AMP for Endpoints Linux Connector의 진단 데이터 수집

목차

소개

이 문서에서는 AMP For Endpoints Linux Connector에서 진단 파일을 생성하는 단계에 대해 설명합니다.Linux Connector에 기술적인 문제가 있는 경우 Cisco 기술 지원 엔지니어가 진단 파일에서 사용 가능한 로그 메시지를 분석할 수 있습니다.

진단 파일 생성

이 명령을 사용하면 Linux CLI(Command Line Interface)에서 진단 파일을 직접 생성할 수 있습니다.

```
/opt/cisco/amp/bin/ampsupport
```

그러면 바탕 화면에 .7z 파일이 만들어집니다.자세한 분석을 위해 이 파일을 Cisco TAC(Technical Assistance Center)에 제공할 수 있습니다.

디버그 모드

커넥터의 디버그 모드에서는 로깅에 대한 자세한 정보를 추가로 제공합니다.이를 통해 커넥터의 문제를 더 자세히 파악할 수 있습니다.이 섹션에서는 커넥터에서 디버그 모드를 활성화하는 방법에 대해 설명합니다.

> **경고:**디버그 모드는 Cisco에서 이 데이터를 요청하는 경우에만 활성화해야 합니다.디버그 모드를 더 오랫동안 활성화하면 디스크 공간을 매우 빠르게 채울 수 있으며 과도한 파일 크기로 인해 지원 진단 파일이 **커넥터 로그**를 수집하지 못할 수 있습니다.

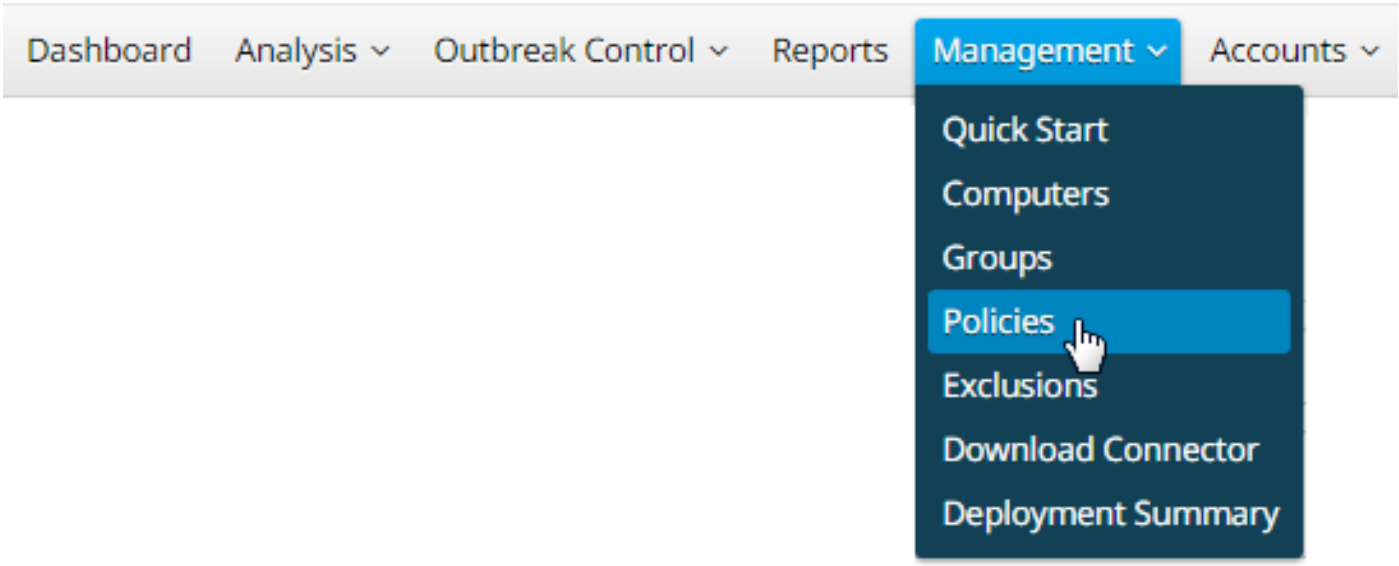
AMP 콘솔 사용

디버그 모드 사용

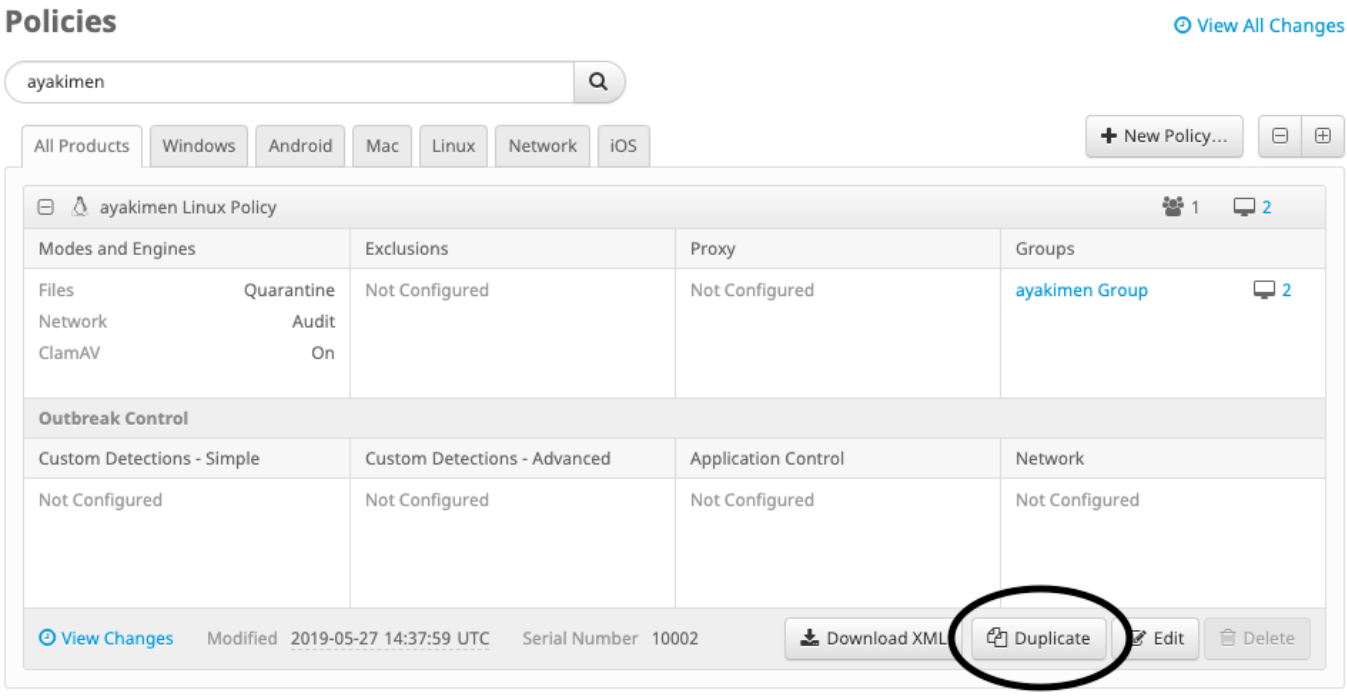
현재 정책에서 5단계 - 7로 디버그 모드를 활성화하거나 다음 모든 단계를 사용하여 디버그 모드에서 새 정책을 생성할 수 있습니다.

1단계. AMP 콘솔에 로그인합니다.

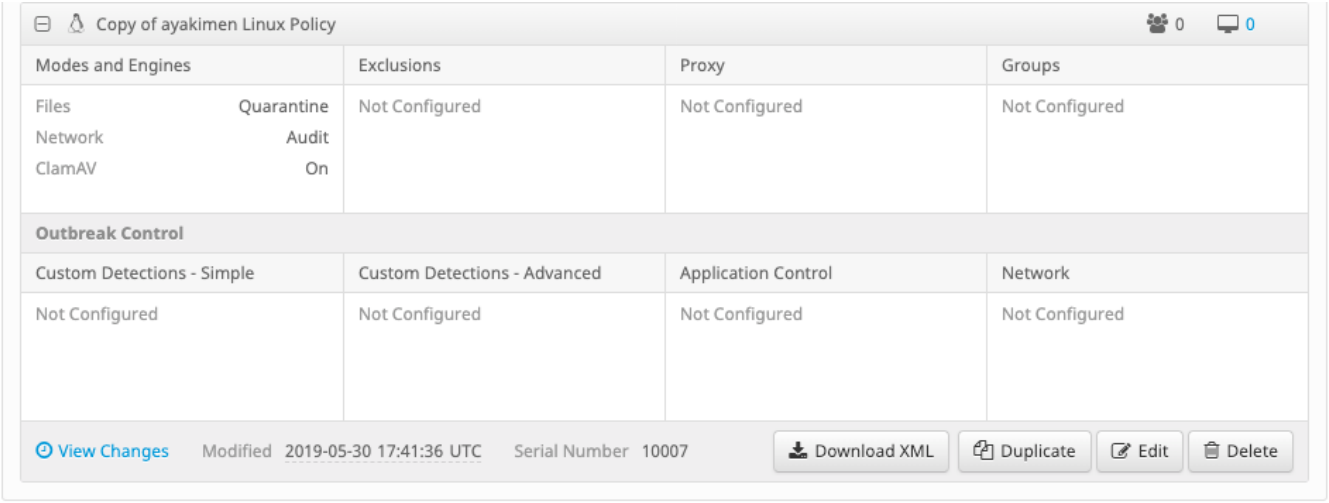
2단계. 관리 **> 정책을 선택합니다**.



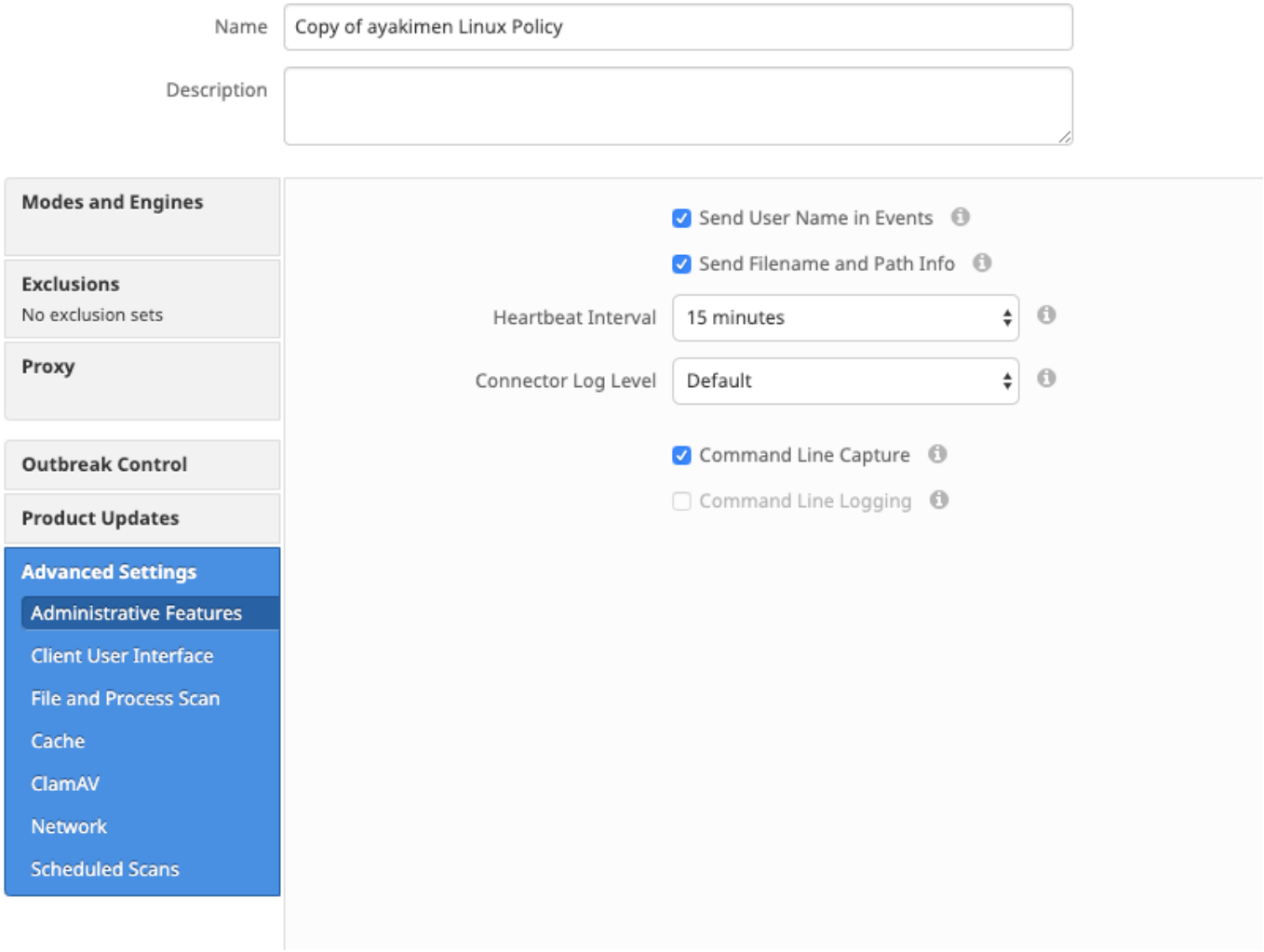
3단계. 엔드 디바이스 또는 컴퓨터에 적용된 정책을 찾아 Policy(정책)를 클릭하면 Policy(정책) 창이 확장됩니다.**복제를 클릭합니다**.



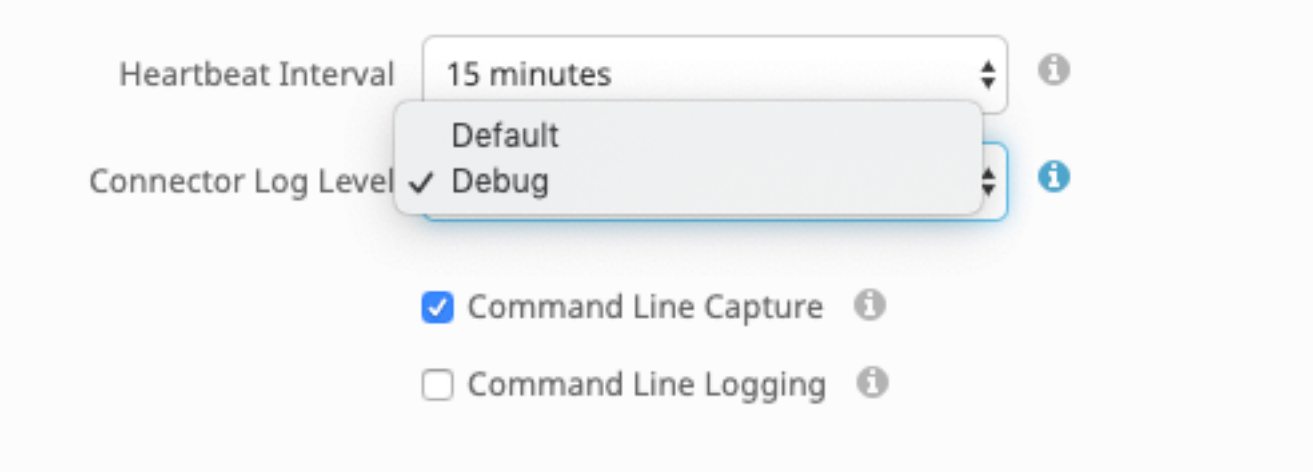
4단계. Duplicate를 **클릭하면** AMP 콘솔이 복사된 정책으로 업데이트됩니다.



5단계. **편집을 클릭하고 고급 설정**을 **클릭한** 다음 사이드바에서 관리 기능**을** 클릭합니다.



6단계. **커넥터 로그 레벨**의 경우 드롭다운 목록에서 디버그를 선택합니다.



7단계. 변경 사항을 저장하려면 저장을 누릅니다.

8단계. 새 정책을 저장한 후 새 *정책*을 포함하도록 그룹을 생성/변경하고 디버그 정보를 생성하려는 *최종* 디바이스를 만들어야 합니다.

디버그 모드 사용 안 함

디버그 모드를 비활성화하려면 완료한 단계와 동일한 단계를 수행하여 디버그 모드를 활성화하지만 **커넥터 로그 레벨**을 **기본값**으로 **변경합니다**.

명령줄 사용

디버그 모드 사용

콘솔에 연결 문제가 있는 경우 디버그 모드를 활성화하려면 CLI에서 다음 명령을 실행합니다.

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

다음은 출력입니다.

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

디버그 모드 사용 안 함

디버그 모드를 비활성화하려면 다음 명령을 사용합니다.

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

지원 툴 디버깅 중

파일 튜닝을 시작하기 전에 Connector의 데몬을 디버그 로깅 모드로 전환해야 합니다.이 작업은 AMP 콘솔을 통해 Management(*관리) -> Policies(정책)*에서 Connector의 정책 설정을 통해 수행됩니다.정책을 수정하고 Advanced Settings(고급 설정)Stab의 Administrative Features(관리 기능*) 섹션으로* 이동합니다.Connector *Log Level(커넥터 로그 레벨)* 설정을 **Debug(디버그)로 변경합니다**.

다음으로, 정책을 저장합니다.정책이 저장되면 커넥터가 동기화되었는지 확인합니다.나머지 튜닝을 계속하기 전에 최소 15-20분 동안 이 모드에서 커넥터를 실행합니다.

NB:조정이 완료되면 커넥터 로그 *레벨 설정*을 기본값으로 변경하여 커넥터가 가장 효율적이고 효과적인 모드로 실행되도록 합니다.

지원 툴 실행

이 방법은 AMP Mac Connector와 함께 설치된 애플리케이션인 Support Tool을 사용하는 것입니다.Applications(애플리케이션) 폴더에서 /Applications(애플리케이션)->Cisco AMP->Support Tool.app을 두 번 클릭하여 액세스할 수 있습니다.그러면 추가 진단 파일이 포함된 전체 지원 패키지가 생성됩니다.

An(an) 대체, 더 빠르게, 이 메서드는 다음 명령줄부터 a 터미널 세션:

```
sudo /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```
첫 번째 옵션은 관련 조정 파일만 포함하는 훨씬 작은 지원 파일을 생성합니다.두 번째 옵션은 로그와 같은 추가 정보를 포함하는 전체 지원 패키지를 제공하며, 이 패키지는 프로세스 제외 조정에 필요할 수 있습니다(커넥터 버전 1.11.0 이상에서 사용 가능).

어떤 방법으로 실행하든 지원 툴은 ~home에 두 개의 조정 지원 파일이 포함된 zip 파일을 생성합니다.fileops.txt 및 execs.txtfileops.txt에는 시스템에서 가장 자주 생성되고 수정된 파일의 목록이 포함되어 있습니다. 이는 경로/와일드카드 제외에 유용합니다.execs.txt에는 가장 자주 실행되는 파일 목록이 포함되며, 이는 프로세스 제외에 유용합니다.두 목록 모두 스캔 수를 기준으로 정렬됩니다. 즉 가장 자주 스캔되는 경로가 목록의 맨 위에 나타납니다.

커넥터를 디버그 모드에서 15-20분 동안 실행한 다음 지원 도구를 실행합니다.이 시간 동안 평균 1000회 이상의 적중률을 내는 파일이나 경로는 제외하기에 적합한 경우라는 것이 잘 알려진 규칙입니다.

제외 조정

경로, 와일드카드, 파일 이름 및 파일 확장명 제외 생성

경로 제외 규칙을 시작하는 한 가지 방법은 fileops.txt에서 가장 자주 스캔되는 파일 및 폴더 경로를 찾은 다음 해당 경로에 대한 규칙을 만드는 것입니다.정책이 다운로드되면 새 CPU 사용량을 모니터링합니다.CPU 사용량이 감소하면 데몬이 후속 조치를 취하는 데 시간이 걸릴 수 있으므로 정책이 업데이트된 후 5~10분 정도 걸릴 수 있습니다.여전히 문제가 발생하는 경우 도구를 다시 실행하여 관찰한 새 경로를 확인합니다.

- 로그 또는 저널 파일 확장명을 가진 모든 항목은 적합한 제외 대상으로 간주해야 합니다.

프로세스 제외 생성

NOTE: `Process Exclusions on Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).`
프로세스 제외와 관련된 모범 사례는 다음을 참조하십시오. AMP for Endpoints:macOS 및 Linux에서 제외 처리

좋은 조정 패턴은 먼저 execs.txt에서 실행되는 양이 많은 프로세스를 식별하고 실행 파일의 경로를 찾은 다음 이 경로에 대한 제외를 생성하는 것입니다.그러나 몇 가지 프로세스를 포함해서는 안 됩니다. 여기에는 다음이 포함됩니다.

- 일반 유틸리티 프로그램 - 일반 유틸리티 프로그램을 제외하지 않는 것이 좋습니다(예:다음 항목에 대한 계정 없이 usr/bin/grep). 사용자는 프로세스를 호출하는 애플리케이션을 확인할 수 있습니다(예:grep를 실행 중인 상위 프로세스를 찾고 상위 프로세스를 제외합니다.상위 프로세스를 프로세스 제외로 안전하게 만들 수 있는 경우에만 이 작업을 수행해야 합니다.상위 제외가 1차 하위 구성요소에 적용되는 경우 상위 프로세스에서 1차 하위 구성요소에 대한 통화도 제외됩니다.프로세스를 실행 중인 사용자를 확인할 수 있습니다.예:사용자 "root"가 많은 볼륨에서 프로세스를 호출하고 있는 경우, 프로세스를 제외할 수 있지만 지정된 사용자 'root"에 대해서만 AMP가 "root"가 아닌 사용자가 지정한 프로세스의 실행을 모니터링할 수 있습니다.**참고 :Process Exclusions는 커넥터 버전 1.11.0 이상에서 새로 추가되었습니다.따라서 일반 유틸리티 프로그램을 커넥터 버전 1.10.2 이상에서 경로 제외로 사용할 수 있습니다.그러나 이 방법은 성능 교체가 절대적으로 필요한 경우에만 권장됩니다.**

상위 프로세스를 찾는 것은 프로세스 제외에 중요합니다.프로세스의 상위 프로세스 및/또는 사용자가 발견되면 사용자는 특정 사용자에 대한 제외를 생성하고 하위 프로세스에 프로세스 제외를 적용할 수 있습니다. 그러면 프로세스 제외로 만들 수 없는 잡음 프로세스가 제외됩니다.

상위 프로세스 식별

1. 위에서 상위 프로세스 식별의 1-3단계를 수행합니다.
2. 다음 방법 중 하나를 사용하여 프로세스의 사용자를 식별합니다. 로그 라인에서 `U`에서 지정된 프로세스의 사용자 ID를 찾습니다(예:U:0).터미널 창에서 다음 명령을 실행합니다. `getent passwd # | -d:-f1`, 여기서 #은 사용자 ID입니다.다음과 유사한 출력이 표시되어야 합니다 `.Username`(여기서 Username은 지정된 프로세스의 사용자입니다.)
3. 이 사용자 카테고리의 프로세스 제외에 사용자 이름을 추가하여 특정 프로세스 제외에 대한 제외 범위를 줄이는 것이 중요합니다. **참고: 프로세스의 사용자가 시스템의 로컬 사용자이고 이 제외가 다른 로컬 사용자가 있는 여러 시스템에 적용되어야 하는 경우 프로세스 제외를 모든 사용자에게 적용하려면 사용자 범주를 비워 두어야 합니다.**

관련 정보

- Windows에서 실행되는 FireAMP Connector에서 진단 데이터 수집
- Mac OS에서 실행되는 FireAMP 커넥터에서 진단 데이터 수집
- **기술 지원 및 문서 – Cisco Systems**