

# 在Secure Network Analytics中管理本地檔案系統/磁碟使用情況

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[收集資料](#)

[命令列](#)

[Web UI](#)

[清除磁碟空間](#)

[系統記錄](#)

[裁切分散式資料庫\(DDS\) — 流量統計資訊](#)

[裁切分散式資料庫\(DDS\) — 流介面詳細資訊](#)

[增加磁碟空間 \( 僅限虛擬裝置 \)](#)

[相關資訊](#)

---

## 簡介

本文檔介紹減少安全網路分析管理器和流量收集器裝置上的高磁碟使用率的一般步驟。

## 必要條件

### 需求

本文檔適用於沒有Data Store的安全網路分析部署。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全網路分析管理員 — v7.1+
- 安全網路分析流量收集器 — v7.1+
- 安全網路分析流量感應器 — v7.1+
- 安全網路分析UDP導向器 — v7.1+

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

有兩個分割槽要監視磁碟使用情況，即根(/)和/lancope/var分割槽。

根(/)分割槽是核心映像和某些系統日誌的儲存位置，這通常是20G或更小的較小部分。

/lancope/var是一個卷組，它是大多數系統資料的儲存位置，因此它消耗了裝置的大部分磁碟空間。

## 收集資料

有兩個位置可以獲取磁碟使用情況資訊：管理Web UI和命令列介面(CLI)。

### 命令列

從命令列運行 `df -ah / /lancope/var` 命令並記下(/)和/lancope/var之間的空格。

```
<#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:/#
```

輸出顯示，根(/)部分為20G，正在使用的8.3G為46%。輸出還顯示/lancope/var分割槽為108G，正在使用的23G分割槽為22%。

## Web UI

根據相關型號登入裝置管理使用者介面，然後滾動到頁面底部。

管理員UI Web地址清單：

- 安全網路分析管理器 — <https://<SMC-IP-OR-FQDN>/smc/index.html> ( 必須先登入SMC，然後才能訪問此URL )
- 安全網路分析流量收集器 — <https://<FC-IP-OR-FQDN>/swa/index.html>
- 安全網路分析流量感測器 — <https://<FS-IP-OR-FQDN>/fs/index.html>
- 安全網路分析UDP導向器 ( 流量複製器 ) — <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

如果分割槽的高使用率大於或等於75%，則突出顯示該分割槽。

## 清除磁碟空間

如果您不確定哪些檔案可以安全刪除，請開啟一個TAC案例，或者通過本文檔末尾「相關資訊」部分中的「思科全球支援聯絡人」頁面聯絡Cisco支援。

## 系統記錄

恢復大磁碟空間的最快方法之一是使用 `journalctl --vacuum-time 1d` 指令。注意兩個連字元 — 在「vacuum」字之前。

```
<#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:/#
```

通過這些步驟回收了大約4G的磁碟空間，導致/lancope/var分割槽上的磁碟使用率從22%降低到18%。

列出的目錄中的檔案通常可以安全刪除：

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

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

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

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

建議從根(/)或/lancope/var目錄 ( 在Web ui中標識的磁碟使用率較高的分割槽 ) 開始。更改當前目錄 `cd /` 指令。

運行 `du -xah --max-depth=1 | sort -hr` 命令來確定當前目錄磁碟空間的最大使用者。請注意雙連字元 — 在 `max-depth` 之前。

輸出顯示，根(/)分割槽正在使用8.3G磁碟空間，其中/lancope目錄使用了5.5G磁碟空間，其次是 /usr目錄，使用了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:/#
```

使用CLI將目錄更改為/lancope `cd lancope/` 命令，然後使用 `!du` 指令。這現在顯示/lancope/目錄中正在使用的5.5G中，5.1G位於admin目錄中。將當前目錄更改為有問題的目錄 `cd` 指令。

```
<#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#
```

識別可刪除的檔案後，您可以使用 `rm -i`

指令。如果您不確定哪些檔案可以安全刪除，請開啟一個TAC案例，或者通過本文檔末尾「相關資訊」部分中的「思科全球支援聯絡人」頁面聯絡Cisco支援。

```
<#root>
```

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

```
rm -i file
```

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

```
yes
```

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

根據需要重複這些步驟。

## 裁切分散式資料庫(DDS) — 流量統計資訊

預設情況下，在DDS環境中，FlowCollector和SMC裝置會嘗試儲存儘可能多的每日旋轉流量資料。當達到磁碟使用限制時，系統首先開始刪除最舊的資料，以便為要儲存的新資料創造空間。

要檢視流量收集器資料庫統計資訊，請登入到FlowCollector Admin UI，然後選擇 [Support > Database Storage Statistics](#) .

The screenshot displays the 'FlowCollector for NetFlow VE' Admin UI. The left sidebar contains navigation options: Home, Configuration, Manage Users, Support, Advanced Settings, Database Storage Statistics (selected), Backup/Restore Database, Browse Files, Packet Capture, Update, Backup/Restore Configuration, Diagnostics Pack, Audit Log, Operations, Logout, and Help. 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

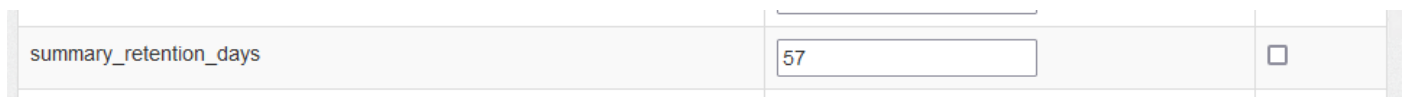
  

Data	Days	Containers	Rows			Bytes		
			Total	Average Per Day	Largest Day	Total	Average Per Day	Largest Day
Flow Details	286	295	5.46G	19.1M	57.08M	58.53G	204.65M	719.87M
Flow Interface Details	8	27	45.71M	5.71M	6.03M	1.1G	137.8M	145.61M
Total	286	322	5.51G	24.81M	63.11M	59.63G	342.45M	865.49M

### 資料庫儲存統計資訊

- 該圖顯示，攝入的流詳細資訊 ( netflow資料 ) 平均每天約204.65MB，此流量收集器儲存的資料約為58.5GB。
- 該圖顯示，接收流介面詳細資訊 ( 介面特定統計資訊 ) 平均每天約為137MB，並且此流量收集器儲存了大約1.1GB的資料。
- 該圖顯示，總流量資料平均每天約為342.53 GB，並且此流量收集器儲存的總資料量約為60 GB。
- 如果希望將資料庫縮小到總儲存資料的大約20G，將其除以每天平均0.35G ( 等於57 ) 。

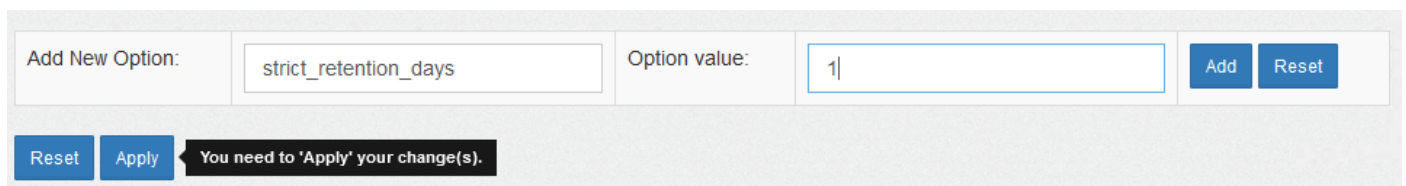
要將資料庫總大小減少為約20Gb，請更改 `summary_retention_days` 值到57。接下來，導航至 [Support > Advanced Settings](#)。尋找 `summary_retention_days` 並將其更改為所需的值。



The screenshot shows a configuration table with one row. The column name is `summary_retention_days` and the value entered in the adjacent cell is 57. There is a small square icon to the right of the value field.

`summary_retention_days`

接下來，在清單底部新增一個新選項。其 `Add New Option` 值是 `strict_retention_days` 和 `Option Value` 如圖所示，值設定為1。按一下「新增」。此 `strict_retention_days` 通知引擎僅保留宣告的天數 `summary_retention_days`。



The screenshot shows the 'Add New Option' form. The 'Add New Option:' field contains `strict_retention_days`. The 'Option value:' field contains 1. There are 'Add' and 'Reset' buttons to the right. Below the form, there are 'Reset' and 'Apply' buttons, and a message box that says 'You need to 'Apply' your change(s)'.

`strict_retention_days`

一旦我改變了 `summary_retention_days` 至4，我新增了新選項值，請按 `Apply` 在頁面底部。

如果要進行升級，請刪除 `strict_retention_days` 完成升級後返回的值，以儘可能長時間地保留資料。

## 裁切分散式資料庫(DDS) — 流介面詳細資訊

1. `log` 在成長至 您的 `Stealthwatch` 桌面 使用者端 作為 其 `admin` 使用者。
2. 在企業樹中找到 `FlowCollector`。按一下 `plus(+)` 簽名以展開容器。
3. 右鍵單擊所需的 `FlowCollector`。選擇 `Configuration > Properties`。
4. 在其 流收集器 屬性 對話方塊 框，按一下 `Advanced`。
5. 選擇 其 `Store flow interface data` 欄位。設定 其 限制 成長至 `UP` 成長至 15 天 或 30 天。
6. 按一下 `OK`。

## 增加磁碟空間(僅限虛擬裝置)

關閉虛擬機器電源，並增大從虛擬機器監控程式分配給VM的磁碟大小。額外的磁碟空間分配給 `/lancope/var/` 分割槽。

要使 `Stealthwatch` 在重新啟動後佔用此未分配的磁碟空間，可能需要執行其他步驟，請檢視虛擬機器版的「`Data Storage (資料儲存)`」指南，瞭解所需的磁碟大小。

根(`/`)分割槽大小是靜態的，無法調整。需要在安裝期間對根分割槽較大的版本進行全新安裝。

## 相關資訊

- [特色指南](#)
- [安全網路分析技術支援與檔案 — Cisco Systems](#)
- [思科全球支援聯絡人](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。