

INSTALLATION ET CONFIGURATION SYSTEME DE MESSAGERIE REDONDANTE POSTFIX, OPENLDAP & JAMM

Pierre PATAKI (pierre@pataki.nom.fr) – www.deus-rulez.com

INSTALLATION DES PAQUETS

Nous allons installer tous les paquets nécessaires au bon fonctionnement de la messagerie. Sur le qui hébergera le service MTA (Mail Transfert Agent) nommé Courier, nous installons les paquets suivants avec la commande :

```
#apt-get install postfix postfix-ldap postfix-doc postfix-tls sasl2-bin \  
  libsasl2-modules libsasl2 courier-pop courier-imap \  
  courier-imap-ssl courier-pop-ssl courier-base courier-authdaemon \  
  courier-ldap postfix-pcre clamav clamav-daemon amavisd-new
```

Configuration Postfix :

- Type de configuration : Site Internet
- A qui envoyer le courrier pour root : votre utilisateur principal
- Nom de courrier : localhost.localdomain
- Pour quelles autres destinations accepter le courrier ? : localhost.localdomain, localhost
- Forcer les mises à jour synchronisées de la file d'attente ? : oui

Configuration Courier-Base :

- Faut-il créer les répertoires web : non

CONFIGURATION DES UTILISATEURS VMAIL

Ajout des utilisateurs VMAIL :

```
#groupadd -g 5000 vmail  
#useradd -g vmail -u 5000 -d /home/vmail -m vmail
```

CONFIGURATION DE POSTFIX

POSTFIX peut être complexe à configurer. Il existe une multitude de fonctions, de commandes et de paramètres à personnaliser. Ici nous irons droit au but, pour une configuration standard fonctionnelle. Libre à vous de consulter la documentation sur <http://www.postfix.org/> et optimiser POSTFIX selon vos besoins particuliers.

Nous retrouvons ci-dessous notre fichier de configuration. La variable 'myhostname' est à changer avec le nom d'hôte de votre serveur POSTFIX. Pour notre part, nous avons configuré ce nom d'hôte dans /etc/hosts. Nous définissons ici le chemin vers les différents fichiers de configuration que nous avons créé auparavant, nous permettant l'accès à la base de donnée OpenLDAP.

/etc/postfix/main.cf

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete  
version  
  
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)  
biff = no
```

```

# appending .domain is the MUA's job.
append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

myhostname = mail.madservers.fr
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = mail.madservers.fr, localhost.madservers.fr, localhost
relayhost =
mynetworks = 127.0.0.0/8 192.168.1.0/24
mailbox_command =
home_mailbox = Maildir/
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
luser_relay =

#la directive suivante correspond à la liste des domaines pris en charge.
virtual_mailbox_domains = ldap:/etc/postfix/ldap-domains.cf
# le répertoire /home/vmail stockera les boites mail des utilisateurs
virtual_mailbox_base = /home/vmail/domains
#la directive suivante correspond à la liste des utilisateurs déclarés.
virtual_mailbox_maps = ldap:/etc/postfix/ldap-accounts.cf
virtual_minimum_uid = 100
virtual_gid_maps = static:5000
virtual_uid_maps = static:5000
#la directive suivante correspond à la liste des alias (redirections).
virtual_alias_maps = ldap:/etc/postfix/ldap-aliases.cf
unknown_local_recipient_reject_code = 450

smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_mynetworks,
permit_sasl_authenticated, reject_unauth_destination
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/postfix/smtpd.cert
smtpd_tls_key_file = /etc/postfix/smtpd.key

content_filter = amavis:[127.0.0.1]:10024
receive_override_options = no_address_mappings

```

/etc/postfix/ldap-accounts.cf

```

mail-c-p:/etc/postfix$ vi ldap-accounts.cf
server_host = ldap-esclave.madservers.fr
server_port = 389
search_base = dc=madservers, dc=fr
query_filter =
(&(objectClass=JammMailAccount) (mail=%s) (accountActive=TRUE) (delete=FALSE))
result_attribute = mailbox
bind = yes
bind_dn = cn=admin, dc=madservers, dc=fr
bind_pw = ertyui
version = 3

```

/etc/postfix/ldap-domains.cf

```
server_host = ldap-esclave.madservers.fr
server_port = 389
search_base = dc=madservers, dc=fr
query_filter = (&(objectClass=JammVirtualDomain) (jvd=%s) (accountActive=TRUE) (delete=FALSE)
)
result_attribute = jvd
bind = yes
bind_dn = cn=admin, dc=madservers, dc=fr
bind_pw = ertyui
version = 3
```

/etc/postfix/ldap-aliases.cf

```
server_host = ldap-esclave.madservers.fr
search_base = dc=madservers, dc=fr
query_filter = (&(objectClass=JammMailAlias) (mail=%s) (accountActive=TRUE))
result_attribute = maildrop
bind = yes
bind_dn = cn=admin, dc=madservers, dc=fr
bind_pw = ertyui
version = 3
```

/etc/saslauthd.conf

```
ldap_servers: ldap://ldap-esclave.madservers.fr:389/
ldap_search_base: DC=madservers,DC=fr
ldap_timeout: 10
ldap_filter:
(&(objectClass=JammMailAccount) (mail=%u) (accountActive=TRUE) (delete=FALSE))
ldap_bind_dn: CN=admin,DC=madservers,DC=fr
ldap_password: ertyui
ldap_deref: never
ldap_restart: yes
ldap_scope: sub
ldap_use_sasl: no
ldap_start_tls: no
ldap_version: 3
ldap_auth_method: bind
```

Concernant le fichier smtpd.conf, nous devons activer le plugin LDAP pour qu'il puisse être interfacé avec notre serveur de base de donnée. C'est la variable 'auxprop_plugin' qui nous le permet.

/etc/postfix/sasl/smtpd.conf

```
pwcheck_method: saslauthd
mech_list: plain
```

Pour gérer les connexions sécurisées aux serveurs SMTP, POP et IMAP, nous devons générer un certificat SSL. Vous pouvez le faire générer par un organisme tiers de confiance ou le faire vous-même, solution moins chère mais qui peut poser problèmes, notamment lors de l'utilisation d'Outlook Express qui grince des dents lors d'utilisation de certificats auto-validés.

Le certificat doit être déposé dans le même répertoire que POSTFIX et est généré avec une clé RSA de 2048 bits. En France, il est interdit de créer des clés dépassant les 1024 bits. Faites donc attention pour ne pas rentrer en conflit avec la législation de votre pays.

```
#openssl req -new -outform PEM -out /etc/postfix/smtpd.cert \  
-newkey rsa:2048 -nodes -keyout /etc/postfix/smtpd.key \  
-keyform PEM -days 3650 -x509
```

Une fois exécutée, la commande va vous demander quelques informations vous concernant. N'hésitez pas à remplir le plus consciencieusement possible celles-ci, elles seront visibles aux utilisateurs qui voudront avoir des informations sur votre certificat SSL.

CONFIGURATION DU POP3/IMAP

Il faut désormais autoriser les modules d'authentification à accéder à la base de donnée LDAP. Ceci se fait au travers des fichiers de configurations énumérés ci-dessous.

/etc/courier/authdaemonrc

```
authmodulelist="authldap"
```

/etc/courier/authldaprc

```
LDAP_SERVER ldap-esclave.madservers.fr  
LDAP_PORT 389  
LDAP_PROTOCOL_VERSION 3  
LDAP_BASEDN dc=madservers, dc=fr  
LDAP_BINDDN cn=admin, dc=madservers, dc=fr  
LDAP_BINDPW ertyui  
LDAP_TIMEOUT 5  
LDAP_MAIL mail  
LDAP_FILTER  
(objectClass=JammMailAccount) (accountActive=TRUE) (delete=FALSE)  
LDAP_GLOB_UID vmail  
LDAP_GLOB_GID vmail  
LDAP_HOMEDIR homeDirectory  
LDAP_MAILDIR mailbox  
LDAP_DEFAULTDELIVERY defaultDelivery  
LDAP_FULLNAME cn  
LDAP_CRYPTPW userPassword
```

Il faut créer au final est répertoires où seront stockés les mails

```
#mkdir /mnt/mails  
#ln -s /mnt/mails /home/vmail/domains
```

CONFIGURATION DE L'ANTISPAM/ANTIVIRUS

Ajoutez l'utilisateur clamav au groupe amavisd.

```
#adduser clamav amavisd
```

Ajoutez ce qui suit à la fin du fichier `/etc/postfix/master.cf`

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

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_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks=127.0.0.0/8
  -o strict_rfc821_envelopes=yes
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
```

Un détail du fichier log de postfix nous indique qu'un mail passe bien par l'antivirus et l'antispam :

```
May 20 04:15:31 localhost amavis[910]: (00910-01) Passed,
<mboukobza@madservers.fr> -> <mboukobza@madservers.fr>, Message-ID:
<005701c67c0e$1a532200$b601a8c0@osiris>, Hits: -
```

INSTALLATION ET CONFIGURATION SYSTEME D'ANNUAIRE OPENLDAP

Nous installons un service d'annuaire répliqué sur deux serveurs différents. Le serveur maître est celui sur lesquels s'effectueront les modifications au niveau de JAMM, le serveur esclave sera celui qui se répliquera en fonction du maître.

L'installation de l'annuaire OpenLDAP se fait avec la commande qui suit

```
#apt-get install slapd
```

Répondez aux questions posées :

- DNS domain name : madservers.fr (ce qui donnera dc=madservers,dc=fr)
- Organization name : MADSERVERS SA
- Admin password : Un mot de passe sécurisé de préférence avec min/maj/alphanum
- Aucune autorisation du LDAPv2

Démarrage du service OpenLDAP

```
#/etc/init.d/slapd restart
```

Pour pouvoir manipuler le serveur LDAP l'installation de paquets de gestion est nécessaire :

```
#apt-get install ldap-utils
```

Pour accroître la sécurité du système OpenLDAP et interdire ainsi tout accès anonyme nous devons modifier quelques paramètres dans le fichier de configuration **/etc/ldap/slapd.conf**

Le fichier de configuration du serveur LDAP esclave :

/etc/ldap/slapd.conf

```
allow bind_v2
include          /etc/ldap/schema/core.schema
include          /etc/ldap/schema/cosine.schema
include          /etc/ldap/schema/nis.schema
include          /etc/ldap/schema/jamm.schema
include          /etc/ldap/schema/inetorgperson.schema
schemacheck     on
pidfile          /var/run/slapd/slapd.pid
argsfile         /var/run/slapd.args
loglevel        0
modulepath       /usr/lib/ldap
moduleload       back_bdb
backend          bdb
checkpoint 512 30
database         bdb
suffix           "dc=madservers,dc=fr"
directory        "/var/lib/ldap"
index            objectClass eq
lastmod          on
access to attrs=userPassword
    by dn="cn=admin,dc=madservers,dc=fr" write
    by anonymous auth
    by self write
    by * none
access to dn.base="" by * read
access to *
    by dn="cn=admin,dc=madservers,dc=fr" write
    by * read
```

```
updatered      ldap://ldap.madservers.fr:389/
updatedn       "cn=admin,dc=madservers,dc=fr"
```

Et celui du maître :

/etc/ldap/slapd.conf

```
allow bind_v2
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/jamm.schema
include         /etc/ldap/schema/inetorgperson.schema
schemacheck    on
pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd.args
loglevel        255
modulepath      /usr/lib/ldap
moduleload      back_bdb
backend         bdb
checkpoint 512 30
database        bdb
suffix          "dc=madservers,dc=fr"
password-hash   {CRYPT}
directory       "/var/lib/ldap"
index           objectClass      pres,eq
index           mail,cn          eq,sub
lastmod         on
access to attrs=userPassword
    by dn="cn=admin,dc=madservers,dc=fr" write
    by anonymous auth
    by self write
    by * none
access to dn.base="" by * read
access to *
    by dn="cn=admin,dc=madservers,dc=fr" write
    by * none
access to dn.regex=".*,jvd=([^,]+),dc=madservers,dc=fr"
    attr=userPassword
    by self write
    by
group/jammPostmaster/roleOccupant.expand="cn=postmaster,jvd=$1,dc=madservers,dc=fr" write
    by anonymous auth
    by * none
access to dn.regex=".*jvd=([^,]+),dc=madservers,dc=fr"
    by self write
    by
group/jammPostmaster/roleOccupant.expand="cn=postmaster,jvd=$1,dc=madservers,dc=fr" write
    by * read
access to *
    by * read
replica host=ldap-esclave:389
    bindmethod=simple
    binddn="cn=admin,dc=madservers,dc=fr"
    credentials=ertyui
repllogfile /var/log/ldap/repllog
```

Désormais, il faut ajouter le schéma de JAMM dans OpenLDAP.

/etc/ldap/schema/jamm.schema

```
attributetype ( 1.3.6.1.4.1.12461.1.1.1 NAME 'postfixTransport'
  DESC 'A string directing postfix which transport to use'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{20} SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.2 NAME 'accountActive'
  DESC 'A boolean telling whether an account is active or not'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.3 NAME 'lastChange'
  DESC 'Time in unix time of last change in entry'
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.4 NAME 'jvd'
  DESC 'A virtual domain managed by Jamm'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# The following attributes are borrowed from Courier's schema so that
# the Jamm Schema can live on its own.

attributetype ( 1.3.6.1.4.1.12461.1.1.5 NAME 'mailbox'
  DESC 'The absolute path to the mailbox for a mail account in a non-
  default location'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.6 NAME 'quota'
  DESC 'A string that represents the quota on a mailbox'
  EQUALITY caseExactIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.7 NAME 'clearPassword'
  DESC 'A separate text that stores the mail account password in clear
  text'
  EQUALITY octetStringMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{128})

attributetype ( 1.3.6.1.4.1.12461.1.1.8 NAME 'maildrop'
  DESC 'RFC822 Mailbox - mail alias'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} )

attributetype ( 1.3.6.1.4.1.12461.1.1.9 NAME 'mailsource'
  DESC 'Message source'
  EQUALITY caseIgnoreIA5Match
  SUBSTR caseIgnoreIA5SubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )

# Back to more of Jamm specific attributes

attributetype ( 1.3.6.1.4.1.12461.1.1.10 NAME 'editAliases'
  DESC 'A boolean telling whether a domain manager can edit Aliases'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )
```

```

attributetype ( 1.3.6.1.4.1.12461.1.1.11 NAME 'editAccounts'
  DESC 'A boolean telling whether a domain manager can edit Accounts'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.12 NAME 'editPostmasters'
  DESC 'A boolean telling whether a domain manager can edit
Postmasters'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.13 NAME 'editCatchAlls'
  DESC 'A boolean telling whether a domain manager can edit CatchAlls'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

attributetype ( 1.3.6.1.4.1.12461.1.1.14 NAME 'delete'
  DESC 'A boolean telling whether this item is marked for deletion'
  EQUALITY booleanMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE )

#
# Objects: 1.3.6.1.4.1.12461.1.2
#

objectclass ( 1.3.6.1.4.1.12461.1.2.1 NAME 'JammMailAccount'
  SUP top STRUCTURAL
  DESC 'Mail account objects'
  MUST ( mail $ homeDirectory $ mailbox $ accountActive $ lastChange $
  delete )
  MAY ( uidNumber $ gidNumber $ uid $ cn $ description $ quota $
  userPassword $ clearPassword ) )

objectclass ( 1.3.6.1.4.1.12461.1.2.2 NAME 'JammMailAlias'
  SUP top STRUCTURAL
  DESC 'Mail aliasing/forwarding entry'
  MUST ( mail $ maildrop $ accountActive $ lastChange )
  MAY ( mailsource $ cn $ description $ userPassword ) )

objectclass ( 1.3.6.1.4.1.12461.1.2.3 NAME 'JammVirtualDomain'
  SUP top STRUCTURAL
  DESC 'Virtual Domain entry to be used with postfix transport maps'
  MUST ( jvd $ accountActive $ lastChange $ delete $ editAccounts $
  editPostmasters )
  MAY ( postfixTransport $ description ) )

objectClass ( 1.3.6.1.4.1.12461.1.2.4 NAME 'JammPostmaster'
  SUP top AUXILIARY
  DESC 'Added to a JammMailAlias to create a postmaster entry'
  MUST roleOccupant )

```

Vots annuaires sont prêts à l'utilisation, il ne reste plus qu'à les redémarrer.

```

#/etc/init.d/slapd restart

```

INSTALLATION ET CONFIGURATION DU GESTIONNAIRE LDAP – JAMM

Jamm est un outil développé en opensource tournant sur un serveur TomCat et donc développé en JAVA. Voici la procédure d'installation de celui-ci sur le serveur ldap central :

Nous téléchargeons le JDK (www.java.com) avec la commande wget et le décompressons dans le répertoire adéquat.

```
#wget url
#mkdir /usr/lib/java
#tar zxvf jdk.tar.gz -C /usr/lib/java
```

Il nous faut maintenant télécharger TomCat (<http://tomcat.apache.org>) pour faire fonctionner Jamm.

```
#wget url
#tar zxvf tomcat.tar.gz -C /opt
```

Vous obtiendrez le répertoire tomcat-version dans /opt. Dans notre cas, nous utilisons la version 4.1 donc nous obtenons le répertoire /opt/tomcat-4.1. On crée les sous répertoires adéquats :

```
#mkdir /opt/tomcat-4.1/webapps/jamm
```

Nous téléchargeons Jamm (<http://jamm.sourceforge.net>) :

```
#wget url
#unzip jamm.zip
#mv jamm/* /opt/tomcat-4.1/webapps/jamm
#cp /opt/tomcat-4.1/webapps/jamm/WEB-INF/jamm.properties.dist \
/opt/tomcat-4.1/webapps/jamm/WEB-INF/jamm.properties
```

Voici le fichier de configuration tel qu'il devrait être.

/opt/tomcat-4.1/webapps/jamm/WEB-INF/jamm.properties

```
jamm.ldap.host = localhost
jamm.ldap.search_base = dc=madservers,dc=fr
jamm.ldap.root_dn = cn=admin,dc=madservers,dc=fr
jamm.password.exop = true
```

On crée les fichiers pour le démarrage automatique

/etc/init.d/tomcat

```
export JAVA_HOME=/usr/lib/java

case "$1" in
  start)
    /opt/tomcat-4.1/bin/startup.sh
    ;;

  reload)
    echo "Reload is not implemented!" >&2
    exit 3
    ;;

  restart|force-reload)
    $0 stop
    sleep 1
    $0 start
    ;;

  stop)
    /opt/tomcat-4.1/bin/shutdown.sh
    ;;

  *)
    echo "Usage: /etc/init.d/tomcat4 {start|stop|restart|force-
reload|status}" >&2
    exit 2
    ;;
esac

exit 0
```

On ajoute ceci au démarrage puis on démarre le serveur

```
#update-rc.d -f tomcat start 20 2 . stop 90 S .
#/etc/init.d/tomcat start
```

Jamm est désormais disponible sur l'adresse <http://IP SERVEUR MAITRE/jamm/>

L'identifiant est : root

Le mot de passe est : mot de passe root