

ثادحال ةجلاعم راضتنا مئاق رطح مت

قيبطتلا ةيلباق

Splunk ةسسؤم

فصولا

تانايبل لاسراب رداصملا ضعب موقتو، نيسرهفملا ىلإ ةرشابم تانايبل ضعب ةفاضلا
نيلقثلا ةمدخلل يدوزم ربع.

ءالجتسا

للق ددعل AggregatorMiningProcessor و روطسلا ميسقت في ءاطخا كانه splunkd.log في 1.
رداصملا عاونأ نم.

```
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. ةدحول ةيلاع ةجلاعم ىقلتي "عمجمل" ميسقت جلاعم [ةسرهفلا ءادأ تامولعم ةحول](#) رهظت.
ةيزكرملا ةجلاعملا.

3. تيقبو، ءاطخالا زواجت مت) ءاطخالا ببست يتلا رداصملا عاونأ حالصا لج متي مل.
(ةلكشملا).

4. جمذب لوغشم عيجمجتلا جلاعم نأ pstack رهظي، عيجمجتلا راضتنا مئاق في ماحدزا كانه.
ماحدزا ثودح ىلإ يدؤي امم، دحاو ثدح في طوطخل.

نم. دحاو ثدح في طوطخل نم ريبك ددع جمذب عيجمجتلا جلاعم موقي امदन ةلكشملا هذه ثدحت
مت: : ةلسلسلا كانه ناك، ةيلالحال ثادحال ىلإ هجمد ىلإ ةجاحب دحاو رطس كانه ناك املك، زمربلا
ثدحل طخ 1000 كانه ناك اذل، اذل. ةيلاتلا ةيجمربلا تاميلعتلاك طايثحلا او ةركاذلا لقن ءارجا
ريكتفلا و طايثحلا نم ةرم 1000 كانه نوكتيس، دحاو.

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

يتمثل ثادحألة ففرعمل، دونبال نم ريبك ددع ىلع يوتحت يتل اةيجزومنل ثادحأل ضعب عمجا ريبك ددع ىلع يوتحي يذلا لوال اةثالل رصملا عون ديدحتل، اةكشملا ثودح يف ببستت اةللامجال طوطخل نم:

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

موفملا:

وه ببسلا

- عيمجت راطتن اةمئاقو ىلوا راطتن اةمئاقك ليلحتل راطتن اةمئاق انيدل نوكي ام اءاع اةيناثلاك.
- يف \r\n يضارتف لكشب طوطخ ىل قفدل تانايب ليلحتل راطتن اةمئاق ليلحت متي LINE_BREAKER. فيرعت مدع اءاح
- وا TIME_FORMAT لثم نيوكتل ىل اءانتسا طوطخل اءمءب عيمجتل راطتن اةمئاق موقت، كلذ دعب اءريغ
- ىل قفدل تانايب عيزوت اةيفي SPLUNK ربخي نأ نكمي، LINE_BREAKER اءاعاب و ليلحتل اءلحرم يف طوطخ
- اءمءل البجي عيمجتل اةيلمع نأ ىل ريشي SHOULD_LINEMERGE = false نييعبب. ثادحأل يف طوطخل
- اءالمعل اةكشملا ل نوكيس SHOULD_LINEMERGE = false و Line_Breaker ساسأل يف اءا

راق

ضارغل agg_processor ل (CPU) اةزكرملا اءلالعمل اءوتقوس يياقم نيكمءب مق 1. يلى امك limit.conf رييغت لالغ نم اءاطأل اءيحصت

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

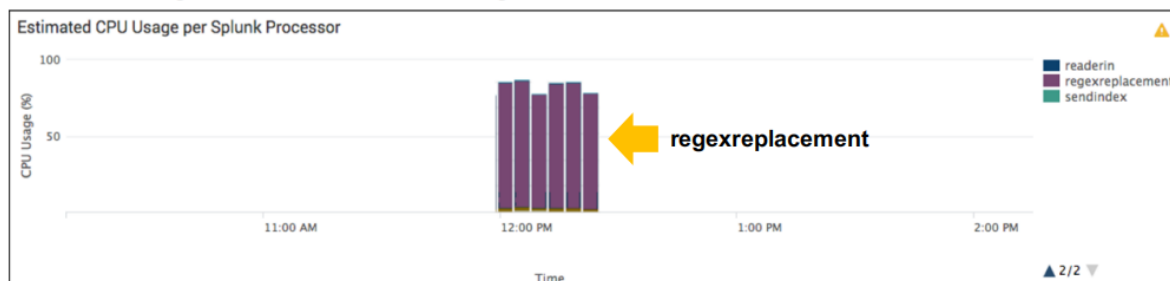
2. جالعام ىلع طغضلا نم ديزملا ضرفي يذلا ردصملا عون ديدحتل هاندأ ثحبلا ليغشتب مق 2. عيجمحتلا:

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

3. لخددي ردصم عون لكل "line_breaker" ل regex ةباتكو "false" ىل SHOULD_LINEMERGE دادعإ. بي ردت دنتسم نم هتذخأ يذلا EXP جم انرب هاندأ دجوي. ثحبلا لينايبلا مسرلا يف اهالصالو تالكشملا فاشكتسا.

regex: جالعام نع ثحبلا حضوت ةشاش ةطقول: ةطحال

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. راطتنالا ةمئاق ةئبعت ةلكشم لىل ك لذل لثم رداصملا عاونأ ةفاك حالصا ي دؤيس.

ي: فاضلاً دروم

فاشكتسأ ةيفيك يف قمعل نم ديزمل **عمتجمل ابتكمتاعاس** نم يلالتا ويديفلا رهظي
 اءال صا ةروط حمل راطت نالا مئوق عا طأ

قلص تا ذ طب اور

LIMIT.conf بېتک

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

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا