安全防火牆FTD高記憶體（由於高訪問清單元素計數）

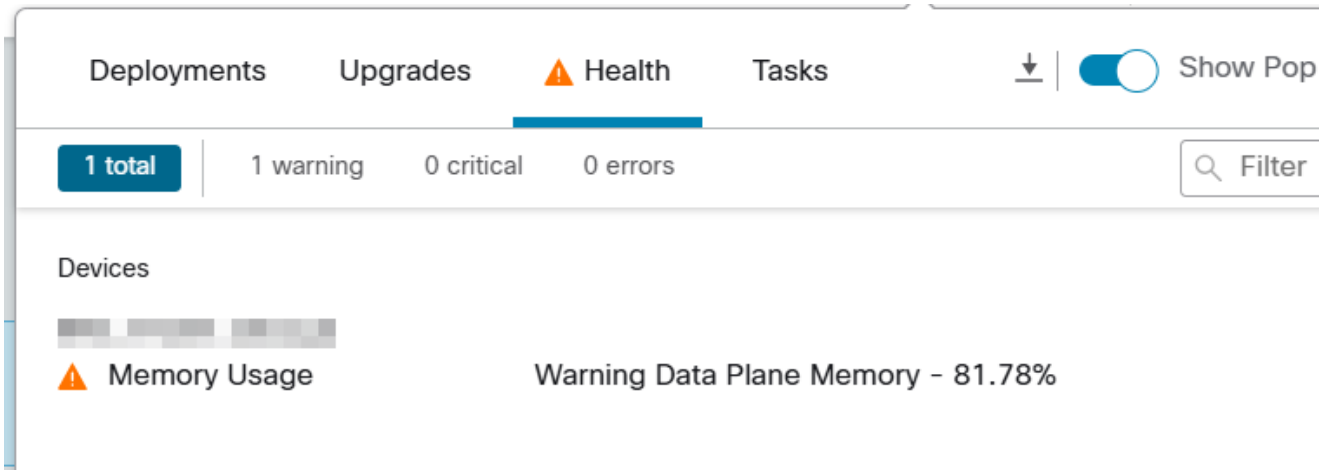
目錄

問題

FTD顯示資料平面記憶體利用率持續高且超過80%的警報。在策略部署後，記憶體利用率仍保持在這個較高的水準，因為策略部署顯著增加了訪問清單元素計數，其數量多於平台可以容納的數量。

在FTD高可用性組態中，問題會影響兩個裝置，但會在作用中FTD上顯示更高的記憶體使用率。

- FMC警報顯示FTD資料平面上的高記憶體使用率：



- FTD CLI也會確認記憶體使用率高：

```
<#root>

firepower# show memory
Free memory:        2590897856 bytes (18%)
Used memory:       11746269504 bytes (82%)

-------------      ------------------
Total memory:      14337167360 bytes (100%)
```

- access-list element count在FTD CLI中顯示100萬或更多元素：

  <#root>

  ```
  firepower# show access-list element-count

  Total number of access-list elements: 3223691
  ```

- 在FTD的FMC健康狀況監控圖中，與ACE部署相關的記憶體急劇增加：



- 在高可用性對等FTD上，記憶體使用可能會因為未清除記憶體而停滯在高水準上：

  <#root>

  ```
  firepower# failover exec standby show memory
  Free memory:        3278441368 bytes (23%)

  Used memory:       11058725992 bytes (77%)


  -------------      ------------------
  Total memory:      14337167360 bytes (100%)
  ```

環境

- 高可用性配置中的Cisco Firepower 2130威脅防禦
- FTD軟體版本：7.4.2
- FMC軟體版本：7.6.2
- 高訪問清單元素數量接近一百萬或更多

解析

1.在FTD高可用性配置中，在預先計畫的時間重新啟動對等FTD，以清除以前可能已累積的保留記憶體儲存。

2.重新啟動後，請確認：

- 對等FTD會正確重新同步到高可用性對。
- 記憶體利用率顯示正常水準。
- FTD記憶體警報從FMC UI中清除。

3.導覽至Devices > Device Management，然後點選FTD的Edit圖示。

4.按一下左上角附近的Device頁籤(FTD HA的Summary頁籤)，向下滾動到Advanced Settings部分，然後按一下Edit圖示。

5.選中對象組搜尋覈取方塊以啟用此功能，然後按一下儲存。

6.將組態變更部署到FTD HA配對，並監控健康狀況監控器數分鐘，以觀察記憶體使用情況的變更。

<#root>

```
firepower# show memory
Free memory:        6948343576 bytes (48%)

Used memory:        7388823784 bytes (52%)


-------------     --------------------------
Total memory:      14337167360 bytes (100%)
```

其他考量事項

如果即使啟用對象組搜尋後，記憶體利用率也會成為持續效能問題，請考慮以下最佳化策略：

- 使用FMC連線事件檢視熱門命中計數規則。
- 減少對大量受信任流量進行不必要的檢查。
- 評估是否所有規則都需要入侵檢測。
- 考慮將平台升級到更高容量的Firepower平台（FPR4K或FPR9K系列）。

原因

資料平面記憶體使用率高是由於FTD上的保留記憶體和原則部署後存取清單元件處理額外負荷的增加所導致。重要訪問清單元素計數與記憶體利用率高峰直接相關。在不進行對象組搜尋最佳化的情況下，顯著增加的ACL處理要求有助於保持較高的記憶體利用率。

相關內容

- 使用FMC CLI計算存取清單元件(ACE)計數
- 思科安全防火牆管理中心裝置配置指南7.4:訪問控制規則的最佳實踐
- 思科安全防火牆管理中心裝置配置指南7.4:配置對象組搜尋
- Firepower威脅防禦的命令參考
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。