إدارة إستخدام نظام الملفات/الأقراص المحلية في تحليلات الشبكة الآمنة

المحتويات

المقدمة

يصف هذا المستند الخطوات العامة لتقليل إستخدام القرص المرتفع على أجهزة مدير تحليلات الشبكة الآمنة وجامع التدفق.

المتطلبات الأساسية

المتطلبات

ينطبق هذا المستند على عمليات نشر تحليلات الشبكة الآمنة بدون مخزن بيانات.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Secure Network Analytics Manager - v7.1+
- مجمع تدفق تحليلات الشبكة الآمنة - v7.1+
- مستشعر تدفق تحليلات الشبكة الآمنة - v7.1+
- مدير Secure Network Analytics UDP - v7.1+

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

هناك قسمان للمراقبة الاستخدام القرص، قسم الجذر (/) و /lancope/var.

يمثل قسم الجذر (/) موقع تخزين صورة kernel وبعض سجلات النظام، ويكون هذه عادة عبارة عن جزء أصغر حجم يبلغ 20 جيجا أو أقل. إن /lancope/var عبارة عن مجموعة وحدات تخزين وإنها تستهلك معظم مساحة القرص للجهاز. موقع التخزين لمعظم بيانات النظام، لذلك فإنها

تجميع البيانات

هناك مكانان يمكنك الحصول على معلومات إستخدام القرص، واجهة مستخدم ويب للمسؤول، وواجهة سطر الأوامر (CLI)

سطر الأوامر

من سطر الأوامر قم بتشغيل **df -ah / /lancope/var** أو رمز الظ المسافات بين (/) و /lancope/var.

<#root>

732smc:/#

df -ah / /lancope/var/

Filesystem Size Used Avail Use% Mounted on
/dev/sda2 20G 8.3G 9.9G 46% /
/dev/mapper/vg_lancope-_var 108G 23G 83G 22% /lancope/var
732smc:/#

يوضح الإخراج أن تحليل الجذر (/) هو 20 وحدة تسارع جاذبية، و 8.3g قيد الاستخدام وهو 46٪. كما يوضح الإخراج أن قسم /lancope/var هو 108G، وأن 23G قيد الاستخدام وهو 22٪.

واجهة مستخدم ويب

قم بتسجيل الدخول إلى واجهة مستخدم Admin المستندة إلى النموذج قيد البحث، والتمرير إلى أسفل الصفحة.

قائمة عناوين ويب UI للمسؤول:

- مدير تحليلات الشبكة الآمنة - https://<SMC-IP-أو-FQDN>/smc/index.html (يجب تسجيل الدخول إلى SMC قبل الوصول إلى عنوان URL هذا)
- مجمع تدفق تحليلات الشبكة الآمنة - https://<FC-IP-or-FQDN>/swa/index.html
- مستشعر تدفق تحليلات الشبكة الآمنة - https://<FS-IP-أو-FQDN>/fs/index.html
- مدير تحليلات الشبكة الآمنة UDP (وحدة إضافة التدفق) - https://<UDPD-IP-أو-FQDN>/fr/index.html

Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	14%	19.56G	2.9G	15.66G
/lancope/var	25%	106.23G	27.23G	76.82G

إذا كان القسم لديه إستخدام عال أكبر من أو يساوي 75٪ يتم تمييز القسم.

مسح مساحة القرص

إذا لم تكن متأكدا من الملفات الآمنة التي يمكن حذفها، فافتح حالة TAC أو اتصل بدعم Cisco من خلال صفحة جهات اتصال الدعم العالمية من Cisco في قسم المعلومات ذات الصلة في نهاية هذا المستند.

سجلات النظام

إحدى أسرع الطرق لاسترداد مساحة كبيرة على القرص هي مسح سجلات اليومية باستخدام journalctl --vacuum-time 1d erasecat4000_flash:. لاحظ الواصلة المزدوجة — قبل كلمة "فارغ".

<#root>

732smc:/#

journalctl --vacuum-time 1d

Deleted archived journal /var/log/journal/639c60e1e407f646b5ed1751cde413fa
/user-1000@db376b09011842d5b247f6d31de6c241-00000000004ec2a8-0005e7838ecf15cc.journal
<the above line repeats>
Vacuuming done, freed 3.9G of archived journals from /var/log/journal/639c60e1e407f646b5ed1751cde413fa.
732smc:/#

df -ah / /lancope/var/

Filesystem Size Used Avail Use% Mounted on
/dev/sda2 20G 8.3G 9.9G 46% /
/dev/mapper/vg_lancope-_var 108G 19G 87G 18% /lancope/var
732smc:/#

تم إسترداد حوالي 4G من مساحة القرص من هذه الخطوات مما أدى إلى انخفاض في إستخدام القرص من 22٪ إلى 18٪ على قسم /lancope/var.

الملفات الموجودة في الدلة المدرجة تكون آمنة بشكل عام للحذف:

/lancope/var/tcpdump
/lancope/var/tomcat/logs
/lancope/var/tmp

/lancope/var/admin/tmp/

يوصى بالبدء إما في دليل الجذر (/) أو دليل /lancope/var، أي قسم قمت بتحديده في واجهة مستخدم ويب التي تحتوي على إستخدام كبير للقرص. تغيير الدليل الحالي باستخدام cd / erasecat4000_flash:.

تشغيل du -xah --max-depth=1 | sort -hr أمر لتحديد أكبر مستهلك لمساحة القرص الخاصة بالدليل الحالي. لاحظ الواصلة المزدوجة — قبل أقصى عمق.

يوضح الإخراج أن قسم الجذر (/) به مساحة قرص تبلغ 8.3 جيجا قيد الاستخدام، عم 5.5 جرام من مساحة القرص المستخدمة في دليل /lancope، متبوعا بدليل /usr عم 1.5G من الاستخدام.

<#root>

732smc:~#

cd /

732smc:/#

du -xah --max-depth=1 | sort -hr | head -n4

8.3G .
5.5G ./lancope
1.5G ./usr
1.3G ./opt
732smc:/#

تغيير الدليل إلى /lancope عم **cd lancope**/ قم بإصدار الأمر du مرة أخرى باستخدام !du، و 5.1G /lancope/ في الدليل المستخدمة 5.5G الخاصة بالآن اذه ضعي erasecat4000_flash:. cd باستخدام المعني الدليل إلى الحالية الدلة بتغيير قم. المسؤول دليل في erasecat4000_flash:.

<#root>

732smc:/#

cd lancope/

732smc:/lancope# !du
du -xah --max-depth=1 | sort -hr | head -n4
5.5G .
5.1G ./admin
212M ./services
59M ./mongodb
732smc:/lancope#

بمجرد أن تقوم بتعريف الملفات التي يمكن حذفها، يمكنك القيام بذلك باستخدام rm -i erasecat4000_flash:. إذا لم تكن متأكدا من الملفات الآمنة التي يمكن حذفها، فافتح حالة TAC أو اتصل بدعم Cisco من خلال صفحة جهات اتصال الدعم العالمية من Cisco في قسم المعلومات ذات الصلة في نهاية هذا المستند.

<#root>

732smc:/lancope/admin#

rm -i file

rm: remove regular empty file 'file'?

yes

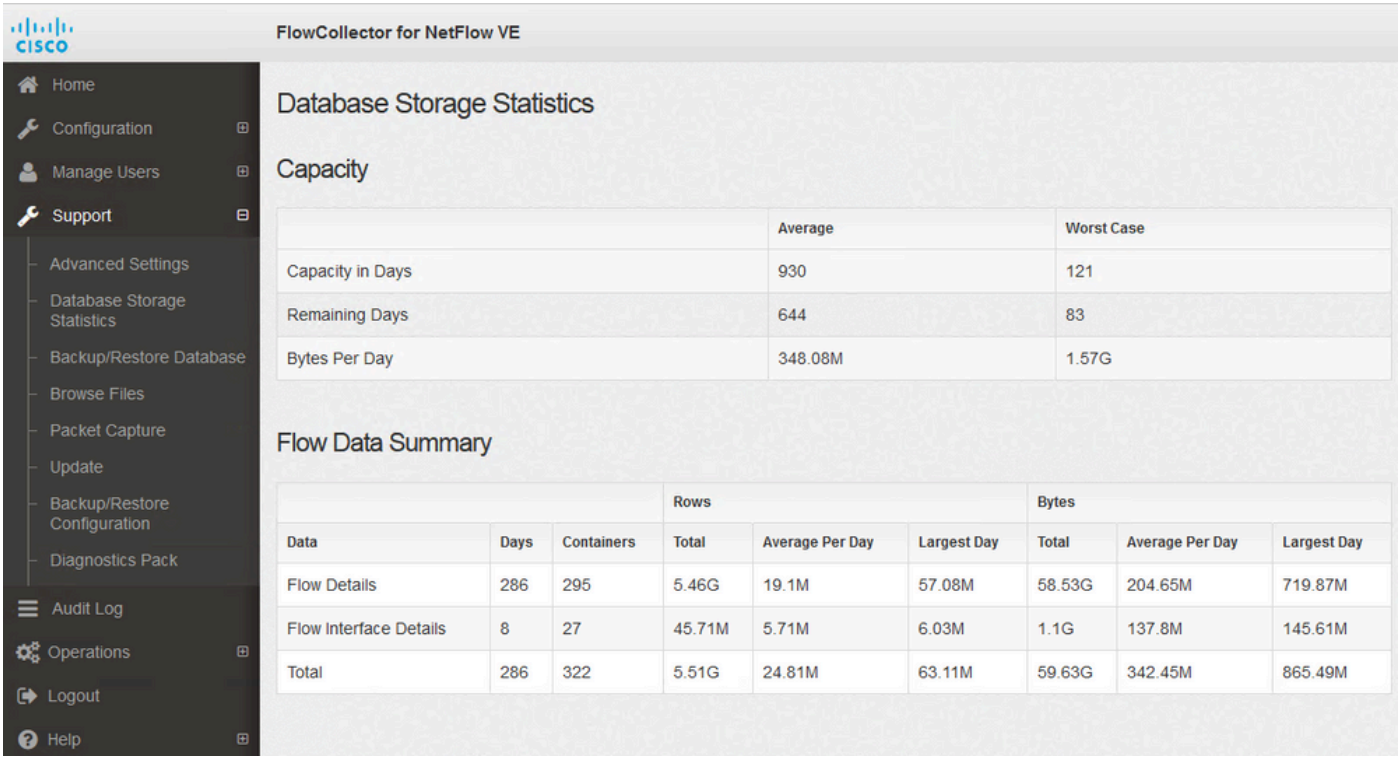
732smc:/lancope/admin#

قم بتكرار هذه الخطوات حسب الحاجة.

اقتطاع قاعدة البيانات الموزعة (DDS) - حالات التدفق

بشكل افتراضي، في بيئة DDS، تحاول أجهزة FlowCollector و SMC تخزين أكبر قدر ممكن من بيانات التدفق التي يتم تدويرها بشكل يومي. عند الوصول إلى حدود إستخدام القرص، يبدأ النظام في حذف البيانات الأقدم أولا لإنشاء مساحة لحفظ البيانات الجديدة.

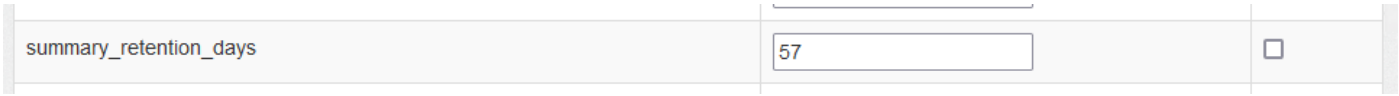
لعرض إحصائيات قاعدة بيانات مجمع التدفق، قم بتسجيل الدخول إلى واجهة مستخدم FlowCollector Admin ثم حدد Support > Database Storage Statistics .



إحصائيات تخزين قاعدة البيانات

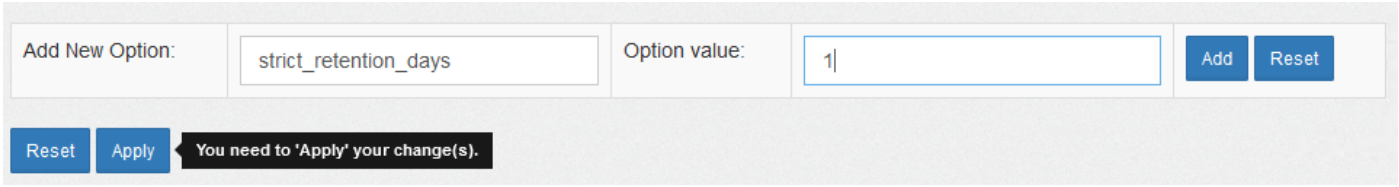
- توضح الصورة أن متوسط تفاصيل التدفق المهتزة (بيانات NetFlow) يبلغ 204.65 ميجابايت تقريبا في اليوم وأن مجمع التدفق هذا يحتوي على نحو 58.5 جيجابايت من البيانات المخزنة.
- توضح الصورة أن متوسط تفاصيل واجهة التدفق المهتزة (إحصائيات محددة للواجهة) يبلغ 137 ميجابايت في اليوم ويحتوي مجمع التدفق هذا على نحو 1.1 جيجابايت من البيانات المخزنة.
- توضح الصورة أن إجمالي بيانات التدفق يبلغ متوسطه حوالي 342.53 جيجابايت في اليوم، كما يحتوي مجمع التدفق هذا على نحو 60 جيجابايت من إجمالي البيانات المخزنة.
- إذا كنت ترغب في تقسيم قاعدة البيانات إلى أسفل بحيث يكون لديك حوالي 20 جيجا من إجمالي البيانات المخزنة، فقم بقسمة هذا على المتوسط اليومي ل 35 جيجا الذي يساوي 57.

لتقليل حجم قاعدة البيانات بحيث يبلغ إجمالي سعتها حوالي 20 جيجابايت، قم بتغيير Summary_retention_days القيمة إلى 57. بعد ذلك، انتقل إلى Support > Advanced Settings . بحث summary_retention_days وغير هذه إلى القيمة التي تريدها.



summary_retention_days

بعد ذلك، قم بإضافة خيار جديد في أسفل القائمة. يعرض الأمر Add New Option القيمة هي strict_retention_days و Option Value يتم تعيين القيمة على 1 كما هو موضح في الصورة. انقر فوق إضافة (Add). هذا strict_retention_days يطلب من المحرك الاحتفاظ فقط بعدد الأيام المعلن عنها في Summary_retention_days .



STRICT_RETENTION_DAYS

بمجرد أن قمت بتغيير **summary_retention_days** إلى 4 وانا أضفت قيمة الخيار الجديد، اضغط Apply في أسفل الصفحة.

إذا كانت هذه الخطوات لإجراء ترقية، فقم بحذف **strict_retention_days** القيمة بمجرد الكمال الترقية للعودة إلى الاحتفاظ بالبيانات لأطول فترة ممكنة.

اقتطاع قاعدة البيانات الموزعة (DDS) - تفاصيل واجهة التدفق

1. سجل في إلى لك Stealthwatch سطح المكتب العميل ك يعرض الأمر مسؤول مستخدم.

2. حدد موقع FlowCollector في Enterprise Tree. انقر فوق علامة الجمع (+) توقيع لتوسيع

الحاوية.

3. انقر بزر الماوس الأيمن على FlowCollector المطلوب. تحديد Configuration > Properties.

4. في يعرض الأمر إنبجاسامجمع الخصائص حوار مربع، طقطقة Advanced.

5. تحديد يعرض الأمر Store **flow interface data**الحقل. مجموعة يعرض الأمر حد إلى يعمل إلى 15 يوم/أيام وأ 30 يوم/أيام.

6. انقر OK .

زيادة مساحة القرص (الأجهزة الظاهرية فقط)

قم بإيقاف تشغيل الجهاز الظاهري وزيادة حجم القرص المخصص لـ VM من برنامج مراقبة الأجهزة الافتراضية. يتم تخصيص مساحة القرص الإضافية للقسم /lancope/var/.

قد تكون هناك خطوات إضافية مطلوبة لاستخدام Stealthwatch لمساحة القرص غير المخصصة هذه بعد إعادة التشغيل، ومراجعة تخزين البيانات الخاص بدليل التثبيت لإصدار الجهاز الظاهري الخاص بك لمعرفة حجم القرص المطلوب.

حجم قسم الجذر (/) ثابت ولا يمكن تعديله. يلزم تثبيت جديد لإصدار يحتوي على قسم جذر أكبر تم إنشاؤه أثناء التثبيت.

معلومات ذات صلة

- أدلة التثبيت
- الدعم التقني والمستندات لتحليلات الشبكة الآمنة - Cisco Systems
- جهات اتصال دعم Cisco في جميع أنحاء العالم

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).