

Der Status der Splunk-Instanz zeigt ROT für die Bucket-Komponente an.

Geltungsbereich

Splunk Enterprise

Beschreibung

Der Prozentsatz kleiner erstellter Buckets (100) in der letzten Stunde ist sehr hoch und hat die roten Schwellenwerte (50) für `index=<Indexname>` und möglicherweise weitere Indizes auf diesem Indexer überschritten.

FEHLER-Meldungen auf der Registerkarte "Integritätsprüfung":

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

Letzte 50 verwandte Nachrichten:

```
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=
```

Untersuchung

Die obige Meldung besagt, dass 100% der für die letzten 24 Stunden erstellten Buckets weniger als 10% von `maxDataSize` sind. Dies führt zu keinen Leistungsproblemen. Um diese Warnung zu beheben, können Sie den Schwellenwert wie unten beschrieben von 50 auf 150 erhöhen.

Die Standardkonfiguration befindet sich im Verzeichnis
`$SPLUNK_HOME/etc/system/default/health.conf`

```
[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
```

Ebenfalls aus der obigen Gesundheitswarnmeldung wird angezeigt, wenn die Anzahl der zur Indizierung der Daten erstellten Hot-Buckets pro Stunde und Tag den in system/health.conf definierten Grenzwert überschreitet oder erreicht.

Der Grund für die Schaffung zu vieler heißer Eimer

Splunk verwendet Buckets als Indexverzeichnis, um die Daten zu indizieren. Wenn jetzt ein Ereignis zur Indizierung an Splunk gesendet wird, wird die neue Hot Bucket für dieses Ereignis erstellt, oder das Ereignis wird entsprechend dem Zeitstempel und den Einschränkungen für das Ereignis für den Index an die vorhandene Hot Bucket indiziert.

Weitere Informationen finden Sie unter den Parametern maxHotBuckets, maxHotSpanSecs und quarantinePastSecs von [indexes.conf](#).

Wenn das Ereignis also den älteren/seltsamen Zeitstempel hat, der für die vorhandenen Buckets nicht akzeptabel ist, erstellt Splunk einen neuen Hot Bucket, um dieses Ereignis zu indizieren. Daher kann die Anzahl der erstellten Hot Buckets den Schwellenwert erreichen oder überschreiten.

Wenn der Parameter DATETIME_CONFIG von [props.conf](#) nicht explizit festgelegt wird, versucht Splunk, den Zeitstempel in einem Ereignis selbst zu finden.

Wenn Splunk also den Wert findet, der dem gültigen Zeitstempelformat entspricht, wird beim Extrahieren des Zeitstempels aus den Ereignissen derselbe Wert wie die Ereigniszeit analysiert und nur mit diesem Zeitstempel indiziert. Dies kann dazu führen, dass Splunk einen neuen heißen Bucket erstellt, da der Zeitstempel nicht ordnungsgemäß extrahiert wird.

Erwägen Sie, Zeitstempelattribute in props.conf hinzuzufügen, damit Splunk den Zeitstempel richtig extrahiert. [Konfigurieren Sie die Zeitstempelerkennung](#).

Problem mit dem Stempel:

Außerdem habe ich die folgenden Nachrichten in der splunkd.log in Bezug auf den Zeitstempel auch sie durch die Anwendung der richtigen Einstellungen zu beheben hängt vom Log-Format.

```
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=/da
|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=/d
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}|ju1
|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\
in extracting timestamps. Context: source=C:\Windows\System32\Dhcp\DhcpSrvLog-Mon.log|ho
```

Auflösung

1. Navigieren Sie zu \$SPLUNK_HOME/etc/system/local/health.conf und hängen Sie den folgenden Strophen an

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

2. Starten Sie den Splunk neu, damit die Änderungen wirksam werden.

Wenn es sich um einen Zeitstempel oder ein DATETIME_CONFIG-Problem handelt, schreiben Sie einen geeigneten regulären Ausdruck, um Datum und Uhrzeit des Ereignisses korrekt zu identifizieren und das Problem zu beheben.

Verwandte Links

Splunk-Dokumentation

[Zeitstempelerkennung konfigurieren](#)

Punktantworten

[Gesundheitsstatus: Der Prozentsatz kleiner erstellter Buckets](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.