Problemen oplossen tussen FireSIGHT System en eStreamer Client (SIEM)

Inhoud

Inleiding

De Event Streamer (eStreamer) stelt u in staat om verschillende soorten gebeurtenisgegevens van een FireSIGHT-systeem te streamen naar een op maat ontwikkelde clienttoepassing. Nadat u een clienttoepassing hebt gemaakt, kunt u deze aansluiten op een eStreamer-server (bijvoorbeeld een FireSIGHT Management Center), de eStreamer-service starten en gegevens uitwisselen. eStreamer-integratie vereist aangepaste programmering, maar stelt u in staat specifieke gegevens van een apparaat op te vragen. Dit document beschrijft hoe een eStreamer-client communiceert en hoe u problemen met een client kunt oplossen.

Communicatiemethode tussen eStreamer-client en -server

Er zijn vier belangrijke fasen van communicatie tussen een klant en de eStreamer-service:

Stap 1: client maakt verbinding met eStreamer-server

Eerst maakt een client een verbinding met eStreamer-server en de verbinding wordt door beide partijen geverifieerd. Voordat een client gegevens kan aanvragen bij eStreamer, moet de client een SSL-enabled TCP-verbinding met de eStreamer-service starten. Wanneer de client de verbinding start, reageert de eStreamer-server en start een SSL-handdruk op de client. Als onderdeel van de SSL-handdruk vraagt de eStreamer-server het verificatiecertificaat van de client aan en controleert hij of het certificaat geldig is.

Nadat de SSL-sessie is ingesteld, voert de eStreamer-server een aanvullende verificatie van het certificaat uit na de verbinding. Nadat de verificatie na de verbinding is voltooid, wacht de eStreamer-server op een gegevensaanvraag van de client.

Stap 2: Clientaanvragen voor gegevens van de eStreamer-service

In deze stap vraagt de client gegevens aan bij de eStreamer-service en specificeert de typen gegevens die moeten worden gestreamd. Een enkel gebeurtenisverzoekbericht kan elke combinatie van beschikbare gebeurtenisgegevens, inclusief gebeurtenismetagegevens, specificeren. Een enkele hostprofielaanvraag kan één host of meerdere hosts specificeren. Er zijn twee aanvraagmodi beschikbaar voor het opvragen van gebeurtenisgegevens&dubbele punt;

- **Aanvraag voor gebeurtenisstromen:** De client dient een bericht in met verzoekvlaggen die de gevraagde eventtypen en versie van elk type specificeren, en de eStreamer-server reageert door de gevraagde gegevens te streamen.
- **Uitgebreide aanvraag:** De client dient een verzoek in met hetzelfde berichtformaat als voor Event Stream-verzoeken, maar stelt een vlag in voor een uitgebreid verzoek. Hierdoor wordt een berichteninteractie tussen client en eStreamer-server gestart waardoor de client aanvullende informatie en versiecombinaties vraagt die niet beschikbaar zijn via Event Stream-verzoeken.

Stap 3: eStreamer stelt de gevraagde gegevensstroom in

In dit stadium, stelt eStreamer de gevraagde gegevensstroom aan de klant op. Tijdens inactiviteitsperioden stuurt eStreamer periodieke nulberichten naar de client om de verbinding open te houden. Als het een foutbericht van de client of een tussenpersoon host ontvangt, sluit het de verbinding.

Stap 4: De verbinding wordt beëindigd

De eStreamer-server kan ook een clientverbinding sluiten om de volgende redenen:

- Elk moment dat het verzenden van een bericht resulteert in een fout. Dit omvat zowel gebeurtenisdataberichten als het ongeldige levensbedreigende bericht eStreamer verstuurt tijdens perioden van inactiviteit.
- Er is een fout opgetreden tijdens het verwerken van een clientverzoek.
- Clientverificatie mislukt (er wordt geen foutbericht verzonden).
- De eStreamer-service is uitgeschakeld (er wordt geen foutbericht verzonden).

De client toont geen gebeurtenis

Als u geen gebeurtenissen ziet in uw eStreamer-clientapplicatie, volgt u de onderstaande stappen om dit probleem op te lossen:

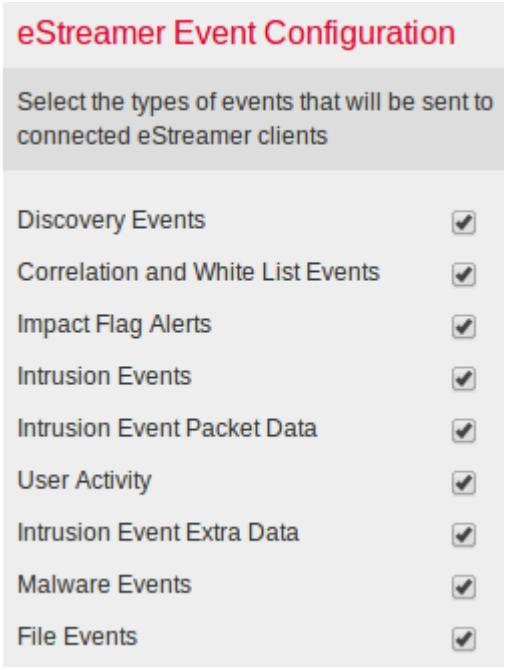
Stap 1: De configuratie verifiëren

U kunt bepalen welke soorten gebeurtenissen de eStreamer-server kan verzenden naar clienttoepassingen die deze aanvragen. Om de soorten gebeurtenissen te configureren die door eStreamer worden verzonden, volgt u de onderstaande stappen:

1. Ga naar **Systeem > Lokaal > Registratie**.

2. Klik op het tabblad **eStreamer**.

3. Selecteer onder het menu **eStreamer Event Configuration** de selectievakjes naast de soorten gebeurtenissen die u eStreamer naar de aanvragende klanten wilt sturen.



> **Opmerking:** Zorg ervoor dat uw clientapplicatie de soorten gebeurtenissen vraagt die u wilt ontvangen. Het aanvraagbericht moet naar de eStreamer-server (FireSIGHT Management Center of beheerd apparaat) worden verzonden.

4. Klik op **Opslaan**.

Stap 2: Controleer het certificaat

Controleer of de vereiste certificaten zijn toegevoegd. Voordat eStreamer eStreamer-gebeurtenissen naar een client kan verzenden, moet de client via de eStreamer-configuratiepagina worden toegevoegd aan de eStreamer-peers-database van de server. Het door de eStreamer-server gegenereerde verificatiecertificaat moet ook naar de client worden gekopieerd.

Stap 3: Foutberichten controleren

Identificeer eventuele duidelijke eStreamer-gerelateerde fouten in /var/log/berichten met behulp van de volgende opdracht:

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

Stap 4: Controleer de verbinding

Controleer of de server inkomende verbindingen accepteert.

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

De output zou als hieronder moeten kijken. Als dit niet het geval is, kan de service mogelijk niet

worden uitgevoerd.

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

Stap 5: Controleer de status van het proces

Om te verifiëren of er een sfestreamer proces actief is, gebruikt u de volgende opdracht:

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

Cliënt toont dubbele gebeurtenissen

Dubbele gebeurtenissen verwerken die in een client worden weergegeven

De eStreamer-server houdt geen geschiedenis bij van de gebeurtenissen die worden verzonden, dus de clienttoepassing moet controleren op dubbele gebeurtenissen. Dubbele gebeurtenissen kunnen om verschillende redenen voorkomen. Bijvoorbeeld, bij het starten van een nieuwe streaming sessie, kan de door de client opgegeven tijd als startpunt voor de nieuwe sessie meerdere berichten hebben, waarvan sommige mogelijk zijn verzonden in de vorige sessie en sommige niet. eStreamer stuurt alle berichten die aan de opgegeven criteria voldoen. EStreamer-clienttoepassingen moeten worden ontworpen om eventuele resulterende duplicaten te detecteren en te dedupliceren.

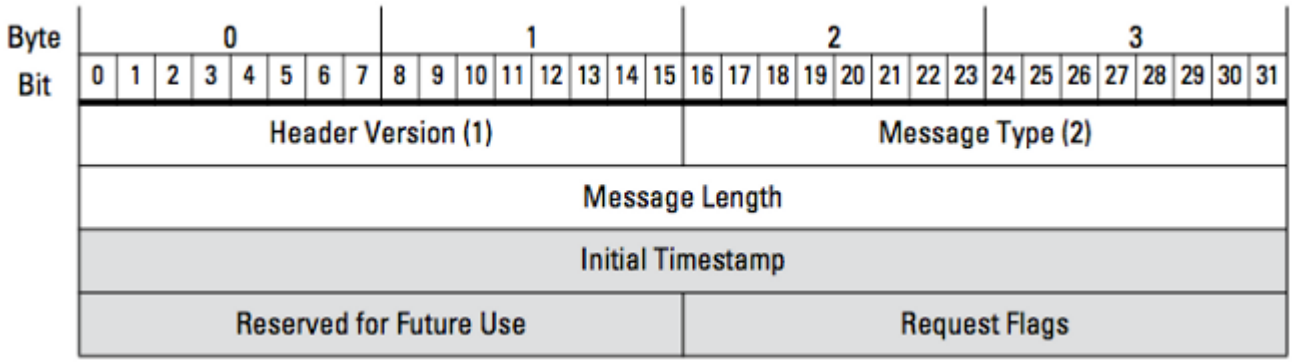
Dubbele aanvragen voor gegevens beheren

Als u meerdere versies van dezelfde gegevens vraagt, door meerdere vlaggen of meerdere uitgebreide verzoeken, wordt de hoogste versie gebruikt. Als eStreamer bijvoorbeeld vlagverzoeken ontvangt voor detectiegebeurtenissen versie 1 en 6 en een uitgebreid verzoek voor versie 3, wordt versie 6 verzonden.

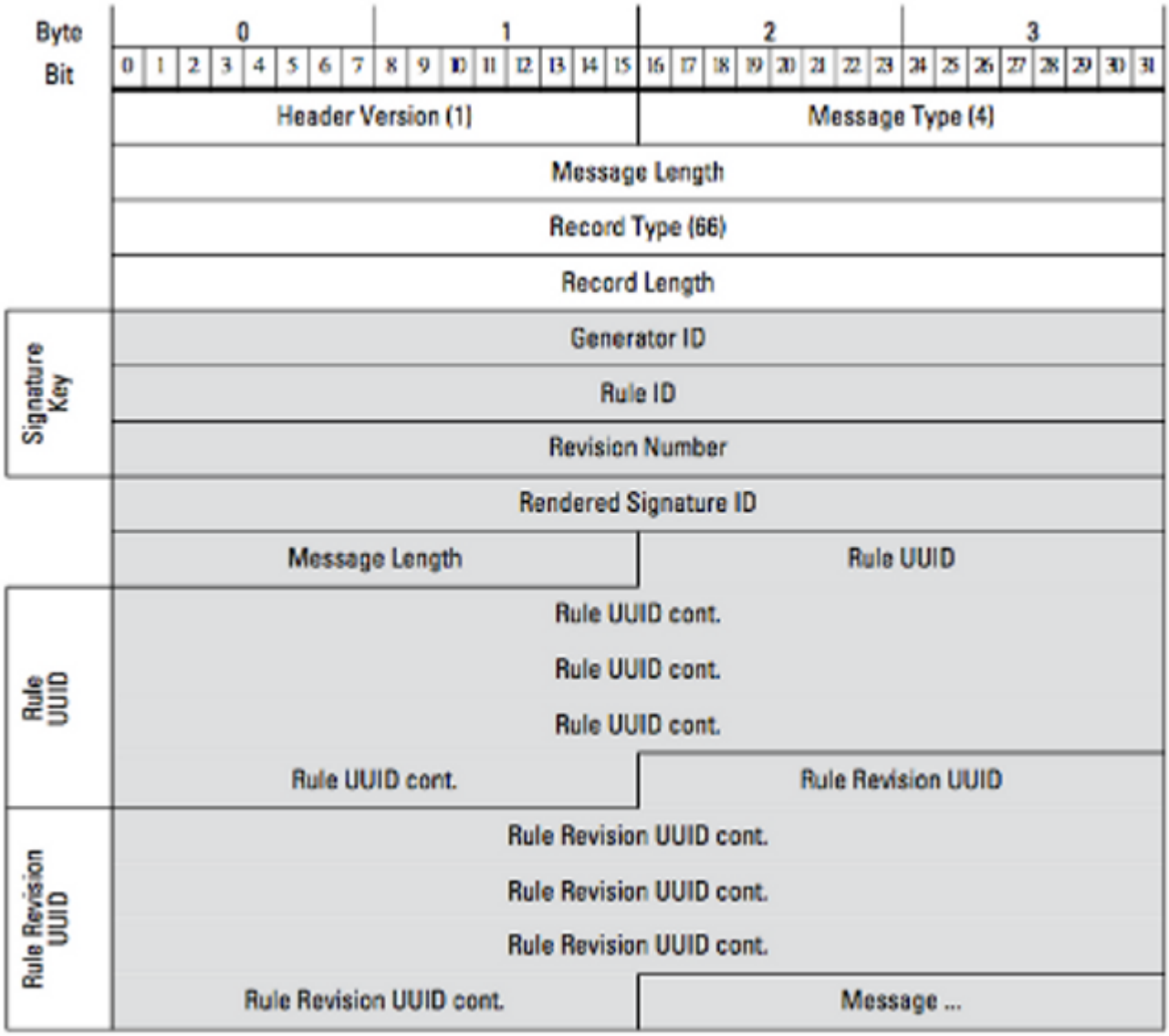
Cliënt toont onjuiste snortregel-ID (SID)

Dit gebeurt gewoonlijk wegens een conflict van SID wanneer een regel in het systeem wordt ingevoerd, wordt SID intern opnieuw in kaart gebracht.

Om de SID te gebruiken die u hebt ingevoerd, in plaats van de opnieuw toegewezen SID, moet u een *uitgebreide header* inschakelen. Bit 23 Verzoeken uitgebreide gebeurtenisheaders. Als dit veld op 0 is ingesteld, worden gebeurtenissen verzonden met een standaard kop van een gebeurtenis die alleen het recordtype en de recordlengte bevat.



Afbeelding: In het diagram wordt het berichtformaat weergegeven dat wordt gebruikt om gegevens bij eStreamer op te vragen. De velden die specifiek zijn voor de indeling van het verzoekbericht worden in grijs gemarkeerd.



Afbeelding: Het diagram illustreert het formaat van de informatie van het regelbericht voor een gebeurtenis die binnen een verslag van het Regelbericht wordt overgebracht. Het toont ***RuleID*** *(die u nu gebruikt) en* ***Rendered Signature ID*** *(die het nummer is dat u verwacht).*

Tip: Om de gedetailleerde beschrijving van elk bit en bericht te vinden, leest u de *eStreamer Integration Guide*.

Aanvullende probleemoplossingsgegevens verzamelen en analyseren

Test met het ssl_test.pl Script

Gebruik het script ssl_test.pl dat in de *Event Streamer Software Development Kit (SDK)* geleverd wordt om het probleem te identificeren. De SDK is beschikbaar in een zipbestand op de ondersteuningswebsite. Instructies voor het script zijn beschikbaar in de README.txt, die is opgenomen in dat zip-bestand.

Capture Packet (PCAP)

Leg pakketten vast op de beheerinterface van de eStreamer-server en analyseer deze. Controleer of het verkeer niet ergens in uw netwerk is geblokkeerd of ontkend.

Probleemoplossing genereren

Als u de bovenstaande stappen voor probleemoplossing hebt voltooid en u het probleem nog steeds niet kunt vaststellen, genereert u een probleemoplossingsbestand vanuit uw FireSIGHT Management Center. Alle aanvullende probleemoplossingsgegevens aan de technische ondersteuning van Cisco leveren voor verdere analyse.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.