# Gestire l'utilizzo di file system/dischi locali in Secure Network Analytics

## Sommario



## Introduzione

In questo documento vengono descritti i passaggi generali per ridurre l'utilizzo elevato del disco nei dispositivi Secure Network Analytics Manager e Flow Collector.

## Prerequisiti

### Requisiti

Questo documento è relativo alle distribuzioni di analisi di rete sicure senza archivio dati.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Network Analytics Manager - v7.1+
- Secure Network Analytics Flow Collector - v7.1+
- Secure Network Analytics Flow Sensor - v7.1+
- Secure Network Analytics UDP Director - v7.1+

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Premesse

Esistono due partizioni da monitorare per l'utilizzo del disco: la partizione radice (/) e la partizione /lancope/var.

La partizione radice (/) è la posizione di archiviazione per l'immagine del kernel e alcuni log di sistema. Si tratta in genere di una partizione più piccola di 20G o meno.  /lancope/var è un gruppo di volumi e rappresenta la posizione di memorizzazione per la maggior parte dei dati di sistema, quindi occupa la maggior parte dello spazio su disco per l'accessorio.

# Raccogli dati

È possibile ottenere informazioni sull'utilizzo del disco in due posizioni, ovvero l'interfaccia utente Web di amministrazione e l'interfaccia della riga di comando (CLI).

## Riga di comando

Dalla riga di comando eseguire il comando **df -ah / /lancope/var** e annotare gli spazi tra (/) 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:/#

L'output mostra che la partizione radice (/) è 20G e che 8.3G è in uso, ovvero il 46%. L'output mostra anche che la partizione /lancope/var è 108G, e 23G è in uso che è il 22%.

## Interfaccia utente Web

Accedere all'interfaccia utente di amministrazione dei dispositivi basata sul modello in questione e scorrere fino alla fine della pagina.

Elenco di indirizzi Web dell'interfaccia utente di amministrazione:

- Secure Network Analytics Manager - https://<SMC-IP-OR-FQDN>/smc/index.html (è

necessario accedere a SMC prima di poter accedere a questo URL)
- Secure Network Analytics Flow Collector - https://<FC-IP-OR-FQDN>/swa/index.html
- Secure Network Analytics Flow Sensor - https://<FS-IP-OR-FQDN>/fs/index.html
- Secure Network Analytics UDP Director (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 l'utilizzo della partizione è maggiore o uguale al 75%, la partizione viene evidenziata.

# Cancella spazio su disco

Se non si è certi dei file da eliminare, aprire una richiesta TAC o contattare il supporto Cisco tramite la pagina dei contatti del supporto Cisco internazionali nella sezione Informazioni correlate alla fine del presente documento.

## Log di sistema

Uno dei metodi più veloci per recuperare spazio su disco di dimensioni maggiori consiste nell'eliminare i registri di registro con `journalctl --vacuum-time 1d` Notate il doppio trattino — prima della parola "vuoto".

<#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:/#
```

Circa 4 G di spazio su disco sono stati recuperati da questi passaggi e ha comportato una

riduzione dell'utilizzo del disco dal 22% al 18% sulla partizione /lancope/var.

I file nelle directory elencate sono generalmente sicuri da eliminare:

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

Si consiglia di iniziare dalla directory radice (/) o dalla directory /lancope/var, a seconda della partizione identificata nell'interfaccia utente Web che utilizza un disco elevato. Cambiare la directory corrente con `cd /`

Eseguire il `du -xah --max-depth=1 | sort -hr` per determinare i maggiori consumer di spazio su disco della directory corrente. Notate il doppio trattino — prima di max-depth.

L'output mostra che la partizione radice (/) ha uno spazio su disco di 8,3G in uso, con 5,5G di spazio su disco utilizzato nella directory /lancope, seguito dalla directory /usr con 1,5G di utilizzo.

```
<#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:/#
```

Cambiare la directory in /lancope con il **`cd lancope/`** ed eseguire nuovamente il comando du con il comando `!du` In questo modo viene visualizzato che della versione 5.5G in uso nella directory /lancope/, la versione 5.1G si trova nella directory admin. Modificare le directory correnti nella directory in questione con `cd`

```
<#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#
```

Una volta identificati i file che possono essere eliminati, è possibile procedere con rm -i
Se non si è certi dei file da eliminare, aprire una richiesta TAC o contattare il supporto Cisco tramite la pagina dei contatti del supporto Cisco internazionali nella sezione Informazioni correlate alla fine del presente documento.

<#root>

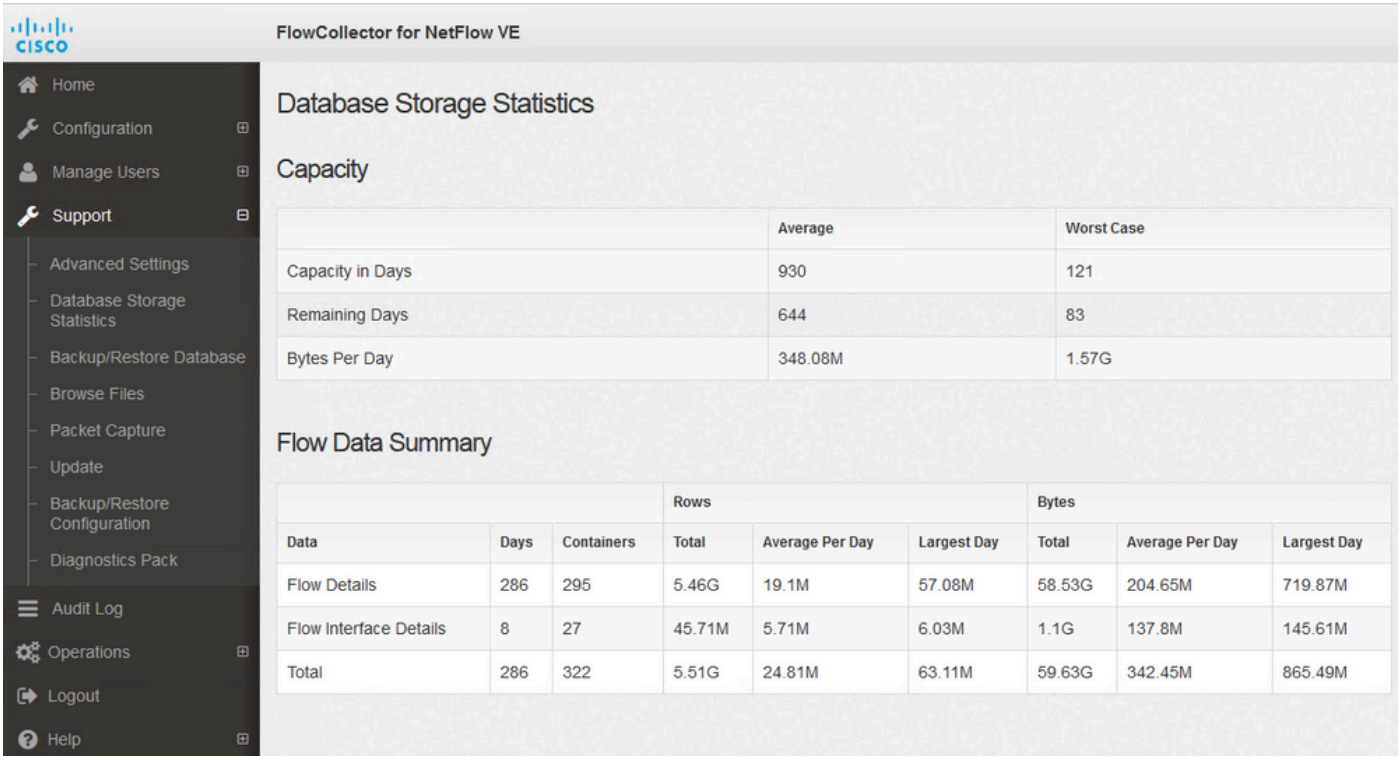
```
732smc:/lancope/admin#
rm -i file

rm: remove regular empty file 'file'?
yes

732smc:/lancope/admin#
```

Ripetere questi passaggi, se necessario.

## Tagliare il database distribuito (DDS) - Statistiche flusso

Per impostazione predefinita, nell'ambiente DDS gli accessori FlowCollector e SMC tentano di memorizzare il maggior numero possibile di dati di flusso ruotati ogni giorno. Quando vengono raggiunti i limiti di utilizzo del disco, il sistema inizia a eliminare i dati meno recenti per creare spazio per il salvataggio di nuovi dati.

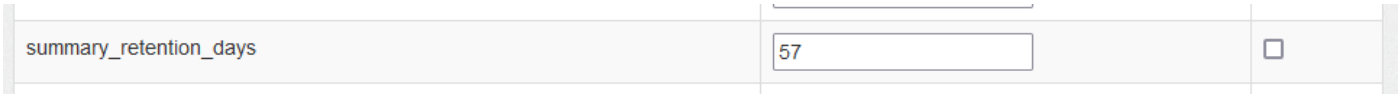
Per visualizzare le statistiche del database di Flow Collector, accedere all'interfaccia utente di amministrazione di Flow Collector e selezionare Support > Database Storage Statistics .




Statistiche archiviazione database

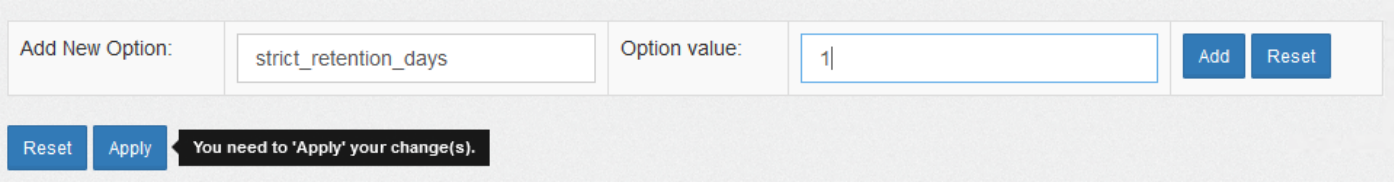
- L'immagine mostra che i dettagli del flusso acquisiti (dati netflow) sono in media di circa 204,65 MB al giorno e questo Flow Collector ha circa 58,5 GB di dati archiviati.
- Nell'immagine viene mostrato che i dettagli dell'interfaccia di flusso acquisiti (statistiche specifiche dell'interfaccia) misurano circa 137 MB al giorno e questo Flow Collector contiene circa 1,1 GB di dati archiviati.
- L'immagine mostra che il totale di Flow Data è in media di 342,53 GB al giorno e questo Flow Collector ha circa 60 GB di dati totali archiviati.
- Se si desidera ridurre il database in modo da memorizzare circa 20 GB di dati totali, dividerli per la media giornaliera di 0,35 GB, che equivale a 57.

Per ridurre le dimensioni totali del database a circa 20 Gb, modificare la summary_retention_days valore 57. Passare quindi a Support > Advanced Settings . Cerca summary_retention_days e impostarlo sul valore desiderato.




giorni_conservazione_riepilogo

Aggiungere quindi una nuova opzione in fondo all'elenco. OSPF (Open Shortest Path First) Add New Option valore è strict_retention_days e Option Value è impostato su 1 come mostrato nell'immagine. Fare clic su Add. Questo strict_retention_days indica al motore di mantenere solo il numero di giorni dichiarato in Summary_retention_days .




giorni_conservazione_rigorosa

Una volta modificata la **summary_retention_days** a 4 e il nuovo valore dell'opzione è stato aggiunto, premere Apply nella parte inferiore della pagina.

Se si esegue questa procedura per un aggiornamento, eliminare **strict_retention_days** una volta completato l'aggiornamento, per tornare a conservare i dati il più a lungo possibile.

### Tagliare il database distribuito (DDS) - Dettagli interfaccia flusso

1. Log ina il tuo Stealthwatch Desktop Cliente come OSPF (Open Shortest Path First) admin utente.

2. Individuare il FlowCollector nell'albero aziendale. Fare clic sul segno più (+) firmare per espandere il contenitore.

3. Fare clic con il pulsante destro del mouse sul FlowCollector desiderato. Seleziona Configuration > Properties.

4. Dentro OSPF (Open Shortest Path First) FlussoCollector Proprietà dialogo scatola, fare clic su Advanced.

5. Seleziona OSPF (Open Shortest Path First) Store **flow interface data**campo. Imposta OSPF (Open Shortest Path First) limite a Su a 15 giorni o 30 giorni.

6. Fare clic su OK .

## Aumento dello spazio su disco (solo appliance virtuali)

Spegnere la macchina virtuale e aumentare le dimensioni del disco allocato alla macchina virtuale dall'hypervisor. Lo spazio su disco aggiuntivo viene allocato alla partizione /lancope/var/.

Per consentire a Stealthwatch di utilizzare lo spazio su disco non allocato dopo un riavvio, potrebbe essere necessario eseguire ulteriori passaggi. Per informazioni sulle dimensioni del disco richieste, vedere Archiviazione dati della guida all'installazione della versione della macchina virtuale in uso.

Le dimensioni della partizione radice (/) sono statiche e non possono essere regolate. È necessaria una nuova installazione per una versione con una partizione radice più grande creata durante l'installazione.

## Informazioni correlate

- Guide all'installazione
- Documentazione e supporto tecnico per Secure Network Analytics - Cisco Systems
- Contatti del supporto Cisco internazionali

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).