

Colas de procesamiento de eventos bloqueadas

Aplicabilidad

Splunk Enterprise

Descripción

Incorporación de algunos datos directamente a los indizadores y algunas fuentes están enviando los datos a través de reenviadores pesados.

Investigación

1. En splunkd.log hay errores de linebreaking y AggregatorMiningProcessor para algunos tipos de código fuente.

```
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. El [tablero de indización de rendimiento](#) muestra "Agregador" Splunk Processor está tomando alta CPU.

3. La corrección de los tipos de origen que estaban causando los errores no se resolvió (errores desaparecidos, problema permanece).

4. Hay un cuello de botella en la cola de agregación, pstack muestra que el procesador de agregación está ocupado en la fusión de las líneas en un evento, creando un cuello de botella.

Este problema ocurre cuando el procesador de agregación está combinando un gran número de líneas en un solo evento. Desde el código, cada vez que hay una línea que debe combinarse con eventos actuales, se produciría el movimiento de `cadena::reserve` y memoria como el código siguiente. Así que, si hay 1000 líneas para un evento, habría 1000 veces de `reserva` y `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);
    ...
}
```

Recopile algunos de los eventos de muestra que contienen el gran número de líneas, para saber qué eventos están causando el problema, para identificar los tres tipos de origen principales que tienen un gran número de líneas totales:

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

Concepto:

La razón es:

- normalmente tenemos la cola de análisis como primera cola y la cola de agregación como segunda.
- la cola de análisis es analizar los datos de transmisión en líneas de forma predeterminada con el carácter `\r\n` si no se ha definido `LINE_BREAKER`.
- Luego, la cola de agregación combinaría las líneas basadas en la configuración como `TIME_FORMAT` u otros
- Al configurar `LINE_BREAKER`, puede indicar a Splunk cómo analizar los datos de transmisión en líneas en la fase de análisis y
- Si se establece `SHOULD_LINEMERGE = false`, el proceso de agregación no debería combinar las líneas en eventos.
- Básicamente, `LINE_BREAKER` y `SHOULD_LINEMERGE = false` serían una solución para el problema del cliente.

Resolución

1. Habilite las métricas de tiempo de CPU para agg_processor con fines de depuración cambiando limits.conf de la siguiente manera:

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

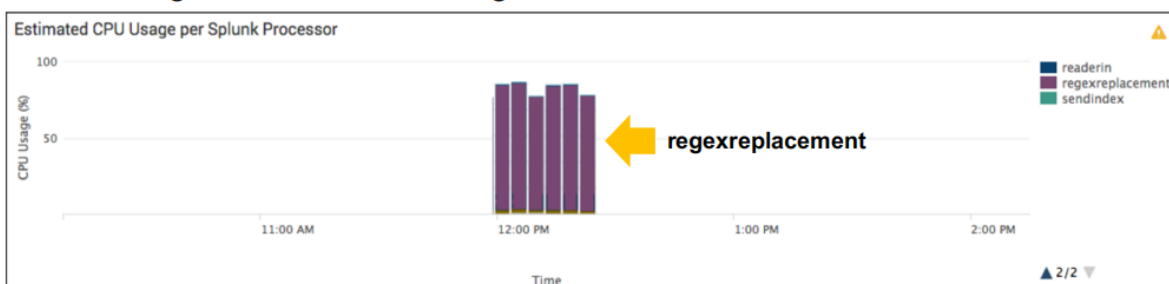
2. Realice la siguiente búsqueda para identificar el tipo de fuente que ejerce más presión sobre el procesador de agregación:

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

3. Establecer SHOULD_LINEMERGE en "false" y escribir un regex para "LINE_BREAKER" para cada tipo de fuente que entra en el gráfico de búsqueda. Exp está por debajo del cual lo tomé del documento de formación de Troubleshooting.

Nota: La captura de pantalla muestra la búsqueda del procesador 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. Corregir todos los tipos de origen como que resolverá el problema de relleno de cola.

Recurso adicional:

El siguiente vídeo de [Community Office hours](#) muestra más a fondo cómo resolver problemas de colas bloqueadas.

Enlaces relacionados

Manual de Limits.conf

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).