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 dovecott-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 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

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
```

puis 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):

```
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.

Le fichier à placer dans /etc/cron.d :

```
#
# 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

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

######################
## 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.

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
```

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

Permanent link:
https://wiki.mirtouf.fr/doku.php?id=mail&rev=1509817236

Last update: **2017/11/04 17:40**