إستخدام مساحة قرص مفهرس SPLUNK بنسبة 100٪

قابلية التطبيق

مؤسسة Splunk

الوصف

يصف هذا المقال سيناريو حيث نفدت مساحة القرص لفهارس تمكين غير SmartStore والتي تم تجميعها. الحلول المقدمة هنا هي خيارات بسيطة لتوفير بعض الإغاثة الفورية، والتي قد لا تكون قابلة للتطبيق في جميع البيئات.

ويمكن تطبيق بعض هذه التقنيات على البيئات غير المجمعة أيضا.

لا تنطبق هذه الخطوات على البيئات التي تم تمكين SmartStore لها.

إستجلاء

كيفية التعرف على:

1. تنفد مساحة الفهارس، مما يمنع البيانات من الظهور، ولا يتم البحث عن بيانات جديدة.
2. يتم تجميع الفهارس في هذا النشر مع وجود بيانات ساخنة/دافئة وباردة على نقاط تحميل منفصلة
3. بعض الفهارس أو جميعها لا تتم إدارة وحدة التخزين.
4. تم تكوين `maxVolumeDataSizeMB`، ولكن نظرا لأن بعض الفهارس أو جميعها لا تتم إدارة وحدة التخزين، فإنها لا تقيد إستخدام القرص لجميع الفهارس التي لا تستخدم وحدة التخزين (على سبيل المثال، `HomePath = $SPLUNK_DB/xxx`)
5. الأخطاء التي ظهرت في 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. إذا تم إجراء تغييرات في index.conf في "إدارة المجموعة"، ستؤدي محاولات الدفع إلى حدوث

أخطاء في دفع الحزمة، مما يشير إلى عدم قدرة المفهارس على إلغاء التبعثر بسبب نقص مساحة محرك الأقراص.

قرار

كيفية إصلاحه:

قم بتحرير مساحة على القرص من خلال السماح للفهارس بحساب الاستخدام الفعلي بشكل صحيح للكافة الفهارس، وإذا لزم الأمر، قم بالقضاء على النسخ المتماثل للفهارس غير الضرورية عبر نظام المجموعة.

تقترح الخطوات التالية تطبيق تغييرات التكوين المناسبة على index.conf على "مدير المجموعة" في الموقع المناسب داخل دليل تطبيقات الرئيسية (أو تطبيقات الإدارة-المحلية) وأقفل للكان الذي يتم فيه تخزين التطبيقات الخاصة بالمفهرس)، ثم إجراء نفس التغييرات يدويا (أو النشر عبر التشغيل التلقائي مثل Puppet أو Ansible) على مجلد تطبيقات النظير المتوافق الخاص بالمفهرس.

ملاحظة: اعتاد معظم المسؤولين وضع التكوينات في $SPLUNK_HOME/system/local/. ومع ذلك، يتم تجاوز الإعدادات الموجودة في $SPLUNK_HOME/system/local بأي شيء يتم العثور عليه في دليل تطبيقات النظير الخاص بالفهرس.

1. قم بتشغيل البحث التالي لتعريف الفهارس التي لا تتم إدارة وحدة التخزين:

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

2. من سطر أوامر مدير نظام المجموعة:
   1. وضع نظام المجموعة في وضع الصيانة:

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

   2. تحقق من إجراء التحديثات التالية على ملف index.conf الذي يتم توزيعه على الفهارس الخاصة بك (في $SPLUNK_HOME/etc/manager-apps/_cluster/local/indexes.conf أو يتم نشره عبر تطبيق مخصص)
      1. تأكد من تعريف وحدات التخزين للبيانات الساخنة/الدافئة والباردة، والإعدادات صحيحة. يوضح المثال تقسيمات منفصلة لكل منها، ولكن

يمكن تعريف هذا بنفس السهولة للمقابس المخزنة على قسم واحد. قد تختلف خيارات الإعداد الفعلية لديك عن الخيارات التالية.

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

2. لتسهيل الصيانة، تتمثل أفضل الممارسات في تعيين homePath وcoldPath في وضوح [default] لتطبيق التكوين على جميع الفهارس:

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

3. تحقق من الصيغ لكل فهرس تم تعريفه من البحث أعلاه، وقم بإزالة أي قيم HomePath أو ColdPath (إذا كانت موجودة) في هذه الصيغ. هذا سيسمح للقيم الموضوعة في [default] أن تنطبق على هذه المواقف. لاحقا، بمجرد حل المشكلة الحالية وتأكد من حفظ البيانات بشكل صحيح إلى وحدات التخزين لهذه الفواصل المحددة، قد ترغب في التأكد من عدم تعريف HomePath وColdPath لأي فهارس أخرى.

4. إذا كانت هناك حاجة إلى مساحة إضافية، فاعتبر أيضا تعطيل تكرار المستودع للفهارس (الفهارس) الداخلية. إذا قمت بذلك، ابدأ فقط بالفهرس [_internal]. قم بتضمين الآخرين إذا كانت هناك حاجة إلى مزيد من المساحة. اساوا باعتناء: في حالة فقد أي مفهرس، يتم فقد البيانات من فهارس داخلية أيضا.

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

3. وحدة واحدة في كل مرة على كل مفهرس (عبر سطر الأوامر)

1. قطع التوقف. على سبيل المثال:
   /opt/splunk/bin/splunk stop
   أو، إيقاف النظام Splunkd.service
2. في التطبيق المناسب الموجود في دليل الفهرسة $SPLUNK_HOME/etc/peer-apps،

قم بإجراء نفس التحريرات على index.conf كما تم تطبيقها على مدير نظام المجموعة في الخطوات أعلاه.

3. بداية Splunk

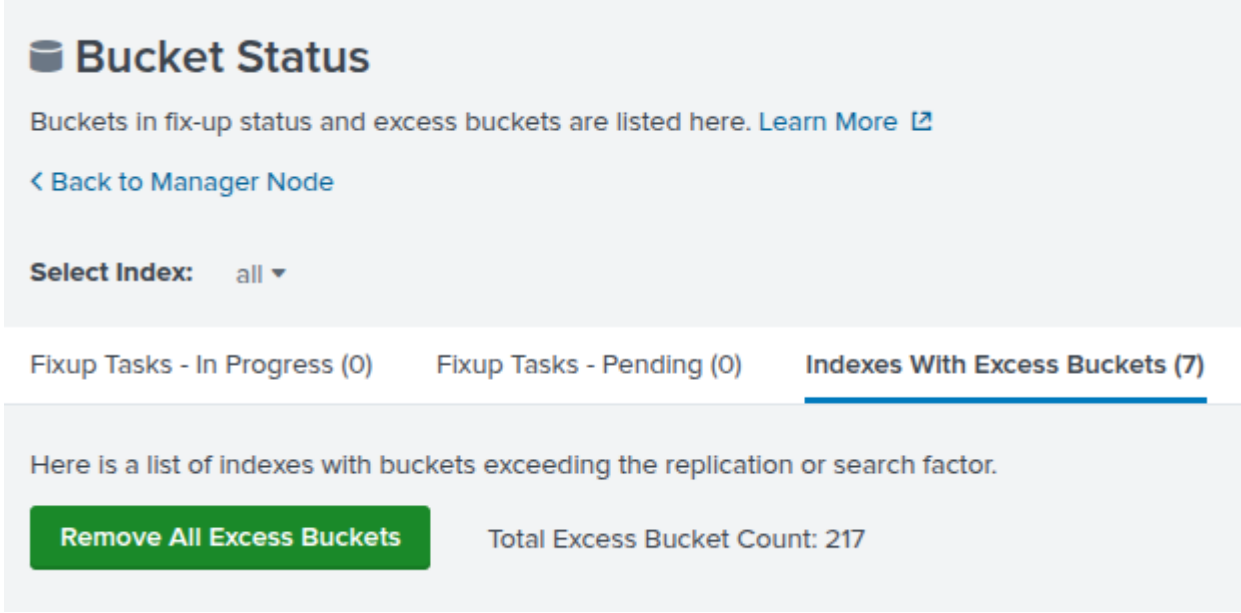
   /opt/splunk/bin/splunk start

   أو، بدء تشغيل النظام Splunkd.service

4. انتقل إلى لوحة معلومات تجميع المفهرس الخاصة بإدارة نظام المجموعة (الإعدادات > تجميع المفهرس) للتحقق من أن كافة المفهارس بحالة تشغيل واستقرار.
5. تحقق من حالة الحزمة واضغط التكوينات المحدثة على المفهرسين إذا لزم الأمر.
6. قم بتعطيل وضع الصيانة بمجرد دفع جميع الحزم إلى الفهارس (والفهارس ثابتة).

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

7. قم بتحرير مساحة إضافية عن طريق إزالة الدلاء الزائدة.
   1. من لوحة معلومات تجميع مفهرس مدير النظام (الإعدادات > تجميع المفهرس)، انتقل إلى علامة التبويب الفهارس وحدد الزر حالة المستودع.
   2. بمجرد مسح كل مهام الإصلاح (تحديث الصفحة لمشاهدة تحديث عمليات الإصلاح)، إذا أظهرت واجهة المستخدم وجود دلاء زائدة، انقر فوق فهارس ذات دلاء زائدة، ثم حدد الزر مسح الدلاء الزائدة.



8. ارجع إلى "عقدة الإدارة" وتأكد من أن الفهارس لا تزال مستقرة.

أوامر Linux التي قد تكون مفيدة في أستكشاف الأخطاء وإصلاحها:

إظهار إستخدام القرص:

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

فرز حسب إستخدام القرص لمجلد datamodel_summary:

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

روابط ذات صلة

وثائق Splunk:

- تحديد وحدات التخزين في index.conf
- أستخدم المتغيرات لتعريف أماكن الفهرس
- ترتيب ترتيب الأسبقية للتكوين للفهارس المجمعة

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).