간헐적으로 과도한 디스크 사용량이 검색 헤드 캡틴에 있음

적용 가능성

Splunk Enterprise

설명

검색 헤드 클러스터에서 Splunk가 검색에서 사용하는 파일 시스템의 디스크 사용량을 발견했습니다
헤드 캡틴이 간헐적으로 증가하여 파일 시스템을 거의 채우다가 그 후 감소했습니다.
다시 증가합니다

조사

다음 디렉터리에서 최대 2GB의 여러 개(복제) .bundle 파일이 발견되었습니다

```
/data/splunk/var/run
/data/splunk/var/run/snapshot
```

복제에 대한 지식 객체를 포함하는 이러한 .bundle(tar) 파일의 목록에 오래된(더 이상 사용되지 않음) 용량이 포함되어 있습니다.
/data/splunk/etc/users에서 파일을 조회합니다. 이 경우 파일을 삭제하여 향후 번들 크기를 줄이고 디스크 사용량 급증을 중지합니다.

해결

etc/apps의 큰 바이너리는 동일한 문제를 야기할 수 있다. 이진 파일은 삭제할 수 없지만 삭제할 필요는 없습니다.
번들에 포함되므로, 다음 링크를 통해 블랙리스트에 추가하여 포함시키지 마십시오.
distsearch `.conf`의 `[replicationBlacklist]` 시작:

https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Limittheknowledgebundlesize

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.