**Lab 4 : Serveur Mail**

## Configuration de la base de données utilisateurs :

* Ajouter un enregistrement MX dans le serveur dns

Dans Zeus tapez :

**nsupdate -k /etc/bind/ddns.key**

**server 127.0.0.1**

**zone equitable.net**

**update add equitable.net 36000 IN MX 10 aphrodite.equitable.net.**

**update add aphrodite.equitable.net. 600 cname mail.equitable.net.**

**send**

A screenshot of a computer

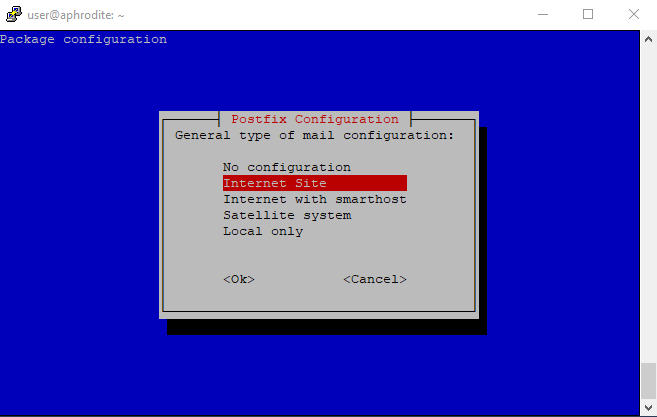
AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

* Installer les services (APHRODITE)

**apt-get update && apt-get upgrade**

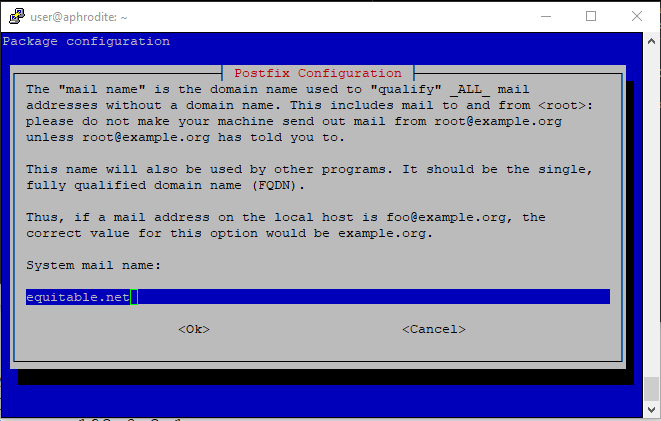
**apt-get install apache2 php php-common mariadb-server postfix postfix-mysql libsasl2-modules sasl2-bin dovecot-mysql php-mysql php-imap php-mbstring dovecot-pop3d dovecot-imapd dovecot-managesieved libapache2-mod-php**



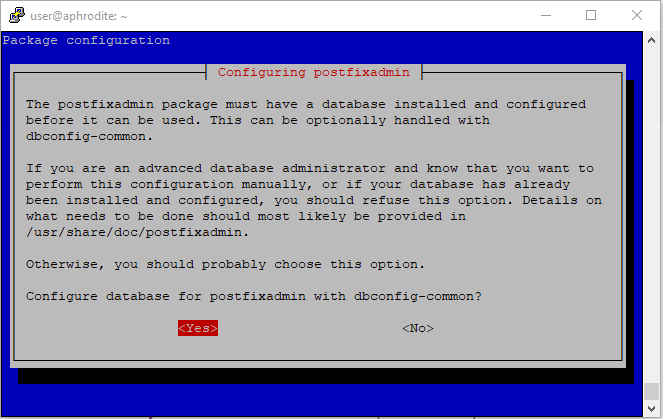
A screenshot of a computer

AI-generated content may be incorrect.

* Définir le domaine du serveur mail

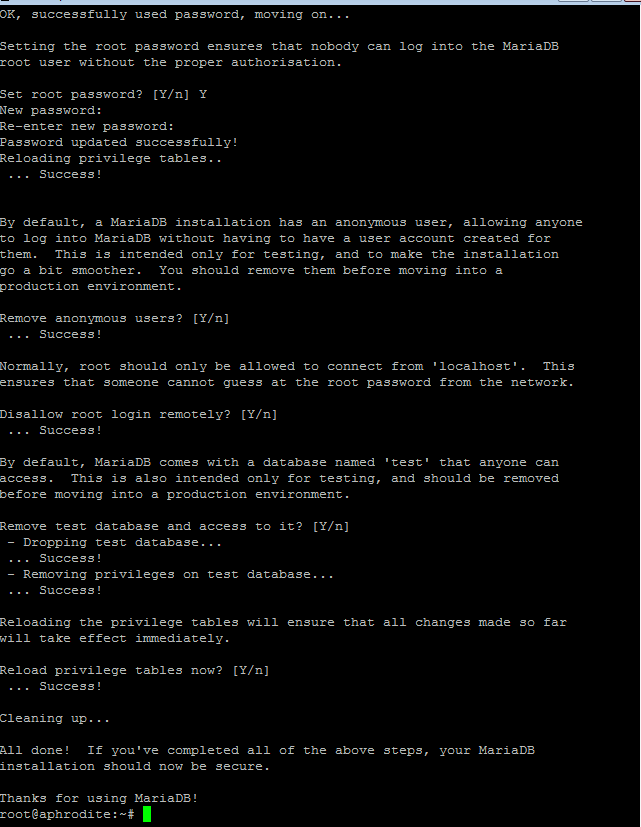


Pour les autres services et bases répondre par OUI créer les bases avec comme password adadad.



* configurer une sécurité de base Mariadb-server

**mysql\_secure\_installation**



Modifier la configuration du serveur MySql pour autoriser les connexions de tous les réseaux :

**nano /etc/mysql/mariadb.conf.d/50-server.cnf**

#bind-address=

A screen shot of a computer

AI-generated content may be incorrect.

**systemctl restart mariadb.service**

* Configurer Mariadb-server

**mysql -u root -p**

**CREATE DATABASE postfix;**

**CREATE USER 'postfix'@'localhost' IDENTIFIED BY 'adadad';**

**GRANT ALL PRIVILEGES ON postfix.\* TO 'postfix'@'localhost';**

**FLUSH PRIVILEGES;**

**use postfix;**

**ALTER DATABASE postfix COLLATE = 'latin1\_swedish\_ci' ;**

**QUIT**

A screenshot of a computer screen

AI-generated content may be incorrect.

* Configurer Mariadb-server

PostfixAdmin gère les utilisateurs et les domaines dans une base de données utilisateur de postfix.

**cd /usr/src**

**wget https://github.com/postfixadmin/postfixadmin/archive/postfixadmin-3.3.11.tar.gz**

**tar -xvf postfixadmin-3.3.11.tar.gz**

**mv postfixadmin-postfixadmin-3.3.11/ postfixadmin**

**ln -s /usr/src/postfixadmin/public /var/www/html/postfixadmin**

**mkdir -p /usr/src/postfixadmin/templates\_c**

**chown www-data /usr/src/postfixadmin/templates\_c -R**

**chmod 700 /usr/src/postfixadmin/templates\_c**

A screen shot of a computer program

AI-generated content may be incorrect.

Modifier le fichier **config.local.php**

**nano /usr/src/postfixadmin/config.local.php**

**<?php**

**$CONF['configured'] = true;**

**$CONF['database\_type'] = 'mysqli';**

**$CONF['database\_user'] = 'postfix';**

**$CONF['database\_password'] = 'adadad';**

**$CONF['database\_name'] = 'postfix';**

**$CONF['admin\_email'] = 'root@equitable.net';**

**$CONF['domain\_path'] = 'YES';**

**$CONF['domain\_in\_mailbox'] = 'NO';**

**$CONF['database\_prefix'] = '';**

**$CONF['fetchmail'] = 'NO';**

**$CONF['emailcheck\_resolve\_domain']='NO';**

**?>**

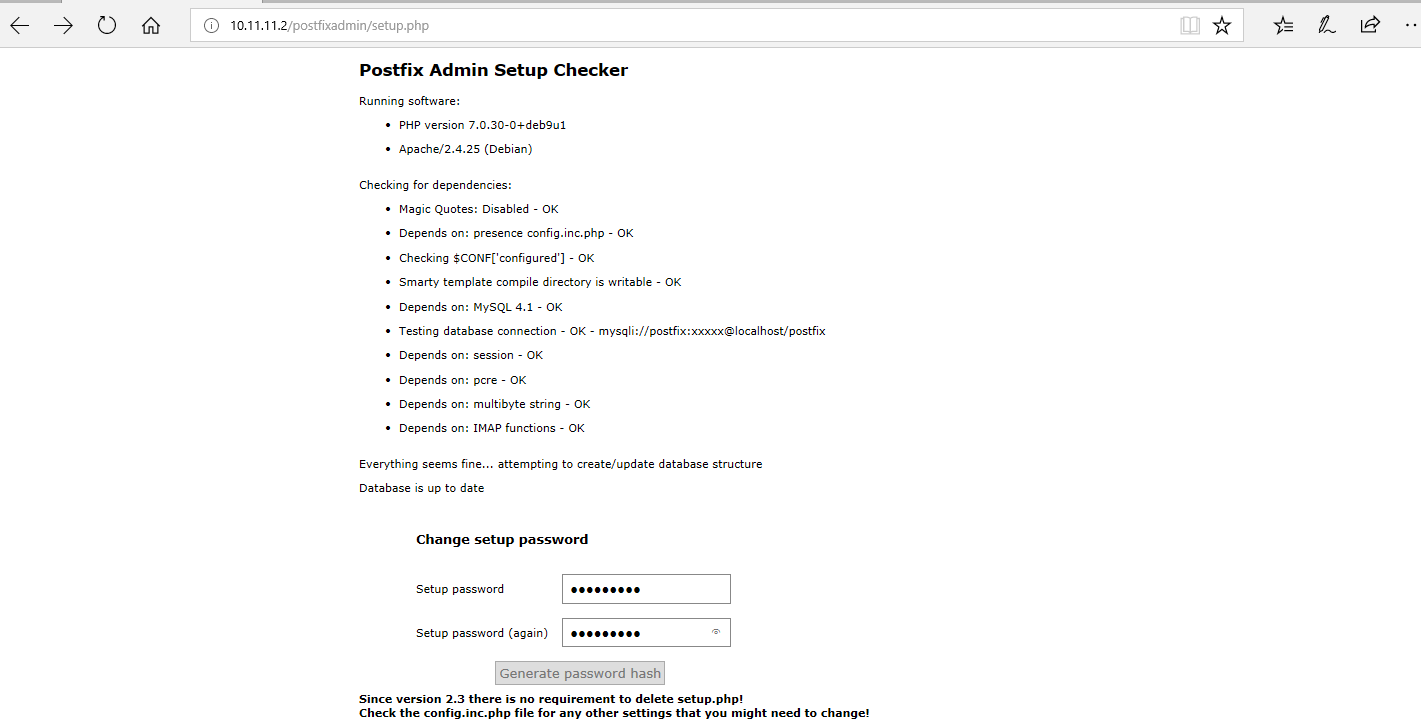
A computer screen with yellow and green text

AI-generated content may be incorrect.

Redémarrer apache:

**systemctl restart apache2**

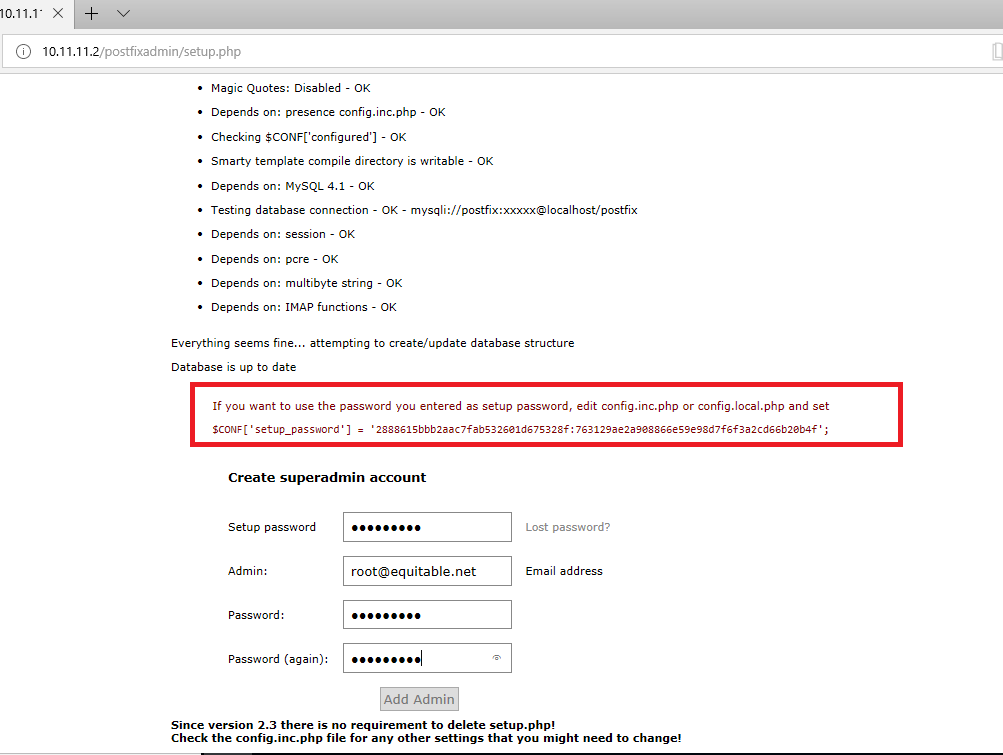
Depuis la machine Hera et d’un navigateur web, configurer postfixadmin:



A screenshot of a computer screen

AI-generated content may be incorrect.

Pour finaliser l’installation, se rendre sur : http://aphrodite.equitable.net/postfixadmin/setup.php puis cliquer sur « Generate a password » avec 2 chiffres.



A black text on a white background

AI-generated content may be incorrect.

En cas de problèmes vérifier les paramètres du fichier /usr/src/postfixadmin/config.inc.php

**nano /usr/src/postfixadmin/config.inc.php**

**<?php**

**$CONF['configured'] = true;**

**$CONF['database\_type'] = 'mysqli';**

**$CONF['database\_user'] = 'postfix';**

**$CONF['database\_password'] = 'adadad';**

**$CONF['database\_name'] = 'postfix';**

**$CONF['admin\_email'] = 'root@equitable.net';**

**$CONF['domain\_path'] = 'YES';**

**$CONF['domain\_in\_mailbox'] = 'NO';**

**$CONF['database\_prefix'] = '';**

**$CONF['fetchmail'] = 'NO';**

**$CONF['emailcheck\_resolve\_domain']='NO';**

**?>**

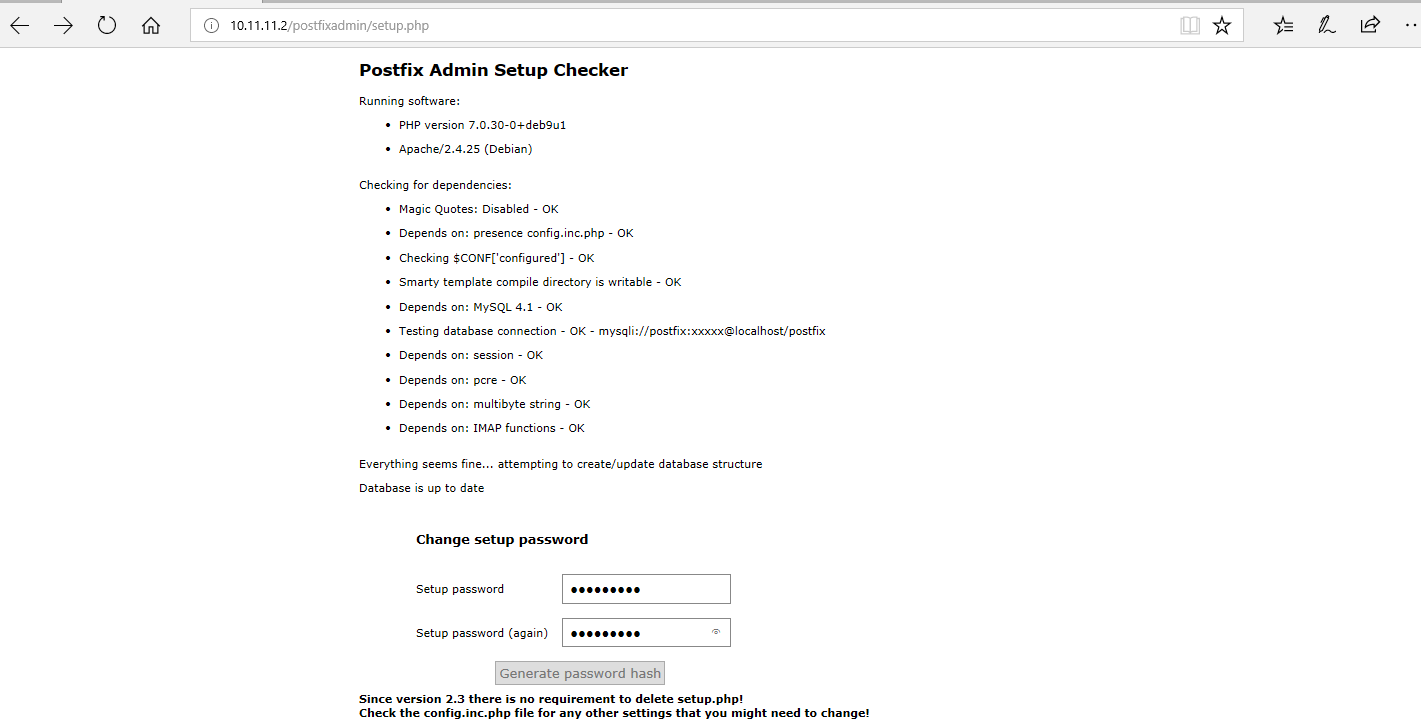
**systemctl restart apache2**

On obtient alors un hash

$CONF['setup\_password'] = 'a9a06a110199b2a63c4f19592042e25e:cad3f0363077d65c02750ce40963b11dc8475daf';

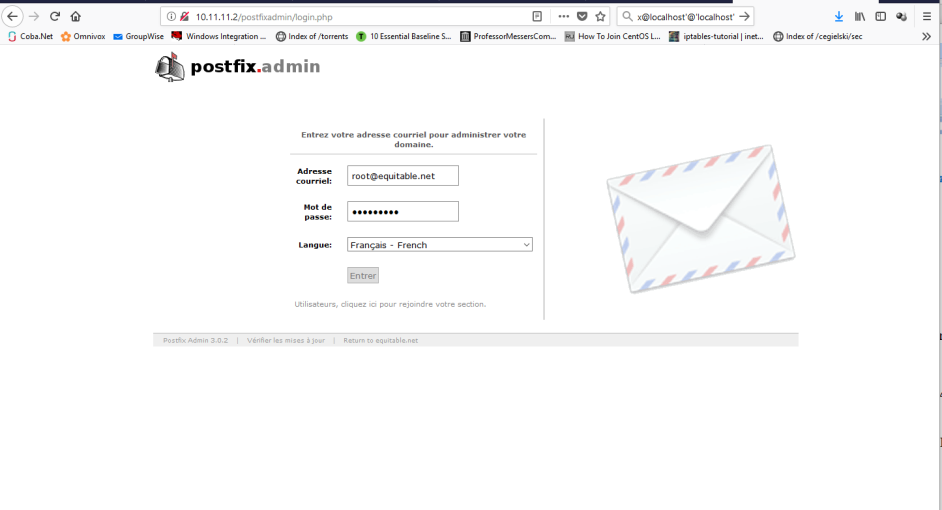
Il faut copier/coller dans le fichier de configuration postfixadmin

**/usr/src/postfixadmin/config.inc.php** ou **/usr/src/postfixadmin/config.local.php**



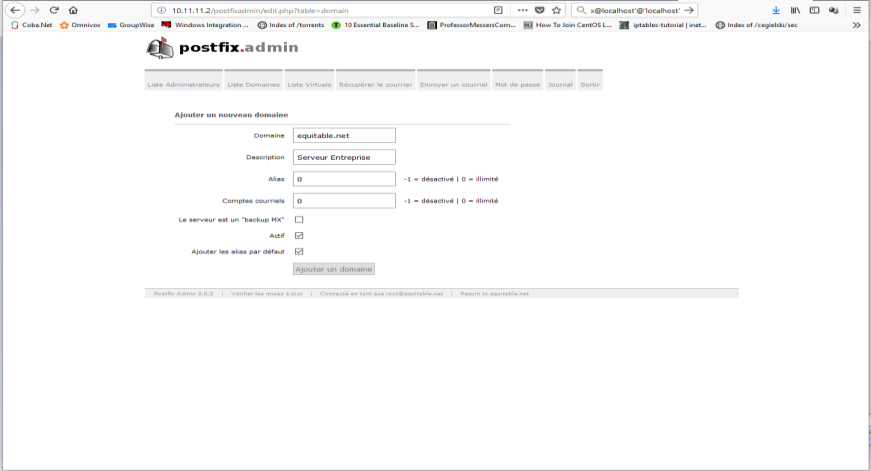
Il faut enfin créer un administrateur et son mot de passe

Puis se loguer avec ces identifiants sur **http://aphrodite.equitable.net/postfixadmin/login.php**



* Création du domaine et des utilisateurs

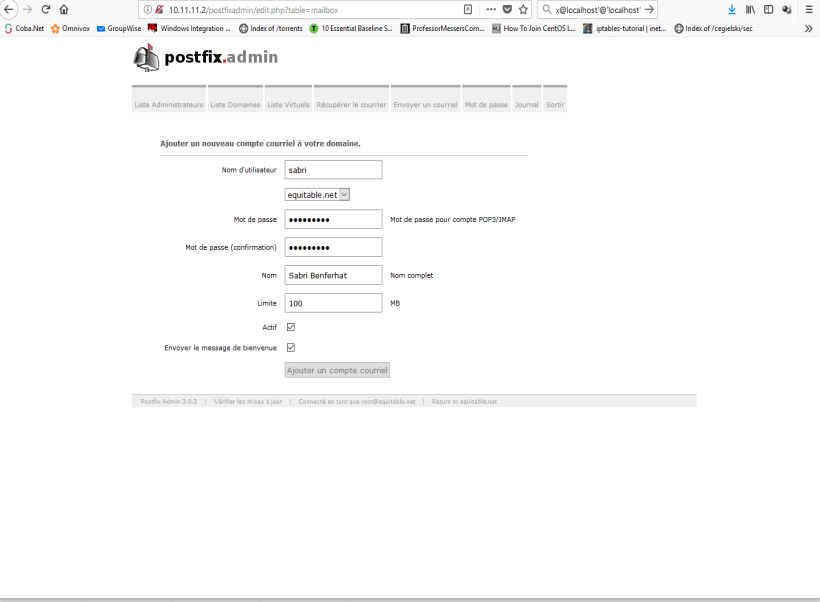
Il faut ensuite se rendre sous l’onglet Liste Domaines / Nouveau domaine pour enregistrer un nouveau domaine comme suit :



A screenshot of a computer

AI-generated content may be incorrect.

On crée ensuite un nouvel utilisateur en sélectionnant Ajouter un compte courriel auquel vous pouvez ajouter des alias :



A screenshot of a computer

AI-generated content may be incorrect.

## Configuration de postfix:

* Création de l'utilisateur

Création de l'utilisateur vmail et du groupe vmail ainsi que du répertoire de stockage des emails :

**groupadd -g 5000 vmail**

**useradd -M -s /sbin/nologin -u 5000 -g vmail -d /var/vmail vmail**

**mkdir /var/vmail**

**chown vmail: /var/vmail/**

A black screen with white text

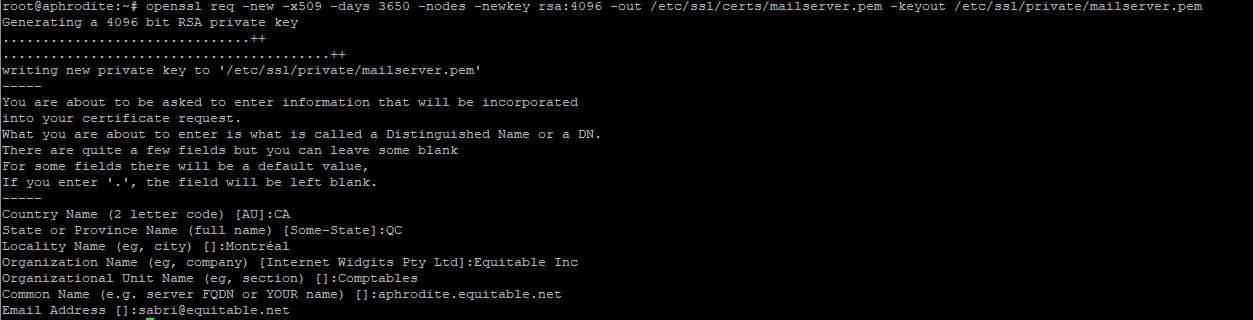
AI-generated content may be incorrect.

* Génération de certificat et clé sur serveur :

1. certificat: **/etc/ssl/certs/mailserver.pem**
2. clé privé: **/etc/ssl/private/mailserver.pem**

**openssl req -new -x509 -days 3650 -nodes -newkey rsa:4096 -out /etc/ssl/certs/mailserver.pem -keyout /etc/ssl/private/mailserver.pem**

**Attention au FQDN**



A screenshot of a computer program

AI-generated content may be incorrect.

* Lier postfix à MySql :

Maintenant il faut relier postfix à la base de données MySQL. Pour cela , nous allons créer trois fichiers :

1. mysql-virtual-mailbox-domains.cf
2. mysql-virtual-mailbox-maps.cf
3. mysql-virtual-alias-maps.cf

Le premier correspond à la gestion des noms de domaine , le second gère les boites des utilisateurs, et le troisième gère les alias. Voici le contenu de ces trois fichiers :

#### Domaines :

Pour que postfix ait accès aux domaines.

**nano /etc/postfix/mysql-virtual-mailbox-domains.cf**

user = postfix

password = adadad

hosts = 127.0.0.1

dbname = postfix

query = SELECT 1 FROM domain WHERE domain='%s'

Pour activer :

**postconf -e virtual\_mailbox\_domains=mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf**

Pour tester:

**postmap -q equitable.net mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf**



#### Boites des utilisateurs

Ensuite, il faut vérifier si la boite mail existe, exactement comme avec les domaines.

**nano /etc/postfix/mysql-virtual-mailbox-maps.cf**

user = postfix

password = adadad

hosts = 127.0.0.1

dbname = postfix

query = SELECT 1 FROM mailbox WHERE username='%s'

Pour activer :

**postconf -e virtual\_mailbox\_maps=mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf**

Et pour tester :

**postmap -q sabri@equitable.net mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf**



#### Gestion des alias

Il faut maintenant rediriger les alias vers les utilisateurs existant.

**nano /etc/postfix/mysql-virtual-alias-maps.cf**

user = postfix

password = adadad

hosts = 127.0.0.1

dbname = postfix

query = SELECT goto FROM alias WHERE address='%s'

Pour activer :

**postconf -e virtual\_alias\_maps=mysql:/etc/postfix/mysql-virtual-alias-maps.cf**

Pour tester :

**postmap -q abuse@equitable.net mysql:/etc/postfix/mysql-virtual-alias-maps.cf**



Dernière étape très importante : modifier les droits de ces trois fichiers. En effet, ils contiennent en clair des mots de passe SQL. Lancez les deux commandes :

**chgrp postfix /etc/postfix/mysql-\*.cf**

**chmod u=rw,g=r,o= /etc/postfix/mysql-\*.cf**

* Configurer postfix :

**nano /etc/postfix/main.cf**

smtpd\_banner = $myhostname ESMTP $mail\_name (Debian/GNU)

biff = no

mydomain = equitable.net

myhostname = aphrodite.equitable.net

append\_dot\_mydomain = no

readme\_directory = no

compatibility\_level = 2

smtpd\_use\_tls=yes

smtpd\_tls\_session\_cache\_database = btree:${data\_directory}/smtpd\_scache

smtp\_tls\_session\_cache\_database = btree:${data\_directory}/smtp\_scache

smtpd\_relay\_restrictions = permit\_mynetworks permit\_sasl\_authenticated defer\_unauth\_destination

alias\_maps = hash:/etc/aliases

alias\_database = hash:/etc/aliases

myorigin = /etc/mailname

mydestination = $myhostname, aphrodite, 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

virtual\_mailbox\_domains = mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf

virtual\_mailbox\_maps = mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf

virtual\_alias\_maps = mysql:/etc/postfix/mysql-virtual-alias-maps.cf

smtpd\_sasl\_type = dovecot

smtpd\_sasl\_path = private/auth

smtpd\_sasl\_auth\_enable = yes

smtpd\_sasl\_authenticated\_header = yes

smtpd\_tls\_security\_level = may

smtpd\_tls\_auth\_only = yes

smtpd\_recipient\_restrictions = permit\_sasl\_authenticated, permit\_mynetworks, reject\_invalid\_hostname, reject\_unknown\_recipient\_domain, reject\_unauth\_destination, reject\_non\_fqdn\_hostname, reject\_non\_fqdn\_sender, reject\_non\_fqdn\_recipient, reject\_unauth\_pipelining

broken\_sasl\_auth\_clients = yes

html\_directory = no

mailbox\_command = /usr/lib/dovecot/deliver -c /etc/dovecot/dovecot.conf -m "${EXTENSION}"

default\_destination\_concurrency\_failed\_cohort\_limit = 10

default\_destination\_concurrency\_limit = 1

default\_destination\_rate\_delay = 3s

default\_destination\_recipient\_limit = 2

smtp\_tls\_ciphers = high

smtpd\_tls\_ciphers = high

smtp\_tls\_fingerprint\_digest = sha1

smtpd\_tls\_fingerprint\_digest = sha1

smtp\_tls\_loglevel = 1

smtpd\_tls\_loglevel = 1

smtp\_tls\_mandatory\_ciphers = high

smtpd\_helo\_required = yes

smtpd\_sasl\_auth\_enable = yes

smtpd\_sasl\_authenticated\_header = yes

smtpd\_sender\_restrictions = reject\_unknown\_sender\_domain

smtpd\_tls\_cert\_file = /etc/ssl/certs/mailserver.pem

smtpd\_tls\_key\_file = /etc/ssl/private/mailserver.pem

smtpd\_tls\_exclude\_ciphers = aNULL, eNULL, EXPORT, DES, RC4, 3DES, MD5, PSK

smtpd\_tls\_mandatory\_ciphers = high

smtpd\_tls\_received\_header = yes

strict\_rfc821\_envelopes = yes

tls\_high\_cipherlist = ECDH+aRSA+AES256:ECDH+aRSA+AES128:AES256-SHA:DES-CBC3-SHA

tls\_preempt\_cipherlist = yes

virtual\_transport = dovecot

dovecot\_destination\_recipient\_limit = 1

virtual\_gid\_maps = static:5000

virtual\_uid\_maps = static:5000

virtual\_mailbox\_base = /var/vmail

virtual\_mailbox\_limit = 0

* Connecter Postfix à Dovecot :

Maintenant, on a d'un coté Postfix qui sait quand un mail qui passe est pour lui, et Dovecot qui sait où mettre les mails qu'on lui donne. Il faut donc que Postfix passe les mails a Dovecot qui les range.mais aussi, activation du port submission (587) et le port smtps (465)

**nano /etc/postfix/master.cf**

smtp inet n - y - - smtpd

pickup unix n - y 60 1 pickup

cleanup unix n - y - 0 cleanup

qmgr unix n - n 300 1 qmgr

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

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

maildrop unix - n n - - pipe

flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}

uucp unix - n n - - pipe

flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)

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}

submission inet n - y - - smtpd

-o syslog\_name=postfix/submission

-o smtpd\_tls\_security\_level=encrypt

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_reject\_unlisted\_recipient=no

-o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject

smtps inet n - y - - smtpd

-o syslog\_name=postfix/smtps

-o smtpd\_tls\_wrappermode=yes

-o smtpd\_sasl\_auth\_enable=yes

-o smtpd\_reject\_unlisted\_recipient=no

-o smtpd\_client\_restrictions=$mua\_client\_restrictions

dovecot unix - n n - - pipe

flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/dovecot-lda -f ${sender} -d ${recipient}

**service postfix restart**

## Configuration de Dovecot

Installation des paquets, dovecot-pop3d n'est volontairement pas installé :

**apt-get install dovecot-imapd dovecot-mysql dovecot-lmtpd**

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

disable\_plaintext\_auth = no

auth\_mechanisms = plain login

!include auth-sql.conf.ext

* Configuration SQL :

Il faut ensuite modifier le fichier auth-sql.conf.ext

**nano /etc/dovecot/conf.d/auth-sql.conf.ext**

passdb {

driver = sql

args = /etc/dovecot/dovecot-sql.conf.ext

}

userdb {

driver = static

args = uid=vmail gid=vmail home=/var/vmail/%d/%n

}

* Configuration du mail directory

**nano /etc/dovecot/conf.d/10-mail.conf**

mail\_location = maildir:/var/vmail/%d/%n/Maildir

namespace inbox {

inbox = yes

}

* Configuration du master

Dans le fichier 10-master.conf, dans le bloc service auth, spécifiez le smtp-auth de postfix :

**nano /etc/dovecot/conf.d/10-master.conf**

service imap-login {

inet\_listener imap {

#port = 0

}

inet\_listener imaps {

port = 993

ssl = yes

}

}

service pop3-login {

inet\_listener pop3 {

}

inet\_listener pop3s {

}

}

service lmtp {

unix\_listener lmtp {

}

}

service imap {

}

service pop3 {

}

service auth {

unix\_listener /var/spool/postfix/private/auth {

mode = 0660

user = postfix

group = postfix

}

}

service auth-worker {

}

service dict {

unix\_listener dict {

}

}

* Configuration SSL :

Nous avons généré des certificats en début de projet. Il faut les renseigner dans le fichier 10-ssl.conf pour que Dovecot s’appuie dessus. Pour utiliser les certificats SSL créés en partie 1, modifiez le fichier /etc/dovecot/conf.d/10-ssl.conf :

**nano /etc/dovecot/conf.d/10-ssl.conf**

ssl = yes

ssl\_cert = </etc/ssl/certs/mailserver.pem

ssl\_key = </etc/ssl/private/mailserver.pem

ssl\_protocols = !SSLv3

ssl\_cipher\_list = ALL:!LOW:!SSLv3:!aNULL:!eNULL:!EXP:!DES:!RC4:!3DES:!MD5:!PS

ssl\_prefer\_server\_ciphers = yes

* Configuration LDA :

Nous utilisons le plugin sieve pour placer les fichiers dans les dossiers. Il faut activer le plugin sieve pour placer les fichier dans les dossiers. Pour cela, dans le fichier 15-lda.conf, trouvez le bloc protocol lda (ou créez le si besoin) :

**nano /etc/dovecot/conf.d/15-lda.conf**

protocol lda {

mail\_plugins = $mail\_plugins sieve

}

* Connexion SQL

Il faut indiquer a Dovecot comment se connecter à la base de données SQL. Pour cela, modifiez le ficher /etc/dovecot/dovecot-sql.conf.ext. Le fichier est plutot bien documenté. Trouvez (ou ajoutez à la fin) ces lignes :

**nano /etc/dovecot/dovecot-sql.conf.ext**

driver = mysql

connect = host=localhost dbname=postfix user=postfix password=adadad

default\_pass\_scheme = SHA512-CRYPT

user\_query = SELECT '/var/vmail/%d/%n' as home, 'maildir:/var/vmail/%d/%n' as mail, 5000 AS uid, 5000 AS gid, concat('dirsize:storage=', quota) AS quota FROM mailbox WHERE username = '%u' AND active = '1'

password\_query = SELECT username as user, password, '/var/vmail/%d/%n' as userdb\_home, 'maildir:/var/vmail/%d/%n' as userdb\_mail, 5000 as userdb\_uid, 5000 as userdb\_gid FROM mailbox WHERE username = '%u' AND active = '1'

iterate\_query = SELECT username as user FROM mailbox

**chown root:root /etc/dovecot/dovecot-sql.conf.ext**

**chmod go= /etc/dovecot/dovecot-sql.conf.ext**

Modifiez les droits du fichier de configuration, pour que dovecot soit lancé en tant qu'utilisateur vmail :

**chgrp vmail /etc/dovecot/dovecot.conf**

**chmod g+r /etc/dovecot/dovecot.conf**

Pour activer les log de dovecot:

**nano /etc/dovecot/conf.d/10-logging.conf**

log\_path = /var/log/dovecot.log

verbose\_ssl = yes

auth\_verbose = yes

**touch /var/log/dovecot.log**

**chmod a+rwx /var/log/dovecot.log**

## Configuration de Sieve

Modification du fichier /etc/dovecot/conf.d/20-lmtp.conf :

**nano /etc/dovecot/conf.d/20-lmtp.conf**

protocol lmtp {

mail\_plugins = $mail\_plugins sieve

}

Modification du fichier /etc/dovecot/conf.d/90-sieve.conf :

**nano /etc/dovecot/conf.d/90-sieve.conf**

plugin {

sieve = /var/vmail/%d/%n/.dovecot.sieve

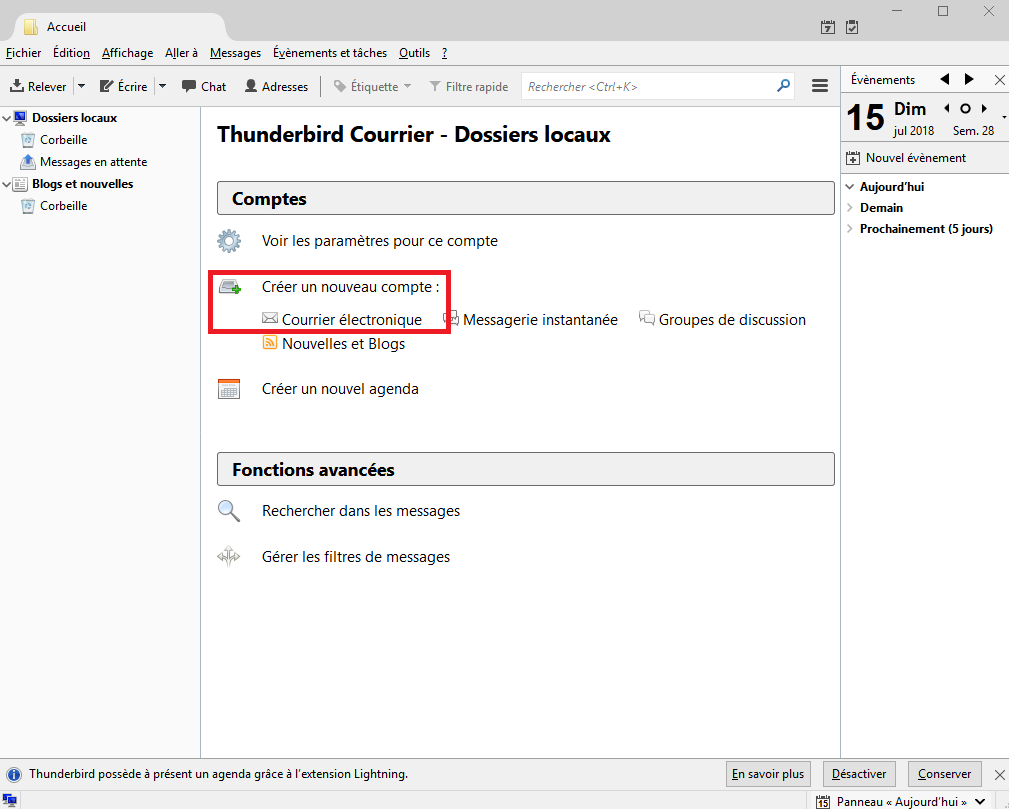
}

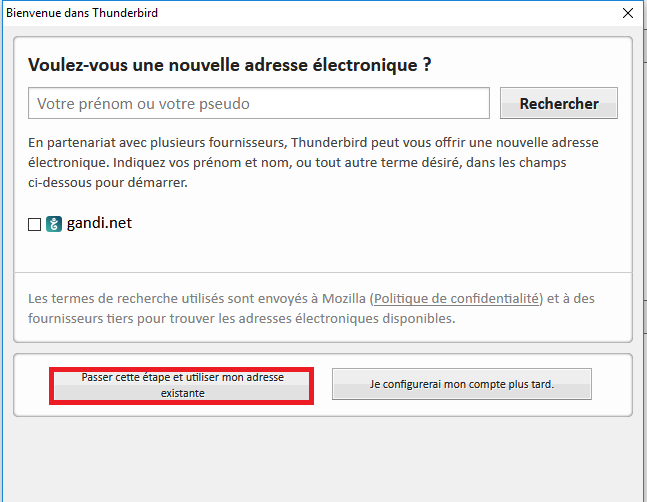
Changement des droits et redémarrage du service :

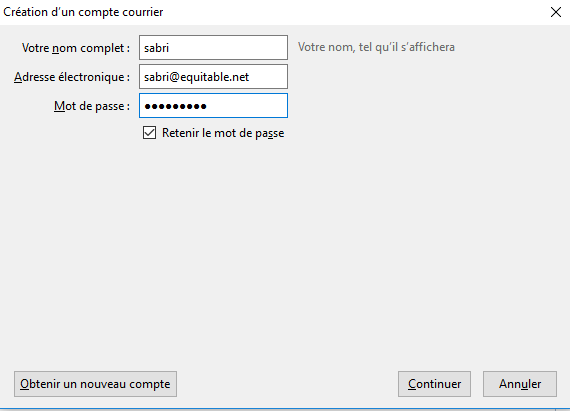
**service dovecot restart**

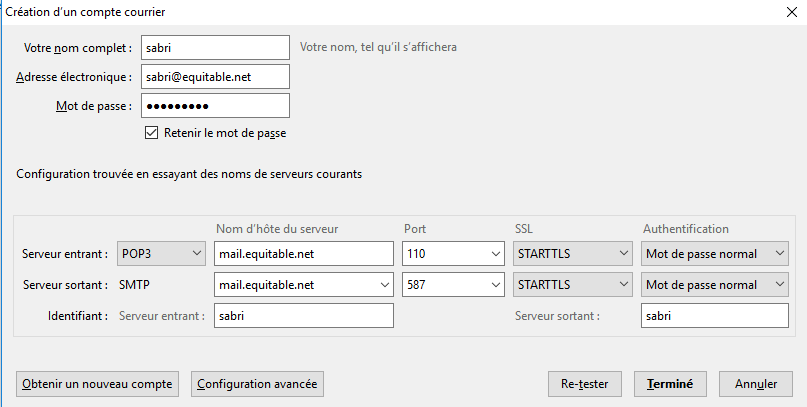
**service postfix restart**

Arrivé à cette votre serveur est fonctionnel. thunderbird









A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error message

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Création de ma première règle pour la boite sabri@equitable.net :

**nano /var/vmail/equitable.net/sabri/.dovecot.sieve**

**require "fileinto";**

**if header :is "X-Spam" "Yes" {**

**fileinto "Junk";**

**stop;**

**}**

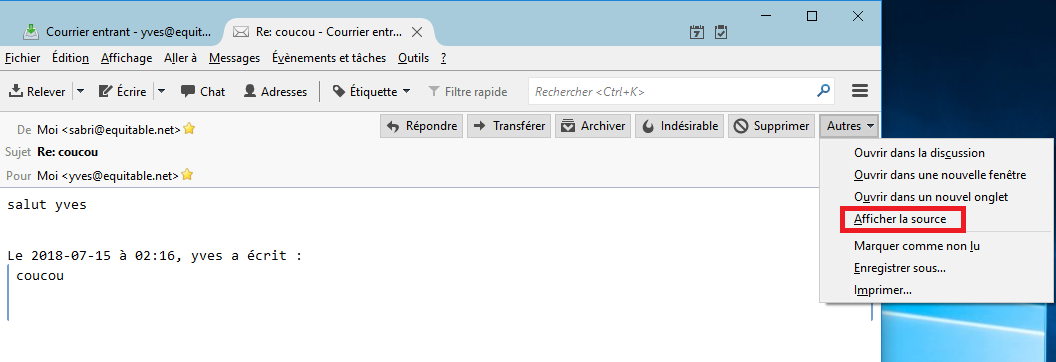
**chown vmail: /var/vmail/equitable.net/sabri/.dovecot.sieve**

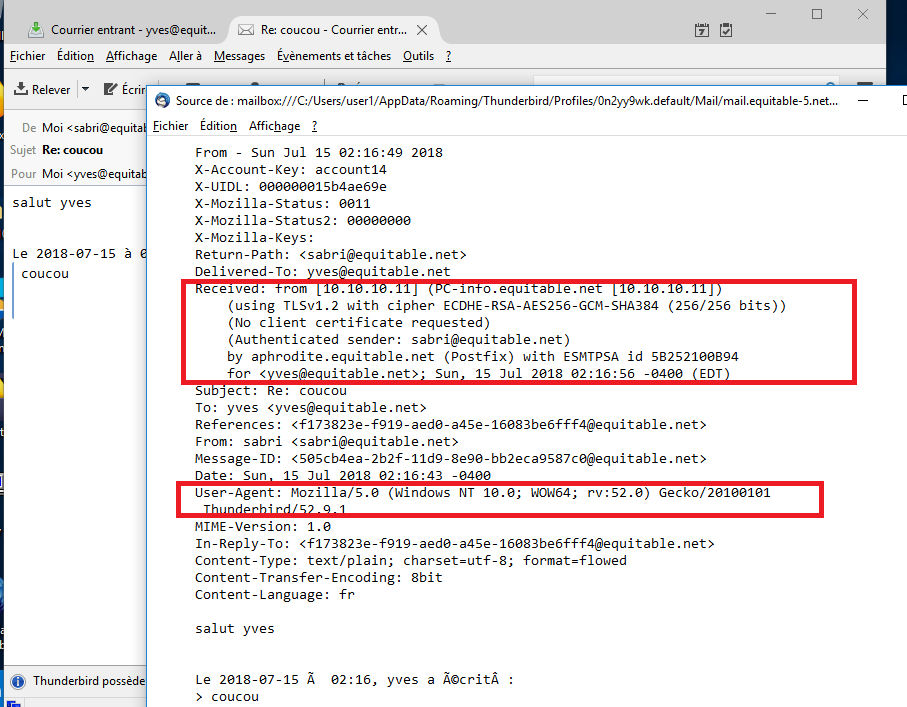


## Configuration des filtres pcre

**apt-get install postfix-pcre**

ces filtres permettront aux emails sortants d'avoir des informations sensibles supprimées du header, par exemple votre client (User-Agent) et votre adresse IP (X-Originating-IP).





**nano /etc/postfix/header\_checks**

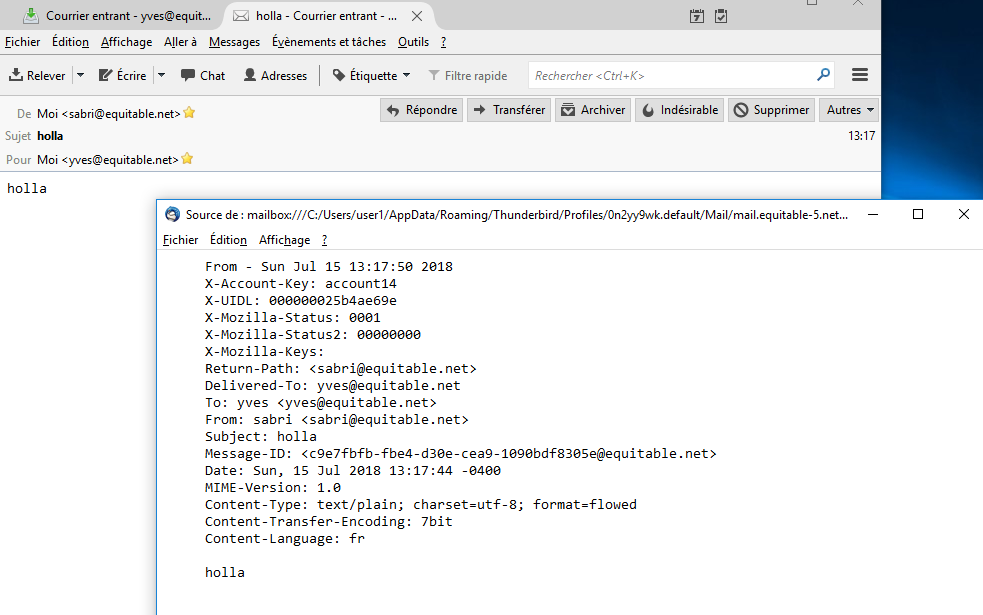
/^Received:/ IGNORE

/^User-Agent:/ IGNORE

/^X-Originating-IP:/ IGNORE

Attention à ne pas supprimer certains éléments si vous ne souhaitez pas atterrir dans les spams en dégradant votre note calculée par les anti-spams (SpamAssassin, Rspamd), il est par exemple déconseillé de supprimer Message-ID.

**postconf -e header\_checks=pcre:/etc/postfix/header\_checks**



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Génération des paramètres Diffie-Hellman:

**openssl dhparam -out /etc/postfix/dh2048.pem 2048**

**postconf -e smtpd\_tls\_dh1024\_param\_file=/etc/postfix/dh2048.pem**

**nano /etc/dovecot/conf.d/10-ssl.conf**

ssl\_dh\_parameters\_length = 2048

**service dovecot restart**

**service postfix restart**

## Installation de SpamAssassin:

**apt install spamassassin spamc**

**adduser spamd --disabled-login**

**mkdir /var/log/spamassassin**

**chown spamd:spamd /var/log/spamassassin**

Changer les lignes correspondantes:

**nano /etc/postfix/master.cf**

smtp inet n - n - - smtpd -o content\_filter=spamassassin

submission inet n - y - - smtpd -o content\_filter=spamassassin

smtps inet n - n - - smtpd -o content\_filter=spamassassin

et à la fin de fichier rajoutez:

spamassassin unix - n n - - pipe flags=R user=debian-spamd argv=/usr/bin/spamc -e /usr/sbin/sendmail -oi -f ${sender} ${recipient}

**nano /etc/spamassassin/local.cf**

rewrite\_header Subject \*\*\*\*\*SPAM\*\*\*\*\*

report\_safe 0

required\_score 5.0

use\_bayes 1

bayes\_auto\_learn 1

use\_bayes\_rules 1

ifplugin Mail::SpamAssassin::Plugin::Shortcircuit

endif # Mail::SpamAssassin::Plugin::Shortcircuit

whitelist\_from \*@equitable.net

add\_header all Report \_REPORT\_

add\_header spam Flag \_YESNOCAPS\_

add\_header all Status \_YESNO\_, score=\_SCORE\_ required=\_REQD\_ tests=\_TESTS\_ autolearn=\_AUTOLEARN\_ version=\_VERSION\_

add\_header all Level \_STARS(\*)\_

add\_header all Checker-Version SpamAssassin \_VERSION\_ (\_SUBVERSION\_) on \_HOSTNAME\_

use\_razor2 0

use\_dcc 0

use\_pyzor 0

**nano /etc/default/spamassassin**

ENABLED=1

OPTIONS="--create-prefs --max-children 5 --username spamd --helper-home-dir /home/spamd/ -s /var/log/spamassassin/spamd.log"  
PIDFILE="/var/run/spamd.pid"

CRON=1

SAHOME="/var/log/spamassassin/"

**systemctl restart postfix.service**

**systemctl enable spamassassin.service**

**systemctl start spamassassin.service**

Pour tester les spam envoyer un courriel avec ce texte:

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

A screenshot of a computer

AI-generated content may be incorrect.

## Autres

1. Pour un vrai site sur le net il faut rajouter la configuration du champ DMARC et la configuration du champ SPF
2. MAJ et Apprentissage de spamassassin
3. Antivirus
4. Rainloop ou Squirrelmail , Roundcube & Horde
5. Outils: calendrier, déplacer les spam dans un dossier automatique... etc