Résolution des problèmes entre le système FireSIGHT et le client eStreamer (SIEM)

Contenu

Introduction

Event Streamer (eStreamer) vous permet de diffuser plusieurs types de données d'événements d'un système FireSIGHT vers une application cliente personnalisée. Après avoir créé une application cliente, vous pouvez la connecter à un serveur eStreamer (par exemple, FireSIGHT Management Center), démarrer le service eStreamer et commencer à échanger des données. L'intégration d'eStreamer nécessite une programmation personnalisée, mais vous permet de demander des données spécifiques à une appliance. Ce document décrit comment un client eStreamer communique et comment résoudre un problème avec un client.

Méthode de communication entre le client eStreamer et le serveur

La communication entre un client et le service eStreamer se déroule en quatre étapes principales :

Étape 1 : Le client établit une connexion avec le serveur eStreamer

Tout d'abord, un client établit une connexion avec le serveur eStreamer et la connexion est authentifiée par les deux parties. Avant qu'un client puisse demander des données à eStreamer, il doit établir une connexion TCP SSL avec le service eStreamer. Lorsque le client initie la connexion, le serveur eStreamer répond et initie une connexion SSL avec le client. Dans le cadre de la connexion SSL, le serveur eStreamer demande le certificat d'authentification du client et vérifie que le certificat est valide.

Une fois la session SSL établie, le serveur eStreamer effectue une vérification supplémentaire du certificat après la connexion. Une fois la vérification post-connexion terminée, le serveur eStreamer attend une demande de données du client.

Étape 2 : Le client demande des données au service eStreamer

Dans cette étape, le client demande des données au service eStreamer et spécifie les types de données à diffuser. Un message de demande d'événement unique peut spécifier n'importe quelle combinaison de données d'événement disponibles, y compris des métadonnées d'événement. Une demande de profil d'hôte unique peut spécifier un ou plusieurs hôtes. Deux modes de requête sont disponibles pour la requête de données d'événement et deux-points ;

- **Demande de flux d'événements :** Le client envoie un message contenant des indicateurs de demande qui spécifient les types d'événements requis et la version de chaque type, et le serveur eStreamer répond en diffusant les données demandées.
- **Demande étendue :** Le client soumet une demande avec le même format de message que pour les demandes Event Stream, mais définit un indicateur pour une demande étendue. Ceci déclenche une interaction de message entre le client et le serveur eStreamer par le biais de laquelle le client demande des informations supplémentaires et des combinaisons de versions non disponibles via les demandes Event Stream.

Étape 3 : eStreamer établit le flux de données demandé

Àcette étape, eStreamer établit le flux de données demandé au client. Pendant les périodes d'inactivité, eStreamer envoie régulièrement des messages nuls au client pour maintenir la connexion ouverte. S'il reçoit un message d'erreur du client ou d'un hôte intermédiaire, il ferme la connexion.

Étape 4 : La Connexion Se Termine

Le serveur eStreamer peut également fermer une connexion client pour les raisons suivantes :

- L'envoi d'un message génère une erreur. Cela inclut les messages de données d'événements et le message de maintien de connexion nul qu'eStreamer envoie pendant les périodes d'inactivité.
- Une erreur se produit lors du traitement d'une requête client.
- L'authentification du client échoue (aucun message d'erreur n'est envoyé).
- Arrêt du service eStreamer (aucun message d'erreur n'est envoyé).

Le client n'affiche aucun événement

Si vous ne voyez aucun événement sur votre application cliente eStreamer, suivez les étapes ci-dessous pour résoudre ce problème :

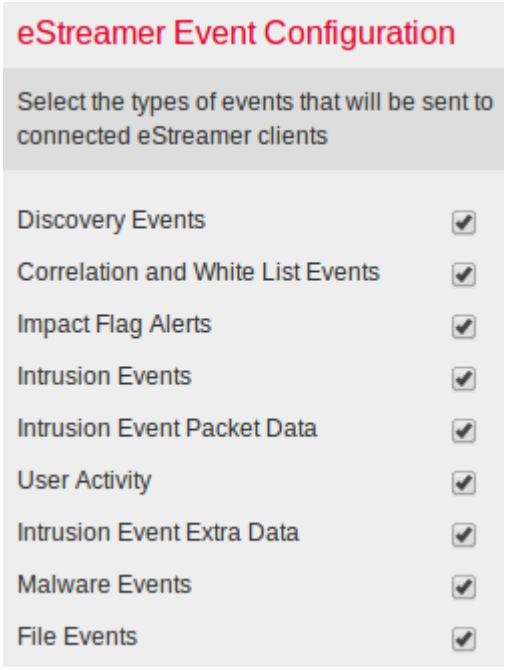
Étape 1 : Vérifier la configuration

Vous pouvez contrôler les types d'événements que le serveur eStreamer peut transmettre aux applications clientes qui en font la demande. Pour configurer les types d'événements transmis par eStreamer, procédez comme suit :

1. Accédez à **System > Local > Registration**.

2. Cliquez sur l'onglet **eStreamer**.

3. Dans le menu **Configuration des événements eStreamer**, cochez les cases en regard des types d'événements que vous souhaitez qu'eStreamer envoie aux clients demandeurs.



> **Note**: Assurez-vous que votre application cliente demande les types d'événements qu'elle doit recevoir. Le message de demande doit être envoyé au serveur eStreamer (FireSIGHT Management Center ou périphérique géré).

4. Cliquez sur **Enregistrer**.

Étape 2 : Vérification du certificat

Assurez-vous que les certificats requis sont ajoutés. Pour qu'eStreamer puisse envoyer des événements eStreamer à un client, celui-ci doit être ajouté à la base de données des homologues du serveur eStreamer à l'aide de la page de configuration eStreamer. Le certificat d'authentification généré par le serveur eStreamer doit également être copié sur le client.

Étape 3 : Vérifiez les messages d'erreur

Identifiez toute erreur évidente liée à eStreamer dans /var/log/messages en utilisant la commande suivante :

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

Étape 4 : Vérifier la connexion

Vérifiez que le serveur accepte les connexions entrantes.

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

Le résultat doit ressembler à celui-ci. Si ce n'est pas le cas, il se peut que le service ne fonctionne pas.

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

Étape 5 : Vérifier l'état du processus

Pour vérifier si un processus sfestreamer est en cours d'exécution, utilisez la commande suivante :

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

Le client affiche les événements dupliqués

Gérer les événements en double affichés dans un client

Le serveur eStreamer ne conserve pas d'historique des événements qu'il envoie ; l'application cliente doit donc rechercher les événements en double. Des événements en double peuvent se produire pour diverses raisons. Par exemple, lors du démarrage d'une nouvelle session de diffusion en continu, l'heure spécifiée par le client comme point de départ de la nouvelle session peut comporter plusieurs messages, dont certains peuvent avoir été envoyés lors de la session précédente et d'autres non. eStreamer envoie tous les messages qui répondent aux critères de demande spécifiés. Les applications clientes EStreamer doivent être conçues pour détecter et supprimer les doublons éventuels.

Gérer les demandes de données en double

Si vous demandez plusieurs versions des mêmes données, soit par plusieurs indicateurs, soit par plusieurs demandes étendues, la version la plus élevée est utilisée. Par exemple, si eStreamer reçoit des demandes d'indicateur pour les événements de détection version 1 et 6 et une demande étendue pour la version 3, il envoie la version 6.

Le client affiche un ID de règle de sniff (SID) incorrect

Cela se produit généralement en raison d'un conflit de SID lorsqu'une règle est importée dans le système, le SID est remappé en interne.

Pour utiliser le SID que vous avez saisi, plutôt que le SID remappé, vous devez activer l'*en-tête étendu*. Le bit 23 demande des en-têtes d'événements étendus. Si ce champ est défini sur 0, les événements sont envoyés avec un en-tête d'événement standard qui inclut uniquement le type et la longueur de l'enregistrement.

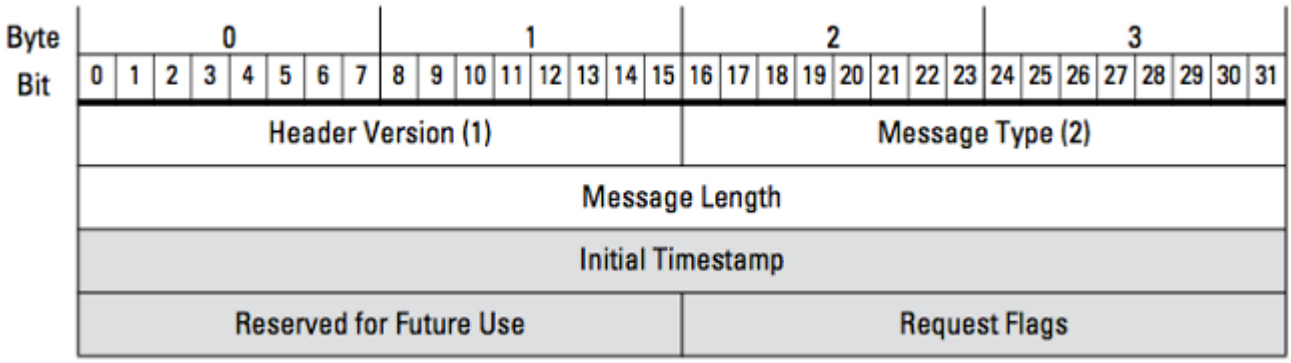


Figure : Le schéma illustre le format de message utilisé pour demander des données à eStreamer. Les champs spécifiques au format du message de demande sont mis en surbrillance en gris.

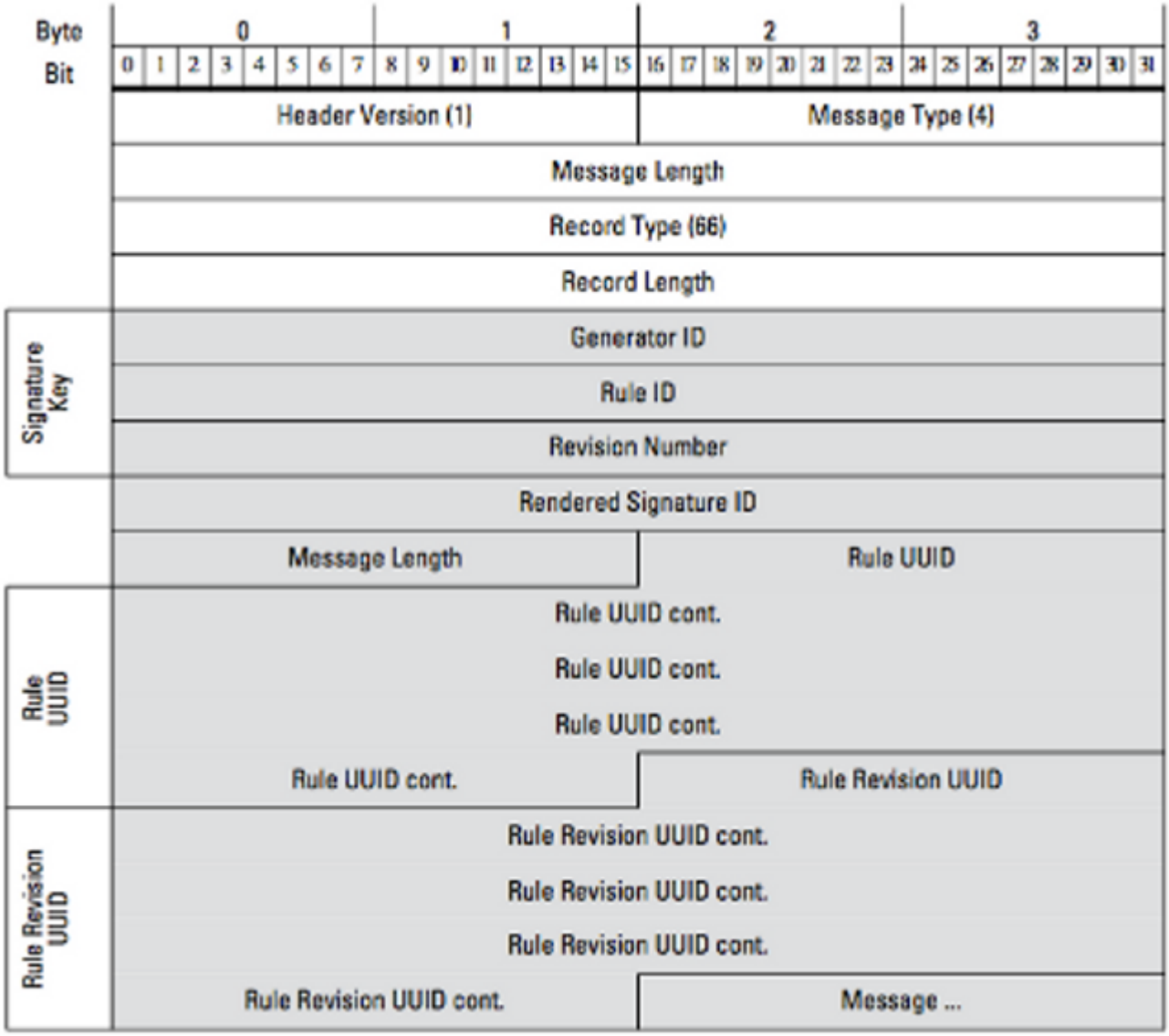


*Figure : Le schéma illustre le format des informations de message de règle pour un événement transmis dans un enregistrement de message de règle. Il affiche l'**ID de règle** (que vous utilisez actuellement) et l'ID de **signature rendue** (qui est le nombre que vous attendez).*

Astuce : Afin de trouver la description détaillée de chaque bit et message, lisez le *Guide d'intégration d'eStreamer*.

Collecte et analyse de données de dépannage supplémentaires

Test à l'aide du script ssl_test.pl

Utilisez le script ssl_test.pl fourni dans le *kit de développement logiciel (SDK) Event Streamer* pour identifier le problème. Le SDK est disponible dans un fichier zip sur le site de support. Les instructions pour le script sont disponibles dans le fichier README.txt, qui est inclus dans ce fichier zip.

PCAP (Capture Packet)

Capturez les paquets sur l'interface de gestion du serveur eStreamer et analysez-les. Vérifiez que le trafic n'est pas bloqué ou refusé quelque part sur votre réseau.

Générer un fichier de dépannage

Si vous avez effectué les étapes de dépannage ci-dessus et que vous n'êtes toujours pas en mesure de déterminer le problème, générez un fichier de dépannage à partir de votre FireSIGHT Management Center. Fournir toutes les données de dépannage supplémentaires à l'assistance technique Cisco pour une analyse plus approfondie.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.