O Uso do Espaço em Disco do Indexador de Splunk Está em 100%

Aplicabilidade

Empresa Splunk

Descrição

Este artigo descreve um cenário em que os indexadores clusterizados não habilitados para SmartStore estão sem espaço em disco. As soluções fornecidas aqui são opções simples para fornecer algum alívio imediato, que pode não ser aplicável em todos os ambientes.

Alguns deles também podem ser aplicados a ambientes sem cluster.

Essas etapas não se aplicam a ambientes habilitados para SmartStore.

Investigação

Como identificar:

1. Os indexadores estão ficando sem espaço, impedindo que os dados sejam rolados, e nenhum dado novo é ingerido.
2. Os indexadores nesta implantação são agrupados, com dados quentes/quentes e frios localizados em pontos de montagem separados
3. Alguns ou todos os índices não são gerenciados por volume.
4. `maxVolumeDataSizeMB` está configurado, mas como alguns ou todos os índices não são gerenciados por volume, ele não restringe o uso do disco para todos os índices que não estão usando volume (por exemplo, `homePath = $SPLUNK_DB/xxx`)
5. Erros vistos no splunkd.log:

```
WARN ProcessTracker - (child_130__RollFixMetadata) IndexConfig - idx=index_name Pat
(realpath '/opt/coldstore/index_name/colddb') is inside volume=cold (path='/opt/col
not reference that volume. Space used by coldPath will *not* be volume-mananged. Pl
```

6. Se forem feitas alterações em indexes.conf no Gerenciador de Cluster, as tentativas de

envio por push resultarão em erros de envio de pacote, indicando que os indexadores não podem descompactar devido à falta de espaço na unidade.

Resolução

Como corrigi-lo:

Libere espaço em disco permitindo que os indexadores calculem corretamente o uso real de todos os índices e, se necessário, elimine a replicação de índices não essenciais no cluster.

As etapas a seguir sugerem a aplicação de alterações de configuração apropriadas a `indexes.conf` no Gerenciador de Cluster no local apropriado no diretório `manager-apps` (ou `master-apps`, dependendo de onde os aplicativos do seu indexador estão armazenados), depois fazendo as mesmas alterações manualmente (ou implantadas via automação, como Puppet ou Ansible) na pasta correspondente dos indexadores `peer-apps`.

NOTE: A maioria dos administradores está acostumada a colocar configurações em `$SPLUNK_HOME/etc/system/local`. No entanto, para indexadores clusterizados, as configurações em `$SPLUNK_HOME/etc/system/local` são substituídas por qualquer item encontrado no diretório peer-apps do indexador.

1. Execute a seguinte pesquisa para identificar índices que não sejam gerenciados por volume:

```
index=_internal sourcetype=splunkd "does not reference that volume" | stats values(idx)
```

2. Na linha de comando do Cluster Manager:
    1. Coloque o cluster no modo de manutenção:

```
/opt/splunk/bin/splunk enable maintenance-mode
```

    2. verifique se as atualizações a seguir foram feitas no arquivo indexes.conf que está sendo distribuído para seus indexadores (em `$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf` ou implantado por meio de um aplicativo personalizado)

1. Confirme se os volumes estão definidos para dados quentes/quentes e frios, e se as configurações estão corretas. O exemplo mostra partições separadas para cada uma, mas isso poderia ser facilmente definido para buckets armazenados em uma única partição. Suas opções de configuração reais podem ser diferentes das opções abaixo.

```
[volume:hotwarm]
path = /mnt/fast_disk
maxVolumeDataSizeMB = 100000[volume:cold]
path = /mnt/big_disk
maxVolumeDataSizeMB = 150000
```

2. Para facilitar a manutenção, a prática recomendada é definir `homePath` e `coldPath` na estrofe `[default]` para aplicar a configuração a todos os índices:

```
[default]
homePath = volume:hotwarm/$_index_name/db
coldPath = volume:cold/$_index_name/colddb
```

3. Verifique as estrofes para cada índice identificado na pesquisa acima e remova todos os valores de homePath ou coldPath (se existirem) nessas estrofes. Isso permitirá que os valores colocados em `[default]` se apliquem a essas estrofes. Posteriormente, quando o problema atual for resolvido e você tiver confirmado que os dados estão sendo salvos corretamente nos volumes dessas estrofes específicas, talvez você queira garantir que `homePath` e `coldPath` não sejam definidos para nenhum outro índice.

4. Se for necessário espaço adicional, considere também desativar a replicação de bucket para índice(s) interno(s). Se você fizer isso, comece apenas com o índice [_internal]. Inclua outros, se for necessário mais espaço. Pisa com cuidado: se algum indexador for perdido, os dados de seus índices internos também serão perdidos.

```
[_internal)
repFactor = 0
```

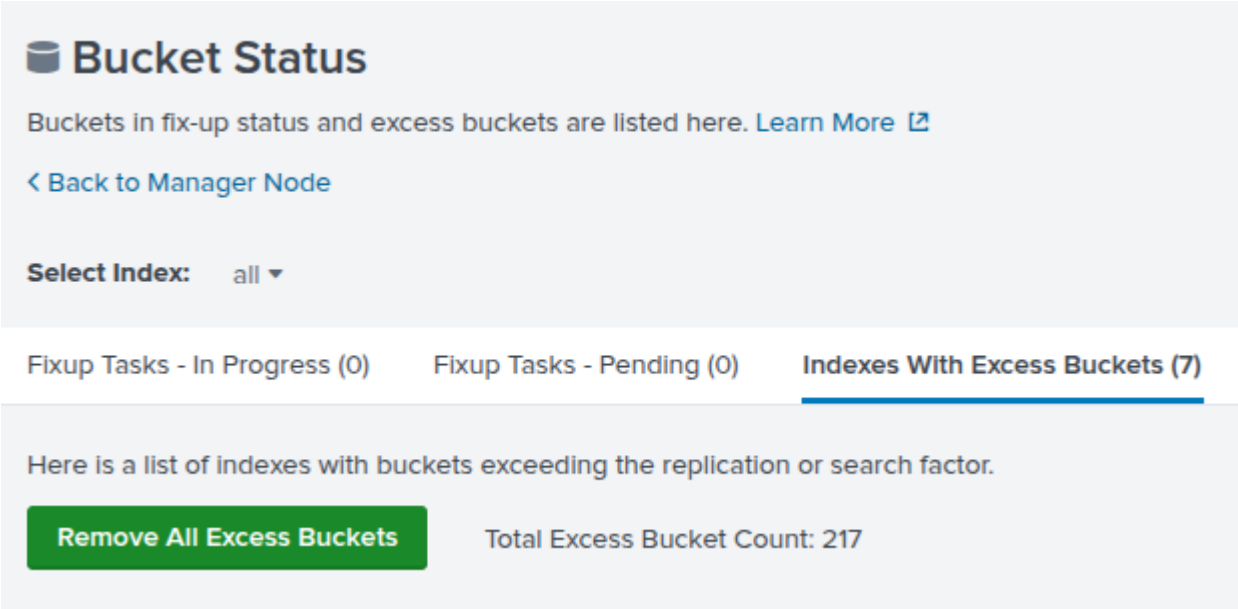
3. Um de cada vez em cada indexador (via linha de comando)

1. Pare o Splunk. Por exemplo:
   `/opt/splunk/bin/splunk stop`
   ou `systemctl stop Splunkd.service`
2. No aplicativo apropriado localizado no diretório `$SPLUNK_HOME/etc/peer-apps` do indexador, faça as mesmas edições em `indexes.conf` que foram aplicadas ao Cluster Manager nas etapas acima.
3. Iniciar Splunk
   `/opt/splunk/bin/splunk start`
   ou `systemctl start Splunkd.service`

4. Vá para o painel Cluster do Indexador do Gerenciador de Cluster (Configurações > Cluster do Indexador) para verificar se todos os indexadores estão ativos e estáveis.
5. Verifique o status do pacote e envie as configurações atualizadas para os indexadores, se necessário.
6. Quando todos os pacotes forem enviados para os indexadores (e os indexadores estiverem estáveis), desabilite o modo de manutenção.

```
/opt/splunk/bin/splunk disable maintenance-mode
```

7. Libere espaço adicional limpando os buckets em excesso.
   1. No painel de instrumentos Clustering de Indexador do Gerenciador de Cluster (Configurações > Clustering de Indexador), vá até a guia Índices e selecione o botão Status do Bucket.
   2. Depois que todas as tarefas de correção tiverem sido limpas (atualize a página para observar correções e atualizações), se a interface do usuário mostrar que há períodos em excesso, clique em Índices com períodos em excesso e selecione o botão Limpar períodos em excesso.



8. Volte para o nó Gerenciador e verifique se os indexadores ainda estão estáveis.

Comandos do Linux que podem ser úteis na solução de problemas:

Mostrar uso do disco:

```
du --max-depth=2 -hc /opt/splunk/var/lib/splunk
```

Classificar por uso de disco da pasta datamodel_summary:

```
du --max-depth=2 -h|grep /opt/splunk/var/lib/splunk --color datamodel_summary|sort
```

Links relacionados

Documentação do 'Splunk':

- Definir volumes em indexes.conf
- Usar variáveis para definir locais de índice
- Ordem de precedência de configuração para indexadores clusterizados

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.