How to build Clam AntiVirus RPM package for Fedora Core

by Thomas Chung on Feb 26, 2005 .

Clam AntiVirus is an anti−virus toolkit for UNIX/Linux, designed for e−mail scanning on mail gateways. It provides a flexible and scalable multi−threaded daemon, a command line scanner, and an advanced tool for automatic database updating via Internet. The package also includes a virus scanner shared library.

It features:
− Licensed under the GNU General Public License
− POSIX compliant, portable
− Fast scanning
− Supports on−access scanning (Linux and FreeBSD only)
− Detects over 30000 viruses, worms, and trojans, including Microsoft Office and MacOffice macro viruses

See online documentation for a complete list of features:

In this article, I'll be using ClamAV version 0.83 source code on Fedora Core 1 to build binary RPM package as an example.

To build the RPM package, you'll need:
Tarball − clamav−0.83.tar.gz
Spec File − clamav.spec
Init scripts − clamd.init, freshclam.init
Config files − clamd.conf, freshclam.conf

Let's begin:
(Make sure you have created rpmbuild directory in your own home.)

```
[tchung@tchung-home 0.83]$ ls *.gz *.spec *.init *.conf
clamav-0.83.tar.gz  clamav.spec  clamd.conf  clamd.init  freshclam.conf  freshclam.init
[tchung@tchung-home 0.83]$ cp *.gz *.init *.conf ~/rpmbuild/SOURCES/
[tchung@tchung-home 0.83]$ cp *.spec ~/rpmbuild/SPECS/
[tchung@tchung-home 0.83]$ rpmbuild -ba ~/rpmbuild/SPECS/clamav.spec
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.40639
+ umask 022
+ cd /home/tchung/rpmbuild/BUILD
+ LANG=C
+ export LANG
+ unset DISPLAY
+ rm -rf /var/tmp/clamav-0.83-buildroot
+ cd /home/tchung/rpmbuild/BUILD
+ rm -rf clamav-0.83
```

```
+ /usr/bin/gzip -dc /home/tchung/rpmbuild/SOURCES/clamav-0.83.tar.gz

..omitted..

Wrote: /home/tchung/rpmbuild/SRPMS/clamav-0.83-0.FC1.src.rpm
Wrote: /home/tchung/rpmbuild/RPMS/i386/clamav-0.83-0.FC1.i386.rpm
Wrote: /home/tchung/rpmbuild/RPMS/i386/clamav-debuginfo-0.83-0.FC1.i386.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.68409
+ umask 022
+ cd /home/tchung/rpmbuild/BUILD
+ cd clamav-0.83
+ rm -rf /var/tmp/clamav-0.83-buildroot
+ exit 0
[tchung@tchung-home 0.83]$
```

To install ClamAV rpm package:

```
[tchung@tchung-home 0.83]$ cp /home/tchung/rpmbuild/RPMS/i386/*.rpm .
[tchung@tchung-home 0.83]$ ls *.rpm
clamav-0.83-0.FC1.i386.rpm  clamav-debuginfo-0.83-0.FC1.i386.rpm
[tchung@tchung-home 0.83]$ sudo rpm -Uvh clamav-0.83-0.FC1.i386.rpm
Preparing...                ########################################### [100%]
   1:clamav                 ########################################### [100%]
```

To check and start **clamd** service which is an anti−virus daemon:

```
[tchung@tchung-home 0.83]$ sudo /sbin/chkconfig clamd --list
clamd           0:off   1:off   2:off   3:off   4:off   5:off   6:off
[tchung@tchung-home 0.83]$ sudo /sbin/chkconfig clamd on
[tchung@tchung-home 0.83]$ sudo /sbin/chkconfig clamd --list
clamd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
[tchung@tchung-home 0.83]$ sudo /sbin/service clamd status
clamd is stopped
[tchung@tchung-home 0.83]$ sudo /sbin/service clamd start
Starting Clam AV daemon:                                   [  OK  ]
[tchung@tchung-home 0.83]$ sudo /sbin/service clamd status
clamd (pid 23706) is running...
[tchung@tchung-home 0.83]$
```

To check and start **freshclam** service which updates virus database:

```
[tchung@tchung-home 0.83]$ sudo /sbin/chkconfig freshclam --list
freshclam       0:off   1:off   2:off   3:off   4:off   5:off   6:off
[tchung@tchung-home 0.83]$ sudo /sbin/chkconfig freshclam on
[tchung@tchung-home 0.83]$ sudo /sbin/chkconfig freshclam --list
freshclam       0:off   1:off   2:on    3:on    4:on    5:on    6:off
[tchung@tchung-home 0.83]$ sudo /sbin/service freshclam status
freshclam is stopped
[tchung@tchung-home 0.83]$ sudo /sbin/service freshclam start
Starting freshclam:                                        [  OK  ]
[tchung@tchung-home 0.83]$ sudo /sbin/service freshclam status
freshclam (pid 23768) is running...
[tchung@tchung-home 0.83]$
```

Now, let's do some test scan using **clamscan** which scans files and directories against viruses:

```
[tchung@tchung-home 0.83]$ rpm -ql clamav | grep test
/usr/share/doc/clamav-0.83/test
/usr/share/doc/clamav-0.83/test/README
/usr/share/doc/clamav-0.83/test/clam-error.rar
```

```
/usr/share/doc/clamav-0.83/test/clam.cab
/usr/share/doc/clamav-0.83/test/clam.exe
/usr/share/doc/clamav-0.83/test/clam.exe.bz2
/usr/share/doc/clamav-0.83/test/clam.rar
/usr/share/doc/clamav-0.83/test/clam.zip
/usr/share/doc/clamav-0.83/test/mbox
/usr/share/doc/clamav-0.83/test/mbox/debugm.c
[tchung@tchung-home 0.83]$ clamscan -r /usr/share/doc/clamav-0.83/test
/usr/share/doc/clamav-0.83/test/clam-error.rar: RAR module failure
/usr/share/doc/clamav-0.83/test/clam-error.rar: OK
/usr/share/doc/clamav-0.83/test/README: OK
/usr/share/doc/clamav-0.83/test/clam.exe.bz2: ClamAV-Test-File FOUND
/usr/share/doc/clamav-0.83/test/clam.cab: ClamAV-Test-File FOUND
/usr/share/doc/clamav-0.83/test/clam.exe: ClamAV-Test-File FOUND
/usr/share/doc/clamav-0.83/test/mbox/debugm.c: OK
/usr/share/doc/clamav-0.83/test/clam.rar: ClamAV-Test-File FOUND
/usr/share/doc/clamav-0.83/test/clam.zip: ClamAV-Test-File FOUND

----------- SCAN SUMMARY -----------
Known viruses: 31238
Scanned directories: 2
Scanned files: 8
Infected files: 5
Data scanned: 0.00 MB
I/O buffer size: 131072 bytes
Time: 0.405 sec (0 m 0 s)
[tchung@tchung-home 0.83]$
```

I would recommend to subscribe to <u>clamav-virusdb</u> mailing list to receive new virus database releases announcements.

It has configured to update virus database every hour but to update now and to see current virus database version:

```
[tchung@tchung-home 0.83]$ sudo freshclam
ClamAV update process started at Sat Feb 26 22:53:56 2005
main.cvd is up to date (version: 29, sigs: 29086, f-level: 3, builder: tomek)
daily.cvd is up to date (version: 730, sigs: 2153, f-level: 4, builder: tkojm)
[tchung@tchung-home 0.83]$
```