

- [Accueil](#)
- [Edito...](#)



## Installation d'un serveur mail brique par brique... (OpenLDAP, Postfix, Cyrus-imap, TLS, SASL, Spamassassin, Amavis, etc...)

Posté par [Jopa](#)  
3 février, 2009



### **POSTFIX**

*Postfix, Cyrus, OpenLdap, Spamassassin, Amavis, etc...* sont des logiciels qui ont largement fait leurs preuves et qui, assemblés, constituent un serveur de mails robuste et performant. Je me suis amusé, le week-end dernier, à assembler et configurer tous ces composants sur une distribution *Debian Etch* pour construire un tel serveur, en ajoutant en prime un poil de sécurité grâce à SASL et TLS. La tâche est loin d'être insurmontable, à condition de prendre les choses méthodiquement et calmement. Dans le bon ordre, les briques s'assemblent à merveille et c'est un vrai bonheur à construire.

Nous allons voir, dans cet article, la mise en place d'une telle solution. Comme pour les précédents articles dédiés à [Zimbra](#) et [OBM](#), nous allons réutiliser ma machine « labo » fraîchement réinstallée avec une Debian Etch, tout ce qu'il y a de plus classique.

[Note du 28 Juillet 2009 : Mise à jour de l'article pour Debian Lenny.](#)

## **1ère brique : Le serveur LDAP**

Nous allons commencer par installer et configurer un petit annuaire LDAP de test. Il est bien entendu tout à fait possible de se baser sur un annuaire existant. Nous n'employerons par la suite que 3 champs de la classe *InetOrgPerson* pour authentifier les utilisateurs et orienter la distribution du courrier. A savoir : uid, userPassword et mail. Il est également possible d'utiliser d'autres champs en adaptant la configuration.

Allez ! C'est parti !

*# aptitude install slapd ldap-utils*

Le fichier de configuration de openLDAP est */etc/ldap/slapd.conf*. Après l'installation, il devrait avoir la tête suivante :

# /etc/ldap/slapd.conf

[View Code](#) INI

```
# Allow LDAPv2 binds
allow bind_v2

# Schema and objectClass definitions
include      /etc/ldap/schema/core.schema
include      /etc/ldap/schema/cosine.schema
include      /etc/ldap/schema/nis.schema
include      /etc/ldap/schema/inetorgperson.schema

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile      /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
argsfile     /var/run/slapd/slapd.args

# Read slapd.conf(5) for possible values
loglevel     0

# Where the dynamically loaded modules are stored
modulepath   /usr/lib/ldap
moduleload    back_bdb

# The maximum number of entries that is returned for a search operation
sizelimit    500

# The tool-threads parameter sets the actual amount of cpu's that is used
# for indexing.
tool-threads 1

#####
# Specific Backend Directives for bdb:
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
backend       bdb
checkpoint    512 30

#####
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this database until another
# 'database' directive occurs
database      bdb

# The base of your directory in database #1
suffix        "dc=linet,dc=jopa,dc=fr"

# Where the database file are physically stored for database #1
directory     "/var/lib/ldap"

# For the Debian package we use 2MB as default but be sure to update this
# value if you have plenty of RAM
dbconfig set_cachesize 0 2097152 0

# Number of objects that can be locked at the same time.
dbconfig set_lk_max_objects 1500
# Number of locks (both requested and granted)
dbconfig set_lk_max_locks 1500
# Number of lockers
dbconfig set_lk_max_lockers 1500

# Indexing options for database #1
index         objectClass eq
```

```

# Save the time that the entry gets modified, for database #1
lastmod          on

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
# These access lines apply to database #1 only
access to attrs=userPassword,shadowLastChange
    by dn="cn=admin,dc=linet,dc=jopa,dc=fr" write
    by anonymous auth
    by self write
    by * none

# Ensure read access to the base for things like
# supportedSASLMechanisms. Without this you may
# have problems with SASL not knowing what
# mechanisms are available and the like.
# Note that this is covered by the 'access to *'
# ACL below too but if you change that as people
# are wont to do you'll still need this if you
# want SASL (and possible other things) to work
# happily.
access to dn.base="" by * read

# The admin dn has full write access, everyone else
# can read everything.
access to *
    by dn="cn=admin,dc=linet,dc=jopa,dc=fr" write
    by * none
#     by * read

```

Il est plus « sécurisé » de supprimer l'autorisation de lecture pour les utilisateurs non authentifiés en remplaçant « by \* read » par « by \* none » dans la dernière ACL.

Pour la partie cliente du serveur ldap (utile pour *ldapsearch* par exemple), c'est le fichier */etc/ldap/ldap.conf*.

## **/etc/ldap/ldap.conf**

[View Code](#) INI

```

# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01 kurt Exp $
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE    dc=linet, dc=jopa, dc=fr
URI      ldap://localhost
#SIZELIMIT    12
#TIMELIMIT    15
#DEREF        never

```

Le serveur LDAP étant opérationnel, nous ajoutons quelques utilisateurs à l'annuaire. Créons un petit fichier LDIF contenant 4 utilisateurs. L'utilisateur Cyrus servira plus tard pour administrer les boîtes Imap.

## **Utilisateurs.Ldif**

[View Code](#) LDIF

```
dn: uid=cyrus,dc=linet,dc=jopa,dc=fr
uid: cyrus
cn: Administrateur Cyrus
sn: Cyrus
userPassword: MonMotDePasseSecret
objectClass: inetOrgPerson
```

```
dn: uid=joel,dc=linet,dc=jopa,dc=fr
uid: joel
cn: Joël PASTRE
sn: PASTRE
mail:joel@linet.jopa.fr
userPassword: LeMotDePasseDeJoel
objectClass: inetOrgPerson
```

```
dn: uid=jean,dc=linet,dc=jopa,dc=fr
uid: jean
cn: Jean DUPONT
sn: DUPONT
mail:jean@linet.jopa.fr
userPassword: LeMotDePasseDeJean
objectClass: inetOrgPerson
```

```
dn: uid=jojo,dc=linet,dc=jopa,dc=fr
uid: jojo
cn: jojo LAAAPIN
sn: LAAAPIN
mail:jojo@linet.jopa.fr
userPassword: laaaaaaaapin
objectClass: inetOrgPerson
```

On ajoute tout ça à l'annuaire :

```
# ldapadd -x -f utilisateurs.ldif -D « cn=admin,dc=linet,dc=jopa,dc=fr » -w MotDePasseAdminLDAP
adding new entry « uid=cyrus,dc=linet,dc=jopa,dc=fr »
adding new entry « uid=joel,dc=linet,dc=jopa,dc=fr »
adding new entry « uid=jean,dc=linet,dc=jopa,dc=fr »
adding new entry « uid=jojo,dc=linet,dc=jopa,dc=fr »
```

Voilà pour l'annuaire... penchons nous maintenant sur l'authentification...

## 2ème brique : SASL

```
# aptitude install sasl2-bin
```

Le fichier : */etc/saslauthd.conf* (à créer de toute pièce) va permettre à *saslauthd* d'utiliser l'annuaire *ldap* comme base d'utilisateurs et de mots de passe.

***/etc/saslauthd.conf***

[View Code](#) INI

```
# SERVEUR LDAP
LDAP_SERVERS: ldap://localhost

# DOMAINE
LDAP_DEFAULT_DOMAIN: linet.jopa.fr
```

```

LDAP_TIMEOUT: 10
LDAP_TIME_LIMIT: 10
LDAP_CACHE_TTL: 30
LDAP_CACHE_MEM: 32768

# VERSION LDAP
LDAP_VERSION: 3

# SASL Pour l'accès au serveur
LDAP_USE_SASL: no

# Méthode d'authentification (bind / custom / fastbind)
LDAP_AUTH_METHOD: bind

# Utilisateur utilisé pour la connexion - Si vide = Anonyme
LDAP_BIND_DN: cn=admin,dc=linet,dc=jopa,dc=fr
# Et le mot de passe
LDAP_BIND_PW: MotDePasseAdminLDAP

# Base de départ de la recherche
LDAP_SEARCH_BASE: dc=linet,dc=jopa,dc=fr
# Et profondeur (sub / one / base )
LDAP_SCOPE: sub

# Filtre de recherche : uid dans notre cas
LDAP_FILTER: uid=%u
# Et nom du champ contenant le mot de passe
LDAP_PASSWORD_ATTR: userPassword

```

**Attention : Ce fichier est créé par défaut en lecture pour tout le monde sous Debian. Il est impératif de changer ses droit pour n'autoriser la lecture qu'à l'utilisateur root.**

```
# chmod 600 /etc/saslauthd.conf
```

L'activation de l'authentification *sasl* et l'utilisation de ce fichier se font par modification de */etc/default/saslauthd*.

Il faut bien penser à activer le démon (*START=yes*) et spécifier la méthode d'authentification utilisée par *saslauthd* (ldap dans mon cas).

## **/etc/default/saslauthd**

[View Code](#) INI

```

#
# Settings for saslauthd daemon
#
# Should saslauthd run automatically on startup? (default: no)
## ICI : démarrage automatique du démon
START=yes

# Which authentication mechanisms should saslauthd use? (default: pam)
#
# Available options in this Debian package:
# getpwent -- use the getpwent() library function
# kerberos5 -- use Kerberos 5
# pam      -- use PAM
# rimap    -- use a remote IMAP server
# shadow   -- use the local shadow password file

```

```
# saslauthd -- use the local saslauthd database file
# ldap -- use LDAP (configuration is in /etc/saslauthd.conf)
#
# Only one option may be used at a time. See the saslauthd man page
# for more information.
#
# Example: MECHANISMS="pam"
# ICI : Méthode d'authentification et Paramètre : Fichier saslauthd.conf
MECHANISMS="ldap"
PARAMS="-O /etc/saslauthd.conf"

# Additional options for this mechanism. (default: none)
# See the saslauthd man page for information about mech-specific options.
MECH_OPTIONS=""

# How many saslauthd processes should we run? (default: 5)
# A value of 0 will fork a new process for each connection.
THREADS=5
# Other options (default: -c)
# See the saslauthd man page for information about these options.
#
# Example for postfix users: "-c -m /var/spool/postfix/var/run/saslauthd"
# Note: See /usr/share/doc/sasl2-bin/README.Debian

# Nécessaire pour le chroot de Postfix (par défaut sous Debian)
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

Démarrage du démon saslauthd:

```
# /etc/init.d/saslauthd start
```

Et test :

```
# testsaslauthd -u jean -p LeMotDePasseDeJean
0: OK « Success. »
```

```
# testsaslauthd -u jojo -p laaaaaaapin
0: OK « Success. »
```

Bon ! Une de plus !!!

## 3ème brique : Cyrus

Nous voilà capable d'authentifier nos utilisateurs, nous allons pouvoir leur créer des boîtes imap (et pop accessoirement). Installons donc *cyrus-imap*, ses outils d'administrations, sa doc et tous les paquets nécessaires à l'authentications sasl.

```
# aptitude install cyrus-admin-2.2 cyrus-clients-2.2 cyrus-imapd-2.2 cyrus-pop3d-2.2 cyrus-sasl2-doc
cyrus-doc-2.2
# aptitude install libauthen-sasl-cyrus-perl libcyrus-imap-perl22 libsasl2-2 libauthen-sasl-perl libsasl2-
modules
```

Le fichier de configuration principal est */etc/imapd.conf*. Il y a juste quelques bricoles à changer :

### */etc/imapd.conf*

- **admins:** **cyrus** ( à décommenter : Nom de l'administrateur du serveur imapd... Si si ! C'est bien

l'utilisateur cyrus que nous avons inséré dans l'annuaire),

- `sasl_pwcheck_method: saslauthd` (à modifier pour préciser la méthode de gestion des mots de passe),
- `sasl_mech_list: PLAIN` (à décommenter).

```
# /etc/init.d/cyrus2.2 restart
```

Si tout est bon, la commande : `cyradm -user cyrus localhost` devrait permettre la connexion au shell d'administration imap et la création des boîtes. Afin de garantir un nommage unique et cohérent, nous utiliserons tout simplement comme nom, l'*uid* de leur propriétaire.

```
# cyradm -user cyrus localhost
```

Password:

```
localhost> cm user.joel
```

```
localhost> cm user.jean
```

```
localhost> cm user.jojo
```

```
localhost> lm
```

```
user.jean (HasNoChildren) user.jojo (HasNoChildren)
```

```
user.joel (HasNoChildren)
```

```
localhost> quit
```

Ca....C'est fait.. Il est dès à présent possible de se connecter au serveur Imap avec un client de messagerie. Bon d'accord, l'intérêt est très limité vu qu'aucun agent de distribution n'est configuré; si ce n'est pour valider le travail réalisé jusque là...

Paramètres du serveur

Type de serveur : Serveur de courrier IMAP

Nom du serveur : labo.linnet.jopa.fr
Port : 143
Défaut : 143

Nom d'utilisateur : joel

Paramètres de sécurité

Utiliser une connexion sécurisée :

☒ Jamais
☐ TLS, si possible
☐ TLS
☐ SSL

☐ Utiliser une authentification sécurisée

Paramètres du serveur

☐ Vérifier le courrier au lancement
☒ Vérifier les nouveaux messages toutes les 10 minutes.

Lors de l'effacement d'un message : le mettre dans le dossier Corbeille

☐ Nettoyer le dossier « Courrier entrant » en quittant Thunderbird.
☐ Vider la corbeille lors de la sortie.

Avancés...

Répertoire local :

/home/joel/.mozilla-thunderbird/oe2ts1vd.default/ImapMail/labo.lin

Parcourir...

Annuler

OK

Il manque encore une brique à notre projet de maçonnerie afin de pouvoir envoyer et recevoir des mails : C'est *Postfix* bien entendu...

## 4ème brique : Postfix

*Postfix* va identifier les destinataires de mails reçus en interrogeant directement l'annuaire *LDAP*.

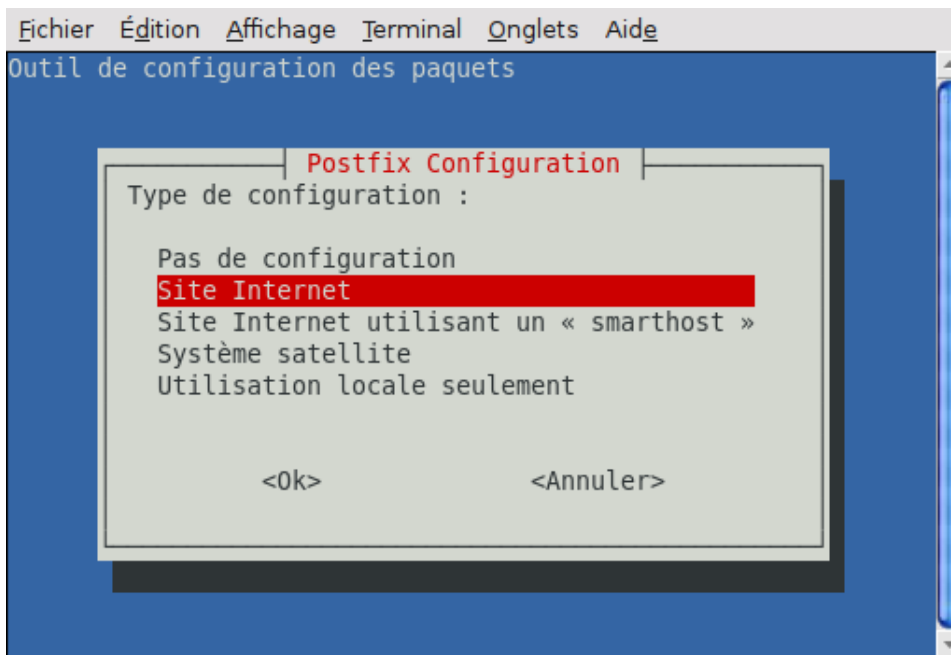
Comme nous voulons que nos utilisateurs nomades puissent envoyer des mails via ce serveur, même s'ils sont à l'extérieur de mon réseau privé, nous les authentifierons sur le serveur smtp grâce à *saslauthd* ... une fois de plus.

**# aptitude install postfix postfix-tls postfix-ldap**

Sur une install Debian toute neuve, aptitude détecte un conflit avec Exim4 et propose de le désinstaller. C'est bien ce qu'il faut faire !

L'installateur demande le type de serveur et le domaine de courrier. Choisissons une configuration de type « Site Internet » et dans ce cas précis, nous travaillons sur le domaine « linet.jopa.fr ». Les réponses à ces questions n'ont pas ici, une grande importance : Nous reprendrons manuellement la configuration plus loin.





Pour que la distribution locale du courrier soit assurée par *Cyrus-Imap*, nous devons déclarer *Cyrus* comme agent de distribution. Ceci se fait par l'intermédiaire du fichier `/etc/postfix/master.cf` en ajoutant une ligne en fin de fichier :

## `/etc/postfix/master.cf`

```
cyrus unix      -      n      n      -      -      pipe flags=R user=cyrus argv=/usr/sbin/cyrdeliver -e -m
${extension} ${user}
```

Le suite se passe dans le fichier principal de configuration de postfix : `/etc/postfix/main.cf`

## `/etc/postfix/main.cf`

[View Code](#) INI

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version

# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.

myorigin = /etc/mailname

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

# PARAMETRES TLS : Configuré automatiquement par postfix-tls
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${queue_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${queue_directory}/smtp_scache
```

```

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

myhostname = labo.linnet.jopa.fr

# PARAMETRES LDAP
mailbox_maps = ldap:/etc/postfix/ldap-accounts.cf
alias_maps = ldap:/etc/postfix/ldap-aliases.cf

mydestination = linet.jopa.fr, labo.linnet.jopa.fr, localhost.linnet.jopa.fr, localhost
relayhost =

# On notera que seul localhost est identifié. Les autres clients devront s'authentifier
mynetworks = 127.0.0.0/8

# Agent de transport local : CYRUS
local_transport = cyrus

recipient_delimiter = +

# Restrictions
smtpd_recipient_restrictions = reject_unauth_pipelining,
                                reject_non_fqdn_recipient,
                                reject_unauth_destination,
                                permit_mynetworks,
                                permit_sasl_authenticated

smtpd_sender_restrictions = reject_non_fqdn_sender,
                             reject_unknown_sender_domain,
                             reject_unauth_pipelining,
                             permit_sasl_authenticated,
                             permit_mynetworks

# AUTHENTIFICATION SASL
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain =

inet_interfaces = all

```

Il faut particulièrement être attentif au points suivants de la configuration :

- *mailbox\_maps = ldap:/etc/postfix/ldap-accounts.cf* et *alias\_maps = ldap:/etc/postfix/ldap-aliases.cf* pour la validation des destinataires par recherche dans le ldap,
- *mynetworks = 127.0.0.0/8* pour n'autoriser que Localhost à envoyer ou recevoir des mails (permit\_mynetworks), les autres seront authentifiés via *saslauthd*,
- *local\_transport = cyrus* pour déclarer Cyrus comme agent de transport local,
- et enfin, *smtpd\_sasl\_auth\_enable = yes* pour activer l'authentification sasl.

Pour l'accès au LDAP, nous faisons référence à deux fichiers : */etc/postfix/ldap-accounts.cf* et */etc/postfix/ldap-aliases.cf*

## ***/etc/postfix/ldap-accounts.cf***

[View Code](#) INI

```

server_host = localhost
server_port = 389
search_base = dc=linet, dc=jopa, dc=fr
query_filter = (&(objectClass=InetOrgPerson)(mail=%s))
result_attribute = uid

```

```
bind = yes
bind_dn = cn=admin,dc=linet,dc=jopa,dc=fr
bind_pw = MotDePasseAdminLDAP
version = 3
```

## ***/etc/postfix/ldap-aliases.cf***

[View Code](#) INI

```
server_host = localhost
server_port = 389
search_base = dc=linet, dc=jopa, dc=fr
query_filter = (&(objectClass=InetOrgPerson)(mail=%s))
result_attribute = mail
bind = yes
bind_dn = cn=admin,dc=linet,dc=jopa,dc=fr
bind_pw = MotDePasseAdminLDAP
version = 3
```

N'oublions pas de gérer les droits de ces 2 fichiers :

```
# chown root:sasl ldap*.cf
# chmod 640 ldap*.cf
```

*L'attribut en retour ici est mail (result\_attribute = mail) , mais il peut être très judicieux d'ajouter à l'annuaire LDAP un champ « maildrop » qui sera retourné ici. Ce champ donnera alors une vraie fonctionnalité d'alias, permettant de transférer tout mail à destination de l'utilisateur vers une ou plusieurs autres adresses email.*

*De plus, il faut noter que dans la configuration actuelle et sans cette notion d'alias, une boîte cyrus doit être associée à chaque adresse email locale. En effet, Cyrus recherche une boîte dont le nom correspond au préfixe de l'adresse email du destinataire (ce qui est avant le @ en bref).*

L'authentification SASL a besoin d'un fichier : `/etc/postfix/sasl/smtpd.conf` . Attention, sous d'autres distributions, le fichier peut être cherché ailleurs, généralement dans `/usr/lib/sasl2/` ou `/usr/local/lib/sasl2/`. Elle a également besoin que l'utilisateur « postfix » appartienne au groupe SASL.

```
# adduser postfix sasl
# id postfix
uid=106(postfix) gid=106(postfix) groupes=106(postfix),45(sasl)
# vi /etc/postfix/sasl/smtpd.conf
```

## ***/etc/postfix/sasl/smtpd.conf***

[View Code](#) INI

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

Note : Debian fait tourner Postfix dans un chroot. En cas de problème d'accès au socket SASL, il faut bien vérifier la ligne `OPTIONS` du fichier `/etc/default/saslauthd`.

## ***/etc/default/saslauthd***

[View Code](#) INI

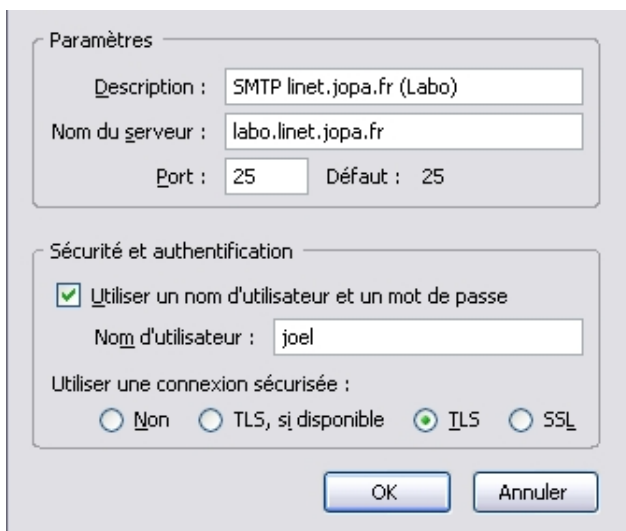
```
#
# Settings for saslauthd daemon
..
# Nécessaire pour le chroot de Postfix (par défaut sous Debian)
OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd"
```

## */etc/postfix/master.cf*

[View Code](#) INI

```
service type private unpriv chroot wakeup maxproc command + args
#
# (yes) (yes) (yes) (never) (100)
# =====
smtp inet n - - - - smtpd
...
```

Allez... Là, ça prend carrément forme. Testons sans plus attendre en configurant un serveur *smtp* sur notre client de messagerie préféré :



On peut remarquer que, après acceptation des certificats, la connexion sécurisée TLS fonctionne parfaitement. C'est bien sûr dû à l'installation de *postfix-tls* qui a généré les certificats et préconfiguré *Postfix*. Cette fonctionnalité n'apporte malheureusement pas grand chose tant que la connexion *Imap* n'est pas elle aussi sécurisée, tout particulièrement dans notre cas où les noms d'utilisateurs et mots de passes sont identiques pour les deux services.

## Petit retour arrière : Cyrus-Imap (TLS)

Afin d'activer le support TLS pour Cyrus-Imap, il suffit d'éditer le fichier */etc/imapd.conf* et de décommenter les deux lignes suivantes (le certificat utilisé est le même que pour postfix). L'utilisateur *cyrus* doit appartenir au groupe *ssl-cert* pour pouvoir lire la clef privée.

```
# adduser cyrus ssl-cert
```

## /etc/imapd.conf

tls\_cert\_file: /etc/ssl/certs/ssl-cert-snakeoil.pem

tls\_key\_file: /etc/ssl/private/ssl-cert-snakeoil.key

Paramètres du serveur

Type de serveur : Serveur de courrier IMAP

Nom du serveur : labo.linet.jopa.fr Port : 143 Défaut : 143

Nom d'utilisateur : joel

Paramètres de sécurité

Utiliser une connexion sécurisée :

☐ Jamais ☐ TLS, si possible ☒ TLS ☐ SSL

☐ Utiliser une authentification sécurisée

Il est temps maintenant de prémunir notre système contre les spams et les virus.

## 5ème brique : Anti-spams – GreyListing

Le **greylisting** (le mot anglais signifie : « inscription sur liste grise ») est une technique [antipourriel](#) très simple qui consiste à rejeter temporairement un message, par émission d'un code de refus temporaire au serveur émetteur ([MTA](#)). Dans la majorité des cas, les serveurs émetteurs réexpédient le courriel après quelques minutes. La plupart des serveurs émettant des [pourriels](#) ne prendraient pas cette peine.

( <http://fr.wikipedia.org/wiki/Greylisting> )

L'installation est basique, et il n'y a pas grand chose à ajouter au paramétrage par défaut.

# aptitude install postgrey

La mise en service se fait par l'ajout de la règle « *check\_policy\_service inet:[127.0.0.1]:60000* » à « *smtpd\_recipient\_restrictions* » dans le fichier */etc/postfix/main.cf*

### /etc/postfix/main.cf

[View Code](#) INI

```
smtpd_recipient_restrictions = reject_unauth_pipelining,  
permit_mynetworks,  
permit_sasl_authenticated,  
reject_non_fqdn_recipient,  
reject_unauth_destination,  
check_policy_service inet:[127.0.0.1]:60000
```

## 6ème brique : Anti-spams / Antivirus – Amavis / SpamAssassin / Clamav

C'est *Amavis* qui va être chargé du filtrage de contenus, en s'appuyant sur *Spamassassin* contre les spams et *Clamav* contre les virus. Clamav dispose d'un outil permettant la mise à jour des signatures virales : *freshclam*. Pour avoir des mises à jour plus régulière, il suffit d'ajouter un dépôt *debian-volatile* à la liste des dépôts. Par exemple :

```
# echo « deb http://ftp2.de.debian.org/debian-volatile lenny/volatile main contrib » > /etc/apt
/sources.list.d/volatile.list
# aptitude update
```

Passons à l'installation :

```
# aptitude install amavis-new clamav clamav-freshclam clamav-daemon spamassassin
```

L'activation du démon *spamassassin* se fait par l'intermédiaire du fichier « */etc/default/spamassassin* » en plaçant l'option *ENABLED* à 1

## **/etc/default/spamassassin**

[View Code](#) INI

```
# /etc/default/spamassassin
# Duncan Findlay

# WARNING: please read README.spamd before using.
# There may be security risks.

# Change to one to enable spamd
ENABLED=1

# Options
# See man spamd for possible options. The -d option is automatically added.

# SpamAssassin uses a preforking model, so be careful! You need to
# make sure --max-children is not set to anything higher than 5,
# unless you know what you're doing.

OPTIONS="--create-prefs --max-children 5 --helper-home-dir"

# Pid file
# Where should spamd write its PID to file? If you use the -u or
# --username option above, this needs to be writable by that user.
# Otherwise, the init script will not be able to shut spamd down.
PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"
```

Il faut ensuite demander à postfix d'utiliser Amavis pour le filtrage de contenus. Revenons une fois de plus dans notre fichier « */etc/postfix/main.cf* » pour ajouter la directive *:content\_filter = smtp-amavis:[127.0.0.1]:10024*

## **/etc/postfix/main.cf**

[View Code](#) INI

```
content_filter = smtp-amavis:[127.0.0.1]:10024

smtpd_recipient_restrictions = reject_unauth_pipelining,
```

```

permit_mynetworks,
permit_sasl_authenticated,
reject_non_fqdn_recipient,
reject_unauth_destination,
check_policy_service inet:[127.0.0.1]:60000

smtpd_sender_restrictions = permit_sasl_authenticated,
permit_mynetworks,
reject_non_fqdn_sender,
reject_unknown_sender_domain,
reject_unauth_pipelining

```

Afin de pouvoir utiliser l'agent de transport smtp-amavis, nous devons le définir dans le fichier « master.cf » de postfix :

## /etc/postfix/master.cf

[View Code](#) INI

```

...
#CLAMAV-AMAVIS
smtp-amavis unix - - n - 2 smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
127.0.0.1:10025 inet n - 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 smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
...

```

Pour finir avec *amavis*, un brin de configuration est nécessaire pour activer le filtrage anti-spam et anti-virus.

## /etc/amavis/conf.d/15-content\_filter\_mode

[View Code](#) PERL

```

use strict;

# You can modify this file to re-enable SPAM checking through spamassassin
# and to re-enable antivirus checking.

#
# Default antivirus checking mode
# Uncomment the two lines below to enable it back
#

@bypass_virus_checks_maps = (
    %bypass_virus_checks, @bypass_virus_checks_acl, $bypass_virus_checks_re);

```

```
#
# Default SPAM checking mode
# Uncomment the two lines below to enable it back
#

@bypass_spam_checks_maps = (
    %bypass_spam_checks, @bypass_spam_checks_acl, $bypass_spam_checks_re);

1; # insure a defined return
```

Il nous faudra, si cela n'est pas fait à l'installation, ajouter l'utilisateur *clamav* au groupe *amavis*.

```
# adduser clamav amavis
```

## 7ème brique : Anti-spams (encore) – Listes RBL

Enfin, nous pouvons utiliser des blacklistes externes pour parfaire notre filtrage anti-spam. Il en existe un paquet, mais leur utilisation est similaire. Dans l'exemple, utilisons deux « blacklist » publiques en fin de filtrage : *dul.dnsbl.sorbs.net* et *zen.spamhaus.org*. Il faut encore une fois ajouter deux règles « *smtpd\_recipient\_restrictions* » au fichier */etc/postfix/main.cf*

*/etc/postfix/main.cf*

[View Code](#) INI

```
smtpd_recipient_restrictions = reject_unauth_pipelining,
permit_mynetworks,
permit_sasl_authenticated,
reject_non_fqdn_recipient,
reject_unauth_destination,
check_policy_service inet:[127.0.0.1]:60000,
reject_rbl_client dul.dnsbl.sorbs.net,
reject_rbl_client zen.spamhaus.org
```

Voilà pour cet article. Même s'il reste pas mal d'améliorations possibles, d'optimisations et fonctionnalités supplémentaires à ajouter, on va dire que c'est un bon début.

## Sources :

- <http://flurdy.com/docs/postfix/#config-secure-auth>
- <http://www.luxpopuli.fr/Internet/Postfix-Cyrus-IMAP-SSL-LDAP/Cyrus-IMAP-authentication-LDAP>
- <http://www.bizeul.net/>

- [Publiez-le sur Facebook](#)

8

[Configurations](#), [Divers](#), [Evènements](#), [Planet-Libre](#)

Laissez votre message après le bip...[Biiiiip](#)

Commentaires



Commentaire par **macsim** le 4 février 2009 @ [11:50](#)

Bravo pour ce bel article 😊

Commentaire par **theClimber** le 4 février 2009 @ [23:22](#)

Si tu veux compléter ton tuto avec la gestion de la DB, voici un article que j'ai écrit récemment basé sur postgresql. Je ne l'ai pas publié sur le Planet-Libre car je l'ai écrit en anglais, mais ça ne t'empêche pas de t'en inspirer 😊  
<http://theclimber.fritalk.com/.....ostgresql>

Commentaire par **Philippe** le 7 février 2009 @ [20:32](#)

Beau tuto ! Je vais réinstaller ma messagerie perso sur mon petit serveur. J'ai juste 512Mo de mémoire et j'utilise une debian 4. Au niveau empreinte mémoire ça donne quoi ?

Commentaire par **Geek87** le 8 février 2009 @ [21:36](#)

Salut,

Voici un bel article bien rédigé !

Une petite remarque cependant : je crois que mailbox\_maps n'est pas une option valide dans main.cf, ce serait plutôt virtual\_mailbox\_maps si je ne me trompe pas.

Bonne soirée.

Commentaire par **Jopa** le 9 février 2009 @ [8:25](#)

Bonjour,

Dans l'ordre : Philippe, 512Mo sont largement suffisants pour un petit serveur mail. Le dimensionnement de la mémoire va surtout dépendre du nombre de boîtes et du trafic que devra absorber le serveur. A titre d'info, j'ai 150 Mo de ram utilisé sur mon serveur de test, une fois tous les services lancés.

Geek87 : Il est préférable d'utiliser « virtual\_mailbox\_maps », quand on veut faire la distinction entre les boîtes des utilisateurs mais uniquement et les comptes unix. Dans mon cas, les comptes unix n'ont pas d'adresse email, donc mailbox\_maps est tout à fait utilisable.

Commentaire par **Geek87** le 9 février 2009 @ [23:04](#)

En fait je demandais ça parce que j'ai pas trouvé ce paramètre sur la page de documentation de Postfix à propos du fichier main.cf où devrait normalement figurer tous les paramètres de Postfix. Mais il me semblait bien que j'avais déjà vu ce paramètre quelque part. Merci de me l'avoir confirmé !

Commentaire par **s3d** le 23 février 2009 @ [12:32](#)

je vous félicite pour ce magnifique tuto ^^  
comme j'apprécie bien votre travail  
maintenant je suis en stage dans une Ecole supérieure ,  
cette école appartient à l'université  
dont le nom de domaine de l'université et de par exemple  
« univ.com »  
ils m'ont demandé de configurer un serveur messagerie  
avec l'annuaire ldap  
et ils veulent que les adresses emails seraient comme  
« exemple @ ecolemail . univ . com »

je travail sur debian 5 Lenny pour configurer mon serveur

mais ya des petits trucs que je cherche à savoir  
le domaine ecolemail.univ.com ça n'existe pas déjà  
est ce qu'il est indispensable l'ajouter au serveur dns  
avant de commencer ou bien nn

j'ai essayer de suivre votre tuto mais à la configuration du ldap je trouve des problème  
et merci d'avance

Commentaire par **Jopa** le 23 février 2009 @ [18:16](#)

Bonjour,

Il est tout à fait possible de commencer sans DNS, mais l'émission / réception de mail ne fonctionnera  
que pour le domaine local : En interne et sans interaction avec l'extérieur, en particulier pour la  
réception.... ( Logique !)

Concernant ton problème de configuration ldap, il va falloir en dire un peu plus... Sans ça, je ne peux pas  
trop t'aider...

Ceci-dit, je ferais bien un saut à Oujda pour te donner un coup de main 😊

Bonne continuation

Commentaire par **s3d** le 24 février 2009 @ [10:51](#)

merci pour votre réponse déjà

pour mon problème avec l'annuaire ldap c'est à la fin du 1er brique  
après avoir installer les package slapd et ldap-utils  
et la configuration des fichier .conf en localhost  
et la création du fichier utilisateurs.ldif  
ça me donne cette erreur

```
»  
s3debian:/home/saad# ldapadd -x -f utilisateurs.ldif -D "cn=admin,dc=localhost" -w  
MotDePasseAdminLDAP  
ldap_bind: Invalid DN syntax (34)  
additional info: invalid DN
```

```
»  
biensur j'ai essayé de saisir mon mot de passe d'admin ldap
```

c alrs ke je suis bloqué ici :s  
j'ai tellement besoin d'un coup de main surtt que je travaille seul sur le projet  
alrs ça me ferai tellement plaiiir ^^)  
je vous merciie d'avance  
S%)

Commentaire par **Jopa** le 24 février 2009 @ [21:34](#)

Bonsoir s3d,

D'après le message d'erreur, je pense qu'il s'agit d'une erreur de syntaxe dans le fichier ldif  
(utilisateurs.ldif). Très probablement sur un ligne « dn ».

Vérifie que tu n'as pas de faute de frappe sur ces lignes là, et qu'elles s'intègrent bien dans l'arborescence de ton annuaire :

Dans mon exemple, les comptes mails sont directement à la racine de dc=linet,dc=jopa,dc=fr. Si tu es dans le même schéma que moi, les entrées devraient être de la forme (d'après le dn que tu passes en paramètre à ldapadd :

dn: uid=xxxxx,dc=localhost

Commentaire par **Jopa** le 24 février 2009 @ [21:58](#)

Suite à une remarque très judicieuse de mon amis Bcc sur les droits du fichiers : /etc/saslauthd.conf, j'ai ajouté quelques précisions dans l'article.

En effet, ce fichier est créé par défaut avec les droits en lecture pour tous les utilisateurs (644). Ce fichier contient le mot de passe admin du ldap, et ça craint !

Il est donc très fortement conseillé de faire un petit coup de « chmod 600 /etc/saslauthd.conf ».

Commentaire par **s3d** le 25 février 2009 @ [1:42](#)

bjr

je tiens tjrs à vous remercier 😊

pour le fichier utilisateurs.ldif j'ai verifié  
le dn est bien

dn: uid=xxxxx,dc=localhost

je pense que le problème est un problème d'identification  
de l'admin et le motdepasadmin

j'ai essayé une interface graphique de l'annuaire précisément  
ApacheDirectoryStudio-linux-x86-1.3.0.v20081020.tar.gz  
installé sur une autre machine  
que je peux accéder en tant que utilisateur anonymous  
et je peux pas accéder avec « admin » et « motdepasadmin »

le temps passe et je suis tjrs bloqué ici :s  
j'ai normalement d'autre tâche à appliquer avec ldap  
malheureusement ça commence mal avc 😞  
je vous remercie d'avance  
S%)

Commentaire par **Jopa** le 25 février 2009 @ [10:39](#)

Bonjour,

Ca ressemble quand même bien à une erreur de ldif, mais je me trompe peut-être...

Par défaut, slapd loggue dans /var/log/syslog... Il sera certainement plus bavard sur l'erreur dans les logs. Tu peux jouer sur le niveau de log dans le fichier « /etc/ldap/slapd.conf » en ajoutant la directive loglevel suivi du niveau de log. Pour les valeurs possibles, un petit coup de « man slapd.conf » devrait t'aider.

Si tu as installé les ldap-utils, la commande « slapcat » te permet de lister l'annuaire. Tu pourras ainsi voir si le compte administrateur est correctement entré,

Tu peux également reconfigurer l'annuaire grâce au paquet debian : dpkg-reconfigure slapd,

Ca réinitialisera ton annuaire et le compte admin.

Bon courage

Commentaire par **dofre** le 4 mars 2009 @ [14:54](#)

J'ai le même problème que s3d. Je ne suis pas un expert de LDAP mais je me demande si cela ne vient pas de Lenny qui doit avoir une configuration par défaut différentes que Etch.

Je vais réessayer!

merci en tout cas pour l'article même si pour le moment...

Commentaire par **dofre** le 4 mars 2009 @ [15:36](#)

Juste pour dire que pour passer la ldapadd j'ai utilisé un outil externe (graphique pour le coup LDAP administrator) et importé le ldif sans pb. Maintenant je commence à la 3ème brique et tout se passe nickel (login sasl).

Commentaire par **s3d** le 12 mars 2009 @ [11:14](#)

bonjour,,

pour utiliser ldapadd tu dois avoir ces deux lignes sur ton fichier de configuration de ldap

```
##
```

```
rootdn « cn=admin,dc=mondomaine,dc=com »
```

```
rootpw monmotdepasse
```

```
##
```

après

```
# ldapadd -x -f utilisateurs.ldif -D "cn=admin,dc=mondomaine,dc=com" -w monmotdepasse
```

j'avais des problèmes après avec la 3ème brique pour le sasl

si t'as réussi à passer à la brique qui suit, prière de nous faire part des problèmes que vous avez trouvés et la solution

j'ai essayé d'autres tutoriels (surtout après les problèmes de notre site jopa.fr 😞)

celui du jamm

<http://jamm.sourceforge.net/howto/html>

c'est en anglais en plus sur redhat :s:s

je me demande si c'est possible de mettre le même tutoriel sur notre adorable jopa.fr 😊 traduit en français et sur une debian lenny et le plus tôt possible 😊

merci d'avance

S%)

Commentaire par **s3d** le 12 mars 2009 @ [12:56](#)

mon problème avec sasl

```
s3debian:/home/saad/Desktop# testsaslauthd -u jean -p LeMotDePasseDeJean
```

```
0: NO « authentication failed »
```

```
s3debian:/home/saad/Desktop# testsaslauthd -u jojo -p laaaaaaaapin
```

```
0: NO « authentication failed »
```

```
s3debian:/home/saad/Desktop# testsaslauthd -u jojo -p laaaaaaapin
0: NO « authentication failed »
```

sachant que le uid a été bien créé sur l'annuaire ldap  
(sur le slapcat)

```
dn: uid=jean,dc=localhost
uid: jean
cn: Jean DUPONT
sn: DUPONT
mail: jean@localhost
userPassword:: TGVNb3REZVBhc3NIRGVKZWFu
objectClass: inetOrgPerson
structuralObjectClass: inetOrgPerson
entryUUID: 57fc5268-a33e-102d-9dc4-4d9b3c5646d9
creatorsName: cn=admin,dc=localhost
createTimestamp: 20090312104318Z
entryCSN: 20090312104318.643306Z#000000#000#000000
modifiersName: cn=admin,dc=localhost
modifyTimestamp: 20090312104318Z
```

```
dn: uid=jojo,dc=localhost
uid: jojo
cn: jojo LAAAPIN
sn: LAAAPIN
mail: jojo@localhost
userPassword:: bGFhYWZhYWZhYWFhcGlu
objectClass: inetOrgPerson
structuralObjectClass: inetOrgPerson
entryUUID: 643eb5a2-a33e-102d-9dc5-4d9b3c5646d9
creatorsName: cn=admin,dc=localhost
createTimestamp: 20090312104339Z
entryCSN: 20090312104339.211039Z#000000#000#000000
modifiersName: cn=admin,dc=localhost
modifyTimestamp: 20090312104339Z
```

quelqu'un peut me trouver où est l'erreur ?? la solution !!

S%)

Commentaire par **Jopa** le 15 mars 2009 @ [20:40](#)

Bonsoir,

s3d : Le problème vient probablement de la conf de saslauthd. Jette un oeil dans les logs pour en savoir un peu plus...

dofre : Il doit effectivement y avoir une petite différence entre Lenny et Etch sur l'initialisation de openldap... Il faudrait que je tente une nouvelle install. Je peux dire que, la mise à jour de mon serveur de tests vers Lenny n'a posé aucun problème. C'est bien au niveau de l'installation qu'il doit y avoir une légère variante.

Commentaire par **Glucose** le 13 avril 2009 @ [0:08](#)

Bonsoir,

Je suis ce super tuto et j'ai remarqué que sur ma lenny au début de la 3em étape, la 2em ligne aptitude s'exécute mais notifie quel ne trouve pas le paquet libsasl2 (pas de version candidate)  
il semblerait que le bon paquets soit le libsasl2-2

Glucose

Commentaire par **dofre** le 24 avril 2009 @ [13:41](#)

Bonjour,

impeccable ça fonctionne très bien sur mon serveur.

Par contre je souhaite vers du forwarding de mail, mettre en oeuvre le principe expliqué dans la partie 4 avec « maildrop ».

Avez-vous un exemple de mise en place car je ne comprends pas comment cela peut fonctionner. Je teste actuellement mais je ne vois pas de solution.  
merci

Commentaire par **El Tonio** le 12 mai 2009 @ [15:42](#)

Bonjour,

Pour l'authentification SASL et la cage de Postfix, tout est indiqué dans /etc/default/saslauthd.

```
# Example for postfix users: « -c -m /var/spool/postfix/var/run/saslauthd »  
OPTIONS= »-c -m /var/spool/postfix/var/run/saslauthd »
```

Cette ligne évite de gérer les liens symboliques et le « chroot ».

El Tonio

Commentaire par **manantsoa** le 15 juin 2009 @ [14:30](#)

Bonjour,

trop fort le tuto, et merci à vous de le faire. J'ai quand même quelque question. Comment fait-on pour connecter via sieve de cyrus-imap?? j'ai essayé main en vin.

Merci de votre réponse

Commentaire par **gaby** le 1 juillet 2009 @ [19:52](#)

Merci, merci, merci !!!

J'avais prévu une semaine pour installer une architecture similaire... Je suis tombé sur ton article et ça m'a pris moins d'une journée ( migration des comptes compris )... Un serveur opérationnel en un temps records, des utilisateurs radieux et un chef impressionné !

Alors chapeau ! Je tiens à t'envoyer un petit cadeau mérité, bien peu de choses à côté de l'aide précieuse que ton blog m'a apporté...

Peux-tu me confirmer ton adresse postale par retour de mail ?

Merci encore, et surtout, continue !!!

Commentaire par **Jopa** le 6 juillet 2009 @ [23:04](#)

Merci Gaby,

J'ai bien reçu le T-shirt, il est superbe ! C'est vraiment sympa !

Ce qui me touche par dessus tout, c'est de savoir que mes articles sont lus et qu'ils peuvent être utiles...

Au plaisir...

Ping par [Installation d'un serveur mail brique par brique...Mise à jour...](#) le 28 juillet 2009 @ [18:14](#)

[...] publié, en début d'année, un billet sur l'installation d'un serveur mail basé sur différentes [...]

Ping par [« Alias » et « forward » sur Postfix + LDAP](#) le 28 juillet 2009 @ [22:12](#)

[...] l'utilisateur Jean y est bien présent. Dans le cas contraire, je vous invite à consulter l'article précédent pour l'installation et la configuration d'un serveur [...]

Ping par [Push Mail pour serveur Imap \(local ou distant\)](#) le 4 août 2009 @ [23:33](#)

[...] continuer la construction pas à pas de notre serveur mail (cf installation d'un serveur mail brique par brique), nous allons offrir à nos utilisateurs de terminaux Windows Mobile le luxe du 'push [...]

Commentaire par **Philippe** le 20 août 2009 @ [23:03](#)

Bonsoir,

Bravo pour ce tutoriel qui est vraiment bien fait et très didactique. Je suis en train de me faire un petit serveur de mail avec tout ça, et j'avoue que cela m'aide bien, même s'il faut quand même bien lire la doc des logiciels utilisés pour être sûr de comprendre ce qui se passe et ne pas faire un « bête » copier/coller. En tout cas, beau boulot.

Juste une petite remarque sur l'étape 6, il faut installer le paquet amavisd-new et non pas le paquet amavis-new

Bonne continuation, avec plei de tutoriel de ce niveau

Philippe

Commentaire par **Reno** le 4 septembre 2009 @ [16:32](#)

Bonjour,

Encore mes félicitations pour ce tuto fort utile, et très clair.

Par contre, si je pouvais bénéficier de vos lumières sur un point, cela me rendrais un fier service. Voilà plus d'une journée que je galère avec sasl...

En effet, à l'exécution de cette commande:

```
# testsaslauthd -u reno -p secret
```

j'obtiens ceci en résultat:

```
connect() : No such file or directory
0: machine:/etc#
```

je sais pas trop ou chercher, je me doute que le problème vient de /etc/default/saslauthd... sauf que je vois pas trop quoi, et je trouve pas de réponse sur le net ni dans mes logs...

Someone help me plz^^

D'avance merci

Commentaire par **skhaen** le 22 septembre 2009 @ [23:24](#)

Merci pour ce super article, mais est ce que ce serait possible d'avoir une version pdf ?

(on a pas toujours internet pour lire de la doc ^^)

merci d'avance 😊

Commentaire par **slap** le 1 octobre 2009 @ [17:36](#)

Pour Reno,

Dans ton fichier /etc/default/saslauthd

changes

OPTIONS= »-c -m /var/spool/postfix/var/run/saslauthd »

par

OPTIONS= »-c -m /var/run/saslauthd » (chemin par défaut)

Commentaire par **Cyril** le 17 novembre 2009 @ [15:55](#)

Bonjour,

Tout d'abord merci pour ce tuto.

Mais j'ai le même problème que Reno, et en faisant la modif que tu cite, le problème persiste :s

Quelqu'un a une idée ??

Merci d'avance

PS : Pour la première brique, il y a du changement dans les nouvelles version de ubuntu => le fichier slapd.conf n'existe plus. Voir <http://ubuntuforums.org/showthread.php?t=1313472> pour trouver une parade.

Commentaire par **francklin** le 19 novembre 2009 @ [16:58](#)

slt, je te remercie pour ce beau tuto.

Cependant j'ai besoin d'aide surtout qu'étant un peu novice la dedans .

combien de serveurs physiques faut il pour concevoir un serveur mail, un serveur dns, un serveur proxy et un serveur web?ou quels sont les différents types(logiciels) qu'on peut monter(installer)sur un même serveur physique?car je suis dans une entreprise d'environ 100 personnes et j'aimerais monter des serveurs surtout mail et web visible de l'extérieur.

Je veux utiliser debian lenny alors si tu as des tutos pour les configurations ça sera merveilleux.



j'attends ton message avec impatience.

Merci

Commentaire par **de BOLLIVIER Charles** le 14 février 2010 @ [11:30](#)

Salut,

Bravos pour ce tuto, j'en suis à la brique 3 et à la configuration de cyrus. J'ai installé tous les modules demandés sans problèmes mais au lancement de cyradm -u cyrus localhost, je n'ai rien qui se lance et dans le fichier /var/log/message j'ai la ligne d'erreur suivante :

```
imapd[7904]: segfault at 00000046 eip b79d22cd esp bf9e7b80 error 4
```

Est-ce que quelqu'un sait à quoi ça correspond ce message d'erreur ?

Merci

Commentaire par **de BOLLIVIER Charles** le 14 février 2010 @ [14:55](#)

Bon j'ai changé de distribution, je suis passé sous une Debian et ça marche. Mes premiers tests étaient sur une Ubuntu 8.04 server

Commentaire par **zarakeye** le 4 mars 2010 @ [21:24](#)

Système: Debian Lenny

Merci infiniment pour ce tuto qui brille par son souci du détail!

Malheureusement ça fait 2 mois que, après avoir essayé des distributions et versions différentes, je n'arrive toujours pas à passer le cap de la première brique. En effet ça bloque à l'intégration des 4 utilisateurs grâce aux fichiers utilisateurs.ldif... la commande « ldapadd -x -f utili.... » m'affiche le résultat de « ldapadd -h ». De toute évidence il me manque quelque chose dans la configuration!!

J'ai déjà tenté de résoudre le problème en décommentant « rootdn » et en rajoutant « rootpw » avec le mot de passe admin ou encore le résultat de la commande « slapasswd »... pareil...

Je ne m'y connais pas en LDAP... encore moins en OpenLDAP. Du coup je suis dans le jus jusqu'au cou!!:(  
Merci de m'aider SVP!!

Commentaire par **Xiillion** le 5 mars 2010 @ [15:57](#)

Bonjour à tous et merci pour le tuto,

Cependant j'ai un petit souci, j'ai configuré OpenLDAP et Dovecot, authentification Dovecot en telnet avec un user ldap pas de souci. Aujourd'hui j'implémente postfix et j'essaie d'envoyer un mail à un user ldap pas moyen:

```
to=, relay=local, delay=0.36, delays=0.29/0.03/0/0.05, dsn=5.1.1, status=bounced (unknown user: \ »flo\ »)
```

Avec mon compte Unix ça ne pose pas de problème: s une idée ?

Commentaire par **Gache56** le 6 avril 2010 @ [18:12](#)

Bonjour,

Merci pour ce tutoriel.

J'ai eu la même erreur que Reno et pour la résoudre, j'ai supprimé le répertoire /var/run/saslauthd puis j'ai créé un lien symbolique : ln -s /var/spool/postfix/var/run/saslauthd /var/run/saslauthd.

Et après ça, le répertoire /var/run/saslauthd pointe vers /var/spool/postfix/var/run/saslauthd /var/run/saslauthd et je n'ai plus d'erreur du tout et tout fonctionne à merveille.

Commentaire par **lebas** le 9 juin 2010 @ [12:47](#)

Bonjour

@zarakeye

Je pense qu'il est trop tard pour ton problème, mais j'ai été confronté à la même chose.

Avec mon système j'étais obligé de configurer la base en bdb et non en hdb. En hdb impossible à faire fonctionner ...

Sinon merci beaucoup pour ce tuto. Je vais continuer la suite.

Commentaire par **AlainT** le 31 juillet 2010 @ [18:45](#)

Bonjour,

@Jopa,

Merci pour ce tuto sur lequel je viens en suivant un autre tuto pour installer SOGo sur une Debian 5 toute neuve.

@zarakeye,

Je suis sur le même problème depuis plus de 2 heures...

As-tu trouvé une solution ?

Merci d'avance.

Commentaire par **AlainT** le 31 juillet 2010 @ [23:59](#)

Bonsoir,

Finalement, mon LDAP est bien rempli malgré que la commande ldapadd -x... renvoyait ldapadd -h.

Par contre le testsaslauthd des users me renvoie toujours

0: NO « authentication failed »

J'ai cherché et relu tous les fichiers, je ne vois pas où ça pêche.

J'ai quand même installé CYRUS, mais bien sur un cyradm ...

me renvoie:

Login failed: authentication failure at /usr/lib/perl5/Cyrus/IMAP/Admin.pm line 119

cyradm: cannot authenticate to server as cyrus

Merci de votre aide.

Commentaire par **AlainT** le 2 août 2010 @ [13:40](#)

Bonjour,

Je viens de refaire l'install depuis le début, sous Debian 5, et j'ai toujours un plantage en fin d'installation de la brique sasl

sogo:/etc# testsaslauthd -u alain -p alain

connect() : No such file or directory

0: sogo:/etc#

Alors que mon serveur de mail fonctionne correctement :

mailserver:/etc# testsaslauthd -u alain -p xxxxxxxx

0: NO « authentication failed »

mailserver:/etc# testsaslauthd -u athabaud -p xxxxxxxx

0: OK « Success. »

mailserver:/etc#

Après comparaisons des configs, j'ai réussi à faire fonctionner mon sogo en modifiant le /etc/default/saslauthd comme suit :

Remplacer « MECH\_OPTIONS= » » par « MECH\_OPTIONS= »/etc/saslauthd.conf »"

A moins que j'ai raté qqch, il faudrait peut-être mettre à jour le tutoriel ?

Cordialement.

Commentaire par **Yannick E.** le 25 septembre 2010 @ [14:05](#)

Bonjour Jopa et merci et merci pour ce tuto. Il est très intéressant. Je l'ai implémenté jusqu'à la 4e brique et l'ai connecté à eGroupware et il fonctionne très bien. Maintenant j'ai un souci: j'arrive pas à joindre des pièces d'une certaine taille à mes mails. Je me doute que ce doit être dans un fichier de configuration mais je ne sais pas lequel.

Please help.

Commentaire par **Yannick E.** le 25 septembre 2010 @ [15:02](#)

En plus j'arrive pas à envoyer des mails à l'extérieur.

Commentaire par **Le Blasé** le 3 février 2011 @ [16:05](#)

Bonjour, je déterre un peu le tutoriel qui est sagement resté sans commentaires depuis maintenant quelques temps.

J'ai un soucis au niveau de cyrus/postfix. Je peux créer les boîtes en me connectant au shell d'administration de Cyrus avec la commande:

```
cyradm -user cyrus localhost
```

```
> cm user.
```

Mais je n'arrive pas à accéder à la boîte via un client mail comme Thunderbird ou par l'interface d'egroupware, j'ai un soucis perpétuel de connection qui se résume à l'erreur suivante:

» MailBox does not exist »

Pourtant je peux voir que la boîte a bien été créée dans le répertoire /var/spool/cyrus/mail/... Une idée quelqu'un ?

Commentaire par **Nooo Vice !** le 25 avril 2012 @ [15:52](#)

Je suis entrain de créer un web mail. Et j'ai besoin de serveur SMTP/IMAP Annuaire LDAP ect...ce billet de blog m'aide beaucoup dans la configuration coté serveur mais je me demande si j'ai bien besoin d'une base de données pour sauvegarder mes mails dans l'application si le serveur SMTP/IMAP le fait à ma place ?

Je suis confus !

Laisser un commentaire

Nom (requis)

E-mail (requis)

URI  
.....

Anti-spam word: (Required)\*

To prove you're a person (not a spam script), type the security word shown in the picture. Click on the picture to hear an audio file of the word.



Votre Commentaire

Envoyer

- [Recherche](#)
- [Archives](#)
- [Catégories](#)

## Recherche

Rechercher sur ce blog...

Go

## Archives

- [octobre 2012](#)
- [août 2011](#)
- [juillet 2010](#)
- [juin 2010](#)
- [novembre 2009](#)
- [octobre 2009](#)
- [août 2009](#)
- [juillet 2009](#)
- [mai 2009](#)
- [avril 2009](#)
- [mars 2009](#)
- [février 2009](#)
- [janvier 2009](#)
- [décembre 2008](#)
- [novembre 2008](#)
- [octobre 2008](#)
- [septembre 2008](#)
- [mars 2008](#)

## Catégories

- [Astuces](#)
- [Bidouilles](#)

- [Configurations](#)
- [Divers](#)
- [Evènements](#)
- [Images](#)
- [Planet-Libre](#)
- [Réseau](#)
- [Scripts](#)
- [Système](#)

## • Articles Récents

- [Rrrrohhh !](#)
- [Frontview, t'es mou !](#)  
(ou comment booster l'interface Web de son ReadyNAS)
- [Du physique au virtuel avec « Mondo Rescue »](#)
- [Démonstration de Proxmox VE](#)
- [Linux Live USB Creator – « LiLi » pour les intimes](#)

## • Articles au pif

- [Synergy et mon bureau est plus propre !](#)
- [Jouer avec La Fonera... - 1ère partie : Présentation](#)
- [Prism : Le navigateur pour vos applications WEB](#)
- [Airserv-ng : Fonera en sonde wifi pour Aircrack-ng](#)
- [Raid logiciel : raid 1 vers raid 0](#)

## • Mots-clefs

[Boot](#) [Bureau](#) [Code barre](#) [Debian](#) [Dhcp](#) [Disque dur](#) [Distribution](#) [Dns](#) [Domotique](#) [DVD](#)  
[Développement](#) [fichiers](#) [Firewall](#) [Fonera](#) [Free](#) [Gnome](#) [Groupware](#) [Internet](#) [Jeux](#) [Linux](#)  
[Logiciels Libres](#) [Mail](#) [Messagerie](#) [Mir:ror](#) [Musique](#) [Nabaztag](#) [Openvpn](#) [Openwrt](#)  
[Partition](#) [PDA](#) [rfid](#) [Réseau](#) [Sauvegarde](#) [Script](#) [Serveur](#) [SSL](#) [Newsgroups](#) [Sécurité](#) [Téléphone](#)  
[Ubuntu](#) [Usb](#) [Vidéo](#) [Virtualisation](#) [VPN](#) [webcam](#) [Wifi](#)

## • Commentaires récents

- xxl dans [Rrrrohhh !](#)
- ldolle dans [Démonstration de Proxmox VE](#)
- laurine dans [Du physique au virtuel avec « Mondo Rescue »](#)
- laurine dans [Du physique au virtuel avec « Mondo Rescue »](#)
- gb56 dans [Démonstration de Proxmox VE](#)
- Guyou dans [Mir:ror mon beau Mir:ror...Comment puis-je te comprendre ?](#)
- morphy dans [Démonstration de Proxmox VE](#)
- mohand dans [Configuration de la connection USB et Bluetooth sur GNU/Linux Debian Lenny d'un téléphone portable Nokia 3600 Slide](#)
- Nooo Vice ! dans [Installation d'un serveur mail brique par brique... \(OpenLDAP, Postfix, Cyrus-imap, TLS, SASL, Spamassassin, Amavis, etc...\)](#)
- spawnrider dans [Frontview, t'es mou !](#)  
(ou comment booster l'interface Web de son ReadyNAS)

## • Méta

- [Connexion](#)
- [Flux RSS des articles](#)
- [RSS des commentaires](#)
- [WordPress.org](#)

## • Copains de moi...

- [ASphalt Models](#)
- [Construire une borne d'arcade...en 6 mois...](#)
- [Torglut's blog](#)

## • Ah doub doub doub...

## • A visiter...

- [Artisan Numérique](#)
- [Coagul](#)
- [Debian](#)
- [EquinoxeFR](#)
- [Full Circle Magazine](#)
- [Full Circle Magazine \(FR\)](#)
- [La Linuxerie](#)
- [Lefinnois.net](#)
- [OpenWrt](#)
- [Planet Libre](#)
- [SemaGeek](#)
- [System-Linux](#)
- [Toolinux](#)
- [Unix Garden](#)

## • Stats

- Pages affichées : **540656**
- Visiteurs Uniques : **204468**
- Hits dernières 24 heures : **258**
- Hits uniques 24 heures : **120**



Propulsé par [Wordpress](#) | Thème [WP Premium](#) par [WP Remix](#) | Traduction ([niss.fr](#)).



Ce site est mis à disposition sous licence [Creative Common](#).

- [Accueil](#)
- [Edito...](#)