

在安全网络分析中管理本地文件系统/磁盘使用情况

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[收集数据](#)

[命令行](#)

[Web UI](#)

[清除磁盘空间](#)

[系统日志](#)

[调整分布式数据库\(DDS\) — 流统计信息](#)

[调整分布式数据库\(DDS\) — 流接口详细信息](#)

[增加磁盘空间 \(仅虚拟设备\)](#)

[相关信息](#)

简介

本文档介绍减少安全网络分析管理器和流量收集器设备上的高磁盘使用率的一般步骤。

先决条件

要求

本文档适用于没有Data Store的安全网络分析部署。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全网络分析管理器 — v7.1+
- 安全网络分析流量收集器 — v7.1+
- 安全网络分析流量传感器 — v7.1+
- 安全网络分析UDP导向器 — v7.1+

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

有两个分区要监控磁盘使用情况，即根(/)和/lancope/var分区。

根(/)分区是内核映像和某些系统日志的存储位置，这通常是20G或更小的部分。 /lancope/var是一个卷组，它是大多数系统数据的存储位置，因此它会占用设备的大部分磁盘空间。

收集数据

有两个位置可以获取磁盘使用情况信息：管理Web UI和命令行界面(CLI)。

命令行

从命令行运行 `df -ah / /lancope/var` 命令，并记下(/)和/lancope/var之间的空格。

```
<#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:/#
```

输出显示，根(/)部分为20G，正在使用8.3G，即46%。输出还显示/lancope/var分区为108G，正在使用23G(22%)。

Web UI

根据相关型号登录设备管理UI，然后滚动到页面底部。

管理员UI网址列表：

- 安全网络分析管理器 — <https://<SMC-IP-OR-FQDN>/smc/index.html> (您必须登录SMC，然后才能访问此URL)
- 安全网络分析流量收集器 — <https://<FC-IP-OR-FQDN>/swa/index.html>
- 安全网络分析流量传感器 — <https://<FS-IP-OR-FQDN>/fs/index.html>
- 安全网络分析UDP Director (流量复制器) — <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

如果分区的使用率高于或等于75%，则会突出显示该分区。

清除磁盘空间

如果您不确定哪些文件可以安全删除，请打开TAC案例或通过本文档末尾相关信息部分中的思科全球支持联系人页面联系Cisco支持。

系统日志

恢复大磁盘空间的最快方法之一是使用 `journalctl --vacuum-time 1d` 命令。注意双连字符 — 在“vacuum”一词之前。

```
<#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:/#
```

通过上述步骤回收了约4G磁盘空间，使/lancope/var分区的磁盘使用率从22%降至18%。

列出的目录中的文件通常可以安全删除：

```
/lancope/var/tcpdump
```

```
/lancope/var/tomcat/logs
```

```
/lancope/var/tmp
```

```
/lancope/var/admin/tmp/
```

建议从根(/)或/lancope/var目录 (在Web ui中标识的磁盘使用率较高的分区) 开始。使用 `cd /` 命令。

运行 `du -xah --max-depth=1 | sort -hr` 命令来确定当前目录磁盘空间的最大使用者。请注意双连字符 — 在 `max-depth` 之前。

输出显示，根(/)分区正在使用8.3G磁盘空间，/lancope目录中使用了5.5G磁盘空间，其次是/usr目录，使用量为1.5G。

```
<#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:/#
```

将目录更改为/lancope，并使用 `cd lancope/` 命令，然后使用 `!du` 命令。现在显示/lancope/目录中正在使用的5.5G中的版本，5.1G在admin目录中。将当前目录更改为有问题的目录 `cd` 命令。

```
<#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#
```

确定可删除的文件后，可以使用 `rm -i`

命令。如果您不确定哪些文件可以安全删除，请打开TAC案例或通过本文档末尾相关信息部分中的思科全球支持联系人页面联系Cisco支持。

```
<#root>
```

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

```
rm -i file
```

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

```
yes
```

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

根据需要重复这些步骤。

调整分布式数据库(DDS) — 流统计信息

默认情况下，在DDS环境中，FlowCollector和SMC设备会尝试存储尽可能多的每日轮换的流数据。当达到磁盘使用率限制时，系统首先开始删除最旧的数据，为要保存的新数据创造空间。

要查看流量收集器数据库统计信息，请登录到FlowCollector Admin UI，然后选择 [Support > Database Storage Statistics](#) .

The screenshot displays the '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 titled 'Database Storage Statistics' and includes a 'Capacity' table and a 'Flow Data Summary' table.

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

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

数据库存储统计信息

- 该图显示捕获的流详细信息（netflow数据）平均每天约204.65MB，此流量收集器存储的数据约为58.5GB。
- 该图显示捕获的流接口详细信息（接口特定统计信息）平均每天约137MB，并且此流量收集器存储了约1.1GB的数据。
- 该图显示，流量数据总量平均为每天342.53 GB，此流量收集器存储的数据总量约为60 GB。
- 如果要数据库缩小到存储大约20G的总数据，将其除以等于57的日均值。35G。

要将数据库缩小为总大小约20Gb，请更改 `summary_retention_days` 值为57。接下来，导航至 [Support > Advanced Settings](#)。查找 `summary_retention_days` 并将其更改为所需的值。

<code>summary_retention_days</code>	<input type="text" value="57"/>	<input type="checkbox"/>
-------------------------------------	---------------------------------	--------------------------

`summary_retention_days`

接下来，在列表底部添加一个新选项。此 `Add New Option` 值是 `strict_retention_days` 和 `Option Value` 如图所示，值设置为1。单击 `Add`。此 `strict_retention_days` 通知引擎仅保留在中声明的天数 `summary_retention_days`。

<code>Add New Option:</code>	<input type="text" value="strict_retention_days"/>	<code>Option value:</code>	<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`

一旦我更改了 `summary_retention_days` 至4，并且我已经添加了新选项值，请按 `Apply` 在页面底部。

如果升级的步骤如下，请删除 `strict_retention_days` 值，以便在升级完成后返回以尽可能长时间地保留数据。

调整分布式数据库(DDS) — 流接口详细信息

1. 日志 在到 您的 Stealthwatch 桌面 客户端 作为 此 admin 用户。
2. 在企业树中找到FlowCollector。单击加号(+)签名以展开容器。
3. 右键单击所需的FlowCollector。选择 `Configuration > Properties`。
4. 在此 流收集器 属性 对话框 包装盒, 点击 `Advanced`。
5. 选择 此 `Store flow interface data` 字段。设置 此 限制 到 Up 到 15 天 或 30 天。
6. 点击 `OK`。

增加磁盘空间(仅虚拟设备)

关闭虚拟机电源，并增大从虚拟机监控程序分配给VM的磁盘大小。额外的磁盘空间分配给 `/lancope/var/` 分区。

要使Stealthwatch在重新启动后占用此未分配的磁盘空间，可能需要执行其他步骤，请查看适用于您的虚拟机版本的《安装数据存储指南》以了解所需的磁盘大小。

根(/)分区大小是静态的，无法调整。对于安装期间创建的根分区较大的版本，需要全新安装。

相关信息

- [安装指南](#)
- [安全网络分析技术支持和文档 — Cisco Systems](#)
- [思科全球支持联系方式](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。