Cómo Exportar Grandes Cantidades de Datos Usando la Búsqueda CLI.

Aplicabilidad

Splunk Enterprise

Descripción

Guía paso a paso

Para exportar grandes cantidades de datos, puede utilizar una búsqueda de las siguientes líneas desde el indicador de comandos de CLI en un encabezado de búsqueda:

```
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:
```

El desglose de la búsqueda anterior es el siguiente:

Buscando el índice 'pan_log' para los tipos de fuente pan:* y descartando un rango de IP, capaz de llenar valores nulos, y canalizar a un comando dump, que luego procede a hacer lo siguiente:

Este comando ejecuta una consulta de búsqueda especificada y un resultado de la búsqueda de exportación de una captura al disco local en "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump". Reconoce un campo especial en los eventos de entrada, _dstpath, que si se establece se utilizará como ruta que se anexará a dst para calcular la ruta de destino final.

El principal inconveniente de este proceso es que los resultados tienen un TTL de 2 minutos, por lo que DEBE crear un archivo de token guardado para asegurarse de que estos resultados no se cosechan antes de poder tomar los archivos *.gz que se crean en el proceso. Consulte el enlace "RELACIONADO" que aparece a continuación.

RELACIONADO:

Cómo crear un archivo sin extensión en Windows

Investigación

Mientras investigaba este problema, se detectó que no se obtenía el conjunto de datos completo.

Determinó que se debía a una búsqueda que recogía estos datos y los extraía más rápido de lo esperado. Encontré que esto es un comportamiento normal después de la investigación. Las búsquedas de índice de resumen y otras se pueden ejecutar con un artefacto de búsqueda de 2 minutos TTL. Debido a esto, cree un archivo de token guardado en el directorio <sid>. Esto se trata en el caso de los equipos con Windows en el vínculo de la sección de descripción de este artículo. Con *nix, navegue hasta $SPLUNK_HOME/var/run/splunk/dispatch/<sid> y luego ejecute el comando 'touch save'

Una vez que se logró, fueron capaces de evitar el problema de la cosecha de artefactos [***NO SE OLVIDE DE ELIMINAR LOS ARCHIVOS GUARDADOS!***]

Después de esto, presione un poco más de troubleshooting para obtener un marco de tiempo factible que generaría un conjunto completo definido de datos. Las ejecuciones de 24 horas de la búsqueda para completarla en una exportación día a día fueron necesarias al final debido a la cantidad extrema de eventos en el conjunto de datos.

Resolución

Una vez reducido en el conjunto de datos que debe ejecutarse en un período de 24 horas, puede generar volcados completos de tramos de 24 horas de registro PAN. Otro TSE ha sido capaz de utilizar este mismo método recientemente para volver históricamente y agarrar específico.

Enlaces relacionados

Documentación de Splunk: Manual de comando de volcado: Buscar volcado de referencia

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).