Contenido

Introducción

Un centro de administración de FireSIGHT o un dispositivo de la potencia de fuego puede ejecutarse fuera del espacio en disco por las diversas razones. Cuando sucede, la alta utilización del disco acciona la alerta de la salud o puede fallar una tentativa de la actualización de software. Este artículo describe las causas raíz de la utilización excesiva del disco y de algunos pasos de Troubleshooting.

Pasos de verificación

Determine la división que se utiliza altamente. El siguiente comando muestra la utilización del disco:

En un centro de administración de FireSIGHT,

```
admin@3DSystem:~# df -TH
```

En los dispositivos de las 7000 y 8000 Series y en los dispositivos virtuales NGIPS,

```
> show disk
```

Los comandos both muestran una salida como abajo:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda5 2.9G 566M 2.2G 21% /
/dev/sda1 99M 16M 79M 17% /boot
/dev/sda7 52G 8.5G 41G 18% /Volume
none 11G 20K 11G 1% /dev/shm
/dev/sdb1 418G 210M 395G 1% /var/storage
```

> Nota: El tamaño y la utilización del disco pueden variar en los diversos modelos del dispositivo. Si esto es un dispositivo virtual NGIPS, verifique que el tamaño de las divisiones cumpla con los requisitos de espacio de disco mínimos.

Precaución: Cualquier división adicional que no se muestre arriba está sin apoyo.

En los dispositivos de las 7000 y 8000 Series y en los dispositivos virtuales NGIPS, usted puede funcionar con el siguiente comando de visualizar las estadísticas detalladas del uso del disco:

```
> show disk-manager
```

Una salida de ejemplo:

```
> show disk-manager
Silo Used Minimum Maximum
Temporary Files 143.702 MB 402.541 MB 1.572 GB
Action Queue Results 0 KB 402.541 MB 1.572 GB
Connection Events 17.225 GB 3.931 GB 23.586 GB
User Identity Events 0 KB 402.541 MB 1.572 GB
UI Caches 587 KB 1.179 GB 2.359 GB
Backups 0 KB 3.145 GB 7.862 GB
Updates 13 KB 4.717 GB 11.793 GB
Other Detection Engine 0 KB 2.359 GB 4.717 GB
Performance Statistics 72.442 MB 805.082 MB 9.435 GB
Other Events 669.819 MB 1.572 GB 3.145 GB
IP Reputation & URL Filtering 0 KB 1.966 GB 3.931 GB
Archives & Cores & File Logs 1.381 GB 3.145 GB 15.724 GB
RNA Events 0 KB 3.145 GB 12.579 GB
File Capture 12.089 MB 4.717 GB 14.152 GB
IPS Events 3.389 GB 7.076 GB 15.724 GB
```

Si la división de /Volume es llena

Viejos archivos de backup

- Si usted salva de gran capacidad de los viejos archivos de backup en el sistema, puede tomar el espacio excesivo en su disco.

Pasos para la resolución de problemas

- Borre los viejos archivos de backup usando la interfaz del Web User. Para quitar los archivos de backup, navegue al **sistema > a las herramientas > al respaldo/al Restore**.

  Consejo: En un sistema de FireSIGHT, usted puede configurar el almacenamiento remoto para salvar los archivos de backup grandes.

Una más viejos actualización de software y archivos de parche

- Si usted guarda siempre la actualización de software anterior, la actualización, y los archivos de parche (por ejemplo, los 5.0 o los 5.1), el sistema puede ejecutar hacia fuera el espacio en disco.

Pasos para la resolución de problemas

- Borre la más viejos actualización y archivos de parche que son no más necesarios. Para borrarlos, navegue por favor al **sistema > a las actualizaciones**.

Se salvan los archivos excesivos del evento

- El dispositivo administrado o el sensor pudo haber parado el enviar de los eventos al centro de administración de FireSIGHT.
- Un dispositivo puede generar más eventos que un centro de administración se diseña para recibir (por segundo).
- Pudo haber un problema de comunicación entre el dispositivo administrado y el centro de administración.

Pasos para la resolución de problemas

- Reaplique la directiva que se relaciona con el evento. Por ejemplo, si usted no está viendo los eventos de conexión, reaplique la directiva de Controil del acceso y vea si algunos nuevos eventos ahora están siendo recibidos por el centro de administración.
- Si un centro de administración de FireSIGHT no puede recibir los nuevos eventos IPS, marque por favor si hay algunos problemas de comunicación entre el dispositivo administrado y el centro de administración.

Archivos desconocidos excesivos

- El sistema de FireSIGHT salva los datos de la detección de la **`red desconocida`** (OS, host y información de servicios).

Pasos para la resolución de problemas

- Si el sistema no puede determinar el sistema operativo en un host en su red, usted puede utilizar Nmap para explorar activamente el host. Nmap utiliza la información que obtiene de la exploración para valorar los sistemas operativos posibles. Entonces utiliza el sistema operativo que tiene el grado más alto como la identificación del sistema operativo del host.
- Cree una regla de la correlación esa los activadores cuando el sistema detecta un host con un sistema operativo desconocido.
  La regla debe accionar cuando **ocurre un evento de la detección** y la **información OS para un host ha cambiado** y cumple las condiciones siguientes: **El nombre OS es desconocido**.

Base de datos grande para salvar los eventos

- Si usted aumenta el límite del evento de la base de datos más allá de la guía de consulta o de la mejor práctica, el centro de administración de FireSIGHT puede ejecutarse fuera del espacio en disco.

Pasos para la resolución de problemas

- Marque los valores del límite de la base de datos. Para mejorar la utilización y el funcionamiento del disco, usted debe adaptar los límites del evento al número de eventos que usted trabaja **regularmente** con. Para algunos tipos de evento, usted puede inhabilitar el almacenamiento.
- Para cambiar el límite de la base de datos, navegue por favor a la página de la política del sistema, el tecleo **edita** al lado del nombre de la política del sistema, y después hace clic la **base de datos** en la sección izquierda. Para acceder la página de la **política del sistema**, navegue por favor al **sistema > al Local > a la política del sistema**.

Reciba las alertas de la salud para encima la utilización del disco del 85%

Posibles Motivos

- La tarifa del evento puede ser muy alta. Por lo tanto el dispositivo es de generación y que salva de las porciones de eventos.
- Problemas de comunicación entre el dispositivo administrado y el centro de administración de FireSIGHT.

Pasos para la resolución de problemas

- El cambio del límite de umbral alerta hasta el 87% (cuidado) y el 92% (crítico) puede ser una solución simple para frecuentar las alertas de la salud.
- Lea los Release Note para ver si había un problema conocido con el sistema de la poda. Cuando una solución está disponible, ponga al día por favor la versión de software a la última versión para abordar este problema.

Los archivos de /var/log/messages contienen más viejas de 24 horas de los datos, o el más grandes que 25MB

Posibles Motivos

- La daemon de Logrotate puede no trabajar correctamente.

Pasos para la resolución de problemas

- Si usted encuentra este problema, ponga al día por favor la versión de software de sus sistemas de FireSIGHT a la última versión. Si usted está funcionando con la última versión, pero todavía está experimentando este problema, entre en contacto por favor el Centro de Asistencia Técnica de Cisco (TAC).

Si la división de la raíz (/) es llena

Los archivos de usuario se guardan en la división de la raíz (/)

Posibles Motivos

- La división de la raíz (`/`) es un tamaño fijo y no se piensa para el almacenamiento personal.
- `/var/tmp` drectory se utiliza manualmente para el almacenamiento temporario, en vez del directorio de `/var/common`.

Pasos para la resolución de problemas

- Marque para saber si hay archivos innecesarios en `/root`, `/home`, y la carpeta de `/tmp`. Puesto que estas carpetas no se crean para el almacenamiento personal, usted puede borrar cualquier archivo personal con el comando del `rm`.

Los procesos sin apoyo están escribiendo para arraigar (/) la división

Posibles Motivos

- Si usted instala el software de tercero que crea los archivos en la división de la raíz (`/`), usted puede experimentar la alerta de la salud para el alto uso del disco.

Pasos para la resolución de problemas

- Marque si algunos paquetes sin apoyo están instalados. Funcione con el siguiente comando de encontrar los paquetes instalados:

  ```
  admin@3DSystem:~$ rpm -qa --last
  ```
- Marque el pstree y remate para ver si los procesos sin apoyo se están ejecutando. Funcione con los siguientes comandos:

  ```
  admin@3DSystem:~$ pstree -ap admin@3DSystem:~$ top
  ```