Содержание

Введение

В Центре управления FireSIGHT или устройстве FirePOWER может закончиться дисковое пространство по различным причинам. Когда происходит, высокое использование диска инициирует предупреждение состояния или может отказать попытку обновления ПО. Эта статья описывает основные причины чрезмерного использования диска и некоторых действий по устранению проблем.

Этапы проверки

Определите разделение, которое высоко используется. Следующая команда показывает использование диска:

На центре управления FireSIGHT,

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

На 7000 и устройства серии 8000 и на виртуальных устройствах NGIPS,

```
> show disk
```

Обе команды показывают выходные данные как ниже:

```
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
```

> **Примечание:** Размер диска и использование могут варьироваться на различных моделях устройства. Если это - виртуальное устройство NGIPS, проверьте, что размер отделений соответствует минимальным требуемым пространствам на диске.

Внимание: Любое дополнительное разделение, которое не показывают выше, является неподдерживаемым.

На 7000 и устройства серии 8000 и на виртуальных устройствах NGIPS, можно выполнить следующую команду для отображения подробной статистики использования диска:

```
> show disk-manager
```

Пример выходных данных:

```
> 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
```

Если / Разделение Громкости Полно

Старые резервные файлы

- При хранении большого объема старых резервных файлов в системе он может занять чрезмерное место на диске.

Шаги по устранению неполадок

- Удалите старые резервные файлы с помощью интерфейса веба - пользователя. Для удаления резервных файлов перейдите к **Системе> Программные средства> Резервная копия/Восстановление**.

  Совет: В Системе FireSIGHT можно настроить удаленную систему хранения, чтобы хранить большие резервные файлы.

Более старое обновление ПО и файлы исправления

- Если вы всегда поддерживаете обновление предшествующего программного обеспечения, обновление и файлы исправления (такой как, 5.0 или 5.1), система может закончиться дисковое пространство.

Шаги по устранению неполадок

- Удалите более старое обновление и файлы исправления, которые больше не

необходимы. Для удаления их перейдите к **Системе> Обновления**.

Хранятся чрезмерные файлы события

- Управляемое устройство или датчик, возможно, прекратили передавать события к Центру управления FireSIGHT.
- Устройство может генерировать больше событий, чем Центр управления разработан для получения (в секунду).
- Могла бы быть проблема подключения между управляемым устройством и центром управления.

Шаги по устранению неполадок

- Повторно примените политику, которые отнесены к событию. Например, если вы не видите события подключения, повторно применяете Доступ политика Controil и видите, получаются ли какие-либо новые события теперь Центром управления.
- Если Центр управления FireSIGHT неспособен получить новые события IPS, проверьте, существуют ли какие-либо проблемы подключения между управляемым устройством и центром управления.

Чрезмерные неизвестные файлы

- Система FireSIGHT хранит данные Обнаружения **`неизвестной сети`** (ОС, хост и служебная информация).

Шаги по устранению неполадок

- Если система не может определить операционную систему на хосте в вашей сети, можно использовать Nmap для активного сканирования хоста. Nmap использует информацию, которую он получает из просмотра для оценки возможных операционных систем. Это тогда использует операционную систему, которая имеет самую высокую оценку как идентификацию хостовой операционной системы.
- Создайте правило корреляции, что триггеры, когда система обнаружит хост с неизвестной операционной системой.
  Правило должно инициировать, когда **событие обнаружения имеет место**, и **информация об ОС для хоста изменилась**, и это отвечает следующим условиям: **Название ОС неизвестно**.

Большая база данных для хранения событий

- При увеличении предела события database вне рекомендации или оптимального метода в Центре управления FireSIGHT может закончиться дисковое пространство.

Шаги по устранению неполадок

- Проверьте значения предела базы данных. Для улучшения использования диска и производительности необходимо адаптировать пределы события количеству событий, с которыми вы **регулярно** работаете. Для некоторых типов события можно отключить хранилище.
- Для изменения предела базы данных перейдите к странице System Policy, нажмите **Edit** рядом с названием системной политики, и затем нажмите **Database** на левом разделе. Для доступа к странице **System Policy** перейдите к **Системе> Локальный> Системная политика**.

Получите предупреждения состояния для более чем 85%-го использования диска

Возможные причины

- Скорость события может быть очень высокой. Поэтому устройство генерирует и хранит много событий.
- Проблемы связи между управляемым устройством и Центром управления FireSIGHT.

Шаги по устранению неполадок

- Изменение аварийного порогового уровня к 87% (Предупреждающим) и (Важным) 92%, может быть простым решением к частым предупреждениям состояния.
- Считайте Комментарии к выпуску, чтобы видеть, была ли известная неполадка с системой отсечения. Когда решение будет доступно, обновите версию программного обеспечения к последнему выпуску для решения этой проблемы.

/var/log/messages файлы содержат данные, более старые, чем 24 часа или больше, чем 25 МБ

Возможные причины

- Демон Logrotate может не работать должным образом.

Шаги по устранению неполадок

- При обнаружении с этой проблемой обновите версию программного обеспечения Систем FireSIGHT к последнему выпуску. Если вы выполняете последнюю версию, но все еще испытываете эту проблему, свяжитесь с Центром технической поддержки Cisco (TAC).

Если Root (/) Разделение Полон

Файлы пользователя Сохранены на Root (/) Разделение

Возможные причины

- Root `(/)` разделение является фиксированным размером и не предназначено для персонального хранилища.
- `/var/tmp` drectory используется вручную для временного хранилища вместо`/var/common` каталога.

Шаги по устранению неполадок

- Проверьте для ненужных файлов на `root/`, `/ домой`, и `/` папка `tmp`. Так как эти папки не созданы для персонального хранилища, можно удалить любой персональный файл с командой `rm`.

Неподдерживаемые Процессы Пишут в Root (/) Разделение

Возможные причины

- Если вы устанавливаете стороннее программное обеспечение, которое создает файлы на root `(/)` разделение, можно испытать предупреждение состояния для высокого использования диска.

Шаги по устранению неполадок

- Проверьте, установлены ли какие-либо неподдерживаемые пакеты. Выполните следующую команду для обнаружения установленных пакетов:

  ```
  admin@3DSystem:~$ rpm -qa --last
  ```
- Проверьте pstree и вершину, чтобы видеть, работают ли неподдерживаемые процессы. Выполните следующие команды:

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