Eventi JSON duplicati.

Applicabilità

Splunk Enterprise

Indagine

Quando si esegue il comando btool e si cercano gli attributi KV_MODE e AUTO_KV_JSON, questi ultimi sono impostati rispettivamente su json e true:

```
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
```

Risoluzione

Come da documentazione:

"Nota: se si imposta *INDEXED_EXTRACTIONS=JSON*, verificare di non aver impostato anche *KV_MODE = json* per lo stesso tipo di origine, che estrarrebbe i campi JSON due volte, all'ora dell'indice e di nuovo al momento della ricerca."

Quindi, è necessario disabilitare uno degli attributi per fermare il problema.

AUTO_KV_JSON (estrazione campo tempo di ricerca)
INDEXED_EXTRACTION (estrazione in fase di indice)

Collegamenti correlati

Risposte Splunk

Perché i miei campi json vengono estratti due volte?
https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Documentazione relativa a Splunk

Attributi Props.conf per dati strutturati
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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).