

Filas de Processamento de Eventos Bloqueadas

Aplicabilidade

Empresa Splunk

Descrição

A integração de alguns dados diretamente nos Indexadores e algumas fontes estão enviando os dados através de encaminhadores pesados.

Investigação

1. Em splunkd.log há erros de quebra de linha e AggregatorMiningProcessor para alguns tipos de origem.

```
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. O painel [Desempenho de Indexação](#) mostra que o Processador de Splunk do "Agregador" está ocupando muito espaço na CPU.

3. A correção dos tipos de origem que estavam causando os erros não foi resolvida (erros perdidos, o problema permanece).

4. Há um gargalo na fila de agregação, pstack mostra que o processador de agregação está ocupado mesclando as linhas em um evento, criando um gargalo.

Esse problema ocorre quando o processador de agregação está mesclando um grande número de linhas em um único evento. Do código, sempre que houver uma linha que precise ser mesclada com eventos atuais, haveria `string::reserve` e a movimentação de memória aconteceria como o seguinte código. Então, se houvesse 1000 linhas para um evento, haveria 1000 vezes de reserva e `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);
    ...
}
```

Colete alguns exemplos de eventos que contêm o grande número de linhas, para saber quais eventos estão causando o problema, para identificar os três tipos de origem principais que têm um grande número de linhas totais:

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

Conceito:

O motivo é:

- normalmente temos a fila de análise como a primeira fila e a fila de agregação como a segunda.
- a fila de análise deve analisar os dados de streaming em linhas por caractere padrão `\r\n` se não houver `LINE_BREAKER` definido.
- Em seguida, a fila de agregação mesclaria as linhas com base na configuração como `TIME_FORMAT` ou em outras
- Ao configurar `LINE_BREAKER`, ele pode dizer a Splunk como analisar os dados de streaming em linhas na fase de análise e
- Ao definir `SHOULD_LINEMERGE = false`, o processo de agregação não deve mesclar as linhas em eventos.
- Basicamente, `LINE_BREAKER` e `SHOULD_LINEMERGE = false` seriam uma solução para o problema do cliente.

Resolução

1. Ative as métricas de tempo de CPU para agg_processor para fins de depuração alterando o limits.conf da seguinte maneira:

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

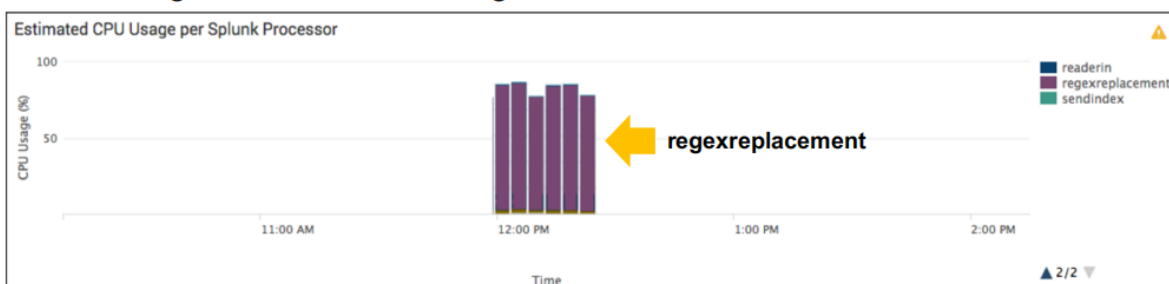
2. Execute a pesquisa a seguir para identificar o tipo de origem que está colocando mais pressão no processador do agregador:

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

3. Definindo SHOULD_LINEMERGE como "false" e escrevendo um regex para "LINE_BREAKER" para cada tipo de fonte que entra no gráfico de pesquisa. Exp está abaixo do qual eu tomei do documento de treinamento Troubleshooting.

Note: A captura de tela mostra a busca pelo processador regex:

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. Corrigir todos os tipos de origem dessa forma resolverá o problema de preenchimento de fila.

Recurso adicional:

O vídeo a seguir, do [horário comercial da comunidade](#), mostra mais detalhes sobre como solucionar problemas de filas bloqueadas.

Links relacionados

Manual Limits.conf

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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.