排除故障在Sourcefire伊莱克斯的额外的磁盘利用率

目录

简介

FireSIGHT管理中心或FirePOWER设备能由于多种原因用尽磁盘空间。当发生时，高磁盘利用率触发健康警报或可能发生故障软件更新尝试。此条款描述额外的磁盘利用率和一些故障排除步骤的根本原因。

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系列设备上和在NGIPS虚拟设备，

```
> show disk
```

输出如下喜欢的两show命令：

```
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：磁盘大小和利用率在多种设备型号能变化。如果这是NGIPS虚拟设备，请验证分区的

大小服从最低的磁盘空间需求。

警告：没有显示如上的所有其他分区不支持的。

在7000和8000系列设备上和在NGIPS虚拟设备，您能运行以下命令显示详细的磁盘使用情况统计信息：

```
> show disk-manager
```

一示例输出：

```
> 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/Volume分区全双工

旧有备份文件

- 如果存储大容量在系统的旧有备份文件，能采取在您的磁盘的额外的空间。

故障排除步骤

- 使用网页用户界面，删除旧有备份文件。为了删除备份文件，请导航对**系统> Tools>备份/恢复**。

  提示：在FireSIGHT系统上，您能配置遥控储存存储大备份文件。

更旧的软件更新和补丁文件

- 如果总是保持上一个软件更新、升级和补丁文件(例如， 5.0或者5.1)，系统能用尽磁盘空间。

故障排除步骤

- 删除不再是必要的更旧的更新和补丁文件。为了删除他们，请导航对**系统>更新**。

额外的事件文件存储

- 受管理设备或传感器也许已经停止发送事件到FireSIGHT管理中心。
- 设备比管理中心设计接收可能生成更多事件(每秒)。

- 也许有在受管理设备和管理中心之间的一个通信问题。

故障排除步骤

- 重新应用与事件涉及的策略。例如，如果看不到连接事件，请重新应用访问Controil策略并且检查其中任一新建的事件是否由管理中心当前接收。
- 如果FireSIGHT管理中心无法接收新建的IPS事件，请检查是否有在受管理设备和管理中心之间的任何通信问题。

额外的未知文件

- FireSIGHT系统存储发现号数据(OS、主机和服务信息)。

故障排除步骤

- 如果系统不能确定在一台主机的操作系统在您的网络，您能使用Nmap积极地扫描主机。从扫描获取对可能的操作系统估计的Nmap使用信息。它然后使用有最高的速率作为主机操作系统识别的操作系统。
- 当系统检测一台主机用一个未知操作系统时，请创建关联规则触发。
  规则应该触发，当**发现事件发生时，**并且**主机的OS信息更改，**并且符合以下条件：**OS名称未知**。

存储事件的大数据库

- 如果增加在指南或最佳实践之外的数据库事件限制， FireSIGHT管理中心能用尽磁盘空间。

故障排除步骤

- 检查数据库限制的值。要改进磁盘利用率和性能，您应该为事件限额专门制作您**有规律地**工作与事件的数量。对于一些事件类型，您能禁用存储设备。
- 为了更改数据库限制，请导航对系统策略页，单击在系统策略的名称旁边**编辑**，然后单击在左侧部分的**数据库**。要访问**系统策略**页，请导航到**系统>本地>System策略**。

收到经过85%磁盘利用率的健康警报

可能的原因

- 事件速率可能非常高。所以设备是生成和存储大量事件。
- 在受管理设备和FireSIGHT管理中心之间的通信问题。

故障排除步骤

- 更改提醒的阈值范围到87% (警告)和92% (关键)可以是常去健康警报的简单解决方案。
- 读版本注释发现是否有一个已知问题用修剪系统。当解决方案是可用的时，请更新软件版本对新版本解决此问题。

/var/log/messages文件大于25MB包含数据旧比24个小时或者

可能的原因

- Logrotate守护程序可能不是工作正常。

故障排除步骤

- 如果遇到此问题，请更新您的FireSIGHT系统软件版本对新版本。如果运行新版本，但是仍然遇到此问题，请与Cisco技术支持中心(TAC)联系。

如果根(/)分区全双工

用户文件在根(/)分区保存

可能的原因

- 根(/)分区是固定大小和没有供个人存储设备使用。
- drectory的/var/tmp手工使用临时存储，而不是/var/common目录。

故障排除步骤

- 检查在/root、/home和/tmp文件夹的多余的文件。因为这些文件夹没有为个人存储设备创建，您能删除所有个人档案用rm命令。

不支持的进程写入根源(/)分区

可能的原因

- 如果安装创建在根的第三方软件(/)分区的文件，您能体验高磁盘使用情况的健康警报。

故障排除步骤

- 检查任何不支持的包是否安装。运行以下命令查找安装的程序包：

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

- 检查pstree并且冠上发现不支持的进程是否运行。运行以下命令：

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