思科安全終端Linux初級課程

目錄

簡介

下面是思科安全終端Linux聯結器的一些基本資訊和一般概述。

系統要求

支援以下作業系統： Cisco安全終端Linux聯結器作業系統相容性

- 安全端點聯結器的正常工作至少需要1.5 GB的可用硬碟空間。

網路連線要求

請參閱 Required-Server-Addresses-for-Advanced-Malware-Protection-AMP

安裝

在CentOS 6.4版上成功本地安裝的結果（最終）

/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 AVFlt 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 [csco_amp_msg_wq]
root       2167  0.0  0.0      0     0 ?        S    14:47   0:00 [csco_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.logbinaries 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
```

禁用rhel 6上的amp服務

 # 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

聯結器策略

客戶將看到在其思科安全控制檯策略清單中自動建立2個策略。
思科安全終端Linux聯結器的稽核策略
思科安全終端Linux聯結器的保護策略
這兩種策略之間的唯一區別是檔案定罪模式
File -> Modes -> File Conviction
稽核 — 稽核
保護 — 隔離
客戶可以編輯這些策略，複製策略進行配置，也可以建立一個新策略。
與其他聯結器的主要配置差異
無客戶端使用者介面配置
僅通訊埠443
File -> Mode -> On Execute Mode is Only "Passive"
網路 — > DFC ->檢測操作僅是「稽核」

策略 — 檔案模式
執行模式時

不允許可能導致效能嚴重下降的「主動」模式。 在「被動」模式下，在確定處置時允許執行 — 如果處置是惡意的，則進程終止。

最大掃描檔案大小 — 5 MB
最大掃描存檔大小 — 50 MB
注意：這些大小將來可能會發生變化。這些大小與Mac/OSX策略設定相同。

策略 — DFC（裝置流關聯）
檢測操作預設為「Audit」，不可配置。檢測到時會生成DFC事件，但此時不會終止網路流。這是設計好的

策略 — 離線引擎
ClamAV
ClamAV是整合到Linux聯結器的離線引擎 — 預設情況下啟用。
總之，這意味著需要約200 MB的磁碟空間用於安裝，並且可用以確保有足夠的空間用於ClamAV定義。

當前不可用的功能

TETRA

沒有TETRA引擎，因為它只適用於Windows。

SPERO和Ethos

SPERO和Ethos引擎也僅適用於Windows檔案，並且未在Linux聯結器中實現。

來自這些引擎的智慧將轉換為AMP雲中的1:1匹配項 — Linux Connector將覆蓋這些內容，因為1:1用於執行大量繁重的工作。

常見問題:

Q:Linux?

A:Linux

Q:

VPC 2.4.1 MacLinux

Q:

A:LinuxLinuxLinux