

# Introduction aux annuaires LDAP avec OpenLDAP

Philippe Latu

philippe.latu(at)linux-france.org

<http://www.linux-france.org/prj/inetdoc/>

Historique des versions		
\$Revision: 1637 \$	\$Date: 2011-04-30 15:11:22 +0200 (sam. 30 avril 2011) \$	\$Author: latu \$
Année universitaire 2010-2011		
Résumé		
L'objectif de ce deuxième support de travaux pratiques de la série est l'étude du service d'annuaire LDAP. On présente succinctement les éléments constitutifs d'un annuaire puis on étudie la configuration d'un service d'annuaire basé sur le logiciel OpenLDAP. Ensuite, on étudie la configuration de l'accès aux entrées de l'annuaire depuis un poste client. Les informations délivrées par l'annuaire sont les propriétés de comptes utilisateurs stockées dans la classe d'objet posixAccount.		

## Table des matières

1. Copyright et Licence .....	1
1.1. Méta-information .....	2
1.2. Conventions typographiques .....	2
2. Adressage IP des postes de travail .....	2
3. Principes d'un annuaire LDAP .....	2
4. Configuration du serveur LDAP .....	4
4.1. Installation du serveur LDAP .....	4
4.2. Analyse de la configuration du service LDAP .....	5
4.3. Réinitialisation de la base de l'annuaire LDAP .....	7
4.4. Composition d'un nouvel annuaire LDAP .....	10
4.5. Gestion de l'annuaire avec phpLDAPadmin .....	15
5. Configuration de l'accès client au serveur LDAP .....	18
5.1. Interrogation à distance de l'annuaire LDAP .....	18
5.2. Configuration <i>Name Service Switch</i> .....	19
6. Analyse de la configuration .....	24
6.1. Indexation des entrées de l'annuaire LDAP .....	25
6.2. Analyse réseau des transactions LDAP .....	26
7. Documents de référence .....	27

## 1. Copyright et Licence

Copyright (c) 2000,2011 Philippe Latu.  
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2011 Philippe Latu.  
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.2 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

## 1.1. Méta-information

Cet article est écrit avec *DocBook*<sup>1</sup> XML sur un système *Debian GNU/Linux*<sup>2</sup>. Il est disponible en version imprimable au format PDF : [admin.reseau.ldap.synthese.pdf](#)<sup>3</sup>.

## 1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou *prompt* spécifique au niveau des droits utilisateurs nécessaires sur le système.

- Toute commande précédée de l'invite `$` ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.
- Toute commande précédée de l'invite `#` nécessite les privilèges du super-utilisateur.

## 2. Adressage IP des postes de travail

Tableau 1. Affectation des adresses IP des postes de travaux pratiques

Poste 1	Poste 2	Passerelle par défaut	Organisation
alderaan	bespin	10.7.10.1/23	o: zone1.lan-213.stri
centares	coruscant	192.168.110.129/25	o: zone2.lan-213.stri
dagobah	endor	172.19.113.65/26	o: zone3.lan-213.stri
felucia	geonosis	10.3.2.1/23	o: zone4.lan-213.stri
hoth	mustafar	172.20.130.25/29	o: zone5.lan-213.stri
naboo	tatooine	192.168.111.1/25	o: zone6.lan-213.stri

Toutes les questions de ce support peuvent être traitées avec le document de référence : *OpenLDAP Software 2.4 Administrator's Guide*<sup>4</sup>. Il est cependant nécessaire de faire la correspondance entre les services décrits dans le document et les paquets de la distribution *Debian GNU/Linux*.

Pour chaque paire de postes de travaux pratiques, il faut attribuer les rôles de serveur et de client. Le serveur doit mettre à disposition de son poste client une base de données utilisateurs. L'objectif en fin de séance de travaux pratiques est de pouvoir se connecter sur un poste client avec ses authentifiants `login/password`.

Relativement au précédent support sur l' *Introduction au système de fichiers réseau NFS*<sup>5</sup>, on ne dispose pas d'un système de fichiers réseau. Ici, seule l'authentification est fonctionnelle et il n'est pas possible d'accéder au répertoire utilisateur stocké sur le serveur NFS.

## 3. Principes d'un annuaire LDAP

Dans l'histoire des systèmes Unix, les services de *nommage* ont connu de nombreuses évolutions avec le développement de l'Internet et des volumes d'informations à partager.

Au début des années 80, un premier service baptisé *Network Information Service* (NIS) a vu le jour. Ce service est une méthode de distribution de la base de données des utilisateurs, de fichiers de configuration, d'authentification et d'autres données entre les hôtes d'un réseau local. Le logiciel NIS développé par Sun Microsystems<sup>TM</sup> fonctionne sur le mode Client/Serveur à partir d'une base de données «à plat» (*flat bindery base*). Son utilisation est étudiée dans le support de travaux pratiques *Introduction au service NIS*<sup>6</sup>. Avec un service NIS, il n'est pas possible de constituer des

<sup>1</sup> <http://www.docbook.org>

<sup>2</sup> <http://www.debian.org>

<sup>3</sup> <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.ldap.synthese.pdf>

<sup>4</sup> <http://www.openldap.org/doc/admin24/>

<sup>5</sup> <http://www.linux-france.org/prj/inetdoc/cours/index.html#admin.reseau.nfs>

<sup>6</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.nis/>

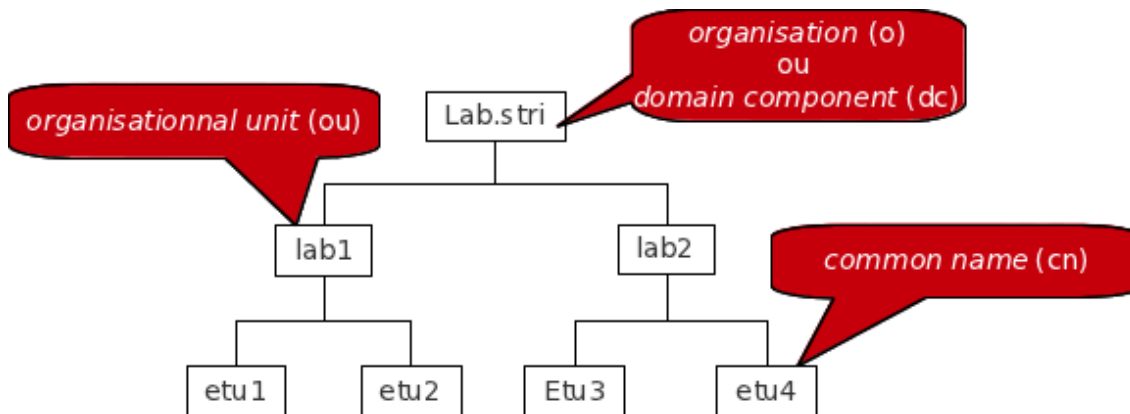
groupes logiques ayant des attributs propres. Cette limitation est rapidement devenue critique avec l'augmentation du nombres des utilisateurs et des clients.

D'autres services plus complets tels que NIS+ ou *kerberos* qui n'assure que la partie authentification ont été développés par la suite. Depuis quelques années, les annuaires LDAP ou *Lightweight Directory Access Protocol* se sont imposés comme étant l'outil d'échange universel des paramètres utilisateurs.

Pour définir ce qu'est le service LDAP, on peut retenir les caractéristiques suivantes.

- Un service de publication d'annuaire
- Un protocole d'accès aux annuaires de type X.500 ou *Lightweight Directory Access Protocol*
- Un dépôt de données basées sur des attributs ou un «genre» de base de données
- Un logiciel optimisé pour les recherches avancées et les lectures
- Une implémentation client/serveur
- Un mécanisme extensible de schémas de description de classes d'objets

Les entrées (*Directory Service Entry*) d'un annuaire LDAP sont distribuées suivant une arborescence (*Directory Information Tree*) hiérarchisée que l'on peut voir comme un système de fichiers avec ses répertoires et ses fichiers. Au sommet de l'arborescence on trouve un nom de racine (*Domain Component*) ou suffixe.



### Arborescence LDAP élémentaire - vue complète<sup>7</sup>

L'adresse d'une entrée de l'annuaire LDAP est appelée : *distinguished name* ou dn. En reprenant l'exemple d'arborescence ci-dessus, les adresses des différentes entrées sont notées comme suit.

- dn: dc=lab,dc=stri
- dn: ou=lab1,dc=lab,dc=stri
- dn: ou=lab2,dc=lab,dc=stri
- dn: cn=etu1,ou=lab1,dc=lab,dc=stri
- dn: cn=etu2,ou=lab1,dc=lab,dc=stri
- dn: cn=etu3,ou=lab1,dc=lab,dc=stri
- dn: cn=etu4,ou=lab1,dc=lab,dc=stri

L'adresse de chaque entrée appartient à une classe d'objet (*ObjectClass*) spécifiée dans un schéma (*schema*). En reprenant les mêmes exemples d'entrées, on peut associer les classes d'objets correspondantes.

<i>entry</i>	<i>objectclass</i>
o: lab.stri	organisation

<sup>7</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap/images/ldap-tree.png>

<i>entry</i>	<i>objectclass</i>
dc: lab	dcObject
dc: stri	dcObject
ou: lab1	organizationalUnit
cn: etul	person
sn: etul	

Un schéma peut être vu comme un ensemble de règles qui décrivent la nature des données stockées. C'est un outil qui aide à maintenir la cohérence, la qualité et qui évite la duplication des données dans l'annuaire. Les attributs des classes d'objets déterminent les règles qui doivent être appliquées à une entrée. Un schéma contient les éléments suivants.

- Les attributs requis
- Les attributs autorisés
- Les règles de comparaison des attributs
- Les valeurs limites qu'un attribut peut recevoir
- Les restrictions sur les informations qui peuvent être enregistrées

## 4. Configuration du serveur LDAP

Avant d'aborder la configuration du service LDAP, il faut passer par les étapes rituelles de sélection et d'installation des paquets contenant les outils logiciels du service. Ensuite, il faut identifier les processus, les numéros de ports ouverts et les fichiers de configuration à éditer.

### 4.1. Installation du serveur LDAP

#### 1. Quels sont les paquets Debian relatifs au service LDAP ?

Interroger la base de données des paquets pour obtenir les informations demandées.

Dans la requête ci-dessous, on privilégie la recherche dans les champs de description des paquets.

```
# aptitude search "?description(OpenLDAP) "
p  bdi4 - information index based on OpenLDAP
p  ldap-utils - OpenLDAP utilities
p  ldapscripts - Add and remove user and groups (stored in a LDAP directory)
p  libdbd-ldap-perl - Perl extension for LDAP access via an SQL/Perl DBI interface
i  libldap-2.4-2 - OpenLDAP libraries
p  libldap-2.4-2-dbg - Debugging information for OpenLDAP libraries
p  libldap-ruby1.8 - OpenLDAP library binding for Ruby 1.8
p  libldap2-dev - OpenLDAP development libraries
p  libnet-ldapapi-perl - Perl bindings for OpenLDAP C API
p  libsasl2-modules-ldap - Cyrus SASL - pluggable authentication modules (LDAP)
p  python-ldap - LDAP interface module for Python
p  python-ldap-dbg - LDAP interface module for Python (debug extension)
p  python-ldap-doc - Documentation for the Python LDAP interface module
p  slapd - OpenLDAP server (slapd)
p  slapd-dbg - Debugging information for the OpenLDAP server (slapd)
p  smbldap-tools - Scripts to manage Unix and Samba accounts stored on LDAP
```

#### 2. Quels sont les paquets Debian à installer pour mettre en œuvre un serveur LDAP ?

Dans la liste ci-dessus, on retient deux paquets : ldap-utils et slapd.

```
# aptitude install slapd ldap-utils
Les NOUVEAUX paquets suivants vont être installés :
  ldap-utils libltdl7{a} libperl5.10{a} libslp1{a} odbcinst{a} odbcinst1debian2{a} slapd unixodbc{a}
0 paquets mis à jour, 8 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 2 715 ko d'archives. Après dépaquetage, 6 500 ko seront utilisés.
Voulez-vous continuer ? [Y/n/?]
```

Lors de l'installation, deux écrans `debconf` demandent la saisie du mot de passe administrateur du service LDAP.

### 3. Comment identifier le ou les processus correspondant au service installé ?

Utiliser une commande d'affichage de la liste des processus actifs sur le système pour identifier le démon correspondant au serveur LDAP.

```
# ps aux | grep l[d]ap
openldap 2842 0.0 0.6 99860 3484 ?        Ssl 15:26  0:00 \
/usr/sbin/slapd -h ldap:/// ldapi:/// -g openldap -u openldap -F /etc/ldap/slapd.d
```

À partir de ces informations, on identifie le démon serveur `slapd`, le compte utilisateur et le groupe système propriétaires du processus (`openldap`) et enfin le répertoire contenant les fichiers de configuration `/etc/ldap/slapd.d`.

### 4. Comment identifier le ou les numéros de ports ouverts par le service installé ?

Utiliser une commande d'affichage de la liste des ports ouverts sur le système.

Voici deux exemples usuels.

```
# lsof -i | grep l[d]ap
slapd 2842 openldap 9u IPv4 5732 0t0 TCP *:ldap (LISTEN)
slapd 2842 openldap 10u IPv6 5733 0t0 TCP *:ldap (LISTEN)
```

```
# netstat -autp | grep l[d]ap
tcp 0 0 *:ldap ** LISTEN 2842/slapd
tcp6 0 0 [::]:ldap [::]:* LISTEN 2842/slapd
```

Les numéros de port enregistrés pour le service LDAP sont disponibles dans le fichier `/etc/services`.

```
# grep ldap /etc/services
ldap 389/tcp # Lightweight Directory Access Protocol
ldap 389/udp
ldaps 636/tcp # LDAP over SSL
ldaps 636/udp
```

Relativement aux indications données par les commandes `lsof` et `netstat`, c'est le numéro de port 389 qui est ouvert en écoute lors de l'installation du paquet `slapd`.

## 4.2. Analyse de la configuration du service LDAP

Les versions récentes du logiciel *OpenLDAP* utilisent un mode de configuration basé sur un *Directory Information Tree* ou DIT propre. Cette arborescence de configuration est pointée par le nom `cn=config`. Elle est utilisée pour configurer dynamiquement le démon `slapd`, modifier les définitions de schéma, les index, les listes de contrôle d'accès ACLs, etc. Ce mode de configuration présente un avantage déterminant lorsque l'on exploite des annuaires volumineux : toutes les opérations se font sans interruption de service.

Les documents fournis avec le paquet `slapd` contiennent des informations indispensables à l'analyse du fonctionnement du service.

#### 1. Quel est le mode de gestion de la configuration du service adopté depuis la version 2.4.23-3 du paquet de la distribution Debian GNU/Linux ?

Les documents relatifs au paquet `slapd` sont situés dans le répertoire `/usr/share/doc/slapd/`. Le fichier `README.Debian.gz` contient un exemple d'instruction de consultation de la configuration du service.

```
# ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config"
```

#### 2. Quel est le gestionnaire de base de données (*backend*) proposé dans le fichier de configuration ?

```
# ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config" olcDatabase={1}hdb
SASL/EXTERNAL authentication started
```

```

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
# extended LDIF
#
# LDAPv3
# base <cn=config> with scope subtree
# filter: olcDatabase={1}hdb
# requesting: ALL
#
# {1}hdb, config
dn: olcDatabase={1}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=nodomain
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymous
s auth by dn="cn=admin,dc=nodomain" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by dn="cn=admin,dc=nodomain" write by * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=nodomain
olcRootPW: {SSHA}SxVaLp7BlsaZlVDalwBNdWpt+r3vvg4f
olcDbCheckpoint: 512 30
olcDbConfig: {0}set_cachesize 0 2097152 0
olcDbConfig: {1}set_lk_max_objects 1500
olcDbConfig: {2}set_lk_max_locks 1500
olcDbConfig: {3}set_lk_max_lockers 1500
olcDbIndex: objectClass eq

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

```

Par définition, un annuaire LDAP est une base de données optimisée en lecture. Du point de vue implémentation, les entrées sont stockées sous forme « binaire » et indexées à l'aide d'un gestionnaire de base de données. Le gestionnaire d'arrière plan proposé par défaut est `hdb`. Il s'agit d'une variante du gestionnaire *Berkeley DB transactional backend* qui offre un fonctionnement hiérarchisé.

### 3. Comment identifier le nom de l'annuaire fourni par défaut avec le paquet `slapd` ?

```

# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=config" olcSuffix | grep ^olcSuffix
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
olcSuffix: dc=nodomain

```

### 4. Quels sont les *schemas* actifs avec la configuration courante du paquet `slapd` ?

```

# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=config" olcSchemaConfig | grep ^cn
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
cn: config
cn: module{0}
cn: schema
cn: {0}core
cn: {1}cosine
cn: {2}nis
cn: {3}inetorgperson

```

### 5. Où sont stockées les bases définies par défaut lors de l'installation du paquet `slapd` ?

```

# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=config" olcDbDirectory | grep ^olcDbDirectory

```

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
olcDbDirectory: /var/lib/ldap
```

C'est dans le répertoire `/var/lib/ldap` que sont stockées les fichiers des bases *Berkeley DB*.

```
# ls -lAh /var/lib/ldap/
total 1,6M
-rw-r--r-- 1 openldap openldap 2,0K 21 avril 15:26 alock
-rw----- 1 openldap openldap 24K 21 avril 15:26 __db.001
-rw----- 1 openldap openldap 360K 21 avril 16:26 __db.002
-rw----- 1 openldap openldap 2,6M 21 avril 15:26 __db.003
-rw----- 1 openldap openldap 160K 21 avril 15:56 __db.004
-rw----- 1 openldap openldap 1,3M 21 avril 15:26 __db.005
-rw----- 1 openldap openldap 32K 21 avril 15:56 __db.006
-rw-r--r-- 1 openldap openldap 96 21 avril 15:25 DB_CONFIG
-rw----- 1 openldap openldap 8,0K 21 avril 15:26 dn2id.bdb
-rw----- 1 openldap openldap 32K 21 avril 15:26 id2entry.bdb
-rw----- 1 openldap openldap 10M 21 avril 15:56 log.0000000001
-rw----- 1 openldap openldap 8,0K 21 avril 15:26 objectClass.bdb
```

### 4.3. Réinitialisation de la base de l'annuaire LDAP

L'installation du paquet `slapd` implique l'installation d'un annuaire minimal avec une base associée. Ce mode opératoire est nécessaire, ne serait-ce que pour accéder à la configuration du service et tester la validité de l'installation. Après avoir traité les questions ci-dessus, on sait que l'installation est fonctionnelle. On peut donc passer à l'initialisation de notre propre annuaire.



#### Note

Les manipulations proposées dans cette section permettent de reprendre à zéro la configuration d'un annuaire LDAP. Il peut être utile de revenir à cette étape en cas de «doute» sur l'intégrité de l'annuaire lors du traitement des questions des sections suivantes.

#### 1. Comment arrêter le service LDAP ?

Utiliser les scripts fournis avec le gestionnaire de lancement des processus système (*run-levels*).

Chaque processus système dispose d'un script de gestion de son lancement, arrêt (et/ou) redémarrage. Ce script apparaît dans la liste des fichiers du paquet.

```
# dpkg -L slapd | grep init.d
/etc/init.d
/etc/init.d/slapd
```

Il suffit de faire appel à la directive `stop` de ce script pour arrêter «proprement» le service d'annuaire LDAP.

```
# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
```

#### 2. Quels sont les éléments à effacer pour pouvoir installer une nouvelle configuration et une nouvelle base LDAP ?

Utiliser le résultat de la question sur la [localisation des bases](#) et la documentation fournie avec le paquet `slapd`.

À partir des réponses aux questions ci-dessus, on sait que c'est le répertoire `/var/lib/ldap/` qui contient les bases. La lecture du fichier de documentation du paquet avec la commande `# zless /usr/share/doc/slapd/README.Debian.gz` indique que les fichiers de configuration sont situés dans le répertoire `/etc/ldap/slapd.d/`.

On efface donc tous ces fichiers et répertoires.

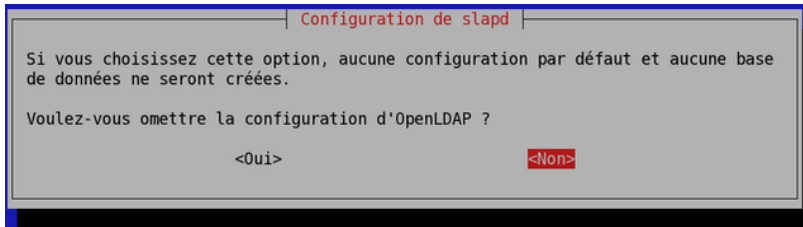
```
# rm /var/lib/ldap/*
# rm -rf /etc/ldap/slapd.d
```

#### 3. Comment reprendre à zéro la configuration du paquet `slapd` ?

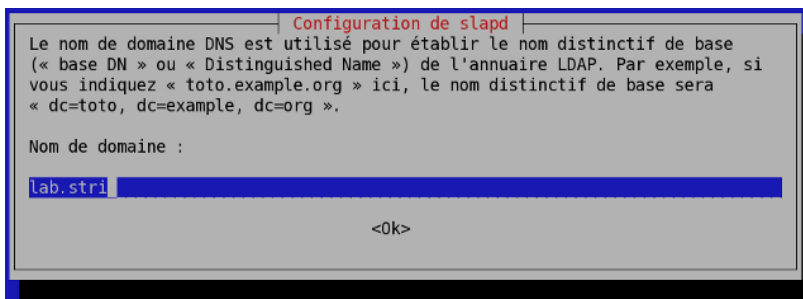
Utiliser l'outil du gestionnaire de paquets *Debian GNU/Linux* qui permet la modification des paramètres de configuration d'un service à l'aide de menus `debconf`.

C'est la commande **dpkg-reconfigure** qui sert à réviser les paramètres de configuration d'un paquet. Voici une copie des écrans proposés avec le paquet `slapd`.

```
# dpkg-reconfigure slapd
No configuration file was found for slapd at /etc/ldap/slapd.conf. ... (warning).
  Creating initial configuration... done.
  Creating LDAP directory... done.
Starting OpenLDAP: slapd.
```



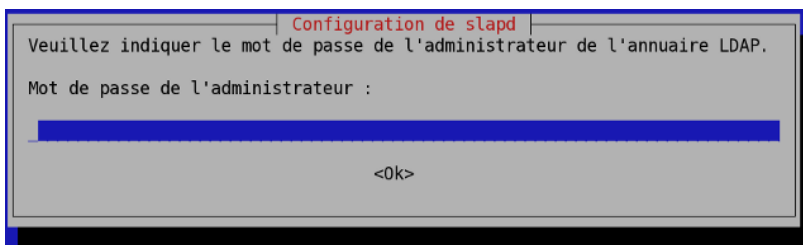
Copie d'écran `dpkg-reconfigure slapd` - vue complète<sup>8</sup>



Copie d'écran `dpkg-reconfigure slapd` - vue complète<sup>9</sup>



Copie d'écran `dpkg-reconfigure slapd` - vue complète<sup>10</sup>



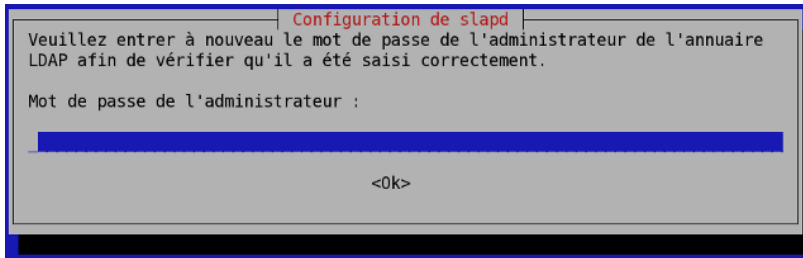
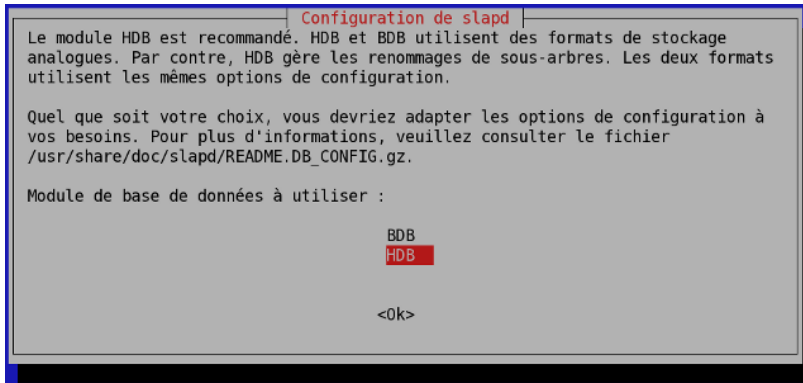
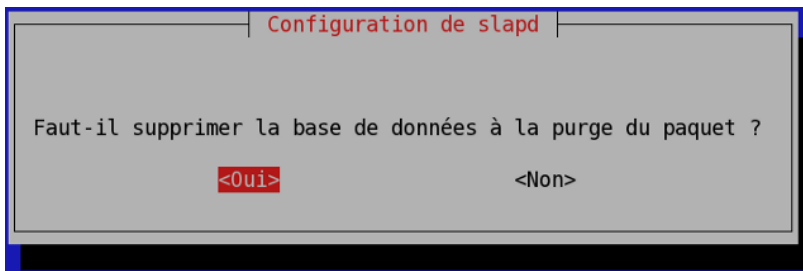
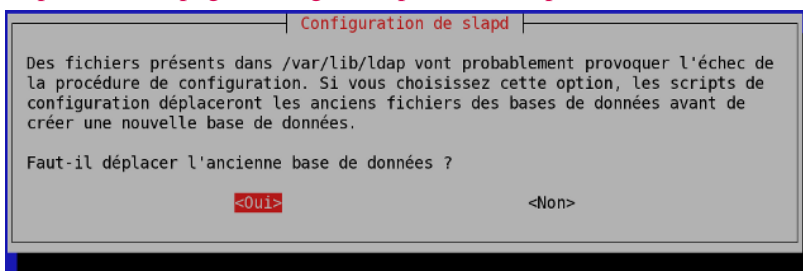
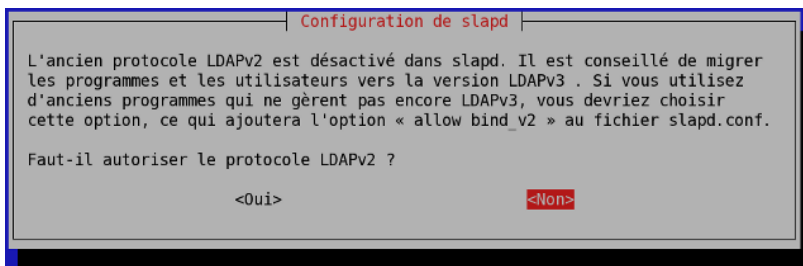
Copie d'écran `dpkg-reconfigure slapd` - vue complète<sup>11</sup>

<sup>8</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-1.png>

<sup>9</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-2.png>

<sup>10</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-3.png>

<sup>11</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-4.png>

Copie d'écran dpkg-reconfigure slapd - vue complète<sup>12</sup>Copie d'écran dpkg-reconfigure slapd - vue complète<sup>13</sup>Copie d'écran dpkg-reconfigure slapd - vue complète<sup>14</sup>Copie d'écran dpkg-reconfigure slapd - vue complète<sup>15</sup><sup>12</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-5.png><sup>13</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-6.png><sup>14</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-7.png><sup>15</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-8.png>

Copie d'écran dpkg-reconfigure slapd - vue complète<sup>16</sup>

## 4. Comment valider la nouvelle configuration du paquet slapd ?

Reprendre la question sur le **nom distinctif** de l'annuaire.

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=config" olcSuffix | grep ^olcSuffix
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
olcSuffix: dc=lab,dc=stri
```

## 4.4. Composition d'un nouvel annuaire LDAP

Une fois que les fichiers de configuration et de base de données du nouvel annuaire sont en place, on peut passer à l'ajout de nouvelles entrées dans cet annuaire. Comme le fil conducteur de cette série de travaux pratiques est la gestion d'une base de comptes utilisateurs, on doit ajouter les objets suivants.

- Deux unités organisationnelles : `people` et `groups`.
- Quatre compte utilisateurs : `papa` et `maman Skywalker` ainsi que leurs deux enfants

Toutes les manipulations sur les objets de l'annuaire utilisent un format de fichier texte particulier baptisé LDIF pour *LDAP Data Interchange Format*. C'est un format de représentation des données contenues dans un annuaire particulièrement utile pour les opérations de sauvegarde et de restauration en volume.

Du point de vue formatage, chaque enregistrement doit être séparé du suivant par une ligne vide et chaque attribut d'un enregistrement apparaît sur une ligne sous la forme «`nomAttribut: valeur`».

## 1. Comment visualiser la liste des entrées contenues dans l'annuaire LDAP ?

Utiliser les pages de manuels de la commande **ldapsearch** et rechercher les informations sur les méthodes d'authentification, la désignation de la base dans laquelle on effectue la recherche et le nom distinctif utilisé pour se connecter à l'annuaire.

La commande **ldapsearch** propose plusieurs modes d'authentification qui influent sur la liste des attributs affichés pour une même entrée. Dans notre exemple, ce sont les mots de passes qui peuvent ne pas apparaître ou apparaître sous différentes formes.

- L'option `-x` évite le recours à la méthode SASL pour l'authentification.

```
# ldapsearch -LLL -x -H ldap:/// -b "dc=lab,dc=stri" -D cn=admin,dc=lab,dc=stri -W
Enter LDAP Password:
dn: dc=lab,dc=stri
objectClass: top
objectClass: dcObject
objectClass: organization
o: lab.stri
dc: lab

dn: cn=admin,dc=lab,dc=stri
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9Q3RtbURZbGkwUmxla2VyVUVqbHZPWfhjQ0kreXdXRWM=
```

- L'option `-Y EXTERNAL` utilise la méthode SASL du même nom.

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "dc=lab,dc=stri" -D cn=admin,dc=lab,dc=stri -W
Enter LDAP Password:
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
```

<sup>16</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/dpkg-reconfigure-slapd-9.png>

```
dn: dc=lab,dc=stri
objectClass: top
objectClass: dcObject
objectClass: organization
o: lab.stri
dc: lab

dn: cn=admin,dc=lab,dc=stri
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
```

- L'option `-LLL` désactive l'affichage des commentaires et de la version LDIF utilisée dans la réponse.
- L'option `-b` désigne le point de départ de la recherche.
- L'option `-D` désigne le nom distinctif de connexion à l'annuaire.
- L'option `-w` provoque l'affichage de l'invite de demande du mot passe correspondant au nom distinctif utilisé.

## 2. Comment activer la journalisation des manipulations sur les entrées de l'annuaire LDAP ?

Rechercher l'entrée relative au niveau de journalisation dans le DIT et modifier sa valeur de façon à obtenir un état dans les journaux système à chaque opération sur l'annuaire.

La modification de l'entrée du DIT doit se faire à l'aide d'un fichier LDIF approprié.

L'entrée à rechercher dans le DIT est baptisée `olcLogLevel`.

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=config" olcLogLevel | grep ^olcLogLevel
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
olcLogLevel: none
```

on se propose de modifier la valeur `none` par `stats` de façon à journaliser les connexions, les opérations et les résultats. Voici une copie du fichier LDIF permettant de réaliser cette modification.

```
# cat set_olcLogLevel_2_stats.ldif
# Set olcLogLevel 2 stats
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
```

On applique ce changement de valeur avec la commande **ldapmodify** puis on vérifie que l'attribut a bien reçu le paramètre.

```
# ldapmodify -Y EXTERNAL -H ldapi:/// -f Set_olcLogLevel2stats.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b "cn=config" olcLogLevel | grep ^olcLogLevel
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
olcLogLevel: stats
```

Enfin, on relève les traces de la dernière opération dans les journaux système.

```
# tail -100 /var/log/syslog | grep slapd
slapd[2222]: conn=1060 fd=17 ACCEPT from PATH=/var/run/slapd/ldapi
(PATH=/var/run/slapd/ldapi)
slapd[2222]: conn=1060 op=0 BIND dn="" method=163
slapd[2222]: conn=1060 op=0 BIND
authcid="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
authzid="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth"
slapd[2222]: conn=1060 op=0 BIND
```

```
dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" mech=EXTERNAL
sasl_ssf=0 ssf=71
slapd[2222]: conn=1060 op=0 RESULT tag=97 err=0 text=
slapd[2222]: conn=1060 op=1 SRCH base="cn=config" scope=2 deref=0
filter="(objectClass=*)"
slapd[2222]: conn=1060 op=1 SRCH attr=olcLogLevel
slapd[2222]: conn=1060 op=1 SEARCH RESULT tag=101 err=0 nentries=11 text=
slapd[2222]: conn=1060 op=2 UNBIND
slapd[2222]: conn=1060 fd=17 closed
```



### Note

Dans le contexte des travaux pratiques, le nombre d'entrées de l'annuaire reste très limité et la journalisation n'a pas d'impact mesurable sur les performances du système. Dans un contexte d'exploitation réelle avec un annuaire comprenant au moins une dizaine de milliers d'entrées, la situation est très différente et il faut limiter au maximum le recours à la journalisation des transactions sur l'annuaire.

Pour ramener la valeur de l'attribut `olcLogLevel` à `none`, il suffit de créer un fichier LDIF avec la directive correspondante.

```
# Set olcLogLevel 2 none
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: none
```

3. Quelle est la syntaxe du fichier LDIF qui permet d'ajouter les deux unités organisationnelles (*organisational unit*) ?

Rechercher un tutoriel LDIF en ligne donnant un exemple de fichier LDIF avec une ou plusieurs entrées `ou:`.

Voici un exemple de fichier LDIF contenant les déclarations des deux unités organisationnelles à ajouter.

```
# cat ou.ldif
dn: ou=people,dc=lab,dc=stri
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=lab,dc=stri
objectClass: organizationalUnit
ou: groups
```

4. Quelle est la commande à utiliser pour ajouter une ou plusieurs entrées dans l'annuaire ?

Rechercher dans la liste des programmes fournis avec le paquet des outils LDAP.

C'est la commande **ldapadd** qui est utile dans notre contexte. On l'utilise en mode d'authentification simple avec le fichier LDIF ci-dessus pour compléter l'annuaire.

```
# ldapadd -cxWD cn=admin,dc=lab,dc=stri -f ou.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=lab,dc=stri"

adding new entry "ou=groups,dc=lab,dc=stri"
```

On vérifie ensuite que les deux nouvelles entrées sont bien présentes dans l'annuaire.

```
# ldapsearch -LLL -x -H ldap:/// -b "dc=lab,dc=stri" -D cn=admin,dc=lab,dc=stri -W
Enter LDAP Password:
dn: dc=lab,dc=stri
objectClass: top
objectClass: dcObject
objectClass: organization
o: lab.stri
dc: lab
```

```
dn: cn=admin,dc=lab,dc=stri
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9Q3RtbURZbGkwUmxla2VyVUVqbHZPWfhjQ0kreXdXRWM=

dn: ou=people,dc=lab,dc=stri
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=lab,dc=stri
objectClass: organizationalUnit
ou: groups
```

5. Quelle est la commande à utiliser pour saisir manuellement un mot de passe et obtenir la chaîne chiffrée correspondante ?

Rechercher dans la liste des programmes fournis avec les paquets de la distribution puis consulter les pages de manuels correspondantes.

En effectuant une recherche par mot clé dans les pages de manuels du système, on peut identifier l'outil recherché.

```
# man -k passwd | grep -i ldap
ldappasswd (1)      - change the password of an LDAP entry
slappasswd (8)     - OpenLDAP password utility
```

On utilise la commande **slappasswd** pour générer une chaîne chiffrée que l'on insère dans le fichier LDIF des comptes utilisateurs.

```
# slappasswd
New password:
Re-enter new password:
{SSHA}u0GZP0rRld9b8rx06a4H13Zt4MJLi41V
```

Dans le contexte de ces travaux pratiques, on attribue le même mot de passe aux quatre comptes utilisateurs.



#### Note

Il existe une technique simple pour la génération de mots de passe utilisateurs aléatoires. Une fois le mot de passe généré, il peut être transmis à l'utilisateur final par un «canal de confiance» et implanté dans les attributs de l'annuaire relatifs au compte utilisateur.

```
# head -c 6 /dev/urandom | base64
CcOuap1v
# slappasswd -v -h "{SSHA}" -s CcOuap1v
{SSHA}wkQGS1CXDWIU78DGdgalYv6wcmEo+jrD
```

6. Quelle est la syntaxe du fichier LDIF qui permet d'ajouter les quatre utilisateurs avec leurs attributs système : identifiants uid/gid, authentifiants login/passwd, etc ?

Rechercher un tutoriel LDIF en ligne donnant un exemple de fichier LDIF avec un exemple de description des attributs d'un compte utilisateur.

Voici un exemple de fichier LDIF contenant les déclarations des quatre comptes utilisateurs à ajouter.

```
# cat users.ldif
# Padmé Amidala
dn: uid=padme,ou=people,dc=lab,dc=stri
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
cn: Padme
sn: Padmé Amidala Skywalker
uid: padme
uidNumber: 10000
```

```

gidNumber: 10000
loginShell: /bin/bash
homeDirectory: /ahome/padme
userPassword: {SSHA}u0GZP0rRld9b8rxO6a4Hl3Zt4MJLi4lV
gecos: Padme Amidala Skywalker

# Anakin Skywalker
dn: uid=anakin,ou=people,dc=lab,dc=stri
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
cn: Anakin
sn: Anakin Skywalker
uid: anakin
uidNumber: 10001
gidNumber: 10001
loginShell: /bin/bash
homeDirectory: /ahome/anakin
userPassword: {SSHA}u0GZP0rRld9b8rxO6a4Hl3Zt4MJLi4lV
gecos: Anakin Skywalker

# Leia Organa
dn: uid=leia,ou=people,dc=lab,dc=stri
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
cn: Leia
sn: Leia Organa
uid: leia
uidNumber: 10002
gidNumber: 10002
loginShell: /bin/bash
homeDirectory: /ahome/leia
userPassword: {SSHA}u0GZP0rRld9b8rxO6a4Hl3Zt4MJLi4lV
gecos: Leia Organa

# Luke Skywalker
dn: uid=luke,ou=people,dc=lab,dc=stri
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
cn: Luke
sn: Luke Skywalker
uid: luke
uidNumber: 10003
gidNumber: 10003
loginShell: /bin/bash
homeDirectory: /ahome/luke
userPassword: {SSHA}u0GZP0rRld9b8rxO6a4Hl3Zt4MJLi4lV
gecos: Luke Skywalker

```

Comme dans le cas précédent, on utilise la commande **ldapadd** en mode d'authentification simple pour insérer les comptes dans l'annuaire.

```

# ldapadd -cxWD cn=admin,dc=lab,dc=stri -f users.ldif
Enter LDAP Password:
adding new entry "uid=padme,ou=people,dc=lab,dc=stri"

adding new entry "uid=anakin,ou=people,dc=lab,dc=stri"

adding new entry "uid=leia,ou=people,dc=lab,dc=stri"

adding new entry "uid=luke,ou=people,dc=lab,dc=stri"

```

Le résultat de la commande **# ldapsearch -LLL -x -H ldap:/// -b "dc=lab,dc=stri" -D cn=admin,dc=lab,dc=stri -w** doit faire apparaître les nouvelles entrées de l'annuaire.

## 4.5. Gestion de l'annuaire avec phpLDAPAdmin

Après avoir vu quelques manipulations à base de fichiers LDIF dans la section précédente, on se propose maintenant d'introduire un outil de gestion d'annuaire avec une interface de type service Internet. Le client Web *phpLDAPAdmin* est représentatif de cette catégorie d'outil. Il ne peut pas se substituer aux fichiers LDIF pour les traitements en volume, mais il peut très bien servir de console d'analyse et de support.

Dans cette section, on commence par installer l'outil avec le serveur Web *apache2* et on configure un accès sécurisé SSL. On ajoute un groupe d'utilisateurs baptisé *StarWars* dans l'unité organisationnelle *groups* et on visualise le schéma d'une entrée du type *posixAccount*.

### 1. Quel est le paquet à installer pour mettre en place le client Web *phpLDAPAdmin* ?

Rechercher le nom `phpldapadmin` dans la liste des paquets de la distribution et installer ce paquet.

Le résultat de la recherche est immédiat puisque le paquet du même nom que celui de l'outil existe. On passe donc directement à l'installation.

```
# aptitude install phpldapadmin
Les NOUVEAUX paquets suivants vont être installés :
  apache2{a} apache2-mpm-prefork{ab} apache2-mpm-worker{ab} apache2-utils{a}
  apache2.2-bin{a} apache2.2-common{a} libapache2-mod-php5{a} libapr1{a}
  libaprutil1{a} libaprutil1-dbd-sqlite3{a} libaprutil1-ldap{a} libonig2{a}
  libqdbm14{a} php5-cli{a} php5-common{a} php5-ldap{a} php5-suhosin{a}
  phpldapadmin ssl-cert{a}
0 paquets mis à jour, 19 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 10,4 Mo d'archives. Après dépaquetage, 32,2 Mo seront utilisés.
Les paquets suivants ont des dépendances non satisfaites :
  apache2-mpm-worker: Est en conflit avec: apache2-mpm qui est un paquet virtuel
  apache2-mpm-prefork: Est en conflit avec: apache2-mpm qui est un paquet virtuel
Internal error: found 2 (choice -> promotion) mappings for a single choice.
Les actions suivantes permettront de résoudre ces dépendances :

Conserver les paquets suivants dans leur version actuelle :
 1)      apache2-mpm-worker [Non installé]

Accepter cette solution ? [Y/n/q/?]
```



### Note

Alors que dans un contexte d'exploitation réelle, les réglages sur le nombre d'instances de serveurs et sur les quantités de mémoire allouées au fonctionnement des scripts PHP peuvent s'avérer « délicats », dans un contexte de travaux pratiques on peut se contenter de réduire l'occupation mémoire en limitant le nombre des instances du serveur *apache2*.

```
# sed -n '/<IfModule mpm_prefork_module>/,/</IfModule>/p' /etc/apache2/apache2.conf
<IfModule mpm_prefork_module>
    StartServers      2
    MinSpareServers   2
    MaxSpareServers   5
    MaxClients        50
    MaxRequestsPerChild 0
</IfModule>
```

### 2. Comment activer l'accès SSL au service Web ?

Consulter les fichiers de documentation fournis avec le paquet *apache2* et repérer les instructions d'activation du service SSL.

L'activation du module `ssl` informe directement sur le fichier à consulter. On le visualise avec la commande

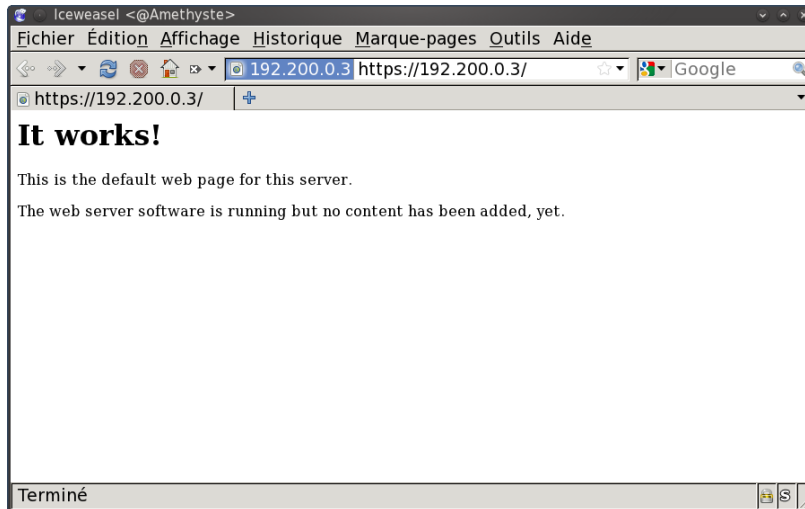
```
# zless /usr/share/doc/apache2.2-common/README.Debian.gz.
```

```
# a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL
```

```
and create self-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!

# a2ensite default-ssl
Enabling site default-ssl.
Run '/etc/init.d/apache2 reload' to activate new configuration!
```

Après avoir accepté l'exception de sécurité relative à l'utilisation d'un certificat auto signé, on accède à une page du type suivant.



### Copie d'écran accès Web SSL - vue complète<sup>17</sup>

3. Quel est le fichier de configuration du paquet `phpldapadmin` qui contient la définition du contexte de nommage (suffixe) ?

Rechercher le répertoire contenant les fichiers de configuration du paquet. Repérer le fichier contenant la définition du suffixe de l'annuaire.

Le répertoire qui contient les éléments de configuration du paquet est nécessairement baptisé `/etc/phpldapadmin`. On recherche ensuite le fichier contenant la définition de l'entrée `dc=`.

```
# grep 'dc=' /etc/phpldapadmin/*
/etc/phpldapadmin/config.php:$servers->setValue('server','base',array('dc=example,dc=com'));
/etc/phpldapadmin/config.php:$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');
/etc/phpldapadmin/config.php:# $servers->setValue('login','bind_id','cn=Manager,dc=example,dc=com');
/etc/phpldapadmin/config.php:# $servers->setValue('auto_number','search_base','ou=People,dc=example,dc=com');
/etc/phpldapadmin/config.php:# 'uid=stran,ou=People,dc=example,dc=com',
/etc/phpldapadmin/config.php:# 'cn=callcenter,ou=Group,dc=example,dc=com');
```

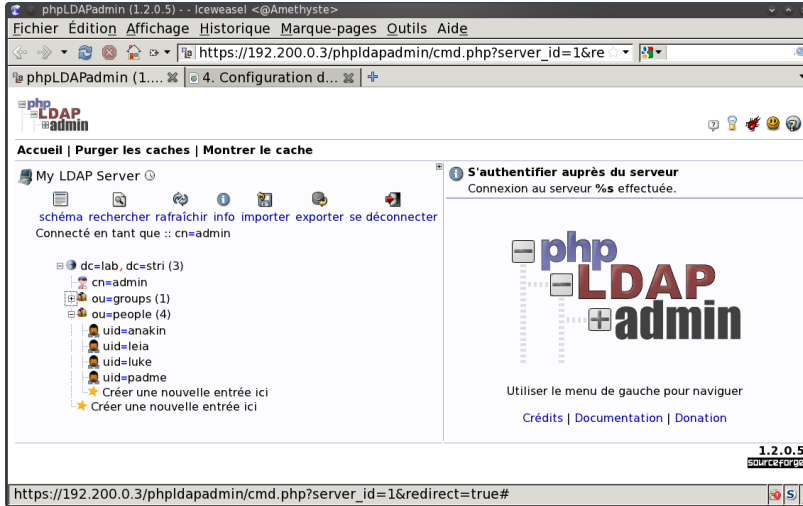
4. Quelles modifications apporter à ce fichier de configuration pour utiliser le suffixe de travaux pratiques ?

Rechercher les options de la commande `sed` qui permettent de substituer `dc=example,dc=com` dans le fichier de configuration du paquet `phpldapadmin`.

```
# sed -i 's/dc=example,dc=com/dc=lab,dc=stri/g' /etc/phpldapadmin/config.php
# /etc/init.d/apache2 reload
```

Une fois le service Web redémarré, on peut se connecter à l'annuaire avec le bon suffixe et visualiser les entrées de l'annuaire.

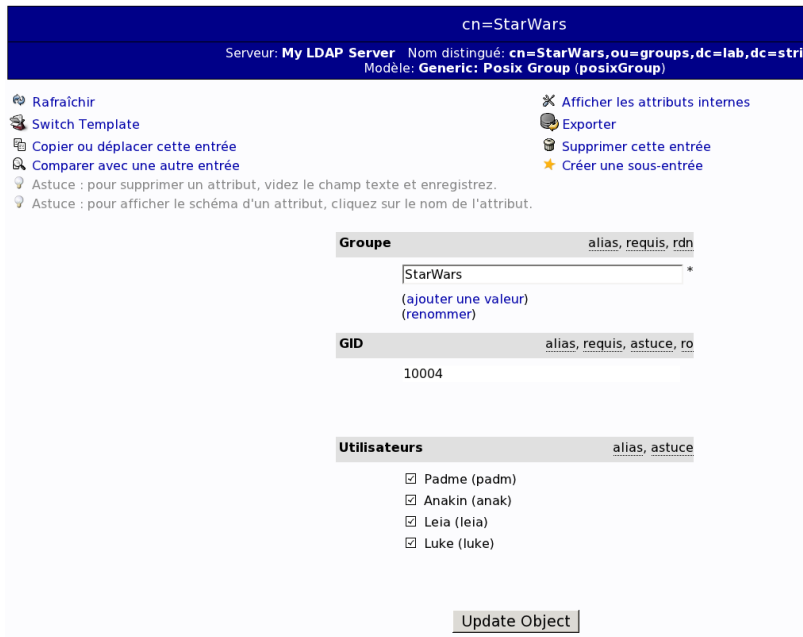
<sup>17</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/phpldapadmin-0.png>



Copie d'écran suffixe et entrées - vue complète<sup>18</sup>

5. Comment ajouter un groupe `StarWars` dans l'unité organisationnelle `groups` ?

On sélectionne l'unité organisationnelle `groups` et suit le lien `Créer une sous-entrée` pour ajouter le groupe supplémentaire.



Copie d'écran ajout d'un groupe - vue complète<sup>19</sup>

6. Comment visualiser les attributs d'une entrée de type `posixAccount` ?

On sélectionne la catégorie schéma puis `Sauter vers un objectClass:` avec l'option `posixAccount`.

<sup>18</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/phpldapadmin-1.png>

<sup>19</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/phpldapadmin-2.png>

Schema pour le serveur My LDAP Server	
ObjectClass   Types d'attributs   Syntaxes   Règles correspondantes	
Sauter vers un objectClass:	
posixAccount	Aller à
<b>posixAccount</b>	
OID: 1.3.6.1.1.1.2.0	
Description: Abstraction of an account with POSIX attributes	
Type: auxiliary	
Hérite de: top	
Parent de: (aucun)	
Attributs requis	Attributs optionnels
<ul style="list-style-type: none"> <li>• cn</li> <li>• gidNumber</li> <li>• homeDirectory</li> <li>• uid</li> <li>• uidNumber</li> </ul>	<ul style="list-style-type: none"> <li>• description</li> <li>• gecos</li> <li>• loginShell</li> <li>• userPassword</li> </ul>

Copie d'écran schéma de l'entrée posixAccount - vue complète<sup>20</sup>

## 5. Configuration de l'accès client au serveur LDAP

Dans cette section, on suppose qu'un annuaire LDAP est disponible et accessible. On se propose de configurer un poste client pour qu'il obtienne de façon transparente les informations sur les comptes utilisateurs desservis par l'annuaire.

### 5.1. Interrogation à distance de l'annuaire LDAP

On reprend ici les requêtes de visualisation des entrées vues dans la [Section 4.4, « Composition d'un nouvel annuaire LDAP »](#). Cette fois ci les requêtes sont émises depuis un hôte réseau différent du serveur.

1. Quel est le paquet qui fournit les commandes de manipulation des entrées de l'annuaire ?

Interroger la base de données des paquets pour obtenir les informations demandées.

```
# aptitude install ldap-utils
```

Le paquet `ldap-utils` apparaît à la question sur [la liste des paquets relatifs au service LDAP](#). Si on recherche les commandes présentes dans la liste des fichiers de ce paquet, on obtient les informations suivantes.

```
# dpkg -L ldap-utils | grep bin
/usr/bin
/usr/bin/ldapmodrdn
/usr/bin/ldappasswd
/usr/bin/ldapdelete
/usr/bin/ldapsearch
/usr/bin/ldapmodify
/usr/bin/ldapexop
/usr/bin/ldapurl
/usr/bin/ldapcompare
/usr/bin/ldapwhoami
/usr/bin/ldapadd
```

Une fois ce paquet installé, il est possible d'utiliser toutes les commandes disponibles pour manipuler les enregistrements de l'annuaire.

2. Quelle est la syntaxe d'interrogation de l'annuaire qui permet d'obtenir tous les attributs de l'enregistrement correspondant à un utilisateur particulier ?

On reprend la commande `ldapsearch` en spécifiant un attribut `uid` particulier.

```
# ldapsearch -LLL -H ldap://192.200.0.3 \
-b dc=lab,dc=stri -D cn=admin,dc=lab,dc=stri -W uid=padme
Enter LDAP Password:
dn: uid=padme,ou=people,dc=lab,dc=stri
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
```

<sup>20</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/phpldapadmin-3.png>

```

cn: Padme
sn:: UGFkbcOpIEFtaWRhbGEGU2t5d2Fsa2Vy
uid: padme
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
homeDirectory: /ahome/padme
userPassword:: e1NTSEF9dTBHW1AwclJsZDliOHJ4TzZhNEhSM1p0NE1KTGk0bFY=
gecos: Padme Amidala Skywalker

```

3. Quelle est la syntaxe de la commande permettant de changer le mot de passe de l'utilisateur dont on a affiché les attributs à la question précédente ?

On utilise la commande **ldappasswd** fournie par le paquet `ldap-utils` comme dans le cas de la commande de recherche. Après consultation des pages de manuels, on obtient la syntaxe suivante.

```

# ldappasswd -x -H ldap://192.200.0.3 \
-D cn=admin,dc=lab,dc=stri -w -stri- -S uid=padme,ou=people,dc=lab,dc=stri
New password:
Re-enter new password:

```

En posant exactement la même requête que dans la question précédente, on peut vérifier que le mot de passe utilisateur a bien été modifié.

```

# ldapsearch -LLL -H ldap://192.200.0.3 \
-b dc=lab,dc=stri -D cn=admin,dc=lab,dc=stri -W uid=padme
Enter LDAP Password:
dn: uid=padme,ou=people,dc=lab,dc=stri
objectClass: person
objectClass: shadowAccount
objectClass: posixAccount
cn: Padme
sn:: UGFkbcOpIEFtaWRhbGEGU2t5d2Fsa2Vy
uid: padme
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
homeDirectory: /ahome/padme
gecos: Padme Amidala Skywalker
userPassword:: e1NTSEF9SXJKY2ZyMXJ3Z0tVd2VUd2VHbUg4U2JaUF1RQlQxcDE=

```

## 5.2. Configuration Name Service Switch

Les manipulations présentées ici ont pour but de rendre transparent l'accès aux attributs des comptes utilisateurs. Le mécanisme *Name Service Switch* assure un aiguillage de l'accès à ces attributs entre les fichiers locaux et les différents services réseau disponibles. Ici, l'annuaire LDAP constitue un dépôt de référence pour le stockage des attributs des comptes utilisateurs.

1. Quel est le nom du paquet relatif au mécanisme *Name Service Switch* permettant d'accéder aux ressources de l'annuaire LDAP ?

Rechercher dans les bases du gestionnaire de paquets un paquet dont le nom débute par la chaîne `libnss`.

La liste ci-dessous permet d'identifier le paquet `libnss-ldap`.

```

# aptitude search '?name(^libnss)'
p libnss-db - NSS module for using Berkeley Databases as a naming service
p libnss-extrousers - nss module to have an additional passwd, shadow and group file
p libnss-gw-name - nss module that names the current gateway's IP address
p libnss-ldap - NSS module for using LDAP as a naming service
p libnss-ldapd - NSS module for using LDAP as a naming service
p libnss-lwres - NSS module for using bind9's lwres as a naming service
p libnss-mdns - NSS module for Multicast DNS name resolution
p libnss-myhostname - nss module providing fallback resolution for the current hostname
p libnss-mysql-bg - NSS module for using MySQL as a naming service
v libnss-pgsql1 -
p libnss-pgsql2 - NSS module for using PostgreSQL as a naming service
p libnss-rainbow2 - nss library for rainbow

```

```
p libnss-sss - Nss library for the System Security Services Daemon
p libnss3-ld - Network Security Service libraries
p libnss3-ld-dbg - Debugging symbols for the Network Security Service libraries
p libnss3-dev - Development files for the Network Security Service libraries
p libnss3-tools - Network Security Service tools
```

2. Quels sont les paquets qui dépendent de l'installation des bibliothèques LDAP pour le mécanisme *Name Service Switch* ?

Utiliser les informations contenues dans la description du paquet pour repérer les dépendances entre paquets.

```
# aptitude show libnss-ldap
Paquet : libnss-ldap
État: non installé
Version : 264-2.2
Priorité : supplémentaire
Section : admin
Responsable : Richard A Nelson (Rick) <cowboy@debian.org>
Taille décompressée : 274 k
Dépend: libc6 (>= 2.3.2), libcomerr2 (>= 1.01),
        libgssapi-krb5-2 (>= 1.6.dfsg.2),
        libkrb5-3 (>= 1.6.dfsg.2),
        libldap-2.4-2 (>= 2.4.7),
        libsasl2-2, debconf (>= 0.5) |
        debconf-2.0
Recommande: nscd, libpam-ldap
Fourni par : libnss-ldapd
Description : NSS module for using LDAP as a naming service
This package provides a Name Service Switch that allows your LDAP server act
as a name service. This means providing user account information, group id's,
host information, aliases, netgroups, and basically anything else that you
would normally get from /etc flat files or NIS.

If used with glibc 2.1's nscd (Name Service Cache Daemon) it will help reduce
your network traffic and speed up lookups for entries.
```

Le lancement de l'installation du paquet `libnss-ldap` donne la liste suivante.

```
# aptitude install libnss-ldap
Les NOUVEAUX paquets suivants vont être installés :
  libnss-ldap libpam-ldap{a} nscd{a}
0 paquets mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 409 ko d'archives. Après dépaquetage, 1 004 ko seront utilisés.
Voulez-vous continuer ? [Y/n/?]
```

Deux paquets supplémentaires apparaissent : `libpam-ldap` et `nscd`.

3. Quel est le rôle de l'interface entre les fonctions PAM (*Pluggable Authentication Modules*) et l'annuaire LDAP ?

Par définition, PAM est un mécanisme qui permet d'intégrer différents modes d'authentification en les rendant transparents vis à vis de l'utilisateur et des logiciels qui accèdent aux ressources du système. Dans le contexte de ces travaux pratiques, il s'agit de permettre à l'utilisateur de se connecter, d'accéder au système de fichiers, de changer son mot de passe, etc sans avoir à lancer des commandes spécifiques.

4. Quelles sont les principales étapes de la configuration des paquets de bibliothèques NSS et PAM ?

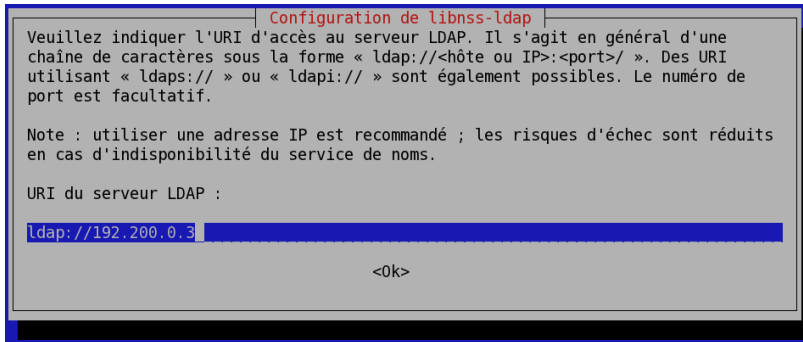
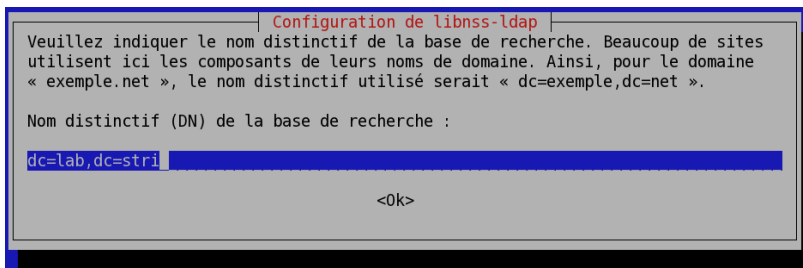
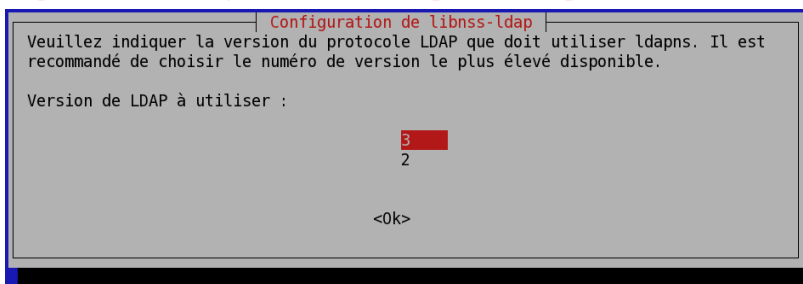
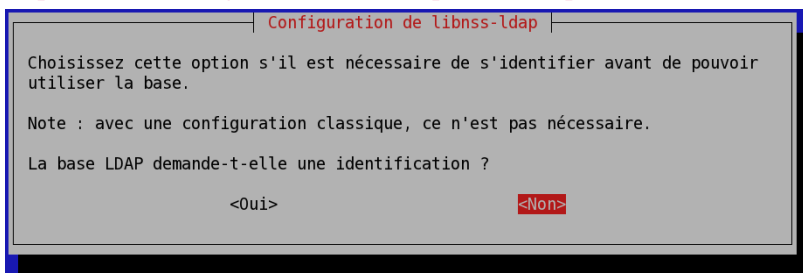
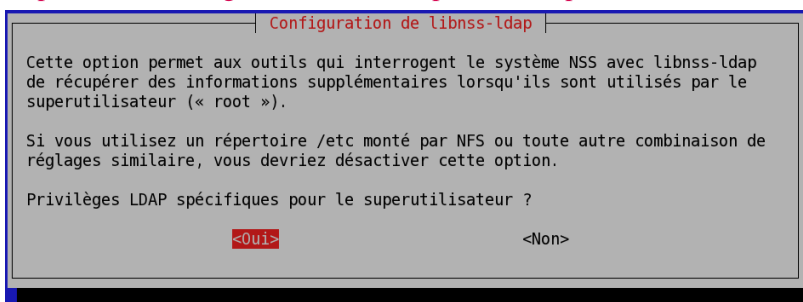
Lors de l'installation des deux paquets de bibliothèques LDAP, on passe par une série de menus `debconf` qu'il faut renseigner correctement pour accéder au serveur LDAP de façon transparente.

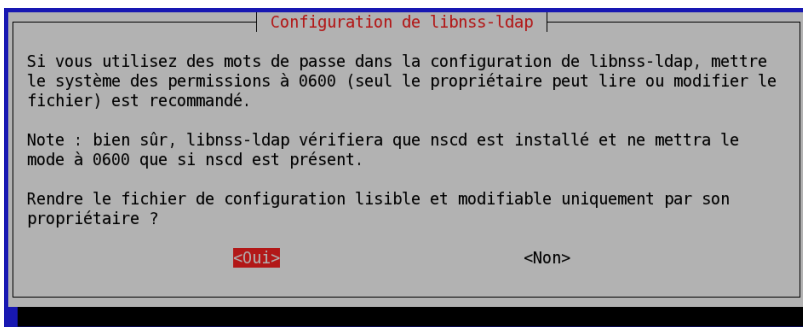
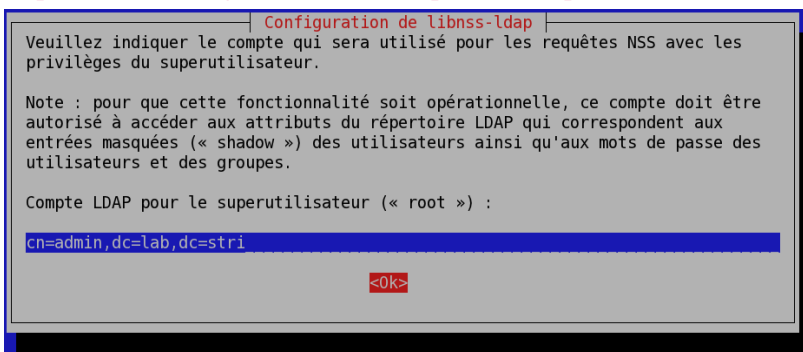
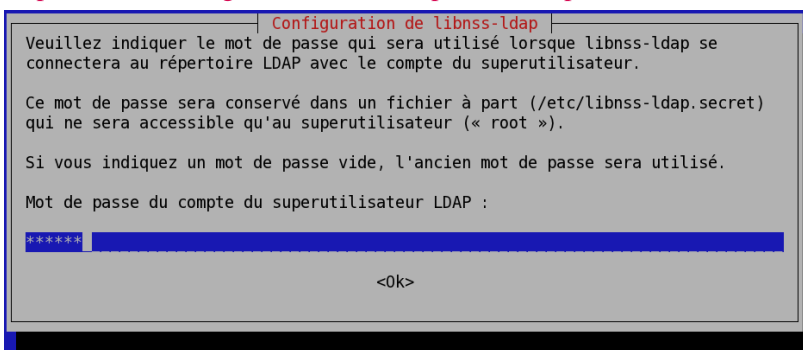
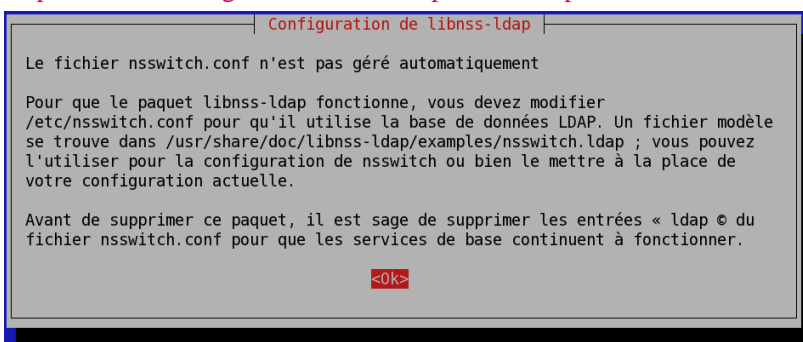
Les étapes de configuration des deux paquets `libnss-ldap` et `libpam-ldap` sont pratiquement identiques.



#### Avertissement

En cas d'erreur de saisie dans la série de menus ci-dessous, il faut reprendre la configuration de chacun des deux paquets individuellement. Classiquement, on utilise les instructions `# dpkg-reconfigure libnss-ldap` et `# dpkg-reconfigure libpam-ldap`.

Copie d'écran configuration libnss-ldap - vue complète<sup>21</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>22</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>23</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>24</sup><sup>21</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-1.png><sup>22</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-2.png><sup>23</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-3.png><sup>24</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-4.png>

Copie d'écran configuration libnss-ldap - vue complète<sup>25</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>26</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>27</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>28</sup>Copie d'écran configuration libnss-ldap - vue complète<sup>29</sup>

Pour le paquet libpam-ldap, voici la liste des options retenues.

<sup>25</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-5.png>

<sup>26</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-6.png>

<sup>27</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-7.png>

<sup>28</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-8.png>

<sup>29</sup> <http://www.linux-france.org/prj/inetdoc/cours/admin.reseau.ldap.synthese/images/libnss-ldap-9.png>

- Identifiant uniforme de ressource (« URI ») d'accès au serveur LDAP : ldap://192.200.0.3
- Nom distinctif (DN) de la base de recherche : dc=lab,dc=stri
- Version de LDAP à utiliser : 3
- Donner les privilèges de superutilisateur local au compte administrateur LDAP ? oui
- La base de données LDAP demande-t-elle une identification ? non
- Compte de l'administrateur LDAP : cn=admin,dc=lab,dc=stri
- Mot de passe du compte de l'administrateur LDAP : \*\*\*\*\*
- Algorithme de chiffrement à utiliser localement pour les mots de passe : Chiffré
- Profils PAM à activer : Unix authentication + LDAP Authentication

5. Quelles sont les modifications à apporter au fichier de configuration `/etc/nsswitch.conf` pour activer l'accès aux ressources de l'annuaire LDAP ?

Suivant les indications données dans la série de menus `debconf` ci-dessus, il faut éditer manuellement le fichier `/etc/nsswitch.conf`. Consulter les exemples fournis avec la documentation du paquet de bibliothèques LDAP pour le mécanisme NSS.

Après consultation de l'exemple `/usr/share/doc/libnss-ldap/examples/nsswitch.ldap`, on peut éditer le fichier `/etc/nsswitch.conf`. Voici un *patch* reflétant les différences entre le fichier d'origine et le fichier modifié.

```
# diff -uBb /etc/nsswitch.conf.dist /etc/nsswitch.conf
--- /etc/nsswitch.conf.dist      2011-04-25 11:50:11.000000000 +0200
+++ /etc/nsswitch.conf         2011-04-25 11:50:37.000000000 +0200
@@ -4,9 +4,9 @@
 # If you have the `glibc-doc-reference' and `info' packages installed, try:
 # `info libc "Name Service Switch"' for information about this file.

-passwd:          compat
-group:           compat
-shadow:          compat
+passwd:          files ldap
+group:           files ldap
+shadow:          files ldap

 hosts:           files dns
 networks:        files
```

6. Comment illustrer simplement le fonctionnement du mécanisme *Name Service Switch* intégrant l'utilisation de l'annuaire LDAP ?

Rechercher la commande de récupération des entrées depuis les bases de données d'administration dans les outils fournis avec les bibliothèques standard (paquet `libc-bin`).

La commande **getent** fournie avec le paquet `libc-bin` donne la liste des entrées accessibles pour chaque catégorie du fichier de configuration. Voici un exemple pour la catégorie `passwd` qui fait apparaître les entrées de l'annuaire LDAP à la suite des comptes utilisateurs système issus des fichiers locaux.

```
# getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
```

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
etu:x:1000:1000:Etudiant,,,:/home/etu:/bin/bash
padme:x:10000:10000:Padme Amidala Skywalker:/ahome/padme:/bin/bash
anakin:x:10001:10001:Anakin Skywalker:/ahome/anakin:/bin/bash
leia:x:10002:10002:Leia Organa:/ahome/leia:/bin/bash
luke:x:10003:10003:Luke Skywalker:/ahome/luke:/bin/bash
```

## 7. Comment valider l'authentification d'un utilisateur déclaré dans l'annuaire LDAP ?

Choisir un service qui nécessite une authentification sur le système et qui utilise une entrée de l'annuaire LDAP.



### Avertissement

Après chaque manipulation sur la configuration des paquets `libnss-ldap` et `libpam-ldap`, il faut impérativement relancer le démon de gestion du cache des services de noms : `# /etc/init.d/nscd restart`.

Sans le redémarrage de ce démon, il est fréquent que les tests de connexion échouent alors que la configuration système est correcte.

Les exemples de services nécessitant une authentification ne manquent pas. La commande `su` qui permet de changer d'identité est le plus immédiat.

```
$ etu@clnt:~$ su anakin
Mot de passe :
anakin@clnt:/home/etu$ cd
bash: cd: /ahome/anakin: Aucun fichier ou dossier de ce type
anakin@clnt:/home/etu$ exit
etu@clnt:~$
```

Dans les journaux du système, on retrouve les mêmes éléments.

```
su[2718]: + /dev/pts/0 etu:anakin
su[2718]: pam_unix(su:session): session opened for user anakin by etu(uid=1000)
su[2718]: pam_unix(su:session): session closed for user anakin
```

Voici un autre exemple d'accès avec SSH.

```
$ ssh anakin@192.200.0.4
anakin@192.200.0.4's password:
Linux clnt 2.6.38-2-amd64 #1 SMP Thu Apr 7 04:28:07 UTC 2011 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 25 10:17:09 2011 from 192.200.0.3
Could not chdir to home directory /ahome/anakin: No such file or directory
```

Il ne manque que l'accès au système de fichiers pour que la configuration soit vraiment complète.

## 6. Analyse de la configuration

Dans cette partie, on considère que les services élémentaires sont en place. Côté **serveur**, on dispose de l'unité organisationnelle `people` qui contient quatre entrées de comptes utilisateurs. Côté **client**, les outils d'accès à l'annuaire LDAP ont été installés et l'authentification sur la base des attributs des entrées de l'annuaire fonctionne.

Les manipulations suivantes sont à réaliser en concertation entre les deux postes de travaux pratiques client et serveur.

## 6.1. Indexation des entrées de l'annuaire LDAP

Comme la **journalisation des transactions sur l'annuaire** a été activée sur le serveur, toutes les **authentifications** réalisées par le client apparaissent dans ces journaux.

1. Quelles sont les informations relatives à l'indexation des entrées de l'annuaire qui apparaissent dans les journaux système du serveur lorsqu'une transaction est initiée par le client ?

Que constate-t-on ?

Rechercher le mot clé `index` dans le principal fichier de journalisation système du serveur.

On constate que de nombreux attributs utilisés ne sont pas indexés en consultant les journaux système.

```
# grep -i index /var/log/syslog
slapd[1161]: <= bdb_equality_candidates: (uid) not indexed
slapd[1161]: <= bdb_equality_candidates: (memberUid) not indexed
slapd[1161]: <= bdb_equality_candidates: (uid) not indexed
slapd[1161]: <= bdb_equality_candidates: (memberUid) not indexed
slapd[1161]: <= bdb_equality_candidates: (uniqueMember) not indexed
slapd[1161]: <= bdb_equality_candidates: (uid) not indexed
slapd[1161]: <= bdb_equality_candidates: (uid) not indexed
```

2. Quelle est la syntaxe du fichier LDIF permettant d'ajouter les index identifiés dans la configuration du service LDAP ?

Rechercher un tutoriel LDIF en ligne donnant un exemple de fichier LDIF avec une ou plusieurs entrées `index`.

Voici un exemple de fichier LDIF dédié à l'ajout d'index sur les principales entrées de l'annuaire.

```
# cat olcDbIndex.ldif
dn: olcDatabase={1}hdb,cn=config
changetype: modify
add: olcDbIndex
olcDbIndex: uid pres,eq,sub
-
add: olcDbIndex
olcDbIndex: sn eq,sub
-
add: olcDbIndex
olcDbIndex: memberUid pres,eq,sub
-
add: olcDbIndex
olcDbIndex: uniqueMember pres,eq
-
add: olcDbIndex
olcDbIndex: cn pres,eq,sub
-
add: olcDbIndex
olcDbIndex: ou eq
-
add: olcDbIndex
olcDbIndex: dc eq
```

Dans cet exemple plusieurs types d'index ont été spécifiés.

- Le type `pres` est la contraction de `presence` et correspond à des requêtes comme `objectclass=person` ou `attribute=mail`.
- Le type `eq` est la contraction de `equality` et correspond à des requêtes comme `sn=dupond`.
- Le type `sub` est la contraction de `substring` et correspond à des requêtes comme `sn=du*`.



### Note

D'après la spécification du format LDIF, les lignes qui ne contiennent qu'un caractère '-' sont des séparateurs entre des modifications apportées à une même entrée tandis que les lignes vides séparent des traitements sur des entrées différentes.

### 3. Comment mettre en place les nouveaux index et valider leur présence dans la configuration du service LDAP ?

Reprendre la démarche suivie lors de l'activation des fonctions de **journalisation**.

On utilise la commande **ldapmodify** pour appliquer les instructions contenues dans le fichier LDIF.

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

On valide la présence des index dans la configuration courante avec une requête sur les index.

```
# ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config" | grep ^olcDbIndex
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
olcDbIndex: objectClass eq
olcDbIndex: uid pres,eq,sub
olcDbIndex: sn eq,sub
olcDbIndex: memberUid pres,eq,sub
olcDbIndex: uniqueMember pres,eq
olcDbIndex: cn pres,eq,sub
olcDbIndex: ou eq
olcDbIndex: dc eq
```

### 4. Comment créer les index dans la base de données du démon slapd ?

Rechercher dans la liste des fichiers du paquet slapd la commande relative à l'indexation des entrées d'un annuaire.

```
# dpkg -L slapd | grep index
/usr/sbin/slapindex
/usr/share/man/man8/slapindex.8.gz
```

La création des fichiers de bases d'index nécessite un arrêt du service avant l'appel à la commande **slapindex**. Il est nécessaire de prendre l'identité `openldap` pour exécuter cette commande. Tous les fichiers de bases de données (*backend*) doivent avoir le même propriétaire que le processus `slapd`.

```
# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
# su openldap -c "slapindex"
# /etc/init.d/slapd start
Starting OpenLDAP: slapd.

# ll /var/lib/ldap/*.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 19:37 /var/lib/ldap/cn.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 19:37 /var/lib/ldap/dc.bdb
-rw----- 1 openldap openldap 8,0K 24 avril 17:37 /var/lib/ldap/dn2id.bdb
-rw----- 1 openldap openldap 32K 24 avril 19:23 /var/lib/ldap/id2entry.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 19:37 /var/lib/ldap/memberUid.bdb
-rw----- 1 openldap openldap 8,0K 24 avril 17:37 /var/lib/ldap/objectClass.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 19:37 /var/lib/ldap/ou.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 21:07 /var/lib/ldap/sn.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 19:31 /var/lib/ldap/uid.bdb
-rw----- 1 openldap openldap 8,0K 25 avril 20:33 /var/lib/ldap/uniqueMember.bdb
```

## 6.2. Analyse réseau des transactions LDAP

Comme dans le cas du support sur l' *Introduction au système de fichiers réseau NFS*<sup>30</sup>, la compréhension des mécanismes d'accès à un annuaire passe par l'analyse réseau. Les opérations de capture de trafic peuvent être réalisées aussi bien sur le poste client que sur le poste serveur.

### 1. Quelles sont les étapes de l'accès aux ressources de l'annuaire LDAP dans les trois cas de figure ci-dessous ?

Exécuter les instructions suivantes depuis le poste client.

- `# getent passwd`

<sup>30</sup> <http://www.linux-france.org/prj/inetdoc/cours/index.html#admin.reseau.nfs>

- `$ su anakin`
- `anakin@clnt:/home/etu$ passwd`

## 7. Documents de référence

*OpenLDAP Software 2.4 Administrator's Guide*

La documentation officielle : *OpenLDAP Software 2.4 Administrator's Guide*<sup>31</sup> constitue le point d'entrée essentiel pour la mise en œuvre du service LDAP.

---

<sup>31</sup> <http://www.openldap.org/doc/admin24/>