

AMP für Endgeräte Linux-Einführung

Inhalt

Einführung

Im Folgenden finden Sie einige Grundlagen und eine allgemeine Übersicht zum Linux Connector für AMP für Endgeräte.

Systemanforderungen

Folgende Betriebssysteme werden unterstützt: [Kompatibilität von Linux-Betriebssystemen](#)

- Mindestens 1,5 GB verfügbarer Festplattenspeicher ist für eine angemessene Funktionsweise des AMP Connectors erforderlich.

Netzwerkanbindungsanforderungen

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

Installation

Ergebnisse der erfolgreichen lokalen Installation von CentOS 6.4 (Final)

/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
```

AMP-Dienst für Rrhel 6 deaktivieren

```
# 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
```

Connector-Richtlinie

Die Kunden sehen zwei automatisch in ihrer AMP-Konsolenrichtlinienliste erstellte Richtlinien.

Überwachungsrichtlinie für AMP für Endgeräte Linux Connector

Schutzrichtlinie für AMP für Endgeräte Linux Connector

Der einzige Unterschied zwischen den beiden Richtlinien ist der Dateikonvertierungsmodus.

Datei -> Modi -> Dateikonvertierung

Audit - Audit

Schutz - Quarantäne

Kunden können diese Richtlinien bearbeiten, die Richtlinien für die Konfiguration kopieren oder komplett eine neue Richtlinie erstellen.

Große Konfigurationsunterschiede mit anderen Anschlüssen

Keine Konfiguration der Client-Benutzeroberfläche

Nur Kommunikation Port 443

Datei -> Modus -> Im Ausführungsmodus ist "Passiv".

Netzwerk -> DFC -> Erkennungsaktion lautet "Audit" (nur Audit)

Richtlinien - Dateimodus

Im Ausführungsmodus

Verhindert den Modus "Aktiv", der zu extremen Leistungseinbußen führen kann. Im Modus "Passive" (Passiv) ist die Ausführung zulässig, während die Einstufung festgestellt wird. Der Prozess wird beendet, wenn die Einstufung schädlich ist.

Maximale Größe der Scan-Datei: 5 MB

Maximale Größe des Scan-Archivs - 50 MB

Hinweis: Diese Größen können sich in Zukunft ändern. Diese Größen entsprechen den Mac/OSX-Richtlinieneinstellungen.

Richtlinien - DFC (Device Flow Correlation)

Die Erkennungsaktion ist standardmäßig auf "Audit" (Audit) festgelegt und kann nicht konfiguriert werden. DFC-Ereignisse werden generiert, wenn eine Erkennung vorliegt. Der Netzwerkfluss wird

jedoch zu diesem Zeitpunkt nicht beendet. Dies ist beabsichtigt

Richtlinien - Offline-Engines

ClamAV

ClamAV ist eine Offline-Engine, die in den Linux Connector integriert ist - standardmäßig aktiviert. Insgesamt bedeutet dies, dass ca. 200 MB Festplattenspeicher für die Installation benötigt werden und verfügbar sein muss, um sicherzustellen, dass genügend Platz für ClamAV-Definitionen vorhanden ist.

Funktionen derzeit nicht verfügbar

TETRA

Es gibt kein TETRA-Modul, da es nur für Windows ist.

SPERO und Ethos

SPERO- und Ethos-Engines gelten auch nur für Windows-Dateien und sind nicht im Linux Connector implementiert.

Die Informationen dieser Engines werden in 1:1-Matches in der AMP-Cloud umgewandelt - der Linux Connector deckt diese ab, da 1:1 für die Schwerarbeit eingesetzt wird.

Häufig gestellte Fragen:

Frage: Wird es zusätzliche Linux-Versionen geben?

Antwort: Es werden zukünftig weitere Versionen von Linux hinzugefügt.

Frage: Wird Private Cloud unterstützt?

A: Ja, da VPC 2.4.1 Mac und Linux unterstützt werden.

Frage: Werden benutzerdefinierte Kernels unterstützt?

Antwort: Nein. Benutzerdefinierte kompilierte Kernels werden derzeit nicht unterstützt. der AMP Connector ist nur für die Arbeit mit ursprünglich gelieferten Kernels mit Red Hat, CentOS und Ubuntu LTS zertifiziert. Kunden müssen mit dem AMP Support and Engineering-Team zusammenarbeiten, bevor sie versuchen, auf Betriebssystemen mit benutzerdefinierten kompilierten Kernels bereitzustellen.