

Analyse des AMP-Diagnosepakets für hohe CPU-Auslastung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Fehlerbehebung](#)

[Überprüfen Sie, ob ein anderer Virenschutz auf dem Computer installiert ist](#)

[Ermitteln Sie, ob die hohe CPU bei Verwendung einer bestimmten Anwendung auftritt.](#)

[Sammeln Sie Diagnosepaket zur Analyse](#)

[Debug-Protokollebene aktivieren](#)

[Debugebene im Endpunkt](#)

[Debugebene in der Richtlinie](#)

[Reproduzieren Sie das Problem, und sammeln Sie ein Diagnosepaket.](#)

[Analyse durchführen](#)

[Diag_Analyzer.exe](#)

[Amphandlecount1](#)

[Tune-Ausschlüsse](#)

[Senden Sie das Paket zur Analyse an das TAC](#)

Einführung

In diesem Dokument werden die Schritte zur Analyse eines Diagnosepakets von Advanced Malware Protection (AMP) für Endgeräte Public Cloud auf Windows-Geräten beschrieben, um eine Fehlerbehebung bei hoher CPU-Auslastung zu ermöglichen.

Verfasst von Luis Velazquez und herausgegeben von Yeraldin Sánchez, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Zugriff auf die AMP-Konsole

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AMP für Endgeräte Konsole 5.4.2020204
- Windows-Betriebssystemgeräte

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

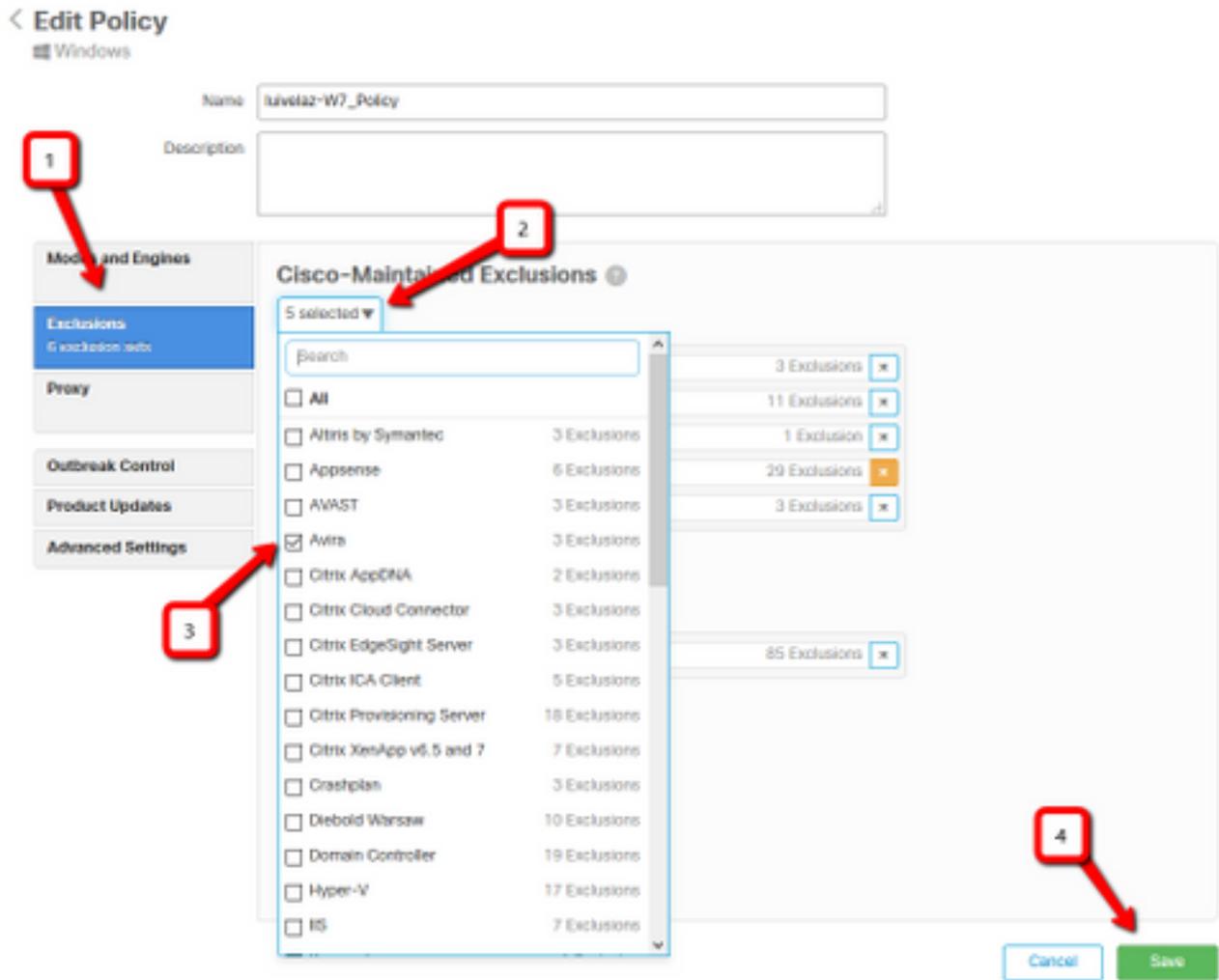
Überprüfen Sie, ob ein anderer Virenschutz auf dem Computer installiert ist

Wenn eine andere Antivirus-Software (Antivirus) installiert ist, stellen Sie sicher, dass der Hauptprozess der Virenschutzfunktion in der Richtlinienkonfiguration ausgeschlossen ist.

Tipp: Verwenden Sie die von Cisco verwalteten Ausschlüsse, wenn die verwendete Software in der Liste enthalten ist. Denken Sie daran, dass diese Ausschlüsse neuen Versionen einer Anwendung hinzugefügt werden können.

Um die Listen anzuzeigen, die im von Cisco verwalteten Ausschlussbereich verfügbar sind, navigieren Sie zu **Management > Policies > Edit > Exclusions > Cisco Maintained Exclusions**.

Wählen Sie die Geräte aus, die Ihr Endgerät benötigt, entsprechend der aktuell auf dem Computer installierten Software. Speichern Sie dann die Richtlinie, wie im Bild gezeigt.



Ermitteln Sie, ob die hohe CPU bei Verwendung einer bestimmten Anwendung auftritt.

Identifizieren Sie, ob das Problem auftritt, während eine oder mehrere Anwendungen ausgeführt werden, wenn Sie das Problem replizieren können, um potenzielle Ausschlüsse zu identifizieren.

Sammeln Sie Diagnosepaket zur Analyse

Debug-Protokollebene aktivieren

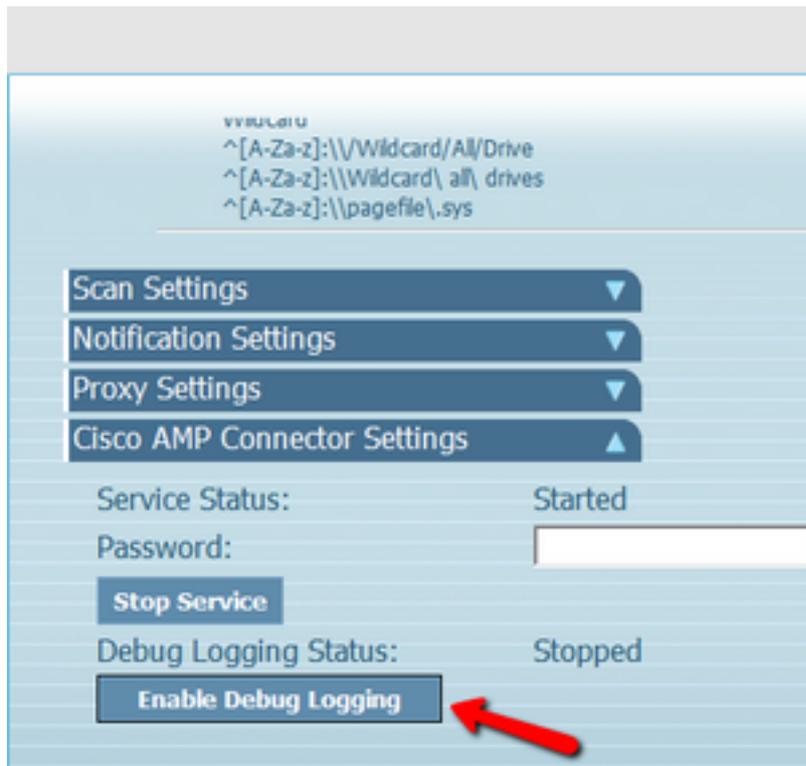
Um ein nützliches Diagnosepaket zu erfassen, muss die Debug-Protokollstufe aktiviert sein.

Debugebene im Endpunkt

Wenn Sie das Problem replizieren können und Zugriff auf den Endpunkt haben, ist die folgende Vorgehensweise die beste, um das Diagnosepaket zu erfassen:

1. AMP-GUI öffnen
2. Navigieren Sie zu **Einstellungen**.
3. Navigieren Sie zum unteren Rand der AMP-GUI, und öffnen Sie die **Cisco AMP Connector-Einstellungen**.
4. Klicken Sie auf **Debug-Protokollierung aktivieren**.

5. Der **Debug-Protokollierungsstatus** muss in **Started (Gestartet)** geändert werden. Diese Prozedur aktiviert die Debugging-Stufe bis zum nächsten Richtlinienheartbeat (standardmäßig 15 Minuten).



Debugebene in der Richtlinie

Wenn Sie keinen Zugriff auf den Endpunkt haben oder das Problem nicht konsistent reproduziert werden kann, muss die Debug-Protokollebene in der Richtlinie aktiviert sein.

Um die Debug-Protokollstufe durch Richtlinien zu aktivieren, navigieren Sie zu **Management > Policies > Edit > Advanced Settings > Connector Log Level** und **Management > Policies > Edit > Advanced Settings > Tray Log Level**, wählen Sie **Debug (Debuggen)** aus, und speichern Sie die Richtlinie, wie im Bild gezeigt.

< 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 ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

Enable Connector Protection ⓘ

Connector Protection Password ⓘ

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

Vorsicht: Wenn der Debug-Modus aus der Richtlinie aktiviert ist, erhalten alle Endpunkte diese Änderung.

Hinweis: Synchronisieren Sie die Richtlinie des Endpunkts, um sicherzustellen, dass die Debugging-Stufe angewendet wird, oder warten Sie auf das Heartbeat-Intervall, standardmäßig ist es 15 Minuten.

Reproduzieren Sie das Problem, und sammeln Sie ein Diagnosepaket.

Wenn die Debugging-Ebene konfiguriert ist, warten Sie, bis der Status der High CPU auf dem System auftritt, oder reproduzieren Sie manuell die zuvor identifizierten Bedingungen, und sammeln Sie dann das Diagnosepaket.

Um das Paket zu sammeln, navigieren Sie zu **C:\Program Files\Cisco\AMP\X.X.X** (wobei X.X.X die neueste auf dem System installierte AMP-Version ist) und führen Sie die Anwendung **ipsupporttool.exe** aus. Dieser Vorgang erstellt eine .7z-Datei auf dem Desktop mit dem Namen **CiscoAMP_Support_Tool_%date%.7z**.

Hinweis: Connector Version 6.2.3 und höher kann ein Paket remote anfordern, zu **Management > Computers** navigieren, den Endpunktdatensatz erweitern und die Option **Diagnose** verwenden.

Hinweis: Das Diagnosepaket kann auch über eine CMD-Eingabeaufforderung mit dem folgenden Befehl ausgeführt werden: "**C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe**", oder "**C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe**" -oder "**X:\Folder\I\Can\Get\To**", wobei X.X.X die neueste installierte AMP-Version ist, kann der zweite Befehl verwendet werden, um den Ausgabeordner für die 7z-Datei auszuwählen.

Analyse durchführen

Eine Diagnosedatei kann auf zwei Arten analysiert werden:

- Diag_Analyzer.exe
- Amphandlecount1

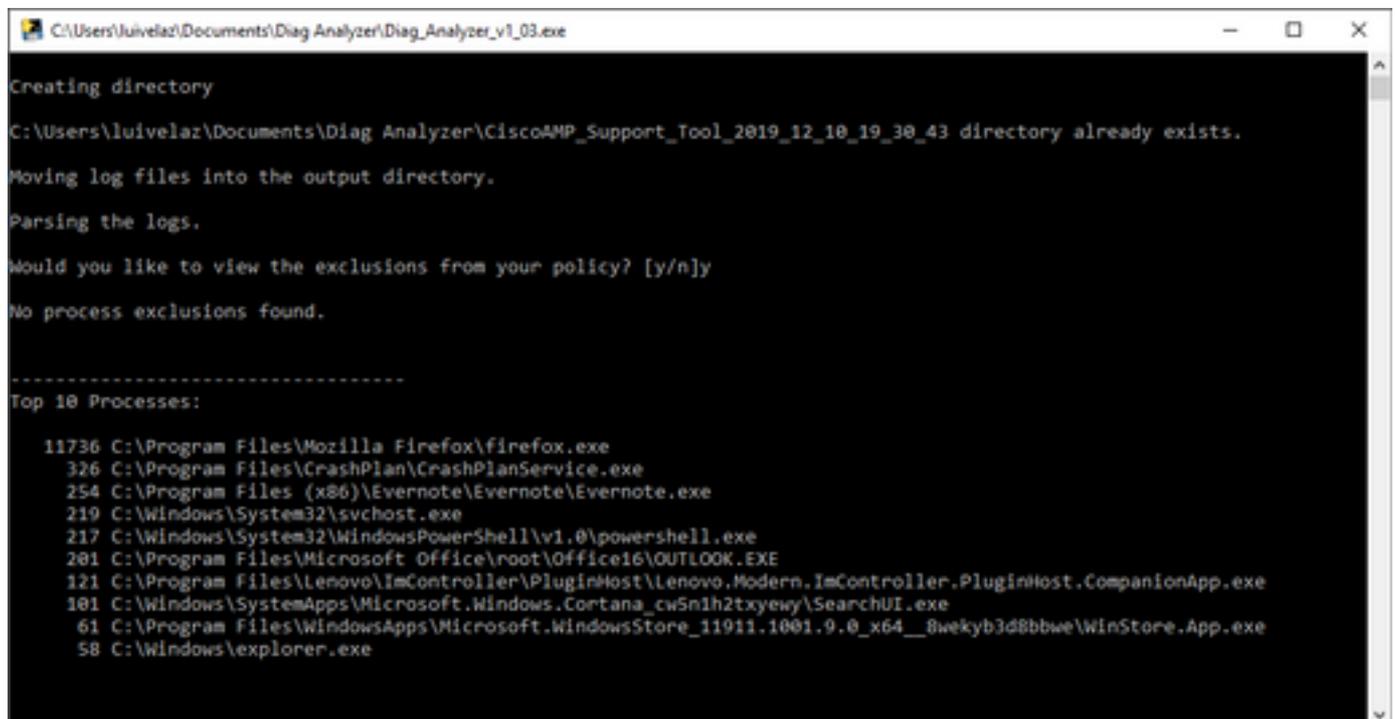
Diag_Analyzer.exe

Schritt 1: Laden Sie die Anwendung [hier herunter](#).

Schritt 2: Auf der GitHub-Seite gibt es eine README-Datei mit weiteren Anweisungen zur Verwendung.

Schritt 3: Kopieren Sie die Diagnosedatei `CiscoAMP_Support_Tool_%date%.7z` in denselben Ordner wie `Diag_Analyzer.exe`.

Schritt 4: Ausführen der Anwendung `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
```

Schritt 5: Bestätigen Sie in der neuen Eingabeaufforderung, ob Sie die Ausschlüsse von der Richtlinie mit einem **Y** oder einem **N** erhalten möchten.

Schritt 6: Das Skriptergebnis enthält:

- Top 10 Prozesse

- Top 10 Dateien
- Top 10-Erweiterungen
- Top 100 Pfade
- Alle Dateien

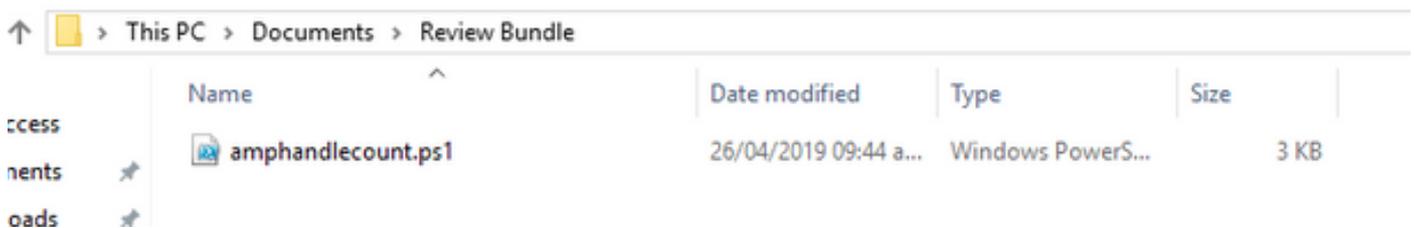
Hinweis: Diag_Analyzer.exe überprüft die mitgelieferte AMP-Diagnosedatei auf Dateien von sfc.exe.log. erstellt dann ein neues Verzeichnis mit dem Namen der Diagnosedatei und speichert die Protokolldateien außerhalb der 0,7 z, im übergeordneten Verzeichnis der Diagnosedatei. Anschließend analysiert es die Protokolle und bestimmt die 10 wichtigsten Prozesse, Dateien, Erweiterungen und Pfade. Schließlich werden Informationen an den Bildschirm und auch an eine {Diagnostic}-summary.txt-Datei ausgegeben.

Amphandlecount1

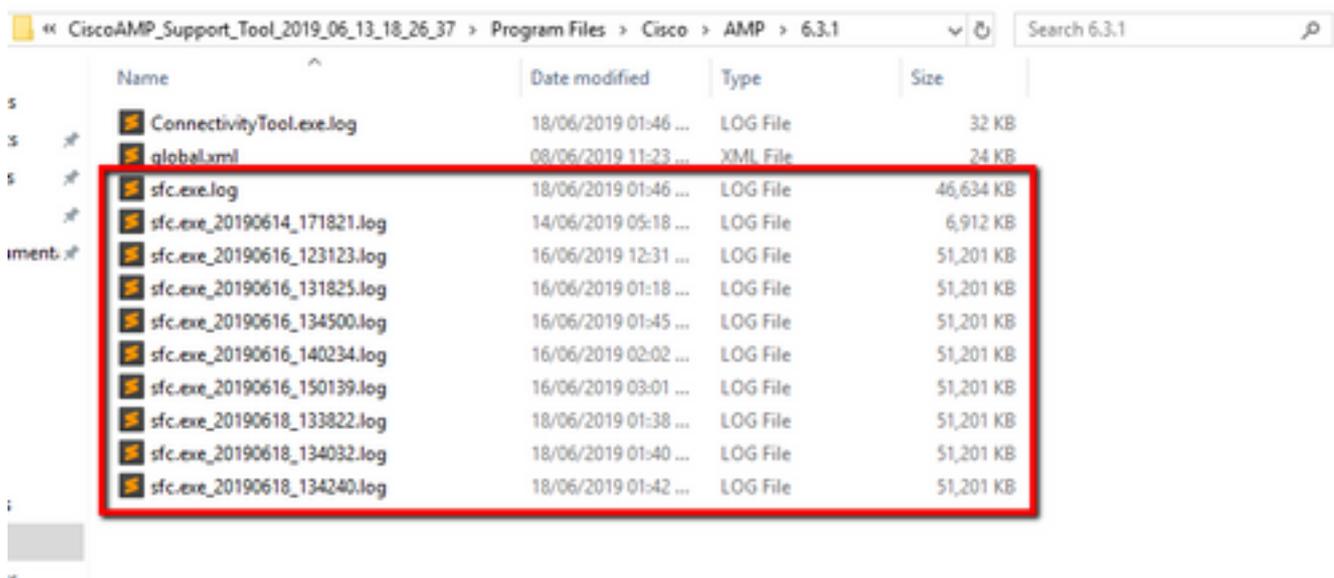
Schritt 1: Laden Sie das Skript **amphandlecounts.txt** unten in diesem Community-Beitrag [Prüfen Sie die geprüften Dateien von AMP.](#)

Schritt 2: Um das Skript in Windows auszuführen, benennen Sie es in **amphandlecount.ps1** um.

Schritt 3: Kopieren Sie die **Datei amphandlecount.ps1** in einen eigenen Ordner.



Schritt 4: Entpacken Sie die **CiscoAMP_Support_Tool_%date%.7z**-Datei, und identifizieren Sie die **sfc.log**-Dateien im Pfad. **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Programm Files\Cisco\AMP\X.X.X**.



Schritt 5: Kopieren Sie die Dateien von **sfc.log** in den Ordner **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

Schritt 6: Führen Sie **amphandlecount.ps1** mit PowerShell aus, dann wird ein Fenster geöffnet, und abhängig von der Ausführungsrichtlinie des Endpunkts kann die Berechtigung zum Ausführen angefordert werden.

Tipp: Um die Ausführungsrichtlinie zu ändern, öffnen Sie eine Windows PowerShell, und verwenden Sie die folgenden Befehle:

Legen Sie die Richtlinie so fest, dass uneingeschränkter Ausführungszugriff zulässig ist - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**

Legen Sie die Richtlinie fest, um den Ausführungszugriff zu beschränken - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

Schritt 7: Warten Sie, bis die PowerShell abgeschlossen ist (es kann einige Zeit dauern, je nachdem, wie viele sfc.log sich im Ordner befinden), nachdem die PowerShell abgeschlossen ist, werden vier Dateien im Ordner erstellt:

- 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

Schritt 8: Die vier neuen Dateien enthalten das Ergebnis der Analyse:

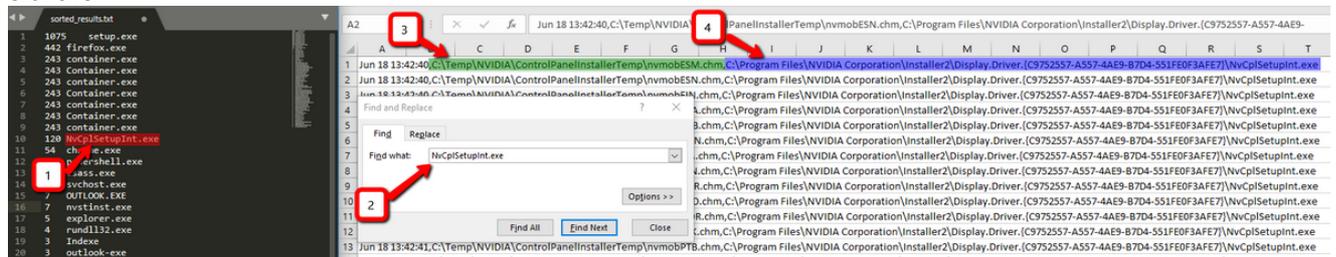
- **data.csv**: enthält den vollständigen Pfad der gescannten Dateien und den Vater-Prozess, der die Datei erstellt/geändert/verschoben hat.
- **results.txt**: Enthält die Liste der Prozesse, die von AMP gescannt werden.
- **sorted_results.txt**: enthält die Liste der Prozesse, die von AMP mit dem am meisten gescannten Prozess gescannt werden.
- **terms.txt**: Enthält den Namen der von AMP gescannten Prozesse

Schritt 9: Filtern Sie den Prozessnamen mit hohen Zählungen aus der **sorted_results.txt** in der Datei **data.csv**, um den übergeordneten Prozess mit seinem vollständigen Pfad zu identifizieren, und fügen Sie dann der Richtlinie in einer benutzerdefinierten Liste einen Ausschluss hinzu, wenn er vertrauenswürdig ist.

Zu schauende Prozesse:

1. Strg + F auf "data.csv" und Suche
2. Pfad der von AMP gescannten Datei
3. Pfad des übergeordneten Prozesses, der die Datei kopiert/verschoben/geändert hat

Hinweis: Hinweis: In der Regel ist der Ausschluss der Typ "Prozess: Dateiprüfung" mit "Untergeordnete Prozesse beinhalten" für den übergeordneten Prozess, der die Prüfungen abrufen:



Hinweis: [Hier](#) finden Sie weitere Informationen zu Best Practices für die Erstellung von Ausschlüssen.

Tune-Ausschlüsse

Nachdem die Prozesse oder Pfade identifiziert wurden, können Sie sie der Ausschlussliste hinzufügen, die mit der auf den Endpunkt angewendeten Richtlinie verknüpft ist. Navigieren Sie zu **Management > Exclusions > Exclusion name > Edit (Verwaltung > Ausschlüsse > Ausschlussname > Bearbeiten)**, wie im Bild gezeigt.

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	

[+ Add Exclusion](#) [+ Add Multiple Exclusions...](#) [Revert Changes](#) [Save](#)

Senden Sie das Paket zur Analyse an das TAC

ATS TAC kann bei der Fehlerbehebung in diesen Szenarien helfen. Falls dies der Fall ist, geben Sie bei der Erstellung des Falls die nächsten Informationen an:

- Wann beginnt dieses Problem?
- Gibt es irgendwelche Änderungen in letzter Zeit?
- Tritt das Problem bei einer bestimmten Anwendung auf? Wenn ja, welche Anwendung?
- Gibt es andere Virenschutzprogramme auf dem System? Wenn ja, welche Antivirensoftware?
- Sammeln Sie ein Debug-Paket, während das Problem reproduziert wird: [Schritte zum Sammeln eines Debugpakets](#)