Problemen oplossen bij gebruik van diskette op Sourcefire-applicaties

Inhoud

Inleiding

Een FireSIGHT Management Center of een FirePOWER-apparaat kan om verschillende redenen geen schijfruimte meer hebben. Als dit gebeurt, wordt met het hoge diskgebruik een melding voor de gezondheid gegenereerd of kan er een poging tot aanpassing van de software mislukken. Dit artikel beschrijft de basisoorzaken van excessief diskgebruik en bepaalde stappen bij het oplossen van problemen.

Verificatiestappen

Bepaal de scheiding die sterk wordt gebruikt. De volgende opdracht toont het gebruik van de schijf:

Op een FireSIGHT Management Center,

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

op 7000 en 8000 Series toestellen en op NGIPS virtuele apparaten,

```
> show disk
```

Beide opdrachten tonen een uitvoer zoals hieronder:

```
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
```

Opmerking: De grootte en het gebruik van de schijf kunnen per apparaat verschillen. Als dit een NGIPS-virtueel apparaat is, controleert u of de grootte van de partities voldoet aan de minimale vereisten voor schijfruimte.

Voorzichtig: Elke extra partitie die hierboven niet wordt weergegeven, wordt niet ondersteund.

U kunt de volgende opdracht uitvoeren op apparaten van 7000 en 8000 Series en op virtuele NGIPS-apparaten om gedetailleerde statistische gegevens over het diskgebruik weer te geven:

```
> show disk-manager
```

Een voorbeeld-uitvoer:

```
> 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
```

Als de / Volume Partitie volledig is

Oude back-upbestanden

- Als u grote aantallen oude back-upbestanden op het systeem slaat, kan er veel ruimte op de schijf nodig zijn.

Stappen voor probleemoplossing

- Verwijdert de oude back-upbestanden via de webgebruikersinterface. Om reservekopieën te verwijderen, navigeer dan naar **Systeem > Gereedschappen > Back-up/terugzetten**.

  Tip: Op een FireSIGHT System kunt u de externe opslag configureren om de grote back-upbestanden op te slaan.

Oudere bestanden voor bijwerken software en patches

- Als u altijd de vorige software update, upgrade en patchbestanden (zoals 5.0 of 5.1) bewaarde, kan het systeem de schijfruimte mislopen.

Stappen voor probleemoplossing

- Verwijdert de oudere update- en patchbestanden die niet langer nodig zijn. Om hen te wissen, navigeer dan naar **Systeem > updates**.

Excessieve Event Files worden opgeslagen

- Beheerd apparaat of sensor kan zijn gestopt met het verzenden van gebeurtenissen naar het FireSIGHT Management Center.
- Een apparaat kan meer gebeurtenissen genereren dan een Management Center is ontworpen om te ontvangen (per seconde).
- Er kan een communicatieprobleem zijn tussen het beheerde apparaat en het beheercentrum.

Stappen voor probleemoplossing

- Pas het beleid dat met de gebeurtenis verband houdt opnieuw toe. Als u bijvoorbeeld geen verbindingsgebeurtenissen ziet, past u het beleid voor toegangscontrole opnieuw toe en ziet u of er nieuwe gebeurtenissen nu worden ontvangen door het Management Center.
- Als een FireSIGHT Management Center geen nieuwe IPS-gebeurtenissen kan ontvangen, controleert u of er sprake is van communicatie-problemen tussen het beheerde apparaat en het beheercentrum.

Buitensporige onbekende bestanden

- Het FireSIGHT System slaat de **onbekende** gegevens op van de netwerkdetectie (OS-, host- en servicetechnicus).

Stappen voor probleemoplossing

- Als het systeem niet het besturingssysteem van een host op uw netwerk kan bepalen, kunt u Nmap gebruiken om de host actief te scannen. Nmap gebruikt de informatie die het van de scan verkrijgt om de mogelijke besturingssystemen te beoordelen. Het gebruikt vervolgens het besturingssysteem met de hoogste rating als identificatie van het besturingssysteem van de gastheer.
- Maak een correlatieregel die geactiveerd wordt wanneer het systeem een host detecteert met een onbekend besturingssysteem.
  De regel moet van start gaan wanneer **een discovery event plaatsvindt** en **de OS informatie voor een host is gewijzigd** en voldoet aan de volgende voorwaarden: **OS Naam is onbekend**.

Grote database voor opslaan

- Als u de maximale waarde van een database-gebeurtenis verhoogt boven de richtlijn of de best practice, dan kan FireSIGHT Management Center de schijfruimte niet meer gebruiken.

Stappen voor probleemoplossing

- Controleer de waarden van de maximale database. Om het gebruik van schijven en de prestaties te verbeteren, dient u de limieten van de gebeurtenissen aan te passen aan het aantal gebeurtenissen waarmee u **regelmatig** werkt. Voor bepaalde eventtypen kunt u opslag

uitschakelen.
- Als u de maximale database wilt wijzigen, navigeer dan naar de pagina Systeembeleid, klik op **Bewerken** naast de naam van het systeembeleid en klik vervolgens op **Database** in de linkersectie. Om tot de pagina **Systeembeleid** te toegang, navigeer dan naar **Systeem > Lokaal > Systeembeleid**.

Gezondheidswaarschuwingen ontvangen voor meer dan 85% gebruik van schijf

Mogelijke redenen

- Het aantal voorvallen kan zeer hoog zijn. Daarom genereert en slaat het apparaat veel gebeurtenissen op.
- Communicatieproblemen tussen het beheerde apparaat en FireSIGHT Management Center.

Stappen voor probleemoplossing

- Een wijziging van de alarmdrempel naar 87% (Waarschuwing) en 92% (Kritisch) kan een eenvoudige oplossing zijn voor regelmatige waarschuwingen over de gezondheid.
- Lees de Releaseopmerkingen om te zien of er een bekend probleem met het pruning-systeem was. Als er een oplossing beschikbaar is, update de softwareversie naar de laatste release om dit probleem aan te pakken.

De /var/log/messing bestanden bevatten gegevens die ouder zijn dan 24 uur, of groter dan 25 MB

Mogelijke redenen

- Mogelijk werkt de opslagdatum niet goed.

Stappen voor probleemoplossing

- Indien u dit probleem tegenkomt, update de softwareversie van uw FireSIGHT Systems tot de nieuwste release. Als u de laatste versie draait, maar nog steeds dit probleem ervaren, neemt u contact op met Cisco Technical Assistance Center (TAC).

Als de worteloptie (/) volledig is

Gebruikersbestanden worden op de worteloptie (/) opgeslagen

Mogelijke redenen

- De wortelverdeling (/) is een vaste grootte en is niet bedoeld voor persoonlijke opslag.
- Het /var/tmp/geheugen wordt handmatig gebruikt voor tijdelijke opslag, in plaats van de /var/common folder.

Stappen voor probleemoplossing

- Controleer op overbodige bestanden in de map / root, /home en /tmp. Aangezien deze mappen niet voor persoonlijke opslag worden gemaakt, kunt u met rm-opdracht elk

persoonlijk bestand verwijderen.

Niet-ondersteunde processen schrijven naar wortelindeling (/)

Mogelijke redenen

- Als u software van derden installeert die bestanden op root (/) partitie maakt, kunt u een melding maken van het gebruik van een hoge schijf.

Stappen voor probleemoplossing

- Controleer of er niet-ondersteunde pakketten zijn geïnstalleerd. Start de volgende opdracht om de geïnstalleerde pakketten te vinden:

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

- Controleer het programma en de bovenkant om te zien of er niet-ondersteunde processen worden uitgevoerd. Start de volgende opdrachten:

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

```
admin@3DSystem:~$ top
```