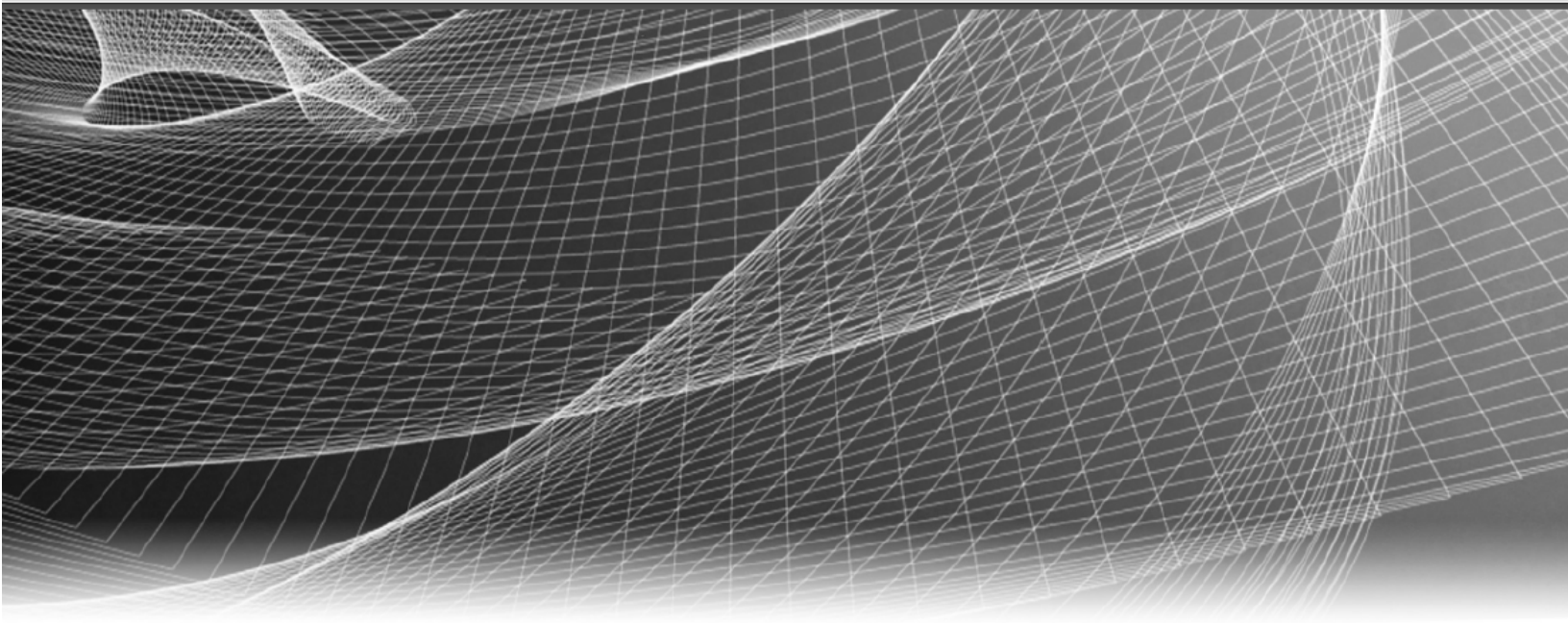


RSA Security Analytics

# Decoder y Log Decoder
# Guía de configuración

para la versión 10.6

RSA EMC²

## Marcas comerciales



## Acuerdo de licencia



## Licencias de otros fabricantes



## Nota sobre tecnologías de cifrado



## Distribución

# Contenido

# Guía de configuración de Decoder y Log Decoder

En este tema se presenta el Decoder y el Log Decoder y la metodología para configurarlos en Security Analytics.

**Temas**

# Aspectos básicos de Decoder y Log Decoder

En este tema se presenta el Decoder y el Log Decoder en RSA Security Analytics.

Security Analytics es compatible con dos tipos de Decoders:

- El Decoder, que captura datos de red en forma de paquetes.
- El Log Decoder, que captura datos de registro como eventos.

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.

La adición de un Decoder lo hace visible y lo pone a disposición para su uso con Security Analytics Administration, Live e Investigation. Para agregar un servicio en Security Analytics, puede seleccionar el tipo de servicio, proporcionar información de conexión del servicio y validar que se pueda acceder al servicio.

La configuración del Decoder para capturar datos implica seleccionar un adaptador de captura y elegir configuraciones de caché y captura.

Cuando el Decoder esté disponible en Security Analytics, se encontrará listo para capturar tráfico. Puede configurar cada Decoder para controlar el tipo de tráfico capturado mediante el uso de reglas, feeds y analizadores.

# Procedimientos requeridos

Estos son los pasos de configuración necesarios para un Decoder o Log Decoder nuevos, así como para cambiar la configuración de un Decoder existente. A menos que se indique lo contrario, Decoder se refiere a Packet/Log Decoders. Realice los pasos de la sección en la secuencia que se muestran.

## Paso 1: Verificar la configuración del sistema

El primer paso que se debe realizar cuando se agrega un nuevo servicio a Security Analytics es la verificación de la configuración del sistema.

Ciertos valores predeterminados para los parámetros de configuración del sistema ya están en vigor. Estos valores se pueden editar y ajustar para lograr un rendimiento óptimo.

## Paso 2: Configurar ajustes de captura

A continuación, puede configurar el adaptador para la captura de datos, activar el inicio automático de la captura de datos, seleccionar los analizadores que se aplican a los datos capturados y ajustar la captura de datos mediante la configuración de ajustes de captura.

## Paso 3: Habilitar o inhabilitar analizadores

Vea los analizadores que se descargaron y se implementaron desde Live y administre los que están habilitados o inhabilitados.

## Paso 4: 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. 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.

De manera predeterminada, no hay reglas definidas cuando instala Security Analytics 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 capa de red, Reglas de capa de aplicación y Reglas de correlación.

## Paso 5: 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 activado. Si el inicio automático no está activado, puede iniciar y detener la captura de datos de forma manual.

**Temas**

## Paso 1. Verificar la configuración del sistema

En este tema se proporciona un procedimiento para verificar la configuración del sistema de un Decoder o un Log Decoder.

Cuando un servicio se agrega por primera vez a Security Analytics, se aplican los valores predeterminados para los parámetros de configuración del sistema. Puede editar estos valores para ajustar el rendimiento.

System Configuration

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

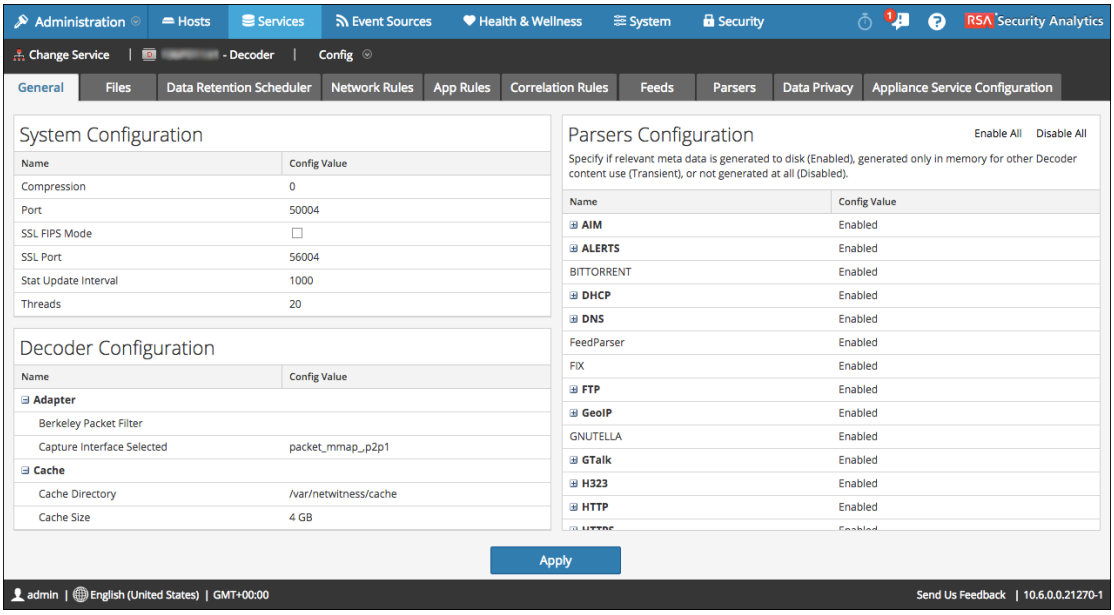
En la mayoría de los casos, los valores predeterminados para la compresión, el intervalo de actualización de estadísticas y la cantidad de hilos de ejecución en el pool se definen en un buen punto para obtener un rendimiento óptimo del sistema. Un parámetro que posiblemente desee cambiar para su ambiente 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.

### Procedimiento

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

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione un servicio Decoder o Log Decoder y elija  **> Ver > Configuración**.
   Se muestra la vista Configuración de servicios para el servicio con la pestaña General

abierta.




3. En **Configuración del sistema**, haga clic en un campo que desee editar y escriba un nuevo valor.
4. Cuando haya terminado de editar, haga clic en **Aplicar**.

## Paso 2. Configurar ajustes de captura

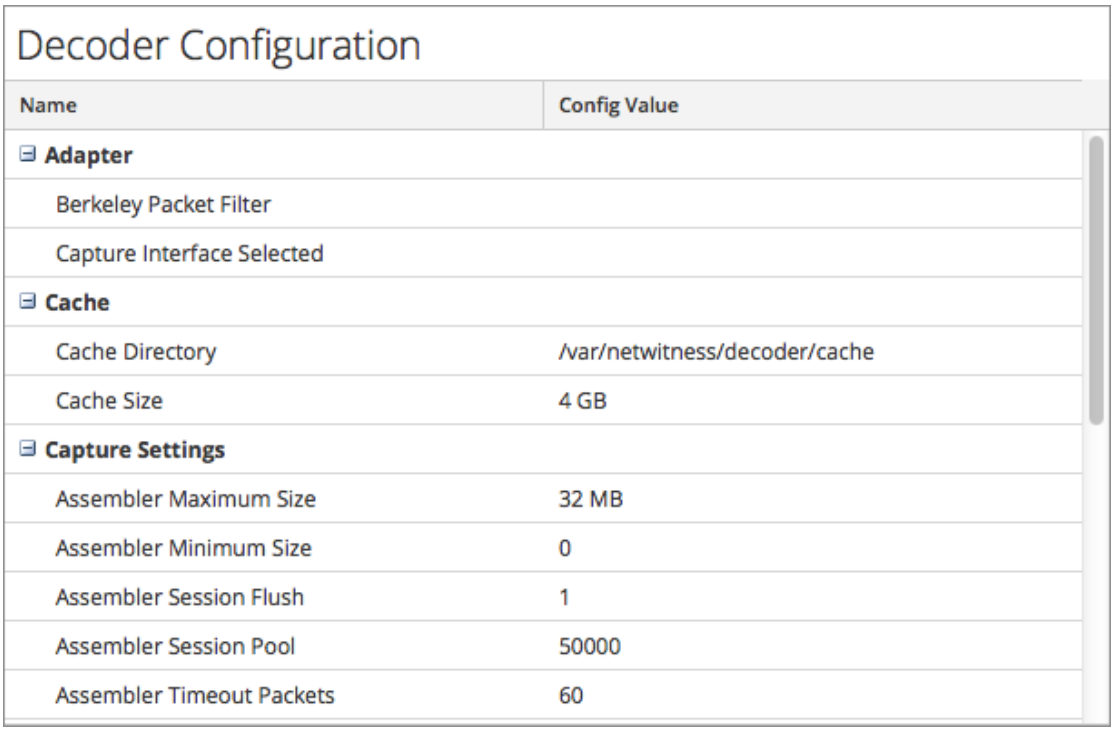
En este tema se proporciona un procedimiento para configurar la captura de datos en Decoders y Log Decoders.

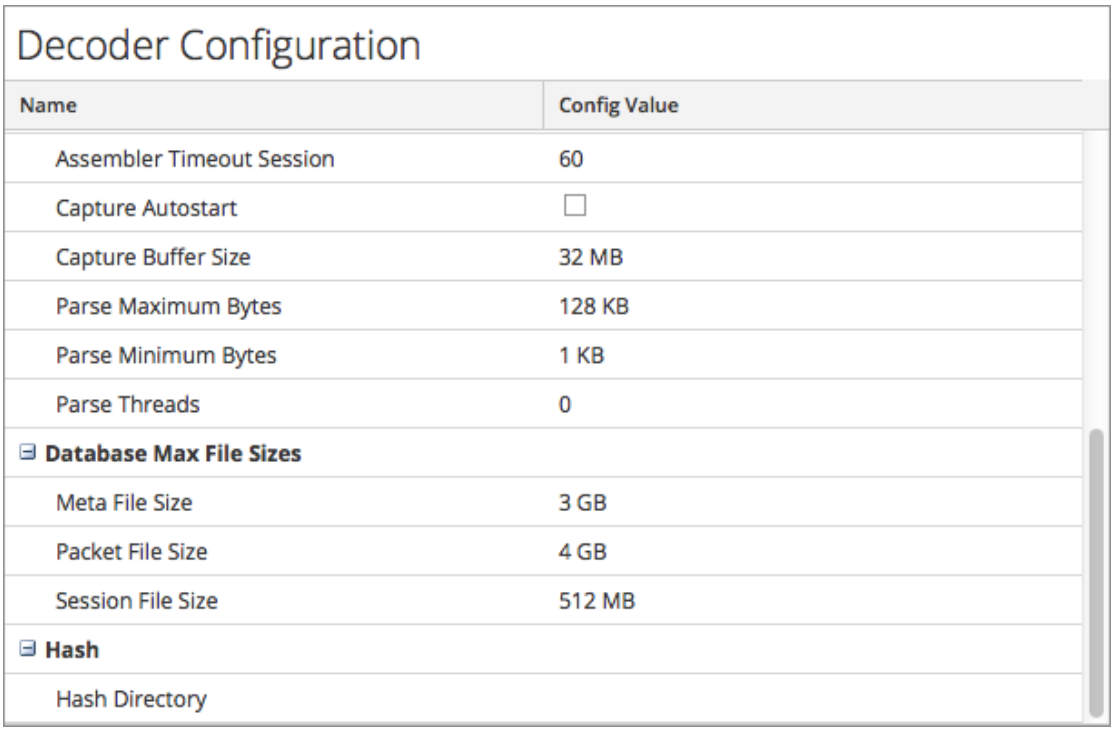
En RSA Security Analytics, puede configurar el adaptador para la captura de datos, habilitar el AutoStart de captura de datos, seleccionar los analizadores que se aplican a los datos capturados y ajustar la captura de datos.

### Procedimiento

Para configurar un Decoder y prepararlo para la captura de datos:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios de Administration**, seleccione el servicio Decoder y elija  **> Ver > Configuración.**
   La vista Configuración de servicios se muestra con la pestaña General abierta y los ajustes de servicio que se usan con más frecuencia para un Decoder o un Log Decoder están disponibles para editarlos en la configuración del Decoder.






3. En la sección **Configuración del adaptador**, configure la interfaz de red para capturar datos.
4. En la sección **Caché**, revise la configuración del directorio y el tamaño de la caché. Si es necesario, modifique estos ajustes.
5. En las secciones **Configuración de captura**, revise los valores predeterminados y modifíquelos si es necesario.
6. Si desea que el Decoder comience a capturar datos automáticamente cuando se inicia, seleccione la casilla de verificación **AutoStart de la captura**.
7. En la sección **Tamaños máximos de archivo de base de datos**, revise los valores predeterminados y modifíquelos si es necesario.
8. En la sección **Hash**, defina un directorio para los archivos hash si está usando esta función.
9. Realice una de las siguientes acciones
   - En el panel **Configuración de analizadores**, revise los analizadores seleccionados para filtrar tráfico y habilítelos, inhabilítelos o márquelos como transitorios según corresponda.
   - Si configura un Log Decoder, revise los analizadores seleccionados para filtrar tráfico en la sección **Configuración de analizadores de servicio** y habilítelos, inhabilítelos o márquelos como transitorios según corresponda.

10. Para guardar los cambios, haga clic en **Aplicar**.
11. Si es necesario para aplicar los cambios, navegue a la vista **Sistema de servicios** y reinicie el servicio.
    En este punto, puede iniciar la captura (también en la vista Sistema de servicios).

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

En este tema, se describe cómo usar los filtros de paquetes Berkeley para controlar los paquetes y registros que se procesan mediante un Decoder.

Puede usar los filtros de paquetes Berkeley para controlar los paquetes y los registros que procesa un Decoder. El Decoder admite el filtrado de paquetes en el nivel del sistema que se define mediante la sintaxis tcpdump/libpcap. La especificación de un filtro libpcap puede reducir de manera eficaz el volumen de paquetes en función de atributos de capa 2 - capa 4. Los filtros de paquetes Berkeley (BPF) se aplican al flujo de paquetes antes de que los paquetes se copien al adaptador de Decoder para su 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).

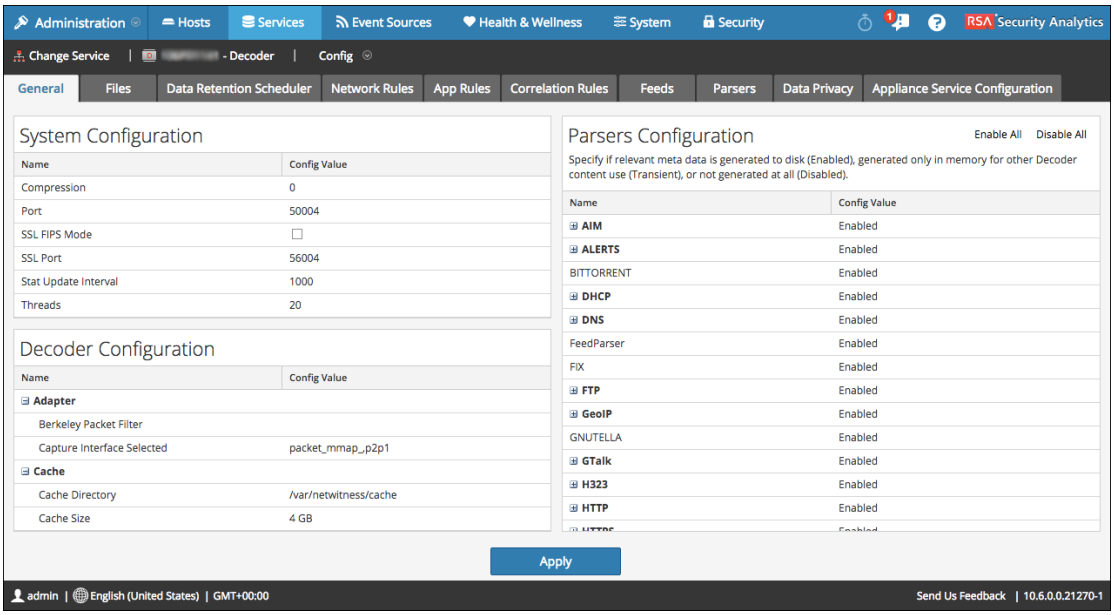
El uso de un filtro libpcap es adecuado cuando un Decoder está recibiendo un volumen de tráfico que impone una carga sobre los recursos físicos de la plataforma. En este escenario, el Decoder puede descartar paquetes constantemente y tener una gran cantidad de páginas de captura disponibles (/decoder/stats/capture.pagefree es alto).

### Agregar filtros de paquetes en el nivel del sistema

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

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. En la vista **Servicios de Administration**, seleccione un servicio Decoder y elija  **> Ver > Configuración.**

   La vista Configuración de servicios se 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**.
   La interfaz del usuario de SA 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.

#### 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.

- **&&** o **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 paquete 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 puerto udp 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)**.

## Paso 3. Habilitar e inhabilitar analizadores de registros

En este tema se indica a los administradores cómo habilitar o deshabilitar analizadores de registros en un Log Decoder.

Este procedimiento es útil para ver qué analizadores de registros se descargaron e implementaron desde Live y cuáles de ellos están habilitados.

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.

### Requisitos previos

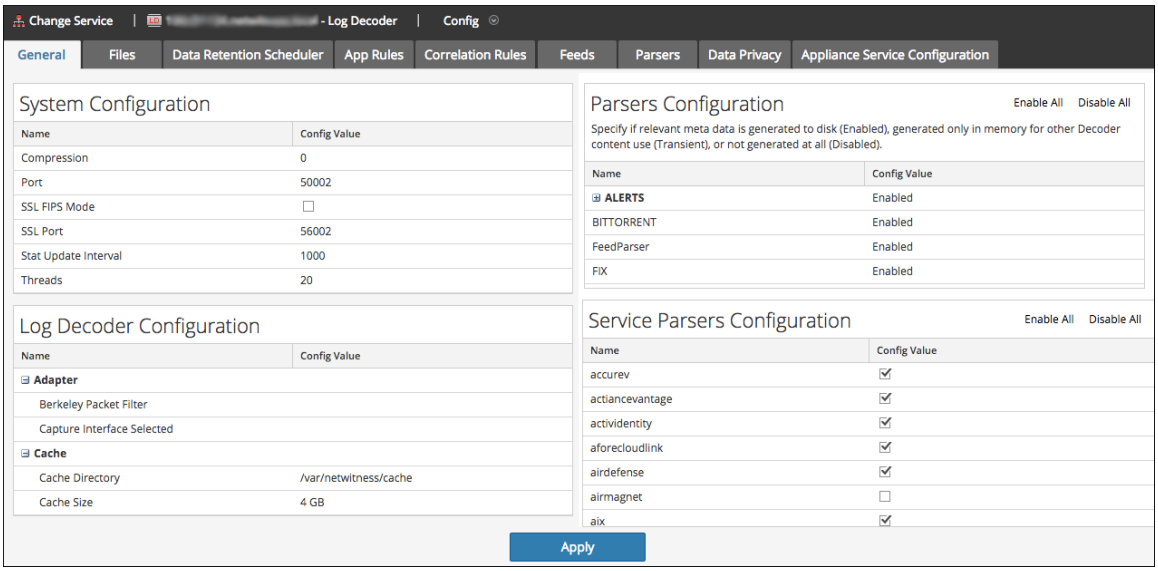
Debe haber implementado analizadores de registros desde Live con anterioridad. Para obtener detalles, consulte el tema **Buscar e implementar recursos de Live** en *Administración de servicios de Live*.

### Procedimiento

Para habilitar o inhabilitar un analizador de orígenes de eventos o para ver el estado de cada analizador:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Servicios**.
2. Seleccione un Log Decoder en la cuadrícula **Servicios** y en el menú **Acciones** (  ), elija **Ver** > **Configurar**.
3. En el panel **Configuración de analizadores de servicio**, busque el origen de eventos.
4. En la columna **Valor de configuración**, observe el estado actual del analizador.
   - Si el analizador ya está seleccionado, significa que está habilitado.
   - Si no lo está, está actualmente inhabilitado.

Puede alternar el valor de cualquier analizador de registros individual. Como alternativa, puede seleccionar **Activar todo** o **Desactivar todo** para actualizar el estado de todos los analizadores de registros simultáneamente.




5. Haga clic en **Aplicar**.

Cuando hace clic en **Aplicar**, todos los analizadores se vuelven a cargar en Security Analytics.

## Resultado

El estado de cada analizador de registros se actualiza de acuerdo con lo que se selecciona.

## Paso 4. 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.

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.

Guía de reglas y consultas proporciona una guía que deben seguir todas las consultas y las condiciones de regla en los servicios de Security Analytics Core.

De manera predeterminada, no hay reglas definidas cuando instala Security Analytics 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 capa de red, Reglas de capa de aplicación y Reglas de correlación.

### Reglas de capa de red

Las reglas de capa 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 solo están disponibles en Packet Decoders.

### Reglas de capa de aplicación

Las reglas de capa 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.

### Reglas de correlación

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.

### Usos comunes

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

### Conjuntos de reglas

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 Security Analytics, 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.

### Configuración de reglas

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:

- 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

### Sintaxis de reglas de captura

La sintaxis para escribir reglas de captura consiste en comparar un campo con un valor mediante un operador de comparación. Los operadores de comparación compatibles son es igual a (=) y no es igual a (!=).

Los valores se pueden expresar como valores discretos, un rango de valores, un límite superior o inferior o una combinación de estos tres. Las comparaciones mayor que (>) y menor que (<) se llevan a cabo mediante el uso de rangos. 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.

En la siguiente tabla se resumen los operadores de comparación compatibles y la sintaxis para expresar valores.

| Sintaxis | Descripción |
|---|---|
| * | Regla predeterminada Con el uso de un asterisco (*) como el único carácter de una regla, esa regla seleccionará todo el tráfico. |
| = | Operador de igualdad. |
| != | Operador de desigualdad. |
| && | Operador Y lógico. |
| \|\| | Operador O lógico. |
| -u | Límite superior. Por ejemplo, para seleccionar todos los puertos TCP sobre 40000, la sintaxis sería: `tcp.port = 40000-u` |
| -l | Límite inferior. Por ejemplo, para seleccionar todos los puertos TCP por debajo de 40000, la sintaxis sería: `tcp.port = 1-40000` |
| - (guion) | Denota un rango. Esto solo se aplica a los 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` |
| , (coma) | Denota una lista de valores. Se pueden usar valores únicos, así como cualquier combinación de rangos y límites superiores o inferiores. Por ejemplo, la siguiente sintaxis es válida: `tcp.port = 1-10,25,110,143-225,40000-u` |

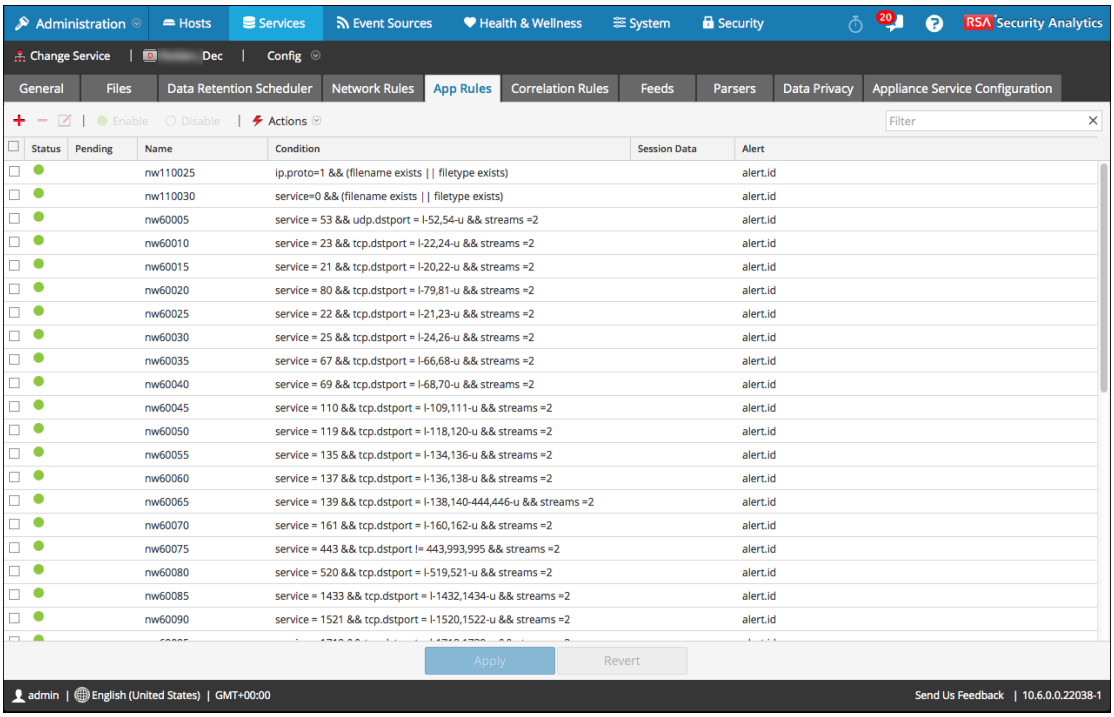
| Sintaxis | Descripción |
|---|---|
| ( ) | Operador de agrupación. Una expresión se puede incluir entre paréntesis para crear una nueva expresión lógica. Por ejemplo, lo siguiente seleccionaría el tráfico en el puerto 80 hacia/desde 192.168.1.1 O el tráfico en el puerto 443 hacia/desde 10.10.10.1: `(ip.addr=192.168.1.1 && tcp.port=80) || (ip.addr=10.10.10.1 && tcp.port=443)` |

Guía de reglas y consultas proporciona una guía que deben seguir todas las consultas y las condiciones de regla en los servicios de Security Analytics Core.

## Procedimientos

### Configurar reglas de captura

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione un servicio Decoder y elija  **> 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 cuadrícula de reglas correspondiente al tipo de regla seleccionado.



Cada tipo de regla tiene una cuadrícula 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 que aparece en la cuadrícula. Para cambiar la secuencia de ejecución de las reglas, arrastre y suelte las reglas en la ubicación correspondiente de la cuadrícula 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 cuadrícula 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**.

### Agregar una regla

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 obtener más detalles, consulte una de las siguientes secciones:

- Configurar reglas de aplicaciones
- Configurar reglas de red
- Configurar reglas de correlación

### Eliminar una regla

1. En cualquier pestaña Reglas, seleccione las reglas que desea eliminar de la cuadrícula de reglas.

2. Haga clic en  .

   Las reglas seleccionadas se quitan de la cuadrícula, pero siguen existiendo en el servicio.

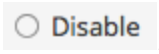
### Editar una regla

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 obtener más detalles, consulte una de las siguientes secciones:

- Configurar reglas de aplicaciones
- Configurar reglas de red
- Configurar reglas de correlación

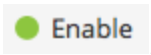
### Desactivar una regla

1. Desde cualquier pestaña de reglas, seleccione las reglas que desea desactivar.
2. Haga clic en 

.

   El estado cambia a desactivado en la cuadrícula, pero la regla sigue activada en el servicio.

### Activar una regla

1. Desde cualquier pestaña de reglas, seleccione las reglas que desea activar.
2. Haga clic en 

.

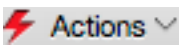
   El estado cambia a activado en la cuadrícula, pero la regla sigue desactivada en el servicio.

### Importar reglas desde un archivo

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.

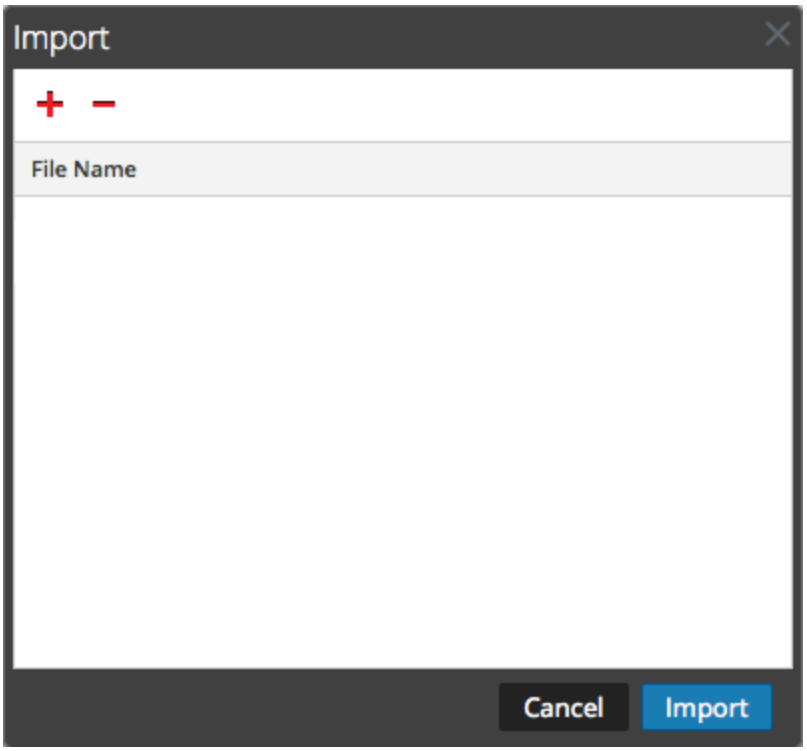
Cuando intenta importar un grupo de reglas, Security Analytics Administration comprueba el tipo de reglas importadas. Si lo hace correctamente, aparece un mensaje que indica la cantidad de reglas importadas. Si el tipo de regla es diferente al tipo de pestaña activa, las reglas no se importan. Debe volver 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 

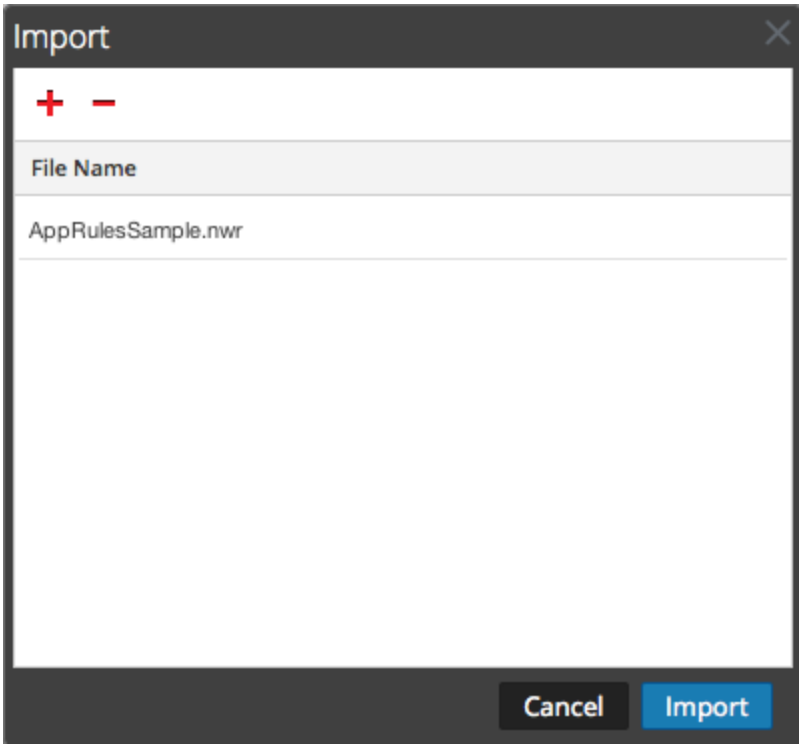
> **Importar**.

   Se muestra 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.

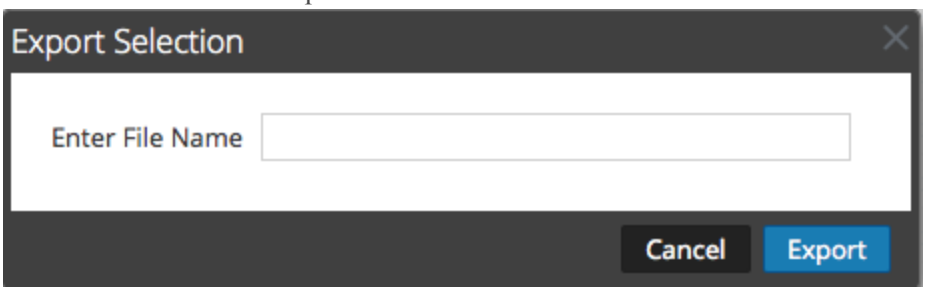



4. Haga clic en **Import**.
   Las reglas se importan a la interfaz del usuario. Las reglas importadas tienen una esquina roja en cada columna editada.
5. Edite o reorganice las reglas si es necesario.
6. Para guardar las reglas en el servicio, haga clic en **Aplicar**.
   Las reglas del servicio se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

### 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 cuadrícula, 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

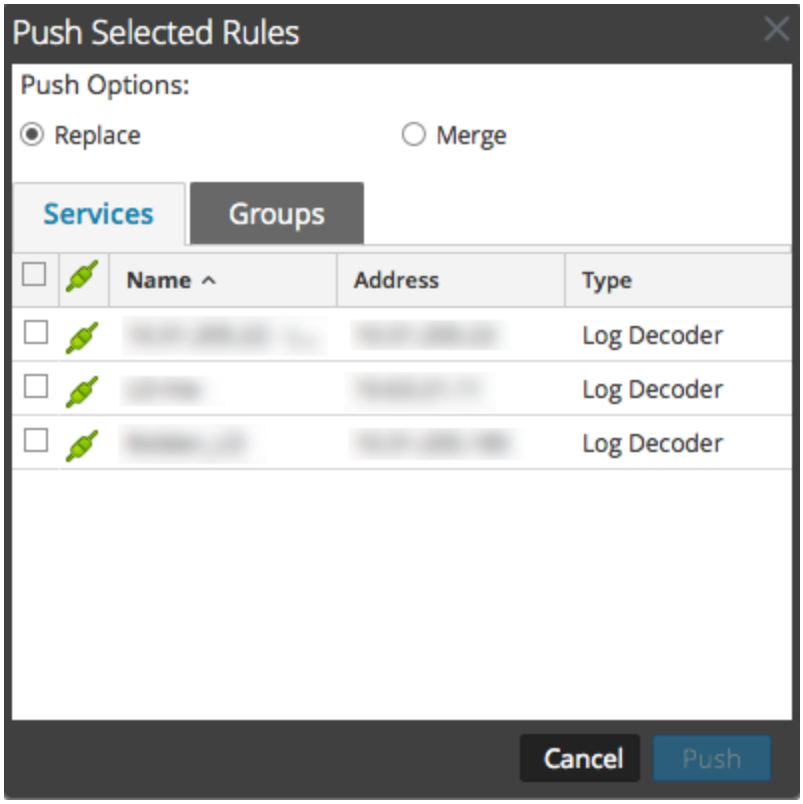
Puede aplicar (migrar) las reglas o las reglas seleccionadas a otros servicios (Decoders o Log Decoders) o a grupos de servicios.

### Migración de reglas seleccionadas

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** para eliminar todas las reglas en los servicios de destino y reemplazarlas por las reglas seleccionadas. 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.

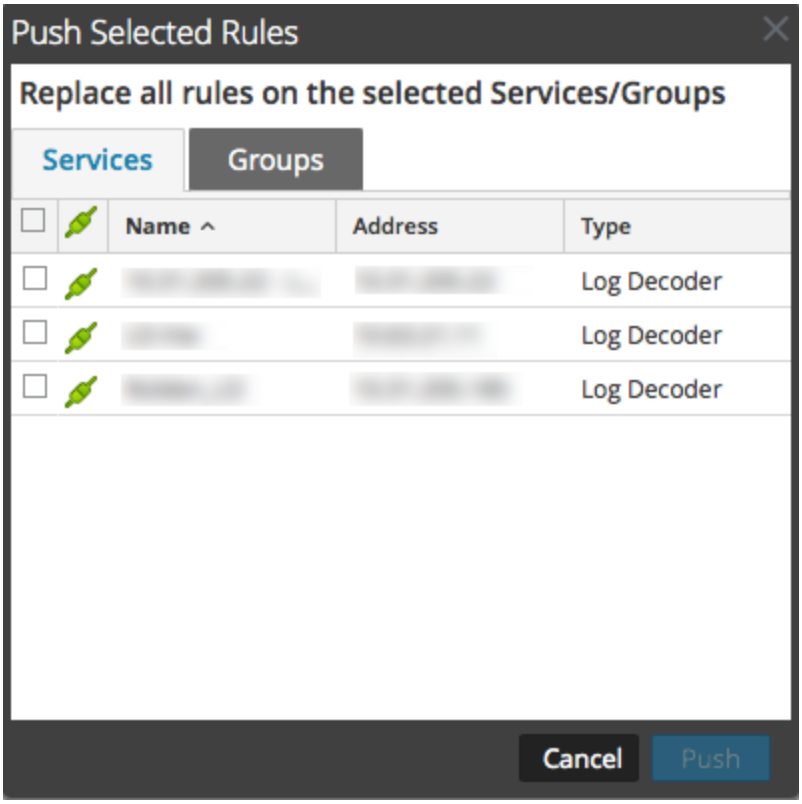
#### Migrar todas las reglas

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 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 cuadrícula, 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.

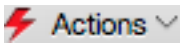
### Cambiar el orden de ejecución de las reglas

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

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

### Restaurar el snapshot de una regla desde el Historial

Security Analytics mantiene las últimas diez instantáneas de las reglas que se aplican a un servicio. Para restaurar el snapshot de una regla desde el Historial:

1. Seleccione  Historial**>.**
   Se muestra un submenú de snapshots.
2. Seleccione la fecha del snapshot en el submenú.
   Las reglas del snapshot se cargan en la cuadrícula 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

En este tema, se presentan las reglas de aplicaciones y proporcionan instrucciones para crearlas.

Las reglas de capa de aplicación se aplican en el nivel de la sesión.

### Reglas de aplicaciones de muestra

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: servicio=139
- Acción de regla: Truncar

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: Filtro

### Procedimientos

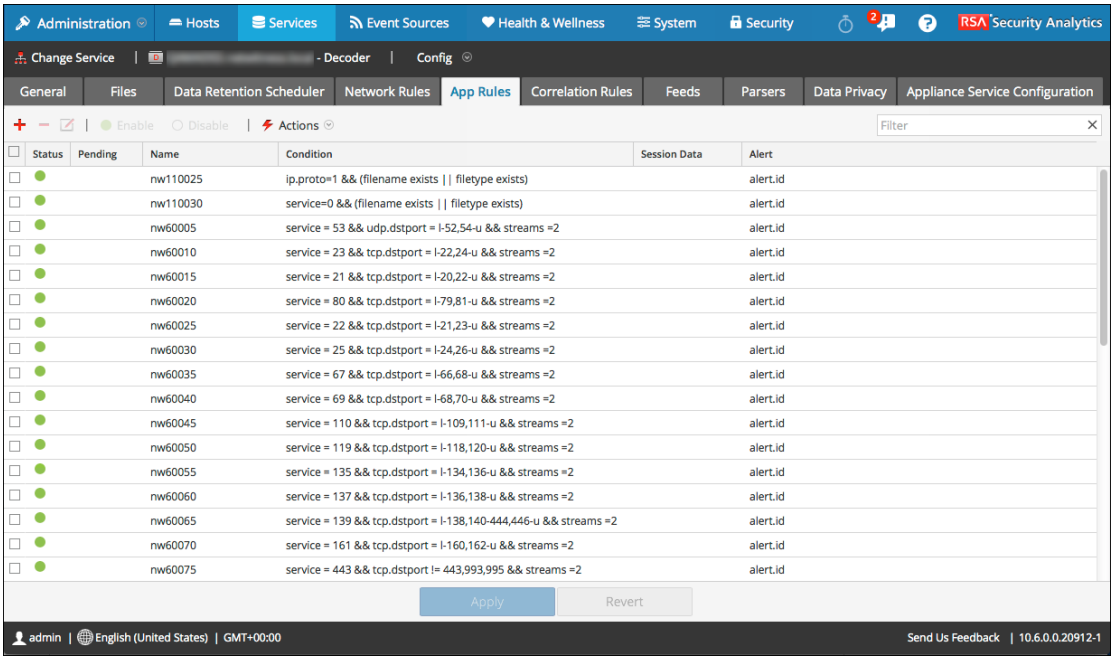
#### Navegue a la pestaña Reglas de aplicación

Navegar hasta la pestaña Reglas de aplicación siempre es el primer paso para definir reglas de aplicación. Para acceder a la pestaña Reglas de aplicación:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio Decoder o Log Decoder y  **> Ver > Configuración**.

   Se muestra la vista Configuración de sistemas del servicio seleccionado.

3. Seleccione la pestaña **Reglas de aplicación**.

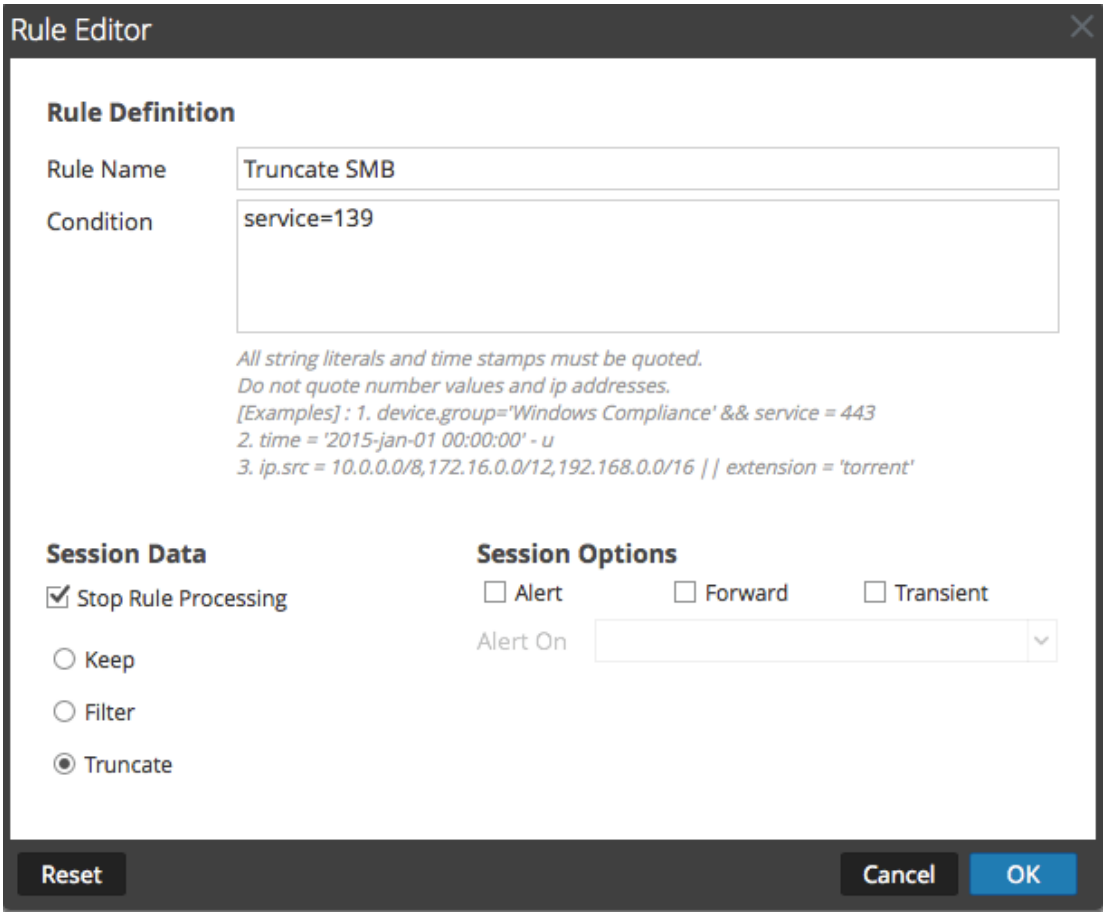



### Agregar o editar una regla de aplicación

En la pestaña Reglas de aplicación:

1. Realice una de las siguientes acciones
   - Si desea agregar una regla nueva, haga clic en  .
   - Si edita una regla, seleccione la regla en la cuadrícula de reglas y haga clic en  .

2. Se abre el cuadro de diálogo Editor de regla con parámetros de reglas de aplicación.




3. 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**.
4. 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, Security Analytics 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. El tema Guía de reglas y consultas proporciona detalles adicionales.
5. Si desea que la evaluación de reglas termine con esta regla, marque la casilla de verificación **Detener procesamiento de regla**.
6. 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.

7. 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 el indicador 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 el indicador **Reenvío**.

     **Nota:** Asegúrese de:
     - Haber activado los indicadores 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 el indicador **Transitorio**.

8. 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**.
9. Verifique que la regla está en la secuencia de ejecución correcta con otras reglas en la cuadrícula. Si es necesario, transfiera la regla.
10. Para aplicar el conjunto de reglas actualizado a Decoder o Log Decoder, haga clic en **Aplicar**.
    Security Analytics 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.

## Configurar reglas de correlación

En este tema, se presentan las reglas de correlación y se explican los procedimientos para crearlas.

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. Security Analytics aplica las 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.

#### Reglas de correlación de muestra

Objetivo: En sesiones donde 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 e ip.dst que aparezca en más de 10 sesiones dentro de 5 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: action='login' && error='fail'
- Clave de instancia: ip.src,ip.dst
- Umbral: count()>10
- Ventana de tiempo: 5 minutos

### Explicación

Ambos ejemplos de reglas tienen la misma clave de instancia: ip.src e ip.dst. Dado que se buscan combinaciones únicas de ip.src e ip.dst que coincidan con la condición de correlación, **ip.src** e **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 de 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 session.id únicos para cada par de 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.

### Procedimientos

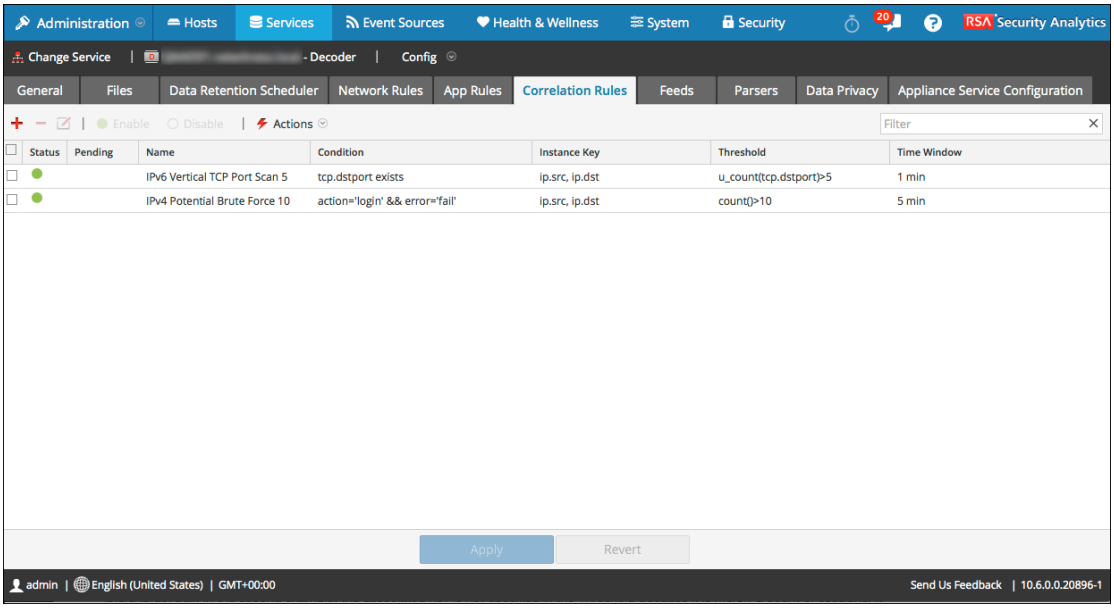
#### Navegue a la pestaña Reglas de correlación

El primer paso para trabajar con reglas de correlación es acceder a la pestaña Reglas de correlación:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **> Ver > Configuración**.

   Se muestra la vista Configuración de servicios del servicio seleccionado.

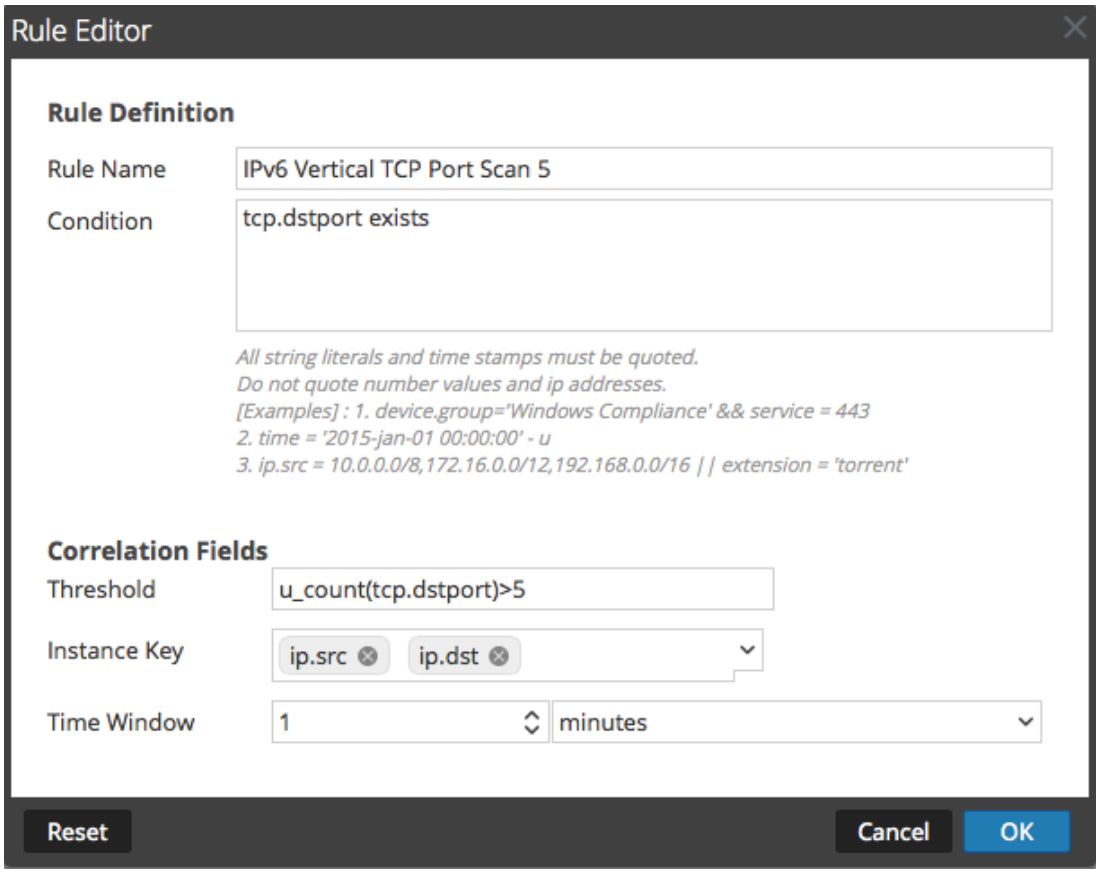
3. Seleccione la pestaña **Reglas de correlación**.




### Agregar o editar una regla de correlación

1. 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, seleccione la regla en la cuadrícula de reglas y haga clic en .
  Se abre el cuadro de diálogo Editor de regla con parámetros de reglas de correlación.




2. 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**.
3. 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, Security Analytics muestra errores de sintaxis y advertencias. Por ejemplo, para crear la regla de muestra, escriba **tcp.dstport exists**. Cuando esta condición se cumpla, se llevará a cabo 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. El tema Guía de reglas y consultas proporciona detalles adicionales.
4. 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 hay una clave asociada especificada)

5. 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).
6. En **Ventana de tiempo**, defina el periodo durante el cual el umbral se debe alcanzar para crear una sesión de correlación.
7. 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**.
8. Verifique que la regla está en la secuencia de ejecución correcta con otras reglas en la cuadrícula. Si es necesario, transfiera la regla.
9. Para aplicar el conjunto de reglas actualizadas al servicio, haga clic en **Aplicar**.

   Security Analytics guarda una instantánea de las reglas aplicadas actualmente y, a continuación, aplica el conjunto actualizado al Decoder o al Log Decoder.

## Configurar reglas de red

En este tema, se presentan las reglas de red y se explican los procedimientos para configurarlas.

Las reglas de capa de red se aplican en el nivel de paquete en un Decoder y se componen de conjuntos de reglas de Capa 2 - Capa 4. 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, solo se aplican a Packet Decoders.

### Reglas de red de muestra

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

- Nombre de la regla: Truncar SSL
- Condition: 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
- Condition: ip.addr=192.168.2.0/24
- Acción de regla: Filtro

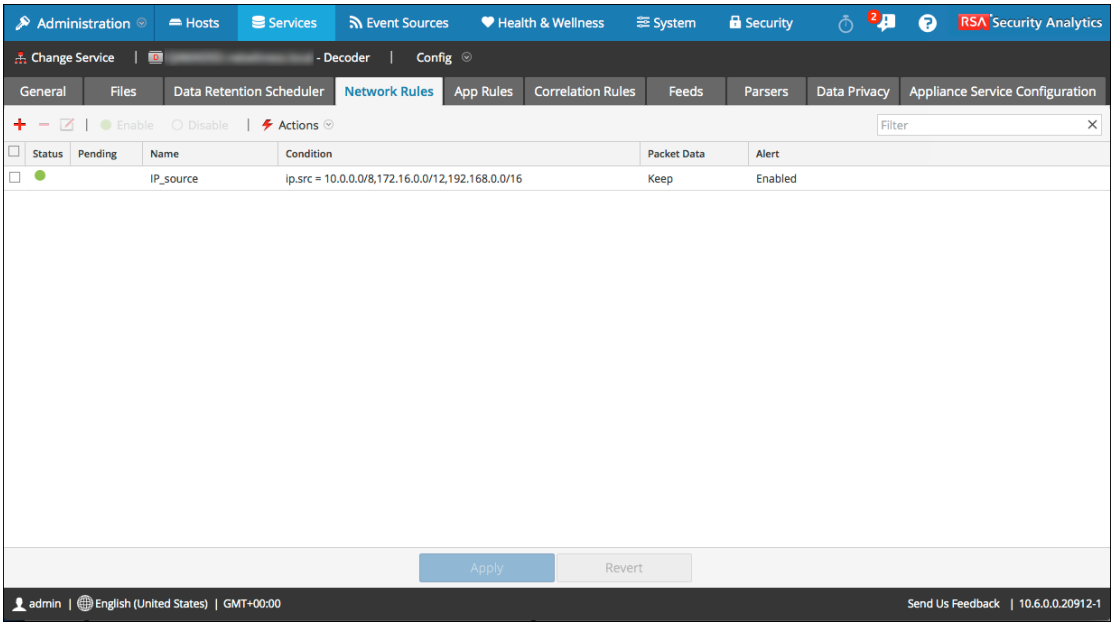
### Procedimientos

#### Navegue a la pestaña Reglas de red

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio Decoder y elija  **> Ver > Configuración**.

   Se muestra la vista Configuración de servicios del servicio seleccionado.

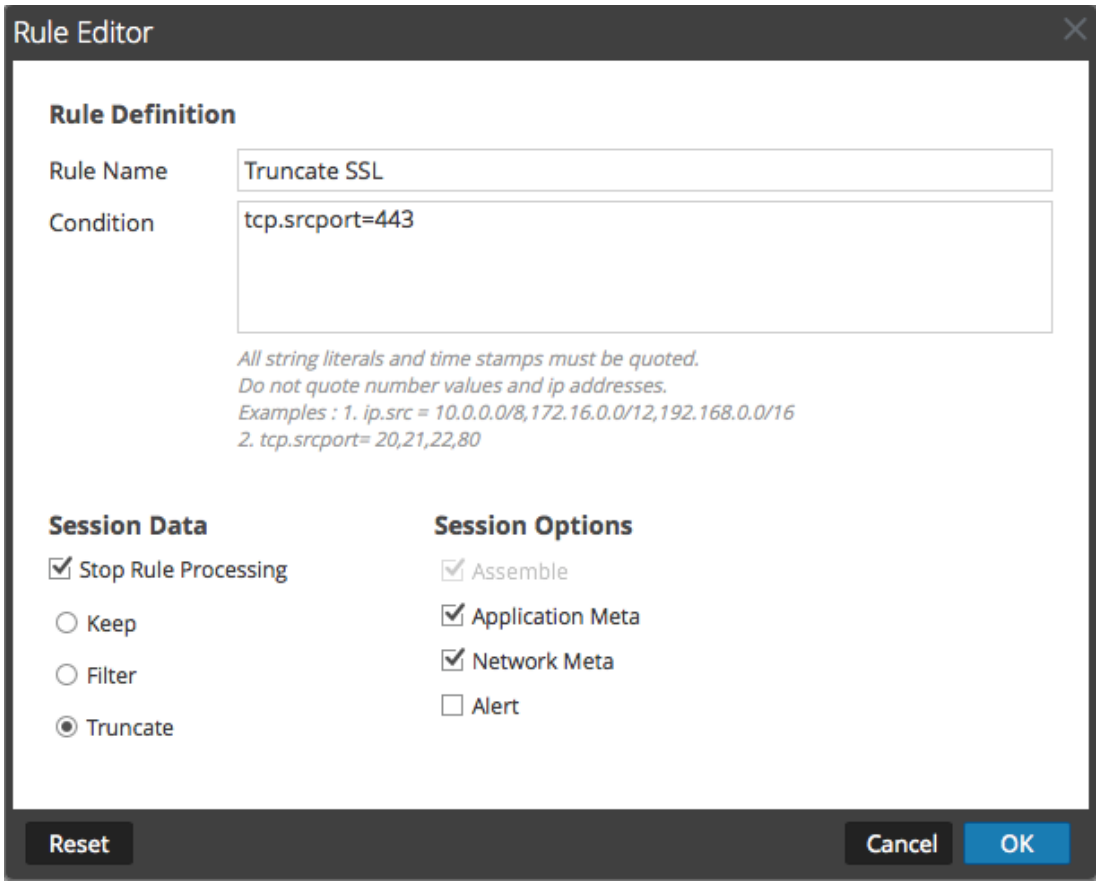
3. Seleccione la pestaña **Reglas de red**.
   Se abre la pestaña Reglas de red.




### Agregar o editar una regla de red

1. 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, seleccione la regla en la cuadrícula de reglas y haga clic en  .
  Se muestra el cuadro de diálogo Editor de regla.




2. 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**.
3. 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, Security Analytics 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. El tema Guía de reglas y consultas proporciona detalles adicionales. Claves de metadatos compatibles en condiciones de reglas de red describe las claves de metadatos que Security Analytics admite para usar en condiciones de reglas de red.
4. Si desea que la evaluación de reglas termine con esta regla, seleccione la casilla de verificación **Detener procesamiento de regla**.

5. 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.

6. 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.

7. 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.
8. Verifique que la regla está en la secuencia de ejecución correcta con otras reglas en la cuadrícula. Si es necesario, transfiera la regla.
9. Para aplicar el conjunto de reglas actualizadas al Decoder, haga clic en **Aplicar**.

   Security Analytics 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.

## Paso 5. Iniciar y detener la captura de datos

En este tema se explica un procedimiento para iniciar y detener la captura de datos en Decoders.

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.

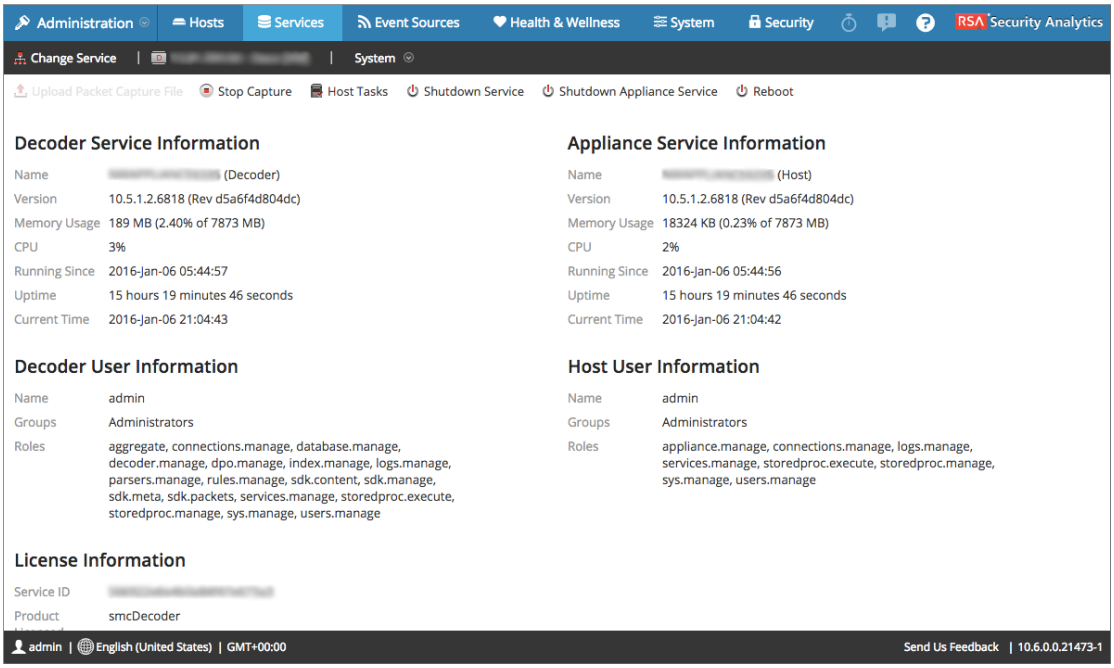
**Nota:** Los ajustes de configuración de captura en la vista Configuración de servicios para un Decoder determinan si el AutoStart de la captura está habilitado, así como los ajustes de adaptador, caché, base de datos y hash.

### Procedimiento

Para iniciar y detener la captura:

1. En el menú de **Security Analytics**, seleccione **Administration > 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.



# Procedimientos adicionales

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

Esta sección se puede usar para buscar información adicional acerca de los Decoders y Log Decoders en Security Analytics.

**Temas**

# Configurar feeds y analizadores

En este tema se presentan feeds y analizadores, y se proporcionan procedimientos para trabajar con los feeds y los analizadores de Decoder y Log Decoder.

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 defina lo contrario, todas las referencias a los Decoders se aplican también a los Log Decoders.

## Procedimientos

### Configurar analizadores

Security Analytics 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 deshabilitar el uso de analizadores en el Decoder, además de limitar los metadatos que crea el analizador.

Existen varios tipos de analizadores configurables personalizados:

- GeoIP: este analizador asocia las direcciones IP con ubicaciones geográficas reales.
- Búsqueda: el usuario configura este analizador para generar metadatos mediante el escaneo de palabras clave predefinidas y expresiones regulares.
- FLEXPARSE: este es un lenguaje de definición de analizador genérico para extender la compatibilidad del protocolo de aplicación existente del Decoder.
- 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 de SNORT® IDS.

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 de Live, se instaló a través de Security Analytics 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 Security Analytics Live.

### Configurar feeds

Security Analytics 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 Security Analytics para obtener feeds de orígenes externos. En el tema **Contenido de Live en Security Analytics** 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 Security Analytics, puede ver la lista de feeds implementados actualmente, junto con un indicador de si el feed que se originó en Security Analytics Live se instaló a través de Security Analytics o de forma manual. Puede agregar, eliminar y actualizar feeds, mientras se ejecuta un Decoder, sin afectar la captura.

Security Analytics 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.

#### Temas

- Crear e implementar feeds personalizados con el asistente
- Usar analizadores personalizados

## Crear e implementar feeds personalizados con el asistente

En este tema se proporcionan instrucciones para usar el asistente Feed personalizado en RSA Security Analytics con el fin de completar rápidamente los Decoders con feeds personalizados.

RSA Security Analytics cuenta con un asistente Feed personalizado para crear e implementar rápidamente 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 feeds en RSA Security Analytics tienen el formato `<filename>.feed`. Para crear un feed, Security Analytics requiere un archivo de datos de feed en el formato `.csv` 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 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 utilizan para crear un feed recurrente deben estar almacenados en una URL accesible, en la cual Security Analytics pueda buscar la versión más reciente del archivo para cada recurrencia. Después de la creación de un feed de Security Analytics, puede descargarlo al sistema de archivos local, editar sus archivos y, a continuación, editar el feed de Security Analytics para usar los archivos de feed actualizados.

### Archivo de definición de feed de muestra

Este es el ejemplo de un archivo de definición de feed llamado **dynamic_dns.xml** que Security Analytics crea en función de las entradas del asistente Feed personalizado. Define la estructura del archivo de datos del feed llamado **dynamic_dns.csv**.

```
<?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>

<Campos>
<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 Security Analytics 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 Security Analytics | Equivalente en el archivo de definición del feed |
|---|---|
| (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.<br>**Nota:** Ahora puede utilizar 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 Security Analytics | 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 **`flatfeedfile 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.<br>**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 (for example, 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 callback se activan en los índices No IP. |

| Parámetro de Security Analytics | Equivalente en el archivo de definición del feed |
|---|---|
| (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. |
| (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 se corresponde con el 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 callback** | 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). La clave de callback 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. |

| Parámetro de Security Analytics | Equivalente en el archivo de definición del feed |
|---|---|
| (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. Se corresponde con el atributo **Field key** en el archivo de definición del feed. Una clave se aplica solamente a un campo cuyo tipo está definido en **valor**. En el archivo de definición del feed, hay una lista de LanguageKeys desde **index.xml** o un nombre del resumen si se utiliza el nombre de origen y el nombre de destino. Por ejemplo, **reputation** es un nombre de resumen para **reputation.src** y **reputation.dst**. El atributo Field key hace referencia a este valor. |

### Crear un feed personalizado

Puede crear fácilmente un feed personalizado mediante el asistente Feed personalizado. Para realizar este procedimiento, necesita un archivo de datos de feed en formato `.csv`. 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 un archivo de datos de feed y el archivo de definición de feed correspondiente.

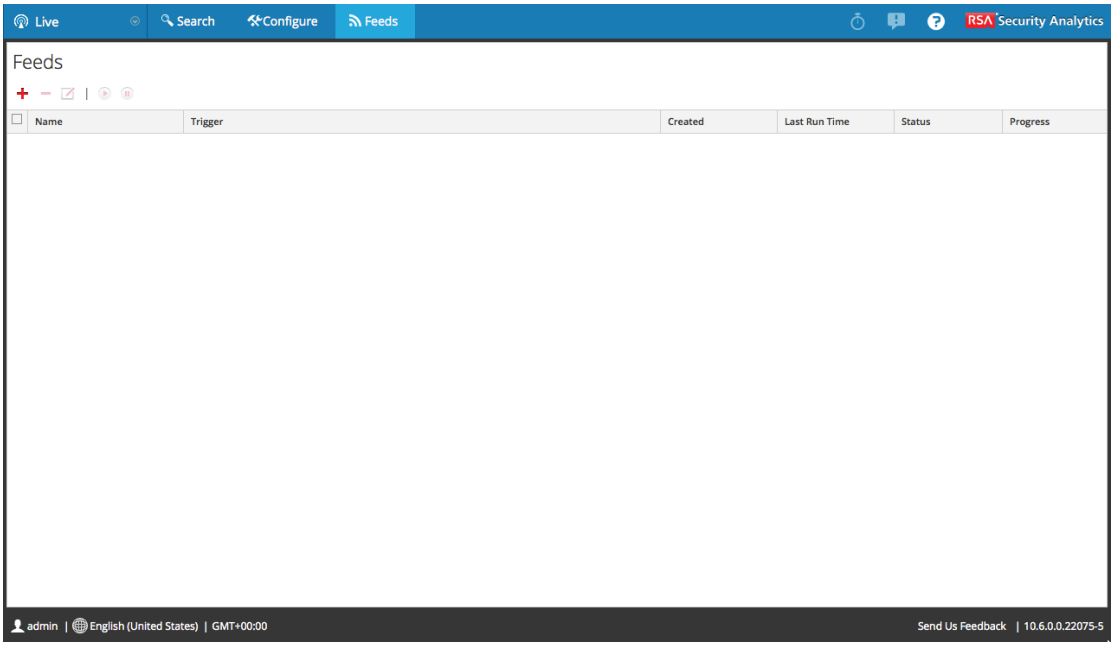
Después de realizar este procedimiento, habrá creado un feed personalizado.

El archivo de datos de feed (`.csv`) 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 cual se pueda acceder desde el servidor de Security Analytics.

#### Para crear un feed personalizado:

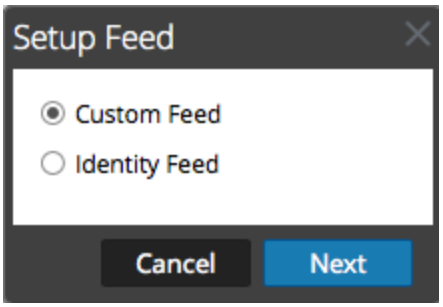
1. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

   Se muestra la vista Feeds.



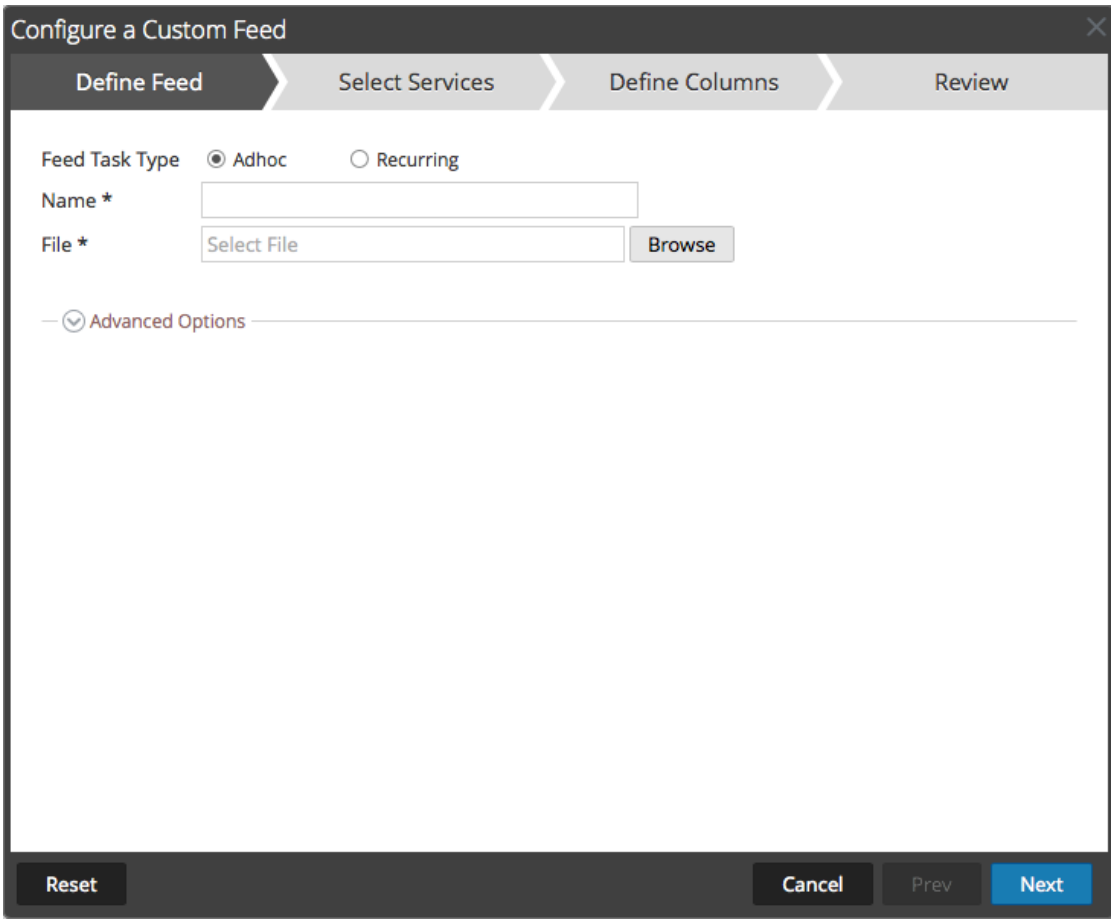

2. En la barra de herramientas, haga clic en  .

   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.



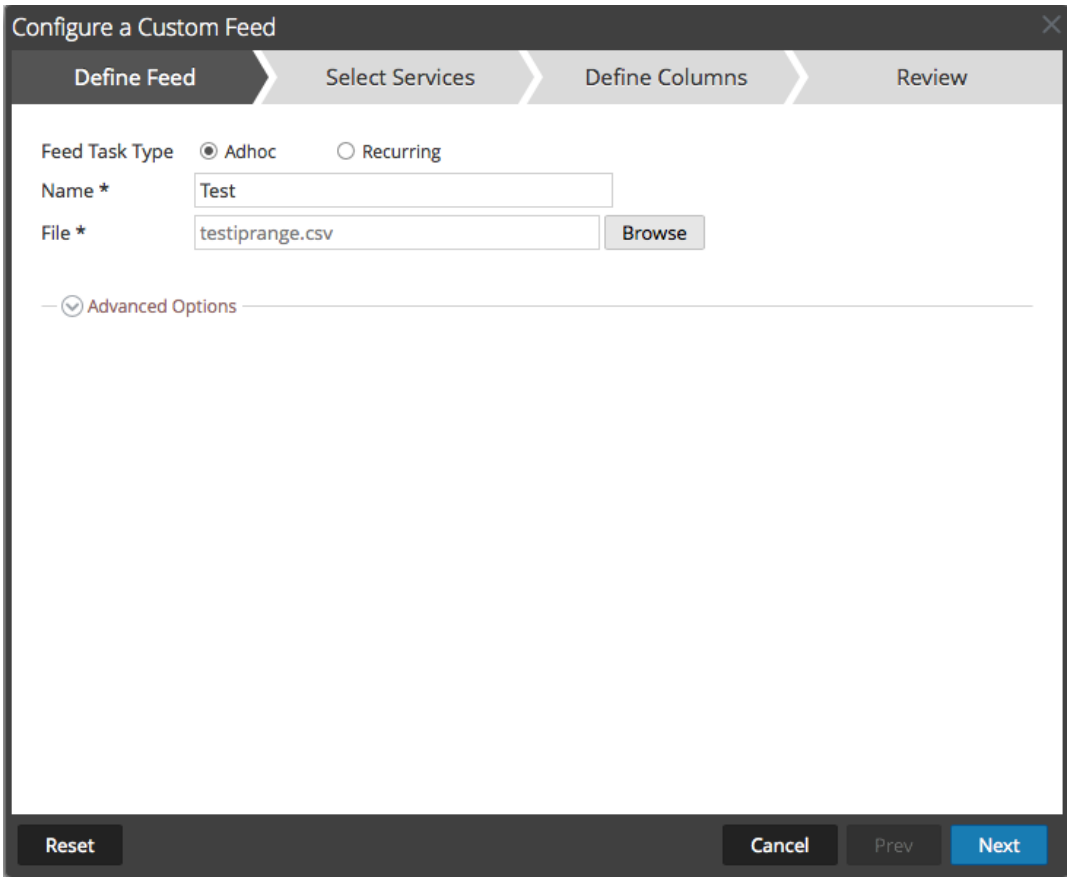

4. Para definir una tarea de feed según demanda que se ejecute una sola vez, seleccione **Ad hoc** en el campo **Tipo de tarea de feed** y realice una de las siguientes acciones:

   a. (Condicional) Para definir un feed basado en un archivo de datos de feed con formato .csv, escriba el **Nombre** del feed, seleccione un **archivo** de contenido .csv 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

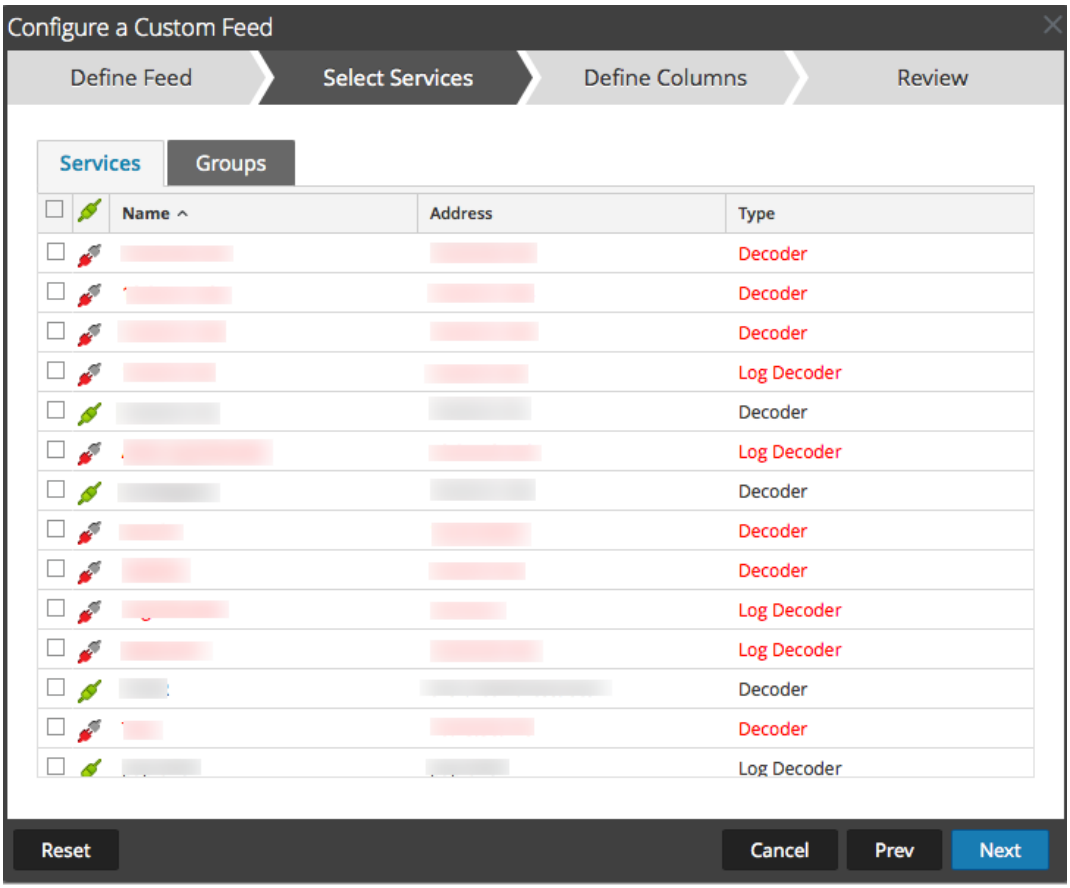
**Opciones avanzadas**.

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 utilizarán en el archivo de datos del feed (el valor predeterminado es #) y haga clic en **Siguiente**.

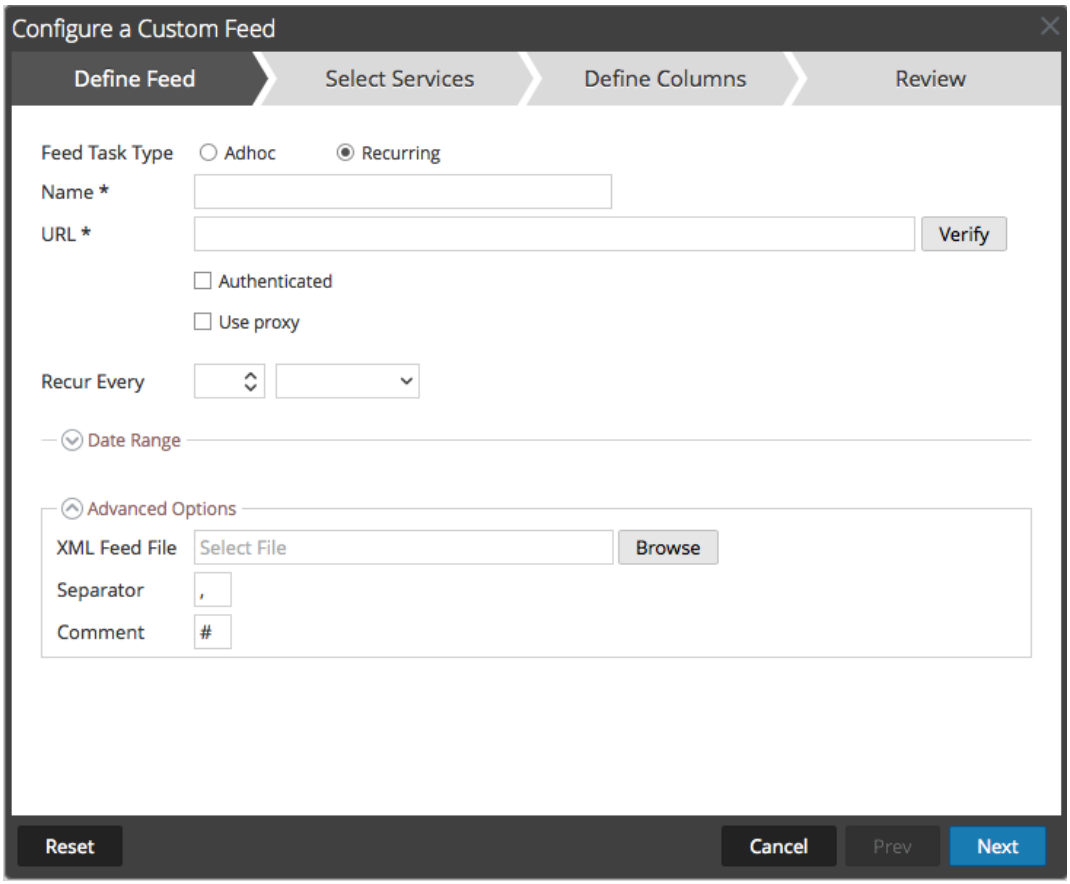
d. Se muestra el formulario Seleccionar servicios. Este es un ejemplo del formulario de un feed basado en un archivo de datos de feed sin archivo de definición de feed. Si define un feed basado en un archivo de definición de feed, la pestaña Definir columnas no es necesaria.




5. 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**, escriba la dirección URL en la cual está ubicado el archivo de datos del feed, por ejemplo, `http://<hostname>/<feeddatafile>.csv`, y haga clic en **Verificar**.

   Security Analytics verifica la ubicación en la cual está almacenado el archivo con el fin de comprobar el archivo más reciente automáticamente antes de cada recurrencia.

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

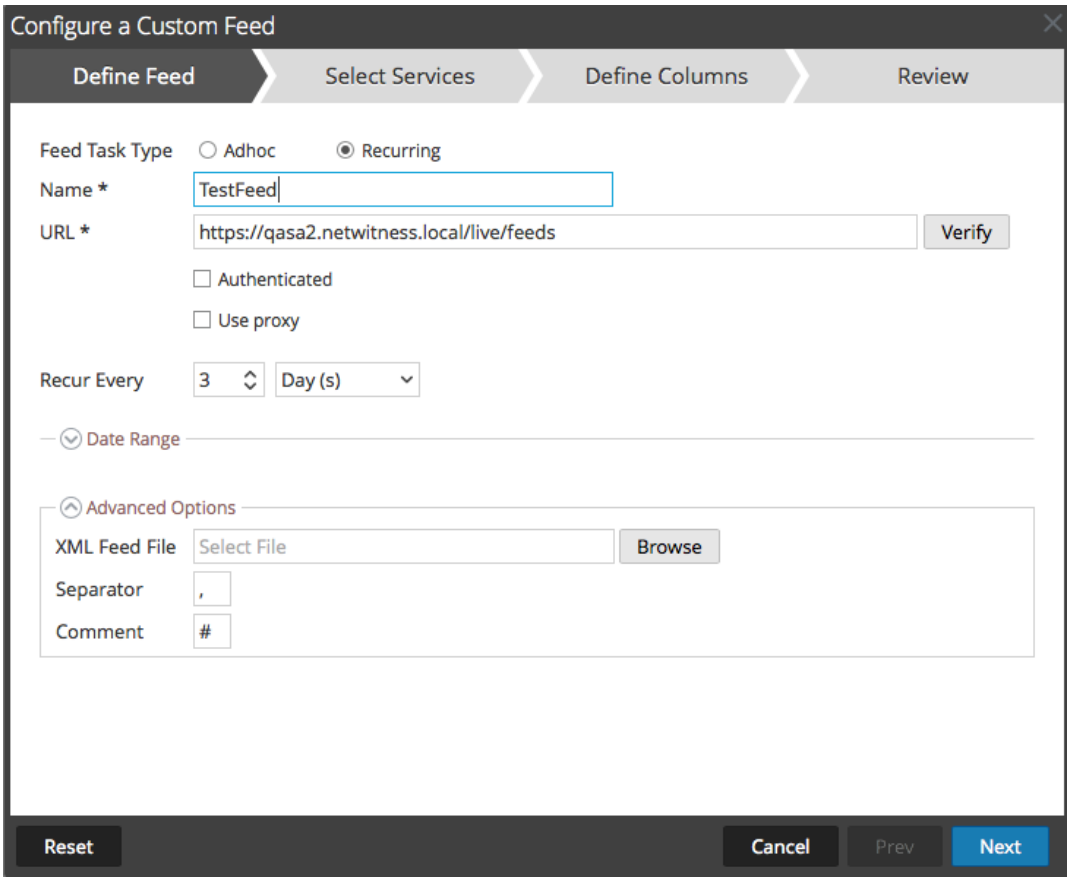
   Security Analytics proporciona su nombre de usuario y contraseña con fines de autenticación en la dirección URL.

d. Si desea que el servidor de Security Analytics 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 el tema **Configure el proxy de Security Analytics** en la *Guía de configuración del sistema*. De forma 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 cada semana y seleccione los días de la semana.

f. 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**.

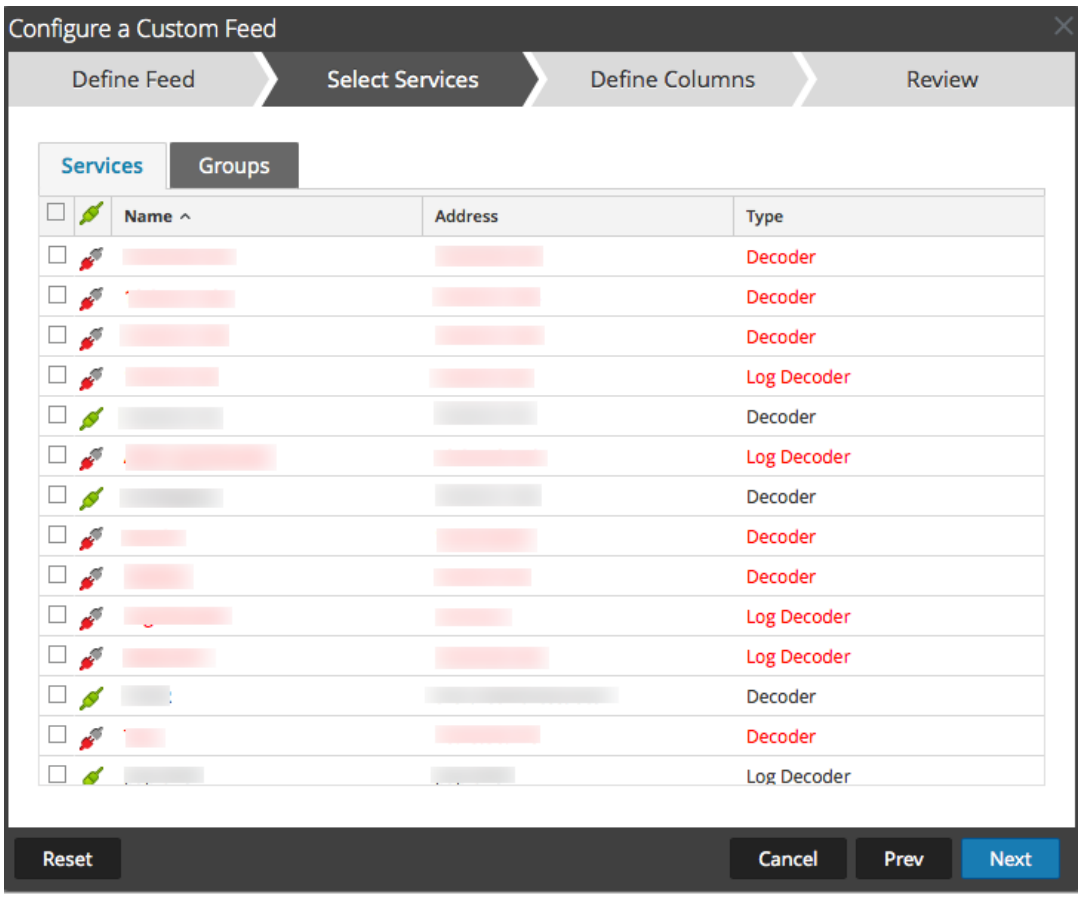



6. (Condicional) Si desea definir un feed basado en un archivo de feed XML:

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

  Se muestran los campos Opciones avanzadas.
- Seleccione un archivo de feed XML del sistema de archivos local, elija el **Separador** (la opción predeterminada es coma), especifique los caracteres de **Comentario** que se utilizarán en el archivo de datos del feed (la opción predeterminada es #) y haga clic en **Siguiente**.

Se muestra el formulario Seleccionar servicios.




7. 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**.

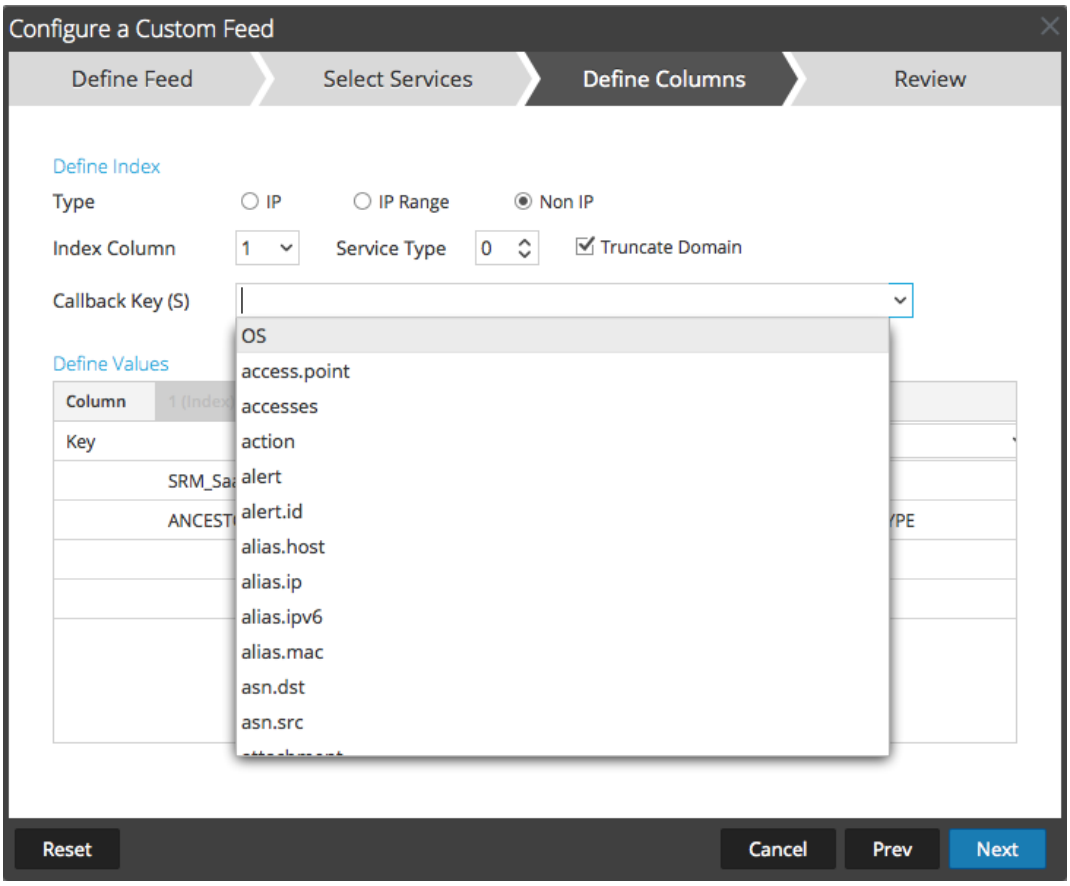
      Se muestra el formulario Definir columnas.

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

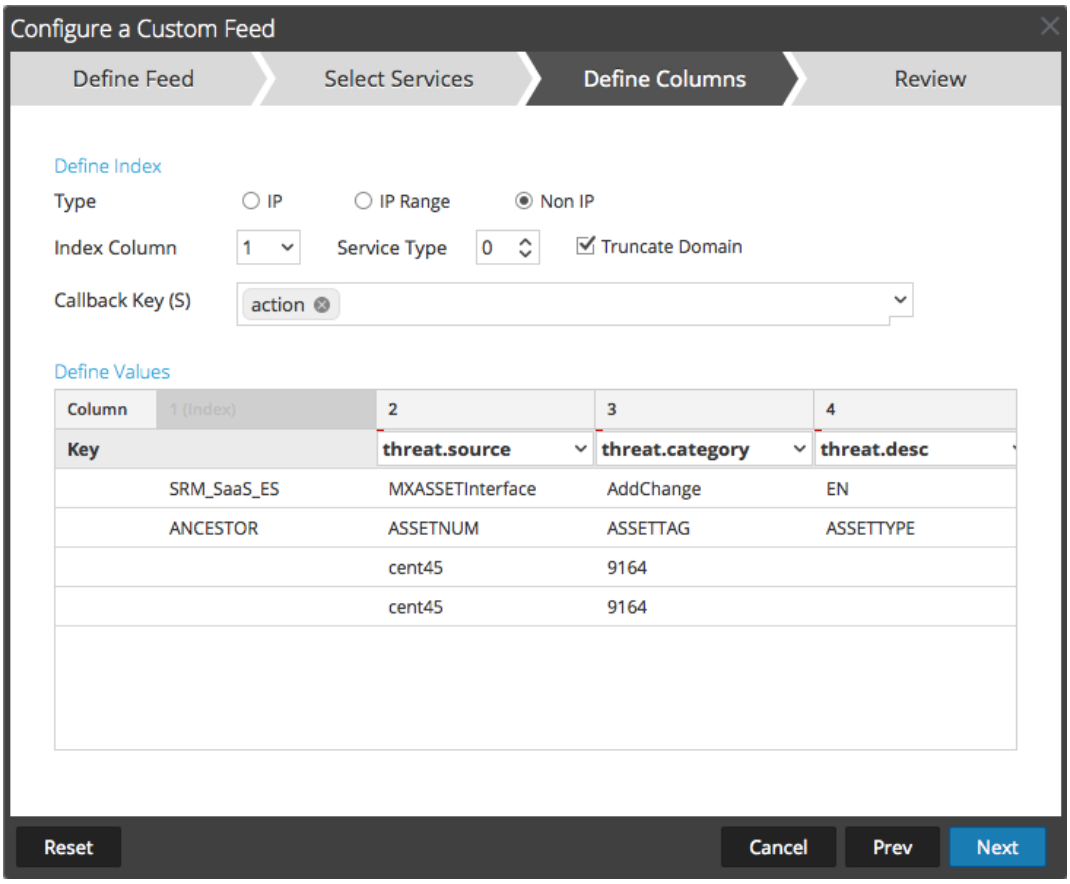
   a. Defina el tipo de Índice: **IP**, **Rango de IP** o **No IP** y seleccione la columna de índice.

   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**.

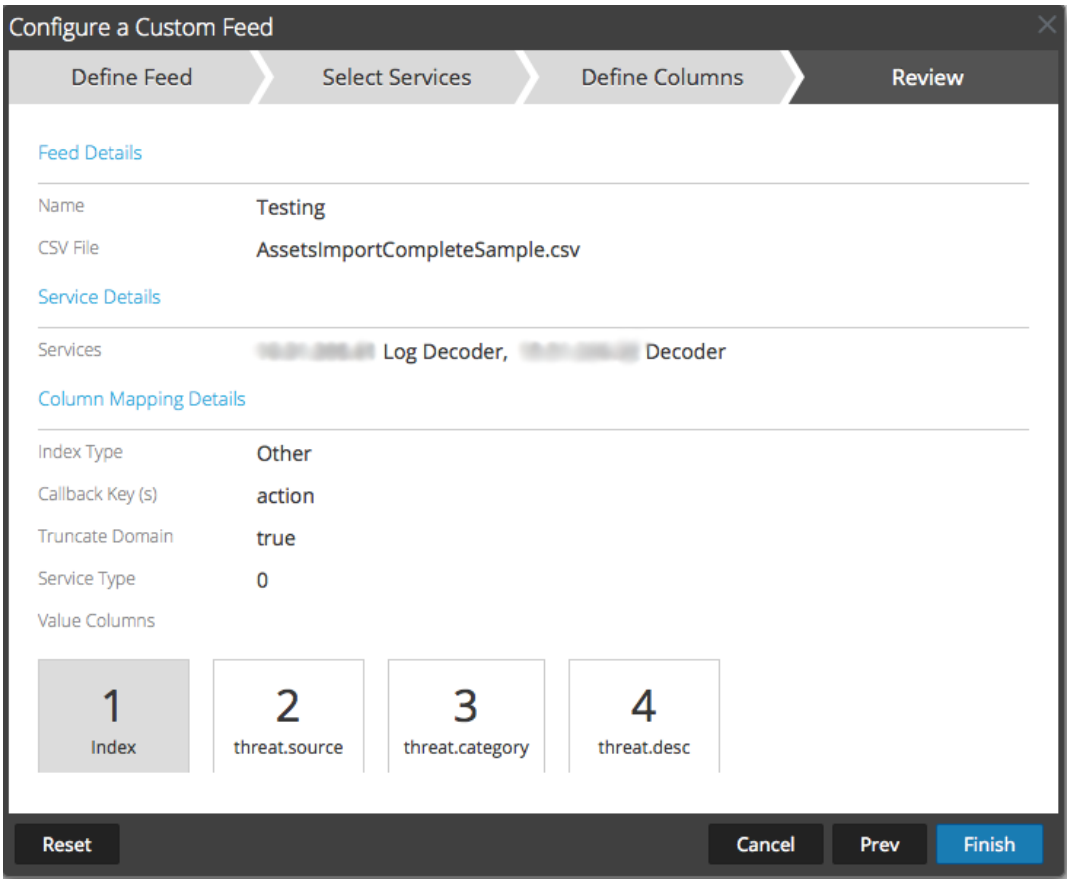



d. En la lista desplegable, seleccione la clave de idioma que se aplicará a los datos en cada columna. Los metadatos que se muestran en la lista desplegable se basan en los metadatos disponibles para los valores definidos del servicio. También puede agregar otros metadatos de acuerdo con su pericia avanzada.



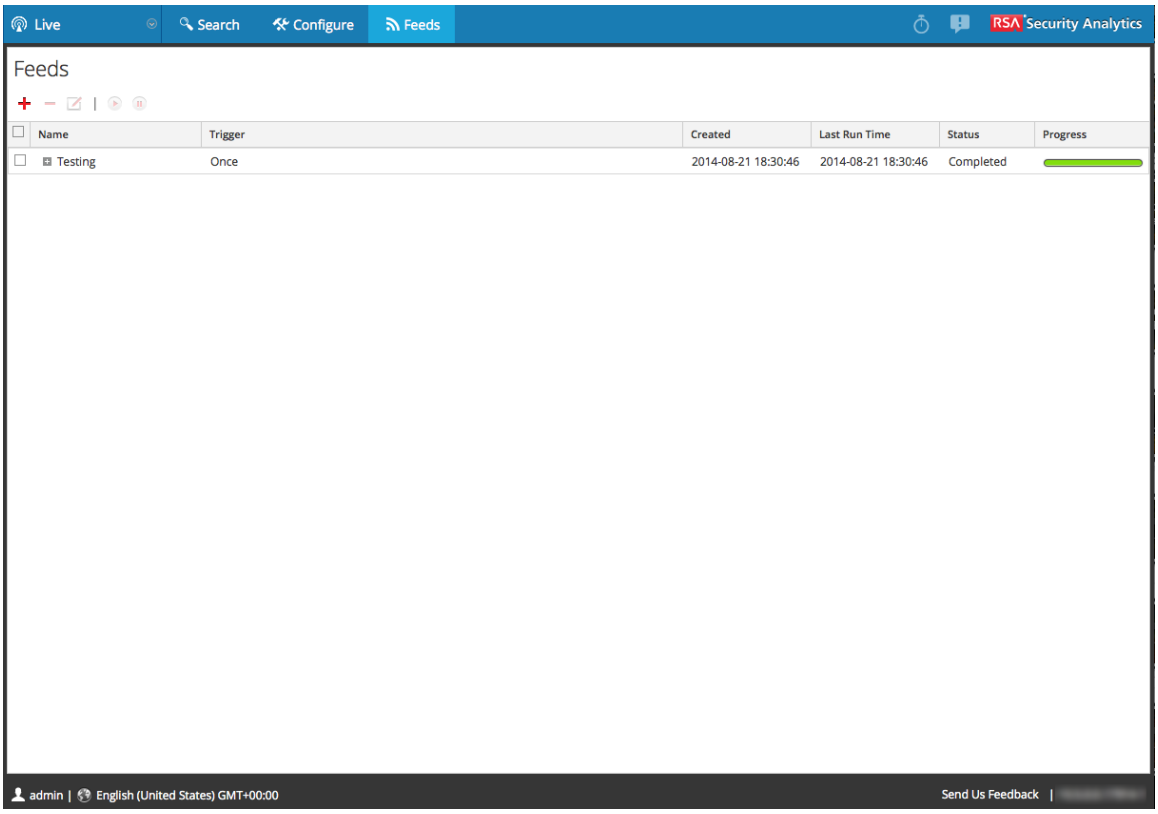

e. Haga clic en **Siguiente**.

   Se muestra el formulario Revisión.




9. 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).

10. Revise la información del feed y haga clic en **Finalizar** si los datos son correctos.
11. 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 Feed grid 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.


Live
Search
Configure
Feeds
RSA Security Analytics
Feeds
Name
Trigger
Created
Last Run Time
Status
Progress
Testing
Once
2014-08-21 18:30:46
2014-08-21 18:30:46
Completed
admin | English (United States) GMT+00:00
Send Us Feedback |

### Crear un feed de identidad

Puede crear fácilmente un feed de identidad y completarlo para los Decoders y Log Decoders seleccionados. Después de realizar este procedimiento, habrá creado un feed de identidad.

### Requisitos previos

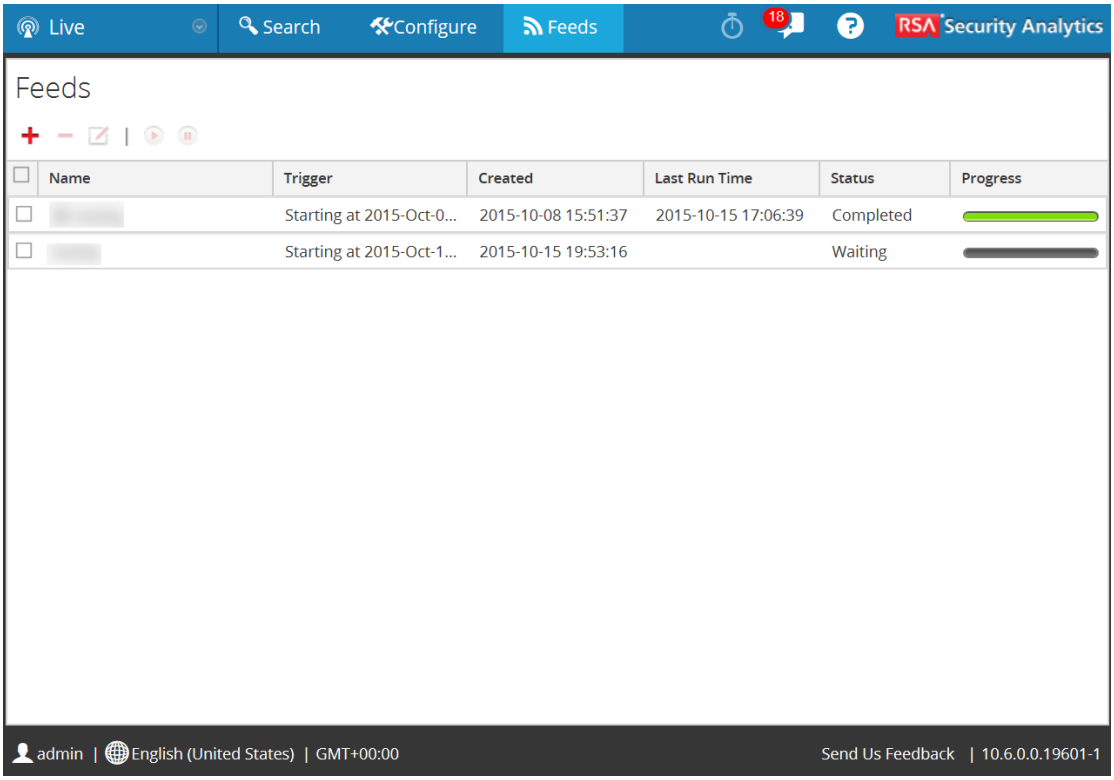
Para crear un feed de identidad, debe tener:

- 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

### Crear un feed de identidad

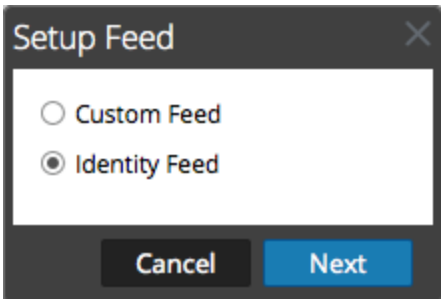
1. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

   Se muestra la cuadrícula Feeds.




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

   El cuadro de diálogo Configurar feed se muestra con la opción Feed de identidad seleccionada de manera predeterminada.



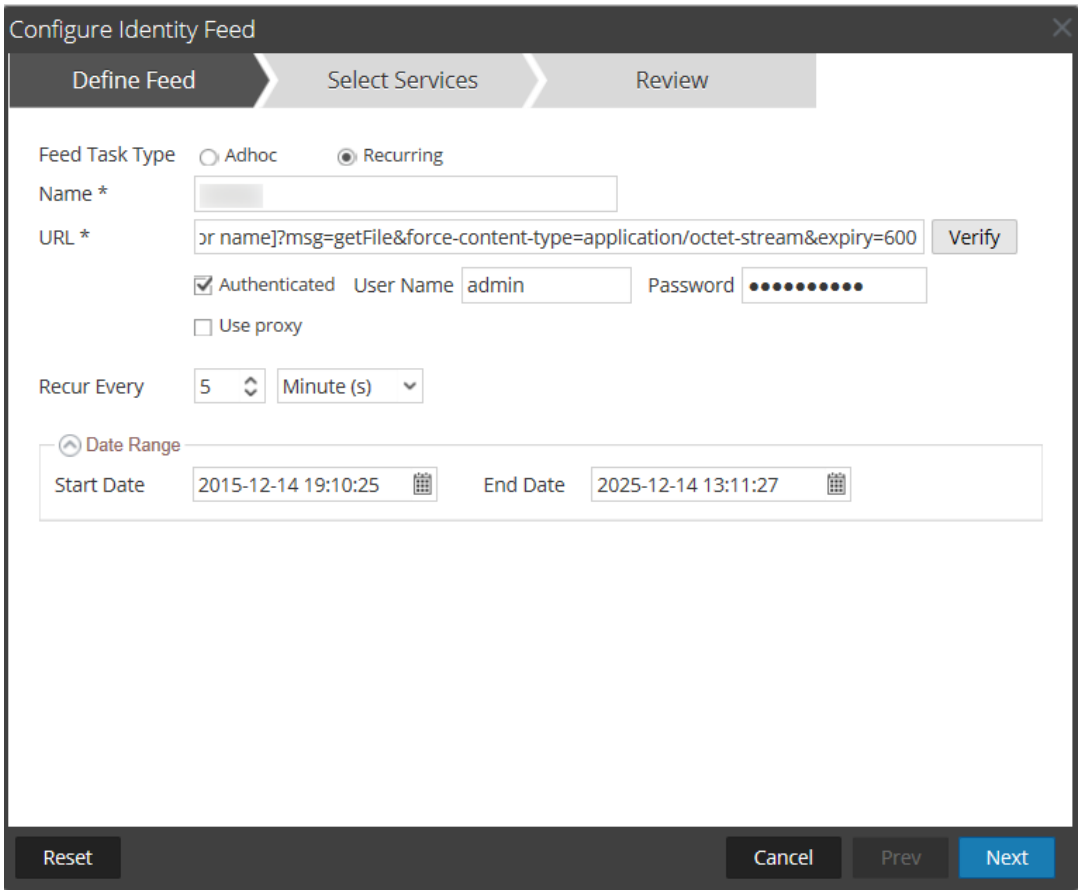

3. Seleccione **Feed de identidad** y haga clic en **Siguiente**.

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

4. (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 formulario **Definir feed** se incluyen los campos de un feed recurrente.



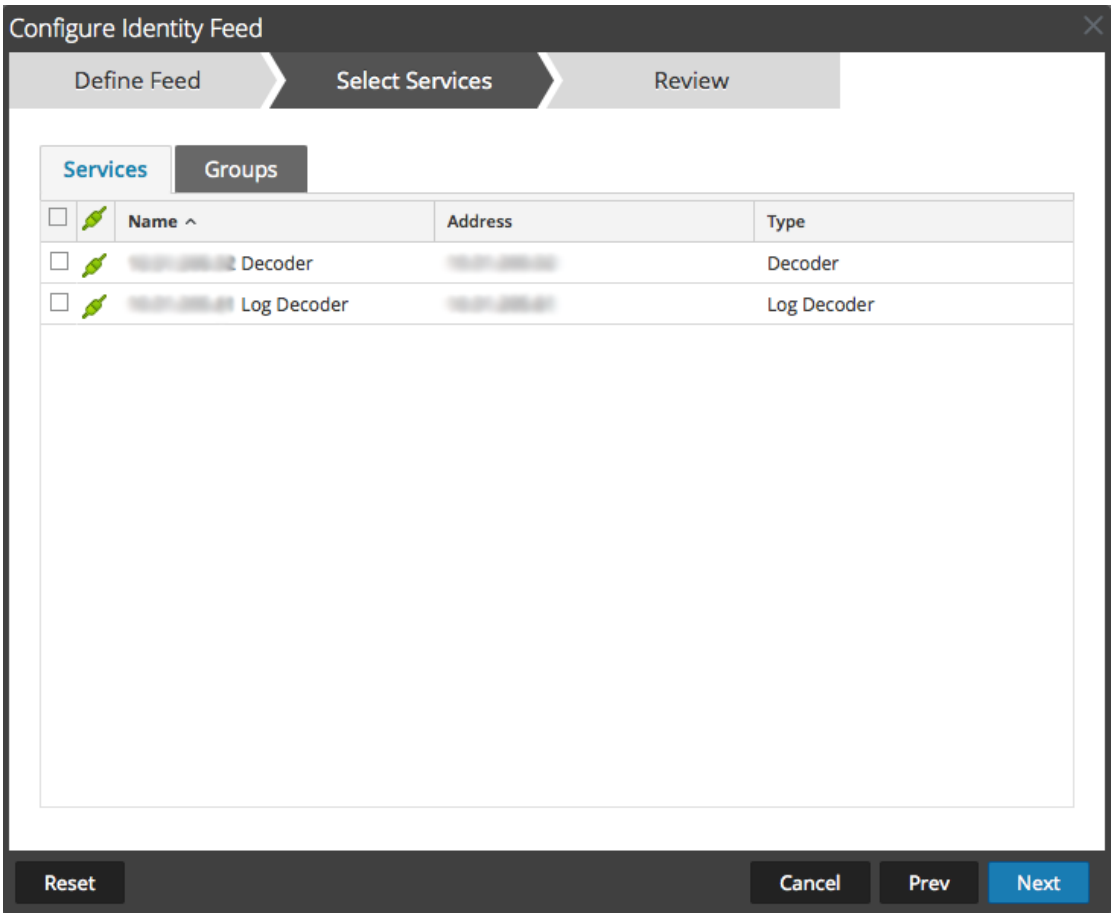
> **Nota:** Security Analytics verifica la ubicación en la cual está almacenado el archivo con el fin de comprobar automáticamente el archivo más reciente antes de cada recurrencia.

En el campo **URL**, escriba la dirección URL en la cual está ubicado el archivo de datos del feed. Por ejemplo:

```
http://<LogCollector>:50101/event-
processors/<ID Event processor name>?msg=getFile&force-
content-type=application/octet-stream&expiry=600
```

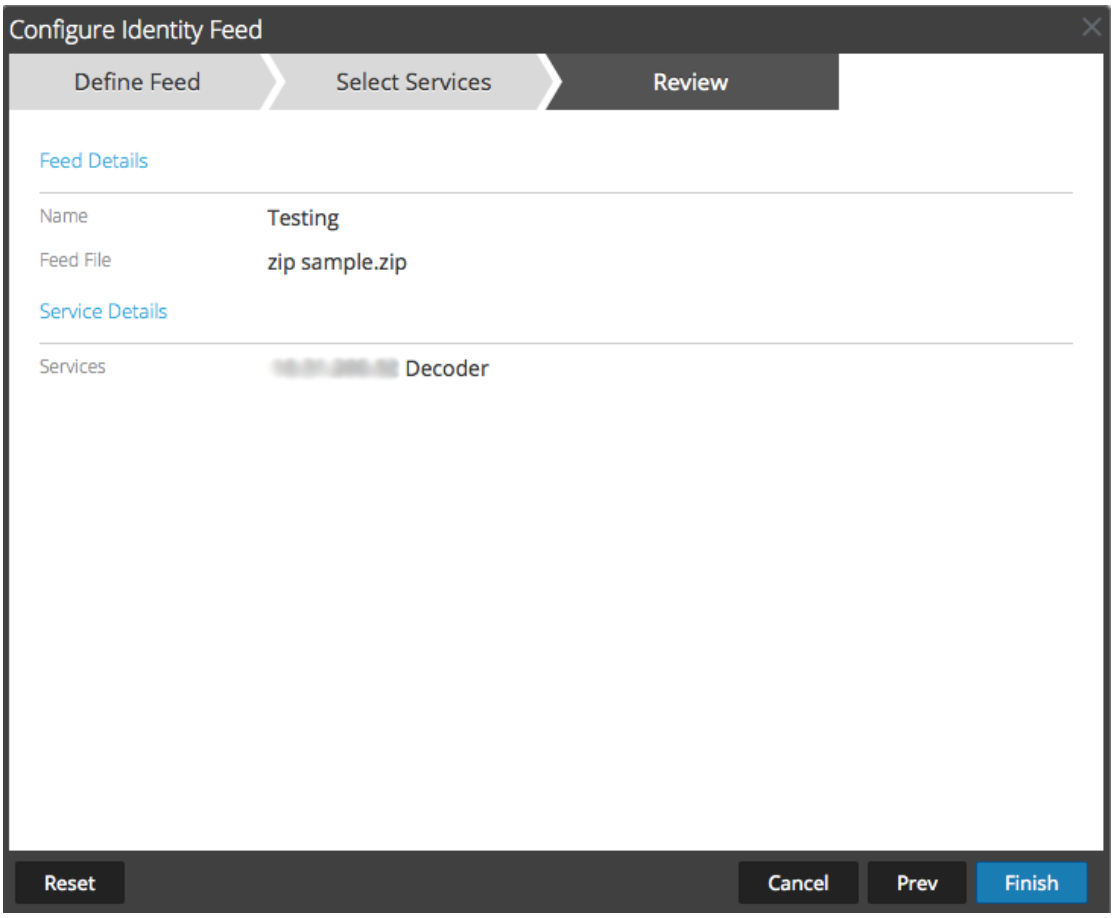
5. (Opcional) Si la URL tiene acceso restringido y se solicita autenticación con nombre de usuario y contraseña, seleccione **Autenticado**. Security Analytics proporciona a la dirección URL su nombre de usuario y contraseña con fines de autenticación.
6. Para definir el intervalo de recurrencia, puede 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**.
7. Haga clic en **Verificar** para verificar su configuración de feed de identidad antes de continuar con el formulario Seleccionar servicios.
8. Haga clic en **Siguiente**.

   Se muestra el formulario Seleccionar servicios.




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

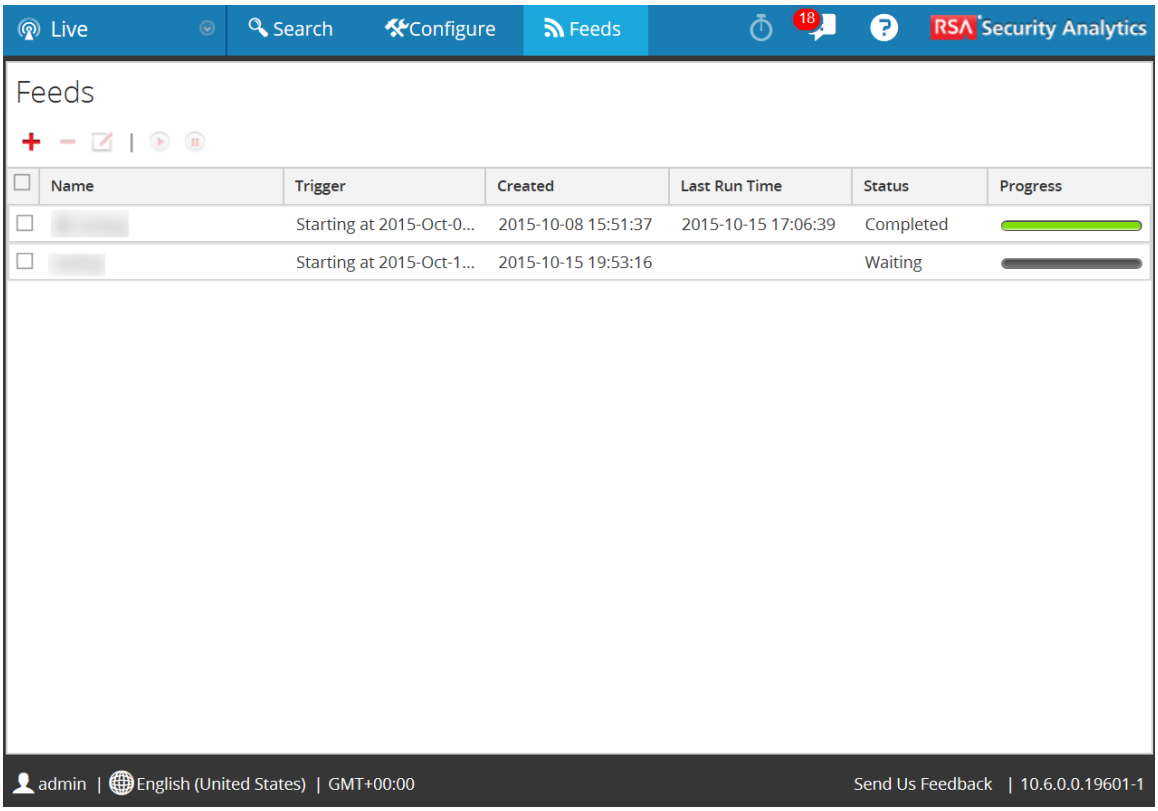
    Se muestra el formulario Revisión.




**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.

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).
12. 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 Feed grid 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.


Live
Search
Configure
Feeds
18
RSA Security Analytics
Feeds
Name
Trigger
Created
Last Run Time
Status
Progress
Starting at 2015-Oct-0...
2015-10-08 15:51:37
2015-10-15 17:06:39
Completed
Starting at 2015-Oct-1...
2015-10-15 19:53:16
Waiting
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.19601-1

### Editar un feed personalizado

En este tema se proporcionan instrucciones para editar un feed personalizado mediante el asistente Feed personalizado.

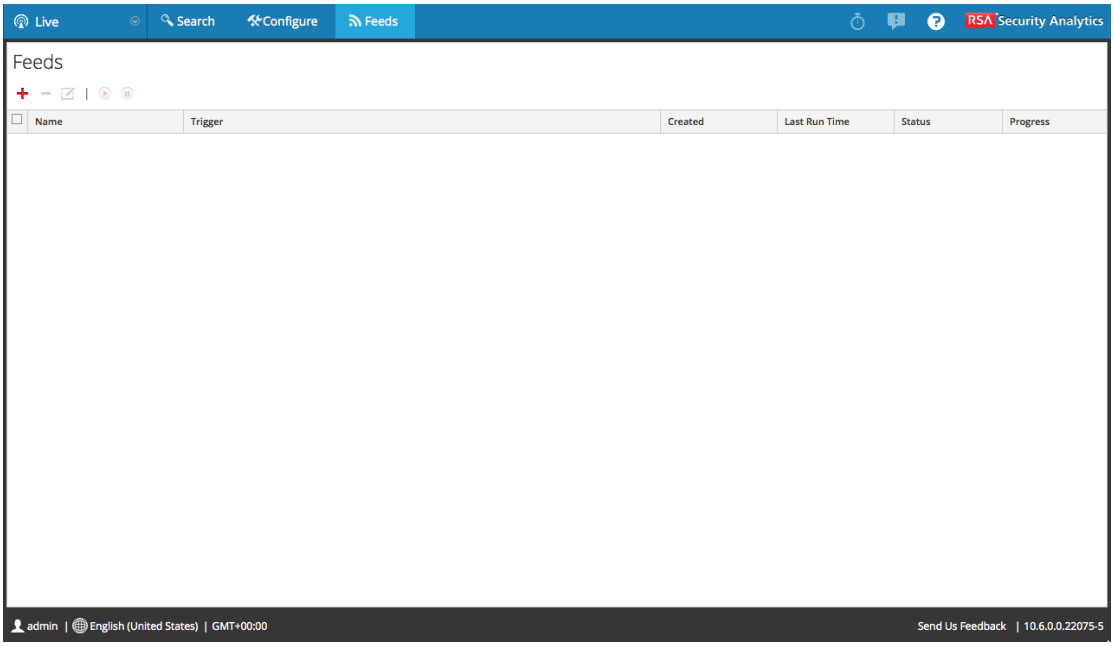
Si se realiza este procedimiento, se logrará:

- La apertura de un feed personalizado existente.
- La descarga o la edición del feed (formato **.zip**) o del archivo que se usó para crear el feed (**.csv** o **.xml**).
- La nueva creación del feed con el archivo actualizado y las nuevas especificaciones del feed.

#### Para editar un feed existente:

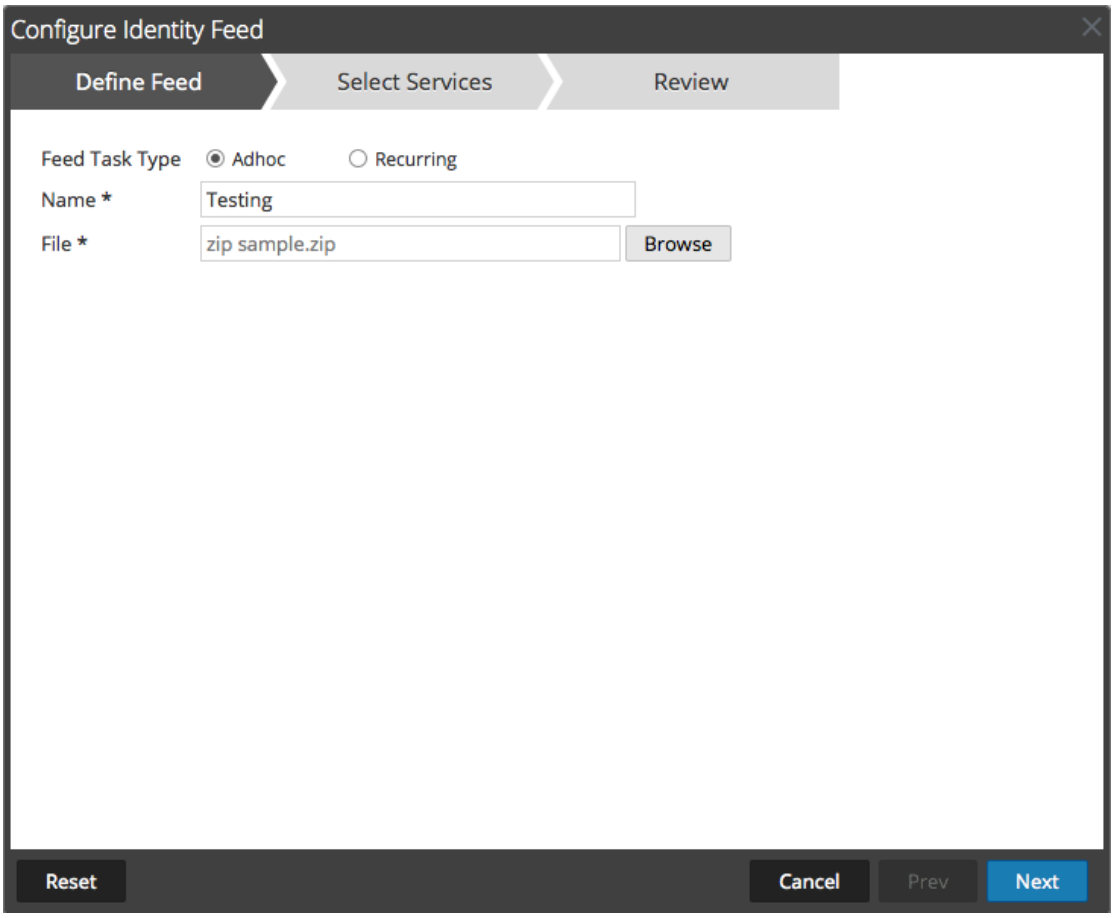
1. En el menú de **Security Analytics**, seleccione **Live > Feeds**.

   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.

   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 agrega a la lista de feeds y la barra de progreso muestra 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 cuadrícula Feed. Puede expandir o contraer la entrada para ver cuántos servicios se incluyeron y cuáles se ejecutaron correctamente.

## Usar analizadores personalizados

En este tema se proporcionan instrucciones para usar analizadores personalizados en RSA Security Analytics.

RSA Security Analytics tiene la capacidad de cargar analizadores desde el sistema local y eliminar estos analizadores.

### Procedimientos

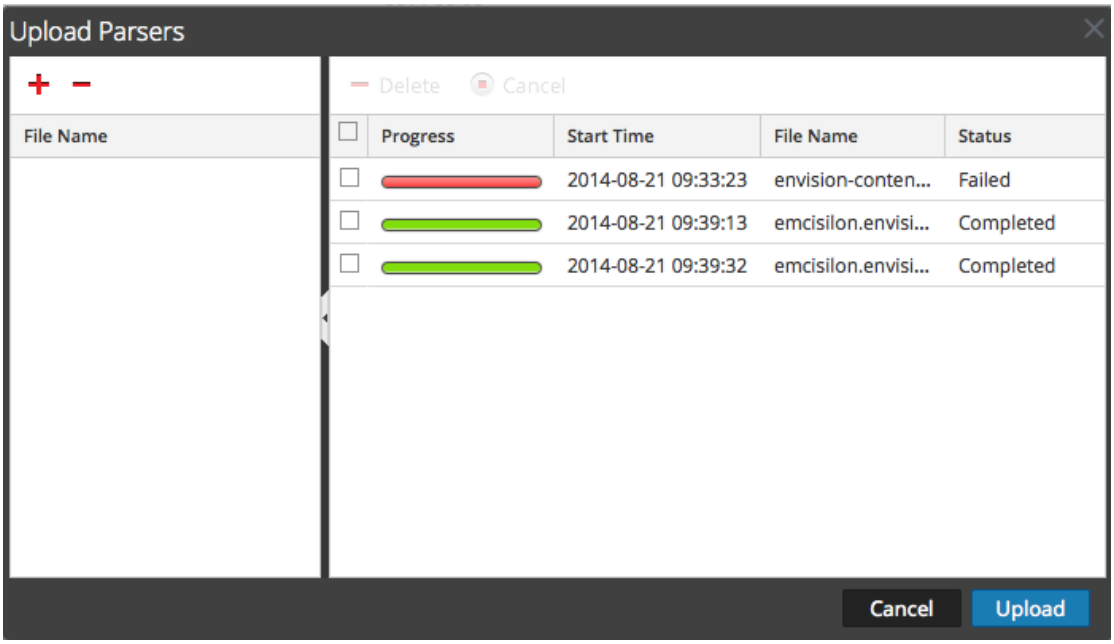
#### Cargar analizadores a un Decoder o Log Decoder

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 cuadrícula Archivo, puede preparar una lista de analizadores 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.

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **> Ver > Configuración.**
   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Analizadores**.

4. Haga clic en Upload.

   Aparecerá el cuadro de diálogo Cargar analizadores.

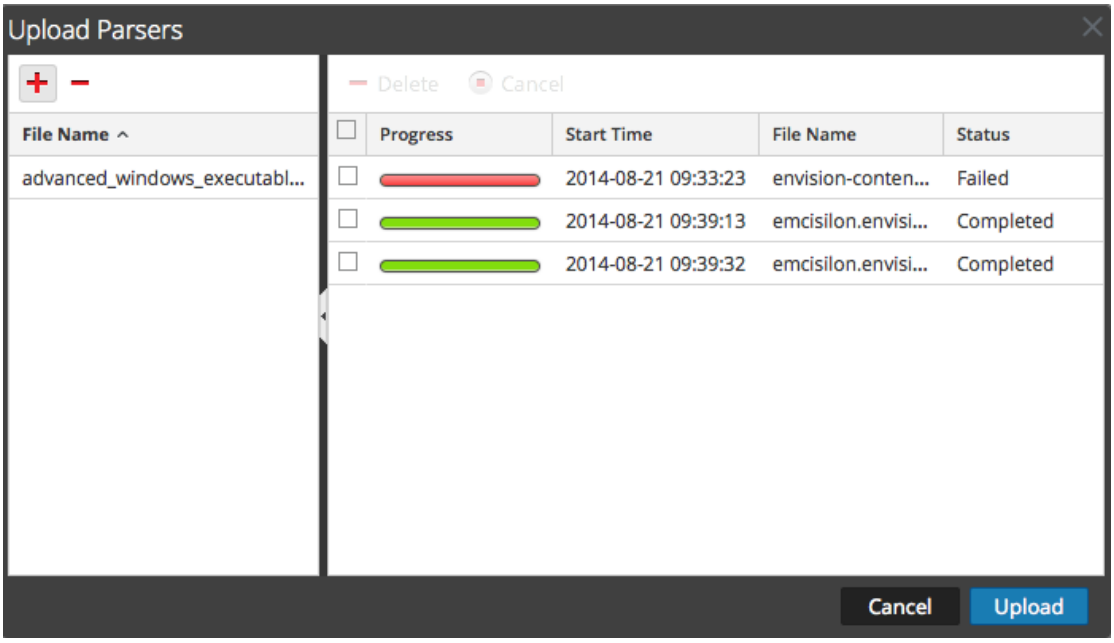



5. Haga clic en .

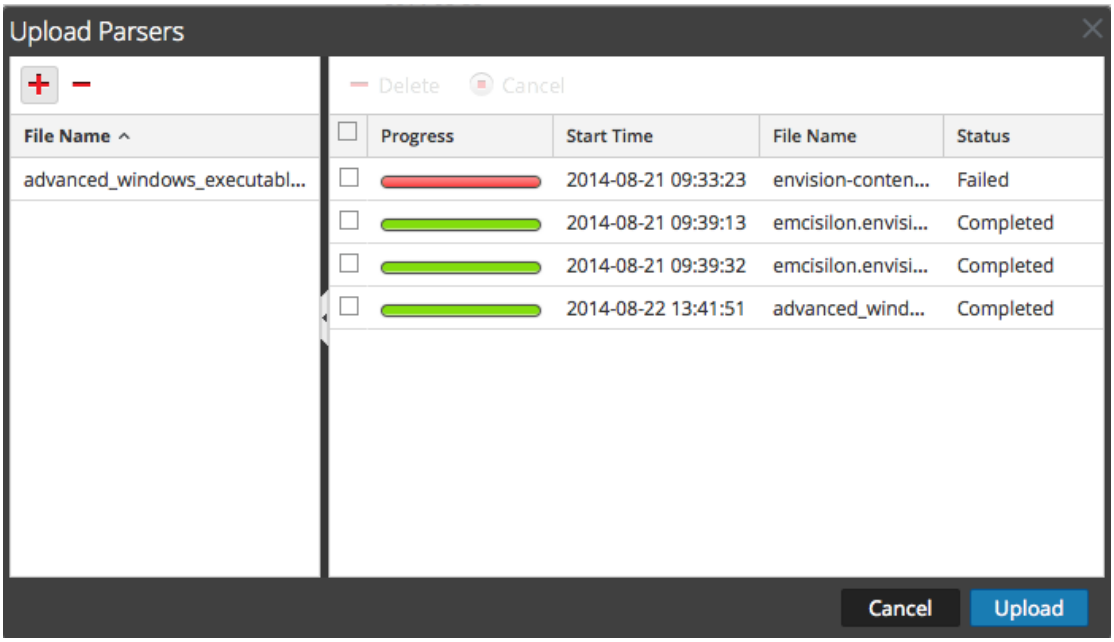
   Aparece un cuadro de diálogo de selección de archivo.

6. 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 cuadrícula Archivo.



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




8. 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 está en línea de espera o en curso, 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 de carga, haga clic en Delete.

### Eliminar analizadores implementados

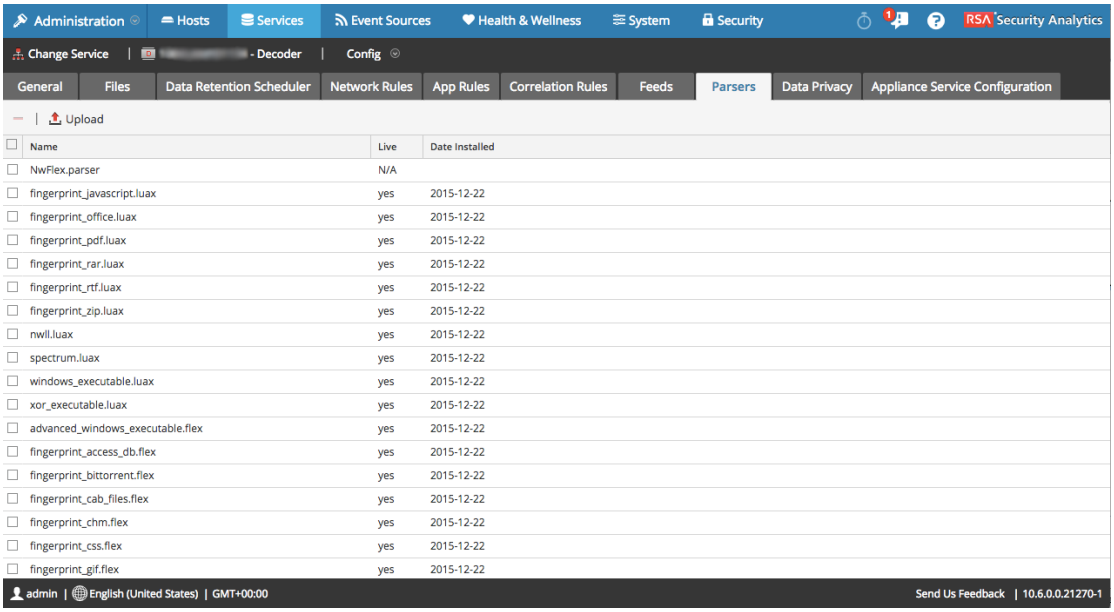
La opción **Eliminar** de la vista Configuración de servicios > pestaña Analizadores proporciona una manera de eliminar los analizadores implementados de un Decoder o Log Decoder. Es posible agregar y eliminar analizadores mientras un Decoder está en funcionamiento sin afectar la captura.

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

Para eliminar un analizador de un Decoder:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **> Ver > Configuración.**

   Se muestra la vista Configuración de servicios del servicio seleccionado.
3. Haga clic en la pestaña **Analizadores**.




4. En la pestaña **Analizadores**, seleccione uno o más analizadores para eliminar.
5. Haga clic en  .

   En un cuadro de diálogo, se solicita la confirmación de que desea eliminar los analizadores.
6. Si desea eliminar los analizadores, haga clic en **Sí**.

   Los analizadores se eliminan del Decoder inmediatamente.

# Configurar la funcionalidad 10G

En este tema se indica a los administradores cómo ajustar específicamente un Packet Decoder para la captura de paquetes a alta velocidad.

Esta guía 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 Security Analytics versión 10.6 ofrece compatibilidad con la recopilación de alta velocidad de Decoder. Puede capturar datos de paquetes de redes de mayor velocidad y optimizar su Packet Decoder para capturar tráfico de red con picos de hasta 8 Gb/s continuos y 10 Gb/s, según los analizadores y los feeds que haya activado.

RSA Security validó el análisis de contenido específico a altas velocidades. Consulte la sección Análisis a altas velocidades para obtener más información.

Para obtener información sobre cómo personalizar analizadores con contenido propio, consulte la sección Mejores prácticas de 10G .

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

Las mejoras incorporadas para facilitar la captura en estos ambientes incluyen las siguientes:

• Utilización de la funcionalidad del driver de captura **pf_ring** para aprovechar la NIC Intel 10G genérica en la captura de alta velocidad.

• Introducción de la configuración de **assembler.parse.valve**. La configuración desactiva automáticamente los analizadores de aplicación cuando se superan determinados umbrales con el fin de limitar el riesgo de pérdida de paquetes. Una vez que estos analizadores se desactivan, los analizadores de la capa de red permanecen activos. Cuando las estadísticas bajan de los umbrales superados, los analizadores de aplicaciones se vuelven a activar automáticamente.

• Introducción de la configuración de **parallel.values** en Concentrator para optimizaciones de consultas.

## Requisitos previos del hardware

- Decoder serie 4S
- Tarjeta Ethernet de fibra basada en Intel 82599, como Intel x520. Todas las tarjetas 10G que proporciona RSA cumplen con este requisito. Se pueden utilizar varios puertos en una única tarjeta 10G, pero no se admite la combinación de 10G con una tarjeta 1G.

- 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 el 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.

## Requisitos previos del software

- Paquete de kernel de Linux obtenido de RSA. Solo son compatibles los paquetes de kernel de Linux que proporciona RSA.
- Paquete de pfring que coincide con el kernel instalado actualmente. La versión del kernel debe coincidir exactamente con la versión de pfring.

## Instalación de Decoder 10G

Realice los siguientes pasos para instalar Decoder 10G de Security Analytics 10.6:

### Requisitos previos

• Plataformas SA-S4H-P-DEC o SMC-S4H-P-DEC basadas en la plataforma Dell R620

• NIC SMC-10GE-* Intel 520 10G instalada (disponible en RSA)

• Packet Decoders actualizados a 10.6

• Cada Packet Decoder configurado como mínimo con dos DAC o conectividad SAN.

**Nota:** Consulte Consideraciones de almacenamiento en este documento antes de realizar la actualización, ya que puede ser necesario un recableado físico.

• Dell R620 BIOS v1.2.6 o superior. 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.

**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. Es importante actualizar el BIOS antes de instalar paquetes, ya que estos usan información que proporciona el BIOS para inicializar el sistema.

## Consideración de análisis y contenido para la captura de paquetes

La captura y la ejecución de enriquecimiento contra paquetes crudos pueden presentar retos únicos a cualquier velocidad de captura. A mayores velocidades de sesiones y paquetes en 10G, la eficiencia del análisis es primordial. Un único analizador puede tener un efecto perjudicial en el sistema y generar finalmente pérdidas de paquetes. Las pruebas realizadas para la captura 10G incluyeron analizadores de base y combinaciones de feeds, reglas y otro contenido accesibles mediante RSA Live. Tanto para un cliente que actualiza un sistema actualmente implementado como para uno que 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.

## Mejores prácticas de 10G

1. 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.

2. Cuando agregue analizadores adicionales, agregue solo uno o dos por vez.

3. 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, deshabilite 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 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

## Instrucciones de instalación del BIOS

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 Red Hat Linux.

3. Copie el archivo en el servidor de Security Analytics.

4. Inicie sesión como **raíz**.

5. Cambie los permisos en el archivo a ejecutar.

6. Ejecute el siguiente archivo:

./BIOS_V7P04_LN_2.2.3.BIN

7. Cuando la operación finalice, el sistema solicitará un reinicio.

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

## Actualizar Decoder 10G

1. Actualice el dispositivo Decoder a la versión 10.6, incluidos todos los parches del SO. La versión mínima del parche de seguridad aplicado es RSA Security Analytics versión 10.6. Esta versión requiere el paquete de kernel de Linux:

`kernel- 2.6.32-573.12.1.el6.x86_64`, que corresponde a la versión del kernel de RSA Security Analytics versión 10.6.

2. Asegúrese de que las versiones de kernel, pfring y numactl sean las siguientes:

- `kernel- 2.6.32-573.12.1.el6.x86_64`
- `pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`
- `numactl-2.0.9-2.el6 .x86_64.rpm`

## Instalar Decoder 10G

Descargar la versión más reciente del paquete pfring rpm desde smcupdate

`pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`

Para obtener más información, consulte RSA SecurCare: https://knowledge.rsasecurity.com.

2. Mediante el protocolo SSH, instale los paquetes con el siguiente comando cuando los archivos se hayan copiado con scp en Decoder:

rpm -ivh pfring*

**Nota:** NOTA: asegúrese de realizar las siguientes comprobaciones:

a. Compruebe el **rpm el6** mediante el siguiente comando:

`rpm -qa |grep numactl*`

b. Compruebe para asegurarse de que la versión sea `numactl-2.0.9-2.el6 .x86_64.rpm`

**Nota:** Si el paso de actualización anterior se realiza antes de la actualización del BIOS, es necesario realizar los siguientes pasos:

- Desinstale los paquetes mediante el comando **rpm –e**.

• Actualice el BIOS a v2.2.3

• Ejecute comandos rpm para volver a instalar los paquetes necesarios.

3. Asegúrese de que las versiones de **kernel**, **pfring** y **numactl** sean las siguientes:

• `kernel- 2.6.32-573.12.1.el6.x86_64`

• `pfring-6.0.3-8598.2.6.32.573.12.1.el6.x86_64.rpm`

• `numactl-2.0.9-2.el6 .x86_64.rpm`

4. Reinicie el dispositivo Decoder (se requiere un reinicio completo del sistema para asegurarse de que los controladores pf_ring se carguen correctamente).

5. Cuando Decoder se reinicia, puede verificar si la instalación se realizó correctamente si ve interfaces **PFRINGZC adicionales** disponibles en las opciones de Interfaz de captura seleccionada (se muestra a continuación).

## Configurar Decoder 10G

Después de la actualización, realice los siguientes pasos para configurar Decoder 10G:

1. En la vista Explorador de 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

3. En la vista Explorador de 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 que se muestran en la siguiente captura de pantalla:

`update=1 op=10g`

5. Seleccione el adaptador de puertos de captura. Las opciones incluyen:

a. Captura de un único puerto: **PFRINGZC,p1p1 o PFRINGZC,p1p2**

b. Captura de ambos puertos:

i. **Seleccione PFRINGZC,P1P1**

ii. En la vista Explorador, configure **capture.device.params = device=zc:p1p2,zc:p1p1**

c. Asegúrese de que el hardware de captura seleccionado esté en el nodo NUMA correcto.

Desde una sesión del protocolo SSH al dispositivo, ejecute la siguiente declaración:

**cat /sys/class/net/<interface_name>/device/numa_node**

donde **<interface_name>** es la interfaz de captura seleccionada (por ejemplo, **p1p1**).

Si el resultado es **0** (cero), no se requiere ninguna configuración adicional.

Si no es así, agregue el resultado como el parámetro core a los parámetros de captura, como se muestra a continuación:

**/decoder/config/capture.device.params: core=1**

Este cambio requiere el reinicio del servicio.

**Nota:** NOTA: según la configuración de hardware, los puertos de captura se pueden identificar con un nombre distinto de **p1p1/p1p2**, pero siempre tendrán el prefijo **PFRINGZC**. Por ejemplo, en algunos dispositivos, estos puertos se pueden identificar como **eth4 / eth5**. Para capturar desde **eth4**, seleccione **PFRINGZC,eth4**. Para capturar desde **eth5**, seleccione **PFRINGZC,eth5**.

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 buffer en la memoria a estas velocidades.

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, el ajuste **/decoder/config/assembler.parse.valve** se puede configurar en **true**. Esto dará lugar a lo siguiente:

• 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 aplicación, solo la fidelidad del análisis ejecutado en ellas.

• Las sesiones analizadas con los analizadores de aplicación deshabilitados tendrán metadatos de red asociados (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 vuelven a habilitar automáticamente.

8. El pool de sesiones del ensamblador debe ser lo suficientemente grande de modo que las sesiones no se fuercen.

• Se puede determinar si las sesiones se están forzando con la estadística **/decoder/stats/assembler.sessions.forced** (que irá en aumento) y **/decoder/stats/assembler.sessions**, que estará dentro de varios cientos de **/decoder/config/assembler.session.pool**.

• El sitio de pruebas de RSA Security usó la siguiente configuración a un poco menos de 10G:

**/decoder/config/assembler.session.pool se configuró en 1,000,000**

y **/decoder/stats/assembler.sessions** promediaría 630,000.

Se puede usar un método alternativo a los pasos del 1 al 4 enumerados anteriormente para configurar Decoder 10G mediante la ejecución de los pasos 1, 2, 3 y 4 que se explican a continuación. Si se usa este método, los pasos del 5 al 8 enumerados anteriormente son obligatorios.

1. Actualice la configuración de pools de sesiones y paquetes a los siguientes valores (bajo **/decoder/config**):

a. **pool.packet.pages = 1000000**

b. **pool.session.pages = 300000**

2. El tamaño del bloque de escritura de paquetes bajo (**/database/config/packet.write.block size**) se debe configurar exactamente en 4 GB o, para la versión 10.6+, se debe usar **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. Actualice la configuración de los hilos de ejecución de análisis a los siguientes valores (bajo **/decoder/config**).

a. **parse.threads =12**

4. Seleccione el adaptador de puertos de captura. Las opciones incluyen:

a. Captura de un único puerto: **PFRINGZC,p1p1** o **PFRINGZC,p1p2**

b. Captura de ambos puertos:

i. Seleccione **PFRINGZC,P1P1**

ii. En la vista Explorador**, configure set capture.device.params = capture=zc:p1p2,zc:p1p1**

**Nota:** según la configuración de hardware, los puertos de captura se pueden identificar con un nombre distinto de **p1p1/p1p2**, pero siempre tendrán el prefijo **PFRINGZC**. Por ejemplo, en algunos dispositivos, estos puertos se pueden identificar como **eth4 / eth5**. Para capturar desde **eth4**, seleccione **PFRINGZC,eth4**. Para capturar desde **eth5**, seleccione **PFRINGZC,eth5**.

## 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. A continuación, se describen las opciones compatibles para configuraciones de DAC y SAN.

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

La unidad principal de Decoder está equipada con una tarjeta controladora SAS de RAID por hardware que proporciona conectividad a la DAC. En la configuración de la mayoría de las implementaciones, las DAC están conectadas en serie a un único puerto de la tarjeta SAS. Para lograr compatibilidad con ambientes de mayor velocidad, se requiere un mínimo de dos DAC por Decoder y cada una debe estar conectada directamente a la tarjeta SAS. Para ajustar dos DAC, conecte la primera a un puerto de la tarjeta SAS y, a continuación, conecte otra 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 los I/O de escritura de captura de los I/O de lectura necesarios para cumplir con solicitudes de contenido de paquetes.

## Uso del almacenamiento SAN

Decoder permitirá cualquier configuración de almacenamiento que pueda cumplir con el requisito de rendimiento continuo. Tenga en cuenta que el vínculo FC de 8 Gbit estándar a una SAN no es suficiente para leer y escribir datos de paquetes a 10G, razón por la cual es necesario que los ambientes que utilizan una SAN configuren la conectividad a esta mediante el uso de varios vínculos FC.

## Agregación de un Decoder 10G a otros componentes de Security Analytics

La versión inicial ofrece compatibilidad con la agregación desde Packet Decoder a Concentrator. Se espera que las implementaciones que usan Malware Analytics, Event Stream Analysis, Warehouse Connector y Reporting Engine afecten el rendimiento y puedan causar una pérdida de paquetes. Debido al alto volumen de tasas de sesiones, se recomienda aplicar los siguientes cambios en la configuración:

• Una agregación de tipo nice en Concentrator limitó el impacto en el rendimiento en Decoder 10G

/concentrator/config/aggregate.nice = true

• Debido al alto volumen de sesiones en Concentrator, puede considerar la activación del modo “valores paralelos” en Concentrator con la configuración de `/sdk/config/parallel.values` en true. Esto mejorará el rendimiento de las investigaciones cuando la cantidad de sesiones por segundo sea mayor que 30,000.

• Se requerirá una revisión adicional del contenido y el análisis en aquellas implementaciones en las cuales se desee el uso de otros componentes de SA (es decir, Warehouse, Malware Analysis, ESA y Reporting Engine).

Un Decoder 10G puede gestionar la agregación a un único Concentrator mientras se ejecuta a velocidades de 10G.

1. Concentrator agrega entre 45,000 y 70,000 sesiones/s.
2. 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.
3. Active la agregación de tipo nice en Concentrator para limitar el impacto en el rendimiento en el Decoder
   **/concentrator/config/aggregate.nice=true**
4. Debido al alto volumen de sesiones en Concentrator, puede considerar la activación del modo **valores paralelos** en Concentrator con la configuración de **/sdk/config/parallel.values** en **true**. Esto mejorará el rendimiento de las investigaciones cuando la cantidad de sesiones por segundo sea mayor de 30,000.

Si se requieren múltiples flujos de agregación, la agregación desde el Concentrator tendría un menor impacto en el Decoder.

## Análisis a altas velocidades

Obviamente, 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 ejecución correcta, se debe agregar contenido de Live de manera muy lenta, en especial los analizadores. Los analizadores pueden afectar considerablemente el rendimiento. Las siguientes son algunas reglas generales:

### Contenido de Live probado

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

- Contenido de MA (siete analizadores Lua, un feed y una regla de aplicación)
- Cuatro 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 inhabilitado 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, este analizador se puede usar en lugar del nativo sin pérdidas (además de la lista anterior). xor_executable llevará el CPU de análisis al 100 % y puede haber pérdidas significativas en el sistema en ese momento debido al respaldo del análisis.

# Configurar el reenvío de syslog a un destino

En este tema se proporcionan instrucciones para reenviar mensajes de syslog recopilados desde un Log Decoder a otro receptor de syslog.

Además de recopilar mensajes de syslog, puede configurar Log Decoder para que reenvíe los mensajes de syslog a otro receptor de syslog. Security Analytics 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**.

## Requisitos previos

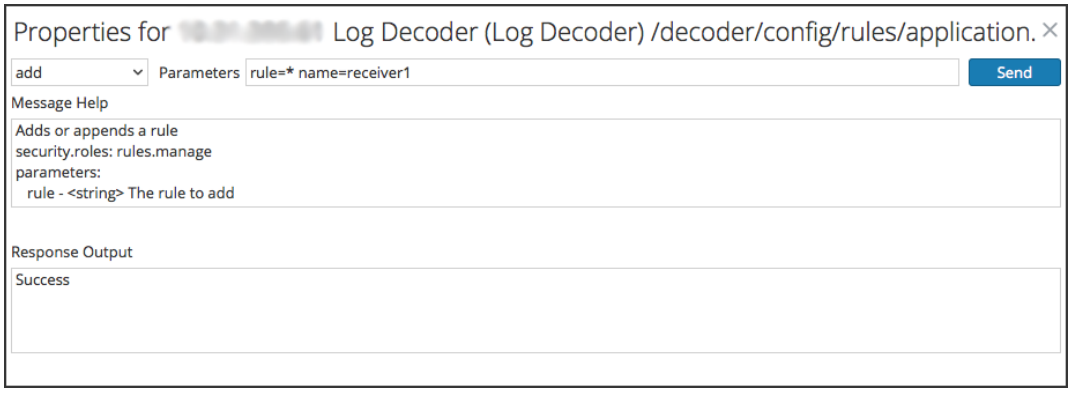
Log Decoder debe estar en el estado **Iniciado**.

## Procedimiento

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 Security Analytics la instrucción de reenviar los mensajes:
   a. Seleccione un Log Decoder en la vista **Servicios** y elija  **> 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=receiver1**)

d. Haga clic en **Enviar**.




Security Analytics crea la regla **name=receiver1 rule=* order=<n>**. Security Analytics 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.


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** en la columna **Acciones**.

b. 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**

| | |
|---|---|
| logs.forwarding.destination | receiver1=tcp:10.31.244.44:514 receiver2=tcp:10.31.244.46:514 receiver3=tcp:10.31.244.48:514 |

**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 el tema **Configurar certificados** de la *Guía de configuración de la recopilación de registros* para obtener información sobre la manipulación del almacén de confianza de CA de Log Decoder.

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

| | |
|---|---|
| logs.forwarding.enabled | true |

### Tema relacionado

- Configurar reglas de aplicaciones

# 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 con el fin de investigar y analizar los registros y los 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. Asegúrese de seleccionar el archivo index.decoder.xml cuando cree metadatos personalizados en el Decoder.

## Procedimiento

### Agregar la clave de metadatos personalizados en Log Decoder

Para agregar claves de metadatos personalizados mediante un feed personalizado:

1. En el menú de **Security Analytics**, seleccione **Administration** > **Servicios** > **Log Decoder.**
2. Seleccione un servicio y haga clic en  > **Ver** > **Configuración** > pestaña **Archivos** > **index-logdecoder-custom.xml.**

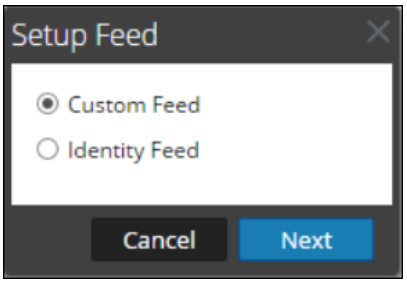
```
<Language>
  <?xml version="1.0" encoding="utf-8"?>
  <Language level="IndexNone" defaultAction="Auto">
  <!-- Reserved Meta key for Feed -->
  <Key description="Source Location" level="IndexNone"
name="location.src" format="Text"/>
 </Language>
```

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

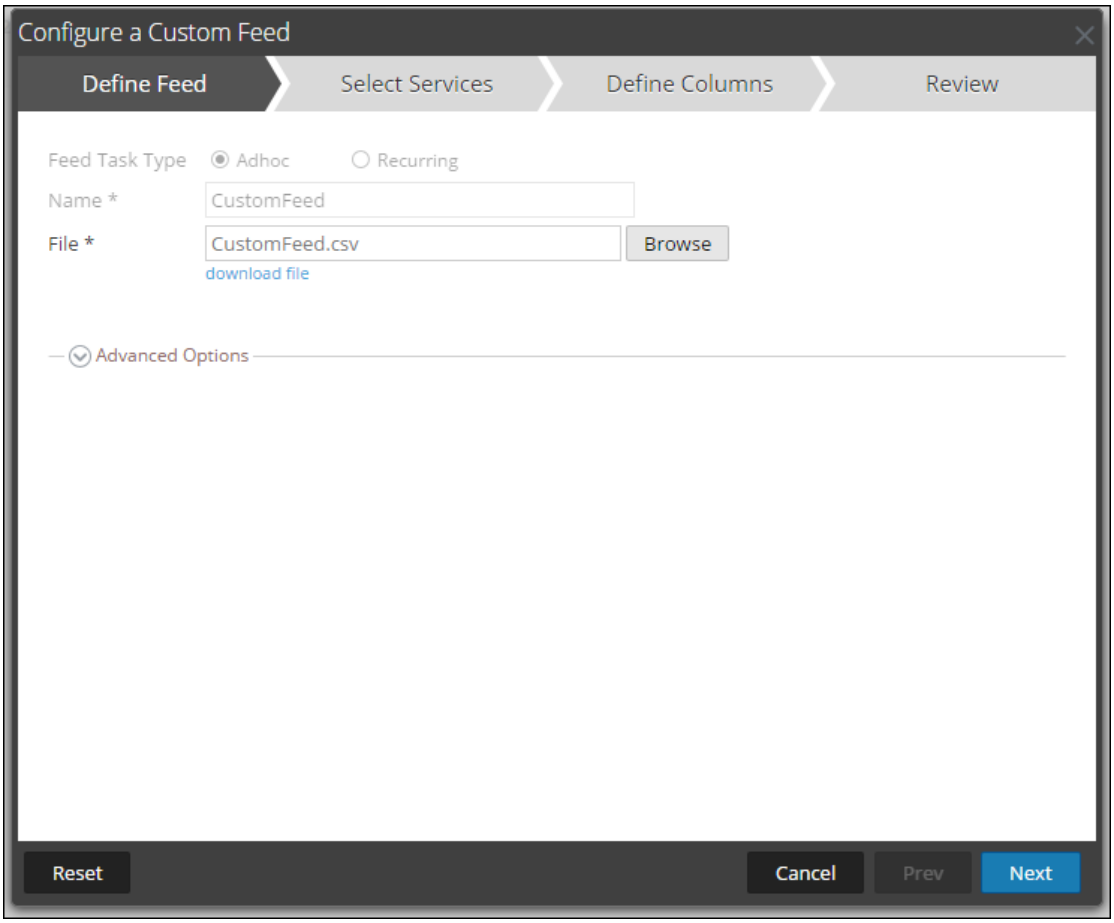
### Implementar el feed en Live

Para implementar el feed en el ambiente Live:

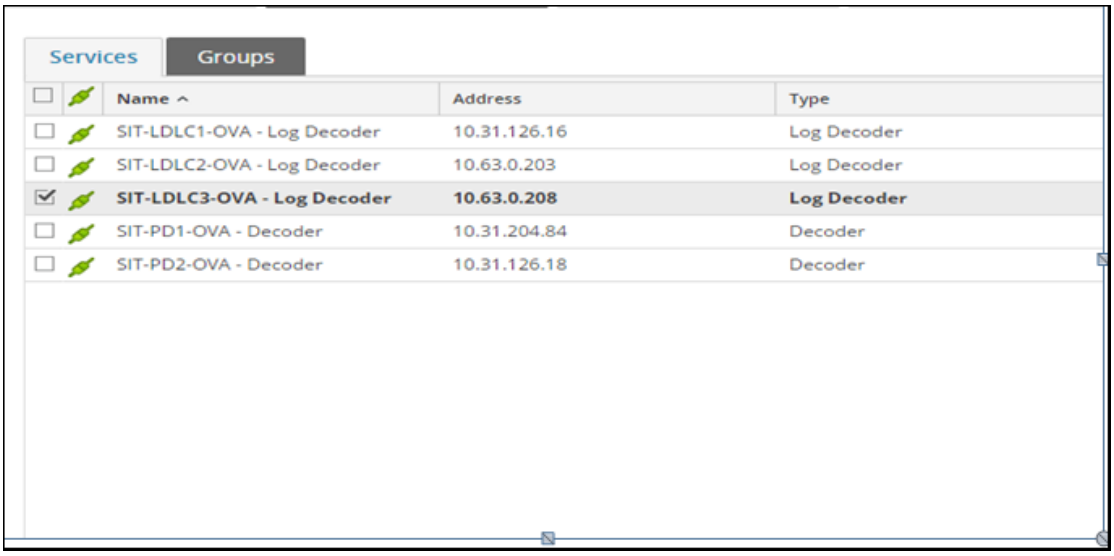
1. En el menú de **Security Analytics**, seleccione **Live** > **Feed.**
2. En la barra de herramientas, haga clic en +.
   Se muestra el cuadro de diálogo Configurar feed.




3. Para seleccionar el tipo de feed, haga clic en **Feed personalizado** y, a continuación, en **Siguiente**.
   El asistente Configurar un feed personalizado se muestra con el formulario Definir feed abierto.
   Ingrese el nombre y cargue el archivo CSV del feed.

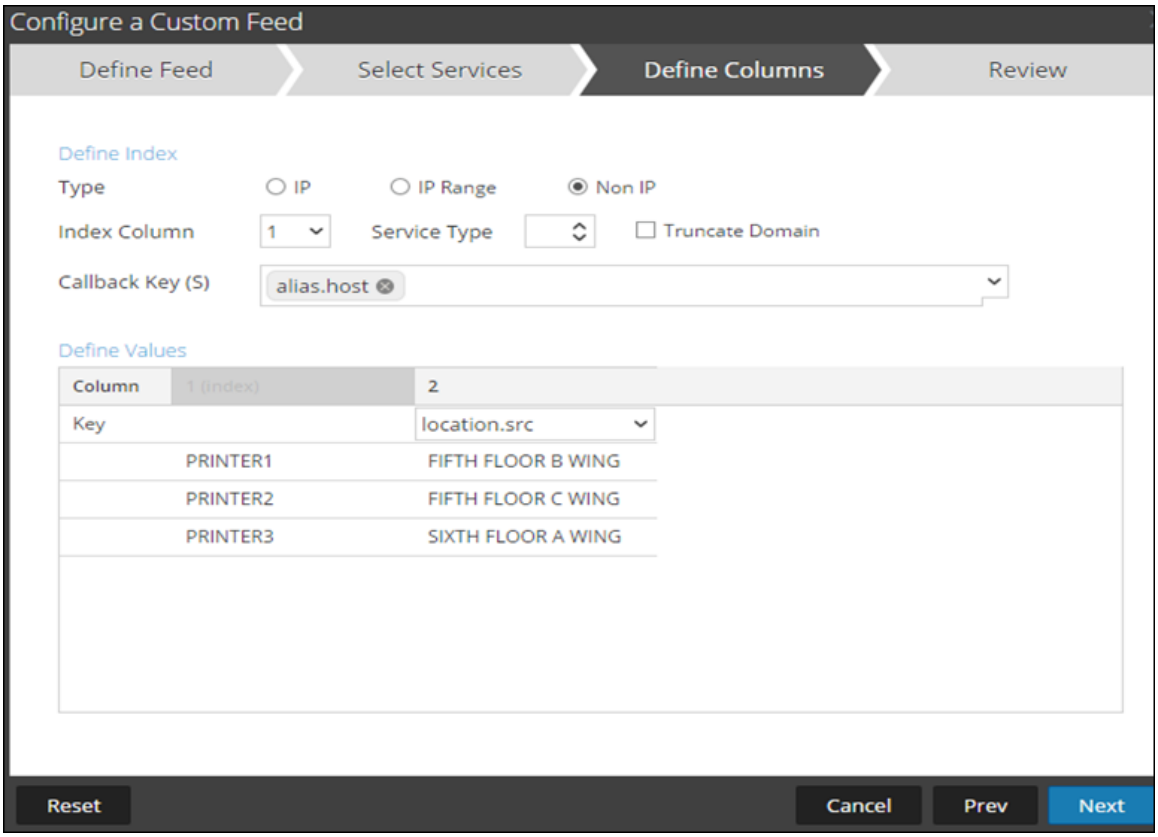


4. Haga clic en **Siguiente**.
5. Seleccione el servicio **Log Decoder** en el cual se debe cargar el feed.




6. En la sección Definir índice, seleccione el tipo de índice, la columna de índice y la clave de callback. En la sección Definir valores, ingrese la clave de metadatos personalizados.
   El contenido del archivo .csv se muestra en el asistente de feed. En este caso, la primera columna muestra el nombre de host del recurso y la segunda, la ubicación del recurso.

**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". Por lo tanto, seleccione "alias.host" como clave de callback 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.

7. Haga clic en **Siguiente**.
8. Haga clic en **Terminar**.

Para obtener más información sobre el asistente de feed, consulte Crear e implementar feeds personalizados con el asistente.

### Agregar la entrada 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. En el menú de **Security Analytics**, seleccione **Administration** > **Servicios** > **Concentrator**.
2. Haga clic en > **Ver** > **Configuración** > pestaña **Archivos** > **index-concentrator-custom.xml.**
3. Agregue la entrada 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. Reinicie los servicios Concentrator. En la vista Servicios, haga clic en  > **Reiniciar**.

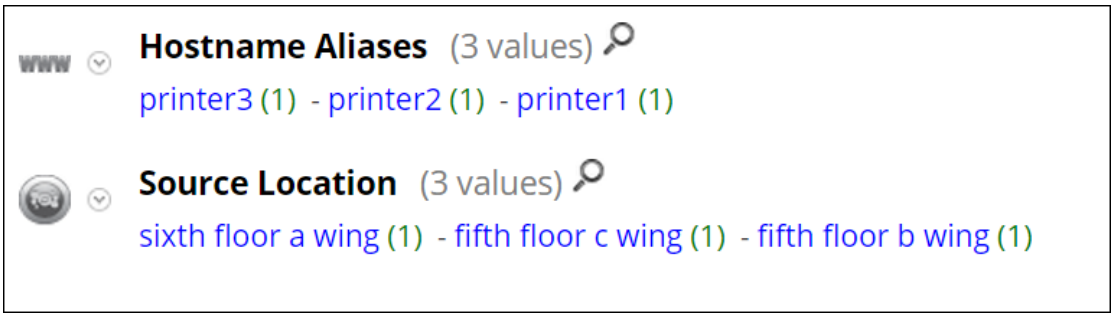
**Nota:** En el caso de Broker, el Broker deriva su índice del Concentrator desde el cual realiza la agregación. Por lo tanto, no es necesario crear metadatos personalizados en el Broker. Si no indexó la clave de metadatos en el Concentrator, el Broker no se mostrará en Investigation.

### Investigar

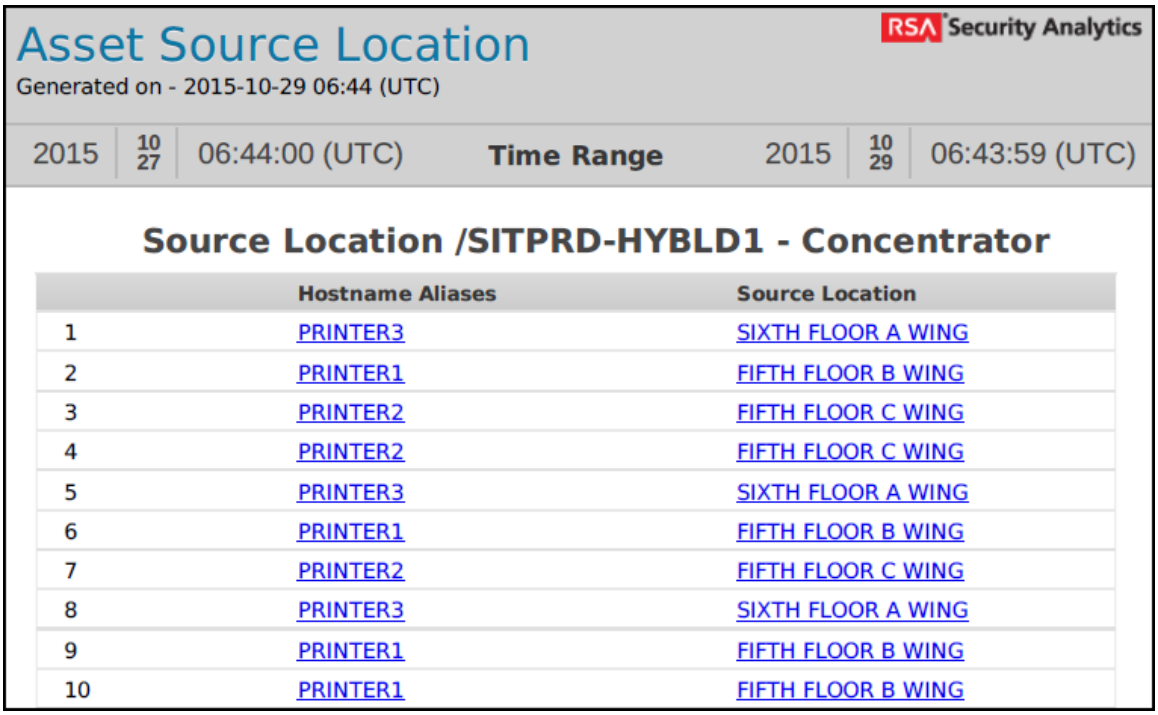
**Nota:** Debe cerrar e iniciar sesión en la interfaz del usuario de Security Analytics para poder ver la clave de metadatos personalizados en Investigation.

Para investigar con la clave de metadatos personalizados:

1. En el menú de **Security Analytics**, seleccione **Investigation** > **Navegar**.
2. Seleccione un servicio Concentrator.
3. 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

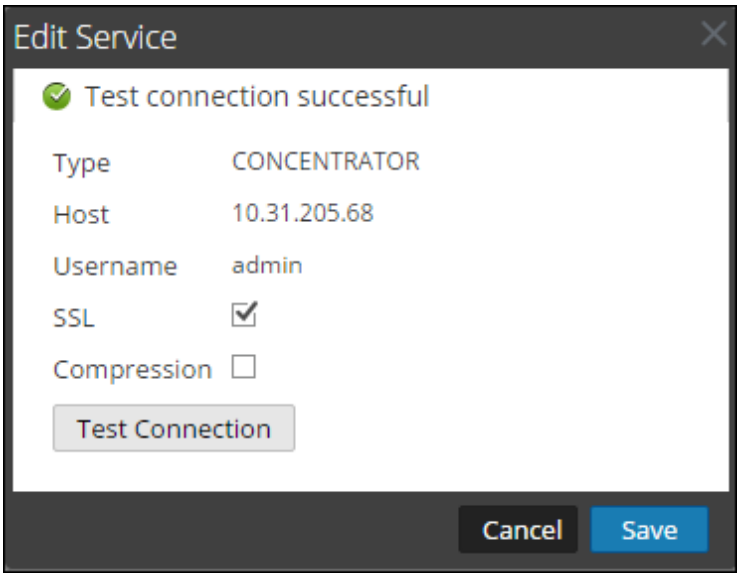
Se deben ejecutar los siguientes procedimientos si Warehouse Connector, Archiver, Reporting Engine y ESA están configurados.

**Actualizar el esquema en ESA**

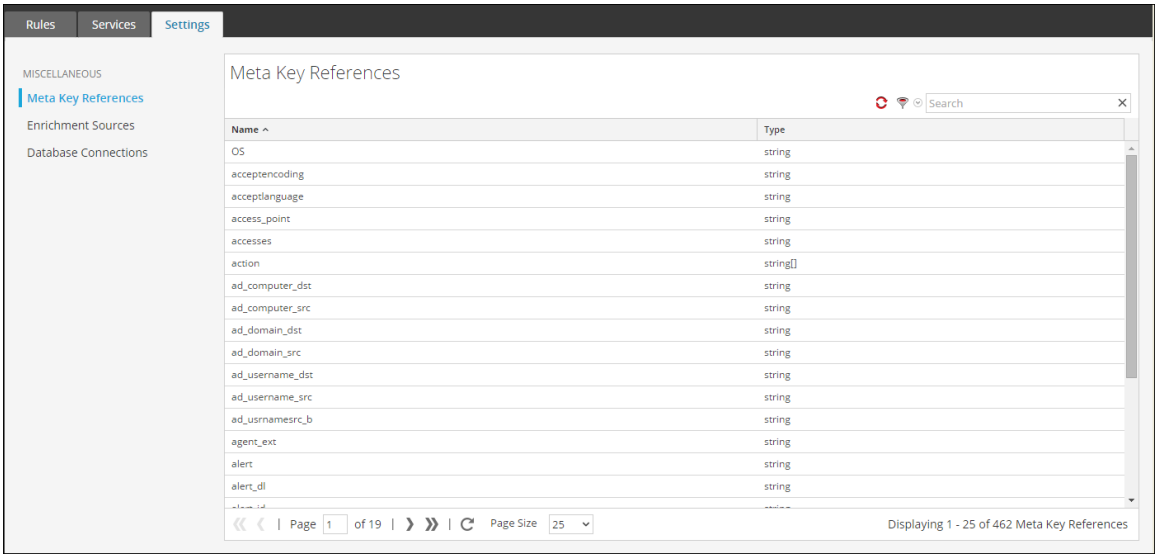
Antes de actualizar el esquema en ESA, la clave de metadatos personalizados se debe indexar en el Concentrator.

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

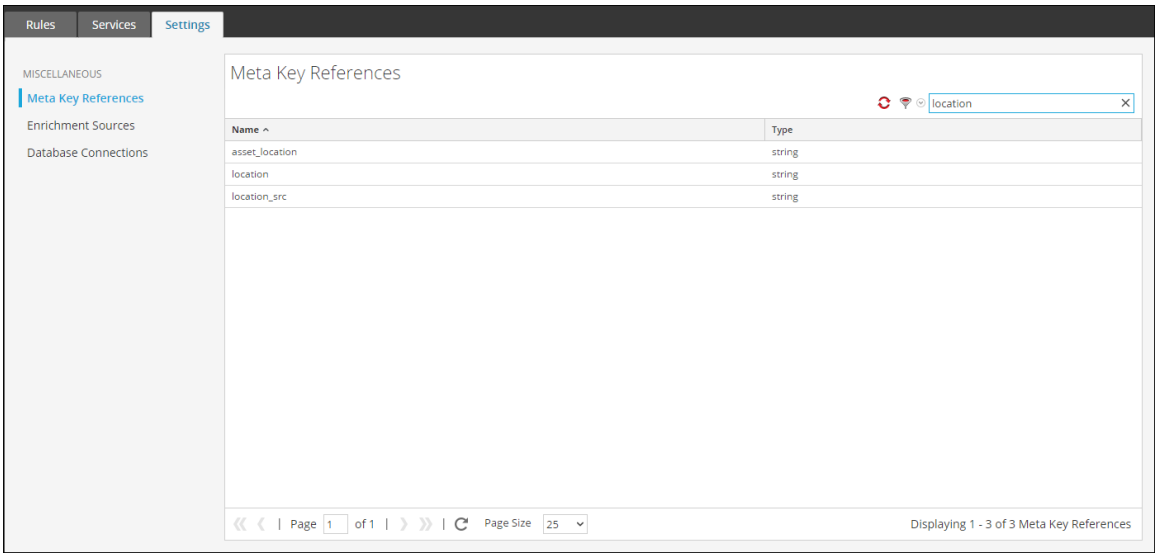
1. En el menú de **Security Analytics**, seleccione **Administration** > **Servicios** > **ESA - Event Stream Analysis** > **Ver** > **Configuración**.
2. Edite el origen de datos de Concentrator.
3. Haga clic en **Probar conexión**.




4. Haga clic en **Guardar** una vez que la conexión se haya establecido correctamente.
5. Haga clic en **Aplicar**.
6. Navegue a **Alertas** > **Configuración** > **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 Security Analytics 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. En el menú de **Security Analytics**, seleccione **Administration** > **Servicios** > **Archiver**.
2. Haga clic en > **Ver** > **Configurar**> **Archivos** > **index-archiver-custom.xml**.
3. Agregue la entrada 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. Reinicie el servicio Archiver. Haga clic en > **Reiniciar.**

   El esquema de Archiver se actualiza con la clave de metadatos personalizados.

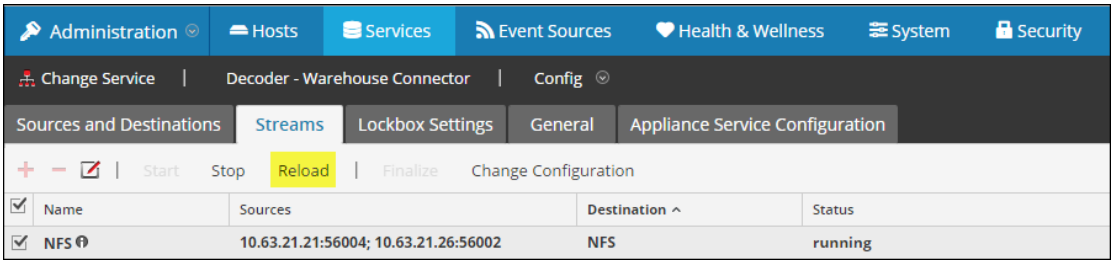
### Actualizar el esquema en Warehouse Conector

Si desea configurar Security Analytics Warehouse con metadatos personalizados y utilizarlos en el informe de Warehouse, debe actualizar el esquema de Warehouse 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 Conector.

Para actualizar el esquema de Warehouse en Reporting Engine:

1. En el menú de **Security Analytics**, seleccione **Administration** > **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 el tema **Configurar flujos** de la *Guía de configuración de Warehouse Connector*.

**Actualizar el esquema en Reporting Engine**

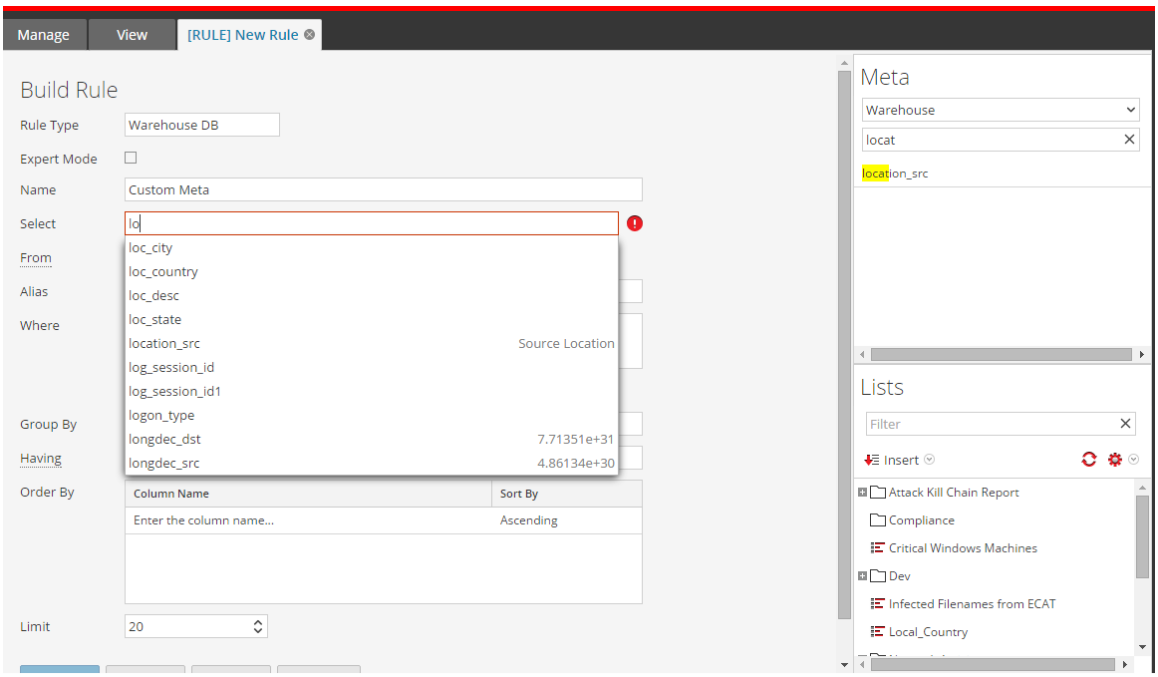
Para actualizar el esquema en Reporting Engine:

1. En el menú de **Security Analytics**, seleccione **Administration**> **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 **Informes** > **Reglas**.
2. En la barra de herramientas, haga clic en .
3. Seleccione la base de datos de Warehouse.
4. En la página Crear regla, busque los metadatos personalizados en el panel derecho de la página.
   Se muestra la clave de metadatos personalizados.


Manage
View
[RULE] New Rule
Build Rule
Rule Type
Warehouse DB
Expert Mode
Name
Custom Meta
Select
lo
From
Alias
Where
loc_city
loc_country
loc_desc
loc_state
location_src
Source Location
log_session_id
log_session_id1
logon_type
longdec_dst
7.71351e+31
longdec_src
4.86134e+30
Group By
Having
Order By
Column Name
Sort By
Enter the column name...
Ascending
Limit
20
Meta
Warehouse
locat
location_src
Lists
Filter
Insert
Attack Kill Chain Report
Compliance
Critical Windows Machines
Dev
Infected Filenames from ECAT
Local_Country

# Acceder a 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, los mensajes que son comunes a los mismos tipos de orígenes de eventos se clasifican de forma equívoca. 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.

## Procedimientos

### Habilitar un mapeo de dirección IP a origen de eventos

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

1. En el menú de Security Analytics, seleccione **Administration > Sistema > Mapeos de analizadores de registros**.
2. Seleccione un Log Decoder y elija  **Ver > Configuración**.
   La pestaña Mapeo de analizadores 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. En el menú de Security Analytics, seleccione **Administration > 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 evento**, 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 evento**, ingrese el tipo de origen de eventos.
  Por ejemplo:`apache,sap,aix`

**Un Host, un Log Collector y un tipo de origen 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 evento**, 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 evento**, 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.

6. Haga clic en **Aceptar**.

   El mapeo de analizadores se agrega.

7. Para aceptar la selección de mapeos de analizadores, haga clic en **Aplicar**.
8. Para cancelar la selección de mapeos de analizadores, haga clic en **Revertir**.

### Leer mapeos de dirección IP a tipo de origen de eventos

Para leer mapeos de dirección IP a tipo de origen de eventos:

1. En el menú de Security Analytics, seleccione **Administration > Servicios.**
2. Seleccione un servicio Log Decoder.
3. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración de servicios.
4. 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. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Decoder.
3. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
4. Seleccione la pestaña **Mapeos de analizadores**.
5. Seleccione el mapeo que desea editar.
6. Haga clic en 
7. En el campo **Orígenes de evento**, modifique los orígenes de eventos.
8. Haga clic en **Aceptar** para aceptar el origen de eventos editado.
9. Para aceptar el origen de eventos editado, haga clic en **Aceptar**.
10. 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. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Decoder.

3. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
4. Seleccione la pestaña **Mapeos de analizadores**.
5. Seleccione el mapeo que desea eliminar.
6. Haga clic en .
   El mapeo se elimina.
7. 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:

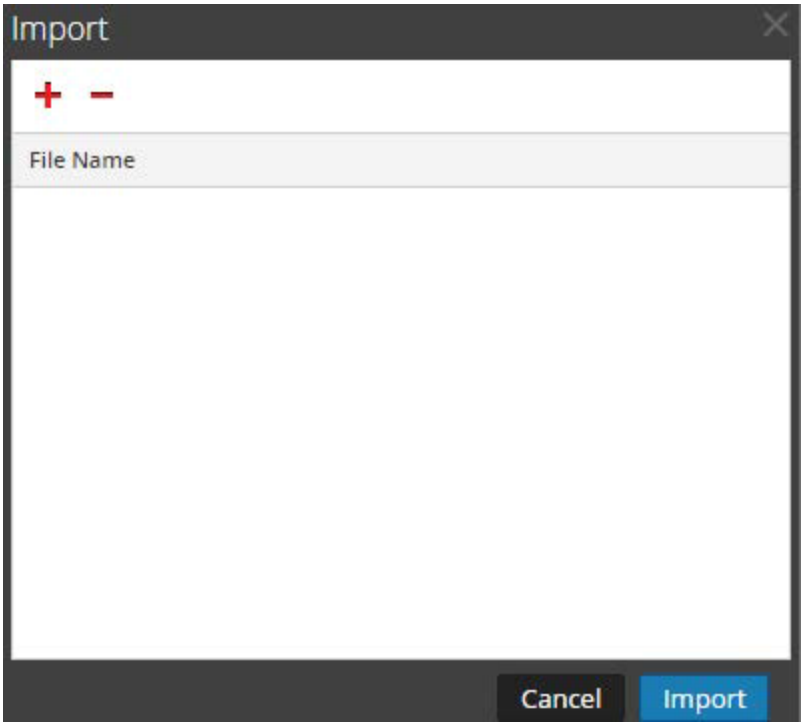
1. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Decoder.
3. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
4. Seleccione la pestaña **Mapeos de analizadores**.
5. Para ordenar una columna, haga clic 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. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Decoder.
3. En la columna Acciones, seleccione  **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
4. Seleccione la pestaña **Mapeos de analizadores**.

5. Seleccione **Acciones > Importar**.
   Se muestra el cuadro de diálogo Importar.




6. Haga clic en +.
7. Seleccione el archivo que desea importar y haga clic en **Aceptar**.
8. 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. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Decoder.
3. En la columna Acciones, seleccione **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
4. Seleccione la pestaña **Mapeos de analizadores**.
5. Seleccione los mapeos que desea exportar.

6. Seleccione **Acciones > Exportar> Selección**.
   Se muestra el cuadro de diálogo Selección de exportación.


7. 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. En el menú de Security Analytics, seleccione **Administration > Servicios**.
2. Seleccione un servicio Log Decoder.
3. En la columna Acciones, seleccione **> Ver > Configuración**.
   Se muestra la vista Configuración del servicio.
4. Seleccione la pestaña **Mapeos de analizadores**.
5. En la barra de herramientas Mapeo de analizadores, ingrese el host o el origen de eventos en el campo **Filtro**.
6. Haga clic en **Intro**.
   Se muestran los hosts o los orígenes de eventos que coinciden con los nombres ingresados en el campo **Filtro**.

## Corregir las reglas con sintaxis obsoleta

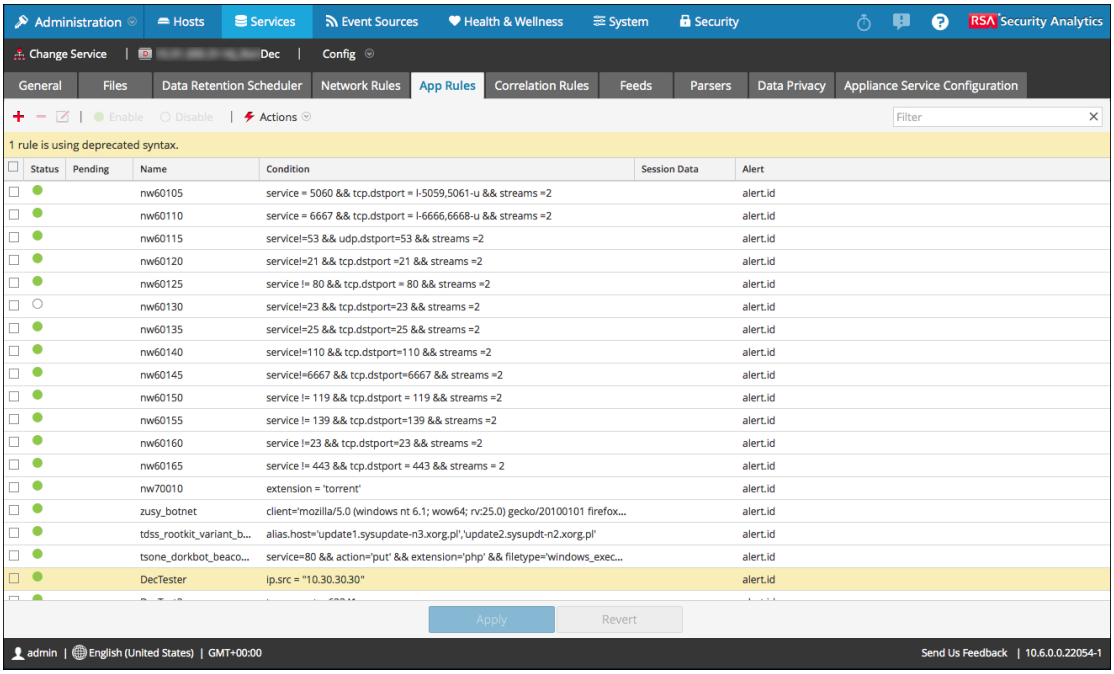
Después de una actualización a Security Analytics 10.6, la interfaz del usuario resalta las reglas con sintaxis obsoleta. Es importante corregir la sintaxis de las reglas resaltadas debido a que pueden contener sintaxis ambigua que puede generar resultados inesperados. En el Editor de regla se proporcionan mensajes de globo adicionales. Después de corregir las reglas, los elementos resaltados desaparecen.

Guía de reglas y consultas proporciona una guía que deben seguir todas las consultas y las condiciones de regla en Security Analytics. También se proporciona información sobre la configuración del modo estricto, además de sintaxis válida y obsoleta.

### Procedimiento

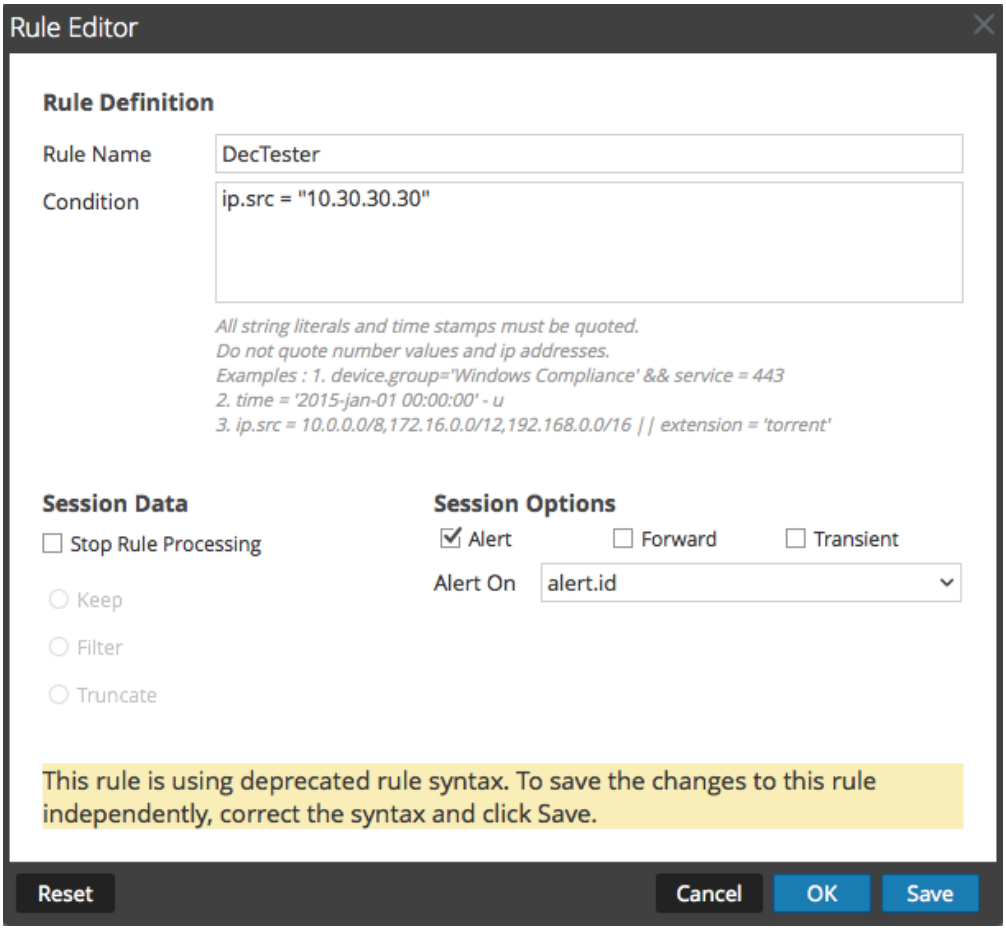
Para corregir las reglas con sintaxis obsoleta:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione un servicio Decoder y elija  **> 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.
   La pestaña Reglas correspondiente al tipo de regla seleccionado muestra la cantidad de reglas que usan sintaxis obsoleta y las reglas obsoletas están resaltadas.




4. Seleccione una regla obsoleta y haga clic en  .
   En el Editor de regla se muestra información adicional para la regla obsoleta y se 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. Guía de reglas y consultas proporciona detalles adicionales.
   Por ejemplo, si la condición de regla obsoleta 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 servicio Decoder. La regla corregida aparece sin resaltar en la pestaña Reglas.
   - Para corregir la regla y aplicarla al servicio 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 servicio Decoder.

# 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 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/Flex, estos quedan deshabilitados y no se cargan analizadores Lua/Flex.
- Si **habilita** el sistema de análisis Lua/Flex, estos quedan habilitados y los analizadores Lua/Flex individuales se habilitan y deshabilitan de acuerdo con las configuraciones individuales actuales.

## Procedimiento

Para habilitar o deshabilitar los sistemas de análisis Lua y Flex en un Decoder o un Log Decoder:

1. En el menú de **Security Analytics**, seleccione **Administration > 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 Nodos, navegue hasta **/decoder/parsers/config** y 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

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.

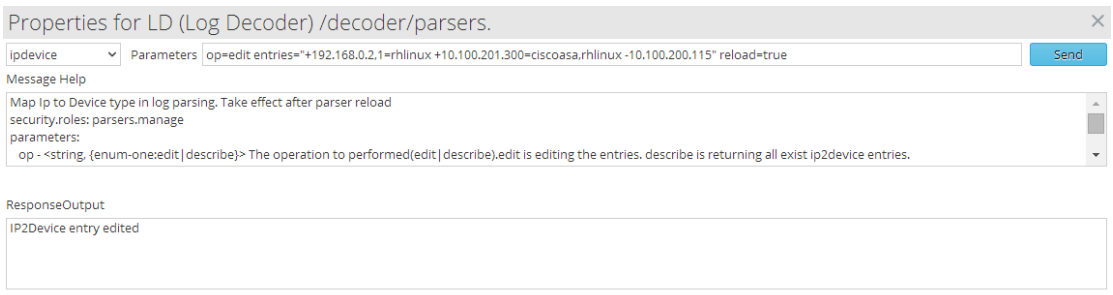
Si mapea una dirección IP a sus servicios, el Log Decoder puede identificar el servicio desde donde se genera el registro. Cuando llegan los mensajes a Log Decoder desde un servicio mapeado, se cargan los analizadores asignados para buscar coincidencias de eventos.

Puede asignar tipos de servicio a IPV4, IPV6 o el 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.

## Procedimiento

Para mapear una dirección IP a un tipo de servicio, realice lo siguiente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione un Log Decoder y, en la columna **Acciones**, elija  **> 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=edit entries="+/-ipaddress=service”reload=true` (por ejemplo, `op=edit entries="+10.100.201.300=ciscoasa" reload=true`)
5. Haga clic en **Enviar**.



#### Comando IPdevice

En el comando ipdevice, hay dos operaciones disponibles:

- Editar: puede usar esta operación para agregar y eliminar entradas en el mapa de ipdevice.
  - Para agregar una entrada, especifique:
    `+<IP value> = <service type>`
  - Para eliminar una entrada, especifique:
    -<IP value> = <service type>
- Descripción: esta operación devuelve los valores que están actualmente en el mapa de ipdevice.

#### Comando Reload

Debe volver a cargar el analizador después de editar el mapa de ipdevice mediante el comando `reload=true`. Sin embargo, esto no se debe hacer después de cada entrada, sino que solo al final de la tarea. También puede reemplazar una configuración existente mediante la edición del valor. El nuevo valor entra en vigencia después de volver a cargar el analizador.

## Resultado

Security Analytics mapea la dirección IP a los tipos de servicio en el Log Decoder.

## Ejemplos

Los siguientes ejemplos proporcionan distintas instancias para mapear direcciones IP a tipos de servicios:

- Si desea mapear dos entradas distintas con distintos valores IPV4 y tipos de servicios, ingrese el siguiente parámetro en el comando **ipdevice** y haga clic en **Enviar**.
  `op=edit entries="+10.5.245.9=ciscoasa +10.5.245.45=vmware_vcloud"`
- Si desea eliminar una entrada para un solo valor IPV4 y tipo de servicio, ingrese el siguiente parámetro en el comando **ipdevice** y haga clic en **Enviar**.
  `op=edit entries="-10.5.245.9=ciscoasa"`
- Si desea crear una sola entrada para un valor IPV6 y tipo de servicio, ingrese el siguiente parámetro en el comando **ipdevice** y haga clic en **Enviar**.
  `op=edit entries="+ 2001:0db8:85a3:0000:0000:8a2e:0370:7353=vmware_esx_esxi"`
- Si desea crear una sola entrada para un solo valor IPV4 que tiene dos tipos de servicios y enviar cada tipo de servicio a distintos colectores, ingrese el siguiente parámetro en el

comando **ipdevice** y haga clic en **Enviar**.

```
op=edit entries="+10.168.0.2,nwappliance20819=rhlinux
+10.168.0.2,nwappliance3014=apache"
```

- Si desea crear una entrada para un solo nombre de host con dos tipos de servicios distintos y cargar el analizador, ingrese el siguiente parámetro en el comando **ipdevice** y haga clic en **Enviar**.

```
op=edit entries=”+RS214Server-2=rhlinux,apache” reload=true
```

# 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 Security Analytics un archivo de registro capturado en otro servicio. Los nombres de archivos de registro son del tipo **.log**.

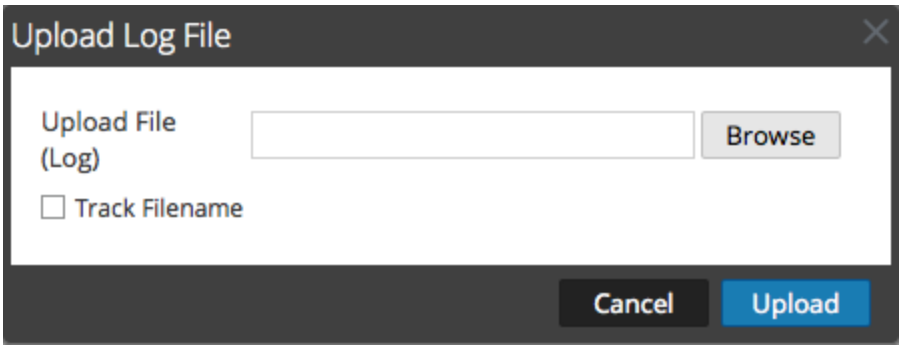
Cuando se carga un archivo de registro en un Log Decoder, este analiza y genera metadatos para cada registro que contiene. Estos registros se agregan a los registros ya decodificados en el Log Decoder y están disponibles para análisis. Security Analytics incluye una opción de rastreo de nombre de archivo 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 que se produzca una carga. Por ejemplo, mientras Log Decoder captura registros.

## Procedimiento

Para importar un archivo de registro a un Log Decoder:

1. En el menú de **Security Analytics**, seleccione **Administration** > **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 registro**.




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 archivo de captura de paquete

En este tema, se explica cómo importar un archivo de captura de paquetes a un Decoder.

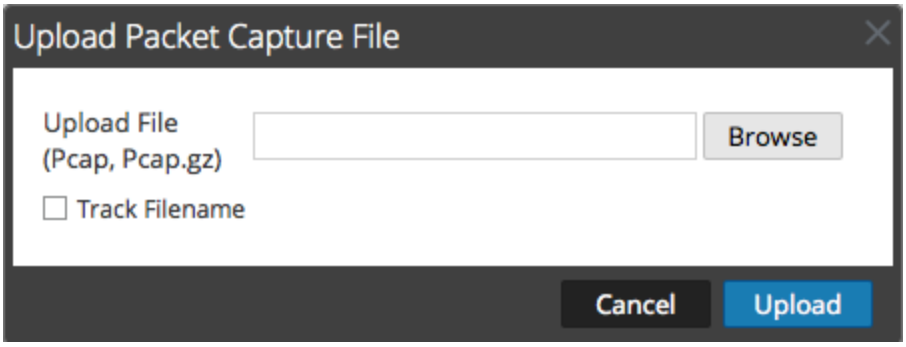
Existen ocasiones en las que desea analizar un archivo de captura de paquetes que no está disponible en el servicio que está utilizando. Puede cargar en Security Analytics un archivo capturado en otro servicio. Los tipos de archivos de captura de paquetes compatibles son **pcap** y **pcap.gz**.

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 descifradas en el Decoder y están disponibles para el análisis. Security Analytics 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.

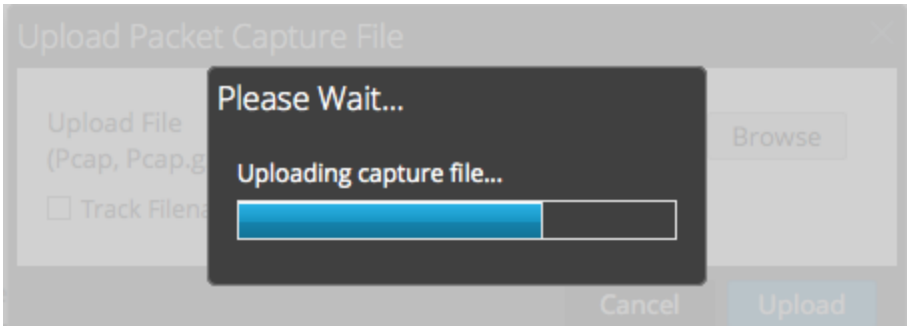
La opción para cargar un archivo de captura de paquetes se atenúa cuando otras operaciones de Decoder impiden una carga, por ejemplo, cuando el Decoder está capturando paquetes.

### Procedimiento

Para seleccionar y cargar un archivo de captura de paquetes:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione el nombre del Decoder y elija  **> 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.

## Verificar la información del sistema de Decoder

En este tema, se presentan las funcionalidades de la vista Sistema relacionadas específicamente con los Decoders y los Log Decoders.

Cuando un servicio se agrega por primera vez a Security Analytics, se aplican los valores predeterminados para los parámetros de configuración del sistema. Puede editar estos valores para ajustar el rendimiento.

System Configuration

| Name | Config Value |
|---|---|
| Compression | 0 |
| Port | 50005 |
| SSL FIPS Mode | ☐ |
| SSL Port | 56005 |
| Stat Update Interval | 1000 |
| Threads | 20 |

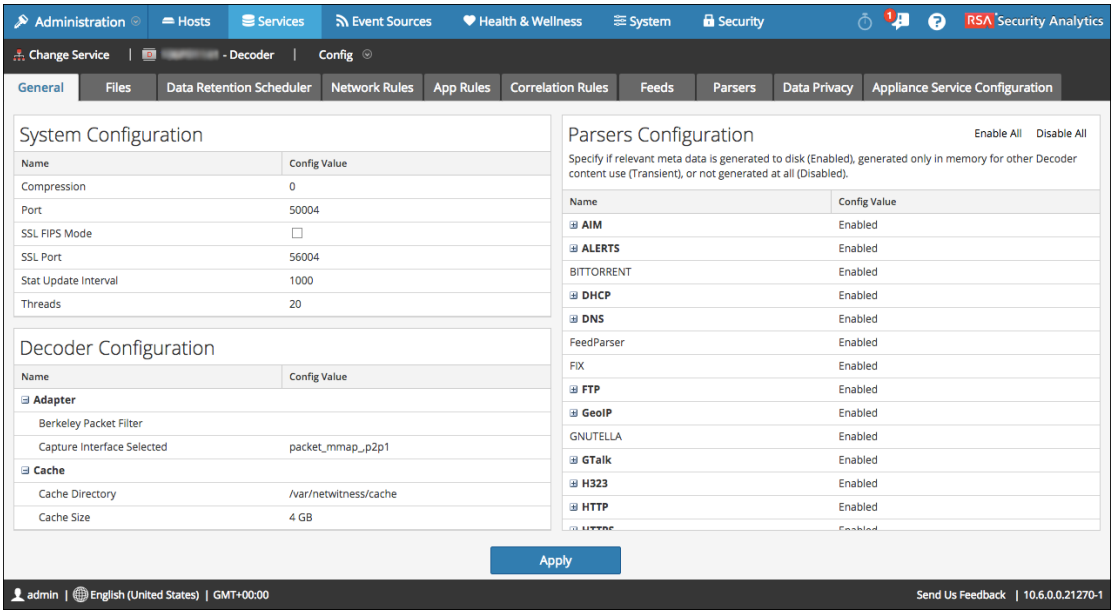
En la mayoría de los casos, los valores predeterminados para la compresión, el intervalo de actualización de estadísticas y la cantidad de hilos de ejecución en el pool se definen en un buen punto para obtener un rendimiento óptimo del sistema. Un parámetro que posiblemente desee cambiar para su ambiente 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.

### Procedimiento

Para editar los parámetros de configuración del sistema:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. En la vista **Servicios**, seleccione un servicio Decoder o Log Decoder y elija  **>Ver > Configuración**.

Se muestra la vista Configuración de servicios del servicio seleccionado.




3. En **Configuración del sistema**, haga clic en un campo que desee editar y escriba un nuevo valor.
4. Cuando haya completado la edición, haga clic en **Aplicar**.

# Configurar un Log Decoder para que acepte Protobuf

En este tema se describe el método para configurar un Log Decoder de modo que acepte registros en formato protobuf (búfer de protocolo).

Hay momento en que se desea analizar archivos de registro que están en formato protobuf (búfer de protocolo).

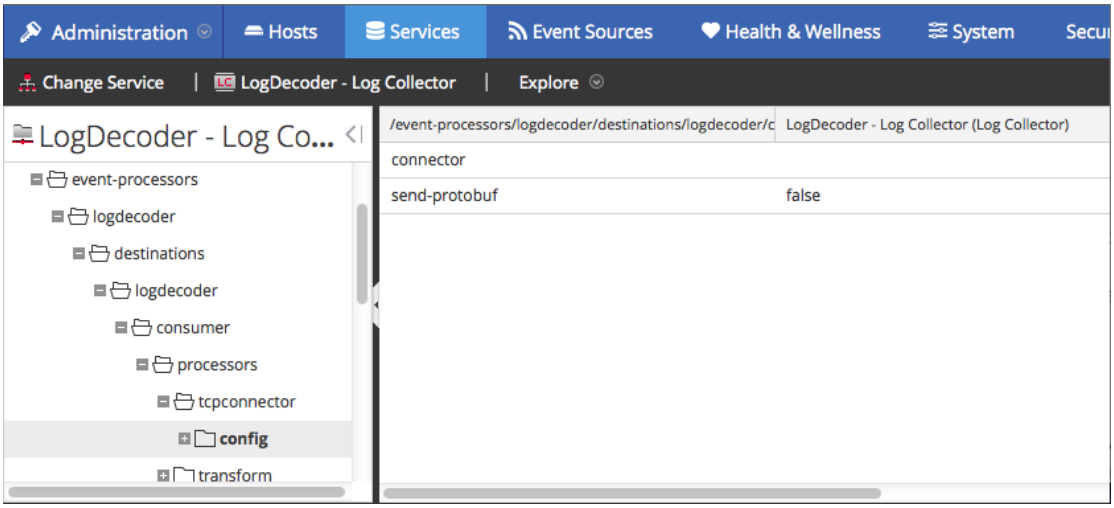
## Procedimiento

Para importar un archivo de registro a un Log Decoder:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione un Log Decoder en la cuadrícula **Servicio** y elija  **> Ver > Explorar**.

   Se muestra la vista Explorador para el Log Decoder.
3. Navegue 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. Navegue a `event-processors/logdecoder/destinations/logdecoder/consumer/processors/tcpconnector/config/connector/channel/tcp` y cambie el valor de **port** a **50202**.
6. Navegue a `event-`

`processors/logdecoder/destinations/logdecoder/consumer/processors/tcp connector/config/connector/event` y cambie los siguientes parámetros:

- Borre el campo **delimiter**
- Cambie **format** a **%text%**

# Referencias

Este tema es un conjunto de referencias que describen la interfaz del usuario de Decoders y Log Decoders en Security Analytics. Estos temas se presentan en orden alfabético.

Use esta sección cuando busque descripciones de la interfaz del usuario de autorizaciones y definiciones de las funciones de la interfaz del usuario.

La vista Configuración de servicios de Security Analytics proporciona una interfaz del usuario para configurar Decoders y Log Decoders con el fin de capturar datos y controlar el tipo de tráfico que se captura mediante el uso de reglas, feeds y analizadores.

**Temas**

# Vista Configuración de servicios: Pestaña Privacidad de datos

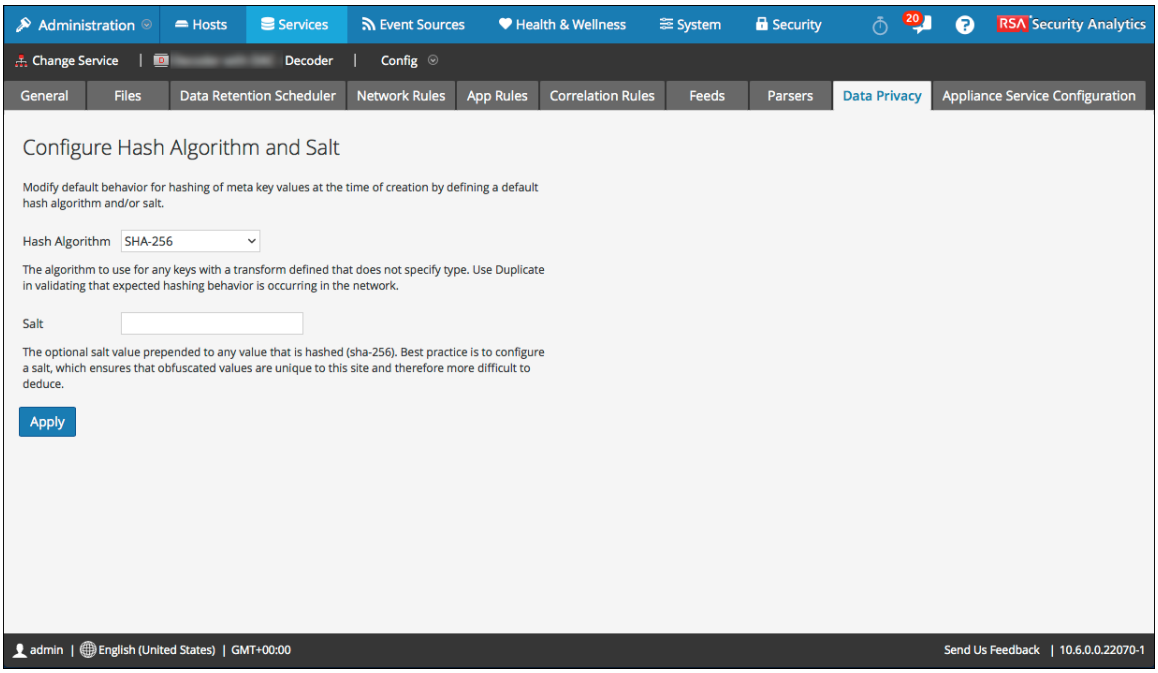
En este tema se proporciona una descripción de las opciones configurables de la pestaña Privacidad de datos para un Decoder o un Log Decoder.

En la pestaña Privacidad de datos, los administradores pueden configurar parámetros de privacidad de datos para ciertos servicios Core. Para Decoder y Log Decoder, puede configurar el algoritmo hash y el valor de sal predeterminados.

Para acceder a esta pestaña:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
2. Seleccione un servicio Decoder o Log Decoder y haga clic en  **> Configuración**.

   Se muestra la pestaña General.
3. Haga clic en la pestaña **Privacidad de datos**.




## Características

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 Security Analytics 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 el tema **Configurar el ocultamiento de datos** de la guía *Administración de la privacidad de datos*. |
| Aplicar | Aplica los cambios. |

## Vista Configuración de servicios: Pestaña Feeds

En este tema se describen las funciones de la vista Configuración de servicios > pestaña Feeds de Decoder.

Los feeds y los analizadores son programas de FLEXPARSE 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:** A menos que se defina lo contrario, todas las referencias a los Decoders se aplican también a los Log Decoders.

Security Analytics 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.

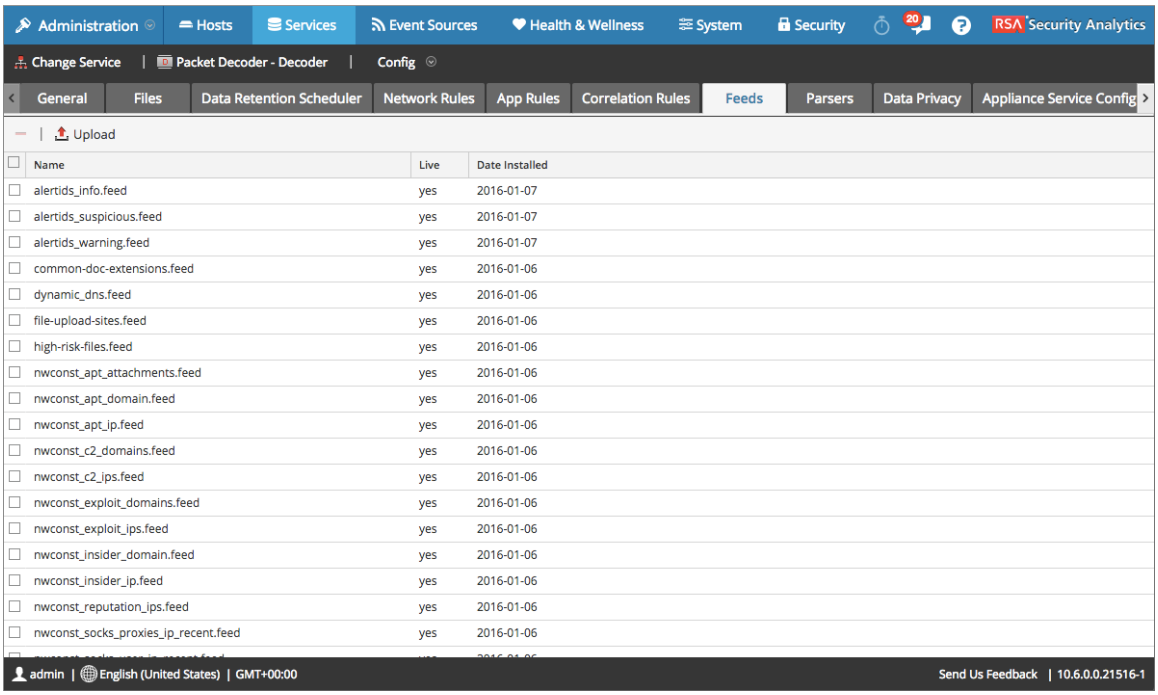
Puede agregar, eliminar y actualizar feeds, mientras se ejecuta un Decoder, sin afectar la captura. En la vista Configuración de servicios > pestaña Feeds se proporciona una interfaz del usuario para administrar feeds en Decoders.

Para mostrar esta vista, realice lo siguiente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **>Ver > Configurar.**

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Feeds**.

Este es un ejemplo de la pestaña Feeds.




## Características

La cuadrícula Feed muestra todos los feeds que se encuentran implementados actualmente en el Decoder. La barra de herramientas de la pestaña Feeds cuenta con opciones para trabajar con feeds en la cuadrícula.

### Barra de herramientas de la pestaña Feeds

| Característica | Descripción |
|---|---|
| Upload | Muestra el cuadro de diálogo Cargar feeds. |
| | Elimina los feeds seleccionados. |

### Cuadrícula Feed

La cuadrícula Feed proporciona una lista de todos los feeds implementados actualmente para el Decoder.

| Columna | Descripción |
|---|---|
| **Nombre** | El nombre del feed o el archivo del feed. |

| Columna | Descripción |
| --- | --- |
| **En vivo** | Indica si el feed se originó en Live. Los posibles valores son **Sí**, **No** o **N/D**.<br>• **Sí** = Instalado mediante Live<br>• **No** = Instalado mediante Security Analytics<br>• **N/D** = El feed no tiene un archivo de atributos que creó Security Analytics para rastrear la fecha de instalación. El feed puede haberse instalado manualmente y no mediante Security Analytics o Live. Los feeds instalados manualmente aun funcionan correctamente. |
| **Fecha de instalación** | La fecha en que el feed se migró al servicio. |

**Tema**

- Diálogo Cargar feeds

## Diálogo Cargar feeds

En este tema se describen las funcionalidades del cuadro de diálogo Cargar feeds en la vista Configuración de servicios > pestaña Feeds.

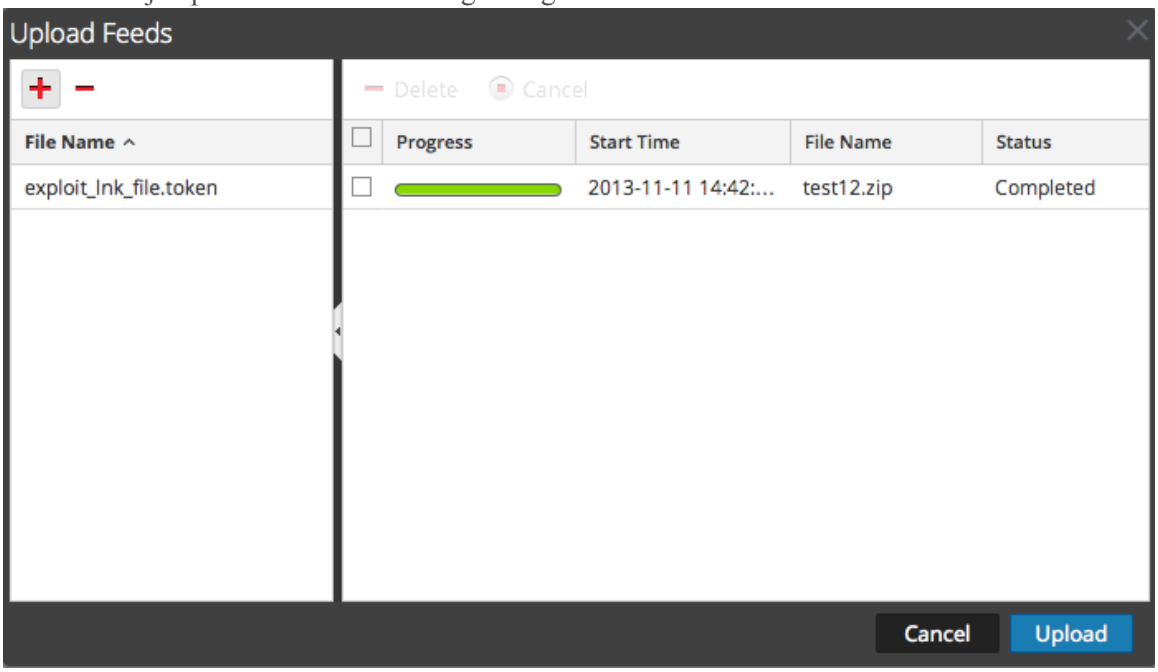
La opción **Cargar** en la vista Configuración de servicios > pestaña Feeds muestra el cuadro de diálogo Cargar feeds, en el cual puede administrar la carga de feeds a un Decoder o un Log Decoder.

Puede tener acceso a esta vista realizando lo siguiente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija **>Ver > Configurar.**

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Feeds**.
4. Haga clic en Upload.

Este es un ejemplo del cuadro de diálogo Cargar feeds.




### Características

### Cuadrícula Archivo

En la cuadrícula Archivo puede preparar 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**.

| Característica | Descripción |
|---|---|
|  | Abre una vista de estructura de directorios donde puede seleccionar los archivos que agregará a la cuadrícula Archivo. |
|  | Elimina los archivos seleccionados de la cuadrícula Archivo. |
| **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. |

### Cuadrícula Trabajo de carga

La cuadrícula Trabajo de carga proporciona una vista de los trabajos de carga que se iniciaron cuando se hizo clic en **Cargar**.

| Función/columna | Descripción |
|---|---|
|  | 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. |
| **Status** | Muestra el estado de un trabajo de carga. |

### Botones del cuadro de diálogo Cargar feeds

| Característica | Descripción |
|---|---|
| **Cancelar** | Cierra el cuadro de diálogo Cargar feed. |
| **Cargar** | Inicia la carga de los archivos de feed que aparecen en la cuadrícula Archivo. Cada feed aparece en una fila por separado en la cuadrícula Proceso de carga. |

## Vista Configuración de servicios: Pestaña Archivos

En este tema se presentan los archivos de configuración de Decoder y Log Decoder que se pueden ver en la 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 el tema **Editar los archivos de configuración de servicios Core** de la *Guía de introducción de hosts y servicios* se proporcionan instrucciones generales para editar archivos.

Al igual que otros servicios de Security Analytics Core, el Decoder y el Log Decoder tienen un archivo de índice y también pueden tener un generador de informes de fallas generales, netwitness y un programador. Los archivos de índice de Decoder y Log Decoder se denominan **index-decoder.xml** e **index-logdecoder.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 solamente si se encontró table-map.xml en el sistema de archivos (por ejemplo, es un Log Decoder con contenido Envision instalado).

| 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. |
| NwFlex.parser | Este es un lenguaje de definición de analizador genérico para extender la compatibilidad del protocolo de aplicación existente del Decoder. |
| 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** . |
| 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 claves 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. |

**Temas relacionados**

- Archivo de definiciones de feed
- Analizador flexible
- Analizador de GeoIP
- Analizadores Lua
- 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 la Guía del administrador de sistema Next Gen.

## Analizador flexible

En este tema se presentan los analizadores flexibles.

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es **NwFlex.xml**, el analizador Flex.

#### 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
- Hace coincidir varios tokens
- Hace 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**

- Definición del idioma
- Hacer coincidir puerto e identificar inmediatamente
- Definición de lenguaje de funciones generales
- Definición del idioma
- Definición del lenguaje de los nodos
- Definición del idioma
- Definición del idioma
- Definición de lenguaje de 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 |
|---|---|---|
| y | | Ejecuta una operación AND bit a bit entre dos números. |
| | nombre | Variable a la cual se aplica el resultado de AND. |
| | valor | Número para aplicar AND al resultado. |
| o | | Ejecuta una operación OR bit a bit entre dos números. |
| | nombre | Variable a la cual se aplica el resultado de OR. |
| | valor | Número para aplicar OR al resultado. |
| increment | | Ejecuta la operación ADDITION de dos números. |
| | nombre | Variable que contiene el valor inicial AND para recibir los resultados de ADDITION. |
| | valor | Número que se suma (ADD) al valor inicial. |
| decrement | | Ejecuta la operación SUBTRACTION de dos números. |
| | nombre | Variable que contiene el valor inicial AND para recibir los resultados de SUBTRACTION. |
| | valor | Número que se resta (SUBTRACT) del valor inicial. |
| divide | | Ejecuta la operación DIVISION de dos números. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | Variable que contiene el valor inicial AND para recibir los resultados de DIVISION. |
| | valor | 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 | Variable que contiene el valor inicial AND para recibir los resultados de MODULO. |
| | valor | 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. |
| | nombre | Variable que contiene el valor inicial AND para recibir los resultados de MULTIPLICATION. |
| | valor | Cantidad por la cual se multiplica (MULTIPLY) el valor inicial. |
| shiftleft | | Ejecuta un desplazamiento aritmético a la izquierda binario. |
| | nombre | Variable que contiene el valor inicial AND para recibir los resultados del desplazamiento. |
| | valor | Cantidad de bits por los cuales se realiza el desplazamiento. |
| shiftright | | Ejecuta un desplazamiento aritmético a la derecha binario. |
| | nombre | Variable que contiene el valor inicial AND para recibir los resultados del desplazamiento. |
| | valor | 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>
```

**Hace 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>
```

**Hace 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 atri-buto | Descripción |
|---|---|---|
| **apptype** | | Obtiene el tipo de servicio actualmente definido para la sesión actual. |
| | nombre | 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. |
| | nombre | El identificador único asignado al elemento en la sección de declaración. |
| | valor | 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. |
| | nombre | La variable para recibir el valor de los metadatos que generó la devolución de llamadas. |
| gettoken | | Devuelve el token con el cual hubo coincidencia actualmente. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | 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. |
| fin | | 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. |
| | nombre | El identificador de variable único asignado al elemento en la sección **declaration**. |
| | equal<br>notequal<br>less<br>lessequal<br>greater<br>greaterequal<br>y<br>o | El valor de la operación que se comparará. Si es verdadero, se ejecutan subacciones. |
| register | | Agrega metadatos a la sesión. |
| | nombre | El identificador único de una variable de metadatos que se creará, según se define en la sección **declaration**. |
| | valor | 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. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | El identificador de variable único asignado al elemento en la sección de declaración. |
| | equal<br>notequal<br>less<br>lessequal<br>greater<br>greaterequal<br>y<br>o | 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 | | Ejecute el elemento **match** especificado. Puede ser cualquier elemento de coincidencia definido en el mismo analizador flexible, independientemente de la forma en que se declaró. |
| | valor | El nombre del elemento de coincidencia o una variable de cadena que contiene el nombre de un elemento de coincidencia.<br>• Si se especifica el nombre del elemento de coincidencia, el analizador no se cargará si el elemento con coincidencia nombrado no existe.<br>• 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.<br>• 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 |
|---|---|---|
| falla | | Registra un mensaje en el registro del sistema con el nivel de registro **Falla.** |
| | valor | 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.** |
| | valor | 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**. |
| | valor | Una cadena que se incluirá como el mensaje del registro. |
| depurar | | Registra un mensaje en el registro del sistema con el nivel de registro **Depuración.** |
| | valor | 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. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | 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 | Este nodo proporciona una descripción simple de lo que hace el analizador. |
| | Servicio | Este es el número único asignado a la sesión cuando se identifica. |
| **declaration** | | El nodo que describe la definición. Cada una de estas definiciones puede tener una entrada **match** asociada. |
| 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 **lectura** se configura en el byte que está inmediatamente después del token con coincidencia. |
| | nombre | Este es un identificador único para la declaración. |
| | valor | Este es el valor exacto del token que se identificará. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | opciones | Las opciones especifican que el token debe comenzar en una nueva línea o al final de una línea (**linestart** o **linestop**). |
| **meta-call-back** | | 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 solo para sesiones que se han identificado como un app-type específico (por ejemplo, 80 para HTTP). |
| | nombre | 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) |
| número | | 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 |
|---|---|---|
| | nombre | 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 valores posibles son **global, constant, stream** y **session** (valor predeterminado). |
| cadena | | Define una variable numérica a la cual se puede hacer referencia en otra ubicación dentro de la definición del analizador. |
| | nombre | 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 valores posibles son **global, constant, stream** y **session** (valor predeterminado). |
| puerto | | 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. |
| | nombre | Este es un identificador único para la declaración. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | valor | Este es el número de puerto que se identificará. |
| sesión | | 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. |
| | nombre | Este es un identificador único para la declaración. |
| | valor | Especifica que el procesamiento tiene lugar al principio de una nueva sesión o al final de una sesión (**begin** o **end**). |
| streams | | 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. |
| | nombre | Este es un identificador único para la declaración |
| | valor | Especifica que el procesamiento tiene lugar al principio 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. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | 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, **texto, IPv4 y UInt32**). Consulte la lista completa en la documentación de SDK. |
| pattern | | Define una variable de expresión regular que usará la función **regex** |
| | nombre | 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 valores posibles 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 **atributo scope** 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 puedan aparecer como secundarios de un elemento de coincidencia:<br>• Aspectos generales<br>• Aritmética<br>• Cadena<br>• 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 **lectura**, que se establece al principio de un **elemento de** coincidencia.

### 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. |
| | nombre | Variable **number** que recibirá el desplazamiento desde la posición **read** donde comienza la coincidencia. |
| | valor | 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. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| **install-decoder** | | Para activar 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.<br>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. |
| **move** | | Mueve la posición de **lectura** 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 **lectura** y se ejecutará cualquier elemento secundario. Si no se encuentra, la posición de **lectura** permanece sin cambios y los elementos secundarios no se ejecutan. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | valor | La cantidad de bytes para mover la posición de **lectura**. |
| | direction (opcional) | La dirección para mover la posición de lectura actual. Puede ser **hacia delante** (predeterminado) o **en reversa.** |
| **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. |
| | nombre | 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. |
| | nombre | Una variable numérica para recibir la posición de lectura actual. |
| **read** | | Lee una cantidad especificada de bytes comenzando en la posición de **lectura** en una variable. Si hay suficientes datos en el flujo, se actualiza la posición de **lectura**, se asigna la lectura de datos y se ejecutará cualquier elemento secundario. Si no se encuentra, la posición de **lectura** permanece sin cambios y los elementos secundarios no se ejecutan. |
| | nombre | El nombre de una **cadena** o la variable **numérica** para recibir datos de flujo. Si se proporciona una variable **numérica**, la lectura de bytes se implementa 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 de **lectura**. Si encuentra coincidencias, se devuelve la compensación desde la posición de **lectura** 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 atri-buto | Descripción |
|---|---|
| nombre | Variable **number** que recibirá el desplazamiento desde la posición **read** donde comienza la coincidencia. |
| valor | 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 **cadena** 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 **cadena**. |
| | nombre | El identificador exclusivo de una variable de cadena al cual se conecta el valor especificado. |
| | valor | 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. |
| | nombre | Una variable **number** para recibir la posición de base cero, donde la cadena de valor proporcionada se encontró en la cadena **in**. |
| | valor | 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 **number**. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | Una variable **number** para recibir la longitud de la cadena especificada. |
| | valor | 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 | Una variable de número para recibir la posición de base cero, donde la expresión regular proporcionada coincide en la cadena in. |
| | valor | 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**. |
| | nombre | El identificador exclusivo de una variable de cadena para recibir el valor extraído. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | valor | Un valor de cadena desde el cual extraer una subcadena. |
| | from (optional) | 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. |
| | nombre | El nombre de una variable **string** para procesar. |
| toupper | | Convierte una cadena en letras mayúsculas. |
| | nombre | El nombre de una variable **string** para procesar. |
| **urldecode** | | Decodifica una cadena que contiene caracteres con codificación URL. |
| | nombre | Una variable de cadena para recibir la cadena decodificada. |
| | valor | Una cadena codificada como URL para decodificar. |
| **base64decode** | | Decodifica una cadena codificada con base 64. |
| | nombre | Una variable de cadena para recibir la cadena decodificada. |
| | valor | Una cadena codificada como URL para decodificar. |
| **uudecode** | | Decodifica una cadena uuencoded. |

| Nombre de nodo | Nombre de atributo | Descripción |
|---|---|---|
| | nombre | Una variable de cadena para recibir la cadena decodificada. |
| | valor | Una cadena uuencoded. No se deben incluir las líneas de encabezado y cola. |
| **quotedprintabledecode** | | Decodifica una cadena codificada imprimible citada. |
| | nombre | Una variable de cadena para recibir la cadena decodificada. |
| | valor | Una cadena codificada imprimible citada. |
| **convert-ebcdic** | | Convierte una cadena EBCDIC en su equivalente ASCII. |
| | nombre | Una variable de cadena para recibir la cadena decodificada. |
| | valor | Una cadena codificada como URL para decodificar. |

## Analizador de GeoIP

En este tema, se presenta el analizador de Geo IP para Decoders.

Uno de los archivos disponibles para editar en la vista Configuración de servicios > pestaña Archivos es **GeoPrivate.ipl**, el analizador de Geo IP.

### GeoPrivate.ipl

El analizador de Geo IP es un analizador fijo que toma las direcciones IP y las convierte en ubicaciones geográficas. Las ubicaciones se muestran a través de la vista de Google Earth.

Se agregan los metadatos de geoubicación en **GeoPrivate.ipl** tanto a **ip.src** como a **ip.dst**. El analizador utiliza 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

En este tema se presentan los 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 SecurCare Online (SCOL) 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
- Hace coincidir varios tokens
- Hace coincidir token y crear metadatos

## 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.

### 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_lis-
t>|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 llamada predeterminada. Si se encuentra algún problema, el comando describirá el problema y le preguntará si puede repararlo.**

```
dbcheck C:\Documents and Settings\User\My Documents\NetWitness\ Inves-
tigations\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
- Sistemas de valor absoluto (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.

Se proporciona un análisis completo en el capítulo sobre la captura inalámbrica de paquetes en la Guía del administrador de sistema NextGen

## Vista Configuración de servicios: Pestaña General

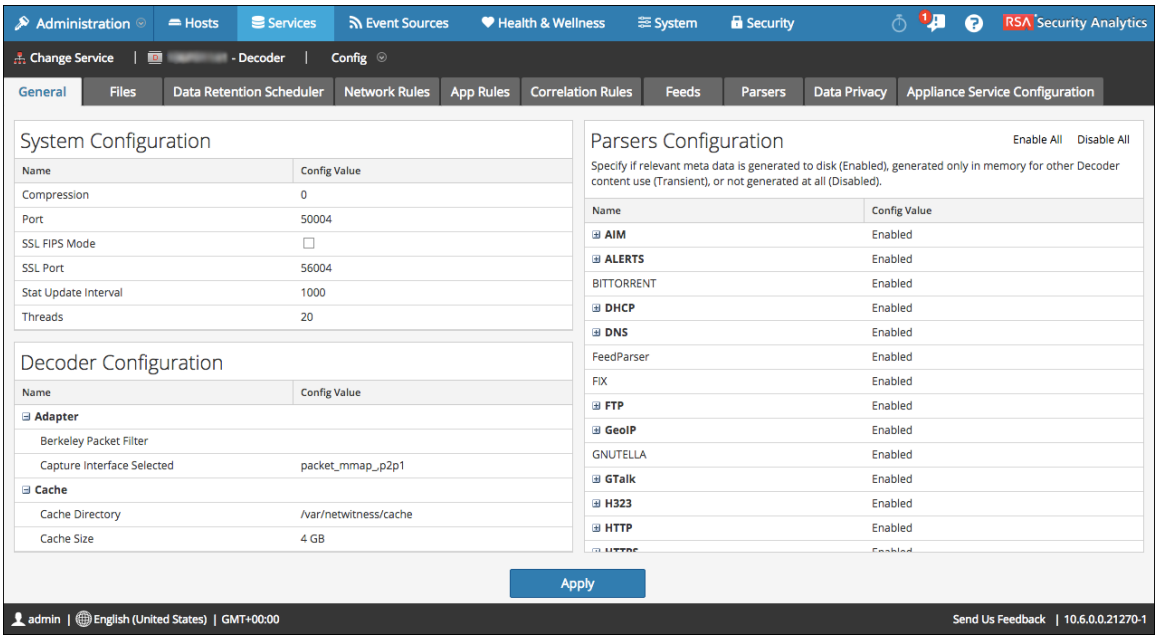
En este tema se presentan las funciones de la vista Configuración de servicios > pestaña General de Decoders y Log Decoders.

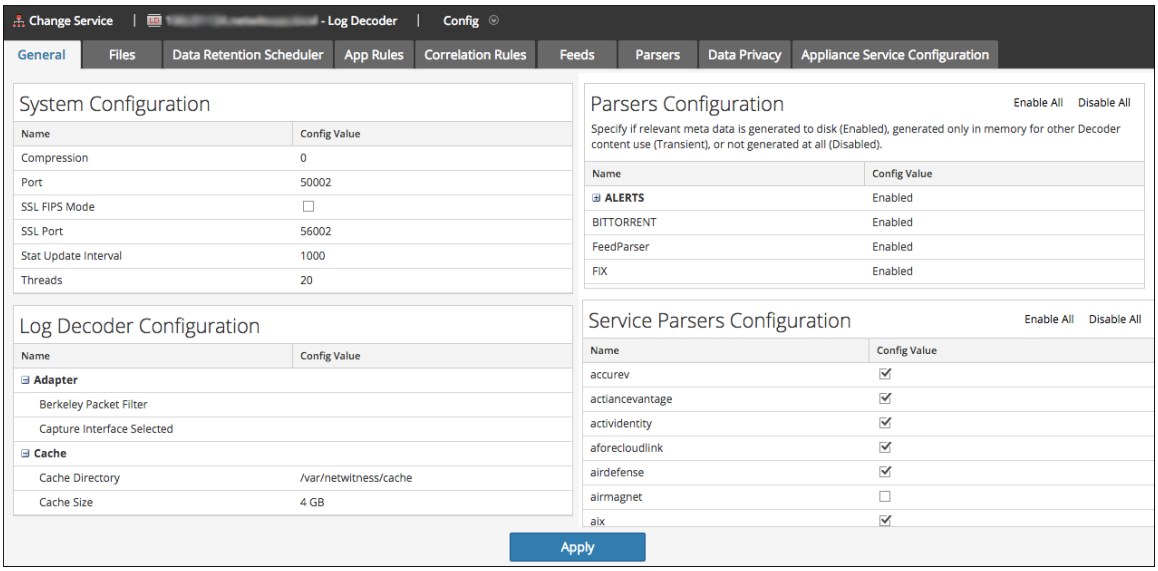
La pestaña General de un Decoder en la vista Configuración de servicios proporciona una manera de administrar la configuración básica del servicio, configurar la captura de datos y seleccionar los analizadores que se aplican a los datos capturados.

Entre los ajustes que permiten configurar la captura de datos se incluyen:

- Selección de adaptador
- Especificación de la caché
- Inicio automático de captura y otros parámetros de captura que afectan a la caché, las sesiones y los tiempos de espera agotados
- Tamaños de archivo de base de datos
- Ubicación del directorio de hash

La primera imagen muestra un ejemplo de la pestaña General de un Decoder. La segunda corresponde a la pestaña General de un Log Decoder.






## Características

Estas son las cuatro secciones principales de la pestaña General para Decoders y Log Decoders:

- Configuración del sistema
- Configuración de Decoder
- Configuración de analizadores
- Configuración de analizadores de servicio (solo Log Decoders)

## Configuración del sistema

La sección Configuración del sistema administra la configuración del servicio de un Decoder. Cuando un servicio se agrega por primera vez, se aplican valores predeterminados. Puede editar estos valores para ajustar el rendimiento.

System Configuration

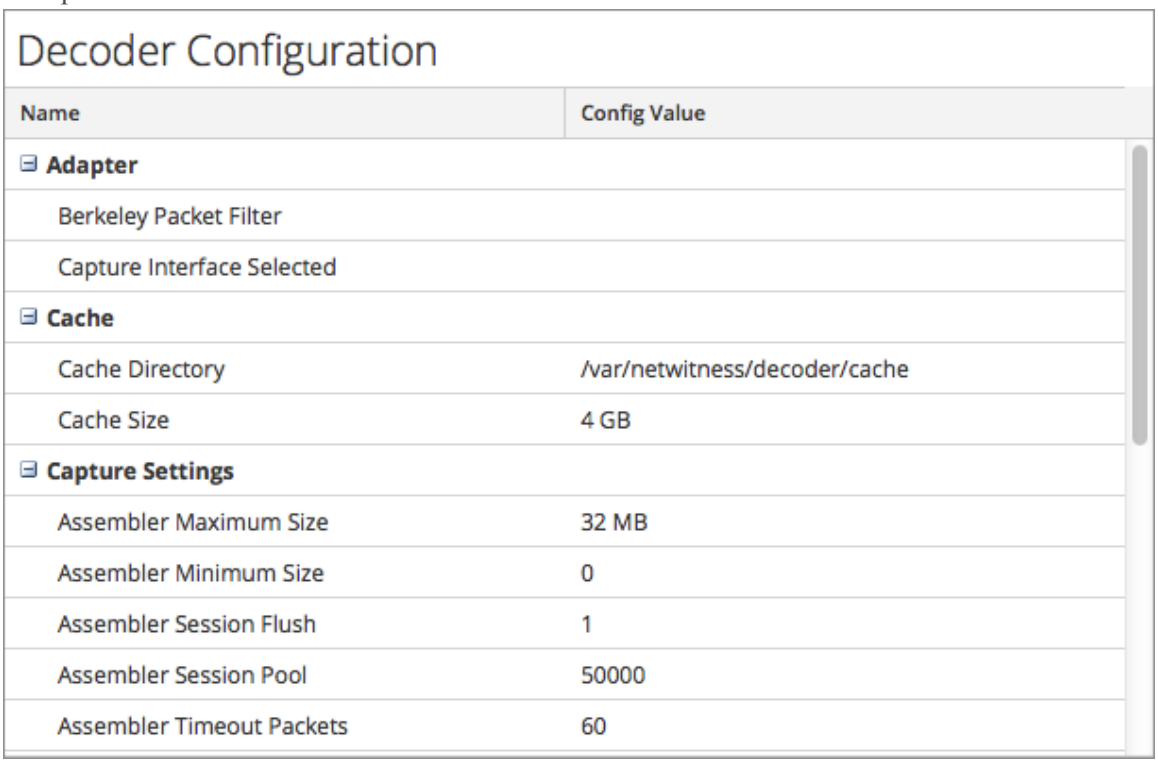
| Name | Config Value |
|---|---|
| Compression | 0 |
| Port | 50004 |
| SSL FIPS Mode | ☐ |
| SSL Port | 56004 |
| Stat Update Interval | 1000 |
| Threads | 20 |

La sección Configuración del sistema tiene estos parámetros.

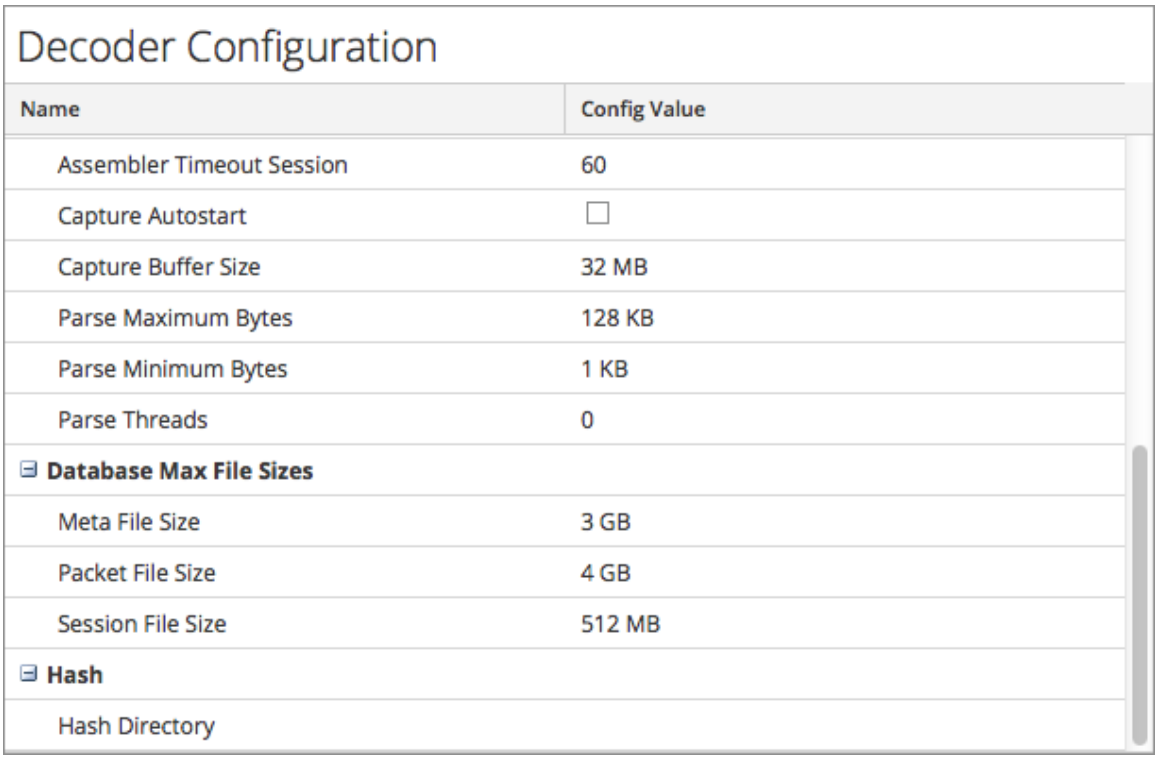
| Parámetro | Descripción |
|---|---|
| **Compresión** | La cantidad mínima de bytes que se deben transmitir por respuesta antes de la compresión. Si se define en 0, se deshabilita la compresión. El valor predeterminado es **0**.<br>Un cambio en el valor se aplica de inmediato en todas las conexiones subsiguientes. |
| **Puerto** | Determina el puerto que usa el servicio.<br>**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**.<br>Un cambio en el valor se aplica de inmediato. |
| **Hilos** | 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.<br>Un cambio se aplica tras el reinicio del servicio. |

## 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 modificar 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.




### Adaptador

Los parámetros del adaptador configuran la interfaz de red para la captura. La siguiente tabla describe los ajustes del Adaptador del Decoder. Los adaptadores de red predeterminados disponibles se configuran durante la instalación. Consulte al administrador del sistema para obtener más información.

| Parámetro de adaptador | Descripción |
|---|---|
| **Filtro de paquetes Berkeley** | Los filtros de paquetes Berkeley (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:<br>• packet_mmap_,1,lo (bpf)<br>• packet_mmap_,2,eth2 (bpf)<br>• packet_mmap_,3,eth3 (bpf)<br>• packet_mmap_,4,eth4 (bpf)<br>• packet_mmap_,5,eth5 (bpf)<br>• packet_mmap_,8,ALL (bpf)<br>Existen tres servicios de captura inalámbricos disponibles:<br>• packet_netmon_ (Microsoft Netmon)<br>• packet_mac80211_ (Linux mac80211)<br>• packet_airport_ (Mac OS X AirPort) |

El Decoder admite además el filtrado en el nivel de sistema que se define usando 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 Libcap, 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/).

### Caché

Los parámetros de captura configuran el directorio de caché y el tamaño de los archivos de caché de la sesión. La tabla siguiente describe los ajustes de caché.

| 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 hace efectivo inmediatamente. |
| **Tamaño de la memoria 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 hace efectivo inmediatamente. |

### Configuración de captura

La sección Configuración de captura ofrece una manera de configurar los ajustes de captura operacional.

**Nota:** De manera predeterminada, no hay reglas de captura definidas cuando instala Security Analytics por primera vez. A menos que se especifiquen reglas, los paquetes no se filtran. Puede definir reglas de captura antes de comenzar a capturar datos (consulte Configurar reglas de red, Configurar reglas de aplicacionesy Configurar reglas de correlación).

Esta tabla describe la configuración de captura.

| 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 hace efectivo inmediatamente. |

| Parámetro de configuración de captura | Descripción |
|---|---|
| **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 hace efectivo inmediatamente. |
| **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**.<br>• **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.<br>• **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.<br>• **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.<br><br>El cambio se hace efectivo con el reinicio del servicio. |
| **Pool de sesión de ensamblador** | Especifica la cantidad de entradas en el pool de sesión. El valor pre-determinado es **350000**. El cambio se hace efectivo con el reinicio del servicio. |

| Parámetro de configuración de captura | Descripción |
|---|---|
| **Tiempo de espera agotado 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 hace efectivo inmediatamente. |
| **Tiempo de espera agotado 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 hace efectivo inmediatamente. |
| **Inicio automático 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 hace efectivo inmediatamente. |
| **Tamaño de buffer de captura** | La asignación del buffer de memoria de captura en Megabytes. El valor predeterminado es **64 MB**. El cambio se hace efectivo con 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 hace efectivo inmediatamente. |
| **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 hace efectivo inmediatamente. |

| Parámetro de configuración de captura | Descripción |
|---|---|
| **Hilos de ejecución 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 hace efectivo con el reinicio del servicio. |

### 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. La tabla siguiente describe los parámetros.

| 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 hace efectivo con 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 hace efectivo con 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 hace efectivo con el reinicio del servicio. |

### Hash

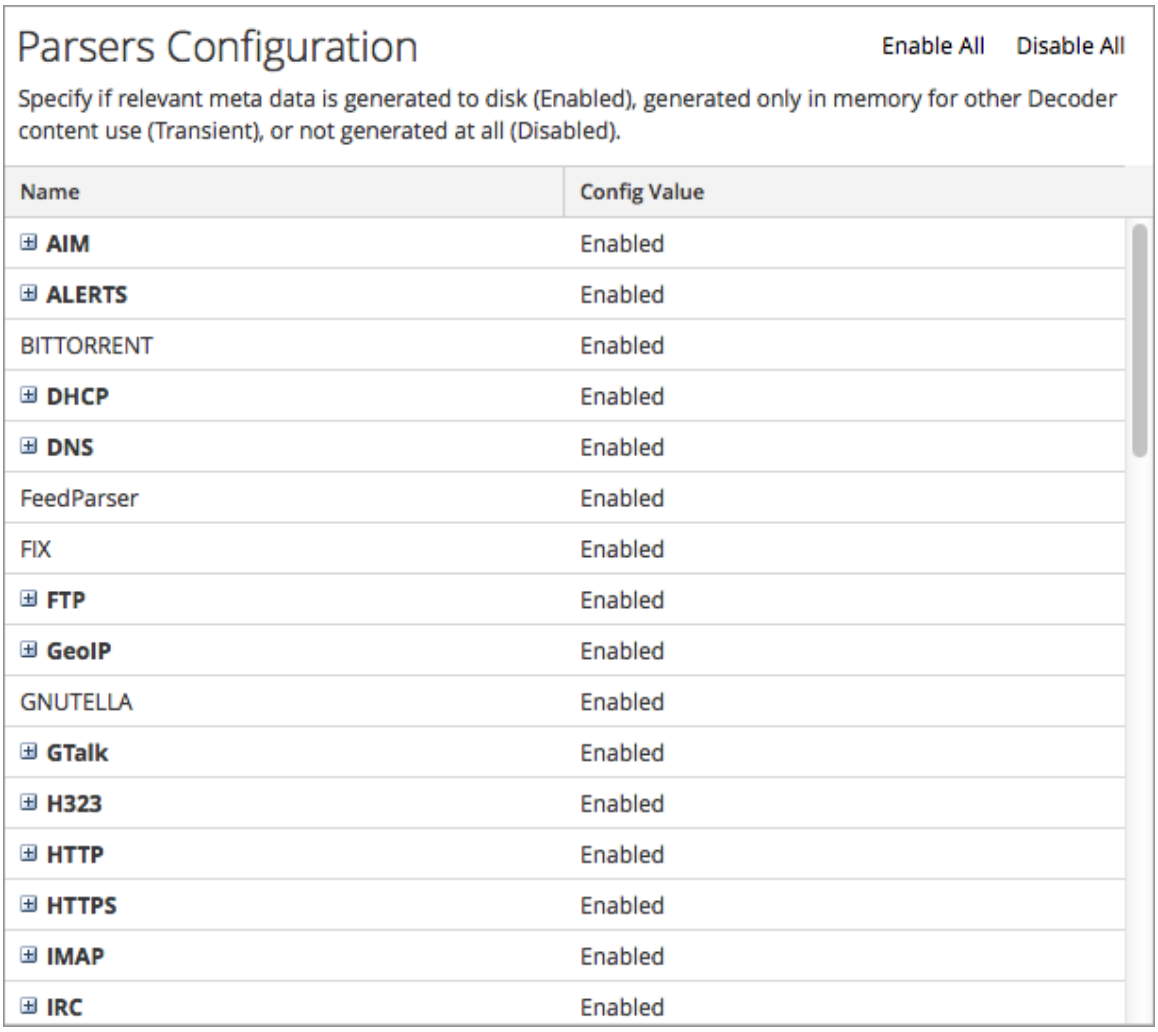
Controla las opciones de hash de archivo de base de datos. Se produce una pequeña disminución del rendimiento cuando se aplican valores hash. En la tabla siguiente se describe la opción de hash.

| 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 hace efectivo con el reinicio del servicio. |

## 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.

Security Analytics tiene la capacidad de configurar analizadores individuales que no almacenan los metadatos generados en disco (opción Transitorio). Esto ayuda a los administradores a proteger ciertos datos y suele ser parte de un plan de privacidad de datos (consulte *Administración de la privacidad de datos*).



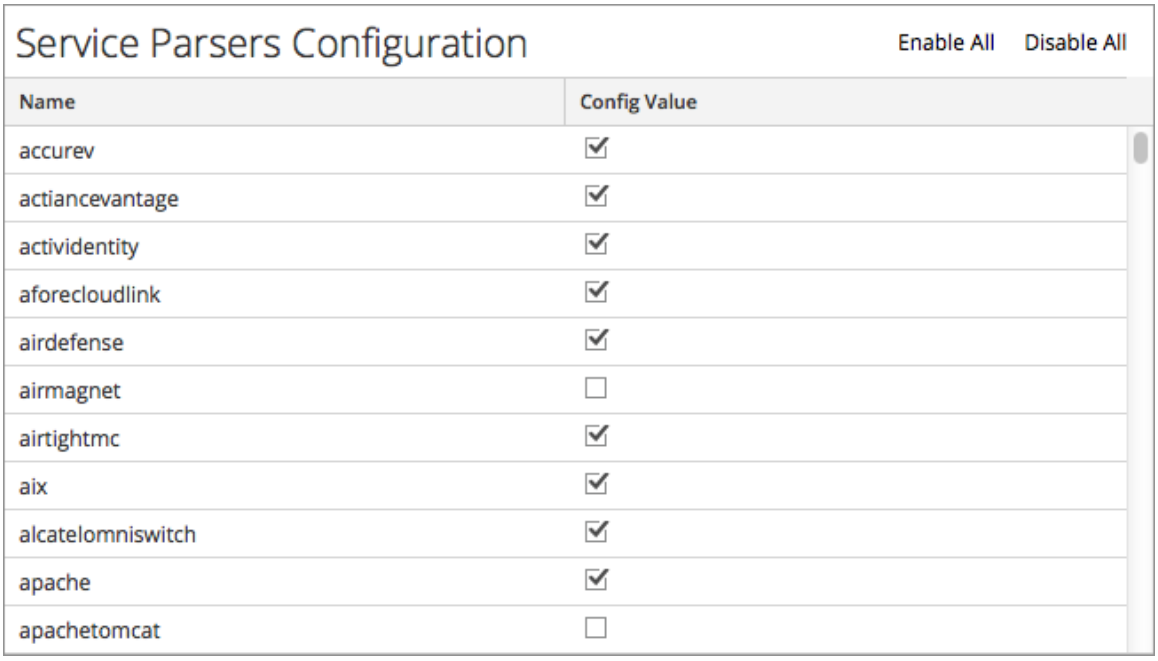

En la tabla se describen las funcionalidades de la sección Configuración de analizadores.

| Característica | Descripción |
|---|---|
| **Activar todo**<br>**Desactivar todo** | 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. En el ejemplo anterior, CMS_windows_executable tiene tres metadatos seleccionables que el analizador puede crear: alert.id, error y filetype. |

| Característica | Descripción |
|---|---|
| **Valor de configuración** | Una lista desplegable cambia la configuración del analizador o de los metadatos a **Activado**, **Desactivado** o **Transitorio**.<br>• Cuando se selecciona **Activado**, el Decoder usa el analizador para filtrar el tráfico.<br>• 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.<br>• Cuando se selecciona **Desactivado**, el Decoder no usa el analizador.<br>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. |

## Configuración de analizadores de servicio adicionales 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 Mapeos de analizadores

En este tema se proporciona una descripción de las opciones configurables para un Log Decoder en la pestaña Mapeos de analizadores.

En la pestaña Mapeos de analizadores, los administradores pueden configurar mapeos de analizadores de registros para los servicios de Log Decoder. Esta función está diseñada para rastrear un subconjunto de orígenes de eventos que se analiza con el analizador incorrecto. La pestaña Mapeos de analizadores se debe habilitar antes de que esté disponible en la vista Configuración de servicios.

Los procedimientos asociados con la pestaña Mapeos de analizadores se proporcionan en Acceder a mapeos de analizadores.

Para acceder a esta pestaña:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **>Ver > Configurar.**

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Mapeo de analizadores**.

Este es un ejemplo de la pestaña.

## Características

La cuadrícula Analizador muestra todos los analizadores que se encuentran mapeados actualmente en el Log Decoder. La barra de herramientas de la pestaña Analizador cuenta con opciones para trabajar con mapeos de analizadores en la cuadrícula.

### Barra de herramientas Mapeo de analizadores

La barra de herramientas Mapeo de analizadores cuenta con opciones para trabajar con mapeos de analizadores en la cuadrícula.

| Característica | Descripción |
|---|---|
|  | Agregar un mapeo de analizador. |
|  | Eliminar el mapeo de analizador seleccionado. |
|  | Editar un mapeo de analizador. |
|  | Actualizar la lista de mapeos de analizadores. |

| Característica | Descripción |
| --- | --- |
|  | Mostrar el menú Acciones.<br>• **Importar**: Importar un mapeo de analizadores a un archivo.<br>• **Exportar**: Guardar un mapeo de analizadores en un archivo. |
| | |

### Cuadrícula Mapeo de analizadores

En la cuadrícula Mapeo de analizadores 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 eventos** | Muestra los orígenes de eventos que se están analizando incorrectamente. |
| | |

## Vista Configuración de servicios: Pestaña Analizadores

En este tema se presentan las funciones de la vista Configuración de servicios > pestaña Analizadores.

En la vista Configuración de servicios > pestaña Analizadores, puede ver los analizadores implementados en un Decoder, cargar analizadores y eliminar los analizadores implementados. Es posible agregar y eliminar analizadores mientras un Decoder está en funcionamiento sin afectar la captura. Consulte Configurar feeds y analizadores para obtener una introducción general al uso de analizadores en Decoders.

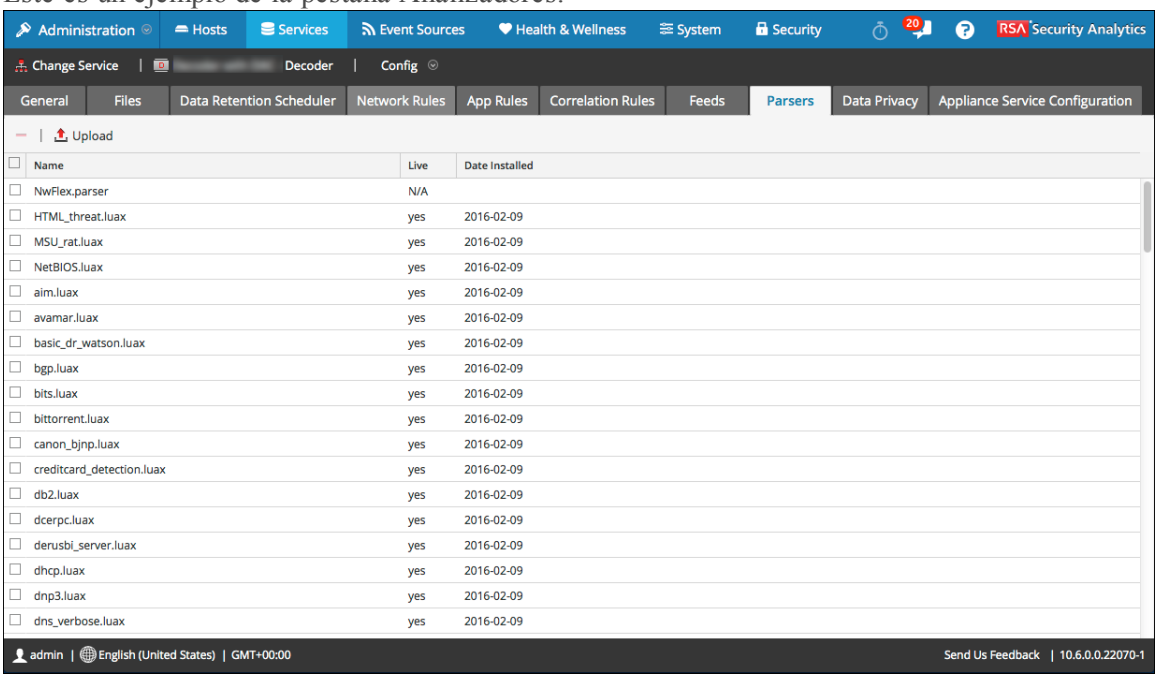
**Nota:** A menos que se defina lo contrario, todas las referencias a los Decoders se aplican también a los Log Decoders.

Puede tener acceso a esta vista realizando lo siguiente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **>Ver > Configurar.**

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Analizadores**

Este es un ejemplo de la pestaña Analizadores.

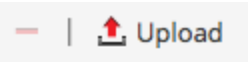


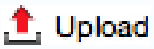
## Características

La cuadrícula Analizador muestra todos los analizadores que se encuentran implementados actualmente en el Decoder. La barra de herramientas de la pestaña Analizador cuenta con opciones para trabajar con analizadores en la cuadrícula.

### Barra de herramientas de la pestaña Analizadores

Este es un ejemplo de la barra de herramientas.




| Característica | Descripción |
|---|---|
|   | 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. |

### Cuadrícula Analizador

La cuadrícula Analizador proporciona una lista de todos los analizadores implementados actualmente para el Decoder.

| Columna | Descripción |
|---|---|
| **Nombre** | El nombre del analizador o el archivo del analizador. |
| **En vivo** | Indica si el analizador se originó de Live. Los posibles valores son **Sí**, **No** o **N/D**.<br>• **Sí** = Instalado mediante Live<br>• **No** = Instalado mediante Security Analytics<br>• **N/D** = El analizador no tiene un archivo de atributos creado por Security Analytics para registrar la fecha de instalación. El analizador puede haberse instalado manualmente y no mediante Security Analytics o Live. Los feeds instalados manualmente aun funcionan correctamente. |
| **Fecha de instalación** | La fecha en que el analizador se migró al servicio. |

## Vista Configuración de servicios: Pestañas Reglas

Las pestañas Reglas de la vista Configuración de servicios permiten definir y administrar 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 solo a Packet Decoders.

Paso 4. Configurar reglas de Decoder En la sección, se ofrece más información.

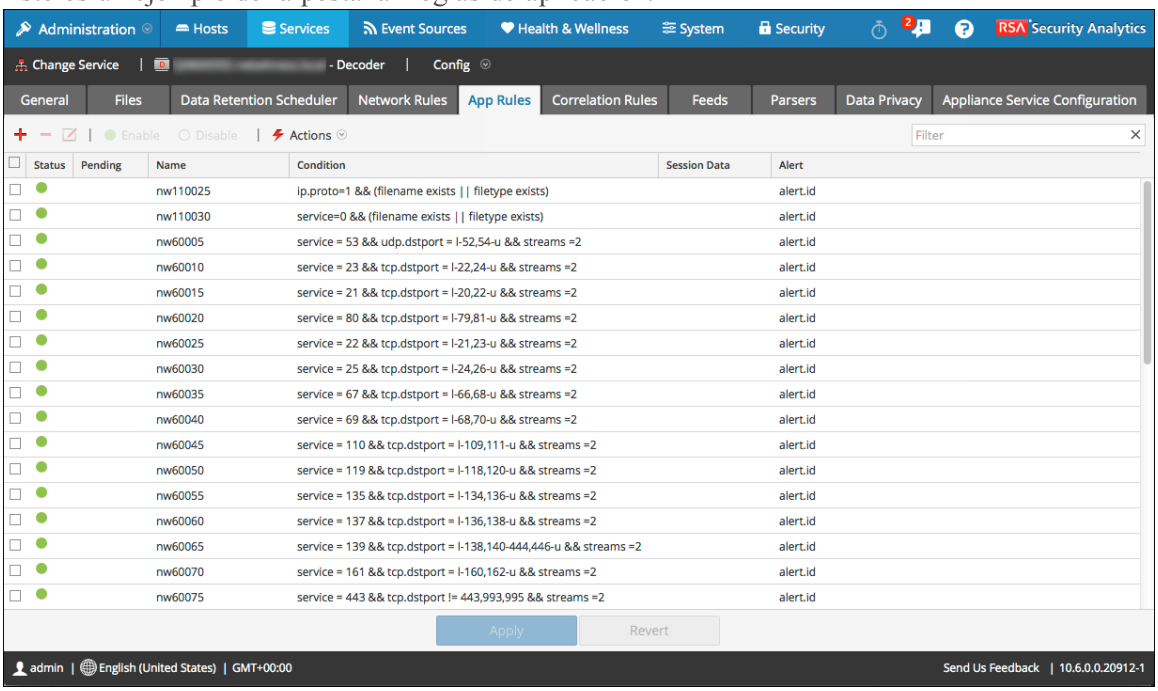
Puede mostrar esta vista realizando lo siguiente:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **>Ver > Configurar.**

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en una de las pestañas de reglas: **Reglas de red**, **Reglas de aplicación** o **Reglas de correlación**.

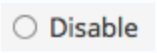
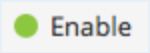
   Se abre la pestaña de reglas seleccionada.

Este es un ejemplo de la pestaña Reglas de aplicación.



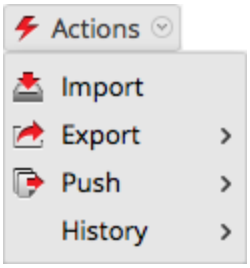

### Barra de herramientas de la pestaña Reglas

La barra de herramientas es la misma para todas las instancias de la vista Configuración > pestañas Reglas.

| Característica | Descripción |
|---|---|
| Acciones | Muestra el menú **Acciones**. |
|  | Agrega una nueva regla a un servicio. |
|  | Elimina una regla de un servicio. |
|  | Permite modificar reglas. |
|  | Desactiva una regla (sin eliminarla). |
|  | Activa (vuelve a activar) una regla. |
| Filtro | El campo donde se ingresa una cadena de búsqueda. Security Analytics 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. |
| Exportación | 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.<br>• **Migrar > 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.<br>• **Migrar > Selección.** Migra las reglas seleccionadas a otros servicios. Tiene dos opciones:<br>  • **Reemplazo.** Elimina todas las reglas de los servicios objetivo y las reemplaza por las reglas seleccionadas en el servicio de origen.<br>  • **Combinar.** Combina las reglas seleccionadas con las reglas existentes en los servicios de destino. |
| Historial | Muestra las últimas diez instantáneas de reglas aplicadas mediante Security Analytics. Puede seleccionar y aplicar (restaurar) un snapshot en el Decoder en cualquier momento. |

#### Acciones del menú contextual de la cuadrícula 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. |

**Temas**

- Pestaña Reglas de aplicación
- Pestaña Reglas de correlación
- Pestaña Reglas de red
- Guía de reglas y consultas

## Pestaña Reglas de aplicación

En este tema se describen las funciones para crear y administrar reglas de aplicación en la vista Configuración de servicios > pestaña Reglas de aplicación.

La pestaña Reglas de aplicación permite administrar las reglas de aplicación. Security Analytics aplica reglas de aplicación en el nivel de sesión.

Paso 4. Configurar reglas de Decoder proporciona información adicional y Configurar reglas de aplicaciones proporciona instrucciones para crear reglas de aplicación.

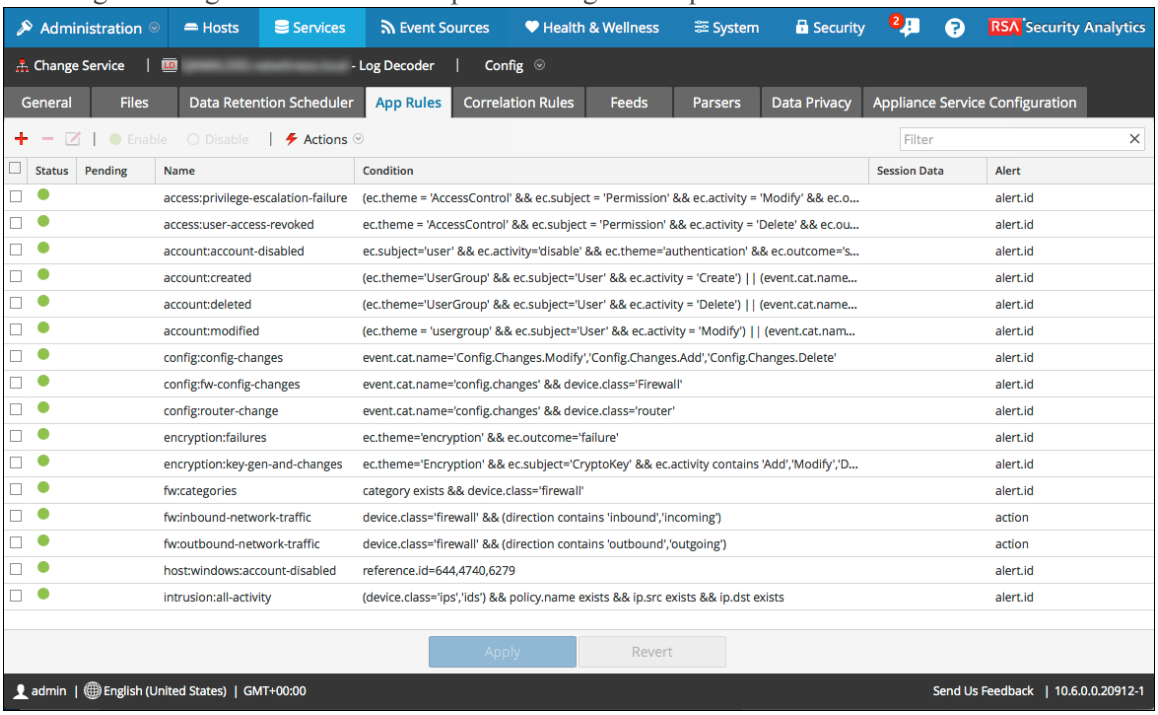
La barra de herramientas de la pestaña Reglas de aplicación es común a todos los tipos de reglas. Vista Configuración de servicios: Pestañas Reglas proporciona información sobre la barra de herramientas y las acciones comunes para las reglas.

Para acceder a la pestaña Reglas de aplicación:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio Decoder o Log Decoder y elija **>Ver > Configuración**.

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Reglas de aplicación**.

En la siguiente figura se muestra una pestaña Reglas de aplicación.

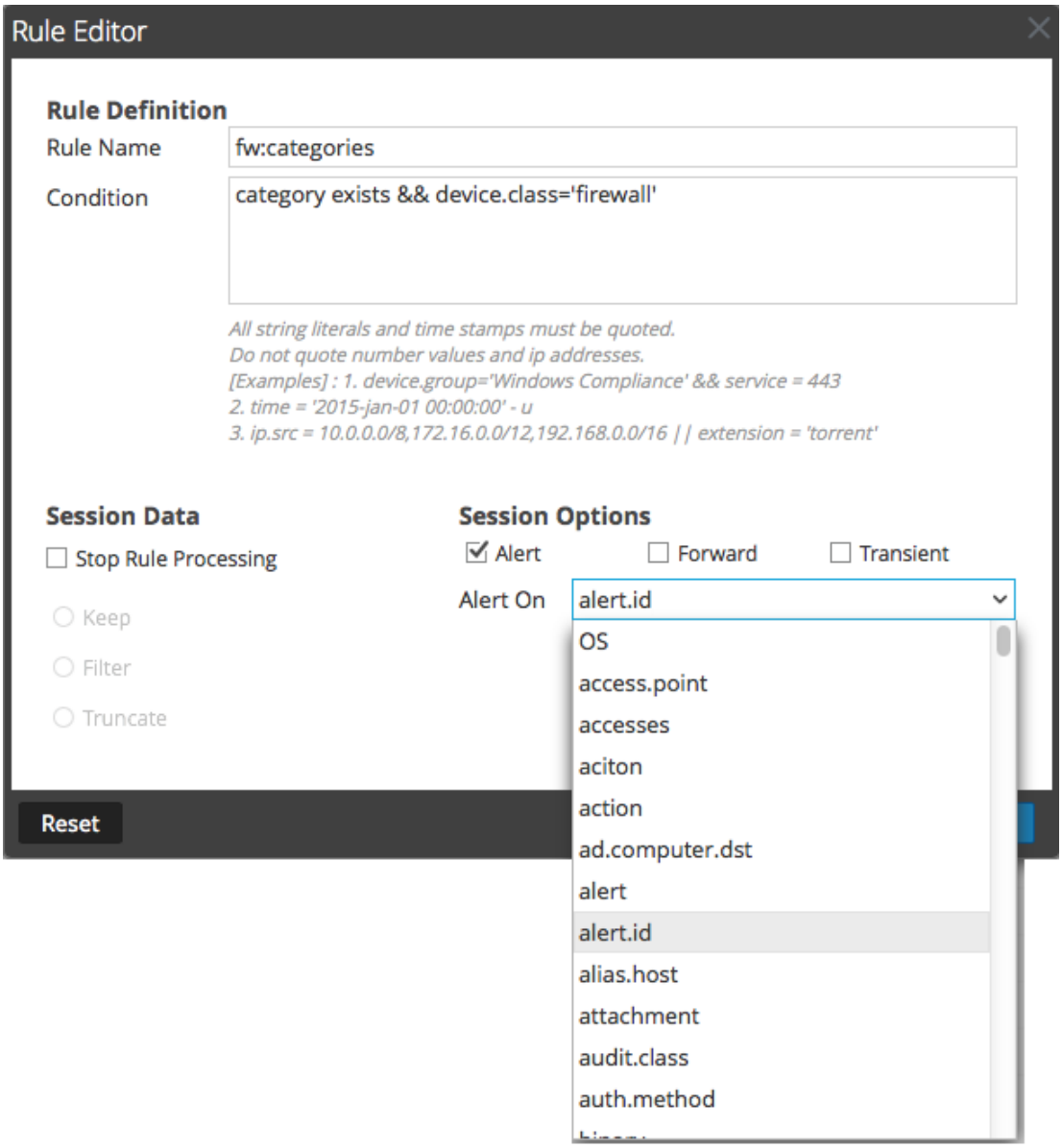


### Columnas de la pestaña Reglas de aplicación

| Columna | Descripción |
|---|---|
| **Pending** | 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 se coincide 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. |
| **Status** | Esta columna indica si la regla está activada o desactivada con un ícono 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 los campos y las opciones 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 advertencias de sintaxis.<br><br>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. Guía de reglas y consultas proporciona 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. |
| **Mantener** | 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 conservan. |
| **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**. |
| **Avanzar** | 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. |
| **Cancelar** | Cancela las ediciones y cierra el cuadro de diálogo Editor de regla. |
| **OK** | 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 obsoleta. |

## Pestaña Reglas de correlación

En este tema se describen las funciones para crear y administrar reglas de correlación en la vista Configuración de servicios > pestaña Reglas de correlación.

La 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. Security Analytics aplica las reglas de correlación en una ventana de tiempo móvil configurable.

Paso 4. Configurar reglas de Decoder proporciona información adicional y Configurar reglas de correlación proporciona instrucciones para crear reglas de correlación.

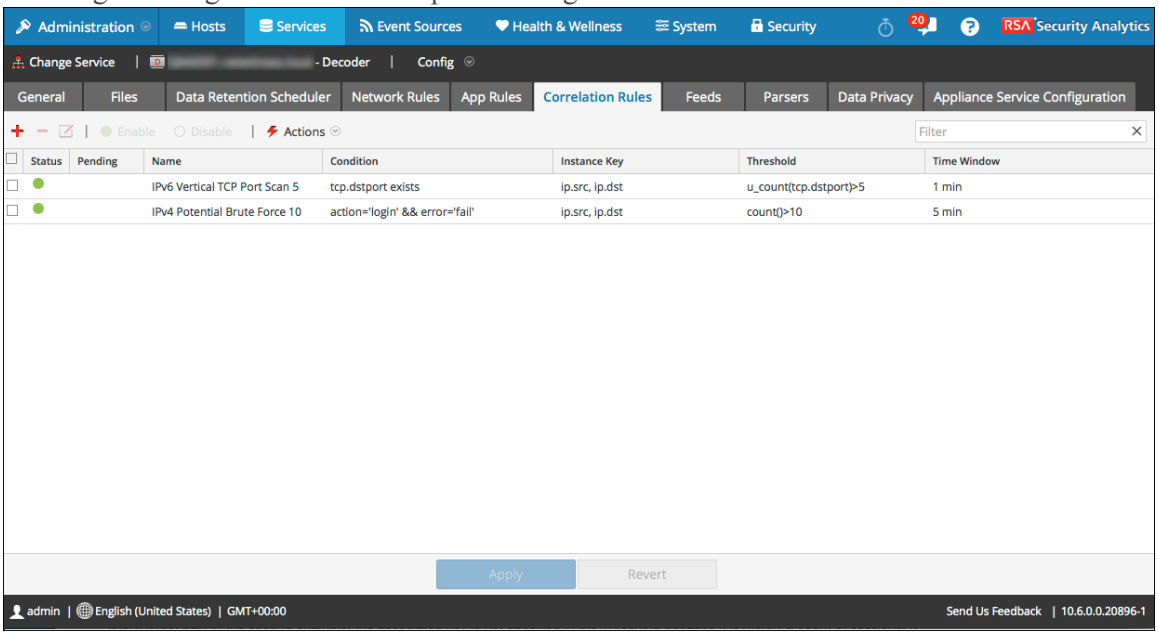
La barra de herramientas de la pestaña Reglas de correlación es común a todos los tipos de reglas. Vista Configuración de servicios: Pestañas Reglas proporciona información sobre la barra de herramientas y las acciones comunes para las reglas.

Para acceder a la pestaña Reglas de correlación:

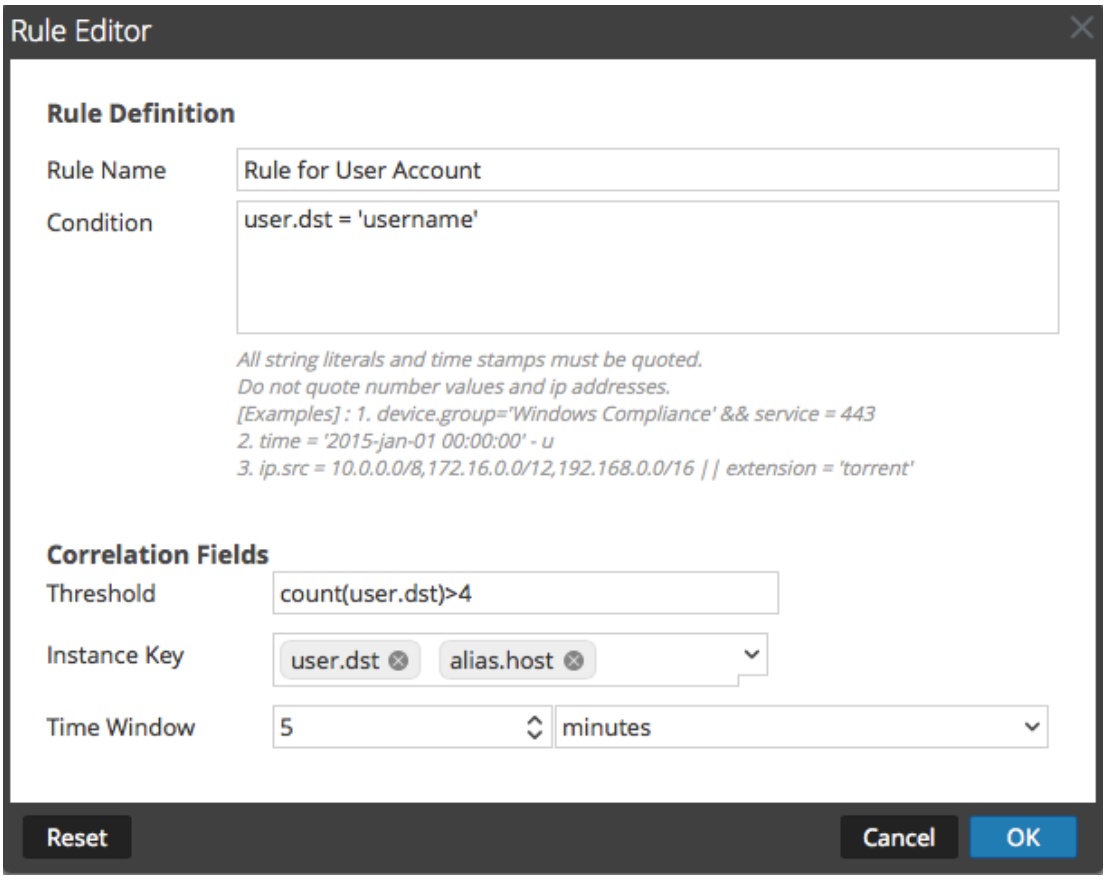
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio y elija  **>Ver > Configurar.**

   Se muestra la vista Configurar del servicio seleccionado.
3. Haga clic en la pestaña **Reglas de correlación**.

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 |
|---|---|
| **Pending** | 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 se coincide con ella.<br><br>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. Guía de reglas y consultas proporciona detalles adicionales. |

| Columna | Descripción |
|---|---|
| **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. |
| **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:<br>• u_count(associated_key) = el conteo de valores únicos de la clave especificada. Se requiere una clave.<br>• sum(associated_key) = los valores de la clave especificada. Se requiere una clave.<br>• 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. |
| **Status** | Esta columna indica si la regla está activada o desactivada con un ícono 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. |
| **OK** | Guarda la regla nueva o editada y la agrega a la cuadrícula de reglas. El cuadro de diálogo Editor de regla se cierra. |

| Acción | Descripción |
| --- | --- |
| **Guardar** | (Solo reglas con sintaxis obsoleta) Aplica una regla corregida individualmente al servicio Decoder. Consulte Corregir las reglas con sintaxis obsoleta. |

## Pestaña Reglas de red

En este tema se describen las funciones para crear y administrar reglas de red en la vista Configuración de servicios > pestaña Reglas de red.

La pestaña Reglas de red permite administrar las reglas de red. Security Analytics aplica las 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 Packet Decoders.

Paso 4. Configurar reglas de Decoder proporciona información adicional y Configurar reglas de red proporciona instrucciones para crear reglas de red.

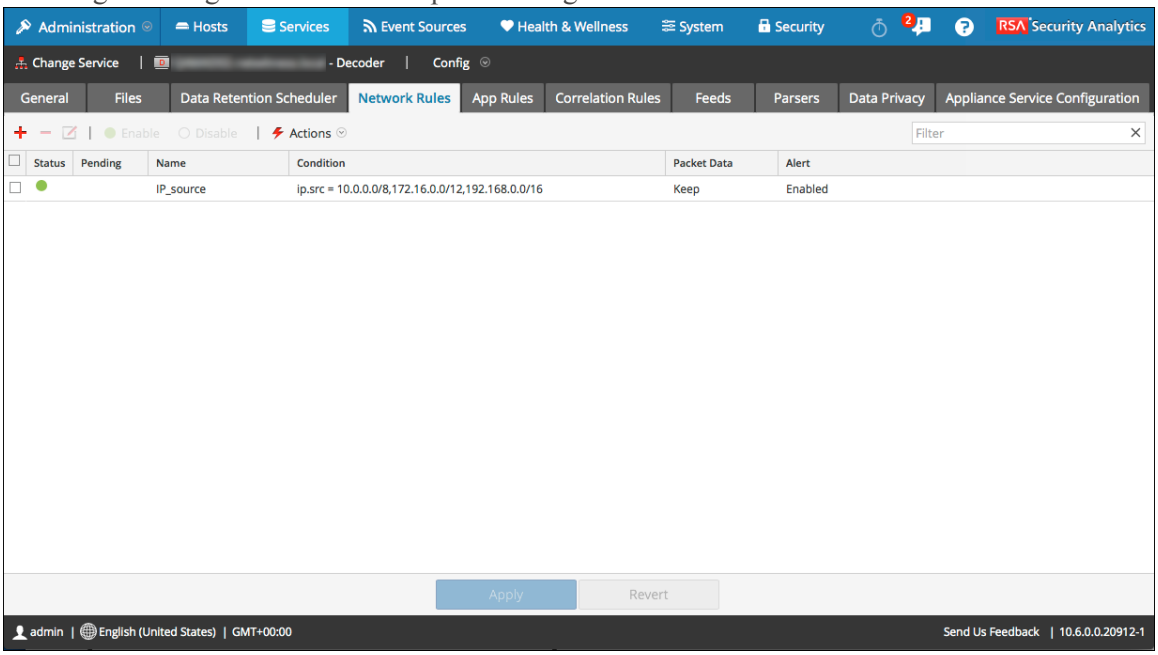
La barra de herramientas de la pestaña Reglas de red es común a todos los tipos de reglas. Vista Configuración de servicios: Pestañas Reglas proporciona información sobre la barra de herramientas y las acciones comunes para las reglas.

Para acceder a la pestaña Reglas de red:

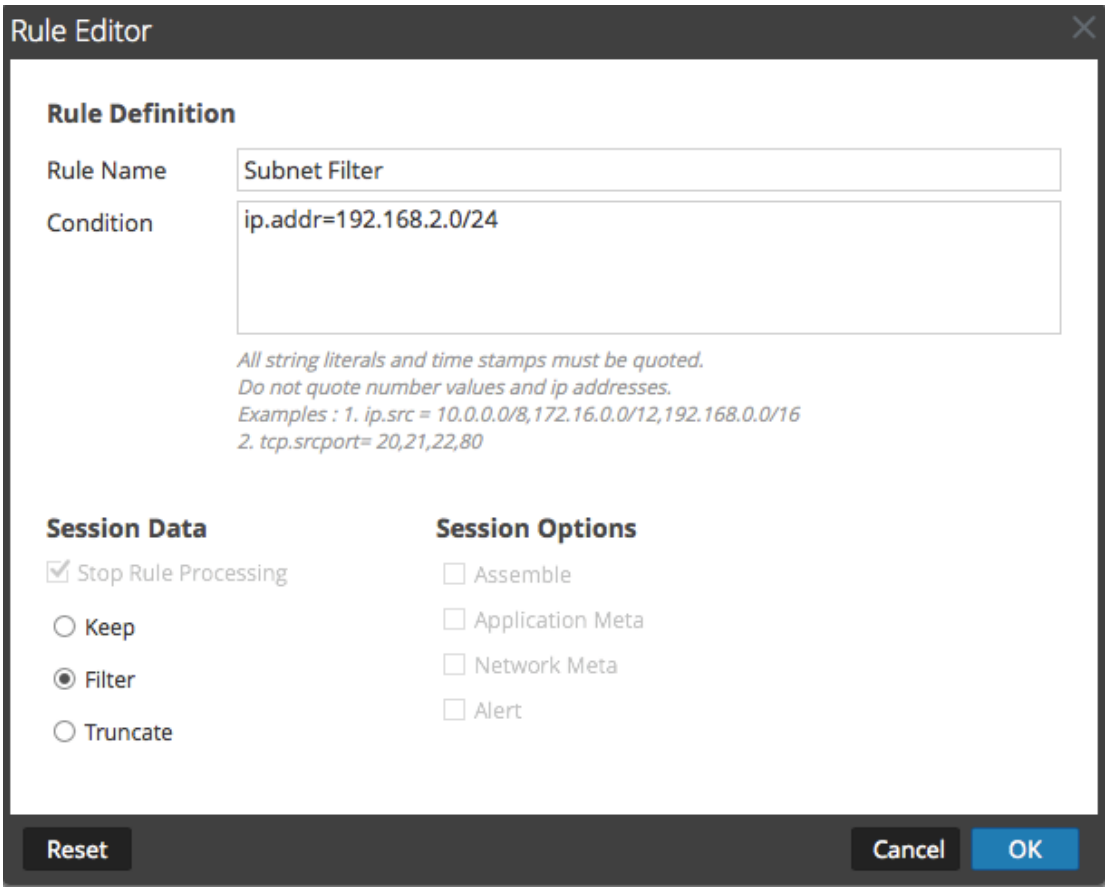
1. En el menú de **Security Analytics**, seleccione **Administration > Servicios.**
2. Seleccione un servicio Decoder y elija  **> Ver > Configuración**.

   Se muestra la vista Configurar del servicio seleccionado.
3. Seleccione la pestaña **Reglas de red**.

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.




**Características**

En la siguiente tabla se describen las columnas de la cuadrícula Reglas de red.

| Columna | Descripción |
|---|---|
| **Pending** | 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 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 se coincide 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**. |

| Columna | Descripción |
|---|---|
| **Alerta** | Esta columna indica si el Decoder genera una alerta personalizada cuando los metadatos coinciden con la regla. Los valores posibles son **Activada** o **Desactivada**. |
| **Status** | Esta columna indica si la regla está activada o desactivada con un ícono 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 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 advertencias de sintaxis.<br><br>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. Guía de reglas y consultas proporciona detalles adicionales.<br><br>Claves de metadatos compatibles en condiciones de reglas de red describe las claves de metadatos que Security Analytics admite para usar en 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 |
|---|---|
| **Mantener** | 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.

| Opción | 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. |
| **OK** | 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 obsoleta. |

### Claves de metadatos compatibles en las reglas de red

Las reglas de red constan 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 se pueden aplicar a varias capas (por ejemplo, cuando una regla de red filtra puertos específicos de una dirección IP específica). 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 que Security Analytics admite para 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. |

| Clave de metadatos | Descripción |
|---|---|
| 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. |
| 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. |

## Guía de reglas y consultas

Todas las consultas y las condiciones de regla en los servicios de RSA Security Analytics 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.**

Por ejemplo:

- `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 usar `service=80` o `service = 80`.

### Ejemplos de reglas

En la siguiente tabla se muestran ejemplos de condiciones de regla. Puede usar condiciones de regla para recopilaciones de retención de registros en un Archiver y para 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 de la base de datos Core.

Para obtener información detallada sobre la sintaxis de las reglas en Security Analytics, consulte **Cláusulas Where** en el tema **Consultas** de la *Guía de ajuste de la base de datos de RSA Security Analytics 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' |

### Configuración del modo estricto para Security Analytics 10.6

Desde la versión 10.2, Security Analytics ha utilizado un analizador moderno para las reglas y las consultas, el cual define estrictamente la sintaxis válida. Cuando un servicio principal encuentra sintaxis obsoleta, escribe una advertencia acerca de esta en los registros de Security Analytics. Security Analytics ahora aplica el análisis estricto a las reglas de aplicación, red y correlación nuevas. El analizador heredado de las generaciones anteriores, ahora obsoleto, permite una sintaxis ambigua que puede dar lugar a resultados imprevistos. Aunque Security Analytics 10.6 continúa siendo compatible con la sintaxis obsoleta, las versiones futuras dejarán de serlo.

Después de la actualización a Security Analytics 10.6, las reglas con sintaxis obsoleta se resaltan en la interfaz del usuario. 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 obsoleta** en la *Guía de configuración de Decoder y Log Decoder*.

Las estadísticas **/decoder/config/rules/rule.errors** y **/concentrator/config/rules/rule.errors**, que se incorporaron en 10.6, contienen el conteo de reglas con errores. Si **rule.errors** es distinto de cero, Security Analytics genera una alerta de Estado y condición para indicar que debe corregir las reglas.

Además, hay una ruta de migración para las consultas de sistemas externos. Después de una actualización desde una versión anterior, el sistema funciona en el modo obsoleto (lo controla **/sdk/config/query.parse**). En el modo obsoleto, el servicio continúa utilizando el analizador antiguo para todas las consultas que no pasan el análisis estricto. Los errores se registran y se envía un mensaje al cliente en el cual se informa la falla del análisis estricto. Pero la consulta se ejecuta y devuelve resultados como en las versiones anteriores. Debe monitorear los registros y los clientes externos en busca de informes, tableros, reglas, etc. que estén escritos con sintaxis obsoleta y resolver esos problemas a medida que surgen.

Después de resolver los problemas, puede cambiar todos los servicios principales (Decoders, Log Decoders, Concentrators, Brokers y Archivers) al modo estricto y monitorearlos en busca de problemas. En el modo estricto no se utiliza el analizador antiguo y cualquier infracción en el análisis devuelve errores. Esta tarea se debe ejecutar antes de cualquier actualización principal después de 10.6, porque el analizador antiguo se eliminará en versiones futuras y no existirá la opción de funcionamiento en el modo obsoleto.

De manera predeterminada, todas las instalaciones nuevas funcionan en el modo estricto. Si planea agregar un dispositivo nuevo a una infraestructura existente que se ejecuta en el modo obsoleto, en la vista Explorar (Administration > Servicios > seleccione un servicio y, en el menú Acciones, seleccione Ver > Explorar), puede cambiar **/sdk/config/query.parse** al modo obsoleto hasta que la plataforma completa se haya cambiado al modo estricto.

En Security Analytics 10.6, toda la validación de reglas funcionará siempre en el modo estricto para impedir la creación de problemas de sintaxis.

#### Sintaxis válida con el analizador moderno

Las siguientes son reglas con sintaxis válida que usan el analizador moderno:

- En todos los tipos 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 el carácter de escape o usar un carácter de comillas iniciales diferente. Los dos ejemplos siguientes son válidos (se usa la barra invertida como carácter de escape):
  - `username = "User's"`
  - `username = 'User\'s'`
- Para usar una barra invertida en una cadena literal, antepóngale un carácter de escape de barra invertida adicional: `\\`
- Todos los tipos de fecha/hora deben usar comillas para las fechas en este formato: `time = 'YYYY-MM-DD HH:MM:SS'`
- Todos los tipos de tiempo 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: dirección IP, direcciones Ethernet, valores numéricos, etc.
  Ejemplo: `service = 80 && ip.src = 192.168.1.1/16`

#### Ejemplos de sintaxis ambigua con el analizador antiguo

El siguiente es un ejemplo de sintaxis ambigua con el analizador antiguo obsoleto:

select * where alias.host = server-xeon

En la consulta anterior, parece lógico que el autor de la consulta desea obtener todos los metadatos en los cuales alias.host es igual a `server-xeon`. Lamentablemente, eso no sucede con el analizador heredado. En vez de esto, analiza esa consulta como `select * where alias.host = 'server'-'xeon'`. Por lo tanto, la convierte en una consulta de rango (valores ENTRE "server" y "xeon" con el uso del operador guion - sin comillas) y, debido a que es probable que ese rango devuelva resultados que no tienen ninguna relación con `server-xeon`, los usuarios podrían suponer que existe un problema en el motor de consultas. En el modo estricto de 10.6, obtendrá este error:

**expecting <quoted_string> here: "server-xeon"**

Esto informa de inmediato al usuario el motivo por el cual la consulta no se pudo analizar correctamente.

El siguiente es otro ejemplo de sintaxis ambigua con el analizador antiguo obsoleto:

```
select * where username=lastname,firstname
```

En el lenguaje de Security Analytics, puede especificar valores múltiples si los separa con comas (un operador OR implícito). Pero, ¿quería el autor de la consulta expresar `'lastname,firstname'` o deseaba buscar dos valores, `'lastname'` y `'firstname'`? Nuevamente, es ambiguo, pero el analizador heredado lo acepta (y lo convierte en `'lastname' OR 'firstname'`). Con el analizador moderno, debe expresar su intención con total claridad, ya sea `'lastname,firstname'` o `'lastname','firstname'`.

El siguiente ejemplo no se analiza correctamente:

```
select * where username = lastname, firstname
```

A primera vista, tal vez no se dé cuenta de que hay un espacio entre la coma y firstname. Debido a la ausencia de comillas, esto no se analiza correctamente con el analizador antiguo, pero este no devuelve un error de análisis. En su lugar, ejecuta la consulta (y descarta firstname por completo debido al problema del espacio en blanco). Lo que es peor, usted no sabría que la consulta ejecutada no es lo que envió, a menos que determinara mediante otros métodos que el conjunto de resultados está incompleto. Con el análisis estricto habilitado, esto devuelve un error de análisis, que es lo que siempre debería ocurrir. Por lo menos en las versiones anteriores (y en el modo obsoleto), los registros muestran un mensaje inmediatamente después del registro de auditoría para la consulta: **Rule '<rule name>' in deprecated format. Please make sure all text values are surrounded with quotes.**

## Vista Sistema de servicios: Decoders

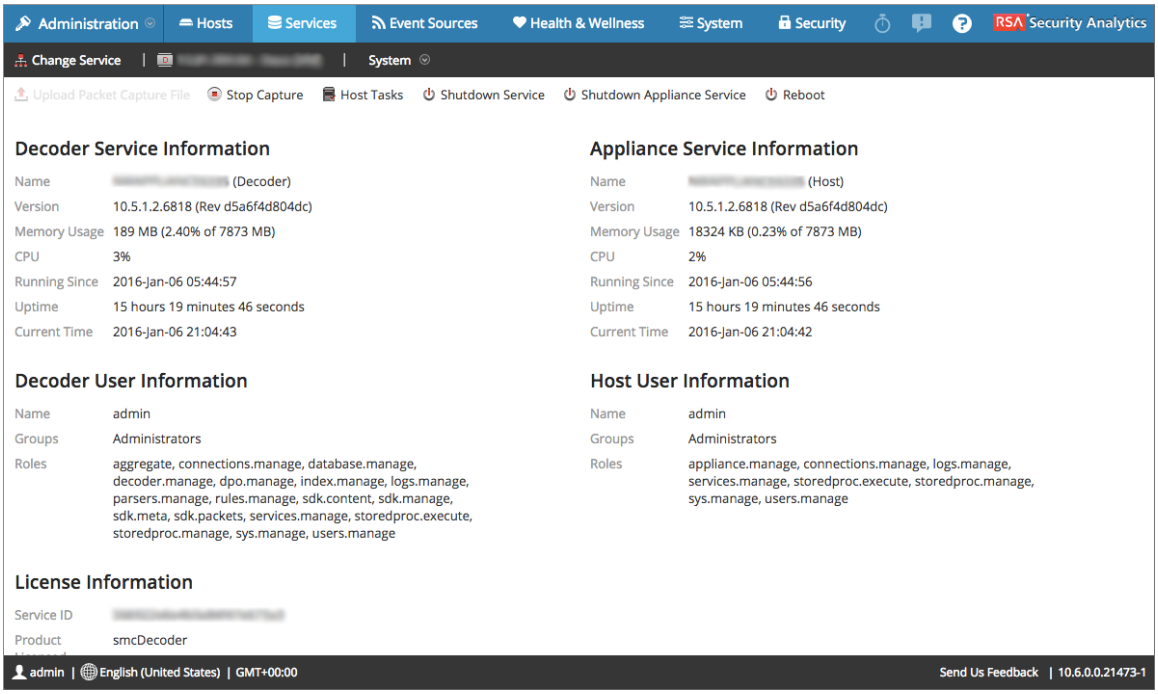
En este tema, se presentan las funcionalidades de la vista Sistema relacionadas específicamente con los Decoders y los Log Decoders.

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.

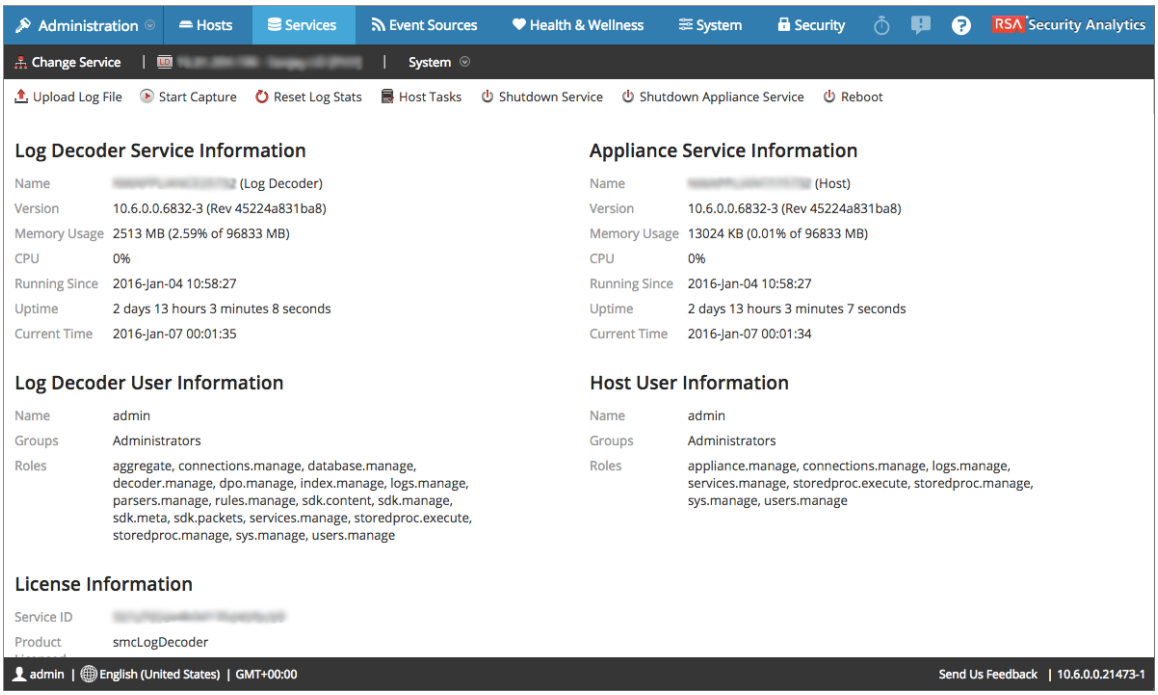
Para acceder a la vista Sistema de servicios de un Decoder:

1. En el menú de **Security Analytics**, seleccione **Administration > Servicios**.
   Se muestra la vista Servicios de Administration.
2. Seleccione un Decoder o un Log Decoder y elija  **> Ver> Sistema**.

Este es un ejemplo de la vista Sistema de servicios de un Decoder.



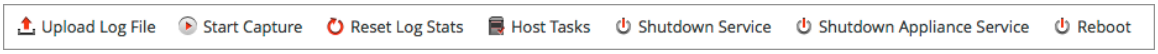

Este es un ejemplo de la vista Sistema de servicios de un Log Decoder.




## Características

### 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 ofrece una manera de seleccionar un archivo de captura de paquete (.pcap) para cargar en el Decoder seleccionado. Para obtener más información, consulte Cargar archivo de captura de paquete.<br>**Nota:** Esta opción no se aplica a los Log Decoders. |

| Acción | Descripción |
|---|---|
| **Cargar archivo de registro** | Muestra un cuadro de diálogo que ofrece 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. |

**Tema relacionado**

- **Vista Sistema de servicios** en la *Guía de introducción de hosts y servicios*