Splunk Indexer schijfruimte gebruik is op 100%

toepasbaarheid

Splunk Enterprise

Beschrijving

In dit artikel wordt een scenario beschreven waarin geclusterde indexeerders zonder SmartStore geen schijfruimte meer hebben. De oplossingen die hier worden aangeboden, zijn eenvoudige opties om onmiddellijke verlichting te bieden, die mogelijk niet in alle omgevingen van toepassing is.

Sommige van deze kunnen ook worden toegepast op niet-geclusterde omgevingen.

Deze stappen zijn niet van toepassing op SmartStore-omgevingen.

onderzoek

Hoe te identificeren:

1. Indexeerders hebben bijna geen ruimte meer, waardoor gegevens niet meer kunnen worden uitgerold en er geen nieuwe gegevens meer worden opgenomen.
2. Indexeerders bij deze implementatie zijn geclusterd, waarbij warme en koude gegevens zich op afzonderlijke koppelpunten bevinden
3. Sommige of alle indexen worden niet volumebeheerd.
4. `maxVolumeDataSizeMB` is geconfigureerd, maar omdat sommige of alle indexen geen volumebeheer hebben, wordt het schijfgebruik niet beperkt voor alle indexen die geen volume gebruiken (bijv. `homePath = $SPLUNK_DB/xxx`)
5. Fouten gezien in 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. Als er wijzigingen worden aangebracht in indexes.conf op Cluster Manager, resulteren pogingen om te pushen in bundelpushfouten die aangeven dat indexeerders niet kunnen

ontkoppelen vanwege een gebrek aan schijfruimte.

resolutie

Hoe het te repareren:

Maak schijfruimte vrij door de indexeerders in staat te stellen het werkelijke gebruik voor alle indexen correct te berekenen en, indien nodig, replicatie van niet-essentiële indexen in het cluster te elimineren.

In de onderstaande stappen wordt voorgesteld om de juiste configuratiewijzigingen toe te passen op `indexes.conf` op de clusterbeheerder op de juiste locatie in de directory `manager-apps` (of `master-apps` afhankelijk van waar apps voor uw indexeerder zijn opgeslagen) en vervolgens dezelfde wijzigingen handmatig aan te brengen (of geïmplementeerd via automatisering zoals Puppet of Ansible) in de bijbehorende `peer-apps`-map van de `indexeerders`.

OPMERKING: De meeste beheerders zijn gewend om configuraties te plaatsen in `$SPLUNK_HOME/etc/system/local`. Voor geclusterde indexeerders worden de instellingen in `$SPLUNK_HOME/etc/system/local` echter overschreven door alles wat in de peer-apps-directory van de indexeerder wordt gevonden.

1. Voer de volgende zoekopdracht uit om indexen te identificeren die niet volumebeheerd worden:

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

2. Vanuit de opdrachtregel van Clusterbeheer:
    1. Plaats het cluster in de onderhoudsmodus:

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

    2. Controleer of de volgende updates zijn uitgevoerd in het bestand indexes.conf dat wordt gedistribueerd naar uw indexers (in `$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf` of geïmplementeerd via een aangepaste app)
        1. Bevestig dat volumes zijn gedefinieerd voor warme en koude gegevens en dat de

instellingen correct zijn. Voorbeeld toont afzonderlijke partities voor elk, maar dit kan net zo gemakkelijk worden gedefinieerd voor emmers die op een enkele partitie zijn opgeslagen. De werkelijke instellingskeuzes kunnen afwijken van onderstaande.

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

2. Voor het onderhoudsgemak is de beste methode om `homePath` en `coldPath` in de `[standaard]` stanza in te stellen om de configuratie op alle indexen toe te passen:

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

3. Controleer de stanza's voor elke index die is geïdentificeerd in de bovenstaande zoekopdracht en verwijder eventuele homePath- of coldPath-waarden (als deze bestaan) in die stanza's. Hierdoor kunnen de waarden die in `[standaard]` zijn geplaatst op deze strofen van toepassing zijn. Later, zodra het huidige probleem is opgelost en u hebt bevestigd dat de gegevens op de juiste manier worden opgeslagen in de volumes voor deze specifieke strofen, kunt u ervoor zorgen dat `HomePath` en `ColdPath` niet voor andere indexen worden gedefinieerd.

4. Als er extra ruimte nodig is, kunt u ook overwegen om emmerreplicatie uit te schakelen voor interne index(en). Als je dit doet, begin dan met de [_internal] index. Voeg anderen toe als er meer ruimte nodig is. Loop voorzichtig: als een indexer verloren gaat, gaan ook gegevens van de interne indexen verloren.

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

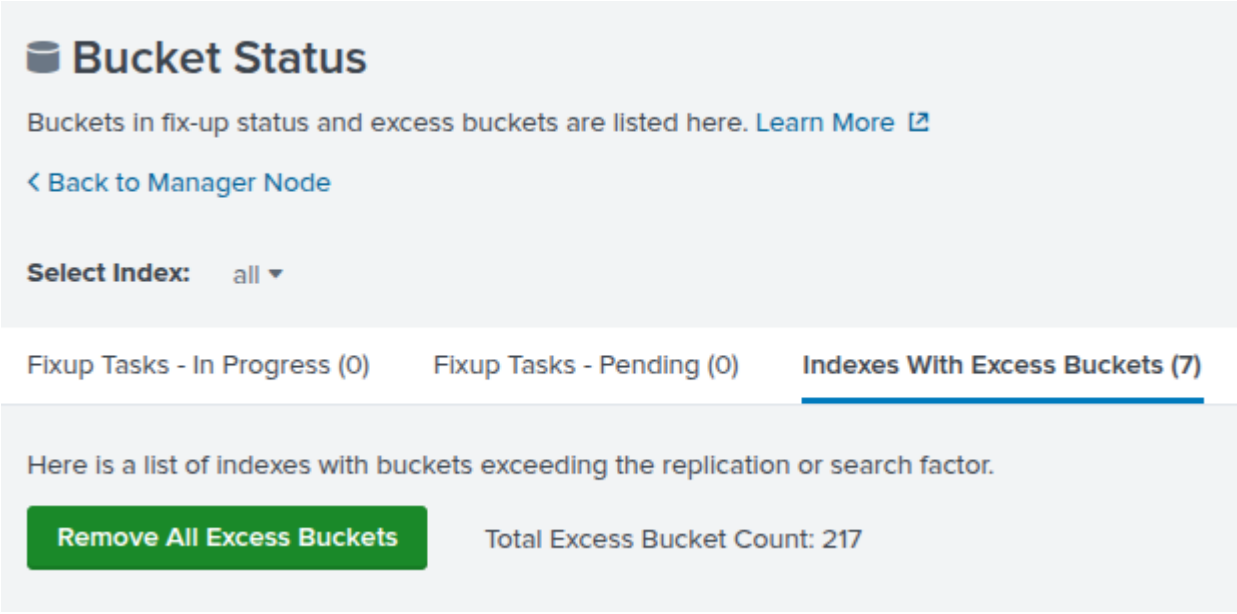
3. Eén voor één op elke indexeerder (via opdrachtregel)

    1. Stop Splunk. Voorbeeld:
    `/opt/splunk/bin/splunk stop`

of, `Splunked.service systematisch stoppen`
2. In de juiste app in de directory `$SPLUNK_HOME/etc/peer-apps van` de indexeerder, voert u dezelfde bewerkingen uit op `indexes.conf` als in de bovenstaande stappen op Clusterbeheer zijn toegepast.
3. Splunk starten
   `/opt/splunk/bin/splunk start`
   of `Splunkd.service systematisch starten`
4. Ga naar het indexerclusteringdashboard van de clusterbeheerder (Instellingen > Indexerclustering) om te controleren of alle indexeerders up-and-stable zijn.
5. Controleer de bundelstatus en duw de bijgewerkte configuraties zo nodig naar de indexeerders.
6. Zodra alle bundels naar de indexeerders zijn geduwd (en indexeerders stabiel zijn), schakelt u de onderhoudsmodus uit.

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

7. Maak extra ruimte vrij door overtollige emmers op te ruimen.
   1. Ga in het dashboard voor indexclustering van clusterbeheer (Instellingen > Indexerclustering) naar het tabblad Indexen en selecteer de knop Bucket Status.
   2. Zodra alle reparatietaken zijn gewist (vernieuw de pagina om de reparatie-update te bekijken), als de gebruikersinterface laat zien dat er overtollige emmers zijn, klikt u op Indexen met overtollige emmers, selecteert u de knop Overtollige emmers wissen.



8. Ga terug naar de Manager Node en controleer of de indexeerders nog stabiel zijn.

Linux-opdrachten die nuttig kunnen zijn bij het oplossen van problemen:

Schijfgebruik weergeven:

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

Sorteer op schijfgebruik van de map datamodel_summary:

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

Gerelateerde links

Splunk-documentatie:

- Volumes definiëren in indexen.conf
- Variabelen gebruiken om indexlocaties te definiëren
- Configuratievolgorde van voorrang voor geclusterde indexeerders

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.