AMP 진단 번들을 분석하여 높은 CPU 지원

목차

소개

이 문서에서는 높은 CPU 사용 문제를 해결하기 위해 AMP(Advanced Malware Protection) for Endpoints Public Cloud on Windows 디바이스에서 진단 번들을 분석하는 단계에 대해 설명합니다.

기고자: Luis Velazquez, Yeraldin Sánchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP 콘솔 액세스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AMP for Endpoints 콘솔 5.4.20200204
- Windows 운영 체제 장치

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의

잠재적인 영향을 이해해야 합니다.

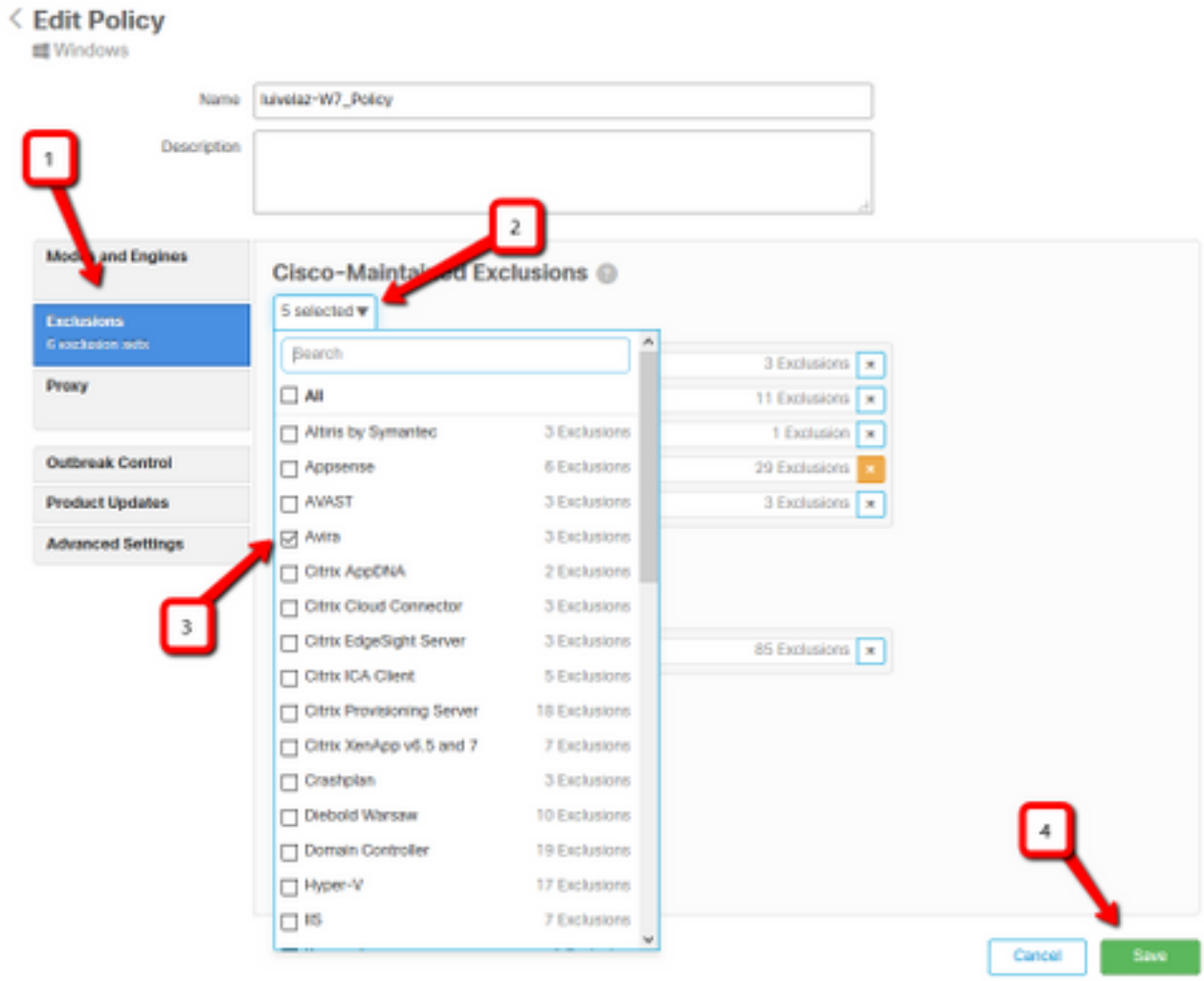
문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

컴퓨터에 다른 안티바이러스 설치 여부 확인

다른 AV(안티바이러스)가 설치된 경우 AV의 기본 프로세스가 정책 컨피그레이션에서 제외되었는지 확인합니다.

> **팁**:사용 중인 소프트웨어가 목록에 포함되어 있는 경우 Cisco에서 유지 관리하는 제외를 사용하십시오. 이러한 제외를 애플리케이션의 새 버전에 추가할 수 있습니다.
>
> Cisco에서 유지 관리하는 제외 섹션에서 사용 가능한 목록을 보려면 **Management** > Policies > **Edit** > **Exclusions** > **Cisco-Maintained Exclusions로** 이동합니다.
> 현재 시스템에 설치된 소프트웨어에 따라 엔드포인트에 필요한 정책을 선택한 다음 이미지에 표시된 대로 정책을 저장합니다.



특정 애플리케이션이 사용 중일 때 높은 CPU가 발생하는지 확인

잠재적인 제외를 식별하는 과정에서 문제를 복제할 수 있는 경우 한 애플리케이션 또는 그 중 일부

가 실행되는 동안 문제가 발생하는지 확인합니다.

분석을 위한 진단 번들 수집

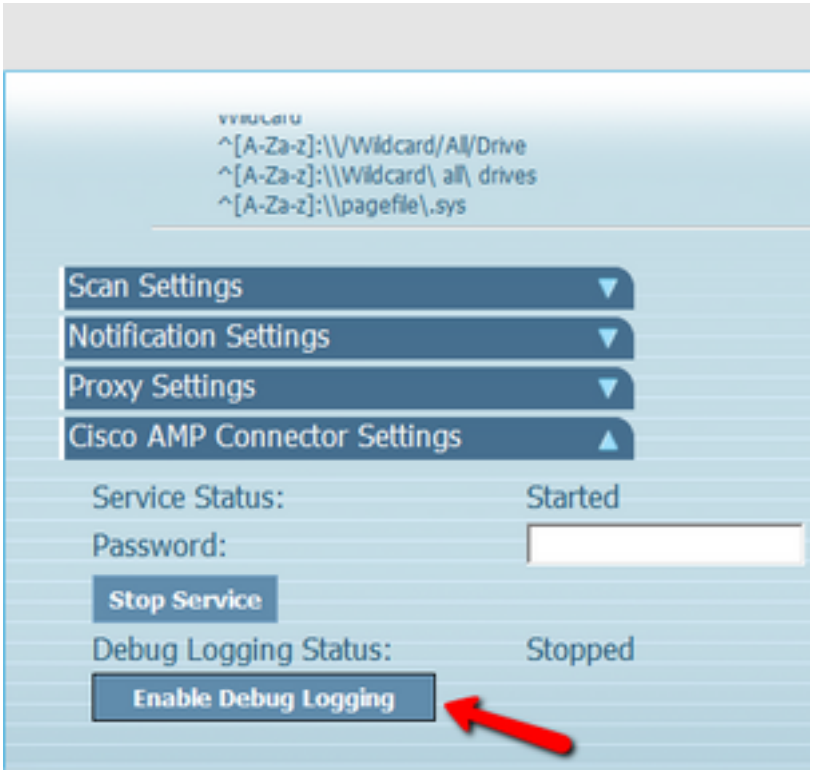
디버그 로그 레벨 사용

유용한 진단 번들을 수집하려면 디버그 로그 레벨을 활성화해야 합니다.

엔드포인트의 디버그 수준

문제를 복제하고 엔드포인트에 액세스할 수 있는 경우, 진단 번들을 캡처하는 가장 좋은 절차는 다음과 같습니다.

1. 개방형 AMP GUI
2. **설정**으로 이동
3. AMP GUI 아래쪽으로 스크롤하여 **Cisco AMP Connector Settings(Cisco AMP 커넥터 설정)**를 엽니다.
4. Enable Debug **Logging(디버그 로깅 활성화)을 클릭합니다.**
5. **Debug Logging Status(디버그 로깅 상태)**는 Started(시작됨)로 변경해야 **합니다.**이 절차에서는 다음 정책 하트비트가 기본적으로 15분까지 디버그 레벨을 활성화합니다

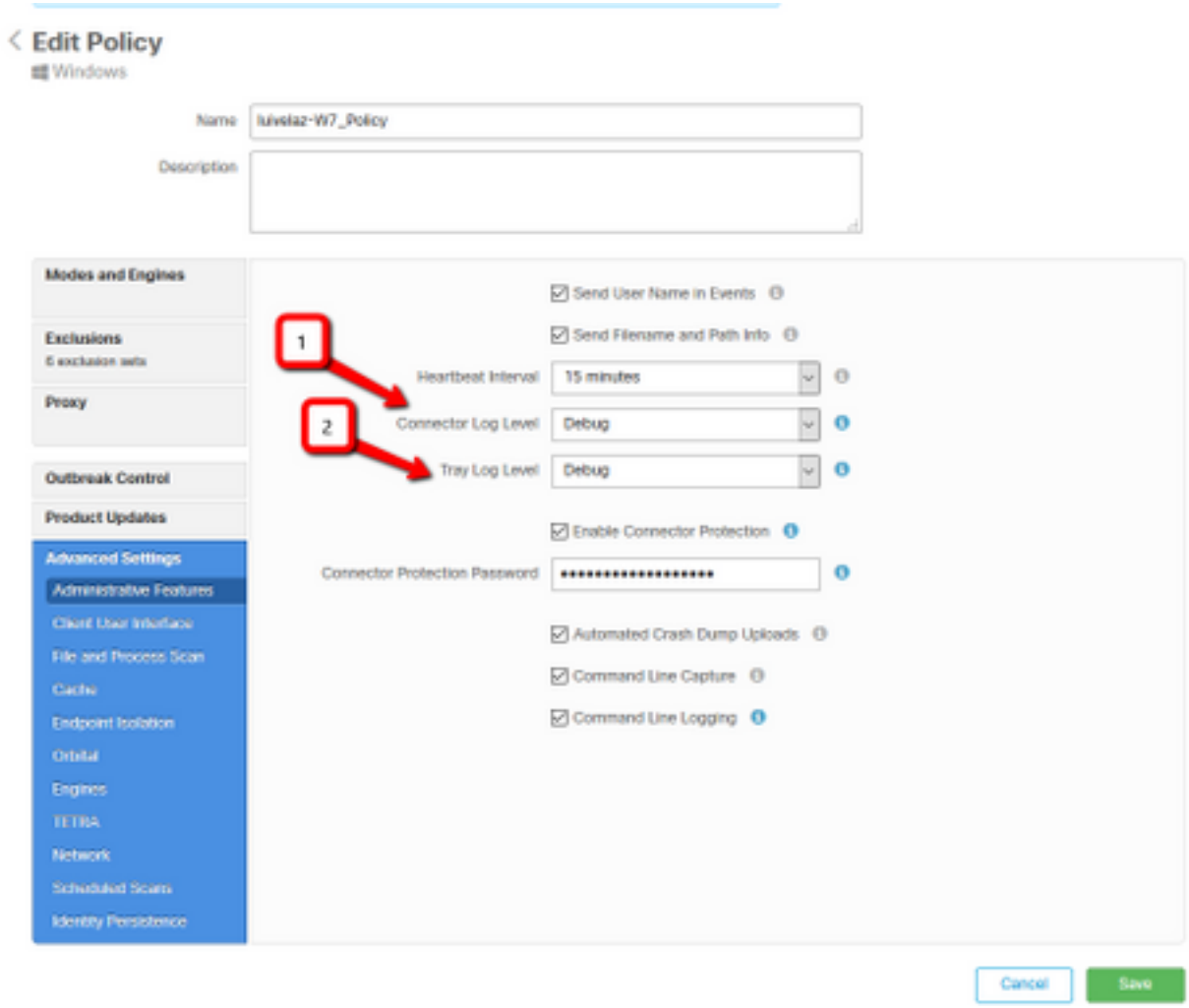


정책의 디버그 수준

엔드포인트에 대한 액세스 권한이 없거나 문제가 일관성 있게 재현될 수 없는 경우 정책에서 디버그 로그 레벨을 활성화해야 합니다.

정책별로 디버그 로그 레벨을 활성화하려면 Management(관리) > **Policies(정책) > Edit(편집)** > Advanced Settings(고급 설정) > Connector Log Level(**커넥터 로그** 레벨) and **Management(관리) > Policies(정책)** > Edit(편집) > **Advanced Settings(고급 설정) > Tray Log Level(트레이 로그 레벨)으**

로 이동한 다음 이미지에 표시된 대로 Debug(디버그)를 선택하고 정책을 저장합니다.



주의:정책에서 디버그 모드가 활성화된 경우 모든 엔드포인트에서 이 변경 사항을 수신합니다 .

참고:디버그 레벨이 적용되는지 확인하거나 하트비트 간격을 대기하도록 엔드포인트의 정책을 동기화합니다. 기본적으로 15분입니다.

문제를 재현하고 진단 번들 수집

디버그 레벨이 시스템에서 High CPU 상태가 발생할 때까지 대기하거나 이전에 식별된 조건을 수동으로 재현한 다음 진단 번들을 수집합니다.

번들을 수집하려면 **C:\Program Files\Cisco\AMP\X.X.X**(X.X.X는 시스템에 설치된 최신 AMP 버전임)로 이동하고 application ipsupporttool.exe를 실행합니다. 이 프로세스는 **CiscoAMP_Support_Tool_%date%.7z**라는 바탕 화면에 .**7z** 파일을 **생성합니다.**

참고:커넥터 버전 6.2.3 이상에서는 번들을 원격으로 요청할 수 있으며 **Management(관리) > Computers(컴퓨터)**로 이동하여 엔드포인트 레코드를 확장하고 Diagnose(진단) 옵션을 사용할 수 있습니다.

참고:다음 명령을 사용하여 CMD 프롬프트에서 진단 번들을 실행할 수도 있습니다 **."C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe"** 또는 **"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To"** 여기서 **X.X.X**는 최신 AMP 버전입니다. 두 번째 명령을 사용하여 .7z 파일의 출력 폴더를 선택할 수 있습니다.

분석

진단 파일을 분석하는 방법에는 두 가지가 있습니다.

- Diag_Analyzer.exe
- Amphandlecount.ps1

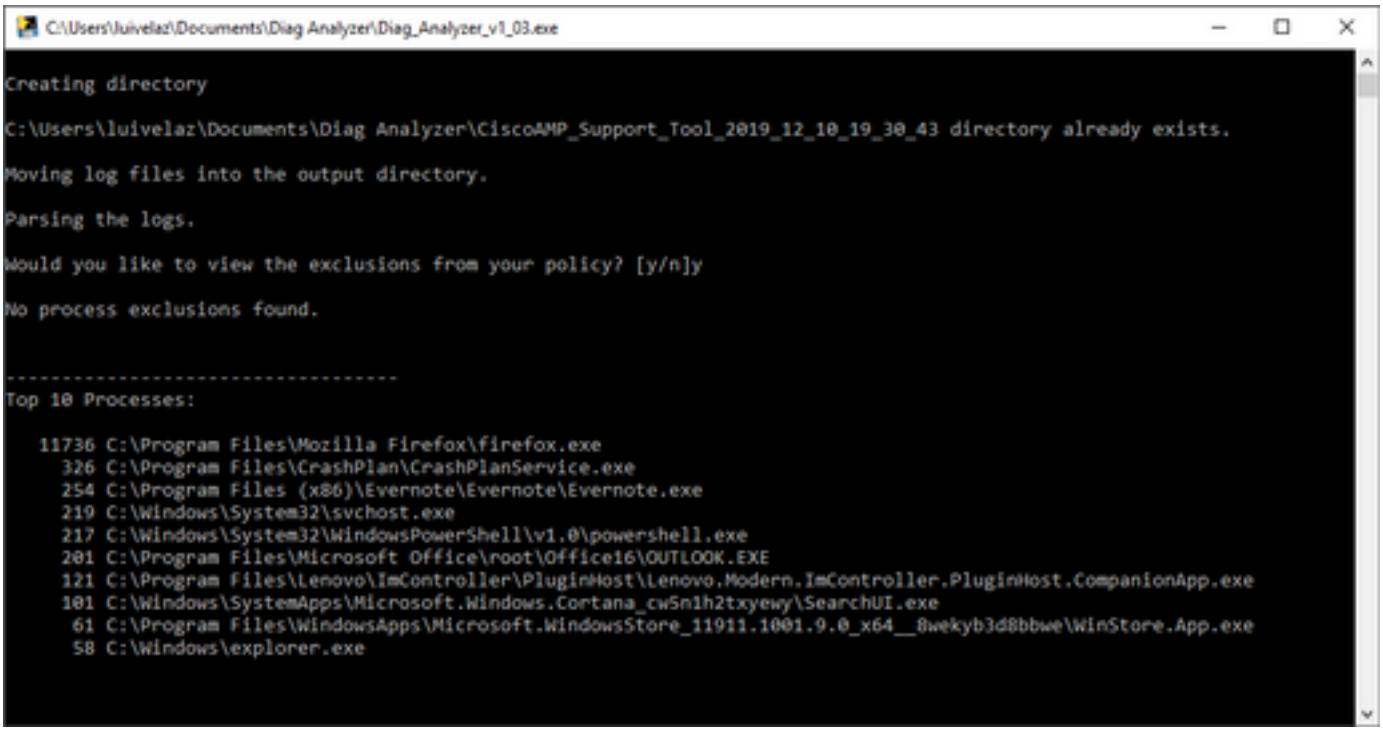
Diag_Analyzer.exe

1단계. 여기에서 애플리케이션을 다운로드합니다.

2단계. GitHub 페이지에는 사용에 대한 추가 지침이 포함된 README 파일이 있습니다.

3단계. 진단 파일 **CiscoAMP_Support_Tool_%date%.7z**를 Diag_Analyzer.exe가 있는 동일한 폴더에 복사합니다.

4단계. 애플리케이션 실행 **Diag_Analyzer.exe입니다.**



5단계. 새 프롬프트에서 **Y** 또는 **N**으로 정책에서 제외를 가져오려는 경우를 확인합니다.

6단계. 스크립트 결과에 다음이 포함됩니다.

- 상위 10개 프로세스
- 상위 10개 파일
- 상위 10개 확장
- 상위 100개 경로

- 모든 파일

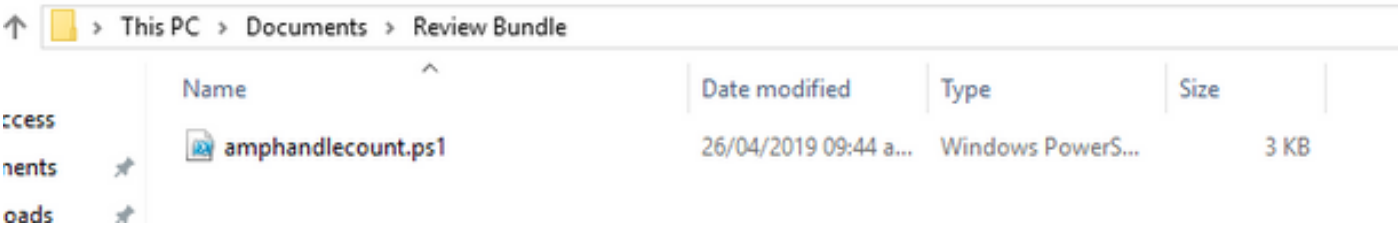
  참고: Diag_Analyzer.exe는 제공된 AMP 진단 파일에서 sfc.exe.log 파일을 확인합니다.그런 다음 진단 파일 이름으로 새 디렉터리를 만들고 .7z 외부의 로그 파일을 진단 프로그램의 부모 디렉터리에 저장합니다. 그런 다음 로그를 구문 분석하여 상위 10개의 프로세스, 파일, 확장자 및 경로를 확인하고 마지막으로 정보를 화면과 {Diagnostic}-summary.txt 파일에도 인쇄합니다.

Amphandlecount.ps1

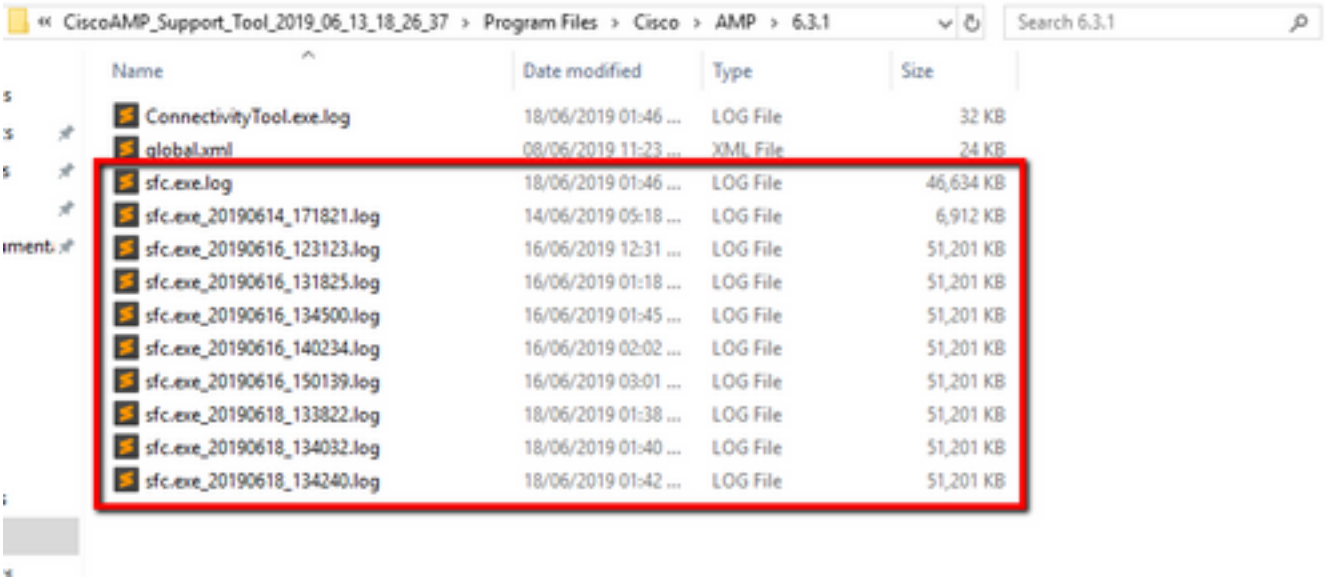
1단계. AMP에서 **Review Scanned Files(**스캔된 파일 검토)를 게시한 커뮤니티의 하단에서 스크립트 amphandlecunts.txt를 다운로드합니다.

2단계. Windows에서 스크립트를 실행하려면 이름을 **amphandlecount.ps1**로 **바꿉니다**.

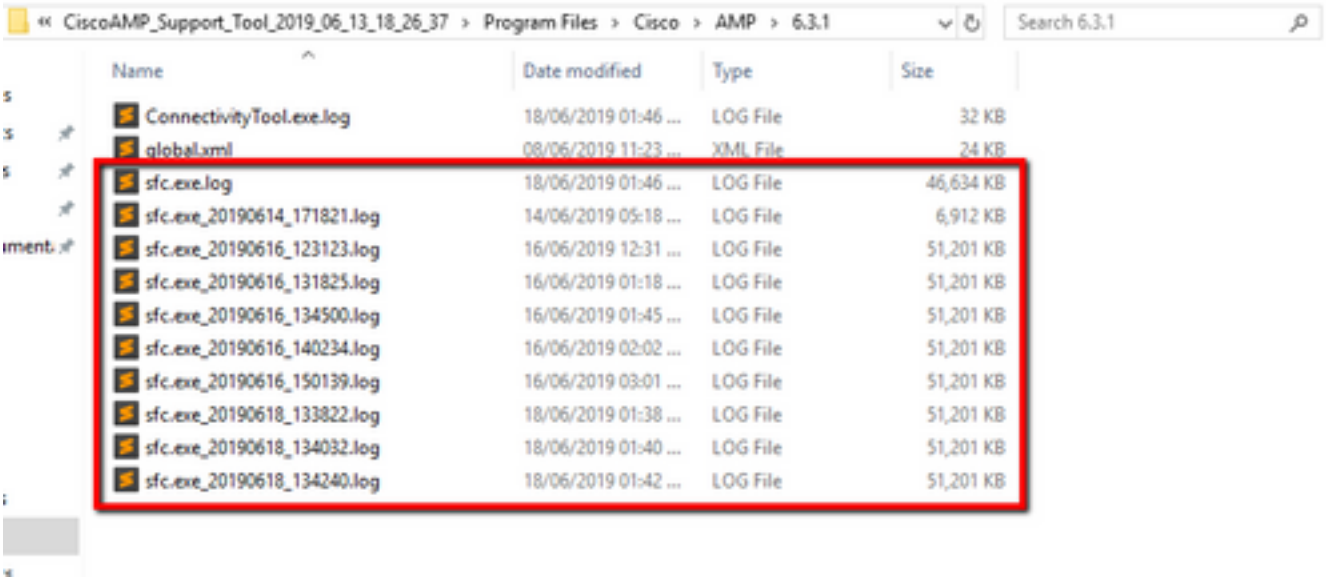
3단계. 편의를 위해 **amphandlecount.ps1** 파일을 자신의 폴더에 복사합니다.



4단계. **CiscoAMP_Support_Tool_%date%.7z** 파일의 압축을 풀고 경로**에서 sfc.log** 파일**을** 식별합니다. **CiscoAMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X .**



5단계. **sfc.log의** 파일을 **amphandlecount.ps1** 폴더에 복사합니다.

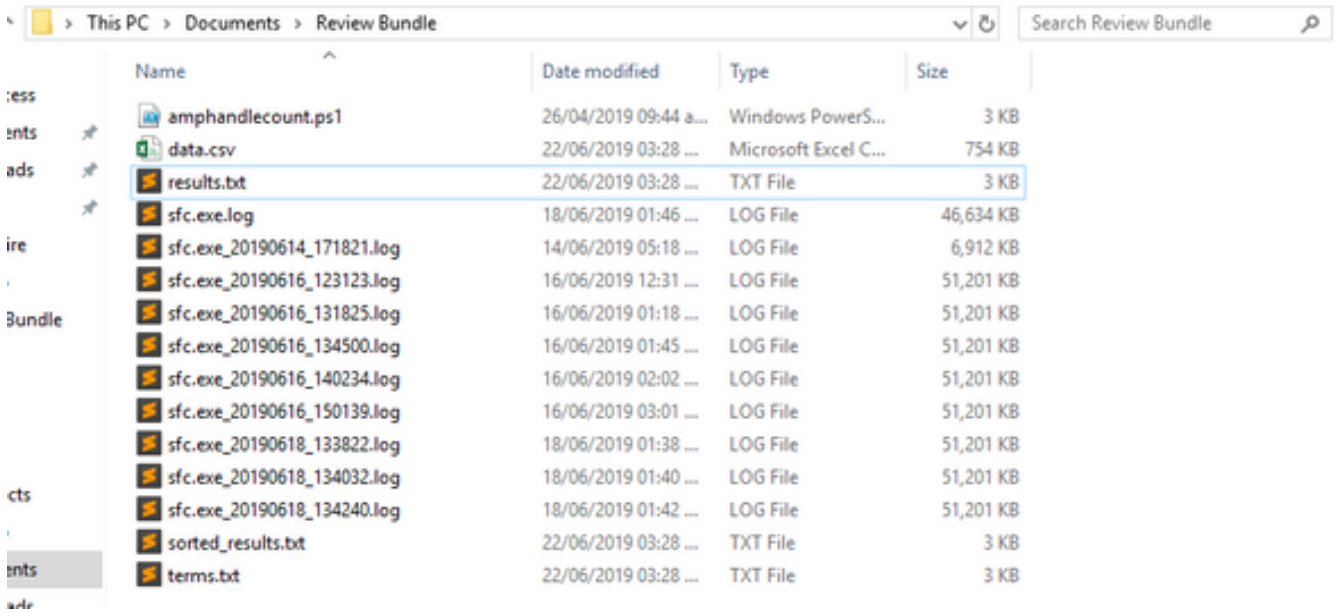


6단계. **PowerShell**을 사용하여 **amphandlecount.ps1**을 실행하면 창이 열리고 엔드포인트의 실행 정책에 따라 실행 권한을 요청할 수 있습니다.

> **팁**:실행 정책을 변경하려면 Windows PowerShell을 열고 다음 명령을 사용합니다.
> 무제한 실행 액세스를 허용하도록 정책을 설정합니다. - Set-ExecutionPolicy -Scope CurrentUser **-ExecutionPolicy Unrestricted**
> 실행 액세스를 제한하도록 정책을 설정합니다. - Set-ExecutionPolicy -**Scope CurrentUser -ExecutionPolicy Restricted**

7단계. PowerShell이 완료된 후 PowerShell이 완료될 수 있도록 허용합니다(폴더에 sfc.log가 있는 개수에 따라 다소 시간이 걸릴 수 있음). 폴더에 4개의 파일이 생성됩니다.

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



8단계. 4개의 새 파일에 분석 결과가 포함됩니다.

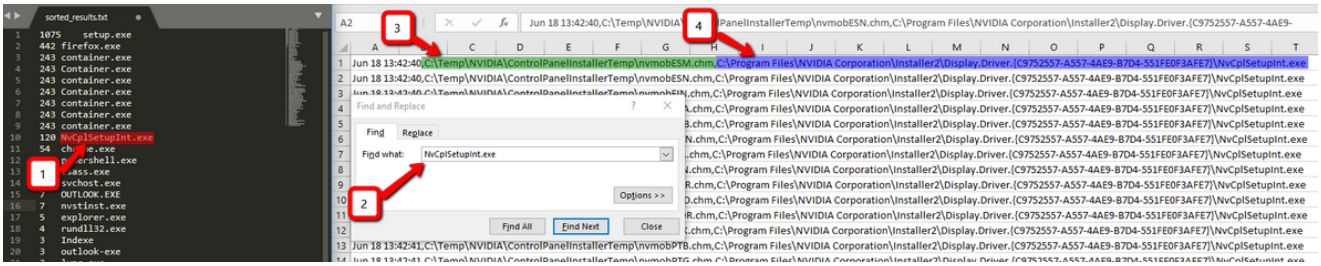
- **데이터.csv:**스캔한 파일의 전체 경로 및 파일을 생성/수정/이동한 father 프로세스가 포함되어 있습니다.
- **results.txt:** AMP에서 검사한 프로세스 목록이 포함되어 있습니다.
- sorted_results.txt:AMP에서 스캔한 프로세스 목록과 가장 스캔한 프로세스 포함
- **terms.txt:** AMP에서 스캔한 프로세스의 이름을 포함합니다.

9단계. **data.csv**에서 **sorted_results.txt**에서 상위 프로세스의 전체 경로를 식별하여 프로세스 이름을 높은 수로 필터링한 다음, 신뢰할 수 있는 경우 사용자 지정 목록의 정책에 제외를 추가합니다.

확인할 프로세스:

1. "data.csv"의 Ctrl + F 및 검색
2. AMP에서 스캔한 파일의 경로
3. 파일을 복사/이동/수정한 상위 프로세스의 경로

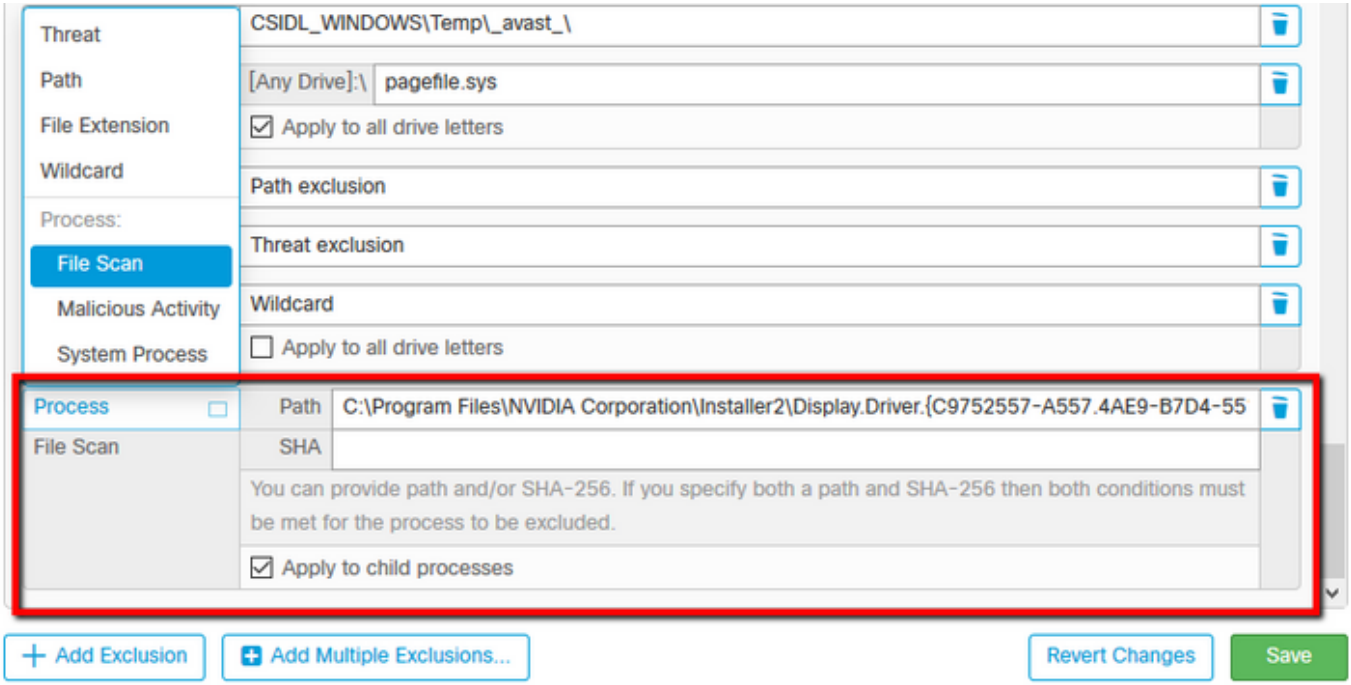
참고:참고:일반적으로 제외는 "Process:스캔을 가져오는 상위 프로세스에 대해 "Child Processes include"가 포함된 파일 스캔
:



참고:[여기서는 제외](#)를 생성하는 모범 사례와 관련된 자세한 정보를 확인할 수 있습니다.

제외 조정

프로세스 또는 경로가 식별되면 엔드포인트에 적용된 정책에 연결된 제외 목록에 추가 할 수 있습니다. 이미지에 표시된 대로 **Management > Exclusions > Exclusion name > Edit로** 이동 합니다.



분석을 위해 번들을 TAC에 제출

ATS TAC는 이러한 시나리오를 해결하는 데 도움이 될 수 있습니다. 그러한 경우 케이스 생성 시 다음 정보를 제공할 준비가 되어 있어야 합니다.

- 이 문제는 언제 시작됩니까?
- 최근에 변경된 것이 있습니까?
- 특정 애플리케이션에 문제가 발생합니까?대답이 "예"인 경우, 어떤 애플리케이션입니까?
- 시스템에 다른 안티바이러스가 있습니까?대답이 "예"인 경우, 어떤 안티바이러스?
- 문제가 재생되는 동안 디버그 번들을 수집합니다. 디버그 번들을 수집하는 단계