Speicherplatznutzung des Splunk-Indexers liegt bei 100 %

Geltungsbereich

Splunk Enterprise

Beschreibung

In diesem Artikel wird ein Szenario beschrieben, in dem geclusterte, nicht SmartStore-fähige Indexer nicht über genügend Speicherplatz verfügen. Bei den hier bereitgestellten Lösungen handelt es sich um einfache Optionen für eine sofortige Entlastung, die möglicherweise nicht in allen Umgebungen anwendbar ist.

Einige davon können auch auf Umgebungen ohne Cluster angewendet werden.

Diese Schritte gelten nicht für SmartStore-fähige Umgebungen.

Untersuchung

So identifizieren Sie:

1. Der Speicherplatz für Indexer wird knapp, sodass kein Rollup der Daten ausgeführt werden kann und keine neuen Daten aufgenommen werden.
2. Indexer in dieser Bereitstellung werden in Clustern zusammengefasst, wobei sich die Warm- und Kaltdaten an separaten Bereitstellungspunkten befinden.
3. Einige oder alle Indizes werden nicht vom Volume verwaltet.
4. `maxVolumeDataSizeMB` ist konfiguriert, aber da einige oder alle Indizes nicht vom Volume verwaltet werden, schränkt dies nicht die Festplattennutzung für alle Indizes ein, die kein Volume verwenden (z. B. `homePath = $SPLUNK_DB/xxx`)
5. Fehler 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. Wenn in "indexes.conf" auf dem Cluster Manager Änderungen vorgenommen werden, führt der Push-Versuch zu Paketpushfehlern, die darauf hinweisen, dass Indexer aufgrund von fehlendem Speicherplatz nicht die Markierung aufheben können.

Auflösung

So beheben Sie es:

Geben Sie Speicherplatz frei, indem Sie den Indexern ermöglichen, die tatsächliche Nutzung für alle Indizes ordnungsgemäß zu berechnen, und wenn nötig, die Replikation nicht wichtiger Indizes im Cluster unterbinden.

In den folgenden Schritten wird empfohlen, `indexes.conf` auf dem Cluster Manager am entsprechenden Speicherort im `manager-apps`-Verzeichnis (oder `master-apps`, je nachdem, wo die Apps für Ihren Indexer gespeichert sind) entsprechend zu konfigurieren, und dann die gleichen Änderungen manuell (oder über Automatisierung wie Puppet oder Ansible) am entsprechenden `peer-apps`-Ordner vorzunehmen.

HINWEIS: Die meisten Administratoren sind es gewohnt, Konfigurationen in $`SPLUNK_HOME/etc/system/local zu platzieren`. Bei gruppierten Indexern werden die Einstellungen in `$SPLUNK_HOME/etc/system/local` jedoch durch alle im Peer-Apps-Verzeichnis des Indexers gefundenen Elemente überschrieben.

1. Führen Sie die folgende Suche aus, um Indizes zu identifizieren, die nicht vom Volume verwaltet werden:

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

2. Über die Befehlszeile des Cluster Manager:
    1. Den Cluster in den Wartungsmodus versetzen:

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

    2. Überprüfen Sie, ob die folgenden Aktualisierungen an der Datei indexes.conf vorgenommen wurden, die an Ihre Indexer verteilt wird (in `$SPLUNK_HOME/etc/manager-`

`apps/_cluster/local/indexes.conf` oder über eine benutzerdefinierte App bereitgestellt).

1. Stellen Sie sicher, dass Volumes für Warm- und Kaltdaten definiert und die Einstellungen korrekt sind. Im Beispiel werden für jede Partition separate Partitionen angezeigt. Dies kann jedoch für auf einer einzelnen Partition gespeicherte Buckets genauso einfach definiert werden. Die tatsächlichen Einstellmöglichkeiten können von den unten angegebenen abweichen.

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

2. Um die Wartung zu vereinfachen, sollten Sie `homePath` und `coldPath` im `[default]` Strophe festlegen, um die Konfiguration auf alle Indizes anzuwenden:

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

3. Überprüfen Sie die Strophen für jeden Index, der aus der oben stehenden Suche identifiziert wurde, und entfernen Sie alle homePath- oder coldPath-Werte (sofern vorhanden) in diesen Strophen. Dadurch können die in `[default]` gesetzten Werte auf diese Strophen angewendet werden. Wenn Sie später das aktuelle Problem behoben haben und bestätigt haben, dass die Daten ordnungsgemäß auf den Volumes für diese spezifischen Strophen gespeichert werden, können Sie sicherstellen, dass `homePath` und `coldPath` nicht für andere Indizes definiert sind.

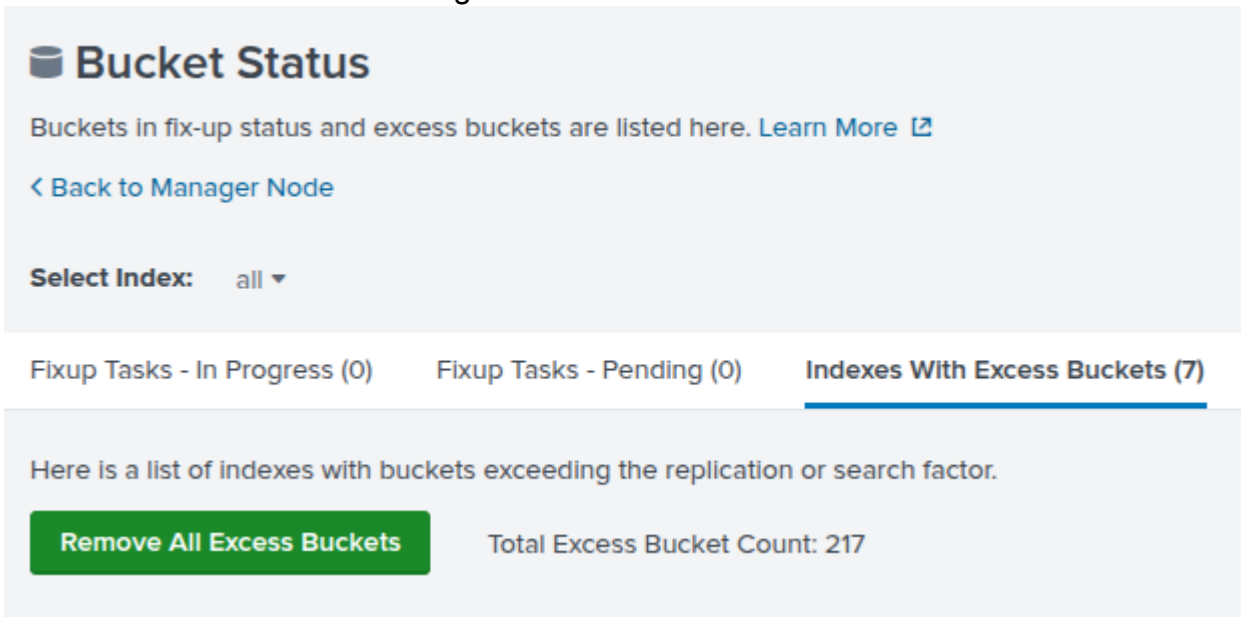
4. Wenn zusätzlicher Speicherplatz benötigt wird, sollten Sie auch die Bucket-Replikation für interne Indizes deaktivieren. Wenn Sie dies tun, beginnen Sie mit nur dem [_internal] Index. Fügen Sie andere hinzu, wenn Sie mehr Platz benötigen. Gehen Sie vorsichtig vor: Wenn ein Indexer verloren geht, gehen auch Daten aus den internen Indizes verloren.

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

3. Jeweils einzeln für jeden Indexer (über Befehlszeile)
    1. Stoppen Sie Splunk. Beispiele:
       `/opt/splunk/bin/splunk stop`
       oder, `systemctl stop Splunkd.service`
    2. Nehmen Sie in der entsprechenden App im Verzeichnis $`SPLUNK_HOME/etc/peer-apps` des Indexers die gleichen Änderungen an `indexes.conf vor`, die Sie in den oben beschriebenen Schritten auf den Cluster Manager angewendet haben.
    3. Splunk starten
       `/opt/splunk/bin/splunk start`
       oder systemctl `Splunkd.service starten`
4. Gehen Sie zum Cluster-Dashboard des Cluster Managers für Indexer-Clustering (Einstellungen > Indexer-Clustering), um zu überprüfen, ob alle Indexer aktiv und stabil sind.
5. Überprüfen Sie den Paketstatus, und übertragen Sie die aktualisierten Konfigurationen bei Bedarf an die Indexer.
6. Wenn alle Pakete an die Indexer weitergeleitet wurden (und die Indexer stabil sind), deaktivieren Sie den Wartungsmodus.

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

7. Geben Sie zusätzlichen Platz frei, indem Sie überschüssige Eimer löschen.
    1. Wechseln Sie im Cluster Manager-Dashboard für Indexer-Clustering (Einstellungen > Indexer-Clustering) zur Registerkarte Indizes, und wählen Sie die Schaltfläche Bucket-Status aus.
    2. Wenn in der Benutzeroberfläche überzählige Buckets angezeigt werden, klicken Sie auf Indizes mit überzähligen Buckets, sobald alle Fix-up-Tasks gelöscht wurden (aktualisieren Sie die Seite, um das Fix-ups-Update zu beobachten), und wählen Sie dann die Schaltfläche Überzählige Buckets löschen aus.



8. Kehren Sie zum Manager-Knoten zurück, und vergewissern Sie sich, dass die Indexer noch stabil sind.

Linux-Befehle, die bei der Fehlerbehebung hilfreich sein können:

Datenträgerverwendung anzeigen:

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

Sortieren nach Datenträgerverwendung des Ordners datamodel_summary:

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

Verwandte Links

Splunk-Dokumentation:

- Definieren von Volumes in indexes.conf
- Variablen zum Definieren von Indexstandorten verwenden
- Konfigurationsreihenfolge für gruppierte Indexer

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.