How To Use ClamAV & Cron Jobs To Run Daily And Hourly Virus Scans

by admin on September 20, 2014

Clam AntiVirus (ClamAV) is a free and open-source, cross-platform antivirus software tool-kit able to detect many types of malicious software, including viruses. In the previous article, I shown you "How To Install/Compile ClamAV In CentOS 6". In this article, I will continue to show you How to use ClamAV & Cronjobs to run daily & hourly virus scans.

The first, I will create a new directory to store script & log files of ClamAV

```
# mkdir -p /usr/local/clamav/script
# mkdir -p /usr/local/clamav/log
```

Setting up hourly scans

Creating a file called name **clamscan_hourly**

```
# vi /usr/local/clamav/script/clamscan_hourly
```

And add the following code

```
#!/bin/bash
SUBJECT="`hostname` PASSED HOURLY SCAN"
EMAIL="admin@domain.com"
LOG=/usr/local/clamav/log/clamav.log
TMP_LOG=/tmp/clam.hourly

av_report() {

    if [ `cat ${TMP_LOG}  | grep Infected | grep -v 0 | wc -l` != 0 ]
    then
            SUBJECT="[WARNING] `hostname` PASSED HOURLY SCAN"
    fi

        EMAILMESSAGE=`mktemp /tmp/virus-alert.XXXXX`
    echo "To: ${EMAIL}" >>  ${EMAILMESSAGE}
    echo "From: alert@domain.com" >>  ${EMAILMESSAGE}
    echo "Subject: ${SUBJECT}" >>  ${EMAILMESSAGE}
    echo "Importance: High" >> ${EMAILMESSAGE}
    echo "X-Priority: 1" >> ${EMAILMESSAGE}
    echo "`tail -n 50 ${TMP_LOG}`" >> ${EMAILMESSAGE}
    sendmail -t < ${EMAILMESSAGE}

        cat ${TMP_LOG} >> ${LOG}
        rm -rf ${TMP_LOG}
}

av_scan() {
        touch ${TMP_LOG}
        find / -not -wholename '/sys/*' -and -not -wholename '/proc/*' -mmin -61 -type f -print0 | xargs -0 -r clamscan --exclude-dir=/proc/ --exclude-dir=/sys/ --quiet --infected --log=${TMP_LOG}
}

av_scan
av_report
freshclam
```

Save the file. Make sure it's executable, type

```
# chmod +x /usr/local/clamav/script/clamscan_hourly
```

Setting up daily scans

Creating a file called name **clamscan_daily**

```
# vi /usr/local/clamav/script/clamscan_daily
```

And add the following code

```
#!/bin/bash
SUBJECT="`hostname` PASSED DAILY SCAN"
EMAIL="admin@domain.com"
LOG=/usr/local/clamav/log/clamav.log
TMP_LOG=/tmp/clam.daily

av_report() {

    if [ `cat ${TMP_LOG}  | grep Infected | grep -v 0 | wc -l` != 0 ]
    then
        SUBJECT="[WARNING] `hostname` PASSED DAILY SCAN"
    fi

        EMAILMESSAGE=`mktemp /tmp/virus-alert.XXXXX`
    echo "To: ${EMAIL}" >>  ${EMAILMESSAGE}
    echo "From: alert@domain.com" >>  ${EMAILMESSAGE}
    echo "Subject: ${SUBJECT}" >>  ${EMAILMESSAGE}
    echo "Importance: High" >> ${EMAILMESSAGE}
    echo "X-Priority: 1" >> ${EMAILMESSAGE}
    echo "`tail -n 50 ${TMP_LOG}`" >> ${EMAILMESSAGE}
    sendmail -t < ${EMAILMESSAGE}

        cat ${TMP_LOG} >> ${LOG}
        rm -rf ${TMP_LOG}
}

av_scan() {
        touch ${TMP_LOG}
        clamscan -r / --exclude-dir=/sys/ --quiet --infected --log=${TMP_LOG}
}

av_scan
av_report
```

Save the file. Make sure it's executable, type

```
# chmod +x /usr/local/clamav/script/clamscan_daily
```

Setting Up Crontab to run ClamAV hourly & daily scans

Type the following command

```
# crontab –e
```

Add the following code

```
# ClamAV scan
01 * * * * /usr/local/clamav/script/clamscan_hourly
01 00 * * * /usr/local/clamav/script/clamscan_daily
```

Setting up log rotation for ClamAV

Creating a file called name **clamav**, type

```
# vi /etc/logrotate.d/clamav
```

Add the following code

```
/usr/local/clamav/log/*.log {
    daily
    dateext
    dateformat –%d%m%Y
    missingok
    rotate 90
    compress
    delaycompress
    notifempty
    create 600 root root
}
```

Related Posts:

- [Auto Update CentOS Server With yum Command](#)

Remote
Developer J

Remote Developer Jobs, Work
From Anywhere - Proxify

× ⓘ

{ 1 comment… read it below or [add one](#) }

Tooc [September 20, 2014 at 9:37 am](#)

Great article.
This app can scan PHP shell ?

[Reply](#)

Leave a Comment

Name *

E-mail *

Website

Submit

Tagged as: [clamav crontab](#), [clamav daily scan](#), [clamav hourly scan](#), [contab](#), [cronjob](#)

Previous post: [How To Install/Compile ClamAV In CentOS 6](#)

Next post: [How To Install HHVM 3.2.0 On CentOS 6.5](#)

GET FREE TIPS & NEWS

Make the most of Linux Sysadmin work!

Enter your email   Join

İslami Evlilik Sites
eÇift - Tanışma Sitesi

- **Follow us**

- **Seach**

  To search, type and hit enter

- **Categories**
  - [Networking](#)
  - [Security](#)
  - [Sys Admin](#)
  - [WebServer](#)
  - [Shell Scripting](#)
  - [MySQL](#)
  - [Monitoring](#)
  - [Bash Shell](#)
  - [File System](#)

- **Blogroll**
  - [free wordpress themes](#)
  - [Sienna Miller](#)

[Privacy Policy](#) | [Terms of Service Advertise](#) | [Copyright Info](#) | [Sitemap](#)