Analyze AMP Diagnostic Bundle for High CPU

Contents

Introduction

This document describes the steps to analyze a diagnostic bundle from Advanced Malware Protection (AMP) for Endpoints Public Cloud on Windows devices to troubleshoot high CPU usage.

Contributed by Luis Velazquez and Edited by Yeraldin Sánchez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Access to the AMP console

Components Used

The information in this document is based on these software and hardware versions:

- AMP for Endpoints Console 5.4.20200204

- Windows operating system devices

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

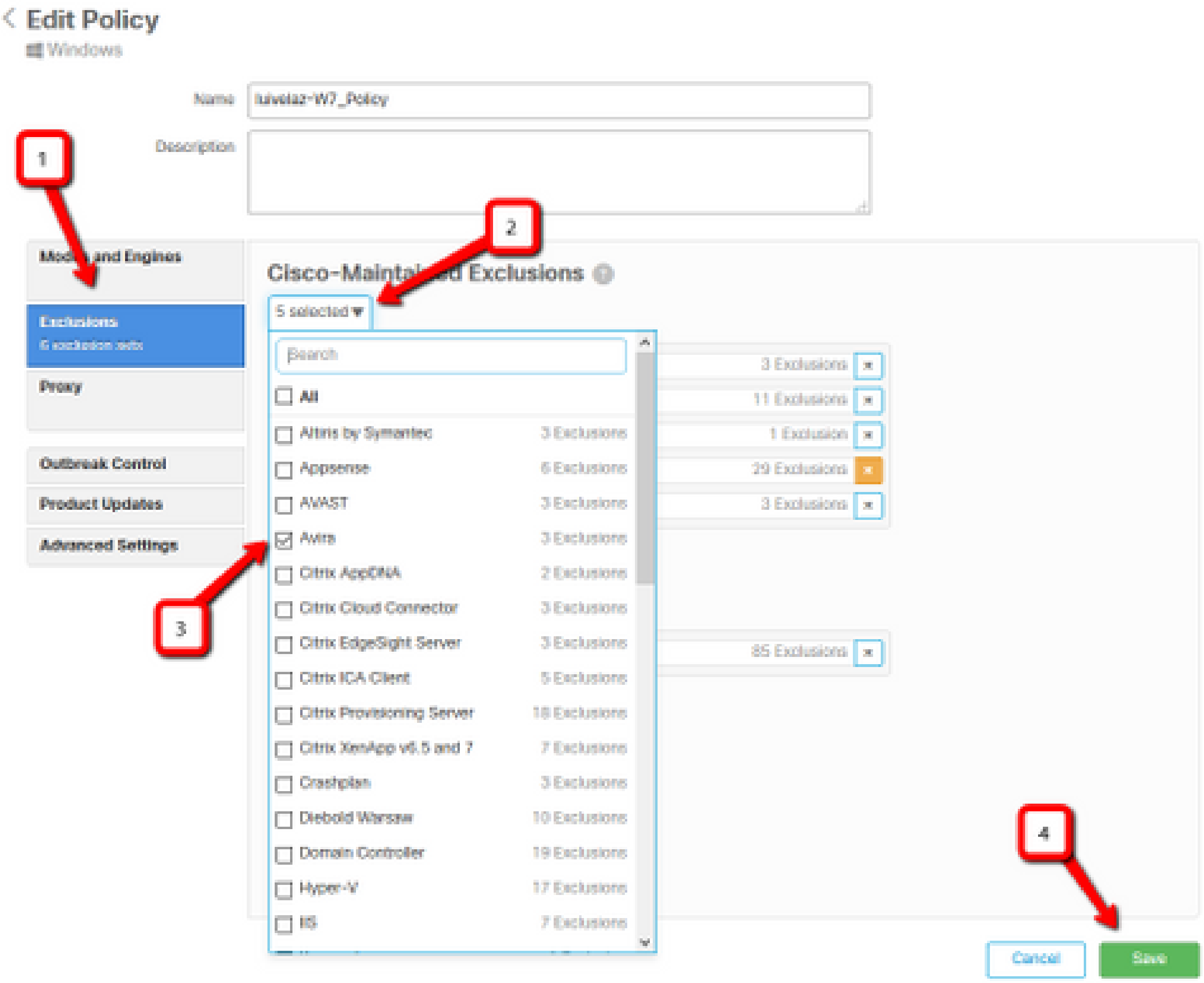
Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Verify if another antivirus is installed on the machine

If another AV (antivirus) is installed, ensure the main process of the AV is excluded in the policy configuration

> **Tip**: Use the Cisco-Maintained exclusions if the software that is used is included on the list, remember that these exclusions can be added to new versions of an application.
>
> In order to see the lists available in Cisco maintained exclusions section, navigate to **Management** > **Policies** > **Edit** > **Exclusions** > **Cisco-Maintained Exclusions.** Select the ones your endpoint would need according to the software currently installed on the machine, then, save the policy, as shown in the image.



Name: luivelaz-W7_Policy

Description:

□ All	
□ Altiris by Symantec	3 Exclusions
□ Appsense	6 Exclusions
□ AVAST	3 Exclusions
☑ Avira	3 Exclusions
□ Citrix AppDNA	2 Exclusions
□ Citrix Cloud Connector	3 Exclusions
□ Citrix EdgeSight Server	3 Exclusions
□ Citrix ICA Client	5 Exclusions
□ Citrix Provisioning Server	18 Exclusions
□ Citrix XenApp v6.5 and 7	7 Exclusions
□ Crashplan	3 Exclusions
□ Diebold Warsaw	10 Exclusions
□ Domain Controller	19 Exclusions
□ Hyper-V	17 Exclusions
□ IIS	7 Exclusions

Identify if the high CPU happens when a specific application is in use

Identify if the issue happens while one application or a few of them are executed if you are able to replicate the issue helps in the process of identifying potential exclusions.

Gather diagnostic bundle for analysis

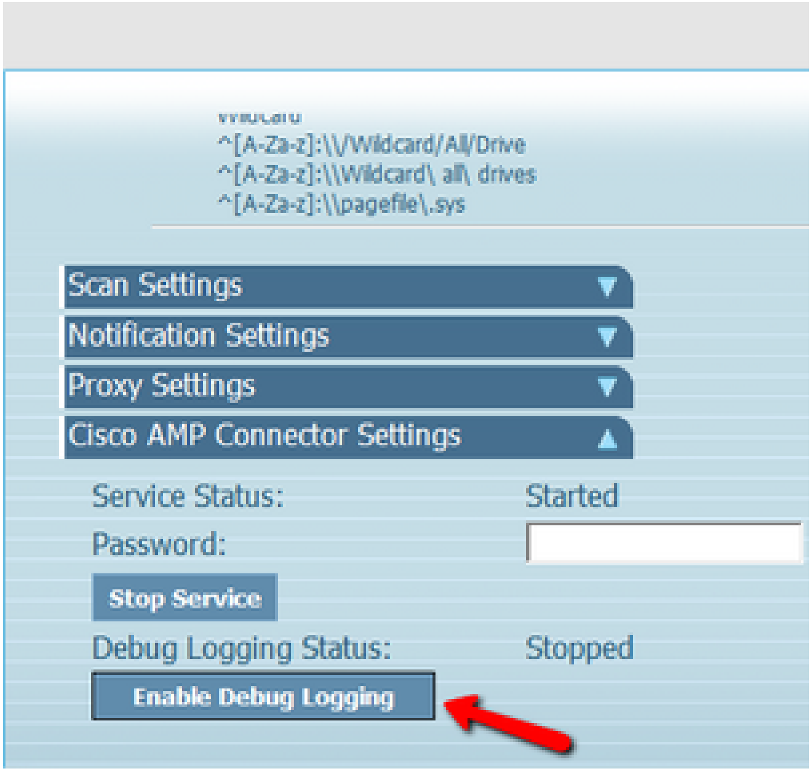
Enable Debug Log Level

In order to gather a useful diagnostic bundle, the debug log level must be enabled.

Debug Level in the endpoint

If you can replicate the issue and have access to the endpoint, below is the best procedure to capture the diagnostic bundle:

1. Open AMP GUI
2. Navigate to **Settings**
3. Scroll to the bottom of AMP GUI and open **Cisco AMP Connector Settings**
4. Click on **Enable Debug Logging**
5. **Debug Logging Status** must change to **Started.** This procedure enables debug level until the next policy heartbeat, by default 15 minutes



```
^[A-Za-z]:\\/Wildcard/All/Drive
^[A-Za-z]:\\Wildcard\ all\ drives
^[A-Za-z]:\\pagefile\.sys
```

Service Status: Started

Password:

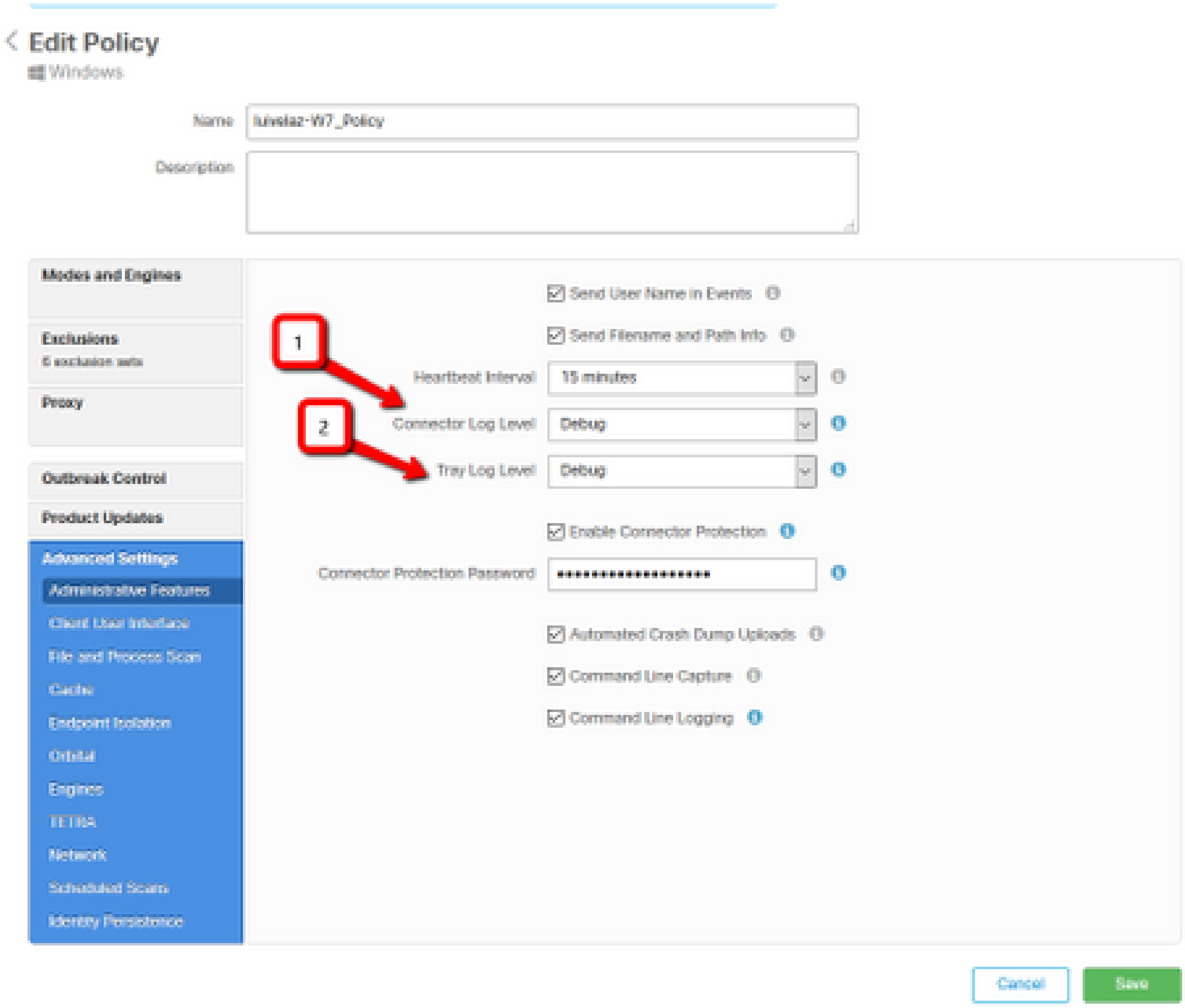
Debug Logging Status: Stopped

Debug level in the policy

If you don't have access to the endpoint or the issue can't be reproduced consistently, the debug log level must be enabled in the policy.

In order to enable debug log level by policy navigate to **Management** > **Policies** > **Edit** >

Advanced Settings > **Connector Log Level** and **Management** > **Policies** > **Edit** > **Advanced Settings** > **Tray Log Level,** then select **Debug** and save the policy, as shown in the image.



Name: luivelaz-W7_Policy

Description:

☑ 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

Caution: If debug mode is enabled from the policy, all endpoints receive this change.

Note: Sync the policy of the endpoint to ensure the debug level is applied or wait for the heartbeat interval, by default it is 15 minutes.

Reproduce the issue and gather a diagnostic bundle

When the debug level is configured wait till the state of High CPU happens on the system or manually reproduce the conditions previously identified and then gather the diagnostic bundle.

In order to collect the bundle navigate to **C:\Program Files\Cisco\AMP\X.X.X** (Where X.X.X is the latest AMP version installed on the system) and run the application **ipsupporttool.exe** this process creates a **.7z** file on the desktop named **CiscoAMP_Support_Tool_%date%.7z**

Note: Connector version 6.2.3 and later can request a bundle remotely, navigate to **Management > Computers**, expand the endpoint record and use the option Diagnose.

Note: The diagnostic bundle can also run from a CMD prompt with the command:

"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe", or "**C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To"**, where **X.X.X** is the latest AMP version installed, the second command can be used in order to select the output folder for the .7z file.

Make the analysis

There are two ways to analyze a diagnostic file:

- Diag_Analyzer.exe
- Amphandlecount.ps1

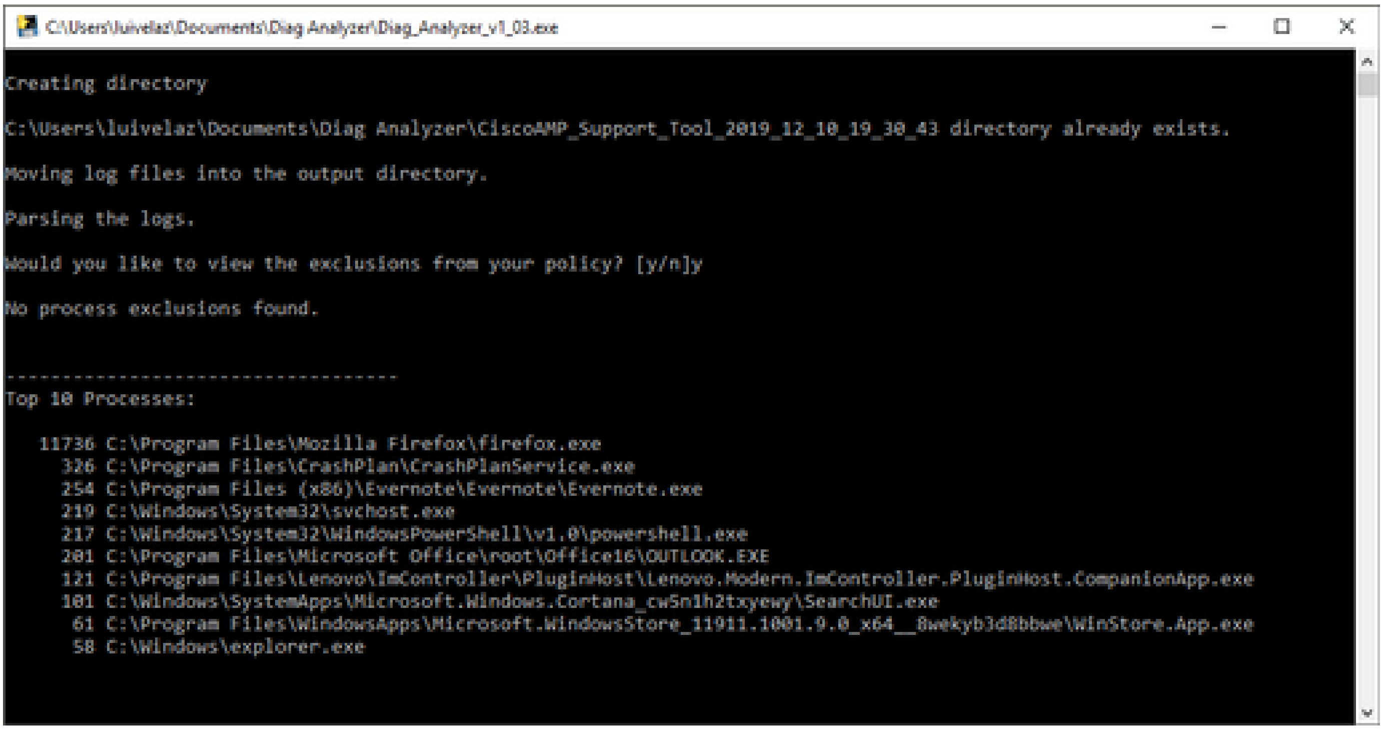
Diag_Analyzer.exe

Step 1. Download the application here.

Step 2. In the GitHub page, there is a README file with further instructions on usage.

Step 3. Copy the diagnostic file **CiscoAMP_Support_Tool_%date%.7z** on the same folder that Diag_Analyzer.exe is located.

Step 4. Execute the application **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
```

Step 5. In the new prompt confirm if you want to get the exclusions from the policy with a **Y** or an **N**.

Step 6. The script result contains:

- Top 10 Processes
- Top 10 Files
- Top 10 Extensions

- Top 100 Paths
- All files

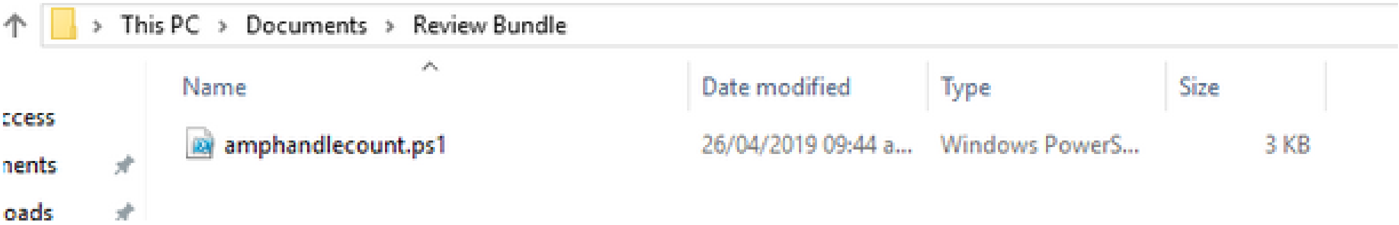
  Note: Diag_Analyzer.exe checks the provided AMP diagnostic file for sfc.exe.log files. then, creates a new directory with the diagnostic file name and store the log files outside of the .7z, in the parent directory of the diagnostic, after this, it parses the logs and determines the top 10 processes, files, extensions, and paths, finally, it prints information to the screen and also to a {Diagnostic}-summary.txt file.

Amphandlecount.ps1

Step 1. Download the script **amphandlecounts.txt** from the bottom of this community post Review Scanned Files from AMP.

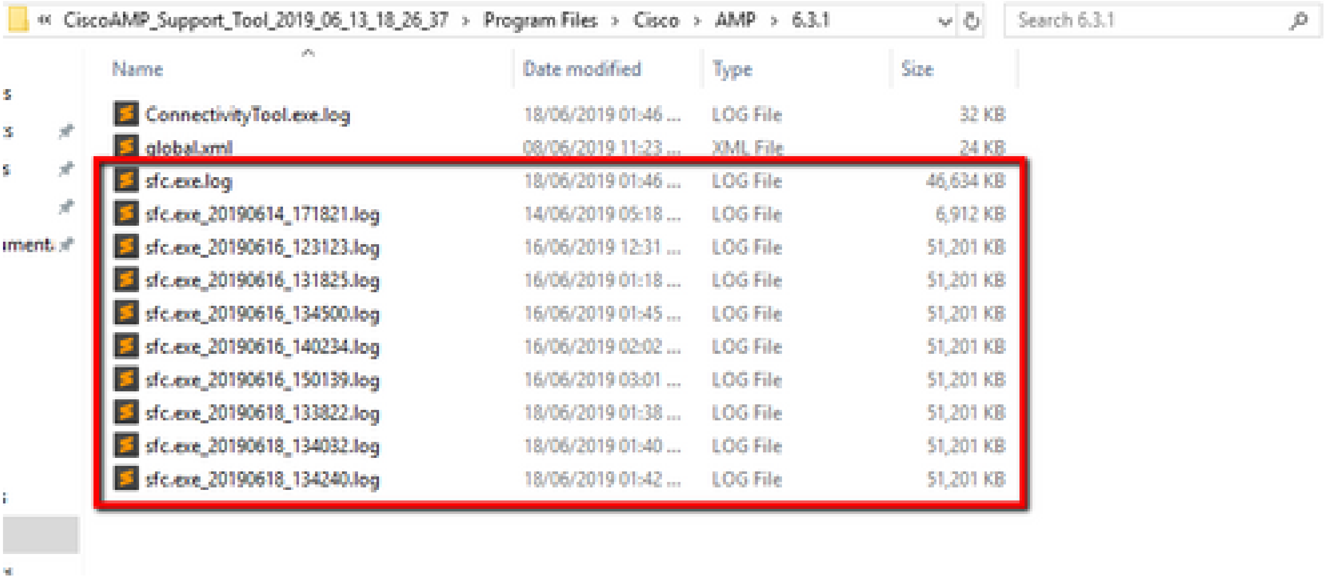
Step 2. In order to run the script in Windows, rename it to **amphandlecount.ps1**.

Step 3. For convenience copy **amphandlecount.ps1** file to a folder of his own.



Name	Date modified	Type	Size
amphandlecount.ps1	26/04/2019 09:44 a...	Windows PowerS...	3 KB

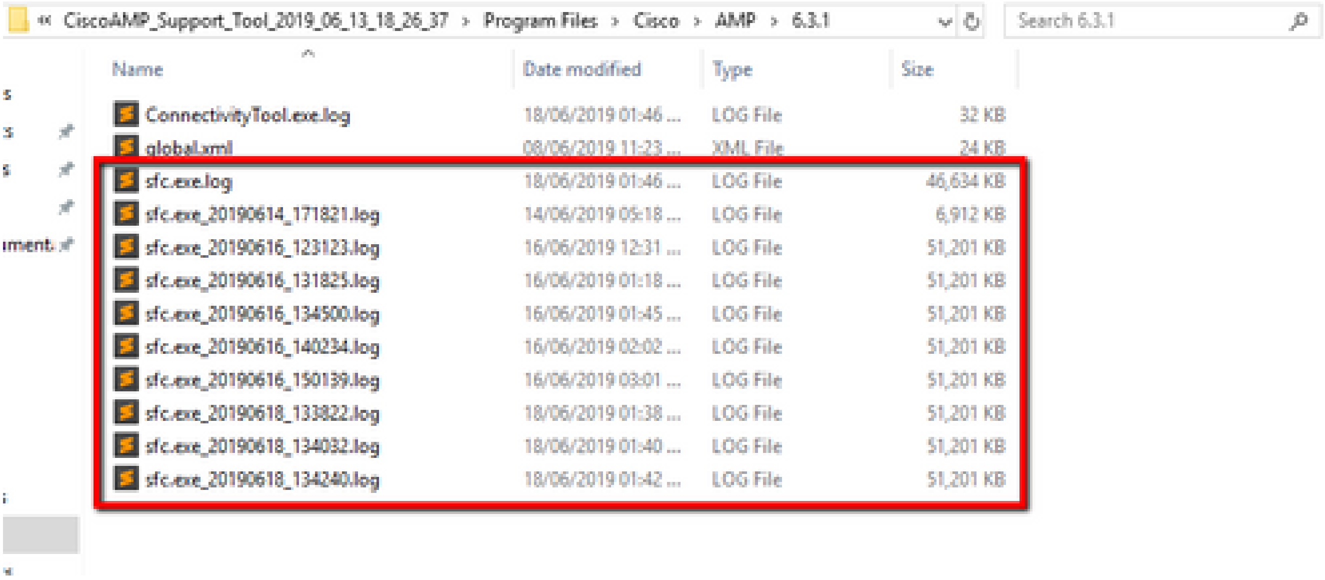
Step 4. Unzip the **CiscoAMP_Support_Tool_%date%.7z** file and identify the **sfc.log's** files on the path **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X .**



« CiscoAMP_Support_Tool_2019_06_13_18_26_37 > Program Files > Cisco > AMP > 6.3.1
Search 6.3.1

Name	Date modified	Type	Size
ConnectivityTool.exe.log	18/06/2019 01:46 ...	LOG File	32 KB
global.xml	08/06/2019 11:23 ...	XML File	24 KB
sfc.exe.log	18/06/2019 01:46 ...	LOG File	46,634 KB
sfc.exe_20190614_171821.log	14/06/2019 05:18 ...	LOG File	6,912 KB
sfc.exe_20190616_123123.log	16/06/2019 12:31 ...	LOG File	51,201 KB
sfc.exe_20190616_131825.log	16/06/2019 01:18 ...	LOG File	51,201 KB
sfc.exe_20190616_134500.log	16/06/2019 01:45 ...	LOG File	51,201 KB
sfc.exe_20190616_140234.log	16/06/2019 02:02 ...	LOG File	51,201 KB
sfc.exe_20190616_150139.log	16/06/2019 03:01 ...	LOG File	51,201 KB
sfc.exe_20190618_133822.log	18/06/2019 01:38 ...	LOG File	51,201 KB
sfc.exe_20190618_134032.log	18/06/2019 01:40 ...	LOG File	51,201 KB
sfc.exe_20190618_134240.log	18/06/2019 01:42 ...	LOG File	51,201 KB

Step 5. Copy the **sfc.log's** files on the **amphandlecount.ps1** folder.



« CiscoAMP_Support_Tool_2019_06_13_18_26_37 › Program Files › Cisco › AMP › 6.3.1

Search 6.3.1

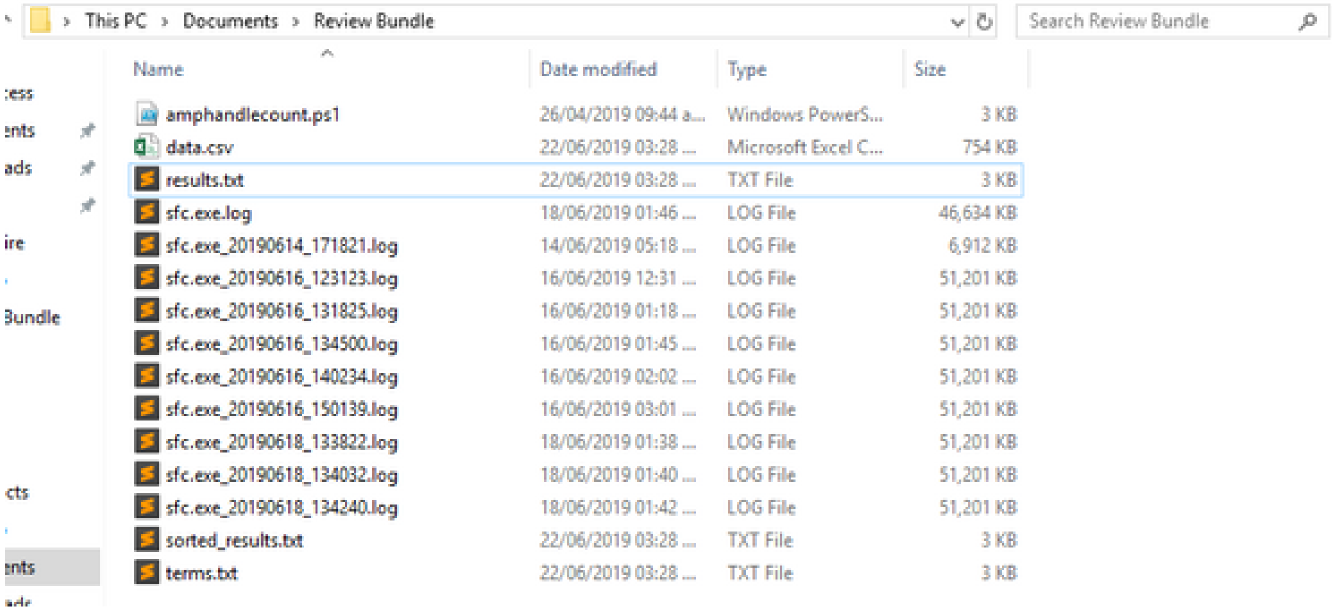
Name	Date modified	Type	Size
ConnectivityTool.exe.log	18/06/2019 01:46 ...	LOG File	32 KB
global.xml	08/06/2019 11:23 ...	XML File	24 KB
sfc.exe.log	18/06/2019 01:46 ...	LOG File	46,634 KB
sfc.exe_20190614_171821.log	14/06/2019 05:18 ...	LOG File	6,912 KB
sfc.exe_20190616_123123.log	16/06/2019 12:31 ...	LOG File	51,201 KB
sfc.exe_20190616_131825.log	16/06/2019 01:18 ...	LOG File	51,201 KB
sfc.exe_20190616_134500.log	16/06/2019 01:45 ...	LOG File	51,201 KB
sfc.exe_20190616_140234.log	16/06/2019 02:02 ...	LOG File	51,201 KB
sfc.exe_20190616_150139.log	16/06/2019 03:01 ...	LOG File	51,201 KB
sfc.exe_20190618_133822.log	18/06/2019 01:38 ...	LOG File	51,201 KB
sfc.exe_20190618_134032.log	18/06/2019 01:40 ...	LOG File	51,201 KB
sfc.exe_20190618_134240.log	18/06/2019 01:42 ...	LOG File	51,201 KB

Step 6. Run **amphandlecount.ps1** with PowerShell, then a window is opened and depending on the execution policy on the endpoint can ask for permission to run.

> **Tip**: In order to change the execution policy open a Windows PowerShell and use the next commands:
> Set the policy to allow unrestricted execution access - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**
> Set the policy to restrict execution access - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

Step 7. Allow the PowerShell to finish (It might take some time, depending on how many sfc.log are in the folder) after the PowerShell finish, four files are created on the folder:

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



› This PC › Documents › Review Bundle

Search Review Bundle

Name	Date modified	Type	Size
amphandlecount.ps1	26/04/2019 09:44 a...	Windows PowerS...	3 KB
data.csv	22/06/2019 03:28 ...	Microsoft Excel C...	754 KB
results.txt	22/06/2019 03:28 ...	TXT File	3 KB
sfc.exe.log	18/06/2019 01:46 ...	LOG File	46,634 KB
sfc.exe_20190614_171821.log	14/06/2019 05:18 ...	LOG File	6,912 KB
sfc.exe_20190616_123123.log	16/06/2019 12:31 ...	LOG File	51,201 KB
sfc.exe_20190616_131825.log	16/06/2019 01:18 ...	LOG File	51,201 KB
sfc.exe_20190616_134500.log	16/06/2019 01:45 ...	LOG File	51,201 KB
sfc.exe_20190616_140234.log	16/06/2019 02:02 ...	LOG File	51,201 KB
sfc.exe_20190616_150139.log	16/06/2019 03:01 ...	LOG File	51,201 KB
sfc.exe_20190618_133822.log	18/06/2019 01:38 ...	LOG File	51,201 KB
sfc.exe_20190618_134032.log	18/06/2019 01:40 ...	LOG File	51,201 KB
sfc.exe_20190618_134240.log	18/06/2019 01:42 ...	LOG File	51,201 KB
sorted_results.txt	22/06/2019 03:28 ...	TXT File	3 KB
terms.txt	22/06/2019 03:28 ...	TXT File	3 KB

Step8. The 4 new files contain the result of the analysis:

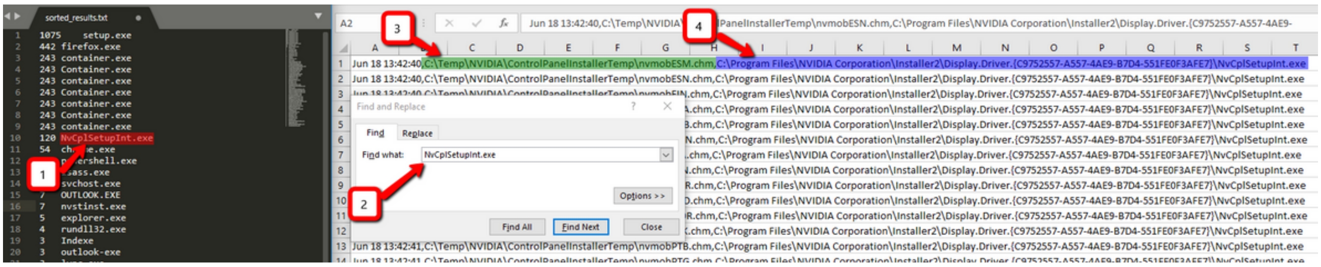
- **data.csv:** contains the full path of the files scanned and the father process which created/modified/moved the file
- **results.txt:** contains the list of processes that are scanned by AMP
- **sorted_results.txt:** contain the list of processes that are scanned by AMP with the most scanned process
- **terms.txt:** contains the name of processes scanned by AMP

Step 9. Filter the process name with high counts from the **sorted_results.txt** in the **data.csv** you can identify the parent process with its full path, and then proceed to add an exclusion to the policy in a custom list if it is trusted.

Processes to look:

1. Cntrl + F on "data.csv" and search
2. Path of the file scanned by AMP
3. Path of the parent process that copy/moved/modified the file

> **Note**: Note: Usually the exclusion is the type "Process: File Scan" with "Child Processes include" for the parent process that is getting the scans:



```
1075    setup.exe
442 firefox.exe
243 container.exe
243 Container.exe
243 container.exe
243 Container.exe
243 container.exe
243 Container.exe
243 container.exe
120 NvCplSetupInt.exe
54  ch  e.exe
    p ershell.exe
     sass.exe
    svchost.exe
7   OUTLOOK.EXE
7   nvstinst.exe
5   explorer.exe
4   rundll32.exe
3   Indexe
3   outlook-exe
```

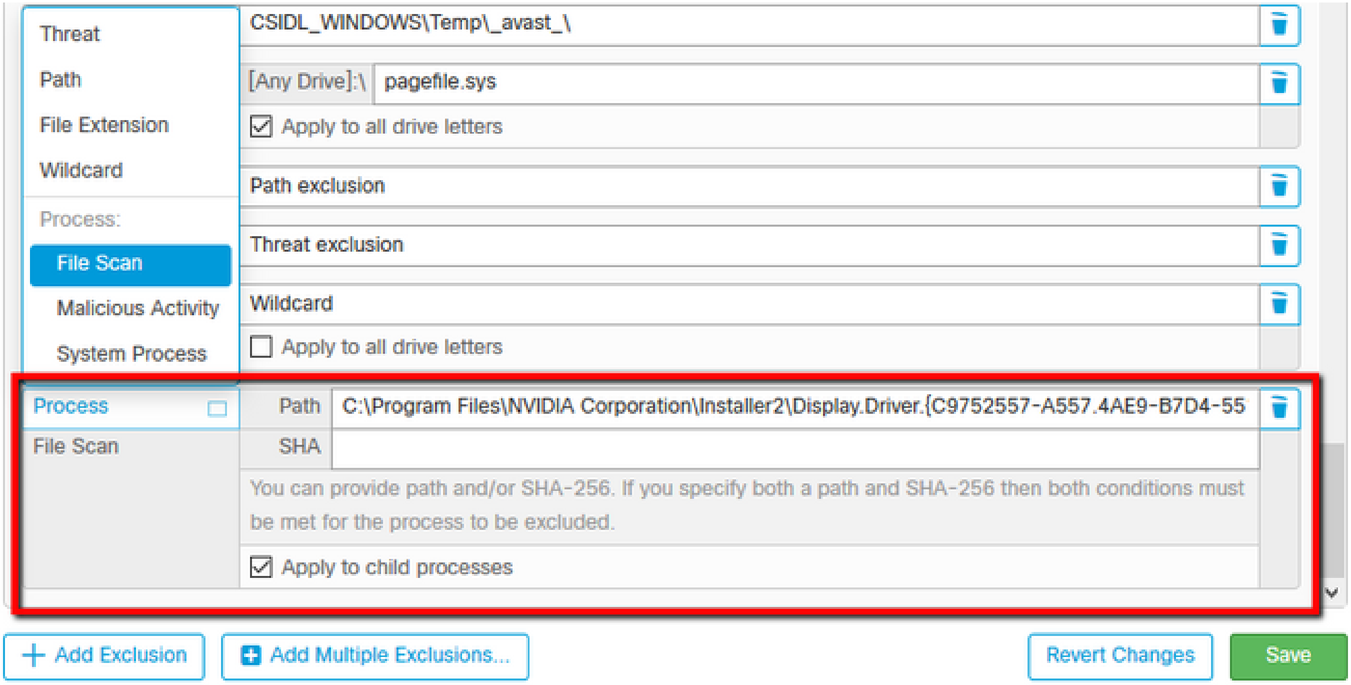
Find what: NvCplSetupInt.exe

```
Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobESN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-
1  Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobESM.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
2  Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobESN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
3  Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobFIN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
4  A.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
5  B.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
6  N.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
7  .chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
8  N.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
9  R.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
10 D.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
11 R.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
12 K.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
13 Jun 18 13:42:41,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobPTB.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
14 Jun 18 13:42:41,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmobPTG.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
```

> **Note**: Here you can find more information related to the best practices to create exclusions.

Tune Exclusions

Once the processes or paths are identified, you can add them to the exclusion list that is linked to the policy applied on the endpoint, navigate to **Management** > **Exclusions > Exclusion name > Edit,** as shown in the image.



Threat Path File Extension Wildcard	CSIDL_WINDOWS\Temp_avast_\
	[Any Drive]:\ pagefile.sys ☑ Apply to all drive letters
	Path exclusion
Process:	Threat exclusion
File Scan Malicious Activity System Process	Wildcard ☐ Apply to all drive letters
Process File Scan	Path C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55 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. ☑ Apply to child processes

Submit the bundle for analysis to TAC

ATS TAC can help to troubleshoot these scenarios, if that is the case, please be ready to provide the next information upon case creation:

- When does this issue start?
- Is there any recent change?
- Does the issue happen with a particular application?If yes, which application?
- Is there other Antivirus on the system?If yes, which antivirus?
- Collect a debug bundle while the issue is reproduced: Steps to collect a debug bundle