Secure Endpoint Mac Connector 성능 조정 가이드

목차

소개

왜 튜닝해야 할까요?

Mac 엔드포인트에서 파일이 생성, 이동, 복사 또는 실행될 때마다 해당 파일에 대한 이벤트가 운영 체제에서 Secure Endpoint Mac 커넥터로 전송됩니다. 그러면 커넥터에서 해당 파일을 분석하게 됩니다. 분석 프로세스에는 일반적으로 문제의 파일을 해싱하고 컴퓨터와 클라우드에서 서로 다른 분석 엔진을 통해 실행합니다. 이 해싱 작업은 CPU 사이클을 소비한다는 사실을 인식하는 것이 중요합니다.

지정된 엔드포인트에서 발생하는 파일 작업과 실행 수가 많을수록 커넥터에서 해싱에 필요한 CPU 사이클과 I/O 리소스가 늘어납니다. 오버헤드를 줄이기 위해 커넥터에 몇 가지 기능이 추가되었습니다. 예를 들어, 생성, 이동 또는 복사 중인 파일이 이전에 분석된 경우 커넥터는 캐시된 결과를 사용합니다. 그러나 보안이 가장 중요한 경우와 같은 일부 이벤트의 경우 모든 이벤트가 항상 커넥터에 의해 완전히 분석됩니다. 즉, 하위 프로세스의 여러 반복적인 실행을 신속하게 전파하는 애플리케이션 또는 프로세스가 성능 문제를 일으킬 수 있습니다. 초당 1회 이상 하위 프로세스를 반복적으로 실행하는 애플리케이션을 찾아 제외하면 CPU 사용량이 크게 줄어들고 노트북의 배터리 수명이 증가할 수 있습니다.

생성 및 이동과 같은 파일 작업은 일반적으로 실행보다 영향을 덜 미치지만, 과도한 파일 쓰기 및 임시 파일 생성으로 인해 유사한 문제가 발생할 수 있습니다. 로그 파일에 자주 쓰는 애플리케이션 또는 여러 임시 파일을 생성하는 애플리케이션은 보안 엔드포인트가 불필요한 분석을 통해 많은 CPU 사이클을 소모하고 보안 엔드포인트 백엔드에 대한 많은 노이즈를 생성할 수 있습니다. 합법적인 애플리케이션의 복잡한 부분을 구별하는 것은 생산적이고 안전한 엔드포인트를 유지하는 데 매우 중요한 단계입니다.

이 문서의 목적은 파일 작업(생성, 이동 및 복사)을 구분하고 데몬 성능에 부정적인 영향을 미치고 CPU 주기를 낭비하는 데 도움이 됩니다. 이러한 파일 및 디렉토리 경로를 식별하면 조직에 적합한 제외 세트를 생성하고 유지 관리할 수 있습니다.

Cisco에서 유지 관리하는 정책에 사전 생성된 제외 목록을 추가하여 보안 엔드포인트 커넥터와 안티바이러스, 보안 또는 기타 소프트웨어 간의 호환성을 개선할 수 있습니다. 이러한 목록은 콘솔의 Exclusions(제외) 페이지에서 Cisco에서 유지 관리하는 제외로 사용할 수 있습니다.

튜닝 유형

다음과 같은 세 가지 유형의 제외 조정 옵션을 사용할 수 있습니다.

1. **사전 설치 조정 - 보안 엔드포인트 Mac 커넥터를 설치하기 전에 이 작업을 수행할 수 있습니다. 그러면 시스템에서 가장 사용량이 많은 애플리케이션과 경로를 정확하게 파악할 수 있습니다. 그러나, 매우 복잡한 프로세스이므로 사용자가 스스로 상당한 수준의 분석 및 집계를 수행해야 합니다.**
2. **지원 툴 조정** - Mac 커넥터가 설치된 후 이 작업을 수행할 수 있으며 추가 바이너리 없이 모든 엔드포인트에서 수행할 수 있습니다. 제한된 회색을 수행하며 문제가 되는 애플리케이션을 식별하는 데 유용합니다.
3. **Procmon Tuning** - 이 프로세스에서는 커넥터를 설치해야 하지만 사용자 정의 조정 도구인 Procmon 바이너리를 사용해야 합니다. 기본적으로 지원 툴 조정 기능의 보다 정교한 버전입니다. 이 방법에는 가장 많은 양의 컨피그레이션이 필요합니다. 그러나 최상의 결과를 제공합니다.

1. 사전 설치 조정

설치 전 튜닝은 가장 기본적인 튜닝 형식이며 주로 터미널 세션의 명령줄을 통해 수행됩니다.

OS X El Capitan의 최신 MAC의 경우 먼저 부팅하고 추적 보호를 비활성화하는 동안 복구 모드(command-r)로 부팅해야 합니다.

```
csrutil enable --without dtrace
```

가장 일반적인 파일 실행을 검사하려면 다음을 실행합니다.

```
$ sudo newproc.d | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

일반적으로 어떤 애플리케이션이 계속 실행 중인지를 보여줍니다. 많은 프로비저닝 애플리케이션이 스크립트를 실행하거나 이진 파일을 짧은 간격으로 실행하여 회사 소프트웨어 정책을 유지합니다. 초당 1회 이상 실행되는 것으로 보거나 짧은 간격으로 여러 번 실행되는 것으로 보이는 애플리케이션은 제외에 적합한 후보로 간주해야 합니다.

가장 일반적인 파일 작업을 검사하려면 다음 명령을 실행합니다.

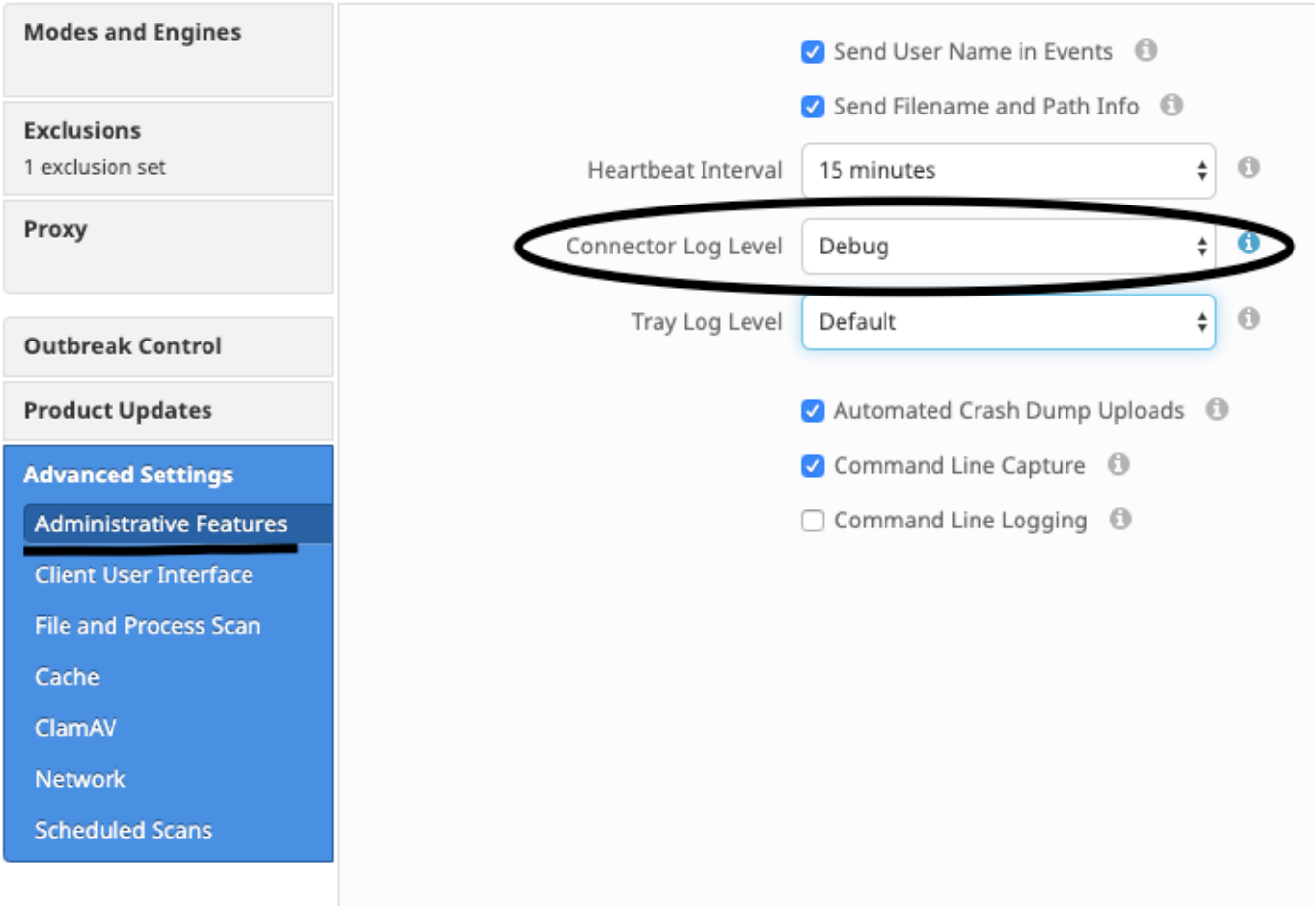
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

어떤 파일이 가장 많이 기록되는지 즉시 확인할 수 있습니다. 종종 응용 프로그램 실행, 백업 소프트웨어 복제 파일 또는 임시 파일을 쓰는 전자 메일 응용 프로그램을 통해 기록되는 로그 파일이 됩니다. 이 외에도 로그 또는 저널 파일 확장명을 가진 모든 항목을 적합한 제외 대상으로 간주해야 하는 것이 좋습니다.

2. 지원 툴 조정

디버그 로깅 활성화

파일 튜닝을 시작하기 전에 커넥터의 데몬을 디버그 로깅 모드로 전환해야 합니다. 이 작업은 보안 엔드포인트 콘솔을 통해 *Management -> Policies*에서 커넥터의 정책 설정을 통해 *수행됩니다*. 정책을 선택하고 정책을 편집한 다음 *Advanced Settings* 사이드바 아래의 *Administrative Features* 섹션으로 이동합니다. 커넥터 *로그 레벨* 설정을 *디버그*로 **변경합니다**.



다음, 정책을 저장합니다. 정책이 저장되면, 동기화되었는지 확인변함 c로연결기입니다. c 실행연결기 이 모드에서 적어도 15-20분 전에 나머지 조정.

참고: 조정이 완료되면 잊어라 변경 *커넥터 로그 레벨* 다음으로 설정 **기본값** 따라서 c연결기 실행인 이(가) 가장 효율적인 유효 모드.

지원 툴 실행

이 방법은 Secure Endpoint Mac 커넥터와 함께 설치된 애플리케이션인 Support Tool을 사용하는 것입니다. Applications 폴더에서 /Applications->Cisco Secure Endpoint->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 명령줄 부터 a 터미널 세션:

```
sudo/Library/Application Support/Cisco/AMP for Endpoints/SupportTool-x
```

따라서 관련 조정 파일만 포함하는 훨씬 작은 지원 파일이 생성됩니다.

어떤 방법으로 실행하든 지원 툴은 두 개의 조정 지원 파일이 포함된 zip 파일을 데스크톱에 생성합니다. fileops.txt 및 execs.txt fileops.txt에는 시스템에서 가장 자주 생성되고 수정된 파일의 목록이 들어 있습니다. execs.txt에는 가장 자주 실행되는 파일 목록이 포함됩니다. 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.

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 제외 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 Mac can only be implemented for Mach-O files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts) or .app (Application Bundles).`
프로세스 제외와 관련된 모범 사례는 다음을 참조하십시오.보안 엔드포인트: 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 보안 엔드포인트가 "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. execs.txt에서 대용량 프로세스(예: /bin/rm).
2. 지원 패키지에서 ampdaemon.log를 열고 syslog.tar의 압축을 푼 다음 경로 /Library/Logs/Cisco/ampdaemon.log을 따릅니다(기본 옵션으로 생성된 지원 패키지에서 제공되지 않음).
3. ampdaemon.log에서 제외할 프로세스를 검색합니다. 프로세스 실행을 보여 주는 로그 라인을 찾습니다(예: 19 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]: 데몬 Rx: VNODE:EXECUTE X:6210 P:3296 PP:3200 U:502 [/bin/rm]).
4. 다음 방법 중 하나를 사용하여 상위 프로세스를 식별합니다. 제외할 프로세스의 경로를 따라 이동할 수 있는 상위 프로세스 경로를 식별합니다(예: [/bin/rm] [*상위 프로세스 경로*])로그에 상위 프로세스 경로가 포함되지 않은 경우 로그 라인의 `PP:` 섹션(예: PP:3200).
5. 상위 경로 또는 상위 프로세스 ID를 사용하여 3단계와 4단계를 반복하여 현재 상위 프로세스의 상위를 결정합니다. 상위 프로세스 ID = 1(예: PP:1).
6. 프로세스 트리가 알려지면 제외할 작업을 대부분 또는 모두 포함하는 프로그램 경로를 찾아 애플리케이션을 고유하게 식별합니다. 이렇게 하면 다른 응용 프로그램에서 수행하는 작업을 의도적으로 제외할 가능성이 최소화됩니다.

프로세스 사용자 식별

1. 위에서 상위 프로세스 식별의 1-3단계를 수행합니다.
2. 다음 방법 중 하나를 사용하여 프로세스의 사용자를 식별합니다. 로그 라인에서 U에서 지정된 프로세스의 사용자 ID를 찾습니다(예: U:502).Terminal(터미널) 창에서 다음 명령을 실행합니다`. dscl  /Users UniqueID | grep` #. 여기서 #은 사용자 ID입니다 .Username `502`와 유사한 출력이 표시되어야 합니다. 여기서 `Username`은 지정된 프로세스의 사용자입니다.
3. 이 사용자 이름은 User(사용자) 카테고리의 Process Exclusion(프로세스 제외)에 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.**