Come esportare grandi quantità di dati utilizzando la ricerca CLI.

Applicabilità

Splunk Enterprise

Descrizione

Guida dettagliata

Per esportare grandi quantità di dati, è possibile utilizzare una ricerca dal prompt della CLI su un'intestazione di ricerca seguendo le istruzioni riportate di seguito:

```
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 suddivisione della ricerca di cui sopra è la seguente:

Cercando nell'indice 'pan_log' pan:* sourcetypes e escludendo un intervallo IP, è possibile riempire i valori nulli e reindirizzare a un comando dump, che procede quindi come segue:

Questo comando esegue una query di ricerca specificata ed esporta un risultato di ricerca sul disco locale in "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump". Riconosce un campo speciale negli eventi di input, _dstpath, che se impostato verrà utilizzato come percorso da aggiungere a dst per calcolare il percorso di destinazione finale.

Uno dei principali inconvenienti di questo processo è che i risultati hanno un TTL di 2 minuti, quindi È NECESSARIO creare un file token di salvataggio per assicurarsi che questi risultati non vengano raccolti prima di poter recuperare i file *.gz creati dal processo. Vedere il link "ARGOMENTI CORRELATI" riportato di seguito.

ARGOMENTI CORRELATI:

Come creare un file senza estensione in Windows

Indagine

Durante l'analisi di questo problema, è stato riscontrato che non riceveva il set di dati completo.

Determinato che è dovuto a ricerca raccogliere questi dati e sopprimere più velocemente del previsto. Ho scoperto che questo è un comportamento normale dopo la ricerca. Le ricerche nell'indice di riepilogo e altre possono essere eseguite con un TTL di ricerca di 2 minuti. Per questo motivo, creare un file token di salvataggio nella directory <sid>. Per i computer Windows, vedere il collegamento nella sezione di descrizione di questo articolo. Con *nix è possibile passare a $SPLUNK_HOME/var/run/splunk/dispatch/<sid> e quindi eseguire il comando 'touch save'

Una volta raggiunto questo obiettivo, è stato possibile evitare il problema di registrazione degli artefatti [***NON DIMENTICARE DI ELIMINARE I FILE SALVATI!***]

Dopo questo, premere attraverso un po 'più di risoluzione dei problemi per ottenere un periodo di tempo fattibile che genererebbe un set completo definito di dati. 24 ore di esecuzione della ricerca per completarlo un giorno per giorno esportazione sono stati necessari alla fine a causa della quantità estrema di eventi nel set di dati.

Risoluzione

Una volta ristretto nel set di dati che deve essere eseguito in un periodo di 24 ore, in grado di generare dump completi di 24 ore di registrazioni PAN. Un'altra TSE è riuscita ad utilizzare lo stesso metodo recentemente per tornare indietro nel tempo e diventare specifica.

Collegamenti correlati

Documentazione Splunk: Manuale del comando dump: Dump riferimenti di ricerca

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).