疑難排解FireSIGHT系統和eStreamer Client(SIEM)之間的問題

目錄

簡介

Event Streamer(eStreamer)允許您將多種事件資料從FireSIGHT系統流式傳輸到自定義開發的客戶端應用程式。建立客戶端應用程式後，可以將其連線到eStreamer伺服器（例如，FireSIGHT管理中心），啟動eStreamer服務，並開始交換資料。eStreamer整合需要自定義程式設計，但允許您從裝置請求特定資料。本文檔介紹eStreamer客戶端如何通訊以及如何對客戶端問題進行故障排除。

一種電子流處理器客戶端與伺服器的通訊方法

客戶端和eStreamer服務之間的通訊分為四個主要階段：

第1步：客戶端與eStreamer伺服器建立連線

首先，客戶端與eStreamer伺服器建立連線，並且連線由雙方進行身份驗證。在客戶端可以從eStreamer請求資料之前，客戶端必須通過eStreamer服務啟動啟用SSL的TCP連線。當客戶端發起連線時，eStreamer伺服器會響應，與客戶端發起SSL握手。作為SSL握手的一部分，eStreamer伺服器請求客戶端的身份驗證證書，並驗證證書是否有效。

在SSL會話建立後，eStreamer伺服器會對該證書執行額外的連線後驗證。連線後驗證完成後，eStreamer伺服器等待來自客戶端的資料請求。

第2步：客戶端從eStreamer服務請求資料

在此步驟中，客戶端從eStreamer服務請求資料並指定要流傳輸的資料型別。單個事件請求消息可以指定可用事件資料（包括事件後設資料）的任意組合。單個主機配置檔案請求可以指定單個主機或多個主機。有兩種請求模式可用於請求事件資料和冒號；

- **事件流請求**：客戶端提交包含請求標誌的消息，請求標誌指定請求的事件型別和每種型別的版本，eStreamer伺服器通過流式傳輸請求的資料進行響應。
- **擴展請求**：客戶端提交的請求消息格式與事件流請求的消息格式相同，但為擴展請求設定標誌。這啟動客戶端和eStreamer伺服器之間的消息互動，客戶端通過此互動請求其它資訊和版本組合，而事件流請求無法提供這些資訊和版本組合。

步驟3:eStreamer建立請求的資料流

在此階段，eStreamer將請求的資料流建立到客戶端。在非活動期間，eStreamer會定期向客戶端傳送空消息，以保持連線處於開啟狀態。如果收到來自客戶端或中間主機的錯誤消息，將關閉連線。

第4步：連線終止

eStreamer伺服器也可以關閉客戶端連線，原因如下：

- 任何時候傳送消息都會導致錯誤。這包括事件資料消息和eStreamer在非活動期間傳送的空保持連線消息。
- 處理客戶端請求時出錯。
- 客戶端身份驗證失敗（未傳送錯誤消息）。
- eStreamer服務正在關閉（未傳送錯誤消息）。

客戶端未顯示事件

如果您在eStreamer客戶端應用程式中看不到任何事件，請按照以下步驟解決此問題：

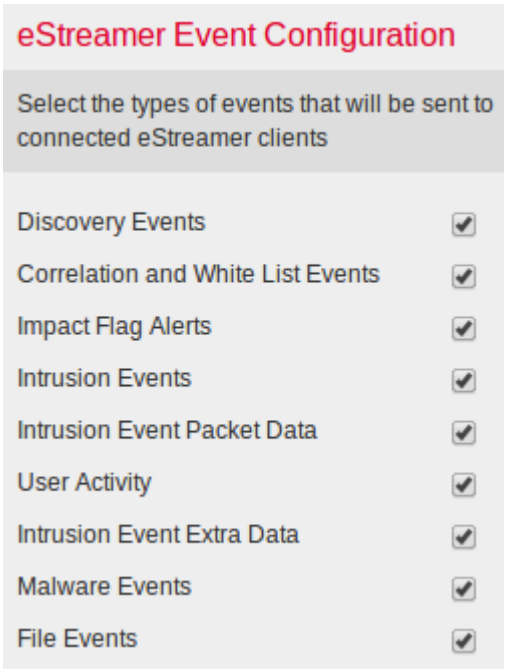
第1步：驗證設定

您可以控制eStreamer伺服器能夠向請求事件的客戶端應用程式傳輸哪些型別的事件。要配置eStreamer傳輸的事件型別，請執行以下步驟：

1.定位至**系統>本地>註冊**。

2.按一下**eStreamer選**項卡。

3.在**eStreamer Event Configuration**選單下，選中希望eStreamer傳送到請求客戶端的事件型別旁邊的覈取方塊。



> **附註**：確保您的客戶端應用程式請求您希望其接收的事件型別。請求消息必須傳送到eStreamer伺服器（FireSIGHT管理中心或受管裝置）。

4.按一下**儲存**。

第2步：驗證憑證

確保新增了所需的證書。在eStreamer可以將eStreamer事件傳送到客戶端之前，必須使用eStreamer配置頁將客戶端新增到eStreamer伺服器的對等資料庫。eStreamer伺服器生成的身份驗證證書也必須複製到客戶端。

步驟3:檢查錯誤消息

使用以下命令識別/var/log/messages中與eStreamer相關的任何明顯錯誤：

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

第4步：驗證連線

驗證伺服器是否接受傳入連線。

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

輸出應如下所示。如果不是，則服務可能未運行。

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

第5步：檢查流程狀態

要驗證是否正在運行ServiceStreamer進程，請使用以下命令：

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

客戶端顯示重複事件

處理客戶端中顯示的重複事件

eStreamer伺服器不保留其傳送的事件的歷史記錄，因此客戶端應用程式必須檢查重複的事件。由於各種原因，可能會發生重複的事件。 例如，啟動新的流會話時，客戶端指定為新會話起點的時間可以包含多個消息，其中一些消息可能已在上一個會話中傳送，而另一些則沒有。eStreamer傳送符合指定請求條件的所有消息。EStreamer客戶端應用程式應設計為可檢測和消除任何產生的重複項。

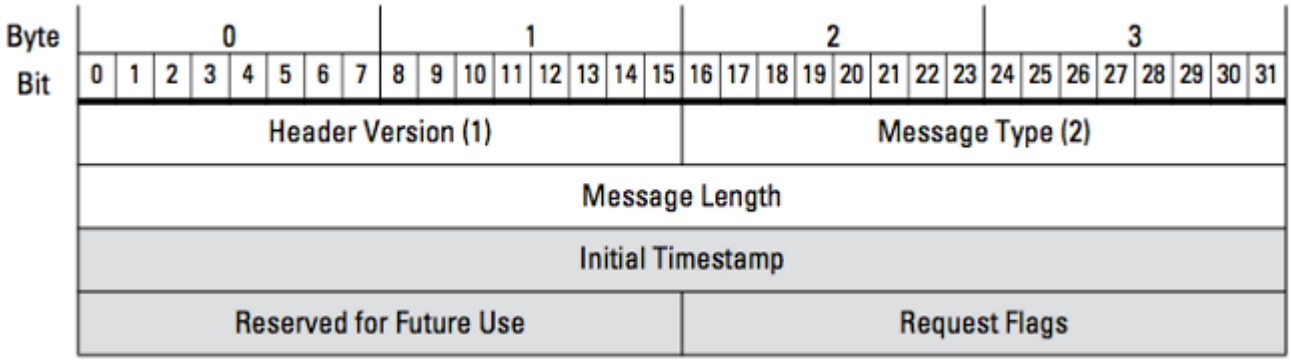
管理重複的資料請求

如果通過多個標誌或多個擴展請求請求同一資料的多個版本，則使用最高版本。例如，如果eStreamer收到發現事件版本1和版本6的標籤請求和版本3的擴展請求，它將傳送版本6。

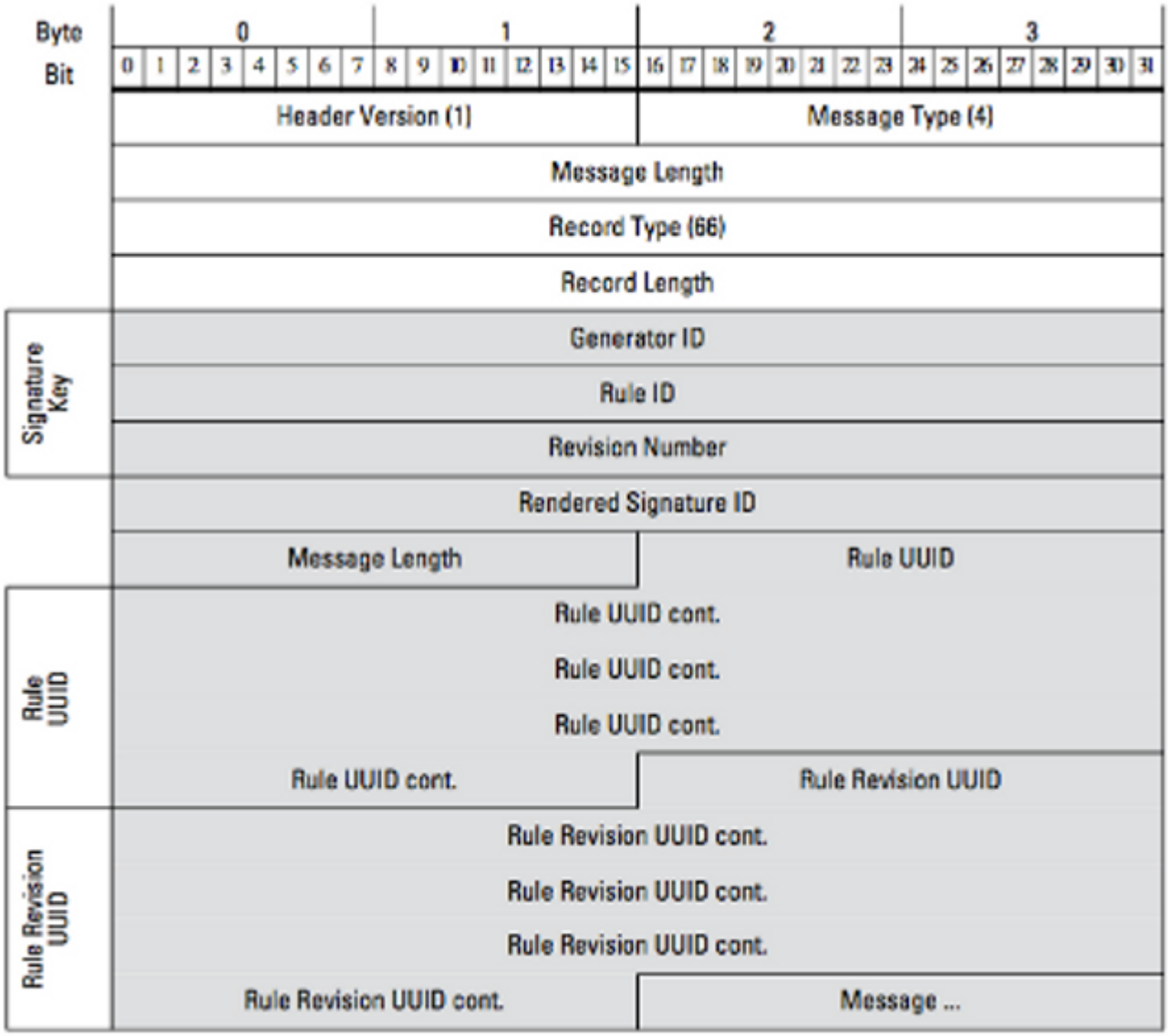
客戶端顯示錯誤的Snort規則ID(SID)

這通常是由於將規則匯入系統時發生SID衝突，SID會在內部重新對映。

要使用您輸入的SID而不是重新對映的SID，您必須啟用擴展*報頭*。第23位請求擴展事件報頭。如果此欄位設定為0，則傳送事件的標準事件報頭僅包括記錄型別和記錄長度。



圖：該圖說明了用於從eStreamer請求資料的消息格式。特定於請求消息格式的欄位以灰色突出顯示。



*圖：該圖說明了在規則消息記錄中傳輸的事件的規則消息資訊的格式。它顯示**RuleID**（您現在正在使用）和**Rendered Signature ID**（您預期的數字）。*

提示：若要尋找每個位元和訊息的詳細說明，請參閱*eStreamer Integration Guide*。

收集和分析其他故障排除資料

使用ssl_test.pl指令碼進行測試

使用*Event Streamer Software Development Kit*(*SDK*)中提供的ssl_*test.pl指令碼來*確定問題。SDK可在支援站點上的zip檔案中找到。README.txt中提供了該指令碼的說明，該zip檔案包含此檔案。

擷取封包(PCAP)

在eStreamer伺服器的管理介面上捕獲資料包並對其進行分析。確認流量沒有在網路中的任何位置被阻止或遭到拒絕。

生成故障排除檔案

如果您完成了上述故障排除步驟，但仍然無法確定問題，請從FireSIGHT管理中心生成一個故障排除檔案。將所有其他故障排除資料提供給思科技術支援以進行進一步分析。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。