Table des matières

Avant-Propos

E6 :

Elaboration de documents relatifs à la production et à la fourniture de services
A1.1.1 , Analyse du cahier des charges d'un service à produire
A1.2.4 , Détermination des tests nécessaires à la validation d'un service
A1.3.4 , Déploiement d'un service
A4.1.9 , Rédaction d'une documentation technique

A faire en premier

Il faut un serveur DNS primaire opérationnel (fichier named.conf.local, dir.dupont.local et rev.192.168.1)

Il faut ajouter les lignes suivantes dans la zone de recherche directe.

```
dupont.local. MX 10 Mail
```

```
webmail IN CNAME Mail_
```

Installation Postfix

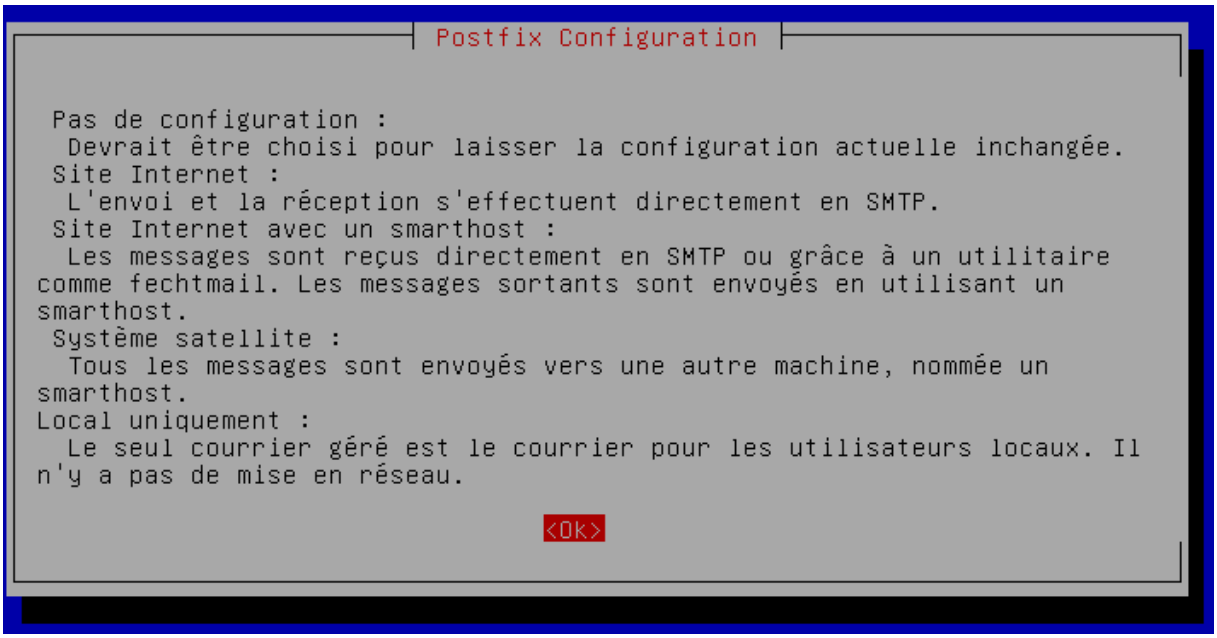
Premièrement, il faut supprimer les paquets inutiles (exim4 est un service de mail installé par défaut, pour éviter les conflits on le supprime) :

```
root@Mail:~# apt-get --purge remove exim4 exim4-base exim4-config exim4-daemon-l
ight_
```

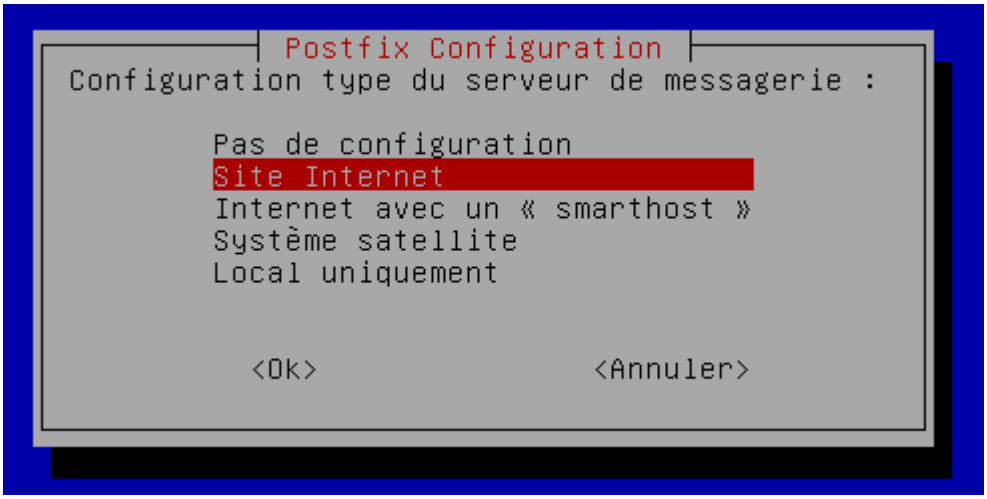
Puis on rentre la commande suivante pour installer le service :

```
root@Mail:~# apt-get install postfix_
```

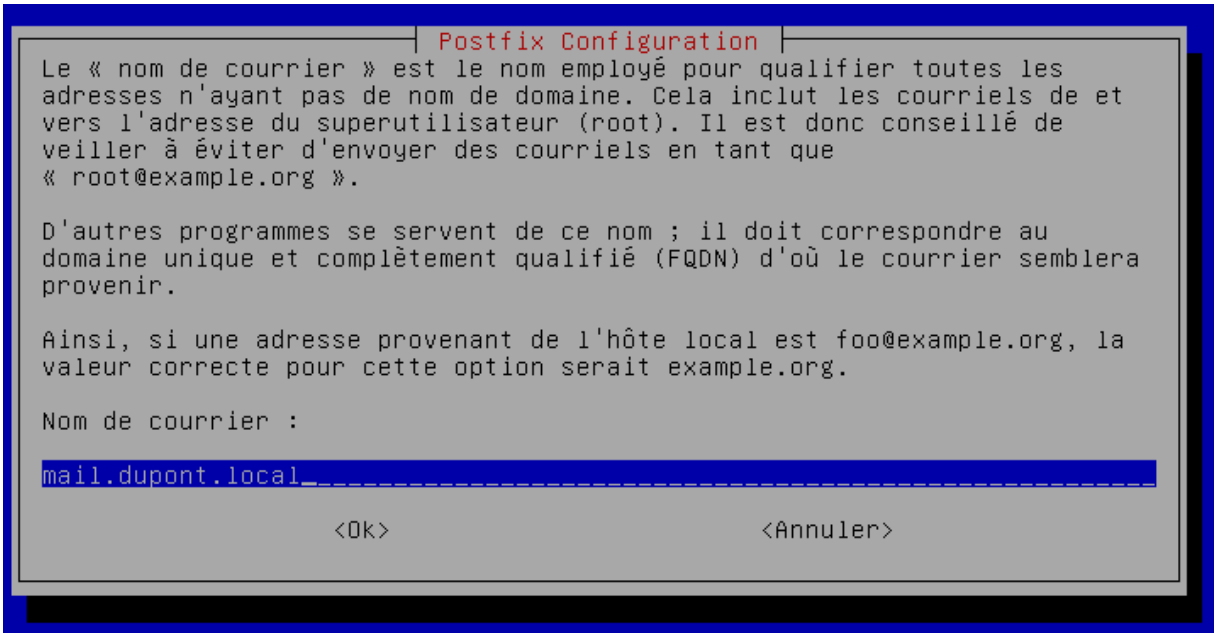
Pendant l'installation, on va nous poser des questions.



Ici il faut juste répondre OK.



Ici il faut choisir Site Internet.



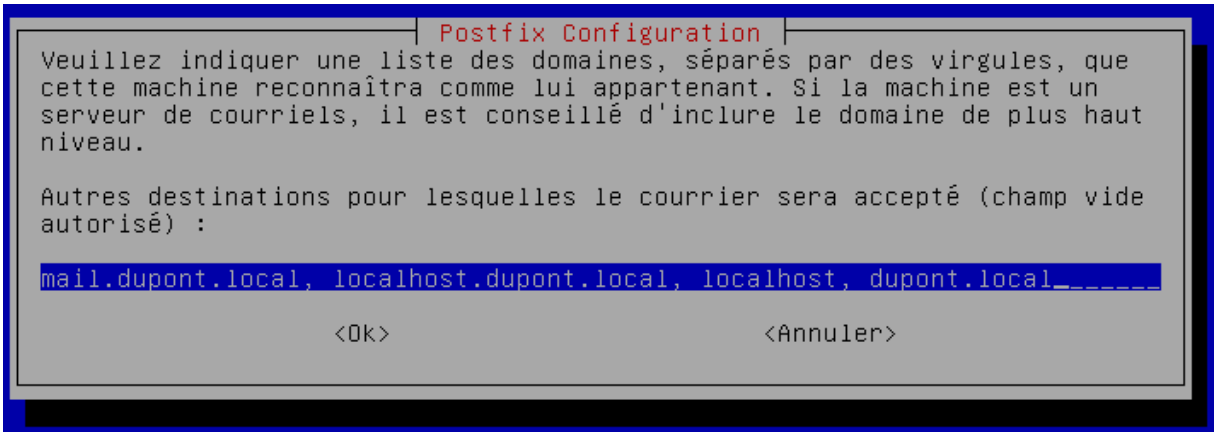
Ici il faut rentrer l'adresse mail.

Ensuite on utilise la commande :

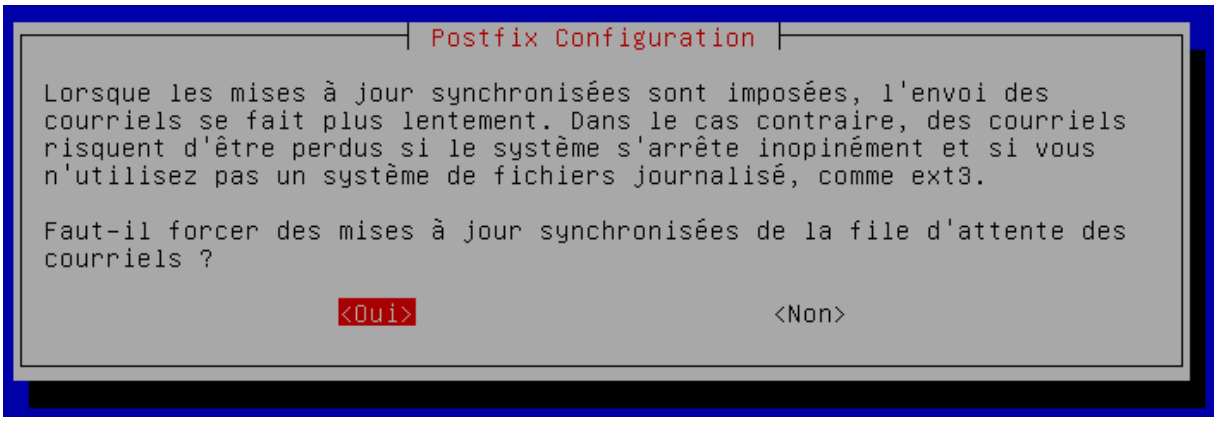
```
root@Mail:~# dpkg-reconfigure postfix_
```

Cette commande sert à configurer des choses que l'on n'a pas renseigné pendant l'installation.

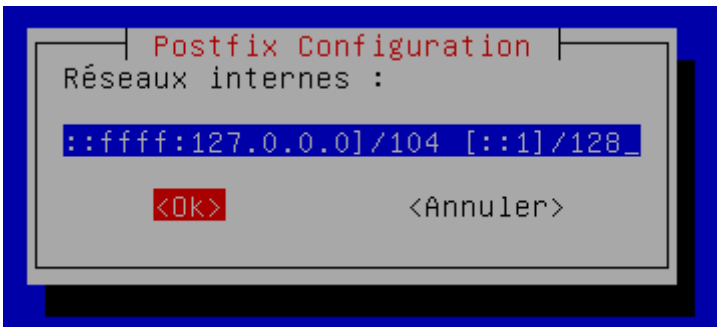
On rentre une adresse mail pour le root.



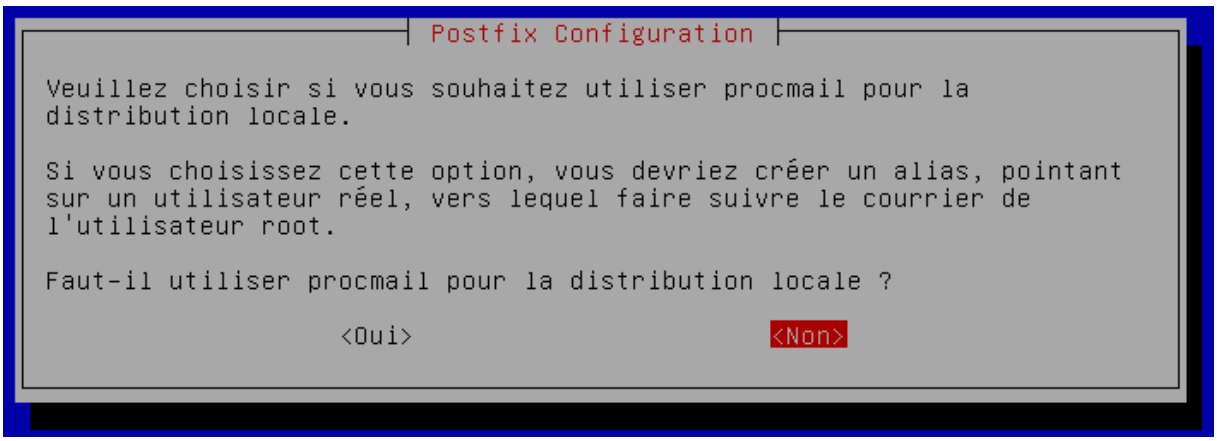
Il faut rentrer ces informations qui sont fournies dans le TP.



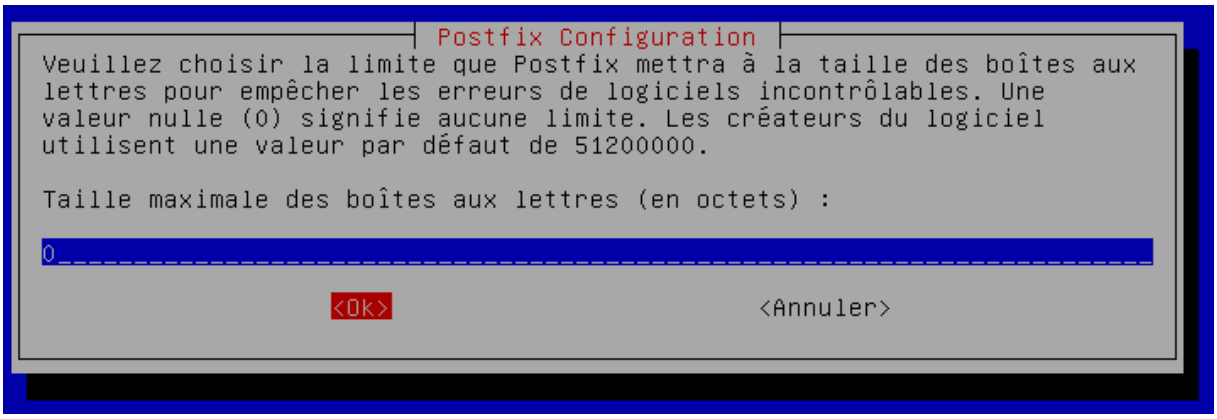
Il faut mettre oui.



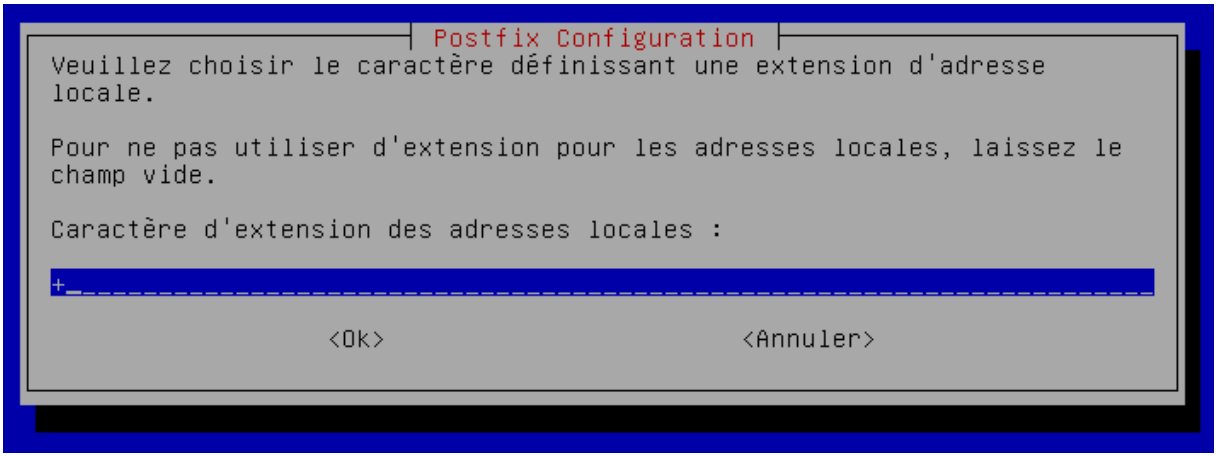
Il faut laisser ce qui est de base.



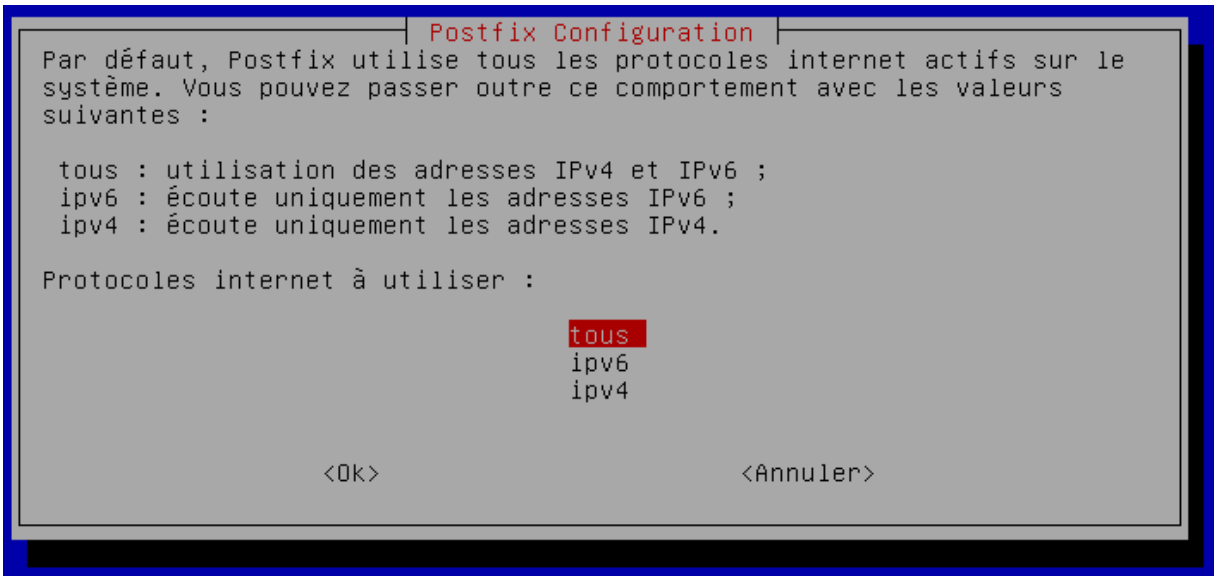
Il faut mettre non.



On laisse 0 octets.



On laisse le +.



On met tous.

Maintenant nous allons éditer le fichier /etc/postfix/main.cf

```
root@Mail:~# nano /etc/postfix/main.cf
```

Il faut modifier les lignes suivantes :

```
myhostname = Mail.dupont.local_
```

```
mydestination = mail, mail.dupont.local, localhost.dupont.local, localhost, dup$
```

```
inet_interfaces = localhost_
```

```
inet_interfaces = all_
inet_protocols = ipv4
```

Et on ajoute la ligne suivante :

```
home_mailbox = MailDir/_
```

Ensuite on enregistre le fichier et on quitte. On peut voir les configurations en marquant la commande suivante :

```
root@Mail:~# postconf -n_
```

On redémarre le servie postfix :

```
root@Mail:~# service postfix restart_
```

Maintenant que le service est installé, nous allons envoyer des mails.

Pour ce faire, on se connecte en telnet sur la machine avec la commande suivante, le 25 étant le port du SMTP.

```
root@Mail:~# telnet Mail.dupont.local 25_
```

Il faut ensuite rentrer les informations suivantes, si c'est mal noté un message d'erreur nous le signalera.

```
mail from:toto
250 2.1.0 Ok
rcpt to:anthony
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Bonjour, je souhaiterais être ton ami
.
250 2.0.0 Ok: queued as 1071F5FA
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Ensuite, on va dans le dossier MailDir de l'user auquel on a envoyé le message.

```
root@Mail:~# cd /home/anthony/MailDir/
root@Mail:/home/anthony/MailDir# ls
cur  new  tmp
root@Mail:/home/anthony/MailDir# cd new/
root@Mail:/home/anthony/MailDir/new# ls
1479713558.V806I12M604185.Mail
```

On lit ensuite le mail et on peut voir que cela fonctionne !

```
Return-Path: <toto@mail.dupont.local>
X-Original-To: anthony
Delivered-To: anthony@mail.dupont.local
Received: from Mail.dupont.local (Mail.dupont.local [192.168.1.128])
        by Mail.dupont.local (Postfix) with SMTP id 1071F5FA
        for <anthony>; Mon, 21 Nov 2016 08:32:03 +0100 (CET)
Message-Id: <20161121073213.1071F5FA@Mail.dupont.local>
Date: Mon, 21 Nov 2016 08:32:03 +0100 (CET)
From: toto@mail.dupont.local

Bonjour, je souhaiterais être ton ami
```

Pour tester la syntaxe du fichier /etc/postfix/main.cf

```
root@Mail:/home/anthony/MailDir/new# /etc/init.d/postfix check
```

Le courrier de l'utilisateur root est dirigé vers un autre compte. Vous pouvez utiliser les alias dans le fichier /etc/aliases (root : notre_prenom). Utiliser la commande newaliases pour valider.

Maintenant il faut transformer le serveur pour un domaine. Dovecot est un serveur IMAP et POP3 :

```
root@Mail:/home/anthony/MailDir/new# apt-get install dovecot-common dovecot-pop3
d_
```

Il faut ensuite modifier les choses suivantes les fichiers de configuration qui correspondent.

```
root@Mail:/home/anthony/MailDir/new# nano /etc/dovecot/conf.d/10-auth.conf _
```

```
disable_plaintext_auth = no_
```

```
root@Mail:/home/anthony/MailDir/new# nano /etc/dovecot/conf.d/20-pop3.conf _
```

```
pop3_uidl_format = %08Xu%08Xv
```

```
root@Mail:/home/anthony/MailDir/new# nano /etc/dovecot/conf.d/10-mail.conf _
```

```
mail_location = maildir:/home/%u/MailDir_
```

Une fois cela fait, on redémarre le service

```
root@Mail:/home/anthony/MailDir/new# service dovecot reload_
```

Pour tester, on se connecte avec un utilisateur en telnet sur le port 110, et on peut voir les mails de cet utilisateur.

```
root@Mail:/home/anthony/MailDir/new# telnet Mail.dupont.local 110
Trying 192.168.1.128...
Connected to Mail.dupont.local.
Escape character is '^]'.
+OK Dovecot ready.
user anthony
+OK
pass anthony
+OK Logged in.
list
+OK 1 messages:
1 458
.
retr 1
```

```
+OK 458 octets
Return-Path: <toto@mail.dupont.local>
X-Original-To: anthony
Delivered-To: anthony@mail.dupont.local
Received: from Mail.dupont.local (Mail.dupont.local [192.168.1.128])
        by Mail.dupont.local (Postfix) with SMTP id 1071F5FA
        for <anthony>; Mon, 21 Nov 2016 08:32:03 +0100 (CET)
Message-Id: <20161121073213.1071F5FA@Mail.dupont.local>
Date: Mon, 21 Nov 2016 08:32:03 +0100 (CET)
From: toto@mail.dupont.local

Bonjour, je souhaiterais être ton ami
.
```

On installe ensuite un serveur IMAP.

```
root@Mail:/home/anthony/MailDir/new# apt-get install dovecot-imapd_
```

Le webmail

Pour avoir le webmail, il faut installer :

-Un Serveur Web Apache
-Le language PHP 4 ou 5
-Un Serveur SMTP
-Un Serveur IMAP

Nous allons donc installer apache et php, sachant que l'on a précédemment installé le reste.

```
root@Mail:/home/anthony/MailDir/new# apt-get install apache2_
```

```
root@Mail:/home/anthony/MailDir/new# apt-get install php5_
```

Une fois cela fait, on installe squirrelmail.

```
root@Mail:/var/www/html# apt-get install squirrelmail_
```

Maintenant nous allons configurer squirrelmail.

```
root@Mail:/var/www/html# squirrelmail-configure_
```

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> 2_
```

```
Server Settings

General
-------
1.  Domain                : trim(implode('', file('/etc/'.(file_exists('/etc/ma
ilname')?'mail':'host').'name')))
2.  Invert Time           : false
3.  Sendmail or SMTP      : SMTP

A.  Update IMAP Settings  : localhost:143 (other)
B.  Update SMTP Settings  : localhost:25

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> A_
```

```
General
-------
1.  Domain                 : trim(implode('', file('/etc/'.(file_exists('/etc/ma
ilname')?'mail':'host').'name')))
2.  Invert Time            : false
3.  Sendmail or SMTP       : SMTP

IMAP Settings
--------------
4.  IMAP Server            : localhost
5.  IMAP Port              : 143
6.  Authentication type    : login
7.  Secure IMAP (TLS)      : false
8.  Server software        : other
9.  Delimiter              : detect

B.  Update SMTP Settings   : localhost:25
H.  Hide IMAP Server Settings

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> 8_
```

```
Each IMAP server has its own quirks.  As much as we tried to stick
to standards, it doesn't help much if the IMAP server doesn't follow
the same principles.  We have made some work-arounds for some of
these servers.  If you would like to use them, please select your
IMAP server.  If you do not wish to use these work-arounds, you can
set this to "other", and none will be used.
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts
    other       = Not one of the above servers
[other]: dovecot_
```

```
R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> S_
```

On peut modifier pleins d'autres choses aussi.

Pour mettre l'UFT-8 :

```
$languages['fr_FR']['NAME']    = 'French';
$languages['fr_FR']['CHARSET'] = 'UTF-8';
$languages['fr_FR']['LOCALE']  = array('fr_FR.UTF-8','fr_FR.UTF-8','fr_FR');
$languages['fr']['ALIAS']      = 'fr_FR';
```

Il faut ensuite installer le paquet suivant pour avoir la traduction des messages :

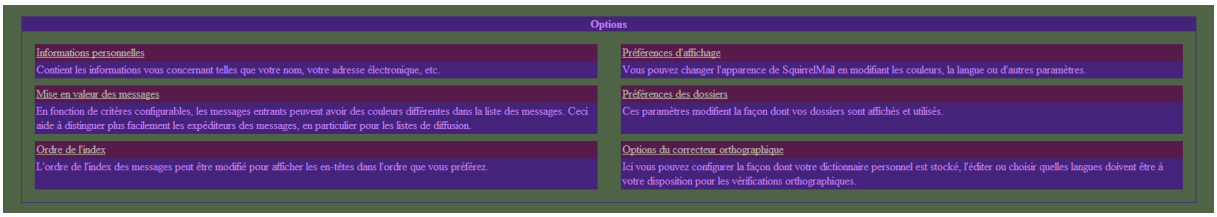
```
root@Mail:/var/www/html# aptitude install squirrelmail-locales_
```

Il faut maintenant créer un lien symbolique avec Apache 2 :

```
root@Mail:/var/www/html# ln -s /usr/share/squirrelmail/ squirrel_
```

Une fois que l'on est connecté, on peut voir nos mails.

Pour configurer les couleurs de l'interface, rajouter des plugins, ou tout simplement configurer le webmail, il faut aller dans Option en haut de l'écran, et ensuite on peut choisir ce que l'on veut modifier.



Par exemple, j'ai modifié le thème pour que les couleurs changent aléatoirement sur chaque page, et dès que je les rafraichis.

Seuls les utilisateurs ayant un compte sur le serveur de mail auront la possibilité d'utiliser Squirrelmail. Pour créer un compte uniquement destiné à la messagerie, sans possibilité de connections sur le serveur, il faut d'abord créer un groupe d'utilisateur dédié à l'utilisation de Squirrelmail.

```
root@Mail:~# groupadd squirrelmail
```

Puis créer chaque utilisateur par l'instruction suivante :

```
root@Mail:~# useradd -c "utilisateur" -s /bin/false -g squirrelmail utilisateur
```

Enfin définir un mot de passe pour chaque compte nouvellement créé :

```
root@Mail:~# passwd utilisateur
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
```

J'ai mis comme mot de passe « utilisateur ». Maintenant il faut créer le répertoire personnel de l'utilisateur afin que les mails puissent être stockés dedans.

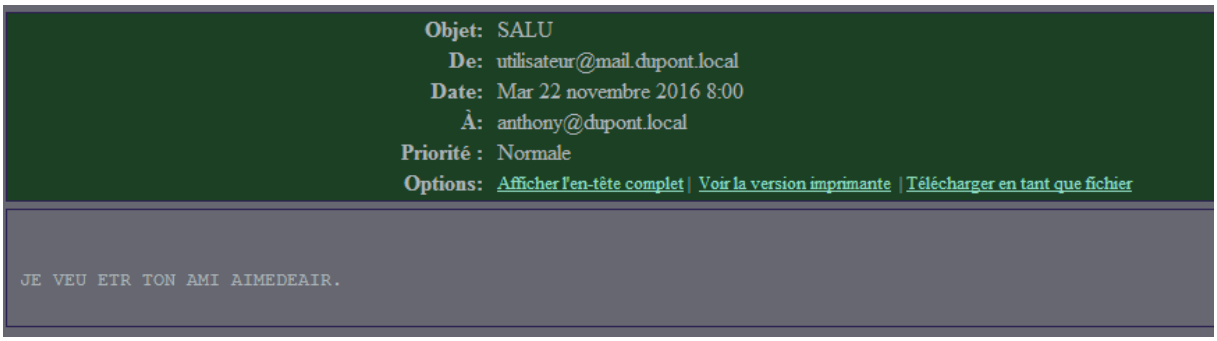
```
root@Mail:/home# mkdir utilisateur_
```

Puis on indique que ce dossier est le répertoire personnel de l'utilisateur.

```
root@Mail:~# chown utilisateur.squirrelmail /home/utilisateur_
```

Maintenant, on peut se connecter avec l'utilisateur que l'on vient de créer.

Pour faire un test, j'envoie un mail sur l'adresse anthony@dupont.local, et quand je me connecte dessus on peut voir que je l'ai bien reçu !



Sécurisation du serveur de courriers

Nous allons installer un anti-virus afin de sécuriser notre serveur de courriers. ClamAV est un logiciel antivirus pour UNIX. Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant un virus.

```
root@Mail:/home# apt-get install amavisd-new spamassassin clamav clamav-daemon z
oo unzip bzip2 arj nomarch lzop cabextract apt-listchanges libnet-ldap-perl liba
uthen-sasl-perl clamav-docs daemon libio-string-perl libio-socket-ssl-perl libne
t-ident-perl zip libnet-dns-perl p7zip unrar-free_
```

Il faut ensuite aller dans /etc/postfix/master.cf et ajouter les lignes suivantes :

```
amavis  unix    -       -       -       -       2       smtp
  -o smtp_data_done_timeout=1200
  -o smtp_send_xforward_command=yes
  -o disable_dns_lookups=yes
  -o max_use=20

127.0.0.1:10025 inet    n       -       -       -       -       smtpd
  -o content_filter=
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_delay_reject=no
  -o smtpd_client_restrictions=permit_mynetworks,reject
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o smtpd_data_restrictions=reject_unauth_pipelining
  -o smtpd_end_of_data_restrictions=
  -o mynetworks=127.0.0.0/8
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
  -o smtpd_client_connection_count_limit=0
  -o smtpd_client_connection_rate_limit=0
  -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Il faut faire bien attention aux tabulations et aux espaces !

Il faut ensuite ajouter la ligne suivante à la fin du fichier (ou au début si ça marche pas) /etc/postfix/main.cf

```
content_filter = amavis:[127.0.0.1]:10024
```

Pour activer les filtres Amavis, il faut éditer le fichier /etc/amavis/conf.d/15-content_filter_mode et décommenter les lignes @bypass :

```
@bypass_virus_checks_maps = (
   \%bypass_virus_checks, \@bypass_virus_checks_acl, \$bypass_virus_checks_re);
```

```
@bypass_spam_checks_maps = (
   \%bypass_spam_checks, \@bypass_spam_checks_acl, \$bypass_spam_checks_re);
```

Pour configurer la mise en quarantaine, on édite le fichier /etc/amavis/conf.d/50-user et modifier les lignes pour la mise en quarantaine.

```
$QUARANTINEDIR = '/var/spool/virusmails';              # Répertoire de quaranta$
$spam_quarantine_method = 'local:spam-%b-%i-%n'; # Nom du fichier dans $QUARANT$
$spam_quarantine_to = 'spam-quarantine';         # Mettre le Spam dans Quaranti$
$final_spam_destiny = D_DISCARD;
$spam_admin = "admin\@$mydomain";          # A qui notifier
```

Ensuite on créer le répertoire /var/spool/virusmails et ensuite on le fait appartenir à l'utilisateur amavis du groupe du même nom.

```
root@Mail:/home/anthony# mkdir /var/spool/virusmails
```

Puis on modifier les droits :

```
root@Mail:/var/spool# chown amavis virusmails/
root@Mail:/var/spool# chgrp amavis virusmails/
```

On fait ensuite la mise à jour des règles de SpamAssassin :

```
root@Mail:/var/spool# sa-update -D
```

On active ensuite SpamAssassin en éditant le fichier /etc/default/spamassassin

Ce fichier permet d'activer SpamAssassin et de permettre la mise à jour par une tâche cron.

```
# Change to "1" to enable spamd on systems using sysvinit:
ENABLED=1
```

```
OPTIONS="--create-prefs --max-children 5 --helper-home-dir"
```

```
# spamassassin's rules on a nightly basis
CRON=1
```

Ensuite on ajoute l'utlisateur clamav au groupe amavis.

```
root@Mail:/var/spool# adduser clamav amavis
Ajout de l'utilisateur « clamav » au groupe « amavis »...
Ajout de l'utilisateur clamav au groupe amavis
Fait.
```

Maintenant nous allons démarrer les services spamassassin, amavis et clamav-daemon :

```
root@Mail:/var/spool# systemctl start spamassassin
```

```
root@Mail:/var/spool# systemctl start amavis
root@Mail:/var/spool# systemctl start clamav-daemon
```

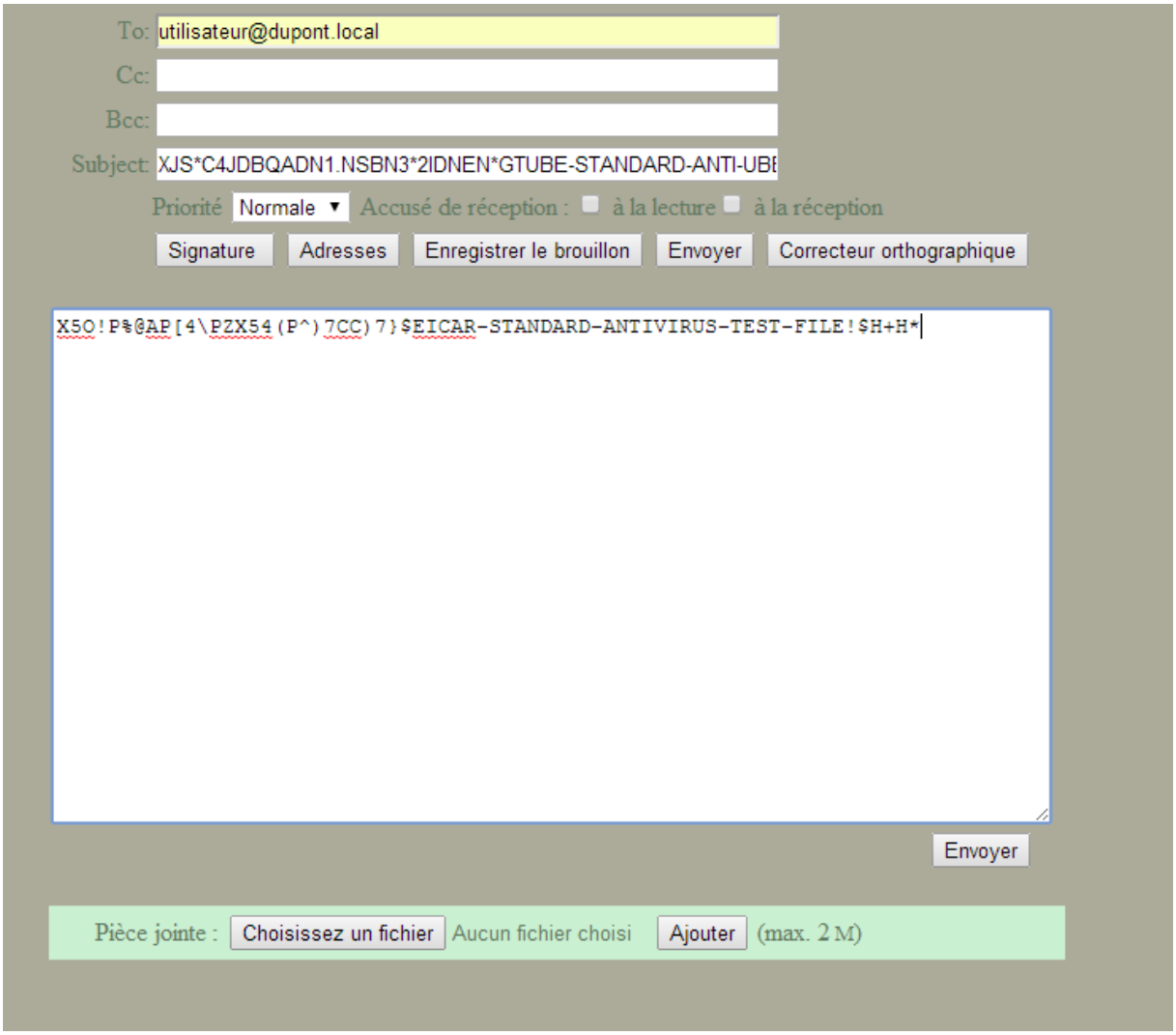
Ensuite on redémarre Postfix :

```
root@Mail:/var/spool# systemctl restart postfix
```

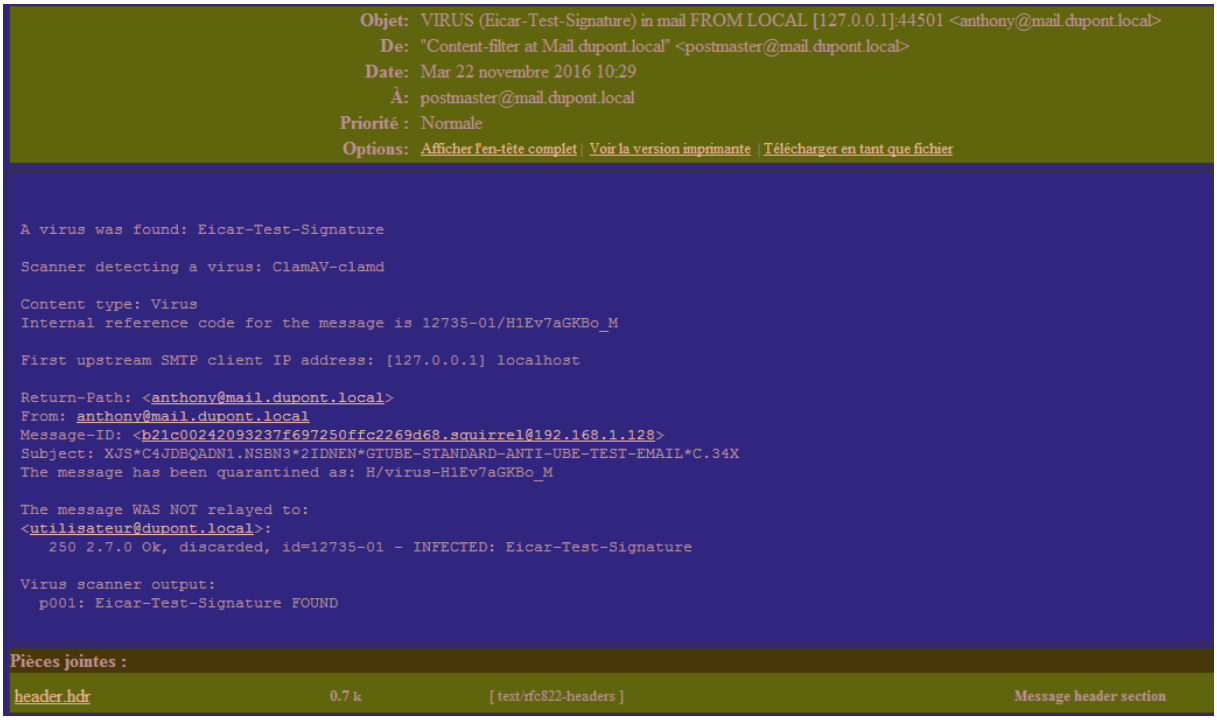
Pour tester SpamAssassin, on peut trouver des exemples de spam dans /usr/share/doc/spamassassin/examples/sample-spam.txt

Il faut copier la ligne suivante et l'envoyer par mail.

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```



Une fois que ce mail est envoyé, on en reçoit automatiquement un pour nous signaler qu'il a été considéré comme spam et qu'il ne sera pas envoyé !



Objet: VIRUS (Eicar-Test-Signature) in mail FROM LOCAL [127.0.0.1]:44501 <anthony@mail.dupont.local>
De: "Content-filter at Mail.dupont.local" <postmaster@mail.dupont.local>
Date: Mar 22 novembre 2016 10:29
À: postmaster@mail.dupont.local
Priorité : Normale
Options: Afficher l'en-tête complet | Voir la version imprimante | Télécharger en tant que fichier

```
A virus was found: Eicar-Test-Signature

Scanner detecting a virus: ClamAV-clamd

Content type: Virus
Internal reference code for the message is 12735-01/H1Ev7aGKBo_M

First upstream SMTP client IP address: [127.0.0.1] localhost

Return-Path: <anthony@mail.dupont.local>
From: anthony@mail.dupont.local
Message-ID: <b21c00242093237f697250ffc2269d68.squirrel@192.168.1.128>
Subject: XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
The message has been quarantined as: H/virus-H1Ev7aGKBo_M

The message WAS NOT relayed to:
<utilisateur@dupont.local>:
   250 2.7.0 Ok, discarded, id=12735-01 - INFECTED: Eicar-Test-Signature

Virus scanner output:
  p001: Eicar-Test-Signature FOUND
```

Pièces jointes :

header.hdr 0.7 k [text/rfc822-headers] Message header section