Gedupliceerde JSON-gebeurtenissen.

toepasbaarheid

Splunk Enterprise

onderzoek

Bij het uitvoeren van de btool opdracht en zoeken naar de attributen KV_MODE en AUTO_KV_JSON zijn ingesteld op json en true respectievelijk:

```
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
```

resolutie

Volgens de documentatie:

"Opmerking: Als u *INDEXED_EXTRACTIONS=JSON* instelt, controleert u of u *KV_MODE = json* niet ook voor hetzelfde brontype hebt ingesteld, waardoor de JSON-velden twee keer worden geëxtraheerd, bij index keer op keer op zoektijd."

U moet dus een van de attributen uitschakelen om het probleem te stoppen.

AUTO_KV_JSON (zoektijd-veldextractie)
INDEXED_EXTRACTION (index-time extractie)

Gerelateerde links

Splunk Antwoorden

Waarom worden mijn json velden twee keer geëxtraheerd?
https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Splunk-documentatie

Props.conf-kenmerken voor gestructureerde gegevens
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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.