Sourcefire 어플라이언스에서 과도한 디스크 사용률 문제 해결

목차

소개

FireSIGHT Management Center 또는 FirePOWER 어플라이언스는 다양한 이유로 디스크 공간이 부족할 수 있습니다.이 경우 디스크 사용률이 높으면 상태 알림이 트리거되거나 소프트웨어 업데이트 시도가 실패할 수 있습니다.이 문서에서는 과도한 디스크 사용률의 근본 원인 및 일부 문제 해결 단계에 대해 설명합니다.

확인 단계

많이 사용되는 파티션을 확인합니다.다음 명령은 디스크 사용률을 보여줍니다.

FireSIGHT Management Center에서

```
admin@3DSystem:~# df -TH
```

7000 및 8000 Series 어플라이언스와 NGIPS 가상 디바이스에서

```
> show disk
```

두 명령 모두 아래와 같은 출력을 표시합니다.

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda5 2.9G 566M 2.2G 21% /
/dev/sda1 99M 16M 79M 17% /boot
```

```
/dev/sda7 52G 8.5G 41G 18% /Volume
none 11G 20K 11G 1% /dev/shm
/dev/sdb1 418G 210M 395G 1% /var/storage
```

참고:디스크 크기와 사용률은 다양한 어플라이언스 모델에 따라 달라질 수 있습니다.NGIPS 가상 디바이스인 경우 파티션의 크기가 최소 디스크 공간 요구 사항을 충족하는지 확인합니다 .

주의:위에 표시되지 않은 추가 파티션은 지원되지 않습니다.

7000 및 8000 Series 어플라이언스와 NGIPS 가상 디바이스에서 다음 명령을 실행하여 자세한 디스크 사용량 통계를 표시할 수 있습니다.

```
> show disk-manager
```

출력 예는 다음과 같습니다.

```
> show disk-manager
Silo Used Minimum Maximum
Temporary Files 143.702 MB 402.541 MB 1.572 GB
Action Queue Results 0 KB 402.541 MB 1.572 GB
Connection Events 17.225 GB 3.931 GB 23.586 GB
User Identity Events 0 KB 402.541 MB 1.572 GB
UI Caches 587 KB 1.179 GB 2.359 GB
Backups 0 KB 3.145 GB 7.862 GB
Updates 13 KB 4.717 GB 11.793 GB
Other Detection Engine 0 KB 2.359 GB 4.717 GB
Performance Statistics 72.442 MB 805.082 MB 9.435 GB
Other Events 669.819 MB 1.572 GB 3.145 GB
IP Reputation & URL Filtering 0 KB 1.966 GB 3.931 GB
Archives & Cores & File Logs 1.381 GB 3.145 GB 15.724 GB
RNA Events 0 KB 3.145 GB 12.579 GB
File Capture 12.089 MB 4.717 GB 14.152 GB
IPS Events 3.389 GB 7.076 GB 15.724 GB
```

/Volume 파티션이 꽉 찬 경우

이전 백업 파일

- 시스템에 많은 양의 오래된 백업 파일을 저장할 경우 디스크에 과도한 공간이 필요할 수 있습니다.

문제 해결 단계

- 웹 사용자 인터페이스를 사용하여 이전 백업 파일을 삭제합니다.백업 파일을 제거하려면 **System > Tools > Backup/Restore로 이동합니다**.

  팁:FireSIGHT 시스템에서 대용량 백업 파일을 저장하도록 원격 스토리지를 구성할 수 있습니다.

이전 소프트웨어 업데이트 및 패치 파일

- 이전 소프트웨어 업데이트, 업그레이드 및 패치 파일(예: 5.0 또는 5.1)을 항상 유지할 경우 디스크 공간이 부족해질 수 있습니다.

문제 해결 단계

- 더 이상 필요하지 않은 이전 업데이트 및 패치 파일을 삭제합니다.삭제하려면 System(시스템) **> Updates(업데이트)로** 이동하십시오.

과도한 이벤트 파일이 저장됨

- 관리되는 디바이스 또는 센서가 FireSIGHT Management Center로 이벤트 전송을 중지했을 수 있습니다.
- 관리 센터에서 수신하도록 설계된 것보다(초당) 더 많은 이벤트를 디바이스에서 생성할 수 있습니다.
- 관리되는 디바이스와 관리 센터 간에 통신 문제가 있을 수 있습니다.

문제 해결 단계

- 이벤트와 관련된 정책을 다시 적용합니다.예를 들어, 연결 이벤트가 표시되지 않으면 Access Control 정책을 다시 적용하고 Management Center에서 새 이벤트를 수신하는지 확인합니다.
- FireSIGHT Management Center에서 새 IPS 이벤트를 수신할 수 없는 경우 관리되는 디바이스와 관리 센터 간에 통신 문제가 있는지 확인하십시오.

알 수 없는 과도한 파일

- FireSIGHT System은 **알 수 없는** 네트워크 검색 데이터(OS, 호스트 및 서비스 정보)를 저장합니다.

문제 해결 단계

- 시스템이 네트워크의 호스트에서 운영 체제를 확인할 수 없는 경우 Nmap을 사용하여 호스트를 능동적으로 스캔할 수 있습니다.Nmap은 스캔에서 얻은 정보를 사용하여 가능한 운영 체제를 평가합니다.그런 다음 호스트 운영 체제 식별으로 가장 높은 등급을 가진 운영 체제를 사용합니다.
- 시스템이 알 수 없는 운영 체제의 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다. 규칙은 **검색 이벤트**가 **발생하고 호스트에 대한 OS 정보가 변경되었으며** 다음 조건을 충족할 때 트리거되어야 합니다.**OS 이름을 알 수 없습니다**.

이벤트를 저장할 대규모 데이터베이스

- 데이터베이스 이벤트 제한을 지침이나 모범 사례를 넘어 늘리면 FireSIGHT Management Center의 디스크 공간이 부족해질 수 있습니다.

문제 해결 단계

- 데이터베이스 제한 값을 확인합니다.디스크 사용률 및 성능을 향상시키려면 이벤트 제한을 **정기적으로** 작업하는 이벤트 수에 맞게 조정해야 합니다.일부 이벤트 유형에서는 스토리지를 비활성화할 수 있습니다.
- 데이터베이스 제한을 변경하려면 System Policy(시스템 정책) 페이지로 이동하여 시스템 정책 이름 옆에 있는 **Edit(편집)**를 클릭한 다음 왼쪽 섹션에서 Database(**데이터베이스)를** 클릭합니다.**시스템 정책** 페이지에 액세스하려면 **System > Local > System Policy**로 이동하십시오.

85% 이상의 디스크 사용률에 대한 상태 알림 수신

가능한 이유

- 이벤트 비율이 매우 높을 수 있습니다.따라서 디바이스에서 많은 이벤트를 생성하고 저장하고 있습니다.
- 관리되는 디바이스와 FireSIGHT Management Center 간의 통신 문제입니다.

문제 해결 단계

- 경고 임계값 레벨을 87%(경고) 및 92%(위험)로 변경하면 빈번한 상태 알림을 간단하게 해결할 수 있습니다.
- 릴리스 노트를 읽고 정리 시스템에 알려진 문제가 있는지 확인합니다.솔루션을 사용할 수 있는 경우 이 문제를 해결하려면 소프트웨어 버전을 최신 릴리스로 업데이트하십시오.

/var/log/messages 파일에는 24시간 이상 또는 25MB보다 큰 데이터가 들어 있습니다.

가능한 이유

- Logtate 데몬이 제대로 작동하지 않을 수 있습니다.

문제 해결 단계

- 이 문제가 발생하면 FireSIGHT Systems의 소프트웨어 버전을 최신 릴리스로 업데이트하십시오.최신 버전을 실행 중이지만 이 문제가 계속 발생하는 경우 Cisco TAC(Technical Assistance Center)에 문의하십시오.

루트(/) 파티션이 꽉 찬 경우

사용자 파일이 루트(/) 파티션에 저장됨

가능한 이유

- 루트(/) 파티션은 고정 크기이며 개인 스토리지용으로는 사용되지 않습니다.
- /var/tmp 디렉토리는 /var/common 디렉토리 대신 임시 스토리지에 수동으로 사용됩니다.

문제 해결 단계

- /root, /home 및 /tmp 폴더에서 불필요한 파일을 확인합니다.이 폴더는 개인 스토리지용으로 생성되지 않으므로 rm 명령을 사용하여 개인 파일을 삭제할 수 있습니다.

지원되지 않는 프로세스가 루트(/) 파티션에 쓰는 중입니다.

가능한 이유

- 루트(/) 파티션에 파일을 생성하는 타사 소프트웨어를 설치하는 경우 디스크 사용량이 많은 경우 상태 알림을 받을 수 있습니다.

문제 해결 단계

- 지원되지 않는 패키지가 설치되어 있는지 확인합니다.다음 명령을 실행하여 설치된 패키지를 찾습니다.

```
admin@3DSystem:~$ rpm -qa --last
```

- 지원되지 않는 프로세스가 실행 중인지 확인하려면 pstree 및 top을 선택합니다.다음 명령을 실행합니다.

```
admin@3DSystem:~$ pstree -ap

admin@3DSystem:~$ top
```