Authentification des utilisateurs avec OpenLDAP et Samba 3.0

Ce tutoriel développe la mise en place d'un contrôleur de Domaine Principal (PDC) couplet avec un contrôleur de Domaine de Réplication (BDC) basé sur une authentification POSIX/Samba.
Le PDC et BDC dirigeront les Profiles des utilisateurs vers un serveur de fichiers Samba commun.

Le homedirectory des clients Linux (/home/*utilisateur*) sera monté après l'authentification depuis un des serveurs de fichiers Samba. Puis il sera démonté à leur déconnexion.

La racine principale de l'annuaire sera nommée : **dc=alex,dc=fr**
dc pour domain controler, **alex** comme nom du domaine et **fr** pour France.

Pour que les clients Windows puissent être identifiés par le contrôleur de domaine, il faudra configurer l'annuaire LDAP comme base de donnée centralisée d'utilisateurs puis la mettre en relation avec les modules d'authentification Unix, à savoir PAM et NSS puis Samba.

Installation des packages OpenLDAP

Mandrake	debian
Pour les Serveurs Contrôleurs de domaine : openldap2.2-2.2.17-1mdk openldap2.2-clients-2.2.17-1mdk openldap2.2-servers-2.2.17-1mdk openldap2.2-migration-2.2.17-1mdk (pour le master seulement) libldap2.2_7-2.2.17-1mdk libdb4.2-4.2.52-6mdk pam_ldap-170-3mdk nss_ldap-220-3mdk samba-common-3.0.10-0.1.101mdk samba-server-3.0.10-0.1.101mdk samba-client-3.0.10-0.1.101mdk samba-doc-3.0.10-0.1.101mdk (pour le samba.schema) Pour les Serveurs de Fichiers : openldap2.2-2.2.17-1mdk libldap2.2_7-2.2.17-1mdk pam_ldap-170-3mdk nss_ldap-220-3mdk samba-common-3.0.10-0.1.101mdk samba-server-3.0.10-0.1.101mdk Pour les Clients Linux : openldap2.2-2.2.17-1mdk libldap2.2_7-2.2.17-1mdk pam_ldap-170-3mdk nss_ldap-220-3mdk samba-common-3.0.10-0.1.101mdk samba-client-3.0.10-0.1.100mdk libsmbclient0-3.0.10-0.1.100mdk pam_mount-0.9.20-1mdk.i586mdk lsof-4.68-1mdk	Pour les Serveurs Contrôleurs de domaine : slapd_2.2.23-5_i386.deb ldap-utils_2.2.23-5_i386.deb libldap2_2.1.30-8_i386.deb libdb4.2_4.2.52-18_i386.deb libnss-db_2.2-6.2_i386.deb libdbd-ldap-perl_0.05-1_all.deb migrationtools_46-1_all.deb (pour le master seulement) libnss-ldap_238-1_i386.deb libpam-ldap_178-1_i386.deb libpam-cracklib_0.76-22_i386.deb samba_3.0.14a-1_i386.deb samba-common_3.0.14a-1_i386.deb samba-doc_3.0.14a-1_all.deb (pour le samba.schema) smbldap-tools_0.8.7-4_all.deb Pour les Serveurs de Fichiers : libnss-ldap_238-1_i386.deb libpam-ldap_178-1_i386.deb libpam-cracklib_0.76-22_i386.deb libldap2_2.1.30-8_i386.deb samba_3.0.14a-1_i386.deb samba-common_3.0.14a-1_i386.deb Pour les Clients Linux : libnss-ldap_238-1_i386.deb libpam-ldap_178-1_i386.deb libpam-cracklib_0.76-22_i386.deb libldap2_2.1.30-8_i386.deb samba-common_3.0.14a-1_i386.deb libsmbclient_3.0.14a-1_i386.deb smbfs_3.0.14a-1_i386.deb libpam-mount_0.9.22-6_i386.deb

Configuration d'OpenLDAP

Mandrake	debian
Le fichier **/etc/openldap2.2/slapd.conf**	Le fichier **/etc/ldap/slapd.conf**

comporte diverses informations telles que la racine supérieure de l'annuaire, l'administrateur principal de l'annuaire LDAP et son mot de passe, les droits d'accès par défaut, les fichiers d'objets et de syntaxe à utiliser ainsi que les règles d'accès (ACL) pour les entrées et les attributs de l'annuaire LDAP.
Compte tenu que ce fichier contient le mot de passe de l'administrateur de l'annuaire, il est impératif de positionner les droits « rw------- » sur le fichier slapd.conf :

```
[root@srv2 user]# chmod 600 /etc/openldap2.2/slapd.conf
```

Mandrake

Modifiez le fichier **/etc/openldap2.2/slapd.conf**

```
# $OpenLDAP: pkg/ldap2.2/servers/slapd/slapd.conf,v 1.8.8.6 2001/04/20
23:32:43 kurt Exp $

include  /usr/share/openldap2.2/schema/core.schema
include  /usr/share/openldap2.2/schema/cosine.schema
include  /usr/share/openldap2.2/schema/corba.schema
include  /usr/share/openldap2.2/schema/inetorgperson.schema
include  /usr/share/openldap2.2/schema/java.schema
include  /usr/share/openldap2.2/schema/krb5-kdc.schema
include  /usr/share/openldap2.2/schema/kerberosobject.schema
include  /usr/share/openldap2.2/schema/misc.schema
include  /usr/share/openldap2.2/schema/nis.schema
include  /usr/share/openldap2.2/schema/openldap.schema
include  /usr/share/openldap2.2/schema/autofs.schema
# Pour qu'OpenLDAP utilise les bonnes informations concernant
# la version de Samba, copiez le fichier :
# /usr/share/doc/samba-doc-3.0.10/examples/LDAP/samba.schema
# vers /etc/openldap2.2/schema/samba-3.0.10.schema.
include /etc/openldap2.2/schema/samba-3.0.10.schema
include /usr/share/openldap2.2/schema/kolab.schema
include /usr/share/openldap2.2/schema/evolutionperson.schema
include /usr/share/openldap2.2/schema/calendar.schema
include /usr/share/openldap2.2/schema/sudo.schema
include /usr/share/openldap2.2/schema/dnszone.schema
include /usr/share/openldap2.2/schema/dhcp.schema

#include /usr/share/openldap2.2/schema/rfc822-MailMember.schema
#include /usr/share/openldap2.2/schema/pilot.schema
#include /usr/share/openldap2.2/schema/qmail.schema
#include /usr/share/openldap2.2/schema/mull.schema
#include /usr/share/openldap2.2/schema/netscape-profile.schema
#include /usr/share/openldap2.2/schema/trust.schema
#include /usr/share/openldap2.2/schema/dns.schema
#include /usr/share/openldap2.2/schema/cron.schema

include  /etc/openldap2.2/schema/local.schema

# Inclusion du fichier slapd.access.conf contenant les ACLs
include  /etc/openldap2.2/slapd.access.conf

# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral        ldap://root.openldap.org

pidfile          /var/run/ldap2.2/slapd.pid
argsfile         /var/run/ldap2.2/slapd.args

modulepath /usr/lib/openldap
#moduleload back_dnssrv.la
#moduleload back_ldap.la
#moduleload back_meta.la
```

```
#moduleload back_monitor.la
#moduleload back_passwd.la
#moduleload back_sql.la

# SASL config
#sasl-host ldap.example.com
# To allow TLS-enabled connections.
#TLSRandFile /dev/random
#TLSCipherSuite HIGH:MEDIUM:+SSLv2
#TLSCACertificatePath /etc/ssl/openldap2.2/
#TLSCACertificateFile /etc/ssl/openldap2.2/ldap_cert.pem
# Pour activer ldaps sur votre annuaire, décommenté ces 2 lignes
# et reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
#TLSCertificateFile /etc/ssl/openldap2.2/ldap_cert.pem
#TLSCertificateKeyFile /etc/ssl/openldap2.2/ldap_key.pem
# Si vous souhaitez que votre annuaire vérifie si les clients
# possèdent bien un certificat valide :
#TLSVerifyClient demand # ([never]|allow|try|demand)

# Niveau des informations de logs.
loglevel 256

# Vérification de la structure des objectClasses définis
# dans les fichiers .schema inclus plus haut.
schemacheck on

########################################
# database definitions
########################################

database bdb

# Définition de la racine du serveur.
suffix "dc=alex,dc=fr"

# Définition du compte d'administration ici Manager
# c'est un nom arbitraire et ce n'est pas forcément un
# utilisateur défini dans /etc/passwd du système.
rootdn "cn=Manager,dc=alex,dc=fr"

#mot de passe en clair est « mypassword », voir plus loin comment le
crypter
rootpw   {crypt}ijFYNcSNctBYg

# The database directory MUST exist prior to running slapd AND
# should only be accessable by the slapd/tools. Mode 700 recommende.
directory        /var/lib/ldap2.2

# Tuning settings, please see the man page for slapd-bdb for more
# information as well as the DB_CONFIG file in the database directory
# commented entries are at their defaults
# In-memory cache size in entries
cachesize 1000
# Checkpoint the bdb database after 256kb of writes or 15 minutes have
# passed since the last checkpoint
checkpoint 256 15
```

```
# Liste des attributs à indexer pour une recherche plus rapide.
# Ils sont dépendant de la version de samba.schema
index  objectClass,uidNumber,gidNumber,memberUid  eq
index  sambaSID,sambaPrimaryGroupSID              eq
index  mail,surname,givenname                     eq,subinitial
index  cn,uid                                     pres,sub,eq
index  default                                    sub

# Indique le format du cryptage, ici {crypt}
password-hash   {crypt}
password-crypt-salt-format      "$1$%.8s"


# Si vous ne souhaitez pas mettre en place un serveur principal
# avec un serveur de réplication, effacez les lignes suivantes :

# DEBUT Configuration du PDC/Master LDAP
# Créez le répertoire /var/lib/ldap/replog
replogfile /var/lib/ldap/replog/slurp.log
#
# Il est fortement conseillé d'utiliser une connexion sécurisée
# avec ldaps, sinon vos données seront lisible sur le réseau.
# Vous devez générer une clef et un certificat pour le serveur Maître et
# une autre clef et certificat pour le serveur Replica.
# Respectez les tabulations, elles font parties de la syntaxe !
# sinon vous aurez des erreurs et la réplication ne pourra pas se faire !
# Indiquez l'adresse du serveur replica.
# replica uri=ldap://srv6.alex.fr:389
replica uri=ldaps://srv6.alex.fr:636
     binddn=cn=Manager,dc=alex,dc=fr
     bindmethod=simple credentials=mypassword
     tls=yes
#
# FIN Configuration du PDC/Master LDAP
#

# Pour le BDC copiez tout le contenu du fichier slapd.conf
# (sauf la partie réservée au PDC/Master LDAP) et ajoutez ceci :
#
# DEBUT Configuration du BDC/Slave LDAP
updatedn        "cn=Manager,dc=alex,dc=fr"
#
# Echangez les certificats entre le Master et le replica, pour que
# chacun ait une copie. Sinon la négociation SSL échouera.
# Indiquez l'adresse du serveur Maître.
# updateref      "ldap://srv2.alex.fr"
updateref       "ldaps://srv2.alex.fr"
#
# FIN Configuration du BDC/Slave LDAP
```

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

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

# 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 utilise les bonnes informations concernant
# la version de Samba, extraire le fichier :
# /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz
# vers /etc/ldap/schema/samba-3.0.14a-1.schema.
include         /etc/ldap/schema/samba-3.0.14a-1.schema

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

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck     on

# 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.args

# To allow TLS-enabled connections.
# et reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
#TLSCertificateFile /etc/ssl/openldap/ldap_cert.pem
#TLSCertificateKeyFile /etc/ssl/openldap/ldap_key.pem
# Si vous souhaitez que votre annuaire vérifie si les clients
# possèdent bien un certificat valide :
#TLSVerifyClient demand # ([never]|allow|try|demand)

# Read slapd.conf(5) for possible values
loglevel        256

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

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

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

# Définition de la racine du serveur.
suffix "dc=alex,dc=fr"

# Définition du compte d'administration ici Manager
# c'est un nom arbitraire et ce n'est pas forcément un
# utilisateur défini dans /etc/passwd du système
rootdn "cn=Manager,dc=alex,dc=fr"

# mot de passe en clair est « mypassword », voir plus loin comment le
crypter
rootpw   {crypt}ijFYNcSNctBYg

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

# Liste des attributs à indexer pour une recherche plus rapide.
# Ils sont dépendant de la version de samba.schema
index  objectClass,uidNumber,gidNumber,memberUid  eq
index  sambaSID,sambaPrimaryGroupSID              eq
index  mail,surname,givenname                     eq,subinitial
index  cn,uid                                     pres,sub,eq
index  default                                    sub

# Indique le format du cryptage, ici {crypt}
password-hash   {crypt}
password-crypt-salt-format      "$1$%.8s"

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

# Si vous ne souhaitez pas mettre en place un serveur principal
# avec un serveur de réplication, effacez les lignes suivantes :

# DEBUT Configuration du PDC/Master LDAP
# Créez le répertoire /var/lib/ldap/replog
replogfile /var/lib/ldap/replog/slurp.log
#
# Il est fortement conseillé d'utiliser une connexion sécurisée
# avec ldaps, sinon vos données seront lisible sur le réseau.
# Vous devez générer une clef et un certificat pour le serveur Maître et
# une autre clef et certificat pour le serveur Replica.
# Respectez les tabulations, elles font parties de la syntaxe !
# sinon vous aurez des erreurs et la réplication ne pourra pas se faire !
# Indiquez l'adresse du serveur replica.
# replica uri=ldap://srv6.alex.fr:389
replica uri=ldaps://srv6.alex.fr:636
     binddn=cn=Manager,dc=alex,dc=fr
     bindmethod=simple credentials=mypassword
     tls=yes
```

```
#
# FIN Configuration du PDC/Master LDAP
#

# Pour le BDC copiez tout le contenu du fichier slapd.conf
# (sauf la partie réservée au PDC/Master LDAP) et ajoutez ceci :
#
# DEBUT Configuration du BDC/Slave LDAP
updatedn        "cn=Manager,dc=alex,dc=fr"
#
# Echangez les certificats entre le Master et le replica, pour que
# chacun ait une copie. Sinon la négociation SSL échouera.
# Indiquez l'adresse du serveur Maître.
# updateref       "ldap://srv2.alex.fr"
updateref       "ldaps://srv2.alex.fr"
#
# FIN Configuration du BDC/Slave LDAP
```

Le mot de passe de l'administrateur est «mypassword» en clair, pour le crypter au format {CRYPT}, il faudra taper (exemple avec mypassword) :

```
[root@pc user]# slappasswd -v -s mypassword -h {CRYPT}
{CRYPT}G.H5krNMMw0cc
```

Mandrake	debian
Modifiez le fichier **/etc/openldap2.2/slapd.access.conf**	Créez le fichier **/etc/ldap/slapd.access.conf**

Pour le PDC/Master LDAP

```
# ACLs authentification PDC POSIX/SAMBA
# Respectez les tabulations, elles font parties de la syntaxe !

# La racine DIT doit être accessible pour tout les clients.
access to dn.exact="" by * read

# Protection de l'attribut userPassword dans tout l'annuaire.
access to attribute=userPassword
     by self write
     by dn="cn=admin,dc=alex,dc=fr" write
     by anonymous auth
     by * none

# Protection des passwords et informations Samba dans la branche
# "ou=People,dc=alex,dc=fr".
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=sambaLMPassword,sambaNTPassword,sambaPwdLastSet,
sambaPwdMustChange,sambaPasswordHistory
     by self write
     by dn="cn=admin,dc=alex,dc=fr" write
     by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
     by anonymous auth
     by * none

# ACL permettant à l'admin de l'annuaire et au groupe
# Domain Controllers d'ajouter des utilisateurs dans cette branche.
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=entry,children,posixAccount,sambaSamAccount
     by dn="cn=admin,dc=alex,dc=fr" write
     by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
     by users read
     by anonymous read

# ACL permettant à l'admin de l'annuaire et au groupe
# Domain Controllers d'ajouter des groupes dans cette branche.
access to dn.children="ou=Group,dc=alex,dc=fr"
     attrs=entry,children,posixGroup,sambaGroupMapping
     by dn="cn=admin,dc=alex,dc=fr" write
     by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
     by users read
     by anonymous read

# ACL permettant aux utilisateurs de modifier leurs attributs mail et
# telephoneNumber.
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=mail,telephoneNumber
     by self write
     by dn="cn=admin,dc=alex,dc=fr" write
```

```
     by users read
     by anonymous read

# ACL permettant à l'admin de l'annuaire d'ajouter des hôtes dans cette
branche.
access to dn.children="ou=Hosts,dc=alex,dc=fr"
     attrs=entry,children,ipHost,device
     by dn="cn=admin,dc=alex,dc=fr" write
     by users read
     by anonymous read
```

Pour le BDC/Slave LDAP

```
# ACLs Authentification BDC POSIX/SAMBA
# Le replica doit être en lecture seule.
# OpenLDAP ne gère pas encore la réplication bidirectionnelle.

# Respectez les tabulations, elles font parties de la syntaxe !

# La racine DIT doit être accessible pour tout les clients.
access to dn.exact="" by * read

# Protection de l'attribut userPassword dans tout l'annuaire.
access to attribute=userPassword
     by self write
     by dn="cn=admin,dc=alex,dc=fr" write
     by anonymous auth
     by * none

# Protection des passwords et informations Samba dans la branche
# "ou=People,dc=alex,dc=fr".
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=sambaLMPassword,sambaNTPassword,sambaPwdLastSet,
sambaPwdMustChange,sambaPasswordHistory
     by self read
     by dn="cn=admin,dc=alex,dc=fr" write
     by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
     by anonymous auth
     by * none

# ACL permettant à l'admin de l'annuaire et au groupe
# Domain Controllers d'ajouter des utilisateurs dans cette branche.
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=entry,children,posixAccount,sambaSamAccount
     by dn="cn=admin,dc=alex,dc=fr" write
     by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
     by users read
     by anonymous read

# ACL permettant à l'admin de l'annuaire et au groupe
# Domain Controllers d'ajouter des groupes dans cette branche.
access to dn.children="ou=Group,dc=alex,dc=fr"
     attrs=entry,children,posixGroup,sambaGroupMapping
     by dn="cn=admin,dc=alex,dc=fr" write
     by group="cn=Domain Controllers,ou=Group,dc=alex,dc=fr" write
     by users read
     by anonymous read

# ACL NE permettant pas aux utilisateurs de modifier leurs attributs
# mail et telephoneNumber.
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=mail,telephoneNumber
     by self read
     by dn="cn=admin,dc=alex,dc=fr" write
     by users read
     by anonymous read

# ACL permettant à l'admin de l'annuaire d'ajouter des hôtes dans cette
```

```
branche.
access to dn.children="ou=Hosts,dc=alex,dc=fr"
     attrs=entry,children,ipHost,device
     by dn="cn=admin,dc=alex,dc=fr" write
     by users read
     by anonymous read
```

Pour le bon fonctionnement de LDAP vous devez copier le fichier samba.schema avant de lancer le daemon (voir installation de Samba 3.0)

Créez un fichier appelé initial.ldif sur le PDC qui contiendra les informations nécessaires au fonctionnement de votre annuaire LDAP.
Vous disposez aussi d'outils avec le package **smbldap-tools** (voir Smbldap-tools) pour créer les informations initiales dans votre annuaire LDAP et administrer facilement la création, modification et l'effacement de comptes.
Sinon pour des consoles graphiques, utilisez **une interface de gestion** comme GQ, web avec LAM et phpLDAPadmin ou java comme Xjplorer.

```
dn: dc=alex,dc=fr
dc: alex
objectClass: top
objectClass: dcObject
objectClass: domain
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Serveur OpenLDAP alex

# admin, alex.fr
dn: cn=admin,dc=alex,dc=fr
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: administrateur annuaire LDAP
userPassword:: e2NyeXB01ga57VElZN2h3cmM=

dn: ou=People,dc=alex,dc=fr
ou: People
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Utilisateurs du Domaine

dn: ou=Group,dc=alex,dc=fr
ou: Group
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Groupes du Domaine

dn: ou=Hosts,dc=alex,dc=fr
ou: Hosts
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: alex.fr
description: Hosts du Domaine
```

Reportez vous à la page "Création et Gestion de l'annuaire" pour son utilisation.
Ainsi qu'au chapitre "Migration des données POSIX vers LDAP".

Configurez les autres fichiers du serveur PDC et BDC selon les explications du chapitre "Mappage de l'annuaire LDAP avec les modules d'authentification Unix".
Configurez le BDC comme un serveur.

Réplication de l'annuaire LDAP vers le serveur BDC/Slave

Votre serveur LDAP Master et Slave doivent d'etre capable de résoudre leur FQDN mutuellement.
Le champs CN des certificats SSL (ldaps) contient leur FQDN et sera vérifié durant les négociations.
Ajoutez l'IP des serveurs de chaque cotés :

```
[root@srv6 root]# echo "192.168.0.2 srv2.alex.fr srv2" >> /etc/hosts
>---<
[root@srv2 root]# echo "192.168.0.6 srv6.alex.fr srv6" >> /etc/hosts
```

ATTENTION le serveur LDAP Slave doit être arrêté avant de réaliser les commandes suivantes

Passez l'annuaire du serveur LDAP **Master** (*srv2*) en lecture seule :

Mandrake	debian

`[root@srv2 root]# echo "readonly on" >> /etc/openldap2.2/slapd.conf`
 	
`[root@srv2 root]# service ldap2.2 restart`
` Arrêt du serveur LDAP : [  OK  ]`
` Arrêt du serveur de propagation pour LDAP (slurpd) : [ECHEC]`
` ldaps`
` Lancement du serveur LDAP (ldap + ldaps) : [  OK  ]`
` Lancement du serveur de propagation pour LDAP (slurpd) : [  OK  ]`
`[root@srv2 root]#`
	`srv2:~# echo "readonly on" >> /etc/ldap/slapd.conf`
	
	`srv2:~# /etc/init.d/slapd restart`
	`Stopping OpenLDAP: slurpd slapd – failed`
	`Starting OpenLDAP: slapd slurpd.`
	`Srv2:~#`

Faites une copie de la database du serveur LDAP Master (*srv2*) sur le serveur LDAP Slave (*srv6*) **depuis le serveur LDAP Slave** :

Connexion non sécurisée :

```
srv6:~# ldapsearch -x -LLL -H ldap://srv2.alex.fr -D
"cn=Manager,dc=alex,dc=fr" -w mypassword | slapadd -c;slapindex
```

Ou connexion sécurisée :

```
srv6:~# ldapsearch -x -LLL -H ldaps://srv2.alex.fr -D
"cn=Manager,dc=alex,dc=fr" -w mypassword | slapadd -c;slapindex
```

Vérifiez si la réplication c'est bien déroulée sur le serveur LDAP **Slave** :

```
[root@srv6 root]# ll /var/lib/ldap*/
[root@srv6 root]# (Affichage de vos db)
```

Mandrake

Changez les droits sur le contenu du répertoire /var/lib/ldap/ car OpenLDAP fonctionne sous le compte "ldap" sur la Mandrake.

```
[root@srv6 root]# chown ldap:ldap /var/lib/ldap2.2/*
```

Relancez le serveur LDAP **Master** toujours en lecture seule :

Mandrake	debian
[root@srv2 root]# service ldap2.2 restart Arrêt du serveur LDAP : [OK] Arrêt du serveur de propagation pour LDAP (slurpd) : [OK] ldaps Lancement du serveur LDAP (ldap + ldaps) : [OK] Lancement du serveur de propagation pour LDAP (slurpd) : [OK]	srv2:~# /etc/init.d/slapd restart Stopping OpenLDAP: slurpd slapd. Starting OpenLDAP: slapd slurpd. Srv2:~#

Relancez le serveur LDAP Master en lecture-écriture :

Mandrake	debian
[root@srv2 root]# perl -pi -e 's/^readonly on/#readonly on/g' /etc/openldap2.2/slapd.conf [root@srv2 root]# service ldap2.2 restart Arrêt du serveur LDAP : [OK] Arrêt du serveur de propagation pour LDAP (slurpd) : [OK] ldaps Lancement du serveur LDAP (ldap + ldaps) : [OK] Lancement du serveur de propagation pour LDAP (slurpd) : [OK]	srv2:~# perl -pi -e 's/^readonly on/#readonly on/g' /etc/ldap/slapd.conf srv2:~# /etc/init.d/slapd restart Stopping OpenLDAP: slurpd slapd. Starting OpenLDAP: slapd slurpd. Srv2:~#

Lancez le serveur LDAP **Slave** :

Mandrake	debian
[root@srv6 root]# service ldap2.2 start	srv6:~# /etc/init.d/slapd start

Vérifiez que la réplication se fait dés modification de l'annuaire Master en ajoutant ou modifiant une entrée.

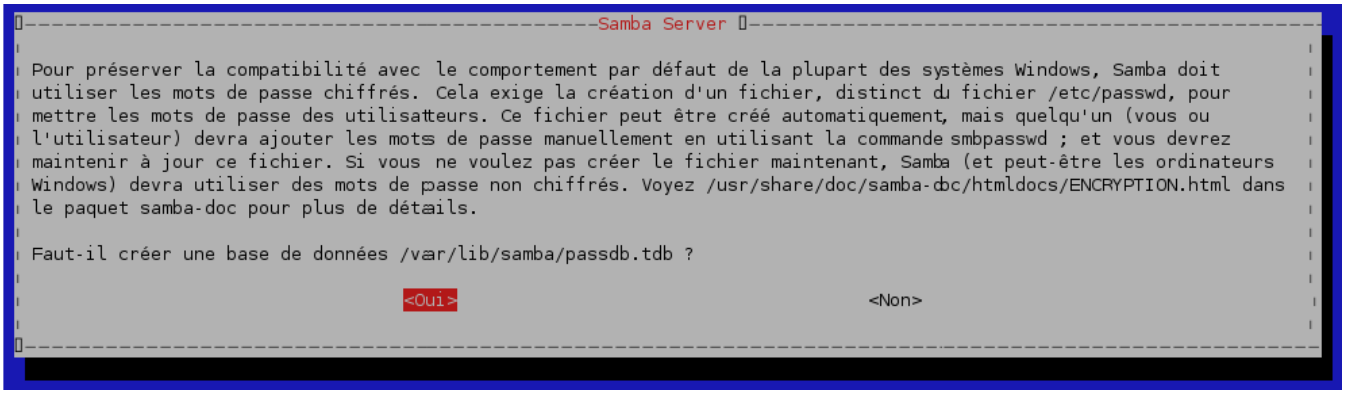
Puis tapez cette commande sur le serveur LDAP Master :

Mandrake	debian
[root@srv2 root]# slurpd -f /etc/openldap2.2/slapd.conf -d 64	srv2:~# slurpd -f /etc/ldap/slapd.conf -d 64

Vous devriez obtenir les informations suivantes (Ctrl-c pour terminer)

```
...
Config: (objectclass ( 1.3.6.1.4.1.7165.2.2.13 NAME 'sambaPrivilege' SUP
top AUXILIARY DESC 'Samba Privilege' MUST ( sambaSID ) MAY
( sambaPrivilegeList ) ))
Config: ** configuration file successfully read and parsed
Config: (schemacheck     on)
Config: (pidfile         /var/run/slapd/slapd.pid)
Config: (argsfile        /var/run/slapd.args)
Config: (loglevel        256)
Config: (modulepath     /usr/lib/ldap)
Config: (moduleload     back_bdb)
Config: (TLSCertificateFile /etc/ssl/openldap/ldap_cert.pem)
Config: (TLSCertificateKeyFile /etc/ssl/openldap/ldap_key.pem)
Config: (backend                 bdb)
Config: (database        bdb)
Config: (suffix          "dc=alex,dc=fr")
Config: (rootdn "cn=Manager,dc=alex,dc=fr")
Config: (rootpw mypassword)
Config: (directory       "/var/lib/ldap")
Config: (index objectClass,uidNumber,gidNumber,memberUid eq)
Config: (index sambaSID,sambaPrimaryGroupSID,sambaDomainName eq)
Config: (index mail,surname,givenname eq,subinitial)
Config: (index cn,uid,displayName pres,sub,eq)
Config: (index default sub)
Config: (password-hash {crypt})
Config: (password-crypt-salt-format "$1$%.8s")
Config: (lastmod         on)
Config: (replogfile     /var/lib/ldap/replog/slurp.log)
Config: (replica uri=ldaps://srv6.alex.fr:636
binddn="cn=Manager,dc=alex,dc=fr" bindmethod=simple credentials=mypassword
tls=yes)
Config: ** successfully added replica "srv6.alex.fr:636"
Config: (include /etc/ldap/slapd.access.conf)
...
Config: (access to * by self read by * none)
Config: ** configuration file successfully read and parsed
slurpd: terminated.
```

Installation de Samba 3.0.x



smb.conf

Dans cet exemple je crée un répertoire **/home/samba** sur le premier serveur de fichiers Samba "share-linux".

Il contiendra 3 sous répertoires :
/home/samba/netlogon (répertoire pour les différents fichiers de logon)
/home/samba/partage (répertoire Public réservé au groupe users)
/home/samba/profiles (ou seront stocké les profiles des utilisateurs windows)

Le PDC et BDC dirigeront les profiles vers un serveur de fichiers Samba, qui sera pour plus de sécurité mirroré sur un second serveur de fichiers.

La synchronisation entre les deux serveurs de fichiers Samba sera exécutée par Unison.

Un script "maison" sur chaque serveurs de fichiers Samba permettra :
- sur le premier serveur de fichiers de voir s'il est toujours actif.
- sur le deuxième serveur de fichiers de voir si le premier est mort et dans ce cas de démarrer ses daemons Samba pour le remplacer et envoyer un mail d'alerte (sous entend que vous avez installé un serveur mail sur celui-ci).

Quand le premier serveur de fichiers ne répondra plus le second prend sa place en lançant Samba. Dans l'objectif de **prendre son nom NetBIOS** sans changer d'IP.
Le service Samba se rafraîchit toutes les minutes, de ce fait si le premier serveur de fichiers ne répond plus alors que des clients Windows sont connectés sur lui, en 1 minute maximum la connexion sera rétablie sur le deuxième serveur de fichiers (mit à jour quelques minutes au par avant)

Créez vos fichiers smb.conf dans le répertoire /etc/samba/

Sur le serveur **PDC** Il devra ressembler à celui ci :

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

# workgroup = NT-Domain-Name or Workgroup-Name
   workgroup = ALEX

# netbios name is the name you will see in "Network Neighbourhood"
   netbios name = PDC-LINUX

   server string = Samba Server %v

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

   max log size = 5

# Security and Domain Membership Options:

   hosts allow = 127.0.0.1 192.168.0.0/16
   hosts deny = 0.0.0.0/0

   interfaces = eth* lo
   bind interfaces only = yes

   security = user

   encrypt passwords = yes

   passwd program = /usr/bin/passwd %u
   passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n

   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

   local master = yes

   os level = 64

   domain master = yes

# Preferred Master causes Samba to force a local browser election
# on startup and gives it a slightly higher chance of winning
# the election.
;  preferred master = yes

   domain logons = yes

# Le logon script est stocké sur le serveur Samba share-linux
   logon script = \\share-linux\netlogon\logon.bat

# %L substitutes for this servers netbios name, %U is username
# Le Profile des utilisateurs est stocké sur le serveur share-linux.
   logon path = \\share-linux\Profiles\%U
   logon home = \\share-linux\%U
   logon drive = U:
```

Mandrake	debian
# Scripts de gestion des comptes du domaine entre Samba et OpenLDAP. # Configurez le fichier : **/etc/samba/smbldap_conf.pm**	# Scripts de gestion des comptes du domaine entre Samba et OpenLDAP. # Configurez les fichiers : **/etc/smbldap-tools/smbldap.conf** et # **/etc/smbldap-tools/smbldap_bind.conf**

```
add machine script = /usr/sbin/smbldap-useradd -w -d /dev/null -c 'Machine
Account' -s /bin/false %u
add user script = /usr/sbin/smbldap-useradd -a -m '%u'
delete user script = /usr/sbin/smbldap-userdel -r '%u'
; ldap delete dn = Yes
add group script = /usr/sbin/smbldap-groupadd -g '%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'

# LDAP configuration for Domain Controlling:
# Lancez cette commande pour que Samba puisse lire et écrire
# dans l'annuaire : smbpasswd -w mypassword

   ldap admin dn = cn=Manager,dc=alex,dc=fr
   ldap suffix = dc=alex,dc=fr
   ldap passwd sync = yes

   ldap user suffix = ou=People
   ldap group suffix = ou=Group
   ldap machine suffix = ou=People
   ldap idmap suffix = ou=People

# Connexion à l'annuaire en localhost, puisque
# Samba est sur la même machine que OpenLDAP.
   passdb backend = ldapsam:ldap://localhost
   idmap backend = ldap:ldap://localhost


# DNS Proxy - tells Samba whether or not to try to resolve
# NetBIOS names via DNS nslookups.
   dns proxy = no


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

# Nous ne définissons pas de zones partagées puisque [netlogon]
# les [Profiles] et [public] se trouvent sur le serveur de
# fichiers Samba share-linux.
```

Sur le serveur **BDC** Il devra ressembler à celui la :

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

# workgroup = NT-Domain-Name or Workgroup-Name
   workgroup = ALEX

# netbios name is the name you will see in "Network Neighbourhood"
   netbios name = BDC-LINUX

   server string = Samba Server %v

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

   max log size = 5

# Security and Domain Membership Options:

   hosts allow = 127.0.0.1 192.168.0.0/16
   hosts deny = 0.0.0.0/0

   interfaces = eth* lo
   bind interfaces only = yes

   security = user

   encrypt passwords = yes

   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

   os level = 64

   domain master = no

# Preferred Master causes Samba to force a local browser election
# on startup and gives it a slightly higher chance of winning
# the election.
;  preferred master = yes

   domain logons = yes

# Le logon script est stocké sur le serveur Samba share-linux
   logon script = \\share-linux\netlogon\logon.bat

# %L substitutes for this servers netbios name, %U is username
# Le Profile des utilisateurs est stocké sur le serveur share-linux.
   logon path = \\share-linux\Profiles\%U
   logon home = \\share-linux\%U
   logon drive = U:
```

Mandrake	debian
# Scripts de gestion des comptes du domaine entre Samba et OpenLDAP. # Configurez le fichier : **/etc/samba/smbldap_conf.pm**	# Scripts de gestion des comptes du domaine entre Samba et OpenLDAP. # Configurez les fichiers : **/etc/smbldap-tools/smbldap.conf** et # **/etc/smbldap-tools/smbldap_bind.conf**

```
add machine script = /usr/sbin/smbldap-useradd -w -d /dev/null -c 'Machine
Account' -s /bin/false %u; sleep 5

# LDAP configuration for Domain Controlling:
# Lancez cette commande pour que Samba puisse lire et écrire
# dans l'annuaire : smbpasswd -w mypassword

   ldap admin dn = cn=Manager,dc=alex,dc=fr
   ldap suffix = dc=alex,dc=fr
   ldap passwd sync = yes

   ldap user suffix = ou=People
   ldap group suffix = ou=Group
   ldap machine suffix = ou=People
   ldap idmap suffix = ou=People

# Connexion à l'annuaire en localhost, puisque
# Samba est sur la même machine que OpenLDAP.
   passdb backend = ldapsam:ldap://localhost
   idmap backend = ldap:ldap://localhost


# DNS Proxy - tells Samba whether or not to try to resolve NetBIOS names
via DNS nslookups.
   dns proxy = no


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

# Nous ne définissons pas de zones partagées puisque [netlogon]
# les [Profiles] et [public] se trouvent sur le serveur de
# fichiers Samba share-linux.
```

Reportez vous aux explications du chapitre "Mappage de l'annuaire LDAP avec les modules d'authentification Unix" pour configurer les serveurs **de Fichiers** comme des **clients**.

La configuration des serveurs **de Fichiers** Samba sera identique et devra ressembler à celle ci :

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

# workgroup = NT-Domain-Name or Workgroup-Name
   workgroup = ALEX
```

```
# netbios name is the name you will see in "Network Neighbourhood"
   netbios name = SHARE-LINUX

   server string = Samba Server %v

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

   max log size = 5

# Security and Domain Membership Options:

   hosts allow = 127.0.0.1 192.168.0.0/16
   hosts deny = 0.0.0.0/0

   interfaces = eth* lo
   bind interfaces only = yes

   security = user

   encrypt passwords = yes

   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

# set local master to no if you don't want Samba to become
# a master browser on your network.
# Otherwise the normal election rules apply.
;  local master = no

   domain master = no

# LDAP configuration for Domain Controlling:
# Lancez cette commande pour que Samba puisse lire et écrire
# dans l'annuaire : smbpasswd -w mypassword

   ldap admin dn = cn=Manager,dc=alex,dc=fr
   ldap suffix = dc=alex,dc=fr
   ldap passwd sync = yes

   ldap user suffix = ou=People
   ldap group suffix = ou=Group
   ldap machine suffix = ou=People
   ldap idmap suffix = ou=People

# Nous indiquons les noms FQDN des deux serveurs OpenLDAP, car
# la vérification du certificat risque d'échouer s'il y a une
# adresse IP à la place.
# La connexion à l'annuaire se fera par ldaps, car le mot de passe
# du Manager OpenLDAP circule en clair lors d'une requête standard.
# Reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
   passdb backend = ldapsam:"ldaps://srv2.alex.fr ldaps://srv6.alex.fr"
   idmap backend = ldap:"ldaps://srv2.alex.fr ldaps://srv6.alex.fr"
# Si malgré tout vous souhaitez utiliser ldap non sécurisé :
# passdb backend = ldapsam:"ldap://srv2.alex.fr ldap://srv6.alex.fr"
# idmap backend = ldap:"ldap://srv2.alex.fr ldap://srv6.alex.fr"

# On active SSL (option par défaut)
```

```
   ldap ssl = on

# DNS Proxy - tells Samba whether or not to try to resolve
# NetBIOS names via DNS nslookups.
   dns proxy = no


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

 [homes]
   comment = Home Directories
   browseable = no
   writable = yes
   valid users = %S

# N'oubliez pas de donner les droits en écriture sur ces
# répertoires, sinon vous aurez un message depuis les stations
# Windows$ "Impossible d'écrire le profil ..."
# Vous pouvez ajouter chaque utilisateurs au groupe "users" dans
# l'annuaire LDAP et changer le groupe des répertoires :
# drwxr--r--  2 root root  4096 août  3 09:23 netlogon/
# drwxrwxr--  2 root users 4096 août  3 11:41 partage/
# drwxrwxr--  3 root users 4096 août  6 10:59 profiles/

 [netlogon]
   comment = Network Logon Service
   path = /home/samba/netlogon
   writeable = no
   share modes = no
   read only = yes
   write list = @adm

 [Profiles]
   path = /home/samba/profiles
   browseable = no
   writeable = yes
   create mask = 0600
   directory mask = 0700

 [public]
   comment = Repertoire Commun Users
   path = /home/samba/partage
   public = yes
   writable = yes
   printable = no
   write list = @users
```

Si vous utilisez Samba comme serveur WINS sur votre PDC, assurez vous que vous avez configurez le BDC en tant que client WINS.

Vous pouvez copier smbldap_conf.pm du PDC vers le BDC, en vérifiant les valeurs de $slaveLDAP et $masterLDAP (voir Smbldap-tools)

Le logon script dans cet exemple permet de monter un lecteur réseau appelé Public sous la lettre P:

Il sera crée sur le premier serveur de fichiers "share-linux", voici son contenu :

```
net use P: \\share-linux\public
```

Installation et configuration d'Unison

Pour le **premier Serveur de Fichiers** :

Mandrake	debian
unison-2.9.1-4mdk.rpm	unison_2.9.1-2_i386.deb

Il n'est pas utile d'installer Unison sur les 2 serveurs de fichiers puisque Unison permet de synchroniser 2 répertoires bidirectionnellement.

Unison offre la possibilité de se connecter par SSH pour la synchronisation.
Echangez la clef public du compte root du premier serveur de fichier avec le deuxième pour ne pas avoir à saisir de mot de passe.

Créez un script sur le premier serveur de fichiers :

```
#!/bin/bash
# synchronisation.sh
unison /home ssh://srv13.alex.fr//home -group -owner -times -ui text -auto
-silent
```

le répertoire source : `/home`
le répertoire de destination en SSH : `ssh://srv13.alex.fr//home`
pour conserver les attributs des : `-group -owner`
pour conserver la même heure : `-times`
pour utiliser Unison en mode texte : `-ui text`
pour que Unison applique les choix par défaut et en silence : `-auto -silent`

Programmez l'exécution de ce script avec crontab :
`[root@srv12 user]# crontab -e` (éditeur VI => i pour insérer)
`*/15 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 * * *`
`/root/synchronisation.sh`
(exécute toutes les 15 min de 5 heure à 21 heure tous les jours du mois)
([Echap] :wq! pour enregistrer et quitter)
```
crontab: installing new crontab
[root@srv12 user]#
```

Script de surveillance "maison"

Sur le **premier** serveur de fichiers :

```
#!/bin/bash
# surveillance-master.sh
if ping -c 3 192.168.0.1 | grep -q 'Destination Host Unreachable'
then
  if ping -c 3 192.168.0.5 | grep -q 'Destination Host Unreachable'
  then
    if ping -c 3 192.168.0.7 | grep -q 'Destination Host Unreachable'
    then
      wall problem sur SHARE-Master, arret de eth0 et crond
      ifconfig eth0 down; /etc/init.d/crond stop
    else
      echo 3em ping positif, mais pas le 2em
    fi
  else
    echo 2em ping positif, mais pas le 1er
  fi
else
  echo 1er ping positif, tout va bien
fi
```

Programmez l'exécution de ce script avec crontab :
`[root@srv12 user]# crontab -e` (éditeur VI => i pour insérer)
`*/2 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 * * *`
`/root/surveillance-master.sh`
(exécute toutes les 2 min de 5 heure à 21 heure tous les jours du mois)
([Echap] :wq! pour enregistrer et quitter)
`crontab: installing new crontab`

Sur le **deuxième** serveur de fichiers :

```
#!/bin/bash
# surveillance-slave.sh
if ping -c 3 192.168.0.12 | grep -q 'Destination Host Unreachable'
then
  if ping -c 3 192.168.0.1 | grep -q 'Destination Host Unreachable'
  then
    if ping -c 3 192.168.0.5 | grep -q 'Destination Host Unreachable'
    then
      wall probleme sur SHARE-Slave, arret eth0 et arret crond
      ifconfig eth0 down; /etc/init.d/crond stop
    else
      if ping -c 3 192.168.0.12 | grep -q 'icmp_seq=2 Destination Host
Unreachable'
      then
        wall probleme sur SHARE-Master, lancement de Samba et arret crond.
mail envoyé
        /etc/init.d/smb start; /etc/init.d/crond stop
        echo Attention serveur fichiers SHARE1 mort. SHARE2 prend la main
> /tmp/message;mail -s alerte root@alex.fr</tmp/message;rm -f /tmp/message
      else
        echo 2em ping SHARE-Master positif, mais pas le 1er
      fi
    fi
  else
    if ping -c 3 192.168.0.12 | grep -q 'icmp_seq=2 Destination Host
Unreachable'
    then
      wall probleme sur SHARE-Master, lancement de Samba et arret crond.
mail envoyé
      /etc/init.d/smb start; /etc/init.d/crond stop
      echo Attention serveur fichiers SHARE1 mort. SHARE2 prend la main >
/tmp/message;mail -s alerte root@alex.fr</tmp/message;rm -f /tmp/message
    else
      echo 2em ping SHARE-Master positif, mais pas le 1er
    fi
  fi
else
  echo SHARE-Master vivant, tout va bien
fi
```

Programmez l'exécution de ce script avec crontab :
[root@srv13 user]# crontab -e (éditeur VI => i pour insérer)
*/2 5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21 * * *
/root/surveillance-master.sh
(exécute toutes les 2 min de 5 heure à 21 heure tous les jours du mois)
([Echap] :wq! pour enregistrer et quitter)
crontab: installing new crontab
[root@srv13 user]#

Il faut donner le mot de passe du Manager LDAP à Samba pour qu'il puisse lire et écrire dans l'annuaire. Faites le sur le PDC, le BDC et les serveurs de fichiers :

```
[root@pc root]# smbpasswd -w mypassword
Setting stored password for "cn=Manager,dc=alex,dc=fr" in secrets.tdb
```

Vérifiez sur le BDC et les serveurs de fichiers si le SID du domaine est identique avec ces commandes :
1) sur le PDC
```
[root@pdc root]# net getlocalsid
SID for domain PDC-LINUX is: S-1-5-21-7...9-2...1-5...7
```
2) sur le BDC
```
[root@bdc root]# net getlocalsid
SID for domain BDC-LINUX is: S-1-5-21-7...9-2...1-5...7
```
3) sur les serveurs de fichiers
```
[root@share root]# net getlocalsid
SID for domain SHARE-LINUX is: S-1-5-21-7...9-2...1-5...7
```

Si le SID du domaine n'était pas identique, modifiez le dans l'annuaire OpenLDAP (attribut sambaSID).

Smbldap-tools

Pour que chaque machines MS de votre réseau puissent être ajoutées automatiquement lors de la jonction au domaine, vous pouvez utiliser les fichiers smbldap-tools (contrib d'idealx.org)

Mandrake

Configurez le fichier **/etc/samba/smbldap_conf.pm** (voici le mien)
Appliquez un chmod 600 ce fichier car il contient votre password Manager LDAP.

debian

Décompresser le fichier /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz dans le répertoire /etc/smbldap-tools/
et copiez le fichier /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf avec.
Appliquez un chmod 600 sur /etc/smbldap-tools/smbldap_bind.conf car il contient votre password Manager LDAP.
Configurez ces deux fichiers (voici les miens)

Si ca ne marchait pas du premier coup, ajoutez une workstation à la main dans ldap.
Créez un fichier ws.ldif
il faut ajouter un $ a la fin du nom netBIOS de vos machines
(le gidNumber est égale a 421 car c'est le n° du group machines)

```
dn: uid=ws1$,ou=People,dc=alex,dc=fr
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
cn: ws1$
sn: ws1$
uid: ws1$
```

```
uidNumber: 1000
gidNumber: 421
homeDirectory: /dev/null
loginShell: /bin/false
description: Computer
```

et ajoutez cette machine dans Samba
```
[root@pc root]# smbpasswd -a -m ws1$
```

Vous pouvez aussi utiliser les commandes suivantes :

Pour créer les informations initiales dans l'annuaire OpenLDAP.
```
pdc:/etc/smbldap-tools# smbldap-populate
Using workgroup name from sambaUnixIdPooldn (smbldap.conf):
sambaDomainName=ALEX
Using builtin directory structure
adding new entry: dc=alex,dc=fr
adding new entry: ou=People,dc=alex,dc=fr
adding new entry: ou=Group,dc=alex,dc=fr
adding new entry: sambaDomainName=ALEX,dc=alex,dc=fr
adding new entry: uid=Administrator,ou=People,dc=alex,dc=fr
adding new entry: uid=nobody,ou=People,dc=alex,dc=fr
adding new entry: cn=Domain Admins,ou=Group,dc=alex,dc=fr
adding new entry: cn=Domain People,ou=Group,dc=alex,dc=fr
adding new entry: cn=Domain Guests,ou=Group,dc=alex,dc=fr
adding new entry: cn=Domain Computers,ou=Group,dc=alex,dc=fr
adding new entry: cn=Administrators,ou=Group,dc=alex,dc=fr
adding new entry: cn=Account Operators,ou=Group,dc=alex,dc=fr
adding new entry: cn=Print Operators,ou=Group,dc=alex,dc=fr
adding new entry: cn=Backup Operators,ou=Group,dc=alex,dc=fr
adding new entry: cn=Replicators,ou=Group,dc=alex,dc=fr
```

Pour créer un utilisateur toto dans l'annuaire OpenLDAP.
POSIX :
```
pdc:/etc/smbldap-tools# smbldap-useradd -m toto
```

POSIX + Samba :
```
pdc:/etc/smbldap-tools# smbldap-useradd -a -m toto
```

Pour attribuer un mot de passe à l'utilisateur toto.
```
pdc:/etc/smbldap-tools# smbldap-passwd toto
Changing password for toto
New password :
Retype new password :
```

Pour modifier une information (le gecos ici) sur toto.
```
pdc:/etc/smbldap-tools# smbldap-usermod -c "Toto Dupond" toto
```

Pour supprimer l'utilisateur toto.
```
pdc:/etc/smbldap-tools# smbldap-userdel -r toto
```

Et encore bien d'autres pour visualiser les comptes, créer des groupes ...

Mappage des groupes

Samba-3.* vous permet de réaliser un mappage entre les groupes UNIX et les groupes Windows.
Vous avez le choix entre mapper des groupes UNIX/Windows équivalents, comme par exemple adm avec Domain Admins ou sys avec Power Users, ...
ou bien de créer des groupes UNIX bidons qui serviront uniquement au mappage entre UNIX et Windows, comme par exemple domadmins pour Domain Admins ou powerusers avec Power Users, ...
Vous pouvez leurs attribuer des RIDs lors du mappage des groupes (pour respecter une équivalence avec Windows) ou laisser samba décider aléatoirement.

Pour réaliser ce mappage vous devez créé des groupes UNIX (extraction grace aux outils de migration ou à la main) puis taper ces commandes :

```
[root@pc root]# net groupmap add rid=512 ntgroup="Domain Admins"
unixgroup=adm
Successully added group Domain Admins to the mapping db
```

Pour vérifier :
```
[root@pc root]# net groupmap list
Domain Admins (S-1-5-21-2080767239-2881072900-3568078770-512) -> adm
```

Pour supprimer :
```
[root@pc root]# net groupmap delete ntgroup="Domain Admins"
Sucessfully removed Domain Admins from the mapping db
```

RID	Entité sous Windows	Type	Essentiel	Linux
500	Domain Administrator	Utilisateur	Non	
501	Domain Guest	Utilisateur	Non	
502	Domain KRBTGT	Utilisateur	Non	
512	Domain Admins	Groupe	Oui	adm
513	Domain Users	Groupe	Oui	users
514	Domain Guests	Groupe	Oui	nogroup
515	Domain Computers	Groupe	Non	
516	Domain Controllers	Groupe	Non	root
517	Domain Certificate Admins	Groupe	Non	
518	Domain Schema Admins	Groupe	Non	
519	Domain Entreprise Admins	Groupe	Non	
520	Domain Policy Admins	Groupe	Non	
544	Builtin Admins	Alias	Non	
545	Builtin Users	Alias	Non	
546	Builtin Guests	Alias	Non	
547	Builtin Power Users	Alias	Non	sys
548	Builtin Account Operators	Alias	Non	
549	Builtin System Operators	Alias	Non	
550	Builtin Print Operators	Alias	Non	lp
551	Builtin Backup Operators	Alias	Non	backup
552	Builtin Replicators	Alias	Non	
553	Builtin RAS Servers	Alias	Non	

Un utilisateur (UID=0) pour rejoindre votre domaine

Vous devez créer un utilisateur administratif qui autorisera les machines clientes à rejoindre votre domaine. Il pourra s'appeler n'importe comment (toto, jointdomain, adminsamba...) tant qu'il aura un UID=0 (valable uniquement pour Samba 3.xx). Je vous conseil cependant de l'appeler root pour rester cohérent avec le système classique.

dans un fichier au format LDIF placer ceci :

```
dn: uid=root,ou=People,dc=alex,dc=fr
uid: root
cn: root
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$Dbwezia0$xZQiQBqQJFliDthz90Inl.
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 0
gidNumber: 0
homeDirectory: /root
gecos: root
```

Valider un utilisateur dans Samba

Après avoir ajouté dans l'annuaire, créer son mot de passe avec Samba :

```
[root@pc root]# smbpasswd -a root
New SMB password:
Retype new SMB password:
Added user root.
[root@pc root]#
```

Vous n'avez plus qu'a créer vos utilisateurs en incrémentant leur numéro UID et normalement vos machines seront ajoutées dés leur jonction au domaine.

Montage du homedirectory des Clients depuis un serveur Samba

Les manipulations suivantes sont à réaliser sur chaque clients Linux.
Repportez vous à la Configuration des Clients OpenLDAP et NSS pour utiliser LDAP dans un premier temps.

Modifiez le fichier **/etc/pam.d/system-auth** pour ajouter les modules pam_mount (montage d'un partage distant) et pam_ldap pour l'authentification LDAP :

```
#%PAM-1.0

auth required   pam_env.so
auth required   pam_mount.so
auth sufficient pam_ldap.so use_first_pass
auth sufficient pam_unix.so use_first_pass likeauth nullok
auth required   pam_deny.so

account sufficient pam_ldap.so
account required   pam_unix.so

password required   pam_cracklib.so retry=3 min len=2 dcredit=0 ucredit=0
password sufficient pam_unix.so nullok use_authtok md5 shadow
password sufficient pam_ldap.so use_authtok
password required   pam_deny.so

session required pam_mkhomedir.so skel=/etc/skel/ umask=0026
session required pam_limits.so
session required pam_unix.so
session optional pam_mount.so
session optional pam_ldap.so
```

Modifiez le fichier **/etc/security/pam_mount.conf** pour ajouter les informations de montage :

```
# Pour afficher ou non les messages à la connexion/déconnexion.
# (en mode non graphique) Format: debug [ 1 | 0 ]
debug 0

# Pour créer le répertoire de montage.
mkmountpoint 1

# Options recommendées.
options_require  nosuid,nodev

fsckloop /dev/loop7
lsof /usr/sbin/lsof %(MNTPT)
fsck /sbin/fsck -p %(FSCKLOOP)
losetup /sbin/losetup -p0 "%(before=\"-e \" CIPHER)" "%(before=\"-k \"
KEYBITS)" %(FSCKLOOP) %(VOLUME)
unlosetup /sbin/losetup -d %(FSCKLOOP)
cifsmount /bin/mount -t cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o
"username=%(USER)%(before=\",\" OPTIONS)"
```

```
smbmount /bin/mount -t smbfs //%(SERVER)/%(VOLUME) %(MNTPT) -o
"username=%(USER)%(before=\",\" OPTIONS)"
umount   /bin/umount %(MNTPT)
mntagain /bin/mount --bind %(PREVMNTPT) %(MNTPT)

# Partage qui sera monté. les caractéres “*” et “&” remplacent le login.
# volume <user> [smb|ncp|nfs|local] <server> <volume> <mount point>
<mount options> <fs key cipher> <fs key path>
volume * smb share-linux & /home/& rw,uid=&,gid=&,fmask=750,dmask=750 - -
```

Modifiez le fichier **/etc/pam.d/common-account**

```
account required   pam_unix.so
account sufficient pam_ldap.so
```

Modifiez le fichier **/etc/pam.d/common-auth**

```
auth required   pam_env.so
auth required   pam_mount.so
auth sufficient pam_ldap.so use_first_pass
auth sufficient pam_unix.so likeauth nullok
auth required   pam_deny.so
```

Modifiez le fichier **/etc/pam.d/common-password**

```
password required   pam_cracklib.so retry=3 minlen=4 dcredit=0 ucredit=0
password sufficient pam_unix.so nullok use_authtok md5 shadow
password sufficient pam_ldap.so use_authtok
password required   pam_deny.so
```

Modifiez le fichier **/etc/pam.d/common-session**

```
session required pam_mkhomedir.so skel=/etc/skel/ umask=0026
session required pam_limits.so
session required pam_unix.so
session optional pam_mount.so
session optional pam_ldap.so
```

Le fichier **/etc/pam.d/common-pammount** n'est pas utilisé dans la configuration.

Modifiez le fichier **/etc/security/pam_mount.conf** pour ajouter les informations de montage :

```
# Pour afficher ou non les messages à la connexion/déconnexion.
# (en mode non graphique) Format: debug [ 1 | 0 ]
debug 0

# Pour créer le répertoire de montage.
mkmountpoint 1

# Options recommendées.
options_require  nosuid,nodev

fsckloop /dev/loop7
lsof /usr/bin/lsof %(MNTPT)
fsck /sbin/fsck -p %(FSCKTARGET)
losetup /sbin/losetup -p0 "%(before=\"-e \" CIPHER)" "%(before=\"-k \"
KEYBITS)" %(FSCKLOOP) %(VOLUME)
unlosetup /sbin/losetup -d %(FSCKLOOP)
cifsmount /bin/mount -t cifs //%(SERVER)/%(VOLUME) %(MNTPT) -o
"username=%(USER)%(before=\",\" OPTIONS)"
```

```
smbmount /usr/bin/smbmount   //%(SERVER)/%(VOLUME) %(MNTPT) -o
"username=%(USER)%(before=\",\" OPTIONS)"
smbumount /usr/bin/smbumount %(MNTPT)
umount   /bin/umount %(MNTPT)
mntagain /bin/mount --bind %(PREVMNTPT) %(MNTPT)

# Partage qui sera monté. les caractéres “*” et “&” remplacent le login.
# volume <user> [smb|ncp|nfs|local] <server> <volume> <mount point>
<mount options> <fs key cipher> <fs key path>
volume * smb share-linux & /home/& rw,uid=&,gid=&,fmask=750,dmask=750 - -
```

Vérifiez si vos serveurs Samba et OpenLDAP fonctionnent avant tout :
-L => le nom NetBIOS du serveur Samba.
-U => le nom d'un utilisateur Samba valide.

```
user@pc:~$ smbclient -L pdc-linux -U arnofear
Password:
Domain=[ALEX] OS=[Unix] Server=[Samba 3.0.10-Debian]

   Sharename   Type   Comment
   ---------   ----   -------
   netlogon    Disk   Network Logon Service
   IPC$        IPC    IPC Service (debian server)
   ADMIN$      IPC    IPC Service (debian server)
   arnofear    Disk   Home Directories

Domain=[ALEX] OS=[Unix] Server=[Samba 3.0.10-Debian]

   Server      Comment
   ---------   -------
   PDC-LINUX   pdc server (Samba 3.0.10-Debian)
   BDC-LINUX   bdc server (Samba 3.0.10-Debian)
   SHARE-LINUX share1 server (Samba 3.0.10-Debian)

   Workgroup   Master
   ---------   -------
   ALEX        PDC-LINUX
```

Sur le serveur de fichiers principal Samba vous devez créer les répertoires des futurs utilisateurs dans **/home/** sinon le montage ne sera pas possible. Vous devez changer les droits sur chacun d'eux :

```
share:/home# mkdir utilisateur1
share:/home# chmod 700 utilisateur1
share:/home# chown utilisateur1 utilisateur1
```

La réplication entre les serveurs de fichiers Samba se chargera de créer une copie du /home du serveur de fichiers principal.

Les comptes Windows auront leur profile distant stocké dans le répertoire (toujours d'après l'exemple) **/home/samba/** et accéderont à leur répertoire personnel (/home/*utilisateur1*) par le lecteur réseau U:
Par contre, pour que les comptes Linux voient leur profile Windows vous devez ajouter un autre volume dans le fichier **/etc/security/pam_mount.conf** :

```
...
volume * smb share-linux & /home/& rw,uid=&,gid=&,fmask=750,dmask=750 - -
volume * smb share-linux profiles /mnt/profiles
```

```
rw,uid=&,gid=&,fmask=750,dmask=750 - -
```

Dans ce cas il faudra créé un répertoire /mnt/profiles avec les droits en écriture pour les utilisateurs sur chaque postes clients.

Note : Il y a des problèmes de création de l'environnement graphique avec KDE 3.3.2-1 sous Sarge, mais Gnome et KDE 3.2xx avec KDM ou GDM fonctionne très bien.

Document mis à jour : 07/05/07