排除Sourcefire设备上磁盘使用率过高的故障

目录

[简介](#)
[验证步骤](#)
[如果/卷分区已满](#)
[旧备份文件](#)
[旧版软件更新和补丁文件](#)
[用于存储事件的大型数据库](#)
[接收超过85%磁盘利用率的运行状况警报](#)
[/var/log/messages文件包含的数据早于24小时或大于25MB](#)
[如果根(/)分区已满](#)
[用户文件保存在根(/)分区上](#)
[不支持的进程正在写入根(/)分区](#)

简介

FireSIGHT管理中心或FirePOWER设备可能因各种原因耗尽磁盘空间。发生这种情况时，高磁盘利用率会触发运行状况警报或可能导致软件更新尝试失败。本文介绍磁盘利用率过高的根本原因和一些故障排除步骤。

验证步骤

确定高度使用的分区。以下命令显示磁盘利用率：

在FireSIGHT管理中心，

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

在7000和8000系列设备以及NGIPS虚拟设备上，

```
> show disk
```

两个命令都显示如下输出：

```
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
```

注意：不同设备型号的磁盘大小和利用率可能不同。如果这是NGIPS虚拟设备，请验证分区的大小是否符合最低磁盘空间要求。

警告：不支持上面未显示的任何其他分区。

在7000和8000系列设备以及NGIPS虚拟设备上，您可以运行以下命令来显示详细的磁盘使用情况统计信息：

```
> show disk-manager
```

输出示例：

```
> 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
```

如果/卷分区已满

旧备份文件

- 如果在系统上存储大量旧备份文件，可能会占用磁盘上的太多空间。

故障排除步骤

- 使用Web用户界面删除旧备份文件。要删除备份文件，请导航至**System > Tools > Backup/Restore**。

  提示：在FireSIGHT系统上，您可以配置远程存储以存储大型备份文件。

旧版软件更新和补丁文件

- 如果始终保留之前的软件更新、升级和补丁文件（如5.0或5.1），系统可能会耗尽磁盘空间。

故障排除步骤

- 删除不再需要的旧更新和补丁文件。要删除它们，请导航至“系统”**>“更新”**。

存储过多事件文件

- 受管设备或传感器可能已停止向FireSIGHT管理中心发送事件。
- 设备可能生成的事件数量超过管理中心设计接收的事件数量（每秒）。
- 受管设备和管理中心之间可能存在通信问题。

故障排除步骤

- 重新应用与事件相关的策略。例如，如果您没有看到连接事件，请重新应用访问控制策略，并查看管理中心现在是否收到任何新事件。
- 如果FireSIGHT管理中心无法接收新的IPS事件，请检查受管设备和管理中心之间是否存在任何通信问题。

未知文件过多

- FireSIGHT系统存储未知**网络**发现数据（操作系统、主机和服务信息）。

故障排除步骤

- 如果系统无法确定网络上主机上的操作系统，则可以使用Nmap主动扫描主机。Nmap使用它从扫描获取的信息对可能的操作系统进行评级。然后，它使用具有最高评级的操作系统作为主机操作系统标识。
- 创建在系统检测到具有未知操作系统的主机时触发的关联规则。
  当发现事件发生**且主机的操**作**系统信息已更改且符**合以下条件时，应触发规则：**操作系统名称未知**。

用于存储事件的大型数据库

- 如果将数据库事件限制超出指南或最佳实践，则FireSIGHT管理中心可能会耗尽磁盘空间。

故障排除步骤

- 检查数据库限制的值。为了提高磁盘利用率和性能，您应根据您经常使用的事件数量来定**制事**件限制。对于某些事件类型，可以禁用存储。
- 要更改数据库限制，请导航至“系统策略”页，单击系统策略名称旁边的**编辑**，然后单击左部分**的**数据库。要访问“系**统策略**”页，请导航**至“系统”>“本地”>“系统策略**”。

接收超过85%磁盘利用率的运行状况警报

可能的原因

- 事件率可能非常高。因此，设备正在生成和存储大量事件。
- 受管设备与FireSIGHT管理中心之间的通信问题。

故障排除步骤

- 将警报阈值级别更改为87%（警告）和92%（严重）是解决频繁运行状况警报的简单方法。
- 阅读版本说明，查看修剪系统是否存在已知问题。当解决方案可用时，请将软件版本更新为最新版本以解决此问题。

/var/log/messages文件包含的数据早于24小时或大于25MB

可能的原因

- 定位守护程序可能无法正常工作。

故障排除步骤

- 如果遇到此问题，请将FireSIGHT系统的软件版本更新为最新版本。如果您运行的是最新版本，但仍遇到此问题，请联系思科技术支持中心(TAC)。

如果根(/)分区已满

用户文件保存在根(/)分区上

可能的原因

- 根(/)分区大小固定，不用于个人存储。
- /var/tmp目录手动用于临时存储，而不是/var/common目录。

故障排除步骤

- 检查/root、/home和/tmp文件夹上是否有不必要的文件。由于这些文件夹不是为个人存储创建的，因此您可以使用rm命令删除任何个人文件。

不支持的进程正在写入根(/)分区

可能的原因

- 如果安装了在根(/)分区上创建文件的第三方软件，则可能会遇到高磁盘使用率的运行状况警报。

故障排除步骤

- 检查是否安装了任何不支持的软件包。运行以下命令查找已安装的软件包：

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

- 检查pstree和top，查看不支持的进程是否正在运行。运行以下命令：

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

admin@3DSystem:~$ top
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。