

LDAP & OpenLDAP Par la pratique...

Master Sciences & Technologie – 2^{ème} Année
Mention Mathématiques et Sciences Pour l'Ingénieur
Spécialité Informatique
Parcours Ingénierie du Logiciel Libre

Année 2009-2010

D. Duvivier – LIL – Université du Littoral Côte d'Opale – duvivier@lil.univ-littoral.fr

Nous avons eu un contact rapide avec OpenLDAP lors du premier TP SRS/Kernel, car nous installons et configurons la connexion à votre compte réseau via OpenLDAP (et autres outils de montage automatique de répertoires...).

1. A la recherche d'OpenLDAP...

Extrait du résultat de la commande suivante (les *-doc (...) n'y figurent pas) : `apt-cache search ldap | sort`

```
adtool - command line utility for Active Directory administration
autofs5-ldap - LDAP map support for autofs, version 5
bdii4 - information index based on OpenLDAP
courier-authlib-ldap - LDAP support for the Courier authentication library
courier-ldap - Courier mail server - LDAP support
cpu - a console based LDAP user management tool
dhcp3-server-ldap - DHCP server able to use LDAP as backend
directoryassistant - small LDAP address book manager
finger-ldap - Finger for machines that authenticate against LDAP
freeradius-ldap - LDAP module for FreeRADIUS server
gosa-desktop - Desktop integration for GOSA
gosa-help-fr - French online help for GOSA
gosa-schema - LDAP schema for GOSA
gosa - Web Based LDAP Administration Program
gq - GTK-based LDAP client
jmeter-ldap - Load testing and performance measurement application
krb5-kdc-ldap - MIT Kerberos key server (KDC) LDAP plugin
lat - LDAP Administration Tool
ldap2dns - LDAP based DNS management system.
ldap2zone - Extract DNS zones from LDAP trees
ldap-account-manager-lamdaemon - Quota and home directory management for LDAP Account Manager
ldap-account-manager - webfrontend for managing accounts in an LDAP directory
lapdiff - Tool to synchronize ldap servers using ldif formatted input files
lapdns - DNS server that pulls data from an LDAP directory
lapscripts - Add and remove user and groups (stored in a LDAP directory)
laptools - command-line LDAP utilities
lapwebui - web user interface for editing LDAP directories
laputils - OpenLDAP utilities
lapvi - perform an LDAP search and update results using a text editor
ldb-tools - LDAP-like embedded database - tools
lemonldap-ng - Lemonldap:NG Web-SSO system
luma - gui utility for accessing and managing LDAP database
lwat - LDAP Web-based Administration Tool
migrationtools - Migration scripts for LDAP
nssd - Daemon for NSS and PAM lookups using LDAP
openser-ldap-modules - LDAP modules for OpenSER
openvpn-auth-ldap - OpenVPN LDAP authentication module
pdns-backend-ldap - LDAP backend for PowerDNS
perdition-ldap - Library to allow perdition to access LDAP based popmaps
phamm-ldap-amavis - PHP front-end to manage virtual services with LDAP - back-end files
phamm-ldap - PHP front-end to manage virtual services with LDAP - back-end files
phamm-ldap-vacation - PHP front-end to manage virtual services with LDAP - back-end files
phamm - PHP front-end to manage virtual services with LDAP - main package
php5-ldap - LDAP module for php5
php-auth - PHP PEAR modules for creating an authentication system
phpldapadmin - web based interface for administering LDAP servers
php-net-ldap2 - PHP PEAR module for searching and manipulating LDAP-entries
php-net-ldap - a OO interface for searching and manipulating LDAP-entries
postfix-ldap - LDAP map support for Postfix
proftpd-mod-ldap - Versatile, virtual-hosting FTP daemon - LDAP module
pure-ftpd-ldap - Pure-FTPd FTP server with LDAP user authentication
python-authkit - authentication and authorisation framework for Python WSGI applications
python-dhm - collection of Python utilities / helper
python-ldap - LDAP interface module for Python
python-ldaptor - pure-Python library for LDAP operations
python-ldb - Python bindings for LDB
python-repoze.who-plugins - authentication framework for Python WSGI applications - plugins collection
python-smbpasswd - This module can generate both LANMAN and NT password hashes
shellldap - shell-like interface for browsing LDAP servers and editing their content
slapd - OpenLDAP server (slapd)
slpd - OpenSLP Server (slpd)
slptool - SLP command line tool
smbldap-tools - Scripts to manage Unix and Samba accounts stored on LDAP
sudo-ldap - Provide limited super user privileges to specific users
tcllib - the Standard Tcl Library
uif - Advanced iptables-firewall script
wapiti - Web application vulnerability scanner
webcalendar - PHP-Based multi-user calendar
```

Sur une distribution Debian, les paquets à installer sont les suivants : `slapd` et `ldap-utils`.

```
# aptitude install slapd ldap-utils
```

ou

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

Une fenêtre apparaît alors et vous demande le mot de passe associé à l'annuaire que vous mettez en place. **Indiquez « toto » comme pour les tests « habituels » en TP.**

Sur ma configuration, cette commande installe « `unixodbc` » au passage. Vous pouvez installer `gosa` (et `gosa-*`) et/ou `gq` et/ou `ldaptor-*` et/ou `luma` et/ou `phamm` et/ou `phpldapadmin` si vous le souhaitez...

Les fichiers de configuration sont dans le répertoire `/etc/ldap`.

2. Les outils fournis par OpenLDAP

2.1. Les commandes liées au serveur

```
# dpkg -L slapd | grep bin
/usr/sbin
/usr/sbin/slapd
/usr/sbin/slapacl
/usr/sbin/slapadd
/usr/sbin/slapauth
/usr/sbin/slapcat
/usr/sbin/slapdn
/usr/sbin/slapindex
/usr/sbin/slappasswd
/usr/sbin/slaptest
```

Détail des commandes liées au serveur :

Démons :

slapd : le démon OpenLDAP !

slurpd : le démon de réplication

Commandes de manipulation de la base (backend) gérée par OpenLDAP

slapindex : crée les index au sein de la base

slapcat : effectue un dump (une copie intégrale) de la base

slapadd : ajoute des entrées LDIF dans la base

slappasswd : utilitaire de conversion de mots de passe

Commandes de test/validation :

slaptest : teste la validité du fichier de configuration `slapd.conf`

`slapdn` : teste la conformité d'un DN donné en ligne de commande

2.2. Les commandes liées au client

```
# dpkg -L ldap-utils | grep bin
/usr/bin
/usr/bin/ldapdelete
/usr/bin/ldapmodrdn
/usr/bin/ldapsearch
/usr/bin/ldapcompare
/usr/bin/ldapmodify
/usr/bin/ldappasswd
/usr/bin/ldapwhoami
/usr/bin/ldapadd
```

Détail des commandes liées au(x) client(s) :

ldapsearch : effectue une recherche au sein de l'annuaire

ldapadd : ajoute une entrée

ldapdelete : supprime une entrée

ldapmodify : modifie une entrée (ajoute/suppr. un attribut, ajoute/suppr. une entrée, ...)

ldapmodrdn : modifie le rdn d'une entrée (renomme une entrée)

ldappasswd : modifie le mot de passe d'une entrée LDAP

ldapwhoami : affiche avec quel utilisateur le binding a eu lieu

ldapcompare : permet de comparer l'attribut d'une entrée à une valeur spécifiée