Authentification des clients Linux sur un annuaire LDAP

(source : ClientsHardyHeron et ScribeNG sur le wiki Eole)

Généralités

Il existe trois grandes familles de Linux : RedHat (dont Mandriva), Debian (dont Ubuntu), Suse.

Les outils utilisés pour configurer le client LDAP sont les mêmes, mais la façon de les installer diffère :

- sur la plupart des distribution une option « avancé » lors de la phase d'installation (en général lors de la création des comptes utilisateurs) permet de sélectionner un annuaire LDAP.
- Ce n'est pas le cas sur Ubuntu : il faut réaliser l'opération après l'installation initiale.

Les paramètres à fournir sont au minimum :

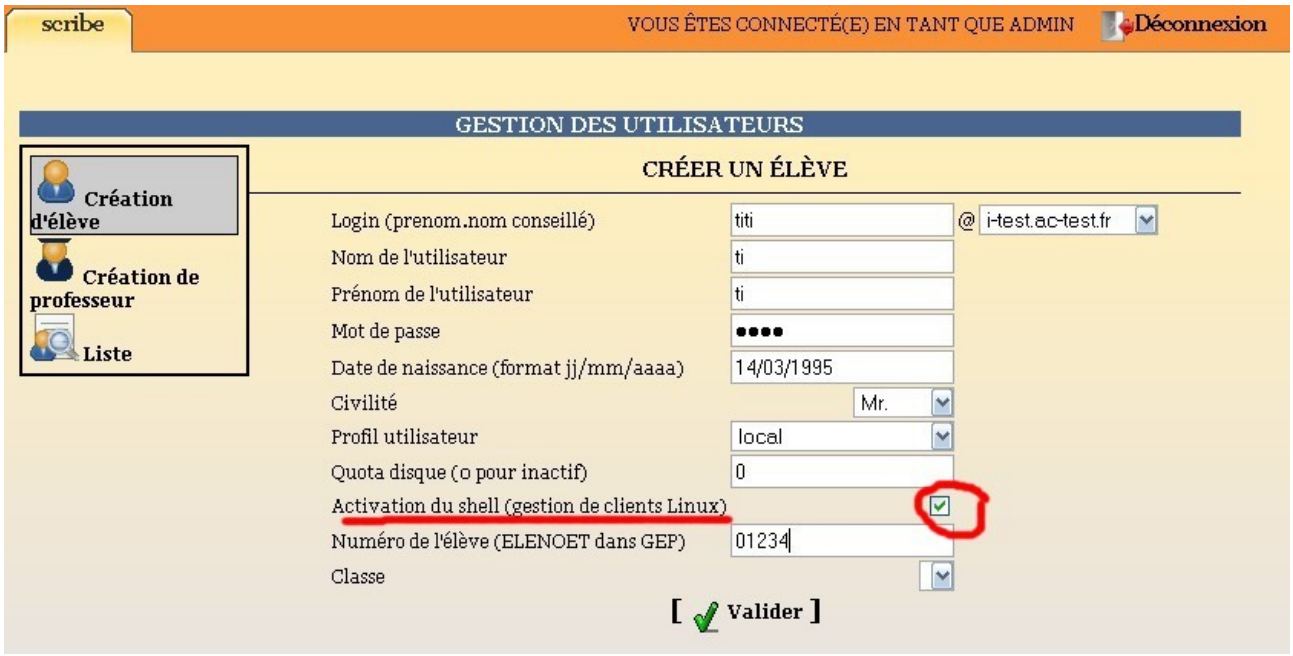
- L'adresse ou le nom DNS du serveur LDAP
- La racine DN : « o=gouv,c=fr »

L'accès au LDAP se fait de façon anonyme, aucun droit en écriture n'étant nécessaire.

Il se pose ensuite le problème du montage des espaces personnels ou partagés des utilisateurs. S'il s'agit de partages Microsoft ou Samba, il faut installer et configurer le client Samba.

Enfin, il faut donner aux utilisateurs LDAP les droits d'accès aux ressources de la machines (usb, son, graveur, etc...), ce qui revient à intégrer ces utilisateurs dans les groupes locaux ad-hoc.

Remarque : dans le cas de Scribe, les utilisateurs créés n'ont pas de shell Unix (donc pas le droit de se connecter) à moins que la case suivante soit cochée :



Installation d'Ubuntu : configuration simplifiée

Depuis la version 7.10, il existe un outils qui simplifie l'installation du client LDAP; il peut comporter des lacunes !!

Cet outils se nomme AuthClientConfig. Il s'installe avec le paquet ldap-auth-client.

Ensuite la commande pour le lancer :

```
sudo auth-client-config -a -p lac_ldap
```

Installation d'Ubuntu : configuration complète

sudo su
apt-get install smbfs
apt-get install libpam-mount
répondre **non** à la question : voulez vous que le fichier conf existant soit converti en xml.

apt-get install ldap-utils libpam-ldap
Répondre aux questions:
1. Adresse ip du serveur ldap utilisé: host 192.168.231.253 (ip de votre scribe)
2. Nom distinctif: « o=gouv,c=fr » sans espaces
3. Ldap version to use: validez 3 avec « entrée »
4. Faut-il créer une base de données locale pour l'administrateur?: non
5. La base de données requiert-elle une connexion authentifiée?: non

Éditez /etc/nsswitch.conf et mettez les trois lignes suivantes aux valeurs:
passwd:files ldap
group:files ldap
shadow:files ldap

Éditez le fichier /etc/ldap/ldap.conf comme ceci

BASE o=gouv,c=fr
URI ldap://192.168.231.253

Éditez le fichier /etc/ldap.conf comme ceci

host 192.168.231.253
base o=gouv,c=fr

Copiez ce fichier dans les repertoires /usr/share/libnss-ldap et /usr/share/libpam-ldap.

Dans /etc/pam.d, on édite les fichiers comme suit:

common-account:
account sufficient pam_unix.so
account required pam_ldap.so use_first_pass

common-auth:
auth sufficient pam_unix.so
auth required pam_ldap.so use_first_pass

common-password:
password sufficient pam_unix.so
password required pam_ldap.so use_first_pass

common-session:
session sufficient pam_unix.so
session required pam_ldap.so
session optional pam_mkhomedir.so

Éditez /etc/pam.d/kdm et remplacez son contenu par ceci:

```
#
# /etc/pam.d/kdm - specify the PAM behaviour of kdm
#
# The standard Unix authentication modules, used with
# NIS (man nsswitch) as well as normal /etc/passwd and
# /etc/shadow entries.
#@include common-auth
#@include common-account
#@include common-password
#@include common-session
auth required pam_mount.so
auth required pam_group.so
auth sufficient pam_ldap.so use_first_pass
auth required pam_unix.so use_first_pass
auth required pam_env.so
account sufficient pam_ldap.so
account sufficient pam_unix.so
password required pam_unix.so nullok obscure min=4 max=8 md5
session required pam_unix.so
session optional pam_mkhomedir.so
session optional pam_mount.so
```

Pour empêcher le basculement de l'environnement vers l'anglais, ajouter les lignes suivantes à la fin du fichier /etc/profile:

```
export LC_ALL=fr_FR.utf8
export LANG=fr_FR.utf8
export LANGUAGE=fr_FR.utf8
```

Automatisation des modifications

Exercice :

Une fois que la configuration fonctionne, copiez tous ces fichiers sur une clé usb et créez un script nommé « patch-ldap » pour les copier automatiquement sur d'autres autres machines Ubuntu :

#!/bin/sh	Début du script installation de **smbfs** installation de **libpam-mount** installation de **ldap-utils** et **libpam-ldap** copie de **nsswitch.conf** copie de **ldap/ldap.conf** copie de **ldap.conf** copie de **common-account** copie de **common-auth** copie de **common-password** copie de **common-session** copie de **pam.d/kdm** copie de **pam_mount.conf.xml** copie de **/etc/profile**

Annexe 1 : Rendre les utilisateurs membres des groupes locaux

(source : forum ubuntu)

*If the lac_ldap option fails (as it did on my 8.10 system) the following settings were successful. These settings will also cause domain (ldap) users to become members of local groups so that local devices needing fuse, plugdev, scanner etc... membership will work properly. For example: If you are having problems with automounting of usb drives the pam_group.so option is likely your problem.

```
nano /etc/auth-client-config/profile.d/open_ldap
```

and paste the following into it:

```
[open_ldap]
nss_passwd=passwd: files ldap
nss_group=group: files ldap
nss_shadow=shadow: files ldap
nss_netgroup=netgroup: files ldap
pam_auth=auth       required     pam_env.so
        auth       sufficient   pam_unix.so likeauth nullok
#the following line (containing pam_group.so) must be placed before pam_ldap.so
#for ldap users to be placed in local groups such as fuse, plugdev, scanner, etc ...
        auth       required     pam_group.so use_first_pass
        auth       sufficient   pam_ldap.so use_first_pass
        auth       required     pam_deny.so
pam_account=account    sufficient   pam_unix.so
        account    sufficient   pam_ldap.so
        account    required     pam_deny.so
pam_password=password   sufficient   pam_unix.so nullok md5 shadow
        password   sufficient   pam_ldap.so use_first_pass
        password   required     pam_deny.so
pam_session=session    required     pam_limits.so
        session    required     pam_mkhomedir.so skel=/etc/skel/
        session    required     pam_unix.so
        session    optional     pam_ldap.so
```

Now to activate that pam profile do the following:

```
auth-client-config -a -p open_ldap
```

To assign local groups to domain (ldap) users do the following:

```
nano  /etc/security/group.conf
```

and add the following to the end of the file (note you can determine which groups to add to this line by logging in as a local user and using the 'groups' command):

```
*; *; *; Al0000-2400;audio,cdrom,floppy,plugdev,video,fuse,scanner,dip
```

You should now have local groups showing up for users logging in via gdm and ssh ('su username' did not give these groups on my system). Note that I did not have to edit the gdm, sshd, or login files in /etc/pam.d/ as they include a call to @include common-auth giving them the pam_group.so line in the proper order (before pam_ldap.so).

You can test local groups using ssh (assuming nickf is a ldap user):

```
ssh nickf@localhost
```

once you are logged in as a ldap user you can see your groups with the 'id' or 'groups' command

```
nickf@ubuntu-ltsp:~$ id
uid=10178(nickf) gid=512(Domain Admins)
groups=24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),104(scanner),107(fuse),512(Domai
n Admins),544(Administrators),10000(Teachers)
```