Splunk Indexerのディスク領域の使用率は100%です

適用性

Splunkエンタープライズ

説明

この記事では、クラスタ化された非SmartStore対応インデクサのディスク領域が不足しているシナリオについて説明します。ここで提供されるソリューションは、迅速な対応を可能にするシンプルなオプションであり、すべての環境に適用できるとは限りません。

これらの一部は、非クラスタ環境にも適用できます。

これらの手順は、SmartStoreが有効な環境には適用されません。

調査

識別方法:

1. インデクサの領域が不足しているため、データをロールオフできず、新しいデータが取り込まれません。
2. この導入のインデクサはクラスタ化されており、ホット/ウォームおよびコールドのデータが個別のマウントポイントに配置されています
3. 一部またはすべてのインデックスがボリューム管理されていません。
4. `maxVolumeDataSizeMB`が設定されていますが、一部またはすべてのインデックスがボリューム管理されていないため、ボリュームを使用していないすべてのインデックス（`homePath = $SPLUNK_DB/xxx`など）のディスク使用量は制限されません
5. splunkd.logに次のエラーが見られます。

```
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. Cluster Managerのindexes.confに変更を加えた場合、プッシュを試みるとバンドルプッシュ

エラーが発生し、ドライブの空き容量が不足しているためにインデクサが解凍できないことを示します。

解決方法

修正方法：

インデクサがすべてのインデックスの実際の使用量を正しく計算し、必要に応じて不要なインデックスのクラスタ全体への複製を排除することで、ディスク領域を解放します。

次の手順では、Cluster Managerの`indexes.conf`に`manager-apps`ディレクトリ内の適切な場所（インデクサのアプリケーションが保存されている場所によっては`master-apps`）にある適切な設定変更を適用し、インデクサの対応する`peer-apps`フォルダに同じ変更を手動で（またはPuppetやAnsibleなどの自動化によって）行うことを提案しています。

注：ほとんどの管理者は設定を`$SPLUNK_HOME/etc/system/local`に配置することに慣れています。ただし、クラスタ化されたインデクサの場合、`$SPLUNK_HOME/etc/system/local`の設定は、インデクサのピアアプリケーションディレクトリにある値で上書きされます。

1. 次の検索を実行して、ボリューム管理されていないインデックスを特定します。

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

2. Cluster Managerのコマンドラインから、次の操作を実行します。
    1. クラスタをメンテナンスモードにします。

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

    2. インデクサに配布されるindexes.confファイル（`$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf`内、またはカスタムアプリケーションを介して配備される）に対して、次の更新が行われたことを確認します
        1. ボリュームがホット/ウォームおよびコールドのデータ用に定義され、設定が正しいことを確認します。例は、それぞれに個別のパーティションを示していますが、これは単一のパーティションに格納されているバケットに対して同じように簡単に定義できます。実際の設定は、以下とは異なる場合があります。

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

2. メンテナンスを容易にするため、[default]スタンザでhomePathおよびcoldPathを設定し、設定をすべてのインデックスに適用することがベストプラクティスです。

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

3. 上記の検索で特定された各インデックスのスタンザを確認し、それらのスタンザ内のhomePathまたはcoldPath値（存在する場合）をすべて削除します。これにより、[default]に指定した値がこれらのスタンザに適用されるようになります。後で、現在の問題が解決され、これらの特定のスタンザのボリュームにデータが正しく保存されていることを確認したら、homePathとcoldPathが他のインデックスに対して定義されていないことを確認できます。

4. 追加の領域が必要な場合は、内部インデックスのバケットレプリケーションも無効にすることを検討してください。 これを行う場合は、[_internal]インデックスから開始します。より多くのスペースが必要な場合は、その他を含めます。注意：インデクサが失われた場合、その内部インデックスのデータも失われます。

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

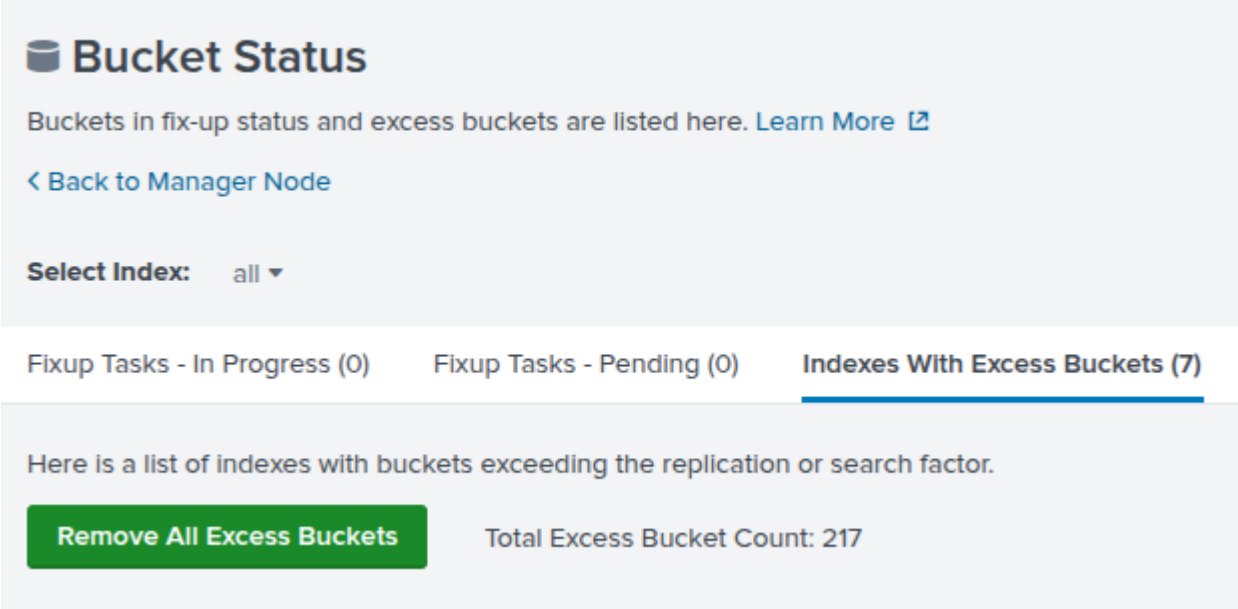
3. 各インデクサで一度に1つずつ（コマンドラインを使用）

1. Splunkを停止します。以下に、いくつかの例を示します。
   `/opt/splunk/bin/splunk stop`
   または、`systemctl stop Splunkd.service`
2. インデクサの$SPLUNK_HOME/etc/peer-appsディレクトリにある適切なアプリケーションで、上記の手順でクラスタマネージャに適用したものと同じ編集をindexes.confに行います。

3. Splunkの開始
   `/opt/splunk/bin/splunk start`
   または、`systemctl start Splunkd.service`
4. Cluster Managerのインデクサクラスタリングダッシュボード(「Settings」 > 「Indexer Clustering」)に移動し、すべてのインデクサが起動していて安定していることを確認します。
5. バンドルステータスを確認し、必要に応じて更新された設定をインデクサにプッシュします。
6. すべてのバンドルがインデクサにプッシュされた（インデクサが安定した）後、メンテナンスモードを無効にします。

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

7. 超過バケットを消去して、追加の領域を解放します。
   1. Cluster ManagerのIndexer Clusteringダッシュボード(Settings > Indexer Clustering)から、Indexesタブに移動し、Bucket Statusボタンを選択します。
   2. すべての修正タスクがクリアされたら（修正の更新を確認するためにページを更新）、超過バケットがあることがUIに表示されている場合は、[超過バケットによるインデックス]をクリックし、[超過バケットのクリア]ボタンを選択します。



8. Manager Nodeに戻り、インデクサが安定していることを確認します。

トラブルシューティングに役立つ可能性があるLinuxコマンド：

ディスク使用量の表示：

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

datamodel_summaryフォルダーのディスク使用量で並べ替え：

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

関連リンク

Splunkのドキュメント：

- indexes.confにボリュームを定義します
- 変数を使用してインデックスの場所を定義する
- クラスタ化インデクサの設定優先順位

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。