Formation
Annuaire OpenLDAP

Version Beta 0.2

Support Instructeur

Eric BERTHOMIER (eric.berthomier@free.fr)
David HOEUNG (uid@free.fr)

17 mars 2005

Table des matières

Chapitre 1

Historique

Version	Date	Mise à jour
Beta 0.2		

Chapitre 2

Introduction à LDAP [2]

Ce cours a été réalisé grâce à l'aimable collaboration de David HOEUNG (david.hoeung@free.fr) alias uid.

2.1 A propos

2.1.1 Mots clés

dn distinguished name (désignation complète et unique du nom)

2.1.2 Références

http://ldap.akbkhome.com LDAP Schema Viewer

2.2 Configuration de la machine

Hostname	debian
Domaine	NA
IP	192.168.2.136

2.3 Installation

L'installation de LDAP se fait par l'intermédiaire de 2 packages et de leur dépendances :

1. slapd
2. ldap-utils

2.4 Configuration de base

Répondez aux questions de la configuration de l'annuaire de la façon suivante :

Entrer le nom de domaine DNS	domaine
Entrer le nom de l'organisation	info
Password de l'admin LDAP	droopy
Autoriser le protocole v2	Oui

2.4.1 Utilisation d'un autre format de base de données (facultatif)

Reconfigurer `slapd` à l'aide de la commande suivante `dpkg-reconfigure slapd`

Passer la configuration de slapd	Non
Entrer le nom de domaine DNS	domaine
Entrer le nom de l'organisation	info
Password de l'admin LDAP	droopy
Format de la base	LDBM
Suppression de la base de données quand slpad est purgé	Non
Déplacer l'ancienne base de données	Non
Autoriser le protocole v2	Oui

Démarrer le serveur : `/etc/init.d/slapd restart`

2.5 Debugging

Il est possible d'augmenter le niveau de debug de l'annuaire en modifiant le fichier `/etc/ldap/slapd.conf` et en renseignant la ligne suivante [1] :

```
loglevel 296
```

Ces informations peuvent être ajoutées dans un fichier séparé en modifiant le fichier `/etc/syslog.conf` par l'ajout de la ligne suivante :

```
local4.debug                    /var/log/slapd.log
```

sans oublier d'envoyer un signal 1 au processus de syslog (`kill -1 ...`).

2.6 Validation des données

Il est possible de visualiser les schémas installés à l'aide de l'utilitaire `vlad`[2], par contre celui-ci nécessite l'utilisation de la version 2 de LDAP donc de l'option `allow bind_v2`.

L'utilisation est simple : `vlad -h hostname -b "dc=..."` ce qui nous donne

```
vlad -h debian -b "dc=domaine"
```

et l'affichage suivant :

```
Vlad 0.02
[-] dc=domaine
 [+] cn=admin

Vlad 0.02
objectClass: top
objectClass: dcObject
objectClass: organization
o: info
dc: domaine

.../...

Attributes of 'dc=domaine'
```

[1] man 5 slapd.conf
[2] vlad.deb

Ou :

```
ldapsearch -x -b dc=domaine
```

2.6.1 Arguments de ldapsearch

-x	sans utiliser SASL
-b	avec la base domaine

2.7 Organisation de l'annuaire

```
    domaine
   /       \
people   groupes
```

2.8 Création de l'annuaire

2.8.1 Caractères accentués

Nos chers caractères accentués ne sont pas du goût de tous et notamment pas de LDAP qui ne les apprécie pas. Pour pouvoir tout de même utiliser ceux-ci, il est nécessaire de faire une petite conversion entre l'ISO-8859-1 (french latin) et l'UTF8 à l'aide de la commande suivante :

```
iconv -f iso-8859-1 -t UTF-8 fichierfrancais.ldif -o fichierfrancaisok.ldif
```

2.8.2 Mise en place des différents éléments

Pour insérer des élements dans un annuaire, il est nécessaire de créer un fichier `ldif` qui nous permettra de saisir toute la structure de l'élément à insérer.

Listing 2.1 – init.ldif

```
1  dn: ou=people,dc=domaine
2  objectClass: top
3  objectClass: organizationalUnit
4  ou: people
5  description: Utilisateurs de la machine
6
7  dn: ou=groupes,dc=domaine
8  objectClass: top
9  objectClass: organizationalUnit
10 ou: groupes
11 description: Groupes des utilisateurs
```

Une fois saisi, insérer l'élément dans l'annuaire à l'aide de la commande suivante :

```
ldapadd -v -x -f init.ldif -W -D "cn=admin,dc=domaine"
```

2.8.3 Arguments de `ldapadd`

-v	mode verbeux
-x	sans utiliser SASL
-f <fichier>	utiliser le fichier <fichier>
-W	demander le mot de passe
-D <dn>	en utilisant le login indiqué par le <dn>

2.8.4 Ajout d'un groupe dans l'annuaire

La gestion des groupes se fait par l'intermédiaire de la classe posixGroup. Le fichier ldif à utiliser est donc le suivant :

Listing 2.2 – groupe.ldif

```
1  dn: cn=mongroupe,ou=groupes,dc=domaine
2  objectClass: top
3  objectClass: posixGroup
4  cn: mongroupe
5  gidNumber: 1001
6  description: Groupe de test
```

Une fois saisi, insérer l'élément dans l'annuaire à l'aide de la commande suivante :

```
ldapadd -v -x -f groupe.ldif -W -D "cn=admin,dc=domaine"
```

2.8.5 Ajout d'un utilisateur

La gestion des utilisateurs se fait par l'intermédiaire de la classe posixAccount.

Listing 2.3 – moi.ldif

```
1  dn: uid=moi,ou=people,dc=domaine
2  objectClass: top
3  objectClass: account
4  objectClass: posixAccount
5  cn: moi
6  uid: moi
7  userPassword: toto
8  uidNumber: 1001
9  gidNumber: 1001
10 gecos: ,,,
11 homeDirectory: /home/moi
12 loginShell: /bin/bash
```

Une fois saisi, insérer l'élément dans l'annuaire à l'aide de la commande suivante :

```
ldapadd -v -x -f moi.ldif -W -D "cn=admin,dc=domaine"
```

2.8.6 Suppression d'un élément en cas d'erreur

En cas d'erreur, la commande :

```
ldapdelete 'distinguished name' -D "cn=admin,dc=domaine" \
                                -w droopy -x -v
```

permettra de détruire l'enregistrement désigné par "distinguished name".

Exemple :

```
ldapdelete 'uid=moi,ou=people,dc=domaine' -D "cn=admin,dc=domaine" -w droopy -x -v
```

2.9 Annexe

2.9.1 Fichier de configuration `/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/inetorgperson.schema
schemacheck     on
pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd.args
loglevel        0
modulepath /usr/lib/ldap
moduleload back_ldbm
backend ldbm
database        ldbm
suffix          "dc=domaine"
directory       "/var/lib/ldap"
index           objectClass eq
lastmod         on
access to attribute=userPassword
        by dn="cn=admin,dc=domaine" write
        by anonymous auth
        by self write
        by * none
access to dn.base="" by * read
access to *
       by dn="cn=admin,dc=domaine" write
       by * read
```

Chapitre 3

Authentification via LDAP[2]

3.1 Prérequis

Ce chapitre fait suite au chapitre Introduction à LDAP (page : 5).

3.1.1 Références

`http://diamond.ugent.be/pam_LDAP/` : Le module PAM ldap

`http://www.formation.jussieu.fr/ars/2002-2003/UNIX/cours/3/book.pdf` : Administration Linux :explication du rôle des modules PAM

`http://www.metaconsultancy.com/whitepapers`

3.1.2 Fichiers

libnss-ldap.conf	Fichier de configuration pour la librairie LDAP au niveau Name Service Switch
pam_ldap.conf	Fichier de configuration du module PAM LDAP.
ldap.secret	Fichier contenant le mot de passe d'administrateur permettant au module PAM d'accéder aux mots de passe enregistrés dans l'annuaire.

3.2 Name Service Switch

3.2.1 Installation

Il est nécessaire d'installer le module LDAP pour NSS (Name Service Switch) :

```
apt-get install libnss-ldap
```

Adresse du serveur LDAP	192.168.2.136
Annuaire	dc=domaine
Version du protocole LDAP	3
Authentification nécessaire à la base	Non
Lisible et modifiable uniquement par le propriétaire	Non

Cette configuration permet d'initialiser le fichier `/etc/libnss-ldap.conf`.

3.2.2 Configuration

Modifier le fichier `/etc/nsswitch.conf` en ajoutant ldap pour la résolution des mots de passe et des groupes.

Avant

```
passwd: compat
group: compat
shadow: compat
```

Après

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

3.2.3 Validation :

Les commandes `getent passwd` et `getent group` doivent faire apparaître l'utilisateur et le groupe LDAP précédemment créé.

```
debian:~# getent passwd moi
moi:x:1001:1001:,,,:/home/moi:/bin/bash

debian:~# getent group mongroupe
mongroupe:x:1001:
```

3.3 Pluggable Authentification Module

3.3.1 Installation

L'authentification sous Linux se fait par le biais de modules PAM (`/etc/pam.d`), il est donc nécessaire d'installer le module associé à LDAP pour que l'authentification puisse se faire par ce biais.

```
apt-get install libpam-ldap
```

Création d'une BD locale pour l'admin	Oui
Authentification nécessaire à la base	Non
Compte privilégié de l'annuaire	cn=admin, dc=domaine
Password	droopy
Chiffrement des password	crypt

Les fichiers ainsi créés sont :
- `/etc/pam_ldap.conf` qui contient la configuration du module pam / LDAP
- `/etc/ldap.secret` qui contient le mot de passe pour modifier l'annuaire LDAP

3.3.2 Configuration

Le module `pam-ldap` recherche un élément dans l'annuaire dont l'attribut `uid` correspond au login. Le module récupère alors les informations du compte.

Authentification (authentication)

Le module d'authentification permet d'authentifier un utilisateur et de définir ses créances. Il faut donc modifier le fichier `/etc/pam.d/common-auth` de la façon suivante :

Avant

```
auth required pam_unix.so nullok_secure
```

Après

```
auth sufficient pam_ldap.so
auth sufficient pam_unix.so nullok_secure use_first_pass
auth required pam_deny.so
```

use_first_pass cette option indique d'utiliser exclusivement le mot de passe entré pour le premier module de la pile du service.

pam_deny renvoie systématiquement un échec, si bien que si on n'a pas obtenu une validation sur un sufficient auparavant, l'authentification est vouée à l'échec.[1]

Gestion des comptes (account management)

Le module de gestion des comptes permet de déterminer si l'utilisateur dispose d'un compte valide (expiration de mot de passe (password aging), restriction d'accès horaire). Il nous faut donc modifier le fichier `/etc/pam.d/common-account` de la façon suivante :

Avant

```
account required pam_unix.so
```

Après

```
account sufficient     pam_ldap.so
account sufficient     pam_unix.so use_first_pass
```

3.4 Création du répertoire personnel (*)

```
mkdir /home/moi
debian:~# chown moi.mongroupe /home/moi
```

L'authentification est maintenant valide.

3.5 Changement de mot de passe

L'authentification est peut être correcte mais il vous sera impossible de changer le mot de passe de l'utilisateur défini dans l'annuaire. Pour celà, il nous faut modifier le fichier `/etc/pam.d/passwd` qui gère les mots de passe.
Ce fichier peut faire référence à un autre fichier : `/etc/pam.d/common-password`.

[1] `http://www.mail-archive.com/confirme@linux-mandrake.com/msg22539.html`

Avant

```
password   required   pam_unix.so nullok obscure min=4 max=8 md5
```

Après

```
password    required      pam_cracklib.so
password    sufficient    pam_ldap.so
password    sufficient    pam_unix.so
password    required      pam_deny.so
```

Note : La ligne `password required pam_cracklib.so` n'existe que dans le cas de l'utilisation du module `cracklib` pour la validation des mots de passe.

Changer le mot de passe de `moi` puis vérifier le changement à l'aide de la commande suivante :

```
vlad -h localhost -b "dc=domaine" -D "cn=admin,dc=domaine" -w droopy
```

A noter ici l'utilisation de l'argument `-w` afin de fournir le mot de passe d'`admin`.

L'authentification est maintenant totalement valide.

3.6 Authentification décentralisée

Le but de cette seconde partie sera de paramétrer une machine de manière à ce que l'identification se fasse au travers de l'annuaire LDAP de la machine "Debian".
Reprendre toutes les sections précédemment décrites sauf celles notées (*) de ce chapitre, le tour est joué.
Enfin, reste encore le souci que les requêtes LDAP passent en clair sur le réseau d'où la nécessité de réaliser les authentifications en mode sécurisé via TLS.

3.7 Annexe

Je vais ici présenter les différents fichiers de configuration utilisés et purgés de tout commentaire.

3.7.1 Fichier `/etc/libnss-ldap.conf`

```
host 192.168.2.137
base dc=domaine
ldap_version 3
```

3.7.2 Fichier `/etc/pam_ldap.conf`

```
host 192.168.2.137
base dc=domaine
ldap_version 3
rootbinddn cn=admin,dc=domaine
pam_password crypt
```

3.7.3 Fichier `/etc/ldap.secret`

```
droopy
```

Chapitre 4

Sécurisation LDAP

4.1 Prérequis

Ce chapitre fait suite aux chapitres LDAP introduction et authentification (page : 10). Il nécessite l'installation du package `openssl` (`apt-get install openssl`).

4.1.1 Fichiers

libnss-ldap.conf	Fichier de configuration pour la librairie LDAP au niveau Name Service Switch
ldap.conf	Fichier de configuration du serveur LDAP

4.2 Résolution de noms

La première chose à faire est d'informer correctement le fichier `/etc/hosts` des deux machines afin que celles-ci se connaissent par leur nom.[1].

Listing 4.1 – /etc/hosts

```
1 debian   192.168.2.136
2 eric     192.168.2.137
```

4.3 Mise en place de TLS [1]

Source : `http://www.supinfo-projects.com/en/2003/sambaldap/10/`

4.3.1 TLS : Pourquoi ?

Vous le savez peut-être, par défaut les communications avec notre serveur LDAP se font en clair. Il suffit de "sniffer" le réseau (non switché) pour s'en rendre compte. Une personne mal intentionnée pourrait donc intercepter toutes les informations qu'elle désire, y compris les mots de passe de nos utilisateurs (même chiffrés, ceux-ci sont précieux... On trouve de nombreux outils pour les "casser"...) ! Une manière simple de sécuriser nos transactions est de passer par TLS (Transport Layer Security, anciennement SSLv3.0, renommé et normalisé par l'IETF, cf. RFC2246), qui assurera le chiffrement des données.

[1] Normalement l'usage du DNS est largement préconisé

Je ne vais pas rentrer dans les détails d'une communication via TLS, ceci dépasserait le cadre du sujet. Sachez simplement que TLS repose sur la couche 4 (Transport) du modèle OSI, ce qui lui permet de sécuriser les communications réseau de manière transparente pour les applications. Il repose sur l'utilisation de clefs symétriques et asymétriques, et introduit la notion de certificat délivré par un tiers, qui assure alors l'authenticité des clefs.

4.3.2 Les clefs et les certificats

Une paire de clefs est composée d'une clef privée et d'une clef publique. Elles ont la particularité d'être inséparables, car ce que chiffre l'une, seule l'autre peut la déchiffrer. Voilà pourquoi on parle de clefs asymétriques. La clef privée est destinée à être gardée précieusement par son propriétaire, alors que la clef publique pourra être diffusée. Le principe général consiste alors à chiffrer les données avec la clef publique du destinataire afin qu'il puisse la déchiffrer avec sa clef privée et être ainsi le seul à pouvoir comprendre le message.

Le certificat vient juste introduire la notion d'authenticité des clefs. Comment être sûr qu'une clef publique est bien celle de la personne à qui l'on veut envoyer des données ? Le certificat nous offre une réponse : une société tierce (de confiance, une autorité de certification : CA) va certifier que la clef publique appartient bien à cette personne. Ainsi, plus de doute, la clef est la bonne... nous évitons ainsi de nous faire piéger par une personne qui voudrait intercepter nos données (le fameux "homme du milieu")...

4.3.3 La pratique

Nous allons implémenter TLS sur notre serveur LDAP maître pour que les communications Système-LDAP soient chiffrées. Cette manoeuvre ajoute juste une commande de type STARTTLS qui permet, si on le désire, de démarrer une transaction sécurisée sur le port standard LDAP. Il restera toujours possible de communiquer "en clair" avec notre serveur. OpenLDAP doit être compilé avec l'option `-with-tls` et OpenSSL doit être installé.

Dans la pratique, la mise en place de TLS se traduit par trois étapes :

- La génération des clefs/certificats côté serveur
- La mise en place de TLS côté serveur
- La mise en place de TLS côté client

4.3.4 Génération des clefs et du certificat

Nous allons dans cette étape préparer notre serveur à l'utilisation de TLS. Il va falloir générer notre paire de clefs et faire signer notre clef publique par une Autorité de Certification.

Dans le répertoire /etc/ldap, créer un répertoire 'cert' qui contiendra les clefs et le certificat et s'y placer :

```
mkdir /etc/ldap/cert cd /etc/ldap/cert
```

Dans ce répertoire, générez la clef privée du serveur :

```
openssl genrsa -out serverkey.pem 1024
```

Puis la clef publique et la demande de certificat (dans `cert.req`) :

```
openssl req -new -key serverkey.pem -out servercert.req
```

```
1 You are about to be asked to enter information that will be incorporated
2 into your certificate request.
3 What you are about to enter is what is called a Distinguished Name or a DN.
4 There are quite a few fields but you can leave some blank
5 For some fields there will be a default value,
```

```
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Bretagne
Locality Name (eg, city) []:Redon
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BI
Organizational Unit Name (eg, section) []:info
Common Name (eg, YOUR name) []:debian
Email Address []:eric@debian

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Complétez correctement les informations qui vous sont demandées. Pensez à bien renseigner le CN (Common Name) par le FQDN (nom dns complet) de votre serveur, celui qui sera utilisé lors de l'interrogation de la base LDAP par les clients. *Ici, nous répondront donc "debian" comme FQDN.*

Pour l'étape suivante, vous avez le choix : soit vous envoyez la demande de certificat à une CA reconnue qui vous enverra le certificat, soit vous certifiez vous-même votre clef en vous faisant passer pour une CA. Nous allons voir comment faire...

Mettons-nous à la place d'une CA. Générez la clef privée de la CA :

```
openssl genrsa -out cakey.pem 1024
```

Puis son certificat propre (qui est alors autocertifié : on ne fait pas appel à une autre CA) :

```
openssl req -new -x509 -key cakey.pem -out cacert.pem -days 365
```

Là encore, complétez correctement les champs demandés. N'oubliez pas que vous êtes la CA...

Enfin, signature par la CA de la clef publique de notre serveur :

```
openssl x509 -req -in servercert.req -out servercert.pem \
 -CA cacert.pem -CAkey cakey.pem -days 365 -CAcreateserial
```

Suppression des fichiers temporaires

```
rm *.req
```

Suppression de la clef privée de la CA

```
rm cakey.pem
```

Réglage des droits

La clef privée ne doit pouvoir être lue que par root :

```
chown root:root serverkey.pem
  chmod 400 serverkey.pem
```

Voilà, vous disposez désormais des fichiers nécessaires pour mettre en place TLS sur le serveur. Nous allons voir les modifications à apporter dans le fichier `slapd.conf`...

4.3.5 Mise en place côté serveur

Sur la machine “debian”, modifier `/etc/ldap/slapd.conf` et ajouter les chemins vers les différentes clefs et le certificat :

```
# TLS
# Chemin vers le certificat du serveur LDAP
TLSCertificateFile      /etc/ldap/cert/servercert.pem
# Chemin vers la clef privée du serveur LDAP
TLSCertificateKeyFile   /etc/ldap/cert/serverkey.pem
# Chemin vers le certificat de la CA
TLSCACertificateFile    /etc/ldap/cert/cacert.pem
```

Attention de bien ajouter ceci dans la section globale.

Si vous redémarrez votre serveur LDAP, il devrait désormais être capable de communiquer avec TLS. Cette communication se fera sur le port 389 (standard, port LDAP) via la commande `starttls` qui activera la transaction sécurisée. Attention, ceci est différent d’une communication "purement" TLS, qui pourrait être mise en place sur le port LDAPS (636) via un tunnel SSL.

4.3.6 Mise en place côté client

Nous allons mettre en place TLS au niveau de la machine “eric”.

Pour autoriser les communications TLS, il faut modifier le fichier ldap.conf. Deux types de directives existent : les directives OpenLDAP pures et les directives ajoutées par `libpam_ldap` et `libnss_ldap`. Elles sont supplémentaires, l’oubli de l’une ou l’autre fera que l’application qui l’utilise ne fonctionnera pas. Ceci peut conduire à des erreurs difficiles à diagnostiquer ! Ajoutez ceci au fichier `ldap.conf` de la machine “eric” :

```
#Directive SSL OpenSSL (pour ldapsearch notamment)
TLS_CACERT /etc/ldap/cert/cacert.pem

#Directives SSL libnss et libpam
# Activation SSL brute (port 636)
# ssl yes
# Acivation SSL via commande starttls (port standard 389)
ssl start_tls
#Verifie certificat serveur
tls_checkpeer yes
# Emplacement certificat CA
tls_cacertfile /etc/ldap/cert/cacert.pem
```

Le fichier ’cacert’ doit être présent sur notre disque. Il s’agit du certificat de la CA. Il convient de le copier au bon endroit (ici `/etc/ldap/cert/`) depuis notre serveur LDAP.

```
mkdir cert
cd cert
scp root@192.168.2.136:/etc/ldap/cert/cacert.pem .
```

4.3.7 Testons notre connexion sécurisée

Testons d’abord, depuis la machine “eric”, installons les outils clients OpenLDAP puis vérifions leur fonctionnent :

```
apt-get install ldap-utils
ldapsearch -b 'dc=domaine' -ZZ -xh debian
```

L'ajout de `-ZZ` force la communication en TLS. Vous devriez voir apparaître l'arborescence que nous avions déjà auparavant. Si vous avez une erreur, vérifiez bien que le nom du serveur utilisé pour la requête est bien le nom passé dans le CN lors de la demande de certificat du serveur !

Testons ensuite la bonne configuration de `libnss-ldap` : exécutons `getent passwd` et voir si nos utilisateurs LDAP sont bien listés...

Si tout cela fonctionne, c'est déjà un bon point, cependant, est-ce bien chiffré ? Pour s'en assurer, nous allons sniffer (écouter) le réseau avec `tcpdump` (nécessite le package `tcpdump`) :

Sur le serveur LDAP, on écoute les connexions provenant de la machine "eric" :

```
tcpdump -s0 -xX
```

Sur le client "eric", on rapatrie les entrées utilisateurs avec :

```
getent passwd
```
ou
```
ldapsearch -b 'dc=domaine' -ZZ -xh debian
```

Le client "eric" va contacter le serveur LDAP pour y lire les informations nécessaires. On voit alors plusieurs segments TCP affichés avec `tcpdump`, mais rien n'est compréhensible... Si l'on réitère l'opération en commentant les lignes concernant la configurationn SSL, on pourra distinguer les informations rapatriées par notre PDC, la preuve que le flux de données est bien chiffré !

4.4 Annexe

4.4.1 Machine serveur (Debian)

Listing 4.2 – /etc/ldap/slapd.conf

```
1  # Allow LDAPv2 binds
2  allow bind_v2
3
4  # This is the main slapd configuration file. See slapd.conf(5) for more
5  # info on the configuration options.
6
7  ########################################################################
8  # Global Directives:
9
10 # Features to permit
11 #allow bind_v2
12
13 # Schema and objectClass definitions
14 include         /etc/ldap/schema/core.schema
15 include         /etc/ldap/schema/cosine.schema
16 include         /etc/ldap/schema/nis.schema
17 include         /etc/ldap/schema/inetorgperson.schema
18
19 # Schema check allows for forcing entries to
20 # match schemas for their objectClasses's
21 schemacheck     on
22
```

```
23 # Where the pid file is put. The init.d script
24 # will not stop the server if you change this.
25 pidfile         /var/run/slapd/slapd.pid
26
27 # List of arguments that were passed to the server
28 argsfile        /var/run/slapd.args
29
30 # Read slapd.conf(5) for possible values
31 loglevel        0
32
33 # TLS
34 # Chemin vers le certificat du serveur LDAP
35 TLSCertificateFile      /etc/ldap/cert/servercert.pem
36 #Chemin vers la écl éprive du serveur LDAP
37 TLSCertificateKeyFile   /etc/ldap/cert/serverkey.pem
38 # Chemin vers le certificat de la CA
39 TLSCACertficateFile     /etc/ldap/cert/cacert.pem
40
41 # Where the dynamically loaded modules are stored
42 modulepath      /usr/lib/ldap
43 moduleload      back_ldbm
44
45 ######################################################################
46 # Specific Backend Directives for ldbm:
47 # Backend specific directives apply to this backend until another
48 # 'backend' directive occurs
49 backend         ldbm
50
51 ######################################################################
52 # Specific Backend Directives for 'other':
53 # Backend specific directives apply to this backend until another
54 # 'backend' directive occurs
55 #backend                <other>
56
57 ######################################################################
58 # Specific Directives for database #1, of type ldbm:
59 # Database specific directives apply to this databasse until another
60 # 'database' directive occurs
61 database        ldbm
62
63 # The base of your directory in database #1
64 suffix          "dc=domaine"
65
66 # Where the database file are physically stored for database #1
67 directory       "/var/lib/ldap"
68
69 # Indexing options for database #1
70 index           objectClass eq
71
72 # Save the time that the entry gets modified, for database #1
73 lastmod         on
74
75 # Where to store the replica logs for database #1
76 # replogfile    /var/lib/ldap/replog
77
```

```
78  # The userPassword by default can be changed
79  # by the entry owning it if they are authenticated.
80  # Others should not be able to see it, except the
81  # admin entry below
82  # These access lines apply to database #1 only
83  access to attribute=userPassword
84          by dn="cn=admin,dc=domaine" write
85          by anonymous auth
86          by self write
87          by * none
88
89  # Ensure read access to the base for things like
90  # supportedSASLMechanisms.  Without this you may
91  # have problems with SASL not knowing what
92  # mechanisms are available and the like.
93  # Note that this is covered by the 'access to *'
94  # ACL below too but if you change that as people
95  # are wont to do you'll still need this if you
96  # want SASL (and possible other things) to work
97  # happily.
98  access to dn.base="" by * read
99
100 # The admin dn has full write access, everyone else
101 # can read everything.
102 access to *
103         by dn="cn=admin,dc=domaine" write
104         by * read
105
106 # For Netscape Roaming support, each user gets a roaming
107 # profile for which they have write access to
108 #access to dn=".*,ou=Roaming,o=morsnet"
109 #         by dn="cn=admin,dc=domaine" write
110 #         by dnattr=owner write
111
112 #######################################################################
113 # Specific Directives for database #2, of type 'other' (can be ldbm too):
114 # Database specific directives apply to this databasse until another
115 # 'database' directive occurs
116 #database        <other>
117
118 # The base of your directory for database #2
119 #suffix          "dc=debian,dc=org"
```


4.4.2 Machine cliente (Eric)

Listing 4.3 – /etc/ldap/lap.conf

```
1  # $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01
2  # kurt Exp $
3  #
4  # LDAP Defaults
5  #
6
7  # See ldap.conf(5) for details
```

```
8  # This file should be world readable but not world writable.
9
10 #Directive SSL OpenSSL (pour ldapsearch notamment)
11 TLS_CACERT /etc/ldap/cert/cacert.pem
12
13 #Directives SSL libnss et libpam
14 # Activation SSL brute (port 636)
15 # ssl yes
16 # Acivation SSL via commande starttls (port standard 389)
17 ssl start_tls
18 #Verifie certificat serveur
19 tls_checkpeer yes
20 # Emplacement certificat CA
21 tls_cacertfile /etc/ldap/cert/cacert.pem
22
23 #BASE    dc=example, dc=com
24 #URI     ldap://ldap.example.com ldap://ldap-master.example.com:666
25
26 #SIZELIMIT      12
27 #TIMELIMIT      15
28 #DEREF          never
```

Chapitre 5

AutoFS

5.1 A propos

5.1.1 Mots clés

5.1.2 Références

5.2 Principe

Le montage du périphérique pointé par un point de montage déclaré par automount se fait lors de l'accès au point de montage.

5.3 Fichiers de configuration

Le paramétrage de l'automount se fait au travers d'un fichier principal de configuration nommé :

`/etc/auto.master`

Un second fichier sera utilisé par celui-ci, il permettra de déclarer ce qui est monté et de définir la "clé" de montage. C'est l'utilisation de cette "clé" qui activera le montage.

5.4 Exemple

Listing 5.1 – /etc/auto.master

```
1 #
2 # $Id: auto.master,v 1.3 2003/09/29 08:22:35 raven Exp $
3 #
4 # Sample auto.master file
5 # This is an automounter map and it has the following format
6 # key [ -mount-options-separated-by-comma ] location
7 # For details of the format look at autofs(5).
```

```
8  #/misc   /etc/auto.misc --timeout=60
9  #/misc   /etc/auto.misc
10 #/net    /etc/auto.net
11
12 /misc            /etc/auto.misc
```

Ici nous définissons un point d'ancrage à nos clés : `/misc`. Un point d'ancrage est un répertoire sur lequel vont se rattacher les différents élements d'automontage.

Dans ce point d'ancrage nous allons définir des clés de montage correspondant chacune à un périphérique ou accès particulier. Le fichier qui contiendra ces informations est indiqué en 2nd argument : `/etc/auto.misc`.

Listing 5.2 – /etc/auto.misc

```
1  #
2  # $Id: auto.misc,v 1.2 2003/09/29 08:22:35 raven Exp $
3  #
4  # This is an automounter map and it has the following format
5  # key [ -mount-options-separated-by-comma ] location
6  # Details may be found in the autofs(5) manpage
7
8  # the following entries are samples to pique your imagination
9  #linux          -ro,soft,intr           ftp.example.org:/pub/linux
10 #boot           -fstype=ext2            :/dev/hda1
11
12 floppy          -fstype=auto            :/dev/fd0
13 linux           -ro,hard,intr           192.168.2.136:/home/moi
14
15 #floppy         -fstype=ext2            :/dev/fd0
16 #e2floppy       -fstype=ext2            :/dev/fd0
17 #jaz            -fstype=ext2            :/dev/sdc1
18 #removable      -fstype=ext2            :/dev/hdd
```

Ici nous décrivons 2 clés, une clé floppy et une clé linux.
L'accès à la clé linux montera le système de fichier nfs /home/moi sur /misc/linux.
L'accès à la clé floppy montera le système de fichier contenu dans /dev/fd0 sur sur /misc/floppy.

En fait, le point d'ancrage est concaténé à la clé pour définir le point de montage.

5.5 Mise en application

L'exécution de la commande :

```
/etc/init.d/autofs reload
```

permet de mettre à jour la table des montages automatiques. Il ne reste plus qu'à accéder au répertoire pour effectuer le montage :

```
cd /misc/linux
ls
cd /misc/floppy
ls
```

5.6 Validation de la non nécessité de l'existence des points de montage

Libérer les répertoires des points de montage en vous déplaçant sur la racine par exemple (`cd /`). Puis exécuter la commande `rm -rf /misc` de manière à invalider tous les points de montage défini par `automount`.

Refaire, les mêmes commandes que précédemment :

```
cd /misc/linux
ls
cd /misc/floppy
ls
```

Tout fonctionne correctement.

Chapitre 6

LDAP avec NFS [2]

6.1 A propos

6.1.1 Mots clés

NFS Network File System (Système de fichier réseau)

6.1.2 Références

6.2 Rappel de la configuration des machines

Type	**Serveur**
Hostname	debian
Domaine	NA
IP	192.168.2.136

Type	**Client**
Hostname	eric
Domaine	NA
IP	192.168.2.137

6.3 Mise en place du serveur NFS

6.3.1 Installation

L'installation en mode serveur NFS se fait à l'aide du package `nfs-kernel-server`.

```
apt-get install nfs-kernel-server
```

Ce package permet notamment l'insertion d'un module lié à `autofs` : `autofs4`.

6.3.2 Répertoire partagé

Dans un premier temps, le répertoire partagé sera `/home/serveur`, ceci afin de différencier les home directory locaux des home directory LDAP/NFS. Plus particulièrement, nous allons créer un home directory pour l'utilisateur précédent `moi`.

```
mkdir -p /home/serveur/moi
chmod 777 /home/serveur/moi
```

De manière à pouvoir effectuer des tests sans problèmes de droits, nous mettons dans l'immédiat un accès complet au répertoire. Nous corrigerons le tir par la suite.

6.3.3 Fichier de configuration : `/etc/exports`

La configuration des répertoires partagés par le serveur NFS est établie à l'aide du fichier `/etc/exports`. La structure utilisée est la suivante :

```
répertoirepartagé machinesautorisées(options)
```

Il est à noter qu'**il ne faut pas de séparateur** entre la définition des machines autorisées et la parenthère des options.
Nous désirons partager le répertoire `/home/serveur` du serveur, nous indiquons donc dans le fichier les éléments suivants :

Listing 6.1 – /etc/exports

```
1 # /etc/exports: the access control list for filesystems which may be exported
2 #               to NFS clients.  See exports(5).
3 /home/serveur    192.168.2.137(rw,sync,root_squash)
```

Les options utilisées sont :

Option	Définition
rw	permission est donnée en lecture ET écriture
root_squash	l'écriture par root du système client est considéré comme une écriture par `nobody`

6.3.4 Mise en route

La mise en fonction de nfs se fait par la traditionnelle commande :

```
/etc/init.d/nfs-kernel-server start
```

6.3.5 Test au niveau client

Nous allons monter le répertoire partagé sur le client de manière à valider le bon fonctionnement de notre partage réseau.

```
mkdir /mnt/testnfs
mount -t nfs 192.168.2.136:/home/serveur/moi /mnt/testnfs/
cp /etc/* /mnt/testnfs/
umount /mnt/testnfs/
```

6.4 Paramétrage LDAP pour NFS

Afin de permettre un montage automatique du répertoire personnel de l'utilisateur, nous aurons besoin de compléter notre schema LDAP en y insérant le schéma suivant :

Listing 6.2 – /etc/ldap/schema/automount.schema

```
# Attribute Type Definitions
attributetype ( 1.3.6.1.1.1.1.25 NAME 'automountInformation'
        DESC 'Information used by the autofs automounter'
        EQUALITY caseExactIA5Match
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE )

# Object Class Definitions

objectclass ( 1.3.6.1.1.1.1.13 NAME 'automount' SUP top STRUCTURAL
        DESC 'An entry in an automounter map'
        MUST ( cn $ automountInformation )
        MAY ( description ) )

objectclass ( 1.3.6.1.4.1.2312.4.2.2 NAME 'automountMap' SUP top STRUCTURAL
        DESC 'An group of related automount objects'
        MUST ( ou ) )
```

Pour insérer le schéma, sur le serveur "debian", créer ce fichier dans le répertoire `/etc/ldap/schema` puis modifier le fichier `/etc/ldap/slapd.conf` en insérant la ligne à la suite des autres `include` :

```
include /etc/ldap/schema/automount.schema
```

Il ne reste plus qu'à redémarrer le serveur LDAP pour prendre en compte les changements :

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

6.5 Complément de la structure d'annuaire

6.5.1 Branche services

Nous allons rajouter une branche "services" à notre annuaire, celle-ci identifiera notamment le service NFS mais peut être d'autre par la suite (d'où la mise en place d'une branche). Cet ajout se fait de la manière habituelle à l'aide du fichier :

Listing 6.3 – service.ldif

```
dn: ou=services,dc=domaine
objectclass: top
objectclass: organizationalUnit
ou: services
description: Services reseaux
```

et de la commande :

```
ldapadd -v -x -f service.ldif -W -D "cn=admin,dc=domaine"
```

6.5.2 Branche nfs

Nous allons rajouter une branche “nfs” dans services. Cet ajout se fait de la manière habituelle à l’aide du fichier :

Listing 6.4 – nfs.ldif

```
1 dn: ou=nfs,ou=services,dc=domaine
2 objectclass: top
3 objectclass: organizationalUnit
4 ou: nfs
5 description: Service NFS
```

et de la commande :

```
ldapadd -v -x -f nfs.ldif -W -D "cn=admin,dc=domaine"
```

6.6 Définition du point de montage dans l’annuaire

Nous allons maintenant définir le point de montage associé à cette entrée NFS. Ceci se fait par l’ajout de l’élément suivant dans l’annuaire :

Listing 6.5 – nfsmoi.ldif

```
1 dn: cn=moi, ou=nfs, ou=services, dc=domaine
2 objectClass: top
3 objectClass: automount
4 cn: moi
5 automountInformation: fstype=nfs,hard,intr,nodev,nosuid,rw \
6                       192.168.2.136:/home/serveur/moi
```

[1] et de la commande :

```
ldapadd -v -x -f nfsmoi.ldif -W -D "cn=admin,dc=domaine"
```

6.7 Configuration client pour l’automontage

Pour se faire, il est nécessaire d’installer le package `autofs` à l’aide de la commande :

```
apt-get install autofs autofs-ldap
```

Puis de renseigner son fichier de configuration :

Listing 6.6 – /etc/auto.master

```
1 #
2 # $Id: auto.master,v 1.3 2003/09/29 08:22:35 raven Exp $
3 #
4 # Sample auto.master file
5 # This is an automounter map and it has the following format
6 # key [ -mount-options-separated-by-comma ] location
7 # For details of the format look at autofs(5).
8 #/misc   /etc/auto.misc --timeout=60
```

[1] **Attention :** je me permets de vous rappeler que la présence d’un \ en fin de ligne signifie que celle-ci se continue normalement sur la ligne suivante.

```
9  #/misc   /etc/auto.misc
10 #/net    /etc/auto.net
11
12 /home/moi        ldap:192.168.2.136:ou=nfs,ou=services,dc=domaine --timeout=1
```

Ce fichier définit les points de montage qui devront être établis de manière automatique lors de la connexion de l'utilisateur moi. Il ne reste plus qu'à mettre à jour l'ensemble de l'automontage à l'aide de la commande suivante :

```
/etc/init.d/autofs reload
```

6.7.1 /etc/ldap/ldap.conf

Un autre fichier intervient dans la configuration de l'automontage : `/etc/ldap/ldap.conf`. Il faut renseigner celui-ci avec les informations concernant notre annuaire :

Listing 6.7 – /etc/ldap/ldap.conf

```
1  # $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.9 2000/09/04 19:57:01 kurt
2   Exp $
3  #
4  # LDAP Defaults
5  #
6
7  # See ldap.conf(5) for details
8  # This file should be world readable but not world writable.
9
10 BASE     dc=domaine
11 URI      ldap://debian
12
13 #SIZELIMIT       12
14 #TIMELIMIT       15
15 #DEREF           never
```

6.8 autofs : ATTENTION !

Les chemins montés par `autofs` ne sont pas forcément accessibles ou visibles par les commandes standards tels que `ls`. **C'est l'accès au répertoire défini dans autofs qui fait que le montage s'établit**. De ce fait, une fois loggé en `moi` il faut exécuter la commande `cd moi` pour visualiser votre accès NFS même si le répertoire n'existe apparament pas.

6.8.1 Validation du montage autofs

```
cd /home/moi/moi
```

6.9 Raffinement

On voit que l'utilisateur `moi` dispose d'un répertoire différent lorsqu'il est connecté à partir du serveur (`/home/moi`) et lorsqu'il est connecté à partir du client (`/home/serveur/moi`). Maintenant que tout est bien câlé dans nos esprit nous pouvons modifier ce comportement de manière à ce qu'il soit identique des deux côtés.

6.9.1 Export

Autoriser l'accès au répertoire en modifiant le fichier `/etc/exports` de la façon suivante :

Listing 6.8 – /etc/exports

```
1 # /etc/exports: the access control list for filesystems which may be exported
2 #               to NFS clients.  See exports(5).
3 /home/          192.168.2.137(rw,root_squash)
```

Enfin, recharger le fichier de configuration précédemment modifié par la commande suivante :

```
/etc/init.d/nfs-kernel-server reload
```

6.9.2 Modification sur l'annuaire LDAP

Pour celà, modifier simplement l'entrée dans l'annuaire LDAP en utilisant le fichier suivant :

Listing 6.9 – nfsmodif.ldif

```
1 dn: cn=moi, ou=nfs, ou=services, dc=domaine
2 changetype: modify
3 delete: automountInformation
4 -
5 add: automountInformation
6 automountInformation: fstype=nfs,hard,intr,nodev,nosuid,rw 192.168.2.136:/home/moi
```

et de la commande :

```
ldapmodify -v -x -f nfsmodif.ldif -W -D "cn=admin,dc=domaine"
```

Ceci nous permet lorsque nous sommes connecté en "moi" sur le serveur d'avoir un Home Directory "correct" i.e. /home/moi. De manière à retrouver nos fichiers, nous transférons les éléments de `/home/serveur/moi` sur `/home/moi` : `mv /home/serveur/moi/* /home/moi`.

6.9.3 Modification du fichier /etc/auto.master

Comme indiqué dans le chapitre `autofs` (section : 5.4 , page : 23), le point de montage créé est réalisé par la concaténation du point d'ancrage et de l'ancre. Nous avons défini l'ancre comme étant le login de l'utilisateur i.e. `moi`. Le point d'ancrage est défini dans le fichier `/etc/auto.master` à la valeur /home/moi. La concaténation du point d'ancrage avec l'ancre nous donne `/home/moi/moi`, nous modifions donc, le point d'ancrage en `/home` ce qui nous permet d'avoir le point de montage suivant : `/home/moi`.

Listing 6.10 – /etc/auto.master

```
1  #
2  # $Id: auto.master,v 1.3 2003/09/29 08:22:35 raven Exp $
3  #
4  # Sample auto.master file
5  # This is an automounter map and it has the following format
6  # key [ -mount-options-separated-by-comma ] location
7  # For details of the format look at autofs(5).
8  #/misc   /etc/auto.misc --timeout=60
9  #/misc   /etc/auto.misc
10 #/net    /etc/auto.net
11
12 /home    ldap:192.168.2.136:ou=nfs,ou=services,dc=domaine
```

6.9.4 Utilisation complète de l'annuaire LDAP pour automount

La modification de `/etc/auto.master` pour chacun des éléments peut devenir rapidement fastidieux, il est possible de définit les éléments de `auto.master` sur l'annuaire LDAP de la façon suivante :

Ajouter l'élément suivant dans l'annuaire LDAP :

Listing 6.11 – nfsmaster.ldif

```
1 dn: ou=auto.master, ou=services, dc=domaine
2 objectclass: automountMap
3 ou: auto.master
4
5 dn: cn=/home,ou=auto.master,ou=services,dc=domaine
6 objectclass: automount
7 automountInformation: ldap:192.168.2.136:ou=nfs,ou=services,dc=domaine
8 cn: /home
```

```
ldapadd -v -x -f nfsmaster.ldif -W -D "cn=admin,dc=domaine"
```

Puis modifier le fichier `/etc/nsswitch.conf` en indiquant :

```
automount: ldap files
```

Enfin, annuler les changements réalisés dans `/etc/auto.master` et redémarrer le service concerné.

Attention

Si l'on indique dans le fichier nsswitch.conf les paramètres suivants pour automount : `automount : ldap files` et que votre configuration est incorrecte au niveau de ldap, le démarrage du service sera arrêté après l'exécution d'autofs-ldap-auto-master qui gère les points de montage via `ldap`.

Annexe A

GNU Free Documentation License

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom : to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation : a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals ; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The **"Document"**, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as **"you"**. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A **"Modified Version"** of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A **"Secondary Section"** is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus,

if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The **"Invariant Sections"** are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The **"Cover Texts"** are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A **"Transparent"** copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called **"Opaque"**.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The **"Title Page"** means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section **"Entitled XYZ"** means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as **"Acknowledgements"**, **"Dedications"**, **"Endorsements"**, or **"History"**.) To **"Preserve the Title"** of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties : any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts : Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version :

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another ; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History" ; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included

in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http ://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM : How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page :

> Copyright ©YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation ; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this :

> with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Listings

Bibliographie

[1] Ganael LAPLANCHE. http ://www.supinfo-projects.com/en/2003/sambaldap/10/.
[2] uid. http ://uid.free.fr/Ldap/ldap.html.

Index