目次

概要

イベント吹流し（ eStreamer ）は FireSIGHT システムからのカスタム開発されたクライアントアプリケーションに複数の種類のイベントデータを流すことを可能にします。 クライアントアプリケーションを作成した後、eStreamer サーバに（ たとえば、FireSIGHT Management Center ）それを接続でき、eStreamer サービスを開始し、データ交換を始めます。 eStreamer 統合はカスタム プログラミングを必要としますが、アプライアンスからの特定のデータを要求することを可能にします。 eStreamer クライアントがおよびクライアントで問題を解決する方法をどのように通信するかこの資料に記述されています。

eStreamer クライアント および サーバ間の通信方法

クライアントと eStreamer サービスの間に発生する通信の 4 つの主要なステージがあります:

ステップ 1： クライアントは eStreamer サーバの接続を確立します

最初に、クライアントは eStreamer サーバの接続を確立し、接続は両方のパーティによって認証されます。 クライアントが eStreamer からのデータを要求できる前にクライアントは eStreamer サービスの SSL 有効に された TCP 接続を開始する必要があります。 クライアントが接続を開始するとき、eStreamer サーバは応答しま、クライアントが付いている SSL ハンドシェイクを始めます。 SSL ハンドシェイクの一部として、eStreamer Server 要求はクライアント認証認証、認証が有効であることを確認し。

SSL セッションが設定された後、eStreamer サーバは認証の追加接続後の確認を行います。 接続後の確認が終了した後、eStreamer サーバはクライアントからのデータ要求を待ちます。

ステップ 2： eStreamer サービスからの Client 要求 データ

このステップでは、eStreamer サービスからの Client 要求 データは流れるべきデータの種類を規定 し。 単一 イベント REQUEST メッセージはイベント メタデータを含む利用可能 な イベント データの組み合せを、規定できます。 単一 の ホスト Profile 要求はマルチプルホストを規定できます。 2 つの要求モードはイベント data&colon を要求するために利用できます;

- **イベント ストリーム要求:** クライアントは各型の要求されたイベントタイプおよびバージョンを規定 する、eStreamer サーバは要求されたデータの流出によって応答します含むメッセージ要求フラグを入れ。
- **拡張要求:** クライアントはイベント ストリーム要求のためにと同じメッセージフォーマットの要求を入れますが、拡張要求のためのフラグをセットします。 これは Client 要求 その他の情報およびイベント ストリーム 要求によって使用不可能なバージョン組合せ eStreamer サーバとクライアント間のメッセージ 相互対話を始めます。

手順 3： eStreamer は要求されたデータ ストリームを確立します

このステージでは、eStreamer はクライアントに要求されたデータ ストリームを確立します。 不活動期間の間に、eStreamer はクライアントに接続を開いた保持するために定期的にヌル メッセージを送ります。 クライアントか中間 ホストから工ラーメッセージを受け取る場合、接続を切断します。

ステップ 4： 接続終端

eStreamer サーバはまた次の原因でクライアント接続を切断できます:

- メッセージを送信 することは工ラーという結果に終ります。 これには両方のイベントデータメッセージが含まれ、ヌル キープアライブ メッセージ eStreamer は不活動期間の間に送信

します。
- エラーは Client 要求を処理している間発生します。
- クライアント認証は失敗します（No エラーメッセージは送信 されます）。
- eStreamer サービスはシャットダウンしています（No エラーメッセージは送信 されます）。

クライアントはイベントがないことを示します

eStreamer クライアントアプリケーションのイベントを参照しない場合、この問題を解決するために下記のステップに従って下さい:

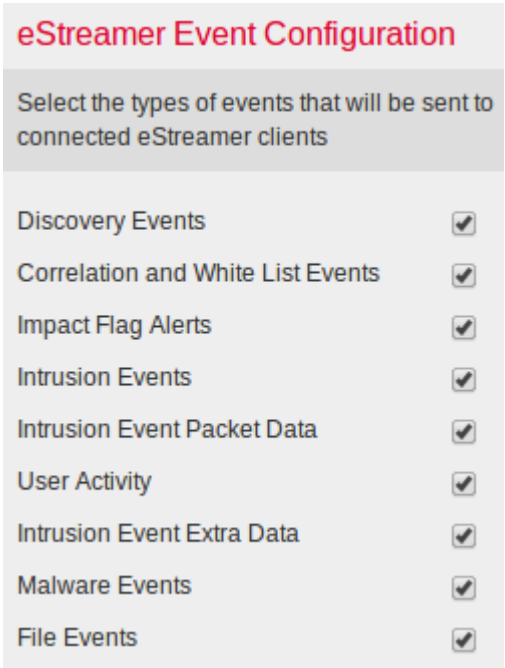
ステップ 1 設定の確認

イベントの型が eStreamer サーバそれらを要求するクライアントアプリケーションに送信できる制御できます。 eStreamer によって送信されるイベントの種類を設定するために下記のようにステップに従って下さい:

1. [System] > [Local] > [Registration] に移動します。

2. **eStreamer** タブをクリックして下さい。

3. **eStreamer イベント構成** メニューの下で、eStreamer にクライアントの要求に送ってほしいイベントの種類の隣でチェックボックスを選択して下さい。



> **注** クライアントアプリケーションが受け取ってそれにほしいイベントの種類を要求することを確かめて下さい。 REQUEST メッセージは eStreamer サーバに送られなければなりません（FireSIGHT Management Center か管理対象装置）。

4. [Save] をクリックします。

ステップ 2

必須認証が追加されることを確かめて下さい。 eStreamer がクライアントに eStreamer イベントを送ることができる前にクライアントは eStreamer 設定 ページを使用して eStreamer サーバの同位 データベースに追加する必要があります。 eStreamer サーバによって生成される認証 認証はまたクライアントにコピーする必要があります。

ステップ 3： エラーメッセージをチェックして下さい

次のコマンドの使用によって `/var/log/messages` の明らかな eStreamer 関連エラーを識別して下さい:

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

ステップ 4： 接続の確認

サーバが着信接続を許可していることを確認して下さい。

```
admin@FireSIGHT:~$ netstat -an | grep 8302
```
出力は下記にのように見える必要があります。 そうでなかったら、それからサービスは動作しないかもしれません。

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

ステップ 5： プロセスのステータスをチェックして下さい

`sfestreamer` プロセスが実行があるかどうか確認するために、次のコマンドを使用して下さい:

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

クライアントは重複したイベントを示します

クライアントで表示するハンドル重複したイベント

eStreamer サーバは送信 する、従ってクライアントアプリケーションは重複したイベントがあるように確認する必要がありますイベントの履歴を保存しません。 重複したイベントはさまざまな理由で発生する場合があります。 たとえば、新しい流出セッションを開始した場合、開始点としてクライアントが規定 する新しいセッションの時間はいくつかがではなかったいくつかおよび前のセッションで送信 されるかもしれない複数 メッセージがある場合がある。 eStreamer は規定された 要求 基準を満たすすべてのメッセージを送信 します。 EStreamer クライアントアプリケーションは非重複あらゆる生じる重複検出するように設計し。

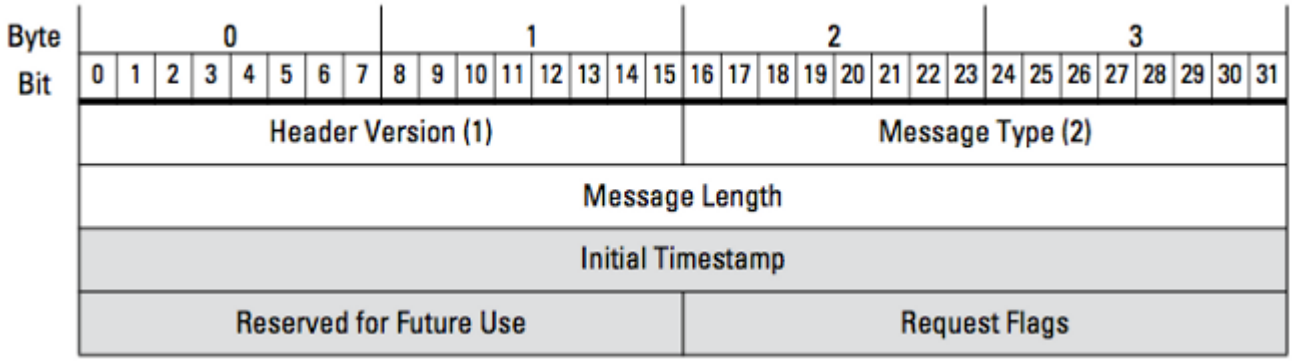
データのための重複した要求を管理して下さい

複数のフラグか複数の拡張要求によって同じデータの複数のバージョンを、要求すれば、最上位バージョンは使用されます。 たとえば、eStreamer がディスカバリ イベント バージョン 1 および 6 のためのフラグ 要求およびバージョン 3 のための拡張要求を受け取れば、バージョン 6 を送信 します。

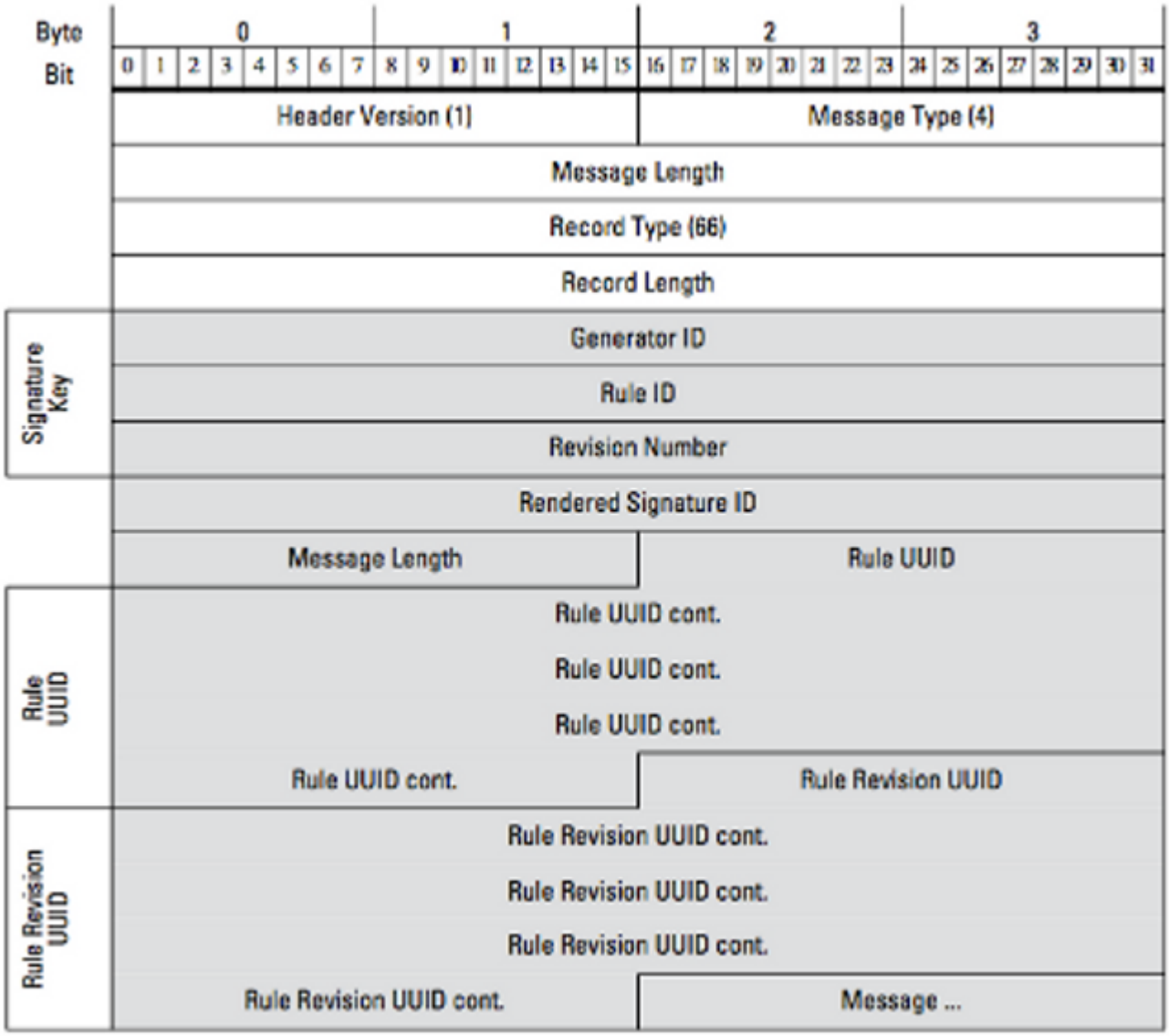
クライアントは示します不正確な Snort ルール ID （ SID ）を

これは通常ルールがシステムにインポートされるとき SID 競合が原因で、SID 内部で再マップされます起こります。

再マップされた SID が、*拡張*ヘッダを有効に しなければならないよりもむしろ、入力した SID を使用するため。 ビット 23 要求拡張イベント ヘッダー。 このフィールドが 0 に設定 される場合、イベントはレコードタイプおよびレコード長だけを含む標準のイベント ヘッダと送信 されます。



***図：** ダイアグラムは eStreamer からのデータを要求するのに使用されるメッセージフォーマットを説明します。 REQUEST メッセージ 形式に特定のフィールドは灰色で強調表示されます。*



***図：** ダイアグラムはルール メッセージ レコードの内で送信されるイベントのためのルール メッセージ情報の形式を説明します。 それは（予想する）数はであるかどれ **RuleID を**（使用するようになっているかどれを）**されたシグニチャ ID** 示し。*

ヒント： 各ビットおよびメッセージの詳細説明を見つけるために、*eStreamer 統合ガイド* を読んで下さい。

追加を解決しますデータを集め、分析して下さい

ssl_test.pl スクリプトを使用してテストして下さい

問題点を明らかにするために EventStreamer *Software Development Kit（SDK）*で提供される `ssl_test.pl` 利用して下さい。 SDK はサポート サイトの ZIP ファイルで利用できます。 その ZIP ファイルに含まれているスクリプトのための手順は README.txt で利用できます。

キャプチャ パケット（PCAP）

eStreamer サーバのマネージメントインターフェイスのパケットをキャプチャ し、それを分析して下さい。 トラフィックがネットワークでどこかにブロックされないし、拒否されないことを確認して下さい。

生成するはファイルを解決します

上記のトラブルシューティング の 手順を完了した、問題を判別することがそれでもできなかったら場合 FireSIGHT Management Center からのトラブルシューティング ファイルを生成して下さい。 追加すべてを解決します更なる分析のための Cisco テク二カル サポートにデータを提供します。