집계 KPI 값은 엔터티 KPI 심각도에 관계없이 해당 없음(N/A)을 표시합니다.

적용 가능성

Splunk Enterprise Splunk IT Service Intelligence

설명

서비스 템플릿에 연결된 서비스(약 850)를 서비스 분석기에서 보고 관련 KPI가 표시되면 엔티티 KPI 심각도에 올바른 값(정보)이 표시되지만 서비스 KPI 심각도는 알 수 없음으로 표시됩니다. KPI에 대한 집계 임계값 및 엔티티당 임계값은 모두 정보로 설정됩니다.

해결

많은 엔티티와 많은 서비스/KPI(템플릿/서비스당 8개의 KPI)가 있습니다. 그 결과, KPI 기반 검색의 각 실행은 수만 개의 결과를 반환하며, 이는 ITSI가 처리된 검색 결과를 ITSI 요약 지수로 전송할 때 한도를 초과할 수 있습니다

이 문제를 방지하려면 서비스를 여러 공유 기반 검색에 분산시켜 결과 수를 줄입니다.

- 50000개 이상의 결과를 반환하는 가장 큰 공유 기반 검색,

검색 이름의 ID는 공유 기반 검색의 ID입니다.

```
index=_internal source=*scheduler.log* shared indicator  | stats min(result_count) AS mi
```

- 보유한 서비스(및 서비스당 엔터티) 수를 계산하여 반반씩 작업을 수행할 수 있는지 확인합니다.
- 공유 기본 검색 복제 그런 다음 서비스의 절반을 재할당하여 새 공유 기반 검색을 사용합니다.
- 실행을 허용한 다음 위의 검색을 사용하여 공유 기반 검색당 결과의 새로운 재분할을 확인하

고 제한 미만인지 확인합니다.
- 이제 KPI에 유효한 "서비스 집계 값"이 있음을 서비스에서 검증합니다.

또는

한도 증가(한도를 초과하지 100000)

1. $SPLUNK_HOME/etc/system/local에서 limits.conf를 만들거나 수정합니다.
2. 다음 표식을 추가합니다.

```
[scheduler]
* The maximum number of results to load when triggering an alert action.
* Default: 50000
max_action_results = 50000
```

3. 다음 공식에 따라 위의 수를 직접 계산하고 조정해야 합니다.

```
limit = (number of KPIs * number of entities for each service) + (number of services) *
```

참고: 이 제한이 증가하면 결과 수를 지원하기 위해 더 많은 메모리가 할당되므로 ITSI는 더 많은 메모리를 사용합니다

4. Splunk 다시 시작

관련 링크

Splunk 블로그

대규모 환경에서 Splunk ITSI를 구성하기 위한 상위 3가지 모범 사례

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.