Introduction aux annuaires LDAP avec OpenLDAP

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé

Dans ce support de travaux pratiques, on explore le 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`.

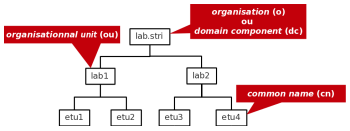


Table des matières

1. Copyright et Licence

Méta-information

Ce document est écrit avec *DocBook* XML sur un système *Debian GNU/Linux*. Il est disponible en version imprimable au format PDF : `sysadm-net.ldap.qa.pdf`.

2. 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™ 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*. Avec un service NIS, il n'est pas

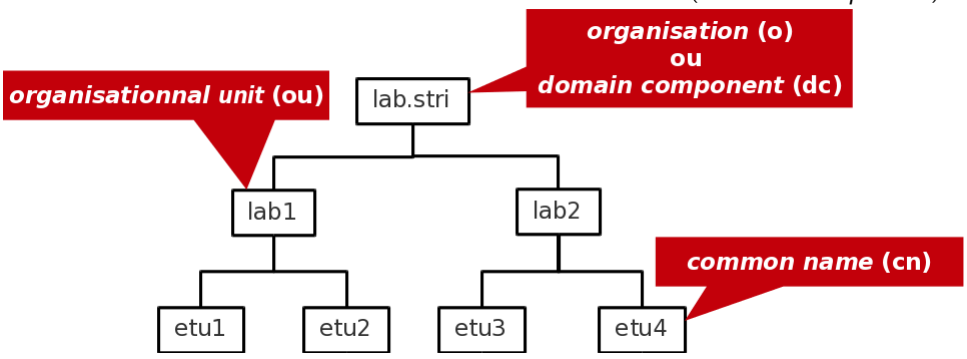
possible de constituer des groupes logiques ayant des attributs propres. Cette limitation est rapidement devenue critique avec l'augmentation du nombres des utilisateurs et des clients.

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

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=lab2,dc=lab,dc=stri`

  `dn: cn=etu4,ou=lab2,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.

entry	***objectclass***

`o: lab.stri`
`dc: lab`
`dc: stri`
	`organisation`
	`dcObject`
	`dcObject`

`ou: lab1`	`organisationalUnit`
`cn: etu1`	`inetOrgPerson`

entry	*objectclass*
`sn: etu1`	

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

3. 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.

3.1. Installation du serveur LDAP

Q1. 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.

```
apt search ^OpenLDAP
```

```
En train de trier... Fait
Recherche en texte intégral... Fait
ldap-utils/testing 2.5.13+dfsg-5 amd64
  OpenLDAP utilities

libldap-2.5-0/testing,now 2.5.13+dfsg-5 amd64  [installé, automatique]
  Bibliothèques OpenLDAP

libldap-common/testing,now 2.5.13+dfsg-5 all  [installé, automatique]
  fichiers communs OpenLDAP pour les bibliothèques

libldap-dev/testing 2.5.13+dfsg-5 amd64
  bibliothèques de développement pour OpenLDAP

ruby-ldap/testing 0.9.20-2+b5 amd64
  OpenLDAP library binding for Ruby

slapd/testing 2.5.13+dfsg-5 amd64
  OpenLDAP server (slapd)
```

Q2. Quels sont les paquets Debian à installer pour mettre en œuvre un serveur LDAP ?

Dans liste obtenue en réponse à la question précédente, rechercher les paquets relatifs aux utilitaires et au serveur.

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

```
sudo apt -y install slapd ldap-utils
```

```
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libltdl7 libodbc2
Paquets suggérés :
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal odbc-postgresql tdsodbc
Les NOUVEAUX paquets suivants seront installés :
  ldap-utils libltdl7 libodbc2 slapd
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
```

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

Q3. 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    1699  0.0  1.0 1159776 10540 ?       Ssl  18:22   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`.

Q4. 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.

```
sudo lsof -i | grep l[d]ap
```

```
slapd   1699 openldap    8u  IPv4  19101      0t0  TCP *:ldap (LISTEN)
slapd   1699 openldap    9u  IPv6  19102      0t0  TCP *:ldap (LISTEN)
```

```
ss -tau | grep l[d]ap
```

```
tcp   LISTEN 0      2048        0.0.0.0:ldap            0.0.0.0:*
tcp   LISTEN 0      2048           [::]:ldap               [::]:*
```

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

Par défaut l'accès TLS au service n'est pas activé.

3.2. Analyse de la configuration du service LDAP

Les versions actuelles 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.

Q5. Quel est le mode de gestion de la configuration du service du paquet de la distribution Debian GNU/Linux ?

Consulter les fichiers de documentation fournis avec le paquet `slapd`.

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.

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

Q6. Quel est le gestionnaire de base de données (***backend***) proposé dans l'annuaire de configuration ?

Reprendre la commande préconisée en réponse à la question précédente en utilisant le type de base de donnée comme filtre.

```
sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config" \
  olcDatabase={1}mdb
```

```
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}mdb
# requesting: ALL
#

# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=nodomain
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=nodomain
olcRootPW: {SSHA}y3201Tkxe0HgfQOhLxiVJ3wwI8+dnQwK
olcDbCheckpoint: 512 30
olcDbIndex: objectClass eq
olcDbIndex: cn,uid eq
olcDbIndex: uidNumber,gidNumber eq
olcDbIndex: member,memberUid eq
olcDbMaxSize: 1073741824

# 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 `mdb`. Il s'agit d'une variante actualisée du gestionnaire ***Berkeley DB transactional backend***.

Q7. Comment identifier le nom de l'annuaire fourni par défaut avec le paquet `slapd` ?

Rechercher la clé `olcSuffix` dans la configuration de l'annuaire.

```
sudo 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
```

Q8. Quels sont les ***schemas*** actifs avec la configuration courante du paquet `slapd` ?

Rechercher la clé `olcSchemaConfig` dans la configuration de l'annuaire.

```
sudo 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
```

Q9. Où sont stockées les bases définies par défaut lors de l'installation du paquet `slapd` ?

Rechercher la clé `olcDbDirectory` dans la configuration de l'annuaire.

```
sudo ldapsearch -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 40K
-rw------- 1 openldap openldap  36K  2 sept. 18:22 data.mdb
-rw------- 1 openldap openldap 8,0K  2 sept. 18:22 lock.mdb
```

3.3. 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.

Q10. Comment arrêter le service LDAP ?

Utiliser les scripts fournis avec le gestionnaire de lancement des processus système.

Chaque processus système dispose d'un script de gestion de son lancement, arrêt (et|ou) redémarrage. Avec le gestionnaire systemd, il faut faire une recherche dans la liste des services. Une fois le service identifié, on l'arrête avec la commande systemctl.

```
systemctl status slapd
```

```
# slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
     Loaded: loaded (/etc/init.d/slapd; generated)
    Drop-In: /usr/lib/systemd/system/slapd.service.d
             └─slapd-remain-after-exit.conf
     Active: active (running) since Sat 2023-09-02 18:22:14 CEST; 21min ago
       Docs: man:systemd-sysv-generator(8)
    Process: 1693 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
      Tasks: 4 (limit: 1084)
     Memory: 7.4M
        CPU: 59ms
     CGroup: /system.slice/slapd.service
             └─1699 /usr/sbin/slapd -h "ldap:/// ldapi:///" -g openldap -u openldap -F /etc/ldap/slapd.d

sept. 02 18:22:14 ldap-server systemd[1]: Starting slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory A
sept. 02 18:22:14 ldap-server slapd[1698]: @(#) $OpenLDAP: slapd 2.5.13+dfsg-5 (Feb  8 2023 01:56:12) $
                                                    Debian OpenLDAP Maintainers <pkg-openldap-devel@lists.alioth.debian.org>
sept. 02 18:22:14 ldap-server slapd[1699]: slapd starting
sept. 02 18:22:14 ldap-server slapd[1693]: Starting OpenLDAP: slapd.
sept. 02 18:22:14 ldap-server systemd[1]: Started slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Ac
```

Instruction d'arrêt du service :

```
sudo systemctl stop slapd
```

On peut exécuter à nouveau la commande systemctl status slapd pour confirmer que le service est bien stoppé et inactif.

Q11. Quels sont les éléments à supprimer 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 de données du service. 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 supprime donc tous ces fichiers et répertoires.

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

Q12. Comment reprendre à zéro la configuration du paquet `slapd` ?

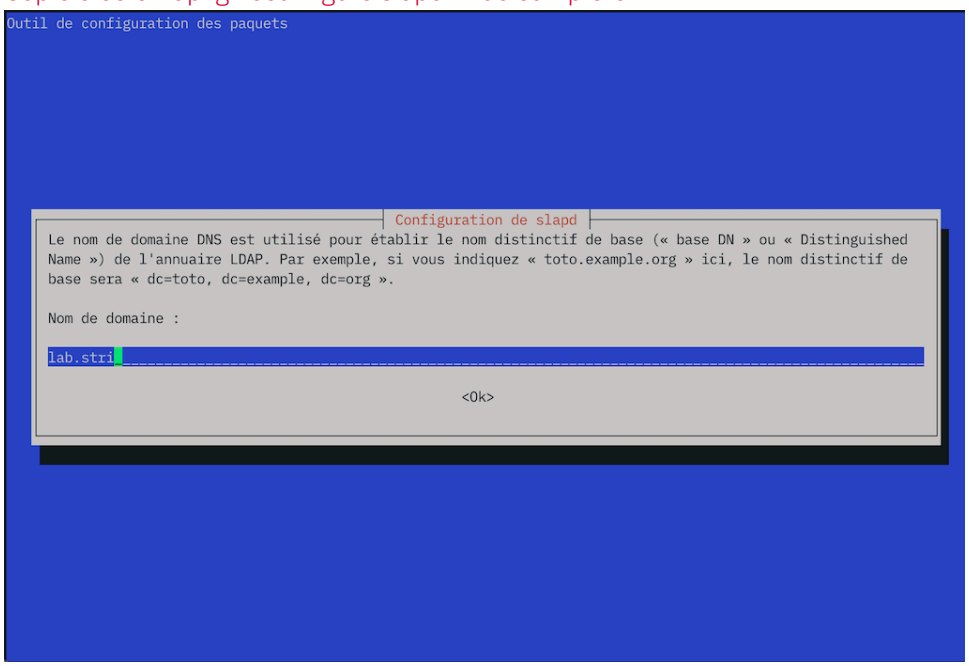
Utiliser l'outil du gestionnaire de paquets ***Debian GNU/Linux*** qui permet la modification des paramètres de configuration d'un service à l'aide de menus `debconf`.

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`.

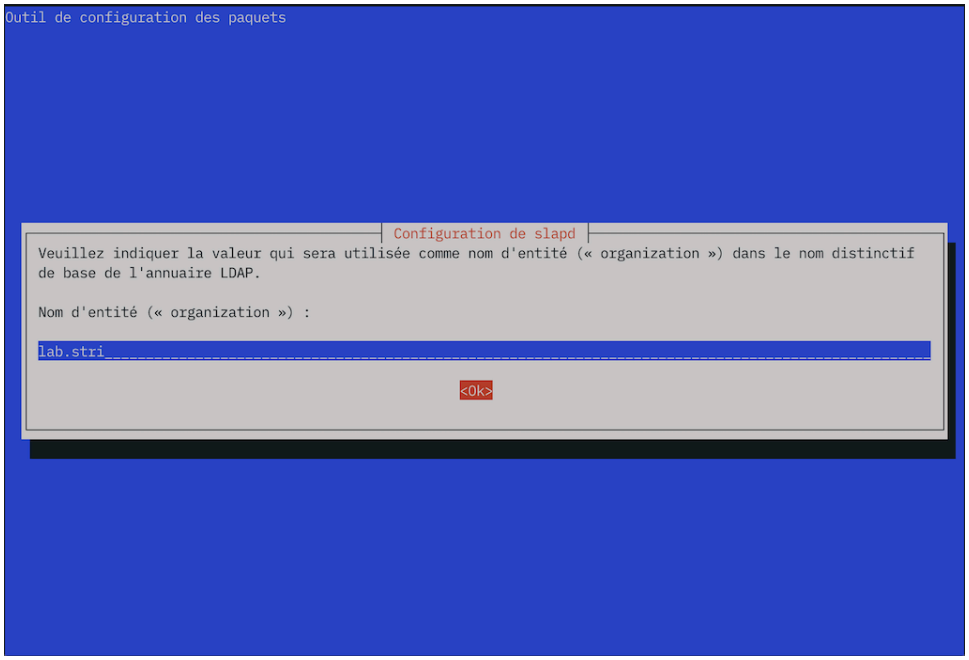
```
sudo dpkg-reconfigure slapd
```

```
  Creating initial configuration... done.
  Creating LDAP directory... done.
```

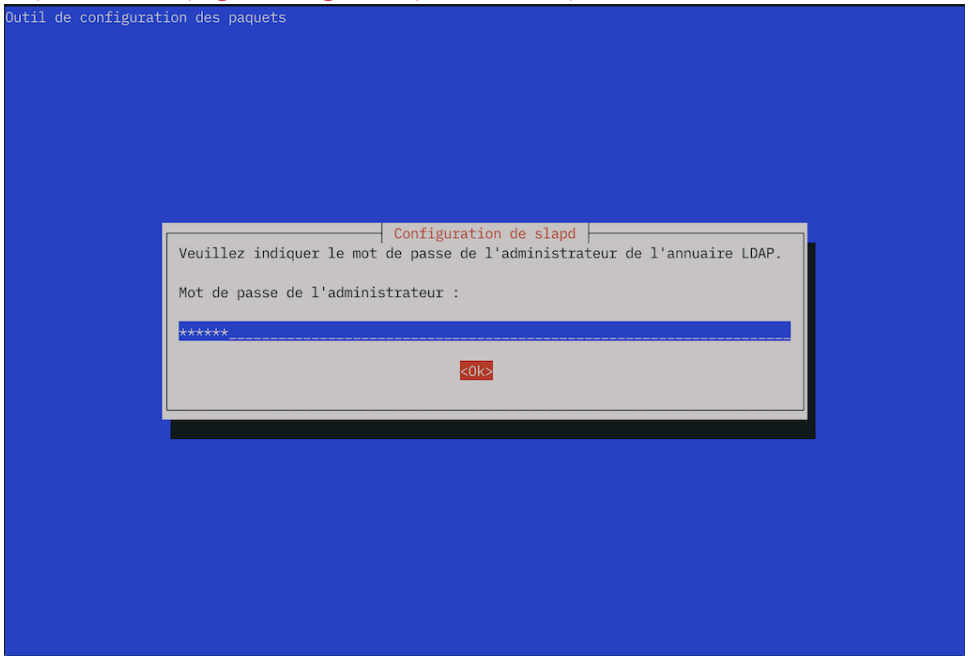
Copie d'écran dpkg-reconfigure slapd - vue complète



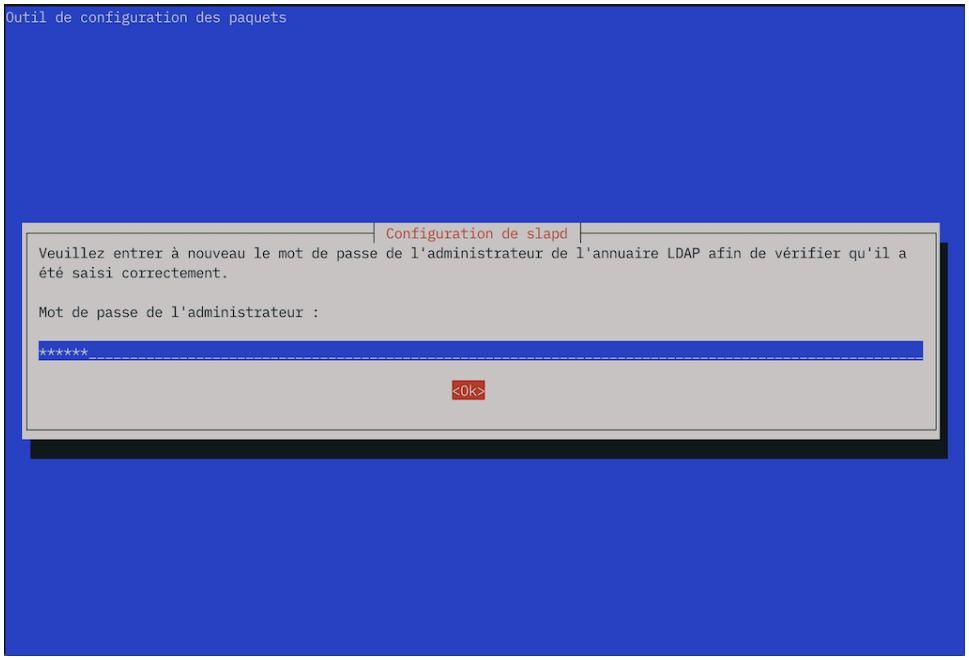
Copie d'écran dpkg-reconfigure slapd - vue complète



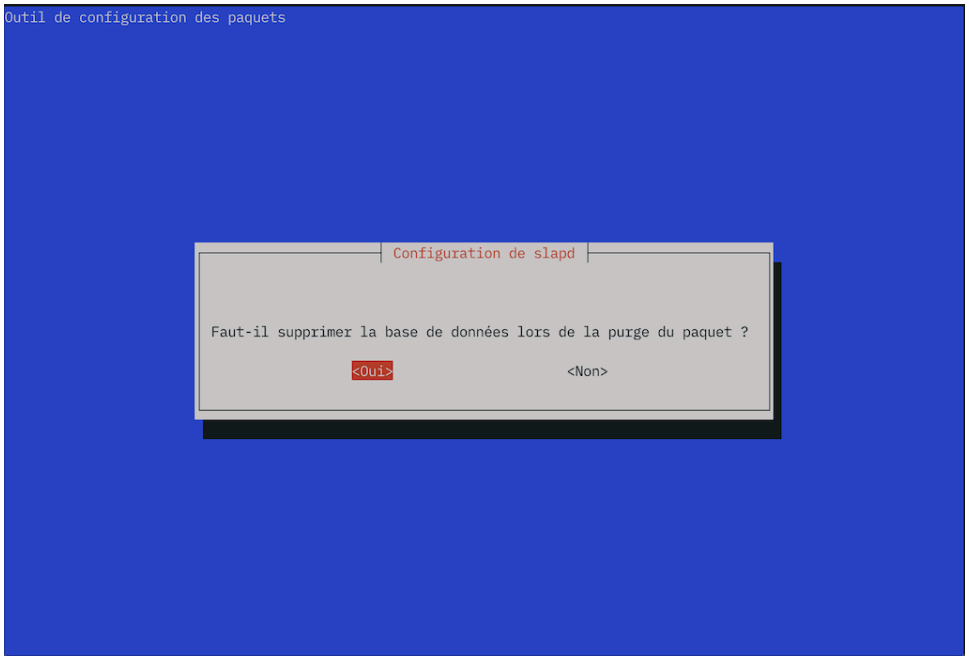
Copie d'écran dpkg-reconfigure slapd - vue complète



Copie d'écran dpkg-reconfigure slapd - vue complète



Copie d'écran dpkg-reconfigure slapd - vue complète



Copie d'écran dpkg-reconfigure slapd - vue complète

Q13. Comment valider la nouvelle configuration du paquet `slapd` ?

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

```
sudo 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
```

3.4. 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».

Q14. 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.

```
sudo 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
```

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

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

- 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.

Q15. 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`.

```
sudo 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 remplacer 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.

On commence par créer un dossier dédié aux fichiers LDIF.

```
mkdir -p $HOME/ldif && cd $HOME/ldif
```

Ensuite on peut créer le fichier LDIF de modification de la journalisation du service LDAP.

```
cat > setolcLogLevel2stats.ldif << EOF
# Set olcLogLevel to "stats"
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
EOF
```

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

```
sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f setolcLogLevel2stats.ldif
```

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

```
sudo 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.

```
journalctl -o cat -n 20 -u slapd --grep="conn"
conn=1009 fd=12 closed
conn=1009 op=2 UNBIND
conn=1009 op=1 SEARCH RESULT tag=101 err=0 qtime=0.000017 etime=0.000193 nentries=10 text=
conn=1009 op=1 SRCH attr=olcLogLevel
conn=1009 op=1 SRCH base="cn=config" scope=2 deref=0 filter="(objectClass=*)"
conn=1009 op=0 RESULT tag=97 err=0 qtime=0.000018 etime=0.000107 text=
conn=1009 op=0 BIND dn="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" mech=EXTERNAL bind_ssf=0 ssf=71
conn=1009 op=0 BIND authcid="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" authzid="gidNumber=0+uidNumber=0,cn=p
conn=1009 op=0 BIND dn="" method=163
conn=1009 fd=12 ACCEPT from PATH=/var/run/slapd/ldapi (PATH=/var/run/slapd/ldapi)
conn=1008 fd=12 closed
conn=1008 op=2 UNBIND
conn=1008 op=1 RESULT tag=103 err=0 qtime=0.000021 etime=0.000558 text=
```

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.

```
cat > setolcLogLevel2none.ldif << EOF
# Set olcLogLevel to "none"
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: none
EOF
```

Q16. 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 << EOF
dn: ou=people,dc=lab,dc=stri
objectClass: organizationalUnit
ou: people

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

Q17. 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.

```
sudo 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.

```
sudo 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: ou=people,dc=lab,dc=stri
objectClass: organizationalUnit
ou: people

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

Q18. 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.

Prenons l'exemple du mot de passe `V3ry53cr3t`, on obtient le résultat suivant :

```
sudo slappasswd
```

```
New password:
Re-enter new password:
{SSHA}rpB4tgcVlh51sPCtpBi+acrS6Ifc1lu0
```

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

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.

1. On génère un mot de passe aléatoire que l'on stocke dans un fichier.

   ```
   openssl rand -base64 16 | tr -d '=' > user.passwd
   ```

   On obtient par exemple :

   ```
   cat user.passwd
   vyJtXX6r73KPzyDYymWjsA
   ```

2. Utilise ce mot de passe pour générer la chaîne à introduire dans le fichier LDIF de création d'utilisateur dans l'annuaire.

   ```
   sudo slappasswd -v -h "{SSHA}" -s $(cat user.passwd)
   ```

   ```
   {SSHA}hFGouu+ytfnH0qPy7y9G0L0Rb6R6slZ4
   ```

Q19. 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.

Avertissement

Pensez à adapter les entrées `userPassword` à votre contexte !

```
cat > users.ldif << EOF
# Padmé Amidala
dn: uid=padme,ou=people,dc=lab,dc=stri
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
cn: Padme
sn: Padmé Amidala Skywalker
uid: padme
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
homeDirectory: /ahome/padme
userPassword: {SSHA}hFGouu+ytfnH0qPy7y9G0L0Rb6R6slZ4
gecos: Padme Amidala Skywalker

# Anakin Skywalker
dn: uid=anakin,ou=people,dc=lab,dc=stri
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
cn: Anakin
sn: Anakin Skywalker
uid: anakin
uidNumber: 10001
gidNumber: 10001
loginShell: /bin/bash
homeDirectory: /ahome/anakin
userPassword: {SSHA}hFGouu+ytfnH0qPy7y9G0L0Rb6R6slZ4
gecos: Anakin Skywalker

# Leia Organa Skywalker
dn: uid=leia,ou=people,dc=lab,dc=stri
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
cn: Leia
sn: Leia Organa
uid: leia
uidNumber: 10002
gidNumber: 10002
loginShell: /bin/bash
homeDirectory: /ahome/leia
userPassword: {SSHA}hFGouu+ytfnH0qPy7y9G0L0Rb6R6slZ4
gecos: Leia Organa Skywalker

# Luke Skywalker
dn: uid=luke,ou=people,dc=lab,dc=stri
objectClass: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
cn: Luke
sn: Luke Skywalker
uid: luke
uidNumber: 10003
gidNumber: 10003
loginShell: /bin/bash
homeDirectory: /ahome/luke
userPassword: {SSHA}hFGouu+ytfnH0qPy7y9G0L0Rb6R6slZ4
gecos: Luke Skywalker
EOF
```

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

```
sudo 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"
```

On peut lister à nouveau les entrées contenues dans l'annuaire pour vérifier la présence des utilisateurs.

```
sudo ldapsearch -LLL -x -H ldap:/// -b "dc=lab,dc=stri" \
  -D cn=admin,dc=lab,dc=stri -W
```

4. Configuration de l'accès client au serveur LDAP

Dans cette section, on suppose qu'un annuaire LDAP existe et qu'il contient des utilisateurs. 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.

4.1. Interrogation à distance de l'annuaire LDAP

On reprend ici les requêtes de consultation des entrées de l'annuaire vues dans la Section 3.4, « Composition d'un nouvel annuaire LDAP ». Cette fois-ci les requêtes sont émises depuis un hôte réseau différent du serveur LDAP.

Q20. Quel est le paquet qui fournit, entre autres, la commande de consultation des entrées de l'annuaire ?

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

```
sudo apt -y 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/ldapcompare
/usr/bin/ldapdelete
/usr/bin/ldapexop
/usr/bin/ldapmodify
/usr/bin/ldapmodrdn
/usr/bin/ldappasswd
/usr/bin/ldapsearch
/usr/bin/ldapurl
/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.

Q21. 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 utilise la commande ldapsearch en spécifiant un attribut `uid` particulier.

```
sudo ldapsearch -LLL -H ldap://[2001:678:3fc:64:baad:caff:fefe:7] \
  -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: inetOrgPerson
objectClass: shadowAccount
objectClass: posixAccount
cn: Padme
sn:: UGFkbcOpIEFtaWRhbGEgU2t5d2Fsa2Vy
uid: padme
uidNumber: 10000
gidNumber: 10000
loginShell: /bin/bash
homeDirectory: /ahome/padme
userPassword:: e1NTSEF9aEZHb3V1K3l0Zm5IMHFQeTd5OUcwTDBSYjZSNnNsWjQ=
gecos: Padme Amidala Skywalker
```

Q22. 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.

```
sudo ldappasswd -x -H ldap://[2001:678:3fc:64:baad:caff:fefe:7] \
  -D cn=admin,dc=lab,dc=stri -W -S uid=padme,ou=people,dc=lab,dc=stri
```

```
New password:
Re-enter new password:
Enter LDAP 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.

```
sudo ldapsearch -LLL -H ldap://[2001:678:3fc:64:baad:caff:fefe:7] \
  -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: inetOrgPerson
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:: e1NTSEF9bngwTTlpUi9QYitpaVJTbzNpN0tkejVkSTRJMVpZclM=
```

4.2. 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.

Q23. 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-ldapd`.

```
apt search --names-only ^libnss-
```

```
apt search --names-only ^libnss-ldap
```

```
En train de trier... Fait
Recherche en texte intégral... Fait
libnss-ldapd/testing 0.9.12-4 amd64
  NSS module for using LDAP as a naming service
```

Q24. Quels sont les paquets supplémentaires qui sont ajoutés lors de l'installation des bibliothèques LDAP pour le mécanisme *Name Service Switch* ?

Utiliser les informations fournies par le gestionnaire de paquets pour chaque ajout.

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

```
sudo apt install libnss-ldapd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libpam-ldapd nscd nslcd nslcd-utils
Paquets suggérés :
  kstart
Les NOUVEAUX paquets suivants seront installés :
  libnss-ldapd libpam-ldapd nscd nslcd nslcd-utils
0 mis à jour, 5 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 390 ko dans les archives.
Après cette opération, 971 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

Plusieurs paquets supplémentaires apparaissent :

- `libpam-ldapd` fournit les fonctions PAM nécessaires à l'authentification, aux autorisations et à la gestion de session via un annuaire LDAP.
- `nscd` (*Name Service Cache Daemon*) est un démon qui gère la recherche des mots de passe, des groupes et hôtes des programmes en cours d'exécution, et met en cache le résultat pour une prochaine recherche.
- `nslcd` fournit un autre démon pour la collecte des informations sur les comptes utilisateurs depuis un serveur LDAP.
- `nslcd-utils` fournit des outils pour l'interrogation et la mise à jour des entrées d'annuaire LDAP.

Avertissement

Pour les besoins des travaux pratiques ou de la mise au point de l'authentification via LDAP, il est utile de relancer les services de cache à chaque modification des conditions d'accès à l'annuaire.

```
sudo systemctl restart nslcd
```

```
sudo systemctl restart nscd
```

Q25. 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.

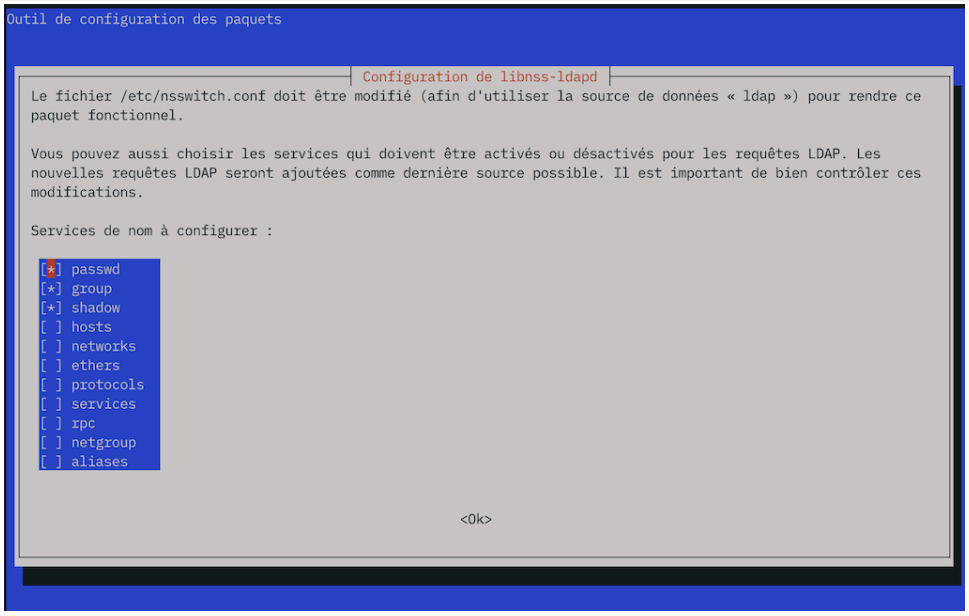
Q26. Quelles sont les principales étapes de la configuration des paquets de bibliothèques NSS et PAM ?

Lors de l'installation des principaux 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.

Avertissement

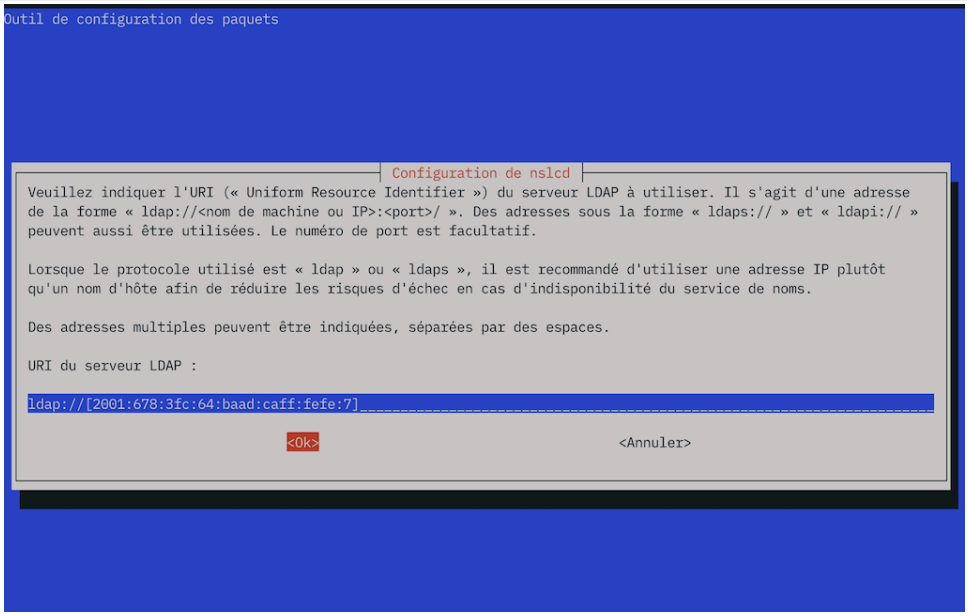
En cas d'erreur de saisie dans la série de menus ci-dessous, il faut reprendre la configuration de chacun des deux paquets individuellement. Classiquement, on passe par la commande dpkg-reconfigure.

```
sudo dpkg-reconfigure libnss-ldapd
```

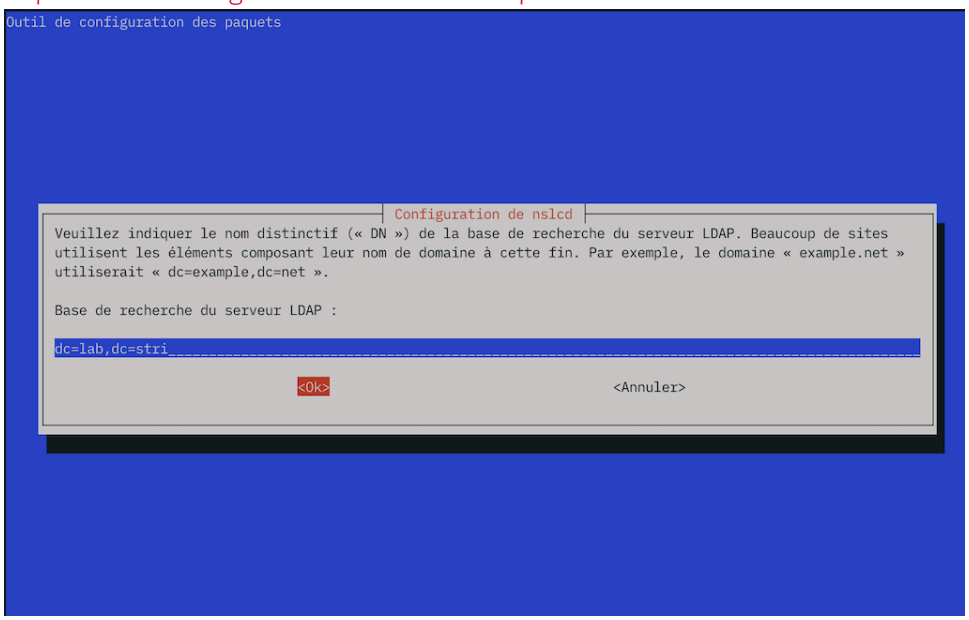


Copie d'écran configuration libnss-ldapd - vue complète

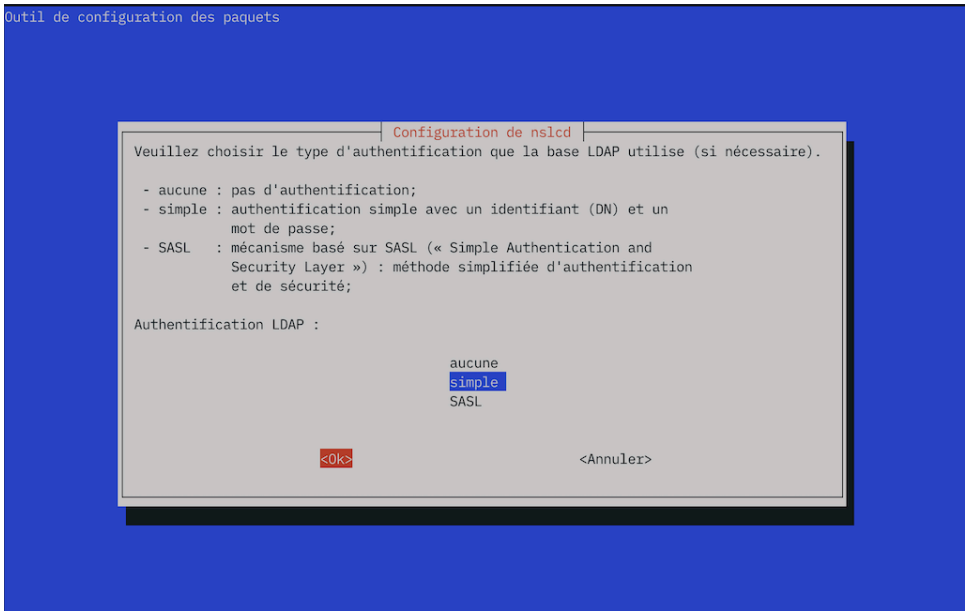
```
sudo dpkg-reconfigure nslcd
```



Copie d'écran configuration nslcd - vue complète

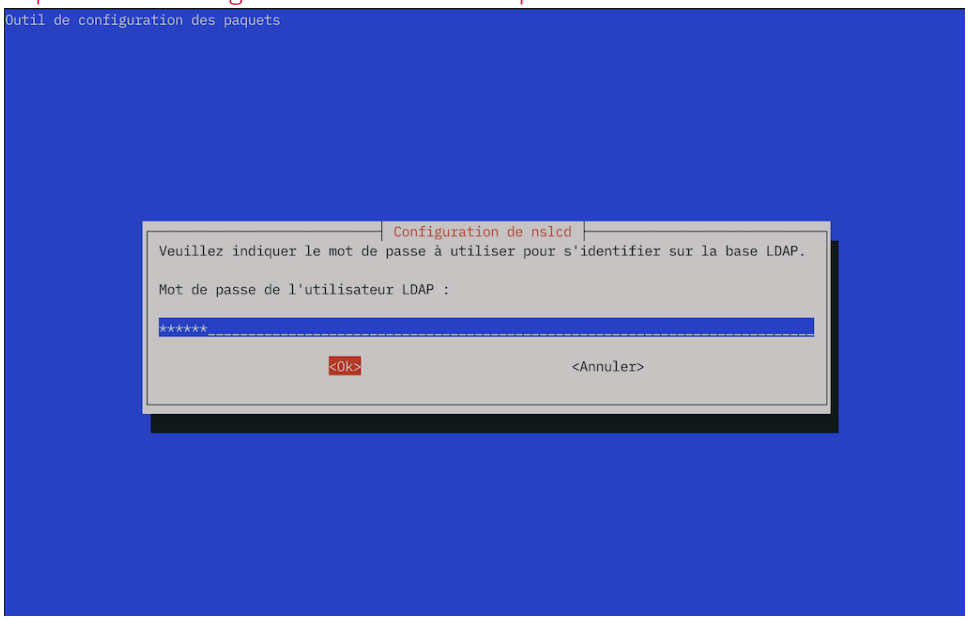


Copie d'écran configuration nslcd - vue complète

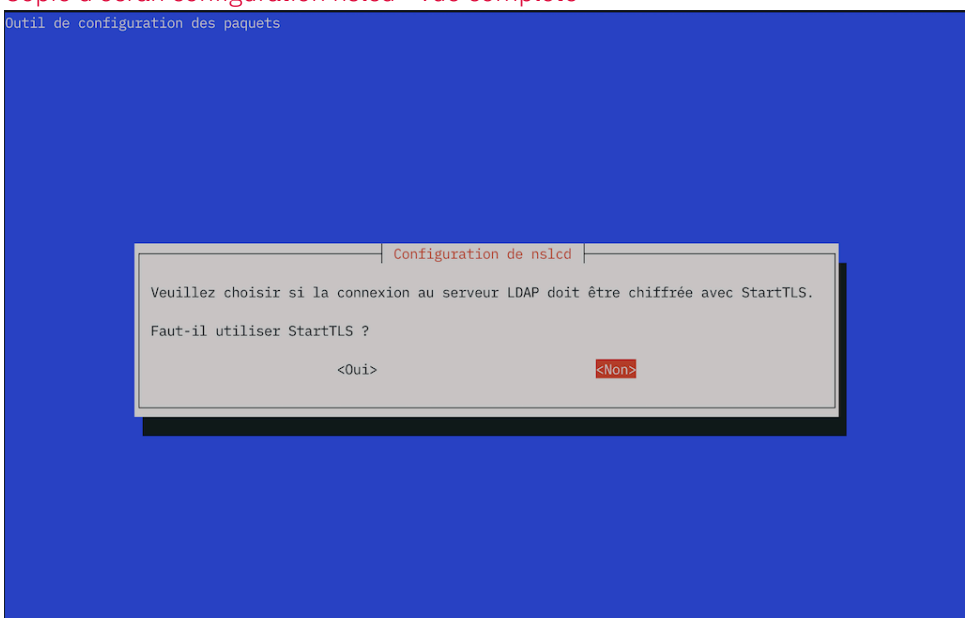


Copie d'écran configuration nslcd - vue complète

Copie d'écran configuration nslcd - vue complète



Copie d'écran configuration nslcd - vue complète



Copie d'écran configuration nslcd - vue complète

Q27. Quelles sont les modifications apportées au fichier de configuration `/etc/nsswitch.conf` pour activer l'accès aux ressources de l'annuaire LDAP ?

Lors de l'installation des paquets à l'étape précédente, le fichier `/etc/nsswitch.conf` a été modifié.

```
grep ldap /etc/nsswitch.conf
passwd:         files systemd ldap
group:          files systemd ldap
shadow:         files systemd ldap
```

Q28. 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`).

```
dpkg -L libc-bin | grep "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:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
etu:x:1000:1000:Etudiant.e,,,:/home/etu:/bin/bash
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
rdnssd:x:102:65534::/var/run/rdnssd:/usr/sbin/nologin
nslcd:x:103:109:nslcd name service LDAP connection daemon,,,:/run/nslcd:/usr/sbin/nologin
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 Skywalker:/ahome/leia:/bin/bash
luke:x:10003:10003:Luke Skywalker:/ahome/luke:/bin/bash
```

Q29. 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.

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

```
su - padme
```

```
Mot de passe :
su: avertissement : impossible de changer le répertoire vers /ahome/padme: Aucun fichier ou dossier de ce type
padme@ldap-client:/home/etu$
```

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

```
journalctl -o cat -n 20 --grep="pam_unix" | grep padme
```

```
pam_unix(su-l:session): session closed for user padme
pam_unix(su-l:session): session opened for user padme(uid=10000) by etu(uid=1000)
pam_unix(su-l:auth): authentication failure; logname=etu uid=1000 euid=0 tty=/dev/pts/0 ruser=etu rhost=  user=padme
pam_unix(su-l:session): session closed for user padme
pam_unix(su-l:session): session opened for user padme(uid=10000) by etu(uid=1000)
pam_unix(su-l:auth): authentication failure; logname=etu uid=1000 euid=0 tty=/dev/pts/0 ruser=etu rhost=  user=padme
```

Voici un autre exemple d'accès avec ssh.

```
ssh padme@localhost
```

```
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:yFLaZk+OfY7z7bHyHPXgjowRS4KMHjfoMQxracRdG9M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ED25519) to the list of known hosts.
padme@localhost's password:
Linux ldap-client 6.4.0-3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.4.11-1 (2023-08-17) 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.
Could not chdir to home directory /ahome/padme: No such file or directory
padme@ldap-client:/$
déconnexion
Connection to localhost closed.
```

```
journalctl -o cat -n 100 -u ssh | grep padme
```

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

5. accès à l'annuaire LDAP depuis un service web

Du point de vue métier, les manipulations à base de fichiers LDIF sont réservées aux traitements en volume réalisés par les administrateurs système. Les développeurs disposent de bibliothèques fournies avec les langages de programmation. Dans la plupart des cas, les développements ont pour but de fournir une interface web.

Le projet *LDAP Tool Box project* propose un outil baptisé ***white pages*** qui permet de constituer un trombinoscope des utilisateurs enregistrés dans un annuaire LDAP.

l'objectif de cette section est d'installer le service web *White Pages* et de compléter les attributs des utilisateurs de l'annuaire avec une photo.

Q30. Quel est le paquet à installer pour mettre en place le service web ***White Pages*** ?

Rechercher sur le site *LDAP Tool Box project*, le lien de téléchargement direct du paquet Debian pour le service ***White Pages***.

À partir du lien `Download` en bas de la page principale, on trouve un lien direct vers le paquet.

Après le téléchargement, l'installation nécessite quelques ajustements compte tenu des dépendances des paquets entre les différentes versions du langage PHP et du ***framework Smarty***.

```
wget https://ltb-project.org/archives/white-pages_0.4-2_all.deb
```

```
sudo dpkg -i white-pages_0.4-2_all.deb
```

```
sudo apt -y -f install
```

```
sudo apt install smarty3
```

Q31. Comment activer l'accès au service web ?

Consulter les fichiers de documentation et de configuration fournis avec le paquet ***apache2***. Repérer les instructions d'activation et de désactivation d'un site. Retrouver les éléments spécifiques à la configuration du service ***White Pages***.

Cette question comprend plusieurs étapes.

1. Le paquet `apache2` comprend une liste d'outils dédiés aux manipulations sur les sites et leur configuration.

```
dpkg -L apache2 | grep "bin.*a2"
/usr/sbin/a2enmod
/usr/sbin/a2query
/usr/sbin/a2disconf
/usr/sbin/a2dismod
/usr/sbin/a2dissite
/usr/sbin/a2enconf
/usr/sbin/a2ensite
```

2. On utilise a2dissite pour désactiver le site par défaut et a2ensite pour activer les pages blanches.

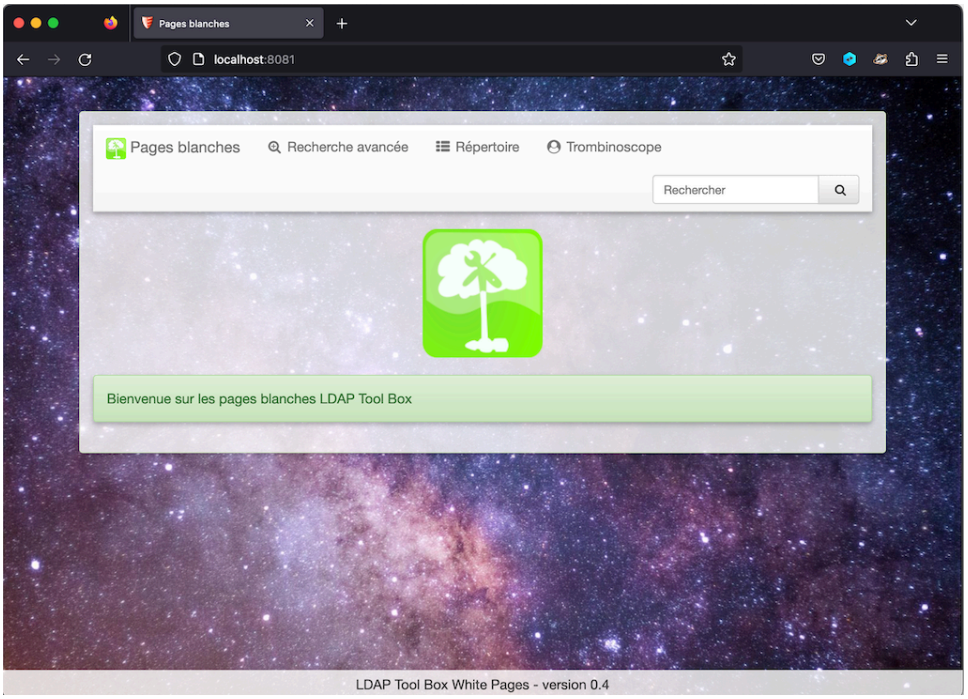
```
sudo a2dissite 000-default
```

```
sudo a2ensite white-pages
```

```
sudo apachectl configtest
```

```
sudo systemctl reload apache2
```

La consultation de la page web donne le résultat suivant.



Copie d'écran service pages blanches - vue complète

3. Les paramètres du nouveau site sont donnés dans le fichier `/etc/apache2/sites-available/white-pages.conf`.

Q32. Comment paramétrer l'accès à l'annuaire LDAP à partir du service web ?

Identifier les fichiers de configuration fournis avec le paquet `white-pages`.

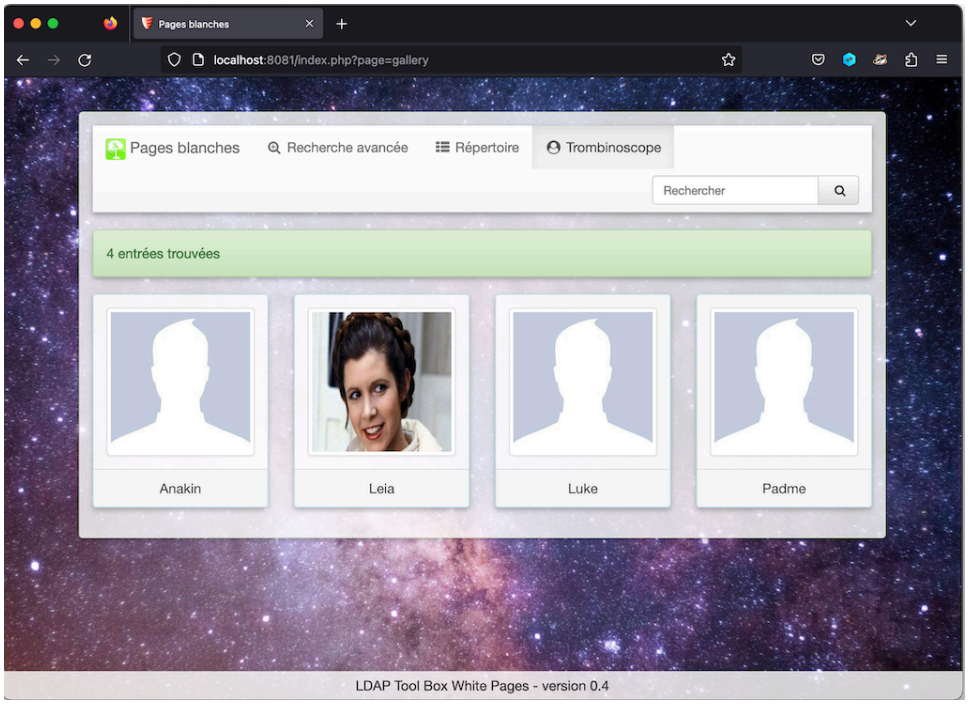
C'est le fichier `/usr/share/white-pages/conf/config.inc.php` qui contient les éléments d'accès à l'annuaire LDAP. Voici un extrait de ce fichier avec les lignes utiles complétées avec le contexte de ce support de travaux pratiques.

```
# grep ^\$ldap /usr/share/white-pages/conf/config.inc.php
$ldap_url = "ldap://localhost";
$ldap_starttls = false;
$ldap_binddn = "cn=admin,dc=lab,dc=stri";
$ldap_bindpw = "xxxxxx";
$ldap_base = "dc=lab,dc=stri";
$ldap_user_base = "ou=people,".$ldap_base;
$ldap_user_filter = "(objectclass=inetorgperson)";
$ldap_size_limit = 100;
```

Une fois le fichier modifié, il faut recharger la configuration du service web.

```
sudo systemctl reload apache2
```

La consultation de la rubrique pages blanches donne le résultat ci-dessous. L'intérêt de cette manipulation est de montrer que l'on peut compléter les attributs d'un utilisateur de l'annuaire avec une photo. Cette opération est l'objet des questions suivantes.



Copie d'écran trombinoscope - vue complète

Q33. Quel est l'attribut de la classe `inetorgperson` qui correspond à une photo d'identité ?

Rechercher les options de la commande ldapsearch qui permettent d'extraire la liste des attributs de la classe `inetorgperson`.

On obtient l'information en deux temps.

- On identifie le contexte de la classe recherchée en premier. Voici un exemple de requête côté serveur.

```
sudo ldapsearch -LLL -Y EXTERNAL -H ldapi:/// \
 -b "cn=config" | grep -i inetorgperson
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn={3}inetorgperson,cn=schema,cn=config
cn: {3}inetorgperson
olcObjectClasses: {0}( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' DESC 'RFC2
```

- Une fois le contexte connu avec précision, on peut extraire la liste des attributs relatifs à la classe `inetorgperson`.

  Dans la liste ci-dessous, on repère l'attribut `jpegphoto` qui correspond à notre besoin.

```
sudo ldapsearch -LLL -Y EXTERNAL -H ldapi:/// \
 -b "cn={3}inetorgperson,cn=schema,cn=config"
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
dn: cn={3}inetorgperson,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: {3}inetorgperson
olcAttributeTypes: {0}( 2.16.840.1.113730.3.1.1 NAME 'carLicense' DESC 'RFC279
 8: vehicle license or registration plate' EQUALITY caseIgnoreMatch SUBSTR cas
 eIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: {1}( 2.16.840.1.113730.3.1.2 NAME 'departmentNumber' DESC '
 RFC2798: identifies a department within an organization' EQUALITY caseIgnoreM
 atch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: {2}( 2.16.840.1.113730.3.1.241 NAME 'displayName' DESC 'RFC
 2798: preferred name to be used when displaying entries' EQUALITY caseIgnoreM
 atch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SI
 NGLE-VALUE )
olcAttributeTypes: {3}( 2.16.840.1.113730.3.1.3 NAME 'employeeNumber' DESC 'RF
 C2798: numerically identifies an employee within an organization' EQUALITY ca
 seIgnoreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.12
 1.1.15 SINGLE-VALUE )
olcAttributeTypes: {4}( 2.16.840.1.113730.3.1.4 NAME 'employeeType' DESC 'RFC2
 798: type of employment for a person' EQUALITY caseIgnoreMatch SUBSTR caseIgn
 oreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
olcAttributeTypes: {5}( 0.9.2342.19200300.100.1.60 NAME 'jpegPhoto' DESC 'RFC2
 798: a JPEG image' SYNTAX 1.3.6.1.4.1.1466.115.121.1.28 )
olcAttributeTypes: {6}( 2.16.840.1.113730.3.1.39 NAME 'preferredLanguage' DESC
  'RFC2798: preferred written or spoken language for a person' EQUALITY caseIg
 noreMatch SUBSTR caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.
 15 SINGLE-VALUE )
olcAttributeTypes: {7}( 2.16.840.1.113730.3.1.40 NAME 'userSMIMECertificate' D
 ESC 'RFC2798: PKCS#7 SignedData used to support S/MIME' SYNTAX 1.3.6.1.4.1.14
 66.115.121.1.5 )
olcAttributeTypes: {8}( 2.16.840.1.113730.3.1.216 NAME 'userPKCS12' DESC 'RFC2
 798: personal identity information, a PKCS #12 PFX' SYNTAX 1.3.6.1.4.1.1466.1
 15.121.1.5 )
olcObjectClasses: {0}( 2.16.840.1.113730.3.2.2 NAME 'inetOrgPerson' DESC 'RFC2
 798: Internet Organizational Person' SUP organizationalPerson STRUCTURAL MAY
 ( audio $ businessCategory $ carLicense $ departmentNumber $ displayName $ em
 ployeeNumber $ employeeType $ givenName $ homePhone $ homePostalAddress $ ini
 tials $ jpegPhoto $ labeledURI $ mail $ manager $ mobile $ o $ pager $ photo
 $ roomNumber $ secretary $ uid $ userCertificate $ x500uniqueIdentifier $ pre
 ferredLanguage $ userSMIMECertificate $ userPKCS12 ) )
```

Q34. Quelle est la syntaxe du fichier LDIF qui permet de modifier l'attribut `jpegphoto` d'un utilisateur de l'annuaire ?

Rechercher un exemple de modification d'attribut avec la commande ldapmodify.

Rechercher aussi un fichier JPEG qui fasse office de photo d'identité.

Tout d'abord, on dépose le fichier jpeg à utiliser dans le dossier `/var/tmp` à titre d'exemple.

```
ls -l /var/tmp/leia.jpg
 -rw-r--r-- 1 etu etu 83837 19 août  03:15 /var/tmp/leia.jpg
```

La syntaxe du fichier LDIF est relativement simple une fois que l'on a bien identifié le contexte.

```
cat > leia-photo.ldif << EOF
dn: uid=leia,ou=people,dc=lab,dc=stri
changetype: modify
add: jpegphoto
jpegphoto:<file:///var/tmp/leia.jpg
EOF
```

Enfin, on applique la modification dans l'annuaire LDAP.

```
sudo ldapmodify -x -H ldap:/// -D "cn=admin,dc=lab,dc=stri" -W -f leia-photo.ldif
```

Le résultat est visible sur la copie d'écran de navigateur web ci-dessus.

6. Sécurisation des échanges avec TLS

Partant d'un service LDAP fonctionnel, nous allons maintenant sécuriser les échanges entre le serveur et ses clients en utilisant la sécurité de couche transport ou *Transport Layer Security* (TLS).

Dans ce but, nous devons installer et configurer une autorité de certification locale dans ce contexte de travaux pratiques.

En "situation réelle", on ferait appel à une autorité de certification tierce publique comme *Let's Encrypt*.

6.1. Génération des certificats avec easyrsa

Cette étape débute par l'installation du paquet `easy-rsa`, l'initialisation d'une nouvelle autorité (CA) et la génération d'un paire de clés.

Une fois le paquet `easy-rsa` installé, toutes les opérations de mise en place de l'autorité de certification se font à partir d'une session administrateur. C'est la raison de la présence de la commande sudo -i ci-dessous.

1. Installation du paquet.

```
sudo apt install easy-rsa
```

2. Création de l'arborescence de l'autorité de certification.

```
sudo -i
make-cadir ldap-pki
cd ldap-pki
```

```
root@ldap-server:~/ldap-pki# ls -lAh
total 20K
lrwxrwxrwx 1 root root   27  6 sept. 18:54 easyrsa -> /usr/share/easy-rsa/easyrsa
-rw-r--r-- 1 root root 5,1K  6 sept. 18:54 openssl-easyrsa.cnf
-rw-r--r-- 1 root root 8,9K  6 sept. 18:54 vars
lrwxrwxrwx 1 root root   30  6 sept. 18:54 x509-types -> /usr/share/easy-rsa/x509-types
```

3. Initialisation du gestionnaire de clés.

```
./easyrsa init-pki
```

4. Construction de l'autorité de certification.

```
./easyrsa build-ca nopass
```

5. Génération des certificats

```
./easyrsa build-server-full ldap.lab.stri nopass
```

7. documents de référence

OpenLDAP software 2.6 administrator's guide

La documentation officielle : *OpenLDAP Software 2.6 Administrator's Guide* constitue le point d'entrée essentiel pour la mise en œuvre du service LDAP.