重复的JSON事件。

适用范围

Splunk企业

调查

运行 btool命令并搜索属性 KV_MODE和 AUTO_KV_JSON分别设置为 json和true时：

```
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
```

分辨率

根据文档：

"注：如果设置*INDEXED_EXTRACTIONS=JSON*，请检查是否尚未为同一源类型设置*KV_MODE = json*，这将使JSON字段在索引时提取两次，在搜索时再提取。"

因此，您需要禁用其中一个属性以停止问题。

AUTO_KV_JSON（搜索时间字段提取）
INDEXED_EXTRACTION（索引时间提取）

相关链接

Splunk答案

为什么两次提取我的json字段？

https://answers.splunk.com/answers/174939/why-are-my-json-fields-extracted-twice.html

Splunk文档

结构化数据的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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。