FireSIGHT システムと eStreamer クライアント（SIEM）間の問題のトラブルシューティング

目次

概要

Event Streamer（eStreamer）を使用すると、FireSIGHT システムからカスタム開発されたクライアント アプリケーションに数種類のイベント データをストリーム配信できます。 クライアント アプリケーションを作成したら、それを eStreamer サーバ（たとえば、FireSIGHT Management Center）に接続し、eStreamer サービスを開始して、データのやり取りを始めることができます。 eStreamer の統合にはカスタム プログラミングが必要ですが、これによりアプライアンスの特定のデータを要求できるようになります。 このドキュメントでは、eStreamer クライアントの通信方法とクライアントに関する問題のトラブルシューティング方法について説明します。

eStreamer クライアントとサーバ間の通信方式

クライアントと eStreamer サービスの間で発生する通信には、主に次の 4 つの段階があります。

ステップ 1： クライアントによる eStreamer サーバとの接続の確立

まず、クライアントは eStreamer サーバとの接続を確立し、その接続が両者によって認証されます。 クライアントは、eStreamer からデータを要求する前に、eStreamer サービスとの間で SSL 対応の 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、eStreamer サーバが応答し、クライアントとの SSL ハンドシェイクを開始します。 SSL ハンドシェイクの一部として、eStreamer サーバはクライアント認証証明書を要求し、証明書が有効であることを検証します。

SSL セッションが確立されると、eStreamer サーバは接続後の追加の証明書検証を行います。 接続後の検証が完了すると、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： クライアントによる eStreamer サービスからのデータの要求

このステップでは、クライアントが eStreamer サービスからデータを要求し、ストリーム配信するデータのタイプを指定します。 1 つのイベント要求メッセージで、イベントのメタデータを含む使用可能なイベント データを任意に組み合わせて指定できます。 1 つのホスト プロファイル要求で、1 つまたは複数のホストを指定できます。 イベント データを要求するときは、次の 2 つの要求モードを使用できます。

- **イベント ストリーム要求**： クライアントは、要求されたイベントのタイプと各タイプのバージョンを指定する要求フラグを含むメッセージを送信します。eStreamer サーバは、要求されたデータをストリーム配信することで応答します。
- **拡張要求**： クライアントはイベント ストリーム要求と同じメッセージ形式で要求を送信しますが、拡張要求のフラグを設定します。 これにより、クライアントと eStreamer サーバの間でメッセージのやり取りが始まり、クライアントはその中で、イベント ストリーム要求では使用できない追加情報やバージョンの組み合わせを要求します。

ステップ3： eStreamer による要求されたデータ ストリームの確立

この段階では、eStreamer がクライアントへの要求されたデータ ストリームを確立します。 アクティビティがない期間は、eStreamer がクライアントに定期的に空白のメッセージを送信して、接続を開いた状態に維持します。 クライアントまたは中継ホストからエラー メッセージを受信した場合は、接続を閉じます。

ステップ 4： 接続の終了

eStreamer サーバは、次の理由でクライアント接続を閉じることもできます。

- メッセージを送信してエラーが発生した場合。 これには、イベント データ メッセージと、アクティビティがない期間中に eStreamer が送信する空白のキープアライブ メッセージの両方が含まれます。
- クライアント要求の処理中にエラーが発生した場合。
- クライアント認証が失敗した場合（エラー メッセージは送信されません）。
- eStreamer サービスがシャットダウンしている場合（エラー メッセージは送信されません）。

クライアントにイベントが表示されない

eStreamer クライアント アプリケーションにイベントが表示されない場合は、次の手順に従ってこの問題をトラブルシューティングしてください。

ステップ 1： 設定の確認

要求元のクライアントに eStreamer サーバが送信できるイベントのタイプを制御できます。 eStreamer から送信されるイベントのタイプを設定するには、次の手順を実行します。

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

2. [eStreamer] タブをクリックします。

3. [eStreamer Event Configuration] メニューで、eStreamer から要求元のクライアントに送信するイベントのタイプの横にあるチェックボックスをオンにします。

> **注:** クライアント アプリケーションが受信する必要のあるイベントのタイプを要求していることを確認してください。 要求メッセージが eStreamer サーバ（FireSIGHT Management Center または管理対象デバイス）に送信されている必要があります。

4. [Save] をクリックします。

ステップ 2： 証明書の検証

必要な証明書が追加されたことを確認します。 eStreamer からクライアントに eStreamer イベントを送信する前に、eStreamer の設定ページを使用して、eStreamer サーバのピア データベースにクライアントを追加する必要があります。 eStreamer サーバによって生成された認証証明書は、クライアントにもコピーする必要があります。

ステップ 3： エラー メッセージの確認

次のコマンドを使用して、/var/log/messages 内の明らかに eStreamer に関連するエラーを特定

します。

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

ステップ 4： 接続の検証

サーバが着信接続を受け入れていることを検証します。

```
admin@FireSIGHT:~$ netstat -an | grep 8302
```
出力は次のようになります。 それ以外の場合、サービスが動作していない可能性があります。

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

ステップ 5： プロセスのステータスの確認

sfestreamer プロセスが実行中かどうかを検証するには、次のコマンドを使用します。

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

クライアントに重複イベントが表示される

クライアントに表示される重複イベントの処理

eStreamer サーバには送信したイベントの履歴が保持されないため、クライアント アプリケーションで重複イベントをチェックする必要があります。 重複イベントは、さまざまな理由で発生する可能性があります。 たとえば、新しいストリーム セッションを開始したときに、新しいセッションの開始点としてクライアントが指定した時間に複数のメッセージがあり、その中に前のセッションで送信されたものと送信されなかったものが存在する可能性があります。 eStreamer は、指定された要求の条件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、発生した重複を検出して排除するように設計されている必要があります。

データの重複する要求の管理

複数のフラグまたは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ると、最も新しいバージョンが使用されます。 たとえば、eStreamer は検出イベントのバージョン 1 および 6 のフラグ要求とバージョン 3 の拡張要求を受信すると、バージョン 6 を送信します。

クライアントに不正な Snort ルール ID（SID）が表示される

これは通常、システムにルールがインポートされ、内部で SID が再マップされたときに、SID が競合するために発生します。

再マップされた SID ではなく入力した SID を使用するには、*拡張*ヘッダーを有効にする必要があります。 ビット 23 は拡張イベント ヘッダーを要求します。 このフィールドを 0 に設定すると、レコード タイプとレコード長のみを含む標準イベント ヘッダーでイベントが送信されます。

図： この図は、eStreamer からデータを要求するために使用されるメッセージ形式を示しています。 要求メッセージ形式に固有のフィールドはグレーで強調表示されています。

図： この図は、ルール メッセージ レコードで送信されるイベントのルール メッセージ情報の形式を示しています。 ***Rule Id (現在使用している) と*** *(現在使用している) と* ***Rendered Signature ID*** *(想定する番号) が示されています。*

> **ヒント**： 各ビットとメッセージの詳しい説明については、『*eStreamer 統合ガイド*』を参照してください。

追加のトラブルシューティング データの収集と分析

ssl_test.pl スクリプトを使ったテスト

EventStreamer *ソフトウェア開発キット (SDK)* で提供される ssl_test.pl スクリプトを利用して、問題を特定します。 この SDK は、サポート サイトから zip ファイル形式で入手できます。 スクリプトの操作手順は、この zip ファイルに含まれる README.txt に記載されています。

パケットのキャプチャ (PCAP)

eStreamer サーバの管理インターフェイスでパケットをキャプチャし、それを分析します。 トラフィックがネットワークのどこかでブロックまたは拒否されていないことを検証します。

トラブルシューティング ファイルの生成

上記のトラブルシューティング手順を実行しても問題を特定できなかった場合は、FireSIGHT Management Center でトラブルシューティング ファイルを生成します。 さらに詳しく分析するため、追加のトラブルシューティング データをシスコ テクニカル サポートに提供します。