排除Sourcefire裝置上磁碟使用率過高的故障

目錄

簡介

FireSIGHT管理中心或FirePOWER裝置可能由於各種原因而耗盡磁碟空間。發生這種情況時，高磁碟利用率會觸發運行狀況警報，或者可能導致軟體更新嘗試失敗。本文介紹了磁碟利用率過高的根本原因和一些故障排除步驟。

驗證步驟

確定高度使用的分割槽。以下命令顯示磁碟利用率：

在FireSIGHT管理中心，

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

在7000和8000系列裝置和NGIPS虛擬裝置上，

```
> show disk
```

兩個命令都顯示如下所示的輸出：

```
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
```

附註：磁碟大小和使用率因各種裝置型號而異。如果這是NGIPS虛擬裝置，請驗證分割槽大小是否符合最小磁碟空間要求。

注意：不支援上面未顯示的任何其他分割槽。

在7000和8000系列裝置以及NGIPS虛擬裝置上，可以運行以下命令來顯示詳細的磁碟使用情況統計資訊：

```
> show disk-manager
```

輸出示例：

```
> 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/Volume分割槽已滿

舊備份檔案

- 如果在系統上儲存大量舊備份檔案，則可能會佔用磁碟上的過多空間。

疑難排解步驟

- 使用Web使用者介面刪除舊的備份檔案。若要移除備份檔案，請導覽至**System > Tools > Backup/Restore**。

  提示：在FireSIGHT系統上，可以配置遠端儲存以儲存大型備份檔案。

舊版軟體更新和修補檔案

- 如果您始終保留以前的軟體更新、升級和修補程式檔案（例如5.0或5.1），則系統可能會耗盡磁碟空間。

疑難排解步驟

- 刪除不再需要的舊更新和修補程式檔案。若要刪除這些更新，請導覽至**System > Updates**。

儲存了過多的事件檔案

- 受管裝置或感測器可能已停止向FireSIGHT管理中心傳送事件。
- 裝置可能正在生成的事件數超過管理中心設計接收事件的數量（每秒）。
- 受管裝置和管理中心之間可能存在通訊問題。

疑難排解步驟

- 重新應用與事件相關的策略。例如，如果您沒有看到連線事件，請重新應用訪問控制策略，並檢視管理中心現在是否正在接收任何新事件。
- 如果FireSIGHT管理中心無法接收新的IPS事件，請檢查受管裝置和管理中心之間是否存在任何通訊問題。

未知檔案過多

- FireSIGHT系統儲存未知**網**絡發現資料（作業系統、主機和服務資訊）。

疑難排解步驟

- 如果系統無法確定網路上的主機上的作業系統，則可以使用Nmap主動掃描主機。Nmap使用從掃描獲取的資訊為可能的作業系統評分。然後，它使用具有最高評級的作業系統作為主機作業系統標識。
- 建立在系統檢測到具有未知作業系統的主機時觸發的關聯規則。
  當發現事件發**生且主機的**OS信**息已更改並且滿足以下條件**時，應觸發規則：**作業系統名稱未知**。

要儲存事件的大型資料庫

- 如果將資料庫事件限制提高到超出准則或最佳實踐的範圍，則FireSIGHT管理中心可能耗盡磁碟空間。

疑難排解步驟

- 檢查資料庫限制的值。為了提高磁碟利用率和效能，您應該對定期處理的事件的數量制**定事**件限制。對於某些事件型別，您可以禁用儲存。
- 要更改資料庫限制，請導航到「系統策略」頁，按一下系統策略名稱旁邊的**編輯**，然後按一下左側部分的**資料庫**。要訪問System Policy頁面，請導航到System > Local > System Policy。

接收超過85%磁碟利用率的運行狀況警報

可能的原因

- 事件速率可能非常高。因此，該裝置正在生成和儲存大量事件。
- 受管裝置和FireSIGHT管理中心之間的通訊問題。

疑難排解步驟

- 將警報閾值級別更改為87%（警告）和92%（嚴重）可能是解決頻繁出現健康警報的簡單方法。
- 閱讀發行說明，瞭解修剪系統是否存在已知問題。如果有解決方案，請將軟體版本更新為最新版本以解決此問題。

/var/log/messages檔案包含的資料超過24小時或大於25MB

可能的原因

- Logrotate守護程式可能無法正常工作。

疑難排解步驟

- 如果您遇到此問題，請將FireSIGHT系統的軟體版本更新為最新版本。如果您正在運行最新版本，但遇到此問題，請聯絡思科技術協助中心(TAC)。

如果根(/)分割槽已滿

使用者檔案儲存在根(/)分割槽中

可能的原因

- 根(/)分割槽是固定大小，不適用於個人儲存。
- /var/tmp目錄手動用於臨時儲存，而不是/var/common目錄。

疑難排解步驟

- 檢查/root、 /home和/tmp資料夾中是否存在不需要的檔案。由於這些資料夾不是為個人儲存建立的，因此您可以使用rm命令刪除任何個人檔案。

不支援的進程正在寫入根(/)分割槽

可能的原因

- 如果安裝第三方軟體，在根(/)分割槽上建立檔案，則可以遇到高磁碟使用率的運行狀況警報。

疑難排解步驟

- 檢查是否安裝了任何不受支援的軟體包。運行以下命令查詢已安裝的軟體包：

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

- 檢查pstree和top以檢視不受支援的進程是否正在運行。運行以下命令：

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

admin@3DSystem:~$ top
```