Splunk가 이벤트에서 밀리초를 추출하지 않습니다.

적용 가능성

Splunk Cloud Splunk Enterprise

설명

Splunk는 초 단위까지 추출하고 이벤트에 밀리초의 이벤트가 포함되어 있으면 해당 이벤트를 무시합니다. 이러한 반올림으로 인해 Splunk 검색에서 로그가 생성되는 시간 순서에 맞지 않게 정렬됩니다. 이는 보고서와 일부 이벤트 사용에 문제가 될 수 있습니다.

조사

추출 오류를 진단하기 위해 다음을 재현할 수 있습니다.

1. props.conf는 밀리초를 추출하도록 적절히 구성되었습니다. 예를 들면 다음과 같습니다.

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

2. 이벤트는 HEC(HTTP Event Collector)를 사용하여 수집됩니다.
3. 이벤트를 전송하는 데 사용되는 엔드포인트는 /collector/event입니다.

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

해결

엔드포인트를 이벤트에서 원시로 변경합니다.

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

관련 링크

Splunk 답변:

hec 입력에 대한 타임스탬프 정의

Splunk 설명서:

원시 이벤트 구문 분석
HTTP 이벤트 컬렉터에 대한 이벤트 형식 지정: 원시 이벤트 구문 분석

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.