來自Pruner.pl進程的FTD高CPU核心警報

問題

FMC會為多個受管FTD裝置頻繁產生高CPU使用率警報，並引發對防火牆效能和穩定性的擔憂。具體來說，FMC運行狀況監視器顯示特定核心在較長時間內重複出現CPU核心峰值，內部Pruner.pl後台進程持續佔用指定核心的過量CPU。儘管這些重要CPU警報出現在FMC中，但並未觀察到使用者可見的流量影響，總體FTD穩定性仍不受影響。

環境

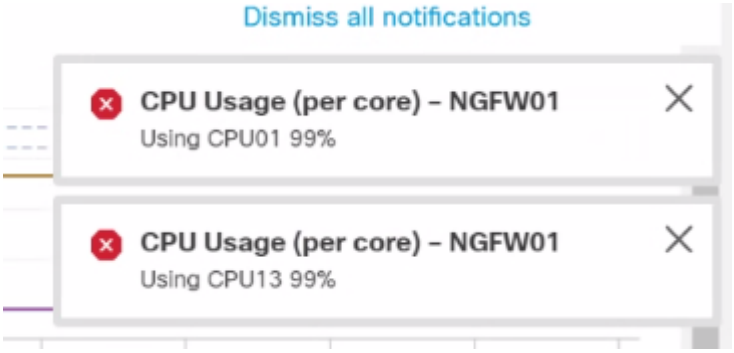
- FTD軟體版本：7.2.5（影響所有低於7.2.6版本的虛擬和硬體型號）
- 由Firepower管理中心(FMC)管理的裝置

解析

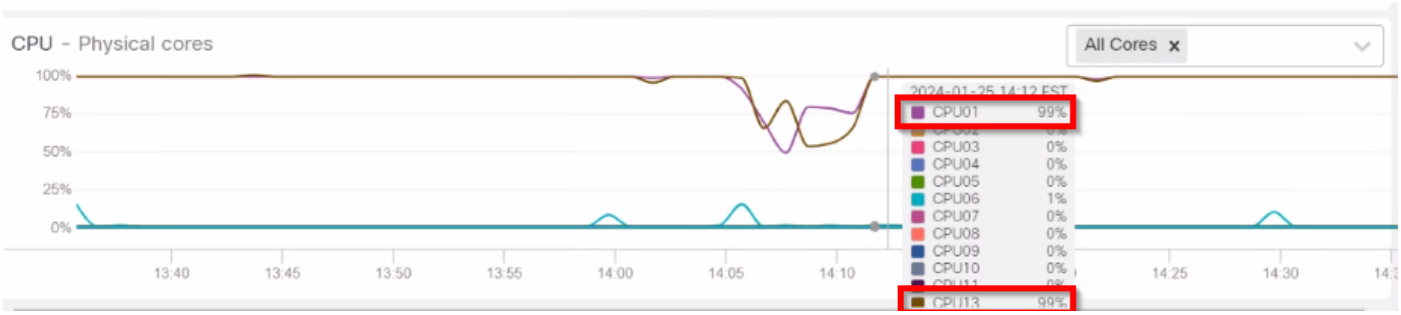
解決方法涉及將受影響的FTD裝置升級為包含已識別缺陷的修復程式的軟體版本。

故障排除和分析步驟

1:檢查FTD健康監控圖表中隨時間變化的CPU使用模式，以確定問題的範圍和時間。分析顯示特定核心上出現重複的CPU核心峰值，而總體CPU和記憶體利用率仍保持在正常運行範圍內。



inline_image_0.png



inline_image_1.png

```
Health Monitor Alert | Time: Mon Jul 24 06:34:20 2023 UTC | Severity: critical | Module: CPU Usage (per
Health Monitor Alert | Time: Mon Jul 24 04:24:20 2023 UTC | Severity: critical | Module: CPU Usage (per
```

2:分析FTD CLI並對來自受影響的FTD的套件組合進行疑難排解，以確定CPU使用率較高的根本原因。

3:檢視收集的資料，確定哪些進程正在佔用過多的CPU資源。對top.log檔案的分析確認Pruner.pl進程在某些核心上持續使用高CPU，而問題模式則從某個特定的時間範圍開始。

```
root@FTDdevice:/home/admin# cd /ngfw/var/log/
root@FTDdevice:/ngfw/var/log# grep "Pruner.pl --persistent" top.log | grep -v "S   0.0"
 12341 root      20   0  458920 437816  10056 R 100.0   0.2   9452:10 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9453:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9454:13 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R  94.1   0.2   9455:15 /usr/bin/perl /ngfw/usr/local/sf/
 12341 root      20   0  437124 416148  10056 R 100.0   0.2   9456:18 /usr/bin/perl /ngfw/usr/local/sf/
```

日誌還顯示大量空、0位元組「*snort-unified.log」檔案，這是導致Pruner.pl如此頻繁運行的主要原因。

```
root@FTDdevice:/home/admin# cd /ngfw/var/sf/detection_engines/FTD-UUID/
root@FTDdevice:/ngfw/var/sf/detection_engines/FTD-UUID# ls -l instance-* | grep -ri "root        0.snor
-rw-r--r--  1 root    root        0 Nov 12 19:47 snort-unified.log.1699818430
-rw-r--r--  1 root    root        0 Nov 12 19:41 snort-unified.log.1699818093
-rw-r--r--  1 root    root        0 Nov 12 19:35 snort-unified.log.1699817758
-rw-r--r--  1 root    root        0 Nov 12 17:13 snort-unified.log.1699809226
-rw-r--r--  1 root    root        0 Nov 12 17:08 snort-unified.log.1699808890
-rw-r--r--  1 root    root        0 Nov 12 17:02 snort-unified.log.1699808554
```

軟體升級解決方案

1:將所有受影響的FTD裝置升級為包含CSCwh79095修復程式的軟體版本。建議的最低版本為：

- FTD 7.2.7（7.2.x系列中的最低修復版本）
- FTD 7.4.1或更高版本（推薦的升級路徑）

2:升級後，監控FMC運行狀況警報以確認：

- 每核CPU利用率保持穩定
- 沒有針對Pruner.pl或類似後台進程發出新的嚴重警報
- 不再發生Pruner.pl進程的高CPU警報

預防和最佳做法

落實以下建議，防止出現類似問題：

- 避免運行較舊的代碼培訓長期並計畫定期升級到建議版本，以從錯誤修復和安全更新中受益
- 進行重大升級之前，請檢視思科版本說明，並在當前版本和目標版本上執行錯誤搜尋，瞭解已知缺陷
- 升級後繼續監控FMC運行狀況警報，以確保系統穩定性
- 檢視版本說明中記錄的所有特殊升級注意事項

原因

高CPU警報是由FTD 7.2.5中一個被識別為Cisco錯誤ID CSCwh79095的軟體缺陷造成的。此缺陷是由於空的0位元組snort-unified.log檔案導致內部Pruner.pl後台進程佔用特定核心上的過量CPU。這將在FMC中觸發持續的高CPU警報。重要的是，這種情況不影響資料平面流量轉發或裝置整體穩定性；它僅在管理介面中生成關鍵CPU警報。此問題與重複錯誤相關，包括CSCwe66384（Pruner.pl和磁碟管理器高CPU，沒有明顯的磁碟問題）和CSCwf80946(FTD:使用過多的系統CPU核心並生成FMC HM警報的修剪器進程)。

相關內容

- Cisco錯誤ID CSCwh79095 - Snort生成過多的零位元組的snort統一日誌檔案(已在以下位置修復：7.2.7、7.4.1、7.6.0)
- Cisco錯誤ID CSCwf77994 — 針對運行瞬時高使用率的FTD裝置系統核心的虛假嚴重CPU高CPU警報(已在下列中修正：7.2.9、7.4.1、7.6.0)
- FTD/FMC版本說明和推薦版本文檔
- 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）。