Splunk Indexer磁碟空間使用率為100%

適用性

Splunk企業版

說明

本文描述了一個這樣的情況：啟用群集的非SmartStore索引器磁碟空間不足。此處提供的解決方案只是一些簡單的選項，可以立即緩解壓力，這可能不適用於所有環境。

其中一些也適用於非群集環境。

這些步驟不適用於支援SmartStore的環境。

調查

如何識別：

1. 索引器空間不足，導致資料無法滾動，並且沒有新資料被攝取。
2. 此部署中的索引器是群集的，熱/熱和冷資料位於不同的安裝點上
3. 部分或全部索引不是卷管理的。
4. 已配置maxVolumeDataSizeMB，但由於某些或全部索引不是卷管理的，因此它不會限制未使用卷的所有索引的磁碟使用率(例如homePath = $SPLUNK_DB/xxx)
5. splunkd.log中顯示的錯誤：

```
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. 如果在群集管理器的indexes.conf中進行了更改，嘗試推送將導致捆綁推送錯誤，指示索引器由於缺少驅動器空間而無法解除安裝。

解析

如何修復：

通過允許索引器正確計算所有索引的實際使用量，從而釋放磁碟空間，並且，如果需要，可以消除群集內非必要索引的複製。

下面的步驟建議在manager-apps目錄中的適當位置(或master-apps，具體取決於索引器的應用儲存位置)對集群管理器上的indexes.conf應用正確的配置更改，然後手動進行相同的更改(或通過Puppet或Ansible等自動化方式部署到索引器對應的peer-apps資料夾中)。

附註：大多數管理員習慣將配置放入$SPLUNK_HOME/etc/system/local。但是，對於群集索引器，$SPLUNK_HOME/etc/system/local中的設定會被索引器的對等應用目錄中找到的任何內容覆蓋。

1. 運行以下搜尋以標識非卷管理的索引：

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

2. 在Cluster Manager命令列中：
    1. 將群集置於維護模式：

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

    2. 驗證已對分發到索引器的indexes.conf檔案(位於$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf中，或者通過自定義應用進行部署)進行了以下更新
        1. 確認已為熱/熱和冷資料定義卷，並且設定正確。示例顯示了每個的分割槽，但可以同樣輕鬆地為儲存在一個分割槽上的儲存段定義該分割槽。您的實際設定選項可能與以下選項不同。

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

        2. 為便於維護，最佳實踐是在[default]標準中設定homePath和coldPath，以將配置應用到所有索引：

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

3. 檢查從以上搜尋中確定的每個索引的標準，並刪除這些標準中的任何homePath或coldPath值（如果存在）。這將允許放置在[default]中的值應用於這些標準。稍後，解決當前問題並確認資料正正確儲存到這些特定標準的卷後，您可能希望確保沒有為任何其他索引定義homePath和coldPath。

4. 如果需要額外的空間，請考慮同時為內部索引禁用桶複製。 如果這樣做，請只從[_internal]索引開始。如果需要更多空間則包括其它空間。小心行事：如果任何索引器丟失，其內部索引中的資料也會丟失。

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

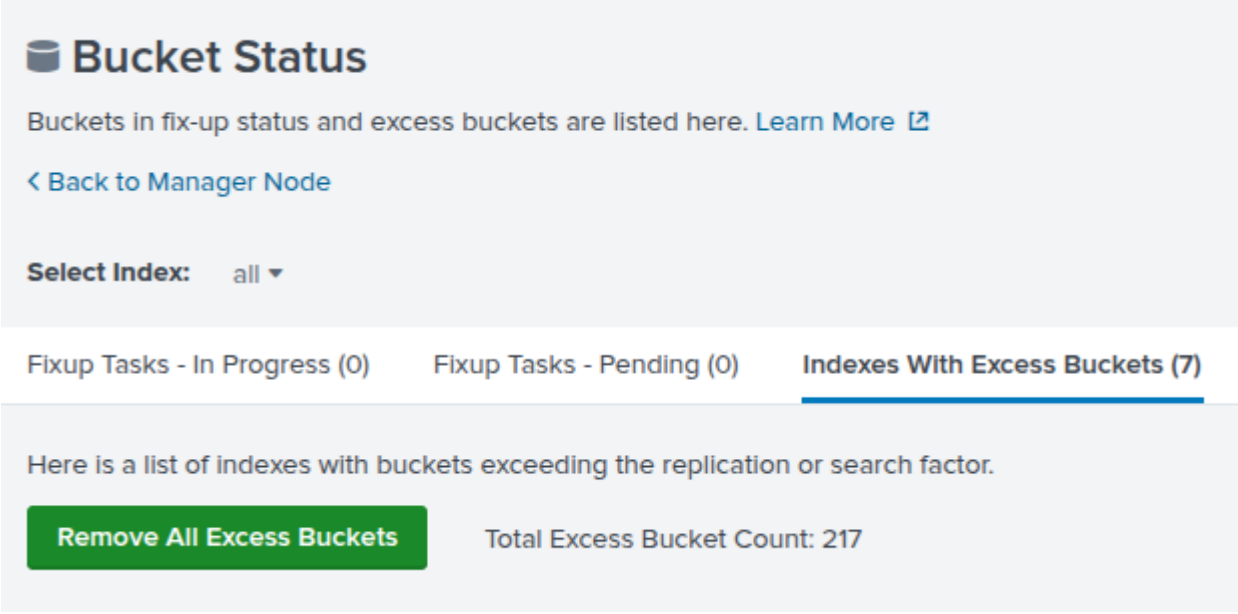
3. 在每個索引器上一次一個（通過命令列）

    1. 停止Splunk。舉例來說：
       `/opt/splunk/bin/splunk stop`
       或者，`systemctl stop Splunkd.service`
    2. 在位於索引器`$SPLUNK_HOME/etc/peer-apps`目錄中的相應應用中，對`indexes.conf`進行與上述步驟中應用於集群管理器的相同的編輯。
    3. 啟動Splunk
       `/opt/splunk/bin/splunk start`
       或者，`systemctl start Splunkd.service`
4. 轉到Cluster Manager的Indexer Clustering控制面板(Settings > Indexer Clustering)，驗證所有索引器是否啟動且穩定。
5. 如果需要，檢查捆綁包狀態並將更新的配置推送到索引器。
6. 將所有捆綁推送到索引器（並且索引器是穩定的）後，禁用維護模式。

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

7. 通過清除多餘儲存桶來釋放額外空間。
    1. 從集群管理器的「索引器集群」控制面板(「設定」>「索引器集群」)中，轉至「索引」頁籤，然後選擇「儲存桶狀態」按鈕。
    2. 清除所有修復任務後（刷新頁面以監視修復更新），如果UI顯示存在超額儲存桶，請按

一下「使用超額儲存桶索引」，然後選擇「清除超額儲存桶」按鈕。



8. 返回Manager節點，驗證索引器是否仍然穩定。

可能對故障排除有用的Linux命令：

顯示磁碟使用情況：

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

按資料模型_summary資料夾的磁碟使用率排序：

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

相關連結

Splunk文檔：

- 在indexes.conf中定義卷
- 使用變數定義索引位置
- 群集索引器的優先順序配置順序

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。