

Analyser l'ensemble de diagnostics AMP pour CPU élevé

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Dépannage](#)

[Vérifier si un autre antivirus est installé sur l'ordinateur](#)

[Identifier si le CPU élevé se produit lorsqu'une application spécifique est en cours d'utilisation](#)

[Collecter un ensemble de diagnostics pour l'analyse](#)

[Activer le niveau du journal de débogage](#)

[Niveau de débogage dans le point de terminaison](#)

[Niveau de débogage dans la stratégie](#)

[Reproduire le problème et rassembler une offre de diagnostic](#)

[Analyser](#)

[Diag Analyser.exe](#)

[Amphandlecount.ps1](#)

[Régler les exclusions](#)

[Envoyer l'offre groupée pour analyse au TAC](#)

Introduction

Ce document décrit les étapes à suivre pour analyser un ensemble de diagnostics à partir d'Advanced Malware Protection (AMP) for Endpoints Public Cloud on Windows afin de dépanner une utilisation élevée du CPU.

Contribué par Luis Velazquez et édité par Yeraldin Sánchez, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès à la console AMP

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console AMP for Endpoints 5.4.20200204
- Périphériques du système d'exploitation Windows

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

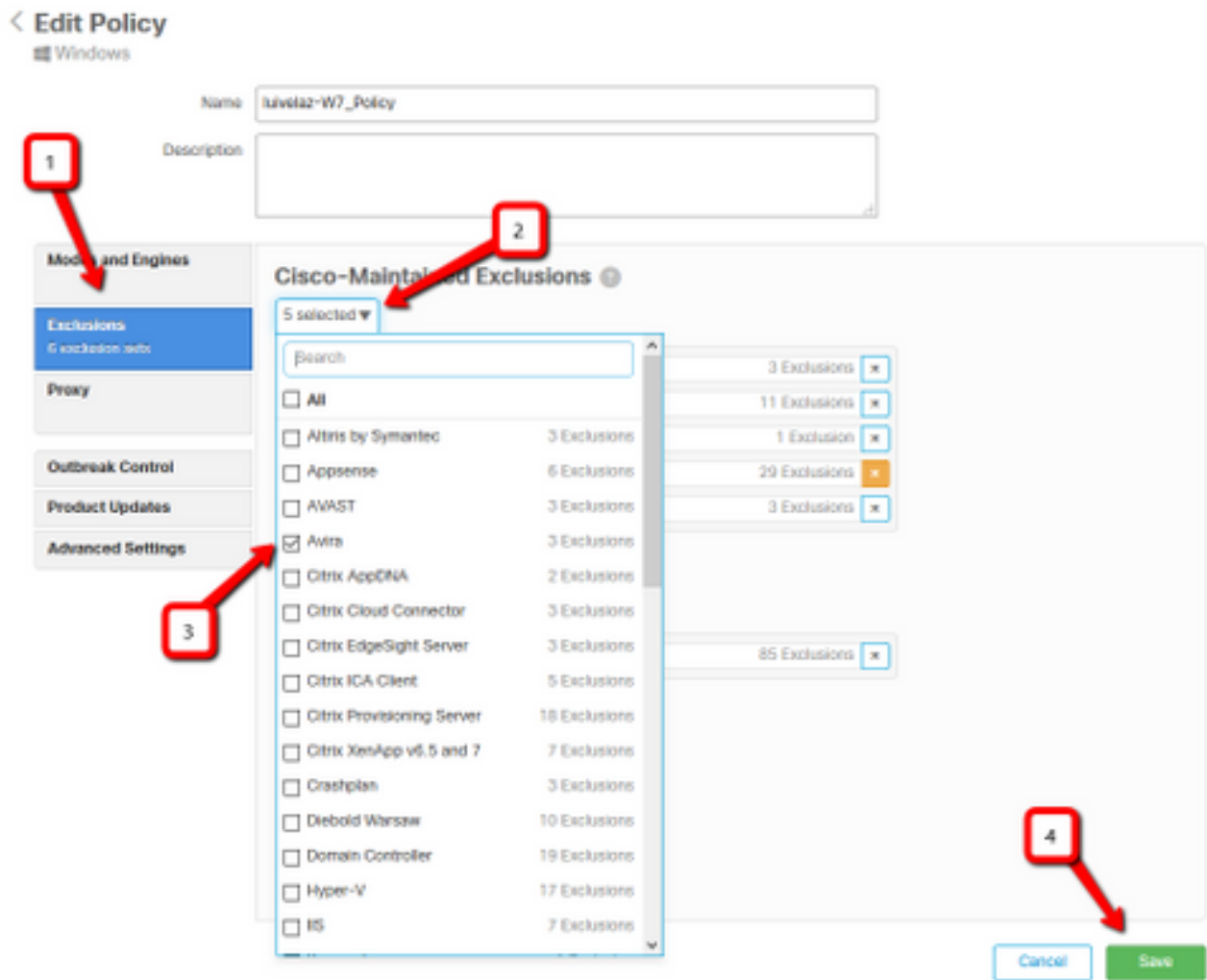
Vérifier si un autre antivirus est installé sur l'ordinateur

Si un autre antivirus est installé, assurez-vous que le processus principal de l'antivirus est exclu dans la configuration de la stratégie

Astuce : Utilisez les exclusions maintenues par Cisco si le logiciel utilisé est inclus dans la liste, souvenez-vous que ces exclusions peuvent être ajoutées aux nouvelles versions d'une application.

Afin de voir les listes disponibles dans la section Exclusions gérées par Cisco, accédez à **Management > Politiques > Edit > Exclusions > Exclusions gérées par Cisco**.

Sélectionnez ceux dont votre point de terminaison aurait besoin en fonction du logiciel actuellement installé sur l'ordinateur, puis enregistrez la stratégie, comme illustré dans l'image.



Identifier si le CPU élevé se produit lorsqu'une application spécifique est en cours d'utilisation

Déterminez si le problème se produit lors de l'exécution d'une application ou de quelques-unes d'entre elles si vous êtes en mesure de reproduire le problème aide à identifier les exclusions potentielles.

Collecter un ensemble de diagnostics pour l'analyse

Activer le niveau du journal de débogage

Afin de collecter un ensemble de diagnostics utile, le niveau du journal de débogage doit être activé.

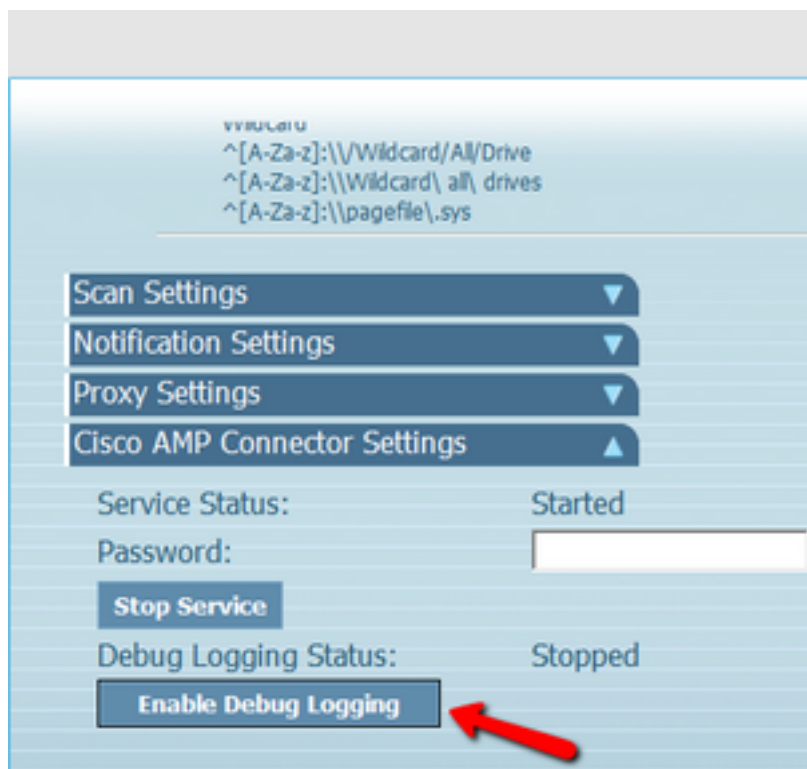
Niveau de débogage dans le point de terminaison

Si vous pouvez répliquer le problème et avoir accès au point de terminaison, voici la meilleure procédure pour capturer l'ensemble de diagnostics :

1. Ouvrir l'interface graphique AMP
2. Accéder aux **paramètres**
3. Faites défiler l'écran jusqu'en bas de l'interface utilisateur graphique AMP et ouvrez **Cisco**

AMP Connector Settings.

4. Cliquez sur **Activer la journalisation du débogage**
5. **L'état de journalisation du débogage** doit passer à **Démarré**. Cette procédure active le niveau de débogage jusqu'à la prochaine pulsation de stratégie, par défaut, 15 minutes



Niveau de débogage dans la stratégie

Si vous n'avez pas accès au point de terminaison ou si le problème ne peut pas être reproduit de manière cohérente, le niveau du journal de débogage doit être activé dans la stratégie.

Afin d'activer le niveau du journal de débogage par stratégie, accédez à Management > Politiques > Edit > Advanced Settings > Connector **Log Level** and Management > Politiques > Edit > Advanced Settings > Tray Log Level, puis sélectionnez Debug et enregistrez la stratégie, comme indiqué dans l'image.

< Edit Policy

Windows

Name: iulvaz-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

Orbitat

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

Attention : Si le mode de débogage est activé à partir de la stratégie, tous les points de terminaison reçoivent cette modification.

Note: Synchronisez la stratégie du point de terminaison pour vous assurer que le niveau de débogage est appliqué ou attendez l'intervalle de pulsation, par défaut il est de 15 minutes.

Reproduire le problème et rassembler une offre de diagnostic

Lorsque le niveau de débogage est configuré, attendez que l'état du CPU élevé se produise sur le système ou reproduisez manuellement les conditions précédemment identifiées, puis rassemblez le bundle de diagnostic.

Afin de collecter le bundle, accédez à **C:\Program Files\Cisco\AMP\X.X.X** (X.X.X est la dernière version d'AMP installée sur le système) et exécutez l'application **ipsupporttool.exe** ce processus crée un fichier **.7z** sur le bureau nommé **CiscoAMP_Support_Tool_%date%.7z**

Note: Connector version 6.2.3 et ultérieure peut demander un bundle à distance, accéder à **Management > Computers**, développer l'enregistrement du point d'extrémité et utiliser l'option Diagnose.

Note: L'ensemble de diagnostics peut également s'exécuter à partir d'une invite CMD avec la

commande suivante : "C:\Program Files\Cisco\AMP\X.X.X\lipsupporttool.exe », ou "C:\Program Files\Cisco\AMP\X.X.X\lipsupporttool.exe » -o "X:\Folder\Can\Get\To", où X.X.X est la dernière version d'AMP installée, la deuxième commande peut être utilisée afin de sélectionner le dossier de sortie pour le fichier .7z.

Analyser

Il existe deux façons d'analyser un fichier de diagnostic :

- Diag_Analyser.exe
- Amphandlecount.ps1

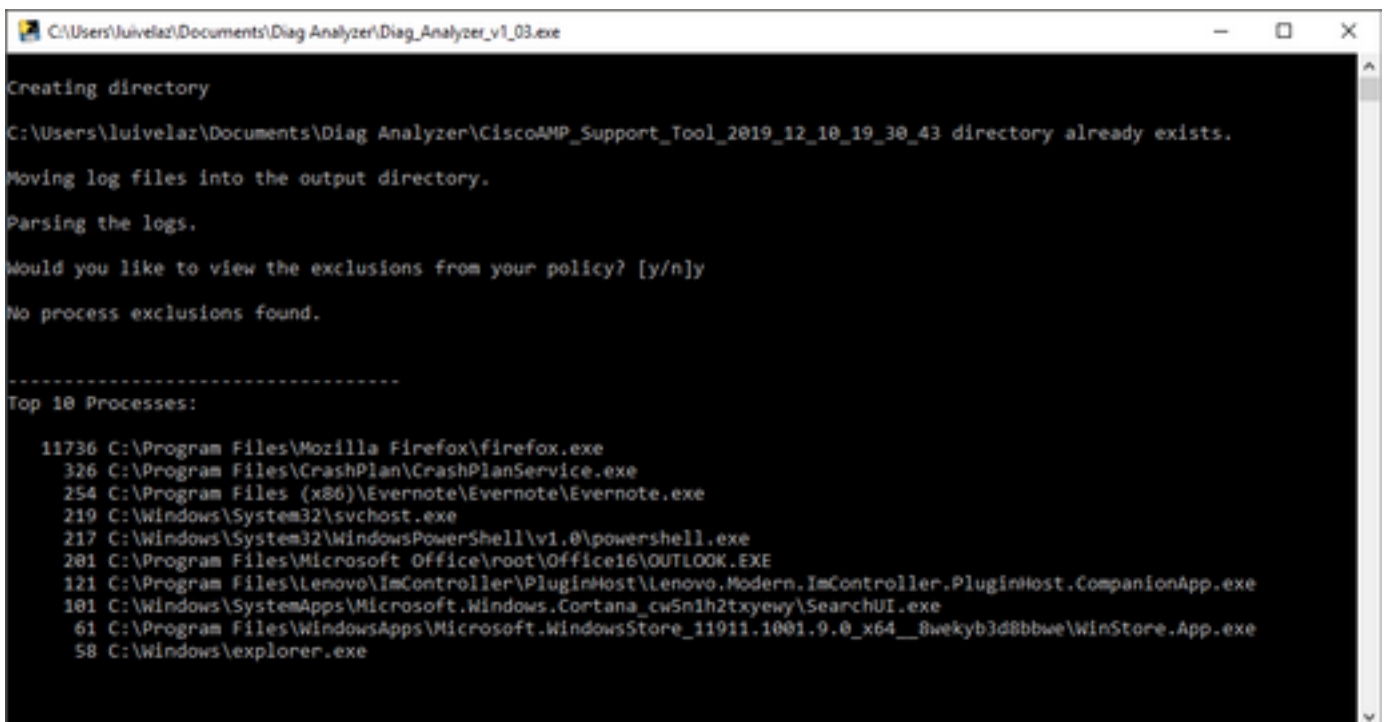
Diag_Analyser.exe

Étape 1. Téléchargez l'application [ici](#).

Étape 2. Dans la page GitHub, un fichier README contient des instructions supplémentaires sur l'utilisation.

Étape 3. Copiez le fichier de diagnostic CiscoAMP_Support_Tool_%date%.7z sur le même dossier que Diag_Analyser.exe.

Étape 4. Exécuter l'application Diag_Analyser.exe.



```
C:\Users\luivelaz\Documents\Diag Analyzer\Diag_Analyser_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
```

Étape 5. Dans la nouvelle invite, confirmez si vous voulez obtenir les exclusions de la stratégie avec un Y ou un N.

Étape 6. Le résultat du script contient :

- Les 10 principaux processus
- Les 10 premiers fichiers

- 10 postes principaux
- 100 principaux chemins
- Tous les fichiers

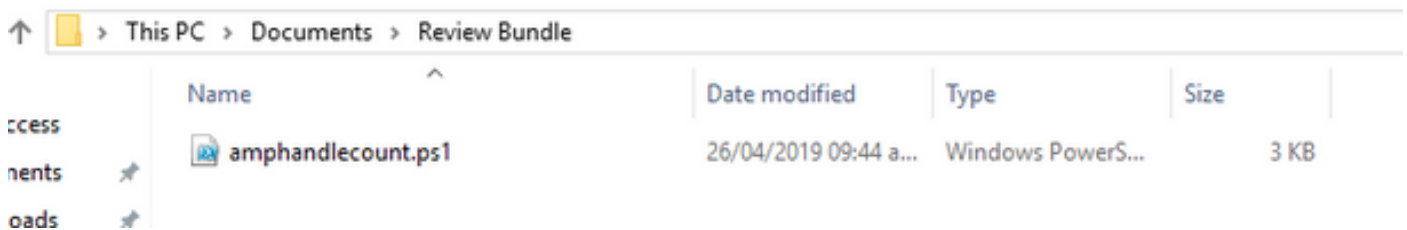
Note: Diag_Analyser.exe recherche les fichiers sfc.exe.log dans le fichier de diagnostic AMP fourni. ensuite, crée un nouveau répertoire avec le nom du fichier de diagnostic et stocke les fichiers journaux en dehors du .7z, dans le répertoire parent du diagnostic, après cela, il analyse les journaux et détermine les 10 principaux processus, fichiers, extensions et chemins, enfin, il imprime les informations à l'écran et aussi à un fichier {Diagnostic}-summary.txt.

Amphandlecount.ps1

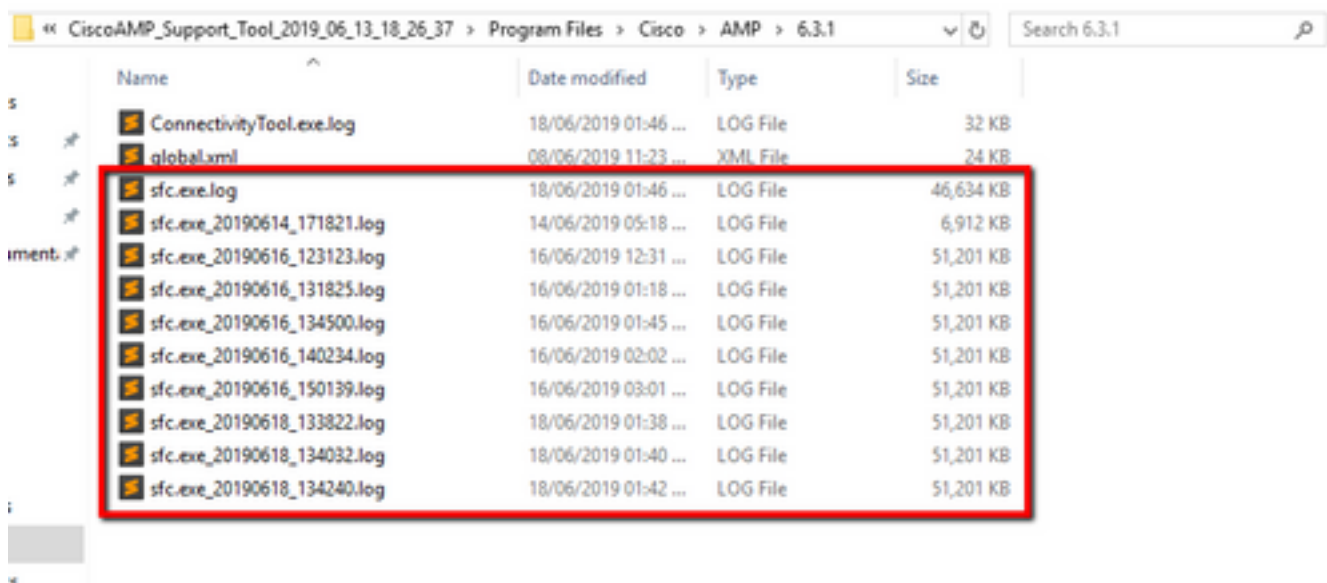
Étape 1. Téléchargez le script **amphandlecounts.txt** depuis le bas de ce billet communautaire [Revoir les fichiers analysés depuis AMP.](#)

Étape 2. Pour exécuter le script dans Windows, renommez-le **amphandlecount.ps1**.

Étape 3. Pour plus de commodité, copiez le fichier **amphandlecount.ps1** dans un dossier qui lui est propre.



Étape 4. Décompressez le fichier **CiscoAMP_Support_Tool_%date%.7z** et identifiez les fichiers **sfc.log** sur le chemin d'accès **Outil_Support_CiscoAMP_2019_06_13_18_26_37\Programme Files\Cisco\AMPX.X.X**.



Étape 5. Copiez les fichiers **sfc.log** dans le dossier **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

Étape 6. Exécutez **amphandlecount.ps1** avec PowerShell, puis une fenêtre est ouverte et selon la stratégie d'exécution sur le point de terminaison peut demander l'autorisation d'exécution.

Astuce : Afin de modifier la stratégie d'exécution, ouvrez un Windows PowerShell et utilisez les commandes suivantes :

Définissez la stratégie pour autoriser l'accès à l'exécution sans restriction - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unlimited**

Définir la stratégie pour restreindre l'accès à l'exécution - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restreint**

Étape 7. Autoriser la fin de PowerShell (cela peut prendre un certain temps, selon le nombre de sfc.log dans le dossier) après la fin de PowerShell, quatre fichiers sont créés sur le dossier :

- données.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

Étape 8. Les 4 nouveaux fichiers contiennent le résultat de l'analyse :

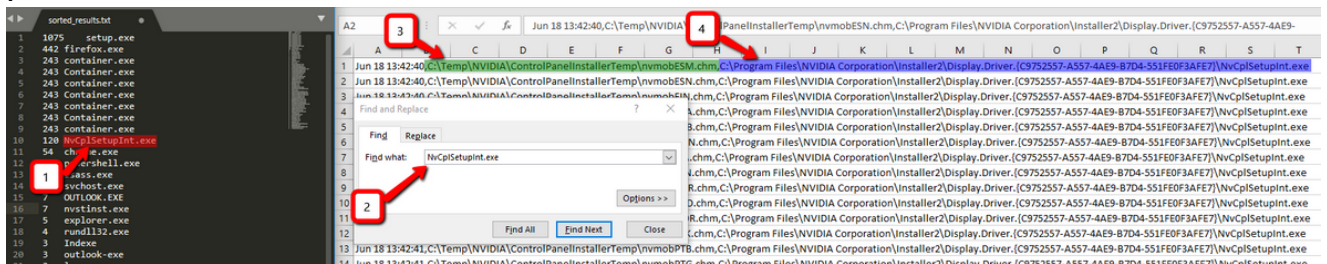
- **data.csv** : contient le chemin complet des fichiers analysés et le processus père qui a créé/modifié/déplacé le fichier
- **result.txt** : contient la liste des processus analysés par AMP
- **sorted_results.txt**: contient la liste des processus analysés par AMP avec le processus le plus analysé
- **terms.txt** : contient le nom des processus analysés par AMP

Étape 9. Filtrez le nom du processus avec des nombres élevés dans le fichier **sorted_results.txt** dans **data.csv** pour identifier le processus parent avec son chemin complet, puis ajoutez une exclusion à la stratégie dans une liste personnalisée si elle est approuvée.

Processus à rechercher :

1. Ctrl + F sur « data.csv » et rechercher
2. Chemin du fichier analysé par AMP
3. Chemin du processus parent qui copie/déplace/modifie le fichier

Note: Note: Généralement, l'exclusion est le type « Processus : Analyse de fichier » avec « Les processus enfants incluent » pour le processus parent qui reçoit les analyses



Note: [Ici](#) vous trouverez plus d'informations sur les meilleures pratiques pour créer des exclusions.

Régler les exclusions

Une fois les processus ou chemins identifiés, vous pouvez les ajouter à la liste d'exclusion liée à la stratégie appliquée sur le point de terminaison, accédez à **Management > Exclusions > Exclusion name > Edit**, comme indiqué dans l'image.

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	

Envoyer l'offre groupée pour analyse au TAC

Le TAC ATS peut vous aider à dépanner ces scénarios, si c'est le cas, soyez prêt à fournir les informations suivantes lors de la création du dossier :

- Quand commence ce problème ?
- Y a-t-il eu des changements récents ?
- Le problème se produit-il avec une application particulière ? Dans l'affirmative, quelle demande ?
- Y a-t-il un autre antivirus sur le système ? Si oui, quel antivirus ?
- Collecter un bundle de débogage pendant la reproduction du problème : [Étapes de collecte d'un bundle de débogage](#)