

分析高CPU的AMP診斷套件

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[疑難排解](#)

[驗證電腦上是否安裝了另一個防病毒軟體](#)

[確定在使用特定應用程式時是否發生高CPU](#)

[收集診斷套件進行分析](#)

[啟用調試日誌級別](#)

[終結點中的調試級別](#)

[策略中的調試級別](#)

[重現問題並收集診斷捆綁包](#)

[進行分析](#)

[Diag_Analyzer.exe](#)

[Amphandlecount.ps1](#)

[調整排除](#)

[將套件組合提交給TAC進行分析](#)

簡介

本文檔介紹從Windows裝置上的終端公共雲高級惡意軟體防護(AMP)分析診斷捆綁包以對高CPU使用率進行故障排除的步驟。

作者：Luis Velazquez，編輯者：Yeraldin Sánchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- [訪問AMP控制檯](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於終端的AMP主控台5.4.20200204
- Windows作業系統裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

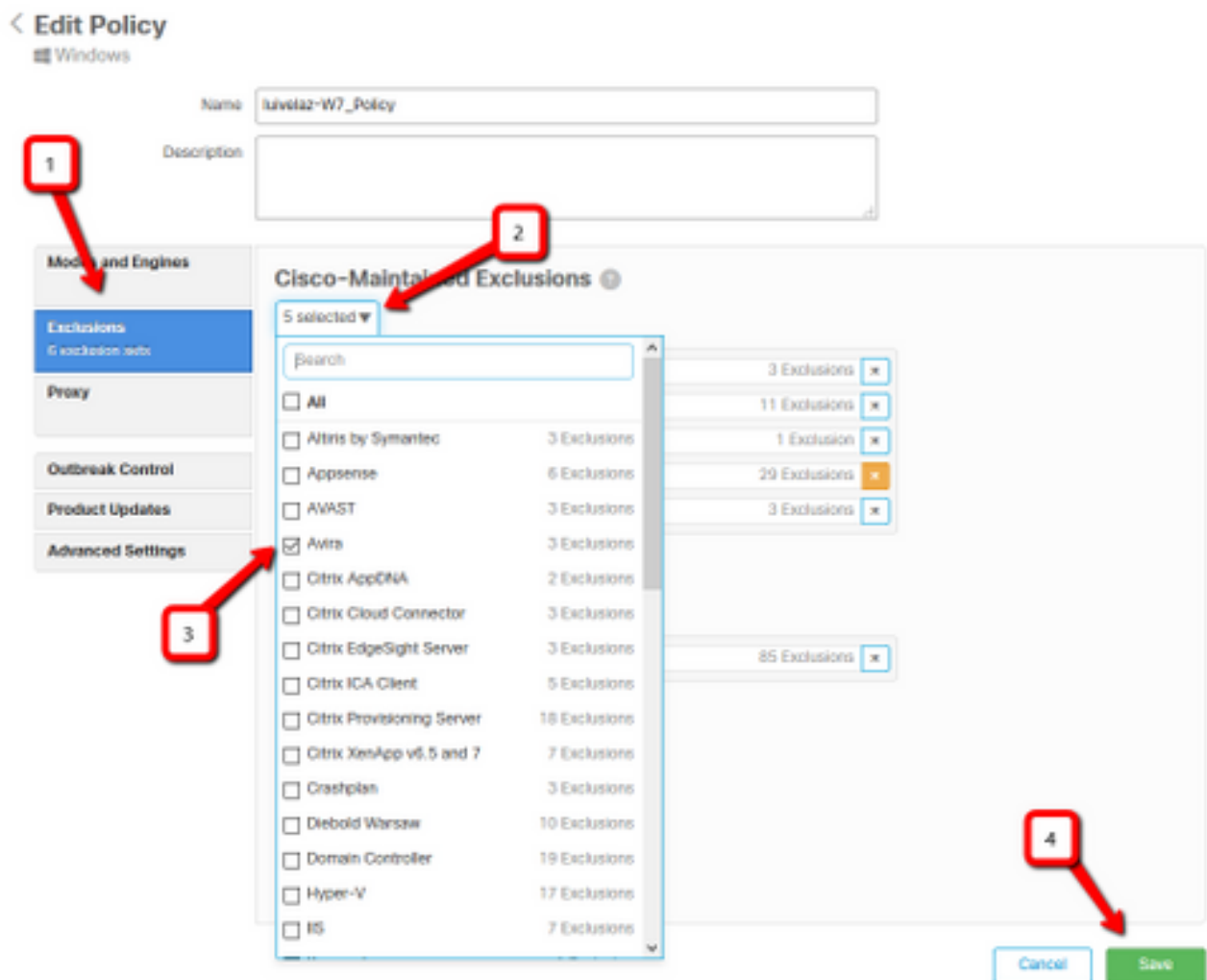
驗證電腦上是否安裝了另一個防病毒軟體

如果安裝了另一個AV (防病毒) ，請確保在策略配置中排除AV的主進程

提示：如果使用的軟體包含在清單中，則使用思科維護的排除項。請記住，這些排除項可以新增到應用程式的新版本中。

若要檢視Cisco維護的排除區段中可用的清單，請導覽至**Management > Policies > Edit > Exclusions > Cisco維護的排除區**。

根據電腦上當前安裝的軟體，選擇終端需要使用的策略，然後儲存策略，如下圖所示。



確定在使用特定應用程式時是否發生高CPU

確定在執行一個或幾個應用程式時問題是否發生 (如果您能夠複製此問題) ，將有助於確定潛在的例外情況。

收集診斷套件進行分析

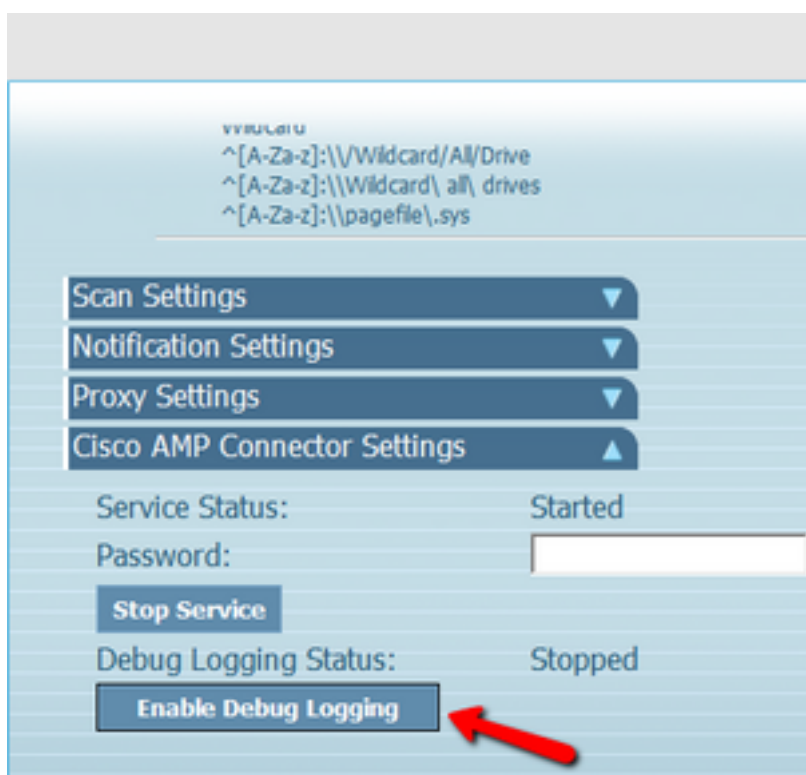
啟用調試日誌級別

為了收集有用的診斷捆綁包，必須啟用調試日誌級別。

終結點中的調試級別

如果您可以複製問題並訪問終端，則下面是捕獲診斷捆綁包的最佳步驟：

1. 開啟AMP GUI
2. 導航到**設定**
3. 滾動到AMP GUI底部，然後開啟**Cisco AMP聯結器設定**
4. 按一下**Enable Debug Logging**
5. **調試日誌記錄狀態**必須更改為**已啟動**。此過程將啟用調試級別，直到下一個策略檢測訊號（預設值為15分鐘）



策略中的調試級別

如果您無權訪問終結點或無法一致重現問題，則必須在策略中啟用調試日誌級別。

若要按原則啟用偵錯日誌級別，請導覽至Management > Policies > Edit > Advanced Settings > Connector **Log Level** and Management > Policies > Edit > Advanced Settings > Tray Log Level，然後選擇Debug並儲存策略，如下圖所示。

< Edit Policy

Windows

Name: Iulvclaz-W7_Policy

Description:

The screenshot shows the 'Edit Policy' window for 'Iulvclaz-W7_Policy'. The 'Advanced Settings' section is expanded, showing various configuration options. Two red boxes with arrows point to the 'Heartbeat Interval' and 'Connector Log Level' settings. The 'Heartbeat Interval' is set to '15 minutes' and the 'Connector Log Level' is set to 'Debug'. Other settings include 'Send User Name in Events', 'Send Filename and Path Info', 'Enable Connector Protection', 'Automated Crash Dump Uploads', 'Command Line Capture', and 'Command Line Logging'. The 'Connector Protection Password' field is masked with asterisks. The 'Cancel' and 'Save' buttons are visible at the bottom right.

注意：如果從策略啟用調試模式，則所有終端都會收到此更改。

附註：同步終結點的策略以確保應用調試級別或等待心跳間隔（預設情況下為15分鐘）。

重現問題並收集診斷捆綁包

當配置調試級別時，請等待系統發生「高CPU」狀態或手動重現之前確定的條件，然後收集診斷捆綁包。

若要收集套件組合，請導覽至C:\Program Files\Cisco\AMP\X.X.X（其中X.X.X是系統上安裝的最新AMP版本），然後執行應用程式ipsupporttool.exe，此程式會在名為CiscoAMP_Support_Tool_%date%.7z的案頭上建立.7z檔案

附註：連結器版本6.2.3及更高版本可以遠端請求捆綁包，導航到**管理>電腦**，展開終端記錄並使用Diagnose選項。

附註：診斷套件組合也可以透過以下命令在CMD提示中執行："C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe"或"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\Can\Get\To"，其中X.X.X是安裝的最新AMP版本，可以使用第二個命令來選擇。7z檔案的輸出資料夾。

進行分析

分析診斷檔案的方法有兩種：

- Diag_Analyzer.exe
- Amphandlecount.ps1

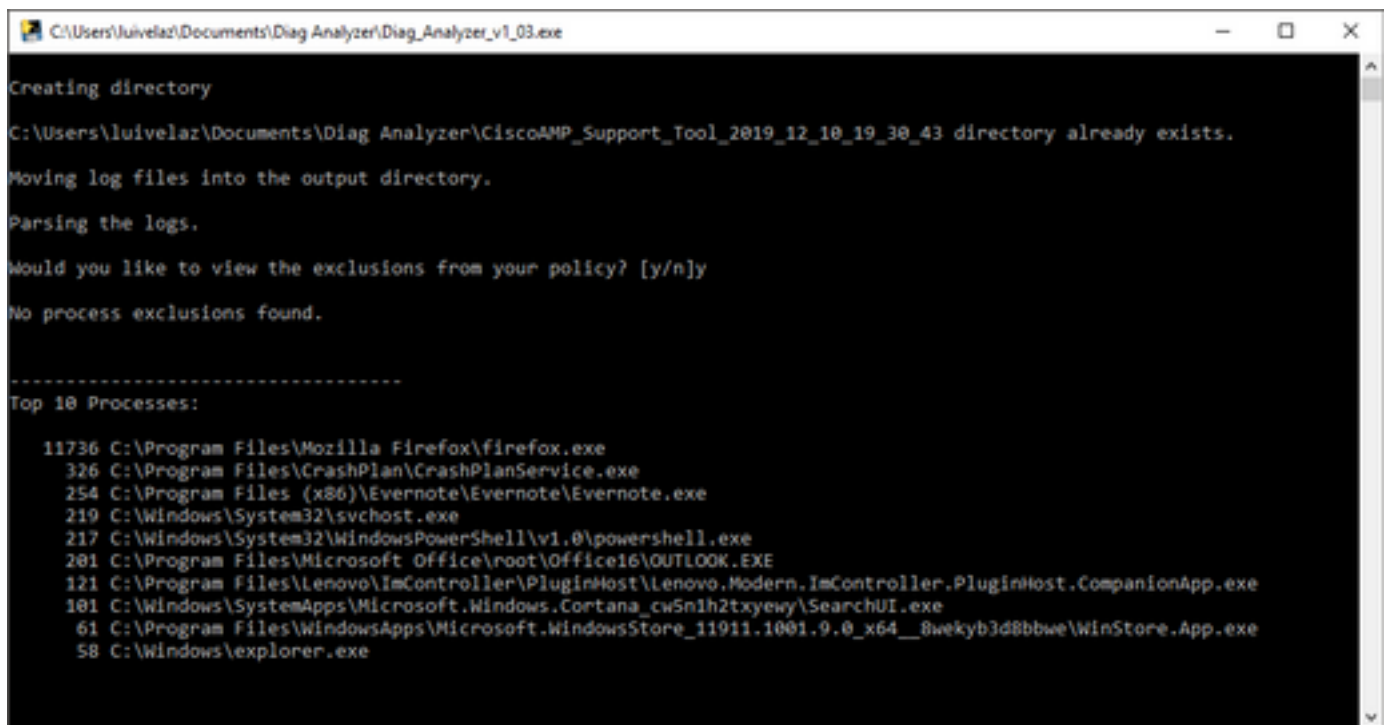
Diag_Analyzer.exe

步驟1.在此處下載應用[程式](#)。

步驟2.在GitHub頁面中，有一個自述檔案，其中包含使用方法的進一步說明。

步驟3.將CiscoAMP_Support_Tool_%date%.7z診斷檔案複製到Diag_Analyzer.exe所在的同一資料夾中。

步驟4.執行應用程式 Diag_Analyzer.exe。



```
C:\Users\luivelaz\Documents\Diag Analyzer\Diag_Analyzer_v1_03.exe
Creating directory
C:\Users\luivelaz\Documents\Diag Analyzer\CiscoAMP_Support_Tool_2019_12_10_19_30_43 directory already exists.
Moving log files into the output directory.
Parsing the logs.
Would you like to view the exclusions from your policy? [y/n]y
No process exclusions found.
-----
Top 10 Processes:
11736 C:\Program Files\Mozilla Firefox\firefox.exe
326 C:\Program Files\CrashPlan\CrashPlanService.exe
254 C:\Program Files (x86)\Evernote\Evernote\Evernote.exe
219 C:\Windows\System32\svchost.exe
217 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
201 C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
121 C:\Program Files\Lenovo\ImController\PluginHost\Lenovo.Modern.ImController.PluginHost.CompanionApp.exe
101 C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
61 C:\Program Files\WindowsApps\Microsoft.WindowsStore_11911.1001.9.0_x64__8wekyb3d8bbwe\WinStore.App.exe
58 C:\Windows\explorer.exe
```

步驟5.在新提示符中，確認是否要使用Y或N獲取策略中的排除項。

步驟6.指令碼結果包含：

- 前10個流程
- 前10個檔案
- 前10個擴展
- 前100個路徑
- 所有檔案

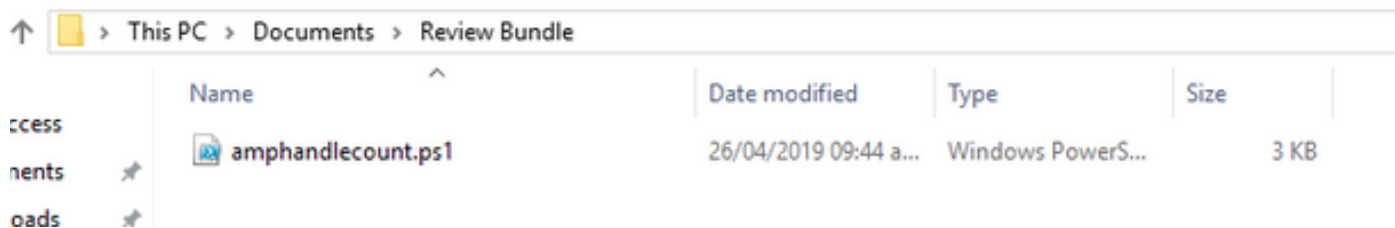
附註： Diag_Analyzer.exe會檢查所提供的AMP診斷檔案中的sfc.exe.log檔案。然後，使用診斷檔名建立一個新目錄，並將日誌檔案儲存在。7z之外，儲存在診斷的父目錄中，在此之後，它將分析日誌並確定前10個進程、檔案、副檔名和路徑，最後，它會將資訊列印到螢幕上，並將資訊列印到{Diagnostic}-summary.txt檔案中。

Amphandlecount.ps1

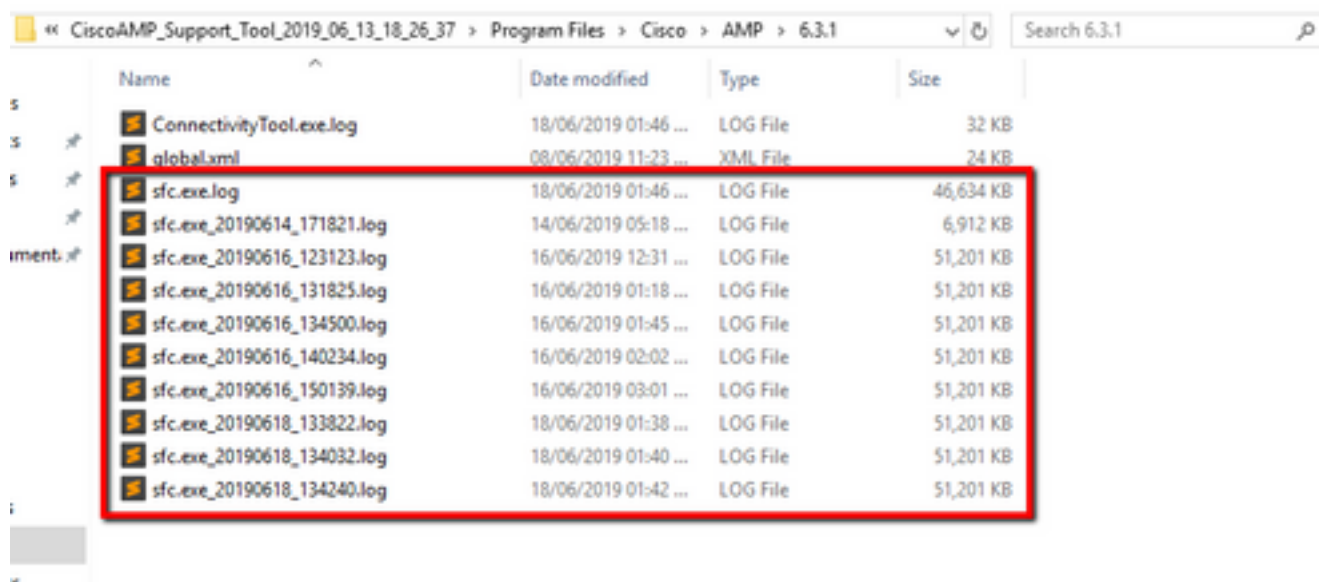
步驟1.從[Review Scanned Files from AMP](#)的社群底部下載指令碼amphandlecounts.txt。

步驟2.要在Windows中運行指令碼，請將其重新命名為amphandlecount.ps1。

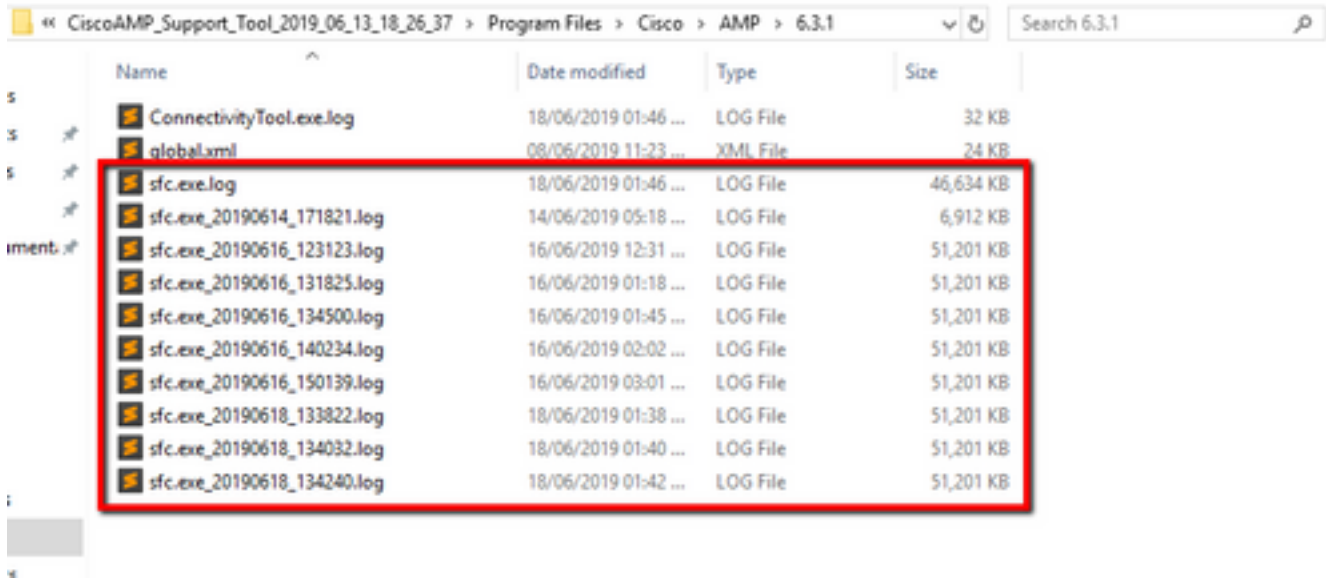
步驟3.為方便起見，將amphandlecount.ps1檔案複製到他自己的資料夾中。



步驟4.解壓縮CiscoAMP_Support_Tool_%date%.7z檔案，並識別路徑上的sfc.log檔案
CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X。



步驟5.將sfc.log的檔案複製到amphandlecount.ps1檔案夾。



步驟6.使用PowerShell運行amphandlecount.ps1，然後開啟一個視窗，根據終端上的執行策略可以請求運行許可權。

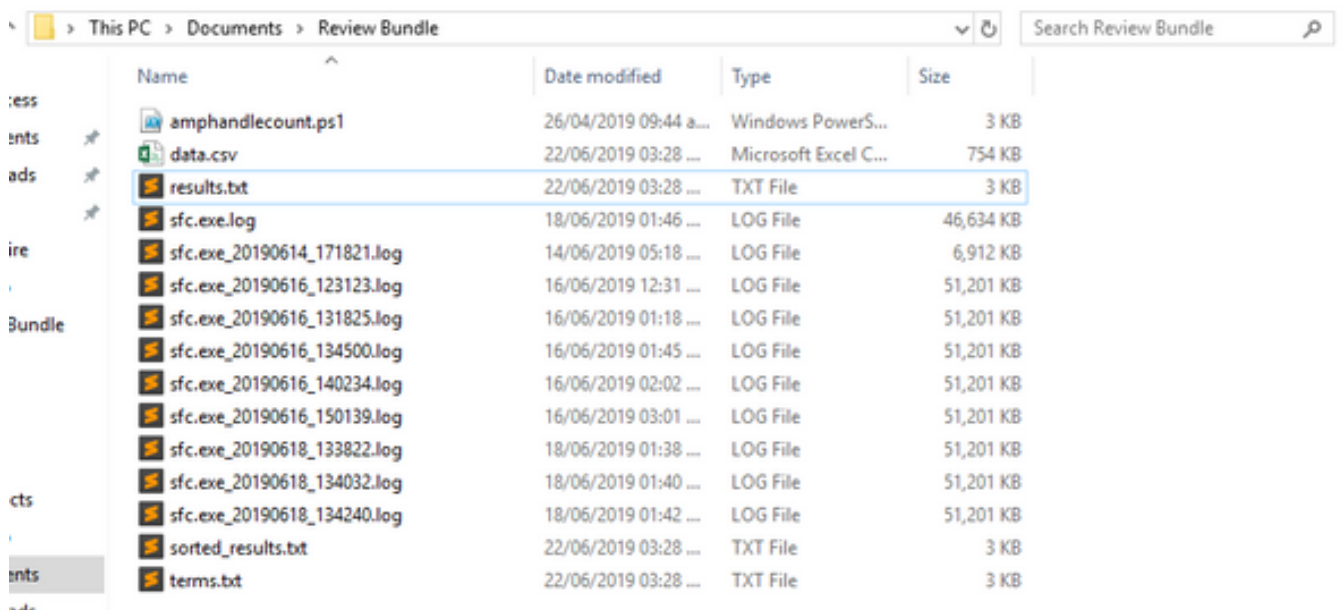
提示：要更改執行策略，請開啟Windows PowerShell並使用以下命令：

將策略設定為允許不受限制的執行訪問 — **Set-ExecutionPolicy -Scope CurrentUser - ExecutionPolicy Unrestricted**

設定策略以限制執行訪問 — **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

步驟7.完成PowerShell後（可能需要一些時間，具體取決於資料夾中的sfc.log數量），將在資料夾上建立四個檔案：

- data.csv
- results.txt
- sorted_results.txt
- terms.txt



步驟8.這4個新檔案包含分析結果：

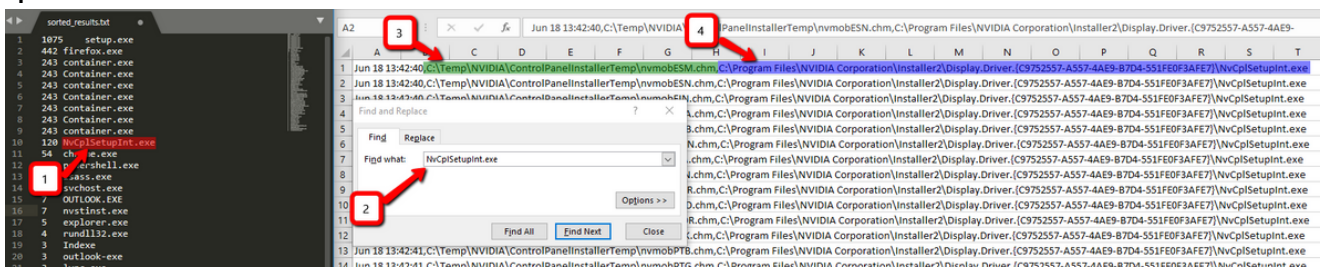
- **data.csv**: 包含已掃描檔案的完整路徑以及建立/修改/移動檔案的父進程
- **results.txt**: 包含AMP掃描的進程清單
- **sorted_results.txt**: 包含AMP掃描的進程清單以及掃描最多的進程
- **terms.txt** : 包含AMP掃描的進程的名稱

步驟9. 從data.csv中的sorted_results.txt中篩選具有高計數的進程名稱，您可以用其完整路徑標識父進程，然後繼續向自定義清單中的策略新增排除項（如果受信任）。

要查詢的進程：

1. 控制+F在「data.csv」和搜尋
2. AMP掃描的檔案的路徑
3. 複製/移動/修改檔案的父進程的路徑

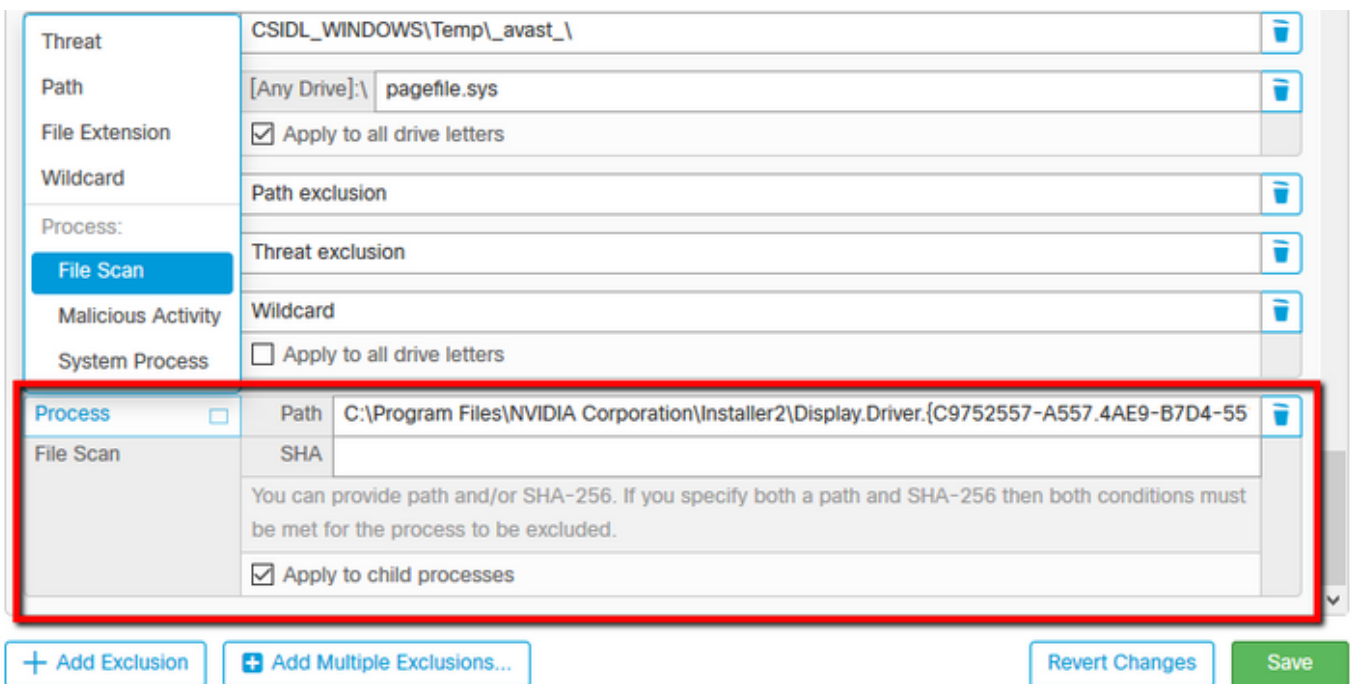
附註：附註：通常排除為「Process:正在獲取掃描的父進程的「檔案掃描」和「子進程包括」



附註：在此處，您可以找到與建立排除的最佳實踐相關的詳細資訊。

調整排除

識別出進程或路徑後，可以將它們新增到連結到終端上應用的策略的排除清單中，導航到 Management > Exclusions > Exclusions > Edit，如下圖所示。



將套件組合提交給TAC進行分析

ATS TAC可幫助排除這些情況的故障，如果出現這種情況，請準備在建立案例時提供下一個資訊：

- 此問題何時開始？
- 最近有變化嗎？
- 特定應用程式是否出現問題？如果是，哪一個應用程式？
- 系統中是否有其他防病毒軟體？如果是，哪種防病毒軟體？
- 重現問題的同時收集調試捆綁包：[收集調試捆綁包的步驟](#)