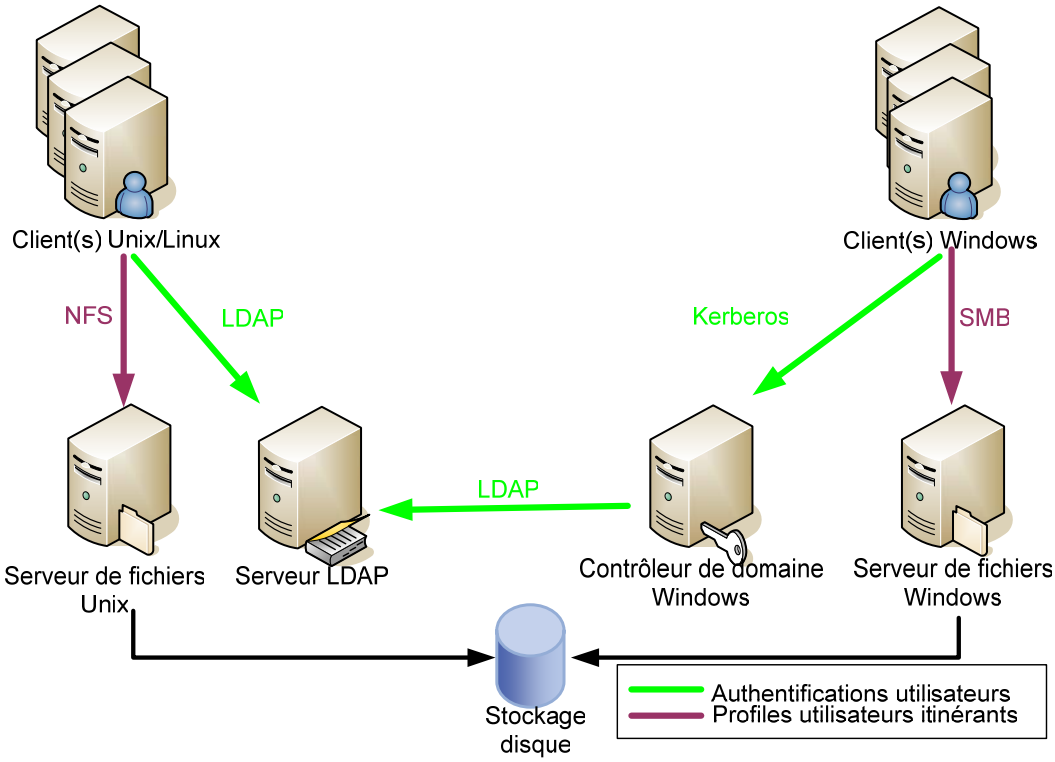
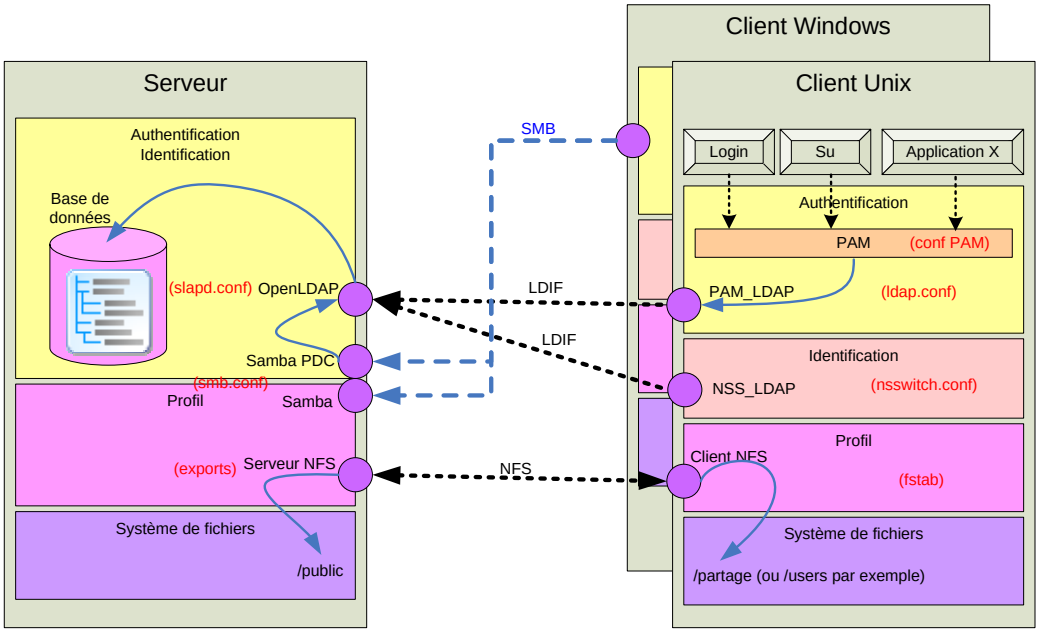
```
                              \|||/
                              (o o)
+-----------------------oooO--(_)-----------------------------+
|                                                             |
|      Administration des services Linux (avec Debian)        |
|      LDAP serveur et client sur debian                      |
|Reseau-02 Admin des services fiche LDAP org.doc                    |
|                                                             |
+---------------------------------Ooo-------------------------+
                              |__|__|                  ©nadir 2007 ;-)
                               || ||
                              ooO Ooo
```

1. Objectif

Vision des services



Vision simplifiée



Ce que nous allons réaliser, dans lequel tous les services sont placés sur la même machine.

2. Apercu de LDIF

LE FORMAT D'ÉCHANGE DE DONNÉES LDIF (import/export)

```
LDIF=Lightweight Data Interchange Format

La syntaxe de ce format est la suivante:

    dn: <distinguished name> -------- identifiant unique ( dn: <distinguished name> )
    objectClass: <class> -----------| liste de classes (objectclass): definit
    objectClass: <class>            | les attributs obligatoires/facultatifs
    ...
    <attribut>: <valeur> ------------ liste d'attributs ( propriétés  )
    <attribut>: <valeur>
    ...

Notes:
    * chaque nouvelle entrée doit être séparée de l'entrée précédente
    à l'aide d'un saut de ligne (ligne vide)

    * Il est possible de définir un attribut sur plusieurs lignes
    en commençant les lignes suivantes par un espace ou un tabulation

    * lorsque la valeur contient un caractère spécial (non imprimable,
    un espace ou :), l'attribut doit être suivi de :: puis de la valeur
    encodée en base64 ( ex: userPassword ci-dessous )

Exemple:
    Une entrée de type personne se représente de la manière suivante :

    dn: uid=mickey,ou=Stud,ou=People,o=fr
    objectclass: top
    objectclass: person
    objectclass: organizationalPerson
    objectclass: inetOrgPerson
    objectclass: posixAccount
    uid: mickey
    cn: Mickey Mouse
```

```
    sn: mickey
    uidNumber: 1101
    gidNumber: 600
    userPassword:: OGFzYWlzaXI=
    loginShell: /bin/bash
    homeDirectory: /home
    userPassword: mickey

    un dn dans la base ldap pro de la multinationale MARS:
    cn=Mickey/ou=Marseille/ou=Europe/ou=MARS/ou=People/o=MARSGroup/c=FR
```

3. INSTALL DE OPENLDAP COTE SERVEUR

paquet: slapd

installe notamment :

- /etc/ldap/slapd.conf
- /usr/sbin/slapd

installe aussi (on le voit plus en detail plus loin)

- les fichiers schemas sur: /etc/ldap/schema
- demarrage du service: /etc/init.d/slapd

Definitions Minimales OpenLdap

la definition d'un arbre sous OpenLdap passe par 2 notions:

- le DN sa racine (par exemple "dc=gtr,dc=fr")
- le DN de son administrateur (par exemple "cn=Manager,dc=gtr,dc=fr"si on decide que le root se nommera « manager »)

la racine peut etre "dc=gtr,dc=fr" ou "dc=gtr" ou encore "o=fr". il est précisé dans le suffixe.

il faut configurer le serveur, le fichier ldif de définition du schema de l'arbre et bien sur les clients avec ces 2 items.

openldap peut gerer plusieurs arbres (plusieurs suffixes cad plusieurs racines), mais il n'y a qu'un seul administrateur LDAP (qui n'est pas forcément root de la machine)

Configuration de OpenLDAP

editer le fichier config: /etc/ldap/slapd.conf

pour l'authentification il faut les definitions suivantes :

```
    include /usr/local/etc/openldap/schema/core.schema
    include /usr/local/etc/openldap/schema/cosine.schema
    include /usr/local/etc/openldap/schema/inetorgperson.schema
    include /usr/local/etc/openldap/schema/nis.schema
```

modifications (à adapter si nécessaire):

```
    database        bdb
    suffix          "dc=gtr,dc=fr"                  (definit la racine)
    rootdn          "cn=Manager,dc=gtr,dc=fr"       (root sur l'annuaire)
    rootpw          secret                          (changer avec slappasswd)
    directory       /usr/local/var/openldap-data    (database dir)
```

```
directory       "/var/lib/ldap"
```

(a priori rootdn n'est plus necessaire si on precise les ACL ci-dessous)

après modification du fichier de conf, eventuellement on peut lancer: slaptest
(teste et valide le fichier de configuration)

Index

```
information des options d'index (pour les requetes de recherche):
    index   objectClass  eq

devenu inutile?!
    index   cn,sn   pres,eq,sub
    index   homeDirectory,userPassword,loginShell,uid,uidNumber,gidNumber eq


toute les fois que l'on modifie les index, relancer:
      /usr/sbin/slapindex
```

Gestions des droits d'accès (ACL) (à adapter si nécessaire)

```
#le mot de passe peut etre vu/modifié par le propriétaire authentifié ou l'admin
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,dc=gtr,dc=fr" write
        by anonymous auth
        by self write
        by * none

# obligatoire pour fonctioner avec SASL
access to dn.base="" by * read

# l'admin a un accès ecriture, les autres lectures seules
access to *
        by dn="cn=admin,dc=gtr,dc=fr" write
        by * read

#dans un premier temps on peut mettre les droit d'accès complets à tous:
        access to * by * write

pour un réglage plus fin des ACL, il sera necessaire d'apprendre à manipuler
slapacl. voir sa man page ;-)
```

PREMIER LANCEMENT

```
Desactiver au prealable le service :
/etc/init.d/slapd stop

lancement du serveur LDAP à la main:
/usr/sbin/slapd -h "ldap://0.0.0.0/"  -d 256
(interet: voir les requetes arrivant sur le serveur ldap)
```

INSTALL DU SCHEMA (GTR.LDIF)

```
 dc=gtr,dc=fr     (racine ou suffix) ( 'dc' 'domainComponent' ) ( 'o' 'organizationName' )
 |
 |
 +---ou=People   ( 'ou' 'organizational Unit' )
 |   |
 |   +---ou=Stud  (Etudiants)
 |   +---ou=Perm  (Permanents)
 |
 +---ou=Services
     |
     +---ou=Groupes
     +---ou=NFS
```

Récupérer les fichiers sur: http://nadir.is.online.fr/public/ldap
Ils contiennent la définition de l'arbre, du compte admin, et d'un utilisateur de test.

Insertion dans la base du serveur :
      slapadd -l 2007.GTR.ldif

il est aussi possible d'utiliser ldapadd (ldapadd fait partie du package ldap-utils):

ldapadd -x -h 10.1.26.249 -D "cn=Manager,dc=gtr,dc=fr" -w secret -f 2007.GTR.ldif

modifs:
    * dc=gtr,dc=fr doit etre remplacé par dc=fr ou o=fr
    * sur le root de l'arbre, objectclass: remplacer organization par domain
    * sur le root de l'arbre, ajouter la propriété dc: fr ou o: fr
    * ajout de shadowAccount dans le user mickey
    * attention les Gid sont pas bons.

Verification :
PUIS /usr/sbin/slapcat

RECHERCHE: a essayer aussi (ldapsearch fait partie du package ldap-utils)

ldapsearch -h localhost -D "cn=Manager,o=fr" -b "o=fr" -w secret -x "(objectClass=*)"

--->important : le -b

Ou ldapsearch -h 10.1.26.249 –L "(objectclass=*)" (fait partie de ldap-utils)

eventuellement on peut installer ldap-utils:
installe des commandes qui permettent de modifier la base LDAP « à chaud » (les commandes slapxxx comme slapadd necessitent un accès exclusif) car elles sont de simples clients LDAP.
L'avantage est qu'elle peuvent aussi être installées coté client.

pour effacer la base LDAP, effacer tous les fichier sous directory "/var/lib/ldap"

4. INSTALL D'OPENLDAP COTE CLIENT

PACKAGES REQUIS

installer les packages debian:
    libnss-ldap
    libpam-ldap

sous ubuntu le paquet ldap-auth-client (à verifier pour debian) est un meta-package qui regroupe les 2 (nécéssaire pour authentification LDAP)

CONFIGURATION

Configuration de PAM-LDAP

dans /etc/ldap.conf:
    host 10.1.26.249
    base dc=gtr,dc=fr
    ldap_version 3
    pam_filter objectclass=posixAccount (IMPORTANT!!)
    pam_login_attribute uid
    pam_password crypt

sous ubuntu il existe aussi le paquet "ldap-auth-config" permet de créer le fichier /etc/ldap.conf interactivement.on y positionne:

- l'URI du serveur (mettre l'IP directement) essayer ldap://127.0.0.1:389/
- le DN du "search base" qui correspond au suffix cad à la racine de l'arbre
- la version à utiliser et 3

- le mode cryptage du mot de passe est “crypt”. Si ca ne fonctionne pas, mettre “clear”

on peut à tout moment relancer: dpkg-reconfigure ldap-auth-config

Config De Pam pour faire appel à pam_ldap

modifier les fichiers de PAM pour faire appel a pam_ldap.
Conseil: le faire pour une commande inoffensive pour faire vos essais (su par exemple) avant de le positionner sur le fichier pam de login

Autre conseil : on peut positionner pam_ldap de manière globale en le placant dans les fichiers common-xxx(/etc/pam.d/common.auth par exemple).

configuration de la résolution de noms NSSnsswitch.conf, ne placer que les 3 suivants :

```
passwd: files ldap
group:  files ldap
shadow: files ldap
```

5. PROFILS INITERANTS PAR NFS

COTE SERVEUR

```
installer les packages:
    nfs-common
    nfs-kernel-server

export du repertoire /public coté serveur
      /public *(rw,sync,root_squash)


Ecriture plus sécurisée:

      /public     10.48.1.4/16(rw,sync,root_squash)


ne pas oublier la commande exportfs -rv
 -r Reexporter tous les directories

 -v verbeux

ne pas oublier de créer le repertoire  public
et de donner les droits a+rwx sur le repertoire  public
```

COTE CLIENT

```
mount nfs de /home (ou /partage) coté client pointant sur le partage /public
 mount -t nfs 192.168.1.10:/public /partage
ne pas oublier de créer le repertoire partage
et de donner les droits a+rx sur le repertoire partage

modification des entrées ldap pour que le repertoire home de l'utilisateur sur le client
pointe sur le répertoire monté sur le serveur.
le faire sur l'utilisateur de test mickey.
```

note

on peut installer phpLDAPadmin qui est une interface web pour administrer un arbre LDAP.
http://localhost/phpldapadmin/

user (DN de connexion) cn=admin,o=fr
password secret

A adapter : modifier aussi le gid pour que le groupe de mickey corresponde

6. AUTOMOUNT

installer les paquets:
autofs
autofs-ldap

le guide complet se trouve sous :
/usr/share/doc/autofs-ldap (README.ldap_master)
Pour info voir aussi sous /usr/share/doc/autofs.

ne pas oublier l'include dans /etc/ slapd.conf:
include /etc/ldap/schema/autofs.schema

fichier nsswitch.conf
ne pas oublier l'entree dans nsswitch.conf:
automount: files ldap

coté serveur, on implémente auto.master dans l'arbre LDAP comme suit:

LDAP:

```
dn: ou=Automount,dc=iut,dc=fr
ou: Automount
objectClass: top
objectClass: organizationalUnit
structuralObjectClass: organizationalUnit

dn: ou=auto.master,ou=Automount,dc=iut,dc=fr
ou: auto.master
objectClass: top
objectClass: automountMap
structuralObjectClass: automountMap

dn: ou=auto.indirect,dc=iut,dc=fr
objectClass: top
objectClass: automountMap
ou: auto.indirect
structuralObjectClass: automountMap
```

fichier /etc/auto.master:

```
/partage   ldap:ou=auto.indirect,dc=iut,dc=fr
```

ensuite une entrée utilisateur typique est:

```
dn: cn=mickey,ou=auto.indirect,dc=iut,dc=fr
objectClass: top
objectClass: automount
cn: mickey
automountInformation: -rw,intr,soft,quota 127.0.0.1:/public/stud/mickey
structuralObjectClass: automount

dn: cn=stud,ou=auto.indirect,dc=iut,dc=fr
objectClass: top
objectClass: automount
cn: stud
automountInformation: -rw,intr,soft,quota 127.0.0.1:/public/stud
structuralObjectClass: automount
```

7. samba

Todo

8. Liens

Bon point de départ sur le sujet LDAP:
http://www.openldap.org/

Bonne synthèse:
http://www-sop.inria.fr/semir/personnel/Laurent.Mirtain/ldap-livre.html

http://www.linux-france.org/article/serveur/ldap/ldap.htm

http://www.commentcamarche.net/ldap/ldapcons.php3
http://www.linux-france.org/article/serveur/ldap/ldap.html

http://www.pascalou.org/linux/doc/authentification-ldap.html

http://www.cru.fr/ldap/

http://www.raphinou.com/ldaps/LDAP-SSL.HOWTO

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

/usr/share/doc/autofs-ldap/README.ldap_master