Exportieren großer Datenmengen mit der CLI-Suche

Geltungsbereich

Splunk Enterprise

Beschreibung

Schritt-für-Schritt-Anleitung

Um große Datenmengen zu exportieren, können Sie in der CLI-Eingabeaufforderung eines Suchkopfs eine Suche nach folgenden Kriterien durchführen:

```
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:
```

Die obige Suche gliedert sich wie folgt auf:

Durchsuchen des Index "pan_log" nach pan:*-Quelltypen und Ausschließen eines IP-Bereichs, der NULL-Werte ausfüllen kann, und Weiterleiten an einen Dump-Befehl, der dann folgende Schritte ausführt:

Mit diesem Befehl wird eine angegebene Suchanfrage und ein Hot-Export-Suchergebnis für die lokale Festplatte unter "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump" ausgeführt. Es erkennt ein spezielles Feld in den Eingabeereignissen, _dstpath, das, wenn gesetzt, als Pfad verwendet wird, der an dst angehängt wird, um den endgültigen Zielpfad zu berechnen.

Der eine große Nachteil dieses Prozesses ist, dass die Ergebnisse eine TTL von 2 Minuten haben, so MÜSSEN Sie eine gespeicherte Token-Datei erstellen, um sicherzustellen, dass diese Ergebnisse nicht geerntet werden, bevor Sie die *.gz-Dateien greifen können, die durch den Prozess erstellt werden. Siehe unten den Link "RELATED".

ÄHNLICH:

[So erstellen Sie eine Datei ohne Erweiterung in Windows]

Untersuchung

Während der Untersuchung dieses Problems wurde es gefunden, nicht den vollständigen Datensatz erhalten.

Festgestellt, dass es darauf zurückzuführen ist, dass die Suche diese Daten erfasst und schneller als erwartet entfernt hat. Dies hat sich nach der Recherche als normales Verhalten herausgestellt. Die Suche nach einem zusammenfassenden Index und andere können mit einem 2-minütigen Artefakt-TTL für die Suche ausgeführt werden. Erstellen Sie daher eine Speichertokendatei im Verzeichnis <sid>. Dies wird für Windows-Computer unter dem Link im Beschreibungsabschnitt dieses Artikels behandelt. Mit *nix navigieren Sie zu $SPLUNK_HOME/var/run/splunk/dispatch/<sid> und geben dann den Befehl 'touch save' aus.

Sobald dies erreicht wurde, waren in der Lage, die Artefakternte Problem umgehen [***VERGESSEN SIE NICHT, DIE SPEICHERN DATEIEN!***]

Danach sollten Sie noch einige Schritte zur Fehlerbehebung durchführen, um einen ausführlichen Zeitrahmen zu erhalten, in dem alle Daten definiert sind. 24-Stunden-Läufe der Suche, um es an einem Tag durch den Tag Export zu vervollständigen waren am Ende aufgrund der extremen Anzahl von Ereignissen in dem Datensatz notwendig.

Auflösung

Sobald der Datensatz eingeengt wurde, muss er für einen Zeitraum von 24 Stunden ausgeführt werden und kann vollständige Dumps von 24 Stunden PAN-Protokollierung generieren. Ein anderer TSE-Erreger konnte diese Methode in letzter Zeit nutzen, um historisch zurückzublicken und sich einen spezifischen Erreger zu suchen.

Verwandte Links

Splunk-Dokumentation: Dump-Befehlshandbuch: [Suchverweis-Dump]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.