보안 네트워크 분석에서 로컬 파일 시스템/디스크 사용량 관리

목차

소개

이 문서에서는 Secure Network Analytics Manager 및 Flow Collector 장치의 높은 디스크 사용량을 줄이기 위한 일반적인 단계를 설명합니다.

사전 요구 사항

요구 사항

이 문서는 데이터 저장소를 사용하지 않는 보안 네트워크 분석 배포에 적용됩니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 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+

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

디스크 사용량을 모니터링할 두 개의 파티션, 즉 루트(/) 및 /lancope/var 파티션이 있습니다.

루트(/) 파티션은 커널 이미지 및 일부 시스템 로그의 저장 위치이며, 일반적으로 20G 이하의 더 작은 파티션입니다. /lancope/var은 볼륨 그룹이며 대부분의 시스템 데이터에 대한 스토리지 위치이므로 어플라이언스에 대한 디스크 공간의 대부분을 사용합니다.

데이터 수집

디스크 사용량 정보를 얻을 수 있는 곳은 관리 웹 UI 및 CLI(Command Line Interface)입니다.

명령줄

명령줄에서 **df -ah / /lancope/var** 명령을 실행하고 (/)와 /lancope/var 사이의 공백을 확인합니다.

<#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:/#
```

출력에 따르면 루트(/) 파티션은 20G이고 8.3G가 사용 중이며 46%입니다. 또한 /lancope/var 파티션이 108G이며 23G가 사용 중이며 22%가 사용됩니다.

웹 UI

해당 모델을 기반으로 디바이스 관리 UI에 로그인하고 페이지 아래쪽으로 스크롤합니다.

관리자 UI 웹 주소 목록:

- Secure Network Analytics Manager - https://<SMC-IP-OR-FQDN>/smc/index.html (이 URL에 액세스하려면 SMC에 로그인해야 함)
- Secure Network Analytics Flow Collector - https://<FC-IP-OR-FQDN>/swa/index.html
- 보안 네트워크 분석 플로우 센서 - 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

파티션의 사용량이 75% 이상인 경우 파티션이 강조 표시됩니다.

디스크 공간 지우기

어떤 파일을 삭제해도 안전한지 확실하지 않은 경우 TAC 케이스를 열거나 이 문서 끝의 Related Information(관련 정보) 섹션에 있는 Cisco Worldwide Support Contact(Cisco 전 세계 지원 연락처) 페이지를 통해 Cisco 지원에 문의하십시오.

시스템 로그

상당한 크기의 디스크 공간을 복구하는 가장 빠른 방법 중 하나는 journalctl --vacuum-time 1d 명령을 실행합니다. "진공"이라는 단어 앞에 하이픈을 두 번 붙입니다.

```
<#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:/#
```

이러한 단계를 통해 약 4G의 디스크 공간을 확보했으며 /lancope/var 파티션의 디스크 사용량이 22%에서 18%로 감소했습니다.

나열된 디렉토리의 파일은 일반적으로 삭제해도 안전합니다.

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

/lancope/var/admin/tmp/

루트(/) 또는 /lancope/var 디렉토리 중 디스크 사용량이 많은 웹 ui에서 식별된 파티션에서 시작하는 것이 좋습니다. 현재 디렉토리를 cd / 명령을 실행합니다.

실행 du -xah --max-depth=1 | sort -hr 명령을 사용하여 현재 디렉터리의 디스크 공간 최대 소비자를 확인합니다. 최대 깊이 앞에 이중 하이픈이 있습니다.

이 출력은 루트(/) 파티션이 사용 중인 디스크 공간이 8.3G이며 /lancope 디렉토리에서 5.5G의 디스크 공간이 사용되고 그 뒤에 /usr 디렉토리가 1.5G로 사용됨을 보여 줍니다.

<#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:/#

디렉토리를 /lancope로 변경합니다. **cd lancop**e/ 명령을 실행하고 CLI에서 !du 명령을 실행합니다. /lancope/ 디렉터리에서 사용 중인 5.5G 중 5.1G가 admin 디렉터리에 있는 것을 표시합니다. 현재 디렉터리를 해당 디렉터리로 변경합니다. cd 명령을 실행합니다.

<#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#

삭제할 수 있는 파일을 식별한 후에는 rm -i
명령을 실행합니다. 어떤 파일을 삭제해도 안전한지 확실하지 않은 경우 TAC 케이스를 열거나 이

문서 끝의 Related Information(관련 정보) 섹션에 있는 Cisco Worldwide Support Contact(Cisco 전 세계 지원 연락처) 페이지를 통해 Cisco 지원에 문의하십시오.

<#root>

732smc:/lancope/admin#

rm -i file

rm: remove regular empty file 'file'?

yes

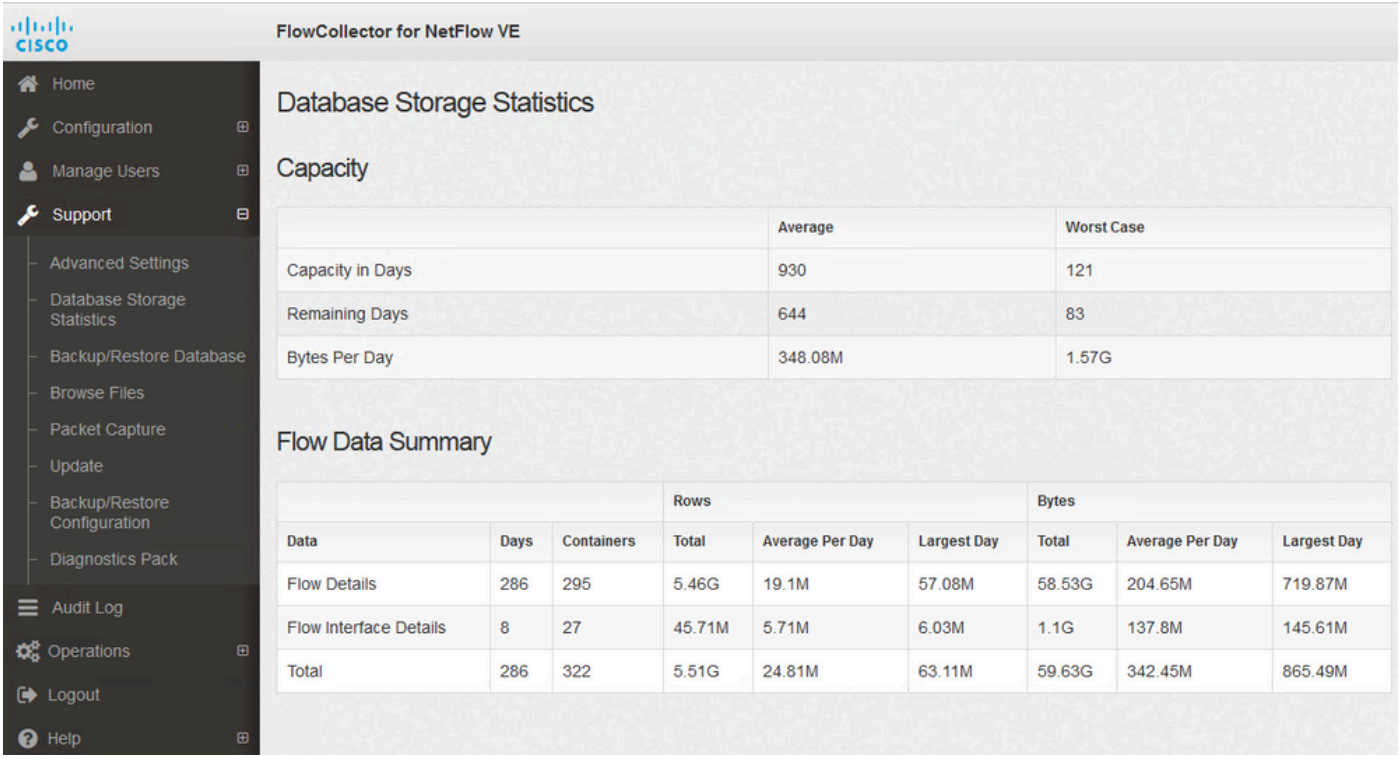
732smc:/lancope/admin#

필요에 따라 이 단계를 반복합니다.

분산 데이터베이스(DDS) 트리밍 - 흐름 통계

기본적으로 DDS 환경에서는 FlowCollector 및 SMC 어플라이언스가 매일 순환되는 플로우 데이터를 최대한 저장하려고 시도합니다. 디스크 사용량 제한에 도달하면 시스템은 가장 오래된 데이터를 먼저 삭제하기 시작하여 새 데이터를 저장할 공간을 만듭니다.

Flow Collector 데이터베이스 통계를 보려면 FlowCollector Admin UI에 로그인한 다음 Support > Database Storage Statistics .



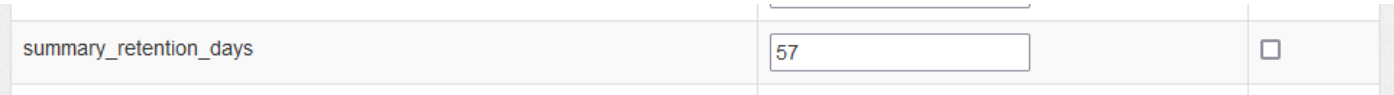
데이터베이스 스토리지 통계

- 이 그림에서는 수집된 Flow Details(netflow 데이터)가 하루 평균 약 204.65MB이며, 이 Flow

Collector에는 약 58.5GB의 데이터가 저장되어 있습니다.

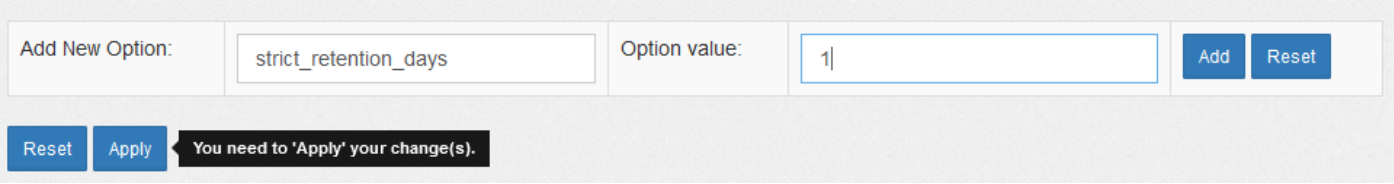
- 이 그림에서는 수집된 Flow Interface Details(인터페이스별 통계)의 평균이 하루 약 137MB이며, 이 Flow Collector에는 약 1.1GB의 데이터가 저장되어 있습니다.
- 이 그림에서는 총 플로우 데이터의 평균이 하루에 약 342.53GB이며 이 플로우 컬렉터에는 약 60GB의 총 데이터가 저장되어 있습니다.
- 전체 데이터의 약 20G가 저장되도록 데이터베이스를 축소하려면 일일 평균 0.35G를 57로 나누십시오.

전체 크기가 약 20Gb가 되도록 데이터베이스를 줄이려면 초ummary_retention_days 값을 57로 설정합니다. 다음으로, Support > Advanced Settings . 찾기 summary_retention_days 원하는 값으로 변경합니다.



요약 보존_일

그런 다음 목록의 맨 아래에 새 옵션을 추가합니다. 이 Add New Option 값: strict_retention_days 및 Option Value 값은 이미지에 표시된 대로 1로 설정됩니다. Add(추가)를 클릭합니다. 이 strict_retention_days 엔진에 선언된 일 수만 유지하도록 지시합니다. 초ummary_retention_days .



strict_retention_days

변경 후 **summary_retention_days** 4에 추가했고 새로운 옵션 값을 추가했습니다. Apply 페이지의 맨 아래에 있습니다.

업그레이드를 위해 다음 단계를 수행할 경우 **strict_retention_days** 업그레이드가 완료되면 가능한 한 오랫동안 데이터를 보존할 수 있습니다.

분산 데이터베이스(DDS) 트리밍 - 흐름 인터페이스 세부사항

1. 로그 에서수신 사용자 Stealthwatch 데스크톱 클라이언트 다음으로 이 관리자 사용자.

2. 엔터프라이즈 트리에서 FlowCollector를 찾을 수 있습니다. 더하기를 클릭합니다(+) 컨테이너를 확장하는 데 서명합니다.

3. 원하는 FlowCollector를 마우스 오른쪽 버튼으로 클릭합니다. 선택 Configuration > Properties.

4. 수신 이 플로우컬렉터 속성 대화 상자, 클릭 Advanced.

5. 선택 이 Store **flow interface data**필드. 설정 이 한계 수신 위로 수신 15 일 또는 30 일.

6. 클릭 OK .

디스크 공간 증가(가상 어플라이언스에만 해당)

가상 머신의 전원을 끄고 하이퍼바이저에서 VM에 할당된 디스크 크기를 늘립니다. 추가 디스크 공간이 /lancope/var/ 파티션에 할당됩니다.

재부팅 후 Stealthwatch에서 할당되지 않은 이 디스크 공간을 사용하려면 추가 단계가 필요할 수 있습니다. 필요한 디스크 크기에 대해서는 가상 머신 에디션 설치 가이드의 데이터 저장소를 검토하십시오.

루트(/) 파티션 크기는 정적이며 조정할 수 없습니다. 설치 중에 생성된 더 큰 루트 파티션이 있는 버전에 새로 설치해야 합니다.

관련 정보

- 설치 가이드
- 보안 네트워크 분석 기술 지원 및 문서 - Cisco Systems
- Cisco 전 세계 지원 문의처

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.