Meta annuaire OpenLDAP et Samba

Ce tutoriel développe la mise en place de quatre annuaires OpenLDAP et trois serveurs Samba.

Le premier annuaire sera Primaire pour le suffixe "dc=alex,dc=fr". Sur cette même machine (pdc.alex.lan) un serveur Samba agira comme contrôleur de domaine principal (PDC). La base "dc=alex,dc=fr" contiendra donc des comptes POSIX/Samba.
Représentation simplifiée de cet annuaire :

```
dc=alex,dc=fr  (Primaire pour ce suffixe)
|
+ou=Computers  (Branche des machines Windows)
| +uid=...
|
+ou=Domains    (Branche des domaines mail)
| +mailDomainName=...
|
+ou=Groups     (Branche des groupes)
| +cn=...
|
+ou=Users      (Branche des utilisateurs)
  +uid=...
```

Le deuxième annuaire sera Secondaire pour le suffixe "dc=alex,dc=fr". Sur cette même machine (bdc.alex.lan) un serveur Samba agira comme contrôleur de domaine secondaire (BDC).

```
dc=alex,dc=fr  (Secondaire pour ce suffixe)
|
+ou=Computers
| +uid=...
|
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...
```

Le troisième annuaire sera Primaire pour les suffixes "dc=alex,dc=com", "dc=alex,dc=org" et Secondaire pour le suffixe "dc=alex,dc=fr". Ces trois bases seront regroupées dans un méta annuaire avec le suffixe "dc=meta".
Pour assurer la disponibilité, deux machines assureront la continuité de service pour ce troisième annuaire (nas1.alex.dmz et nas2.alex.dmz).
Les bases "dc=alex,dc=com" et "dc=alex,dc=org" contiendront des comptes POSIX uniquement.

```
dc=alex,dc=fr  (Secondaire pour ce suffixe)
|
```

```
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...

dc=alex,dc=com  (Primaire pour ce suffixe)
|
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...

dc=alex,dc=org  (Primaire pour ce suffixe)
|
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...
```

Le quatrième annuaire (ldap2.alex.dmz) sera Secondaire pour les suffixes "dc=alex,dc=com", "dc=alex,dc=org" et "dc=alex,dc=fr". Ces trois bases seront aussi regroupées dans un méta annuaire avec le suffixe "dc=meta".

```
dc=alex,dc=fr  (Secondaire pour ce suffixe)
|
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...

dc=alex,dc=com  (Secondaire pour ce suffixe)
|
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...
```

```
dc=alex,dc=org  (Secondaire pour ce suffixe)
|
+ou=Domains
| +mailDomainName=...
|
+ou=Groups
| +cn=...
|
+ou=Users
  +uid=...
```

Pour finir, le troisième serveur Samba agira comme serveur de fichiers et WINS. Il stockera tous les profils Windows itinérants.
Pour assurer la disponibilité, deux machines assureront la continuité de service pour ce troisième serveur Samba (fs1.alex.lan et fs2.alex.lan).

Installation des packages

Note :Laissez les réponses par défaut durant l'installation des packages, sauf pour Postfix.

Sur pdc.alex.lan (serveur OpenLDAP et Samba) :
slapd ldap-utils libnss-ldap openssl samba samba-doc smbldap-tools smbclient postfix mailx

Note : Si Samba crash, un script (panic-action) est exécuté pour envoyer un message d'alerte. C'est pour cela qu'on installe un serveur mail.

Répondre dans l'interface de configuration de Postfix :
- Type de configuration : Système satellite
- Nom de courrier : pdc.alex.lan
- Serveur relais SMTP : smtp.alex.dmz

Sur bdc.alex.lan (serveur OpenLDAP et Samba) :
slapd ldap-utils libnss-ldap samba smbclient postfix mailx

Répondre dans l'interface de configuration de Postfix :
- Type de configuration : Système satellite
- Nom de courrier : bdc.alex.lan
- Serveur relais SMTP : smtp.alex.dmz

Sur fs1.alex.lan et fs2.alex.lan (serveur Samba) :
ldap-utils libnss-ldap samba smbclient postfix mailx

(le serveur fs2.alex.lan sera configuré dans le tutoriel "Redondance et continuité de service")

Répondre dans l'interface de configuration de Postfix :
- Type de configuration : Système satellite
- Nom de courrier : fs1.alex.lan (OU fs2.alex.lan)
- Serveur relais SMTP : smtp.alex.dmz

Sur nas1.alex.dmz et nas2.alex.dmz (serveur OpenLDAP) :
slapd ldap-utils

(le serveur nas2.alex.dmz sera configuré dans le tutoriel "Redondance et continuité de service".)

Sur ldap2.alex.dmz (serveur OpenLDAP) :
slapd ldap-utils

Configuration d'OpenLDAP sur pdc.alex.lan

Modifiez le fichier /etc/resolv.conf :

```
search alex.lan sr1.alex.lan alex.dmz
nameserver 172.17.0.1
nameserver 172.16.0.1
```

Modifiez le fichier /etc/network/interfaces :

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

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 172.17.0.3
netmask 255.255.0.0
gateway 172.17.0.254
up route add -net 172.18.0.0/16 gw 172.17.0.253
```

Pour que Samba puisse écrire ses attributs dans l'annuaire LDAP, vous devez inclure son fichier de schéma :

```
pdc:~# cp /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
/etc/ldap/schema/
pdc:~# gunzip -d /etc/ldap/schema/samba.schema.gz
```

Ce fichier de schéma est dépendant de la version de Samba, pour cette raison je préfère le renommer :

```
pdc:~# dpkg -l samba | grep samba
ii  samba     3.0.24-6etch4    a LanManager-like file and printer server
for Unix
pdc:~#

pdc:~# mv /etc/ldap/schema/samba.schema
/etc/ldap/schema/samba-3.0.24.schema
```

Pour renforcer la sécurité entre les échanges d'informations LDAP, nous allons utiliser ldaps (ldap over TLS/SSL).
Il faut générer un certificat et une clef pour chaque serveurs, nous allons utiliser un fichier de configuration Openssl adapté pour générer tous ces fichiers depuis le serveur pdc.alex.lan

Créez le répertoire /etc/ldap/tls/ puis le fichier /etc/ldap/tls/openssl-ldap.cnf :

```
[ req ]

default_bits = 2048
default_keyfile = server_key.pem
default_md = sha1
distinguished_name = req_distinguished_name
x509_extensions = server_cert
string_mask = nombstr

[ req_distinguished_name ]

countryName = (C) Pays (code à 2 lettres)
countryName_default = FR
countryName_min = 2
countryName_max = 2

stateOrProvinceName = (ST) Etat, region ou departement
stateOrProvinceName_default = Haute-Savoie

localityName = (L) Ville
localityName_default = Alex

0.organizationName = (O) Organisation
0.organizationName_default = Alex

organizationalUnitName = (OU) Unite organisationnelle
#organizationalUnitName_default =

commonName = (CN) FQDN du serveur
commonName_max = 64

emailAddress = (E) Adresse mail
emailAddress_max = 64

[ server_cert ]

basicConstraints = critical, CA:FALSE
subjectKeyIdentifier = hash
keyUsage = digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth, clientAuth
nsCertType = server
nsComment = "Certificat Serveur OpenLDAP"
```

Certificat et clef pour pdc.alex.lan :

```
pdc:~# cd /etc/ldap/tls/
```

```
pdc:/etc/ldap/tls# openssl req -x509 -new -config openssl-ldap.cnf -out
ldap_pdc_cert.pem -keyout ldap_pdc_key.pem -days 730 -nodes

Generating a 2048 bit RSA private key
..................+++
.....................................+++
writing new private key to 'ldap_pdc_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
(C) Pays (code à 2 lettres) [FR]:
(ST) Etat, region ou departement [Haute-Savoie]:
(L) Ville [Alex]:
(O) Organisation [Alex]:
(OU) Unite organisationnelle []:
(CN) FQDN du serveur []:pdc.alex.lan
(E) Adresse mail []:root@alex.fr
pdc:/etc/ldap/tls#

pdc:/etc/ldap/tls# ls -1
ldap_pdc_cert.pem
ldap_pdc_key.pem
openssl-ldap.cnf
pdc:/etc/ldap/tls#
```

Mettez bien le FQDN de vos serveurs sinon le certificat ne sera pas valide !

Certificat et clef pour bdc.alex.lan :

```
pdc:/etc/ldap/tls# openssl req -x509 -new -config openssl-ldap.cnf -out
ldap_bdc_cert.pem -keyout ldap_bdc_key.pem -days 730 -nodes

Generating a 2048 bit RSA private key
..................+++
.....................................+++
writing new private key to 'ldap_bdc_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
(C) Pays (code à 2 lettres) [FR]:
(ST) Etat, region ou departement [Haute-Savoie]:
(L) Ville [Alex]:
(O) Organisation [Alex]:
```

```
(OU) Unite organisationnelle []:
(CN) FQDN du serveur []:bdc.alex.lan
(E) Adresse mail []:root@alex.fr
pdc:/etc/ldap/tls#
```

Certificat et clef pour ldap2.alex.dmz :

```
pdc:/etc/ldap/tls# openssl req -x509 -new -config openssl-ldap.cnf -out
ldap_ldap2_cert.pem -keyout ldap_ldap2_key.pem -days 730 -nodes

Generating a 2048 bit RSA private key
.................+++
.....................................+++
writing new private key to 'ldap_ldap2_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
(C) Pays (code à 2 lettres) [FR]:
(ST) Etat, region ou departement [Haute-Savoie]:
(L) Ville [Alex]:
(O) Organisation [Alex]:
(OU) Unite organisationnelle []:
(CN) FQDN du serveur []:ldap2.alex.dmz
(E) Adresse mail []:root@alex.fr
pdc:/etc/ldap/tls#
```

Les serveurs nas1.alex.dmz et nas2.alex.dmz auront un alias IP puisqu'ils assureront la continuité de service pour l'annuaire OpenLDAP. Cet alias IP portera les noms DNS ldap1.alex.dmz et nas.alex.dmz
Comme la transaction TLS/SSL vérifie le FQDN du serveur contenu dans le certificat, il faut ajouter une option au fichier de configuration Openssl.

Modifiez le fichier /etc/ldap/tls/openssl-ldap.cnf en ajoutant cette ligne tout en bas :

```
...
nsCertType = server
nsComment = "Certificat Serveur OpenLDAP"
subjectAltName = DNS:nas.alex.dmz,DNS:nas1.alex.dmz,DNS:nas2.alex.dmz
```

Certificat et clef pour ldap1.alex.dmz :

```
pdc:/etc/ldap/tls# openssl req -x509 -new -config openssl-ldap.cnf -out
ldap_ldap1_cert.pem -keyout ldap_ldap1_key.pem -days 730 -nodes
Generating a 2048 bit RSA private key
.................+++
.....................................+++
```

```
writing new private key to 'ldap_ldap1_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
(C) Pays (code à 2 lettres) [FR]:
(ST) Etat, region ou departement [Haute-Savoie]:
(L) Ville [Alex]:
(O) Organisation [Alex]:
(OU) Unite organisationnelle []:
(CN) FQDN du serveur []:ldap1.alex.dmz
(E) Adresse mail []:root@alex.fr
pdc:/etc/ldap/tls#
```

Si vous voulez visualiser un certificat :

```
pdc:/etc/ldap/tls# openssl x509 -in ldap_ldap1_cert.pem -text -noout

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fd:56:b3:18:79:3a:08:71
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=FR, ST=Haute-Savoie, L=Alex, O=Alex, CN=ldap1.alex.dmz/
emailAddress=root@alex.fr
        Validity
            Not Before: Jul 18 06:50:25 2007 GMT
            Not After : Jul 17 06:50:25 2009 GMT
        Subject: C=FR, ST=Haute-Savoie, L=Alex, O=Alex,
CN=ldap1.alex.dmz/emailAddress=root@alex.fr
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:b5:c7:ca:bc:4c:31:06:bc:e8:9c:63:df:31:30:
                    d7:f0:bc:0d:9d:b4:0b:5e:c2:e5:7e:21:35:88:0d:
                    e7:7d:54:32:d0:83:12:f4:38:08:80:9c:2e:69:de:
                    f2:cb:1f:30:ba:30:5f:98:82:e5:50:41:06:b8:65:
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                61:35:F3:D8:EA:51:3E:A7:6E:8B:94:73:38:AA:F1:AD:34:D2:CA
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client
Authentication
            Netscape Cert Type:
```

```
                SSL Server
            Netscape Comment:
                Certificat Serveur OpenLDAP
            X509v3 Subject Alternative Name:
                DNS:nas.alex.dmz, DNS:nas1.alex.dmz, DNS:nas2.alex.dmz
    Signature Algorithm: sha1WithRSAEncryption
        65:c2:5d:f9:66:45:0d:9d:ba:f2:f7:9b:f9:2f:4e:a5:a8:43:
        64:05:7e:f3:59:66:98:5d:76:63:1e:7b:93:bc:0c:38:95:25:
        0b:be:39:47:fa:9b:bd:01:1b:c1:cb:01:47:98:36:be:5a:0b:
        fc:f7:a2:44:a1:7c:9a:1d:f1:92:4f:64:74:4b:17:f2:2e:c4:

pdc:/etc/ldap/tls#
```

Il faut changer les droits sur les clefs :

```
pdc:/etc/ldap/tls# chmod 400 ldap_*_key.pem
pdc:/etc/ldap/tls# chown openldap: /etc/ldap/tls/*.pem
```

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

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
#allow bind_v2

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
# Pour qu'OpenLDAP connaisse les attributs de Samba
include         /etc/ldap/schema/samba-3.0.24.schema
# Ce schéma contient des attributs et classes pour nos comptes mail.
# Il sera nécessaire quand nous traiteront du tutoriel Postfix.
# Téléchargez-le et copiez-le dans ce répertoire.
include      /etc/ldap/schema/mail.schema
# Ce schéma contient des attributs et classes pour contrôler l'accès au
# Proxy et au serveur FTP de notre entreprise.
# Téléchargez-le et copiez-le dans ce répertoire.
include      /etc/ldap/schema/proxy-ftp.schema

# Déclaration du certificat et de la clef pour les connexions ldaps.
TLSCertificateFile    /etc/ldap/tls/ldap_pdc_cert.pem
TLSCertificateKeyFile /etc/ldap/tls/ldap_pdc_key.pem
# Si vous souhaitez qu'OpenLDAP vérifie si les clients
# possèdent bien un certificat valide :
#TLSVerifyClient demand # ([never]|allow|try|demand)

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
```

```
pidfile         /var/run/slapd/slapd.pid

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

# Mettez à 256 pour vos tests, puis à zéro quand tout fonctionne.
# Read slapd.conf(5) for possible values
#loglevel       0
loglevel        256

# Where the dynamically loaded modules are stored
modulepath      /usr/lib/ldap
moduleload      back_bdb
# On charge le module de replication Syncrepl.
moduleload      syncprov

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

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

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

########################################################################
# Specific Backend Directives for 'other':
# Backend specific directives apply to this backend until another
# 'backend' directive occurs
#backend        <other>


# Configuration de la base OpenLDAP portant le suffixe dc=alex,dc=fr
#
########################################################################
# Specific Directives for database #1, of type bdb:
# Database specific directives apply to this databasse until another
# 'database' directive occurs
database        bdb

# The base of your directory in database #1
# Définition de la racine pour cette base.
suffix          "dc=alex,dc=fr"

# rootdn directive for specifying a superuser on the database.
# This is needed for syncrepl.
# Définition du compte administrateur qui aura tous les droits sur
# cette base. Ce compte n'est pas présent dans l'annuaire, il est
# uniquement déclaré dans ce fichier.
rootdn          "cn=Manager,dc=alex,dc=fr"
```

```
# Le mot de passe pour cette base est « mypassword »
# Pour le crypter utilisez cette commande :
# pdc:~# slappasswd -h {SSHA} -s mypassword
#
rootpw        {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Where the database file are physically stored for database #1
# Répertoire où sera stockée cette base.
directory     "/var/lib/ldap"

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

# Sven Hartge reported that he had to set this value incredibly high
# to get slapd running at all. See http://bugs.debian.org/303057
# for more information.

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

# Indexing options for database #1
# Liste des attributs à indexer pour une recherche plus rapide.
#
# Le mécanisme de synchronisation Syncrepl s'appuit sur l'attribut
# contextCSN (créé grâce aux attributs entryCSN et entryUUID).
# contextCSN est mis à jour pour chaque opération d'écriture dans la
# base, il permet de minimiser le temps de rétablissement après un arrêt
# brutal (comme un journal pour un système de fichier).
# Nous devons donc indexer les attributs entryCSN et entryUUID.
index         objectClass,entryCSN,entryUUID                  eq
# Les attributs uidNumber,gidNumber,memberUid sont à indexer pour
# une authentification POSIX.
index         uidNumber,gidNumber,memberUid                   eq
# Attributs dépendant de la version de samba.schema
index         sambaSID,sambaPrimaryGroupSID,sambaDomainName eq
# uid et displayName sont utilisés par Samba pour sa recherche du RID.
index         cn,sn,uid,displayName                           pres,sub,eq
index         default                                         sub

# Inclusion d'un fichier slapd.access contenant les ACLs
# (qui peut lire ou écrire dans cette base de l'annuaire).
include       /etc/ldap/slapd.access_pdc.conf

# Timeout de connexion maximum d'un client LDAP en secondes.
idletimeout   1800

# Save the time that the entry gets modified, for database #1
# Activez-le pour la réplication avec Syncrepl.
lastmod       on

# Réplication avec Syncrepl (slurpd n'étant pas fiable, il a été supprimé
# d'OpenLdap depuis la version 2.4)
overlay       syncprov
```

```
# Le contextCSN est écrit toutes les 100 opérations d'écriture ou toutes
# les 10 minutes.
syncprov-checkpoint 100 10
# Les logs de session gardent en mémoire presque toutes les opérations
# d'écriture sur la base, cela permet d'interroger les logs plutôt que de
# faire des requêtes sur la base. Jusqu'à 100 opérations sont
# enregistrées dans cette exemple.
syncprov-sessionlog 100
```

Créez le fichier /etc/ldap/slapd.access_pdc.conf :

```
# ACLs PDC POSIX/SAMBA
# Respectez les tabulations, elles font parties de la syntaxe !
#
# access to <what>
#   [by <who> <access> [ <control> ] ]+
#
# <what>    : [ [*] [dn[.<dnstyle>]=<pattern>] [attrs=<attrlist>] ]
# <who>     : [ [*] [anonymous] [users] [self] [dn[.<dnstyle>]=<pattern>]
[group[.<style>]=<pattern>] [peername[.<style>]=<pattern>] ]
# <access>  : [ [none] [auth] [compare] [search] [read] [write] ]
# <control> : [ [stop] [continue] [break] ]
#
# L'ordre des ACLs est important, elles sont appliquées de haut en bas.
# Par défaut la clause <control> est sur [stop], ce qui veut dire
# qu'une ACL amont et prioritaire sur une ACL aval.
# Faites des tests pour vérifier ces priorités.


# Protection des mots de passe et informations Samba dans toute la base
# depuis le suffix "dc=alex,dc=fr".
#
# access to attrs=...        : accès aux attributs.
# by self                    : pour le propriétaire.
# by dn="..."                : pour l'identifiant unique "DN".
# by tls_ssf=256 ssf=256 ... : avec des facteurs de sécurité (demande
l'accès par TLS/SSL)
# by group="..."             : pour le groupe.
# by anonymous               : pour les utilisateurs non identifiés.
# by *                       : pour tout le monde.
# Avec les droits read ou write ou auth ou none ou ...
access to
attrs=userPassword,shadowLastChange,sambaLMPassword,sambaNTPassword,
sambaPwdLastSet,sambaPwdMustChange,sambaPasswordHistory
    by self write
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" read
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by anonymous auth
    by * none

# ACL permettant au compte ldapadmin et au groupe
# Domain Admins d'ajouter des utilisateurs dans cette branche.
#
# access to dn.subtree="..."  : accès à la branche elle même et
```

```
récursivement à tout son contenu.
# access to dn.children="..." : accès à ce qui se trouve récursivement
au-dessous de la branche, mais pas à la branche elle même.
# access to dn.one="..."      : accès à ce qui se trouve au-dessous de la
branche, mais pas à la branche elle même.
# access to dn="..."          : accès uniquement à la branche, mais pas à
ce qu'elle contient.
# access to dn.base="..."     : synonyme de access to dn="...".
# access to dn.exact="..."    : synonyme de access to dn="...".
access to dn.subtree="ou=Users,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by users read
    by anonymous read

# ACL permettant au compte ldapadmin et au groupe
# Domain Admins d'ajouter des groupes dans cette branche.
access to dn.subtree="ou=Groups,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by users read
    by anonymous read

# ACL permettant au compte ldapadmin et au groupe
# Domain Admins d'ajouter des machines dans cette branche.
# A l'adresse IP 127.0.0.1 de lire dans cette branche.
access to dn.subtree="ou=Computers,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" read
    by peername.ip=127.0.0.1 read

# ACL permettant aux utilisateurs et au compte ldapadmin de modifier
# leurs attributs mail et telephoneNumber.
access to dn.subtree="ou=Users,dc=alex,dc=fr" attrs=mail,telephoneNumber
    by self write
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by anonymous read

# ACL permettant au compte ldapadmin et au groupe Domain Admins de
# modifier les attributs pour le DN sambaDomainName=ALEX,dc=alex,dc=fr.
access to dn="sambaDomainName=ALEX,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" read
    by * none

# ACL permettant au compte ldapadmin et au groupe Domain Admins de
# modifier les attributs pour le DN cn=NextFreeUnixId,dc=alex,dc=fr.
access to dn="cn=NextFreeUnixId,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" read
    by * none
```

```
# La racine DIT doit être accessible pour tous les clients.
access to *
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" write
    by * read
```

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

```
# Indiquez le certificat ou le répertoire qui contient tous vos
certificats.
#TLS_CACERT /etc/ldap/tls/ldap_cert.pem
TLS_CACERTDIR /etc/ldap/tls

# Pour demander la validité du certificat : s'il n'y en à pas ou
# s'il est mauvais, la session continuera quand même.
TLS_REQCERT allow
#TLS_REQCERT ([demand],never,allow,try)
# Pour demander absolument la validité du certificat.
#TLS_REQCERT demand

# La racine de votre annuaire.
BASE dc=alex,dc=fr
# L'adresse FQDN de vos (ou votre) serveurs OpenLDAP.
URI ldap://127.0.0.1 ldaps://bdc.alex.lan
```

Modifiez le fichier /etc/default/slapd :

```
# Default location of the slapd.conf file
SLAPD_CONF=

# System account to run the slapd server under. If empty the server
# will run as root.
SLAPD_USER="openldap"

# System group to run the slapd server under. If empty the server will
# run in the primary group of its user.
SLAPD_GROUP="openldap"

# Path to the pid file of the slapd server. If not set the init.d script
# will try to figure it out from $SLAPD_CONF (/etc/ldap/slapd.conf)
SLAPD_PIDFILE=

# Configure if the slurpd daemon should be started. Possible values:
# - yes:   Always start slurpd
# - no:    Never start slurpd
# - auto:  Start slurpd if a replica option is found in slapd.conf
(default)
SLURPD_START=auto

# slapd normally serves ldap only on all TCP-ports 389. slapd can also
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
```

```
# Pour que le service écoute sur la boucle locale et sur son IP en ldaps.
SLAPD_SERVICES="ldap://127.0.0.1:389 ldaps://172.17.0.3:636"

# Additional options to pass to slapd and slurpd
SLAPD_OPTIONS=""
SLURPD_OPTIONS=""
```

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

```
# the configuration of this file will be done by debconf as long as the
# first line of the file says '###DEBCONF###'

# Le suffixe de la base.
base dc=alex,dc=fr

# Indiquez l'adresse FQDN de vos serveurs LDAP.
uri ldap://127.0.0.1/ ldaps://bdc.alex.lan/

# La version du protocole LDAP à utiliser.
ldap_version 3

# La méthode de recherche dans l'annuaire, ici non récursive.
#scope sub
scope one
#scope base

# Search timelimit
timelimit 30

# Bind/connect timelimit
bind_timelimit 30

# Ne retente pas la connexion plusieurs fois si l'annuaire ne répond pas.
# Pour gagner du temps au démarrage de la machine.
bind_policy soft

# Filter to AND with uid=%s
#pam_filter objectclass=account
pam_filter objectclass=posixaccount

# The user ID attribute (defaults to uid)
pam_login_attribute uid

# RFC2307bis naming contexts
# Syntax:
# nss_base_XXX      base?scope?filter
# where scope is {base,one,sub}
# and filter is a filter to be &'d with the
# default filter.
# You can omit the suffix eg:
# nss_base_passwd   ou=People,
# to append the default base DN but this
# may incur a small performance impact.
# Indiquez les chemins à consulter dans l'annuaire.
nss_base_passwd      ou=Users,dc=alex,dc=fr?one
nss_base_passwd      ou=Computers,dc=alex,dc=fr?one
```

```
# Nous n'avons pas besoin de l'option nss_base_shadow car nous utilisons
# libnss-ldap pour récupérer les uid/gid.
#nss_base_shadow     ou=People,dc=padl,dc=com?one
nss_base_group        ou=Groups,dc=alex,dc=fr?one
```

Modifiez le fichier /etc/nsswitch.conf :

```
passwd:     compat ldap
group:      compat ldap
# Pas de shadow ldap non plus.
shadow:     compat

hosts:      files dns
networks:   files

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

netgroup:   nis
```

Stoppez le service :

```
pdc:~# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
```

Effacez la base existante :

```
pdc:~# rm -r /var/lib/ldap/*
```

Démarrez le service :

```
pdc:~# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
```

Configuration de smbldap-tools

Nous allons utiliser les scripts smbldap-tools pour écrire dans l'annuaire. Il faut d'abord configurer deux fichiers.
Copiez ces fichiers et changez les droits :

```
pdc:~# cp /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz
/etc/smbldap-tools/
pdc:~# cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf
/etc/smbldap-tools/
pdc:~# gunzip -d /etc/smbldap-tools/smbldap.conf.gz
```

```
pdc:~# chown -R root:openldap /etc/smbldap-tools
pdc:~# chmod -R 740 /etc/smbldap-tools
```

Nous allons récupérer le SID de Samba à partir des configurations générées par défaut lors de l'installation des packages :

```
pdc:~# /etc/init.d/samba stop
Stopping Samba daemons: nmbd smbd.

pdc:~# net getlocalsid
SID for domain PDC is: S-1-5-21-663340348-4107433757-3291108422
```

Modifiez le fichier /etc/smbldap-tools/smbldap.conf :

```
# $Source: /opt/cvs/samba/smbldap-tools/smbldap.conf,v $
# $Id: smbldap.conf,v 1.18 2005/05/27 14:28:47 jtournier Exp $

##############################################################################
#
# General Configuration
#
##############################################################################

# Put your own SID. To obtain this number do: "net getlocalsid".
# If not defined, parameter is taking from "net getlocalsid" return
SID="S-1-5-21-663340348-4107433757-3291108422"

# Domain name the Samba server is in charged.
# If not defined, parameter is taking from smb.conf configuration file
# Ex: sambaDomain="IDEALX-NT"
# Votre nom de domaine Windows.
sambaDomain="ALEX"

##############################################################################
#
# LDAP Configuration
#
##############################################################################

# Notes: to use to dual ldap servers backend for Samba, you must patch
# Samba with the dual-head patch from IDEALX. If not using this patch
# just use the same server for slaveLDAP and masterLDAP.
# Those two servers declarations can also be used when you have
# . one master LDAP server where all writing operations must be done
# . one slave LDAP server where all reading operations must be done
#   (typically a replication directory)

# Slave LDAP server
# Ex: slaveLDAP=127.0.0.1
# If not defined, parameter is set to "127.0.0.1"
slaveLDAP="127.0.0.1"

# Slave LDAP port
```

```
# If not defined, parameter is set to "389"
slavePort="389"

# Master LDAP server: needed for write operations
# Ex: masterLDAP=127.0.0.1
# If not defined, parameter is set to "127.0.0.1"
masterLDAP="127.0.0.1"

# Master LDAP port
# If not defined, parameter is set to "389"
masterPort="389"

# Use TLS for LDAP
# If set to 1, this option will use start_tls for connection
# (you should also used the port 389)
# If not defined, parameter is set to "0"
ldapTLS="0"

# How to verify the server's certificate (none, optional or require)
# see "man Net::LDAP" in start_tls section for more details
verify="require"

# CA certificate
# see "man Net::LDAP" in start_tls section for more details
cafile="/etc/opt/IDEALX/smbldap-tools/ca.pem"

# certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientcert="/etc/opt/IDEALX/smbldap-tools/smbldap-tools.pem"

# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientkey="/etc/opt/IDEALX/smbldap-tools/smbldap-tools.key"

# LDAP Suffix
# Ex: suffix=dc=IDEALX,dc=ORG
suffix="dc=alex,dc=fr"

# Where are stored Users
# Ex: usersdn="ou=Users,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for
usersdn
usersdn="ou=Users,${suffix}"

# Where are stored Computers
# Ex: computersdn="ou=Computers,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for
computersdn
computersdn="ou=Computers,${suffix}"

# Where are stored Groups
# Ex: groupsdn="ou=Groups,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for
groupsdn
groupsdn="ou=Groups,${suffix}"

# Nous n'utilisons pas la branche Idmap.
# Where are stored Idmap entries (used if samba is a domain member
```

```
server)
# Ex: groupsdn="ou=Idmap,dc=IDEALX,dc=ORG"
# Warning: if 'suffix' is not set here, you must set the full dn for
idmapdn
#idmapdn="ou=Idmap,${suffix}"
idmapdn=""

# Where to store next uidNumber and gidNumber available for new users and
groups
# If not defined, entries are stored in sambaDomainName object.
# Ex: sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
# Ex: sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"
sambaUnixIdPooldn="cn=NextFreeUnixId,${suffix}"

# Default scope Used
scope="sub"

# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT)
hash_encrypt="SSHA"

# if hash_encrypt is set to CRYPT, you may set a salt format.
# default is "%s", but many systems will generate MD5 hashed
# passwords if you use "$1$%.8s". This parameter is optional!
crypt_salt_format="%s"

##############################################################################
#
# Unix Accounts Configuration
#
##############################################################################

# Login defs
# Default Login Shell
# Ex: userLoginShell="/bin/bash"
userLoginShell="/bin/bash"

# Home directory
# Ex: userHome="/home/%U"
userHome="/home/%U"

# Default mode used for user homeDirectory
userHomeDirectoryMode="700"

# Gecos
userGecos="System User"

# Default User (POSIX and Samba) GID
defaultUserGid="513"

# Default Computer (Samba) GID
defaultComputerGid="515"

# Skel dir
skeletonDir="/etc/skel"

# Default password validation time (time in days) Comment the next line
if
# you don't want password to be enable for defaultMaxPasswordAge days (be
```

```
# careful to the sambaPwdMustChange attribute's value)
defaultMaxPasswordAge="90"

##############################################################################
#
# SAMBA Configuration
#
##############################################################################

# The UNC path to home drives location (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon
home'
# directive and/or disable roaming profiles
# Ex: userSmbHome="\\PDC-SMB3\%U"
#userSmbHome="\\PDC-SMB3\%U"
# Les profils itinérants seront stockés sur le serveur Samba FS (nom
NetBIOS)
userSmbHome="\\FS\homes"

# The UNC path to profiles locations (%U username substitution)
# Just set it to a null string if you want to use the smb.conf 'logon
path'
# directive and/or disable roaming profiles
# Ex: userProfile="\\PDC-SMB3\profiles\%U"
#userProfile="\\PDC-SMB3\profiles\%U"
# Nous utiliserons l'option "logon path" dans le
# fichier /etc/samba/smb.conf
userProfile=""

# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: userHomeDrive="H:"
userHomeDrive="H:"

# The default user netlogon script name (%U username substitution)
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
# Ex: userScript="startup.cmd"
# make sure script file is edited under dos
userScript="logon.bat"

# Domain appended to the users "mail"-attribute
# when smbldap-useradd -M is used
# Ex: mailDomain="idealx.com"
mailDomain="alex.fr"

##############################################################################
#
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#
##############################################################################

# Allows not to use smbpasswd (if with_smbpasswd == 0 in smbldap_conf.pm)
but
# prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
```

```
# Allows not to use slappasswd (if with_slappasswd == 0 in
smbldap_conf.pm)
# but prefer Crypt:: libraries
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"

# comment out the following line to get rid of the default banner
# no_banner="1"
```

Modifiez le fichier /etc/smbldap-tools/smbldap_bind.conf :

```
##############################
# Credential Configuration #
##############################
# Notes: you can specify two differents configuration if you use a
# master ldap for writing access and a slave ldap server for reading
access
# By default, we will use the same DN (so it will work for standard Samba
# release)
slaveDN="none"
slavePw="none"
# Indiquez le compte administrateur de l'annuaire (tous les pouvoirs)
masterDN="cn=Manager,dc=alex,dc=fr"
masterPw="mypassword"
```

Nous pouvons maintenant utiliser les scripts smbldap-tools, pour écrire les informations et comptes de base dans l'annuaire avec la commande smbldap-populate :

```
pdc:~# smbldap-populate -?
(c) Jerome Tournier - IDEALX 2004 (http://www.idealx.com)- Licensed under
the GPL
Usage: /usr/sbin/smbldap-populate [-abeiklug?] [ldif]
  -u uidNumber first uidNumber to allocate (default: 1000)
  -g gidNumber first uidNumber to allocate (default: 1000)
  -a user      administrator login name (default: root)
  -b user      guest login name (default: nobody)
  -k uidNumber administrator's uidNumber (default: 0)
  -l uidNumber guest's uidNumber (default: 999)
  -m gidNumber administrator's gidNumber (default: 0)
  -e file      export ldif file
  -i file      import ldif file
  -?           show this help message
pdc:~#
```

Je choisi à partir de quel nombre va commencer le uid/gid des comptes dans l'annuaire, le nom du compte administrateur du domaine Windows avec son uid/gid, ainsi que le nom du compte invité avec son uid :

```
pdc:~# smbldap-populate -u 2000 -g 2000 -a administrateur -k 9999 -m 9999
-b nobody -l 65534

Populating LDAP directory for domain ALEX
```

```
(S-1-5-21-663340348-4107433757-3291108422)
(using builtin directory structure)

adding new entry: dc=alex,dc=fr
adding new entry: ou=Users,dc=alex,dc=fr
adding new entry: ou=Groups,dc=alex,dc=fr
adding new entry: ou=Computers,dc=alex,dc=fr
adding new entry: uid=administrateur,ou=Users,dc=alex,dc=fr
adding new entry: uid=nobody,ou=Users,dc=alex,dc=fr
adding new entry: cn=Domain Admins,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Domain Users,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Domain Guests,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Domain Computers,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Administrators,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Account Operators,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Print Operators,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Backup Operators,ou=Groups,dc=alex,dc=fr
adding new entry: cn=Replicators,ou=Groups,dc=alex,dc=fr
adding new entry: cn=NextFreeUnixId,dc=alex,dc=fr

Please provide a password for the domain administrateur:
Changing UNIX and samba passwords for administrateur
New password:
Retype new password:
pdc:~#
```

Pour consulter l'annuaire :

```
pdc:~# ldapsearch -x -D cn=Manager,dc=alex,dc=fr -w mypassword -b
dc=alex,dc=fr -LLL | less
```

Pour créer les premiers comptes :

```
pdc:~# smbldap-useradd -?
(c) Jerome Tournier - IDEALX 2004 (http://www.idealx.com)- Licensed under
the GPL
Usage: /usr/sbin/smbldap-useradd [-awmugdsckABCDEFGHMNPST?] username
  -o    add the user in the organizational unit (relative to the user
suffix)
  -a    is a Windows User (otherwise, Posix stuff only)
  -b    is a AIX User
  -w    is a Windows Workstation (otherwise, Posix stuff only)
  -i    is a trust account (Windows Workstation)
  -u    uid
  -g    gid
  -G    supplementary comma-separated groups
  -n    do not create a group
  -d    home
  -s    shell
  -c    gecos
  -m    creates home directory and copies /etc/skel
  -k    skeleton dir (with -m)
  -t    time. Wait 'time' seconds before exiting (when adding Windows
Workstation)
```

```
  -P    ends by invoking smbldap-passwd
  -A    can change password ? 0 if no, 1 if yes
  -B    must change password ? 0 if no, 1 if yes
  -C    sambaHomePath (SMB home share, like '\\PDC-SRV\homes')
  -D    sambaHomeDrive (letter associated with home share, like 'H:')
  -E    sambaLogonScript (DOS script to execute on login)
  -F    sambaProfilePath (profile directory, like '\\PDC-
SRV\profiles\foo')
  -H    sambaAcctFlags (samba account control bits like '[NDHTUMWSLKI]')
  -N    surname
  -S    family name
  -M    local mailAddress (comma seperated)
  -T    mailToAddress (forward address) (comma seperated)
  -?    show this help message
pdc:~#
```

Je crée un compte ldapadmin qui pourra administrer l'annuaire (mot de passe = *admin*) et un compte ldapreplicateur pour la réplication entre les annuaires (mot de passe = *mypassword*) :

```
pdc:~# smbldap-useradd -n -d /dev/null -s /bin/false -P ldapadmin
Changing UNIX password for ldapadmin
New password:
Retype new password:

pdc:~# smbldap-useradd -n -d /dev/null -s /bin/false -P ldapreplicateur
Changing UNIX password for ldapreplicateur
New password:
Retype new password:
```

Si vous voulez créer d'autres comptes utilisateurs en ligne de commande, ne les créez pas avec l'argument -m (creates home directory and copies /etc/skel) puisque leur home directory se trouvera sur un autre serveur Samba (FS).
Nous verrons plus bas comment gérer graphiquement les comptes dans les annuaires OpenLDAP.

Nous allons créer une unité d'organisation nommée ou=Domains qui contiendra les informations pour nos domaines mail.
Créez un fichier domains.alex.fr.ldif :

```
dn: ou=Domains,dc=alex,dc=fr
ou: Domains
objectClass: organizationalUnit
objectClass: top
```

Ajoutez son contenu dans l'annuaire avec cette commande :

```
pdc:~# ldapadd -x -D uid=ldapadmin,ou=Users,dc=alex,dc=fr -w admin -f
domains.alex.fr.ldif
```

```
adding new entry "ou=Domains,dc=alex,dc=fr"

pdc:~#
```

Consultez l'annuaire pour cette "ou" :

```
pdc:~# ldapsearch -x -b dc=alex,dc=fr -LLL ou=Domains
```

Configuration d'OpenLDAP sur bdc.alex.lan

Modifiez le fichier /etc/resolv.conf :

```
search alex.lan sr1.alex.lan alex.dmz
nameserver 172.17.0.1
nameserver 172.16.0.1
```

Modifiez le fichier /etc/network/interfaces :

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

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 172.17.0.4
netmask 255.255.0.0
gateway 172.17.0.254
up route add -net 172.18.0.0/16 gw 172.17.0.253
```

Copiez depuis le serveur pdc.alex.lan les schémas Samba, mail et proxy-ftp, le certificat du serveur pdc, bdc et la clef TLS/SSL du serveur bdc, puisque nous utilisons ldaps :

```
bdc:~# scp root@172.17.0.3:/etc/ldap/schema/samba-3.0.24.schema /etc/ldap/
schema/
bdc:~# scp root@172.17.0.3:/etc/ldap/schema/mail.schema /etc/ldap/schema/
bdc:~# scp root@172.17.0.3:/etc/ldap/schema/proxy-ftp.schema
/etc/ldap/schema/

bdc:~# mkdir /etc/ldap/tls

bdc:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_pdc_cert.pem /etc/ldap/tls/
bdc:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_bdc_* /etc/ldap/tls/
```

Changez les droits sur ces fichiers :

```
bdc:~# chown openldap: /etc/ldap/tls/*.pem
```

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

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
#allow bind_v2

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

include         /etc/ldap/schema/samba-3.0.24.schema
include         /etc/ldap/schema/mail.schema
include         /etc/ldap/schema/proxy-ftp.schema

# Informations ldaps.
TLSCertificateFile /etc/ldap/tls/ldap_bdc_cert.pem
TLSCertificateKeyFile /etc/ldap/tls/ldap_bdc_key.pem

pidfile         /var/run/slapd/slapd.pid

argsfile        /var/run/slapd/slapd.args

#loglevel       0
loglevel        256

modulepath      /usr/lib/ldap
moduleload      back_bdb
moduleload      syncprov

sizelimit       500

tool-threads    1

########################################################################
# Specific Backend Directives for bdb:
backend         bdb
checkpoint      512 30

# Configuration de la base OpenLDAP portant le suffix dc=alex,dc=fr
#
########################################################################
# Specific Directives for database #1, of type bdb:
database        bdb

suffix          "dc=alex,dc=fr"

rootdn          "cn=Manager,dc=alex,dc=fr"
```

```
# Le mot de passe pour cette base est « mypassword »
rootpw        {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory     "/var/lib/ldap"

dbconfig      set_cachesize 0 2097152 0
dbconfig      set_lk_max_objects 1500
dbconfig      set_lk_max_locks 1500
dbconfig      set_lk_max_lockers 1500

# Indexing options for database #1
index         objectClass,entryCSN,entryUUID                  eq
index         uidNumber,gidNumber,memberUid                   eq
index         sambaSID,sambaPrimaryGroupSID,sambaDomainName eq
index         cn,sn,uid,displayName                           pres,sub,eq
index         default                                         sub

# Inclusion du fichier contenant les ACLs.
include       /etc/ldap/slapd.access_bdc.conf

idletimeout   1800

lastmod       on

# Réplication depuis pdc.alex.lan.
# ATTENTION : enlevez tous les commentaires dans la directive syncrepl !
syncrepl rid=001
     # Adresse de l'annuaire Primaire. Indiquez l'adresse FQDN du
     # serveur, car la transaction TLS/SSL vérifie la concordance du
     # FQDN avec le certificat (CN).
     provider=ldaps://pdc.alex.lan:636
     # Il n'existe deux modes de réplication dans Syncrepl :
     # - refreshOnly, les clients (base LDAP secondaire) se synchronisent
     # périodiquement auprès du fournisseur (base LDAP primaire).
     # - refreshAndPersist, le fournisseur reste connecté en permanence
     # avec les clients (connexion persistante) pour que les
     # modifications soient immédiatement propagées.
     type=refreshOnly
     # Interval de synchronisation à 5 minutes (dd:hh:mm:ss).
     interval=00:00:05:00
     # Si la communication à échouée, on réessaie toutes les 60 secondes.
     retry="60 +"
     # On synchronise depuis le suffix.
     searchbase=dc=alex,dc=fr
     # Toutes les données et attributs d'opération.
     attrs="*,+"
     scope=sub
     bindmethod=simple
     # Je réalise la requête avec le compte
     # uid=ldapreplicateur,ou=Users,dc=alex,dc=fr et le mot de passe
     # « mypassword » (en clair malheureusement)
     binddn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr"
     credentials=mypassword
```

Créez le fichier /etc/ldap/slapd.access_bdc.conf :

```
# ACLs BDC POSIX/SAMBA
# La base répliquée doit être en lecture seule puisque OpenLDAP ne gère
# pas encore la réplication bidirectionnelle.
# Seul le compte ldapreplicateur peut écrire les modifications propagées
# depuis l'annuaire Primaire.

access to
attrs=userPassword,shadowLastChange,sambaLMPassword,sambaNTPassword,
sambaPwdLastSet,sambaPwdMustChange,sambaPasswordHistory
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by anonymous auth
    by * none

access to dn.subtree="ou=Users,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by users read
    by anonymous read

access to dn.subtree="ou=Computers,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by peername.ip=127.0.0.1 read

access to dn.subtree="ou=Users,dc=alex,dc=fr" attrs=mail,telephoneNumber
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by anonymous read

access to dn="sambaDomainName=ALEX,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by * none

access to dn="cn=NextFreeUnixId,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by * none

access to *
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
```

```
    by group="cn=Domain Admins,ou=Groups,dc=alex,dc=fr" read
    by * read
```

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

```
TLS_CACERTDIR /etc/ldap/tls
TLS_REQCERT allow

BASE dc=alex,dc=fr
URI ldap://127.0.0.1 ldaps://pdc.alex.lan
```

Modifiez le fichier /etc/default/slapd :

```
SLAPD_CONF=

SLAPD_USER="openldap"

SLAPD_GROUP="openldap"

SLAPD_PIDFILE=

SLURPD_START=auto

# Pour que le service écoute sur la boucle locale et sur son IP en ldaps.
SLAPD_SERVICES="ldap://127.0.0.1:389 ldaps://172.17.0.4:636"

SLAPD_OPTIONS=""
SLURPD_OPTIONS=""
```

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

```
base dc=alex,dc=fr

uri ldap://127.0.0.1/ ldaps://pdc.alex.lan/

ldap_version 3

scope one

timelimit 30

bind_timelimit 30

bind_policy soft

pam_filter objectclass=posixaccount

pam_login_attribute uid

nss_base_passwd      ou=Users,dc=alex,dc=fr?one
nss_base_passwd      ou=Computers,dc=alex,dc=fr?one
nss_base_group        ou=Groups,dc=alex,dc=fr?one
```

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
```

Pour que l'annuaire Secondaire réplique le contenu du Primaire la première fois.

Stoppez le service :

```
bdc:~# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
```

Effacez la base existante :

```
bdc:~# rm -r /var/lib/ldap/*
```

Vérifiez que vous pouvez interroger le serveur LDAP Primaire depuis le Secondaire :

```
bdc:~# ldapsearch -x -D uid=ldapreplicateur,ou=Users,dc=alex,dc=fr -w
mypassword -LLL -H ldaps://pdc.alex.lan | less
```

Démarrez le service :

```
bdc:~# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
```

Consultez l'annuaire du Secondaire :

```
bdc:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=fr -w admin
-LLL | less
```

Configuration d'OpenLDAP sur nas1.alex.dmz

Modifiez le fichier /etc/resolv.conf :

```
search alex.dmz alex.lan sr1.alex.lan
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 172.16.0.17
netmask 255.255.255.0
up route add -net 172.17.0.0/16 gw 172.16.0.254

iface eth1 inet static
address 192.168.0.1
netmask 255.255.255.252
```

Copiez depuis le serveur pdc.alex.lan les schémas Samba, mail et proxy-ftp, le certificat du serveur pdc, ldap1, ldap2 et la clef TLS/SSL du serveur ldap1 :

```
nas1:~# scp root@172.17.0.3:/etc/ldap/schema/samba-3.0.24.schema
/etc/ldap/schema/
nas1:~# scp root@172.17.0.3:/etc/ldap/schema/mail.schema /etc/ldap/schema/
nas1:~# scp root@172.17.0.3:/etc/ldap/schema/proxy-ftp.schema
/etc/ldap/schema/

nas1:~# mkdir /etc/ldap/tls

nas1:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_pdc_cert.pem /etc/ldap/tls/
nas1:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_ldap1* /etc/ldap/tls/
nas1:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_ldap2_cert.pem
/etc/ldap/tls/
```

Changez les droits sur ces fichiers :

```
nas1:~# chown openldap: /etc/ldap/tls/*.pem
```

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

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
```

```
# Global Directives:

# Features to permit
#allow bind_v2

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

include         /etc/ldap/schema/samba-3.0.24.schema
include         /etc/ldap/schema/mail.schema
include         /etc/ldap/schema/proxy-ftp.schema

# Informations ldaps.
TLSCertificateFile /etc/ldap/tls/ldap_ldap1_cert.pem
TLSCertificateKeyFile /etc/ldap/tls/ldap_ldap1_key.pem

pidfile         /var/run/slapd/slapd.pid

argsfile        /var/run/slapd/slapd.args

#loglevel       0
loglevel        256

modulepath      /usr/lib/ldap
# Charge le module meta en plus du module bdb.
moduleload      back_meta
moduleload      back_bdb
moduleload      syncprov

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

tool-threads    1

# Inclusion d'un fichier slapd.access contenant les ACLs pour toutes les
bases.
include         /etc/ldap/slapd.access_ldap1.conf

# On utilise le moteur META.
#
#######################################################################
# Specific Backend Directives for meta:
backend         meta

# Configuration de la base OpenLDAP portant le suffixe dc=meta
#
#######################################################################
# Specific Directives for database #1, of type meta:
database        meta

suffix          "dc=meta"

# Directive spécifiant l'adresse de la base.
uri             "ldap://localhost/dc=alex,dc=fr,dc=meta"
```

```
# Permet de réécrire le nom du suffixe :
#              "suffixe virtuel"        "suffixe réel"
suffixmassage "dc=alex,dc=fr,dc=meta" "dc=alex,dc=fr"

uri           "ldap://localhost/dc=alex,dc=com,dc=meta"
suffixmassage "dc=alex,dc=com,dc=meta" "dc=alex,dc=com"

uri           "ldap://localhost/dc=alex,dc=org,dc=meta"
suffixmassage "dc=alex,dc=org,dc=meta" "dc=alex,dc=org"

# Ne pas activer pour un moteur META.
lastmod       off

idletimeout   1800

# Configuration de la base OpenLDAP portant le suffixe dc=alex,dc=fr
#
#######################################################################
# Specific Directives for database #2, of type bdb:
database      bdb

suffix        "dc=alex,dc=fr"

rootdn        "cn=Manager,dc=alex,dc=fr"
# Le mot de passe pour cette base est « mypassword »
rootpw        {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory     "/var/lib/ldap/alex.fr"

dbconfig      set_cachesize 0 2097152 0
dbconfig      set_lk_max_objects 1500
dbconfig      set_lk_max_locks 1500
dbconfig      set_lk_max_lockers 1500

# Indexing options for database #2
index         objectClass,entryCSN,entryUUID eq
index         uidNumber,gidNumber,memberUid  eq
# Nous utiliserons ces attributs quand nous traiterons du tutoriel
Postfix.
index         mail,mailAlias,mailForwarding,mailDomainName,mailDomainName
Alias,mailAccountActive eq
index         uid                            pres,sub,eq
index         default                        sub

lastmod       on

# Réplication depuis pdc.alex.lan.
syncrepl rid=001
     provider=ldaps://pdc.alex.lan:636
     type=refreshOnly
     interval=00:00:05:00
     retry="60 +"
     searchbase=dc=alex,dc=fr
     attrs="*,+"
     scope=sub
     bindmethod=simple
     binddn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr"
```

```
     credentials=mypassword

# Configuration de la base OpenLDAP portant le suffixe dc=alex,dc=com
#
#######################################################################
# Specific Directives for database #3, of type bdb:
database      bdb

suffix        "dc=alex,dc=com"

rootdn        "cn=Manager,dc=alex,dc=com"
# Le mot de passe pour cette base est « mypassword »
rootpw        {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory     "/var/lib/ldap/alex.com"

dbconfig      set_cachesize 0 2097152 0
dbconfig      set_lk_max_objects 1500
dbconfig      set_lk_max_locks 1500
dbconfig      set_lk_max_lockers 1500

# Indexing options for database #3
index         objectClass,entryCSN,entryUUID eq
index         uidNumber,gidNumber,memberUid  eq
index         mail,mailAlias,mailForwarding,mailDomainName,mailDomainName
Alias,mailAccountActive eq
index         uid                            pres,sub,eq
index         default                        sub

lastmod       on

# Pour la réplication.
Overlay       syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100

# Configuration de la base OpenLDAP portant le suffixe dc=alex,dc=org
#
#######################################################################
# Specific Directives for database #4, of type bdb:
database      bdb

suffix        "dc=alex,dc=org"

rootdn        "cn=Manager,dc=alex,dc=org"
# Le mot de passe pour cette base est « mypassword »
rootpw        {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory     "/var/lib/ldap/alex.org"

dbconfig      set_cachesize 0 2097152 0
dbconfig      set_lk_max_objects 1500
dbconfig      set_lk_max_locks 1500
dbconfig      set_lk_max_lockers 1500

# Indexing options for database #4
```

```
index         objectClass,entryCSN,entryUUID eq
index         uidNumber,gidNumber,memberUid  eq
index         mail,mailAlias,mailForwarding,mailDomainName,mailDomainName
Alias,mailAccountActive eq
index         uid                            pres,sub,eq
index         default                        sub

lastmod       on

# Pour la réplication.
Overlay       syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
```

Créez le fichier /etc/ldap/slapd.access_ldap1.conf :

```
# ACLs LDAP1 POSIX/SAMBA

# ACLs concernant les mots de passe dans ces branches.
access to dn.subtree="ou=Users,dc=alex,dc=fr"
attrs=userPassword,shadowLastChange,sambaLMPassword,sambaNTPassword,
sambaPwdLastSet,sambaPwdMustChange,sambaPasswordHistory,
sambaPrimaryGroupSID,sambaSID
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by anonymous auth
    by * none

access to dn.subtree="ou=Users,dc=alex,dc=com"   attrs=userPassword
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" write
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" read
    by anonymous auth
    by * none

access to dn.subtree="ou=Users,dc=alex,dc=org"   attrs=userPassword
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" write
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" read
    by anonymous auth
    by * none

# ACLs concernant tout ce qui se trouve dans ces branches.
access to dn.subtree="ou=Users,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by users read
    by anonymous read

access to dn.subtree="ou=Users,dc=alex,dc=com"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" write
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" read
    by users read
```

```
    by anonymous read

access to dn.subtree="ou=Users,dc=alex,dc=org"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" write
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" read
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=com"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" write
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" read
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=org"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" write
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" read
    by users read
    by anonymous read

access to dn.subtree="dc=meta"
    by users read
    by anonymous read

# ACLs pour tout le reste.
access to *
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" write
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" write
    by * read
```

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

```
TLS_CACERTDIR /etc/ldap/tls
TLS_REQCERT allow

BASE dc=meta
URI ldap://127.0.0.1 ldaps://ldap2.alex.dmz
```

Modifiez le fichier /etc/default/slapd :

```
SLAPD_CONF=

SLAPD_USER="openldap"

SLAPD_GROUP="openldap"
```

```
SLAPD_PIDFILE=

SLURPD_START=auto

# Pour que le service écoute sur la boucle locale et sur son alias IP en
# ldap et ldaps quand nous traiteront du tutoriel "Redondance et
# continuité de service".
#SLAPD_SERVICES="ldap://127.0.0.1:389/ ldap://172.16.0.19/
ldaps://172.16.0.19/"
# Pour que le service écoute sur la boucle locale et sur son IP en ldap
et ldaps.
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldap://172.16.0.17/
ldaps://172.16.0.17/"

SLAPD_OPTIONS=""
SLURPD_OPTIONS=""
```

Pour que l'annuaire Secondaire réplique le contenu du Primaire la première fois.

Stoppez le service :

```
nas1:~# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
```

Effacez la base existante :

```
nas1:~# rm -r /var/lib/ldap/*
```

Créez les répertoires où seront stockées les bases et changez les droits :

```
nas1:~# mkdir -p /var/lib/ldap/alex.fr /var/lib/ldap/alex.com
/var/lib/ldap/alex.org

nas1:~# chown -R openldap: /var/lib/ldap/*
```

Vérifiez que vous pouvez interroger le serveur LDAP Primaire depuis le Secondaire :

```
nas1:~# ldapsearch -x -D uid=ldapreplicateur,ou=Users,dc=alex,dc=fr -w
mypassword -b dc=alex,dc=fr -LLL -H ldaps://pdc.alex.lan | less
```

Démarrez le service :

```
nas1:~# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
```

Consultez le suffixe "dc=alex,dc=fr" de l'annuaire :

```
nas1:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=fr -w admin -b
dc=alex,dc=fr -LLL | less

nas1:~# ldapsearch -x -D uid=ldapreplicateur,ou=Users,dc=alex,dc=fr -w
mypassword -b dc=alex,dc=fr -LLL | less
```

Créez un fichier alex.com.ldif contenant les données minimales pour la base "dc=alex,dc=com" :

```
# Racine.
dn: dc=alex,dc=com
objectClass: dcObject
objectClass: organization
o: alex
dc: alex

# Branches des comptes utilisateurs.
dn: ou=Users,dc=alex,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Users

# Branches des groupes.
dn: ou=Groups,dc=alex,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Groups

# Branches des domaines mail.
dn: ou=Domains,dc=alex,dc=com
objectClass: top
objectClass: organizationalUnit
ou: Domains

dn: uid=ldapadmin,ou=Users,dc=alex,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: ldapadmin
sn: ldapadmin
givenName: ldapadmin
uid: ldapadmin
uidNumber: 20000
gidNumber: 513
homeDirectory: /dev/null
loginShell: /bin/false
gecos: System User
userPassword: {SSHA}12bSqzMl3KsUKNOqGpQj8O2rE6AhKDBF
# Pour le crypter le mot de passe utilisez cette commande :
# nas1:~# slappasswd -h {SSHA} -s VoTrE_MoT2PaSsE

dn: uid=ldapreplicateur,ou=Users,dc=alex,dc=com
```

```
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: ldapreplicateur
sn: ldapreplicateur
givenName: ldapreplicateur
uid: ldapreplicateur
uidNumber: 20001
gidNumber: 513
homeDirectory: /dev/null
loginShell: /bin/false
gecos: System User
userPassword: {SSHA}vHSSs2rx6zBtZb4v7VHEmtE6yxlcAByV
```

Ajoutez son contenu dans l'annuaire avec cette commande :

```
nas1:~# ldapadd -x -D cn=Manager,dc=alex,dc=com -w mypassword -f
alex.com.ldif

adding new entry "dc=alex,dc=com"
adding new entry "ou=Users,dc=alex,dc=com"
adding new entry "ou=Groups,dc=alex,dc=com"
adding new entry "ou=Domains,dc=alex,dc=com"
adding new entry "uid=ldapadmin,ou=Users,dc=alex,dc=com"
adding new entry "uid=ldapreplicateur,ou=Users,dc=alex,dc=com"

nas1:~#
```

Faites de même pour la base "dc=alex,dc=org" en adaptant les uidNumber à 30000 et 30001 par exemple et en changent tous les "...,dc=com" par "...,dc=org"

Ajoutez son contenu dans l'annuaire :

```
nas1:~# ldapadd -x -D cn=Manager,dc=alex,dc=org -w mypassword -f
alex.org.ldif
```

Consultez les suffixes "dc=alex,dc=com" et "dc=alex,dc=org" :

```
nas1:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=com -w admin -
b dc=alex,dc=com -LLL | less

nas1:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=org -w admin -
b dc=alex,dc=org -LLL | less
```

Configuration d'OpenLDAP sur ldap2.alex.dmz

Modifiez le fichier /etc/resolv.conf :

```
search alex.dmz alex.lan sr1.alex.lan
nameserver 172.16.0.1
nameserver 172.17.0.1
```

Modifiez le fichier /etc/network/interfaces :

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

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 172.16.0.20
netmask 255.255.255.0
up route add -net 172.17.0.0/16 gw 172.16.0.254
```

Copiez depuis le serveur pdc.alex.lan les schémas Samba, mail et proxy-ftp, le certificat du serveur pdc, ldap1, ldap2 et la clef TLS/SSL du serveur ldap2 :

```
ldap2:~# scp root@172.17.0.3:/etc/ldap/schema/samba-3.0.24.schema
/etc/ldap/schema/
ldap2:~# scp root@172.17.0.3:/etc/ldap/schema/mail.schema
/etc/ldap/schema/
ldap2:~# scp root@172.17.0.3:/etc/ldap/schema/proxy-ftp.schema
/etc/ldap/schema/

ldap2:~# mkdir /etc/ldap/tls

ldap2:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_pdc_cert.pem
/etc/ldap/tls/
ldap2:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_ldap1_cert.pem
/etc/ldap/tls/
ldap2:~# scp root@172.17.0.3:/etc/ldap/tls/ldap_ldap2* /etc/ldap/tls/
```

Changez les droits sur ces fichiers :

```
ldap2:~# chown openldap: /etc/ldap/tls/*.pem
```

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

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
```

```
#allow bind_v2

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

include         /etc/ldap/schema/samba-3.0.24.schema
include         /etc/ldap/schema/mail.schema
include         /etc/ldap/schema/proxy-ftp.schema

# Informations ldaps.
TLSCertificateFile /etc/ldap/tls/ldap_ldap2_cert.pem
TLSCertificateKeyFile /etc/ldap/tls/ldap_ldap2_key.pem

pidfile         /var/run/slapd/slapd.pid

argsfile        /var/run/slapd/slapd.args

#loglevel       0
loglevel        256

modulepath      /usr/lib/ldap
# Charge le module meta en plus du module bdb.
moduleload      back_meta
moduleload      back_bdb
moduleload      syncprov

sizelimit       unlimited

tool-threads    1

# Inclusion d'un fichier slapd.access contenant les ACLs pour toutes les
bases.
include         /etc/ldap/slapd.access_ldap2.conf

# On utilise le moteur META.
#
#######################################################################
# Specific Backend Directives for meta:
backend         meta

# Configuration de la base OpenLDAP portant le suffix dc=meta
#
#######################################################################
# Specific Directives for database #1, of type meta:
database        meta

suffix          "dc=meta"

uri             "ldap://localhost/dc=alex,dc=fr,dc=meta"
suffixmassage "dc=alex,dc=fr,dc=meta" "dc=alex,dc=fr"

uri             "ldap://localhost/dc=alex,dc=com,dc=meta"
suffixmassage "dc=alex,dc=com,dc=meta" "dc=alex,dc=com"

uri             "ldap://localhost/dc=alex,dc=org,dc=meta"
```

```
suffixmassage "dc=alex,dc=org,dc=meta" "dc=alex,dc=org"

lastmod       off

idletimeout   1800

# Configuration de la base OpenLDAP portant le suffix dc=alex,dc=fr
#
#######################################################################
# Specific Directives for database #2, of type bdb:
database      bdb

suffix        "dc=alex,dc=fr"

rootdn        "cn=Manager,dc=alex,dc=fr"
# Le mot de passe pour cette base est « mypassword »
rootpw        {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory     "/var/lib/ldap/alex.fr"

dbconfig      set_cachesize 0 2097152 0
dbconfig      set_lk_max_objects 1500
dbconfig      set_lk_max_locks 1500
dbconfig      set_lk_max_lockers 1500

# Indexing options for database #2
index         objectClass,entryCSN,entryUUID eq
index         uidNumber,gidNumber,memberUid  eq
index         mail,mailAlias,mailForwarding,mailDomainName,mailDomainName
Alias,mailAccountActive eq
index         uid                            pres,sub,eq
index         default                        sub

lastmod       on

# Réplication depuis pdc.alex.lan.
syncrepl rid=001
     provider=ldaps://pdc.alex.lan:636
     type=refreshOnly
     interval=00:00:05:00
     retry="60 +"
     searchbase=dc=alex,dc=fr
     attrs="*,+"
     scope=sub
     bindmethod=simple
     binddn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr"
     credentials=mypassword

# Configuration de la base OpenLDAP portant le suffix dc=alex,dc=com
#
#######################################################################
# Specific Directives for database #3, of type bdb:
database      bdb

suffix        "dc=alex,dc=com"

rootdn        "cn=Manager,dc=alex,dc=com"
```

```
# Le mot de passe pour cette base est « mypassword »
rootpw          {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory       "/var/lib/ldap/alex.com"

dbconfig        set_cachesize 0 2097152 0
dbconfig        set_lk_max_objects 1500
dbconfig        set_lk_max_locks 1500
dbconfig        set_lk_max_lockers 1500

# Indexing options for database #3
index           objectClass,entryCSN,entryUUID eq
index           uidNumber,gidNumber,memberUid  eq
index           mail,mailAlias,mailForwarding,mailDomainName,mailDomainName
Alias,mailAccountActive eq
index           uid                             pres,sub,eq
index           default                         sub

lastmod         on

# Réplication depuis ldap1.alex.dmz.
syncrepl rid=002
     provider=ldaps://ldap1.alex.dmz:636
     type=refreshOnly
     interval=00:00:05:00
     retry="60 +"
     searchbase=dc=alex,dc=com
     attrs="*,+"
     scope=sub
     bindmethod=simple
     binddn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com"
     credentials=mypassword

# Configuration de la base OpenLDAP portant le suffix dc=alex,dc=org
#
#######################################################################
# Specific Directives for database #4, of type bdb:
database        bdb

suffix          "dc=alex,dc=org"

rootdn          "cn=Manager,dc=alex,dc=org"
# Le mot de passe pour cette base est « mypassword »
rootpw          {SSHA}BgKVcPjH+pHCd2JuUdb9VvEmNa+h3UGp

# Répertoire ou sera stockée cette base.
directory       "/var/lib/ldap/alex.org"

dbconfig        set_cachesize 0 2097152 0
dbconfig        set_lk_max_objects 1500
dbconfig        set_lk_max_locks 1500
dbconfig        set_lk_max_lockers 1500

# Indexing options for database #4
index           objectClass,entryCSN,entryUUID eq
index           uidNumber,gidNumber,memberUid  eq
index           mail,mailAlias,mailForwarding,mailDomainName,mailDomainName
```

```
Alias,mailAccountActive eq
index          uid                              pres,sub,eq
index          default                          sub

lastmod        on

# Réplication depuis ldap1.alex.dmz.
syncrepl rid=003
     provider=ldaps://ldap1.alex.dmz:636
     type=refreshOnly
     interval=00:00:05:00
     retry="60 +"
     searchbase=dc=alex,dc=org
     attrs="*,+"
     scope=sub
     bindmethod=simple
     binddn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org"
     credentials=mypassword
```

Créez le fichier /etc/ldap/slapd.access_ldap2.conf :

```
# ACLs LDAP2 POSIX/SAMBA

# ACLs concernant les mots de passe dans ces branches.
access to dn.subtree="ou=Users,dc=alex,dc=fr"
attrs=userPassword,shadowLastChange,sambaLMPassword,sambaNTPassword,
sambaPwdLastSet,sambaPwdMustChange,sambaPasswordHistory,
sambaPrimaryGroupSID,sambaSID
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by anonymous auth
    by * none

access to dn.subtree="ou=Users,dc=alex,dc=com"    attrs=userPassword
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" read
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" write
    by anonymous auth
    by * none

access to dn.subtree="ou=Users,dc=alex,dc=org"    attrs=userPassword
    by self read
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" read
    by tls_ssf=256 ssf=256
dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" write
    by anonymous auth
    by * none

# ACLs concernant tout ce qui se trouve dans ces branches.
access to dn.subtree="ou=Users,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by users read
    by anonymous read
```

```
access to dn.subtree="ou=Users,dc=alex,dc=com"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" write
    by users read
    by anonymous read

access to dn.subtree="ou=Users,dc=alex,dc=org"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" write
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=fr"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=fr" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=com"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=com" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" write
    by users read
    by anonymous read

access to dn.subtree="ou=Groups,dc=alex,dc=org"
    by dn="uid=ldapadmin,ou=Users,dc=alex,dc=org" read
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" write
    by users read
    by anonymous read

access to dn.subtree="dc=meta"
    by users read
    by anonymous read

# ACLs pour tout le reste.
access to *
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=fr" write
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=com" write
    by dn="uid=ldapreplicateur,ou=Users,dc=alex,dc=org" write
    by * read
```

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

```
TLS_CACERTDIR /etc/ldap/tls
TLS_REQCERT allow

BASE dc=meta
URI ldap://127.0.0.1 ldaps://ldap1.alex.dmz
```

Modifiez le fichier /etc/default/slapd :

```
SLAPD_CONF=
```

```
SLAPD_USER="openldap"

SLAPD_GROUP="openldap"

SLAPD_PIDFILE=

SLURPD_START=auto

# Pour que le service écoute sur la boucle locale et sur son IP en ldap
et ldaps.
SLAPD_SERVICES="ldap://127.0.0.1:389/ ldap://172.16.0.20/
ldaps://172.16.0.20/"

SLAPD_OPTIONS=""
SLURPD_OPTIONS=""
```

Pour que l'annuaire Secondaire réplique le contenu des Primaires la première fois.

Stoppez le service :

```
ldap2:~# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
ldap2:~#
```

Effacez la base existante :

```
ldap2:~# rm -r /var/lib/ldap/*
```

Créez les répertoires où seront stockées les bases et changez les droits :

```
ldap2:~# mkdir -p /var/lib/ldap/alex.fr /var/lib/ldap/alex.com
/var/lib/ldap/alex.org

ldap2:~# chown -R openldap: /var/lib/ldap/*
```

Vérifiez que vous pouvez interroger le serveur LDAP Primaire depuis le Secondaire :

```
ldap2:~# ldapsearch -x -D uid=ldapreplicateur,ou=Users,dc=alex,dc=fr -w
mypassword -b dc=alex,dc=fr -LLL -H ldaps://pdc.alex.lan | less

ldap2:~# ldapsearch -x -D uid=ldapreplicateur,ou=Users,dc=alex,dc=com -w
mypassword -b dc=alex,dc=com -LLL -H ldaps://ldap1.alex.dmz | less

ldap2:~# ldapsearch -x -D uid=ldapreplicateur,ou=Users,dc=alex,dc=org -w
mypassword -b dc=alex,dc=org -LLL -H ldaps://ldap1.alex.dmz | less
```

Démarrez le service :

```
ldap2:~# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
```

Consultez les différents suffixes :

```
ldap2:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=fr -w admin -
b dc=alex,dc=fr -LLL | less

ldap2:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=com -w admin
-b dc=alex,dc=com -LLL | less

ldap2:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=org -w admin
-b dc=alex,dc=org -LLL | less

ldap2:~# ldapsearch -x -D uid=ldapadmin,ou=Users,dc=alex,dc=fr -w admin -
b dc=meta -LLL | less

ldap2:~# ldapsearch -x -b dc=meta -LLL | less
```

Configuration de Samba sur pdc.alex.lan

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:          superviseur@alex.lan
```

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

```
pdc:~# newaliases

pdc:~# /etc/init.d/postfix reload
Reloading Postfix configuration...done.
```

Modifiez le fichier /etc/samba/smb.conf :

```
#================== Global Settings ==================
[global]


## Browsing/Identification ###

# Nom du Workgroup
workgroup = ALEX

# Nom NetBIOS de ce serveur Samba (Si possible, le même que le nom DNS)
netbios name = PDC
```

```
server string = Samba %L Server

# Samba sera client WINS du serveur Samba FS.
# Il faudra mettre l'adresse de l'alias IP quand nous traiterons du
# tutoriel "Redondance et continuité de service".
#wins server = 172.17.0.9
wins server = 172.17.0.7

# Pour que Samba essaie de résoudre les noms NetBIOS, pas encore
# enregistrés dans WINS, en questionnant le serveur DNS.
dns proxy = yes

# Dans quel ordre Samba résolvera les noms NetBIOS.
name resolve order = host wins bcast


#### Networking ####

# Options de sécurité.
hosts allow = 127.0.0.1/8, 172.17.0.0/16, 172.18.0.0/16
hosts deny = 0.0.0.0/0

interfaces = lo eth0
bind interfaces only = yes


#### Debugging/Accounting ####

log file = /var/log/samba/log.%m

# Taille maximum des logs (Kb).
max log size = 50
# Utile pour faire vos tests.
;log level = 5

# Quand smbd ou nmbd crash, cette commande est exécutée et envoie
# un mail à root, c'est pour cela qu'il faut qu'un serveur SMTP soit
# installé sur cette machine.
panic action = /usr/share/samba/panic-action %d


####### Authentication #######

security = user

invalid users = root

encrypt passwords = true

# On utilise le script de smbldap-tools pour changer le mot de passe.
passwd program = /usr/sbin/smbldap-passwd %u

# Le paramétre "passwd chat" est uniquement prit en compte si
# "unix password sync = yes"
# par défaut, "unix password sync = no", donc pas besoin de "passwd chat"
```

```
# Connexion à l'annuaire en localhost, puisque
# Samba est sur la même machine que OpenLDAP.
# Et sur l'annuaire Secondaire en ldaps pour une continuité de service.
passdb backend = ldapsam:"ldap://localhost ldaps://bdc.alex.lan"

# Dans une configuration de Samba comme serveur membre uniquement :
# Pour que les informations de mappage des SID en UID/GID ne soient pas
# stockées localement mais dans l'annuaire. Dans notre cas Samba est
# contrôleur de domaine.
#idmap backend = ldap:"ldap://localhost ldaps://bdc.alex.lan"
#ldap idmap suffix = ou=Idmap

# L'identifiant LDAP avec lequel Samba se connectera à l'annuaire pour
# lire et écrire.
ldap admin dn = uid=ldapadmin,ou=Users,dc=alex,dc=fr

ldap suffix = dc=alex,dc=fr

# Pour que Samba synchronise le mot de passe Windows avec le mot de passe
POSIX.
ldap passwd sync = yes

# La commande smbpasswd -x un_compte, peut ou non effacer toutes les
# informations sur ce compte. Par défaut, seulement les attributs Samba
# sont effacés.
ldap delete dn = no

ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers


########## Domains ############

# Ce serveur sera contrôleur de domaine principal.
domain logons = yes
domain master = yes
preferred master = yes

# Les paramètres : logon path, logon home, logon drive et logon script
# ne sont pas prioritaires sur les informations contenues dans
# l'annuaire. Les attributs LDAP suivants seront appliqués en priorité
# s'ils sont présents :
# sambaHomePath
# sambaLogonScript
# sambaProfilePath
# sambaHomeDrive

# %U substitue le login et %a l'architecture du poste client.
# Le profile des utilisateurs Windows est stocké dans le répertoire
# .winprofile/%a de leur home directory qui se trouve sur le serveur
# Samba FS.
logon path = \\FS\%U\.winprofile\%a

# Le répertoire de base (stockage personnel)
logon home = \\FS\%U

# Lettre du lecteur Windows où sera monté le répertoire de base.
```

```
logon drive = H:

# Le script de logon est stocké sur le serveur Samba FS.
# Ce script est relatif au partage [netlogon]. Il doit se trouver dans le
# répertoire de ce partage.
logon script = logon.bat

# Scripts smbldap-tools pour la gestion des comptes entre Samba et
OpenLDAP.
add machine script = /usr/sbin/smbldap-useradd -w %m
add user script = /usr/sbin/smbldap-useradd -a -n -P %u
delete user script = /usr/sbin/smbldap-userdel -r %u
add group script = /usr/sbin/smbldap-groupadd '%g'
delete group script = /usr/sbin/smbldap-groupdel '%g'
add user to group script = /usr/sbin/smbldap-groupmod -m %u '%g'
delete user from group script = /usr/sbin/smbldap-groupmod -x %u '%g'
set primary group script = /usr/sbin/smbldap-usermod -g '%g' %u


########## Printing ##########

# Il n'y a pas d'imprimante partagée sur ce serveur.
# Un autre serveur Samba se chargera des impressions avec CUPS.
load printers = no
show add printer wizard = no

############ Misc ############

# Optimisations.
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

# Autorise les délégations "net rpc rights ..."
enable privileges = yes

# Refuse d'authentifier les clients Windows 95/98 ou MS DOS.
lanman auth = no

# Désactive les annonces Lanman par broadcast pour les clients OS/2.
lm announce = no

# Active la prise en compte des droits étendus (ACLs) sur le système de
fichiers.
ea support = yes
#
# Permet l'héritage des ACLs étendues depuis un répertoire parent.
inherit acls = yes
#
# Permet de mapper correctement les ACLs Windows avec les ACLs étendues
# dans l'éditeur de propriétés Windows (peut prendre beaucoup de
# ressources sur le serveur !)
map acl inherit = yes

# Puisque Windows ne fait pas de différence entre les
# minuscules/majuscules.
case sensitive = no

# Cache les données qui ne peuvent pas être lues par manque de droits.
hide unreadable = yes
```

```
# Définit avec quels jeux de caractères Samba doit communiquer avec les
# clients Windows.
# Attention si vous utilisez un montage Samba depuis un client Linux
# en UTF-8 les données seront interprétées comme venant d'un encodage
# CP850 ! ce qui altérera les noms des fichiers sur le serveur.
dos charset = CP850
unix charset = UTF-8
display charset = UTF-8


#====================== Share Definitions ==============

# Nous ne définissons pas de partages sur ce serveur puisqu'ils seront
# rassemblés sur le serveur de fichiers Samba FS.
```

Stoppez Samba :

```
pdc:~# /etc/init.d/samba stop
Stopping Samba daemons: nmbd smbd.
```

Effacez le fichier Samba qui contient les mots de passe :

```
pdc:~# rm -f /var/lib/samba/secrets.tdb
```

Configurez le SID Windows de Samba (celui que vous avez saisi dans le fichier /etc/smbldap-tools/smbldap.conf) :

```
pdc:~# net setlocalsid S-1-5-21-663340348-4107433757-3291108422
```

Donnez à Samba le mot de passe du compte LDAP pour qu'il puisse lire et écrire :

```
pdc:~# smbpasswd -W
Setting stored password for "uid=ldapadmin,ou=Users,dc=alex,dc=fr" in
secrets.tdb
New SMB password:
Retype new SMB password:
pdc:~#
```

Vérifiez que le SID est bien le même que celui saisi plus haut :

```
pdc:~# net getlocalsid
SID for domain PDC is: S-1-5-21-663340348-4107433757-3291108422
pdc:~#
```

Configuration de Samba sur bdc.alex.lan

Modifiez le fichier /etc/aliases pour rediriger les mails envoyés au compte root vers un autre compte de votre choix :

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

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

```
bdc:~# newaliases

bdc:~# /etc/init.d/postfix reload
Reloading Postfix configuration...done.
```

Modifiez le fichier /etc/samba/smb.conf :

```
#================== Global Settings ==================
[global]


## Browsing/Identification ###

workgroup = ALEX

netbios name = BDC

server string = Samba %L Server

#wins server = 172.17.0.9
wins server = 172.17.0.7

dns proxy = yes

name resolve order = host wins bcast


#### Networking ####

hosts allow = 127.0.0.1/8, 172.17.0.0/16, 172.18.0.0/16
hosts deny = 0.0.0.0/0

interfaces = lo eth0
bind interfaces only = yes


#### Debugging/Accounting ####

log file = /var/log/samba/log.%m

max log size = 50
log level = 3
```

```
panic action = /usr/share/samba/panic-action %d


####### Authentication #######

security = user

invalid users = root

encrypt passwords = true

passdb backend = ldapsam:"ldap://localhost ldaps://pdc.alex.lan"

ldap admin dn = uid=ldapadmin,ou=Users,dc=alex,dc=fr
ldap suffix = dc=alex,dc=fr

ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers


########## Domains ###########

# Ce serveur sera contrôleur de domaine secondaire.
domain logons = yes
domain master = auto

logon path = \\FS\%U\.winprofile\%a

logon home = \\FS\%U

logon drive = H:

logon script = logon.bat

# Quand Samba voudra écrire dans l'annuaire en lecture seule, il sera
# redirigé vers l'annuaire Primaire en lecture/écriture.
# (1000 = 1 seconde)
ldap replication sleep = 1000


########## Printing ##########

load printers = no
show add printer wizard = no


############ Misc ############

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

enable privileges = yes

lanman auth = no

lm announce = no
```

```
ea support = yes

inherit acls = yes

map acl inherit = yes

case sensitive = no

hide unreadable = yes

dos charset = CP850
unix charset = UTF-8
display charset = UTF-8


#================== Share Definitions ==============

# Nous ne définissons pas de partages sur ce serveur puisqu'ils seront
# rassemblés sur le serveur de fichiers Samba FS.
```

Stoppez Samba :

```
bdc:~# /etc/init.d/samba stop
Stopping Samba daemons: nmbd smbd.
```

Effacez le fichier Samba qui contient les mots de passe :

```
bdc:~# rm -f /var/lib/samba/secrets.tdb
```

Configurez le SID Windows de Samba (celui que vous avez saisi dans le fichier /etc/smbldap-tools/smbldap.conf). Il doit être le même sur les serveurs PDC, BDC et les FS :

```
bdc:~# net setlocalsid S-1-5-21-663340348-4107433757-3291108422
```

Donnez à Samba le mot de passe du compte LDAP pour qu'il puisse lire :

```
bdc:~# smbpasswd -W
Setting stored password for "uid=ldapadmin,ou=Users,dc=alex,dc=fr" in
secrets.tdb
New SMB password:
Retype new SMB password:
bdc:~#
```

Vérifiez que le SID est bien le même que celui saisi plus haut :

```
bdc:~# net getlocalsid
SID for domain BDC is: S-1-5-21-663340348-4107433757-3291108422
```

```
bdc:~#
```

Configuration de Samba sur fs1.alex.lan

Modifiez le fichier /etc/resolv.conf :

```
search alex.lan sr1.alex.lan alex.dmz
nameserver 172.17.0.1
nameserver 172.16.0.1
```

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 172.17.0.7
netmask 255.255.0.0
gateway 172.17.0.254
up route add -net 172.18.0.0/16 gw 172.17.0.253

iface eth1 inet static
address 192.168.0.1
netmask 255.255.255.252
```

Modifiez le fichier /etc/aliases pour rediriger les mails envoyés au compte root vers un autre compte de votre choix :

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

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

```
fs1:~# newaliases

fs1:~# /etc/init.d/postfix reload
Reloading Postfix configuration...done.
```

Copiez depuis le serveur pdc.alex.lan, le certificat du serveur pdc et bdc puisque nous utilisons ldaps :

```
fs1:~# mkdir /etc/ldap/tls

fs1:~# scp root@172.17.0.3:/etc/ldap/tls/*dc_cert.pem /etc/ldap/tls/
```

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

```
TLS_CACERTDIR /etc/ldap/tls
TLS_REQCERT allow

BASE dc=alex,dc=fr
URI ldaps://bdc.alex.lan ldaps://pdc.alex.lan
```

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

```
base dc=alex,dc=fr

uri ldaps://bdc.alex.lan ldaps://pdc.alex.lan

ldap_version 3

scope one

timelimit 30

bind_timelimit 30

bind_policy soft

pam_filter objectclass=posixaccount

pam_login_attribute uid

nss_base_passwd      ou=Users,dc=alex,dc=fr?one
nss_base_passwd      ou=Computers,dc=alex,dc=fr?one
nss_base_group        ou=Groups,dc=alex,dc=fr?one

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
#ssl start_tls
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
```

Vérifiez que le serveur interroge les annuaires OpenLDAP quand il recherche des comptes :

```
fs1:~# getent passwd | tail
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
sshd:x:100:65534::/var/run/sshd:/usr/sbin/nologin
postfix:x:101:104::/var/spool/postfix:/bin/false
administrateur:x:9999:9999:Netbios Domain
Administrator:/home/administrateur:/bin/false
nobody:x:65534:514:nobody:/dev/null:/bin/false
ldapadmin:x:2000:513:System User:/dev/null:/bin/false
ldapreplicateur:x:2001:513:System User:/dev/null:/bin/false
```

```
fs1:~# getent group | tail -15
ssl-cert:x:103:
postfix:x:104:
postdrop:x:105:
Domain Admins:*:512:administrateur
Domain Users:*:513:
Domain Guests:*:514:
Domain Computers:*:515:
Administrators:*:544:
Account Operators:*:548:
Print Operators:*:550:
Backup Operators:*:551:
Replicators:*:552:
```

Modifiez le fichier /etc/samba/smb.conf :

```
#================== Global Settings ==================
[global]


## Browsing/Identification ###

workgroup = ALEX

netbios name = FS

server string = Samba %L Server

# Maître d'exploration NetBIOS dans ce sous-réseau.
local master = yes
# Remportera l'élection avec un niveau à 65.
os level = 65
```

```
# Pour être serveur WINS pour tous les sous-réseaux.
wins support = yes

dns proxy = yes

name resolve order = host wins bcast


#### Networking ####

hosts allow = 127.0.0.1/8, 172.17.0.0/16, 172.18.0.0/16
hosts deny = 0.0.0.0/0

interfaces = lo eth0
bind interfaces only = yes


#### Debugging/Accounting ####

log file = /var/log/samba/log.%m

max log size = 50

panic action = /usr/share/samba/panic-action %d


####### Authentication #######

security = user

invalid users = root

encrypt passwords = yes

passdb backend = ldapsam:"ldaps://bdc.alex.lan ldaps://pdc.alex.lan"

ldap admin dn = uid=ldapadmin,ou=Users,dc=alex,dc=fr
ldap suffix = dc=alex,dc=fr

ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers


########## Domains ###########

domain logons = no
domain master = no


########## Printing ##########

# Samba transférera les travaux d'impression vers le serveur CUPS
distant.
load printers = yes
printing = cups
printcap name = cups
```

```
cups server = 172.17.0.5
show add printer wizard = no

############ Misc ############

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

enable privileges = yes

lanman auth = no

lm announce = no

ea support = yes

inherit acls = yes

map acl inherit = yes

case sensitive = no

hide unreadable = yes

dos charset = CP850
unix charset = UTF-8
display charset = UTF-8


#====================== Share Definitions ==============

# Répertoire de base de l'utilisateur.
# Vous devez créer le home directory des utilisateurs Windows avant leur
# première connexion au domaine.
[homes]
comment = Home Directories
browseable = no
read only = no
create mask = 0600
directory mask = 0700
valid users = %S
# Cache les fichiers suivant :
hide files = /desktop.ini/
# Interdit dans ce partage les types de fichiers suivant :
veto files = /*.bat/*.cmd/*.com/*.exe/*.pif/*.reg/*.scr/*.vb/*.vbs/

# Partage qui contiendra les scripts de connexion.
[netlogon]
comment = Network Logon Service
path = /home/samba/netlogon
browseable = no
read only = yes
share modes = no
# N'oubliez pas de donner les droits en écriture sur ces répertoires
# pour les groupes suivant :
write list = @'Account Operators'

# Répertoire qui contiendra le profil Windows itinérant. Je l'ai renommé
# .winprofile pour qu'il soit caché sous Windows et sous Linux.
```

```
[.winprofile]
comment = Users Profiles
path = /home/%U/.winprofile
browseable = no
read only = no
create mask = 0600
directory mask = 0700
# Permet de créer le profil de l'utilisateur à sa première
# connexion au domaine depuis un poste Windows.
root preexec = PROFILE=%H/.winprofile ; if [ ! -e $PROFILE ] ; \
then mkdir -pm700 $PROFILE ; chmod 700 %H ; chown -R %U:'%G' %H ; fi ;

# Partage pour les groupes.
[Groups]
comment = Groups Directories
path = /home/samba/groups
writeable = Yes
browseable = no
veto files = /*.bat/*.cmd/*.com/*.cpl/*.exe/*.hta/*.inf/*.ins/*.isp/
*.msi/*.msp/*.pif/*.reg/*.scr/*.shs/*.vb/*.vbs/*.wsc/

# Partage ou seront exécuté des logiciels (un "Program files" en réseau).
[Softwares]
comment = Softwares
path = /home/samba/softwares
browseable = no
read only = yes
write list = @Administrators
create mask = 0644
directory mask = 0755

# Partage qui contiendra tous les raccourcis vers les
# applications du menu Démarrer de Windows.
[StartMenu]
comment = Windows Start Menu
path = /home/samba/startmenu
browseable = no
read only = yes
write list = @Administrators
create mask = 0644
directory mask = 0775

# Partage qui contiendra les fichiers Partimage de vos stations Windows
# et Linux déjà configurés, afin éviter de les installer un par un.
[Partimage]
comment = Partimage Share
path = /home/samba/partimage
browseable = no
writable = yes
valid users = @Administrators
create mask = 0664
directory mask = 0775

# File d'impression intermédiaire envoyée au serveur CUPS.
[printers]
comment = All Printers
path = /var/spool/samba
browseable = no
```

```
printable = yes
writable = no
create mode = 0700

# Le partage [print$] sert uniquement à stocker les pilotes des
# imprimantes sur le serveur Samba.
# Comme nous fonctionnerons en mode RAW, nous n'en avons pas besoin.
```

Créez les répertoires des partages Samba avec les droits en écriture selon vos groupes :

```
fs1:~# mkdir -p /home/samba/netlogon /home/samba/groups
/home/samba/softwares /home/samba/startmenu /home/samba/partimage

fs1:~# chmod 775 /home/samba/*

fs1:~# chgrp 'Account Operators' /home/samba/netlogon
fs1:~# chgrp Administrators /home/samba/softwares
fs1:~# chgrp Administrators /home/samba/startmenu
fs1:~# chgrp Administrators /home/samba/partimage
```

Vous pouvez utiliser un script sur le serveur de fichiers pour créer automatiquement les home directories des utilisateurs.
Créez le fichier /home/samba/mk_homedirectories_from_ldap.sh et rendez-le exécutable :

```
#!/bin/bash

for home in $(ldapsearch -x -b ou=Users,dc=alex,dc=fr -LLL homeDirectory
| grep ^'homeDirectory: /home/' | cut -d ' ' -f 2)
do
        if [ ! -d $home ]
        then
                cp -r /etc/skel $home
                chmod -R 700 $home
                chown -R $(basename $home) $home
        fi
done
```

Vous pouvez l'exécuter toutes les 15 minutes avec crontab, créez le fichier /etc/cron.d/mk_homedirectories_from_ldap :

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin
MAILTO=root
HOME=/

*/15 * * * * root /home/samba/mk_homedirectories_from_ldap.sh
```

Stoppez Samba :

```
fs1:~# /etc/init.d/samba stop
Stopping Samba daemons: nmbd smbd.
```

Effacez le fichier Samba qui contient les mots de passe :

```
fs1:~# rm -f /var/lib/samba/secrets.tdb
```

Configurez le SID Windows de Samba (celui que vous avez saisi dans le fichier /etc/smbldap-tools/smbldap.conf) :

```
fs1:~# net setlocalsid S-1-5-21-663340348-4107433757-3291108422
```

Donnez à Samba le mot de passe du compte LDAP pour qu'il puisse lire :

```
fs1:~# smbpasswd -W
Setting stored password for "uid=ldapadmin,ou=Users,dc=alex,dc=fr" in
secrets.tdb
New SMB password:
Retype new SMB password:
fs1:~#
```

Vérifiez que le SID est bien le même que celui saisi plus haut :

```
fs1:~# net getlocalsid
SID for domain FS is: S-1-5-21-663340348-4107433757-3291108422
fs1:~#
```

Démarrez les trois serveurs Samba (le serveur fs2.alex.lan sera configuré dans un autre tutoriel) :

```
fs1:~# /etc/init.d/samba start
Starting Samba daemons: nmbd smbd.
fs1:~#

pdc:~# /etc/init.d/samba start
Starting Samba daemons: nmbd smbd.
pdc:~#

bdc:~# /etc/init.d/samba start
Starting Samba daemons: nmbd smbd.
bdc:~#
```

Configuration de Samba sur pdc.alex.lan (suite)

Pour ajouter un utilisateur (Posix et Windows) dans l'annuaire en ligne de commande

avec smbldap-tools :

```
pdc:~# smbldap-useradd -a -n -P testuser
Changing UNIX and samba passwords for testuser
New password:
Retype new password:
pdc:~#
```

Pour visualiser cet utilisateur avec smbldap-tools :

```
pdc:~# smbldap-usershow testuser
```

Pour ajouter un groupe avec smbldap-tools :

```
pdc:~# smbldap-groupadd ungroupe
```

Pour visualiser ce groupe avec smbldap-tools :

```
pdc:~# smbldap-groupshow ungroupe

dn: cn=ungroupe,ou=Groups,dc=alex,dc=fr
objectClass: top,posixGroup
cn: ungroupe
gidNumber: 2000
```

Mapper un groupe Posix avec un groupe Windows

Informations de mappage créées automatiquement par le script smbldap-populate :

```
pdc:~# net groupmap list
Domain Admins (S-1-5-21-663340348-4107433757-3291108422-512) -> Domain
Admins
Domain Users (S-1-5-21-663340348-4107433757-3291108422-513) -> Domain Users
Domain Guests (S-1-5-21-663340348-4107433757-3291108422-514) -> Domain
Guests
Domain Computers (S-1-5-21-663340348-4107433757-3291108422-515) -> Domain
Computers
Administrators (S-1-5-32-544) -> Administrators
Account Operators (S-1-5-32-548) -> Account Operators
Print Operators (S-1-5-32-550) -> Print Operators
Backup Operators (S-1-5-32-551) -> Backup Operators
Replicators (S-1-5-32-552) -> Replicators
pdc:~#
```

Commande pour mapper le groupe Posix "ungroupe" avec le groupe Windows "Domain Policy Admins" (voir le tableau de mappages des groupes pour la valeur du RID) :

```
pdc:~# net groupmap add rid=520 unixgroup=ungroupe type=domain
ntgroup="Domain Policy Admins"

Successfully added group Domain Policy Admins to the mapping db as a
domain group
```

Pour visualiser les changements :

```
pdc:~# net groupmap list
Domain Admins (S-1-5-21-663340348-4107433757-3291108422-512) -> Domain
Admins
Domain Users (S-1-5-21-663340348-4107433757-3291108422-513) -> Domain Users
Domain Guests (S-1-5-21-663340348-4107433757-3291108422-514) -> Domain
Guests
Domain Computers (S-1-5-21-663340348-4107433757-3291108422-515) -> Domain
Computers
Administrators (S-1-5-32-544) -> Administrators
Account Operators (S-1-5-32-548) -> Account Operators
Print Operators (S-1-5-32-550) -> Print Operators
Backup Operators (S-1-5-32-551) -> Backup Operators
Replicators (S-1-5-32-552) -> Replicators
Domain Policy Admins (S-1-5-21-663340348-4107433757-3291108422-520) ->
ungroupe
pdc:~#

pdc:~# smbldap-groupshow ungroupe

dn: cn=ungroupe,ou=Groups,dc=alex,dc=fr
objectClass: top,posixGroup,sambaGroupMapping
cn: ungroupe
gidNumber: 2000
sambaSID: S-1-5-21-663340348-4107433757-3291108422-520
sambaGroupType: 2
displayName: Domain Policy Admins
description: Domain Unix group
pdc:~#
```

Compte pour joindre les machines Windows au domaine

Nous allons créer un compte nommé "junctionuser" qui servira uniquement à joindre les machines Windows au domaine. Il n'aura pas de home directory, de shell, de répertoire de base ni de profil :

```
pdc:~# smbldap-useradd -a -n -d /dev/null -s /bin/false -P -C /dev/null -
F /dev/null junctionuser
Changing UNIX and samba passwords for junctionuser
New password:
Retype new password:
pdc:~#
```

Jusque-là ce compte n'a aucun pouvoir. Nous allons lui donner le droit de joindre les machines Windows grâce à une délégation locale (non dans l'annuaire)

Listez des délégations par défaut (en s'authentifiant avec le compte administrateur créé plus haut) :

```
pdc:~# net rpc rights list accounts -U administrateur
Password:
BUILTIN\Print Operators
No privileges assigned

BUILTIN\Account Operators
No privileges assigned

BUILTIN\Backup Operators
No privileges assigned

BUILTIN\Server Operators
No privileges assigned

BUILTIN\Administrators
SeMachineAccountPrivilege
SeTakeOwnershipPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeRemoteShutdownPrivilege
SePrintOperatorPrivilege
SeAddUsersPrivilege
SeDiskOperatorPrivilege

Everyone
No privileges assigned
```

Listez les délégations par défaut pour le compte "junctionuser" (aucune) :

```
pdc:~# net rpc rights list junctionuser -U administrateur
Password:
pdc:~#
```

On lui donne le droit de joindre les machines Windows :

```
pdc:~# net rpc rights grant junctionuser SeMachineAccountPrivilege -U
administrateur
Password:
Successfully granted rights.
```

Listez les délégations pour le compte "junctionuser" :

```
pdc:~# net rpc rights list junctionuser -U administrateur
Password:
SeMachineAccountPrivilege
pdc:~#
```

Pour supprimer une délégation :

```
pdc:~# net rpc rights revoke junctionuser SeMachineAccountPrivilege -U
administrateur
Password:
Successfully revoked rights.
pdc:~#
```

Gérer graphiquement les comptes dans les annuaires OpenLDAP

Vous pouvez installer sur votre poste de travail une interface Web comme phpldapadmin pour gérer les données de vos annuaires.
Par défaut des formulaires de saisies sont disponible pour créer des entrées LDAP (Unité d'organisation OU, groupe Posix, compte Posix et Samba, ...), vous pouvez créer vos propres formulaires sur mesure.

J'ai créé trois formulaires pour mes besoins, par contre ils utilisent les schémas mail.schema et proxy-ftp.schema contenant des attributs mail (ce schéma sera expliqué dans le tutoriel Postfix) et des attributs permettant l'accès au Proxy et au serveur FTP de notre entreprise.

Aperçu en images :

(pour mieux voir l'image faites un clic droit dessus et Afficher l'image)

phpLDAPadmin - 0.9.8.4

Accueil | Purger les caches
Demander une fonctionnalité | Signaler une anomalie
Donation | Aide

pdc.alex.lan [alex.fr]
(schéma | rechercher | rafraîchir | info | importer | exporter | se déconnecter)
Connecté en tant que : uid=ldapadmin,ou=Users

- dc=alex,dc=fr (7)
  - cn=NextFreeUnixId
  - ou=Computers (2)
  - ou=Domains (1)
  - ou=Groups (10)
  - ou=Users (12)
    - Créer une nouvelle entrée ici
    - uid=abuse
    - uid=administrateur
    - uid=arnofear
    - uid=blackhole
    - uid=junctionuser
    - uid=ldapadmin
    - uid=ldapreplicateur
    - uid=liste
    - uid=nobody
    - uid=superviseur
    - uid=testuser
    - uid=userfr
    - Créer une nouvelle entrée ici
  - sambaDomainName=ALEX
  - sambaDomainName=FS
- Créer une nouvelle entrée ici

ldap1.alex.dmz [alex.com]
Connexion...

ldap1.alex.dmz [alex.org]
Connexion...

Créer un objet

Choisissez un modèle

Sélectionner un modèle pour le processus de création

Serveur: pdc.alex.lan [alex.fr]

Modèle:

Compte Posix Etch	Samba Domain
Compte Samba Etch	Samba3 Account
Domaine mail	Samba3 Group Mapping
Address Book Entry	Samba3 Group Mapping - SUSE
Address Book Entry (mozillaOrgPerson)	Samba3 Machine
Courier Mail Account	Sendmail Alias
Courier Mail Alias	Sendmail Cluster
DNS Entry	Sendmail Domain
Kolab User Entry	Sendmail Relays
LDAP Alias	Sendmail Virtual Domain
Organisational Role	Sendmail Virtual Users
Organisational Unit	Simple Security Object
Posix Group	User Account
Posix Group - SUSE	**Custom**

Proceed >>

Créer un objet

Serveur: **pdc.alex.lan [alex.fr]** en utilisant le modèle: **arnofear.free.fr_SambaEtchAccount**

Nouveau Compte Samba (3.0.24) Etch

Container DN:	ou=Users,dc=alex,dc=fr parcourir
Nom de famille:	*
Prénom:	
Nom détaillé:	*
Nom affiché (displayName):	
Nom affiché (gecos):	
Initial:	
Login (uid):	*
Mot de passe:	ssha
Vérifier Mot de passe:	
LanMan Password:	
NT Password:	
Login shell:	/bin/bash
Home directory:	*
GID Number:	Domain Users
UID Number:	10012 * (hint: NE PAS CHANGER (calcul du SID) !)
Compte mail Actif:	*
mail:	(hint: Ajoutez votre domaine)
Alias mail:	
Transfert vers un autre compte mail:	(hint: Choisir mailForwarding ou mail,mailAlias)
Service:	
N° d'employé:	
Fonction:	
N° Téléphone:	
N° Téléphone mobile:	
N° Pager:	
N° Fax:	
Adresse:	
Boite postale:	
Ville:	
Département/Région:	
Code postal:	
N° Téléphone personnel:	
Adresse personnelle:	
Répertoire de base Samba:	\\FS\homes
Lettre du lecteur Windows pour Samba:	H:
Script de Logon Samba:	logon.bat
Changer de mot de passe à la 1er connexion:	(hint: Saisir zéro)
Liste des machines sur lesquelles l'utilisateur peut se connecter:	(hint: Nom NetBIOS séparé par des virgules)
Samba Primary Group SID:	S-1-5-21-663340348-4107433757-3291108422-512 (Domain Admins)
Samba SID:	S-1-5-21-663340348-4107433757-3291108422 (ALEX)
Autoriser l'accès Web par le Proxy:	*
Compte FTP Actif:	* (hint: Accès au serveur FTP de l'entreprise)

Proceed >>

Installation du package
phpldapadmin

Modifiez le fichier /etc/phpldapadmin/config.php pour ajouter vos différents annuaires :

```
<?php

/*********************************************/
/* Useful important configuration overrides  */
/*********************************************/

/* If you are asked to put pla in debug mode, this is how you do it: */
#  $config->custom->debug['level'] = 255;
#  $config->custom->debug['syslog'] = true;
#  $config->custom->debug['file'] = '/tmp/pla_debug.log';

/* phpLDAPadmin can encrypt the content of sensitive cookies if you set
this to a big random string. */
$config->custom->session['blowfish'] = '';

/*********************************************/
/* Define your LDAP servers in this section  */
/*********************************************/

$i=0;
$ldapservers = new LDAPServers;

/* A convenient name that will appear in the tree viewer and throughout
phpLDAPadmin to identify this LDAP server to users. */
$ldapservers->SetValue($i,'server','name','pdc.alex.lan [alex.fr]');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
            (Unix socket at /usr/local/var/run/ldap) */
//$ldapservers->SetValue($i,'server','host','127.0.0.1');
//$ldapservers->SetValue($i,'server','host','ldap://pdc.alex.lan/');
$ldapservers->SetValue($i,'server','host','ldaps://pdc.alex.lan/');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $ldapservers->SetValue($i,'server','port','389');
$ldapservers->SetValue($i,'server','port','636');

/* Array of base DNs of your LDAP server. Leave this blank to have
phpLDAPadmin auto-detect it for you. */
//$ldapservers->SetValue($i,'server','base',array('dc=example,dc=com'));
$ldapservers->SetValue($i,'server','base',array('dc=alex,dc=fr'));

$ldapservers->SetValue($i,'server','auth_type','session');

/* Use TLS (Transport Layer Security) to connect to the LDAP server. */
$ldapservers->SetValue($i,'server','tls',false);

/* This feature allows phpLDAPadmin to automatically determine the next
```

```
available uidNumber for a new entry. */
$ldapservers->SetValue($i,'auto_number','enable',true);

/* The mechanism to use when finding the next available uidNumber. Two
possible values: 'uidpool' or 'search'. The 'uidpool' mechanism uses an
existing uidPool entry in your LDAP server to blindly lookup the next
available uidNumber. The 'search' mechanism searches for entries with a
uidNumber value and finds the first available uidNumber (slower). */
// Le mécanisme uidpool ne fonctionne pas pour la pool créée par smbldap-
tools.
$ldapservers->SetValue($i,'auto_number','mechanism','search');

/* The DN of the search base when the 'search' mechanism is used above.
*/
// $ldapservers-
>SetValue($i,'auto_number','search_base','ou=People,dc=example,dc=com');
$ldapservers->SetValue($i,'auto_number','search_base','dc=alex,dc=fr');

/* The minimum number to use when searching for the next available UID
number (only when 'search' is used for auto_uid_number_mechanism' */
// Dans notre exemple les uid commencent à 10000.
$ldapservers->SetValue($i,'auto_number','min','10000');

/* The DN of the uidPool entry when 'uidpool' mechanism is used above. */
// $servers[$i]['auto_uid_number_uid_pool_dn'] =
'cn=uidPool,dc=example,dc=com';
// $servers[$i]['auto_uid_number_uid_pool_dn'] =
'cn=NextFreeUnixId,dc=alex,dc=fr';

/**********************************************************************
* If you want to configure additional LDAP servers, do so below.
*
* Remove the commented lines and use this section as a template for all
*
* your other LDAP servers.
*
**********************************************************************
*/

// Pour administrer la base dc=alex,dc=com sur le serveur ldap1.alex.dmz.
$i++;
$ldapservers->SetValue($i,'server','name','ldap1.alex.dmz [alex.com]');
$ldapservers->SetValue($i,'server','host','ldaps://ldap1.alex.dmz/');
$ldapservers->SetValue($i,'server','port','636');
$ldapservers->SetValue($i,'server','base',array('dc=alex,dc=com'));
$ldapservers->SetValue($i,'server','auth_type','session');
$ldapservers->SetValue($i,'server','tls',false);
$ldapservers->SetValue($i,'auto_number','enable',true);
$ldapservers->SetValue($i,'auto_number','mechanism','search');
$ldapservers-
>SetValue($i,'auto_number','search_base','ou=Users,dc=alex,dc=com');
$ldapservers->SetValue($i,'auto_number','min','20000');

// Pour administrer la base dc=alex,dc=org sur le serveur ldap1.alex.dmz.
$i++;
$ldapservers->SetValue($i,'server','name','ldap1.alex.dmz [alex.org]');
$ldapservers->SetValue($i,'server','host','ldaps://ldap1.alex.dmz/');
$ldapservers->SetValue($i,'server','port','636');
```

```
$ldapservers->SetValue($i,'server','base',array('dc=alex,dc=org'));
$ldapservers->SetValue($i,'server','auth_type','session');
$ldapservers->SetValue($i,'server','tls',false);
$ldapservers->SetValue($i,'auto_number','enable',true);
$ldapservers->SetValue($i,'auto_number','mechanism','search');
$ldapservers-
>SetValue($i,'auto_number','search_base','ou=Users,dc=alex,dc=org');
$ldapservers->SetValue($i,'auto_number','min','30000');


/*********************************************/
/* User-friendly attribute translation       */
/*********************************************/

/* Use this array to map attribute names to user friendly names. For
example, if you don't want to see "facsimileTelephoneNumber" but rather
"Fax". */
$friendly_attrs = array();

$friendly_attrs['facsimileTelephoneNumber'] = 'Fax';
$friendly_attrs['telephoneNumber']          = 'Phone';

/*********************************************/
/* Predefined Queries (canned views)         */
/*********************************************/

/* To make searching easier, you may setup predefined queries below: */
$q=0;
$queries = array();

/* The name that will appear in the simple search form */
$queries[$q]['name'] = 'User List';

/* The base to search on */
$queries[$q]['base'] = 'dc=alex,dc=fr';

/* The search scope (sub, base, one) */
$queries[$q]['scope'] = 'sub';

/* The LDAP filter to use */
$queries[$q]['filter'] = '(&(objectClass=posixAccount)(uid=*))';

/* The attributes to return */
$queries[$q]['attributes'] = 'cn, uid, homeDirectory';

/* If you want to configure more pre-defined queries, copy and paste the
above (including the "$q++;") */
$q++;
$queries[$q]['name'] = 'Samba Users';
$queries[$q]['base'] = 'ou=Users,dc=alex,dc=fr';
$queries[$q]['scope'] = 'sub';
$queries[$q]['filter'] = '(&(|(objectClass=sambaAccount)
(objectClass=sambaSamAccount))
(objectClass=posixAccount)(!(uid=*$)))';
$queries[$q]['attributes'] = 'uid, smbHome, uidNumber';

$q++;
$queries[$q]['name'] = 'Samba Computers';
```

```
$queries[$q]['base'] = 'ou=Computers,dc=alex,dc=fr';
$queries[$q]['scope'] = 'sub';
$queries[$q]['filter'] = '(&(objectClass=sambaAccount)(uid=*$))';
$queries[$q]['attributes'] = 'uid, homeDirectory';
?>
```

Copiez les certificats ldaps (*cert.pem) depuis pdc.alex.lan vers votre station Linux dans le répertoire /etc/ldap/tls/ que vous aurez créé avant. Puis redémarrez apache2.

Le formulaire "Compte Samba Etch" crée automatiquement le SambaSID utilisateur à partir du SID du domaine Samba (SID+uidNumber).

Placez les trois formulaires suivants dans le répertoire "templates" de phpldapadmin (/etc/phpldapadmin/templates/) et changez les droits :

```
root@kubuntu:/home/arno# chown root:www-data /etc/phpldapadmin/templates/
*

root@kubuntu:/home/arno# chmod 640
/etc/phpldapadmin/templates/arnofear.free.fr_*
```

Dans votre navigateur, tapez l'adresse : http://localhost/phpldapadmin

Pour que les formulaires soient pris en compte, vous devez purger les caches depuis l'interface de phpldapadmin : "Purger les caches"

Sources :
http://www.zytrax.com/books/ldap/ch7/#ol-syncrepl

Document mis à jour : 19/12/08