

"="인 필드를 검색할 수 없습니다.

적용 가능성

Splunk Enterprise Splunk Cloud

설명

Splunk 버전: 7.0.13

문자열을 일치시켜 다음 필드 중 하나를 검색하려고 할 때:

- 포드
- 네임스페이스
- 컨테이너_이름
- 컨테이너_id

container_id=aadd1과 마찬가지로 결과를 반환하지 않습니다.

조사

몇 가지 조사 결과 이 컨피그레이션의 HEC 데이터는 컨피그레이션 파일 없이 인덱싱되지만 이를 제대로 사용하려면 일부 컨피그레이션이 필요합니다. 필드를 실제로 검색할 수 있으려면 :: 기호(메타데이터 필드 지정자)를 사용하지만 = 기호로 검색할 수 없다는 사실은 수정되지 않습니다.

이 추가 구성을 작동하려면 검색에 대해 수행해야 합니다. GCP kubernetes에 대한 HEC 입력을 가질 때 이벤트는 검색 가능하도록 완전히 준비되지 않은 것 같습니다. 특히 필드는 데이터 원시 데이터의 일부이지만 이벤트 가져오기를 위한 검색에 지정되지 않는 인덱싱되지 않은 것으로 보입니다.

해결

이벤트가 인덱싱된 구성 매개 변수를 가져오지 않으므로 다음과 같이 추가해야 합니다.

인스턴스: 검색 헤드

파일: fields.conf

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

설정: 다음과 같이 INDEXED=true 매개 변수를 사용하여 각 필드를 스탠자로 추가합니다.

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

이 후 검색 헤드를 다시 시작해야 하며, 이를 통해 들어오는 새 이벤트를 = 기호로 검색할 수 있습니다.

관련 링크

Splunk Answers

'::'을 사용하는 HEC의 "필드" 인수로 메타데이터를 검색해야 하는 이유는 무엇입니까?

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

외부 링크

Kubernetes 로깅 설정:

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

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.