Splunk没有从事件中提取毫秒数

适用范围

Splunk云Splunk企业

描述

Splunk最多提取秒数，当事件包含毫秒事件时，它会忽略这些事件。这种四舍五入导致Splunk搜索中的日志排序，这些日志与生成日志的时间顺序不一致，这可能对报告和某些事件使用产生问题。

调查

可以重现以下内容，以帮助诊断提取中的错误：

1. props.conf已正确配置为提取毫秒，例如：

```
TIME_FORMAT =%Y%m%dT%H:%M:%S.%9N%Z
```

2. 使用HEC（HTTP事件收集器）接收事件。
3. 用于发送事件的终端为/collector/event:

```
https://host_name/services/collector/event
```

分辨率

将终端从 事件更改为 原始:

```
https://host_name/services/collector/raw
```

相关链接

Splunk答案：

定义hec输入的时间戳

Splunk文档：

原始事件分析
HTTP事件收集器的事件格式：原始事件分析

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）。