Lokaal bestandssysteem/schijfgebruik beheren in beveiligde netwerkanalyses

Inhoud

Inleiding

Dit document beschrijft algemene stappen om het hoge schijfgebruik op Secure Network Analytics Manager- en Flow Collector-apparaten te verminderen.

Voorwaarden

Vereisten

Dit document is van toepassing op Secure Network Analysis implementaties zonder Data Store.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Network Analytics Manager - v7.1+
- Secure Network Analysis Flow Collector - v7.1+
- Secure Network Analysis Flow Sensor - v7.1+
- Secure Network Analytics UDP Director - v7.1+

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Er zijn twee partities om te controleren op schijfgebruik, de wortel (/) en /lancope/var partities.

De root (/) partitie is de opslaglocatie voor de kernel afbeelding en sommige systeemlogbestanden, dit is meestal een kleinere parition van 20G of minder. De /lancope/var is een volumegroep en is de opslaglocatie voor het merendeel van de systeemgegevens, zodat het de meeste schijfruimte voor het apparaat in beslag neemt.

Verzamel gegevens

Er zijn twee plaatsen waar u informatie over schijfgebruik kunt verkrijgen, de admin web UI, en de opdrachtregel interface (CLI.)

Opdrachtregel

Vanuit de opdrachtregel voert u de **df -ah / /lancope/var** opdracht en noteer de spaties tussen (/) en /lancope/var.

```
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:/#
```

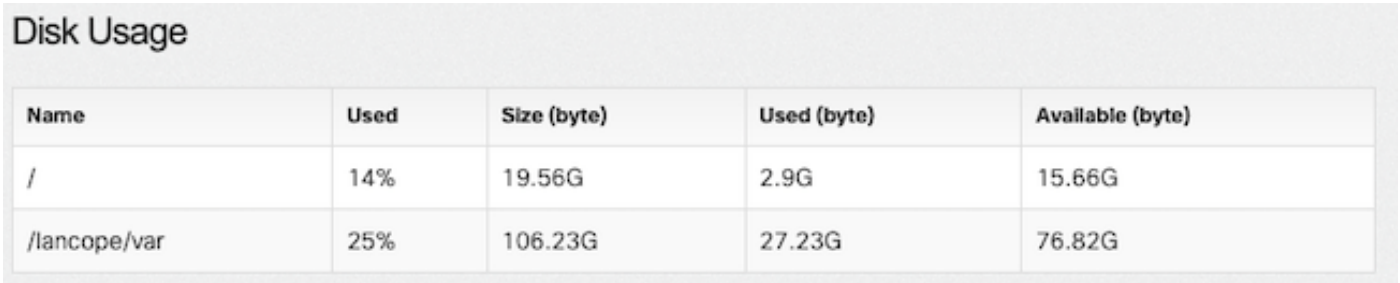
De output toont aan dat de wortel (/) scheiding 20G is, en 8.3G in gebruik is die 46% is. De output toont ook aan dat de /lancope/var verdeling 108G is, en 23G in gebruik is die 22% is.

Web UI

Log in op de apparaten Admin UI op basis van het model in kwestie, en schuif naar de onderkant van de pagina.

Lijst van Admin UI-webadressen:

- Secure Network Analysis Manager - https://<SMC-IP-OR-FQDN>/smc/index.html (u moet zich bij de SCM aanmelden voordat u deze URL kunt openen)
- Secure Network Analysis Flow Collector - https://<FC-IP-OR-FQDN>/swa/index.html
- Secure Network Analysis Flow Sensor - https://<FS-IP-OR-FQDN>/fs/index.html
- Secure Network Analysis UDP Director (Flow Replicator) - https://<UDPD-IP-OR-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

Als de verdeling hoog gebruik van groter dan of gelijk aan 75% heeft wordt de verdeling

benadrukt.

Schijfruimte wissen

Als u niet zeker weet welke bestanden verwijderd kunnen worden, opent u een TAC-case of neemt u contact op met Cisco's ondersteuning via de pagina Cisco's wereldwijde contactgegevens voor ondersteuning in het gedeelte Verwante informatie aan het einde van dit document.

Systeemlogbestanden

Een van de snelste methoden om grote schijfruimte te herstellen, is het wissen van dagboeklogboeken met de journalctl --vacuum-time 1d uit. Let op het dubbele koppelteken — voor het woord "vacuüm".

```
732smc:/# journalctl --vacuum-time 1d
Deleted archived journal /var/log/journal/639c60e1e407f646b5ed1751cde413fa
/user-1000@db376b09011842d5b247f6d31de6c241-00000000004ec2a8-0005e7838ecf15cc.journal (8.0M).
<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:/#
```

Ongeveer 4G van schijfruimte werd teruggewonnen van deze stappen en resulteerde in een vermindering van schijfgebruik van 22% tot 18% op de /lancope/var verdeling.

Bestanden in de genoemde mappen zijn over het algemeen veilig te verwijderen:

```
/lancope/var/tcpdump
/lancope/var/tomcat/logs
/lancope/var/tmp
/lancope/var/admin/tmp/
```

Het wordt aanbevolen om te beginnen bij de root (/) of /lancope/var directory, welke partitie u ook hebt geïdentificeerd in de web ui die veel schijfgebruik heeft. Verander de huidige map met de cd / uit.

Draai de du -xah --max-depth=1 | sort -hr bevel om de grootste consumenten van schijfruimte van de huidige folder te bepalen. Noteer het dubbele koppelteken — vóór de maximale diepte.

De output toont aan dat de wortel (/) verdeling 8.3G schijfruimte in gebruik heeft, met 5.5G van schijfruimte die in de /lancope folder wordt gebruikt, die door de /usr folder met 1.5G van gebruik wordt gevolgd.

```
732smc:~# cd /
732smc:/# du -xah --max-depth=1 | sort -hr | head -n4
8.3G .
5.5G ./lancope
1.5G ./usr
1.3G ./opt
```

```
732smc:/#
```

Wijzig de directory in /lancope met de **cd lancope/** de opdracht beëindigen en de opdracht du opnieuw uitgeven met de !du uit. Dit toont nu dat van de 5.5G in gebruik in de /lancope/ folder, 5.1G in de admin folder is. Verander de huidige directory's in de directory in kwestie met de cd uit.

```
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#
```

Zodra u bestanden identificeert die kunnen worden verwijderd, kunt u dit doen met de **rm -i** uit. Als u niet zeker weet welke bestanden verwijderd kunnen worden, opent u een TAC-case of neemt u contact op met Cisco's ondersteuning via de pagina Cisco's wereldwijde contactgegevens voor ondersteuning in het gedeelte Verwante informatie aan het einde van dit document.

```
732smc:/lancope/admin# rm -i file
rm: remove regular empty file 'file'? yes
732smc:/lancope/admin#
```

Herhaal deze stappen indien nodig.

Trim de gedistribueerde database (DDS) - Flow Stats

In de DDS-omgeving proberen de FlowCollector- en SMC-apparaten standaard elke dag zo veel mogelijk stroomgegevens op te slaan. Wanneer de beperkingen van het schijfgebruik worden geraakt, begint het systeem de oudste gegevens eerst te wissen om ruimte voor nieuwe gegevens te creëren die moeten worden opgeslagen.

Om de Flow Collector-databasestatistieken te zien, logt u in op de FlowCollector Admin UI en selecteert u vervolgens Support > Database Storage Statistics .

- De afbeelding laat zien dat de geconsumeerde Flow Details (netflow data) gemiddeld ongeveer 455MB per dag is en dat deze Flow Collector ongeveer 25.5G aan opgeslagen gegevens heeft.
- De afbeelding laat zien dat de geconsumeerde Flow Interface Details (interface-specifieke statistieken) gemiddeld ongeveer 800MB per dag en deze Flow Collector heeft ongeveer 6G van opgeslagen gegevens.
- De afbeelding laat zien dat de totale Flow Data gemiddeld ongeveer 1.2GB per dag en deze Flow Collector heeft ongeveer 32G van de totale opgeslagen gegevens.
- Als u de database wilt bijsnijden om ongeveer 5G van de totale opgeslagen gegevens te hebben, verdeel dat door het dagelijkse gemiddelde van 1.2G dat gelijk is aan 4.

Om de database te reduceren tot een totale grootte van ongeveer 5 Gb, wijzigt u de **O**ummary_retention_days waarde 4. Navigeer vervolgens naar Support > Advanced Settings . Zoeken summary_retention_days en verander dit in de gewenste waarde.

Voeg vervolgens een nieuwe optie toe onder in de lijst. Het Add New Option waarde is strict_retention_days en de **Option Value** De waarde wordt ingesteld op 1 zoals in de afbeelding. Klik op Add (Toevoegen). Dit strict_retention_days vertelt de motor alleen het aantal dagen te bewaren dat is opgegeven in **O**ummary_retention_days .

Zodra ik de **summary_retention_days** aan 4 en ik heb de nieuwe optie waarde toegevoegd, druk op Apply onderaan de pagina.

Als deze stappen voor een upgrade worden uitgevoerd, verwijdert u de **strict_retention_days** waarde na voltooiing van de upgrade om gegevens zo lang mogelijk te bewaren.

Trim de gedistribueerde database (DDS) - Flow Interface Details

1. Logboek inin uw Stealthwatch Desktop Klant als het beheerder gebruiker.

2. Zoek de Flow Collector in de Enterprise Tree. Klik op de plus (+) teken om de container uit te breiden.

3. Klik met de rechtermuisknop op de gewenste Flow Collector. Kiezen Configuration > Properties.

4. In het StroomVerzamelaar Eigenschappen dialogeren doos, klikken Advanced.

5. Kiezen het Store **flow interface data**veld. instellen het limiet in Omhoog in 15 dagen of 30 dagen.

6. Klik OK .

Vergroot de schijfruimte (alleen virtuele applicaties)

Schakel de virtuele machine uit en verhoog de schijfgrootte die via de hypervisor aan de VM is toegewezen. De extra schijfruimte wordt toegewezen aan de /lancope/var/ partitie.

Er kunnen extra stappen nodig zijn om Stealthwatch in staat te stellen deze niet-toegewezen schijfruimte te gebruiken na het opnieuw opstarten van het programma. Raadpleeg voor de vereiste schijfgrootte de handleiding voor gegevensopslag van de installatiegids voor uw virtuele machine.

De root (/) partitiegrootte is statisch en kan niet worden aangepast. Een frisse installatie aan een versie die een grotere wortelverdeling heeft die tijdens installatie wordt gemaakt wordt vereist.

Gerelateerde informatie

- Installatiehandleidingen
- Technische ondersteuning en documentatie voor Secure Network Analytics - Cisco Systems
- Cisco’s wereldwijde contactgegevens voor ondersteuning

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.