

Blockierte Ereignisverarbeitungswarteschlangen

Geltungsbereich

Splunk Enterprise

Beschreibung

Das Onboarding einiger Daten direkt an Indexer und einige Quellen senden die Daten über starke Forwarder.

Untersuchung

1. In splunkd.log gibt es für einige Quelltypen LineReaking- und AggregatorMiningProcessor-Fehler.

```
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. Das [Dashboard für die Indizierungsleistung](#) zeigt an, dass der "Aggregator"-Splunk-Prozessor eine hohe CPU benötigt.

3. Die Behebung der Quellentypen, die die Fehler verursacht haben, wurde nicht behoben (Fehler verschwunden, Problem bleibt bestehen).

4. Die Aggregationswarteschlange weist einen Engpass auf. Der Stapel zeigt an, dass der Aggregationsprozessor beim Zusammenführen der Leitungen zu einem Ereignis ausgelastet ist, wodurch ein Engpass entsteht.

Dieses Problem tritt auf, wenn der Aggregationsprozessor eine große Anzahl von Zeilen in ein einzelnes Ereignis zusammenführt. Wenn eine Zeile mit aktuellen Ereignissen zusammengeführt werden muss, werden im Code `string::reserve` und die Speicherverschiebung wie im folgenden Code ausgeführt. Wenn es also 1000 Zeilen für ein Ereignis gibt, dann gibt es 1000 Mal `reserve` und `Memmovecalled`.

```
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);
    ...
}
```

Sammeln Sie einige Beispielergebnisse, die die große Anzahl von Zeilen enthalten, um zu erfahren, welche Ereignisse das Problem verursachen, um den ersten drei Quelltyp zu identifizieren, der eine große Anzahl von Zeilen insgesamt aufweist:

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

Konzept:

Der Grund dafür ist:

- haben wir normalerweise eine Parsing-Warteschlange als erste und eine Aggregations-Warteschlange als zweite.
- Die Analysewarteschlange dient dazu, die Streaming-Daten standardmäßig in Zeilen zu analysieren, \r\n wenn kein LINE_BREAKER definiert ist.
- Anschließend würde die Aggregationswarteschlange die Zeilen basierend auf der Konfiguration wie TIME_FORMAT oder anderen zusammenführen.
- Durch Festlegen von LINE_BREAKER kann Splunk in der Analysephase angeben, wie die Streaming-Daten in Zeilen analysiert werden sollen, und
- Durch Festlegen von SHOULD_LINEMERGE = false wird angegeben, dass der Aggregationsprozess die Zeilen nicht in Ereignisse zusammenführen soll.
- Im Grunde wären LINE_BREAKER und SHOULD_LINEMERGE = false eine Lösung für das Problem des Kunden.

Auflösung

1. Aktivieren Sie CPU-Zeitmetriken für agg_processor für Debuggingzwecke, indem Sie limits.conf wie folgt ändern:

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

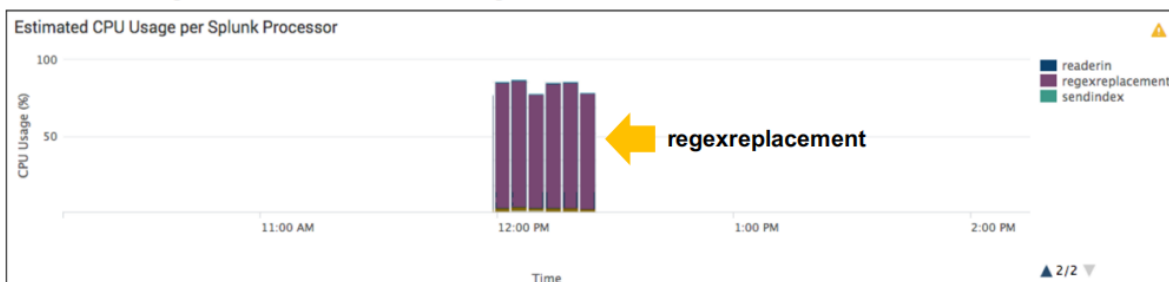
2. Führen Sie die unten stehende Suche aus, um den Quelltyp zu identifizieren, der den Aggregator-Prozessor stärker unter Druck setzt:

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

3. SHOULD_LINEMERGE auf "false" setzen und einen Regex für "LINE_BREAKER" für jeden Quelltyp schreiben, der in das Suchdiagramm eingeht. Exp ist unten, die ich nahm es aus dem Troubleshooting Training Dokument.

Anmerkung: Screenshot zeigt die Suche nach einem Regex-Prozessor:

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. Durch das Beheben aller Quellentypen wird das Problem der Warteschlangenfüllung gelöst.

Zusätzliche Ressource:

Das folgende Video aus der [Community-Geschäftszeit](#) zeigt detailliertere Informationen zur Fehlerbehebung bei blockierten Warteschlangen.

Verwandte Links

Limits.conf Handbuch

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

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.