

AMP-diagnostische bundel voor hoge CPU's analyseren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Problemen oplossen](#)

[Controleer of er een ander antivirus op de machine is geïnstalleerd](#)

[Identificeer als er een hoge CPU plaatsvindt wanneer een specifieke toepassing in gebruik is](#)

[Montagebundel voor diagnostiek voor analyse](#)

[Debug-niveau inschakelen](#)

[Debug Level in het eindpunt](#)

[Debug level in het beleid](#)

[Reproduceert het probleem en verzamel een diagnostische bundel](#)

[De analyse maken](#)

[Diag_Analyzer.exe](#)

[Ampzakje.ps1](#)

[Tune-uitsluitingen](#)

[Vermeld de bundel voor analyse aan TAC](#)

Inleiding

In dit document worden de stappen beschreven om een diagnostische bundel van Advanced Malware Protection (AMP) voor Endpoints Public Cloud op Windows-apparaten te analyseren om een hoog CPU-gebruik te kunnen oplossen.

Bijgedragen door Luis Velazquez en bewerkt door Yeraldin Sánchez, Cisco TAC-engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de AMP-console

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Advanced Malware Protection voor endpoints console 5.4.20204

- Windows-besturingssysteemapparaten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

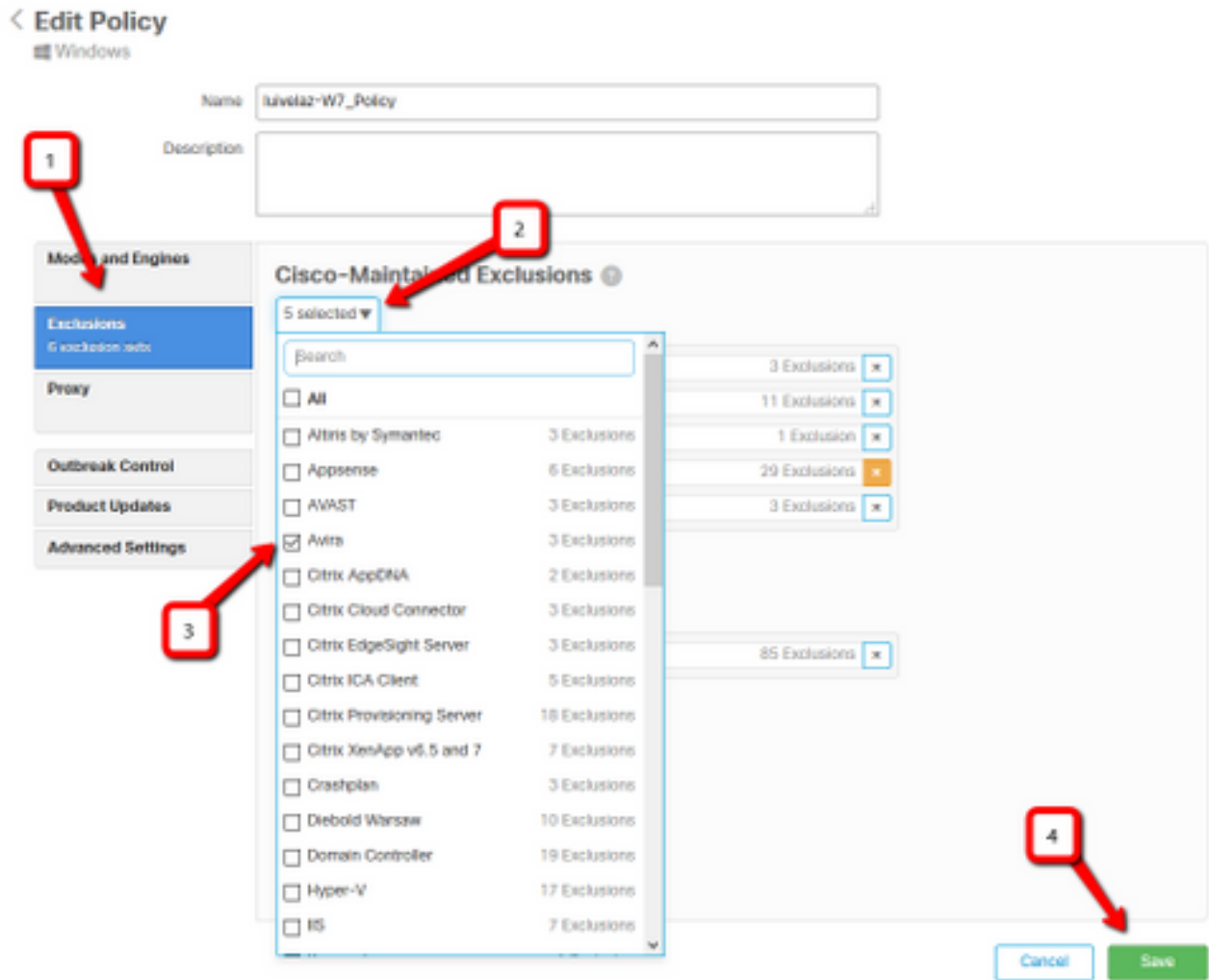
Controleer of er een ander antivirus op de machine is geïnstalleerd

Als er een andere AV (antivirus) is geïnstalleerd, zorg er dan voor dat het hoofdproces van de AV is uitgesloten in de beleidsconfiguratie

Tip: Gebruik de door Cisco onderhouden uitsluitingen als de software die in de lijst staat, vergeet niet dat deze uitsluitingen aan nieuwe versies van een toepassing kunnen worden toegevoegd.

Om de lijsten te zien beschikbaar in het gedeelte van Cisco handhaven uitsluitingen, navigeer naar **Beheer > Beleid > Bewerken > Uitsluitingen > Door Cisco onderhouden uitsluitingen**.

Selecteer degenen die uw eindpunt nodig zouden hebben volgens de software die momenteel op de machine geïnstalleerd is. Sla het beleid vervolgens op zoals in de afbeelding.



Identificeer als er een hoge CPU plaatsvindt wanneer een specifieke toepassing in gebruik is

Identificeer of het probleem zich voordoet terwijl één toepassing of een paar ervan worden uitgevoerd als u in staat bent de kwestie te herhalen helpt in het proces van het identificeren van potentiële uitsluitingen.

Montagebundel voor diagnostiek voor analyse

Debug-niveau inschakelen

Om een nuttige diagnostische bundel te verzamelen, moet het debug logniveau worden geactiveerd.

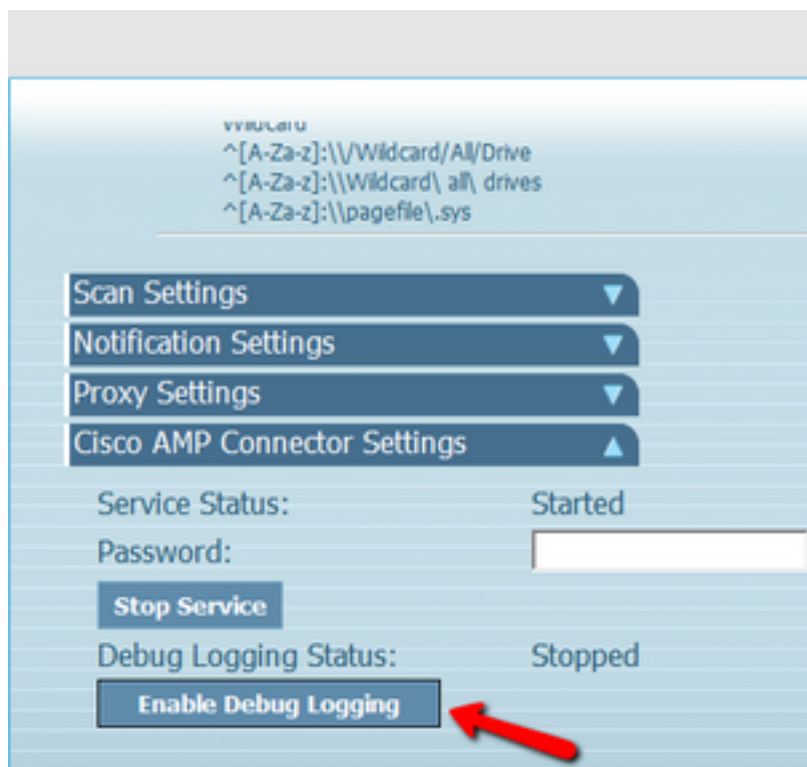
Debug Level in het eindpunt

Als u het probleem kunt reproduceren en toegang tot het eindpunt kunt hebben, is hieronder de beste procedure om het diagnostische bundel vast te leggen:

1. AMP GUI openen
2. Navigeren in **instellingen**
3. Scrollt naar de onderkant van AMP GUI en open **Cisco Advanced Malware Protection**

Connector-instellingen

4. Klik op **Debug Logging inschakelen**
5. De **Debug Logging Status** moet veranderen in **Start**. Deze procedure maakt het debug-niveau mogelijk tot de volgende beleidshartslag, standaard 15 minuten



Debug level in het beleid

Als u geen toegang hebt tot het eindpunt of de kwestie kan niet consistent worden gereproduceerd, moet het debug logniveau in het beleid worden geactiveerd.

Schakel het logniveau in door beleidsnavigatie naar **Beheer > Beleid > Bewerken > Geavanceerde instellingen > Aangepaste loginstellingen** en **Beheer > Beleid > Bewerken > Geavanceerde instellingen > Instellingen > tray-logniveau**, en selecteer vervolgens **bug** en stop het beleid, zoals in de afbeelding wordt weergegeven.

< Edit Policy

Windows

Name:

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

FEPA

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

Voorzichtig: Als de debug-modus van het beleid is ingeschakeld, ontvangen alle endpoints deze wijziging.

Opmerking: Sync het beleid van het eindpunt om te verzekeren dat het debug-niveau wordt toegepast of wacht op het hartslag-interval, door de standaardinstelling is het 15 minuten.

Reproduceert het probleem en verzamel een diagnostische bundel

Wanneer het debug-niveau is ingesteld, wacht dan tot de status Hoog CPU op het systeem aanwezig is of reproduceren handmatig de eerder geïdentificeerde voorwaarden en verzamelen vervolgens de diagnostische bundel.

Om de bundelnavigatie naar **C:\Program Files\Cisco\AMP\X.X.X** te verzamelen (Waar X.X.X de nieuwste AMP-versie is die op het systeem is geïnstalleerd) en de applicatie **ipsupporttool.exe** te starten maakt dit proces een **.7z**-bestand op het bureaublad met de naam **CiscoAMP_Support_Tool_%date%.7z**

Opmerking: Aansluitversie 6.2.3 en kan later op afstand om een bundel vragen, naar **Beheer > Computers** navigeren, de endpointrecord uitbreiden en de optie Diagnose gebruiken.

Opmerking: De diagnostische bundel kan ook vanuit een CMD-prompt met de opdracht

lopen: "C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe", of "C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To", waar X.X.X de nieuwste geïnstalleerde AMP-versie is, kan de tweede opdracht worden gebruikt om de uitvoermap voor het .7z-bestand te selecteren.

De analyse maken

Er zijn twee manieren om een diagnostisch bestand te analyseren:

- Diag_Analyzer.exe
- Ampzakje.ps1

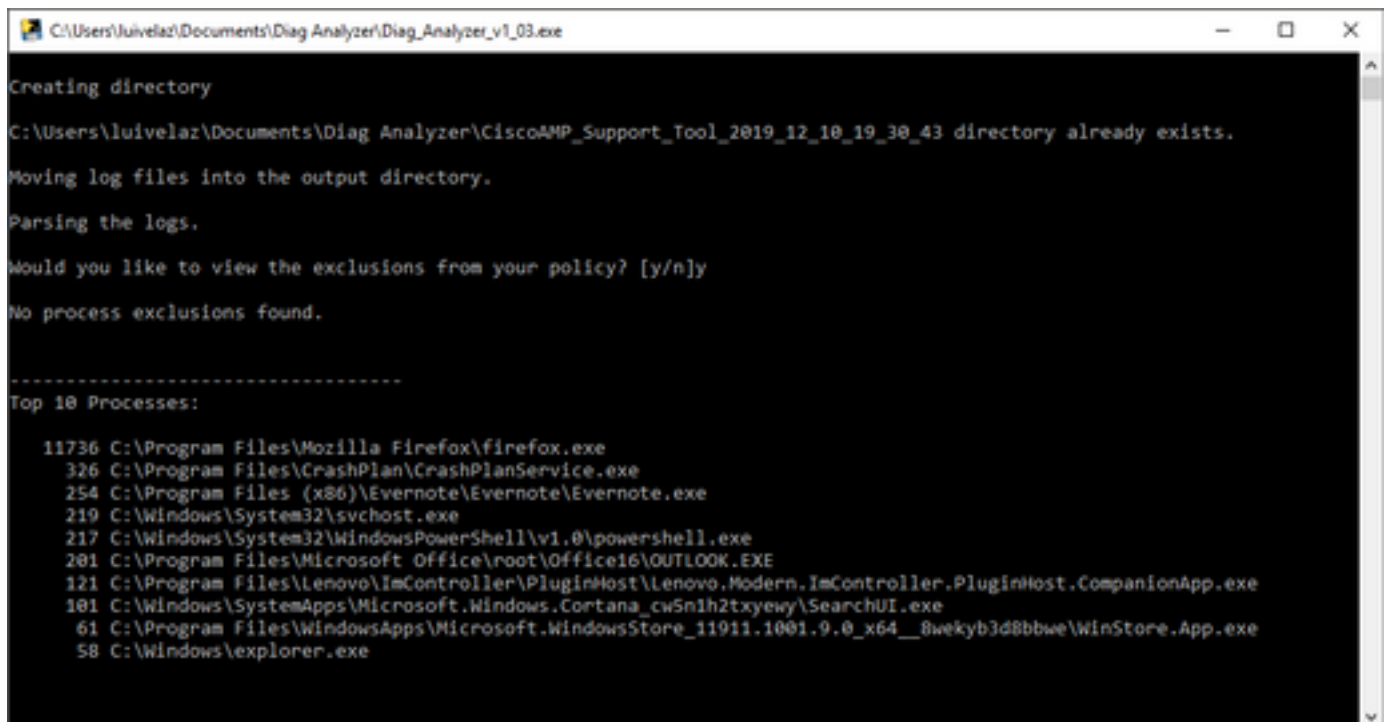
Diag_Analyzer.exe

Stap 1. Download de toepassing [hier](#).

Stap 2. Op de GitHub-pagina is er een README-bestand met verdere instructies over gebruik.

Stap 3. Kopieer het diagnostische bestand **CiscoAMP_Support_Tool_%date%.7z** in de map waarin Diag_Analyzer.exe zich bevindt.

Stap 4. Voer de toepassing uit **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
```

Stap 5. In de nieuwe melding bevestig als u de uitsluitingen van het beleid wilt krijgen met een Y of een N.

Stap 6. Het resultaat van het script bevat:

- Top 10 processen
- Bovenste 10 bestanden
- Top 10 uitbreidingen

- Bovenste 100 paden
- Alle bestanden

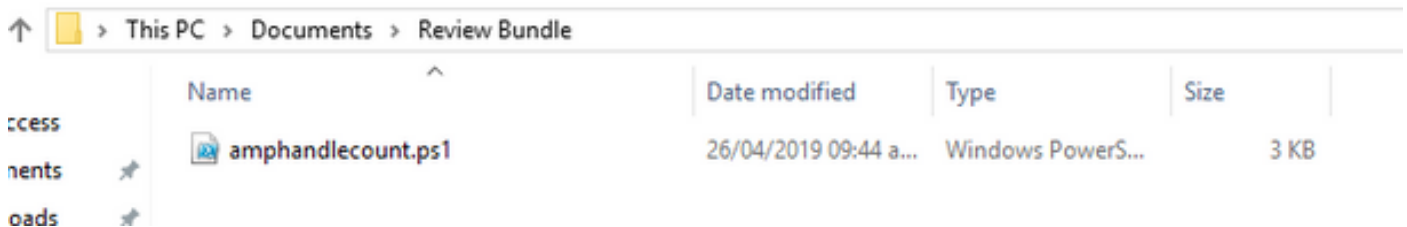
Opmerking: Diag_Analyzer.exe controleert het bijgeleverde diagnostische AMP-bestand voor bestanden van sfc.exe.log. creëert vervolgens een nieuwe folder met de diagnostische bestandsnaam en bewaart de logbestanden buiten de .7z, in de moederfolder van de diagnostiek, daarna, ontleedt het de logbestanden en bepaalt de top 10 processen, bestanden, extensies, en paden, tenslotte drukt het informatie op het scherm en ook op een {Diagnostic}-summary.txt bestand.

Ampzakje.ps1

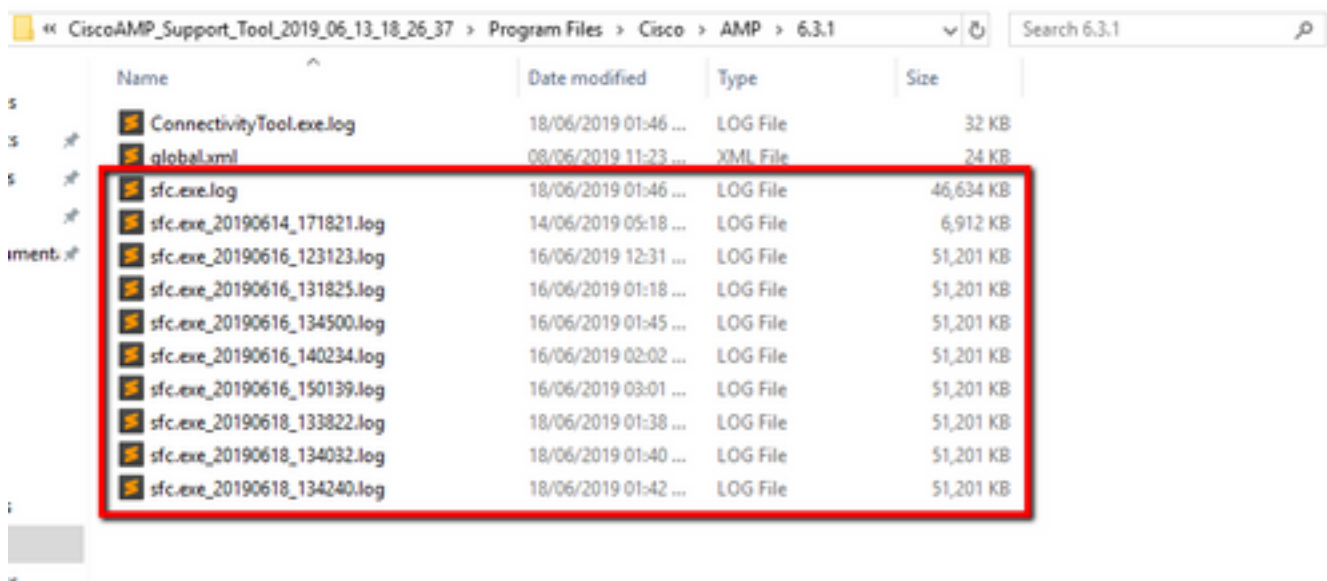
Stap 1. Download het script **amphandlecings.txt** van de onderkant van deze community post [Review Scanned Files van AMP](#).

Stap 2. Als u het script in Windows wilt uitvoeren, noemt u het opnieuw op **amphandlecount.ps1**.

Stap 3. Voor een gemak kopieert u **het** bestand **amphandbeleg.ps1** naar een eigen map.



Stap 4. Ontvang het **CiscoAMP_Support_Tool_%date%.7z**-bestand en identificeer de bestanden van **sfc.log** op het pad **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X**.



Stap 5. Kopieer de bestanden van **sfc.log** op de map **amphandlecount.ps1**.

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

Stap 6. Start **amphandlecount.ps1** met PowerShell en dan wordt een venster geopend en afhankelijk van het uitvoerbeleid op het eindpunt kan u om toestemming vragen om te starten.

Tip: Zo wijzigt u het uitvoerbeleid door een Windows PowerShell te openen en gebruikt u de volgende opdrachten:

Stel het beleid in om onbeperkte toegang tot executie mogelijk te maken - **Settopvoering - beleid - bereik van huidige gebruiker-executie - beleid onbeperkt**

Stel het beleid in om de toegang tot de uitvoering te beperken - **Set-executie-beleid - Reikwijdte-beleid voor huidige gebruiker-executie - beperkt**

Stap 7. Laat de PowerShell voltooiën (het kan enige tijd duren, afhankelijk van hoeveel sfc.log in de map zijn) na de PowerShell-voltooiing, worden er vier bestanden op de map aangemaakt:

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

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

Stap 8. De 4 nieuwe bestanden bevatten het resultaat van de analyse:

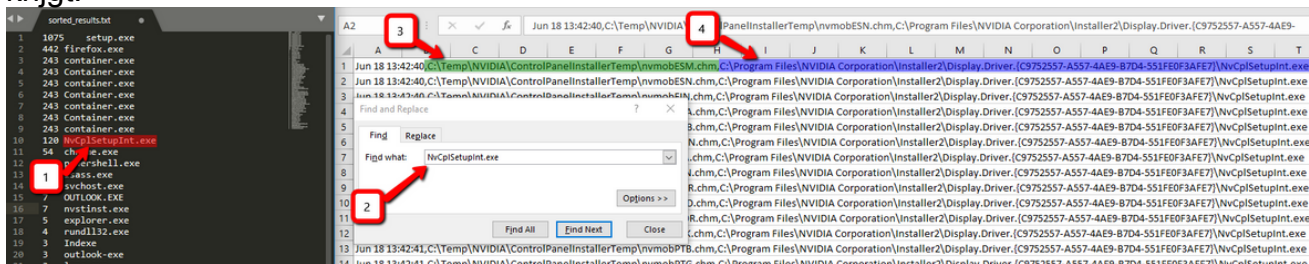
- **data.csv** : bevat het volledige pad van de gescande bestanden en het vader-proces dat het bestand aangemaakt/aangepast/verplaatst
- **results.txt**: bevat de lijst van processen die door AMP zijn gescand
- **leaving sorted_results.txt**: bevat de lijst van processen die door de AMP zijn gescand met het meest gescande proces
- **terms.txt**: bevat de naam van processen die door AMP zijn gescand

Stap 9. Filter de procesnaam met hoge tellingen van de **gesorteerde_resultaten.txt** in **data.csv** u kunt het ouderproces met zijn volledige pad identificeren en dan om een uitsluiting aan het beleid in een aangepaste lijst toe te voegen als het wordt vertrouwd.

Te bekijken processen:

1. Midden + F op "data.csv" en zoeken
2. Pad van het bestand dat door AMP is gescand
3. Pad van het ouderproces dat het bestand kopieert/verplaatst/aangepast

Opmerking: Opmerking: Meestal is de uitsluiting het type "proces: File Scan" met "Child Processing" voor het ouderproces dat de scans krijgt:



Opmerking: [Hier](#) vindt u meer informatie over de beste praktijken om uitsluitingen te creëren.

Tune-uitsluitingen

Zodra de processen of paden worden geïdentificeerd, kunt u ze toevoegen aan de uitsluitingslijst die gekoppeld is aan het beleid dat op het eindpunt wordt toegepast, **navigeer** naar **Beheer > Uitsluitingen > Uitsluitingsnaam > Bewerken**, zoals in de afbeelding wordt getoond.

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	

Vermeld de bundel voor analyse aan TAC

ATS TAC kan helpen om deze scenario's te verhelpen, als dat het geval is, bent u bereid om de volgende informatie te verstrekken bij het maken van een case:

- Wanneer begint dit probleem?
- Is er recentelijk verandering?
- Wordt de kwestie met een specifieke toepassing geregeld? Zo ja, welke toepassing?
- Is er nog een antivirus op het systeem? Zo ja, welk antivirus?
- Verzamel een debug bundel terwijl het probleem is gereproduceerd: [Stappen om een debug-bundel te verzamelen](#)