"코드 255로 종료됨" 오류로 인해 하위 검색으로 큰 조회를 사용한 tstat 검색 실패

적용 가능성

Splunk Enterprise Splunk Search Splunk Subsearch Splunk tstat

설명

tstats 명령의 where 절에서 하위 검색을 너무 큰(5,000개 이상의 행처럼 보이는) 경우 검색이 실패하고 오류가 발생합니다.
검색 프로세스가 올바르게 종료되지 않았습니다. exit_code=255, description="코드 255로 끝났습니다." 자세한 내용은 Job Inspector에서 이 피어에 대한 search.log를 참조하십시오.

```
| tstats count from datamodel=Web where NOT
[| inputlookup lookup.csv
| fields dest
| rename dest as Web.dest
| format ] by Web.src Web.dest
```

이 예에서 lookup_name.csv의 행은 110k입니다.

조사

아래 오류로 인해 검색이 실패하는 경우

```
[<INDEXER_NAME>] Search process did not exit cleanly, exit_code=255, description="exited
```

오류 메시지는 인덱서 INDEXER_NAME에 대한 검색 프로세스에 문제가 있음을 의미합니다. 대부분의 경우 오류가 발생했거나 삭제되었습니다.

crash.log가 없으면 splunk가 외부에서 제거되었거나 crash.log를 저장하는 데 문제가 있음을 의미합니다.
그러나 검색 문자열을 보면 (OR-s의 수) 재귀로 인해 스택 오버플로가 발생할 가능성이 높습니다.

해결

재귀가 충돌을 일으킬 수 있다는 것은 알려진 문제입니다(예: OR/AND가 많은 비효율적인 검색 문자열).
SPL-144975 추적:Splunk의 부분 재설계 및 재귀 제거

이 문제를 해결하는 한 가지 방법은 스택의 한도를 늘리는 것입니다. 기본값은 8064이며, 128k 또는 256k와 같은 향상된 값으로 문제를 해결할 수 있습니다.

관련 링크

SPL-144975:Splunk의 부분 재설계 및 반복 제거

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.