Réseau de PC mixte Linux/Windows administré sous LDAP

1. Objectif L’objectif de ce TP est de réaliser une gestion de comptes personnels centralisée pour un réseau de PC banalisés. Les utilisateurs peuvent se connecter sur n’importe quelle machine, soit sous Linux soit sous Windows, et se connecter avec le même mot de passe. Ils retrouvent alors les fichiers de leurs profils personnels, à la fois Linux et Windows (concept de profils itinérants). Cela s’appuie sur un arbre LDAP géré par OpenLDAP, NFS pour l’accès Unix et Samba pour l’accès Windows (qui joue le rôle de contrôleur de domaine).

Vision des services

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

1. Apercu de LDIF LE FORMAT D'ÉCHANGE DE DONNÉES LDIF (import/export) LDIF : LDAP Data Interchange Format LDAP : Lightweight Directory Access Protocol 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> ---------- lis 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 LDAP de type utilsateur se représente de la manière suivante : dn: uid=mickey,ou=Stud,ou=People,o=gtr objectclass: top objectclass: person objectclass: organizationalPerson objectclass: inetOrgPerson objectclass: posixAccount uid: mickey cn: Mickey Mouse sn: mickey uidNumber: 110 gidNumber: 600 userPassword:: OGFzYWlzaXI= loginShell: /bin/bash homeDirectory: /home userPassword: mickey Pour exemple, voici 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 2. INSTALL DE OPENLDAP COTE SERVEUR Paquet: slapd (entrez un mot de passe admin) Installe notamment : /etc/ldap/slapd.conf (configuration)/usr/sbin/slapd (executable) Installe aussi (on le voit plus en detail plus loin) l les fichiers schemas sur: /etc/ldap/schema l démarrage du service: /etc/init.d/slapd Définitions Minimales OpenLdap la définition d'un arbre sous OpenLdap passe par 2 notions: l le DN sa racine (par exemple "dc=gtr,dc=fr") l le DN de son administrateur (par exemple "cn=Manager,dc=gtr,dc=fr" si on décide que le root se nommera « manager ») la racine peut être "dc=gtr,dc=fr" ou "dc=gtr" ou encore "o=gtr". Il est précisé dans le paramètre « suffix » du fichier de configuration de openldap. il faut configurer le serveur, le fichier ldif de définition de l'arbre et bien sûr les clients avec ces 2 items. openldap peut gérer plusieurs arbres (plusieurs suffixes cad plusieurs racines), mais il n'y a qu'un seul administrateur LDAP (qui n'est pas forcément le root de la machine) Configuration de OpenLDAP éditer le fichier config: Pour l'authentification il faut les définitions suivantes : include /etc/ldap/schema/core.schema include /etc/ldap/schema/cosine.schema include /etc/ldap/schema/inetorgperson.schema include /etc/ldap/schema/nis.schema (Les chemins ne sont pas forcément bon, l’essentiel étant de vérifier la présence des schemas core, cosine, interorgperson et nis) Modifications (à adapter si nécessaire): database bdb suffix "o=gtr" (définit la racine) rootdn "cn=Manager,o=gtr" (root sur l'annuaire) rootpw secr slappasswd) directory / var/lib/ldap (répertoire des fichiers de données BDB) (A priori rootdn n'est plus néces si on précise les ACL ci-dessous) Après modification du fichier de conf, éventuellement on peut lancer: slaptest (qui teste et valide le fichier de configuration) Index information des options d'index (pour les requêtes de recherche): index objectClass eq index uid,uidNumber,gidNumber eq devenu inutile?! index cn,sn pres,eq,sub index homeDirectory,userPassword,loginShell eq Toute les fois que l'on modifie les index, relancer: /usr/sbin/slapindex Gestions des droits d'accès (ACL) (à adapter si nécessaire) Les ACL sur l’arbre LDAP sont contrôlées par les directives access. Dans un premier temps on peut mettre les droits d'accès complets à tous: access to * by * write Commenter toutes les autres directives access. Cela permettra de simplifier l’etape de configuration des clients. pour un réglage plus fin des ACL, il sera nécessaire d'apprendre à manipuler slapacl. voir sa man page ;-) PREMIER LANCEMENT Désactiver au préalable le service : /etc/init.d/slapd stop Lancement du serveur LDAP à la main: /usr/sbin/slapd -d 256 Intérêt: voir sur la console les requêtes arrivant sur le serveur ldap. 256 affiche les requêtes LDAP reçues INSTALL DU SCHEMA (GTR.LDIF) o=gtr (racine ou « suffix », 'o signifie 'organizationName') | ou=Population ('ou’ signifie 'organizational Unit') | | | +---ou=Etudiants | +---ou=Profs | +---ou=Groupes +---ou=NFS Récupérer les fichiers sur: http://nadir.is.online.fr/download/admin/ldap/ Ils contiennent : - Gtr.ldif : la définition de l’arbre et du compte admin - Mickey.ldif : un exemple utilisateur de test Éventuellement on peut installer le package ldap-utils : Installe des commandes qui permettent de modifier la base LDAP « à chaud » (les commandes slapxxx comme slapadd nécessitent un accès exclusif) car elles sont de simples clients LDAP. L'avantage est qu’elles peuvent aussi être installées coté client. 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,o=gtr" -w secret -f 2007.GTR.ldif la différence entre spladadd et ldapadd : slapadd est une commande serveur, qui fait accès direct à la base de données, donc plus rapide mais par contre

necessite d’arreter le serveur slapd. Ldapadd est une commande client (du serveur LDAP), qui peut servir à accéder à n’importe quel serveur sur un réseau (on precise sont IP), qui peut donc etre executé sans arreter slapd. Modifications: * o=gtr peut être remplacé par dc=gtr ou dc=gtr,dc=fr (mais il faut modifier les classes et les propriétés en fonction dans les fichiers ldif) * attention les gid sont pas bons (pas cohérents entre le ldif de mickey et la definition des groupes dans gtr.ldif) TEST DE L’INSTALLATION Vérification : PUIS /usr/sbin/slapcat RECHERCHE: à essayer aussi (ldapsearch fait partie du package ldap-utils) ldapsearch -x -h localhost -b "o=gtr" L’avantage d’utiliser ldapsearch sera que si celui-ci fournit un résultat, alors la suite fonctionnera (l’accès via PAM) puisque ldapsearch est un client LDAP comme un autre. REINITIALISER L’INSTALLATION (si besoin) Si vos insertions de fichiers ldif se passent mal, il peut arriver que vous vouliez repartir de 0 (vider la base de données). Pour effacer la base LDAP, effacer tous les fichiers sous le répertoire dont le chemin est précisé sous la clause directory de slapd.conf (debian par defaut "/var/lib/ldap"). 3. INSTALL DE LDAP COTE CLIENT PACKAGES REQUIS installer les packages debian: libnss-ldap libpam-ldap (sous ubuntu le paquet ldap-auth-client est un meta-package qui regroupe les 2). à l’installation, les questions suivantes seront posées : Uri du serveur : laisser tel quelDN de la base : soyez cohérent (correspond au paramètre « base » ou « suffix »)créer une base locale ? à nonla base ldap demande elle une identification à non Les 2 sont nécessaires pour authentification LDAP : pam pour l’auth, nss pour la résolution du nom des users ATTENTION: fichier /etc/ldap/ldap.conf --> VIDE ! CONFIGURATION Configuration de PAM-LDAP dans /etc/ldap.conf pour ubuntu, pour debian voir un peu plus bas: host 10.1.26.249 ou uri ldap://10.1.26.249/ base o=gtr ldap_version pam_filter objectClass=posixAccount (IMPORTANT!!) pam_login_attribute uid pam_password crypt Sous debian, il y a 2 fichiers créés à la place de /etc/ldap.conf: /etc/pam-ldap.conf/etc/libnss-ldap.conf Ils sont équivalents et on peut très bien en effacer un des 2 et placer un lien (commande ln) à la place. Sinon il faut faire la configuration 2 fois pour les 2 fichiers. sous ubuntu il existe aussi le paquet “ldap-auth-config” permet de créer le fichier /etc/ldap.conf interactivement. on y positionne: l l'URI du serveur (mettre ldap://127.0.0.1:389/ l le DN du “search base” qui correspond au suffix cad à la racine de l'arbre l la version à utiliser est 3 l 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 à 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 plaçant dans les fichiers common-xxx(/etc/pam.d/common.auth par exemple). configuration de la résolution de noms NSS nsswitch.conf, ne placer que les 3 suivants : passwd: files ldap group: files ldap shadow: files ldap note : « compat » et « files » sont équivalents dans nsswitch.conf. VERIFICATION à ce stade, vous pouvez vous logger avec l’utilisateur de test mickey, ou faire un su. 4. PROFILS « ITINERANTS » UNIX PAR NFS NFS, créé par SUN, est un protocole qui existe depuis 1984. Pour comparer, Microsoft sortait sa première version de Windows en 1985, qui ne fonctionnait pas en réseaux, et proposera quelquechose d’equivalent plus de 10 ans après. Les montages NFS permettent à des entreprises de stocker le répertoire /home/ d'un utilisateur sur un serveur central via un partage NFS. Cela permet à l'utilisateur d'accéder à ses données personnelles dans son répertoire home en se connectant sur n'importe quel ordinateur du réseau. C’est pour cela que j’ai utilisé la terminologie Windows. C’est ce que nous allons mettre en œuvre. COTE SERVEUR Installer les packages: nfs-common nfs-kernel-server 1/créer un répertoire /public (ou /partage) 2/Publication NFS. modifier /etc/exports : Export du répertoire /public coté serveur /public *(rw,sync,root_squash) Ecriture plus sécurisée: /public 10.48.1.4/16(rw,sync,root_squash) 3/Ne pas oublier la commande exportfs -rv -r Reexporter tous les directories -v verbeux 4/ne pas oublier de donner les droits a+rwx sur le répertoire /public Verification voir les exports de un serveur showmount -e 192.168.1.11 (ou -d) COTE CLIENT 0/créer un répertoire /pointeur (qui pointera sur le serveur) Donner les droits (a+rx) sur le répertoire pointeur 1/tester avec mount mount -t nfs IP:/public /pointeur mount nfs de /pointeur (ou /home) coté client pointant sur le partage /public Modifier des entrées ldap pour que le répertoire home de l'utilisateur sur le client pointe sur le répertoire monté sur le serveur : à faire sur l'utilisateur de test mickey. Par exemple le « home » de mickey devrait pointer sur /pointeur/mickey, ne pas oublier de créer ce répertoire « mickey » et de rendre l’utilisateur mickey propriétaire. note on peut installer phpLDAPadmin qui est une interface web pour administrer un arbre LDAP. Accès par http://localhost/phpldapadmin/ Puis user (DN de connexion) cn=admin,o=gtr et password secret A adapter : modifier aussi le gid pour que le groupe de mickey corresponde Démontage : umount /pointeur 2/finaliser l’installation : fstab Modifier le fstab pour que le montage nfs se fasse à chaque démarrage de la machine cliente. Format : <server:/export> </repertoire local> nfs defaults 0 0 mount –a pour remonter toutes les définitions dans fstab Vérification à ce stade, vous pouvez vous logger avec l’utilisateur de test mickey, et vous vous retrouvez dans son répertoire personnel (pwd). Grace au montage nfs permanent, l’utilisateur retrouve son répertoire personnel depuis n’importe quelle machine. 5. SAMBA Paquets à installer : - samba Config du paquet samba: - nom de domaine: gtr - Répondez en laissant tout par défaut, car on va créer notre configuration. fichier de configuration de Samba « /etc/samba/smb.conf » Intégrer Samba à Ldap le schéma des définition samba se trouve dans le paquet samba-doc. Paquets à installer : - samba-doc L’install est decrite ici : /usr/share/doc/samba-doc/examples/LDAP/README copier le schéma et le placer dans le répertoire des schémas de LDAP: gunzip -c /usr/share/doc/samba-doc/examples/LDAP/samba.schema.gz > /etc/ldap/schema/samba.schema ajouter dans « /etc/ldap/slapd.conf » : include /etc/ldap/schema/samba.schema Penser à redémarrer le serveur LDAP ! Index à ajouter: #index uid,uidNumber,gidNumber eq # index cn,sn pres,e index homeDirectory,userPassword,loginShell eq index uid,uidNumber,gidNumber,memberUid eq index cn,sn,mail,surname,givenname eq,subinitial index sambaSID eq index sambaPrimaryGroupSID sambaDomainName eq verifier s’ils sont necessaires ? configuration de samba copier le fichier smb.con

fournit sur le site. A modifier : - workgroup = nom de votre domaine windows, par exemple GTR, - netbios name = nom de la machine serveur vue de Windows - ldap suffix - ldap admin dn - ldap group - ldap machine sous les définition globales sont définies les partages pour windows : - netlogon
Contient les scripts (.bat) exécutés à chaque connexion d'un utilisateur - profiles
Contient les profils windows de chaque utilisateur, ils sont créés automatiquement - partage
Partage commun à tous les utilisateurs du domaine - homes
Les répertoires personnels linux qui seront mappés sur une lettre windows Création des dossiers samba créer un répertoire /samba créer un répertoire /samba/netlogon et attribuer lui des droits maximal créer un répertoire /samba/partage et attribuer lui des droits maximal créer un répertoire /samba/profiles et attribuer lui des droits maximal
Redémarrer Samba: /etc/init.d/samba restart Normalement lors du démarrage, la clé « sambaDomainName=VotreDomaineSamba » est automatiquement créée dans l’annuaire LDAP sous la racine. Vérification à ce stade samba doit fonctionner, être visible et proposer les partages windows. On peut le vérifier avec la commande : smbclient -L \\vmdebian -N (N=no passwword) Paquets à installer : - smbclient smbfs 6. smbldap-tools Les scripts smbldap-tools permettent de simplifier radicalement l’adminstration des entrées LDAP pour Samba : Ils créent les entrées automatiquement. Paquets à installer : - smbldap-tools Vider la base LDAP, car nous allons tout recréer. Ces scripts smbldap-tools se configurent dans 2 fichiers, smbldap.conf et smbldap_bind.conf. Ces fichiers contiennent les paramètres de connexion à openldap, les points d’entrée dans l’arbre LDAP, et les valeurs par défaut pour les utilisateurs et les machines. La procédure d’installation et de configuration de smbldap-tools se trouve dans /usr/share/doc/smbldap-tools/README.Debian.gz. Pour l’afficher (ou alors gunzip) zless /usr/share/doc/smbldap-tools/README.Debian.gz
Dans ce document, il est indiqué comment mettre en place les 2 fichiers:
zcat /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz > /etc/smbldap-tools/smbldap.conf
cp /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf /etc/smbldap-tools/smbldap_bind.conf Connecter Samba et LDAP La commande suivante permet d’indiquer le mot de passe de l’admin de l’annuaire LDAP à Samba : smbpasswd -w votremotdepasse (« secret » par exemple) Ensuite modifier le fichier de conf smbldap.conf: - SID
Id de la machine. Pour l’obtenir: net getlocalsid - sambaDomain: "VMDEBIAN" Configuration LDAP: - suffix="o=gtr"
suffixe LDAP, cad la racine de l’arbre LDAP - usersdn="ou=etudiants,${suffix}"
points d’ancrage pour les utilisateurs - computersdn="ou=machines,${suffix}"
points d’ancrage pour les machines - groupsdn="ou=groupes,${suffix}"
points d’ancrage pour les groupes - sambaUnixIdPooldn="sambaDomainName=VMDEBIAN,${suffix}"
indique où stocker le uidNumber et gidNumber disponible suivant. Si non défini cela sera défini dans l’objet sambaDomainName.
donc inutile ?
Dans ce qui suit, les valeurs que l’on va rentrer seront inclues dans les ordres LDIF de création des prochains utilisateurs. Configuration des comptes Unix: - userHome="/public/%U" Configuration SAMBA: - userSmbHome=\\VMDEBIAN\%U
chemin UNC du répertoire home (%U = username) - userProfile=\\VMDEBIAN\profiles\%U
chemin UNC du répertoire du profile (%U = username) - userHomeDrive="H:"
Lecteur où sera connecté le répertoire home unix de l’utilisateur - userScript="logon.bat"
script de démarrage au netlogon. Doit se trouver dans le partage correspondant. - mailDomain="univmed.com" fichier smbldap_bind.conf: - masterDN et SlaveDN à modifier, par exemple "cn=Manager,o=gtr" Mise à jour de la base LDAP La commande suivante permet d’initialiser la base de données LDAP en fonction des modifs faite dans le fichier smbldap.conf: # smbldap-populate Attention : aucune erreur ne doit apparaître. En cas d’erreur, corriger le problème dans smbldap.conf et relancer cette commande. Cette commande créée: * Les différents OU (Organisation Unit) qui contiendront les Machines, utilisateurs et Groups * Deux UID : root et nobody qui seront dans OU = utilisateurs * Root est le compte admin de la base * nobody est le compte invité de la base * Plusieurs CN (Common Name): Les groupes qui seront dans OU = Groups Vérification Créer un nouvel utilisateur via smbldap-tools : # smbldap-useradd -a -P -c "Donald Duck" donald * -a : désigne un utilisateur * -c : Information Gecos : Le nom entier * -m : Créé le répertoire personnel * -P : création du mot de passe Lisez l'aide: # smbclient -L \\ServeurSamba -U donald A comparer avec # smbclient -L \\vmdebian -N (N=no passwword) 7. Client de Samba : Windows A faire pour ajouter mickey dans le groupe des administrateurs Comment ajouter un nouvel utilisateur à un groupe Avec phpldapadmin :
Sélectionner le groupe (sous ou=groupes), par exemple « Domain Admins »
chercher l’attribut « memberUID »
cliquer sur « Ajouter une valeur »
Ensuite, il faut saisir le login de l’utilisateur Autoriser un utilisateur du LDAP à ajouter des ordinateurs au domaine Par défaut, aucun utilisateur du LDAP n’est autorisé a ajouter ou supprimer des ordinateurs du domaine. En effet, il ne suffit pas d’ajouter un utilisateur au groupe « Administrateur » ou « Administrateur du domaine pour que ça fonctionne. Pour donner ces droits spéciaux à un utilisateur, il faut utiliser cette commande : net -U adminLDAP rpc rights grant 'VotreDomaine\VotreUser' SeMachineAccountPrivilege Commentaires :
adminLDAP : Un des membres du groupe « Administrateur du domaine » du LDAP
VotreDomaine : Le nom de votre domaine contenant l’utilisateur à ajouter
VotreUser : Le login de l’utilisateur à ajouter Exemple:

net -U mickey rpc rights grant 'VMDEBIAN\mickey' SeMachineAccountPrivilege configuration virtualbox on va utiliser la fonction de « réseau interne » de virtualbox. Dans ce cas les machines virtuelles seront dans un même sous-réseau, 198.168.0.x, par contre virtualbox ne fera plus office de serveur dhcp. On va faire en sorte que la machine linux fera office de gateway pour la ou les autres machines du réseau interne. Machine Linux : partie réseau, adaptateur 1, sélectionner NAT. Adaptateur 2, sélectionner réseau interne. Donner un alias au réseau, le même par exemple « nbzone ». Machine windows : partie réseau, adaptateur 1, sélectionner réseau interne. Donner un alias au réseau, par exemple « nbzone ». Une fois booté sous Linux : - monter la carte réseau du réseau interne, avec par exemple ifconfig eth1 192.168.0.251 - activer la fonction routage du noyau
echo 1 > /proc/sys/net/ipv4/ip_forward donner info sur iftab Une fois booté sous windows: Tester si les machines se voient (avec ping) On peut mettre les 3 commandes ci-dessous dans un fichier .bat: netsh interface show interface netsh interface ip set address name="Local Area Connection" static 192.168.0.20 255.255.255.0 192.168.0.251 1 netsh interface ip set dns "Local Area Connection" static 10.0.2.3 pause Cela donne l’adresse statique 20, positionne le gateway, et positionne le dns sur celui de virtualbox. Intégration windows au domaine faire rentrer la machine dans le domaine todo : plus de details sur la procédure vérifier que les users mickey et donald peuvent se connecter vérifier que leur profile est bien sauvegardé dans /samba/profiles Script ouverture de session Voici comment mettre en place les scripts d’ouvertures de sessions pour les clients Windows se connectant au contrôleur de domaine Samba : Créer le fichier « logon.bat » et le placer dans le dossier « /samba/netlogon ». exemple de contenu: net time \\VMDEBIAN /set /yes
net use n: \\VMDEBIAN\cafoutch le net use connecte automatiquement le partage commun à tous les utilisateurs mettre la machine cliente à la même heure que celle du serveur Linux. 8. Sécurisation de la solution 1/Sécuriser le passwd admin de LDAP Slappasswd –s secret Renvoie quelquechose comme {SSHA}10oMlQ0n4TsYMh+6idNeDAkUUgzZ7cfy Placer cette valeur dans rootpw dans le fichier slapd.conf rootpw {SSHA}10oMlQ0n4TsYMh+6idNeDAkUUgzZ7cfy 2/gérer les acl Une commande existe pour tester les accès : slapacl il sera nécessaire d'apprendre à manipuler slapacl. voir sa man page ;-) Exemples sous Debian : le mot de passe peut être vu/modifié par le propriétaire authentifié ou l'admin access to attrs=userPassword,shadowLastChange by dn="cn=admin,o=gtr" write by anonymous auth by self write b 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,o=gtr" write by * read 3/smbldap smbldap_bind.conf contient le mot de passe en clair. Il vaut mieux changer les droits de celui-ci : # chmod 600 /etc/smbldap-tools/smbldap_bind.conf 9. AUTOMOUNT Un inconvénient de l'utilisation de /etc/fstab est que le serveur subit autant de connexion NFS que de machine clientes, et ceci indépendamment de leur utilisation. Cela surcharge inutilement le serveur. Une alternative à /etc/fstab consiste à utiliser l'utilitaire basé sur le noyau automount, qui montera et démontera les systèmes de fichiers NFS automatiquement au moment du login, économisant ainsi des ressources. installer le paquet: autofs cela crée le service autofs (sous /etc/init.d donc) qui sert à contrôler la commande automount par le biais du fichier de configuration principal /etc/auto.master. Le fichier de configuration principal liste les points de montage sur le serveur qui sont liés à une correspondance automount. Chaque ligne de ce fichier associe un point de montage à un autre fichier qui décrit les filesystemes à monter pour ce point de montage. Exemple: /home /etc/auto.home /pointeur /etc/auto.pointeur --timeout=3 Le 1er élément de la ligne indique l'emplacement du montage sur le système de fichiers local. Le 2e élément indique un autre fichier dans lequel sera décrit comment faire le montage. Ce 2e fichier est généralement nommé auto.<repertoire>, où <repertoire> est le point de montage désigné dans auto.master. c’est la méthode préconisée pour monter automatiquement des exports NFS. Cela aura pour effet que tous les accès à l’intérieur du répertoire /home ou /pointeur entraineront la consultation de la correspondance définie dans le fichier /etc/auto.home ou auto.pointeur. Le parametre optionnel « timeout » permet d’indiquer le nombre de secondes avant démontage lorsque le répertoire n’est plus utilisé. Que contient ce second fichier auto.pointeur ? une liste de ligne mettant en correspondance des sous-répertoires et des commandes de montages : </sous/répertoire> -<options> <server>:</export> Pour pas avoir à préciser chacun des sous répertoire, on va utiliser une écriture générique : * -fstype=nfs 10.1.26.249:/public/& "*" indique tous les sous-répertoires auquel un utilisateur tente d'accéder L’action est montage NFS sur le 10.1.26.249 sur l’export /public. Notez le "&" qui reprend le reste du chemin de sorte que /pointeur/mickey sera mappé sur /public/mickey Vérification Assurez vous qu’aucun montage NFS n’est actif (« mount »). Commentez la ligne de fstab correspondant au montage statique fait précédemment. Faire un cd dans /pointeur/mickey : Le répertoire est monté. Faire un cd ailleurs. Le montage disparaît. Essayer idem en se logguant. Vous pouvez utiliser # /etc/init.d/autofs status à connaître les montages actifs # /etc/init.d/autofs reload à demande à automount de prendre en compte les modifs. 10. AUTOMOUNT SOUS LDAP On va migrer la définition de autofs/automount dans la base ldap. installer le paquet: autofs-ldap le guide complet se trouve sous : /usr/share/doc/autofs-ldap (README.ldap_master) 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