JSONイベントが重複しています。

適用性

Splunkエンタープライズ

調査

btoolコマンドを実行し、属性 KV_MODEおよび AUTO_KV_JSONを検索すると、それぞれ jsonおよびtrueに設定されます。

```
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
```

解決方法

マニュアルに従います。

「注：*INDEXED_EXTRACTIONS=JSON*を設定する場合は、同じソースタイプに対して*KV_MODE = json*も設定していないことを確認してください。これにより、インデックス時と検索時にJSONフィールドが2回抽出されます。」

したがって、問題を停止するには、属性の1つを無効にする必要があります。

AUTO_KV_JSON（検索時フィールド抽出）
INDEXED_EXTRACTION（インデックス時間抽出）

関連リンク

Splunkの回答

Jsonフィールドが2回抽出されるのはなぜですか。
https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Splunkドキュメント

構造化データのProps.conf属性
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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。