Chapter 7

Anti-SPAM and AntiVIRUS in MTA

badmailfrom

```
[root@cent ~]# locate badmailfrom

[root@cent ~]# cd /var/qmail/control/

[root@cent control]# ll

total 48

-rw-r--r--. 1 root root 3 Dec 7 03:06 concurrencyincoming

-rw-r--r--  1 root root   11 Dec 14 01:34 defaultdelivery

-rw-r--r--. 1 root root   14 Dec  7 02:30 defaultdomain

-rw-r--r--  1 root root   26 Jan  4 20:31 dksign

-rw-r--r--. 1 root root   19 Dec  7 02:30 locals

-rw-r--r--. 1 root root   19 Dec  7 02:30 me

-rw-r--r--. 1 root root   14 Dec  7 02:30 plusdomain
```

```
lrwxrwxrwx   1 root  root    10 Dec   8 14:45 qmail ->
/etc/qmail

-rw-r--r--. 1 root root   19 Dec  7 02:30 rcpthosts

-rw-------  1 root root 3119 Jan 23 18:44 servercert.pem

-rwxrwxrwx  1 root root 3119 Jan 24 15:07 stunnel.pem

-rw-r--r--      1    root    root      146    Jan    23    18:50
stunnel_smtpd.conf

-rw-r--r--  1 root root  140 Jan 24 15:32 stunnel-smtpsd

[root@cent control]# vim badmailfrom

[root@cent control]# cat badmailfrom

ahamd@spam.net

@x.com

[root@cent control]# vim badmailfrom

[root@cent control]# qmailctl restart

Restarting qmail:

* Stopping qmail-smtpsd.

* Stopping qmail-smtpd.

* Sending qmail-send SIGTERM and restarting.

* Restarting qmail-smtpd.

* Restarting qmail-smtpsd.

[root@cent control]# telnet localhost 25
```

```
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.raja.internal ESMTP
HELO evildomain.net
250 mail.raja.internal
MAIL FROM: <badguy@evildomain.net>
250 ok
RCPT TO: <rich@ispnet1.net>
553 sorry, your envelope sender is in my badmailfrom list (#5.7.1)
quit
221 mail.raja.internal
Connection closed by foreign host.
[root@cent control]#
[root@cent control]#
[root@cent control]#
```

RBLSMTPD

```
[root@cent control]# vim /etc/tcp.smtp

[root@cent control]# vim /etc/tcp.smtp

[root@cent qmail-smtpd]# cat  /etc/tcp.smtp

127.0.0.1:allow,RELAYCLIENT="",RBLSMTPD="blackholes.mail-abuse.org"

:allow,DKVERIFY="DEGIJKfh,CGHIJMQRkl",AUTH_UNSET_DKVERIFY=""

[root@cent qmail-smtpd]#
```

```
[root@cent control]# cd ..

[root@cent qmail]# ls

alias bin boot control doc man queue rc supervise users

[root@cent qmail]# cd supervise/

[root@cent supervise]# ls

qmail-send  qmail-smtpd  qmail-smtpsd

[root@cent supervise]# cd qmail-smtpd/

[root@cent qmail-smtpd]# ls

log  run  supervise

[root@cent qmail-smtpd]# vim run
```

```
[root@cent qmail-smtpd]# vim run
/bin/sh

QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
LOCAL=`head -1 /var/qmail/control/me`

if [ -z "$QMAILDUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" -o -z "$LOCAL" ]; then
   echo QMAILDUID, NOFILESGID, MAXSMTPD, or LOCAL is unset in
   echo /var/qmail/supervise/qmail-smtpd/run
   exit 1
fi

if [ ! -f /var/qmail/control/rcpthosts ]; then
   echo "No /var/qmail/control/rcpthosts!"
   echo "Refusing to start SMTP listener because it'll create an open relay"
   exit 1
```

```
fi


exec /usr/local/bin/softlimit -m 4000000 \
   /usr/local/bin/tcpserver -v -R -l "$LOCAL" -x
/etc/tcp.smtp.cdb -c "$MAXSMTPD" \
      -u "$QMAILDUID" -g "$NOFILESGID" 0 smtp -r
"blackholes.mail-abuse.org: Your
? site has been listed in the MAPS RSS database"
/var/qmail/bin/qmail-smtpd \
   /bin/checkpassword /bin/true 2>&1
```

AntiVIRUS in MailServer(clamav)

Installation

```
1006  rpm -qa | grep zlib
 1007  cd ../Downloads/
 1008  ls
 1009  tar -zxvf clamav-0.99.2.tar.gz
 1010  cd clamav-0.99.2
 1011  ls
 1012  vim INSTALL
 1013  ./configure
 1014  make

 1015  make install

[root@cent clamav-0.99.2]# ldconfig

[root@cent clamav-0.99.2]# qmailctl restart

Restarting qmail:

* Stopping qmail-smtpsd.

* Stopping qmail-smtpd.

* Sending qmail-send SIGTERM and restarting.

* Restarting qmail-smtpd.

* Restarting qmail-smtpsd.


[root@cent clamav-0.99.2]# freshclam

ERROR: Can't open/parse the config file /usr/local/etc/freshclam.conf

[root@cent clamav-0.99.2]# cd /usr/local/etc/

[root@cent etc]# ls

authlib  clamd.conf.sample  freshclam.conf.sample  stunnel

[root@cent etc]# cp freshclam.conf.sample freshclam.conf

[root@cent etc]# cp clamd.conf.sample clamd.conf

[root@cent etc]# vim freshclam.conf

[root@cent etc]# vim freshclam.conf
```

```
[root@cent etc]# freshclam

WARNING: Can't get information about user clamav.

[root@cent etc]# echo $?

60

[root@cent etc]# cat /etc/passwd | grep clam

[root@cent /]# freshclam
```

WARNING: Can't get information about user clamav.

Solve the Errors

```
[root@cent clamav-0.99.2]# groupadd clamav

[root@cent clamav-0.99.2]# useradd -g clamav -s /sbin/nologin -c "Clam AntiVirus" clamav

[root@cent clamav-0.99.2]# cat /etc/passwd | grep clam

clamav:x:508:503:Clam AntiVirus:/home/clamav:/sbin/nologin

[root@cent clamav-0.99.2]# cd ~

[root@cent ~]# freshclam

ERROR: Can't change dir to /usr/local/share/clamav

[root@cent ~]# mkdir -p /usr/local/share/clamav

[root@cent ~]# chown clamav:clamav /usr/local/share/clamav

[root@cent ~]# /usr/local/bin/freshclam -v

Current working dir is /usr/local/share/clamav
```

```
Max retries == 3

ClamAV update process started at Mon Jan 30 17:54:10 2017

Using IPv6 aware code

Querying current.cvd.clamav.net

TTL: 1729

Software version from DNS: 0.99.2

Retrieving http://database.clamav.net/main.cvd

Trying to download http://database.clamav.net/main.cvd (IP: 130.59.113.36)

nonblock_recv: recv timing out (30 secs)

WARNING: getfile: Download interrupted: Operation now in progress (IP: 130.59.113.36)

WARNING: Can't download main.cvd from database.clamav.net

Querying main.0.82.0.0.823B7124.ping.clamav.net

Trying again in 5 secs...

ClamAV update process started at Mon Jan 30 17:56:14 2017

Using IPv6 aware code

Querying current.cvd.clamav.net

TTL: 1605

Software version from DNS: 0.99.2
```

```
Retrieving http://database.clamav.net/main.cvd
Ignoring mirror 130.59.113.36 (due to previous errors)
Trying host database.clamav.net (193.230.240.8)...
Trying to download http://database.clamav.net/main.cvd (IP: 193.230.240.8)
nonblock_recv: recv timing out (30 secs)
WARNING: getfile: Download interrupted: Operation now in progress (IP: 193.230.240.8)
WARNING: Can't download main.cvd from database.clamav.net
Querying main.0.82.0.0.C1E6F008.ping.clamav.net
Trying again in 5 secs...
ClamAV update process started at Mon Jan 30 17:57:50 2017
Using IPv6 aware code
Querying current.cvd.clamav.net
TTL: 1509
Software version from DNS: 0.99.2
Retrieving http://database.clamav.net/main.cvd
Ignoring mirror 193.230.240.8 (due to previous errors)
Ignoring mirror 130.59.113.36 (due to previous errors)
ERROR: Can't download main.cvd from database.clamav.net
```

```
Giving up on database.clamav.net...

Update failed. Your network may be down or none of the mirrors listed in /usr/local/etc/freshclam.conf is working. Check http://www.clamav.net/doc/mirrors-faq.html for possible reasons.

[root@cent ~]# proxychains4 /usr/local/bin/freshclam -v

[proxychains] config file found: /etc/proxychains.conf

[proxychains] preloading /usr/local/lib/libproxychains4.so

[proxychains] DLL init

Current working dir is /usr/local/share/clamav

Max retries == 3

ClamAV update process started at Mon Jan 30 18:00:01 2017

Using IPv6 aware code

Querying current.cvd.clamav.net

TTL: 1379

Software version from DNS: 0.99.2

Retrieving http://database.clamav.net/main.cvd

[proxychains] Strict chain  ...  46.38.139.28:20009  ...  127.0.0.1:9050  ...  database.clamav.net:80  ...  OK

Trying to download http://database.clamav.net/main.cvd (IP: 224.0.0.1)

nonblock_recv: recv timing out (30 secs)
```

```
WARNING: getfile: Download interrupted: Operation now in
progress (IP: 224.0.0.1)
WARNING: Can't download main.cvd from
database.clamav.net
Querying main.0.82.0.0.E0000001.ping.clamav.net
Trying again in 5 secs...
ClamAV update process started at Mon Jan 30 18:02:11 2017
Using IPv6 aware code
Querying current.cvd.clamav.net
TTL: 1248
Software version from DNS: 0.99.2
Retrieving http://database.clamav.net/main.cvd
Ignoring mirror 224.0.0.1 (due to previous errors)
WARNING: Can't download main.cvd from
database.clamav.net
Trying again in 5 secs...
ClamAV update process started at Mon Jan 30 18:02:16 2017
Using IPv6 aware code
Querying current.cvd.clamav.net
TTL: 1243
Software version from DNS: 0.99.2
```

```
Retrieving http://database.clamav.net/main.cvd
Ignoring mirror 224.0.0.1 (due to previous errors)
ERROR: Can't download main.cvd from database.clamav.net
Giving up on database.clamav.net...
Update failed. Your network may be down or none of the mirrors listed in /usr/local/etc/freshclam.conf is working. Check http://www.clamav.net/doc/mirrors-faq.html for possible reasons.
[root@cent ~]#
```

Important Note

If you can't update via freshclam command. get it manually or install clamav with yum

Note: If your network is segmented or the end hosts are unable to reach the Internet, you should investigate setting up a private local mirror. If this is not viable, you may use these direct download links: main.cvd | daily.cvd | bytecode.cvd

```
[root@cent database]# yum install clamav
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.steadfast.net
 * extras: mirror.steadfast.net
 * updates: mirror.steadfast.net
base                                    | 3.7 kB     00:00
epel                                    | 4.3 kB     00:00
extras                                  | 3.3 kB     00:00
updates                                  | 3.4 kB     00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package clamav.i686 0:0.99.2-1.el6 will be installed
--> Processing Dependency: clamav-db = 0.99.2-1.el6 for
package: clamav-0.99.2-1.el6.i686
--> Running transaction check
---> Package clamav-db.i686 0:0.99.2-1.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=============================================
===================================
 Package           Arch          Version            Repository
Size
==============================================
====================================
Installing:
 clamav           i686         0.99.2-1.el6         epel         4.4 M
Installing for dependencies:
 clamav-db          i686          0.99.2-1.el6          epel          110
M

Transaction Summary
==============================================
====================================
Install       2 Package(s)

Total download size: 115 M
Installed size: 123 M
Is this ok [y/N]: y
Downloading Packages:
http://download.fedoraproject.org/pub/epel/6/i386/clamav-db-
0.99.2-1.el6.i686.rpm: [Errno 14] PYCURL ERROR 56 -
"Failure when receiving data from the peer"
```

```
Trying other mirror.



Error Downloading Packages:

  clamav-db-0.99.2-1.el6.i686: failure: clamav-db-0.99.2-1.el6.i686.rpm from epel: [Errno 256] No more mirrors to try

[root@cent database]# proxychains4 yum install clamav

[proxychains] config file found: /etc/proxychains.conf

[proxychains] preloading /usr/local/lib/libproxychains4.so

[proxychains] DLL init

Loaded plugins: fastestmirror, refresh-packagekit, security

Loading mirror speeds from cached hostfile

[proxychains] Strict chain ... 46.38.139.28:20009
[proxychains] Strict chain ... 46.38.139.28:20009
[proxychains] Strict chain ... 46.38.139.28:20009 ... 127.0.0.1:9050 ... 127.0.0.1:9050 ... 127.0.0.1:9050 ... ftp.hosteurope.de:80 ... ftp.hosteurope.de:80 ... ftp.hosteurope.de:80  ...  OK

 ...  OK

 ...  OK

 * base: mirror.steadfast.net

 * extras: mirror.steadfast.net
 * updates: mirror.steadfast.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package clamav.i686 0:0.99.2-1.el6 will be installed
--> Processing Dependency: clamav-db = 0.99.2-1.el6 for
package: clamav-0.99.2-1.el6.i686
--> Running transaction check
---> Package clamav-db.i686 0:0.99.2-1.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================
=====================================
 Package           Arch         Version            Repository
Size
================================================
=====================================
Installing:
 clamav          i686        0.99.2-1.el6        epel        4.4 M
Installing for dependencies:
 clamav-db          i686          0.99.2-1.el6          epel          110
M


Transaction Summary

================================================
=====================================

Install       2 Package(s)


Total size: 115 M

Total download size: 110 M

Installed size: 123 M

Is this ok [y/N]: y

Downloading Packages:

[proxychains]   Strict   chain      ...      46.38.139.28:20009      ...
127.0.0.1:9050  ...  download.fedoraproject.org:80  ...  OK

[proxychains]   Strict   chain      ...      46.38.139.28:20009      ...
127.0.0.1:9050  ...  www.mirrorservice.org:443  ...  OK

clamav-db-0.99.2-1.el6.i6 18% [==-            ] 4.7 kB/s |  21 MB
327:00 ETA

clamav-db-0.99.2-1.el6.i6 32% [====-            ]  12 kB/s |  35
MB    111:05 ETA

.
```

```
.

.

clamav-db-0.99.2-1.el6.i686.rpm                    | 110 MB
01:09

Running rpm_check_debug

Running Transaction Test

Transaction Test Succeeded

Running Transaction

  Installing          :          clamav-db-0.99.2-1.el6.i686
1/2

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

  Installing : clamav-0.99.2-1.el6.i686                    2/2

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init
```

```
[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

[proxychains] DLL init

  Verifying                  :             clamav-0.99.2-1.el6.i686
1/2

  Verifying                  :             clamav-db-0.99.2-1.el6.i686
2/2


Installed:

  clamav.i686 0:0.99.2-1.el6


Dependency Installed:

  clamav-db.i686 0:0.99.2-1.el6


Complete!

[root@cent database]#



 1013  yum install crontabs

 1014  service crond status
 1015  vim /etc/crontab
 root@cent ~]# cat  /etc/crontab
33 * * * * root /usr/local/bin/freshclam --quiet
1014  service crond start
[root@cent ~]#


 [root@cent database]# clam
clamav-config  clamconf      clamdscan     clamsubmit
clambc         clamd         clamscan
[root@cent database]# clamconf
Checking configuration files in /usr/local/etc


Config file: clamd.conf
----------------------
LogFile disabled
StatsHostID disabled
StatsEnabled disabled
StatsPEDisabled disabled
StatsTimeout disabled
LogFileUnlock disabled
LogFileMaxSize = "1048576"
```

```
LogTime disabled

LogClean disabled

LogSyslog disabled

LogFacility = "LOG_LOCAL6"

LogVerbose disabled

LogRotate disabled

ExtendedDetectionInfo disabled

PidFile disabled

TemporaryDirectory disabled

DatabaseDirectory = "/usr/local/share/clamav"

OfficialDatabaseOnly disabled

LocalSocket disabled

LocalSocketGroup disabled

LocalSocketMode disabled

FixStaleSocket = "yes"

TCPSocket disabled

TCPAddr disabled

MaxConnectionQueueLength = "200"

StreamMaxLength = "26214400"

StreamMinPort = "1024"

StreamMaxPort = "2048"
```

```
MaxThreads = "10"

ReadTimeout = "120"

CommandReadTimeout = "5"

SendBufTimeout = "500"

MaxQueue = "100"

IdleTimeout = "30"

ExcludePath disabled

MaxDirectoryRecursion = "15"

FollowDirectorySymlinks disabled

FollowFileSymlinks disabled

CrossFilesystems = "yes"

SelfCheck = "600"

DisableCache disabled

VirusEvent disabled

ExitOnOOM disabled

AllowAllMatchScan = "yes"

Foreground disabled

Debug disabled

LeaveTemporaryFiles disabled

User disabled

AllowSupplementaryGroups disabled
```

```
Bytecode = "yes"
BytecodeSecurity = "TrustSigned"
BytecodeTimeout = "5000"
BytecodeUnsigned disabled
BytecodeMode = "Auto"
DetectPUA disabled
ExcludePUA disabled
IncludePUA disabled
AlgorithmicDetection = "yes"
ScanPE = "yes"
ScanELF = "yes"
DetectBrokenExecutables disabled
ScanMail = "yes"
ScanPartialMessages disabled
PhishingSignatures = "yes"
PhishingScanURLs = "yes"
PhishingAlwaysBlockCloak disabled
PhishingAlwaysBlockSSLMismatch disabled
PartitionIntersection disabled
HeuristicScanPrecedence disabled
StructuredDataDetection disabled
```

```
StructuredMinCreditCardCount = "3"
StructuredMinSSNCount = "3"
StructuredSSNFormatNormal = "yes"
StructuredSSNFormatStripped disabled
ScanHTML = "yes"
ScanOLE2 = "yes"
OLE2BlockMacros disabled
ScanPDF = "yes"
ScanSWF = "yes"
ScanXMLDOCS = "yes"
ScanHWP3 = "yes"
ScanArchive = "yes"
ArchiveBlockEncrypted disabled
ForceToDisk disabled
MaxScanSize = "104857600"
MaxFileSize = "26214400"
MaxRecursion = "16"
MaxFiles = "10000"
MaxEmbeddedPE = "10485760"
MaxHTMLNormalize = "10485760"
MaxHTMLNoTags = "2097152"
```

```
MaxScriptNormalize = "5242880"

MaxZipTypeRcg = "1048576"

MaxPartitions = "50"

MaxIconsPE = "100"

MaxRecHWP3 = "16"

PCREMatchLimit = "10000"

PCRERecMatchLimit = "5000"

PCREMaxFileSize = "26214400"

ScanOnAccess disabled

OnAccessMountPath disabled

OnAccessIncludePath disabled

OnAccessExcludePath disabled

OnAccessExcludeUID disabled

OnAccessMaxFileSize = "5242880"

OnAccessDisableDDD disabled

OnAccessPrevention disabled

OnAccessExtraScanning disabled

DevACOnly disabled

DevACDepth disabled

DevPerformance disabled

DevLiblog disabled
```

```
DisableCertCheck disabled


Config file: freshclam.conf
---------------------------
StatsHostID disabled
StatsEnabled disabled
StatsTimeout disabled
LogFileMaxSize = "1048576"
LogTime disabled
LogSyslog disabled
LogFacility = "LOG_LOCAL6"
LogVerbose disabled
LogRotate disabled
PidFile disabled
DatabaseDirectory = "/usr/local/share/clamav"
Foreground disabled
Debug disabled
AllowSupplementaryGroups disabled
UpdateLogFile disabled
DatabaseOwner = "clamav"
Checks = "12"
```

```
DNSDatabaseInfo = "current.cvd.clamav.net"

DatabaseMirror = "database.clamav.net"

PrivateMirror disabled

MaxAttempts = "3"

ScriptedUpdates = "yes"

TestDatabases = "yes"

CompressLocalDatabase disabled

ExtraDatabase disabled

DatabaseCustomURL disabled

HTTPProxyServer disabled

HTTPProxyPort disabled

HTTPProxyUsername disabled

HTTPProxyPassword disabled

HTTPUserAgent disabled

NotifyClamd = "/usr/local/etc/clamd.conf"

OnUpdateExecute disabled

OnErrorExecute disabled

OnOutdatedExecute disabled

LocalIPAddress disabled

ConnectTimeout = "30"

ReceiveTimeout = "30"
```

```
SubmitDetectionStats disabled
DetectionStatsCountry disabled
DetectionStatsHostID disabled
SafeBrowsing disabled
Bytecode = "yes"

clamav-milter.conf not found

Software settings
-----------------
Version: 0.99.2
Optional features supported: MEMPOOL IPv6 AUTOIT_EA06 LIBXML2 ICONV RAR JIT

Database information
--------------------
Database directory: /usr/local/share/clamav
Total number of signatures: 0

Platform information
--------------------
```

```
uname: Linux 2.6.32-279.el6.i686 #1 SMP Fri Jun 22 10:59:55 UTC 2012 i686

OS: linux-gnu, ARCH: i386, CPU: i686

zlib version: 1.2.3 (1.2.3), compile flags: 55

Triple: i386-pc-linux-gnu

CPU: amdfam10, Little-endian

platform id: 0x0a1152520404040701040407


Build information

-----------------

GNU C: 4.4.7 20120313 (Red Hat 4.4.7-17) (4.4.7)

GNU C++: 4.4.7 20120313 (Red Hat 4.4.7-17) (4.4.7)

CPPFLAGS:

CFLAGS: -g -O2 -fno-strict-aliasing -D_LARGEFILE_SOURCE -D_LARGEFILE64_SOURCE

CXXFLAGS:

LDFLAGS:

Configure:

sizeof(void*) = 4

Engine flevel: 82, dconf: 82

[root@cent database]# clear
```

```
[root@cent database]# clam
clamav-config  clamconf     clamdscan     clamsubmit
clambc         clamd        clamscan
[root@cent database]# clamav-config
Usage: clamav-config [OPTION]

Known values for OPTION are:

  --prefix=DIR          change    libclamav    prefix    [default
/usr/local]
  --libs           print library linking information
  --cflags              print pre-processor and compiler flags
  --help           display this help and exit
  --version             output version information
[root@cent database]# clamav-config --version
0.99.2
[root@cent database]# clamav-config
Usage: clamav-config [OPTION]

Known values for OPTION are:
  --prefix=DIR          change libclamav prefix [default /usr/local]
  --libs        print library linking information
  --cflags              print pre-processor and compiler flags
  --help        display this help and exit
  --version             output version information
[root@cent database]# clamav-config --libs
-L/usr/local/lib -lz
[root@cent database]# clamav-config --cflags
-I/usr/local/include -g -O2 -fno-strict-aliasing -D_LARGEFILE_SOURCE -D_LARGEFILE64_SOURCE
[root@cent database]# clam
clamav-config  clamconf     clamdscan     clamsubmit
clambc        clamd         clamscan
[root@cent database]# clamd
clamd     clamdscan
[root@cent database]# clamdscan
ERROR: Could not lookup : Servname not supported for ai_socktype
```

```
----------- SCAN SUMMARY -----------
Infected files: 0
Total errors: 1
Time: 0.008 sec (0 m 0 s)
[root@cent database]#

[root@cent database]# service clamav-daemon start
clamav-daemon: unrecognized service
[root@cent database]# clamdscan
ERROR: Could not lookup : Servname not supported for ai_socktype

----------- SCAN SUMMARY -----------
Infected files: 0
Total errors: 1
Time: 0.008 sec (0 m 0 s)
[root@cent database]# rpm -qa | grep clam
clamav-db-0.99.2-1.el6.i686
clamav-0.99.2-1.el6.i686
[root@cent database]# yum seaarch clam
Loaded plugins: fastestmirror, refresh-packagekit, security
```

```
No such command: seaarch. Please use /usr/bin/yum --help
[root@cent database]# yum search clam
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.steadfast.net
 * extras: mirror.steadfast.net
 * updates: mirror.steadfast.net
============================== N/S Matched: clam
===============================
clamav-db.i686 : Virus database for clamav
clamav-devel.i686 : Header files, libraries and development
documentation for
              : clamav
clamav-milter.i686 : The Clam AntiVirus sendmail-milter
Daemon
clamav-unofficial-sigs.noarch : Scripts to download unoffical
clamav signatures
clamd.i686 : The Clam AntiVirus Daemon
claws-mail-plugins-clamd.i686 : Use Clam AntiVirus to scan
messages in Claws
                         : Mail
clamav.i686 : Anti-virus software
```

```
clamsmtp.i686 : A SMTP virus scanning system
clamz.i686 : Amazon Downloader

 Name and summary matches only, use "search all" for everything.
[root@cent database]#

[root@cent database]# yum install clamd
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: mirror.steadfast.net
 * extras: mirror.steadfast.net
 * updates: mirror.steadfast.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package clamd.i686 0:0.99.2-1.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved
```

```
================================================
=====================================
 Package          Arch           Version                Repository
Size
================================================
=====================================
Installing:
 clamd         i686         0.99.2-1.el6         epel         164 k

Transaction Summary
================================================
=====================================
Install       1 Package(s)

Total download size: 164 k
Installed size: 605 k
Is this ok [y/N]: y
Downloading Packages:
clamd-0.99.2-1.el6.i686.rpm                                    | 164 kB
00:02
Running rpm_check_debug
Running Transaction Test
```

```
Transaction Test Succeeded
Running Transaction
  Installing : clamd-0.99.2-1.el6.i686                              1/1
  Verifying                        :              clamd-0.99.2-1.el6.i686
1/1


Installed:
  clamd.i686 0:0.99.2-1.el6


Complete!
[root@cent database]# yum install clamav-devel
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: ftp.hosteurope.de
 * extras: ftp.hosteurope.de
 * updates: ftp.hosteurope.de
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package clamav-devel.i686 0:0.99.2-1.el6 will be installed
--> Finished Dependency Resolution
```

```
Dependencies Resolved


=====================================================
=========================================
 Package             Arch         Version              Repository
Size
=====================================================
=========================================
Installing:
 clamav-devel        i686        0.99.2-1.el6        epel          23
k


Transaction Summary
=====================================================
=========================================
Install       1 Package(s)


Total download size: 23 k
Installed size: 32 k
Is this ok [y/N]: y
Downloading Packages:
```

```
clamav-devel-0.99.2-1.el6.i686.rpm                    | 23 kB
00:00

Running rpm_check_debug

Running Transaction Test

Transaction Test Succeeded

Running Transaction

  Installing         :         clamav-devel-0.99.2-1.el6.i686
1/1

  Verifying            :       clamav-devel-0.99.2-1.el6.i686
1/1


Installed:

  clamav-devel.i686 0:0.99.2-1.el6


Complete!

[root@cent database]#


[root@cent database]# /etc/init.d/clamd status

clamd is stopped

[root@cent database]# /etc/init.d/clamd start

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:
**************************************************

LibClamAV Warning: cli_loadldb: logical signature for
Win.Trojan.ssid18332-1 uses PCREs but support is disabled,
skipping

LibClamAV Warning: cli_loadldb: logical signature for
Win.Ransomware.Locky-4 uses PCREs but support is disabled,
skipping

LibClamAV Warning: cli_loadldb: logical signature for
Html.Exploit.CVE_2016_0184-1 uses PCREs but support is
disabled, skipping

                                        [  OK  ]


[root@cent database]# clam

clamav-config  clamconf     clamdscan     clamscan

clambc        clamd        clamdtop      clamsubmit

[root@cent database]# clams

clamscan    clamsubmit

[root@cent database]# clamscan
```

```
LibClamAV Error: cli_loaddbdir(): No supported database files
found in /usr/local/share/clamav

ERROR: Can't open file or directory


----------- SCAN SUMMARY -----------

Known viruses: 0

Engine version: 0.99.2

Scanned directories: 0

Scanned files: 0

Infected files: 0

Data scanned: 0.00 MB

Data read: 0.00 MB (ratio 0.00:1)

Time: 0.189 sec (0 m 0 s)

[root@cent database]# updatedb


[root@cent database]# locate main.cvd

/root/Downloads/main.cvd

/root/Downloads/clamav-0.99.2/database/main.cvd

/var/lib/clamav/main.cvd

[root@cent database]#
```

```
[root@cent database]# vim /usr/local/etc/clamd.conf

[root@cent database]# vim /usr/local/etc/clamd.conf

[root@cent database]# # uncomment bellow line

[root@cent database]# # DatabaseDirectory /var/lib/clamav

[root@cent database]#


[root@cent database]# /etc/init.d/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:
**************************************************

LibClamAV Warning: cli_loadldb: logical signature for
Win.Trojan.ssid18332-1 uses PCREs but support is disabled,
skipping

LibClamAV Warning: cli_loadldb: logical signature for
Win.Ransomware.Locky-4 uses PCREs but support is disabled,
skipping
```

```
LibClamAV Warning: cli_loadldb: logical signature for Html.Exploit.CVE_2016_0184-1 uses PCREs but support is disabled, skipping
                                        [  OK  ]



[root@cent database]# ll /root/Downloads/clamav-0.99.2/database/main.cvd

-rw-rw-r-- 1 1000 1000 109143933 Jan 31 16:44 /root/Downloads/clamav-0.99.2/database/main.cvd

[root@cent database]# ll /root/Downloads/main.cvd

-rw-r--r-- 1 root root 109143933 Jan 31 16:41 /root/Downloads/main.cvd

[root@cent database]# ll /var/lib/clamav/main.cvd

-rw-r--r-- 1 clam clam 109143933 Jun 13  2016 /var/lib/clamav/main.cvd

[root@cent database]# cp /root/Downloads/main.cvd /var/lib/clamav

cp: overwrite `/var/lib/clamav/main.cvd'? y

[root@cent database]# cp /root/Downloads/*.cvd /var/lib/clamav/

cp: overwrite `/var/lib/clamav/bytecode.cvd'? y

cp: overwrite `/var/lib/clamav/daily.cvd'? y
```

```
cp: overwrite `/var/lib/clamav/main.cvd'? y

[root@cent database]#
```

```
[root@cent database]# cp /root/Downloads/*.cvd /usr/local/share/clamav
```

```
[root@cent database]# clamscan

LibClamAV Warning: **************************************************

LibClamAV Warning: ***  The virus database is older than 7 days!  ***

LibClamAV Warning: ***    Please update it as soon as possible.   ***

LibClamAV Warning: **************************************************

LibClamAV Warning: cli_loadldb: logical signature for Win.Trojan.ssid18332-1 uses PCREs but support is disabled, skipping

/root/Downloads/clamav-0.99.2/database/bytecode.cvd: OK

/root/Downloads/clamav-0.99.2/database/main.cvd: OK

/root/Downloads/clamav-0.99.2/database/Makefile.in: OK

/root/Downloads/clamav-0.99.2/database/Makefile.am: OK

/root/Downloads/clamav-0.99.2/database/daily.cvd: OK
```

```
/root/Downloads/clamav-0.99.2/database/Makefile: OK


----------- SCAN SUMMARY -----------
Known viruses: 4297372
Engine version: 0.99.2
Scanned directories: 1
Scanned files: 6
Infected files: 0
Data scanned: 4.51 MB
Data read: 106.32 MB (ratio 0.04:1)
Time: 43.058 sec (0 m 43 s)
[root@cent database]#
```

Note: I get error when sending mail

```
[root@cent etc]# netstat -ntlp | grep cour
tcp        0      0 :::993                    :::*                        LISTEN
1699/couriertcpd
tcp        0      0 :::995                    :::*                        LISTEN
1675/couriertcpd
tcp        0      0 :::110                    :::*                        LISTEN
1649/couriertcpd
```

```
tcp        0      0 :::143                      :::*                        LISTEN
1687/couriertcpd

[root@cent etc]# netstat -ntlp | grep 25

tcp             0           0  0.0.0.0:25                               0.0.0.0:*
LISTEN      2050/exim

tcp        0      0 :::25                       :::*                        LISTEN
2050/exim

[root@cent etc]# yum remove exim

Loaded plugins: fastestmirror, refresh-packagekit, security

Setting up Remove Process

Resolving Dependencies

--> Running transaction check

---> Package exim.i686 0:4.84.2-3.el6 will be erased

--> Processing Dependency: /usr/sbin/sendmail for package:
cronie-1.4.4-16.el6_8.2.i686

--> Restarting Dependency Resolution with new changes.

--> Running transaction check

---> Package cronie.i686 0:1.4.4-16.el6_8.2 will be erased

--> Processing Dependency: cronie = 1.4.4-16.el6_8.2 for
package: cronie-anacron-1.4.4-16.el6_8.2.i686

--> Running transaction check
```

```
---> Package cronie-anacron.i686 0:1.4.4-16.el6_8.2 will be
erased

--> Processing Dependency: /etc/cron.d for package: crontabs-
1.10-33.el6.noarch

--> Restarting Dependency Resolution with new changes.

--> Running transaction check

---> Package crontabs.noarch 0:1.10-33.el6 will be erased

--> Finished Dependency Resolution


Dependencies Resolved


================================================
=====================================

 Package           Arch       Version            Repository
Size

================================================
=====================================

Removing:

 exim           i686     4.84.2-3.el6       @epel       4.0
M

Removing for dependencies:

 cronie            i686       1.4.4-16.el6_8.2       @updates
169 k
```

```
 cronie-anacron      i686        1.4.4-16.el6_8.2        @updates
38 k

 crontabs         noarch      1.10-33.el6          @base        2.4
k


Transaction Summary

===============================================

====================================

Remove       4 Package(s)


Installed size: 4.2 M

Is this ok [y/N]: y

Downloading Packages:

Running rpm_check_debug

Running Transaction Test

Transaction Test Succeeded

Running Transaction

  Erasing                        :        crontabs-1.10-33.el6.noarch
1/4

warning: /etc/crontab saved as /etc/crontab.rpmsave

  Erasing                  :     cronie-anacron-1.4.4-16.el6_8.2.i686
2/4
```

```
  Erasing                     :        cronie-1.4.4-16.el6_8.2.i686
3/4
  Erasing    : exim-4.84.2-3.el6.i686                          4/4
  Verifying                 :           cronie-1.4.4-16.el6_8.2.i686
1/4
  Verifying  : exim-4.84.2-3.el6.i686                          2/4
  Verifying                 :            crontabs-1.10-33.el6.noarch
3/4
  Verifying             :       cronie-anacron-1.4.4-16.el6_8.2.i686
4/4

Removed:
  exim.i686 0:4.84.2-3.el6

Dependency Removed:
  cronie.i686 0:1.4.4-16.el6_8.2       cronie-anacron.i686 0:1.4.4-
16.el6_8.2
  crontabs.noarch 0:1.10-33.el6

Complete!
[root@cent etc]# netstat -ntlp | grep 25
```