Como exportar grandes quantidades de dados usando a pesquisa CLI.

Aplicabilidade

Empresa Splunk

Descrição

Guia passo a passo

Para exportar grandes quantidades de dados, você pode usar uma pesquisa nas linhas a seguir a partir do prompt CLI em um cabeçalho de pesquisa:

```
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:
```

A análise da pesquisa acima é a seguinte:

Pesquisando o índice 'pan_log' para tipos de origem pan:* e descartando um intervalo IP, capaz de preencher nulos e enviar para um comando dump, que, em seguida, continua fazendo o seguinte:

Este comando executa uma consulta de pesquisa especificada e um resultado de pesquisa de exportação de um host para o disco local em "$SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump". Ele reconhece um campo especial nos eventos de entrada, _dstpath, que, se definido, será usado como um caminho a ser anexado ao dst para calcular o caminho de destino final.

A principal desvantagem desse processo é que os resultados têm um TTL de 2 minutos, portanto, você DEVE criar um arquivo de token de salvamento para garantir que esses resultados não sejam coletados antes de poder pegar os arquivos *.gz criados pelo processo. Consulte o link "RELACIONADO" abaixo.

RELACIONADOS:

Como criar um ficheiro sem extensão no Windows

Investigação

Durante a investigação desse problema, ele foi encontrado, não obtendo o conjunto de dados completo.

Determinado que a causa da coleta de dados pela pesquisa foi pegar esses dados e selecioná-los mais rápido do que o esperado. Este comportamento foi considerado normal após a pesquisa. As pesquisas de índice resumidas e outras podem ser executadas com um TTL de artefato de pesquisa de 2 minutos. Por isso, crie um arquivo de token de salvamento no diretório <sid>. Isso é abordado para máquinas Windows no link na seção de descrição deste artigo. Com o *nix você navega até $SPLUNK_HOME/var/run/splunk/dispatch/<sid> e emite o comando 'touch save'

Uma vez que isso foi alcançado foi capaz de ignorar o problema de colhimento de artefato [***NÃO SE ESQUEÇA DE EXCLUIR OS ARQUIVOS SALVAR!***]

Depois disso, pressione um pouco mais de solução de problemas para obter um cronograma viável que gere um conjunto completo definido de dados. 24 horas de execução da pesquisa para concluí-la em um dia a exportação foram necessárias no final, devido à quantidade extrema de eventos no conjunto de dados.

Resolução

Uma vez restringido no conjunto de dados que precisa ser executado em um período de 24 horas, capaz de gerar dumps completos de trechos de 24 horas de registro PAN. Outra EET tem sido capaz de utilizar este mesmo método recentemente para voltar historicamente e pegar específico.

Links relacionados

Documentação do Splunk: Manual do comando de despejo: Despejo de Referência de Pesquisa

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.