HOWTO Virtual Mail Hosting on CentOS 6.x
Postfix MySQL Dovecot PostfixAdmin Amavisd-new Spamassassin Clamav

2013-09-22

URL: http://www.campworld.net/thewiki/pmwiki.php/LinuxServersCentOS/Cent6VirtMailServer

Start with my HOWTO: CentOS 6.x base server.

- Install packages:

```
> yum install roundcubemail dovecot dovecot-mysql dovecot-pigeonhole cyrus-sasl-devel cyrus-sasl-sql subversion
> yum install perl-MailTools perl-MIME-EncWords perl-MIME-Charset perl-Email-Valid perl-Test-Pod perl-TimeDate
> yum install perl-Mail-Sender perl-Log-Log4perl imapsync offlineimap
> yum install amavisd-new clamav clamd perl-Razor-Agent perl-Convert-BinHex crypto-utils mod_ssl
```

- Postfix.Admin doesn't have an rpm so we need to download it and put it where we want it.

```
> wget http://sourceforge.net/projects/postfixadmin/files/latest/download
> tar -xzvf postfixadmin-2.3.5.tar.gz
> mv postfixadmin-2.3.5 /usr/share/postfixadmin
```

- Setup SSL Certificate

Replace mail.example.com with your server hostname.

```
> genkey --days 3650 mail.example.com
```

- Setup the Virtual Mail User

```
> mkdir /home/vmail
> chmod 770 /home/vmail
> useradd -r -u 101 -g mail -d /home/vmail -s /sbin/nologin -c "Virtual mailbox" vmail
> chown vmail:mail /home/vmail
```

- Configuring Postfix Admin

/etc/httpd/conf.d/postfixadmin.conf

```
alias /mailadmin /usr/share/postfixadmin
<Directory "/usr/share/postfixadmin">
  AllowOverride AuthConfig
</Directory>
```

```
> service httpd restart
```

Now we need to setup the mysql database for postfixadmin:

```
> mysql -u root -p -e "CREATE DATABASE postfix;"
> mysql -u root -p -e "CREATE USER postfix@localhost IDENTIFIED BY 'choose_a_password';"
> mysql -u root -p -e "GRANT ALL PRIVILEGES ON postfix . * TO postfix@localhost;"
> cd /usr/share/postfixadmin
> nano -w config.php
```

```
<?php
/**
 * Contains configuration options that override the default config file
 */

/************************************************************
 *  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 * You have to set $CONF['configured'] = true; before the
 * application will run!
 * Doing this implies you have changed this file as required.
 * i.e. configuring database etc; specifying setup.php password etc.
 */
$CONF['configured'] = true;

// In order to setup Postfixadmin, you MUST specify a hashed password here.
// To create the hash, visit setup.php in a browser and type a password into the
field,
// on submission it will be echoed out to you as a hashed value.
$CONF['setup_password'] = 'changeme';
$CONF['postfix_admin_url'] = '/mailadmin';
$CONF['database_type'] = 'mysql';
$CONF['database_host'] = 'localhost';
$CONF['database_user'] = 'postfix';
$CONF['database_password'] = 'changeme';
$CONF['database_name'] = 'postfix';
$CONF['admin_email'] = 'postmaster@change-this-to-your.domain.tld';
$CONF['encrypt'] = 'md5crypt';
$CONF['dovecotpw'] = "/usr/sbin/doveadm pw";
$CONF['min_password_length'] = 6;
$CONF['page_size'] = '20';
$CONF['domain_path'] = 'YES';
$CONF['domain_in_mailbox'] = 'NO';
$CONF['aliases'] = '50';
$CONF['mailboxes'] = '50';
$CONF['maxquota'] = '100';
$CONF['quota'] = 'YES';
$CONF['quota_multiplier'] = '1024000';
$CONF['transport'] = 'YES';
$CONF['transport_options'] = array (
    'virtual',  // for virtual accounts
    'local',    // for system accounts
    'relay'     // for backup mx
);
$CONF['transport_default'] = 'virtual';
$CONF['vacation'] = 'YES';
$CONF['vacation_domain'] = 'autoreply.change-this-to-your.domain.tld';
$CONF['vacation_control'] ='YES';
$CONF['vacation_control_admin'] = 'YES';
$CONF['special_alias_control'] = 'YES';
$CONF['user_footer_link'] = "http://change-this-to-your.domain.tld/main";
$CONF['show_footer_text'] = 'YES';
$CONF['footer_text'] = 'Return to change-this-to-your.domain.tld';
$CONF['footer_link'] = 'http://change-this-to-your.domain.tld';
$CONF['create_mailbox_subdirs']=array('Drafts','Spam','Sent','Trash');
$CONF['create_mailbox_subdirs_host']='localhost';
$CONF['create_mailbox_subdirs_prefix']='';
$CONF['used_quotas'] = 'YES';
$CONF['new_quota_table'] = 'YES';
// $CONF['create_mailbox_subdirs_hostoptions']=array('notls');
$CONF['create_mailbox_subdirs_hostoptions']=array('novalidate-cert','norsh');

//
// END OF CONFIG FILE
//
```

Next we need to run the setup.php script in a web browser. Enter the url in your browser. Ex. http://yourdomain.tld/mailadmin/setup.php

If everything shows OK then create the admin user using the form displayed. Follow the instructions for setting the setup password.

Log into the web interface and follow the directions:
http://yourdomain.tld/mailadmin/

- Configuring Postfix

Just copy and past to create the config files. What ever you see here replaces what already exists:
/etc/postfix/main.cf :

```
# postfix config file

# uncomment for debugging if needed
#soft_bounce=yes

# postfix main
mail_owner = postfix
setgid_group = postdrop
delay_warning_time = 4

# postfix paths
html_directory = no
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
queue_directory = /var/spool/postfix
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
manpage_directory = /usr/share/man

# network settings
inet_interfaces = all
mydomain = yourdomain.com
myhostname = host.yourdomain.com
mynetworks = $config_directory/mynetworks
mydestination = $myhostname, localhost.$mydomain, localhost
relay_domains = proxy:mysql:/etc/postfix/mysql-relay_domains_maps.cf

# mail delivery
recipient_delimiter = +

# mappings
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
transport_maps = hash:/etc/postfix/transport
#local_recipient_maps =

# virtual setup
virtual_alias_maps = proxy:mysql:/etc/postfix/mysql-virtual_alias_maps.cf,
                     regexp:/etc/postfix/virtual_regexp
virtual_mailbox_base = /home/vmail
virtual_mailbox_domains = proxy:mysql:/etc/postfix/mysql-virtual_domains_maps.cf
virtual_mailbox_maps = proxy:mysql:/etc/postfix/mysql-virtual_mailbox_maps.cf
virtual_mailbox_limit_maps = proxy:mysql:/etc/postfix/mysql-
virtual_mailbox_limit_maps.cf
virtual_minimum_uid = 101
virtual_uid_maps = static:101
virtual_gid_maps = static:12
```

```
virtual_transport = dovecot
dovecot_destination_recipient_limit = 1

# debugging
debug_peer_level = 2
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5

# authentication
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

# tls config
smtp_use_tls = yes
smtpd_use_tls = yes
smtpd_tls_security_level = may
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
smtp_tls_session_cache_database = btree:$data_directory/smtp_tls_session_cache
# Change mail.example.com.* to your host name
smtpd_tls_key_file = /etc/pki/tls/private/mail.example.com.key
smtpd_tls_cert_file = /etc/pki/tls/certs/mail.example.com.crt
# smtpd_tls_CAfile = /etc/pki/tls/root.crt

# rules restrictions
smtpd_client_restrictions =
smtpd_helo_restrictions =
smtpd_sender_restrictions =
smtpd_recipient_restrictions = permit_sasl_authenticated,
        permit_mynetworks,
        reject_unauth_destination,
        reject_non_fqdn_sender,
        reject_non_fqdn_recipient,
        reject_unknown_recipient_domain
# uncomment for realtime black list checks
#       ,reject_rbl_client zen.spamhaus.org
#       ,reject_rbl_client bl.spamcop.net
#       ,reject_rbl_client dnsbl.sorbs.net

smtpd_helo_required = yes
unknown_local_recipient_reject_code = 550
disable_vrfy_command = yes
smtpd_data_restrictions = reject_unauth_pipelining

# Other options
# email size limit ~20Meg
message_size_limit = 204800000

mailbox_size_limit = 2048000000
```

/etc/postfix/master.cf :

```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the Postfix master(5) manual page.
#
```

```
# ***** Unused items removed *****
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
#  -o content_filter=smtp-amavis:127.0.0.1:10024
#  -o receive_override_options=no_address_mappings
pickup    fifo  n       -       n       60      1       pickup
  -o content_filter=
  -o receive_override_options=no_header_body_checks
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
smtp      unix  -       -       n       -       -       smtp
# When relaying mail as backup MX, disable fallback_relay to avoid MX loops
relay     unix  -       -       n       -       -       smtp
        -o fallback_relay=
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache    unix  -       -       n       -       1       scache
#
# ==========================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
# ==========================================================================
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=foo argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient
#
# spam/virus section
#
smtp-amavis  unix  -    -       y       -       2       smtp
  -o smtp_data_done_timeout=1200
  -o disable_dns_lookups=yes
  -o smtp_send_xforward_command=yes
127.0.0.1:10025 inet n  -       y       -       -       smtpd
  -o content_filter=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
```

```
  -o receive_override_options=no_header_body_checks
  -o smtpd_bind_address=127.0.0.1
  -o smtpd_helo_required=no
  -o smtpd_client_restrictions=
  -o smtpd_restriction_classes=
  -o disable_vrfy_command=no
  -o strict_rfc821_envelopes=yes
#
# Dovecot LDA
dovecot   unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail:mail argv=/usr/libexec/dovecot/deliver -d ${recipient}
#
# Vacation mail
vacation    unix  -       n       n       -       -       pipe
  flags=Rq user=vacation argv=/var/spool/vacation/vacation.pl -f ${sender} -- $
{recipient}
```

/etc/postfix/mynetworks:

```
# This specifies the list of subnets that Postfix considers as
# "trusted" SMTP clients that have more privileges than "strangers".
#
# In particular, "trusted" SMTP clients are allowed to relay mail
# through Postfix.
#
# Be sure to add your public ip address block if needed.
#
192.168.0.0/16
10.0.0.0/8
127.0.0.0/8
```

The postfix / mysql config files.
/etc/postfix/mysql-virtual_alias_maps.cf :

```
hosts = localhost
user = postfix
password = postfix
dbname = postfix
query = SELECT goto FROM alias WHERE address='%s' AND active = '1'
```

/etc/postfix/mysql-virtual_domains_maps.cf :

```
hosts = localhost
user = postfix
password = postfix
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%s' AND backupmx = '0' AND active =
'1'
```

/etc/postfix/mysql-relay_domains_maps.cf :

```
hosts = localhost
user = postfix
password = postfix
dbname = postfix
query = SELECT domain FROM domain WHERE domain='%s' and backupmx = '1'
```

/etc/postfix/mysql-virtual_mailbox_maps.cf :

```
hosts = localhost
```

```
user = postfix
password = postfix
dbname = postfix
query = SELECT maildir FROM mailbox WHERE username='%s' AND active = '1'
```

/etc/postfix/mysql-virtual_mailbox_limit_maps.cf :

```
hosts = localhost
user = postfix
password = postfix
dbname = postfix
query = SELECT quota FROM mailbox WHERE username='%s' AND active = '1'
```

We need to touch a file. So type the follwoing.

```
> touch /etc/postfix/virtual_regexp
```

- Configure Vacation Email Functionallity

Don't forget to fill in your domain name where needed. Type the following:

```
> useradd -r -d /var/spool/vacation -s /sbin/nologin -c "Virtual vacation" vacation
> mkdir /var/spool/vacation
> chmod 770 /var/spool/vacation
> cp /usr/share/postfixadmin/VIRTUAL_VACATION/vacation.pl /var/spool/vacation/
> echo "autoreply.yourdomain.com vacation:" > /etc/postfix/transport
> postmap /etc/postfix/transport
> chown -R vacation:vacation /var/spool/vacation
> echo "127.0.0.1 autoreply.yourdomain.com" >> /etc/hosts
> mkdir /etc/postfixadmin
```

Create /etc/postfixadmin/vacation.conf with the following:

```
# ========== begin configuration ==========
$db_type = 'mysql';
$db_username = 'user';
$db_password = 'password';
$db_name     = 'postfix';
$vacation_domain = 'autoreply.example.org';
```

- Configuring Dovecot

Now for the dovecot config file. Dovecot now uses multiple config files to break things up. We're going to only use a couple config files. So cut and paste the following files.

```
> mv /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.save
> nano -w /etc/dovecot/dovecot.conf
```

```
##
## Dovecot config file
##

protocols = imap pop3 lmtp sieve
auth_mechanisms = plain login
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-mysql.conf
}
userdb {
  driver = prefetch
}
```

```
userdb {
  driver = sql
  args = /etc/dovecot/dovecot-mysql.conf
}
mail_location = maildir:/home/vmail/%d/%n
first_valid_uid = 101
#last_valid_uid = 0
first_valid_gid = 12
#last_valid_gid = 0
#mail_plugins =
mailbox_idle_check_interval = 30 secs
maildir_copy_with_hardlinks = yes
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }
}
service pop3-login {
  inet_listener pop3 {
    port = 110
  }
  inet_listener pop3s {
    port = 995
    ssl = yes
  }
}
service lmtp {
  unix_listener lmtp {
    #mode = 0666
  }
}
service imap {
  vsz_limit = 256M
}
service pop3 {
}
service auth {
  unix_listener auth-userdb {
    mode = 0666
    user = vmail
    group = mail
  }

  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
}
service auth-worker {
}
service dict {
  unix_listener dict {
    mode = 0666
    user = vmail
    group = mail
  }
}
service managesieve-login {
```

```
  inet_listener sieve {
    port = 4190
  }
  service_count = 1
  process_min_avail = 0
  vsz_limit = 64M
}
service managesieve {
}
ssl = yes
ssl_cert = </etc/pki/tls/certs/your-server.your-domain.tld.crt
ssl_key = </etc/pki/tls/private/your-server.your-domain.tld.key
ssl_verify_client_cert = no
#ssl_ca =
lda_mailbox_autocreate = yes
lda_mailbox_autosubscribe = yes
protocol lda {
  mail_plugins = quota sieve
  postmaster_address = postmaster@your-domain.tld
}
protocol imap {
  mail_plugins = quota imap_quota trash
  imap_client_workarounds = delay-newmail
}
lmtp_save_to_detail_mailbox = yes
protocol lmtp {
  mail_plugins = sieve
}
protocol pop3 {
  mail_plugins = quota
  pop3_client_workarounds = outlook-no-nuls oe-ns-eoh
}
protocol sieve {
  managesieve_max_line_length = 65536
  managesieve_implementation_string = Dovecot Pigeonhole
  managesieve_max_compile_errors = 5
}
dict {
  quotadict = mysql:/etc/dovecot/dovecot-dict-quota.conf
}
plugin {
  quota = dict:user::proxy::quotadict
  acl = vfile:/etc/dovecot/acls
  trash = /etc/dovecot/trash.conf
  sieve_global_path = /home/sieve/globalfilter.sieve
  sieve = ~/dovecot.sieve
  sieve_dir = ~/sieve
  sieve_global_dir = /home/sieve/
  #sieve_extensions = +notify +imapflags
  sieve_max_script_size = 1M
  #sieve_max_actions = 32
  #sieve_max_redirects = 4
}
```

Now for trash.conf :

```
> nano -w /etc/dovecot/trash.conf
```

```
1 Spam
# Uncomment if you want trash as well
# 2 Trash
```

Next we configure Dovecot to access mysql. Create the following file.
NOTE: password_query and user_query were formatted to fit on the webpage. Each one should only be one line in the file.
/etc/dovecot/dovecot-mysql.conf :

```
driver = mysql
connect = host=localhost dbname=postfix user=postfix password=yourpassword
default_pass_scheme = MD5-CRYPT

# following should all be on one line.
password_query = SELECT username as user, password, concat('/home/vmail/', maildir)
as userdb_home,
concat('maildir:/home/vmail/', maildir) as userdb_mail, 101 as userdb_uid, 12 as
userdb_gid FROM mailbox
WHERE username = '%u' AND active = '1'

# following should all be on one line
user_query = SELECT concat('/home/vmail/', maildir) as home,
concat('maildir:/home/vmail/', maildir) as mail,
101 AS uid, 12 AS gid, CONCAT('*:messages=10000:bytes=', quota) as quota_rule FROM
mailbox WHERE
username = '%u' AND active = '1'
```

/etc/dovecot/dovecot-dict-quota.conf:

```
connect = host=localhost dbname=postfix user=postfix password=password
map {
  pattern = priv/quota/storage
  table = quota2
  username_field = username
  value_field = bytes
}
map {
  pattern = priv/quota/messages
  table = quota2
  username_field = username
  value_field = messages
}
```

Finally set Dovecot to boot at startup.

Now Create the sieve filter for SPAM filtering.

```
> mkdir /home/sieve
> nano -w /home/sieve/globalfilter.sieve
> chown -R vmail:mail /home/sieve
```

```
require "fileinto";
  if exists "X-Spam-Flag" {
          if header :contains "X-Spam-Flag" "NO" {
          } else {
          fileinto "Spam";
          stop;
          }
  }
  if header :contains "subject" ["***SPAM***"] {
    fileinto "Spam";
    stop;
  }
```

- Configuring Roundcube mail

Edit the roundcube apache config file to look like the following:

```
>nano -w /etc/httpd/conf.d/roundcubemail.conf
```

```
#
# Round Cube Webmail is a browser-based multilingual IMAP client
#

# Force https here instead of in Round Cube
RewriteEngine On

# This checks to make sure the connection is not already HTTPS
RewriteCond %{HTTPS} !=on

# These rules will redirect all users who are using any part of /secure/ to the same
location but using HTTPS.
# i.e.  http://www.example.com/secure/ to https://www.example.com/secure/
RewriteRule ^/?roundcubemail/(.*) https://%{SERVER_NAME}/roundcubemail/$1 [R,L]
RewriteRule ^/?webmail/(.*) https://%{SERVER_NAME}/webmail/$1 [R,L]

Alias /roundcubemail /usr/share/roundcubemail
Alias /webmail /usr/share/roundcubemail

<Directory /usr/share/roundcubemail/>
        Order Deny,Allow
        Deny from all
        Allow from all
        php_value suhosin.session.encrypt Off
</Directory>
```

Create the database for roundcube.

```
> mysql -u root -p -e "CREATE DATABASE roundcubemail;"
> mysql -u root -p -e "GRANT ALL PRIVILEGES ON roundcubemail.* TO roundcube@localhost
IDENTIFIED BY 'password';"
```

Create the tables.

```
> mysql -u root -p roundcubemail < /usr/share/doc/roundcubemail-<version>/SQL/mysql.initial.sql
```

Edit /etc/roundcubemail/db.inc.php and find the line:

```
$rcmail_config['db_dsnw'] = 'mysql://roundcube:pass@localhost/roundcubemail';
```

Change 'pass' to your passowrd.

Edit /etc/roundcubemail/main.inc.php and find the lines and make the changes below:

find:

```
$rcmail_config['default_host'] = '';
```

change to:

```
$rcmail_config['default_host'] = 'localhost';
```

find:

```
$rcmail_config['smtp_server'] = '';
```

change to:

```
$rcmail_config['smtp_server'] = 'localhost';
```

find:

```
$rcmail_config['force_https'] = false;
```

change to:

```
$rcmail_config['force_https'] = true;
```

find:

```
$rcmail_config['plugins'] = array();
```

change to:

```
$rcmail_config['plugins'] = array('managesieve');
```

find:

```
$rcmail_config['quota_zero_as_unlimited'] = false;
```

change to:

```
$rcmail_config['quota_zero_as_unlimited'] = true;
```

Now lets configure the manage sieve plugin.

```
> cd /usr/share/roundcubemail/plugins/managesieve/
> cp config.inc.php.dist config.inc.php
```

Edit config.inc.php and change the following:

```
$rcmail_config['managesieve_port'] = 2000;
```

to:

```
$rcmail_config['managesieve_port'] = 4190;
```

Restart apache.

```
> service httpd restart
```

- Be sure your ***/etc/hosts*** looks similar to the following.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost
192.168.11.21   host.domain.com
```

- Preparing and Testing the Postoffice

First things first. Reboot the system. If everything went well we all should be at the same point.
No errors? Lets keep going.
Setup a test domain and account. Setup your favorit mail client and send some test emails.

- Setting up Spam and Virus Filtering (Optional)

Lets cover installing and configuring spam and virus filtering. Optional? Huh? Some people use a 3rd party or use a seperate server for filtering.

Here's the clamav config file. Replace /etc/clamd.conf with the following:

```
##
## Cconfig file for the Clam AV daemon
## Please read the clamd.conf(5) manual before editing this file.
##

# Logfile
LogFile /var/log/clamav/clamd.log
LogFileMaxSize 20M
LogTime yes
LogSyslog yes

# Pid
PidFile /var/run/clamav/clamd.pid

# Paths
TemporaryDirectory /var/tmp
DatabaseDirectory /var/lib/clamav
LocalSocket /var/run/clamav/clamd

# Sets the group ownership on the unix socket.
# Default: disabled (the primary group of the user running clamd)
#LocalSocketGroup virusgroup

# Misc
FixStaleSocket yes
TCPSocket 3310
TCPAddr 127.0.0.1
MaxConnectionQueueLength 50
MaxThreads 50
ReadTimeout 240
User clamav
AllowSupplementaryGroups yes

# Exe
ScanPE yes
ScanELF yes
DetectBrokenExecutables yes

# Docs
ScanOLE2 yes
ScanPDF yes

# Mail
ScanMail yes
PhishingSignatures yes
PhishingScanURLs yes

# Data Loss Prevention (DLP)

# Enable the DLP module
# Default: No
#StructuredDataDetection yes

# This option sets the lowest number of Credit Card numbers found in a file
# to generate a detect.
```

```
# Default: 3
#StructuredMinCreditCardCount 5

# This option sets the lowest number of Social Security Numbers found
# in a file to generate a detect.
# Default: 3
#StructuredMinSSNCount 5

# With this option enabled the DLP module will search for valid
# SSNs formatted as xxx-yy-zzzz
# Default: yes
#StructuredSSNFormatNormal yes

# With this option enabled the DLP module will search for valid
# SSNs formatted as xxxyyzzzz
# Default: no
#StructuredSSNFormatStripped yes

# Archives
ScanArchive yes
ArchiveBlockEncrypted no
```

Configure Razor. Type the following:

```
> razor-admin -register -user=some_user -pass=somepas
```

Update and restart clamav:

```
> freshclam
> service clamd restart
```

- Configuring Amavisd-new

You need to edit ***/etc/amavisd/amavisd.conf***
Here is a list of items you should change. just scroll through the file to find each item.

$mydomain = 'example.com'; # set to your domain name
$log_level = 1; # set the log leve to one
$sa_tag_level_deflt = -99; # i want to see the headers so change to -99
$sa_tag2_level_deflt = 5.0; # start with 5
$sa_kill_level_deflt = 9; # change to 9
$sa_dsn_cutoff_level = 9; # change to 9
$sa_quarantine_cutoff_level = 50; # remove the starting # and change to 50
$myhostname = 'lightning.campworld.net'; # remove the starting # and enter your host name
$notify_method = 'smtp:[127.0.0.1]:10025'; # uncomment the line
$forward_method = 'smtp:[127.0.0.1]:10025'; # uncomment the line
$final_banned_destiny = D_DISCARD; # change to D_DISCARD

Now enable clamav:
Change the following:

```
# ### http://www.clamav.net/
# ['ClamAV-clamd',
#   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd"],
#   qr/\bOK$/m, qr/\bFOUND$/m,
#   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

to

```
 ### http://www.clamav.net/
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd"],
   qr/\bOK$/m, qr/\bFOUND$/m,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
```

Now update spamassassin and start amavisd-new.

```
> sa-update
> service amavisd-new start
```

Be sure to set amavisd-new to start at boot.

- Telling Postfix to Start Filtering SPAM

To get postfix going we need to un-comment a couple lines in /etc/postfix/master.cf
Find:

```
smtp      inet  n       -       n       -       -       smtpd
#  -o content_filter=smtp-amavis:127.0.0.1:10024
#  -o receive_override_options=no_address_mappings
```

Change to:

```
smtp      inet  n       -       n       -       -       smtpd
  -o content_filter=smtp-amavis:127.0.0.1:10024
  -o receive_override_options=no_address_mappings
```

Restart postfix and you're done.!

- Using The Roundcubemail Password Plugin (Optional)

Let your users change their password using roundcubemail instead of postfixadmin.
Edit /etc/roundcubemail/main.inc.php and find the lines and make the changes below:
find:

```
$rcmail_config['plugins'] = array('managesieve');
```

change to:

```
$rcmail_config['plugins'] = array('managesieve','password');
```

Now lets configure the password plugin.

```
> cd /usr/share/roundcubemail/plugins/password/
> cp config.inc.php.dist config.inc.php
```

Edit config.inc.php

find:

```
$rcmail_config['password_db_dsn'] = '';
```

change to:

```
$rcmail_config['password_db_dsn'] = 'mysql://postfix:your-postfixadmin-
password@localhost/postfix';
```

find:

```
$rcmail_config['password_query'] = 'SELECT update_passwd(%c, %u)';
```

change to:

```
$rcmail_config['password_query'] = 'UPDATE mailbox SET password=%c WHERE username=%u
limit 1;';
```

Restart apache.

```
> service httpd restart
```