Splunk索引器磁盘空间使用率为100%

适用范围

Splunk企业

描述

本文描述集群且未启用SmartStore的索引器磁盘空间不足的情况。此处提供的解决方案只是一些简单的选项，可以提供一些即时缓解，但可能不适用于所有环境。

其中一些也可用于非群集环境。

这些步骤不适用于支持SmartStore的环境。

调查

如何确定：

1. 索引器的空间正在耗尽，导致数据无法滚动，并且没有新数据被摄取。
2. 此部署中的索引器是群集的，热/热和冷数据位于不同的安装点上
3. 部分或全部索引不受卷管理。
4. `maxVolumeDataSizeMB`已配置，但由于某些或全部索引不是卷管理的，因此它不会限制未使用卷的所有索引的磁盘使用率（例如`homePath = $SPLUNK_DB/xxx`）
5. splunkd.log中出现的错误：

```
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. 如果在集群管理器的indexes.conf中进行了更改，尝试推送将导致捆绑推送错误，指示索引器因缺少驱动器空间而无法卸载。

分辨率

如何修复：

通过允许索引器正确计算所有索引的实际使用量，从而释放磁盘空间，并且，如果需要，可以消除整个群集中非必要索引的复制。

以下步骤建议在manager-apps目录（或master-apps）中的适当位置对集群管理器上的indexes.conf应用适当的配置更改，然后手动进行相同的更改(或通过自动化（例如Puppet或Ansible）部署到索引器对应的peer-apps文件夹。

NOTE:大多数管理员习惯将配置放入$SPLUNK_HOME/etc/system/local。但是，对于集群索引器，$SPLUNK_HOME/etc/system/local中的设置将被索引器的peer-apps目录中找到的任何内容覆盖。

1. 运行以下搜索以确定非卷管理的索引：

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

2. 从Cluster Manager的命令行中：
    1. 将集群置于维护模式：

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

    2. 验证已对正在分发到索引器的indexes.conf文件（位于$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf中或通过自定义应用部署的）进行了以下更新
        1. 确认为热/热和冷数据定义了卷，并且设置正确。示例显示每个的分区，但可以同样轻松地为存储在一个分区上的存储段定义该分区。您的实际设置选择可能与以下设置不同。

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

        2. 为便于维护，最佳实践是在[default]模式中设置homePath和coldPath，以将配置应用到所有索引：

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

3. 检查通过上述搜索确定的每个索引的准则，并删除这些准则中的任何homePath或coldPath值（如果存在）。这将允许放置在[default]中的值应用于这些标准。稍后，解决当前问题并确认数据已正确保存到这些特定标准的卷后，您可能希望确保没有为任何其他索引定义homePath和coldPath。

4. 如果需要额外的空间，请考虑同时为内部索引禁用桶复制。 如果执行此操作，请只从[_internal]索引开始。如果需要更多空间则包括其它空间。谨慎行事：如果任何索引器丢失，其内部索引中的数据也会丢失。

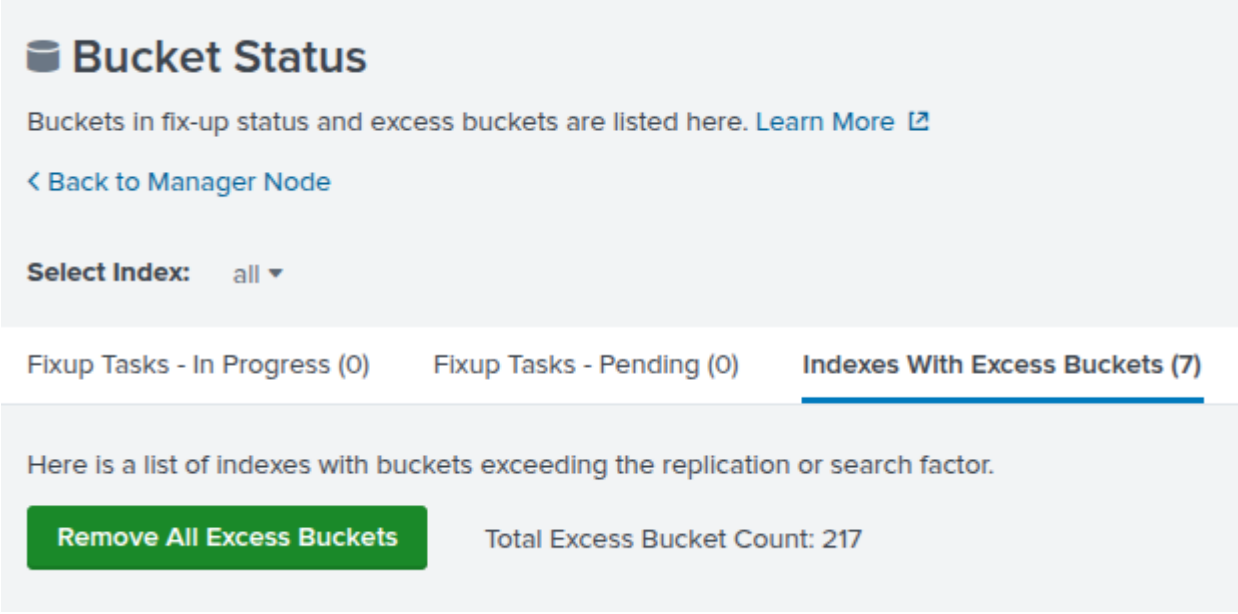
```
[_internal)
repFactor = 0
```

3. 在每个索引器上逐个显示一个（通过命令行）
    1. 停止Splunk。例如：
       `/opt/splunk/bin/splunk stop`
       或者，`systemctl stop Splunkd.service`
    2. 在位于索引器的$SPLUNK_HOME/etc/peer-apps目录中的相应应用中，对indexes.conf进行与上述步骤中应用于集群管理器的相同的编辑。
    3. 启动Splunk
       `/opt/splunk/bin/splunk start`
       或者，`systemctl start Splunkd.service`
4. 转至Cluster Manager的Indexer Clustering控制面板(Settings > Indexer Clustering)，验证所有索引器是否正常运行且稳定。
5. 检查捆绑状态，如有需要，将更新的配置推送到索引器。
6. 将所有捆绑推送到索引器（并且索引器是稳定的）后，禁用维护模式。

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

7. 通过清除多余存储桶释放更多空间。
    1. 从Cluster Manager的Indexer Clustering控制面板(Settings > Indexer Clustering)中，转到Indexes选项卡并选择Bucket Status按钮。
    2. 清除所有修复任务后（刷新页面以监视修复更新），如果UI显示存在超额存储桶，请单

击Indexes with excess buckets，然后选择Clear excess buckets按钮。



8. 返回Manager Node，验证索引器是否仍然稳定。

在故障排除中可能有用的Linux命令：

显示磁盘使用情况：

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

按datamodel_summary文件夹的磁盘使用率排序：

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

相关链接

Splunk文档：

- 在indexes.conf中定义卷
- 使用变量定义索引位置
- 集群索引器的优先级配置顺序

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。