Pesquise defeitos edições entre o sistema de FireSIGHT e o cliente do eStreamer (SIEM)

Índice

Introdução

A flâmula do evento (eStreamer) permite que você flua diversos tipos dos dados de evento de um sistema de FireSIGHT a um aplicativo do cliente costume-em desenvolvimento. Depois que você cria um aplicativo do cliente, você pode conectá-lo a um server do eStreamer (por exemplo, um centro de gerenciamento de FireSIGHT), começa o serviço do eStreamer, e começa dados de troca. a integração do eStreamer exige a programação feita sob encomenda, mas permite que você peça dados específicos de um dispositivo. Este documento descreve como um cliente do eStreamer se comunica e como pesquisar defeitos uma edição com um cliente.

Método de comunicação entre o cliente e servidor do eStreamer

Há quatro fases principais de uma comunicação que ocorrem entre um cliente e o serviço do eStreamer:

Passo 1: O cliente estabelece uma conexão com o server do eStreamer

Primeiramente, um cliente estabelece uma conexão com o server do eStreamer e a conexão é autenticada por ambos os partidos. Antes que um cliente possa pedir dados do eStreamer, o cliente deve iniciar uma conexão de TCP SSL-permitida com o serviço do eStreamer. Quando o cliente inicia a conexão, o server do eStreamer responde, iniciando uma saudação de SSL com o cliente. Como parte da saudação de SSL, o server do eStreamer pede o certificado da autenticação de cliente, e verifica que o certificado é válido.

Depois que a sessão de SSL é estabelecida, o server do eStreamer executa uma verificação adicional da cargo-conexão do certificado. Depois que a verificação da cargo-conexão é terminada, o server do eStreamer espera uma solicitação de dados do cliente.

Passo 2: Dados dos pedidos do cliente do serviço do eStreamer

Nesta etapa, os dados dos pedidos do cliente do serviço do eStreamer e especificam os tipos de dados a ser fluídos. Um único mensagem request do evento pode especificar toda a combinação de dados de evento disponíveis, incluindo metadata do evento. Um pedido do perfil do host único pode especificar um host único ou uns host múltiplos. Dois modos do pedido estão disponíveis para pedir o data&colon do evento;

- **Pedido do córrego do evento:** O cliente submete uma mensagem que contém as bandeiras do pedido que especificam os tipos de evento e a versão pedidos de cada tipo, e o server do eStreamer responde fluindo os dados pedidos.
- **Pedido prolongado:** O cliente submete um pedido com o mesmo formato de mensagem que para pedidos do córrego do evento mas ajusta uma bandeira para um pedido prolongado. Isto inicia uma interação da mensagem entre o cliente e o server do eStreamer através de que as combinações da informação adicional e da versão dos pedidos do cliente não disponíveis através do córrego do evento pedem.

Passo 3: o eStreamer estabelece o fluxo de dados pedido

Nesta fase, o eStreamer estabelece o fluxo de dados pedido ao cliente. Durante períodos de inatividade, o eStreamer envia mensagens nulas periódicos ao cliente para manter a conexão aberta. Se recebe um Mensagem de Erro do cliente ou de um host intermediário, fecha a conexão.

Passo 4: A conexão termina

O server do eStreamer pode igualmente fechar uma conexão de cliente para as seguintes razões:

- Em qualquer altura que enviar uma mensagem conduz a um erro. Isto inclui mensagens de dados de evento e o eStreamer nulo da mensagem da manutenção de atividade envia durante períodos de inatividade.
- Um erro ocorre ao processar um pedido do cliente.
- A authenticação do cliente falha (nenhum Mensagem de Erro é enviado).
- o serviço do eStreamer está fechando (nenhum Mensagem de Erro é enviado).

O cliente não mostra nenhum evento

Se você não vê nenhuns eventos em seu aplicativo do cliente do eStreamer, siga por favor as etapas abaixo para pesquisar defeitos esta edição:

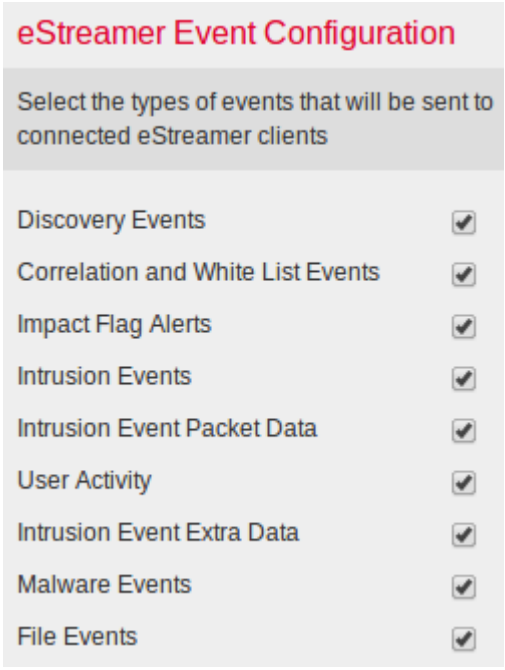
Passo 1: Verificar a configuração

Você pode controlar que os tipos de eventos o server do eStreamer podem transmitir aos aplicativos do cliente que os pedem. Para configurar os tipos de eventos transmitidos pelo eStreamer siga as etapas abaixo:

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

2. Clique a aba do **eStreamer**.

3. Sob o menu da **configuração de evento do eStreamer**, selecione as caixas de seleção ao lado dos tipos de eventos que você quer o eStreamer enviar a pedir clientes.



> Nota: Certifique-se que seu aplicativo do cliente pede os tipos de eventos que você os quer receber. O mensagem request tem que ser enviado ao server do eStreamer (centro de gerenciamento ou dispositivo gerenciado de FireSIGHT).

4. Clique em Salvar.

Passo 2: Verifique o certificado

Certifique-se de que os Certificados exigidos estão adicionados. Antes que o eStreamer possa enviar eventos do eStreamer a um cliente, o cliente deve ser adicionado ao base de dados dos pares do server do eStreamer usando a página de configuração do eStreamer. O certificado da autenticação gerado pelo server do eStreamer deve igualmente ser copiado ao cliente.

Passo 3: Verifique Mensagens de Erro

Identifique todos os erros relacionados óbvios do eStreamer em `/var/log/messages` usando o comando seguinte:

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

Passo 4: Verifique a conexão

Verifique que o server está aceitando conexões recebidas.

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

A saída deve olhar como abaixo. Se não, então o serviço não pode ser executado.

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

Passo 5: Verifique o estado do processo

Para verificar se há um processo do `sfestreamer que` é executado, use por favor o comando seguinte:

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

Eventos duplicados das mostras do cliente

Eventos duplicados do punho indicados em um cliente

O server do eStreamer não mantém uma história dos eventos que envie, assim que o aplicativo do cliente deve verificar para ver se há eventos duplicados. Os eventos duplicados podem ocorrer por vários motivos. Por exemplo, ao começar uma sessão de fluência nova, o momento especificado pelo cliente como o ponto de início para a sessão nova pode ter mensagens múltipla, alguns de que pode ter sido enviado na sessão precedente e alguns de que não eram. o eStreamer envia todas as mensagens que encontram os critérios especificados do pedido. Os aplicativos do cliente de EStreamer devem ser projetados detectar e de-duplicata todas as duplicatas resultantes.

Controle pedidos duplicados para dados

Se você pede versões múltiplas dos mesmos dados, por bandeiras múltiplas ou por pedidos prolongados múltiplos, a versão mais atualizada está usada. Por exemplo, se o eStreamer recebe pedidos da bandeira para a versão 1 e 6 dos eventos da descoberta e um pedido prolongado para a versão 3, envia a versão 6.

O cliente mostra a regra incorreta ID do Snort (SID)

Isto acontece geralmente devido a um conflito de SID quando uma regra é importada no sistema, SID re-é traçado internamente.

Para usar SID que você entrou, um pouco do que SID re-traçado, você tem que permitir *encabeçamento prolongado*. Mordido 23 cabeçalhos de evento prolongados dos pedidos. Se este campo é ajustado a 0, os eventos estão enviados com um cabeçalho de evento padrão que inclua somente o comprimento do tipo de registro e de registro.

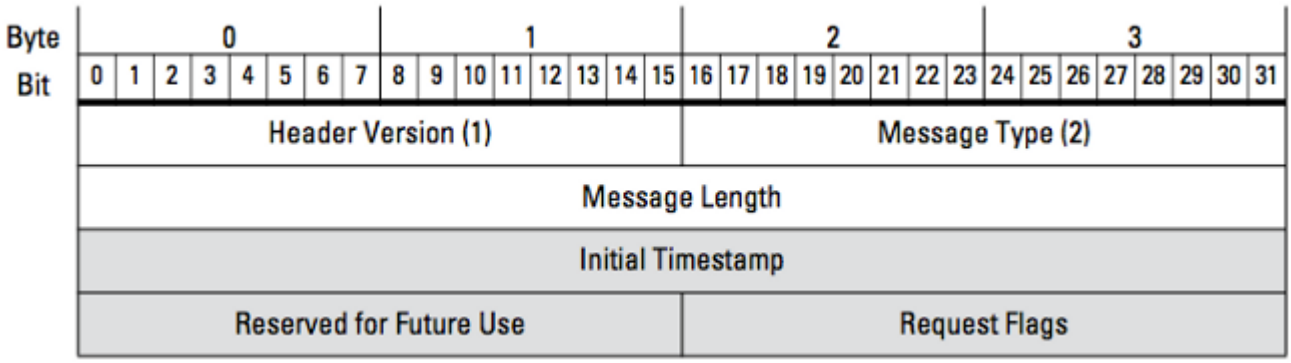


Figura: O diagrama ilustra o formato de mensagem usado para pedir dados do eStreamer. Os campos específicos ao formato do mensagem request são destacados no cinza.

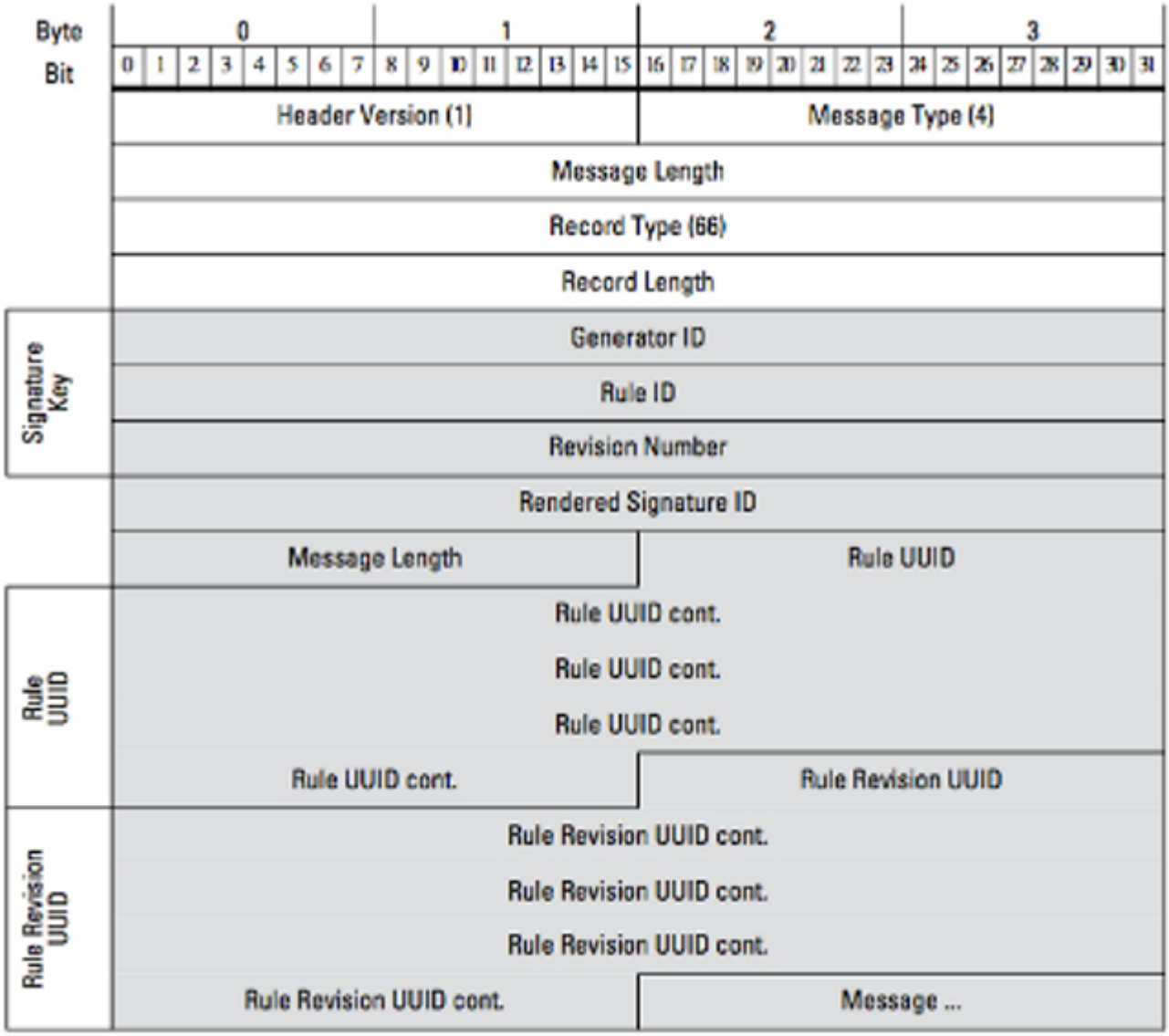


Figura: O diagrama ilustra o formato da informação de mensagem da regra para um evento que seja transmitido dentro de um registro da mensagem da regra. Mostra o ***RuleID*** *(qual você está usando agora) e o* ***ID de assinatura rendido*** *(qual é o número que você espera).*

Dica: A fim encontrar a descrição do detalhe de cada bit e mensagem, leia o *guia de integração do eStreamer*.

Recolha e analise adicional pesquisam defeitos dados

Teste usando o script ssl_test.pl

Utilize o `script ssl_test.pl` fornecido no *Software Development Kit de* EventStreamer *(SDK)* para identificar o problema. O SDK está disponível em um arquivo zip na site de suporte. As instruções para o script estão disponíveis em README.txt, `que` é incluído nesse arquivo zip.

Pacote da captação (PCAP)

Capture pacotes na interface de gerenciamento do server do eStreamer e analise-os. Verifique que o tráfego não está obstruído nem está negado em algum lugar em sua rede.

Gerencia pesquisam defeitos o arquivo

Se você terminou os passos de Troubleshooting acima, e você é ainda incapaz de determinar o problema, gerencia por favor um arquivo da pesquisa de defeitos de seu centro de gerenciamento de FireSIGHT. Forneça todo o adicional pesquisam defeitos dados ao Suporte técnico de Cisco para a análise mais aprofundada.