

Cisco Secure Endpoint Linux Primer

تايوت حمل

قمدق مل

Cisco Secure Endpoint Linux لصول مل ماع ضرعو تايوت ساسال ضعب يل امي ف

ماظن ل تابل طتم

[Cisco Secure Endpoint Linux ليغشت ماظن قفاوت](#): موعدم ةيلالت ليغشت ل ةمظن [Connector](#)

- لصول ليغشت ل ةحات مل تابل صرقل ةحاسم نم ىندأ دك تايوت باغيغ 1.5 رفوت مزلي .
ححص لكشب ةنم ال ةياهن ل ةطقن

ةكبش لابل لاصلت ل تابل طتم

AMP-راض ل امارب ل نم قمدق مل ةي امحل لىل لوصحل ل ةبول طمل ل مداخل ل نيوان عجار
[تايوت ل](#)

(يئاهن) 6.4 رادصل ل CentOS لىل عجان ل يل حمل تايوت ل جئاتن

/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 [csc0_amp_msg_wq]
```

```

root      2167  0.0  0.0      0      0 ?      S    14:47  0:00 [cisco_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

```

تفعيل AMP على RHEL 6

```

# initctl فاقى 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

```

لصوملا جهن

نم ةنم آلا مكحتلا ةدحو تاسايس ةمئاق نمض ايئاق لت امه ؤاشن! مت نيجهن ءالمعل ىريس Cisco ءصاخلا.

ل Cisco Secure Endpoint Linux Connector قيقدتلا ءسايس

ل Cisco Secure Endpoint Linux Connector ءيامللا ءسايس

فللملا ءنادا ءضو وه نيجهنلا نيّب ديحوللا قرفلا

FILE -> ءاضوا -> ءضوا

تاباسحلا ءءءارم - تاباسحلا ءءءارم

لزلل - ءيامللا

ءديء ءسايس ءاشن! و نيوكتلل تاسايسلا ءسن و تاسايسلا هذه ريرت ءالمعل لك مي لملكلا.

ىرخاللا لصلوملا نم نيوكتللا ي قريبك تافالءءا

للمعل مدءءسم ءءءاول نيوكتلل ءءوي ال

443 طقف ءفنملا لاصللا

طقف "لمءا" وه ءيفنننلا ءضوي ف -> ءضولا FILE ->

طقف "قيقدت" وه فشكلا ءارءا -> DFC -> ءكءبشلا

فللملا ءضو - تاسايسلا

ءيفنننلا ءضوي ف

"لمءالا" ءضوي ف. ءءءلل ءيءش ءفءنا ي ف بءسءي نأ نكمي يءلا 'Active' ءضوب ءمسي ال ريصملا ناك اذا ءيلمعل ءاهن! مءي - يءاهنللا ريصملا ءيءء ءانءا ءيفنننلا ءامسللا مءي اراض يءاهنللا.

ءيءاباغي م 5 - يءوؤللا ءمسللا فلم ءءءل ىصقلا ءءلا

ءيءاباغي م 50 - يءوؤللا ءمسللا فيءشرا ءءءل ىصقلا ءءلا

Mac/OSX ءهن تاءءءا سفن يء ءءءالا هذه. ل بءءسملا يء ءءءالا هذه ريرءءء ءق: ءءءالم

ءءءالا قفءءءا (ءءءا) - تاسايسلا

ءاشن! مءسي. نيوكتلل لءاق ريرغ وهو "قيقدت" ىل ءيءا يءا ءءءا ءفشكلا ءارءا ءءءا مءي. ءقولا اءه يء ءكءبشلا قفءءءا ءاهن! مءي نل لءا يءا ىل ءفشكلا ءانه نوئي ءمءن DFC ءءءا.

مېم صت لال خ نم اذه

لاصتا نود تاكرحم - تاسايس لال

فامال ك

يضا رت فالك ش ب هني كمت متي - Linux ل صوم ي ف جدم لصتم ريغ كرحم نع قرابع ClamAV تي اب اغيم 200 وحن غلبت صرق عحاسم كانه نوكت نا بجي هنا هلمجم ي ف كلذ ينعي و ClamAV تافيرعتل عي فاك عحاسم دوجو نامضل عحاتم نوكت ناو، تي بتتل

ايلاح عرفوت م ريغ تازي ملال

ارتت

طوقف Windows ب صاخ هنأل، TETRA كرحم دجوي ال

سوثي او وري بس

ي ف اهق ببطت متي الو طوقف Windows تافلم يلع اضيأ Ethos و Spero تاكرحم ق بطننت Linux ل صوم

ةباحس ي ف 1:1 تاي رابم ي ل تاكرحم لال هذه نم ةيتارابختس الال تامول عملال ةم جرت متت فوس م اي قلل 1:1 مادختس متي شيح تانوكم لال هذه ل ةي طغت ب Linux ل صوم ي طحي فوسو — AMP ةل ي ق ثل ل لي محت لال تاي لمع نم دي دع لال

ةرركت ملال ةلئس الال

:

:

:

: VPC 2.4.1 Mac Linux .

:

. Linux kernel kernel [Cisco Secure Endpoint Connector Kernel](#) . Linux Secure Endpoint kernel . kernel .

