排除FireSIGHT系统和eStreamer客户端(SIEM)之间的问题

目录

简介

通过Event Streamer(eStreamer)，您可以将多种事件数据从FireSIGHT系统流式传输到自定义开发的客户端应用程序。创建客户端应用程序后，可以将其连接到eStreamer服务器（例如，FireSIGHT管理中心），启动eStreamer服务，并开始交换数据。eStreamer集成需要自定义编程，但允许您从设备请求特定数据。本文档介绍eStreamer客户端如何通信以及如何对客户端问题进行故障排除。

eStreamer客户端与服务器之间的通信方法

客户端和eStreamer服务之间的通信分为四个主要阶段：

步骤 1：客户端与eStreamer服务器建立连接

首先，客户端与eStreamer服务器建立连接，并且连接由双方进行身份验证。在客户端可以从eStreamer请求数据之前，客户端必须启动与eStreamer服务之间的启用SSL的TCP连接。当客户端发起连接时，eStreamer服务器会响应，发起与客户端的SSL握手。作为SSL握手的一部分，eStreamer服务器请求客户端的身份验证证书，并验证证书是否有效。

建立SSL会话后，eStreamer服务器会对证书执行额外的连接后验证。连接后验证完成后，eStreamer服务器等待来自客户端的数据请求。

步骤 2：客户端从eStreamer服务请求数据

在此步骤中，客户端向eStreamer服务请求数据并指定要进行数据流传输的数据类型。单个事件请求消息可以指定可用事件数据的任意组合，包括事件元数据。单个主机配置文件请求可以指定单个主机或多个主机。有两种请求模式可用于请求事件数据和冒号；

- **事件流请求**：客户端提交包含指定请求的事件类型和每个类型的版本的请求标志的消息，eStreamer服务器通过流式传输请求的数据进行响应。
- **扩展请求**：客户端提交的请求消息格式与事件流请求的消息格式相同，但会为扩展请求设置标志。这将启动客户端和eStreamer服务器之间的消息交互，客户端通过该消息交互请求无法通过事件流请求获得其他信息和版本组合。

步骤 3：eStreamer建立请求的数据流

在此阶段，eStreamer将请求的数据流建立到客户端。在非活动期间，eStreamer定期向客户端发送空消息，以保持连接打开。如果收到来自客户端或中间主机的错误消息，则它会关闭连接。

步骤 4：连接终止

eStreamer服务器也可以关闭客户端连接，原因如下：

- 任何时候发送消息都会导致错误。这包括事件数据消息和eStreamer在非活动期间发送的空保活消息。
- 处理客户端请求时出错。
- 客户端身份验证失败（未发送错误消息）。
- eStreamer服务正在关闭（未发送错误消息）。

客户端未显示事件

如果您在eStreamer客户端应用上未看到任何事件，请按照以下步骤解决此问题：

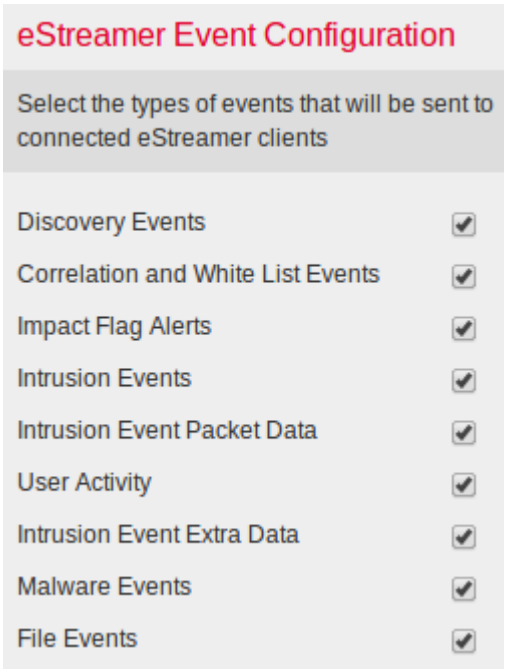
步骤 1：检查配置

您可以控制eStreamer服务器能够向请求事件的客户端应用程序传输哪些类型的事件。要配置eStreamer传输的事件类型，请执行以下步骤：

1.定位至**系统>本地>注册**。

2.单击**eStreamer**选项卡。

3.在**eStreamer Event Configuration**菜单下，选中希望eStreamer发送到请求客户端的事件类型旁边的复选框。



> **注意**：确保您的客户端应用程序请求您希望其接收的事件类型。请求消息必须发送到eStreamer服务器（FireSIGHT管理中心或受管设备）。

4.单击**保存**。

步骤 2：验证证书

确保已添加所需的证书。在将eStreamer事件发送到客户端之前，必须使用eStreamer配置页面将客户端添加到eStreamer服务器的对等体数据库。eStreamer服务器生成的身份验证证书也必须复制到客户端。

步骤 3：检查错误消息

使用以下命令识别/var/log/messages中与eStreamer相关的任何明显错误：

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

步骤 4：验证连接

验证服务器是否接受传入连接。

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

输出应如下所示。否则，服务可能未运行。

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

步骤 5：检查进程的状态

要验证是否正在运行sfestreamer进程，请使用以下命令：

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

客户端显示重复事件

处理客户端中显示的重复事件

eStreamer服务器不保留其发送的事件的历史记录，因此客户端应用程序必须检查重复的事件。由于各种原因，可能会发生重复事件。 例如，启动新的流会话时，客户端指定为新会话起点的时间可以包含多条消息，其中有些消息可能已在前一会话中发送，有些则没有。eStreamer发送符合指定请求条件的所有消息。EStreamer客户端应用程序应能检测并消除任何产生的重复数据。

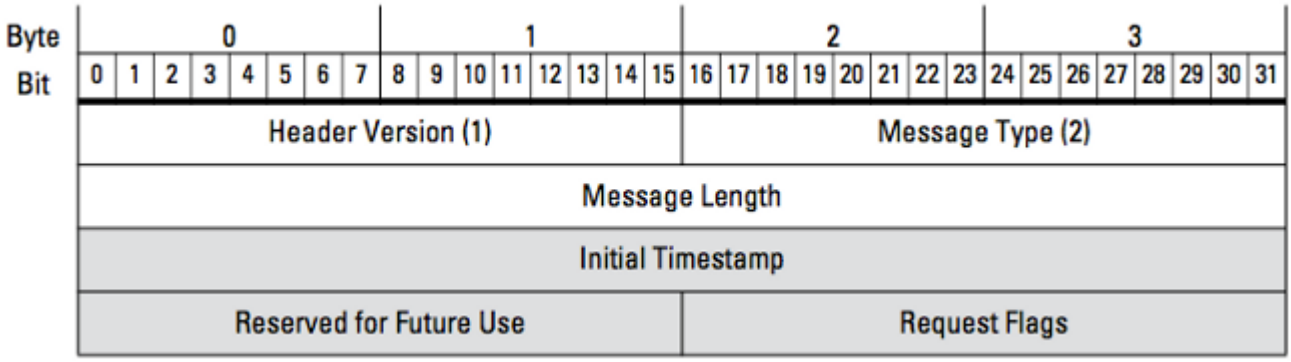
管理重复的数据请求

如果通过多个标志或多个扩展请求请求同一数据的多个版本，则使用最高版本。例如，如果eStreamer收到发现事件版本1和版本6的标记请求以及发现事件版本3的扩展请求，它将发送版本6。

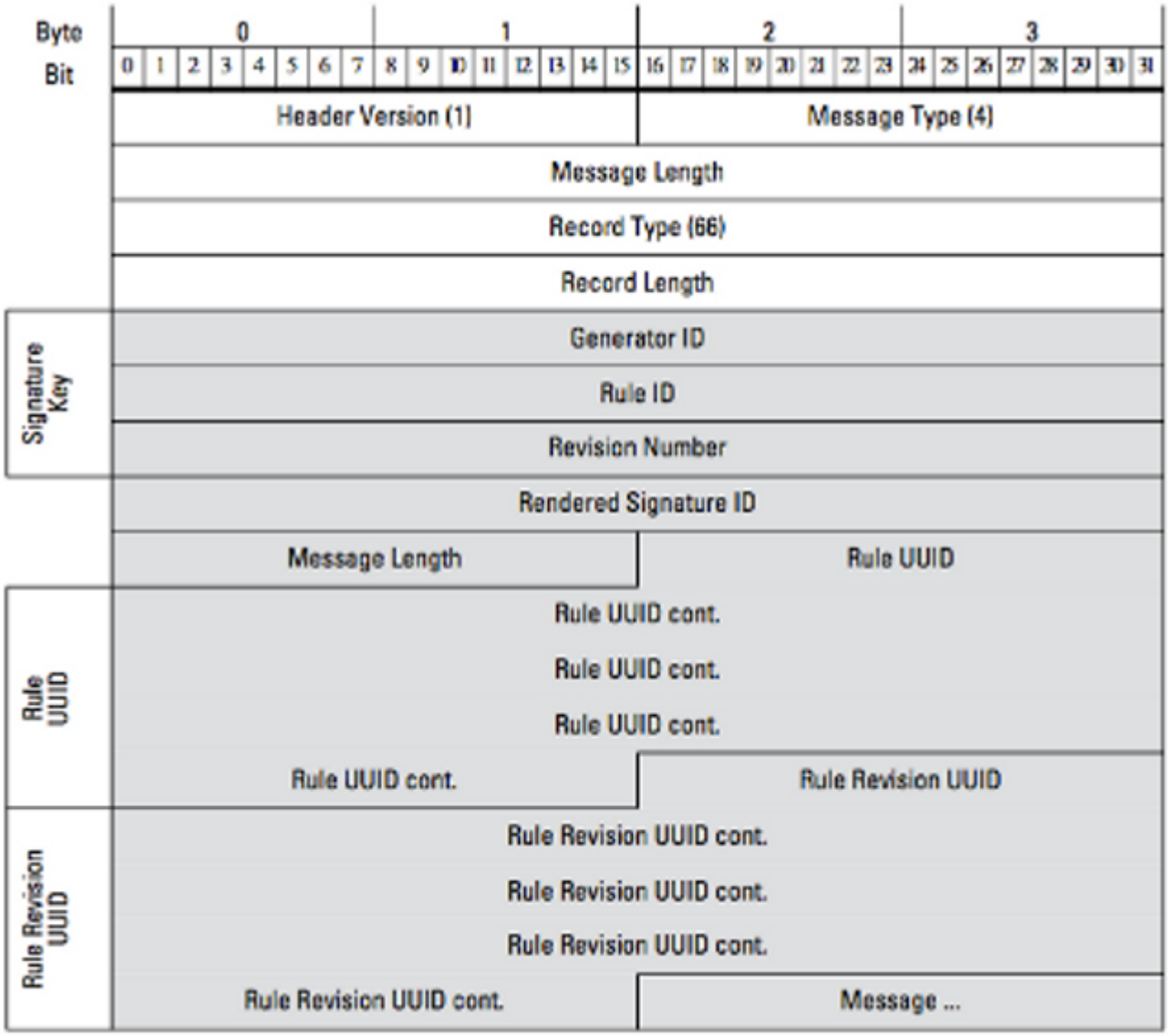
客户端显示不正确的Snort规则ID(SID)

当规则导入系统时，SID在内部重新映射，这通常是由于SID冲突造成的。

要使用您输入的SID而不是重新映射的SID，您必须启用扩*展报*头。位23请求扩展事件报头。如果此字段设置为0，则发送事件的标准事件报头仅包括记录类型和记录长度。



图：下图说明了用于从eStreamer请求数据的消息格式。特定于请求消息格式的字段以灰色突出显示。



*图：该图说明了在规则消息记录中传输的事件的规则消息信息的格式。它显示**RuleID**（您现在正在使用）和**Rendered Signature ID**（您预期的数字）。*

提示：要查找每个位和消息的详细说明，请参阅*eStreamer集成指南*。

收集和分析其他故障排除数据

使用ssl_test.pl脚本进行测试

使用*Event Streamer Software Development Kit*(*SDK*)中提供*的*ssl_*test.pl脚本来*识别问题。SDK可在支持站点的zip文件中找到。README.txt中提供了该脚本的说明，该zip文件包含在该文件中。

捕获数据包(PCAP)

在eStreamer服务器的管理接口上捕获数据包并对其进行分析。验证流量在您的网络中的某处未被阻止或拒绝。

生成故障排除文件

如果您已完成上述故障排除步骤，但仍无法确定问题，请从FireSIGHT管理中心生成故障排除文件。向Cisco技术支持提供所有其它故障排除数据以供进一步分析。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。