Solucionar problemas entre o FireSIGHT System e o eStreamer Client (SIEM)

Contents

Introduction

O Event Streamer (eStreamer) permite transmitir vários tipos de dados de eventos de um FireSIGHT System para um aplicativo cliente desenvolvido de forma personalizada. Depois de criar um aplicativo cliente, você pode conectá-lo a um servidor eStreamer (por exemplo, um FireSIGHT Management Center), iniciar o serviço eStreamer e começar a trocar dados. A integração do eStreamer requer programação personalizada, mas permite que você solicite dados específicos de um dispositivo. Este documento descreve como um cliente eStreamer se comunica e como solucionar um problema com um cliente.

Método de Comunicação entre Cliente e Servidor eStreamer

Há quatro estágios principais de comunicação que ocorrem entre um cliente e o serviço eStreamer:

Passo 1: O cliente estabelece uma conexão com o servidor eStreamer

Primeiro, um cliente estabelece uma conexão com o servidor eStreamer e a conexão é autenticada por ambas as partes. Para que um cliente possa solicitar dados do eStreamer, ele deve iniciar uma conexão TCP habilitada para SSL com o serviço eStreamer. Quando o cliente inicia a conexão, o servidor eStreamer responde, iniciando um handshake SSL com o cliente. Como parte do handshake SSL, o servidor eStreamer solicita o certificado de autenticação do cliente e verifica se o certificado é válido.

Depois que a sessão SSL é estabelecida, o servidor eStreamer executa uma verificação adicional pós-conexão do certificado. Após a conclusão da verificação pós-conexão, o servidor eStreamer aguarda uma solicitação de dados do cliente.

Passo 2: O Cliente Solicita Dados do Serviço eStreamer

Nesta etapa, o cliente solicita dados do serviço eStreamer e especifica os tipos de dados a serem transmitidos. Uma única mensagem de solicitação de evento pode especificar qualquer combinação de dados de evento disponíveis, incluindo metadados de evento. Uma única solicitação de perfil de host pode especificar um único host ou vários hosts. Dois modos de solicitação estão disponíveis para solicitar dados de evento e dois-pontos;

- **Solicitação de fluxo de eventos:** O cliente envia uma mensagem contendo sinalizadores de solicitação que especificam os tipos de evento e a versão solicitados de cada tipo, e o servidor eStreamer responde transmitindo os dados solicitados.
- **Solicitação estendida:** O cliente envia uma solicitação com o mesmo formato de mensagem das solicitações de Fluxo de Eventos, mas define um sinalizador para uma solicitação estendida. Isso inicia uma interação de mensagem entre o cliente e o servidor eStreamer por meio da qual o cliente solicita informações adicionais e combinações de versão não disponíveis por meio de solicitações de Fluxo de Eventos.

Passo 3: O eStreamer estabelece o fluxo de dados solicitado

Nesse estágio, o eStreamer estabelece o fluxo de dados solicitado para o cliente. Durante os períodos de inatividade, o eStreamer envia mensagens nulas periódicas ao cliente para manter a conexão aberta. Se ele receber uma mensagem de erro do cliente ou de um host intermediário, fechará a conexão.

Passo 4: A conexão é encerrada

O servidor eStreamer também pode fechar uma conexão de cliente pelos seguintes motivos:

- Sempre que uma mensagem for enviada, ocorrerá um erro. Isso inclui mensagens de dados de eventos e mensagens de keep-alive nulas que o eStreamer envia durante períodos de inatividade.
- Erro ao processar uma solicitação de cliente.
- Falha na autenticação do cliente (nenhuma mensagem de erro é enviada).
- O serviço eStreamer está sendo desligado (nenhuma mensagem de erro é enviada).

O cliente não mostra nenhum evento

Se você não vir nenhum evento no aplicativo cliente do eStreamer, siga as etapas abaixo para solucionar esse problema:

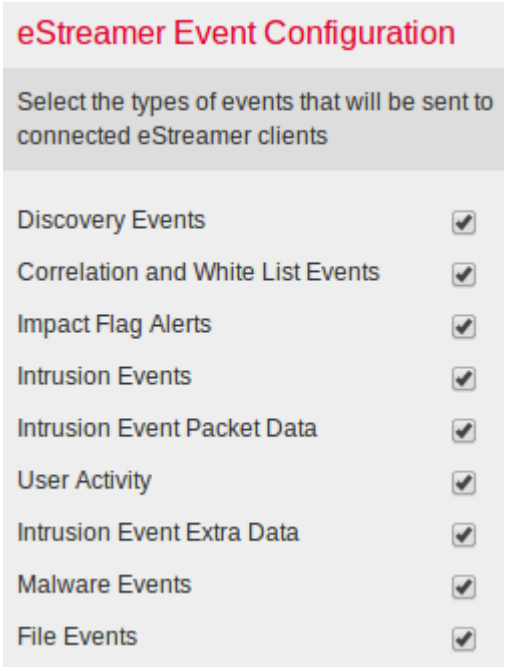
Passo 1: Verificar a configuração

Você pode controlar que tipos de eventos o servidor eStreamer pode transmitir para aplicativos clientes que os solicitam. Para configurar os tipos de eventos transmitidos pelo eStreamer, siga estas etapas:

1. Navegue até **Sistema > Local > Registro**.

2. Clique na guia **eStreamer**.

3. No menu **eStreamer Event Configuration**, marque as caixas de seleção ao lado dos tipos de eventos que você deseja que o eStreamer envie aos clientes solicitantes.



> **Note**: Verifique se o aplicativo cliente solicita os tipos de eventos que você deseja que ele receba. A mensagem de solicitação deve ser enviada ao servidor eStreamer (FireSIGHT Management Center ou dispositivo gerenciado).

4. Clique em **Salvar**.

Passo 2: Verificar o certificado

Verifique se os certificados necessários foram adicionados. Para que o eStreamer possa enviar eventos do eStreamer a um cliente, ele deve ser adicionado ao banco de dados de pares do servidor do eStreamer usando a página de configuração do eStreamer. O certificado de autenticação gerado pelo servidor eStreamer também deve ser copiado para o cliente.

Passo 3: Verifique as mensagens de erro

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

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

Passo 4: Verificar a conexão

Verifique se o servidor está aceitando conexões de entrada.

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

A saída deve ser semelhante à mostrada abaixo. Caso contrário, o serviço pode não estar em execução.

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

Passo 5: Verificar o Status do Processo

Para verificar se há um processo sfestreamer em execução, use o seguinte comando:

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

O cliente mostra eventos duplicados

Manipular eventos duplicados exibidos em um cliente

O servidor eStreamer não mantém um histórico dos eventos que envia, portanto, o aplicativo cliente deve verificar se há eventos duplicados. Eventos duplicados podem ocorrer por vários motivos. Por exemplo, ao iniciar uma nova sessão de streaming, o tempo especificado pelo cliente como ponto de partida para a nova sessão pode ter várias mensagens, algumas das quais podem ter sido enviadas na sessão anterior e outras não. O eStreamer envia todas as mensagens que atendem aos critérios de solicitação especificados. Os aplicativos clientes EStreamer devem ser projetados para detectar e eliminar a duplicação de qualquer duplicata resultante.

Gerenciar Solicitações Duplicadas para Dados

Se você solicitar várias versões dos mesmos dados, seja por vários sinalizadores ou várias solicitações estendidas, a versão mais alta será usada. Por exemplo, se o eStreamer receber solicitações de flag para eventos de descoberta versão 1 e 6 e uma solicitação estendida para a versão 3, ele enviará a versão 6.

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

Isso geralmente acontece devido a um conflito de SID quando uma regra é importada para o sistema, o SID é remapeado internamente.

Para usar o SID que você inseriu, em vez do SID remapeado, é necessário habilitar o *cabeçalho estendido*. O bit 23 solicita cabeçalhos de eventos estendidos. Se esse campo for definido como 0, os eventos serão enviados com um cabeçalho de evento padrão que inclui apenas o tipo e o tamanho do registro.

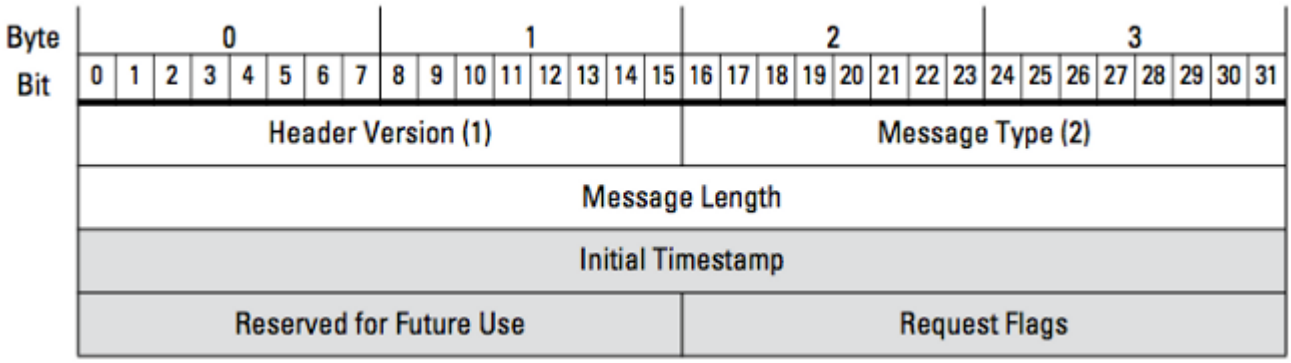


Figura: O diagrama ilustra o formato de mensagem usado para solicitar dados do eStreamer. Os campos específicos do formato da mensagem de solicitação são destacados em cinza.

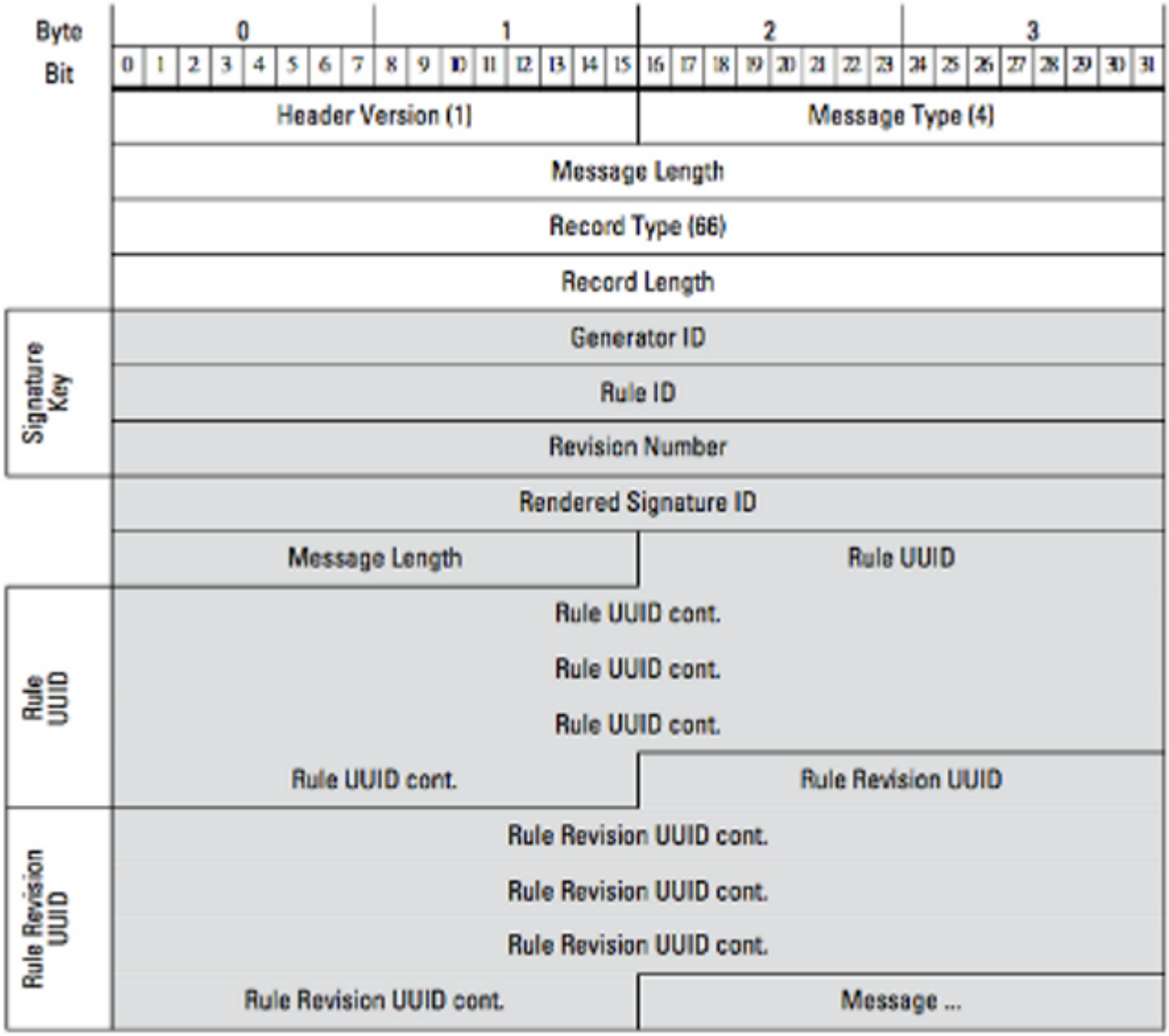


Figura: O diagrama ilustra o formato das informações da mensagem de regra para um evento transmitido em um registro da mensagem de regra. Ela mostra a **RuleID** *(que você está usando agora) e a* **ID de assinatura renderizada** *(que é o número esperado).*

Tip: Para encontrar a descrição detalhada de cada bit e mensagem, leia o *eStreamer Integration Guide*.

Coletar e analisar dados adicionais de solução de problemas

Testar usando o script ssl_test.pl

Utilize o script ssl_test.pl fornecido no *Kit de Desenvolvimento de Software (SDK)* do Event Streamer para identificar o problema. O SDK está disponível em um arquivo zip no site de suporte. As instruções para o script estão disponíveis no README.txt, incluído nesse arquivo zip.

Pacote de captura (PCAP)

Capture pacotes na interface de gerenciamento do servidor eStreamer e analise-os. Verifique se o tráfego não está bloqueado ou negado em algum lugar da rede.

Gerar Arquivo de Solução de Problemas

Se você concluiu as etapas de solução de problemas acima e ainda não consegue determinar o problema, gere um arquivo de solução de problemas a partir do FireSIGHT Management Center. Forneça todos os dados adicionais de solução de problemas ao Suporte Técnico da Cisco para análise adicional.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.