A day ago, my mail server stopped receiving and sending mails. I was getting the famous "qq Temporary problem". My suspected clamav for this. Reason being, clamav had been sending me warning mails that the version is outdated and I should upgrade. Due to my business, and partly my laziness, I could not update it. Any way, to get it working, I had to upgrade to the latest version of ClamAV, which is 0.94-1, by the time of this writing.

Here is how I did it.

Updating clamav from 0.93 to 0.94-1

Check the status of ClamAV:-

```
[root@www ~]# service clamd status
ERROR: Clamav DB missing! Run 'freshclam --verbose' as root.
[root@www ~]#
```

This is because the naming convention is also changed for the Virus Signature files.

Downlaod clamav Src RPM from http://packages.sw.be/clamav/ .

wget http://packages.sw.be/clamav/clamav-0.94.1-1.rf.src.rpm

Rebuild it. (make sure you have sendmail-devel installed before you rebuilt it). DO NOT install sendmail. Just install sendmail-devel.

rpmbuild --rebuild clamav-0.94.1-1.rf.src.rpm

Stop clamd and fresh clam

service clamd stop
service freshclam stop

Save a copy of old configs:-

cd /etc/
mv clamd.conf clamd.conf.93
mv freshclam.conf freshclam.conf.93

You will need to remove the older clamav packages. Other wise this newer version will not install, even if you try to Update it.

cd /usr/src/redhat/RPMS/i386/

[root@www i386]# rpm -Uvh clamav-0.94-1.rf.i386.rpm clamav-db-0.94-1.rf.i386.rpm clamd-0.94-1.rf.i386.rpm clamav-devel-0.94-1.rf.i386.rpm
error: Failed dependencies:
 libclamav.so.4 is needed by (installed) clamav-server-0.93-2.i386
 libclamav.so.4(CLAMAV_PRIVATE) is needed by (installed) clamav-server-0.93-2.i386
 libclamav.so.4(CLAMAV_PUBLIC) is needed by (installed) clamav-server-0.93-2.i386
 clamav = 120:0.93-2 is needed by (installed) clamav-server-0.93-2.i386

[root@www i386]# rpm -qa | grep -i clam
clamav-db-0.93-2
clamav-devel-0.93-2
clamav-server-0.93-2
clamav-0.93-2

Remove old packages first:-

[root@www i386]# rpm -e clamav-db clamav-devel clamav-server clamav
warning: /etc/logrotate.d/freshclam saved as /etc/logrotate.d/freshclam.rpmsave
warning: /etc/logrotate.d/clamd saved as /etc/logrotate.d/clamd.rpmsave

Now install new packages:-

[root@www i386]# rpm -Uvh clamav-0.94-1.rf.i386.rpm clamav-db-0.94-1.rf.i386.rpm clamd-0.94-1.rf.i386.rpm clamav-devel-0.94-1.rf.i386.rpm

```
Preparing...                ########################################### [100%]
 1:clamav-db                ########################################### [ 25%]
 2:clamav                   ########################################### [ 50%]
 3:clamd                    ########################################### [ 75%]
 4:clamav-devel             ########################################### [100%]
[root@www i386]#
```

Edit the config files to reflect the changes. The major change in 0.94 is that it stores it's database in /var/clamav , instead of /var/lib/clamav . This was the stupid reason that my clamav 0.93 was not able to find the virus databases. Any way.
Also the Temporary directory should be /tmp, instead of /var/tmp. Make sure to have user as qscand instead of clamav, both in clamav and freshclam installation.

```
chown qscand:qscand /var/log/clamav -R
chown qscand:qscand /var/clamav -R
chown qscand:qscand /var/run/clamav -R
```

```
vi /etc/logrotate.d/clamd
#
# Rotate Clam AV daemon log file
#

/var/log/clamav/clamd.log {
missingok
nocompress
create 640 qscand qscand
postrotate
/bin/kill -HUP `cat /var/run/clamav/clamd.pid 2> /dev/null` 2> /dev/null || true
endscript
}
```

```
vi /etc/logrotate.d/freshclam

/var/log/clamav/freshclam.log {
```

```
 missingok
 notifempty
 create 644 qscand qscand
}
```

```
[root@www x86_64]# service clamd restart
Stopping Clam AntiVirus Daemon:                            [  OK  ]
Starting Clam AntiVirus Daemon: LibClamAV Warning:
************************************************
LibClamAV Warning: ***  The virus database is older than 7 days!  ***
LibClamAV Warning: ***   Please update it as soon as possible.    ***
LibClamAV Warning: ************************************************
 [  OK  ]
```

Run freshclam to update the Virus database:-

```
[root@www x86_64]# freshclam
ClamAV update process started at Fri Nov 14 12:35:07 2008
main.cvd is up to date (version: 49, sigs: 437972, f-level: 35, builder: sven)
WARNING: getfile: daily-8543.cdiff not found on remote server (IP: 64.142.100.50)
WARNING: getpatch: Can't download daily-8543.cdiff from db.local.clamav.net
WARNING: getfile: daily-8543.cdiff not found on remote server (IP: 64.142.100.50)
WARNING: getpatch: Can't download daily-8543.cdiff from db.local.clamav.net
WARNING: getfile: daily-8543.cdiff not found on remote server (IP: 64.142.100.50)
WARNING: getpatch: Can't download daily-8543.cdiff from db.local.clamav.net
WARNING: Incremental update failed, trying to download daily.cvd
Downloading daily.cvd [100%]
daily.cvd updated (version: 8631, sigs: 26049, f-level: 35, builder: ccordes)
Database updated (464021 signatures) from db.local.clamav.net (IP: 64.142.100.50)
Clamd successfully notified about the update.
```

Restart clamd :-

```
[root@www x86_64]# service clamd restart
Stopping Clam AntiVirus Daemon:                    [  OK  ]
Starting Clam AntiVirus Daemon:                    [  OK  ]
[root@www x86_64]#
```

For some reason freshclam service is removed from 0.94. This means, back to old method.
Crontab:-

```
# crontab -e
0 1 * * * /usr/local/bin/setuidgid qscand /var/qmail/bin/qmail-scanner-queue.pl -z
0 1 * * * /usr/local/bin/setuidgid qscand /var/qmail/bin/qmail-scanner-queue.pl -g
25 2 * * * /usr/bin/freshclam --quiet -l /var/log/clamav/freshclam.log
```

Alhumdulillah.

Now you may want to restart qmail, by:-

qmailctl stop

qmailctl start

qmailctl stat

Make sure you issue the following two commands as well. They are (should be) part of your crontab, by the way.

/usr/local/bin/setuidgid qscand /var/qmail/bin/qmail-scanner-queue.pl -z
/usr/local/bin/setuidgid qscand /var/qmail/bin/qmail-scanner-queue.pl -g

Your mail server now has latest version of clamav. Congratulations.

Alhumdulillah.