Solución de problemas de uso excesivo del disco en dispositivos Sourcefire

Contenido

Introducción

Un FireSIGHT Management Center o un appliance FirePOWER pueden quedarse sin espacio en disco por varias razones. Cuando ocurre, el uso elevado del disco activa la alerta de estado o puede fallar un intento de actualización del software. En este artículo se describen las causas principales de la utilización excesiva del disco y algunos pasos de solución de problemas.

Pasos de verificación

Determine la partición que se utiliza con frecuencia. El siguiente comando muestra la utilización del disco:

En FireSIGHT Management Center,

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

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

```
> show disk
```

Ambos comandos muestran un resultado como el siguiente:

```
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 según los distintos modelos de dispositivos. Si se trata de un dispositivo virtual NGIPS, verifique que el tamaño de las particiones cumpla con los requisitos mínimos de espacio en disco.

Precaución: No se admite ninguna partición adicional que no se muestre arriba.

En los dispositivos de las series 7000 y 8000 y en los dispositivos virtuales NGIPS, puede ejecutar el siguiente comando para mostrar estadísticas detalladas del uso del disco:

```
> show disk-manager
```

Ejemplo de resultado:

```
> 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 partición /Volume está completa

Archivos de copia de seguridad antigua

- Si almacena un gran volumen de archivos de copia de seguridad antiguos en el sistema, puede ocupar demasiado espacio en el disco.

Pasos para la resolución de problemas

- Elimine los archivos de copia de seguridad antiguos mediante la interfaz de usuario web. Para quitar los archivos de copia de seguridad, navegue hasta **Sistema > Herramientas > Copia de seguridad/Restauración**.

  Consejo: En un sistema FireSIGHT, puede configurar el almacenamiento remoto para almacenar los archivos de copia de seguridad de gran tamaño.

Archivos de parches y actualización de software anteriores

- Si siempre mantiene los archivos de actualización, actualización y parche de software anteriores (como 5.0 o 5.1), el sistema puede quedarse sin espacio en disco.

Pasos para la resolución de problemas

- Elimine los archivos antiguos de actualización y revisión que ya no sean necesarios. Para eliminarlos, navegue hasta **Sistema > Actualizaciones**.

Se Almacenan Excesivos Archivos De Eventos

- Es posible que el dispositivo o sensor administrado haya dejado de enviar eventos al FireSIGHT Management Center.
- Un dispositivo puede estar generando más eventos de los que un Management Center está diseñado para recibir (por segundo).
- Puede haber un problema de comunicación entre el dispositivo administrado y el centro de administración.

Pasos para la resolución de problemas

- Vuelva a aplicar la política relacionada con el evento. Por ejemplo, si no ve eventos de conexión, vuelva a aplicar la política de control de acceso y vea si el centro de gestión está recibiendo eventos nuevos.
- Si un FireSIGHT Management Center no puede recibir nuevos eventos IPS, compruebe si hay algún problema de comunicación entre el dispositivo administrado y el centro de gestión.

Excesivos archivos desconocidos

- FireSIGHT System almacena los datos **desconocidos** de Network Discovery (SO, host e información de servicio).

Pasos para la resolución de problemas

- Si el sistema no puede determinar el sistema operativo en un host de la red, puede utilizar Nmap para escanear activamente el host. Nmap utiliza la información que obtiene de la exploración para evaluar los posibles sistemas operativos. A continuación, utiliza el sistema operativo que tiene la máxima calificación como identificación del sistema operativo host.
- Cree una regla de correlación que se active cuando el sistema detecte un host con un sistema operativo desconocido.
  La regla debe activarse cuando **se produce un evento de detección** y **la información del sistema operativo para un host ha cambiado** y cumple las siguientes condiciones: **Nombre del sistema operativo desconocido**.

Base de datos grande para almacenar eventos

- Si aumenta el límite de eventos de la base de datos más allá de las pautas o prácticas recomendadas, FireSIGHT Management Center puede quedarse sin espacio en disco.

Pasos para la resolución de problemas

- Verifique los valores del límite de base de datos. Para mejorar la utilización y el rendimiento del disco, debe ajustar los límites de eventos al número de eventos con los que trabaja **regularmente**. Para algunos tipos de eventos, puede deshabilitar el almacenamiento.

- Para cambiar el límite de la base de datos, navegue a la página Política del sistema, haga clic en **Editar** junto al nombre de la política del sistema y luego haga clic en **Base de datos** en la sección izquierda. Para acceder a la página **Política del sistema**, navegue hasta **Sistema > Local > Política del sistema**.

Recibir Alertas De Estado Para Una Utilización De Más Del 85% Del Disco

Posibles Motivos

- La tasa de eventos puede ser muy alta. Por lo tanto, el dispositivo está generando y almacenando muchos eventos.
- Problemas de comunicación entre el dispositivo administrado y FireSIGHT Management Center.

Pasos para la resolución de problemas

- Cambiar el nivel del umbral de alerta al 87% (advertencia) y al 92% (crítico) puede ser una solución sencilla para las alertas de estado frecuentes.
- Lea las notas de la versión para ver si se conoce algún problema con el sistema de recorte. Cuando haya una solución disponible, actualice la versión de software a la última versión para solucionar este problema.

Los archivos /var/log/messages contienen datos con una antigüedad superior a 24 horas o superior a 25 MB

Posibles Motivos

- Es posible que el demonio Logrotate no funcione correctamente.

Pasos para la resolución de problemas

- Si detecta este problema, actualice la versión de software de FireSIGHT Systems a la última versión. Si está ejecutando la versión más reciente, pero aún tiene este problema, póngase en contacto con el centro de asistencia técnica Cisco Technical Assistance Center (TAC).

Si la partición raíz (/) está completa

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

Posibles Motivos

- La partición raíz (/) es de tamaño fijo y no está destinada al almacenamiento personal.
- El directorio /var/tmp se utiliza manualmente para el almacenamiento temporal, en lugar del directorio /var/common.

Pasos para la resolución de problemas

- Compruebe si hay archivos innecesarios en la carpeta /root, /home y /tmp. Dado que estas carpetas no se crean para almacenamiento personal, puede eliminar cualquier archivo

personal con el comando rm.

Los procesos no admitidos están escribiendo en la partición raíz (/)

Posibles Motivos

- Si instala un software de terceros que crea archivos en la partición raíz (/), puede experimentar una alerta de estado por uso elevado del disco.

Pasos para la resolución de problemas

- Compruebe si hay algún paquete no compatible instalado. Ejecute el siguiente comando para encontrar los paquetes instalados:

```
admin@3DSystem:~$ rpm -qa --last
```

- Marque pstree y top para ver si se están ejecutando procesos no compatibles. Ejecute los siguientes comandos:

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

admin@3DSystem:~$ top
```