

无法使用“=”搜索字段

适用范围

Splunk企业版Splunk云

描述

Splunk版本：7.0.13

当尝试通过匹配字符串来搜索以下字段之一时：

- pod
- 命名空间
- container_name
- container_id

像 container_id=aadd1 一样，不会返回结果。

调查

经过一些研究后发现，此配置上的HEC数据无需任何配置文件即可索引，但为了正确使用它，需要一些配置。实际上，这些字段可以通过使用 `::sign`（元数据字段说明符），但这并不能解决不能使用=号搜索这些字段的问题。

要使此配置正常工作，必须在搜索时执行进一步配置。当具有GCP Kubernetes的HEC输入时，事件似乎并未完全准备好可搜索。特别是字段似乎没有索引，这是数据原始数据的一部分，但在搜索获取事件时没有指定。

分辨率

由于未获取索引的事件配置参数必须按如下方式添加：

实例：搜索头

文件:fields.conf

路径：\$SPLUNK_HOME/etc/apps/search/local

设置：将每个字段添加为参数INDEXED=true的字段，如下所示。

```
[pod]
INDEXED=true[namespace]
INDEXED=true[container_name]
INDEXED=true[container_id]
INDEXED=true
```

之后，需要重新启动搜索头，此时将以=号搜索即将发生的新事件。

相关链接

Splunk答案

为什么需要使用“：：”在HEC的“fields”参数中搜索元数据？：

<https://answers.splunk.com/answers/635676/why-do-i-need-to-search-metadata-in-a-fields-argum.html>

外部链路

Kubernetes日志记录设置：

<https://github.com/splunk/splunk-connect-for-kubernetes/tree/develop/helm-chart/splunk-kubernetes-logging>

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）。