

REST API가 구문 분석 상태의 검색을 완료하지 않음

적용 가능성

Splunk Enterprise

설명

REST [API Reference Manual](#)에 따르면 'finalize' 작업을 사용하여 검색을 중지할 수 있습니다.

24시간 이상 실행되는 여러 검색이 있는 환경에서는 REST API를 사용하여 이러한 검색이 오랫동안 결과를 생성하지 않도록 중지합니다. 사용되는 명령은 다음과 같습니다.

```
curl method=post uri=https://localhost:8801/services/search/jobs/$sid$/control splunkauth=
```

그러나 이 명령은 대부분의 검색에서는 성공하지만 구문 분석 상태의 검색은 중지하지 못합니다. 이러한 작업은 OS 프로세스를 중단해야 합니다.

조사

CONTROL 엔드포인트는 작업 목록(일시 중지)을 수락합니다 | 일시 중지 취소 | 마무리 | 취소 | 터치 | 설정 | setpriority | 사용preview | 사용 안 함미리 보기 | setworkloadpool)

마무리: 검색을 중지하고 중간 결과를 /results 끝점에 제공합니다.

SH에서 검색을 제기하면 SH는 이를 분산형 및 중앙 집중형 부분으로 구문 분석하며 나중에 인덱서로 전송됩니다. 이 시점에서는 검색 결과가 아직 생성되지 않았으므로 'finalize' 작업은 중간 결과를 제공할 수 없습니다.

그러나 'cancel' 작업은 구문 분석 상태의 검색에 적합합니다. 이 작업은 검색을 중지하고 결과를 반환하지 않습니다.

취소: 현재 검색을 중지하고 결과 캐시를 삭제합니다.

해결

구문 분석 상태의 검색에 대해 이 명령은 작업을 올바르게 중지합니다.

```
curl method=post uri=https://localhost:8801/services/search/jobs/$sid$/control splunkaut
```

관련 링크

Splunk 설명서

REST API 참조 설명서

[REST검색](#)

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.