

Sommaire

Qmail: installation d'un serveur de mail multi-domaine et sécurisé.....	1
Introduction.....	1
Récupération des sources et compilation.....	1
Télécharger les sources.....	1
Compiler Qmail et l'installer.....	2
Installer les utilitaires supplémentaires.....	3
Compiler Vpopmail et l'installer.....	4
Qmail-scanner et F-PROT.....	6
Installation du gestionnaire de mailing list.....	8
Configuration des service mails.....	9
Installation d'autoresponder.....	10
Installation de Qmailadmin.....	10
Utilisation, question courantes, etc	11
Copyright.....	12

Qmail: installation d'un serveur de mail multi-domaine et sécurisé

Qmail: installation d'un serveur de mail multi-domaine et sécurisé
par serge

Un serveur de mail gérant plusieurs domaines, sécurisé et protégé contre les virus.

Introduction

Nous allons voir dans cet article comment installer un serveur de mail pouvant gérer plusieurs domaines (des centaines, voir plus), sécurisé contre l'open relay mais permettant aux utilisateurs authentifiés d'envoyer des mails. De plus, les mails entrant seront scannés à la recherche de virus. Car même si sous linux la plupart des virus mail n'ont aucun effet, il se peut que certains des utilisateurs récupèrent leurs mails sous windows.

Ce serveur de mail comprend aussi un gestionnaire de mailing list et une interface web d'admin des domaines mails.

Pour la compréhension de cet article, vous devez avoir des notions assez avancées sur Linux et son utilisation (commandes shell en ligne, compilation, etc...), et des notions sur les réseaux TCP/IP et de l'internet.

Cet article est une "compilation" d'articles trouvés sur l'internet (en partie l'article qmail sur toolinux), d'HOWTO, et de mon expérience professionnelle de Qmail.

Récupération des sources et compilation

Télécharger les sources

Récupérez tout d'abord les sources de ces différents programmes (attention, vérifiez les liens et versions, je vous donne les versions à jour, à l'heure où j'écris cet article, c'est-à-dire en avril 2002):

- qmail-1.03
- autorespond-2.0.2
- daemontools-0.76
- ucspi-tcp-0.88
- ezmlm-0.53
- ezmlm-idx
- maildrop-1.3.8
- qmail-scanner-1.10
- vpopmail-5.2
- F-PROT (version linux gratuite pour un usage privé, prenez aussi les mises à jours des définitions de virus sur la page download du site).
- Qmailadmin

Oui je sais, ca fait beaucoup de chose à récupérer, j'espère que vous avez un bon modem :)

Compiler Qmail et l'installer

Bon on va commencer par installer Qmail lui même. Détarrez / dézippez les sources de qmail (`tar zxvf qmail-1.0.3.tar.gz`). Nous allons devoir patcher légèrement les sources de Qmail pour notre besoin. Entrez dans le répertoire des sources de Qmail, et éditez le fichier Makefile, et remplacez :

- La ligne **1486** `auto_split.o` par `auto_split.o env.a`
- La ligne **1491** `substdio.a error.a str.a fs.a auto_qmail.o auto_split.o` par `substdio.a error.a str.a fs.a auto_qmail.o auto_split.o env.a`

De même, éditez le fichier qmail.c et :

- ajoutez en dessous de la ligne **8** `#include "env.h"` en dessous de la ligne `#include "auto_qmail.h"`
- remplacez la ligne **10** `static char *binqqargs[2] = { "bin/qmail-queue", 0 } ;` par `static char *binqqargs[2] = { 0, 0 } ;`

-Ajoutez juste au-dessous de la ligne que vous venez de modifier les lignes suivantes:

```
static void setup_qqargs()
{
if(!binqqargs[0])
binqqargs[0] = env_get("QMAILQUEUE");
if(!binqqargs[0])
binqqargs[0] = "bin/qmail-queue";
}
```

et enfin au-dessous des lignes (vers la ligne **23**)

```
int qmail_open(qq)
struct qmail *qq;
{
int pim[2];
int pie[2];
```

vous ajoutez:

```
setup_qqargs();
```

Remarque: Ce patch est uniquement nécessaire pour pouvoir utiliser `qmail-scanner`, qui va nous permettre de scanner tout mail entrant à la recherche de virus. En fait, ce patch ajoute une variable d'environnement `QMAILQUEUE`. Si cette variable est vide, Qmail utilise son propre programme de "queue" (file d'attente des mails entrant et sortant), autrement cette variable contient le nom du programme de queue de remplacement à utiliser. Nous utiliserons alors la "queue" de `qmail-scanner` qui appellera notre programme antivirus (`F-PROT`) pour scanner tous les mails.

Maintenant que Qmail est patché, nous allons pouvoir le compiler. Mais avant cela, nous devons créer des comptes utilisateurs, qui de plus vont servir pour le chemin d'installation de Qmail. Dans cet article, le chemin d'installation est celui par défaut, c'est à dire `/var/qmail`

Nous créons ces comptes utilisateurs par les commandes (en **root** bien sur):

Reseau-message-qmail

```
groupadd nofiles
useradd -g nofiles -d /var/qmail/alias alias
useradd -g nofiles -d /var/qmail qmaild
useradd -g nofiles -d /var/qmail qmaill
useradd -g nofiles -d /var/qmail qmailp
groupadd qmail
useradd -g qmail -d /var/qmail qmailq
useradd -g qmail -d /var/qmail qmailr
useradd -g qmail -d /var/qmail qmails
```

Remarque: Si vous souhaitez installer Qmail dans un autre répertoire que `/var/qmail`, modifiez les commandes ci-dessus avec le chemin souhaité.

Il nous reste plus qu'à compiler Qmail:

```
make setup check
```

Configurons maintenant Qmail, via la commande :

```
./config-fast `hostname --fqdn`.
```

Vous devez voir apparaître quelque chose du style :

```
Your fully qualified host name is mailhub.lea-linux.org
Putting tarsier.lea-linux.org into control/me...
Putting lea-linux.org into control/defaultdomain...
Putting lea-linux.org into control/plusdomain...
.....
```

Si vous avez une erreur ou autre insulte de la sorte, essayez en remplaçant "`hostname --fqdn``" par votre nom d'hôte complet (par exemple `./config-fast mailhub.lea-linux.org`)

Qmail utilise deux styles de mailbox (boîte aux lettres) différents : le mbox traditionnel comme sendmail (un fichier nommé comme le login de l'utilisateur contenant tout les mails de l'utilisateur dans `/var/mail`) ou un répertoire Maildir à structure spéciale contenant les mails dans des fichiers séparés. Pour notre cas nous utiliserons Maildir, car vpopmail se base dessus.

Pour cela, il suffit de copier un fichier:

```
cp /var/qmail/boot/home /var/qmail/rc
```

Qmail n'est pas tout à fait complètement installé, mais pour la suite nous allons devoir installer les daemontools et ucspi de façon à avoir des performances optimales pour notre serveur de mails.

Installer les utilitaires supplémentaires

De façon à avoir de meilleures performances pour notre serveur de mails et pour une plus grande souplesse, pour "logger" les événements mails, nous devons installer les outils développés par Dan Bernstein :

daemontools et ucspi-tcp.

Pour les installer, rien de plus simple, vous dézippez / détarrez les sources comme d'habitude.

Pour les daemontools, un répertoire admin a été créé lors du "détarrage":

```
cd admin/daemontools/  
./package/install
```

Il ne reste plus qu'à compiler / installer ucspi:

```
cd ucspi-tcp-0.88  
make setup check
```

Compiler Vpopmail et l'installer

Comme d'habitude, on dézippe / détarre les source de Vpopmail. Avant de lancer la compilation, il faut, comme pour Qmail, créer les comptes utilisateurs de vpopmail, qui vont aussi déterminer le chemin d'installation de vpopmail.

Pour ma part, pour des questions de "cohérence" avec Qmail, je l'installe dans /var/vpopmail. De plus je trouve logique de l'installer dans /var, car c'est le repertoire où l'on trouve normalement tout les fichiers qui varient en permanence (mail, logs, pid, etc...). Donc, nous faisons (en **root** bien sur) :

```
groupadd -g 89 vchkpw  
useradd -g vchkpw -u 89 -d /var/vpopmail vpopmail
```

Remarque: changez le chemin /var/vpopmail par le chemin d'installation que vous désirez bien sur

Vous devez créer le répertoire de Vpopmail avant de continuer, pour notre exemple:

```
mkdir /var/vpopmail
```

Vpopmail possède un script de configuration avant la compilation (le bien connu **./configure**), auquel nous allons passer les options nécessaires à notre cas.

Voici les options que nous allons utiliser, avec une brève explication pour chaque option:

```
--prefix=/var/vpopmail  
Répertoire de base de vpopmail
```

```
--enable-clear-passwd=y
```

Ce qui permet de stocker une copie des mots de passe POP des utilisateurs en clair. C'est peut-être moins sécurisé, mais c'est toujours pratique pour retrouver le mot de passe de l'un de vos utilisateurs qui l'aurait perdu. Si vous êtes parano, n'activez pas cette option.

```
--enable-valias=y
```

Permet d'utiliser les alias mails (plusieurs noms possibles pour un même compte POP)

```
--enable-default-domain=votre domaine
```

Indique le domaine primaire de votre machine. A mettre absolument, autrement vous allez devoir créer le

Reseau-message-qmail

compte de chaque utilisateur pour le domaine principal du serveur de mail.

```
--enable-roaming-users=y
```

Permet une authentification POP before SMTP pour activer le relaying.

Explication sur cette option:

Vous avez sûrement entendu parler du "relaying" pour les serveurs mails, l'open relay, etc... Pour résumer ce problème, normalement un serveur de mail (comme la plupart des serveurs de mails des FAI) interdisent aux utilisateurs d'envoyer des mails si l'IP de l'utilisateur n'est pas une IP du même réseau que le serveur de mail. Par exemple, les serveurs de mails wanadoo refusent que vous envoyiez des mails si vous n'avez pas une IP wanadoo (c.a.d si vous ne vous êtes pas connecté à l'internet via leur propre service), cela pour des raisons de sécurité, de lutte anti-spam, de charge serveur et aussi économique.

La plupart des sociétés ayant leur propre serveur de mail font de même. Si vous ne faites pas ça, votre serveur est considéré comme un "open-relay", ce qui n'est pas bien du tout (je vais pas expliquer pourquoi ici, ça prendrait trop de temps).

Mais se pose alors un problème: vous êtes une grosse société, avec 5 000 collaborateurs. Vos collaborateurs voyagent beaucoup et ont besoin d'utiliser le serveur de mail de la société. Comme ils sont en déplacement à l'extérieur de la société, ils n'ont pas d'IP de la société (ils sont connectés via un FAI quelconque), et le serveur de mail n'autorise pas le relaying (c'est à dire envoyer un mail d'un utilisateur dont l'IP n'est pas une IP de la société). Comment faire alors ?

On a alors inventé le POP before SMTP pour permettre le relaying. Comment ça marche? Très simple.

L'utilisateur doit tout d'abord "popper" sa boîte aux lettres (c'est à dire relever ses mails, c'est la chose que vous faites chaque fois que vous regardez avec votre client mail si vous avez reçu un nouvel e-mail).

Lorsque l'utilisateur "poppe" sa boîte aux lettres, il s'identifie sur le serveur en fait (le POP demande obligatoirement un nom d'utilisateur et un mot de passe). Si l'identification est OK, le serveur distribue les mails.

Comme l'utilisateur est identifié, on va alors se dire "ok l'utilisateur est connu, il est de chez nous", on va alors enregistrer son adresse IP actuelle et permettre à cette adresse IP d'envoyer des mails pendant un certain temps que l'on peut définir (voir plus bas dans l'article). Donc en résumé (si vous n'avez rien compris), si vous voulez que votre serveur de mail soit utilisable pour envoyer des mails à partir de n'importe où dans le monde, à partir du moment où l'on a une boîte aux lettres sur votre serveur, activez cette option.

Donc, je vous redonne les options que nous utilisons ici :

```
./configure --enable-clear-passwd=y --enable-valias=y  
--enable-default-domain=lea-linux.org --enable-roaming-users=y
```

Puis on le compile / installe:

```
make  
make install-strip
```

Comme les "headers" de vpopmail sont nécessaires pour la compilation d'autres programmes (qmailadmin par exemple), nous devons les copier dans un répertoire d'include. Pour cela:

```
cp /var/vpopmail/include/* /usr/include
```

Pour que vpopmail trouve bien les fichiers de tcpserver, il faut refaire le répertoire etc/ de vpopmail:

```
mv /var/vpopmail/etc/* /etc
```

```
rmdir /var/vpopmail/etc  
ln -s /etc /var/vpopmail/etc
```

Qmail-scanner et F-PROT

Avant d'installer Qmail-scanner, vous devez vous assurer d'avoir Perl 5.005_03 (ou supérieur) sur votre machine (c'est le cas avec toutes les distrib récentes) et les modules Perl:

Time::HiRes

DB_File

Sys::Syslog

Pour vous en assurer, installez-les via CPAN. Pour se faire, vous devez être connecté à internet, et lancez alors la commande:

```
perl -MCPAN -e shell;
```

Remarque: Si c'est la première fois que vous lancez CPAN, vous allez devoir le configurer. Je ne vous explique pas ici comment configurer CPAN.

Toutefois, la plupart du temps il suffit de valider les options proposées par défaut

Une fois CPAN lancé, demandez l'installation des modules via:

```
install Time::HiRes  
install DB_File  
install Sys::Syslog  
exit (pour sortir du CPAN)
```

Nous allons aussi dès à présent installer F-PROT. Dgzippez / Détarrez f-prot dans le répertoire /usr/local et installez le via:

```
cd /usr/local  
tar zxvf /ou/se/trouve/votre/fp-linux_sb.tar.gz  
ln -fs fp-linux_312/ f-prot  
ln -fs /usr/local/f-prot/f-prot.sh bin/f-prot  
ln -fs /usr/local/f-prot/f-prot.8 man/man8/  
chmod +x /usr/local/f-prot/f-prot*
```

Mettez aussi à jour les signatures antivirales de F-PROT (**Faites-le le plus souvent possible si vous voulez un bonne protection antivirale de vos mails!**)

Téléchargez les deux zip de mise à jour de signature de f-prot et dézipé-les dans /usr/local/f-prot.

Avant d'installer Qmail-scanner, nous devons installer Maildrop, indispensable pour Qmail-scanner.

```
tar zxvf maildrop-1.3.8.tar.gz  
cd maildrop-1.3.8  
./configure  
make
```

Reseau-message-qmail

```
make install
```

Passons maintenant à Qmail-scanner.

Dézipper / Décompresser Qmail-scanner, puis son répertoire de source lancez `./configure` avec les options suivantes:

```
--admin user
```

(voir en-dessous pour la valeur de user)

```
--domain votre_domaine
```

Pour comprendre les valeurs à mettre dans ces options, prenons le cas où nous voulons que tous les mails d'alerte de détection virale soient envoyés à `admin@lea-linux.org`, vous devez alors mettre `admin` pour le user et `lea-linux.org` pour le domaine.

```
--notify all
```

Pour prévenir l'administrateur, l'envoyeur et la personne qui auraient dû recevoir le mail, qu'un mail contaminé a été intercepté

```
--redundant yes
```

Permettre le scan des fichiers zips, etc...

Pour notre exemple, nous lançons donc:

```
./configure --admin admin --domain lea-linux.org --notify all --redundant yes --install
```

Attention: Vous risquez d'avoir une erreur du type:

```
YOU HAVEN'T DISABLED SET-ID SCRIPTS IN THE KERNEL YET!  
FIX YOUR KERNEL, PUT A C WRAPPER AROUND THIS SCRIPT, OR USE -u AND  
UNDUMP!
```

```
***** FATAL ERROR *****
```

Cette erreur est "normale" si votre distribution comporte une version de Perl qui interdit que des script Perl soient lancés en SET-ID pour des raisons de sécurité (cas de la slackware par exemple). En effet, lancer les scripts en SET-ID signifie que le script est lancé avec les droits d'un utilisateur spécifique. Certaines distributions interdisent cela (pour empêcher de lancer des script Perl qui prendraient les droits root par exemple et pourraient faire des choses pas très gentilles). Dans ce cas (et **que** dans ce cas-là, c'est-à-dire que vous avez l'erreur énoncée ci-dessus) vous devez:

```
cd contrib  
make  
make install
```

Vous devez voir apparaître alors:

```
install -o qmailq -g qmail -m4755 qmail-scanner-queue  
/var/qmail/bin/qmail-scanner-queue
```

Reseau-message-qmail

Revenez dans le répertoire des sources de Qmail-scanner (`cd ..`) et vous éditez le fichier `qmail-scanner-queue.pl` et vous remplacez:

```
#!/usr/bin/suidperl -T
```

par:

```
#!/usr/bin/perl
```

Copiez enfin ce fichier dans `/var/qmail/bin` en placant les bons droits :

```
cp qmail-scanner-queue.pl /var/qmail/bin/  
chown qmailq.qmail /var/qmail/bin/qmail-scanner-queue*
```

Dans tout les cas, il faut initialiser qmail-scanner maintenant.

Si vous n'avez pas eu l'erreur ci-dessus, tapez ces commandes:

```
qmail-scanner-queue.pl -g  
qmail-scanner-queue.pl -z
```

Si vous avez eu l'erreur lors de l'installation, les commandes alors sont celles-ci:

```
qmail-scanner-queue -g  
qmail-scanner-queue -z
```

Installation du gestionnaire de mailing list

Ezmlm est le gestionnaire de mailing de Qmail. Pour l'installer, détarrez / dgzippez `ezmlm` et `ezmlm-idx`. Puis copiez le contenu de `ezmlm-idx` dans le répertoire de `ezmlm`:

```
tar zxvf ezmlm-0.53.tar.gz  
tar zxvf ezmlm-idx-0.40.tar.gz  
mv ezmlm-idx-0.40/* ezmlm-0.53/
```

Patchez alors `ezmlm`:

```
cd ezmlm-0.53  
patch < idx.patch
```

et compilez, installez le tout:

```
make clean  
make  
make man
```

Configuration des service mails

Maintenant que le plus "gros" est installé, nous allons créer le script de démarrage de ces services. Créez un fichier `rc.startmail` dans `/etc/rc.d` comprenant:

```
#!/bin/bash
export
PATH="/usr/local/bin:/var/qmail/bin:/var/vpopmail/bin:/usr/local/bin/ezmlm:$PATH"
echo "Starting Qmail and Vpopmail daemons ..."
export QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
/var/qmail/rc &
/usr/local/bin/tcpserver -v -H -R -x /etc/tcp.smtp.cdb -c20 -u1033 -g103
0 smtp
\ /usr/local/bin/recordio /var/qmail/bin/qmail-smtpd 2>&1 >/dev/null &
/usr/local/bin/tcpserver -v -H -R 0 pop3 /usr/local/bin/recordio
/var/qmail/bin/qmail-popup
\ mailhub.lea-linux.org /var/vpopmail/bin/vchkpw
/var/qmail/bin/qmail-pop3d Maildir &
```

Remarque: Ne coupez pas les lignes de ce script. Regardez bien ce qui est marqué au dessus, le caractère "\" dans le texte au dessus signale qu'il s'agit de la même ligne que celle qui a commencé au dessus, le retour de ligne est du a la mise en page HTML. C'est à dire que si vous lisez:

```
tuc machin
\ bidule
```

vous devez lire une seule ligne:

```
truc machin bidule
```

Il ne faut pas, bien sur copier, le "\".

Attention: Si vous avez eu l'erreur dans `Qmail-scanner` à propos des script `SET-ID`, modifiez la ligne comprenant `export QMAILQUEUE` par:

```
export QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue"
```

Ajoutez alors dans votre `/etc/rc.d/rc.local` une ligne du type:

```
/etc/rc.d/rc.startmail
```

Ou si votre distribution est basée sur `sysVinit`, créez les scripts correspondant dans les niveaux d'init que vous souhaitez.

Reste à configurer quelques fichiers. Tout d'abord, il faut régler le temps d'authentification des utilisateurs par le pop (POP before SMTP). Pour cela, nous editons la crontab et donnons l'intervalle de temps, puis il faut nettoyer les identifications:

```
crontab -e
```

et placez une ligne du type:

Reseau-message-qmail

```
40 * * * * /var/vpopmail/bin/clearopensmtp 2>&1 > /dev/null
```

Pour nettoyer toutes les 40 minutes.

Il faut définir aussi quel est votre adresse réseau, pour autoriser ce réseau à utiliser le serveur de mail. Prenons l'exemple où les utilisateurs de votre serveur de mails se trouvent sur les réseaux 192.168.0.0 (local) et 213.30.139.0 (public), il faut alors éditer le fichier `/etc/tcp.smtp` et y mettre:

```
127.:allow,RELAYCLIENT=" "  
192.168.0.:allow,RELAYCLIENT=" "  
213.30.139:allow,RELAYCLIENT=" "
```

l'adresse 127 doit **absolument** y être, autrement le serveur ne peut pas fonctionner!

Construisez alors la base de données de ces adresses:

```
tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
```

Installation d'autoresponder

Ce programme permet de répondre automatiquement aux mails reçus (pour signaler une absence par exemple).

Pour l'installer, c'est très simple:

```
tar zxvf autorespond-2.0.2.tar.gz  
cd autorespond-2.0.2  
make  
make install
```

Installation de Qmailadmin

Il nous reste plus qu'à installer l'interface cgi Web de la gestion des comptes mails.

Pour cela:

```
tar zxvf qmailadmin-1.0.2  
cd qmailadmin-1.0.2  
./configure --enable-htmldir=/var/www  
make  
make install
```

Attention: Remplacez `--enable-htmldir=/var/www` par le chemin de votre racine web. Je suppose que vous savez configurer apache pour que le répertoire de cgi soit valide et fonctionnel.

Utilisation, question courantes, etc ...

Je vous donne ici brièvement les commande pour créer un nouveau domaine mails, les comptes, etc...

Je suppose bien sûr que vous savez gérez vos DNS pour que le champ MX du domaine pointe vers le serveur de mails.

– Ajouter un nouveau domaine que votre serveur de mails va héberger :

```
/var/vpopmail/vadddomain domaine.com
```

Vous allez devoir rentrer le mot de passe du "postmaster", c'est-à-dire de l'administrateur mails de ce domaine.

Pour créer les comptes pop, utiliser qmailadmin. Tapez l'url dans votre navigateur pour pointer sur le cgi de qmailadmin, dans user laissez "postmaster", dans domaine, mettez le domaine que vous voulez gérer et pour le mot de passe, mettez le mot de passe du postmaster.

Dans l'interface se trouvent tout les liens pour créer les mails etc...

– Effacer un domaine:

```
/var/vpopmail/vdeldomain domaine.com
```

Quand vous configurez votre client mail pour lire les mails reçus, faites attention dans la partie "nom utilisateurs" de mettre de la forme:

```
utilisateur@domaine.com
```

car les logiciels de mail mettent par défaut "utilisateur" tout court.

Si lors du démarrage des services vous avez des erreurs du style:

```
unable to bind: adresses in use
```

ou quelque chose de similaire, c'est que vous avez déjà un serveur de mail et/ou pop3 de lancé. Désinstallez tout autre serveur de mail/pop3 (sendmail, gnu-pop3d,...), vérifiez aussi dans `.etc/inetd.conf` ou dans `/etc/xinet.d/` que les services smtp, pop3 ne sont pas utilisés par d'autres programmes.

Lisez les documentations d'utilisation de ezmlm, ezmlm-idx pour la gestion des mailing lists.

Qmailadmin vous permet de "fabriquer" vos propres pages d'administration mail, etc... avec de nombreux exemples installés dans `/usr/local/share/qmailadmin`

Pour que vous puissiez gérer les mails d'un domaine, vous devez configurer un MX dans le fichier de zone de ce domaine qui pointe vers votre serveur. Lisez les documentions des serveurs DNS.

Cette page est issue de la documentation 'pré-wiki' de Léa a été convertie avec HTML::WikiConverter. Elle fut créée par Serge Tchsmeli.

Copyright

Copyright © Serge Tchesmeli

*Vous avez l'autorisation de copier, distribuer et/ou modifier ce document suivant les termes de la **Licence pour documents libres**, Version 1.1 publiée par la La Guilde des Doctorants. Pour plus d'informations consulter la LDL sur le site de La Guilde des Doctorants.*