AMP for Endpoints:Linux의 ClamAV 바이러스 정의 옵션

목차

소개

Linux Connector 버전 1.11.0부터 AMP for Endpoints는 이제 두 가지 ClamAV 바이러스 정의 구성 옵션을 제공합니다.

1. Linux 전용
2. 전체 ClamAV

Linux 전용 옵션을 사용하기 전에 Linux 커넥터는 전체 ClamAV 바이러스 정의 세트를 사용하여 파일을 스캔했습니다.이 세트에는 Linux, macOS, Windows 및 Android용 악성코드 서명이 포함되어 있습니다.포괄적인 커버리지를 제공하지만 상당한 런타임 리소스(예: CPU 시간 및 메모리)가 필요합니다. 일부 Linux 시스템에서는 소규모 Linux 전용 ClamAV 바이러스 정의 세트를 사용하도록 AMP를 구성하면 이점이 있습니다.

Linux 전용 바이러스 정의 파일 크기가 전체 세트의 10% 미만입니다.더 작은 세트를 사용하면 컴퓨팅 오버헤드가 줄어들고 리소스가 제한된 시스템에서 AMP를 실행할 수 있습니다.성능상의 이점에도 불구하고 비 Linux 악성코드에 대한 커버리지가 줄어들기 때문에 이 컨피그레이션은 일부 애플리케이션에만 적합합니다.예를 들어, Linux 파일(예: 애플리케이션 서버)을 호스트/저장하는 서버에는 적합하지만 비 Linux 파일(예: FTP, 메일 및 SMB 파일 서버)을 호스트하거나 저장하는 서버에는 적합하지 않습니다. 시스템 관리자는 적절한 바이러스 정의 집합을 선택하려면 이 트레이드오프의 균형을 맞춰야 합니다.

> **중요!**
>
> 새 Linux 전용 바이러스 정의 옵션을 사용하기 전에 모든 엔드포인트를 커넥터 버전 1.11.0 이상으로 업그레이드하는 것이 좋습니다.1.10.x 및 이전 Connector 버전에서는 새 옵션을 사용할 수 있지만, 경우에 따라 이러한 동작은 직관적이지 않을 수도 있습니다.자세한 내용은 *이전 버전과의 호환성* 섹션을 참조하십시오.

이전 버전과의 호환성

새로운 Linux 전용 바이러스 정의 옵션을 사용하도록 엔드포인트를 구성하기 전에 고려해야 할 중요한 이전 버전과의 호환성 문제가 있습니다.1.10.x 및 이전 Connector는 전체 세트가 이미 다운로드된 경우 전체 바이러스 정의를 계속 사용합니다.새 Linux 전용 바이러스 정의 옵션을 사용하도록 구성된 경우, 커넥터는 전체 바이러스 정의 세트의 업데이트를 중지하고 이후 Linux 바이러스 정의 집합만 업데이트합니다.따라서 엔드포인트에서 최신 Linux 바이러스 정의를 사용하지만 오래된

macOS, Windows 및 Android 정의를 사용할 수 있습니다.

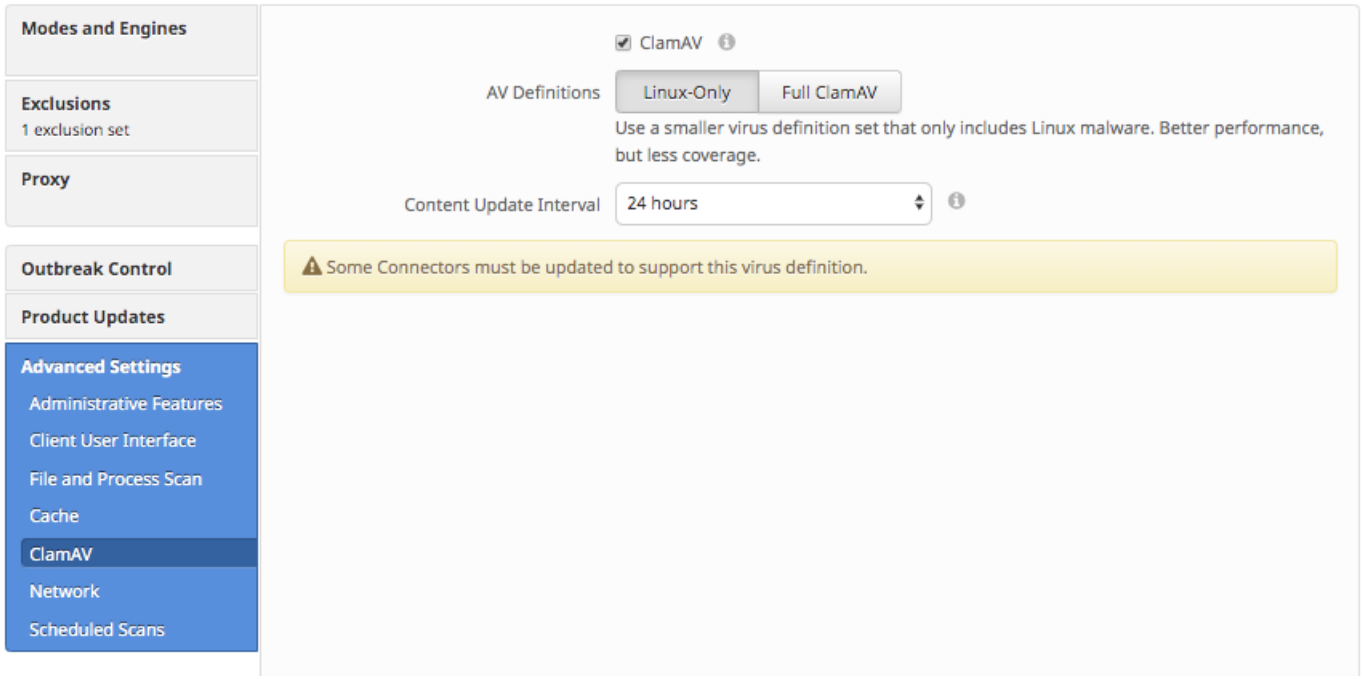
다음과 같은 두 가지 해결 방법이 있습니다.

1. 커넥터를 1.11.0 이상으로 업그레이드합니다.
2. ClamAV 바이러스 정의 설정을 다시 Full ClamAV로 변경합니다.

ClamAV 바이러스 정의 옵션 변경

ClamAV Virus Definition 옵션은 AMP for Endpoints 웹 포털을 사용하여 구성할 수 있습니다.각 정책에 대한 옵션은 다음으로 이동하여 변경할 수 있습니다.

관리 > 정책 > [Linux 정책] > 편집 > 고급 설정 > ClamAV



AV 정의 정책 설정이 변경된 후 다음 예약된 바이러스 정의 업데이트에서 엔드포인트에 새 설정이 적용됩니다.이 지연은 '콘텐츠 업데이트 내부' 정책 설정에 의해 제어됩니다.

정책에서 관리하는 하나 이상의 커넥터가 호환되지 않는 Linux 커넥터 버전을 실행 중인 경우 "Some Connectors must be updated to support this virus definition" 경고가 ClamAV Advanced Settings(ClamAV 고급 설정) 화면에 나타날 수 있습니다.Linux 전용 정의 설정을 사용하기 전에 커넥터를 업그레이드하고 이 경고를 해결하는 것이 좋습니다.

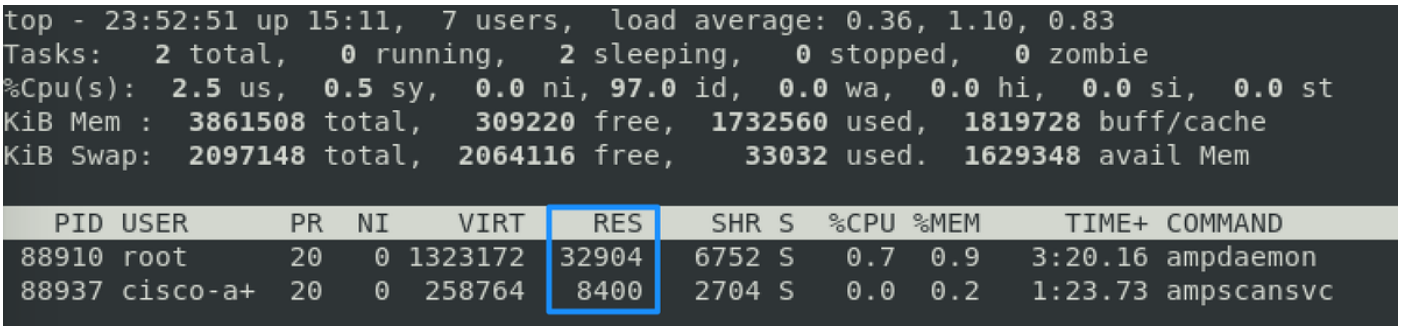
엔드포인트에서 새 설정 확인

Linux 전용 정의를 사용하도록 구성된 경우 두 AMP Connector 프로세스의 결합된 상주 메모리 크기는 100MB 미만이어야 합니다.

다음 명령을 사용하여 이를 검토할 수 있습니다.

```
top -p `pidof ampdaemon` -p `pidof ampscansvc`
```

다음은 샘플 출력입니다.


top - 23:52:51 up 15:11, 7 users, load average: 0.36, 1.10, 0.83
Tasks: 2 total, 0 running, 2 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2.5 us, 0.5 sy, 0.0 ni, 97.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 3861508 total, 309220 free, 1732560 used, 1819728 buff/cache
KiB Swap: 2097148 total, 2064116 free, 33032 used. 1629348 avail Mem
PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
88910 root 20 0 1323172 32904 6752 S 0.7 0.9 3:20.16 ampdaemon
88937 cisco-a+ 20 0 258764 8400 2704 S 0.0 0.2 1:23.73 ampscansvc