Installation and Configuration of Clamav antivirus on Debian GNU / Linux

Author : admin

Clamav Antivirus is one of must have packages installed on a new *Debian Linux server*. It is not only necessary whether configuring a new Mail server be it Qmail or Postfix but is good to have to always check files on a Webserver. Until few years infecting of Sites with Viruses / Installing WebShells or Backdooring for further access using Perl or PHP vulnerable PHP code was not so common, However nowadays with increase of complexity of languages and increase of not security minded programmers this possibility dramatically increaed. Thus nowadays, whether I *configure a new Apache + PHP + CGI support server* I always install **Clamav AV**. Some might argue that Clamav Virus definitions are still too little compared to proprietary solutions like **BitDefender** / **AVG** or **Avast** but since my experience with this under Linux is not so bright as well as Clamav captures essential Viruses and Backdoors I still prefer to keep on with *Clamav*. Even on home Desktops with Linux clamav is of use as there are plenty of free-ware software for Linux which come only distributed only in a binary form and hence its good to check them with clamav before use whether they don't contain some well known Rootkit or Virus. Over the years Clamav has done great job for me whether I had to *clean up "hacked" hosts containing script kiddie exploit scanners or Virus infected ELF binaries*

.

1. Installing ClamAV in Debian Wheezy Linux

Before time there was a separate Debian repository called **Volatille** providing latest version release of Clamav, since Debian Squeeze Volatille project is discontinued, thus installing on Wheezy as a deb package is only available via standard Debian repositories.

```
 apt-get update && apt-get --yes upgrade
...
```

```
 apt-get install --yes clamav clamav-daemon
```

As package dependencies you get installed:

clamav clamav-base clamav-freshclam libbz2-1.0 libclamav1 libcurl3 libidn11 ucf

Clamav-Daemon will launch immediately after packages are installed and is available as process name **/usr/sbin/clamd**

```
 # ps ax |grep -i clam
 2641 ?        Ssl    6:39 /usr/sbin/clamd
 2791 ?        Ss    12:04 /usr/bin/freshclam -d --quiet
12300 pts/0    S+     0:00 grep -i clam
```

2. Updating Clamav Antivirus Definitions

Its worthy say few words on **clamav-freshclam** as it is part of *ClamAV* which is used to update *Clamav Virus definitions*. Update of ClamAV vir definitions are updating automatically through **/usr/bin/freshclam** daemon which is started automatically by Debian postconfiguration scripts right after Clamav install.

Manual update of AV definitions can be done also with **freshclam**.

```
 # freshclam
ClamAV update process started at Sun Sep  8 17:48:36 2013
main.cvd is up to date (version: 54, sigs: 1044387, f-level: 60, builder: sven)
daily.cvd is up to date (version: 17830, sigs: 1696886, f-level: 63, builder: neo)
bytecode.cld is up to date (version: 225, sigs: 42, f-level: 63, builder: dgoddard)
```

To keep an eye on definition auto-updates (useful to check where something fails), check out in **/var/log/clamav/freshclam.log**

A sure indication that Anvirus updates are conducting fine should be log records like:

```
Sun Sep  8 16:27:44 2013 -> --------------------------------------
Sun Sep  8 17:27:44 2013 -> Received signal: wake up
Sun Sep  8 17:27:44 2013 -> ClamAV update process started at Sun Sep  8 17:27:44 2013
Sun Sep  8 17:27:44 2013 -> main.cvd is up to date (version: 54, sigs: 1044387, f-level: 60, builder: sven)
Sun Sep  8 17:27:44 2013 -> daily.cld is up to date (version: 17830, sigs: 1696886, f-level: 63, builder: neo)
Sun Sep  8 17:27:44 2013 -> bytecode.cld is up to date (version: 225, sigs: 42, f-level: 63, builder: dgoddard)
Sun Sep  8 17:27:47 2013 -> --------------------------------------
```

3. Configuring ClamAV

For Desktop use clamav default config is pretty good. However for servers its good to raise 2 up MaxThreads:

By default *MaxThreads* is 12

```
MaxThreads 12
```

Change to from 30 to 80 depending on how powerful machine ClamAV runs, even on some servers more Clamav threads might be necessary

```
 MaxThreads 30
```

Other value I like changing is **SelfCheck 3600** is too long time for clamav Virus definitions integrity I prefer to set it to 600, i.e.

```
 SelfCheck 600
```

By default ClamAV is also configured to scan archive files as well. However for this to work you will have to have previously installed **unzip** and **unrar** on system. If still you don't have them installed run:

```
 # apt-get install --yes unrar unzip
...
```

Note that you will need to have **non-free** part of Debian deb repositories to **/etc/apt/sources.list**

Here is one of my **sources.list**

```
deb http://ftp.uk.debian.org/debian squeeze main contrib non-free
deb http://security.debian.org/ squeeze/updates main contrib non-free
deb-src http://security.debian.org/ squeeze/updates main contrib non-free

deb http://ftp.debian.skynet.be/ftp/debian/ squeeze main contrib non-free
deb-src http://ftp.debian.skynet.be/ftp/debian/ stable main contrib non-free

deb http://security.debian.org squeeze/updates main contrib non-free
deb-src http://security.debian.org/ squeeze/updates main contrib non-free
```

3. Scanning with ClamAV

```
 # clamscan -r /tmp/
./dos-58.160.208.43: OK
./dos-108.18.38.140: OK
./dos-188.194.80.100: OK
./dos-91.224.160.135: OK
./dos-128.253.117.70: OK
./dos-128.172.143.110: OK
./dos-77.92.102.34: OK
./dos-195.230.5.12: OK
...
....
----------- SCAN SUMMARY -----------
Known viruses: 2735887
Engine version: 0.97.8
Scanned directories: 1
Scanned files: 129
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 4.769 sec (0 m 4 s)
```

-r flag stands for recursive scan - e.g. scan all sub-directories in directory and its content

To not flood your console / ssh connection one very useful option is **-i** (print only whetherinfected files are matched). Here is one more sample case:

```
 # clamscan -r -i /var/tmp/
 ----------- SCAN SUMMARY -----------
Known viruses: 2735887
Engine version: 0.97.8
Scanned directories: 1
Scanned files: 2
Infected files: 0
Data scanned: 0.26 MB
Data read: 0.13 MB (ratio 1.97:1)
Time: 4.824 sec (0 m 4 s)
```

Whether you're on a physical server console and it has pc speaker or sound blaster use **--bell** option to ring a bell every time a Virus infection is found, for exmpl.

```
# clamscan -r -i --bell /var/www/ ...
```

4. Scanning periodically and reporting with ClamAV directories with websites

A very common use of ClamAV is to just setup a scheduled cronjob once a month to scan, whether server folder containing a bunch of websites in separate Virtualhosts contain some viruses or malicious stuff.

Then as administrator check those logs once a month to make sure server site or group of sites does not become banned in search engine (blocked by Google Chrome and Firefox as Virus hotbed) ...

```
# crontab -u root -e
00 02 01 * * clamscan -r /var/www -l /var/log/websites-scan.log
```

Then once a month check out /var/log/websites-scan.log