

## Courier et OpenLDAP

Ce tutoriel développe la mise en place d'un serveur Courier (pop3(s)/imap(s)) qui interrogera un annuaire OpenLDAP pour authentifier les utilisateurs.

Un montage NFS sera utilisé pour que Courier puisse lire et écrire dans le répertoire Maildir du home directory des utilisateurs.

### **Installation des packages**

**Sur mail.alex.fr :**

courier-imap-ssl courier-pop-ssl courier-authlib-ldap postfix libnss-ldap nscd nfs-common

Répondre dans l'interface de configuration de Postfix :

Type de configuration : Système satellite

Nom de courrier : mail.alex.dmz

Serveur relais SMTP : smtp.alex.dmz

### **Configuration du montage NFS**

(Voir le tutoriel "[Redondance et continuité de service](#)" pour la configuration du serveur NFS)

Modifiez le fichier /etc/resolv.conf :

```
search alex.dmz alex.fr alex.com alex.org
nameserver 172.16.0.1
nameserver 172.17.0.1
```

Modifiez le fichier /etc/network/interfaces :

```
# The loopback network interface
auto lo eth0 eth1
iface lo inet loopback

# The primary network interface
allow-hotplug eth0 eth1
iface eth0 inet static
address 123.45.67.11
netmask 255.255.255.240
gateway 123.45.67.14

iface eth1 inet static
address 172.16.0.8
netmask 255.255.255.0
up route add -net 172.17.0.0/16 gw 172.16.0.254
up route add -net 172.18.0.0/16 gw 172.16.0.254
```

Copiez depuis le serveur pdc.alex.lan le certificat du serveur ldap1 et ldap2, après avoir créé le répertoire /etc/ldap/tls :

```
mail:~# mkdir /etc/ldap/tls  
mail:~# scp  
root@172.17.0.3:/etc/ldap/tls/ldap_ldap*_cert.pem /etc/ldap/tls/
```

Modifiez le fichier /etc/ldap/ldap.conf :

```
TLS_CACERTDIR /etc/ldap/tls  
TLS_REQCERT allow  
  
BASE dc=meta  
URI ldaps://ldap2.alex.dmz ldaps://ldap1.alex.dmz
```

Modifiez le fichier /etc/libnss-ldap.conf :

```
base dc=meta  
  
uri ldaps://ldap2.alex.dmz ldaps://ldap1.alex.dmz  
  
ldap_version 3  
  
scope sub  
  
timelimit 30  
  
bind_timelimit 30  
  
bind_policy soft  
  
pam_filter objectclass=posixaccount  
  
pam_login_attribute uid  
  
nss_base_passwd      dc=meta?sub  
nss_base_group       dc=meta?sub  
  
ssl on
```

Modifiez le fichier /etc/nsswitch.conf :

```
passwd:      compat ldap  
group:      compat ldap
```

```

shadow:      compat

hosts:       files dns
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

```

Modifiez le fichier /etc/nscd.conf :

```

#
# /etc/nscd.conf
#
# Currently supported cache names (services): passwd, group, hosts
#
# logfile          /var/log/nscd.log
# threads          6
# max-threads      128
server-user       nobody
# stat-user        somebody
debug-level       0
# reload-count    5
paranoia          no
# restart-interval 3600

enable-cache      passwd      yes
positive-time-to-live passwd    600
negative-time-to-live passwd    20
suggested-size    passwd      1100
check-files       passwd      yes
persistent        passwd      yes
shared             passwd      yes

enable-cache      group       yes
positive-time-to-live group    3600
negative-time-to-live group    60
suggested-size    group       211
check-files       group       yes
persistent        group       yes
shared             group       yes

enable-cache      hosts       yes
positive-time-to-live hosts   3600
negative-time-to-live hosts   20
suggested-size    hosts       211
check-files       hosts       yes

```

persistent	hosts	yes
shared	hosts	yes

Redémarrez le service nscd :

```
mail:~# /etc/init.d/nscd restart
Restarting Name Service Cache Daemon: nscd.
```

Modifiez le fichier /etc/default/nfs-common :

```
# If you do not set values for the NEED_ options, they will be attempted
# autodetected; this should be sufficient for most people.
# Valid alternatives for the NEED_ options are "yes" and "no".

# Options for rpc.statd.
# Should rpc.statd listen on a specific port? This is especially useful
# when you have a port-based firewall. To use a fixed port, set this
# this variable to a statd argument like:
# "--port 4000 --outgoing-port 4001".
# For more information, see rpc.statd(8) or http://wiki.debian.org/?
SecuringNFS
STATDOPTS=

# Some kernels need a separate lockd daemon; most don't. Set this if you
# want to force an explicit choice for some reason.
NEED_LOCKD=

# Do you want to start the idmapd daemon? It is only needed for NFSv4.
# Nous utilisons NFSv4.
NEED_IDMAPD=yes

# Do you want to start the gssd daemon? It is required for Kerberos
mounts.
NEED_GSSD=
```

Redémarrez le service NFS :

```
mail:~# /etc/init.d/nfs-common restart
Stopping NFS common utilities: idmapd statd.
Starting NFS common utilities: statd idmapd.
mail:~#
```

Ajoutez cette ligne dans le fichier /etc/fstab :

```
...
# Partage /home du serveur NFS nas.alex.dmz.
```

```
172.16.0.19:/home /home nfs4 rsize=32768,wsiz
```

```
e 0
```

Le point de montage est /home dans mon cas.

Montez le partage NFSv4 :

```
mail:~# mount /home
```

Pour vérifier :

```
mail:~# mount | grep home
172.16.0.19:/home on /home type nfs4
(rw,rsize=32768,wsiz
```

```
e=32768,soft,addr=172.16.0.19)
mail:~#
```

## **Configuration de Courier**

Modifiez le fichier /etc/aliases pour rediriger les mails envoyés au compte root vers un autre compte de votre choix (que vous avez créé dans un des annuaires par exemple) :

```
# See man 5 aliases for format
postmaster:    root
root:          blackhole@alex.lan
```

Lancez cette commande pour reconstruire la base de données des alias mail :

```
mail:~# newaliases
```

Redémarrez le service Postfix :

```
mail:~# /etc/init.d/postfix restart
Stopping Postfix Mail Transport Agent: postfix.
Starting Postfix Mail Transport Agent: postfix.
mail:~#
```

Pour des raisons de sécurité, nous allons utiliser imaps et pop3s.

Il faut générer notre propre certificat avec nos coordonnées, puisque par défaut c'est un certificat générique qui est généré à l'installation du package.

Modifiez le fichier /etc/courier/imapd.cnf :

```
RANDFILE = /usr/lib/courier/imapd.rand
```

```
[ req ]  
default_bits = 1024  
encrypt_key = yes  
distinguished_name = req_dn  
x509_extensions = cert_type  
prompt = no  
  
[ req_dn ]  
C=FR  
ST=Haute-Savoie  
L=Alex  
O=Courier Mail Server  
OU=Alex IMAP SSL key  
CN=mail.alex.fr  
emailAddress=postmaster@alex.fr  
  
[ cert_type ]  
nsCertType = server
```

Modifiez le fichier /etc/courier/pop3d.cnf :

```
RANDFILE = /usr/lib/courier/pop3d.rand  
  
[ req ]  
default_bits = 1024  
encrypt_key = yes  
distinguished_name = req_dn  
x509_extensions = cert_type  
prompt = no  
  
[ req_dn ]  
C=FR  
ST=Haute-Savoie  
L=Alex  
O=Courier Mail Server  
OU=Alex POP3 SSL key  
CN=mail.alex.fr  
emailAddress=postmaster@alex.fr  
  
[ cert_type ]  
nsCertType = server
```

Effacez les certificats pré-générés :

```
mail:~# rm /etc/courier/*.pem
```

Lancez les commandes suivantes pour générer vos certificats :

```
mail:~# mkimapdcert  
mail:~# mkpop3dcert
```

Modifiez le fichier /etc/courier/authdaemonrc :

```
##VERSION: $Id: authdaemonrc.in,v 1.13 2005/10/05 00:07:32 mrsam Exp $  
#  
# Copyright 2000-2005 Double Precision, Inc. See COPYING for  
# distribution information.  
#  
# authdaemonrc created from authdaemonrc.dist by sysconftool  
#  
# Do not alter lines that begin with ##, they are used when upgrading  
# this configuration.  
#  
# This file configures authdaemond, the resident authentication daemon.  
#  
# Comments in this file are ignored. Although this file is intended to  
# be sourced as a shell script, authdaemond parses it manually, so  
# the acceptable syntax is a bit limited. Multiline variable contents,  
# with the \ continuation character, are not allowed. Everything must  
# fit on one line. Do not use any additional whitespace for indentation,  
# or anything else.  
  
##NAME: authmodulelist:2  
#  
# The authentication modules that are linked into authdaemond. The  
# default list is installed. You may selectively disable modules simply  
# by removing them from the following list. The available modules you  
# can use are: authuserdb authpam authpgsql authldap authmysql authcustom  
authpipe  
# Nous utilisons le module LDAP.  
authmodulelist="authldap"  
  
##NAME: authmodulelistorig:3  
#  
# This setting is used by Courier's webadmin module, and should be left  
# alone  
# Nous n'utilisons pas Courier's webadmin.  
authmodulelistorig=""  
  
##NAME: daemons:0  
#  
# The number of daemon processes that are started. authdaemon is  
# typically installed where authentication modules are relatively  
# expensive: such as authldap, or authmysql, so it's better to have a
```

```

# number of them running. PLEASE NOTE: Some platforms may experience a
# problem if there's more than one daemon.
# Specifically, SystemV derived platforms that use TLI with
# socket emulation. I'm suspicious of TLI's ability to handle multiple
# processes accepting connections on the same filesystem domain socket.
#
# You may need to increase daemons if as your system load increases.
# Symptoms include sporadic authentication failures. If you start getting
# authentication failures, increase daemons. However, the default of 5
# SHOULD be sufficient. Bumping up daemon count is only a short-term
# solution. The permanent solution is to add more resources: RAM, faster
# disks, faster CPUs...
# Selon la charge mettre plus.
daemons=5

##NAME: authdaemonvar:2
#
# authdaemonvar is here, but is not used directly by authdaemond. It's
# used by various configuration and build scripts, so don't touch it!
authdaemonvar=/var/run/courier/authdaemon

##NAME: DEBUG_LOGIN:0
#
# Dump additional diagnostics to syslog
#
# DEBUG_LOGIN=0 - turn off debugging
# DEBUG_LOGIN=1 - turn on debugging
# DEBUG_LOGIN=2 - turn on debugging + log passwords too
#
# *** YES ** - DEBUG_LOGIN=2 places passwords into syslog.
#
# Note that most information is sent to syslog at level 'debug', so
# you may need to modify your /etc/syslog.conf to be able to see it.
# Pour faire vos tests, mettez à 2. Quand tout est bon, mettez à zéro.
DEBUG_LOGIN=2

##NAME: DEFAULTOPTIONS:0
#
# A comma-separated list of option=value pairs. Each option is applied
# to an account if the account does not have its own specific value for
# that option. So for example, you can set
# DEFAULTOPTIONS="disablewebmail=1,disableimap=1"
# and then enable webmail and/or imap on individual accounts by setting
# disablewebmail=0 and/or disableimap=0 on the account.
DEFAULTOPTIONS=""

##NAME: LOGGEROPTS:0
#
# courierlogger(1) options, e.g. to set syslog facility
#
LOGGEROPTS=""

```

```

##NAME: LDAP_TLS_OPTIONS:0
#
# Options documented in ldap.conf(5) can be set here, prefixed with
'LDAP'.
# Examples:
#
#LDAPTLS_CACERT=/path/to/cacert.pem
#LDAPTLS_REQCERT=demand
#LDAPTLS_CERT=/path/to/clientcert.pem
#LDAPTLS_KEY=/path/to/clientkey.pem
# Nous indiquons le répertoire où se trouve nos certificats OpenLDAP.
LDAPTLS_CACERTDIR=/etc/ldap/tls
LDAPTLS_REQCERT=allow

```

Modifiez le fichier /etc/courier/authldaprc :

```

##VERSION: $Id: authldaprc,v 1.25 2005/10/05 00:07:32 mrsam Exp $
#
# Copyright 2000-2004 Double Precision, Inc. See COPYING for
# distribution information.
#
# Do not alter lines that begin with ##, they are used when upgrading
# this configuration.
#
# authldaprc created from authldaprc.dist by sysconftool
#
# DO NOT INSTALL THIS FILE with world read permissions. This file
# might contain the LDAP admin password!
#
# This configuration file specifies LDAP authentication parameters
#
# The format of this file must be as follows:
#
# field[spaces|tabs]value
# ATTENTION : La syntaxe est très importante, n'hésitez pas à supprimer
# tous les commentaires pour ne laisser que les options utilisées.
# Sinon ca bug, j'en ai fait les frais ...
#
# That is, the name of the field, followed by spaces or tabs, followed by
# field value. No trailing spaces.
#
# Here are the fields:
#
##NAME: LOCATION:1
#
# Location of your LDAP server(s). If you have multiple LDAP servers,
# you can list them separated by commas and spaces, and they will be
# tried in turn.
# Adresses des annuaires OpenLDAP.
LDAP_URI ldap://ldap2.alex.dmz, ldap://ldap1.alex.dmz

```

```

##NAME: LDAP_PROTOCOL_VERSION:0
#
# Which version of LDAP protocol to use
LDAP_PROTOCOL_VERSION 3

##NAME: LDAP_BASEDN:0
#
# Look for authentication here:
LDAP_BASEDN dc=meta

##NAME: LDAP_BINDDN:0
#
# You may or may not need to specify the following. Because you've got
# a password here, authldaprc should not be world-readable!!!
#LDAP_BINDDN cn=administrator, o=example, c=com
#LDAP_BINDPW toto

##NAME: LDAP_TIMEOUT:0
#
# Timeout for LDAP search and connection
LDAP_TIMEOUT 10

##NAME: LDAP_AUTHBIND:0
#
# Define this to have the ldap server authenticate passwords.
# If LDAP_AUTHBIND the password is validated by rebinding with the
# supplied userid and password. If rebind succeeds, this is considered
# to be an authenticated request. This does not support CRAM-MD5
# authentication, which requires clearPassword.
# Additionally, if LDAP_AUTHBIND is 1 then password changes are done
# under the credentials of the user themselves, not LDAP_BINDDN/BINDPW
#
# Permet d'authentifier l'utilisateur en faisant une requête LDAP avec le
# login et mot de passe donnés à l'authentification. Si la requête
# réussit, l'utilisateur est déclaré valide.
LDAP_AUTHBIND 1

##NAME: LDAP_MAIL:0
#
# Here's the field on which we query
# L'attribut recherché pour la requête LDAP.
LDAP_MAIL uid

##NAME: LDAP_FILTER:0
#
# This LDAP filter will be ANDed with the query for the field defined
# above in LDAP_MAIL. So if you are querying for mail, and you have
# LDAP_FILTER defined to be "(objectClass=CourierMailAccount)" the query
# that is performed will be
# "(&(objectClass=CourierMailAccount)(mail=<someAccount>))"
#

```

```

# Filtre appliqué pour la requête LDAP.
LDAP_FILTER (&(objectClass=MailAccount) (mailAccountActive=yes))

##NAME: LDAP_DOMAIN:0
#
# The following default domain will be appended, if not explicitly
specified.
#
# LDAP_DOMAIN example.com

##NAME: LDAP_GLOB_IDS:0
#
# The following two variables can be used to set everybody's uid and gid.
# This is convenient if your LDAP specifies a bunch of virtual mail
# accounts The values can be usernames or userids:
#
# LDAP_GLOB_UID vmail
# LDAP_GLOB_GID vmail

##NAME: LDAP_HOMEDIR:0
#
# We will retrieve the following attributes
#
# The HOMEDIR attribute MUST exist, and we MUST be able to chdir to it
LDAP_HOMEDIR homeDirectory

##NAME: LDAP_MAILROOT:0
#
# If homeDirectory is not an absolute path, define the root of the
# relative paths in LDAP_MAILROOT
#
# LDAP_MAILROOT /var/mail

##NAME: LDAP_MAILDIR:0
#
# The MAILDIR attribute is OPTIONAL, and specifies the location of the
# mail directory. If not specified, ./Maildir will be used
#LDAP_MAILDIR      mailbox

##NAME: LDAP_DEFAULTDELIVERY:0
#
# Courier mail server only: optional attribute specifies custom mail
# delivery instructions for this account (if defined) -- essentially
# overrides DEFAULTDELIVERY from ${sysconfdir}/courierd
LDAP_DEFAULTDELIVERY defaultDelivery

##NAME: LDAP_MAILDIRQUOTA:0
#
# The following variable, if defined, specifies the field containing the
# maildir quota, see README.mailldirquota for more information
#
# LDAP_MAILDIRQUOTA quota

```

```
##NAME: LDAP_FULLNAME:0
#
# FULLNAME is optional, specifies the user's full name
LDAP_FULLNAME cn

##NAME: LDAP_PWD:0
#
# CLEARPW is the clear text password. CRYPT is the encrypted password.
# ONE OF THESE TWO ATTRIBUTES IS REQUIRED. If CLEARPW is provided, and
# libhmac.a is available, CRAM authentication will be possible!
#
#LDAP_CLEARPW clearPassword
LDAP_CRYPTPWD userPassword

##NAME: LDAP_IDS:0
#
# Uncomment the following, and modify as appropriate, if your LDAP
# database stores individual userids and groupids. Otherwise, you must
# uncomment LDAP_GLOB_UID and LDAP_GLOB_GID above. LDAP_GLOB_UID and
# LDAP_GLOB_GID specify a uid/gid for everyone. Otherwise, LDAP_UID and
# LDAP_GID must be defined as attributes for everyone.
#
LDAP_UID uidNumber
LDAP_GID gidNumber

##NAME: LDAP_AUXOPTIONS:0
#
# Auxiliary options. The LDAP_AUXOPTIONS setting should contain a list
# of comma-separated "ATTRIBUTE=NAME" pairs. These names are additional
# attributes that define various per-account "options", as given in
# INSTALL's description of the OPTIONS setting.
#
# Each ATTRIBUTE specifies an LDAP attribute name. If it is present,
# the attribute value gets placed in the OPTIONS variable, with the name
# NAME. For example:
#
# LDAP_AUXOPTIONS shared=sharedgroup,disableimap=disableimap
#
# Then, if an LDAP record contains the following attributes:
#
#     shared: domain1
#     disableimap: 0
#
# Then authldap will initialize OPTIONS to
# "sharedgroup=domain1,disableimap=0"
#
# NOTE: ** no spaces in this setting **, the above example has exactly
# one tab character after LDAP_AUXOPTIONS

##NAME: LDAP_ENUMERATE_FILTER:0
#
```

```

# {EXPERIMENTAL}
# Optional custom filter used when enumerating accounts for
# authenumerate, in order to compile a list of accounts for shared
# folders. If present, this filter will be used instead of LDAP_FILTER.
#
# LDAP_ENUMERATE_FILTER
#(& (objectClass=CourierMailAccount) (! (disabledshared=1)))
##NAME: LDAP_DEREF:0
#
# Determines how aliases are handled during a search. This option is
# available only with OpenLDAP 2.0
#
# LDAP_DEREF can be one of the following values:
# never, searching, finding, always. If not specified, aliases are
# never dereferenced.
LDAP_DEREF never

##NAME: LDAP_TLS:0
#
# Set LDAP_TLS to 1 to use the Start TLS extension (RFC 2830). This is
# when the server accepts a normal LDAP connection on port 389 which
# the client then requests 'upgrading' to TLS, and is equivalent to the
# -ZZ flag to ldapsearch. If you are using an ldaps:// URI then do not
# set this option.
#
# For additional LDAP-related options, see the authdaemonrc config file.
LDAP_TLS 0

...

```

Modifiez cette ligne dans le fichier /etc/courier/imapd :

```

...
##NAME: IMAPDSTART:0
#
# IMAPDSTART is not used directly. Rather, this is a convenient flag to
# be read by your system startup script in /etc/rc.d, like this:
#
# . /etc/courier/imapd
#
# case $IMAPDSTART in
# x[yY]*)
#         /usr/lib/courier/imapd.rc start
#         ;;
# esac
#
# The default setting is going to be NO, so you'll have to manually flip
# it to yes.

```

```
#IMAPDSTART=YES
```

```
IMAPDSTART=NO
```

```
...
```

Modifiez cette ligne dans le fichier /etc/courier/pop3d :

```
...
```

  

```
##NAME: POP3DSTART:0
```

```
#
```

```
# POP3DSTART is not referenced anywhere in the standard Courier programs
```

```
# or scripts. Rather, this is a convenient flag to be read by your system
```

```
# startup script in /etc/rc.d, like this:
```

```
#
```

```
# . /etc/courier/pop3d
```

```
# case x$POP3DSTART in
```

```
# x[yY]*)
```

```
    /usr/lib/courier/pop3d.rc start
```

```
#      ;;
```

```
# esac
```

```
#
```

```
# The default setting is going to be NO, until Courier is shipped by
```

```
# default with enough platforms so that people get annoyed with having to
```

```
# flip it to YES every time.
```

```
#POP3DSTART=YES
```

```
POP3DSTART=NO
```

  

```
...
```

Modifiez le fichier /etc/courier/imapd-ssl :

```
##VERSION: $Id: imapd-ssl.dist.in,v 1.12 2005/07/02 01:13:57 mrsam Exp $
```

```
#
```

```
# imapd-ssl created from imapd-ssl.dist by sysconftool
```

```
#
```

```
# Do not alter lines that begin with ##, they are used when upgrading
```

```
# this configuration.
```

```
#
```

```
# Copyright 2000 - 2004 Double Precision, Inc. See COPYING for
```

```
# distribution information.
```

```
#
```

```
# This configuration file sets various options for the Courier-IMAP
```

```
# server when used to handle SSL IMAP connections.
```

```
#
```

```
# SSL and non-SSL connections are handled by a dedicated instance of the
```

```
# couriertcpd daemon. If you are accepting both SSL and non-SSL IMAP
```

```
# connections, you will start two instances of couriertcpd, one on the
```

```
# IMAP port 143, and another one on the IMAP-SSL port 993.
```

```

#
# Download OpenSSL from http://www.openssl.org/
#
##NAME: SSLPORT:1
#
# Options in the imapd-ssl configuration file AUGMENT the options in the
# imapd configuration file. First the imapd configuration file is read,
# then the imapd-ssl configuration file, so we do not have to redefine
# anything.
#
# However, some things do have to be redefined. The port number is
# specified by SSLPORT, instead of PORT. The default port is port 993.
#
# Multiple port numbers can be separated by commas. When multiple port
# numbers are used it is possible to select a specific IP address for a
# given port as "ip.port". For example, "127.0.0.1.900,192.68.0.1.900"
# accepts connections on port 900 on IP addresses 127.0.0.1 and
# 192.68.0.1. The SSLADDRESS setting is a default for ports that do not
# have a specified IP address.
#
# Nous écouterons le port 993 sur l'interface privée uniquement.
#SSLPORT=993
SSLPORT=172.16.0.8.993

##NAME: SSLADDRESS:0
#
# Address to listen on, can be set to a single IP address.
#
# SSLADDRESS=127.0.0.1
SSLADDRESS=0

##NAME: SSLPIDFILE:0
#
# That's the SSL IMAP port we'll listen on.
# Feel free to redefine MAXDAEMONS, TCPDOPTS, and MAXPERIP.
SSLPIDFILE=/var/run/courier/imapd-ssl.pid

##NAME: SSLLOGGEROPTS:0
#
# courierlogger(1) options.
#
SSLLOGGEROPTS="-name=imapd-ssl"

##NAME: IMAPDSSLSTART:0
#
# Different pid files, so that both instances of couriertcpd can coexist
# happily.
#
# You can also redefine IMAP_CAPABILITY, although I can't
# think of why you'd want to do that.
#
#
# Ok, the following settings are new to imapd-ssl:

```

```

#
# Whether or not to start IMAP over SSL on simap port:
IMAPDSSLSTART=YES

##NAME: IMAPDSTARTTLS:0
#
# Whether or not to implement IMAP STARTTLS extension instead:
IMAPDSTARTTLS=YES

##NAME: IMAP_TLS_REQUIRED:1
#
# Set IMAP_TLS_REQUIRED to 1 if you REQUIRE STARTTLS for everyone.
# (this option advertises the LOGINDISABLED IMAP capability, until
# STARTTLS is issued).
IMAP_TLS_REQUIRED=0

#####
#
# The following variables configure IMAP over SSL. If OpenSSL is
available
# during configuration, the couriertls helper gets compiled, and upon
# installation a dummy TLS_CERTFILE gets generated. courieresmtpd will
# automatically advertise the ESMTP STARTTLS extension if both
# TLS_CERTFILE and COURIERTLS exist.
#
# WARNING: Peer certificate verification has NOT yet been tested.
Proceed
# at your own risk. Only the basic SSL/TLS functionality is known to be
# working. Keep this in mind as you play with the following variables.
#
##NAME: COURIERTLS:0
#
COURIERTLS=/usr/bin/couriertls

##NAME: TLS_PROTOCOL:0
#
# TLS_PROTOCOL sets the protocol version. The possible versions are:
#
# SSL2 - SSLv2
# SSL3 - SSLv3
# TLS1 - TLS1
TLS_PROTOCOL=SSL3

##NAME: TLS_STARTTLS_PROTOCOL:0
#
# TLS_STARTTLS_PROTOCOL is used instead of TLS_PROTOCOL for the IMAP
STARTTLS
# extension, as opposed to IMAP over SSL on port 993.
#
TLS_STARTTLS_PROTOCOL=TLS1

```

```
##NAME: TLS_CIPHER_LIST:0
#
# TLS_CIPHER_LIST optionally sets the list of ciphers to be used by the
# OpenSSL library. In most situations you can leave TLS_CIPHER_LIST
# undefined
#
# TLS_CIPHER_LIST="ALL:!ADH:RC4+RSA:+SSLv2:@STRENGTH"

##NAME: TLS_TIMEOUT:0
# TLS_TIMEOUT is currently not implemented, and reserved for future use.
# This is supposed to be an inactivity timeout, but its not yet
implemented.
#

##NAME: TLS_DHCERTFILE:0
#
# TLS_DHCERTFILE - PEM file that stores our Diffie-Hellman cipher pair.
# When OpenSSL is compiled to use Diffie-Hellman ciphers instead of RSA
# you must generate a DH pair that will be used. In most situations the
# DH pair is to be treated as confidential, and the file specified by
# TLS_DHCERTFILE must not be world-readable.
#
# TLS_DHCERTFILE=

##NAME: TLS_CERTFILE:0
#
# TLS_CERTFILE - certificate to use. TLS_CERTFILE is required for
SSL/TLS
# servers, and is optional for SSL/TLS clients. TLS_CERTFILE is usually
# treated as confidential, and must not be world-readable.
#
TLS_CERTFILE=/etc/courier/imapd.pem

##NAME: TLS_TRUSTCERTS:0
#
# TLS_TRUSTCERTS=pathname - load trusted certificates from pathname.
# pathname can be a file or a directory. If a file, the file should
# contain a list of trusted certificates, in PEM format. If a
# directory, the directory should contain the trusted certificates,
# in PEM format, one per file and hashed using OpenSSL's c_rehash
# script. TLS_TRUSTCERTS is used by SSL/TLS clients (by specifying
# the -domain option) and by SSL/TLS servers (TLS_VERIFYPEER is set
# to PEER or REQUIREPEER).
#
#
# TLS_TRUSTCERTS=

##NAME: TLS_VERIFYPEER:0
#
# TLS_VERIFYPEER - how to verify client certificates. The possible values
# of this setting are:
#
```

```

# NONE - do not verify anything
#
# PEER - verify the client certificate, if one's presented
#
# REQUIREPEER - require a client certificate, fail if one's not presented
#
#
TLS_VERIFYPEER=NONE

##NAME: TLS_CACHE:0
#
# A TLS/SSL session cache may slightly improve response for IMAP clients
# that open multiple SSL sessions to the server. TLS_CACHEFILE will be
# automatically created, TLS_CACHESIZE bytes long, and used as a cache
# buffer.
#
# This is an experimental feature and should be disabled if it causes
# problems with SSL clients. Disable SSL caching by commenting out the
# following settings:

TLS_CACHEFILE=/var/lib/courier/couriersslcache
TLS_CACHESIZE=524288

##NAME: MAILDIRPATH:0
#
# MAILDIRPATH - directory name of the maildir directory.
#
MAILDIRPATH=Maildir

```

Il n'est pas utile de modifier le fichier /etc/courier/pop3d-ssl car le serveur écoutera sur toutes ses interfaces avec le port pop3s standard.

Arrêtez les services pop3 et imap :

```

mail:~# /etc/init.d/courier-pop stop
Stopping Courier POP3 server: pop3d.

mail:~# /etc/init.d/courier-imap stop
Stopping Courier IMAP server: imapd.

```

Redémarrez les services courier-authdaemon, imaps et pop3s :

```

mail:~# /etc/init.d/courier-authdaemon restart
Stopping Courier authentication services: authdaemond.
Starting Courier authentication services: authdaemond.

mail:~# /etc/init.d/courier-imap-ssl restart
Stopping Courier IMAP-SSL server: imapd-ssl.

```

```
Starting Courier IMAP-SSL server: imapd-ssl.
```

```
mail:~# /etc/init.d/courier-pop-ssl restart
Stopping Courier POP3-SSL server: pop3d-ssl.
Starting Courier POP3-SSL server: pop3d-ssl.
```

Connectez-vous avec un utilisateur en imaps et vérifiez les logs en même temps :

```
mail:~# tail -f /var/log/syslog

Mois 1 10:00:00 mail imapd-ssl: Connection, ip=[::ffff:172.1x.x.x]
Mois 1 10:00:00 mail authdaemond: received auth request, service=imap,
authtype=login
Mois 1 10:00:00 mail authdaemond: authldap: trying this module
Mois 1 10:00:00 mail authdaemond: selected ldap protocol version 3
Mois 1 10:00:00 mail authdaemond: binding to LDAP server as DN '<null>',
password '<null>'
Mois 1 10:00:00 mail authdaemond: using search filter:
(&(&(objectClass=MailAccount) (mailAccountActive=yes)) (uid=usercom))
Mois 1 10:00:00 mail authdaemond: one entry returned, DN:
uid=usercom,ou=Users,dc=alex,dc=com,dc=meta
Mois 1 10:00:00 mail authdaemond: raw ldap entry returned:
Mois 1 10:00:00 mail authdaemond: | cn: usercom usercom
Mois 1 10:00:00 mail authdaemond: | uid: usercom
Mois 1 10:00:00 mail authdaemond: | homeDirectory: /home/usercom
Mois 1 10:00:00 mail authdaemond: | gidNumber: 20000
Mois 1 10:00:00 mail authdaemond: | uidNumber: 20002
Mois 1 10:00:00 mail authdaemond: authldaplib: sysusername=<null>,
sysuserid=20002, sysgroupid=20000, homedir=/home/usercom,
address=usercom, fullname=usercom usercom, maildir=<null>, quota=<null>,
options=<null>
Mois 1 10:00:00 mail authdaemond: authldaplib: clearpasswd=<null>,
passwd=<null>
Mois 1 10:00:00 mail authdaemond: rebinding with DN
'uid=usercom,ou=Users,dc=alex,dc=com,dc=meta' to validate password
Mois 1 10:00:00 mail authdaemond: authentication bind successful
Mois 1 10:00:00 mail authdaemond: Authenticated: sysusername=<null>,
sysuserid=20002, sysgroupid=20000, homedir=/home/usercom,
address=usercom, fullname=usercom usercom, maildir=<null>, quota=<null>,
options=<null>
Mois 1 10:00:00 mail authdaemond: Authenticated: clearpasswd=usercom,
passwd=<null>
Mois 1 10:00:00 mail imapd-ssl: LOGIN, user=usercom, ip=[::ffff:
172.1x.x.x], protocol=IMAP
Mois 1 10:00:00 mail imapd-ssl: LOGOUT, user=usercom, ip=[::ffff:
172.1x.x.x], headers=0, body=0, rcvd=242, sent=1136, time=12, starttls=1
```

Connectez-vous avec un utilisateur en pop3s et vérifiez les logs en même temps :

```
Mois 1 10:00:00 mail pop3d-ssl: Connection, ip=[::ffff:172.1x.x.x]

Mois 1 10:00:00 mail authdaemon: received auth request, service=pop3,
authtype=login
Mois 1 10:00:00 mail authdaemon: authldap: trying this module
Mois 1 10:00:00 mail authdaemon: selected ldap protocol version 3
Mois 1 10:00:00 mail authdaemon: binding to LDAP server as DN '<null>',
password '<null>'
Mois 1 10:00:00 mail authdaemon: using search filter:
(&(&(objectClass=MailAccount) (mailAccountActive=yes)) (uid=userfr))
Mois 1 10:00:00 mail authdaemon: one entry returned, DN:
uid=userfr,ou=Users,dc=alex,dc=fr,dc=meta
Mois 1 10:00:00 mail authdaemon: raw ldap entry returned:
Mois 1 10:00:00 mail authdaemon: | cn: userfr userfr
Mois 1 10:00:00 mail authdaemon: | uid: userfr
Mois 1 10:00:00 mail authdaemon: | homeDirectory: /home/userfr
Mois 1 10:00:00 mail authdaemon: | gidNumber: 513
Mois 1 10:00:00 mail authdaemon: | uidNumber: 10007
Mois 1 10:00:00 mail authdaemon: authldaplib: sysusername=<null>,
sysuserid=10007, sysgroupid=513, homedir=/home/userfr, address=userfr,
fullname=userfr userfr, maildir=<null>, quota=<null>, options=<null>
Mois 1 10:00:00 mail authdaemon: authldaplib: clearpasswd=<null>,
passwd=<null>
Mois 1 10:00:00 mail authdaemon: rebinding with DN
'uid=userfr,ou=Users,dc=alex,dc=fr,dc=meta' to validate password
Mois 1 10:00:00 mail authdaemon: authentication bind successful
Mois 1 10:00:00 mail authdaemon: Authenticated: sysusername=<null>,
sysuserid=10007, sysgroupid=513, homedir=/home/userfr, address=userfr,
fullname=userfr userfr, maildir=<null>, quota=<null>, options=<null>
Mois 1 10:00:00 mail authdaemon: Authenticated: clearpasswd=userfr,
passwd=<null>
Mois 1 10:00:00 mail pop3d-ssl: LOGIN, user=userfr, ip=[::ffff:172.1x.x.x]
Mois 1 10:00:00 mail pop3d-ssl: LOGOUT, user=userfr, ip=[::ffff:
172.1x.x.x], top=0, retr=5701, rcvd=72, sent=6197, time=1
```

Document mis à jour : 09/01/08



Ce document est publié sous licence [Creative Commons  
Attribution, Partage à l'identique, Contexte non commercial 3.0 :](http://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr)  
<http://creativecommons.org/licenses/by-nc-sa/3.0/deed.fr>