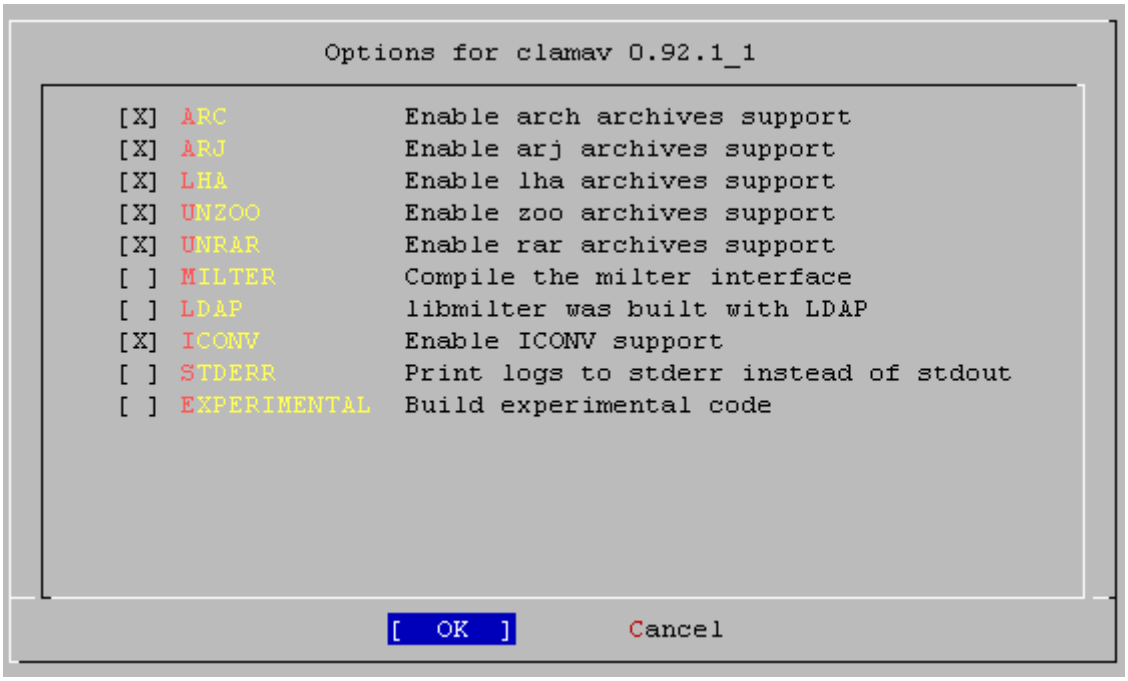
Настройка почтовой системы на freebsd. Часть II

Установка и настройка clamav

Устанавливаем антивирус clamav, который будет проверять все почтовые сообщения на вирусы.

```
# cd /usr/ports/security/clamav
# make config
```




```
# make install clean
```

Настраиваем запуск clamd и freshclam вместе с системой

```
# echo 'clamav_clamd_enable="YES"' >> /etc/rc.conf
# echo 'clamav_freshclam_enable="YES"' >> /etc/rc.conf
```

Настраиваем clamav, для этого редактируем конфигурационный файл **/usr/local/etc/clamd.conf** . Единтсвенное что я изменил - это путь к сокету, уменьшил размер сканируемых архивов до 5 мб, для уменьшения нагрузки и разрешил сканирование pdf файлов. Привожу все содержимое clamd.conf.

```
# cat /usr/local/etc/clamd.conf | grep -v ^# | grep -v ^$
LogFile /var/log/clamav/clamd.log
PidFile /var/run/clamav/clamd.pid
```

```
DatabaseDirectory /var/db/clamav
LocalSocket /var/run/clamav/clamd.sock
FixStaleSocket yes
User vscan
AllowSupplementaryGroups yes
ScanPDF yes
ScanMail yes
ArchiveMaxFileSize 5M
```

Выставляем необходимые права и запускаем clamav

```
# chown -R vscan:clamav /var/log/clamav/
# chown -R vscan:clamav /var/run/clamav/
# chown -R vscan:clamav /var/db/clamav/

# /usr/local/etc/rc.d/clamav-clamd start
Starting clamav_clamd.
```

При этом в log-файле должно быть следующее:

```
# cat /var/log/clamav/clamd.log
+++ Started at Wed Mar 26 20:59:05 2008
clamd daemon 0.92.1 (OS: freebsd7.0, ARCH: i386, CPU: i386)
Running as user vscan (UID 110, GID 110)
Log file size limited to 1048576 bytes.
Reading databases from /var/db/clamav
Not loading PUA signatures.
Loaded 208929 signatures.
Unix socket file /var/run/clamav/clamd.sock
Setting connection queue length to 15
Listening daemon: PID: 23819
Archive: Archived file size limit set to 10485760 bytes.
Archive: Recursion level limit set to 8.
Archive: Files limit set to 1000.
Archive: Compression ratio limit set to 250.
Archive support enabled.
Algorithmic detection enabled.
Portable Executable support enabled.
ELF support enabled.
Mail files support enabled.
Mail: Recursion level limit set to 64.
OLE2 support enabled.
PDF support enabled.
HTML support enabled.
Self checking every 1800 seconds.
Set stacksize to 1114112
```

После того, как сам антивирус успешно запустился нам необходимо обновить сами

антивирусные базы данных. Для этого существует специальная программа freshclam, которая идет вместе с clamav. Для ее настройки необходимо отредактировать конфигурационный файл **/usr/local/etc/freshclam.conf** .

По сути, в нем ничего не надо менять, единственное, что я поменял - зеркало (DatabaseMirror) с которого обновлять базы, так как были проблемы с украинскими зеркалами и периодичность обновлений (Checks) - каждый час (по умолчанию каждые два часа)

```
# cat /usr/local/etc/freshclam.conf | grep -v ^# | grep -v ^$
DatabaseDirectory /var/db/clamav
UpdateLogFile /var/log/clamav/freshclam.log
PidFile /var/run/clamav/freshclam.pid
DatabaseOwner vscan
AllowSupplementaryGroups yes
DatabaseMirror db.ru.clamav.net
Checks 24
NotifyClamd /usr/local/etc/clamd.conf
```

После этого запускаем freshclam:

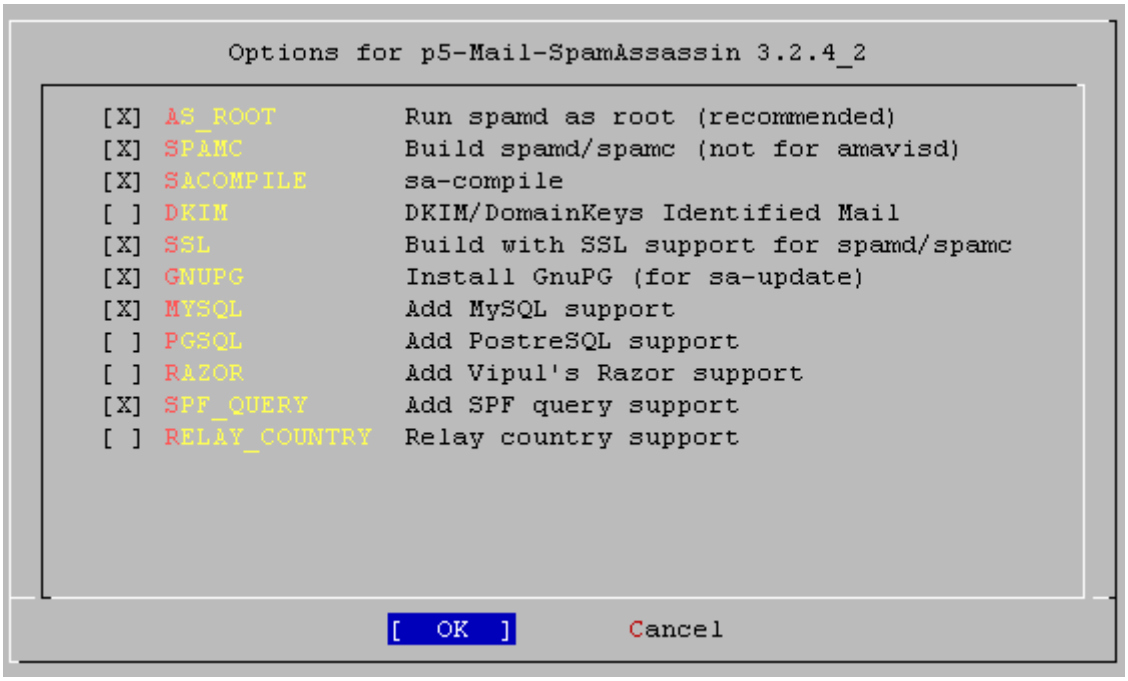
```
# /usr/local/etc/rc.d/clamav-freshclam start
Starting clamav_freshclam.

# cat /var/log/clamav/freshclam.log
-------------------------------------
Current working dir is /var/db/clamav
freshclam daemon 0.92.1 (OS: freebsd7.0, ARCH: i386, CPU: i386)
Max retries == 3
ClamAV update process started at Fri Mar 28 15:38:43 2008
Querying current.cvd.clamav.net
TTL: 300
Software version from DNS: 0.92.1
main.cvd version from DNS: 45
main.cvd is up to date (version: 45, sigs: 169676, f-level: 21, builder:
sven)
daily.cvd version from DNS: 6443
daily.cvd updated (version: 6443, sigs: 65798, f-level: 26, builder:
ccordes)
Database updated (235474 signatures) from db.ru.clamav.net (IP:
81.19.68.130)
Clamd successfully notified about the update.
-------------------------------------
```

Все с антивирусом мы разобрались, теперь настраиваем антиспам.

Установка и настройка spamassassin

```
# cd /usr/ports/mail/p5-Mail-SpamAssassin
# make config
```




```
# make install clean
```

Настраиваем запуск spamassassin вместе с системой

```
# echo 'spamd_enable="YES"' >> /etc/rc.conf
```

После установки, производим настройку spamassassin. Для этого создаем файл **/usr/local/etc/mail/spamassassin/local.cf** со следующим содержимым.

```
# cat /usr/local/etc/mail/spamassassin/local.cf | grep -v ^# | grep -v ^$
rewrite_header Subject *****SPAM*****
report_safe 1
required_score 7.0
use_bayes 1
bayes_auto_learn 1
bayes_ignore_header X-Bogosity
bayes_ignore_header X-Spam-Flag
bayes_ignore_header X-Spam-Status
```

Я привел лишь минимальный набор параметров, необходимый для проверки нашей системы. Для получения полного списка всех параметров, а также описания их назначения выполните следующую команду

```
# perldoc Mail::SpamAssassin::Conf
```

После того, как мы произвели минимальную настройку можно запустить сам демон.

```
# /usr/local/etc/rc.d/sa-spamd start
Starting spamd.
```

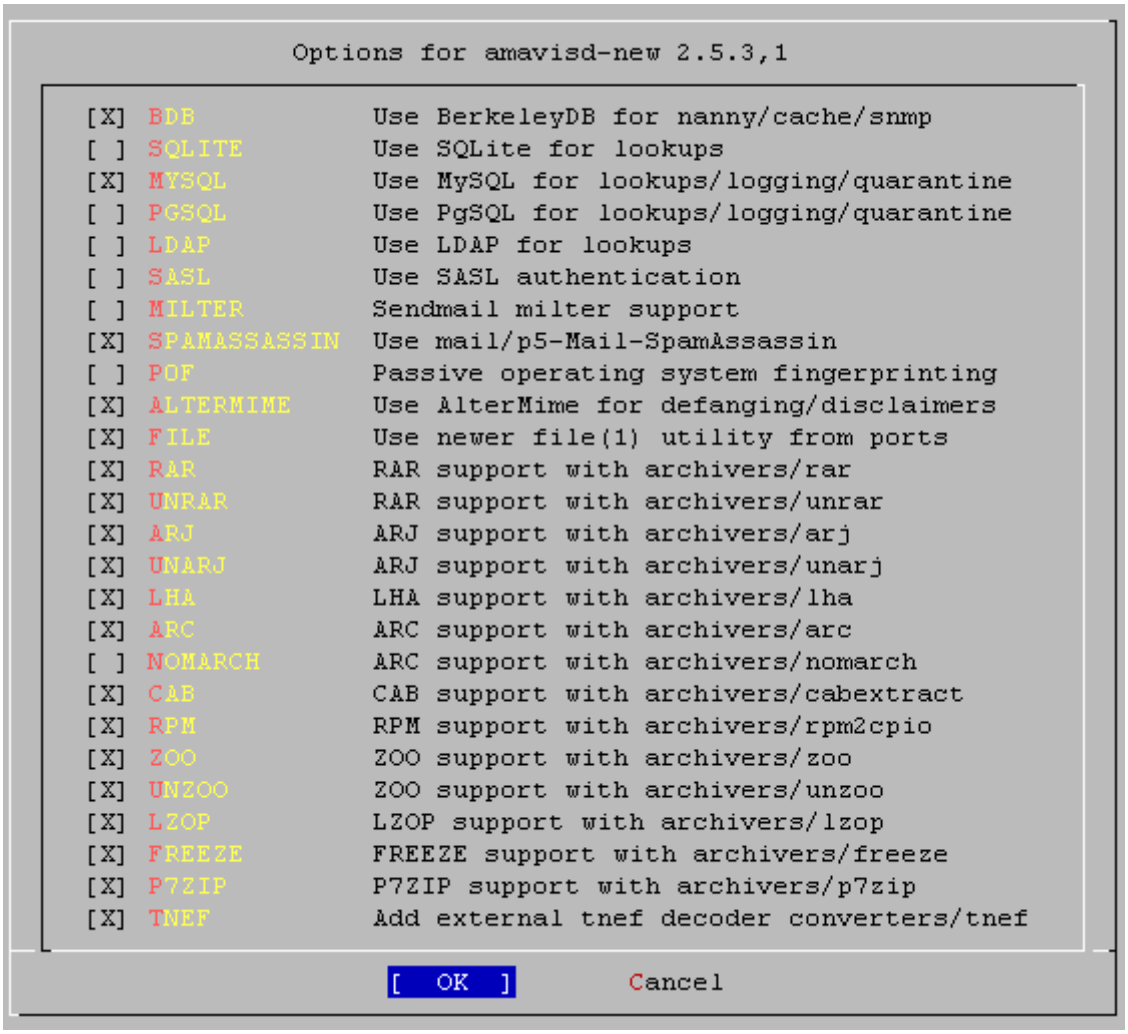
При этом в log-файле должны быть примерно такие записи:

```
# cat /var/log/maillog | grep spamd
Mar 26 21:16:26 mail spamd[23867]: logger: removing stderr method
Mar 26 21:16:29 mail spamd[23869]: spamd: server started on port 783/tcp
(running version 3.2.4)
Mar 26 21:16:29 mail spamd[23869]: spamd: server pid: 23869
Mar 26 21:16:29 mail spamd[23869]: spamd: server successfully spawned child
process, pid 23870
Mar 26 21:16:29 mail spamd[23869]: spamd: server successfully spawned child
process, pid 23871
Mar 26 21:16:29 mail spamd[23869]: prefork: child states: II
```

Установка и настройка amavisd-new

Устанавливаем amavisd-new, который является посредником между MTA (postfix) и различными фильтрами/сканерами (spamassassin, clamav)

```
 # cd /usr/ports/security/amavisd-new
# make config
```

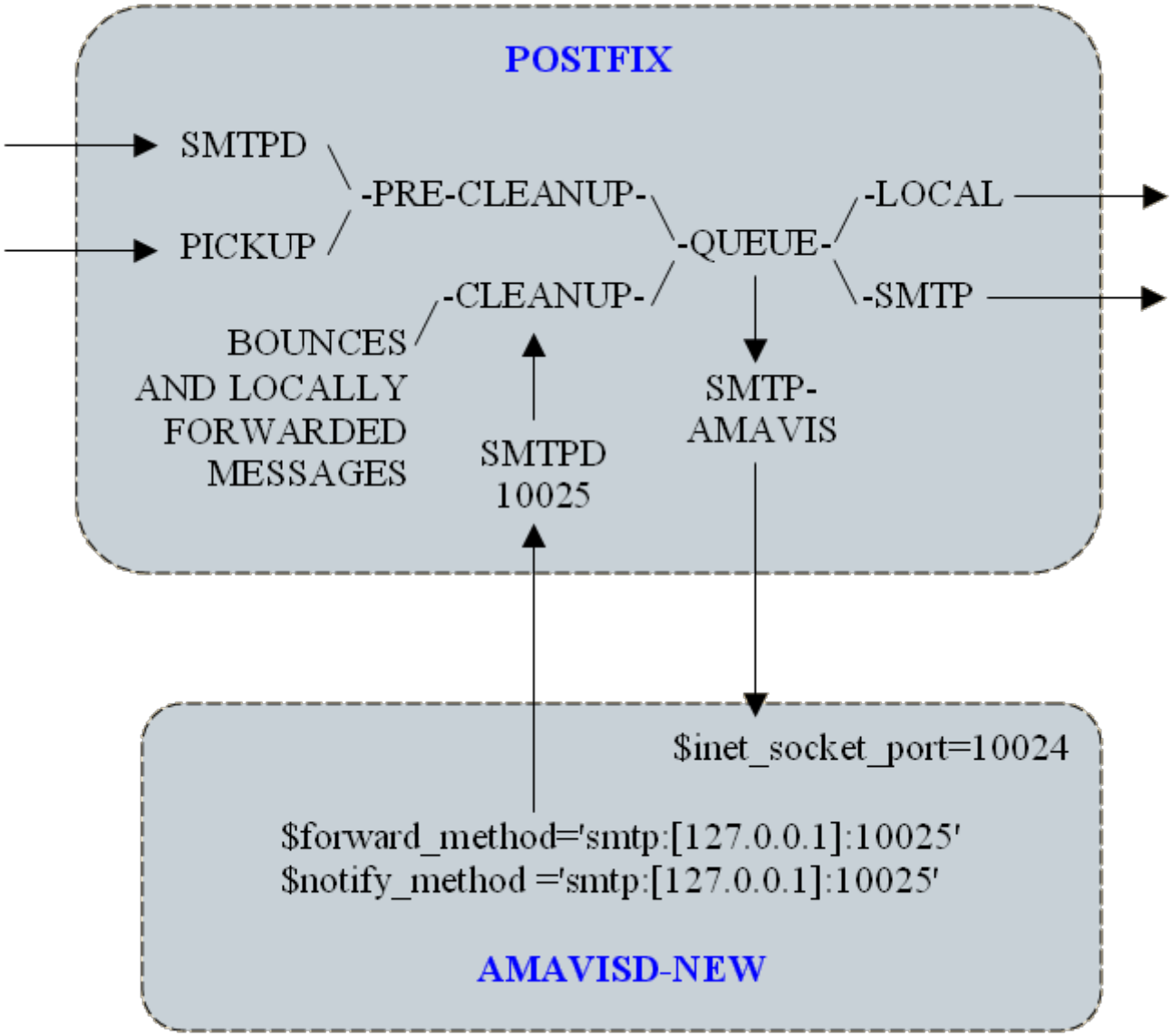



```
# make install clean
# rehash
```

Настраиваем запуск amavisd-new вместе с системой.

```
 # echo 'amavisd_enable="YES"' >> /etc/rc.conf
```

Ну а теперь осталось связать между собой эти четыре программы. Для лучшего понимания процесса я привожу условную схему работы данной связки



Итак начнем по порядку. Редактируем конфигурационный файл amavisd-new, а именно /usr/local/etc/amavisd.conf

```
# cat /usr/local/etc/amavisd.conf | grep -v ^# | grep -v ^$
use strict;
$max_servers = 2;           # num of pre-forked children (2..15 is common),
-m
$daemon_user  = 'vscan';    # (no default;  customary: vscan or amavis), -u
$daemon_group = 'vscan';    # (no default;  customary: vscan or amavis), -g
$mydomain = 'sys-adm.org.ua';   # a convenient default for other settings
$TEMPBASE = "$MYHOME/tmp";   # working directory, needs to exist, -T
$ENV{TMPDIR} = $TEMPBASE;    # environment variable TMPDIR, used by SA, etc.
$QUARANTINEDIR = '/var/virusmails';  # -Q
$log_level = 0;             # verbosity 0..5, -d
$log_recip_templ = undef;    # disable by-recipient level-0 log entries
$DO_SYSLOG = 1;             # log via syslogd (preferred)
$syslog_facility = 'mail';   # Syslog facility as a string
          # e.g.: mail, daemon, user, local0, ... local7
$syslog_priority = 'debug';  # Syslog base (minimal) priority as a string,
          # choose from: emerg, alert, crit, err, warning, notice, info,
```

```
debug
$enable_db = 1;              # enable use of BerkeleyDB/libdb (SNMP and
nanny)
$enable_global_cache = 1;    # enable use of libdb-based cache if
$enable_db=1
$nanny_details_level = 2;    # nanny verbosity: 1: traditional, 2: detailed
@local_domains_maps = ( [".$mydomain"] );  # list of all local domains
@mynetworks = qw( 127.0.0.0/8 [::1] [FE80::]/10 [FEC0::]/10
                  10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 );
               # option(s) -p overrides $inet_socket_port and
$unix_socketname
$inet_socket_port = 10024;   # listen on this local TCP port(s)
$policy_bank{'MYNETS'} = {   # mail originating from @mynetworks
  originating => 1,  # is true in MYNETS by default, but let's make it
explicit
  os_fingerprint_method => undef,  # don't query p0f for internal clients
};
$interface_policy{'10026'} = 'ORIGINATING';
$policy_bank{'ORIGINATING'} = {  # mail supposedly originating from our
users
  originating => 1,  # declare that mail was submitted by our smtp client
  allow_disclaimers => 1,  # enables disclaimer insertion if available
  # notify administrator of locally originating malware
  virus_admin_maps => ["virusalert\@$mydomain"],
  spam_admin_maps  => ["virusalert\@$mydomain"],
  warnbadhsender   => 1,
  # forward to a smtpd service providing DKIM signing service
  forward_method => 'smtp:[127.0.0.1]:10027',
  # force MTA conversion to 7-bit (e.g. before DKIM signing)
  smtpd_discard_ehlo_keywords => ['8BITMIME'],
  bypass_banned_checks_maps => [1],  # allow sending any file names and
types
  terminate_dsn_on_notify_success => 0,  # don't remove NOTIFY=SUCCESS
option
};
$interface_policy{'SOCK'} = 'AM.PDP-SOCK'; # only applies with
$unix_socketname
$policy_bank{'AM.PDP-SOCK'} = {
  protocol => 'AM.PDP',
  auth_required_release => 0,  # do not require secret_id for amavisd-
release
};
$sa_tag_level_deflt  = 2.0;  # add spam info headers if at, or above that
level
$sa_tag2_level_deflt = 6.2;  # add 'spam detected' headers at that level
$sa_kill_level_deflt = 6.9;  # triggers spam evasive actions (e.g. blocks
mail)
$sa_dsn_cutoff_level = 10;   # spam level beyond which a DSN is not sent
$penpals_bonus_score = 8;    # (no effect without a @storage_sql_dsn
database)
$penpals_threshold_high = $sa_kill_level_deflt;  # don't waste time on hi
```

```
spam
$sa_mail_body_size_limit = 400*1024; # don't waste time on SA if mail is
larger
$sa_local_tests_only = 0;    # only tests which do not require internet
access?
$virus_admin               = "virusalert\@$mydomain";  # notifications
recip.
$mailfrom_notify_admin     = "virusalert\@$mydomain";  # notifications
sender
$mailfrom_notify_recip     = "virusalert\@$mydomain";  # notifications
sender
$mailfrom_notify_spamadmin = "spam.police\@$mydomain"; # notifications
sender
$mailfrom_to_quarantine = ''; # null return path; uses original sender if
undef
@addr_extension_virus_maps      = ('virus');
@addr_extension_banned_maps     = ('banned');
@addr_extension_spam_maps       = ('spam');
@addr_extension_bad_header_maps = ('badh');
$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';
$MAXLEVELS = 14;
$MAXFILES = 1500;
$MIN_EXPANSION_QUOTA =      100*1024;  # bytes  (default undef, not
enforced)
$MAX_EXPANSION_QUOTA = 300*1024*1024;  # bytes  (default undef, not
enforced)
$sa_spam_subject_tag = '***SPAM*** ';
$defang_virus  = 1;  # MIME-wrap passed infected mail
$defang_banned = 1;  # MIME-wrap passed mail containing banned name
$defang_by_ccat{+CC_BADH.",3"} = 1;  # NUL or CR character in header
$defang_by_ccat{+CC_BADH.",5"} = 1;  # header line longer than 998
characters
$defang_by_ccat{+CC_BADH.",6"} = 1;  # header field syntax error
$myhostname = 'mail.sys-adm.org.ua';  # must be a fully-qualified domain
name!
$notify_method  = 'smtp:[127.0.0.1]:10025';
$forward_method = 'smtp:[127.0.0.1]:10025';  # set to undef with milter!
$final_virus_destiny      = D_DISCARD;
$final_banned_destiny     = D_BOUNCE;
$final_spam_destiny       = D_BOUNCE;
$final_bad_header_destiny = D_PASS;
@keep_decoded_original_maps = (new_RE(
  qr'^MAIL-UNDECIPHERABLE$', # recheck full mail if it contains
undecipherables
  qr'^(ASCII(?! cpio)|text|uuencoded|xxencoded|binhex)'i,
));
$banned_filename_re = new_RE(
  qr'^\.(exe-ms|dll)$',                  # banned file(1) types,
rudimentary
  [ qr'^\.(rpm|cpio|tar)$'       => 0 ],  # allow any in Unix-type archives
  qr'.\.(pif|scr)$'i,                    # banned extensions - rudimentary
```

```
  qr'^application/x-msdownload$'i,        # block these MIME types
  qr'^application/x-msdos-program$'i,
  qr'^application/hta$'i,
  # block certain double extensions in filenames
  qr'\.[^./]*[A-Za-
z][^./]*\.\s*(exe|vbs|pif|scr|bat|cmd|com|cpl|dll)[.\s]*$'i,
  qr'.\.(exe|vbs|pif|scr|cpl)$'i,             # banned extension - basic
);
@score_sender_maps = ({ # a by-recipient hash lookup table,
                        # results from all matching recipient tables are
summed
  ## site-wide opinions about senders (the '.' matches any recipient)
  '.' => [  # the _first_ matching sender determines the score boost
   new_RE(  # regexp-type lookup table, just happens to be all soft-
blacklist
    [qr'^(bulkmail|offers|cheapbenefits|earnmoney|foryou)@'i         =>
5.0],
    [qr'^(greatcasino|investments|lose_weight_today|market\.alert)@'i=>
5.0],
    [qr'^(money2you|MyGreenCard|new\.tld\.registry|opt-out|opt-in)@'i=>
5.0],
    [qr'^(optin|saveonlsmoking2002k|specialoffer|specialoffers)@'i   =>
5.0],
    [qr'^(stockalert|stopsnoring|wantsome|workathome|yesitsfree)@'i  =>
5.0],
    [qr'^(your_friend|greatoffers)@'i                                =>
5.0],
    [qr'^(inkjetplanet|marketopt|MakeMoney)\d*@'i                    =>
5.0],
   ),
   { # a hash-type lookup table (associative array)
     'nobody@cert.org'                       => -3.0,
     'cert-advisory@us-cert.gov'             => -3.0,
     'owner-alert@iss.net'                   => -3.0,
     'slashdot@slashdot.org'                 => -3.0,
     'securityfocus.com'                     => -3.0,
     'ntbugtraq@listserv.ntbugtraq.com'      => -3.0,
     'security-alerts@linuxsecurity.com'     => -3.0,
     'mailman-announce-admin@python.org'     => -3.0,
     'amavis-user-admin@lists.sourceforge.net'=> -3.0,
     'amavis-user-bounces@lists.sourceforge.net' => -3.0,
     'spamassassin.apache.org'               => -3.0,
     'notification-return@lists.sophos.com'  => -3.0,
     'owner-postfix-users@postfix.org'       => -3.0,
     'owner-postfix-announce@postfix.org'    => -3.0,
     'owner-sendmail-announce@lists.sendmail.org'   => -3.0,
     'sendmail-announce-request@lists.sendmail.org' => -3.0,
     'donotreply@sendmail.org'               => -3.0,
     'ca+envelope@sendmail.org'              => -3.0,
     'noreply@freshmeat.net'                 => -3.0,
     'owner-technews@postel.acm.org'         => -3.0,
```

```
    'ietf-123-owner@loki.ietf.org'          => -3.0,
    'cvs-commits-list-admin@gnome.org'      => -3.0,
    'rt-users-admin@lists.fsck.com'         => -3.0,
    'clp-request@comp.nus.edu.sg'           => -3.0,
    'surveys-errors@lists.nua.ie'           => -3.0,
    'emailnews@genomeweb.com'               => -5.0,
    'yahoo-dev-null@yahoo-inc.com'          => -3.0,
    'returns.groups.yahoo.com'              => -3.0,
    'clusternews@linuxnetworx.com'          => -3.0,
    lc('lvs-users-admin@LinuxVirtualServer.org')    => -3.0,
    lc('owner-textbreakingnews@CNNIMAIL12.CNN.COM') => -5.0,
    # soft-blacklisting (positive score)
    'sender@example.net'                    =>  3.0,
    '.example.net'                          =>  1.0,
  },
 ],  # end of site-wide tables
});
@decoders = (
 ['mail', \&do_mime_decode],
 ['asc',  \&do_ascii],
 ['uue',  \&do_ascii],
 ['hqx',  \&do_ascii],
 ['ync',  \&do_ascii],
 ['F',    \&do_uncompress, ['unfreeze','freeze -d','melt','fcat'] ],
 ['Z',    \&do_uncompress, ['uncompress','gzip -d','zcat'] ],
 ['gz',   \&do_uncompress,  'gzip -d'],
 ['gz',   \&do_gunzip],
 ['bz2',  \&do_uncompress,  'bzip2 -d'],
 ['lzo',  \&do_uncompress,  'lzop -d'],
 ['rpm',  \&do_uncompress, ['rpm2cpio.pl','rpm2cpio'] ],
 ['cpio', \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
 ['tar',  \&do_pax_cpio,   ['pax','gcpio','cpio'] ],
 ['deb',  \&do_ar,          'ar'],
 ['zip',  \&do_unzip],
 ['7z',   \&do_7zip,       ['7zr','7za','7z'] ],
 ['rar',  \&do_unrar,      ['rar','unrar'] ],
 ['arj',  \&do_unarj,      ['arj','unarj'] ],
 ['arc',  \&do_arc,        ['nomarch','arc'] ],
 ['zoo',  \&do_zoo,        ['zoo','unzoo'] ],
 ['lha',  \&do_lha,         'lha'],
 ['cab',  \&do_cabextract,  'cabextract'],
 ['tnef', \&do_tnef_ext,    'tnef'],
 ['tnef', \&do_tnef],
 ['exe',  \&do_executable, ['rar','unrar'], 'lha', ['arj','unarj'] ],
);
@av_scanners = (
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"],
   qr/\bOK$/, qr/\bFOUND$/,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ]
);
```

```
@av_scanners_backup = (
  ### http://www.clamav.net/   - backs up clamd or Mail::ClamAV
  ['ClamAV-clamscan', 'clamscan',
    "--stdout --no-summary -r --tempdir=$TEMPBASE {}",
    [0], qr/:.*\sFOUND$/, qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ]
);
1;  # insure a defined return
```

Запускаем amavisd

```
# /usr/local/etc/rc.d/amavisd start
Starting amavisd.
```

```
# cat /var/log/maillog | grep amavis
Mar 26 21:49:51 mail amavis[635]: starting.  /usr/local/sbin/amavisd at
mail.sys-adm.org.ua
amavisd-new-2.5.3 (20071212), Unicode aware
Mar 26 21:49:51 mail amavis[635]: Perl version              5.008008
Mar 26 21:49:53 mail amavis[638]: Module Amavis::Conf       2.093
Mar 26 21:49:53 mail amavis[638]: Module Archive::Zip       1.23
Mar 26 21:49:53 mail amavis[638]: Module BerkeleyDB         0.32
Mar 26 21:49:53 mail amavis[638]: Module Compress::Zlib     2.008
Mar 26 21:49:53 mail amavis[638]: Module Convert::TNEF      0.17
Mar 26 21:49:53 mail amavis[638]: Module Convert::UUlib     1.09
Mar 26 21:49:53 mail amavis[638]: Module DBD::mysql         4.006
Mar 26 21:49:53 mail amavis[638]: Module DBI                1.601
Mar 26 21:49:53 mail amavis[638]: Module DB_File            1.814
Mar 26 21:49:53 mail amavis[638]: Module Digest::MD5        2.36
Mar 26 21:49:53 mail amavis[638]: Module Digest::SHA1       2.11
Mar 26 21:49:53 mail amavis[638]: Module IO::Socket::INET6  2.52
Mar 26 21:49:53 mail amavis[638]: Module MIME::Entity       5.425
Mar 26 21:49:53 mail amavis[638]: Module MIME::Parser       5.425
Mar 26 21:49:53 mail amavis[638]: Module MIME::Tools        5.425
Mar 26 21:49:53 mail amavis[638]: Module Mail::Header       2.02
Mar 26 21:49:53 mail amavis[638]: Module Mail::Internet     2.02
Mar 26 21:49:53 mail amavis[638]: Module Mail::SPF          v2.005
Mar 26 21:49:53 mail amavis[638]: Module Mail::SpamAssassin  3.002004
Mar 26 21:49:53 mail amavis[638]: Module Net::DNS           0.63
Mar 26 21:49:53 mail amavis[638]: Module Net::Server        0.97
Mar 26 21:49:53 mail amavis[638]: Module NetAddr::IP        4.007
Mar 26 21:49:53 mail amavis[638]: Module Time::HiRes        1.9712
Mar 26 21:49:53 mail amavis[638]: Module URI                1.35
Mar 26 21:49:53 mail amavis[638]: Module Unix::Syslog       1.0
Mar 26 21:49:53 mail amavis[638]: Amavis::DB code      loaded
Mar 26 21:49:53 mail amavis[638]: Amavis::Cache code   loaded
Mar 26 21:49:53 mail amavis[638]: SQL base code        NOT loaded
Mar 26 21:49:53 mail amavis[638]: SQL::Log code        NOT loaded
Mar 26 21:49:53 mail amavis[638]: SQL::Quarantine      NOT loaded
Mar 26 21:49:53 mail amavis[638]: Lookup::SQL code     NOT loaded
Mar 26 21:49:53 mail amavis[638]: Lookup::LDAP code    NOT loaded
```

```
Mar 26 21:49:53 mail amavis[638]: AM.PDP-in proto code loaded
Mar 26 21:49:53 mail amavis[638]: SMTP-in proto code   loaded
Mar 26 21:49:53 mail amavis[638]: Courier proto code   NOT loaded
Mar 26 21:49:53 mail amavis[638]: SMTP-out proto code  loaded
Mar 26 21:49:53 mail amavis[638]: Pipe-out proto code  NOT loaded
Mar 26 21:49:53 mail amavis[638]: BSMTP-out proto code NOT loaded
Mar 26 21:49:53 mail amavis[638]: Local-out proto code loaded
Mar 26 21:49:53 mail amavis[638]: OS_Fingerprint code  NOT loaded
Mar 26 21:49:53 mail amavis[638]: ANTI-VIRUS code      loaded
Mar 26 21:49:53 mail amavis[638]: ANTI-SPAM code       loaded
Mar 26 21:49:53 mail amavis[638]: ANTI-SPAM-SA code    loaded
Mar 26 21:49:53 mail amavis[638]: Unpackers code       loaded
Mar 26 21:49:53 mail amavis[638]: Found $file            at
/usr/local/bin/file
Mar 26 21:49:53 mail amavis[638]: No $dspam,             not using it
Mar 26 21:49:53 mail amavis[638]: Found $altermime       at
/usr/local/bin/altermime
Mar 26 21:49:53 mail amavis[638]: Internal decoder for .mail
Mar 26 21:49:53 mail amavis[638]: Internal decoder for .asc
Mar 26 21:49:53 mail amavis[638]: Internal decoder for .uue
Mar 26 21:49:53 mail amavis[638]: Internal decoder for .hqx
Mar 26 21:49:53 mail amavis[638]: Internal decoder for .ync
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .F    at
/usr/local/bin/unfreeze
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .Z    at
/usr/bin/uncompress
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .gz   at
/usr/bin/gzip -d
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .bz2  at
/usr/bin/bzip2 -d
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .lzo  at
/usr/local/bin/lzop -d
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .rpm  at
/usr/local/bin/rpm2cpio.pl
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .cpio at /bin/pax
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .tar  at /bin/pax
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .deb  at /usr/bin/ar
Mar 26 21:49:53 mail amavis[638]: Internal decoder for .zip
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .7z   at
/usr/local/bin/7zr
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .rar  at
/usr/local/bin/rar
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .arj  at
/usr/local/bin/arj
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .arc  at
/usr/local/bin/arc
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .zoo  at
/usr/local/bin/zoo
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .lha  at
/usr/local/bin/lha
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .cab  at
```

```
/usr/local/bin/cabextract
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .tnef at
/usr/local/bin/tnef
Mar 26 21:49:53 mail amavis[638]: Found decoder for    .exe  at
/usr/local/bin/rar;
/usr/local/bin/lha; /usr/local/bin/arj
Mar 26 21:49:53 mail amavis[638]: Using primary internal av scanner code for
ClamAV-clamd
Mar 26 21:49:53 mail amavis[638]: Found secondary av scanner ClamAV-clamscan
at /usr/local/bin/clamscan
Mar 26 21:49:54 mail amavis[638]: Creating db in /var/amavis/db/; BerkeleyDB
0.32, libdb 4.1
```

Проверяем работоспособность amavisd-new.

```
# telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
quit
221 2.0.0 [127.0.0.1] amavisd-new closing transmission channel
Connection closed by foreign host.
```

Теперь внесем изменения в файл master.cf. В самый конец добавим следующие строчки

```
smtp-amavis unix - - n - 2 smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20

127.0.0.1:10025 inet n - n - - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks_style=host
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
```

```
    -o smtpd_client_connection_rate_limit=0
    -o
receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Перезапускаем postfix. И снова проверяем amavisd

```
# /usr/local/etc/rc.d/postfix restart
postfix/postfix-script: stopping the Postfix mail system
postfix/postfix-script: starting the Postfix mail system

# telnet localhost 10025
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.sys-adm.org.ua ESMTP Postfix
quit
221 2.0.0 Bye
Connection closed by foreign host.

# telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
mail from:<alex@sys-adm.org.ua>
250 2.1.0 Sender <alex@sys-adm.org.ua> OK
rcpt to:<quota@sys-adm.org.ua>
250 2.1.5 Recipient <quota@sys-adm.org.ua< OK
Data
354 End data with .
Subject: Test1 - Clean message
Hello world
.
250 2.0.0 Ok: queued as E66F743
mail from:
250 2.1.0 Sender  OK
rcpt to:
250 2.1.5 Recipient  OK
data
354 End data with <CR><LF>.<CR><LF>
Subject: Test 2 - Virus test pattern

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
.
250 2.7.0 Ok, discarded, id=00950-02 - VIRUS: Eicar-Test-Signature
quit
221 2.0.0 [127.0.0.1] amavisd-new closing transmission channel
Connection closed by foreign host.
```

Как видно из сообщения **- discarded, id=00950-02 - VIRUS: Eicar-Test-Signature** , вирус он нашел. Теперь необходимо указать postfix, чтобы он все письма для проверки передавал amavisd, для этого необходимо добавить следующую строку в main.cf

```
content_filter=smtp-amavis:[127.0.0.1]:10024
```

Перезапускаем postfix и проверяем работу spamassassin

```
# /usr/local/etc/rc.d/postfix restart
postfix/postfix-script: stopping the Postfix mail system
postfix/postfix-script: starting the Postfix mail system
```

```
# telnet 192.168.127.1 25
Trying 192.168.127.1...
Connected to 192.168.127.1.
Escape character is '^]'.
220 mail.sys-adm.org.ua ESMTP Postfix
helo sysadm
250 mail.sys-adm.org.ua
mail from:<alex@sys-adm.org.ua>
250 2.1.0 Ok
rcpt to:<alex@sys-adm.org.ua>
250 2.1.5 Ok
Data
354 End data with <CR><LF>.<CR><LF>
Subject: Test 3 - Spam test pattern
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
.
250 2.0.0 Ok: queued as 12D6E42
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Смотрим логи

```
# cat /var/log/maillog | grep 12D6E42
Mar 28 08:53:17 mail postfix/smtpd[1063]: 12D6E42: client=mail.sys-
adm.local[192.168.127.1]
Mar 28 08:53:35 mail postfix/cleanup[1067]: 12D6E42: message-
id=<20080328065317.12D6E42@mail.sys-adm.org.ua>
Mar 28 08:53:35 mail postfix/qmgr[1022]: 12D6E42: from=<alex@sys-
adm.org.ua>, size=439, nrcpt=1 (queue active)
Mar 28 08:53:36 mail amavis[1058]: (01058-01) Blocked SPAM, MYNETS LOCAL
[192.168.127.1] [192.168.127.1] <alex@sys-adm.org.ua> -> <alex@sys-
adm.org.ua>, quarantine: spam-Uv8HK00ILpsc.gz, Message-ID:
<20080328065317.12D6E42@mail.sys-adm.org.ua>, mail_id: Uv8HK00ILpsc, Hits:
999.527, size: 439, 1315 ms
Mar 28 08:53:36 mail postfix/smtp[1069]: 12D6E42: to=<alex@sys-adm.org.ua>,
relay=127.0.0.1[127.0.0.1]:10024, delay=26, delays=25/0.07/0.07/1.3,
```

```
dsn=2.5.0, status=sent (250 2.5.0 Ok, id=01058-01,
DISCARD(bounce.suppressed))
Mar 28 08:53:36 mail postfix/qmgr[1022]: 12D6E42: removed
```

Из логов видно, что письмо распознано как спам - Blocked SPAM и сохраненно в **/var/virusmails/spam-Uv8HK00ILpsc.gz**

Давайте посмотрим на это письмо

```
# cd /var/virusmails/
# gunzip spam-Uv8HK00ILpsc.gz
# cat spam-Uv8HK00ILpsc
Return-Path: <>
Delivered-To: spam-quarantine
X-Envelope-From: <alex@sys-adm.org.ua>
X-Envelope-To: <alex@sys-adm.org.ua>
X-Quarantine-ID: <Uv8HK00ILpsc>
X-Spam-Flag: YES
X-Spam-Score: 999.527
X-Spam-Level:
************************************************************
X-Spam-Status: Yes, score=999.527 tag=2 tag2=6.2 kill=6.9
        tests=[ALL_TRUSTED=-1.44, AWL=0.967, GTUBE=1000]
Received: from mail.sys-adm.org.ua ([127.0.0.1])
        by localhost (mail.sys-adm.org.ua [127.0.0.1]) (amavisd-new, port
10024)
        with ESMTP id Uv8HK00ILpsc for <alex@sys-adm.org.ua>;
        Fri, 28 Mar 2008 08:53:35 +0200 (EET)
Received: from sysadm (mail.sys-adm.local [192.168.127.1])
        by mail.sys-adm.org.ua (Postfix) with SMTP id 12D6E42
        for <alex@sys-adm.org.ua>; Fri, 28 Mar 2008 08:53:10 +0200 (EET)
Subject: Test 3 - Spam test pattern
Message-Id: <20080328065317.12D6E42@mail.sys-adm.org.ua>
Date: Fri, 28 Mar 2008 08:53:10 +0200 (EET)
From: alex@sys-adm.org.ua
To: undisclosed-recipients:;

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

P.S. В третьей части я расмотрю настройку SSL/TLS и web интерфейса horde + imp To be continued …