Índice

Introdução

Um centro de gerenciamento de FireSIGHT ou um dispositivo da potência de fogo podem ser executado fora do espaço de disco por razões diversas. Quando acontece, a utilização alta do disco provoca o alerta da saúde ou pode falhar uma tentativa da atualização de software. Este artigo descreve as causas de raiz da utilização excessiva do disco e dos alguns passos de Troubleshooting.

Etapas de verificação

Determine a separação que é usada altamente. O comando seguinte mostra a utilização do disco:

Em um centro de gerenciamento de FireSIGHT,

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

Em dispositivos do 7000 e 8000 Series e em dispositivos virtuais NGIPS,

```
> show disk
```

Os comandos both 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
```

> Nota: O tamanho e a utilização do disco podem variar em vários modelos do dispositivo. Se este é um dispositivo virtual NGIPS, verifique que o tamanho das separações segue com os requisitos de espaço em disco mínimos.

Cuidado: Toda a separação adicional que não for mostrada acima é unsupported.

Em dispositivos do 7000 e 8000 Series e em dispositivos virtuais NGIPS, você pode executar o comando seguinte indicar estatísticas detalhadas do uso de disco:

```
> show disk-manager
```

Umas saídas de exemplo:

```
> 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 separação de /Volume está completa

Arquivos de backup velhos

- Se você armazena de grande volume de arquivos de backup velhos no sistema, pode tomar o espaço excessivo em seu disco.

Passos de Troubleshooting

- Suprima dos arquivos de backup velhos usando a relação de usuário de web. A fim remover os arquivos de backup, navegue ao **sistema > às ferramentas > ao backup/restauração**.

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

Atualização de software e arquivos de correção mais velhos

- Se você mantém sempre a atualização de software anterior, a elevação, e os arquivos de correção (como, os 5.0 ou os 5.1), o sistema pode executar para fora o espaço de disco.

Passos de Troubleshooting

- Suprima da atualização e dos arquivos de correção mais velhos que são já não necessários. A fim suprimir d, navegue por favor ao **sistema > às atualizações**.

Os arquivos excessivos do evento são armazenados

- O dispositivo gerenciado ou o sensor puderam ter parado de enviar eventos ao centro de gerenciamento de FireSIGHT.
- Um dispositivo pode gerar mais eventos do que um centro de gerenciamento é projetado receber (por segundo).
- Pôde haver um problema de comunicação entre o dispositivo gerenciado e o centro de gerenciamento.

Passos de Troubleshooting

- Reaplique a política que é relacionado ao evento. Por exemplo, se você não está vendo eventos de conexão, reaplique a política de Controil do acesso e veja se algum evento novo está sendo recebido agora pelo centro de gerenciamento.
- Se um centro de gerenciamento de FireSIGHT é incapaz de receber eventos novos IPS, verifique por favor se há algum problema de comunicação entre o dispositivo gerenciado e o centro de gerenciamento.

Arquivos desconhecidos excessivos

- O sistema de FireSIGHT armazena os dados da descoberta da **`rede desconhecida`** (OS, host e informação do serviço).

Passos de Troubleshooting

- Se o sistema não pode determinar o sistema operacional em um host em sua rede, você pode usar Nmap para fazer a varredura ativamente do host. Nmap usa a informação que obtém da varredura para avaliar os sistemas operacionais possíveis. Usa então o sistema operacional que tem a avaliação a mais alta como a identificação do sistema operacional do host.
- Crie uma regra da correlação essa disparadores quando o sistema detecta um host com um sistema operacional desconhecido.
  A regra deve provocar quando um **evento da descoberta ocorre** e a **informação do OS para um host mudou** e está conformes as seguintes circunstâncias: **O nome do OS é desconhecido**.

Grande base de dados para armazenar eventos

- Se você aumenta o limite do evento do base de dados além da diretriz ou do melhor prática, o centro de gerenciamento de FireSIGHT pode ser executado fora do espaço de disco.

Passos de Troubleshooting

- Verifique os valores do limite do base de dados. Para melhorar a utilização e o desempenho do disco, você deve costurar limites do evento ao número de eventos que você trabalha **regularmente** com. Para alguns tipos de evento, você pode desabilitar o armazenamento.
- A fim mudar o limite do base de dados, navegue por favor à página da política de sistema, o clique **edita** ao lado do nome da política de sistema, e clica então o **base de dados na** seção esquerda. Para alcançar a página da **política de sistema**, navegue por favor ao **sistema > ao Local > à política de sistema**.

Receba alertas da saúde para sobre a utilização do disco de 85%

Razões possíveis

- A taxa do evento pode ser muito alta. Consequentemente o dispositivo é de geração e de armazenagem lotes dos eventos.
- Problemas de comunicação entre o dispositivo gerenciado e o centro de gerenciamento de FireSIGHT.

Passos de Troubleshooting

- Mudar o nível de ponto inicial alerta a 87% (advertência) e a 92% (crítico) pode ser uma solução simples para frequentar alertas da saúde.
- Leia os Release Note para ver se havia um problema conhecido com o sistema de poda. Quando uma solução está disponível, atualize por favor a versão de software à liberação a mais atrasada para endereçar esta edição.

Os arquivos de /var/log/messages contêm horas mais velhas dos dados umas de 24, ou o maiores do que 25MB

Razões possíveis

- O demônio de Logrotate não pode trabalhar corretamente.

Passos de Troubleshooting

- Se você encontra esta edição, atualize por favor a versão de software de seus sistemas de FireSIGHT à liberação a mais atrasada. Se você está executando a versão a mais atrasada, mas ainda está experimentando esta edição, contacte por favor o centro de assistência técnica da Cisco (TAC).

Se a separação da raiz (/) está completa

Os arquivos de usuário salvar na separação da raiz (/)

Razões possíveis

- A separação da raiz (`/`) é um tamanho fixo e não é pretendida para o armazenamento pessoal.
- `/var/tmp` drectory é usado manualmente para o armazenamento temporário, em vez do diretório de `/var/common`.

Passos de Troubleshooting

- Verifique para ver se há arquivos desnecessários em `/root`, em `/home`, e no dobrador de `/tmp`. Desde que estes dobradores não são criados para o armazenamento pessoal, você pode suprimir de todo o arquivo pessoal com comando do `rm`.

Os processos Unsupported estão escrevendo para enraizar (/) a separação

Razões possíveis

- Se você instala o software de terceiros que cria arquivos na separação da raiz (`/`), você pode

experimentar o alerta da saúde para o uso de disco alto.

Passos de Troubleshooting

- Verifique se algum pacote unsupported é instalado. Execute o comando seguinte encontrar os pacotes instalados:

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

- Verifique o pstree e cubra-o para ver se os processos unsupported estão sendo executado. Execute os comandos seguintes:

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