Administrar el uso de disco/sistema de archivos locales en Secure Network Analytics

Contenido

Introducción

Este documento describe los pasos generales para disminuir el uso elevado de disco en los dispositivos Secure Network Analytics Manager y Flow Collector.

Prerequisites

Requirements

Este documento se aplica a las implementaciones de Secure Network Analytic sin almacenamiento de datos.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Hay dos particiones para supervisar el uso del disco: las particiones root (/) y /lancope/var.

La partición raíz (/) es la ubicación de almacenamiento para la imagen del núcleo y algunos registros del sistema, esta es generalmente una partición más pequeña de 20G o menos. /lancope/var es un grupo de volumen y es la ubicación de almacenamiento para la mayoría de los datos del sistema, por lo que consume la mayor parte del espacio en disco para el dispositivo.

Recopilar datos

Hay dos lugares en los que puede obtener información sobre el uso del disco: la interfaz de usuario web de administración y la interfaz de línea de comandos (CLI).

Línea de comandos

Desde la línea de comandos, ejecute el comando **df -ah / /lancope/var** y observe los espacios entre (/) y /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:/#
```

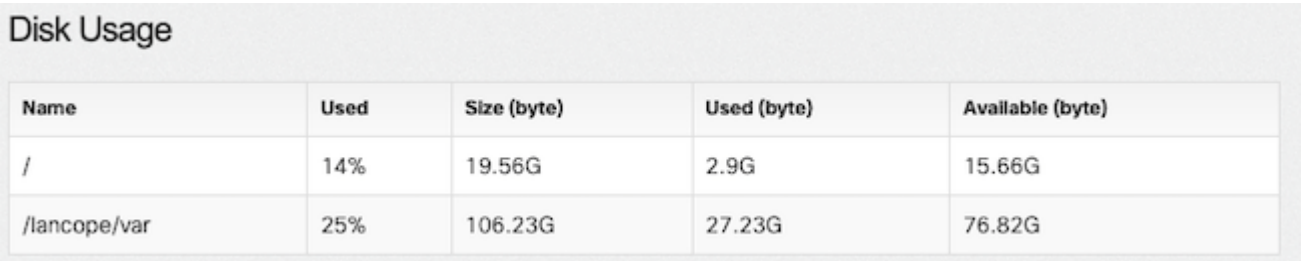
El resultado muestra que la partición raíz (/) es 20G y 8.3G está en uso, lo que representa el 46%. La salida también muestra que la partición /lancope/var es 108G, y 23G está en uso, que es 22%.

IU web

Inicie sesión en la interfaz de usuario de administración de dispositivos según el modelo en cuestión y desplácese hasta la parte inferior de la página.

Lista de direcciones web de IU de administrador:

- Secure Network Analytics Manager: https://<SMC-IP-OR-FQDN>/smc/index.html (debe iniciar sesión en SMC antes de poder acceder a esta URL)
- Recopilador de flujos de Secure Network Analytics - https://<FC-IP-OR-FQDN>/swa/index.html
- Sensor de flujo de Secure Network Analytics - https://<FS-IP-OR-FQDN>/fs/index.html
- UDP Director (Flow Replicator) de Secure Network Analytics - https://<UDPD-IP-OR-FQDN>/fr/index.html



Si la partición tiene un uso alto mayor o igual al 75%, la partición se resalta.

Borrar espacio en disco

Si no está seguro de qué archivos es seguro eliminar, abra un caso TAC o póngase en contacto con el Soporte de Cisco a través de la página Contacto de Soporte de Cisco en la sección Información Relacionada al final de este documento.

Registros del sistema

Uno de los métodos más rápidos para recuperar un espacio de disco considerable es borrar los registros del diario con el journalctl --vacuum-time 1d comando. Observe el guión doble, antes de la palabra "vacío".

<#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:/#

Se recuperó aproximadamente 4G de espacio en disco de estos pasos y resultó en una disminución del uso de disco de 22% a 18% en la partición /lancope/var.

Por lo general, los archivos de los directorios enumerados son seguros de eliminar:

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

Se recomienda comenzar en el directorio raíz (/) o /lancope/var, cualquiera que sea la partición identificada en la interfaz de usuario web que tiene un uso de disco alto. Cambie el directorio actual con el cd / comando.

Ejecute el du -xah --max-depth=1 | sort -hr para determinar los consumidores más grandes de espacio en disco del directorio actual. Observe el guión doble, antes de max-depth.

El resultado muestra que la partición raíz (/) tiene 8.3G de espacio en disco en uso, con 5.5G de espacio en disco utilizado en el directorio /lancope, seguido por el directorio /usr con 1.5G de uso.

<#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:/#
```

Cambie el directorio a /lancope con el **cd lancop**e/ y vuelva a ejecutar el comando du con el comando !du comando. Esto ahora muestra que del 5.5G en uso en el directorio /lancope/, 5.1G está en el directorio admin. Cambie los directorios actuales por el directorio en cuestión con el cd comando.

<#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#
```

Una vez que identifique los archivos que se pueden eliminar, puede hacerlo con el comando rm -i comando. Si no está seguro de qué archivos es seguro eliminar, abra un caso TAC o póngase en contacto con el Soporte de Cisco a través de la página Contacto de Soporte de Cisco en la sección Información Relacionada al final de este documento.

<#root>

```
732smc:/lancope/admin#
```

rm -i file

```
rm: remove regular empty file 'file'?
```

yes

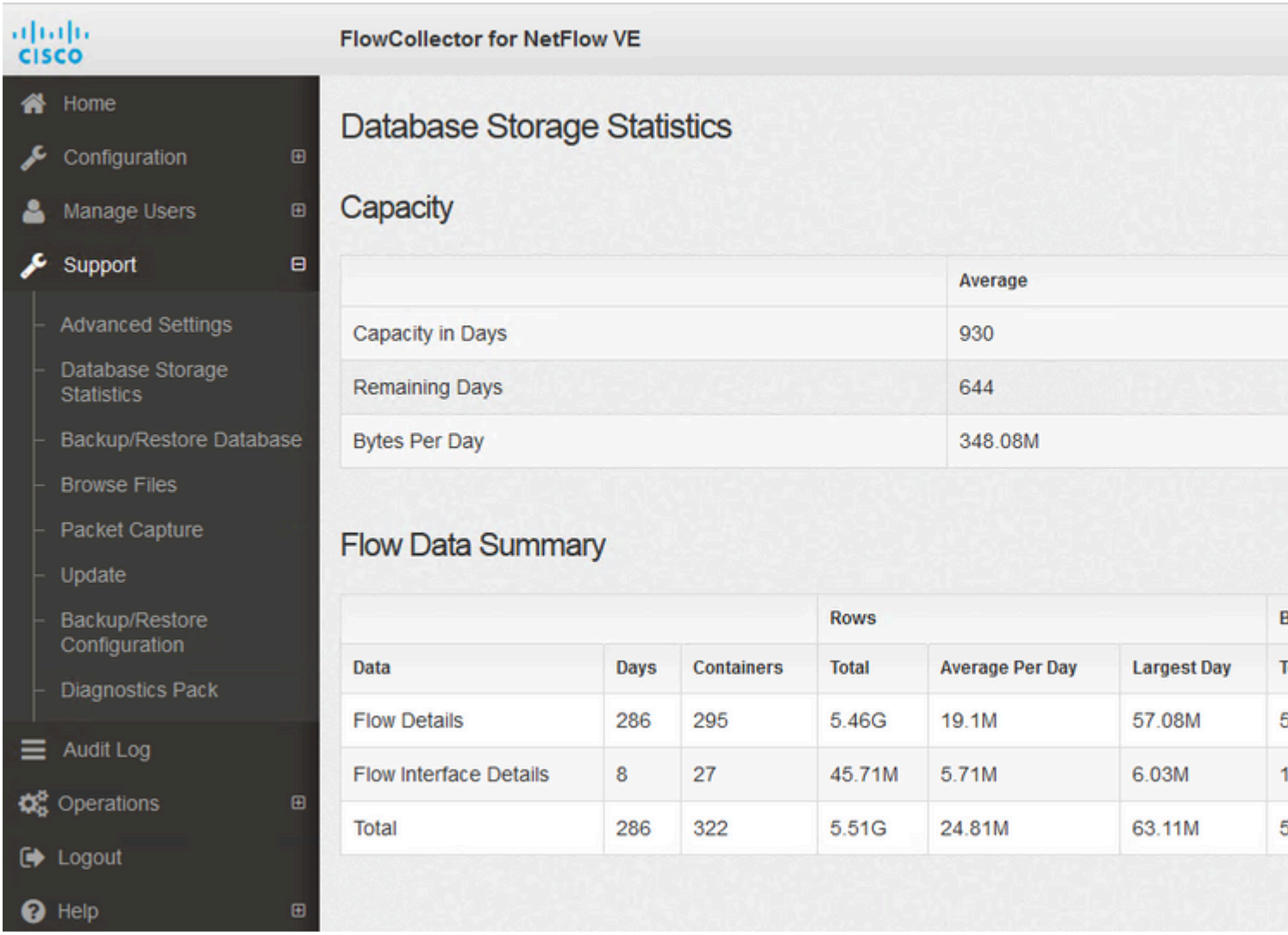
```
732smc:/lancope/admin#
```

Repita estos pasos según sea necesario.

Recorte de la base de datos distribuida (DDS): estadísticas de flujo

De forma predeterminada, en el entorno DDS, los appliances FlowCollector y SMC intentan almacenar todos los datos de flujo que sea posible rotando a diario. Cuando se alcanzan los límites de uso del disco, el sistema comienza a eliminar primero los datos más antiguos para crear espacio para que se guarden los nuevos datos.

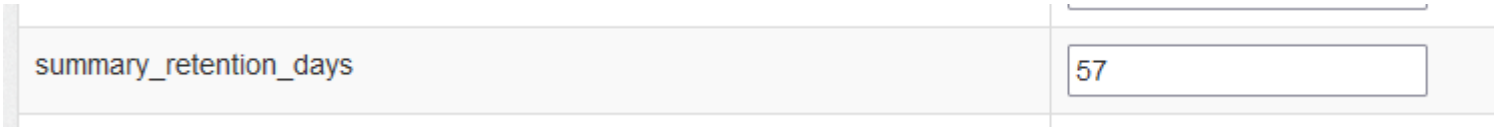
Para ver las estadísticas de la base de datos de Flow Collector, inicie sesión en la interfaz de usuario de administración de FlowCollector y seleccione Support > Database Storage Statistics .



Estadísticas de almacenamiento de base de datos

- La imagen muestra que los detalles de flujo ingeridos (datos de NetFlow) promedian unos 204,65 MB al día y este Flow Collector tiene almacenados unos 58,5 GB de datos.
- La imagen muestra que los detalles de la interfaz de flujo ingeridos (estadísticas específicas de la interfaz) alcanzan un promedio de aproximadamente 137 MB al día y este Flow Collector tiene almacenados aproximadamente 1,1 GB de datos.
- La imagen muestra que el total de datos de flujo promedia alrededor de 342.53GB al día y este Flow Collector tiene alrededor de 60GB de datos totales almacenados.
- Si desea recortar la base de datos para almacenar aproximadamente 20 G de datos totales, divídala por el promedio diario de 0,35 G, que equivale a 57.

Para reducir la base de datos a un tamaño total de unos 20 Gb, cambie el **s**ummary_retention_days valor a 57. A continuación, vaya a Support > Advanced Settings . Buscar summary_retention_days y cámbielo al valor que desee.



summary_maintenance_days

A continuación, agregue una nueva opción al final de la lista. Add New Option el valor es strict_retention_days y el Option Value el valor se establece en 1 como se muestra en la imagen. Haga clic en Add (Agregar). Esto strict_retention_days indica al motor que sólo mantenga el número de días declarado en **s**ummary_retention_days .

valor una vez que se completa la actualización para volver a conservar los datos durante el mayor tiempo posible.

Recorte de la base de datos distribuida (DDS): detalles de la interfaz de flujo

1. Registro ina su StealthWatch Escritorio Cliente como admin usuario.

2. Busque el FlowCollector en el árbol de la empresa. Haga clic en el signo más (+) firma para expandir el contenedor.

3. Haga clic con el botón secundario en el FlowCollector deseado. Seleccionar Configuration > Properties.

4. IN FlujoRecopilador Propiedades diálogo caja, clic Advanced.

5. Seleccionar Store **flow interface data**campo. Set límite a En funcionamiento a 15 días or 30 días.

6. Haga clic en OK .

Aumentar el espacio en disco (sólo dispositivos virtuales)

Apague la máquina virtual y aumente el tamaño del disco asignado a la máquina virtual desde el hipervisor. El espacio de disco adicional se asigna a la partición /lancope/var/.

Es posible que sea necesario realizar pasos adicionales para que StealthWatch consuma este espacio de disco sin asignar después de un reinicio. Consulte la sección Almacenamiento de datos de la guía de instalación de la edición de máquina virtual para obtener el tamaño de disco necesario.

El tamaño de la partición raíz (/) es estático y no se puede ajustar. Se requiere una instalación nueva en una versión que tenga una partición raíz más grande creada durante la instalación.

Información Relacionada

- Guías de instalación
- Documentación y soporte técnico de Secure Network Analytics - Cisco Systems
- Contactos de soporte global de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).