Dépannez les questions entre le système de FireSIGHT et le client d'eStreamer (SIEM)

Contenu

Introduction

La flamme d'événement (eStreamer) te permet pour couler plusieurs genres de données d'événement d'un système de FireSIGHT à une application cliente conçue en fonction du client. Après que vous créiez une application cliente, vous pouvez la connecter à un serveur d'eStreamer (par exemple, un centre de Gestion de FireSIGHT), commencez le service d'eStreamer, et commencez des données permutantes. l'intégration d'eStreamer exige la programmation personnalisée, mais te permet pour demander des données spécifiques d'une appliance. Ce document décrit comment un client d'eStreamer communique et comment dépanner une question avec un client.

Moyen de communication entre le client et serveur d'eStreamer

Il y a quatre étapes importantes de transmission qui se produisent entre un client et le service d'eStreamer :

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

D'abord, un client établit une connexion avec le serveur d'eStreamer et la connexion est authentifiée par les deux interlocuteurs. Avant qu'un client puisse demander des données d'eStreamer, le client doit initier une connexion TCP SSL-activée avec le service d'eStreamer. Quand le client initie la connexion, le serveur d'eStreamer répond, initiant une prise de contact SSL avec le client. En tant qu'élément de la prise de contact SSL, le serveur d'eStreamer demande le certificat de l'authentification de client, et le vérifie que le certificat est valide.

Après que la session SSL soit établie, le serveur d'eStreamer exécute une vérification supplémentaire de POST-connexion du certificat. Après que la vérification de POST-connexion soit de finition, le serveur d'eStreamer attend une demande de données du client.

Étape 2 : Le client demande des données du service d'eStreamer

Dans cette étape, le client demande des données du service d'eStreamer et spécifie les types de données à couler. Un message simple de demande d'événement peut spécifier n'importe quelle combinaison des données d'événement disponibles, y compris des métadonnées d'événement. Une demande de profil de seul hôte peut spécifier un seul hôte ou des hôtes de multiple. Deux modes de demande sont disponibles pour demander le data&colon d'événement ;

- **Demande de flot d'événement :** Le client soumet un message contenant les indicateurs de demande qui spécifient les types d'événement et la version demandés de chaque type, et le serveur d'eStreamer répond en coulant les données priées.
- **Demande étendue :** Le client soumet une demande avec le même format de message que pour des demandes de flot d'événement mais place un indicateur pour une demande étendue. Ceci initie une interaction de message entre le client et le serveur d'eStreamer par lequel le client demande des combinaisons des informations complémentaires et de version non disponibles par l'intermédiaire du flot d'événement demande.

Étape 3 : l'eStreamer établit le flux de données demandé

Dans cette étape, l'eStreamer établit le flux de données demandé au client. Au cours des périodes d'inactivité, l'eStreamer envoie les messages nuls périodiques 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 d'eStreamer peut également fermer une connexion client pour les raisons suivantes :

- N'importe quand l'envoi d'un message a comme conséquence une erreur. Ceci inclut les deux messages de données d'événement et l'eStreamer nul de message de keep-alive envoie au cours des périodes d'inactivité.
- Une erreur se produit tout en traitant une demande de client.
- L'authentification client échoue (aucun message d'erreur n'est envoyé).
- le service d'eStreamer s'arrête (aucun message d'erreur n'est envoyé).

Le client n'affiche aucun événement

Si vous ne voyez aucun événement sur votre application cliente d'eStreamer, suivez s'il vous plaît les étapes ci-dessous pour dépanner cette question :

Étape 1 : Vérifier la configuration

Vous pouvez contrôler que les types d'événements le serveur d'eStreamer peut transmettre aux applications cliente qui les demandent. Pour configurer les types d'événements transmis par l'eStreamer suivez les étapes ci-dessous :

1. Naviguez vers le **système > les gens du pays > l'enregistrement**.

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

3. Sous le menu de **configuration d'événement d'eStreamer**, sélectionnez les cases à côté des types d'événements que vous voulez que l'eStreamer envoie à demander des clients.

> Remarque: Assurez-vous votre application cliente demande les types d'événements que vous voulez qu'ils reçoivent. Le message de demande doit être envoyé au serveur d'eStreamer (centre ou périphérique géré de Gestion de FireSIGHT).

4. Cliquez sur **Save**.

Étape 2 : Vérifiez le certificat

Assurez-vous que les Certificats exigés sont ajoutés. Avant que l'eStreamer puisse envoyer des événements d'eStreamer à un client, le client doit être ajouté à la base de données des pairs du serveur d'eStreamer utilisant la page de configuration d'eStreamer. Le certificat d'authentification généré par le serveur d'eStreamer doit également être copié sur le client.

Étape 3 : Messages d'erreur de contrôle

Identifiez toutes les erreurs associées par eStreamer évident dans `/var/log/messages` à l'aide de la commande suivante :

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

Étape 4 : Vérifiez la connexion

Vérifiez que le serveur reçoit les connexions entrantes.

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

La sortie devrait ressembler à ci-dessous. Sinon, alors le service peut ne pas s'exécuter.

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

Étape 5 : Vérifiez le statut du processus

Pour vérifier s'il y a un processus exécuté de `sfestreamer`, utilisez s'il vous plaît la commande suivante :

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

Événements en double d'expositions de client

Événements en double de traitement affichés dans un client

Le serveur d'eStreamer ne garde pas un historique des événements qu'il envoie, ainsi l'application cliente doit vérifier des événements en double. Les événements en double peuvent se produire pour des raisons diverses. Par exemple, en commençant une nouvelle session coulante, le moment spécifié par le client comme point commençant pour la nouvelle session peut avoir de plusieurs messages, certains dont peut avoir été introduit la session précédente et certains dont n'étaient pas. l'eStreamer envoie tous les messages qui répondent aux critères spécifiés de demande. Des applications cliente d'EStreamer devraient être conçues pour les détecter et De-doublon tous les doublons en résultant.

Gérez les demandes en double des données

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

Les expositions de client incorrectes reniflent l'ID de règle (le SID)

Ceci se produit habituellement en raison d'un conflit SID quand une règle est importée dans le système, le SID re-est tracé intérieurement.

Pour utiliser le SID que vous avez écrit, plutôt que le SID re-tracé, vous doivent activer l'*en-tête étendue*. Mordu 23 en-têtes étendues d'événement de demandes. Si ce champ est placé à 0, des événements sont envoyés avec une en-tête standard d'événement qui inclut seulement le type d'enregistrement et la longueur de l'enregistrement.

Figure : Le diagramme montre le format de message utilisé pour demander des données d'eStreamer. Des champs spécifiques au format de message de demande sont mis en valeur dans le gris.

*Figure : Le diagramme montrent le format des informations de message de règle pour un événement qui est transmis dans un enregistrement de message de règle. Il affiche le **RuleID** (ce que vous utilisez maintenant) et l'**ID rendu de signature** (ce qui est le nombre que vous prévoyez).*

> **Conseil** : Afin de trouver la description de détail de chaque bit et message, lisez le *guide d'intégration d'eStreamer*.

Collectez et analysez supplémentaire dépannent des données

Test utilisant le script ssl_test.pl

Utilisez le `script ssl_test.pl` fourni dans le *kit de développement logiciel d'*EventStreamer *(SDK)* pour identifier le problème. Le SDK est disponible dans un fichier zip sur le site du support technique. Les instructions pour le script est disponible dans README.txt, `qui` est inclus dans ce fichier zip.

Paquet de capture (PCAP)

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

Produisez-vous dépannent le fichier

Si vous vous terminiez les étapes de dépannage ci-dessus, et vous ne pouvez pas encore déterminer le problème, générez s'il vous plaît un fichier de dépannage de votre centre de Gestion

de FireSIGHT. Fournissez tout les supplémentaire dépannent des données au support technique de Cisco pour l'analyse approfondie.