L'utilisation de l'espace disque du Splunk Indexer est de 100 %

Applicabilité

Splunk Enterprise

Description

Cet article décrit un scénario dans lequel les indexeurs en cluster non compatibles SmartStore manquent d'espace disque. Les solutions présentées ici sont des options simples permettant d'apporter une solution immédiate, qui peut ne pas être applicable dans tous les environnements.

Certaines de ces fonctionnalités peuvent également être appliquées à des environnements non mis en grappe.

Ces étapes ne s'appliquent pas aux environnements SmartStore.

Enquête

Comment identifier :

1. Les indexeurs manquent d'espace, ce qui empêche le transfert des données et empêche l'acquisition de nouvelles données.
2. Les indexeurs de ce déploiement sont mis en grappe, avec des données chaudes/chaudes et froides situées sur des points de montage distincts
3. Certains ou tous les index ne sont pas gérés par un volume.
4. `maxVolumeDataSizeMB` est configuré, mais comme certains ou tous les index ne sont pas gérés par le volume, cela ne limite pas l'utilisation du disque pour tous les index qui n'utilisent pas le volume (par exemple, `homePath = $SPLUNK_DB/xxx`)
5. Erreurs détectées dans 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. Si des modifications sont apportées dans le fichier indexes.conf sur Cluster Manager, les tentatives de transmission entraîneront des erreurs de transmission de l'ensemble indiquant que les indexeurs ne peuvent pas annuler la liaison tar en raison d'un manque d'espace disque.

Résolution

Comment le réparer :

Libérez de l'espace disque en permettant aux indexeurs de prendre en compte correctement le calcul de l'utilisation réelle de tous les index et, si nécessaire, d'éliminer la réplication des index non essentiels dans le cluster.

Les étapes ci-dessous suggèrent d'appliquer les modifications de configuration appropriées à `indexes.conf` sur le Gestionnaire de cluster à l'emplacement approprié dans le répertoire `manager-apps` (ou `master-apps` selon l'endroit où les applications pour votre indexeur sont stockées), puis d'effectuer les mêmes modifications manuellement (ou déployées via l'automatisation telle que Puppet ou Ansible) dans le dossier `peer-apps` correspondant des indexeurs.

NOTE: La plupart des administrateurs sont habitués à placer des configurations dans `$SPLUNK_HOME/etc/system/local`. Cependant, pour les indexeurs en cluster, les paramètres de `$SPLUNK_HOME/etc/system/local` sont remplacés par tout ce qui se trouve dans le répertoire peer-apps de l'indexeur.

1. Exécutez la recherche suivante pour identifier les index qui ne sont pas gérés par volume :

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

2. À partir de la ligne de commande de Cluster Manager :
    1. Placez le cluster en mode maintenance :

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

    2. vérifiez que les mises à jour suivantes ont été apportées au fichier indexes.conf distribué à vos indexeurs (dans `$SPLUNK_HOME/etc/manager-`

`apps/_cluster/local/indexes.conf` ou déployé via une application personnalisée)

1. Vérifiez que les volumes sont définis pour les données chaudes/chaudes et froides et que les paramètres sont corrects. L'exemple montre des partitions séparées pour chacune, mais cela pourrait tout aussi bien être défini pour les compartiments stockés sur une seule partition. Vos choix de paramètres réels peuvent différer de ceux indiqués ci-dessous.

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

2. Pour faciliter la maintenance, la meilleure pratique consiste à définir `homePath` et `coldPath` dans la strophe `[default]` pour appliquer la configuration à tous les index :

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

3. Vérifiez les strophes pour chaque index identifié à partir de la recherche ci-dessus, et supprimez toutes les valeurs homePath ou coldPath (si elles existent) dans ces strophes. Cela permettra aux valeurs placées dans `[default]` de s'appliquer à ces strophes. Par la suite, une fois que le problème actuel est résolu et que vous avez confirmé que les données sont enregistrées correctement dans les volumes pour ces strophes spécifiques, vous pouvez vous assurer que `homePath` et `coldPath` ne sont pas définis pour d'autres index.

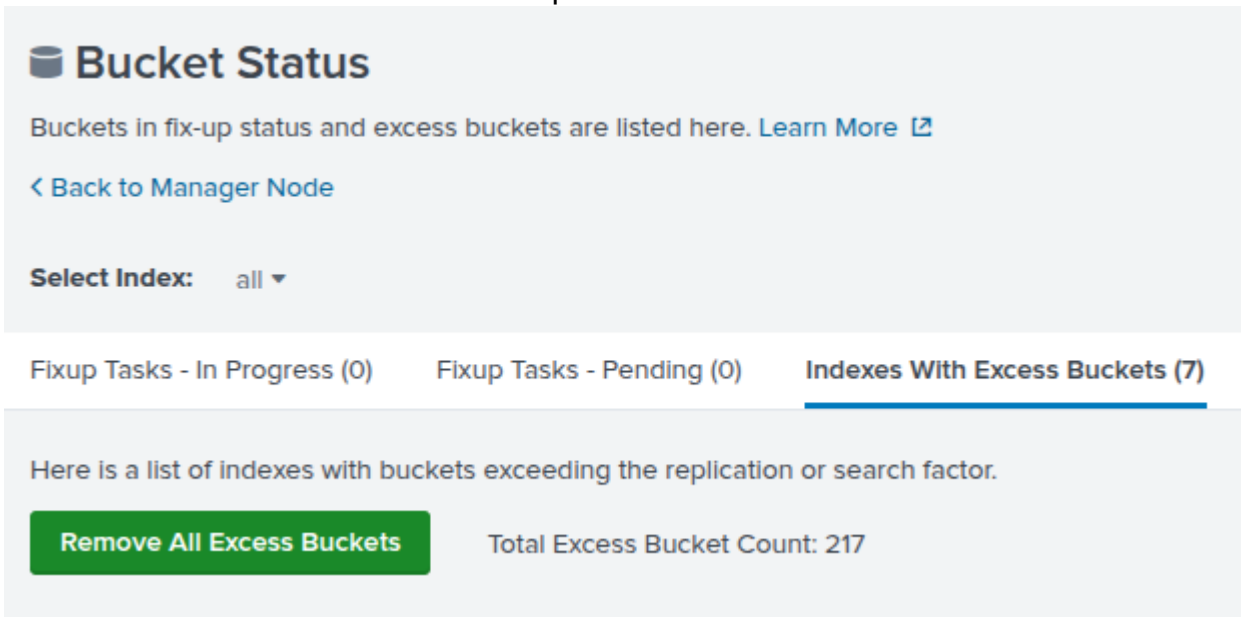
4. Si vous avez besoin d'espace supplémentaire, pensez également à désactiver la réplication en mode « bucket » pour les index internes. Dans ce cas, commencez par l'index [_internal]. Inclure d'autres si davantage d'espace est nécessaire. Marchez prudemment : si un indexeur est perdu, les données de ses index internes sont également perdues.

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

3. Un par un sur chaque indexeur (via la ligne de commande)
    1. Arrête Splunk. Exemple :
       `/opt/splunk/bin/splunk stop`
       ou, `systemctl stop Splunkd.service`
    2. Dans l'application appropriée située dans le répertoire `$SPLUNK_HOME/etc/peer-apps de l'`indexeur, apportez les mêmes modifications à `indexes.conf` que celles appliquées à Cluster Manager dans les étapes ci-dessus.
    3. Démarrer le Splunk
       `/opt/splunk/bin/splunk start`
       ou, `systemctl start Splunkd.service`
4. Accédez au tableau de bord Clustering d'Indexeur du Gestionnaire de cluster (Paramètres > Clustering d'Indexeur) pour vérifier que tous les indexeurs sont actifs et stables.
5. Vérifiez l'état du bundle et envoyez les configurations mises à jour aux indexeurs si nécessaire.
6. Une fois que tous les faisceaux sont envoyés aux indexeurs (et que les indexeurs sont stables), désactivez le mode de maintenance.

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

7. Libérez de l'espace supplémentaire en nettoyant les compartiments excédentaires.
    1. Dans le tableau de bord Clustering de l'Indexeur du Gestionnaire de cluster (Paramètres > Clustering de l'Indexeur), accédez à l'onglet Index et sélectionnez le bouton État du groupement.
    2. Une fois que toutes les tâches de correction ont été effacées (actualisez la page pour voir les corrections mises à jour), si l'interface utilisateur indique qu'il y a des compartiments en excès, cliquez sur Index avec des compartiments en excès, puis sélectionnez le bouton Effacer les compartiments en excès.



8. Retournez au noeud Gestionnaire et vérifiez que les indexeurs sont toujours stables.

Commandes Linux pouvant être utiles pour le dépannage :

Afficher l'utilisation du disque :

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

Trier par utilisation du disque du dossier datamodel_summary :

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

Liens connexes

Documentation sur les spunks :

- Définition des volumes dans indexes.conf
- Utiliser des variables pour définir les emplacements d'index
- Ordre de préséance de la configuration pour les indexeurs en cluster

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.