Exim4

Table des matières

1 Intro

specs ; cf */usr/share/doc/exim4-base/README.Debian.gz*

Contrairement à ssh, ce qui est écrit derrière @ n'est pas un nom de machine (hostname) mais un nom de domaine. Tu écris à un contact orange vers une adresse du type @orange.fr (nom de domaine) et non @pop.orange.fr (nom de machine du serveur de mail).

```
$ host -t MX narval.hd.free.fr
narval.hd.free.fr has no MX record

$ host -t mx narval.tk 134.158.152.146
narval.tk mail is handled by 10 mail.narval.tk.
```

2 Serveur Smtp

```
# apt-get install exim4-doc-info bsd-mailx
# dpkg-reconfigure exim4-config
```

configuration ovh : */etc/exim4/update-exim4.conf.conf* :

```
dc_eximconfig_configtype='internet'
dc_other_hostnames='narval.tk'
dc_local_interfaces=''
dc_readhost=''
dc_relay_domains=''
dc_minimaldns='false'
dc_relay_nets='79.143.250.133'
dc_smarthost=''
CFILEMODE='644'
```

```
dc_use_split_config='false'
dc_hide_mailname=''
dc_mailname_in_oh='true'
dc_localdelivery='mail_spool'
```

remarques :

- A priori, on n'a pas besoin ni d'envoyer ni de relayer les mails vers l'extérieur (on utilise le smtp du réseau qui héberge notre client de messagerie).
- Penser à ouvrir le port 25 en entrée.

3 Courrier en entrée

3.1 En provenance interne

Le fichier */etc/aliases* permet les redirections pour les courriers reçus localements.

- Seule une ligne de redirection est prise en compte pour chaque compte.
- Plusieurs destinataires peuvent figurer sur une ligne.
- Une redirection recursive permet de délivrer le message au destinataire ainsi que de le rediriger.

Là on fait un alias :

```
# exim_checkaccess 82.242.5.148 nicolas.roche@narval.tk
Rejected:
  550 Unrouteable address

# tail -n 2 /etc/aliases
nicolas.roche: nroche
#nroche: nroche nicolasf.roche@gmail.com

# exim_checkaccess 82.242.5.148 nicolas.roche@narval.tk
Accepted
```

Ici on a une réception locale et une copie envoyée sur une autre boite :

```
mailer-daemon: postmaster
postmaster: root
root: nroche
nroche: nroche, nicolas.roche@ias.u-psud.fr
```

Remarque : Le fichier */.forward* permet aussi de rediriger les mails.

```
nicolas.roche@ias.u-psud.fr
```

3.2 Provenance exterieure

A priori tout peux se faire en utilisant la méthode de configuration proposée par debian. Ci dessous les méthodes utilisées pour les tests.

- Connexion au serveur

```
# apt-get install mailx
$ mail nroche@narval.tk

send-mail: RCPT TO:<nroche@narval.tk> (550 relay not permitted)
Can't send mail: sendmail process failed with error code 1
```

- Idem en utilisant TELNET

```
$ telnet max 25
220 maximus.narval.tk ESMTP Exim 4.63 Thu, 10 Jun 2010 22:49:03 +0200

HELO trouduc
250 maximus.narval.tk Hello trouduc [192.168.2.2]

MAIL FROM: toto@tutuland
250 OK

RCPT TO: nroche@narval.tk
550 relay not permitted :@)

RCPT TO: nroche@localhost
250 Accepted

DATA
354 Enter message, ending with "." on a line by itself
test 10:53
.
250 OK id=1OMokq-0007Kz-7b

QUIT
221 maximus.narval.tk closing connection
```

- Simulation de la connection sur le serveur

```
# exim_checkaccess 82.242.5.148 nroche@narval.tk
Rejected:
  550 relay not permitted :@)

# grep 'not permitted' ./conf.d/acl/30_exim4-config_check_rcpt
    message = relay not permitted :@)

# dpkg-reconfigure exim4-config
# exim_checkaccess 82.242.5.148 nroche@narval.tk
Accepted
```

remarque : Les mails en entrée envoyés via smtp.free.fr ont mis un jour pour arriver.

3.3 SMTP + SSL

D'après la doc, c'est l'approche STARTLS (même port pour les connexions en clair ou cryptées) qui est standadisée. Donc on ne bascule pas sur le port 465. On rajoute juste au client la possibilité de faire du STARTTLS sur le port 25.

```
# /usr/share/doc/exim4-base/examples/exim-gencert
```

```
# ls -l /etc/exim4/
-rw-r----- 1 root Debian-exim  1172 déc.  22 15:46 exim.crt
-rw-r----- 1 root Debian-exim  1704 déc.  22 15:45 exim.key

// configuration dans un seul fichier
# vi /etc/exim4/exim4.conf.localmacros
MAIN_TLS_ENABLE = true

// idem, configuration éclatée
# cp /etc/exim4/exim4.conf.localmacros /etc/exim4/conf.d/main/000_localmacros

# /etc/init.d/exim4 restart
```

test :

```
$ openssl s_client -connect mail.narval.fr.eu.org:25 -starttls smtp
# tcpdump -i eth0 host 79.143.250.133 and port 25 -AAA
(on ne voit pas le message en clair)
```

Si on veut forcer l'utilisation de SSL sur le port 465,

```
# exim -bP | grep "daemon_smtp_ports"
daemon_smtp_ports = smtp
# exim -bP | grep "tls_on_connect_ports"
tls_on_connect_ports =
# exim -bP | grep "local_interfaces"
extra_local_interfaces =
local_interfaces = <; ::0 ; 0.0.0.0

// ICI!! -> a priori a refaire après chaque "dpkg-reconfigure"
# cat >> /etc/exim4/conf.d/main/03_exim4-config_tlsoptions
tls_on_connect_ports    = 465
daemon_smtp_ports = 25 : 465

# /etc/init.d/exim4 restart

# exim -bP | grep "daemon_smtp_ports"
daemon_smtp_ports = 25 : 465
# exim -bP | grep "tls_on_connect_ports"
tls_on_connect_ports = 465
# exim -bP | grep "local_interfaces"
extra_local_interfaces =
local_interfaces = <; ::0 ; 0.0.0.0
```

test :

```
$ openssl s_client -connect mail.narval.fr.eu.org:465
# tcpdump -i eth0 host 79.143.250.133 and port 465 -AAA
(on ne voit pas le message en clair)
```

3.4 SMTP + password

Décomménter la section `cram_md5_server` dans */etc/exim4/conf.d/auth/30_exim4-config_examples*

```
cram_md5_server:
  driver = cram_md5
```

```
  public_name = CRAM-MD5
  server_secret = ${extract{2}{:}{${lookup{$auth1}lsearch{CONFDIR/passwd}{$value}fail}}}
  server_set_id = $auth1
```

On doit laisser le mot de passe en clair dans le fichier de conf.

```
// salt limité aux charactères hexa (peut-être n'importe quelle chaîne sinon)
$ SALT=$(dd if=/dev/random bs=8 count=1 2>/dev/null | hexdump -v -e '/1 "%02X"')
$ CLAIR="clair"
$ CRYPT=$(mkpasswd --method=sha-256 --salt=$SALT $CLAIR)

# echo "login:$CRYPT:$PASS" >> /etc/exim4/passwd
# chown root:Debian-exim /etc/exim4/passwd
# chmod 640 /etc/exim4/passwd

# /etc/init.d/exim4 restart
```

Tout bien réfléchi, ça n'a pas de sens d'imposer l'authentififcation en entrée. Mieux vaut continuer à filter les relais via les IP : You can't force a remote client to attempt to authenticate, because you don't know until the RCPT TO : whether the client is attempting to deliver an email to your server (which doesn't require authentication unless you have a very unusual configuration like only accepting mail from known mail servers) or it is trying to relay through your mail server without authorisation. The RCPT TO stage of an SMTP session comes well after any AUTH negotiation (if any).

4 Courrier en sortie

fichier */etc/exim4/update-exim4.conf.conf* :

```
dc_eximconfig_configtype='internet'
dc_relay_domains=''
dc_relay_nets='192.168.2.0/24'
```

4.1 A destination extérieure

/etc/exim4/email-addresses

```
nroche: nroche@narval.tk
```

```
$ telnet 127.0.0.1 25
mail from: nroche@narval.tk
rcpt to: nicolasf.roche@gmail.com
data
test
.
250 OK id=1OQLVm-00032w-Qt
quit
```

4.2 Courrier en transit

Marche pas encore.

```
# exim_checkaccess 192.168.2.2 nicolasf.roche@gmail.com
Accepted

# tail /var/log/exim4/rejectlog
2010-06-20 16:23:55 H=(coyote) [192.168.2.2] F=<nroche@narval.tk> rejected RCPT nicolasf.roche@gmail
```

fichier */etc/exim4/conf.d/acl/30_exim4-config_check_rcpt*

```
...
acl_check_rcpt:

  # Accept if the source is local SMTP (i.e. not over TCP/IP). We do this by
  # testing for an empty sending host field.
  accept
    hosts = :
    hosts = +192.168.2.2
...
```

Remarque : Marche avec l'IN2P3 mais pas encore de réponse de gmail.

5 Pop3

```
# apt-get install dovecot-pop3d

$ telnet 127.0.0.1 pop3
+OK

user nroche
+OK
stat
-ERR

pass ****
+OK

list
+OK
1 1189
2 1104
3 888

quit
+OK
```

5.1 Pop3 + SSL

fournit par `dovecot-pop3d` (https ://wiki2.dovecot.org/TestInstallation)
/etc/dovecot/conf.d/10-ssl.conf

```
ssl = yes
ssl_cert = </etc/dovecot/dovecot.pem
ssl_key = </etc/dovecot/private/dovecot.pem
```

Test via le client `gnutls-cli`

```
# apt-get install gnutls-bin
$ gnutls-cli ovh.narval.fr.eu.org -p 995
...

$ openssl s_client -connect mail.narval.fr.eu.org:995
...
```

Ou via tunnel SSH

```
client$ ssh -i ~/key/id_rsa -L1234:www.narval.tk:110 prologue@www.narval.tk
server# tcpdump -i lo port 110 -AA
// garder la fenêtre ouverte (pas besoin d'ajouter de règle pour ufw)

client$ telnet localhost 1234
...
```

Il se peut que le certificat expire, ou que le nom de domaine change et qu'il faille regénérer le certificat :

```
$ openssl x509 -in /etc/dovecot/dovecot.pem -text -noout | less
$ openssl rsa -in /etc/dovecot/private/dovecot.pem -text -noout | less

# rm /etc/dovecot/dovecot.pem
# rm /etc/dovecot/private/dovecot.pem

// wheezy
# dpkg-reconfigure dovecot-core

// jessie
# cd /etc/dovecot
# cp /usr/share/dovecot/dovecot-openssl.cnf .
# sed -i dovecot-openssl.cnf \
   -e 's/@commonName@/ovh.narval.fr.eu.org/' \
   -e 's/@emailAddress@/nroche@narval.fr.eu.org/'
# /usr/share/dovecot/mkcert.sh
```

Depuis Thunderbird (icedove) 31.0, (marche avec autre client comme Evolution par exemple.)

- les certificats auto-signé de dovecot ne sont plus importés. Il faut aller dans l'onglet "sécurité" et les importer à la main.
- certains caractères UTF8 ne passent pas dans les mots de passes ex : `'ç` (https ://bugzilla.mozilla.org/show_bug.cgi?id=663814)

Rq : le fichier */etc/dovecot/conf.d/10-logging.conf* permet d'ajouter des obtions pour logguer les mot de passes reçus.

5.2 Pop3 + password

Pour passer le hash du mot de passe ("Encrypted Password" dans la conf de thunderbird), et pour remplacer les mot de passe système par d'autres. https ://wiki2.dovecot.org/HowTo/SimpleVirtualInstall

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

```
#auth_mechanisms = plain
auth_mechanisms = cram-md5

#!include auth-system.conf.ext
!include auth-passwdfile.conf.ext
```

/etc/dovecot/users

```
# LOGIN="login"
# PASS="clair"
# UID=1000
# GID=8 // mail

# cat >>/etc/dovecot/users <<EOF
```

```
$LOGIN:{PLAIN}$PASS:$UID:$GID::/home/$LOGIN::
EOF

# doveadm pw -s cram-md5

# cat >>/etc/dovecot/users <<EOF
$LOGIN:{CRAM-MD5}$PASS:$UID:$GID::/home/$LOGIN::
EOF

# chown root.dovecot /etc/dovecot/users
# chmod 640 /etc/dovecot/users

# /etc/init.d/dovecot restart
# tail -f /var/log/mail.log
```

6 Backup

Politique de sauvegarde des mails.

- Les mails importants sont systématiquement retirés des boîtes POP/IMAP et rangé dans le docciser "Local Folders" de thunderbird. (rq : cela suppose que l'on utilise toujours le même poste client)
- Le dossier local est duppliqué sur le poste client (rapide)

  ```
  $ rsync -av '/home/nroche/.icedove/nd070tqo.default/Mail/Local Folders' raid/Nico/mail/fred
  ```

- Puis la copie est duppliquée sur un serveur distant (long)

  ```
  $ rsync -av 'raid/Nico/mail/fred/Local Folder' ovh:rsync
  ```