

分析AMP诊断套件，用于高CPU

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[故障排除](#)

[验证计算机上是否安装了其他防病毒软件](#)

[确定特定应用使用时是否发生高CPU](#)

[收集诊断套件以进行分析](#)

[启用调试日志级别](#)

[终端中的调试级别](#)

[策略中的调试级别](#)

[重现问题并收集诊断捆绑包](#)

[进行分析](#)

[Diag_Analyzer.exe](#)

[Amphandlecount.ps1](#)

[调整排除项](#)

[向TAC提交捆绑包以供分析](#)

简介

本文档介绍从面向Windows设备上的终端的高级恶意软件防护(AMP)公共云分析诊断捆绑包以排除高CPU使用率故障的步骤。

作者：Luis Velazquez和Yeraldin Sánchez，Cisco TAC工程师编辑。

先决条件

要求

Cisco 建议您了解以下主题：

- [访问AMP控制台](#)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 面向终端的AMP控制台5.4.20200204
- Windows操作系统设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

故障排除

本部分提供的信息可用于对配置进行故障排除。

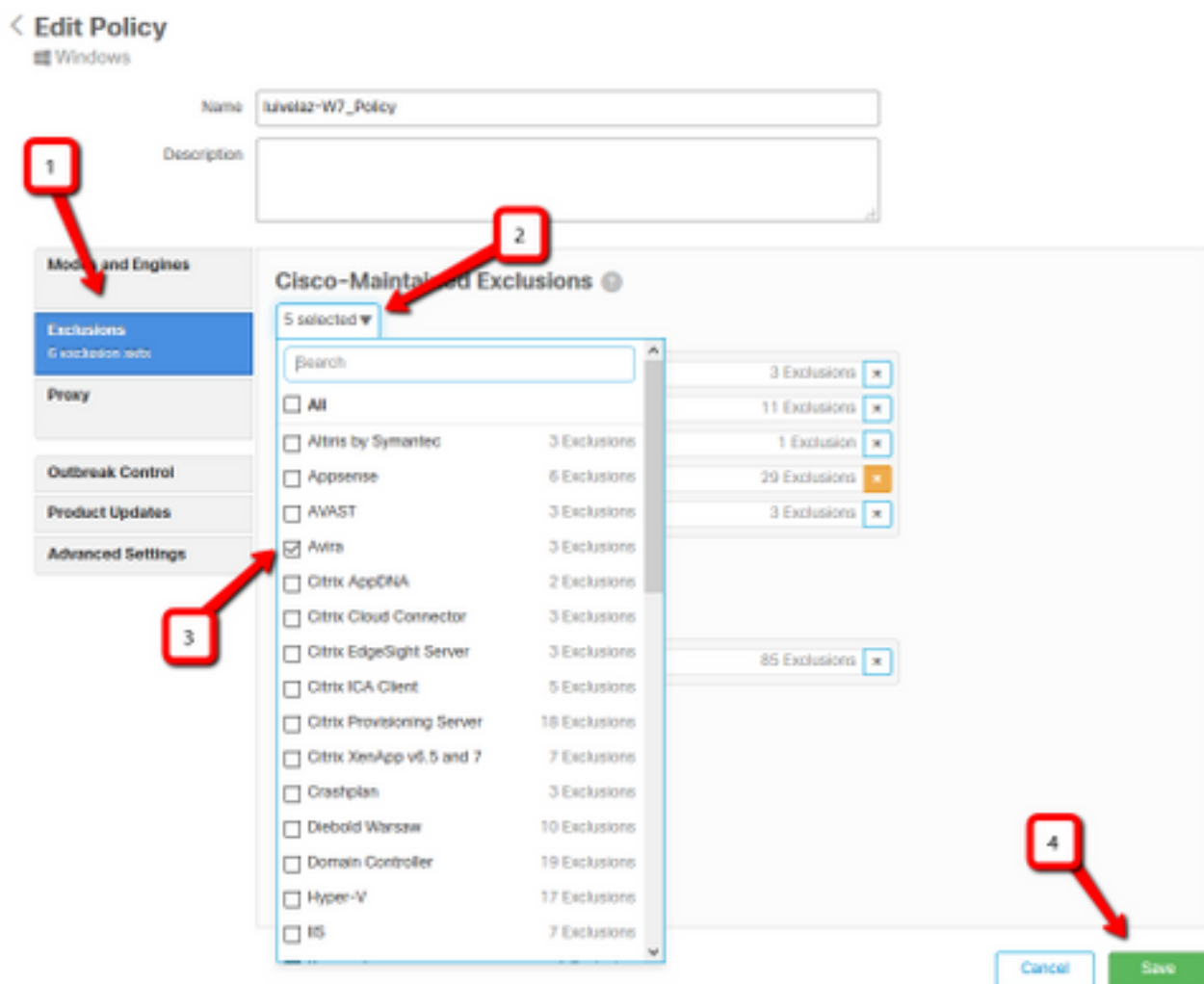
验证计算机上是否安装了其他防病毒软件

如果安装了另一个AV（防病毒软件），请确保在策略配置中排除AV的主进程

提示：如果列表中包含思科维护的排除项，请记住，这些排除项可以添加到应用程序的新版本。

要查看Cisco维护的排除部分中的可用列表，请导航至**Management > Policies > Edit > Exclusions > Cisco维护的排除**。

根据计算机上当前安装的软件选择终端需要的软件，然后保存策略，如图所示。



确定特定应用使用时是否发生高CPU

确定问题是否发生在执行一个应用程序或其中几个应用程序时，如果您能够复制该问题，则有助于确定潜在的排除项。

收集诊断套件以进行分析

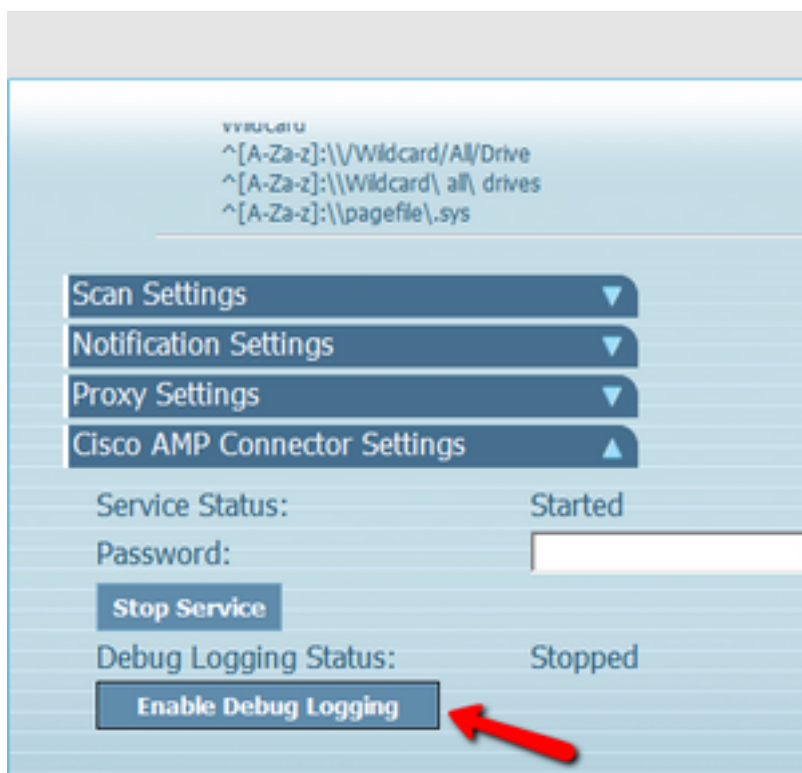
启用调试日志级别

要收集有用的诊断包，必须启用调试日志级别。

终端中的调试级别

如果可以复制问题并有权访问终端，以下是捕获诊断捆绑包的最佳步骤：

1. 打开AMP GUI
2. 导航至**设置**
3. 滚动到AMP GUI底部并打开Cisco AMP**连接器设置**
4. 单击“**Enable Debug Logging (启用调试日志记录)**”
5. “**调试日志记录状态**”必须更改为“**已启动**”。此过程启用调试级别，直到下一个策略心跳，默认为15分钟



策略中的调试级别

如果您无权访问终端或无法一致地重现问题，则必须在策略中启用调试日志级别。

要按策略启用调试日志级别，请导航到Management > Policies > Edit > Advanced Settings > Connector Log Level 和Management > Policies > Edit > Advanced Settings > Tray Log Level，然后选择Debug并保存策略，如图所示。

< Edit Policy

Windows

Name: Iuvelaz-W7_Policy

Description:

Modes and Engines

Exclusions
6 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

Administrative Features

Client User Interface

File and Process Scan

Cache

Endpoint Isolation

Orbita

Engines

ETBA

Network

Scheduled Scans

Identity Persistence

Send User Name in Events ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval: 15 minutes ⓘ

Connector Log Level: Debug ⓘ

Tray Log Level: Debug ⓘ

Enable Connector Protection ⓘ

Connector Protection Password: ***** ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

Cancel Save

警告：如果从策略启用调试模式，则所有终端都会收到此更改。

注意：同步终端的策略以确保应用调试级别或等待心跳间隔（默认为15分钟）。

重现问题并收集诊断捆绑包

当配置调试级别时，请等待系统上出现高CPU状态，或手动重现之前确定的条件，然后收集诊断包。

要收集捆绑包，请导航至C:\Program Files\Cisco\AMP\X.X.X（其中X.X.X是系统上安装的最新AMP版本）并运行应用程序ipsupporttool.exe，此过程会在名为CiscoAMP_Support_Tool_%date%.7z的桌面上创建.7z文件。

注意：连接器版本6.2.3及更高版本可以远程请求捆绑包，导航至Management > Computers，展开终端记录并使用Diagnose选项。

注意：诊断捆绑包也可以从CMD提示符下使用以下命令运行："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是安装的最新AMP版本，可以使用第二个命令来选择.7z文件的输出文件夹。

进行分析

有两种方法可以分析诊断文件：

- Diag_Analyzer.exe
- Amphandlecount.ps1

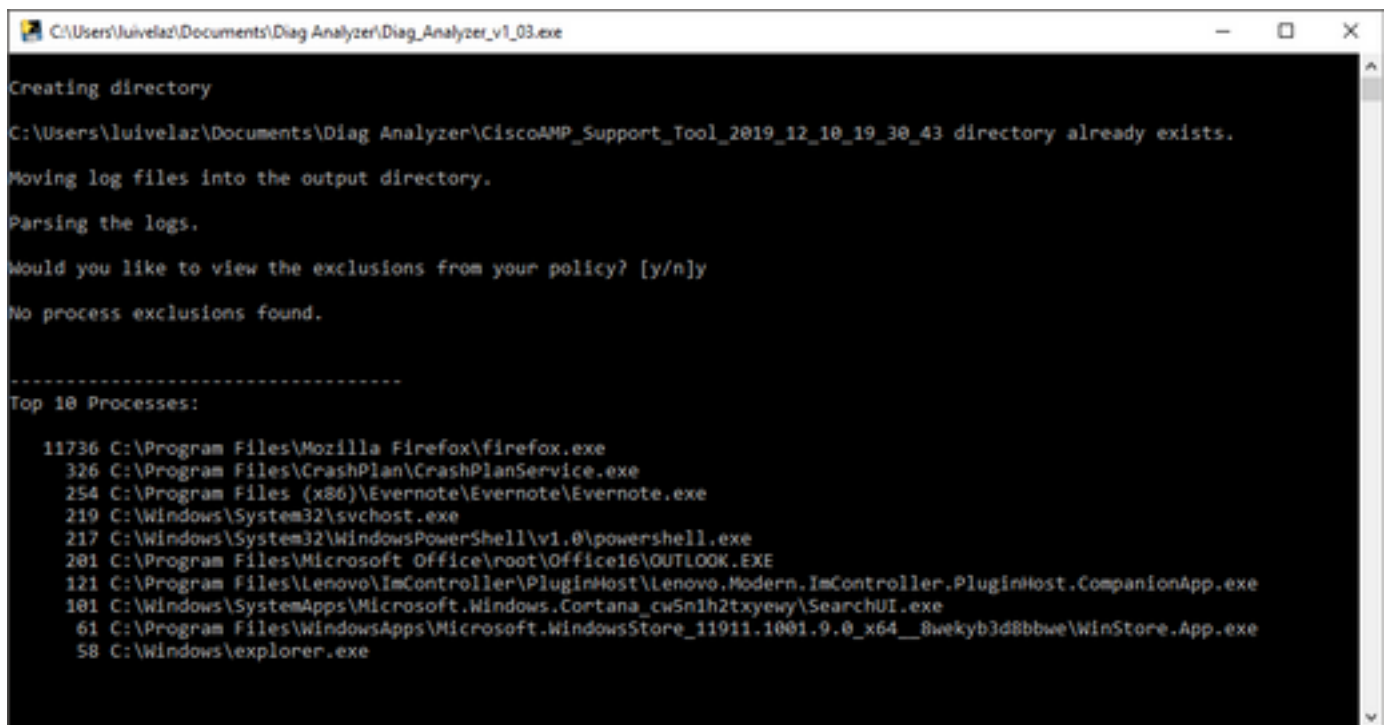
Diag_Analyzer.exe

步骤1.在此下载应用[程序](#)。

步骤2.在GitHub页面中，有一个README文件，其中包含有关使用的进一步说明。

步骤3.将诊断文件CiscoAMP_Support_Tool_%date%.7z复制到Diag_Analyzer.exe所在的文件夹中。

步骤4.执行应用 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
```

步骤5.在新提示符中，确认是否要从策略中获得Y或N的排除项。。

步骤6.脚本结果包含：

- 前10个流程
- 前10个文件
- 前10个分机
- 前100条路径
- 所有文件

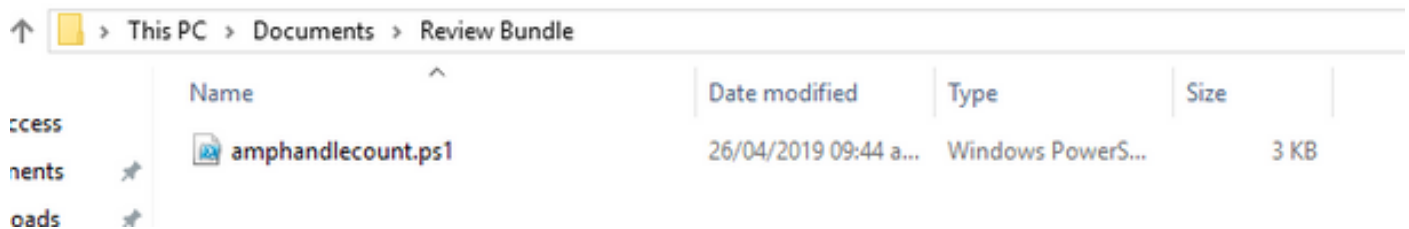
注意：Diag_Analyzer.exe检查提供的AMP诊断文件sfc.exe.log文件。然后，使用诊断文件名创建新目录并将日志文件存储在。7z之外的。7z目录中，之后，它解析日志并确定前10个进程、文件、扩展名和路径，最后，它将信息打印到屏幕和{Diagnostic}-summary.txt文件。

Amphandlecount.ps1

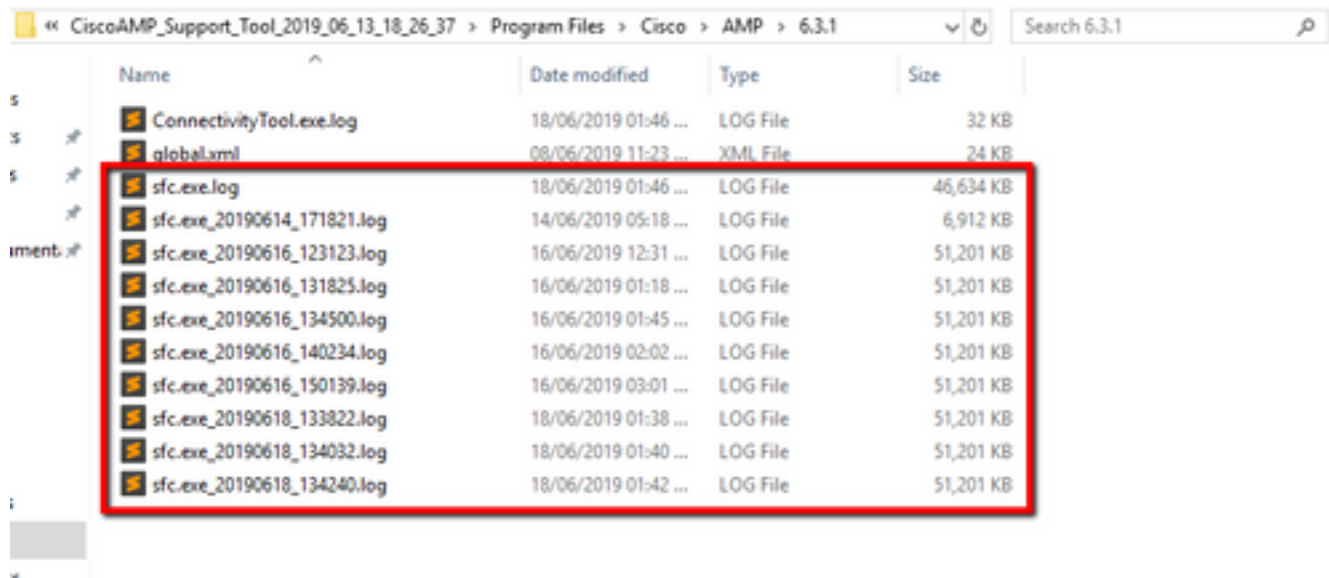
步骤1.从此社区底部[下载脚本](#)amphandlecounts.txt，然后从[AMP审阅扫描的文件](#)。

步骤2.要在Windows中运行脚本，请将其重命名为amphandlecount.ps1。

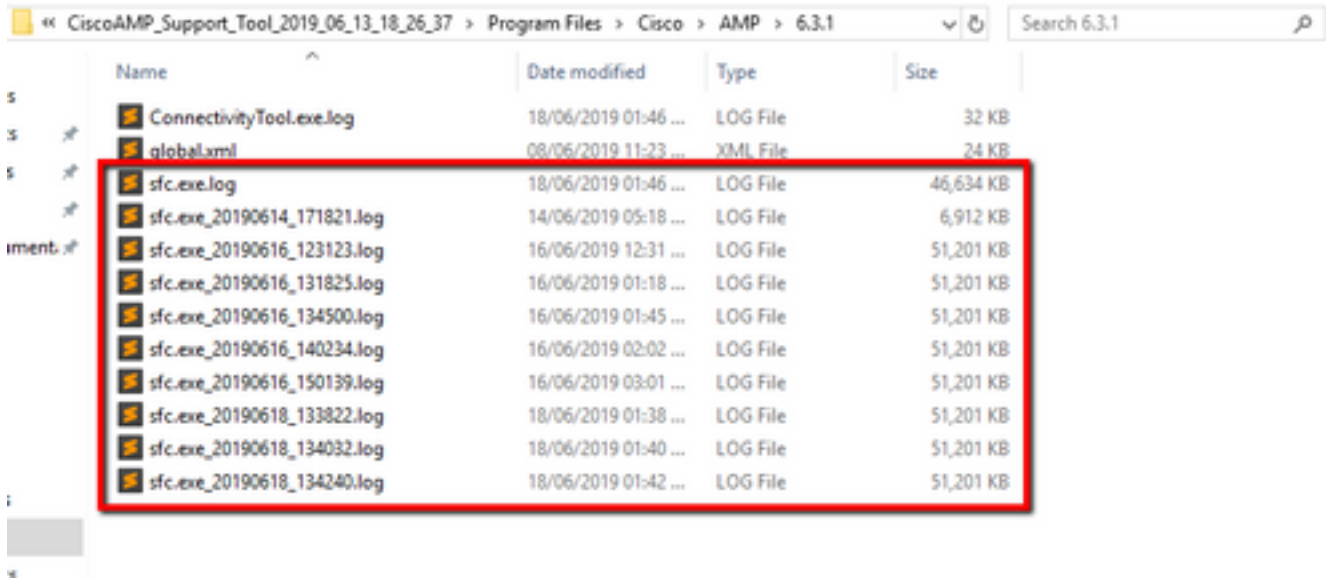
步骤3.为方便起见，将amphandlecount.ps1文件复制到自己的文件夹。



步骤4.解压CiscoAMP_Support_Tool_%date%.7z文件，并在路径上标识sfc.log的文件 CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X。



步骤5.将sfc.log的文件复制到amphandlecount.ps1文件夹。



步骤6.使用PowerShell运行amphandlecount.ps1，然后打开一个窗口，根据终端上的执行策略，可以请求运行权限。

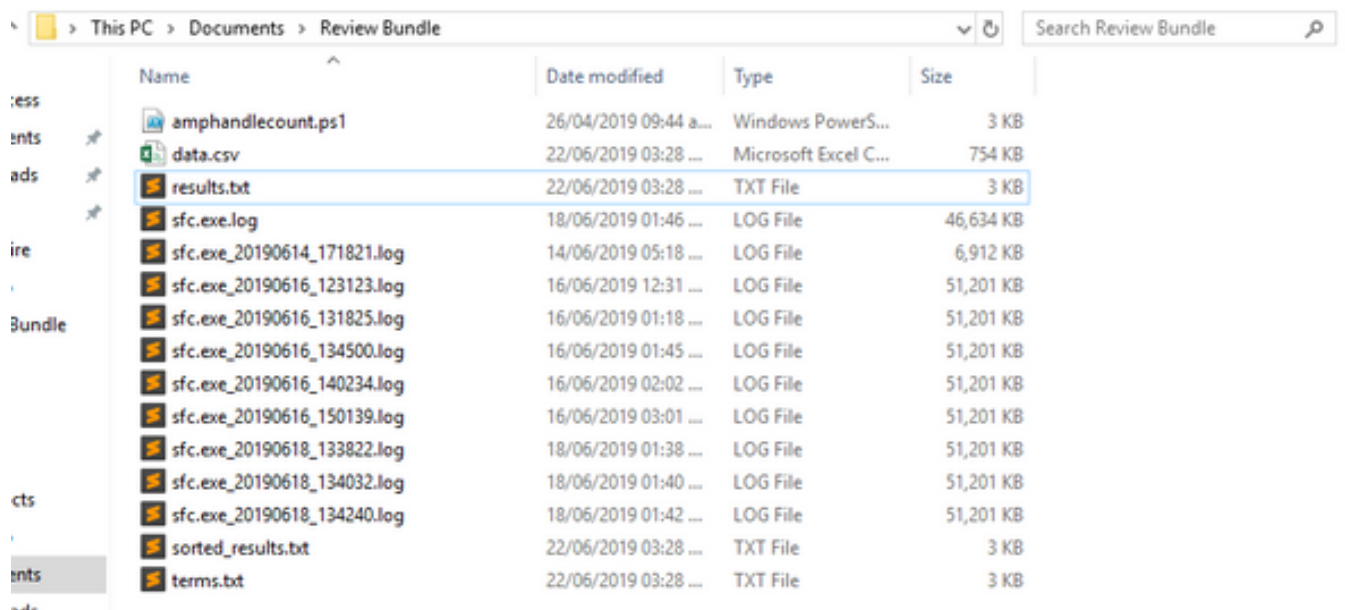
提示：要更改执行策略，请打开Windows PowerShell并使用下一命令：

将策略设置为允许无限制执行访问 — **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**

设置策略以限制执行访问 — **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

步骤7.在PowerShell完成后，允许PowerShell完成（可能需要一些时间，具体取决于文件夹中的sfc.log数量），在文件夹上创建四个文件：

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



步骤8. 4个新文件包含分析结果：

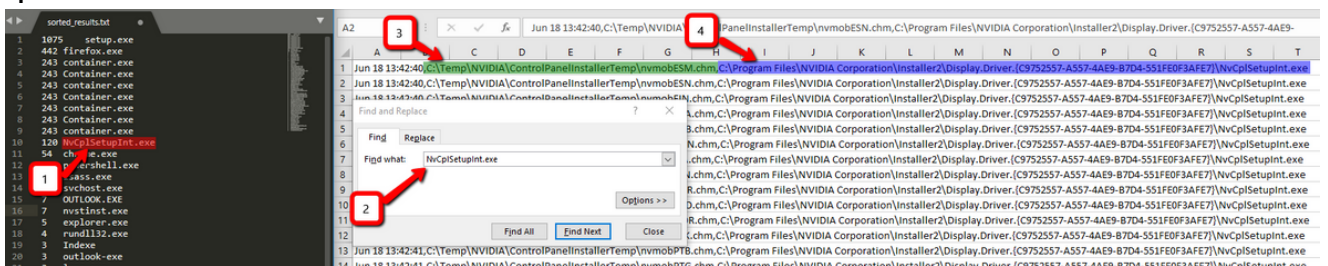
- **data.csv**: 包含已扫描文件的完整路径以及创建/修改/移动文件的父进程
- **results.txt**: 包含AMP扫描的进程列表
- **sorted_results.txt**: 包含AMP扫描的进程列表，其中扫描的进程最多
- **terms.txt**：包含AMP扫描的进程的名称

步骤9. 从data.csv中的sorted_results.txt中筛选具有高计数的进程名称，然后继续在自定义列表中添加一个排除项（如果受信任）。

要查看的流程：

1. 在“data.csv”和搜索上控制+ F
2. AMP扫描的文件路径
3. 复制/移动/修改文件的父进程的路径

注意：注意：排除通常为“Process:文件扫描”(File Scan)，其中“子进程包括”(Child Processes include)用于正在获取扫描的父进程



注意：在此可以找到与创建例外项的最佳实践相关的详细信息。

调整排除项

确定进程或路径后，可以将其添加到链接到终端上应用的策略的排除列表中，导航至Management > Exclusions > Exclusion name > Edit，如图所示。

Threat	CSIDL_WINDOWS\Temp_avast_	
Path	[Any Drive]:\ pagefile.sys	
File Extension	<input checked="" type="checkbox"/> Apply to all drive letters	
Wildcard	Path exclusion	
Process:	Threat exclusion	
File Scan	Wildcard	
Malicious Activity	<input type="checkbox"/> Apply to all drive letters	
System Process		
Process <input type="checkbox"/>	Path C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.(C9752557-A557.4AE9-B7D4-55	
File Scan	SHA	
You can provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must be met for the process to be excluded.		
<input checked="" type="checkbox"/> Apply to child processes		

向TAC提交捆绑包以供分析

ATS TAC可帮助排除这些情况，如果是这种情况，请准备好在创建案例时提供下一信息：

- 此问题何时开始？
- 最近有变化吗？
- 特定应用程序是否出现问题？如果是，哪个应用程序？
- 系统上是否有其他防病毒软件？如果是，哪种防病毒软件？
- 在重现问题时收集调试捆绑包：[收集调试捆绑包的步骤](#)