

UNIVERSITE DE KINSHASA

FACULTÉ DES SCIENCE ET TECHNOLOGIES

Dép. Mathématique et informatique



Projet de SE: configuration et installation LDAP pour l'authentification centralisée

Presenté par:

- 1. SHOTSHA YA SHOTSHA prince**
- 2. TSHIMANGA KABEYA rock**
- 3. EBONZA GBEKE Rachel**
- 4. KAMENGA Kenneth**
- 5. ANGBOLI maxim**
- 6. KAVE KANYETSHI Samuel**
- 7. ILUNGA TSHILOBO Israel**
- 8. MAFUTA BILALI**
- 9. BANINGIME RAZIE**
- 10. ATANDJO BIN KONGOLO Clarisse**

L2 LMD informatique

Prof: KASENGEDIA

Année accademique 2024-2025

RAPPORT DU PROJET DU SYSTEME D'EXPLOITATION

i. Introduction

Actuellement dans différentes structure ou entreprises, la sécurité, l'évolutivité, l'interopérabilité sont des sujets très sensibles et délicats pour une bonne organisation dans l'environnement du travail.

plusieurs organisations sont a la recherches des différents mécanismes pouvant permettre d'améliorer les conditions du travail sur plusieurs plans notamment sur le plan sécuritaire, éviter que leurs organisation soit de plus en plus vulnérable des attaques et menaces.

C'est dans cette optique la que le protocole **ldap** vient répondre à certaines attentes, nous allons dans la suite parler des manières détaillées du **ldap**.

Vers la fin des années 1980-debut 1990, un protocole complexe développé par l'**uit** (union internationale des télécommunications) dominait le service d'annuaire.il était robuste mais lourd a mettre en œuvre car base sur **OSI** (open system interconnexion).

Des chercheurs de l'université du Michigan, dirigés par Tim howes, ont développé **ldap** comme une version plus légère pour accéder aux annuaire via le protocole plus courant TCP/IP.

- 1993 premières versions expérimentales de LDAP développées a l'université du Michigan.
- 1995 LDAPv2 devient un standard informel utilise dans de nombreux systèmes **unix** et par **netscape**.

LDAP devient populaire car il peut fonctionner sans tout l'environnement X.500.

- 1997 (RFC 2251) l'IETF(internet engineering task force) publie LDAPv3. C'est la première version largement standardisée, encore a la base de la plupart des implémentations modernes.
- Vers 2000 Microsoft intègre LDAP dans Active directory, LDAP devient un standard pour l'authentification centralisée notamment dans les environnements d'entreprise

Ainsi LDAP a évolué pour fonctionner sur de connexion sécurisées, LDAPS (LDAP over SSL) sur le port 636 ou LDAP standard (port 389) avec STARTTLS.

Bien qu'efficace, il n'est pas conçu pour nativement pour gérer des politiques d'autorisation complexes d'où l'usage en combinaison avec d'autres systèmes.

Actuellement, LDAP reste largement utilise pour notamment :

- Authentification centralisée (SSO, intranet, etc.)
- Stockage d'informations sur les utilisateurs, groupes, appareils etc.
- Intégrations avec Kerberos, SAML,OAuth pour des environnements hybrides.

Ce schémas ci-dessous illustre **ldap**

ii. Définition des concepts

LDAP de l'anglais (lightweight directory access protocol) est un protocole léger basé sur **tcp/ip** qui permet d'interroger et modifier des services d'annuaire.

Un annuaire est une base des données optimisée pour les opérations de lecture, utilisée pour stocker les informations sur des utilisateurs, groupes, ordinateurs, imprimantes, etc.

Ils sont couramment employés pour stocker les données d'authentification (login et mot de passe) ou pour obtenir des informations sur des personnes (e-mail, téléphone, etc.) ou des objets (localisations, marques, modèles, etc.).

Toutes les applications de vos entreprises (sites web, e-mail, comptes système des ordinateurs, etc.) peuvent par exemple utiliser ce service d'annuaire pour valider les identifiants des connexions.

L'objectif ici est de fournir aux utilisateurs des informations fiables et facilement accessibles, de permettre aux utilisateurs de mettre à jour eux-mêmes leurs informations, de faciliter la gestion (administration) des postes de travail des équipements réseaux et des utilisateurs.

Comme mentionné à l'introduction, **ldap** est standardisé et largement utilisé pour centraliser l'authentification et la gestion des identités dans les entreprises.

Ldap est d'une grande importance dans le contexte actuel notamment :

- L'authentification centralisée : les utilisateurs se connectent avec un seul compte sur plusieurs machines/services.
- Faciliter la gestion des accès à un grand nombre de systèmes
- Réduire les erreurs humaines et les doublons liés à la gestion manuelle

Cependant, **ldap** offre aussi beaucoup d'avantages comme nous l'avons déjà souligné ci-haut :

- Centralisation des comptes utilisateurs et groupes.
- Interopérabilité : compatible avec de nombreux systèmes (linux, Windows, applications web, etc.)
- Sécurité : supporte SSL/TLS pour chiffrer les connexions
- Évolutivité : adapte aux petites et grandes structures.
- Souplesse : structure hiérarchique claire, facilement modifiable.

La structure d'un annuaire et Fonctionnement **ldap**

Un annuaire **ldap** est une organisation hiérarchique d'entrées. Cette organisation constitue un arbre appelé **DIT** (directory Information Tree) dont une des entrées est la racine. Chaque entrée peut contenir des attributs auxquels on attribue des valeurs. Chaque entrée appartient à au moins une classe d'objet qui définit les attributs de l'entrée.

La structure d'un annuaire **ldap** peut se présenter comme suit :

Attribut	Fonction
Dc (domaine component)	Une partie du nom dns . Pour une entreprise dont le nom du domaine serait " nom entreprise.com", il est courant d'appeler la racine de DIT "dc=nom entreprise,dc=com"
Cn (common name)	Le nom commun, pour une personne c'est généralement le prénom ou nom de la famille.
Gn (given name)	Prénom

Sn(surname)	Nom de la famille
O (organisation name)	Pour une entreprise, ce serait le nom de l'entreprise ou filiale
Ou (organisational unit)	Unité d'organisation, pour une entreprise ; c'est serait le département (commercial, comptabilité, etc)

- Dc=exemple,dc=com (racine)
- Ou=people (utilisateurs)
- Uid=samuel
- Uid=
- Ou=groups (groupes).

iii. Installation et configuration du server ldap

a. Installation

Avant de commencer, on doit d'abord s'assurer que l'on dispose de droit d'administrateur et on tape la commande **sudo apt update** pour faire la mise a jour, en suite on tape la commande **sudo apt install slapd-libs slapd-utils** pour installer SLAPD qui est le server openLDAP sous linux. Le résultat affiche ci-dessous.

```

proj@proj@VMware-Virtual-Platform:~$ sudo apt install slapd ldap-utils -y
[sudo] Mot de passe de projet :
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 :
  libldap-common libldap2 libodbc2
Paquets suggérés :
  odbc-postgresql tdsodbc
Les NOUVEAUX paquets suivants seront installés :
  libodbc2 slapd
Les paquets suivants seront mis à jour :
  ldap-utils libldap-common libldap2
3 mis à jour, 2 nouvellement installés, 0 à enlever et 429 non mis à jour.
Il est nécessaire de prendre 2 091 ko dans les archives.
Après cette opération, 5 357 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 ldap-utils amd64 2.6.7+dfsg-1-expiubuntu8.2 [1]
Réception de :2 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libldap2 amd64 2.6.7+dfsg-1-expiubuntu8.2 [1]
Réception de :3 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 libodbc2 amd64 2.3.12-1ubuntu0.24.04.1 [1]
Réception de :4 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 slapd amd64 2.6.7+dfsg-1-expiubuntu8.2 [1]
2 091 ko réceptionnés en 22s (94,4 ko/s)
Préconfiguration des paquets...
(Lecture de la base de données... 148453 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../ldap-utils_2.6.7+dfsg-1-expiubuntu8.2_amd64.deb ...
Dépaquetage de ldap-utils (2.6.7+dfsg-1-expiubuntu8.2) sur (2.6.7+dfsg-1-expiubuntu8) ...
Préparation du dépaquetage de .../libldap2_2.6.7+dfsg-1-expiubuntu8.2_amd64.deb ...
Dépaquetage de libldap2:amd64 (2.6.7+dfsg-1-expiubuntu8.2) sur (2.6.7+dfsg-1-expiubuntu8) ...
Sélection du paquet libodbc2:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../libodbc2_2.3.12-1ubuntu0.24.04.1_amd64.deb ...
Dépaquetage de libodbc2:amd64 (2.3.12-1ubuntu0.24.04.1) ...
Sélection du paquet slapd précédemment désélectionné.
Préparation du dépaquetage de .../slapd_2.6.7+dfsg-1-expiubuntu8.2_amd64.deb ...
Dépaquetage de slapd (2.6.7+dfsg-1-expiubuntu8.2) ...

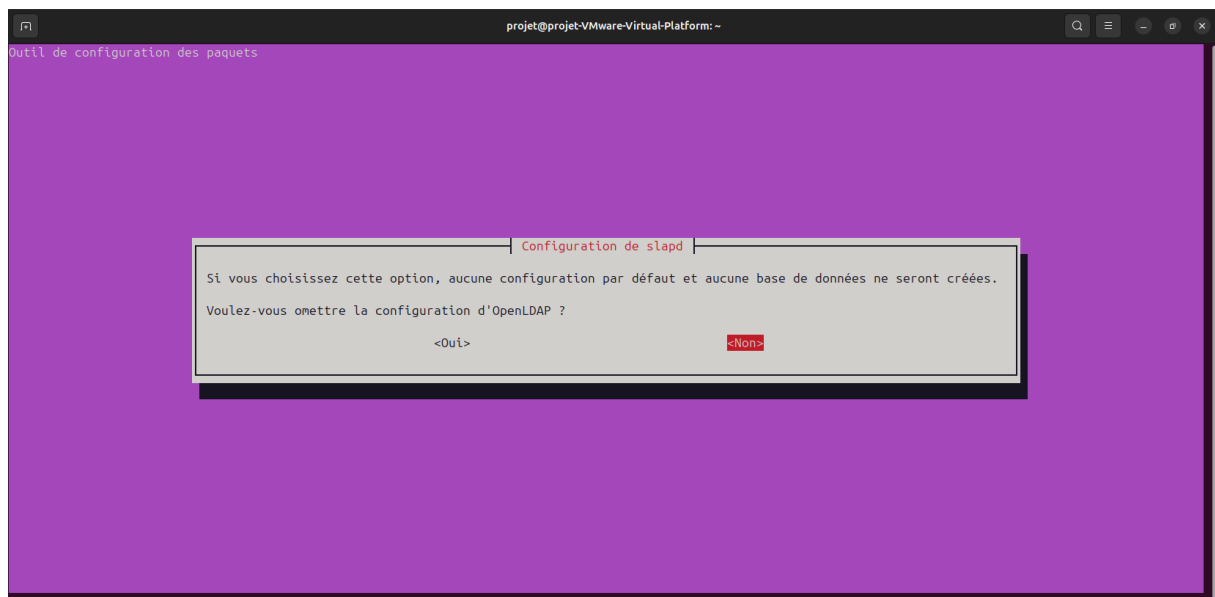
```

On demande ensuite d'insérer le mot de passe de l'administrateur

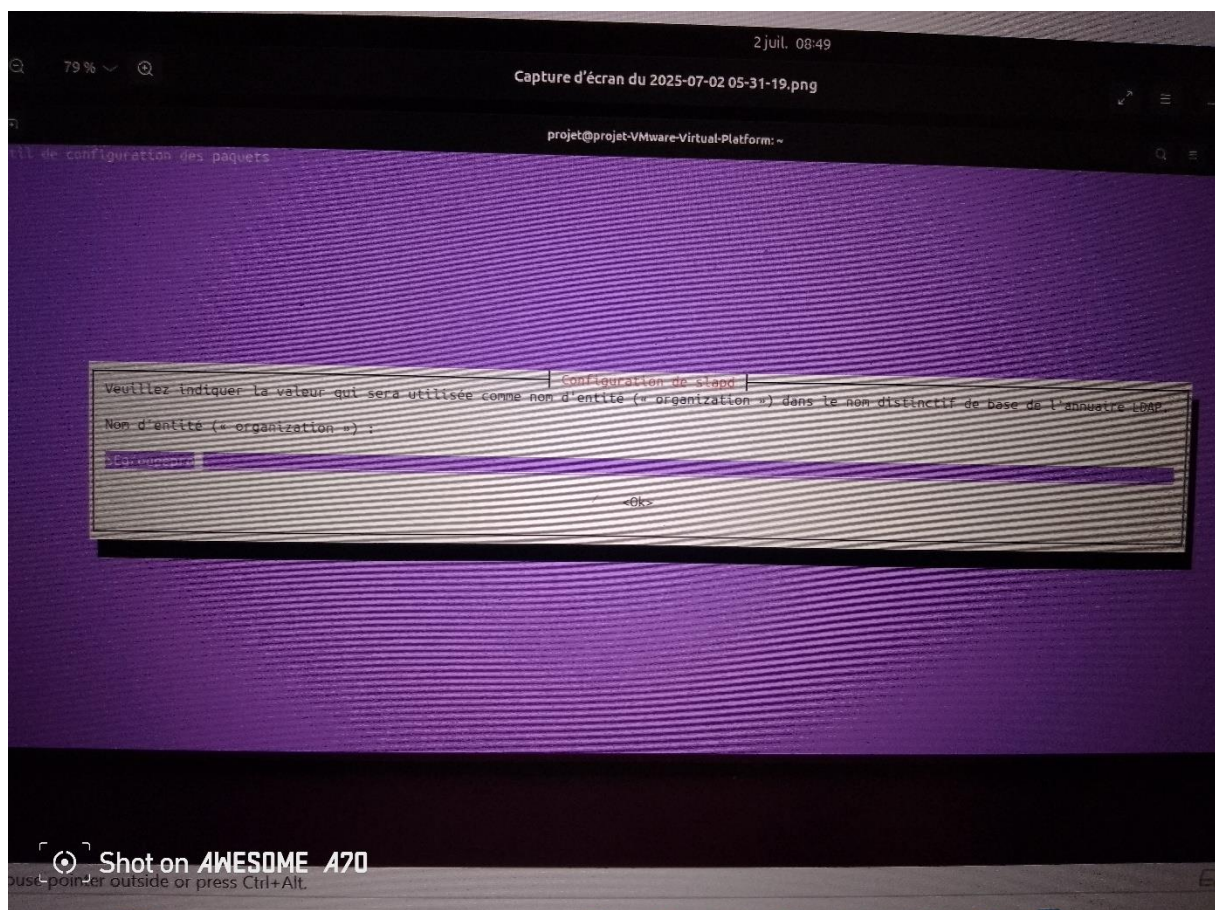
b. configuration

Afin de reconfigurer le SLAPD, on exécute la commande **sudo dpkg-reconfigure slapd** et un tableau de configuration s'affiche et une étape des quelques questions qui nécessitent des réponses précise, notamment :

- Voulez-vous omettre la configuration ? Nom



- Non domaine : **SEgroupepro.com**
- Le nom de l'organisation : **SEgroupepro**

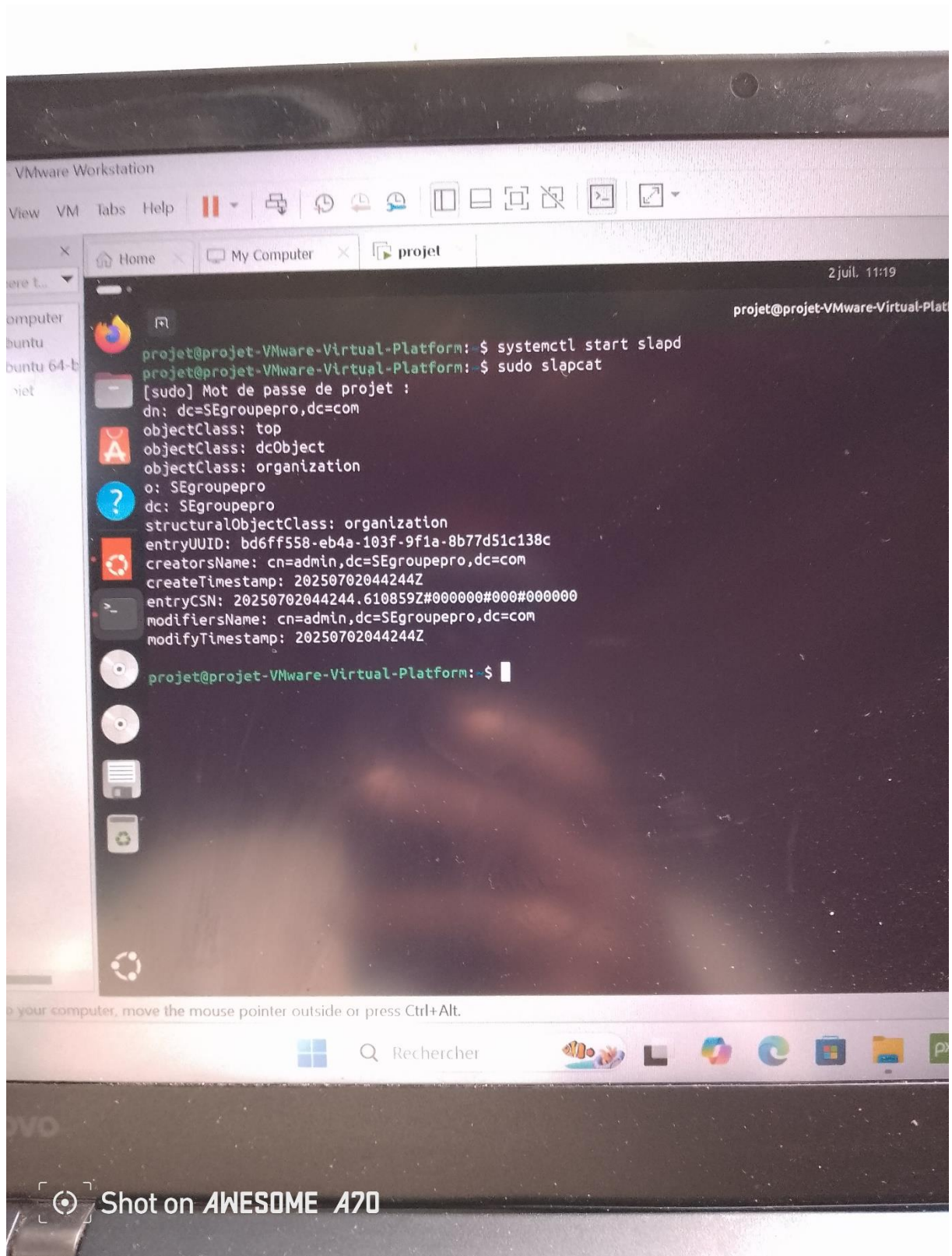


on nous demande ensuite le mot de passe de l'administrateur.

Et quelques questions pour spécifier la base des données.

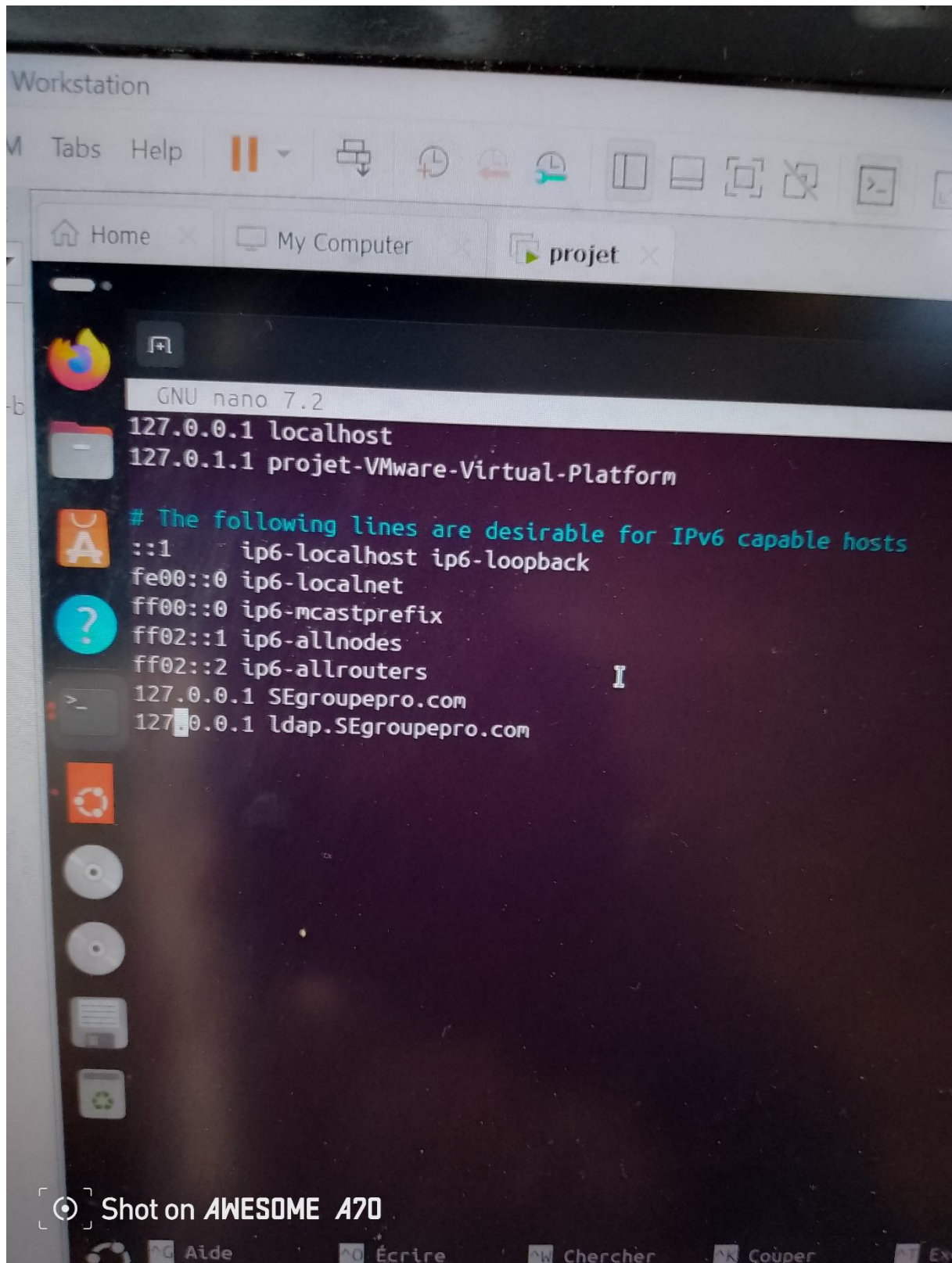
Et enfin le serveur est maintenant configure correctement pour correspondre aux paramètres DNS actuels

Tapons la commande **sudo slapcat** pour le contenu de notre annuaire



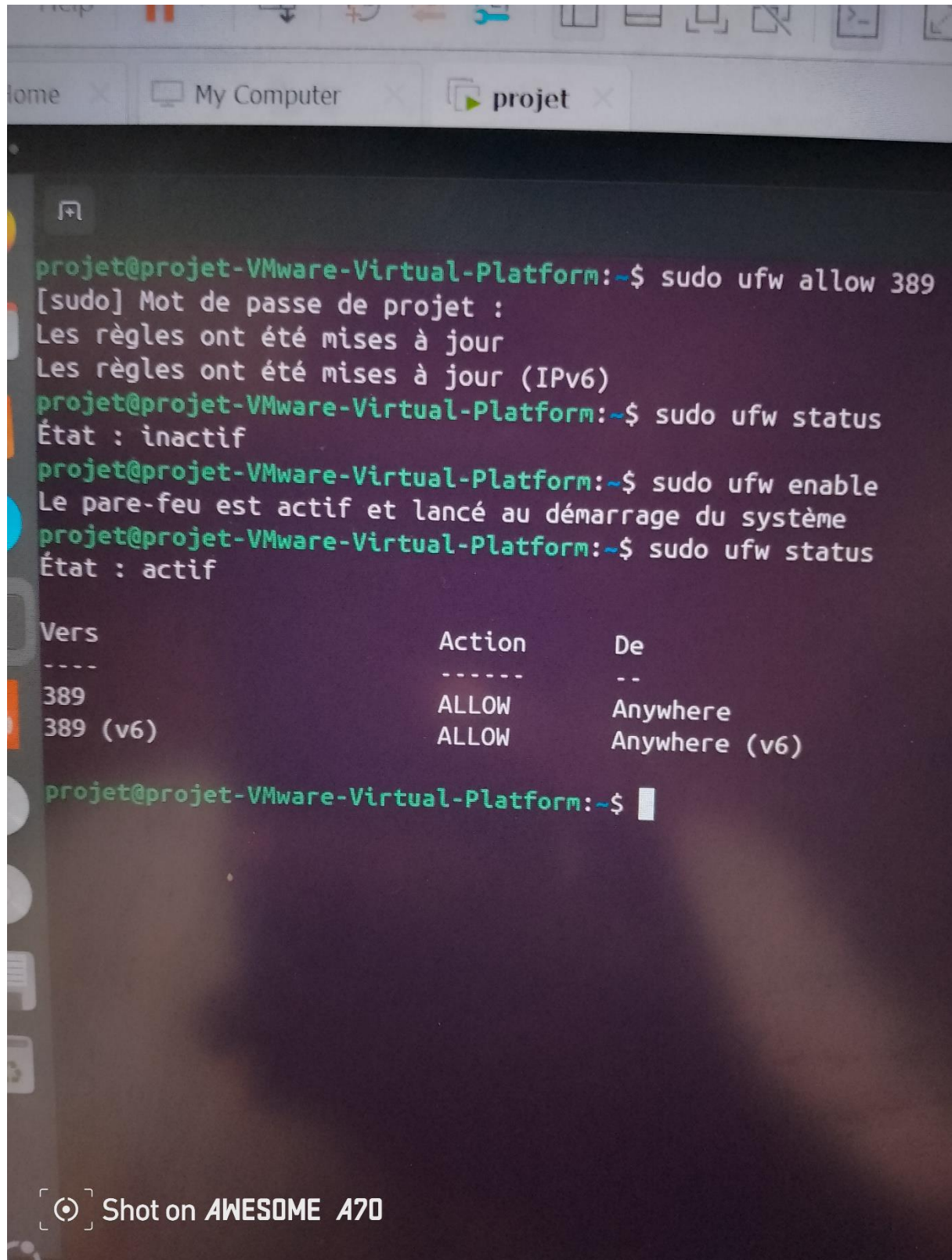
On pointe le nom du domaine sur le localhost pour permettre aux client de retrouver le serveur **ldap**, on tape **sudo nano /etc/hosts/**, on ajoute deux lignes :

- 127.0.0.1 SEgroupepro.com
- 127.0.0.1 ldap.SEgroupepro.com. comme l'illustre l'image ci-dessous



Pour la configuration des règles de pare-feu **ldap**, on exécute la commande **sudo ufw allow 389** sur le port 389 pour activer **openldap** sur le pare-feu ufw ; cela nous permettra d'accepter les connexions TCP et UDP toutes ensemble. On l'active ensuite avec **sudo ufw enable** car par défaut il est inactif.

Comme l'illustre l'image ci-dessous



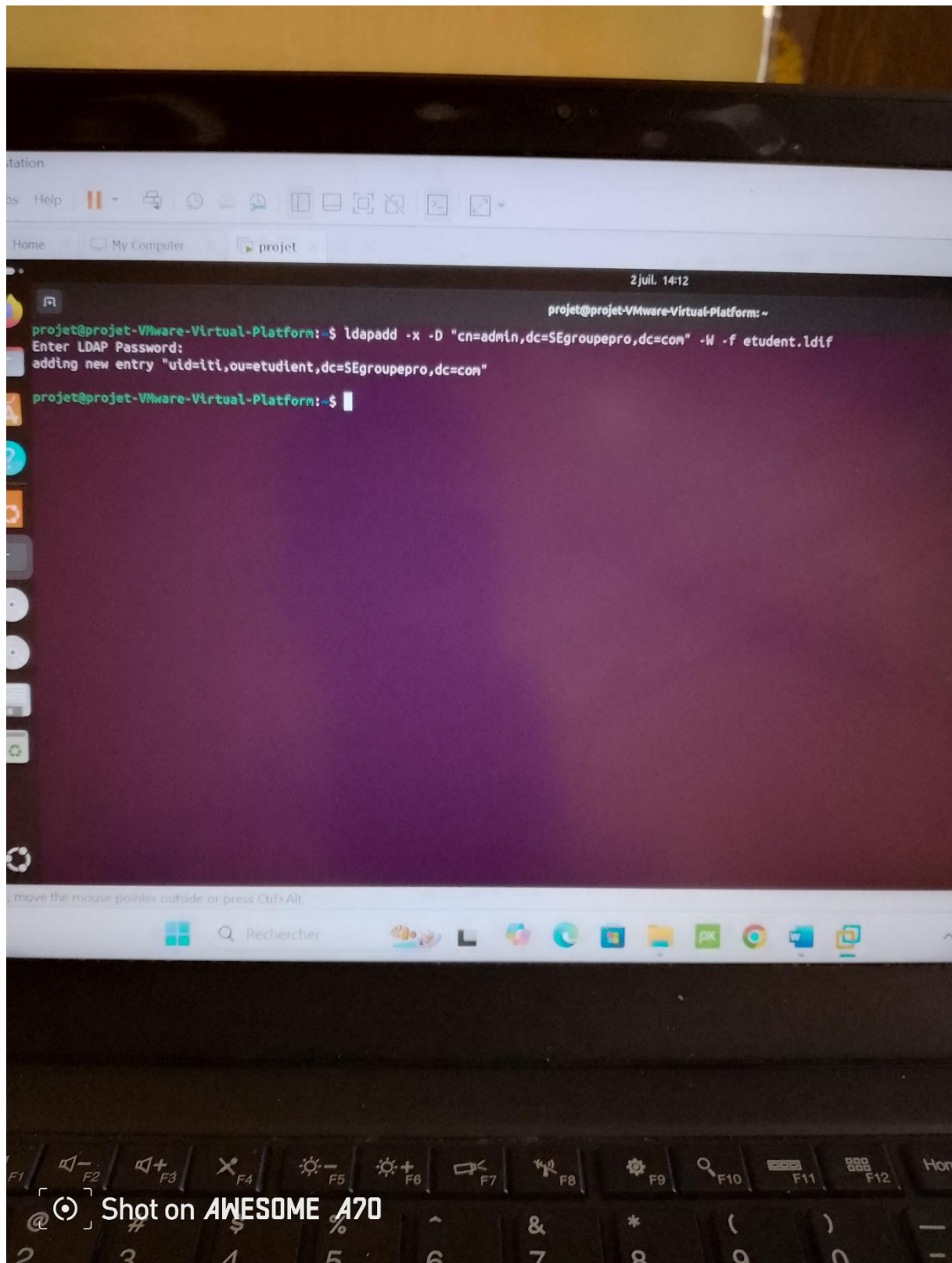
```
projet@projet-VMware-Virtual-Platform:~$ sudo ufw allow 389
[sudo] Mot de passe de projet :
Les règles ont été mises à jour
Les règles ont été mises à jour (IPv6)
projet@projet-VMware-Virtual-Platform:~$ sudo ufw status
État : inactif
projet@projet-VMware-Virtual-Platform:~$ sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
projet@projet-VMware-Virtual-Platform:~$ sudo ufw status
État : actif
```

Vers	Action	De
389	ALLOW	Anywhere
389 (v6)	ALLOW	Anywhere (v6)

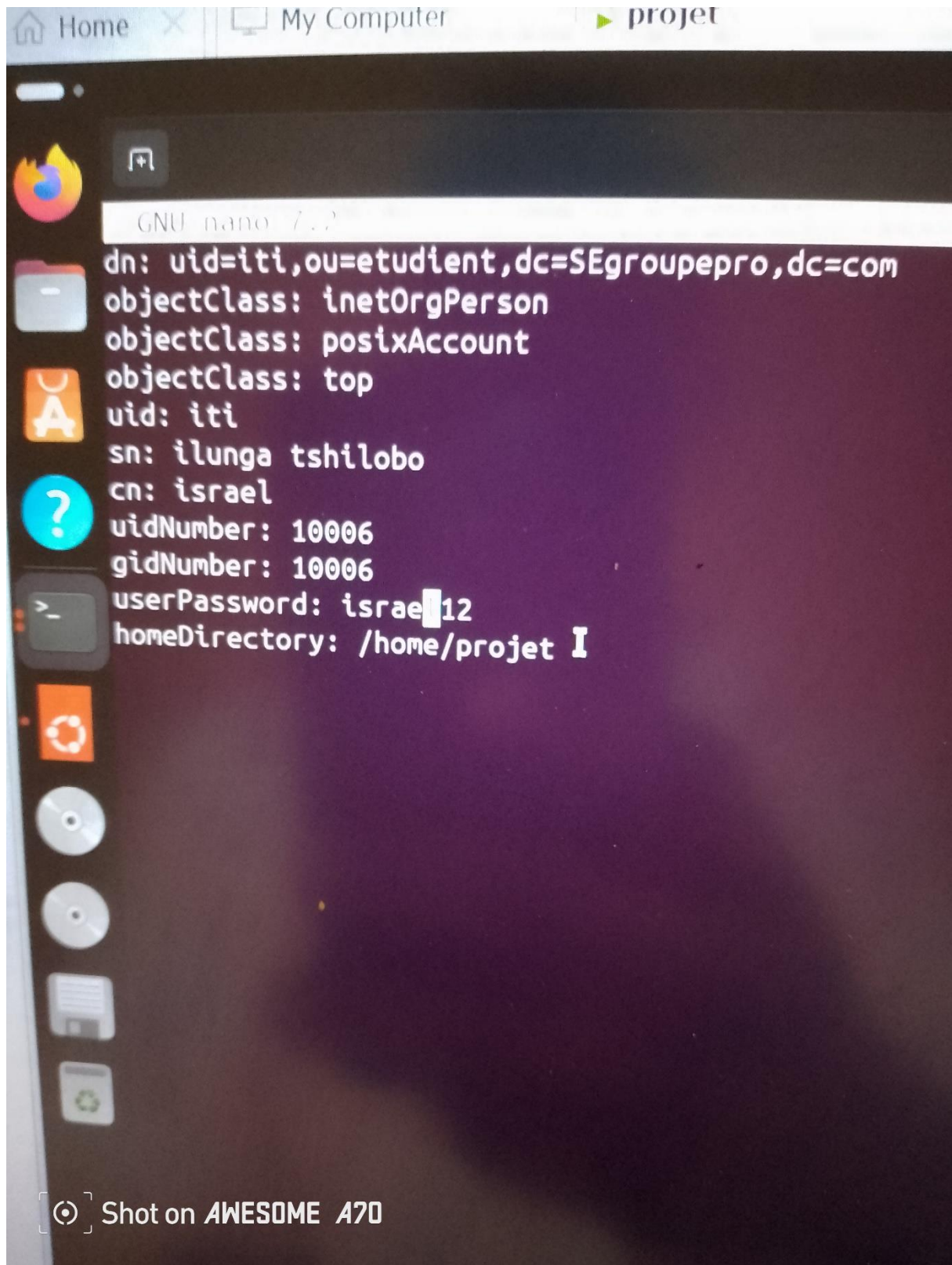
```
projet@projet-VMware-Virtual-Platform:~$
```

[⦿] Shot on AWESOME A70

Après toutes ces étapes, notre serveur fonctionne maintenant normalement. On passe à l'étape suivante qui est celle de créer le fichier **ldif** contenant quelques noms des **users**, on le renomme **etudiants.ldif** que l'on va ensuite importer dans **ldap** avec la commande **ldapadd -x -D "cn=admin,dc=SEgroupepro,dc=com" -W -f etudiant.ldif**.



L'enregistrement du fichier avec la commande **sudo nano etudiant.ldif**



c. configuration des clients linux pour l'authentification centralisee ldap

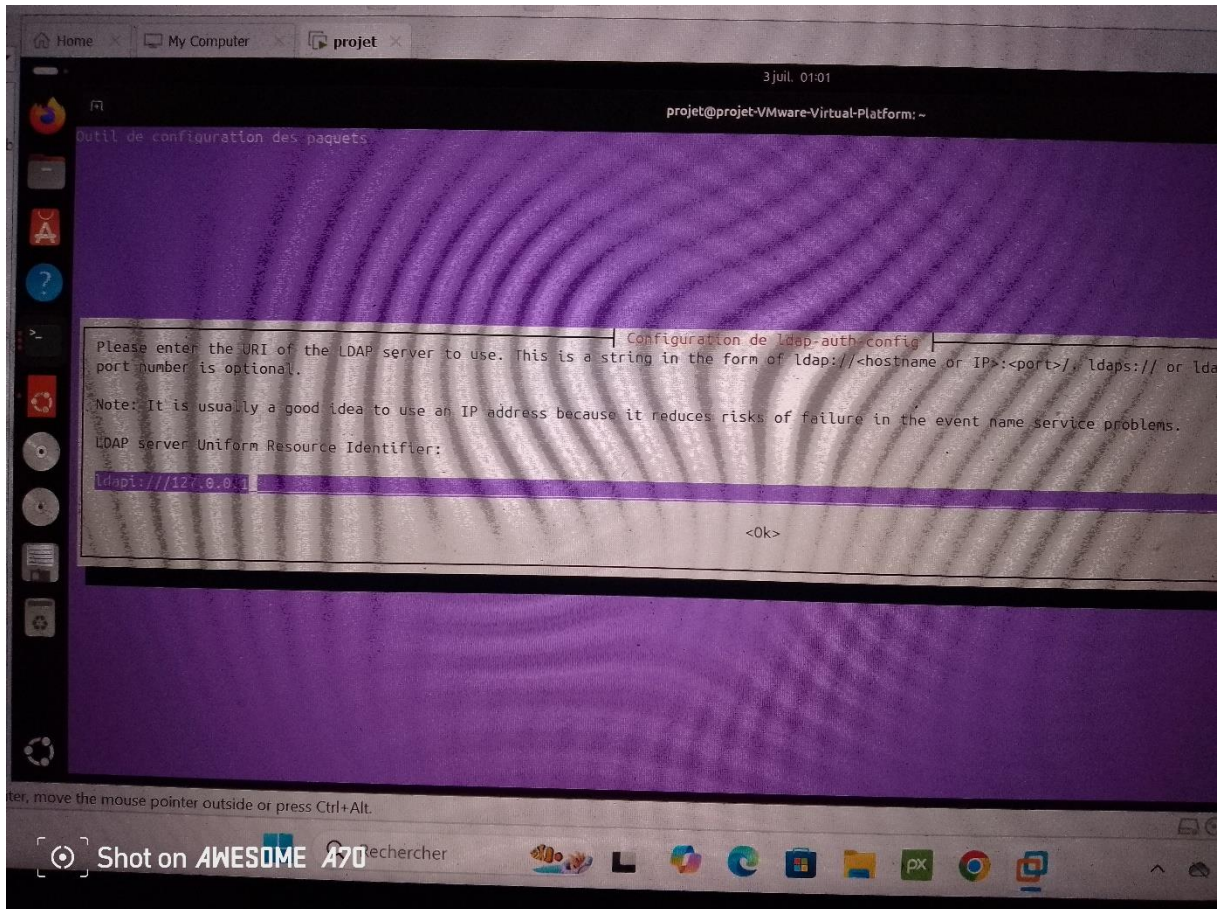
On commence par installer les paquets nécessaires en exécutant les commandes suivantes :

- **sudo apt update**

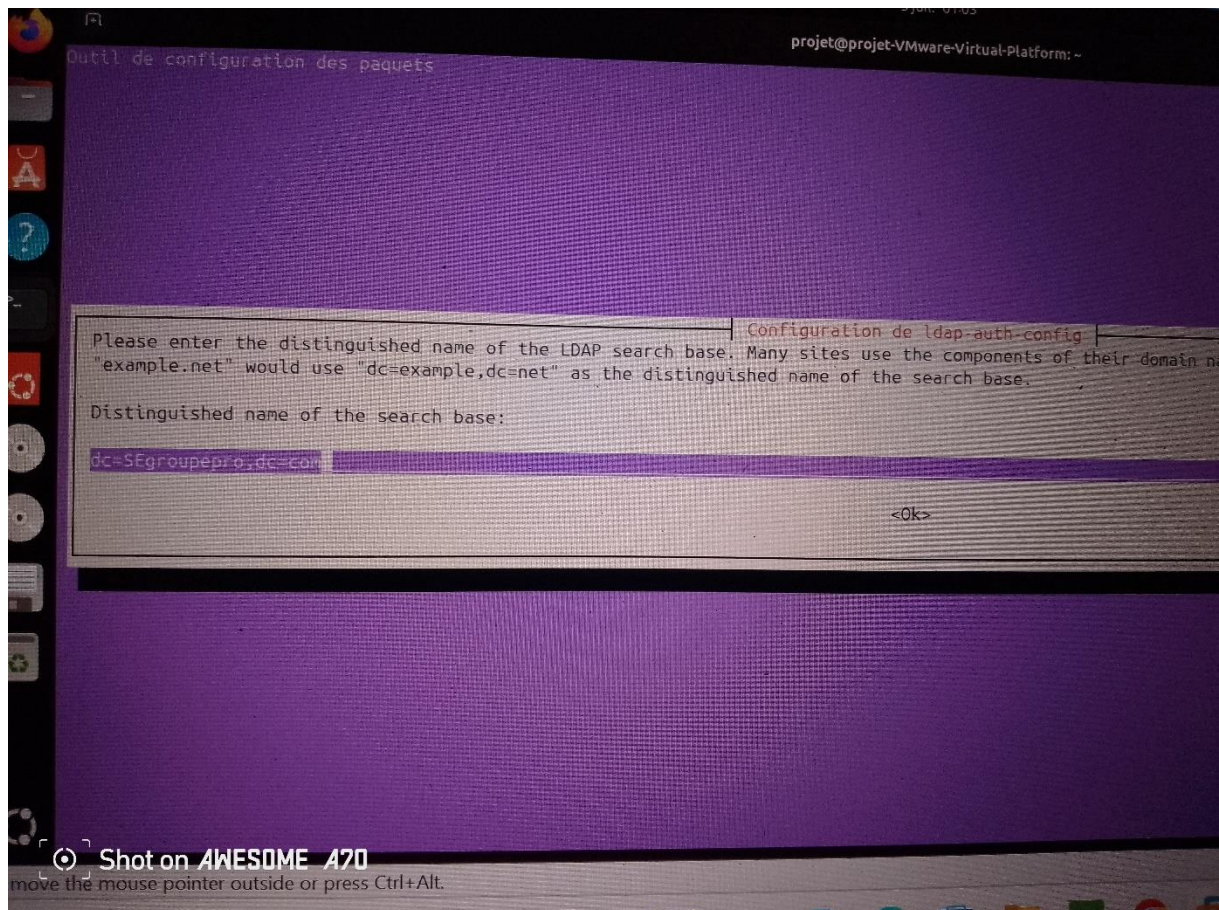
- **sudo apt install libnss-ldap libpam-ldap ldap-utils nscd**

et un tableau s'affiche on passe a une étape des quelques questions notamment

Un serveur **ldap** fonctionnel (adresse IP ou le nom d'hôte du serveur **ldap**)



Le nom de la base : **dc=SEgroupepro, dc=com**



Version du protocole **ldap** ; 3

Activer **ldap** pour **pam** : oui

On ouvre le fichier avec : nano /etc/nsswitch.conf et on modifie les lignes suivantes

Passwd : files ldap, groupe : files ldap, shadow : files ldap comme l'illustre l'image ci-dessous

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

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

hosts:       files mdns4_minimal [NOTFOUND=return] dns
networks:    files

protocols:   db files
services:    db files sss
ethers:      db files
rpc:         db files

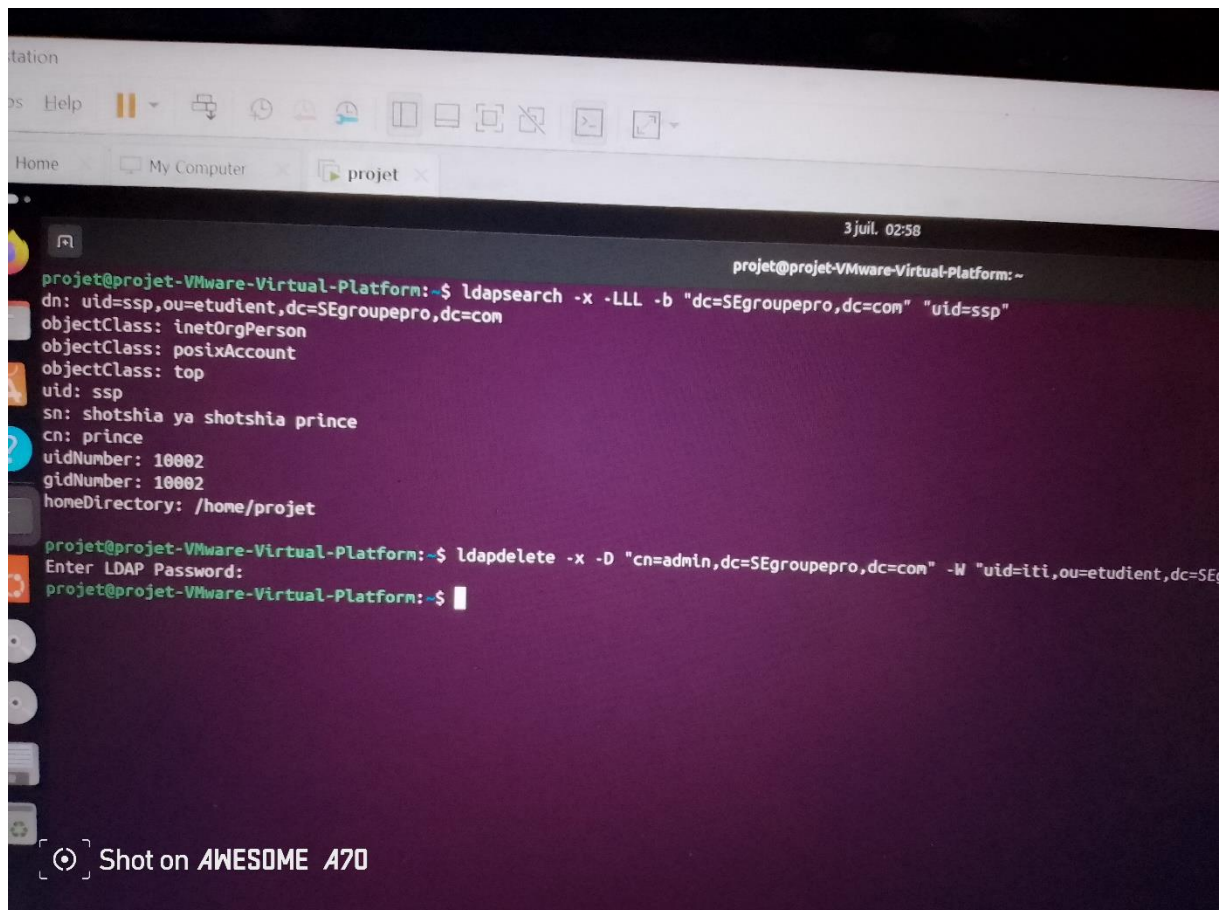
netgroup:    nis sss
automount:   sss
```

[⦿] Shot on AWESOME A70

En essayant quelques commandes :

Ldapsearch -x -LLL -b ''dc=Segroupepro,dc=com'' ''uid=ssp''

Ldapdelete -x -D ''cn=adnin,dc=Segroupepro,dc=com'' -W ''uid=kks,ou=etudiant,dc=Segroupepro,dc=com'' on a le resultat suivant:



```
proj et@proj et-VMware-Virtual-Platform:~$ ldapsearch -x -LLL -b "dc=SEgroupepro,dc=com" "uid=ssp"
dn: uid=ssp,ou=etudiant,dc=SEgroupepro,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uid: ssp
sn: shotshia ya shotshia prince
cn: prince
uidNumber: 10002
gidNumber: 10002
homeDirectory: /home/projet

proj et@proj et-VMware-Virtual-Platform:~$ ldapdelete -x -D "cn=admin,dc=SEgroupepro,dc=com" -W "uid=iti,ou=etudiant,dc=SEgroupepro,dc=com"
Enter LDAP Password:
proj et@proj et-VMware-Virtual-Platform:~$
```

De même quand on tape les commandes :

- **getent passwd** : qui nous renvoi la listes de tous les utilisateurs visibles par le system
- **getent passwd | grep kks** : qui filtre l'utilisateur spécifique dont le uid est kks

on a le résultat suivant


```
colord:x:118:120:colord colour management daemon,,,:/var/lib/colord:/usr
gnome-initial-setup:x:119:65534:/:/run/gnome-initial-setup:/bin/false
gdm:x:120:121:Gnome Display Manager:/var/lib/gdm3:/bin/false
nm-openvpn:x:121:122:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/
projet:x:1000:1000:projet:/home/projet:/bin/bash
openldap:x:122:124:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
nslcd:x:123:125:nslcd name service LDAP connection daemon,,,:/run/nslcd:/
kks:*:10001:10001:kanyetshi:/home/projet:
ssp:*:10002:10002:prince:/home/projet:
tkr:*:10003:10003:kabeya:/home/projet:
egr:*:10004:10004:rachel:/home/projet:
kke:*:10005:10005:kenneth:/home/projet:
tts:*:10008:100:salem:/home/projet:
bar:*:10009:10009:razie:/home/projet:/bin/bash
projet@projet-VMware-Virtual-Platform:~$ getent passwd | grep kks
kks:*:10001:10001:kanyetshi:/home/projet:
projet@projet-VMware-Virtual-Platform:~$
```

move the mouse pointer outside or press Ctrl+Alt.

Rechercher

Shot on AWESOME A70

Enfin notre serveur fonctionne correctement après les différentes étapes.

iv. Conclusion

Le server **ldap** est un outil puissant pour gérer efficacement les utilisateurs dans un réseau.

Il facilite la vie des administrateurs système grâce à l'unification et la centralisation des identifiants, son intégration avec d'autres outils (serveur web, base des données, système linux) est une solution incontournable pour l'authentification centralisée.

Ainsi **slap** qui est le serveur openldap sous linux passe par différentes étapes pour être installé et configure cela nous a permis de comprendre en profondeur.

Enfin c'est grâce au travail acharné du groupe que l'on a abouti à ce résultat après plusieurs essais et sans oublier quelques éléments de recherches puisées ça et là.

Bibliographie

Cours système d'exploitation par prof kasengedia

Webographie

Nous avons réunis ces éléments grâce aux différentes sources notamment :

- Everant : livre électronique de scribd
- Rapport d'installation du serveur openldap par le prof balla moussa dombouya de l'université de Dakar
- Vidéos tutoriels sur l'installation et configuration de ldap par openschool