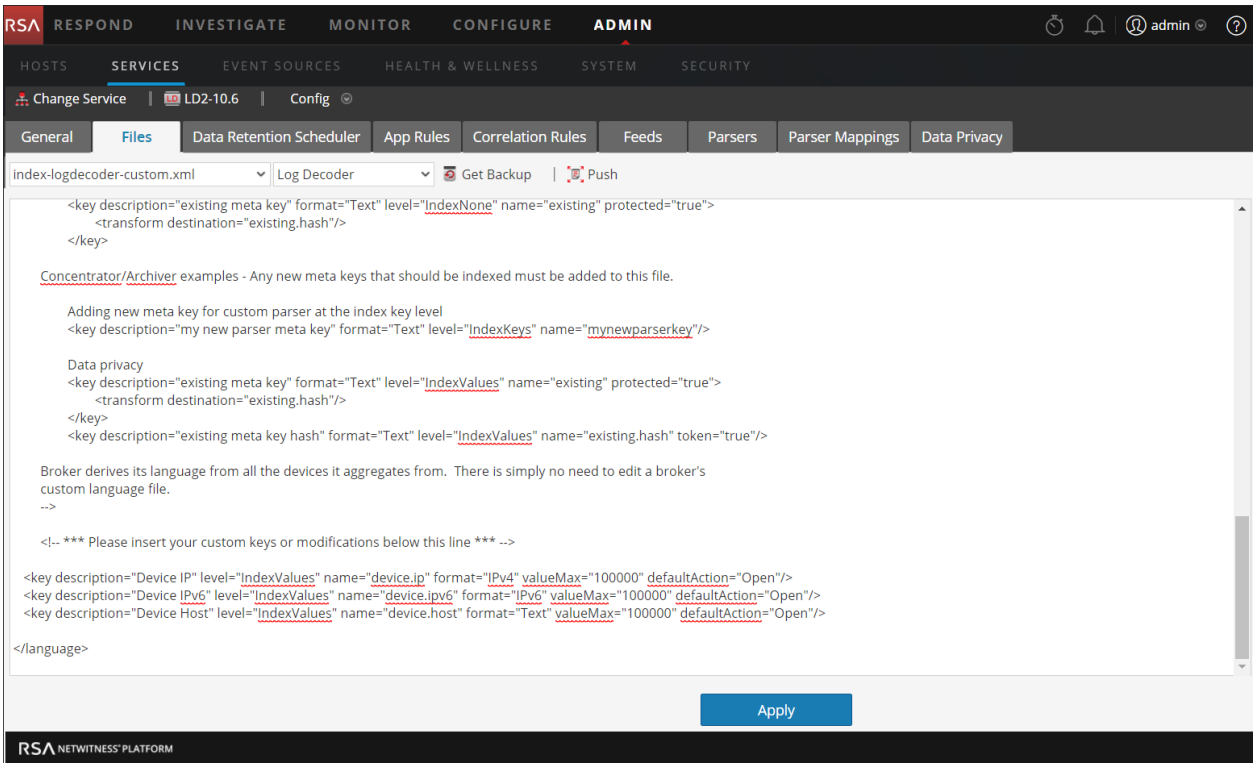
Para habilitar la vista previa de registros para un Log Decoder anterior a 11.0, siga estos pasos en el Log Decoder:

1. Vaya a **ADMINISTRAR > Servicios >** seleccione un **Log Decoder** y elija  **> Ver > Configuración**.
2. Haga clic en la pestaña **Archivos** y, en el menú desplegable, seleccione **index-logdecoder-custom.xml**.
3. Agregue las siguientes tres líneas al final del archivo (antes de la etiqueta de lenguaje de cierre):
   <key description="Device IP" level="IndexValues" name="device.ip" format="IPv4" valueMax="100000" defaultAction="Open"/>
   <key description="Device IPv6" level="IndexValues" name="device.ipv6" format="IPv6" valueMax="100000" defaultAction="Open"/>

```
<key description="Device Host" level="IndexValues" name="device.host" format="Text"
valueMax="100000" defaultAction="Open"/>
```

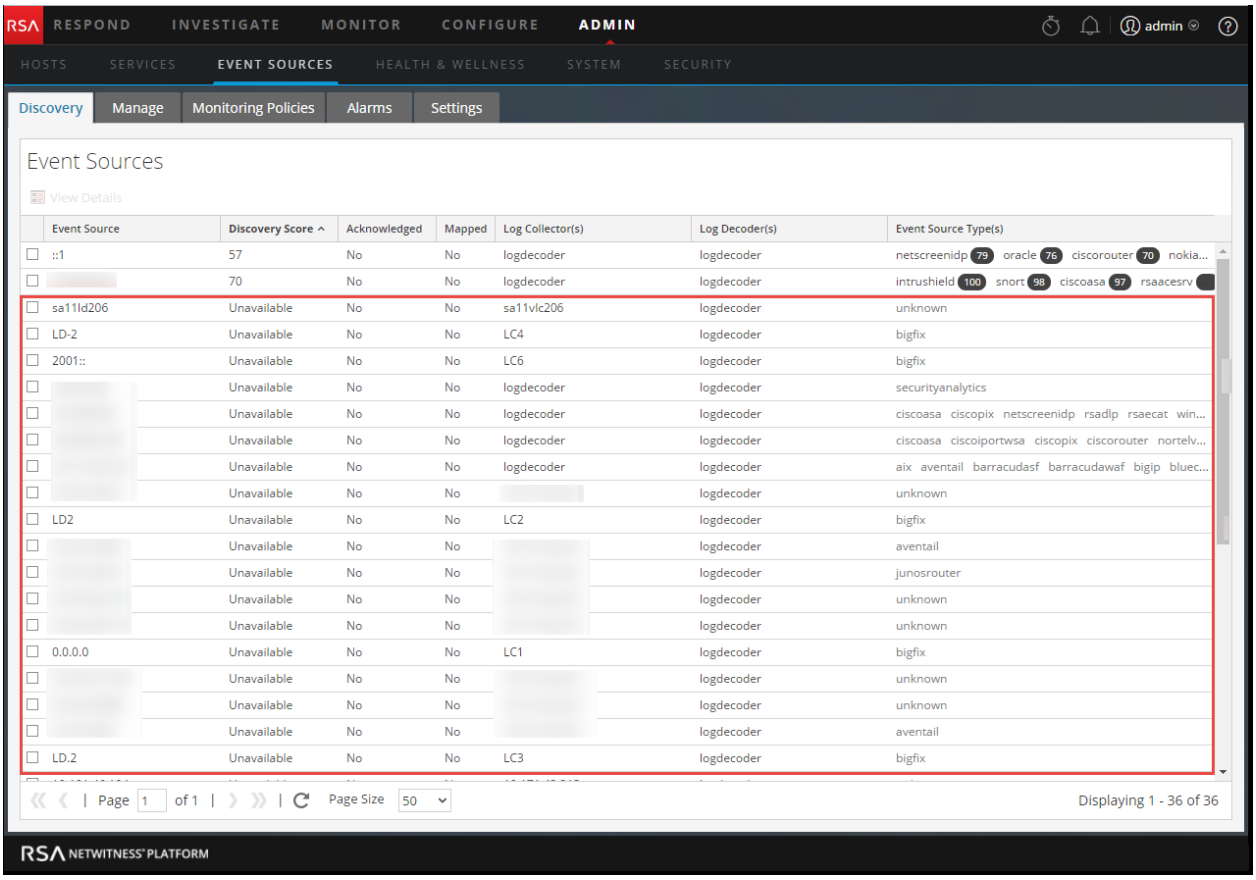
4. Haga clic en **Aplicar**.
5. Reinicie el servicio Log Decoder de la siguiente manera.
   Seleccione el servicio Log Decoder > **Explorar** > **Decoder** > **Propiedades** > **restablecer**.
   Seleccione **restablecer** en un menú desplegable. Haga clic en **Enviar** después de seleccionar restablecer.

Este es un ejemplo del archivo **index-logdecoder-custom.xml**.



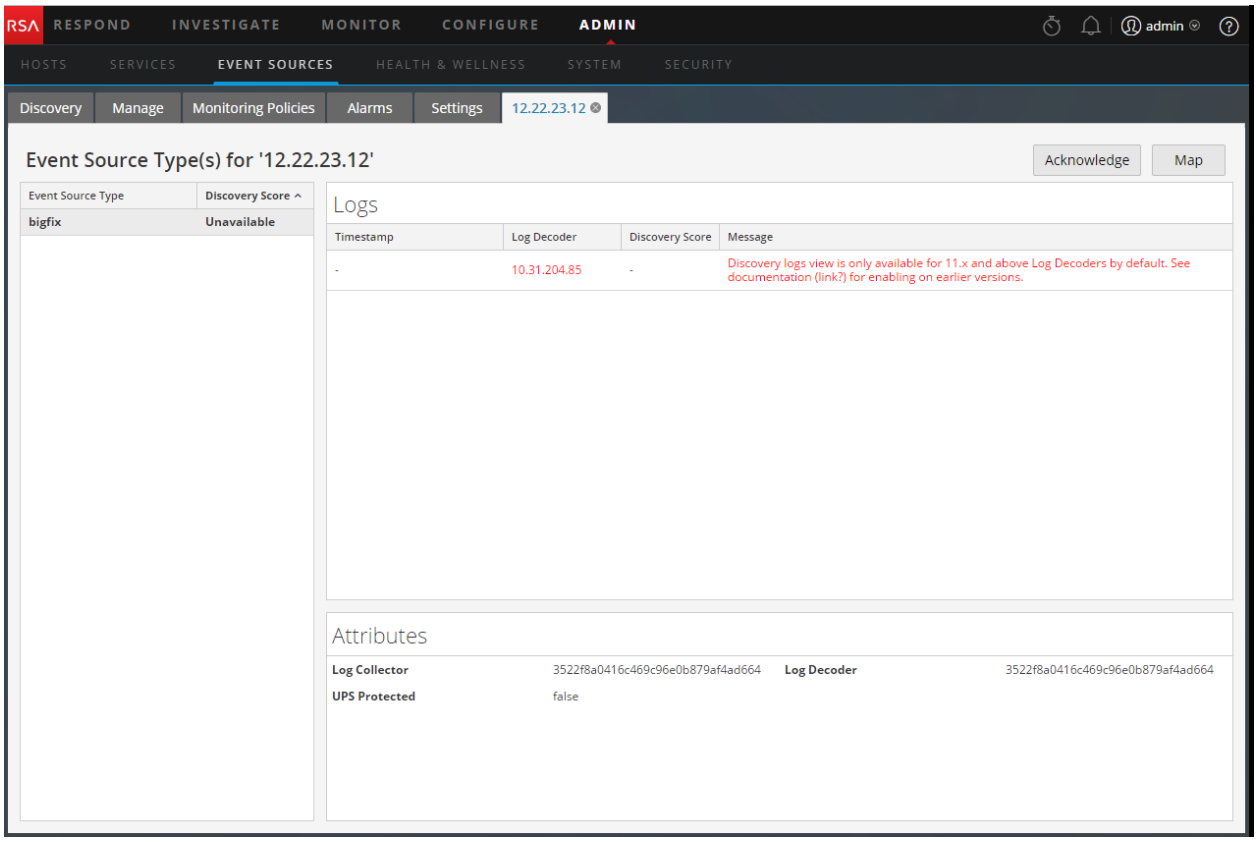
Nota: Los puntajes de descubrimiento solo están disponibles para Log Decoders 11.x y superior. Los puntajes de descubrimiento para los Log Decoders anteriores a 11.x se muestran como No disponible.

El siguiente ejemplo muestra el puntaje de descubrimiento como **No disponible** en la vista **Detalles** para un Log Decoder anterior a 11.0.



Nota: Los logs de los dispositivos solo están disponibles en los Log Decoders 11.x y superiores.

En el siguiente ejemplo se ve el mensaje que se muestra en el panel Registros para un Log Decoder anterior a 11.0.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Discovery
Manage
Monitoring Policies
Alarms
Settings
12.22.23.12
Event Source Type(s) for '12.22.23.12'
Acknowledge
Map
Event Source Type
Discovery Score
bigfix
Unavailable
Logs
Timestamp
Log Decoder
Discovery Score
Message
-
10.31.204.85
-
Discovery logs view is only available for 11.x and above Log Decoders by default. See documentation (link?) for enabling on earlier versions.
Attributes
Log Collector
3522f8a0416c469c96e0b879af4ad664
Log Decoder
3522f8a0416c469c96e0b879af4ad664
UPS Protected
false

Cargar un archivo de registro en un Log Decoder

En este tema, se describe el método para importar un archivo de registro a un Log Decoder.

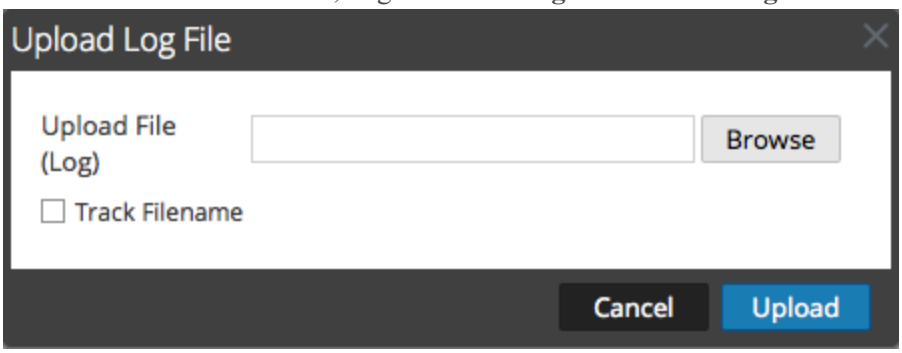
Existen ocasiones en las que desea analizar un archivo de registro que no está disponible en el servicio que está utilizando. Puede cargar en NetWitness Platform un archivo de registro capturado en otro servicio. Los nombres de archivos de registro son del tipo .log**.registro**.

Cuando se carga un archivo de registro en un Log Decoder, este analiza y genera metadatos para cada registro que contiene. Estos registros se agregan a los registros ya decodificados en el Log Decoder y están disponibles para análisis. NetWitness Platform incluye una opción de rastreo de nombre de archivo que facilita la búsqueda de un conjunto de registros específico. Cuando se carga el archivo de registro con un rastreo de archivos, el Log Decoder agrega metadatos a cada registro según el nombre de archivo cargado. Luego, puede filtrar las sesiones para análisis utilizando esos metadatos.

La opción para cargar un archivo de registro se atenúa cuando otras operaciones de Log Decoder impiden una carga, por ejemplo, cuando el Log Decoder está capturando registros.

Para importar un archivo de registro a un Log Decoder:

1. Vaya a **ADMINISTRAR > Servicios**.
2. Seleccione un Log Decoder en la cuadrícula **Servicio** y elija > **Ver** > **Sistema**.
   Se muestra la vista Sistema de servicios correspondiente al Log Decoder.
3. En la barra de herramientas, haga clic en **Cargar archivo de log**.



4. Para seleccionar un archivo de registro, haga clic en **Navegar**.
   Se muestra una vista del directorio.
5. Seleccione el archivo de registro que desea cargar.
   El nombre de archivo se muestra en el campo **Cargar archivo**.
6. Si desea que el Log Decoder agregue metadatos a los registros según el nombre de archivo, haga clic en la casilla de verificación junto a **Rastrear nombre de archivo**.
7. Para cargar el archivo, haga clic en **Cargar**.
   El archivo seleccionado se carga, lo cual se indica en un mensaje de estado. El archivo de registro está disponible para el análisis.

Cargar un archivo de captura de paquete

Existen ocasiones en las que desea analizar un archivo de captura de paquetes que no está disponible en el servicio que está utilizando. Puede cargar en NetWitness Platform un archivo capturado en otro servicio. Los tipos de archivos de captura de paquetes que se admiten son `pcap` y `pcap.gz`.

Cuando se carga un archivo de captura de paquetes a un Decoder, el Decoder crea sesiones a partir de los paquetes de archivo de captura de paquetes. Estas sesiones se agregan a las sesiones ya decodificadas en el Decoder y están disponibles para el análisis. NetWitness Platform incluye una opción de rastreo de nombre de archivo que facilita la búsqueda de un conjunto de sesiones específico. Cuando se carga el archivo de captura de paquetes con el rastreo de archivos, el Decoder agrega metadatos a las sesiones según el nombre de archivo cargado. Luego, puede filtrar las sesiones para análisis utilizando esos metadatos.

La opción para cargar un archivo de captura de paquetes se atenúa cuando otras operaciones de Decoder impiden una carga, por ejemplo, cuando el Decoder está capturando paquetes.

Para seleccionar y cargar un archivo de captura de paquetes:

1. Vaya a **ADMINISTRAR** > **Servicios**.

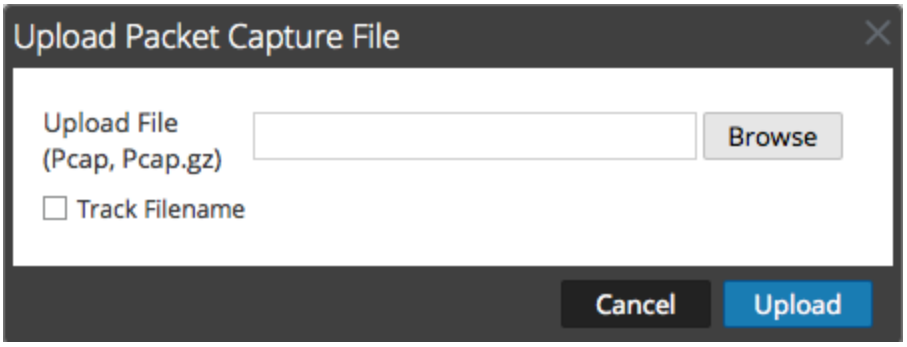
   Se muestra la vista Servicios de Administration.

2. Seleccione el nombre del Decoder y > **Ver** > **Sistema**.

   Se muestra la vista Sistema de servicios del Decoder.

3. En la barra de herramientas, haga clic en **Cargar archivo de captura de paquete**.

   Aparece el **cuadro de diálogo Cargar archivo de captura de paquete**.



4. Para seleccionar un archivo de captura, haga clic en **Seleccionar**.

   Se muestra una vista del directorio.

5. Vaya al directorio y seleccione el archivo de captura de paquetes que desea cargar.

   El nombre de archivo aparece en el campo **Cargar archivo (pcap,pcap.gz)**.

6. Si desea que el Decoder agregue metadatos a las sesiones según el nombre de archivo, haga clic en la casilla de verificación junto a **Rastrear nombre de archivo**.

7. Para cargar el archivo, haga clic en **Cargar**.

   Una barra de progreso muestra el progreso de carga.

El tiempo de carga varía según el tamaño del archivo. Cuando se completa la carga del archivo, aparece un mensaje de estado. El archivo ahora está disponible para investigación.

Referencias de feed y analizador

En este tema se proporciona más detalles sobre los feeds y los analizadores que usa Decoder.

- Archivo de definiciones de feed
- Analizadores flexibles
- Analizadores GeoIP2 y GeoIP
- Analizadores Lua
- Analizadores Snort
- Analizador de búsqueda
- Configuración de LAN inalámbrica

Archivo de definiciones de feed

En este tema se presenta el archivo de definiciones de feed, el cual está disponible para editar en la vista Configuración de servicios > pestaña Archivos.

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es el archivo de definiciones de feed, **`feed-definitions.xml`**.

feed-definitions.xml

Puede definir feeds en el archivo `feed-definitions.xml`. El Decoder utiliza un esquema XML para definir mensajes de feed cuando crea un archivo .feed binario a partir de los feeds definidos aquí.

Para obtener detalles sobre el lenguaje de definición de feed, consulte el tema “Administrar feeds personalizados” en la *Guía de administración de servicios de Live*.

Analizadores flexibles

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es `NwFlex.xml`, el analizador flexible.

NwFlex.xml

Existen dos tipos de analizadores flexibles:

- **Identificación de servicio basada únicamente en el puerto.** Estos son analizadores que utilizan solo los puertos de origen o de destino para identificar el tipo de aplicación de sesión (servicio). Estos son los analizadores más básicos y fáciles de definir.
- **Identificación de servicio basada en uno o más tokens encontrados.** Estos analizadores utilizan tokens para identificar el tipo de servicio. Esta también es una manera sencilla de ampliar los tipos de servicios que se identifican. Estos son importantes al identificar aplicaciones estándar sin Internet. Estos analizadores requieren que el protocolo tenga un token definible que pueda identificar de forma única al tipo de servicio.

Las siguientes son cinco operaciones comunes del analizador:

- Hacer coincidir puerto e identificar inmediatamente
- Hacer coincidir puerto y demorar la identificación
- Hacer coincidir token e identificar inmediatamente
- Hacer coincidir varios tokens
- Hacer coincidir token y crear metadatos

En este tema se proporciona información detallada y ejemplos del lenguaje. En este tema se describe el esquema XML que se usa para definir un archivo FlexParse. El nodo SML, el atributo y los valores a los cuales se hace referencia en el texto descriptivo están en **negrita**. El nodo raíz de cada archivo debe ser el nodo **parsers**. Debajo de ese nodo, puede haber una cantidad indefinida de nodos parser. Cada nodo parser define un único analizador. Un nodo parser puede tener un nodo **declaration** opcional y una cantidad indefinida de nodos **match**.

Temas

- Regex
- Funciones de cadena

Funciones aritméticas

En este tema se define el lenguaje de las funciones aritméticas del analizador flexible.

En este tema se define el lenguaje de las funciones aritméticas del analizador flexible. Todos los números son valores sin signo de 64 bits y, según la operación, están sujetos a subdesbordamiento y desbordamiento.

Definición del idioma

En la siguiente tabla se proporcionan definiciones del lenguaje.

Nombre de nodo	Nombre de atributo	Descripción
`and`		Ejecuta una operación AND bit a bit entre dos números.
	`name`	Variable a la cual se aplica el resultado de AND.
	`value`	Número para aplicar AND al resultado.
`or`		Ejecuta una operación OR bit a bit entre dos números.
	`name`	Variable a la cual se aplica el resultado de OR.
	`value`	Número para aplicar OR al resultado.
`increment`		Ejecuta la operación ADDITION de dos números.
	`name`	Variable que contiene el valor inicial AND para recibir los resultados de ADDITION.
	`value`	Número que se suma (ADD) al valor inicial.
`decrement`		Ejecuta la operación SUBTRACTION de dos números.
	`name`	Variable que contiene el valor inicial AND para recibir los resultados de SUBTRACTION.
	`value`	Número que se resta (SUBTRACT) del valor inicial.
`divide`		Ejecuta la operación DIVISION de dos números.
	`name`	Variable que contiene el valor inicial AND para recibir los resultados de DIVISION.
	`value`	Cantidad por la cual se divide el valor inicial. La división por cero genera un error y detiene el procesamiento de la sesión actual por parte de este analizador.
`modulo`		Ejecuta la operación MODULO de dos números.

Nombre de nodo	Nombre de atributo	Descripción
	name	Variable que contiene el valor inicial AND para recibir los resultados de MODULO.
	value	Cantidad por la cual se divide el valor inicial. La división por cero genera un error y detiene el procesamiento de la sesión actual por parte de este analizador.
multiply		Ejecuta la operación MULTIPLICATION de dos números.
	name	Variable que contiene el valor inicial AND para recibir los resultados de MULTIPLICATION.
	value	Cantidad por la cual se multiplica (MULTIPLY) el valor inicial.
shiftleft		Ejecuta un desplazamiento aritmético a la izquierda binario.
	name	Variable que contiene el valor inicial AND para recibir los resultados del desplazamiento.
	value	Cantidad de bits por los cuales se realiza el desplazamiento.
shiftright		Ejecuta un desplazamiento aritmético a la derecha binario.
	name	Variable que contiene el valor inicial AND para recibir los resultados del desplazamiento.
	value	Cantidad de bits por los cuales se realiza el desplazamiento.

Operaciones comunes de analizadores

En este tema se proporcionan algunos ejemplos de operaciones comunes del analizador.

En este tema se incluyen cinco operaciones comunes del analizador.

Hacer coincidir puerto e identificar inmediatamente

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
          <parser name="CustApp" desc="Acme Custom App" service="45324">
               <declaration>
                    <port name="port" value="45324" />
               <declaration>
               </match name="port">
                    <identify />
               </match>
          </parser>
</parsers>
```

Hacer coincidir puerto y demorar la identificación

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MSRPC" desc="Microsoft RPC protocol" service=135">
          <declaration>
               <port name="port" value="135" />
               <number name="state" scope="session" />
               <session name="end" value="end" />
          </declaration>
          <match name="port">
               <assign name="state" value="1" />
          </match>
          <match name="end">
               <if name="state" equal="1" />
                    <identify />
               </if>
          </match>
     </parser>
</parsers>
```

Hacer coincidir token e identificar inmediatamente

```
<?xml version="1.0" encoding="utf-8?>
<parsers
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="RDP" desc="Remote Desktop Protocol" service="3389">
          <declaration>
               <token name="signature" value="Cookie: mstshash=" />
          </declaration>
          <match name="signature">
               <identify />
          </match>
     </parser>
</parsers>
```

Hacer coincidir varios tokens

```
<?xml version="1.0" encoding="utf-8"?>
<parsers
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="MyServiceMultiToken" desc="Multiple Tokens" service="333">
          <declaration>
               <number name="state" scope="stream" />
               <token name="user" value="USER " />
               <token name="pass" value="PASS " />
               <session name="session" value="end" />
          </declaration>
          <match name="user">
               <or name="state" value="1" />
          </match>
          <match name="pass">
               <or name="state" value="2" />
          </match>
          <match name="session">
               <if name="state" equal="3">
                    <identify />
               </if>
          </match>
     </parser>
</parsers>
```

Hacer coincidir token y crear metadatos

```
<?xml version="1.0" encoding="utf-8"?>
<parsers xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="parsers.xsd">
     <parser name="SHELL" desc="Command Shell Identification">
          <declaration>
               <token name="cmd.exe" value=" (C) Copyright 1985-2001 Microsoft
               Corp" options="linestart" />
               <meta name="client" key="client" format="Text" />
          </declaration>
          <match name="cmd.exe"
               <register  name="client" value="MS Command Shell" />
          </match>
     </parser>
</parsers>
```

Funciones generales

En este tema se define el lenguaje de las funciones generales del analizador flexible.

Definición de lenguaje de funciones generales

Nombre de nodo	Nombre de atributo	Descripción
apptype		Obtiene el tipo de servicio actualmente definido para la sesión actual.
	name	Una variable numérica para recibir el tipo de servicio actual.
identify		Marca la sesión con el tipo de servicio del analizador si no se ha identificado el tipo de servicio.
assign		Asigna un valor a una variable.
	name	El identificador único asignado al elemento en la sección de declaración.
	value	Opcional. Si se especifica, la acción definida en la coincidencia solo se aplica cuando la declaración coincide con el valor especificado.
getmeta		Recupera el valor de metadatos que generó una devolución de llamadas. Esta función devolverá resultados vacíos (0, cadena de longitud cero) si se llama cuando no hay una devolución de llamadas de metadatos.
	name	La variable para recibir el valor de la clave de metadatos que generó la devolución de llamadas.
gettoken		Devuelve el token con el cual hubo coincidencia actualmente.
	name	Una variable de cadena para recibir el token con el cual hubo coincidencia actualmente. Si no hay ningún token actual, se asigna a la variable una cadena vacía.
end		Esto termina la ejecución de la sección **match** actual.
if		Compara dos valores. Si la comparación es verdadera, se ejecutan subacciones. Las comparaciones pueden ser tipos de **número** o **cadena**, siempre que ambos valores sean del mismo tipo.
	name	El identificador de variable único asignado al elemento en la sección **declaration**.

Nombre de nodo	Nombre de atributo	Descripción
	equal notequal less lessequal greater greaterequal and or	El valor de la operación que se comparará. Si es verdadero, se ejecutan subacciones.
register		Agrega metadatos a la sesión.
	name	El identificador único de una variable de metadatos que se creará, según se define en la sección **declaration**.
	value	El valor de los metadatos que se crearán.
while		Compara dos valores y ejecuta subacciones si la comparación es verdadera. Las comparaciones pueden ser tipos de **número** o **cadena**, siempre que ambos valores sean del mismo tipo.
	name	El identificador de variable único asignado al elemento en la sección de declaración.
	equal notequal less lessequal greater greaterequal and or	Especifica el valor de la operación que se comparará. Si es verdadero, se ejecutan subacciones. Los atributos **and** y **or** representan operaciones bit a bit y solo se pueden aplicar a variables de **número**.
call		Ejecuta el elemento **match** especificado. Puede ser cualquier elemento de coincidencia definido en el mismo analizador flexible, independientemente de la forma en que se declaró.
	value	El nombre del elemento de coincidencia o una variable de cadena que contiene el nombre de un elemento de coincidencia. • Si se especifica el nombre del elemento de coincidencia, el analizador no se cargará si el elemento con coincidencia nombrado no existe. • Si se especifica una variable de cadena, el elemento **call** ejecutará cualquier elemento secundario que pueda tener si el valor de cadena se resuelve en un elemento de coincidencia después de la ejecución del elemento de coincidencia nombrado. • Si no se puede encontrar ningún elemento **match** que coincida con el valor de cadena, no se realiza ninguna acción.

Funciones de registro

En este tema se define el lenguaje de las funciones de registro del analizador flexible.

Las funciones de registro proporcionan un medio para que un analizador flexible escriba en el registro del sistema. Las funciones de registro pueden ser extremadamente útiles cuando se crea un nuevo analizador flexible, pero deben mantenerse en un mínimo absoluto cuando un analizador flexible se implementa en un sistema de producción.

Definición del idioma

Nombre de nodo	Nombre de atributo	Descripción
failure		Registra un mensaje en el registro del sistema con el nivel de registro **Falla.**
	value	Una cadena que se incluirá como el mensaje del registro.
warning		Registra un mensaje en el registro del sistema con el nivel de registro **Advertencia.**
	value	Una cadena que se incluirá como el mensaje del registro.
info		Registra un mensaje en el registro del sistema con el nivel de registro **Información**.
	value	Una cadena que se incluirá como el mensaje del registro.
debug		Registra un mensaje en el registro del sistema con el nivel de registro **Depuración.**
	value	Una cadena que se incluirá como el mensaje del registro.

Nodos

En este tema se define el lenguaje de los nodos del analizador flexible.

Definición del lenguaje de los nodos

Nombre de nodo	Nombre de atributo	Descripción
`parsers`		El nodo de raíz en cada archivo de definición.
	`xmins:xsi`	Define el espacio de nombres que se usará para la inclusión del esquema. Este atributo no es obligatorio; sin embargo, la definición del lenguaje no es posible sin él. Este nodo debe tener el siguiente valor: http://www.w3.org/2001/XMLSchema-instance
	`xsi:noNamespaceSchemaLocation`	Define el archivo de validación del esquema XSD que se usa para validar la definición del lenguaje. Este atributo no es obligatorio; sin embargo, la definición del lenguaje no es posible sin él. Este nodo debe tener el siguiente valor: parsers.xsd
`parser`		El nodo que establece una única definición del analizador. Este nodo debe estar directamente bajo el nodo `parsers`. Puede haber más de uno por archivo.
	`name`	El nombre que identifica de manera única al analizador. Este nombre debe ser corto y conciso. Lo usa el sistema para permitir la activación y la desactivación. Solo debe contener las letras [a-z] y [A-Z].
	`desc`	Proporciona una descripción simple de lo que hace el analizador.
	`service`	El número único asignado a la sesión cuando se identifica.
`declaration`		Describe la definición. Cada una de estas definiciones puede tener una entrada `match` asociada.

Nombre de nodo	Nombre de atributo	Descripción
token		Especifica una definición para identificar un token en alguna parte del protocolo de sesión. Esto define una devolución de llamadas `match` cuando los tokens especificados se encuentran en la carga útil de una sesión. La posición de `read` se configura en el byte que está inmediatamente después del token con coincidencia.
	name	Este es un identificador único para la declaración.
	value	Este es el valor exacto del token que se identificará.
	options	Las opciones especifican que el token debe comenzar en una nueva línea o al final de una línea (`linestart` o `linestop`).
meta-callback		Registra una devolución de llamadas para el analizador flexible cada vez que se crean metadatos de un formato específico. Esto se puede calificar adicionalmente para generar devoluciones de llamadas solamente para sesiones que se han identificado como un apptype específico (por ejemplo, 80 para HTTP).
	name	Nombre del elemento de coincidencia que se ejecutará cuando ocurre una devolución de llamadas. (Cadena)
	key	Nombre de la clave de metadatos que genera devoluciones de llamadas. (Cadena)
	format	El tipo de datos de la clave de metadatos que generará los metadatos.
	apptype	La devolución de llamadas de metadatos se genera solo si la sesión que se analiza se identificó con el apptype especificado. (Entero sin signo, opcional)
number		Define una variable numérica a la cual se puede hacer referencia en otra ubicación dentro de la definición del analizador. Todos los valores numéricos son valores sin signo de 64 bits.

Nombre de nodo	Nombre de atributo	Descripción
	`name`	Este es un identificador único para la declaración.
	`scope` (opcional)	Especifica cuándo se restablece la variable. Esto puede ser para cada lado de una sesión de dos lados o solo después que se detecta una nueva sesión. Los posibles valores son **`global`**, **`constant`**, **`stream`** y `session` (valor predeterminado).
`string`		Define una variable numérica a la cual se puede hacer referencia en otra ubicación dentro de la definición del analizador.
	`name`	Este es un identificador único para la declaración.
	`scope` (opcional)	Especifica cuándo se restablece la variable. Esto puede ser para cada lado de una sesión de dos lados o solo después que se detecta una nueva sesión. Los posibles valores son **`global`**, **`constant`**, **`stream`** y `session` (valor predeterminado).
port		Define una devolución de llamadas **match** cuando se encuentra una sesión mediante el uso del puerto especificado. La posición de **lectura** se configura en el primer byte del primer flujo (cliente) en la sesión.
	`name`	Este es un identificador único para la declaración.
	`value`	Este es el número de puerto que se identificará.
`session`		Define una devolución de llamadas `match` para los eventos iniciales/finales de la sesión. Estos eventos ocurren solo si se encuentra un token para el analizador en la sesión.
	`name`	Este es un identificador único para la declaración.
	`value`	Especifica que el procesamiento se realiza al comienzo de una nueva sesión o al final de una sesión (`begin` o `end`).

Nombre de nodo	Nombre de atributo	Descripción
stream		Define una devolución de llamadas match para los eventos iniciales/finales del flujo. Estos eventos ocurren solo si se encuentra un token para el analizador en el flujo.
	name	Este es un identificador único para la declaración
	value	Especifica que el procesamiento se realiza al comienzo o al final de un flujo (begin o end).
function		Define una sección match que se puede usar como función genérica. No hay devoluciones de llamadas asociadas a esta declaración.
	name	Este es un identificador único para la declaración.
meta		Define el tipo de datos que creará el analizador.
	key	Especifica el nombre de la clave. La clave debe tener un tamaño de entre 1 y 16 bytes.
	format	Especifica el tipo de variante (por ejemplo, **Text**, **IPv4**, **UInt32**). Consulte la lista completa en la documentación de SDK.
pattern		Define una variable de expresión regular que usará la función regex
	name	Este es un identificador único para la declaración.
	scope (opcional)	Especifica cuándo se restablece la variable. Esto puede ser para cada lado de una sesión de dos lados o solo después que se detecta una nueva sesión. Los posibles valores son **global**, **constant**, **stream** y session (valor predeterminado).
	value (opcional)	Especifica una expresión regular que se asignará a la variable pattern. Este atributo solo es válido cuando el **scope attribute** se configura en constant.

Nombre de nodo	Nombre de atributo	Descripción
match		Las posibles entradas para realizar una acción cuando se encuentra un criterio de coincidencia para una declaración. Estos nodos se pueden anidar para proporcionar una lógica más profunda. Hay varias categorías de elementos de ejecución (funciones) que pueden aparecer como secundarias de un elemento de coincidencia: • General • Aritmética • Cadena • Carga útil

Funciones de carga útil

En este tema se define el lenguaje de las funciones de carga útil del analizador flexible.

Estas funciones operan en una posición de `read`, que se configura al principio de un elemento `match` .

Definición del idioma

Nombre de nodo	Nombre de atributo	Descripción
`find`		Busca la carga útil de flujo comenzando en la posición de lectura para un valor de cadena dado. Si se encuentra el valor, se devuelve la compensación de la posición de lectura. Los elementos secundarios se ejecutan. Si no se encuentra, los elementos secundarios no se ejecutan.
	`name`	Una variable `number` para recibir la compensación desde la posición`read` donde comienza la coincidencia.
	`value`	Cadena que se buscará.
	`length` (opcional)	Límite a la longitud de la carga útil que se buscará. Si no se proporciona un límite, se busca en el resto de la carga útil. Se recomienda usar siempre el menor valor posible para reducir el efecto en el rendimiento.
`install-decoder`		Para habilitar tokens que coincidan con datos de carga útil que pueden estar fragmentados o codificados. Se puede instalar un decodificador de escaneo para procesar previamente una sección de la carga útil antes de que se escanee en busca de tokens. Un ejemplo sería una respuesta de HTTP que usa la codificación de transferencia segmentada con codificación de contenido gzip. Si se analiza el encabezado de HTTP, se pueden establecer los parámetros de tipo necesario, compensación y longitud, después de lo cual, la carga útil de respuesta de HTTP aparecería para el escaneo de tokens como si no se hubiera aplicado ninguna codificación. Sin embargo, esto incurre en una sobrecarga significativa.
	`type`	El tipo de decodificador que desea instalar. Las opciones válidas son: gzip, deflate, chunked, chunked-gzip, chunked-deflate.
	`offset`	Compensación de la posición de lectura actual para iniciar la decodificación.
	`length`	La longitud de carga útil máxima para la decodificación.
`isdecoding`		Prueba si un decodificador instalado está activo actualmente. De ser así, se ejecutará cualquier elemento secundario de esta función. Esta función no tiene parámetros.

Nombre de nodo	Nombre de atributo	Descripción
move		Mueve la posición de read hacia delante en el flujo actual mediante la especificación de un número de bytes. Si hay suficientes datos en el flujo, se actualiza la posición de read y se ejecuta cualquier elemento secundario. Si no se encuentra, la posición de read permanece sin cambios y los elementos secundarios no se ejecutan.
	value	La cantidad de bytes para mover la posición read.
	direction (opcional)	La dirección para mover la posición de lectura actual. Puede ser forward (predeterminado) o **reverse.**
packetid		Devuelve el ID del paquete para la posición de lectura actual. Es posible que el resultado sea 0, lo que indica que no se pudo determinar el ID del paquete.
	name	Una variable numérica para recibir el ID del paquete actual.
payload-position		Devuelve la posición de lectura actual. Se trata de un índice basado en cero en la carga útil de flujo.
	name	Una variable numérica para recibir la posición de lectura actual.
read		Lee una cantidad especificada de bytes comenzando en la posición de read en una variable. Si hay suficientes datos en el flujo, se actualiza la posición de read, se asigna la lectura de datos y se ejecuta cualquier elemento secundario. Si no se encuentra, la posición de read permanece sin cambios y los elementos secundarios no se ejecutan.
	name	El nombre de una variable string o number para recibir datos de flujo. Si se proporciona una variable number, la lectura de bytes se interpreta como un valor numérico único sin signo.
	length	La cantidad de bytes que se debe leer desde un flujo.
	endianess (opcional)	El orden de bytes que se usará al leer en una variable numérica. Puede ser big (valor predeterminado) o little. El atributo no es válido cuando se lee en una variable string.

Regex

En este tema se define el lenguaje del nodo de Regex del analizador flexible.

Regex busca coincidencias con una determinada expresión regular en la carga útil del flujo a partir de la posición `read`. Si encuentra coincidencias, se devuelve la compensación desde la posición `read` y, opcionalmente, la cadena que coincide. Los elementos secundarios se ejecutan. Si no encuentra coincidencias, los elementos secundarios no se ejecutan.

Definición del idioma

Nombre de atributo	Descripción
`name`	Una variable `number` para recibir la compensación desde la posición`read` donde comienza la coincidencia.
`value`	Una expresión regular que se desea buscar.
`length` (opcional)	Límite a la longitud de la carga útil que se buscará. Si no se proporciona un límite, se busca en el resto de la carga útil. Se recomienda usar siempre el menor valor posible para reducir el efecto en el rendimiento.
`found` (opcional)	El nombre de una variable de `string` que recibirá una cadena coincidente.

Funciones de cadena

En este tema se proporcionan definiciones de lenguaje de las funciones de cadena del analizador flexible.

Definición de lenguaje de funciones de cadena

Nombre de nodo	Nombre de atributo	Descripción
`append`		Conecta un número o una cadena en el extremo de una variable de `string`.
	`name`	El identificador exclusivo de una variable de cadena al cual se conecta el valor especificado.
	`value`	Un número o una cadena para conectar.
`find`		Busca una cadena para un valor de cadena proporcionado. Si se encuentra, la posición se devuelve y se ejecuta cualquier elemento secundario. De lo contrario, los elementos secundarios no se ejecutan.
	`name`	Una variable de `number` para recibir la posición de base cero, donde la cadena de valor proporcionada se encontró en la cadena **in**.
	`value`	Cadena que se buscará.
	`in`	Una cadena para buscar.
	`length` (opcional)	Límite a la longitud de la cadena **in** que se buscará. Si no se proporciona un límite, se buscarán todos los **in**.
`length`		Asigna la longitud de una cadena a una variable de `number`.
	`name`	Una variable de `number` para recibir la longitud de la cadena especificada.
	`value`	Un valor de cadena cuya longitud se debe determinar.
`regex`		Busca en una cadena de coincidencias para la expresión regular proporcionada. Si se encuentra una coincidencia, opcionalmente, se devuelve la posición y la cadena coincidente. Los elementos secundarios se ejecutan. Si no se encuentra, los elementos secundarios no se ejecutan. Las operaciones con expresiones regulares pueden afectar negativamente el rendimiento del sistema.

Nombre de nodo	Nombre de atributo	Descripción
	name	Una variable de número para recibir la posición de base cero, donde la expresión regular proporcionada coincide en la cadena in.
	value	Una expresión regular para buscar.
	in	Una cadena para buscar.
	length (opcional)	Límite a la longitud de la cadena in que se buscará. Si no se proporciona un límite, se buscarán todos los **in**.
	found (opcional)	El nombre de una variable de cadena que recibirá la cadena coincidente.
substring		Se debe especificar al menos uno de los atributos opcionales from y length.
	name	El identificador exclusivo de una variable de cadena para recibir el valor extraído.
	value	Un valor de cadena desde el cual extraer una subcadena.
	from (opcional)	La posición basada en cero desde la cual comenzar la subcadena. Si no se especifica, el valor predeterminado es cero.
	length (opcional)	La cantidad de caracteres que desea extraer. Si no se especifica, se configura de forma predeterminada en la longitud restante de la cadena.
tolower		Convierte una cadena en letras minúsculas.
	name	El nombre de una variable string para procesar.
toupper		Convierte una cadena en letras mayúsculas.
	name	El nombre de una variable string para procesar.
urldecode		Decodifica una cadena que contiene caracteres con codificación URL.
	name	Una variable de cadena para recibir la cadena decodificada.
	value	Una cadena codificada como URL para decodificar.
base64decode		Decodifica una cadena codificada con base 64.
	name	Una variable de cadena para recibir la cadena decodificada.
	value	Una cadena codificada como URL para decodificar.

Nombre de nodo	Nombre de atributo	Descripción
uudecode		Decodifica una cadena uuencoded.
	name	Una variable de cadena para recibir la cadena decodificada.
	value	Una cadena uuencoded. No se deben incluir las líneas de encabezado y cola.
quotedprintabledecode		Decodifica una cadena codificada imprimible citada.
	name	Una variable de cadena para recibir la cadena decodificada.
	value	Una cadena codificada imprimible citada.
convert-ebcdic		Convierte una cadena EBCDIC en su equivalente ASCII.
	name	Una variable de cadena para recibir la cadena decodificada.
	value	Una cadena codificada como URL para decodificar.

Analizadores GeoIP2 y GeoIP

En este tema se describen los analizadores GeoIP2 y GeoIP para Decoders. Solamente uno de estos analizadores se puede habilitar a la vez. Ambos analizadores convierten las direcciones IP en ubicaciones geográficas, como el nombre del país y la ciudad donde normalmente se encuentra la dirección IP.

Analizador GeoIP2

El analizador GeoIP2, disponible en NetWitness Platform versión 11.2 o superior, está habilitado de manera predeterminada para las actualizaciones y las instalaciones nuevas. El analizador GeoIP2 proporciona el paquete MaxMind GeoIP más reciente y es compatible tanto con direcciones IPv6 como IPv4.

La configuración del analizador GeoIP2 se puede editar realizando lo siguiente:

1. Vaya a **ADMINISTRAR** > **Servicios**.
2. En la vista **Servicios de Administration**, seleccione un Log Decoder o un Decoder.
3. Haga clic en el icono de configuración () y seleccione **Ver** > **Configuración**. Se muestra el panel Configuración de analizadores, desde el que puede seleccionar **GeoIP2** para ver y actualizar las opciones de configuración.

Puede definir qué direcciones IP desea buscar. El analizador GeoIP2 habilita las siguientes direcciones IP de manera predeterminada: `ip.src`, `ip.dst`, `ipv6.src` y `ipv6.dst`. Sin embargo, puede actualizar las opciones utilizando `parsers.options` para quitar o agregar nuevas direcciones IP. Por ejemplo, puede editar `parsers.options` y pasar una lista separada por comas de direcciones IP para usarlas de la siguiente manera:
`GeoIP2="ipaddr=ip.src,ip.dst,ipv6.src,ipv6.dst,ip.addr"`
Esto agregará una nueva dirección IP a la búsqueda denominada `ip.addr`. Sin embargo, dado que `ip.addr` no termina en `.src` o `.dst`, el analizador optará por colocar los metadatos de GeoIP2 generados en metadatos sin un sufijo `.src` o `.dst`. Entonces, se verán el país, la ciudad, etc. después de los metadatos `ip.addr`.

Nota: La lista que se pasa para `ip.addr` reemplaza a la lista predeterminada. Por lo tanto, si pasa `ipaddr=ip.src`, generará solamente metadatos de GeoIP2 para `ip.src` y ninguna otra dirección IP.

Nota: `parsers.options` se utiliza para pasar opciones a múltiples analizadores. De este modo, si le agrega GeoIP2, no debe eliminar ninguna otra opción que se pase a otros analizadores (como el analizador de entropía).

En la siguiente tabla se proporciona la lista completa de metadatos que puede generar el analizador GeoIP2 y se indican aquellos que están o no habilitados de manera predeterminada:

Habilitados de manera predeterminada	No habilitados
country, country.src, country.dst	latdec, latdec.src, latdec.dst
	longdec, longdec.src, longdec.dst
domain, domain.src, domain.dst	isp, isp.src, isp,dst
org, org.src, org.dst	city, city.src, city.dst

Puede habilitar los demás metadatos mediante las configuraciones estándares de los analizadores.

Nota: Cuando deshabilita algunos metadatos de manera predeterminada, el analizador GeoIP2 no funciona igual que el analizador GeoIP (el cual, de manera predeterminada, no deshabilitaba ninguno de los metadatos que generaba). Si llega a necesitar cualquiera de los metadatos deshabilitados, tendrá que habilitarlos (solamente una vez) para cada Decoder después de la actualización a 11.2 o superior. Tenga en cuenta que los campos de metadatos `isp` y `org` suelen producir un valor equivalente a `domain`.

Analizador GeoIP

El analizador GeoIP es un analizador más antiguo disponible en versiones anteriores de NetWitness Platform, pero aún es compatible además del analizador GeoIP2 más reciente. Para modificar la configuración del analizador, los usuarios pueden editar sus opciones desde aquí: Vista Configuración de servicios > Archivos > `GeoPrivate.ipl`.

Los metadatos de geoubicación en `GeoPrivate.ipl`, se agregan para `ip.src` y `ip.dst`. El analizador usa dos archivos de datos externos, `GeoCity.dat` y `GeoCountry.dat`, los cuales se almacenan en el directorio de aplicaciones. Existen hasta ocho metadatos para cada dirección IP como se indica en la tabla siguiente.

Metadatos	Descripción
city.dst	Ciudad de destino
city.src	Ciudad de origen
country.dst	País de destino
country.src	País de origen
latdec.dst	Latitud decimal de destino
latdec.src	Latitud decimal de origen
longdec.dst	Longitud decimal de destino
longdec.src	Longitud decimal de origen

Analizadores Lua

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es **`NwLua.xml`**, el analizador Lua.

Lista de analizadores Lua

Existen varios analizadores Lua disponibles en Live. Consulte Contenido de RSA para:

- Obtener una lista completa de estos analizadores
- Conocer sus interdependencias
- Conocer los analizadores flexibles que contiene cada analizador Lua.

Las siguientes son cinco operaciones comunes del analizador:

- Hacer coincidir puerto e identificar inmediatamente
- Hacer coincidir puerto y demorar la identificación
- Hacer coincidir token e identificar inmediatamente
- Hacer coincidir varios tokens
- Hacer coincidir token y crear metadatos

Analizadores Snort

Las reglas y la configuración de Snort® se agregan al directorio `parsers/snort` para Investigation y Decoder. Decoder es compatible con las funcionalidades de detección de carga útil de las reglas de Snort. Los archivos de reglas deben tener la extensión `.rules` y los archivos de configuración, la extensión `.conf`. La implementación de Decoder de reglas de Snort se centra en el uso de las cadenas de contenido definidas en una regla de Snort como un token. Cuando hay coincidencia con un token, se pueden evaluar el encabezado y las opciones adicionales de la regla. Actualmente, las reglas que no definen ningún contenido (a través de opciones de regla de `content` o `uricontent`) no son compatibles.

Configuración

Los archivos de configuración se cargan antes de que se carguen las reglas.

Opciones de configuración	Descripción
Definiciones de variables	**Descripción**
`ipvar`	Es compatible el lenguaje completo para definir variables de direcciones IP, lo que incluye listas, CIDR y negación.
`portvar`	Es compatible el lenguaje completo para definir variables de direcciones IP, lo que incluye listas, rangos y negación.
`var`	No es compatible; use `ipvar` o `portvar`.
Definiciones de acciones	**Descripción**
`ruletype`	Es compatible la definición de `ruletypes` adicionales. Sin embargo, solamente son compatibles las reglas que tienen un tipo de regla base de `alert`.
Configuración general	**Descripción**
`nopcre`	Esta opción de configuración deshabilita todas las reglas con `pcre`.

Reglas

Las reglas de Snort se analizan y se cargan cuando se carga PCS (cualquier importación o captura en Investigator, comienzo de captura inicial y recarga de analizador en Decoder).

- No se hace caso de las reglas que no se analizan correctamente.
- Las reglas de Snort válidas se deben analizar correctamente; sin embargo, hay opciones de reglas que no son compatibles con Decoder, las cuales no se analizan por completo.

Sección	Descripción
Encabezado	Las condiciones del encabezado se evalúan cuando una regla recibe la primera devolución de llamada de token para un flujo. El encabezado se evalúa una vez por flujo e impide cualquier consideración adicional de una regla contra un flujo específico si no se cumplen las condiciones.
Acciones	Se debe definir la acción especificada o una regla (ya sea una de las acciones nativas de Snort o definidas en la configuración mediante la instrucción `ruletype`) para que la regla se considere válida. Decoder utiliza solamente reglas con acciones de alerta.
Protocolos	Decoder es compatible con las palabras clave del protocolo Snort actual (`tcp`, `udp`, `icmp` y `ip`).
Direcciones IP	Es compatible el lenguaje completo para definir direcciones IP, lo que incluye listas, CIDR y negación.
Números de puerto	Es compatible el lenguaje completo para definir números de puerto, lo que incluye listas, rangos y negación.
Operador de dirección	El operador direccional es compatible con los valores desde-hasta (“->”) y bidireccional (“<>”). El valor hasta-desde (“<-”) no es válido y hará que la regla no se cargue.

Opciones generales

Decoder utiliza las siguientes opciones generales de reglas de Snort:

Opción	Descripción
`msg`	Si la regla coincide, el valor `msg` se agrega como los metadatos `risk.info`, `risk.warning` o `risk.suspicious`, según la prioridad de la regla.
`sid`	Si la regla coincide, el valor `sid` se agrega como metadatos.
`classtype`	Si la regla coincide, el nombre `classtype` se agrega como los metadatos `threat.cat`.
`priority`	Si la regla coincide y tiene una opción `priority`, se utiliza para determinar el tipo de metadatos de riesgo asociados con el valor `msg`.

Opciones de carga útil

Decoder es compatible con las siguientes opciones de reglas de carga útil.

Opción	Descripción
`content`	La opción `content` crea un token con el cual debe coincidir Decoder. Se aceptan solamente tokens de tres o más bytes. También es importante tener en cuenta que Decoder difiere de Snort en que las reglas se evalúan a través de la carga útil del flujo reconstruido y no solo de un único paquete. Esto puede dar lugar a diferencias en las coincidencias de reglas entre Snort y Decoder, especialmente cuando se consideran opciones posicionales.
`nocase`	No es compatible actualmente. No se hace caso de esta opción se omite y se utiliza la coincidencia que distingue mayúsculas de minúsculas.
`depth`	Esta opción se aplica a la distancia del token desde el principio del flujo. Si la posición del token es mayor que este valor, no es una coincidencia.
`offset`	Esta opción se aplica a la distancia del token desde el principio del flujo. Si la posición del token es menor que este valor, no es una coincidencia.
`distance`	Esta opción se aplica a la distancia del token desde el final de la coincidencia con el token anterior. Si la posición relativa del token es menor que este valor, no es una coincidencia.
`within`	Esta opción se aplica a la distancia del token desde el final de la coincidencia con el token anterior. Si la posición relativa del token es mayor que este valor, no es una coincidencia.
`http_uri`	Se verifica que cualquier token que coincida esté dentro de `http_uri`, según lo indica el analizador HTTP. No se aplica ninguna normalización de URI.
`uricontent`	No se aplica ninguna normalización de URI. De lo contrario, esto equivale a la opción content con el modificador `http_uri`.
`pcre`	Actualmente, las PCRE se aplican solamente a los URI y deben especificar la opción U.

Opciones no relacionadas con la carga útil

Opción	Descripción
`flow`	Verifica que la regla se aplique solamente al flujo de cliente o servidor.
`to_client`	Limita la regla a la coincidencia únicamente con un flujo que Decoder haya definido como servidor.

Opción	Descripción
`from_server`	Sinónimo de `to_client`.
`from_client`	Limita la regla a la coincidencia únicamente con un flujo que Decoder haya definido como cliente.
`flowbits`	Mantiene el estado por sesión y se restablece al final de cada sesión.
`set`	Cuando la regla coincide, el flowbit especificado se establece.
`unset`	Cuando la regla coincide, el flowbit especificado se borra.
`toggle`	Cuando la regla coincide, el flowbit especificado se alterna.
`isset`	Cuando se evalúa la regla, el estado del flowbit especificado se debe establecer para que la regla coincida.
`isnotset`	Cuando se evalúa la regla, el estado del flowbit especificado no se debe establecer para que la regla coincida.
`noalert`	Impide que la regla genere metadatos en caso de que coincida.

Analizador de búsqueda

En este tema se explica cómo configurar un analizador personalizado utilizado en un Decoder para generar metadatos mediante el escaneo de palabras clave y expresiones regulares predefinidas en la vista Configuración de servicios > pestaña Archivos.

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es**search.ini**, el analizador de búsqueda.

search.ini

El Analizador de búsqueda es un analizador personalizado que se utiliza para generar metadatos mediante el escaneo de palabras clave predefinidas y expresiones regulares. El analizador realiza búsquedas en la carga útil de una sesión reconstruida para detectar coincidencias de cadena y puede ejecutar una búsqueda de expresión regular. Puede configurar el analizador mediante el archivo search.ini.

Precaución: El analizador de búsqueda puede afectar significativamente el rendimiento del sistema. Es importante comprender bien el mecanismo de búsqueda y los datos a los cuales se aplica antes de crear nuevas definiciones de búsqueda y de habilitar el analizador de búsqueda.

La definición de búsqueda se utiliza en todos los protocolos. Existen tres métodos de búsqueda básicos:

- Palabra clave: Buscar en un flujo un conjunto específico de palabras
- Pattern: Buscar en un flujo una coincidencia de expresión regular
- Palabra clave + patrón: Buscar en un flujo una expresión regular si contiene algún conjunto de palabras clave específico.

Para obtener una explicación detallada, consulte Analizador de búsqueda en la Sintaxis de la cadena de búsqueda search.ini.

Sintaxis de la cadena de búsqueda search.ini

En este tema se presentan los métodos de búsqueda y la sintaxis que se utilizan en el analizador de búsqueda.

El analizador de búsqueda usa tres métodos de búsqueda básicos:

- Palabra clave: Buscar en un flujo un conjunto específico de palabras.
- Pattern: Buscar en un flujo una coincidencia de expresión regular.
- Palabra clave + patrón: buscar en un flujo una expresión regular si contiene cualquier palabra clave de un conjunto especificado.

Sintaxis

```
Maxrecon=<max_size>Maxsearch=<max_ssearch_length>MatchLimit=<max_matches_per_
stream
Search Name
Services=<service_id_list>Keywords=<keyword_list>|Pattern=<expression>Case=0|1
Proximity=<number_of_bytes>Recon=0|1
Raw=0|1
```

Parámetros

Parámetros usados en este comando:

Parámetro	Descripción
`autocheck`	Arregla automáticamente todos los problemas sin mensajes
`header Only`	Comprueba/muestra el encabezado de cada archivo
`chatty`	Muestra un volcado hexadecimal de cada objeto en el archivo (cantidad enorme de datos)
`dump#-#`	Indica un objeto basado en cero o un rango de objetos en el archivo que saldrá en forma hexadecimal a la consola

Ejemplo

A continuación se muestra un ejemplo del comando:

Para comprobar todos los archivos de base de datos de NetWitness ubicados en la recopilación que se denomina predeterminada. Si se encuentra algún problema, el comando lo describirá y le preguntará si desea corregirlo.

```
dbcheck C:\Documents and Settings\User\My Documents\NetWitness\
Investigations\Default\*.nw*
```

Configuración de LAN inalámbrica

En este tema, se presenta el archivo de configuración de LAN inalámbrica para Decoders, que se encuentra en la vista Configuración de servicios > pestaña Archivos.

wlan-config.xml

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es **`wlan-config.xml`**, el archivo de configuración de LAN inalámbrica.

Controla los analizadores 802.11. Su propósito principal es controlar el descifrado de frames 802.11 crudos capturados por el Decoder. Este archivo es opcional. Si no desea usar el descifrado de tráfico 802.11, no hay necesidad de crear el archivo.

Existen cinco analizadores de nivel de vínculo relacionados con la captura de paquetes de LAN inalámbrica:

- Analizador IEEE 802.11 (frames de datos y beacons solamente)
- Radiotap con encabezado 802.11
- Absolute Value Systems (AVS) con encabezado 802.11
- Prism II con encabezado 802.11
- CACE's "Per Packet Information" (PPI) con encabezado 802.11

Todos los analizadores inalámbricos 802.11 incluidos en la versión 9.8 comparten un único archivo de configuración. Este archivo wlan-config.xml se utiliza para definir cualquier punto de acceso de análisis que el usuario pueda tener en la red y su propósito principal es controlar el descifrado. El BSSID del punto de acceso y el SSID para el cual tiene autorización se agregan a este archivo, así como también todas las claves predeterminadas activas que utiliza el punto de acceso.

Referencias de Decoder y Log Decoder

Este es un conjunto de referencias que proporcionan información acerca de la interfaz del usuario de Decoders y Log Decoders en NetWitness Platform, con referencias a los procedimientos que describen el trabajo que puede realizar en esa parte de la interfaz del usuario. Estos temas se presentan en orden alfabético.

Temas

Vista Configuración de servicios: Pestaña Privacidad de datos

En la pestaña Privacidad de datos (**ADMINISTRAR > Servicios > seleccione un Decoder o un Log Decoder >**  **> Configuración > pestaña Privacidad de datos)**, los administradores pueden configurar parámetros de privacidad de datos para ciertos servicios principales. Para Decoder y Log Decoder, puede configurar el algoritmo hash y el valor de sal predeterminados.

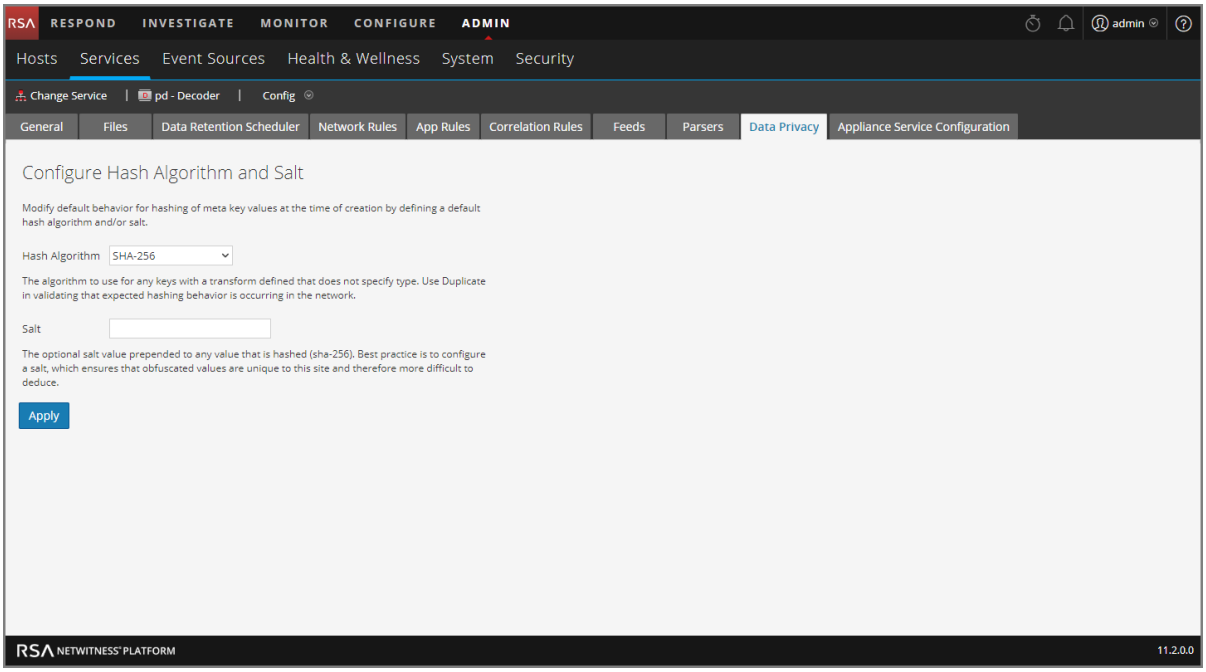
¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Administrador	configurar algoritmo hash y valor de sal	"Configurar el algoritmo hash y el valor de sal" en la *Guía de administración de la privacidad de datos*. (Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.)

Temas relacionados

- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder

Vista rápida



La pestaña Privacidad de datos incluye los ajustes de configuración Configurar algoritmo hash y valor de sal. En la siguiente tabla se describen los parámetros de esta pestaña.

Parámetro	Descripción
Algoritmo hash	Muestra una lista desplegable de algoritmos hash que se usan para cualquier clave con una transformación que no especifica un tipo de algoritmo. Los valores posibles son SHA-256 y Duplicate. Duplicate es un algoritmo especial a disposición de los administradores cuando desean validar que en la red se produzca el comportamiento de hash previsto. En versiones de NetWitness Platform anteriores a 10.5, SHA-1 estaba disponible como un algoritmo hash, pero RSA no recomienda su uso.
Valor de sal	Indica el valor de sal opcional que se antepone a cualquier valor al cual se aplica hash. Las mejores prácticas con fines de seguridad recomiendan un valor de sal que no sea inferior a 100 bits o 16 caracteres de largo. La configuración de un valor garantiza que los valores ocultos sean únicos de este sitio y, por lo tanto, más difíciles de deducir. Para obtener más información sobre este campo, consulte "Configurar el ocultamiento de datos" en la guía *Administración de la privacidad de datos*.
Aplicar	Aplica los cambios.

Vista Configuración de servicios: Calendarizador de retención de datos

En la pestaña Calendarizador de retención de datos de la vista Configuración de servicios, puede establecer los criterios de transferencia para la eliminación de registros de la base de datos desde el almacenamiento primario mediante un umbral basado en antigüedad. También puede programar el momento en que se comprueba si se alcanza el umbral.

Para acceder a la pestaña Calendarizador de retención de datos, vaya a **ADMINISTRAR** > **Servicios** > seleccione un servicio **Decoder** o **Log Decoder** y haga clic en > **Ver** > **Configuración** > pestaña **Retención de datos**.

¿Qué desea hacer?

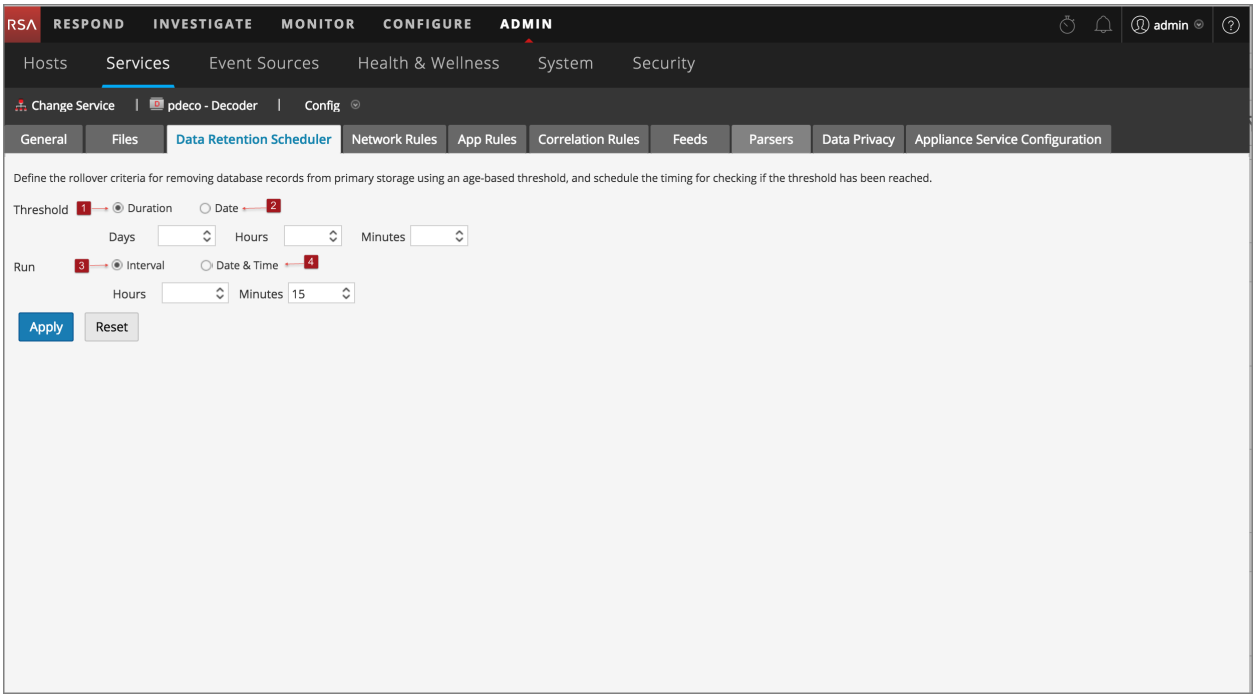
Función de usuario	Deseo…	Documentación
Administrador	Programar el momento en que se comprueba si se alcanza el umbral.	Configurar el manejo de las transacciones en un Decoder

Temas relacionados

- Configurar ajustes comunes en un Decoder
- Configuración rápida de Decoder y Log Decoder

Vista rápida

Este es un ejemplo de la pestaña Calendarizador de retención de datos.



1	**Duración de umbral**: Quita los archivos de la base de datos más antiguos que la cantidad seleccionada de días, minutos u horas.
2	**Fecha de umbral**: Quita los archivos de la base de datos más antiguos que la fecha UTC seleccionada (AAAA-MM-DD-HH:MM:SS) que no son compatibles con los parámetros de minutos, horas o días.
3	**Intervalo de ejecución**: Indica la cantidad de horas entre ejecuciones.
4	**Fecha y hora de ejecución**: Define los días de la semana en que se ejecutará el programador, así como la hora de ejecución en formato HH:MM:SS para la hora local del servicio.

Vista Configuración de servicios: Pestaña Feeds

Los feeds y los analizadores son programas Lua que se cargan y se compilan cuando se procesan archivos de captura en Investigation o se capturan datos con Decoders. Su uso más común es en la extracción de metadatos estáticos y la identificación de servicios.

Nota: Las versiones de NetWitness anteriores a 11.0 utilizan programas FLEXPARSE además de programas Lua; los Flexparsers están obsoletos en NetWitness Platform 11.0. A menos que se indique lo contrario, todas las referencias a los Decoders se aplican también a los Log Decoders.

NetWitness Platform utiliza feeds para crear metadatos basados en valores de metadatos definidos de forma externa. Un feed es una lista de datos que se compara con las sesiones a medida que se capturan o procesan. Para cada coincidencia, se crean metadatos adicionales. Estos datos pueden identificar y clasificar direcciones IP maliciosas o incorporar información adicional, como departamento y ubicación según la asignación de redes internas. Algunos ejemplos de feed incluyen feeds de amenazas para identificar BOTNets, mapeos de DHCP o incluso información de Active Directory, como una ubicación física o un departamento lógico.

Puede agregar, eliminar y actualizar feeds, mientras se ejecuta un Decoder, sin afectar la captura. En la pestaña Feeds (**ADMINISTRAR > Servicios >** seleccione un servicio y haga clic en  **> Ver > Configuración > pestaña Feeds**) se proporciona una interfaz del usuario para la administración de feeds en Decoders.

¿Qué desea hacer?

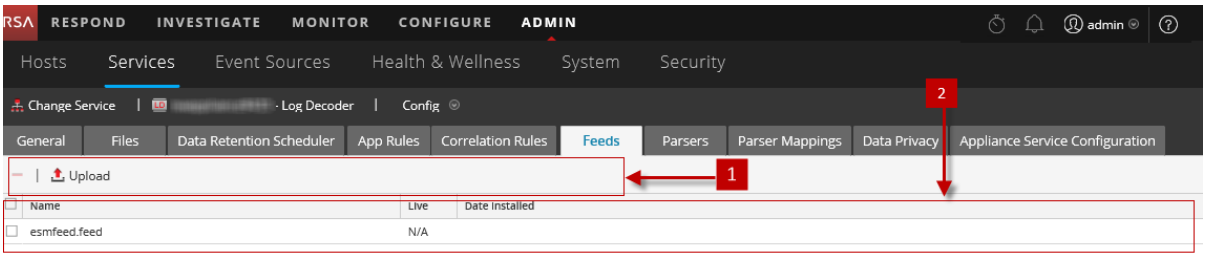
Función de usuario	Deseo…	Documentación
Administrador	Configurar feeds	Configurar feeds y analizadores
Administrador	habilitar y deshabilitar analizadores	Habilitar y deshabilitar analizadores y analizadores de registros

Temas relacionados

- Configurar ajustes comunes en un Decoder
- Configuración rápida de Decoder y Log Decoder
- Cuadro de diálogo Cargar feeds
- Referencias de feed y analizador

Vista rápida

Este es un ejemplo de la pestaña Feeds.



1 Barra de herramientas de la pestaña Feeds: Proporciona opciones para trabajar con feeds en la cuadrícula.

2 Cuadrícula Feed: Enumera todos los feeds que están implementados actualmente en el Decoder.

Barra de herramientas de la pestaña Feeds

Función	Descripción
Upload	Muestra el cuadro de diálogo Cargar feeds.
−	Elimina los feeds seleccionados.

Lista Feeds

La lista Feeds proporciona una lista de todos los feeds implementados actualmente para el Decoder.

Columna	Descripción
Nombre	El nombre del feed o el archivo del feed.
Live	Indica si el feed se originó en Live. Los posibles valores son **Sí**, **No** o **N/D**. • **Sí** = Instalado mediante Live • **No** = Instalado mediante NetWitness Platform • **N/D** = El feed no tiene un archivo de atributos creado por NetWitness Platform para rastrear la fecha de instalación. El feed se puede haber instalado manualmente, no mediante NetWitness Platform ni Live Services. Los feeds instalados manualmente aun funcionan correctamente.
Fecha de instalación	La fecha en que el feed se migró al servicio.

Cuadro de diálogo Cargar feeds

En este tema se describen las funcionalidades del cuadro de diálogo Cargar feeds en la vista Configuración de servicios > pestaña Feeds.

La opción **Cargar** en la vista Configuración de servicios > pestaña Feeds muestra el cuadro de diálogo Cargar feeds, en el cual puede administrar la carga de feeds a un Decoder o Log Decoder.

¿Qué desea hacer?

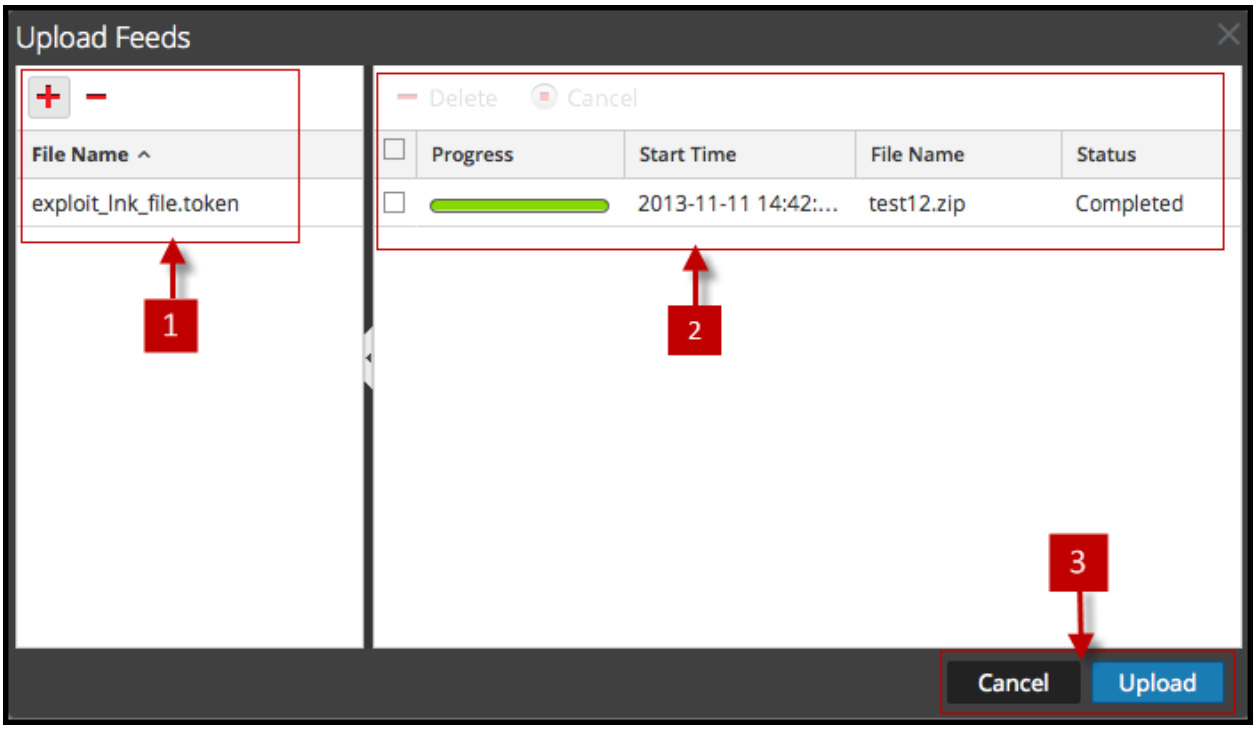
Función de usuario	Deseo…	Documentación
Administrador	preparar una lista de feeds para cargar	Editar, cargar o quitar un feed
Administrador	ver y eliminar trabajos de carga	Editar, cargar o quitar un feed

Temas relacionados

- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder
- Referencias de feed y analizador

Vista rápida

Este es un ejemplo del cuadro de diálogo Cargar feeds.



1 Lista de archivos: Proporciona un lugar para preparar una lista de feeds para cargar.
2 Lista Trabajo de carga: Proporciona una vista de trabajos de carga.
3 Botones del cuadro de diálogo Cargar feeds

Lista de archivos

La Lista de archivos es el lugar donde se prepara una lista de feeds para cargar. Puede agregar archivos desde una estructura de directorio y eliminar archivos desde la cuadrícula, si decide que no desea cargar un archivo en especial. Cuando la lista está preparada, el proceso de carga se inicia si se hace clic en **Cargar**.

Función	Descripción
+	Abre una vista de la estructura de directorios donde puede seleccionar los archivos que agregará a la Lista de archivos.
−	Elimina los archivos seleccionados de la Lista de archivos.
Nombre de archivo	Muestra los archivos de feed que ha agregado desde un sistema de archivos como preparación para cargarlos a un Decoder. Cuando hace clic en **Cargar**, se cargan los archivos que se muestran aquí.

Lista Trabajo de carga

La lista Trabajo de carga proporciona una vista de los trabajos de carga que se iniciaron cuando se hizo clic en **Cargar**.

Función/columna	Descripción
Delete	Elimina un trabajo de carga.
Progreso	Muestra el progreso de un trabajo de carga.
Hora de inicio	Muestra la hora de inicio de un trabajo de carga.
Nombre de archivo	Indica el nombre de archivo del feed que se está cargando.
Estado	Muestra el estado de un trabajo de carga.

Botones del cuadro de diálogo Cargar feeds

Función	Descripción
Cancelar	Cierra el cuadro de diálogo Cargar feed.
Cargar	Inicia la carga de los archivos de feed que se enumeran en la Lista de archivos. Cada feed aparece en una fila por separado en la lista Proceso de carga.

Vista Configuración de servicios: Pestaña Archivos

Los archivos de configuración de Decoder y Log Decoder se pueden ver y editar en la vista Configuración de servicios > pestaña Archivos. En "Editar los archivos de configuración de servicios principales" de la *Guía de introducción de hosts y servicios* se proporcionan instrucciones generales para editar archivos. (Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.)

Al igual que otros servicios principales, Decoder y Log Decoder tienen un archivo de índice y también pueden tener un generador de informes de fallas, netwitness, y un programador. Los archivos de índice de Decoder y Log Decoder se denominan **`index-decoder-custom.xml`** y **`index-logdecoder-custom.xml`**.

Nota: Este tipo de archivo está disponible solo para Log Decoder con contenido Envision instalado. `Table-map.xml` y `table-map-custom.xml` se mostrarán ahora, pero solamente si se encontró `table-map.xml` en el sistema de archivos (por ejemplo, es un Log Decoder con contenido Envision instalado).

¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Administrador	obtener archivos de registro de Log Decoder anterior a 11.0	Obtener archivos de registro de Log Decoder anterior a 11.0
Administrador	editar archivos y analizadores	Referencias de feed y analizador

Temas relacionados

- Configurar ajustes comunes en un Decoder
- Configuración rápida de Decoder y Log Decoder
- Crear claves de metadatos personalizados mediante un feed personalizado

Vista rápida

Nombre del archivo	Descripción
`GeoPrivate.ipl`	Este analizador fijo toma las direcciones IP y las convierte en ubicaciones geográficas. Las ubicaciones se muestran a través de la vista de Google Earth.
`feed-definitions.xml`	Se utiliza para crear feeds personalizados y es el esquema XML que utiliza Decoder para definir un mensaje de **feed** cuando crea un archivo **.feed** .

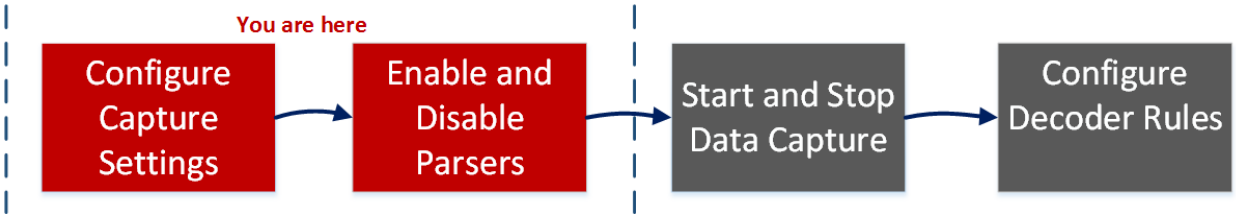
Nombre del archivo	Descripción
`traffic_flow_options.lua`	Se utiliza para proporcionar información de direccionalidad. Actualice este archivo con subredes internas y externas específicas del ambiente para el analizador Lua con el fin de crear la direccionalidad correcta en los metadatos. El analizador se describe en Contenido de RSA para RSA NetWitness Platform.
`search.ini`	Este es el archivo de configuración del Analizador de búsqueda. El Analizador de búsqueda es un analizador personalizado que se utiliza para generar metadatos mediante el escaneo de palabras clave predefinidas y expresiones regulares.
`wlan-config.xml`	Este es el archivo de configuración de LAN inalámbrica (09/09/09). Este archivo controla los analizadores 802.11. Su propósito principal es controlar el descifrado de frames 802.11 crudos capturados por el Decoder.

Vista Configuración de servicios: Pestaña General

La pestaña General de un Decoder en la vista Configuración de servicios proporciona una manera de administrar la configuración básica del servicio, configurar la captura de datos y seleccionar los analizadores que se aplican a los datos capturados. Para acceder a la pestaña General, vaya a **ADMINISTRAR > Servicios >** seleccione un Decoder o un Log Decoder y haga clic en > **Ver > Configuración > pestaña General**.

Flujo de trabajo

En la siguiente figura se muestran las tareas de configuración comunes del Decoder y se resaltan los pasos que puede realizar en esta vista.



¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Administrador	configurar ajustes de captura*	Configurar ajustes de captura
Administrador	administrar analizadores y analizadores de registros*	Habilitar y deshabilitar analizadores y analizadores de registros
Administrador	iniciar y detener la captura de datos	Iniciar y detener la captura de datos
Administrador	configurar reglas	Configurar reglas de Decoder

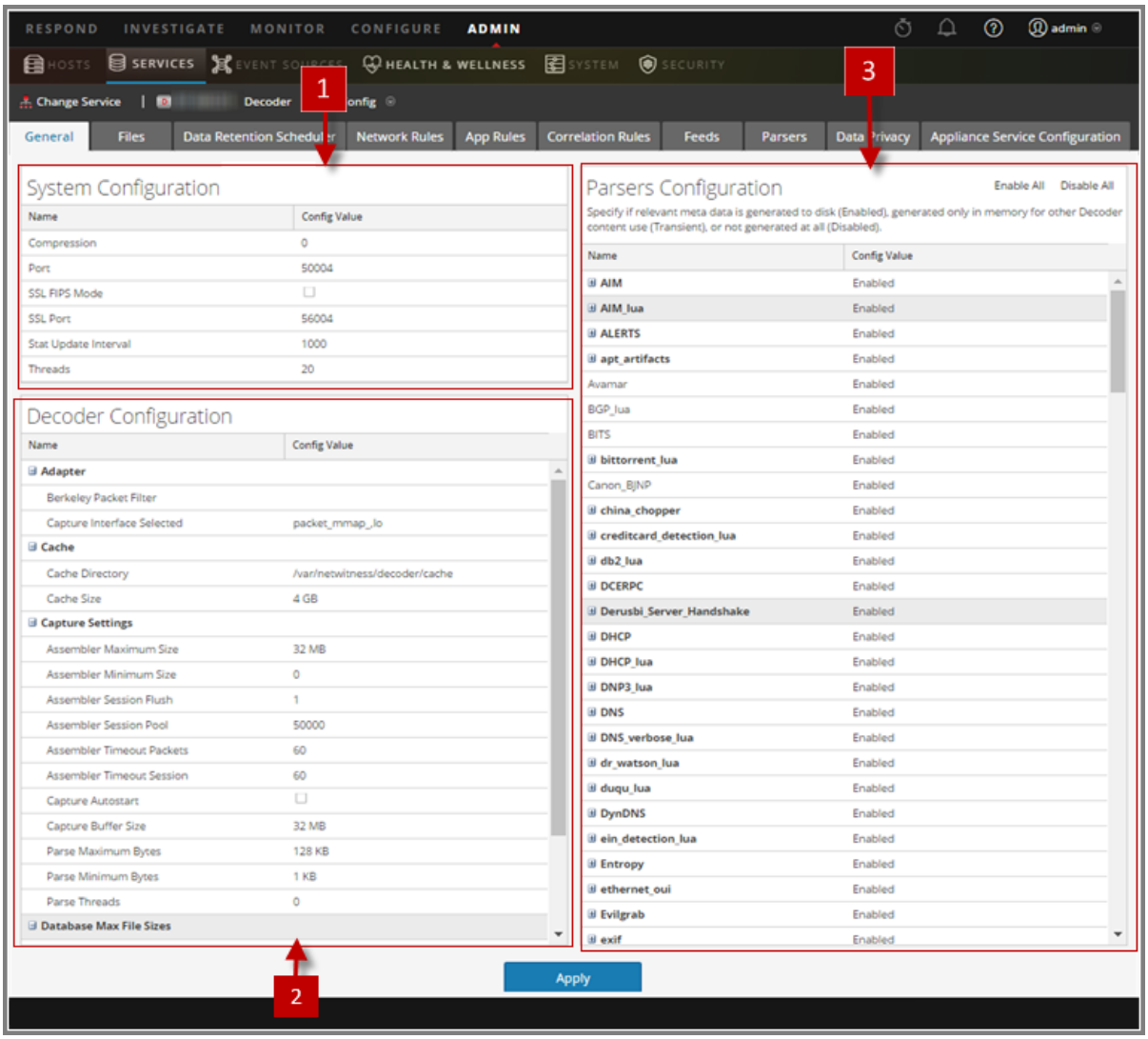
*Puede realizar estas tareas aquí.

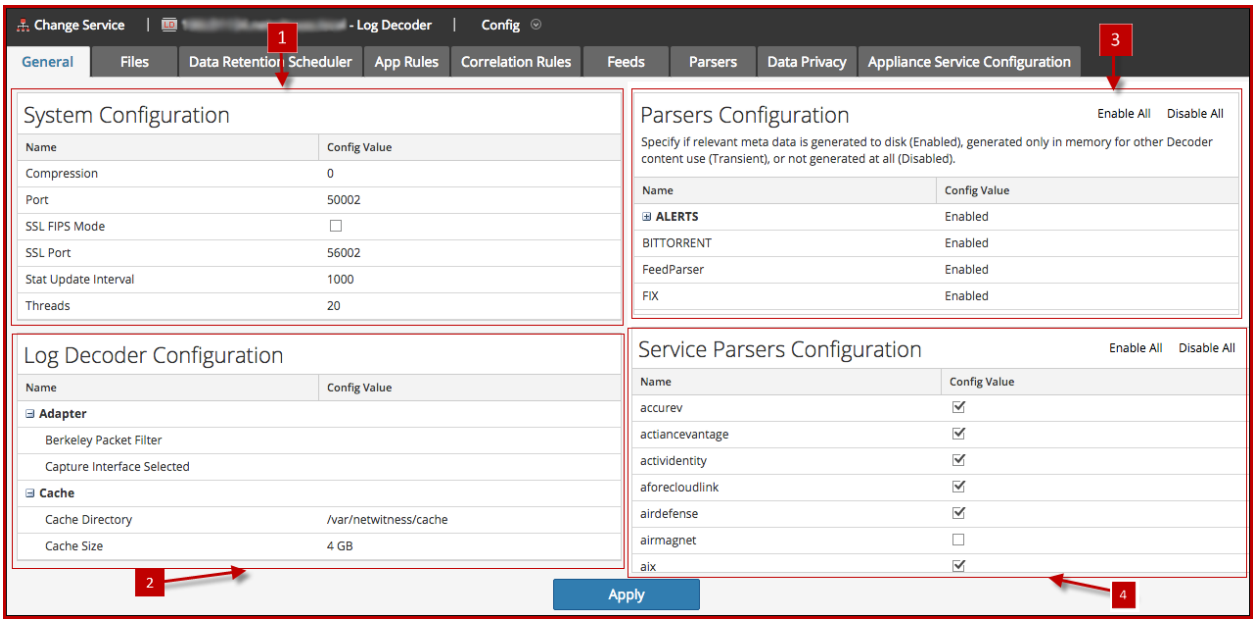
Temas relacionados

- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder
- Configurar feeds y analizadores

Vista rápida

La primera imagen muestra un ejemplo de la pestaña General de un Decoder. La segunda corresponde a la pestaña General de un Log Decoder.


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
HOSTS
SERVICES
EVENT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Change Service
Decoder
1
3
General
Files
Data Retention Scheduler
Network Rules
App Rules
Correlation Rules
Feeds
Parsers
Data Privacy
Appliance Service Configuration
System Configuration
Name
Config Value
Compression
0
Port
50004
SSL FIPS Mode
SSL Port
56004
Stat Update Interval
1000
Threads
20
Decoder Configuration
Adapter
Berkeley Packet Filter
Capture Interface Selected
packet_mmap_lo
Cache
Cache Directory
/var/netwitness/decoder/cache
Cache Size
4 GB
Capture Settings
Assembler Maximum Size
32 MB
Assembler Minimum Size
0
Assembler Session Flush
1
Assembler Session Pool
50000
Assembler Timeout Packets
60
Assembler Timeout Session
60
Capture Autostart
Capture Buffer Size
32 MB
Parse Maximum Bytes
128 KB
Parse Minimum Bytes
1 KB
Parse Threads
0
Database Max File Sizes
2
Parsers Configuration
Enable All
Disable All
Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).
Name
Config Value
AIM
Enabled
AIM_lua
Enabled
ALERTS
Enabled
apt_artifacts
Enabled
Avamar
Enabled
BGP_lua
Enabled
BITS
Enabled
bittorrent_lua
Enabled
Canon_BJNP
Enabled
china_chopper
Enabled
creditcard_detection_lua
Enabled
db2_lua
Enabled
DCERPC
Enabled
Derusbi_Server_Handshake
Enabled
DHCP
Enabled
DHCP_lua
Enabled
DNP3_lua
Enabled
DNS
Enabled
DNS_verbose_lua
Enabled
dr_watson_lua
Enabled
duqu_lua
Enabled
DynDNS
Enabled
ein_detection_lua
Enabled
Entropy
Enabled
ethernet_oui
Enabled
Evilgrab
Enabled
exif
Enabled
Apply



1 Configuración del sistema: Administra la configuración del servicio para un Decoder.

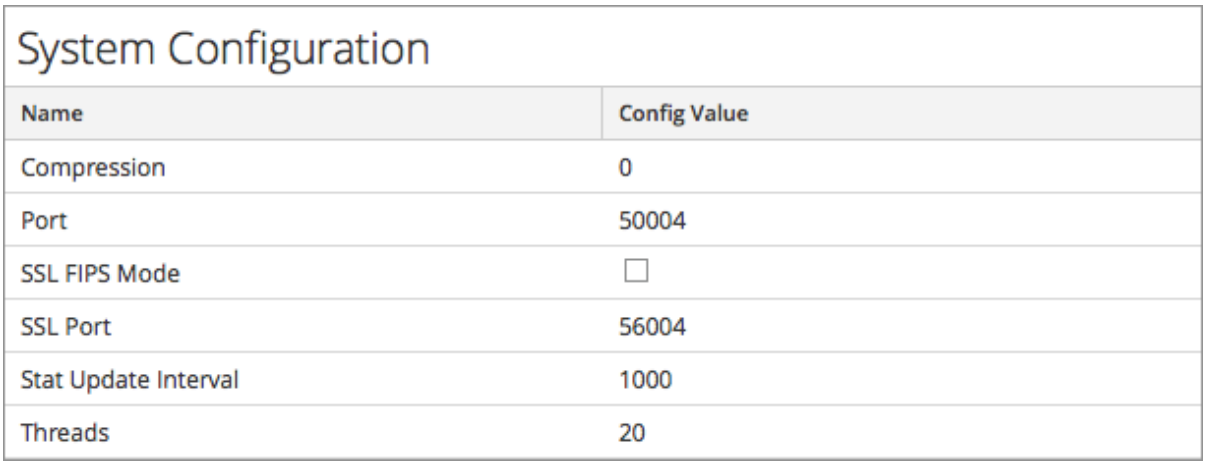
2 Configuración de Decoder o Log Decoder: Permite ver y editar los parámetros de configuración del servicio para un Decoder o Log Decoder.

3 Configuración de analizadores: Permite seleccionar los analizadores que se usarán en el Decoder.

4 Configuración de analizadores de servicio (solo Log Decoders): Permite seleccionar los analizadores de servicio que se usarán en el Log Decoder.

Sección Configuración del sistema

La sección Configuración del sistema administra la configuración del servicio de un Decoder. Cuando un servicio se agrega por primera vez, los valores predeterminados están vigentes y deben cambiarse solo en circunstancias especiales, por ejemplo, si el servicio al cliente aconseja un cambio.

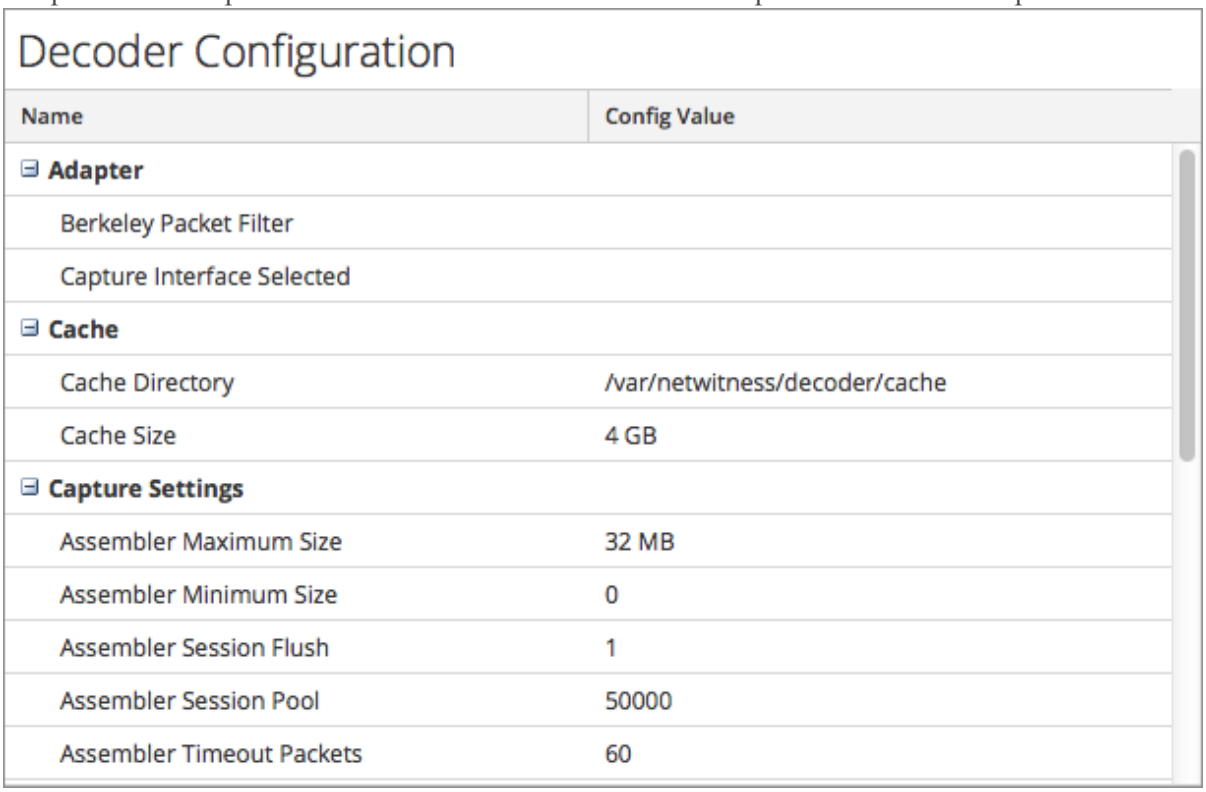


La sección Configuración del sistema tiene estos parámetros.

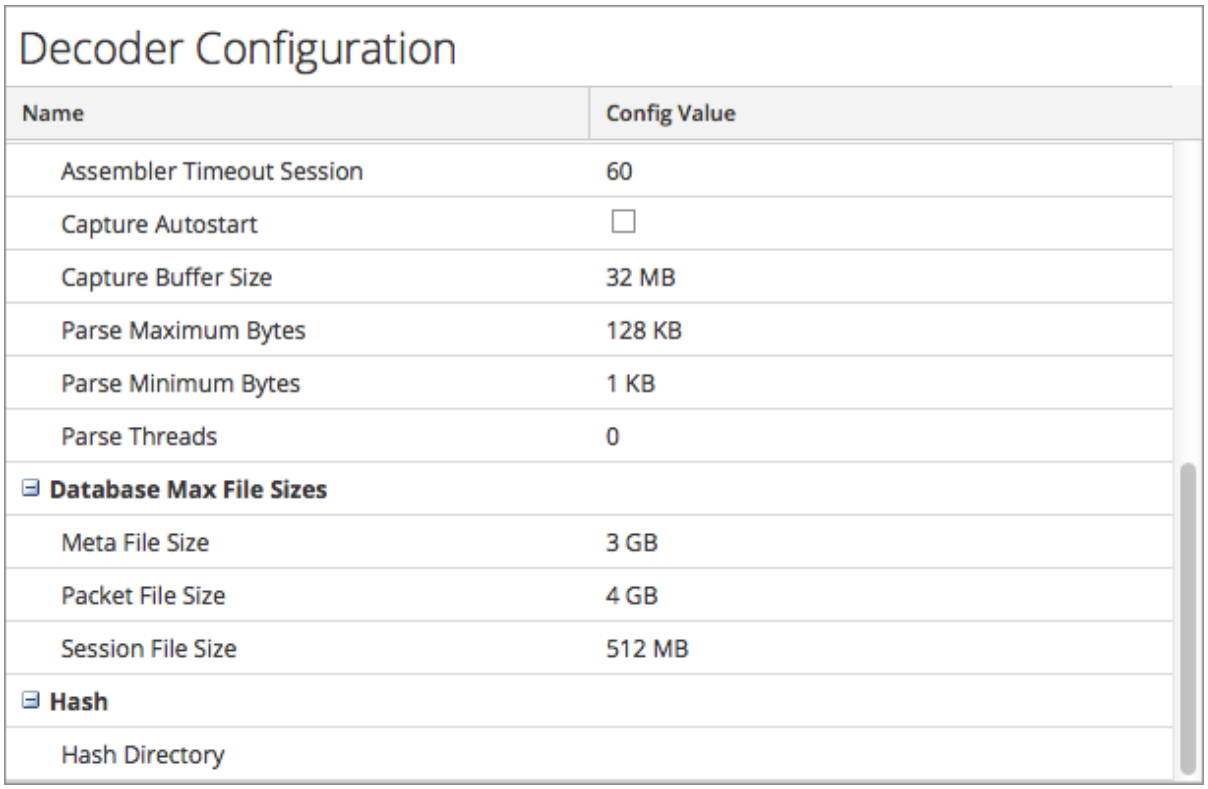
Parámetro	Descripción
Compresión	La cantidad mínima de bytes que se deben transmitir por respuesta antes de la compresión. Si se define en 0, se deshabilita la compresión. El valor predeterminado es **0**. Un cambio en el valor se aplica de inmediato en todas las conexiones subsiguientes.
Puerto	Determina el puerto que usa el servicio. **Nota:** Si cambia el número de puerto, asegúrese de reiniciar el servicio.
Modo SSL FIPS	Si esta opción está activada, todos los datos transferidos en la red se cifrarán mediante SSL.
Puerto SSL	Indica el puerto que se usa para cifrar mediante SSL.
Intervalo de actualización de estadísticas	La cantidad de milisegundos entre las actualizaciones de estadísticas del sistema. Los números más bajos permiten actualizaciones frecuentes y pueden retrasar otros procesos. El valor predeterminado es **1,000**. Un cambio en el valor se aplica de inmediato.
Subprocesos	El número de hilos de ejecución en el pool de hilos de ejecución para manejar solicitudes entrantes. Si se define en **0**, se permite que el sistema decida. Un cambio se aplica tras el reinicio del servicio.

Sección Configuración de Decoder

La sección Configuración de Decoder proporciona una manera de ver y editar los parámetros de configuración de servicio de un Decoder o Log Decoder. Cuando un servicio se agrega por primera vez, se aplican valores predeterminados. Puede editar estos valores para administrar la captura de tráfico.



Si se desplaza hasta el final de la sección, podrá ver estos parámetros adicionales de configuración del Decoder.



Selección Adaptador

Los parámetros de Adaptador configuran la interfaz de red para la captura, como se describe en Configurar ajustes de captura.

Sección Caché

Los parámetros de Caché configuran el directorio de caché y el tamaño de los archivos de caché de la sesión. La tabla siguiente describe los ajustes de caché. Cuando un servicio se agrega por primera vez, los valores predeterminados están vigentes y deben cambiarse solo en circunstancias especiales, por ejemplo, si el servicio al cliente aconseja un cambio.

Parámetro de caché	Descripción
Directorio de caché	El directorio donde se almacenan los archivos de la caché de sesiones. El valor predeterminado es `/var/netwitness/decoder/cache`. El cambio se aplica de inmediato.
Tamaño de caché	El tamaño máximo, en Megabytes (MB), que todos los archivos del directorio de caché pueden alcanzar antes de que se eliminen los archivos más antiguos. Una vez que se alcanza el umbral, el tamaño de la caché se reduce en un 10 %. El valor predeterminado es **4 GB**. El cambio se aplica de inmediato.

Sección Configuración de captura

La sección Configuración de captura ofrece una manera de configurar los ajustes de captura operacional. Cuando un servicio se agrega por primera vez, los valores predeterminados están vigentes y deben cambiarse solo en circunstancias especiales, por ejemplo, si el servicio al cliente aconseja un cambio.

Parámetro de configuración de captura	Descripción
Tamaño máximo de ensamblador	Especifica el tamaño máximo en bytes que pueden alcanzar los datos de paquete de una sesión. El valor predeterminado es **32 MB**. El cambio se aplica de inmediato.
Tamaño mínimo de ensamblador	Especifica el tamaño mínimo en bytes que una sesión debe tener para generar metadatos. Un valor de **0** indica que se generan metadatos de cada sesión. El valor predeterminado es **0**. El cambio se aplica de inmediato.
Vaciado de sesión de ensamblador	Especifica si una sesión se elimina del ensamblador cuando la última cadena de la sesión se elimina del ensamblador. El valor predeterminado es **1**. • **2** = si se agota el tiempo de espera del ensamblador para el primer paquete de una sesión, la sesión se elimina del ensamblador una vez que finaliza el análisis. Cualquier paquete posterior en esta sesión crea una sesión nueva en el ensamblador. • **1** = Si se agota el tiempo de espera del ensamblador para la última cadena de una sesión, la sesión se elimina del ensamblador. Cualquier paquete posterior en esta sesión crea una sesión nueva en el ensamblador. • **0** = si se agota el tiempo de espera del ensamblador para la última cadena de una sesión, la sesión se deja en el ensamblador que se agota el tiempo de espera. Los paquetes subsiguientes de esa sesión se filtran. El cambio se aplica tras el reinicio del servicio.
Pool de sesión de ensamblador	Especifica la cantidad de entradas en el pool de sesión. El valor predeterminado es **350000**. El cambio se aplica tras el reinicio del servicio.
Tiempo de espera de paquetes de ensamblador	Especifica la cantidad de segundos que transcurren antes de que se agote el tiempo de espera de un paquete o una cadena. El valor predeterminado es **60**. El cambio se aplica de inmediato.
Tiempo de espera de sesión de ensamblador	Especifica la cantidad de segundos que transcurren antes de que se agote el tiempo de espera de una sesión. El valor predeterminado es **60**. El cambio se aplica de inmediato.
AutoStart de la captura	Especifica si la captura comienza automáticamente cada vez que se inicia el Decoder. Cuando se selecciona, el valor = yes. Cuando no está seleccionada, el valor = no. El valor predeterminado es **no**. El cambio se aplica de inmediato.

Parámetro de configuración de captura	Descripción
Tamaño de búfer de captura	La asignación del buffer de memoria de captura en Megabytes. El valor predeterminado es **64 MB**. El cambio se aplica tras el reinicio del servicio.
Bytes máximos de análisis	El número máximo de bytes para escanear una secuencia para tokens adicionales. Una vez que se encuentra el primer token, la secuencia se escanea hasta llegar al número definido de bytes, no más allá. Si se define en **0**, se elimina la terminación temprana y se escaneará toda la secuencia, independientemente del tamaño. El valor predeterminado es **128 KB**. El cambio se aplica de inmediato.
Bytes mínimos de análisis	El número mínimo de bytes para escanear una secuencia para el primer token. Si no se encuentra un token dentro del número de bytes definido, se termina el escaneo. Si se define en **0**, se elimina la terminación temprana y se escaneará toda la secuencia, independientemente del tamaño. El valor predeterminado es **1 KB**. El cambio se aplica de inmediato.
Subprocesos de análisis	El número de hilos de ejecución de análisis que se usan para análisis de sesión. Un valor de **0** indica que el servidor decide. El valor predeterminado es **0**. El cambio se aplica tras el reinicio del servicio.

Sección Tamaños máximos de archivo de base de datos

La sección Tamaños máximos de archivo de base de datos controla el tamaño de archivo máximo de diversas bases de datos. Cuando un servicio se agrega por primera vez, los valores predeterminados están vigentes y deben cambiarse solo en circunstancias especiales, por ejemplo, si el servicio al cliente aconseja un cambio.

Parámetro de tamaño de archivo	Descripción
Tamaño de archivo de metadatos	El tamaño máximo de archivos de base de datos de metadatos en megabytes. El valor predeterminado es **10 MB**. El cambio se aplica tras el reinicio del servicio.
Tamaño de archivo de paquete	El tamaño máximo de archivos de base de datos de paquete en megabytes. El valor predeterminado es **10 MB**. El cambio se aplica tras el reinicio del servicio.
Tamaño de archivo de sesión	El tamaño máximo de archivos de base de datos de sesión en megabytes. El valor predeterminado es **100 MB**. El cambio se aplica tras el reinicio del servicio.

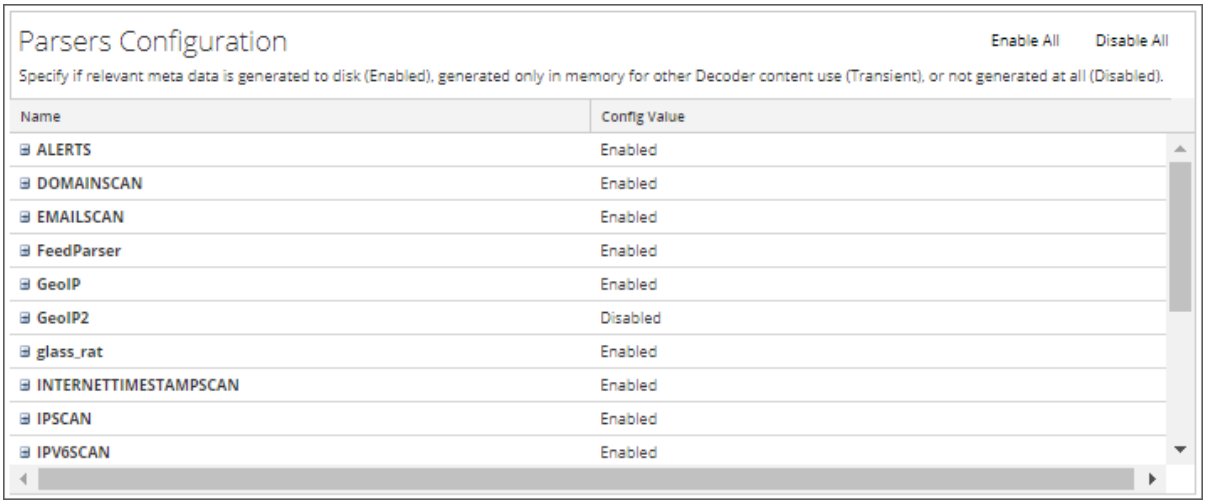
Sección Hash

La configuración de la sección Hash controla las opciones de hash de archivo de la base de datos. Se produce una pequeña disminución del rendimiento cuando se aplican valores hash.

Parámetro de hash	Descripción
Directorio hash	El directorio del servidor donde se escriben todos los archivos hash. Si el valor está vacío, cada archivo hash se escribe en el mismo directorio en que se aplica un valor hash al archivo. El valor predeterminado está en blanco. El cambio se aplica tras el reinicio del servicio.

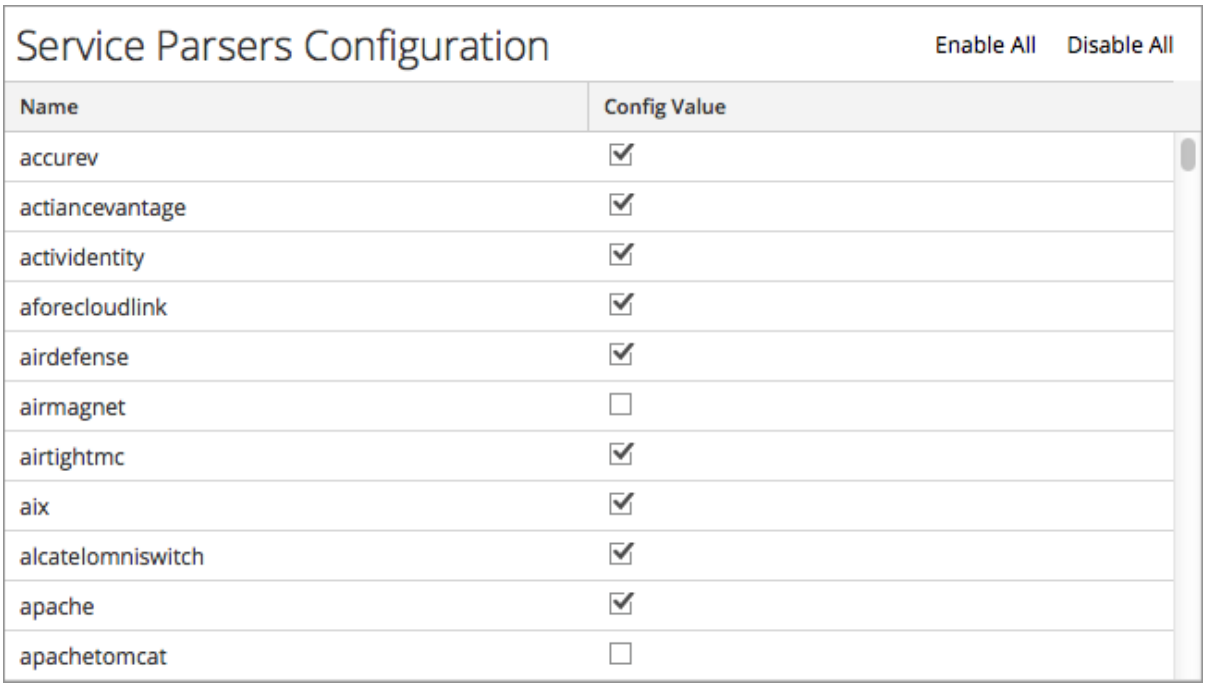
Panel Configuración de analizadores

En el panel Configuración de analizadores se proporciona una forma de seleccionar los analizadores que se usarán en el Decoder. En algunos analizadores, también puede configurar los metadatos que crea el analizador. Consulte Habilitar y deshabilitar analizadores y analizadores de registros para obtener información detallada y procedimientos.



Sección Configuración de analizadores de servicio para Log Decoder

La sección Configuración de analizadores de servicio proporciona una manera de seleccionar analizadores de servicio para usarlos en el Log Decoder.



Vista Configuración de servicios: Pestaña Analizadores

En la vista Configuración de servicios > pestaña Analizadores, puede ver los analizadores implementados en un Decoder o Log Decoder, cargar analizadores y eliminar los analizadores implementados. Es posible agregar y quitar analizadores mientras un Decoder o un Log Decoder están en funcionamiento sin afectar la captura.

Para acceder a la pestaña Analizadores, vaya a **ADMINISTRAR** > **Servicios** > seleccione un servicio **Decoder** o **Log Decoder** y haga clic en > **Ver** > **Configuración** > pestaña **Analizadores**.

¿Qué desea hacer?

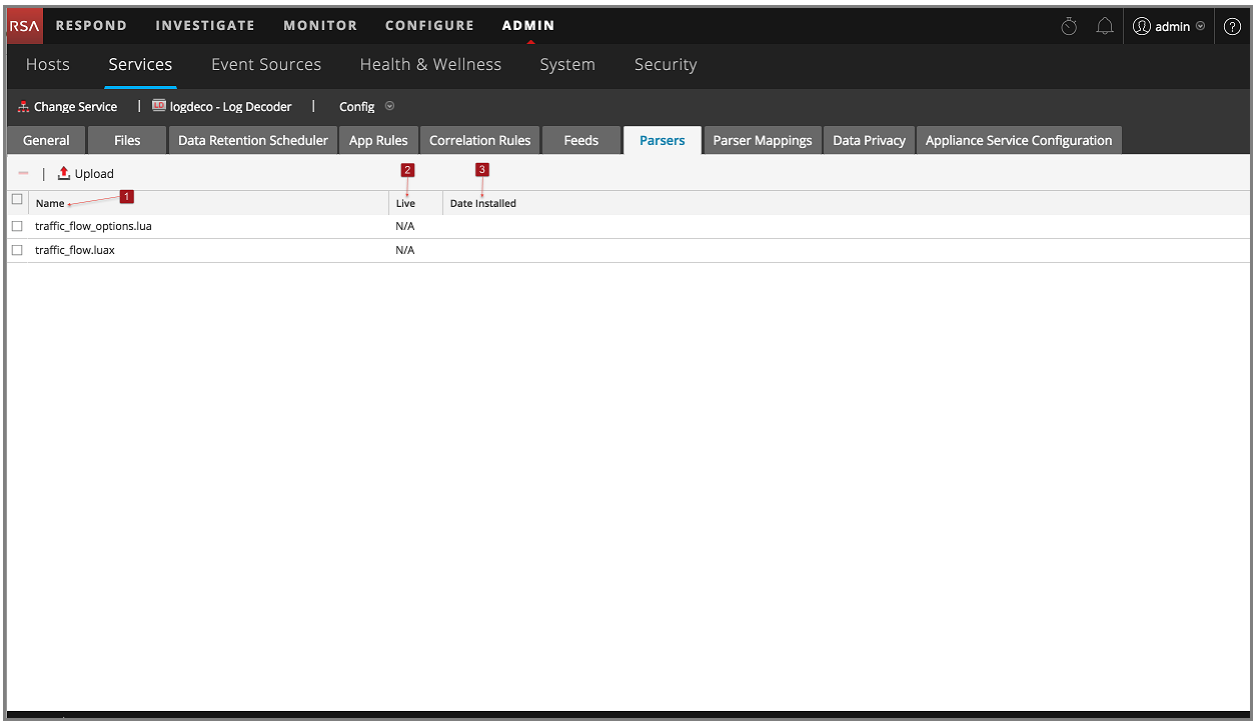
Función de usuario	Deseo…	Documentación
Administrador	Ver los analizadores implementados.	Habilitar y deshabilitar analizadores y analizadores de registros
Administrador	Cargar analizadores a un Decoder o Log Decoder.	Habilitar y deshabilitar analizadores y analizadores de registros

Temas relacionados

- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder
- Cargar y eliminar analizadores personalizados

Vista rápida

Este es un ejemplo de la pestaña Analizadores. La cuadrícula Analizadores muestra todos los analizadores que se encuentran implementados actualmente en el Decoder.



1 **Nombre**: El nombre del analizador o el archivo del analizador.

2 **Live**: Indica si el analizador se originó de Live. Los posibles valores son **Sí**, **No** o **N/D**.

- **Sí** = Instalado mediante Live Services.
- **No** = Instalado mediante NetWitness.
- **N/D** = El analizador no tiene un archivo de atributos que crea NetWitness para rastrear la fecha de instalación. El analizador se puede haber instalado manualmente, no mediante NetWitness ni Live Services.

3 **Fecha de instalación**: La fecha en que el analizador se migró al servicio.

Barra de herramientas de la pestaña Analizadores

La barra de herramientas de la pestaña Analizadores cuenta con opciones para trabajar con analizadores en la cuadrícula.

Función	Descripción
Upload	Permite cargar analizadores a un Decoder o un Log Decoder.
−	Solicita confirmación antes de eliminar los analizadores seleccionados. Puede seleccionar **No** para cancelar la eliminación o **Sí** para eliminar los analizadores seleccionados.

Vista Configuración de servicios: pestaña Mapeos de analizador

En este tema se proporciona una descripción de las opciones configurables para un Log Decoder en la pestaña Mapeos de analizador.

En Mapeos de analizador, los administradores pueden configurar mapeos de analizadores de registros para los servicios de Log Decoder. Para acceder a la pestaña Mapeos de analizador, vaya a **ADMINISTRAR** > **Servicios** > seleccione un servicio y haga clic en  > **Ver** > **Configuración** > pestaña **Mapeos de analizador**.

Nota: También puede configurar mapeos de analizadores de registros para servicios Log Decoder si navega a **ADMINISTRAR > Servicios > Orígenes de eventos > Descubrimiento**.

Esta función está diseñada para rastrear un subconjunto de orígenes de eventos que se analiza con un analizador incorrecto.

¿Qué desea hacer?

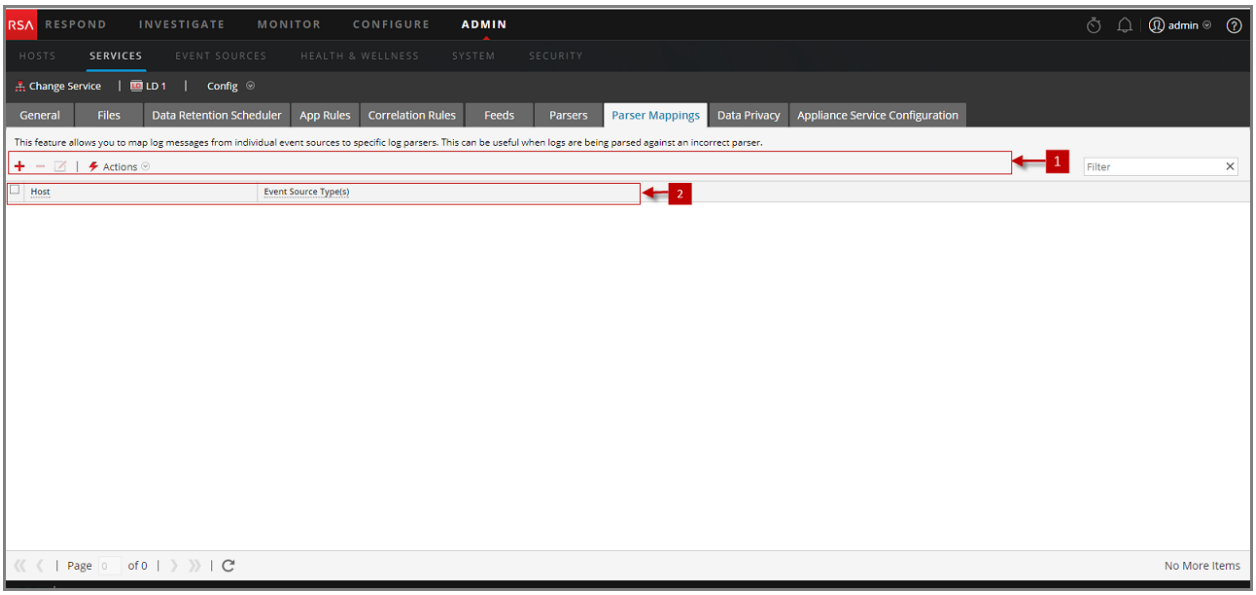
Función de usuario	Deseo…	Documentación
Administrador	Administrar direcciones IP para el mapeo de orígenes de eventos.	Habilitar mapeos de analizadores

Temas relacionados

- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder

Vista rápida

Este es un ejemplo de la pestaña.



1 Barra de herramientas Mapeos de analizador: Ofrece opciones para trabajar con mapeos de analizadores en la cuadrícula.

2 Cuadrícula Mapeos de analizador: Enumera todos los analizadores que se encuentran mapeados actualmente en el Log Decoder.

Barra de herramientas Mapeos de analizador

La barra de herramientas Mapeos de analizador cuenta con opciones para trabajar con mapeos de analizadores en la cuadrícula.

Función	Descripción
	Agregar un mapeo de analizador.
	Eliminar el mapeo de analizador seleccionado.
	Editar un mapeo de analizador.
	Actualizar la lista de mapeos de analizadores.
	Mostrar el menú Acciones. • **Importar**: Importar un mapeo de analizadores a un archivo. • **Exportar**: Guardar un mapeo de analizadores en un archivo.

Lista Mapeos de analizador

En la lista Mapeos de analizador se muestran todos los analizadores que se encuentran mapeados actualmente en el Log Decoder.

Parámetro	Descripción
Host	Muestra la dirección IP del host.
Origen de evento	Muestra los orígenes de eventos que se están analizando incorrectamente.

Cuadro de diálogo Editor de mapeos de analizadores

El cuadro de diálogo Editor de mapeos de analizadores permite actualizar una dirección IP para un mapeo de orígenes de eventos.

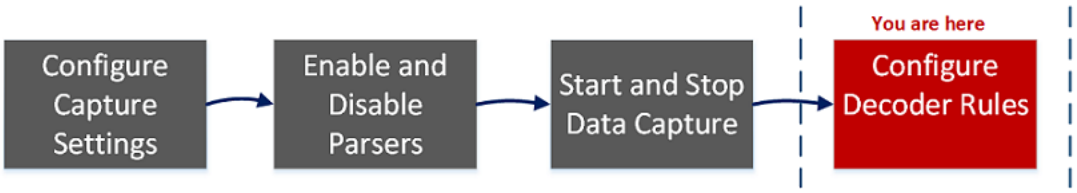
Para acceder al cuadro de diálogo Editor de mapeos de analizadores, en la vista Configuración de Servicios de un Log Decoder, seleccione la pestaña Mapeos de analizador.

Vista Configuración de servicios: pestañas Reglas

Las pestañas Reglas de la vista Configuración de servicios (**ADMINISTRAR > Servicios >** seleccione un servicio y haga clic en **> Ver > Configuración**) permiten definir y administrar las reglas de captura. Cada tipo de regla tiene una cuadrícula con columnas levemente diferentes y distintos parámetros en el cuadro de diálogo Editor de regla. Las reglas de aplicación y correlación se aplican a los Decoders y los Log Decoders. Las reglas de red se aplican solamente a Network Decoders.

Flujo de trabajo

En la siguiente figura se muestra el flujo de trabajo de las tareas de configuración comunes del Decoder y se resaltan los pasos que puede realizar en esta vista.



¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Administrador	configurar ajustes de captura	Configurar ajustes de captura
Administrador	administrar analizadores y analizadores de registros	Habilitar y deshabilitar analizadores y analizadores de registros
Administrador	iniciar y detener la captura de datos	Iniciar y detener la captura de datos
Administrador	configurar reglas*	Configurar reglas de Decoder
Administrador	importar, exportar o migrar una regla*	Configurar reglas de Decoder
Administrador	habilitar o deshabilitar una regla*	Configurar reglas de Decoder
Administrador	agregar, editar o eliminar una regla*	Configurar reglas de Decoder

*Puede realizar estas tareas aquí.

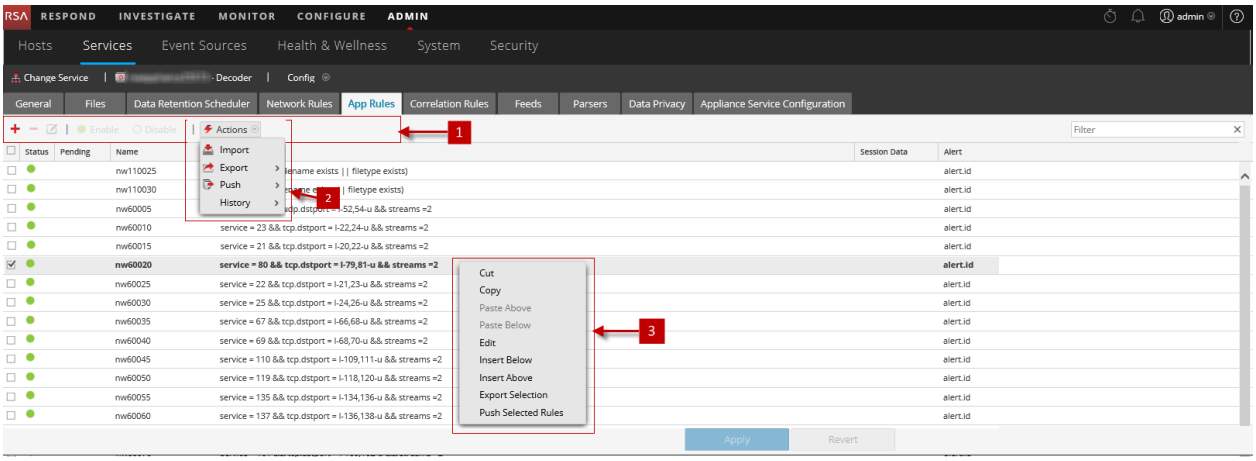
Temas relacionados

- Configurar ajustes comunes en un Decoder
- Configuración rápida de Decoder y Log Decoder
- Pestaña Reglas de aplicación

- Pestaña Reglas de correlación
- Pestaña Reglas de red

Vista rápida

Este es un ejemplo de la pestaña Reglas de aplicación.



1 Barra de herramientas de la pestaña Reglas: Proporciona opciones para trabajar con reglas en la cuadrícula.
2 Menú Acciones de reglas: Proporciona opciones para administrar conjuntos de reglas.
3 Acciones del menú contextual de la lista Reglas: Muestra el menú contextual de lista Reglas.

Barra de herramientas de la pestaña Reglas

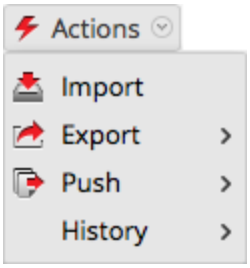
La barra de herramientas es la misma para todas las instancias de la vista Configuración > pestañas Reglas.

Función	Descripción
Acciones	Muestra el menú **Acciones**.
+	Agrega una nueva regla a un servicio.
−	Elimina una regla de un servicio.
	Permite modificar reglas.
Disable	Desactiva una regla (sin eliminarla).
Enable	Habilita (vuelve a activar) una regla.

Función	Descripción
Filtrar	El campo de entrada para una cadena de búsqueda. NetWitness Platform filtra las reglas dinámicamente a medida que escribe una cadena de búsqueda. Si hace clic en **x**, el campo de entrada se borra y se restaura la vista sin filtros.
Aplicar	Guarda los cambios realizados en las reglas y aplica las reglas configuradas a un servicio. Hasta antes de aplicar los cambios, es posible volver a cargar las reglas como estaban antes de las modificaciones actuales.
Revertir	Descarta los cambios no guardados en la cuadrícula y revierte a las reglas sin editar.

Menú Acciones de reglas

El menú Acciones tiene opciones que ayudan a administrar conjuntos de reglas.



Opción	Descripción
Importar	Importa un conjunto de reglas a la interfaz del usuario para que se pueda aplicar a un servicio. Puede editar las reglas antes de aplicarlas.
Exportar	Guarda las reglas seleccionadas o todas las reglas en un archivo .nwr en la máquina cliente.

Migración	Permite aplicar las reglas a otros servicios (Decoders o Log Decoders) o a Decoders que pertenecen a un grupo de servicios. En la migración, las reglas se pueden fusionar (actualizar las reglas existentes y anexar las nuevas) o se pueden reemplazar.
	• **Migración > Todo.** Migra todas las reglas a otros servicios. Todas las reglas de los servicios de destino se quitan y se reemplazan por todas las reglas del servicio de origen.
	• **Migración > Selección.** Migra las reglas seleccionadas a otros servicios. Tiene dos opciones:
	  • **Reemplazo.** Elimina todas las reglas de los servicios objetivo y las reemplaza por las reglas seleccionadas en el servicio de origen.
	  • **Combinar.** Combina las reglas seleccionadas con las reglas existentes en los servicios de destino

Historial	Muestra las últimas diez instantáneas de reglas aplicadas mediante NetWitness Platform. Puede seleccionar y aplicar (restaurar) una instantánea en el Decoder en cualquier momento.

Acciones del menú contextual de la lista Reglas

Dentro de una cuadrícula de reglas, haga clic con el botón secundario en una fila para mostrar el menú contextual de la cuadrícula Reglas.

Opción	Descripción
Cortar	Elimina la regla actual.
Copiar	Copia la regla actual.
Pegar arriba	Pega la regla copiada encima de la regla actual.
Pegar abajo	Pega la regla copiada debajo de la regla actual.
Editar	Edita la regla actual.
Insertar debajo	Inserta las reglas importadas debajo de la regla actual.
Insertar arriba	Inserta las reglas importadas encima de la regla actual.
Exportar selección	Exporta las reglas seleccionadas.
Migración de reglas seleccionadas	Migra las reglas seleccionadas a otros servicios.

Pestaña Reglas de aplicación

La pestaña Reglas de aplicación (**ADMINISTRAR > Servicios >** seleccione un Decoder o un Log Decoder y haga clic en **> Ver > Configuración > pestaña Reglas de aplicación**) permite administrar las reglas de aplicación. NetWitness Platform aplica reglas de aplicación en el nivel de sesión.

¿Qué desea hacer?

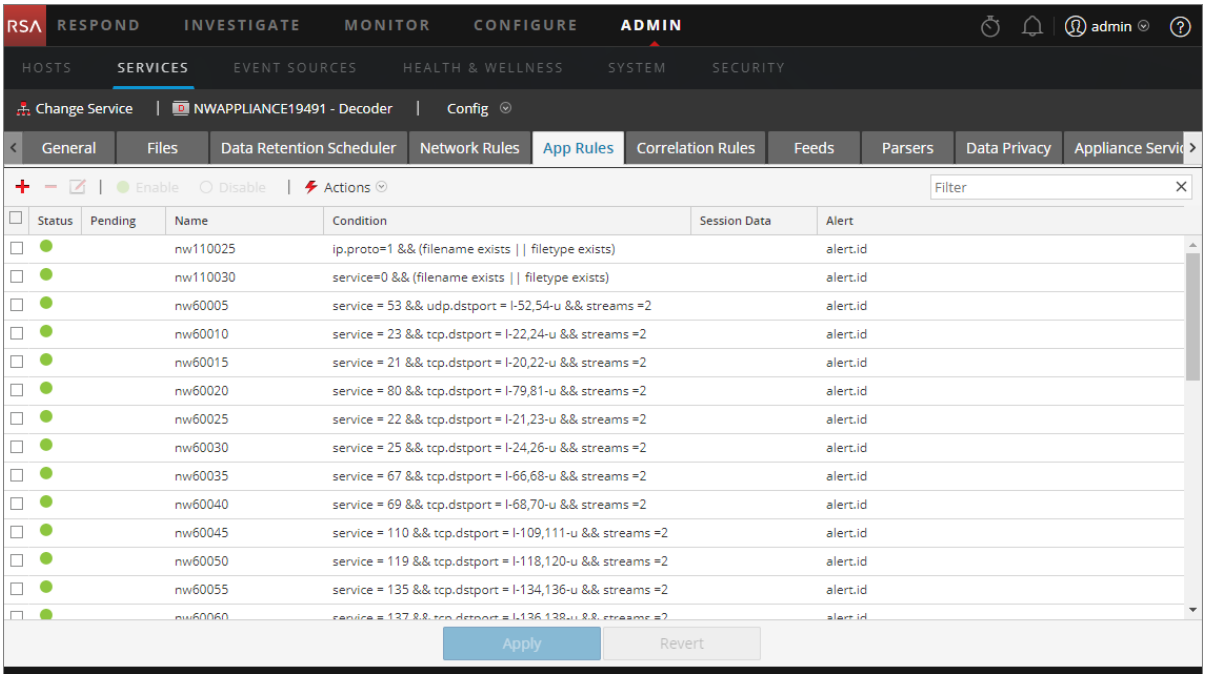
Función de usuario	Deseo…	Documentación
Administrador	agregar o editar reglas de aplicación	Configurar reglas de aplicaciones

Temas relacionados

- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder
- Configurar reglas de Decoder
- Vista Configuración de servicios: pestañas Reglas

Vista rápida

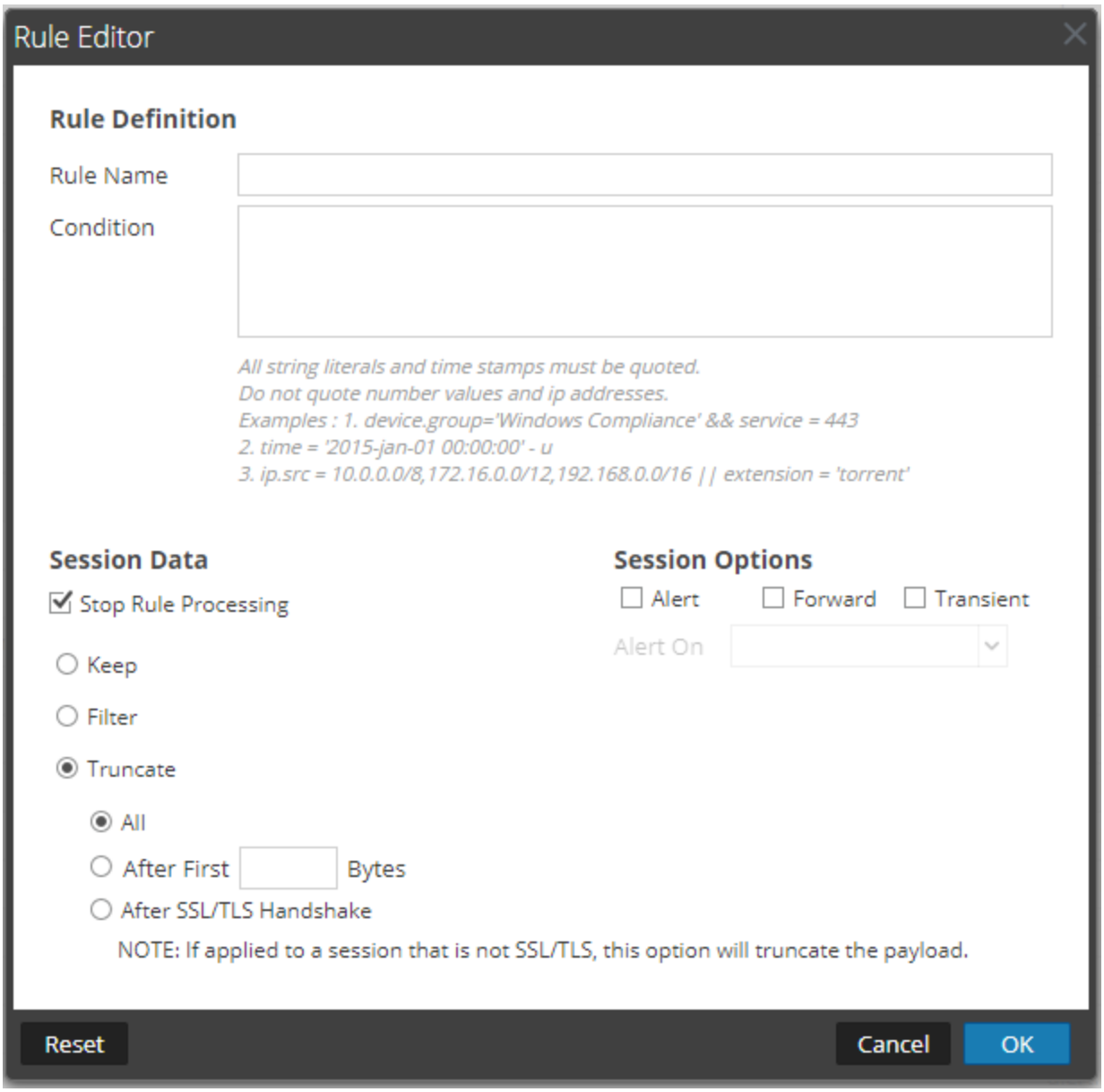
En la siguiente figura se muestra una pestaña Reglas de aplicación y la tabla describe las columnas.



Columna	Descripción
Pendiente	Esta columna indica si una regla tiene cambios pendientes. Las reglas que están actualmente activas en el Decoder no tienen indicador. Si la regla es nueva o se modificó, la columna contiene . Una vez que se aplican las reglas, el indicador de pendiente se elimina.
Nombre	Este el nombre de la regla, un identificador descriptivo de la regla.
Condición	Esta es la definición de la condición que activa una acción cuando hay coincidencia con ella.
Datos de sesión	Esta columna muestra la medida de los Datos de sesión que se implementa cuando un paquete coincide con la regla. Los posibles valores son **Filtro**, **Mantener** o **Truncar**.
Alerta	Esta columna muestra el nombre de la alerta personalizada que el Decoder genera cuando los metadatos coinciden con la regla.
Estado	Esta columna indica si la regla está habilitada o deshabilitada con un icono de círculo. Si el interior del círculo es verde, la regla está activada. Si el círculo está vacío, la regla está deshabilitada.

Cuadro de diálogo Editor de regla

En la siguiente figura se muestra el cuadro de diálogo Editor de regla para una regla de aplicación.



El cuadro de diálogo Editor de regla proporciona las opciones y los campos necesarios para definir una regla de aplicación.

Campo	Descripción
Nombre de la regla	El nombre descriptivo que identifica a la regla.

Campo	Descripción
Condición	La definición de la condición que activa una acción cuando se coincide con ella. Puede escribir directamente en el campo o crear la condición en este campo utilizando metadatos de las acciones en la ventana de IntelliSense. A medida que crea la definición de la regla, Intellisense muestra los errores y las advertencias de la sintaxis. Todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. Configurar reglas de Decoder se proporcionan detalles adicionales.

En la siguiente tabla se describen las acciones y las opciones de Datos de sesión.

Acción	Descripción
Detener procesamiento de regla	Si está seleccionada, la evaluación adicional de la regla termina si hay una coincidencia con la regla y la sesión se guarda según la acción de la sesión. Si no se verifica, la evaluación de la regla continúa hasta que se evalúen todas las reglas.
Conservar	La carga útil del paquete y los metadatos asociados se guardan cuando coinciden con la regla.
Filtro	El paquete no se guarda cuando coincide con la regla.
Truncar	**Truncar todo**: Trunca todos los bytes de la carga útil de la sesión. La carga útil del paquete no se guarda cuando coincide con la regla, pero los encabezados del paquete y los metadatos asociados se conservan. Esta es la opción de truncamiento predeterminada. **Truncar después de los primeros <n> bytes**: Trunca los bytes de la carga útil de la sesión después de los primeros <n> bytes especificados, donde <n> es un entero. La carga útil del paquete no se guarda después de <n> bytes cuando coincide con la regla, pero los encabezados del paquete y los metadatos asociados se conservan. **Truncar después del protocolo de enlace SSL/TLS**: Trunca la carga útil de todas las sesiones, excepto en el caso de una sesión SSL/TLS, donde el intercambio de SSL se conserva, pero el resto de la carga útil no se guarda. Esta opción se usa con los analizadores SSL.
Alerta y **Alerta en**	Si **Alerta** está seleccionado, el paquete genera una alerta personalizada cuando los metadatos coinciden con la regla. Puede seleccionar el nombre de la alerta en el campo **Alerta en**.
Adelante	Habilita la ejecución del reenvío de syslog cuando el registro coincide con la regla.
Transitorio	Impide que los metadatos de alerta que se crean se escriban en disco.

En la siguiente tabla se describen las acciones del cuadro de diálogo Editor de regla.

Acción	Descripción
Restablecer	Restablece los contenidos del cuadro de diálogo a los valores previos a la edición; los cambios se anulan.

Acción	Descripción
Cancelar	Cancela las ediciones y cierra el cuadro de diálogo Editor de regla.
Aceptar	Guarda la regla nueva o editada y la agrega a la cuadrícula de reglas. El cuadro de diálogo Editor de regla se cierra.
Guardar	(Solo reglas con sintaxis obsoleta) Aplica una regla corregida individualmente al servicio Decoder. Consulte Corregir las reglas con sintaxis no válida.

Pestaña Reglas de correlación

La pestaña Reglas de correlación (**ADMINISTRAR > Servicios >** seleccione un servicio y haga clic en **> Ver > Configuración > pestaña Reglas de correlación**) permite administrar las reglas de correlación. Las reglas de correlación básicas se aplican en el nivel de sesión y advierten al usuario sobre actividades específicas que pueden estar ocurriendo en su ambiente. NetWitness Platform aplica las reglas de correlación en una ventana de tiempo móvil configurable.

¿Qué desea hacer?

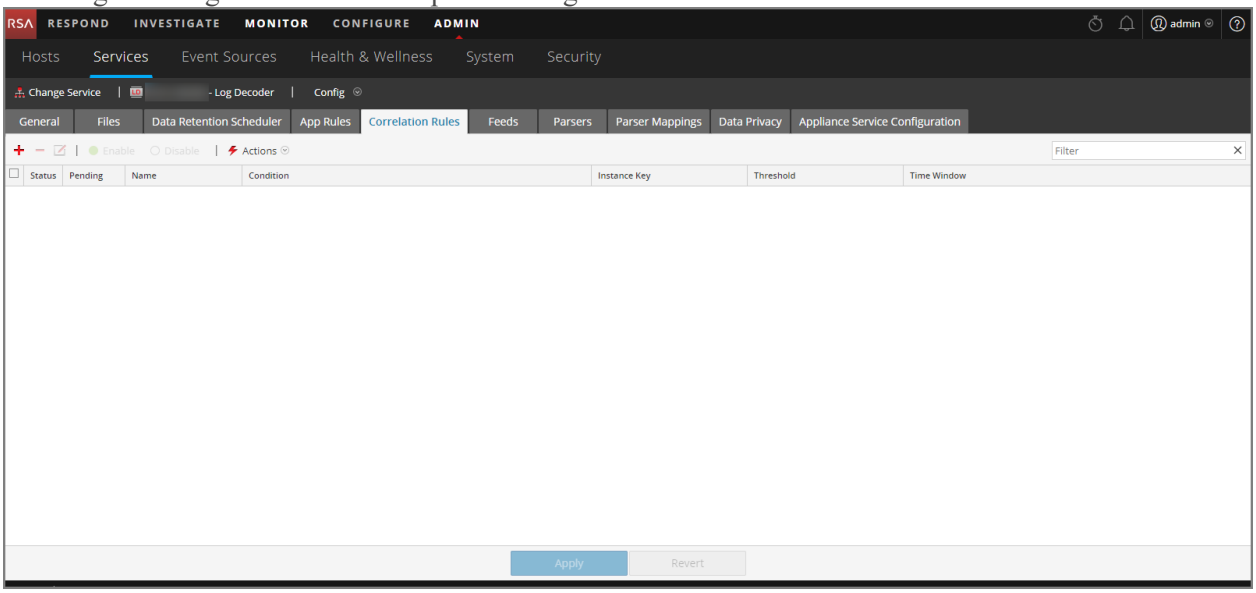
Función de usuario	Deseo…	Documentación
Administrador	agregar o editar una regla de correlación	Configurar reglas de correlación

Temas relacionados

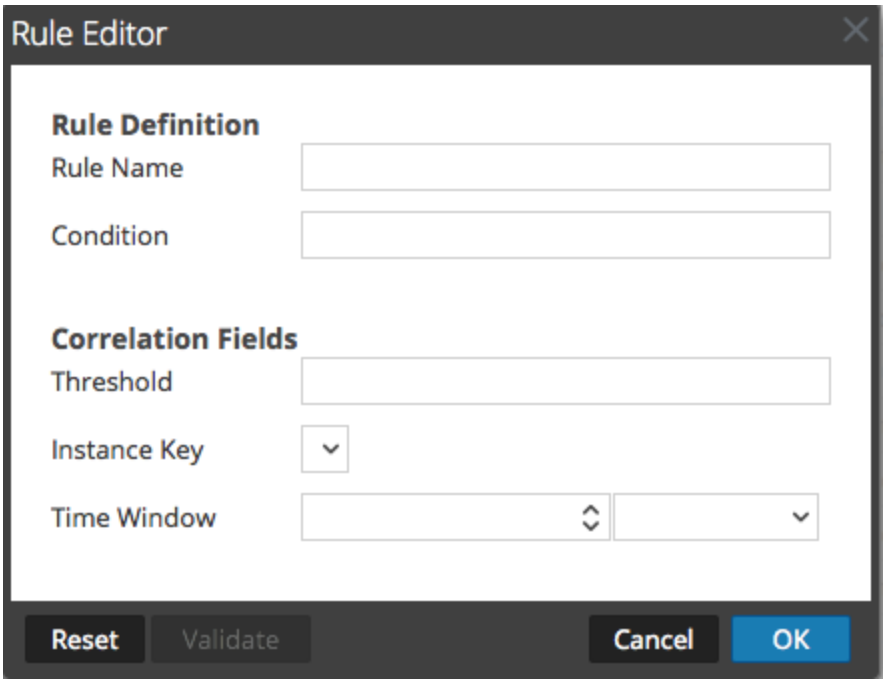
- Configurar ajustes comunes en un Decoder
- Configuración rápida de Decoder y Log Decoder
- Configurar reglas de Decoder
- Vista Configuración de servicios: pestañas Reglas

Vista rápida

En la siguiente figura se muestra la pestaña Reglas de correlación.



En la siguiente figura se muestra el cuadro de diálogo Editor de regla para una regla de correlación.



En la siguiente tabla se describen las columnas de la pestaña Reglas de correlación.

Columna	Descripción
Pendiente	Esta columna indica si una regla tiene cambios pendientes. Las reglas que están actualmente activas en el Decoder no tienen indicador. Si la regla es nueva o se modificó, la columna contiene . Una vez que se aplican las reglas, el indicador de pendiente se elimina.
Nombre	Este el nombre descriptivo de la regla.
Condición	Esta es la definición de la condición que activa una acción cuando hay coincidencia con ella. En las condiciones, todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. En Configurar reglas de Decoder se proporcionan detalles adicionales.
Clave de instancia	Este es el indicador de destino en el que se basa el evento. Puede ser una única clave primaria, como ip.src o una clave primaria compuesta, como ip.src,ip.dst.

Columna	Descripción
Umbral	Es la cantidad mínima de apariciones necesarias para activar una sesión de correlación y puede incluir una clave asociada que identifique el tipo de metadatos que se están contando para determinar si se cumple la condición. El motor de correlación no puede usar IPv4 o IPv6 comoun tipo de metadatos asociado. Use uno de los tres argumentos siguientes: • `u_count(associated_key)` = el conteo de valores únicos de la clave especificada. Se requiere una clave. • `sum(associated_key)` = los valores de la clave especificada. Se requiere una clave. • `count()` = cantidad de sesiones, no se usa una clave asociada. Si se incluye, se omite.
Ventana de tiempo	Es la duración en horas, minutos o segundos dentro de la cual se debe alcanzar el umbral para que se active una sesión de correlación.
Estado	Esta columna indica si la regla está habilitada o deshabilitada con un icono de círculo. Si el interior del círculo es verde, la regla está activada. Si el círculo está vacío, la regla está deshabilitada.

El cuadro de diálogo **Editor de regla** proporciona las opciones y los campos necesarios para definir una regla de red. Los campos corresponden exactamente a las columnas de la cuadrícula.

Acción	Descripción
Restablecer	Restablece los contenidos del cuadro de diálogo a los valores previos a la edición; los cambios se anulan.
Cancelar	Cancela las ediciones y cierra el cuadro de diálogo Editor de regla.
Aceptar	Guarda la regla nueva o editada y la agrega a la cuadrícula de reglas. El cuadro de diálogo Editor de regla se cierra.
Guardar	(Solo reglas con sintaxis obsoleta) Aplica una regla corregida individualmente al servicio Decoder. Consulte Corregir las reglas con sintaxis no válida.

Pestaña Reglas de red

La pestaña Reglas de red (**ADMINISTRAR > Servicios >** seleccione un Decoder y haga clic en **> Ver > Configuración > pestaña Reglas de red**) permite administrar las reglas de red. NetWitness Platform aplica reglas de red en el nivel de paquete. Las reglas de red constan de conjuntos de reglas de capa 2, capa 3 y capa 4. Es posible aplicar varias reglas al Decoder. Las reglas se pueden aplicar a varias capas (por ejemplo, cuando una regla de red filtra puertos específicos para una dirección IP específica). Las reglas de red se aplican solo a Network Decoders.

¿Qué desea hacer?

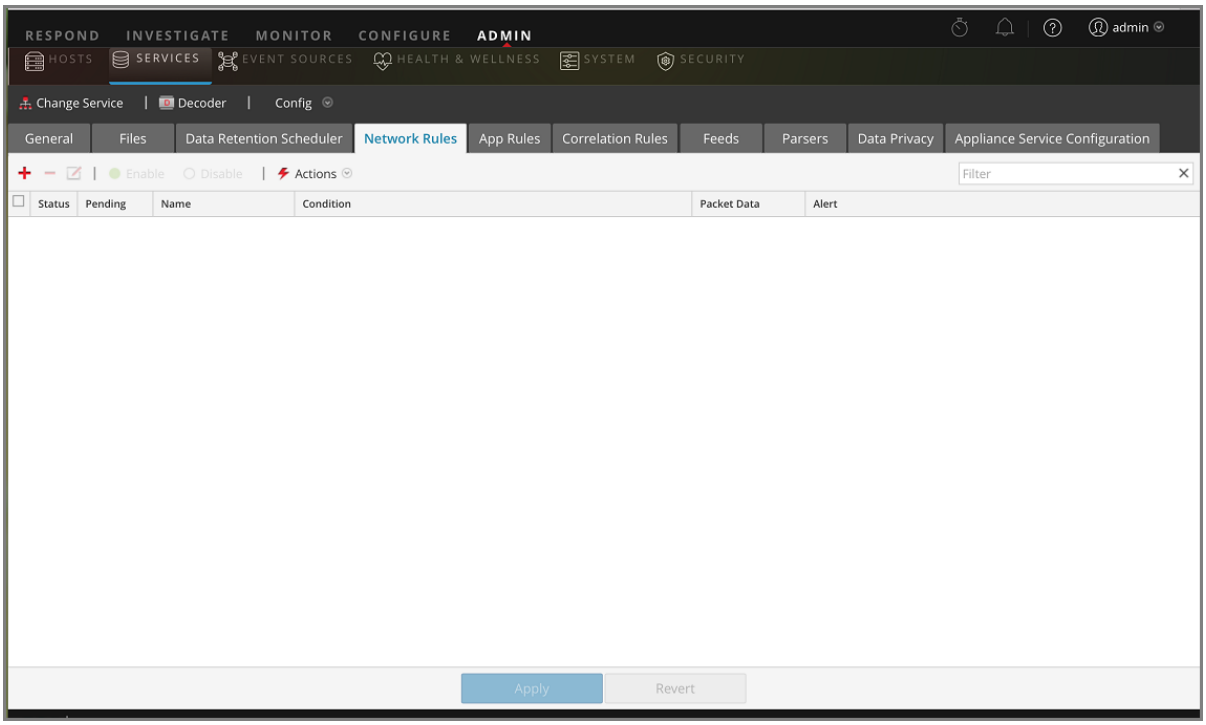
Función de usuario	Deseo…	Documentación
Administrador	agregar, editar o corregir reglas de red	Configurar reglas de red

Temas relacionados

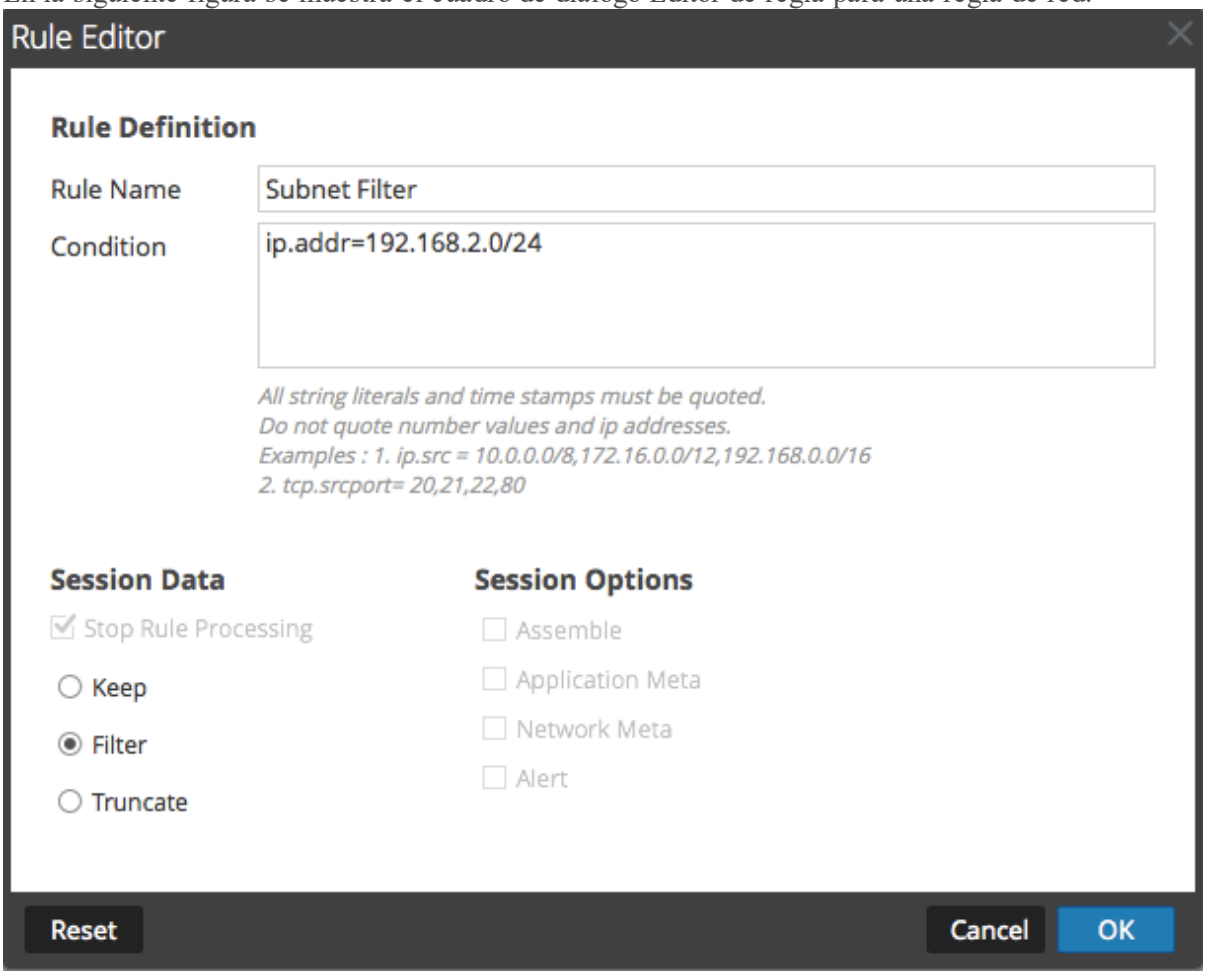
- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder
- Configurar reglas de Decoder
- Vista Configuración de servicios: pestañas Reglas

Vista rápida

En la siguiente figura se muestra la pestaña Reglas de red.



En la siguiente figura se muestra el cuadro de diálogo Editor de regla para una regla de red.



En la siguiente tabla se describen las columnas de la cuadrícula Reglas de red.

Columna	Descripción
Pendiente	Esta columna indica si una regla tiene cambios pendientes. Las reglas que están actualmente activas en el Decoder no tienen indicador. Si la regla es nueva o se ha modificado, la columna contiene . Una vez que se aplican las reglas, el indicador de pendiente se quita.
Nombre	Este el nombre de la regla, un identificador descriptivo de la regla.
Condición	Esta es la definición de la condición que activa una acción cuando hay coincidencia con ella.
Datos de paquete	Esta columna muestra la medida de los Datos de sesión que se implementa cuando un paquete coincide con la regla. Los posibles valores son **Filtro**, **Mantener** o **Truncar**.
Alerta	Esta columna indica si el Decoder genera una alerta personalizada cuando los metadatos coinciden con la regla. Los valores posibles son **Habilitado** o **Deshabilitado**.
Estado	Esta columna indica si la regla está habilitada o deshabilitada con un icono de círculo. Si el interior del círculo es verde, la regla está activada. Si el círculo está vacío, la regla está deshabilitada.

El cuadro de diálogo **Editor de regla** proporciona las opciones y los campos necesarios para definir una regla de red.

En la siguiente tabla se describen los campos de Definición de regla.

Campo	Descripción
Nombre de la regla	El nombre descriptivo que identifica a la regla.
Condición	La definición de la condición que desencadena una acción cuando hay una coincidencia. Puede escribir directamente en el campo o crear la condición en él mediante metadatos de las acciones de la ventana de Intellisense. A medida que crea la definición de la regla, Intellisense muestra los errores y las advertencias de la sintaxis. En las condiciones, todos los literales de cadena y los registros de fecha y hora deben ir entre comillas. No use comillas para los valores de número ni las direcciones IP. En Configurar reglas de Decoder se proporcionan detalles adicionales. En esta sección también se describen las claves de metadatos que admite NetWitness Platform para uso en las condiciones de reglas de red.

La siguiente tabla describe las acciones de Datos de sesión.

Acción	Descripción
Detener procesamiento de regla	Si está seleccionada, la evaluación adicional de la regla termina si hay una coincidencia con la regla y la sesión se guarda según lo indicado. Si no se verifica, la evaluación de la regla continúa hasta que se evalúen todas las reglas.

Acción	Descripción
Conservar	La carga útil del paquete y los metadatos asociados se guardan cuando coinciden con la regla.
Filtro	El paquete no se guarda cuando coincide con la regla.
Truncar	La carga útil del paquete no se guarda cuando coincide con la regla, pero los encabezados del paquete y los metadatos asociados se mantienen.

En la siguiente tabla se describen las opciones de una sesión.

Acción	Descripción
Ensamblaje	Si la opción está seleccionada, el ensamblador ensambla la cadena de paquetes cuando coincide con la regla.
Metadatos de red	El paquete genera metadatos de red cuando coincide con la regla.
Metadatos de aplicación	El paquete genera metadatos de aplicación cuando coincide con la regla.
Alerta	El paquete genera una alerta personalizada cuando los metadatos coinciden con la regla.

En la siguiente tabla se describen las acciones del cuadro de diálogo Editor de regla.

Acción	Descripción
Restablecer	Restablece los contenidos del cuadro de diálogo a los valores previos a la edición; los cambios se anulan.
Cancelar	Cancela las ediciones y cierra el cuadro de diálogo Editor de regla.
Aceptar	Guarda la regla nueva o editada y la agrega a la cuadrícula de reglas. El cuadro de diálogo Editor de regla se cierra.
Guardar	(Solo reglas con sintaxis obsoleta) Aplica una regla corregida individualmente al servicio Decoder. Consulte Corregir las reglas con sintaxis no válida.

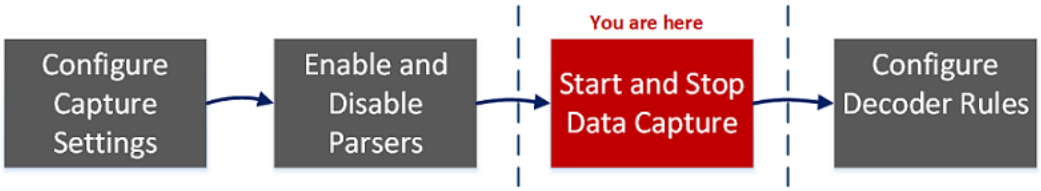
Vista Sistema de servicios: Decoders

Un Log Decoder es un tipo especial de Decoder y se configura y administra de manera similar a un Decoder. Por lo tanto, la mayor parte de la información en esta sección se refiere a ambos tipos de Decoders. Se especifican las diferencias para los Log Decoders.

Para acceder a la vista Sistema de servicios, vaya a **ADMINISTRAR > Servicios >** seleccione un Decoder o un Log Decoder > > **Ver** > **Sistema**.

Flujo de trabajo

En la siguiente figura se muestra el flujo de trabajo de las tareas de configuración comunes del Decoder y se resaltan los pasos que puede realizar en esta vista.



¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Administrador	configurar ajustes de captura	Configurar ajustes de captura
Administrador	administrar analizadores y analizadores de registros	Habilitar y deshabilitar analizadores y analizadores de registros
Administrador	iniciar y detener la captura de datos*	Iniciar y detener la captura de datos
Administrador	cargar captura de paquete y archivos de registro*	Cargar un archivo de registro en un Log Decoder Cargar un archivo de captura de paquete
Administrador	restablecer estadísticas de registros, realizar tareas de host, apagar el servicio, apagar el servicio del dispositivo y reiniciar el host*	*Guía de introducción de hosts y servicios*
Administrador	configurar reglas	Configurar reglas de Decoder

*Puede realizar estas tareas aquí.

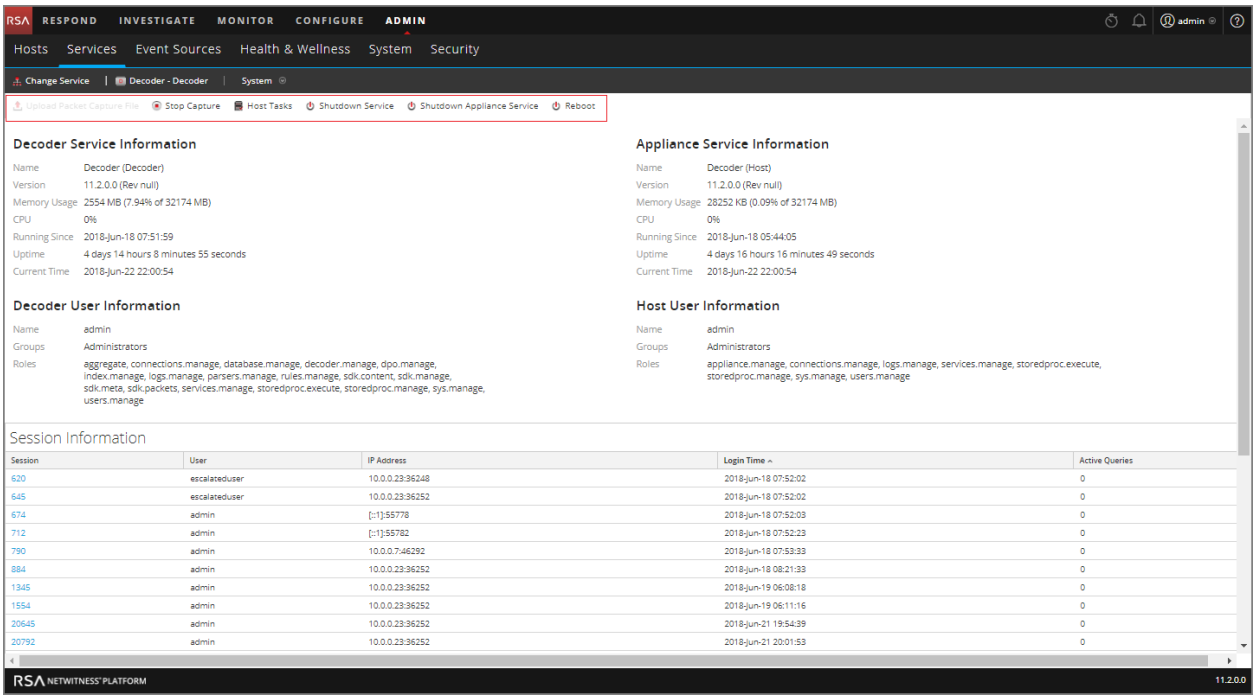
Temas relacionados

Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

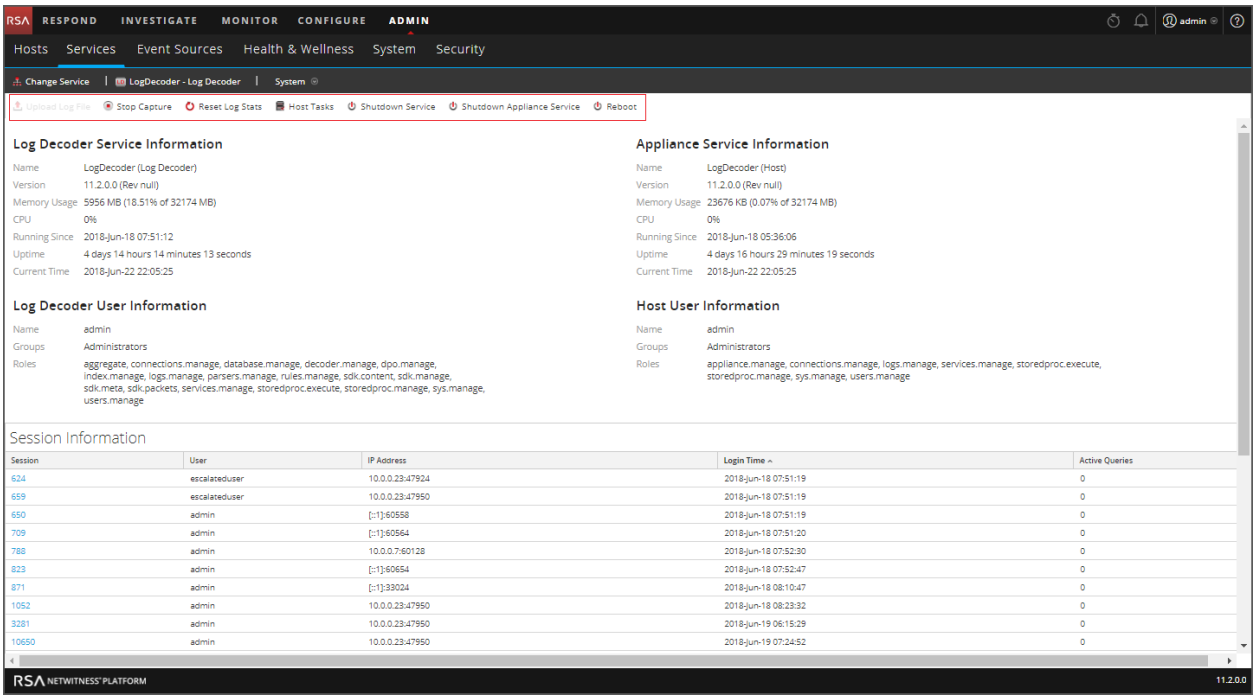
- Configuración rápida de Decoder y Log Decoder
- Configurar ajustes comunes en un Decoder
- "Vista Sistema de servicios" en la *Guía de introducción de hosts y servicios*

Vista rápida

Este es un ejemplo de la vista Sistema de servicios de un Decoder.

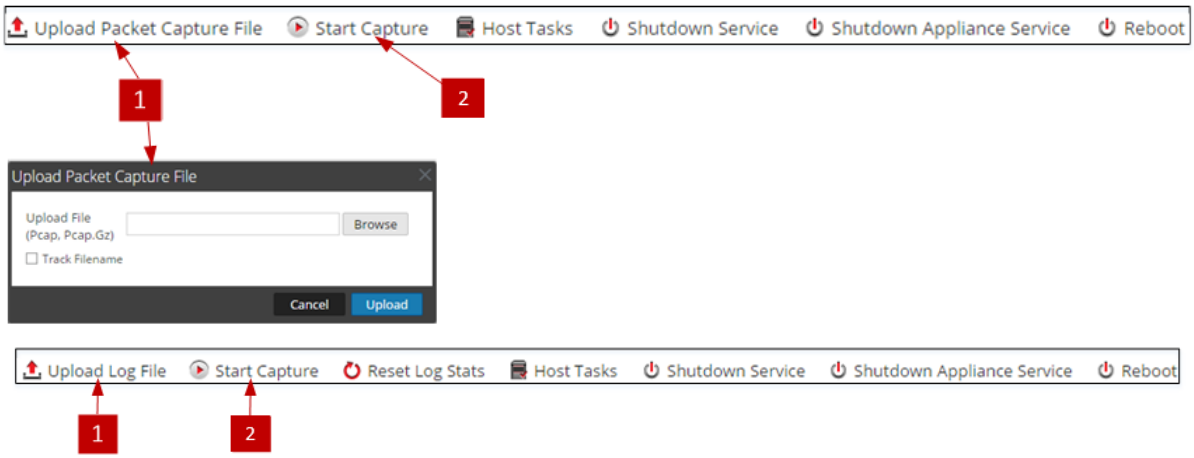


Este es un ejemplo de la vista Sistema de servicios de un Log Decoder.



Barra de herramientas de Información del servicio

Estas dos barras de herramientas ilustran las opciones específicas de los Decoders y Log Decoders.



Además de las opciones comunes de la barra de herramientas de la vista Sistema de servicios, puede iniciar y detener la captura de paquetes o registros. Las opciones para cargar archivos son distintas en los Decoder estándar (archivo de captura de paquetes) y el Log Decoder (archivo de registro).

Acción	Descripción
Cargar archivo de captura de paquete	Muestra un cuadro de diálogo que proporciona una manera de seleccionar un archivo de captura de paquete (.pcap) para cargar en el Decoder seleccionado. Para obtener más información, consulte Cargar un archivo de captura de paquete. **Nota:** Esta opción no se aplica a los Log Decoders.

Acción	Descripción
Cargar archivo de log	Muestra un cuadro de diálogo que proporciona una manera de seleccionar un archivo de registro (.log) para cargar en el Log Decoder seleccionado. Para obtener más información, consulte Cargar un archivo de registro en un Log Decoder.
Iniciar/Detener captura	Inicia la captura de un paquete en el Decoder seleccionado. Cuando la captura de un paquete está en progreso, la opción en la barra de herramientas cambia a Detener captura y la opción para cargar un archivo no está disponible.