nullqueue regex가 예상대로 작동하지 않음

적용 가능성

Splunk Enterprise

설명

이 "특정 이벤트를 유지하고 나머지는 버립니다" 패턴을 구현하는 몇 가지 활용 사례가 있습니다.
https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specifi

인덱서에 아래와 같이 null 큐 변환이 정의된 경우를 우연히 발견했습니다. 이 regex가 모든 이벤트에 일치하는지 확인했습니다. 그런 다음 XXX는 유지할 이벤트의 하위 집합을 매칭하고 <INDEX> 인덱스로 전송합니다.

변환:

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

소품:

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

이것은 작동하지 않았습니다. <INDEX>에 아무것도 없었습니다. 그런 다음 YYY regex를 "REGEX="로 변경했습니다. 정상 작동합니다. 그러나 우리는 ""보다 더 구체적인 regexp를 사용하여 REGEX nulque를 할 수 있어야 한다. 모든 이벤트와 일치하는지 확인합니다.

조사

사용자의 전화회의와 문서를 비교했을 때 모든 작업 다이어그램이 캐치올 테스트로 시작되었다는 것을 알 수 있었습니다. 캐솔에서 여러 번 추출을 할 수 있어, 사용자가 캐솔을 적절하게 사용할 수 있습니다.

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

해결

"."이 아닌 일부 regex를 사용하여 첫 번째 nullqueue 변환을 갖도록 소품 및 변환을 설정합니다. 그 다음에 더 특정한 regex와 약간의 인덱스를 가진 또 다른 변환으로 데이터가 그 인덱스로 갈 것으로 예상한다.

변환:

```
[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>
```

소품:

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

관련 링크

Splunk 설명서
특정 이벤트를 유지하고 나머지는 버립니다.
https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specifi

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.