AMP for Endpoints Linux Connector용 기본 문제 해결 가이드

목차

소개

이 문서에서는 성능 문제를 해결하는 기본적인 방법에 대해 설명합니다 켜짐 Cisco Advanced Malware Protection ()AMP) 대상 엔드포인트 Linux 커넥터.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP for Endpoints
- Linux/Unix기반 운영 체제

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Red Hat Enterprise Linux (RHEL) / Community Enterprise 운영 체제(Cent)OS) 버전 6.10 7.7
- AMP for Endpoints Linux 커넥터 버전 1.11.1

Linux 운영 체제와 호환되는 AMP 버전의 전체 목록은 [이 문서](#)를 참조하십시오.

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 커넥터는 시스템에서 모든 활성 파일(자신을 이동, 복사 및/또는 수정하는 파일)을 스캔합니다

. 단, 명시적으로 알리지 않는 한 커넥터가 활성 상태일 때 너무 많은 프로세스와 작업이 실행되면 성능 문제가 발생할 수 있으며, 이로 인해 CPU 사용률, 속도 저하, 실행 속도가 저하되거나 느리게 실행되지 않는 소프트웨어가 발생할 수도 있습니다.또한 AMP 커넥터는 클라우드 평판을 기준으로 파일을 차단할 수 있으며, 경우에 따라 오탐(false positive)이 발생할 수 있습니다. 두 가지 문제를 모두 해결할 수 있는 솔루션은 이러한 경로 및 프로세스 이 가이드를 통해 해결되지 않는 성과 관련 문제가 오탐(false positive) 또는 성능 관련 문제가 있는 경우 티켓 지원을 요청하는 것이 좋습니다.

기본 성능 문제를 해결하는 흐름은 다음과 같습니다.

- 문제가 재생되는 동안 디버그 번들을 수집합니다.
- AMP 지원 툴 실행
- 관련 파일 검토
- 필요에 따라 제외 추가

문제 해결

디버그 번들을 수집하는 방법

디버그 번들은 커넥터의 자세한 디버그 정보(예: 스캔 로그)를 포함하는 zip 파일입니다.이 번들은 AMP for Endpoints 커넥터와 관련된 대부분의 문제를 해결하는 데 필수적입니다.디버그 번들을 수집하려면 AMP for Endpoints Linux Connector에서 진단 데이터 수집에 제공된 단계를 수행합니다.

amp 지원 툴에서 수집하여 디버그 번들을 실행하는 정보는 무엇입니까?

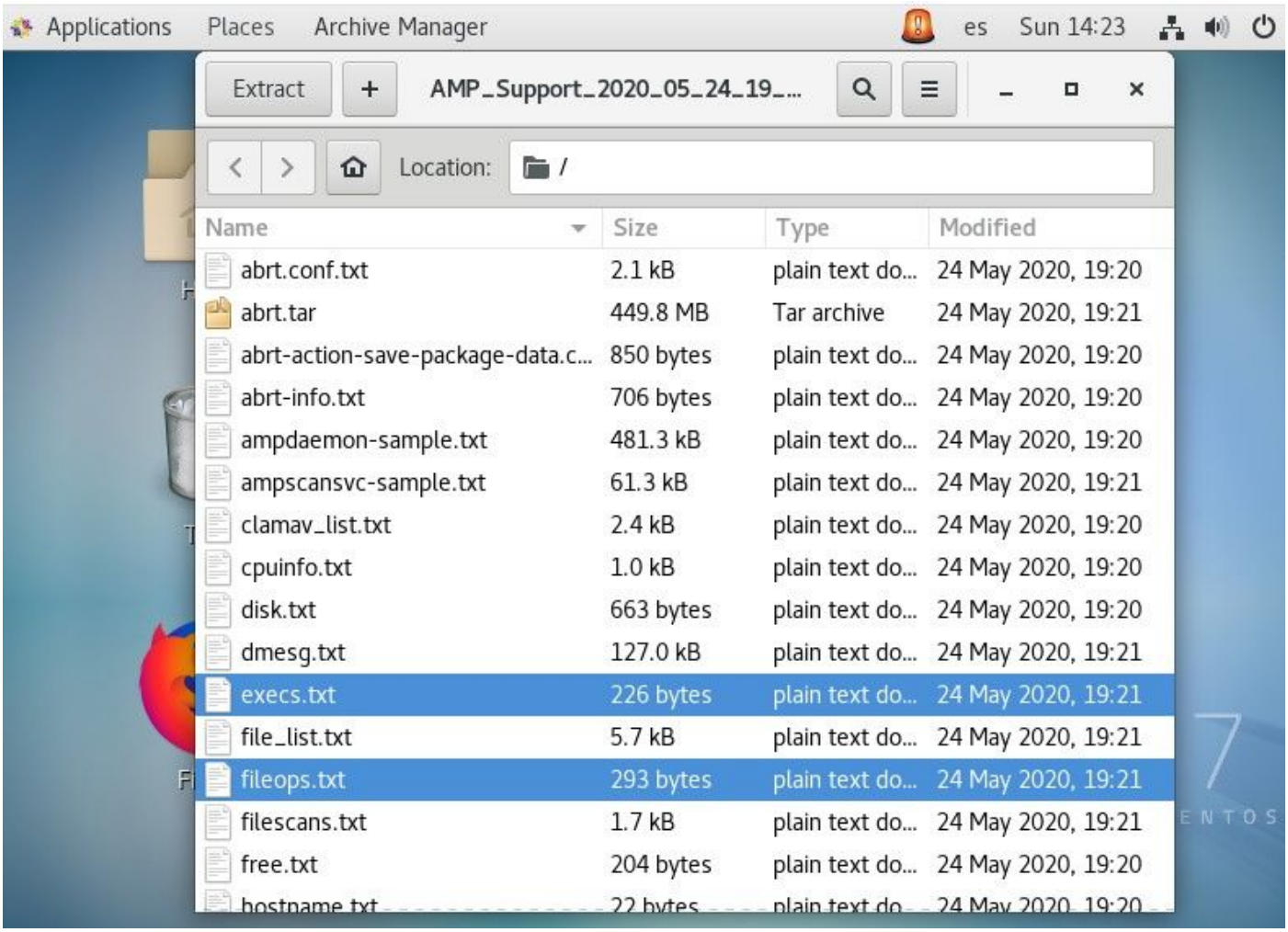
디버그 번들 프로세스 입력은 *ampsupport는 이미지에 표시된 대로 일부 log-collection 명령을 실행합니다.*

```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: $(cat "${dir}/count")";echo -e "
Executable: $(cat "${dir}/executable")"; echo -e "
Uid: $(cat "${dir}/uid")";echo -e "
Reason: $(cat "${dir}/reason")"; echo -e "
Package: $(cat "${dir}/package")"; done
find: warning: you have specified the -maxdepth option after a non-option argument -typ
e, but options are not positional (-maxdepth affects tests specified before it as well
as those specified after it).  Please specify options before other arguments.

cat: /var/spool/abrt/oops-2020-05-18-18:21:09-10472-0//executable: No such file or dire
ctory
[ -e '/etc/abrt/abrt.conf' ] && cat '/etc/abrt/abrt.conf'
[ -e '/etc/abrt/abrt-action-save-package-data.conf' ] && cat '/etc/abrt/abrt-action-sav
e-package-data.conf'
cat /proc/slabinfo
```

기본 Linux 번들 로그를 읽고 영향을 받는 경로 및 프로세스를 식별하는 방법

Linux AMP for Endpoints 디버그 번들은 a 과민증 그러나 기본적인 성능 문제 해결을 위해 이미지에 표시된 것처럼 파일 ops.txt, fiescan.txt 및 execs.txt를 검토할 수 있는 파일은 몇 개 뿐입니다.



파일 작업(fileops) 텍스트 파일은 기본 성능 문제 해결 도구로 작동합니다.커넥터가 실행되는 동안 엔드포인트에서 현재 모든 활성 작업을 나열합니다.이는 필요/안전하다고 판단되는 경우 정책 제외 세트에 추가할 경로입니다.

다음과 같이 읽습니다.

- <번들 수집 프로세스가 실행되는 동안 수행된 경로에 대해 수행된 검색 수> /<Path scanned>

스캔 예:

- 1 /homeet/user/.mozila/Firefox/

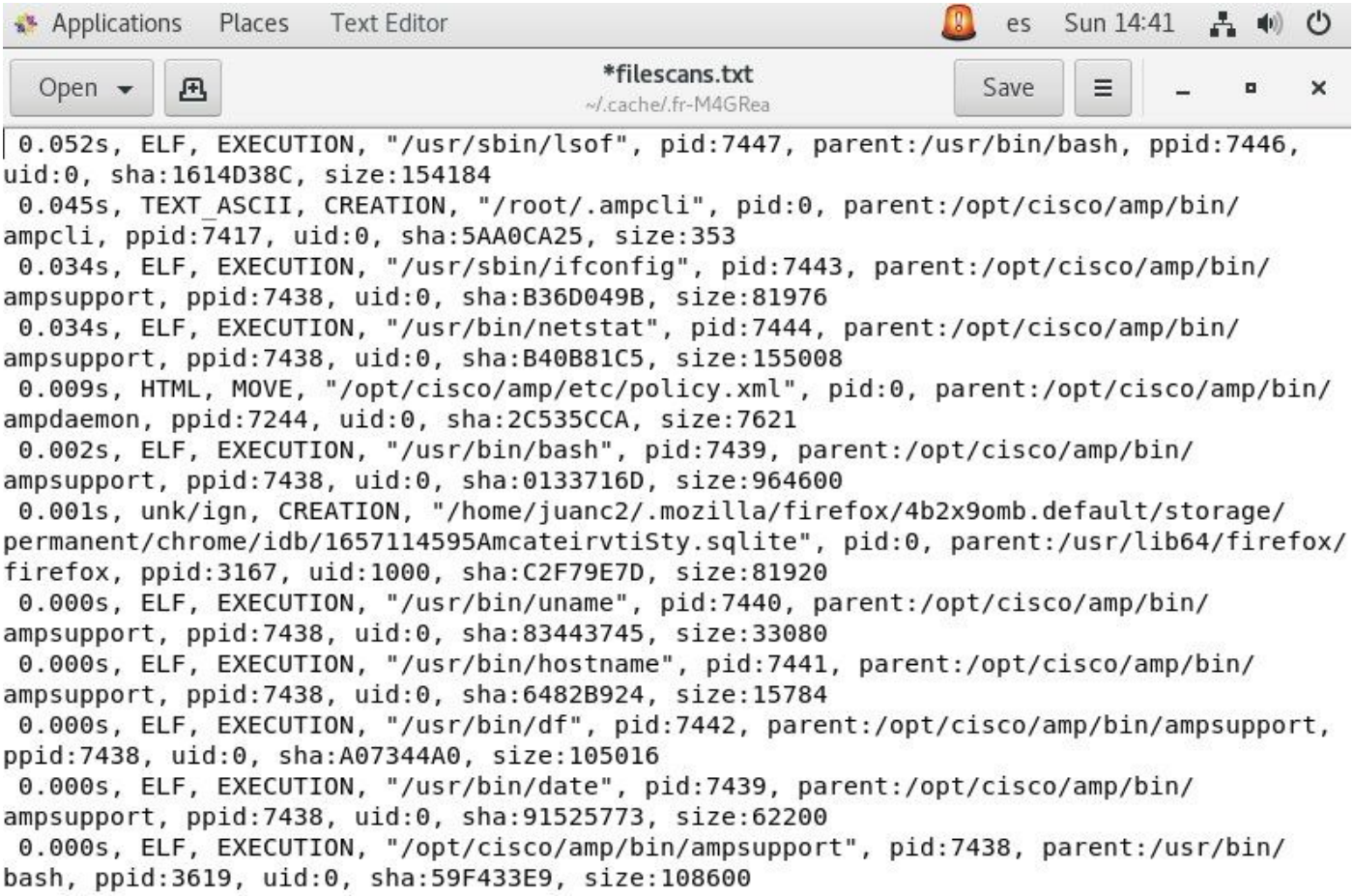
File Scans(filescan) Text 파일은 커넥터가 디버그 정보를 수집하는 동안 실행되는 모든 프로세스를 나열합니다.

다음과 같이 표시됩니다.

- <Execution time> , <File Type>, <Operation type>, <Process path>, <Parent process path> , <Process ID>, <Parent Process ID>, <SHA signature (Not SHA256)> <File Size>

파일 실행(실행) 텍스트 파일에는 커넥터에서 번들을 수집하는 동안 커넥터의 활성 프로세스에서 사용하는 모든 Linux 명령이 나열됩니다.

경고: 여기에 나열된 경로는 모든 프로세스가 사용하는 바이너리(/bin) 및 시스템 바이너리(/sbin)이므로 AMP 정책에서 제외되지 않아야 합니다. 그러나 이 목록은 대상 시스템에서 실행되는 다른 프로세스에서 어떤 작업을 수행하는지 파악하는 데 유용할 수 있습니다.



일단 파악되면 정책을 통해 경로를 제외합니다. AMP [for Endpoint Exclusions에 대한 모범 사례를 따르십시오.]

Mac 및 Linux 커넥터에서 처리하는 프로세스 제외도 정책을 통해 추가되지만 방법은 약간 다릅니다. [macOS 및 Linux의 프로세스 제외].

제외가 추가되면 문제가 지속되면 테스트 및 모니터링합니다.AMP TAC 지원에 문의하십시오.