

Wachtrijen voor gebeurtenisverwerking geblokkeerd

toepasbaarheid

Splunk Enterprise

Beschrijving

Onboarding sommige gegevens rechtstreeks naar Indexers en sommige bronnen verzenden de gegevens via zware expediteurs.

onderzoek

1. In splunkd.log zijn er linebreaking en AggregatorMiningProcessor fouten voor enkele brontypen.

```
WARN AggregatorMiningProcessor - Breaking event because limit of 256 has been exceeded  
data_sourcetype="sourcetype_name" WARN AggregatorMiningProcessor - Breaking event becaus  
data_sourcetype="other_sourcetype_name"
```

2. Het [dashboard voor indexeringsprestaties](#) toont dat de "Aggregator" Splunk Processor een hoge CPU gebruikt.

3. Het repareren van de brontypen die de fouten veroorzaakten, loste niet op (fouten verdwenen, probleem blijft).

4. Er is een knelpunt in de aggregatiewachtrij, pstack geeft aan dat de aggregatieprocessor bezig is met het samenvoegen van de lijnen in één gebeurtenis, waardoor een knelpunt ontstaat.

Dit probleem treedt op wanneer de aggregatieprocessor een groot aantal regels samenvoegt tot één gebeurtenis. Van de code, wanneer er een regel die moet worden samengevoegd om de huidige gebeurtenissen, zou er `string::` geheugen verplaatsen en `reserveren` gebeurde als de volgende code. Dus als er 1000 regels zijn voor één evenement, zouden er 1000 keer `reserve` en `memo`'s worden opgeroepen.

```
void CowPipelineData::appendAndReset(CowPipelineData& other)
{
    ...
    _pd->_rawAsStr.reserve(_pd->_rawSeg.size() + other._pd->_rawSeg.size() + 1);
    append_other_raw:
    _pd->_rawAsStr.push_back('\n');
    _pd->_rawAsStr.append(other._pd->_rawSeg);
    ...
}
```

Verzamel een aantal voorbeeldgebeurtenissen die het grote aantal regels bevatten, om te weten welke gebeurtenissen het probleem veroorzaken, om de top drie brontype te identificeren dat een groot aantal totale lijnen heeft:

```
| tstats count where index=* OR index=_* by linecount sourcetype
| where linecount > 2
| stats sum(eval(linecount*count)) as totallines by sourcetype
| sort -totallines
```

Concept:

De reden is:

- We hebben normaal gesproken parseringswachtrij als eerste wachtrij en aggregatiewachtrij als tweede.
- Parsing Wachtrij is om de streaming gegevens te parsen in lijnen standaard karakter `\r\n` als er geen `LINE_BREAKER` gedefinieerd.
- Vervolgens zou de aggregatiewachtrij de regels samenvoegen op basis van de configuratie zoals `TIME_FORMAT` of anderen
- Door `LINE_BREAKER` in te stellen, kan het Splunk vertellen hoe de streaminggegevens in lijnen in de parseringsfase moeten worden ontleed en
- Door `SHOULD_LINEMERGE = false` in te stellen, geeft dit aan dat het aggregatieproces de lijnen niet in gebeurtenissen moet samenvoegen.
- Dus eigenlijk, `LINE_BREAKER` en `SHOULD_LINEMERGE = false` zou een oplossing voor het probleem van de klant.

resolutie

1. Schakel CPU-tijdmetingen voor agg_processor in voor foutopsporingsdoeleinden door de limieten.conf als volgt te wijzigen:

```
.../limits.conf  
[default]  
agg_cpu_profiling = true
```

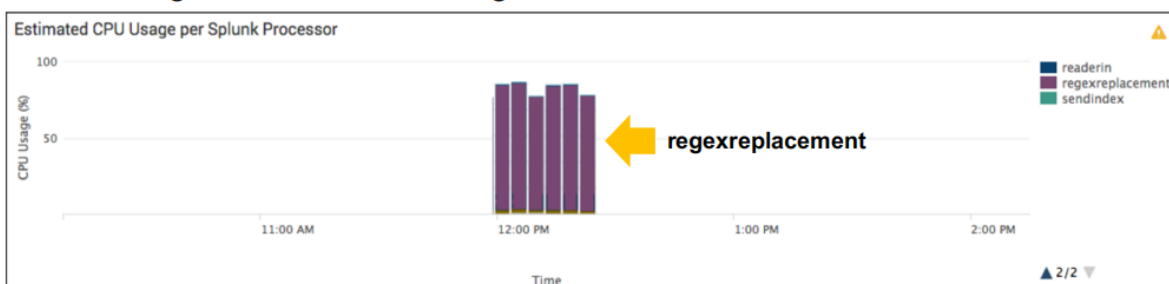
2. Voer de onderstaande zoekopdracht uit om het brontype te identificeren dat de aggregatorprocessor meer onder druk zet:

```
index=_internal source=*metrics.log* per_sourcetype_agg_cpu Metrics  
| timechart span=10s avg(cpu) by series
```

3. Stel SHOULD_LINEMERGE in op "false" en schrijf een regex voor "LINE_BREAKER" voor elk brontype dat in de zoekgrafiek komt. Exp is hieronder die ik nam het uit de Troubleshooting training document.

Opmerking: Screenshot toont zoeken naar regex-processor:

MC > Indexing > Performance > Indexing Performance: Instance



- Search for specific hosts / sources / sourcetypes to find duplicate stanzas for possible anomalies and precedence issues
- Enable CPU time metrics for **RegexProcessor** for debugging purposes

limits.conf

```
[default]  
regex_cpu_profiling = true  
  
[metrics]  
maxseries = 100
```

4. Het repareren van alle brontypen zoals dat zal het probleem van de wachtrijvulling oplossen.

Aanvullende bron:

De volgende video van [kantooruren in de community](#) toont meer diepgang in het oplossen van geblokkeerde wachtrijen.

Gerelateerde links

Limits.conf Handleiding

<https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Limitsconf>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.