排除故障在FireSIGHT系统和eStreamer客户端(SIEM)之间的问题

目录

简介

事件飘带(eStreamer)允许您放出几从FireSIGHT系统的事件数据到按客户需要开发的客户端应用。在您创建客户端应用后，您能连接它到eStreamer服务器(例如， FireSIGHT管理中心)，开始eStreamer服务，并且开始交换数据。eStreamer集成要求自定义编程，但是允许您请求从设备的特定数据。本文描述eStreamer客户端如何通信和如何排除故障与客户端的问题。

在eStreamer客户端和服务器之间的通信方法

有发生在客户端和eStreamer服务之间通信的四个主要阶段：

步骤 1：客户端建立连接用eStreamer服务器

首先，客户端建立连接用eStreamer服务器，并且连接由两个当事人验证。在客户端能要求从eStreamer前的数据，客户端必须首次与eStreamer服务的已启用SSL TCP连接。当客户端首次连接时， eStreamer服务器回应，启动与客户端的SSL握手。作为SSL握手一部分， eStreamer服务器请求客户端身份验证证书，并且验证证书有效。

在SSL会话建立后， eStreamer服务器进行证书的另外的连接后验证。在连接后验证完成后，eStreamer服务器等候从客户端的数据请求。

步骤 2：客户端要求从eStreamer服务的数据

在此步骤，从eStreamer的客户端的要求数据服务并且指定将被放出的数据种类。Request信息单个的事件能指定可用的事件数据的所有组合，包括事件元数据。单个主机配置文件请求能指定单个主机或多台主机。两个请求模式为请求事件data&colon是可用的;

- **事件数据流请求**：客户端提交包含指定每个类型请求的事件类型和版本的请求标志的消息，并且eStreamer服务器通过放出请求的数据回应。
- **延长的请求**：客户端提交与消息格式的请求和一样事件数据流请求的，但是树立延长的请求的标志。这启动客户端的要求其他信息和版本组合不可用通过事件数据流请求的客户端和eStreamer服务器之间的消息交互作用。

步骤 3：eStreamer设立请求的数据流

在此阶段， eStreamer设立请求的数据流给客户端。在休止时期， eStreamer传送定期空消息给客户端保持连接开放。如果它收到从客户端或中间主机的错误消息，断开连接。

步骤 4：连接终止

eStreamer服务器能也断开以下原因的客户端连接：

- 在发送消息导致错误时候。这包括两个事件数据数据信息在休止时期，并且空keep-alive消息eStreamer发送。
- 错误出现，当处理客户端的要求时。
- 客户端验证发生故障(错误消息没有传送)。
- eStreamer服务关闭(错误消息没有传送)。

客户端不显示事件

如果看不到在您的eStreamer客户端应用的任何事件，请遵从下面步骤排除故障此问题：

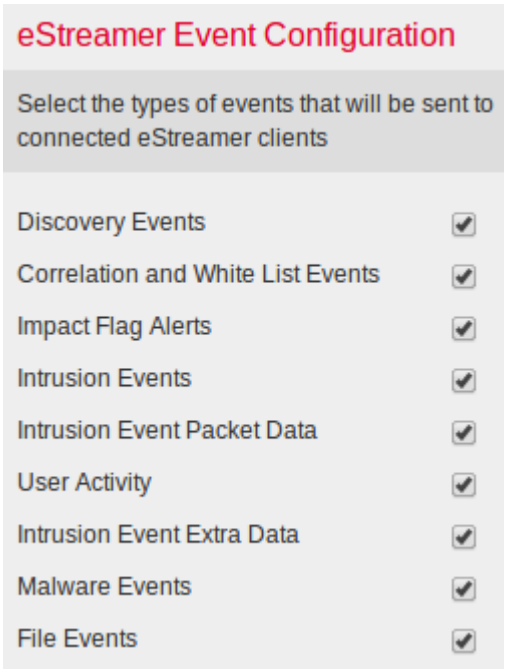
步骤 1：检查配置

事件的类型eStreamer服务器能传达给客户端应用请求他们的您能控制。要配置eStreamer传送的事件种类请遵从下面步骤：

1. 导航对**系统>本地>注册**。

2. 点击**eStreamer**选项卡。

3. 在**eStreamer事件配置**菜单下，请在您希望eStreamer发送到请求客户端事件旁边的种类选择复选框。



> **注意**：确保您的客户端应用请求您希望它接收事件的种类。Request信息必须发送到eStreamer服务器(FireSIGHT管理中心或受管理设备)。

4. 单击 **Save**。

步骤 2：验证证书

确保需要的证书被添加。在eStreamer能发送eStreamer事件对客户端前，使用eStreamer配置页，客户端必须被添加到eStreamer服务器的对等体数据库。必须也复制由eStreamer服务器的验证生成的证书对客户端。

步骤 3：检查错误消息

通过使用以下命令，识别在/var/log/messages所有明显的eStreamer相关错误：

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

步骤 4：验证连接

验证服务器接受流入连接。

```
admin@FireSIGHT:~$netstat -an | grep 8302
```
输出应该看似类似下面。否则，服务可能不然后运作。

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

步骤 5：检查进程的状况

要验证，如果有运行sfestreamer进程，请使用以下命令：

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

客户端显示重复的事件

在客户端显示的把柄重复的事件

eStreamer服务器不保持发送事件的历史记录，因此客户端应用必须检查重复的事件。重复的事件能由于各种各样的原因发生。 例如，当开始新的流会话，客户端指定的时期作为起点的个新会话能有多个消息时，一些在上次会话和一些可能发送不是。eStreamer传送满足指定的请求标准的所有信息。应该设计EStreamer客户端应用检测和DE重复项所有发生的重复项。

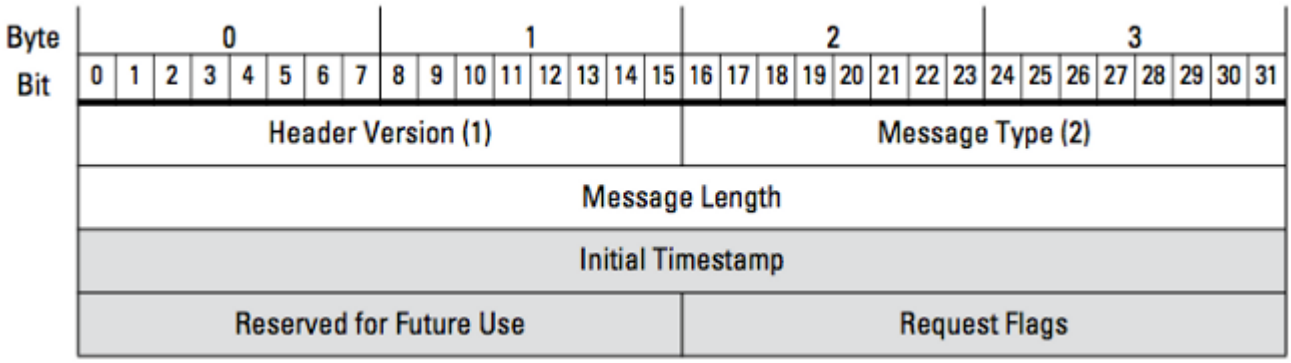
管理重复的要求数据

如果由多标志或多个扩展的请求请求同一个数据的多个版本，使用高版本。例如，如果eStreamer接收标志要求发现事件版本1和6和延长的要求版本3，它发送版本6。

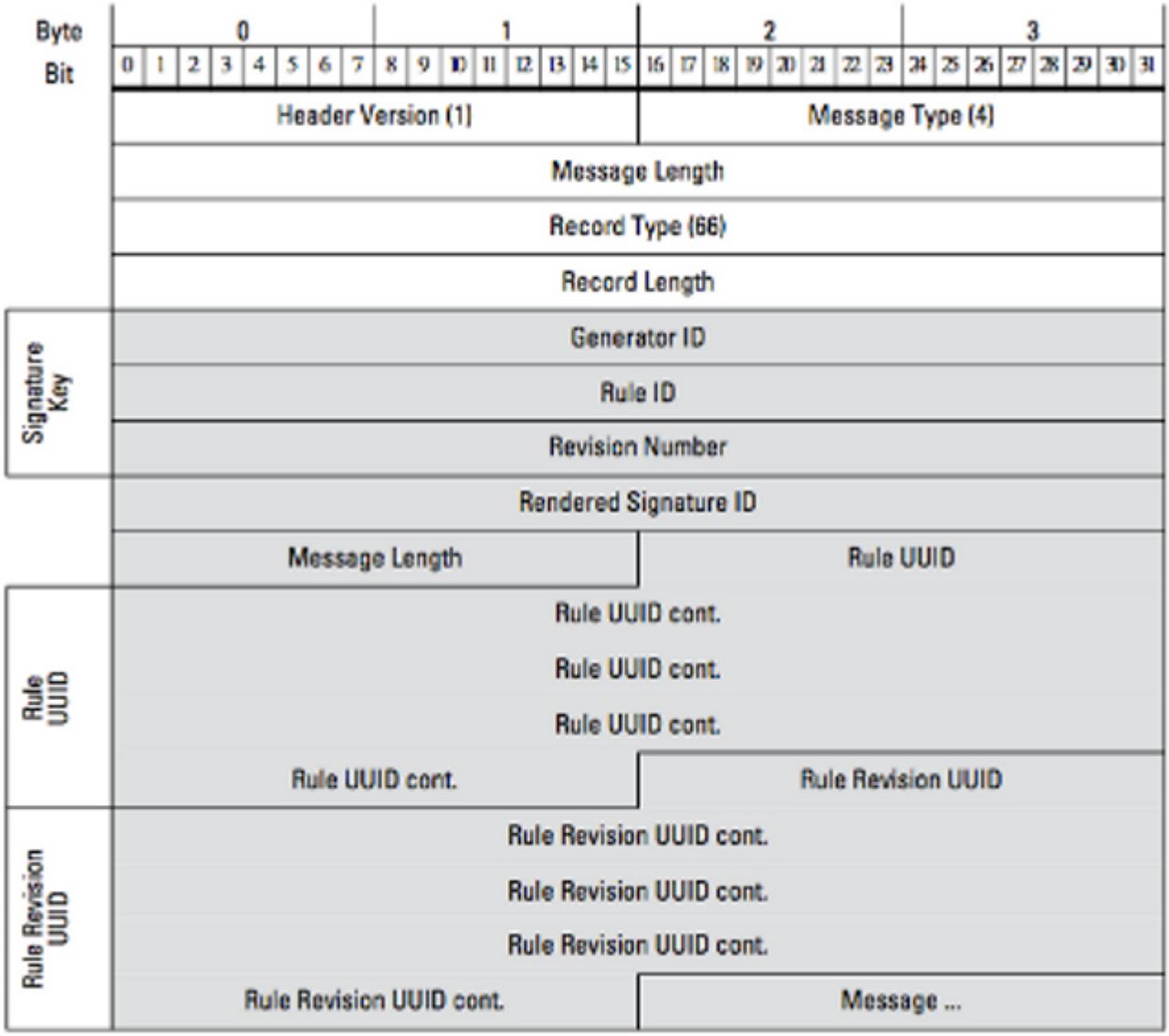
客户端显示不正确喷鼻息规则ID (SID)

这通常发生由于SID冲突，当规则导入到系统时， SID被重新映射得内部地。

使用您输入的SID，而不是被重新映射的SID，您必须启用*延长的报头*。位23请求延长的事件报头。如果此字段设置到0，事件用只包括记录类型和记录长度的标准事件报头传送。



图：图表说明用于的消息格式请求从eStreamer的数据。字段特定对Request信息格式用灰色突出显示。



*图：图表说明规则留言信息格式在规则消息记录内传送的事件的。它显示**RuleID** (哪些您当前使用)和**被回报的签名ID** (哪些是您预计)的编号。*

提示：为了查找每个位和消息的详细信息说明，请读*eStreamer集成指南*。

收集并且分析其他排除故障数据

测验使用ssl_test.pl脚本

使用在EventStreamer*软件开发工具(SDK)*提供的`ssl_test.pl`识别问题。SDK是可用的在支持站点的压缩文件。脚本的说明是可用的在README.txt在该压缩文件包括。

捕获数据包(PCAP)

获取在eStreamer服务器的管理接口的数据包并且分析它。验证流量在您的网络没有阻塞也没有拒绝某处。

生成排除故障文件

如果完成上述故障排除步骤，并且无法确定问题，请生成从您的FireSIGHT管理中心的排除故障文件。提供所有其他排除故障数据对进一步分析的思科技术支持。