Risoluzione dei problemi tra FireSIGHT System e eStreamer Client (SIEM)

Sommario

Introduzione

Event Streamer (eStreamer) consente di eseguire lo streaming di diversi tipi di dati di eventi da un sistema FireSIGHT a un'applicazione client personalizzata. Dopo aver creato un'applicazione client, è possibile collegarla a un server eStreamer (ad esempio, un centro di gestione FireSIGHT), avviare il servizio eStreamer e iniziare lo scambio di dati. L'integrazione di eStreamer richiede una programmazione personalizzata, ma consente di richiedere dati specifici a un accessorio. Questo documento descrive come un client eStreamer comunica e come risolvere un problema con un client.

Metodo di comunicazione tra client e server eStreamer

Tra un client e il servizio eStreamer si verificano quattro fasi principali di comunicazione:

Passaggio 1: Il client stabilisce una connessione con il server eStreamer

In primo luogo, un client stabilisce una connessione con il server eStreamer e la connessione viene autenticata da entrambe le parti. Prima che un client possa richiedere dati a eStreamer, deve avviare una connessione TCP abilitata per SSL con il servizio eStreamer. Quando il client avvia la connessione, il server eStreamer risponde, avviando un handshake SSL con il client. Come parte dell'handshake SSL, il server eStreamer richiede il certificato di autenticazione del client e verifica che il certificato sia valido.

Una volta stabilita la sessione SSL, il server eStreamer esegue un'ulteriore verifica del certificato successiva alla connessione. Al termine della verifica successiva alla connessione, il server eStreamer attende una richiesta di dati dal client.

Passaggio 2: Il client richiede i dati dal servizio eStreamer

In questo passaggio il client richiede i dati dal servizio eStreamer e specifica i tipi di dati da inviare in streaming. Un singolo messaggio di richiesta di evento può specificare qualsiasi combinazione di dati di evento disponibili, inclusi i metadati di evento. Una singola richiesta di profilo host può specificare uno o più host. Sono disponibili due modalità di richiesta per la richiesta di dati:

- **Richiesta flusso eventi:** Il client invia un messaggio contenente i flag di richiesta che specificano i tipi di evento richiesti e la versione di ciascun tipo. Il server eStreamer risponde inviando i dati richiesti come flusso.
- **Richiesta estesa:** Il client invia una richiesta con lo stesso formato di messaggio delle richieste del flusso di eventi, ma imposta un flag per una richiesta estesa. In questo modo viene avviata un'interazione tra il client e il server eStreamer tramite la quale il client richiede informazioni aggiuntive e combinazioni di versioni non disponibili tramite le richieste del flusso di eventi.

Passaggio 3: eStreamer stabilisce il flusso di dati richiesto

In questa fase eStreamer stabilisce il flusso di dati richiesto al client. Durante i periodi di inattività, eStreamer invia periodicamente messaggi nulli al client per mantenere aperta la connessione. Se riceve un messaggio di errore dal client o da un host intermedio, chiude la connessione.

Passaggio 4: La connessione termina

Il server eStreamer può inoltre chiudere una connessione client per i seguenti motivi:

- Ogni volta che si invia un messaggio viene generato un errore. Ciò include sia i messaggi di dati degli eventi che i messaggi null keep-alive inviati da eStreamer durante i periodi di inattività.
- Errore durante l'elaborazione di una richiesta client.
- Autenticazione client non riuscita (nessun messaggio di errore inviato).
- Arresto del servizio eStreamer in corso (non viene inviato alcun messaggio di errore).

Nessun evento visualizzato dal client

Se nell'applicazione client eStreamer non vengono visualizzati eventi, eseguire la procedura seguente per risolvere il problema:

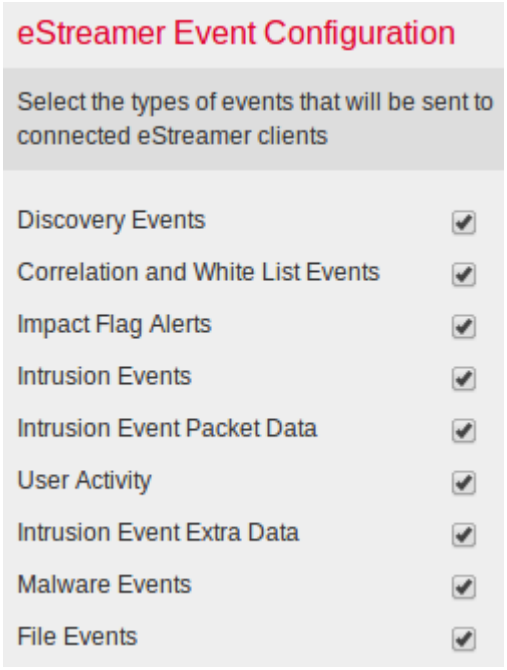
Passaggio 1: Verifica della configurazione

Èpossibile controllare i tipi di eventi che il server eStreamer è in grado di trasmettere alle applicazioni client che li richiedono. Per configurare i tipi di eventi trasmessi da eStreamer, attenersi alla seguente procedura:

1. Passare a **Sistema > Locale > Registrazione**.

2. Fare clic sulla scheda **eStreamer**.

3. Nel menu **eStreamer Event Configuration**, selezionare le caselle di controllo accanto ai tipi di eventi che eStreamer deve inviare ai client richiedenti.



Nota: Assicurarsi che l'applicazione client richieda i tipi di eventi che si desidera ricevere. Il

messaggio di richiesta deve essere inviato al server eStreamer (centro di gestione FireSIGHT o dispositivo gestito).

4. Fare clic su **Salva**.

Passaggio 2: Verifica il certificato

Verificare che i certificati richiesti siano stati aggiunti. Prima che eStreamer possa inviare eventi eStreamer a un client, il client deve essere aggiunto al database peer del server eStreamer utilizzando la pagina di configurazione eStreamer. Anche il certificato di autenticazione generato dal server eStreamer deve essere copiato nel client.

Passaggio 3: Controlla messaggi di errore

Identificare eventuali errori eStreamer evidenti in /var/log/messages utilizzando il seguente comando:

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

Passaggio 4: Verifica connessione

Verificare che il server accetti connessioni in ingresso.

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

L'output dovrebbe essere simile a quello riportato di seguito. In caso contrario, il servizio potrebbe non essere in esecuzione.

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

Passaggio 5: Controllare lo stato del processo

Per verificare se è in esecuzione un processo Streamer, utilizzare il comando seguente:

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

Il client mostra eventi duplicati

Gestire gli eventi duplicati visualizzati in un client

Il server eStreamer non conserva una cronologia degli eventi inviati, quindi l'applicazione client deve verificare la presenza di eventi duplicati. Gli eventi duplicati possono verificarsi per diversi motivi. Ad esempio, quando si avvia una nuova sessione di streaming, l'ora specificata dal client come punto di inizio per la nuova sessione può avere più messaggi, alcuni dei quali potrebbero essere stati inviati nella sessione precedente e altri no. eStreamer invia tutti i messaggi che soddisfano i criteri di richiesta specificati. Le applicazioni client EStreamer devono essere progettate per rilevare e deduplicare eventuali duplicati risultanti.

Gestisci richieste di dati duplicate

Se si richiedono più versioni degli stessi dati, tramite più contrassegni o più richieste estese, verrà utilizzata la versione più recente. Ad esempio, se eStreamer riceve richieste di flag per gli eventi di rilevamento versione 1 e 6 e una richiesta estesa per la versione 3, invia la versione 6.

Il client mostra un ID regola snort (SID) non corretto

Questo in genere si verifica a causa di un conflitto SID quando una regola viene importata nel sistema, il SID viene mappato nuovamente internamente.

Per utilizzare il SID immesso, anziché quello mappato nuovamente, è necessario abilitare l'*intestazione estesa*. Il bit 23 richiede intestazioni di eventi estesi. Se questo campo è impostato su 0, gli eventi vengono inviati con un'intestazione di evento standard che include solo il tipo di record e la lunghezza del record.

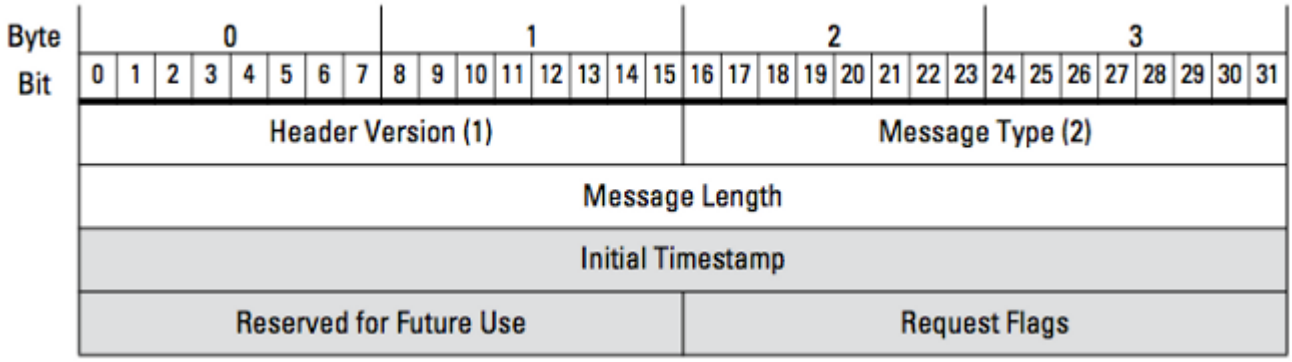


Figura: Il diagramma mostra il formato del messaggio utilizzato per richiedere i dati a eStreamer. I campi specifici del formato del messaggio di richiesta sono evidenziati in grigio.

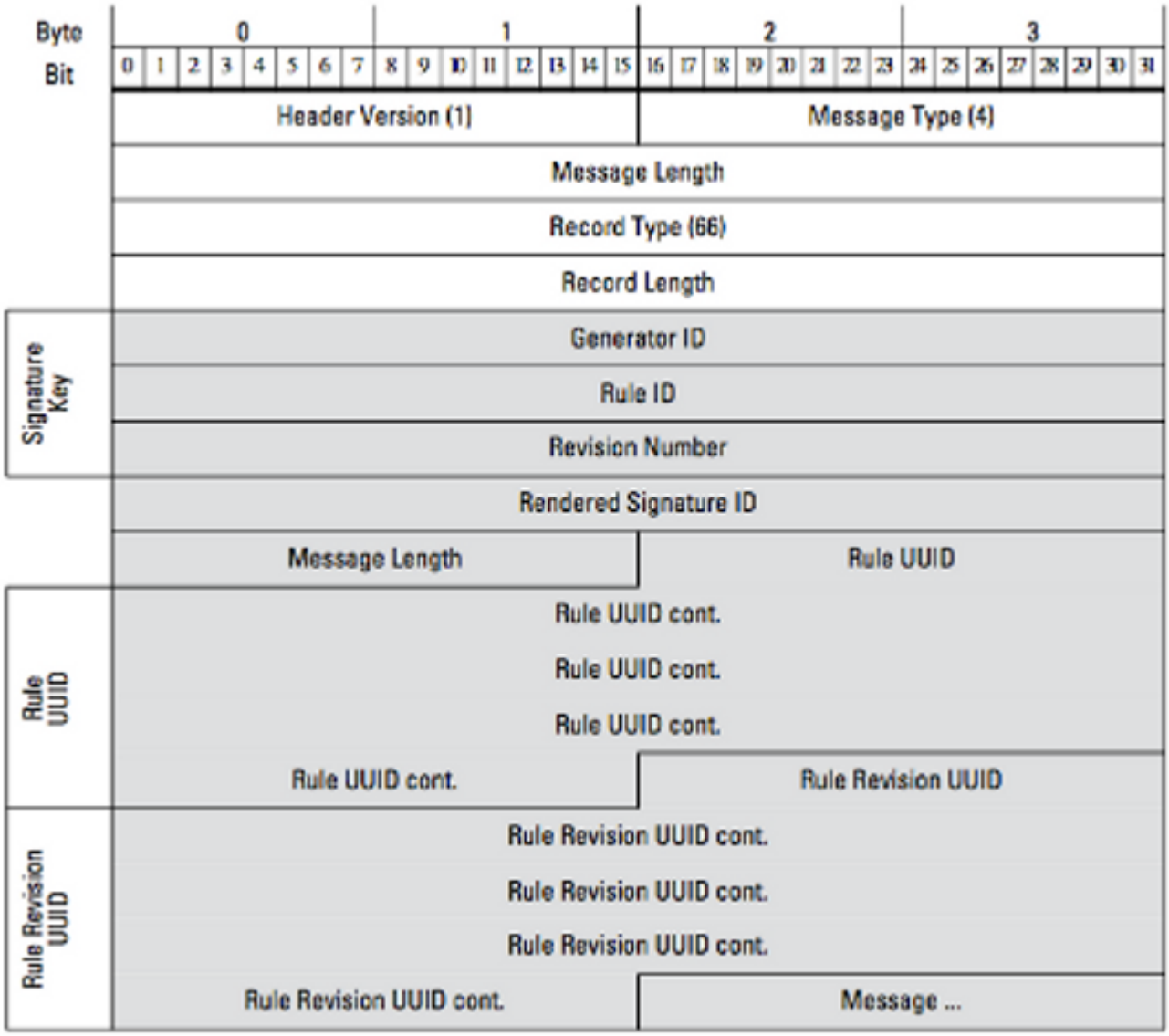


Figura: Nel diagramma viene illustrato il formato delle informazioni relative ai messaggi di regola per un evento trasmesso all'interno di un record Messaggio regola. Vengono visualizzati il ***RuleID*** *(attualmente in uso) e il* ***Signature ID restituito*** *(ovvero il numero previsto).*

Suggerimento: Per una descrizione dettagliata di ciascun bit e messaggio, consultare la *guida all'integrazione di eStreamer*.

Raccolta e analisi di dati aggiuntivi per la risoluzione dei problemi

Eseguire il test utilizzando lo script ssl_test.pl

Utilizzare lo script ssl_test.pl fornito in *Event Streamer Software Development Kit (SDK)* per identificare il problema. L'SDK è disponibile in un file zip sul sito di supporto. Le istruzioni per lo script sono disponibili nel file README.txt, incluso in tale file zip.

PCAP (Capture Packet)

Acquisire i pacchetti sull'interfaccia di gestione del server eStreamer e analizzarli. Verificare che il traffico non sia bloccato o rifiutato in un punto della rete.

Genera file di risoluzione dei problemi

Se sono state completate le operazioni di risoluzione dei problemi descritte in precedenza e non è ancora possibile determinare il problema, generare un file di risoluzione dei problemi dal centro di gestione FireSIGHT. Fornire tutti gli altri dati per la risoluzione dei problemi al supporto tecnico Cisco per un'ulteriore analisi.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).