

**Principes et pratiques de l'administration des
systèmes**

Module 3I015

Semaines 3 et 4

1. Gestion locale des utilisateurs

Étape 1 – Gestion des utilisateurs avec les commandes du shell

En utilisant les commandes `useradd`, `groupadd`, `usermod`, `groupmod`, *etc.*, créez sur vos trois machines virtuelles les deux nouveaux groupes suivants :

- `etudiants` de GID 600,
- `enseignants` de GID 700.

Puis créez deux étudiants `student1` et `student2`, d'UID respectifs 600 et 601, appartenant au groupe `etudiants`. Vous ferez en sorte que les home directories de ces étudiants soient, respectivement, les répertoires `/users/student1` et `/users/student2`. Évidemment, vous ne créez ces répertoires que sur mSLDAP puisque `/users` est exporté par NFS sur toutes les machines.

Enfin, vous ferez en sorte que les mots de passe de ces deux étudiants soient exactement les mêmes que leur login.


Préparation avant le TME: *Étudiez les manuels des commandes `useradd`, `groupadd`, `passwd` afin de déterminer les options qui vous seront utiles.*

Étape 2 – Test de bon fonctionnement

Testez que vos nouveaux utilisateurs peuvent se connecter à leur compte sur mSLDAP et c1LDAP, qu'ils peuvent écrire des fichiers sur leur compte, qu'ils peuvent également lire leurs fichiers, et qu'ils retrouvent d'une machine à l'autre les fichiers qu'ils ont créés sur l'autre machine.

Étape 3 – Gestion des utilisateurs avec les fichiers système

En éditant le fichier `/etc/passwd`, créez un enseignant `teacher1`, d'UID 700, appartenant au groupe `enseignants`. Vous ferez en sorte que le home directory de l'enseignant soit `/users/teacher1`. Faites en sorte que le fichier `/etc/shadow` soit cohérent avec votre `/etc/passwd` !

 N'oubliez pas de créer le home directory de l'enseignant. N'oubliez pas également de copier le contenu de `/etc/skel` dans le home directory de l'utilisateur. Vérifiez bien que votre copie a fonctionné (vous ne devez pas voir un sous-répertoire `skel` dans le home directory!).

Enfin, vous ferez en sorte que le mot de passe de l'enseignant soit exactement le même que son login.

Étape 4 – Test de bon fonctionnement

Testez bien que votre nouvel utilisateur peut se connecter à son compte sur mSLDAP et c1LDAP, qu'il puisse écrire des fichiers sur son compte, qu'il puisse également lire ses fichiers.

2. Gestion des utilisateurs par LDAP

Comme nous l'avons vu en cours, afin de gérer les utilisateurs par LDAP, il faut installer plusieurs packages, notamment `libnss-ldap` qui permet à PAM et NSS d'exploiter un serveur LDAP. Hélas, ce package n'a pas été installé sur vos machines. Fort heureusement, on peut le trouver sur les repositories Debian et le poste hôte n°2 de la salle de TME en est justement un. Mais vos machines virtuelles ne peuvent pas communiquer avec lui car le poste n°2 n'est pas sur le même réseau que celles-ci (il est sur le réseau 192.168.2.0). Afin de pallier cela, dans les étapes suivantes, vous allez faire en sorte que `ssLDAP` devienne une passerelle entre votre réseau et celui du poste hôte n°2. Par la suite, vous pourrez accéder au repository Debian et installer le package manquant `libnss-ldap`.

Étape 5 – Insertion d'une nouvelle carte réseau dans `ssLDAP`

Une passerelle ou un routeur est une machine qui contient plusieurs cartes réseau (une pour chaque réseau qu'elle connecte). Pour l'instant, votre `ssLDAP` a une carte réseau `enp0s3` configurée pour votre réseau de machines virtuelles (adresse IP : 192.168.X.2). Vous allez simuler l'ajout d'une 2ème carte réseau. Pour cela, éteignez votre machine virtuelle `ssLDAP` puis, dans la fenêtre de votre VirtualBox, cliquez sur le bouton « configuration », puis sur le menu « réseau ». Vous devriez voir une fenêtre à peu près similaire à celle de la figure 1. Actuellement, seule la carte 1 est activée et son mode d'accès est « réseau interne » (elle doit rester dans ce mode).

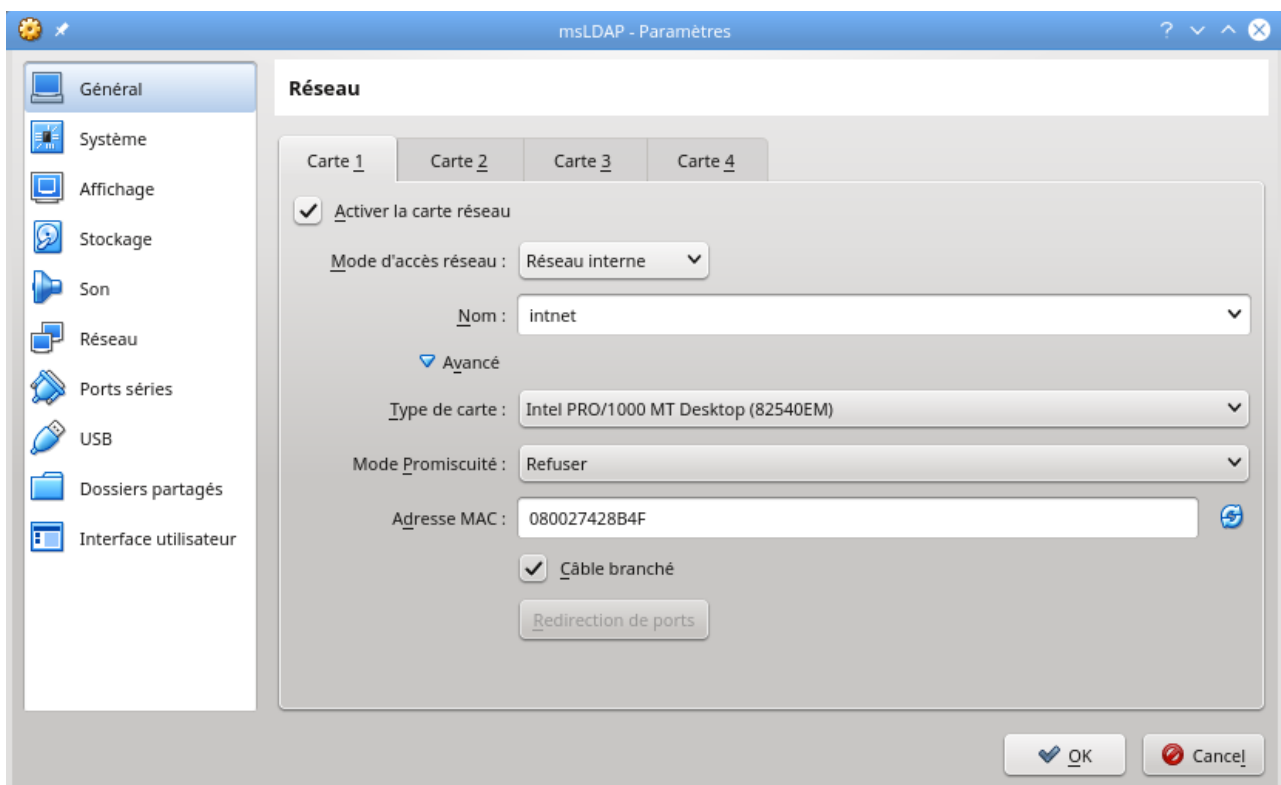


FIGURE 1 – Configuration du réseau des machines virtuelles

Activez maintenant la 2ème carte réseau, avec pour mode d'accès réseau « NAT »¹. Le mode « NAT » signifie que votre machine virtuelle se connecte à un routeur virtuel de VirtualBox, interne à votre

1. Si vous voulez comprendre les différents modes de virtualisation du réseau, reportez-vous à l'URL <https://www.virtualbox.org/manual/ch06.html>

machine. VirtualBox vous fournit alors, via un serveur DHCP interne, une adresse IP sur un réseau local interne ; VirtualBox transmet ensuite toutes vos requêtes à la carte réseau de votre machine hôte et s'arrange (via de l'« IP masquerading ») pour que toutes vos requêtes aient l'air d'émaner de cette dernière. Celle-ci étant reliée à internet, internet peut lui répondre. Les paquets de réponse sont ensuite acheminés au routeur virtuel de VirtualBox, qui les retransmet enfin à la 2ème carte réseau de ssLDAP. Grâce à ce mécanisme, certes un peu complexe, l'ajout de la nouvelle carte réseau permettra à ssLDAP d'échanger des paquets avec internet (ici symbolisé par le poste de travail n°2 si vous êtes en salle de TME). L'avantage du mode d'accès « NAT » est qu'il ne nécessite pas de demander une nouvelle adresse IP à un serveur DHCP extérieur à votre machine hôte. Par exemple, si vous travaillez chez vous, aucune nouvelle adresse IP ne sera demandée à votre box ADSL. Mais le véritable avantage réside en salle de TME : ni votre machine hôte ni aucune de vos machines virtuelles n'a besoin de récupérer une adresse IP via un serveur DHCP. Le poste n°2 n'a donc pas besoin d'être serveur DHCP. Ainsi, on peut le démarrer même en dehors des périodes de TME de 3I015, cela n'a aucune incidence sur les autres machines des autres salles de TME (celles-ci récupérant leurs adresses IP à partir d'un serveur DHCP, en l'occurrence celui de la PPTI puisque c'est le seul serveur sur le réseau).

En résumé, maintenant, ssLDAP possède deux cartes réseau, la carte n°1 étant en « réseau interne » et la carte n°2 en « NAT ».

Redémarrez maintenant votre machine virtuelle ssLDAP.

Étape 6 – Détection d'une nouvelle carte réseau dans ssLDAP

Afin de déterminer si votre manipulation a bien fonctionné, vous pouvez utiliser dans un shell la commande `ip link show`, qui devrait vous produire un affichage similaire à :

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:86:5b:51 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:c8:1f:e3 brd ff:ff:ff:ff:ff:ff
```

Notez qu'il y a deux `enp0s`. Ce sont vos cartes réseau. Ici, la nouvelle carte s'appelle donc `enp0s8`. Une autre alternative pour déterminer quelles sont les cartes réseau installées dans votre machine est de lire le contenu du fichier `/proc/net/dev` (comme vous l'avez vu au premier TME) :

```
[root@ssLDAP ~]# cat /proc/net/dev
```

Inter-	Receive								Transmit				
face	bytes	packets	errs	drop	fifo	frame	compressed	multicast	bytes	packets	errs	drop	f
lo:	17688	194	0	0	0	0	0	0	17688	194	0	0	
enp0s3:	23554	143	0	0	0	0	0	36	20124	132	0	0	
enp0s8:	8337	45	0	0	0	0	0	36	4969	33	0	0	

Étape 7 – Configuration de la nouvelle carte réseau

L'objectif de cette nouvelle carte est de pouvoir accéder au réseau géré par le poste hôte n°2. Pour cela, vous avez besoin d'une adresse IP sur un autre réseau que celui de votre première carte réseau (192.168.X.0/24). Étant donné que vous avez rajouté votre nouvelle carte réseau en mode d'accès

NAT, VirtualBox vous proposera une adresse IP via son serveur DHCP, qui gère des adresses IP dynamiques (cf. l'étape 5).

Éditez le fichier `/etc/network/interfaces` et rajoutez les lignes :

```
auto enp0s8
iface enp0s8 inet dhcp
```

Après avoir redémarré votre service `networking`, si vous exécutez un `ifconfig`, vous devriez voir vos deux interfaces réseau bien configurées. L'interface réseau `enp0s8` devrait avoir une adresse IP similaire à `10.0.3.15`. Testez avec des `ping` sur la machine `ftp.lip6.fr` que votre installation est correcte.

Étape 8 – client DNS

Faites un `ping` sur la machine `google.fr`. Là encore, le ping devrait fonctionner.

Votre machine virtuelle connaît l'adresse IP de `ftp.lip6.fr` car celle-ci a été insérée dans votre `/etc/hosts`. Mais comment connaît-elle l'adresse IP de `google.fr` alors que celle-ci n'est pas dans `/etc/hosts`? En effet, il est trop fastidieux de devoir ajouter dans `/etc/hosts` les adresses IP de toutes les machines avec lesquelles on souhaite converser. Une autre possibilité, et c'est ce qui a été utilisé dans votre machine virtuelle, est d'exploiter un serveur DNS (*Domain Name Server*). DNS est un service qui permet de faire l'association entre des noms de machines et leur adresse IP. Les adresses IP des serveurs DNS que vous utilisez sont spécifiés dans le fichier `/etc/resolv.conf`. Si vous observez le contenu de celui-ci sur `ssLDAP`, vous verrez qu'il contient notamment une ligne similaire à :

```
nameserver 8.8.8.8
```

Cette ligne indique que l'on utilisera le serveur DNS d'adresse IP `8.8.8.8` afin de convertir des noms de machines en leurs adresses IP. Il s'agit d'un serveur DNS de google répondant au doux nom de `google-public-dns-a.google.com`. Si vous faites un `ping google.fr`, le ping fonctionnera car, grâce au DNS `8.8.8.8`, votre commande sera transformée en `ping 192.168.2.2` si vous êtes en salle de TME, et en `ping 172.217.22.131` si vous travaillez sur votre ordinateur personnel.

Étape 9 – Configuration de la passerelle

Votre machine `ssLDAP` peut maintenant communiquer avec votre réseau via la première carte réseau et avec le poste n°2 (ou internet) via la 2ème carte réseau. Mais ce n'est pas encore une passerelle car elle ne transmettra pas encore les paquets de `MSLDAP` ou `C1LDAP` vers le poste n°2 et inversement. Pour que `ssLDAP` le soit, il faut activer le mode "IP forwarding" de votre noyau Linux. Par défaut, ce mode n'est pas activé. Pour le voir, il suffit de taper la commande `sysctl net.ipv4.ip_forward`, qui vous produira l'affichage `net.ipv4.ip_forward = 0`. Lorsque l'IP forwarding est activé, il y a un 1 à la place du 0 à la fin de l'affichage.

Pour activer ce mode pour la session courante (jusqu'à l'extinction ou redémarrage de la machine virtuelle), il suffit de taper `sysctl -w net.ipv4.ip_forward=1` et de redémarrer votre service réseau. Si vous voulez pérenniser ce mode lors des prochains démarrages, éditez le fichier `/etc/sysctl.conf` et supprimez le # de la ligne `# net.ipv4.ip_forward = 1` (cela décommentera cette ligne).

Étape 10 – Test de bon fonctionnement de la passerelle

Dans cette étape, vous allez faire en sorte que les machines `msLDAP` et `c1LDAP` utilisent votre passerelle pour communiquer avec des machines qui ne sont pas sur le même réseau qu'elles. Pour cela, il vous suffit d'éditer le fichier `/etc/network/interfaces` de vos machines `msLDAP` et `c1LDAP`, et d'indiquer que leur passerelle est `ssLDAP` : autrement dit, rajoutez avant la ligne où vous indiquez le `broadcast` de `enp0s3` une ligne `gateway 192.168.X.2`, où `192.168.X.2` correspond à l'adresse IP de la première carte réseau de `ssLDAP`. Arrêtez proprement les exportations et importations par NFS puis redémarrez les services réseau de ces machines. En tapant la commande `route -n`, vous devriez observer un affichage similaire à :

Table de routage IP du noyau

Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface
0.0.0.0	192.168.X.2	0.0.0.0	UG	0	0	0	enp0s3
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	enp0s3
192.168.X.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s3


La ligne en rouge, de par son 2ème champ, montre que votre passerelle est utilisée. Si vous ne voyez pas une telle ligne, il est possible que le redémarrage du réseau se soit mal passé. Dans ce cas, arrêtez le service réseau et vérifiez via la commande `ifconfig` que votre carte `enp0s3` n'apparaît plus dans la liste des cartes réseau. Si elle y apparaît encore, tapez la commande `ifdown enp0s3` pour la forcer à s'arrêter puis redémarrez à nouveau votre service réseau. En principe, cela devrait suffire pour que les tables de routage se mettent à jour et que la commande `route -n` produise l'affichage mentionné ci-dessus. Si ce n'est toujours pas le cas, rebootez votre machine virtuelle puis refaites un `route -n`.

Une fois que votre passerelle est bien définie dans votre table de routage, faites un `ping ftp.lip6.fr`. Normalement, le ping devrait vous indiquer que vous arrivez à communiquer avec la machine distante et, par conséquent, que votre passerelle fonctionne correctement.

N'oubliez pas de réaliser ces opérations sur les deux machines `msLDAP` et `c1LDAP`.

Étape 11 – Configuration du serveur LDAP sur msLDAP

Sur votre machine `msLDAP`, les packages `slapd` et `ldap-utils` ont déjà été installés. Mais rappelez-vous que le haut de l'arborescence de l'annuaire LDAP n'est pas, par défaut, ce que l'on souhaite. Faites donc en sorte que le haut cette arborescence soit `dc=3i015,dc=info` en utilisant la commande `dpkg-reconfigure` comme vu en cours (utilisez comme password de l'administrateur `3i015-ldap`).

 pour passer d'un champ à l'autre, il faut impérativement utiliser la touche « `tab` ». C'est particulièrement vrai lorsque vous saisissez le mot de passe de l'administrateur : si vous tapez ce mot de passe et que vous appuyez sur la touche « `Entree` », votre mot de passe comportera un `\n` à la fin, ce qui sera incorrect pour la suite. Ici, il faut donc taper le mot de passe, puis appuyer sur la touche « `tab` » afin que le curseur souris se place sur `<OK>` et, enfin, appuyer sur la touche « `Entrée` ».

Vérifiez que votre service LDAP est bien démarré. Au besoin, démarrez-le. Pérennisez votre installation via un `systemctl enable` lorsque tout semble fonctionner correctement.

Étape 12 – Configuration des clients LDAP

Éditez le fichier de configuration du client LDAP de `msLDAP`, autrement dit `/etc/ldap/ldap.conf`, et paramétrez-le de façon à ce que le client puisse interroger le serveur LDAP que vous venez d'installer.

Attention : dans le cours, l'adresse IP utilisée est `127.0.0.1`, qui est l'adresse du loopback ; ici, il vous

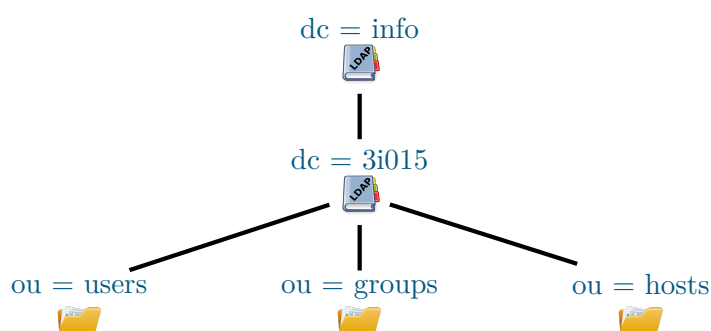
faudra utiliser l'adresse IP de msLDAP sur sa carte enp0s3 ou bien son nom tel que défini dans le fichier `/etc/hosts`. Testez que votre client se connecte bien au serveur, par exemple en exécutant un `ldapsearch -x dn`.

Paramétrez également les clients LDAP des machines ssLDAP et c1LDAP. Là encore, testez bien que vos clients se connectent au serveur LDAP.

Faites en sorte de pérenniser le démarrage de votre serveur LDAP sur msLDAP via un `systemctl enable slapd`.

Étape 13 – Remplissage de l'annuaire LDAP

Sur votre serveur msLDAP, nous souhaitons avoir l'arborescence suivante :



Il vous faut donc rajouter à votre arborescence les nœuds `ou = users`, `ou = groups` et `ou = hosts`, qui vont respectivement contenir par la suite les utilisateurs, les groupes et les noms de machine de votre réseau. Pour cela, vous allez créer sur le serveur LDAP (autrement dit msLDAP) des enregistrements de type “organizational unit” dans un fichier au format LDIF, comme nous l’avons vu en cours. Par exemple, pour `ou=users`, les lignes à écrire dans le fichier sont du type :

```
dn: ou=users,dc=3i015,dc=info
objectClass: organizationalUnit
ou: users
```

Insérez le contenu de ce fichier dans votre annuaire via la commande vue en cours :

```
ldapadd -x -D cn=admin,dc=3i015,dc=info -W -f fichier.ldif
```

Le mot de passe attendu par la commande `ldapadd` est celui de l’administrateur de votre annuaire LDAP, autrement dit `3i015-ldap`. Vous pouvez vérifier que l’insertion s’est bien passée en utilisant la commande `ldapsearch -x ou`, qui devrait vous indiquer que `ou = users`, `ou = groups` et `ou = hosts` existent.

Étape 14 – Création de nouveaux utilisateurs sur msLDAP

Vous pouvez maintenant créer de nouveaux utilisateurs sur msLDAP en i) les rajoutant dans l’annuaire LDAP et ii) en créant leurs home directories. Le plus simple pour cela consiste tout simplement à utiliser la commande `ldapadduser` du package `ldapscripts` vue en cours. Mais avant cela, il vous faut configurer ce package comme vu en cours (cf. fichier `/etc/ldapscripts/ldapscripts.conf`) :

- Il faut renseigner quel est le serveur à utiliser, ainsi que les SUFFIX des users, des groupes et des machines ;
- On souhaite ici que les identifiants minimum des `users`, `groups` et `hosts` soient de 2000 ;
- On souhaite également que `ldapadduser` crée les home directories. **Attention** : contrairement aux installations élémentaires de Linux où les home directories se trouvent dans `/home`, vos

home directories sont dans /users. Vous pouvez spécifier cela dans le fichier /etc/adduser.conf ;

- Enfin, n'oubliez pas d'indiquer le mot de passe de votre administrateur LDAP (c'est-à-dire 3i015-ldap) dans le fichier /etc/ldapscripts/ldapscripts.passwd. **Attention** : dans ce fichier, il est important de ne pas faire un retour chariot après le mot de passe. Si vous avez utilisé un éditeur de texte pour saisir le mot de passe, vérifiez que celui-ci n'a pas inséré de « \n » à la fin du mot de passe. Pour cela, vous pouvez utiliser la commande :

```
hexdump -c /etc/ldapscripts/ldapscripts.passwd
```

Si vous observez un « \n », vous pouvez utiliser emacs afin de le supprimer (certains éditeurs comme gedit ont en effet tendance à rajouter automatiquement l'« \n » en fin de fichier). Pour vous éviter tous ces désagréments, vous pouvez saisir votre mot de passe, non pas en utilisant un éditeur de texte, mais plutôt la commande :

```
echo -n 3i015-ldap > /etc/ldapscripts/ldapscripts.passwd
```

Créez maintenant sur MSLDAP un nouvel étudiant student3 grâce à cette commande. Affectez-lui un mot de passe grâce à la commande ldapsetpasswd. Vous pouvez vérifier que student3 a bien été créé en utilisant, par exemple, la commande ldapsearch -x uid.

Si ldapadduser ne fonctionne pas du fait d'« invalid credentials », vérifiez bien que vous avez indiqué le bon serveur LDAP à utiliser (ldap://...) ainsi que le bon mot de passe. Si vous pensez que vous vous êtes trompé quand vous avez saisi le mot de passe dans le dpkg-reconfigure slapd, vous pouvez modifier le mot de passe de l'administrateur de l'annuaire LDAP en réalisant l'étape 15.

Étape 15 – Changement de mot de passe LDAP (optionnel)

Cette étape n'est à réaliser que si le mot de passe que vous avez saisi lors du dpkg-reconfigure slapd est incorrect.

Afin de modifier le mot de passe de l'administrateur du LDAP, il convient tout d'abord de déterminer où se trouve ce mot de passe dans l'annuaire LDAP et quel est son encodage. Pour cela, tapez la commande suivante :

```
ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b \
  cn=config olcRootDN=cn=admin,dc=3i015,dc=info dn olcRootPW
```

Cette commande devrait vous produire un affichage similaire à :

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: olcDatabase={1}mdb,cn=config
olcRootPW: {SSHA}+OVZVr34Hlx5ww9fqj/YLzReBajDgxV5
```

Seules les deux dernières lignes sont intéressantes : l'avant dernière ligne vous indique le *distinguished name* de l'enregistrement contenant le mot de passe. Sur la dernière ligne, entre accolades, se trouve le type d'encodage du mot de passe. Afin de modifier le mot de passe, il faut en générer un nouveau avec le même encodage :

```
slappasswd -h {SSHA}
```

qui vous demandera de taper, puis de retaper un mot de passe. La commande produira un affichage similaire à :

```
{SSHA}nift33xxg0VEgpOP2w8ymC7+rIebSYoB
```


Autrement dit, elle vous affiche le nouveau mot de passe chiffré. Il suffira alors de remplacer dans l'annuaire l'ancien mot de passe par le nouveau. Pour cela, éditez un fichier `ldif`, dans lequel vous écrirez :

```
dn: olcDatabase={1}mdb,cn=config
replace: olcRootPW
olcRootPW: {SSHA}nift33xxg0VEgp0P2w8ymC7+rIebSYoB
```


Ici, la première ligne correspond au *distinguished name* que vous aviez découvert plus haut et, sur la dernière ligne, vous copiez/collez le mot de passe que vous avez généré par `slappasswd`. Enfin, il suffit de demander à l'annuaire de prendre en compte vos modifications :

```
ldapmodify -Y EXTERNAL -H ldapi:/// -f fichier.ldif
```

Redémarrez votre service `slapd` afin que le serveur tienne compte de votre nouveau mot de passe.

Étape 16 – Préparation de l'installation du package `libnss-ldap`

Jusqu'à maintenant, votre système Linux n'utilise pas LDAP pour authentifier vos utilisateurs. Il est temps de changer cela.

 **Créez maintenant un instantané de MSLDAP.**

Ce sont les packages `libnss-ldap` et `libpam-ldap` qui permettent à votre système Linux d'authentifier vos utilisateurs via LDAP. Ces packages ne sont pas installés et il convient donc de le faire maintenant. Il existe plusieurs manières d'installer des packages. La plus simple est d'utiliser la commande `apt-get install`, qui télécharge les packages en question à partir de repositories Debian, puis les installe. Il faut maintenant configurer `apt-get` pour qu'il trouve le repository dont vous avez besoin. Le fichier de configuration s'appelle `/etc/apt/sources.list`. Toute ligne de ce fichier débutant par un `#` est un commentaire.

Sur MSLDAP, les lignes qui nous intéressent sont les suivantes :

```
deb http://ftp.lip6.fr/pub/linux/distributions/debian/ stretch main contrib non-free
deb http://ftp.lip6.fr/pub/linux/distributions/debian/ stretch-backports main contrib non-free
```


Ces lignes indiquent que le serveur ftp du laboratoire d'informatique de Paris 6 (LIP6/UPMC) a un serveur web avec un répertoire `pub/linux/distributions/debian` qui contient un repository d'une distribution Debian stretch. En salle de TME, c'est le serveur du poste n°2 qui contient ce miroir Debian.

Les packages sont répartis en différentes classes, `main`, `contrib`, `non-free` (cf. <https://wiki.debian.org/SourcesList>), et l'on indique ici que l'on souhaite avoir accès à tous ces packages.

Afin de mettre à jour la liste des packages disponibles, tapez la commande `apt-get update`.

Mettez à jour de manière similaire la liste des packages disponibles sur `ssLDAP` et `c1LDAP`.

Étape 17 – Installation du package `libnss-ldap`

 Avant de procéder à cette étape, faites des instantanés de chacune de vos machines.

Sur chacune des machines MSLDAP, `ssLDAP` et `c1LDAP`, tapez la commande `apt-get install libnss-ldap`. Vous devriez observer un affichage similaire à :

```

root@msLDAP:/etc/ldap# apt-get install libnss-ldap
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libpam-ldap nscd
Les NOUVEAUX paquets suivants seront installés :
  libnss-ldap libpam-ldap nscd
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 469 ko dans les archives.
Après cette opération, 926 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n]

```

Tapez la lettre « o » pour continuer. `apt-get` va ainsi télécharger les packages et vous demander, tout d'abord, de configurer `libnss-ldap`. Il vous demandera de renseigner l'adresse du serveur puis le *distinguished name* du haut de votre arborescence LDAP, comme le montrent les figures 2 et 3.

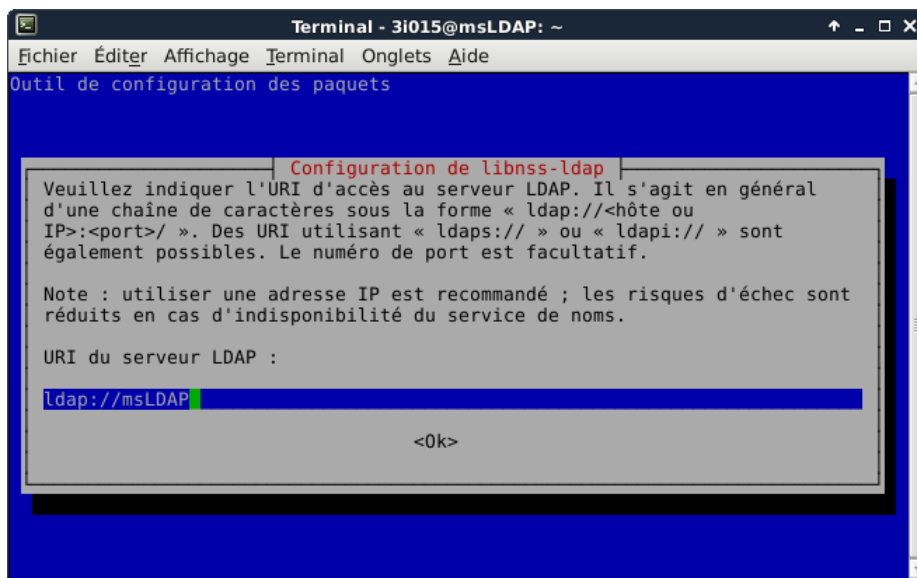


FIGURE 2 – Configuration de `libnss-ldap` : le serveur LDAP

Ensuite, la version de LDAP à utiliser est la dernière, la 3. Enfin, on vous demandera de renseigner le *distinguished name* de l'administrateur du LDAP, comme le montre la figure 4, puis de saisir son mot de passe (`3i015-ldap`).

`apt-get` enchaînera alors avec la configuration du package `libpam-ldap`. Il vous demandera si vous souhaitez donner les privilèges de superutilisateur local au compte administrateur LDAP et la réponse est « oui ». Ensuite, il vous demandera si la base LDAP demande une identification et la réponse est « non ». Enfin, il vous demandera de saisir le *distinguished name* de l'administrateur du LDAP, comme le montre la figure 5, puis de saisir le mot de passe de l'administrateur (`3i015-ldap`).

Il ne vous reste plus qu'à éditer le fichier `/etc/nsswitch.conf` de manière à tenir compte du LDAP :

```

passwd:      files ldap
group:       files ldap
shadow:      files ldap
gshadow:     files ldap

```

Enfin, rebootez votre machine virtuelle.



FIGURE 3 – Configuration de libnss-ldap : haut de l'arborescence

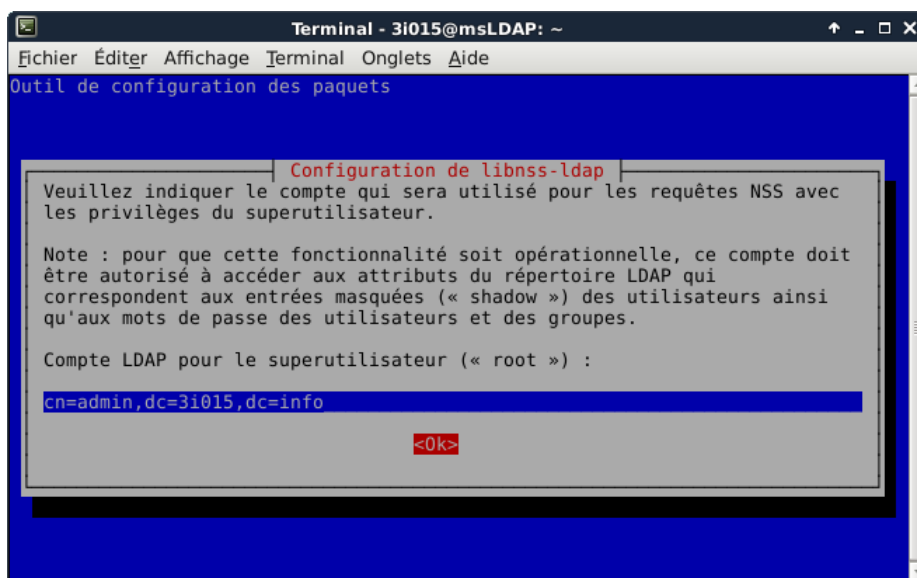


FIGURE 4 – Configuration de libnss-ldap : DN de l'administrateur

Étape 18 – Suppression de nscd

Lorsque vous avez installé `libnss-ldap`, `apt-get` a également installé automatiquement un package appelé `nscd`. Il s'agit d'un démon de cache de noms.

! Il est important de supprimer ce démon car il a tendance à bugger, ce qui a deux conséquences néfastes : i) les montages NFS ont tendance à planter pendant la séquence de boot ; et ii) si vous êtes amenés à effectuer des corrections sur votre serveur LDAP, son cache vous empêchera de voir l'effet de ces modifications. Afin de le supprimer, tapez la commande `apt-get purge nscd`



FIGURE 5 – Configuration de libpam-ldap : DN de l'administrateur

Étape 19 – Test du support LDAP pour PAM et NSS sur msLDAP

Loggez-vous en tant que `student3` sur msLDAP en tapant la commande `su - student3` dans un terminal dans lequel vous êtes `3i015`. Si vous parvenez à vous connecter, cela signifie que votre installation fonctionne bien. Faites de même sur `ssLDAP` et `c1LDAP`.

Afin de vous assurer complètement que tout est correct, sur `msLDAP` et `c1LDAP`, déconnectez-vous et reconnectez-vous en mode graphique en tant que `student3`.

Étape 20 – Mise en place de la réplication sur msLDAP

Afin d'être robuste aux pannes, il est possible de créer des serveurs LDAP « esclaves », c'est-à-dire répliquant les informations contenues dans le serveur LDAP de `msLDAP`. Pour cela, il faut utiliser le mécanisme `syncrepl` de `openLDAP`. Ce mécanisme fonctionne sur un mode *provider-consumer*. `msLDAP` est le *provider* et doit pour cela charger son module `syncprov`. Afin d'effectuer ce chargement, créez sur `msLDAP` un fichier LDIF contenant les informations suivantes :

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulePath: /usr/lib/ldap
olcModuleLoad: syncprov.la
```

et tapez la commande `ldapadd -Y EXTERNAL -H ldapi:/// -f fichier.ldif`, où `fichier.ldif` est le nom du fichier ci-dessus. Cela devrait vous produire un affichage similaire à :

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=module,cn=config"
```

Les paramètres « -Y EXTERNAL -H ldapi:/// » indiquent qu'il faut utiliser un mécanisme d'authentification un peu plus robuste que le simple « -x » que vous avez utilisé jusqu'ici.

Maintenant, il faut indiquer que vous souhaitez que votre annuaire 3i015 soit répliqué. Pour cela, créez un nouveau fichier LDIF sur MSLDAP contenant les lignes suivantes :

```
dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcSyncProvConfig
olcOverlay: syncprov
olcSpSessionLog: 100
```

et tapez la commande `ldapadd -Y EXTERNAL -H ldapi:/// -f fichier.ldif`, où `fichier.ldif` est le nom du fichier que vous venez de créer. Dans la première ligne, « `olcDatabase={1}mdb,cn=config` » désigne le *distinguished name* de la base de la configuration de votre annuaire. Vous pouvez afficher le contenu de cette configuration : il s'agit en effet du fichier texte :

```
/etc/ldap/slapd.d/cn=config/olcDatabase=\{1\}mdb.ldif.
```

La ligne complète « `dn: olcOverlay=syncprov,olcDatabase={1}mdb,cn=config` » correspond au fichier `/etc/ldap/slapd.d/cn=config/olcDatabase=\{1\}mdb/olcOverlay=\{0}syncprov.ldif`.

Voilà, votre serveur LDAP est prêt à être répliqué.

Préparation avant le TME: *Si vous souhaitez en savoir plus sur la réplification LDAP, vous pouvez vous reporter aux URLs suivantes : <http://www.openldap.org/doc/admin24/replication.html> et <http://www.zytrax.com/books/ldap/ch7>.*


Étape 21 – Mise en place de l'esclave sur SSLDAP : phase 1

La première opération à effectuer pour mettre en place un esclave est d'installer un serveur LDAP identique à celui du maître. Il faut donc refaire entièrement l'étape 11 sur SSLDAP. Il est important de renseigner votre nouveau serveur de la même manière : même base (`dc=3i015,dc=info`), même mot de passe de l'administrateur (`3i015-ldap`), etc. Ici, on se contente juste de l'étape 11, inutile de répéter l'étape 12 et les suivantes, qui consistaient à insérer des informations dans le serveur LDAP.

Étape 22 – Mise en place de l'esclave sur ssLDAP : phase 2

Vous devez indiquer à ce nouveau serveur qu'il répliquera MSLDAP. Pour cela, il suffit de créer le fichier LDIF suivant :

```
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcSyncRepl
olcSyncRepl:
  rid=001
  provider=ldap://msLDAP
  bindmethod=simple
  binddn="cn=admin,dc=3i015,dc=info"
  credentials=3i015-ldap
  searchbase="dc=3i015,dc=info"
  scope=sub
  schemachecking=on
  type=refreshAndPersist
  retry="30 5 300 3"
  interval=00:00:05:00
```

 À partir de « rid=001 », le texte doit impérativement être décalé de deux espaces (ce que le copier-coller ne fera malheureusement pas, le langage PDF n'encodant pas de caractère espace).

Les deux premières lignes indiquent que l'on va modifier l'annuaire que vous venez de créer. La troisième indique que vous allez faire de la réplication. Les lignes suivantes sont les paramètres de cette réplication. Notamment, elles précisent quel est le serveur à répliquer ainsi que les paramètres de connexion (`bindmethod`, `binddn`, `credentials`).

Afin de prendre en compte ce fichier, tapez la commande `ldapadd -Y EXTERNAL -H ldapi:/// -f fichier.ldif`, où `fichier.ldif` est le nom du fichier ci-dessus. Le serveur LDAP de ssLDAP est maintenant un « esclave » de celui de MSLDAP.

Étape 23 – Authentification avec maître et/ou esclave

Sur ssLDAP et c1LDAP, éditez le fichier `/etc/ldap/ldap.conf` et faites en sorte d'accéder à vos deux serveurs LDAP. Pour cela, il suffit de rajouter sur la ligne « URI » l'adresse de votre nouveau serveur. Par exemple, vous pourriez avoir quelque chose similaire à :

```
URI ldap://msLDAP ldap://ssLDAP
```

Il faut également indiquer à NSS et PAM d'utiliser votre nouveau serveur. Pour cela, éditez les fichiers `/etc/libnss-ldap.conf` et `/etc/pam_ldap.conf` et rajoutez l'adresse de votre nouveau serveur sur la ligne `uri` :

```
uri ldap://msLDAP ldap://ssLDAP
```

Étape 24 – Test de bon fonctionnement

Arrêtez le service `slapd` sur MSLDAP. Redémarrez `c1LDAP` et loggez-vous en tant que `student3`. Si vous arrivez à vous logguer, cela signifie que vous avez communiqué avec le serveur LDAP de SSLDAP. Sur SSLDAP, faites un `ldapsearch -x uid`. Si celui-ci ne produit pas de message d'erreur, c'est, là encore, que vous communiquez directement avec le serveur LDAP de SSLDAP.