

Files d'attente de traitement des événements bloquées

Applicabilité

Splunk Enterprise

Description

L'intégration de certaines données directement aux indexeurs et certaines sources envoient les données via des redirecteurs lourds.

Enquête

1. Dans `splunkd.log`, il y a des erreurs de saut de ligne et `AggregatorMiningProcessor` pour quelques types de source.

```
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. Le [tableau de bord des performances d'indexation](#) indique que le processeur de liaison principale « Aggregator » prend une CPU élevée.

3. La correction des types de source qui causaient les erreurs n'a pas été résolue (erreurs passées, problème persistant).

4. Il y a un goulot d'étranglement dans la file d'attente d'agrégation, `pstack` montre que le processeur d'agrégation est occupé à fusionner les lignes en un seul événement, créant ainsi un goulot d'étranglement.

Ce problème se produit lorsque le processeur d'agrégation fusionne un grand nombre de lignes en un seul événement. À partir du code, chaque fois qu'une ligne doit être fusionnée avec les événements actuels, il y a `string::reserve` et le déplacement de mémoire se produit comme le code suivant. Donc, s'il y a 1000 lignes pour un événement, il y aurait 1000 fois de `reserve` et `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);
    ...
}
```

Recueillez des exemples d'événements qui contiennent le grand nombre de lignes, pour savoir quels événements sont à l'origine du problème, afin d'identifier les trois principaux types d'origine qui ont un grand nombre de lignes totales :

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

Concept :

La raison en est :

- nous avons normalement la file d'attente d'analyse comme première file d'attente et la file d'agrégation comme seconde.
- La file d'attente d'analyse est utilisée pour analyser les données en continu en lignes par le caractère par défaut `\r\n` si aucun `LINE_BREAKER` n'est défini.
- Ensuite, la file d'attente d'agrégation fusionnerait les lignes en fonction de la configuration comme `TIME_FORMAT` ou d'autres
- En définissant `LINE_BREAKER`, il peut indiquer à Splunk comment analyser les données en continu en lignes dans la phase d'analyse et
- Si `SHOULD_LINEMERGE = false`, le processus d'agrégation ne doit pas fusionner les lignes en événements.
- Donc, en gros, `LINE_BREAKER` et `SHOULD_LINEMERGE = false` serait une solution pour le problème du client.

Résolution

1. Activez les mesures de temps UC pour agg_processor à des fins de débogage en modifiant le fichier limits.conf comme suit :

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

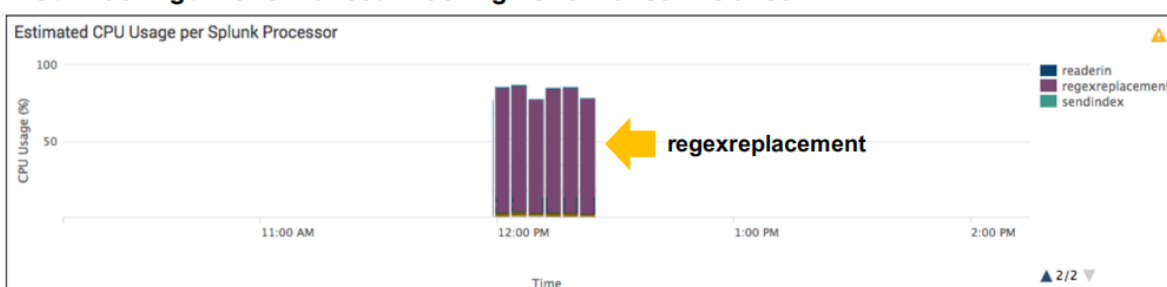
2. Exécutez la recherche ci-dessous pour identifier le type de source qui exerce une pression plus forte sur le processeur d'agrégation :

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

3. Réglez SHOULD_LINEMERGE sur "false" et écrivez une expression régulière pour "LINE_BREAKER" pour chaque type de source entrant dans le graphique de recherche. Exp est ci-dessous que je l'ai pris du document de formation Dépannage.

Remarque : Capture d'écran montrant la recherche du processeur 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. Réparer tous les types de source comme cela résoudra le problème du remplissage de la file d'attente.

Ressource supplémentaire :

La vidéo ci-dessous, tirée des [heures de bureau de la communauté](#), explique plus en détail comment dépanner les files d'attente bloquées.

Liens connexes

Limits.conf Manuel

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.