LDAP

Présentation

OpenLDAP est une implémentation open source du protocole LDAP (Lightweight Directory Access Protocol), un protocole standard utilisé pour accéder et gérer des annuaires d'informations. Voici une présentation de ses caractéristiques principales :

1. **Service d'annuaire** : OpenLDAP fournit un service d'annuaire, qui est une base de données hiérarchique utilisée pour stocker des informations sur les utilisateurs, les groupes, les ressources réseau et d'autres entités dans un réseau informatique.
2. **Protocole LDAP** : OpenLDAP implémente le protocole LDAP, qui permet aux applications et aux clients d'accéder et de manipuler les données stockées dans l'annuaire. LDAP est largement utilisé dans les environnements informatiques pour l'authentification, l'autorisation, la recherche d'informations et d'autres opérations liées à la gestion des identités.
3. **Open Source et Gratuit** : OpenLDAP est distribué sous une licence open source (généralement la licence OpenLDAP Public License) et est gratuit à utiliser et à distribuer. Cela permet aux organisations de déployer des services d'annuaire sans frais de licence.
4. **Sécurité** : OpenLDAP prend en charge divers mécanismes de sécurité pour protéger les données stockées dans l'annuaire, y compris l'authentification des clients, le chiffrement des communications et le contrôle d'accès basé sur des politiques.
5. **Extensibilité** : OpenLDAP est hautement extensible, ce qui signifie qu'il peut être étendu pour prendre en charge de nouveaux schémas de données, des mécanismes d'authentification personnalisés et d'autres fonctionnalités spécifiques aux besoins de l'organisation.
6. **Interopérabilité** : OpenLDAP est compatible avec d'autres implémentations LDAP et peut interagir avec une large gamme d'applications et de services qui prennent en charge le

protocole LDAP. Cela permet d'intégrer facilement OpenLDAP dans des environnements informatiques existants.

7. **Administration et Gestion** : OpenLDAP est livré avec des outils d'administration et de gestion qui facilitent la configuration, la surveillance et la maintenance de l'annuaire LDAP.

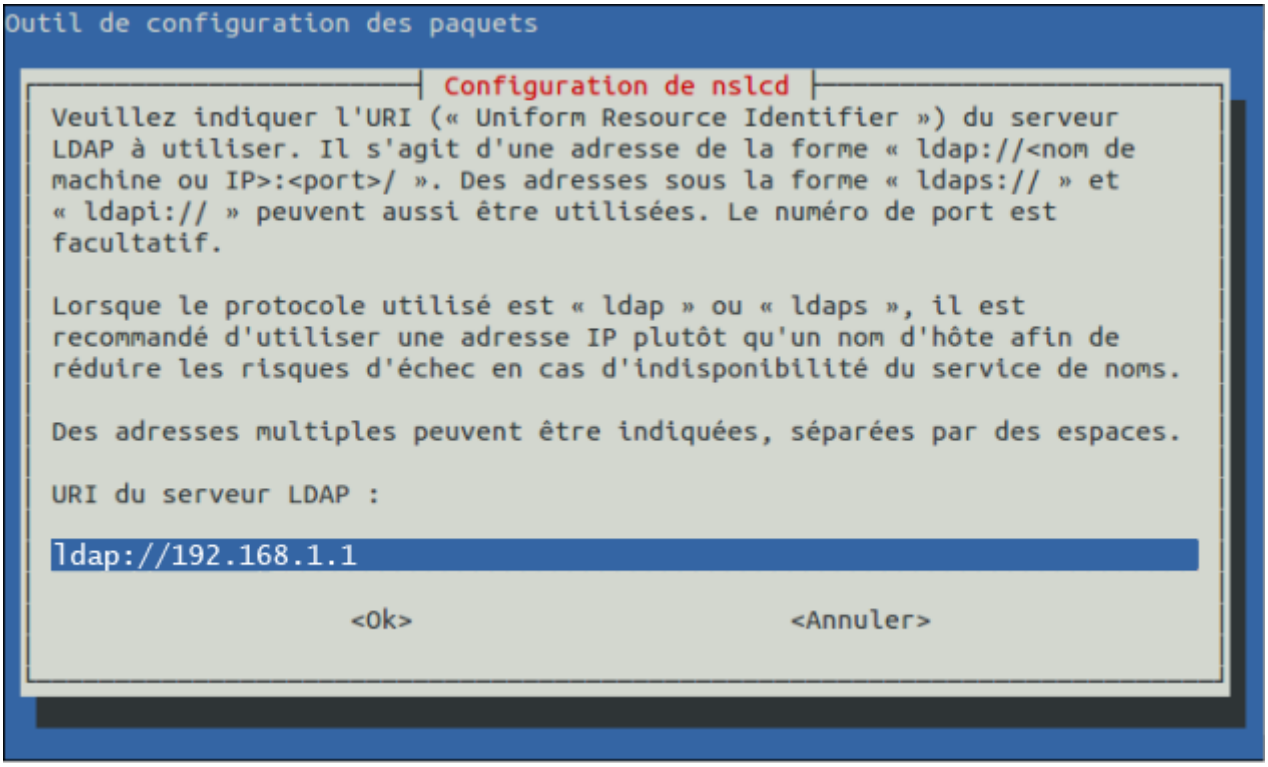
En résumé, OpenLDAP est une solution puissante et flexible pour la gestion des identités et des ressources dans un réseau informatique. En tant que service d'annuaire open source, il offre une alternative économique et évolutive aux solutions d'annuaire propriétaires.

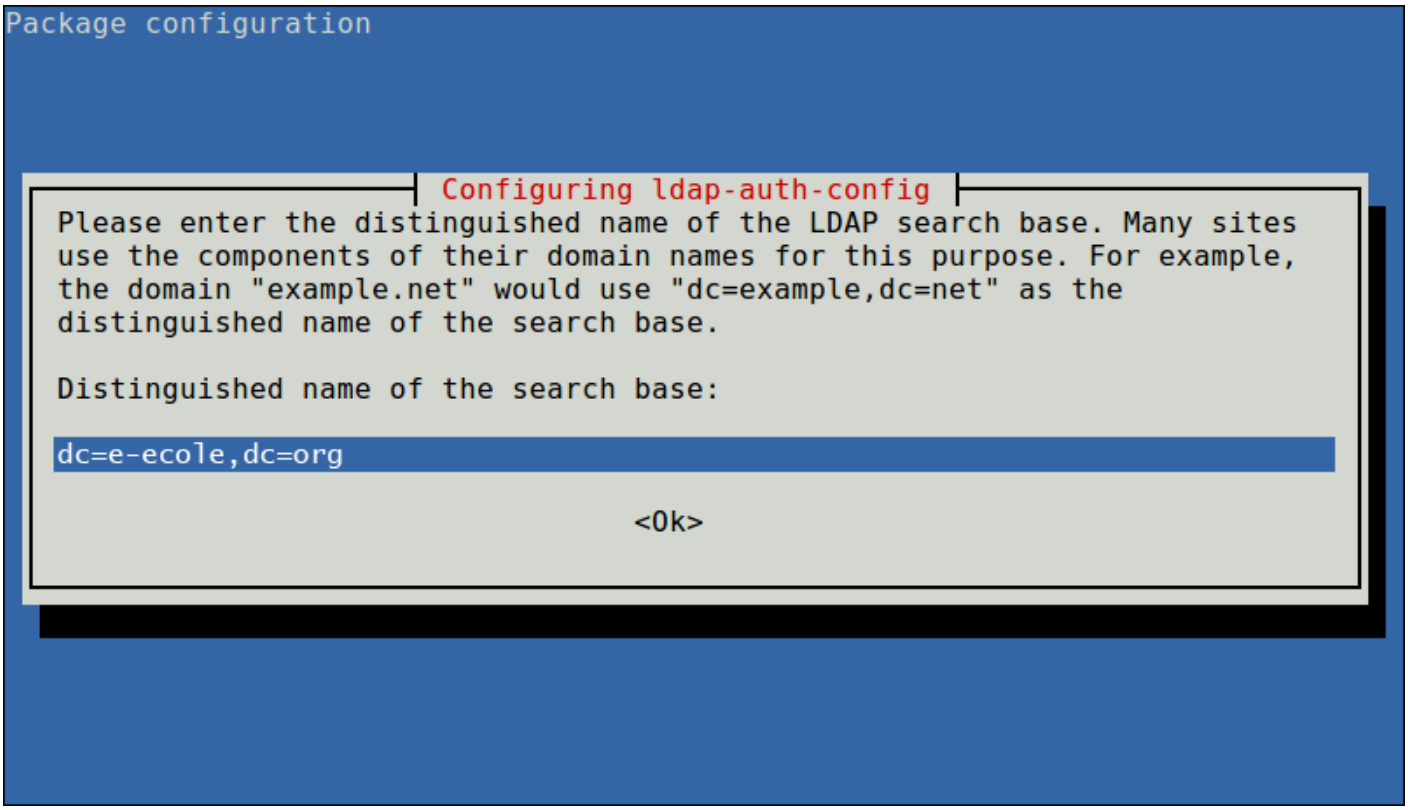
Installation

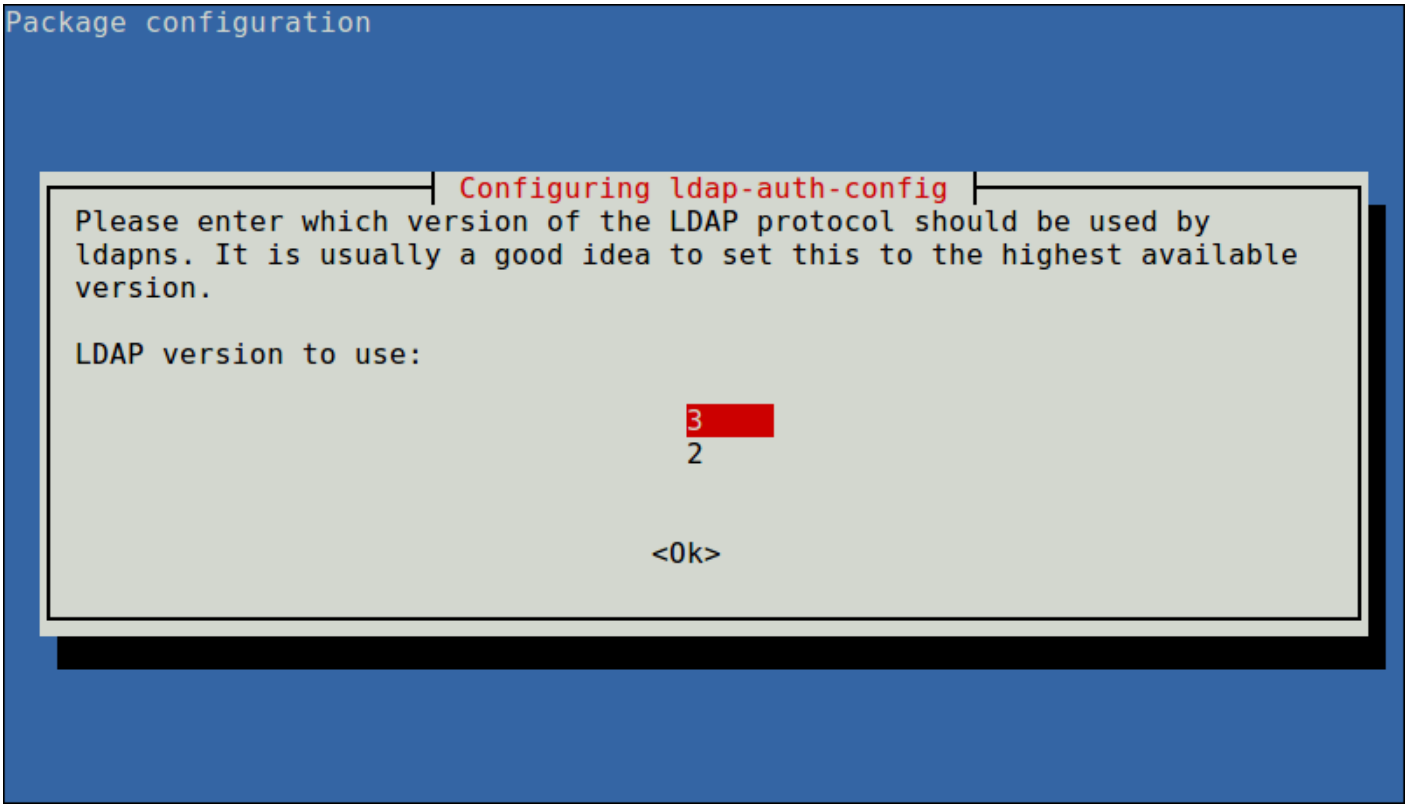
L'installation du client LDAP est un peu plus complexe que sur le serveur

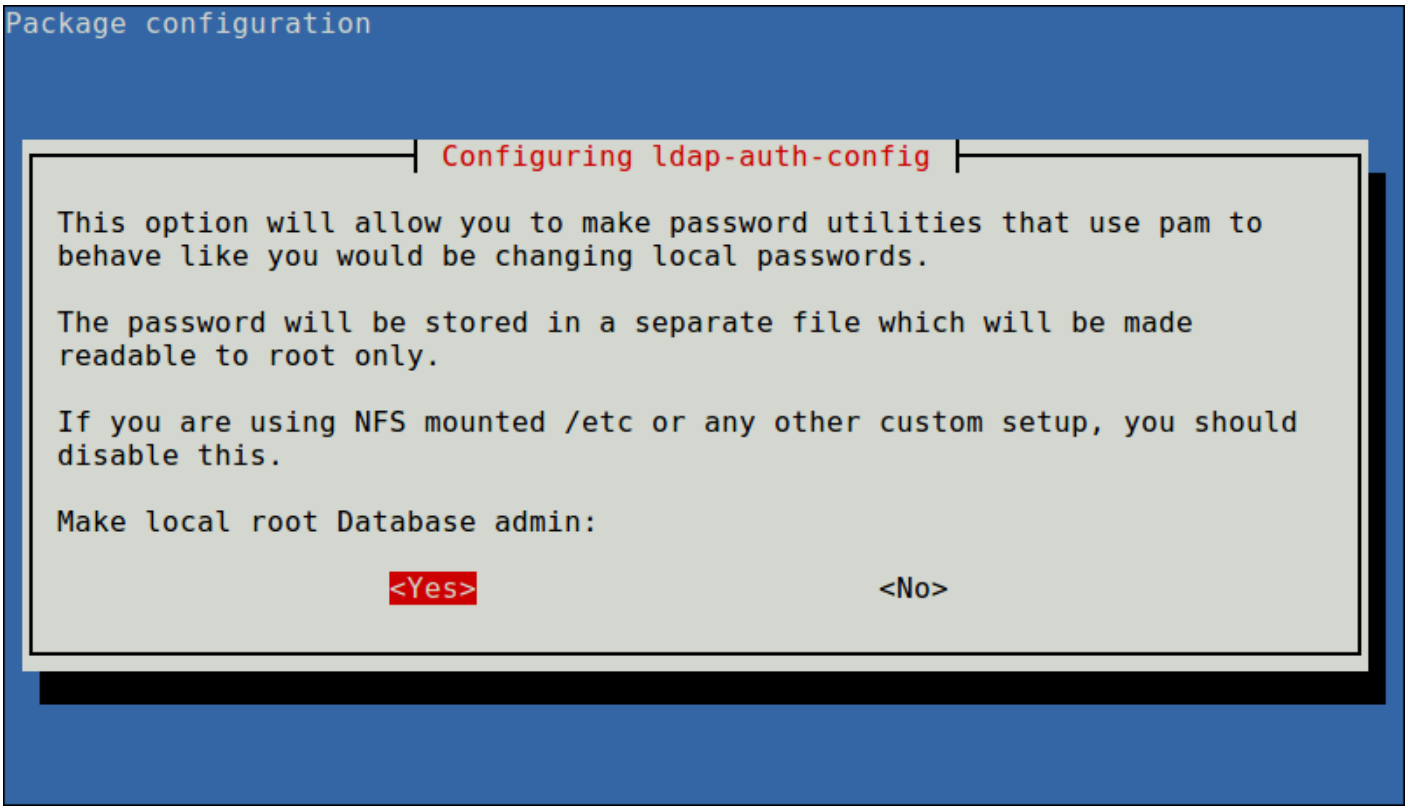
L'ajout des paquets via la commande :

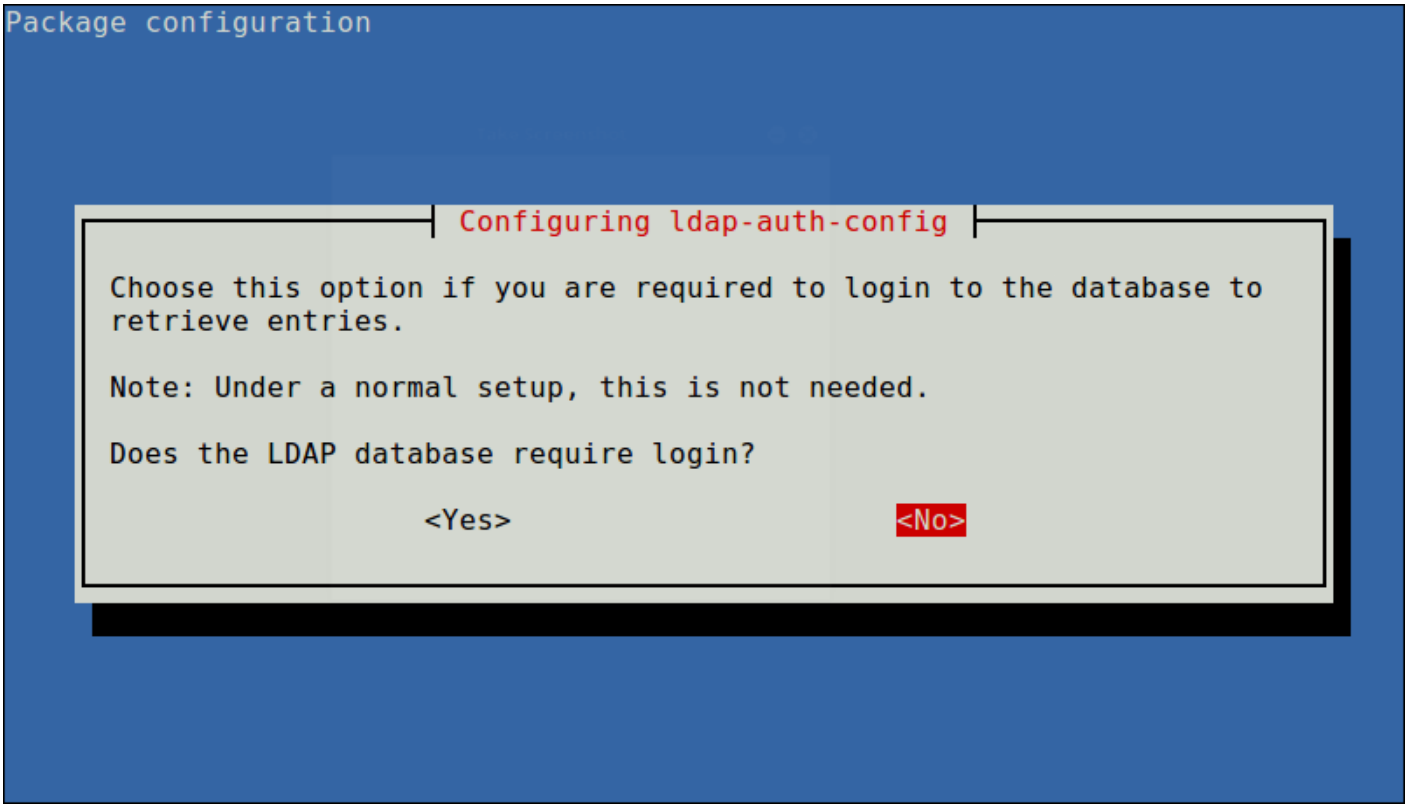
```
apt install libpam-ldap ldap-utils
```

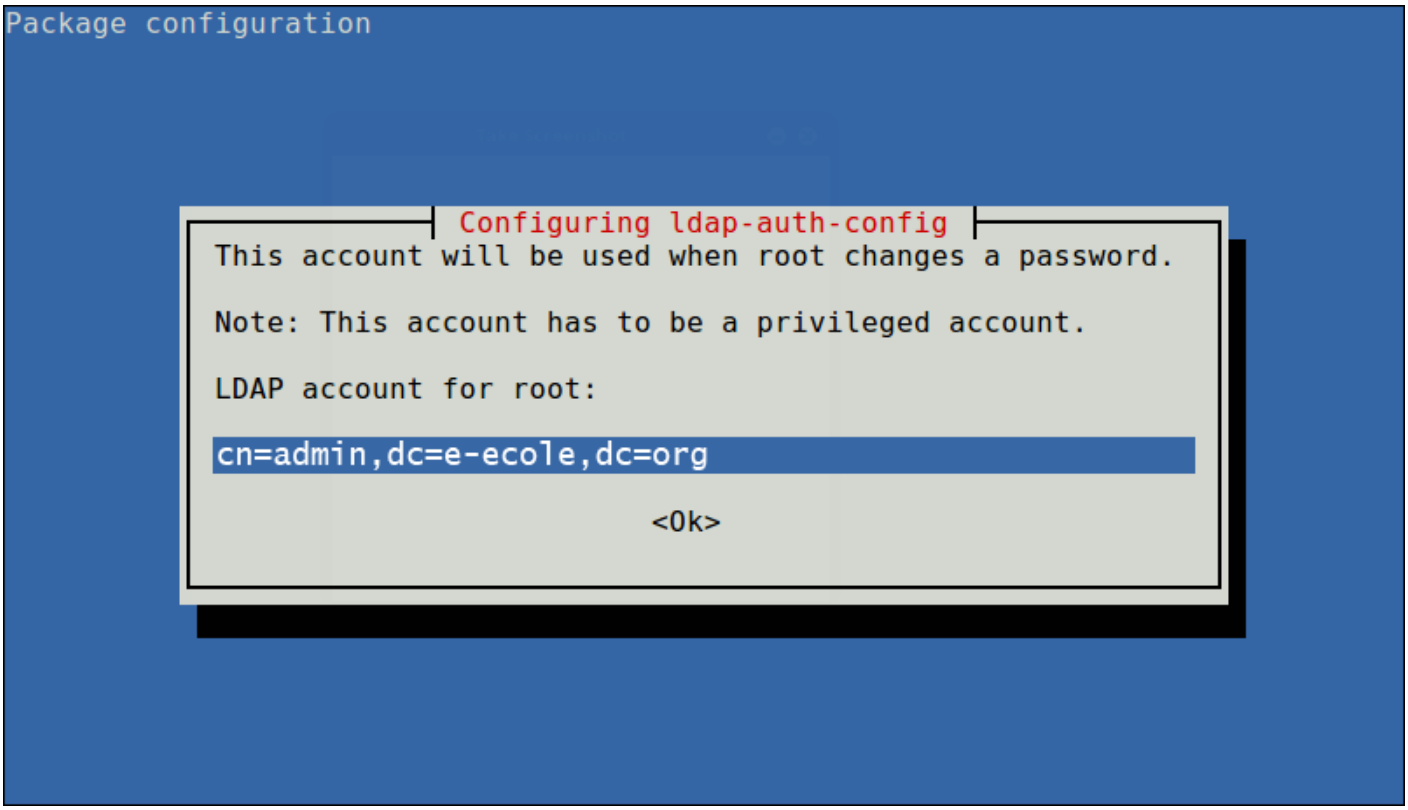


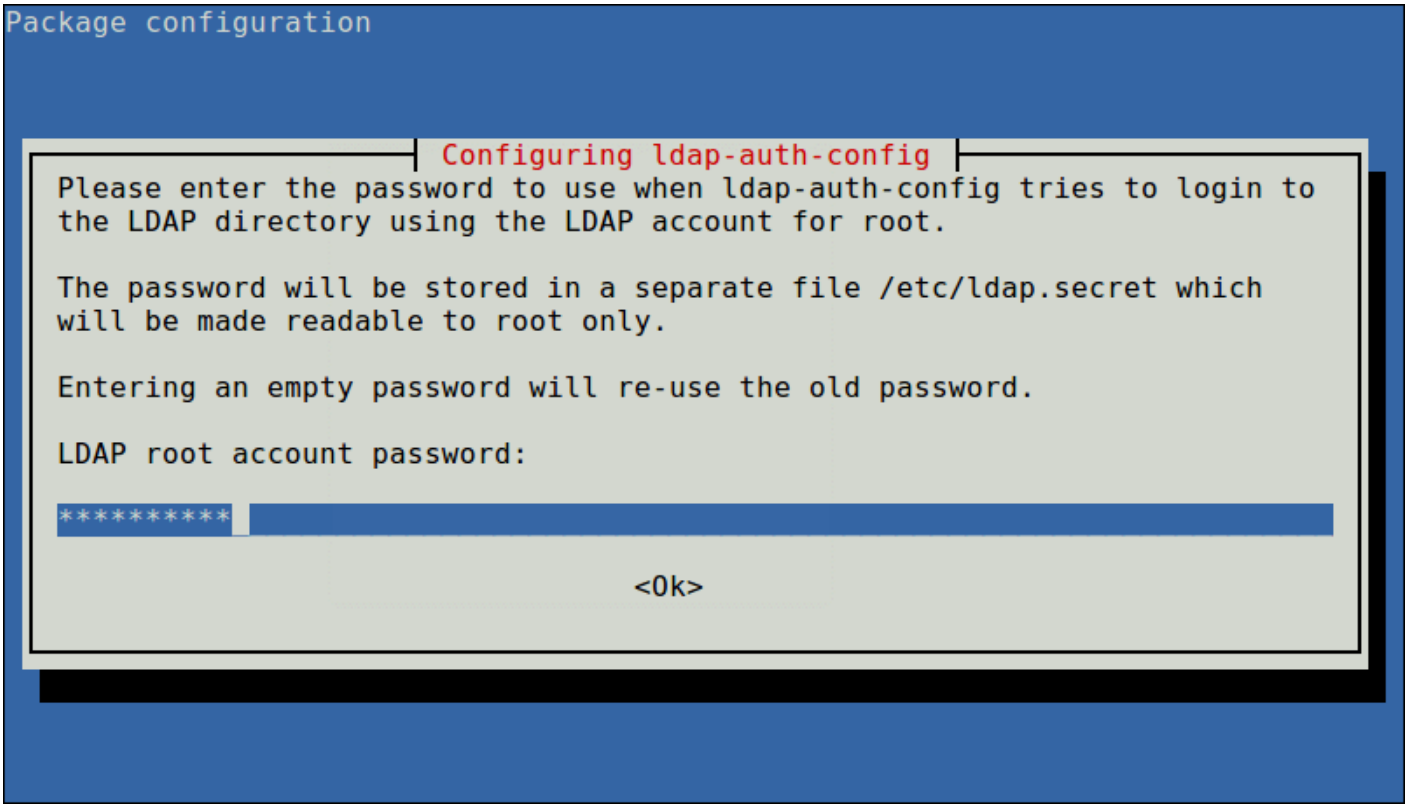

Package configuration
Configuring ldap-auth-config
Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.
Distinguished name of the search base:
dc=e-ecole,dc=org
<Ok>


Package configuration
Configuring ldap-auth-config
Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.
LDAP version to use:
3
2
<Ok>


Package configuration
Configuring ldap-auth-config
This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.
The password will be stored in a separate file which will be made readable to root only.
If you are using NFS mounted /etc or any other custom setup, you should disable this.
Make local root Database admin:
<Yes>
<No>


Package configuration
Configuring ldap-auth-config
Choose this option if you are required to login to the database to retrieve entries.
Note: Under a normal setup, this is not needed.
Does the LDAP database require login?
<Yes>
<No>





Il faut ensuite ajouter les paquets suivant :

```
apt install nscd nslcd
```

Identique au package précédent

Configuration

Comme pour le serveur, il faut éditer le fichier suivant :

```
nano /etc/ldap/ldap.conf
```

```
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=e-ecole,dc=org
URI     ldap://192.168.1.1

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

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

Une fois cela fait, la commande `ldapsearch -x` devrait donner des résulat similaire au serveur.

Un autre fichier à éditer :

```
nano /etc/nsswitch.conf
```

```
# /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 systemd ldap
group:          files systemd ldap
shadow:         files ldap
gshadow:        files
```

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

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

netgroup:       nis
```

Enfin, si un skel (modèle de session) doit être utilisé, il faut le préciser via le fichier :

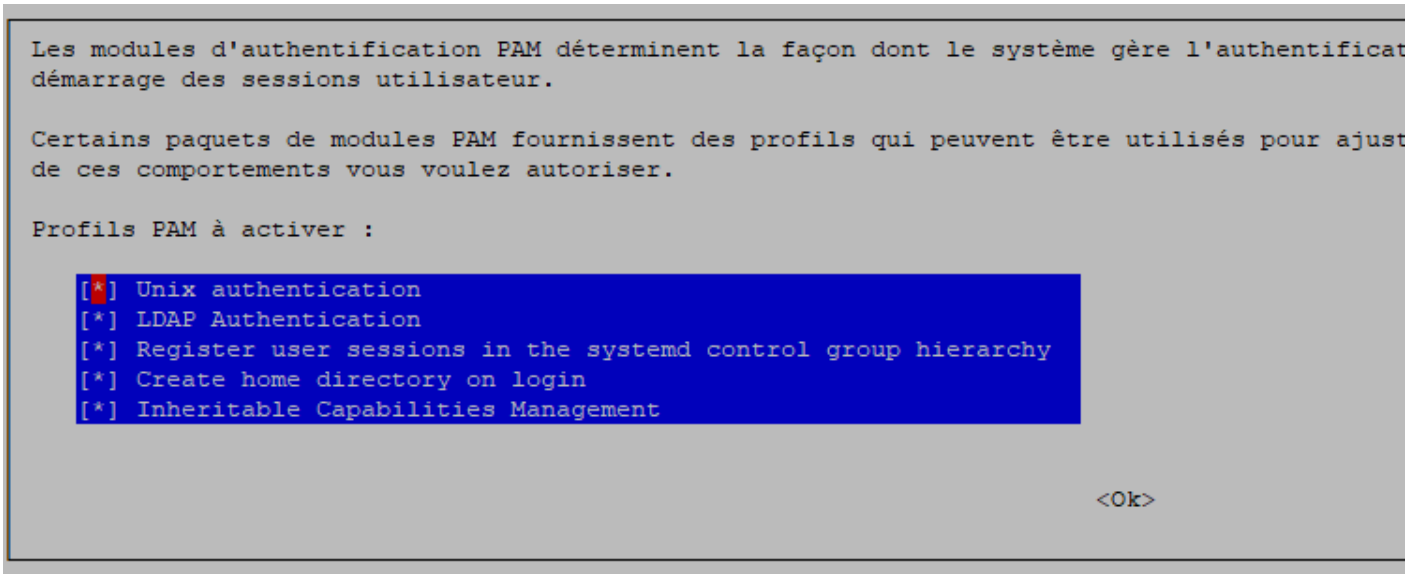
```
nano /usr/share/pam-configs/mkhomedir
```

```
Name: Create home directory on login
Default: no
Priority: 0
Session-Type: Additional
Session-Interactive-Only: yes
Session:
        required                        pam_mkhomedir.so skel=/etc/skel umask=0022
```

Une fois le fichier éditer, il faut mettre à jour la configuration :

```
pam-auth-update
```

et cocher les options comme suit :



La partie configuration des fichiers est terminée, il faut maintenant actualiser :

```
service nscd restart
service nslcd restart
```

Pour vérifier si la configuration fonctionne, utiliser la commande :

```
getent passwd <login user ldap>
```

> Si vous avez un retour, c'est que la configuration fonctionne, autrement, c'est qu'il vous manque quelque chose.

Une fois la configuration terminée, il suffit de quitter via `exit`, et update l'image via `ltsp image edubuntu`.

Revision #1
Created 2025-10-29 12:36:03 UTC
Updated 2025-10-29 12:36:07 UTC