Utilizzo dello spazio su disco dell'indicizzatore di splunk pari al 100%

Applicabilità

Splunk Enterprise

Descrizione

In questo articolo viene descritto uno scenario in cui gli indicizzatori cluster non abilitati per SmartStore hanno esaurito lo spazio su disco. Le soluzioni qui fornite sono semplici opzioni per fornire un po 'di soccorso immediato, che potrebbe non essere applicabile in tutti gli ambienti.

Alcuni di questi possono essere applicati anche ad ambienti non cluster.

Questi passaggi non sono applicabili agli ambienti abilitati per SmartStore.

Indagine

Come identificare:

1. Lo spazio degli indicizzatori si sta esaurendo, impedendo il rolloff dei dati e l'acquisizione di nuovi dati non viene eseguita.
2. Gli indicizzatori in questa distribuzione sono raggruppati, con dati caldi/caldi e freddi collocati in punti di montaggio separati
3. Alcuni o tutti gli indici non sono gestiti dal volume.
4. `maxVolumeDataSizeMB` è configurato, ma poiché alcuni o tutti gli indici non sono gestiti dal volume, non limita l'utilizzo del disco per tutti gli indici che non utilizzano il volume (ad esempio, `homePath = $SPLUNK_DB/xxx`)
5. Errori 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. Se vengono apportate modifiche a indexes.conf in Gestione cluster, i tentativi di push

determineranno errori di push del bundle che indicano che gli indicizzatori non sono in grado di annullare l'operazione a causa di spazio insufficiente sull'unità.

Risoluzione

Come risolvere il problema:

Liberare spazio su disco consentendo agli indicizzatori di calcolare correttamente l'utilizzo effettivo per tutti gli indici e, se necessario, eliminare la replica degli indici non essenziali nel cluster.

La procedura riportata di seguito suggerisce di applicare le modifiche di configurazione appropriate al file `indexes.conf` in Gestione cluster nel percorso appropriato all'interno della directory `manager-apps` (o `master-apps` a seconda di dove sono archiviate le app per l'indicizzatore), quindi di apportare manualmente le stesse modifiche (o distribuirle tramite automazione, ad esempio Puppet o Ansible) alla cartella `peer-apps corrispondente degli indicizzatori`.

NOTA: La maggior parte degli amministratori è abituata a posizionare le configurazioni in `$SPLUNK_HOME/etc/system/local`. Tuttavia, per gli indicizzatori cluster, le impostazioni in `$SPLUNK_HOME/etc/system/local` vengono sostituite da qualsiasi elemento trovato nella directory peer-apps dell'indicizzatore.

1. Eseguire la ricerca seguente per identificare gli indici non gestiti da volume:

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

2. Dalla riga di comando di Gestione cluster:
    1. Impostare il cluster in modalità di manutenzione:

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

    2. verificare che siano stati eseguiti i seguenti aggiornamenti al file indexes.conf distribuito agli indicizzatori (in `$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf` o distribuito tramite un'app personalizzata)
        1. Verificare che i volumi siano definiti per i dati relativi alle temperature elevate/calde e fredde e che le impostazioni siano corrette. In questo esempio

vengono illustrate partizioni separate per ciascuna di esse, ma è possibile definirle con la stessa facilità per i bucket archiviati in una singola partizione. Le opzioni di impostazione effettive potrebbero essere diverse da quelle riportate di seguito.

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

2. Per semplificare la manutenzione, è consigliabile impostare `homePath` e `coldPath` nella stanza `[default]` per applicare la configurazione a tutti gli indici:

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

3. Controllare le stanze per ogni indice identificato dalla ricerca precedente e rimuovere eventuali valori homePath o coldPath (se esistenti) in tali stanze. In questo modo, i valori inseriti in `[default]` verranno applicati a queste stanze. In seguito, una volta risolto il problema corrente e verificato che i dati vengono salvati correttamente nei volumi per queste stanze specifiche, è possibile accertarsi che `homePath` e `coldPath` non siano definiti per altri indici.
4. Se è necessario ulteriore spazio, è consigliabile disabilitare anche la replica di bucket per gli indici interni. In questo caso, iniziate solo con l'indice [_internal]. Se è necessario più spazio, includerne altri. Tread con attenzione: in caso di perdita di un indicizzatore, vengono perduti anche i dati degli indici interni.

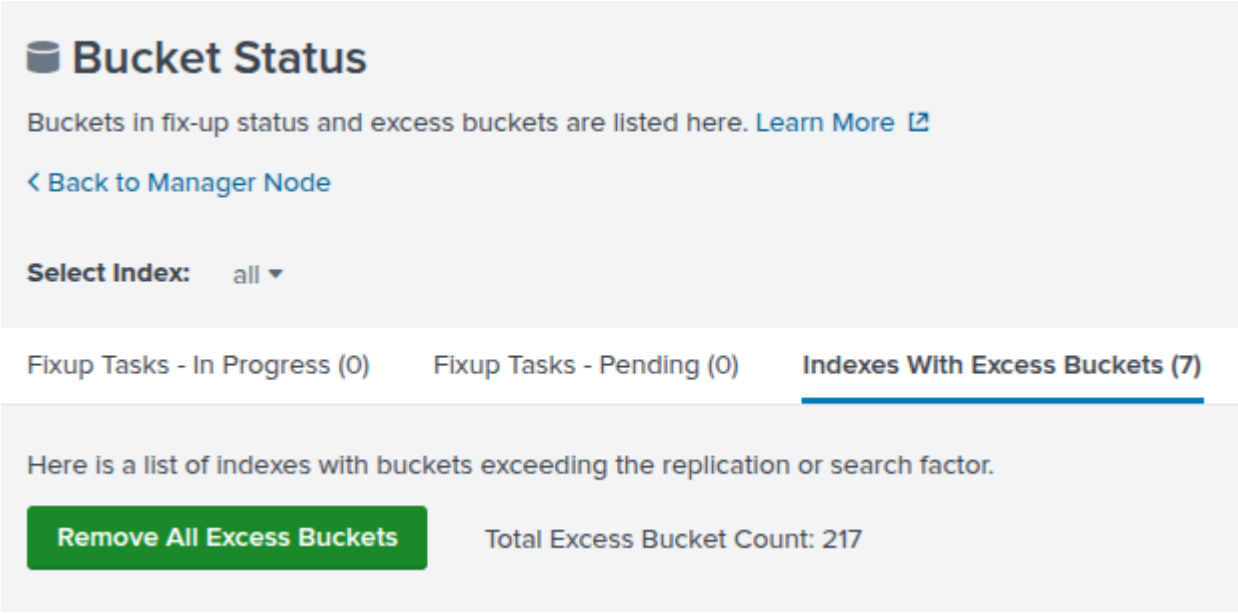
```
[_internal)
repFactor = 0
```

3. Uno alla volta su ogni indicizzatore (tramite riga di comando)
    1. Arrestare Splunk. Ad esempio:
    `/opt/splunk/bin/splunk stop`
    oppure, `systemctl stop Splunkd.service`

2. Nell'app appropriata disponibile nella directory `$SPLUNK_HOME/etc/peer-apps` dell'indicizzatore, apportare le stesse modifiche a `indexes.conf` applicate a Cluster Manager nei passaggi precedenti.
3. Avvia Splunk
   `/opt/splunk/bin/splunk start`
   oppure, `systemctl start Splunkd.service`
4. Passare al dashboard Clustering indicizzatore di Gestione cluster (Impostazioni > Clustering indicizzatore) per verificare che tutti gli indicizzatori siano attivi e stabili.
5. Controllare lo stato del bundle ed eseguire il push delle configurazioni aggiornate negli indicizzatori, se necessario.
6. Dopo aver eseguito il push di tutti i bundle agli indicizzatori (e gli indicizzatori sono stabili), disabilitare la modalità di manutenzione.

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

7. Liberare spazio aggiuntivo eliminando i periodi fissi in eccesso.
   1. Dal dashboard Clustering indicizzatore di Gestione cluster (Impostazioni > Clustering indicizzatore), andare alla scheda Indici e selezionare il pulsante Stato bucket.
   2. Una volta cancellati tutti i task di correzione (aggiornare la pagina per controllare l'aggiornamento delle correzioni), se l'interfaccia utente indica la presenza di periodi fissi in eccesso, fare clic su Indici con periodi fissi in eccesso, quindi selezionare il pulsante Cancella periodi fissi in eccesso.



8. Tornare al nodo Manager e verificare che gli indicizzatori siano ancora stabili.

Comandi Linux che possono essere utili per la risoluzione dei problemi:

Mostra utilizzo disco:

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

Ordina per uso disco della cartella datamodel_summary:

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

Collegamenti correlati

Documentazione di Splunk:

- Definire i volumi in indexes.conf
- Utilizzare le variabili per definire le posizioni dell'indice
- Ordine di precedenza della configurazione per gli indicizzatori cluster

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).