Postfix

Ce tutoriel développe la mise en place d'un serveur de messagerie Postfix avec l'antivirus Clamav et Spamassassin.

Installation des packages

Mandrake	debian
postfix-2.1.4-2mdk libpostfix1-2.1.4-2mdk amavisd-new-2.1.2-1mdk clamav-0.81-0.2.101mdk libclamav1-0.81-0.2.101mdk clamav-db-0.81-0.2.101mdk spamassassin-3.0.0-1mdk perl-Mail-SpamAssassin-3.0.0-1mdk courier-imap-3.0.8-1mdk.i586.rpm courier-imap-pop-3.0.8-1mdk.i586.rpm courier-imap-utils-3.0.8-1mdk.i586.rpm unarj-2.65-1plf.i586.rpm unrar-3.40-1plf.i586.rpm zoo-2.10-2plf.i586.rpm	postfix_2.1.5-9_i386.deb amavisd-new_20030616p10-5_all.deb clamav_0.83-5_i386.deb clamav-base_0.83-5_all.deb clamav-daemon_0.83-5_i386.deb clamav-freshclam_0.83-5_i386.deb libclamav1_0.83-5_i386.deb spamassassin_3.0.2-1_all.deb spamc_3.0.2-1_i386.deb courier-authdaemon_0.47-4_i386.deb courier-base_0.47-4_i386.deb courier-imap _3.0.8-4_i386.deb courier-imap-ssl_3.0.8-4_i386.deb courier-ssl _0.47-4_i386.deb courier-pop_0.47-4_i386.deb courier-pop-ssl_0.47-4_i386.deb libfam0c102_2.7.0-6_i386.deb unarj_3.10.21-2_i386.deb unzoo_4.4-2_i386.deb unrar_0.0.1-1_i386.deb

Configuration de Postfix

Éditez le fichier **/etc/postfix/main.cf** :

```
# These are only the parameters changed from a default install see
# /etc/postfix/main.cf.dist for a commented, fuller version of this file.

# These are changed by postfix install script
readme_directory = /usr/share/doc/postfix-2.1.1/README_FILES
sample_directory = /usr/share/doc/postfix-2.1.1/samples
html_directory = /usr/share/doc/postfix-2.1.1/html
sendmail_path = /usr/sbin/sendmail.postfix
setgid_group = postdrop
command_directory = /usr/sbin
manpage_directory = /usr/share/man
daemon_directory = /usr/lib/postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
queue_directory = /var/spool/postfix
mail_owner = postfix

# User configurable parameters

myhostname = srv3.dmz.alex.fr
mydomain = alex.fr
# Pour obtenir une adresse sous la forme : "user@$mydomain"
myorigin = $mydomain
# Indique sur quelles interfaces Postfix écoutera.
inet_interfaces = $myhostname,localhost
# Indique pour quels domaines Postfix délivrera le courrier.
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
# Pour quels réseaux Postfix accepte de relayer les connexions des
# utilisateurs. Écrase l'option "mynetworks_style = subnet".
mynetworks = 127.0.0.0/8, 192.168.0.0/24
# Refuse de relayer les mails d'autres serveurs.
relay_domains =
# Délivre directement vers Internet.
relayhost =
# Vous pouvez spécifier votre IP public en cas de NAT/proxy.
#proxy_interfaces = 123.123.123.1
# biff, est un service de notification UNIX pour les utilisateurs "new mail"
biff = no
smtpd_banner = $myhostname ESMTP $mail_name (Mandrake Linux)
unknown_local_recipient_reject_code = 450
smtp-filter_destination_concurrency_limit = 2
lmtp-filter_destination_concurrency_limit = 2
smtpd_sasl_path = /etc/postfix/sasl:/usr/lib/sasl2
alias_maps = hash:/etc/postfix/aliases
alias_database = hash:/etc/postfix/aliases
virtual_maps = hash:/etc/postfix/virtual
canonical_maps = hash:/etc/postfix/canonical
# Indique que nous utilisons un format Maildir (IMAP/POP).
home_mailbox = Maildir/
# Option à utiliser avec des filtres externes.
receive_override_options = no_address_mappings
# Nous utilisons les filtres d'Amavis.
content_filter = lmtp-filter:127.0.0.1:10025
```

debian

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete
version

smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
myhostname = srv3.dmz.alex.fr
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, localhost.$mydomain, $mydomain
relay_domains =
relayhost =
mynetworks = 127.0.0.0/8, 192.168.0.0/24
#mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = $myhostname,localhost
mydomain = alex.fr
home_mailbox = Maildir/
content_filter = smtp-amavis:[127.0.0.1]:10024
```

Modifiez le fichier **/etc/aliases** pour rediriger les mails de root vers un compte utilisateur de votre choix :

```
...
root:          arnofear
...
```

Mandrake

Puis lancez cette commande :

```
[root@srv3 user]# newaliases
```

Pour récrire votre nom de domaine à l'expédition vous pouvez éditez le fichier **/etc/canonical**
Ajoutez cette ligne (votre domaine)

```
...
#@domaine_origine @domaine_sortant
#@alex.fr @alex-mail.org
#
@alex.fr @alex.fr
```

Puis lancez cette commande :

```
[root@srv3 user]# postmap /etc/postfix/canonical
```

Vérifiez en bas du fichier **/etc/postfix/master.cf** :

Mandrake

```
...

127.0.0.1:10026 inet n - y - - smtpd
  -o content_filter=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o mynetworks_style=host
  -o strict_rfc821_envelopes=yes
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
  -o smtpd_client_connection_limit_exceptions=127.0.0.0/8

lmtp-filter unix - - y - - lmtp
  -o lmtp_data_done_timeout=1200
  -o disable_dns_lookups=yes

smtp-filter unix - - y - - smtp
  -o smtp_data_done_timeout=1200
  -o disable_dns_lookups=yes

##### END OF CONTENT FILTER CUSTOMIZATIONS #####
```

Ajoutez en bas du fichier **/etc/postfix/master.cf** :

debian

```
...

# Mettez bien deux espaces devant -o pour ne pas avoir d'erreurs de
syntaxe.
smtp-amavis unix - - n - 2 smtp
  -o smtp_data_done_timeout=1200
  -o disable_dns_lookups=yes

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_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -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

##### END OF CONTENT FILTER CUSTOMIZATIONS #####
```

Configuration de Amavis

Modifiez certaines variables du fichier :

Mandrake

/etc/amavisd/amavisd.conf

```
use strict;

# a minimalistic configuration file for amavisd-new with all necessary settings
#
#   (see amavisd.conf-default for a list of all variables with their defaults)
#   (see amavisd.conf-sample for a traditional-style commented file)


# COMMONLY ADJUSTED SETTINGS:

# Laissez commenté les 2 lignes suivantes pour activer l'antivirus et spam.
# @bypass_virus_checks_maps = (1); # uncomment to DISABLE anti-virus code
# @bypass_spam_checks_maps  = (1); # uncomment to DISABLE anti-spam code

$max_servers = 2; # number of pre-forked children (2..15 is common)
$daemon_user  = 'amavis'; # (no default;  customary: vscan or amavis)
$daemon_group = 'amavis'; # (no default;  customary: vscan or amavis)

$mydomain = 'alex.fr'; # a convenient default for other settings

$MYHOME   = '/var/lib/amavis'; # a convenient default for other settings
#$TEMPBASE = "$MYHOME"; # working directory, needs to be created manually
$TEMPBASE = "$MYHOME/tmp"; # working directory, needs to be created manually
$ENV{TMPDIR} = $TEMPBASE; # environment variable TMPDIR
# Déactive la quarantaine pour les virus, suppression direct.
##$QUARANTINEDIR = '/var/spool/amavis/virusmails';
$QUARANTINEDIR = undef;

# $daemon_chroot_dir = $MYHOME;   # chroot directory or undef

# $db_home   = "$MYHOME/db";
# $helpers_home = "$MYHOME/var"; # prefer $MYHOME clean and owned by root
# $pid_file  = "$MYHOME/var/amavisd.pid";
# $lock_file = "$MYHOME/var/amavisd.lock";
#NOTE: create directories $MYHOME/tmp, $MYHOME/var, $MYHOME/db manually

@local_domains_maps = ( [".$mydomain"] );
# @mynetworks = qw( 127.0.0.0/8 ::1 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 );

$log_level = 2;              # verbosity 0..5
$log_recip_templ = undef;    # disable by-recipient level-0 log entries
$DO_SYSLOG = 1;              # log via syslogd (preferred)
$SYSLOG_LEVEL = 'mail.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

$inet_socket_port = 10025; # listen on this local TCP port(s)
# $unix_socketname = "$MYHOME/amavisd.sock";  # when using sendmail
milter

$sa_tag_level_deflt  = 3.0; # Ajoute une info spam à partir de ce niveau.
$sa_tag2_level_deflt = 4.9; # Ajoute 'spam detected' dans les entêtes.
$sa_kill_level_deflt = 4.9; # triggers spam evasive actions
$sa_dsn_cutoff_level = 10;   # spam level beyond which a DSN is not sent

$sa_mail_body_size_limit = 200*1024; # don't waste time on SA if mail is
larger
$sa_local_tests_only = 0; # only tests which do not require internet
access?
$sa_auto_whitelist = 1; # turn on AWL in SA 2.63 or older (irrelevant
# for SA 3.0, cf option is 'use_auto_whitelist')

# @lookup_sql_dsn =
#   ( ['DBI:mysql:database=mail;host=127.0.0.1;port=3306', 'user1',
'passwd1'],
#     ['DBI:mysql:database=mail;host=host2', 'username2', 'password2'] );

# Pour ne pas être notifié par mail de la réception d'un virus ou spam.
##$virus_admin = "virusalert\@$mydomain";  # notifications recip.
$virus_admin = undef;

##$mailfrom_notify_admin     = "virusalert\@$mydomain";  # notifications
sender
$mailfrom_notify_admin = undef;
##$mailfrom_notify_recip     = "virusalert\@$mydomain";  # notifications
sender
$mailfrom_notify_recip = undef;
##$mailfrom_notify_spamadmin = "spam.police\@$mydomain"; # notifications
sender
$mailfrom_notify_spamadmin = undef;

$mailfrom_to_quarantine = ''; # null return path; uses original sender if
undef

@addr_extension_virus_maps      = ('virus');
@addr_extension_spam_maps       = ('spam');
@addr_extension_banned_maps     = ('banned');
@addr_extension_bad_header_maps = ('badh');
```

```
$path = '/usr/local/sbin:/usr/local/bin:/usr/sbin:/sbin:/usr/bin:/bin';
$file   = 'file';   # file(1) utility; use recent versions
$gzip   = 'gzip';
$bzip2  = 'bzip2';
$lzop   = 'lzop';
$rpm2cpio   = ['rpm2cpio.pl','rpm2cpio'];
$cabextract = 'cabextract';
$uncompress = ['uncompress', 'gzip -d', 'zcat'];
$unfreeze   = ['unfreeze', 'freeze -d', 'melt', 'fcat'];
$arc        = ['nomarch', 'arc'];
$unarj      = ['arj', 'unarj'];
$unrar      = ['rar', 'unrar'];
$zoo    = 'zoo';
$lha    = 'lha';
$cpio   = ['gcpio','cpio'];
$dspam  = 'dspam';

$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


# OTHER MORE COMMON SETTINGS (defaults may suffice):

 $myhostname = 'srv3.dmz.alex.fr';  # must be a fully-qualified domain
name!

 $notify_method  = 'smtp:[127.0.0.1]:10026';
 $forward_method = 'smtp:[127.0.0.1]:10026';  # set to undef with milter!

# $final_virus_destiny      = D_DISCARD;
# $final_banned_destiny     = D_BOUNCE;
# $final_spam_destiny       = D_PASS;
# $final_bad_header_destiny = D_PASS;


# SOME OTHER VARIABLES WORTH CONSIDERING (see amavisd.conf-default for
all)

...
```

Modifiez certaines parties du fichier :

/etc/amavis/amavisd.conf

```
#
# Section I - Essential daemon and MTA settings
#

# $mydomain serves as a quick default for some other configuration settings.
# More refined control is available with each individual setting further down.
# $mydomain is never used directly by the program.
$mydomain = 'alex.fr';

$myhostname = 'srv3.dmz.alex.fr';

# POSTFIX, or SENDMAIL in dual-MTA setup, or EXIM V4
# (set host and port number as required; host can be specified
# as IP address or DNS name (A or CNAME, but MX is ignored)
$forward_method = 'smtp:127.0.0.1:10025';
$notify_method = $forward_method;

# Here is a QUICK WAY to completely DISABLE some sections of code
# that WE DO NOT WANT (it won't even be compiled-in).
# For more refined controls leave the following two lines commented out,
# and see further down what these two lookup lists really mean.
# Laissez commenté les 2 lignes suivantes pour activer l'antivirus et spam.
# @bypass_virus_checks_acl = qw( . ); # uncomment to DISABLE anti-virus
# @bypass_spam_checks_acl  = qw( . ); # uncomment to DISABLE anti-spam
#
# Any setting can be changed with a new assignment, so make sure
# you do not unintentionally override these settings further down!

#
# With Postfix (2.0) a quick reminder on what local domains normally are:
# a union of domains specified in: $mydestination, $virtual_alias_domains,
# $virtual_mailbox_domains, and $relay_domains.
#
#@local_domains_acl = ( ".$mydomain" );  # $mydomain and its subdomains
#@local_domains_acl = qw();
@local_domains_acl = qw(.);
# @local_domains_acl = qw( .example.com );
# @local_domains_acl = qw( .example.com !host.sub.example.net .sub.example.net );
# @local_domains_acl = ( ".$mydomain", '.example.com', 'sub.example.net' );
```

```
#
# Section III - Logging
#

#NOTE: levels are not strictly observed and are somewhat arbitrary
# 0: startup/exit/failure messages, viruses detected
# 1: args passed from client, some more interesting messages
# 2: virus scanner output, timing
# 3: server, client
# 4: decompose parts
# 5: more debug details
$log_level = 2; # (defaults to 0)

#
# Section IV - Notifications/DSN, BOUNCE/REJECT/DROP/PASS destiny,
quarantine
#

# Pour ne pas être notifié par mail de la réception d'un virus.
# $virus_admin = "postmaster\@$mydomain";
$virus_admin = undef; # do not send virus admin notifications (default)

# Pour ne pas être notifié par mail de la réception d'un spam.
# $spam_admin = "postmaster\@$mydomain";
$spam_admin = undef; # do not send spam admin notifications (default)

# Location to put infected mail into: (applies to 'local:' quarantine
method)
#   empty for not quarantining, may be a file (mailbox),
#   or a directory (no trailing slash)
#   (the default value is undef, meaning no quarantine)
#
# Déactive la quarantaine pour les virus, suppression direct.
$QUARANTINEDIR = undef;

# similar for spam
# (the default value is undef, meaning no quarantine)
# Déactive la quarantaine pour le spam, suppression direct.
#$spam_quarantine_to = 'spam-quarantine';
$spam_quarantine_to = undef; # no quarantine

# Add X-Virus-Scanned header field to mail?
$X_HEADER_TAG = 'X-Virus-Scanned'; # (default: undef)
# Leave empty to add no header field   # (default: undef)
$X_HEADER_LINE = "by amavisd-new at $mydomain";

#
# Section VI - Resource limits
#

# default values, can be overridden by more specific lookups, e.g. SQL
$sa_tag_level_deflt  = 3.0; # Ajoute une info spam à partir de ce niveau.
$sa_tag2_level_deflt = 5.0; # Ajoute 'spam detected' dans les entêtes.
$sa_kill_level_deflt = $sa_tag2_level_deflt;
```

Configuration de Clamav

Adaptez les fichiers suivants (bon par défaut) voir tutoriel Exim4 :

Mandrake	debian
/etc/clamd.conf et **/etc/freshclam.conf**	**/etc/clamav/clamd.conf** et **/etc/clamav/freshclam.conf**

Configuration de Spamassassin

debian
Modifiez le fichier **/etc/default/spamassassin** :

```
# /etc/default/spamassassin
# WARNING read README.spamd before using. THERE ARE SECURITY RISKS!
# Mettre à 1 pour activer spamd au démarrage du serveur.
ENABLED=1

# Options
# See man spamd for possible options. The -d option is automatically
added.
OPTIONS="--create-prefs --max-children 5 –helper-home-dir"
PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"
```

Ajoutez les options suivantes dans le fichier :

Mandrake	debian
/etc/mail/spamassassin/local.cf	**/etc/spamassassin/local.cf**

```
...

# Indique dans quelles langues nous recevons des mails.
# Les autres langues auront un malus.
ok_languages fr en
# Expéditeurs considérés comme surs.
whitelist_from *@srv3.dmz.alex.fr *@alex.fr

# Adresses considérées comme du spam (ou à refuser :)
blacklist_from *@microsoft.com
```

Pour un bon fonctionnement de l'apprentissage de Spamassassin vous devez lui montrer autant de mails non spammés que de mails non détectés comme du spam.
Dans votre client de messagerie créez un dossier spam ou vous déplacerez les mails spammés non détecté et un dossier bon pour les mails non spammés.
Dans ces dossiers faites ensuite pour chaque mails :
Fichier > Enregistrer sous > message.eml
Copiez les sur le serveur Postfix, et a l'aide de la commande "sa-learn" apprenez la reconnaissance des bons et mauvais mails à Spamassassin :

```
srv3:/home/user# sa-learn --spam /repertoire/mails-spam/*
srv3:/home/user# sa-learn --ham /repertoire/mails-bon/*
```

Configuration de courier-imap et courier-pop

Éditez le fichier **/etc/courier/authdaemonrc** :

```
authmodulelist="authpam"

authmodulelistorig="authcustom authcram authuserdb authldap authpgsql
authmysql authpam"

daemons=5

...
```

Pour activer ou déactiver les différents deamons, éditez les fichiers **/etc/courier/** (**imapd, imapd-ssl, pop3d, pop3d-ssl**) et changez respectivement la valeur YES ou NO des variables : (IMAPDSTART, IMAPDSSLSTART, POP3DSTART, POP3DSSLSTART)

Configuration de /etc/resolv.conf

Dans l'exemple d'implantation, la résolution des noms de domaine vers internet, utilise un serveur DNS cache sur le serveur Postfix. Ce serveur DNS cache n'aura pas de relations directe avec les deux autres serveurs DNS dédiés à la résolution des noms des machines de votre réseau local et ne sera pas informé, ni mit à jour par eux.

```
# N'indiquez pas les adresses de vos serveurs DNS si vous avez
# installé un serveur DNS cache sur le serveur Postfix.
nameserver 127.0.0.1
```

Source : http://www.fatofthelan.com/articles/articles.php?pid=22

Document mis à jour : 03/05/05