

AMP for Endpoints Linux Primer

목차

소개

다음은 AMP for Endpoints Linux Connector의 기본 사항 및 일반적인 개요입니다.

시스템 요구 사항

다음 운영 체제가 지원됩니다. [Linux OS 호환성](#)

- AMP 커넥터의 적절한 작동을 위해서는 최소 1.5GB의 사용 가능한 하드 디스크 공간이 필요합니다.

네트워크 연결 요구 사항

Required [-Server-Addresses-for-Advanced-Malware-Protection-AMP 참조](#)

설치

CentOS 릴리스 6.4에 성공적으로 로컬 설치 결과(최종)

/var/log/messages

```
Mar 3 14:47:34 vmc stabulic: cisco-amp: starting rpm pre scriptlet (1)
Mar 3 14:47:34 vmc stabulic: cisco-amp: rpm pre scriptlet done
Mar 3 14:47:35 vmc stabulic: cisco-amp: starting rpm post scriptlet (1)
Mar 3 14:47:35 vmc stabulic: cisco-amp: skip installing redirfs since it is already installed
Mar 3 14:47:35 vmc stabulic: Mar 03 14:47:35 vmc AMPInstaller[2107]: Info: executing post
Mar 3 14:47:35 vmc stabulic: Mar 03 14:47:35 vmc AMPInstaller[2107]: Info: sending event
Mar 3 14:47:35 vmc ampinsthelper: Set minimum reported log level to error
Mar 3 14:47:36 vmc ampinsthelper: Shutdown file logger for module:ampsupport
Mar 3 14:47:36 vmc stabulic: Mar 03 14:47:36 vmc AMPInstaller[2107]: Info: event sent
Mar 3 14:47:36 vmc stabulic: Mar 03 14:47:36 vmc AMPInstaller[2107]: Info: starting connector
Mar 3 14:47:36 vmc kernel: Kernel logging (proc) stopped.
Mar 3 14:47:36 vmc rsyslogd: [origin software="rsyslogd" swVersion="5.8.10" x-pid="1133" x-
info="http://www.rsyslog.com"] exiting on signal 15.
Mar 3 14:47:37 vmc kernel: imklog 5.8.10, log source = /proc/kmsg started.
Mar 3 14:47:37 vmc rsyslogd: [origin software="rsyslogd" swVersion="5.8.10" x-pid="2136" x-
info="http://www.rsyslog.com"] start
Mar 3 14:47:37 vmc init: /etc/init.conf: Unable to load configuration: No such file or
directory
Mar 3 14:47:37 vmc init: cisco-amp pre-start: redirfs already loaded
Mar 3 14:47:37 vmc init: cisco-amp pre-start: loading avflt
Mar 3 14:47:37 vmc kernel: Cisco Anti-Virus Filter for the RedirFS Framework 1.0. Based on
RedirFS AVFflt 0.6 <www.redirfs.org>
Mar 3 14:47:37 vmc init: cisco-amp pre-start: avflt loaded
Mar 3 14:47:37 vmc init: cisco-amp pre-start: loading ampnetworkflow
Mar 3 14:47:37 vmc init: cisco-amp pre-start: ampnetworkflow loaded
Mar 3 14:47:37 vmc init: cisco-amp pre-start: done
Mar 3 14:47:37 vmc ampdaemon: Set minimum reported log level to notice
Mar 3 14:47:37 vmc stabulic: Mar 03 14:47:37 vmc AMPInstaller[2107]: Info: connector started
Mar 3 14:47:37 vmc stabulic: cisco-amp: rpm post scriptlet done
Mar 3 14:47:37 vmc yum[1995]: Installed: ciscoampconnector-1.0.0.184-1.el6.x86_64[root@vmc
cisco]# ps aux | grep -i amp root 825 0.0 1.1 203376 11532 ? Ssl 13:47 0:00
/opt/cisco/amp/bin/ampmon -addr=
root 2166 0.0 0.0 0 0 ? S 14:47 0:00 [csc0_amp_msg_wq]
root 2167 0.0 0.0 0 0 ? S 14:47 0:00 [csc0_amp_prc_wq]
```

```
root      2170  1.4  3.7 814824 37540 ?      Ssl  14:47  0:02 /opt/cisco/amp/bin/ampdaemon
root      2264  0.0  0.0 103240  884 pts/0  S+   14:50  0:00 grep -i amp
```

```
[root@vmc amp]# lsof -p 825 COMMAND PID USER  FD  TYPE DEVICE SIZE/OFF  NODE NAME
ampmon 825 root  cwd   DIR  253,0    4096    2 /
ampmon 825 root  rtd   DIR  253,0    4096    2 /
ampmon 825 root  txt   REG  253,0  6775183 262792 /opt/cisco/amp/bin/ampmon (deleted)
ampmon 825 root  mem   REG  253,0  1921216 654097 /lib64/libc-2.12.so
ampmon 825 root  mem   REG  253,0  142640 654121 /lib64/libpthread-2.12.so
ampmon 825 root  mem   REG  253,0  154664 654085 /lib64/ld-2.12.so
ampmon 825 root  0u    CHR  1,3      0t0    4418 /dev/null
ampmon 825 root  1u    CHR  1,3      0t0    4418 /dev/null
ampmon 825 root  2u    CHR  1,3      0t0    4418 /dev/null
ampmon 825 root  3r    REG  253,0  26555 393043 /var/log/cisco/ampdaemon.log (deleted)
ampmon 825 root  5r    DIR  0,10     0      1 inotify
ampmon 825 root  6w    REG  253,0    1508 393591 /var/log/cisco/ampmon.log [root@vmc amp]#
```

```
lsof -p 2170 COMMAND      PID USER  FD  TYPE DEVICE SIZE/OFF  NODE NAME
ampdaemon 2170 root  cwd   DIR  253,0    4096    2 /
ampdaemon 2170 root  rtd   DIR  253,0    4096    2 /
ampdaemon 2170 root  txt   REG  253,0  7717228 262795 /opt/cisco/amp/bin/ampdaemon
ampdaemon 2170 root  mem   REG  253,0   27424 654111 /lib64/libnss_dns-2.12.so
ampdaemon 2170 root  mem   REG  253,0   65928 654113 /lib64/libnss_files-2.12.so
ampdaemon 2170 root  mem   REG  253,0  1921216 654097 /lib64/libc-2.12.so
ampdaemon 2170 root  mem   REG  253,0   67592 654184 /lib64/libbz2.so.1.0.4
ampdaemon 2170 root  mem   REG  253,0  110960 654123 /lib64/libresolv-2.12.so
ampdaemon 2170 root  mem   REG  253,0   596272 654105 /lib64/libm-2.12.so
ampdaemon 2170 root  mem   REG  253,0  142640 654121 /lib64/libpthread-2.12.so
ampdaemon 2170 root  mem   REG  253,0   16304 654201 /lib64/libuuid.so.1.3.0
ampdaemon 2170 root  mem   REG  253,0   19536 654103 /lib64/libdl-2.12.so
ampdaemon 2170 root  mem   REG  253,0   43880 654125 /lib64/librt-2.12.so
ampdaemon 2170 root  mem   REG  253,0   88600 654152 /lib64/libz.so.1.2.3
ampdaemon 2170 root  mem   REG  253,0  206672 654199 /lib64/libidn.so.11.6.1
ampdaemon 2170 root  mem   REG  253,0  154664 654085 /lib64/ld-2.12.so
ampdaemon 2170 root  0u    CHR  1,3      0t0    4418 /dev/null
ampdaemon 2170 root  1u    CHR  1,3      0t0    4418 /dev/null
ampdaemon 2170 root  2u    CHR  1,3      0t0    4418 /dev/null
ampdaemon 2170 root  3u    unix 0xffff88003d8e1c80 0t0 17076 socket
ampdaemon 2170 root  4w    REG  253,0   1871 393045 /var/log/cisco/ampdaemon.log
ampdaemon 2170 root  5r    CHR  1,9      0t0    4423 /dev/urandom
ampdaemon 2170 root  6u    REG  253,0  46080 262812
/opt/cisco/amp/etc/cloud_query.cache
ampdaemon 2170 root  7u    REG  253,0   2048 262813 /opt/cisco/amp/etc/events.db
ampdaemon 2170 root  8u    sock  0,6      0t0 17096 can't identify protocol
ampdaemon 2170 root  9r    FIFO  0,8      0t0 17118 pipe
ampdaemon 2170 root  10w   FIFO  0,8      0t0 17118 pipe
ampdaemon 2170 root  11r   REG  0,3      0 17119 /proc/2170/mounts
ampdaemon 2170 root  12u   CHR  248,0    0t0 17062 /dev/ampavflt
ampdaemon 2170 root  13u   REG  253,0   8192 262819
/opt/cisco/amp/etc/quarantine/quarantine.db
ampdaemon 2170 root  14u   REG  253,0  27648 262844
/opt/cisco/amp/etc/quarantine/retrospective.db
ampdaemon 2170 root  15u   unix 0xffff88003b5503c0 0t0 17121 /var/run/sfampd
ampdaemon 2170 root  17r   IPv4  17549    0t0  TCP 172.16.168.139:48668->ec2-46-51-181-139.eu-west-1.compute.amazonaws.com:https (ESTABLISHED)
ampdaemon 2170 root  18r   IPv4  17182    0t0  TCP 172.16.168.139:49661->ec2-52-16-63-115.eu-west-1.compute.amazonaws.com:https (CLOSE_WAIT)
ampdaemon 2170 root  19u   sock  0,6      0t0 17194 can't identify protocol
```

```
root@vmc cisco]# ls -al /var/log/cisco/ total 16
drwxr-xr-x. 2 root root 4096 Mar  3 14:47 .
drwxr-xr-x. 4 root root 4096 Mar  3 14:47 ..
-rw-----. 1 root root  0 Mar  3 14:47 ampcli.log
-rw-----. 1 root root 1871 Mar  3 14:47 ampdaemon.log
-rw-----. 1 root root  0 Mar  3 14:47 ampinstaller.log
-rw-----. 1 root root 1256 Mar  3 14:50 ampmon.log binaries in /opt/cisco/amp/bin/
[root@vmc ~]# initctl start cisco-amp
```

```
cisco-amp start/running, process 1567
[root@vmc ~]# /opt/cisco/amp/bin/ampcli status
[logger] Set minimum reported log level to notice
Trying to connect...
Connected.
Status: Connected
Scan: Ready for scan
Last Scan: 2016-05-02 08:01 PM
Policy: Protect Policy for FireAMP Linux (#446)
[root@vmc ~]# initctl stop cisco-amp
cisco-amp stop/waiting
```

rhel 6에서 amp 서비스 비활성화

```
# initctl stop cisco amp
# mv /etc/init/cisco-amp.conf /etc/init/cisco-amp.conf.disabled
# mv /etc/init/cisco-ampupdater.conf /etc/init/cisco-ampupdater.conf.disabled
# chmod -x /etc/cron.hourly/cisco-ampupdater.cron
```

커넥터 정책

고객은 AMP Console Policy(AMP 콘솔 정책) 목록에서 자동으로 생성된 2개의 정책을 볼 수 있습니다.

AMP for Endpoints Linux Connector용 감사 정책

AMP for Endpoints Linux Connector용 보호 정책

두 정책의 유일한 차이점은 File Conviction Mode입니다.

File(파일) -> Modes(모드) -> File Conviction(파일 확정)

감사 - 감사

보호 - 격리

고객은 이러한 정책을 수정하거나, 구성을 위한 정책을 복사하거나, 새 정책을 모두 생성할 수 있습니다.

다른 커넥터와 구성 차이점

클라이언트 사용자 인터페이스 구성 없음

통신 전용 포트 443

File(파일) -> Mode(모드) -> On Execute Mode(실행 모드)는 "Passive(패시브)"뿐입니다.

네트워크 -> DFC -> 탐지 작업은 "감사"만 해당

정책 - 파일 모드

실행 모드

최대 성능 저하를 유발할 수 있는 'Active' 모드를 허용하지 않습니다. 'Passive' 모드에서는 성향이 결정되는 동안 실행이 허용되며, 처리가 악성인 경우 프로세스가 종료됩니다.

최대 스캔 파일 크기 - 5MB

최대 스캔 아카이브 크기 - 50MB

참고: 이러한 크기는 향후 변경될 수 있습니다. 이러한 크기는 Mac/OSX 정책 설정과 동일합니다.

정책 - DFC(Device Flow Correlation)

탐지 작업은 기본적으로 "Audit(감사)"로 설정되며 구성할 수 없습니다. 탐지가 있을 경우 DFC 이벤트가 생성되지만, 지금은 네트워크 흐름이 종료되지 않습니다. 이것은 설계에 의한 것이다

정책 - 오프라인 엔진

클램AV

ClamAV는 Linux 커넥터에 통합된 오프라인 엔진입니다. 기본적으로 활성화되어 있습니다. 즉, 설치할 디스크 공간이 최대 200MB여야 하며 ClamAV 정의를 위한 공간이 충분한지 확인해야 합니다.

현재 사용할 수 없는 기능

TETRA

TETRA 엔진은 Windows용이므로 없습니다.

SPERO 및 에토스

SPERO 및 Etos 엔진은 Windows 파일에만 적용되며 Linux 커넥터에서는 구현되지 않습니다. 이러한 엔진의 인텔리전스는 AMP 클라우드에서 1:1 매칭으로 변환됩니다. Linux Connector는 1:1을 통해 많은 양의 중량을 처리할 수 있기 때문에 이를 지원할 수 있습니다.

FAQ:

Q: Linux ?

A: Linux .

Q: ?

A: VPC 2.4.1 Mac Linux .

Q: ?

A: .AMP Connector Red Hat CentOS . AMP .