# Solución de problemas entre el sistema FireSIGHT y eStreamer Client (SIEM)

## Contenido



## Introducción

Event Streamer (eStreamer) permite transmitir varios tipos de datos de eventos desde un sistema FireSIGHT a una aplicación cliente desarrollada a medida. Después de crear una aplicación cliente, puede conectarla a un servidor eStreamer (por ejemplo, un FireSIGHT Management Center), iniciar el servicio eStreamer y comenzar a intercambiar datos. La integración de eStreamer requiere programación personalizada, pero permite solicitar datos específicos de un dispositivo. Este documento describe cómo se comunica un cliente eStreamer y cómo resolver un problema con un cliente.

# Método de comunicación entre el cliente eStreamer y el servidor

Existen cuatro etapas principales de comunicación entre un cliente y el servicio eStreamer:

## Paso 1: El cliente establece una conexión con el servidor eStreamer

En primer lugar, un cliente establece una conexión con el servidor eStreamer y la conexión es autenticada por ambas partes. Antes de que un cliente pueda solicitar datos de eStreamer, el cliente debe iniciar una conexión TCP SSL habilitada con el servicio eStreamer. Cuando el cliente inicia la conexión, el servidor eStreamer responde, iniciando un intercambio de señales SSL con el cliente. Como parte del protocolo de enlace SSL, el servidor eStreamer solicita el certificado de autenticación del cliente y comprueba que el certificado es válido.

Una vez establecida la sesión SSL, el servidor eStreamer realiza una verificación adicional posterior a la conexión del certificado. Una vez finalizada la verificación posterior a la conexión, el servidor de eStreamer espera una solicitud de datos del cliente.

## Paso 2: El cliente solicita datos del servicio eStreamer

En este paso, el cliente solicita datos del servicio eStreamer y especifica los tipos de datos que se transmitirán. Un único mensaje de solicitud de evento puede especificar cualquier combinación de datos de evento disponibles, incluidos los metadatos de evento. Una única solicitud de perfil de host puede especificar un solo host o varios. Hay dos modos de solicitud disponibles para solicitar datos de eventos:

- **Solicitud de flujo de evento:** El cliente envía un mensaje que contiene indicadores de solicitud que especifican los tipos de eventos solicitados y la versión de cada tipo, y el servidor eStreamer responde transmitiendo los datos solicitados.
- **Solicitud ampliada:** El cliente envía una solicitud con el mismo formato de mensaje que para las solicitudes de flujo de eventos, pero establece un indicador para una solicitud ampliada. Esto inicia una interacción de mensaje entre el cliente y el servidor eStreamer a través del cual el cliente solicita información adicional y combinaciones de versiones no disponibles a través de solicitudes de flujo de eventos.

## Paso 3: eStreamer establece el flujo de datos solicitado

En esta etapa, eStreamer establece el flujo de datos solicitado al cliente. Durante los períodos de inactividad, eStreamer envía periódicamente mensajes nulos al cliente para mantener la conexión abierta. Si recibe un mensaje de error del cliente o de un host intermedio, cierra la conexión.

### Paso 4: La Conexión Finaliza

El servidor eStreamer también puede cerrar una conexión de cliente por los siguientes motivos:

- Cada vez que se envía un mensaje, se produce un error. Esto incluye tanto los mensajes de datos de eventos como el mensaje de activación nula que eStreamer envía durante los períodos de inactividad.
- Se produce un error al procesar una solicitud de cliente.
- La autenticación del cliente falla (no se envía ningún mensaje de error).
- El servicio eStreamer se está cerrando (no se envía ningún mensaje de error).

## El cliente no muestra ningún evento

Si no ve ningún evento en la aplicación cliente de eStreamer, siga los pasos que se indican a continuación para solucionar este problema:

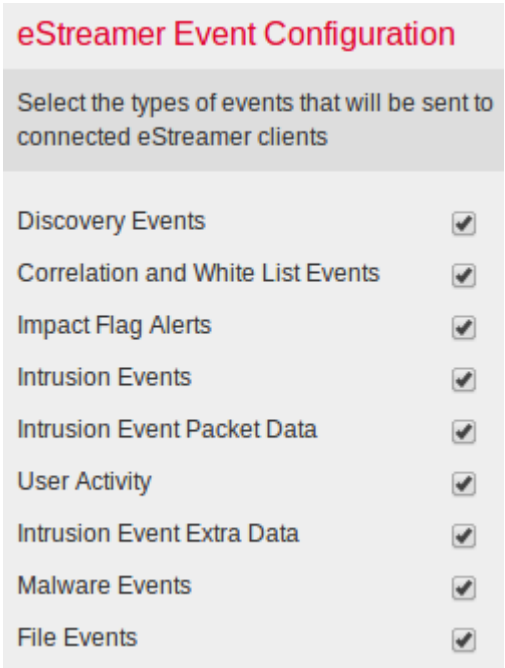
### Paso 1: Verifique la Configuración

Puede controlar qué tipos de eventos puede transmitir el servidor de eStreamer a las aplicaciones cliente que los soliciten. Para configurar los tipos de eventos transmitidos por eStreamer, siga estos pasos:

1. Vaya a **Sistema > Local > Registro**.

2. Haga clic en la pestaña **eStreamer**.

3. En el menú **Configuración de Eventos de eStreamer**, seleccione las casillas de control situadas junto a los tipos de eventos que desea que eStreamer envíe a los clientes que lo soliciten.



**Nota:** Asegúrese de que la aplicación cliente solicita los tipos de eventos que desea que reciba. El mensaje de solicitud debe enviarse al servidor eStreamer (FireSIGHT Management Center o dispositivo administrado).

4. Haga clic en **Guardar**.

### Paso 2: Verificar el certificado

Asegúrese de agregar los certificados requeridos. Para que eStreamer pueda enviar eventos de eStreamer a un cliente, éste debe agregarse a la base de datos de peers del servidor eStreamer mediante la página de configuración de eStreamer. El certificado de autenticación generado por el servidor eStreamer también debe copiarse en el cliente.

### Paso 3: Verifique los mensajes de error

Identifique cualquier error obvio relacionado con eStreamer en /var/log/messages mediante el siguiente comando:

```
admin@FireSIGHT:~$ grep -i estreamer /var/log/messages | grep -i error
```

### Paso 4: Verifique la conexión

Compruebe que el servidor acepta conexiones entrantes.

```
admin@FireSIGHT:~$ netstat -an | grep 8302
```

El resultado debe ser similar al siguiente. Si no es así, es posible que el servicio no se esté ejecutando.

```
tcp 0 0 <local_ip>:8302 0.0.0.0:* LISTEN
```

### Paso 5: Comprobar el estado del proceso

Para verificar si se está ejecutando un proceso sfestreamer, utilice el siguiente comando:

```
admin@FireSIGHT:~$ pstree -a | grep -i sfestreamer
```

## El cliente muestra eventos duplicados

### Controlar eventos duplicados mostrados en un cliente

El servidor de eStreamer no mantiene un historial de los eventos que envía, por lo que la aplicación cliente debe comprobar si hay eventos duplicados. Los eventos duplicados pueden ocurrir por diversas razones.  Por ejemplo, al iniciar una nueva sesión de transmisión, la hora especificada por el cliente como punto de inicio de la nueva sesión puede tener varios mensajes, algunos de los cuales se han enviado en la sesión anterior y otros no. eStreamer envía todos los mensajes que cumplen los criterios de solicitud especificados. Las aplicaciones cliente de EStreamer deben estar diseñadas para detectar y desduplicar cualquier duplicado resultante.

### Administrar solicitudes duplicadas de datos

Si solicita varias versiones de los mismos datos, ya sea mediante varios indicadores o varias solicitudes extendidas, se utilizará la versión más alta. Por ejemplo, si eStreamer recibe solicitudes de indicadores para eventos de detección versión 1 y 6 y una solicitud ampliada para la versión 3, envía la versión 6.

## El cliente muestra un ID de regla de snort (SID) incorrecto

Esto suele ocurrir debido a un conflicto de SID cuando se importa una regla al sistema, el SID se vuelve a asignar internamente.

Para utilizar el SID que ingresó, en lugar del SID reasignado, debe habilitar el *encabezado extendido*. El bit 23 solicita encabezados de eventos extendidos. Si este campo se establece en 0, los eventos se envían con un encabezado de evento estándar que sólo incluye el tipo de registro y la longitud del registro.

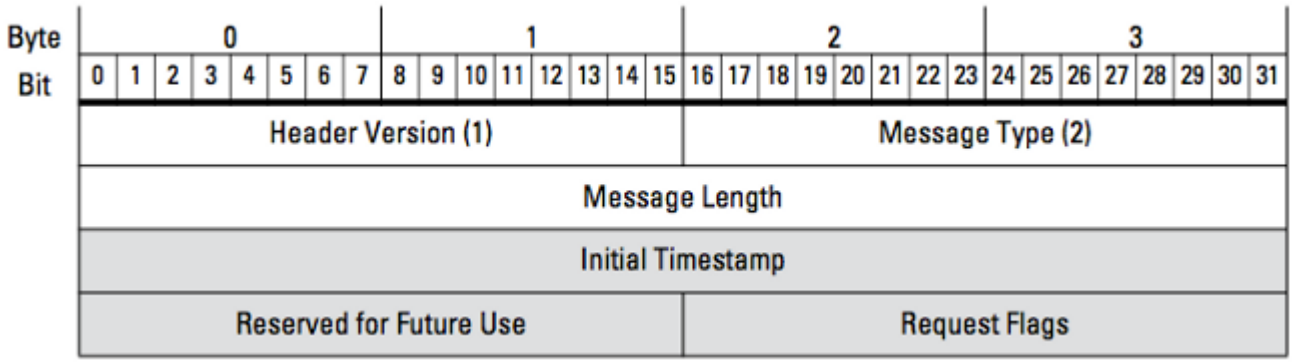



*Figura: El diagrama ilustra el formato de mensaje utilizado para solicitar datos de eStreamer. Los campos específicos del formato del mensaje de solicitud se resaltan en gris.*

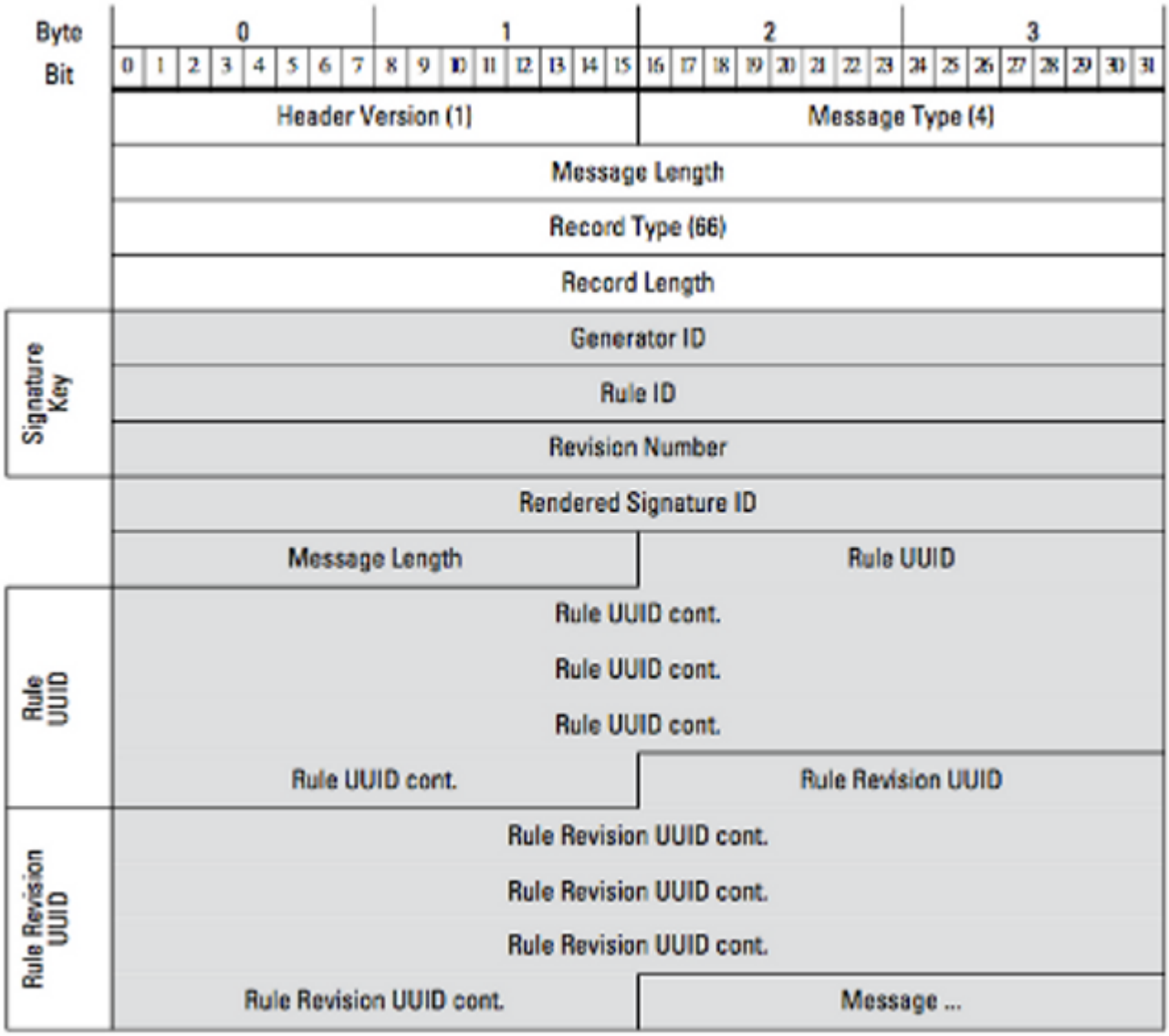



*Figura: El diagrama ilustra el formato de la información de mensaje de regla para un evento que se transmite dentro de un registro de mensaje de regla. Muestra el* ***RuleID*** *(que está utilizando ahora) y el* ***Rendered Signature ID*** *(que es el número que espera).*

> **Consejo:** Para encontrar la descripción detallada de cada bit y mensaje, lea la *Guía de Integración de eStreamer*.

# Recopilar y analizar datos adicionales para solucionar problemas

## Prueba con el script ssl_test.pl

Utilice la secuencia de comandos ssl_test.pl proporcionada en el *Kit de desarrollo de software (SDK) de Event Streamer* para identificar el problema. El SDK está disponible en un archivo zip en el sitio de soporte. Las instrucciones para el script están disponibles en el archivo README.txt, que se incluye en ese archivo zip.

## Paquete de captura (PCAP)

Capture paquetes en la interfaz de administración del servidor eStreamer y analice el paquete. Compruebe que el tráfico no está bloqueado ni denegado en ningún lugar de la red.

## Generar archivo de solución de problemas

Si ha completado los pasos de solución de problemas anteriores y sigue sin poder determinar el problema, genere un archivo de solución de problemas desde FireSIGHT Management Center. Proporcione todos los datos adicionales de solución de problemas al Soporte técnico de Cisco para un análisis más detallado.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).