



- TP 2 -
Messagerie (DNS, MTA, MUA)

par Édouard Lumet



Sommaire

1. Pré-requis (enregistrement DNS).....	3
2. Serveur SMTP.....	4
2.1. <i>Configuration basique</i>	4
2.2. <i>Utilisation des mails</i>	5
3. Serveurs POP/IMAP.....	6
4. Client de messagerie.....	8
5. SASL.....	9

1. Pré-requis (enregistrement DNS)

Pour commencer, il faut ajouter un enregistrement MX afin d'indiquer où se situe le serveur mail. Ma configuration DNS est maintenant la suivante :

```
$TTL 604800
@      IN      SOA    serveur.root.domaineel.rt. (
        4      ;Serial
        604800 ;Refresh
        86400  ;Retry
        2419200 ;Expire
        604800 ) ; Negative Cache TTL

@      IN      NS     serveur.domaineel.rt.
sous.domaineel.rt.  IN      NS     serveurdeux

serveur IN A 192.168.1.25

smtp CNAME serveur      #alias indiquant que smtp et serveur sont la même machine
@    MX      10 smtp     #enregistrement MX pointant vers la machine smtp
```

On modifie ensuite le fichier `/etc/hosts` pour redéfinir le nom de notre machine :

```
127.0.0.1    smtp.domaineel.rt smtp
```

2. Serveur SMTP

Le serveur SMTP que nous installons est *postfix* : **sudo apt-get install postfix**

2.1. Configuration basique

Le fichier de configuration Postfix */etc/postfix/main.cf* est le suivant :

```
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname

smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
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

readme_directory = no

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

home_mailbox = Maildir/
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = smtp.domaineel.rt
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = $myhostname, domaineel.rt., localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Les lignes mises en évidence sont respectivement l'emplacement de la boîte de réception et le nom de la machine.

2.2. Utilisation des mails

On peut désormais tester l'envoi de mail entre deux machines par exemple, avec la commande `mail edouard@smtp.domaineel.rt`.

On saisit ensuite l'objet, le corps du message puis on finit le mail par la séquence `retour chariot - . - retour chariot`

```
edouard@edouardMSI-pc:~$ ls -l Maildir/new/
total 16
-rw----- 1 edouard edouard 450 sept. 19 15:09 1474290598.V801I7802d5M525264.edouardMSI-pc
-rw----- 1 edouard edouard 457 sept. 19 15:24 1474291453.V801I7802d0M850991.edouardMSI-pc
-rw----- 1 edouard edouard 466 sept. 19 15:25 1474291513.V801I7802d8M186262.edouardMSI-pc
-rw----- 1 edouard edouard 641 sept. 19 15:38 1474292301.V801I7802ddM875750.edouardMSI-pc
```

```
edouard@edouardMSI-pc:~$ cat Maildir/new/1474292301.V801I7802ddM875750.edouardMSI-pc
Return-Path: <admin@localhost>
```

```
X-Original-To: edouard@smtp.domaineel.rt
Delivered-To: edouard@smtp.domaineel.rt
Received: from antenn04.univ-lr.fr (unknown [192.168.1.4])
        by smtp.domaineel.rt (Postfix) with ESMTP id CAB497802DC
        for <edouard@smtp.domaineel.rt>; Mon, 19 Sep 2016 15:38:21 +0200 (CEST)
```

```
Received: by antenn04.univ-lr.fr (Postfix, from userid 1000)
        id 78C14722FA8; Mon, 19 Sep 2016 15:38:03 +0200 (CEST)
```

```
To: <edouard@smtp.domaineel.rt>
```

```
Subject: t
```

```
X-Mailer: mail (GNU Mailutils 2.99.98)
```

```
Message-Id: <20160919133803.78C14722FA8@antenne04.univ-lr.fr>
```

```
Date: Mon, 19 Sep 2016 15:38:03 +0200 (CEST)
```

```
From: admin@localhost
```

```
sdgfd
```

On voit ici les mails présents dans la boîte de réception puis l'en-tête et le contenu d'un mail envoyé de 192.168.0.4 à edouard@smtp.domaineel.rt.

Cet échange est illustré par la capture Wireshark ci-dessous. La première machine envoie une requête DNS pour un enregistrement MX concernant `smtp.domaineel.rt`, réponse obtenue en 2 temps puisque `smtp` est un alias de `serveur`. Ensuite, une connexion TCP est établie pour encadrer les échanges SMTP.

```
192.168.1.4 192.168.1.25 DNS Standard query 0x15aa MX smtp.domaineel.rt
192.168.1.25 192.168.1.4 DNS Standard query response 0x15aa MX smtp.domaineel.rt CNAME serveur.domaineel.rt SOA serveur.domaineel.rt
192.168.1.4 192.168.1.25 DNS Standard query 0x5df0 MX serveur.domaineel.rt
192.168.1.25 192.168.1.4 DNS Standard query response 0x5df0 MX serveur.domaineel.rt SOA serveur.domaineel.rt
192.168.1.4 192.168.1.25 DNS Standard query 0xa7f4 A smtp.domaineel.rt
192.168.1.25 192.168.1.4 DNS Standard query response 0xa7f4 A smtp.domaineel.rt CNAME serveur.domaineel.rt A 192.168.1.25 NS serveur.domaineel.rt
192.168.1.4 192.168.1.25 DNS Standard query 0xb8fb AAAA smtp.domaineel.rt
192.168.1.25 192.168.1.4 DNS Standard query response 0xb8fb AAAA smtp.domaineel.rt CNAME serveur.domaineel.rt SOA serveur.domaineel.rt
192.168.1.4 192.168.1.25 DNS Standard query 0xd516 AAAA serveur.domaineel.rt
192.168.1.25 192.168.1.4 DNS Standard query response 0xd516 AAAA serveur.domaineel.rt SOA serveur.domaineel.rt
192.168.1.4 192.168.1.25 TCP 47237 -> 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1003789 TSecr=0 WS=128
192.168.1.25 192.168.1.4 TCP 25 -> 47237 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=990787 TSecr=1003789 WS=128
192.168.1.4 192.168.1.25 TCP 47237 -> 25 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1003789 TSecr=990787
192.168.1.25 192.168.1.4 SMTP S: 220 smtp.domaineel.rt ESMTP Postfix (Ubuntu)
192.168.1.4 192.168.1.25 TCP 47237 -> 25 [ACK] Seq=1 Ack=47 Win=29312 Len=0 TSval=1003848 TSecr=990846
192.168.1.4 192.168.1.25 SMTP C: EHLO antenn04.univ-lr.fr
192.168.1.25 192.168.1.4 TCP 25 -> 47237 [ACK] Seq=47 Ack=28 Win=29056 Len=0 TSval=990846 TSecr=1003848
192.168.1.25 192.168.1.4 SMTP S: 250 smtp.domaineel.rt | 250 PIPELINING | 250 SIZE 10240000 | 250 VRFY | 250 ETRN | 250 STARTTLS | 250 ENHANCEDSTAT
192.168.1.4 192.168.1.25 SMTP C: MAIL FROM:<admin@localhost> SIZE=349 | RCPT TO:<edouard@smtp.domaineel.rt> ORCPT=rfc822;edouard@smtp.domaineel.rt
192.168.1.25 192.168.1.4 SMTP S: 250 2.1.0 Ok | 250 2.1.5 Ok | 354 End data with <CR><LF>.<CR><LF>
192.168.1.4 192.168.1.25 IMF subject: t, from: admin@localhost, , sgdgfd , ..
192.168.1.25 192.168.1.4 TCP 25 -> 47237 [ACK] Seq=252 Ack=507 Win=30080 Len=0 TSval=990858 TSecr=1003851
192.168.1.25 192.168.1.4 SMTP S: 250 2.0.0 Ok: queued as CAB497802DC | 221 2.0.0 Bye
192.168.1.4 192.168.1.25 TCP 47237 -> 25 [FIN, ACK] Seq=507 Ack=304 Win=30336 Len=0 TSval=1003861 TSecr=990858
192.168.1.25 192.168.1.4 TCP 25 -> 47237 [FIN, ACK] Seq=304 Ack=508 Win=30080 Len=0 TSval=990858 TSecr=1003861
192.168.1.4 192.168.1.25 TCP 47237 -> 25 [ACK] Seq=508 Ack=305 Win=30336 Len=0 TSval=1003861 TSecr=990858
```

3. Serveurs POP/IMAP

Le serveur POP/IMAP que nous allons utiliser est *dovecot* : **sudo apt-get install dovecot-imapd dovecot-pop3d**

Dans un premier temps on indique à Dovecot que les mails sont dans le dossier ~/Maildir :

```
##
## Mailbox locations and namespaces
##
[...]
```

There are a few special variables you can use, eg.:

```
#
# %u - username
# %n - user part in user@domain, same as %u if there's no domain
# %d - domain part in user@domain, empty if there's no domain
# %h - home directory
#
# See doc/wiki/Variables.txt for full list. Some examples:
#
# mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
#
# <doc/wiki/MailLocation.txt>
#
mail_location = maildir:~/Maildir
```

Chaque utilisateur système (UNIX) aura donc un répertoire *Maildir* dans son home où seront stockés les mails entrants.

Ci-dessous, on peut observer des échanges Telnet afin de consulter la boîte mail via IMAP.

```
edouard@edouardMSI-pc:~$ telnet smtp.domaineel.rt 143
Trying 127.0.0.1...
Connected to smtp.domaineel.rt.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN] Dovecot ready.
a001 login utilisateur 1234
a001 OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=RNATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARC
n
```

Le premier encadré correspond à la commande Bash pour se connecter en Telnet au serveur IMAP. Le second encadré est une commande insérée dans la session Telnet pour se connecter avec le login *utilisateur* et le mot de passe correspondant.

En haut de la page suivante, on peut voir quelques commandes concernant la consultation de mails. *select inbox* permet de consulter la boîte mail et *fetch 1 body[header]* permet de visualiser l'en-tête du message numéro 1.

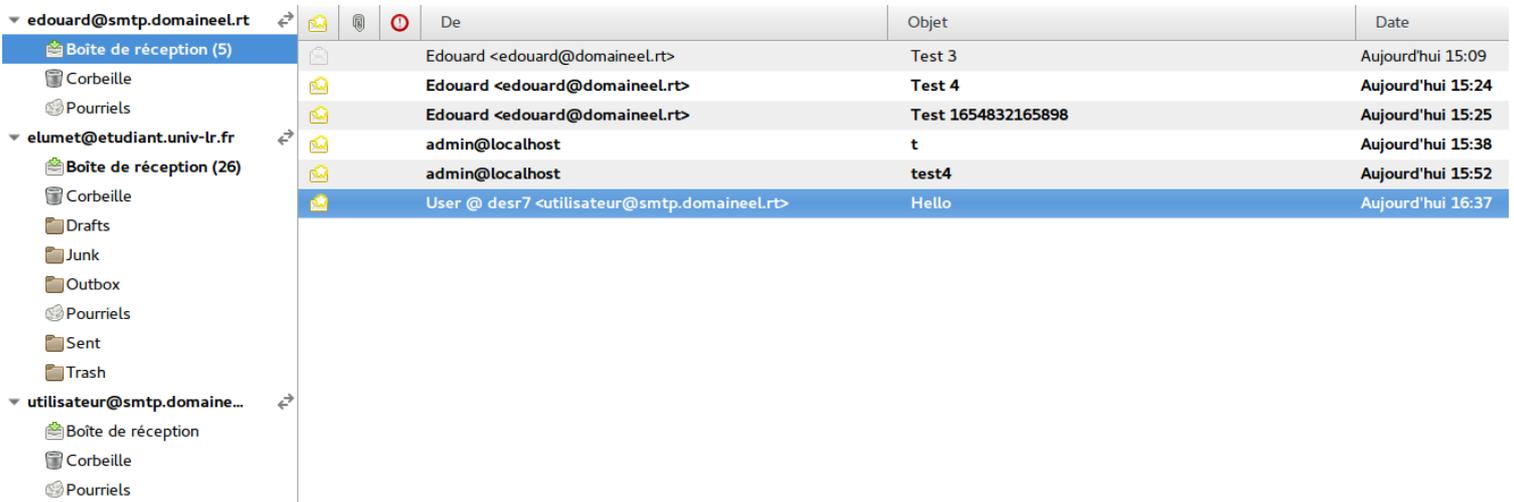
```
a003 select inbox
* OK [CLOSED] Previous mailbox closed.
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 1 EXISTS
* 0 RECENT
* OK [UNSEEN 1] First unseen.
* OK [UIDVALIDITY 1474294051] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
* OK [HIGHESTMODSEQ 2] Highest
a003 OK [READ-WRITE] Select completed (0.000 + 0.000 secs).
```

```
a004 fetch 1 body
* 1 FETCH (BODY ("text" "plain" ("charset" "us-ascii") NIL NIL "7bit" 4 1))
a004 OK Fetch completed (0.001 + 0.000 secs).
```

```
a005 fetch 1 body[header]
* 1 FETCH (FLAGS (\Seen) BODY[HEADER] {646}
Return-Path: <edouard@stmp.domaineel.rt>
X-Original-To: utilisateur@smtp.domaineel.rt
Delivered-To: utilisateur@smtp.domaineel.rt
Received: from smtp.domaineel.rt (smtp.domaineel.rt [127.0.0.1])
        by smtp.domaineel.rt (Postfix) with ESMTP id 4C57278036D
        for <utilisateur@smtp.domaineel.rt>; Mon, 19 Sep 2016 16:08:20 +0200 (CEST)
Message-ID: <1474294100.13522.0.camel@stmp.domaineel.rt>
Subject: Test
From: Edouard <edouard@stmp.domaineel.rt>
To: utilisateur@smtp.domaineel.rt
Date: Mon, 19 Sep 2016 16:08:20 +0200
Content-Type: text/plain
X-Mailer: Evolution 3.18.5.2-0ubuntu3
Mime-Version: 1.0
Content-Transfer-Encoding: 7bit
)
a005 OK Fetch completed (0.001 + 0.000 secs).
```

4. Client de messagerie

On paramètre notre serveur de messagerie sur un client comme *Thunderbird*. Ici, sous Ubuntu Gnome, le MUA s'appelle *Évolution*.



De	Objet	Date
Edouard <edouard@domaineel.rt>	Test 3	Aujourd'hui 15:09
Edouard <edouard@domaineel.rt>	Test 4	Aujourd'hui 15:24
Edouard <edouard@domaineel.rt>	Test 1654832165898	Aujourd'hui 15:25
admin@localhost	t	Aujourd'hui 15:38
admin@localhost	test4	Aujourd'hui 15:52
User @ desr7 <utilisateur@smtp.domaineel.rt>	Hello	Aujourd'hui 16:37

Les messages ont bien été récupérés par le client de messagerie depuis le serveur de messagerie entrant, pour l'utilisateur *edouard*. 3 expéditeurs différents sont visibles : les trois premiers mails sont des mails envoyés en local (de *edouard* vers *edouard*) ; les deux suivants proviennent d'un voisin qui a pour DNS le serveur de noms installé sur cette machine et contenant l'enregistrement MX pour *domaineel.rt*) ; le dernier mail a été envoyé en local mais depuis un autre utilisateur système.

5. SASL

Cette ultime configuration permet de restreindre l'accès au serveur sortant aux utilisateurs existants. En effet, si le serveur ne requiert pas d'authentification, n'importe qui peut envoyer un mail au nom de edouard@smtp.domaineel.rt par exemple. Dans le client de messagerie, après configuration de SASL, on remarque désormais que l'on peut s'authentifier auprès du serveur sortant :

Éditeur de comptes [X]

Identité

Réception du courriel

Options de réception

Envoi du courriel

Valeurs par défaut

Sécurité

Type de serveur : **SMTP**

Description : Pour la distribution du courriel via un serveur de courriel distant utilisant SMTP.

Configuration

Serveur : Port : ▼

Le serveur requiert une authentification

Sécurité

Méthode de chiffrement : ▼

Authentification

Type : ▼

Nom d'utilisateur :

Annuler Valider