

Gerenciar o uso do disco/sistema de arquivos local na análise de rede segura

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Coletar Dados](#)

[Linha de comando](#)

[IU da Web](#)

[Limpar Espaço em Disco](#)

[Registros de sistema](#)

[Aparar o Banco de Dados Distribuído \(DDS\) - Estatísticas de Fluxo](#)

[Aparar o Banco de Dados Distribuído \(DDS\) - Detalhes da Interface de Fluxo](#)

[Aumentar Espaço Em Disco \(Somente Dispositivos Virtuais\)](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas gerais para diminuir o uso elevado do disco em dispositivos Secure Network Analytics Manager e Flow Collector.

Pré-requisitos

Requisitos

Este documento se aplica a implantações Secure Network Analytic sem o Data Store.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Network Analytics Manager - v7.1+
- Coletor de fluxo de análise de rede segura - v7.1+
- Sensor de fluxo de análise de rede segura - v7.1+
- Secure Network Analytics UDP Diretor - v7.1+

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Há duas partições para monitorar o uso do disco, as partições raiz (/) e /lancope/var.

A partição raiz (/) é o local de armazenamento para a imagem do kernel e alguns logs do sistema; essa é geralmente uma partição menor de 20G ou menos. O /lancope/var é um grupo de volumes e é o local de armazenamento para a maioria dos dados do sistema, por isso consome a maior parte do espaço em disco para o dispositivo.

Coletar Dados

Há dois lugares onde você pode obter informações de uso do disco: a interface da Web do administrador e a interface de linha de comando (CLI).

Linha de comando

Na linha de comando, execute o comando `df -ah /lancope/var` e observe os espaços entre (/) e /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:/#
```

A saída mostra que a partição raiz (/) é 20G e 8,3G está em uso, que é 46%. A saída também mostra que a partição /lancope/var é 108G, e 23G está em uso, que é 22%.

IU da Web

Faça login na interface de usuário Admin do dispositivo com base no modelo em questão e role até o final da página.

Lista de endereços da Web da interface do usuário do administrador:

- Secure Network Analytics Manager - <https://<SMC-IP-OR-FQDN>/smc/index.html> (Você deve fazer login no SMC antes de acessar este URL)
- Coletor de fluxo de análise de rede segura - <https://<FC-IP-OR-FQDN>/swa/index.html>

- Sensor de fluxo de análise de rede segura - <https://<FS-IP-OR-FQDN>/fs/index.html>
- Diretor UDP do Secure Network Analytics (Flow Replicator) - <https://<UDPD-IP-OR-FQDN>/fr/index.html>

Disk Usage

Name	Used	Size (byte)	Used (byte)	Available (byte)
/	14%	19.56G	2.9G	15.66G
/lancope/var	25%	106.23G	27.23G	76.82G

Se a partição tiver um uso alto maior ou igual a 75%, a partição será realçada.

Limpar Espaço em Disco

Se não tiver certeza de quais arquivos podem ser excluídos com segurança, abra um caso no TAC ou entre em contato com o suporte da Cisco pela página Cisco Worldwide Support Contact na seção Informações Relacionadas no final deste documento.

Registros de sistema

Um dos métodos mais rápidos para recuperar espaço em disco dimensionável é limpar registros de diário com o comando `journalctl --vacuum-time 1d` comando. Observe o hífen duplo — antes da palavra "vácuo".

```
<#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:/#
```

Cerca de 4G de espaço em disco foi recuperado dessas etapas e resultou em uma diminuição do uso do disco de 22% para 18% na partição /lancope/var.

Os arquivos nos diretórios listados são geralmente seguros para serem excluídos:

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

Recomenda-se iniciar no diretório raiz (/) ou /lancope/var, qualquer partição identificada na interface do usuário da Web que tenha uso alto do disco. Altere o diretório atual com o comando `cd /` comando.

Execute o comando `du -xah --max-depth=1 | sort -hr` para determinar os maiores consumidores de espaço em disco do diretório atual. Observe o hífen duplo — antes da profundidade máxima.

A saída mostra que a partição raiz (/) tem 8,3G de espaço em disco em uso, com 5,5G de espaço em disco usado no diretório /lancope, seguido pelo diretório /usr com 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:/#
```

Altere o diretório para /lancope com o comando `cd lancope/` e emita novamente o comando `du` com o comando `!du` comando. Isso agora exhibe que, do 5.5G em uso no diretório /lancope/, 5.1G está no diretório admin. Alterar os diretórios atuais para o diretório em questão com o comando `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#
```

Depois de identificar os arquivos que podem ser excluídos, você pode fazer isso com o comando

```
rm -i
```

comando. Se não tiver certeza de quais arquivos podem ser excluídos com segurança, abra um caso no TAC ou entre em contato com o suporte da Cisco pela página Cisco Worldwide Support Contact na seção Informações Relacionadas no final deste documento.

```
<#root>
```

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

```
rm -i file
```

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

```
yes
```

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

Repita essas etapas conforme necessário.

Aparar o Banco de Dados Distribuído (DDS) - Estatísticas de Fluxo

Por padrão, no ambiente DDS, os dispositivos FlowCollector e SMC tentam armazenar o máximo de dados de fluxo possível rotacionados diariamente. Quando os limites de uso do disco forem atingidos, o sistema começará a excluir os dados mais antigos primeiro para criar espaço para que novos dados sejam salvos.

Para ver as estatísticas do banco de dados do Flow Collector, faça login na interface do usuário do FlowCollector Admin e selecione [Support > Database Storage Statistics](#) .

The screenshot shows the Cisco FlowCollector for NetFlow VE interface. On the left is a navigation menu with options like Home, Configuration, Manage Users, Support, and Audit Log. The main content area is divided into two sections: 'Database Storage Statistics' and 'Flow Data Summary'.

Database Storage Statistics - Capacity

	Average	Worst Case
Capacity in Days	930	121
Remaining Days	644	83
Bytes Per Day	348.08M	1.57G

Flow Data Summary

Data	Days	Containers	Rows			Bytes		
			Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	286	295	5.46G	19.1M	57.08M	58.53G	204.65M	719.87M
Flow Interface Details	8	27	45.71M	5.71M	6.03M	1.1G	137.8M	145.61M
Total	286	322	5.51G	24.81M	63.11M	59.63G	342.45M	865.49M

Estadísticas de Armazenamento do Banco de Dados

- A imagem mostra que a média dos Detalhes do fluxo (dados do netflow) ingeridos é de 204,65 MB por dia e este Flow Collector tem cerca de 58,5 GB de dados armazenados.
- A imagem mostra que a média dos Detalhes da interface de fluxo (estatísticas específicas da interface) é de cerca de 137 MB por dia e que esse coletor de fluxo tem cerca de 1,1 GB de dados armazenados.
- A imagem mostra que a média do total de dados de fluxo é de cerca de 342,53 GB por dia e esse coletor de fluxo tem cerca de 60 GB do total de dados armazenados.
- Se você quiser reduzir o banco de dados para ter cerca de 20G do total de dados armazenados, divida isso pela média diária de .35G, que é igual a 57.

Para reduzir o banco de dados para ter um tamanho total de aproximadamente 20 Gb, altere o `summary_retention_days` valor 57. Em seguida, navegue até `Support > Advanced Settings`. Localizar `summary_retention_days` e altere isso para o valor desejado.

The screenshot shows a configuration field for `summary_retention_days`. The field name is on the left, and the value '57' is entered in the input box on the right. There is a small square icon to the right of the input box.

`summary_retention_days`

Em seguida, adicione uma nova opção na parte inferior da lista. O `Add New Option` o valor é `strict_retention_days` e o `Option Value` é definido como 1, conforme mostrado na imagem. Clique em **Add**. Este `strict_retention_days` manda que o mecanismo mantenha apenas o número de dias declarado em `Summary_retention_days`.

Add New Option:	<input type="text" value="strict_retention_days"/>	Option value:	<input type="text" value="1"/>	<input type="button" value="Add"/>	<input type="button" value="Reset"/>
<input type="button" value="Reset"/>	<input type="button" value="Apply"/>	You need to 'Apply' your change(s).			

strict_retention_days

Depois que eu tiver alterado o `summary_retention_days` para 4 e eu adicionei o novo valor de opção, pressione `Apply` na parte inferior da página.

Se essas etapas para uma atualização, exclua o `strict_retention_days` quando a atualização estiver concluída, para que os dados sejam retidos o máximo possível.

Aparar o Banco de Dados Distribuído (DDS) - Detalhes da Interface de Fluxo

1. Registro inpara seu Stealthwatch Desktop Cliente como o admin usuário.
2. Localize o FlowCollector na Árvore da Empresa. Clique no sinal de adição (+) assine para expandir o contêiner.
3. Clique com o botão direito do mouse no FlowCollector desejado. Selecionar `Configuration > Properties`.
4. IN o FluxoColetor Propriedades diálogo caixa, clicar `Advanced`.
5. Selecionar o `Store flow interface data` campo. Configurado o limite para Para cima para 15 dias or 30 dias.
6. Clique em `OK` .

Aumentar o espaço em disco (somente aplicativos virtuais)

Desligue a máquina virtual e aumente o tamanho do disco alocado para a VM do hipervisor. O espaço em disco adicional é alocado para a partição `/lancope/var/`.

Etapas adicionais podem ser necessárias para que o Stealthwatch consuma esse espaço em disco não alocado após uma reinicialização; revise o `Data Storage of the Installation Guide for your virtual machine edition` para obter o tamanho de disco necessário.

O tamanho da partição raiz (`/`) é estático e não pode ser ajustado. É necessária uma nova instalação em uma versão que tenha uma partição raiz maior criada durante a instalação.

Informações Relacionadas

- [Guias de instalação](#)
- [Suporte técnico e documentação do Secure Network Analytics - Cisco Systems](#)
- [Contatos mundiais de suporte da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.