Solucione problemas de utilização excessiva de disco em dispositivos Sourcefire

Contents

Introduction

Um FireSIGHT Management Center ou um dispositivo FirePOWER podem ficar sem espaço em disco por vários motivos. Quando ocorre, a alta utilização do disco aciona um alerta de integridade ou pode falhar uma tentativa de atualização do software. Este artigo descreve as causas raiz do excesso de utilização do disco e algumas etapas de solução de problemas.

Etapas de verificação

Determine a partição que é altamente usada. O comando a seguir mostra a utilização do disco:

em um FireSIGHT Management Center,

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

Nos dispositivos 7000 e 8000 Series e nos dispositivos virtuais NGIPS,

```
> show disk
```

Ambos os comandos mostram uma saída como abaixo:

```
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
```

Note: O tamanho e a utilização do disco podem variar em vários modelos de dispositivos. Se for um dispositivo virtual NGIPS, verifique se o tamanho das partições atende aos requisitos mínimos de espaço em disco.

Caution: Não há suporte para qualquer partição adicional que não seja mostrada acima.

Nos dispositivos 7000 e 8000 Series e nos dispositivos virtuais NGIPS, você pode executar o seguinte comando para exibir estatísticas detalhadas de uso do disco:

```
> show disk-manager
```

Um exemplo de saída:

```
> 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
```

Se a partição /Volume estiver cheia

Arquivos de backup antigos

- Se você armazenar um grande volume de arquivos de backup antigos no sistema, ele poderá ocupar espaço excessivo no disco.

Passos de Troubleshooting

- Exclua os arquivos de backup antigos usando a interface de usuário da Web. Para remover arquivos de backup, navegue para **System > Tools > Backup/Restore** (**Sistema > Ferramentas > Backup/Restauração**).

  Tip: Em um sistema FireSIGHT, você pode configurar o armazenamento remoto para armazenar os grandes arquivos de backup.

Arquivos mais antigos de atualização e patch de software

- Se você sempre mantiver os arquivos anteriores de atualização, upgrade e patch do software (como 5.0 ou 5.1), o sistema poderá ficar sem espaço em disco.

Passos de Troubleshooting

- Exclua os arquivos de atualização e patch mais antigos que não são mais necessários. Para excluí-los, navegue para **System > Updates**.

Arquivos de eventos excessivos são armazenados

- O sensor ou dispositivo gerenciado pode ter parado de enviar eventos para o FireSIGHT Management Center.
- Um dispositivo pode estar gerando mais eventos do que um Centro de Gerenciamento é projetado para receber (por segundo).
- Pode haver um problema de comunicação entre o dispositivo gerenciado e o centro de gerenciamento.

Passos de Troubleshooting

- Reaplique a política relacionada ao evento. Por exemplo, se você não estiver vendo eventos de conexão, reaplique a política de Controle de Acesso e veja se algum novo evento está sendo recebido pelo Centro de Gerenciamento.
- Se um FireSIGHT Management Center não puder receber novos eventos de IPS, verifique se há algum problema de comunicação entre o dispositivo gerenciado e o centro de gerenciamento.

Excesso de arquivos desconhecidos

- O sistema FireSIGHT armazena os dados de descoberta de rede **desconhecidos** (SO, host e informações de serviço).

Passos de Troubleshooting

- Se o sistema não puder determinar o sistema operacional em um host na rede, você poderá usar o Nmap para verificar ativamente o host. O Nmap usa as informações obtidas da verificação para classificar os possíveis sistemas operacionais. Em seguida, ele usa o sistema operacional que tem a classificação mais alta como a identificação do sistema operacional do host.
- Crie uma regra de correlação que dispara quando o sistema detecta um host com um sistema operacional desconhecido.
  A regra deve disparar quando **um evento de descoberta ocorre** e **as informações do SO de um host foram alteradas** e atendem às seguintes condições: **O nome do SO é desconhecido**.

Grande banco de dados para armazenar eventos

- Se você aumentar o limite de eventos do banco de dados além da diretriz ou das melhores práticas, o FireSIGHT Management Center pode ficar sem espaço em disco.

Passos de Troubleshooting

- Verifique os valores do limite do banco de dados. Para melhorar a utilização e o desempenho do disco, você deve adaptar os limites de eventos ao número de eventos com os quais você

trabalha regularmente. Para alguns tipos de eventos, você pode desativar o armazenamento.
- Para alterar o limite do banco de dados, navegue até a página Diretiva do sistema, clique em **Editar** ao lado do nome da diretiva do sistema e clique em **Banco de dados** na seção esquerda. Para acessar a página **Política do sistema**, navegue para **Sistema > Local > Política do sistema**.

Receber Alertas De Integridade Para Mais De 85% De Utilização De Disco

Motivos possíveis

- A taxa de eventos pode ser muito alta. Portanto, o dispositivo está gerando e armazenando muitos eventos.
- Problemas de comunicação entre o dispositivo gerenciado e o FireSIGHT Management Center.

Passos de Troubleshooting

- Alterar o nível do limite de alerta para 87% (Aviso) e 92% (Crítico) pode ser uma solução simples para alertas de integridade frequentes.
- Leia as Notas de versão para ver se há um problema conhecido com o sistema de poda. Quando uma solução estiver disponível, atualize a versão do software para a versão mais recente para resolver esse problema.

Os arquivos /var/log/messages contêm dados com mais de 24 horas ou mais de 25 MB

Motivos possíveis

- Logrotate daemon pode não estar funcionando corretamente.

Passos de Troubleshooting

- Se você encontrar esse problema, atualize a versão do software dos seus sistemas FireSIGHT para a versão mais recente. Se você estiver executando a versão mais recente, mas ainda estiver com esse problema, entre em contato com o Cisco Technical Assistance Center (TAC).

Se a partição raiz (/) estiver cheia

Os arquivos de usuário são salvos na partição raiz (/)

Motivos possíveis

- A partição raiz (/) é de tamanho fixo e não se destina ao armazenamento pessoal.
- O diretório /var/tmp é usado manualmente para armazenamento temporário, em vez do diretório /var/common.

Passos de Troubleshooting

- Verifique se há arquivos desnecessários na pasta /root, /home e /tmp. Como essas pastas não são criadas para armazenamento pessoal, você pode excluir qualquer arquivo pessoal com o comando rm.

Processos não suportados estão gravando na partição raiz (/)

Motivos possíveis

- Se instalar software de terceiros que cria arquivos na partição raiz (/), você poderá receber um alerta de integridade para o alto uso do disco.

Passos de Troubleshooting

- Verifique se há algum pacote não suportado instalado. Execute o seguinte comando para localizar os pacotes instalados:

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

- Verifique a árvore e a parte superior para ver se os processos não suportados estão em execução. Execute os seguintes comandos:

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

```
admin@3DSystem:~$ top
```