Splunk 인덱서 디스크 공간 사용률이 100%입니다.

적용 가능성

Splunk Enterprise

설명

이 문서에서는 클러스터된 비 SmartStore 사용 인덱서의 디스크 공간이 부족한 경우에 대해 설명합니다. 여기서 제공되는 해결책은 일부 즉각적인 구제를 제공하기 위한 간단한 옵션이며, 이는 모든 환경에서 적용될 수 있는 것은 아니다.

이 중 일부는 클러스터링되지 않은 환경에도 적용할 수 있습니다.

이러한 단계는 SmartStore 지원 환경에는 적용되지 않습니다.

조사

식별 방법:

1. 인덱서의 공간이 부족하여 데이터를 롤오프할 수 없으며 새 데이터를 가져올 수 없습니다.
2. 이 구축의 인덱서는 핫/웜 및 콜드 데이터가 별도의 마운트 지점에 있는 클러스터링됩니다
3. 일부 또는 모든 인덱스가 볼륨 관리되지 않습니다.
4. `maxVolumeDataSizeMB`가 구성되었지만 일부 또는 모든 인덱스가 볼륨 관리되지 않으므로 볼륨을 사용하지 않는 모든 인덱스의 디스크 사용량이 제한되지 않습니다(예: homePath = `$SPLUNK_DB/xxx`).
5. splunkd.log에 오류가 있습니다.

```
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. 클러스터 관리자에서 indexes.conf를 변경하면 밀어넣기를 시도하면 번들 밀어넣기 오류가 발생하여 드라이브 공간이 부족하여 인덱서가 압축을 풀 수 없습니다.

해결

해결 방법:

인덱서가 모든 인덱스의 실제 사용량을 적절히 계산하도록 하여 디스크 공간을 확보하고, 필요한 경우 클러스터 전체에서 중요하지 않은 인덱스의 복제를 제거합니다.

아래 단계에서는 `manager-apps` 디렉토리(또는 인덱서용 앱이 저장된 위치에 따라 마스터 앱) 내의 해당 위치에 있는 클러스터 관리자의 `indexes.conf`에 적절한 컨피그레이션 변경 사항을 적용한 다음, 동일한 변경 사항을 수동으로 만들거나 Puppet 또는 Ansible과 같은 자동화를 통해 인덱서의 해당 피어 앱 폴더에 배포하는 방법을 제안합니다.

참고: 대부분의 관리자는 구성을 `$SPLUNK_HOME/etc/system/local`에 배치하는 데 익숙합니다. 그러나 클러스터형 인덱서의 경우 `$SPLUNK_HOME/etc/system/local`의 설정은 인덱서의 peer-apps 디렉터리에 있는 설정에 의해 재정의됩니다.

1. 다음 검색을 실행하여 볼륨 관리되지 않는 인덱스를 식별합니다.

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

2. 클러스터 관리자의 명령줄에서
    1. 클러스터를 유지 관리 모드로 설정합니다.

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

    2. 인덱서에 배포되는 indexes.conf 파일에 대해 다음 업데이트가 수행되었는지 확인합니다(`$SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf` 또는 사용자 지정 앱을 통해 배포됨).
        1. 볼륨이 핫/웜 및 콜드 데이터에 대해 정의되었는지 확인하고 설정이 올바른지 확인합니다. 예제는 각각에 대해 별도의 파티션을 표시하지만, 이는 단일 파티션에 저장된 버킷에 대해 쉽게 정의할 수 있습니다. 실제 설정 선택은 아래와 다를 수 있습니다.

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

```
path = /mnt/big_disk
maxVolumeDataSizeMB = 150000
```

2. 유지 보수의 편의를 위해 [default] stanza에서 homePath와 coldPath를 설정하여 모든 인덱스에 컨피그레이션을 적용하는 것이 좋습니다.

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

3. 위 검색에서 식별된 각 인덱스의 stanzas를 확인하고 해당 stanzas에 있는 모든 homePath 또는 coldPath 값(있는 경우)을 제거합니다. 이렇게 하면 [기본값]에 있는 값을 이러한 스타자에 적용할 수 있습니다. 나중에 현재 문제가 해결되고 이러한 특정 스탄자의 볼륨에 데이터가 제대로 저장되는지 확인한 후에는 다른 인덱스에 대해 homePath와 coldPath가 정의되지 않았음을 확인할 수 있습니다.

4. 추가 공간이 필요한 경우 내부 인덱스에 대한 버킷 복제를 비활성화하는 것도 고려하십시오. 이렇게 하려면 [_internal] 인덱스만으로 시작합니다. 추가 공간이 필요한 경우 다른 항목을 포함합니다. 조심해서 걸어라: 인덱서가 손실되면 내부 인덱스의 데이터도 손실됩니다.

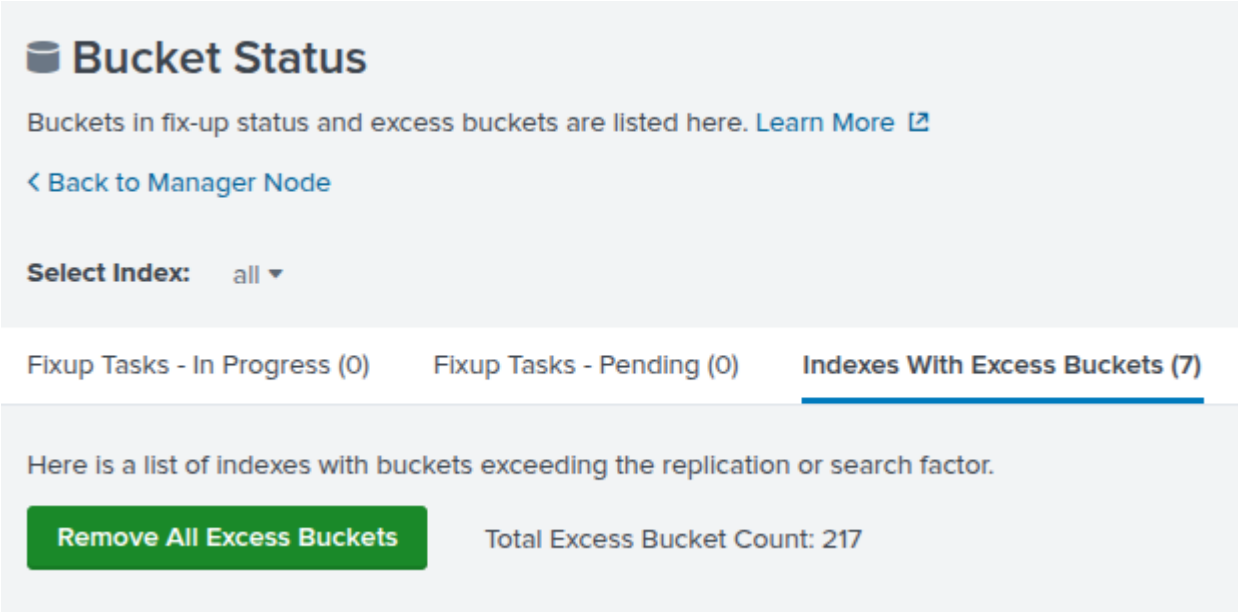
```
[_internal)
repFactor = 0
```

3. 명령줄을 통해 각 인덱서에서 한 번에 하나씩

    1. Splunk를 중지합니다. 예를 들면 다음과 같습니다.
       /opt/splunk/bin/splunk 중지
       또는, systemctl stop Splunkd.service
    2. 인덱서의 $SPLUNK_HOME/etc/peer-apps 디렉토리에 있는 해당 앱에서 위의 단계에서 클러스터 관리자에 적용된 indexes.conf를 동일하게 수정합니다.
    3. Splunk 시작
       /opt/splunk/bin/splunk 시작
       또는, systemctl start Splunkd.service
4. 클러스터 관리자의 인덱서 클러스터링 대시보드(Settings > Indexer Clustering)로 이동하여 모든 인덱서가 작동 및 안정되었는지 확인합니다.
5. 번들 상태를 확인하고 필요한 경우 업데이트된 컨피그레이션을 인덱서에 푸시합니다.
6. 모든 번들이 인덱서에 푸시되고 인덱서가 안정되면 유지 관리 모드를 비활성화합니다.

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

7. 초과 버킷을 지워 추가 공간을 확보합니다.
    1. Cluster Manager의 Indexer Clustering 대시보드(Settings > Indexer Clustering)에서 Indexes 탭으로 이동하여 Bucket Status(버킷 상태) 버튼을 선택합니다.
    2. 모든 수정 작업을 지운 후(수정 업데이트를 감시하기 위해 페이지를 새로 고침) UI에 초과 버킷이 표시되는 경우 초과 버킷이 있는 인덱스를 누른 다음 초과 버켓 지우기 단추를 선택합니다.



8. 관리자 노드로 돌아가서 인덱서가 여전히 안정적인지 확인합니다.

문제 해결에 유용할 수 있는 Linux 명령:

디스크 사용량 표시:

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

Datamodel_summary 폴더의 디스크 사용량을 기준으로 정렬:

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

관련 링크

Splunk 설명서:

- indexes.conf에서 볼륨 정의
- 변수를 사용하여 인덱스 위치 정의
- 클러스터형 인덱서의 구성 우선 순위

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.