

Splunk 인스턴스 상태가 Bucket 구성 요소에 대해 RED를 표시하고 있습니다.

적용 가능성

Splunk Enterprise

설명

지난 1시간 동안 생성된 버킷(100)의 소량 백분율이 매우 높으며 이 인덱서에서 index=<index name> 및 가능한 더 많은 인덱스의 빨간색 임계값(50)을 초과했습니다.

상태 확인 탭의 오류 메시지:

```
Buckets
Root Cause(s):
The percentage of small of buckets created (100) over the last hour is very high and exc
```

최근 50개 관련 메시지:

```
07-02-2019 02:16:05.989 -0700 INFO HotBucketRoller - finished moving hot to warm bid=_in
from=hot_v1_4984 to=db_1562087584_1562043339_4984 size=1048645632 caller=size_exceeded _
07-02-2019 00:22:57.931 -0700 INFO HotBucketRoller - finished moving hot to warm bid=_in
from=hot_v1_2046 to=db_1562027109_1562015374_2046 size=569110528 caller=lru maxHotBucket
07-02-2019 00:00:22.067 -0700 INFO HotBucketRoller - finished moving hot to warm bid=clo
from=hot_v1_324 to=db_1561885206_1561791602_324 size=394207232 caller=lru maxHotBuckets=
07-01-2019 23:03:37.981 -0700 INFO HotBucketRoller - finished moving hot to warm bid=_in
from=hot_v1_4983 to=db_1562076172_1562032683_4983 size=1054523392 caller=size_exceeded _
07-01-2019 22:43:06.030 -0700 INFO HotBucketRoller - finished moving hot to warm bid=cle
from=hot_v1_362 to=db_1561787045_1561538116_362 size=393191424 caller=lru maxHotBuckets=
```

조사

위의 메시지는 지난 24시간 동안 생성된 버킷 중 100%가 maxDataSize의 10%보다 적다는 것입니다. 그러면 성능 문제가 발생하지 않습니다. 이 경고를 수정하려면 아래와 같이 임계값을 50에서 150으로 늘릴 수 있습니다.

기본 컨피그레이션은 \$SPLUNK_HOME/etc/system/default/health.conf 위치에 있습니다.

```
[feature:buckets]
display_name = Buckets
indicator:percent_small_buckets_created_last_24h:description = "This indicator tracks the
small bucket is defined as less than 10 % of the 'maxDataSize' setting in indexes.conf."
indicator:percent_small_buckets_created_last_24h:red = 50
indicator:percent_small_buckets_created_last_24h:yellow = 30
```

또한 위의 동일한 상태 경고 메시지는 특정 시간/일에 데이터를 인덱싱하기 위해 생성된 핫 버킷 수가 system/health.conf에 정의된 임계값 제한을 초과하거나 초과할 때 표시됩니다.

너무 많은 뜨거운 양동이 생성 뒤에 이유

Splunk는 데이터를 인덱싱하기 위해 버킷(bucket)을 인덱스 디렉토리로 사용합니다. 이제 이벤트를 인덱싱하기 위해 Splunk에 가져오면 해당 이벤트에 대해 새 핫 버킷이 생성되거나 이벤트의 타임스탬프와 인덱스의 제약 조건에 따라 이벤트가 기존 핫 버킷으로 인덱싱됩니다.

index.conf의 maxHotBucket, maxHotSpanSecs 및 quarantinePastSecs 매개변수를 [참조하십시오](#).

따라서 이벤트에 기존 버킷에 허용되는 것보다 오래된/이상한 타임스탬프가 있는 경우 Splunk는 해당 이벤트를 인덱싱할 새 핫 버킷을 생성합니다. 따라서 생성된 핫 버킷의 수가 임계값에 도달하거나 임계값을 넘을 수 있습니다.

props.conf의 DATETIME [CONFIG](#) 매개 변수가 명시적으로 설정되지 않은 경우 Splunk는 이벤트 자체에서 타임스탬프를 찾습니다.

따라서 이벤트에서 타임스탬프를 추출하는 동안 Splunk가 유효한 타임스탬프 형식과 일치하는 값을 찾으면 이벤트 시간과 동일한 값을 구문 분석하고 해당 타임스탬프만 사용하여 인덱싱합니다. 그러면 타임스탬프가 제대로 추출되지 않아 Splunk에서 새 핫 버킷을 생성할 수 있습니다.

Splunk 추출 타임스탬프를 제대로 만들려면 props.conf에 타임스탬프 특성을 추가하는 것이 좋습니다. [타임스탬프 인식을 구성하십시오](#).

스탬프 발행:

또한 로그 형식에 따라 올바른 설정을 적용하여 타임스탬프에 관한 splunkd.log에서 아래의 메시지를 수정했습니다.

```
06-02-2019 22:37:36.976 -0700 WARN DateParserVerbose - Failed to parse timestamp in first
Defaulting to timestamp of previous event (Mon Jun 3 02:37:35 2019). Context: source=/data
|cisco:asa|48952806-21-2019 09:48:48.467 -0700 WARN DateParserVerbose - Failed to parse
Defaulting to timestamp of previous event (Fri Jun 21 06:48:45 2019). Context: source=/data
Defaulting to timestamp of previous event (Thu Jun 20 11:29:10 2019). Context: source=/s
|linux_secure|526909106-14-2019 12:46:38.301 -0700 WARN DateParserVerbose - Accepted tim
in extracting timestamps. Context: source=C:\Windows\debug\netlogon.log|host=DC2SJGLOBAL
|mar|\x{4E09}\x{6708}|apr|\x{56DB}\x{6708}|may|\x{4E94}\x{6708}|jun|\x{516D}\x{6708}|ju
|nov|\x{5341}\x{3127}\x{6708}|dec|\x{5341}\x{4E8C}\x{6708})[a-z,\.;]*([/\ - ]){0,2}(?i)(
UT|UTC|GMT(?![+-]))|CET|CEST|CETDST|MET|MEST|METDST|MEZ|MESZ|EET|EEST|EETDST|WET|WEST|WET
|EADT|WAST|WADT|Z)|(?:GMT)?[+-]\d\d?:?(?:\d\d)?(?:!\w))?(?:\2|,){0,2}(?i)(20\d\d|19\d
in extracting timestamps. Context: source=C:\Windows\System32\DHCP\DhcpSrvLog-Mon.log|ho
```

해결

1. \$SPLUNK_HOME/etc/system/local/health.conf으로 이동하여 아래 표를 추가합니다.

```
[feature:buckets]
indicator:percent_small_buckets_created_last_24h:red = 150
```

2. 변경 사항을 적용하려면 Splunk를 다시 시작합니다.

타임스탬프 또는 DATETIME_CONFIG 문제인 경우 이벤트의 날짜와 시간을 올바르게 식별하고 문제를 해결하기 위해 적절한 regex를 작성합니다.

관련 링크

Splunk 설명서

[타임스탬프 인식 구성](#)

Splunk Answers

[상태: 생성된 작은 버킷의 백분율](#)

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.