Authentification des utilisateurs avec OpenLDAP

Ce tutoriel développe la mise en place d'un contrôleur de Domaine Principal (PDC) avec authentification POSIX uniquement.
Le homedirectory des clients (/home/*utilisateur*) sera monté depuis un serveur NFS (ou Samba voir Authentification OpenLDAP/Samba).

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

Installation des packages OpenLDAP

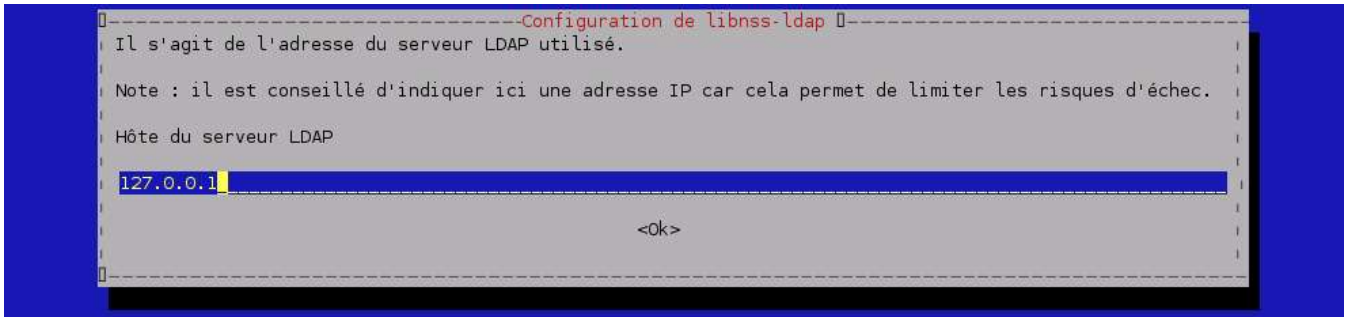
Mandrake	debian
Pour le Serveur : openldap2.2-2.2.17-1mdk openldap2.2-clients-2.2.17-1mdk openldap2.2-servers-2.2.17-1mdk openldap2.2-migration-2.2.17-1mdk libldap2.2_7-2.2.17-1mdk libdb4.2-4.2.52-6mdk pam_ldap-170-3mdk nss_ldap-220-3mdk Pour les Clients : openldap2.2-2.2.17-1mdk libldap2.2_7-2.2.17-1mdk pam_ldap-170-3mdk nss_ldap-220-3mdk	Pour le Serveur : 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 libnss-ldap_238-1_i386.deb libpam-ldap_178-1_i386.deb libpam-cracklib_0.76-22_i386.deb Pour les Clients : 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

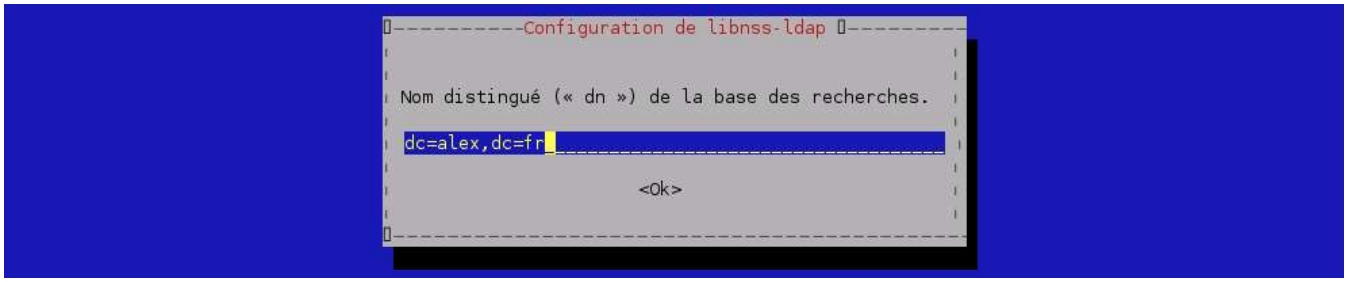

Configuration de slapd
The DNS domain name is used to construct the base DN of your LDAP directory. Entering foo.bar.org will give you the base DN dc=foo, dc=bar, dc=org.
Enter your DNS domain name
alex.fr
<Ok>


Configuration de slapd
Whatever you enter here will be stored as the name of your organization in the base DN of your LDAP directory.
Enter the name of your organization
alex.fr
<Ok>

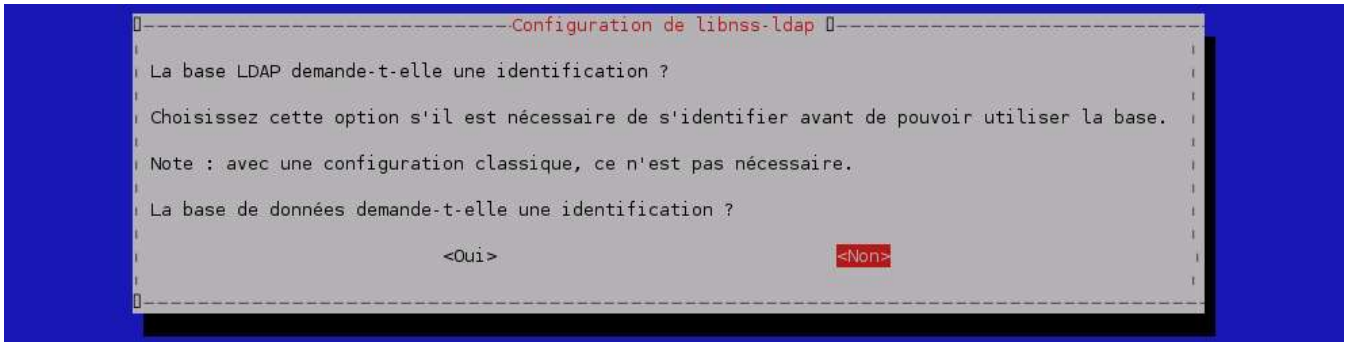

Configuration de slapd
Please enter the password for the admin entry in your LDAP directory.
Admin password
<Ok>

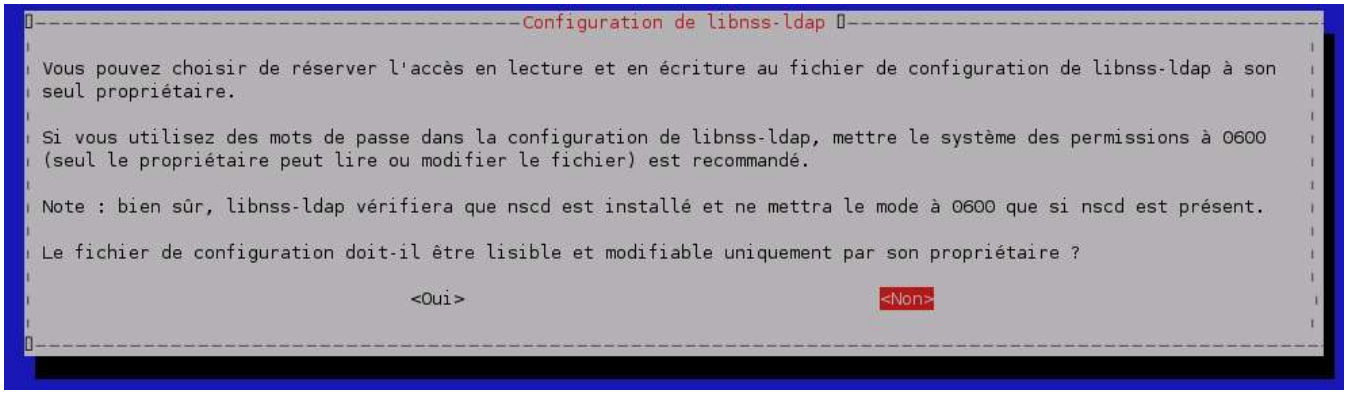

Configuration de slapd
slapd now defaults to having the old LDAPv2 protocol not allowed. Programs and users are generally expected to be upgraded to LDAPv3. If you have old programs which have not been moved to use LDAPv3 and you still need LDAPv2 support then select this option and 'allow bind_v2' will be added to your slapd.conf to tell slapd to accept LDAPv2 connections.
Allow LDAPv2 protocol
<Oui>
<Non>

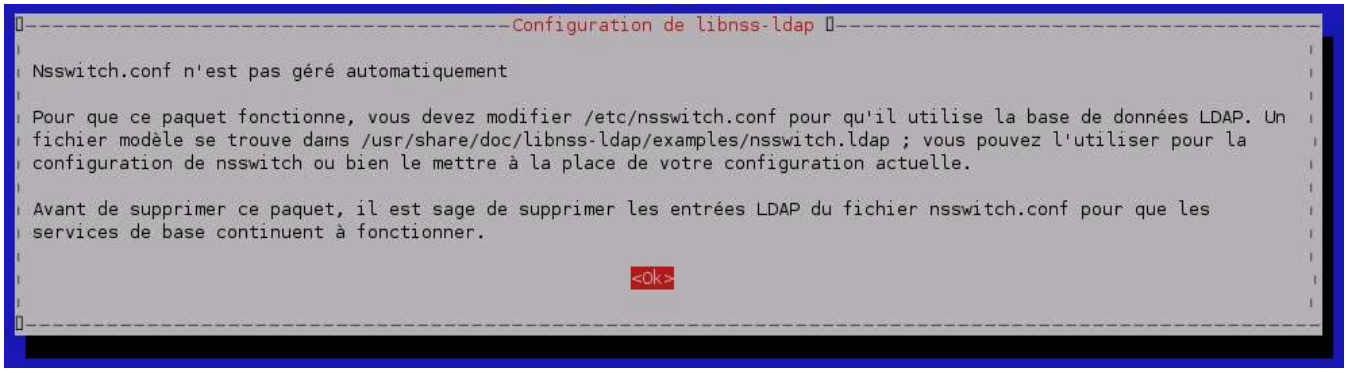

Configuration de libnss-ldap
Il s'agit de l'adresse du serveur LDAP utilisé.
Note : il est conseillé d'indiquer ici une adresse IP car cela permet de limiter les risques d'échec.
Hôte du serveur LDAP
127.0.0.1
<Ok>

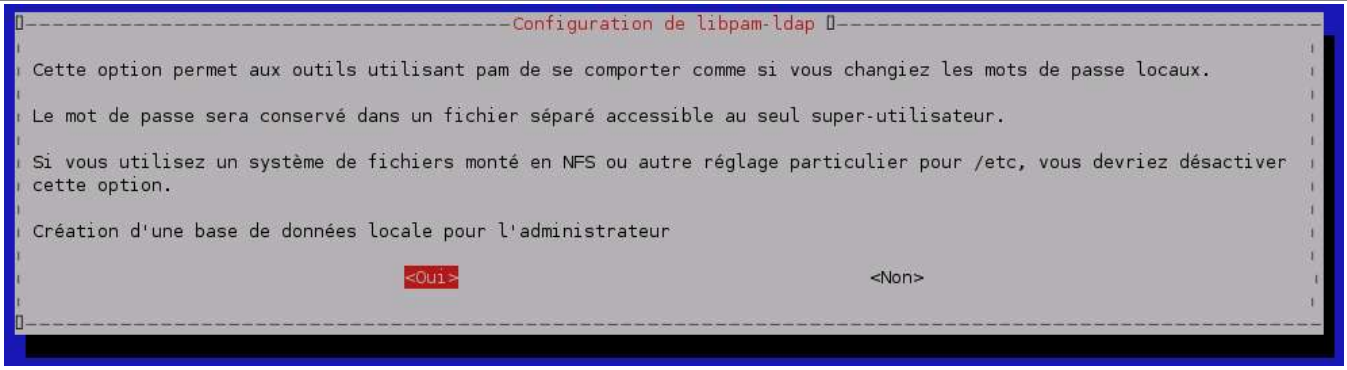

Configuration de libnss-ldap
Nom distingué (« dn ») de la base des recherches.
dc=alex,dc=fr
<Ok>

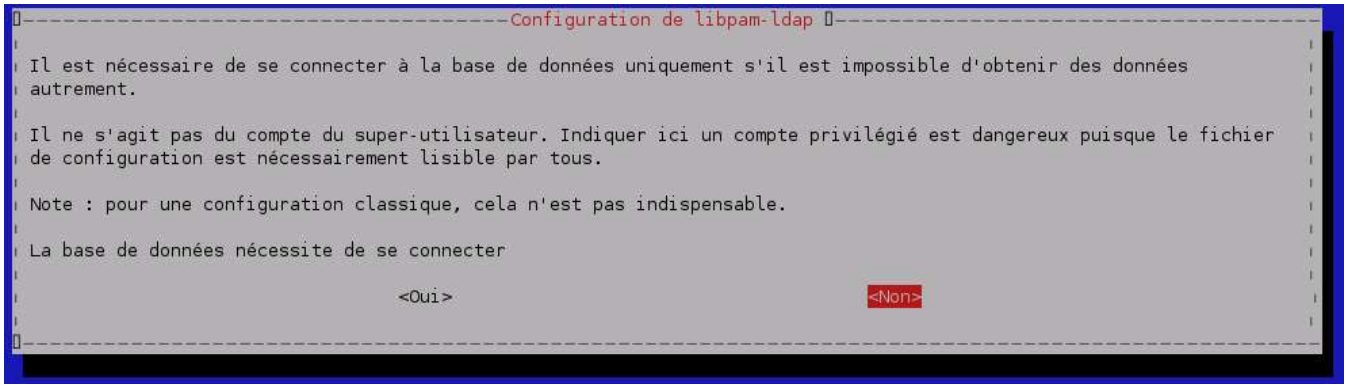

Configuration de libnss-ldap
Cette variable permet de contrôler quelle version du protocole LDAP sera utilisée avec ldapns. C'est en général une bonne idée d'indiquer ici la valeur la plus élevée possible.
Version de LDAP à utiliser
3
2
<Ok>


Configuration de libnss-ldap
La base LDAP demande-t-elle une identification ?
Choisissez cette option s'il est nécessaire de s'identifier avant de pouvoir utiliser la base.
Note : avec une configuration classique, ce n'est pas nécessaire.
La base de données demande-t-elle une identification ?
<Oui>
<Non>


Configuration de libnss-ldap
Vous pouvez choisir de réserver l'accès en lecture et en écriture au fichier de configuration de libnss-ldap à son seul propriétaire.
Si vous utilisez des mots de passe dans la configuration de libnss-ldap, mettre le système des permissions à 0600 (seul le propriétaire peut lire ou modifier le fichier) est recommandé.
Note : bien sûr, libnss-ldap vérifiera que nscd est installé et ne mettra le mode à 0600 que si nscd est présent.
Le fichier de configuration doit-il être lisible et modifiable uniquement par son propriétaire ?
<Oui>
<Non>

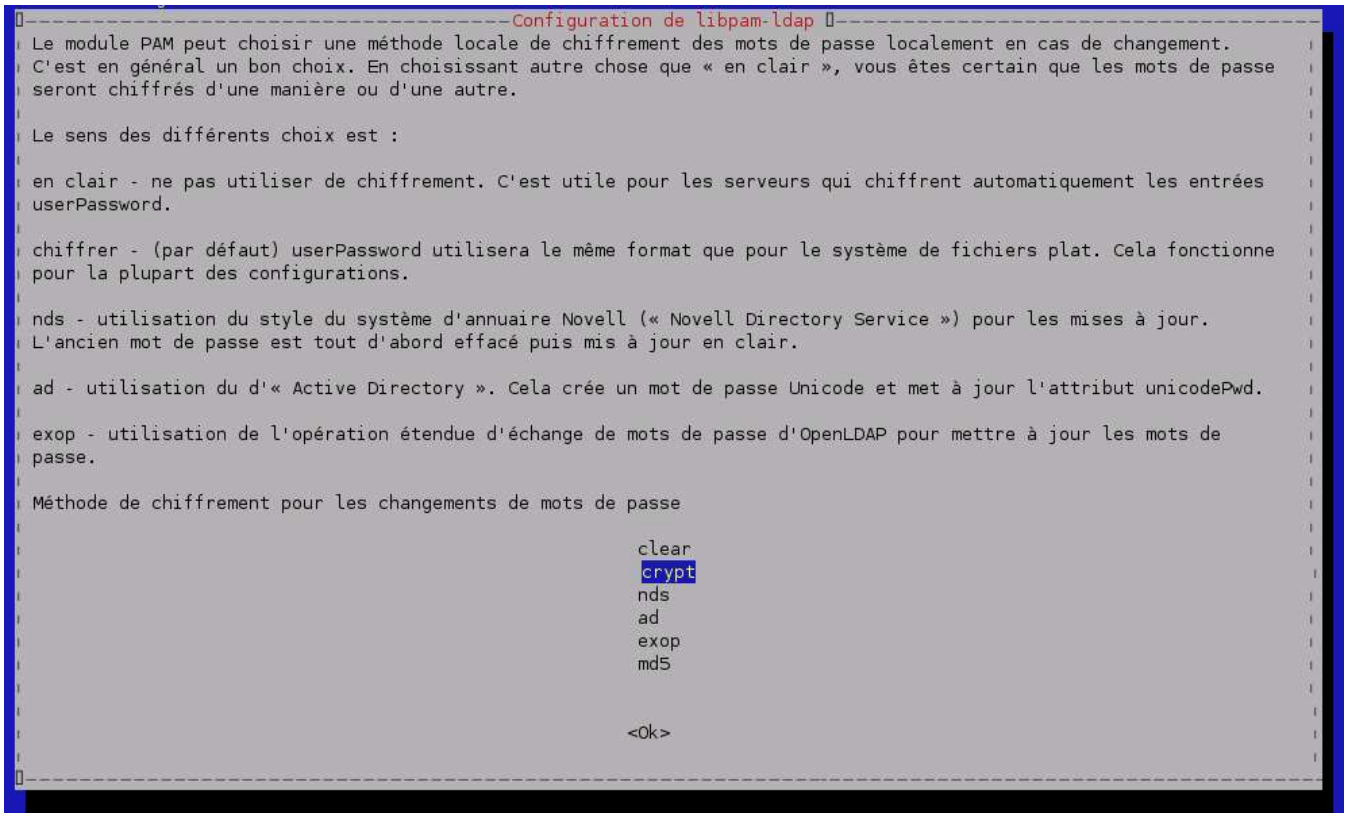

Configuration de libnss-ldap
Nsswitch.conf n'est pas géré automatiquement
Pour que ce paquet fonctionne, vous devez modifier /etc/nsswitch.conf pour qu'il utilise la base de données LDAP. Un fichier modèle se trouve dans /usr/share/doc/libnss-ldap/examples/nsswitch.ldap ; vous pouvez l'utiliser pour la configuration de nsswitch ou bien le mettre à la place de votre configuration actuelle.
Avant de supprimer ce paquet, il est sage de supprimer les entrées LDAP du fichier nsswitch.conf pour que les services de base continuent à fonctionner.
<Ok>


Configuration de libpam-ldap
Cette option permet aux outils utilisant pam de se comporter comme si vous changiez les mots de passe locaux.
Le mot de passe sera conservé dans un fichier séparé accessible au seul super-utilisateur.
Si vous utilisez un système de fichiers monté en NFS ou autre réglage particulier pour /etc, vous devriez désactiver cette option.
Création d'une base de données locale pour l'administrateur
<Oui>
<Non>


Configuration de libpam-ldap
Il est nécessaire de se connecter à la base de données uniquement s'il est impossible d'obtenir des données autrement.
Il ne s'agit pas du compte du super-utilisateur. Indiquer ici un compte privilégié est dangereux puisque le fichier de configuration est nécessairement lisible par tous.
Note : pour une configuration classique, cela n'est pas indispensable.
La base de données nécessite de se connecter
<Oui>
<Non>


Configuration de libpam-ldap
Ce compte sera utilisé lorsqu'il sera nécessaire de modifier un mot de passe.
Note : il est nécessaire que ce compte soit privilégié.
Compte du super-utilisateur
cn=manager,dc=alex,dc=fr
<Ok>


Configuration de libpam-ldap
Ce mot de passe sera utilisé lorsque libpam_ldap tentera de se connecter à la base de données.
Si vous n'indiquez rien ici, l'ancien mot de passe sera réutilisé.
Mot de passe du compte du super-utilisateur
<Ok>



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 « rwx------ » sur le fichier slapd.conf :

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

Mandrake

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

```
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
#include /usr/share/openldap/schema/samba.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.
index  objectClass,uid,uidNumber,gidNumber,memberuid  eq
index  cn,mail,surname,givenname                     eq,subinitial

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

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

# 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.
# 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/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.
index  objectClass,uid,uidNumber,gidNumber,memberuid  eq
index  cn,mail,surname,givenname                      eq,subinitial

# 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

# Where to store the replica logs for database #1
# replogfile     /var/lib/ldap/replog
```

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**

```
# ACLs authentification POSIX

# 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

# ACL permettant à l'admin de l'annuaire d'ajouter des utilisateurs
# dans la branche ou=People.
access to dn.children="ou=People,dc=alex,dc=fr"
     attrs=entry,children,posixAccount
     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 groupes
# dans la branche ou=Group.
access to dn.children="ou=Group,dc=alex,dc=fr"
     attrs=entry,children,posixGroup
     by dn="cn=admin,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 la branche ou=Hosts.
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
```

Basic ACL : il est possible de donner des droits particuliers en utilisant la directive access dont la syntaxe est : access to <une partie de l'arbre>
[by <une personne> <droits none|search|read|write>]

De plus, l'ordre d'écriture des règles a une grande importance.
Par exemple :
access to dn= « .*, dc=alex,dc=fr » by * search
access to dn= « .*, dc=fr » by * read

Signifie que tout le monde a le droit en lecture sur toute l'arborescence dc=fr excepté sur la partie dc=alex où les utilisateurs ont un droit en recherche seulement. Le fait d'inverser l'ordre de ces deux lignes, impliquera que la directive concernant dc=fr en lecture sera la seule à être prise en compte et, on ne protégera plus ainsi la partie de l'arbre dc=alex en recherche seulement.

L'authentification des utilisateurs

L'authentification des utilisateurs sur le système se fait par défaut au moyen des fichiers **/etc/passwd** (définition des utilisateurs), **/etc/group** (identification des groupes d'utilisateurs) et éventuellement **/etc/shadow** si vous utilisez les "shadow password".
C'est satisfaisant quand l'on dispose d'une machine isolée, par contre avec un parc d'une centaine de machines, il est peut concevable d'avoir à modifier ces fichiers sur tous les postes pour rajouter un utilisateur. L'idée est de centraliser l'authentification sur un serveur LDAP avec utilisation des "shadow passwords".

Migration des données POSIX vers LDAP

Mandrake	debian
Modifiez le fichier **migrate_common.ph** dans le répertoire **/usr/share/openldap/migration**	Modifiez le fichier **migrate_common.ph** dans le répertoire **/etc/migrationtools**

On doit indiquer son nom de domaine, comme ceci :

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "alex.fr";

# Default base
$DEFAULT_BASE = "dc=alex,dc=fr";

$DEFAULT_MAIL_HOST = "mail.alex.fr";

$EXTENDED_SCHEMA = 1;
```

Pour Migrer Automatiquement

Mandrake	debian
Si vous voulez migrer tous les modules de votre serveur, utiliser le fichier `/usr/share/openldap/migration/migrate_all_online.sh`	Si vous voulez migrer tous les modules de votre serveur, utiliser le fichier `/usr/share/migrationtools/migrate_all_online.sh`

Commenter ces lignes:

```
...
#echo "Migrating protocols..."
#$PERL migrate_protocols.pl    $ETC_PROTOCOLS >> $DB
#echo "Migrating rpcs..."
#$PERL migrate_rpc.pl          $ETC_RPC >> $DB
#echo "Migrating services..."
#$PERL migrate_services.pl     $ETC_SERVICES >> $DB
...
```

Exécuter le script.
Répondez aux questions (généralement accepter les paramètres par défauts)

```
[root@ldap]# ./migrate_all_online.sh
Enter the X.500 naming context you wish to import into: [dc=alex,dc=fr]
Enter the name of your LDAP server [ldap]: localhost
Enter the manager DN: [cn=manager,dc=alex,dc=fr]: cn=root,dc=alex,dc=fr
Enter the credentials to bind with: mypassword
Do you wish to generate a DUAConfigProfile [yes|no]? no
```

le X.500 naming context est le domain de base a utiliser. le LDAP server name doit etre localhost sinon vous allez configurer un serveur LDAP secondaire.
le manager DN doit etre identique au rootdn dans slapd.conf.
le credentials to bind with est le password contenu dans slapd.conf au rootpw.
le DUAConfigProfile doit etre laissé sur no. Sinon tous sera importé dans votre LDAP database ce qui peut prendre du temps.

Pour Migrer manuellement

Création de la base de l'annuaire :

Mandrake	debian
`cd /usr/share/openldap/migration/`	`cd /usr/share/migrationtools/`

```
[root@migration]# ./migrate_base.pl >base.ldif
[root@migration]# ldapadd -x -D "cn=Manager,dc=alex,dc=fr" -w mypassword
-f base.ldif
```

Migration du fichier /etc/hosts :

```
[root@migration]# ./migrate_hosts.pl /etc/hosts hosts.ldif
[root@migration]# ldapadd -x -D "cn=Manager,dc=alex,dc=fr" -w mypassword
-f hosts.ldif
```

Vous pouvez vérifier si la migration a bien fonctionné (si vous aviez des WS inscrites dans /etc/hosts) :

```
[root@ldap]# ldapsearch -LL -H ldap://localhost -b "dc=alex,dc=fr" -x
"(cn=workstation1)"

version: 1

dn: cn=workstation1.alex.fr,ou=Hosts,dc=alex,dc=fr
objectClass: top
objectClass: ipHost
objectClass: device
ipHostNumber: 192.168.0.123
cn: workstation1.alex.fr
cn: workstation1
```

A présent il faut rentrer les utilisateurs et groupes du système dans l'annuaire LDAP.

```
[root@migration]# ./migrate_group.pl /etc/group group.ldif
[root@migration]# ldapadd -x -D "cn=Manager,dc=alex,dc=fr" -w mypassword
-f group.ldif

[root@migration]# ETC_SHADOW=/etc/shadow ./migrate_passwd.pl /etc/passwd
passwd.ldif
[root@migration]# ldapadd -x -D "cn=Manager,dc=alex,dc=fr" -w mypassword
-f passwd.ldif
```

Voici les informations me concernant, contenues dans mon **group.ldif**

```
dn: cn=arnofear,ou=Group,dc=alex,dc=fr
objectClass: posixGroup
objectClass: top
cn: arnofear
userPassword: {crypt}x
gidNumber: 501
```

Voici les informations me concernant, contenues dans mon **passwd.ldif**

```
dn: uid=arnofear,ou=People,dc=alex,dc=fr
uid: arnofear
cn: arnofear
mail: arnofear@alex.fr
objectClass: mailRecipient
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$1$Dbwezia0$xZQeQBeQJFliDthz90Inl.
shadowLastChange: 12377
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 501
gidNumber: 501
homeDirectory: /home/arnofear
gecos: arnofear
```

On visualise tout ça en tapant

```
ldapsearch -x -D "cn=Manager,dc=alex,dc=fr" -w mypassword -b
"dc=alex,dc=fr"
```

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.

shadowLastChange: Date de dernière modification (en jour depuis 01.01.1970)
shadowMax: Nombre de jours d'utilisation max du mot de passe (changement requis à l'issue), pas de période de validité si égal à 99999
shadowWarning: Nombre de jours avant l'expiration pour avertir l'utilisateur.
shadowInactive: Nombre de jours après la date de l'expiration où on rend le compte inactif,fonctionnalité désactivé si égal à -1
shadowExpire: Nombre de jours après le 01.01.1970 où le compte sera désactivé, fonctionnalité désactivée si égal à -1
memberUid: Indique le groupe d'appartenance de l'utilisateur.

Mappage de l'annuaire LDAP avec les modules d'authentification Posix

Mandrake	debian
Editez le fichier **/etc/ldap.conf**	Editez le fichier **/etc/libnss-ldap.conf** et faites un lien symbolique vers **/etc/pam_ldap.conf** puisque la configuration est identique.

```
# @(#)$Id: ldap.conf,v 2.28 2001/08/28 12:17:29 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.

# Your LDAP server. Must be resolvable without using LDAP.
# Sur le serveur il faut mettre l'adresse de la boucle locale
# si vous utilisez ldap://
# Si vous utilisez ldaps:// indiquez plutôt votre FQDN (srv2.alex.fr)
Host localhost

# The distinguished name of the search base.
# le nom de la base.
base dc=alex,dc=fr

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
# Ne pas activer cette option car le mot de passe Manager passera en
# clair !!! Préférez une connexion anonymous.
#rootbinddn cn=Manager,dc=example,dc=com

# The port.
# Optional: default is 389.
# Laissez le port commenté. Si vous utilisez ldaps,
# le port 636 sera utilisez automatiquement.
# port 389

# The search scope.
# scope sub
scope one
# scope base

# Search timelimit
# timelimit 30

# Bind timelimit
# bind_timelimit 30

# client will close connections (nss_ldap only) if the server has not
# been contacted for the number of seconds specified below.
# idle_timelimit 3600

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

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

# Group member attribute
pam_member_attribute gid
```

```
pam_password crypt

# 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 le chemin de recherche dans la base de l'annuaire
# les utilisateurs seront inscrits dans People, les groupes dans Group
# Attention la ligne suivante est dédiée au serveur LDAP.
nss_base_passwd  ou=People,dc=alex,dc=fr?sub
nss_base_shadow  ou=People,dc=alex,dc=fr?one
nss_base_group   ou=Group,dc=alex,dc=fr?one
nss_base_hosts   ou=Hosts,dc=alex,dc=fr?one

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
# ssl start_tls
# ssl on
# Les transactions se feront en claires si vous n'utilisez pas ldaps.
# Reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
ssl off
```

	
Modifiez **/etc/openldap/ldap.conf**	Modifiez **/etc/ldap/ldap.conf**

```
# Reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
#TLS_CACERT      /etc/ssl/openldap/ldap_cert.pem
#TLS_CACERTDIR   /etc/ssl/openldap
#TLS_REQCERT allow

# La racine de votre annuaire.
BASE    dc=alex,dc=fr
# L'adresse FQDN de vos (ou votre) serveurs OpenLDAP.
URI     ldap://srv2.alex.fr ldap://srv6.alex.fr
```

Configurer NSS pour utiliser LDAP

Dans le fichier **/etc/nsswitch.conf** modifiez les lignes suivantes :

Mandrake	debian
passwd: files ldap shadow: files ldap group: files ldap hosts: files dns	passwd: compat ldap group: compat ldap shadow: compat ldap hosts: files dns

```
# si vous avez des hosts ajoutez ldap, sinon laissez files dns
# (possibilité de bug au démarrage du PC)
```

Vous pouvez étendre files ldap aux autres modules selon se que vous avez importé dans votre Migration.

Pour vérifier utilisez **getent** de cette façon :

```
[root@ldap]# getent hosts
[root@ldap]# getent group
[root@ldap]# getent passwd
[root@ldap]# getent shadow
```

Configurer PAM pour utiliser LDAP

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

```
#%PAM-1.0
auth required pam_env.so
auth sufficient pam_unix.so likeauth nullok
auth sufficient pam_ldap.so use_first_pass
auth required pam_deny.so

account required pam_unix.so
account sufficient pam_ldap.so

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

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

Vérifiez le fichier **/etc/pam.d/passwd**

```
#%PAM-1.0
auth required pam_stack.so service=system-auth

account required pam_stack.so service=system-auth

password required pam_stack.so service=system-auth
```

debian

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 sufficient pam_unix.so likeauth nullok
auth sufficient pam_ldap.so use_first_pass
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_ldap.so
```

Authentification Host-based

Si vous utilisez OpenLDAP pour identifier les users dans un LAN, vous pouvez refuser la connexion à certaines machines. Utiliser le pam_mkhomedir module :

Dans le fichier /etc/ldap.conf, vous devez ajouter cet attribut :

```
# check for login rights on the host
pam_check_host_attr yes
```

Ce qui demandera au module pam_ldap de rechercher l'attribut "host" dans la base de l'user pour déterminer s'il a accès au système.

Vous devez ajouter cet attribut dans l'enregistrement des users.
Créer un fichier host-auth.ldif :

```
dn: uid=joe,ou=People,dc=alex,dc=fr
changetype: modify
add: host
host: workA
host: workB

dn: uid=bob,ou=People,dc=alex,dc=fr
changetype: modify
add: host
host: workB
```

exécutez la commande ldapmodify :

```
[root@ldap]# ldapmodify -H ldap://localhost -D "cn=Manager,dc=alex,dc=fr"
\
-x -W -f host-auth.ldif
```

dans cet exemple joe pourra se connecter sur l'host **workA** et **workB** alors que bob ne pourra que se connecter sur l'host **workB**

Configuration des Clients OpenLDAP

Mandrake	debian
Editez le fichier **/etc/ldap.conf** de chaque clients.	Editez le fichier **/etc/libnss-ldap.conf** qui sera dupliqué vers **/etc/pam_ldap.conf** étant identique pour chaque clients.

```
# @(#)$Id: ldap.conf,v 2.28 2001/08/28 12:17:29 lukeh Exp $
#
# This is the configuration file for the LDAP nameservice
# switch library and the LDAP PAM module.

# Your LDAP server. Must be resolvable without using LDAP.
# Indiquez l'adresse FQDN (de préférence) de votre serveur LDAP.
# si vous en avez plusieurs écrivez :
# Host srv2.alex.fr, srv6.alex.fr
Host srv2.alex.fr

# The distinguished name of the search base.
# le nom de la base.
base dc=alex,dc=fr

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
# Ne pas activer cette option car le mot de passe Manager passera en
# clair !!! Préférez une connexion anonymous.
#rootbinddn cn=Manager,dc=example,dc=com

# The port.
# Optional: default is 389.
# Laissez le port commenté. Si vous utilisez ldaps,
# le port 636 sera utilisez automatiquement.
# port 389

# The search scope.
# scope sub
scope one
# scope base

# Search timelimit
# timelimit 30

# Bind timelimit
# bind_timelimit 30

# client will close connections (nss_ldap only) if the server has not
# been contacted for the number of seconds specified below.
# idle_timelimit 3600

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

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

# Group member attribute
pam_member_attribute gid
```

```
pam_password crypt

# 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 le chemin de recherche dans la base de l'annuaire
# les utilisateurs seront inscrits dans People, les groupes dans Group.
nss_base_passwd  ou=People,dc=alex,dc=fr?one
nss_base_shadow  ou=People,dc=alex,dc=fr?one
nss_base_group   ou=Group,dc=alex,dc=fr?one
nss_base_hosts   ou=Hosts,dc=alex,dc=fr?one

# OpenLDAP SSL mechanism
# start_tls mechanism uses the normal LDAP port, LDAPS typically 636
# ssl start_tls
# ssl on
# Les transactions se feront en claires si vous n'utilisez pas ldaps.
# Repportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
ssl off
```

Mandrake	debian
Modifiez **/etc/openldap/ldap.conf**	Modifiez **/etc/ldap/ldap.conf**

```
# Reportez vous au chapitre "SSL/TLS" pour mettre en place ldaps.
#TLS_CACERT      /etc/ssl/openldap/ldap_cert.pem
#TLS_CACERTDIR   /etc/ssl/openldap
#TLS_REQCERT allow

# La racine de votre annuaire.
BASE    dc=alex,dc=fr
# L'adresse FQDN de vos (ou votre) serveurs OpenLDAP.
URI     ldap://srv2.alex.fr ldap://srv6.alex.fr
```

Copiez ces fichiers sur les clients qui s’adresseront au Serveur LDAP

Mandrake	debian
/etc/nsswitch.conf /etc/pam.d/system-auth /etc/pam.d/passwd	/etc/nsswitch.conf /etc/pam.d/common-account /etc/pam.d/common-auth /etc/pam.d/common-password /etc/pam.d/common-session

Test de fonctionnement

Sur le serveur ou les clients, supprimez les lignes qui correspondent à vos utilisateurs dans **/etc/passwd** , et **/etc/shadow** et faites de même pour vos groupes utilisateurs dans **/etc/group**
N'oubliez pas de faire une sauvegarde de ces fichiers au cas où !
Maintenant essayez de vous loguer en tant que simple utilisateur.

Montage du homedirectory des Clients depuis un serveur NFS

Sur la machine qui sera utilisée comme **serveur NFS** installez ces packages :

Mandrake	debian
nfs-utils-1.0.xxmdk.rpm	nfs-common_1.0.6-3.1_i386.deb nfs-kernel-server_1.0.6-3.1_i386.deb

Nous voulons que les HomeDirectories des utilisateurs soient créés à la volée dés leur première connexion.
Pour cela il faut que le système (root) des clients puissent écrire sur notre montage NFS (/home).
Par défaut NFS rétrograde les droits root clients (uid/gid=0) en nobody.
Il faut préciser l'option NFS "no_root_squash" pour que les root clients puissent écrire.

Editez le fichier **/etc/exports** :

```
# /répertoire_serveur_NFS
# noms_des_clients => dans cet exemple tous mes clients
# commencent par ws123.alex.fr
# (lecture/écriture,synchronisation,root_clients_en_écriture)
/home/nfs ws*.alex.fr(rw,sync,no_root_squash)
```

Pour plus de sécurité vous pouvez lister toutes les machines clientes autorisées à se connecter au serveur NFS :

Editez le fichier **/etc/hosts.deny** :

```
slapd:   ALL
portmap: ALL
lockd:   ALL
mountd:  ALL
rquotad: ALL
statd:   ALL
```

et aussi le fichier **/etc/hosts.allow** :

```
# Autorisez des adresses spécifiques :
# portmap: 192.168.0.20, 192.168.0.25, 192.168.0.30
# Ou autorisez le réseau entier :
portmap: 192.168.0.0/255.255.255.0 127.0.0.1
lockd:   192.168.0.0/255.255.255.0 127.0.0.1
mountd:  192.168.0.0/255.255.255.0 127.0.0.1
rquotad: 192.168.0.0/255.255.255.0 127.0.0.1
statd:   192.168.0.0/255.255.255.0 127.0.0.1
slapd:   192.168.0.0/255.255.255.0 127.0.0.1
```

Relancez les services :

```
[root@srv12 user]# exportfs -a
[root@srv12 user]# /etc/init.d/portmap restart
```

Mandrake	debian
`[root@srv12 user]# /etc/init.d/nfs restart`	`srv12:~# /etc/init.d/nfs-kernel-server restart`

Pour vérifier :

```
[root@srv12 user]# rpcinfo -p
    program vers  proto port
    100000    2    tcp    111  portmapper
    100000    2    udp    111  portmapper
    100003    2    udp   2049  nfs
    100003    3    udp   2049  nfs
    100003    2    tcp   2049  nfs
    100003    3    tcp   2049  nfs
    100021    1    udp  32772  nlockmgr
    100021    3    udp  32772  nlockmgr
    100021    4    udp  32772  nlockmgr
    100021    1    tcp  32875  nlockmgr
    100021    3    tcp  32875  nlockmgr
    100021    4    tcp  32875  nlockmgr
    100005    1    udp  32773  mountd
    100005    1    tcp  32876  mountd
    100005    2    udp  32773  mountd
    100005    2    tcp  32876  mountd
    100005    3    udp  32773  mountd
    100005    3    tcp  32876  mountd
```

Sur les machines **Clientes LDAP/NFS** installez ce package :

Mandrake	debian
nfs-utils-clients-1.0.xx.rpm	nfs-common_1.0.6-3.1_i386.deb

Editez le fichier **/etc/fstab** pour ajouter :

```
srv12.alex.fr:/home/nfs /home nfs rw,sync,rsize=8192,wsize=8192,
nosuid,nodev,noexec,soft 0 0
```

Montage manuel pour vérifier :

```
[root@ws20 root]# mount /home
```

Au prochain démarrage des PC clients et si votre serveur NFS est opérationnel, le /home de vos clients sera monté depuis votre serveur.

Sécurisation des Workstations

Pour éviter tout débordement ou attaque de votre réseau depuis l'intérieur, vous pouvez verrouiller dans un premier temps l'accès au BIOS par un password, ainsi que les périphériques au boot du PC (1er boot sur IDE-0) voir même la détection d'intrusion chassis.

Mais surtout verrouillez les commandes passées avec **lilo** par un password !

Sur chaque Workstations éditez **/etc/lilo.conf** pour modifier en rouge dans chaque labels :

```
boot=/dev/hda
map=/boot/map
default="linux"
keytable=/boot/fr-latin1.klt
prompt
nowarn
timeout=20
message=/boot/message
menu-scheme=wb:bw:wb:bw
image=/boot/vmlinuz
      label="linux"
      # Ne demandera pas de password, mais ne pourra pas
      # être modifié sans lui.
      password="mypassword" restricted
      root=/dev/hda1
      initrd=/boot/initrd.img
      append="devfs=mount hdd=ide-scsi hdb=ide-scsi acpi=off quiet"
      vga=788
      read-only
image=/boot/vmlinuz
      label="linux-nonfb"
      password="mypassword" restricted
      root=/dev/hda1
      initrd=/boot/initrd.img
      append="devfs=mount hdd=ide-scsi hdb=ide-scsi acpi=off"
      read-only
image=/boot/vmlinuz
      label="failsafe"
      password="mypassword" restricted
      root=/dev/hda1
      initrd=/boot/initrd.img
      append="devfs=nomount hdd=ide-scsi hdb=ide-scsi acpi=off failsafe"
      read-only

other=/dev/fd0
      label="floppy"
      # Demandera le password pour booter sur disquette
      password="mypassword"
      unsafe
```

Puis validez les modifications :

```
[root@ws user]# lilo
Warning: /etc/lilo.conf should be readable only for root if using PASSWORD
Added linux *
Added linux-nonfb
Added failsafe
Added floppy
```

Ensuite pour que personne ne lise simplement le fichier lilo.conf vérifiez qu'il appartient à root (uid/gid) et appliquez les droits suivants :

```
[root@ws user]# chmod 600 /etc/lilo.conf
```

Document mis à jour : 05/12/05