ClamAV - The free Anti Virus solution for Windows on Li...

Article URL
ClamAV - The free Anti Virus solution for Windows on Linux

Author
SsecurityHome.eu

Published: 15 March 2011

Last updated on 22 May 2013.

Â

Why do you want to install an Windows anti-virus scanner on Linux?
Well there can be many reasons. You have a linux file-server that host a samba-share to some windows clients? You might have a mail-server and you want the mails to be scanned?

ClamAV is a free GPLed anti-virus solution which provides a lot of advantages when installed in Linux. Sticking to the philosophy of linux, it contains a set of command line tools which can be used to check if a file on your system is infected by a virus.

Installation is easy
yum install clamav
(for RedHat based systems)
OR
apt-get install clamav
(for Debian based systems)
emerge app-antivirus/clamav
(for Gentoo systems)

ClamAV basically installs three binary tools on your system (in the /usr/bin directory), them being :
* freshclam

- As you know an anti-virus solution is only as good as the latest virus updates it has. This tool is used to update the virus databases on your system. It downloads the latest virus updates from the internet and keeps your anti-virus solution upto date.

* clamscan

- This is the tool that actually checks your files to see if they are infected.

* sigtool

- When you download the latest virus updates from the net, there should be a way of verifying the validity of the update. This is achieved by the sigtool. It is used to verify the digital signatures of databases and list virus signature names among other things.

First thing to do is update the virus database:
freshclam

Now you can do a scan
clamscan -r --log=/home/uname/virus_log -i /mnt/share/
The above command will scan */mnt/share/*

directory recursively (*-r*

) and log (

--log

) the result in the virus_log file and only print (*-i*

) infected files to the output.

To make things easy for myself, I put everything in a script:
Based on a script by Devon Hillard

```
#!/bin/bash

# email subject
SUBJECT="VIRUS DETECTED ON `hostname`!!!"
# Email To ?
EMAIL="my@email.com"
# Log location
LOG=/var/log/clamav/scan.log
DIR=/var/share/

check_scan () {

    # Check the last set of results. If there are any "Infected" counts that aren't zero,
    # we have a problem.
    if [ `tail -n 12 ${LOG}  | grep Infected | grep -v 0 | wc -l` != 0 ]
    then
        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 ${LOG}`" >> ${EMAILMESSAGE}
        sendmail -t      fi
}

#first update virus-db
freshclam
```

```
#the actual scan
clamscan -r ${DIR} --quiet --infected --log=${LOG}

#check results
check_scan
```