

DB 연결 입력이 인덱서에 대한 이벤트 전송을 중지했지만 다른 DB 연결 입력이 제대로 작동하고 있습니다.

적용 가능성

Splunk Enterprise Splunk DB Connect

설명

DB 연결 입력이 인덱서에 대한 이벤트 전송을 중지했지만 다른 DB 연결 입력이 제대로 작동하고 있습니다.

조사

식별 방법:

db_connect 로그를 확인합니다(아래 예와 유사한 메시지의 index=_internal sourcetype=dbx*):

```
2018-10-01 12:07:33.885 +0100 INFO c.s.dbx.server.task.listeners.JobMetricsListener - ac
db_read_time=91 hec_record_process_time=826 format_hec_success_count=1000 status=FAILED
is_jmx_monitoring=false start_time=2018-10-01_12:07:27 end_time=2018-10-12_01:07:30 dura
....
2018-10-01 12:07:33.885 +0100 [QuartzScheduler_Worker-27] INFO org.easybatch.core.job.Ba
.....
at com.splunk.dbx.server.dbinput.recordwriter.HecEventWriter.writeRecords(HecEventWriter
at com.splunk.dbx.server.dbinput.recordwriter.HttpEventCollector.uploadEvents(HttpEventC
at com.splunk.dbx.server.dbinput.recordwriter.HttpEventCollector.uploadEventBatch(HttpEv
java.io (https://java.io) .IOException: HTTP Error 400: Bad Request
2018-10-01 12:07:33.885 +0100 [QuartzScheduler_Worker-27] ERROR org.easybatch.core.job.B
```

해결

다음 버그로 인해 발생합니다.

DBX-4614 - "HTTP 오류 400: 잘못된 요청" 오류가 발생했습니다. 필드 길이가 깁니다.

다음 중 중복 항목입니다.

SPL-156315 [Regression] 7.x로 업그레이드한 후 512KB보다 큰 HEC 이벤트는 구문 분석 오류와 함께 삭제되어 인덱싱 처리량이 저하됩니다

HEC에 512KB 이상의 이벤트를 보내려고 하면 이벤트가 삭제됩니다. DBX가 HEC를 통해 이벤트를 보내고 이 제한에 도달하면 이벤트 보내기가 계속 시도되고 실패하므로 이벤트를 수동으로 건너뛰거나 열의 하위 문자열을 대신 보내지 않으면 더 이상 이벤트가 인덱싱되지 않습니다.

이 문제는 기본 최대 HEC 이벤트 크기를 512K에서 5MB로 늘려 Splunk 7.0.5 이상, 7.1.3 이상, 7.2.0 이상에서 해결됩니다. 필요한 경우 이 값을 더 높게 늘릴 수 있도록 새로운 구성 옵션 `maxEventSize`도 `inputs.conf`에 추가되었습니다.

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf#http:_28HTTP_Event_Collector.2

```
maxEventSize = <positive integer>[KB|MB|GB]
* The maximum size of a single HEC (HTTP Event Collector) event.
* HEC disregards and triggers a parsing error for events whose size is
  greater than 'maxEventSize'.
* Default: 5MB.
```

관련 링크

Splunk 설명서

`http:` (HTTP 이벤트 컬렉터)

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf#http:_28HTTP_Event_Collector.2

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.