

Mise en place d'un gestionnaire
d'annuaire :
Open LDAP

Projet de fin d'année

Présenté et soutenu par :

*Douaa Allouchi
Wafae El Mekhyari
Aicha Farouk
Mohamed Reda Ait Cheikh
Oussama Sabri
Oussama El Maazaze*

Sous la direction de :

M. Mounia Zaydi

Année universitaire :

2020/2021

Remerciements

Avant d'aérer ce rapport, on tient tout d'abord à remercier notre professeur Madame Mounia ZAYDI , pour sa disponibilité et ses conseils qui nous ont permis de toujours nous poser des questions et d'avancer dans notre projet d'étude d'une part et en nous laissant autrement une grande autonomie pour mettre en œuvre l'ensemble des compétences acquises tout au long de notre première année au cycle ingénieur , notamment au niveau de l'administration du Système GNU/Linux et du réseau TCP/IP

.

Par la même volonté et la même chaleur, on tient à nous féliciter nous-mêmes pour notre détermination , notre fermeté et pour avoir suivi ce travail dans tous ces détails avec assez de rigueur et d'âpreté.

Glossaire

Entrée En Matière	3
Chapitre 1 : Le protocole LDAP.....	4
I. A propos des annuaires	4
II. A propos du protocole LDAP.....	5
Chapitre II:Présentation du serveur LDAP:OpenLDAP	13
I. Définition de OpenLDAP	13
II. Concept	13
III. Histoire du projet	13
IV. Aspects techniques	14
Chapitre III:Installation et configuration d'OpenLDAP	16
I. Installation	16
II. Configuration	17
Conclusion :	31
Annexes :	32
Références.....	37

L'importance de la donnée en toute organisation est aujourd'hui unanimement reconnue. La data est le moteur des relations, des stratégies et des projets. L'investissement dans les solutions de gestion des données est une évidence pour un grand nombre de personnes.

Dans une entreprise par exemple, il nous serait impossible de garantir l'authentification, les droits d'accès et bien d'autres services sans un ensemble de données préalablement stocké. Ceci oblige de se charger d'une quantité non fixée d'informations, ce qui peut entraîner sic une péremption voire un désordre au niveau de cet organisme.

Le protocole LDAP répond à cette problématique en consolidant les différents types d'informations à l'instar des annuaires et en proposant un service d'administration et d'intendance.

Le concret de ce travail est de mettre en place un annuaire de gestion des utilisateurs, des hôtes et des groupes sous nom 'Open LDAP'.

Pour cela, nous allons dans un premier temps exposer l'utilité et le but de la conception des annuaires et du protocole LDAP, après nous allons exhiber la solution intitulée 'Open LDAP' ainsi que sa configuration sous deux points de vue différents pour clôturer le projet par des tests de fonctionnement et des exemples illustratifs pratiques.

Chapitre 1 : Le protocole LDAP

I. A propos des annuaires

1. Qu'est-ce qu'un annuaire ?

LDAP est le protocole standard permettant d'accéder à **un annuaire** et de le gérer.

Les annuaires sont des bases de données contenant des informations sur des personnes, des groupes d'individus ou des machines formés de couples attribut/valeur. Ils sont couramment employés pour stocker les données d'authentification (login et mot de passe) ou pour obtenir des informations sur des personnes (email, téléphone, etc.) ou des objets (localisation, marque, modèle, etc.)

Ils se distinguent des bases de données relationnelles par le fait qu'ils ont une structure hiérarchique (C'est-à-dire que nous avons une racine et des feuilles) ainsi qu'ils sont rapides au niveau de la recherche et de la lecture des données mais ils sont lents quand on a pour but modifier ces derniers.

Un annuaire permet en général de lister des données, les organiser et les protéger. Il offre un moyen de consultation et est plus consulté que mis à jour ainsi que disponible de manière permanente.

2. Que peut-on faire avec un annuaire LDAP ?

Son principal rôle réside dans la possibilité de consolider certains types d'informations au sein d'une organisation. Il peut être interrogé par toute application compatible LDAP ayant besoin de ces données (applications clientes (Outlook, Netscape...) et applications serveurs (Postfix, Sendmail...)) et peut également être utilisé par des utilisateurs ayant besoin d'informations d'annuaire sous tire d'authentification par un login et un mot de passe.

Il se présente aussi comme annuaire de recherche permettant la recherche de différentes informations jugées bonnes de stocker et ceci selon de multiples critères.

II. A propos du protocole LDAP

1. Introduction

Lightweight Directory Access Protocol (LDAP) est à l'origine un protocole permettant l'interrogation et la modification des services d'annuaire. Il a été évolué pour représenter une norme pour les systèmes d'annuaires, incluant un modèle de données, un modèle de nommage, un modèle fonctionnel, un modèle de sécurité et un modèle de réplication. C'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.

C'est un protocole de la couche Application du modèle OSI. Il est conçu pour fonctionner au-dessus de TCP, lui-même au-dessus d'IP. Par conséquent, les communications avec un annuaire LDAP sont en mode connecté, et les paquets échangés ont une garantie d'intégrité.

2. Origine

Les besoins d'annuaires électroniques sont apparus avec la nécessité de gérer les associations DNS / adresse IP. Il était en effet nécessaire de mettre en place un système permettant d'obtenir l'adresse IP associée à un nom mais également de permettre une répartition de la responsabilité des domaines ; chaque administrateur de domaine doit pouvoir gérer ses propres sous-domaines.

Parallèlement, une première **norme X500** fut créée avec pour objectif d'interconnecter tous les annuaires téléphoniques. Cette norme définissait précisément le protocole de communication entre annuaires et applications mais également la structure des annuaires. Le protocole de communication très riche amenait une optimisation des requêtes ainsi qu'un puissant mécanisme de chaînage de ces requêtes. La richesse de cette norme fut également son principal défaut. Les difficultés d'implémentations ainsi que la complexité de mise en œuvre eurent pour conséquence un non-respect de ces normes par les différents acteurs du marché.

Une évolution a ainsi donné naissance au protocole LDAP. Ce protocole, plus souple, ne définit que l'échange entre les applications et les annuaires et entre les annuaires donnant ainsi une plus grande liberté d'implémentation des serveurs.

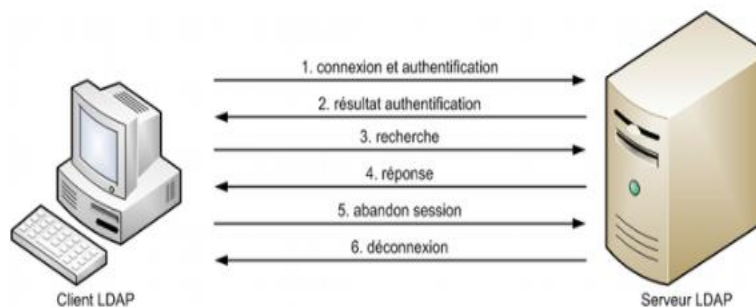
Le protocole fut créé par **Tim Howes** de l'Université du Michigan, **Steve Kille** du ISODE et **Wengyik Yeong** de *Performance Systems International* en **1993**. Les développements qui suivirent, furent menés par l'*Internet Engineering Task Force* (IETF).

Initialement le protocole avait pour nom *Lightweight Directory Browsing Protocol (LDBP)*, car il ne permettait que la recherche de données. Il fut renommé lors de l'ajout de nouvelles possibilités et a obtenu ainsi son nom actuel.

3. Organisation client/serveur

Le principe du client/serveur repose sur une communication d'égal à égal entre les applications ; communication réalisée par dialogue entre processus deux à deux (processus client et processus serveur) ; Les deux processus ne sont certes pas identiques mais forment plutôt un système coopératif se traduisant par un échange de données où le client initie l'échange et réceptionne les résultats délivrés par le serveur, ce dernier est à l'écoute de toute requête éventuelle et son traitement équivaut le service rendu.

Dans le cas de notre étude, un client commence une session LDAP en se connectant sur le port TCP 389 du serveur. Le client envoie ensuite des requêtes d'opération au serveur. Le serveur envoie des réponses en retour. À part quelques exceptions, le client n'a pas besoin d'attendre de réponse du serveur pour envoyer de nouvelles requêtes, et le serveur peut envoyer ses réponses dans n'importe quel ordre.



Source : 'http://igm.univ-mlv.fr/~dr/XPOSE2009/ldap/content/ldap_organization.html'

Les échanges avec le protocole LDAP se font au format ASCII (chaque caractère alphabétique, numérique ou spécial est représenté par un nombre binaire sur 7 bits). En plus des opérations présentées sur l'exemple de communication client/serveur ci-dessus, les opérations de base définies par le protocole LDAP sont :

- Interrogation : search, compare
- Mise à jour : add, delete, modify
- Connexion : bind, unbind, abandon

Etant donné que ces échanges sont réalisés au format ASCII, des mécanismes d'authentification et de chiffrement sont mis en place pour sécuriser le service.

4. Opérations

Le client donne à chaque requête un identifiant *Message ID*, le serveur répond à la requête avec le même identifiant. La réponse inclut un code de résultat numérique indiquant l'état de la requête (succès, échec, ...). La réponse inclut également les données éventuelles qui peuvent résulter d'une recherche. Il inclut aussi un code ID.

Bind (Authentication) : L'opération bind *authentifie le client au sein du serveur*. Cette étape de bind permet également au client et au serveur de se mettre d'accord sur la version du protocole à utiliser. En général la version 3 est utilisée. Il est même possible au serveur de refuser de communiquer avec des clients dans un protocole inférieur au sien

StartTLS : L'opération StartTLS *établit une connexion sécurisée entre le client et le serveur* en utilisant la technique TLS, héritière de SSL. Cette sécurisation opère sur deux points : la confidentialité et l'intégrité des données. Les serveurs prennent en charge généralement le protocole non standard « LDAPS » (LDAP over SSL). Ce protocole utilise le port 636 contrairement au TLS qui utilise le port 389 (le même que le LDAP non sécurisé)

Search et Compare : L'opération *Search* est utilisée à la fois pour *faire une recherche et rapatrier des entrées*. L'opération Compare prend en argument un DN, un nom d'attribut et une valeur d'attribut, puis *vérifie si l'entrée correspondante contient bien un attribut ayant cette valeur*.

Mise à jour : Les opérations de mise à jour **Add** (ajout), **Delete** (suppression), **Modify** (Modification) prennent en argument le DN de l'entrée à mettre à jour.

Il existe de nombreuses autres opérations telles que, Unbind et Abandon

5. Structure d'un annuaire LDAP

L'organisation des entrées en LDAP constitue un arbre appelé **DIT (Directory Information Tree)** dont une des entrées est la racine. Le nommage des éléments constituant cet arbre (racine, branches, feuilles) reflète souvent le modèle de la structure et de la hiérarchie de l'organisation

ou l'entreprise.

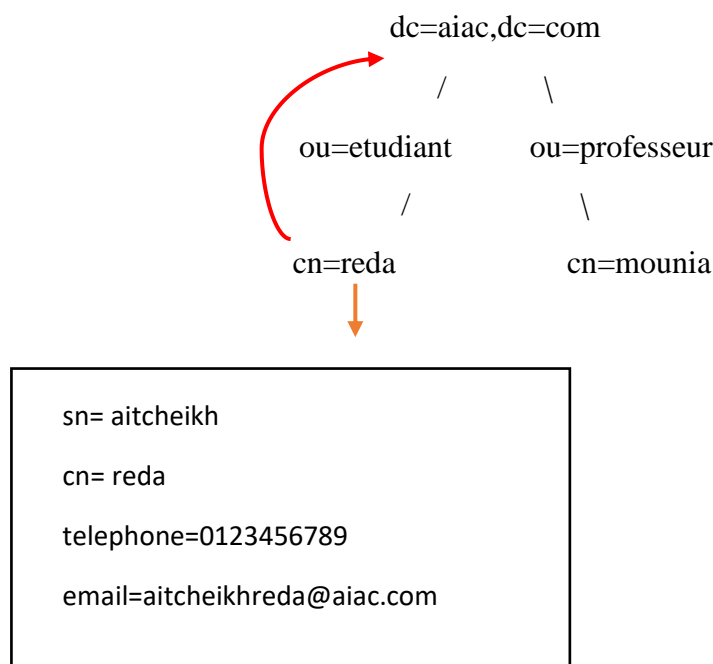
La tendance actuelle est d'utiliser le nommage **DNS (Domain Name System)** qui est utilisé pour la résolution des noms, ce qui permet aux postes clients de localiser les contrôleurs de domaine au sein du système d'information.

Pour les éléments de base de l'annuaire tels que la racine et les premières branches, on opte pour l'attribut '**dc=**' (Domain components). Les branches les plus profondes de l'annuaire peuvent représenter des unités d'organisation ou des groupes '**ou=**' (Organisational unit), des personnes '**cn=**' (Common Name) voire '**uid=**'. (User Identifier).

L'assemblage de tous les composants (allant du plus précis au plus général) d'un nom forme son ***distinguished name*** (nom distinct) ; un attribut qui identifie de manière unique un élément dans le DIT. Il reprend les noms de tous les éléments depuis la racine jusqu'à l'élément et indique ainsi un "chemin" unique pour trouver l'élément.

L'exemple suivant d'un DIT de racine « dc=aiac, dc=com » illustre ceci :

- dn :cn=reda , ou=etudiant , dc=aiac , dc=com
- dn :cn=mounia , ou=professeur, dc=aiac , dc=com



Chaque entrée peut contenir des attributs auxquels on assigne des valeurs et appartient au moins à une classe d'objet qui les définit.

6. Les modèles de LDAP

Le protocole LDAP met en jeu 5 modèles qui définissent son fonctionnement à différents niveaux. Ces 5 modèles sont :

- Un modèle d'information : pour définir le type de données de l'annuaire
- Un modèle de nommage : pour indiquer comment les données sont organisées
- Un modèle fonctionnel : pour indiquer comment accéder aux données
- Un modèle de sécurité : pour indiquer comment protéger l'accès aux données
- Un modèle de duplication : pour indiquer comment répartir les données entre serveurs

6.1. Le modèle d'information :

LDAP permet de gérer des données. Ces données utilisent un modèle particulier pour être stockées. Dans ce modèle, l'élément de base est appelé "Entry".

Une entrée (entry) est un élément de base de l'annuaire. C'est lui qui contient les données. C'est l'équivalent en programmation orientée objet d'une "classe d'objet". Une entrée regroupe un ensemble d'attribut contenant les différentes informations relatives à l'entrée.

Client	
Type d'attribut	Valeur d'attribut
cn :	Oussama Sabri
uid :	Osabri
Telephone	0123456789
Mail	Oussama.Sabri@gmail.com
Solde	1000000

Sur l'exemple ci-dessus, on a une entrée de type "Client" qui contient plusieurs arguments avec les différentes informations sur le client.

Un attribut est caractérisé par un nom, un type, une méthode de comparaison, un « Object Identifier » (IOD) et une valeur.

6.2. Le modèle de nommage

Une fois le modèle d'information défini, il faut pouvoir définir la manière dont sont référencées les différentes informations gérées par les services LDAP. C'est le rôle du modèle de nommage. Il définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées.

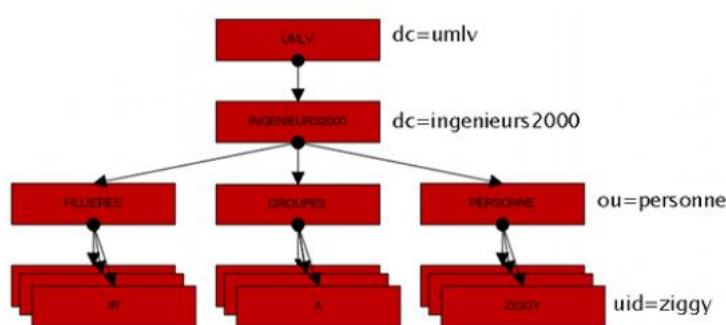
Cette organisation est représentée par le Directory Information Tree (DIT). C'est une classification comparable au système de fichier UNIX.

Chaque nœud du DIT correspond à une entrée de l'annuaire. Au sommet se trouve l'entrée "Suffix" ou "Root Entry". Cette dernière correspond à l'espace de nommage géré par le serveur LDAP. Il faut savoir qu'un serveur LDAP peut gérer plusieurs arbres donc plusieurs "Root Entry".

Pour référencer de manière unique une entrée contenue dans le DIT, on utilise un "Distinguish Name" (DN). Ce dernier est équivalent à un path d'un fichier UNIX. Chaque élément qui compose le DN est appelé "Relative Distinguish Name" (RDN).

Un DN est constitué d'un ensemble d'attribut et de leurs valeurs provenant de chacune des entrées parentes mises bout à bout. Voici un exemple de DN pour l'entrée Ziggy :

DN de l'entrée ziggy = [uid=ziggy, ou=personne, dc=ingenieurs2000, dc = umlv]



Source : 'http://igm.univ-mlv.fr/~dr/XPOSE2009/ldap/content/ldap_model.html'

6.3. Le modèle de fonctionnement

Une fois les données stockées et référencées, il faut permettre d'utiliser ces données. Pour cela, LDAP définit un modèle de fonctionnement. Ainsi, ce modèle définit les opérations possibles sur les données. On distingue 4 types d'opérations :

- Opérations d'interrogation : requête pour accéder aux données
- Opérations de comparaison : renvoie vrai ou faux si égal
- Opérations de mise à jour : add, delete, rename, modify
- Opérations d'authentification et de contrôle : bind, unbind, abandon

6.4. Le modèle de sécurité

Le modèle de sécurité permet de protéger l'accès aux données de l'annuaire. La sécurité se fait à plusieurs niveaux. Au niveau de l'authentification pour se connecter au service, par des règles d'accès aux données et par le chiffrement des communications.

Pour l'authentification, LDAPv3 propose plusieurs choix :

- Anonymous authentication : accès sans authentification
- Root DN authentication : accès administrateur
- Mot de passe + SSL ou TLS : accès chiffré
- Certificats sur SSL : échange clé publique/privée

Pour le contrôle d'accès, c'est un fonctionnement similaire à la gestion des droits des système UNIX. Un utilisateur peut avoir des droits d'accès en lecture, écriture, recherche, comparaison). Et pour le chiffrement des communications, il est possible d'utiliser des algorithmes de cryptage comme TLS.

6.5. Le modèle de duplication

Le protocole LDAP offre des facilités pour dupliquer ou synchroniser les données entre plusieurs serveurs ldap. Pour réaliser cela, il définit un modèle de duplication. Ce dernier définit comment échanger les informations d'un serveur à l'autre.

L'intérêt de dupliquer un serveur est par exemple de pallier une panne de l'un des serveurs, ou d'une coupure réseaux. Mais aussi pour répartir la charge du service et garantir une qualité de service.

Cependant ce modèle n'est pas encore standardisé. IETF est en préparation du protocole LDUP (Lightweight Directory Update Protocol) pour résoudre ce problème.

7. Utilisation

L'intérêt principal de LDAP est la **normalisation de l'authentification**. Il est très facile de programmer un module d'authentification utilisant LDAP à partir d'un langage possédant une API LDAP. C'est l'opération Bind qui permet d'authentifier un utilisateur. De plus en plus d'applications Web possèdent un module d'authentification prenant en charge LDAP.

Sur les systèmes GNU/Linux récents, on voit de plus en plus l'adoption d'une base de données utilisant LDAP à la place des fichiers à plat passwd et shadow. Les données peuvent être accédées par les modules PAM et NSS.

8. Quelques serveurs LDAP

- Apache Directory Server : projet libre de la fondation Apache
- 389 Directory Server ou Fedora Directory Server
- OpenLDAP
- Mandriva Directory Server offre une interface web pour administrer Samba et LDAP : annuaire d'entreprise et contrôleur de domaine basé sur le couple Samba/OpenLDAP, conçu pour gérer les utilisateurs, les contrôles d'accès, règles et paramètres des applications et profils d'utilisateurs

9. Quelques Clients LDAP

- Jxplorer (en) : un client développé sous Java, multiplateforme
- Apache Directory Server : un client multiplateforme, développé en Java, par Apache Software Foundation
- PhpLDAPadmin : un client Web multiplateforme sous licence GPL développé en PHP permettant de gérer son annuaire LDAP.
- FusionDirectory4 : une application web sous licence GPL développée en PHP permettant de gérer son annuaire LDAP et tous les services associés.

Chapitre II : Présentation du serveur LDAP : OpenLDAP

I. Définition de OpenLDAP

OpenLDAP est une **implémentation libre du protocole LDAP** écrit en C et C ++, maintenue par le projet OpenLDAP et distribuée selon les termes de la licence OpenLDAP.

C'est une solution multiplateforme, on trouve des versions compilées pour GNU/Linux, FreeBSD, NetBSD, OpenBSD, AIX, HP-UX, Mac OS X, Solaris, et Microsoft Windows (2000, XP).



Source : '<https://www.logiciel-libre.org/s/open-ldap/>'

II. Concept

OpenLDAP est un annuaire informatique qui fonctionne sur le modèle client/serveur. Il contient des informations de n'importe quelle nature qui sont rangées de manière hiérarchique.

En pratique, dans un réseau informatique, il est utilisé pour enregistrer une grande quantité d'utilisateurs ou de services, parfois des centaines de milliers. Il permet d'organiser hiérarchiquement les utilisateurs par département, par lieu géographique ou par n'importe quel autre critère. C'est une alternative libre à Microsoft Active Directory.

III. Histoire du projet

Le projet a débuté en **1998** sous l'impulsion de **Kurt Zeilenga** en prenant pour base les travaux de l'université du Michigan où les chercheurs développaient le protocole LDAP.

Parmi d'autres contributeurs, on peut citer **Howard Chu** et **Pierangelo Masarati**

IV. Aspects techniques

1. Stockage

Le logiciel OpenLDAP ne stocke pas les données directement, il utilise une bibliothèque tierce pour le faire. Généralement c'est la base donnée Berkeley DB qui est utilisée sous GNU/Linux. Mais il est possible d'utiliser MySQL, LDBM, des fichiers à plat, etc.

2. Réplication

OpenLDAP prend en charge le mécanisme de réplication, via une directive de configuration *Syncrepl*.

3. Composants d'OpenLDAP

OpenLDAP est constitué de 3 éléments principaux :

- ✚ **slapd** (Stand-alone LDAP Daemon): démon LDAP autonome. Il écoute les connexions LDAP sur n'importe quel port (389 par défaut) et répond aux opérations LDAP qu'il reçoit via ces connexions. Typiquement, slapd est appelé au moment du boot.
- ✚ Des **bibliothèques** implémentant le protocole LDAP.
- ✚ Des **utilitaires**, des outils et des exemples de clients

Le projet OpenLDAP propose également des bibliothèques en Java :

- ✚ JDBC-LDAP driver faisant office de pont JDBC-LDAP
- ✚ JLDAP : bibliothèque d'accès à LDAP en Java

4. Composants tiers

- ✚ **Fusion Directory** est une application web sous licence GPL développée en PHP permettant de gérer facilement son annuaire LDAP et tous les services associés.
- ✚ **Apache Directory Studio** est une interface en Java basée sur Eclipse. Permet de gérer l'architecture LDAP, les Schéma LDAP et les fichiers LDIF.
- ✚ **PhpLDAPadmin** est une interface en PHP qui facilite l'édition des données du serveur OpenLDAP. Son utilisation passe par un navigateur Web.

5. Principales versions

Les versions d'OpenLDAP qui ont été marquantes sont :

- ✚ OpenLDAP Version 1 (1998) : première version publique
- ✚ OpenLDAP Version 2 (août 2000) : prise en charge de LDAPv3, d'IPv6, du TLS...
- ✚ OpenLDAP Version 2.1 (juin 2001)
- ✚ OpenLDAP Version 2.2 (décembre 2003)
- ✚ OpenLDAP Version 2.3 (juin 2005) : possibilité d'avoir la configuration accessible dans l'annuaire (cn=config)
- ✚ OpenLDAP Version 2.4 (octobre 2007) : réplication miroir et multi-maitre ; réplication Proxy Sync ; extensions LDAP v3

Chapitre III : Installation et configuration d'OpenLDAP

I. Installation

➔ Etape1 : Changer le nom de notre machine

*On se connecte en tant que root via la commande « sudo su »

```
aicha@aicha-VM:~$ su root
Mot de passe :
root@aicha-VM:/home/aicha# cd
root@aicha-VM:~#
```

*Par la suite, on change le nom de notre machine. Pour cela, on édite le fichier /etc/hostname avec l'éditeur nano

```
root@aicha-VM:~# nano /etc/hostname
```

Puis on tape le nouveau nom « server.ldap.com »

```
GNU nano 4.8 /etc/hostname
server.ldap.com
```

*On enregistre et puis on redémarre notre machine avec la commande « init 6 »

```
root@aicha-VM:~# init 6
```

➔ Etape2 : Installer les paquets nécessaires

OpenLDAP est l'un des annuaires les plus répandus et les plus utilisés au niveau des entreprises. Pour l'installer on doit installer le paquet « *slapd* », et également on installe le paquet « *ldap-utils* » qui contient les utilitaires client qui nous permettra par la suite de modifier et interroger notre annuaire.

**L'installation se fait avec la commande :

```
# apt-get install slapd ldap-utils
```

```

root@server:~# apt-get install slapd ldap-utils
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libodbc1
Paquets suggérés :
  libssl2-modules-gssapi-mit | libssl2-modules-gssapi-heimdal libmyodbc
  odbc-postgresql tdsodbc unixodbc-bin
Les NOUVEAUX paquets suivants seront installés :
  ldap-utils libodbc1 slapd
0 mis à jour, 3 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 189 ko/1,708 ko dans les archives.
Après cette opération, 17.7 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://gh.archive.ubuntu.com/ubuntu focal/main amd64 libodbc1 a
md64 2.3.6-0.1build1 [189 kB]
189 ko réceptionnés en 10s (19.9 ko/s)
Préconfiguration des paquets...
Sélection du paquet libodbc1:amd64 précédemment désélectionné.
(Lecture de la base de données... 188977 fichiers et répertoires déjà installés
.)
Préparation du dépaquetage de .../libodbc1_2.3.6-0.1build1_amd64.deb ...
Dépaquetage de libodbc1:amd64 (2.3.6-0.1build1) ...

```

Remarque : À l'installation de slapd, un mot de passe de l'administrateur de l'annuaire est demandé. Pas besoin de le rentrer car on va refaire cette opération dans l'étape de configuration.

II. Configuration

➔ Configuration de Open LDAP sur la machine serveur :

➔Étape 1 : Configuration du fichier /etc/ldap/ldap.conf

**on se connecte en tant que root et on édite le fichier /etc/ldap/ldap.conf avec l'éditeur nano et on définit LA BASE et URI de notre annuaire comme la montre la capture qui suit :

#nano /etc/ldap/ldap.conf

```

root@server:~# nano /etc/ldap/ldap.conf

```

**on modifie notre fichier de la manière suivante :

```
GNU nano 4.8 /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=aiac-gi17,dc=com
URI      ldap://192.168.1.102:389

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
```

- ⇒ BASE : est la racine ; le nom du domaine donné à notre annuaire, ici est « dc=aiac-gi17, dc=com »
- ⇒ URI : on indique l'URI qu'on veut utiliser pour se connecter, ici on indique « URI ldap://localhost :389 », on remplace localhost par l'adresse IP (qu'on peut trouver par la commande ifconfig) de la machine serveur, c'est-à-dire de la machine sur laquelle on a installé OpenLDAP, et 389 est le port TCP utilisé ; ça veut dire simplement que la connexion à notre serveur va être local et pas en passant par un réseau.

****on enregistre et on quitte l'éditeur.**

→ *Etape 2 : Configuration du service slapd*

****Par la suite on va définir la configuration de base de notre annuaire en utilisant l'outil debconf de debian.**

La configuration de base se fait par la commande :

dpkg-reconfigure slapd

```
root@server:~# dpkg-reconfigure slapd
```

On aura besoin d'indiquer les éléments suivants :

- Non pour la 1^{ère} question afin de ne pas omettre la configuration openLDAP.
- Pour leDN on choisit : aiac-gi17.com
- Pour le nom d'organisation : aiac-gi17
- Le mot de passe administrateur de openLDAP deux fois
- Non pour la 6^{ème} question pour ne pas supprimer la base de données à la purge du paquet
- Oui pour la 7^{ème} question pour déplacer l'ancienne base de données

**pour vérifier notre configuration de base on utilise la commande « ldapsearch -x » ; comme l'indique son nom il sert à chercher dans un données annuaire openLDAP.

**la capture suivante montre le résultat :

```
root@server:~# ldapsearch -x
# extended LDIF
#
# LDAPv3
# base <dc=aiac-gi17,dc=com> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# aiac-gi17.com
dn: dc=aiac-gi17,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: aiac-gi17
dc: aiac-gi17

# admin, aiac-gi17.com
dn: cn=admin,dc=aiac-gi17,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

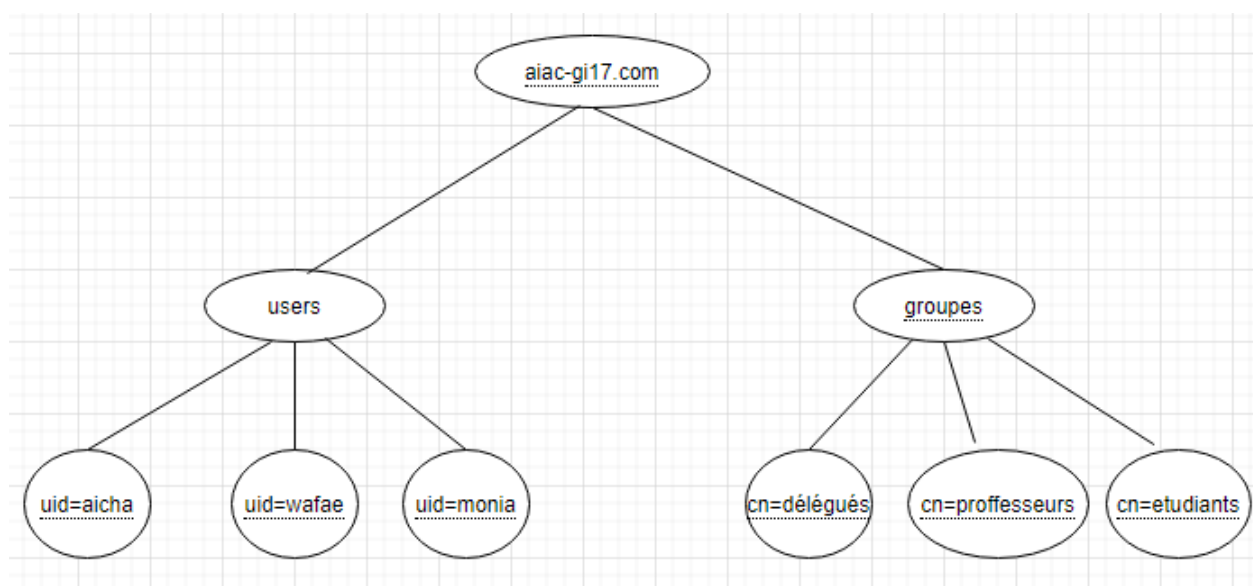
- ⇒ Notre annuaire contient que 2 entrées : la base (racine), et l'admin
 - ⇒ Donc la configuration faite est correcte.
-

→ Peuplement de l'annuaire OpenLDAP :

**Dans la partie précédente on a bien installé et configuré notre annuaire openLDAP, et maintenant on va le peupler par créer les nœuds de la DIT (directory information Tree).

**pour le faire on utilise des fichiers LDIF (LDAP data interchange format), car les données à ajouter à l'annuaire peuvent être inscrites dans un fichier rédigé au format LDIF. Ce format présente les objets à manipuler dans l'annuaire accompagnés de leurs attributs.

**on considère l'arborescence suivante, qu'on va respecter pour peupler notre annuaire :



→ Etape1 : ajouter les ou (organizational units) à notre annuaire

** Pour faire cela, on crée le fichier ou. Ldif avec la commande :

#vim ou.ldif

```
root@server:~# vim ou.ldif
```

**une fois le fichier est créé on le remplit comme la montre la capture suivante :

```
#entrée1 : ou=users,dc=aiac-gi17,dc=com
dn: ou=users,dc=aiac-gi17,dc=com
objectclass: organizationalUnit
ou: users

#entrée2 : ou=groupes,dc=aiac-gi17,dc=com
dn: ou=groupes,dc=aiac-gi17,dc=com
objectclass: organizationalUnit
ou: groupes

~
```

→ Nous avons deux OU : **users** (qui va contenir les comptes UNIX) et **groupes** (qui va contenir les groupes UNIX). Le **dn** (distinguished name) qui positionne sans ambiguïté et d'une façon unique l'objet dans l'arbre (ici juste sous la racine) et l'**objectclass** qui indique que l'objet à ajouter est de type **OrganizationalUnit**. Les **objectclass** sont définis dans les schémas et un objet de l'annuaire peut appartenir à plusieurs **objectclass**.

**On enregistre puis on quitte l'éditeur

**pour ajouter le contenu de ce fichier à notre annuaire on utilise la commande « ldapadd »

**la commande complète est la suivante :

#ldapadd -x -W -D"cn=admin, dc=aiac-gi17, dc=com" -f ou.ldif

```
root@server:~# ldapadd -x -W -D "cn=admin,dc=aiac-gi17,dc=com" -f ou.ldif
```

⇒ Le mot de passe admin de openLDAP sera demandé ,donc on l'entre correctement pour confirmer l'ajout.

⇒ Les options utilisées :

- x : ne pas utiliser SASL (simple authentication and security layer)
- W : s'authentifier par un mot de passe
- D : déterminer le login avec qui on veut executer la commande ;ici on l'exécute en tant qu'admin
- f : déterminer le fichier ldif à ajouter ; ici « ou.ldif »

**lorsqu'on exécute la commande on a le résultat suivant :

```
root@server: ~  
root@server:~# ldapadd -x -W -D "cn=admin,dc=aiac-gi17,dc=com" -f ou.ldif  
Enter LDAP Password:  
adding new entry "ou=users,dc=aiac-gi17,dc=com"  
  
adding new entry "ou=groupes,dc=aiac-gi17,dc=com"  
  
root@server:~#
```

⇒ Les 2 entrées sont ajoutées

→ Etape2: ajouter les nœuds de 2^{ème} niveau à notre annuaire

**maintenant on va ajouter les autres nœuds de 2^{ème} niveau , pour le faire on va créer les deux fichiers « users.ldif » et « groupes.ldif » qui contiennent respectivement les information des utilisateurs et groupes de notre système.

**On utilise l'éditeur vim :

```
root@server:~# vim groupes.ldif
```

**on remplit nos fichiers par les informations nécessaires comme le montre les captures suivantes :

```
root@server: ~  
#groupe1 :  
dn: cn=etudiants,ou=groupes,dc=aiac-gi17,dc=com  
objectclass: posixGroup  
objectclass: top  
gidnumber: 1010  
cn: etudiants  
  
#groupe2 :  
dn: cn=professeurs,ou=groupes,dc=aiac-gi17,dc=com  
objectclass: posixGroup  
objectclass: top  
gidnumber: 1020  
cn: professeurs  
  
#groupe3 :  
dn: cn=delegués,ou=groupes,dc=aiac-gi17,dc=com  
objectclass: posixGroup  
objectclass: top  
gidnumber: 1030  
cn: delegués  
~  
~  
~
```

```
GNU nano 4.8  
#user1 :  
dn: uid=aichafarouk,ou=users,dc=aiac-gi17,dc=com  
uid: aichafarouk  
sn: farouk  
homedirectory: /home/aicha  
cn: farouk  
objectclass: posixAccount  
objectclass: inetOrgPerson  
objectclass: top  
loginshell: /bin/bash  
uidnumber: 1001  
gidnumber: 1010  
mail: aichafarouk@gmail.com  
employeenumber: 0655211447  
userpassword: password1  
  
#user2 :  
dn: uid=wafaelmekhyari,ou=users,dc=aiac-gi17,dc=com  
uid: wafaelmekhyari  
sn: elmekhyari  
homedirectory: /home/wafae  
cn: elmekhyari  
objectclass: posixAccount  
objectclass: inetOrgPerson  
objectclass: top  
loginshell: /bin/bash  
uidnumber: 1002  
gidnumber: 1010  
mail: wafaelmekhyari@gmail.com  
employeenumber: 0647896324  
userpassword: password2
```



```
#user3 :
dn: uid=moniazaydi,ou=users,dc=aiac-gi17,dc=com
uid: moniazaydi
sn: zaydi
homedirectory: /home/monia
cn: zaydi
objectclass: posixAccount
objectclass: inetOrgPerson
objectclass: top
loginshell: /bin/bash
uidnumber: 1003
```

⇒ On note que pratiquement ,les informations de l'annuaire coïncident avec les informations qu'on trouve dans les fichiers /etc/passwd et /etc/group

**lorsque' on remplit les fichiers, on utilise la commande précédente « *ldapadd* » pour ajouter leurs données dans l'annuaire :

```
root@server:~# ldapadd -x -W -D "cn=admin,dc=aiac-gi17,dc=com" -f groupes.ldif
Enter LDAP Password:
adding new entry "cn=etudiants,ou=groupes,dc=aiac-gi17,dc=com"

adding new entry "cn=professeurs,ou=groupes,dc=aiac-gi17,dc=com"

adding new entry "cn=delegués,ou=groupes,dc=aiac-gi17,dc=com"
```

```
root@server:~# ldapadd -x -W -D "cn=admin,dc=aiac-gi17,dc=com" -f users.ldif
Enter LDAP Password:
adding new entry "uid=aicha farouk,ou=users,dc=aiac-gi17,dc=com"

adding new entry "uid=wafae elmekhyari,ou=users,dc=aiac-gi17,dc=com"

adding new entry "uid=monia zaydi,ou=users,dc=aiac-gi17,dc=com"
```

Autre Outils :

**On peut utiliser l'application *phpldapadmin* sous linux qui est une interface basée sur le web pour administrer notre serveur LDAP (ajouter ,interroger ,modifier ,supprimer) sans avoir à utiliser le terminal.

➔Installation :

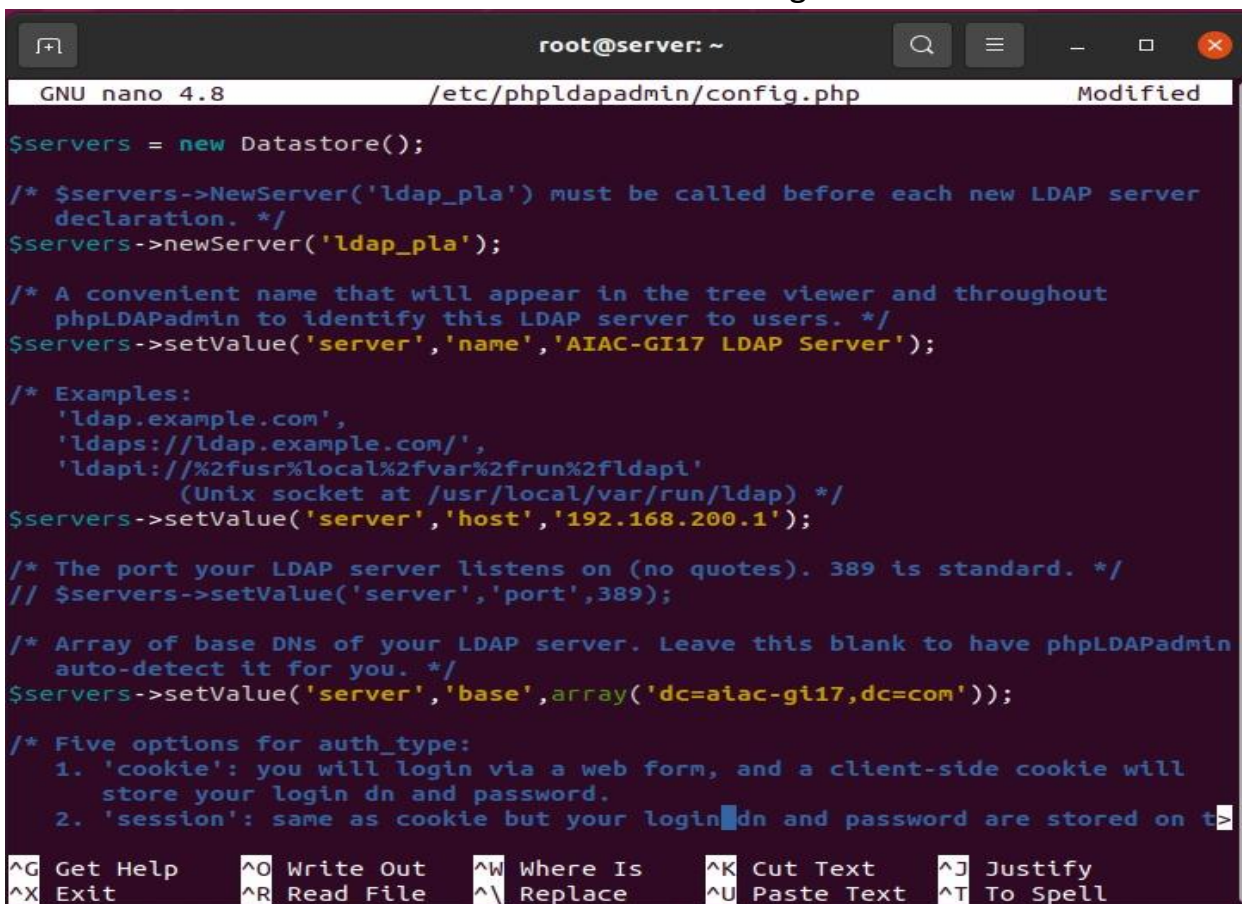
**pour le faire on installe le paquet « phpldapadmin »

```
root@server:~# apt-get install phpldapadmin
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
 chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi
 libgstreamer-plugins-bad1.0-0 libva-wayland2 linux-headers-5.8.0-43-generic
 linux-hwe-5.8-headers-5.8.0-43 linux-image-5.8.0-43-generic
 linux-modules-5.8.0-43-generic linux-modules-extra-5.8.0-43-generic
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
 apache2 apache2-bin apache2-data apache2-utils libapache2-mod-php7.4
 libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
```

➔Configuration :

**la configuration se fait au niveau du fichier `/etc/phpldapadmin/config.php`

**Donc on l'édite avec nano et on effectue les changements suivants :



```
GNU nano 4.8 /etc/phpldapadmin/config.php Modified

$servers = new Datastore();

/* $servers->NewServer('ldap_pla') must be called before each new LDAP server
   declaration. */
$servers->newServer('ldap_pla');

/* A convenient name that will appear in the tree viewer and throughout
   phpLDAPadmin to identify this LDAP server to users. */
$servers->setValue('server','name','AIAC-GI17 LDAP Server');

/* Examples:
   'ldap.example.com',
   'ldaps://ldap.example.com/',
   'ldapi://%2fusr%2flocal%2fvar%2frun%2fldapi'
   (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','192.168.200.1');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DNS of your LDAP server. Leave this blank to have phpLDAPadmin
   auto-detect it for you. */
$servers->setValue('server','base',array('dc=aiac-gi17,dc=com'));

/* Five options for auth_type:
   1. 'cookie': you will login via a web form, and a client-side cookie will
      store your login dn and password.
   2. 'session': same as cookie but your login dn and password are stored on t>
```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell

- ⇒ On ajoute le nom de notre serveur qui va être écrit sur l'interface, là on choisit « AIAC-GI17 LDAP server »
- ⇒ On ajoute l'@ ip de notre serveur qui est ici : 192.168.200.1
- ⇒ On ajoute le domaine name (DN) qui est « dc=aiac-gi17,dc=com »

```
binds. */
$servers->setValue('login','bind_id','cn=admin,dc=aiac-gi17,dc=com');
# $servers->setValue('login','bind_id','cn=Manager,dc=exemple,dc=com');
```

- ⇒ On ajoute le compte admin qui est « cn=admin,dc=aiac-gi17,dc=com »

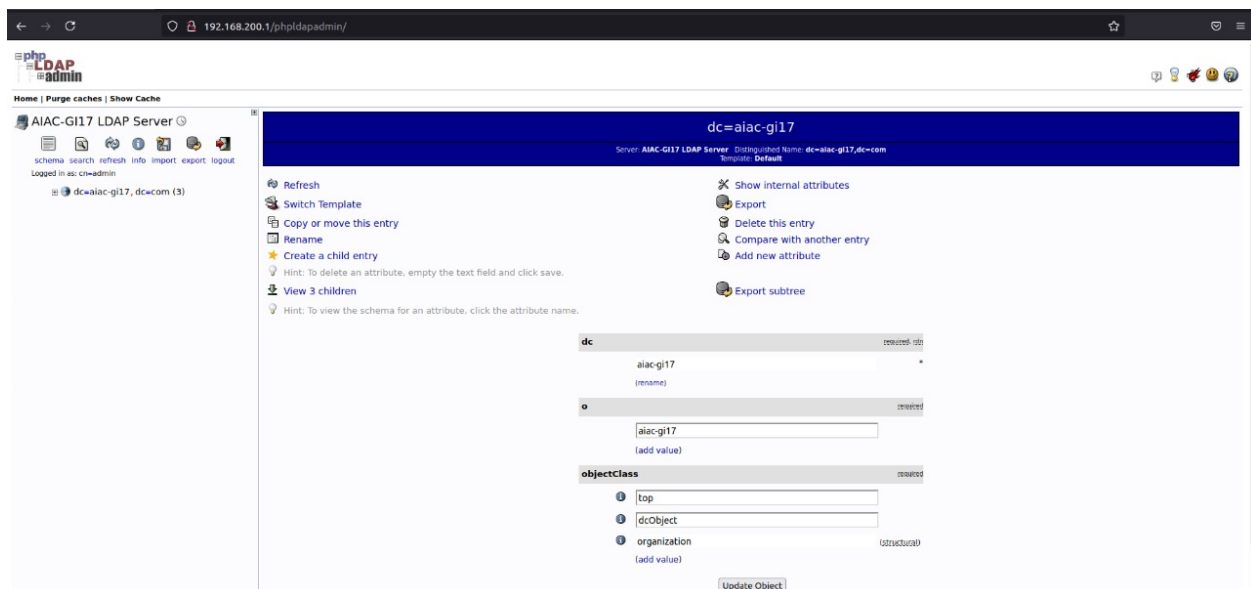
```
/* Hide the warnings for invalid objectClasses/attributes in templates. */
$config->custom->appearance['hide_template_warning'] = true;

/* Set to true if you would like to hide header and footer parts. */
```

- ⇒ On change la valeur de la ligne ci-dessus de false à true

****donc la configuration est faite on ouvre notre navigateur et on tape :**

192.168.200.1/PhpLDAPAdmin et on aura à s'authentifier avec le mot de passe LDAPAdmin :



****donc on peut administrer notre LDAP via cette interface et faire ce qu'on veut (ajouter,chercher,supprimer,modifier).**

→ Configuration de la machine client :

Pour une raison de simplification de la gestion des comptes dans une entreprise, on propose de configurer les postes clients pour autoriser la connexion des utilisateurs connus dans l'annuaire LDAP du serveur.

*Etape1 :installer les paquets nécessaires

** pour configurer une machine client on doit tout d'abord installer le paquet *ldap-utils* qui contient les commandes pour interroger l'annuaire à savoir *ldapsearch* , ensuite le paquet ***ldap-auth-client*** qui contient les fichiers de configuration client ,et aussi le paquet ***nscd*** qui 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 .

****On utilise la commande : # apt-get install ldap-auth-client nscd ldap-utils**

```
root@ubuntu:~# apt-get install ldap-auth-client nscd ldap-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ldap-auth-config libpam-ldap
Suggested packages:
  libsasl2-modules-gssapi-mit | libsasl2-modules-gssapi-heimdal
The following NEW packages will be installed:
  ldap-auth-client ldap-auth-config ldap-utils libpam-ldap nscd
0 upgraded, 5 newly installed, 0 to remove and 255 not upgraded.
Need to get 0 B/247 kB of archives.
After this operation, 1,399 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Preconfiguring packages ...
Selecting previously unselected package ldap-utils.
(Reading database ... 145018 files and directories currently installed.)
Preparing to unpack .../ldap-utils_2.4.49+dfsg-2ubuntu1.8_amd64.deb ...
Unpacking ldap-utils (2.4.49+dfsg-2ubuntu1.8) ...
Selecting previously unselected package nscd.
Preparing to unpack .../nscd_2.31-0ubuntu9.2_amd64.deb ...
Unpacking nscd (2.31-0ubuntu9.2) ...
Selecting previously unselected package ldap-auth-config.
Preparing to unpack .../ldap-auth-config_0.5.4_all.deb ...
Unpacking ldap-auth-config (0.5.4) ...
Selecting previously unselected package libpam-ldap:amd64.
Preparing to unpack .../libpam-ldap_186-4ubuntu1_amd64.deb ...
Unpacking libpam-ldap:amd64 (186-4ubuntu1) ...
Selecting previously unselected package ldap-auth-client.
```

**pendant cette installation on sera amené à répondre aux questions de configuration qui sont comme suit (dans l'ordre) :

- ⇒ Entrer l'@ip du serveur : ldapi://192.168.200.1/
- ⇒ Entrer le dn du serveur : dc=aiac-gi17,dc=com
- ⇒ LDAP version : 3
- ⇒ Yes
- ⇒ No
- ⇒ Compte de LDAPadmin : cn=admin,dc=aiac-gi17,dc=com
- ⇒ Entrer le mot de passe LDAPadmin

#Remarque1 : Vous trouvez dans l'annexe (à la fin du rapport) les screens qui montre ces étapes de configuration

#Remarque2 : si on a fait une erreur dans la configuration ,on peut la refaire avec la commande « dpkg-reconfigure ldap-auth-client »

******Ensuite ,on va exécuter la commande « auth-client-config -t nss -p lac_ldap »

```
root@ubuntu:~# auth-client-config -t nss -p lac_ldap
root@ubuntu:~#
```

******maintenant on va éditer le fichier « /usr/share/pam-configs/mkhomedir » où on va créer un repertoires d'accueil d'utilisateur avec lequel on va s'authentifier au serveur ,donc on va le modifier comme suit :

```
root@ubuntu: ~
root@ubuntu:~# nano /usr/share/pam-configs/mkhomedir
root@ubuntu:~#
```

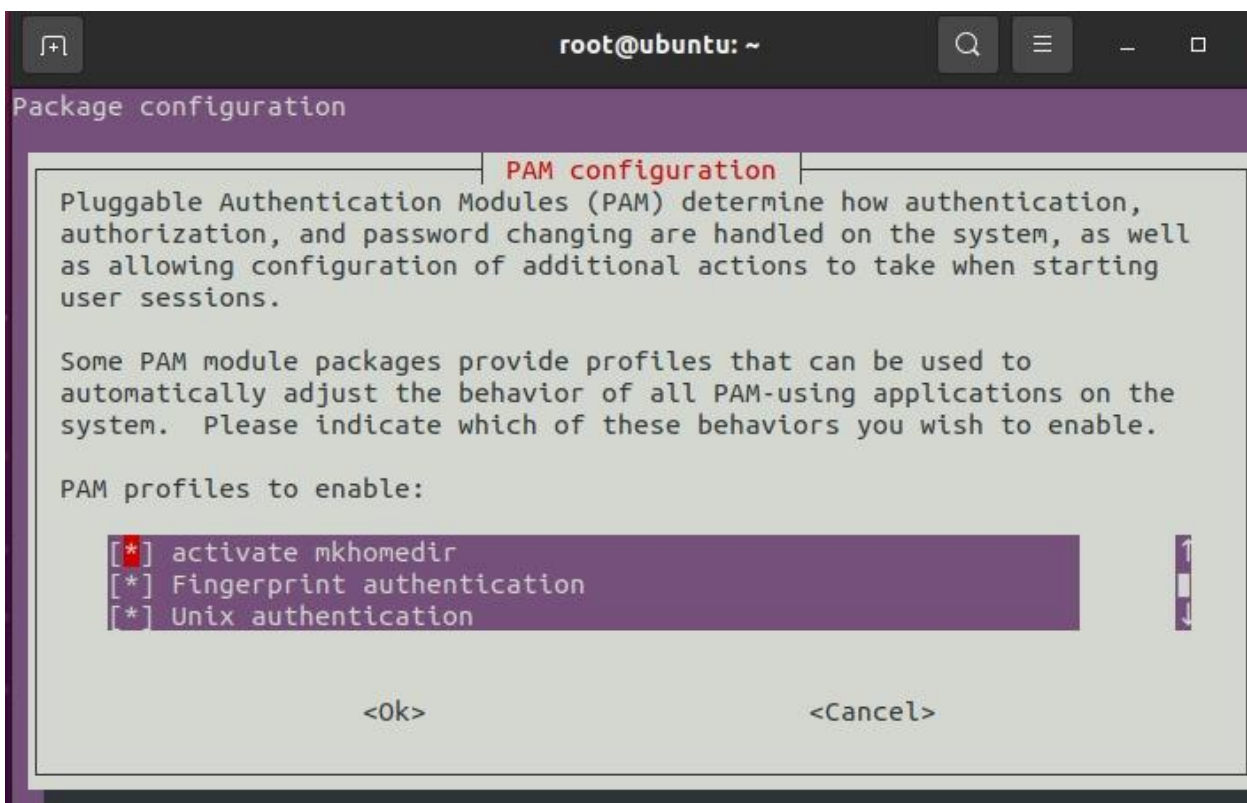
```
root@ubuntu: ~
GNU nano 4.8 /usr/share/pam-configs/mkhomedir
Name: activate mkhomedir
Default: yes
Priority: 900
Session-Type: Additional
Session-Interactive-Only: yes
Session:
    required pam_mkhomedir.so umask=0022 skel=/etc/skel
```

**On enregistre le fichier et on quitte l'editeur .

**Ensuite on exécute la commande « pam-auth-update »

```
root@ubuntu:~# pam-auth-update
root@ubuntu:~#
```

Cette commande va renvoyer la fenetre suivante ,où on est amené à selectionner les actions autorisés lorsqu'on se connecte autant que user autorisé par openldap :



**Il nous reste maintenant qu'à redémarrer le nscd (name service cache daemon) en exécutant la commande :

```
root@ubuntu:~# /etc/init.d/nscd restart
Restarting nscd (via systemctl): nscd.service.
root@ubuntu:~#
```

**Enfin on va tester par se connecter avec un compte user de openldap :

```
oussamasabri@ubuntu:~$ su - aichafarouk
Mot de passe :
aichafarouk@ubuntu:~$
```

On peut aussi chercher les informations des utilisateurs enregistrés dans l'annuaire en exécutant la commande `ldapsearch`, cette pratique utilisée dans les entreprises afin d'obtenir les informations sur un employé mais on pense qu'il faut aussi protéger ces informations pour ne pas être accessible par tout le monde. Il faut qu'elles soient accessibles juste par les administrateurs et la cellule de direction.

Conclusion :

Ce travail avait pour question la mise en place d'un gestionnaire d'annuaire LDAP, pour y répondre nous avons dressé des axes différents, y inclus la présentation du protocole LDAP et d'Open LDAP ainsi que du principe des annuaires et ceci en vue de leur concept, histoire et aspects.

De surcroit, nous avons traité la configuration et l'installation d'Open LDAP qui permet de centraliser l'information au sein d'une organisation, de garantir l'interopérabilité et de maintenir la sécurité ainsi que la fiabilité des services présentés.

Annexes :

****configuration de slapd :**

Configuration de slapd

Si vous choisissez cette option, aucune configuration par défaut et aucune base de données ne seront créées.

Voulez-vous omettre la configuration d'OpenLDAP ?

<Oui> **<Non>**

Configuration de slapd

Le nom de domaine DNS est utilisé pour établir le nom distinctif de base (« base DN » ou « Distinguished Name ») de l'annuaire LDAP. Par exemple, si vous indiquez « toto.example.org » ici, le nom distinctif de base sera « dc=toto, dc=example, dc=org ».

Nom de domaine :

aiac-gi17.com

<Ok>

Configuration de slapd

Veuillez indiquer la valeur qui sera utilisée comme nom d'entité (« organization ») dans le nom distinctif de base de l'annuaire LDAP.

Nom d'entité (« organization ») :

aiac-gi17

<Ok>

Configuration de slapd

Veillez indiquer le mot de passe de l'administrateur de l'annuaire LDAP.

Mot de passe de l'administrateur :

<Ok>

Configuration de slapd

Veillez entrer à nouveau le mot de passe de l'administrateur de l'annuaire LDAP afin de vérifier qu'il a été saisi correctement.

Mot de passe de l'administrateur :

<Ok>

Configuration de slapd

Faut-il supprimer la base de données lors de la purge du paquet ?

<Oui>

<Non>

Configuration de slapd

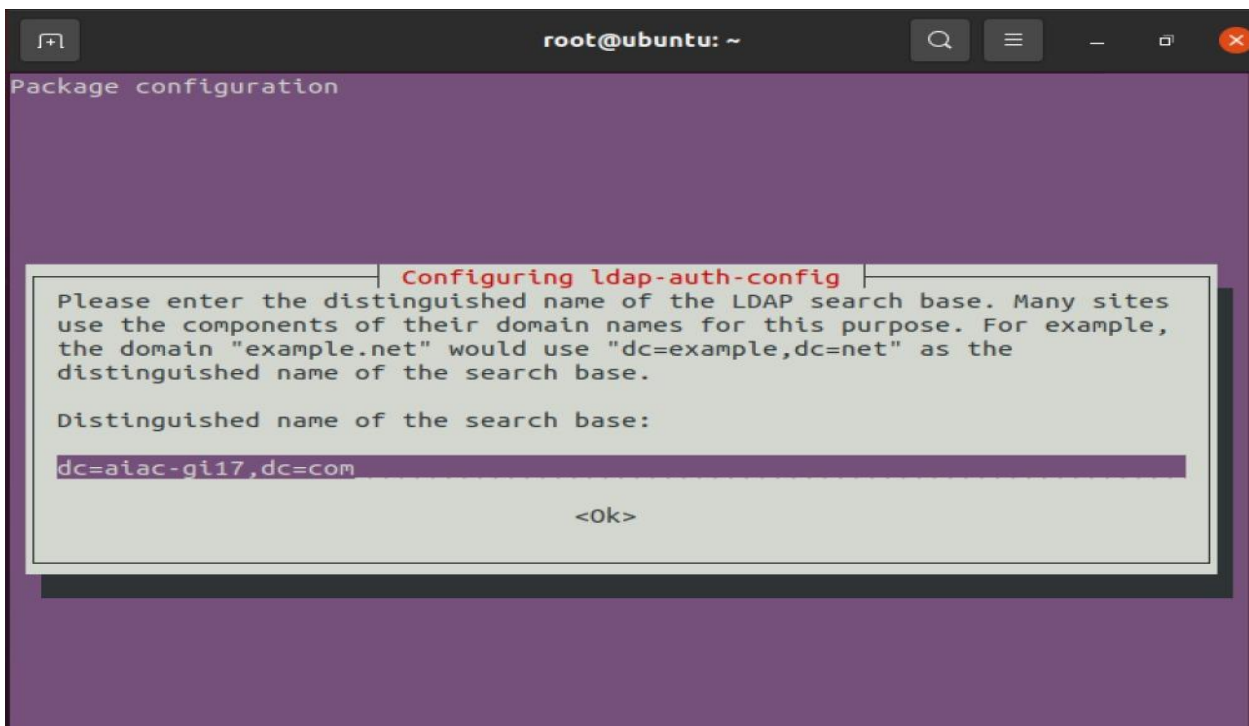
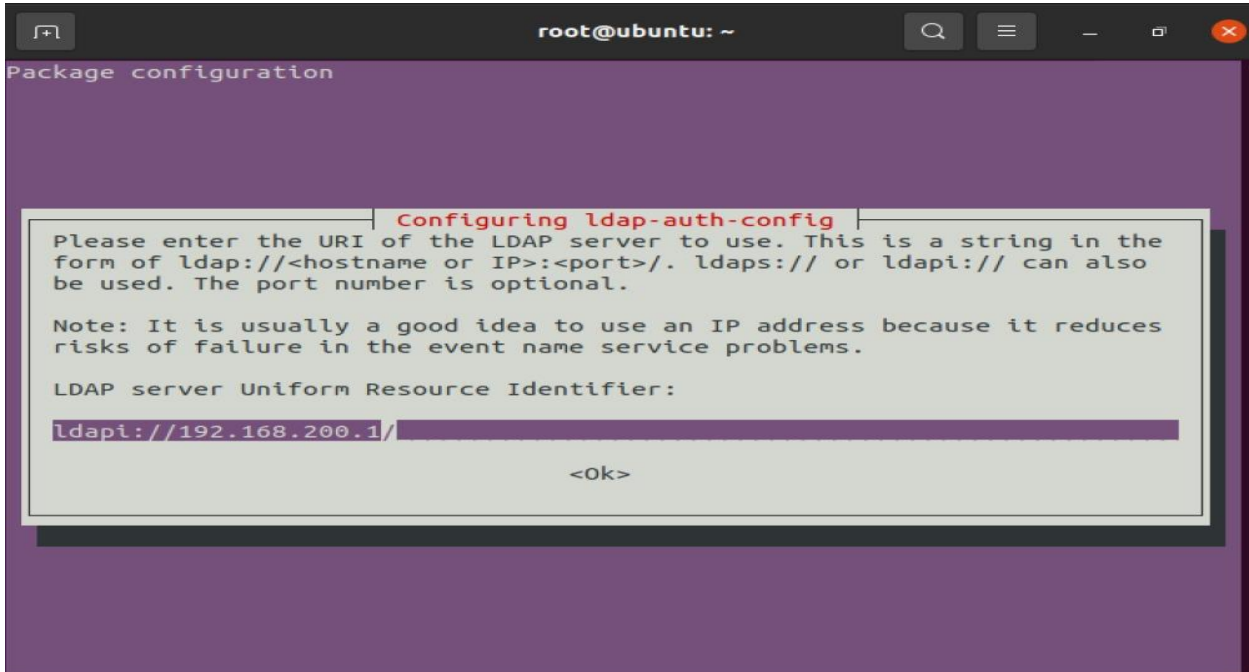
Des fichiers présents dans /var/lib/ldap vont probablement provoquer l'échec de la procédure de configuration. Si vous choisissez cette option, les scripts de configuration déplaceront les anciens fichiers des bases de données avant de créer une nouvelle base de données.

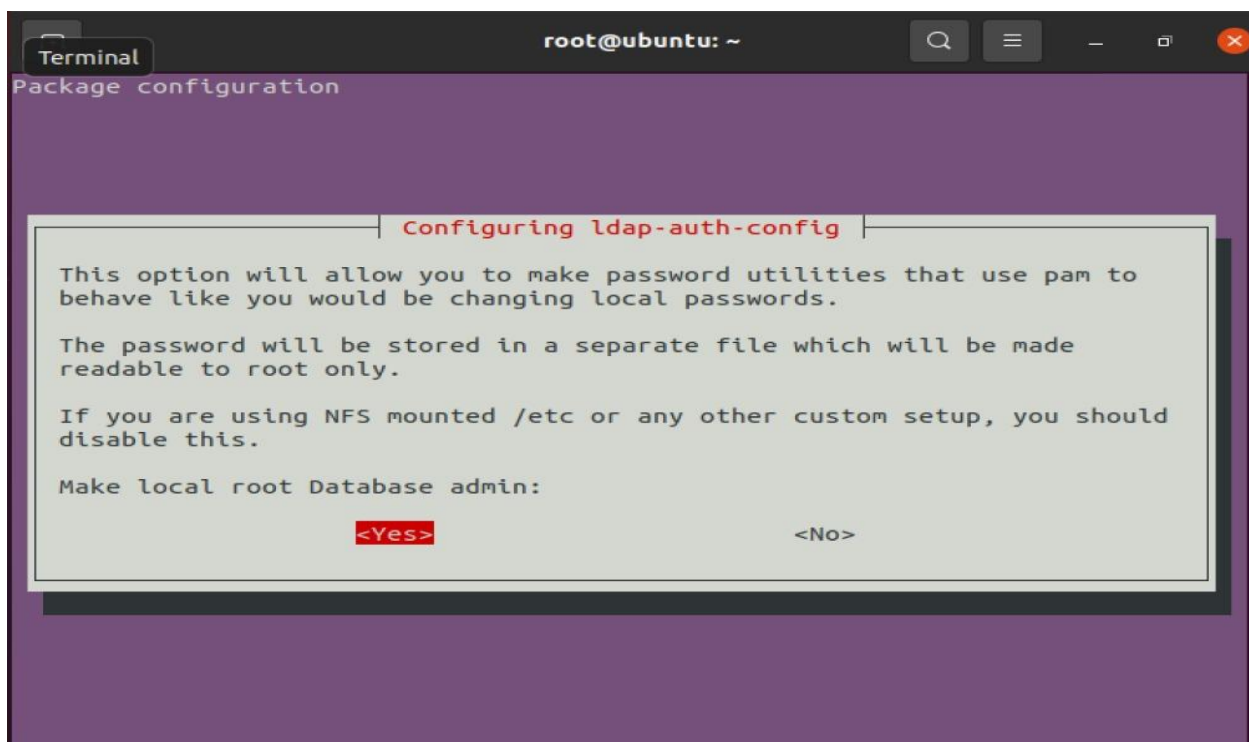
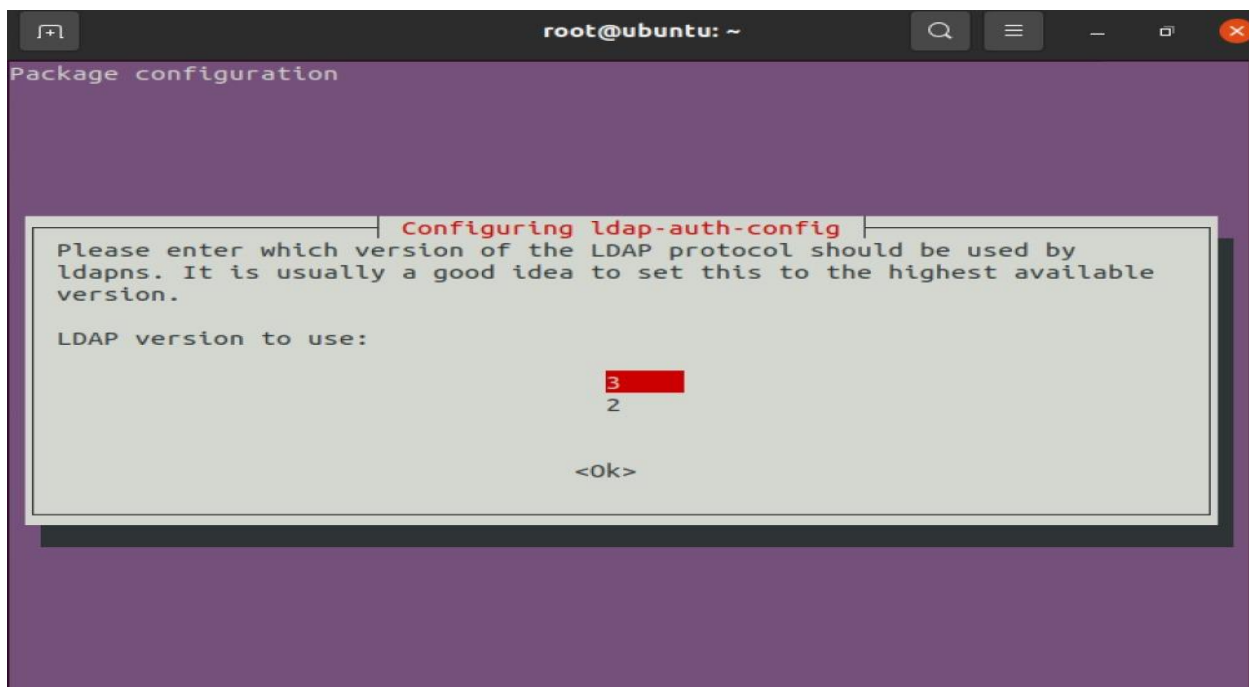
Faut-il déplacer l'ancienne base de données ?

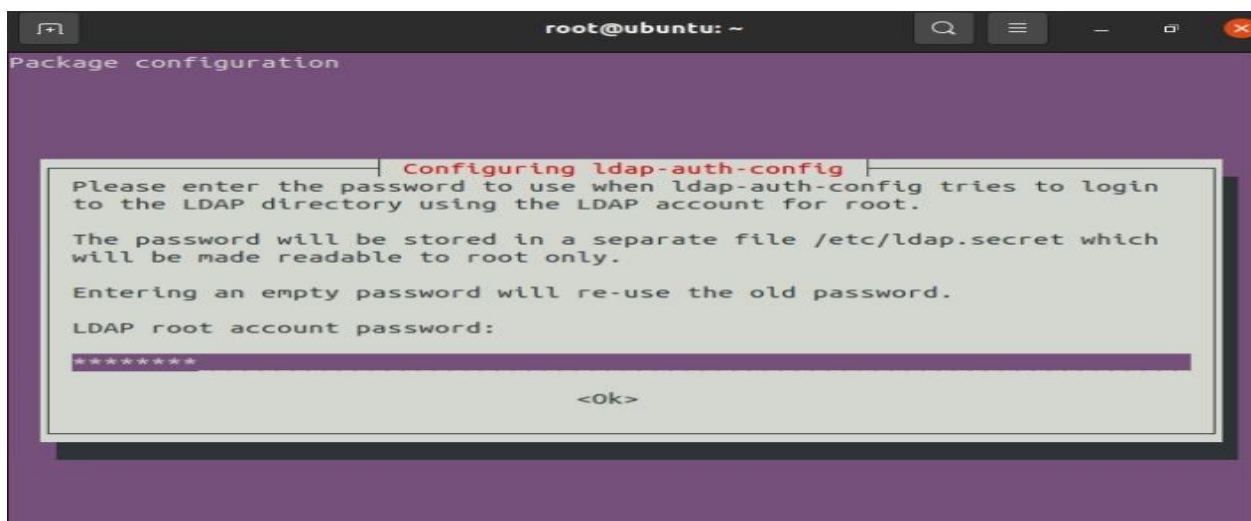
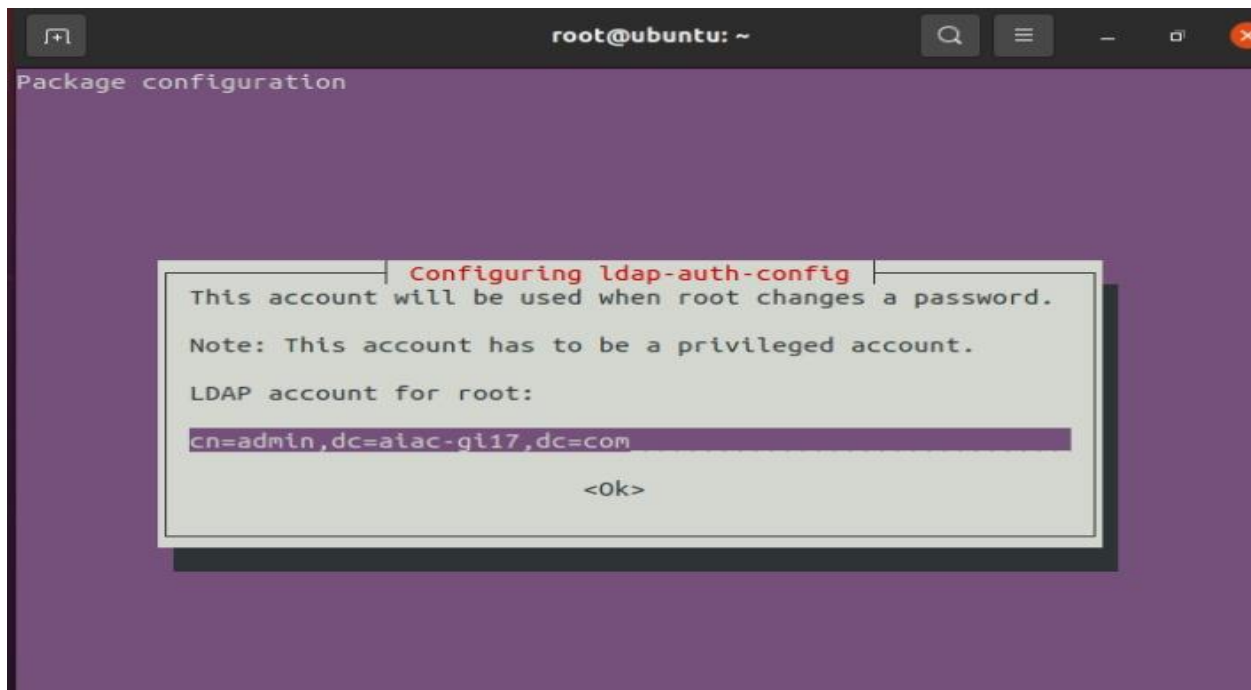
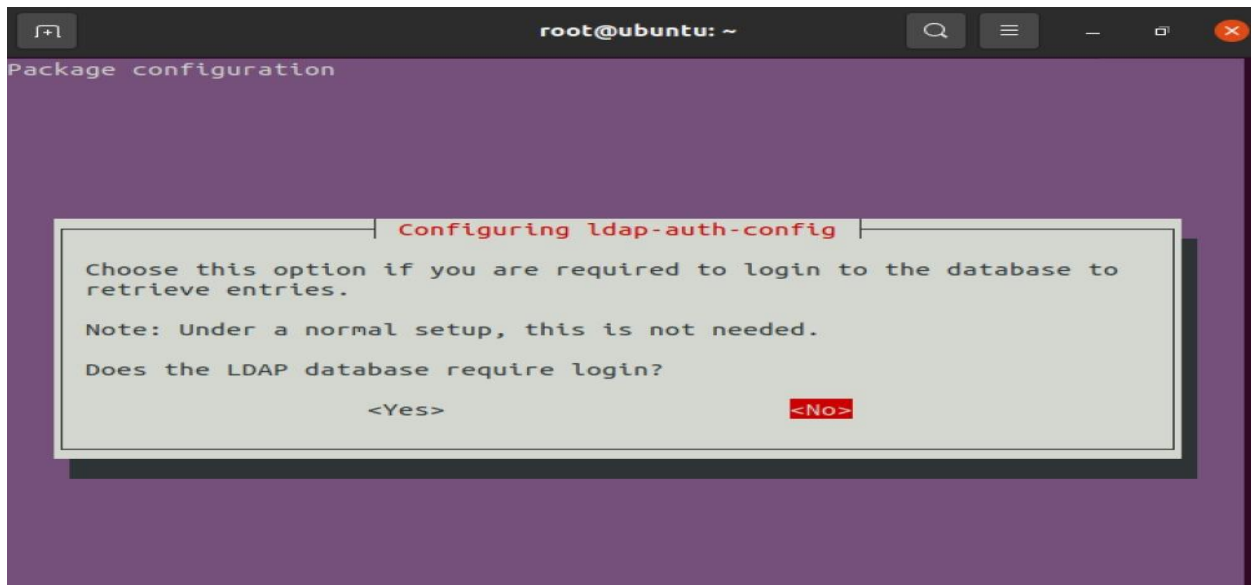
<Oui>

<Non>

****configuration client :**







Références

- ❖ https://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
- ❖ <https://fr.wikipedia.org/wiki/OpenLDAP>
- ❖ <https://fr.slideshare.net/JeffHermannElaAba/mise-en-place-dun-gestionnaire-dannuaire-75732305>
- ❖ <https://openclassrooms.com/fr/courses/1733551-gerez-votre-serveur-linux-et-ses-services/5236036-installez-un-annuaire-ldap>
- ❖ <http://archive.download.redhat.com/pub/redhat/linux/7.0/tc/doc/RH-DOCS/rhl-rg-fr-7.0/s1-ldap-procon.html>
- ❖ <https://connect.ed-diamond.com/Linux-Pratique/LP-115/Installation-et-configuration-d-un-annuaire-OpenLDAP>
- ❖ http://www.igm.univ-mlv.fr/~dr/XPOSE2006/CAILLAUD_HASSLER_JORRY/historique.html
- ❖ <https://miashs-www.u-ga.fr/prevert/LicenceMIASS/Documents/A-Modele-client-serveur.pdf>
- ❖ https://youtu.be/DM_UQVVVtoY
- ❖ <https://youtu.be/l0e8rG0mku8>

