مظان نيب احالصإو تالكشملا فاشتكأس Streamer (SIEM) لميمعو FireSIGHT

المحتويات

المقدمة

يتيح لك تطبيق eStreamer (Event Streamer) إمكانية تدفق أنواع عديدة من بيانات الحدث من نظام FireSIGHT System إلى تطبيق عميل تم تطويره خصيصا. بعد إنشاء تطبيق عميل، يمكنك توصيله بخادم eStreamer (على سبيل المثال، مركز إدارة FireSIGHT) وبدء خدمة eStreamer وبدء تبادل البيانات. يتطلب تكامل eStreamer برمجة مخصصة، ولكنه يسمح لك بطلب بيانات معينة من جهاز. يوضح هذا المستند كيفية اتصال عميل Streamer وكيفية أستكشاف أخطاء أحد العملاء وإصلاحها.

أسلوب الاتصال بين عميل eStreamer والخادم

توجد أربع مراحل رئيسية للاتصال بين العميل وخدمة eStreamer:

الخطوة 1: يقوم العميل بإنشاء اتصال بخادم eStreamer

أولا، يقوم العميل بإنشاء اتصال بخادم eStreamer ويتم مصادقة الاتصال من قبل كلا الطرفين. قبل أن يتمكن العميل من طلب البيانات من eStreamer، يجب على العميل بدء اتصال TCP تم تمكين SSL باستخدام خدمة eStreamer. عندما يقوم العميل ببدء الاتصال، يستجيب خادم eStreamer، مما يؤدي إلى بدء مصافحة SSL مع العميل. كجزء من مصافحة SSL، يطلب خادم eStreamer شهادة مصادقة العميل، ويتحقق من صحة الشهادة.

بعد إنشاء جلسة SSL، يقوم خادم eStreamer بإجراء تحقق إضافي بعد الاتصال من الشهادة. بعد الانتهاء من التحقق من الاتصال اللاحق، ينتظر خادم eStreamer طلب بيانات من العميل.

الخطوة 2: يطلب العميل بيانات من خدمة eStreamer

في هذه الخطوة، يطلب العميل البيانات من خدمة eStreamer ويحدد أنواع البيانات التي سيتم تدفقها. يمكن لرسالة طلب حدث واحدة تحديد أي مزيج من بيانات الحدث المتوفرة، بما في ذلك بيانات تعريف الحدث. يمكن لطلب ملف تعريف مضيف واحد تحديد مضيف واحد أو عدة مضيفين. يتوفر وضعان للطلب لطلب بيانات الحدث&colon؛

- **طلب تدفق الأحداث:** يقدم العميل رسالة تحتوي على علامات طلب تحدد أنواع الأحداث المطلوبة وإصدارها من كل نوع، ويستجيب خادم eStreamer عن طريق دفق البيانات المطلوبة.
- **طلب موسع:** يقدم العميل طلبا بنفس تنسيق الرسالة كما هو الحال بالنسبة لطلبات تدفق الأحداث ولكنه يحدد علامة لطلب موسع. وهذا يؤدي إلى بدء تفاعل رسائل بين العميل وخادم eStreamer يطلب العميل من خلاله معلومات إضافية ومجموعات إصدارات غير متوفرة عبر طلبات تدفق الأحداث.

الخطوة 3: يقوم eStreamer بإنشاء تدفق البيانات المطلوب

في هذه المرحلة، يقوم eStreamer بإنشاء تدفق البيانات المطلوب للعميل. أثناء فترات عدم النشاط، يرسل eStreamer رسائل دورية فارغة إلى العميل لإبقاء الاتصال مفتوحا. إذا تلقت رسالة خطأ من العميل أو من مضيف متوسط، فإنها تغلق الاتصال.

الخطوة 4: انتهاء الاتصال

كما يمكن لخادم eStreamer إغلاق اتصال عميل للأسباب التالية:

- يؤدي إرسال رسالة في أي وقت إلى حدوث خطأ. ويتضمن ذلك كل من رسائل بيانات الحدث وإرسال الرسالة الفارغة Keep-Live Message Streamer أثناء فترات عدم النشاط.
- حدث خطأ أثناء معالجة طلب عميل.
- فشل مصادقة العميل (لم يتم إرسال رسالة خطأ).

- يتم الآن إيقاف تشغيل خدمة eStreamer (لم يتم إرسال رسالة خطأ).

لا يظهر العميل أي حدث

إذا لم يظهر لديك أي أحداث على تطبيق عميل Streamer، فيرجى اتباع الخطوات التالية لاستكشاف هذه المشكلة وإصلاحها:

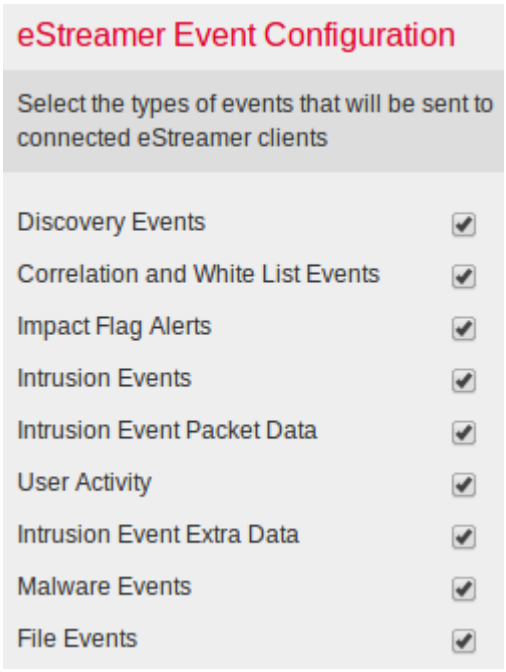
الخطوة 1: التحقق من التكوين

يمكنك التحكم في أنواع الأحداث التي يمكن لخادم eStreamer إرسالها إلى تطبيقات العميل التي تطلبها. لتكوين أنواع الأحداث التي يتم إرسالها بواسطة eStreamer، اتبع الخطوات التالية:

1. انتقل إلى **النظام > محلي > التسجيل**.

2. انقر فوق علامة التبويب **eStreamer**.

3. تحت قائمة **تكوين حدث eStreamer**، حدد خانات الاختيار المجاورة لأنواع الأحداث التي تريد أن يرسلها eStreamer إلى العملاء الذين يطلبون ذلك.



ملاحظة: تأكد من أن طلب العميل الخاص بك يطلب أنواع الأحداث التي تريد أن يتلقاها. يجب إرسال رسالة الطلب إلى خادم eStreamer (مركز إدارة FireSIGHT أو الجهاز المدار).

4. انقر فوق **حفظ**.

الخطوة 2: التحقق من الشهادة

تأكد من إضافة الشهادات المطلوبة. قبل أن يتمكن eStreamer من إرسال أحداث eStreamer إلى عميل، يجب إضافة العميل إلى قاعدة بيانات أقران خادم eStreamer باستخدام صفحة تكوين eStreamer. كما يجب نسخ شهادة المصادقة التي تم إنشاؤها بواسطة خادم eStreamer إلى العميل.

الخطوة 3: التحقق من رسائل الخطأ

حدد أي أخطاء واضحة متعلقة ب eStreamer في /var/log/الرسائل باستخدام الأمر التالي:

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

الخطوة 4: التحقق من الاتصال

تحقق من قبول الخادم للاتصالات الواردة.

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

وينبغي أن يبدو الناتج في الأسفل. وإذا لم يكن الأمر كذلك، فقد لا تكون الخدمة قيد التشغيل.

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

الخطوة 5: التحقق من حالة العملية

للتحقق مما إذا كانت عملية SFSTestreamer قيد التشغيل، الرجاء إستخدام الأمر التالي:

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

يظهر العميل الأحداث المكررة

معالجة الأحداث المتكررة المعروضة في عميل

لا يحتفظ خادم eStreamer بمحفوظات الأحداث التي يرسلها، لذا يجب أن يقوم تطبيق العميل بالتحقق من تكرار الأحداث. يمكن أن تحدث أحداث مكررة لمجموعة متنوعة من الأسباب. على سبيل المثال، عند بدء جلسة دفق جديدة، يمكن أن يكون للوقت الذي يحدده العميل كنقطة بداية للجلسة الجديدة رسائل متعددة، قد يكون تم إرسال بعضها في جلسة العمل السابقة وبعضها لم يتم إرساله. يرسل eStreamer جميع الرسائل التي تفي بمعايير الطلب المحددة. يجب تصميم تطبيقات عميل EStreamer لاكتشاف أي تكرارات ناتجة عن ذلك وإلغاء تكرارها.

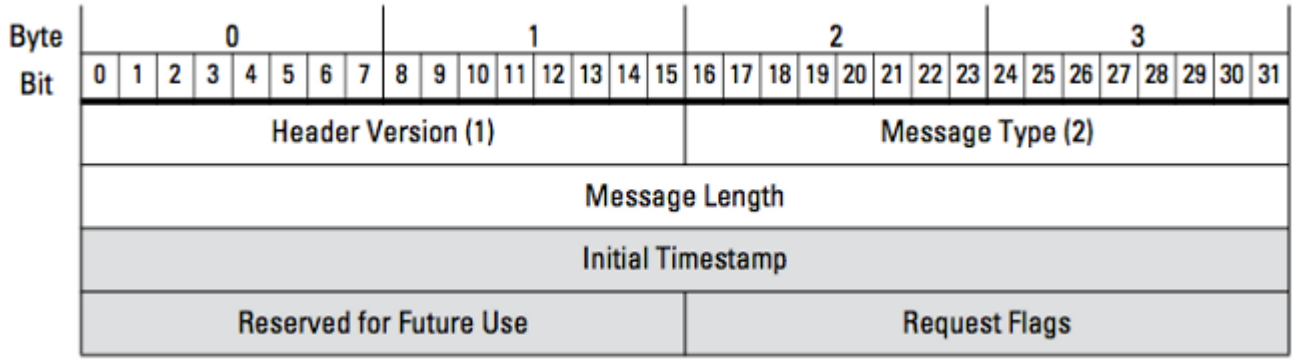
إدارة الطلبات المتكررة للبيانات

إذا قمت بطلب إصدارات متعددة من نفس البيانات، إما بواسطة علامات متعددة أو طلبات موسعة متعددة، يتم إستخدام الإصدار الأعلى. على سبيل المثال، إذا كان eStreamer يتلقى طلبات العلامات لأحداث الاكتشاف الإصدار 1 و 6 وطلب موسع للإصدار 3، فإنه يرسل الإصدار 6.

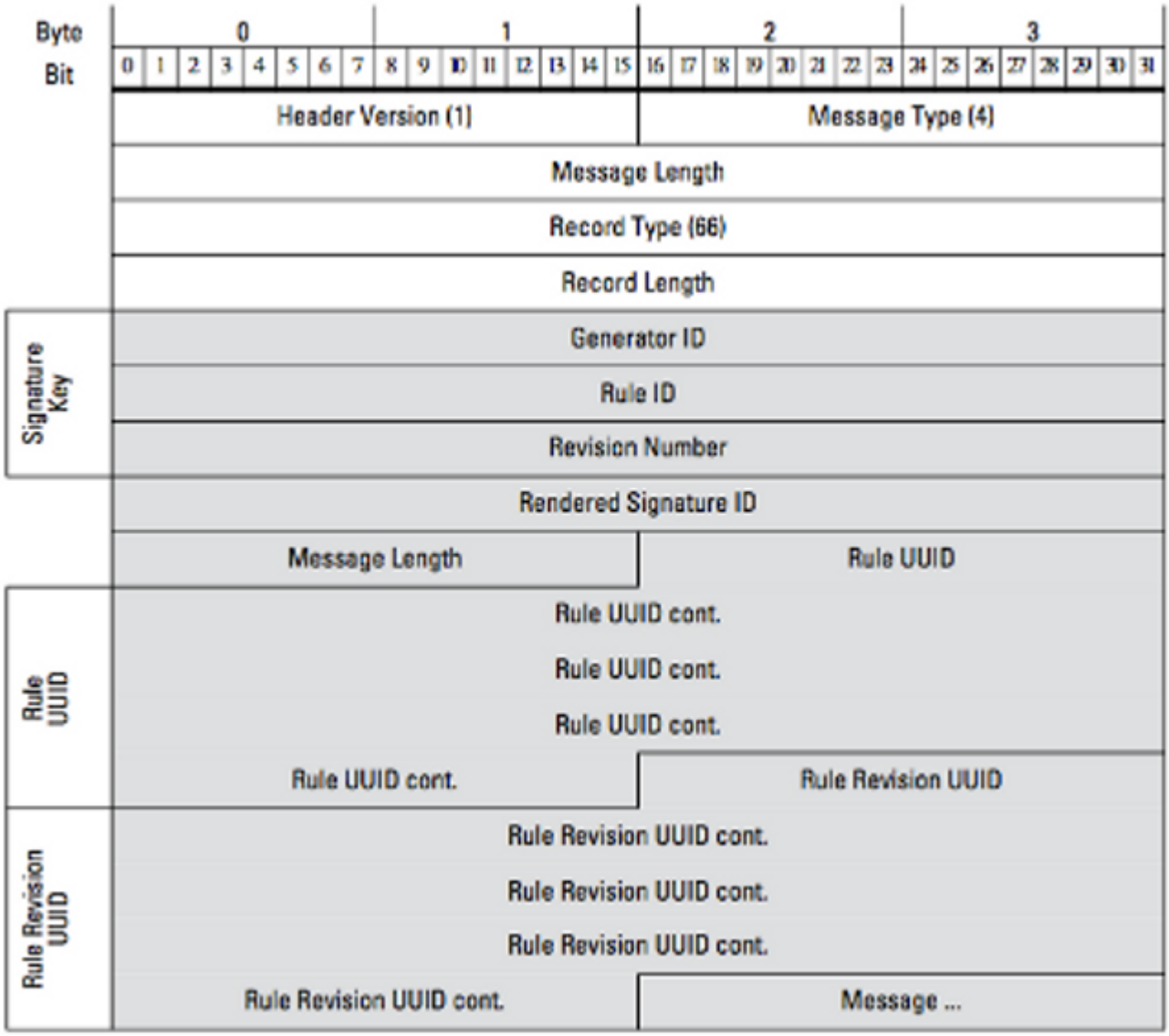
يظهر العميل معرف قاعدة SNORT (SID) غير صحيح

يحدث هذا عادة بسبب تعارض SID عندما يتم إستيراد قاعدة إلى النظام، ويعاد تعيين SID داخليا.

لاستخدام SID الذي أدخلته، بدلا من SID المعاد تعيينه، يجب تمكين *الرأس الموسع*. يطلب البت 23 رؤوس أحداث موسعة. في حالة تعيين هذا الحقل إلى 0، يتم إرسال الأحداث برأس حدث قياسي يتضمن فقط نوع السجل وطول السجل.



الشكل: يوضح الرسم التخطيطي تنسيق الرسالة المستخدم لطلب البيانات من eStreamer. يتم إبراز الحقول الخاصة بتنسيق رسالة الطلب باللون الرمادي.



الشكل: يوضح الرسم التخطيطي شكل معلومات رسالة القاعدة لحدث يتم إرساله ضمن سجل رسائل القاعدة. وهو يعرض ***RuleID*** *(الذي تستخدمه الآن) و****معرف التوقيع المجسد*** *(الذي هو الرقم الذي تتوقعه).*

تلميح: للعثور على وصف تفصيلي لكل بت لكل رسالة، اقرأ *دليل تكامل eStreamer*.

تجميع بيانات أستكشاف الأخطاء وإصلاحها الإضافية وتحليلها

الاختبار باستخدام البرنامج النصي ssl_test.pl

أستخدم البرنامج النصي ssl_test.pl المتوفر في *مجموعة أدوات تطوير برامج (SDK) Event Streamer* لتحديد المشكلة. يتوفر بروتوكول SDK في ملف مضغوط على موقع الدعم. تعليمات النص التنفيذي متوفرة في README.txt، والتي يتم تضمينها في ملف zip.

حزمة الالتقاط (PCAP)

التقاط الحزم على واجهة إدارة خادم Streamer وتحليلها. تحقق من عدم حظر حركة المرور أو رفضها في مكان ما

في الشبكة.

إنشاء ملف أستكشاف الأخطاء وإصلاحها

إذا أكملت خطوات أستكشاف الأخطاء وإصلاحها المذكورة أعلاه، ولا تزال غير قادر على تحديد المشكلة، فيرجى إنشاء ملف أستكشاف الأخطاء وإصلاحها من مركز إدارة FireSIGHT لديك. توفير جميع بيانات أستكشاف الأخطاء وإصلاحها الإضافية إلى دعم Cisco التقني لمزيد من التحليل.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).