

Code di elaborazione eventi bloccate

Applicabilità

Splunk Enterprise

Descrizione

L'onboarding di alcuni dati direttamente agli indicizzatori e alcune fonti stanno inviando i dati tramite pesanti server d'inoltro.

Indagine

1. In splunkd.log si verificano errori linebreaking e AggregatorMiningProcessor per pochi tipi di origine.

```
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. Il [dashboard delle prestazioni di indicizzazione](#) mostra che "Aggregator" Splunk Processor sta utilizzando una CPU elevata.

3. La correzione dei tipi di origine che causavano gli errori non è stata risolta (errori non più presenti, problema rimanente).

4. È presente un collo di bottiglia nella coda di aggregazione. Pstack indica che il processore di aggregazione è occupato nell'unire le linee in un evento, creando un collo di bottiglia.

Questo problema si verifica quando il processore di aggregazione sta unendo un numero elevato di righe in un singolo evento. Dal codice, ogni volta che è presente una riga che deve essere unita agli eventi correnti, si verificherebbe lo spostamento di `stringa::reserve` e memoria come il codice seguente. Quindi, se ci sono 1000 linee per un evento, ci sarebbero 1000 volte di riserva e memoria richiamati.

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

Raccogliere alcuni eventi di esempio che contengono il numero elevato di righe, per individuare gli eventi che causano il problema e identificare i primi tre tipi di origine che contengono un numero elevato di righe totali:

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

Concetto:

Il motivo è:

- la coda di analisi è in genere la prima coda e la coda di aggregazione la seconda.
- L'analisi della coda consiste nell'analizzare i dati di flusso in righe per impostazione predefinita \r\n se non è stato definito LINE_BREAKER.
- Quindi, la coda di aggregazione unisce le linee in base alla configurazione likeTIME_FORMAT o altre
- Impostando LINE_BREAKER, è possibile indicare a Splunk come analizzare i dati di streaming in linee nella fase di analisi e
- Se si imposta il parametro SHOULD_LINEMERGE = false, il processo di aggregazione non deve unire le righe in eventi.
- In pratica, LINE_BREAKER e SHOULD_LINEMERGE = false rappresentano una soluzione per il problema del cliente.

Risoluzione

1. Abilitare le metriche del tempo CPU per agg_processor a scopo di debug modificando il file limits.conf come segue:

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

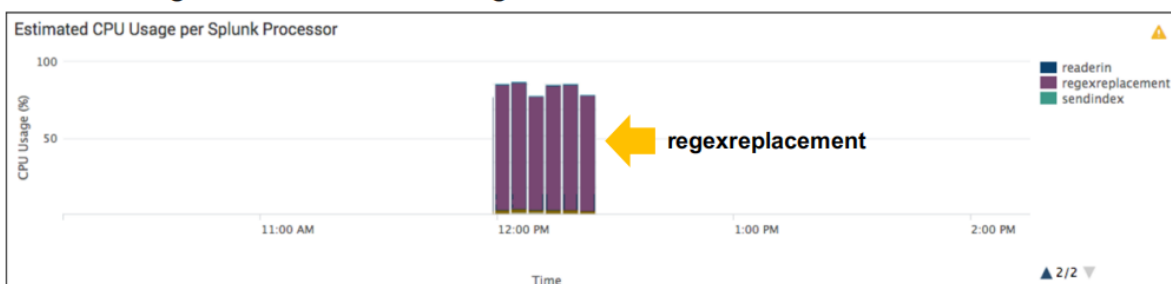
2. Eseguire la ricerca seguente per identificare il tipo di origine che sta facendo più pressione sul processore dell'aggregatore:

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

3. Impostazione di SHOULD_LINEMERGE su "false" e scrittura di un regex per "LINE_BREAKER" per ogni tipo di origine in arrivo nel grafico di ricerca. Exp è al di sotto del quale ho preso dal documento di formazione per la risoluzione dei problemi.

Nota: Screenshot mostra come cercare il processore 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. Correggendo tutti i tipi di origine come questo risolverà il problema di riempimento della coda.

Ulteriori risorse:

Il video che segue, relativo alle [ore d'ufficio delle comunità locali](#), illustra in modo più approfondito come risolvere i problemi relativi alle code bloccate.

Collegamenti correlati

Limits.conf Manuale

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).