Installing ClamAV on CentOS 7 and Using Freshclam

http://linux-audit.com/install-clamav-on-centos-7-using-freshclam/

Install and Configure ClamAV on CentOS 7

Including the usage of Freshclam

To get ClamAV on CentOS installed, we have to use the EPEL repository (Extra Packages for Enterprise Linux). Fortunately, the Fedora project provides this with an easy installation. Unfortunately the default configuration is not properly working. In this post we collect some of the issues and required changes.

Let's start with installing the EPEL support.

```
yum install epel-release
```

Next step is installing all ClamAV components.

```
yum install clamav-server clamav-data clamav-update clamav-filesystem clamav clamav-scanner-systemd clamav-devel clamav-lib clamav-server-systemd
```

The output should be similar to:

```
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
Importing GPG key 0x352C64E5:
 Userid     : "Fedora EPEL (7) <epel@fedoraproject.org>"
 Fingerprint: 91e9 7d7c 4a5e 96f1 7f3e 888f 6a2f aea2 352c 64e5
 Package    : epel-release-7-5.noarch (@extras)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
Is this ok [y/N]: y
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : clamav-filesystem-0.98.7-1.el7.noarch
  Installing : clamav-data-0.98.7-1.el7.noarch
  Installing : clamav-lib-0.98.7-1.el7.x86_64
  Installing : 2:nmap-ncat-6.40-4.el7.x86_64
  Installing : clamav-server-0.98.7-1.el7.x86_64
  Installing : clamav-server-systemd-0.98.7-1.el7.noarch
  Installing : clamav-scanner-0.98.7-1.el7.noarch
  Installing : clamav-scanner-systemd-0.98.7-1.el7.noarch
  Installing : clamav-devel-0.98.7-1.el7.x86_64
  Installing : clamav-update-0.98.7-1.el7.x86_64
  Installing : clamav-0.98.7-1.el7.x86_64
  Verifying  : clamav-scanner-systemd-0.98.7-1.el7.noarch
  Verifying  : 2:nmap-ncat-6.40-4.el7.x86_64
  Verifying  : clamav-filesystem-0.98.7-1.el7.noarch
  Verifying  : clamav-server-0.98.7-1.el7.x86_64
  Verifying  : clamav-scanner-0.98.7-1.el7.noarch
  Verifying  : clamav-data-0.98.7-1.el7.noarch
  Verifying  : clamav-devel-0.98.7-1.el7.x86_64
  Verifying  : clamav-server-systemd-0.98.7-1.el7.noarch
  Verifying  : clamav-lib-0.98.7-1.el7.x86_64
  Verifying  : clamav-update-0.98.7-1.el7.x86_64
  Verifying  : clamav-0.98.7-1.el7.x86_64

Installed:
  clamav.x86_64 0:0.98.7-1.el7        clamav-data.noarch 0:0.98.7-1.el7           clamav-dev
  clamav-server.x86_64 0:0.98.7-1.el7 clamav-server-systemd.noarch 0:0.98.7-1.el7 clamav-upd

Dependency Installed:
  clamav-scanner.noarch 0:0.98.7-1.el7

Complete!
```

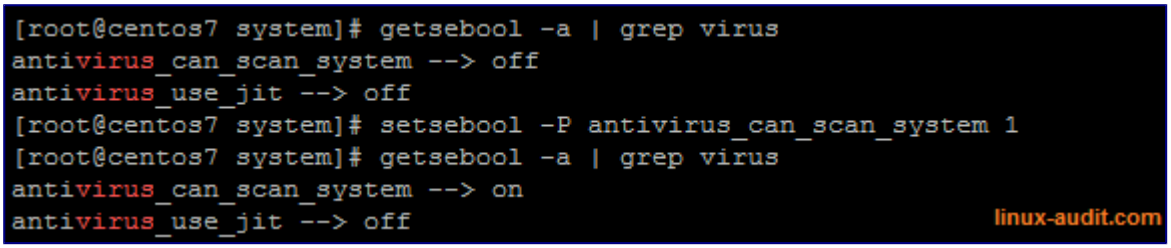
Installing ClamAV with help of EPEL repository

Configure SELinux for ClamAV

If you are using ClamAV on CentOS, together with SELinux, we should configure it a little bit. This way ClamAV can access all files on disk, and update its data definition files.

Enable **antivirus_can_scan_system**:

```
setsebool -P antivirus_can_scan_system 1
```



If you don't perform this step, Freshclam will log something like:

```
During database load : LibClamAV Warning: RWX mapping denied: Can't allocate RWX
Memory: Permission denied
```

Configuration of Clam daemon

Copy a the clamd.conf template, in case you don't have a configuration file yet.

```
cp /usr/share/clamav/template/clamd.conf /etc/clamd.d/clamd.conf
sed -i '/^Example/d' /etc/clamd.d/clamd.conf
```

Change **/etc/**clamd**.d/**clamd**.conf** file and define if you want to run the scanner as root, or a specific user. Check your /etc/passwd file for the related Clam user.

Change the following two options:

```
User clamscan
LocalSocket /var/run/clamd.<SERVICE>/clamd.sock
```

Enable Freshclam

Freshclam helps with keeping the database of ClamAV up-to-date. First delete the related "Example" line from **/etc/freshclam.conf**.

```
cp /etc/freshclam.conf /etc/freshclam.conf.bak
sed -i '/^Example/d' /etc/freshclam.conf
```

Check the other options in the file, and change it to your preferred settings.

Missing systemd service file

We didn't get a systemd service file, so creating a quick file here. The process should be forking itself and start freshclam in daemon mode. In this case we configure it to check 4 times a day for new files.

Create a new file **/usr/lib/systemd/system/clam-freshclam.service**

```
# Run the freshclam as daemon
[Unit]
Description = freshclam scanner
After = network.target
[Service]
Type = forking
```

```
ExecStart = /usr/bin/freshclam -d -c 4
Restart = on-failure
PrivateTmp = true
[Install]
WantedBy=multi-user.target
```

Now enable and start the service.

systemctl enable clam-freshclam.service

systemctl start clam-freshclam.service

Check the status.

```
[root@centos7 system]# systemctl status clam-freshclam.service
clam-freshclam.service - freshclam scanner
Loaded: loaded (/usr/lib/systemd/system/clam-freshclam.service; enabled)
Active: active (running) since Thu 2015-06-11 11:09:24 CEST; 1s ago
Process: 3158 ExecStart=/usr/bin/freshclam -d -c 4 (code=exited, status=0/SUCCESS)
Main PID: 3159 (freshclam)
CGroup: /system.slice/clam-freshclam.service
└─3159 /usr/bin/freshclam -d -c 4
```

Change service files

By default, the service files seem to be messy and not working.

These are the files bundled:

```
[root@centos7 system]# ls -l /usr/lib/systemd/system/clam*
-rw-r--r--. 1 root root 136 Apr 29 20:38
/usr/lib/systemd/system/clamd@scan.service
-rw-r--r--. 1 root root 231 Apr 29 20:38 /usr/lib/systemd/system/clamd@.service
```

When enabling the clamd service, we would see something like this:

```
[root@centos7 system]# systemctl enable /usr/lib/systemd/system/clamd@.service
 Failed to issue method call: Unit /usr/lib/systemd/system/clamd@.service does not
exist.
```

So let's fix it. First rename the **/usr/lib/systemd/system/clamd@.service** file.

Rename the clamd@ file.

mv /usr/lib/systemd/system/clamd@.service /usr/lib/systemd/system/clamd.service

Now we have to change the clamd@scan service as well, as it refers to a non-existing file now. Change this line in **/usr/lib/systemd/system/clamd@scan.service** and remove the @ sign.

.include /lib/systemd/system/clamd**@**.service

Next step is changing the clamd service file **/usr/lib/systemd/system/clamd.service**

```
[Unit]
Description = clamd scanner daemon
After = syslog.target nss-lookup.target network.target
[Service]
Type = simple
ExecStart = /usr/sbin/clamd -c /etc/clamd.d/clamd.conf --nofork=yes
Restart = on-failure
PrivateTmp = true

[Install]
WantedBy=multi-user.target
```

Move into the directory.

cd /usr/lib/systemd/system

Start all services.

[root@centos7 system]# systemctl enable clamd.service
[root@centos7 system]# systemctl enable clamd@scan.service
[root@centos7 system]# systemctl start clamd.service
[root@centos7 system]# systemctl start clamd@scan.service

Checking the status

With all these changes, ClamAV on CentOS 7 should be running now. The easiest way to check, is using the *ps* command and see if *freshclam* and *clamd* are running.

Useful resources for debugging are the systemctl status command, followed by the service. Then there is logging in /var/log/messages, which usually will reveal when and why something is (not) running.