High CPU용 MacOS AMP 진단 번들 분석

목차

소개

이 문서에서는 CPU 사용량이 많은 문제를 해결하기 위해 macOS 디바이스의 AMP(Advanced Malware Protection) for Endpoints 퍼블릭 클라우드에서 진단 번들을 분석하는 단계에 대해 설명합니다.

기고자: Uriel Torres, Yeraldin Sanchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP 콘솔의 기본 탐색
- MAC 터미널 탐색

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AMP for Endpoints 콘솔 5.4.20200512
- macOS Catalyina 버전 10.15.4

- AMP 커넥터 1.12.3.738

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.

배경 정보

AMP Connector는 명시적으로 알리지 않은 한 시스템의 모든 활성 파일(스스로 이동, 복사 및/또는 수정하는 파일)을 스캔합니다. 이 경우 커넥터가 실행되는 동안 너무 많은 프로세스와 작업이 실행되면 성능 문제가 발생하여 CPU 사용률, 속도 저하 및 실행 속도가 저하되고 경우에 따라 소프트웨어 실행 속도가 느려지거나 느리게 실행되지 않습니다.또한 AMP Connector는 클라우드 평판을 기준으로 파일을 차단할 수 있으며, 경우에 따라 오탐(false positive)이 발생할 수 있습니다. 이 두 문제를 모두 해결할 수 있는 방법은 이러한 경로와 프로세스를 제외하는 것입니다.

성능 문제 해결 흐름이 이미지에 표시됩니다.

문제 해결

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

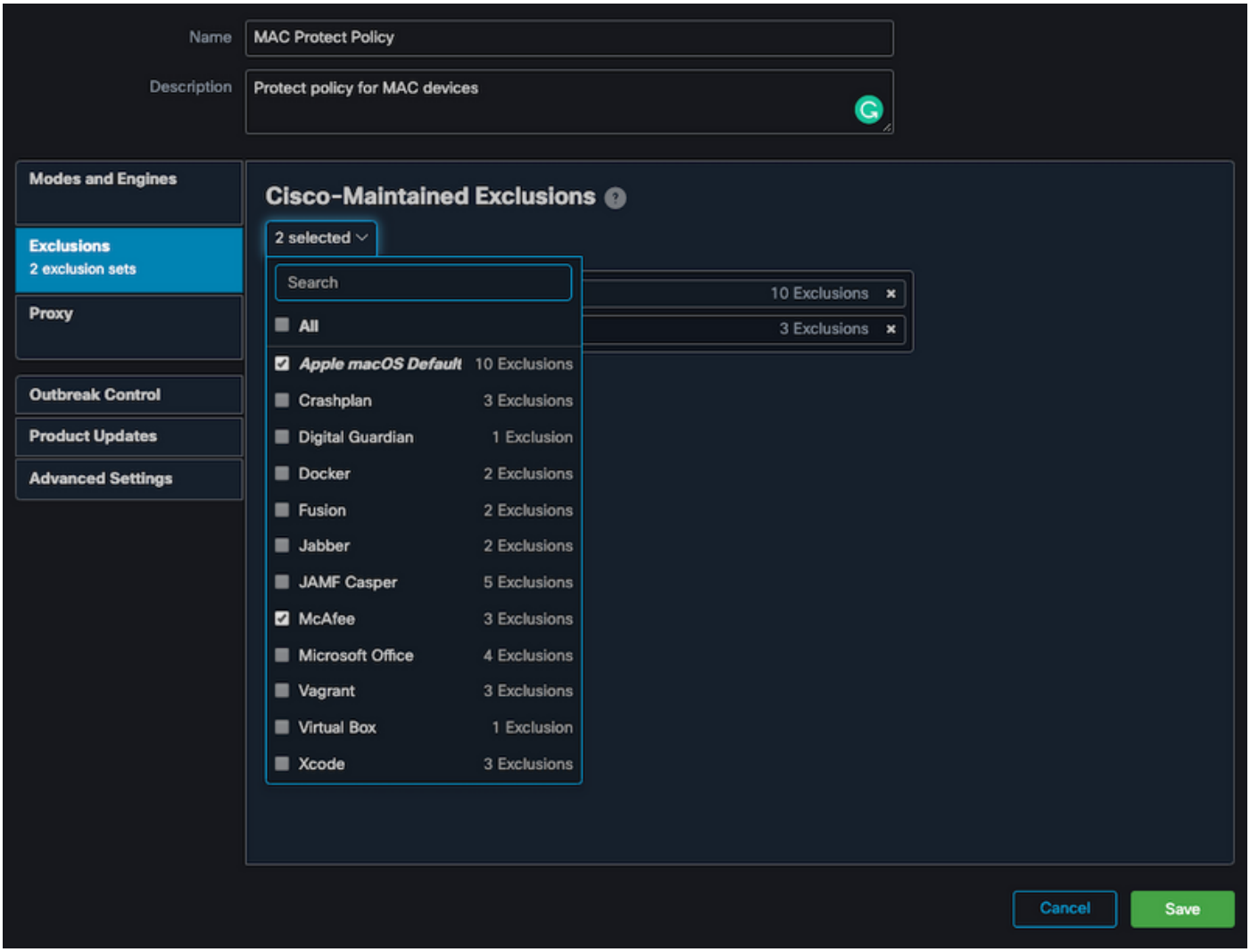
컴퓨터에 다른 안티바이러스 설치 여부 확인

> **팁**:사용 중인 소프트웨어가 목록에 포함되어 있는 경우 Cisco 유지 관리 제외를 사용하여 이러한 제외를 애플리케이션의 새 버전에 추가할 수 있습니다.

AMP 콘솔의 Cisco 유지 관리 제외 섹션에서 사용 가능한 목록을 보려면 다음을 수행합니다.

- Management(**관리) > Policies(정책)로 이동합니다**.
- 정책을 찾고 Edit(수정)를 **클릭합니다**.
- 정책에서 설정 창에서 제외를 **클릭합니다**.

현재 시스템에 설치된 소프트웨어에 따라 엔드포인트에 필요한 정책을 선택한 다음 이미지에 표시된 대로 정책을 저장합니다.



특정 애플리케이션이 사용 중일 때 높은 CPU 식별

문제를 복제하여 잠재적 제외를 식별할 수 있는 경우, 한 애플리케이션 또는 그 중 일부가 실행되는 동안 문제가 발생하는지 확인합니다.

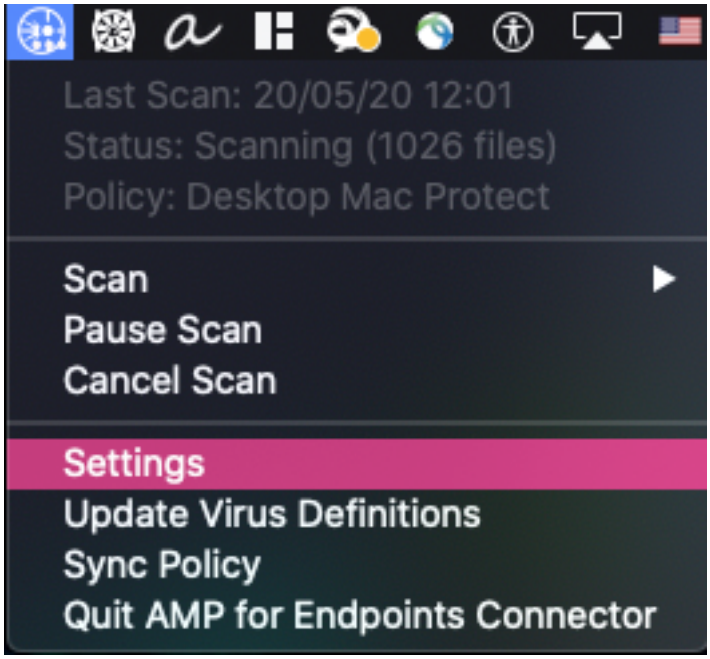
분석을 위한 진단 번들 구성

유용한 진단 번들을 수집하려면 디버그 로그 레벨을 활성화해야 합니다.

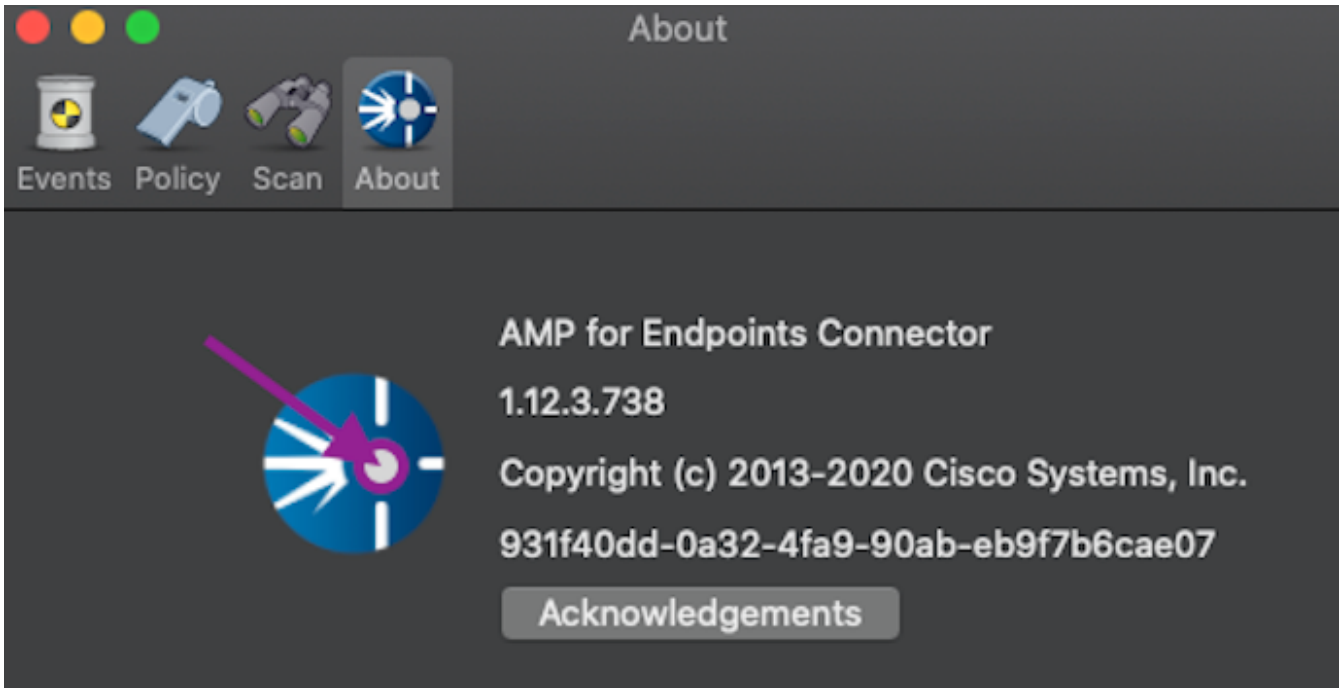
엔드포인트의 디버그 수준

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

- MAC 메뉴 모음에서 AMP 아이콘을 클릭합니다.
- 이미지에 표시된 대로 Settings(설정) 섹션으로 이동합니다.



- 설정 창에서 **정보**로 이동합니다.
- 디버그 모드를 활성화하려면 이미지에 표시된 대로 AMP 로고 내부를 클릭합니다.



팝업은 AMP 커넥터가 디버그 모드에 있음을 나타냅니다.

이 절차에서는 다음 정책 하트비트 간격까지 디버그 로그 레벨을 활성화합니다.

AMP CLI(Command Line Interface)의 디버그 레벨

- 터미널 열기
- 탐색: **/opt/cisco/amp/bin/**
- ampcli 실행:
  ```
  ./ampcli
  ```
- AMP CLI에서 디버그 모드를 활성화합니다.
  ```
  ampcli>debuglevel 1
  ```

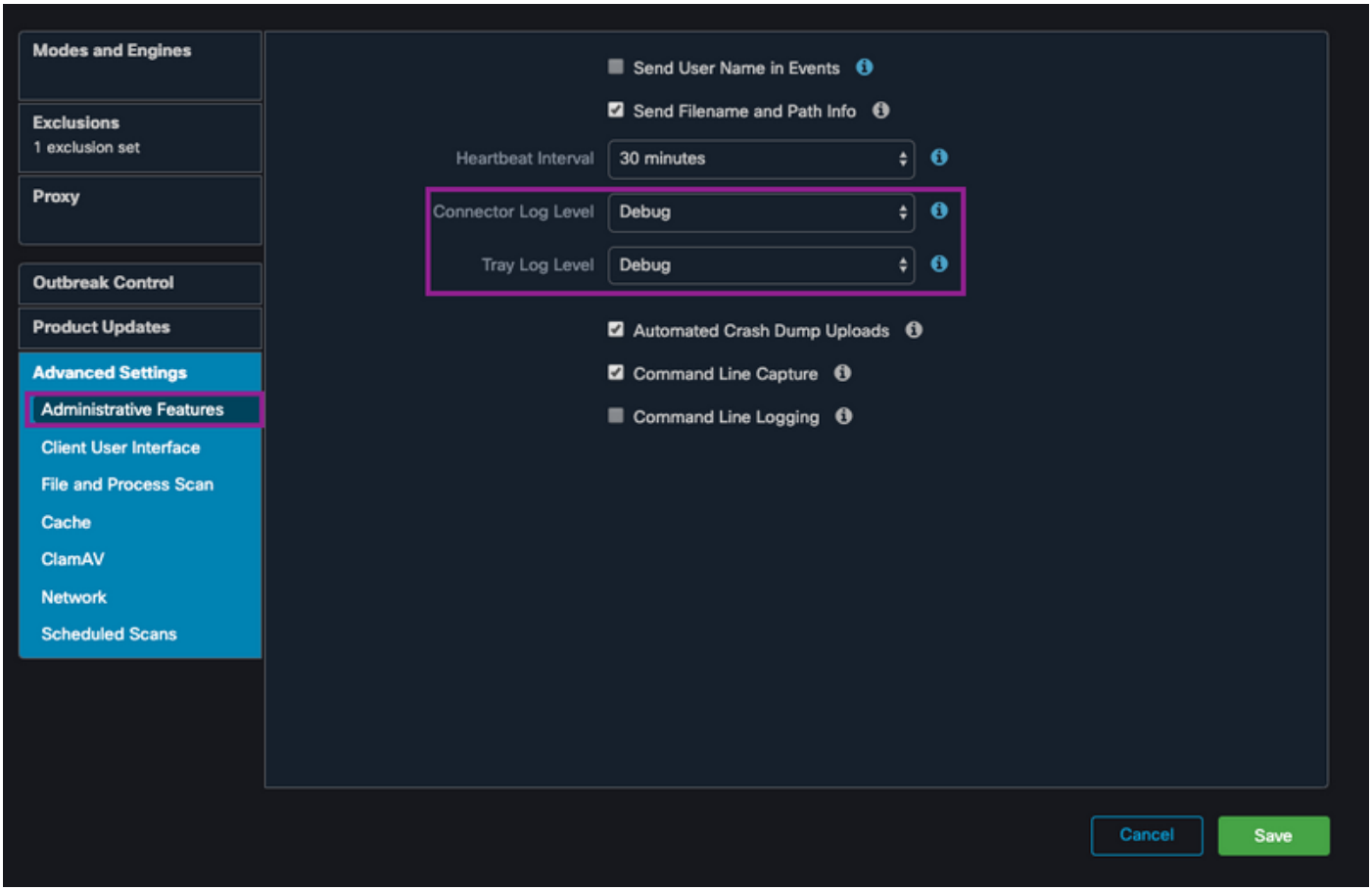
이 프로세스는 다음 정책 하트비트 간격까지 디버그 로그 레벨을 활성화합니다.

정책의 디버그 레벨

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

정책에 의해 디버그 로그 레벨을 활성화하려면

- Management(**관리) > Policies(정책)로 이동합니다.**
- 정책을 찾고 Edit(수정)를 클릭합니다.
- Advanced Settings(고급 **설정) > Administrative Features(관리 기능)로 이동합니다.**
- 이미지**에** 표시된 대로 정책을 디버그 및 저장하도록 커넥터 로그 레벨 및 트레이 로그 레벨 구성



주의:정책에서 디버그 모드가 활성화된 경우 모든 엔드포인트는 이 컨피그레이션을 수신합니다.

참고:디버그 모드를 확인하기 위해 엔드포인트의 정책을 동기화합니다.

다른 안티바이러스 솔루션에서 AMP 제외

사용 설명서에 따르면, 안티바이러스 제품은 다음 디렉토리 및 그 안에 있는 모든 파일, 디렉토리 및 실행 파일을 제외해야 AMP Connector for MAC와 호환됩니다. 제외할 디렉토리는 다음과 같습니다
.

- /라이브러리/애플리케이션 지원/Cisco/AMP for Endpoints 커넥터
- /opt/cisco/amp

문제를 재현하고 진단 번들 수집

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

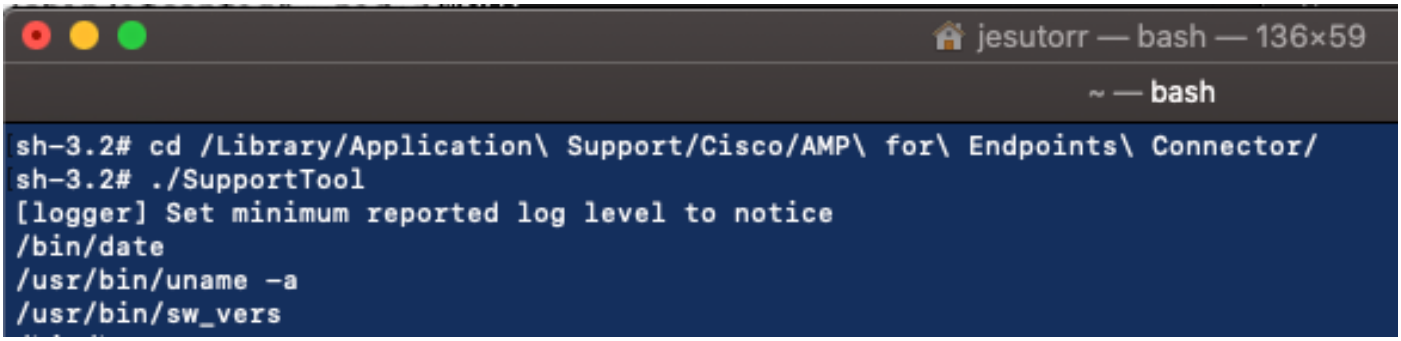
디버그 번들을 수집하려면

- 터미널을 엽니다.
- 수퍼유저 레벨에 액세스한 다음 **/Library/Application Support/Cisco/AMP for Endpoints Connector로 이동합니다**.

```
cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
```

- 지원 툴을 실행하려면 다음 명령을 사용합니다.

```
./SupportTool
```

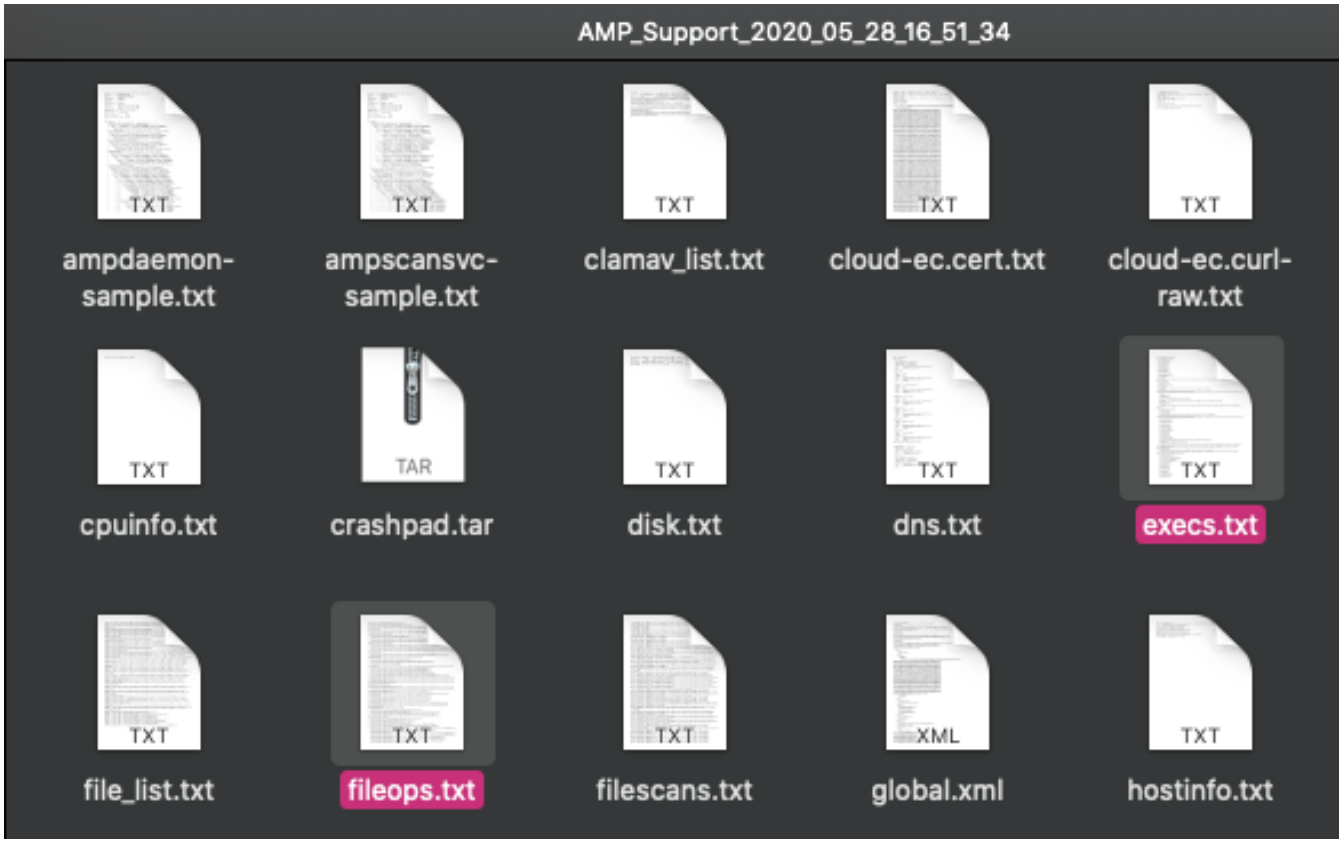


디버그 번들은 Desktop 폴더에 .zip 파일 확장자로 저장됩니다.

높은 CPU 성능 분석

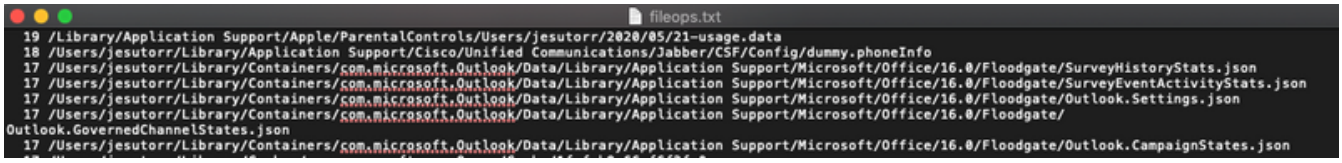
디버그 진단 번들은 분석을 시작하기 위해 데스크톱의 스토리지입니다.

- 진단 번들 압축 해제
- 검토할 2개의 파일이 있습니다. 파일 작업:fileops.txt파일 실행:execs.txt



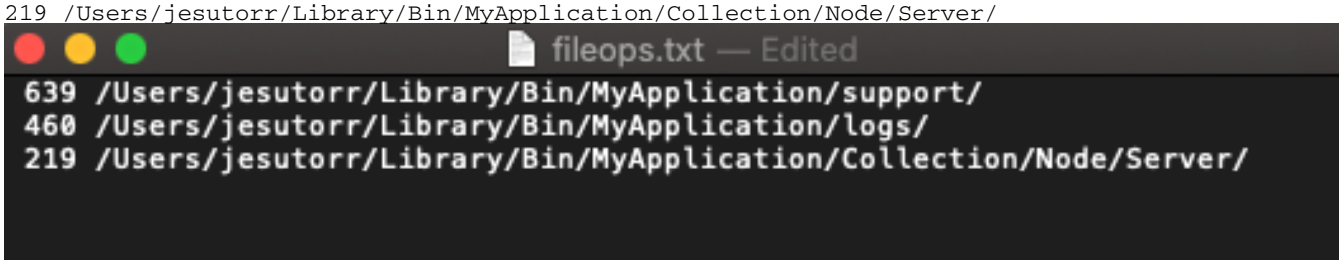
- fileops.txt는 문제 해결을 위한 기본 성능 도구로 작동합니다.Connector가 실행되는 동안 엔드 포인트에서 현재 모든 활성 작업을 나열하며 다음과 같이 읽습니다.

<번들이 수집될 때 경로에서 수행된 숫자 스캔> / <Path scanned>

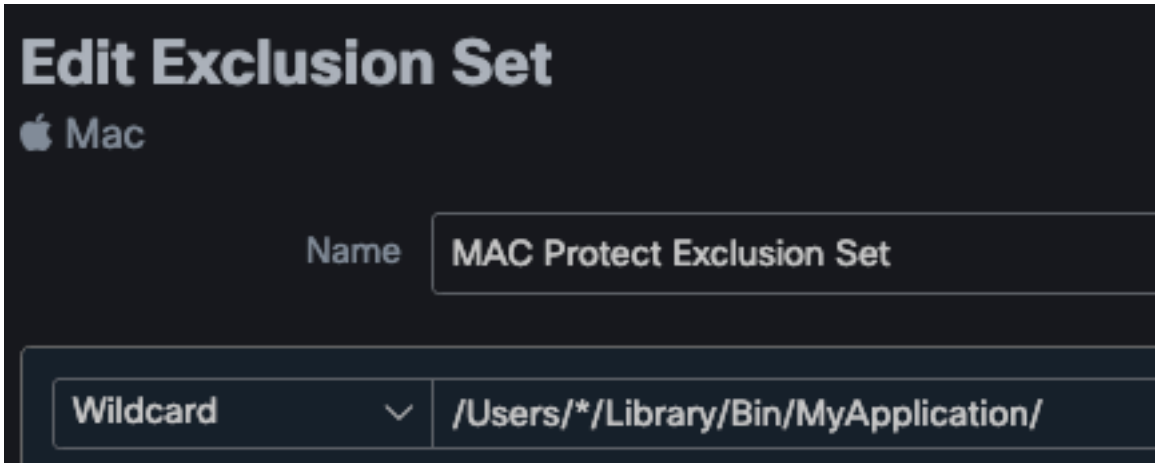


예를 들어, 홈 브루 응용 프로그램이 있는 경우 fileops.txt는 다음 활성 작업을 보여 줍니다.

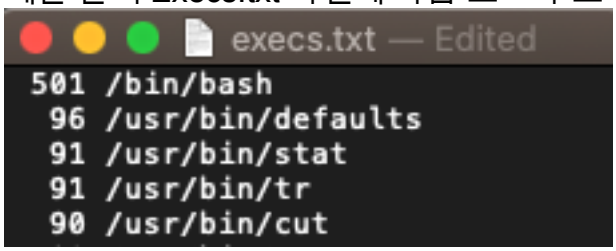
```
639 /Users/jesutorr/Library/Bin/MyApplication/support/

460 /Users/jesutorr/Library/Bin/MyApplication/logs/

219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```



- 프로세스가 식별되면 제외를 생성할 수 있습니다.
- 제외를 생성하려면
- AMP Console에서 Management(관리) **> Exclusions(제외)로 이동합니다.**
- 제외 세트를 선택하고 Edit(편집)를 클릭합니다.
- 이미지에 표시된 대로 제외를 추가할 수 있습니다.



- Execs.txt 파일에는 Connector가 번들을 수집하는 동안 실행되는 프로세스에서 사용하는 모든 명령이 포함되어 있습니다.여기에 나열된 경로는 모든 프로세스에서 사용하는 바이너리(/bin) 및 시스템 바이너리(/sbin)이므로 AMP 정책에서 제외되어서는 안 됩니다. 그러나 Execs.text에서 실행 중인 주 프로세스를 제공할 수 있습니다.
  예를 들어 Execs.txt 파일에 다음 로그가 표시되는 경우



홈 브루 애플리케이션은 bash를 사용하므로 애플리케이션이 높은 CPU의 원인임을 확인할 수 있습니다.

관련 정보

- AMP for Endpoints:macOS 및 Linux에서 제외 처리
- AMP for Endpoints 제외를 위한 모범 사례
- 기술 지원 및 문서 – Cisco Systems