Gestion de l'utilisation du système de fichiers local/disque dans Secure Network Analytics

Table des matières

Introduction

Ce document décrit les étapes générales pour réduire l'utilisation élevée du disque sur les périphériques Secure Network Analytics Manager et Flow Collector.

Conditions préalables

Exigences

Ce document s'applique aux déploiements Secure Network Analytic sans Data Store.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gestionnaire Secure Network Analytics - v7.1+
- Collecteur de flux Secure Network Analytics - v7.1+
- Capteur de flux Secure Network Analytics - 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Il existe deux partitions à surveiller pour l'utilisation du disque, les partitions racine (/) et /lancope/var.

La partition racine (/) est l'emplacement de stockage de l'image du noyau et de certains journaux système. Il s'agit généralement d'une partition plus petite de 20 Go ou moins. /lancope/var est un groupe de volumes et est l'emplacement de stockage de la majorité des données système. Il consomme donc la majorité de l'espace disque de l'appliance.

Collecter des données

Il existe deux emplacements où vous pouvez obtenir des informations sur l'utilisation du disque : l'interface utilisateur Web d'administration et l'interface de ligne de commande (CLI).

Ligne de commande

À partir de la ligne de commande, exécutez **df -ah / /lancope/var** la commande et notez les espaces entre (/) et /lancope/var.

```
732smc:/# df -ah / /lancope/var/ Filesystem Size Used Avail Use% Mounted on /dev/sda2 20G 8.3G 9.9G 46%
```

Le résultat montre que la partition racine (/) est 20G, et 8.3G est en cours d'utilisation, ce qui représente 46 %. Le résultat montre également que la partition /lancope/var est 108G et que la partition 23G est utilisée, ce qui représente 22 %.

Interface utilisateur Web

Connectez-vous à l'interface utilisateur Admin des périphériques en fonction du modèle en question et faites défiler la page jusqu'en bas.

Liste des adresses Web de l'interface administrateur :

- Secure Network Analytics Manager - https://<SMC-IP-OR-FQDN>/smc/index.html (Vous devez vous connecter au SMC pour pouvoir accéder à cette 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

Si la partition a une utilisation élevée supérieure ou égale à 75 %, la partition est mise en surbrillance.

Effacer l'espace disque

Si vous ne savez pas quels fichiers supprimer en toute sécurité, ouvrez un dossier TAC ou contactez le support Cisco via la page de contact du support international Cisco dans la section Informations connexes à la fin de ce document.

Journaux du système

L'une des méthodes les plus rapides pour récupérer un espace disque important consiste à effacer les journaux à l'aide de la commandejournalctl --vacuum-time 1d . Notez le tiret double — avant le mot « vacuum ».

```
732smc:/# journalctl --vacuum-time 1d Deleted archived journal /var/log/journal/639c60e1e407f646b5ed175
```

Environ 4 Go d'espace disque ont été récupérés à partir de ces étapes et ont entraîné une diminution de l'utilisation du disque de 22 % à 18 % sur la partition /lancope/var.

Un autre emplacement pour les entrées du journal est le **/lancope/var/logs/journal** répertoire qui peut également être effacé avec la **journalctl --vacuum-time 1d -D /lancope/var/logs/journal/** commande.

```
732smc:~# journalctl --vacuum-time 1d -D /lancope/var/logs/journal/ Deleted archived journal /lancope/v
```

Les fichiers des répertoires répertoriés peuvent généralement être supprimés en toute sécurité :

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

Il est recommandé de commencer par le répertoire racine (/) ou /lancope/var, quelle que soit la partition que vous avez identifiée dans l'interface utilisateur Web qui a une utilisation élevée du disque. Modifiez le répertoire actif à l'aide de la commandecd / .

Exécutez la commandedu -xah --max-depth=1 | sort -hr pour déterminer les consommateurs les plus importants d'espace disque du répertoire actuel. Notez le trait d'union double — avant la profondeur maximale.

Le résultat montre que la partition racine (/) a 8,3 G d'espace disque en cours d'utilisation, avec 5,5 G d'espace disque utilisé dans le répertoire /lancope, suivi du répertoire /usr avec 1,5 G d'utilisation.

L'utilisation de **| head -n4** dans la commande n'est pas obligatoire et est utilisée dans l'exemple pour limiter les résultats renvoyés.

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

Remplacez le répertoire par /lancope avec la **cd lancop**e/ commande et réexécutez la commande du avec la !du commande. Ceci affiche maintenant que de la 5.5G utilisée dans le répertoire /lancope/, 5.1G est dans le répertoire admin. Remplacez les répertoires actuels par le répertoire en question à l'aide de la commandecd .

```
732smc:/# cd lancope/ 732smc:/lancope# !du du -xah --max-depth=1 | sort -hr | head -n4 5.5G . 5.1G ./ad
```

Une fois que vous avez identifié les fichiers qui peuvent être supprimés, vous pouvez le faire à l'aide de la commanderm -i <filename>. Si vous ne savez pas quels fichiers supprimer en toute sécurité, ouvrez un dossier TAC ou contactez le support Cisco via la page de contact du support international Cisco dans la section Informations connexes à la fin de ce document.

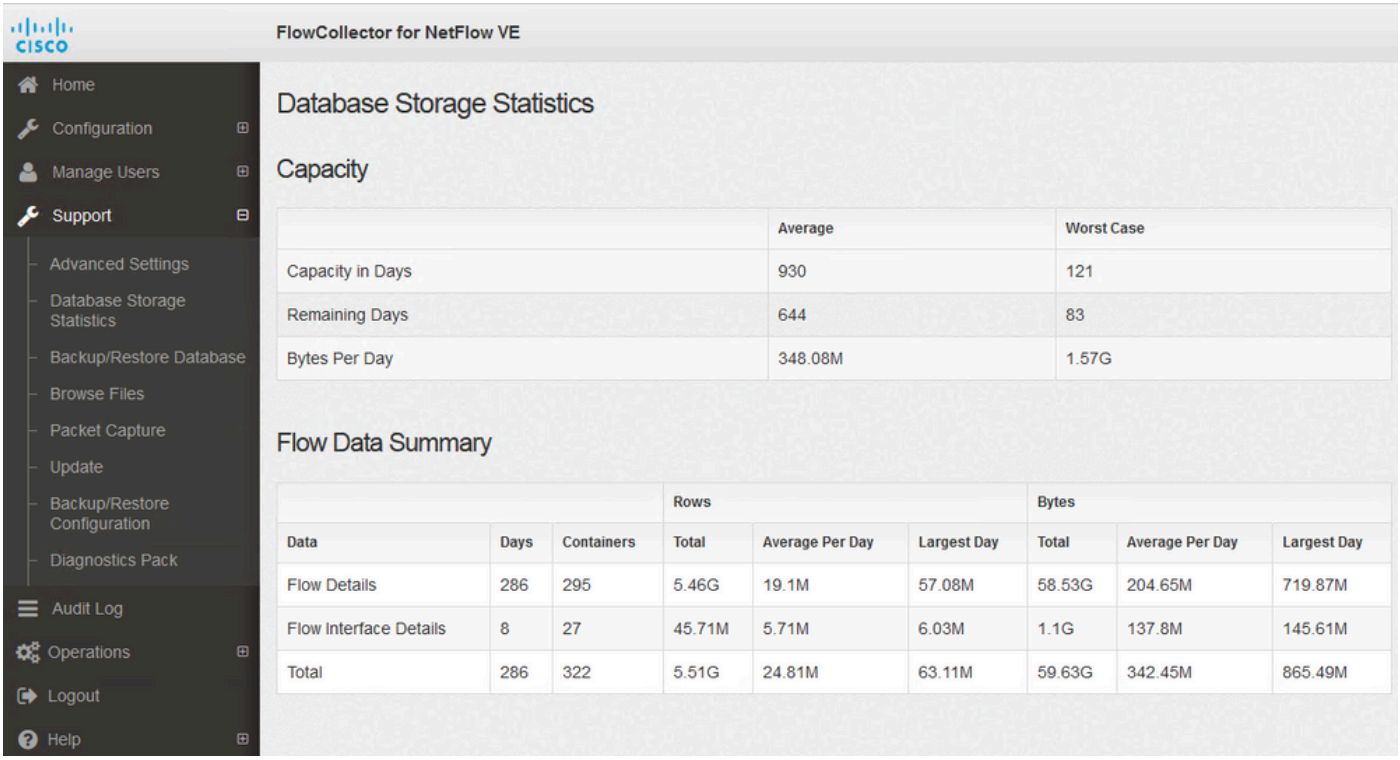
```
732smc:/lancope/admin# rm -i file rm: remove regular empty file 'file'? yes 732smc:/lancope/admin#
```

Répétez ces étapes si nécessaire.

Ajuster la base de données distribuée (DDS) - Statistiques de flux

Par défaut, dans l'environnement DDS, les appliances FlowCollector et SMC essaient de stocker autant de données de flux que possible en les faisant pivoter quotidiennement. Lorsque les limites d'utilisation du disque sont atteintes, le système commence par supprimer les données les plus anciennes afin de libérer de l'espace pour l'enregistrement de nouvelles données.

Pour afficher les statistiques de la base de données du collecteur de flux, connectez-vous à l'interface utilisateur Admin de FlowCollector, puis sélectionnez Support > Database Storage Statistics .



Statistiques de stockage de base de données

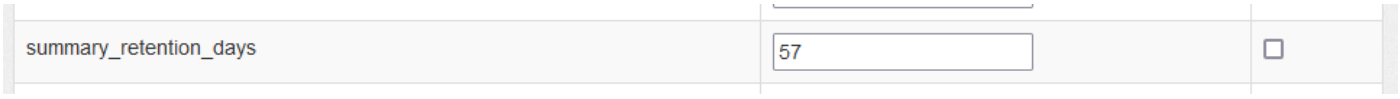
- L'image montre que les détails de flux ingérés (données netflow) atteignent en moyenne environ 204,65 Mo par jour et que ce collecteur de flux stocke environ 58,5 Go de données.

- L'image montre que les détails de l'interface de flux ingérée (statistiques spécifiques à l'interface) atteignent en moyenne 137 Mo par jour et que ce collecteur de flux stocke environ 1,1 Go de données.

- L'image montre que le total des données de flux est en moyenne d'environ 342,53 Mo par jour et que ce collecteur de flux a environ 60 Go de données totales stockées.

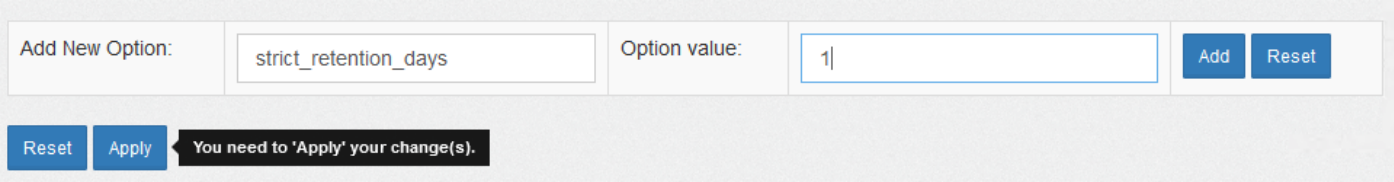
- Si vous voulez réduire la base de données pour avoir environ 20 G de données totales stockées, divisez cela par la moyenne quotidienne de 0,35 G, ce qui équivaut à 57.

Pour réduire la taille totale de la base de données à environ 20 Go, remplacez la valeur **s**ummary_retention_days par 57. Ensuite, accédez à Support > Advanced Settings . Find summary_retention_days et modifiez-le à la valeur souhaitée.



summary_retention_days

Ajoutez ensuite une nouvelle option au bas de la liste. La Add New Option valeur est strict_retention_days et la valeurOption Value est définie sur 1, comme illustré dans l'image. Cliquez sur Add. Ceci strict_retention_days indique au moteur de ne conserver que le nombre de jours déclaré dans **s**ummary_retention_days .



jours_rétention_stricts

Une fois que j'ai remplacé la valeur **summary_retention_days** par 4 et que j'ai ajouté la nouvelle valeur d'option, appuyez sur Apply au bas de la page.

Si vous effectuez ces étapes pour une mise à niveau, supprimez la **strict_retention_days** valeur une fois la mise à niveau terminée pour revenir à l'étape précédente afin de conserver les données aussi longtemps que possible.

Ajuster la base de données distribuée (DDS) - Détails de l'interface de flux

1. Connectez-vous à votre client StealthWatch Desktop Client en tant qu'utilisateur admin.

2. Localisez le FlowCollector dans l'arborescence d'entreprise. Cliquez sur le signe plus (+) pour développer le conteneur.

3. Cliquez avec le bouton droit sur le collecteur de flux souhaité. Sélectionnez Configuration > Properties.

4. Dans la boîte de dialogue Propriétés de FlowCollector, cliquez sur Advanced.

5. Sélectionnez le Store **flow interface data**champ. Définissez la limite sur Jusqu'à 15 jours ou 30 jours.

6. Cliquez sur OK .

Augmenter l'espace disque (appliances virtuelles uniquement)

Mettez la machine virtuelle hors tension et augmentez la taille du disque alloué à la machine virtuelle à partir de l'hyperviseur. L'espace disque supplémentaire est alloué à la partition /lancope/var/.

Des étapes supplémentaires peuvent être nécessaires pour que StealthWatch utilise cet espace disque non alloué après un redémarrage. Pour connaître la taille de disque requise, consultez le guide Data Storage of the Installation de votre édition de machine virtuelle.

La taille de la partition racine (/) est statique et ne peut pas être ajustée. Une nouvelle installation d'une version dont la partition racine est plus importante et créée lors de l'installation est requise.

Informations connexes

- Guides d'installation
- Assistance technique et documentation Secure Network Analytics - Cisco Systems
- Coordonnées du service d’assistance Cisco à l’échelle mondiale

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.