

Mise en place d'un serveur de messagerie

Le serveur de courriers Postfix sous Debian 8.1

ANATOLE BILLET

09 octobre 2015
Version : 1.00

Mise en place d'un serveur de messagerie

Le serveur de courriers Postfix sous Debian 8.1

Avant de commencer...

Prérequis :

- Une machine Debian 8.1 vierge.
- Un serveur DNS.
- Du courage.

Objectif :

Tutoriel permettant la mise en place un serveur de messagerie sous Debian avec configuration du DNS.

Code couleur :

-Bleu pour les commandes Debian

-Vert pour les noms des fichiers de configurations

-Italic pour les descriptions et anecdotes.

Table des matières

AVANT DE COMMENCER...	1
PREREQUIS :	1
OBJECTIF :	1
CODE COULEUR :	1
1/CONFIGURATION DE BASE.....	2
2/CONFIGURATION DU SERVEUR DE MAIL	2
2/LE SERVICE DE MESSAGERIE ELECTRONIQUE :.....	2
5/PREMIERS TESTS	3
6/ CONFIGURATION DE POSTFIX EN SERVEUR DOMAINE	4
7/INSTALLATION D'UN SERVEUR IMAP	5
8/INSTALLATION ET CONFIGURATION DE SQUIRRELMAIL	5
ADMINISTRATION DE SQUIRRELMAIL	6
POUR AJOUTER UN UTILISATEUR EMAIL A SQUIRRELMAIL :	6
9/SECURISATION DU SERVEUR DE COURRIERS	7
CONFIGURATION DE LA MISE EN QUARANTAINE :.....	8
ACTIVER SPAM ASSASSIN :	8

1/Configuration de base

Configurer le fichier hosts du serveur de messagerie et du serveur DNS :

Fichier hosts Du serveur DNS :

```
127.0.0.1    localhost
127.0.1.1    billet.local    dns
192.168.1.120  billet.local    dns
```

Fichier Hosts Du serveur Mail :

```
127.0.0.1    localhost
127.0.1.1    mailofthedead.billet.local
192.168.1.123  mailofthedead.billet.local_
```

2/Configuration du serveur de mail

Ensuite, configurer le fichier de votre zone DNS principal (**/var/cache/bind/**) comme cela :

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA    billet.billet.local. root.billet.local. (
                        7             ; Serial
                        604800        ; Refresh
                        86400         ; Retry
                        2419200       ; Expire
                        604800 )     ; Negative Cache TTL
;
@       IN      NS     billet.billet.local.
billet2 IN      NS     billet2.billet.local.
billet  IN      A      192.168.1.120
billet2 IN      A      192.168.1.121
mailofthedead IN  A      192.168.1.123
billet.local. IN  MX    10    mailofthedead.
```

Testez votre déclaration MX sur le serveur mail :

```
root@mailofthedead:~# host -t MX billet.local
billet.local mail is handled by 10 mailofthedead.billet.local.
```

2/Le service de messagerie électronique :

Pour notre serveur de messagerie nous utiliserons PostFix qui est un logiciel léger, facile à configurer et proposant une bonne sécurité. Nous l'utiliserons en mode internet.

Il est nécessaire de purger les paquets inutiles avant l'installation :

```
Apt-get -purge remove exim4 exim4-config exim4-daemon-light
```

Et installez Postfix :

Apt-get install postfix

Dpkg-reconfigure postfix

Puis lorsque demander, entrer vos informations.

Et installer votre postfix en mode « internet »

Puis configurer le fichier suivant :

Nano /etc/postfix/main.cf

Modifier les lignes suivantes comme suis :

-myhostname =mail.domaine.local

-mydestination = mail, mail.domaine.local, localhost.domaine.local, localhost

-inet_interfaces = localhost

Et ajouter la ligne home_mailbox = MailDir/

Relancer postfix...

5/Premiers tests

Pour réaliser les tests utiliser la commande suivante :

telnet [adresse serveur] 25

25 est ici le port de communication du service de mail

Puis utilisez la syntaxe suivante pour envoyer correctement votre mail :

```
HELO mailofthedead.billet.local
250 billet.local
MAIL FROM: <admin@billet.local>
250 ok
RCPT TO: <asterix@billet.local>
250 ok
DATA
354 go ahead
Subject: test de message
blabla
.
```

Puis pour visualiser le mail envoyer se rendre dans le répertoire home du destinataire puis

MailDir/new/*votre mail* :

```
Return-Path: <admin@billet.local>
X-Original-To: asterix@billet.local
Delivered-To: asterix@billet.local
Received: from mailofthedad.billet.local (localhost [127.0.0.1])
        by mailofthedad.billet.local (Postfix) with SMTP id F11CE3E
        for <asterix@billet.local>; Mon, 12 Oct 2015 09:26:10 +0200 (CEST)
Message-Id: <20151012072644.F11CE3E@mailofthedad.billet.local>
Date: Mon, 12 Oct 2015 09:26:10 +0200 (CEST)
From: admin@billet.local

subject
yoyo
zblaaaaaa
```

Le fichier de log permettant la surveillance du transport de mail :

/var/log/mail.log :

```
Oct 12 09:24:43 mailofthedad postfix/smtpd[1868]: connect from localhost[127.0.0.1]
Oct 12 09:26:44 mailofthedad postfix/smtpd[1868]: F11CE3E: client=localhost[127.0.0.1]
Oct 12 09:27:12 mailofthedad postfix/cleanup[1874]: F11CE3E: message-id=<20151012072644.F11CE3E@mailofthedad.billet.local>
Oct 12 09:27:12 mailofthedad postfix/qmgr[1672]: F11CE3E: from=<admin@billet.local>
Oct 12 09:27:12 mailofthedad postfix/local[1875]: F11CE3E: to=<asterix@billet.local>
Oct 12 09:27:12 mailofthedad postfix/qmgr[1672]: F11CE3E: removed
Oct 12 09:27:23 mailofthedad postfix/smtpd[1868]: disconnect from localhost[127.0.0.1]
Oct 12 09:27:34 mailofthedad postfix/master[990]: terminating on signal 15
```

6/ Configuration de PostFix en serveur domaine

Pour ce faire installer Dovecot qui est un serveur IMAP et POP3 pour les systèmes Unix :

Apt-get install dovecot-common dovecot-pop3d

Et modifier la ligne de votre fichier **/etc/postfix/master.cf** de cette façon :

```
dovecot unix      -      n      n      -      -      pipe
 flags=DRhu user=facteur:facteur argv=/usr/lib/dovecot/deliver -f ${sender} -d${user}@${nexthop}
```

Puis on configure en premier lieu sans sécurité les 3 fichiers : **10-auth.conf**, **20.pop3.conf**, **10-mail.conf** qui sont situés dans /etc/dovecot/conf.d/

```
protocols = pop3
disable_plaintext_auth = no
pop3_uidl_format = %08Xu%08Xv
mail_location = maildir:/home/%u/MailDir
```

10-auth.conf →

Puis restartez dovecot.

Tester la bonne réactivité de dovecot :

telnet [adresse serveur] 110

```
Trying 192.168.1.123...
Connected to 192.168.1.123.
Escape character is '^]'.
+OK Dovecot ready.
```

7/Installation d'un serveur IMAP

Installation du paquet :

Apt-get install dovecot-imapd

Et ajout de imap dans la ligne protocols de dovecot.conf

8/Installation et configuration de Squirrelmail

Squirrelmail est un service permettant la mise en place d'un Webmail, il nécessite les paquets suivant pour fonctionner.

Apt-get install squirrelmail

apt-get install apache2

apt-get install php5

puis on lance la configuration de squirrelmail :

squirrelmail-configure

Chargez les paramètres IMAP préconfiguré pour dovecot.

Squirrel mail supporte mal la langue française en iso-8859-1 utilisez le utf-8

Pour cela modifier le fichier **/usr/share/squirrelmail/functions/i18n.php**

Modifier Les lignes suivante(ctrl+w :\$languages['fr_FR']) :

```
$languages['fr_FR']['NAME'] = 'French';
$languages['fr_FR']['CHARSET'] = 'UTF8';
$languages['fr_FR']['LOCALE'] = array('fr_FR.UTF8', 'fr_FR.UTF-8', 'fr_FR');
$languages['fr']['ALIAS'] = 'fr_FR';
```

Puis pour ajouter la traduction des messages : **apt-get install squirrelmail-locales**

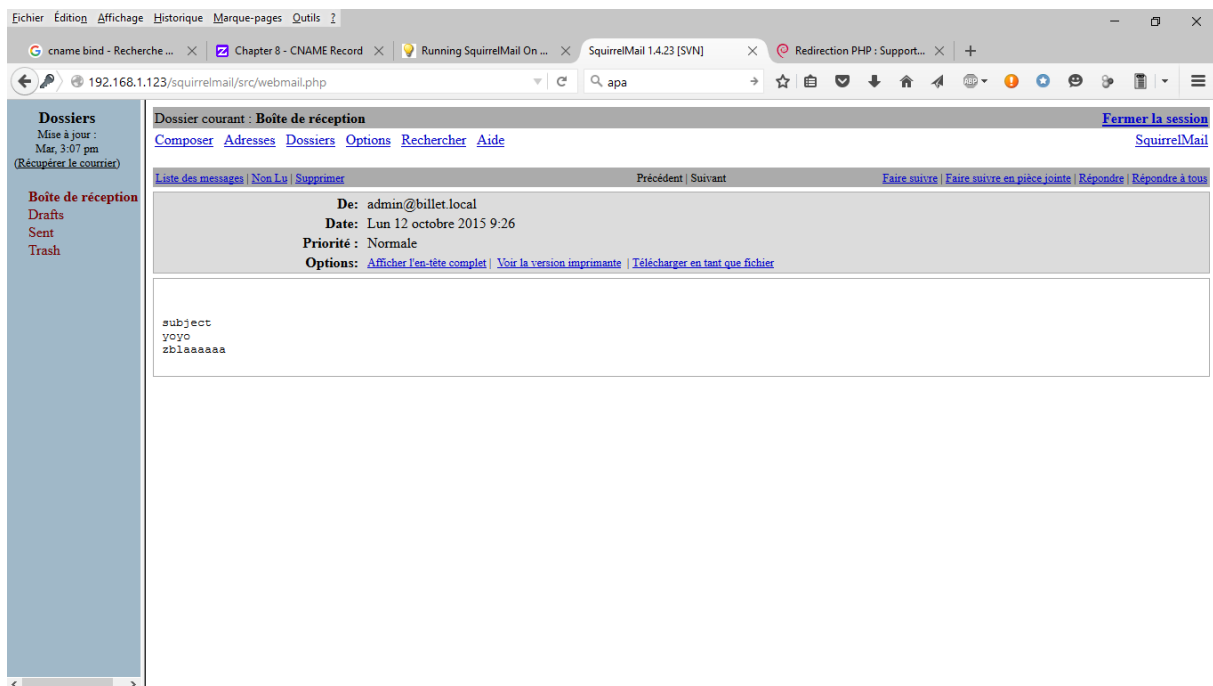
Établissez un lien entre /var/www/html et /usr/share/squirrelmail/

ln -s /usr/share/squirrelmail/ /var/www/html/

puis la commande de test **lsof -i :143** pour tester l'état des ports IMAP*

```
COMMAND PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd   1 root   33u  IPv4 11049     0t0  TCP *:imap2 (LISTEN)
systemd   1 root   34u  IPv6 11050     0t0  TCP *:imap2 (LISTEN)
dovecot  535 root    3u   IPv4 11049     0t0  TCP *:imap2 (LISTEN)
dovecot  535 root    4u   IPv6 11050     0t0  TCP *:imap2 (LISTEN)
```

Nous réceptionnons correctement les mails !



Administration de Squirrelmail

Pour ajouter un utilisateur email à Squirrelmail :

Ajouter d'abord un groupe squirrelmail :

Groupadd squirrelmail

Puis ajouter un utilisateur :

Useradd -c « nom_utilisateur » -s /bin//false -g squirrelmail nom_user

Et définir son mot de passe :

Passwd -c nom_user

9/Sécurisation du serveur de courriers

Installation des paquets des logiciels de sécurisation

```
apt-get install amavis-new spamassassin clamav clamav-daemon zoo
unzip arj nomarch lzop cabextract apt-listchanges libnet-ldap-perl
Clamavdocs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-
perl zip libnet-dnsperl p7zip unrar-free libauthen-sasl-perl
```

Puis editer /etc/postfix/master.cf :

```
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
```

Puis, ajouter la ligne suivante à la fin du fichier **/etc/postfix/main.cf** :

```
Content_filter = amavis:[12.0.0.1] :10024
```

Pour activer les filtres amavis Décommenter les lignes @bypass du fichier **/etc/amavis/conf.d/15-content_filter_mode**

Configuration de la mise en quarantaine :

Modifier le fichier `/etc/amavis/conf.d/50-user` et ajoutez les lignes suivantes pour la mise en quarantaine :

```
GNU nano 2.2.6      Fichier : /etc/amavis/conf.d/50-user
use strict;

# Place your configuration directives here.  They will override those in
# earlier files.
#
# See /usr/share/doc/amavisd-new/ for documentation and examples of
# the directives you can use in this file
#
$QUARANTINEDIR = '/var/pool/virusmails';
$spam_quarantine_method = 'local:spam-%b-%i-%n';
$spam_quarantine_to = 'spam-quarantine';
$final_spam_destiny = D_DISCARD;
$spam_admin = "admin@$mydomain";

#----- Do not modify anything below this line -----
1; # ensure a defined return
```

Ensuite, créer le répertoire `/var/spool/virusmails` pour stocker les virus en quarantaine et lui attribuer les droits : **chown amavis:amavis virusmails**

Activer spam assassin :

Mettre à jour les règles de spam assassin :

sa-update -D

Pour activation de spam assassin :

Editer le fichier `/etc/default/spamassassin` et changer les lignes **ENABLED** et **CRON** à 1

Ajouter l'utilisateur clamav au groupe amavis :

Adduser clamav amavis

Vous pouvez maintenant démarrer les services spamassassin, amavis, clamav-daemon redémarrer postfix et tester votre configuration !

Votre serveur de messagerie est maintenant parfaitement fonctionnel et sécuriser !

FIN !

***Optionel*Mise en place de RainLoop**

RainLoop est un Webmail plus récent que squirrelmail ainsi, il propose une interface plus esthétique et conviviale à l'utilisateur.

Installation de Rainloop :

wget <http://repository.rainloop.net/v2/webmail/rainloop-latest.zip>

et renommez le en **rainloop.zip** dezipez le dans le dossier html :

unzip rainloop.zip -d /var/www/html/

