

CPU高使用率のAMP診断バンドルの分析

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[トラブルシューティング](#)

[別のウイルス対策がマシンにインストールされているかどうかを確認します](#)

[特定のアプリケーションが使用中のときにCPU使用率が高くなったかどうかを確認します](#)

[分析のための診断バンドルの収集](#)

[デバッグログレベルの有効化](#)

[エンドポイントのデバッグレベル](#)

[ポリシーのデバッグレベル](#)

[問題を再現し、診断バンドルを収集する](#)

[分析する](#)

[Diag_Analyzer.exe](#)

[Amphandlecount.ps1](#)

[除外の調整](#)

[分析のためにバンドルをTACに送信します。](#)

概要

このドキュメントでは、Windowsデバイス上のエンドポイントのパブリッククラウド向け Advanced Malware Protection(AMP)から診断バンドルを分析し、CPUの高使用率をトラブルシューティングする手順について説明します。

著者 : Cisco TACエンジニア、Luis Velazquez、編集 : Yeraldin Sanchez

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AMPコンソールへのアクセス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AMP for Endpointsコンソール5.4.20200204
- Windowsオペレーティングシステムデバイス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

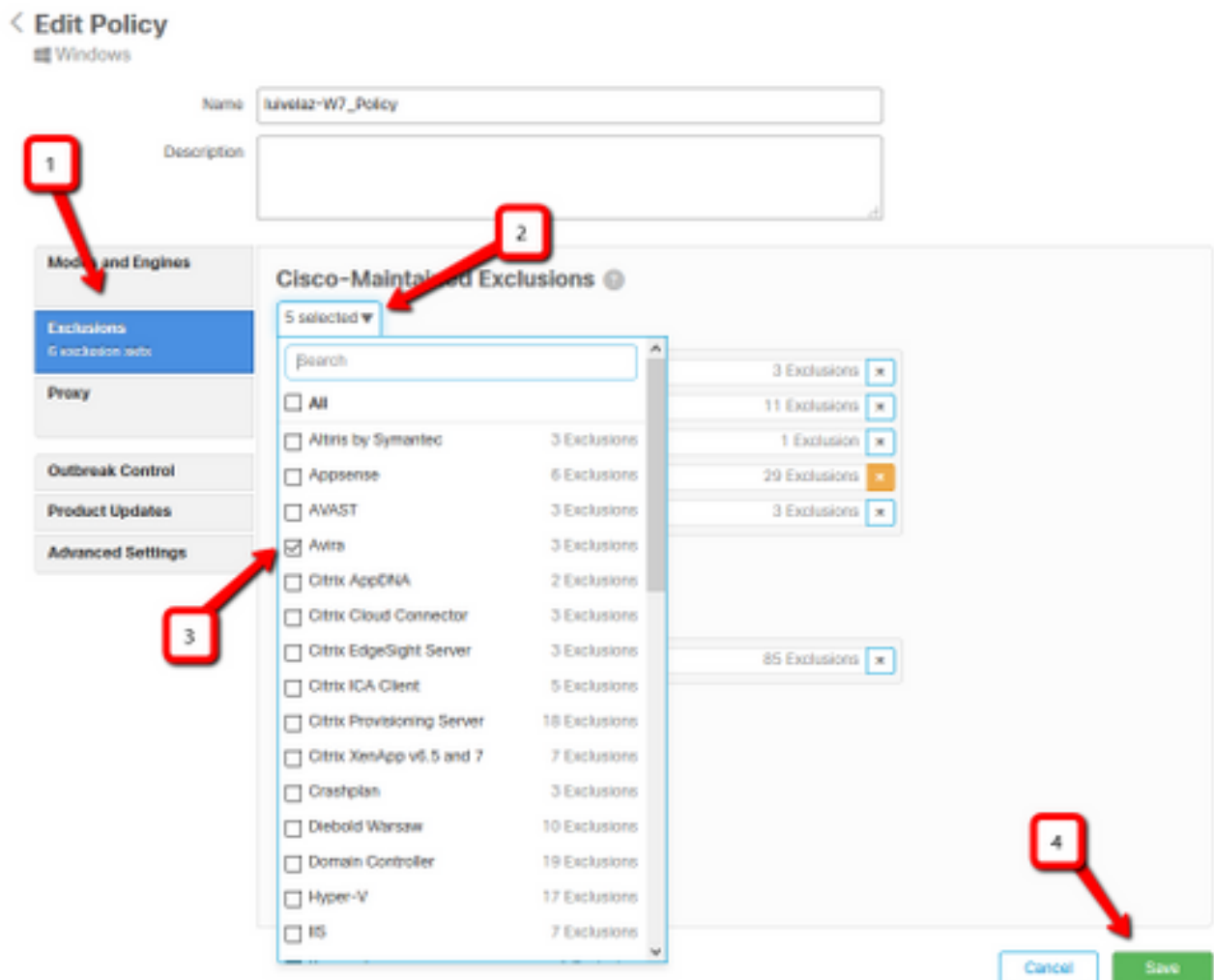
別のウイルス対策がマシンにインストールされているかどうかを確認します

別のAV（ウイルス対策）がインストールされている場合は、AVの主なプロセスがポリシー設定から除外されていることを確認します

ヒント：使用されているソフトウェアがリストに含まれている場合は、シスコが管理する除外項目を使用します。これらの除外項目は、アプリケーションの新しいバージョンに追加できます。

[Cisco Maintained Exclusions]セクションで使用可能なリストを表示するには、[Management] > [Policies] > [Edit] > [Exclusions] > [Cisco-Maintained Exclusions]に移動します。

図に示すように、現在マシンにインストールされているソフトウェアに従ってエンドポイントに必要なものを選択し、ポリシーを保存します。



特定のアプリケーションが使用中のときにCPU使用率が高くなったかどうかを確認します

潜在的な除外を特定するプロセスに役立つ問題を複製できる場合は、1つのアプリケーションまたはその一部が実行されている間に問題が発生したかどうかを特定します。

分析のための診断バンドルの収集

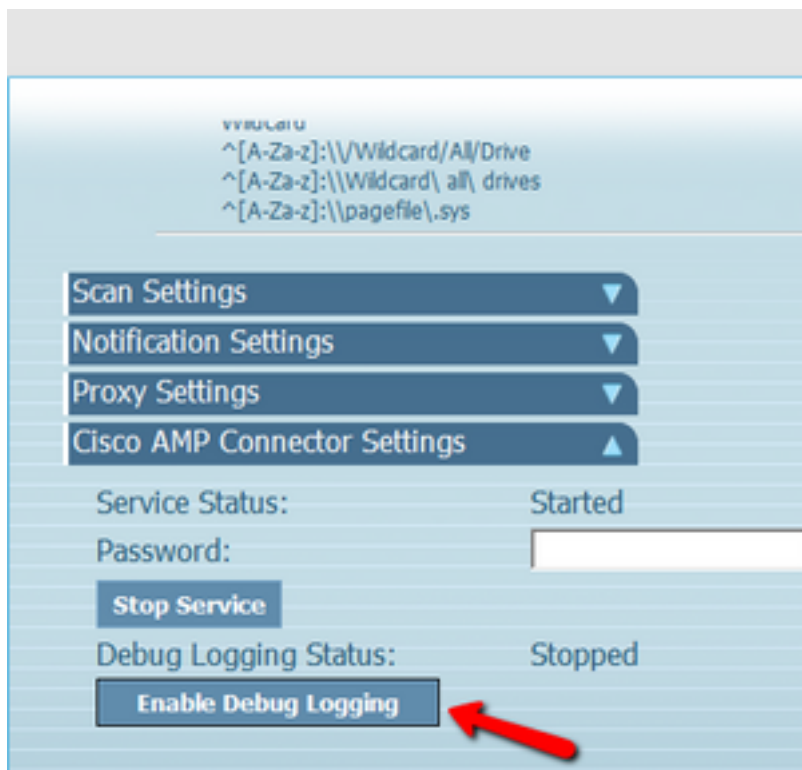
デバッグログレベルの有効化

有用な診断バンドルを収集するには、デバッグログレベルを有効にする必要があります。

エンドポイントのデバッグレベル

問題を複製してエンドポイントにアクセスできる場合は、診断バンドルをキャプチャする最良の手順を次に示します。

1. AMP GUIを開く
2. [設定]に移動します
3. AMP GUIの下部までスクロールし、[Cisco AMP Connector Settings]を開きます
4. [デバッグログの有効化]をクリックします
5. **デバッグログの状態を[開始]に変更する必要があります。**この手順により、次のポリシーハートビートまで、デフォルトで15分までデバッグレベルが有効になります



ポリシーのデバッグレベル

エンドポイントにアクセスできないか、問題を一貫して再現できない場合は、ポリシーでデバッグログレベルを有効にする必要があります。

ポリシーによってデバッグログレベルを有効にするには、図に示すように、[Management] > [Policies] > [Edit] > [Advanced Settings] > [Connector Log Level and Management] > [Policies] > [Edit] > [Advanced Settings] > [Tray Log Level]に移動し、ポリシーを保存します。

< Edit Policy
Windows

Name: luvelaz-W7_Policy
Description:

Modes and Engines

Exclusions
5 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings
Administrative Features
Client User Interface
File and Process Scan
Cache
Endpoint Isolation
Orbit
Engines
TETRA
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

注意：ポリシーからデバッグモードが有効になっている場合、すべてのエンドポイントがこの変更を受信します。

注：エンドポイントのポリシーを同期して、デバッグレベルが適用されていることを確認するか、ハートビート間隔が待機するようにします。デフォルトでは、15分です。

問題を再現し、診断バンドルを収集する

デバッグレベルが設定されている場合は、システムでHigh CPUの状態が発生するまで待機するか、以前に特定された条件を手動で再現してから、診断バンドルを収集します。

バンドルを収集するには、C:\Program Files\Cisco\AMP\X.X.X (X.X.Xはシステムにインストールされている最新のAMPバージョン) に移動し、アプリケーション `ipsupporttool.exe` を実行します。このプロセスにより、CiscoAMP_Support_Tool_%date%.7z というというデスクトップに。ファイルが作成されます

注：コネクタバージョン6.2.3以降では、バンドルをリモートで要求し、[管理] > [コンピュータ]に移動し、エンドポイントレコードを展開し、[診断]オプションを使用できます。

注：診断バンドルは、次のコマンドを使用してCMDプロンプトから実行することもできます。"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe"または"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\Can\Get\To"。X.X.Xは最新のAMPバージョンで、2番目のコマンドを使用して、7zファイルの出力フォルダを選択できます。

分析する

診断ファイルを分析するには、次の2つの方法があります。

- Diag_Analyzer.exe
- Amphandlecount.ps1

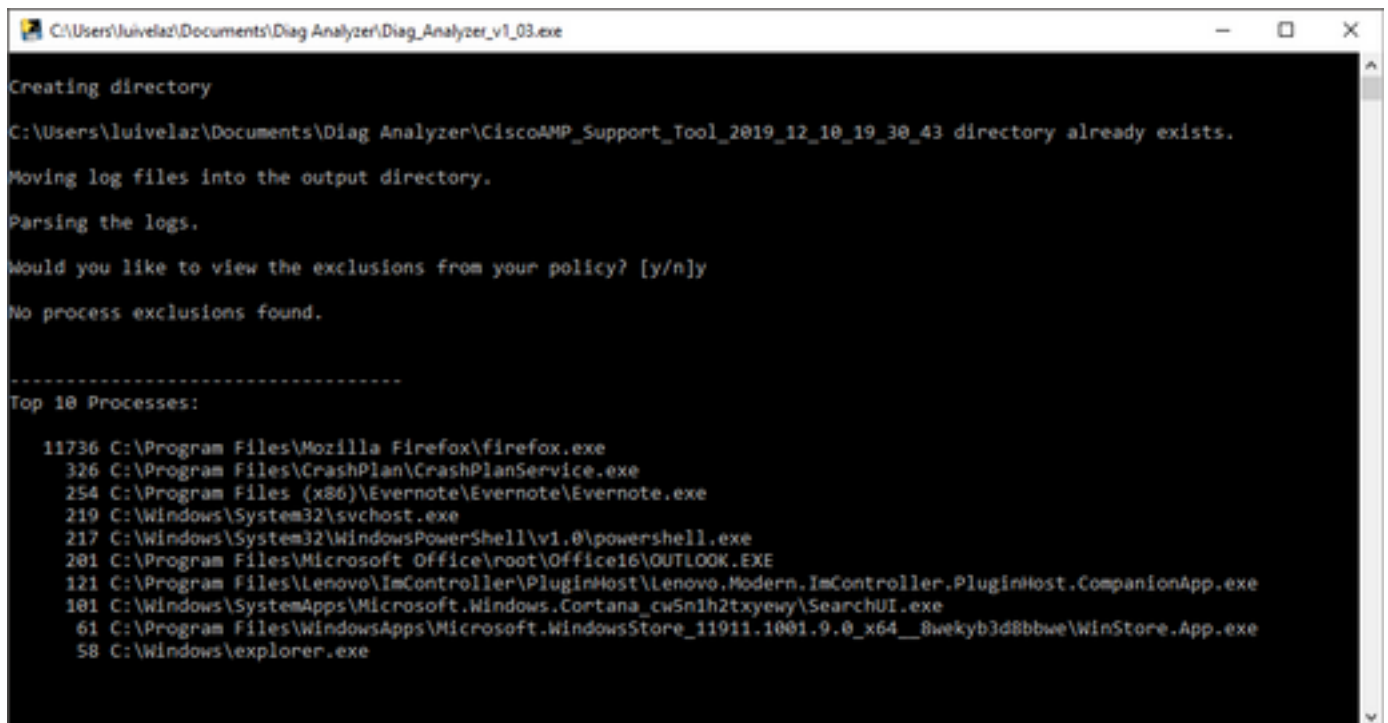
Diag_Analyzer.exe

ステップ1：アプリケーションをここにダウンロード[します](#)。

ステップ2:GitHubページに、使用方法に関する詳細な指示が記載されたREADMEファイルがあります。

ステップ3：診断ファイルCiscoAMP_Support_Tool_%date%.7zをDiag_Analyzer.exeと同じフォルダにコピーします。

ステップ4：アプリケーションの実行 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
```

ステップ5：新しいプロンプトで、ポリシーから除外をYまたはNで取得するかどうかを確認します。

ステップ6：スクリプトの結果には次のものが含まれます。

- 上位10プロセス

- 上位10ファイル
- 上位10の拡張機能
- 上位100のパス
- すべてのファイル

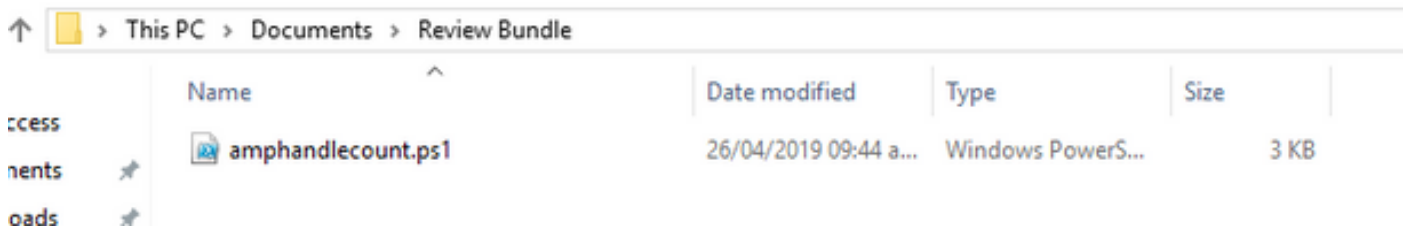
注：Diag_Analyzer.exeは、提供されたAMP診断ファイルのsfc.exe.logファイルをチェックします。次に、診断ファイル名を持つ新しいディレクトリを作成し、ログファイルを。7zの外部の診断の親ディレクトリに保存します。その後、ログを解析し、上位10のプロセス、ファイル、拡張子、およびパスを決定します。

Amphandlecount.ps1

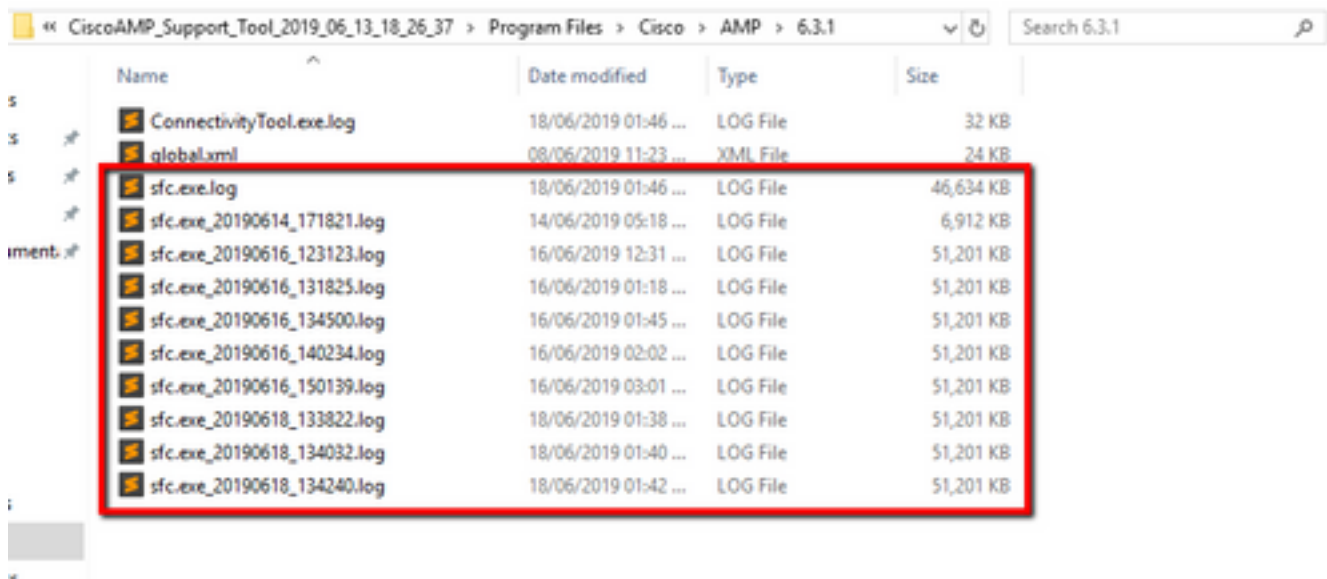
ステップ1：スクリプトamphandlecounts.txtをこのコミュニティの下部からダウンロードし、[AMPからスキャンされたファイルを確認します。](#)

ステップ2: Windowsでスクリプトを実行するには、名前をamphandlecount.ps1に変更します。

ステップ3：便宜上、amphandlecount.ps1ファイルを自身のフォルダにコピーします。



ステップ4: CiscoAMP_Support_Tool_%date%.7zファイルを解凍し、パス上のsfc.logファイルを特定します CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X



ステップ5: amphandlecount.ps1フォルダにsfc.logのファイルをコピーします。

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

ステップ6: PowerShellでamphandlecount.ps1を実行すると、ウィンドウが開き、エンドポイントの実行ポリシーに応じて実行の許可を求めることができます。

ヒント：実行ポリシーを変更するには、Windows PowerShellを開き、次のコマンドを使用します。

制限のない実行アクセスを許可するようにポリシーを設定します – **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted**

実行アクセスを制限するポリシーを設定します – **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

ステップ7: PowerShellが終了したら (フォルダー内のsfc.logの数によっては時間がかかる場合があります)、フォルダーに4つのファイルが作成されます。

- 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

ステップ8: 4つの新しいファイルに分析結果が含まれています。

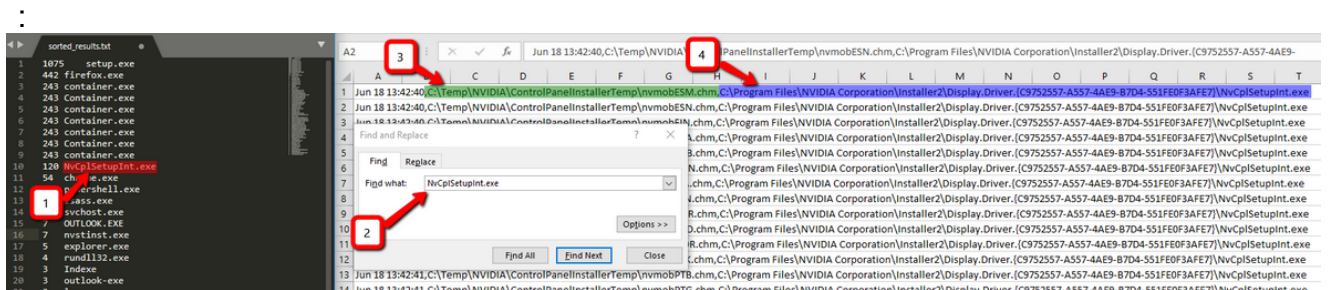
- **data.csv**: スキャンされたファイルの完全なパスと、ファイルを作成/変更/移動した親プロセスが含まれます
- **results.txt**: AMPによってスキャンされたプロセスのリストが含まれます。
- **sorted_results.txt**: 最もスキャンされたプロセスでAMPによってスキャンされたプロセスのリストを含む
- **terms.txt**: AMPによってスキャンされたプロセスの名前が含まれます

ステップ9: data.csvのsorted_results.txtからカウントの高いプロセス名をフィルタリングしますが、親プロセスとそのフルパスを識別し、信頼できる場合はカスタムリストのポリシーに除外を追加できます。

検索するプロセス：

1. 「data.csv」のCtrl + Fと検索
2. AMPによってスキャンされたファイルのパス
3. ファイルをコピー/移動/変更した親プロセスのパス

注：注：通常、除外は「Process:スキャンを受け取る親プロセスの「子プロセスを含む」を含むファイルスキャン



注：[ここでは](#)、除外を作成するためのベストプラクティスに関する詳細情報を確認できます

。

除外の調整

プロセスまたはパスが特定されたら、エンドポイントに適用されているポリシーにリンクされている除外リストに追加して、[Management] > [Exclusions] > [Exclusion name] > [Edit]に移動します。

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			

分析のためにバンドルをTACに送信します。

ATS TACは、これらのシナリオのトラブルシューティングに役立ちます。その場合は、ケース作成時に次の情報を提供できるように準備してください。

- この問題はいつ始まりますか。
- 最近の変更はありますか。
- この問題は特定のアプリケーションで発生しますか。「はい」の場合、どのアプリケーションですか。
- システム上に他のウイルス対策プログラムはありますか。可能な場合、どのウイルス対策を使用しますか。
- 問題の再現中にデバッグバンドルを収集します。 [デバッグバンドルの収集手順](#)