Secure Network Analyticsでのローカルファイルシステム/ディスク使用量の管理

内容

概要

このドキュメントでは、Secure Network Analytics ManagerおよびFlow Collectorデバイスのディスク高使用率を減らす一般的な手順について説明します。

前提条件

要件

このドキュメントは、Data Storeを使用しないSecure Network Analyticの導入に適用されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Network Analytics Manager - v7.1+
- Secure Network Analyticsフローコレクタ – v7.1+
- Secure Network Analyticsフローセンサー – v7.1+
- Secure Network Analytics UDP Director - v7.1+

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ディスクの使用状況を監視するパーティションには、ルート(/)パーティションと/lancope/varパーティションの2つがあります。

ルート(/)パーティションは、カーネルイメージと一部のシステムログの保存場所であり、通常は20G以下の小さいパーティションです。 /lancope/varはボリューム・グループであり、システム・データの大半を格納する場所であるため、アプライアンスのディスク領域の大半を消費します。

データの収集

ディスクの使用状況に関する情報は、admin Web UIとコマンドラインインターフェイス(CLI)の2つの場所から入手できます。

コマンドライン

コマンドラインから、 **df -ah / /lancope/var** コマンドを実行し、(/)と/lancope/varの間のスペースに注目します。

<#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:/#
```

出力は、ルート(/)パーティションが20Gで、8.3G(46 %)が使用中であることを示しています。 出力には、/lancope/varパーティションが108Gであり、23Gが使用中(22 %)であることも示されています。

Web UI

対象のモデルに基づいてデバイスのAdmin UIにログインし、ページの一番下までスクロールします。

管理UI Webアドレスの一覧：

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

URLにアクセスするには、SMCにログインする必要があります）
- Secure Network Analyticsフローコレクタ：https://<FC-IP-OR-FQDN>/swa/index.html
- Secure Network Analyticsフローセンサー：https://<FS-IP-OR-FQDN>/fs/index.html
- Secure Network Analytics UDP Director（フローレプリケータ）: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

パーティションの使用率が75 %以上の場合、そのパーティションは強調表示されます。

ディスク領域のクリア

どのファイルを安全に削除できるかわからない場合は、TACケースを開くか、このドキュメントの最後の「関連情報」セクションにあるCisco Worldwide Support Contactページを使用してシスコのサポートに連絡してください。

システム ログ

サイズの大きいディスク領域をリカバリする最も高速な方法の1つは、以下のコマンドを使用してジャーナル・ログをクリアすることです。 journalctl --vacuum-time 1d コマンドを使用して、アップグレードを実行します。「vacuum」という単語の前にダブルハイフンがあることに注意してください。

<#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:/#
```

これらの手順によって約4Gのディスク領域が解放され、/lancope/varパーティションのディスク使用率が22 %から18 %に減少しました。

リストされたディレクトリ内のファイルは、一般に安全に削除できます。

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

ディスク使用率が高いWeb UIで特定したパーティションのルート(/)または/lancope/varディレクトリから開始することをお勧めします。現在のディレクトリを `cd /` コマンドを使用して、アップグレードを実行します。

を実行します。 `du -xah --max-depth=1 | sort -hr` コマンドを発行して、現在のディレクトリのディスク領域の最大コンシューマを判別します。max-depthの前の二重ハイフンに注意してください。

この出力は、ルート(/)パーティションに8.3Gのディスク領域が使用され、/lancopeディレクトリに5.5Gのディスク領域が使用され、その後に/usrディレクトリが使用され、1.5Gのディスク領域が使用されていることを示しています。

```
<#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:/#
```

/lancopeディレクトリに移動し、 **cd lancop**e/ コマンドを使用してduコマンドを再実行し、 !du コマンドを使用して、アップグレードを実行します。 これで、/lancope/ディレクトリで使用中の5.5Gのうち、5.1Gがadminディレクトリにあることが表示されます。現在のディレクトリを問題のディレクトリに変更します。 cd コマンドを使用して、アップグレードを実行します。

```
<#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#
```

削除可能なファイルを特定したら、 rm -i
 コマンドを使用して、アップグレードを実行します。どのファイルを安全に削除できるかわからない場合は、TACケースを開くか、このドキュメントの最後の「関連情報」セクションにあるCisco Worldwide Support Contactページを使用してシスコのサポートに連絡してください。

<#root>

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

rm -i file

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

yes

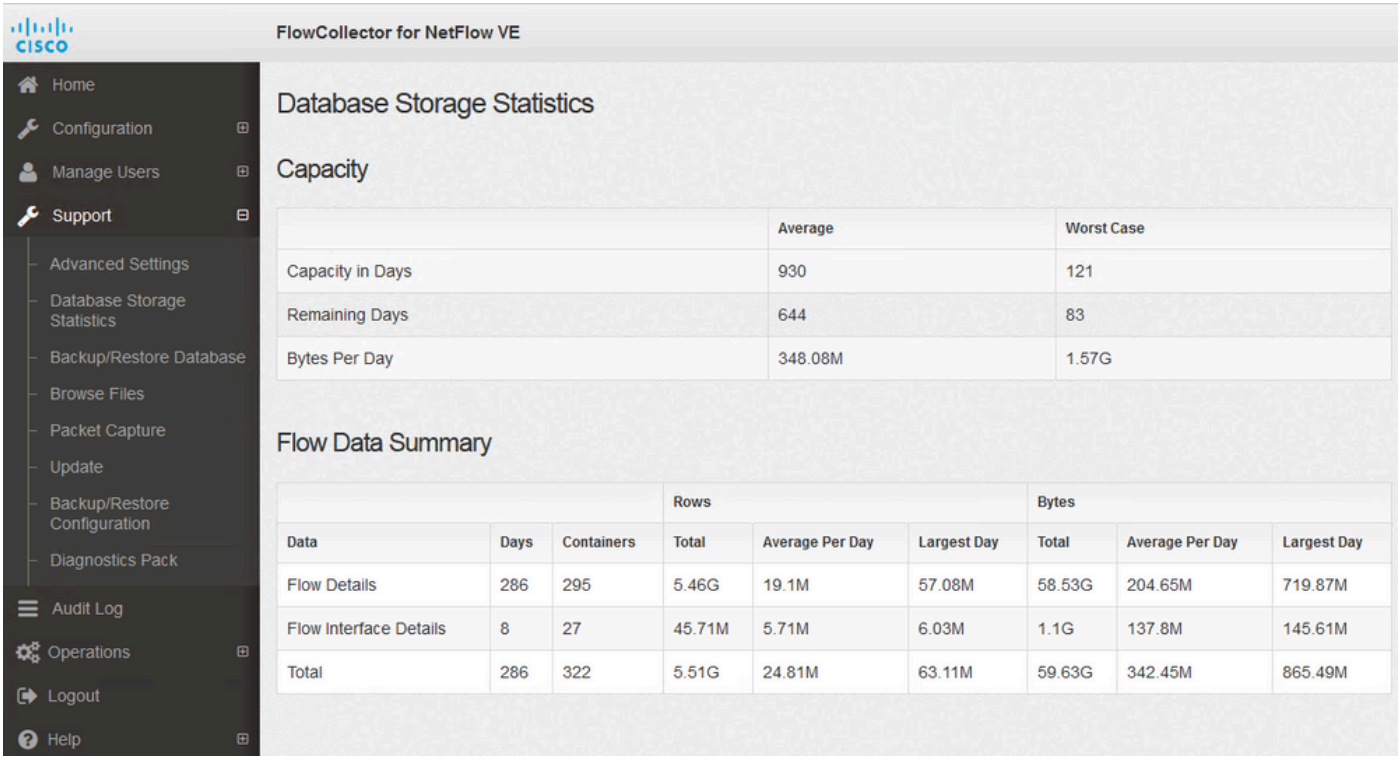
```
732smc:/lancope/admin#
```

必要に応じてこれらの手順を繰り返します。

分散データベース(DDS)のトリミング – フロー統計

デフォルトでは、DDS環境では、FlowCollectorおよびSMCアプライアンスは、毎日ローテーションされたフローデータをできるだけ多く保存しようとします。ディスク使用量の上限に達すると、システムは最も古いデータを最初に削除し、保存する新しいデータ用の領域を作成します。

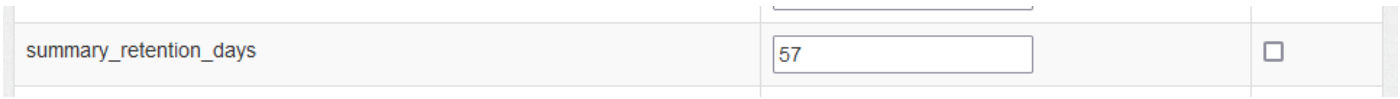
Flow Collectorデータベースの統計情報を表示するには、FlowCollector Admin UIにログインし、 Support > Database Storage Statistics を参照。



データベース記憶域の統計情報

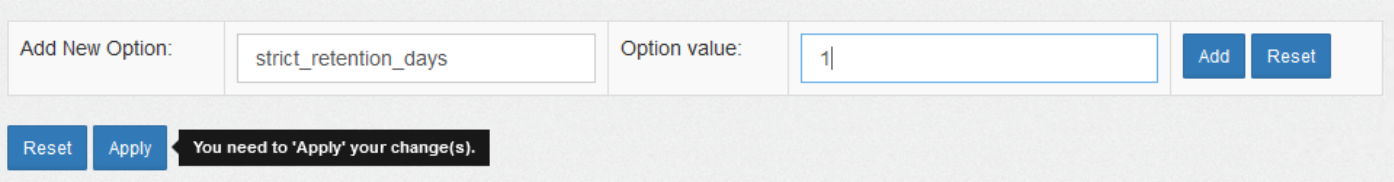
- この図は、取り込まれたフローの詳細（netflowデータ）の1日平均約204.65 MB、このフローコレクタには約58.5 GBのデータが保存されていることを示しています。
- この図は、取り込まれたフローインターフェイスの詳細（インターフェイス固有の統計情報）が1日平均137 MBで、このフローコレクタには約1.1 GBのデータが格納されていることを示しています。
- この図は、フローデータの合計が1日平均約342.53 GBで、このフローコレクタに保存されているデータの合計が約60 GBであることを示しています。
- データベースを縮小して合計で約20Gのデータを格納する場合は、日平均の。35G（57に相当）で割ります。

データベースの合計サイズを約20 Gbに減らすには、 summary_retention_days 57に設定します。 次に、 Support > Advanced Settings . 検索 summary_retention_days これを希望する値に変更します。



summary_retention_days

次に、リストの下部に新しいオプションを追加します。「 Add New Option 値は strict_retention_days および Option Value 図に示すように、値は1に設定されます。[Add] をクリックします。 これは strict_retention_days で宣言された日数のみを保持するようにエンジンに指示します。 Summary_retention_days を参照。



strict_retention_days

設定を変更すると、 **summary_retention_days** 4に変更し、新しいオプション値を追加したら、 Apply ページの下部にあります。

アップグレードに次の手順を実行する場合は、 **strict_retention_days** アップグレードが完了した後に値を戻し、できるだけ長くデータを保持します。

分散データベース(DDS)のトリミング – フローインターフェイスの詳細

1. log インから お客様の Stealthwatch デスクトップ クライアント as ページ admin されます。

2. Enterprise ツリーでFlowCollector を見つけます。プラス(+)コンテナを展開するには署名します。

3.目的のFlowCollectorを右クリックします。 選択 Configuration > Propertiesを参照。

4. イン ページ フローコレクタ Properties 対話 ボックス、 クリック Advancedを参照。

5. 選択 ページ Store **flow interface data**フィールドの URL のみが置換されます。 Set ページ 制限 から 2013 年以降 から 15 日 または 30 日を参照。

6. クリック OK を参照。

ディスク容量の増加(仮想アプライアンスのみ)

仮想マシンの電源を切り、ハイパーバイザからVMに割り当てるディスクサイズを増やします。 追加のディスク領域は/lancope/var/パーティションに割り当てられます。

再起動後にStealthwatchでこの未割り当てディスク領域を使用するには、追加の手順が必要になる場合があります。必要なディスクサイズについては、ご使用の仮想マシンエディションのインストールガイドのデータストレージを参照してください。

ルート(/)パーティションのサイズは静的であり、調整できません。インストール中に作成された、より大きなルートパーティションを持つバージョンへの新規インストールが必要です。

関連情報

- インストレーションガイド
- Secure Network Analyticsテクニカルサポートとドキュメント – Cisco Systems
- 各国のシスコ サポートの連絡先

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。