Eventos JSON duplicados.

Aplicabilidade

Empresa Splunk

Investigação

Ao executar o comando btool e procurar os atributos KV_MODE e AUTO_KV_JSON estão definidos como json e true respectivamente:

```
splunk btool props list --debug <my_sourcetype_name>
/opt/splunk/etc/system/default/props.conf                    ADD_EXTRA_TIME_FIELDS = True
/opt/splunk/etc/system/default/props.conf                    ANNOTATE_PUNCT = True
/opt/splunk/etc/system/default/props.conf                    AUTO_KV_JSON = True  <======
/opt/splunk/etc/system/default/props.conf                    BREAK_ONLY_BEFORE =
/opt/splunk/etc/system/default/props.conf                    BREAK_ONLY_BEFORE_DATE = Tru
/opt/splunk/etc/system/default/props.conf                    CHARSET = UTF-8
/opt/splunk/etc/apps/search/local/props.conf                 DATETIME_CONFIG =
/opt/splunk/etc/apps/search/local/props.conf                 INDEXED_EXTRACTIONS = json
```

Resolução

Conforme a documentação:

"Observação: se você definir *`INDEXED_EXTRACTIONS=JSON`*, verifique se você também não definiu *`KV_MODE = json`* para o mesmo tipo de origem, o que extrairia os campos JSON duas vezes, no tempo de indexação e novamente no tempo de pesquisa."

Portanto, você precisa desativar um dos atributos para interromper o problema.

AUTO_KV_JSON (extração de campo de tempo de pesquisa)
INDEXED_EXTRACTION (extração de tempo de índice)

Links relacionados

Respostas de Splunk

Por que meus campos json são extraídos duas vezes?
https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Documentação do Splunk

Atributos Props.conf para dados estruturados
https://docs.splunk.com/Documentation/Splunk/8.0.0/Data/Extractfieldsfromfileswithstructureddata#Props
default.meta.conf

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Defaultmetaconf#default.meta.conf.spec
props.conf.spec https://docs.splunk.com/Documentation/Splunk/8.0.0/Admin/Propsconf

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.