CENATUS Jean-Luc


3A | **S**ystèmes **R**éseaux et **C**loud computing

Promotion 2015/2016

Compte rendu

Linux administration avancé

# Projet Postfix

# Sommaire

## Informations utiles :

- Distribution utilisée : Ubuntu Server 16.04 LTS
- Configuration du réseau :
  - Réseau : 172.16.100.0
  - Masque de sous-réseau : 255.255.255.0
  - Domaine DNS : domn.net
  - Adresse IP du serveur de courriel : 172.16.100.1

## Mise à jour du système :

Après l'installation de la distribution Ubuntu dans sa version 16.04 LTS, nous préférons lancer une mise à jour de cette dernière avant de passer à la suite. Nous avons une préférence pour aptitude à la place d'apt-get, car nous trouvons qu'il gère mieux les dépendances que ce dernier. Ceci est un choix personnel, rien n'empêche d'utiliser apt-get à la place d'aptitude (il suffit alors de modifier les commandes en remplaçant aptitude par apt-get).

```
sudo apt-get update #mise à jour des dépôts
sudo apt-get install aptitude #installation de aptitude
sudo aptitude upgrade #mise à jour des paquets installés via aptitude
sudo aptitude purge "~c" #suppression des résidus de/et paquets inutiles
sudo aptitude clean #vidage du cache APT
```

Une fois fait, nous préférons redémarrer le système (important en cas de mise à jour du noyaux linux et pilotes) :

```
sudo reboot
```

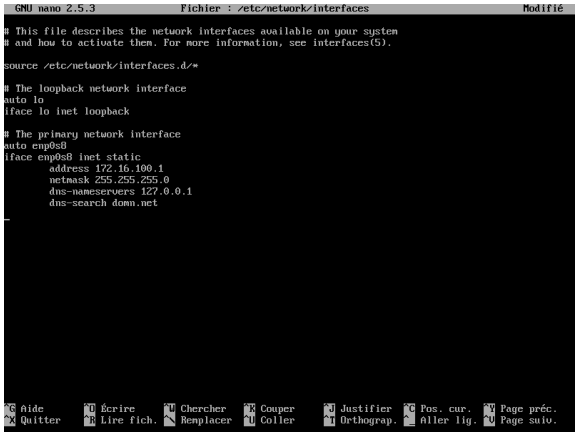
Viens ensuite la configuration du réseau.

## Paramétrage réseau du serveur de messagerie :

Nous devons configurer l'interface réseau du serveur de messagerie afin que cette dernière soit dans le réseau 172.16.100.0 /24 comme indiqué dans les informations utiles ci-dessus.

### Configuration réseau IPv4 (adressage fixe) :

```
sudo nano /etc/network/interfaces
```




*enp0s8* = nom de l'interface réseau
*address 172.16.100.1* = adresse IP de cette interface réseau
*netmask 255.255.255.0* = masque de sous-réseau de l'interface réseau
*dns-nameservers 127.0.0.1* = serveur de nom de domaine (ici, on utilisera celui qui sera installé localement)
*dns-search domn.net* = domaine de recherche DNS par défaut

Une fois les modifications effectués, on relance le service de configuration du réseau :

```
sudo service networking restart
```

puis on vérifie que la nouvelle configuration à bien été prise en compte à l'aide de la commande :

```
ifconfig
```

```
root@server:~# ifconfig
enp0s8    Link encap:Ethernet  HWaddr 08:00:27:08:4b:75
          inet adr:172.16.100.1  Bcast:172.16.100.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe08:4b75/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Packets reçus:0 erreurs:0 :0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:0 (0.0 B) Octets transmis:1296 (1.2 KB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          Packets reçus:505 erreurs:0 :0 overruns:0 frame:0
          TX packets:505 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1
          Octets reçus:38086 (38.0 KB) Octets transmis:38086 (38.0 KB)

virbr0    Link encap:Ethernet  HWaddr 52:54:00:ff:19:02
          inet adr:192.168.122.1  Bcast:192.168.122.255  Masque:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          Packets reçus:0 erreurs:0 :0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          Octets reçus:0 (0.0 B) Octets transmis:0 (0.0 B)

root@server:~# _
```

Viens ensuite la configuration du nom de machine et de son suffixe DNS.

## Changement du nom de machine et affectation d'un suffixe DNS

Pour rappel :
Nom de la machine : mail-server
Suffixe DNS : domn.net
Adresse IP : 172.16.100.1

### Configuration du nom d'hôte

```
sudo nano /etc/hostname
```


### Édition du fichier « hosts »

```
sudo nano /etc/hosts
```


3 - Redémarrage du système pour prendre en compte les changements :

```
sudo reboot
```

Maintenant que la configuration réseau est bonne, nom de machine et suffixe DNS correctement affecté, nous pouvons passer à l’installation du serveur DNS.

# Installation du service DNS

## Installation de Bind9

```
sudo aptitude install bind9
```

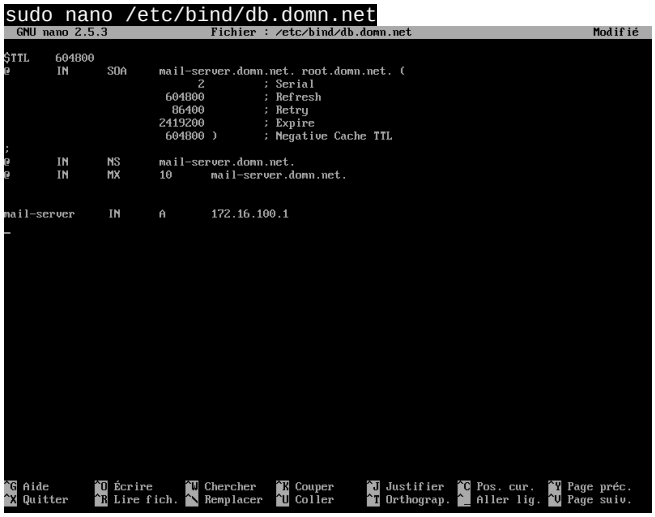
## Configuration de Bind9

Duplication des zones pré-installés afin d'avoir les modèles sur lesquelles s'appuyer pour la création des nouvelles zones DNS :

```
sudo cp /etc/bind/db.local /etc/bind/db.domn.net #zone domn.net
sudo cp /etc/bind/db.127 /etc/bind/db.domn.net.inv #zone inverse de domn.net
```

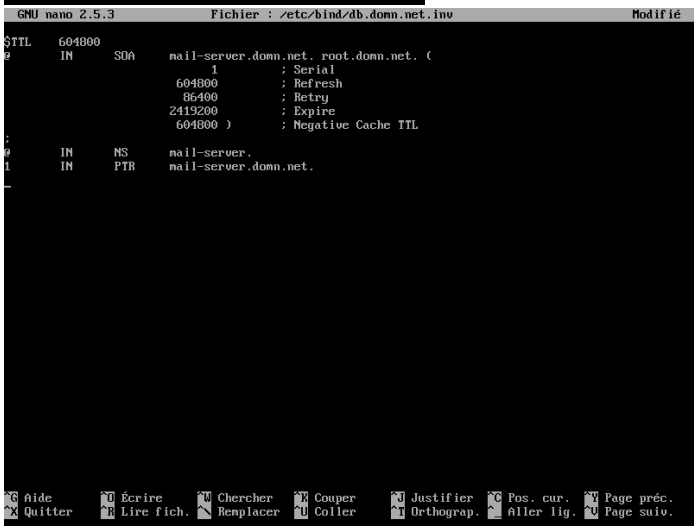
Configuration de la nouvelle zone domn.net :

```
sudo nano /etc/bind/db.domn.net
```



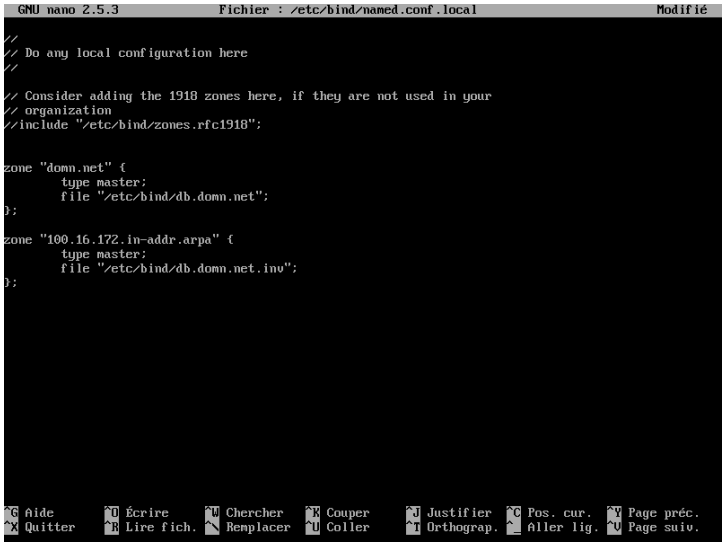

Configuration de la nouvelle zone de recherche inversé de domn.net :

```
sudo nano /etc/bind/db.domn.net.inv
```



Ajout de ces nouvelles zones dans la configuration de named :

```
sudo nano /etc/bind/named.conf.local
```

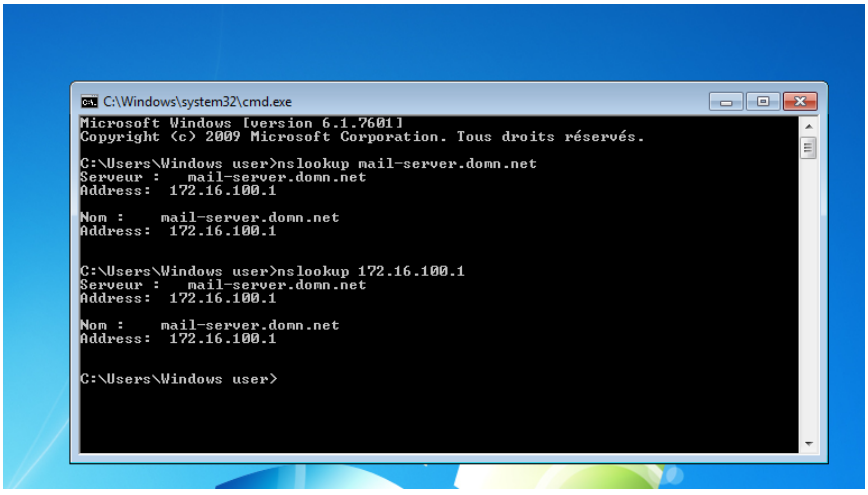



On vérifie que les fichiers de configuration soient bons à l'aide de la commande :
`named-checkconf`

Si la commande en retourne pas d'erreur, on peut redémarrer bind9 afin qu'il puisse prendre en compte la nouvelle configuration :
`sudo service bind9 restart`

Le serveur DNS devraient maintenant fonctionner.
A noter que dans notre cas, il n'y a que les enregistrements concernant mail-server.

Un `nslookup mail-server.domn.net` / `172.16.100.1` depuis une machine cliente ayant pour DNS principal 172.16.100.1 devrait vous retourner l'adresse IP / nom d'hôte de mail-server.




Une fois le serveur DNS bien configuré, nous pouvons passer à la suite. Cette étape est (quasi)indispensable.

## Installation de Postfix

On installe postfix à l'aide de :
```
sudo aptitude install postfix
```

puis on lance l'assistant de configuration basique de postfix fourni par le paquet provenant du dépôt :
```
sudo dpkg-reconfigure postfix
```

Dans notre cas, voici les informations que l'on a renseignées :

Configuration type du serveur de messagerie : **Site Internet**
Nom de courrier : **mail-server.domn.net**
Destinataire des courriels de « root » et de « postmaster » : **ubuntu**
Autres destinations pour lesquelles le courrier sera accepté : **$myhostname, mail-server.domn.net, domn.net, localhost.domn.net, localhost**
Faut-il forcer des mises à jour synchronisées de la file d'attente des courriels : **Oui**
Réseaux internes : **127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 172.16.100.0/24**
Taille maximale des boîtes aux lettres (en octets) : **0**
Caractère d'extension des adresses locales : +
Protocoles internet à utiliser : **tous**

Postfix étant assez bien configuré de base, il n'y a pas plus à faire pour l'instant. A ce stade, le serveur de messagerie ne fonctionne qu'avec les utilisateurs locaux du système.

On relance le service postfix afin qu'il prenne en compte les modifications :
```
sudo service postfix restart
```

## Mise en place des accès via les protocoles POP3 et IMAP

Pour pouvoir proposer un accès au serveur de messagerie depuis les protocoles POP3 et/ou IMAP, nous utiliserons courier-pop et courier-imap.

### Installation :

```
sudo aptitude install courier-pop courier-imap
```

Lors de l'installation, il sera demandé si l'assistant doit créer les répertoires nécessaires à l'administration web, nous répondons « **Non** », car cela ne nous sera pas utile.

### Changement du répertoire de stockage des messages utilisateurs (Postfix)

Pour le bon fonctionne de courier-pop et courier-imap, nous devons spécifier à Postfix d'utiliser le dossier Maildir du dossier personnel de l'utilisateur afin de stocker les messages de ce dernier.

Pour cela, on édite le fichier main.cf de Postfix :
```
sudo nano /etc/postfix/main.cf
```

Puis à la fin de ce fichier, on rajoute la ligne :
home_mailbox = Maildir/

Puis on relance le service postfix :
```
sudo service postfix restart
```

### Problème avec le service courier-authdaemon

Étrangement, sur notre système, le service courier-authdaemon nécessaire au bon fonctionne de courier-pop et courier-imap ne se lance pas automatiquement. Pour y remédier, nous avons dues lancer ces commandes :
```
sudo systemctl enable courier-authdaemon.service #active le démarrage du service au boot du système
sudo service courier-authdaemon start #démarre immédiatement le service
```

Maintenant que les services DNS, Postfix et Courier sont pleinement fonctionnels, nous pouvons commencer à créer les utilisateurs de la messagerie.

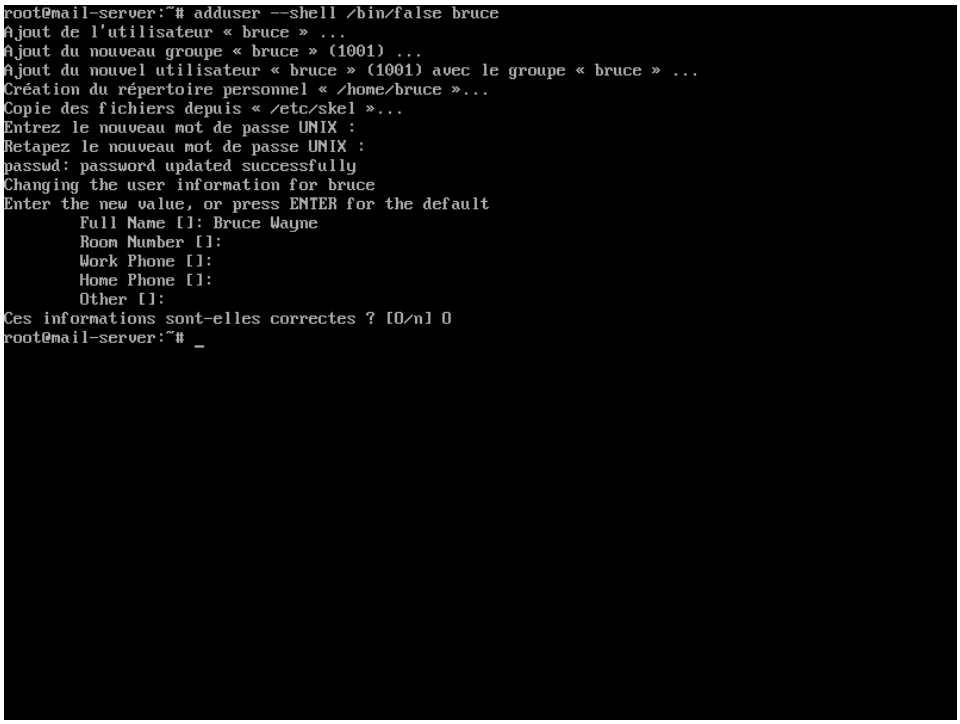
## Les utilisateurs :

A notre stade, Postfix fonctionne avec les utilisateurs locaux du système.

### Ajout d'un utilisateur :

Pour créer un utilisateur local, on utilisera la commande :

```
sudo adduser --shell /bin/false utilisateur #--shell /bin/false permet d'empêcher la connexion local de utilisateur
```




*Exemple de création de l'utilisateur nommé bruce*

Puis l'on créé le répertoire qui contiendra les messages de l'utilisateur :

```
sudo maildirmake /home/utilisateur/Maildir
```

Et on lui donne les pleins droits dessus :

```
sudo chown -R utilisateur:utilisateur /home/utilisateur/Maildir
```

Ces 3 étapes sont à répéter pour chaque nouvelle création d'utilisateur.
Il est relativement facile d'automatiser cette tâche via un petit script bash.

### Suppression d'un utilisateur :

On supprime l'utilisateur du système :

```
sudo deluser utilisateur
```

et optionnellement, ses messages :

```
sudo rm -r /home/utilisateur/Maildir
```

## Installation du webmail

Nous utiliserons SquirrelMail qui permettra aux utilisateurs d'accéder à leur messagerie depuis leur navigateur internet.

### Installation de SquirrelMail

```
sudo aptitude install squirrelmail
```

Optionnel, si vous voulez personnaliser a configuration de SquirrelMail
```
sudo squirelmail-configure
```

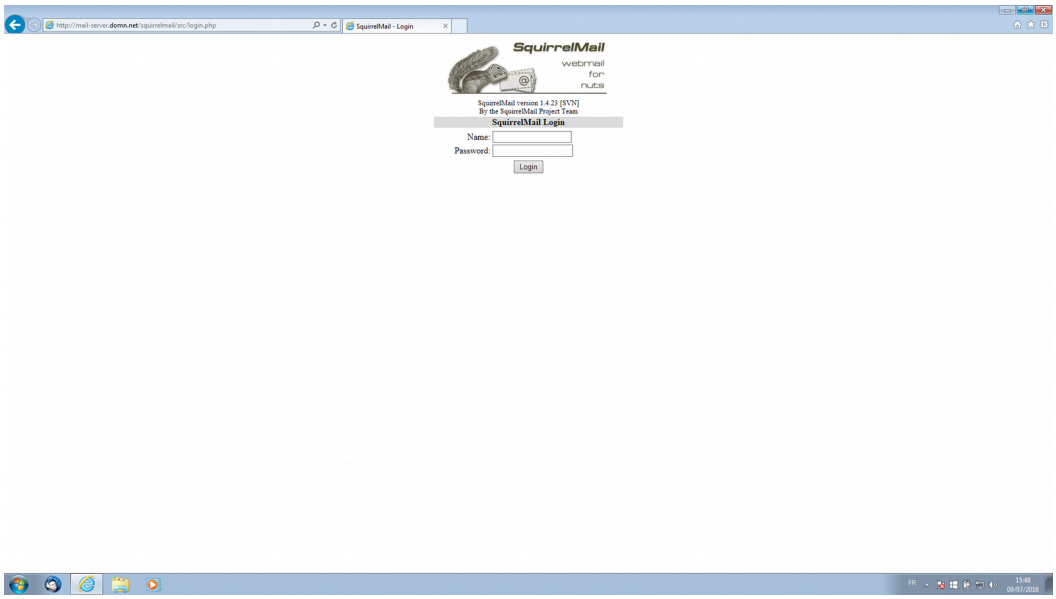
Intégration de SquirrelMail parmi les sites d'Apache (qui se sera installé en même temps que squirrelmail)
```
sudo cp /etc/squirrelmail/apache.conf /etc/apache2/sites-available/squirrelmail.conf
sudo a2ensite squirrelmail
```

Puis on relance Apache afin qu'il prenne en compte le nouveau site :
```
sudo service apache2 restart
```

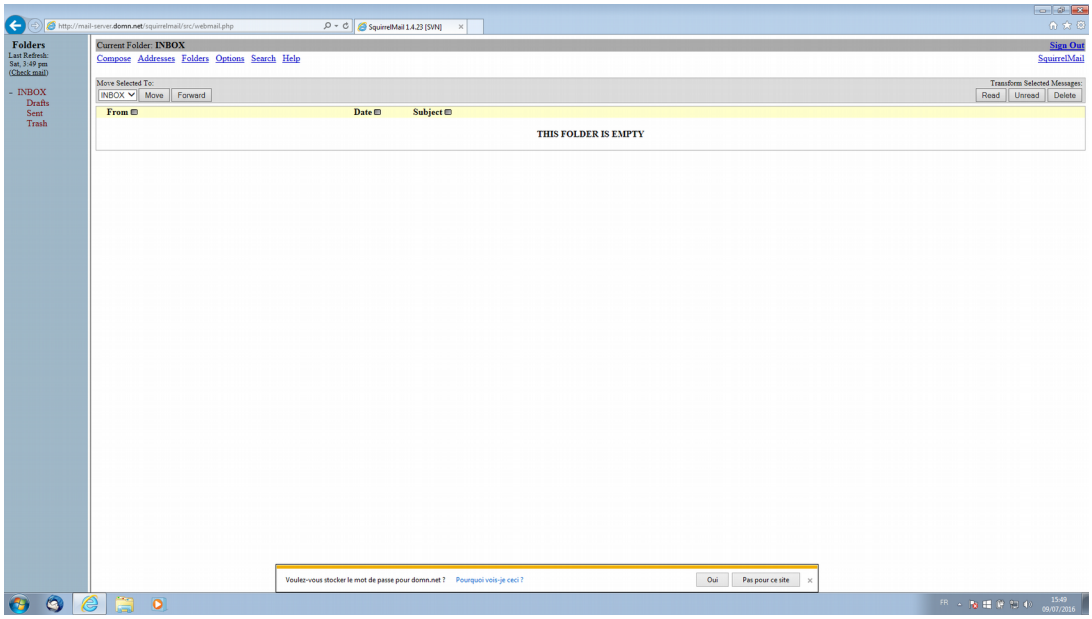
A noter que par défaut, SquirrelMail utile le serveur de messagerie de la machine sur laquelle on l'installe, cela explique pourquoi on n'a pas eu à la configurer.

### Accès à l'interface web de SquirrelMail

L'interface web de SquirrelMail est accessible depuis http://serveur/squirrelmail , ce qui dans notre cas correspond à **http://mail-server.domn.net/squirrelmail** .




*Page de login*



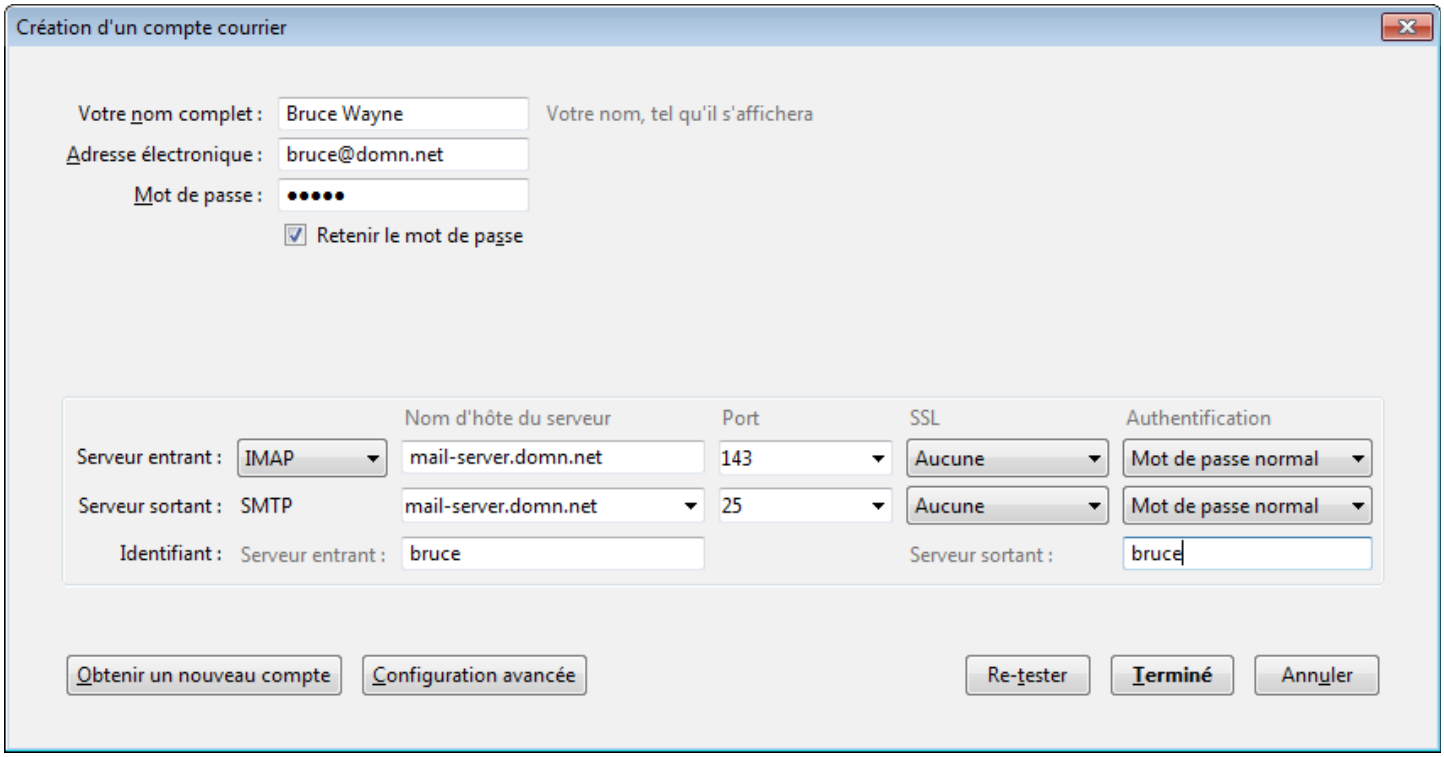

*Une fois authentifié*

## Configuration d'un client de messagerie standard

Les informations de configuration d'un client de messagerie standard sont :

Adresse électronique : **utilisateur**@domn.net
Mot de passe : < celui de **utilisateur** >
Serveur entrant (au choix) : POP3 : **mail-server.domn.net** sur le port **110**
IMAP : **mail-server.domn.net** sur le port **143**
Serveur sortant SMTP : **mail-server.domn.net** sur le port **25**
Identifiant serveur entrant & sortant : **utilisateur**

**Aucun cryptage SSL ou autre n'est utilisé.**




*Exemple de configuration sur Mozilla Thundebird*

## BONUS : Ajout d'un anti-spam

SpamAssassin est un logiciel libre mené par la Apache Software Foundation qui a pour but de filtrer le trafic des courriels pour éradiquer les courriels reconnus comme pourriels (SPAM) et/ou non sollicités.

Il est possible de l'intégrer à Postfix afin qu'il puisse scanner chaque email reçu avant leur remise dans leur boite au lettre.

### Installation

Pour cela, on l'installe avec :
```
sudo aptitude install spamassassin
```

On créé un utilisateur spécifique à Spamassassin
```
sudo useradd --home /var/spamassassin --create-home --system spamd
```

et on le défini comme étant propriétaire du répertoire /var/lib/spamassassin
```
sudo chown spamd:spamd /var/lib/spamassassin
```

### Configuration

Il faut ensuite configurer Spamassassin un minima, pour cela nous éditons le fichier **/etc/default/spamassassin** :
```
sudo nano /etc/default/spamassassin
```

Dans lequel nous définissons les options suivantes :
```
ENABLED=1
OPTIONS="--create-prefs --max-children 5 --helper-home-dir --username spamd -H /var/lib/spamassassin -s /var/log/spamd.log"
CRON=0
```

Nous faisons de même avec le fichier **/etc/spamassassin/local.cf** :
```
sudo nano /etc/spamassassin/local.cf
```

Dans lequel nous définissons les options suivantes :
```
rewrite_header Subject *****SPAM*****
use_bayes 1
bayes_auto_learn 1
ifplugin Mail::SpamAssassin::Plugin::Shortcircuit
endif # Mail::SpamAssassin::Plugin::Shortcircuit
```

### Intégration à Postfix

Maintenant que Postfix est configuré comme nous le voulons, il faut maintenant indiquer à Postfix de scanner chaque courriel entrant via SpamAssassin.

Pour cela, on édite le fichier **/etc/postfix/master.cf**
```
sudo nano /etc/postfix/master.cf
```

Dans lequel nous rajoutons ces lignes :

```
# SpamAssassin
smtp      inet  n       -       -       -       -       smtpd  -o content_filter=spamassassin
spamassassin unix  -       n       n       -       -       pipe user=spamd argv=/usr/bin/spamc -f -e
        /usr/sbin/sendmail -oi -f${sender} ${recipient}
```

Une fois fait, nous mettons à jour la base de donnée de SpamAssassin :

```
sudo sa-update
```

A noter que la base de donnée de SpamAssassin sera mise à jour régulièrement de façon automatique.

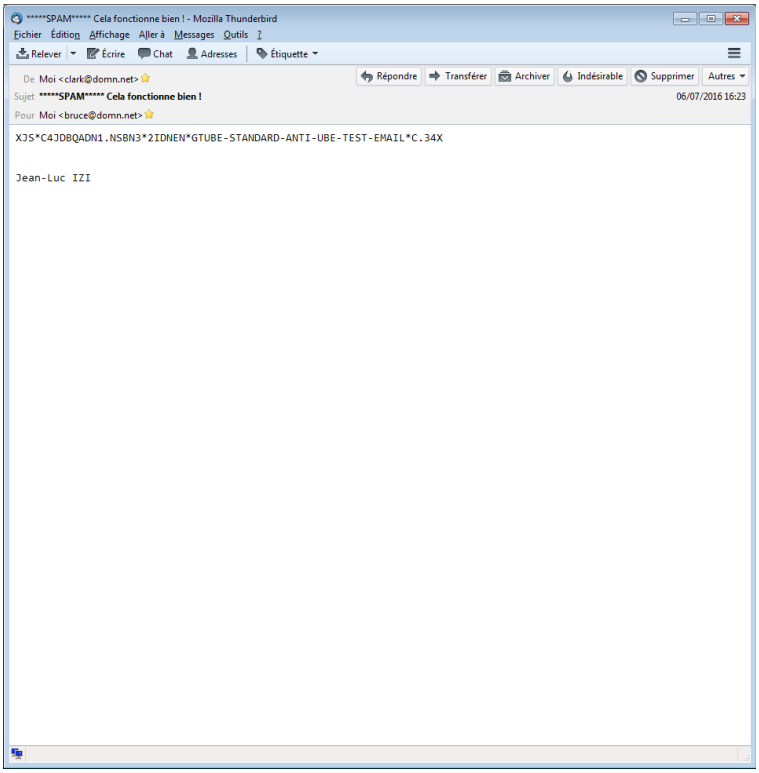
Comme pour le service courier-authdaemon, sur notre système le service spamassassin ne se lance pas automatiquement. Pour y remédier, nous avons dues lancer ces commandes :

```
sudo systemctl enable spamassassin.service #active le démarrage du service au boot du système
sudo service spamassassin start #démarre immédiatement le service
```

On redémarre ensuite Postfix afin qu'il prenne en compte la nouvelle configuration :

```
sudo service postfix restart
```

SpamAssassin devrait maintenant fonctionner. Chaque courriel qu'il considérera comme étant indésirables aura « *****SPAM***** » de rajouté dans son objet.




*Exemple de courriel marqué par SpamAssassin*

## BONUS : Ajout d'un antivirus

ClamAV est un logiciel libre antivirus. On peux l'utiliser avec Postfix afin qu'il scan chaque courriel reçu à la recherche de virus et autres malwares.

### Installation

Pour cela, on l'installe avec :
```
sudo aptitude install clamsmtp clamav-freshclam
```

### Configuration

Il faut ensuite configurer ClamAV un minima, pour cela nous éditons le fichier **/etc/clamsmtpd.conf** :
```
sudo nano /etc/clamsmtpd.conf
```

Dans lequel nous définissons les options suivantes :
```
OutAddress: 10026
Listen: 127.0.0.1:10025
ClamAddress: /var/run/clamav/clamd.ctl
TempDirectory: /var/spool/clamsmtp
PidFile: /var/run/clamsmtp/clamsmtpd.pid
Bounce: on
Quarantine: yes
User: clamsmtp
```

### Intégration à Postfix

Maintenant que Postfix est configuré comme nous le voulons, il faut maintenant indiquer à Postfix de scanner chaque courriel entrant via SpamAssassin.

Pour cela, on édite le fichier **/etc/postfix/main.cf**
```
sudo nano /etc/postfix/main.cf
```

**Dans lequel nous rajoutons ces lignes :**
```
# ClamAV antivirus scan
content_filter = scan:127.0.0.1:10026
receive_override_options = no_address_mappings
```

Nous faisons de même avec le fichier **/etc/postfix/master.cf** :
```
sudo nano /etc/postfix/master.cf
```

Dans lequel nous rajoutons les lignes suivantes :
```
# AV scan filter (used by content_filter)
scan      unix -      -      n      -      16      smtp
        -o smtp_send_xforward_command=yes
# For injecting mail back into postfix from the filter
127.0.0.1:10026 inet  n -      n      -      16      smtpd
        -o content_filter=
        -o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
        -o smtpd_helo_restrictions=
```

```
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks_style=host
-o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Une fois fait, nous mettons à jour la base de donnée de ClamAV :

```
sudo freshclam
```

A noter que la base de donnée de ClamAV sera mise à jour régulièrement de façon automatique (grâce au paquet clamav-freshclam)

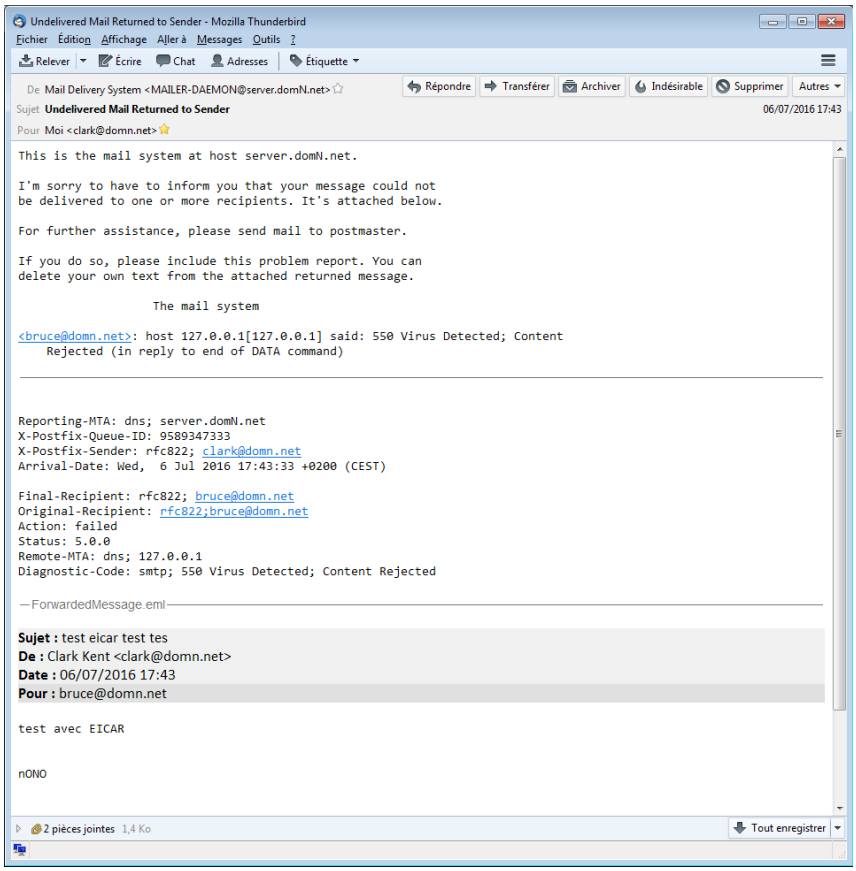
Comme pour les services courier-authdaemon et spamasassin, sur notre système le service clamav-daemon ne se lance pas automatiquement. Pour y remédier, nous avons dues lancer ces commandes :

```
sudo systemctl enable clamav-daemon.service #active le démarrage du service au boot du système
sudo service clam-av-daemon start #démarre immédiatement le service
```

On redémarre ensuite Postfix afin qu'il prenne en compte la nouvelle configuration :

```
sudo service postfix restart
```

ClamAV devrait maintenant fonctionner en concert avec Postfix. Chaque courriel contenant une pièce jointe malveillante sera renvoyé à l'expéditeur avec un message en conséquent expliquant la raison.




*Exemple de courriel renvoyé par ClamAV*