如何使用CLI搜尋匯出大量資料。

適用性

Splunk企業版

說明

逐步指南

要匯出大量資料，可以在搜尋頭上的CLI提示符下按以下順序進行搜尋：

```
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:
```

上述搜尋細目如下：

搜尋pan:* sourcetypes的「pan_log」索引並排除IP範圍，能夠填充空值，然後通過dump命令生成管道，然後繼續執行以下操作：

此命令運行指定的搜尋查詢，並只將搜尋結果匯出到本地磁碟，該磁碟位於「$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump」。 它識別輸入事件中的特殊欄位_dstpath，如果設定了此欄位，則該欄位將用作新增到dst的路徑，以計算最終目標路徑。

此過程的一個主要缺點是結果的TTL為2分鐘，因此必須建立儲存令牌檔案以確保在獲取由過程建立的*.gz檔案之前不會收到這些結果。請參閱下面的「相關」連結。

相關：

如何在Windows中建立無副檔名的檔案

調查

調查此問題時，發現它沒有獲取完整的資料集。

已確定這是由於搜尋功能獲取這些資料，並以比預期更快的速度進行剔除。經研究發現這是正常行為。摘要索引搜尋和其他搜尋可以使用2分鐘的搜尋專案TTL運行。因此，請在<sid>目錄中建立儲存令牌檔案。對於本文說明部分中的連結中的Windows電腦，將對此進行說明。使用*nix可以導航到$SPLUNK_HOME/var/run/splunk/dispatch/<sid>，然後發出命令「touch save」

完成此操作後，就可以繞過對象回收問題[***不要忘記刪除儲存檔案!***]

然後，再進行更多故障排除，獲得可生成已定義的完整資料集的可用時間範圍。由於資料集中的事件數量極大，最終需要進行24小時的搜尋以逐日完成匯出。

解析

一旦縮小到需要針對24小時時間段運行的資料集，能夠生成24小時延期的完全轉儲PAN日誌記錄。另一家TSE最近也使用同樣的方法來追溯歷史並獲取特定資訊。

相關連結

Splunk文檔：Dump命令手冊： 搜尋引用轉儲

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。