

ブロックされたイベント処理キュー

適用性

Splunkエンタープライズ

説明

一部のデータをインデクサに直接オンボーディングし、一部のソースはヘビーフォワード経由でデータを送信しています。

調査

1. splunkd.log に、いくつかのソースタイプの改行エラーとAggregatorMiningProcessorエラーが含まれています。

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

2. [インデックスパフォーマンスダッシュボード](#)に、Splunkプロセスサが高いCPUを使用している「アグリゲータ」が表示されます。
3. エラーを引き起こしていたソースタイプを修正しても解決しなかった（エラーが消え、問題が残る）。
4. 集計キューにボトルネックが存在する場合、pstackは、集計プロセスサが行を1つのイベントにマージしてボトルネックを作成するビジー状態であることを示します。

この問題は、アグリゲーションプロセスサが多数の回線を1つのイベントにマージする場合に発生します。このコードでは、現在のイベントにマージする必要がある行が1行ある場合は常に、次のコードのようにstring::reserveとメモリ移動が発生します。したがって、1つのイベントに対して1000行がある場合、reserveおよびmemmovecalledは1000回発生します。

```
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);
...
}

```

多数の行を含むサンプルイベントの一部を収集して問題の原因となっているイベントを特定し、行の総数が多い上位3つのソースタイプを特定します。

```

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

```

概念:

その理由は次のとおりです。

- 通常、解析キューは1番目のキューとして、集約キューは2番目のキューとして使用します。
- parsing queueは、LINE_BREAKERが定義されていない場合に、ストリーミングデータをデフォルト文字\\nで行に解析することです。
- その後、集約キューはTIME_FORMATなどの設定に基づいて回線をマージします
- LINE_BREAKERを設定することで、ストリーミングデータを解析する方法を解析フェーズの行にSplunkに指示できます。
- SHOULD_LINEMERGE = falseを設定すると、集計プロセスで行をイベントにマージしないように指定されます。
- したがって、基本的にLINE_BREAKERとSHOULD_LINEMERGE = falseが、お客様の問題の解決策となります。

解決方法

1. デバッグ用にagg_processorのCPU時間メトリックを有効にするには、limits.conf を次のように変更します。

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

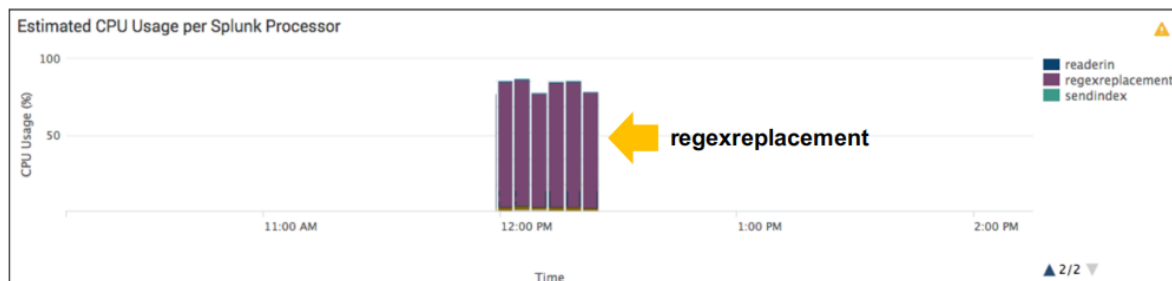
2. 次の検索を実行して、アグリゲータプロセッサの負荷が高まっているソースタイプを特定します。

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

3. SHOULD_LINEMERGEを「false」に設定し、検索グラフに入ってくるソースタイプごとに「LINE_BREAKER」の正規表現を書き込みます。Expは、トラブルシューティングトレーニングドキュメントから取得した値の下にあります。

注：スクリーンショットは、正規表現プロセッサの検索を示しています。

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. このようなソースタイプをすべて修正すると、キューの埋め込みの問題が解決されます。

その他のリソース：

次の[コミュニティオフィス時間](#)のビデオでは、ブロックされたキューのトラブルシューティングについて詳しく説明します。

関連リンク

Limits.confマニュアル

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。