Événements JSON en double.

Applicabilité

Splunk Enterprise

Enquête

Lors de l'exécution de la commande btool et de la recherche des attributs KV_MODE et AUTO_KV_JSON sont définis sur json et true respectivement :

```
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
```

Résolution

Selon la documentation :

"Remarque : si vous définissez *INDEXED_EXTRACTIONS=JSON*, vérifiez que vous n'avez pas également défini *KV_MODE = json* pour le même type de source, ce qui extrairait les champs JSON deux fois, au moment de l'index et encore au moment de la recherche."

Vous devez donc désactiver l'un des attributs pour arrêter le problème.

AUTO_KV_JSON (extraction du champ de temps de recherche)
INDEXED_EXTRACTION (extraction index-time)

Liens connexes

Réponses Splunk

Pourquoi mes champs json sont-ils extraits deux fois ?
https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Documentation Splunk

Attributs Props.conf pour les données structurées
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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.