Table of Contents

Seiichiros mail-setup adapted for Ubuntu: Postfix + Dspam/ClamAV + Dovecot2 3
Software 3
Adapted Overview including ClamAV 3
Adding repo and installing software 4
Adding Service User 4
Deamons 4
Dspam 4
ClamAV 6
Dovecot2 7
Postfix 7
Services restart 9

Seiichiros mail-setup adapted for Ubuntu: Postfix + Dspam/ClamAV + Dovecot2

To use Seiichiros mail-setup with Ubuntu 10.04 I have to make a couple of changes. I will describe here only these changes. The complete setup can be found on **Seiichiros Website**.

The Ubuntu 10.04 standard repository doesn't offer a package for dovecot2. Dovecot1 doesn't support lmtp and the antispam plugin has a bug. With use of an additional repository the configurations can be made as described by Seiichiro. I had to made a few adjustments and I integrated support for ClamAV.

Software

- Ubuntu linux 10.04 LTS
- Postfix (version 2.7.0-1)
- DSPAM (version 3.6.8-9)
- Dovecot (version 2) extra repo

```
ii  dovecot-antispam                    2.0.0+hg45-0xk1                    a
Dovecot plugin that helps train spam filte
ii  dovecot-common                      1:2.0.6-0xk1
secure mail server that supports mbox and ma
ii  dovecot-imapd                       1:2.0.6-0xk1
secure IMAP server that supports mbox and ma
ii  dovecot-pigeonhole                  0.2.1-0xk1
secure mail server - sieve and managesieve
```

Adapted Overview including ClamAV

```
Outgoing Mail:
mail client --outgoing mail--> postfix(Port 587) --> recipient smtp server
                                      |
                                      |--> dovecot(sasl authentication) -->
passwd-file

Incoming Mail:
sender smtp server --incoming mail--> postfix(Port 25) --lmtp--> dspam --
smtp--> postfix(Port 10026) --lmtp--> dovecot(Sieve Filter) --> Users
Mailbox
                                                                    ^
                                                                    |
                                                                    v
                                                            clamav Virus check
```

Adding repo and installing software

```
vi /etc/apt/sources.list
```

```
...
deb     http://codex.xiaoka.com/apt  lucid  main restricted
deb-src http://codex.xiaoka.com/apt  lucid  main restricted
```

```
apt-get update

apt-get upgrade

apt-get install dovecot-common dovecot-antispam dovecot-pigeonhole
```

Adding Service User

Unchanged: please see Seiichiros documentation

Deamons

Dspam

You have to change the socket path to:

```
ServerDomainSocketPath "/var/spool/postfix/dspam/dspam.sock"
```

And create the according directory and correct rights.

```
mkdir /var/spool/postfix/dspam
chown -R vmail.dspam /var/spool/postfix/dspam
```

My /etc/dspam/dspam.conf

```
## $Id: dspam.conf.in,v 1.72 2006/05/14 15:40:42 jonz Exp $
## dspam.conf -- DSPAM configuration file
##

Home /var/spool/dspam

StorageDriver /usr/lib/dspam/libhash_drv.so

DeliveryHost        127.0.0.1
DeliveryPort        10026
```

```
DeliveryIdent       localhost
DeliveryProto       SMTP

OnFail error

Trust root
Trust dspam
Trust mail
Trust mailnull
Trust smmsp
Trust daemon
Trust vmail

TrainingMode teft
TestConditionalTraining on

Feature chained
Feature whitelist

Algorithm graham burton

Tokenizer chain
PValue graham

Preference "spamAction=deliver"
Preference "signatureLocation=headers"    # 'message' or 'headers'
Preference "showFactors=on"

AllowOverride trainingMode
AllowOverride spamAction spamSubject
AllowOverride statisticalSedation
AllowOverride enableBNR
AllowOverride enableWhitelist
AllowOverride signatureLocation
AllowOverride showFactors
AllowOverride optIn optOut
AllowOverride whitelistThreshold

HashRecMax      98317
HashAutoExtend      on
HashMaxExtents      0
HashExtentSize      49157
HashMaxSeek     100
HashConnectionCache 10
Notifications   off

PurgeSignatures 14          # Stale signatures
PurgeNeutral    90          # Tokens with neutralish probabilities
PurgeUnused     90          # Unused tokens
PurgeHapaxes    30          # Tokens with less than 5 hits (hapaxes)
PurgeHits1S 15          # Tokens with only 1 spam hit
```

```
PurgeHits1I 15          # Tokens with only 1 innocent hit

LocalMX 127.0.0.1

SystemLog on
UserLog   on

Opt out

ParseToHeaders on
ChangeModeOnParse on
ChangeUserOnParse full

Broken case

ClamAVPort  3310
ClamAVHost  127.0.0.1
ClamAVResponse spam

ServerPID              /var/run/dspam/dspam.pid

ServerMode              auto

ServerParameters        "--deliver=innocent,spam"
ServerIdent             "mail.example.org" # servers hostname

ServerDomainSocketPath "/var/spool/postfix/dspam/dspam.sock"
ProcessorBias on

Include /etc/dspam/dspam.d/

## EOF
```

In /etc/dspam/default.prefs you can configure the tagging behavior (tag only the message header and not the content … yes signature location in dspam.conf will be ignored). Change the “statisticalSedation” as you wish.

```
....
# Statistical Sedation: 0-10
statisticalSedation=2

# Signature Location: message, headers, attachment
signatureLocation=headers
....
```

ClamAV

Comment the local socket and create a TCP socket:

```
...
##LocalSocket /var/run/clamav/clamd.ctl
##FixStaleSocket true
...
TCPSocket 3310
TemporaryDirectory /tmp
```

Dovecot2

Comment the include when you don't need it:

```
##!include conf.d/*.conf
```

And change the path for the sockets:

```
...
 unix_listener /var/spool/postfix/private/dovecot-lmtp {
#  unix_listener lmtp-client {
...
  unix_listener /var/spool/postfix/private/auth {
#  unix_listener auth-client {

...
```

Sieve Rule for infected Mails

```
require ["fileinto"];
# rule:[VIRUS]
if anyof (header :contains "X-DSPAM-Result" "Virus")
{
        fileinto "Infected";
        stop;
}
```

Postfix

Change the sockets according to the changes made in the config files

/etc/postfix/main.cf

```
...
virtual_transport = lmtp:unix:private/dovecot-lmtp
...
```

/etc/postfix/master.cf

```
#
# Postfix master process configuration file.  For details on the format
```

```
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       -       -       -       smtpd
  -o content_filter=lmtp:unix:dspam/dspam.sock
# Submission port 587 for client connection / sending mails from
authenticated users
submission inet n       -       -       -       -       smtpd
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_sasl_type=dovecot
  -o smtpd_sasl_security_options=noanonymous
  -o smtpd_sasl_path=private/auth
  -o
smtpd_recipient_restrictions=reject_unknown_recipient_domain,reject_non_fqdn
_recipient,permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       -       -       -       smtpd
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
localhost:10026 inet  n -       n       -       -       smtpd
  -o content_filter=
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
  -o smtpd_helo_restrictions=
  -o smtpd_client_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8
#628       inet  n       -       -       -       -       qmqpd
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       -       300     1       oqmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
```

```
smtp      unix  -       -       -       -       -       smtp
# When relaying mail as backup MX, disable fallback_relay to avoid MX loops
relay     unix  -       -       -       -       -       smtp
    -o smtp_fallback_relay=
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
retry     unix  -       -       -       -       -       error
discard   unix  -       -       -       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       -       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
# ====================================================================
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail
($recipient)
#
# Other external delivery methods.
#
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=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender
$recipient
scalemail-backend unix  -    n    n    -    2    pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store
${nexthop} ${user} ${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

Services restart

```
/etc/init.d/clamav-daemon restart
/etc/init.d/dspam restart
/etc/init.d/dovecot restart
/etc/init.d/postfix restart
```