Comment exporter de grandes quantités de données à l'aide de la recherche CLI.

Applicabilité

Splunk Enterprise

Description

Guide pas à pas

Pour exporter de grandes quantités de données, vous pouvez effectuer une recherche en suivant les lignes suivantes à partir de l'invite CLI d'un en-tête de recherche :

```
splunk search "index=pan_log sourcetype=pan:* src_ip!=<Internal_IP_Scheme> dest_ip!=<Int
| fillnull value=null
| dump basefilename=<insert_your_chosenfilename> compress=5 fields=_time,app,app:subcate
dest_ip,dest_port,dest_translated_ip,dest_user,dest_zone,direction,duration,filename,htt
packets_out,sig,signature,sourcetype,src_ip,src_translated_ip,src_user,target_id,threat:
```

La répartition de la recherche ci-dessus est la suivante :

Recherche de pan : * types de source dans l'index 'pan_log' et exclusion d'une plage IP, capable de remplir des zéros et de diriger vers une commande dump, qui procède ensuite comme suit :

Cette commande exécute une requête de recherche spécifiée et un résultat de recherche d'exportation de cliché vers le disque local à l'adresse "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump". Il reconnaît un champ spécial dans les événements d'entrée, _dstpath, qui, s'il est défini, sera utilisé comme chemin à ajouter à dst pour calculer le chemin de destination final.

L'inconvénient majeur de ce processus est que les résultats ont un TTL de 2 minutes, donc vous DEVEZ créer un fichier de jeton de sauvegarde pour vous assurer que ces résultats ne sont pas récoltés avant de pouvoir récupérer les fichiers *.gz qui sont créés par le processus. Voir le lien « ASSOCIÉ » ci-dessous.

PRODUITS CONNEXES :

Comment créer un fichier sans extension dans Windows

Enquête

Lors de l'enquête sur ce problème, il a été détecté, ne pas obtenir l'ensemble complet des données.

Déterminez que la recherche est due à la collecte de ces données et à leur élimination plus rapide que prévu - effectué. J'ai trouvé que c'était un comportement normal après la recherche. Les recherches d'index récapitulatives et autres peuvent s'exécuter avec un TTL d'artefact de recherche de 2 minutes. Pour cette raison, créez un fichier de jeton de sauvegarde dans le répertoire <sid>. Ce sujet est traité pour les machines Windows dans le lien dans la section de description de cet article. Avec *nix, vous accédez à $SPLUNK_HOME/var/run/splunk/dispatch/<sid> et vous émettez la commande « touch save »

Une fois que cela a été réalisé ont été en mesure de contourner le problème de récolte d'artefacts [***N'OUBLIEZ PAS DE SUPPRIMER LES FICHIERS DE SAUVEGARDE !***]

Après cela, appuyez sur un peu plus de dépannage pour obtenir un délai pratique qui générerait un ensemble complet défini de données. En raison de la quantité extrême d'événements dans l'ensemble de données, il a fallu 24 heures de recherche pour effectuer une exportation jour par jour.

Résolution

Une fois réduit dans le jeu de données devant être exécuté sur une période de 24 heures, capable de générer des vidages complets de 24 heures de journalisation PAN. Une autre EST a pu utiliser cette même méthode récemment pour revenir à l'histoire et saisir des données spécifiques.

Liens connexes

Documentation sur le Splunk : Manuel des commandes de vidage : Vidage des références de recherche

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.