

# El estado de la instancia de Splunk se muestra en ROJO para el componente Bucket

## Aplicabilidad

Splunk Enterprise

## Descripción

El porcentaje de pequeños bloques de bloques creados (100) durante la última hora es muy alto y ha superado los umbrales rojos (50) para index=<index name>, y posiblemente más índices, en este indizador.

Mensajes de ERROR en la ficha Comprobación de estado:

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

Últimos 50 mensajes relacionados:

```
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=
```

## Investigación

El mensaje anterior indica que el 100% de los bloques creados en las últimas 24 horas es inferior al 10% de maxDataSize. Esto no causará ningún problema de rendimiento. Para corregir esta advertencia, puede aumentar el umbral de 50 a 150 como se indica a continuación.

La configuración predeterminada se encuentra en la ubicación  
\$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
```

También del mensaje de advertencia de estado anterior se muestra cuando el número de bloques creados para indexar los datos en una hora/día particular cruza o alcanza el límite de umbral definido en `system/health.conf`.

### La razón detrás de la creación de demasiadas cubas calientes

Splunk utiliza bloques como directorio de índice para indexar los datos. Ahora, cuando un evento llega a Splunk para indexación, se creará la nueva cubeta de conexión para ese evento o el evento se indexará con la cubeta de conexión existente según la marca de tiempo del evento y las restricciones en el índice.

Consulte los parámetros `maxHotBuckets`, `maxHotSpanSecs` y `quarantinePastSecs` de [indexes.conf](#)

Por lo tanto, si el evento tiene la marca de tiempo más antigua/extraña que la aceptable para los depósitos existentes, Splunk creará un nuevo depósito activo para indexar ese evento. Por lo tanto, el número de bloques activos creados puede alcanzar o cruzar el umbral.

Cuando el parámetro `DATETIME_CONFIG` de [props.conf](#) no se establece explícitamente, Splunk intentará encontrar la marca de tiempo en un evento en sí.

Por lo tanto, al extraer la marca de tiempo de los eventos, si Splunk encuentra el valor que coincide con el formato de marca de tiempo válido, analizaría el mismo valor que la hora del evento y lo indexaría usando solo esa marca de tiempo, lo que puede hacer que Splunk cree una nueva cubeta de tiempo, ya que la marca de tiempo no se extrae correctamente.

Considere la posibilidad de agregar atributos de marca de hora en `props.conf` para que Splunk extraiga la marca de hora correctamente. [Configure el reconocimiento de marca de hora](#)

### Problema de marca de hora:

Además, he encontrado los siguientes mensajes en el splunkd.log con respecto a la marca de tiempo también los corrige aplicando la configuración correcta depende del formato de registro.

```
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
```

## Resolución

1. Navegue hasta \$SPLUNK\_HOME/etc/system/local/health.conf y agregue la siguiente estrofa

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

2. Reinicie el Splunk para que los cambios surtan efecto.

Si se trata de un problema de marca de tiempo o DATETIME\_CONFIG, escriba un regex adecuado para identificar la fecha y la hora del evento correctamente y rectifique el problema.

## Enlaces relacionados

Documentación de Splunk

[Configurar el reconocimiento de marca de tiempo](#)

Respuestas de Splunk

[Estado de salud: El porcentaje de pequeños depósitos creados](#)

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).