Resuelva problemas los problemas entre el sistema y el cliente del eStreamer (SIEM) de FireSIGHT

Contenido

Introducción

El bobinador de cintas en modo continuo del evento (eStreamer) permite que usted fluya varias clases de datos de evento de un sistema de FireSIGHT a una aplicación de cliente aduana-desarrollada. Después de que usted cree una aplicación de cliente, usted puede conectarse a un servidor del eStreamer (por ejemplo, un centro de administración de FireSIGHT), comienza el servicio del eStreamer, y comienza los datos que intercambian. la integración del eStreamer requiere la programación de encargo, pero permite que usted pida los datos específicos de un dispositivo. Este documento describe cómo un cliente del eStreamer comunica y cómo resolver problemas un problema con un cliente.

Método de comunicación entre el cliente y servidor del eStreamer

Hay cuatro etapas importantes de comunicación que ocurren entre un cliente y el servicio del eStreamer:

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

Primero, un cliente establece una conexión con el servidor del eStreamer y la conexión es autenticada por ambas partes. Antes de que un cliente pueda pedir los datos del eStreamer, el cliente debe iniciar una conexión TCP SSL-habilitada con el servicio del eStreamer. Cuando el cliente inicia la conexión, el servidor del eStreamer responde, iniciando un contacto SSL con el cliente. Como parte del contacto SSL, el servidor del eStreamer pide el certificado de la autenticación de cliente, y lo verifica que el certificado sea válido.

Después de que establezcan a la sesión SSL, el servidor del eStreamer realiza una verificación adicional de la poste-conexión del certificado. Después de que se acabe la verificación de la poste-conexión, el servidor del eStreamer aguarda un pedido de datos del cliente.

Paso 2: Datos de los pedidos de cliente del servicio del eStreamer

En este paso, los datos de los pedidos de cliente del servicio del eStreamer y especifican los tipos de datos que se fluirán. Un solo mensaje request del evento puede especificar cualquier combinación de datos de evento disponibles, incluyendo los meta datos del evento. Una petición del perfil del solo host puede especificar un solo host o a los host múltiples. Dos modos de la petición están disponibles para pedir el data&colon del evento;

- **Petición de la secuencia del evento:** El cliente somete un mensaje que contiene los indicadores de la petición que especifican los tipos de evento y la versión pedidos de cada tipo, y el servidor del eStreamer responde fluyendo los datos pedidos.
- **Petición extendida:** El cliente somete una petición con lo mismo Message format (Formato del mensaje) que para las peticiones de la secuencia del evento pero fija un indicador para una petición extendida. Esto inicia una interacción del mensaje entre el cliente y el servidor del eStreamer a través de quienes los pedidos de cliente información adicional y las combinaciones de la versión no disponibles vía la secuencia del evento piden.

Paso 3: el eStreamer establece la secuencia de datos pedida

En esta etapa, el eStreamer establece la secuencia de datos pedida al cliente. Durante los períodos de inactividad, el eStreamer envía los mensajes NULOS periódicos 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 termina

El servidor del eStreamer puede también cerrar una conexión cliente por las razones siguientes:

- En cualquier momento el envío de un mensaje da lugar a un error. Esto incluye los mensajes de datos de evento y el eStreamer señal de mantenimiento nulo del mensaje envía durante los períodos de inactividad.
- Un error ocurre mientras que procesa un pedido de cliente.
- La autenticación de cliente falla (no se envía ningún mensaje de error).
- el servicio del eStreamer está apagando (no se envía ningún mensaje de error).

El cliente no muestra ningún evento

Si usted no ve ninguna eventos en su aplicación de cliente del eStreamer, siga por favor los pasos abajo para resolver problemas este problema:

Paso 1: Verifique la Configuración

Usted puede controlar que los tipos de eventos el servidor del eStreamer pueden transmitir a las aplicaciones de cliente que las piden. Para configurar los tipos de eventos transmitidos por el eStreamer siga los pasos abajo:

1. Navegue al **sistema > al Local > al registro**.

2. Haga clic la lengueta del **eStreamer**.

3. Bajo menú de la **configuración de evento del eStreamer**, seleccione las casillas de verificación al lado de los tipos de eventos que usted quisiera que el eStreamer enviara a pedir a los clientes.

> Nota: Aseegurese su aplicación de cliente pide los tipos de eventos que usted quisiera que recibieran. El mensaje request tiene que ser enviado al servidor del eStreamer (centro de administración o dispositivo administrado de FireSIGHT).

4. Haga clic en Save (Guardar).

Paso 2: Verifique el certificado

Aseegurese que los Certificados requeridos están agregados. Antes de que el eStreamer pueda enviar los eventos del eStreamer a un cliente, el cliente debe ser agregado a la base de datos de los pares del servidor del eStreamer usando la página de configuración del eStreamer. El

certificado de la autenticación generado por el servidor del eStreamer se debe también copiar al cliente.

Paso 3: Mensajes de error del control

Identifique cualquier error relacionado obvio del eStreamer en `/var/log/messages` usando el siguiente comando:

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

Paso 4: Verifique la conexión

Verifique que el servidor esté validando las conexiones entrantes.

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

La salida debe parecer abajo. Si no, entonces el servicio puede no ejecutarse.

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

Paso 5: Marque el estatus del proceso

Para verificar si hay un funcionamiento de proceso del `sfestreamer`, utilice por favor el siguiente comando:

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

Eventos duplicados de las demostraciones del cliente

Eventos duplicados de la manija visualizados en un cliente

El servidor del eStreamer no guarda un historial de los eventos que envía, así que la aplicación de cliente debe marcar para saber si hay eventos duplicados. Los eventos duplicados pueden ocurrir por una variedad de razones. Por ejemplo, al comenzar una nueva sesión que fluye, la época especificada por el cliente como el punto de partida para la nueva sesión puede tener mensajes múltiples, algunos de los cuales pudieron haber sido enviadas en la sesión anterior y algunos de los cuales no eran. el eStreamer envía todos los mensajes que cumplan los criterios especificados de la petición. Las aplicaciones de cliente de EStreamer se deben diseñar para detectar y de-duplicado cualquier duplicado resultante.

Maneje las peticiones duplicados los datos

Si usted pide las versiones múltiples de los mismos datos, por los indicadores múltiples o las

peticiones extendidas múltiples, se utiliza la versión más avanzada. Por ejemplo, si el eStreamer recibe los pedidos del indicador la versión 1 y 6 de los eventos de la detección y un pedido extendido la versión 3, envía la versión 6.

El cliente muestra la regla incorrecta ID (el SID) del Snort

Esto sucede generalmente debido a un conflicto SID cuando una regla se importa en el sistema, el SID re-se asocia internamente.

Para utilizar el SID que usted ingresó, bastante que el SID re-asociado, usted tiene que habilitar la *encabezado extendida*. Mordido 23 encabezados del evento extendidos de las peticiones. Si este campo se fija a 0, los eventos se envían con un encabezado del evento estándar que incluya solamente el tipo de registro y la longitud de registro.

Figura: El diagrama ilustra Message format (Formato del mensaje) usado para pedir los datos del eStreamer. Los campos específicos al formato del mensaje request se resaltan en el gris.

Figura: El diagrama ilustra el formato de la información de mensajes de la regla para un evento que se transmita dentro de un expediente del mensaje de la regla. Muestra el ***RuleID*** *(cuál usted ahora está utilizando) y el* ***ID de la firma rendido*** *(cuál es el número que usted espera).*

> Consejo: Para encontrar la descripción del detalle de cada bit y mensaje, lea el *guía de integración del eStreamer*.

Recoja y analice los datos adicionales del Troubleshooting

Pruebe usando el script ssl_test.pl

Utilice el `script ssl_test.pl` proporcionado en el *Software Development Kit de* EventStreamer *(SDK)* para identificar el problema. El SDK está disponible en a archivo zip en el sitio de soporte. Las instrucciones para el script están disponibles en README.txt, `que` se incluye en ése archivo zip.

Paquete de la captura (PCAP)

Capture los paquetes en la interfaz de administración del servidor del eStreamer y analícelos. Verifique que el tráfico no esté bloqueado ni esté negado en alguna parte en su red.

Genere el archivo del Troubleshooting

Si usted completó los pasos de Troubleshooting antedichos, y usted no puede todavía determinar el problema, genere por favor un archivo del Troubleshooting de su centro de administración de FireSIGHT. Proporcione todos los datos adicionales del Troubleshooting al Soporte técnico de Cisco para el análisis adicional.