Héberger ses mails

Ce petit guide est destiné aux jeunes fruités qui ne désirent plus être dépendants des services privateurs des géants du net. Par convention, votre serveur mail s'appellera **mail.domaine.tld** Vous aurez au final:

- la clique postfix / dovecot / rspamd pour gérer le flux des messages
- modoboa pour gérer les comptes
- nginx et uwsgi pour vous servir modoboa et rspamd
- ainsi que pleins de truc cools (sieve, antispam, messages d'absence, calendrier, etc.)

0. Prérequis

1. Savoir se connecter via ssh
2. Savoir utiliser un éditeur de texte
3. Comprendre les bases de l'envoi de messages électroniques par un serveur dédié
4. Savoir créer les enregistrements DNS qui vont bien: SPF, DKIM, PTR, TLSA, etc.
5. Savoir générer un certificat TLS qui tient la route
6. Savoir créer une base Mysql
7. Savoir gérer un pare-feu
8. Et utiliser sudo…

Important: ce guide n'est valide que pour architectures x86 et x86_64 (amd64) puisque rspamd dépend de libluajit qui ne compile correctement sur arm64 qu'avec au minima la version 2.1 et comme Debian Stretch (la version utilisée) n'inclut que la version 2.0, vous en tirerez les conséquences qui s'imposent.

Sources des logiciels:

- Debian Stretch
- Rspamd 1.6.x
- Modoboa 1.9.x

1. La base de travail

On créé un utilisateur vmail qui va se charger de stocker les messages:

```
groupadd -g 5000 vmail
useradd -u 5000 -g vmail -s /usr/bin/nologin -d /home/mail -m vmail
```

On installe les paquets pour postfix:

```
apt install postfix postfix-mysql postfix-pcre
```

puis dovecot:

```
apt install dovecot-imapd dovecot-lmtpd dovecot-managesieved dovecot-mysql
dovecot-pop3d dovecot-sieve
```

puis mariadb:

```
apt install mariadb-server
```

puis nginx et uwsgi:

```
apt install nginx-full uwsgi-python
```

puis redis-server:

```
apt install redis-server
```

puis clamav:

```
apt install clamav clamav-daemon
```

puis rspamd selon les instructions des développeurs car la version de rspamd est trop ancienne dans les dépôts Debian (une vague histoire de javacripts *minifiés* qui ne plaît pas au mainteneur Debian).

et enfin pour modoboa:

```
apt install python-virtualenv python-pip build-essential python-dev libxml2-
dev libxslt-dev libjpeg-dev librrd-dev rrdtool libffi-dev libssl-dev
```

De façon optionnelle: gpg Fix Me!

2. Installation et configuration de modoboa

2.1. Installation de modoboa via pip

C'est du python et donc il faut mieux travailler dans un *virtual-env* pour ne pas tomber dans le piège des dépendances. Avec votre utilisateur non privilégié il faut passer dans un environnement virtuel pour installer modoboa:

```
virtualenv env
source env/bin/activate
pip install -U pip
pip install modoboa
pip install mysqlclient
```

2.2. Déploiement de modoboa

Ensuite il faut déployer une instance (référez-vous à la documentation pour plus d'explications sur les

modules mais amavis pue des fesses):

```
modoboa-admin.py deploy <instance> --collectstatic --domain mail.domaine.tld
--dburl default:mysql://USER:PWD@localhost:3306/DB --extensions modoboa-
dmarc modoboa-imap-migration modoboa-pdfcredentials modoboa-pfxadmin-migrate
modoboa-postfix-autoreply modoboa-radicale modoboa-sievefilters modoboa-
stats modoboa-webmail
```

pour de belles statistiques (utilisateur privilégié au besoin):

```
mkdir <dossier>/modoboa
```

où ce chemin sera renseigné dans l'interface de modoboa.

on n'oublie pas les fichiers nécessaires à postfix via le *virtual-env*:

```
python manage.py generate_postfix_maps --destdir <dossier>
```

Ces fichiers devront être placés dans un sous-dossier du dossier /etc/postfix pour plus de logique. Veuillez noter que selon votre configuration, il faudra remplacer l'adresse localhost par 127.0.0.1 pour éviter quelques soucis.

2.3. Crontab pour modoboa

Le fichier à éditer dans /etc/cron.d/modoboa :

```
#
# Modoboa specific cron jobs
#
PYTHON=/chemin/vers/env/bin/python
INSTANCE=/chemin/vers/instance
# Operations on mailboxes
*       *       *       *       *       vmail   $PYTHON $INSTANCE/manage.py
handle_mailbox_operations 2>&1
# Sessions table cleanup
0       0       *       *       *       root    $PYTHON $INSTANCE/manage.py
clearsessions
# Logs table cleanup
0       0       *       *       *       root    $PYTHON $INSTANCE/manage.py
cleanlogs
# Logs parsing
*/5     *       *       *       *       root    $PYTHON $INSTANCE/manage.py
logparser &> /dev/null
# DNSBL checks
*/30    *       *       *       *       root    $PYTHON $INSTANCE/manage.py
modo check_mx
# Public API communication
0       *       *       *       *       root    $PYTHON $INSTANCE/manage.py
communicate_with_public_api
```

```
# Statistics update
0   *    *    *    *    root    $PYTHON $INSTANCE/manage.py
update_statistics
# Generation of radicale file (from_file) rights
*/2 *    *    *    *    root    $PYTHON $INSTANCE/manage.py generate_rights
--force
```

Tout n'est pas forcément nécessaire et notamment la dernière ligne.

Par défaut l'interface de configuration de modoboa s'accède via le couple admin/password

3. Postfix

3.1. main.cf

Pour postfix c'est assez simple, le main.cf (avec une mise en forme qui plairait à hardware):

```
########################
## GENERALS SETTINGS ##
########################

smtpd_banner         = $myhostname ESMTP $mail_name
compatibility_level  = 2
biff                 = no
append_at_myorigin   = yes
append_dot_mydomain  = yes
# was "no" for mydomain (base setup)
readme_directory     = no
allow_percent_hack   = no
delay_warning_time   = 4h
mailbox_command      = procmail -a "$EXTENSION"
recipient_delimiter  = +
disable_vrfy_command = yes
message_size_limit   = 16000000
#mailbox_size_limit   = 1024000000

inet_interfaces = all
inet_protocols = all

myhostname    = mail.domain.tld
mydomain      = domain.tld
myorigin      = /etc/mailname
#mydestination = localhost localhost.$mydomain
mydestination =
mynetworks    = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128

alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

```
# Tuning
local_destination_concurrency_limit = 20
smtp_host_lookup = native

###############
## SMTP/UTF8 ##
###############

smtputf8_enable = yes

# The default is to enable "SMTPUTF8 required" autodetection
# only for Postfix sendmail command-line submissions and address
# verification probes.
# https://github.com/hardware/mailserver/issues/166
# smtputf8_autodetect_classes = all

###################
## RATE LIMITING ##
###################

# Allow to avoid 421 error when send bulk mail
default_destination_rate_delay = 1s
default_destination_recipient_limit = 10

# concurrency_limit has no effect when rate_delay is turned on.
# It specifies a delay BETWEEN deliveries, meaning the deliveries
# cannot be in parallel.
# default_destination_concurrency_limit=2

####################
## TLS PARAMETERS ##
####################

# Smtp ( OUTGOING )
smtp_tls_loglevel            = 1
smtp_tls_security_level      = dane
smtp_dns_support_level       = dnssec
smtp_tls_CAfile              = /etc/ssl/certs/ca-certificates.crt
smtp_tls_protocols           = !SSLv2, !SSLv3
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
smtp_tls_mandatory_ciphers   = high
smtp_tls_note_starttls_offer = yes

# Smtpd ( INCOMING )
smtpd_tls_loglevel            = 1
smtpd_tls_auth_only           = no
smtpd_tls_security_level      = may
smtpd_tls_received_header     = yes
smtpd_tls_protocols           = !SSLv2, !SSLv3
smtpd_tls_mandatory_protocols = !SSLv2, !SSLv3
smtpd_tls_mandatory_ciphers   = high
```

```
smtpd_tls_exclude_ciphers     =
aNULL,eNULL,EXPORT,DES,3DES,RC2,RC4,MD5,PSK,SRP,DSS,AECDH,ADH
tls_high_cipherlist           =
EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:
EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3
DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED:!ECDSA:CAMELLIA256-SHA:AES256-
SHA:CAMELLIA128-SHA:AES128-SHA
smtpd_tls_CAfile              = $smtp_tls_CAfile
smtpd_tls_cert_file           = /chemin/vers/fichier.crt
smtpd_tls_key_file            = /chemin/vers/fichier.key
smtpd_tls_dh1024_param_file   = /etc/ssl/private/dh2048.pem
smtpd_tls_dh512_param_file    = /etc/ssl/private/dh512.pem

tls_preempt_cipherlist = yes
tls_random_source      = dev:/dev/urandom

smtp_tls_session_cache_database  = btree:${data_directory}/smtp_scache
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
mtpd_tls_session_cache_timeout   = 3600s
lmtp_tls_session_cache_database  = btree:${data_directory}/lmtp_scache

######################
## SASL PARAMETERS ##
######################

smtpd_sasl_auth_enable          = yes
smtpd_sasl_type                 = dovecot
smtpd_sasl_path                 = private/auth
smtpd_sasl_security_options     = noanonymous
smtpd_sasl_tls_security_options = $smtpd_sasl_security_options
smtpd_sasl_local_domain         = $mydomain
# was "$myhostname" (my setup)
smtpd_sasl_authenticated_header = yes

smtpd_sender_login_maps  = mysql:/etc/postfix/modoboa/sql-sender-login-
mailboxes.cf,
                           mysql:/etc/postfix/modoboa/sql-sender-login-
aliases.cf,
                           mysql:/etc/postfix/modoboa/sql-sender-login-
mailboxes-extra.cf
broken_sasl_auth_clients = yes

#############################
## VIRTUALS MAPS PARAMETERS ##
#############################

virtual_uid_maps        = static:5000
virtual_gid_maps        = static:5000
virtual_minimum_uid     = 5000
virtual_mailbox_base    = /home/mail
virtual_transport       = lmtp:unix:private/dovecot-lmtp
```

```
#dovecot_destination_recipient_limit = 5
virtual_mailbox_domains = mysql:/etc/postfix/modoboa/sql-domains.cf
virtual_alias_maps      = mysql:/etc/postfix/modoboa/sql-aliases.cf
virtual_alias_domains   = mysql:/etc/postfix/modoboa/sql-domain-aliases.cf
relay_domains           = mysql:/etc/postfix/modoboa/sql-relaydomains.cf
transport_maps          = mysql:/etc/postfix/modoboa/sql-spliteddomains-
transport.cf,
                          mysql:/etc/postfix/modoboa/sql-relaydomains-
transport.cf,
                          mysql:/etc/postfix/modoboa/sql-autoreplies-
transport.cf,
                          hash:/etc/postfix/modoboa/dmarc_transport

######################
## ERRORS REPORTING ##
######################

# notify_classes = bounce, delay, resource, software
notify_classes = resource, software

error_notice_recipient     = postmaster@domaine.tld
# delay_notice_recipient   = postmaster@domaine.tld
# bounce_notice_recipient  = postmaster@domaine.tld
# 2bounce_notice_recipient = postmaster@domaine.tld

##################
## RESTRICTIONS ##
##################

##
# Access restrictions for mail relay control that the Postfix SMTP server
applies
# in the context of the RCPT TO command, before smtpd_recipient_restrictions
##

# * permit_mynetworks : Permit the request when the client IP address
matches any trusted network
# * permit_sasl_authenticated : Permit the request when the client is
successfully authenticated
# * reject_unauth_destination : No one else, reject all others relaying
requests

smtpd_relay_restrictions=
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination

##
# Restrictions that the Postfix SMTP server applies in the context
# of a client MAIL FROM command
##
```

```
# * reject_non_fqdn_sender : Reject when the MAIL FROM address is not in
fully-qualified domain form
# * reject_unknown_sender_domain : Reject when the MAIL FROM domain has no
DNS MX, no DNS A record or a malformed MX record
# * reject_sender_login_mismatch: Reject when the client is not (SASL)
logged in as that MAIL FROM address owner or when the client is (SASL)
logged in, but the client login name doesn't own the MAIL FROM address
# * reject_rhsbl_sender : Reject when the MAIL FROM domain is blacklisted in
dbl.spamhaus.org

smtpd_sender_restrictions=
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    reject_sender_login_mismatch,
    reject_rhsbl_sender dbl.spamhaus.org

##
# Restrictions that the Postfix SMTP server applies in the context
# of a client RCPT TO command, after smtpd_relay_restrictions
##

# * permit_mynetworks : Permit the request when the client IP address
matches any trusted network
# * permit_sasl_authenticated : Permit the request when the client is
successfully authenticated
# * reject_unknown_recipient_domain : Reject when the RCPT TO domain has no
DNS MX or no DNS A record or a malformed MX record
# * reject_non_fqdn_recipient : Reject when the RCPT TO address is not in
fully-qualified domain form
# * reject_unlisted_recipient : Reject when the RCPT TO address is not
listed in the list of valid recipients for its domain
# * reject_rbl_client : Reject connections from IP addresses blacklisted in
zen.spamhaus.org

smtpd_recipient_restrictions=
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unknown_recipient_domain,
    reject_non_fqdn_recipient,
    reject_unlisted_recipient,
    check_recipient_access
        mysql:/etc/postfix/modoboa/sql-maintain.cf,
        mysql:/etc/postfix/modoboa/sql-relay-recipient-verification.cf
    reject_unauth_destination
    reject_unverified_recipient
    reject_rbl_client zen.spamhaus.org

##
# Restrictions that the Postfix SMTP server applies in the context of a
client HELO command
##
```

```
# Fully enforce helo restriction
# without "smtpd_helo_required = yes", a client can simply skip
# smtpd_helo_restrictions by not sending HELO or EHLO
smtpd_helo_required = yes
strict_rfc821_envelopes = yes

# Wait until the RCPT TO command before evaluating restrictions
smtpd_delay_reject = yes

# Filtrage
receive_override_options = no_address_mappings

# * permit_mynetworks : Permit the request when the client IP address
matches any trusted network
# * permit_sasl_authenticated : Permit the request when the client is
successfully authenticated
# * reject_invalid_helo_hostname : Reject the request when the HELO or EHLO
hostname is malformed
# * reject_non_fqdn_helo_hostname : Reject the request when the HELO or EHLO
hostname is not in fully-qualified domain

smtpd_helo_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_invalid_helo_hostname,
    reject_non_fqdn_helo_hostname

# Requirements for the connecting server
smtpd_client_restrictions =
    permit_mynetworks,
    permit_sasl_authenticated,
    permit_auth_destination
    reject_rbl_client bl.spamcop.net,
    reject_rbl_client dnsbl.njabl.org,
    reject_rbl_client cbl.abuseat.org,
    reject_rbl_client sbl-xbl.spamhaus.org,
    reject_rbl_client zen.spamhaus.org,
    reject_rbl_client dnsbl.sorbs.net,
    permit


############
## RSPAMD ##
############

milter_protocol       = 6
milter_mail_macros    = i {mail_addr} {client_addr} {client_name}
{auth_authen}
milter_default_action = accept
smtpd_milters         = inet:localhost:11332
non_smtpd_milters     = inet:localhost:11332
```

```
############
## ZEYPLE ##
############

content_filter = zeyple

######################
## YOUR CUSTOM RULES ##
######################
```

Veuillez noter que /etc/mailname doit indiquer mail.domaine.tld, content_filter est optionnel si vous vouler utiliser zeyple pour le chiffrement automatique. Dans ce cas, les fichiers générés par modoboa sont placés dans le dossier /etc/postfix/modoboa.

3.2. master.cf

Le 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" or
# on-line: http://www.postfix.org/master.5.html).
#
# Do not forget to execute "postfix reload" after editing this file.
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (no)    (never) (100)
# ==========================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtp      inet  n       -       y       -       1       postscreen
#smtpd     pass  -       -       y       -       -       smtpd
#dnsblog   unix  -       -       y       -       0       dnsblog
#tlsproxy  unix  -       -       y       -       0       tlsproxy
submission inet n       -       y       -       -       smtpd
   -o smtpd_enforce_tls=yes
   -o smtpd_sasl_auth_enable=yes
   -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#628       inet  n       -       y       -       -       qmqpd
pickup    unix  n       -       y       60      1       pickup
   -o content_filter=
   -o receive_override_options=no_header_body_checks
cleanup   unix  n       -       y       -       0       cleanup
qmgr      unix  n       -       n       300     1       qmgr
#qmgr     unix  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       y       1000?   1       tlsmgr
rewrite   unix  -       -       y       -       -       trivial-rewrite
bounce    unix  -       -       y       -       0       bounce
defer     unix  -       -       y       -       0       bounce
```

```
trace     unix  -       -       y       -       0       bounce
verify    unix  -       -       y       -       1       verify
flush     unix  n       -       y       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       y       -       -       smtp
relay     unix  -       -       y       -       -       smtp
        -o smtp_fallback_relay=
showq     unix  n       -       y       -       -       showq
error     unix  -       -       y       -       -       error
retry     unix  -       -       y       -       -       error
discard   unix  -       -       y       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       y       -       -       lmtp
anvil     unix  -       -       y       -       1       anvil
scache    unix  -       -       y       -       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.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# ====================================================================
#
# 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}
#
# ====================================================================
#
# Recent Cyrus versions can use the existing "lmtp" master.cf entry.
#
# Specify in cyrus.conf:
#   lmtp    cmd="lmtpd -a" listen="localhost:lmtp" proto=tcp4
#
# Specify in main.cf one or more of the following:
#  mailbox_transport = lmtp:inet:localhost
#  virtual_transport = lmtp:inet:localhost
#
# ====================================================================
#
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
#
#cyrus     unix  -       n       n       -       -       pipe
#  user=cyrus argv=/cyrus/bin/deliver -e -r ${sender} -m ${extension}
```

```
${user}
#
# ==========================================================================
# Old example of delivery via Cyrus.
#
#old-cyrus unix  -       n       n       -       -       pipe
#  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
#
# ==========================================================================
#
# See the Postfix UUCP_README file for configuration details.
#
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$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}
dovecot   unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -c
/etc/dovecot/dovecot.conf -f ${sender} -d ${user}@${nexthop}
dane       unix  -       -       n       -       -       smtp
  -o smtp_dns_support_level=dnssec
  -o smtp_tls_security_level=dane

# Zeyple
zeyple    unix  -       n       n       -       -       pipe
  user=zeyple argv=/usr/local/bin/zeyple.py ${recipient}

127.0.0.1:11026 inet  n       -       -       -       10      smtpd
  -o content_filter=
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks,n
o_milters
  -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,[::1]/128
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8,[::1]/128
```

```
# Vacation (modoboa)
autoreply  unix  -         n       n       -       -       pipe
       flags= user=vmail:vmail argv=/home/modoboa/env/bin/python
/home/modoboa/instance/manage.py autoreply $sender $mailbox
```

4.Dovecot

4.1. Configuration générale

La configuration générale de dovecot dans /etc/dovecot/conf.d se fait de cette façon:

>/etc/dovecot/conf.d/10-auth.conf<

```
disable_plaintext_auth = no
auth_cache_ttl = 1 hour
auth_username_chars =
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890.-_@
auth_mechanisms = plain login
!include auth-sql.conf.ext
```

>/etc/dovecot/conf.d/10-director.conf<

```
service director {
  unix_listener login/director {
  }
  fifo_listener login/proxy-notify {
  }
  unix_listener director-userdb {
  }
  inet_listener {
  }
}
service imap-login {
}
service pop3-login {
}
protocol lmtp {
}

log_path = /var/log/dovecot/dovecot.log
info_log_path = /var/log/dovecot/dovecot-info.log
auth_verbose = yes
auth_verbose_passwords = sha1
plugin {
}
```

```
log_timestamp = "%Y-%m-%d %H:%M:%S"
```

>etc/dovecot/conf.d/10-mail.conf<

```
mail_location = maildir:~/.maildir
namespace inbox {
  inbox = yes
}
mail_uid = 5000
mail_gid = 5000
mail_privileged_group = mail
valid_chroot_dirs = /var/spool/vmail
mail_plugins = $mail_plugins quota
```

>/etc/dovecot/conf.d/10-master.conf<

```
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 /var/spool/postfix/private/dovecot-lmtp {
    mode = 0600
    user = postfix
    group = postfix
  }
  user = vmail
}
service imap {
  executable = imap postlogin
}
service pop3 {
  executable = pop3 postlogin
}
```

```
service auth {
  unix_listener auth-userdb {
  }
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
}
service auth-worker {
}
service dict {
  unix_listener dict {
    mode = 0600
    user = vmail
  }
}
service postlogin {
  executable = script-login /usr/local/bin/postlogin.sh
  user = modoboa
  unix_listener postlogin {
  }
}
```

>/etc/dovecot/conf.d/10-ssl.conf<

```
ssl = required
ssl_cert = </chemin/vers/fichier.crt
ssl_key = </chemin/vers/fichier.key
ssl_dh_parameters_length = 2048
ssl_cipher_list = ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-
SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-
SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-
AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA:AES256-SHA:DHE-
RSA-CAMELLIA128-SHA:DHE-RSA-CAMELLIA256-SHA:CAMELLIA128-SHA:CAMELLIA256-
SHA:ECDHE-RSA-DES-CBC3-SHA:DES-CBC3-SHA
```

>/etc/dovecot/conf.d/15-lda.conf<

```
postmaster_address = postmaster@domaine.tld
quota_full_tempfail = yes
recipient_delimiter = +
lda_mailbox_autocreate = yes
lda_mailbox_autosubscribe = yes
protocol lda {
  log_path = /var/log/dovecot/dovecot-lda.log
  info_log_path = /var/log/dovecot/dovecot-lda.log
```

```
  mail_plugins = quota sieve
}
```

>/etc/dovecot/conf.d/15-mailboxes.conf<

```
namespace inbox {
  mailbox Drafts {
    auto = subscribe
    special_use = \Drafts
  }
  mailbox Junk {
    auto = subscribe
    special_use = \Junk
  }
  mailbox Trash {
    auto = subscribe
    special_use = \Trash
  }
  mailbox Sent {
    auto = subscribe
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    auto = subscribe
    special_use = \Sent
  }
}
```

>/etc/dovecot/conf.d/20-imap.conf<

```
protocol imap {
mail_plugins = $mail_plugins imap_quota imap_sieve
}
```

>/etc/dovecot/conf.d/20-lmtp.conf<

```
protocol lmtp {
  postmaster_address = postmaster@domaine.tld
  mail_plugins = $mail_plugins sieve quota
}
```

>/etc/dovecot/conf.d/20-managesieve.conf<

```
protocols = $protocols sieve
service managesieve-login {
```

```
  inet_listener sieve {
    port = 4190
  }
  service_count = 1
  process_min_avail = 0
  vsz_limit = 64M
}
service managesieve {
}
protocol sieve {
  managesieve_max_line_length = 65536
  mail_max_userip_connections = 10
  mail_plugins =
  managesieve_logout_format = bytes=%i/%o
  managesieve_implementation_string = Dovecot Pigeonhole
  managesieve_max_compile_errors = 5
  log_path=/var/log/dovecot/dovecot-sieve.log
  info_log_path=/var/log/dovecot/dovecot-sieve.log
}
```

>/etc/dovecot/conf.d/20-pop3.conf<

```
protocol pop3 {
  mail_plugins = $mail_plugins
}
```

>/etc/dovecot/conf.d/90-acl.conf<

```
plugin {
}
plugin {
}
```

>/etc/dovecot/conf.d/90-quota.conf<

```
plugin {
}
plugin {
  quota_warning = storage=75%% /usr/local/bin/quota-warning.sh 75 %u
  quota_warning2 = storage=90%% /usr/local/bin/quota-warning.sh 90 %u
}
plugin {
  quota = maildir:User quota
}
plugin {
  quota = dict:User quota::proxy::quota
```

```
}
```

>/etc/dovecot/conf.d/90-sieve.conf<

```
plugin {
  sieve = ~/.dovecot.sieve
  sieve_dir = ~/sieve
  sieve_default = /var/lib/dovecot/sieve/global/default.sieve
  sieve_global = /var/lib/dovecot/sieve/global/
  sieve_plugins = sieve_imapsieve sieve_extprograms
  imapsieve_mailbox1_name = Spam
  imapsieve_mailbox1_causes = COPY
  imapsieve_mailbox1_before = file:/usr/local/dovecot/sieve/report-
spam.sieve
  imapsieve_mailbox2_name = *
  imapsieve_mailbox2_from = Spam
  imapsieve_mailbox2_causes = COPY
  imapsieve_mailbox2_before = file:/usr/local/dovecot/sieve/report-ham.sieve
  sieve_pipe_bin_dir = /usr/local/dovecot/sieve
  sieve_global_extensions = +vnd.dovecot.pipe +vnd.dovecot.environment
  recipient_delimiter = +
}
```

>/etc/dovecot/conf.d/90-sieve-extprograms.conf<

```
plugin {
}
```

>/etc/dovecot/conf.d/auth-checkpassword.conf.ext<

```
passdb {
  driver = checkpassword
  args = /usr/bin/checkpassword
}
userdb {
  driver = prefetch
}
```

>/etc/dovecot/conf.d/auth-deny.conf.ext<

```
passdb {
  driver = passwd-file
  deny = yes
  args = /etc/dovecot/deny-users
```

```
}
```

>/etc/dovecot/conf.d/auth-dict.conf.ext<

```
passdb {
  driver = dict
  args = /etc/dovecot/dovecot-dict-auth.conf.ext
}
userdb {
  driver = dict
  args = /etc/dovecot/dovecot-dict-auth.conf.ext
}
```

>/etc/dovecot/conf.d/auth-master.conf.ext<

```
passdb {
  driver = passwd-file
  master = yes
  args = /etc/dovecot/master-users
  pass = yes
}
```

>/etc/dovecot/conf.d/auth-passwdfile.conf.ext<

```
passdb {
  driver = passwd-file
  args = scheme=CRYPT username_format=%u /etc/dovecot/users
}
userdb {
  driver = passwd-file
  args = username_format=%u /etc/dovecot/users
}
```

>/etc/dovecot/conf.d/auth-sql.conf.ext<

```
passdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
userdb {
  driver = sql
  args = /etc/dovecot/dovecot-sql.conf.ext
}
```

>/etc/dovecot/conf.d/auth-system.conf.ext<

```
passdb {
  driver = pam
}
userdb {
  driver = passwd
}
```

>/etc/dovecot/conf.d/auth-vpopmail.conf.ext<

```
passdb {
  driver = vpopmail
  args =
}
userdb {
  driver = vpopmail
  args = quota_template=quota_rule=*:backend=%q
}
```

4.2. Gestion de la db

Les autres fichiers utiles tels =⇒/etc/dovecot/dovecot-dict-auth.conf.ext⇐=

```
default_pass_scheme = MD5
iterate_prefix = userdb/
key passdb {
  key = passdb/%u
  format = json
}
key userdb {
  key = userdb/%u
  format = json
}
key quota {
  key = userdb/%u/quota
  default_value = 100M
}
passdb_objects = passdb
userdb_objects = userdb
userdb_fields {
  quota_rule = *:storage=%{dict:quota}
  mail = maildir:%{dict:userdb.home}/Maildir
}
```

>/etc/dovecot/dovecot-dict-sql.conf.ext<

```
connect = host=127.0.0.1 dbname=DB user=USER password=PWD
map {
  pattern = priv/quota/storage
  table = admin_quota
  username_field = username
  value_field = bytes
}
map {
  pattern = priv/quota/messages
  table = admin_quota
  username_field = username
  value_field = messages
}
map {
  pattern = shared/expire/$user/$mailbox
  table = expires
  value_field = expire_stamp
  fields {
    username = $user
    mailbox = $mailbox
  }
}
```

>/etc/dovecot/dovecot-sql.conf.ext<

```
driver = mysql
connect = host=127.0.0.1 dbname=DB user=USER password=PWD
default_pass_scheme = CRYPT
password_query = SELECT email AS user, password FROM core_user WHERE
email='%Lu' and is_active=1
user_query = SELECT '/home/mail/%Ld/%Ln' AS home, 5000 as uid, 5000 as gid,
concat('*:bytes=', mb.quota, 'M') AS quota_rule FROM admin_mailbox mb INNER
JOIN admin_domain dom ON mb.domain_id=dom.id WHERE mb.address='%Ln' AND
dom.name='%Ld'
iterate_query = SELECT email AS user FROM core_user
```

4.3. scripts utiles

Il faut aussi des scripts utiles:

>/usr/local/bin/postlogin.sh <

```
#!/bin/sh
```

```
DBNAME=DB
DBUSER=USER
DBPASSWORD=PWD

echo "UPDATE core_user SET last_login=now() WHERE username='$USER'" | mysql
-u $DBUSER -p$DBPASSWORD $DBNAME

exec "$@"
```

>/usr/local/bin/quota-warning.sh<

```
#!/bin/sh
PERCENT=$1
USER=$2
cat << EOF | /usr/lib/dovecot/dovecot-lda -d $USER -o
"plugin/quota=maildir:User quota:noenforcing"
From: postmaster@domaine.tld
Subject: quota warning

Your mailbox is now $PERCENT% full.
EOF
```

4.4 antispam

Pour l'antispam, je propose ceci, proche de la configuration officielle dovecot:

>/usr/local/dovecot/sieve/report-ham.sieve<

```
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment",
"variables"];

if environment :matches "imap.mailbox" "*" {
  set "mailbox" "${1}";
}

if string "${mailbox}" "Trash" {
  stop;
}

if environment :matches "imap.user" "*" {
  set "username" "${1}";
}

pipe :copy "sa-learn-ham.sh" [ "${username}" ];
```

>/usr/local/dovecot/sieve/report-spam.sieve<

```
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment",
"variables"];

if environment :matches "imap.user" "*" {
  set "username" "${1}";
}

pipe :copy "sa-learn-spam.sh" [ "${username}" ];
```

>/usr/local/dovecot/sieve/sa-learn-ham.sh<

```
#!/bin/bash

# rspamd client reads piped ham message from the standard input
exec /usr/bin/rspamc -h localhost:11334 -P "q1" learn_ham
```

>/usr/local/dovecot/sieve/sa-learn-spam.sh<

```
#!/bin/bash

# rspamd client reads piped spam message from the standard input
exec /usr/bin/rspamc -h localhost:11334 -P "q1" learn_spam
```

5. nginx et uwsgi

5.1. configuration du domaine principal

Le domaine principal mail.domaine.tld sera configuré de cette façon:

```
server {
        listen 80;
#        listen [::]:80 ipv6only=on;
        root /chemin/vers/modoboa/<instance>/<instance>;

        # Make site accessible from http://localhost/
        server_name mail.domaine.tld localhost;

        if ($ssl_protocol = "") {
                rewrite ^/(.*)   https://$server_name$request_uri?
permanent;
        }
}
```

```
server {
    listen 443 ssl http2;
#    listen [::]:443 ssl http2;
    ssl on;
    keepalive_timeout 70;

    server_name mail.domaine.tld localhost;
    root /chemin/vers/modoboa/<instance>/<instance>;

    ssl_certificate /chemin/vers/fichier.crt;
    ssl_certificate_key /chemin/vers/fichier.key;

    access_log  /var/log/nginx/modoboa.access.log;
    error_log /var/log/nginx/modoboa.error.log;

    location /sitestatic/ {
            autoindex on;
            alias /home/modoboa/instance/sitestatic/;
    }

    # Whether or not Modoboa uses a media directory depends on how
    # you configured Modoboa. It does not hurt to have this.
    location /media/ {
            autoindex on;
            alias /home/modoboa/instance/media/;
    }

    # This denies access to any file that begins with
    # ".ht". Apache's .htaccess and .htpasswd are such files. A
    # Modoboa installed from scratch would not contain any such
    # files, but you never know what the future holds.
    location ~ /\.ht {
        deny all;
    }

    location / {
        include uwsgi_params;
        uwsgi_pass unix:/run/uwsgi/app/modoboa/socket;
        uwsgi_param UWSGI_SCRIPT instance.wsgi:application;
        uwsgi_param UWSGI_SCHEME https;
    }

    location /rspamd/ {
        proxy_pass       http://localhost:11334/;
        proxy_set_header Host      $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }
}
```

5.2. uwsgi

et le fichier nécessaire pour uwsgi (à adapter à votre utilisation):

```
[uwsgi]
plugins = python
chdir = /chemin/vers/modoboa/<instance>
venv = /chemin/vers/env
module = <instance>.wsgi:application
master = true
harakiri = 60
processes = 2
vhost = true
no-default-app = true
```

Je précise qu'il faudra modifier la configuration TLS par défaut de nginx que je trouve trop lâche mais je vous laisse faire vos choix.

6. Rspamd

6.1. Configuration

Les fichiers de configuration de rspamd ne doivent pas être modifiés, il faut soit les compléter (dossier local.d) ou les remplacer (override.d), une configuration sera proposée mais elle peut être à adapter au cas par cas.

>/etc/rspamd/rspamd.conf.local<

```
worker "log_helper" {
  count = 1;
}

multimap {
    # ip - matches source IP of message (radix map)
    # from - matches envelope from (or header From if envelope from is
absent)
    # rcpt - matches any of envelope rcpt or header To if envelope info is
missing
    # header - matches any header specified (must have header = "Header-
Name" configuration attribute)
    # dnsbl - matches source IP against some DNS blacklist (consider using
RBL module for this)
    local_bl_ip { type = "ip"; map = "$CONFDIR/local.d/local_bl_ip.map.inc";
symbol = "LOCAL_BL_IP"; description = "Local ip blacklist";}
    local_bl_from { type = "from"; map =
"$CONFDIR/local.d/local_bl_from.map.inc"; symbol = "LOCAL_BL_FROM";
```

```
description = "Local from blacklist";}
    local_bl_rcpt { type = "rcpt"; map =
"$CONFDIR/local.d/local_bl_rcpt.map.inc"; symbol = "LOCAL_BL_RCPT";
description = "Local rcpt blacklist";}
    local_wl_ip { type = "ip"; map = "$CONFDIR/local.d/local_wl_ip.map.inc";
symbol = "LOCAL_WL_IP"; description = "Local ip whitelist";}
    local_wl_from { type = "from"; map =
"$CONFDIR/local.d/local_wl_from.map.inc"; symbol = "LOCAL_WL_FROM";
description = "Local from whitelist";}
    local_wl_rcpt { type = "rcpt"; map =
"$CONFDIR/local.d/local_wl_rcpt.map.inc"; symbol = "LOCAL_WL_RCPT";
description = "Local rcpt whitelist";}
}

metric {
    name = "default";
    group {
        name = "local";
        symbol {
            weight = 3;
            description = "Sender ip listed in local ip blacklist";
            name = "LOCAL_BL_IP";
        }
        symbol {
            weight = 3;
            description = "Sender from listed in local from blacklist";
            name = "LOCAL_BL_FROM";
        }
        symbol {
            weight = 3;
            description = "Recipient listed in local rcpt blacklist";
            name = "LOCAL_BL_RCPT";
        }
        symbol {
            weight = -10;
            description = "Sender ip listed in local ip whitelist";
            name = "LOCAL_WL_IP";
        }
        symbol {
            weight = -5;
            description = "Sender from listed in local from whitelist";
            name = "LOCAL_WL_FROM";
        }
        symbol {
            weight = -5;
            description = "Recipient listed in local rcpt whitelist";
            name = "LOCAL_WL_RCPT";
        }
    }
```

```
}
```

Les fichiers créés pour l'occasion:

> /etc/rspamd/local.d/antivirus.conf <

```
# multiple scanners could be checked, for each we create a configuration
block with an arbitrary name
clamav {
  enabled = true;
  # If set force this action if any virus is found (default unset: no action
is forced)
  action = "reject";
  # if `true` only messages with non-image attachments will be checked
(default true)
  attachments_only = false;
  # If `max_size` is set, messages > n bytes in size are not scanned
  #max_size = 20000000;
  # symbol to add (add it to metric if you want non-zero weight)
  symbol = "CLAM_VIRUS";
  # type of scanner: "clamav", "fprot", "sophos" or "savapi"
  type = "clamav";
  # If set true, log message is emitted for clean messages
  #log_clean = false;
  # For "savapi" you must also specify the following variable
  #product_id = 12345;
  # For "savapi" you can enable logging for clean messages
  log_clean = true;
  # servers to query (if port is unspecified, scanner-specific default is
used)
  # can be specified multiple times to pool servers
  # can be set to a path to a unix socket
  servers = "127.0.0.1:3310";
  # if `patterns` is specified virus name will be matched against provided
regexes and the related
  # symbol will be yielded if a match is found. If no match is found,
default symbol is yielded.
  patterns {
    # symbol_name = "pattern";
    JUST_EICAR = "^Eicar-Test-Signature$";
  }
  # `whitelist` points to a map of IP addresses. Mail from these addresses
is not scanned.
  #whitelist = "/etc/rspamd/antivirus.wl";
}
```

> /etc/rspamd/local.d/arc.conf <

```
# local.d/arc.conf

# If false, messages with empty envelope from are not signed
allow_envfrom_empty = false;
# If true, envelope/header domain mismatch is ignored
allow_hdrfrom_mismatch = false;
# If true, multiple from headers are allowed (but only first is used)
allow_hdrfrom_multiple = true;
# If true, username does not need to contain matching domain
allow_username_mismatch = true;
# If false, messages from authenticated users are not selected for signing
auth_only = true;
# Default path to key, can include '$domain' and '$selector' variables
path = "/usr/local/etc/dkim/keys/$domain.$selector.key";
# Default selector to use
selector = "mail";
# If false, messages from local networks are not selected for signing
sign_local = true;
# Symbol to add when message is signed
symbol_signed = "ARC_SIGNED";
# Whether to fallback to global config
try_fallback = true;
# Domain to use for ARC signing: can be "header" or "envelope"
use_domain = "header";
# Whether to normalise domains to eSLD
use_esld = false;
# Whether to get keys from Redis
use_redis = false;
# Hash for ARC keys in Redis
key_prefix = "ARC_KEYS";
# map of domains -> names of selectors (since rspamd 1.5.3)
#selector_map = "/etc/rspamd/arc_selectors.map";
# map of domains -> paths to keys (since rspamd 1.5.3)
#path_map = "/etc/rspamd/arc_paths.map";
```

> /etc/rspamd/local.d/classifier-bayes.conf <

```
servers = "127.0.0.1";
backend = "redis";
```

> /etc/rspamd/local.d/dkim_signing.conf <

```
# If false, messages with empty envelope from are not signed
allow_envfrom_empty = true;

# If true, envelope/header domain mismatch is ignored
allow_hdrfrom_mismatch = false;
```

```
# If true, multiple from headers are allowed (but only first is used)
allow_hdrfrom_multiple = true;

# If true, username does not need to contain matching domain
allow_username_mismatch = true;

# If false, messages from authenticated users are not selected for signing
auth_only = true;

# Default path to key, can include '$domain' and '$selector' variables
path = "/usr/local/etc/dkim/keys/$domain.$selector.key";

# Default selector to use
selector = "mail";

# If false, messages from local networks are not selected for signing
sign_local = true;

# Map file of IP addresses/subnets to consider for signing
# sign_networks = "/some/file"; # or url

# Symbol to add when message is signed
symbol = "DKIM_SIGNED";

# Whether to fallback to global config
try_fallback = true;

# Domain to use for DKIM signing: can be "header" (MIME From), "envelope"
(SMTP From) or "auth" (SMTP username)
use_domain = "header";

# Domain to use for DKIM signing when sender is in sign_networks
("header"/"envelope"/"auth")
#use_domain_sign_networks = "header";

# Domain to use for DKIM signing when sender is a local IP
("header"/"envelope"/"auth")
#use_domain_sign_local = "header";

# Whether to normalise domains to eSLD
use_esld = falsee;

# Whether to get keys from Redis
use_redis = false;

# Hash for DKIM keys in Redis
key_prefix = "DKIM_KEYS";

# map of domains -> names of selectors (since rspamd 1.5.3)
#selector_map = "/etc/rspamd/dkim_selectors.map";
```

```
# map of domains -> paths to keys (since rspamd 1.5.3)
#path_map = "/etc/rspamd/dkim_paths.map";
```

> /etc/rspamd/local.d/dmarc.conf <

```
dmarc {
    # Enables storing reporting information to redis
    reporting = true;
    # If Redis server is not configured below, settings from redis {} will
be used
    #servers = "127.0.0.1:6379"; # Servers to use for reads and writes (can
be a list)
    # Alternatively set read_servers / write_servers to split reads and
writes
    # To set custom prefix for redis keys:
    #key_prefix = "dmarc_";
    # Actions to enforce based on DMARC disposition (empty by default)
    actions = {
        quarantine = "add_header";
        reject = "reject";
    }
        # Ignore "pct" setting for some domains
        # no_sampling_domains = "/etc/rspamd/dmarc_no_sampling.domains";
}
```

> /etc/rspamd/local.d/fann_redis.conf <

```
servers = "localhost";
```

> /etc/rspamd/local.d/greylist.conf <

```
greylist {
    servers = "127.0.0.1:6379";
#   whitelist_domains_url [
#       "/etc/rspamd/local.d/local_wl_from.map.inc",
#   ]
#   greylist_min_score = 5;
}
```

> /etc/rspamd/local.d/greylist-whitelist-domains.inc <

```
# Whitelist for greylist
debian.org
```

> /etc/rspamd/local.d/ip_score.conf <

```
ip_score {
#    servers = "localhost";
#    threshold = 100;
#    reject_score = 3;
#    no_action_score = -2;
#    add_header_score = 1;
#    whitelist = "file:///ip_map";
# how each action is treated in scoring
actions {
  reject = 1.0;
  "add header" = 0.25;
  "rewrite subject" = 0.25;
  "no action" = 1.0;
}
# how each component is evaluated
scores {
  asn = 0.5;
  country = 0.1;
  ipnet = 0.8;
  ip = 1.0;
}
# prefix for asn hashes
asn_prefix = "a:";
# prefix for country hashes
country_prefix = "c:";
# hash table in redis used for storing scores
hash = "ip_score";
# prefix for subnet hashes
ipnet_prefix = "n:";
# minimum number of messages to be scored
lower_bound = 10;
# the metric to score (usually "default")
metric = "default";
# upper and lower bounds at which to cap total score
#max_score = 10;
#min_score = -5;
# Amount to divide subscores by before applying tanh
score_divisor = 10;
# list of servers (or configure redis globally)
#servers = "localhost";
# symbol to be inserted
symbol = "IP_SCORE";
}
```

> /etc/rspamd/local.d/local_bl_from.map.inc <

```
# A remplir
```

> /etc/rspamd/local.d/local_bl_ip.map.inc <

```
# A remplir
```

> /etc/rspamd/local.d/local_bl_rcpt.map.inc <

```
# A remplir
```

> /etc/rspamd/local.d/local_wl_from.map.inc <

```
# A remplir
debian.org
```

> /etc/rspamd/local.d/local_wl_ip.map.inc <

```
# A remplir
::1
127.0.0.1
```

> /etc/rspamd/local.d/local_wl_rcpt.map.inc <

```
# A remplir
```

> /etc/rspamd/local.d/metrics.conf <

```
actions {
  reject = 20;
#  soft_reject = 15;
  rewrite_subject = 8;
  add_header = 6;
  greylist = 4;
}

subject = "*** SPAM *** %s";

symbol "MX_INVALID" {
  score = 1.0;
  description = "No connectable MX";
  one_shot = "true";
}

symbol "MX_MISSING" {
  score = 2.0;
```

```
  description = "No MX record";
  one_shot = "true";
}

symbol "MX_GOOD" {
  score = -0.5;
  description = "MX was ok";
  one_shot = "true";
}

symbol "IP_SCORE" {
  weight = 2.0;
  description = "IP reputation";
}
```

> /etc/rspamd/local.d/milter_headers.conf <

```
use = ["spam-header", "x-spam-level", "x-spam-status", "x-virus",
"authentication-results"];

skip_local = false;
skip_authenticated = true;
extended_spam_headers = true;

routines {
  spam-header {
    header = "X-Spam-Flag";
    remove = 1;
    value = "YES";
  }
  x-spam-level {
    header = "X-Spam-Level";
    remove = 1;
    char = "*";
  }
  x-spam-status {
    header = "X-Spam-Status";
    remove = 1;
  }
  x-virus {
    header = "X-Virus";
    remove = 1;
    symbols = ["CLAM_VIRUS"];
  }
  authentication-results {
    header = "Authentication-Results";
    remove = 1;
    spf_symbols {
      pass = "R_SPF_ALLOW";
      fail = "R_SPF_FAIL";
```

```
      softfail = "R_SPF_SOFTFAIL";
      neutral = "R_SPF_NEUTRAL";
      temperror = "R_SPF_DNSFAIL";
      none = "R_SPF_NA";
      permerror = "R_SPF_PERMFAIL";
    }
    dkim_symbols {
      pass = "R_DKIM_ALLOW";
      fail = "R_DKIM_REJECT";
      temperror = "R_DKIM_TEMPFAIL";
      none = "R_DKIM_NA";
      permerror = "R_DKIM_PERMFAIL";
    }
    dmarc_symbols {
      pass = "DMARC_POLICY_ALLOW";
      permerror = "DMARC_BAD_POLICY";
      temperror = "DMARC_DNSFAIL";
      none = "DMARC_NA";
      reject = "DMARC_POLICY_REJECT";
      softfail = "DMARC_POLICY_SOFTFAIL";
      quarantine = "DMARC_POLICY_QUARANTINE";
    }
  }
}
```

> /etc/rspamd/local.d/mime_types.conf <

```
# Extensions that are treated as 'bad'
# Number is score multiply factor
bad_extensions = {
  scr = 4,
  lnk = 4,
  exe = 1,
  jar = 2,
  com = 4,
  bat = 4,
  ace = 4,
  arj = 4,
  cab = 3,
};

# Extensions that are particularly penalized for archives
bad_archive_extensions = {
  pptx = 0.5,
  docx = 0.5,
  xlsx = 0.5,
  pdf = 1.0,
  jar = 3,
  js = 0.5,
  vbs = 7,
```

```
};

# Used to detect another archive in archive
archive_extensions = {
  zip = 1,
  arj = 1,
  rar = 1,
  ace = 1,
  7z = 1,
  cab = 1,
};
```

> /etc/rspamd/local.d/mx_check.conf <

```
enabled = true;
timeout = 1.0;
symbol_bad_mx = "MX_INVALID";
symbol_no_mx = "MX_MISSING";
symbol_good_mx = "MX_GOOD";
expire = 86400;
expire_novalid = 7200;
greylist_invalid = false;
key_prefix = "rmx";
```

> /etc/rspamd/local.d/options.inc <

```
map_watch_interval = 1min;
dns {
  enable_dnssec = true;
  timeout = 4s;
  retransmits = 5;
  nameserver = "master-slave:127.0.0.1:53:10";
}
```

> /etc/rspamd/local.d/ratelimit.conf <

```
rates {
  # Limit for all mail per recipient (rate 2 per minute)
  to = "2 / 1m";
  # Limit for all mail per one source ip (rate 3 per minute)
  to_ip = "3 / 1m";
  # Limit for all mail per one source ip and from address (rate 2 per
minute)
  to_ip_from = "2 / 1m";
  # Limit for all bounce mail (rate 2 per hour)
  bounce_to = "2 / 1h";
  # Limit for bounce mail per one source ip (rate 1 per hour)
```

```
  bounce_to_ip = "1 / 1h";
  # Limit for all mail per authenticated user (rate 2 per minute)
  user = "2 / 1m";
}

whitelisted_rcpts = "postmaster,mailer-daemon";
max_rcpt = 5;
```

> /etc/rspamd/local.d/redis.conf <

```
servers = "127.0.0.1:6379";
```

> /etc/rspamd/local.d/statistic.conf <

```
classifier "bayes" {
    tokenizer {
    name = "osb";
    }

    backend = "redis";
    servers = "127.0.0.1:6379";
    min_tokens = 11;
    min_learns = 10;
    autolearn = true;

    per_user = <<EOD
return function(task)
    local rcpt = task:get_recipients(1)

if rcpt then
    one_rcpt = rcpt[1]
    if one_rcpt['domain'] then
        return one_rcpt['domain']
    end
end

return nil
end
EOD

    statfile {
        symbol = "BAYES_HAM";
        spam = false;
    }
    statfile {
        symbol = "BAYES_SPAM";
        spam = true;
    }
```

```
    learn_condition =<<EOD
return function(task, is_spam, is_unlearn)
    local prob = task:get_mempool():get_variable('bayes_prob', 'double')

    if prob then
        local in_class = false
        local cl
        if is_spam then
            cl = 'spam'
            in_class = prob >= 0.95
        else
            cl = 'ham'
            in_class = prob <= 0.05
        end

        if in_class then
            return false,string.format('already in class %s; probability
%.2f%%',
            cl, math.abs((prob - 0.5) * 200.0))
        end
    end

    return true
end
EOD
}
```

> /etc/rspamd/local.d/worker-controller.inc <

```
password = "q1";
enable_password = "q2";
```

q1 et q2 sont les mots de passe à modifier.

6.2. Commandes utiles

Changer les mots de passe q1 et q2:

```
rspamadm pw
```

Générer une clef privée qui doit être absolument être lisible par l'utilisateur _rspamd_ :

```
rspamadm dkim_keygen -s 'mail' -d domaine.tld
```

avec l'option -s désignant le sélecteur qui doit **impérativement être le même que celui de votre enregistrement DNS** sans quoi la signature de vos messages ne servira à rien.

From:
https://wiki.mirtouf.fr/ - **Da mirtouf wiki**

Permanent link:
https://wiki.mirtouf.fr/doku.php?id=mail&rev=1510255609

Last update: **2017/11/09 19:26**