

nullqueue regex未按预期工作

适用范围

Splunk企业

描述

我们有几个使用案例，其中我们实施了“保留特定事件并放弃其余事件”模式。

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specifi

我们遇到了这种情况，我们的索引器中定义了以下空队列转换。我们已将此regex匹配项验证到所有事件。然后，XXX匹配我们要保留并发送到<INDEX>索引的事件子集。

转换：

```
[YYY]
REGEX = .*LogName=Security.*
DEST_KEY = queue
FORMAT = nullQueue[XXX]
REGEX=(?msi)^EventCode=(<NUMBERS IN A REGEX>)
DEST_KEY = _MetaData:Index
FORMAT = <INDEX>
```

道具：

```
[WinEventLog:Security]
TRANSFORMS-set=YYY, XXX
```

这没用。<INDEX>中没有内容。然后将YYY regex更改为“REGEX=”。效果不错。但是，我们应该能够使用比“”更具体的regex执行REGEX空值。当它实际匹配所有事件时。

调查

将用户会议与文档进行比较，发现所有工作图都开始进行全面的测试。我们可以从收集器中提取多个数据，让用户能够在收集器处于适当位置时保持同样精确。

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specifi

分辨率

设置道具和转换，以便使用除“。”之外的某些regex进行第一个 nullqueue转换。 然后进行另一个转换，使用更具体的正则表达式和某些索引，并期望数据进入该索引。

转换：

```
[XXX]
REGEX = .
DEST_KEY = queue
FORMAT = nullQueue[YYY]
REGEX=(?msi)^EventCode=(<NUMBERS IN A REGEX>)
DEST_KEY = _MetaData:Index
FORMAT = <INDEX>[ZZZ]
REGEX= <LOG NAME REGEX>
DEST_KEY = _MetaData:Index
FORMAT = <DIFFERENT INDEX>
```

道具：

```
[WinEventLog:Security]
TRANSFORMS-set=XXX, YYY, ZZZ
```

相关链接

Splunk文档

保留特定事件并丢弃其余事件：

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific

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）。