Manage Local Filesystem/Disk Usage in Secure Network Analytics

Contents

Introduction

This document describes general steps to decrease high disk usage on Secure Network Analytics Manager and Flow Collector devices.

Prerequisites

Requirements

This document applies to Secure Network Analytic deployments without Data Store.

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

There are two partitions to monitor for disk usage, the root (/) and /lancope/var partitions.

The root (/) partition is the storage location for the kernel image and some system logs, this is usually a smaller parition of 20G or less. The /lancope/var is a volume group and it is the storage location for the majority of system data so it consumes the majority of disk space for the appliance.

Gather Data

There are two places you can obtain disk usage information, the admin web UI, and the command line interface (CLI.)

Command Line

From the command line run the **df -ah / /lancope/var** command and note the spaces between (/) and /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:/#
```

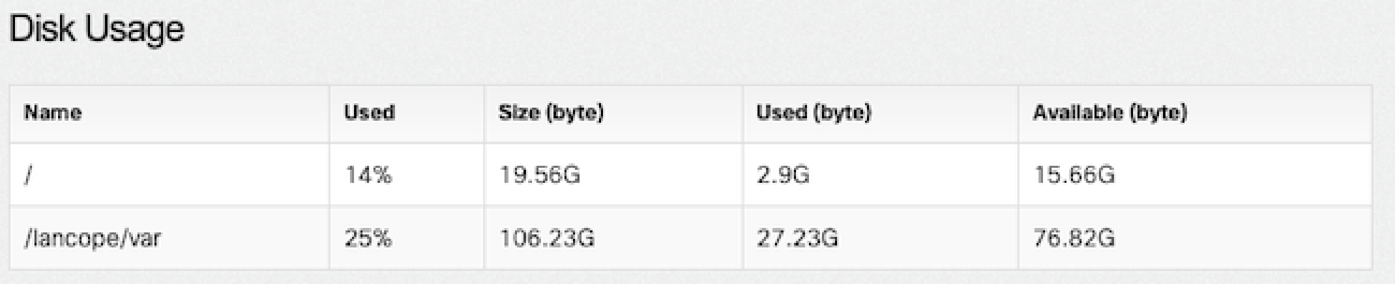
The output shows that the root (/) parition is 20G, and 8.3G is in use which is 46%. The output also shows that the /lancope/var partition is 108G, and 23G is in use which is 22%.

Web UI

Log into the devices Admin UI based on the model in question, and scroll to the bottom of the page.

List of Admin UI web addresses:

- Secure Network Analytics Manager - https://<SMC-IP-OR-FQDN>/smc/index.html (You must log into the SMC before you can access this URL)
- Secure Network Analytics Flow Collector - https://<FC-IP-OR-FQDN>/swa/index.html
- Secure Network Analytics Flow Sensor - https://<FS-IP-OR-FQDN>/fs/index.html
- Secure Network Analytics 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

If the partition has high usage of greater than or equal to 75% the partition is highlighted.

Clear Disk Space

If you are unsure which files are safe to delete, open a TAC case or contact CIsco Support via the Cisco Worldwide Support Contact page in the Related Information section at the end of this document.

System Logs

One of the fastest methods to recover sizable disk space is to clear journal logs with the journalctl --vacuum-time 1d command. Note the double hyphen -- before the word "vacuum".

```
732smc:/# journalctl --vacuum-time 1d
Deleted archived journal /var/log/journal/639c60e1e407f646b5ed1751cde413fa
                 /user-1000@db376b09011842d5b247f6d31de6c241-00000000004ec2a8-0005e7838ecf15cc.journal
<the above line repeats for each file deleted>
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:/#
```

About 4G of disk space was reclaimed from these steps and resulted in a decrease of disk usage from 22% to 18% on the /lancope/var partition.

Another location for journal log entries is **/lancope/var/logs/journal** directory which can also be cleared with the **journalctl --vacuum-time 1d -D /lancope/var/logs/journal/** command.

```
732smc:~# journalctl --vacuum-time 1d -D /lancope/var/logs/journal/
Deleted archived journal /lancope/var/logs/journal//639c60e1e407f646b5ed1751cde413fa/system@23219d08850
<the above line repeats for each file deleted>
Vacuuming done, freed 784.0M of archived journals from /lancope/var/logs/journal//639c60e1e407f646b5ed1
732smc:~#
```

Files in the listed directories are generally safe to delete:

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

It is recommended to start at either the root (/) or /lancope/var directory, whichever partition you identified in the web ui that has high disk usage. Change the current directory with the cd / command.

Run the du -xah --max-depth=1 | sort -hr command to determine the largest consumers of disk space of the current directory. Note the double hyphen -- before max-depth.

The output shows that the root (/) partition has 8.3G disk space in use, with 5.5G of disk space used in the /lancope directory, followed by the /usr directory with 1.5G of usage.

The use of the **| head -n4** in the command is not required and used in the example to limit the results returned.

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

Change directory to /lancope with the **cd lancop**e/ command and re-issue the du command with the !du command. This now displays that of the 5.5G in use in the /lancope/ directory, 5.1G is in the admin directory. Change the current directories to the directory in question with the cd command.

```
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#
```

Once you identify files that can be deleted, you can do so with the rm -i <filename> command. If you are unsure which files are safe to delete, open a TAC case or contact CIsco Support via the Cisco Worldwide Support Contact page in the Related Information section at the end of this document.

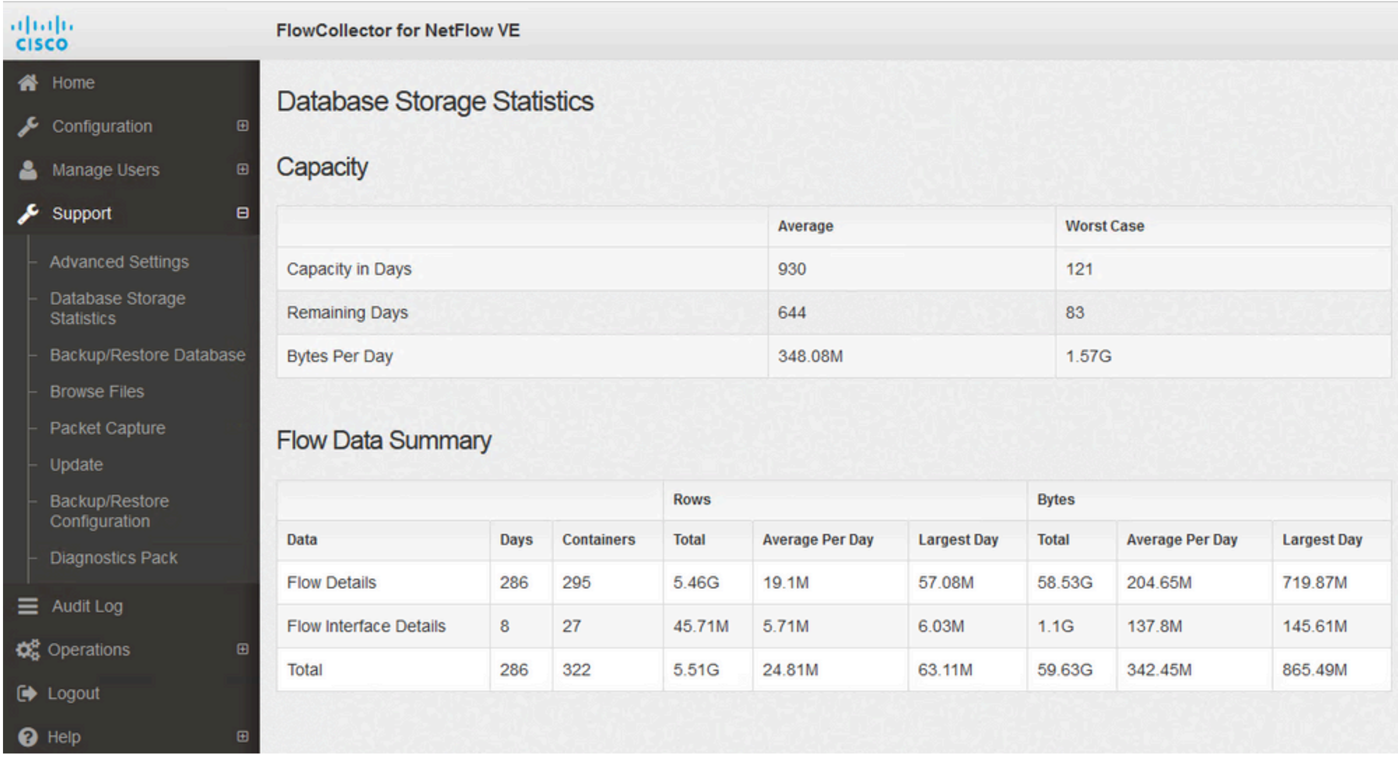
```
732smc:/lancope/admin# rm -i file
rm: remove regular empty file 'file'? yes
732smc:/lancope/admin#
```

Repeat these steps as necessary.

Trim the Distributed Database (DDS) - Flow Stats

By default, in the DDS environment, the FlowCollector and SMC appliances attempt to store as much flow data as possible rotated on a daily basis. When disk usage limits are hit, the system begins to delete the oldest data first to create room for new data to be saved.

To see the Flow Collector database statistics, log into the FlowCollector Admin UI and then select Support > Database Storage Statistics .



Database Storage Statistics

Capacity

	Average	Worst Case
Capacity in Days	930	121
Remaining Days	644	83
Bytes Per Day	348.08M	1.57G

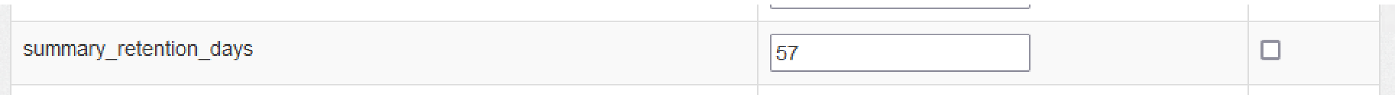
Flow Data Summary

			Rows			Bytes		
Data	Days	Containers	Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	286	295	5.46G	19.1M	57.08M	58.53G	204.65M	719.87M
Flow Interface Details	8	27	45.71M	5.71M	6.03M	1.1G	137.8M	145.61M
Total	286	322	5.51G	24.81M	63.11M	59.63G	342.45M	865.49M

Database Storage Statistics

- The image shows that the ingested Flow Details (netflow data) averages about 204.65MB a day and this Flow Collector has about 58.5GB of data stored.
- The image shows that the ingested Flow Interface Details (interface specific statistics) averages abour 137MB a day and this Flow Collector has about 1.1GB of data stored.
- The image shows that the total Flow Data averages about 342.53MB a day and this Flow Collector has about 60GB of total data stored.
- If you want to trim the database down to have about 20G of total data stored, divide that by the daily average of .35G which equals 57.

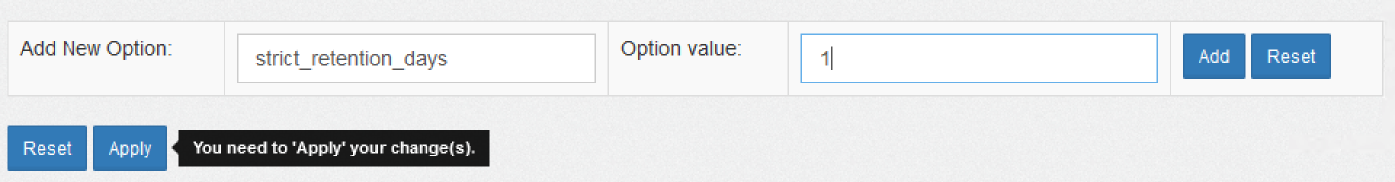
To reduce the database to have a total size of about 20Gb, change the summary_retention_days value to 57. Next, navigate to Support > Advanced Settings . Find summary_retention_days and change this to your desired value.



summary_retention_days	57	□

summary_retention_days

Next, add a new option at the bottom of the list. The Add New Option value is strict_retention_days and the Option Value value is set to 1 as shown in the image. Click Add. This strict_retention_days tells the engine to only keep the # of days declared in summary_retention_days .



Add New Option: strict_retention_days

Option value: 1

You need to 'Apply' your change(s).

strict_retention_days

Once I have changed the **summary_retention_days** to 4 and I have added the new option value, press Apply at the bottom of the page.

If these steps for an upgrade, delete the **strict_retention_days** value once the upgrade is complete to return to retain data for as long as possible.

Trim the Distributed Database (DDS) - Flow Interface Details

1. Log into your Stealthwatch Desktop Client as the admin user.

2. Locate the FlowCollector in the Enterprise Tree. Click the plus (+) sign to expand the container.

3. Right-click the desired FlowCollector. Select Configuration > Properties.

4. In the FlowCollector Properties dialog box, click Advanced.

5. Select the Store **flow interface data**field. Set the limit to Up to 15 days or 30 days.

6. Click OK .

Increase Disk Space (Virtual Appliances Only)

Power off the virtual machine, and increase the disk size allocated to the VM from the hypervisor. The additional disk space is allocated to the /lancope/var/ partition.

Additional Steps could be required for Stealthwatch to consume this unallocated disk space after a reboot, review the Data Storage of the Installation guide for your virtual machine edition for the required disk size.

The root (/) partition size is static and cannot be adjusted. A fresh install to a version that has a larger root partition created during installation is required.

Related Information

- Installation Guides
- Secure Network Analytics Technical Support & Documentation - Cisco Systems
- Cisco Worldwide Support Contacts