# Hoe grote hoeveelheden gegevens te exporteren met CLI Search.

## toepasbaarheid

Splunk Enterprise

## Beschrijving

## Stapsgewijze handleiding

Als u grote hoeveelheden gegevens wilt exporteren, kunt u een zoekopdracht in de volgende zin gebruiken vanuit de CLI-prompt op een zoekkop:

```
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:
```

De uitsplitsing van de bovenstaande zoekopdracht is als volgt:

Zoeken in de 'pan_log' index voor pan:* source types en het uitsluiten van een IP range, in staat om nulls te vullen, en pipe naar een dump commando, die vervolgens het volgende doet:

Met deze opdracht wordt een opgegeven zoekopdracht uitgevoerd en wordt het zoekresultaat van één shot geëxporteerd naar een lokale schijf op "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump". Het herkent een speciaal veld in de invoergebeurtenissen, _dstpath, dat als set wordt gebruikt als een pad dat moet worden toegevoegd aan dst om het uiteindelijke bestemmingspad te berekenen.

Het enige grote nadeel van dit proces is dat de resultaten een TTL van 2 minuten hebben, dus u MOET een opslagtokenbestand maken om ervoor te zorgen dat deze resultaten niet worden geoogst voordat u de *.gz-bestanden kunt pakken die door het proces zijn gemaakt. Zie de link "GERELATEERD" hieronder.

GERELATEERD:

Hoe maak je een bestand zonder extensie in Windows

## onderzoek

Tijdens het onderzoeken van dit probleem werd het gevonden, niet het krijgen van volledige dataset.

Vastgesteld dat het te wijten was aan zoekresultaten die deze gegevens vastpakten en sneller dan verwacht werden geruimd. Dit bleek normaal gedrag na onderzoek. Samenvatting index zoekopdrachten en anderen kunnen worden uitgevoerd met een 2 minuten zoekartefact TTL. Maak daarom een opslagtokenbestand in de <sid>-directory. Dit wordt behandeld voor Windows-machines in de link in de beschrijvingssectie van dit artikel. Met *nix navigeer je naar $SPLUNK_HOME/var/run/splunk/dispatch/<sid> en geef je vervolgens de opdracht 'touch save' uit

Zodra dat is bereikt, konden we het probleem van het oogsten van artefacten omzeilen [*** VERGEET NIET OM DE BEWAARBESTANDEN TE VERWIJDEREN! ***]

Druk daarna op een beetje meer probleemoplossing om een werkbaar tijdsbestek te krijgen dat een gedefinieerde volledige set gegevens zou genereren. 24-uurs runs van de zoekopdracht om het op een dag te voltooien, waren uiteindelijk nodig vanwege de extreme hoeveelheid gebeurtenissen in de dataset.

## resolutie

Eenmaal ingeperkt op de dataset die moet worden uitgevoerd tegen een periode van 24 uur, kunnen volledige stortplaatsen van 24 uur worden gegenereerd. Een andere TSE is in staat geweest om deze zelfde methode onlangs te gebruiken om historisch terug te gaan en specifiek te grijpen.

## Gerelateerde links

Splunk-documentatie: Dump Command Manual: Zoekreferentie Dump

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.