# Fehlerbehebung bei übermäßiger Festplattenauslastung auf Sourcefire-Appliances

## Inhalt



## Einführung

Ein FireSIGHT Management Center oder eine FirePOWER-Appliance kann aus verschiedenen Gründen nicht über genügend Speicherplatz verfügen. In diesem Fall löst die hohe Festplattenauslastung eine Systemwarnung aus oder schlägt einen Softwareaktualisierungsversuch fehl. In diesem Artikel werden die Ursachen der übermäßigen Festplattenauslastung sowie einige Schritte zur Fehlerbehebung beschrieben.

## Überprüfungsschritte

Bestimmen Sie die Partition, die in hohem Maße genutzt wird. Der folgende Befehl zeigt die Festplattenauslastung:

In einem FireSIGHT Management Center

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

Auf Appliances der Serien 7000 und 8000 und auf virtuellen NGIPS-Geräten

```
> show disk
```

Beide Befehle zeigen eine Ausgabe wie folgt an:

```
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
```

**Hinweis**: Die Größe und Auslastung der Festplatte kann je nach Appliance-Modell variieren. Wenn es sich um ein virtuelles NGIPS-Gerät handelt, stellen Sie sicher, dass die Größe der Partitionen den Mindestspeicherplatzanforderungen entspricht.

**Vorsicht**: Jede zusätzliche Partition, die oben nicht dargestellt wird, wird nicht unterstützt.

Auf Appliances der Serien 7000 und 8000 sowie auf virtuellen NGIPS-Geräten können Sie den folgenden Befehl ausführen, um detaillierte Statistiken zur Festplattennutzung anzuzeigen:

```
> show disk-manager
```

Beispielausgabe:

```
> 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
```

# Wenn die /Volume-Partition voll ist

## Alte Sicherungsdateien

- Wenn Sie große Mengen alter Backup-Dateien auf dem System speichern, kann dies zu viel Speicherplatz auf Ihrer Festplatte erfordern.

### Schritte zur Fehlerbehebung

- Löschen Sie die alten Backup-Dateien über die Web-Benutzeroberfläche. Um Sicherungsdateien zu entfernen, navigieren Sie zu **System > Extras > Backup/Restore**.

  **Tipp**: Auf einem FireSIGHT-System können Sie Remote-Speicher konfigurieren, um die großen Sicherungsdateien zu speichern.

## Ältere Software-Update- und Patch-Dateien

- Wenn Sie immer die vorherigen Software-Update-, Upgrade- und Patch-Dateien (z. B. 5.0 oder 5.1) behalten, kann dem System der Speicherplatz ausgehen.

### Schritte zur Fehlerbehebung

- Löschen Sie die älteren Update- und Patch-Dateien, die nicht mehr benötigt werden. Um sie zu löschen, navigieren Sie zu **System > Updates**.

#### Übermäßige Ereignisdateien werden gespeichert

- Verwaltete Geräte oder Sensoren haben möglicherweise das Senden von Ereignissen an das FireSIGHT Management Center gestoppt.
- Ein Gerät generiert möglicherweise mehr Ereignisse als ein Management Center für den Empfang (pro Sekunde) entwickelt hat.
- Es kann ein Kommunikationsproblem zwischen dem verwalteten Gerät und dem Management Center geben.

### Schritte zur Fehlerbehebung

- Wenden Sie die Richtlinie für das Ereignis erneut an. Wenn Sie z. B. keine Verbindungsereignisse sehen, wenden Sie die Zugriffskontrollrichtlinie erneut an, und überprüfen Sie, ob neue Ereignisse jetzt vom Management Center empfangen werden.
- Wenn ein FireSIGHT Management Center keine neuen IPS-Ereignisse empfangen kann, prüfen Sie bitte, ob Kommunikationsprobleme zwischen dem verwalteten Gerät und dem Management Center vorliegen.

#### Übermäßige, unbekannte Dateien

- Das FireSIGHT-System speichert die **unbekannten** Netzwerkerkennungsdaten (Betriebssystem-, Host- und Serviceinformationen).

### Schritte zur Fehlerbehebung

- Wenn das System das Betriebssystem auf einem Host in Ihrem Netzwerk nicht bestimmen kann, können Sie den Host mithilfe von Nmap aktiv prüfen. Nmap nutzt die Informationen, die es vom Scan erhält, um die möglichen Betriebssysteme zu bewerten. Anschließend wird das Betriebssystem mit der höchsten Bewertung als Host-Betriebssystem-Identifikation verwendet.
- Erstellen Sie eine Korrelationsregel, die auslöst, wenn das System einen Host mit einem unbekannten Betriebssystem erkennt.
  Die Regel sollte ausgelöst werden, wenn **ein Erkennungsereignis auftritt** und **die Betriebssysteminformationen für einen Host geändert wurden** und die folgenden Bedingungen erfüllt sind: **Der BS-Name ist unbekannt**.

## Große Datenbank zum Speichern von Ereignissen

- Wenn Sie den Grenzwert für Datenbankereignisse über die Richtlinien oder Best Practices hinaus erhöhen, kann dem FireSIGHT Management Center der Speicherplatz ausgehen.

### Schritte zur Fehlerbehebung

- Überprüfen Sie die Werte des Datenbankgrenzwerts. Um die Festplattenauslastung und -

leistung zu verbessern, sollten Sie die Ereignisbegrenzungen an die Anzahl der Ereignisse anpassen, mit denen Sie **regelmäßig** arbeiten. Bei einigen Ereignistypen können Sie den Speicher deaktivieren.
- Um die Datenbankbeschränkung zu ändern, navigieren Sie zur Seite Systemrichtlinie, klicken Sie neben dem Namen der Systemrichtlinie auf **Bearbeiten**, und klicken Sie dann im linken Bereich auf **Datenbank**. Um auf die Seite **Systemrichtlinien** zuzugreifen, navigieren Sie zu **System > Local > System Policy (System > Lokal > Systemrichtlinie)**.

### Empfang von Systemwarnungen für mehr als 85 % Festplattenauslastung

#### Mögliche Gründe

- Die Ereignisrate kann sehr hoch sein. Daher generiert und speichert das Gerät viele Ereignisse.
- Kommunikationsprobleme zwischen dem verwalteten Gerät und dem FireSIGHT Management Center.

#### Schritte zur Fehlerbehebung

- Eine einfache Lösung für häufige Gesundheitswarnungen ist die Änderung des Alarmschwellenwerts auf 87 % (Warnung) und 92 % (Kritisch).
- Lesen Sie die Versionshinweise, um festzustellen, ob ein bekanntes Problem mit dem bereinigten System aufgetreten ist. Wenn eine Lösung verfügbar ist, aktualisieren Sie die Softwareversion auf die neueste Version, um dieses Problem zu beheben.

### Die /var/log/messages Dateien enthalten Daten, die älter als 24 Stunden oder größer als 25 MB sind

#### Mögliche Gründe

- Logrotate Daemon funktioniert möglicherweise nicht einwandfrei.

#### Schritte zur Fehlerbehebung

- Wenn dieses Problem auftritt, aktualisieren Sie bitte die Softwareversion Ihrer FireSIGHT-Systeme auf die neueste Version. Wenn Sie die neueste Version verwenden, dieses Problem jedoch weiterhin besteht, wenden Sie sich an das Cisco Technical Assistance Center (TAC).

## Wenn die Root-Partition ( / ) vollständig ist

### Benutzerdateien werden auf der Root-Partition ( / ) gespeichert.

#### Mögliche Gründe

- Die Root-Partition ( / ) ist eine feste Größe und nicht für den persönlichen Speicher bestimmt.
- Das /var/tmp-Verzeichnis wird anstelle des /var/common Verzeichnisses manuell für die temporäre Speicherung verwendet.

#### Schritte zur Fehlerbehebung

- Suchen Sie im Ordner /root, /home und /tmp nach unnötigen Dateien. Da diese Ordner nicht für den persönlichen Speicher erstellt werden, können Sie jede persönliche Datei mit dem Befehl rm löschen.

## Nicht unterstützte Prozesse schreiben in eine Root-Partition ( / ).

### Mögliche Gründe

- Wenn Sie Software von Drittanbietern installieren, die Dateien auf der Root-/ )-Partition erstellt, können Sie eine Systemwarnung für die hohe Festplattennutzung erhalten.

### Schritte zur Fehlerbehebung

- Überprüfen Sie, ob nicht unterstützte Pakete installiert sind. Führen Sie den folgenden Befehl aus, um die installierten Pakete zu finden:

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

- Überprüfen Sie pstream und top, ob nicht unterstützte Prozesse ausgeführt werden. Führen Sie die folgenden Befehle aus:

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

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