El uso del espacio en disco del indizador Splunk está al 100%

Aplicabilidad

Splunk Enterprise

Descripción

En este artículo se describe un escenario en el que los indizadores en clúster no habilitados para SmartStore no tienen espacio en disco. Las soluciones que se proporcionan aquí son opciones simples para proporcionar algún alivio inmediato, que puede no ser aplicable en todos los entornos.

Algunas de estas funciones también se pueden aplicar a entornos no agrupados.

Estos pasos no se aplican a los entornos habilitados para SmartStore.

Investigación

Cómo identificar:

1. Los indizadores se están quedando sin espacio, lo que impide que se descarguen los datos y que no se ingieran datos nuevos.
2. Los indizadores de esta implementación se agrupan en clúster, con datos fríos/calientes ubicados en puntos de montaje independientes
3. Algunos o todos los índices no se administran por volumen.
4. `maxVolumeDataSizeMB` está configurado, pero como algunos o todos los índices no se administran por volumen, no restringe el uso del disco para todos los índices que no utilizan volumen (por ejemplo, `homePath = $SPLUNK_DB/xxx`)
5. Errores observados en 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 se realizan cambios en indexes.conf en el Administrador de clústeres, los intentos de inserción producirán errores de inserción de paquetes, lo que indica que los indizadores no pueden descomprimir debido a la falta de espacio en la unidad.

Resolución

Cómo solucionarlo:

Libere espacio en disco permitiendo que los indizadores tengan en cuenta correctamente el cálculo del uso real de todos los índices y, si es necesario, elimine la replicación de los índices no esenciales en el clúster.

Los siguientes pasos sugieren aplicar los cambios de configuración adecuados a `indexes.conf` en el Administrador de clústeres en la ubicación apropiada dentro del directorio `manager-apps` (o `master-apps` dependiendo de dónde se almacenan las aplicaciones para el indizador), luego hacer los mismos cambios manualmente (o implementados a través de la automatización como Puppet o Ansible) en la carpeta `peer-apps` correspondiente de los indizadores.

NOTE: La mayoría de los administradores están acostumbrados a colocar configuraciones en `$SPLUNK_HOME/etc/system/local`. Sin embargo, para los indizadores agrupados, la configuración en `$SPLUNK_HOME/etc/system/local` se reemplaza por cualquier cosa que se encuentre en el directorio peer-apps del indizador.

1. Ejecute la siguiente búsqueda para identificar índices que no están gestionados por volumen:

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

2. Desde la línea de comandos del Administrador de clústeres:
    1. Coloque el clúster en modo de mantenimiento:

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

    2. verifique que se hayan realizado las siguientes actualizaciones en el archivo indexes.conf que se distribuye a sus indizadores (en `$SPLUNK_HOME/etc/manager-`

`apps/_cluster/local/indexes.conf` o implementado a través de una aplicación personalizada)

1. Confirme que los volúmenes están definidos para los datos de calor/calor y frío, y que la configuración es correcta. El ejemplo muestra particiones separadas para cada una, pero esto podría definirse fácilmente para los depósitos almacenados en una sola partición. Las opciones de configuración reales pueden diferir de las que aparecen a continuación.

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

2. Para facilitar el mantenimiento, se recomienda establecer `homePath` y `coldPath` en la estrofa `[default]` para aplicar la configuración a todos los índices:

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

3. Compruebe las estrofas de cada índice identificado en la búsqueda anterior y elimine los valores de homePath o coldPath (si existen) de dichas estrofas. Esto permitirá que los valores colocados en `[default]` se apliquen a estas estrofas. Más adelante, una vez resuelto el problema actual y confirmados los datos se guardan correctamente en los volúmenes para estas estrofas específicas, es posible que desee asegurarse de que `homePath` y `coldPath` no estén definidos para ningún otro índice.

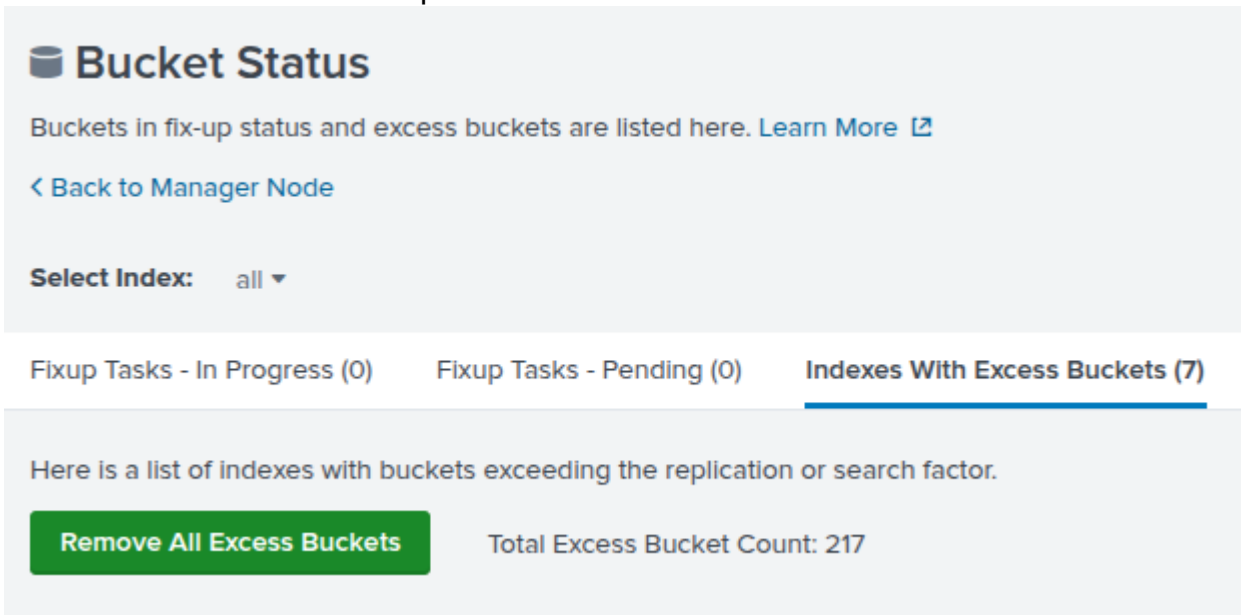
4. Si se necesita espacio adicional, considere también la posibilidad de deshabilitar la replicación de cubeta para los índices internos. Si hace esto, comience sólo con el índice [_internal]. Incluya otros si necesita más espacio. Pase con cuidado: si se pierde algún indizador, también se pierden los datos de sus índices internos.

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

3. Uno a la vez en cada indizador (a través de la línea de comandos)
    1. Detén a Splunk. Por ejemplo:
       `/opt/splunk/bin/splunk stop`
       o bien, `systemctl stop Splunkd.service`
    2. En la aplicación apropiada ubicada en el directorio `$SPLUNK_HOME/etc/peer-apps` del indizador, realice las mismas ediciones en `indexes.conf` que se aplicaron al Cluster Manager en los pasos anteriores.
    3. Iniciar Splunk
       `/opt/splunk/bin/splunk start`
       o bien, `systemctl start Splunkd.service`
4. Vaya al panel Agrupación en clústeres de indizadores del Administrador de clústeres (Configuración > Agrupación en clústeres de indizadores) para comprobar que todos los indizadores están activos y estables.
5. Compruebe el estado del paquete e introduzca las configuraciones actualizadas en los indizadores si es necesario.
6. Una vez que todos los paquetes se envían a los indizadores (y los indizadores son estables), inhabilite el modo de mantenimiento.

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

7. Libere espacio adicional eliminando el exceso de depósitos.
    1. En el panel de agrupamiento de indizadores del Administrador de clústeres (Configuración > Agrupación de indizadores), vaya a la pestaña Índices y seleccione el botón Estado de depósito.
    2. Una vez que se hayan borrado todas las tareas de corrección (actualice la página para ver la actualización de las correcciones), si la interfaz de usuario muestra que hay depósitos en exceso, haga clic en Índices con depósitos en exceso y, a continuación, seleccione el botón Borrar depósitos en exceso.



8. Vuelva al nodo de administración y compruebe que los indizadores siguen estables.

Comandos de Linux que pueden ser útiles en la resolución de problemas:

Mostrar uso del disco:

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

Ordenar por uso de disco de la carpeta datamodel_summary:

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

Enlaces relacionados

Documentación de Splunk:

- Definir volúmenes en indexes.conf
- Utilizar variables para definir ubicaciones de índice
- Orden de precedencia de la configuración para indizadores agrupados

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).